جامعة أبي بكر بلقايد/ تلمسان
كلية الحقوق والعلوم السياسية

أطروحة دكتوراه تحت عنوان

جرائم الأنترنت
دراسة مقارنة

من إعداد الطالبة:
هروال هبة نبيلة

تحت إشراف:
أ.دكتور: قلفاط شكري

لجنة المناقشة:

أ.د. بوعزة ديدن	أستاذ التعليم العالي	جامعة تلمسان	رئيساً
أ.د. قلفاط شكري	أستاذ التعليم العالي	جامعة تلمسان	مشرفاً ومقرراً
أ.د. بوسندة عباس	أستاذ التعليم العالي	جامعة سيدي بلعباس	مناقشاً
د. محي الدين عبد المجيد	أستاذ محاضر "أ"	جامعة سيدي بلعباس	مناقشاً

السنة الجامعية 2013_2014

إهـــــــداء

كن عالما أو متعلما أو مستمعا ولا تكن الرابع فتهلك.

ما مات عالم ترك علما يتداول فتعاطيه إنفاق له، وصدقة جارية يجزى بها.

إلى روح المغفور له الدكتور مامون عبد الكريم الذي شاءت الأقدار أن يرحل إلى جوار ربه قبل أن يرى ثمرة إشرافه وتوجيهاته.

عن كل المجهودات التي أفادنا بها و النصح الذي أسداه لنا حتى تخرج هذه الرسالة إلى النور.

طيب الله ثراه و أسكنه فسيح جنانه وجزاه عنا وعن طلبته خير الجزاء .

تشكـــــرات

قال الله تعالى **"فاذكروني أذكركم وأشكروا لي أشكركم"** الآية 152 من سورة البقرة

الشكر هو الكلمة الطيبة أصلها ثابت وفرعها في السماء، يلجأ إليها الإنسان حينما يثقل كاهله عظيم الإحسان، و إذا كان الاعتراف بالحق فضيلة، فإن إسداء الشكر لمستحقيه فضيلة، لقوله صلى الله عليه وسلم "من لم يشكر الناس لم يشكر الله"

ومن هذا المقام لايسعني إلا أن أتقدم بأسمى آيات الشكر و التقدير و العرفان والاحترام إلى الأستاذ الدكتور قلفاط شكري لما أولاه لي من شرف قبول الإشراف على هذه الرسالة رغم كثرة مشاغله، فشملني بعلمه الغزير وخلقه الرفيع وفضله الوفير فأضاء لي طريق البحث و ساعدني على التقدم فيه وحببني فيه بعطف الوالد وتواضع العلماء وكان لتوجيهاته السديدة الأثر البالغ في إثراء هذه الرسالة على النحو الذي نأمل أن تكون عليه، فهو خير معلم ونعم الأستاذ فله مني جزيل الشكر ووافر التقدير و الاحترام، جعله الله ذخرا لطلبته ومتعه بموفور الصحة و العافية، وأحاطه برعايته، نسأله عز وجل أن يجزيه عنا خير الجزاء وبارك له في وقته وعمله.

كما لا يفوتني أن أتقدم بأسمى آيات الشكر و التقدير و العرفان و الاحترام للأساتذة الأفاضل أعضاء لجنة المناقشة، و في مقدمتهم الأستاذ الدكتور بوعزة ديدن لتفضله قبول رئاسة لجنة مناقشة هذه الرسالة وهذا ما يزيدها قيمة ووزنا. وكذا الأستاذ الدكتور بوسندة عباس و الدكتور محي الدين عبد المجيد لقبولهما الاشتراك في المناقشة و الحكم على هذه الرسالة و لما بذلوه من جهد ووقت في قراءتها رغم كثرة أعبائهم.

وأسأل الله عز وجل أن ينفعني بملاحظاتهم التي ستزيد قيمة ووزنا و رونقا لهذه الرسالة، وكذا أن يمتعهم بالصحة ويحفظهم.

أهم المختصرات :

أ/ باللغة العربية:

ص: صفحة.

د: دكتور.

ج ر ع: جريدة رسمية عدد.

ب/ باللغة الأجنبية:

ATM : Automatic Transfer Machine.
Bull.crim : Bulletin de la chambre criminelle de la cour de cassation (de France).
CERN : Centre européen de recherches nucléaires.
Cass.crim : Cour de cassation, chambre criminelle.
CA : Cour d'appel.
Cal.Penal.code: Californie pénal code.
CRS : Centre de recherche sociopolitique.
Ch. : Chambre.
CSPA : Computer Systems Protection Act.
CFAA :Computer Fraud and Abuse Act.
Dr : Docteur.
DC :Dalloz critique.
DI :Droit intellectuel.
Doc: document.
D : Recueil Dalloz.
Doct : Doctrine.
d. :décret.
DP : Dalloz périodique.
éd : édition.
ENST : école nationale supérieure des télécommunications.
ECP : école centrale des Arts et Manufactures de Paris.
FATF : Financial Action Task Force on money laundering.
F: Feuillet.
GP : Gazette du Palais.
HADOPI : Haute Autorité pour la diffusion et protection des œuvres sur Internet.
IP : Internet Protocol.
INPES : Institut National de prévention et d'éducation pour la santé.
Ibid : Ibidem (au même endroit).
IEHEI : Institut européen des hautes études internationales .
INPES : Institut national de prévention et d'éducation en santé.

JCP: Juris classeur périodique.
LDP : Loi de protection des données.
LSD : Lysergique Acide diéthylamide.
LGDJ : Librairie générale de droit et de jurisprudence.
MDMA: Methyline Dioxy Methan Apletamine.
NWC : National White collar crime center.
n° : Numéro.
NSF.net : National sciences foundation net.
NTIC :Nouvelles technologies de l'information et de la communication.
OLPD : Ordonnance relative à la loi fédérale sur la protection des données.
OFDT: Observatoire Français des drogues et des Toxicomanies.
Op.cit : Opere citato (ouvrage cité).
OMPI : Organisation mondiale de la propriété industrielle (Genève).
P: Page(s).
PC: personal computer.
PUF :Presses universitaires de France.
PDF : Portable Document Format.
Réf: référence.
Rec. : recueil.
RDTI : Revue du droit des technologies de l'information.
RDIT :Revue de droit d'information et de technologie.
Rép.pénale.Dalloz : Répertoire Dalloz de droit pénal.
RSC : Revue de science criminelle et droit pénal comparé.
RD : Recueil Dalloz.
SET : Secure electronic transactions.
Somm : Sommaire.
Sec: Section.
TGI : Tribunal de grande instance.
USC : United State code.
VOL: volume.
& : et.

المقدمة

المقدمة:

شهد القرن العشرين غزواً تكنولوجياً و علميا هائلا أثر على كافة مجالات الحياة الاقتصادية والاجتماعية والسياسية، مغيرا في ذلك سير حياة المجتمعات المتقدمة منها والنامية. إذ أصبحت تلك الأخيرة، تشهد ثورة من نمط جديد و فريد ومميز و مختلف لم يسبق للبشرية معرفته في القرون السابقة[1]، والمعروفة بالثورة الصناعية الثالثة أو الثورة المعلوماتية[2] والتي أعلنت عن بزوغ فجر عصر جديد هو العصر المعلوماتي[3] المتميز والمنفرد من نوعه بمعجزات لم تشهدها باقي العصور. ومن أبرزها وأهمها استغلال الحاسبات الآلية والشبكات المتصلة بها حول المعمورة، ولاسيما تلك المعروفة بالانترنت كود النقل اللامتزامن[4]، و التي أثرت خاصة في مجال الاتصال والإعلام و قلبت موازينه، حيث استطاعت أن تجمع بين مختلف وسائل الإعلام فى وسيلة واحدة. فأصبح المستخدم يستطيع قراءة ومشاهدة وسماع كل ما يرغبه.وكذا التفاعل مع هذه الشبكة العجيبة، بتجوله من بلد إلى آخر، ومن شبكة إلى أخرى و بدون قطع تذاكر سفر من الجزائر إلى مصر أو إلى لندن أو واشنطن أو إلى أي مكان فى المعمورة، وهو جالس على كرسيه فى مكتبه أو غرفته وأمام كمبيوتره المرتبط عبر الهاتف بالأقمار الصناعية بشبكة الشبكات (الإنترنت). أي أنها حولت عالمنا هذا إلى مجرد قرية صغيرة بدون حواجز يتبادل الناس فيها أخبارهم و يبدون آراءهم و تعليقاتهم بكل حرية ويحصلون فيها على أية معلومات يريدونها بسرعة فائقة وبدون أي عناء مستغنين فى ذلك عن كثير من التقليديات.[5] و مغيرة بذلك مجتمعاتنا إلى مجرد عالم شفاف نرى فيه بيوتنا عارية، ومعلوماتنا المالية

---

[1]– لقد شهدت البشرية في القرون الماضية ثورتين غيرتا وجه التاريخ وطبيعة الحياة، هما الثورة الزراعية والصناعية.

[2]– لقد أطلقت عدة تسميات عن الثورة التي أفرزها التطور التكنولوجي و العلمي كتسميتها بالثورة الثالثة أو الموجة الثالثةأو ثورة تكنولوجيا المعلومات. ينظر على التوالي: د/ محمد محمد الألفي: بعض أنماط جرائم الإنترنت، ورقة عمل مقدمة في دورة الجوانب القانونية والفنية في المعاملات الالكترونية في الفترة من 08 – 2012/04/12 بكلية الحقوق، جامعة القاهرة، ص2. د/ محمود صالح العادلي: الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية، http:// dreladly.com

[3]– يطلق على ذلك العصر كذلك تسمية عصر ثورة المعلومات أو مجتمع المعلومات ويرجع الفضل في هذه التسمية الأخيرة إلى المفكر الأمريكي "ألفين توفلر" لمزيد من التفاصيل ينظر د/ طارق ابراهيم الدسوقي عطية: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009، ص11.

[4]– لقد اختلفت التسميات التي أطلقت على الإنترنت ما بين "الشبكة العالمية الالكترونية" أو " شبكة الشبكات" أو "الشبكة الأم" أو "الفضاء السيبراني" أو "الشبكة العنكبوتية" أو "طريق المعلومات فائق السرعة" أو "الطريق السريع الرقمي". ينظر في ذلك على التوالي: د/ إسماعيل عبد النبي شاهين: أمن المعلومات في الإنترنت بين الشريعة والقانون، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000، ص3. د/ السيد عتيق: جرائم الإنترنت، دار النهضة العربية، القاهرة، 2000، ص25.

[5]–المقصود من التقليديات: الصحف اليومية، والمجلات، وكذا النقود السائلة. إذ تم الاستغناء عنها بما تقدمه شبكة الشبكات اليوم من خدمات، أضف إلى ذلك ظهور التعاقد عبر الإنترنت؛ وكذا ظهور البطاقات الائتمانية... الخ.

واجتماعاتنا وحالتنا العقلية والجسمانية أمام أي مشاهد عابرة[1]. ومحوّلة إنسان القرن الحادي والعشرين إلى مواطن عالمي[2].

و تعرف الإنترنت لغة بأنها كلمة جديدة فى القاموس اللغوى لمختلف لغات العالم. وهى كلمة إنجليزية مركبة ومختصرة من مقطعين (inter) وهى اختصار (International) وتعني دولى، و (net) وهى اختصار لكلمة (net work) والتى تعني الشبكة.

وبجمع الكلمتين أي international network، فإن المعنى الكامل المتحصل عليه هو الشبكة الدولية.[3]

و هي تعرف وفقاً لمعجم الإنترنت والمعلوماتية هى: "شبكة عالمية تجمع بين وسائل الاتصالات والحواسيب، وهى مخصصة لتبادل البريد الإلكترونى للمعلومات المتعددة الوسائل والملفات، وهى تشتغل وفقاً لبروتوكول مشترك، يسمح بسيرورة إرسال الرسائل المنقسمة إلى طرود مستقلة".[4] كما تعرف الانترنت بأنها الشبكة المعلوماتية الدولية[5].

أما فقها فقد تعددت تعريفات هذه الشبكة، و يمكن حصرها فى الاتجاهين التاليين[6]:

الاتجاه التقنى فى تعريف الإنترنت و الذي يعتبر أن الإنترنت ظاهرة تقنية صرفة، إذ يعرفها بأنها: شبكة تجتمع تحتها مجموعة من شبكات المعلوماتية المختلفة والتى يتم التبادل بينها باستخدام بروتوكول واحد (Tcp/ip) للبريد الإلكترونى والملفات والمعلومات والأداء وكذا بنوك المعلومات.[7]

والإنترنت وفقاً لهذا الاتجاه هى مصطلح حديث تماماً، إذ يرجح البعض من أنصاره سبب ظهورها إلى مبتكرى القاعدة الانفتاحية للإنترنت (Tcp/ip) العالمين الأمريكيين Bob Khan, Vint Serf وما نتج عن ذلك من ظهور بروتوكول"Internet protocol-ip"، وكذا برتوكول التحكم فى الإرسال "Tcp.

---

[1]- ينظر د/ هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1995، ص184.

[2]- د/ حسين الغافري، محمد الألفي: جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، 2008، ص4.

[3]- أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة: جرائم الحاسب الإلى والإنترنت، دراسة مقارنة، ط 1، دار وائل للطباعة والنشر، الأردن، 2001، ص 60.

[4] -Vocabulaire de l'informatique et de l'Internet، http:// www.oc-nancy-metz.Fr.

Internet: Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients destiné à l'échange de messages électroniques d'informations multimédias et de Fichiers. Il Fonctionne en utilisant un protocole commun qui permet: L'acheminement de poches de messages découpés en paquets indépendants ».

[5]-قاموس أطلس للطلاب، ط 1، دار أطلس للنشر، 2003، ص 576.

[6]- د/ عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004، ص32.

[7]-Internet: est un réseau permettant de relier entre eux plusieurs réseaux informatiques de types différents dans lequels s'échangent grâce à l'utilisation d'un protocole unique (Tcp/ip) du courrier (e-mail)، des fichiers (FTp)، des informations et opinions (newsgroups) ainsi que des banques d'informations (gopher-wais-web).Voir Definiton of internet، http:// www.futura-sciences.com; et La definition de l'internet , http://www.lyceeb.com.

"transmission protocol. ضف إلى ذلك فهى تتمتع – وفقاً لهذا الرأى – بشكل مميز من حيث كونها مفتوحة على العالم، إذ ليس لأحد سلطان عليها.

ولقد انبثقت عن هذا الاتجاه منظمات ذات اهتمام بالإنترنت، تبنت التعريف السابق، كمجلس الشبكات الفدرالية الأمريكية[1]. ولقد أخذ البعض من الفقه بذلك التعريف[2].

أما الاتجاه الثاني فيتمثل في الاتجاه التقنى الإنسانى ويأخذ به أغلب الفقه[3] ، وهو يهدف إلى رصد القيمة القانونية الإنسانية للإنترنت بوصفه التقنية الحديثة إلى جانب التقنية القديمة فى خدمة الإنسانية. ووفقاً لهذا الاتجاه فالإنترنت هى: "شبكة دولية فسيحة تسمح لكافة أنواع الحاسوب المشاركة فى الخدمات والاتصالات بشكل مباشر كما لو كانت كلها جهاز حاسوب واحد"[4].

وفى مقام الموازنة بين الاتجاهين السابقين، نرجح الاتجاه الثانى أى "الاتجاه التقنى الإنسانى" على أساس أن ذلك الاتجاه يجعلنا نقف على طبيعة وحقيقة الإنترنت. فالإنترنت هذه التقنية المتميزة هى من طبيعة "تقنية إنسانية" ناتجة عن اجتماع التقنية والمعلومات. كما أنها في الحقيقة هي وسيلة تواصل بين الشبكات إلى درجة اعتبارها "الشبكة الأم".

وانطلاقاً من هذا يمكن اعتبار الإنترنت بأنها: "شبكة عالمية دولية، ووسيلة من وسائل الاتصال والتواصل بين الشبكات، تجمع مجموعة من أجهزة الحاسب الآلى المرتبطة ببعضها البعض، إمّا عن طريق خطوط التليفون، أو عن طريق الأقمار الصناعية[5]. وتعمل وفقاً لبروتوكول وحيد (TCP/ IP)، وتقدم الإنسانية

---

[1]–Voir The Federal Networking Council: resolution dated، October 24، 1995، definition of internet, http://www.Fnc.gov.

[2]–لمزيد من التفاصيل ينظر: د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص35، د/ عبد الفتاح بيومى حجازى: الأحداث والإنترنت، دار الفكر الجامعى، الإسكندرية، 2004، ص19، محمد عبد الله منشاوى: جرائم من منظور شرعى وقانونى، بحث منشور فى الإنترنت على الموقع التإلى: http:// . minshawi.comwww.

–J. SOHIER: le guide d'exploration de l'internaute، Montèrial éd. Logiques، 1995، p. 26

[3]–ينظر على التوالي: د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص35 وما بعدها؛ د/ محمد فتحى عيد: الإنترنت ودوره فى انتشار المخدرات، بحث منشور فى أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص23؛ د/ مصطفى محمد موسى: دليل التحرى عبر شبكة الإنترنت، دار الكتب القانونية، 2005، ص95، د/إبراهيم الدسوقى أبو الليل: الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمى، جامعة الكويت، 2003، ص23 وما بعدها، د/ فريد عبد المعز فرح: التعاقد عبر الإنترنت، مجلة البحوث الفقهية والقانونية، تصدرها كلية الشريعة والقانون جامعة الأزهر، فرع دمنهور، العدد الثامن عشر، 2003، ص473؛ محمدأمين أحمد الشوابكة: جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة، عمان، 2004، هامش (1)، ص7؛ د/ عبد الرحمن بن عبد الله السند: الأحكام الفقهية للتعاملات الإلكترونية "الحاسب الإلى وشبكة المعلومات (الإنترنت)"، الطبعة الأولى، دار الوراق، 2004، ص33؛ د/ محمد فتحي عيد: الإنترنت، ماهيته و خدماته، الأمن و الحياة، العدد 242، السنة 21، سبتمبر/أكتوبر 2002، ص 41.

[4]–د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص35.

[5]–يمكن الاتصال بالإنترنت من خلال أربع وسائل وهى الاتصال المباشر وهو وسيلة تتيح الاتصال بشك لدائم ومباشر بشبكة بروتوكول التحكم فى النقل الخاصة بالإنترنت Tcp/ip.

جملة من الخدمات كالبريد الالكتروني[1] وتبادل المعلومات في منتديات الحوار و غرف الدردشة[1]..... أو هي بنك شائع من المعلومات ووسيلة اتصال مباشرة وأداة متعددة الوسائل.

الاتصال المباشر عند الطلب: يمكن الاتصال المباشر بالإنترنت باستخدام بروتوكول الربط بين نقطتين "PPP" وجهاز مودم متصل بكمبيوتر مقدم خدمة الإنترنت.

الاتصال الطرفى التليفونى: وهو يتم عن طريق الربط بأحد مقدمى خدمة الإنترنت.

الاتصال البريدى فقط: وهى وسيلة مسخرة لإرسال واستقبال البريد الإلكترونى فقط.

ينظر لمزيد من التفاصيل: د/ السيد عتيق، المرجع السابق، ص22 وما بعدها؛ د/ أحمد عبد الكريم سلامة: الإنترنت والقانون الدولى الخاص "فراق أم تلاقى"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000، ص3.

[1]– يمثل البريد الإلكترونى إحدى الميزات الرئيسية للإنترنت، وأكثر خدماتها انتشاراً واستخداماً فى جميع الشبكات المرتبطة بها. كما يعد هذا الأخير أول مكتشفات تقنية الإنترنت التى تم تحقيقها إذ يعود ميلاده إلى عام 1971 على يد المهندس الأمريكى "Ray Tomlison"، أى فى عهد Arpanet. وشهد أول انطلاقة له عام 1987 وبالضبط إلى الصين.ويشير مصطلح البريد الإلكترونى (E–Mail) إلى الجيل الثالث فى بث وتوزيع الرسائل. وهو يرمز له بالرمز @ المعروف باللفظ "A+". ولقد شاعت تسميته بين مستخدمى الإنترنت بـ: E–Mail. ويعطى الباحثون فى مجالات الاتصالات وبعض التشريعات (كالتشريع الأمريكى فى قانون الاتصالات الإلكترونية المقنن فى الموسوعة الفدرالية الأمريكية. كما عرفت الجريدة الرسمية الفرنسية الصادرة بتاريخ 2 ديسمبر 1997 و20 يونيو 2003 البريد الإلكترونى). وبعض القضاء عدداً من التعاريف والمفاهيم الخاصة بالبريد الإلكترونى و منها التعريف الذي يعطيها:

– تعريف ضيق ودقيق: "وهو تعريف مواز لعمل الناسخ الهاتفى (الفاكسميلى)؛ ورديف له فى عمله. فهو الجهاز أو المحطة المستخدمة فى دوائر البريد بطريقة الاستنساخ الإلكترونى طبق الأصل والإرسال عبر الخطوط الهاتفية للنبضات الرقمية (Digital Puls)، ملائمة للنقل الهاتفى. ثم تقوم المحطة الثانية المستعملة بالتحويل العكسى للإرشادات التشابهية إلى النبضات الرقمية التى تتحول إلى معلومات وثائقية فى الجانب الآخر".

– تعريف عام وشامل: ويعنى بالبريد الإلكترونى: "جميع تقنيات الاتصال التى تقوم بتناقل المعلومات عبر الوسائل الإلكترونية مثل:

التيليتكس أو نقل النصوص عن بعد.

الفاكسميلى أو الناسخ الهاتفى.

الفيديوتكس المتفاعل أو الفيوداتا.

المحطات الطرفية أو الطرفيات التى تكون بشكل حاسبات مايكروية (Micro–computer) أو بشكل محطة طرفية (Terminal) مستقلة أو مرتبطة بذاكرة (Memory)". ينظر على التوالي كلا من: د/ مصطفى محمد موسى، المرجع السابق، ص169؛ وليد الزيدى، المرجع السابق، ص20؛ د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص40؛ د/ عبد الفتاح بيومى جازى،المرجع السابق، ص23؛ د/ علاء عبد الباسط خلاف، المرجع السابق، ص156؛ د/ ربحى مصطفى عليان: البريد الإلكترونى، مجلة الأمن والحياة، العدد 234، السنة الحادية والعشرون، 2003، ص66.

– Une histoire de l'e–mail,http:// www.arobase.org

– Décision n° 2004–496 DC، 10 juin 2004 du conseil constitutionnel, http:// www.droit–tic.om.

– Brigite FILLON: la messagerie électronique sur Internet, http:// www.piaf.asso.Fr.

وترجع أصول هذه الشبكة إلى نظام اتصالاتي معلوماتي أمريكي طور بشكل سري في الستينيات لأغراض عسكرية. إذ شهد العالم ميلاد هذه التقنية الحديثة سنة 1969 على يد مجموعة مهرة من علماء التقنية العاملين فى وكالة الأبحاث والمشروعات المتطورة، أى إبان إطلاق مشروع Arpanet فى وزارة الدفاع الأمريكى، الذى كان يهدف إلى وضع القوات الأمريكية فى حالة تأهب قصوى داخل مراكز إدارة الصواريخ، خاصة فى حالة نشوب حرب نووية أو أى اعتداء عسكري عليها[2].

ولقد عرفت هذه التقنية أول اتصال لها يوم 21 نوفمبر 1969، وذلك عن طريق ربط جامعة سانتاباربرا (Santa Barbara) بكاليفورنيا بتلك المتواجدة فى ستانفورد (Stanford) بواسطة جهاز كمبيوتر متواجد فى جامعة لوس أنجلوس (Losengeles)[3].

ثم تطورت تلك الاتصالات لتصبح اتصالات دولية سنة 1973، وكان أول اتصال بشبكة Arpanet مع جامعة كلية لندن[4]. ولقد نتج عن هذه الاتصالات، اختراع بروتوكول (Tcp/ip) من قبل العالم الأمريكى Vitnon Lerf سنة 1974، كلغة محادثة مشتركة بين أجهزة الكمبيوتر[5].

وبمرور الزمن وزوال خطر الحرب، بدأت الدعوات[6] لنقل هذه التقنية للاستعمال السلمي إلى جانب العسكري، حيث انقسم المشروع Arpanet إلى شبكتين. احتفظت إحداهما باسمها وبالغرض الأساسى الذى أنشئت من أجله وهو خدمة جهاز المخابرات الأمريكية (CIA)، أما الثانية فسميت بـ Milnet وقد

---

[1]– يقصد بمنتديات الحوار والدردشة تلك الأماكن والساحات الإفتراضية للقاء والتحادث بين مستخدمى الشبكة من ذوى الاهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعة نقاش وتبادل للبيانات والمعلومات والأفكار حول موضوع أو قضية معينة. وتعتبر هذه الوسيلة الدافع الرئيسى لأكثر من 40% من مستخدمى الإنترنت، نظراً لما تتمتع به من مزايا وما تقدمه من خدمات. إذ أنها تعتبر نوع من الاتصال بين الناس والذى يقتصر على تبادل النصوص بين المتحاورين، ولذلك فهى نوع من الحوار الفكرى البحت. وإلى جانب نظام الدردشة على شبكة الإنترنت، هناك منتديات الحوار عن طريق المجموعة الإخبارية والتى تعتبر هى الأخرى وسيلة من وسائل الاتصال، إذ تقوم بجمع وتوجيه جميع الرسائل والمعلومات إلى ملقم خاص بكل منتدى أو مجموعة إخبارية، والذى تجرى من خلاله وتحت إشرافه ورقابته تلك الحوارات والنقاشات، وهذا ما يميزها عن القوائم البريدية . ينظر على التوالي: د/ محمد فتحى عيد، المرجع السابق، ص27.د/ عبد الفتاح بيومى حجازى، المرجع السابق، ص23.وليد الزيدى، المرجع السابق، ص21.

Dr/ Mohamed BUZABAR: La Criminalité informatique sur l'Internet، journal of Law، n°. 1, vol. 20, 2002، p 18. Jurisclasseur، communication، 2002، p. 24.

[2]–ينظر على التوالي: د/ عبد العزيز بن حمد الزومان: شبكة الإنترنت، دليل تعريفي، مكتبة الملك فهد الوطنية، الرياض، ص 5 و6؛ تاريخ الإنترنت، http:// www.marefa.org.

[3] – Voir Sandy RIHANA : Introduction à l'internet, p 4, http:// www.nachez.info.

[4]– Voir Yanis DELMAS : Histoire de l' informatique، d'internet et du web, http://Delmas-rigoutsas.nom.fr. ; Jean-Chrysostome BOLOT, Walid DABBOUS :L'Internet, Historique et évolution.Quel avenir prévisible?, p1 et suite, http:// planete.inria.fr

[5]– Voir Dr/ Mohamed BUZABAR،op cit، p. 15.

[6]– ويرجع الفضل فى ذلك إلى المرشح الجمهورى للرئاسة الأمريكية Albert ALGORE ، ينظر أسامة أحمد المناعسة،جلال محمد الزعبى ،صايل فاضل الهواوشة، المرجع السابق، ص61.

خصصت للاستخدامات السلمية المدنية. وظهرت إلى جانب ذلك شبكات أخرى عديدة تقدم جماعات ومؤسسات مختلفة مثل شبكة Bitnet (والتى تستخدم للاتصالات الأكاديمية)، وشبكة CSnet والتى تربط مجموعة من مراكز الأبحاث[1].

وفى عام 1985 تم نقل تشغيل Arpanet من إدارة الدفاع الأمريكى إلى شبكة مؤسسة العلوم الوطنية NSF Net. ومع بداية التسعينات، انتهت Arpanet لتتحول إلى Internet كتسمية جديدة، ولم تعد حينها مقتصرة على الأبحاث العسكرية والجامعية. بل تعدتها إلى الأعمال التجارية، فأصبحت بذلك فى متناول الجميع وخصوصاً عندما ظهرت شبكة المعلومات الدولية World Wide Web والتى يرمز لها بـ www أو W_3 على يد مهندس الاتصالات الإنجليزي Tim Berners Lee[2]، وانطلاقها من المركز الأوروبى للبحوث النووية CERN بجنيف. وكذا مع ظهور نوافذ جديدة Windows العالمية والمسماة بالفسيفساء Mosaic ومع ظهور "Nets cape"[3].

ومنذ ذلك التاريخ وعدد مستخدمي الانترنت في تزايد مستمر ومتواصل في العالم[4] لدرجة ظهور دولة جديدة تضمهم تسمى بدولة المتعاملين مع الانترنت، والتي يبلغ تعداد سكانها أكثر من حوالي 40 مليون مواطن يتزايدون بنسبة 5% شهريا[5] وهذا كله راجع لما تقدمه تلك الشبكة من خدمات بطريقة سريعة وسهلة وما تتميز به من صفات وخصائص فريدة من نوعها.[6]

---

[1]–منير محمد الجنبيهى، وممدوح محمد الجنبيهى: جرائم الإنترنت، دار الفكر الجامعي، الاسكندرية،2004 ، ص8.

[2]– لمزيد من التفاصيل عن التطور التاريخي للإنترنت ينظر د/ مدحت رمضان : جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000، ص 3 وما بعدها.

[3]– Voir Departement of computer science: A Brief History of the Internet, http// www.cs.ucsb.edu.

[4]– لمزيد من التفاصيل ينظر د/ محمد فتحي عيد: الإنترنت و دوره في انتشار المخدرات، أكادمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 25 و ما بعدها. وكذا د/ محمد فتحي عيد، (الإنترنت...) مرجع سابق، ص42 – 43. و لقد كشفت الاحصائيات العالمية أن إجمالي عدد مستخدمي الإنترنت في العالم العربي بلغ 38 مليون، حيث سجلت دولة الامارات أعلى معدل إنتشار وصل إلى 49.8 % من إجمالي عدد السكان، تلتها قطر بنسبة 34.8% و البحرين ب 34.7% . ينظر عطاف الشمري: عدد مستخدمي الإنترنت في العالم العربي يتجاوزون ال38 مليون مستخدم، جريدة الرياض،العدد 14983، 2 يوليو 2009،http:// alriyadh.com.

[5] – د/مدحت رمضان، المرجع السابق، ص 5.

[6] – تتميز شبكة الإنترنت بالعديد من الخصائص التي جعلتها في الوقت الحالي تتربع على عرش وسائل الاتصالات ومنها: طابع الحرية، افتراضية المجتمع، عابرة للحدود، وسيلة تواصلية، الإنترنت تستلزم المعلومات، رواج الاستعمال....لمزيد من التفاصيل ينظر: د/ محمد محمد الألفي،المرجع السابق،الموضع السابق؛ د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص40. أسامة أحمد المناعسة، جلال محمد الزعبى، صايل فاضل الهواوشة، المرجع السابق، ص63؛ محمد عبد الله منشاوى، البحث السابق،.http:// www.minshawi.com. د/ هلإلى عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،دراسة مقارنة،ط1، دار النهضة العربية، القاهرة،1997 ، ص17 وما بعدها.

أما بالنسبة للجزائر فظهرت الانترنت فيها لأول مرة عام 1993 عن طريق مركز البحث للمعلومات العلمية و التقنية. و ظهرت أولى شركات التزويد الخاصة في عام 1998 عند صدور المرسوم الوزاري رقم 265 لعام 1998 و الذي بموجبه أنهى احتكار خدمة الانترنت من الدولة و سمح للشركات الخاصة بتقديم هذه الخدمة، وارتفعت أعداد الشركات التي تزود الزبائن الى 18 شركة بحلول شهر مارس 2000.[1] و لقد بلغ عدد مستخدمي الانترنت فيها عام 2010 4.367.201 مستخدم[2]. و بلغ عام 2012 9 ملايين و قدرت نسبة استخدام الانترنت 29%.[3]

و تجدر الاشارة إلى أن هذه النسبة ترتفع بين فئة الشباب يحتل فيها المتعلمون الصدارة من جامعيين وطلبة الثانويات، كما أن النسبة الأكبر من المستخدمين تتمركز في ولايات الوسط. [4] و تحتل الجزائر المرتبة 58 في ترتيب الدول و ذلك حسب البيانات التي جمعها الإتحاد الدولي للإتصالات و إحصاءات عدد السكان[5]

ولكن ولسوء الحظ و بالرغم من الإيجابيات التي تقدمها تلك الشبكة إلا أنها أصبحت في ذات الوقت مرتعا و تربة خصبة لمريضي الأنفس من المجرمين في ارتكاب ما يشاؤون من جرائم غير مألوفة و متميزة عن تلك التقليدية تستخدم فيها الانترنت كأداة أو محلا لارتكابها تسمى بجرائم الانترنت.

فالانترنت يعد اليوم نظاما مفتوحا يستطيع أي شخص بلوغ ما يحتويه من خدمات عامة، يقدم بيانات ومعلومات هائلة تسهل الطريق الصعب و العسير الذي كان يعاني منه المجرمين في ارتكابهم جرائم عديدة و متميزة بكل هدوء و طمأنينة، جالسين وراء حواسيبهم في منازلهم أو مكاتبهم أو مقاهي الانترنت و بدون بذل أي عناء أو دفع أي تكلفة مادية، بالضغط فقط على لوحة مفاتيح الحاسوب المربوط بتلك الشبكة. فلقد أصبحت تلك الشبكة تستخدم كسلاح معلوماتي يشهر في وجه البشرية ويهدد ويضر مصالح المجتمعات وذلك بارتكاب أو تسهيل ارتكاب شتى أنواع الإعتداءات المعلوماتية التقليدية أو المستحدثة الواقعة على الأشخاص أو الأموال أو أسرار الدول المتقدمة منها أو النامية. وفي هذا الصدد تقول روى جودسون – خبيرة بالمركز الوطني الأمريكي للمعلومات– بأن "الجريمة أصبحت أكثر قوة بفضل التقنية الحديثة"[6]، ويقول الدكتور ديفد كارتر بأن "السلاح لم يعد في الوقت الحالي يمثل الدرع الواقي لحماية و اصيانة المصالح و الأموال بل أن هذه السلطة انتقلت إلى الأرقام و النبضات الاليكترونية...". [7] ويقول كولين روز

---

[1]– لمزيد من التفاصيل ينظر الإنترنت في الجزائر ،http://www.wikipédia.org

[2]– ملحق: قائمة الدول حسب عدد مستخدمي الإنترنت، http ;//www.wikipédia.org

[3]– عدد مستخدمي الإنترنت في الشرق الأوسط و شمال إفريقيا،http://youtube.com

[4] – عادل راوتي : 60% من مستخدميها شباب، الإنترنت تتفوق على مصادر الخبر،الاذاعة الجزائرية، radioalgérie.dz http:// .

[5] – ملحق: قائمة الدول حسب عدد مستخدمي الإنترنت http://www.wikipédia.org

[6] – آمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، الجزائر، 2006، ص6

[7] – د/ عفيفي كامل عفيفي: جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، الطبعة الثانية، بدون دار نشر، 2000، ص 4.

بأن "جرائم الانترنت أصبحت تحتل المرتبة الثالثة من حيث الخطورة و التهديد لمصالح الدول الكبرى المتقدمة بعد الأسلحة الكيماوية و البكتورولوجية و النووية".[1] ولكن و في المقابل هناك حالات تكون فيها تلك الأخيرة محلا لارتكاب الجريمة، أي هدفها وغايتها (الضحية) و ما أكثرها. ويسمى النوع الأول من هذه الإعتداءات بالإجرام غير المعلوماتي على شبكة الانترنت، أما الثاني فيسمى بالإجرام المعلوماتي على هذه الشبكة و الذي يندرج تحته نوعان من الإعتداءات، اعتداءات منطقية كإرسال الفيروسات و القنبلة المعلوماتية و الدودة المعلوماتية.... [2]، و اعتداءات مادية كالاعتراض المتعمد للبيانات و التشويش والتفخيخ... [3]

وبالرغم من أن هذا النوع من الإعتداءات خطير ويهدد عالمنا و يضر مصالحه جراء النتائج الوخيمة اللاحقة عنه، و لكنه ليس أخطر من النوع الأول و التي تكون فيه الانترنت أداة لارتكاب الجريمة أي الإجرام غير المعلوماتي على شبكة الانترنت. ذلك أن هناك جرائم عديدة و معروفة و غير معروفة سهلت هذه الشبكة ارتكابها بصورة سريعة و غير مرئية تكون ضحيتها إما الأشخاص أو أموالهم بل حتى الدول بزعزعة أمنها و استقرارها.

هذا من جهة و من جهة أخرى، فقد انعكست نتائجها و آثارها و مردودها على النسق القيمي و الأخلاقي لاسيما في الجرائم الإباحية.و مما يزيد من خطورة هذا النوع من الاجرام أنه لا يقتصر على تخريب الحواسيب المتصلة بالانترنت أي على الجانب التقني، بل تمتد من الحياة العامة لتخرتق الحياة الخاصة للأفراد سواء أكان ذلك في صورة الاطلاع على أسرارهم الشخصية أو المالية أو الفكرية وبدون استئذان. فهي تجعل حياة الفرد كالكتاب المفتوح يقرؤه من يشاء الصالح و الطالح، صاحب الخير و صاحب الشر. و بذلك تتجلى لنا خطورة هذا النوع من الإجرام العصري لجرائم الانترنت.

ولهذا ارتأينا حصر بحثنا هذا لتفصيل هذا النوع من الإجرام دون غيره، أي دراسة "**الإجرام غير المعلوماتي على شبكة الانترنت**".

لقد أصبح العالم اليوم يتكلم عن شبكة اتصال عالمية اشتهرت تسميتها بالانترنت لا تكتفي بنقل المواد المرسلة و استقبالها و إنما بانتقال الإنسان بكامل حواسه و دون أن يبرح من أحد طرفي الأرض إلى الطرف الآخر ليتصل و يتفاعل مع نظيره من هذا الطرف الأقصى. فأصبح صيحة العصر و لغة العالم الجديد.

ولكن و كما هو شأن كل اكتشاف أو اختراع جديد أدى الاستخدام المتزايد لشبكة الانترنت التي تعتبر إحدى عجائب هذا القرن إلى كثير من المخاطر تتمثل في إمكانية استغلالها كسلاح مدمر وفتاك قد تفوق

---

[1] – COLIN Rose: «La cybercriminalité est la troisième grande menace pour les grandes puissances، après les armes chimiques، bactériologiques، et nucléaires ». Mohamed CHAWKI: Essai sur la notion de cybercriminalité, IEHEI, juillet 2006, p2

[2] – لمزيد من التفاصيل ينظر وليد الزيدي، مرجع السابق ، ص 45 و ما بعدها

[3] – لمزيد من التفاصيل ينظر وليد الزيدي، نفس المرجع، ص51-52

قوته بعض الأحيان السلاح النووي من قبل نوعية معينة من المجرمين الفائقين الذكاء في مجال الحوسبة في ارتكاب جرائم مستحدثة أفرزها التقدم التقني و التكنولوجي، و ولدت نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة تسمى بجرائم الانترنت، و التي باتت تأثر سلبا و تهدد كلا من النسق القيمي و الأخلاقي و الشخصي و المالي للفرد بل حتى الدول. إذ استخدمت تلك الشبكة كوسيلة لارتكاب أصناف عديدة من الجرائم التقليدية و المستحدثة مثل جرائم النصب و الاحتيال وإساءة الائتمان و كذا الجرائم الإباحية و التعدي على الحياة الخاصة و الإرهاب و التجسس و المخدرات وغسل الأموال... أي أن هذا الفضاء المعلوماتي أصبح كالغابة، لا يحكمها قانون يجد فيه مريضي الأنفس مرتعا لضالتهم المنشودة في ارتكاب ما كان يصعب عليهم في السابق ارتكابه من أعمال إجرامية بكل طمأنينة و هدوء و ارتياح، و بدون بذل أي جهد عضلي أو دفع أي تكلفة مالية باهضة. وذلك من خلال البريد الاليكتروني و غرف الدردشة و التعرف العابر عبر الشبكة الدولية والمواقع الاليكترونية المنتشرة عبرها. و إزاء هذا الوضع الخطير وجب على القانون الجنائي أن يحافظ على مواكبته لهذه التطورات التكنولوجية التي تقدم فرصا واسعة لاساءة استخدام إمكانيات هذا الفضاء.إذ أنه لم يعد للجرائم التقليدية التي كانت ترتكب قبل ظهور الانترنت محلا للإعراب. أو بصيغة أخرى لم يعد لها نفس الوصف القانوني المألوف (سرقة أو اختلاس أو نصب) بذات المفهوم التقليدي، و لكنها تطورت مع تطور النظام القانوني العالمي أو الإقليمي. فاستهدفت جريمة السرقة و النصب بطاقات الائتمان.و تعدت جريمة الاختلاس نطاقها الإقليمي ليكون من السهل أن تمتد عمليات الاختلاس لبنوك في بقع أخرى و دولة ثانية....

ونظرا لأن موضوع جرائم الانترنت بصفة عامة و الإجرام غير المعلوماتي على شبكة الانترنت بصفة خاصة هو من المواضيع الحديثة و القليل البحث فيها فقها لاسيما في مجتمعاتنا العربية. حاولنا من خلال هذه الدراسة توضيح معنى هذه الجريمة المستحدثة المصنفة ضمن جرائم التقنية العالية، و كذا تبيان كيفية تأثير هذه الجريمة على حياة المجتمعات بصفة عامة وحياة الفرد بصفة خاصة و ما هي الجرائم التي تستخدم فيها تلك الشبكة كوسيلة لارتكابها.

ومن بين الصعوبات التي واجهتنا في إنجاز هذه الرسالة هي قلة المراجع التي تحسب على الأصابع لاسيما فيما يخص الفقه العربي. إذ أن هذا الأخير كثيرا ما يجملها مع جريمة الحاسب الآلي أو الجريمة المعلوماتية أو جريمة نظم المعلومات و يعتبرها تفيد ذات المعنى أو أنها مجرد اختلاف في المصطلحات. و لكن الأمر مختلف تماما لذلك، فهي تختلف بكثير عن مجموع هذه الجرائم و قد حاولنا تبيان ذلك في رسالتنا هذه داعين الله التوفيق.

و كما هو متعارف عليه فإن أي تطور تشهده الإنسانية يفرز جانبين إيجابي و آخر سلبي، و هو ما نتج عن التقدم التقني و التكنولوجي لاسيما في مجال شبكة الشبكات و غزوها للعالم في وقت قياسي مذهل و التي طغى فيها الجانب السلبي عن نظيره الإيجابي بإساءة إستخدامها و إستغلالها من طرف مجرمين محترفين يعتمدون على الذكاء دون العنف في إرتكاب أنماط جديدة من الجرائم المستحدثة و المتميزة عن تلك التقليدية عرفت بجرائم الانترنت؛الأمر الذي أدى إلى ظهور إشكالات قانونية تواجه رجال العدالة،

دعت الفقه والقضاء في بعض الدول إلى البحث عن حلول لها لكي يتمكن المشرع الجنائي من بناء أرضية واضحة لوضع قوانين تحد منها و تردع أي شخص يحاول ارتكاب أي نوع منها. و يمكن أن نجملها في: ماذا نعني بجرائم الانترنت؟ و كيف تستخدم هذه الشبكة كأداة للإضرار بالأشخاص و الأموال و الدول؟ و ما هي الجرائم التقليدية التي يمكن ارتكابها بواسطة هذه الشبكة و ما هي الجرائم المستحدثة التي ترتكب عن طريق هذه لأخير؟ ؛ و ما الفرق بين الجرائم التقليدية التي تقع عن طريق الانترنت و تلك التي تقع بدونها؟ ؛ وهل المنظومة الجزائية التقليدية كافية و قادرة للتصدي لمثل هذه النوعية من الجرائم المستحدثة في ظل قانون عقوبات وضع في وقت لم تكن فيه هذه الشبكة معروفة؟ وهل يتعين على المشرع بصفة عامة و المشرع الجزائري بصفة خاصة أن يتدخل لمواجهة هذا النمط من الإجرام المتميز و الخطير، بوضع قوانين خاصة به توائم البيئة التي ارتكب فيها. أم عليه الاكتفاء فقط بالإشارة إليه عن طريق تعديل قوانينه العقابية بضم نصوص جديدة تعاقب عليه؟ أو بصيغة أخرى هل يتضمن قانون العقوبات الجزائري نصوصا خاصة بهذا الاجرام أم لا؟ و هل الآليات الحديثة في قانون العقوبات بصفة عامة و في القانون الجزائري بصفة خاصة كفيلة بحماية الإستعمال اليومي للإنترنت؟ و هل التكييف القانوني للجرائم التقليدية هو ذاته الذي يطلق عليها إذا وقعت عن طريق الانترنت؟ وكيف يمكن أن يتصرف القاضي في ظل غياب تشريعي يعاقب على هذه الجريمة و في ظل تتقيده بقاعدة شرعية الجرائم و العقوبات و كذا عدم جواز القياس؟ .

و لقد اخترنا لدراسة هذا الموضوع الدقيق المنهج الاستقرائي و التحليلي و النقدي والمقارن.

استقرائي تحليلي و نقدي: و ذلك باستقراء النصوص القانونية لمختلف تشريعات العالم العقابية و بالأخص قانون العقوبات الجزائري وتحليلها واستخلاص النتائج منها و كذا في تعداد الآراء الفقهية و التعاريف و نقدها.

مقارن: وذلك بعقد مقارنة بين تشريعات الدول التي تناولت هذا الموضوع و التي كانت السباقة في إقرار نصوص عقابية مستحدثة تجرم و تعاقب على مثل هذه السلوكيات غير المشروعة الناتجة عن سوء إستغلال شبكة الإنترنت و بين غيرها من التشريعات لا سيما العربية السائرة في طريق النمو، و بالأخص المشرع الجزائري الذي واكب هذا التطور التكنولوجي – و خاصة المتعلق بظهور الإنترنت و إنتشار إستعمالها في كل مجالات الحياة – بمراجعة قوانين الجمهورية و ذلك بتعديله لقانون العقوبات الجزائري بإصداره عدة قوانين كالقانون رقم 04-15 المؤرخ في 10نوفمبر 2004 و الذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية و ذلك في القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 إلى 394 مكرر7 و الأمر 97-10 المؤرخ في 6 مارس 1997 المتعلق بحقوق المؤلف و الحقوق المجاورة و الذي ألغى أحكام المواد 390 إلى 394 من قانون العقوبات. و كذا بإصداره للقانون رقم 09-04 المؤرخ في 2009/8/5 و المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

و لدراسة هذا الموضوع إستندنا على خطة علمية حاولنا من خلالها الإحاطة بالموضوع قدر الإمكان فقمنا بتقسيمه إلى ثلاث أبواب منتهجين في ذلك التقسيم التقليدي للجرائم[1] و ذلك كالتالي:

باب أول تطرقنا فيه إلى الجرائم الواقعة على الأشخاص عبر الانترنت و قسمناه إلى ثلاث فصول تناولنا في كل فصل الجرائم التالية: جرائم البث العلني و جريمة الإعتداء على حرمة الحياة الخاصة و جريمة المطاردة و الجرائم الأخلاقية، وباب ثان سلطنا الضوء فيه على الجرائم الواقعة على الأموال عبر الانترنت و قسمناه كنظيره إلى ثلاث فصول و هي جريمة السرقة و النصب و الإعتداء على الملكية الفكرية، و جريمتي غسل الأموال و المخدرات، و الجرائم الواقعة على التجارة الإلكترونية. و باب ثالث تناولنا فيه الجرائم الواقعة على أمن الدولة عبر الانترنت و الذي بدوره قسم إلى فصلين يتمثلان في جريمة الإرهاب عبر الإنترنت و جريمة التجسس عبر الإنترنت.

و لكن و قبل التفصيل في تلك الأبواب كان من الضروري أن نبتدئ دراستنا هذه بفصل تمهيدي عرفنا فيه ماهية جرائم الانترنت. لأن الجرائم التي ستكون محل بحثنا ما هي في الحقيقة إلا نوع من جرائم الانترنت.

و أنهينا الدراسة بخاتمة تضمنت النتائج التي تم التوصل إليها و الإقتراحات و التوصيات التي توصلنا إليها.

---

[1]– لقد تضاربت الآراء لتحديد أنواع جرائم الانترنت وتعددت التصنيفات،فهناك من عددها بحسب موضوع الجريمة ، وأخر قسمهابحسب طريقة ارتكابها ، وقد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقتها بالجرائم التقليدية ، فاعتبر ان الصنف الأول يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة ، والصنف الثاني تضمن دعم الأنشطة الإجرامية ويتعلق الأمر بما تلعبه الشبكة من دورفي دعم جرائم غسيل الأموال،المخدرات ،الاتجار بالأسلحة ،واستعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات ،بينما يتعلق الصنف الثالث بجرائم الدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب ، بينما الصنف الرابع فتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف ،وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الانترنت، وأخيرا صنف الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها باي صورة طبقا لقانون حماية الملكية الفكرية . في حين عددت وزارة العدل الأمريكية عام 2000 في معرض تجديدها للمكاتب المحلية لإنفاذ القانون الفيدرالي المتعلق بجرائم الكمبيوتر دون أن تقوم بتصنيفها وهي: السطو على بيانات الكمبيوتر ، الاتجار بكلمات السر ، حقوق الطبع ، سرقة الأسرار التجارية ، تزوير الماركات، تزوير العملة ، الصور الفاضحة الجنسية ، واستغلال الأطفال ،الاحتيال، الإزعاج عن طريق شبكة الانترنت ، التهديد ، الاتجار بالمتفجرات أو الأسلحة النارية أو المخدرات وغسيل الأموال عبرالشبكة. بينما يذهب الاتجاه العالمي الجديد خاصة ما ورد بالاتفاقية الأوربية لعام2001 لجرائم الكمبيوتر والانترنت فقد قسمت هذه الجرائم الى :

1– الجرائم التي تستهدف عناصر المعطيات والنظم

2– الجرائم المرتبطة بالمحتوى بالكمبيوتر "التزوير والاحتيال".

3– "الجرائم المرتبطة بالمحتوى " الافعال الإباحية و الأخلاقية".

4– الجرائم المرتبطة بحقوق المؤلف والحقوق المجـــاورة.

الفصل التمهيدي:

ماهية جرائم الانترنت.

منذ الأزل و الجريمة جزء لا يتجزأ من سلوك الإنسان في المجتمع، حيث ندرة الموارد وحاجة هذا الأخير وأطماعه التي ليس لها حدود تجعل من تضارب المصالح و التناحر عليها سمة يتميز بها كل مجتمع بصرف النظر عن درجة ثقافته و تقدمه الاقتصادي و العلمي. وعلى الرغم من الجهود الحثيثة التي تبذلها كل دولة لمقاومة الظاهرة الإجرامية، إلا أن الإحصائيات تشير دوما إلى زيادة نسبة الإجرام في الغالبية العظمى من دول العالم، وخصوصا في القرن الأخير الذي شهد ثورة معلوماتية من نمط مميز. وما أفرزته تلك الأخيرة من جرائم مستحدثة[1]، لم يسبق أن عرفها العالم تتميز عن تلك التقليدية بحداثتها من حيث الأساليب و الأدوات المستعملة في تنفيذها وكذا في أسلوب ذلك التنفيذ[2].

ومن هذه الجرائم المستحدثة جرائم التقنية العالية[3]و بالضبط تلك المرتبطة بالانترنت.

والجريمة لغة: " كلمة مشتقة من الجرم وهو التعدي أو الذنب. وجمع الكلمة إجرام وجروم وهو الجريمة.

وقد جرم يجرم وإجترم وأجرم فهو مجرم و جريم"[4].

وهي طبقا للمفهوم الإجتماعي: " كل فعل أو إمتناع يتعارض مع القيم و الأفكار التي استقرت في كيان الجماعة"[5].

أما قانونا فهي: " كل سلوك إرادي غير مشروع، يصدر عن شخص مسؤول جنائيا، في غير حالات الإباحة، عدوانا على مال أو مصلحة أو حق محمي بجزاء جنائي"[6].

---

[1]– يقصد بالجرائم المستحدثة أنماط من الجرائم التي لم يألفها المجتمع في السابق، من حيث أسلوب ارتكابها و نوع الجناة فيها و حجمها. أو هي الجرائم المخطط لها و التي يستعين المجرمون عند تنفيذها من معطيات العلم الحديث مثل جرائم الإرهاب و المخدرات وجرائم الحاسوب الآلي و الإنترنت أو هي تلك التي يشترط لاستخدامها التقنية الحديثة لتسهيل تنفيذها وإخفاء معالمها. د/محمد الأمين البشيري:التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 8 و 9.

[2]– لمزيد من التفاصيل ينظر د/محمد الأمين البشيري، نفس المرجع، ص 9

[3]– تضم الجرائم المستحدثة: الجريمة المنظمة و جرائم التقنية العالية، و جرائم الإرهاب وجرائم عسل الأموال، وحوادث الطيران المدني. و تعتبر جرائم التقنية العالية High–Technology crime نتائج طبيعية لبيئة التقنية العالي –High Environment Technology التي يعيش فيها، و الذي يشكل الحاسب الآلي أساسها ينظر د/محمد الأمين البشيري، نفس المرجع، ص 4 و ص 85.

[4]– القاموس الجديد للطلاب،معجم عربي مدرسي ألفبائي، الطبعة 7، المؤسسةالوطنية للكتاب، الجزائر،1991، ص251.

[5]– لمزيد من التفاصيل، ينظر أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة، المرجع السابق، ص 80

[6]– د/ عبد الفتاح الصيفي: الأحكام العامة للنظام الجنائي في الشريعة الإسلامية و القانون، دار النهضة العربية، القاهرة، 2004، ص43، ينظر كذلك: عبد الله سليمان: شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول، "الجريمة"، ديوان المطبوعات الجامعية، 1996، ص 58 و ما بعدها، د/جلال ثروت: نظم القسم العام في قانون العقوبات، طبعة منقحة، دار الهدى للمطبوعات، الإسكندرية،بدون سنة طبع، ص 113 وما بعدها.

ولما كانت جرائم الانترنت تصنف ضمن الجرائم المستحدثة، أي من تلك الجرائم التي أعجزت كلا من الفقهاء ورجال القانون ودعتهم إلى تكثيف أبحاثهم و مؤلفاتهم للبحث عن نظرية عامة توفر الحماية الجنائية لشبكة الانترنت من جهة و لمستخدميها من جهة أخرى من الجرائم التي ترتكب عليها أو حيالها ويكونون هم ضحاياها بالدرجة الأولى.

ضف إلى ذلك استخلاصهم لعدم كفاية قواعد القانون الجنائي التقليدية بشقيه (العقوبات و الإجراءات الجزائية) لتطبيقها على الكثير من تلك الأخيرة (جرائم الانترنت) وقصورها التام على مواجهتها.

– ومن أهم الإشكالات القانونية التي يطرحها موضوعنا في هذا الفصل التمهيدي: ما المقصود بجرائم الانترنت ؟ ما الفرق بينها وبين ما يلتبس بها من مصطلحات ؟ وما هي خصائصه ؟

و للإجابة عن هذه الأسئلة ارتأينا تقسيم هذا الأخير إلى مبحثين كالتالي:

المبحث الأول: تعريف جرائم الانترنت وتطورها التاريخي.

المبحث الثاني: خصائص جرائم الانترنت و الفرق بينها وبين غيرها من الجرائم.

المبحث الأول:

تعريف جرائم الانترنت و تطورها التاريخي.

إذا كانت الثورة المعلوماتية التي شهدها العالم في القرون الأخيرة، قد ساهمت في تسهيل الحياة البشرية وتقدمها في جميع الميادين، وخصوصا مع ظهور الطريق السريع للمعلومات" الانترنت" وما يقدمه من خدمات جمة ومتميزة بسهولة الاستخدام من كافة فئات المجتمع، ضف إلى ذلك عالميته أي عدم الاعتراف بالحدود السياسية وتعديه للدول و الأقاليم...

و لكن بالرغم من كل هذه الخدمات و التسهيلات لم تنج هذه الشبكة من يد المجرمين المحترفين، إذ أصبحت أداة فتاكة لارتكاب جرائمهم أو محلا لها. وهذا ما أدى إلى ظهور نوعا جديدا ومميزا من الإجرام المهدد لمصالح المجتمعات والدول سواء المتقدمة منها أو النامية، وسواء على المستوى الوطني أو الدولي يسمى بجرائم الانترنت.

ولما كان هذا الأخير من المواضيع الحديثة و الخطيرة التي تشغل اهتمام الفقهاء و رجال القانون (من مشرعين و قضاة ورجال الضبطية القضائية...) حول فهم طبيعتها وأسبابها، وتجعل القانون الجنائي قاصرا وعاجزا عن مواجهتها و مكافحتها، كان من الواجب علينا تخصيص هذا المبحث لدراسة هذا النوع من الجرائم المستحدثة من حيث التطرق إلى النقاط التالية في المطلبين التاليين:

االمطلب الأول: تعريف جرائم الانترنت

المطلب الثاني: التطور التاريخي و إحصائيات حول جرائم الانترنت.

المطلب الأول:

تعريف جرائم الانترنت.

رافق التطور الهائل و السريع في استخدام شبكة الانترنت، تطورا آخر في تعدد وتنوع أساليب ارتكاب الجرائم التي تتم عن طريقها أو تكون هي محلا لها.

و نظرا لطبيعة هذه الجرائم و لحداثتها و قصور التشريعات الجنائية عن تناولها و بالتالي عجزها التام عن مواجهتها. كان لزاما علينا تحديد المقصود من هذه الجرائم المستحدثة و الخطيرة، و التي أصبحت تمثل هاجسا أمنيا أو شبحا يرعب كل مجتمعاتنا ودولنا على السواء.

ولقد خصصنا هذا المطلب لتحديد المقصود من تلك الجرائم و ذلك من خلال تقسيمه إلى ثلاث فروع، نتناول في الأول منها التعريفات المختلفة التي قيلت بشأنها من الناحية القانونية (رأي المشرع)، أما في ثانيها فتعرضنا فيه إلى التعريفات المختلفة من الناحية الفقهية، أما الفرع الثالث فخصصناه للتطرق إلى النقد الموجه لتلك التعريفات (سواء القانونية أو الفقهية)، ومن ثم اقتراح التعريف الذي يكون أقل عرضة للنقد. وذلك كما يلي:

الفرع الأول: تعريف جرائم الانترنت قانونا.

الفرع الثاني: تعريف جرائم الانترنت فقها.

الفرع الثالث: النقد الموجه لهذه التعريفات.

الفرع الأول: تعريف جرائم الانترنت قانونا.

لما كانت جرائم الانترنت من الجرائم المستحدثة و بالضبط من جرائم التقنية العالية، ولما كان قانون العقوبات في حالته الراهنة غير كاف وفعال بالدرجة المطلوبة والمرضية[1]، لمواجهة هذا الشكل الجديد من الإجرام، فإن كثيرا من رجال القانون يواجهون صعوبات جمة حول فهم طبيعته و دوافعه وخصائصه. وعلى هذا كان من الواجب علينا أن نخصص هذا الفرع لتحديد المقصود من جرائم الانترنت قانونا. فماذا يعني هذا الإجرام المستحدث من الناحية القانونية؟.

منذ عشر سنوات مضت لم يكن المشرع (سواء في البلدان العربية أو الغربية) يعبأ وعلى نحو جدي بانعكاسات استخدام شبكة الانترنت وغيرها من تطبيقات التقنية الحديثة، سواء كانت تلك الانعكاسات إيجابية (إبرام وتنفيذ وتسهيل المعاملات المدنية و التجارية عن طريق عقود تسمى بالعقود الإلكترونية وعن

---

[1]– يرجع سبب ذلك إلى أن نصوص قانون العقوبات و النظريات و المبادئ القانونية التي يتضمنها أو تقف ورائه، مورثوه بعضها من القرن 19 م حيث لم يكن ثمة فنيون وقتئذ و إنما أصحاب مهن و حرفيين، و هذا ما أدى إلى بطئها مقابل ما تشهده تقنية الإنترنت من سرعة التطور. ضف إلى ذلك حداثة جرائم الإنترنت و الحاسب الآلي. ينظر على التوالي: د/هشام فريد رستم: جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، العدد17، جوان 1995، ص 108. د/محمد الأمين البشيري، المرجع السابق، ص 89 وما بعدها.

طريق التجارة الإلكترونية...، تسهيل وتنفيذ مهام سلطات الدولة عن طريق ما يسمى بالحكومة الإلكترونية...) أو سلبية (ارتكاب الجرائم المستحدثة وبالضبط جرائم الانترنت). ونظرا لتفوق الجانب السلبي لهذه الانعكاسات على الجانب الإيجابي، أصبح من الضروري وضع قوانين عقابية تحكم وتواجه ظاهرة إجرام الانترنت. و الإشكال المطروح هنا هو: هل تناول المشرع في هذه القوانين العقابية تعريف جرائم الانترنت؟.

– تعد مسألة تعريف جرائم الانترنت من المسائل الشائكة التي تقف كحجر عائق أمام رجال القانون. إذ أنه وحتى الآن يصعب الاتفاق على وضع تعريف جامع مانع شامل لها.[1]

فهي كما قيل تقاوم التعريف[2]، والسبب في ذلك يرجع إلى أن التقدم العلمي و التقني في مجال الاتصالات وتكنولوجيا المعلومات و في شبكة الانترنت أفرز أنماطا مستحدثة من الجرائم الجديدة و الفريدة من نوعها ذات الطبيعة المعقدة من حيث طرق ارتكابها ووسائل كشفها وذات الطابع الدولي التي لم يكن للبشرية سابق عهد بها.[3]

و الأصل – كما هو متعارف عليه في القانون الجنائي– أن المشرع لا يعرف الجريمة لأن ذلك ليس من اختصاصه بل من اختصاص الفقه و القضاء (في بعض الأحيان). غير أنه وللضرورة الملحة يجد نفسه مضطرا إلى ذلك، إما لتحديد أركان الجريمة العامة أو الخاصة، أو تحديد السلوك الإجرامي المستحدث للجريمة.

و الشأن ذاته بالنسبة لجرائم الانترنت، فالمشرع لم يعرفها تاركا ذلك للفقه والقضاء كما سبق ذكره. ولكن بالرغم من ذلك نجد أن الاتفاقية الأوروبية بشأن الجريمة السيبرانية التي عقدت في بودابست عام 2001، تعتبر أن مصطلح جرائم الإنترنت يتناول النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكومبيوتر وباستخدام الشبكة العنكبوتية. وقد صنّفت هذه الجرائم إلى أربعة أنواع هي:

الجرائم ضد سلامة المعلومات وخصوصيتها، الجرائم ذات الصلة بالكمبيوتر، الجرائم المتعلقة بمحتوى الكمبيوتر، الجرائم التي تتعلّق بالعلامات التجارية والملكية الفكرية.

فأما النوع الأول فيشمل الافعال التالية: الدخول غير المشروع، التجسس على البيانات والمعلومات، الإعتراض غير القانوني للبيانات، التدخل في البيانات والمعلومات، التدخل في أنظمة الكمبيوتر وبرامجه.

---

[1]– و هذا ما أكدته قمة برلين، و ذلك كما يلي:

« Le sommet de Berlin ،relatif à la cybercriminalité n'aura permis de dégager qu'une seule certitude ، une définition universelle de la cybercriminalité et l'on peut même se demander si une entente sera un jour possible ». L'impossible définition universel de la cybercriminalité, http:// www.vilage – _justice.com

[2]– د/ محمد سامي الشوا: ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص 5.

[3]– تصريح د/ محمد شوقي، القاضي بمجلس الدولة و رئيس مجلس إدارة الجمعية الدولية لمكافحة الإجرام السيبراني بفرنسا في المقال المعنون بـ: جرائم الإنترنت... من الإباحية للإرهاب، المنشور بتاريخ 2008/08/12، www.moheet.com http://

بينما يشمل النوع الثاني الافعال التالية: الغش والإحتيال ذات الصلة بالكمبيوتر، استخدام الكمبيوتر للتزوير، سرقة الهوية.أما النوع الثالث فيتضمن الافعال التالية : وجود مضمون جنسي أو إباحي، وجود مواد إباحية ذات علاقة بالأطفال، وجود بيانات التحريض على العنصرية و الكراهية وتمجيد العنف، التعرّض للأديان، ألعاب القمار غير المشروعة والألعاب على الإنترنت، التشهير والمعلومات الكاذبة، ارسال البريد المزعج .أما النوع الرابع و الاخير فيضم الافعال غير المشروعة التالية: تبادل الأغاني والملفات والبرامج المحمية في حقوق التأليف والنشر من خلال برامج تبادل المعلومات، التحايل على نظم إدارة الحقوق الرقمية، إستخدام العلامات التجارية في أنشطة إجرامية بهدف التضليل، الجرائم ذات الصلة بإسم المواقع الإلكترونية.[1]

كما نجد أن النائب السيد جون مارك ناسم[2] قد قدم تقريرا – باسم لجنة الأعمال الخارجية –حول مشروع القانون رقم: 905 المجيز قبول نفاذ الاتفاقية الأوروبية المبرمة بشأن جرائم الانترنت عرف فيه مصطلح جرائم الانترنت بأنه "مجموعة الجرائم الجنائية المرتكبة عبر شبكة الانترنت، والتي تشمل ثلاثة أنواع مختلفة من الجرائم:

1: جرائم المحتوى،

2: المساس بالملكية الفكرية،

3: الجرائم المعلوماتية."[3]

هذا من جهة ومن جهة أخرى، نجد أن القانون الأمريكي قد عرف الجريمة المعلوماتية في القانون رقم 1213 لسنة 1982 الخاص بمواجهة الكمبيوتر و الجريمة المعلوماتية بأنها:"الإستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات، أو الإستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات. و تتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة"[4].

---

[1]– تم التوقيع على الاتفاقية الاوروبية حول جرائم الإنترنت في 2001/11/23 في بودابست/ المجر من قبل 30 دولة أوروبية بالاضافة إلى الدول الاربعة من غير الاعضاء في المجلس الاوروبي و المتمثلة في: كندا، و اليابان، و جنوب افريقيا، و الولايات المتحدة الامريكية، و هي تعد الاساس الاول لامكانية التعاون الدولي في المكافحة الدولية للجريمة عبر الإنترنت. لمزيد من التفاصيل ينظر د/ جورج لبكي: المعاهدات الدولية للإنترنت، حقائق وتحدّيات، مجلة الدفاع الوطني،ص3،http:// www.lebarmy.gov.lb، د/ عمر محمد أبو بكر بن يونس، المرجع السابق، 198 و ما بعدها.

[2]– النائب السيد جون مارك ناسم هو عضو بالمجلس الوطني الفرنسي.

[3]– La cybercriminalité peut se définir comme l'ensemble des infractions pénales commises sur le réseau d'Internet et elle correspond à trois catégories distinctes d'infraction:

Les infractions de contenu ،les atteintes à la propriété intellectuelle et les infractions informatiques.

M le député Jean-Marc NESME: Assemblée Nationale ،rapport fait au nom de la commission des affaires étrangères sur le projet de loi n° 905 autorisant l'approbation de la convention sur la cybercriminalité. 17/12/200,http://www.assemblee-nationale.fr

[4]– مقال جرائم الإنترنت، http://djelfa.info:

أما فيما يخص قانون العقوبات الكالفورني وقانون العقوبات لتكساس فقد عرفا جرائم الإنترنت انطلاقا من حصرهما لمجموعة من الأفعال غير المشروعة تدخل في نطاق هذه الجرائم.اذ نص القسم 502 من قانون العقوبات الكالفورني على اعتبار جريمة الانترنت:" كل فعل الدخول أو السماح بالدخول العمدي إلى نظام أو شبكة معلوماتية بهدف:

التخطيط و التنظيم لكل مخطط للاحتيال.

كسب الأموال و الخدمات من أجل الاحتيال.

تخريب أو تحطيم كل نظام، شبكة، برمجية، أو بيانات معلوماتية."

أما القسم 33.02 من قانون العقوبات لتكساس فنص على اعتبار جريمة الانترنت:" كل دخول إلى الحاسب الآلي، شبكة، أو نظام معلوماتي دون الحصول على إذن مسبق من صاحبه."[1]

هذا فيما يخص موقف المشرع الأجنبي حيال تعريف جرائم الإنترنت، أما بالنسبة لموقف المشرع العربي من هذا التعريف، فقد عرف المشرع الإماراتي في المادة الأولى من القانون العربي النموذجي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات الجريمة المعلوماتية دون جرائم الانترنت حيث نص على أنها: "كل فعل مؤثم يتم ارتكابه عبر أي وسيط إليكتروني"[2].و ذات الشأن بالنسبة للمشرع المصري اذ نجده عرف في المادة الأولى من القانون المصري النموذجي الجرائم المعلوماتية دون جرائم الإنترنت بأنها:" كل فعل يتم ارتكابه عبر أي وسيط إليكتروني و يقصد في تطبيق أحكام هذا القانون بالكلمات و العبارات الآتية....."[3].

أما المشرع السعودي فقد عرفها(الجريمة المعلوماتية) من خلال نظام مكافحة جرائم المعلوماتية بأنها:" كل فعل يرتكب متضمنا إستخدام الحاسب الآلي و الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".[4]

---

[1]– Le code pénal de Californie (section 502)définit une liste d'actes illicites qui tombent sous le coup de la cybercriminalité. Il considère comme cybercriminalité: « le fait D'accès ،ou de permettre intentionnellement l'accès à tout système ou réseau informatique afin:

a)– de concevoir ou réaliser tout plan ou artifice pour frauder ou extorquer.

b)–d' acquérir de l'argent, des biens, des services, dans le but de frauder.

c)– d'altérer, de détruire, ou d'endommager tout système, réseau, programme ou données informatiques ».

Le code pénal du Texas (section 33.02) considère comme cybercriminalité: « le fait D'accès à un ordinateur ،un réseau ،ou à un système informatique sans l'autorisation de son maitre ».Voir Mohamed CHAWKI, op.cit,p 9.

[2]– د/ عبد الفتاح بيومي حجازي: نحو صياغة نظرية عامة في علم الجريمة و المجرم المعلوماتي،الطبعة الأولى، منشأة المعارف،الإسكندرية،2009،ص14؛ ينظر كذلك د/عمر فاروق فحل: خطر الجرائم المعلوماتية الالكترونية، دراسة مقارنة، مجلة المحامون،سوريا، العدد4/3، السنة 72،ص314.

[3]– مقال جرائم الإنترنت، المنشور على الموقع السابق.

[4]– المادة 8/1 من نظام مكافحة جرائم المعلوماتية السعودي.

وعلى نفس النهج سار مشرعنا الجزائري، اذ لم يعرف جرائم الانترنت بل عرف الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال(الجرائم الإلكترونية) في المادة الثانية فقرة أولى من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، على النحو التالي:" يقصد في مفهوم هذا القانون بـ:

الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الاليكترونية".

و تجدر الإشارة إلى أن المشرع الجزائري لم يعرف جرائم الإنترنت في القانون رقم 15/04 المؤرخ في 2004/11/10 المعدل و المتمم لقانون العقوبات، بل عدد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و التي تعتبر جزء من ظاهرة إجرامية حديثة و خطيرة تسمى الجريمة المعلوماتية،

و اكتفى بالعقاب عليها ضمن الكتاب الثالث المعنون بالجنايات و الجنح و عقوبتها في الفصل الثالث المعنون بالجنايات و الجنح ضد الأموال في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر إلى غاية المادة 394 مكرر7.

الفرع الثاني: تعريف جرائم الانترنت فقها

لقد صك الفقهاء و الدارسون لظاهرة إجرام الانترنت عددا ليس بالقليل من التعريفات تتمايز وتتباين تبعا للمعيار الذي يستند إليه هؤلاء فيها فاختلفت بذلك تعريفاتهم و صعب الاتفاق على تعريف واحد جامع مانع شامل لها.

ويمكن تقسيم هذه الأخيرة إلى ثلاث فئات: فئة تستند في تعريفها إلى أداة ارتكاب الجريمة وأخرى ترجعه إلى أداة وموضوع الجريمة أي تجمع بينهما، وغيرها تعرفها وفقا لصفات الجاني الشخصية... الخ.

---

[1]– صدر القانون رقم04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها بتاريخ 5 أوت2009 . و يأتي هذا القانون لتعزيز نفس قواعد القانون رقم 04-15 المؤرخ في نوفمبر2004 المعدل والمتمم لقانون العقوبات و الذي نص على حماية جزائية لأنظمة معلوماتية من خلال تجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة الإفتراضية.

هذا من و من جهة أخرى، فهو يجمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية و بين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبيها.

و لقد تم اختيار عنوان"القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها"حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالاهداف و الغايات التي ترمي إليها التكنولوجيا كما أن التركيز على مجالي الاعلام و الاتصال بين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الاجرام و الوقاية منه.ينظر الأزرق بن عبد الله، أحمد عمراني: نظام المعلوماتية في القانون الجزائري،واقع و آفاق، ورقة مقدمة إلى المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، البيئة المعلومات الآمنة، المفاهيم و التشريعات و التطبيقات المنعقد بمدينة الرياض خلال الفترة 7 آبريل 2010،ص15.

أولا:التعريفات التي تستند إلى أداة ارتكاب الجريمة:

تعددت و تنوعت تعريفات أصحاب هذه الفئة، و لكنها إشتركت و اتفقت في نقطة واحدة ألا و هي أن جرائم الإنترنت أداة ارتكابها شبكة الإنترنت. فمنها من عرفها بأنها:"أفعال غير مشروعة ترتكب من خلال شبكة الانترنت إضرارا بالغير..."[1]، أو بأنها: "جميع الأفعال المخالفة للشريعة الإسلامية وأنظمة المملكة العربية السعودية المرتكبة بواسطة الحاسب الآلي، من خلال شبكة الانترنت ويشتمل ذلك الجرائم الجنسية، و الممارسات غير الأخلاقية، جرائم الإختراقات، جرائم المالية، جرائم إنشاء و ارتياد المواقع المعادية، جرائم القرصنة "[2]. أو بأنها: "مصطلح يقصد كل جريمة أو أسلوب إجرامي إليكتروني تستخدم فيه الانترنت كوسيلة لتنفيذه و يدخل من ضمن ذلك الجرائم المادية التي ارتبطت بأسباب ووسائل إلكترونية تمت عبر الانترنت مثل ترويج المخدرات و بيع السلع المسروقة عبر الانترنت" أو هي "أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثات و البريد الإليكتروني".[3] كما تعرف جرائم الانترنت بأنها "مجموعة الجرائم الجنائية المرتكبة عبر شبكة الانترنت"[4].أو بأنها "كل جريمة يرتكبها المجرم من خلال شبكة الانترنت."[5] أو بأنها: "جميع الأفعال المخالفة للقانون و الشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت."[6]

كما يعرفها البعض بأنها:"كل سلوك غير مشروع ناتج عن الربط بين الأنظمة المعلوماتية و شبكات الاتصالات "[7]. أو هي:" كل الجرائم التي ترتكب بالاستخدام غير المشروع و الاحتيالي للشبكات المعلوماتية وهي تضم:

- المساس بنظم المعلوماتية أو المعطيات المعلوماتية .
- إرسال حثالة البريد الإليكتروني أو جريمة تضخم البريد الإليكتروني (Spam).
- الإعتداء على حرمة الحياة الخاصة و المعطيات الشخصية.
- الاحتيال باستخدام بطاقة الائتمان.
- العنصرية أو النازية أو التصرفات المعادية.
- تبييض الأموال.

---

[1]– د/حسين الغافري، محمد الالفي،المرجع السابق،ص37.

[2]– محمد محمد عبد الله المنشاوي، البحث السابق المنشور على الموقع www.minshawi.com http://

[3]– أمير فرج يوسف: الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية،بدون سنة نشر، ص107 و113.

[4]–« la cybercriminalité, c'est l'ensemble des infractions pénales qui se commettent sur le réseau internet. »Voir la cybercriminalité, http://www.interieur.gouv.fr

[5]– حسن طاهر داود: جرائم نظم المعلومات،الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2000،ص40.

[6]– د/ عبد الفتاح مراد: شرح جرائم الكمبيوتر و الإنترنت، بدون دار النشر، بدون سنة نشر، ص40.

[7] –Mohamed CHAWKI, op.cit,p23.

– تنظيم مواقع الاستغلال الجنسي و مواقع الدعارة وكذا مواقع الإرهاب."[1]

ثانيا: التعريفات التي تستند إلى أداة ارتكاب الجريمة وموضوعها أو محلها:

يرى أصحاب هذه التعريفات أن جرائم الانترنت تتحقق في الحالة التي تكون فيها تلك الشبكة إما أداة لارتكابها أو محلا لها و منها:

إعتبارها "كل نشاط إجرامي تكون لشبكة الانترنت دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية ولا يختلف الأمر سواء تم النشاط عبر الانترنت أو كانت الشبكة وسيلة لارتكابه، ففي كلتا الحالتين ينبغي أن يكون لشبكة الانترنت دورا مؤثرا في إتمام النشاط الاجرامي"[2]. أو أنها "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر شبكة الانترنت أو تبث عبر محتوياتها".[3] أو بأنها:"هي تلك الأعمال غير المشروعة التي تكون شبكة الانترنت أو أحد تطبيقاتها إما وسيلة أو ضحية مستهدفة من قبل الفاعل أو الفاعلين"[4].

بينما يعرفها البعض الآخر بأنها:" كل اعتداء يقع على نظم الحاسب الآلي[5] وشبكاته أو بواسطتها."[6]

---

[1]–« sous le terme la cybercriminalité sont regroupées toutes les infractions commises par l'utilisation illicite ou frauduleuse des réseaux informatiques ;

–Atteinte aux systèmes d'information ou au données informatisées.

–Envoie de courriers commerciaux non sollicité (spam).

–Violation de la vie privée et des données personnelles.

–Fraude à la carte bancaire.

–Acte raciste ou néonazis.

–Blanchiment d'argent.

–Organisation de réseaux de prostitutions ou encore de réseaux de terroristes » . Voir l'harmonisation des moyens de lutte contre la cybercriminalité, revue de web réalisée le 22/04/2004, http://www.finances.gouv.fr

[2]– د/سليمان أحمد فضل: المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة،2007،ص 18.

[3]–د/عادل عبد الجواد محمد: إجرام الإنترنت،مجلة الأمن و الحياة،العدد221،السنة 20،ديسمبر2000/يناير 2001، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ص70.

[4]–حوار د/ فايز عبد الله الشهري مع هداية نت،الجريدة اليومية الالكترونية للصحافة، السعودية،30 يناير2001، http:// www.hedayah.net

[5]–يقصد بنظم الحاسب الآلي(computer systems) كل مكونات الحاسب المادية (hardware) أو المعنوية (software) و شبكات الاتصال الخاصة به (networks)، بالإضافة إلى الأشخاص. والتي يمكن تحقيق وظيفة أو هدف محدد. د/ هلالي عبد اللاه أحمد،المرجع السابق،ص15.

[6]– محمدأمين أحمد الشوابكة: جرائم الحاسوب و الإنترنت، الطبعة الأولى، دار الثقافة،عمان، 2004، ص10.

أو بأنها: "كل سلوك تكون فيه الأنظمة و الشبكات المعلوماتية وسيلة، أو هدفا أو محلا لارتكاب أفعالا إجرامية".[1]

و تجدر الإشارة إلى أنه و وفقا لـM.WALL فان مصطلح جريمة الانترنت لا يعني ارتباط السلوك غير المشروع بالحاسوب.[2]

ثالثا: تعريف الجريمة وفقا لسمات الجاني الشخصية:

على عكس التعريفات السابقة، يستند أصحاب هذا التعريف إلى معيار شخصي مفاده وجوب إلمام الفاعل (الجاني) بتقنية المعلومات، إضافة إلى استخدام كلا من الحاسب الآلي و الانترنت بالأخص كوسيلة لارتكاب تلك الجرائم، أي أن هذا النوع من الجرائم يتطلب لارتكابه الدراية و المعرفة التقنية الكافية واللازمة بتكنولوجيا المعلومات. وعلى هذا نجد أن البعض قد عرف جرائم الانترنت بأنها: "تلك الجرائم التي لا تعرف الحدود الجغرافية Crime transborder والتي يتم ارتكابها بأداة هي الحاسب الآلي computer عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة بهما"[3].ونفس الشأن بالنسبة لآخرين الذين عرفوها بأنها "هي الجريمة التي ترتكب بأداة الكمبيوتر، وعن طريق شبكة الانترنت، ومن قبل أشخاص على دراية باستخدام الانترنت و الكمبيوتر."[4]

كما عرفت بأنها: "مصطلح يقصد به لجوء ذوي القدرات العالية إلى توظيف قدراتهم لارتكاب الجريمة بطريق الانترنت."[5]

وهناك من الفقه من عرفها وفقا **لمعيار قانوني**، فاعتبرها: "كل ما يمكن ارتكابه من أفعال غير مشروعة يعترف قانون الانترنت[6] بكونها جرائم."[7]

---

[1] –« le cybercrime ،ou la cybercriminalité est largement repandue pour décrire une activité dans laquelle les systèmes informatiques sont un outil, une cible ou un lieu pour réaliser des activités criminelles ». Voir Cyber crime, http://fr.wikipedia.org

[2] –M. WALL déclare que « le terme cybercriminalité ne signifie plus qu'un acte illicite qui est d'une façon ou d'une autre relatif à l'ordinateur » Voir Mohamed CHAWKI, op.Cit, p9.

[3]– منير محمد الجذبيهي، ممدوح محمد الجنبيهي: جرائم الإنترنت، دار الفكر الجامعي، الاسكندرية، 2004، ص13.

[4]– شيرين الياس دبابنة:التأثير الاجتماعي و الاقتصادي لجرائم الإنترنت في المجتمع الاردني،رسالة دكتوراه في علم الاجتماع، كلية الدراسات العليا، الجامعة الاردنية،2008،ص39.

[5] – د/ عبد الفتاح بيومي حجازي،المرجع السابق،ص266.

[6]– قانون الإنترنت، Cyber law هو نوع جديد من فروع القانون، و هو يجمع في علاقة واحدة مباشرة بين معالجة البيانات و المعلومات و بين خدمات الاتصال. ينظر د/ عمر محمد أبو بكر بن يونس،المرجع السابق، ص 103 و ما بعدها. و لقد تم ميلاده سنة 1996.

Voir Vincent FAUCHOUX ، Pierre DEPREZ: Le droit de l'internet ,lois, contrats et usage,litec, Paris, 2008, p2.

[7]– حوار مجتمع المعرفة مع د/عمر محمد أبو بكر بن يونس: جرائم الإنترنت و القوانين الدولية، http://www.mengo.net

وإلى جانب هذه التعريفات الفقهية توجد تعريفات أخرى لجرائم الانترنت، كتعريف قسم العدالة في الولايات المتحدة الأمريكية بأنها: "كل ما يمكن ارتكابه من أفعال غير مشروعة تنتهك وتخترق كلا من قانون العقوبات و الإجراءات الجزائية باستخدام تكنولوجيا المعلومات سواء بطريقة مباشرة أو غير مباشرة (المساهمة في ارتكابها)."[1] و كذا التعريف الذي تبناه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا في الفترة من 10-2000/4/17 و الذي إعتبرها: "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب فتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في البيئة الإليكترونية". أو بأنها: "كل سلوك غير مشروع يشمل جميع الأعمال الاليكترونية الهادفة أمن النظم المعلوماتية و المعطيات المعالجة آليا ".[2]

والتعريف الذي وضعه وزير الداخلية الفرنسي سابقا دومينيك دوفالبان بأنها: "مجموعة الجرائم الجنائية التي ترتكب عبر شبكة الانترنت."[3]

كما عرف المركز الفدرالي للشرطة السويسرية جرائم الانترنت بأنها:" كل الأشكال المستحدثة من الجرائم المتصلة بتكنولوجيا المعلومات الحديثة، و كل الجرائم التقليدية التي ترتكب بواسطة نظام حاسوبي أو شبكة حاسوبية."[4] أما معهد الشرطة الكندية فعرفها بأنها: " أي جريمة يستعمل الحاسوب كمحل لها أو وسيلة

---

[1] -Selon le Département de la justice (United States Department of Justice) la Cybercriminalité est considérée comme « une violation du droit pénal impliquant la connaissance de la technologie de l'information pour sa perpétration ،son investigation ،ou ses procédures pénales»
U.S. Department of justice,http:// www.justice.gov.

[2]-Selon l'O.N.U., la« cybercriminalité » doit recouvrir « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent » ، et dans une acception plus large « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique ».

ينظرعلى التوالي: محمد أمين أحمد الشوابكة، المرجع السابق، ص10. و أسامة أحمد المناعسة ،جلال محمد الزغبي، صايل فاضل الهواوشة، المرجع السابق، ص 78.

-Deuxième Congrès des Nation Unies, à Vienne, sous le titre « la prévention du crime et le traitement des délinquants»,10-17 /04/2000, http:// www.uncjin.org.

[3]- La cybercriminalité: « C'est l'ensemble des infractions pénales qui se commettent sur le réseau Internet »ou «C'est l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP ،appelés communément l'internet». La définition donnée par le ministre de l'intérieur français،http:// vsabouni.free.fr et http://www.interieur.gouv.fr.

[4]- Pour l'Office fédéral de la police suisse, la cybercriminalité s'entend « des Nouvelles formes de criminalité spécifiquement liées aux technologies modernes de l'information ،et de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels ». Voir Mohamed CHAWKI, op.Cit, p7.

لارتكابها."[1] بينما يعرفها مكتب الشكاوى ضد جرائم الإنترنت بأنها:"أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الإنترنت، مثل مواقع الإنترنت، و غرف المحادثة، أو البريد الإلكتروني، و يمكن أن تشمل أيضا أي أمر غير مشروع بدء من عدم تسليم البضائع أو الخدمات مرورا باقتحام الكمبيوتر(التسلل إلى ملفات الكمبيوتر)، وصولا إلى إنتهاك حقوق الملكية الفكرية، و التجسس الإقتصادي(سرقة الأسرار التجارية)، و الإبتزاز على الإنترنت، و تبييض الأموال الدولي، و سرقة الهوية، و قائمة متنامية من الجرائم الأخرى التي يسهلها الإنترنت."[2]

الفرع الثالث: النقد الموجه لهذه التعريفات:

بعد استعراضنا للتعريفات التي قيلت بشأن جرائم الانترنت سواء القانونية أو الفقهية، فإنه وكما سبق ذكره في البداية لا يوجد أي من تلك التعريفات التي حددت المقصود من هذه الجرائم بصورة جامعة مانعة شاملة لها.

أولا: النقد الموجه للتعريفات القانونية:

الحقيقة أن من اختصاص المشرع تحديد المصالح المهمة في المجتمع ليقوم بحمايتها، عن طريق تجريمه الأفعال التي تهدرها أو تهددها بالخطر، و ليس من اختصاصه التعاريف التي هي أصلا من اختصاص الفقه و القضاء أحيانا. و لكن و بالرغم من ذلك وجدت هناك تعاريف قانونية لجرائم الإنترنت إلاّ أنّها لم تسلم من الانتقادات. و منها:

عدم تعريف الاتفاقية الاوروبية لجرائم الانترنت و اكتفت بتسمية مجموعة من الاعمال غير المشروعة و حثت الدول الاعضاء فيها على تجريمها في قانونها الداخلي.

قصور التعريف الذي قال به النائب الفرنسي جون مارك ناسم، اذ اعتبر أن هذه الجرائم قائمة في حالة واحدة لا غير، ألا و هي الحالة التي تستخدم فيها تلك الشبكة كوسيلة لارتكابها؛ أي أنه حصرها في تلك الحالة متناسيا في ذلك أنها من الممكن أن تكون محلا أو هدفا أو ضحية لارتكاب تلك الأفعال الإجرامية غير المشروعة، كما هو الشأن في حالة إرسال القنبلة المنطقية (bombe informatique).

وذات الشأن بالنسبة للقانون الأمريكي، فقد عرف المشرع الأمريكي جريمة الحاسب الآلي دون جرائم الإنترنت.

أما بالنسبة لقانوني العقوبات لكاليفورنيا ولتكساس، فيعاب عليهما أنهما لم يعرفا جرائم الإنترنت بل حصراها في أفعال معينة واعتبراها قائمة فقط في تلك الحالات لا غير، ألا و هي الحالة التي يتم فيها الدخول أو السماح بالدخول العمدي إلى نظام أو شبكة معلوماتية بهدف التخطيط و التنظيم لكل مخطط للاحتيال،أو

---

[1]– le Collège canadien de police définit la cybercriminalité comme « la criminalité ayant l'ordinateur pour objet ou pour instrument de perpétration principale ».Centre Canadien de la statistique juridique، http://collection.nlc-bnc.ca.

2– جرائم الإنترنت، مقال سابق http://djelfa.inf

لكسب الأموال و الخدمات من أجل الاحتيال، أو لتخريب و تحطيم كل نظام،أوشبكة،أوبرمجية،أو بيانات معلوماتية. أو في حالة الدخول إلى الحاسب الآلي أو الشبكة أو إلى نظام معلوماتي دون الحصول على إذن مسبق من صاحبه، متناسين في ذلك أن هذه الحالة هاتين الحالتين ما هي إلا نوع من بين أنواع جرائم الانترنت و بالضبط الإجرام غير المعلوماتي على شبكة الانترنت.

أما بالنسبة لتعريف المشرع العربي في المادة 1 من القانون العربي النموذجي الموحد في شأن مكافحة سوء استخدام تكنولوجيا المعلومات و الاتصالات فقد خلى من تعريف جرائم الانترنت، فالمشرع في المادة السابقة عرف الجريمة المعلوماتية التي تختلف بالكثير عن جرائم الانترنت كما سنرى لاحقا[1].

هذا من جهة ومن جهة أخرى، أعتبر أن الجريمة المعلوماتية تكون قائمة في حالة واحدة وهي الحالة التي يستخدم فيها الوسيط الالكتروني كوسيلة لارتكابها. والمقصود بالوسيط الالكتروني وفقا لنص المادة السابقة من القانون السابق " شبكة الحاسب الآلي أو الانترنت أو أي شبكة الكترونية أخرى " مثل خدمة أو شبكة المينيتال (Minitel) في فرنسا[2]، في حين نجد أن جرائم الانترنت يشترط لارتكابها وجود شبكة وحيدة تسمى بالانترنت أو شبكة الشبكات وتكون هي بذاتها محلا لذلك الإعتداء غير المشروع أو وسيلة له. والشأن ذاته بالنسبة لتعريف المشرع المصري في القانون المصري النموذجي والمشرع السعودي في نظام مكافحة جرائم المعلوماتية الذين عرفا الجريمة المعلوماتية دون جرائم الإنترنت. و الحال ذاته بالنسبة لتعريف المشرع الجزائري، اذ لم يعرف جرائم الانترنت سواء في القانون رقم 09-04 و الذي اكتفى فيه بتعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لا غير، أو في القانون 15/04 و الذي تطرق فيه إلى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[3] و التي تعتبر نوع من أنواع الجريمة المعلوماتية.

ثانيا: النقد الموجه للتعريفات الفقهية:

اختلف الفقه و تعددت تعريفاته لجرائم الانترنت نظرا للمعيار الذي استند إليه هؤلاء في تعريفاتهم لها.

---

[1]- ينظر ص64 من هذه الرسالة.

[2]-تتحقق شبكة أو خدمة المينيتال عن طريق جهاز يحمل ذات الاسم، حيث شاع استخدامه في فرنسا على نحو واسع منذ منتصف الثمانينات في القرن الماضي. و تتم هذه الخدمة عن طريق هذا الجهاز الذي يشبه جهاز الحاسب الآلي الشخصي (PC) و لكنه صغير الحجم نسبيا، و يتكون من شاشة صغيرة، و لوحة أزرار تشمل على حروف و أرقام مثل تلك الخاصة بالكمبيوتر، و هو وسيلة اتصال مرئية تنقل الكتابة على الشاشة دون الصور، أي أنها وسيلة اتصال بالكتابة، و يكفي استعماله أن يتم اتصاله بخط الهاتف، و قد أخذ مكانة هامة في عالم الاتصالات والمعلومات، كما استخدم كوسيلة لإبرام العقود الاليكترونية. د/ عبد الفتاح بيومي حجازي، المرجع السابق، ص 43.

[3]- تسمى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بجرائم المعطيات ويقصد بها:"كل عدوان على معطيات الحاسب الآلي في سريتها أو موفوريتها(إتاحتها) أو في سلامتها(تكاملها)، و ذلك بالإطلاع غير المشروع عليها، أو حذفها أو تغييرها أو ادخال معطيات أخرى عليها(التلاعب بها) أو تعطيل أنظمة معالجتها". لمزيد من التعاريف ينظر محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن، دار الجامعة الجديدة، الإسكندرية،2007،ص78 و ما بعدها.

– **فأما أصحاب الاتجاه الأول،** فيعاب عليهم قصورهم وحصرهم لجرائم الانترنت سواء في الفعل أو النظام الذي يحكم الدول. إذ اعتبروها قائمة فقط في حالة واحدة، و هي تلك التي تستعمل فيها الانترنت كوسيلة لارتكابها وهذا غير صحيح، لأنه يمكن أن تكون تلك الشبكة هدفا أو ضحية أو محلا لارتكاب مثل هذه الأفعال غير القانونية.

هذا من جهة ومن جهة أخرى، نجد أن من تلك التعريفات من قصرها على الأفعال المخالفة للشريعة الإسلامية ولأنظمة دولة معينة (أنظمة المملكة العربية السعودية). في حين كان من اللازم عدم فعل ذلك، لكون أن جرائم الانترنت هي ظاهرة عالمية تأرق وترهب جميع الدول الغربية و العربية ، المتقدمة والنامية، اذ يمكن أن تكون هذه الأخيرة وطنية أو دولية[1].

ضف إلى ذلك فإننا نعرف أن الدول المتقدمة تعترف بالقانون الوضعي وحده كمصدر للقانون في تنظيم وتسيير شؤونها وأمورها وحل نزاعاتها، ولا تعترف بالشريعة الإسلامية أبدا كمصدر من مصادر ذلك الأخير، ولذلك كان من الواجب عدم حصرها في الجرائم المخالفة للشريعة الإسلامية ولأنظمة المملكة العربية السعودية.

–**أما فيما يخص الاتجاه الثاني** فيعاب على الذين عرفوا جرائم الانترنت بأنها: " كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها " استخدامهم لمصطلحات واسعة وغير دقيقة، كمصطلح نظم الحاسب الآلي والذي يضم مكونات الحاسب الآلي وشبكاته المحلية والممتدة وكذا الأشخاص الذين تتحقق من خلالهم تلك الوظيفة.

وعلى هذا كان من الواجب وكما هو متفق عليه في لغة القانون استخدام مصطلحات دقيقة تعبر عن تلك الجرائم، والاقتصار فقط على عبارة " نظم الحاسب الآلي " لا غير بما أنها تضم الشبكات.

– أما بالنسبة للتعريف الذي تبناه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، فإنه وبالرغم من كونه من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي بصورة عامة إلا أنه لم يعرف جرائم الانترنت، فقد اشتمل على جرائم الحاسب الآلي و الجرائم التي ترتكب عبر الشبكات سواء المحلية أو الممتدة.

أما فيما يخص كلا من تعريف المركز الفدرالي للشرطة السويسرية ومعهد الشرطة الكندية فقد وسعا في التعريف ليشمل الجريمة المعلوماتية دون جريمة الانترنت.

أما بالنسبة لتعريف مكتب شكاوى الإنترنت فبالرغم من تعريفه لجرائم الإنترنت إلاّ أنّه قصره فقط على الحالة التي تستخدم فيها تلك الشبكة كوسيلة لإرتكاب الجرائم التقليدية منها أو المستحدثة، متناسيا أنّ هناك حالة أخرى تكون فيها تلك الأخيرة محلا لارتكاب أفعال غير مشروعة عليها.

---

[1]– ينظر ص39 من هذه الرسالة.

وعلى هذا نرى أنه يمكننا تعريف جرائم الانترنت بأنها: " كل سلوك إرادي غير مشروع، صادر عن شخص مسئول جنائيا ذا دراية فائقة بمجال الحوسبة، معاقب عليه قانونا بجزاء جنائي تكون شبكة الانترنت محلا له أو وسيلة لارتكابه ".

و عليه فجرائم الإنترنت هي كل سلوك إجرامي، وكما هو متعارف عليه في لغة القانون الجنائي، السلوك الإجرامي يضم كلا من السلوك الإيجابي الذي يتمثل في القيام بفعل يجرمه القانون،و السلوك السلبي الذي يتمثل في الامتناع عن القيام بفعل يلزمه القانون، بشرط أن يكون هذا السلوك إراديا أي صادرا عن إرادة يعتد بها القانون الجنائي حرة، مختارة، مميزة و مدركة، سواء أكان ذلك عمدا أو خطأ أو متعديا للقصد.

إلا أنه من الملاحظ أن جرائم الانترنت ترتكب غالبا عن طريق السلوك الإيجابي[1] و المتمثل في كل حركة عضوية إرادية صادرة عن الجاني و الذي يتوصل بها إلى ارتكاب فعل يجرمه القانون، ويكون في مثل هذه الجرائم بالضغط على زر لوحة مفاتيح الحاسوب المربوط بالانترنت وهو جالس وراءه دون الحاجة إلى مبارحة مكانه. مثل المصرفي الذي ينوي سرقة مبالغ من المصرف الذي يعمل فيه باستخدام الانترنت، وذلك بممارسة نشاط التعامل مع الحاسوب و الولوج إلى الانترنت، ثم الدخول على شبكة المصرف عبر مزودات مجهولة يمكن الاستعانة من خلالها ببرمجيات اختراق موضوعة على مواقع هكرة يتم تجديدها باستمرار. أو الولوج بقصد اللهو في حركة أو مسار القطارات، فيخرج الأمر عن السيطرة و يتم تدمير بيانات تحريك القطارات عبر الحاسوب، و بالتالي تحدث كارثة تكون نتيجتها خسائر مادية و بشرية كبيرة أو تحريض القصر على الانحراف الجنسي من خلال شبكة الانترنت،أو تهديد الأمن القومي للدول بطريق الانترنت عن طريق التجسس عن أسرار الدول العسكرية عبر الانترنت مثلما حدث في الفترة ما بين عامي 1990-1991م. حيث استطاع خمسة متسللين من هولندا من التسلل إلى 43 نظاما من أنظمة الحاسب الآلي في مواقع الجيش الأمريكي على شبكة الانترنت، بما في ذلك المواقع التي كانت موجهة مباشرة لعملية عاصفة الصحراء. حيث استطاعوا الحصول على معلومات في غاية الأهمية عن مواقع دقيقة للقوات الأمريكية و أنواع الأسلحة التي تمتلكها تلك القوات، و قدرة صواريخ باتريوت، و حركة السفن الحربية في منطقة الخليج..... كما قد تقع عن طريق السلوك السلبي و المتمثل في الإمتناع عن القيام بفعل يفرضه القانون و يعاقب على عدم القيام به. وصورته في مثل هذه الحالة هي امتناع متعهد الايواء[2]

---

[1]- يقصد بالجرائم الايجابية: هي التي يتمثل السلوك الاجرامي المكون لركنها المادي في فعل يمنعه القانون و يعاقب عليه. و يقصد بالجرائم السلبية تلك الجرائم التي يتمثل السلوك الاجرامي لركنها المادي في الامتناع عن القيام بفعل يفرضه القانون على عدم القيام به. د/عبد القادر عدو: مبادئ قانون العقوبات الجزائري، القسم العام، نظرية الجريمة- نظرية الجزاء الجنائي، دار هومة، الجزائر، 2010، ص 260.

[2]- يطلق على متعهد الايواء عدة تسميات كالمورد المستضيف و مورد الايواء و يقصد به كل شخص طبيعي أو معنوي يتولى تخزين و حفظ البيانات و المعلومات لعملائه و يوفر الوسائل الفنية و المعلوماتية التي تسمح لهم بالحصول على هذه البيانات و المعلومات طوال ساعات اليوم و ذلك عبر الإنترنت. لمزيد من التعاريف ينظر د/ عبد الفتاح محمود كيلاني:مدى المسؤولية القانونية لمقدمي خدمة الإنترنت، ص24،http:// www.flaw.bu.eg

و متعهد الوصول[1] و ناقل المعلومات في الإنترنت[2] في حالة علمه بوجود سلوك إجرامي عن الإبلاغ أو التدخل للحفاظ على حقوق الغير أو للحفاظ على أسرار الدولة في جرائم أمن الدولة.[3]

ضف إلى ذلك فان ارتكابها يحتاج بالضرورة إلى منطق تقني، أي أنها تتم عبر الانترنت أو باستخدام المعالجة الآلية للبيانات[4]، كما أنها تحتاج إلى ممارسة نشاط تقني محدد يتمثل في استخدام الحاسوب والانترنت.

هذا من جهة ومن جهة أخرى، يجب أن يكون صادرا عن شخص مسئول مسؤولية جنائية ولا يعترضه أي مانع من موانع هذه المسئولية من صغر السن أو إكراه أو جنون أو كان ذلك السلوك نتيجة حالة الضرورة. وسواء أكان بالغا للسن الرشد الجنائي أو حدثا.

كما يجب أن يكون هذا السلوك غير مشروع أي غير مباح باعتبار أن الإباحة تخرج السلوك الإجرامي من دائرة التجريم.

و اضافة لذلك يجب أن يكون هذا السلوك معاقب عليه قانونا بجزاء جنائي، أي صادر عن قاعدة قانونية مكلفة، لأن إصباغ الصفة الإجرامية لا يتحقق في مجال التشريع الجنائي إلا بإرادة المشرع الجنائي ومن خلال النص على ذلك، حتى ولو كان السلوك مخالفا للأخلاق. ضف إلى ذلك يجب أن يكون هذا السلوك صادرا عن شخص ذا دراية فائقة بمجال الحوسبة، لما يتطلبه هذا النوع من الإجرام من خبرة وحرفية فنية عالية سواء عند ارتكابها أو عند العمل على عدم اكتشاف مرتكبها.

والجدير بالذكر أننا حاولنا عدم حصر هذه الجرائم في تلك التي تستخدم فيها شبكة الانترنت كوسيلة لارتكابها آخذين بعين الإعتبار الجرائم التي تقع على تلك الشبكة أي التي تكون ضحية فيها وما أكثرها...

1- يطلق على متعهد الوصول عدة تسميات منها متعهد الخدمة أو مقدم الخدمة أو مزود الخدمة. و هو يعرف وفقا لنص المادة 2 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها بأنه: أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات. أو هو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها. لمزيد من التعاريف لمتعهد الوصول ينظر أكمل يوسف السعيد يوسف: المسؤولية الجنائية لمقدمي المواد الاباحية عبر الإنترنت، مجلة البحوث القانونية و الاقتصادية، كلية الحقوق، جامعة المنصورة،2011، ص 6.

2 – ناقل المعلومات في الإنترنت أو مورد المحتوى أو المحتوى هو شخص طبيعي أو معنوي يقوم ببث المعلومات و الرسائل المتعلقة بموضوع معين على الإنترنت، بحيث يتمكن مستخدم هذه الشبكة من الحصول عليها مجانا أو بمقابل مادي. لمزيد من التعاريف ينظر د/ عبد الفتاح محمود كيلاني، المرجع السابق، ص17، المنشور على الموقع السابق.

3– د/ابراهيم محمود اللبيدي: السلوك الإجرامي في جرائم الإنترنت،ص25، http:// www.policemc.gov.bh

4–يقصد بالمعالجة الآلية للبيانات أو المعلومات:"مجموعة من العمليات المترابطة و المتسلسلة بدء من جمع البيانات وادخالها إلى الحاسب الآلي و معالجتها وفقا للبرامج التي تعمل بها الحاسبات وصولا إلى تحليلها و اخراجها بصورة معلومات".محمود أحمد عبابنة:جرائم الحاسوب و أبعادها الدولية، دار الثقافة،عمان،2005،ص83.

المطلب الثاني:

التطور التاريخي و إحصائيات حول جرائم الانترنت

لقد أحدث التحول الحضاري و التقدم الذي اجتاح عالمنا في العصر الحديث تغيرا ملموسا في نوعية الجرائم والمجرمين، فبعد أن كانت الغلبة للجرائم القائمة على العنف أو القسوة أصبحت الغلبة للجرائم القائمة على المقدرة الذهنية و الذكاء. بحيث استغل المجرمون هذا التقدم في تطويع المخترعات العلمية الحديثة لخدمة أهدافهم الإجرامية.

وتعتبر الانترنت إحدى وأهم نتائج هذا التقدم العلمي إذ حولت العالم بأكمله إلى قرية صغيرة يتبادل الناس أخبارهم فيها انطلاقا من أماكنهم دون الحاجة إلى مبارحتها. وفي المقابل أصبحت تهدد ذلك الأخير نتيجة سوء استغلالها، وذلك بظهور جرائم تسمى بجرائم الانترنت تستخدم الشبكة فيها كوسيلة أو كمحل لارتكابها. وتجدر الإشارة إلى أن هذه الجرائم في تزايد متواصل ومستمر ومرعب مهدد لمصالح الدول بأكملها، و هذا ما تبينه الإحصائيات و الدراسات التي أجريت حولها. وعلى هذا ارتأينا تقسيم هذا المطلب إلى الفرعين التاليين:

الفرع الأول: التطور التاريخي لجرائم الانترنت و العوامل التي ساعدت في انتشارها.

الفرع الثاني: الإحصائيات التي أجريت حول جرائم الانترنت.

الفرع الأول: التطور التاريخي لجرائم الانترنت و العوامل التي ساعدت في انتشارها.

لقد تحولت شبكة الانترنت نتيجة انتشارها وزيادة استخدامها بشكل هائل من مجرد شبكة بحث أكاديمي إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات ثم إلى بيئة مكيفة للإجرام والمجرمين. وفي هذا يقول بعض الفقه واصفا إياها بأنها "أصبحت الآن مرتعا للنازيين الجدد الداعين للعنصرية والاضطهاد للعديد من فئات بني البشر، وطريقا لالتقاء أصحاب الشذوذ الجنسي، ووسيلة للاتصال والتنظيم بين الإرهابيين والقائمين على الجريمة المنظمة وكل من هو صادر ضده "أمرا بإلقاء القبض عليه نظير جريمته ".[1]

أولا: التطور التاريخي لجرائم الانترنت

ولقد ظهرت جرائم الانترنت[2] في حقل جرائم التقنية العالية في نهاية الثمانينات وكان ذلك من خلال جرائم العدوان الفيروسي أو بالضبط "جريمة دودة موريس" المؤرخة واقعتها في 2 نوفمبر 1988، حيث تمكن طالب يبلغ من العمر 23 سنة ويسمى " روبار موريس" (Robert Moris) من إطلاق ونشر فيروس إلكتروني عرف بدودة موريس (Moris Worms)، تمكن من خلاله من مهاجمه 6 آلاف جهاز كمبيوتر

---

[1]– د/ حسين الغافري، محمد الألفي، المرجع السابق، ص 35

[2]– يقابل مصطلح جرائم الإنترنت في اللغة الانجليزية Internet crime و Cyber crime و في اللغة الفرنسية Cybercriminalité أو Cyberdélinquance أو La criminalité informatique sur l'Internet

مرتبط بالانترنت (من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية). وقد سبب ذلك أضرارا وخسائر بالغة وجسيمة أبرزها إيقاف آلاف الأنظمة عن العمل وتعطيل وإنكار الخدمة وقد حكم على موريس بالسجن مدة 3 سنوات و10 آلاف دولار غرامة.[1]

وفي عام 1995 نجح هجوم مخطط له عرف باسم "IP-SPOOFING" في وقف عمل الكمبيوترات المتصلة بالانترنت وتشغيل كمبيوترات وهمية في مكانها تظاهرت بأنها الكمبيوترات الموثقة. ومن ذلك التاريخ بدأت العديد من الهجمات مستفيدة من نقاط الضعف في الأنظمة، فقد شهد عام 1996 هجمات خطيرة عرفت باسم" هجمات إنكار الخدمة"Denial –of- service attaks.استهدفت تعطيل النظام عن العمل من خلال ضخ سيل من المعلومات والرسائل تؤدي إلى عدم قدرة النظام المستهدف على التعامل مع الطلبات الصحيحة، أو تجعله مشغولا عنها. كما سعت أيضا الهجمات المعتمدة على الانترنت نفسها لتعطيل مواقع الانترنت. كما تعرضت كل من وكالة المخابرات الأمريكية ووزارة العدل الأمريكية و الدفاع الجوي الأمريكي ونازا الفضاء ومجموعة من مواقع شركات التقنية و الوسائط المتعددة في أمريكا وأوروبا وكذلك عدد من المواقع الإسلامية لهجمات من هذا النوع[2].

وتجدر الإشارة إلى أن أول استخدام لمصطلح جرائم الانترنت (Internet Crime) كان في مؤتمر جرائم الانترنت المنعقد في أستراليا للفترة 16-1998/02/17.[3] وأن أول استخدام لمصطلح الانحراف الانترنتي كان من طرف المختصون بمركز البحوث والدراسات بإدارة شرطة دبي، بدولة الإمارات العربية المتحدة.[4]

هذا من جهة ومن جهة أخرى، نجد أن مؤتمر القانون والانترنت المنعقد في لشبونة / البرتغال يوم 2001/01/26 قد أشار إلى ملاحظة هامة جدا تتمثل في وجوب عدم الالتفات إلى المصطلحات غير دقيقة للتعبير عن جرائم الانترنت[5]، واعتماد فقط مصطلح سيبار كرايم (Cyber crime) دون غيره للتعبير

---

[1]– أمير فرح يوسف، المرجع السابق، ص 99. و كذا د/ أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007، ص 100و د/ عمر محمد أبو بكر بن يونس،المرجع السابق، ص 61.

[2]– د/ أيمن عبد الله فكري، المرجع السابق، ص 101

[3]– محمد محمد عبد الله المنشاوي، المرجع السابق، http:// www.minshawi.com

[4] – ينظر في ذلك الامن و الإنترنت، بحث صادر عن مركز البحوث و الدراسات بشرطة دبي، www.dubaipolice.gov .http://

[5]– يستخدم الكثير من الباحثين مصطلحات غير الدقيقة للتعبير عن جرائم الإنترنت، إذ نجد البعض يستخدم مثل مصطلح الإجرام المعلوماتي أو مثل مصطلح جرائم التكنولوجيا المتقدمة أو مصطلح الغش المعلوماتي.في حين أنه يجب استخدام المصطلح الدقيق و المتماشي مع طبيعة تلك الجرائم و هو جريمة الإنترنت. ذلك أن الإجرام المعلوماتي و إن كان يقصد التعبير عن الجرائم الواقعة عن طريق جهاز الكمبيوتر، إلا أن هذا لا يعني أن الإعتداء على المعلومة يتحقق دائما باستخدام الكمبيوتر و خصوصا باستخدام الإنترنت. ذلك لان الوسائل التقليدية هي دائما ما تكون أداة لارتكاب تلك الجريمة. وبالتالي فالجريمة المعلوماتية قد تكون أشمل من جرائم الإنترنت، و ذات الشأن بالنسبة للغش المعلوماتي وكذا جرائم التكنولوجيا المتقدمة.

عنها، مع الأخذ في الإعتبار التمييز بين الجرائم التي يمكن ارتكابها عبر الانترنت وتلك التي لايمكن ارتكابها عبرها.[1]

ثانيا: العوامل التي ساعدت في انتشار جرائم الانترنت.

ظهور جرائم الانترنت و اجتياحها بصورة سريعة و مرهبة لم يأت من فراغ و إنما كان وليد جملة من العوامل ساهمت و ساعدت في انتشار هذه الطائفة من الاجرام المستحدث. و هي:

- التطورات العلمية.
- التحولات الاقتصادية و الاجتماعية و الثقافية العالمية و المحلية.[2]
- السعي الدءوب لأولياء الأمور لتوفير طلبات و احتياجات الأسرة من الناحية المادية مما أدى الى غياب كل منهم عن المنزل لساعات طويلة مما نتج عنه وجود جيل يفقد الكثير من القيم و المبادئ الدينية والخلقية.
- ضعف الدخل المادي و الارتباطات المالية كالقروض يؤدي الى وجود نوع من ابتكار الوسائل المختلفة البديلة للحصول على هذا الدخل.
- عدم وجود العقوبة الرادعة تؤدي الى تفاقم الجريمة.
- الاهتمام والتركيز الاعلامي على مثل هذه القضايا و الحوادث ساهم في ابراز هذه المشاكل الى السطح، فالجريمة كانت موجودة و لكنها كانت متخفية تحت قيود الأعراف الاجتماعية، خاصة مع ازدياد معدلات البطالة و الفراغ الذي يعيشه بعض الشباب في وجود الانفتاح على القنوات الاباحية و انعدام التأهيل الجيد لضبط مرتكبي مثل هذه الجرائم و ضعف المؤسسات التشريعية و القانونية المختصة.[3]

و نتيجة لذلك تعولمت الجريمة و ظهرت أنماط جديدة منها، و أصبحت تنفذ عن بعد و دون الحاجة الى الفعل الفيزيقي.

الفرع الثاني: الإحصائيات التي أجريت حول جرائم الانترنت.

لقد أحدثت ثورة تكنولوجيا للمعلومات تغيرا جذريا وشاملا هز كيان عالمنا سواء بالإيجاب كظهور وسائل اتصال جديدة لم يسبق للبشرية معرفتها، أو بالسلب حيث أنها أفرزت أنماطا مستحدثة من الجرائم المتميزة والخطيرة، أهمها جرائم التقنية العالية وبالضبط جرائم الانترنت التي هي محل دراستنا.

---

[1]- د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 158.

[2]- لمزيد من التفاصيل ينظر على التوالي: د/حسين الغافري، محمد الألفي، المرجع السابق، ص50 و 51؛ وكذا د/صالح سليمان عبد العظيم: الأبعاد و التأثيرات الاجتماعية المرتبطة باستخدام الإنترنت على الاسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الامارات العربية، ورقة مقدمة إلى مؤتمر واقع الاسرة في المجتمع: تشخيص للمشكلات و استكشاف لسياسات المواجهة المنعقد بدار الضيافة، جامعة عين شمس 26-28 سبتمبر 2004، كلية الآداب، قسم علم الاجتماع، مركز الدراسات المعرفية، المعهد العالي للفكر الاسلامي، ص 25.

[3]- د/حسين الغافري، محمد الألفي، المرجع السابق، ص54.

وبالرغم من أن هذه الظاهرة الإجرامية حديثة ومتميزة، إلا أنها تمكنت وفي وقت قياسي قصير جدا من غزو واجتياح العالم بأكمله، وأصبحت تهدد مصالح دوله (المتقدمة والنامية) في جميع المجالات الاقتصادية والاجتماعية و السياسية وحتى القانونية. وهذا ما تثبته الإحصائيات والدراسات التي أجريت حولها.

أولا:الإحصائيات في الدول المتقدمة:

لقد تأثرت الدول المتقدمة – بالدرجة الأولى – من التطور التكنولوجي الذي شهده عالمنا وما أفرزه من آثار سلبية ضارة بالمجتمعات، تمثلت في بروز جرائم مستحدثة وبشكل خاص ظهور جرائم الانترنت، نتيجة سوء استخدام تلك التقنية الحديثة والعالمية واستغلالها لارتكاب جرائم (سواء كانت في دلك وسيلة أو محلا). ولكن بالرغم من حداثة هذه الجرائم نسبيا، إلا أنها لقت اهتمام الباحثين، فأجريت حولها دراسات وإحصائيات تبين مدى خطورتها وبالتالي وجوب مكافحتها والحد منها. ففي أحدث التقارير السنوية لمركز شكاوى احتيال الانترنت الأمريكي (IFCC)[1]، تبين أن عدد الشكاوى المقدمة لهذا المركز قد تضاعف سنة 2003 ليصل إلى 120.000 شكوى مقارنة بتلك التي سجلت في السنوات السابقة (2000 و 2001 و2002) أي بنسبة 60% مقارنة بسنة 2002[2].

وقد بلغت الخسائر الناجمة عن تلك الجرائم (54) مليون دولار على عكس السنوات السابقة.[3]

---

[1]– مركز شكاوى احتيال الإنترنتifc هو مركز مخصص لتلقي شكاوى الناس في الولايات المتحدة الامريكية والعالم أجمع ضد جرائم الاحتيال الواقعة عبر الإنترنت. وقد تم تأسيسه سنة 1999 في مورجانتاون بولاية وست فرجينيا من طرف مكتب التحقيقات الفيدرالي fbi و المركز الوطني لجرائم الياقات البيضاءNW3C من أجل مكافحة ظاهرة الاحتيال عبر الإنترنت المتصاعدة و ذلك بوضع موقع خاص لتلقي الشكاوى من ضحايا الاحتيالات بعنوان: http://www.ifcfbi.gov

– Service de presse national de fbi: internet fraud center, http:// www.ifccfbi.gov

[2]– حيث سجل مركز شكاوى احتيال الإنترنت الامريكي عدد16775 شكوى بينما سجلت الشكاوى سنة 2000التي تلقاها المركز منذ بدء أعماله في ماي 2000حتى شهر نوفمبر من نفس العام (أي خلال 6أشهر فقط) 2087 شكوى من ضمنها 5273حالة تتعلق باختراق الكمبيوتر عبر الإنترنت و 814 تتعلق بوسائل الدخول و الاقتحام الاخرى، كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي. ينظر على التوالي:

Richmond VA:Internet Fraud Center,9/4/03, http:// www.ifccfbi.gov

–جرائم الكمبيوتر و الإنترنت،www.Gamra.com. http://

يونس عرب: جرائم الكمبيوتر و الإنترنت، إنجاز في المفهوم و النطاق و الصور و القواعد الاجرائية للملاحقة والاثبات، ورقة عمل مقدمة إلى مؤتمر الامن العربي، تنظيم المركز العربي للدراسات و البحوث الجنائية، أبو ظبي، 10-2002/2/12 ، http:// arablaw.org.

[3]–بلغت الخسائر الناجمة عن جرائم الإنترنت في سنة 2000 (46) مليون دولار. أما في سنة 2001 فقد بلغت (17) مليون دولار، أي ما يقارب 33% من حجم الخسائر الناشئة عن جرائم الاحتيال التقليدية المرتكبة في نفس الفترة، و أن 22% من هذه الخسائر نجمت عبر الإنترنت دون أن يتم تسليم البضاعة فعليا للمشترين، و أن 5% منها نشأت عن احتيال بطاقات الائتمان. ينظر على التوالي:

Richmond VA ,op.cit,http:// www.ifccfbi.gov.

وتجدر الإشارة إلى أن هذه الحالات التي تم التبليغ عنها – وإن كانت تتعلق فقط بجريمة الاحتيال عبر الانترنت والتي هي واحدة من أنماط جرائم الانترنت[1]– لا تعكس الأرقام الحقيقية لذلك الشبح الذي يرعب ويؤرق دول العالم. إذ أن الكثير من تلك الجرائم ترتكب وتظل في طي الكتمان، وهذا ما يعبر عنه علماء الإجرام "بالرقم الأسود "أو "الرقم المخفي" (Le chiffre noir).[2]

وإلى جانب ذلك فقد أجريت عدة دراسات وقدمت عدة تقارير عن مخاطر تقنية المعلومات وتحديدا الانترنت، فوفقا لمركز الاستراتيجيات والدراسات العالمية الأمريكي، فإن الشرطة الفيدرالية الأمريكية قدرت أن حجم الجرائم الالكترونية يصل إلى 10 بليون سنويا، لكن المبلغ عنها إلى الجهات المختصة يقدر بـ:(17 %) فقط. وفي دراسة أخرى قدرت تلك الأخيرة أضرار جرائم الانترنت والكمبيوتر بحوالي 5 مليارات دولار سنويا وأضافت إلى أن تكلفة جريمة الحاسب الآلي والانترنت الواحدة تساوي 6000 دولار سنويا مقابل ذات المبلغ تكلفة جرائم السرقة بالإكراه.[3]

أما في بريطانيا فقد أجرى اتحاد الصناعات البريطاني إحصاء تحصل فيه على النتائج التالية:

1 – تؤدي جرائم الانترنت إلى إحجام الشركات وخاصة الصغيرة منها– التي يقل عدد موظفيها عن 500 موظف – عن بيع السلع والخدمات عبر الانترنت.

2 – ارتكاب جرائم الانترنت تختلف نسبها وفقا لمرتكبها. فمخربي الانترنت يحتلون المرتبة الأولى من حيث كونهم يرتكبون أخطر هذه الجرائم بنسبة (5،44 %) سنويا، عكس الموظفين السابقين الذين ينفذون

جرائم الكمبيوتر و الإنترنت، المقال السابق المنشور على الموقع السابق. د/أيمن عبد الله فكري، المرجع السابق، ص102و103.

[1]– جريمة احتيال الإنترنت تصنف إلى سبعة أنواع رئيسية و الجدول التالي يوضح لنا نسبة توزيع كل نوع من الأنواع في الفترة بين ماي – نوفمبر 2000.

% 48.8	احتيال مزاد
% 19.2	عدم التسليم المادي
% 16.9	احتيال في السندات المالية
% 4.8	احتيال بطاقة إئتمان
% 2.9	سرقة هوية
% 2.5	فرص عمل
% 1.2	خدمات محترفة
% 3.7	آخر

ينظر د/ أيمن عبد الله فكري، نفس المرجع، الهامش رقم 02، ص102.

[2]– الرقم الأسود أو الرقم الخفي يتمثل في الفرق بين الجرائم الحقيقية التي ارتكبت فعلا و بين تلك التي تظهر في الاحصاءات الرسمية، وبصفة خاصة الصادرة عن وزارة الداخلية. د/ علي عبد القادر القهوجي: مبادئ علم الاجرام، مؤسسة الثقافة الجامعية، الاسكندرية،1992، ص23.

[3]– د/أيمن عبد الله فكري، المرجع السابق، ص 103.

(8،12 %) من تلك الجرائم- في حين تنفذ عصابات الجريمة المنظمة (11،5 %) منها وموظفي الشركات (7،9 %).

أما الشركات المنافسة فترتكب (8،5 %) منها، أما الجماعات المناهضة لسياسات معينة فتنفذ (6،2 %) من تلك الجرائم. والشأن ذاته بالنسبة للجماعات الإرهابية التي تقدر نسبة ارتكابها لتلك الأخيرة (1،4 %).

3 – خشية الشركات العاملة في قطاع الخدمات المالية من الخسائر المادية التي يلحقها بها مخربو الانترنت، على عكس تلك العاملة في قطاعات أخرى، إذ تتركز مخاوفها على الخسارة المعنوية والمتمثلة في فقدان ثقة عملائها فيها نتيجة الضرر الذي لحق بها وهز سمعتها.

كما أظهر الإحصاء أن نسبة (4 %) من مخاطر تلك الجرائم تمثلت في الجرائم المتعلقة ببطاقات الائتمان، وأن (40 %) من الشركات لا تحتوي على أقسام مختلفة بمواجهة جرائم الانترنت.

وفي هذا يقول "ديجي جونز" مدير عام اتحاد الصناعات البريطانية "أن نتائج الإحصاء تؤكد أن جرائم الانترنت تعطل نمو الشركات، وأن السبيل الوحيد لتجاوز تلك المشكلة هو تشديد الرقابة وقوانين مكافحة جرائم الانترنت."[1]

ثانيا:الإحصائيات في الدول النامية: (دول العالم العربي).

وإذا كان الوضع في دول الوطن العربي يختلف بكثير عن ذلك الموجود في دول العالم المتقدمة، من حيث كونها أقل تأثرا بالتقنية العالمية وما أفرزته من أثار سلبية وبالخصوص الجرائم المستحدثة الفريدة من نوعها،التي ظهرت نتيجة سوء استخدام تلك التقنية وبالضبط جرائم الانترنت. إلا أن هذا لا ينكر عدم تعرضها لمثل تلك الجرائم، خاصة مع ظهور الانترنت واجتياحها للعالم العربي في جميع نواحي وميادين الحياة، ولهذا كان لزاما على الباحثين العرب الاهتمام بهذه الظاهرة الإجرامية الحديثة وذلك بمحاولة فهم طبيعتها ومن ثم مواجهتها والتحكم فيها.

ولقد أجريت العديد من الدراسات المختلفة حولها ومنها الدراسة التي أجرتها منظمة (Business Software Aliance) في الشرق الأوسط، والتي تبين من خلالها وجود تباين بين دول تلك المنطقة في حجم الخسائر، حيث تراوحت بين 3 ملايين دولار في المملكة العربية السعودية والإمارات العربية المتحدة ومليون وأربعمائة ألف دولار أمريكي في لبنان.[2]

وأظهرت دراسة أخرى، أن معظم الجرائم التي تتم في العالم العربي عبارة عن اختراقات وتشويه المعلومات بالإضافة إلى عمليات التخريب، وذلك عن طريق إرسال الفيروسات إلى المؤسسات العامة أو الخاصة مما يؤدي إلى وجود أضرار كبيرة وفادحة تقدر حجم خسائرها في الدول العربية كالآتي:

البحرين والإمارات العربية المتحدة تقدر فيها الخسائر نسبة (92 %)، أما الكويت وقطر فنسبة الخسائر تقدر بـ: (91 %)، بينما الأردن فنسبة الخسائر فيها هي: (87 %) ليليها عمان بـ: (86 %) ثم مصر بـ:

---

[1]– أمير فرج يوسف، المرجع السابق، ص 77و78.

[2]– منير محمد الجنبيهي و ممدوح محمد الجنبيهي،المرجع السابق، ص 18.

(87 %) ثم السعودية و لبنان ب (77 %).أما باقي الشرق الاوسط فيقدر فيه حجم الخسائر بنسبة (87%).

و لقد أظهرت أرقام رسمية لمديرية الأمن العام في الأردن أنه تم تسجيل 3649 جريمة تتعلق بتكنولوجيا المعلومات خلال سنة 2009 و بلغ عدد المتورطين فيها 186 شخصا بينهم 168 أردنيا و 18 من الجنسية الأجنبية.[1]

أما في الجزائر فهي كغيرها من دول العالم ليست في منأى عن جرائم الانترنت، حيث يعتبر هذا الشكل الجديد من الإجرام العابر للحدود تهديدا حقيقيا للمؤسسات و الشركات و خاصة بعد بداية انتشار استعمال تكنولوجيا الإعلام و الاتصال الحديثة في جميع المجالات. و هذا ما كشفته إحصائيات قدمها مركز البحوث القانونية و القضائية التابع لوزارة العدل إذ وصل عدد الهجمات اليومية على مختلف المواقع الإليكترونية (منها مواقع رسمية وخاصة مواقع هيئات وجرائد وطنية بينها موقع جريدة "الشروق" الذي استعمل لبيع قطع أثرية لولاية عنابة و عرض صور خليعة على الانترنت، و اختراق منظومة البنك الجزائري و الجمارك الوطنية من طرف شاب يتحكم في الإعلام الآلي من ولاية أم البواقي) إلى 3000 هجمة في الشهر.

هذا من جهة و من جهة أخرى، و حسب ذات الإحصائيات فإن عدد الجرائم المعلوماتية تطور من 12 قضية سنة 2005 تتضمن 20 متهما إلى 12 قضية تتضمن 51 متهما سنة 2006.و لقد بلغ عدد الأشخاص المتابعين في الجرائم المعلوماتية في أبريل 882010 شخصا.

و من جهة ثالثة، فإنه ووفقا للتقرير الذي عرضه ذلك المركز في منتدى حول الجريمة السيبرانية الذي نظم في الجزائر العاصمة في 2010/05/05 فان الطلبة و المختصين في تكنولوجيا المعلومات الذين تتراوح أعمارهم بين 25 و 30 سنة عادة ما يكونوا متورطين في الجريمة الإليكترونية و أشارت الخبر إلى أنه من بين دوافع المذنبين الأسباب المالية أو الانتقام أو الفضول.[2]

كما تشير أحدث الاحصاءات المقدمة من طرف الفرق المتخصّصة في مكافحة الجرائم الإلكترونية للأمن الوطني خلال سنة 2012 من أنه تم ضبط 47 قضية تتعلّق بجرائم الأنترنت– قُدّم من خلالها الدليل المادي على تورط 48 شخصا، منهم 04 نساء تراوحت أعمارهن ما بين 18 و50 سنة– و تمثلت في: 14 قضية انتحال هوية الغير و10 قضايا تمسّ أنظمة المعالجة الآلية للمعطيات، إلى جانب ثمانية قضايا لها علاقة بالقذف عن طريق الأنترنت وستّة قضايا متعلّقة بالمساس بحرمة الحياة الخاصّة، بالإضافة إلى

[1]– بحث منشور على الإنترنت على الموقع التالي:http:// swmsa.net

[2]–وليد الرمزي:التعاون الدولي حاسم في حرب الجزائر ضد الجريمة السيبرانية، مقال منشور على الإنترنت يوم 2010/05/11على الموقع التالي:http:// magharebba.com

أربع قضايا متعلّقة بالتهديد بالتشهير وثلاث قضايا تتعلّق بالنّصب والاحتيال عن طريق الأنترنت وقضيتين لهما علاقة بنشر الصور المخلة بالحياء.[1]

ولقد اتضح من جهة أخرى وفي دراسة مغايرة أن حوالي (65 %) من مستخدمي الانترنت عبر العالم كانوا ضحايا جرائم الانترنت (سواء جرائم مهاجمة الشبكة بالفيروسات أو انتحال شخصية الفرد (Usurpation d'identité) (أو إساءة استخدام بطاقات الائتمان). وذلك باختلاف نسب دوله من دول إلى أخرى وذلك كما يلي:[2]

- بالنسبة للصين 85 %
- بالنسبة للهند و البرازيل 76 %
- بالنسبة للولايات المتحدة الأمريكية 73 %
- بالنسبة لنيوزلندا (الجديدة) 70 %
- بالنسبة لأستراليا وإيطاليا 69 %
- بالنسبة لكندا 64 %
- بالنسبة لألمانيا واسبانيا 62 %
- بالنسبة لبريطانيا 59 %
- بالنسبة لفرنسا 57 %
- بالنسبة للسويد 56 %
- بالنسبة لليابان 36 %

ومن الثابت أن غالبية جرائم الانترنت بموجب أحد الإحصائيات تم اقترافها من قبل موظفي الشبكة، إذ قدرت نسبتهم في ارتكاب تلك الجرائم بـ: (2385 %) وذلك راجع إلى الرغبة في الانتقام من رؤسائهم الإداريين الذين يسيطرون عليهم من خلال الجهاز الإداري المنتمين إليه.[3]

هذا من ناحية ومن ناحية أخرى، بين مسح أجري في مارس 2008 أن نسبة الاختراقات بالانترنت عالميا في تزايد مستمر ومخيف وذلك كالآتي:

- نسبة الاختراقات في القارة الإفريقية بلغت (5،3 %)، أما في القارة الأسيوية فبلغت (14،0 %) وعلى غرارها بلغت النسبة في القارة الأوربية (47،7%)، أما أستراليا فحددت النسبة بـ: (57 %) إلا أننا نلاحظ

---

[1]- لمزيد من التفاصيل ينظر الأمن يضبط47 جريمة إلكترونية، جريدة أخبار اليوم، 2013/03/11، http:// www.akhbarelyoum.dz

[2]- « Les cybercriminels rarement attrapés ،faute de plainte », http://generation.t.com

[3]- أمجد دخل الله: القرصنة الالكترونية، مجلة المحامون، العددان3و4، السنة 72، سوريا،عام 2007، ص 27.

ازدياد النسبة وضخامتها في القارة الأمريكية، إذ تقدر في أمريكا الشمالية بـ: (1،73 %)، بينما تبلغ في أمريكا الجنوبية نسبة (8،23 %).[1]

هذا وتجدر الإشارة إلى أن هجمات الهاكرز صنفت في قمة مخاطر الشبكات في إفريقيا وشرق آسيا على وجه الخصوص في حين أظهر المسح الذي أجري عام 2000 ارتفاع عدد الشركات المتضررة من تلك الجرائم، حيث وصل إلى (273) شركة بلغ مجموع خسائرها أكثر من 256 مليون دولار. [2]

هذا من جهة و من جهة أخرى، فان خبراء الامن يتوقعون أن تتضاعف النشاطات غير المشروعة عبر الانترنت ارتباطا بالانتشار الواسع للتكنولوجيا في الدول، حيث أن ايرادات الجرائم على الانترنت أكبر من ايرادات مبيعات المخدرات غير المشروعة، وتجاوزت ال105مليارات دولار[3].

و لعل ما ساعد جرائم الانترنت على ترتيب تلك الخسائر، الصفات و المميزات التي تتميز وتنفرد بها عن غيرها من الجرائم لا سيما التقليدية منها.فيا ترى ما هي خصائص هذه الجرائم ؟ و ما الفرق بينها و بين غيرها من الجرائم؟.

المبحث الثاني:

خصائص جرائم الانترنت و الفرق بينها وبين غيرها من الجرائم

إذا كان للتقدم التقني إيجابيته التي لا يمكن لأحد إنكارها، فإن له في المقابل سلبيات متمثلة في إمكانية استخدام شبكة الشبكات في ارتكاب أفعال تقع تحت طائلة قانون العقوبات سواء كانت تمثل في ذلك الوسيلة أو المحل. و لقد سبق و أن انتهينا إلى تعريف لجرائم الانترنت بأنها: "كل سلوك إرادي غير مشروع،صادر عن شخص مسئول جنائيا ذا دارية فائقة بمجال الحوسبة، معاقب عليه قانونا بجزاء جنائي تكون شبكة الانترنت محلا له أو وسيلة لارتكابه"

و على هذا تتمتع هذه الجرائم بمجموعة من الخصائص تميزها و تنفرد بها عن غيرها من الجرائم و خاصة التقليدية. و لهذا خصصنا هذا المبحث للتعرف عن مجموع هذه الخصائص و لنبين الفروقات الموجودة بين هذه الجرائم و غيرها،و ذلك في المطلبين التاليين:

المطلب الأول: خصائص جرائم الانترنت

المطلب الثاني: الفرق بين جرائم الانترنت و غيرها من الجرائم.

---

[1]– " Les cybercriminels rarement attrapés ،faute de plainte " , disponible à l'adresse précédente.

[2]– منير محمد الجنبيهي و ممدوح محمد الجنبيهي،المرجع السابق، ص 18.و محمد محمد عبد الله المنشاوي، المرجع السابق،http://www.minshawi.com .

[3]– شيرين الياس دبابنة، المرجع السابق، ص41.

المطلب الأول:

خصائص جرائم الانترنت.

تعرف جرائم الانترنت بأنها كل سلوك إرادي غير مشروع، صادر عن شخص مسئول جنائيا ذا دراية فائقة بمجال الحوسبة، معاقب عليه قانونا بجزاء جنائي تكون شبكة الانترنت محلا له أو وسيلة لارتكابه.

باستقرائنا لهذا التعريف نستخلص أن جرائم الانترنت تتميز بجملة من الخصائص تجعلها فريدة من نوعها و تميزها عن باقي الجرائم لا سيما تلك التقليدية. و يمكن إجمالها في:

أنها من الجرائم المستحدثة الواقعة على شبكة الانترنت أو بواسطتها من قبل شخص على دراية فائقة بمجال الحوسبة.... و لقد خصصنا هذا المطلب لتفصيل هذه الخصائص من خلال تقسيمه إلى الفروع التالية:

الفرع الأول: جرائم الانترنت جرائم محلها، وسيلتها شبكة الانترنت وأداة ارتكابها الحاسوب

الفرع الثاني: جرائم الانترنت عابرة للحدود و صعبة الإثبات

الفرع الثالث: مرتكب جرائم الانترنت شخص له خبرة فائقة بمجال الحوسبة

الفرع الأول: جرائم الانترنت جرائم محلها، وسيلتها شبكة الانترنت وأداة ارتكابها الحاسوب

تعتبر جرائم الانترنت إحدى الجرائم المستحدثة التي تصنف ضمن جرائم التقنية العالية والتي أفرزها التطور التكنولوجي الذي عرفه عالمنا إثر ثورة تعرف بثورة المعلوماتية، والتي تتقدم بسرعة مذهلة تفوق بكثير الثورة الصناعية، والتي قوامها الحواسيب الآلية وشبكة الانترنت.

ولما كانت هذه الجرائم عبارة عن سلوك إجرامي تكون فيه شبكة الانترنت إما محلا أو وسيلة لارتكابها، وذلك كله عن طريق جهاز يسمى بالحاسب الآلي تطل من خلاله تلك الشبكة على العالم الخارجي.

كان من اللازم التطرق لخاصية مهمة لا تقل أهمية عن الخصائص الأخرى التي تتميز وتنفرد بها جرائم الانترنت ألا وهي أنها جرائم محلها أو وسيلتها شبكة الانترنت وأداة ارتكابها الحاسب الآلي في االنقطتين التاليين:

أولا: جرائم الانترنت جرائم محلها،وسيلتها شبكة الانترنت

تعتبر شبكة الانترنت أو كما يطلق عليها " الشبكة العالمية العنكبوتية " أو شبكة الشبكات " أو "الفضاء السيبراني" الحقل الخصب الذي تقع فيه جرائم الانترنت، ذلك لأنها تمثل حلقة الوصل بين كافة أهداف مجرمي التقنية المحتملة، مهما كانت طبيعة ضحاياها سواء أكانوا أشخاصا طبيعية أو معنوية كالبنوك والمؤسسات المالية والشركات الصناعية وغيرها. ومن أمثلة هذه الجرائم مهاجمة الشبكة بالفيروسات أو

بالقنبلة المعلوماتية وغيرها مما يصنف ضمن الإعتداءات المنطقية أو الإعتداءات المادية (كالاعتراض المتعمد للبيانات، التشويش، الاكتساح والتفخيخ...)[1].

ولكن وفي المقابل ذلك حولت تلك الأخيرة إلى وسيلة فتاكة يستخدمها ذلك المجرم لارتكاب جريمته ولتحقيق أهدافه غير المشروعة، ومن أمثلة هذا النوع من الإجرام: الجرائم الجنسية،الجرائم المالية و جرائم الاختراقات عبر الانترنت...[2]

ثانيا: جرائم الانترنت جرائم أداة ارتكابها الحاسب الآلي:

من المتعارف عليه في القانون الجنائي أن أي جريمة من الجرائم وبالضبط التي يكون فيها السلوك إيجابيا عموما، يجب لارتكابها أداة أو سلاح يسمى بسلاح الجريمة فمثلا: جريمة القتل أداة ارتكابها تكون سلاحا ناريا أو أبيضا أو سما، وجرائم الانترنت كغيرها من الجرائم يجب لارتكابها وسيلة والمتمثلة في جهاز الحاسب الآلي[3]. وتعتبر هذه الخاصية من أهم الخصائص التي تميز هذه الجرائم عن غيرها لاسيما تلك التقليدية. ذلك لأن الانترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة، ولذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه، باعتباره النافذة والعيون التي تطل وتشاهد بها تلك الشبكة العالم الخارجي،فهو بذلك وسيلة استخدام الانترنت. وإن كنا اليوم نعاصر إمكانية استعمال الانترنت عبر الهاتف المحمول أو الخلوي[4]. أو عبر وسائل الاتصال الالكترونية الحديثة بصفة عامة كالهواتف الذكية و الأجهزة اللوحية .[5]

ويقصد بالحاسب الآلي [6] وفقا للموسوعة الشاملة لمصطلحات الحاسب الإليكتروني: "كل جهاز إليكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال (Data imput) أو إخراج معلومات

---

[1]– لمزيد من التفاصيل ينظر وليد الزيدي، المرجع السابق، ص 15 و ما بعدها.

[2]– وليد الزيدي، المرجع السابق،ص 22 و مابعدها. و ينظر كذلك الإنترنت يتحول مسرحا لارتكاب الجرائم الالكترونية والسعودية و الامارات في الصدارة، http:// teknotel.info

[3]– مقال دور الحاسوب في الجريمة المعلوماتية و محل الجريمة، ص6 ،f3.eeds.feedburner.com //:http.

[4]–تجدر الإشارة إلى أن المحمول أو الهاتف الخلوي ما هو إلا تقنية من تقنيات الحوسبة المتطورة.

[5] – و من أمثلتها الجيل الجديد من الهواتف النقالة و كذا ما يسمى بأي باد. ينظر منتديات الجزائر: ما هو الجيل الثالث للهاتف النقال و ما الجديد فيه ؟ ،www.eljazayera.com //:http

dunumérique.com.www.maisonQuest-ce qu'une tablette tactile ? Définition, http://

[6]–الحاسب لغة مصدره الفعل حسب أو نحوه، و علم الحساب علم الأعداد و هو من العدد و التدبير و التدقيق. يقابله في اللغة الانجليزية كلمة « Computer » المشتقة من فعل « Comput » و في اللغة الفرنسية كلمة « Ordinateur ». و قد استعملت مصطلحات عربية كثيرة للدلالة عليه، كالحاسب الإليكتروني و الحاسب الآلي و العقل الإليكتروني و الرقابة والنظامة الكمبيوتر. ويقصد بالحاسب وفقا لمعجم الحسابات عن مجمع اللغة العربية لسنة 2003 "جهاز أو منظومة لتنفيذ مجموعة من العمليات المحددة بتسلسل سبق إعداده، و تشمل عمليات حسابية و منطقية أو عمليات نقل للبيانات بين أجزاء الحاسب المختلفة و تخزينها و استرجاعها، و قد يعتمد تسلسل العمليات على قيم البيانات المتداولة. و يسمى تسلسل

(Information Output)، وإجراء عمليات حسابية أو منطقية. وهو يقوم بالكتابة على أجهزة الإخراج (Output devices) أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب (Opérator) عن طريق وحدات الإدخال أو استرجاعها من وحدة المعالجة المركزية. وبعد معالجة البيانات، تتم كتابتها على أجهزة الإخراج. [1]

وهو يتكون من كيانين، أحدهما مادي يضم الأجهزة المادية المختلفة والتي تشمل وحدات الإدخال والإخراج ووحدات التشغيل المركزية. والآخر معنوي يشمل البرمجيات الجاهزة و البيانات والمعلومات المنطقية. [2]

الفرع الثاني: جرائم الانترنت عابرة للحدود و صعبة الاكتشاف.

كما تتميز جرائم الانترنت بخاصية ثانية تتمثل في كونها لا تعترف بالحدود الجغرافية و أنها صعبة الاكتشاف والإثبات.

أولا: جرائم الانترنت عابرة للحدود:

يزداد حجم جرائم الانترنت وتتنوع أساليب ارتكابها وتتعاظم خسائرها وأخطارها، وذلك نظرا لما تتميز به من خصائص لا تتوفر في الجرائم التقليدية (في أسلوبها وطريقة ارتكابها) ومن أبرزها: أنها جرائم لا تعترف بالحدود الجغرافية (Transbounder Crimes). ذلك لأن شبكة الانترنت ألغت كل الحدود المتعارف عليها في العالم المادي، بحيث أصبح مستخدميها يبحرون ويتبادلون أخبارهم ويحصلون على أية معلومات يريدونها بسرعة فائقة وبدون أي عناء انطلاقا من أماكنهم (منازل، مقاهي الانترنت) جالسين وراء أجهزة الحواسيب الآلية دون الحاجة إلى مبارحتها، فمثلا: يستطيع شخص موجود في الجزائر أن يحصل على ما يشاء ويرغب من معلومات من فرنسا وهو جالس في منزله وراء حاسوبه الخاص. وبذلك حولت تلك الشبكة الأم معمورتنا إلى مجرد قرية إليكترونية صغيرة تتدفق المعلومات بين أرجائها في سهولة وسرعة وغزارة ويتنقل الناس في دولها بل حتى قاراتها بدون الحاجة إلى وسيلة نقل أيا كان نوعها.

العمليات برنامجا، و تخزن البيانات و البرامج في وسط للتخزين يسمى بذاكرة الحاسب"معجم الحاسبات،طبعة ثالثة، مجمع اللغة العربية، القاهرة، 2003، ص 66. ينظر كذلك د/عفيفي كمال عفيفي، المرجع السابق، ص 8. د/هلالي عبد اللاه أحمد، المرجع سابق، ص 15. أما إصطلاحا فقد تعددت تعريفاته، فقد عرفه الدكتور علي عبد القادر القهوجي بأنه "عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات و معالجتها و تخزينها و استشارتها أو استرجاعها عند الطلب". د/ علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة ، الإسكندرية، 1997، ص 3. ينظر كذلك كلا من أسامة أحمد المناعسة و جلال الزعبي و صايل فاضل الهواوش، المرجع السابق، ص 60. و د/هلالي عبد اللاه أحمد، المرجع السابق، ص 16. و ينظر د/ علاء عبد الباسط خلاف: الحماية الجنائية لوسائل الاتصال الحديثة (الحاسب الإليكتروني "الكمبيوتر" الإنترنت)،بدون دار نشر، 2004، ص 13. و كذا وليد الزيدي،المرجع السابق، ص 8. و د/ عبد الفتاح مراد، المرجع السابق، ص 492 و ما بعدها.

[1]- د/ هلالي عبد اللاه أحمد، المرجع السابق، ص16و17.

[2]- د/ علي عبد القادر القهوجي،(الحماية الجنائية لبرامج...) مرجع سابق، ص 3.

وهنا يطرح إشكال جوهري حول طبيعة جرائم الانترنت وفقا لهذه الخاصية فهل تعتبر هذه الأخيرة جرائم داخلية[1] أم هي جرائم دولية ؟ [2] أم هي جرائم ذات بعد دولي؟.[3]

---

[1]–الجريمة الداخلية هي تلك الجريمة التي تقع كاملة في نطاق إقليمي محدد وينطبق عليها القانون الجنائي بفرعيه لذلك الإقليم (الدولة).د/عمر محمد ابو بكر بن يونس،المرجع السابق،ص194

[2]–الجريمة الدولية هي: "اعتداء على مصلحة يحميها القانون (المصلحة الدولية الأجدر بالحماية) والمقصود بالقانون هنا القانون الجنائي الذي تكفل بإصباغ الحماية الجنائية على مصلحة جديرة بتلك الحماية الجنائية الدولية بعد ما انتشرت الحروب الطاحنة والإعتداءات المتكررة على أمن البشرية والإنسان عموما. ويقوم المشرع الدولي عن طريق العرف أو الاتفاقات و المعاهدات الدولية بتحديد النموذج القانوني للجريمة الدولية وقد عرف البعض الجريمة الدولية بأنها "سلوك إرادي غير مشروع يصدر عن فرد باسم الدولة أو تشجيع أو رضاء منها ويكون منطويا على المساس بمصلحة دولية محمية قانونا". وهي تقوم على ثلاث أركان الركن المادي الذي يتضمن سلوك تترتب عليه نتيجة إجرامية، الركن المعنوي الذي يقتضي أن يكون السلوك صادرا عن إرادة حرة واعية ومدركة. أي يجب توافر عناصر المسؤولية الجنائية، الركن الدولي ويقتضي أن يكون الفعل المرتكب واردا في اتفاقية أو معاهدة دولية أو عن طريق العرف الدولي والمستقر بين الدول. وقد عرفها جانب من الفقه بأنها: "كل واقعة ترتكب إخلالا بقواعد القانون الدولي والتي من شأنها إلحاق الضرر بالمصالح التي يوفر لها ذلك القانون حماية جنائية. وتعرف الجريمة الدولية وفقا لستيفان جلا سر بأنها: " كل فعل (أو امتناع عن فعل) مخالف لأحكام القانون الدولي ومضر بمصالح الجماعة المحمية بهذا القانون من دول وسواها، على أن يثبت من خلال علاقات الدول ببعضها الاقتناع بأن هذا الفعل (أو الامتناع عن الفعل) ينبغي معاقبته جنائيا " أو هي:" كل سلوك – فعلا كان أم امتناعا – إنساني يصدر عن فرد باسم الدولة أو برضاء منه، صادر عن إرادة إجرامية يترتب عليه المساس بمصلحة دولية، مشمولة بحماية القانون الدولي عن طريق الجزاء الجنائي". وتجدر الإشارة إلى أن المنظمات الدولية وخاصة الأمم المتحدة قد اهتمت بالجريمة الدولية، إذ أبرمت اتفاقيات جنيف الأربعة لسنة 1949 والتي وضعت ضوابط وقواعد لحماية الأسرى والمرضى و الجرحى و السكان المدنيين أثناء الحرب.وقد ظهرت الجريمة الدولية في أقدم العصور حيث كانت جريمة القرصنة البحرية في أعالي البحار وجريمة قانون الشعوب. وبعد ذلك أقر القانون الدولي جرائم الحرب، حيث كان التجسس والخيانة الحربية أقدم صور هذه الجرائم. ينظر على التوالي كلا من أحمد عبد الحكيم عثمان: الجرائم الدولية في ضوء القانون الدولي الجنائي والشريعة الإسلامية، دار الكتب القانونية، مصر، 2009، ص 12و 13 و 18 .د/ منصور بن خضروان الداموك: مبادئ القانون الدولي و تطبيقاته في المملكة العربية السعودية، الطبعة الأولى، مكتبة الملك فهد الوطنية، الرياض، 1424، ص 201 و ما بعدها. د/محمود صالح العادلي: الجريمة الدولية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2003، ص 61 و ما بعدها.

[3]–يقصد بالجرائم ذات البعد الدولي Transnational crime: هي تلك النوعية من الجرائم التي اتفق المجتمع الدولي بمقتضى عهدا أو مشارطة دولية أيا كانت على كونها تشكل عدوانا في كل دولة مثلما هو الحال في إجرام المخدرات وتهريب الأسلحة و غسل الأموال. د/ عمر محمد أبو بكر بن يونس، المرجع السابق،. ص 195.

تعتبر جرائم الانترنت من الجرائم التي لها عدة أبعاد: يتجسد البعد الاول لها في النطاق المحلي، مما يعني أن الاختصاص ينعقد فيها للمشرع الجنائي الداخلي.

في حين يتجسد بعدها الثاني في النطاق الدولي، و يتحقق ذلك عندما يكون مرتكب الجريمة دولة أو أحد مؤسساتها أو أحد أشخاص القانون الدولي[1]، أو أن تكون الجريمة موجهة ضد دولة ما كما حدث في التجسس الذي قامت به الولايات المتحدة الأمريكية، إذ استخدمت الأسلحة المعلوماتية الفتاكة أثناء القصف الجوي للحلف الأطلنطي Nato في كوسوفو عن طريق انتهاك أنظمة حاسوب أعدائها.[2]

كما أنها قد تكون ذات بعد دولي، عندما ترتكبها عصابات إجرام أو منظمات إجرامية أو أفراد، من ذلك مثلا جريمة ترويج المواد المخدرة عبر الانترنت وكذلك العدوان الذي باشره القاتل الإليكتروني الصيني بنسفه لقاعدة بيانات السفارة الأمريكية في بكين وبلغراد إثر قصف الولايات المتحدة الأمريكية للسفارة الصينية في بلغراد إبان الحرب الأمريكية الصربية.[3]

وتجدر الإشارة إلى أن موضوع تدويل ظاهرة الاختراق تثار في ظل الجريمة الدولية والجريمة ذات البعد الدولي في إطار الانترنت، لكونها جريمة يمكن أن يتأثر بها المجتمع الدولي برمته، كما هو الشأن في جريمة إغراق الخوادم / الانترنت (The denial of services) الذي حدثت في شهر فيفري 2000 وانتشرت انتشارا دوليا[4]، وكذلك بالنسبة لدودة الحب[5] والشفرة الحمراء[6].

نستخلص من هذا كله أن جرائم الانترنت تستلزم لإقرارها اعتراف المشرع الداخلي بها، ثم إنها تأخذ بعدا دوليا لاعتراف المشرع الدولي بإمكانية ارتكابها من قبل الدولة حتى لو كانت في صيغة تأييد مثلما قامت به عصابات الكيان الصهيوني من دعوة لاجتماع الهكرة في مؤتمر عالمي في شهر ماي 2000 في فلسطين المحتلة وأخيرا تأخذ هذه الأخيرة صورة الجريمة ذات البعد الدولي، من حيث إمكانية أن يكون العمل

---

[1]– تعتبر أشخاصا للقانون الدولي تلك الاشخاص التي تتمتع بشخصية دولية و معنية بالمخاطبة بقواعد القانون الدولي وهي على وجه الخصوص:الدولة،المنظمات الدولية بأنواعها،الشركات المتعددة الجنسيات،حركات التحرر الوطني.

[2]– د/ عمر محمد أبو بكر بن يونس، المرجع السابق ، ص 196–197.

[3]– د/ عمر محمد أبو بكر بن يونس، نفس المرجع، ص 197.

[4]– د/ عمر الفاروق: جرائم الكمبيوتر و الجرائم الأخرى في مجال تكنولوجيا المعلومات، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 28/25 أكتوبر 1993، ص 465.

[5]– صممت دودة الحب بواسطة شاب فلبينى و هي دودة حاسوبية مدمرة سريعة الانتشار ضربت أجهزة الحاسوب فى عام 2000 مستغلة ثغرة فى نظام ويندوز و ضعف نظام البريد الإلكترونى ، عرف هذا الفيروس بكونه واحدا من أول الفيروسات التي تخدع المستخدمين لفتح ملف ما، و هو يأتي على شكل رسالة غرامية ويرسل أعدادا هائلة منها بعنوان " I Love You "، و وصل عدد الأجهزة التي تأثرت به إلى 10% ، مما سبب خسارة قدرت بنحو يبدأ من 5 مليار دولار حتى 10 بلايين دولار. لمزيد من التفاصيل ينظر محمد فارس: أخطر 10 فيروسات في التاريخ، http:// itwadi.com

[6]– الشفرة الحمراء: و هي دودة حاسوبية ظهرت مطلع شهر أوت 2001 وهي الاكثر تدميرا و تخريبا لأجهزة الكمبيوتر وواقع الإنترنت. حيث ضربت أكثر من 150 موقعا في العالم، و تسببت في خسائر قدرت ب 2 مليار دولار. لمزيد من التفاصيل ينظر حسني عبد الصبور: قضية الساعة، الإنترنت و فيروس الشفرة الحمراء، جريدة الأهرام،2001/8/11، س126، العدد 41886، http:// ahram.org.eg.

Adrian THAM : What is code red worm ?,Aug4,2001,SANS institut , p2 et suite.

الإجرامي عبر الانترنت أو عليها من طبيعة عالمية يمس القاعدة البشرية والإنسانية من حيث كونها تعد جريمة داخلية إلا أنها تمتد إلى خارج إقليم الدولة مما يعني خضوعها لأكثر من قانون جنائي كما هو الشأن في جرائم المخدرات والإرهاب والتجسس الاقتصادي. إذن الأشكال الثلاثة تجتمع في جريمة واحدة، فجرائم الانترنت جرائم وطنية (داخلية) ودولية وذات بعد دولي في الوقت ذاته.

وعلى أساس هذه النظرة إلى طبيعة جريمة الانترنت دعا البعض إلى الإقرار بوجود قانون عقوبات الحاسوب الدوليInternational criminal computer law والذي يعرفونه بأنه: "دراسة نهج المجرمين وجرائمهم التي تتطلب معرفة بنظام الحاسوب في الوقت الذي يستلزم وجود عنصر دولي أو ذي بعد دولي في الواقعة الجنائية أو السلوك الجنائي تحديدا." [1]

ثانيا:صعوبة اكتشاف جرائم الانترنت وإثباتها.

تعتبر جرائم الانترنت ظاهرة إجرامية مستحدثة وفريدة من نوعها، وهي تقرع في جنباتها أجراسا لتنبه مجتمعات العصر الراهن المتقدمة والنامية لحجم المخاطر وهول الخسائر الناجمة عنها. [2] ويرجع السبب في ذلك إلى أنها جرائم تتميز وتتمتع بطابع خاص لا نظير له في الجرائم الأخرى خاصة التقليدية، يتمثل في صعوبة اكتشافها وإثباتها نظرا لوجود الأسباب الجوهرية التالية:

1/ خفاء الجريمة:

الجرائم التي تقع عبر الانترنت أو عليها، هي في جل صورها مستترة وخفية لا يلحظها المجني عليه أو يدرى حتى بوقوعها، وذلك لأنها لا تترك أي أثر خارجي بعد ارتكابهالانعدام الدليل المرئي الملموس. فلا توجد جثث لقتلى ولا أثار لاقتحام سرقة الأموال ولا أثار للدماء في مثل هذه الجرائم[3].

2/ صعوبة الاحتفاظ الفني بآثار الجريمة إن وجدت:

تتميز جرائم الانترنت تتميز في الغالب بعدم وجود دليل مرئي ملموس، إذ تعتبر الأدلة فيها غير مرئية، لكونها أدلة الكترونية[4] فهي عبارة عن نبضات اليكترونية تنساب عبر أجزاء الحاسوب والشبكة كما تنساب الكهرباء عبر الأسلاك.[5] وهذا ما يهيئ الجو المناسب للجاني ويتيح له سهولة محو أدلة الإدانة أو تدميرها

---

[1] – Joao GODOY : Computer and international criminal law,High tech crimes and criminals,New England International and Comparative Law Annal, 2000, http://Lexisnexis.com.

[2]– أمير فرج يوسف، المرجع السابق، ص 214.

[3]– محمد عبد الله المنشاوي،، البحث السابق المنشور علىwww.minshawi.com//:http.

[4]– يعرف الدليل الالكتروني بأنه: بيان أو معلومة يتم استخدامها من أحد أجهزة الحاسب الآلي و بغض النظر عما إذا كانت نشأتها بتدخل الانسان أو من غيره. لمزيد من التافاصيل حول أنواع الدليل الالكتروني ينظر الدليل الجنائي و مشكلة تحصيله في الجرائم الالكترونية، ص 14، www.arabipcenter.com // :http

[5] – د/ عبد الفتاح بيومي حجازي: الدليل الجنائي في جرائم الكمبيوتر و الإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر، بدون سنة نشر، ص 36 و ما بعدها.

في زمن متناه القصر،[1] قد لا يستغرق أكثر من ثوان. فضلا عن سهولة تنصله من مسؤولية هذا العمل بإرجاعه حسب ما تشهد بذلك وقائع عديدة سابقة إلى الخطأ في نظام الحاسوب وفي الأجهزة والشبكة.[2]

ضف إلى ذلك وما يزيد من صعوبة الاحتفاظ الفني بآثار الجريمة و يعرقل عملية الإثبات في مجال هذه الجرائم، إعاقة الوصول إلى الدليل غير المرئي بوسائل الحماية الفنية. فهو في الغالب يكون مرمزا أو مشفرا (كاستخدام المجرم المعلوماتي لكلمات السر أو دس تعليمات خفية فيها أو ترميزها) بحيث لا يمكن للإنسان قراءتها دون اللجوء إلى الآلة وبظهوره على شاشة الحاسوب. [3]

3/ إحجام المجني عليه عن الإبلاغ في مجتمع الأعمال:

وتجدر الإشارة إلى أن كثيرا ما تكتشف هذه الجرائم بمحض الصدفة البحتة، والدليل على هذا ما أثبتته الإحصائيات و الدراسات التي أجريت حولها، إذ لم يتم الكشف عن تلك الأخيرة إلا بنسبة 1 % وذلك لأنها تبقى عادة في طي الكتمان وهذا ما يعبر عنه علماء الإجرام بالرقم الأسود أو " الرقم الخفي"[4].

ومن بين أسباب اختفاء هذه الجرائم: إحجام المجني عليه عن الإبلاغ عنها، إذ نجد أن أغلب الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك تكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للأضرار بسمعتها و مكانتها، وخصوصا إذا كان المجني عليه عبارة عن مؤسسة مالية كالبنوك و المؤسسات الإدخارية و مؤسسات الأقراض السمسرة،حيث تخشى مجالس إدارتها عادة من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها. [5]

و يجدر التنويه إلى أن جرائم الانترنت الذي تم الإبلاغ عنها إلى السلطات المختصة لم يتعد 15% من النسبة السابقة (1%) وحتى بالنسبة إلى الجرائم التي طرحت أمام القضاء، فإن أدلة الإدانة لم تكن كافية إلا في حدود الخمس فقط[6] فمثلا نجد أن بريطانيا تشهد حوالي 300 جريمة انترنت، ولا يبلغ إلا على 90 منها وذلك لجهل الأشخاص بها وبمدى خطورتها واعتقادهم بنقص خبرة الشرطة وعدم قدرتها في ملاحقة مرتكبها والتحقيق فيها. [7]

---

[1]– د/ هشام فريد رستم،(قانون العقوبات و .....) مرجع سابق، ص 42. د/جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجيات الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، الكتاب الأول، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص14.

[2]– د/هشام فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994،ص22.

[3]– د/ جميل عبد الباقي الصغير، المرجع السابق، ص16.

[4]– ينظر ص32 من هذه الرسالة.

[5]–د/هشام فريد رستم، (الجوانب الإجرائية للجرائم المعلوماتي) مرجع سابق، ص 25.

[6]– د/ جميل عبد الباقي الصغير، المرجع السابق، ص 17–18. و ينظر كذلك د/عفيفي كمال عفيفي،المرجع السابق، ص 22. إبراهيم أبو كامش: فضاء الإنترنت في فلسطين تنخره السرقة و الابتزاز و الاحتيال و التشهير، مجلة الحياة و السوق، س2، العدد 56، 2012، ص 2.

[7]– شريط التكنولوجيا الحديثة، بث على التليفزيون الجزائري، القناة الأولى يوم 2008/11/05.

4/ نقص خبرة الشرطة وجهات الإدعاء و القضاء:

يستلزم لكشف جرائم الانترنت والاهتداء إلى مرتكبها وملاحقتهم قضائيا استراتجيات تحقيق وتدريب خاصة، أي خبرة فنية تتلاءم مع طبيعة هذا الجرم وتسمح بتفهم ومواجهة الخصوصيات التي يقوم ويرتكز عليها هذا الأخير والأساليب التي تستخدم في ارتكابه. [1]

لهذا وجدت أجهزة العدالة (الضبطية القضائية، جهات التحقيق، القضاة) نفسها غير قادرة على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع المستحدث والفريد من الإجرام، أي أنها أصبحت فاشلة في مواجهته. ضف إلى ذلك إمكانية تحطيم أو تدمير الدليل من طرف الشرطة أو الجهات المختصة بالتحقيق أثناء جمع الأدلة أو من طرف الخبير والجهة المجني عليها نتيجة خطأ مشترك بينها.[2] وعلى هذا كان لزاما استحداث أجهزة عدالة متطورة تتماشى مع التطور التكنولوجي وما يفرزه من إجرام مميز ومستحدث،[3] و منها استحداث شرطة مختصة لهذا النوع من الجرائم تسمى بشرطة الانترنت.[4]

---

[1]– محمد محمد عبد الله المنشاوي، البحث السابق المنشور على http:// www.minshawi.com

[2]–د/هشام فريد رستم، (الجوانب الإجرائية للجرائم المعلوماتية) مرجع سابق، ص27.

[3]- وهذا ما دعت و أكدت عليه الدول وكذا ما تضمنته توصية المجلس الأوروبي رقم ر(95)13في 1995/09/11. و كذا ما دعا اليه وزير الداخلية الفرنسي السابق Dominique de Villepin و أيضا ما أوصى به المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة في الفترة ما بين 25-1993/10/28. ينظر على التوالي: د/عبد الله حسين علي محمود:سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية،دار النهضة العربية، القاهرة، 2002، الهامش رقم 2، ص 354. علاء الدين محمد شحاتة: رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي،المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة ما بين 25-1993/10/28، مشكلات المسؤولية الجنائية في مجال الجرائم الواقعة على البيئة، الجرائم الواقعة في مجال تكنولوجيا المعلومات، دار النهضة العربية، القاهرة،1993،ص 587. د/جميل عبد الباقي الصغير :الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة،2002، ص77.

-Jed ALL: une cyber-patrouille de police sur internet ،publié le 25 mars 2005,http://aliquid.free.fr

-G8:cybercriminalité,http:// www.finance.diplomatie.fr

[4]– لقد أطلق على هذه الضبطية القضائية المختصة في مكافحة جرائم الإنترنت عدة تسميات– و لكنها متقاربة–اضافة لشرطة الإنترنت(cyber police)أو (police de net)، "درك الإنترنت"(cyber gendarme) أو" دورية شرطة الإنترنت"(cyber patrouille) أو" متحري الإنترنت"(cyberdétective). ويقصد بشرطة الإنترنت: ""نوع من الاجراءات والضمانات للمحافظة على أموال الغير و أسرارهم". وهي ضبطية قضائية مختلفة تماما عن تلك التي تقوم بالكشف عن الجرائم التقليدية، لكونها لا تعتمد على التدريبات المادية أو الفيزيولوجية التي يتلقاها رجال الشرطة للوصول إلى هذه المرتبة، و انما تعتمد على قوة تكوين البناء العلمي و التكنولوجي لأفرادها. وهي تتولى في ذلك مهمة مباشرة جمع الاستدلالات والتحري في العالم الإفتراضي، من أجل كشف النقاب عن هذا النوع المتميز من الاجرام. كما يمكنها أن تطارد الهكرة ومخترقي الانظمة على كافة المستويات".

5/ تعتمد هذه الجرائم على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها، فقد يستخدم الجاني اسما مستعارا أو يرتكب فعله من خلال إحدى مقاهي الانترنت[1] فجرائم التزوير عبر الانترنت تتم دون تحديد شخص مرتكبها أو ضبط المحرر المزور.

ولقد أثير في المؤتمر الدولي لجرائم الحاسوب المنعقد في أسل6/ النرويج في الفترة ما بين 29 – 2000/05/31، موضوع عدم إمكانية البنية التحتية للإنترنت من التوصل إلى تحديد شخصية مرتكب الجريمة أو المصدر الحقيقي لها وموقعه على وجه التحديد. وإن كانت توفر إمكانية التعرف على عنوان ورقم الحاسوب فقط المرتبط بالانترنت و المستعمل كوسيلة لارتكاب الجريمة، أي ما يطلق عليه في النظام التقني (I.P.) [2] ، و بالتالي تحديد الشخص صاحب ذلك الرقم بسهولة. لتبدأ بعد ذلك سلسلة إثبات ارتكابه للجريمة من عدمه. ولكن وفي مقابل ذلك، فإن هذا الرقم ليس موحدا على المستوى العالمي، إذ أن هناك أقلية من الدول التي تتبعه دون غيرها وخاصة الدول العربية.[3]

6/ كما تعتمد هذه الجرائم على قمة من الذكاء و المهارة في ارتكابها.

7/ كما أن للبعد الزمني (اختلاف المواقيت بين الدول) وكذا المكاني (كثيرا من هذه الجرائم عادة ما ترتكب من مسافات بعيدة باستخدام وحدات طرفية أو باتصال هاتفي يمكن للجاني من خلالها إعطاء تعليمات للحاسب الآلي. فقد حدث أن أحد الهواة في أوربا تمكن من حل شفرة أحد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية) وأصبح السبيل أمامه مفتوحا للعبث ببيانات هذه المراكز[4]) والقانوني (أي قانون يطبق) دور مهم في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم.[5]

الفرع الثالث: مرتكب جرائم الانترنت شخص ذو خبرة فائقة بمجال الحوسبة.

تتطلب جرائم الانترنت على عكس نظيرتها التقليدية حرفية فنية عالية لارتكابها، أي يجب أن يتمتع المجرم فيها المسمى بمجرم الانترنت " أو "المجرم التقني " أو "المجرم المعلوماتي" أو "الهاكر" بجملة من السمات.

ويمكن تعريف المجرم التقني بأنه:"كل مجرم سلك سبيل التقنية لارتكاب جرائمه، ذلك عن طريق استخدامه لتقنية المعلومات".[6] كما يمكن تعريف الهاكر بأنه:"شخص فائق الذكاء في المعلوماتية". أي أنه يتمتع بمستوى مهاري خاص يدل على الكفاءة والصلاحية و الأهلية التقنية.إذ يملك هذا الأخير الجبروت في الاختراق وارتكاب أفعال تقنية عبر العالم الإفتراضي بطريقة لا يمكن للعامة القيام بها، حتى ولو كانوا

---

[1]– د/ سليمان أحمد فضل، المرجع السابق، ص21

[2] – يقصد بـip adresse: هو العنوان الرقمي الذي يميز و يحدد هوية جهاز بشكل فريد في الإنترنت. د/صالح مسند: مصطلحات الإنترنت، ص 5 ، http:// faculty.ksu.edu.sa

[3]– د/ عمر محمد أبو بكر بن يونس،المرجع السابق، ص 81.

[4]–د/جميل عبد الباقي الصغير، (الجوانب الاجرائية للجرائم المتعلقة بالإنترنت) مرجع سابق، ص 77.

[5]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص 16. و ينظر حوار د/فايز بن عبد الله الشهري مع هداية نت، المرجع السابق المنشور علىhttp:// www.hedayah.net

[6] – د/عمر محمد أبو بكر بن يونس، المرجع السابق، ص 235.

يملكون خاصية التعامل الحاسوبي. أو هو:"شخص يرغب و يهوى فهم و استخدام الحيل التقنية لاكتشاف أسرار الانظمة." كما يعرف مرتكب جرائم الانترنت بأنه:"شخص يملك المهارات لاكتشاف تفاصيل الأنظمة المبرمجة والاستحواذ على موجوداتها التي تهمه ."[1] و قد عرفته جامعة ميري لاند بأنه:" الشخص الذي لديه التأهيل الاكاديمي لعلم الحاسوب و يقوم بالبحث عن المعطيات بشكل عشوائي، حتى تظهر أي معلومة يمكن أن يبني عليها و يستفيد منها".[2] كما عرف بأنه:"الشخص الذي يخترق جهاز الحاسوب، فيستطيع مشاهدة ما به من ملفات أو سرقتها أو تدمير ذلك الجهاز أو التلصص و مشاهدة ما يفعله المستخدم على الشبكة".[3] كما يعرف المجرم المعلوماتي بأنه:"شخص طفل، رجل، أنثى يأتي أفعالا ارادية تشكل سلوكا ايجابيا أو سلبيا باستخدام تقنية المعلوماتية بالإعتداء على حق أو مصلحة مشروعة."[4]

و تجدر الاشارة الى أن الفضل في الكشف عن مصطلح الهكترةHACKERS يعود الى كاتب الخيال العلمي الامريكي ويليام جيبسون W.JIBSON في مؤلفه The Neu-Romancerعام 1984.[5]

---

[1]– Hacker «C'est un jeune surdoué en informatique ». et « c'est un Cybertalent et petit prodige du piratage »

Ce terme désigne à l'origine ،« une personne qui aime comprendre et utiliser les finesses techniques des programmes. Il qualifie aussi aujourd'hui les délinquants pénétrant par effraction dans des sites informatiques ».Voir Dr/Mohamed BUZABAR ،op.cit ،p44.

[2] – أمجد دخل الله، المرجع السابق، ص25.

[3]– الهاكرز.....لصوص برؤية عصرية،www.kufur-kasem.com http://

[4]– د/ هيثم عبد الرحمن البقلي: الجريمة المعلوماتية،www.kennaoline.com http://

[5] – ظهر هذا المصطلح لاول مرة في الستينات ولم يكن يشر أبدا إلى الاجرام، اذ أطلق في بدايته على المبدعين المبرمجين ذووي قدرات تقنية عالية المستوى في معهد ماساشوستس للتكنولوجيا وكذا جامعة ستانفورد و جامعة باركلي في الولايات لمتحدة الامريكية. و لقد استخدم بهدف الكشف عن نقاط الضعف للانظمة المعلوماتية وكذا وضع طريقة لحمايتها وخاصة فيما يخص وسائل الاتصال. فنظام Unix مثلا هو من اختراع الهاكر: "كان تومبسون Ken THOMPSON".

هذا من جهة و من جهة أخرى، فقد مر هذا المصطلح بأربعة أجيال لكي يصل إلى ما هو عليه الآن ويفيد الاجرام، فقد تشكل الجيل الأول له في فترة الستينات من القرن العشرين ليتم اطلاقه على المبدعين المبرمجين (Ingénieurs) ذووي قدرات تقنية عالية المستوى في معهد ماساشوستس للتكنولوجيا وكذا جامعة ستانفورد و جامعة باركلي في الولايات المتحدة الامريكية. ثم امتد ليطلق على مطوري علوم الحاسوب و تقنية الاتصالات و ذلك ضمن الجيل الثاني له والذي كان في السبعينات من القرن العشرين و تم تسميتهم بPhreaker و الذي يعني كل شخص لديه القدرة التقنية على استكشاف نظام الهاتف لكي يحصل على خدمة اتصالات هاتفية مجانية من منطلق التجربة. وفي الثمانينات من القرن المذكور أطلق هذا المصطلح على مخترقي الالعاب الالكترونية وحقوق النسخ الكومبيوترية و ذلك ضمن الجيل الثالث أو جيل الحاسوب الشخصي. و لقد قامت تنظيمات عصابية منذ ذلك التاريخ ، و منها التنظيم العصابيs414 الذي قام بأكثر من 40 حالة اختراق آنذاك، ثم تطور أخيرا إلى ماهو عليه الآن ليستقر عند المجرمين و التافهين و هم العناصر البشرية للجيل الرابع . و أشهرهم المخترقون الذين يظلون مجهولين عند اختراقهم للنظام و مكوثهم فيه لفترات طويلة دون أن يدري بهم أحد والمسمون ب Crasher ou Nukers.ومثال ذلك ما حدث مع شركة مايكروسوفت، حيث تم اختراقها من قبل مجهول ما بين الفترة

ومن السمات التي يجب أن يتمتع بها هذا المجرم ذا المهارات الخاصة، إضافة إلى الشروط العامة اللازمة توفرها فيه من سلوك منحرف وعلم وإرادة نتائج هذا السلوك:

– **أن يكون هذا الأخير مجرما متخصصا:** أي يجب أن يكون الشخص خبيرا بالقدر الكافي واللازم بأمور الحوسبة ومحترفا حتى يستطيع أن يقدم على مثل هذا النوع الخطير والمستحدث من الإجرام، فقد ثبت في عديد من القضايا أن عددا من المجرمين يتخصصون في ارتكاب مثل هذه الجرائم دون سواها.[1]

– **يعتبر هذا المجرم مجرما عائدا إلى الإجرام:** أي أن العديد من مجرمي هذا الصنف من الإجرام يرجعون إلى ارتكاب جرائم إنترنت أخرى يتفنون فيها ويسدون الثغرات التي أدت إلى التعرف عليهم فيها وإلى تقديمهم للمحاكمة في المرة السابقة.أو بعبارة أخرى فهو يوظف مهاراته في كيفية عمل الحواسيب وتخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات[2].

– كما يتميز هذا المجرم بالذكاء (ruse) و الاحتراف و الشعور بالعظمة و القدرة على التفوق على الآخرين.

اذ يصنف الهاكر ضمن نوابغ المعلوماتية ذوي المستوى المهاري الخاص والرفيع من الذكاء. أي أنه ينتمي إلى الطبقة المتعلمة المثقفة المحكومة برغبة جامحة في تحدي كل ما هو جديد ومبتكر[3]. وهذا ما أثبتته التجارب العلمية في هذا الميدان، إذ أن العديد ممن تم إلقاء القبض عليهم أفادوا بمحاضر التحقيقات بأنهم قاموا بذلك رغبة منهم في تحدي وقهر الأنظمة المحوسبة. [4]

هذا من جهة ومن جهة أخرى، فإن هذا الأخير عادة وفي الغالب ما يكون من العاملين بنفس الجهة المجني عليها – الضحية – التي تثق به ثقة عمياء ولا تشك في نزاهته، مما يؤدي به إلى ارتكاب جريمته بكل أمان وراحة، منتهزا في ذلك جهل موظفيها وكبار مديريها بعلوم وتقنيات الحاسوب ولا سيما استخدام

من 14إلى 28 أكتوبر 2000 ومكث فيها لمدة أربعة عشر يوما. ولم يرتكب ضررا ما سوى قيامه بنسخ ثم ارسال موضوع الشفرة الخاص ببرمجياتها إلى روسيا و خرج بعد ذلك تاركا وراءه التعبير المشار اليه على أوجه العاملين فيها ثم لحق ذلك الاختراق تسلل هولندي لخطأ فني في ثغرة باحدى الملقمات ليلج إلى احدى آلات التقنية في ذات الشركة مايكروسوفت خاصة. ولقد تم اكتشاف الاختراق بعد ذلك حسبما صرح بذلك المتحدث الرسمي باسم الشركة المذكور Rick Miller .

لمزيد من التفاصيل ينظر د/عمر محمد أبو بكر بن يونس،المرجع السابق، ص 233–234– 235.

Mohamed N.SALAM : Le piratage informatique,definition et problemes juridiques, Mémoire pour l'obtention du diplôme d'etudes approfondies en droit interne et international des affaires, Universite Libanaise,2004, p14–15–29–31–32.

[1]– د/ عبد الفتاح بيومي حجازي،(نحو صياغة نظرية ....) مرجع سابق، ص 97. د/ عبد الله حسين علي محمود، المرجع السابق، ص46. د/فؤاد جمال:جرائم الحاسبات والإنترنت، http:// www.tashreaat. com

[2]– د/ عبد الفتاح بيومي حجازي،(نحو صياغة نظرية ....) مرجع سابق، ص 98.

[3]–Dr/Mohamed BUZABAR,op.cit,p 45

[4]– لمزيد من التفاصيل ينظرد/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 237 و ما بعدها

الانترنت. وكذا إحجامها (الجهة المجني عليها) عن الإبلاغ عن هذه الجرائم تجنبا للأضرار بسمعتها ومكانتها (وخصوصا إذا كانت تلك الجهة عبارة عن مؤسسة مالية).

ضف إلى ذلك فإن إجرام هذا الأخير ينتمي إلى **إجرام الحيلة** الذي يعتمد أساسا على قوة الذكاء ولا يحتاج إلى أدنى مجهود عضلي (مجرم الانترنت مجرم غير عنيف). فجرائم الانترنت هي جرائم سريعة التنفيذ، اذ غالبا ما تنفذ بوسائل سهلة و سريعة – بحيث أن هيئات تنفيذ القوانين لا يمكن أن تجاريها– مع امكانية تنفيذها عن بعد و دون التواجد في مسرح الجريمة مع وجود ضخامة في الفوائد و المكاسب، فهي بذلك اذن **جرائم ناعمة ومغرية** لمرتكبها.

هذا من جهة ومن جهة أخرى،فان الخسائر التي تسببها جرائم الانترنت عادة ما تكون باهظة في أغلبية الجرائم.[1]

ومن جهة ثالثة،فان الدراسات القليلة للجوانب السيكولوجية لمجرمي الحاسب عامة و مجرمي الانترنت خاصة، أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الاجرامية و بلا مشروعية الأفعال التي يقترفونها. كذلك الشعور بعدم استحقا قهم للعقاب عن هذه الافعال.فحدود الشر و الخير متداخلة لدى هذه الفئة، وتغيب في داخلهم مشاعر الاحساس بالذنب. وهذه المشاعر في الحقيقة تبدو متعارضة مع ما تظهره الدراسات من خشية مرتكبي جرائم نظم المعلومات من اكتشافهم و افتضاح أمرهم. و لكن هذه الرهبة و الخشية يفسرها انتماؤهم في الاعم الاغلب الى فئة اجتماعية متعلمة و مثقفة[2]. فمجرم الانترنت هو " **مجرم اجتماعي**" يتكيف ويتأقلم مع المجتمع الذي ينتمي إليه ويعيش فيه، فهو قبل كل شيء إنسان متكيف اجتماعي، وهذا ما ساعده على التميز بالسمات والصفات السابقة خاصة الذكاء[3].

كما أنه عادة لا يضع نفسه في عداء مع ذلك المجتمع، وهذا ما يزيد من خطورته الإجرامية،[4] والدليل على ذلك النماذج الإجرامية التالية التي وقعت من كبار وأحداث صغار، وكان لها أثار خطيرة.

ففي إسرائيل ألقي القبض على كاتب إسرائيلي بتهمة الإعتداء على أمن الدولة، وذلك لكونه نشر معلومات محظورة على شبكة الانترنت، تتعلق باختفاء غواصة في البحر المتوسط عام 1968[5].

وفي الولايات الامريكية، تمكن قرصان أمريكي لم يتجاوز 12عاما من اختراق نظام وزارة الدفاع الامريكية–البنتاجون– غير عابئ بنظم الحماية عالية التقنيةو الجدران النارية التي وضعت لحماية هذه

---

[1]– شرين إلياس دبابنة، المرجع السابق، ص40. و ينظر كذلك د/ عبد الفتاح بيومي حجازي، (نحو صياغة نظرية عامة في علم الجريمة و....) مرجع سابق، ص 98.

[2]–د/ أيمن عبد الله فكري، المرجع السابق، ص 114–115.

[3]– د/ عبد الفتاح بيومي حجازي،(المجرم المعلوماتي...) مرجع سابق، ص99.

[4]–د/ عبد الفتاح بيومي حجازي، نفس المرجع، ص 100. د/ عبد الله حسين علي محمود، المرجع السابق، ص41.

[5]– د/ جميل عبد الباقي الصغير: الإنترنت و القانون الجنائي، الطبعة الأولى،دار النهضة العربية، القاهرة، 1996، ص34.

النظم،و كان بامكانه تعريض البشرية للابادة لو تمكن من الوصول الى المخزون النووي الاستراتيجي، وفك الشفرة الخاصة به، وضبطها و كذلك تصويب القنابل النووية.[1]

الحدث ماكسوس[2] الذي استولى على بطاقات الائتمان وحول الأرصدة والحسابات من خلال شبكة الانترنت لدرجة أنه استطاع الاستيلاء على ثلاثمائة بطاقة في حين لم يتجاوز عمره ثمانية عشر عاما،

الأمر الذي أثار ذعرا لدى البنوك الأمريكية.[3]

الهجوم الذي تعرضت إليه سلسلة من مواقع الانترنت الأمريكية العالمية في 2000/02/09، حيث تعرضت مواقع مثل فراد– أي– بي دوت كوم وأمازون دوت كوم وسي إن – إن دوت كوم لأعمال التخريب، بعد تلك الأعمال التي تعرض لها موقعي ياهو، ودوت كوم العالميين...إلخ.[4]

كذلك فقد ذكر أن أحد القراصنة من هولندا و حال غزو العراق للكويت، تمكن من سرقة أسرار عسكرية أمريكية بالغة الخطورة عن تحركات القوات الامريكية ومواقعها وأسلحتها وتحركات الطائرات المقاتلة،و أرسلها الى العراق قبيل اندلاع الحرب، لكن العراق رفض الهدية خشية أن يكون في الامر خدعة.[5]

زيادة على ذلك فإن معظم هؤلاء المجرمين تتراوح أعمارهم ما بين 18 – 46 سنة، ومتوسط العمري لهم 25 سنة.[6] ففي الكويت مثلا يتراوح المتوسط العمري لمجرمي الانترنت ما بين 15 – 25 سنة[7] وفي الجزائر ما بين 25– 30 سنة،[8] وفي أمريكا يتراوح أعمار معظم الهكرة الخطيرين ما بين 18 – 35 سنة[9].

و في هذا شهد التحري الخاصJoseph G. DEGNAN بقسم خدمات التحقيق الجنائي في البحرية الامريكية The naval criminal investigative services بأن الهاكر النموذجي يبلغ من العمر ما

---

[1]– د/ عبد الفتاح بيومي حجازي،(نحو صياغة نظرية عامة في علم الجريمة و....) مرجع سابق،ص109.

[2]–ماكسوس هو حدث يبلغ من العمر 18 عاما وتتلخص قصته في قيامه بسرقة أرقام الآلاف من بطاقات ائتمان الزبائن في أحد مواقع الشراء عبر الإنترنت و نشرها على تلك الشبكة، و استخدامها بالفعل و خصم مبيعات منها بمبلغ مالي كبير. وذلك كله نتيجة رفض الشركات عروض بتقديم المساعدة لها مقابل مبلغ من المال. و تعد هذه العملية من أوسع عمليات السطو عبر شبكات الإنترنت هذا من جهة و من جهة أخرى، فانه ووفقا للمحللون لم يكن ماكسوس يعمل وحده بل ضمن مجموعة متخصصة بسرقة وتزوير بطاقات الائتمان، و مقرها روسيا.لمزيد من التفاصيل ينظر د/ عبد الفتاح بيومي حجازي: الأحداث و الإنترنت، دراسة متعمقة عن أثر الإنترنت في انحراف الأحداث، دار الفكر الجامعي، الإسكندرية، 2004، الهامش 2، ص 86 و ما بعدها.

[3]– د/ عبد الفتاح بيومي حجازي، نفس المرجع، ص 86.

[4]– د/ عبد الفتاح بيومي حجازي، نفس المرجع، هامش رقم 2،ص 190.

[5]– د/ عبد الفتاح بيومي حجازي،(نحو صياغة نظرية عامة في علم الجريمة و....) مرجع سابق،ص109.

[6]– د/ عبد الله حسين علي محمود، المرجع السابق،،ص 42.

[7]– Dr/ Mohamed BUZABAR, op.cit, sous titrage n°73 , p 4

[8]– وليد الرمزي،(التعاون الدولي.....) مقال سابق، منشور علىhttp:// magharebba.com

[9]– د/حسين الغافري، محمد الالفي، المرجع السابق،ص 38.

بين 14عاما و 25 عاما،و ليس هناك اهتمام من والديه أو من الوصي عليه بما يفعله أثناء الليل حال وجوده في غرفته أمام الحاسوب.[1]

ومن النماذج المدللة على ذلك ما قامت به مجموعة من الطلبة في ثانوية بأمريكا، اختراق موقع تابع لوزارة الدفاع الأمريكية ومسح مجموعة من البرامج من على هذا الأخير. وكذا ما قام به أحد الطلبة المتميزين في استخدام الحاسبات في إحدى الجامعات الأمريكية من اختراق موقع الجامعة على شبكة الانترنت وتدمير بعض نظم تلك الأخير، مما كلف الجماعة مبالغ كبيرة في إصلاحها[2].

وقد أوضحت دراسة أخرى قام بها باحث في جامعة أوهايو ظاهرة تفشي تردد الشباب والشابات على كل ما فيه إباحية ومواد جنسية، واستدل فيها بنموذج القاتل السفاح المعروف باسم "تيدر أندي" الذي خطف وعذب وشوه وقتل – عن طريق التعذيب والخنق والاغتصاب ونهش وأكل لحوم ضحاياه – ما يقارب 40 ضحية (امرأة) من بينها طفلة تبلغ من العمر 10 سنوات. [3]

ضف إلى ذلك ما قام به الشاب "ديفيد سميث" [4] بانشائه ونشره لفيروس البريد الالكتروني المعروف باسم "ميليسا"[5] الذي أحدث اضطرابا عالميا في البريد الالكتروني بشبكة الانترنت، و قد قضى ضده بالسجن

---

[1]–د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 236.

[2]–د/حسين الغافري، محمد الالفي، المرجع السابق،ص 39.

[3]–د/ مشعل بن عبد الله القدهي: المواقع الاباحية على شبكة الإنترنت و أثرها على الفرد و المجتمع، ص12، http:// www.minshawi.com.

[4]–ديفيد سميث شاب يبلغ من العمر 30 عاما و هو يعمل كمبرمج كمبيوتر في مختبرات At&T في فلورهام وأيضا مستشار موقع On –Site Consultant. أمير فرج يوسف، المرجع السابق، ص97.

[5]–و تتلخص قصة فيروس ميليسا في أنه في 1999/3/26أصيبت الالاف من أجهزة الحاسب الالي بفيروس أثقل كاهل عمل البريد الالكتروني في مختلف أنحاء العالم،و هو فيروس يستنسخ نفسه و يسخر برمجيات البريد الالكتروني لارسال قائمة بعناوين المواقع الجنسية الفاضحة و نشرها بسرعة من خلال الإنترنت. الامر الذي أجبر العديد من الشركات على اغلاق مزودات خدمة البريد الالكتروني لديها و خاصة شركات الكمبيوتر العملاقة مثل انتل و مايكروسوفت وكذلك لدى وزارة الدفاع الامريكية. و يرسل هذا الفيروس قائمة بعناوين 80 موقعا جنسيا إلى 50 شخص في سجل عناوين المجني عليهم أصحاب البريد الالكتروني. فلو أصيب جهاز واحد بهذا الفيروس فانه يعمد إلى ارسال 50 رسالة إلى 50 جهة مسجلة في العنوان الواحد الذي أصابه.و كانت الرسالة الملوثة بالفيروس والتي ترسل إلى المشترك تحمل عبارة باسم صاحب الجهاز و هي Message from user name و ذلك عقب رسالة important subject حتى يسارع صاحب البريد الالكتروني بفتح الرسالة، و التي كانت تتضمن عبارات مشوقة مثل here is that document you asked for don't show anyone else و بمجرد فتح هذه الرسالة و النص المربوط بها، يرسل الفيروس مرة أخرى إلى خمسين شخصا آخرين، وهذا هو السبب الذي جعل الفيروس ينتشر في نظم البريد الالكتروني خلال ساعات محدودة منذ اطلاقه. و الجدير بالذكر كذلك أن هذا الفيروس كان يعمل بصفة متكاملة حسب برنامج أوتلوك، لكن في برامج أخرى مثل لوتس نوتس، توفيل جروب وليز، نتسكيبماستجر، فان الفيروس لم يكن ينتشر بصفة تلقائية، انما كان يلوث البرامج بالجهاز الذي أرسل اليه و كذلك ملفات word في ذات الجهاز ان أعيد فتحه مرة أخرى. لمزيد من التفاصيل ينظر د/عبد الفتاح بيومي حجازي، (الاحداث

لعقوبات تصل الى 40 عاما، و غرامة نقدية قيمتها 480 ألف دولار، وكان اطلاق سراح ديفيد سميث بكفالة مقدارها 100ألف دولار.[1]

وكذا الحدث "كيفن ميتنك" [2] من اختراقات وتحطيم لأية شبكة معلومات تقع في طريقه والنفاذ إلى داخلها والإحاطة بالأسرار التي بها.

وكذا ما قام به مراهقون – تتراوح أعمارهم ما بين 15 و17 سنة – في ولاية كاليفورنيا، من التسلل عبر الشبكة الانترنت والحصـول علـى آلاف الشفـرات الخاصـة بالتسـلل لمواقع شبكات معلوماتية عن مـختبرين

والإنترنت) مرجع سابق،الهامش رقم 1، ص 177 و ما بعدها؛ محمد فارس، المرجع السابق المنشور على: itwadi.com http://؛ أمير فرج يوسف، المرجع السابق، الموضع السابق.

[1]– و تجدر الإشارة إلى أنه قد تم القبض عليه بعد تتبعه من طرف المباحث الفيدرالية الأمريكية بالتعاون مع فنيين من شركة أمريكا أون لاين. أمير فرج يوسف، المرجع السابق، ص97–98.

[2]–كيفن ميتنك هو حدث جانح ساهمت الظروف الشخصية التي أحاطت به في انحرافه عن طريق الإنترنت (من انفصال والديه في صغر سنه+ الحرمان العاطفي و المادي الذي عاشه) وذلك في شكل اختراق و تحطيم أية شبكة معلومات تقع في طريقه و النفاذ إلى داخلها و الأسرار التي بها، حيث كانت بداياته في اختراق شركة الهاتف المحلية ثم المؤسسات الكبرى ثم وصل إلى البنتاجون بوزارة الدفاع في الولايات المتحدة الأمريكية.و لقد تم القبض على هذا الهاكر مساء يوم 1995/02/15 بإحدى ضواحي مدينة رالي متلبسا باختراق إحدى الشبكات من طرف المباحث الفيدرالية الأمريكية بالتعاون مع أشهر خبير في أمن الشبكات و البرمجة المدعو شيمومورا (و الذي يعمل كمستشار لمكتب التحقيقات الفيدرالي، و القوات الجوية، ووكالة الأمن القومي الأمريكية،و هو يعمل كذلك كمطور لبرامج الكمبيوتر الخاصة بحماية نظم شبكات الكمبيوتر من الاختراق).وتم حبسه احتياطيا على ذمة تقديمه للمحاكمة مع رفض كافة الالتماسات لإطلاق سراحه بكفالة، و لقد اتخذت إجراءات مشددة ضده، حيث لم يتمكن الدفاع عنه من الإطلاع على الأدلة المتخذة ضده. وفي ذلك سابقة تحدث لأول مرة في تاريخ القضاء الأمريكي طبقا لما ورد على لسان دفاعه في المحكمة التي قضت بإدانته في مارس 1999 بالسجن لمدة 68 شهرا في سجن فيدرالي (قضى منها 59شهرا و7أيام و أخلي سبيله لحسن سلوكه) بالإضافة إلى 3سنوات تحت المراقبة، عن جرائم ارتكبها ما بين فبراير1992 وحتى فبراير1995. ولقد تضمنت فترة المراقبة، فضلا عن عدم محدودية مدتها، حظر قيامه بحيازة و لأي سبب كان هواتف نقالة، حواسيب، أية برمجيات حاسوب، ملحقات حاسوب أو دعامة تجهيزه، مساعدات معلوماتية شخصية، مزود اتصالي،أية وسيلة تمكن من الدخول إلى شبكات الحاسوب، و في النهاية كل وسيلة الكترونية و كذلك كل وسيلة تكنولوجية مستقبلة يمكن أن تتحول أو تعمل من خلاله أو لديها القدرة على أن تكون بمثابة نظام حاسوب أو تمكن من الدخول إلى نظام حاسوب أو إلى شبكة حاسوب أو شبكة اتصالات،ذلك كله سواء مباشرة أم من خلال طرف ثالث. وبالإضافة إلى ذلك فقد حظر عليه نظام المراقبة العمل في الاستشارات سواء لأشخاص أو مؤسسات أو مجموعات ذات علاقة بأنشطة الحاسوب. ولكن سمح له باقتناء هاتف بخط اتصالات أرضي فقط.ويعد كيفن ميتنك من أشهر الهكرة الذين تم تصنيفهم في أطر القرصنة الخبيثة في المرحلة المعاصرة وأطلقت عليه تسميات تصنفه في عداد الخطرين على أمن الشبكات و تكنولوجيا المعلومات مثل كاهن العالم الإفتراضيCyberspace Culticon و مطلوب على لائحة المباحث الفيدرالية، حتى أنه لشهرته تهافتت عليه أهزة الاعلام و مؤسساته لنشر سيرته الذاتية و انتاجها سينمائيا أيضا. لمزيد من التفاصيل حول قصة كيفن ينظر مقال:كيفن ميتنك الهاكر الاكبر،نسر ينقض على شبكات الكومبيوتر على الموقع: http:// www.ditnet.Co.ae ؛ و د/ عمر محمد أبو بكر بن يونس،المرجع السابق،ص243 و ما بعدها.

أمريكيين (مختبر ساندیا وأوك بيج) يعملان في إطار برنامج الأسلحة النووية...ألخ.[1]

وقد تم حصر فئات الجناة في مجال جرائم الانترنت في ثلاث طوائف[2] وهي:

أ- **المخترقون أو المتطفلون Crackers&Hackers**

يرتكب أفراد هذه الطائفة هذه الجرائم بدافع التحدي الابداعي و يجدون أنفسهم متفقين الى درجة أنهم ينصبون أنفسهم أوصياء على أمن نظم المعلومات في المؤسسات المختلفة، والسمة الغالبة على أعضاء هذه الطائفة صغر السن و قلة الخبرة و عدم التمييز بين الانظمة محل الاختراق. ولكن هذا لم يمنع مجرموها من اختراق مختلف أنواع نظم المعلومات التابعة للشركات المالية و التقنية

و البنوك و مصانع الالعاب و المؤسسات الحكومية و مؤسسات الخدمة العامة. ومن النماذج المدللة على ذلك: اختراق أحد الصبية الذي يبلغ من العمر 14 عاما نظام المعلومات العائد للبانتجون و آخر لا يتجاوز عمره 17عاما تمكن من اختراق كمبيوترات العديد من المؤسسات الاستراتيجية في أوروبا و الولايات المتحدة الامريكية و من بينها الكمبيوترات المتصلة ببرنامج حرب النجوم الذي كان مخطط لتنفيذه من قبل الولايات المتحدة الامريكية في حقبة الحرب الباردة.

ضف الى ذلك فانهم يتبادلون المعلومات بتشاركهم في وسائل الاختراق و آليات نجاحها و اطلاعهم على مواطن الضعف في نظم المعلومات والشبكات وذلك عن طريق النشرات الإعلامية الالكترونية ومجموعات الاخبار.[3]

وهذه الطائفة من المخترقين أو المتطفلين تنقسم إلى فئتين:

- **فئة الهاكرز الآمن Hacker**: وهو مستخدم حاسوب غرضه التوصل إلى الدخول غير المصرح به إلى نظم الحاسوب، ويقتصر دوره في التسلية لا غير فهو غير مؤذ، فقط إنه يريد أن يسبح بحرية وسلام المفقودين في العالم المادي.مثل ما حدث بنظام شركة مايكروسوفت الأمني في أكتوبر 2000 حيث قامت مجموعة مجهولة من اختراقه دون أن تخربه. أي أنه متطفل همه الوحيد هو تحدي إجراءات أمن النظم والشبكات[4].

---

[1]- ينظر د/ عبد الفتاح بيومي حجازي،(الاحداث و الإنترنت....) مرجع سابق، ص230.

[2]- ينظر د/ جميل عبد الباقي الصغير،(القانون الجنائي و التكنولوجيا الحديثة) مرجع سابق، ص115. وتجدر الاشارة إلى أن هناك من حصر فئات جناة جرائم الإنترنت إلى أربع فئات –وفقا لبعض الدراسات المتخصصة في برامج الإنترنت–و هم:

الفئة الاولى: العاملون على أجهوة الحاسب الآلي في منازلهم.

الفئة الثانية:الموظفون الساخطون على منظماتهم التي يعملون بها.

الفئة الثالثة:فئة المتسللين Crackers&Hackers.

الفئة الرابعة: العاملون في الجريمة المنظمة. لمزيد من التفاصيل ينظر د/حسين الغافري، محمد الالفي، المرجع السابق، ص39- 40.

[3]-د/ أيمن عبد الله فكري، المرجع السابق، ص 108.

[4]-د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 240.

وتجدر الإشارة إلى أن الهاكر في هذه الفئة يعتبر كالمستكشف Exploiter.

- الفئة الثانية: وهو الكراكر cracker أو الهاكر الخبيث أو المحترف أو المخترق ذو النوايا الإجرامية أو العنكبوت araignées[1] ويمثل هذا الأخير التهديد المباشر والكامل والخطير للمصالح عبر الانترنت إذ يتسلل بصورة خفية إلى مواقع مختارة بعناية لارتكاب جريمته سواء كانت في صورة الإتلاف،أو التخريب أو الإرهاب أو الابتزاز أو العدوان على الأموال بالسرقة والنصب.[2] ولا تعيقه في ذلك الظروف المختلفة حتى لو كانت سيئة، لأن الذي يحكمه هي فكرة البطولة الطفولية. ومن الأمثلة على ذلك: ما حدث أثناء محادثات السلام في كامب ديفيد الثانية، من اختراق لنظام توزيع البريد الإليكتروني للصور التابع لوزارة الخارجية الأمريكية.[3] وما حدث يوم 2001/01/05 من قيام الهكرة من معادي العولمة الاقتصادية باختراق معلوماتي واختلاس معلومات سرية عن المنتدى وعن الرئيس الأمريكي الأسبق "بيل كلينتون" وعدد من قادة منتدى دافوس الاقتصادي.[4] و لعل المظهر الخطر في هذه الفئة هو قسم الأطفال المهرة whiz-kids الذين لا يدركون أعمالهم.

هذا من جهة و من جهة أخرى، وللدلالة على خطورتهم فإنهم يتبادلون المعلومات بتشاركهم في وسائل الاختراق و آليات نجاحها و إطلاعهم على مواطن الضعف في نظم المعلومات والشبكات و ذلك عن طريق النشرات الإعلامية الالكترونية و مجموعات الاخبار(newsgroups ou mailing lists).أو عن طريق تنظيم مؤتمرات وتجمعات لمخترقي نظم المعلومات يدعى لها الخبراء من بينهم للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم فيما بينهم كما هو الشأن في Chao Computer Club de Hambourg وجمعية تصفية واختراق الحواسيب (CLODO) في فرنسا والتي تقدر (الاختراقات) ب 90%.[5]

---

[1]- لقد برز هذا المصطلح مع العام 1985.

-«Les cracker se cachent dans l'ombre ،laissent des traces déplaisantes de leur passage et peuvent être dangereux.on les appelle araignées (spiders) ».Voir Dr/ Mohamed BUZABAR,op.cit, p 47. Mohamed N.SALAM , op.cit,p28-29.

[2]- Voir Mohamed N.SALAM, ibid,p30

[3]- تتلخص وقائع هذه القضية في أن قراصنة قاموا بإرسال فيروسا جديدا غير معروف إلى مجموعة من الموظفين والصحفيين ترتب عليه عدم إمكانية تحميل صور الرؤساء المجتمعين،و كانت الرسائل مرسلة إلى عنوان وزارة الخارجية/ مكتب الدبلوماسية العامة و تحمل عنوان" نكت ضاحكة". و بمجرد فتحها فان فيروسا غير معروف يبدأ في تدمير القرص الصلب ثم يرسل إلى كل عنوان بريدي موجود في الجهاز. د/ عمر محمد أبو بكر بن يونس،المرجع السابق، الموضع السابق.

[4]-د/ عمر محمد أبو بكر بن يونس، نفس المرجع، ص 241.

[5]-Dr/ Mohamed BUZABAR,op.cit, p 47

ب- مجرمي المعلوماتية المحترفون Crasher ou Nukers:

تتميز هذه الطائفة بسعة الخبرة و الإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم و التخطيط للأنشطة التي ترتكب من قبل أفرادها ولذلك التي ترتكب من قبل أفرادها[1]. و لذلك فان هذه الطائفة تعد الأخطر من مجرمي التقنية، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم نظم المعلومات عامة وجرائم الانترنت خاصة. كما تهدف إلى تحقيق أغراض سياسية و التعبير عن موقف فكري أو نظري أو فلسفي.[2]

ويقسم أفراد هذه الطائفة إلى مجموعات متعددة إما تبعا لتخصصهم بنوع معين من الجرائم أو تبعا للوسيلة المتبعة من قبلهم في ارتكاب الجريمة.وعلى عكس أفراد الطائفة الأولى (المخترقون أو المتطفلون Crackers&Hackers) فان أفراد هذه الطائفة يتسمون بالتكتم. فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة و يحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم. [3]

هذا من جهة ومن جهة أخرى،فان أفراد هذه الطائفة - وفقا للدراسات-هم من الشباب الأكبر سنا من الطائفة الأولى.إذ أن معظمهم تتراوح أعمارهم ما بين 26-40 عاما.[4]

ج- الحاقدون:

و على عكس الطائفتين السابقتين فان أفراد هذه الطائفة أقل خطورة و يغلب عليهم عدم توفر أهداف وأغراض الجريمة، فهم لا يسعون إلى إثبات المقدرات التقنية و المهارية و لا حتى إلى تحقيق مكاسب مادية أو سياسية، و إنما يحرك أنشطتهم الرغبة بالانتقام و الثأر كأثر لتصرف صاحب العمل معهم عندما لا يكونوا موظفين فيها. و لهذا فإنهم ينقسمون إما إلى مستخدمين للنظام بوصفهم موظفين أو مشتركين أو على علاقة بالنظام محل الجريمة، و إلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم. إذ تلجأ هذه الفئة غالبا إلى استخدام تقنيات الفيروسات و البرامج الضارة و تخريب النظام أو إتلاف كل أو بعض معطياته أو نشاط إنكار الخدمة و تعطيل النظام أو الموقع المستهدف التي تسبب أضرارا جسيمة و خسائر فادحة بالمؤسسات المستهدفة.[5]

و تجدر الإشارة إلى أن هؤلاء الجناة تحكمهم دوافع[6] و أهداف عديدة ومتنوعة في ارتكابهم لجرائم الانترنت فقد تكون من أجل جمع المعلومات التي تكون محفوظة على أجهزة الحاسب الآلي أو منقولة عبر شبكة

---

[1]-Voir Mohamed N.SALAM,op.cit, p31-32.

[2]- د/ أيمن عبد الله فكري، المرجع السابق، ص110.

[3]- د/ يونس عرب:جرائم الكمبيوتر و الإنترنت، المعنى و الخصائص و الصور و إستراتيجية المواجهة القانونية، http:// www.arablaw. Org

[4]- د/ يونس عرب، نفس المرجع، المنشور على نفس الموقع.

[5]- د/ يونس عرب، المرجع السابق ، المنشور على الموقع السابق.

[6]- الدافع أو الباعث أو الغاية تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي،تتصل بما يعرف بالقصد الجنائي الخاص، و هي مسألة تثير جدلا فقهيا و قضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد

الانترنت، وقد تكون من أجل الإضرار بأشخاص أو جهات معينة، وقد تكون سعيا وراء الربح المادي أو إبراز الذات أو تهديد للأمن القومي والعسكري وغيرها.[1]

المطلب الثاني:

الفرق بين جرائم الانترنت وغيرها من الجرائم.

إن جرائم الانترنت هي إفراز ونتاج للتقدم العلمي والتكنولوجي وكذا لتقنية المعلومات، المفترض تسخيرها لخدمة الدول والمجتمعات إلى إعطائها طابعا قانونيا خاصا يميزها عن غيرها من الجرائم سواء التقليدية أو الجرائم المستحدثة المشابهة لها.

وعلى هذا جاء تقسيم هذا المطلب إلى الفرعين التاليين كما يلي:

الفرع الأول: الفرق بين جرائم الانترنت والجرائم التقليدية

الفرع الثاني: الفرق بين جرائم الانترنت والجرائم المستحدثة المشابهة لها.

الفرع الأول: الفرق بين جرائم الانترنت والجرائم التقليدية:

لقد سبق وأن عرفنا في بداية فصلنا هذا الجريمة (التقليدية) بأنها:

"كل سلوك إنساني غير مشروع صادر عن إرادة إجرامية، يفرض له القانون جزاء جنائيا".[2] وانتهينا إلى اعتبار جرائم الانترنت بأنها: "كل سلوك رادي غير مشروع، صادر عن شخص ذي دراية فائقة بأمور الحوسبة، معاقب عليه قانونا بجزاء جنائي تكون شبكة الانترنت محلا له أو وسيلة لارتكابه"[3].

الجنائي و أن الباعث لا أثر له في وجود القصد الجنائي.ويقصد بالباعث " العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة و الشفقة و البغضاء و الانتقام"، أو هو " ا لمصلحة أو الإحساس الذي حرك الجاني أو دفعه لارتكاب الجريمة".أي أنه عبارة عن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة.و هو يختلف من جريمة إلى أخرى، تبعا لاختلاف الناس من حيث السن و الجنس ودرجة التعليم و غير ذلك من المؤثرات. كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر.ينظر على التوالي:د/محمد زكي أبو عامر:قانون العقوبات، القسم العام، دار الجامعة الجديدة، الإسكندرية، 2007، 258-260.د/محمود نجيب حسني: شرح قانون العقوبات، القسم العام، الطبعة السابعة، دار النهضة العربية، القاهرة، 1989، ص1052.د/أحمد فتحي سرور: الوسيط في قانون العقوبات، القسم العام، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991، ص 427.د/ علي عبد القادر القهوجي: شرح قانون العقوبات، القسم العام، الكتاب الأول، دار المطبوعات الجامعية، الإسكندرية، 1997، ص48.د/فتوح عبد الله الشاذلي: قانون العقوبات، القسم العام، الكتاب الأول، دار المطبوعات الجامعية، الإسكندرية،1998، ص 69.د/فوزية عبد الستار: شرح قانون العقوبات، القسم العام، دار النهضة العربية،القاهرة،1992،ص479.

[1]- لمزيد من التفاصيل ينظر د/حسين الغافري، محمد الألفي، المرجع السابق،ص 45 وما بعدها؛ د/ جميل عبدالباقي الصغير،(الإنترنت و القانون الجنائي) مرجع سابق، ص23؛ د/ يونس عرب، المرجع السابق ، الموجود على الموقع السابق؛ دور الحاسوب في الجريمة المعلوماتية و محل الجريمة، مقال سابق ، ص5، http://feeds.feedburner.com

[2]- ينظر ص12من هذه الرسالة.

[3]- ينظر ص26 من هذه الرسالة.

وانطلاقا من هذا يمكن استخراج نقاط الاختلاف بين الجريمتين، وسيتم ذلك عن طريق استخلاص أوجه التشابه و الاختلاف.وهذا كما يلي:

أولا: أوجه التشابه بين الجريمتين:

ويمكننا حصر أوجه الشبه بين الجريمتين في النقاط التالية:

1/ غياب التعريف القانوني لكلا الجريمتين: فالمشرع و كما هو متعارف عليه في لغة القانون لا يعرف الجريمة لأن ذلك ليس من اختصاصه بل من اختصاص الفقه و القضاء (في بعض الأحيان). غير أنه وللضرورة الملحة يجد نفسه مضطرا إلى ذلك، إما لتحديد أركان الجريمة العامة أو الخاصة، أو تحديد السلوك الإجرامي المستحدث للجريمة[1].

2/ كلاهما يمثل جريمة تهدد مصالح وكيان المجتمع: إذ يعتبر كلا منهما سلوكا إراديا إنسانيا غير مشروع يهدد مصلحة أو حق أو مال محمي قانونا بجزاء جنائي.

3/ يفرض القانون مقابل ارتكابهما جزاء جنائيا: أي يعاقب على اقترافهما إما بعقوبة (إعدام، سالبة للحرية، غرامة مالية) أو بتدبير أمن.

4/ يشترط لقيام كلتا الجريمتين أركان، وأن اختلف الفقه الجنائي حول عددها من ركنين إلى ثلاثة أركان.أي عدم اعترافهم بوجود ركن شرعي معتبرينه شرطا أوليا للتجريم أو أنه من شروط التجريم التي يتعين البحث في توافرها قبل البحث في أركان الجريمة ذاتها.و مبررين ذلك بأنه لا يمكن أن يكون هذا الأخير ركنا في هذه الجرائم باعتباره خالقها، فكيف يصبح الخالق جزء في المخلوق ؟...، فهم بذلك يعترفون بوجود ركنين فقط وهما: الركن المادي والركن المعنوي.[2]

5/تمر هاتين الجريمتين بالمراحل التي تمر بها أية جريمة: من مرحلة التفكير و التخطيط و التحضير فالتنفيذ.

6/ يوجد في كلتا الجريمتين جاني يمثل الطرف الايجابي فيها و مجني عليه يمثل الطرف السلبي فيها.

---

[1]– ينظر ص15 من هذه الرسالة.

[2]–انقسم الفقه الجنائي إلى مذاهب شتى في تحديد أركان الجريمة. فهناك من رأى أن لها ركنا واحدا هو الركن المادي (الاتجاه الموضوعي أو المادي)و على عكس الرأي السابق، يوجد اتجاه آخر يرى أن الركن المعنوي هو الركن الوحيد للجريمة (الاتجاه الغائي) و هناك من يرى أن لها ثلاثة أركان: ركن شرعي، ركن مادي، ركن معنوي.و هناك من يكتفي بوجود الركنين الأخيرين فقط، أما الركن الشرعي فيعتبرونه شرطا أوليا للتجريم أو من شروط التجريم التي يتعين البحث في توافرها قبل البحث في أركان الجريمة ذاتها.ينظر على التوالي د/ علي عبد القادر القهوجي،(شرح قانون العقوبات) مرجع سابق، ص 41 و ما بعدها.د/فتوح عبد الله الشاذلي، المرجع السابق، ص66. د/زكي أبو عامر، د/سليمان عبد المنعم: القسم العام من قانون العقوبات، دار الجامعة الجديدة، الإسكندرية، 2002 ص 135 و ما بعدها.د/ عبد الفتاح الصيفي، المرجع السابق، ص 63.د/ جلال ثروت، المرجع السابق،ص 136 و ما بعدها.عبد الله سليمان، المرجع السابق، ص68 وما بعدها.

ثانيا: أوجه الاختلاف بين الجريمتين:

وفي مقابل ذلك فهما يختلفان في النقاط التالية:

1/ من حيث الطبيعة القانونية: تعتبر جرائم الانترنت من الجرائم المستحدثة والخطيرة المصنفة ضمن جرائم التقنية العالية و بالضبط جرائم نظم المعلومات والتي تكون فيها الشبكة الأم إما وسيلة لارتكابها أو محلا لها و يستخدم فيها الحاسب الآلي كأداة لتسهيل ارتكابها.على عكس الجرائم التقليدية التي هي جرائم عادية (وقد تكون خطيرة في بعض المرات) وتستخدم في ارتكابها وسائل تقليدية كالأسلحة النارية أو البيضاء أو السم في جرائم القتل، أو المفاتيح المقلدة في جريمة سرقة البيوت... الخ[1].

2/ من حيث الأدلة: لقد سبق التأكيد على أن جرائم الانترنت تمتاز بمجموعة من الخصائص تميزها عن غيرها من الجرائم لا سيما تلك التقليدية ومن أهمها: صعوبة إثباتها واكتشافها، لكون الأدلة فيها أدلة الكترونية غير مرئية وغير مادية و غير ملموسة فهي عبارة عن نبضات إلكترونية تنساب عبر أجهزة الحواسيب وشبكة الشبكات[2]، وعلى هذا يمكن القول بأن جرائم الانترنت، جرائم تستهدف معنويات وليست ماديات محسوسة [3]،على عكس الجرائم التقليدية التي تكون فيها الأدلة مادية محسوسة ومرئية. فعلى سبيل المثال يكون الدليل في جريمة القتل إما وجود بصمات الجاني على سلاح الجريمة أو على الجثة، أو وجود سلاح الجريمة على مسرح الجريمة كأن يكون مسدسا أو سكينا.. وكأن يكون ذلك الدليل في جريمة تزوير المحررات توقيع المزور، وفي جريمة الاغتصاب نطفة أو بصمة وراثية أخرى....[4]

وتجدر الإشارة إلى أنه ونظرا لطبيعة الأدلة في جرائم الانترنت، فإنه يمكن تدميرها وإخفاء معالم الجريمة في ثوان معدودة. عكس الجرائم التقليدية التي قد يستغرق ذلك ساعات قد تصل إلى أيام فشهور..[5]

3/ من حيث مسرح الجريمة: مسرح الجريمة في جرائم الانترنت هو العالم الإفتراضي أي عالم الشبكات الإلكترونية أو هو الفضاء الإلكتروني الذي لا حدود له،[6] فهو بذلك غير موجود.على عكس الجرائم

---

[1]– لمزيد من التفاصيل ينظر الحلقة العلمية: الدليل الرقمي و التحقيق في الجرائم الالكترونية، المنعقدة من 22 إلى 1429/12/27، كلية علوم الادلة الجنائية، جامعة نايف العربية للعلوم الامنية، ص 27.

[2]– ينظر ص42 من هذه الرسالة.

[3]– د/ أيمن عبد الله فكري، المرجع السابق، ص93.

[4]– لمزيد من التفاصيل ينظر الحلقة العلمية (الدليل الرقمي و التحقيق في الجرائم الالكترونية) مرجع سابق، ص9؛ سامح محمد عبد الحكم : جرائم الإنترنت الواقعة على الأشخاص في إطار التشريع البحريني، دراسة مقارنة بالتشريع المصري، دار النهضة العربية، القاهرة، 2007 ، ص 3.

[5]– ينظر ص42 من هذه الرسالة.

[6]– د/ عبد الله عبد الكريم عبد الله:جرائم غسل الأموال على شبكة الإنترنت، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2008،ص 39.

التقليدية التي يوجد فيها مسرح للجريمة فيه أدلة مادية ثابتة للمعاينة.[1]

4/ من حيث طبيعة الركن المادي:

من المعروف في القانون الجنائي بأن الركن المادي[2] يتكون من عناصر ثلاثة وهي: السلوك الإجرامي أو النشاط الإجرامي والنتيجة وعلاقة السببية. والنشاط الإجرامي في الجرائم الانترنت يختلف عن ذلك في الجرائم التقليدية، لأن هذا الأخير يعتبر عملا خياليا للغاية.[3]

هذا من جهة ومن جهة أخرى، يجب أن يشتمل على نشاط تقني محدد يتمثل في استخدام الحاسوب والانترنت أي أنه لارتكاب جرائم الانترنت يجب توفر منطق تقني.[4]على عكس الجرائم التقليدية الذي يكون فيها النشاط الإجرامي ماديا لا يحتاج إلى التقنية العالية اللازم توفرها في الجرائم الأولى.

5/ من حيث القانون المطبق: تخضع الجرائم التقليدية إلى تطبيق نصوص القوانين الجنائية التقليدية (قانون العقوبات + قانون الإجراءات الجزائية)،على عكس جرائم الانترنت التي تعجز تلك القوانين عن مواجهتها وتعتبر قاصرة عن التطبيق عليها،و خصوصا قانون الإجراءات الجزائية وما تتضمنه من إجراءات تمس بحقوق وحريات الأفراد. إذ يجب أن تتعامل هذه الأخيرة بشكل عصري متقدم يتناسب مع طبيعة هذا الإجرام المنفرد وخاصة فيما يتعلق بإجراءات التفتيش والمعاينة و المحافظة على الأدلة، وكذا ضبطها...الخ[5]. أو بعبارة أخرى فإن المواجهة التشريعية تسير بسرعة السلحفاة في مواجهة جرائم الانترنت التي تنطلق كالصاروخ بسرعة الضوء.

هذا من جهة ومن جهة أخرى، فجرائم الانترنت تتميز بتعديها للحدود الجغرافية و القضائية. إذ لا تقتصر على دولة معينة، وإنما تتخذ من العالم كله مسرحا لها. الأمر الذي يثير مشكلة تحديد القانون الجنائي الواجب التطبيق بين الدول المختلفة، بل تثير مشكلة تحديد المحكمة المختصة داخل الدولة الواحدة، إذا وقعت الجريمة ضمن اختصاص محكمتين قضائيتين محليتين أو أكثر،فتثور في هذه الحالة مشكلة التنازع الإيجابي في الاختصاص.[6] على عكس الجرائم التقليدية التي ترتكب داخل إقليم دولة معينة ويطبق عليها

---

[1]– سامح محمد عبد الحكم،المرجع السابق، ص 7؛ الحلقة العلمية (الدليل الرقمي و التحقيق في الجرائم الالكترونية) مرجع سابق، ص3.

[2]– يقصد بالركن المادي: تجسيد للحالة النفسية و الباطنية للفاعل لأنه ينقل الفكر الباطني إلى العالم الخارجي بماديات الجريمة.د/معز أحمد محمد الحيارى: الركن المادي للجريمة، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2010، ص93.

[3]– د/ عبد الله عبد الكريم عبد الله،المرجع السابق، الموضع السابق.

[4]– أي أنها تتطلب وجود بيئة رقمية و اتصال بالإنترنت، و كذا معرفة بداية هذا النشاط و الشروع فيه و نتيجته. لمزيد من التفاصيل ينظر د/ محمد قطب: الجرائم المعلوماتية و طرق مواجهتها، الجزء الثاني، الاكاديمية الملكية للشرطة، البحرين، 2010، ص3.

[5]– د/ محمود صالح العادلي، (الفراغ التشريعي في مجال مكافحة الجرائم الالكترونية) بحث سابق، http://dreladly.com

[6]– د/جميل عبد الباقي الصغير،(الجوانب الإجرائية للجرائم المتعلقة بالإنترنت) مرجع سابق، ص 8.

قانون ذلك الإقليم وتحدد المحكمة المختصة فيه. كما يتحدد الاختصاص المحلي لأجهزة العدالة فيها(ضبطية قضائية+قاضي التحقيق+ النيابة العامة) وفقا لقواعد عامة معروفة في القانون الإجراءات الجزائية وهي: إما مكان وقوع الجريمة أو مكان القبض على المتهم أو أحد المساهمين في الجريمة حتى ولو كان هذا القبض قد حصل لسبب آخر،أو محل إقامتهم.[1]

6/ من حيث المحل:محل الإعتداء في جرائم الانترنت أو وسيلة هذا الإعتداء تتمثل في مفردات جديدة تختلف عن مفردات الجرائم التقليدية وهي البرامج والبيانات.[2]

7/ من حيث صفات الجاني: يختلف الجاني في جرائم الانترنت عن مثيله في الجرائم التقليدية:

فالجاني في هذه الجرائم يسمى إما مجرما تقنيا أو هاكرا أو مجرما معلوماتيا أو مجرم الانترنت وهو يتمتع في غالب الأحيان بقدر كاف من العلم و بالمعرفة التقنية لدرجة تساويه في السمات مع مجرمي ذوي الياقات البيضاء.[3]

وهو يختلف عن المجرم العادي الذي يرتكب الجرائم التقليدية، في كونه يتمتع بشخصية مستقلة. فهو من جهة مثال منفرد عن المجرم الذكي، بامتلاكه الجبروت في الاختراق وارتكاب أفعال تقنية عبر العالم الإفتراضي بطريقة لا يمكن للناس العاديين أو العامة القيام بها.

وهو من جهة أخرى إنسان اجتماعي بطبيعته.[4]

هذا من جهة ومن جهة أخرى، فإنه يصعب ملاحقة مرتكب هذه الجرائم لاستحالة تحديد هويتهم، سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها. وذلك راجع لاستخدامهم الأسماء المستعارة أو من خلال دخولهم للشبكة عن طريق مقاهي الانترنت. ضف إلى ذلك إمكانية إقامة هؤلاء الجناة في دولة أخرى لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه.[5]

---

[1]– ينظر المواد التالية من قانون الإجراءات الجزائية الجزائري: المادة 16،37،40.

[2]– د/حسنين المحمدي بوادي: إرهاب الإنترنت، الخطر القادم، الطبعة الأولى، دارا لفكر الجامعي، الإسكندرية،2006،ص76.

[3]– يقصد بجرائم ذوي الياقات البيضاء White Collar Crime أو La criminalité en colblanc تلك الجرائم التي يرتكبها مجرمون ذات طبيعة خاصة و هم الفئة التي لديها من الخبرات و المعرفة بالتقنية الكثير و لا سيما في جرائم الرشوة و الاستيلاء على الأموال و تزوير البيانات و المستندات و تزوير الأوراق المالية و التلاعب بأسواق البورصة. ولقد تم اكتشافها من قبل الأمريكي SUTHERLAND من خلال دراسته المسمات ب white collar criminality التي أجراها عام 1939م.ينظر لمزيد من التفاصيل كلا من: أمير فرج يوسف، المرجع السابق، ص64

Mohamed CHAWKI , op.cit,p28-29-30.

[4]– د/ عبد الفتاح بيومي حجازي، (نحو صياغة نظرية عامة في علم.....) مرجع سابق،ص96.

[5]– د/جميل عبد الباقي الصغير،(الجوانب الإجرائية.....) مرجع سابق،ص6.

ومن جهة ثالثة، فإن هؤلاء المجرمين يختلفون عن المجرمين التقليديين لأنهم يقضون أوقاتا طويلة على جهاز الحاسوب، كما أن سلاحهم ليس ناريا أو أداة حادة وإنما عقل وبرنامج وفيروسات لاختراق برامج حاسوبية[1].

8/ من حيث طريقة تنفيذ الجريمة: من تتميز الجرائم التقليدية بأنها جرائم يستعمل فيها العنف وتسفك الدماء عند ارتكابها على عكس جرائم الانترنت التي تعتمد على الذكاء، فهي كما سبق الذكر من جرائم الإغراء و الحيلة فلا عنف فيها ولا سفك للدماء، ولا آثار لاقتحام لسرقة الأموال[2].

9/ من حيث الضحايا:جرائم الانترنت غالبا ما تقيد ضد مجهول، وفي حالة اكتشافها فمن الصعب إقامة الدليل عليه ومحاكمته. ولكن في الغالب يحجم المجتمع (مجتمع الأعمال) عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة في كفاءته.[3] على عكس الجرائم التقليدية التي قد تقيد ضد المجهول أو ضد معلوم.

10/ من حيث الوسيلة المستعملة في ارتكاب الجريمة: يشترط لقيام جرائم الانترنت وجود شبكة إنترنت مرتبطة بالحاسب الآلي الذي يعتبر أداة لارتكابها على عكس الجرائم التقليدية التي تتنوع أدوات ارتكابها ولكنها تظل أدوات تقليدية وإن أمكن ارتكابها عن طريق الانترنت[4].

11/ من حيث الاضرار الناتجة عن الجريمة: كما أن هذه الجرائم تسبب ازدياد نسب وحجم الخسائر مقارنة بالجرائم التقليدية[5].

و تجدر الاشارة إلى أنه في ظل جرائم الانترنت يصعب الفصل بين العمل التحضيري و البدء في النشاط الاجرامي. ضف إلى ذلك فإنه و إن كان القانون لا يعاقب على الاعمال التحضيرية، إلا أن الامر يختلف في مجال تكنولوجيا المعلومات فحيازة صور دعارة للاطفال أو شراء برامج اختراق أو معدات لفك شفرات وكلمات المرور تمثل في حد ذاتها جرائم.[6]

الفرع الثاني: الفرق بين جرائم الانترنت و الجرائم المستحدثة المشابهة لها:

لقد سبق وأن بينا نقاط التشابه والاختلاف بين جرائم الانترنت والجرائم التقليدية. بحيث اعتبرت تلك الجرائم مستحدثة ومن التقنية العالية و الخطيرة و كذا المتجاوزة للحدود الجغرافية على عكس الجرائم التقليدية.

غير أن اختلافها هذا لا يقتصر على تلك النوعية من الجرائم باعتبارها تقليدية وعادية ومنحصرة في إقليم معين. بل قد تختلف وتتفق مع غيرها من الجرائم المستحدثة والمشابهة لها، كالجريمة المنظمة وجريمة

---

[1]– د/محمد صالح العادلي،(الفراغ التشريعي في مجال مكافحة الجرائم الالكترونية) بحث سابق، http://dreladly.com

[2]– ينظر ص48 من هذه الرسالة .

[3]– ينظر ص43 من هذه الرسالة .

[4]– ينظر ص38 من هذه الرسالة .

[5]– ينظر ص31 و ما بعدها من هذه الرسالة .

[6]– د/محمد قطب: جرائم الاخلاق و الآداب عبر الشبكة الدولية للمعلومات(الإنترنت) و دور التدريب في مواجهتها، مجلة الامن العام، العدد 199، س 49، أكتوبر 2007، ص 91 و ما بعدها.

الحاسوب أو ما تسمى الجريمة المعلوماتية و الجريمة التقنية وجريمة الاتصال عن بعد. وسيتم توضيح ذلك في النقطتين التاليتين:

أولا: أوجه التشابه بين جرائم الانترنت و غيرها من الجرائم المستحدثة المشابهة لها.

ثانيا: أوجه الاختلاف بينها وبين غيرها من الجرائم المستحدثة المشابهة لها.

غير أنه قبل الخوض في ذلك يجب أن نعرف كلا من تلك الجرائم.

– تعريف الجريمة المنظمة:

"هي نشاط إجرامي يتم خارج إطار القانون و الضوابط الاجتماعية، ويضم بين طياته الآلاف من المجرمين الذين يعملون وفقا لنظام بالغ التعقيد و الدقة، يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها لأحكام قانونية سنوها لأنفسهم تفرض أحكاما بالغة القسوة على من يخرج على قاموس الجماعة المنظمة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة ويجنون من وراءها الأرباح الطائلة".[1]

– تعريف جريمة الحاسوب أو الجريمة المعلوماتية:لقد تعددت التعريفات حول جرائم الحاسوب[2]، و يمكن تعريفها بأنها: نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.

---

[1]– هذا التعريف انتهت إليه لجنة من رجال القضاء و الأمن لدراسة ظاهرة الإجرام المنظم في الولايات المتحدة الأمريكية عام 1987.و تعرف الجريمة المنظمة كذلك بأنها:"جريمة ذات أبعاد جديدة تفوق عصابات المافيا من حيث الدقة و التنظيم، وتتسم بعناصر تجعل من العصابات المنظمة وحدة متناسقة تمتلك القوة المالية و الوحشية في آن واحد، و ذلك بهدف الحفاظ على كيانها الداخلي من جهة، ولمواجهة أي تدخل خارجي من جهة أخرى."أو "بأنها أشكال مختلفة من الأنشطة المشروعة التي ساعدتها على مد نفوذها و التغلغل إلى أجهزة الدولة و اقتصادها"أو بأنها " شكل من أشكال التجارة الاقتصادية بوسائل غير قانونية تنطوي على التهديد باستعمال القوة البدنية و الإكراه و الفساد و الابتزاز و غير ذلك من الأساليب التي تساعدها على تقديم الخدمات غير المشروعة"و عرفت من قبل الوفد المصري في المؤتمر التاسع لمنع الجريمة و معاملة المجرمين بأنها "مشروع إجرامي يمارسه مجموعة من الأفراد بتنظيم مؤسس ثابت، له بناء هرمي و مستويات للقيادة، و مستويات للتنفيذ و فرص للترقي، و يحكمه نظام داخلي صارم، ويستخدم الإجرام و العنف و التهديد و الابتزاز و الرشوة في إفساد المسئولين و فرض السطوة بهدف تحقيق أرباح طائلة بوسائل غير مشروعة، حتى ولو اتخذ قالبا شرعيا من الناحية القانونية ".لمزيد من التعاريف ينظر: د/عبد الفتاح بيومي حجازي، (الأحداث و الإنترنت....) مرجع سابق، ص60 و ما بعدها، د/ محمد الأمين البشري، المرجع السابق، ص 41–42، د/ هدى حامد قشقوش:جريمة غسل الأموال في نطاق التعاون الدولي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1998،ص 62 وما بعدها، 1/أمير فرج يوسف، المرجع السابق، ص61، مصطفى إبراهيم عيسى: جرائم العصر، مجلة الأمن و الحياة، العدد340،السنة 29أوت / سبتمبر 2010، ص 60–61. د/ شريف سيد كامل: الجريمة المنظمة في القانون، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001، ص12.

[2]– فمنها من تناولت الجانب الموضوعي لهذه الجرائم ومنها من ركزت على الوسيلة. ومنها من عرفتها باعتبارها جرائم مرتبطة بالمعرفة الفنية أو التقنية. و من هذه التعريفات نذكر تعريف TIEDEMANN المعتبر إياها:"كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"،و في تعريف آخر بأنها:"اعتداءات غير مشروعة ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"،و عرفها كلا منA.HARDCASTLEG&R.TATTOY بأنها:"تلك الجرائم التي يكون قد وقع في

– تعريف الجريمة التقنية:

" ويتسع مدلول هذه الجريمة لكي يشمل كل الجرائم التي تستخدم فيها الوسائل التكنولوجية لارتكابها كجرائم الحاسوب والانترنت وجرائم استخدامات التقنية – والتي يعتد فيها بالوسيلة – مثل استخدام تقنية الهاتف النقال لارتكاب جرائم السب والقذف"[1]

– تعريف جريمة الاتصال عن بعد:

" هي كل عمل يقوم على الاحتيال في استخدام الهاتف أو أجهزة الموجات الدقيقة أو أجهزة البث أو أي أنظمة اتصال عن بعد."[2]

أولا:أوجه التشابه بين جرائم الانترنت وغيرها من الجرائم المستحدثة المشابهة لها.

تعرف جرائم الانترنت بأنها: كل سلوك إرادي غير مشروع، صادر عن شخص ذا دراية فائقة بمجال الحوسبة، معاقب عليه قانونا بجزاء جنائي، تكون شبكة الانترنت محلا له أو وسيلة لارتكابه.

ومن خلال ما تقدم يمكننا حصر أوجه التشابه بين جرائم الانترنت و غيرها من الجرائم المستحدثة في النقاط التالية:

1/ من حيث الطبيعة القانونية: تعتبر هذه الجرائم أو تصنف ضمن الجرائم المستحدثة والخطيرة التي تهدد مصالح المجتمع وتهز كيانه، وهي تختلف كثيرا عن الجرائم التقليدية. وتجدر الإشارة إلى اشتراك كلا من جرائم الانترنت والجرائم المعلوماتية (جرائم الحاسوب) في طبيعتهما القانونية. فهي تصنف في خانة الجرائم المستحدثة الخطيرة وبالتحديد جرائم التقنية العالية أي جرائم نظم المعلومات، التي يترتب عنها نتائج وخيمة وضارة بجميع المستويات سواء الاجتماعية أو الاقتصادية أو السياسية، وسواء كانت شخصية (متعلقة بفرد) أو دولية (متعلقة بدولة).

مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسب،و بعبارة أخرى تلك الجرائم التي يكون دور الحاسب فيها ايجابيا أكثر منه سلبيا"، و عرفها فريق آخر من الفقه بأنها:"كل سلوك غير مشروع معاقب عليه قانونا صادر عن ارادة اجرامية محله معطيات الحاسب "، أو بأنها:" كل جريمة يستخدم فيها الحاسب كأداة لارتكابها أو يمثل اغراء بذلك أو هي جريمة يكون الحاسب نفسه ضحيتها"، أو بأنها:" الجريمة التي يتم ارتكابها اذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني "، أو كما يعرفها David THOMPSON بأنها:":" أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".....الخ. ينظر في ذلك كلا من: د/عبد الفتاح بيومي حجازي، (نحو صياغة نظرية عامة....) مرجع سابق، ص21 و ما بعدها، د/ عبد الفتاح مراد، المرجع السابق، ص 40، د/ أيمن عبد الله فكري، المرجع السابق، ص82 و ما بعدها، د/ طارق إبراهيم الدسوقي عطية: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية،2009، ص 149 و ما بعدها، محمد أمين أحمد الشوابكة، المرجع السابق،ص 9 و ما بعدها، محمد خليفة، المرجع السابق، ص 77 وما بعدها، أسامة أحمد المناعسة و جلال محمد الزغبي وصايل فاضل الهواوشة، المرجع السابق، ص 72 و ما بعدها.

1– د/ عمر محمد أبو بكر بن يونس،المرجع السابق، ص 219.

2– د/ عمر محمد أبو بكر بن يونس، نفس المرجع، ص 222.

هذا من جهة ومن جهة أخرى، ففي كلتيهما تستعمل التقنية العالية لارتكابهما. أي الانترنت والحاسب الآلي الذي يعتبر سلاح الجريمتين أو بالأحرى أداة لارتكاب الجريمتين. كما يجب أن يتمتع مرتكبها بصفات وسمات عالية تتماشى مع مستوى المحيط الذي يتعامل معه ومع نوع الجريمة الذي يرغب في ارتكابها.[1]

كما تشترك جرائم الانترنت و الجرائم المعلوماتية في خاصية صعوبة اكتشافها وإثباتها، وذلك راجع إلى الأدلة المتميزة بأنها غير مرئية – على العموم – ويمكن محوها وتدميرها في ثوان قليلة معدودة على الأصابع، إما من طرف المجرم أو من المحقق في هذه الجرائم، بسبب خطئه أو إهماله أو نتيجة التعامل بخشونة مع الأقراص المرنة.[2]

2/ من حيث العقاب: يعاقب القانون على ارتكاب هذه الجرائم بفرض جزاءات جنائية تتلاءم مع هذه النوعية من الجرائم.

3/ من حيث النظام القانوني: يشترط لقيام كل من هذه الجرائم ثلاث أركان: وهي الركن الشرعي، الركن المادي، الركن المعنوي. أي أنها كغيرها من الجرائم لها أركانها وعناصرها.

4/ من حيث الخصائص التي تتمتع بها: تشترك جرائم الانترنت و الجرائم المستحدثة المشابهة لها في خاصية عدم اعترافها بالحدود الجغرافية المتعارف عليها في العالم المادي، إذ تعتبر هذه الجرائم جرائم عابرة للحدود الدولية والتي تتخذ شكلا بعيدا عن الطابع الإقليمي – مع الإشارة إلى إمكانية وقوعها داخل إقليم دولة ما، أو بين عدة دول في نفس الوقت – فتجعل العالم بذلك قرية صغيرة.[3]

5/ من حيث مراحل ارتكابها: تمر هذه الجرائم المستحدثة كغيرها من الجرائم بذات المراحل التي تمر بها أية جريمة من مرحلة التفكير والتخطيط والتحضير فالتنفيذ.

6/ من حيث اجراءات الملاحقة و الكشف عن مرتكبيها:يتطلب الكشف والاهتداء إلى مرتكبي هذه الجرائم وملاحقتهم قضائيا استراتجيات تحقيق وتدريب ومهارات خاصة تسمح بتفهم ومواجهة التقنيات والأساليب المستخدمة في هذا النوع من الجرائم، فكثيرا ما تخفق وتفشل أجهزة الشرطة في ملاحقة وضبط مرتكبيها. كما تتطلب هذه الجرائم ضرورة وجود تعاون دولي لمكافحتها والحد منها.[4]

7/ من حيث الغرض المرتكبة من أجله: تهدف كل جريمة من هذه الجرائم إلى تحقيق أرباح مادية طائلة، في الوقت الذي تسبب فيه أضرارا وخسائر مادية ومعنوية ضخمة وهائلة.

ثانيا:أوجه الاختلاف بين جرائم الانترنت وغيرها من الجرائم المستحدثة المشابهة لها .

سبق التأكيد على أن طريق المعلومات فائق السرعة (الانترنت) يتميز بجملة من الخصائص من أبرزها ارتباطه بالحاسوب، إذ يعتبر هذا الأخير النافذة أو البوابة التي يطل بها على العالم الخارجي. الأمر الذي

---

[1]– ينظر ص45 و ما بعدها من هذه الرسالة .

[2]– ينظر د/ هشام محمد فريد رستم،(الجوانب الإجرائية.....) مرجع سابق، ص 29.

[3]– ينظر ص39 من هذه الرسالة .

[4]– ينظر د/ محمد الأمين البشري، (التحقيق في الجرائم المستحدثة) مرجع سابق، ص104 و ما بعدها.

أدى بالفقهاء إلى اعتبار أن جرائم الانترنت هي ذاتها جرائم الحاسب الآلي، أو بالأحرى هي ذاتها الجريمة المعلوماتية، ولكنها في حقيقة الأمر ما هي إل نوع منها.

هذا من جهة ومن جهة أخرى، أدت خاصية عبورها وعدم اعترافها بالحدود الجغرافية المرسومة في العالم المادي، إلى اشتراكها وتشابهها مع الجرائم المستحدثة المذكورة أعلاه. و السؤال المطروح هنا: هل تختلف جرائم الانترنت عن جرائم المعلوماتية (جرائم الحاسب الآلي)؟ أم هي جرائم واحدة تختلف فقط في التسمية؟ وما هي نقاط الاختلاف بين جرائم الانترنت والجرائم المستحدثة المشابهة لها ؟.

1/ أوجه الاختلاف بين جرائم الانترنت وجرائم الحاسب الآلي (الجرائم المعلوماتية).

باستقرائنا للتعريفين السابقين لكلا الجريمتين تتضح لنا الفروقات التالية:

أ- من حيث استخدام شبكة الانترنت: لا يشترط لقيام جرائم الحاسب الآلي (سواء أكان ذلك الجهاز يستعمل كوسيلة أو ضحية) وجود شبكة الانترنت، إذ قد تتم تلك الأخيرة دون الحاجة إلى الربط بالشبكة الأم مثل: توظيف الحاسبات وملحقاتها في جرائم التزوير و التزييف أو سرقة المعلومات وتدميرها.

على عكس جرائم الانترنت التي تتم عن طريق جهازين كمبيوتر أو أكثر متصلين فيما بينهم عبر الانترنت. أو بصيغة أخرى يعتبر وجود جهاز كمبيوتر في هذه الجرائم شرطا أساسيا لإتمام أركانها، فبدون وصل ذلك الجهاز بشبكة الانترنت لا تقوم تلك الأخيرة[1].

ب- من حيث التطور التاريخي: إذ يرجع الفقه الجنائي ظهور جرائم الحاسب الآلي إلى الستينات، باعتبار أن استخدام الكمبيوتر شاع في تلك الحقبة.[2]

على عكس جرائم الانترنت التي يرجعها إلى العام الذي أفاق فيه العالم على دودة موريس أي عام 1988[3]، والتي كانت السيد في تعديل التشريع الفدرالي الأمريكي.

ج- من حيث تسمية المجرم: يسمى المجرم الذي يرتكب جرائم الانترنت " بالمجرم المعلوماتي" أو" المجرم التقني" أو" الهاكر"، الذي يتخذ الشكل الخبيث له في مصطلح" كراكر" (cracker). ولكن لتمييزه عن المجرم المعلوماتي الذي يرتكب الجرائم المعلوماتية، فيستحسن تسميته "بالهاكر" أو" المخترق "الذي يرتبط نشاطه بظاهرة الاختراق Intrusion وهو يتمتع بالهكترة أو المهارات الخاصة على عكس القرصان [4] (مجرم المعلوماتي في الجرائم المعلوماتية) المشهور بارتكاب جرائم العدوان على حقوق الملكية الأدبية

---

[1]- أي أن أنشطة الإنترنت تتطلب أجهزة كمبيوتر تقارف بواسطتها، و هي تستهدف أيضا معلومات مخزنة أو معالجة ضمن أجهزة كمبيوتر أيضا هي الخوادم التي تستضيف مواقع الإنترنت و تديرها. لمزيد من التفاصيل ينظر د/ سليمان أحمد الفضل، المرجع السابق، ص30؛ يونس عرب، المرجع السابق، ص75، http:// www.arablaw.org

[2]- لمزيد من التفاصيل ينظر د/ عبد الفتاح مراد،المرجع السابق، ص 38.

[3]- لمزيد من التفاصيل ينظر أمير فرج يوسف،المرجع السابق، ص 99.

[4]- د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 235.

والفكرية عامة. وجرائم استخدام التقنية الحديثة للسيطرة على تشغيل الحاسوب، خاصة اختراق كلمات العبور بملفات مشفرة مخزنة في الحاسوب، أي يرتبط نشاطه بظاهرة القرصنة[1].

هذا من جهة ومن جهة أخرى، يختلف الهاكر (مجرم الانترنت) عن القرصان (مجرم الحاسب الآلي)، في كونه لا يتمتع بمدارك علمية أو تخصصية ذات طابع أكاديمي. وإنما هو يملك التحكم في تقنية الانترنت دون الحاجة لأن يكون دارسا لها، ويعتبر مرتكبيها من الأحداث أحسن وأفضل مثال أو دليل على ذلك[2].

د- من حيث القانون المنظم: الانترنت يحكمها قانون يسمى "بقانون الانترنت"، وفي المقابل يحكم الحاسوب "قانون الحاسوب"[3].

هـ- من حيث مسرح الجريمة: يختلف مسرح جرائم الحاسب الآلي عن ذلك في جرائم الانترنت، فقد يكون مسرحها مثل مسرح الجرائم الأخرى التقليدية، خاصة عند ما يكون الهدف منها التخريب أو إتلاف البرامج أو تزوير المستندات و الوثائق أو تفجير المباني و المنشآت[4]. أما مسرح جرائم الانترنت فهو مسرح غير موجود ويتمثل في الفضاء الإلكتروني بأثره.[5]

و- من حيث الأدلة: يمكن إثبات جريمة الحاسب الآلي بالأدلة المعروفة في القانون الجنائي، وقد تكون أدلتها مادية ملموسة ومرئية مثل: الورق، جهاز الحاسب الآلي وملحقاته، الأقراص المدمجة، الشرائط الممغنطة...الخ. على عكس جرائم الانترنت التي يصعب أثباتها والتي تعرف أدلتها بالكامل بغير المرئية وغير المادية والغير الملموسة فهي عبارة عن نبضات إلكترونية تنساب عبر أجهزة الحواسيب وشبكة الشبكات. فكما سبق ذكره، فان هذه الجرائم تستهدف معنويات وليست ماديات محسوسة. على عكس جرائم الحاسب الآلي التي قد تستهدف ماديات محسوسة وقد تستهدف معنويات في الوقت نفسه.[6]

ي- من حيث موضوع الجريمتين: قد ترتكب جرائم الحاسب الآلي على الحاسب الإلكتروني نفسه سواء على مكوناته المادية أو المعلوماتية أو غير المادية وقد يستخدم الحاسب ذاته كأداة لارتكاب إحدى هذه الجرائم. وبالتالي يلزم أن نفرق هنا بين ثلاث حالات:

---

[1]- لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، نفس المرجع ، ص 236.

Mohamed N.SALAM, op.cit, p 20 et suite.

[2]- لمزيد من التفاصيل ينظر د/ محمد عبد الله المنشاوي: جرائم الإنترنت في المجتمع السعودي،

www.minshawi.comhttp://

[3]- لمزيد من التفاصيل ينظر يونس عرب: قانون الكمبيوتر، النظرية و المشتملات، منشورات اتحاد المصارف العربية، 2001، ص 20 و ما بعدها.

[4]- د/ عبد الفتاح مراد، المرجع السابق، ص62.

[5]- ينظر ص58 من هذه الرسالة .

[6]- د/هشام محمد فريد رستم، (الجوانب الاجرائية للجرائم ...) مرجع سابق،ص 29

الحالة الأولى: وتتمثل في وقوع الجريمة عل المكونات المادية للحاسوب.

وتتحقق هذه الحالة إذا كانت أجهزة الحاسب الآلي من معدات وكابلات وشبكات ربط وآلات طباعة وشرائط خام من التي يسجل عليها البرامج و المعطيات هي محلا أو موضوعا لهذه الجرائم و بالتالي لا تثير هذه الحالة مشكلة، باعتبار أن هذه المكونات المادية محل الإعتداء تتمتع بالحماية الجنائية للنصوص التقليدية باعتبارها من الأموال المنقولة التي تخضع سرقتها وإتلافها للنصوص الجنائية التقليدية. وبالتالي فإن الأمر هنا لا يثير أي مشكلة حيال تطبيق النصوص التقليدية على هذه الأموال.[1]

الحالة الثانية: وقوع الجريمة على المكونات المعلوماتية أو الغير مادية للحاسوب.

وتتحقق هذه الحالة عندما تكون مكونات الحاسوب المعلوماتية محلا أو موضوعا للجريمة، كتدمير برامجه وسرقتها وتقليدها أو العبث ببياناته أو بالمعلومات المخزنة في ذاكرته. ويثور الإشكال هنا حول طبيعة المعطيات الواقع عليها الإعتداء. باعتبارها ليست من طبيعة مادية منقولة ملموسة ومدى ملائمة النصوص العقابية التقليدية في الانطباق عليها فالإعتداء هنا يطال المال المعلوماتي الذي يتطلب معالجة قانونية ذات طبيعة خاصة.[2]

الحالة الثالثة: عندما يتم ارتكاب الجريمة بواسطة الحاسب الآلي:

وهنا يستخدم هذا الجهاز كوسيلة أو كأداة لإحداث الإعتداء، كاستخدام الحاسب الآلي للإطلاع على الحياة الخاصة أو الاستيلاء على الأموال. وفي هذه الحالة يثور الإشكال حول وجوب وضع قوانين عقابية تتلاءم مع نوعية هذه الجرائم غير تلك التقليدية.[3]

على عكس جرائم الانترنت التي قد تكون فيها شبكة الانترنت وسيلة لارتكاب الإعتداء،أو محلا لذلك الإعتداء.

ر- من حيث طبيعة الفيروس: يختلف فيروس الانترنت كجريمة تقنية عن فيروس الحاسب الآلي فيما يلي:

- من حيث النشأة التاريخية: اذ برز فيروس الحاسب الآلي لأول مرة سنة 1974 في شركة xerox[4] على عكس فيروس الانترنت الذي شهد ميلاده سنة 1988.

- من حيث الأثر: يتميز فيروس الانترنت بأنه سريع الانتشار سرعة البرق، طالما أن الشبكة تعمل وحتى لو أغلق أحد الحواسيب أو الشبكات أو الخوادم. أضف إلى ذلك أن مهامه تتجاوز عملية التخريب إلى عملية الاختلاس المعلوماتي. ومثال ذلك ما كشف عنه التطور الفيروسي عن وجود دودة يطلق عليها اسم badtrans.13312amm و التي تلعب دور المختلس المعلوماتي الذي يختلس النظام المعلوماتي وما يحويه من معلومات مخزنة.[5]

---

[1]- محمود أحمد عبابنة، المرجع السابق،ص 38

[2]- محمود أحمد عبابنة، نفس المرجع ، ص 39

[3]- محمود أحمد عبابنة، نفس المرجع ،ص 38.

[4]- لمزيد من التفاصيل ينظر د/ عبد الفتاح مراد،المرجع السابق، الموضع السابق.

[5]- لمزيد من التفاصيل ينظر مقال فيروسات الكمبيوتر و الإنترنت، http:// kenanaonline.com.

و تجدر الإشارة إلى أن انتشاره السريع لا يلزمه تدخل إنسان بينما نجد أن فيروس الحاسب الآلي يملك القدرة على الاختراق و يتسبب في تغيير خصائص الحاسب الآلي و البرامج التي عليه، ويتوالد ويتكاثر عادة بنسخ نفسه ملايين المرات. وهو يكمن في الحاسوب المصاب به ويتكاثر ولا ينتقل إلى حواسيب أخرى إلا عند انتقال ملف أو برمجية من الحاسوب المصاب إلى الحاسوب غير المصاب. ضف إلى ذلك فإن هذا الفيروس يلزمه للانتشار تدخل إنساني.[1]

وخلاصة قولنا أن هناك فروق جمة بين الجريمة المعلوماتية (جرائم الحاسب الآلي) وجرائم الانترنت، كما توجد هناك نقاط تشابه بينهما. ولكن استخدام مصطلح الجريمة المعلوماتية للدلالة على جرائم الانترنت هو استخدام ناقص، لأنه يعبر عن نوعية محددة من جرائم الانترنت، وهي تحديدا الاستيلاء على المعلومات عبر الانترنت، كما هو الشأن في جرائم التجسس الاقتصادي عبر الانترنت في التشريع الأمريكي.[2]

2/ أوجه الاختلاف بين جرائم الانترنت و الجريمة المنظمة:

تشترك الجريمة المنظمة مع جرائم الانترنت في نقاط عدة ومعينة أهمها: أنهما جريمتين عابرتين للحدود الجغرافية،و أن المجرم في كلتيهما يتمتع بسمات المجرم ذو الياقات البيضاء. ولكنهما في المقابل تختلفان عن بعضهما في نقاط أخرى نذكرها كما يلي:

أ- **من حيث الطبيعة القانونية:** الجريمة المنظمة ما هي إلا جرائم ومخالفات عادية تنص عليها معظم القوانين العقابية، وتضع لها عقاب. كما أن مصطلح الجريمة المنظمة هو مصطلح عام وليس مصطلح قانوني وهو يفيد معنى التنظيم سواء من حيث العدد أو أساليب إدارة المنظمة الإجرامية وطرق تجنيد أفرادها وتدريبهم وإدارة إمكانات المنظمة بمختلف شؤونها المالية و الفنية و القانونية. [3]

بينما جرائم الانترنت هي من جرائم التقنية العالية، والتي يعتبر الحاسب الآلي والانترنت أدواتها أو محلا لها. والتي تعجز القوانين العقابية التقليدية عن مواجهتها والكف عنها عن طريق وضع نصوص قانونية تحكمها وتتواءم مع طبيعتها الخاصة.[4]

هذا من جهة ومن جهة أخرى، فالجريمة المنظمة قد يستخدم فيها وسائل تقليدية كالأسلحة النارية (الجريمة المنظمة العادية)،كما قد تستخدم فيها وسائل الاتصالات والتقنية الحديثة (الجريمة المنظمة المستحدثة).

بينما جرائم الانترنت فوسيلتها شبكة الشبكات فقط.[5]

---

[1]- حوار د/ فايز عبد الله الشهري مع هداية نت،http:// www.hedayah.net

[2]- د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 221.

[3]- محمد الأمين البشري، المرجع السابق، ص 36.

[4] - د/محمد صالح العادلي،البحث السابق،http:// dreladly.com

[5]- د/ عبد الفتاح الصيفي، د/ مصطفى عبد المجيد كاره، د/ أحمد محمد النكلاوي: الجريمة المنظمة، التعريف و الانماط ولاتجاهات،أكاديمية نايف العربية للعلوم الامنية،الرياض، 1999، ص18- 19.

ب- من حيث طريقة تنفيذها: تتسم الجريمة المنظمة بالعنف و الاستعداد لاستعمال العنف والقوة لارتكابها عند اللزوم، على عكس جرائم الانترنت التي هي جرائم مغرية تعتمد على الذكاء في ارتكابها.[1]

وتجدر الإشارة إلى أن أساليب تمويل الجريمة المنظمة هي: السرقة وتجارة المخدرات والأسلحة وغسل الأموال...الخ.[2]

ج- من حيث مدة ارتكابها: تأخذ الجريمة المنظمة شكلا نظاميا ومستمرا على سبيل الاختراق، إذ يعتبر ذلك شرطا فيها وإحدى لوازمها وهي لا تقوم بصفة مؤقتة.[3]

على عكس جرائم الانترنت التي لا يشترط فيها ضرورة الاستمرارية،أي يمكنها أن ترتكب بصفة مؤقتة وذلك عندما لا يستغرق وقوعها غير برهة يسيرة أو وقتا محدودا حتى تتم الجريمة،وهذا ما ينطبق على جريمة السب أو القذف عبر الانترنت، فهذه الجريمة وقتية [4] (مؤقتة) تحدث وتنتهي بمجرد قيام واقعة السب أو القذف.

وفي المقابل، يمكن أن ترتكب تلك الجريمة بصفة مستمرة وذلك عندما يستغرق ارتكاب ركنها المادي وقتا طويلا من الزمن، كما حدث في حالة الاختراق الذي تعرض له نظام المعالجة الآلية للمعلومات لشركة مايكروسوفت عام 2000، حيث مكث مجهول في ذلك النظام مدة أسبوعين.[5]

فهنا الجريمة مستمرةطوال المدة التي تم فيها المكوث في ذلك النظام[6].

MITONGO KALONI Tresor-Ghautier : Notion de cybercriminalite، Praxis d'une penalisation delinquance electronique en droit penal Congolais, Université de Lubumbashi, 2010 , p 17, http:// www.leganet.cd.

[1]- لمزيد من التفاصيل ينظر د/ أحمد فاروق زاهر: الجريمة المنظمة، ماهيتها،خصائصها و أركانها، بحث مقدم إلى الحلقة العلمية جرائم الاحتيال و الاجرام المنظم،جامعة نايف العربية للعلوم الامنية، الرياض، 2008، ص39.

[2]- لمزيد من التفاصيل ينظر د/ دياب البدانية: مواجهة الجريمة المنظمة العابرة للحدود الوطنية، من المحلية إلى الكونية، جامعة مؤتة، الاردن، ص8.، http://www.mutah.edu.jo

[3]- لمزيد من التفاصيل ينظر د/ دياب البدانية، نفس المرجع، ص11.

[4]-يقصد بالجريمة الوقتية:الجريمة التي يقبل ركنها المادي في طبيعته أن يتحقق في لحظة زمنية محددة على حال ينتهي تحقق الركن المادي بانتهائها.د/ محمد زكي أبو عامر، المرجع السابق،ص 361.عبد الله سليمان، المرجع السابق، ص 346،د/ عبد الفتاح الصيفي، المرجع السابق، ص 188.

[5]- د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 335.

[6]- يقصد بالجريمة المستمرة:الجريمة التي يقبل ركنها المادي بطبيعته استمرار في الزمان طالما شاء له الجاني أن يستمر. د/ محمد زكي أبو عامر، المرجع السابق،الموضع السابق.عبد الله سليمان، المرجع السابق، الموضع السابق،د/ عبد الفتاح الصيفي، المرجع السابق، الموضع السابق.

د- من حيث التطور التاريخي:

عرفت الجريمة المنظمة منذ أقدم العصور، فظهرت في البداية كظاهرة اجتماعية مثلت في شكل عمل وطني أو إنساني يهدف لنصرة الضعفاء ومساعدة الفقراء[1]. إلا أن هذه الظاهرة قد تطورت في العصر الحديث كعمل إجرامي منظم يستهدف عائدات مالية وسيطرة اقتصادية وسياسية في كثير من دول العالم.[2]

في حين نجد أن جرائم الانترنت هي نتيجة للتطور التكنولوجي الذي أصاب العالم في القرن الحادي والعشرين،أي هي مولود للثورة المعلوماتية الذي أفرزته للوجود سنة 1988 من خلال دودة موريس.[3]

هـ- من حيث الدوافع و الاثر المترتب عنها: تتميز الجريمة المنظمة بصفتها التجارية وعائداتها المالية غير المشروعة، وهي تعيق مسيرة التنمية الاقتصادية وتهدف دائما إلى الربح المادي.[4] على عكس جرائم الانترنت التي تهدد جميع المجالات و المصالح وتتنوع أهدافها ودوافعها من ارتكابها ولعا في جمع المعلومات وتعلمها أو الاستيلاء عليها أو رغبة في قهر النظام و التفوق على تعقيد الوسائل التقنية أو الأضرار بالأشخاص أو سعيا وراء الربح المادي أو تهديدا للأمن القومي والعسكري.[5]

و- من حيث الصفات التي يتمتع بها المجرم: فمجرم الانترنت هو مجرم يتمتع بصفات خاصة ويملك مهارات خارقة تدل على كفاءته وصلاحيته وأهليته التقنية، وقد يرتكب هذا المجرم جرائم الانترنت لوحده، كما يمكن أن يشترك مع غيره في ارتكابها ويسمى حينئذ بمجرم المعلوماتي، على عكس الجريمة المنظمة، فيشترط أن تضم الآلاف من المجرمين الذين يعملون خارج إطار القانون وفقا لنظام بالغ التعقيد والدقة يفوق ذلك الذي تتبعها أكثر المؤسسات تطورا وتقدما ويسمى "المجرم هنا المجرم المنظم"[6].

وتجدر الإشارة إلى أن أفراد هذا التنظيم يخضعون لأحكام قانونية شرعوها لأنفسهم، تفرض أحكاما بالغة

---

[1]-بحيث تقوم مجموعة من الرجال الخارجين على القانون بارتكاب جرائم السرقات و النهب و جمع عائداتها بهدف توزيعها على الأسر الضعيفة. كما أنهم كانوا يخدمون الضعفاء المظلومين عن طريق انتزاع حقوقهم من أيادي الأقوياء و إعادتها لهم. د/محمد الأمين البشري، المرجع السابق، ص 38.

[2]-لمزيد من التفاصيل ينظر د/محمد الأمين البشري، نفس المرجع ، نفس الموضع.

[3]- ينظر التطور التاريخي لجرائم الإنترنت ص35 من هذه الرسالة.

[4]- Carlo MORSELLI,Thomas GABOR,jhon KIEDROWSKI,M.A : Les facteurs qui façonnent le crime organisé,Rapport n° 00 7 préparé pour la Division de la recherche et de la coordination nationale sur le crime organisé Secteur de la police et de l'application de la loi Sécurité publique Canada , Canada, 2010,p 37, http://publications.gc.ca.

[5]- ينظر ص30 من هذه الرسالة .

[6] -Margaret BEARE : Les femmes et le crime organisé,Rapport n° 013 préparé à l'intention de la division de la recherche et de la coordination nationale sur le crime organisé Secteur de la police et de l'application de la loi Sécurité publique Canada ,Canada,2010,p 6, http://publications.gc.ca.

القسوة على من يتمرد عليها ويخرج على قاموس الجماعة.[1]

ي- من حيث طبيعة ضحاياها: ضحايا الجريمة المنظمة يكونون من دول مختلفة[2]، على عكس ضحايا جرائم الانترنت التي يمكن أن يكونوا من نفس الدولة في حالة ارتكاب تلك الجرائم داخل دولة واحدة (جريمة داخلية) أو من دول مختلفة (في حالة ما تكون عابرة للحدود)[3].

3/ أوجه الاختلاف بين جرائم الانترنت وجرائم التقنية ، و بينها و بين جرائم الاتصال عن بعد:

تختلف كل من هذه الجرائم في وسائل ارتكابها، ففي جرائم الاتصال عن بعد يكون الاحتيال باستخدام الهاتف أو أجهزة الموجات الدقيقة أو أجهزة البث أو أي أنظمة اتصال عن بعد.

أما في جرائم التقنية، فتستخدم فيها التقنية والتي هي غير مقصورة على الانترنت، بل كل وسائل التقنية مثل استخدام تقنية الهاتف النقال لارتكاب جريمة القذف والسب.

في حين نجد أن جرائم الانترنت وسيلتها في ارتكاب الجرائم هي شبكة الشبكات أي الانترنت لا غير. وجرائم الانترنت نوعان، الأول حين تكون شبكة الانترنت هدف الجريمة و غايتها، و يسمى هذا النوع ب **الاجرام المعلوماتي على الانترنت** ". أما النوع الثاني فيقع الإعتداء فيه باستخدام الانترنت كأداة لارتكاب الجريمة. و يسمى هذا النوع ب "**الاجرام غير المعلوماتي على شبكة الانترنت**". و الذي سنقتصر على دراسته في هذه الرسالة دون التطرق الى نظيره.

---

[1]- لمزيد من التفاصيل ينظر كلا من: د/ دياب البدانية، المرجع السابق، ص8.

- Carlo MORSELLI,Thomas GABOR, Jhon KIEDROWSKI,M.A, op.cit,p 21.

[2] - Voir Carlo MORSELLI, Thomas GABOR,Jhon KIEDROWSKI,M.A, ibid,p 30.

[3]- ينظر ص39 من هذه الرسالة .

خلاصة الفصل التمهيدي

نستخلص من هذا الفصل التمهيدي ما يلي:

– تعدد و تنوع و تباين التعريفات الفقهية حول جرائم الانترنت، وفقا للمعيار المستند إليه فيها، فمنها من تناولت الجانب الموضوعي لها، و منها من ركزت على الوسيلة، وغيرها عرفتها وفقا لصفات الجاني.....الأمر الذي نتج عنه صعوبة الاتفاق على تعريف فقهي جامع شامل مانع لها.

في مقابل غيابه التام بالنسبة للتشريع، إذ أنه و بالرغم من وجود بعض القوانين والنصوص الخاصة في بعض الدول كالقانون رقم 04/09 الموجود في الجزائر المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إلا أنها لم تعرف جريمة الانترنت بالتحديد. بل تضمنت تعريفات واسعة تضم الجريمة المعلوماتية أو الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. و يرجع السبب في ذلك إلى أن التقدم العلمي والتقني في مجال الاتصالات وتكنولوجيا المعلومات و في شبكة الانترنت أفرز أنماطا مستحدثة من الجرائم الجديدة و الفريدة من نوعها ذات الطبيعة المعقدة من حيث طرق ارتكابها ووسائل كشفها وذات الطابع الدولي التي لم يسبق للبشرية معرفتها.

و يمكن تعريف لهذا جرائم الانترنت بأنها كل سلوك إرادي غير مشروع، صادر عن شخص مسئول جنائيا ذا دراية فائقة بمجال الحوسبة، معاقب عليه قانونا بجزاء جنائي تكون شبكة الانترنت محلا له أو وسيلة لارتكابه. و هي تصنف ضمن جرائم التقنية العالية و التي ترتكب غالبا في صورة سلوك إيجابي.

– يعتبر مصطلح سيبار كرايم (Cyber crime) أفضل وأصوب مصطلح للتعبير عن جرائم الانترنت.

– جرائم الانترنت هي جرائم وطنية ودولية وذات بعد دولي في الوقت ذاته.

– تتميز جرائم الانترنت بجملة من الخصائص المميزة لها ككونها جرائم عابرة للحدود و صعبة الاكتشاف و أن محلها ووسيلتها شبكة الانترنت و أداة ارتكابها الحاسب الآلي و أن مرتكبها شخص ذو خبرة فائقة بمجال الحوسبة يسمى المجرم التقني.

– تحصر فئات الجناة في جرائم الإنترنت في ثلاث طوائف و هي المخترقون أو المتطفلون و المحترفون و الحاقدون.

– مجرم الإنترنت هو مجرم إجتماعي غير عنيف متخصص يعتمد في إجرامه على قوة الذكاء و لا يحتاج إلى أدنى مجهود عضلي.

– تختلف جرائم الانترنت عن الجرائم التقليدية في نقاط جمة و منها أن الأدلة فيها غير مرئية وغير مادية و غير ملموسة يمكن تدميرها وإخفاء معالم الجريمة فيها في ثوان معدودة لكون أن مسرح الجريمة فيها غير موجود لأنه عبارة عن العالم الإفتراضي و أن مرتكبها يعتمد على قوته الذهنية أكثر من قوته الجسدية....

و ذات الشأن بالنسبة للجرائم المستحدثة المشابهة لجرائم الانترنت كالجريمة المنظمة و الجريمة المعلوماتية وجريمة الاتصال عن بعد و الجريمة التقنية فهي تختلف عنها في أنه ليست كل جريمة انترنت هي جريمة معلوماتية، بل نوع منها فقط. أما بالنسبة لجرائم الإتصال عن بعد و جرائم التقنية فتختلف عنها في وسيلة

ارتكابها، و التي تكون في جرائم الاتصال عن بعد عن طريق استخدام الهاتف أو أجهزة الموجات الدقيقة أو أجهزة البث أو أي أنظمة اتصال عن بعد.و في جرائم التقنية، فعن طريق استخدام التقنية و منها الانترنت. أما فيما يخص الجريمة المنظمة فهي تختلف عنها في كونها جريمة عادية و مستمرة يغلب عليها طابع العنف، يرتكبها أفراد خاضعون لأحكام قانونية شرعوها لأنفسهم،و غايتها الوحيدة هي الربح المادي.

الباب الأول:

جرائم الإعتداء على الأشخاص عبر الانترنت

يقصد بجرائم الإعتداء على الأشخاص بصفة عامة:"تلك الجرائم التي تنال بالإعتداء أو التهديد بالخطر حقوقا ذات طابع شخصي بحت، أي تلك الحقوق اللصيقة بشخص المجني عليه و التي تعبر عن المقومات الأساسية لشخصيته. و هي تخرج عن دائرة التعامل الاقتصادي؛ و أهمها الحق في الحياة و في سلامة الجسم، و الحق في الحرية و في صيانة العرض و الحق في الشرف و الإعتبار"[1]. أو هي:"مجموعة من الجرائم التي تقع اعتداء على جوانب الشخصية الإنسانية، و من ثم فهي تستهدف إما المساس بشخصية الإنسان الطبيعية أو العضوية، فتمس بذلك حقه في الحياة أو سلامته البدنية أو عرضه أو حريته، وإما تستهدف المساس بشخصية الإنسان المعنوية، أي بقيمته المعنوية أو الإعتبارية كجرائم الشرف و الإعتبار"[2].

وتعد هذه الأخيرة من الجرائم التقليدية الأكثر وقوعا وانتشارا في مجتمعاتنا، و التي تصدت لها و تناولتها مختلف التشريعات العقابية.

ولكن ونظرا لما عرفه عالمنا من ثورة رقمية، أثرت بالسلب عليه بإفرازها لجرائم مستحدثة و فريدة من نوعها، تختلف عن نظيرتها التقليديةلاسيما في وسيلة أو محل ارتكابها. إذ أتاحت للمجرم المعلوماتي أو ما يعرف بالهاكرز إمكانيه تسخير العالم الإفتراضي لتحقيق رغباته في ارتكاب أغلب الجرائم، وخاصة تلك الواقعة على الأشخاص من جنح بسيطة إلى جنايات كبرى (سواء أكان فاعلا أصليا أم فاعلا معنويا)[3]. وبأبسط الأساليب من خلال التلاعب ببرمجية البيانات عن بعد و بضغطة زر واحدة و هو جالس في مكانه دون الحاجة إلى مبارحته.

و يمكن تصنيف جرائم الإعتداء على الأشخاص عبر الانترنت إلى جرائم البث العلني و جرائم الإعتداء على حرمة الحياة الخاصة و جرائم المطاردة و الجرائم الأخلاقية.

و سيتم التطرق إلى كل نوع من هذه الجرائم في الفصول التالية:

الفصل الأول: جرائم البث العلني عبر الإنترنت.

الفصل الثاني: جرائم الإعتداء على حرمة الحياة الخاصة و جريمة المطاردة عبر الانترنت

الفصل الثالث: الجرائم الأخلاقية عبر الانترنت

---

[1]– جرائم الإعتداء على الأشخاص ،http:// www.alayam.com

[2]– القانون الجنائي، جرائم الإعتداء على الأشخاص و على الأموال ، http://ta3lam.mortadarabi.com

[3]– يكون الجاني فاعلا معنويا في مثل هذه الجرائم إذا قام شخص مثلا بإرسال بريد إليكتروني لطفل صغير يطلب منه أن يقوم بتسليم مادة سامة لأخر مدعيا أنها دواء للعلاج، فيموت من جراء تناولها الشخص.

الفصل الأول:

جرائم البث العلني عبر الإنترنت

يعد البث العلني أحد الخصائص التي تتميز بها تقنية الانترنت،فهي فضلا عن كونها وسيلة حية وحيوية للبث، فهي تعتبر كذلك مظهرا للبث السمعي المرئي، لاحتوائها قوة وسائل وأدوات البث التقليدية (المقروءة، المسموعة، المرئية). ولكن ذلك الأخير (البث العلني) لم يرحمه أصحاب النفوس المريضة، فقد وجدوا من خلاله متنفسا لأحقادهم ومرتعا لشهواتهم، واستعملوه في نشر الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعب سواء كانت تلك الرموز فكرية أو سياسية أو دينية وأيضا في قذف وسب وتشويه سمعة تلك الرموز بهدف تشكيك الناس في مدى مصداقية هؤلاء الأفراد ومحاولة فض الناس من حولهم ليخلو لهم الجو في محاولة منهم لتسميم أفكار الناس.

وتتخذ جرائم البث العلني مظاهر عدة يمكن حصرها في:الجرائم الماسة بسمعة الشخص وشرفه واعتباره وجرائم النشر الإليكتروني، وجرائم العنف و القتل عبر الانترنت.

و عليه ارتأينا تقسيم هذا الفصل الى المبحثين التاليين:

المبحث الأول: الجرائم الماسة الشرف و الاعتبار عبر الإنترنت.

المبحث الثاني: جرائم الصحافة الإليكترونية وجرائم العنف عبر الانترنت.

المبحث الأول:

الجرائم الماسة بالشرف و الاعتبار عبر الإنترنت.

يقصد بالشرف:" قيمة الإنسان وحياته الاجتماعية التي تتكون من سلوكه والتي تتأثر به".[1] أما الإعتبار:"فهو سمعة الشخص، ويرتبط بالصفات والمركز الذي يحتله ذلك الأخير في مجتمعه، ويتصل بصلاحيته لأداء دوره، كما يحدد واجباته نحو غيره وعلاقاته والتزاماته الوظيفية و المهنية."[2]

فهما يمثلان (الشرف والإعتبار) حصيلة مجموع تصرفات الفرد، فبهما تتكون سمعته وتتحدد مكانته واعتباره في المجتمع.[3]

وتعد جرائم القذف والسب والتشهير من أبرز الجرائم التقليدية الماسة بسمعة الشخص وشرفه واعتباره، إذ تؤثر سلبا على شخص الإنسان خاصة بعد ظهور شبكة الانترنت، التي أصبحت وسيلة تستخدم للنيل من

---

[1]– ينظر محمد محمد حسن: جريمة القذف، دراسة مقارنة بين قانون الجنائي الوضعي والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، 1996،ص21.

[2] – ينظر محمد محمد حسن، نفس المرجع، نفس الموضع.

[3]– تجدر الإشارة إلى أن المكانة التي يتمتع بها الشخص في المجتمع تتكون من مجموعة الصفات المدونة والمكتسبة. وهي تتحدد طبقا لضابط موضوعي يتمثل في الرأي السائد لدى الوسط الاجتماعي الذي يعيش فيه هذا الأخير. القانون الجنائي، بحث سابق، http:// ta3lam.mortadarabi.com

شرف الغير أو كرامته أو اعتباره، أو تعرضه إلى بغض الناس واحتقارهم، بما يتم إسناده للمجني عليه على شكل رسالة بيانات.[1]

ولقد ارتأينا لدراسة هذه الجرائم تقسيم هذا المبحث إلى مطلبين، نتطرق في أولهما إلى الأحكام العامة التي تحكم هذه الجرائم، ثم نعرض في ثانيهما إلى تبيان الكيفية التي ترتكب بها هذه الجرائم التقليدية عبر الإنترنت. و ذلك على النحو التالي:

المطلب الأول: الأحكام العامة للجرائم الماسة بالشرف و الاعتبار.

المطلب الثاني: جرائم القذف و السب والتشهير عبر الإنترنت.

المطلب الأول:

الأحكام العامة للجرائم الماسة بالشرف و الاعتبار.

نتناول في هذا المطلب التعريف بهذه الجرائم الماسة بسمعة و شرف و اعتبار الشخص و المتمثلة في القذف و السب و التشهير، ثم نتطرق لتبيان أركانها العامة و الخاصة. وسيكون ذلك من خلال الفرعين التاليين:

الفرع الأول: تعريف القذف و السب و التشهير.

الفرع الثاني: أركان جريمة القذف و السب.

الفرع الأول:تعريف القذف والسب و التشهير.

نتطرق في هذا الفرع إلى تعريف القذف أولا ثم السب ثانيا ثم التشهير ثالثا. و ذلك كمايلي:

أولا: تعريف القذف:

1/ لغة:" الرمي، ويقال قذف الشخص أي رماه بقوة على دفعات". والقذف بالقول: "هو التكلم من غير تدبر". وقذف المحصن: "هو اتهامه بالزنا."[2]

2/ اصطلاحا فهو "الرمي بالزنا أو الرمي باللواط".[3]

---

[1] – رسالة بيانات: "تعني معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك وعلى سبيل المثال لا الحصر والتبادل الالكتروني للبيانات أو البريد الالكتروني أو البرق أو التلكس أو النسخ البرقي". ينظر المادة (2) من قانون اليونسترال النموذجي بشأن التوقيعات الالكترونية وكذا المتعلقة بالتجارة الالكترونية الدولية لسنة 1996.

[2] – مرشد الطلاب،المرشد الجزائري، قاموس مدرسي عربي، ص36.

[3] – د/ حسين الغافري و محمد الألفي، المرجع السابق، ص100.

و يعرف القذف كذلك بأنه:"إسناد واقعة محددة في مكان عام أو على مسمع أو مرأى من شخص آخر غير الضحية، تستوجب عقاب من تنسب إليه أو تؤذي سمعته"[1]. أي نسبة أمر شائن للمقذوف عمدا بشكل علني يستوجب في حالة صدق ذلك عقابه بالعقوبات المقررة قانونا أو ازدراء الناس و احتقارهم له.

ثانيا:تعريف السب.

1/ لغة هو:"الشتم سواء بإطلاق اللفظ الصريح الدال علنية أو باستعمال المعاريض الذي تؤدي إليه."[2]

2/ اصطلاحا فهو:"خدش شرف شخص واعتباره عمدا بإلصاق صفة عيب أو لفظ جارح أم مشين إليه[3]".

كما يعرف بأنه: "الاسناد العمدي لواقعة غير معينة إلى المجني عليه خادشة لشرفه و اعتباره".[4]

وعلى هذا فالسب هو خدش شرف شخص و اعتباره عمدا دون أن يتضمن ذلك إسناد واقعة معينة، و هذا ما يميزها عن جريمة القذف[5].

ثالثا:تعريف التشهير.

1/ لغة: هو من شهره شهرا وشهرة أي أعلنه وأذاعه. واشتهرت فلانا: استخففت به وفضحته وجعلته شهرة[6].

2/اصطلاحا: فهو "عبارة عن إذاعة السوء عن شخص وجعله معروفا بين الناس[7]". أو هو "إشاعة السوء عن إنسان بقصد الإضرار بسمعته والحط من قدره بذكر عيوبه ومثالبه وصفاته السيئةوالتنقيص منه وذكر أخطائه التي وقع فيها ".[8]

---

[1]– د/ محمود نجيب حسني: الموجز في شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة،1993،ص 517. وقد تصدى القضاء إلى تعريف القذف، و منها القضاء المصري و ذلك في العديد من أحكامه ، ومنها الحكم الذي قضي فيه بأن القذف الذي يستوجب العقاب قانونا هو الذي يتضمن إسناد فعل يعد جريمة يقررها القانون عقوبة جنائية أو يوجب احتقار المسند إليه عند أهل وطنه. الطعن رقم 474 لسنة 55 ق جلسة 1985/3/3، ص 28.

[2]– القاموس الجديد للطلاب، معجم عربي مدرسي ألفبائي، الطبعة السابعة، المؤسسة الوطنية للكتاب، الجزائر،1991، ص449.

[3] – معوض عبد التواب: القذف و السبب و البلاغ الكاذب و إفشاء الأسرار و شهادة الزور، دار المطبوعات الجامعية، الاسكندرية، 1988، ص 143

[4]– د/ فوزية عبد الستار: شرح قانون العقوبات، القسم الخاص، الطبعة الثانية، دار النهضة العربية، القاهرة،2000، ص592. وقد تصدى القضاء إلى تعريف السب، و منها محكمة النقض المصرية و التي عرفته في العديد من أحكامها، ومنها الحكم الذي قضت فيه بأن:"المراد بالسب في أصل اللغة الشتم سواء بإطلاق اللفظ الصريح الدال عليه أو باستعمال المعارض الذي تشير إليه، و هو المعنى الملحوظ في إصطلاح القانون الذي اعتبر السب كل إلصاق تعبير أو تعبير يحط من قدر الشخص عن نفسه أو يخدش سمعته لدى غيره. الطعن رقم 61341 لسنة 59 ق جلسة 1991/1/7.

[5] – حمزة نادي: ما هي الفروق القانونية بين جريمتي السب و القذف؟ ، http://www.almoltaqa.com

[6] – المنجد في اللغة و الإعلام، الطبعة السابعة و العشرون، دار المشرق، بيروت، ص 406.

[7] – مقال منشور على الإنترنت على الموقع: http://www.nooralislam.alafdal.net

[8] – محسن بن محسن بن باعث الرويلي: تجريم الأفعال الإباحية الاليكترونية و العقاب عليها، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض 2010، ص 98.

وتتعدد الأهداف والدوافع من وراء التشهير، فقد يكون لهدف الابتزاز (جنسي أو مالي)، أو الإنتقام كأن تكون عداوة مع الشخص المشهر به، وقد تكون أحيانا من باب الكيد والحسد أو لأي سبب أخر.

الفرع الثاني:أركان جريمة القذف و السب.

و على غرار الفرع السابق، نعرض في هذا الفرع إلى تبيان أركان جريمة القذف و السب. و ذلك كمايلي:

أولا: أركان جريمة القذف.

يتطلب لقيام جريمة القذف توفر ثلاث أركان، ركن شرعي و ركن مادي و ركن معنوي.و سنتناول كل واحد منها بالشرح و التفصيل كما يلي:

1/ الركن الشرعي: والمتمثل في النص الواجب التطبيق والذي يجرم السلوك، أو بالأحرى الذي يضفي عليه الصفة غير المشروعة. ويتمثل في النصوص القانونية التي تناولت جريمة القذف كالمادة 29 من القانون المؤرخ في 1881/07/29 بشأن الصحافة في فرنسا المعدل بالقانون المؤرخ في 1986 و التي عرفت في فقرتها الأولى القذف العلني بأنه:"هو إخبار أو إسناد لفعل يمس شرف و اعتبار الشخص أو الهيئة التي أسند إليها هذا الفعل...."والمادة 1/302 من قانون العقوبات المصري و التي عرفت القذف بأنه: "يعد قاذفا كل من أسند لغيره بواسطة إحدى الطرق المبينة في المادة 171 من هذا القانون أمورا لو كانت صادقة لأوجبت احتقاره عند أهل وطنه".[1] و المادة المادة188 من قانون العقوبات الاردني في فقرتها الأولى والتي عرفت الذم[2] بأنه:"هو اسناد مادة معينة إلى شخص و لو في معرض الشك و الإستفهام، من شأنها أن تنال من شرفه أو كرامته، أو تعرضه إلى بغض الناس و احتقارهم، سواء أكانت تلك المادة جريمة تستلزم العقاب أم لا". و المادة 296 من قانون العقوبات الجزائري و التي عرفت هي الأخرى القذف بأنه:"يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف و اعتبار الأشخاص أو الهيئة المدعى عليها به أو اسنادها اليهم أو إلى تلك الهيئة ..."

2/ الركن المادي: لوقوع جريمة القذف العلني يشترط تحقق ثلاث عناصر:

أ– فعل الإسناد: ويتمثل في إسناد واقعة محددة أو أمر ما إلى شخص معين سواء أكان ذلك الأخير شخصا طبيعيا أو شخصا معنويا، أو كان المقذوف لا يتمتع بالشخصية القانونية.[3] وذلك بأي وسيلة من وسائل التعبير عن المعنى بالقول أو الكتابة أو الإشارة، و يتحقق الإسناد سواء على سبيل القطع أو الشك.

---

[1]– ينظر كذلك المواد 2/302و 303و 304 و 305من ذات القانون و التي تناولت الأحكام الخاصة بالاباحة و العقاب على القذف و الظروف المشددة.

[2] – تجدر الإشارة أن المشرع الأردني يسمي جريمة القذف هنا بجريمة الذم.

[3]– فلقد خص القانون المصري الهيئات العامة بحماية خاصة بنصه في المادة 184عقوبات على جريمة اهانة تلك الهيئات و رصد له عقوبة مشددة عن عقوبة القذف البسيط و هي عقوبة الحبس. أما اذا كان المقذوف لا يتمتع بالشخصية القانونية كأن تكون عبارات القذف موجهة ضد جماعة من الناس كمجلس الأقباط المثلي مثلا، فتعتبر موجهة أيضا إلى أفراد الجماعة.و ذات الشأن بالنسبة لقانون العقوبات الجزائري في المادة 296 في العبارة التالية:"... أو الهيئة المدعي عليها به أو اسنادها اليهم أو إلى تلك الهيئة ..." و المادة 298 و التي تعاقب بالحبس من شهر إلى سنة و الغرامة من 300 إلى 3000 دينار اذا كان القذف موجها إلى شخص أو أكثر ينتمون إلى مجموعة عنصرية أو مذهبية أو إلى دين معين إذا كان الغرض هو التحريض على الكراهية بين المواطنين أو السكان.

و في هذا الصدد ينبغي الإشارة إلى أن هذا الشرط في القانون الفرنسي يتوافر بالإسناد imputation أو بالإخبار allégation. أي أن المشرع الفرنسي وكذا باقي المشرعين الذين انتهجوا نفس النهج (المصري، الأردني، الجزائري...) لم يفرقوا بين الإسناد الذي يفيد نسبة الأمر إلى شخص المقذوف على سبيل التأكيد و بين الإخبار و الذي يدل على معنى الرواية على لسان الغير أو ذكر الخبر محتملا الكذب والصدق. بل شملوا بالعقاب كل حالات التعبير التي من شأنها أن تنال من شرف و اعتبار الأشخاص أو الهيئة المدعى عليها به و لو كان ذلك بطريقة تفيد التشكيك أو الإستفهام أو الغموض[1]، و سواء أكان ذلك في حضوره أم في غيابه، علم بها أم لم يعلم. كما أنه يستوي في ذلك وسيلة القول و وسيلة الكتابة،فقد يكون القول الحاصل بالمحادثات العربية أو بالمحادثات الأجنبية، و لكن بشرط أن تكون المحادثة ذاتها مفهومة. كما تستوي وسيلة الكتابة بمعنى أن الإسناد ذاته يتحقق سواء أكانت الكتابة تمت بخط اليد أو بالآلة الكاتبة أو بالكمبيوتر. و كذلك قد يتحقق بالإشارة إذا كانت مفهومة و متعارف عليها و قصد بها نسبة واقعة محددة لشخص آخر.[2]

و لا يشترط صدور أو ترديد عبارات القذف من القاذف، فقد يتحقق القذف بصيغة الإيجاب ردا على استفهام من ردد هذه العبارات.[3]

ب- موضوع الإسناد: فيجب أن تتحدد تلك الواقعة، وأن تجعل من أسندت إليه محلا للعقاب طبقا للقانون أو محلا للازدراء، أي الاحتقار عند أهل وطنه أومن يخالطهم أو يعاشرهم.أو أن تكون ماسة بالعرض أو خادشة لسمعة الشخص أو سمعة عائلته[4].

ج – علانية الإسناد: باستقرائنا لنصوص المواد التي عالجت جريمة القذف في التشريعات العقابية المختلفة نستخلص بأن أهم عنصر في هذه الجريمة وهو العلانية، والتي يقصد بها اتصال علم الجمهور بالتعبير الصادر عن فكرة المتهم أو رأيه أو شعوره عبر إحدى الوسائل التعبيرية والتي يمكن سردها كما يلي[5] :

– علانية القول أو الصياح أو ترديده: ويقصد بالجهر النطق وترديد عبارات القذف بصوت مرتفع بحيث يسمعه من كان حاضرا من الجمهور في أماكن عامة. أما الصياح فقد يكون كل صوت له معنى متعارف عليه ولو لم يكن مركبا من عبارات واضحة. ويمكن أن تتحقق هذه العلانية سواء على طريق ترديد القول أو الصياح من قبل الجاني بإحدى الوسائل الآلية (الوسائل الميكانيكية والوسائل اللاسلكية) التي من شأنها

---

[1]– د/محمد صبحي نجم، شرح قانون العقوبات الجزائري، القسم الخاص، ديوان المطبوعات الجامعية، الجزائر، ص99.

[2]– سامح محمد عبد الحكم، المرجع السابق، ص6.

[3]– ينظر د/محمد صبحي نجم، المرجع السابق، الموضع السابق.

[4]– د/أحمد شوقي أبو خطوة: شرح الأحكام العامة لقانون العقوبات الاماراتي، الطبعة الأولى، الجزء الأول، 1989، ص273.

[5] – أحمد عاصم أحمد عجيلة: ورقة عمل في موضوع رؤية قانونية حول ثبوت جرائم السب و القذف عبر الإنترنت في القانون المصري، المؤتمر الدولي الأول حول الخصوصية و أمن المعلومات في قانون الإنترنت، جوان 2008، http:// www.mohamoun-mountada.com

نقل الصوت أو تكبيره أو تعيده أو تعمل على نشره في مساحة أوسع كالميكروفون مثلا ومكبرات الصوت أو الإذاعة والتليفزيون أو الهاتف. وقد تتحقق العلانية بالقول والصياح في الأماكن العامة، والمقصود بها الأماكن المفتوحة للجمهور والتي يرتادها من يشاء ومتى شاء بصفة دائمة ومعتادة بدون قيود (سواء أكان ارتيادها مجانا أو بمقابل)، مثل الطرق العامة والحدائق العامة والشوارع والأزقة أو المسارح والمقاهي والمطاعم[1]. ويمكن تقسيمها إلى أماكن عامة بطبيعتها[2]. وأماكن عامة بالتخصيص وأماكن عامة بالصدفة.[3]

– علانية الأفعال أو الإشارات أو الحركات: وتتحقق تلك العلانية إذا وقعت في أماكن عامة، أو نقلت إلى المتواجد ين بتلك الأماكن بوسيلة من الوسائل الآلية.كما تتحقق إذا وقعت في مكان خاص وكان باستطاعة من كان متواجد في الأماكن العامة رؤيته أو تحول ذلك المكان إلى مكان عام بالصدفة[4].

–علانية الكتابة والرسوم والصور والأفلام والرموزو غيرها من طرق التعبير الأخرى: وتتم هذه الأخيرة في ثلاث صور:

العرض: ويقصد به عرض الكتابة أو طرق التعبير الأخرى في أماكن عامة، بحيث يمكن للجمهور رؤيتها أثناء تواجدهم فيها.

التوزيع: وتعني تسليم المكتوب أو غيره من طرق التعبير الأخرى إلى الغير بطريقة مباشرة أو غير مباشرة بدون تمييز. كأن يتم التوزيع باليد أو بالبريد العادي أو الإليكتروني أو بالفاكس أو بالوضع في الأماكن مختلفة[5].

البيع والعرض للبيع: ويقصد به إما بيع الصور أو الرسوم أو الأفلام للشخص الذي يريد الحصول عليها مقابل ثمن معين، أو إعداد المكتوب أو الرسوم أو غيرها من طرق التعبير وطرحها للبيع،أو الإعلان عنها للبيع سواء أكان ذلك في مكان عام أو خاص[6].

---

[1] – من الجرائم الأكثر شيوعا السب و القذف، www.nooralislam.alafdal.nethttp://

[2] – المكان العام بطبيعته هو المكان الذي يباح للجمهور ارتياده في أي وقت و في كل وقت كالطرق و الميادين العامة والحدائق. وسواء أكان مملوكا للدولة أم للمؤسسات أو أفراد.

المكان العام بالتخصيص هو المكان الذي قد يباح للأفراد ارتياده أو دخولها في أوقات محددة كالمسجد، المسارح و المقاهي و المطاعم و المدارس.

[3] – المكان العام بالصدفة: و هو المكان الخاص في الاصل و يمكن أن يسمح للافراد بدخوله و لكن بصفة عرضية مثل المطاعم و المحلات التجارية و العيادات الخاصة. د/ طارق سرور: قانون العقوبات، القسم الخاص، جرائم الإعتداء على الاشخاص، دار النهضة العربية، القاهرة، 2000، ص 341.

[4] – مثل سماع عدد من أفراد الجمهور قذفا على سلم منزل أو كان منزل يقطنه عدد من السكان بحيث يرد على أسماعهم ما يقع الجهر به من قذف على سلم ذلك المنزل، د/ طارق سرور، المرجع السابق،الموضع السابق.

[5] – د/ عدلي أمير خالد: المستحدث في جرائم الإعتداء على الأشخاص في ضوء المستحدث من القوانين و أحكام النقض والدستورية العليا، دار الفكر الجامعي، الاسكندرية، 2013، ص 350.

[6] – د/مدحت رمضان: دروس في قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1998، ص 590.

3/ الركن المعنوي:

القذف في جميع حالاته جريمة عمدية لا بد لقيامها من ثبوت القصد الجنائي و بالضبط القصد الجنائي العام لدى الجاني، أي اتجاه إرادته نحو نشر وإذاعة البيانات أو الأمور المتضمنة للقذف مع علمه بأن من شأنها أن تجعل من أسندت إليه محلا للعقاب والإزدراء[1].

ثانيا:أركان جريمة السب.

يتطلب لقيام جريمة السب كنظيرتها السابقة توفر ثلاث أركان، ركن شرعي و ركن مادي و ركن معنوي.

1/ **الركن الشرعي:** و يتمثل في النصوص القانونية التي تناولت جريمة السب كالمادة 2/29 من القانون المؤرخ في 1881/07/29 بشأن الصحافة في فرنسا المعدل بالقانون المؤرخ في 1986 و التي عرفت في السب العلني بأنه:" كل تعبير مهين أو ألفاظ تحقير أو قدح لا يشتمل على أي فعل محدد ". والمادة 306 من قانون العقوبات المصري و التي عرفت السب بأنه: "كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشاً للشرف أو الإعتبار يعاقب عليه في الأحوال المبينة بالمادة 171 بالحبس مدة لا تتجاوز سنة وبغرامة لا تقل عن ألف جنيه ولا تزيد على خمسة آلاف جنيه أو بإحدى هاتين العقوبتين." [2] المادة 188 من قانون العقوبات الاردني في فقرتها الثانية والتي عرفت القدح[3] بأنه:"هو الإعتداء على كرامة الغير أو شرفه أو اعتباره، و لو في معرض الشك و الاستفهام من دون بيان مادة معينة". و المادة 297 من قانون العقوبات الجزائري و التي عرفت هي الأخرى السب بأنه:"يعد سبا كل تعبير مشين أو عبارات تتضمن تحقيرا أو قدحا لا ينطوي على اسناد أية واقعة ."[4]

2/ الركن المادي:وتجدر الاشارة هنا أن جريمة السب تشترك في هذا الركن مع جريمة القذف، إلا أنها تختلف عنها في عنصر فعل الاسناد، اذ يتحقق السب بكل ما يمس اعتبار الإنسان وشرفه و ذلك بإسناد عيب معين أو غير معين إلى المجني عليه أو بكل ما ينطوي على معنى الاحتقار والتصغير. كمن يصف آخر بأنه ماجن، أو عربيد، أو كمن يقول عن واحد أنه منحط الخلق.[5]

---

[1] – وهذا ما أكدته محكمة النقض المصرية بأنه "لا يتطلب القانون في جريمة القذف قصدا خاصا، بل يكتفي بتوافر القصد العام و الذي يتحقق من نشر القاذف للأمور المتضمنة للقذف و هو عالم أنه لو كانت صادقة لأوجبت عقاب المقذوف أو احتقاره..." سامح محمد عبد الحكيم، المرجع السابق، ص 14.

[2] – ينظر المادة 306 من قانون العقوبات المصري.

[3] – تجدر الإشارة أن المشرع الأردني يسمي جريمة السب هنا بجريمة القدح.

[4] – ينظر المادة 297 من قانون العقوبات الجزائري.

[5]– د/ خالد ممدوح ابراهيم: فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الاسكندرية، 2010، ص328.

3/ الركن المعنوي:

تعتبر جريمة السب جريمة عمدية كما هو الشأن في جريمة القذف، اذ لا بد من توفر القصد الجنائي العام لدى الجاني و الذي يتحقق بانصراف ارادته إلى اذاعة الامور الخادشة للشرف أو الإعتبار مع علمه بمعناها[1].

و لقد تأثرت جريمة القذف و السب و التشهير كجرائم تقليدية بالتطور التكنولوجي في وسائل الاتصال، اذ أصبحت ترتكب عن طريق وسائل حديثة أهمها شبكة الانترنت. فظهر ما يسمى بجرائم السب و القذف والتشهير عبر الانترنت و ما أكثرها و أسهلها، إذ أنها ترتكب بمجرد الضغط على أزرار الكمبيوتر المتصل بتلك الشبكة أو الهاتف النقال المتصل بها، و دون الحاجة إلى بذل جهد عضلي في التنقل من مكان لآخر. فالجاني يبقى جالسا في منزله أو في مقاهي الانترنت وراء أجهزة الكمبيوتر أو حاملا لهاتفه النقال ويرتكب تلك الجرائم التقليدية الماسة بالشرف و الإعتبار. الأمر الذي أدى إلى زيادة عدد وحجم هذه الجرائم في ظل غياب نصوص قانونية تضبط هذه السلوكيات المستحدثة غير المشروعة. و على هذا فالسؤال الجوهري المطروح هنا هو: في ظل الفراغ القانوني الذي تعاني منه معظم التشريعات العقابية فهل يمكن تطبيق النصوص القانونية التقليدية و ما تضمنته من عقوبات على مثل تلك الجرائم التقليدية التي ترتكب بواسطة شبكة الانترنت؟ و هل تعتبر تلك الأخيرة طريقة من طرق العلانية التي تستلزمها جريمة القذف و السب كشرط أساسي و عنصر جوهري لقيامها؟.

المطلب الثاني:

جرائم القذف و السب والتشهير عبر الإنترنت.

و سنتناول تحت هذا المطلب الاجابة على السؤال المطروح أعلاه و ذلك بتقسيمه إلى فرعين نتناول في أولهما ماهية هذه الجرائم الواقعة عبر الانترنت، لنبين في ثانيهما موقف التشريعات المقارنة من هذه الجرائم الماسة بالشرف و الإعتبار الالكترونية. و ذلك على النحو التالي:

الفرع الأول: ماهية الجرائم الماسة بالشرف و الإعتبار الواقعة عبر الانترنت.

الفرع الثاني: موقف التشريعات المقارنة من هذه الجرائم الماسة بالشرف و الإعتبار الواقعة عبر الانترنت.

الفرع الأول: ماهية الجرائم الماسة بالشرف و الإعتبار الواقعة عبر الانترنت.

سنتطرق تحت هذا الفرع إلى تعريف كلا من جريمة القذف و السب و التشهير عبر الانترنت، ثم نبين صورها فالأساليب أو الكيفية التي ترتكب بها مثل هذه الجرائم عبر الانترنت. و ذلك كمايلي:

---

[1]– د/ خالد ممدوح ابراهيم، المرجع السابق، الموضع السابق.

أولا: تعريف جريمة القذف و السب و التشهير عبر الانترنت.

لقد ساعد التطور التكنولوجي الذي شهده عالمنا المجرمون لا سيما بعد ظهور الانترنت و غزوها للمجتمع، اذ شجعتهم على زيادة عدد و حجم جرائمهم دون زيادة في الجهد المبذول سابقا. و بذلك تطورت الجريمة التقليدية من حيث الوسائل المستخدمة في ارتكابها، و كذا في طريقة ارتكابها و من بينها الجرائم الماسة بالشرف و الإعتبار أي جريمة القذف و السب و التشهير، و التي أصبحت ترتكب عبر الانترنت بصورة سهلة و سريعة مقارنة بنظيرتها التقليدية. و يعرف القذف الالكتروني بأنه:" هو اسناد واقعة محددة تستوجب عقاب من تنسب اليه، و قد يكون بالقول أو الاشارة أو الكتابة. كما يمكن أن يكون في مواجهة المقذوف في مجلس أو مكان عام، أو في غيابه أمام الناس أو عبر وسائل الاعلام المقروءة أو المسموعة أو المرئية، كما يمكن أن يكون عبر المواقع الالكترونية كالمنتديات و شبكات التواصل الاجتماعي و الصحف الالكترونية و البريد الالكتروني، كما أنه يمكن أن يحدث عبر أجهزة الاتصالات كالجوال و الرسائل النصية و رسائل الوسائط المتعددة."[1]

ثانيا: صور القذف و السب و التشهير عبر الانترنت.

تتنوع صور القذف والسب والتشهير عبر الانترنت بتنوع الغرض والطريقة التي تستخدم بها تلك الأخيرة، فقد يكون وجاهيا عبر خطوط الاتصال المباشر، أي عن طريق المبادلات الاليكترونية الصوتية، أو كتابيا أو غيابيا عن طريق المبادلات الاليكترونية الكتابية أو فيديوية. وهي إما أن تكون بين طرفيات انترنت متصلة[2]، و إما أن تكون بواسطة طرفية انترنت منفصلة[3].

1/ المراسلات الاليكترونية عبر طرفية انترنت متصلة:

تقدم الانترنت جملة من الخدمات، إلا أن تلك الأخيرة لم تسلم من يد المجرمين إذ أصبحت ساحة لارتكاب أبشع جرائمهم و تحقيق أخطر أغراضهم الإجرامية.و تنقسم هذه الخدمات إلى قسمين: خدمات ذات طابع خاص و أخرى ذات طابع عام.

أ- خدمات ذات طابع خاص:

تتسم بعض الخدمات المتاحة عر الانترنت كخدمة البريد الاليكتروني و خدمة الاتصال المباشر عن بعد وكذا خدمة نقل الملفات بطابع الخصوصية، والمقصود بذلك انحصار الاتصال فيهم بين طرفين معلومين لبعضهم، إذ لا يجوز للغير الاطلاع على مضمون الرسائل المتبادلة بينهم إلا بمعرفة صاحب المصلحة.

---

[1]- القذف الالكتروني بأسماء وهمية،.http:// alryadh.com و ينظر كذلك

خالد حسين عبد التواب أحمد: جرائم القذف و السب العلني عبر الإنترنت، رسالة دكتوراه، جامعة عين شمس، 2011، ص17 و ما بعدها و ص255.

[2] – يشكل كل جهاز كمبيوتر متصل بشبكة الإنترنت بواسطة مودم عبر خطوط الهاتف طرفية متصلة بشبكة الإنترنت.

[3] – تمثل طرفية انترنت مستقلة، كل تقنية علمية حديثة عبر الحاسوب، تسمح بصورة مباشرة أو غير مباشرة بالتبادل الاليكتروني للبيانات أي ما يعرف بالشريك الاليكتروني.

مما يعني أنها تدخل في نطاق المراسلات الخاصة[1] التي تتمتع بالحماية القانونية المقررة لسرية الاتصالات عن بعد، مما يكفل عدم قدرة الآخرين على الاطلاع عليها أو كشف مضمونها[2].

و في هذه الحالات إذا وجد الشخص ألفاظا أو عبارات ماسة بسمعة و شرف أحد الناس في بريده الاليكتروني، فإن الجريمة لا تتحقق لانتفاء أهم عنصر فيها و هو العلانية. إذ أن الدخول إلى ذلك البريد والاطلاع على محتواه لا يكون متاحا للجميع- فهو عبارة عن مراسلة خاصة – حيث يستوجب الأمر استخدام بعض المعطيات التقنية كاسم المستخدم و كلمة المرور. ولكن و في المقابل يمكن أن تتحقق هذه الجريمة، إذا قام الجاني بتوزيع الرسائل لعدد غير محدود من المتعاملين مع الانترنت و بدون تمييز بينهم، إذ في هذه الحالات تتوافر العلانية التي تقوم عليها تلك الجريمة، حتى و لو كان الاستقبال يتوقف على شرط الاشتراك أو دفع مقابل[3].

إلا أن السؤال المطروح هنا هو: ما الوضع فيما لو احتفظ الشخص ببعض الألفاظ و العبارات الماسة بالشرف و الإعتبار في بريده الاليكتروني دون أن يرسلها لأحد، فهل تتحقق هنا تلك الجريمة أم لا؟.

و الجواب يكون بالايجاب، أي أن الجريمة تتحقق في هذه الحالة لأن البريد الاليكتروني موجود في ظل شبكة الانترنت التي يرتادها مختلف الناس و من بينهم تلك الذين يعرفون بالهاكر و الذين يتمتعون بقدرات خارقة، قد تكمنهم من الاطلاع على ذلك البريد و ما يحتويه من رسائل أو معلومات أو بيانات، التي قد يتصرفون فيها حسب ما شاءوا و يغيرونها (إما بالزيادة أو النقصان أو الحذف)[4].

فعلى هذا فعنصر العلنية يتحقق هنا بمجرد وضع الكلمات و العبارات الماسة بشرف و سمعة أحد الأشخاص و حفظها بالبريد الاليكتروني في شبكة الانترنت حتى و إن لم ترسل إلى الغير. ذلك لأن شبكة الانترنت تعتبر في حد ذاتها أحد أهم طرق العلانية. و البريد الاليكتروني ان تعذر الوصول إليه لدى البعض فإن غيرهم يمكنهم الوصول إليه و الاطلاع عما بداخله[5].

ب- خدمات ذات طابع عام:

و نقصد بها تلك الخدمات التي تتميز بطابع العمومية، أي أنها متاحة للجميع من حيث الابحار في ذلك الفضاء الفسيح كتصفح مواقع الويب و غرف المحادثة، أو إنشاء مواقع على شبكة الويب العالمية و التي يمكن لأي شخص أن يطلع عليها في جميع أنحاء العالم. و عليه إذا قام شخص بنشر كتابات أو عرض

---

[1] – يقصد بالمراسلة الخاصة: تلك الرسالة المخصصة لشخص واحد أو لعدة أشخاص طبيعية أو معنوية بصفة محددة وشخصية". د/ أحمد السيد عفيفي: الأحكام العامة للعلانية في قانون العقوبات، القاهرة، 2001، ص 29.

[2]– أحمد عاصم أحمد عجيلة، المرجع السابق، http:// www.mohamoun-mountada.com

[3]– أحمد عاصم أحمد عجيلة، نفس المرجع ، نفس الموقع.

[4]– لمزيد من التفاصيل ينظر د/ خالد ممدوح ابراهيم: حجية البريد الالكتروني في الاثبات، دار الفكر الجامعي، 2005، ص177.

[5]– ينظر حسين بن سعيد بن سيف الغافري:السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراه حقوق، جامعة عين شمس، 2005، ص246.

صور أو رسومات تتضمن معاني مؤذية و خادشة لشرف و سمعة و اعتبار شخص آخر، و تم عرضها على إحدى مواقع الويب، فهنا تتحقق الجريمة الماسة بسمعة و اعتبار الغير لتوفر العلانية. و هذا ما قضت به المحاكم الفرنسية باعتبار أن تلك الألفاظ المذاعة و المنتشرة عبر الانترنت موجهة لعدد غير محدود من الناس الذين يمكنهم الدخول إليها في أي لحظة؛ فتلك الجريمة تقع من لحظة وضع هذه التعبيرات على شبكة الانترنت في مواجهة جمهور احتمالي غير متوقع[1].

وصور الجهر بالقول أو الصياح أو ترديده عن طريق الوسائل الآلية، هي أكثر صور العلانية انطباقا على استخدامات الانترنت. فتتحقق تلك الأخيرة إذا استخدم الجاني الانترنت لإذاعة القول أو الصياح أو ترديده، و هذا نظرا لأن المشرع قد استخدم للتعبير عن ذلك عبارات مرنة، يمكن أن تندرج تحتها الانترنت. كما أن الرسائل الاليكترونية يمكن أن تشتمل على صوت و عادة ما ترسل من أماكن خاصة، فإن الجهر بها باستخدام الانترنت يتحقق به عنصر العلنية[2].

2/ المراسلات الاليكترونية عبر طرفية انترنت منفصلة:

تعد الجرائم الماسة بشرف و اعتبار الأشخاص أحد صور إساءات استخدام أجهزة الهواتف الخلوية التي يمكنها استقبال أو إرسال بيانات على شكل رسائل قصيرة SMS أو إلى أي بريد اليكتروني. وكذلك يمكنها الاتصال بأي موقع على الشبكة للاستفسار عن أية معلومات يريدها المستخدم أو إجراء تحويلات اليكترونية.

و السؤال المطروح هنا: ما مدى انطباق النصوص التقليدية على مثل هذه الممارسات؟.

بادئ ذي بدئ يمكن القول أن هناك حالتين لارتكاب تلك الجرائم من خلال تلك الطرفيات[3] :

الحالة الأولى: تتعلق بالرسائل الاليكترونية (رسائل السمع البصرية) المتضمنة عبارات القذف أو السبب أو الشتم من شبكة الانترنت إلى الهاتف النقال. و في هذه الحالة لا تقوم الجريمة لانتفاء عنصر العلنية. إذ أن المجني عليه وحده يمكنه رؤية أو سماع ما أسند إليه من عبارات لتمتعها بطابع الخصوصية.

الحالة الثانية: تتعلق بالرسائل الاليكترونية من الهاتف النقال إلى شبكة الانترنت من خلال خدماتها المتاحة كالبريد الاليكتروني أو شبكة الويب.... و في هذه الحالة تتحقق تلك الجريمة لتوفر عنصر العلنية.

ثالثا: الأساليب المستعملة في ارتكاب هذه الجرائم:

ومن الأساليب المستعملة للقذف و السب و التشهير عبر الانترنت:

1/ الألفاظ: و قد تكون بالكتابة أو شفاهة و يمكن حصرها في أربعة أنواع:

– ألفاظ تبين أن الشخص كان يمارس الزنا أو اللواط، كقوله كان زانيا أو يفعل فعل قوم لوط.

---

[1]–T.G.I Paris,réf 30 avril 1997, D.1998.Somm Convenentes,p 79.

[2]– أحمد عاصم أحمد عجيلة، المرجع السابق، http:// www.mohamoun-mountada.com

[3]– محمد أمين أحمد الشوابكة، المرجع السابق، ص 48.

– ألفاظ تمس الأخلاق كاعتياد الشخص على ارتياد الأماكن المخلة بالآداب (الملاهي الليلية و أماكن الدعارة).

– ألفاظ تمس أمانة الشخص ككونه خائن الأمانة أو مرتشي....

– ألفاظ تمس بالعقيدة كقولهم أنه علماني أو ليبرالي أو أصولي.[1]

2/ نشر الصور: صورا ضوئية أو فيديوية وسواء أكانت حقيقية أو كانت كاذبة (مركبة).

فأما الحقيقية فتكون في حالتين:

– نشر صور شخص في فعل حقيقي، كأن يمارس الجنس مع زوجته أو غيرها، أو يقبل امرأة تحل له أو لا تحل له.....

– نشر صور لشخص غير معروف بين الناس في وضع غير لائق اجتماعيا.

بينما تركيب الصور فيقسم إلى ثلاثة أقسام:

– نشر صور رأس شخص في أوضاع مخلة جنسيا.

– نشر صور رأس شخص في وضع مضحك، كأن يركب وجهه على صورة حيوان أو تركيب صورة متدين على صورة مغني.

– تركيب صورة شخص على صورة شخص يشرب الخمر أو يلعب القمار[2].

الفرع الثاني: موقف التشريعات المقارنة من جريمة القذف و السب و التشهير الواقعة عبر الانترنت:

و سنعرض تحت هذا الفرع موقف التشريعات الجنائية المقارنة من هذه الجرائم الماسة باعتبار و شرف الاشخاص وذلك بتقسيمها إلى موقفين، نخصص أولهما لتبيان موقف التشريعات الغربية.و في المقابل نخصص ثانيهما لتبيان موقف التشريعات العربية مركزين في ذلك على موقف التشريع الجزائري خاصة حيال هذه الجريمة التقليدية المرتكبة عبر الانترنت. و ذلك كمايلي:

أولا: موقف التشريعات الغربية من الجرائم الماسة باعتبار وشرف الاشخاص الواقعة عبر الانترنت.

و سنحصر موقف التشريعات الغربية من الجرائم الماسة باعتبار و شرف الاشخاص عبر الانترنت في موقف التشريع الفرنسي فقط . وذلك كالآتي:

جرم المشرع الفرنسي جرائم القذف و السب العلني بنصوص خاصة في قانون 29 جويلية 1881 بشأن حرية الصحافة، اذ عرفت المادة 29 منه في فقرتيها الاولى و الثانية هاتين الجريمتين كالتالي: "يعتبر قذفا علنيا إخبار أو إسناد لفعل يمس شرف و إعتبار الشخص أو الهيئة التي أسند إليها هذا الفعل. "[3]. ويعتبر

---

[1] – د/ حسين الغافري، محمد الألفي، المرجع السابق، ص 112.

[2] – د/ حسين الغافري، محمد الألفي، نفس المرجع ، ص 113.

[3] - Article 29 /1: «…….Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation . La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable، même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés، mais dont l'identification est rendue possible par les termes des discours، cris، menaces، écrits ou imprimés، placards ou affiches incriminés. »

سبا علنيا كل تعبير مهين أو ألفاظ تحقير أو قدح لا يشتمل على أي فعل محدد." [1] و هي تستوجب لقيام هاتين الجريمتين توافر شرط العلانية[2] و الذي يتحقق عن طريق وسيلتان: وسيلة القول أو الصياح أو التهديد. و وسيلة الكتابة أو وسائل التمثيل الأخرى كالصور و الرسوم و الرموز و النقوش . و لقد اعترف صراحة بامكانية وقوع هذه الجريمة عبر شبكة الانترنت من خلال المادة 23 من ذات القانون[3] . و لقد طبق القضاء الفرنسي هذه النصوص على جريمة القذف و السب عبر شبكة الانترنت و اعتبرها صورة من صور جرائم النشر.[4]

ثانيا:موقف التشريعات العربية من الجرائم الماسة باعتبار وشرف الاشخاص الواقعة عبر الانترنت.

و سنعرض في هذه النقطة موقف التشريعات العربية بصفة عامة حيال الجرائم الماسة باعتبار وشرف الاشخاص الواقعة عبر الانترنت بداية، لنوضح بعدها موقف التشريع الجزائري منها .

---

[1] – Article 29 /2 : « Toute expression outrageante، termes de mépris ou invective qui ne renferme l'imputation d 'aucun fait est une injure ».

[2]– تجدر الاشارة إلى أنه في حالة تخلف شرط العلانية، فهذا لا يؤثر على السلوك الاجرامي الواقع على شرف و إعتبار الأشخاص و إنما يصبح يشكل جريمة سب غير العلني و التي تكيف على أنها مخالفة وفقا لقانون العقوبات الفرنسي الجديد وفقا للمادة 1/621– 2/621 و معاقب عليها بغرامة قدرها أكثر من 38 يورو وفقا للمادة 131–13 من قانون العقوبات الفرنسي.

[3] – Article 23: «Seront punis comme complices d'une action qualifiée crime ou délit ceux qui، soit par des discours، cris ou menaces proférés dans des lieux ou réunions publics، soit par des écrits، imprimés، dessins، gravures، peintures، emblèmes، images ou tout autre support de l'écrit، de la parole ou de l'image vendus ou distribués، mis en vente ou exposés dans des lieux ou réunions publics، soit par des placards ou des affiches exposés au regard du public، soit par tout moyen de communication au public par voie électronique، auront directement provoqué l'auteur ou les auteurs à commettre ladite action، si la provocation a été suivie d'effet.

Cette disposition sera également applicable lorsque la provocation n'aura été suivie que d'une tentative de crime prévue par l'article 2 du code

pénal ».

[4] – Voir Diffamation et injures sur l'internet : le Tribunal de grande instance est déclaré compétent,Ordonnance du 22 janvier 2003 du TGI Paris , http:// www.foruminternet.org

و تجدر الاشارة إلى أن محكمة النقض الفرنسية في هذا المقام إعتبرت جريمة القذف عن طريق النشر هي جريمة وقتية تتم بارتكاب أول فعل نشر. كما أن القضاء الفرنسي الحديث قد أقر التوسع في الوسيلة لقبول الوسائل التقنية الحديثة التي لم تكن معروفة عند صدور قانون 1881. ينظر د/خالد ممدوح ابراهيم، (فن التحقيق الجنائي في الجرائم الالكترونية) مرجع سابق، ص 234. وكذا د/ عبد المجيد زعلاني: قانون العقوبات الخاص، الطبعة الثانية، دار هومة، الجزائر، ص 126.

1/ موقف التشريعات العربية بصفة عامة من الجرائم الماسة باعتبار وشرف الاشخاص الواقعة عبر الانترنت.

أما فيما يخص التكييف القانوني لهذه الجرائم الماسة بسمعة الشخص واعتباره التي تتم باستخدام الانترنت وبواسطة إنشاء مواقع خاصة بقذف وسب والتشهير سواء بشخص معين أو بدولة من الدول أو بدين من الأديان، فيمكن القول بأن التشريعات العربية انقسمت بشأنها إلى قسمين، قسم فضل تكييف هذه الجرائم تحت طائلة نفس النصوص القانونية التي تجرم تلك الأفعال متى تمت بالطرق **التقليدية**. مثل **القانون المصري** الذي جرم تلك الأفعال و عاقب عليها من خلال المواد من 302 – 310 من قانون العقوبات المصري. و قسم آخر خصها **بقوانين خاصة** تلاءم طبيعة المحيط المرتكبة فيه مثل **نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية السعودي** حيث جرم المشرع السعودي جريمة التشهير عبر الإنترنت في المادة 5/3 منه.[1]

ونفس الشأن بالنسبة **للمشرع الإماراتي** وذلك في المادة 15 [2] من القانون الاتحادي رقم 2 لسنة 2006 بشأن جرائم تقنية المعلومات، إذ جرم فعل السب والإساءة إلى المقدسات والشعائر الدينية وإلى إحدى الأديان السماوية.

وأسباب ذلك التجريم تنطوي على أن الحرية والديمقراطية التي تنعم بها الشعوب لا يجب أن تنطوي على الإخلال بها وتجريح الأشخاص في أعراضهم ومبادئهم وشرفهم ونسب أمور غير صحيحة لهم لغرض التشهير بهم وبمبادئهم والخوض في أعراضهم وفي حياتهم الخاصة التي هي ملك لهم وحدهم دون أن يكون لأي شخص أخر أن يخوض أو يتدخل فيها بأي شكل من الأشكال[3].

2/ موقف التشريع الجزائري من الجرائم الماسة باعتبار وشرف الاشخاص الواقعة عبر الانترنت

عالج القانون الجزائري الجرائم الماسة باعتبار وشرف الاشخاص في القسم الخامس من الباب الثاني المعنون بالجنايات و الجنح ضد الأفراد، في المواد 296 – 299 عقوبات جزائري. إذ عرف القذف في

---

[1] – تنص المادة 5/3 من نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية السعودي على :"يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:.....

5– التشهير بالآخرين، وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة."

[2] – تنص المادة 15 من القانون الاتحادي رقم 2 لسنة 2006 بشأن جرائم تقنية المعلومات على : "يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين كل من ارتكب إحدى الجرائم التالية عن طريق شبكة المعلوماتية أو إحدى وسائل تقنية المعلومات

1 – الإساءة إلى إحدى المقدسات أو الشعائر الإسلامية

2 – الإساءة إلى إحدى المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات و الشعائر مصونة وفقا لأحكام الشريعة الإسلامية.

3 – سب أحد الأديان السماوية المعترف بها... ".

[3] – منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص 37.

المادة 296 قانون عقوبات[1] ، في حين عرف السب في المادة 297 عقوبات[2] . و يتضح من خلال هذين النصين أن المشرع الجزائري يتطلب لقيام هاتين الجريمتين توافر صفة العلانية و التي تستخلص من الوسائل أو الطرق المستعملة المنصوص عليها في المادة 296 من قانون العقوبات و التي هي ذاتها بالنسبة لجريمة السب بالرغم من سكوت المشرع عن النص عنها.[3]

هذا من جهة و من جهة أخرى، فإنه و بالرجوع لنص المادة 296 السالفة الذكر نستخلص أن المشرع الجزائري ميز بين ثلاث طوائف تقوم بهم العلانية. و هي:

– العلانية بطريق القول أو الصياح أو ترديده: و التي تتحقق إذا حصل الجهر و الافصاح بالكلام بكيفية تسمح بسماعها من الغير، أي أن تكون في أماكن عمومية مثل المحافل الحفلية أو الطرق العامة او أي مكان مطروق من الجمهور. و تعتبر هذه الصورة من صور العلانية الأكثر انطباقا في شبكة الانترنت، خاصة و أن هذه الأخيرة تقدم خدمات كثيرة كغرف الدردشة و المجموعات الاخبارية تعتمد أساسا على تقنيات الصوت و الصورة. و بالتالي تتحقق العلانية فيما لو استخدم الجاني شبكة الانترنت في إذاعة القول أو الصياح او التهديد.

– العلانية بطريق الكتابة أو المنشورات او اللافتات أو الاعلانات: و تتحقق العلانية في هذه الصورة بعملية التوزيع على العامة دون تمييز، أو التعريض للأنظار بحيث يراها من يمر بالمكان المعروضة فيه، أو البيع أو العرض للبيع. و تتحقق هذه الصورة أيضا على شبكة الانترنت لا سيما أن الاستخدام الأكبر للانترنت مازال يعتمد على الكتابة.

– العلانية بوسائل أخرى: و هذا ما نصت عليه المواد 1/144 مكرر و144 مكرر 2 و 146 من قانون العقوبات[4]، و التي يتضح من استقرائها على امكانية وقوع جريمة القذف و السب عبر الانترنت لما تكون

---

[1]– تنص المادة 296 من قانون العقوبات الجزائري على:"يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف أو إعتبار الأشخاص أو الهيئة المدعى عليها بها أو إسنادها إليهم أو إلى تلك الهيئة و يعاقب على نشر هذا الادعاء أو ذلك الاسناد مباشرة أو بطريق إعادة النشر حتى و لو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم،و لكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الاعلانات موضوع الجريمة."

[2]– تنص المادة 297 من قانون العقوبات الجزائري على :" يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة."

[3]– يمكن استخلاص طرق العلانية بقراءة لنص المادة 463 بمفهوم المخالفة و الذي يكيف فيها السب كمخالفة حينما يكون غير علني. و قد أقر القضاء صراحة الطابع العلني لجريمة القذف و هو ما ينطبق أيضا على السب و تطلب وجوب التصريح به في الحكم. أشار إليها د/ عبد المجيد زعلاني، المرجع السابق ، ص 123.

[4]– تنص المادة 1/144 مكرر من قانون العقوبات على أنه :" يعاقب بالحبس من ثلاثة (3) أشهر إلى إثني عشر (12) شهرا و بغرامة من 50000 دج إلى 250000 دج أو باحدى هاتين العقوبتين فقط كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصوير أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى." و تنص المادة 144 مكرر 2 على أنه:" يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات و بغرامة من 50000 دج إلى 100000 دج أو بإحدى هاتين العقوبتين فقط كل من أساء و كما اعترف في إلى الرسول (صلى الله عليه و سلم) أو بقية الأنبياء أو استهزأ بالمعلوم من الدين بالضرورة أو بأية شعيرة من شعائر الإسلام سواء عن طريق الكتابة أو الرسم أو التصريح أو أية وسيلة أخرى." أما المادة 1/146 فتنص على :" تطبق على الاهانة أو السب أو القذف الموجه بواسطة الوسائل التي حددتها المادتان 144 مكرر و 144

موجهة لرسول الله (صلى الله عليه و سلم) أو لرئيس الجمهورية أو الهيئات النظامية أو المؤسسات العمومية إذا تمت بأية آلية لبث الصوت أو الصورة أو أية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.
أما فيما يخص العقوبة المقررة للجريمتين فهي تختلف حسبما إذا كانتا موجهتين إلى أفراد عاديين أو عامين. فأما بالنسبة لعقوبة القذف و السب الموجهان إلى الأفراد العاديين فهي طبقا للمادة 1/289[1] قانون عقوبات الحبس من 5 أيام إلى ستة أشهر و بغرامة 5000 دج إلى 50000 دج أو باحدى هاتين العقوبتين هذا بالنسبة للقذف، أما السب فالعقوبة المقررة له طبقا للمادة 299 تتمثل في الحبس من ستة أيام إلى ثلاثة أشهر مع توقيع نفس الغرامة المقررة للقذف.
أما بالنسبة لعقوبة القذف و السب الموجهان إلى أشخاص ينتمون إلى بعض المجموعات كالعرقية أو المذهبية أو إلى دين معين بغرض التحريض على الكراهية بين المواطنين أو السكان فهي طبقا للمادة 2/289[2] عقوبات الحبس من شهر إلى سنة و بغرامة من 10000 دج إلى 100000 دج أو باحدى هاتين العقوبتين.
و أما فيما يخص القذف و السب الموجهان إلى مؤسسات و هيئات ذات طابع عام فالعقوبة مقررة كالتالي:
– القذف و السب الموجهان إلى رئيس الجمهورية : فطبقا للمادة 144 مكرر فالعقوبة المقررة لمرتكبيها هي الحبس من ثلاثة أشهر إلى اثني عشر شهرا و بغرامة من 50000 دج إلى 250000 دج أو باحدى هاتين العقوبتين. و يشدد العقاب بمضاعفته في حالة العود.
– القذف و السب الموجهان ضد الهيئات و المؤسسات العمومية الأخرى: و تطبق على مرتكبيها ذات العقوبة المقررة لرئيس الجمهورية.
– القذف و السب الموجهان ضد رموز الدين: فالعقوبة المقررة نصت عليها المادة 144 مكرر 2 قانون عقوبات و هي الحبس من ثلاث (3) سنوات إلى خمس (5) سنوات و بغرامة من 50000 دج إلى 100000 دج.
و عليه نستخلص أن المشرع الجزائري اعترف بوقوع الجرائم الماسة بشرف و اعتبار الأشخاص عبر الانترنت.

مكرر1 ضد البرلمان أو إحدى غرفتيه أو ضد المجالس القضائية أو المحاكم أو ضد الجيش الوطني الشعبي أو أية هيئة نظامية أو عمومية أخرى، العقوبات المنصوص عليها في المادتين المذكورتين أعلاه."

[1]– ينظر المادة 1/289 من قانون العقوبات الجزائري .

[2]– ينظر المادة 2/289من قانون العقوبات الجزائري .

و من الأمثلة الواقعية عن هذه الجرائم نذكر:

– ألقت إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بوزارة الداخلية في مصر القبض على محام انتحل صفة مخرج تليفزيوني عبر موقع الفيس بوك على الإنترنت وقام بإرسال رسائل إلكترونية تحمل عبارات سب وقذف لجميع معارفه انتقاما منه لوجود خلافات بينه وبين شقيقة زوجة المخرج[1].

– وفي حادثة أخرى ، تعرضت فتاة تونسية للتشهير عبر الإنترنت من طرف خطبيها السابق المصري الجنسية والذي قام بإظهار صورتها وذكر اسمها ولقبها وبشتمها وسبها وقذفها وبخدش شرفها، ولم يكتف ذلك الأخير بأن نشر فضيحتها بين عائلتها وذويها بل أكثر من ذلك للإساءة ولإفساد علاقتها مع أصدقائها وأرباب عملها، إذ هددها بنشر صور تثبت وجود علاقة حميمية كاذبة بينهما عبر النت[2].

– وفي الخليج و مع بداية دخول الخدمة في تلك المنطقة وقعت حادثة مشهورة جرى تداولها بين مستخدمي الإنترنت، حيث قام شخص في دولة خليجية بإنشاء موقع شبكة الإنترنت نشر فيه صورة لفتاة وهي عارية مع صديقها، وكان قد تحصل على تلك الصور بعد التسلل إلى جهاز الحاسب الآلي الخاص

---

[1] – جريدة الأهرام، 2009/04/17، ص 12. وفي قضية أخرى تتلخص وقائعها في أنه وذات يوم فوجئت المدرسة زوجة مهندس الكمبيوتر برسائل سب وقذف وإتهام في عرضها على الإيميل الخاص بالمدرسة التي تعمل بها. واتهمت بذلك خطيبها السابق الذي صدر بشأنه حكم بالحبس لمدة سنة وغرامة 5 آلاف جنيه للإزعاج عن طريق النت والسب والقذف. وفي قضية ثالثة موضوعها قذف وسب مديرة تسويق شركة إلكترونيات، تتلخص وقائعها في أن المجني عليها اتهمت المدير التنفيذي بالشركة ومسؤولا أخر بسبها وخدش شرفها وذلك بنشره صور خاصة بها عبر الإنترنت. ضف إلى ذلك تضررها من مجهول صمم موقعا باسمها على شبكة الإنترنت يضم صورا مأخوذة من جهازها الشخصي (اللابتوب) المتروك في الشركة، وأنها تلقت رسائل على بريدها الإلكتروني تتضمن عبارات تسيء لها ولزوجها، تحتوي على عبارات سب وقذف منها وصفها وزوجها "بالغباء" وصورة لقرد يحمل ورد وأسفله عبارة: "خلي جوزك يغير الورد دة. وفي قضية مماثلة تمكنت المباحث المصرية من ضبط مهندس مصري يقوم بنشر معلومات كاذبة على إحدى مواقع الويب بهدف التشهير لعائلة مسؤول مصري وابنته. وفي ذات السياق أمرت النيابة العامة بحبس المتهم نتيجة الشائعات التي حدثت في المجتمع الطبي داخل مصر وخارجها والتي أثرت سلبا على سمعة الدواء وكذا على الدخل القومي إذ تتلخص وقائع القضية في أن موظف يقسم المعلومات بهيئة المصل واللقاح قام بإنشاء موقعين عبر شبكة الإنترنت مستخدما البريد الإلكتروني لهما، وهما يحملان الاسم التجاري للهيئة على شبكة الإنترنت وأرسل إلى الشركات العالمية والمتعاملين مع الهيئة وكالتها في مصر والخارج، رسائل تتضمن سب وقذف وتشهيرا بالشركة (الشركة القابضة للمستحضرات الطبية) وتخوفا من منتجاتها وخاصة الأنسولين والمستحضرات الأخرى. ينظر على التوالي: أحمد رزق رياض: عقوبة جريمة الازعاج على النت تصل إلى الحبس سنة، 17 أوت 2010، جريدة الجمهورية. قضية منشورة على الإنترنت من صحيفة الخبر الاليكترونية بعنوان: غدا الحكم في دعوى مديرة التسويق للإساءة لشرفها عبر الإنترنت يوم 2010/09/26.http://www.gn4me.com . د/ حسين الغافري، محمد الألفي، المرجع السابق، ص 110–111.

[2] – التشهير عبر الإنترنت، برنامج 90 دقيقة، قناة المحور، يوم 2010/12/22..

بها ونسخ منه تلك الصور. ولما حاول ابتزازها جنسيا بتلك الصور ورفضت قام بإنشاء ذلك الموقع ونشر فيه تلك الصور مما أدى بالفتاة إلى أن تنتحر بعد ما سببه لها من فضيحة بين أهلها وذويها.[1]

– وفي بريطانيا قام جندي بسب كايت ميدلتون على الفايسبوك لأنها لم تعره انتباهها بمرورها في السيارة مع خطيبها الأمير ويليام[2].

– كما وقعت حادثة تشهير أخرى من قبل تصدى لها من أسموا أنفسهم "الأمجاد هكرز"، حيث أصدروا بيان نشر على الإنترنت بواسطة البريد الإلكتروني ووصل للعديد من مشتركي الإنترنت أوضحوا فيه قيام شخص بالتطاول في أحد المنتديات (منتديات الحجاز للجوال) بالسب والقذف على شيخ الإسلام "ابن تيمية" وغيره من رموز الفكر الإسلامي الذي يلتف حولهم المسلمون لمعرفة أمور دينهم ودنياهم وقد إستطاع من أسموا أنفسهم "الأمجاد هكرز" إختراق البريد الإلكتروني لهذا الشخص الذي قام بالتطاول على رموز الإسلام ومن ثم نشر صوره وكشف أسراره في موقعهم على الإنترنت لتجرئه على ما ارتكبه في حق رموز الإسلام[3].

المبحث الثاني:

جرائم الصحافة الالكترونية و العنف عبر الانترنت

شهدت بدايات التسعينات من القرن الماضي نقلة نوعية لم يسبق لها مثيل في تاريخ البشرية في مجال الانفجار الضخم و غير المسبوق في مجال المعلومات التي ترافقت مع التطبيق التجاري لشبكة الانترنت في مختلف دول العالم، وما شكلته من أداة ووسيط و مرجع في نقل و تخزين وتبادل ومعالجة واسترجاع المعلومات والبيانات مستعينة بالامكانات العملاقة للحواسيب المستعملة والموصولة بالشبكة العنكبوتية.فتأثرت بذلك وسائل نقل المعلومات ونشرها، وبالأخص الصحافة. اذ ظهرت كثمرة لهذا التطور

---

[1]– أما في السعودية نشرت صحيفة الرياض السعودية خبرا بإدانة شخصين سبا أخر عبر منتدى إلكتروني وتتلخص وقائع القضية في أن سعوديين في العقد الثالث من العمر، تطاولا بالسب والشتم والاتهامات الكاذبة بلا حجة لأحد الموظفين عبر أحد المنتديات الإلكترونية بمنطقة القصيم (السعودية). حيث قام الأول بكتابة مقال تضمن السب والشتم والاتهامات الكاذبة عبر المنتدى الإلكتروني. أما الثاني فقام بالتعليق على موضوع الأول بمزيد من السب والشتم والاتهامات الكاذبة. و في قضية أخرى حكم على شاب بالسجن لمدة 20 يوما وبغرامة قدرها 5000 ريال لتهجمه على موظف حكومي بالسب والشتم عن طريق الإنترنت. وفي دولة الإمارات العربية المتحدة أدانت محكمة جنح دبي أحد مشجعي كرة القدم بتهمة القذف والسب لشرطة دبي على شبكة الإنترنت، حيث أنه أنشأ موقعا خاصا به على الشبكة تعرض فيه القذف والسب لشرطة دبي بزعم أنها ضربته بعد إحدى المباريات وقضت بتغريمه ثلاثة آلاف درهم إماراتي. ينظر على التوالي: منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص 36. قضية منشورة على الإنترنت على الموقع http://www.alsaha.com. الحكم بالسجن و الغرامة على شاب شتم موظفا عاما على الإنترنت، www.brzan.com http:// . خبر منشور على الإنترنت على الموقع التالي:www.alwatan.com.sa http:// .

[2] – خبر منشور على موقع قناة العربية يوم 2011/04/26 على http://www.alarabya.net

[3] – محمد محمد عبد الله المنشاوي، البحث السابق، المنشور على http://www.minshawi.com

صحافة الكترونية ناتجة عن النشر الالكتروني، الذي مكن من تحميل المعلومات على الوسائط الالكترونية التي تتم اعادة تشغيلها و عرضها عن طريق جهاز الحاسوب. و الصحافة الالكترونية هي نوع من الاتصال بين البشر يتم عبر الفضاء الالكتروني (الانترنت و شبكات المعلومات و الاتصالات الاخرى) تستخدم فيه فنون و آليات و مهارات العمل في الصحافة المطبوعة مضافا اليها مهارات و آليات تقنيات المعلومات التي تناسب استخدام الفضاء الالكتروني كوسيط أو وسيلة اتصال بما في ذلك استخدام النص والصوت و الصورة و المستويات المختلفة من التفاعل مع المتلقي، لاستقصاء الأنباء الآنية و غير الآنية و معالجتها و تحليلها و نشرها على الجماهير عبر الفضاء الالكتروني بسرعة.[1]

ولكنه و في المقابل لم تسلم هذه الصحافة و بالرغم ما تقدمه للبشرية من استخدامها في نشر الأكاذيب والاشاعات و التحريض على القيام بأعمال تهدد مصالح دول العالم باستعمال الانترنت، الأمر الذي حصل في الدول العربية التي اجتاحها بما يسمى بالربيع العربي وخصوصا بعدما ظهرت مواقع التواصل الإجتماعي من التويتر و الفايسبوك و اجتياحها للعالم و تحولها من مجرد وسائل للهو و التواصل الإجتماعي الى وسائل جديدة أثرت كثيرا على وسائل الإعلام التقليدية و أصبحت تساهم بفعالية في الحراك المجتمعي و السياسي في العالم. و على هذا ظهر نوع مستحدث من الاجرام الواقع على الصحافة يسمى باجرام الصحافة الالكترونية.

هذا من جهة و من جهة أخرى، فإنه و من أخطر الآفات الاجتماعية التي تهز كيان المجتمع و تضعه على حافة الانهيار هي آفة العنف اذا ما انتشرت بين أبنائه، و لكنه و مع الأسف بدأت هذه الظاهرة في الآونة الأخيرة تشهد انتشارا رهيبا كانتشار النار في الهشيم، و لا سيما مع ظهور الانترنت والتي قد تكون سببا لدفع مستخدميها الى العنف و التشاجر مع الآخرين أو تكون سببا في ارتكاب جرائم قتل.وعليه ظهرت جرائم عنف من ضرب و جرح وقتل سببها الوحيد الانترنت.وسيتم تبيان ذلك في المطلبين التاليين:

المطلب الأول: جرائم الصحافة الالكترونية.

المطلب الثاني: العنف عبر الانترنت.

المطلب الأول:

جرائم الصحافة الالكترونية.

و سنحدد في هذا المطلب الأحكام العامة التي تحكم جرائم الصحافة في الفرع الأول، أما الفرع الثاني فخصصناه لتعريف جرائم الصحافة الالكترونية و أركانها. ثم حددنا موقف التشريعات المقارنة من هذه الجرائم في الفرع الثالث.و ذلك كمايلي:

الفرع الأول:الأحكام العامة لجرائم الصحافة.

الفرع الثاني: تعريف جرائم الصحافة الالكترونية و أركانها.

الفرع الثالث: موقف التشريعات المقارنة من جرائم الصحافة الالكترونية.

---

[1]– تعريف الصحافة الالكترونية ، http:// forums.m7taj.org

الفرع الأول: الأحكام العامة لجرائم الصحافة.

و سنتطرق في هذا الفرع إلى تعريف جرائم الصحافة و إلى تبيان أركانها. و ذلك كمايلي:

أولا: تعريف جرائم الصحافة.

تعددت محاولات الفقهاء لتعريف جرائم الصحافة[1]، فذهب جانب من الفقه إلى القول بأن هذه الجرائم هي جرائم ذهنية تتمثل في الإعلان عن فكرة أو رأي بسوء قصد، يعاقب عليها القانون[2]. و ذهب رأي فقهي آخر إلى تعريفها بأنها جرائم القانون العام تتمثل في الاعلان عن فكرة أو رأي تجاوز حدوده، و تكون وسائل الاعلام بمثابة أداة التي أستعملت في ارتكابها.[3] كما يمكن تعريف جرائم الصحافة بأنها:" جرائم تعبير عن الرأي و الفكر يقع الاعتداء فيها على مصالح الفرد و الجماعة بواسطة وسيلة من وسائل الاعلام أو ما يماثلها"[4]. ومثالها: جريمة نشر الأخبار الكاذبة وجريمة ترويج الإشاعات وجريمة الترويج لتغيير مبادئ الدستور الأساسية أو النظم الأساسية للهيئة الإجتماعية وجريمة إذاعة أسرار الدفاع،أو اذاعة فحوى المداولات السرية للجهات القضائية وأيضا حيازة محررات أو مطبوعات تتضمن إشاعات كاذبة إذا كانت معدة للتوزيع أو إطلاع الغير عليها، وكذا جريمة تحريف الكتب الدينية وتقليد إحتفال ديني بقصد السخرية، والتحريض على القتل أو النهب أو الحرق، أو الإخلال بأمن الدولة وجريمة إهانة و قذف وسب رئيس الجمهورية أو حيازة صور تسيء إلى سمعة البلاد[5].

ثانيا:أركان جرائم الصحافة.

تقوم الجرائم الصحفية كغيرها من الجرائم على ثلاث أركان و هي:

1/ الركن الشرعي: والمتمثل في النصوص القانونية المجرمة لمثل ذلك الأفعال كالمواد 96 و100 و102 و144 مكرر – 144 مكرر و147 إلخ... من قانون العقوبات الجزائري و274 – 290 – 291 – 317 – 318 – 319 – 320 عقوبات ليبي.

2/الركن المادي: والذي يتحقق النشاط المادي فيه بنشر الفكرة و بنتيجة و التي تتحقق على إثر هذا السلوك. ففي جريمة السب و القذف مثلا يجب أن يترتب على نشر الفكرة المساس بشرف و اعتبار المجني عليه من خلال اسناد واقعة باحدى الطرق التي تتحقق بها العلانية . و العلانية هنا تعتبر عنصرا مميزا لتلك الجريمة و هي تمثل أساس العقاب عليها. و نقصد بها اتصال علم الجمهور بعبارات و ألفاظ

---

[1] – تسمى تلك الجرائم كذلك جرائم النشر أو جرائم الرأي أو الجرائم الإعلامية.

[2] – http://palmoon.net ينظر جرائم الاعلام ،:http://dc307.4shared.

[3] – ينظر جرائم الاعلام ،http://palmoon.net

[4] –الطيب بلواضح: حق الرد و التصحيح في جرائم النشر الصحفي و أثره على المسؤولية الجنائية في ظل قانون الإعلام الجزائري رقم 90–07، أطروحة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2012–2013، ص 29.

[5] –حمدي الأسيوطي: جرائم النشر و الصحافة و حماية الصحافي،http:// www.kafishokr.com

شائنة، تم التعبير عنها بالقول او الفعل او الكتابة أو بأية وسيلة أخرى من وسائل التعبير عن الرأي أو المعنى.[1]

3/الركن المعنوي: تصنف جرائم الصحافة ضمن الجرائم العمدية التي يستلزم فيها قصد جنائي. أي يجب توفر العلم بتحقق أركان الجريمة مع اتجاه إرادة الجاني إلى ارتكابها. وعموما يكفي تحقق القصد الجنائي العام في مثل هذه الجرائم، واستثناء قد يتطلب المشرع إلى جانبه توفر قصد جنائي خاص[2] . ومن أمثلة ذلك جريمة نشر أمور بقصد إحداث التأثير في القضاة التي تنص عليها المادة 147 من قانون العقوبات الجزائري والتي تقابلها المادة 187 من قانون العقوبات المصري.

وتعد جرائم الصحافة إحدى جرائم البث العلني المصنفة ضمن جرائم الإعتداء على الأشخاص والتي تصدت لها معظم المدونات العقابية وغير العقابية[3].

وتجدر الإشارة إلى أن هذه الجرائم ترتكب في أغلب الأحوال بالكتابة، وتتوفر وسائل العلانية بالكتابة إذا ما تحققت ثلاثة شروط: التوزيع والعرض و البيع أو العرض للبيع.[4]

الفرع الثاني:تعريف جرائم الصحافة الالكترونية و أركانها:

و سنبين في هذا الفرع على غرار الأول ما المقصود من جرائم الصحافة الالكترونية، ثم نحدد أركانها. وذلك كمايلي:

أولا: تعريف جرائم الصحافة الالكترونية.

تعتبر جرائم الصحافة الالكترونية من الجرائم المستحدثة التي أفرزها عصر يتكلم بلغة المعلوماتية، لا سيما مع ظهور الإنترنت والتي حولت الإعلام المقروء بوسائله التقليدية إلى إعلام إلكتروني يتم بثه عن طريق الإنترنت، إذ ظهر بذلك ما يسمى بالصحافة الإلكترونية الفورية[5]، إضافة إلى ذلك أصبح بمقدور الفرد العادي غير المنتمي إلى مؤسسة صحفية القيام بإنشاء موقع خاص به، يبدي من خلاله بآرائه في مواضيع معينة، دون شروط أو قيود تحد من مشاركته أو من المساحة المتاحة له للتعبير عن آرائه.أو بصيغة أخرى

---

[1]– ينظر مقال جرائم الصحافة ، http://www.djelfa.info

[2]– ينظر شريف سيد كامل: جرائم الصحافة في القانون المصري، الطبعة الثانية، دار النهضة العربية، القاهرة،1997، ص33.

[3] – و كمثال عن القوانين غير العقابية في مصر قانون تنظيم الصحافة رقم 1996/96 و قانون الطفل رقم 1996/12 وقوانين تقييد حرية الرأي و التعبير و الصحافة كقانون المطبوعات و قانون حماية المعلومات العسكرية والقانون الخاص بالمحافظة على الوثائق الرسمية للدولة و في فرنسا القانون المؤرخ في 1881/07/29 بشأن الصحافة.و في الجزائر قانون الاعلام رقم 05/12 المؤرخ في 12 جانفي 2012 و المعدل لقانون الاعلام 07/90.

[4] – ينظر د/عادل عمر: الجرائم الأخلاقية و أثرها على إنتشار الجريمة،http://news.elfagr.org

[5]– يقصد بالصحافة الالكترونية تلك الصحافة التي تستعين بالحاسبات في عمليات الانتاج و النشر الالكتروني و هي ذات طبيعة خاصة و يتم قراءتها من خلال جهاز الكمبيوتر و غالبا ما تكون متاحة عبر الإنترنت. ينظر لمزيد من التفاصيل ما هو مفهوم الصحافة الالكترونية؟، http:// tqanbs.com

لا يستدعي النشر عبر الإنترنت لزوم إتخاذ الإجراءات القانونية (اتخاذ إجراءات إيداع المصنف + يجب أن يكون ذلك النشر محاطا بضمانات النظام العام والآداب العامة) التي يتطلبها القانون لنشر صحيفة في العالم المادي. [1]

و يمكن تعريف جرائم الصحافة الإلكترونية بأنها:" هي تلك الأفعال غير المشروعة المتصلة بأعمال الصحافة والمرتكبة عبر شبكات الحاسب الآلي."

ثانيا: أركان جرائم الصحافة الالكترونية.

وجرائم الصحافة الإلكترونية يشترط لقيامها نفس أركان جرائم الصحافة التقليدية من ركن شرعي ومادي ومعنوي.

1/ أما بالنسبة للركن الشرعي فنجد أن القانون المؤرخ في: 1881/07/29 بشأن حرية الصحافة في فرنسا قد عاقب على البث الإجرامي العلني إذا تم عبر الإنترنت بأسلوب السمعي البصري Audiovisuelle، كما لو تم عبر أحد حلقات النقاش مثلا. والشأن نفسه بالنسبة لقانون العقوبات الجزائري الذي عاقب في المادة 144 مكر 1 على جريمة الإساءة لرئيس الجمهورية بعبارات تتضمن إهانة أو سب أو قذف عن طريق مجموعة من وسائل العلانية ومن بينها وسيلة إلكترونية أو معلوماتية... إلخ. ويمكن القول هنا أن هذه الوسيلة تنطبق أكثر على استخدامات الحواسيب المتصلة بالإنترنت.

2/ أما بخصوص الركن المادي، فهو ذاته بالنسبة لجرائم الصحافة و التي يقوم أساسا على العلانية.

3/ أما الركن المعنوي، فهو ذاته الواجب توفره في جرائم الصحافة التقليدية، أي يوجب لقيامها توافر القصد الجنائي لدى الجاني،أي أنها جرائم عمدية.

الفرع الثالث: موقف التشريعات المقارنة من جرائم الصحافة الالكترونية.

و سنوضح في هذا الفرع موقف التشريع الفرنسي بداية من هذه الجريمة ممثلا للتشريعات الغربية، ثم موقف التشريع الجزائري منها ثانيا ممثلا للتشريعات العربية. و ذلك كمايلي:

أولا: موقف التشريع الفرنسي من جرائم الصحافة الالكترونية.

تناول المشرع الفرنسي جرائم الصحافة الالكترونية من خلال قانون 1881/7/29 المتعلق بالصحافة، حيث جرم البث العلني إذا تم عبر الانترنت و ذلك في المادة 23 من هذا القانون[2] و التي عددت وسائل العلانية

---

[1] – د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 466.

[2] - Article 23 : « Seront punis comme complices d'une action qualifiée crime ou délit ceux qui, soit par des discours, cris ou menaces proférés dans des lieux ou réunions publics، soit par des écrits , imprimés, dessins,gravures,peintures, emblèmes,images ou tout autre support de l'écrit,de la parole ou de l'image vendus ou distribués,mis en vente ou exposés dans des lieux ou réunions publics,soit par des placards ou des affiches exposés au regard du public، soit par tout moyen de communication au public par voie électronique، auront directement provoqué l'auteur ou les auteurs à commettre ladite action، si la provocation a été suivie d'effet.

Cette disposition sera également applicable lorsque la provocation n'aura été suivie que d'une tentative de crime prévue par l'article 2 du code pénal».

التي تقوم بها هذه الجرائم و من بينها الوسائل المستحدثة الالكترونية و التي من بينها شبكة الانترنت.[1]

ثانيا: موقف التشريع الجزائري من جرائم الصحافة الالكترونية.

عالج المشرع الجزائري جرائم الصحافة الالكترونية في قانون الاعلام رقم 05/12 و كذا في قانون العقوبات الجزائري. فأما فيما يخص قانون الاعلام رقم 05/12[2] فقد خص المشرع الجزائري الباب التاسع للتطرق إلى المخالفات المرتكبة في اطار ممارسة النشاط الصحفي، اذ أخرج بعض الأفعال عن دائرة و مجال حرية الصحافة و أدخلها في دائرة التجريم و أفرد لها عقوبات مناسبة لها. و تتمثل هذه الأفعال في الإمتناع عن نشر الرد و التصحيح[3] و الأفعال المـخلة بالسالمـير الحسن للعدالة[4] و إعارة الإسم و إصدار دورية بدون

---

[1] –Voir Direction des affaires criminelles et des graces : Le traitement judiciaire de la cybercriminalité, guide méthodologique,Ministère de la justice,Trait d'union le Mans,mai 2002,p 15 et suite.

[2]– صدر قانون الاعلام 05/12 في 8 جانفي 2012 معدلا لقانون الاعلام رقم 07/90. وقد خص فيه الباب الخامس لوسائل الاعلام الالكترونية، فعرف في المادة 67 الصحافة الالكترونية بأنها:"كل خدمة اتصال مكتوب عبر الإنترنت موجهة للجمهور أو فئة منه، و ينشر بصفة مهنية من قبل شخص طبيعي أو معنوي يخضع للقانون الجزائري، و يتحكم في محتواها الافتتاحي". و عرف في المادة 68 نشاط الصحافة المكتوب عبر الإنترنت بأنه يتمثل في انتاج مضمون أصلي موجه إلى الصالح العام، و يجدد بصفة منتظمة. و يتكون من أخبار لها صلة بالأحداث و تكون موضوع معالجة ذات طابع صحفي. أما المادة 69 فعرفت خدمة السمعي البصري عبر الإنترنت بأنها كل خدمة اتصال سمعي بصري عبر الإنترنت (واب– تلفزيون، واب– اذاعة) موجهة للجمهور أو فئة منه، و تنتج و تبث بصفة مهنية من قبل شخص طبيعي أو معنوي يخضع للقانون الجزائري و يتحكم في محتواها الافتتاحي. و يقصد بأنشطة الاعلام وفقا للمادة 3 كل نشر أو بث لوقائع أحداث أو آراء أو أفكار أو معارف، عبر أية وسيلة مكتوبة أو مسموعة أو متلفزة أو الكترونية، تكون موجهة للجمهور او لفئة منه.

[3]– تنص المادة 100 من قانون الاعلام على:"يجب على المدير مسؤول النشرية أو مدير خدمة الاتصال السمعي البصري أو مدير وسيلة إعلام إلكترونية ، أن ينشر أو يبث مجانا كل تصحيح يبلغه إياه شخص طبيعي أو معنوي بشأن وقائع أو آراء ، تكون قد أوردتها وسيلة الإعلام المعنية بصورة غير صحيحة ".

كما تنص المادة 101على:" يحق لكل شخص يرى أنه تعرض لاتهامات كاذبة من شأنها المساس بشرفه أو سمعته أن يستعمل حقه في الرد ."

كما تنص المادة 108 على:"في حالة رفض الرد أو السكوت عن الطلب في ظرف الثمانية (8) أيام التي تلي استلامه ،يمكن الطالب اللجوء إلى المحكمة التي تنظر في القضايا الاستعجالية ، ويصدر أمر الاستعجال في غضون ثلاثة (3) أيام.

يمكن أن تأمر المحكمة إجباريا بنشر الرد."

[4]– تنص المادة 119 على:" يعاقب بغرامة من خمسون ألف دينار (50.000 دج) إلى مائة ألف دينار (100.000دج) كل من نشر أو بث بإحدى وسائل الإعلام ا لمنصوص عليها في هذا القانون العضوي ، أي خبر أو وثيقة تلحق ضررا بسر التحقيق الابتدائي في الجرائم ".

كما تنص المادة 120 على:" يعاقب بغرامة من مائة ألف دينار (100.000 دج) إلى مائتي ألف دينار (200.000دج) كل من نشر أو بث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي ،فحوى مناقشات الجهات القضائية التي تصدر الحكم ، إذا كانت جلساتها سرية ."

تصريح [1]

و كذا الجرائم الماسة بشرف و اعتبار الشخص[2]. و التي كلها يمكن أن تتم عبر الانترنت بسرعة و بدون عراقيل.

و يعاقب المشرع الجزائري على جرائم النشر الالكتروني في قانون العقوبات من خلال المواد 296 و 297 و 144مكرر و 144مكرر 1 و 2 و 146 من قانون العقوبات و التي سبق التفصيل فيها[3] مؤسسا ذلك العقاب على عنصر العلانية الذي يلعب دورا هاما في تحققها اذ لا تقوم الجريمة بدونها.

أما فيما يخص المسؤولية الجنائية عن جريمة الصحافة بصفة عامة و الصحافة الإلكترونية بصفة خاصة فقد نظمها المشرع الجزائري في الباب الثامن من قانون الاعلام رقم 05/12 في المادة 115[4] و كذا في قانون العقوبات في المادة144 مكرر 1 [5].

كما تنص المادة 122 على:" يعاقب بغرامة من خمسة وعشرين ألف دينار (25.000 دج)إلى مائة ألف دينار (100.000 دج) كل من نشر أو بث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي، صورا أو رسوما أو أية بيانات توضيحية أخرى تعيد تمثيل كل أو جزء من ظروف الجنايات أو الجنح المذكورة في المواد 255 و 256 و 257 و 258 و 259 و 260 و 261 و 262 و263 مكرر و 334 333و 335 و 336 و 337 و 338 و 339 و341 و 342 من قانون العقوبات

[1]– تنص المادة 118 على:" يعاقب بغرامة من مائة ألف دينار (100.000 دج) إلى خمسمائة ألف دينار (500.000دج) كل من يقوم عن قصد بإعارة اسمه إلى أي شخص طبيعي أو معنوي بغرض إنشاء نشرية، ولا سيما عن طريق اكتتاب سهم أو حصة في مؤسسة للنشر.

ويعاقب بنفس العقوبة المستفيد من عملية "إعارة الاسم".

يمكن أن تأمر المحكمة بوقف صدور النشرية ."

[2]–تنص المادة 123 على:" يعاقب بغرامة من خمسة وعشرين ألف دينار (25.000 دج) إلى مائة ألف دينار (100.000دج) كل من أهان بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي ، رؤساء الدول الأجنبية وأعضاء البعثات الدبلوماسية المعتمدين لدى حكومة الجمهورية الجزائرية الديمقراطية الشعبية."

[3]– ينظر ص 89 من هذه الرسالة.

[4]– تنص المادة 115 من قانون الاعلام على : "يتحمل المدير مسؤول النشرية أو مدير جهاز الصحافة الإلكترونية وكذا صاحب الكتابة أو الرسم مسؤولية كل كتابة أو رسم يتم نشرهما من طرف نشرية دورية أو صحافة إلكترونية.

ويتحمل مدير خدمة الاتصال السمعي البصري أو عبر الإنترنت وصاحب الخبر الذي تم بثه المسؤولية عن الخبر السمعي و/ أو البصري المبث من قبل خدمة الاتصال السمعي البصري أو عبر الإنترنت. "

[5]– تنص المادة 144 مكرر 1 من قانون العقوبات على:"عندما ترتكب الجريمة المنصوص عليها في المادة 144 مكرر بواسطة نشرية يومية أو أسبوعية أو شهرية أو غيرها، فإن المتابعة الجزائية تتخذ ضد مرتكب الاساءة و ضد المسؤولين عن النشرية و عن تحريرها و كذلك ضد النشرية نفسها.

ويستخلص من نص المادة 115 أن المشرع الجزائري قد اختار تأسيس المسؤولية في جرائم الصحافة الالكترونية على أساس فكرة التدرج أو التتابع و التي تقضي بأن يتابع كاتب المقال كفاعل أصلي و مدير النشر كشريك[1]. و بوجه عام يتحمل مسؤولية المخالفات المرتكبة، المكتوبة و المنطوقة،أو المصورة المديرون و الناشرون في أجهزة الاعلام، و الطابعون، أو الموزعون، أو الباثون، و البائعون و ملصقو الاعلانات الحائطية[2]. كما رتب المشرع الجزائري مسؤولية جنائية تتحملها النشرية بالرغم من عدم تمتعها بالشخصية المعنوية في المادة 144 مكرر 1 من قانون العقوبات .

المطلب الثاني:

جرائم العنف عبر الانترنت

قد لا يصدق البعض أن الانترنت قد تكون سببا لدفع مستخدميها الى العنف و التشاجر مع الآخرين أو تكون سببا في ارتكاب جرائم قتل، و على هذا ارتأينا تقسيم هذا المطلب الى الفرعين التاليين:

الفرع الأول: تعريف جرائم العنف.

الفرع الثاني:بعض النماذج الواقعية عن جرائم العنف التي تكون الانترنت سببا في وقوعها.

الفرع الأول:تعريف جرائم العنف.

بداية وقبل الخوض في تعريف لجرائم العنف يجب علينا أن نعرف العنف في حدذاته، اذ أن هناك نظريتان في محيط الفقه الجنائي حول مفهومه. الأولى و هي التقليدية و التي تشير الى القوة المادية بالتركيز على ممارسة القوة الجسدية، و الثانية تشير الى الضغط و الاكراه الارادي بالتركيز ليس على الوسيلة و انما على نتيجة استخدام وسائل معينة من شأنها اجبار ارادة الغير على اتيان سلوك معين.[3]

و في هذه الحالة، يعاقب مرتكبو الجريمة بالحبس من ثلاثة (3) أشهر إلى إثنى عشر (12) شهرا و بغرامة من 50000 دج إلى 250000 دج أو باحدى هاتين العقوبتين فقط و تعاقب النشرية بغرامة من 500000 دج إلى 2500000 دج.

تباشر النيابة العامة اجراءات المتابعة الجزائية تلقائيا.

في حالة العود، تضاعف عقوبات الحبس و الغرامة المنصوص عليها في هذه المادة."

[1]– لمزيد من التفاصيل ينظر درايلة عمري: تنظيم المسؤولية الجنائية عن جرائم الصحافة المكتوبة، رسالة ماجستير، كلية الحقوق بن عكنون، جامعة الجزائر،2004، ص 56. زيتوني نصيرة: المسؤولية الجنائية عن جرائم الاعلام، بحث لنيل شهادة الماجستير في القانون الجنائي و العلوم الجنائية، كلية الحقوق بن عكنون، الجزائر، 2002، ص51.

[2]– ينظر المادة 42 من قانون الاعلام رقم 07/90.

[3]– لمزيد من التفاصيل ينظر د/ كمال عبد الرشيد:جرائم العنف العائلي(رؤية أمنية)، دراسة مقدمة إلى ندوة جرائم العنف العائلي بتاريخ 1992/2/9، كلية الحقوق، جامعة المنصورة، ص23.

والواقع أن القانون الوضعي لا يأخذ العنف بمعنى الضغط الارادي، فالقتل والجرح هما النماذج الأزلية للعنف و لايعتد فيهما المشرع بارادة المجني عليه، و يجب استبعاد فكرة أن المشرع قد أخذ بمفهومين للعنف يختلفان باختلاف الجرائم. والحقيقة هي أنه اذا كان المشرع قد حمى الحرية المعنوية للأفراد من أفعال العنف، فهو لم يهدف الى حماية التكوين الارادي. و انما أراد حماية الحق في الحرية المعنوية و اذي يتمثل في الحق في عدم تحمل أي تدخل غير مشروع للغير في محيط المجال النفسي للفرد سواء فيما تعلق بوعيه وادراكه و فكره، و أخيرا سواء تعلق بتكوين ارادته. وهذا الحق الشخصي للفرد يعترف به المشرع لجميع الأفراد منذ اللحظة التي تثبت لهم صفة الانسان بغض النظر عن أحوالهم أو أهليتهم.وعليه يمكن تعريف العنف بأنه:"تجسيد الطاقة أو القوى المادية في الاضرار المادي بشخص آخر أو بشيء".[1]

أو هو:"الاستعمال المتعمد للقوة الفيزيائية أو القدرة، سواء بالتهديد أو الاستعمال المادي الحقيقي ضد الذات أو ضد شخص آخر أو ضد مجموعة أو مجتمع، بحيث يؤدي الى حدوث (أو رجحان حدوث) اصابة أو موت أو اصابة نفسية أو سوء النماء أو الحرمان".[2] أو هو:" قيام الانسان بسلوك عدواني يلحق ضررا ماديا(كالضرر الجسدي الذي يلحق بالانسان نتيجة للضرب أو الذي يلحق المكان نتيجة التدمير)

أو معنويا (أي الأثر النفسي الذي يلحق المتضررين نتيجة للاحتقار أو الاهانات) بمن يقع عليه هذا السلوك"[3].أو هو:"سلوك عدي موجه نحو هدف،سواء لفظي أو غير لفظي و يتضمن مواجهة الآخرين ماديا أو معنويا أو مصحوبا بتعبيرات تهديدية، وله أساس غريزي".[4]

و يعتبر القتل و الجرح و الضرب هم النماذج الأزلية للعنف.ويمكن تعريف جريمة القتل بأنها:"ازهاق روح الانسان عمدا"[5]. أو هو " اهدار حق المجني عليه في الحياة بازهاق روحه عن قصد، بما كانت الوسيلة وفعل الإعتداء على الحياة هو الذي يتمثل في سلوك الجاني باتيانفعل يؤدي بطبيعته الى الوفاة مقترنا بنية القتل و تحقق وفاة المجني عليه بالفعل"[6]. و بالتالي فجريمة القتل محلها الإعتداء على حق الانسان في الحياة. أما جريمة الضرب و الجرح فهما جريمتين محلها الإعتداء على حق الانسان في سلامة جسمه. ويقصد بالضرب:"كل ضغط مادي على الجسم، لا يؤدي الى احداث قطع فيه أو تمزيق لأنسجته، و لا يشترط أن يكون الضغط على جسم الانسان باستعمال أداة معينة، و انما قد يحدث ذلك بغير استعمال أداة لذلك يعتبر من قبيل الضرب توجيه صفعة باليد. و لا يتطلب القانون في الضرب المعاقب عليه أن يكون

---

[1]– د/كمال عبد الرشيد، المرجع السابق،ص25

[2]– هذا تعريف التقرير العالمي حول العنف و الصحة 2002 الصادر من منظمة الصحة العالمية.ينظر في ذلك تعريف العنف و الاساءة، http://www.nfsp.org.sa

[3]– مقال تعريف العنف ، http://Dr-alhassani.com

[4]– مقال تعريف العنف ، http://Mawdoo3.com

[5] – المادة 254 من قانون العقوبات الجزائري.

[6]– د/حسين فريجة: شرح قانون العقوبات الجزائري،جرائم الأشخاص – جرائم الأموال، ديوان المطبوعات الجامعية، الجزائر، 2006،ص 29.

على درجة معينة من الجسامة، فالعقاب على الضرب واجب مهما كان بسيطا و لو لم يترك أثر ظاهر في الجسم ".[1] أما الجرح فيقصد به:"كل مساس بجسم الانسان يؤدي الى احداث تمزيق يفض الى تحطيم الوحدة التي تجمع بين جزيئات هذه الأنسجة. و يختلف قطع الجسم عن تمزيق الأغشية، لأن قطع الجسم يكون سطحيا و يقتصر على مادة الجلد. بينما تمزيق الأنسجة يكون عميقا لكونه ينال الأنسجة التي يكسوها الجلد.[2] و يستوي أن يكون الجرح ظاهريا أو خارجيا، ويدخل في مفهوم الجرح كسر العظام لأن الكسر يحدث تمزقا للأنسجة التي تكسو العظام كما يشمل في مفهومه التسلخات و الرضوض و الخدوش والكدمات و العض".[3] ويحدث الجرح بأي شيء مادي يلامس الجسم و يصدمه كالسلاح الناري أو عصا أو أداة قاطعة كالسكين، وقد يستخدم حيوان في الجرح كالكلب أو يستعمل الجاني أعضاء جسمه في الجرح كالأسنان والأظافر و نحوها.و لا عبرة اذا كان الدم قد سال من الجرح خارج الجسم أو يتجمع تحت الجلد و يحدث زرقة قاتمة يظهر أثرها على الجلد.[4]

ونظرا للتطور التكنولوجي الذي شهده عالمنا، ولا سيما مع ظهور الانترنت و سرعة انتشارها و كثرة مستخدميها، فانه و الى جانب وجهها المشرق ومنه اختزالها للمسافات إلا أنها قد تكون سببا لدفع مستخدميها الى العنف و التشاجر مع الآخرين أو تكون سببا في ارتكاب جرائم قتل.و لهذا خصصنا النقطة الثانية لنسوق بعض الوقائع للتأكيد على امكانية وقوع العنف أو القتل بسبب الانترنت.

الفرع الثاني: بعض النماذج الواقعية عن جرائم العنف التي تكون الانترنت سببا في وقوعها.

و من النماذج الواقعية عن جرائم العنف التي تكون الإنترنت سببافي وقوعها، نذكر:

الواقعة الأولى: على إثر مشاداة بين شخصين في أحد مجموعات المناقشة التي انتهت بمشاجرة في ولاية نيوجرسي الأمريكية، حيث قام المتهم بتتبع عنوان المجني عليه من خلال الانترنت ثم اصطحب زملائه الى هذا العنوان و اعتدوا عليه بالضرب.[5]

الواقعة الثانية: و وقعت في فرنسا، حيث أدانت محكمة Nanterre بفرنسا أحد الجناة بالحبس لمدة شهرين مع الايقاف لأنه بعث برسالة تهديد بالقتل عن طريق البريد الالكتروني الى أحد رجال السياسة هناك.[6]

---

[1]– د/حسين فريجة، المرجع السابق، ص 141.

[2]– د/محمد صبحي نجم، المرجع السابق، ص49.

[3]– د/محمد صبحي نجم، نفس المرجع، نفس الموضع.

[4]– د/حسين فريجة،المرجع السابق،الموضع السابق

[5]– د/جميل عبد الباقي الصغير،(القانون الجنائي و الإنترنت) مرجع سابق، ص41.

[6]– د/جميل عبد الباقي الصغير، نفس المرجع ، نفس الموضع.

الواقعة الثالثة: و حدث فيها القتل العمد بطريق الانترنت، حين قام أحدهم بقتل زوجته و التي كانت موضوعة تحت جهاز Monitoring بأن دخل عن طريق الانترنت الى الشبكة الداخلية للمستشفى و غير في الوصفات الطبية الخاصة بها على نحو قاتل. و حين أعطيت الأدوية من الممرضة – التي عدت بمثابة وسيلة مادية لا قصد لديها – ماتت المريضة.[1]

الواقعة الرابعة:و هي واقعة ضرب مبرح كادت أن تؤدي الى جريمة قتل بين صديقين أحدهما يدعى عمر و الآخر سالم، حيث انتحل الأخير صفة فتاة عبر غرف الدردشة و تعرف على الأول و أقام معه علاقة عاطفية من خلال التحاور في غرف الدردشة، حتى وقع عمر في غرامها و تقدم لخطبتها، وهنا اكتشف تلاعب زميله به طيلة هذه الفترة. ومن هنا قام بالانتقام منه بضربه بعصا غليظة كسرت قدمه و أسالت دماء وجهه، و أراد أن يدهسه بسيارته ثم عدل عن ذلك تاركا اياه في مكان بالصحراء لا تمتد اليه يد الغوث و كاد أن يهلك.[2]

---

[1]– د/جميل عبد الباقي الصغير، نفس المرجع، نفس الموضع.

[2]– ينظر لمزيد من التفاصيل حول هذه الواقعة د/ عبد الفتاح بيومي حجازي،(الأحداث و الإنترنت) مرجع سابق،ص244 وما بعدها. و من الأمثلة الأخرى عن جرائم العنف عبر الإنترنت و التي أشار إليها د/ عبد الفتاح بيومي حجازي في نفس مؤلفه نذكر: جريمة قتل وقعت بسبب الدردشة في منتديات انترنت و كان المجني عليه و يدعى" برايان " قد قتله صديقه "داني" لمنافسته في حب "سارة" و كلهم التقوا و تصادقوا من خلال الدردشة في منتديات الحوار على الإنترنت. و تتلخص حيثياتها في:

تلقت الشرطة الأمريكية في احدى المدن بالولايات المتحدة الأمريكية عام 1998مكالمة هاتفية من تليفون عمومي تفيد العثور على جثة بين الأشجار باحدى مناطق المدينة، وتبين أن الجثة موضوعة في كيس، و أن المجني عليه قتل رميا بالرصاص.و التي اتضح أنها جثة الشابالمدعوببرايان.و عند انتقال رجال المحققين إلى مسكنه الذي يقع قريبا من المكان الذي عثر فيه على الجثة،وجدوا الكمبيوتر الخاص به لا زال يعمل، ومفتوحا على شبكة الإنترنت،حيث فتح المحققون صندوق الرسائل الالكترونية الواردة للمجني عليه"inbox" و تبين أن أحدث رسالة وصلت منذ الساعة الخامسة و عشر دقائق من اليوم السابق على الجريمة.وفحص المحققون الرسالة التي كان مضمونها " أعتذر عن مرافقتك، اذهب بمفردك و سوف أتحدث اليك لاحقا لأعرف ما دار بينكما....سارة".ولما اتجه المحققون نحو سجل تليفونات المجني عليه تبين وجود اسم " سارة جونسون"و رقم هاتفها الخاص،التي تم الاتصال بها و التي أفادت– بعد تحديد ميعاد معها للحصول على معلومات في التحقيق– أنها تعرف الضحية و قررت الالتقاء به منذ ثلاثة أيام كآخر لقاء بينهما. و أنها أرسلت رسالة عبر البريد الالكتروني تعتذر له عن مصاحبته لزيارة صديقها داني. و كانت المرة الأولى التي سيرون بعضهم فيها رغم أنهم يعرفون بعضهم جيدا منذ شهرين من خلال غرف الدردشة، حيث أبدى داني رغبته في معرفة برايان وجها لوجه و دعاه لمنزله، واستبعدت سارة أن يكون داني هو القاتل تأسيسا على أنه شخص ليس لديه سبب للقتل.و قد قام المحقق بالتحفظ على جهاز كمبيوتر المجني عليه و على سارة كشاهد في القضية. و حين التقى المحقق بالمدعو داني اعترف بأنه حدد ميعادا لصديقه برايان كي يزوره لكن تخلف عن الميعاد، وتم التحفظ على أجهزة حاسب آلي ثلاثة وجدت في منزله علها تفيد في كشف لغز الحقيقة.و عند البحث في تلك الأجهزة تبين وجود علاقة عاطفية ما بين سارة و داني، الأمر الذي دفع المحقق إلى الشك في أن الجريمة قد وقعت بسبب التنافس على حب سارة، و لذلك اتجه فكر المحقق إلى ذلك المجهول الذي اتصل بالشرطة وأبلغها بوجود جثة المجني عليه، ولا بد من وجود صلة بينه و بين الجاني.و عندها عاد المحقق إلى تحليل الرسائل

الالكترونية الخاصة بالمدعو داني و استعان بسارة لمعرفة أكثر الأصدقاء قربا منه، و توصل المحقق إلى شخص يدعى سام، حيث انهار أثناء التحقيق معه و اعترف بأن داني أبلغه أثناء حديثهما في غرفة دردشة خاصة privateعبر الإنترنت، أنه تورط بقتل برايان و طلب منه المساعدة في نقل الجثة، و اعترف كذلك أنه ذهب بالفعل إلى منزل داني وساعده في نقلهاو إلقائها في الأحراش، لكنه بعد ذلك لم يتمكن من الندم. لذلك توجه إلى الشارع، ومن أقرب تليفون عمومي اتصل بالشرطة و أبلغهم بوجود الجثة في المكان المحدد لذلك. وعندما قام المحقق بمواجهة المجرم داني بهذه الأدلة، لم يبق أمامه سوى الاعتراف. مبررا فعلته بأنه يحب سارة و لم يحب سواها رغم بلوغه سن الأربعين، و عندما اكتشف أن علاقة سارة بالمجني عليه اتجهت نحو منحنى عاطفي، قرر أن يضع حدا لهذه العلاقة و ذلك بدعوة كلا من سارة و برايان إلى منزله وأن يدفع سارة لاتخاذ موقف واضح من كليهما، و أنه كان يثق في حب سارة له لكن ما حدث أن سارة لم تحضر. الأمر الذي أصابه بالتوتر و طلب من برايان الابتعاد عن سارة لأنه يفكر بالزواج منها، الا أن برايان سخر منه و قال له أنه في عمر والدها و يفضل أن يبتعد هو عن طريقهما، و يبحث عن امرأة تناسب كهولته، الأمر الذي أفقده توازنه و دفعه إلى قتل برايان.وقد قضى بالسجن لمدة عشر سنوات ضد داني بتهمة القتل العمد،و قضى كذلك بالسجن لمدة سنة واحدة ضد صديقه سام و ذلك لمساعدته في اخفاء معالم الجريمة.

و في قضية ثانية و التي كانت العبارة التالية " في وجود انترنت يصبح بامكانك الحصول على ما تريد بطريقة سهلة مهما كان خطيرا و مهما كان غير مشروع". السبب في جريمة قتل ارتكبها المدعو مارك مع صديقته التي تعرف عليها خلال حفل تعارف أقامته الجامعة في بداية العام الدراسي، حيث أعجب بشخصيتها و حاول التقرب منها، لكنها صدته و أخبرته أنه صديق مميز لها، لكن لا تفكر في الوقت الحالي في أن ترتبط بعلاقة عاطفية. لكن مارك استغرب في ردها و انتظر علها تغير موقفها لكن انتظاره طال،و حينئذ استشار أحد أصدقاءه الذي طلب منه التسليم بالأمر الواقع و أن يترك لها حرية القرار. وعليه فكر أن يلجأ إلى أخصائي نفسي يسأله، لكنه أبعد الفكرة خجلا و ربما كبرياء.ثم فكر في التوجه إلى الإنترنت للاستشارة من خلال موقع يناقش فيه الشباب مشاكلهم، و يتلقون مساعدة من قبل آخرين مشاركين في هذه النقاشات، ومن بينهم من يدعى أنه أخصائي نفسي.و عندما طرح مارك مشكلته، أكد له أحد المشاركين أن صديقته تعاني من الخجل أو الخوف من اقامة علاقة مع شاب و تتذرع بالدراسة، و لذلك فهي تحتاج إلى علاج. حيث قرر له مشارك آخر أن لديه علاجا جربه مع صديقته كي يخلصها من عقدة الخوف، حيث أعطاها عقارا له مواصفات سحرية و أتبع مشورته حيث نبهه بصعوبة الحصول على هذا العقار.لكنه أعطاه عنوانا لموقع يمكن أن يساعده في الحصول عليه.و يعود ذا الموقع المنحرف إلى رجل في المعاش يدعى لوسيانو كان يعمل في مصنع أدوية، و بعد احالته للمعاش كان عليه أن يدبر سبل معيشته، لذلك فقد تذكر تركيبة عقار يخدر الأعصاب و يشل المقاومة تماما يسمى "عقار الاغتصاب"،و أنشأ موقعايبيع فيه المواد اللازمة لصنع هذا العقار بالاضافة إلى الوصفة التي تشرح طريقة التحضير. و قد تردد مارك في زيارة الموقع، ثم زاره بعد ذلك و استفسر عن العقار و تأثيره و أضراره و جاءته التأكيدات بأنه آمن بالطبع، خاصة اذا تم اتباع الوصفة المرافقة بدقة. و تردد مارك كذلك في الاقدام على هذه الخطوة مع صديقته، لكن بعد تفكير توجه إلى شبكة الإنترنت عله يحصل على مشورة تعينه على تنفيذ ما فكر فيه. و قد نصحه أحدهم بأن يجرب العقار مع صديقته و لن يخسر شيئا.و عمل مارك بالنصيحة حيث االشترى العقار من موقع ويب، و قام بتركيبه بنفسه ثم دسه خلسة في كأس العصير الذي قدمه لصديقته، لكن خسارته كانت فادحة اذ بعد ان شربت صديقته العصير فارقت الحياة خلال فترة قصيرة. و قد قضى بالسجن ضد مارك بتهمة القتل غير العمد.أما موقع الويب المنحرف فقد أغلقته السلطات المختصة و أحالت صاحبه إلى المحكمة للفصل في هذه الواقعة.

الفصل الثاني:

جرائم الإعتداء على حرمة الحياة الخاصة وجريمة المطاردة عبر الإنترنت.

شهدت الإنترنت نماء كبيرا نحو التوجه لجميع البيانات المتوفرة في العالم المادي، إذ أصبحت تتدفق فيها المعلومات والإتصالات عبر الحدود دون أي اعتبار للجغرافيا والسيادة لدرجة أنها صارت تعتبر أكبر آلة لجمع ومعالجة ونقل البيانات الشخصية وكذا نقل النشاط الإجتماعي والتجاري والسياسي والثقافي والإقتصادي من العالم المادي إلى العالم الإفتراضي.

وتجدر الإشارة إلى أن التصفح والتجول عبر الإنترنت يترك لدى المواقع المزارة كمية واسعة من المعلومات على الرغم من أن جزء من هذه الأخيرة لازم لإتاحة الربط بالإنترنت والتصفح أي أن مستخدم الإنترنت يترك أثارا ودلالات كثيرة تتصل به بشكل سجلات رقمية تتضمن الموقع الذي زاره والوقت الذي قضاه على الشبكة والأمور التي بحث عنها والمواد التي قام بتنزيلها والرسائل التي أرسلها والخدمات والبضائع التي قام بطلبها وشرائها. وهذا ما يهدد خصوصيته وحريته العامة. و بهذا أصبحت الإنترنت أكبر خطر يهدد الأفراد في خصوصيتهم وحرياتهم العامة، إذ صارت تستخدم من طرف مريضي الأنفس والتنصت على الأفراد ولالتقاط بياناتهم الشخصية وخاصة التجارية واستغلالها في غير موضعها أي في ارتكاب أفعال غير مشروعة.

هذا من جهة ومن جهة أخرى، فإنه وفي ذات الوقت استخدمت هذه الشبكة لابتزاز ومطاردة وإزعاج وتهديد مستخدمي الإنترنت من رجال ونساء وأطفال وبث أفكار معادية للأجانب من عنصرية وكراهية لتحقيق أهداف مختلفة ومتنوعة.

وعلى هذا خصصنا هذا الفصل لدراسة جريمتين من أخطر أنواع الإجرام غير المعلوماتي الواقع على الأشخاص وهما: جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت و جريمة المطاردة عبر الإنترنت.وذلك كما يلي:

المبحث الأول: جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

المبحث الثاني: جريمة المطاردة عبر الإنترنت

المبحث الأول:

جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

حظيت الحياة الخاصة للأفراد بحماية دستورية و قانونية و دولية[1] في مختلف دول العالم.

[1]– فقد كفل الدستور الجزائري تلك الحماية للحقوق و الحريات الفردية في الفصل الرابع من المواد 29 إلى 59. فمثلا نص في المادة 1/34 منه على:"تضمن الدولة عدم انتهاك حرمة الانسان"و في المادة 39 منه على:"لا يجوز انتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، ويحميها القانون سرية المرسلات و الاتصالات الخاصة بكل أشكالها مضمونة."وفي المادة

40 على:"تضمن الدولة عدم انتهاك حرمة المسكن". أما الدستور الأردني فكفلها في الفصل الثاني منه و التي تشمل الحقوق الطبيعية اللصيقة بشخص الانسان أو تلك المتعلقة بالحقوق والحريات الاقتصادية. فمثلا نص في المادة 7 منه على أن:"الحرية الشخصية مصونة"، و نص في المادة 18 منه على أن:"تعتبر جميع المراسلات البريدية والبرقية والخطابات الهاتفية سرية فلا تخضع للمراقبة أو التوقيف الا في الأحوال المعينة في القانون ".أما الدستور البحريني فخصها بالباب الثالث تحت المتعلق بالحقوق و الواجبات العامة على الحق في الحرية الشخصية، اذ تنص المادة 1/19 منه على:"(أ)- الحرية الشخصية مكفولة وفقا للقانون"، كما تنص المادة 25منه على:"للمساكن حرمة فلا يجوز دخولها أو تفتيشها بغير اذن أهلها الا استثناء في حالات الضرورة القصوى التي يعينها القانون، وبالكيفية المنصوص عليها فيه "، و تضيف المادة 26 منه أن:"حرية المراسلة البريدية والبرقية والهاتفية والالكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو افشاء سريتها الا في الضرورات التي يبينها القانون، ووفقا للاجراءات والضمانات المنصوص عليها فيه". وقد حرص الدستور المصري على النص على حرمة الحياة الخاصة للمواطنين، اذ قرر في المادة 45 منه على أن:"للمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الاتصالات الخاصة حرمتها و سريتها و هي محمية بالقانون ولا يجوز مصادرتها أو الاطلاع عليها أو رقابتها الا بأمر قضائي مسبب ولمدة محددة وفقا للقانون ". وتضيف المادة 57 منه أن:"كل اعتداء على الحرية الشخصية أو حرية الحياة الخاصة للمواطنين وغيرها من الحقوق والحريات العامة يعد جريمة لا تسقط الدعوى الجنائية والمدنية الناشئة عنها بالتقادم وتكفل تعويضا عادلا لمن وقع عليه الإعتداء". كما حظر التعديل الرابع للدستور الأمريكي الإعتداءات أو الشروع في الإعتداء على حرمة الحياة الخاصة للمواطن. أما على النطاق التشريعي فقد حرصت معظم التشريعات الوطنية بالتأكيد على ما ورد في دساتيرها و في التزاماتها الدولية.فعلى سبيل المثال نجد أن المشرع البحريني قد نص في قانون العقوبات البحريني في المادة 370على:" يعاقب بالحبس مدة لا تزيد على ستة أشهر و بالغرامة التي لا تتجاوز خمسين دنارا أو باحدى هاتين العقوبتين من نشر باحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد و لو كانت صحيحة اذا كان من شأن نشرها الاساءة اليهم".و إلى جانبه نجد المشرع الجزائري قد حمى تلك الحقوق و الحريات في قانون العقوبات في المادة 303 منه الناصة على أنه:" كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير و ذلك بسوء نية و في غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر إلى سنة و بغرامة من 25.000دج إلى 100.000دج أو باحدى هاتين العقوبتين فقط"، و يضيف في المادة 303 مكرر أن:"يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 50.000دج إلى 300.000دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت و ذلك:1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة،أو سرية بغير اذن صاحبها أو رضاه،2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص،أو سرية بغير اذن صاحبها أو رضاه.يعاقب على الشروع فيارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة. و يضع صفح الضحية حدا للمتابعة الجزائية".

أما على المستوى الدولي فقد حرص الجتمع الدولي على كفالة حرمة الحياة الخاصة للمواطن و ذلك بادراج حق المواطن في صيانة حياته الخاصة من أي عبث أو تقص غير مشروعين ضمن العديد من المواثيق الدولية و التي على رأسها الاعلان العالمي لحقوق الانسان الذي صدر عن الجمعية العامة للأمم المتحدة في ديسمبر 1948، و الذي نص في المادة 12 منه على أن:" حماية الفرد من التدخل التعسفي في حياته الخاصة أو مراسلاته و لكل شخص الحق في الحماية القانونيةضد هذا التدخل أو تلك الإعتداءات "

كما نصت العديد من الاتفاقات الدولية على حماية هذا الحق حيث نصت المادة 17 من الاتفاقية الدولية للحقوق المدنية والسياسية الصادرة عن الجمعية العامة للأمم المتحدة في سنة 1966 على:"عدم جواز التدخل بشكل تعسفي و غير قانوني في حياة الأفراد الخاصة...."

وتعتبر فكرة الحياة الخاصة من الأفكار الصعبة التعريف، إذ عانى الفقه والقضاء كثيرا في محاولة إيجاد مدلول محدد لها. الأمر الذي حدا بالبعض إلى القول بأن مضمون هذا الحق نسبي أكثر منه مطلق.[1]
هذا من جهة ومن جهة أخرى، يصنف الحق في الحياة الخاصة ضمن الحقوق الشخصية[2] التي تثبت لكل شخص باعتباره إنسان وتمكنه من الاستفراد بأسراره دون أن يطلع عليها غيره إلا إذا كانت برضاه.

كما نصت المادة 12 من مشروع ميثاق حقوق الانسان و الشعوب في الوطن العربي لسنة 1986 على أن:"للحياة الخاصة لكل انسان حرمة و تشتمل هذه الحياة الخاصة على خصوصيات الأسرة و حرمة المسكن و سرية المراسلات و غيرها من سبل المخابرة الخاصة و لايجوز المساس بها الا في حدود القانون." لمزيد من التفاصيل ينظر عفيفي كامل عفيفي، المرجع السابق،ص 264– 265. و كذا محمد أمين أحمد الشوابكة، المرجع السابق، ص 59. و سامح محمد عبد الحكم، المرجع السابق،ص38.

[1]– يرجع الفقيه Waks سبب صعوبة الاتفاق على تعريف واحد للحق في الحياة الخاصة إلى اتساعه و بأنه صعب المأخذ، و يمكن رد مدلوله إلى ثلاث اتجاهات:

1/ الاتجاه المعياري: و يحاول أنصاره تعريف ذلك الحق استنادا على معيار معين دون التطرق إلى بيان عناصره و تحيد حالاته. ومن أنصاره الفقيه NERSON وA FAWSTON و C DENNIS و FERRER وNIZA و الفقيه الأمريكي COOLEY و كذا تعريف مؤتمر استكهولم لرجال القانون المنعقد في عام 1967. فهم يأخذون بفكرة الخلوة و الحرية كمعيار لتحديد مفهوم هذا الحق.

2/ الاتجاه التعدادي: و يحدد أنصاره هذا الحق عن طريق وضع قوائم بتعداد حالاته و تحديد العناصر المكونة له. و من أنصاره الفقيه MARTIN وMALHERBE وLINDON وROBERT .

ج/الاتجاه المختلط:_و هو يجمع بين الاتجاهين السابقين، اذ يعرف أنصاره الحق في الحياة استنادا إلى معيار معين ثم يعددون الأمور و الحالات التي تدخل في نطاقه و تعتبر من عناصره. ومن أنصاره الفقيه WASTON. و ازاء صعوبة وضع تعريف جامع مانع للحق في الحياة الخاصة، فضل البعض ضرورة ترك هذا الأمر ليتولاه القضاء على أن يتم تحديده وفقا لأسس معينة مستمدة من التقاليد و الثقافة و القيم الدينية السائدة و النظام السياسي لكل مجتمع بما يكفل الانسان أن تحترم ذاته مما يضمن له الهدوء و السكينة و الأمن بالنأي بالآخرين ن التدخل في خصوصياته.

و تجدر الاشارة إلى أن التشريعات التي تضمنت النص على ذلك الحق لم تقم في واقع الامر بوضع تعريف له لكون أن فكرة الحياة الخاصة هي من الأفكار المرنة التي ليس لها حدود ثابتةأو مستقرة. فهي لا تختلف باختلاف الأقطار و الأزمان فحسب بل باختلاف الأفراد أنفسهم و بحسب أعمارهم و شخصياتهم و ما يستدلونه من حرمة على خصوصياتهم. أضف إلى ذلك أن تقدير كل مجتمع للقيم التي تتعارض مع حماية هذا الحق. لمزيد من التفاصيل ينظر د/ عفيفي كامل عفيفي، المرجع السابق، ص 244 و ما بعدها، و د/حسين الغافري و محمد الألفي، المرجع السابق،ص 64. و د / هشام محمد فريد رستم، (قانون العقوبات ومخاطر تقنية المعلومات) مرجع سابق، ص 175.

[2]– لقد اختلف الفقه حول الطبيعة القانونية لهذا الحق فهناك من اعتبره من حقوق الملكية على أساس أن الشخص يملك جسده الشكل الذي يعطيه مطلق الحرية بالتصرف فيه أو استغلاله أو استعماله (وهي المكنات الثلاث التي يخولها حق الملكية). و هناك من يصنفه ضمن الحقوق اللصيقة بالشخصية، لانه يعتبر من خصائص الشخصية الانسانية. و هناك من ادرجه ضمن الحقوق المعنوية، بحيث يمكن تشبيهه بحق الملكية الصناعية.ينظر في ذلك د/ ممدوح خليل بحر: حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر و التوزيع، الأردن، 1996، ص 269 وما بعدها.

ولكنه نظرا للتطور التكنولوجي الذي يشهد عالمنا أصبحت تلك الحماية غير كافية، إذ باتت النصوص التقليدية التي تكفلها عاجزة عن مواجهة ذلك التطور، لا سيما بعد ظهور وانتشار استخدام الحواسيب وشبكة الإنترنت والتي أصبحت عبرها خصوصيات الأفراد وأسرارهم ومعلوماتهم الخاصة تنتهك وتغتصب عن طريق البيانات المجموعة في بنوك المعلومات[1]. وتعد صورة استخدام تلك البنوك لاستغلال البيانات المخزنة فيها لغاية غير التي تم تجميعها من أجلها من أبرز مخاطر بنوك المعلومات على الحياة الخاصة. ومثال ذلك ما حصل في ألمانيا عام 1984 لما قامت المحكمة بتوقيف الإحصاء بعد أن ثبت لها أن وزارة الداخلية استطاعت الحصول على عناوين مجموعة إرهابية متطرفة من خلال استمارة الإحصاء. الأمر الذي اعتبرته تلك الأخيرة إساءة لاستخدام البيانات التي جمعت من أجل غاية واحدة لا غير وهي الإحصاء الرسمي. وبالتالي يعد ذلك انتهاكا للحياة الخاصة وسرية البيانات[2].

هذا من جهة ومن جهة أخرى، فإن بنوك المعلومات الخاصة تشكل خطرا آخر على سلامة الحياة الخاصة، لكونها تضم كما هائلا وبالغ الأهمية من البيانات الخاصة بالأعضاء المشتركين في تلك البنوك وشركات التأمين والمؤسسات المالية وكذا عملائها. وهذا ما يمثل هدفا كافيا يمكن من خلاله انتهاك حرمة الحياة الخاصة. وبالتالي يمكن عن طريق إنشاء هذه البنوك أن تقوم الدولة بجمع ما تريد جمعه من معلومات وبيانات خاصة بالأفراد قد تتضمن كل كبيرة وصغيرة عنهم كما حدث في كل من فنلندا والدانمارك.[3] ولهذا وجب على الدول استحداث دساتيرها،وتشريعاتها لحماية تلك الحياة في مواجهة أخطار البنوك. والسؤال الجوهري المطروح هنا هو: كيف تهدد الإنترنت الحياة الخاصة للأفراد؟ ولماذا تعتبر وسيلة لانتهاك حرمة تلك الحياة؟.

---

[1]– ويقصد ببنوك المعلومات (Les banques des données – data banks) الجهات التي تقوم بتجميع المعلومات المتصلة بموضوع معين بقصد معالجتها آليا تمهيدا لاستغلالها. أو هي تكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين ومعالجتها بواسطة أجهزة الحاسبات الالكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة وهي نوعان: بنوك معلومات عامة: وهي التي تفوز فيها الدولة أو إحدى مؤسساتها بتجميع المعلومات المتصلة بموضوع معين– وبنوك معلومات خاصة: وهي التي تجمع فيها البنوك وشركات التأمين والمؤسسات المالية البيانات الخاصة بأعضائها وعملائها. وتحتوي مثل هذه البنوك على معلومات مالية أو وطنية أو صحية أو أمنية والمستمدة من الأخبار والأنباء ومن البيانات الاسمية، ليتم تسجيلها فيما بعد في أسطوانات أو شرائط، ثم بموضوع معين– وبنوك معلومات خاصة: وهي التي تجمع فيها البنوك وشركات التأمين والمؤسسات المالية البيانات الخاصة بأعضائها وعملائها. وتحتوي مثل هذه البنوك على معلومات مالية أو وطنية أو صحية أو أمنية والمستمدة من الأخبار والأنباء ومن البيانات الاسمية، ليتم تسجيلها فيما بعد في أسطوانات أو شرائط، ثم إدخالها في الحاسب الآلي وتخزينها.ينظر على التوالي:. د/أسامة عبد الله قايد: الحماية الجنائية للحياة الخاصة و بنوك المعلومات، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1994، ص 48. محمود أحمد عبابنة، المرجع السابق،ص 70.

– Définition de « banque de données »، http://dictionnaire-sensageant.com

[2]– د/أسامة عبد الله قايد، المرجع السابق، ص 53.

[3]– د/عفيفي كامل عفيفي، المرجع السابق، ص 250.

وتمت الاجابة على هذا الاشكال وفق المطلبين التاليين:

المطلب الأول: ماهية جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت .

المطلب الثاني: أنواع جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت و التكييف القانوني لها.

المطلب الأول:

ماهية جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

و تناولنا تحت هذا المطلب تعريف جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت في الفرع الأول، ثم تطرقنا إلى طرق الإعتداء على الحياة الخاصة عبر الإنترنت في الفرع الثاني. و ذلك كما يلي:

الفرع الأول:تعريف جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت .

الفرع الثاني: طرق الإعتداء على الحياة الخاصة عبر الانترنت.

الفرع الأول: تعريف جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت .

لقد أصبح التطور التكنولوجي الذي يشهده عصر ثورة المعلومات يهدد الأفراد في حياتهم الخاصة، لاسيما بعد شيوع استخدام الإنترنت والحواسيب في شتى مجالات الحياة، حيث تم اعتبارهما وسيلة لتخزين بيانات شخصية مختلفة ومتعددة – كالبيانات الخاصة بالحالة الصحية والمالية والمهنية والعائلية– تتعلق بالحق في الحياة الخاصة للمرء وتسمى بالبيانات الاسمية[1] وذلك على ما يصطلح عليه بنوك أو مراكز المعلومات. مما يشكل تهديدا وانتهاكا غير مسبق لخصوصيتهم نظرا لسوء استخدامها أو استخدامها لغير الغرض الذي جمعت من أجله من قبل الجهات المختصة بذلك. فتتحمل بذلك حياة الفرد إلى جحيم بعدما كانت هذه المعلومات والبيانات في ظل الطرق التقليدية في مأمن لا يطلع عليها إلا صاحب الشأن نفسه بإتباع إجراءات معينة، لتصبح كالكتاب المفتوح والمقروء من قبل من كان لديه الإمكانية التقنية والفنية الكافية للوصول إليها سواء أكان تابعا لهذه الجهات أو كان فردا غير مرخص له أساسا بالإطلاع عليها. وهذا ما أكده بعض الخبراء من أن هناك إمكانية في متابعة ومراقبة المواقع التي قد يزورها الشخص على شبكة الإنترنت. فاستخدام الإنترنت هو في الحقيقة ظاهر بوضوح أمام من يريد مراقبته ولا يمكنه التنكر. والمثال الواقعي لذلك هو ما نشر مؤخرا من أنه على مدار عام داوم شخص يدعى كريستوفر كانترس على الإشتراك في المناقشات الدائرة في مجموعة المناقشة المنتشرة على الإنترنت. حيث أضاف آراءه إلى الأعداد الكبيرة من الآراء الموجودة في هذه المجموعات. إلى حين اختياره من قبل صحيفة "مينيا بولس ستار تريبيون" بصورة عشوائية لجمع المعلومات الخاصة به من الشبكة بناء على ما نشره بنفسه، مستخدمة

---

[1]– و يقصد بالبيانات الاسمية:" البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء، كالبيانات الخاصة بحالته الصحية و المالية و الوظيفية و المهنية و العائلية،عندما تكون هذه البيانات محلا للمعالجة الآلية".محمد أمين أحمد الشوابكة، المرجع السابق، ص 63.

في ذلك موقعا على الويب يطلق عليه Deja News والذي يتيح البحث في مجموعات الأخبار الموجودة على الإنترنت بواسطة اسم شخص. وتعتبر المعلومات التي تمكنت الصحيفة من جمعها ذات أهمية كبيرة ولا يستهان بها عن كريستوفر حيث شملت كل ما هو شخصي من مكان مولده والمدرسة التي ذهب إليها والجامعة التي درس بها ومكان عمله الحالي والسابق والمسرح الذي يذهب إليه والمطاعم التي يرتادها وحبه لأجهزة الماكنتوش وكراهيته لبيل جيتس وولاية أنديانا وقضاءه إجازته بباريس وروما عام 1995. وعلى هذا يعد ما قامت به الصحيفة ولو أنه تم بموافقة كريستوفر مثلا حيا لكيفية جمع البيانات الشخصية من الشبكة، بحيث يمكن لأي شخص جمع وفهرسة كل كلمة في مجموعات الأخبار ومعرفة المواقع التي تزورها على موقع الويب التابع لشبكة الإنترنت.بل الأدهى والأمر من ذلك يستطيع أن يطلع على بريدك الإلكتروني ويجري عمليات التسويق ويتعامل مع البنوك باسمك من خلال الإنترنت.[1]

وعلى هذا فإن شبكة الإنترنت قد سهلت الكثير من الأمور الحياتية بتجاوزها لعديد من العقبات التي كانت تعتبر من ضروب المستحيل، إذ أصبح بإمكان أي شخص الإبحار عبرها والولوج إلى أي موقع يرغب فيه والحصول على ما يريده من معلومات وبيانات خاصة سواء أكانت تتعلق بالأفراد أو بمؤسسات وذلك بطرق غير مشروعة دون الحاجة لقطع المسافات أو تضييع الأوقات وإهدار الأموال. الأمر الذي جعل الحياة الخاصة لهؤلاء الأشخاص في محك، تتعرض لجملة من الانتهاكات لم يعرف لها مثيل لا سيما وأن تلك الشبكة لا تتوفر فيها السرية الكاملة واللازمة للإحاطة بتلك البيانات الخاصة، إذ كل اتصال بالإنترنت يمكن أن يترك أثرا ما، حتى ولو لم يدرك مستخدم الشبكة ذلك. فأصبح بإمكان بعض الأشخاص الولوج إلى أنظمة وأجهزة تخص آخرين، والحصول على معلومات وعن أسرار حياتهم أو أية معلومات أخرى تخصهم ويرغب صاحبها في إضفاء طابع السرية عليها. و يمكن تعريف الخصوصية المعلوماتية بأنها " حق الافراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للاخرين" أو بأنها " قدرة الافراد على التحكم بدورة المعلومات التي تتعلق بهم"[2].

وعليه يمكن تعريف جريمة الإعتداء على الخصوصية عبر الإنترنت بأنها:"كل اعتداء على البيانات الاسمية عبر الانترنت، و ذلك عن طريق التمركز في موقع معين داخل شبكة الانترنت و العمل على تسجيل و حفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية." [3]

الفرع الثاني: طرق الإعتداء على الحياة الخاصة عبر الانترنت:

تعرف جريمة الإعتداء على الحياة الخاصة عبر الانترنت بأنها كل اعتداء على البيانات الاسمية عبر الانترنت، و ذلك عن طريق التمركز في موقع معين داخل شبكة الانترنت و العمل على تسجيل و حفظ

---

[1]– د/عفيفي كامل عفيفي، المرجع السابق، ص 253

[2]– لمزيد من التفاصيل ينظر د/ حسين بن سعيد الغافري: الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الإلكترونية العماني، ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت القاهرة 2-4 يونيو 2008 ، http:// www.shaimaaatalla.com

[3]– وليد الزيدي، المرجع السابق، ص 55

البيانات المتبادلة فيما بين الأنظمة المعلوماتية، أي عن طريق استغلالهم النقاط الضعيفة في منظومة الأمن باستخدامهم لمبرمجات الحواسيب، والتي هي عبارة عن جسيمات تنصت على الويب تمثل بنقاط على الشاشة تعمل كأجهزة إرسال متناهية صغيرة. وبالتالي يسهل انتهاكهم وإطلاعهم على البيانات الموجودة على شبكة ومن دون أن تصدهم أية صعوبات أو إعاقات[1].

ويرى "شيلر" أن هذا الأسلوب يعد واحدا من أخطر التهديدات لأمن الشبكات الحديثة لسهولة استخدامه في **استراق السمع والتنصت أو الرقابة الالكترونية**[2]،أي في التجسس والاستماع سرا وخلصة لمراسلات الأفراد ومكامن خصوصياتهم وذلك دون رضاهم، ولا أدل على ذلك من الشبكة المعروفة carnivore والتي استخدمت كمشروع تتنصت فيه الحكومة الأمريكية على مزودي خدمة الإنترنت لمراقبة وسائل البريد الالكتروني والتراسل الفوري لمشتركي الإنترنت[3]. ويقصد بالتصنت: "الاستماع سرا بوسيلة أيا كانت نوعها إلى كلام له صفة الخصوصية صادر عن شخص ما أو متبادل بين شخصين أو أكثر دون رضاء من هؤلاء"[4].

هذا من جهة ومن جهة أخرى، يعتبر **الدخول غير المرخص به للمعلومات** أو الدخول غير المشروع أو الاختراق والإطلاع عليها دون إذن أو ترخيص صورة من صور انتهاك لحقوق الإنسان في خصوصيته عبر الإنترنت ويتم ذلك عن طريق الحصول على كلمة السر أو كلمة المرور (mot de passe) أو (passward) للملفات المخزنة. وبالتالي التسلل إلى الشبكة كما لو كان ذلك الشخص هو المستخدم الحقيقي، واستغلاله لتلك المعلومات الخاصة في غير محلها أو الاطلاع عليها بدون إذن من صاحبها. فمثلا يمكن اعتراض الرسائل المنقولة بواسطة البريد الالكتروني وقراءة فحواها الذي يفترض أنه سري قبل وصولها للمرسل إليه،أو يمكن الدخول في الموقع بدون ترخيص بقصد الحصول على بيانات أو معلومات أمنية تمس الأمن والاقتصاد القومي للبلاد أو إلغاؤها. ويعرف الدخول غير المشروع بأنه:"الولوج غير المصرح به وبشكل غير مشروع إلى نظام معالجة آلية للبيانات باستخدام الحاسوب".[5] أو:"هو دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع الكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"[6]. أو:"هو دخول شخص عادي أو موظفا عاما متعمدا موقعا أو نظام معلومات أو شبكة الكترونية دون أن يكون له مصرحا له بذلك ويقوم بالاطلاع على البيانات أو نسخها أو إلغاءها أو حذفها أو تدميرها أو إفشاءها أو تغييرها بشكل يحدث ضررا لصاحب النظام".

---

[1]– وليد الزيدي، المرجع السابق، ص 56.

[2]– د/عفيفي كامل عفيفي، المرجع السابق، ص 254.

[3]– محمد أمين أحمد الشوابكة، المرجع السابق، ص 66.

[4]– محسن بن محسن بن باعث الرويلي، المرجع السابق، ص 98.

[5]– د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 331.

[6]– المادة 7/1 من نظام مكافحة الجريمة المعلوماتية السعودي.

وتجدر الإشارة إلى أنه إذا كان هذا الشخص الذي دخل الموقع أو النظام "موظفا عاما" فهو يدخله دون تفويض من الجهة التي يعمل بها لذلك أو يقوم بتسهيل ذلك الدخول للغير[1].

كما يعد **تسجيل المحادثات الخاصة** التي تدور في منتديات المناقشة وفي مجموعات الأخبار ضربا آخر من الجرائم الماسة بالحياة الخاصة عبر الإنترنت. فمثلا يقوم موقع www.dejanews.com بنسخ إجمالي لكامل منتديات المناقشة ويحفظه داخل ملقمات خاصة.[2]

هذا من جهة ومن جهة أخرى، فإن **التقاط ونقل الصور دون موافقة صاحبها** يعد مظهرا خطيرا وآخر من مظاهر التعدي على خصوصية الإنسان، كأن يكون ذلك عن طريق الكاميرا الموصولة بالإنترنت التي يستخدمها العديد من مستخدمي هذه الشبكة و بخاصة الشباب منهم و يطلقون عليها لفظ "الكام" اختصارا للكاميرا، و هي توضع على جهاز الكمبيوتر و تنقل الصورة و الصوت في ذات الوقت للطرف الآخر، ويمكن بالطبع للطرف الآخر تسجيل الصورة و كذلك الصوت و من ثم نقله على دعامة (ديسك) أو قرص ممغنط و الاحتفاظ به أو اذاعته و نشره عبر الانترنت نكاية بصاحبه و لافشاء محتوى أسراره و أدق خصوصياته.هذا بالنسبة للالتقاط و النقل عبر شبكة الانترنت من طرف لآخر. أما الجديد أيضا فهو الالتقاط و النقل و لكن عبر الهاتف المحمول و سواء أكان الالتقاط لمجرد الصورة فحسب أم مقطع لمادة فيلمية، و في الحالتين بعد أن يتم الالتقاط يمكن النقل عن طريق استخدام تقنية البلوتوث(Blue tooth) أو خاصية الوسائط المتعددة سواء لهاتف محمول أو أكثر من هاتف محمول يحتوي على ذات الخاصية. وكذلك النقل عبر تحميل تلك الصور أو المواد على جهاز الكمبيوتر عن طريق ذات الخاصية، و التي أصبحت متوافرة الآن في أجهزة الكمبيوتر و من ثم بات من الممكن التقاط أي صورة أو لقطة أو مادة فيلمية عن طريق كاميرا الهاتف المحمول ثم نقلها الى الكمبيوتر عن طريق خاصية البلوتوث المتوافرة حاليا بأجهزة الكمبيوتر. و بالتالي امكانية ارسالها عن طريق البريد الالكتروني أو نشرها و اذاعتها عبر شبكة الانترنت أو تحميلها على أقراص ممغنطة أو دعامات لعرضها لمن يرغب في رؤيتها.

---

[1]– الفصل الثاني من قانون جرائم المعلوماتية السوداني و المعنون بجرائم نظم ووسائط و شبكات المعلومات المقصود بها الجرائم المتعلقة بانتهاك سرية البيانات و المعلومات حفاظا عليها من الإعتداء حيث أنها تمثل قيمة من حيث محتواها ويمكن أن يشكل اختراقها ضررا كبيرا لصاحب النظام. ومن بين الإعتداءات التي تندرج تحتها:

1– دخول المواقع و الأنظمة للغير.

2– دخول المواقع و الأنظمة من موظف عام.

3– التنصت أو التقاط أو اعتراض الرسائل.

4– دخول المواقع عمدا للحصول على بيانات أو معلومات أمنية.

5– ايقاف أو تعطيل أو اتلاف البرامج أو البيانات أو المعلومات.

6– اعاقة أو تشويش او تعطيل الوصول للخدمة. ينظر محمد محمود:الجريمة الإلكترونية و جرائم المعلوماتية في القانون السوداني، ، http://www.smu.edu

[2]– د/حسين الغافري و محمد الألفي، المرجع السابق، ص 71، هامش رقم 84.

و تجدر الاشارة هنا الى أنه يشترط أن يتم ذلك في مكان خاص. و المقصود بالمكان الخاص هنا المكان الذي لا يمكن دخوله دون اذن الشخص الذي يشغله سواء أكان ذلك بطريقة دائمة أم مؤقتة.[1]

كما أوجدت شبكة الإنترنت برامج رصد متطورة تسمى بالكعكات والتي هي: "عبارة عن ملفات صغيرة يخزنها موقع الإنترنت في الذاكرة الرئيسية لجهاز حاسوب المستخدم لاستخدامات كثيرا ما تكون مفيدة، مثل أخذ المعلومات الخاصة بالمتصفح–كضغط كلمة السر الخاصة به– وعدد المرات التي زار فيها الموقع". وبذلك أصبحت تلك الشبكة من أنجح الوسائل في تتبع الأشخاص وفي كشف أسرار حياتهم كما استخدمت لبناء الدراسات المتعلقة بالتسويق وملاحقة الزبائن ومضايقتهم.[2]

أما الوسيلة الأخطر في تلك المضايقات للخصوصية عبر الإنترنت تتمثل في **برمجيات التتبع / الشم** وهي:" وسيلة تتبع لجمع أكثر قدر ممكن من المعلومات السرية والخاصة عن طريق ما يعرف بأنظمة جمع المعلومات".[3]

ونخلص مما سبق أن هناك تحديات جديدة أوجدتها شبكة الإنترنت في مواجهة خطط حماية الخصوصية أو الحياة الخاصة. فهي زادت من كمية البيانات المجمعة و المعالجة و المنشأة، و أتاحت عولمة المعلومات و الاتصالات.[4]

المطلب الثاني:

أنواع جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت و التكييف القانوني لها.

و على غرار المطلب الأول فقد قسمنا هذا المطلب إلى فرعين، تناولنا في الأول منه أنواع جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت. أما الثاني فخصصناه لتبيان موقف التشريعات المقارنة من هذه الجريمة. و ذلك كالتالي:

الفرع الأول: أنواع جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

الفرع الثاني: موقف التشريعات المقارنة من جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

---

[1]– سامح محمد عبد الحكم، المرجع السابق، ص 44.

[2]– منير محمد الجنبيهي و ممدوح محمد الجنبيهي: أمن المعلومات الالكترونية، دار الفكر الجامعي، الإسكندرية، 2005،ص 108. و ينظر كذلك وليد الزيدي، المرجع السابق، ص 57 و د/أيمن عبد الله فكري، المرجع السابق، ص 657 و ما بعدها.

[3]– يونس عرب: المخاطر التي تهدد الخصوصية و خصوصية المعلومات في العصر الرقمي، www.arablaw.com http://

[4]– لمزيد من التفاصيل ينظر د/أيمن عبد الله فكري، المرجع السابق، ص 653 و ما بعدها.

الفرع الأول: أنواع جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

وتجدر الإشارة هنا أنه لا يوجد تصنيف محدد أو دقيق يحدد كيفية انتهاك حرمة تلك الحياة بواسطة شبكة الإنترنت، ولكنه يمكن أن نورد الأساليب الإجرامية الشائعة في التعدي على الخصوصية ومنها:

أولا: استعمال بيانات شخصية غير حقيقية:

و هنا نميز بين حالتين:

1/ المحو أو التلاعب في بيانات شخصية بمعرفة أفراد غير مصرح لهم بالاطلاع أواستعمال هذه البيانات.

2/ استعمال بيانات شخصية غير حقيقية بواسطة المسموح لهم قانونا.

فبخصوص الحالة الأولى فيهدف هذا التلاعب أو المحو للبيانات المختزنة آليا الى تحقيق غاية مادية للجناة. ومن الأمثلة الواقعية عن هذا الأسلوب، حالة شركة TR.W.COMPANY- CREDIT DATA الأمريكية؛ اذ تختص هذه الأخيرة بتزويد عملائها من البنوك و المتاجر الكبرى و غيرهم بالمعلومات الكافية عن المركز الائتماني لدى شخص تريد هذه الجهات التعامل معه، الأمر الذي دفع بستة عاملين في هذه الشركة الى الاتصال بالأفراد والمؤسسات ذوي المركز الائتماني السيء حتى يحصلوا على مقابل مالي لهم مقابل تعديل البيانات الخاصة بهم. وبذلك تورط الكثير من عملاء هذه الشركة في تعاملات تجارية ومالية مع أفراد لا يتمتعون بمركز ائتماني جيد. [1]

أما الحالة الثانية يكون الاهمال فيها هو السبب وراء عملية جمع أو معالجة أو نشر البيانات الشخصية الغير صحيحة بواسطة المسموح لهم قانونا مع امكانية تصور حدوث ذلك بصورة عمدية[2].

ثانيا: جمع أو معالجة بيانات حقيقية بدون ترخيص.

حيث تقوم جهات أو أشخاص ليس لهم الحق في القيام بتجميع أو تخزين بيانات حقيقية تخص أفراد، وذلك باستخدام أساليب تتسم بعدم المشروعية كالتقاط الارتجاجات التي تحدثها الأصووات في الجدران الاسمنتية للحجرات ومعالجتها بحاسوب مزود ببرنامج خاص لترجمتها الى كلمات وعبارات ومراقبة واعتراض وتفريغ الرسائل المتبادلة عن طريق البريد الالكتروني وتوصيل أسلاك بطريقة خفية الى الحاسب الذي تخزن بداخله البيانات، والتوصل بطريق غير مشروع الى ملفات تخص آخرين[3]. و من الأمثلة الواقعية عن هذا الأسلوب قيام مراهق ألماني لا يتجاوز الستة عشر سنة بنصب مصيدة بيانات نجح من خلالها في التقاط البيانات الشخصية بمستعملي نظام الفيديوتكس، بالاضافة الى قيامه بعمليات تلاعب و اتلاف لبيانات بعض المستخدمين، وتغيير كلمات السر التي يستخدمها بعضهم للتعامل مع النظام.[4]

---

[1]– د/عفيفي كامل عفيفي، المرجع السابق، ص 256.

[2]– لمزيد من التفاصيل ينظر د/ هشام محمد فريد رستم، (قانون العقوبات و مخاطر تقنية المعلومات) مرجع سابق، ص189–191.

[3]– لمزيد من التفاصيل ينظر د/أسامة عبد الله قايد، المرجع السابق، ص 90.

[4]– لمزيد من التفاصيل ينظر د/ هشام محمد فريد رستم،(قانون العقوبات و مخاطر تقنية المعلومات) مرجع سابق، هامش رقم 1، ص191.

ثالثا: إنشاء بيانات بصورة غير قانونية وإساءة استعمالها

وفي هذه الحالة يتم الجمع والتخزين والمعالجة لبيانات شخصية بصورة مشروعة و لكنه في المقابل يتم إفشاؤها من قبل القائمين على حفظها بصورة غير مشروعة أو قد يساء استخدامها من قبلهم بشكل أو بآخر.ومن الأمثلة الواقعية عن هذه الحالة، قيام ضابط شرطة نمساوي باعطاءأحد المخبرين الخاصين معلومات قيمة تخص بعض الأفراد و متعلقة بحالتهم الجنائية المخزنة في ذاكرة الحاسب الذي تستخدمه الشرطة.[1]

رابعا: عدم الالتزام بالقواعد الشكلية الخاصة بتنظيم عملية وجمع ومعالجة ونشر البيانات الشخصية

قد يوجب القانون قيام الجهات الراغبة في جمع وتخزين ومعالجة بيانات شخصية ضرورة الحصول على ترخيص مسبق لممارسة هذا النشاط قبل مزاولتها إياه.[2]

الفرع الثاني: موقف التشريعات المقارنة من جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

أثارت مسألة حماية الخصوصية الفردية في مواجهة أخطار المعلوماتية قلقا في مختلف الأنظمة القانونية، حيث لم تأخذ التشريعات المقارنة مسلكا موحدا لحماية الحق في حرمة الحياة الخاصة في مواجهة الأخطار الناجمة عن استخدام الحاسب الالكتروني و الانترنت كبنك للمعلومات، سواء في دساتيرها أو تشريعاتها. ويمكننا تقسيم موقف هذه التشريعات المقارنة إلى موقفين، الأول نخص به التشريعات الغربية.أما الثاني فخصصناه للتشريعات العربية.

و قبل ذلك يجب التطرق أولا إلى تبيان **الجهود الدولية المبذولة لحماية الحياة الخاصة في مواجهة نظم المعلومات** ، فلقد أثارت مسألة حرمة الحياة الخاصة للأفراد اهتمامات المنظمات العالمية والإقليمية، والتي أكدت على حق الإنسان في حرمة حياته الخاصة من أخطار الإعتداء على البيانات الشخصية. حيث برزت في هذا الإطار جهود منظمة الأمم المتحدة والمجلس الأوربي وكذا منظمة التعاون الاقتصادي.

– ففي منظمة الأمم المتحدة، توجت جهودها في ميدان حماية الحياة الخاصة في مواجهة أخطار بنوك المعلومات ، من خلال المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان و الذي تم عقده بطهران عام 1968، حيث تبنت الجمعية العامة للأمم المتحدة توصياته، وكان من أبرزها اعتبار الحاسبات الإلكترونية أكبر تهديد للحياة الخاصة و الحرية الشخصية، لانها تعد من

---

[1]– لمزيد من التفاصيل ينظر د/ هشام محمد فريد رستم، المرجع السابق ، ص 192–194.

[2]– لمزيد من التفاصيل ينظر د/ هشام محمد فريد رستم، نفس المرجع ، ص 200–201.و د/أسامة عبد الله قايد، المرجع السابق، ص 86.

أدوات المراقبة و أجهزة التطفل الحديثة خاصة ما إذا تم تخزين البيانات الشخصية على الحاسب الآلي وتحليلها.[1]

– أما فيما يخص دور المجلس الأوروبي فقد برز من خلال التوقيع على معاهدة مجلس أوروبا و الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية عام 1981، فضلا عن ذلك فقد أصدر مجلس أوروبا العديد من التوصيات لتؤكد على توسيع نطاق الحماية لتشمل قطاعات الأنشطة الخاصة كالبيانات الطبية والبحثية والإحصائية ومن أبرزها:

التوصية رقم: 13/80 بشأن تبادل المعلومات القانونية المتصلة بحماية البيانات.

التوصية رقم: 1/81 بشأن تنظيم البيانات الطبية المعالجة آليا في بنوك المعلومات.

التوصية رقم: 10/83 والخاصة بحماية البيانات الشخصية المستعملة للبحوث العلمية[2].

– ولقد تناولت الاتفاقية الأوروبية حول جرائم الإنترنت المنعقدة ببودابست والتي تم توقيعها في 2001/11/29 حماية سرية وسلامة وإتاحة تهيئة البيانات والنظم المعلوماتية من المواد 2 إلى 10.[3]

و إلى جانب جهود المجلس الأوروبي في توفير الحماية للخصوصية الفردية في مواجهة أخطار بنوك المعلومات، فقد اهتمت منظمة التعاون الاقتصادي والتنمية[4] بتوفير هذه الحماية من خلال وضع قواعد ارشادية تحمي كل من خصوصية ونقل و تدفق البيانات الشخصية . وقد تم تبني هذه القواعد من قبل مجلس المنظمة في عام 1980 مع التوصية للاعضاء بالالتزام بها ، ولا تعد هذه القواعد الزامية وانما مجرد ارشادات وتوصيات ، وتغطي هذه القواعد الاشخاص الطبيعين فقط وتطبق على القطاعين العام

---

[1]– يونس عرب: جرائم الحاسوب، دراسة مقارنة، رسالة مقدمة لنيل درجة الماجستير في الحقوق، كلية الدراسات العليا، الجامعة الأردنية،1994، ص125.

[2]– وقعت على هذه الاتفاقية كل من النمسا، بلجيكا، الدنمارك، ألمانيا الغربية (قبل الاتحاد)، فرنسا،اليونان، أيسلندا،ايطاليا، لوكسمبورج، النرويج، البرتغال، السويد، تركيا، المملكة المتحدة، و قد صدقت عليها كل من فرنسا، ألمانيا، النرويج،إسبانيا،السويد. وقد بدأ السريان الفعلي لهذه الاتفاقية في أكتوبر 1985، و التي انطوت على توجيهات بصدد وجوب توفير قواعد تكفل حماية البيانات الشخصية من مخاطر المعالجة الآلية.

و تجدر الاشارة إلى أن نطاق تطبيق هذه الاتفاقية يقتصر على الأشخاص الطبيعيين، و تسري على القطاعين العام والخاص بشأن الملفات المعدة آليا، حيث تحظى بالزامية أحكامها لتحقيق حماية البيانات الشخصية المعالجة آليا. لمزيد من التفاصيل ينظر يونس عرب: الخصوصية و حماية البيانات، ص5، http:// www.arablaw.org ؛ وكذالك محمد أمين أحمد الشوابكة، المرجع السابق، ص74–75.

[3]– د/هلالي عبد اللاه أحمد: الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، على ضوء اتفاقية بودابست الموقعة في 2001/11/23، الطبعة الأولى، دار النهضة العربية، القاهرة،2003، ص25 وما بعدها.

[4] – منظمة التعاون الاقتصادي والتنمية : تضم منظمة التعاون الاقتصادي والتنمية في عضويتها 29 دولة حتى اواخر عام 2000 وغرضها الرئيس تحقيق اعلى مستويات النمو الاقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية.

والخاص ، وتتعلق ايضا بالبيانات المعالجة اليا او غير المعالجة اليا ، وتتضمن التوجيهات المبادئ الثمانية الرئيسة لحماية الخصوصية او الحق في حماية البيانات الخاصة وهي:

تحديد حصر عمليات جمع البيانات والاقتصار على طبيعة البيانات الشخصية وتحديد الغرض وحصر الاستخدام بالغرض المحدد و توفير و تحديد وسائل حماية وأمن المعلومات والعلانية والحق في المشاركة و المساءلة[1] . كما تضمنت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 14 جريمة الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.[2]

أولا: موقف التشريعات الغربية من جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

إن جرائم الإعتداء على حرمة الحياة الخاصة هي من أخطر الجرائم التي يمكن أن تقع بطريق الانترنت، ونظرا لعدم وجود الحماية التقنية الفاعلة لما يتم تداوله من معلومات و أسرار و مراسلات بطريق الإنترنت، فلقد تدخل المشرع في القوانين الغربية – ضمن نصوص دستورية أو تشريعات خاصة– و جرم و عاقب كل من دخل بطريق غير مشروع إلى أنظمة الإتصالات بغية التجسس و الإعتداء على الحياة الخاصة، وكفل مقابل ذلك حماية خاصة للمراسلات الخاصة التي تتم بطريق وسائل الاتصال و لا سيما الانترنت. ولتبيان موقف التشريعات الغربية من جرائم الإعتداء على حرمة الحياة الخاصة عبر الانترنت ارتأينا تقسيمه إلى قسمين، نبين في الأول منهما بعض الدول الغربية التي كفلت دساتيرها حماية البيانات الشخصية في مواجهة أخطار البنوك ، ثم نتناول في ثانيهما موقف التشريعات اللاتينية ثم موقف التشريعات الأنجلوسكسونية. وذلك كالآتي:

1/ الدول الغربية التي نصت دساتيرها على حماية خاصة في مواجهة أخطار بنوك المعلومات:

نظرا للتطور التكنولوجي الذي يشهده عالمنا و الذي أثر بصورة مباشرة و خاصة على الحياة الخاصة للافراد، بحيث أصبح بامكان كل من دب و هب انتهاك حرمة تلك الحياة في ظل غياب نصوص قانونية تضمن الحماية الكافية في مواجهة ما يسمى بأخطار بنوك المعلومات. و لهذا وجب على الدول استحداث دساتيرها و تشريعاتها. و من الدول الغربية التي كفلت دساتيرها حماية البيانات الشخصية: بلجيكا (المادة22 المضافة بموجب التعديل 1994)، السويد (الفقرة 3 من المادة 3 من الفصل الثاني (اسبانيا) المادة 2/18)، السلوفاك (المادة 16)،كوريا الجنوبية (المواد 16–18)، روسيا (المادة 23)، أذربيجان (المادة32)، شيلي (المادة19)، الصين (المادة 40)، ألبانيا (المادة53)، الارجنتين (في المواد 18و19و43)، بلغاريا (المادة32)، استونيا (المواد 42–44)، هولندا (المادة 10)، حيث كفلت دساتير هذه الدول حماية البيانات الشخصية الخاضعة للمعالجة الالكترونية.[3]

---

[1]– لمزيد من التفاصيل ينظر محمد أمين أحمد الشوابكة، المرجع السابق، ص76.

[2]– المادة 14 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات تنص على:"جرائم الإعتداء على حرمة الحياة الخاصة: الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات."

[3]– لمزيد من التفاصيل ينظر منير محمد الجنبيهي، ممدوح محمد الجنبيهي، (أمن المعلومات الالكترونية) مرجع سابق،ص98 و ما بعدها.

2/ موقف التشريعات اللاتينية من أخطار بنوك المعلومات على الحياة الخاصة:

و سنتناول تحت هذه النقطة موقف بعض التشريعات اللاتينية، و يمكن حصرها في موقف التشريع الفرنسي ثم موقف التشريع الألماني و النمساوي و النرويجي و الدنماركي.

أ- موقف التشريع الفرنسي:

تناول المشرع الفرنسي حماية الحياة الخاصة في مواجهة أخطار بنوك المعلومات من خلال القانون رقم17 لسنة 1978، والخاص بالمعالجة الالكترونية للبيانات الاسمية والذي اشتهرت تسميته بقانون نظم المعالجة الرقمية والحرية Informatique et liberté [1]. اذ نص في الباب السادس منه (الخاص بالمعالجة الالكترونية للبيانات الاسمية) على عدة جرائم تتعلق بالمعالجة الالكترونية للبيانات الشخصية للأفراد[2].

هذا من جهة و من جهة أخرى، فقد وضع المشرع الفرنسي عدة قوانين راعى فيها التطور التكنولوجي في عالم الاتصالات والكمبيوتر في مواجهة الخصوصية. ومنها:

قانون 12 جويلية 1980 والمتعلق بإثبات التصرفات القانونية ذات المعالجة الالكترونية.

قانون 29 جوان 1982 والذي أقر بمبدأ حرية الإتصال السمعي والبصري.

قانون 90 سبتمبر 1986 المعدل بقانون 17 جانفي 1989 بشأن الاتصالات السمعية والبصرية والذي جاء في محل قانون 1982 المشار إليه سابقا[3].

قانون العقوبات الجديد لعام 1992[4] و ذلك من خلال المواد 226-1 و 226-2 و226-8[5]. اذ جرم في المادة 226-1 التقاط أو تسجيل أو نقل أحاديث خاصة أو سرية دون موافقة المجني عليه، وكذلك تثبيت

---

[1]- إذ نصت المادة (1) منه على مبدأ وجوب أن تكون معالجة المعلومات في خدمة كل مواطن.

[2]- تجدر الاشارة إلى أن المشرع الجنائي قصر نطاق حماية البيانات على الأشخاص الطبيعية دون المعنوية في هذا القانون. كما أنه يتطلب ضرورة إخطار اللجنة الوطنية للمعلوماتية و الحريات(CNIL) عند معالجة أي بيانات شخصية من قبل أشخاص القانون الخاص، أو الحصول على تصريح مسبق عنها إذا كان من يقوم بجمع المعلومات أحد أشخاص القانون العام أو أحد أشخاص القانون الخاص العاملين لحساب الدولة. لمزيد من التفاصيل ينظر محمد أمين أحمد الشوابكة، المرجع السابق،ص 84 و ما بعدها؛ د/ مدحت رمضان: الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية،2001،ص85.

[3]- لمزيد من التفاصيل ينظر محمد أمين أحمد الشوابكة، المرجع السابق،ص80.

[4]- تناول المشرع الفرنسي في قانون العقوبات القديم بالتجريم الإعتداء على حرمة الحياة الخاصة في المواد 368- 372. لمزيد من التفاصيل ينظر د/مدحت رمضان،المرجع السابق، ص102 و ما بعدها.

[5]-226-1 : « Est puni d'un an d'emprisonnement et de 45000 euros d'amende le fait، au moyen d'un procédé quelconque، volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant، enregistrant ou transmettant، sans le consentement de leur auteur، des paroles prononcées à titre privé ou confidentiel ; 2° En fixant، enregistrant ou transmettant، sans le consentement de celle-ci، l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés، alors qu'ils étaient en mesure de le faire، le consentement de ceux-ci est présumé ».

أو تسجيل أو نقل صورة شخص في مكان خاص دون رضاء منه. بينما جرم حفظ أو وضع أو السماح بوضع في متناول الجمهور أو الغير أو استعمال بأي وسيلة كانت تسجيل أو وثيقة تم الحصول عليه بأحد الأفعال المشار إليها بالمادة 226-1، في المادة 226-2.أما المادة 226-8 فجرم فيها المشرع الفرنسي نشر مونتاج (تركيب) لصوت أو صورة شخص دون رضاء منه.

هذا من جهة و من جهة أخرى، و نظرا لخطورة ما يترتب على معالجة البيانات الإسمية من تهديد لخصوصيات الأفراد، فقد قرر المشرع الفرنسي من خلال قانون العقوبات الفرنسي الجديد[1] حماية لخمسة أنواع من الجرائم بشأن المعالجة الإلكترونية للبيانات الإسمية، و التي تتمثل في جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص (المادة 226-16)[2] و جريمة التسجيل غير المشروع للبيانات الإسمية (المادتين 226-17 و 226-19)[3] وجريمة الحفظ غير المشروع

226-2 : « Est puni des mêmes peines le fait de conserver، porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.

Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle، les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables ».

226-8 : « Est puni d'un an d'emprisonnement et de 15000 euros d'amende le fait de publier، par quelque voie que ce soit، le montage réalisé avec les paroles ou l'image d'une personne sans son consentement، s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle، les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables ».

[1]- أحيلت المواد 41-44 و المادة 46 من القانون رقم 17 لسنة 1978، معدلة بالقانون 1336 لسنة 1992 من قانون العقوبات الفرنسي الجديد إلى المواد من 226-16 إلى 226-24 من ذلك القانون .

[2]- 226-16 : « Le fait، y compris par négligence، de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Est puni des mêmes peines le fait، y compris par négligence، de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique، aux fichiers et aux libertés ».

[3]-226-17 : « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier1978 précitée est puni de cinq ans d'emprisonnement et de

300 000 Euros d'amende».

226-19 : « Le fait، hors les cas prévus par la loi، de mettre ou de conserver en mémoire informatisée، sans le consentement exprès de l'intéressé، des données à caractère personnel qui،

للبيـانات الإسمية (المادة 226-20)[1]

وجريمة الإنحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الإسمية (المادة 226-21) [2]

وجريمة الإفشاء غير المشروع للبيانات الإسمية (المادة 226-22) [3].

و من التطبيقات القضائية عن هذه الجريمة :

- إدانة محكمة Privas الفرنسية يوم 1997/09/03 طالبا في الإعلام الآلي على فعل نشر صور لإحدى صديقاته على صفحة الاستقبال الشخصية التابعة له للانتقام منها، و كانت تلك الصور تمثل صاحبتها وهي عارية و تمارس أفعالا اباحية. كما أرفق المتهم تلك الصور بتعليقات مشينة حول أخلاق الفتاة المذكورة. و لقد استندت المحكمة في ادانتها لهذا الأخير على المادة 226-19 قانون العقوبات الفرنسي، والتي تنص على المعاقبة بالحبس و الغرامة ضد كل من يضع في الذاكرة المعلوماتية دون رضا صاحبها معلومات تعيينية تـدل بصفــة مباشــرة أو غيــر مباشــرة عن أصلــه أو عرقه أو آرائه السياسية

---

directement ou indirectement، font apparaître les origines raciales ou ethniques، les opinions politiques، philosophiques ou religieuses، ou les appartenances syndicales des personnes، ou qui sont relatives à la santé ou à l'orientation ou identité sexuelle de celles-ci، est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. Est puni des mêmes peines le fait، hors les cas prévus par la loi، de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions، des condamnations ou des mesures de sûreté ».

[1]- 226-20 : « Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement، par la demande d'autorisation ou d'avis، ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés، est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende، sauf si cette conservation est effectuée à des fins historiques، statistiques ou scientifiques dans les conditions prévues par la loi.

Est puni des mêmes peines le fait، hors les cas prévus par la loi، de traiter à des fins autres qu'historiques، statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa».

[2]- 226-21 : « Le fait، par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement، de leur classement، de leur transmission ou de toute autre forme de traitement de détourner ces informations de leur finalité telle que définie par la disposition législative، l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé، ou par les déclarations préalables à la mise en oeuvre de ce traitement، est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

[3] - 226-22 : « Le fait، par toute personne qui a recueilli، à l'occasion de leur enregistrement، de leur classement، de leur transmission ou d'une autre forme de traitement، des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée، de porter، sans autorisation de l'intéressé، ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents، la poursuite ne peut être exercée que sur plainte de la victime، de son représentant légal ou de ses ayants droit. »

لمزيد من التفاصيل حول هذه الجرائم ينظر محمد أمين أحمد الشوابكة، المرجع السابق، 87 و مابعدها.

أو الدينية أو انتمائه النقابي أو أخلاقه.[1]

ب- موقف التشريع الألماني و النمساوي و الدنماركي و النرويجي:

أما في ألمانيا فقد تناول المشرع الألماني حماية الحياة الخاصة في مواجهة أخطار بنوك المعلومات من خلال:

قانون حماية المعطيات لعام 1977.[2]

مشروع قانون حماية البيانات عام 2000 المتوافق مع القانون الأوروبي لعام 1995.

- أما بالنسبة للنمسا فتناول المشرع النمساوي تلك الحماية من خلال:

القانون الفدرالي لحماية المعطيات لعام 1978.[3]

قانون حماية البيانات لعام 2000.

- أما الدانمارك فكانت الحماية من خلال:

قانون التسجيل الخاص رقم 293 لعام 1978 المعدل عام 1988.

قانون تسجيل السلطات العامة لعام 1978المعدل أيضا عام 1988.

قانون معالجة البيانات الشخصية لعام 2000.

- أما بالنسبة للنرويج فقد نص المشرع النرويجي على تلك الحماية من خلال:

قانون تسجيل المعطيات الشخصية رقم 48 لعام 1978.[4]

قانون تسجيل البيانات الشخصية لعام 2000.

3/ موقف التشريعات الأنجلوسكسونية:

ونتطرق تحت هذه النقطة إلى موقف التشريع الأمريكي ثم موقف التشريع الأنجليزي.

أ- موقف التشريع الأمريكي:

أما في أمريكا فهناك أكثر من قانون لحماية الخصوصية المعلوماتية للأفراد؛ و يمكن تبيان موقف المشرع الأمريكي من خلال تقسيمه إلى موقفين، الأول يتمثل في موقف المشرع الفدرالي و الثاني في موقف المشرع الولائي الأمريكي.

- موقف المشرع الفدرالي:

لقد فرض المشرع الفدرالي حماية لخصوصية الأفراد المعلوماتية من خلال:

قانون الخصوصية لعام 1974 The privacy act المقنن في (5USC sec.552 a)[5] والذي يهدف إلى حماية الحياة الخاصة للمواطن الأمريكي في مواجهة الحاسب الآلي الذي بات يهددها بشكل متزايد

---

[1]- TGI de Privas،03/09/1997، http://Legalis.net.

[2]- تجدر الاشارة إلى أن هذا القانون قد عدل جذريا بتاريخ 1990/12/20 كما جرى تعديله في العام 1994.

[3]- تجدر الاشارة إلى أن هذا القانون هو الآخر عدل بالقوانين التالية رقم: 314 لسنة 81،228 لسنة 1982، 370 لسنة 1986،605 لسنة 1987،233 لسنة 1988،609 لسنة 1989،91 لسنة 1993،79 و 632لسنة 1994.

[4]- تجدر الاشارة إلى أن هذا القانون هو الآخر عدل بالقوانين التالية رقم: 55 لسنة 1987و 66 لسنة 1991و 78لسنة 1993.

[5]- تنص المادة 552/أ على أنه:"لا يجوز لأي جهة أن تفشي أي معلومات يتضمنها نظام للمعلومات بأي وسيلة من الوسائل لأي شخص أو لأي جهة أخرى؟ ما لم يكن ذلك بناء على طلب كتابي بموافقة صاحب الشأن الذي تتعلق به المعلومات، مع ايراد استثناء يتعلق بالمصلحة العامة أو بناء على أمر المحكمة". و تجدر الإشارة إلى أن قانون الخصوصية

ومستمر. كما أنه فرض حماية لخصوصية الأفراد أثناء عمليات الإتصال وتبادل المعلومات و ذلك بإصداره:

قانون خصوصية الاتصالات الالكترونية لعام 1986. [1]

قانون حماية خصوصية المستهلك لعام 1997.

قانون خصوصية الاتصالات لعام 1997.

قانون حماية خصوصية الضمان الاجتماعي على الخط لعام1997.

وكذلك يعاقب قانون ولاية فلوريدا على كل ولوج بسوء نية في نظام أو شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير، أو كل من أدخل معلومات مصطنعة بقصد تحسين أو إساءة سمعة الغير. [2]

- موقف المشرع الولائي الأمريكي:

تأخذ سياسة التشريع الولائي الأمريكي أبعادا متفاوتة فيما بينها، اذ هناك مثلا المشرع الكالفورني الذي يرتقي بحماية الخصوصية إلى المستوى الدستوري، عبر ما هو مقرر في المادة الأولى من دستور ولاية كاليفورنيا. و هناك المشرع النيويوركي الذي أصدر قانونا خاصا لحماية الخصوصية، فيما يسمى بقانون الحريات المدنية CIVIL RIGHTS LAW ، و الذي يتضمن أيضا حماية فعالة الخصوصية كحظر الحيازة غير المشروعة لأسماء الأشخاص(انتحال الشخصية) بغرض الإستخدام التجاري، كما أن القانون يضيق من الدخول إلى البيانات الإسمية عبر المؤسسات بما في ذلك الحالة الجنائية. [3]

ب- موقف التشريع الإنجليزي:

أما بالنسبة لإنجلترا فالأمر يختلف، لأن المشرع الإنجليزي يرفض الإعتراف باستقلالية الحق في الحياة الخاصة، فهو لا يعترف بأن الخصوصية لها طابع الحقوق و من ثم تعد مظهر من مظاهر الحياة

قد وضع على إثر إساءة إستخدام المعلومات الخاصة لفضيحة وترجيت و الذي إستلزم ضرورة تحري الدقة حين الحصول على المعلومات، على أن يكون مصدرها دائما أصليا و ليس نقليا. د/ عمر محمد أبو بكر بن يونس، المرجع السابق،ص605.

[1]- يحظر قانون خصوصية الاتصالات الالكترونية حجز و حصر أو بث الاتصالات الالكترونية الخاصة، حيث يجرم الدخول غير المشروع إلى الاتصالات الالكترونية المخزنة و المبثوثة،و هي بدورها تتضمن البريد الصوتي أو البريد الالكتروني. حيث أن الدخول إلى بريد الكتروني لشخص ما بدون اذنه يشكل انتهاكا لقانون خصوصية الاتصالات الالكترونية. و تجدر الاشارة إلى أن هذا القانون و ان كان يجرم ما سبق ذكره،الا أنه ليس هناك أي توضيح أو اشارة إلى تجريم الدخول إلى ملفات موضوعة و مثبتة على مناطق عامة في النظام الالكتروني مثل دليل شبكة الويب العالمية. لمزيد من التفاصيل ينظر محمد أمين أحمد الشوابكة، المرجع السابق، ص 79.

[2]- أسامة أحمد المناعسة:جرائم الحاسب الآلي و الإنترنت،دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر، الأردن، 2001،ص 223.

[3]- لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، المرجع السابق،ص610-611.

الانسانية.ولقد سايره في ذلك القضاء الإنجليزي في العديد من الأحكام،[1] مؤسسا ذلك على أن فكرة الخصوصية في حد ذاتها فكرة نسبية غير محددة المضمون، وهي تمس مسائل حساسة دستورية وسياسية، وأنه لا يوجد أي أساس قانوني لإمكانية الإضرار بها. ومن الصعوبة بإمكان وضع حدود فاصلة بين ما يعد من العموم وما يعد من الخصوص. ضف إلى ذلك انعدام السوابق القضائية في هذا الخصوص. غير أن هذا الاتجاه لا يمكن الأخذ به على إطلاقه، لكون أن المشرع الانجليزي وبالرغم من عدم اعترافه باستقلالية ذلك الحق في الخصوصية. إلا أنه أصدر قوانين تخص ذلك الأخير ومنها:

قانون حماية المعطيات لعام 1984 المعدل بقانون حماية البيانات لعام 1998 The Data Protection Act، بهدف حماية و مراقبة استخدام البيانات الشخصية المحوسبة. [2]

قانون حقوق الانسان لعام 1998 (The Human Rights Act).

قانون حرية المعلومات لعام 2000[3](The Data Libertie Act).

ثانيا: موقف التشريعات العربية من جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

هذا فيما يخص موقف التشريعات الغربية، أما بالنسبة لموقف التشريعات العربية من جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت، فيمكن أن نقسمه إلى موقفين. نتطرق في أولهما إلى موقف التشريعات العربية بصفة عامة من هذه الجريمة، أما الموقف الثاني فارتأينا تخصيصه للتشريع الجزائري.

و تجدر الإشارة إلى أنه و على عكس التشريعات الغربية فلم تنص دساتير الدول العربية على توفير حماية خاصة في مواجهة أخطار بنوك المعلومات.

1/ موقف التشريعات العربية بصفة عامة من جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت.

و سنحدد في هذه النقطة الدول العربية التي وضعت قوانين خاصة في مواجهة أخطار بنوك المعلومات ثم نعرج إلى الدول العربية التي التزمت الصمت حيال هذا الاشكال الخطير و الجسيم المهدد للخصوصية المعلوماتية للافراد. و من الدول العربية التي خصصت حماية قانونية للخصوصية المعلوماتية للافراد

---

[1]– ففي قضية كوريللي الشهيرة رفضت المحكمة الحكم للمدعية على أساس أن الادعاء غير مؤسس قانونا لغياب النص الذي يجرم ما قام به المدعي عليه و المتمثل بنشرو بيع صور المدعية دون اذنها. اضافة إلى أن نشر صورة المدعية لا ينطوي على التشهير بها.

-Y.AKDEMY et J.BELL:la vie privée et l'internet perspective du Royaume-Uni , chapitre 8 , p150 ، http://Asmp.fr

[2]– Y.AKDEMY et J.BELL , op.cit, p152.

– La violation de droit de l'homme sur internet,http:// www.educnet.education.fr

[3]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي،(أمن المعلومات الالكترونية) مرجع سابق، ص94.

تونس، اذ نجد أن **القانون التونسي** أفرد فيه حماية خاصة للمعطيات الشخصية في مواجهة التطور التقني في المواد من 38-42 من قانون التجارة الالكترونية لعام2000[1].

وكذا **السعودية** من خلال نظام مكافحة الجريمة المعلوماتية في المادة 3 منه في الفقرتين 1و4.[2] وكذا **الامارات العربية المتحدة** من خلال القانون الاتحادي رقم (2) سنة 2006 بشأن مكافحة جرائم تقنية

---

[1]- تنص المادة 38 على أنه:"لا يمكن لمزود خدمات المصادقة الالكترونية معالجة المعطيات الشخصية، الا بعد موافقة صاحب الشهادة المعني.

و يمكن اعتماد الاعلام الالكتروني بالموافقة اذا ضمن المزود:

اعلام صاحب الشهادة لحقه في سحب الموافقة في كل وقت.

امكانية تحديد هوية الأطراف المستعملة للمعطيات الشخصية.

الاحتفاظ بحجة الموافقة التي لايمكن تغييرها." و تنص المادة 39على أنه:" باستثناء حالة موافقة صاحب الشهادة، لا يمكن لمزود خدمات المصادقة الالكترونية أو أحد أعوانه جمع المعلومات الخاصة بصاحب الشهادة الا ما كان منها ضروريا لابرام العقد و تحديد محتواه و تنفيذه و اعداد و اصدار الفاتورة.

لا يمكن استعمال المعطيات المجمعة طبقا للفقرة الأولى من هذا الفصل لغير الغاية المذكورة أعلاه من قبل المزور أو غيره الا اذا تم اعلام صاحب الشهادة بذلك و لم يعارضه." أما المادة 40 فتنص على مستعملي العطيات الشخصية الممعة طبقا للفصل 39 من هذا القانون،ارسال الوثائق الالكترونية إلى صاحب الشهادة الذي يرفض صراحة قبولها.

ويتعين على صاحب الشهادة اعلام الوكالة الوطنية للمصادقة الالكترونية باعتراضه بواسطة رسالة مضمونة الوصول مع اعلام بالبلوغ.

و يعتبر هذا الاعلام قرينة قاطعة على معرفة كل المزودين و الغير لهذا الاعتراض". أما المادة41 فتنص على أنه:"يتعين على مزود خدمات المصادقة الالكترونية، قبل كل معالجة للمعلومات الشخصية، اعلام صاحب الشهادة بواسطة اشعار خاص بالاجراءات المتبعة من قبله في مجال حماية المعطيات الشخصية.

و يتعين أن تمكن هذه الاجراءات صاحب الشهادة من الاطلاع آليا وبطريقة مبسطة على محتوى المعطيات.

و يجب أن تحدد هذه الاجراءات هوية المسؤول عن المعالجة و طبيعة المعطيات والغاية من المعالجة و أصناف و أماكن المعالجة، و عند الاقتضاء كل معلومة ضرورية لضمان المعالجة الأمنية للمعطيات".و كذلك تنص المادة 42 على أنه:"يمكن لصاحب الشهادة في كل وقت بطلب ممضي بخط اليد أو الكترونيا النفاذ و التعديل الدخول على جميع المعطيات الشخصية المتعلقة بصاحب الشهادة.

ويتعين على المزود وضع الامكانيات التقنية اللازمة لتمكين صاحب الشهادة من ارسال مطلبه لتعديل المعلومات أو فسخها بطريقة اليكترونية".

[2]- تنص المادة 1/3 و4 من نظام مكافحة الجريمة المعلوماتية السعودي على: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو باحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من الجرائم الآتية:

1- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.

4 – المساس بالحياة الخاصة عن طريق اساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها".

المعلومات في المادة 8 و 12 منه[1]. و كذا **السودان** من خلال قانون جرائم المعلوماتية لسنة 2007 وذلك في المادة 6 و 16.[2]

- وعلى عكس الدول العربية السابقة فقد اكتفت معظم التشريعات العربية لتوفير تلك الحماية بالنصوص القانونية التقليدية الخاصة بحماية الأسرار، المتناثرة ما بين قوانين العقوبات وقوانين الإجراءات الجزائية وقوانين البريد والاتصالات.[3]

2/ موقف التشريع الجزائري من أخطار بنوك المعلومات على الحياة الخاصة:

أما بالنسبة للجزائر، و لما كانت هذه الأخيرة من الدول العربية التي طالها تسونامي جرائم الإنترنت بجميع أنواعها و لا سيما جرائم التعدي على حرمة الحياة الخاصة بكل أشكالها. و لما كانت خصوصية الأفراد من أهم الحريات المكرسة في المواثيق الدولية و الدساتير و القوانين ، و كان التعدي عليها وانتهاكها يشكل جريمة و انتهاكا لحقوق و حريات الافراد، كان من اللازم على المشرع الجزائري توفير الحماية الواجبة لهذه الحرمة و تجريم كل أشكال الإعتداءات التي يمكن أن تمس و تهز هذه الاخيرة، و هذا من خلال المواد الدستورية و كذا من خلال مواد قانون العقوبات و الاجراءات الجزائية.

فأما فيما يخص الحماية الدستورية لهذه الحرمة، فقد كفل الدستور الجزائري تلك الحماية للحقوق و الحريات الفردية في الفصل الرابع من المواد 29 الى 59. و من ذلك ما نص عليه في المادة 1/32 منه على أن:"الحريات الاساسية و حقوق الانسان و المواطن مضمونة." و في المادة 1/34 منه على أنه :"تضمن الدولة عدم انتهاك حرمة الانسان". و في المادة 39 منه على أنه:"لا يجوز انتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، ويحميها القانون.

سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة."

و تجسيدا لهاته الحماية الدستورية لخصوصيات الافراد فقد تدخل المشرع الجزائري و وضع حدا لكل اعتداء على حرمة هذه الحياة و ذلك بتجريم كل أنواع المساس بحرمة الحياة الخاصة باستخدام وسائل

---

[1]– تنص المادة 8 من القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على:"كل من تنصت أو التقط أو اعترض عمدا، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو باحدى وسائل تقنية المعلومات، يعاقب بالحبس و بالغرامة أو باحدى هاتين العقوبتين"، أما المادة 12 فتنص على:"كل من اعتدى على أي من المبادئ و القيم الأسرية أو نشر أخبارا أو صورا تتصل بحرمة الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، عن طريق الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات، يعاقب بالحبس مدة لا تقل عن سنة و بالغرامة التي لاتقل عن خمسين ألف درهم أو باحدى هاتين العقوبتين."

[2]– تنص المادة 6 من قانون جرائم المعلوماتية لسنة 2007 السوداني على: :" كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها أو يلتقطها أو يعترضها ، دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً ".و تنص المادة 16 على:" كل من ينتهك أو يسئ أي من المعتقدات الدينية أو حرمة الحياة الخاصة عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها ، يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً."

[3]– ينظر محمد أمين أحمد الشوابكة، المرجع السابق، ص 83.

التكنولوجيا الحديثة بدء من المادة 303 مكرر إلى 303 مكرر3 من قانون 06- 23 المؤرخ في 2006/12/20 المعدل و المتمم لقانون العقوبات.[1]

و باستقرائنا لنص هاتين المادتين نستخلص مايلي:

1- أن المشرع الجزائري اقتبس لفظا و مضمونا أحكام النصوص التي تكفل حماية حرمة الحياة الخاصة من قانون العقوبات الفرنسي الجديد من المادتين 226-1 226-2.

2- أن المشرع الجزائري قد حدد الجرائم التي تقع على حرمة الحياة الخاصة على سبيل الحصر، و هي: جريمة التقاط أو تسجيل او نقل صورة لشخص في مكان خاص و بغير رضا صاحبها، جريمة التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية و بدون اذن صاحبها، جريمة الاحتفاظ أو اذاعة أو استعمال التسجيلات أو الصور أو الوثائق المتحصل عليها من الجريمتين السابقتين.

3- أن محل التجريم في المادة 303 مكرر و المادة 303 مكرر1 هو ارتكاب أفعالا غير مشروعة تشكل في حد ذاتها اعتداء على حرمة الحياة الخاصة و هي الالتقاط أو التسجيل أو النقل لأحاديث أومكالمات سرية أو للصورة في مكان خاص بدون رضا صاحبها، أو الاحتفاظ أو اذاعة أو استعمال التسجيلات أو الصور أو الوثائق، و لا يهم في مقابل ذلك التقنية المستعملة في ارتكاب تلك الأفعال غير المشروعة.

4- أن الغاية من التجريم في هاتين المادتين هي توفير الحماية القانونية لأي معلومات تتعلق بالحياة الخاصة للأفراد في مواجهة وسائل التكنولوجيا الحديثة.

5- أن من بين أسباب تعديل قانون العقوبات بالقانون رقم 06-23 و الذي أضاف المواد 303 مكرر إلى 303 مكرر3 هي: تعرض وزير سابق مكلف بالعلاقات مع البرلمان للاعتداء على حرمته الخاصة في مكتبه، حيث تم اكتشاف وجود كاميرا تراقبه و تسجل كل ما يقوم به. و من هنا تفطن المشرع الجزائري لوجود فراغ قانوني في قانون العقوبات يسمح لمثل هذه الإعتداءات الواقعة على خصوصية الأفراد

---

[1]- تنص في المادة 303 مكرر على انه:"يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بالغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت و ذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة،أو سرية بغير اذن صاحبها أو رضاه،

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص،أو سرية بغير اذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حدا للمتابعة الجزائية". و تنص المادة 303 مكرر1 على أنه:"يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة، تطبق الأحكام الخاصة المنصوص عليها في القوانين ذات العلاقة، لتحديد الأشخاص المسؤولين.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حدا للمتابعة الجزائية".

باستخدام وسائل التكنولوجيا الحديثة كالكاميرا غير مجرمة و بالتالي مشروعة، و هو ما يتعارض مع الواقع. لذلك كان من اللازم على المشرع الجزائري التدخل لسد هذا الفراغ بادخال تعديلات على قانون العقوبات وتجريم كل اعتداء يقع على حرمة الحياة الخاصة للافراد الناتج عن استخدام وسائل التكنولوجيا الحديثة.[1]

6- أن موضوع الجريمة المعاقب عليها في المادة 303 مكرر من قانون العقوبات الجزائري هو المحادثات سواء جرت في مكان خاص أو بطريق التليفون (مكالمات)، و لا يشترط هنا أن يكون الحديث بلغة معينة بل يمكن أن يكون بالاشارة كاللغة الخاصة بالصم و البكم، و بالتالي لا تشمل الحماية الاصوات غير المنطوقة و الضوضاء و الموسيقى[2]. و يقصد بالمحادثة الخاصة كل صوت له دلالة معينة متبادل بين شخصين أو أكثر بأي لغة مستعملة[3].

ضف إلى ذلك فإن المشرع الجزائري قد أقر الحماية القانونية لصورة الشخص في المكان الخاص.

7- أن النشاط المادي لهذه الجريمة يتحقق في صورتها الأولى عن طريق إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير اذن صاحبها أو رضاه.والإلتقاط يعني إسترق السمع و التصنت ، أي أن يسمع الجاني الحديث بأذنه بغفلة من الضحية. أما تسجيل الحديث فيعني إلتقاطه لسماعه فيما بعد، و هو يفترض حفظ الحديث على مادة أيا كانت طبيعتها للاستماع اليها فيما بعد. أما نقل الحديث فيقصد به إلتقاطه وإرساله من مكان لآخر[4].

و يتحقق في صورتها الثانية عن طريق التقاط أو تسجيل أو نقل صورة شخص في مكان خاص. و يقصد بالتقاط الصورة تثبيتها في أجهزة التصوير[5].أما النقل فيفترض تمكين الآخرين من الاطلاع على الصورة وذلك بارسالها من مكان لآخر ولو كان عاما[6]. هذا و يشترط المشرع للعقاب على هذا الفعل مجموعة من الشروط هي:

- أن يتم الفعل باستخدام أجهزة مهما كان نوعها، فالمشرع لم ينص على أجهزة بعينها حيث إستعمل عبارة "بأي تقنية كانت" و التي تفيد الأجهزة الخاصة للتجسس و للمراقبة كأن يقع مثلا التقاط الصور أو تسجيل الأحاديث بواسطة كاميرا الفيديو أو كاميرا الهاتف النقال أو كاميرا انترنت webcam أو عن طريق الاحتفاظ بتلك التسجيلات أو الالتقاطات في القرص الصلب التابع للحاسب الآلي أو عن طريق

---

[1]- Lyes AFLOU : Le gouvernement algérien révise le Code pénal pour protéger la vie privée,http:// Magharebia.com.

[2]- د/ مدحت رمضان، المرجع السابق، ص115.

[3]- و يعرف الحديث كذلك بأنه الكلام الذي له دلالة مفهومة سواء أكان هذا الكلام موجها لعامة الناس أو لفئة مجردة منهم. ينظر في ذلك د/ بوفليح سالم: محاضرات قيمة في القانون الجنائي، http://montada.elkhabar.com؛ د/ محمود نجيب حسني: شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة،1988، ص767.

[4] - د/ مدحت رمضان، المرجع السابق ، ص116.

[5] - د/ بوفليح سالم: محاضرات قيمة في القانون الجنائي، الموقع السابق.

[6]- د/ مدحت رمضان، المرجع السابق، ص117.

افشائها عبر موقع الشبكة المعلوماتية بهدف استغلالها لأغراض تجارية أو لتلبية نزوات انتقامية فمثلا يمكن التقاط صور أو تسجيل علاقات حميمية لأشخاص في أماكن خاصة كالاعراس أو الحمامات البخارية أو المسابح و نسخها على جهاز سكانير ثم وضعها على صفحات انترنت[1] . فكل جهاز يكشف عنه التطور العلمي، ويسمح بالنقل والإلتقاط أو التسجيل يشكل وسيلة لارتكاب هذه الجريمة .

– أن تكون المحادثة خاصة أو سرية.

– أن تكون الصورة متعلقة بانسان حي متواجد في مكان خاص[2].

– عدم رضا صاحب المحادثة أو الصورة، فإذا رضي بذلك تنتفي الجريمة.

– أن يتم التجسس أو النقل أو التسجيل أو الالتقاط للحديث أو الصورة في غير الاحوال المصرح بها قانونا، فاذا تمت تلك الأفعال بناء على أمر من السلطة المختصة في التحقيق وفقا لأحكام قانون الاجراءات الجزائية فلا تقوم جريمة الإعتداء على حرمة الحياة الخاصة، وذلك لأن المشرع بصفة عامة والمشرع الجزائري بصفة خاصة يسعى دائما إلى خلق نقطة توازن بين قمع الجريمة و حماية حرمة الحياة الخاصة من خلال وضع ضوابط قانونية تجعل من هذه الأساليب الحديثة في البحث و التحري تدخل في اطار الشرعية الاجرائية و ذلك بالنص على ضرورة الحصول على اذن من وكيل الجمهورية المختص أو قاضي التحقيق، و أن تتم هذه العمليات تحت اشرافه.[3]

---

[1]– و في هذا الصدد تناقلت الصحافة الجزائرية خلال سنة 2007 أخبارا مفادها أن كثيرا من الفتيات و النساء المتزوجات كن عرضة للمساومات بسبب التقاط صور لهن بواسطة كاميرا الهواتف النقالة داخل الحمامات الجماعية من طرف نساء أخريات متواطئات مع رجال محتالين. و كانت المساومات واقعة على نزوات لا ترضاها المرأة الشريفة تحت طائلة التشهير بها.عبد العزيز النويري: المخاطر القانونية للانترنت على حرية التعبير و الحياة الخاصة، التواصل،العدد 26، جوان 2010، كلية الحقوق، جامعة الحاج لخضر، باتنة، ص 19.

[2]– المكان الخاص هو المكان الذي لا يمكن لأي شخص ارتياده الا باذن خاص من صاحبه أو حائزه. ينظر د/ طارق سرور، المرجع السابق، ص341.

[3]– لقد أجاز المشرع الجزائري من خلال القانون رقم 22/06 المعدل و المتمم لقانون الاجراءات الجزائية اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و ذلك في المواد من 65 مكرر5 إلى 65 مكرر10، كأساليب حديثة للبحث و التحري. حيث نص في المادة 65 مكرر5 على:"اذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف و كذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية.

– وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.....". كما أنه أجاز بوضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها من خلال القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها

8- أن النشاط المادي للجريمة المنصوص عليها في المادة 303 مكرر 1 من قانون العقوبات الجزائري هو اذاعة أو تسهيل اذاعة التسجيلات أو الصور أو الوثائق المتحصل عليها عن طريق الإلتقاط أو التسجيل أو النقل.

9- أما بالنسبة للركن المعنوي لهذه الجرائم فإن المشرع الجزائري يتطلب أن ترتكب هذه الأخيرة عمدا.

10- أن المشرع إعتبر أن هذه الجريمة هي كذلك جنحة وقرر لهاعقوبة الحبس من 6 أشهر إلى 3 سنوات والغرامة المالية من 50 ألف إلى 300 ألف دينار. كما عاقب على الشروع في إرتكابها، و اعتبر أن صفح الضحية يضع حدا للمتابعة .

و تجدر الاشارة إلى أن هذه الجريمة يمكن أن تقع عن طريق الصحافة، وتخضع عندئذ للاحكام الخاصة المحددة في قانون الإعلام.

هذا من جهة و من جهة أخرى، فإن المشرع أضاف في المادة 303 مكرر 2 من قانون العقوبات الجزائري عقوبات تكميلية [1] إلى جانب العقوبات الأصلية التي نص عليها في المادتين السابقتين و هي:

الحرمان من حق أو أكثر من الحقوق الوطنية و المدنية و العائلية المنصوص عليها في المادة 9 مكرر 1 لمدة لا تتجاوز 5 سنوات.

و ذلك في جرائم و حالات معينة نصت عليها المادة 4 و هذا كالآتي:" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب و الجرائم الماسة بأمن الدولة؛

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

ج- لمقتضيات التحريات و التحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية؛

د- في ا طار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز اجراء عمليات المراقبة في الحالات المنصوص عليها أعلاه إلا بإذن من السلطة القضائية المختصة.....

تكون الترتيبات التقنية الموضوعة للاغراض المحددة في الفقرة (أ) من هذه المادة موجهة حصريا لتجميع و تسجيل معطيات ذات صلة بالوقاية من أفعال الإرهاب و الإعتداءات على أمن الدولة و مكافحتها و ذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة."

[1] - يقصد بالعقوبات التكميلية: هي تلك العقوبات التي ترتبط بالعقوبات الاصلية، و التي يجب أن ينطق بها القاضي. لمزيد من التفاصيل ينظر عبد الله سليمان: شرح قانون العقوبات الجزائري، القسم العام، الجزء الثاني، الجزاء الجنائي، الطبعة الرابعة،ديوان المطبوعات الجامعية، الجزائر،2005،ص 478.

نشر حكم الادانة بأكمله أو مستخرج منه في جريدة أو أكثر معينة من طرف المحكمة، أو بتعليقه في الأماكن المبينة من طرف تلك الأخيرة.[2]

مصادرة وسائل الجريمة .

هذا فيما يخص العقوبات المطبقة على الأشخاص الطبيعية، أما فيما يخص العقوبات المطبقة على الأشخاص المعنوية فقد نصت عليها المادة 303 مكرر3 من قانون العقوبات الجزائري و ذلك كما يلي:" يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم المحددة في الأقسام 3 و 4 و5 من هذا الفصل، و ذلك طبقا للشروط المنصوص عليها في المادة 51 مكرر.

و تطبق على الشخص المعنوي عقوبة الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر، وفي المادة 18 مكرر2 عند الاقتضاء.

و يتعرض أيضا لواحدة أو أكثر من عقوبات التكميلية المنصوص عليها في المادة 18 مكرر."

باستقرائنا لنص هذه المادة يتضح لنا أن المشرع الجزائري يعاقب الشخص المعنوي الذي يرتكب جريمة الإعتداء على الحياة الخاصة وذلك بالحصول على المحادثة الخاصة أو إلتقاط صور خاصة أو إيداع أو تسجيل هذه الصور و المحادثات لحسابه الخاص، و ذلك بتوقيع عقوبة الغرامة – كعقوبة أصلية –

1- تنص المادة 9 مكرر1 من قانون العقوبات الجزائري على:"يتمثل الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية في:

1-العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة،

2-الحرمان من حق الانتخاب أو الترشح ومن حمل أي وسام،

3- عدم الأهلية لأن يكون مساعدا محلفا، أو خبيرا،أو شاهدا على أي عقد، أو شاهدا أمام القضاء إلا على سبيل الاستدلال،

4- الحرمان من الحق في حمل الأسلحة، و في التدريس، و في إدارة مدرسة أو الخدمة في مؤسسة للتعليم بوصفه أستاذا أو مدرسا أو مراقبا،

5-عدم الأهلية لأن يكون وصيا أو قيما،

6-سقوط حقوق الولاية آلها أو بعضها.

في حالة الحكم بعقوبة جنائية، يجب على القاضي أن يأمر بالحرمان من حق أو أكثر من الحقوق المنصوص عليها أعلاه لمدة أقصاها عشر (10) سنوات، تسري من يوم انقضاء العقوبة الأصلية أو الإفراج عن المحكوم عليه."

2- تنص المادة 18 من قانون العقوبات الجزائري على:"للمحكمة عند الحكم بالإدانة أن تأمر في الحالات التي يحددها القانون بنشر الحكم بأكمله أو مستخرج منه في جريدة أو أكثر يعينها، أو بتعليقه في الأماكن التي يبينها، و ذلك كله على نفقة المحكوم عليه، على ألا تتجاوز مصاريف النشر المبلغ الذي يحدده الحكم بالادانة لهذا الغرض، و ألا تتجاوز مدة التعليق شهرا واحدا.

يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) و بغرامة من 25000 دج إلى200000 دج كل من قام باتلاف أو اخفاء أو تمزيق المعلقات الموضوعة تطبيقا للفقرة السابقة كليا أو جزئيا، و يأمر الحكم من جديد بتنفيذ التعليق على نفقة الفاعل."

حسب الكيفيات المنصوص عليها في المادة 18 مكرر/1 [1] وفي المادة 18 مكرر2 عند الاقتضاء[2]. بالإضافة إلى إمكانية تعريضه لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر2[3] كحله مثلا.

ولكن و في مقابل ذلك يشترط أن لا يكون هذا الشخص المعنوي مؤسسة عمومية لأنها مستثناة من العقاب وهذا بنص المادة 51 مكرر من قانون العقوبات[4] و التي تؤكد المسؤولية الجزائية للشخص المعنوي بإستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام.و تجدر الاشارة هنا إلى أن مسؤولية الشخص المعنوي لاتمنع من مساءلة الشخص الطبيعي (كفاعل أصلي أو شريك)، إذا ثبت أن المؤسسة تابعة لشخص معين فيتابع شخصيا بالإضافة إلى متابعة المؤسسة كشخص معنوي.

---

[1]– تنص المادة 18 مكرر/1 على:" العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات و الجنح هي:
1– الغرامة التي تساوي مرة (1) إلى خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة."

[2]– تنص المادة 18 مكرر2 على:" عندما لا ينص القانون على عقوبة الغرامة بالنسبة للأشخاص الطبيعيين سواء، في الجنايات أو الجنح، و قامت المسؤولية الجزائية للشخص المعنوي طبقا لأحكام المادة 51 مكرر، فإن الحد الأقصى للغرامة لتطبيق النسبة القانونية المقررة للعقوبة فيما يخص الشخص المعنوي يكون كالآتي:
–2000000 دج عندما تكون الجناية معاقبا عليها بالإعدام أو السجن المؤبد.
– 1000000دج عندما تكون الجناية معاقبا عليها بالسجن المؤقت،
– 500000دج بالنسبة للجنحة."

[3]– تنص المادة 18 مكرر/2 على:"....2– واحدة أو أكثر من العقوبات التكميلية الآتية:
–حل الشخص المعنوي،
– غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات،
– إقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات،
– المنع من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات،
– مصادرة الشيء الذي أستعمل في ارتكاب الجريمة أو نتج عنها،
– نشر و تعليق حكم الإدانة،
– وضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات، و تنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي أرتكبت الجريمة بمناسبته."

[4]– تنص المادة 51 مكرر على:"باستثناء الولة و الجماعات المحلية و الأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك.
ان المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل اصلي او شريك في نفس الافعال."

و على هذا فإن المشرع الجزائري كان له موقفا صريحا اتجاه تأثير الانترنت على الحياة الخاصة.

ومن القضايا الشهيرة في مجال الإعتداء على البيانات الخاصة الحادثة التي حصلت في جنوب إفريقيا حيث أمكن للمعتدين الوصول إلى الأشرطة التي خزنت عليها المعلومات الخاصة بمصابي أمراض الإيدز وفحوصاتهم، وقد تم تسريب هذه المعلومات الخاصة والسرية إلى جهات عديدة. ومن الحوادث الشهيرة الأخرى حادثة حصلت عام 1989 عندما تمكن أحد أكبر موظفي أحد البنوك السويسرية بمساعدة سلطات الضرائب الفرنسية، بأن سرب إليها شريطا يحتوي على أرصدة عدد من الزبائن، وقد تكررت مثل هذه الحادثة في ألمانيا أيضا.[1]

وفي واقعة أخرى تم فيها التقاط مادة فيلمية لاحدى الفنانات حال وجودها بمركز للتجميل باحدى الدول العربية دون علمها، عن طريق هاتف محمول، و انتشار المادة الفيلمية عبر خاصية البلوتوث بالهواتف المحمولة و من ثم انتشارها أيضا عبر الانترنت، و قد قامت الفنانة على اثر ذلك برفع دعوى قضائية ضد مركز التجميل للتعويض عن الأضرار الأدبية التي أصابتها من جراء ذلك.[2]

المبحث الثاني:

جريمة المطاردة عبر الإنترنت:

يقصد بالمطاردة "كل سلوك يتكون من متابعة المجني عليه بتطفل مثل ظهور الجاني بطريقة غير متوقعة أو غير مرغوب فيها لدى المجني عليه"[3].أو هي "نموذج غير عادي من التهديد أو الإزعاج والتحرش المباشر تجاه شخص محدد".[4]

---

[1]– لمزيد من التفاصيل ينظر د/ أيمن عبد الله فكري، المرجع السابق، ص 650.

[2]– سامح محمد عبد الحكم، المرجع السابق، ص 45.

[3]–Boij: Victims of cyber stalking,http://www.firstmonday.dk

[4] –Traquer: « est une forme de harcèlement névrotique. Le stalking est un terme communément utilisé pour faire référence à une attention obsessive et non désirée accordée à un individu ou à un groupe de personnes. Le stalking est un comportement en relation avec le harcèlement et l'intimidation et peut inclure le fait de suivre ou surveiller des victimes. Le mot stalking est utilisé, avec différents sens, dans le domaine de la psychologie et de la

وتجدر الإشارة إلى أن جريمة التهديد هي من أشهر جرائم المطاردة عموما. والتي يقوم فيها الشخص بإنذار آخر – شفاهة أو كتابة (بأي عبارة من شأنها إلقاء الرعب في نفس أو مال أو عرض أي شخص يهمه أمره)– بخطر يريد إيقاعه بشخصه أو ماله أو بشخص أو مال غيره. وتعد هذه الجريمة قائمة سواء تمت في مواجهة الشخص المهدد أم لا[1]. لأنها تصنف ضمن الجرائم الشكلية[2]، أي من الجرائم ذات السلوك المحض التي لا يستلزم فيها حدوث النتيجة بل أن النشاط المادي المكون للركن المادي يعتبر في حد ذاته جريمة تهدد بخطر بمصلحة أو حقا أو مالا محمي قانونا بجزاء جنائي و بالتالي يستحق مرتكبها العقاب. وهي على نوعين تهديد مشدد وآخر بسيط. [3]

---

psychiatrie et aussi dans certaines juridictions comme étant une infraction criminelle ». Stalking, http:// Fr.wikipedia.org.

[1]– و في هذا قضت محكمة النقض المصرية على وقوع الجريمة بقيام الجاني باعداد رسالة التهديد لتصل إلى علم المراد تهديده سواء أرسلها اليه فتلقاها مباشرة أم بعث بها إلى شخص آخر فتلقاها هذا الآخر ثم أبلغه اياه أو لم يبلغها. و يكفي أن يثبت في حق الجاني أنه يتوقع حتما أن المرسل اليه بحكم وظيفته أو بسبب علاقته أوصلته بالشخص المقصود بالتهديد سيبلغه الرسالة.نقض في 1955/4/26، مجموعة أحكام النقض،العدد 2 لسنة 7ق، ص 958.

[2]– يعاقب القانون الولائي الأمريكي على التهديد كجريمة شكلية و مثال ذلك القانون العقابي لولاية كاليفورنيا في القسم 71 منه و422. و ذلك كمايلي:،

penal code section 71 provides، in relevant part: " (a) Every person who, with intent to cause، attempts to cause or causes، any officer or employee of any public or private educational institution or any public officer or employee to do، or refrain from doing, any act in the performance of his duties، bymeans of a threat، directly communicated to such person، to inflict an unlawful injury upon any person or property، and it reasonably appears to the recipient of the threat that such threat could be carried out، is guilty of a public offense punishable as follows

(1) Upon a first conviction، such person is punishable by a fine not exceeding ten thousand dollars ($10،000), or by imprisonment pursuant to subdivision (h) of Section 1170, or in a county jail not exceeding one year، or by both that fine and imprisonment.

(2) If the person has been previously convicted of a violation of this section,such previous conviction shall be charged in the accusatory pleading, and if that previous conviction is found to be true by the jury, upon a jury trial, or by the court، upon a court trial، or is admitted by the defendant, he or she is punishable by imprisonment pursuant to subdivision (h) of Section 1170.

(b) As used in this section, "directly communicated" includes, but is not limited to، a communication to the recipient of the threat by telephone, telegraph, or letter"

[3]– يقصد بالتهديد المشدد هو الذي يكون في حالات معينة و هي:

– حالة الحصول بالتهديد على سند أو التوقيع عليه أو التعديل فيه أو الغائه او اتلافه.

– حالة إذا نشأ عن التهديد جروح .

– حالة إذا نشأ عنه موت شخص أو اذا كان التهديد بانشاء أو اسناد أمور خادشة للشرف.

ولقد تأثرت جريمة المطاردة كغيرها من الجرائم التقليدية بالتطور التكنولوجي، خاصة مع ظهور طريق المعلومات فائق السرعة الإنترنت وغزوه للعالم في جميع المجالات، وسوء استخدامها من قبل مريضي الأنفس في تحقيق وارتكاب جرائم من صنف خاص ومميز. ومن بينها جريمة المطاردة والإزعاج عبر الإنترنت. فماذا نعني بهذه الجريمة؟ وهل تطبق عليها القواعد القانونية التقليدية التي تطبق على نظيرتها التقليدية؟.أسئلة سيتم الاجابة عنها وفق المطلبين التاليين:

المطلب الأول: تعريف جريمة المطاردة عبر الإنترنت و الأساليب المتبعة في ذلك.

المطلب الثاني: التكييف القانوني لجريمة المطاردة عبر الانترنت

المطلب الأول:

تعريف جريمة المطاردة عبر الإنترنت و الأساليب المتبعة في ذلك.

و سنتناول تحت هذا المطلب تعريف هذه الجريمة التقليدية الواقعة عبر الانترنت، ثم نبين الأساليب المتبعة في ارتكابهاعبر تلك الشبكة و ذلك في الفرعين التاليين:

الفرع الأول: تعريف جريمة المطاردة عبر الإنترنت.

الفرع الثاني:الأساليب المتبعة في ارتكاب جريمة المطاردة عبر الانترنت.

الفرع الأول: تعريف جريمة المطاردة عبر الإنترنت

يقصد بالمطاردة عبر الإنترنت":كل سلوك يتسم بالتطفل والخبث على شبكة الإنترنت وتستخدم فيه هذه الشبكة لارتكاب نوعين من هذا السلوك:

1 – جمع معلومات خاصة عن المجني عليه ليقرر ويدعم المطاردة.

2 – أو الاتصال بالضحية مع تهديدها الضمني أو العلني لتعزيز الخوف"[1].

ويعرفها أخرون بأنها: "مجموعة من السلوكيات التي تقع على الشخص أو عدة أشخاص أو منظمات باستخدام الإنترنت وتكنولوجيا الاتصالات لإحداث إزعاج أو ضرر، ومثل هذا السلوك قد يشمل الأفعال المجرمة الآتية: نقل التهديدات، الاتهامات الزائفة، سرقة الهوية، سرقة بيانات، تدمير البيانات والأجهزة بإغراء المستخدمين القصر وتحريضهم على ارتكاب أفعال جنسية، أي فعل من الأفعال التعدي على

أما التهديد البسيط فيقصد به كل من حمل غيره بطريق التهديد على تسليم نقود أو أشياء. لمزيد من التفاصيل ينظر سامح محمد عبد الحكم، المرجع السابق، ص33 و ما بعدها.

[1]–Paul BAY: cyber stalking ، harassment in the internet age and how to protect your family، British library ،2004،p 7.

الآخرين".[1] أما البعض الآخر فيعرفونها بأنها:"قيام عضو الإنترنت بمراسلة واتصال مستمر بعضو من أعضاء آخرين يقصد إزعاجهم وتهديدهم ومضايقتهم وإقلاق راحتهم".[2]

أما المشرع السوداني فقد عرف التهديد أو الابتزاز بأنه: "استغلال شبكة المعلومات أو الوسائط التكنولوجية أو ما في حكمها التهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عن فعل ولو كان هذا الفعل أو الامتناع مشروعا".[3]

أما المشرع السعودي فيعرفها في المادة 2/3 من نظام مكافحة جرائم المعلوماتية السعودي بأنه: "الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا."

وعلى هذا فسلوك المطاردة يعني القيام بمجموعة أفعال تقوم على أساس فكرة الخوف من أفعال تجعل المجني عليه يعتقد اعتقادا جازما بأنه عرضة لنتائج إجرامية من نوع ما.وضحايا جريمة المطاردة عبر الإنترنت عديدة ومتنوعة، إذ يمثل العنصر النسائي الهدف الأكثر تفاعلا مع هذه الجريمة. إضافة إلى مطاردة الموظف العام وكذا الأطفال ونشر وزرع الأفعال المعادية (العنصرية والكراهية) للأجانب.[4]

وتجدر الإشارة إلى أن معدل نمو هذه الجريمة يتزايد كل سنة ويتضاعف، وهذا ما بينته الإحصائيات والدراسات التي أجريت حولها، ومنها تلك التي تبين تلقي منظمة حكومة الإنترنت[5] حوالي 46000 شكوى متعلقة بتلك الجريمة[6].

الفرع الثاني: الأساليب المتبعة في ارتكاب جريمة المطاردة عبر الانترنت.

أصبح من المعتاد في الآونة الأخيرة استخدام الإنترنت كوسيلة يلجأ إليها الجاني لارتكاب جريمته وتحقيق أغراضه الإجرامية المطلوبة.وهناك عدة طرق يمكن للجاني استخدامها كوسيلة لارتكاب جريمة المطاردة عبر الإنترنت. أي أن ذلك السلوك يجد له متسعا عبر الانترنت. و من هذه الطرق:

أولا: استخدام البريد الالكتروني:

---

[1] – Cyber stalking : « is the use of the internet or other electronic means to stelk or harssemant individual or an organization.it may include false accusations monitoring ،making threats، identity theft ،or gathering information in order to harass ».Cyber stalking ,http:// www.wikipedia.org.

[2]– د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 475.

[3]– ينظر المادة 10 من قانون جرائم المعلوماتية السوداني لسنة2007.

[4]– Voir Josselyne ABADI : Du harcelement au reseau, au harcelement global,21 octobre 2011, p 8 et 13، http://conscience-vraie.info; Nicolas DESURMONT : Vers une problémitique du harcelement criminel en reseau، revue internationale de criminologie et de police technique، vol 49، juillet-septembre 2006، p 18 et suite.

[5]– منظمة حكومة الإنترنت: تأسست سنة 1986، وهي أقدم وأكبر منظمة أمنية في العالم .

[6] –Harassement statistic ,http:// www.haltabuse.org

وذلك بقيام الجاني بإرسال رسالة الكترونية إلى المجني عليه أو رسالة لحظية (MSM) يهدده بارتكاب جناية ضد نفسه أو ماله مثلا أو ضد نفس أو مال الغير، أو باسناد أمور خادشة للشرف أو بافشائها، سواء أكان ذلك مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل أو كان مقصودا به ذلك. ويجب أن يستمر ذلك الأخير في تهديده هذا، أي يجب أن يرتكب الجاني فعل المطاردة مرتين على الأقل لكي يمكن القول بتوافر الركن المادي كاملا في الجريمة [1]. و بذلك يعاقب ذلك الأخير وفقا للنصوص التقليدية لجريمة التهديد وخصوصا أن المشرع لم يهتم بالوسيلة التي ترتكب بها تلك الأخيرة.ولقد بلغت التهديدات والإهانات عن طريق رسائل البريد الالكتروني نسبة 88 , 39% أما عن طريق الرسائل الخطية فقد وصلت نسبتها 38, 69%.[2]

ثانيا: استخدام حلقات النقاش و غرف الدردشة:

كما يمكن لعضو الإنترنت القيام بمطاردة شخص آخر في حلقات النقاش أو ما يسمى بالمجموعات الإخبارية و غرف الدردشة بهدف تهديده و إزعاجه و بث الرعب و الخوف لديه. كما يمكن أن يتقمص شخصية المجني عليه في تلك الغرف أو يرسل رسائل باسمه إلى المجموعات الإخبارية، و غالبا ما يحدث في ذلك كأسلوب متعمد لإيذاء المجني عليه أو لدفع المستخدمين الآخرين للمشاركة في إزعاجه أو اهانته، و قد يتقمص تلك الشخصية للقيام بشراء بضائع أو خدمات باسمه.ولقد بلغت التهديدات أو الإهانات عن طريق غرف المحادثات نسبة 47.62 %. أما فيما يخص نسبة إرسال الإشاعات الكاذبة أو المعلومات الزائفة لتلك الغرف فوصلت إلى 24.40%. ووصلت تلك النسبة فيما يخص تشجيع المستخدمين الآخرين على مطاردة و إهانة و إزعاج المجني عليه نسبة 23.81%، و فيما يخص طلب شراء خدمات أو بضائع على حساب المجني عليه فبلغت 2.98% [3].

ثالثا: انشاء موقع ويب خاص بالجاني:

كما قد تقع جريمة المطاردة حين يقوم شخص بإنشاء موقع ويب خاص به و ينشر عليه تهديد لشخص آخر، أو كأن يقوم بتهديد بإتلاف محتويات أحد المواقع الخاصة بالمجني عليه أو أحد المواقع التي تهمه.[4]

و تجدر الإشارة إلى أنه لا يشترط نشاطا موحدا للمطاردة عبر الانترنت أو شكلا معينا. كما لو يقوم الجاني بمطاردة شخص آخر في حلقة نقاش ثم بعد ذلك يتولى مطاردته باستخدام البريد الإليكتروني أو بمراسلته عبر قاعدة بيانات سجل الزيارات في الصفحة الخاصة به على موقعه عبر الانترنت. كذلك لا يشترط أن يكون المظهر الإجرامي ظاهرا في سلوك الجاني. فأسلوب الحث على استمرار الحديث عبر حلقة النقاش مع شخص محدد ربما يكون ظاهرا منه حسن النية، و مع ذلك يكفي مجرد القيام بهذا النشاط للقول بتوافر الجريمة. ففي مثل هذه الحالة يكفي أن يكون المجني عليه غير مطمئن لاستمرار هذا

---

[1]– د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 479.

[2] –Harassement statistic, article disponible à l'adresse précédente .

[3]– بحث منشور على الإنترنت على .http://www.gn4me.com

[4]– سامح محمد عبد الحكم، المرجع السابق، ص 36.

الشخص في النقاش معه فإذا استمر الجاني في تتبع المجني عليه من غرفة إلى أخرى ففي هذه الحالة تتوافرالمطاردة، شريطة أن يكون المجني عليه قد أعلن له صراحة أو ضمنا – عدم القيام بالرد على مراسلات الجاني أو بإيجاب طلباته – ممانعته في استمرار النقاش معه أو مطالبته عبر البريد الاليكتروني بالكف عن مراسلته[1].

المطلب الثاني

موقف التشريعات المقارنة من جريمة المطاردة عبر الانترنت

و نتناول تحت هذا المطلب موقف التشريعات المقارنة من جريمة المطاردة عبر الانترنت، و ذلك بتقسيمها إلى موقفين نتطرق في الأول منهما إلى موقف التشريعات الغربية، لنبين في ثانيهما موقف التشريعات العربية. و ذلك في الفرعين التاليين:

الفرع الأول: موقف التشريعات الغربية من جريمة المطاردة عبر الانترنت.

الفرع الثاني: موقف التشريعات العربية من جريمة المطاردة عبر الانترنت.

الفرع الأول: موقف التشريعات الغربية من جريمة المطاردة عبر الانترنت.

و سيتم تبيان موقف التشريعات الغربية من جريمة المطاردة عبر الانترنت بتقسيمه إلى قسمين، نبين في الأول منهما موقف التشريع الفرنسي من هذه الجريمة، ثم نتناول في ثانيهما موقف التشريعات الأنجلوسكسونية منها. وذلك كالآتي:

أولا: موقف التشريع الفرنسي من جريمة المطاردة عبر الانترنت.

لقد نص المشرع الفرنسي على جريمة التهديد عبر الانترنت في المادة 222–18 من قانون العقوبات الفرنسي الجديد[2]. حيث تناول المشرع الفرنسي فيها عقاب كل من هدد غيره بأي وسيلة كانت بإرتكاب جناية أو جنحة ضد الأفراد و كان التهديد مصحوباً بطلب أو بتكليف بأمر بالحبس لمدة ثلاث سنوات وغرامة45000 يورو.و تضاعف العقوبة إلى الحبس 5 سنوات و غرامة 75000 يورو إذا كان التهديد يتعلق بالقتل.

يتضح من خلال هذا النص أن المشرع الفرنسي قد اعترف بارتكاب جريمة التهديد عبر الانترنت. ويستخلص هذا من العبارة التالية" كل من هدد بأي وسيلة كانت...."و لما كانت الانترنت عبارة عن وسيلة

---

[1] – د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 480.

[2] – 222–18 : « La menace، par quelque moyen que ce soit، de commettre un crime ou un délit contre les personnes، est punie de trois ans d'emprisonnement et de 45000 euros d'amende، lorsqu'elle est faite avec l'ordre de remplir une condition. La peine est portée à cinq ans d'emprisonnement et à 75000 euros d'amende s'il s'agit d'une menace de mort. »

اتصال يمكن استغلالها لبث رسائل الكترونية تحوي عبارات تهديد للغير أو عن طريق غرف الدردشة...، فإنه يمكن القول بامكانية تطبيق هذه المادة على التهديد الذي يتم بواسطة الانترنت.

ثانيا: موقف التشريعات الانجلوسكسونية من جريمة المطاردة عبر الانترنت.

ونتطرق تحت هذه النقطة إلى موقف التشريع الأمريكي ثم موقف التشريع الأنجليزي.

1/ موقف التشريع الأمريكي:

تم اصدار تشريعات لمكافحة جريمة المطاردة عبر الانترنت في 47 ولاية أمريكية، و بعضها يكتفي بوجود أي شكل من أشكال المطاردة، في حين يتطلب البعض الآخر قيام مرتكب الجريمة بإرسال تهديد حقيقي للمجني عليه و عائلته أو أي شخص[1].

كما أن هناك بعض الولايات الأخرى قامت بمد نطاق نصوص الاتصالات الهاتفية الفاحشة على أفعال الاتصال بشخص و تهديده بارتكاب ضرر به أو بعائلته باستخدام أجهزة اتصالات اليكترونية.و تعد من أوائل الولايات التي سنت تشريع يعاقب على ارتكاب جريمة المطاردة ولاية كاليفورنيا الأمريكية[2] cal.penal.code sec 646.9، و تلاها سبع ولايات أخرى و هي: Alaska، Connecticut، Delaware، Michigan، Montana، Oklahoma، Wyoming.[3]

ومن التشريعات الولائية الحديثة التي تأخذ بتقرير جريمة المطاردة عبر الانترنت تشريع ولاية أركنساس الأمريكية التي تجرم قيام أي شخص بغرض التخويف أو التهديد أو الإساءة بالقيام بمطاردة أي شخص باستخدام المراسلة أو البريد الاليكتروني أو أية وسائل اتصالية حاسوبية. و تتضمن هذه المراسلات التهديد بارتكاب أضرار مادية أو عدوان على الملكية أو كانت تحتوي هذه المراسلات على أسلوب فاحش أو فاسق[4].

و يجرم التشريع الفيديرالي الأمريكي المطاردة عبر الانترنت في القسم US Code 18 Section 2261A[5] و يعاقب عليها في ذات القسم Section 2261B.بعقوبة السجن لمدى الحياة إذا تسبب التهديد في موت الضحية أو السجن المؤقت أو لمدة 20 سنة[1].

---

[1] – د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص475.

[2]– اذ أصدر المشرع الكاليفورني ذلك القانون سنة 1990.

[3]– و كان ذلك 1999.

[4]– Voir Cyberstalking Laws,http:// www.haltabuse.org.

[5] –US Code 18 Section 2261A: "Whoever

(1) travels in interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States، or enters or leaves Indian country، with the intent to kill، injure، harass، or place under surveillance with intent to kill، injure، harass، or intimidate another person، and in the course of، or as a result of، such travel places that person in reasonable fear of the death of، or serious bodily injury to، or causes substantial emotional distress to that person، a member of the immediate family (as defined in section 115) of that person، or the spouse or intimate partner of that person; or

(2) with the intent

فقد أدين الطالب جاك باكر[2] بمقتضى نص القسم USCode Tit.18 sec.875(c) الذي يلزم للعقاب على مثل هذه الجريمة ثبوت ثلاث عناصر أساسية: القيام بالتداول بين الولايات، أن يكون هناك اتصال يتضمن التهديد، أن يكون التهديد بقصد إحداث ضرر أو خطف شخص آخر[3]. كما يعاقب على مطاردة

(A) to kill، injure، harass، or place under surveillance with intent to kill، injure، harass، or intimidate، or cause substantial emotional distress to a person in another State or tribal jurisdiction or within the special maritime and territorial jurisdiction of the United States; or

(B) to place a person in another State or tribal jurisdiction، or within the special maritime and territorial jurisdiction of the United States، in reasonable fear of the death of، or serious bodily injury to

(i) that person;

(ii) a member of the immediate family (as defined in section 115 of that person;or

(iii) a spouse or intimate partner of that person;

uses the mail، any interactive computer service، or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of، or serious bodily injury to، any of the persons described in clauses (i) through (iii) of subparagraph (B); shall be punished as provided in section 2261 (b) of this title."

[1] –Section 2261 (B):

"(b) Penalties.A person who violates this section or section 2261A shall be fined under this title، imprisoned

(1) for life or any term of years، if death of the victim results;

(2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results;

(3) (3) for not more than 10 years، if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense;

(4) as provided for the applicable conduct under chapter 109A if the offense would constitute an offense under chapter 109A (without regard to whether the offense was committed in the special maritime and territorial jurisdiction of the nited States or in a Federal prison); and

(5) for not more than 5 years، in any other case،or both fined and imprisoned.

(6) Whoever commits the crime of stalking in violation of a temporary or permanent civil or criminal injunction، restraining order، no–contact order، or other order described in section 2266 of title 18، United States Code، shall be punished by imprisonment for not less than 1 year."

[2]– ولد جاك باكر في مارس 1974، وكان طالبا جامعيا في جامعة Michigan في شعبة الآداب و الفنون و العلوم. و تتلخص وقائع هذه القضية أنه في جانفي 1995، قام جاك باكر ببث قصة حقيقية عن زميله جان دو باستخدام البريد الالكتروني و المجموعة الاخبارية يشرح فيها بالتفصيل كيفية الاغتصاب فالتعذيب فالقتل الذي كان ضحيتها. و على هذا الأساس تم توقيفه من قبل الشرطة الفديرالية على أساس أنه يمثل تهديدا لزملائه الطلبة من خلال بثه لتلك القصة. و تم إدانته بخمس تهم أهمها: تهمة إرسال تهديدات بجرح و خطف شخص عن طريق استخدام البريد الالكتروني (أي القيام بتداول تلك التهديدات عبر الإنترنت). ينظر لمزيد من التفاصيل عن وقائع هذه القضية

United States Cour of Appeals : USA v.Abraham Jacob Alkhabaz، January 29، 1997، 104f. 3d، 1492، http://en.wikipedia.org

[3] –Uscode Tit 18 Sec. 871: " (a) Whoever knowingly and willfully deposits for onveyance in the mail or for a delivery from any post office or by any letter carrier any letter، paper، writing، print، missive، or document containing any threat to take the life of، to kidnap، or to inflict bodily harm upon the President of the United

الرئيس الامريكي إذا اقترنت هذه المطاردة بتهديد ما بأي وسيلة اتصال (مكتوبة أو مقروءة أو مسموعة أو ورقية أو مطبوعة أو رسالة أو وثيقة)، و أن يكون التهديد ذا خصوصية صادرة عن الجاني وموجهة إلى الرئيس الأمريكي[1]، فعلى سبيل المثال تم معاقبة أربعة تلاميذ بريطانيين بحرمانهم من استخدام البريد الاليكتروني من مدرستهم و ذلك لقيامهم بارسال بريد اليكتروني بعنوان تهنئة بمناسبة أعياد عام 2000 إلى الرئيس الأمريكي السابق "بيل كلينتون " يطالبونه فيها بمليون دولار أمريكي و إلا سيفجرون البيت الأبيض[2].

كما تجدر الاشارة في هذا الصدد أنه تم التصديق مؤخرا في يناير 2006 على قانون أصدرته وزارة العدل الأمريكية حول العنف ضد المرأة، يقضي بتوقيع عقوبة السجن لمدة سنتين مع توقيع غرامة مالية ضد كل من يثبت أنه استخدم الانترنت في اخفاء شخصيته و يوجه رسائل أو كتابات بنية المضايقة أو الايذاء أو التهديد.[3]

2/ موقف التشريع الانجليزي:

و كما هو الشأن بالنسبة للولايات المتحدة الأمريكية، فقد تم اصدار قانونين في انجلترا لمكافحة جريمة المطاردة عبر الانترنت ألا و هما:

قانون الاتصالات لسنة 1984 و الذي يعد أول قانون يحكم واقعة المطاردة، حيث يعاقب القسم 43 منه على استخدام نظام اتصال عمومي لإرسال تهديدا أو موادا فاحشة أو مضرة[4]. وكذا قانون الحماية ضد الإزعاج لسنة 1997[5] و الذي يكمل القانون الأول.

States، the President- elect، the Vice President or other officer next in the order of succession to the office of President of the United States، or the Vice President-elect، or knowingly and willfully otherwise makes any such threat against the President، President-elect، Vice President or other officer next in the order of succession to the office of President، or Vice President-elect، shall be fined under this title or imprisoned not more than five years، or both.

(b) The terms "President-elect" and "Vice President-elect" as used in this section shall mean such persons as are the apparent successful candidates for the offices of President and Vice President، respectively، as ascertained from the results of the general elections held to determine the electors of President and Vice President in accordance with title 3، United States Code، sections 1 and 2. The phrase "other officer next in the order of succession to the office of President" as used in this section shall mean the person next in the order of succession to act as President in accordance with title 3، United States Code، sections 19 and 20".

[1] – لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، المرجع السابق، الهامش رقم 2 ، ص 480.

[2] – بحث جرائم الكمبيوتر و الإنترنت (الجريمة الاليكترونية)، www.islamonline.net/

[3] – سامح محمد عبد الحكم، المرجع السابق، ص35

[4] – Voir Louise ELLISON and Yaman AKDENIZ : Cyber-stalking، the Regulation of Harassment on the Internet ،Criminal Law Review، December 1998، Special Edition: Crime، Criminal Justice and the Internet، p6.

[5] – Cyberstalking , http://www.wikipedia.org.

الفرع الثاني: موقف التشريعات العربية من جريمة المطاردة عبر الانترنت.

و لتبيان موقف التشريعات العربية من هذه الجريمة التقليدية الواقعة عبر الانترنت قسمنا هذا الفرع إلى نقطتين الأولى خصصناها لتوضيح موقف هذه التشريعات بصفة عامة، أما الثانية فسلطنا الضوء فيها لموقف التشريع الجزائري من هذه الجريمة.

أولا: موقف التشريعات العربية بصفة عامة من جريمة التهديد عبر الانترنت.

إنقسمت التشريعات العربية في تكييفها لهذه الجريمة إلى قسمين: تشريعات عربية تطبق النصوص العقابية التقليدية الخاصة بجريمة التهديد على تلك الجريمة المستحدثة، لغياب تشريع جنائي خاص يواجه مثل تلك الآفات الإجرامية المستحدثة، و تشريعات عربية خصت هذه الجريمة بنصوص خاصة تلائم طبيعتها. ومن **التشريعات التي صمتت و اكتفت بتطبيق نصوص قوانينها العقابية التقليدية:**

قانون العقوبات الليبي في المواد 359-472[1]، و **قانون العقوبات المصري** في المواد 326-327[2]، **وقانون العقوبات البحريني** في المواد 389-390[3].... الخ.

---

[1]- تنص المادة 359 عقوبات ليبي:"يعاقب بالحبس مدة لا تزيد على سنة و بغرامة لا تقل على مائة دينار و لاتجاوز 500 دينار أو باحدى هاتين العقوبتين، كل من استعمل القوة أو العنف أو الإرهاب أو التهديد أو التدابير غير المشروعة، بقصد ارغام الغير على الامتناع عن العمل أو ارغام رب العمل على استخدام شخص ما أو مانعه من ذلك،و تطبق العقوبة ذاتها اذا كان القصد منع أي شخص من الاشتراك بأية نقابة.و يطبق حكم هذه المادة و ان استعملت القوة أو العنف أو الإرهاب أو التدابير غير المشروعة مع زوج الشخص أو مع أولاده. وتعد من التدابير غير المشروعة الأفعال الآتية على الأخص:
أولا:منع الشخص المقصود من مزاولة عمله باخفاء أدواته أو ملابسه أو أي شيء آخر مما يستعمله أو بأية طريقة أخرى، ثانيا: تتبعه بطريقة مستمرة في غدوه و رواحه، ثالثا: الوقوف موقف التهديد بالقرب من منزله أو بالقرب من أي مكان يقطنه أو يشتغل فيه".

[2]- تنص المادة 326 عقوبات مصري على:"كل من حصل بالتهديد على اعطائه مبلغا من النقود أو أي شيء آخر يعاقب بالحبس، ويعاقب على الشروع في ذلك بالحبس مدة لا تتجاوز سنتين ". و تضيف المادة 327 عقوبات مصري:"كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو السجن المشدد أو السجن أو بافشاء أمور أو نسبة أمور مخدشة بالشرف، و كان التهديد مصحوبا بطلب أو بتكليف بأمر، وكل من هدد غيره شفهيا بواسطة شخص آخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على 500جنيه سواء أكان التهديد مصحوبا بتكليف بأمر أم لا، و كل تهديد سواء أكان بالكتابة أو شفهيا بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على 200 جنيه."

[3]- تنص المادة 389 عقوبات بحريني:"كل من اغتصب بالقوة أو التهديد سندا مثبتا أو موجدا لدين أو تصرف أو براءة أو سندا ذا قيمة أدبية أو اعتبارية أو أوراقا تثبت وجود حالة قانونية أو اجتماعية أو أكره أحدا بالقوة أو التهديد على امضاء ورقة مما تقدم أو ختمها يعاقب بالأشغال الشاقة المؤقتة" وتضيف المادة 390 من ذات القانون على أنه:"كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقبا عليها بالقتل أو الأشغال الشاقة المؤبدة أو المؤقتة أو بافشاء أمور أو نسبة أمور مخدشة بالشرف، و كان التهديد مصحوبا بطلب أو بتكليف بأمر يعاقب بالسجن".

و لكنه في المقابل نجد بعض الدول العربية و التي تعد على الأصابع قد وضعت **نصوصا خاصة لمواجهة هذا السلوك الخطير و الأخطر باستعمال الانترنت** و منها:

السعودية من خلال المادة 3[1] من نظام مكافحة جرائم المعلوماتية السعودي ، وكذا **الامارات المتحدة العربية** في المادة 9[2] من القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، و كذا **السودان** من خلال المادة 10[3] من قانون جرائم المعلوماتية لسنة 2007.

ثانيا: موقف التشريع الجزائري من جريمة المطاردة عبر الانترنت:

عالج المشرع الجزائري جريمة التهديد من خلال قانون العقوبات الجزائري في مواده 284-287، اذ تنص المادة 284 عقوبات جزائري على:"كل من هدد بارتكاب جرائم القتل أو السجن أو أي اعتداء آخر على الأشخاص مما يعاقب عليها بالاعدام أو السجن المؤبد و كان ذلك بمحرر موقع أو غير موقع عليه، أو بصور أو رموز أو شعارات يعاقب بالحبس من سنتين الى عشر سنوات و بغرامة من 500 الى 5000 دج، اذا كان التهديد مصحوبا بأمر بايداع مبلغ من النقود في مكان معين أو بتنفيذ أي شرط آخر.

و يجوز علاوة على ذلك أن يحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 و بالمنع من الاقامة من سنة على الأقل الى خمس سنوات على الأكثر."

كما نص عليها في المادة 371 من قانون العقوبات و التي تضمت جريمة ابتزاز المال بالتهديد و التي عرفتها كمايلي: "كل من تحصل بطريق التهديد كتابة أو شفاهة أو بإفشاء او نسبة أمور شائنة على الأموال أو أوراق مالية أو على توقيع أو على المحررات المبينة في المادة 370".

يتضح من المادتين أن المشرع الجزائري:

---

[1]- تنص المادة 3 من نظام مكافحة جرائم المعلوماتية السعودي على:" يعاقب بالسجن مدة لا تزيد على سنة و بغرامة لاتزيد على 500ألف ريال، أو باحدى هاتين العقوبتين ؛كل شخص يرتكب أيا من الجرائم المعلوماتية التالية:.....2- الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا."

[2]- تنص المادة 9 من القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على: "كل من استعمل الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه يعاقب بالحبس مدة لا تزيد على سنتين و بالغرامة التي لاتزيد على 50ألف درهم أو باحدى هاتين العقوبتين، فان كان التهديد بارتكاب جناية أو باسناد أمور خادشة للشرف أو الإعتبار كانت العقوبة السجن مدة لا تزيد على عشر سنوات."

[3]- تنص المادة 10 من قانون جرائم المعلوماتية لسنة 2007 السوداني على:"كل من يستعمل شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها في تهديد أو إبتزاز شخص آخر لحمله علي القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الإمتناع مشروعاً، يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً."

– يعتبر أن التهديد هو ذلك الفعل الذي يقوم به الشخص و الذي ينذر آخر بخطر يريد إيقاعه بشخصه أو ماله أو هو الإعلان عن شر يراد إلحاقه بشخص معين أو بماله و من شأن ذلك أن يسبب له ضرر. و قد يكون ذلك بمحرر موقع عليه أو غير موقع عليه أو بصور أو رموز أو شعارات.[1] و هو نوعان إما أن يكون مصحوبا بأمر أو شرط و الذي يتحقق في التهديد الكتابي و التهديد الشفوي [2] أو بدونهما و الذي يتحقق في التهديد الكتابي لا غير[3].

و هو من الجرائم العمدية و يشترط توفر فيه القصدين العام و الخاص[4].

– يشترط لقيام جريمة الإبتزاز بالتهديد أربعة أركان و هي: أن يكون موضوع التهديد إفشاء أو نسبة أمور شائنة من شأنها تلطيخ سمعة المهدد أو تمس باعتباره، أن يكون التهديد بهدف الحصول على ربح غير شرعي و بهدف الحصول على مال أو توقيع أو محررات، أن يكون المهدد ذا نية سيئة (توفر القصد الجنائي).[5]

– لم يشر إلى إمكانية إرتكاب هذه الجريمة عبر الانترنت مسايرا في ذلك التشريعات العربية التي صمتت في مواجهتها لجريمة التهديد عبر الانترنت، و اكتفى بتطبيق نصوص قانون العقوبات التقليدية على تلك الجريمة.

و **من النماذج القضائية عن جريمة المطاردة عبر الانترنت:**

قضت محكمة جنايات الجيزة بمعاقبة الطبيب (أ.ي.ع)البالغ من العمر 28 سنة بالحبس سنة مع الشغل لاتهامه بمساومة موظفة ببنك لممارسة الفحشاء معها. وذلك بعد تهديدها بأمور تخدش الشرف عن طريق البريد الالكتروني، و كانت النيابة قد أحالت الطبيب للمحاكمة لاتهامه بتهديد الموظفة بنشر صورتها

---

[1]– ينظر جريمة التهديد في القانون الجزائري،http:// droit7.blogspot.com

[2]– التهديد المصحوب بأمر أو شرط : هو نوع من التهديد و يشترط لتكوين الجريمة توفر شروط معينة منها أن يحدث التهديد بالكتابة وأن يكون على درجة من الجسامة ومصحوبا بشرط أو أمر والتهديد الكتابي أشد وأخطر من الشفوي المنصوص عليه في المادة 286ق.ع.ج كونه يصدر دوما عن تصميم وتفكير سابق على خلاف التهديد الشفوي فإنه يصدر عن انفعال نفسي عارض و نتيجة ذلك نجد أن المشرع يعاقب على التهديد بالكتابة في كل الأحوال ووضع له عقوبات أشد من عقوبات التهديد الشفوي. لمزيد من التفاصيل حول التهديد الشفوي ينظر جرينة التهديد الشفوي، http://Jurispedia.org

[3]– التهديد الغير المصحوب بأمر أو شرط : و هو النوع الثاني من التهديد الذي نصت عليه المادة 285 قانون عقوبات جزائري بصورة واضحة و لكن يشترط المشرع من تكوينه أن يكون التهديد بالكتابة و أن يكون بالشيء مما ذكر في المادة السابقة و يعاقب على هذا النوع من التهديد بعقوبة أقل شدة وهي الحبس من سنة إلى 03 سنوات وغرامة من 500 إلى 2500 د.ج.

[4]– ينظر جريمة التهديد في القانون الجزائري،المنشورة على الموقع السابق.

[5]– لمزيد من التفاصيل ينظر د/دردوس مكي: القانون الجنائي الخاص في التشريع الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، قسنطينة، 2007، 74 و ما بعدها.

الحقيقية على صور جنسية مخلة بالآداب و نشرها عبر الانترنت، و طلب منها مبلغ 500ألف دولار، بالاضافة لممارسة الرذيلة معه لعدم تنفيذ التهديد.[1]

وقضت أحد المحاكم المصرية بحبس أحد مبرمجي الحاسب الآلي ستة أشهر، لاتهامه بممارسة الابتزاز والبلطجة ضد بعض الشركات عبر الانترنت، إذ قام بتهديد إحدى شركات التجارة و الخدمات بتدمير موقعها على شبكة الانترنت و تدمير قواعد المعلومات الموجودة بالموقع. كما هدد بالتشهير بها لدى عملائها إذا لم تدفع له مبلغ ألفي دولار.

و في الجزائر هدد بطال عشيقته بنشر و التشهير بصورها في مواقع التواصل الاجتماعي في الانترنت إن لم تقم سرقة مجوهرات جدتها.[2]

و في إحدى الدول الأوروبية تم ضبط أحد الأفراد بعد قيامه بتهديد شركة من شركة المياه الغازية طالبا مبلغا من المال مقابل عدم قيامه بوضع صورة زجاجة مياه غازية من إنتاج الشركة و بداخلها حشرة على موقع الانترنت[3].

ومن ناحية أخرى أدانت محكمة " Nanterre " بفرنسا قيام أحد الجناة ببعث رسالة تهديد عبر الانترنت عن طريق البريد الإلكتروني إلى احد رجال السياسة يهدده فيها بالقتل وحكمت عليه بالحبس لمدة شهرين مع الإيقاف[4].

و في بلجيكا هدد خبير كمبيوتر بلجيلكي عن طريق إرساله لرسالة الكترونية عبر موقع البريد الإلكتروني بصحيفة "هيت لانيست نيوز" بكسر شفرة كمبيوتر محولات الكهرباء في بلجيكا يوم الأربعاء 1999/12/29 في الفترة المسائية الممتدة بين 13h 30 إلى 15h30، و قطع الكهرباء على بلجيكا برمتها واصفا إياه بالأمر الهين و السهل[5].

وفي أمريكا و بالضبط في شهر أكتوبر 1999 قام شخص كندي يدعى " تيموثي أندرد " ببث رسالة الكترونية نصها " سوف أقتل الرئيس" من بريده الإلكتروني عبر الانترنت إلى الرئيس الأمريكي " بيل كلنتون"[6].

---

[1]– سامح محمد عبد الحكم، المرجع السابق، ص35 .

[2]– لمزيد من التفاصيل ينظر وقائع هذه القضية في جريدة النهار، العدد1323، فيفري 2012، ص9.

[3] – هشام فريد رستم،(الجوانب الإجرائية للجرائم المعلوماتية) مرجع سابق، ص 41

[4]– ينظر د/جميل عبد الباقي صغير، (القانون الجنائي والتكنولوجيا الحديثة) مرجع سابق، ص41 وما بعدها.

[5]– ينظر د/حسنين المحمدي بوادي، المرجع السابق، ص95

[6]– لمزيد من التفاصيل ينظر د/حسنين المحمدي بوادي، نفس المرجع ، ص 90–91. و من الأمثلة التي يذكرها د/ حسنين المحمدي بوادي في ذات مؤلفه: أنه في مناسبات أعياد الميلاد لسنة 2001، استغل أربعة تلاميذ بريطانيين من بلدة " جيراردكروس" في مقاطعة بكنجهام شاير في وسط بريطانيا هذه المناسبة في إرسال عبر شبكة الإنترنت برقية تهنئة إلى الرئيس الامريكي "كلينتون "، الا أنهم تمادوا في كتابتها إذ أضافوا إلى رسالتهم تلك عبارة: " أرسل مليون دولار والا سنفجر البيت الأبيض ". وفي قضية أخرى و بالضبط يوم 2001/09/12 أرسل الأمريكي االمسمى "كينيث هاريل" رسالة تهديد الكترونية على احد المواقع الرياضية الشهيرة، يهدد فيها بتفجير نهائيات بطولة البيسبول وقتل ما لا يقل عن ستين ألف

الفصل الثالث

الجرائم الأخلاقية عبر الانترنت

لقد ظهرت على شبكة الإنترنت مواقع مشبوهة جندت نفسها لهدف واحد هو الإخلال بالآداب العامة من خلال نشر الفساد والانحلال وهدم الأخلاق[1] والقيم التي تبنى عليها مجتمعاتنا لا سيما العربية المسلمة. فلقد وفرت أكثر الوسائل فعالية وجانبية لصناعة ونشر الإباحية الجنسية ولانتهاك الآداب والأخلاق العامة. وبرزت بذلك جرائم هدفها الوحيد الإطاحة بالآداب والأخلاق وجعلها في تدني مستمر في غياب الوازع الديني والرقابة الذاتية، سميت بالجرائم الأخلاقية، والتي يمكن تقسيمها إلى جرائم انتهاك الآداب العامة وجرائم جنسية.و التي سيتم تناولها في المبحثين التاليين:

المبحث الأول: جرائم انتهاك الآداب العامة الواقعة عبر الانترنت.

المبحث الثاني: الجرائم الجنسية الواقعة عبر الانترنت.

متفرج كان من المقرر ان يشاهدوا المباراة النهائية في الملعب وكان نص الرسالة كالتالي " المهمة لم تنتهي بعد.....نستعد لتفجير نهائي بطولة البيسبول و قتل ستين ألف أمريكي آخرين ".

كما هددت مجموعة تطلق على نفسها اسم (بانتس/هاجيس) بإطلاق فيروس يخرب الانظمة المعلوماتية في العالم، ان لم يتم إطلاق سراح صديقهم القرصان المعلوماتي المشهور " كيفن ميتنيك" الذي حكم عليه بالحبس لمدة 5 سنوات و الوضع تحت الرقابة لمدة 3 سنوات مع الإجبار على البقاء بعيدا على الوسائل الإلكترونية و شبكات المعلوماتية. و لقد ظهر هذا التهديد لفترة قصيرة على صفحة موقع " yahoo " على الإنترنت خلال شهر ديسمبر سنة 1997.ولقد كان نص رسالة التهديد كالتالي: " يوم عطلة الميلاد 1997 سيتحرك القسم المتفجر من هذا الفيروس لينشر الفوضى في جميع شبكات العالم سيكون بالإمكان تأمين "مضاد" لهذا الفيروس في حال أطلق سراح "كيفين ميتنيك".

وفي قضية أخرى هدد شاب أمريكي يدعى " جاها برج ويل " كل من مدير شركة ميكروسوفت و المدير التنفيذي لشركة MPI بنسف الشركة إذا لم تدفع له مبلغ 5 ملايين دولار أمريكي.

وفي كولومبيا وفي نوفمبر 1999 أرسل صبي لم يتجاوز عمره 12 عاما رسالة تهديد عبر الكمبيوتر الخاص بالعائلة إلى الرئيس الكولومبي " باسترانا" يهدد فيها بنسف موكبه الرئاسي وبقتله. ينظر ص 92 و ما بعدها.

[1]– تعرف الأخلاق بأنها:"تصور و قييم ما ينبغي أن يكون عليه السلوك متمشية في ذلك مع مثل أعلي أو مبدأ أساسي تضع له التصرفات الانسانية. ويكون مؤازر الجانب الخير في الطبيعة البشرية.محسن بن محسن بن باعث الرويلي، المرجع السابق، ص 24

المبحث الأول

جرائم انتهاك الآداب العامة الواقعة عبر الإنترنت.

يقصد بالآداب العامة: "مجموعة القواعد الأخلاقية الأساسية والتي تكون غايتها حفظ النظام في المجتمع"[1]. أو هي": ما تعارف عليه الناس من خروج على الاحتشام مما تحرج رؤيته أو سماع شعور الجمهور، كالصور والأفلام وغير ذلك... أيا كانت درجة الفحش الذي تمثله أو تنطوي عليه."[2]

ولقد جرمت معظم التشريعات العقابية هذا النوع من الجرائم والذي تتضمن أفعالا مخالفة لتعاليم كافة الأديان السماوية، وخاصة تعاليم ديننا الإسلامي الحنيف الذي يعتبر معيار الأخلاق فيه ثابت لا يتغير أبدا.على عكس التشريعات الأجنبية التي يصعب التوصل فيها إلى تبني قواعد مشتركة حول مواضيع حساسة كالأخلاق العامة أو حماية القاصرين أو كرامة الإنسان. فمعيار القيم الأخلاقية في الغرب يتغير بتغير الأزمان والأجيال، مثل التعري على الشواطئ وممارسة القبلات بالأماكن العامة بين الجنسين. فهذه التصرفات مقبولة لديهم وتدخل في إطار الحريات الشخصية. بالإضافة لتقبل بعض مجتمعاتهم للشذوذ الجنسي والزواج المثلي[3]. و السؤال المطروح هو ماذا نعني بهذه الجريمة الواقعة عبر الانترنت ؟ و ما هو التكييف القانوني لها ؟. و سيتم الإجابة على هذه الإشكالات وفق المطلبين التاليين:

المطلب الأول: ماهية جريمة انتهاك االآداب العامة الواقعة عبر الانترنت.

المطلب الثاني: موقف التشريعات المقارنة من جريمة انتهاك االآداب العامة الواقعة عبر الانترنت.

المطلب الأول

ماهية جريمة انتهاك الآداب العامة الواقعة عبر الانترنت

و سنتناول في هذا المطلب تعريف جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت في الفرع الأول ثم نبين بعد ذلك أركانها. و ذلك كمايلي:

الفرع الأول: تعريف جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت.

الفرع الثاني:أركان جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت.

الفرع الأول: تعريف جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت.

جريمة الاخلال بالآداب العامة هي كل فعل يتضمن مخالفة القواعد الأخلاقية الأساسية التي يبنى عليها المجتمع و كذا تعاليم كافة الأديان السماوية. وإذا كان الإنترنت يعد مكانا مطروقا من الكثير من

---

[1] – ابتسام القزام، المصطلحات القانونية في التشريع الجزائري، قاموس باللغتين العربية و الفرنسية، قصر الكتاب، البليدة، ص 41.

[2]– د/ جميل عبد الباقي الصغير: قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1998، ص 128.

[3]– د/مدحت رمضان، المرجع السابق،ص 145.

الشخصيات من كافة الجنسيات على مستوى العالم، يسمح بإجراء المبادلات الالكترونية صوتا وصورة وكتابة. فإن أي فعل منافي للحياء يرتكب من خلاله يعد تعرضا للأخلاق والآداب العامة، خصوصا وأن هذه الشبكات تتصف بصفة العلانية المشروطة لارتكاب تلك الجريمة. فهي زيادة على ما تتصف به من خصائص الطريق العام، بإمكان أي شخص من مرتاديها الإطلاع على تلك المواقع والصفحات الخادشة والمخلة بالحياء. وإن تم ذلك في مكان خاص يمكن لمن كان في مكان عام أن يراه كمقاهي الإنترنت مثلا.و عليه يمكن تعريف هذه الجريمة التقليدية التي تقع عن طريق الانترنت بأنها:"هي كل فعل يتضمن مخالفة القواعد الأخلاقية الأساسية التي يبنى عليها المجتمع و كذا تعاليم كافة الأديان السماوية و ذلك باستخدام الانترنت كنشر و بث الصفحات الخادشة والمخلة بالحياء عبر مواقعه أو إنتاج أو إعداد أو تهيئة أو إرسال أو تخزين أو ترويج أي محتوى يخل بالحياء أو النظام العام والآداب عن طريق شبكة المعلومات".

الفرع الثاني: أركان جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت.

تقوم جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت كغيرها من الجرائم على ثلاث أركان و هي الركن الشرعي و الركن المادي و الركن المعنوي.

أولا: الركن الشرعي.

و المتمثل في النصوص القانونية المجرمة لمثل هذا السلوك المشين و منها المادة 6 من نظام مكافحة الجريمة المعلوماتية السعودي و المادة 20 من القانون الإتحادي رقم 2 بشأن مكافحة جرائم تقنية المعلومات.[1]

ثانيا: الركن المادي.

يتضمن الركن المادي لجريمة انتهاك الآداب العامة الواقعة عبر الإنترنت العناصر الأساسية الآتية:

1/ ارتكاب السلوك الإجرامي، و يأخذ الصور التالية:

أ- إنشاء موقع الكتروني: لتســـــهيل او ترويج برامج أو أفكار مخالفة للنظام العام أو الآداب .

وإنشاء الموقع بوجه عام يتم بإحدى الطريقتين الآتيين:

الطريقة الأولى :وهي طريقة مجانية يتم بمقتضاها إنشاء الموقع عن طريق الدخول إلى موقع يقدم هذه الخدمة مجاناً، ثم تقديم المعلومات التي تريدها الشركة المزودة للخدمة التي بتقديمها يتم الإنشاء التلقائي للموقع.

الطريقة الثانية : و وفقاً لهذه الطريقة يتم إنشاء الموقع من خلال دفع تكلفة مالية بسيطة ووفق إجراءات معينة تبدأ بحجز دومين أي مجال معين للموقع يتم شراءه من قبل احد المواقع العالمية ثم تصميم صفحات الويب أي الشبكة من قبل مهندس متخصص، ثم بعد ذلك بث الموقع بالرجوع الى إحدى شركات المواقع

[1]- ينظر لمزيد من التفاصيل ص148 و ما بعدها من هذه الرسالة.

المتخصصة في تزويد خدمة الانترنيت مقابل مبلغ معين و عندما تعمد إحدى الشركات إلى إنشاء موقع ما لأحد العملاء تقوم باستخدام جهاز خدمة امن وبمقتضاه يتفق الحاسبان على استخدام رموز مشفرة تستخدم تقنية تامين البيانات في تفكيكها وإعادة جمعها .[1]

ب- أن يعد الجاني أو يهيء ، أويرسل ،أو يخزن ،أو يروج أي محتوي مخل بالنظام العام او الآداب:

فأما بالنسبة لإعداد المحتوي ، فمثالها أن يقوم الشخص بتصوير صور فاضحة ، أويكتب كلاماً فاحشاً، أماالتهيء لهذا الفعل فمثاله أن يقوم بتجهيز جهاز الحاسوب أو يساهم في إحضار الأشخاص للتصوير أو جمع الصور أو الأقوال المنافية للآداب .

أما إرسال المحتوي المخالف للنظام العام و الآداب العامة فيكون عن طريق البريد الإلكتروني أو الرسائل القصيرة بجهاز الهاتف المحمول ، أما بالنسبة لتخزين المحتوى في ذاكرة أجهزة الحاسوب او الهاتف المحمول المربوط بالإنترنت ومافي حكمها ، وأما فيما يخص الترويج للمحتوي فيكون ذلك بإرسال الرسائل بأي وسيلة إلكترونية للحث على دخول موقع يحتوي عليها أو الترويج لشرائها أو تداولها [2].

2/ النتيجة:

تعتبر جريمة إنتهاك الآداب العامة الواقعة عبر الإنترنت من جرائم الخطر التي لا يشترط لقيامها تحقق النتيجة الجرمية إذ يعتبر السلوك الإجرامي المتمثل في إنشاء موقع إلكتروني أو نشر معلومات تحوي بيانات مخالفة للنظام العام و الآداب العامة مهددا في حد ذاته للصالح العام، أي أن الجريمة تتحقق بمجرد إرتكاب السلوك الإجرامي.[3]

3/ وسيلة إرتكاب الجريمة: و التي يجب أن تتمثل في شبكة الإنترنت دون غيرها من وسائل التقنية العالية.[4]

ثالثا:الركن المعنوي

إن جريمة إنتهاك الآداب العامة الواقعة عبر الإنترنت هي من الجرائم العمدية القائمة على القصد الجنائي العام بعنصريه من علم للجاني بأن سلوكه من شأنه الإخلال بالآداب العامة إلى جانب إنصراف إرادته إلى ذلك.[5]

---

[1]- لمزيد من التفاصيل ينظر نوفل علي عبد الله، محمد عزت: جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، مجلة الرافدين للحقوق، المجلد 12، العدد 44، السنة 2010، ص 18 و ما بعدها.

[2]-نقلا عن د/إبراهيم قسم السيد: شرح قانون جرائم المعلوماتية السوداني لسنة 2007 مقارنا بالقانون السعودي و الإماراتي، ص 14.

[3]- ينظر نوفل علي عبد الله، محمد عزت، المرجع السابق، ص 22.

[4]-ينظر د/إبراهيم قسم السيد، المرجع السابق، ص 12 و مابعدها.

[5]-ينظر د/إبراهيم قسم السيد، نفس المرجع ، ص 13.

المطلب الثاني

موقف التشريعات المقارنة من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

وسنبين في هذا المطلب موقف التشريعات الغربية أولا من هذه الجريمة، ثم نعرض بعد ذلك إلى توضيح موقف التشريعات العربية منها. و ذلك في الفرعين التاليين:

الفرع الأول: موقف التشريعات الغربية من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

الفرع الثاني: موقف التشريعات العربية من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

الفرع الأول: موقف التشريعات الغربية من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

و سيتم تقسيم هذا الفرع إلى نقطتين نحدد في أولاهما موقف التشريع الفرنسي من هذه الجريمة، و في ثانيهما موقف التشريع الأمريكي باعتباره نموذجا للتشريعات الأنجلوسكسونية. و ذلك كمايلي:

أولا: موقف التشريع الفرنسي من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

تناول المشرع الفرنسي جريمة انتهاك الآداب العامة بصفة عامة في قانون العقوبات الفرنسي القديم و ذلك من خلال المادتين 283 و 284. اذ تعاقب المادة 283 بالحبس لمدة لا تقل عن شهر و لاتزيد على سنتين و بغرامة لاتقل عن 360 فرنك فرنسي و لا تزيد على 30000 فرنك فرنسي كل من صنع أو حاز بقصد الاتجار أو التوزيع أو التأجير أو الإعلان أو العرض أو استورد بنفسه أو بالوساطة أو صدر أو صدر بالواسطة أو نقل أو نقل بالواسطة عمدا و لذات الغرض، أو أعلن أو عرض أو نشر على الجمهور، أو باع أو أجر أو عرض للبيع أو للايجار حتى في غير علانية، أو أعطى، و لو دون مقابل، و لو في غير غلانية، بأي شكل كان، بصورة مباشرة أو ملتوية، أو وزع أو أعطى بقصد التوزيع بأي وسيلة كانت كل مطبوعات أو كتابة أو رسم أو ملصقات أو حفر أو صور أو كل شيء أو صورة مخلة بحسن الآداب[1].

---

[1] – Article 283 : « Sera puni d'un emprisonnement d'un mois à deux ans et d'une amende de 360 F à 30.000 F quiconque aura :

Fabriqué ou détenu en vue d'en faire commerce، distribution، location، affichage ou exposition ;

Importé ou fait importer، exporté ou fait exporter، transporté ou fait transporter sciemment aux mêmes fins ;

Affiché، exposé ou projeté aux regards du public ;

Vendu، loué، mis en vente ou en location، même non publiquement ;

Offert، même à titre gratuit، même non publiquement، sous quelque forme que ce soit، directement ou par un moyen détourné ;

Distribué ou remis en vue de leur distribution par un moyen quelconque،

Tous imprimés، tous écrits، dessins، affiches، gravures، peintures، photographies، films ou clichés، matrices ou reproductions phonographiques، emblèmes، tous objets ou images contraires aux bonnes moeurs.

أما المادة 284 فتعاقب بذات العقوبات السابقة على كل من أذاع علانية أغاني أو صياح أو حديث يخل بالآداب العامة. و كذلك كل من قام علانية بجذب الانتباه إلى حالة من حالات الانحلال أو نشر إعلانا أو مراسلة من هذا النوع أيا ما كانت العبارات.[1]

أما فيما يخص جريمة انتهاك الآداب العامة الواقعة عبر الانترنت فقد تناولها في المادة 227-24 في فقرتها الأولى[2] من قانون العقوبات الفرنسي المعدل و المتمم بالقانون 2007-297 المؤرخ في 5 مارس 2007، إذ عاقبت هذه المادة كل من صنع أو نقل أو نشر أو باع كل دعامة تحوي مراسلات ذات طابع عنيف أو مخلة بالآداب و الأخلاق العامة أو تمس بالكرامة الإنسانية بالحبس لمدة ثلاث سنوات و بغرامة مالية تقدر ب75000 يورو إذا تم عرضها و رؤيتها من قبل قاصر.

ثانيا: موقف التشريع الأمريكي من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

تناول المشرع الأمريكي جريمة انتهاك الآداب العامة الواقعة عبر الانترنت في القسمين 1462 و1465 من الباب 18. حيث جرم في القسم 1462 من الباب 18 كل استخدام لكلمات فاحشة بطريق المراسلة سواء أكانت على شكل كتاب أو كتيب أو صورة أو رسالة أو أي وسيلة إعلانية تحوي كل مادة فاحشة أو بذيئة.[3] وجرم في القسم 1465 من الباب 18 كل نقل أو إنتاج لمواد فاحشـــة موجودة في كتب أو صور أو

Le condamné pourra en outre faire l'objet، pour une durée ne dépassant pas six mois، d'une interdiction d'exercer، directement ou par personne interposée، en droit ou en fait، des fonctions de direction de toute entreprise d'impression، d'édition ou de groupage et de distribution de journaux et de publications périodiques. Quiconque contreviendra à l'interdiction visée ci-dessus sera puni des peines prévues au présent article. »

[1]- Article 284 : « Sera puni des mêmes peines:

Quiconque aura fait entendre publiquement des chants، cris ou discours contraires aux bonnes moeurs ;

Quiconque aura publiquement attiré l'attention sur une occasion de débauche ou aura publié une annonce ou une correspondance de ce genre، quels qu'en soient les termes. »

[2]-227-24 : « Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur ».

[3] -18 usc sec 1462 : « Whoever brings into the United States، or any place subject to the jurisdiction thereof، or knowingly uses any express company or other common carrier or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934)، for carriage in interstate or foreign commerce

(a) any obscene، lewd، lascivious، or filthy book، pamphlet، picture، motion-picture film، paper، letter، writing، print، or other matter of indecent character; or

(b) any obscene، lewd، lascivious، or filthy phonograph recording، electrical transcription، or other article or thing capable of producing sound; or

(c) any drug، medicine، article، or thing designed، adapted، or intended for producing abortion، or for any indecent or immoral use; or any written or printed card، letter، circular، book، pamphlet، advertisement، or notice

فيلم أو ورقة أو رسالة أو طباعة قصد بيعها أو توزيعها.[1]

الفرع الثاني: موقف التشريعات العربية من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

و على غرار الفرع الأول سنقسم هذا الفرع إلى نقطتين نوضح في أولهما موقف التشريعات العربية بصفة عامة، أما في النقطة الثانية فسنخصصها لتبيان موقف التشريع الجزائري. و ذلك كمايلي:

أولا: موقف التشريعات العربية بصفة عامة من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت.

انقسم موقف التشريعات العربية حيال جريمة انتهاك الآداب العامة الواقعة عبر الانترنت، فأغلبيتها اكتفت بتطبيق نصوص قوانينها العقابية التقليدية عكس الأقلية التي خصت لمواجهة هذه الجريمة التقليدية الواقعة عبر الانترنت قوانين خاصة تحوي نصوصا تتلاءم مع طبيعة هذه الجريمة. و من **التشريعات العربية التي اكتفت بتطبيق قوانين عقوباتها التقليدية لمواجهة هذه الجريمة:**

المشرع الأردني و الذي جرم التعرض للآداب والأخلاق العامة من خلال نص المادتين 319 و320 من قانون العقوبات الأردني.[2] فأما المادة الأولى منهما فحرصت على تجريم أية مادة بذيئة مطبوعة أو مخطوطة أو أية صورة شمسية أو رسم أو نموذج أو أي شيء آخر يؤدي إلى إفساد الأخلاق، وذلك إذ ما تم بيعها أو إحرازها بقصد البيع أو التوزيع. ويشمل التحريم كذلك كل من طبع أو أعاد طبع مثل هذه المواد بأية طريقة أخرى، شريطة أن يكون ذلك بقصد بيعها أو توزيعها.

ويجرم المشرع الأردني كل عرض لتلك المواد البذيئة في محل عام أو توزيعها لعرضها في مكان عام، سواء تمثلت في أي تصوير أو صورة شمسية أو رسم أو نموذج بذيء أو أي شيء آخر طالما يفسد الأخلاق. ويمتد نطاق التجريم أيضا ليشمل كل من أدار أو اشترك في إدارة محل يتعاطي بيع أو نشر أو

---

of any kind giving information، directly or indirectly، where، how، or of whom، or by what means any of such mentioned articles، matters، or things may be obtained or made; or

Whoever knowingly takes or receives، from such express company or other common carrier or interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934) any matter or thing the carriage or importation of which is herein made unlawful

Shall be fined under this title or imprisoned not more than five years، or both، for the first such offense and shall be fined under this title or imprisoned not more than ten years، or both، for each such offense thereafter".

[1] – 18 usc 1465 : « Whoever knowingly produces with the intent to transport، distribute، or transmit in interstate or foreign commerce، or whoever knowingly transports or travels in، or uses a facility or means of، interstate or foreign commerce or an interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934) in or affecting such commerce، for the purpose of sale or distribution of any obscene، lewd، lascivious، or filthy book، pamphlet، picture، film، paper، letter، writing، print، silhouette، drawing، figure، image، cast، phonograph recording، electrical transcription or other article capable of producing sound or any other matter of indecent or immoral character، shall be fined under this title or imprisoned not more than five years، or both.

The transportation as aforesaid of two or more copies of any publication or two or more of any article of the character described above، or a combined total of five such publications and articles، shall create a presumption that such publications or articles are intended for sale or distribution، but such presumption shall be rebuttable.

[2] – ينظر المادة 319 و 320 من قانون العقوبات الأردني.

عرض أشياء بذيئة مطبوعة كانت أو مخطوطة أو صورة شمسية أو رسم أو نماذج أو أية أشياء أخرى قد تؤدي إلى إفساد الأخلاق. وكل من أعلن أو أذاع بأية وسيلة من الوسائل أن شخصا يتعاطى بيع هذه المواد أو طبعها أو عرضها أو توزيعها.

وتجدر الإشارة إلى أن عبارة أية وسيلة أخرى تشمل الوسائل الحديثة التي يكشف عنها العلم كالإنترنت مثلا.

أما التجريم الثاني الذي جاء به المشرع الأردني فيتمثل في إتيان الفعل المنافي للحياء أو إبداء إشارة منافية للحياء في مكان عام أو في مجتمع عام أي علنا، وهذا ما جاءت به المادة 320 من قانون العقوبات الأردني.[1]

أما بالنسبة **للمشرع المصري** فقد وردت الأحكام الخاصة بجريمة الإخلال بالآداب العامة في المادتين 178 و 178 مكرر. ودرء للتكرار فقد جرم المشرع المصري المواد البذيئة التي تؤدي إلى إفساد الأخلاق، والتي سبق سردها. ولكنه أضاف الصور المحفورة أو منقوشة اليدوية أو الصور العام إذا كانت منافية للآداب. أما المادة 178 مكرر فقد حمل فيها المسؤولية الجنائية الكاملة لرؤساء التحرير والناشرون إذا ارتكبت تلك الجريمة المنصوص عليها في المادة 178 عن طريق النشر[2].

أما بالنسبة للمشرع البحريني فقد تناول الجرائم المتعلقة بالكتابات أو الرسومات أو الصور أو الأفلام أو الرموز المخلة بالآداب العامة بمقتضى نص المادة 355 عقوبات. أما المادة 356 من ذات القانون فقد جرمت كل نداء أو صياح أو خطابا مخالفا للآداب بشرط أن يكون ذلك علنا وجهرا.[3]

والمشرع بتجريمه لمثل هذه الأفعال المنافية للأخلاق أراد حماية مصلحة معينة وهي الحياء العام. وبالتالي فالقانون أراد بتلك النصوص حماية هذه المصلحة في مواجهة ما يخدش هذا الحياء، وما يستدرج أفراد المجتمع بغرض إفساد أخلاقهم. وتعتبر هذه الجريمة من جرائم الخطر العام لكونها تعرض المصلحة المحمية للخطر، وبالتالي فلا يشترط لوقوعها حدوث ضرر[4].

وعلى عكس التشريعات العربية السابقة وجدت **تشريعات عربية وضعت نصوصا قانونية خاصة لمواجهة هذه الجريمة الخطيرة الواقعة على الأخلاق و الماسة بالآداب العامة و النظام العام** ، و من هذه التشريعات نجد **المشرع السوداني** و الذي جرم هذه الأفعال المخلة بالآداب و الواقعة عبر الانترنت من خلال قانون جرائم المعلوماتية السوداني لسنة 2007 في فصله الرابع بحيث اعتبر الإخلال بالنظام العام والآداب العامة:"كل فعل يقوم به شخص ويتضمن إنتاج أو إعداد أو تهيئة أو إرسال أو تخزين أو ترويج أي محتوى يخل بالحياء أو النظام العام والآداب عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما

---

[1]– محمد دأمين أحمد الشوابكة، المرجع السابق، ص 109.

[2]– د/ مدحت رمضان، المرجع السابق، ص 144.

[3]– سامح محمد عبد الحكم، المرجع السابق، ص 63–64.

[4]– د/ أحمد فتحي سرور: الوسيط في قانون العقوبات، القسم الخاص، الطبعة الرابعة، دار الطباعة الحديثة، القاهرة، 1990، ص 686.

في حكمها".أويقصد به:"أي شخص يوفر أو يسجل عمدا أو بإهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمه لأي شخص آخر للوصول لمحتوى مخل بالحياء أو مناف للنظام العام أو الآداب"[1]. كما اعتبر تعرضا للنظام العام والآداب كل:"إنشاء أو نشر أو استخدام مواقع على الشبكة أو أحد أجهزة الحاسوب أو ما في حكمها لتسهيل أو ترويج برامج أو أفكار تؤدي إلى إفساد الأخلاق"[2].

أما **المشرع السعودي** فقد تناولها في نظام مكافحة الجريمة المعلوماتية في المادة 1/6 منه، إذ اعتبره:"كل إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي"، وكذا **المشرع الإماراتي** حيث تناولها في المادة 20 من قانون الاتحادي رقم (2) لسنة 2000 بشأن مكافحة جرائم تقنية المعلومات وذلك كما يلي: "كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية وإحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة يعاقب بالحبس مدة لا تزيد عن خمس سنوات."

ثانيا: موقف التشريع الجزائري من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت

تناول المشرع الجزائري جريمة التعرض للآداب والأخلاق بصورتها التقليدية في القسم السادس من الكتاب الثالث في المواد 333 – 341 من قانون العقوبات الجزائري، تحت عنوان " انتهاك الآداب"، بحيث حرص على تجريم في المادة 333 مكرر[3] صنع أو حيازة أو استيراد أو السعي نحو الاستيراد من أجل التجارة أو توزيع أو تأجير أو تلصيق أو البيع أو الشروع فيه أو التوزيع أو الشروع فيه كل مادة بذيئة تؤدي إلى افساد الأخلاق وإلى الإخلال بالحياء والمتمثلة إما في مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صورا فوتوغرافية أو أصل الصورة أو إنتاج أي شيء آخر يسعى إلى هدف الإخلال بالحياء.

ويجرم كذلك عرض تلك المواد البذيئة أو الشروع في عرضها للجمهور في أماكن عامة، كإقامة المعارض .

---

[1]– تنص المادة 14. من قانون جرائم المعلوماتية السوداني على:"(1) كل من ينتج أو يعد أو يهيئ أو يرسل أو يخزن أو يروج عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها،أي محتوى مخل بالحياء أو النظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً.

(2) كل من يوفر أو يسهل عمداً أو بإهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها للوصول لمحتوى مخل بالحياء أو منافٍ للنظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً .

(3) إذا وجه الفعل المشار إليه في البندين (1) و(2) إلى حدث يعاقب مرتكبها بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً".

[2]– تنص المادة 15 من ذات القانون على :" كل من ينشئ أو ينشر أو يستخدم موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسوب أو ما فى حكمها لتسهيل أو ترويج برامج أو أفكار مخالفة للنظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز .ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً. "

[3]– ينظر المادة 333 مكرر من قانون العقوبات الجزائري.

وتجدر الإشارة إلى أن المشرع الجزائري وسع في نطاق التجريم عندما أورد عبارة: "إنتاج أي شيء آخر"، بحيث يشمل صنع وإنتاج كل المواد البذيئة غير المذكورة في المادة وطرق تكوينها، والتي قد تكشف عنها التكنولوجيا. كتلك المتعلقة بالتقنية الرقمية والتي تشمل على تركيب ودمج الصور.

ويعتبر أيضا تعرضا للآداب والأخلاق العامة اتيان الفعل الفاضح المخل للحياء علنا. وهذا ما نصت عليه المادة 333 من قانون العقوبات الجزائري والذي يقصد به: "كل سلوك عمدي يخل بحياء من تلمسه حواسه".[1]

و على هذا فالمشرع الجزائري يصنف ضمن التشريعات العربية التي صمتت عن تجريم هذه الجريمة واكتفت بتطبيق نصوص قوانينها العقابية التقليدية. و في هذا يرى البعض أنه وإن أمكن التعرض للآداب والأخلاق العامة لمستخدمي الإنترنت بأحد الأفعال الواردة في المواد السابقة في مختلف القوانين السابقة- المشار إليها- فإن هذه النصوص لا يمكن التوسع فيها لتنطبق على جريمة انتهاك الآداب والأخلاق العامة عبر الإنترنت. لأن القياس في النصوص الجزائية أو التوسع فيها ممنوع وفقا للمبادئ المتعارف عليها في القانون الجنائي . ولهذا وجب على المشرع العربي **(الجزائري، المصري، الأردني...)** تعديل هذه النصوص وفقا لمتطلبات التطور التكنولوجي الذي نعيشه في عصرنا هذا عصر المعلوماتية، بحيث يجب النص على تجريم التعرض للآداب والأخلاق العامة عبر الإنترنت صراحة تطبيقا لمبدأ شرعية الجرائم والعقوبات وتدابير الأمن.[2]

والسؤال المطروح هنا هو: هل مزودي خدمة الإنترنت [3] ومقدمي هذه الخدمة – أصحاب مقاهي الإنترنت- مسئولون جنائيا عن ما يتم تداوله من مواد بذيئة تؤدي إلى إفساد الأخلاق؟

اختلف الفقه الجنائي والقوانين المقارنة حول قيام المسؤولية الجنائية ضد مزود الخدمة من عدم قيامها في أي حال من الأحوال. ومن الدول التي اتجهت قوانينها بالفعل إلى تحميل مزود الخدمة أو مقدمها للمسؤولية الجنائية إذا ما أخل بالالتزامات والواجبات المفروضة عليه:

الولايات المتحدة الأمريكية، وذلك من خلال قانون آداب الاتصالات[4].

فرنسا، وذلك من خلال قانون الاتصال عن بعد[5].

---

[1]- د/ محمد صبحي نجم، المرجع السابق،ص83.

[2]- ينظر محمد أمين أحمد الشوابكة، المرجع السابق، ص 110.

[3]- مزود خدمة الإنترنت أو متعهد الوصول هو الوسيط بين مستخدمي الإنترنت وبين موردي الخدمات و يتم عن طريقه اتصال مستخدمي الإنترنت بالمواقع التي يرغبون في الدخول عليها. لمزيد من التفاصيل ينظر د/ عبد الفتاح كيلاني: مدى المسؤولية القانونية لمقدمي خدمات الإنترنت، ص 39 و مابعدها.

[4]- لمزيد من التفاصيل ينظر د/عمر محمد أبو بكر بن يونس، المرجع السابق، ص449.

[5]- لمزيد من التفاصيل ينظر سامح محمد عبد الحكم، المرجع السابق، ص72.

-Alexandra GREENWOOD : Le statut de l'hebergeur et le web 2.0، mémoire master 2 professionnel- droit de l'internet public، Université Paris، Sorbonne، Année Universitaire 2008-2009، p 23 et suite.

الأردن، وذلك من خلال قانون الاتصالات رقم: 13 لسنة 1995 في المادة 75 فقرة (ب)[1].

الجزائر، و ذلك من خلال المرسوم التنفيذي رقم 98-256 المعدل و المتمم للجزء التنظيمي من الأمر 75- 89 و المتضمن قانون البريد و المواصلات في المادة 14 التي تنص على مسؤولية مزودي خدمات الانترنت عن المادة المنشورة و المواقع التي يقومون باستضافتها. و ينص نفس المرسوم على ضرورة اتخاذهم كافة الاجراءات المطلوبة للتأكد من وجود رقابة دائمة على المحتوى لمنع الوصول الى المواد التي تتعارض مع الأخلاق أو ما يوافق الرأي العام[2].

أما غيرها من الدول فاكتفت بوضع برامج لمنع المواقع المخلة بالآداب العامة من قبل المؤسسة المعنية بالاتصالات أو الهيئة المختصة بالاتصالات التي تزود المشتركين بخدمات الانترنت. و يطلق على تلك الأخيرة اسم البروكسي (proxy) وهي عبارة عن برامج تتلخص مهمتها في منع أي شخص من الاتصال بمثل هذه الأماكن فتعمل كجدار ناري يمنع الدخول لهذه المواقع إلا بكلمة سر معينة.[3]

المبحث الثاني

الجرائم الجنسية عبر الانترنت.

تعتبر شبكة الإنترنت سلاح ذو حدين، فهي إما تستخدم في نشر العلم والخير وتبادل الثقافات وتثبيت العقيدة، أو تكون وسيلة للإفساد والانحراف ونشر الانحلال مهدم للقيم وذلك نظرا لما تشهده من جرائم مخلة بالأخلاق والعرض والآداب العامة وخاصة تلك المسماة بالجرائم الجنسية إذ صارت تلك الشبكة تمثل في الوقت الحالي تربة خصبة لمثل تلك الجرائم.أو بالأحرى تحولت تلك الأخيرة إلى أرشيف ضخم تجمع فيه الصور الماجنة والمقالات الفاضحة والأفلام الخليعة والتي تبث عبر مواقع مخصصة لذلك، غايتها تحقيق

---

[1]- لمزيد من التفاصيل ينظر محمد أمين أحمد الشوابكة، المرجع السابق، ص 114 و ما بعدها.

[2]- تنص المادة 6/14 و7 و8 من المرسوم التنفيذي رقم 98-256 المعدل و المتمم للجزء التنظيمي من الأمر 75-89 والمتضمن قانون البريد و المواصلات على:"يلتزم مقدم خدمات أنترنات خلال ممارسة نشاطاته بما يأتي:

- احترام قواعد حسن السيرة بالامتناع خاصة عن استعمال أية طريقة غير مشروعة سواء تجاه المستعملين أو تجاه مقدمي خدمات الانترنات الآخرين،
- تحمل مسؤولية محتوى الصفحات و موزعات المعطيات التي يستخرجها و يأويها، طبقا للأحكام التشريعية المعمول بها،
- اتخاذ كل الاجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه، قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق."

[3]- د/ بيومي حجازي،(الأحداث و الإنترنت) مرجع سابق، ص134 و ينظر لمزيد من التفاصيل د/ ممدوح عبد الحميد: جرائم استخدام شبكة المعلومات العالمية، جرائم الإنترنت من منظور أمني، بحث مقدم إلى مؤتمر القانون و الكمبيوتر والإنترنت، كلية الشريعة و القانون، جامعة الامارات العربية المتحدة، ماي2000،ص 29.

الربح المادي تسمى بالمواقع الجنسية الإباحية unihibited locatins وعن طريق الدردشة الإباحية والقوائم البريدية الجنسية.[1] التي أصبحت تجتاح عالمنا وتقتحم منازل ومكاتب الجميع.

و تعرف الجرائم الجنسية أو مايطلق عليها بالجرائم الاباحية[2] بصفة عامة بأنها:"تلك الجرائم التي ترتكب من قبل جاني على مجني عليه في شرفه أو عرضه حيث يمس الجاني شرف المجني عليه أو عرضه بإيقاعه فعل جنسي عليه قد يكون لمس أو تقبيل أو وطء،و ذلك يكون دون رغبة من المجني عليه أو بالكراهية أو التي ترتكب من قبل فاعلين مشتركين في الجريمة بالاتفاق حيث يكون الفاعل والمفعول به جناة مساهمين في الجريمة."[3] أو هي:" كل عمل يستخدم لغرض الاثارة الجنسية".أو:" كل عمل يرى جمهور الناس على أنه فاحش أو داعر".أو: "كل عمل تم انجازه بهدف اثارة الشهوة الجنسية لدى جمهور المشاهدين أو المستمعين أو القراء"[4]. و السؤال المطروح هنا هو: ماذا نعني بهذه الجريمة الواقعة عبر الانترنت ؟ و ما هي أسبابها ؟و ما هي الطرق المستعملة لانتشار الجنس عبر الانترنت؟ و ماهو موقف التشريعات المقارنة من هذه الجريمة؟. و سيتم الاجابة على هذه الاشكالات بتقسيم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: ماهية الجرائم الجنسية عبر الانترنت.

المطلب الثاني: موقف التشريعات المقارنة من الجرائم الجنسية عبر الانترنت.

---

[1]– تختلف المواقع الإباحية عن القوائم البريدية في كون أن هذه الأخيرة سهلة الإنشاء وغالبا ما تكون مجانية يتبادل فيها أعضاؤها المشتركون الصور والأفلام الإباحية بالإرسال والاستقبال على عناوينهم البريدية وذلك بشكل يومي. ضف إلى ذلك فإن القوائم البريدية تكون أبعد عن إمكانية المتابعة الأمنية حيث يركز نشاطها على الرسائل البريدية.

أما المواقع الإباحية فكما سبق ذكره أعلاه غالبا ما يكون الهدف منها تحقيق الربح المادي، حيث يستلزم على متصفح هذه المواقع دفع مبالغ معينة مقابل مشاهدة فيلم إباحي لوقت محدد أو دفع اشتراك شهري أو سنوي مقابل الاستفادة من خدماتهذه المواقع، وإن كانت البعض منها تحاول جذب مرتاديها عن طريق إرسال صور جنسية مجانية يومية على عناوينهم البريدية. ضف إلى ذلك وعلى عكس القوائم البريدية فإن تصفح مثل هذه المواقع يستلزم الاتصال المباشر بشبكة الإنترنت، الأمر الذي يتيح لبعضالدول إمكانية حجب هذه المواقع من خلال فلترتها من قبل الحكومة. فلا يمكن الوصول إليه إلا باستخدام البر وكيسي و ذلك ما حصل في الصين اذ أغلقت 60 ألف موقع الكتروني إباحي منذ إطلاق حملة الإباحية في البلاد في ديسمبر 2009 حيث تمت من خلالها معالجة 2197 قضية تتعلق بالإباحية على الإنترنت. الصين تغلق 60 ألف موقع إباحي ،.http://news .maktoob.com ؛

محمد عبد الله المنشاوي، البحث السابق، http://www.minshawi.com

[2]– هناك صعوبة في تحديد مفهوم الاباحية و يرجع ذلك إلى صعوبة تحديد ما هو الفحش الذي تتناوله الجرائم أو المواد الاباحية، ويعرف الكتاب المادة الاباحية بأنها مصطلح يعرف عادة بالبرنو أو البرنوجرافي. وهو في أصله كلمة مشتقة من كلمة يونانية تعني الكتابة إلى البغايا. ميلود بن عبد العزيز: الجرائم الإباحية وأثرها على المجتمع من منظور شرعي وقانوني،مقال منشور ضمن أعمال الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية المنعقد بالجلفة ليومي27-2009/04/28،مجلة دراسات وأبحاث، جامعة الجلفة،العدد2009/01،ص11.

[3]– نسرين عبد الحميد بنيه: الإجرام الجنسي، دار الجامعة الجديدة، الإسكندرية، 2008، ص15

[4]– ميلود بن عبد العزيز، المرجع السابق،الموضع السابق.

المطلب الأول

ماهية الجرائم الجنسية عبر الانترنت.

نتناول في هذا المطلب تعريف الجرائم الجنسية الواقعة عبر الانترنت، ثم نوضح الأسباب التي ساهمت في انتشارها، لنبين بعد ذلك طرق و أساليب نشر هذه الجرائم. و ذلك في الفروع التالية:

الفرع الأول: تعريف الجرائم الجنسية الواقعة عبر الانترنت.

الفرع الثاني: أسباب انتشار الجرائم الجنسية الواقعة عبر الانترنت.

الفرع الثالث:أساليب و طرق نشر الجرائم الجنسية الواقعة عبر الانترنت.

الفرع الأول: تعريف الجرائم الجنسية الواقعة عبر الانترنت.

لقد تحولت شبكة الانترنت إلى أرشيف ضخم تجمع فيه الصور الماجنة والمقالات الفاضحة والأفلام الخليعة والتي تبث عبر مواقع مخصصة لذلك، غايتها تحقيق الربح المادي تسمى بالمواقع الجنسية الإباحية unihibited locatins وعن طريق الدردشة الإباحية والقوائم البريدية الجنسية، التي أصبحت تجتاح عالمنا وتقتحم منازل ومكاتب الجميع.فهي لا تفرق بين صغير وكبير ولا بين أنثى وذكر، أي أنها لا تستثني أحد. فعلى سبيل المثال تبين في المجتمع البريطاني أنه واحد من كل 5 سيدات يزرن وبشكل مستمر مثل هذه المواقع وأن 25% من الرجال و15% من النساء يمارسون الجنس عبر الإنترنت.و تقدر قيمة صناعة الجنس عالميا برقم مهول يكاد يصل الى 57 مليون دولار. يوجد على شبكة الانترنت أكثر من 372 مليون صفحة تروج مواد جنسية مختلفة، كما تبلغ ايرادات صناعة الجنس على الانترنت أكثر من 2 مليار و نصف دولار سنويا:89 % من الاغراءات الجنسية للأطفال و المراهقين تتم في غرف الدردشة، أكثر من 20 ألف صورة جنسية للأطفال تبث عبر الانترنت أسبوعيا، أكثر شريحة أطفال مستهلكة للمواد الجنسية عبر الانترنت هم الفئة من 12–17 سنة[1]. و في هذا يقول جيمس رستون في مجلة نيويورك تايمز بأن:" خطر الطاقة الجنسية قد يكون في نهاية الأمر أكبر من خطر الطاقة الذرية." وفي ذات السياق تشير احصاءات مصالح الشرطة في الجزائر أنه سجلت في الفترة من 2004–2008 أكثر من 7292 اعتداء جنسي على الأطفال[2].

و عليه يمكن تعريف الجرائم الجنسية عبر الانترنت بأنها:"بث الصور الماجنة والمقالات الفاضحة والأفلام الخليعة عبر الانترنت و على مواقع مخصصة لذلك، غايتها تحقيق الربح المادي تسمى بالمواقع الجنسية الإباحية unihibited locatins أو عن طريق الدردشة الإباحية والقوائم البريدية الجنسية".

---

[1]– د/ حسين الغافري، محمد الألفي، المرجع السابق، ص 86. خبراء يثنون على سياسة حجب بعض المواقع و يشددون على أهمية التوعية،http://up.graaam.com

[2]– ميلود بن عبد العزيز، المرجع السابق،ص11.

الفرع الثاني:أسباب انتشار الجرائم الجنسية الواقعة عبر الانترنت.

ولعل ما شجع ذلك هو سهولة الوصول و تحميل الملفات الإباحية التي تتمتع بنفس السهولة التي يمكن الوصول فيها إلى ملفات الموسيقى (MP3) وتحميلها[1]، الأمر الذي يسر زيارتها وأكثر الإقبال عليها بشكل رهيب. إذ أصبحت تمثل أغلب الصفحات والمواقع إقبالا وطلبا وبحثا في كل العالم في غياب المنافس لها، وخصوصا أثناء أوقات العمل وهذا ما كشفته احدى الدراسات اذ أن معدل التدفق على المواقع الإباحية تكثر في أوقات العمل (أي من 9h00 صباحا إلى 17h00 عصرا) إلى 70% من إجمالي نسبة التدفق على تلك المواقع. بل الأدهى و الأمر من ذلك أصبحت تلك الأخيرة تشكل بالفعل مشكلة حقيقية تعاني منها جميع المجتمعات على حد سواء. وهذا ما أثبتته وأكدته عدة دراسات ومنها: دراسة الدكتور مشعل القدهي، حيث ذكرت شركة "Play Boy" الإباحية بأن 70،4 مليون زائر يزورون صفحاتها على شبكة الإنترنت أسبوعيا، وأن هناك مائة صفحة مشابهة تستقبل أكثر من 20.000 زائر يوميا، وأن هناك بعض الصفحات الإباحية المشابهة يزورها 280.034 زائر يوميا وأكثر من ألفين صفحة مشابهة تستقبل أكثر من 1400 زائر يوميا، وأن صفحة من هذه الصفحات استقبلت خلال عامين عدد 43.613.508 مليون زائر. كما أثبتت دراسة إحصائية قام بها باحثون من جامعة كازين جيميلون بأن نصف الصور المسترجعة من بين 917.410 صورة هي صور إباحية، 5،83% منها متداولة في المجموعات الإخبارية.[2]

هذا من جهة ومن جهة أخرى، فقد أوضحت البيانات التي عرضها الموقع المخصص لإحصاء المواقع الإباحية على النت أن عدد الصفحات الإباحية في موقع N2H2 في تنامي وتزايد مستمر ومخيف يمكن تشبيهه بتسونامي العصر الهائل الذي يجتاح العالم ويخرب ويزيح كل من في طريقه. إذ وصل عددها عام 2003 إلى 260.000.000 صفحة على 1300.000 موقعا إباحيا مقارنة بالسنوات السابقة.[3]

ضف إلى ذلك فقد تبين من خلال استطلاع قامت به جريدة النهار الجزائرية في عدد من ولايات الجزائر، بأن هناك 68 % من الزبائن المراقبين زاروا مواقع إباحية في ولاية بومرداس، وتتمثل هذه الأخيرة إما في مواقع تبث صورا أو موقع تتجسد في مقاطع فيديو[4]. أما مقاهي الإنترنت بتيزي وزو فتحولت أيامنا هذه إلى أوكار للدعارة والانحلال الأخلاقي وذلك في غياب السلطات المختصة وانعدام المراقبة، إذ أصبحت الأبواب فيها مفتوحة بصدر رحب للإبحار وزيارة المواقع الإباحية الجنسية[5].

---

[1]– تقرير شبكة CNN الإخبارية بعنوان:"سهولة الوصول إلى الملفات الاباحية " المنشور على الموقع http:// www.cnn.com

[2]– د/ مشعل عبد الله القدهي:" المواقع الاباحية على شبكة الإنترنت و أثرها على الفرد و المجتمع"، بحث منشور على الموقعhttp:// www.aljra.net

[3]– لمزيد من التفاصيل ينظر د/ حسين الغافري، محمد الألفي، المرجع السابق، ص 84.

[4]– جريدة النهار،المواقع الاباحية تتصدر قائمة التصفح الالكتروني لدى شباب بومرداس،02-08-2010،ص 9.

[5]– جريدة النهار،مقاهي الإنترنت في تيزي وزو تتحول إلى أوكار للدعارة و الجهاد دون مراقبة،02-08-2010،ص 9.

أما فيما يخص ولايات الجنوب، فقد أجمع رواد و أصحاب مقاهي الإنترنت المنتشرة فيها بأن أكثر المواقع إقبالا ومتابعة وبحثا في الشبكة العنكبوتية هي المواقع الإباحية، فمثلا في ولاية الوادي تبين أن 70 % من المترددين على مقاهي الإنترنت يفضلون مواقع إباحية ويبحثون بالضبط عن ما يسمى بالجنس الالكتروني، ذلك الحديث الذي يشبع الغريزة بأسهل الطرق مع كافة الأجناس سواء عربيات، أو محليات أو أوروبيات فاتنات من الشقراوات عن طريق الدردشة الجنسية التي تكون إما من خلال السكايب أو الفايسبوك أو في نادي أو المسنجر، في حين تظل المواقع الجادة والعلمية في آخر دائرة الاهتمامات بنسبة لا تتجاوز إلا 8 %.[1]

وأضافت جريدة الفجر الجزائرية أن مقدار المبالغ التي يتم صرفها من طرف عينة متكونة من 1000 شخص يزورون مواقع إباحية موزعين عبر 100 نادي انترنت في كل مدن الجزائر يدفعون 50 الى 60 دينار، فان نفقاتهم تساوي حسابيا 180 مليار سنتيم.[2]

وقد كشفت دراسة جزائرية حديثة قام بها مركز التدريب الاعلامي بالجزائر – شملت 50 مقهى في العاصمة – أن 65% من الشباب الجزائري مدمن على المواقع الاباحية بمعدل مشاهدة 3 ساعات يوميا، و أن بعض تلك المواقع جزائرية الهوية.و أوصت بحظر 150 موقعا اباحيا الأكثر زيارة في الجزائر.[3]

وتجدر الإشارة من جهة أخرى، إلى أن الإدمان على المواقع الإباحية لا تقل خطورة عن خطر المخدرات. فقد قام نخبة من المختصين بعلم النفس بالولايات المتحدة الأمريكية بالتحذير من تبعت الإدمان على الصور الإباحية عند الإدلاء بشهاداتهم أمام الكونجرس الأمريكي واصفين الإدمان على تلك الصور بأنه أشد من الكراك كوكايين. وأن شبكة الإنترنت هي الوسيط الأمثل لنقل وتوصيل هذا المخدر. وما يدل على ذلك ما تناقلته وسائل الإعلام من أن أحد الممثلين المشاهير وهو "ديفيد دوكافني" يعالج من حالة إدمان الصور الإباحية بالإنترنت في إحدى العيادات النفسية المتخصصة في ولاية كاليفورنيا.[4]

وقد جرى حصر القوائم الإباحية العربية فقط دون الأجنبية في بعض المواقع شبكة الإنترنت ومنها موقع (yahoo) فوجد أنها تصل إلى 171 قائمة، بلغ أقل عدد أعضائها الى 3 أعضاء. في حين بلغ عدد أكثر أعضائها إلى 8683 عضوا والعدد في ازدياد. أما موقع (Globe list) فقد احتوى 6 قوائم عربية إباحية في حين وجدت 5 مواقع إباحية على موقع (Topica) [5]. ومن أمثلة تلك المواقع موقع www.adulfriendfinder.com. والذي يعد أكبر المواقع للإعلانات الجنسية للأشخاص حيث يبلغ عدد المشتركين المصريين فيه عشرة آلاف و 559 شخصا من بينهم 340 رجل يطلبون رجل و 9749 رجل

---

[1]– جريدة النهار،مقاهي الإنترنت في الجنوب فضاءات للانحلال و أخرى للتعارف و قليل منها للعلم،02-08-2010،ص9.

[2]– جريدة الفجر، 180 مليار سنتيم قيمة نفقات تصفح الجزائريين على الإنترنت،02-12-2009،ص7.

[3]– سماح خميلي:التكنولوجيا بين أيد غير أمينة في الجزائر(الإنترنت وظاهرة الجنس الالكتروني)، www.chihab.net

[4] – Voir http://www.el –Burhan.Com

[5]– د/ محمد عبد الله المنشاوي، البحث السابق ، http:// www.minshawi.com.

يطلبون امرأة و1132 رجل يطلبون ثنائي و930 رجل يطلبون مجموعة و371 امرأة تطلب امرأة و284 امرأة تطلب رجل و107 امرأة تطلب ثنائي و64 تطلب مجموعة و57 ثنائي يطلبون ثنائي و23 ثنائي يطلبون مجموعة. أما في لبنان فيبلغ عدد المشتركين فيه 2974 مشترك وفي الجزائر 609 وأما في المغرب 945 وقطر 589 وفي السعودية 1245 وفي الأردن 1938 مشترك.[1] وهناك قوائم أخرى تصنف تحت دول محددة بل وأكثر من ذلك ربطت بالإسلام كموقع "السحاقيات المسلمات" [2].

هذا من جهة و من جهة أخرى، فانه ووفقا لاحصائيات تم استخلاصها من موقع ALEX[3] تبين تصدر الولايات المتحدة الأمريكية لعدد الزيارات الى المواقع الاباحية، ثم تليها ايران ثم الامارات العربية المتحدة ومصر ثم الكويت بالمرتبة السابعة تليها السعودية بالمركز الحادي عشر.[4]

و الدافع الأساسي وراء نشر الجنس و الاباحية عبر الانترنت هو السعي وراء تحقيق الربح المادي عن طريق المتاجرة بتلك المواقع الخليعة بفرض مقابل معين للدخول اليها. و هذا ما تؤكده الاحصائيات، اذ أن مجموع مشتريات مواد الدعارة من خلال الشبكة الأم يلحظ تزايدا مستمرا مقارنة بدخل التجارة الالكترونية، إذ بلغ سنة 2004 (11%) من دخل تلك التجارة والبالغ (3،2 ترليون دولار). كما بلغت مجموعة الأموال المنفقة على الدخول على الصفحات الإباحية حوالي 44 مليار دولار عام 2008.[5]

وتعتبر الولايات المتحدة الأمريكية وحسب ما أكدته جمعية (NCH) البريطانية من أكبر الدول المصدرة للمواد الإباحية خاصة فيما يتعلق بالأطفال حيث أنها تتيح ما يقل عن 55% من تلك المواد وأن 20% من سكانها يزورون تلك الصفحات الإباحية. لتليها روسيا بنسبة 23 %.[6]

ولقد صاحب الانتشار الرهيب لهذه المواقع الإباحية ارتفاع في نسب جرائم الاغتصاب لا سيما اغتصاب الأطفال. وكذا زيادة في العنف الجنسي وفقدان الأسرة لقيمها ومبادئها بتدني أخلاق أفرادها وتغير الشعور نحو النساء إلى التحقير بدلا من الاحترام. ويفسر الباحثين في علم الإجرام ذلك بأن هناك علاقة طردية بين الانحراف والجرائم المرتكبة وبين مشاهدة أشرطة الفيديو الجنسية سواء على الإنترنت أو خارجها. وهذا ما أثبتته إحدى الدراسات المتخصصة بتفسير ارتكاب الجريمة الجنسية في المجتمع السعودي، والتي أجريت في الإصلاحيات المركزية بالمملكة بأن 7،53% من مرتكبي الجرائم الجنسية كان لهم اهتمامات بالصور الجنسية، وأن فئة كبيرة منهم كانوا يميلون إلى مشاهدة الأفلام الخليعة وقت فراغهم. كما تبين من الدراسة قوة تأثير مثل هذه الصور في ارتكاب جرائم الإعتداء الجنسي من قبل مجرمي اغتصاب الإناث

---

[1]– د/ حسين الغافري، محمد الألفي، المرجع السابق، ص 94

[2]– د/ محمد عبد الله المنشاوي، البحث السابق المنشور على الموقع السابق

[3]– موقع ALEX هو من أشهر مواقع تحليل زيارات صفحات الإنترنت

[4]– Voir http:// www.alex.com

[5]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي،(جرائم الإنترنت..) مرجع سابق، ص31.

[6]– د/ محمد عبد الله المنشاوي، البحث السابق، http:// www.minshawi.com

وهالكي أعراض الذكور بالقوة[1]. ضف إلى ذلك فإن عالم النفس الأمريكي "Edward Donnerstein" أكد بأن الاعتياد على خوض الدعارة والإباحية له تأثير سلبي وقوي وواضح على سلوك من يقدمون عليها، حيث تزيد لديهم درجة العنف في مقابل عدم الاكتراث لمصائب الآخرين وتقبلهم لجرائم الاغتصاب.

الفرع الثالث: طرق و أساليب نشر الجرائم الجنسية الواقعة عبر الانترنت

بالإضافة إلى ما سبق فإن شبكة الإنترنت أصبحت الآن وبالفعل تمثل مستنقعا للساقطات والساقطين من خلال ما تقدمه من خدمات غير أخلاقية يغيب فيها الوازع الديني والرقابة الذاتية، عن طريق ترويج المواقع الإباحية والدردشة الإباحية (cyber sex). وتسهيل القيام بنشاط إباحي عبرها كترتيب مواعيد جنسية واختيار الهدف الجنسي من خلال العرض المرئي السمعي (audio visuel) مع دفع قيمة ذلك. وكذلك يتم عبر الترويج للرقيق الأبيض وتجارة القاصرات ودعارة الأطفال بقصد الاستخدام الجنسي (cyberteen). ومن أمثلة الدردشة الإباحية برنامج البال توك الذي تدعمه شركة يهودية أمريكية، والذي يدخله أكثر من 140.000 شخص في لحظة واحدة من جميع أنحاء العالم، حيث يتم تبادل الأحاديث الجنسية والحوارات الساخنة صوتا وصورة مع إضافة الإيماءات الجنسية[2].

هذا من جهة ومن جهة أخرى، فإن تلك المواقع الإباحية المعروضة من خلال تلك الشبكة هي موجهة إلى شريحة كبيرة من المستهلكين بصرف النظر عن أعمارهم أو جنسهم، ولا سيما شريحة الشباب الفضولي الذي يرغب في معرفة محتوياتها ليتطور الأمر بعد ذلك إلى الإدمان. إذ كشفت دراسة بأن أكثر زوار هذه المواقع هم أطفال وشباب تتراوح أعمارهم ما بين 12 و15 سنة إلى غاية 35 سنة أي أنهم رجال ونساء المستقبل، الذين يعتبرون طعما سهلا لأصحاب تلك المواقع. إذ يقومون باستغلال ضعفهم وعدم نضجهم لإرضاء رغبة أو شهوة جنسية يسعى إليها الغير، خاصة وأن هذه الفئة تمر بمرحلة المراهقة والتي تكثر فيها المشاكل والمغامرات، والتي يجب أن يعتني فيها بالحدث وتقوم فيها أخلاقه وتشدد فيها الرقابة. وهذا ما أدى إلى ظهور حالات للاستغلال الجنسي للأطفال عبر الإنترنت مثل القوادة والحث أو التحريض على البغاء وكذلك الاتجار وتسجيل لأفلام البورنو الخليعة Films pornographiques، حيث يتم إخراجها لأطفال يستغلون جنسيا في أعمار مختلفة. ضف إلى ذلك نشر ووضع صور خليعة لأطفال حقيقيين أو افتراضيين (الصور الزائفة).حيث يتم تركيب صور أطفال على أجساد عارية، مثلما حدث في فضيحة شكسبير بإنجلترا، حيث قام المتهم بتركيب صور لرؤوس بنات صغيرات على صور أجساد عارية.[3] ولقد صرح "Michael MELATA" بوجود اتجاه ملحوظ يسير نحو تصوير الأطفال صورا خليعة، بحيث زادت نسبتها من 15% عام 1994 إلى 20% عام 1996. كما أن صحيفة الغارديان البريطانية نقلت عن مؤسسة "تصفح الإنترنت" وجود 3000 موقع على شبكة الإنترنت باللغة الإنجليزية تعرض صورا إباحية

---

[1]– د/ محمد عبد الله المنشاوي، المرجع نفسه، نفس الموقع.

[2]– د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 455.

[3]– د/ مدحت رمضان، المرجع السابق، ص 132.

للأطفال.وفحصت 34.871 تقرير قدمها العامة كشفت فيه عن وجود 2755 موقع محصن يقدم محتويات تتضمن استغلالا جنسيا للأطفال وتنشر على مستوى واسع في العالم[1]. وقد برزت الأخطار المحتملة ضد الأطفال عبر شبكة الإنترنت نتيجة ثلاث مخاوف رئيسية هي:

– سهولة وصول الأطفال إلى مواقع خليعة رئيسية تنظم دعارة الأطفال عبر شبكة الإنترنت.

– الإنترنت هي المكان المناسب لبيع منتجات منتجي دعارة الأطفال.

– وجود أشخاص خطيرين ومنجذبين نحو الأطفال على شبكة الإنترنت، والذين يسحرون ضحاياهم إلى لقاءات حقيقية في الحياة من خلال تخاطب البريد أو غرف التخاطب أو من خلال المراسلة عبر البريد الالكتروني. وهو الأمر الذي حدث في الولايات المتحدة الأمريكية، إذ أدين أمريكي بتهمة اغتصاب فتاة شابة كان قد تعرف عليها من خلال إحدى مؤتمرات المناقشة على شبكة الإنترنت، بعد أن قدم نفسه على أنه شاب يبلغ من العمر 18 سنة.[2]

–غياب رقابة الأولياء،فقد ذكر المرصد الوطني لحقوق الطفل بالجزائر في دراسة له بأن 72% من الاطفال المستجوبين في ايطار دراسة قدنها حول الموضوع يتجولون عبر مختلف مواقع الانترنت ونرقابة، و86%منهم يسمح لهم أوليائهم بالذهاب الى بيوت أصدقائهم للابحار في عالم الانترنت بحجة انجاز البحوث. وهذه الحرية سهلت على 55% من المستجوبين بالتوجه الى الدردشة الالكترونية، في حين ربط 35% منهم علاقات عبر الشبكة، و بينما صدم 46% منهم بصور لا أخلاقية، تلقى 30% منهم عروضا للتعارف أو اقامة علاقات مشبوهة.[3]

المطلب الثاني

التكييف القانوني للجرائم الجنسية الواقعة عبر الانترنت.

و سنتناول في هذا المطلب تبيان الجهود الدولية في مكافحة الجرائم الجنسية الواقعة عبر الانترنت، ثم نوضح موقف التشريعات المقارنة من هذه الجرائم. و ذلك في الفرعين التاليين:

الفرع الأول: الجهود الدولية في مكافحة الجرائم الجنسية الواقعة عبر الانترنت.

الفرع الثاني: موقف التشريعات المقارنة من الجرائم الجنسية الواقعة عبر الانترنت.

الفرع الأول: الجهود الدولية في مكافحة الجرائم الجنسية الواقعة عبر الانترنت.

لقد أدى انتشار الصور الفاضحة على شبكة الإنترنت إلى دعوة أعضاء المجتمع الدولي إلى مؤتمر عقد عام 1999 بباريس، ومؤتمر آخر في ذات العام عقد في النمسا. وكانت أهداف هذين المؤتمرين:

---

[1]– شيرين الياس دبابنة، المرجع السابق، ص 42.

[2]– د/ جميل عبد الباقي الصغير،(الإنترنت والقانون الجنائي) مرجع سابق، ص 45.

[3]– أسامة غربي: الاباحية الالكترونية،،مقال منشور ضمن أعمال الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية المنعقد بالجلفة ليومي27–2009/04/28،مجلة دراسات و أبحاث، جامعة الجلفة،العدد2009/01، ص 09.

1– كفالة التعاون الدولي في مجال مكافحة عرض وتوزيع الصور الجنسية للأطفال عبر الإنترنت.

2 – ضرورة توعية الجمهور لمواجهة الاستغلال الجنسي للأطفال عبر تلك الشبكة.

3 – دعوة المشرع الوطني لمحاربة التجارة الجنسية عبر الإنترنت من خلال تجريم كافة صور المعاملات التي تجري على صور الجنسية للأطفال، سواء عن طريق إنتاجها وتوزيعها أو استيرادها أو حيازتها أو تخزينها داخل الكمبيوتر أو التعامل فيها بأي طريق من الطرق.

4 – السماح بتفتيش الحواسيب حتى ولو كانت خارج حدود الدولة، وذلك لضبط الجناة.

5 – ضرورة إقامة رسائل للاتصال الدائم لتحقيق التعاون الدولي في هذا المجال.

ولقد استجابت بعض الدول لنداء هذين المؤتمرين وقامت باتخاذ إجراءات تشريعية أو قضائية في هذا الشأن مثل فنلندا وهولندا وأستراليا.[1]

ومن ناحية أخرى أكد دعوة المجلس الأوروبي على ضرورة مكافحة الإباحية التي موضوعها الأطفال على الإنترنت في 29 ديسمبر 1998.

وتجدر الإشارة إلى أن هذا الأمر كان موضوعا للاجتماع الدولي لخبراء الإنتربول بليون (فرنسا) في ماي 1998.[2]

ولقد جاء في الاتفاقية الأوروبية لجرائم الإنترنت تجريم الإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية في المادة 09 منه. حيث صنفت ضمن ما يعرف بجرائم المتصلة

---

[1]– محمد أمين الرومي: جرائم الكمبيوتر و الإنترنت، دار المطبوعات الجامعية، الإسكندرية،2004، ص130.

[2]– Yaman AKDENIZ: International Developments Section Of Regulation Of Child Pornography on the internet، http:// www.cyber-righs.org

أتاحت عملية نفُذت على الصعيد العالمي واستهدفت أفرادا يستخدمون الشبكات الاجتماعية لتبادل مواد الإعتداء الجنسي على الأطفال تبيُّن 55 مشبوها رئيسيا في 20 بلدا وتوقيف عدد منهم، فضلا عن تحديد هوية 12 طفلا وإبعادهم عن الخطر. وقد بدأت هذه العملية، التي أُطلق عليها اسم لامينار، في أكتوبر 2010 بفتح تحقيق سري أجرته على الإنترنت الوحدة المعنية بالتحقق من الامتثال لقرارات الرقابة التابعة لوزارة الداخلية في نيوزيلاندا، فنبّهت الفريق المعني بمكافحة الجرائم المرتكبة ضد الأطفال في الإنتربول وأجهزة إنفاذ القانون الدولية إلى أنها اكتشفت كميات كبيرة من صور الإعتداءات الجنسية على الأطفال التي يجري تبادلها عبر مواقع الشبكات الاجتماعية، و لا سيما فيسبوك وغرو بي أس وسوشيلغو.

والتحقيقات التي ينسقها الإنتربول، بالتعاون مع الوحدة المعنية بالتحقيقات في الاستغلال الجنسي للأطفال ضمن جهاز إنفاذ قوانين الهجرة والجمارك في الولايات المتحدة التابع لشعبة التحقيقات في شؤون الأمن الداخلي، وبمساعدة الإدارة المعنية بقضايا الاستغلال الجنسي للأطفال ومكافحة خلاعيات الأطفال في وزارة العدل، أتاحت الكشف عن حوالى 80 مجموعة تُشارك في عرض وتو زيع صور الاستغلال الجنسي للأطفال التي سبق أن نُشرت والتي لم تُنشر بعد.وقد أُجر يَت التحقيقات بدعم ومساعدة القيّمِين على شبكة فيسبوك، بعد أن تم تحديد هوية الأشخاص المستهدفين بشكل رئيسي والمجموعات المرتبطة بهم. ينظر لمزيد من التفاصيل عملية دولية تنقضّ خلالها أجهزة إنفاذ القانون على أفراد يستغلون الأطفال جنسيا ويتبادلون صورهم عبر الإنترنت، http:// .www.interpol.int

بالمحتوى. ولقد دعت هذه الاتفاقية من خلال الفقرة الأولى من تلك المادة على وجوب اتخاذ الإجراءات التشريعية و غيرها من الإجراءات التي تراها الدول الأعضاء ضرورية لتجريم هذه الأفعال بقوانينها المحلية و ذلك عند ارتكابها عن عمد و دون وجه حق:

- إنتاج مواد إباحية طفولية بغرض نشرها عبر نظم معلوماتي.
- تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتي.
- النشر أو النقل لمادة إباحية طفولية عبر نظام معلوماتي.
- الحصول على أو تزويد الغير بمادة إباحية طفولية عبر نظام معلوماتي.
- حيازة مادة إباحية طفولية في نظام معلوماتي أو في أي وسيلة لتخزين البيانات المعلوماتية.

كما حددت تلك الاتفاقية مفهوم المادة الإباحية الطفولية بشمولها لكل مادة اباحية التي تتخذ إحدى الصور التالية:

إشتراك قاصر في سلوك جنسي صريح.

إستغلال قاصر في أي سلوك جنسي فاضح.

صور خيالية أو واقعية تمثل قاصر يقوم بسلوك جنسي.

و القاصر وفقا لهذه الاتفاقية هو أي شخص عمره أقل من 18 عاما، و مع ذلك فإنه يمكن لأي طرف أن يستوجب حدا عمريا أقل بشرط ألا يقل عن 16 عاما.[1]

كما تأكد حديثا تبني بروتوكول اختياري لاتفاقية الأمم المتحدة لحقوق الطفل المرتبط ببيع الأطفال ودعارة الأطفال والمواد الإباحية الآثمة للأطفال و الذي من أهم ما جاء فيه:

1- حظر البروتوكول على الدول الأطراف بيع الأطفال و استغلالهم في البغاء و في المواد الإباحية.

2- عرف هذا البروتوكول استغلال الطفال في البغاء بأنه استخدام طفل لغرض أنشطة جنسية لقاء مكافأة أو أي شكل آخر من أشكال العرض.

3- يقصد بإستغلال الأطفال في المواد الإباحية وفقا للبروتوكول تصوير أي طفل، بأي وسيلة كانت يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة، أو أي تصوير للأعضاء الجنسية للطفل لإشباع الرغبة الجنسية أساسا.

4- تكفل كل دولة طرف أن تغطي كحد أدنى الأفعال و الأنشطة التالية تغطية كاملة بموجب قانونها أو قانون العقوبات فيها سواء أكانت هذه الجرائم ترتكب محليا أم دوليا أم كانت ترتكب على أساس فردي أو منظم:

أ- في سياق بيع الأطفال كما هو معرف في المادة 2:

---

[1]- لمزيد من التفاصيل ينظر د/ هلالي عبد اللاه أحمد،(الجوانب الموضوعية و الاجرائية لجرائم المعلوماتية ...) مرجع سابق، ص 117 و ما بعدها. و محمد الألفي: المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، الطبعة الأولى، المكتب المصري الحديث، القاهرة، 2005، ص181 و ما بعدها.

1- عرض أو تسليم أو قبول طفل بأي طريقة كانت لغرض من الأغراض التالية:

الاستغلال الجنسي للطفل.

نقل أعضاء الطفل توخيا للربح.

تسخير الطفل لعمر قسري.

2- القيام كوسيط – بالحفز غير اللائق على اقرار تبني طفل و ذلك على النحو الذي يشكل خرقا للصكوك القانونية الواجبة التطبيق بشأن التبني.

ب- عرض أو تأمين أو تدبير أو تقديم طفل بغرض استغلاله في البغاء على النحو المعرف في المادة 2.

ج- انتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد اباحية متعلقة بالطفل على النحو المعرف في المادة 2.[1]

ولقد كان المشرع الأوروبي نشطا في نهاية القرن العشرين في مجال حماية الأخلاق عبر الإنترنت،لاسيما بعد قيامه بإصدار التوجيه رقم: 95/46/EC المؤرخ في 1995/10/24 المتعلق بالتداول الحر للبيانات عبر الإنترنت. فقد أصدر مجلس أوروبا الكتاب الأخضر بشأن حماية القاصرين المنشور في أكتوبر 1996.[2]

و إضافة إلى هذا فقد جرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الاباحية في المادة 12 منها و اعتبرتها مرتكبة في الحالات التالية: انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة الحياء بواسطة تقنية المعلومات.و تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر إذا ما تعلق الأمر بحيازة مواد إباحية أو مواد مخلة بالحياء للأطفال و القصرعلى تقنية المعلومات أو وسيط تخزين تلك التقنيات[3].

الفرع الثاني: موقف التشريعات المقارنة من الجرائم الجنسية الواقعة عبر الانترنت.

لم تتفق التشريعات المقارنة في الدول المختلفة على آلية مكافحة الجرائم الجنسية الواقعة عبر الانترنت، اذ فضل البعض منها اصدار قوانين خاصة لتجريم و عقاب مثل هذه الجرائم المخلة بالآداب المستحدثة، وهناك دول أخرى و منها غالبية الدول العربية اكتفت بالصمت و بتطبيق قوانينها العقابية التقليدية و قوانين الأخلاق و الآداب العامة على تلك الجرائم. و سنتناول في هذا الفرع موقف التشريعات الغربية من الجرائم الجنسية الواقعة عبر الانترنت أولا ثم نبين موقف التشريعات العربية حيال هذه الجرائم ثانيا.

---

[1]- لمزيد من التفاصيل حول هذا البروتوكول ينظر د/ أسامة بن غانم العبيدي: جريمة الاستغلال الجنسي للأطفال عبر شبكة الإنترنت، دراسة قانونية مقارنة، مجلة الشريعة و القانون، العدد 53، السنة 27، يناير 2013، كلية القانون، جامعة الإمارات العربية المتحدة، ص 101 و ما بعدها.

[2]- محمد أمين أحمد الشوابكة، المرجع السابق، ص118.

[3]- ينظر المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أولا: موقف التشريعات الغربية من الجرائم الجنسية الواقعة عبر الانترنت.

لم تسلك الدول الغربية مسلكا موحدا في مكافحة الجرائم الجنسية الواقعة عبر الانترنت، حيث جرمت بعض الدول الغربية هذه الجرائم، في حين اكتفت بعض الدول الغربية بتطبيق قوانينها العقابية و قوانين الأخلاق و الآداب العامة المعمول بها لديها. و سنبين فيمايلي كل من موقف التشريع الفرنسي بداية لنعرج بعد ذلك لتوضيح موقف التشريعات الأنجلوسكسونية.

1/ موقف التشريع الفرنسي من الجرائم الجنسية الواقعة عبر الانترنت:

لقد عالج المشرع الفرنسي الجرائم الجنسية و لا سيما تلك التي يكون محلها الأطفال في قانون العقوبات الفرنسي الجديد، وخاصة بعد انضمام فرنسا ومصادقتها لاتفاقية الأمم المتحدة لحقوق الطفل، بحيث قام المشرع الفرنسي بتوفير الحماية للطفل أو القاصر بمقتضى المواد 225-12-1 و 225-12-2[1]، 227 – 22، 227 -23، 227 -24 ، 227-25، 227-26[2] من خلال تجريمه لجميع الأفعال التي تنطوي على

---

[1]– 225-12-1 : « Le fait de solliciter، d'accepter ou d'obtenir، en échange d'une rémunération ou d'une promesse de rémunération، des relations de nature sexuelle de la part d'un mineur qui se livre à la prostitution، y compris de façon occasionnelle، est puni de trois ans d'emprisonnement et 45000 euros d'amende.

Est puni des mêmes peines le fait de solliciter، d'accepter ou d'obtenir، en échange d'une rémunération ou d'une promesse de rémunération، des relations sexuelles de la part d'une personne qui se livre à la prostitution, y compris de façon occasionnelle، lorsque cette personne présente une particulière vulnérabilité، apparente ou connue de son auteur، due à une maladie، à une infirmité، à une déficience physique ou psychique ou à un état de grossesse ».

225-12-2 : « Les peines sont portées à cinq ans d'emprisonnement et 75 000 euro d'amende :

1°Lorsque l'infraction est commise de façon habituelle ou à l'égard de plusieurs personnes ;

2° Lorsque la personne a été mise en contact avec l'auteur des faits grâce à l'utilisation، pour la diffusion de messages à destination d'un public non déterminé، d'un réseau de communication ;

3° Lorsque les faits sont commis par une personne qui abuse de l'autorité que lui confèrent ses fonctions ;

4° Lorsque l'auteur des faits a délibérément ou par imprudence mis la vie de la personne en danger ou a commis contre elle des violences.

Les peines sont portées à sept ans d'emprisonnement et 100 000 euros d'amende lorsqu'il s'agit d'un mineur de quinze ans. »

[2]– 227-22 : « Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Ces peines sont portées à sept ans d'emprisonnement et 100000 euros d'amende lorsque le mineur lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation، pour la diffusion de messages à destination d'un public non déterminé، d'un réseau de communications électroniques ou que les faits sont commis dans les établissements d'enseignement ou d'éducation ou dans les locaux de l'administration، ainsi que، lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci، aux abords de ces établissements ou locaux. Les mêmes peines sont notamment applicables au fait، commis par un majeur، d'organiser des réunions comportant des exhibitions ou des relations sexuelles auxquelles un mineur assiste ou participe ou d'assister en connaissance de cause à telles réunions.

Les peines sont portées à dix ans d'emprisonnement et 1 000000 Euros d'amende lorsque les faits ont été commis en bande organisée ou à l'encontre d'un mineur de 15 ans ».

227-22-1 : « Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 Euros d'amende. Ces peines sont portées à cinq ans d'emprisonnement et 75 000 Euros d'amende lorsque les propositions ont été suivies d'une rencontre ».

227-23 : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende.

Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.

Les peines sont portées à sept ans d'emprisonnement et à 100 000 Euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.

Le fait de consulter habituellement ou en contrepartie d'un paiement, un service de communication au public en ligne mettant à disposition une telle image ou représentation d'acqurir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende.

Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 Euros d'amende lorsqu'elles sont commises en bande organisée.

La tentative des délits prévus au présent est punie des meme peines.

Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image ».

227-24 : « Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables ».

227-25 : « Le fait, par un majeur, d'exercer sans violence, contrainte, menace ni surprise une atteinte sexuelle sur la personne d'un mineur de quinze ans est puni de cinq ans d'emprisonnement et de 75000 euros d'amende ».

227-26 : « L'infraction définie à l'article 227-25 est punie de dix ans d'emprisonnement et de 150000 euros d'amende :

1° Lorsqu'elle est commise par un ascendant ou par toute autre personne ayant sur la victime une autorité de droit ou de fait ;

2° Lorsqu'elle est commise par une personne qui abuse de l'autorité que lui confèrent ses fonctions ;

3° Lorsqu'elle est commise par plusieurs personnes agissant en qualité d'auteur ou de complice ;

4° Lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique ;

استغلاله جنسيا، كاستغلال صوره في الأعمال الجنسية أو تعرضه للعنف أو للانحراف أو إفساده أو التدخل في تكوين فكره وثقافته بمعلومات ذات دلالة جنسية، والتي جميعها أفعال قد تقع عن طريق الإنترنت. فعلى سبيل المثال كثيرا ما تستغل عصابات الجريمة المنظمة صورة القاصر في الأعمال الجنسية بهدف تحقيق سياحة جنسية من خلال شبكة الإنترنت وهذا ما أكدته بعض التقارير الصادرة عن الولايات المتحدة الأمريكية، بأن هناك أكثر من 900.000 صورة جنسية تبث كل عام من خلال هذه الشبكة. أما فيما يخص إفساد القاصر، فقد أثبتت الدراسات أن شبكة الإنترنت تتضمن حوالي مليون صورة أو رواية أو وصف لهذه الصور والتي لها علاقة مباشرة و واضحة بالجنس. ضف إلى ذلك فإنها توفر معلومات عن بيوت الدعارة في العديد من بلدان العالم. كما تبث بعض المؤسسات من خلالها أحاديث هاتفية تؤديها فتيات مدربات مقابل الحصول على نسبة من عائد تلك المكالمات.والهدف وراء تجريم مثل هذه الأفعال يتمثل في تقرير حماية الأطفال من هؤلاء الذي يستغلون ضعفهم وعدم نضجهم لإرضاء رغبة أو شهوة يسعى إليها الغير[1].

2/ موقف التشريعات الأنجلوسكسونية من الجرائم الجنسية الواقعة عبر الانترنت.

أ- موقف التشريع الأمريكي من هذه الجرائم:

جرم المشرع الأمريكي التقاط صور إباحية للأطفال (2252 usc 18) أو الإعلان عنها أو عرضها (18 usc 2252 (a)2(A))[2] من خلال القانون الاتحادي لعام 1936 دون أن يعرفها. ولهذا جيء بالتعديل التشريعي لذلك القانون عام 1996 من خلال إصدار بما يسمى قانون آداب الاتصال[3] و الذي جرم نقل الصور الفاحشة للأطفال باستخدام الانترنت، كما جرم التصوير الجنسي و الصور ذات الطبيعة الجنسية و كذلك أحاديث الفحش باستخدام الانترنت. و قد وسع هذا الأخير من مفهوم التصوير الإباحي للأطفال

5° Lorsqu'elle est commise par une personne agissant en état d'ivresse manifeste ou sous l'emprise manifeste de produits stupéfiants ».

[1]- د/ عبد الفتاح بيومي حجازي، (الاحداث و الإنترنت) مرجع سابق،ص133.

[2] -18 USC Sec. 2252A :"(a) Any person who

(1) knowingly mails، or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means، including by computer، any child pornography;

(2) knowingly receives or distributes

(A) any child pornography that has been mailed، or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means، including by computer; or

(B) any material that contains child pornography that has been mailed، or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means، including by computer;…."

[3]- يعتبر هذا التعديل أول جهد للكونجرس الأمريكي لتنظيم أوجه اباحية الأطفال عبر الإنترنت، و الذي ظهرت في المجتمع الأمريكي عام 1995.

ليعتبره كل تصوير مرئي – يتضمن صورة أو فيلم أو فيديو أو رسما أو رسم كمبيوتر أو صورة منتجة بطريق الكمبيوتر بوسيلة الكترونية أو ميكانيكية أو بأي وسيلة أخرى– لأي سلوك جنسي مباشر اذا:

– كان انتاجه يقوم على استخدام طفل في وضع جنسي مباشر

– اذا كان هذا التصوير يبدو كما لو كان هناك طفل في وضع جنسي مباشر

– اذا كان هذا التصوير قد صنع أو عدل ليظهر طفلا في وضع جنسي مباشر

– اذا تم توزيع أو اعلان أو دعاية لتصوير، بحيث يوحي أنه ينطوي على طفل في وضع جنسي ويعاقب القانون بالسجن لمدة 15سنة لكل من يقوم بانتاج أو توزيع صورة اباحية للأطفال و بالسجن لمدة 5 سنوات لمن يحوز هذه الصور، بالسجن المؤبد من يقوم بالاستغلال الجنسي للأطفال[1] ، والذي تلاه تعديل آخر لذلك القانون عام 1998 سمي بقانون حماية الأطفال على الخط أو قانون آداب الاتصالات الثاني، والذي أضفى حماية أوسع وأشمل من تلك التي كانت من قبل للأطفال على الإنترنت. إذ أصبحت أحكامه تطبق على الأعمال والمواد التي تجرى على الخط (الإنترنت) من حيث تجريم نقلها وكذا على الاتفاق أو الاشتراك الجنائي على ذلك، والذي يشكل اعتداء على الأطفال من التعرض للمواد غير الملائمة. كما كفل الحماية للطفل من الإعتداء الجنسي والسيكولوجي معا في المادة ("2"1402)، وجرم توزيع أي مواد ضارة على الأحداث ("4"1402).

أما فيما يخص القضاء الأمريكي فقد أبدى موقفه حيال هذه الجريمة في الحكم بالسجن لمدة 37 شهر على شخص يدعى "روبرت" والحكم لمدة 30 شهر على فتاة تدعى "كارولين توماس" بتهمة التشجيع على الفحش في مفيس (بولاية Tennessee)، بحيث كانا يديران أنظمة لوحة النشرات للبالغين من كاليفورنيا، وزودوا خدماتهم لشراء زبائن من خلال تحميل صور فاحشة عبر أجهزة الكمبيوتر، حيث أدينا بعشرة مواد اتهامية[2].

ب–موقف التشريع الإنجليزي من هذه الجرائم:

تناول المشرع الانجليزي الجرائم الجنسية من خلال قانون المنشورات الفاحشة Obscene Publication Act لعام 1959 و 1964 ، و الذي جرم فيه الأفعال التي تتضمن مواد ذات طبيعة جنسية.[3] كما

---

[1]– تجدر الاشارة إلى أن التعديل التشريعي الذي جاء بقانون آداب الاتصال قضي بعدم دستوريته لدى احدى محاكم الاستئناف في الولايات المتحدة الأمريكية لكونه يجرم الصور الالكترونية المصنعة بطريق الكمبيوتر على الرغم من أنها قد لا تنطوي على اشتراك فعلي لأي طفل حقيقي، أو على الرغم من أنها قد لا تنطوي على أطفال يمكن التعرف عليهم، فضلا عن عمومية و غموض الألفاظ و العبارات المستخدمة من قبل المشرع. د/ مدحت رمضان، المرجع السابق، ص 134.

[2]– محمدأمين أحمد الشوابكة، المرجع السابق، ص 123.

[3]– جرمت المادة 1/1 من قانون 1959 أية مواد يعتقد أنها فاحشة اذا كان تأثيرها ينصب على إفساد الأخلاق أو إفساد الأشخاص الذين ينجذبون اليها، و لديهم إهتمام بقراءة و مشاهدة أو سماع محتوى المواد المدرجة فيها. كما جرمت المادة 1/2 من ذات القانون نشر مواد فاحشة بقصد نشرها و استغلالها تجاريا. و قد وسع المشرع الانجليزي نطاق التجريم باصدار قانون المنشورات الفاحشة 1964 حيث جرم الحصول على مواد فاحشة بقصد التملك أو الحيازة أو توجيهها للعرض بقصد نشرها و تحقيق الربح. محمد أمين أحمد الشوابكة، المرجع السابق، ص 124 و ما بعدها.

أصدر قانون حماية الطفل الصادر في 1978 Child Protection Act (CPA) و الذي جرم في مادته الأولى قيام أي شخص بالتقاط أو السماح بالتقاط أو انتاج أية صورة ضوئية فاحشة حقيقية[1] أو زائفة لطفل، أو قيامه بتوزيع أو عرض أي من هذه الصور الضوئية الفاحشة الحقيقية أو الزائفة ". كما تضمن التعديل الذي أضافه الأمر الخاص بالعدالة الجنائية والنظام العام لسنة 1994، حماية اضافية للأطفال بتجريمه صور الأطفال الزائفة المخزنة في الكمبيوتر[2]. حيث نص في المادة 84 منه على أن :" يعاقب بالحبس لمدة لا تتجاوز الستة أشهر كل شخص يحصل على صور خليعة أو زائفة للأطفال بقصد حيازتها."ولقد استهدف التعديل الجديد مواجهة استخدام التكنولوجيا الحديثة ممثلة في الكمبيوتر و الانترنت في تركيب صور أطفال على أجساد للبالغين أو لغيرهم من الصغار.

أما بالنسبة لموقف القضاء الإنجليزي من جرائم الاستغلال الجنسي للأطفال على الإنترنت فقد أصدرت محكمة صلح بيرمنجهام حكما بالسجن لمدة 3 شهور على شخص يدعى "كريستوفر شارب" بتهمة حيازة أكثر من 900 صورة خلاعية للأطفال.[3]

ثانيا: موقف التشريعات العربية من الجرائم الجنسية الواقعة عبر الانترنت.

لم تصدر غالبية الدول العربية قوانين خاصة لمكافحة الجرائم الجنسية الواقعة عبر الانترنت، و اكتفت بتطبيق نصوص قوانينها العقابية التقليدية، و على عكس ذلك قامت دول أخرى بسن قوانين خاصة تجرم وتعاقب على جرائم الحاسوب و الانترنت و منها الجرائم الجنسية الواقعة عبر الانترنت و لا سيما جريمة الاستغلال الجنسي للأطفال عبر تلك الشبكة. و لقد خصصنا هذه النقطة لتوضيح موقف الدول العربية من تلك الجريمة بصفة عامة، ثم نبين موقف التشريع الجزائري من تلك الجريمة.

1/ موقف التشريعات العربية بصفة عامة حيال هذه الجرائم:

فرض **المشرع الأردني**[4] حماية للأطفال من الإعتداءات الجنسية الواقعة عبر الأنظمة المعلوماتية أو شبكة

---

[1]– عرفت المادة 7(7) من نفس القانون الصورة الضوئية غير الحقيقية بأنها:"صورة سواء أنتجت بواسطة الرسم بالكمبيوتر أو تبدو على أنها كذلك".

[2]– لقد أضاف الأمر الخاص بالعدالة الجنائية و النظام العام الصادر في 1994 مادة فرعية للمادة 7(7) ليشمل التجريم البيانات المخزنة على أسطوانة الكمبيوتر أو بأي وسيلة الكترونية أخرى، بحيث يمكن تحويلها إلى صور ضوئية..د/ مدحت رمضان، المرجع السابق، ص 132.

[3]– يعتبر كريستوفر شارب أول شخص يحاكم في انجلترا في قضية تتضمن صورا خلاعية حصل عليها عبر الإنترنت.محمدأمين أحمد الشوابكة، المرجع السابق، ص 127.

–Thibault VERBIEST: Pornographie enfantine et internet : comment réprimer ? ,http://www.droit– technologie.org.

[4]– تجدر الاشارة إلى أن القانون الأردني لم ينص في أي موقع من المواقع عن الاستغلال الجنسي للأطفال وإنما تطرق إلى ذلك في مواضع تجريمية تقليدية مختلفة، حيث أورد نصوصا مختلفة تجرم الإعتداء على الأطفال فيما يتعلق بالجرائم المخلة بالأخلاق والآداب العامة، كتلك المتعلقة بالإعتداء على العرض كجرائم الاغتصاب وهتك العرض والخطف والإغراء والتهتك وخرق حرمة الأماكن الخاصة بالنساء أو المتعلقة بالحض على الفجور والتعرض للأخلاق والآداب العامة والواردة في الفصلين الأول والثاني من الباب السابع من قانون العقوبات الأردني رقم 1960/16. كما بين الباب السادس من قانون

الانترنت من خلال إصداره لقانون جرائم أنظمة المعلومات لسنة 2010 و في المواد 9 و 10 و 12[1].
و ذات الشأن بالنسبة **للمشرع الإماراتي**[2] اذ عالج جريمة الإعتداء الجنسي الواقعة عبر الانترنت عامة و لا سيما الذي يكون محلها الطفل من خلال القانون الاتحادي رقم 2 لعام 2006 في شأن مكافحة جرائم تقنية المعلومات في المواد 12 و 13 و20[3]. أما فيما يخص القضاء الإماراتي، فقد قضت محكمة دبي بحبس

العقوبات الأردني الجرائم التي تمس بالأسرة في المواد 219–278 . ينظر كلا من وضاح محمود الحمود و نشأت مفضي المجالي: جرائم الإنترنت، دار المنار للنشر و التوزيع، عمان، 2005، ص 48، محمد أمين أحمد الشوابكة، المرجع السابق، ص 110 و ما بعدها.

[1]– تنص المادة 9 من قانون جرائم أنظمة المعلومات الأردني على أنه:" كل من أرسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصدا كل ما هو مسموع أو مقروء أو مرئي مناف للحياء موجه إلى شخص أو يمس شخصا لم يبلغ الثامنة عشرة من العمر يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر و بغرامة لا تقل عن ثلاثمائة دينار و لا تزيد على خمسة آلاف دينار.

يعاقب بالحبس مدة لا تقل عن ستة أشهر و بغرامة لا تقل عن خمسمائة دينار و لا تزيد على خمسة آلاف دينار كل من قام قصدا باستخدام نظام معلومات أو الشبكة المعلوماتية في اعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو توزيع أنشطة أو أعمال إباحية تتعلق بتحريض أو تأثير من لم يبلغ الثامنة عشرة من العمر و استغلاله في الدعارة و الأعمال الإباحية أو التشهير به أو بيعه أو تحريضه على الانحراف أو تسخيره في ارتكاب جريمة." كما نصت المادة 10 على أنه:" كل من قام قصدا باستخدام الشبكة المعلوماتية أو أي نظام معلومات للترويج للدعارة أو الفجور يعاقب بالحبس مدة لا تقل عن ستة أشهر و بغرامة لا تقل عن ثلاثمائة دينار و لا تزيد على خمسة آلاف دينار." أما المادة 12 فقد شدد فيها المشرع العقوبة المنصوص عليها في المواد السابقة لتتضاعف في حالة تكرار أي من الجرائم المنصوص عليها سابقا.

[2]– تجدر الاشارة أن المشرع الامارتي وفر الحماية للطفل من الاستغلال الجنسي للأطفال من خلال القانون العقوبات الاتحادي في المواد 354، 356، 358، 360، 362 منه.

[3]– تنص المادة 12 من القانون الاتحادي رقم 2 لعام 2006 في شأن مكافحة جرائم تقنية المعلومات على أنه:" كل من أنتج أو أعد أو هيأ أو أرسل أو خزن بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه المساس بالآداب العامة أو دار مكانا لذلك يعاقب بالحبس و بالغرامة أو باحدى هاتين العقوبتين، فإذا كان الفعل موجها إلى الحدث فتكون العقوبة الحبس مدة لا تقل عن ستة أشهر و الغرامة لا تقل عن ثلاثين ألف درهم." كما نصت المادة 13 على أنه:" يعاقب بالسجن و بالغرامة من حرض ذكرا أو أنثى أو أغواه فرتكاب الدعارة أو الفجور أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. فإن كان المجني عليه حدثا كانت الالعقوبة السجن مدة لا تقل عن خمس سنوات و الغرامة". و كذلك فقد نصت المادة 20 على:" كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعى لتسهيل و ترويج برامج و أفكار من شأنها الإخلال بالنظام العام و الآداب العامة يعاقب بالحبس مدة لا تزيد على خمس سنوات."

طالب عاما مع الإبعاد عن الدولة لقيامه بهتك عرض طفل يبلغ من العمر 12 عام وعرض و نشر صور له و هو بأوضاع مشينةعلى شبكة الانترنت.[1]

أما بالنسبة **للمشرع السعودي** فقد جرم استخدام شبكة الانترنت في الاستغلال الجنسي للأطفال و إنشاء المواقع الإباحية و إنتاج المواد الإباحية وارسالها و تخزينها و نشرها و ترويجها سواء أكان ذلك عبر شبكة الانترنت أم بواسطة الحاسب الآلي من خلال نظام مكافحة الجرائم المعلوماتية السعودي في المادة 6 و 8 و9 و10 و12. حيث ورد بالفقرة الثالثة من المادة 06 من نظام مكافحة جرائم المعلوماتية تجريم كل إنشاء لمواد وبيانات متعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها. ولقد جرم في المادة 3/8 من نفس النظام جميع أنواع استغلال القصر ومن في حكمهم استغلالا جنسيا.[2]

2/ موقف التشريع الجزائري من هذه الجرائم:

فرض المشرع الجزائري حماية جنائية للطفل من الإعتداءات الجنسية من خلال قانون العقوبات رقم 66- 156 المعدل والمتمم وذلك في الفصل الثاني من الباب الثاني منه والمعنون بالجنايات والجنح ضد الأسرة والآداب العامة في القسم السابع المعنون بتحريض القصر على الفسق و الدعارة من المادة 342 إلى غاية 349. وكذا في القسم السادس في المواد 334- 335- 336- 337. حيث نص في المادة 342 على جريمة تحريض القصر على الفسق و افساد الأخلاق[3] سواء بصورة عرضية أو صورة الإعتياد[4] وذلك عن طريق التحريض أو التشجيع أو المساعدة على الاقدام على مثل هذه الأفعال الجنسية المشينة سواء بالقول أو بغيره و بغض النظر عن الوسيلة المستعملة في ذلك و التي يمكن أن تقع عن طريق الانترنت. أما المادة 343 فجرمت جريمة الدعارة اذ نصت من خلال الفقرة الأولى منها على:" يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة من 500 إلى 20000 دج و ما لم يكن الفعل المقترف جريمة أشد، كل من ارتكب عمدا أحد الأفعال الآتية:

ساعد أو عاون أو حمى دعارة الغير أو أغرى الغير على الدعارة و ذلك بأية طريقة كانت،..." و قرر المشرع في المادة 344 تشديد العقوبة السابقة، أي تقرير الحبس من خمس إلى عشر سنوات و بغرامة من 10000 إلى 100000 دج اذا ارتكبت الجريمة ضد قاصر لم يكمل التاسعة عشرة. و على هذا يمكن أن تتم هذه الجريمة عن طريق الانترنت، و هذا ما يستخلص من عبارة "بأية طريقة كانت". أما فيما يخص

1- أشار اليه عبد الله عبد الكريم عبد الله: جرائم المعلوماتية و الإنترنت، الطبعة الأولى،منشورات الحلبي الحقوقية، بيروت، 2007، ص 70.

2- محسن بن محسن بن باعث الرويلي، الرجع السابق، ص 39.

3- يهدف المشرع الجزائري من خلال هذه النصوص إلى حماية الطفل من الفساد. و يعتبر السماح للطفل بدخول الحانات و تحريضه على تناول الخمر أو مشاهدة الأفلام الخليعة يعد فعلا من شأنه تعريض أخلاقه للفساد.

4- يقصد بالجريمة العرضية: اذا كان الطفل قاصر لم يكمل 16 سنة. أما الجريمة في صورة اعتياد يقصد بها: أن القاصر أكمل سن 16 سنة و لم يبلغ 19 سنة. د/ عبد العزيز سعد: الجرائم الأخلاقية في قانون العقوبات، الشركة الوطنية للنشر والتوزيع، الجزائر،1982، ص 84

جريمة الاستغلال الجنسي للأطفال فالمشرع الجزائري صمت حيال هذه الجريمة الخطيرة و التي يكون ضحيتها الأطفال، أي انعدام وجود نص صريح بشأن العقاب على هذه الجريمة في قانون العقوبات الجزائري . ومع ذلك فإنه" يعاقب بالحبس من خمس إلى عشرة سنوات كل من ارتكب فعلا مخلا بالحياء ضد قاصر لم يكمل السادسة عشرة ذكرا كان أو أنثى بغير عنف أو شرع في ذلك.ويعاقب بالسجن المؤقت من خمس إلى عشر سنوات أحد الأصول الذي يرتكب فعلا مخلا بالحياء ضد قاصر ولو تجاوز السادسة عشرة من عمره ولم يصبح بعد راشدا بالزواج.[1]

وإذا وقعت جريمة ارتكاب الفعل المخل بالحياء ضد إنسان على قاصر لم يكمل السادسة عشرة يعاقب الجاني بالسجن المؤقت من عشر سنوات إلى عشرين سنة[2].

وإذا وقع هتك العرض ضد قاصرة لم تكمل السادسة عشرة فتكون العقوبة السجن المؤقت من عشر سنوات إلى عشرين سنة. [3]معتبرا ذلك انتهاكا للآداب العامة للمجتمع.

هذا من جهة و من جهة أخرى، يمكن القول بتطبيق المادة 394 مكرر2 من قانون العقوبات الجزائري على الجرائم الجنسية الواقعة عبر الانترنت. إذ نص على معاقبة كل من سولت له نفسه بالقيام عمدا و عن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار أو حيازة أو استعمال لأي غرض كان المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية. فإذا كانت هذه المعطيات تحوي صورا إباحية كنا أمام جريمة جنسية .

و لكن و في ظل غياب نص قانوني يضمن الحماية الكاملة للطفل من هذه الجرائم عامة وعبر شبكة الإنترنت خاصة فإنه بإمكان المؤسسات المعنية وضع نظم تحجب المواقع نهائيا على الكبار والصغار على السواء.و هذا ما أكده وزير الاتصال وتكنولوجيات الاتصال الجزائري السيد موسى بن حماد في تصريحه لجريدة الشروق اليومية من" أن الميثاق المتعلق بحماية الاطفال من مخاطر استعمالات الانترنت، والذي ساهمت فيه وزارة البريد ممثلة في مجمع اتصالات الجزائر في إعداده إلى جانب عدد من الوزارات والهيئات المعنية و الذي تم تدعيمه بسلسلة من النصوص التشريعية التي من شأنها العمل على حماية حقوق هذه الشريحة من المجتمع ,سيدخل حيز التنفيذ مع مطلع سنة 2012 [4]. و هذا ما تم فعلا في 22 أوت

---

[1]– المادة 334 قانون العقوبات الجزائري.

[2]– المادة 335 قانون العقوبات الجزائري.

[3]– المادة 2/336 قانون العقوبات الجزائري.

[4]– إن أي مجهود لتطوير تكنولوجيات المعلومات و الاتصالات لا يمكن أن يتحقق إذا لم تحض حماية الأطفال بالاهتمام اللازم. لذلك أطلقت وزارة البريد و تكنولوجيات الإعلام و الاتصال مشروعا انضمت إليه عدة قطاعات حكومية و كانت ثمرته الاتفاقية لحماية الأطفال في الفضاء السيبراني الموقعة في 2009 من طرف الهيئات الفاعلة في وزارة الدفاع الوطني ووزارة الداخلية و الجماعات المحلية و وزارة التربية الوطنية و الوزارة المنتدبة المكلفة بالأسرة و قضايا المرأة.

و من أهم ما نصت عليه الاتفاقية هو ضرورة وضع خطة وطنية لحماية الأطفال من مخاطر الاستعمالات السلبية للإنترنت. من أجل تحقيق ذلك تم إنشاء فريق عمل مكون من ممثلين عن الشركاء الفاعلين و عن المتعامل العمومي

2013 حيث أطلقت شركة إتصالات الجزائر نظاما جديدا لحجب المواقع الإرهابية و الإباحية و غير المرغوب فيها أطلق عليه تسمية " في أمان"[1] و الذي من خلاله يسمح للأولياء بمراقبة حركة تصفح الإنترنت لأبنائهم لحمايتهم من التأثيرات السلبية لتلك المواقع غير المرغوب فيها و كذا الإدمان على الإنترنت من خلال ضبط التوقيت الذين يرونه مناسبا.[2]

ومن الجرائم الجنسية التي وقعة عبر شبكة الإنترنت نذكر على سبيل المثال:

– في الولايات المتحدة الأمريكية قامت المباحث الفدرالية عام 1997 بالقبض على 1500 شخص مشتبه فيهم بالتعامل في دعارة الأطفال عبر شبكة الإنترنت وبث صور ماجنة للقصر في قضية Opération Rip lord. ولقد قادت عمليات البحث والتقصي حول دعارة الأطفال عبر الإنترنت في ألمانيا والمملكة المتحدة والولايات المتحدة الأمريكية إلى الكشف عن مائتين ألف صورة من صور دعارة الأطفال، كما تمت مصادرة مائة وسبعة وثلاثين ألف حاسوب شخصي منزلي. كما قامت المباحث الفدرالية الأمريكية بالتحقيق في قضية أطلق عليها Innocent Images، وهو التحقيق الذي بدأ إثر اختفاء طفل أمريكي في ولاية مريلاند في العاشرة من عمره. وهي القضية التي أدين فيها 161 شخصا.

– أما بالنسبة للشرطة الإنجليزية ففي عام 1995 قامت بعملية سميت بـ: Opération Starburst استخدمت فيها الإنترنت كمجال لدعارة الأطفال وتوزيع صور فاضحة لهم، ولقد أدين في هذه الجريمة تسعة رجال إنجليز. كما تم الاستدلال على مجموعة أخرى– لاسيما أنها قضية اتخذ فيها التحقيق بعدا دوليا– عبر أوربا وأمريكا اللاتينية وشرق آسيا ووصل حينئذ عدد المدانين فيها 37 شخصا. وفي العام 1998 قام البوليس الإنجليزي بعملية كبرى أطلق عليها اسم Cathédral بالتعاون مع الشرطة في 21 دولة في أوربا وأستراليا والولايات المتحدة الأمريكية والبوليس الدولي (الأنتربول) بضبط حوالي مائة شخص ممن يتعاملون في دعارة الأطفال عبر الانترنت. وفي شهر أكتوبر 2000 قام المدعي العام الإيطالي Alfredo Ormanni بإحالة 831 متهما إلى القضاء الجنائي بتهمة إنزال صور دعارة أطفال عبر الإنترنت واستدعاء 660 من جنسيات أجنبية يعتقد أن أغلبهم من روسيا وفرنسا وماليزيا.[3]

"اتصالات الجزائر" . ينظر لمزيد من التفاصيل الخطة الوطنية لحماية الأطفال في الفضاء السيبراني، www.itu.int http://. نوارة باشوش: نظام معلوماتي لحماية الأطفال من تفحص مواقع العنف والإباحية ، جريدة الشروق اليومي 2011/12/18، ص 4.

[1]– برنامج في أمان هو عبارة عن برنامج يشبه البرامج المطاردة للفيروسات وضع خصيصا لتمكين الأولياء من مراقبة أطفالهم عند إبحارهم على شبكة الإنترنت و منعهم من الوصول و الدخول إلى المواقع الحساسة كالمواقع الإرهابية و الإباحية. إتصالات الجزائر تعلن عن حلول رقابة لفائدة الأولياء على الإنترنت، جريدة الأحداث الجزائرية، http:// www.elahdath.net، و ينظر كذلك لمزيد من التفاصيل عن هذا البرنامج ينظر إتصالات الجزائر، خدمة مراقبة تصفح الإنترنت " في أمان" تدخل حيز الخدمة اليوم، الإذاعة الجزائرية، www.radioalgerie.dz http://، إتصالات الجزائر تطلق "في أمان" لمراقبة إستخدام الأطفال للإنترنت، جريدة المساء،http:// www.el-massa.com

[2]– ينظر هكذا سيمنع الآباء أبنائهم من دخول المواقع الإرهابية و الإباحية،http://www.elbilad.net

[3]– د/عمر محمد أبو بكر بن يونس، المرجع السابق، ص456

وتعتبر هذه الأمثلة من الوقائع الكبرى في مكافحة جريمة دعارة الأطفال عبر الإنترنت.

– وفي إسبانيا أعلنت الشرطة الإسبانية أنها فكت شبكة دولية تعتبر الأكبر في مجال ترويج الصور الإباحية للأطفال على نطاق أوربا حيث بلغ مجموع ما قامت بنشره وتوزيعه عبر شبكة الإنترنت نحو عشرون ألف ما بين صورة وفيلم فيديو.[1]

– وفي الصين قضت إحدى محاكم في جزيرة هونج كونج في 2003 بالسجن لمدة عام على شخص بعد إدانته بالتحرش الجنسي بفتتاين عن طريق شبكة الإنترنت، حيث قام بإرسال بريد الكتروني إباحي لهن يضم صورا إباحية وقصص مرعبة عن حوادث اغتصاب الطالبات[2].

– وفي إسرائيل قام حزب العمل الإسرائيلي ببث صور عارية لزوجة رئيس الوزراء الإسرائيلي الأسبق "نتنياهو" عن طريق البريد الالكتروني.

– وذات الشأن بالنسبة لدولة الإمارات العربية المتحدة حيث قضت محكمة أبو ظبي على شخص قام ببث صورة لامرأة عارية إلى المشتركين في البريد الالكتروني والتي تبدأ أسماءهم بحروف (xx7) بغرامة قدرها 10 آلاف درهم مع مصادرة الصورة المضبوطة.[3]

– وفي لبنان تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الإنترنت وذلك إثر تلقي النيابة برقية من الأنتربول بهذا الخصوص في ألماني.[4]

– وفي السعودية قامت شرطة الظهران الشرقية بالقبض على سعودي ثلاثيني قام بإنشاء موقع إباحي على شبكة الإنترنت بهدف التحرش بالذكور.[5]

– وفي مصر قام أحد الأشخاص باستغلال امتلاكه لوكالة أزياء واستدراجه الفتيات لإيقاعهن في العمل في الدعارة عن طريق الدعاية لذلك بالإعلان عبر الإنترنت بطلب فتاة لشغل وظيفة مساعدة لمدير محطة تليفزيونية أو عارضة أزياء بإحدى الوكالات الأجنبية، وأن الوظيفة تتطلب ارتدائهن لملابس تظهر أجسادهن تحت إغراء المال والشهرة. واتضح أن عرضه أباحي ليعملن بالدعارة. حيث تم ضبط رسائل جنسية فاضحة تحتوي صورا ببريده الالكتروني.[6]

---

[1] –http://www.aljazeera.net

[2] – د/عبد الفتاح بيومي حجازي،(نحو صياغة نظرية عامة في علم....) مرجع سابق، ص 202.

[3] – د/عبد الفتاح بيومي حجازي، المرجع السابق، ص 203.

[4] – د/ حسين الغافري، محمد الألفي، المرجع السابق، ص89.

[5] – محسن بن محسن بن باعث الرويلي، المرجع السابق، ص 39.

[6] – محسن بن مسحن بن باعث الرويلي، نفس المرجع ، ص 40.

خلاصة الباب الأول:

لقد استغل مجرمو القرن الحادي و العشرين السلبيات التي أفرزتها شبكة الإنترنت لخدمة أهدافهم الإجرامية ؛ اذ أصبحت تستخدم كسلاح فتاك و لا مثيل له في ارتكاب جرائم كانت تعتبر في الماضي صعبة وتحتاج الى جهد عضلي و عنف، و منها جرائم الإعتداء على الأشخاص التقليدية و التي وجد هؤلاء الأخيرين ضالتهم المنشودة في ارتكابها في تلك البيئة الرقمية بكل راحة و طمأنينة، و ذلك بمجرد الضغط على زر واحد من لوحة مفاتيح الحاسوب المربوط بالإنترنت، و هم جالسين في أماكنهم ومحتسين لمشروباتهم ودون الحاجة الى مبارحتها. و من أكثر صور جرائم الإعتداء على الأشخاص وقوعا عبر شبكة الإنترنت: **جرائم البث العلني** و التي تضم الجرائم الماسة بسمعة الأشخاص و شرفه و اعتباره وجرائم النشر الإلكتروني والعنف **وجرائم الإعتداء على حرمة الحياة الخاصة و جرائم المطاردة والجرائم الأخلاقية** والتي تضم جرائم انتهاك الأداب العامة و الجرائم الجنسية، حيث أن النتائج المتوصل اليها في هذا الفصل هي على الشكل التالي:

أولا–فيما يخص الجرائم الماسة بسمعة الأشخاص و شرفه و اعتباره عبر الإنترنت، فانها تقع بواسطة إنشاء مواقع خاصة بقذف وسب والتشهير سواء بشخص معين أو بدولة من الدول أو بدين من الأديان.

تتنوع صور القذف و السب و التشهير عبر الانترنت بتنوع الغرض و الطريقة التي تستخدم بها تلك الأخيرة، فقد يكون وجاهيا عبر خطوط الاتصال المباشر، أي عن طريق المبادلات الاليكترونية الصوتية، أو كتابيا أو غيابيا عن طريق المبادلات الاليكترونية الكتابية أو فيديوية. و هي إما أن تكون بين طرفيات انترنت متصلة، وإما أن تكون بواسطة طرفية انترنت منفصلة.

ثانيا–أما فيما يخص جرائم النشر الإلكتروني و العنف عبر الانترنت فهي تلك الأفعال غير المشروعة المتصلة بأعمال الصحافة و المرتكبة عبر شبكات الحاسب الآلي.ولا يستدعي النشر عبر الإنترنت لزوم إتخاذ الإجراءات القانونية التي يتطلبها القانون لنشر صحيفة في العالم المادي.

أما الكلام عن العنف عبر الإنترنت فمعناه أن تلك الشبكة قد تكون سببا لدفع مستخدميها الى العنف والتشاجر مع الآخرين أو تكون سببا في ارتكاب جرائم قتل.

ثالثا–أما ما يتعلق بجريمة الإعتداء على حرمة الحياة الخاصة، فانها تتحقق بكل اعتداء على البيانات الاسمية عبر الانترنت، و ذلك عن طريق التمركز في موقع معين داخل شبكة الانترنت و العمل على تسجيل و حفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية، ويكون التمركز عن طريق استغلال النقاط الضعيفة في منظومة الأمن باستخدام مبرمجات الحواسيب، ومن الأساليب الإجرامية الشائعة في التعدي على الخصوصية عبر الإنترنت: استعمال بيانات شخصية غير حقيقية،جمع أو معالجة بيانات حقيقية بدون ترخيص،إنشاء بيانات بصورة غير قانونية وإساءة استعمالها،عدم الالتزام بالقواعد الشكلية الخاصة بتنظيم عملية وجمع ومعالجة ونشر البيانات الشخصية.

رابعا- أما فيما يتعلق بجريمة المطاردة عبر الإنترنت، فيقصد بهاكل سلوك يتسم بالتطفل والخبث على شبكة الإنترنت وتستخدم فيه هذه الشبكة لارتكاب نوعين من هذا السلوك: جمع معلومات خاصة عن المجني عليه ليقرر ويدعم المطاردة، الاتصال بالضحية مع تهديدها الضمني أو العلني لتعزيز الخوف.

خامسا- في حين فان جريمة انتهاك الآداب العامة عبر الإنترنت، فانها تعني كل فعل يتضمن مخالفة القواعد الأخلاقية الأساسية التي يبنى عليها المجتمع و كذا تعاليم كافة الأديان السماوية و ذلك باستخدام الانترنت كنشر و بث الصفحات الخادشة والمخلة بالحياءعبر مواقعه أو إنتاج أو إعداد أو تهيئة أو إرسال أو تخزين أو ترويج أي محتوى يخل بالحياء أو النظام العام والآداب عن طريق شبكة المعلومات.

سادسا- أما الجرائم الجنسية عبر الإنترنت، فتتحقق ببث الصور الماجنة والمقالات الفاضحة والأفلام الخليعة عبر الانترنت و على مواقع مخصصة لذلك، غايتها تحقيق الربح المادي تسمى بالمواقع الجنسية الإباحية أوعن طريق الدردشة الإباحية والقوائم البريدية الجنسية.

ومن أسباب انتشارها سهولة الوصول و تحميل الملفات الإباحية التي تتمتع بنفس السهولة التي يمكن الوصول فيها إلى ملفات الموسيقى (MP3) وتحميلها.

الباب الثاني:

جرائم الإعتداء على الأموال عبر الانترنت

لم تقتصر أساليب إساءة استخدام الثورة المعلوماتية على الإعتداء على الأشخاص، بل تعدتها لتطال الذمة المالية للغير، لاسيما فيما يخص إساءة استخدام تقنية الانترنت التي أتاحت– نظرا لما تتمتع به من خصائص فريدة من نوعها – الفرصة لمجرمي المعلوماتية و هيأت لهم المناخ المناسب في تسهيل ارتكاب شتى أنواع الجرائم المالية و ذلك بكل ارتياح و طمأنينة بجلوس الشخص وراء حاسوبه المرتبط بالانترنت وبارتكاب ما شاء له من الجرائم كانت في السابق تصعب عليه، و ذلك بمجرد النقر بأقل مجهود ممكن ومن دون خسائر مالية على لوحة مفاتيح الحاسوب المربوط بالانترنت. و على هذا ظهرت صور مستحدثة من هذا النوع من الجرائم محلها الأموال ووسيلة ارتكابها الانترنت.

و يمكن تعريف جرائم الأموال بأنها:" تلك الجرائم التي تقع على الحقوق المالية للإنسان [1]. و هي تشمل كافة الأموال سواء المنقولة أو العقارية." [2]

و يقصد بالمال كل نافع للإنسان، و كل ما يشبع حاجته يسمى مالا. و هو نوعان إما مادي أو معنوي تبعا لما إذا كانت الحاجة التي يشبعها مادية أو معنوية[3]. وعليه فالإعتداء على المال قد يكون محله عقارا (مالا ماديا) حين يتخذ صورة الحرق و التخريب والإتلاف وانتهاك حرمة ملك الغير، وإزالة الحدود أو محو معالمها و إتلافها. و قد يكون الإعتداء على المال المنقول (سواء أكان ماديا أو معنويا كالأفكار) [4] حين يتخذ صورة السرقة والنصب و خيانة الأمانة و الإعتداء على الملكية الأدبية.

و يمكن تقسيم الجرائم المالية التي تتم عبر الإنترنت إلى:

- جرائم السرقة و النصب
- جرائم الإعتداء على الملكية الفكرية
- جرائم غسل الأموال و المخدرات
- جرائم الإعتداء على التجارة الاليكترونية

و لقد خصصنا هذا الباب لدراسة هذا النوع من الجرائم و الذي قسمناه إلى ثلاث فصول كالآتي:

---

[1]– د/ حسين فريجة: شرح قانون العقوبات الجزائري، جرائم الإعتداء على الأشخاص – جرائم الإعتداء على الأموال، ديوان المطبوعات الجامعية، الجزائر، 2006، ص 187

[2]– لقد عرفت المادة 683 من القانون المدني الجزائري العقار بأنه:"كل شيء مستقر بحيزه و ثابت فيه،و لا يمكن نقله من دون تلف. أما ما عداه عبارة عن منقول". لمزيد من التفاصيل ينظر د/إسحاق إبراهيم منصور، المرجع السابق، ص 260 وما بعدها

[3]– د/ طارق إبراهيم الدسوقي عطية،(الأمن المعلوماتي) مرجع سابق، ص 255.

[4]– المال المعنوي هو الذي يكون له كيان ملموس فهو غير محسوس و غير مادي مثل الأفكار و الابتكارات و المخترعات و الألحان الموسيقية. و لذلك تسمى الحقوق التي ترد على المال المعنوي بالحقوق الأدبية و الحقوق الذهنية. د/ إسحاق إبراهيم منصور، المرجع السابق، ص 252.

الفصل الأول: جريمة السرقة و النصب والإعتداء على الملكية الفكرية عبر الانترنت.
الفصل الثاني: جرائم غسل الأموال و المخدرات عبر الانترنت.
الفصل الثالث: جرائم الإعتداء على التجارة الاليكترونية عبر الانترنت.

الفصل الأول:

جريمة السرقة والنصب والإعتداء على الملكية الفكرية عبر الانترنت.

تعتبر هذه الجرائم من الجرائم التقليدية التي تقع على الأموال المنقولة(سواء المادية أو المعنوية) في أغلب الأوقات، ولقد عرفت انتشارا واسعا عبر شبكة الانترنت[1]. الأمر الذي دق ناقوس الخطر و دفع بمجموعة متخصصة في أبحاث التكنولوجيا في الولايات المتحدة الأمريكية من تحذير مستخدمي الانترنت بأنهم على الدوام هم عرضة للسرقة و النصب والإعتداء على الملكية الفكرية عبر هذه الشبكة، و أنه من المرجح تضاعف ضحايا هذه الجرائم في الأعوام القادمة، وذلك بسبب عدم كفاية الجهود المبذولة لتنفيذ القانون وتزايد فرص لارتكاب الجرائم عبر الانترنت اللذان قد تركا الباب مفتوحا أمام سرقة ملايين الدولارات.[2]
و لقد تم التطرق في هذا الفصل إلى هذه الجرائم الخطيرة و الأوسع انتشارا عبر الانترنت و ذلك بتقسيمه إلى المباحث التالية:

المبحث الأول: جريمة السرقة عبر الانترنت
المبحث الثاني: جريمة النصب عبر الانترنت
المبحث الثالث:جريمةالإعتداء على الملكية الفكرية عبر الإنترنت.

المبحث الأول:

جريمة السرقة عبر الانترنت

السرقة هي اختلاس مال منقول مملوك للغير بقصد تملكه. و هي تعد من أخطر أنواع العدوان على المال في العالم المادي؛ إذ تحتل المرتبة الأولى في هذا الشأن. و هي تقوم على أركان ثلاثة: موضوع أو محل الإعتداء و يتمثل في مال منقول ذا طبيعة مادية مملوك للغير. و تكمن العلة في ذلك أن جريمة السرقة هي في الأصل جريمة اعتداء على الملكية[3].و ركن مادي هو فعل الاختلاس أي نقل الحيازة المادية

---

[1]– الأسباب التي ساعدت في انتشار هاتين الجريمتين: مجهولية المصدر بالنسبة إلى مستخدمي هذه الشبكة، فضلا عن عدم توفر سبل الحماية الكافية للحد من تلك الجرائم. ينظر وليد الزيدي، المرجع السابق، ص 65.

[2]– وليد الزيدي، نفس المرجع، نفس الموضع.

[3]– عماد علي الخليل: التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت، دراسة عملية في ظل أحكام قانون العقوبات الأردني، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الإنترنت، 2000، ص8.

للأموال إلى السارق بدون رضا مالكها. و ركن معنوي يتخذ صورة القصد الجنائي الذي يتضمن من بين عناصره نية تملك المال المختلس[1].

و لقد جرمت تشريعات العالم العقابية المختلفة هذه الجريمة[2]، و صنفتها كسيدة جرائم الإعتداء على الأموال في العالم المادي.

و كغيرها من الجرائم فقد تأثرت هذه الأخيرة بالتقدم التكنولوجي و المعلوماتي و ما وفره من تسهيلات في ارتكابها من طرف مريضي الأنفس في وقت قصير جدا و من أماكن بعيدة و باستخدام التقنية العالية في تنفيذها من حاسب آلي و انترنت. و هذا ما أدى إلى إفراز جريمة مستحدثة في جرائم الإعتداء على الأموال تسمى بالسرقة المعلوماتية، أين تكون المعلومة هي موضوع الإعتداء و يكون الحاسوب أداةلارتكابها. و الى ظهور نوع جديد من هذه الأخيرة و هو السرقة عبر الانترنت أين تستخدم فيها الانترنت كأداة تخزين و حيازة و تعامل بالمال المعلوماتي.و الاشكال المطروح هنا هو: ماذا نعني بهذه ؟ وهل تختلف عن مثيلتها التقليدية ؟ و ما هي أركانها؟و ما هو التكييف القانوني لها؟.

و سيتم الإجابة على هذه الإشكالات وفق المطلبين التاليين:

المطلب الأول: ماهية السرقة عبر الانترنت.

المطلب الثاني: موقف التشريعات المقارنة من السرقة عبر الانترنت

المطلب الأول

ماهية السرقة عبر الانترنت.

و سنتطرق في هذا المطلب إلى تعريف السرقة عبر الانترنت في الفرع الأول و إلى أركان هذه الجريمة المستحدثة الواقعة على الأموال في الفرع الثاني. و ذلك كما يلي:

الفرع الأول: تعريف السرقة عبر الانترنت.

الفرع الثاني: أركان السرقة عبر الانترنت.

الفرع الأول: تعريف السرقة عبر الانترنت

تختلف السرقة في العالم المادي عن تلك الواقعة في العالم الإفتراضي في كون أن محل الإعتداء هو المعلومات، و التي تعتبر مالا معلوماتيا ذا طبيعة معنوية التي لا يمكن أن تقع في حيازة مادية مباشرة من قبل السارق.

هذا من جهة و من جهة أخرى، ذلك أن المعلومات لكي تكون جزء في عالم الانترنت و تكنولوجيا المعلومات لابد أن تمر بمرحلة القيام بمعالجتها ثم تخزينها في قالب يجعلها مؤهلة للقيام بدور معلوماتي.

---

[1]– د/ حسين فريجة، المرجع السابق، ص 188.

[2]– ينظر ص 187 من هذه الرسالة.

هذا ويجب لكي تتمتع هذه الأخيرة بهذه الصفة أن تكون محلا للاستدعاء من قبل طالبها، و إلا كانت مجرد بيانات ذات الطابع الثنائي. كما يجب أن يكون هذا الأخير على بينة من المعلومات المراد سرقتها عبر الانترنت. لذلك نجد أن استخدام تكنولوجيا المعلومات لارتكاب سرقة تحتاج إلى منطق استيعاب فكرة استدعاء المعلومة المراد سرقتها، أو نسخ كافة البيانات التي يراد التعرف من خلالها عليها[1].

كما أن السرقة في ظل تكنولوجيا المعلومات قد تراجعت عن مكانتها و مرتبتها التي تحتلها في العالم المادي، اذ يتسيد الأمر هناك جريمة النصب و الاحتيال. لدرجة أن هناك اتجاه يحصر جرائم الأموال عبر الانترنت في تلك الجريمتين لا غير[2].

و على هذا يمكن تعريف السرقة عبر الانترنت بأنها اختلاس للمعلومات و نقلها من حيازة صاحبها (و إن لم تكن حيازة كاملة) إلى الغير باستخدام الانترنت و ذلك إما بالدخول إلى بعض المواقع وسرقة بطاقات الإئتمان مثلا و من ثم الحصول على أموال من جراء ذلك، أو بدخول الجاني على حساب بعض العملاء في المصارف و تحويل تلك الأخيرة إلى حسابه الخاص و ذلك باستخدام برمجيات معينة، أو عن طريق نسخ الملفات أو نقل محتوى المعلومات باستخدام الفيروسات و دود الإنترنت.

و هي بهذا و كنظيرتها التقليدية تقوم على ثلاثة أركان و لكن تتميز بطبيعة خاصة نظرا للوسط الذي ترتكب فيه، أي من موضوع أو محل الإعتداء و ركن مادي و ركن معنوي.

الفرع الثاني: أركان السرقة عبر الانترنت.

تقوم جريمة السرقة عبر الانترنت على ثلاثة أركان تتميز بطبيعة خاصة نظرا للوسط الذي ترتكب فيه، وهي موضوع أو محل الإعتداء و يتمثل في المعلومات أو بالأحرى المال المعلوماتي و ركن مادي و يتمثل في فعل الاختلاس المعلوماتي و ركن معنوي و يتمثل في القصد الجنائي.و سيتم تفصيل كل ركن على حدى كما يلي:

أولا: موضوع أو محل السرقة عبر الانترنت:

يشترط لقيام السرقة عبر الانترنت شرطان وهما أن يكون موضوع السرقة مالا و أن يكون مملوكا للغير ومنقولا.

1/ أن يكون موضوع السرقة شيء مادي:

تختلف السرقة عبر الانترنت في نقاط كثيرة عن السرقة التقليدية، ومن أهمها أنها ترد على معلومات تأخذ شكل نبضات إليكترونية وذات طبيعة معنوية.على عكس السرقة التقليدية و التي ترد على مال منقول ذا طبيعة مادية ملموسة أو محسوسة. فهل تعتبر المعلومات مالا ليصلح محلا للسرقة؟.

اختلفت الآراء الفقهية في تحديد ما إذا كانت المعلومات تعد أموالا أم لا، و انقسمت إلى اتجاهين متباينين:

---

[1]– د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 407.

[2]– د/ عمر محمد أبو بكر بن يونس، نفس المرجع ، ص 399.

أ- اتجاه معارض لإضفاء وصف المال على المعلومات: يرى هذا الاتجاه عدم صلاحية المعلومات لأن تكون محلا للاعتداء عليها. و يرجع ذلك إلى طبيعتها، فهي من طبيعة معنوية لا مادية؛إذ أن الأشياء المحسوسة فقط هي التي تعتبر من قبيل الأشياء المادية، و انعدام الكيان المادي للمعلومات لا يجعلها محلا لحق مالي من نوع الحقوق المتعارف عليها في الفقه التي ترد على كيانات مادية، مما يؤدي إلى ضرورة استبعادها من طائفة الأموال[1].

ب- اتجاه مؤيد لإضفاء وصف المال على المعلومات:

و على عكس الاتجاه الأول، فأنصار هذا الاتجاه يرون صلاحية المعلومات لأن تكون محلا للاعتداء عليها؛ و ذلك باعتبارها أنها في حد ذاتها مالا ماديا. أما الطبيعة المعنوية لها فهي تعكس طبيعة حق صاحب الشيء عليها[2]. و يستند فقهاء هذا الاتجاه لتبرير صلاحية خضوع المعلومات المختزنة في الحواسيب و المتبادلة عن طريق شبكة الشبكات أو الشبكات الداخلية لوصف السرقة إلى الحجج التالية:

- شمول كلمة شيء (Chose) الواردة في المادة 311 من قانون العقوبات الفرنسي الجديد للأشياء المادية و غير المادية. و بالتالي من الممكن حيازة المعلومات و في المقابل سلب هذه الحيازة.

- أن الاستيلاء على المعلومة لا يمكن أن يتحقق عن طريق السمع أو المشاهدة، ومن ثم يمكن أن تنتقل المعلومة من عقل لآخر، و من ذمة مالية إلى أخرى.كون المعلومة محل الاختلاس يمكن تحييزها داخل إطار و الاستئثار بها، و ذلك بتدوينها أو بتسجيلها على دعامة و حرمان صاحبها من الانتفاع بها.[3]

- إن سرقة المعلومات (وليس سرقة الدعامة) هي السبب الذي من أجله أدانت محكمة النقض الفرنسية عاملا قام بنسخ مستندات سرية بدون علم و رضا المالك الشرعي. كما أدانت هذه الأخيرة شخصا بتهمة إخفاء معلومات تتعلق بسر التصنيع. و على شخص آخر لكونه قدم للمحكمة صورة منسوخة من مستند مسروق أعدها بنفسها و بمعرفة شخص مجهول الهوية. [4]

- أن المعلومة قابلة للتحديد و القياس مثل الطاقة الكهربائية، إذ يمكن قياسها بمقياس معين (كالبايت والكيلوبايت، و الميجابايت) [5].

- إن المعلومة منفصلة عن دعامتها المادية هي مال يمكن تملكه لما له من قيمة اقتصادية، فهي تطرح في السوق للتداول مثلها مثل أي سلعة و لها سوق تجاري يخضع لقوانين السوق الاقتصادية. و على هذا يمكن للجاني استغلال المعلومات بأن يبرم عقود مع الغير كتأجيرها و بيعها أو حفظها أو تقويمها باعتبارها

---

[1]- ينظر كلا من د/ السيد عتيق، المرجع السابق، ص 880.

-PASCAL Alix : Le droit de l'entreprise,(Virtualegis), 3/8/2009, http:// virtualegis.com.

[2]- د/ السيد عتيق، المرجع السابق ، الموضع السابق.

[3]- محمد أمين أحمد الشوابكة، المرجع السابق، ص152

[4]- Voir M.CHAWKI : Le vol d'information، quel cadre juridique aujourd'hui ?، Droit-Tic، Juillet 2006، p5.

[5]- د/ السيد عتيق،المرجع السابق، ص 89.

خدمة. و بحيث تكون هذه المعلومات المخزنة أو المنقولة محلا لها، و بالتالي حرمان صاحبها من عائدها المادي[1].

أما فيما يخص القضاء الفرنسي فقد اعترف بتوسيع مصطلح الشيء الواردة في المادة 311 من قانون العقوبات الفرنسي الجديد ليضم البرامج المعلوماتية، و بالتالي امكانية وقوع السرقة على معطيات معلوماتية[2]. كما أنه كان يرفض اعتبار المال المعلوماتي مندرجا في إطار فكرة الملكية. و بالتالي يصعب تناوله في إطار جريمة السرقة،إلا أن الحال تطور لهذا المفهوم لكي يصبح المال المعلوماتي محل الاختلاس، أي أصبح مدلول السرقة يتسع لمدلول العالم الإفتراضي أيضا[3].

2/ أن يكون موضوع السرقة منقولا و مملوكا للغير:

يشترط القانون لقيام جريمة السرقة أن يكون الشيء محل الاختلاس منقولا و مملوكا للغير؛ أي أن يتم اختلاس المال بنزع حيازته من مالكه الأصلي و إدخاله في حيازة الجاني. و هذا ما ينطبق مع الأموال المعلوماتية المادية و ما يؤكده القانون رقم 652/82 الصادر في 29 جويلية 1982، و الذي عرف المعلومات على انها:"أصوات و صور و وثائق و معطيات أو رسائل أيا كانت طبيعتها". وعلى هذا فهي تصلح لأن تكون محلا للسرقة و ذلك بالاستيلاء عليها و تبديل حيازتها.

هذا من جهة و من جهة أخرى، يلزم أن يكون المال المنقول ملكا للغير وقت الاختلاس. إذ لا تقوم جريمة السرقة إذا كان المال المنقول مملوكا للجاني وقت اختلاسه و لو كان للغير على هذا المنقول حقوقا تخوله حبسه و تجعله أولى بحيازته من مالكه، أو كان مالك الشيء ملزما بترك حيازته إلى غيره لسبب ما (كالوعد بالبيع). و كذلك الحال فيما لو استخدم الشخص مالا لا يملكه أحد و تصرف فيه، إذ يمثل اكتسابا مشروعا لملكيته[4].

ثانيا: الركن المادي.

يتمثل السلوك الاجرامي في جريمة السرقة عبر الانترنت في فعل الاختلاس و الذي يقصد به كل فعل يقوم به الجاني و يؤدي إلى انتزاع و أخذ أو الاستيلاء على مال الغير أو أي شيء منقول مملوك للغير بدون علم أو رضاء صاحب أو حائز هذا الشيء[5]. و لا يقوم الاختلاس إلا إذا توافر عنصران: عنصر مادي وهو الاستيلاء و تبديل الحيازة و عنصر معنوي و هو عدم رضاء مالك الشيء أو حائزه عن الفعل الذي وقع. و يسمى الاختلاس في هاته الجريمة بالاختلاس المعلوماتي. فماذا نعني به؟ و ما الفرق بينه و بين الاختلاس التقليدي؟.

---

[1]– آمال قارة، المرجع السابق، ص 17.

[2] –CA Anvers,13/12/1984,Paris,RDIT, 1986, p 224. Voir aussi Cass.Crim، 12/01/1989,Bull.Crim,n°4.

[3]– Voir M.CHAWKI ,(Le vol d'information….),op.cit,p11.

[4]– محمد أمين أحمد الشوابكة، المرجع السابق، ص 155.

[5]– د/ محمد صبيحي نجم، المرجع السابق، ص 116.

يذهب جانب من الفقه في تعريف الاختلاس المعلوماتي و المتعلق بسرقة المعلومات و البيانات المعالجة آليا بأنه "الاستيلاء على المعلومات و البيانات دون علم و إرادة صاحبه الشرعي سواء كانت مخزنة على أشرطة ممغنطة أو أسطوانات مدمجة "[1] كما هو الحال عندما يقوم الشخص بتوجيه المعلومات و البيانات الخاصة بالغير إلى حاسوبه الشخصي و يطلع عليها، أو يقوم بالتقاطها من خلال الموجات الكهرومغناطيسية التي يبثها الحاسوب، ثم يقوم بمعالجتها و إظهارها من جديد و بشكل واضح على حاسوبه الخاص. ففي هذه الحالة يتحقق الاختلاس المعلوماتي.

و في تعريف آخر يحصره في نطاق محدد يعرف الاختلاس المعلوماتي بأنه "الاستيلاء غير المشروع على الأرقام و المعلومات الخاصة بالبطاقات الائتمانية المملوكة للغير عبر شبكة المعلومات بهدف الحصول على السلع و الخدمات".[2] كما يعرف بأنه: "الحصول على معلومات التحويلات الإليكترونية للنقود أو الخدمات بقصد مشاركة أو حرمان من له الحق فيها"[3].

باستقرائنا لهذه التعريفات المختلفة للاختلاس المعلوماتي،يمكن القول أن الاختلاس المعلوماتي يتفق مع الاختلاس التقليدي في أنهما يقومان على نفس الفكرة. و الغرض منهما الاستيلاء على مال المجني عليه دون علم منه أو رضاه. كما أنهما لا يقومان إلا بتوافر عنصران: عنصر مادي و هو الاستيلاء و تبديل الحيازة، و عنصر معنوي و هو عدم رضا مالك الشيء أو حائزه أو عدم علمه.

و لكنهما في المقابل يختلفان في النقاط التالية:

أ- **في المحل:** يقع الاختلاس المعلوماتي على المعلومات أو بالأحرى على المال المعلوماتي الذي يعتبر ذا طبيعة معنوية.على عكس الاختلاس التقليدي الذي يقع على مال منقول ذا طبيعة مادية.[4]

ب- **في المفهوم:** و يرجع سبب ذلك إلى الوسائل و الطرق المعلوماتية التي تدخل في وقوع الاختلاس المعلوماتي. كما أن هذا الأخير تغلب فيه مشاركة الجاني لصاحب المعلومات في الانتفاع بها دون أن يتم حرمانه في الغالب منها، و ذلك بعكس الحال في مفهوم الاختلاس التقليدي الذي يشترط فيه حرمان المجني عليه من حيازة المال.[5]

---

[1]- د/ غنام محمد غنام: عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ،بحث مقدم لمؤتمر القانون و الكمبيوتر و الإنترنت، خلال الفترة من 1-3 ماي بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون، ص 12 و ما بعدها.

[2]- عماد علي الخليل: التكييف القانوني لاساءة استخدام أرقام البطاقات عبر شبكة الإنترنت،بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، خلال الفترة من 1-3 ماي بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون، ص 2.

[3]- د/ أيمن عبد الله فكري، المرجع السابق، ص 532.

[4]- ينظر د/ محمد صبحي نجم، المرجع السابق، ص121.

[5]- ينظر د/ دردوس مكي: القانون الجنائي الخاصفي التشريع الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر، 2007، ص14.

ج- **في الوسائل المستخدمة:** تختلف الوسائل المستخدمة في الاختلاس المعلوماتي. إذ تستخدم لارتكابه التقنية العالية من حاسب آلي- في الغالب- و انترنت(اذا ارتكبت السرقة عبر الانترنت). أما الاختلاس التقليدي فيستخدم فيه الوسائل التقليدية كالسرقة باستعمال مفاتيح مصطنعة. [1]

د- **في الخصائص:** يتميز الاختلاس المعلوماتي بعدة خصائص و منها كونه يعد من الجرائم العابرة للحدود،لا سيما اذا ارتكب بواسطة شبكة الانترنت. كما يصعب فيه الاثبات لانعدام الآثار المادية. [2]

و- **في صفات المجرم:** المجرم الذي يرتكب الاختلاس المعلوماتي هو مجرم يستخدم العقل و مهارته الفنية في ارتكابه، على عكس المجرم الذي يرتكب الاختلاس التقليدي فهو مجرم تقليدي عادي يعتمد على العنف و القوة في ارتكابه. [3]

ي- **في الشكل:**تأخذ صور الاختلاس المعلوماتي أشكالا ووسائل عديدة و خاصة إذا استخدمت فيه الانترنت، و لعل أشهرها استخدام دودة الانترنت للحصول على نسخ من المعلومات التجارية و المالية والاقتصادية. [4]

و السؤال المطروح هنا: هل تدخل الجرائم الناشئة عن الاستخدام غير المشروع للمعلومات ممن ليس لهم الحق في الاطلاع عليها في نطاق مفهوم الاختلاس لكي يمكن القول بقيام جريمة السرقة أم لا؟

و للإجابة على هذا التساؤل يجب التطرق إلى العنصرين الذي يقوم عليهما الاختلاس و هما:الاستيلاء وعدم رضا المجني عليه.

- الاستيلاء و تبديل الحيازة:

و تتحقق بإخراج الشيء من حيازة صاحبه إلى حيازة الجاني. و عليه هل يمكن أن ينطبق هذا الكلام على الاستيلاء الواقع على المعلومات المخزنة و المتبادلة بين الحواسيب عبر شبكة الانترنت؟.

ظهر اتجاهان مختلفان في الفقه الفرنسي حول تكييف واقعة اختلاس المعلومات، و ما إذا كانت تخضع للأحكام الخاصة التقليدية لجريمة السرقة أم لا. فذهب اتجاه إلى اعتبار أن المعلومات في حد ذاتها يمكن أن تكون موضوعا للسرقة، و بالتالي يمكن القول بتجريم سرقة المعلومات. فالنشاط المادي الصادر عن الجاني و المتمثل في الاستيلاء على المعلومات بأية وسيلة فنية على غير إرادة صاحبها أو حائزها الشرعي يعد اختلاسا تقوم به جريمة السرقة إذا اكتملت باقي أركانها[5]. ضف الى ذلك فقد ساوى هذا الاتجاه ما بين اختلاس مادة الشيء و قيمته ؛ فتجريد الشيء من قيمته كلها أو بعضها هو مما رأى فيه القضاء

---

[1]- محمد داحي: جريمتا السرقة و الإبتزاز، دراسة مقارنة، دار الهدى، الجزائر، 2006، ص 13.

[2]- ينظر ص42 من هذه الرسالة.

[3]- ينظر ص 45 من هذه الرسالة.

[4]- لمزيد من التفاصيل ينظر دودة حاسوب،http://ar.wikipedia.org . ديدان الإنترنت،http://www.4jam3a.net .

[5]- لمزيد من التفاصيل ينظر د/ السيد عتيق، المرجع السابق، ص 103.

الفرنسي أن يقوم به ركن الاختلاس[1]، و ذلك عندما طبق هذا الأمر في حالة الحصول على الطاقة الموجودة بالبطارية و ذلك دون أن يتم الاستيلاء على هيكلها المادي، و ذلك باعتبار أنه قد تم الاستيلاء على الطاقة. و هو ذات الأمر الذي يحدث عندما يقوم الشخص بنسخ أو نقل المعلومات التي لا يملكها ولا له حق التصرف فيها، و يترتب على ذلك حرمان مالكها من الاستئثار و الانتفاع بها.[2]

و تجدر الإشارة إلى أن فريق من أصحاب هذا الرأي يرى أن هنالك حالات لا يوجد فيها استيلاء بالمعنى التقليدي للكلمة، مثل إذاعة استعمال معلومات أو قراءة معلومات على الشاشة و إعادة نقل المعلومات على جهاز مملوك للجاني.

وقد أكد القضاء الفرنسي توافر ركن الاختلاس في الاستيلاء الواقع على المعلومات، و ذلك بتكييف المعلومة على أنها شيء، و ذلك في حكم لمحكمة Clermont-Ferrand في قضية تتلخص وقائعها في قيام موظفة باختلاس ملفات معلوماتية تحوي معطيات معلوماتية سرية عن مديرها السابق لاستغلالها لذاتها بعد تركها لعملها فيها، حيث قررت المحكمة "أن المتهمة قد اغتصبت هذه المعلومات التي تتعلق بمستخدمه السابق،و قد خانت الأمانة و أرتكبت جريمة سرقة. و قد حكم عليها بالحبس 3 أشهر مع إيقاف التنفيذ"[4] . و كذا في حكم لمحكمةMontpelier في قضية تتلخص وقائعها في قيام مبرمج بنسخ معلومات احتفظ بها لنفسه أثناء احدى الزيارات لمؤسسته الأولى بعد تركه لعمله فيها، حيث قررت المحكمة " أن المتهم قد اغتصب هذه المعلومات التي تتعلق بمستخدمه السابق، دون أن تنتقل اليه بحيازتها بطريقة أو بأخرى. و قد حكم عليه بشهر حبس مع ايقاف التنفيذ".[3]

و اذا كان هذا الاتجاه يقر بامكانية اختلاس المعلومات استقلالا عن دعامتها المادية، الا أن بقاء المعلومات في حيازة صاحبها بعد وقوع الاختلاس (بالنسخ أو نقل المحتوى المعلوماتي) ظلت مسألة تشكل عائقا كبيرا أمام أنصار هذا الاتجاه ؛ لكون أن هذا الأمر يتناقض و مفهوم الاختلاس الذي يقع على ملكية و حيازة المال المادي و الذي لا يقتصر فيه على مجرد المشاركة في الحصول على منفعة الشيء بل الاستيلاء عليه بجميع سلطاته و مكانته [4]. و على هذا الأساس استند أنصار الاتجاه المعارض إذ

---

[1]– كانت الموظفة (س) تشتغل في مؤسسة فرنسية و بعد سوء تفاهم بينها و بين مديرها، قامت هذه الأخيرة بقصد الإنتقام باختلاس معلومات سرية عن هذه المؤسسة و بيعها لعملاء آسياويين.لمزيد من التفاصيل ينظر :

– Première sanction d'un vol de données numériques par un tribunal، Article du 3/10/2011، Le Figaro، p 1 et suite،http:// le figaro.fr.

[2]– د/ علي عبد القادر القهوجي:الحماية الجنائية للبيانات المعالجة الكترونيا،بحث مقدم لمؤتمر القانون و الكمبيوتر والإنترنت، خلال الفترة من 1–3 ماي بجامعة الامارات العربية المتحدة، كلية الشريعة و القانون، ص67.

[4] –TGI de Clermont–Ferrand،Chambre Correctionelle, Jugement du 26 Septembre 2011, http://www.legalis.net

[3]– نقلا عن أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2000، ص492 و493.

[4]– د/ علي عبد القادر القهوجي،(الحماية الجنائية للبيانات و المعالجة الكترونيا) مرجع سابق، ص 68 و ما بعدها.

ذهبوا إلى عدم إمكانية خضوع المعلومات في حالة سرقتها للنصوص التقليدية، مستندين في ذلك إلى طبيعة المعلومات التي هي في الحقيقة عبارة عن شيء غير مادي و غير قابل للتملك،في حين أن السرقة هي جريمة اعتداء على الملكية أي تقع على الأشياء المادية القابلة للانتقال و الحيازة و التملك. و قدهذا ما أكدته أحكام القضاء الفرنسي المختلفة و منها حكم محكمة النقض الفرنسية الصادر في 1994، و القاضي بأن:"تقريب الحصول على خدمات عن بعد بواسطة الانترنت بسرقة التيار الكهربائي كان غير مناسب، إذ أن المعلومات هي إبداع فكري محمي بقوانين حماية حق المؤلف"[1].

أما بالنسبة لموقف الفقه العربي من هذا الاشكال، فالاتجاه الراجح يرى عدم امكانية تجريم تلك الحالات التي يتم فيها الإعتداء على المعلومات استقلالا عن دعامتها المادية في داخل إطارالاختلاس وفقا لجريمة السرقة، و ذلك بسبب طبيعتها غير المادية.[2]

- عدم رضا المجني عليه:

لا يكفي لتوافر ركن اختلاس المعلومات خروج تلك الأخيرة من حائزها أو مالكها إلى الغير. بل يلزم أيضا أن يتم كل ذلك بدون رضا المجني عليه. فإذا وجدالرضا انتفت الجريمة كلية. و حتى يكون الرضا نافيا للاختلاس يجب أن يصدر عن إدراك و إرادة حقيقةحرة، و أن يكون صادرا قبل وقوع الاختلاس أو معاصرا لوقوعه، لأن الرضا اللاحق لا ينفي الجريمة، بل قد يلعب دورا في تخفيف العقوبة أو التنازل عن المطالبة بالتعويض المدني[3].

و تتخذ جريمة السرقة في معنى الاختلاس المعلوماتي أبعادا جديدة من حيث الكيفية التي يمكن بها ارتكاب السلوك أو النشاط المادي. إذ قد تشكل الانترنت حلقة وصل بين السارق و بين المحل الذي تقع عليه الجريمة، و حلقة الاتصال هذه قد تتخذ الطابع الوقتي أو الطابع المستمر. فقد يقوم السارق بالحصول على ملفات في حاسوب مؤسسة اقتصادية كمصرف ما أو مؤسسة مالية، و ذلك باستخدام برمجيات تحقق هدفه مثل برمجيات « Sniffer». و قد حكمت محكمة باريس بانطباق المادة 3/323 من قانون العقوبات الفرنسي الجديد على واقعة استخدمت فيها مثل هذه البرمجيات بتجميع المعلومات[4]، فقد يقوم السارق عبر الانترنت بإجراء تحويلات مصرفية من حسابات العملاء في أحد المصارف إلى حسابه الخاص باستخدام تلك البرمجيات و هذا يعد استيلاء على الحيازة حتى و إن كان المال محل الجريمة هنا لا يزال في حيازة (ملك) المصرف. و هو الشأن الذي قام به الشاب الروسي Vladimir LIVEN حيث أجرى تحويلات مصرفية من حساب الغير إلى حسابه الخاص عن طريق الاستناد إلى تلك البرمجيات[5].

---

[1]- لمزيد من التفاصيل ينظر د/ السيد عتيق، المرجع السابق، ص 98 و ما بعدها.

[2]- لمزيد من التفاصيل حول موقف الفقه العربي من هذه المسألة ينظر د/ أيمن عبد الله فكري، المرجع السابق، ص 548 وما بعدها.

[3]- د/محمد صبحي نجم، المرجع السابق، ص 121.

[4] -TGI Paris،1Ch.Correctionelle، Jugement du 16 Décembre 1996, http:// www.legalis.net

[5]- د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئةعن استخدام الإنترنت) مرجع سابق، ص 403.

هذا من جهة و من جهة أخرى، فمن الممكن أيضا أن تتخذ جريمة الاختلاس طابع النسخ المستمر أي العدوان على المال المعلوماتي بالمشاركة في الحيازة. وصورة ذلك بأن يقوم السارق بوضع ملفات برمجته على أساس قيامها باستنساخ ما يحتويه الحاسوب من ملفات و القيام بإرسالها إلى حاسوبه الخاص به. ومن أشكال هذه الملفات استخدامها في شكل فيروسات و دود عبر لانترنت كما هو الشأن في دودة w32badtrams.13312@mm و التي تعمل على سرقة البيانات المخزنة في الحواسيب التي تصيبها ثم ترسلها إلى مرسل الدودة[1].

ثالثا: الركن المعنوي.

من المتعارف عليه بأن جريمة السرقة هي جريمة عمدية يشترط فيها قصد جنائي عام و خاص في الوقت ذاته. فأما بالنسبة للقصد الجنائي العام في السرقة عبر الانترنت فيكون بعلم الجاني بأن الإعتداء على النظام المعلوماتي يكون اما بفعل الدخول غير المشروع،و الذي يكون بانتهاك النظام المعلوماتي الخاص والمبرمج بسرقة كلمة المرور و اختراق نظامه الأمني (كجدار النار). أو بالبقاء غير المشروع في النظام المعلوماتي و ارتكاب الجرائم الأخرى.و لا يكفي في هذا الشأن العلم بعدم مشروعية الدخول إلى النظام المعلوماتي بل يجب أيضا أن تتجه إرادته إلى الاستيلاء على المعلومة.

أما القصد الجنائي الخاص فيتمثل في نية تملك المعلومة محل الإعتداء؛ و ذلك باتجاه إرادة الجاني إلى الاستيلاء على المعلومات و تبديل حيازتها و ممارسة سلطات المالك عليها[2] ، و يجب أن يكون هناك تزامن بين هذه النية و فعل الاختلاس. أما إذا كان القصد الجنائي الخاص لاحقا لفعل الاختلاس فإن الجريمة لا تقع[3].

و تجدر الاشارة الى أنه يمكن استخلاص القصد الجنائي الخاص بمجرد الدخول غير المشروع في النظام و تجاوز أنظمة الحماية المنذرة بعدم أحقية الدخول إلى النظام الآلي. و من الناحية الواقعية، فإن وجود نظام حماية يسمح للشخص المتواجد في النظام بمعرفة الحد الذي ينبغي تجاوزه. و قد أقر الفقه الفرنسي أن انتهاك نظام الأمن الذي يعتبر في حد ذاته دليلا ضمنيا على وجود القصد و سوء نية مرتكب الفعل، حيث يعد هذا الانتهاك في حد ذاته وسيلة إثبات. حيث أن الدخول غير المشروع يلزم كعنصر مقترن للجريمة لفكرة الإعتداء على النظام[4].

---

[1]– لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، نفس المرجع، نفس الموضع.

[2]– محمد أمين أحمد الشوابكة، المرجع السابق، ص160 وما بعدها.

[3]– د/ محمد صبحي نجم، المرجع السابق، ص 126.

[4]– نقلا عن أحمد حسام طه تمام، المرجع السابق، ص 514

المطلب الثاني

موقف التشريعات المقارنة من جريمة السرقة عبر الانترنت

وسنوضح في هذا المطلب موقف التشريعات المقارنة من خلال تبيان موقف التشريعات الغربية ثم التشريعات العربية. و ذلك في الفرعين التاليين:

الفرع الأول: موقف التشريعات الغربية من جريمة السرقة عبر الانترنت.

الفرع الثاني: موقف التشريعات العربية من جريمة السرقة عبر الانترنت.

الفرع الأول: موقف التشريعات الغربية من جريمة السرقة عبر الانترنت.

و سنبين في هذا الفرع موقف التشريعات الغربية من خلال تقسيمها إلى قسمين، الأول نفصل فيه موقف التشريع الفرنسي. أما الثاني فنخصصه لموقف التشريع الأنجلوسكسوني، و ذلك كالآتي:

أولا: موقف التشريع الفرنسي من جريمة السرقة عبر الانترنت.

على عكس الموقف الصريح الذي أخذه كلا من الفقه و القضاء الفرنسي من جريمة السرقة المعلوماتية،فإن المشرع الفرنسي صمت و لم يتناولها صراحة بل اكتفى بالنص على جريمة السرقة التقليدية دون المعلوماتية و منها الواقعة عبر الانترنت في المادة 311-1 من قانون العقوبات الفرنسي الجديد على أنها:"اختلاس الشيء المملوك للغير"[1] و في المادة 311-2 اذ اعتبر أن اختلاس الطاقة اضرارا بالغير يعد سرقة.[2]

ثانيا: موقف التشريعات الأنجلوسكسونية من جريمة السرقة عبر الانترنت.

وتم تبيان هذا الموقف من خلال تقسيمه إلى موقف التشريع الأمريكي أولا ثم التشريع الانجليزي ثانيا. وذلك كمايلي:

1/ موقف التشريع الأمريكي:

حذت بعض الولايات الفدرالية حذو القانون الفدرالي الخاص بحماية أنظمة الكمبيوتر لعام 1977 (CSPA) في تجريمها لجريمة السرقة المعلوماتية، حيث أصدرت عدة قوانين تعرف المال بأنه "كل شيء يمثل قيمة"؛ و يشمل هذا التعريف الأموال المعلوماتية و البيانات و المعلومات و الكيانات المنطقية بوصفها تمثل قيمة. فأي اختلاس للبيانات أو المعلومات أو الكيانات المنطقية بمعالجتها آليا هي مجرمة تحت القانون الفدرالي.فالمعلومة وفقا لهذا القانون يمكن أن تقوم على أنها خدمة أي تدخل في الذمة المالية للشخص و تعتبر اعتداء على الذمة المالية للشخص.

---

[1] -311-1 : « Le vol est la soustraction frauduleuse de la chose d'autrui ».

[2] -311-2 : « La soustraction frauduleuse d'énergie au préjudice d'autrui est assimilée au vol ».

و قد طبقت المحكمة الفدرالية العليا القوانين الخاصة بالسرقة على سرقة المعلومات في قضية ضد "جيرار Gérard" حيث تمسكت بأن بيع المعلومة التي تم الحصول عليها من عدة بيانات خاصة بالحاسب الآلي، كافية لتأييد إدانة موظف حكومي بالسرقة، إعمالا لنص المادة 64/18 من قانون العقوبات الأمريكي[1].

و قد أضفى المشرع حماية للمعلومات السرية و التجارية من السرقة بإصداره قانون الولايات المتحدة للتجسس الاقتصادي Economic espionage في عام 1996، حيث يحظر اختراق النظام المعلوماتي للبحث عن أية معلومة مملوكة للغير.و في عام 1997 صدر قانون السرقة الاليكترونية Thief Electronic Actالذي يحمي البرامج و المعلومات من السرقة، و يحظر تداول البرامج غير الشرعية. [2]

2/ موقف التشريع الانجليزي:

تناول المشرع الانجليزي جريمة السرقة في القانون الصادر سنة 1916 و القانون الصادر في 1986، حيث تنص المادة 15 من التشريع الأول على أنه:" يعد مرتكبا لجريمة السرقة كل من حصل بطريق الغش و بصفة غير مشروعة على مال يخص الغير بغرض حرمانه منه بصفة دائمة".[3] و تنص المادة الأولى من التشريع الثاني على:"يعد مرتكبا لجريمة السرقة كل من حصل بطريق الغش و بصفة غير مشروعة على منفعة الغير." [4]

يتضح من خلال هذه النصوص أن القانون الانجليزي لم يعترف بجريمة السرقة للمال المعلوماتي عبر الانترنت، ذلك لأنه لا يعتبر المعلومات من قبيل المال الذي تصلح حيازته للانتقال من صاحبه إلى السارق. و هذا ما أقره الفقه و القضاء الانجليزي في الكثير من القضايا[5].

الفرع الثاني: موقف التشريعات العربية من جريمة السرقة عبر الانترنت.

و على غرار الفرع السابق سيقسم هذا الفرع إلى موقفين خصص أولهما لابراز موقف التشريعات العربية بصفة عامة من جريمة السرقة عبر الانترنت، في حين خصص ثانيهما لتوضيح موقف التشريع الجزائري من هذه الجريمة المستحدثة. و ذلك كمايلي:

---

[1]– ينظر د/ السيد عتيق، المرجع السابق، ص106.

[2]– محمد أمين أحمد الشوابكة، المرجع السابق، ص163.

[3] –la loi de 1916 sur le vol considère comme voleur celui qui، en connaissance de cause، et avec l'intention de commettre une fraude، prend et emporte « takes and carries away» une « chose mobilière » appartenant à autrui.

[4] – l'article 1de loi de 1968 sur le vol dispose que la personne est coupable d'infraction de vol si elle prend par un moyen malhonnête les biens d'autrui dans l'intention d'appropriation.

[5]– أقر القضاء الانجليزي هذا المبدأ في قضية Boardman v. Phipps. و الذي قضى فيها أن المعلومات لا تمثل أبدا أموالا و هي متاحة لأي شخص يستطيع قراءتها أو سماعها. و كذا في قضية Oxford v. Moss. لمزيد من التفاصيل ينظر حول تفاصيل هذه القضايا :

M.CHAWKY،(Le vol d'informations) op.cit، p15

أولا: موقف التشريعات العربية بصفة عامة من جريمة السرقة عبر الانترنت.

لم تأخذ التشريعات العربية على عكس نظيرتها الغربية موقفا صريحا يجرم مثل هذا النوع المستحدث من الجرائم الواقعة على الأموال عبر الانترنت، بل اكتفت بتطبيق قوانينها العقابية التقليدية الخاصة بجريمة السرقة. و منها قانون العقوبات المصري و الذي تناول هذه الجريمة في المواد 311 إلى 327 من الباب الثامن المعنون بالسرقة و الاغتصاب. حيث عرف جريمة السرقة عن طريق تعريف السارق في المادة 311 منه على أنه:"كل من اختلس منقولا مملوكا لغيره فهو سارق." وعلى نفس النهج سار كلا من المشرع التونسي و البحريني في المواد 258 عقوبات تونسي، 1/331 عقوبات بحريني.

أما بالنسبة للمشرع الليبي فنص على جريمة السرقة في المادة 444 من قانون العقوبات الليبي بأنه: "كل من اختلس منقولا مملوكا للغير يعاقب بالحبس.ويعد من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية و جميع أنواع الطاقة ذات القيمة الاقتصادية."

ثانيا: موقف التشريع الجزائري من جريمة السرقة عبر الانترنت.

لقد ساير المشرع الجزائري موقف التشريعات العربية في التزام الصمت حيال هذه الجريمة الواقعة عبر الانترنت على معلومات و معطيات ذات طبيعة معنوية، اذ تناول جريمة السرقة في القسم الأول من الفصل الثالث المعنون بالسرقات و ابتزاز الأموال في المواد من 350 إلى 369 من قانون العقوبات الجزائري. فعرف السرقة في المادة 350 من قانون العقوبات[1] بأنها إختلاس شيء مملوك للغير

ومن خلال استقراء نص هذه المادة يمكننا القول بأن كلمة الشيء التي ذكرها المشرع في الفقرة الأولى منها جاءت مطلقة دون قيد و دون أن يصف هذا الشيء بالمادي أو المعنوي. و إن عدم تحديد طبيعة الشيء محل السرقة هو الذي دفع المشرع لامكانية تجريم اختلاس المياه و الغاز و الكهرباء على الرغم من أنها ليست لها طبيعة مادية، و علة ذلك تكمن في أن الاستيلاء على الطاقة يطبق على كل قوة أو طاقة يمكن اخضاعها لسيطرة الانسان و يكون بوسعه أن يوجهها على النحو الذي يحقق منفعته، و عليه يمكن اعتبار الأفكار و المعلومات طاقة ذهنية يصدق عليها المعنى و تقبل التملك و الحيازة من خلال الدعامة التي توجد عليها، و لا تنقل إلا بموافقة حائزها عن طريق كلمة السر. إذن فهي على هذا النحو – و على الرغم من طبيعتها غير المادية – تصلح لأن تكون محلا لجريمة السرقة، و لا يمثل هذا خروجا عن مبدأ الشرعية فنصوص السرقة تقبل هذا التفسير لأنها:

- لا تحدد صفة الشيء محل الجريمة، مادي أو معنوي.
- هي أشياء معنوية يصدق عليها وصف المال (قيمة اقتصادية).[2]

---

[1]– تنص المادة 350 من قانون العقوبات الجزائري على: "كل من اختلس شيئا غير مملوك له يعد سارقا و يعاقب بالحبس من سنة(1) إلى خمس (5) سنوات و بغرامة من 100.000 دج إلى 500.000 دج .

و تطبق نفس العقوبة على اختلاس المياه و الغاز و الكهرباء....".

[2]– آمال قارة، المرجع السابق، ص 29.

و على هذا يمكن للقاضي الجزائي الجزائري أن يطبق نص المادة 350 على كل شخص يختلس معلومات أو أفكار أو بطاقات ائتمان أو أموال أو يشرع في ذلك عبر الانترنت.

ومن القضايا الواقعية التي يمكن الإشارة إليها في هدا الصدد ما يلي:

– جريمة سرقة الأموال عبر الانترنت و التي جرت أحداثها في إمارة دبي بدولة الإمارات العربية المتحدة في أواخر عام 2001،حيث قام الهاكر بالعديد من السرقات المالية لحسابات عملاء في 13 بنكا محليا وعالميا.و ذلك باختلاس الأموال من الحسابات الشخصية و تحويلها إلى حسابات وهمية قام هو بتخليقها.وكان ذلك من خلال إحدى مقاهي الانترنت العامة المنتشرة في دبي. و قد بلغت قيمة الاختلاسات حولي 300 ألف درهم من البنوك المحلية بالإمارات فقط.

– و في حادثة أخرى، حكمت فيها محكمة دبي بمعاقبة متهم بالحبس ستة أشهر مع ابعاده عن البلاد ومصادرة المضبوطات لأنه تمكن من وضع برنامج تجسس في محل الانترنت الذي تتردد عليه المجني عليها بدبي مما مكنه من التوصل الى الرقم السري لحسابها في المصرف على شبكة الانترنت، و من ثم قام بواسطة الحاسب الآلي الموجود بغرفته من الدخول في المصرف تمهيدا للقيام بتحويل المبلغ المختلس الى حساب آخر ثم تمكن من سحبه بواسطة بطاقة الصراف الآلي.[1]

– و في جريمة أخرى جرت وقائعها لأحد فروع سيتي بنك بالولايات المتحدة الأمريكية عام 1994 و كان بطلها مواطن روسي الجنسية الذي استطاع الاستيلاء على ما يقارب 400 ألف دولار أمريكي[2].

– و في قضية أخرى تمكن طالبان جامعيان في مصر من سحب نصف مليون جنيه مصري من رصيد عميل في أحد البنوك الحكومية عن طريق شبكة الانترنت، و قد استخدما المبلغ فيما بعد في مشاهدة أفلام متنوعة على الشبكة طوال سبعة أشهر بعد أن استطاعا معرفة الرقم السري لحساب العميل على شبكة الانترنت[3].

– و في قضية أخرى قامت عصابة من القراصنة بالسطو على شبكات الكمبيوتر ضد عدد من الشركات المتعددة الجنسيات، حيث سرق القراصنة الملفات السرية للشركات، و طلبوا فدية من مؤسسة فيزا للبطاقات الائتمانية، قيمتها عشرة ملايين جنيه إسترليني، و إلا أفشوا أسرار هذه الشركات و عرضوا أنشطتها للخطر.

---

[1]–و في قضية أخرى و تتمثل في اختراق موقع شركة المقاولات و تتلخص وقائعها في أنه تقدمت شركة مقاولات كبرى بالظفر بمناقصة ضخمة، و لما علمت الشركة المنافسة لها بادرت إلى الاتصال بأحد قراصنة الحاسوب حيث قام مقابل مبلغ من المال باختراق موقع الشركة الإليكتروني و التسلل إلى ملفاتها و نجح في أن يضع يده على الملف الخاص بالمناقصة وتمكنت الشركة المنافسة من الاطلاع على عطاء منافستها و الإسراع بإعطاء عطاء بقليل من عطاء الأولى لتفوز بالمشروع الذي بلغت قيمته 20 مليون دولار. و في قضية أخرى و تتمثل تجسس على أسئلة الامتحانات إذ تمكن قرصان من الولايات المتحدة الأمريكية من تجاوز القيود الأمنية على قواعد المعلومات و الاطلاع على أسئلة الامتحانات لإحدى الجامعات دون تنبه الجامعة لذلك إلا بعد الإعلان عن النتائج. ينظر د/عمر فاروق فحل، المرجع السابق، ص314 و317.

[2]– بحث الجريمة عبرالإنترنت ، http:// www.meus.bbc.com.

[3]– وليد الزيدي، المرجع السابق، ص61

و أكد أحد المحققين أن العصابة تؤجر أيضا خدماتها لمن يريد و قال متحدث باسم "فيزا" أن مسئولي المؤسسة أبلغوا الشرطة البريطانية (سكوتلاندريارد) و مكتب التحقيقات الفيدرالي الأمريكي بالحادث بعدما تلقوا رسائل بالبريد الإليكتروني تطلب الفدية، و حذر المتحدث من أنه في حالة تنفيذ العصابة تهديداتها بالسطو على كل شبكة كمبيوتر المؤسسة و عدم الاقتصار على الكلمات السرية، فإن خسارة المؤسسة ستتجاوز عشرات الملايين من الجنيهات الإسترلينية[1].

و في قضية أخرى استطاع الهكرة الروس ارتكاب 500 محاولة سطو على مصرف روسيا المركزي خلال المدة من 1994 الى 1996، و قاموا بتحويل مبلغ 250 مليون روبل الى حساباتهم الخاصة.و لقد كان فلادمير لوفين أحد أقوى هؤلاء الهكرة حيث اخترق شبكة حاسوب مصرفCITIBANK في مدينة Parsipenny بولاية New Jersey الأمريكية، و استولى على عدة ملايين باستخدام حاسوب محمول في أحد شوارع روسيا. كما قام باجراء تحويلات من حسابات عملائها الى حسابات خاصة به قام بفتحها في مصارف في هولندا و ألمانيا و الولايات المتحدة و اسرائيل، والتي وصلت قيمتها الى 12 مليون دولار أمريكي.[2]

المبحث الثاني:

جريمة النصب عبر الانترنت

النصب هو استخدام طرق ووسائل احتيالية يمكن بطريقها تحقيق منفعة مادية غير مشروعة للجاني. أو هو الاستيلاء على مال منقول مملوك للغير بوسيلة احتيالية تحمل المجني عليه على التسليم في ماله.و يقع النشاط الإجرامي في جريمة النصب على أساس تغيير الحقيقة، وجوهره هو تشويه الحقيقة في ذهن المجني عليه مما يدفعه إلى قبول تصرف ضارب و هو يقترب بذلك من جريمة التزوير باعتبارهما نوعين من أنواع الغش.

و تختلف جريمة النصب عن جريمة السرقة في في أن تسليم المال فيها يتم برضاء مشوب بغلط نتيجة الاحتيال الذي مارسه الجاني ضد المجني عليه. أما في السرقة فيتم الاستيلاء على المال دون رضا المالك أو الحائز للمال.و يتسم النشاط الإجرامي في جريمة النصب بأنه نشاط مركب و ليس بسيطا، فهو يتكون من فعلين الاحتيال و الاستيلاء. وأول الفعلين يتقدم على الثاني من حيث الزمن و يفضي إليه بحكم المنطق. و لقد تأثرت هذه الجريمة كغيرها من الجرائم الواقعة على الأموال بظهور الانترنت، و التي فتحت الأبواب أمام مجرمي المعلوماتية لارتكاب ما شاء لهم من جرائم لا سيما النصب و الاحتيال. و هذا ما أدى الى ظهور نوع مستحدث من الجرائم الأشد و الأكثر تداولا عبر الانترنت تسمى بجريمة النصب عبر الانترنت.فماذا نعني بهذه الجريمة ؟ و ما هي أشكالها؟ و ما هو التكييف القانوني لها؟.

---

[1]– د/ عبد الفتاح مراد، المرجع السابق، 394.

[2]– لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص 409.

أسئلة سيتم الاجابة عليها في المطلبين التاليين كما يلي:

المطلب الأول: تعريف النصب عبر الانترنت و أشكاله.

المطلب الثاني: موقف التشريعات المقارنة من جريمة النصب عبر الانترنت.

المطلب الأول:

تعريف النصب عبر الانترنت و أشكاله.

و سنعرض في هذا المطلب إلى تعريف جريمة النصب عبر الانترنت ثم نعدد أشكالها المختلفة التي يمكن أن تقع عبر تلك الشبكة التي أصبحت سلاحا ذو حدين. و ذلك في الفرعين التاليين:

الفرع الأول: تعريف جريمة النصب عبر الانترنت.

الفرع الثاني: أشكال جريمة النصب عبر الانترنت

الفرع الأول: تعريف جريمة النصب عبر الانترنت

تعتبر جريمة النصب عبر الانترنت Internet Fraud أو ما يصطلح عليها جريمة الاحتيال المعلوماتي[1] أشد أو أكثر جرائم الأموال المتداولة و المنتشرة عبر الشبكة، إذ أنها تحتل المرتبة الأولى في العالم الإفتراضي على عكس ما هو متعارف عليه في العالم المادي أين تتسيد جريمة السرقة جرائم الأموال.

و يكمن سر ذلك في طبيعة ذلك العالم لكونه بذاته يعد أسلوبا فنيا، و الحركة فيه ذات قيمة فنية لدرجة تجعل مسألة إيقاع الشخص في الغلط المكون لجريمة النصب عبر الانترنت أكثر سهولة و أعمق و أوسع تأثير في نفسية ذلك الأخير، عما هو الحال عليه في العالم المادي و الذي تبرز فيه شخصية الجاني

---

[1]– الاحتيال هو كل تظاهر أو إيحاء يكون صالحا لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة الاحتيال هو "من جازت عليه حيلة الجاني فانخدع لها و سلمه ماله. أو أنه عبارة عن ادعاءات كاذبة يدعمها الجاني بمظاهر خارجية من شأنها إيهام المجني عليه بأمر من الأمور التي نص عليها القانون على سبيل الحصر. أو هو الإيحاء أو التظاهر الذي يكون صالحا لإيقاع المجني عليه بطريقة تؤدي إلى الاقتناع المباشر بالمظهر العادي الخارجي و الانخداع به و التسليم في ماله".

و تجدر الإشارة إلى أن الاحتيال لا يقع فقط على الشخص الطبيعي، بل أن الشخص المعنوي يكون ضحية فيه أي مجنيا عليه، فالشركات و المؤسسات العامة و الخاصة هي من الأشخاص الإعتبارية في نظر القانون.

و يختلف الاحتيال عن النشاط الإجرامي في جريمة خيانة الأمانة في أن التسليم في الأول ينقل الحيازة الكاملة للمال. أما في الثاني فهو ينقل الحيازة الناقصة.

و لقد حدد المشرع طرق النصب بنص قانوني و هي استعمال الطرق الاحتيالية

– اتخاذ اسم كاذب أو صفة.

– التصرف في مال ثابت أو منقول ليس ملكا له و لا له حق التصرف فيه. ينظر على التوالي: محمد أمين الشوابكة، المرجع السابق، ص 135. د/ أحمد شوقي عمر أبو خطوة: جرائم الإعتداء على الأموال، القسم الخاص، دار النهضة العربية، القاهرة 1994، ص199–200. د/ محمد سامي الشوا، المرجع السابق، ص 123.

ماديا، بحيث يمكن التعرف عليه بالاتصال الذي يحدثه هذا الأخير مع الضحية، على عكس ما إذا ارتكبت عبر الانترنت و الذي يتم في الغالب دون الحاجة إلى بروز الجاني، و إنما من خلال صفحة أو موقع أو برمجية سمعية بصرية يعدها الجاني لإيهام و إيقاع الناس في مصيدة الاحتيال بهدف سلبهم و الاستيلاء على أموالهم. إذ أنه من السهولة بمكان مثل الانترنت اتخاذ اسم كاذب (مزور)أو صفة مزورة أو إحداث الأمل بفوز أي شيء أو وقوع أي حادث أو إعداد برمجية وهمية أو إعداد سندات مالية خيالية و يرجع ذلك لسببين:

– الابهار الذي تركت أثره تلك الشبكة في نفوس مستخدميها لاسيما في التعاملات الاقتصادية مما أدى إلى طغيان و استحواذ فكرة تحسين ظروفهم الاقتصادية، سواء باقتراح الأفكار و استقبالها.

– لأن الشبكة و بمجموع ما تتصف به من خصائص لاسيما انعدام الرقابة عليها (باعتبارها ليست ملك لأي أحد) و كذا كونها مفتوحة للجميع...، باتت تشكل المسرح الملائم و الحيوي لمثل تلك الاختراقات [1].

و يمكن تعريف جريمة النصب عبر الانترنت بأنها: "أي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي."[2] كما يعرف الاحتيال المعلوماتي[3] بأنه:"كل سلوك احتيالي يرتبط بعملية التحسيب الإليكتروني بهدف كسب فائدة أو مصلحة مالية".[4] أو بأنه " قيام الجاني بالتلاعب في البيانات المخزنة بالحاسب أو برامجه وفقا لأساليب متعددة، و بهدف تحويل كل أو بعض أرصدة الغير أوفوائدها لحسابه."[5] أو بأنه "التلاعب بالبرامج أو البيانات بالتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها و التسليم بها."[6]

وتجدر الإشارة هنا إلى أن النصب عبر الانترنت Internet Fraud يعتبر نوعا من الاحتيال المعلوماتيFraude informatique[7]. إذ أصبحت تلك الشبكة أو عدت من الوسائل التي تساعد على

---

[1] – د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص 412

[2] – د/ عمر محمد أبو بكر بن يونس، نفس المرجع ، ص 411

[3]– وصف الاحتيال بالمعلوماتي يشير إلى صورة مستحدثة تقوم على اساءة استخدام الحاسبات و التلاعب في نظم المعالجة الالكترونية للبيانات للحصول بغير حق على أموال أو أصول أو خدمات. وهي صورة تميزه عن مثيله التقليدي لاسيما فيما يتعلق بالتعقيد الناتج عن استخدام المفاتيح و الشفرات و الدلائل الالكترونية في ارتكابه، و نظرة الكثيرين اليه باعتباره نوعا من التحدي الذي يثير الرغبة في اتيانه، و كذلك امكانية اقترافه عن بعد، و عدم تركه آثار مادية تدل على وقوعه. بالاضافة إلى فداحة خسائر و سهولة طمسه و اخفائه.ينظر د/هشام فريد رستم،(قانون العقوبات و مخاطر تقنية المعلومات) مرجع سابق، ص 45 و ما بعدها. أحمد فضل سليمان، المرجع السابق، ص 197.

[4] – محمد أمين أحمد الشوابكة، المرجع السابق، ص 180

[5] – د/ محمد سامي الشوا، المرجع السابق، ص 121

[6] – د/ هدى حامد قشوقش، المرجع السابق، ص 132

[7]– يقع الاحتيال المعلوماتي على البينات المخزنة في الحاسب أو برامجه دون ضرورة ارتباط ذلك الأخير بالانترنت

Dr/ Mohamed BUZABAR, Op cit, p 23

إتمام جرائم الأموال عامة و النصب بصفة خاصة. فعن طريقها يستخدم الجاني بسهولة جميع طرق الاحتيال الممكنة لإيهام المجني عليه و إيقاعه في مصيدة الاحتيال.

الفرع الثاني: أشكال النصب عبر الانترنت.

تأخذ جريمة النصب عبر الانترنت الأشكال التالية:

أولا: إرسال رسائل غير مرغوب فيها عن طريق البريد الإليكتروني: إن من بين أبرز الوسائل المستخدمة في جريمة النصب و الاحتيال عبر شبكة الانترنت هو وسيلة البريد الاليكتروني التي يستخدمها المجرمون في ارتكابها، و ذلك عن طريق إرسال رسائل غير مرغوب فيها إلى المشتركين في هذه الخدمة و بكم هائل، و قد أطلقت على هذه الرسائل تسمية القائمة القذرة و التي تضم رسائل تتحدث عن الموضوعات التالية:

– فرص تجارية تمني المشتركين بزيادة دخولهم من خلال استثمار صغير لا يتطلب الكثير من الوقت والمال.

– إغراءات بجني المال من خلال إرسال الرغبات بالبريد الإليكتروني عن نطاق واسع.

– توجيه خطابات تزعم أن بالإمكان كسب مبالغ طائلة في مدة قصيرة.

– الترويج لبرامج العمل في المنزل، و يعرض هذا النوع من الرسائل فرصة لتحقيق المال دون أن يخرج الفرد من منزله.

– عرض طائفة من الخدمات مجانا.

– الترويج لجوائز الإجازات.

– تقديم قروض بشروط ميسرة.[1]

ثانيا: إعداد مزادات خادعة عبر الانترنت: لكون أن هذه الأخيرة توفر مجرد صور للمواد و السلع محل المزادات دون الماديات. كما هو الشأن في العالم المادي حيث يتم الاطلاع على تلك السلع و اقتناؤها فور رسو المزاد. ففي الولايات المتحدة الأمريكية تعرض 41% من مستخدمي الانترنت للاحتيال و السرقة من خلال مشاركتهم في المزادات التي تتم عبر الانترنت، و التي غالبا ما كانت تدور حول سلع ذات أسعار مرتفعة[2].

و تجدر الإشارة إلى أن هذه الجريمة تعد الأكثر انتشارا في العالم الإفتراضي لأن حجم المخاطر المالية للمشاركين فيها مرتفع جدا[3].

---

[1] – وليد االزيدي، المرجع السابق، ص 66–67

[2] – و هذا ما أثبتته إحصائيات لجنة التجارة الفيدرالية و لجنة مراقبة النصب عبر الإنترنت، ينظر وليد الزيدي، نفس المرجع، ص 68.

[3] – د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت)مرجع سابق، ص 616.

ثالثا: الاستيلاء على متعلقات الهوية: و صورته الاستيلاء على أرقام تخص الفرد و تبرز هويته؛ كأرقام بطاقات الائتمان و أرقام الضمان الاجتماعي.

و تجدر الإشارة إلى أن النصب ببطاقات الائتمان يعتبر أشهر صور النصب و الاحتيال عبر الانترنت، ويكثر هذا عند ارتياد المجني عليه مواقع غير مشروعة كالمواقع الإباحية، و التي يستخدم فيها ذلك الأخير بطاقة ائتمانه أو يقوم بملء استمارة ما تتضمن ما يدل على هويته. و هكذا يكون طعما جاهزا لمصيدة المحتالين سواء أكان هو محل تلك الجريمة أو كان الغير، و ذلك باستخدام هوية المجني عليه بطريقة غير مشروعة. و مثال ذلك الاحتيال الذي تم على مصرف Delaware Bank من خلال الحصول على أسماء و أرقام التأمين الاجتماعي لمجموعة كبيرة من العسكرين و استخدامها في ذلك الشأن.و في مثال ثان يتمثل في قيام الهاكر ابراهيم عبد الله بالاحتيال على مائتين من أثرياء أمريكا، و جنيه من جراء ذلك عشرات الملايين من الدولارات[1].

رابعا: الاحتيال في نقل الأموال إليكترونيا: حيث يقوم الجاني بالحصول على بعض الوسائل المرتبطة بحماية العلامات مثل كلمات المرور و تفاصيل الحسابات، و التي يمكن من خلالها الوصول إلى قواعد البيانات الخاصة بشركات الأعمال و المؤسسات المالية. و في بعض الظروف قد ينقل المحتالون الأموال إليكترونيا من خلال إرسال أوامر بالبريد الإليكتروني[2].

خامسا: الاحتيال في الأسهم والاستثمار: ومن أمثلة هذا النوع من النصب قيام المحتالين باستخدام الانترنت لنشر معلومات خاطئة لجذب المستثمرين أو التلاعب بالأسهم، كما هو الشأن في استخدام أسلوب Pump- and- dump؛ و الذي يعني الإعلان المزيف عن الوضع المالي لمؤسسة اقتصادية، كشركة ما لرفع قيمة أسهمها والتأثير في سوق المال (The pump) ثم القيام ببيعها بمجرد بروز أثر إيجابي على هذه الخديعة (The dump)، ومن ذلك قضية Park الذي استخدم هذا الأسلوب. مما جعل لجنة الأمن والصرافة الأمريكية تحرك الدعوى الجنائية ضده، مطالبة بمعاقبته بمقتضى القسم Tit.15sec.88b–5 والقسم Tit.15sec.80b–5[3].

سادسا: الاحتيال في التحصيل الالكتروني: وذلك عن طريق التزييف أو التلاعب الكترونيا أو حل شفرة التوقيع الرقمي. والسبب في ذلك هو انعدام الرقابة الداخلية عندما يتم تنفيذ أنظمة التحصيل الالكتروني الجديدة[4].

---

[1] – تجدر الإشارة إلى أن إبراهيم عبد الله هو مبرمج حاسوب أمريكي من أصل عربي و يعد من كبار الهكرة في مجال العدوان على الأموال باستيلائه على هويات أعضاء الإنترنت و اختراقه للبنوك العالمية. د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص 417.

[2] – د/ عصام عبد الفتاح مطر، المرجع السابق، ص 348.

[3] – د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص 417.

[4] – د/ عصام عبد الفتاح مطر، المرجع السابق، ص 349.

سابعا: الاحتيال بأسلوب انتحال الشخصية: تعتبر جرائم انتحال شخصية الآخرين من الجرائم القديمة.إلا أن التنامي المتزايد لشبكة الانترنت أعطى المجرمين قدرة أكبر على جمع المعلومات الشخصية المطلوبة عن الضحية و الاستفادة منها في ارتكاب جرائمهم، فتنتشر في شبكة الانترنت الكثير من الاعلانات المشبوهة و التي تداعب عادة غريزة الطمع الإنساني. و هذا ما يؤدي إلى سهولة الوقوع في مصيدة المحتالين. و يعد الاحتيال بأسلوب انتحال الشخصية من أعلى معدلات الإجرام عبر الانترنت، حيث يقوم المحتال و عن عمد بالاستيلاء على معلومات اختيارية من الضحية أو بالحصول على معلومات اقتصادية أو حيازة أو تحويل أو استخدام وثائق اثبات شخصية تخص الآخرين، فمثلا يوضع على إحدى مواقع الانترنت إعلان عن جائزة ضخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية. و الذي يتطلب بطبيعة الحال الافصاح عن بعض المعلومات الشخصية كالأسهم و العنوان و الأهم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية[1].

و نظرا لخطورة هذا النوع من الاحتيال لاعتباره تعدي صارخ على حقوق الغير و انتهاكا لملكياتهم التي صانها المشرع لهم، فقد جرمه ذلك الأخير وخصوصا لما استخدمت فيه الانترنت. و نص عليه كجريمة في قانون ولاية ماساشوستس الأمريكية Mass.Ann.Laws.CH266sec.33e و تشريع ولاية أوكلاهوما الأمريكية Okla.Stat.Tit.21sec1533.1.

و جريمة النصب عبر الانترنت هي جريمة عمدية كما هو الحال في العالم المادي. تقوم على القصد الجنائي، سواء العام و المتمثل في العلم بالاحتيال، أي أن يعلم الجاني بأنه يرتكب فعل تدليس شأنه إيقاع المجني عليه في غلط يدفعه إلى تسليم أمواله باستعماله طرق احتيالية.أو الخاص، أي توافر نية سلب ثروة الغير كلها أو جزءها أو بالأحرى نية التملك. [2]

المطلب الثاني:

موقف التشريعات المقارنة من جريمة النصب عبر الانترنت

لقد انقسمت التشريعات العقابية المقارنة في تناولها للنصب في صورته المستحدثة، فمنها من يرى إمكانية تطبيق النصوص التقليدية الخاصة بجريمة النصب على تلك الواقعة عبر الانترنت.

و منها من خصت لها قوانين تجرمها و تعاقب عليها. و سنحدد موقف هذه التشريعات بتقسيمها إلى قسمين. الأول نوضح فيه موقف التشريعات الغربية من هذه الجريمة المستحدثة، أما الثاني فخصصناه لتبيان موقف التشريعات العربية منها. و ذلك في الفرعين التاليين:

الفرع الأول: موقف التشريعات الغربية من جريمة النصب عبر الانترنت.

الفرع الثاني: موقف التشريعات العربية من جريمة النصب عبر الانترنت.

---

[1] – محمد عبد الله المنشاوي، البحث السابق،http:// www.minshawi.com.

[2] – د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص 417

الفرع الأول: موقف التشريعات الغربية من جريمة النصب عبر الانترنت.

و سنخصص هذا الفرع لإظهار موقف كلا من التشريع اللاتيني أولا، ثم التشريع الأنجلوسكسوني ثانيا من جريمة النصب عبر الانترنت. و ذلك كمايلي:

أولا: موقف التشريع اللاتيني من جريمة النصب عبر الانترنت.

و سنحدد في هذه النقطة موقف المشرع الأوروبي من خلال إتفاقية بودابست ثم موقف المشرع الفرنسي من جريمة النصب عبر الانترنت.

1/ موقف المشرع الأوروبي من جريمة النصب عبر الانترنت:

كان للمشرع الأوروبي موقفا صريحا من خلال إتفاقية بودابست في تجريم و عقاب مثل هذه الجريمة المستحدثة الواقعة على الذمة المالية للأشخاص. اذ استخدم مصطلح الغش المعلوماتي Fraude informatique للتعبير عن الاحتيال المعلوماتي في نص المادة 8 و الناصة على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية و أية إجراءات أخرى يرى أنها ضرورية لتجريم، تبعا لقانونه الداخلي، عمدا و دون حق التسبب في إحداث ضرر مالي للغير عن طريق:

أ- الادخال، الاتلاف، المحو أو الطمس لبيانات الحاسب.

ب- كل شكل للاعتداء على وظيفة الحاسب بنية إجرامية مشابهة،من أجل الحصول دون حق على منفعة اقتصادية له أو للغير".[1]

2/ موقف المشرع الفرنسي من جريمة النصب عبر الانترنت:

أما المشرع الفرنسي فنص على جريمة النصب التقليدية دون المستحدثة في المادة 1/313 من قانون العقوبات الفرنسي الجديد و اعتبره بأنه "واقعة خداع شخص طبيعي أو معنوي سواء باستعمال اسم كاذب أو صفة كاذبة أو التعسف في صفة غير صحيحة أو باستعمال حيلة تدليسية من شأنها حمل الغير على تسلم أموال أو قيمة أو مال ما أو تقديم خدمة أو الموافقة على عمل ينتج عنه التزام أو تحرر من التزام"[2].

---

[1]- ينظر لمزيد من التفاصيل د/ هلالي عبد اللاه أحمد،(الجوانب الموضوعية و الإجرائية...) مرجع سابق، ص 112 و ما بعدها.

[2]- Art 313-1 « L'escroquerie c'est-à-dire le fait soit par l'usage d'un faux nom ou d'une fausse qualité soit par l'abus d'une qualité vraie ،soit par l'emploi de manœuvres frauduleuses ،de tromper une personne physique ou morale et de la déterminer ainsi ،à son préjudice ou au préjudice d'un tiers ،à remettre des fonds ،des valeurs ou un bien quelconque ،à fournir un service ou à consentir un acte opérant obligation ou décharge »

وعلى عكس قانون العقوبات الفرنسي الجديد تناول قانون العقوبات الألماني في القسم 263 و قانون العقوبات النرويجي في المادة 270 عقوبات خاصة بجريمة النصب الواقع على نظم المعلومات بقصد الحصول على ربح غير مشروع و ذلك عن طريق استعمال بيانات غير صحيحة أو غير كاملة أو عن طريق التلاعب في المعلومات أو برامج الحاسب الآلي. اذ ساوت هاتين المادتين بين الاحتيال الواقع على الشخص الطبيعي و ذلك الواقع على نظم المعلومات، ينظر د/ أيمن عبد الله فكري، المرجع السابق، ص 579.

ثانيا: موقف التشريعات الأنجلوسكسونية من جريمة النصب عبر الانترنت.

و نقصد هنا بالتشريعات الأنجلوسكسونية القانون الأمريكي و القانون الإنجليزي على وجه الخصوص، والذي سنوضح موقفهما حيال هذه الجريمة كمايلي:

1/ موقف التشريع الأمريكي:

على عكس المشرع الفرنسي خص المشرع الأمريكي[1] جريمة الاحتيال المعلوماتي بنص خاص يجرمه و يعاقب عليه و ذلك من خلال قانون الاحتيال و إساءة إستخدام "الكمبيوتر CFAA في القسم 1030 من الباب 18 و التي تعتبر أن الولوج المصطنع إلى أنظمة الحاسب الآلي يتم متى كان هذا الدخول غير شرعي إلى:

أ- كمبيوترات الحكومة.

ب- أي كمبيوتر يحتوي على أسرار أو معلومات حكومية محددة، كالبيانات المتعلقة بالدفاع القومي أو العلاقات الأجنبية.

ج- أي كمبيوتر للحصول على تسجيلات مالية، و تكوين الأموال.

د- أي كمبيوتر يستخدم للحصول على معلومات بطاقات الائتمان.

و- أي كمبيوتر يستخدم كوسيلة في استطلاع المستهلكين للحصول على معلومات إئتمانية.

ي- الاهتمامات الفيدرالية في الحاسب الآلي.[2]

---

[1]-لقد تقدمت وزارة العدل الأمريكية في شهر أوت 1984 بمشروع قانون يستهدف مباشرة حالة الغش المعلوماتي، و الذي يعاقب كل من رتب أو صمم خطة ما أو حيلة بغرض ارتكاب غش أو الاستيلاء على مبلغ من النقود أو مال لا يخصه، و ولج أو حاول الولوج في حاسب آلي بغرض تنفيذ هذه الخطة أو الحيلة أو لارتكاب أو محاولة ارتكاب مثل هذا النصب أو هذه السرقة أو الاختلاس. و يشمل مصطلح المال وفقا لهذا المشروع كل الوسائل المالية و المعلومات التي تحتوي على بيانات معالجة و المكونات الالكترونية و الكيانات المنطقية و برامج الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للانسان، و كل قيمة أخرى ذات طابع مادي أو معنوي. د/ سامي الشوا، المرجع السابق، ص 130.

2 -18 usc 1030 : « (a) Whoever

(1) having knowingly accessed a computer without authorization or exceeding authorized access، and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations، or any restricted data، as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954، with reason to believe that such information so obtained could be used to the injury of the United States، or to the advantage of any foreign nation willfully communicates، delivers، transmits، or causes to be communicated، delivered، or transmitted، or attempts to communicate، deliver، transmit or cause to be communicated، delivered، or transmitted the same to any person not entitled to receive it، or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access، and thereby obtains

(A) information contained in a financial record of a financial institution، or of a card issuer as defined in section 1602 (n) of title 15، or contained in a file of a consumer reporting agency on a consumer، as such terms are defined in the Fair Credit Reporting Act;

و لقد أضفت القوانين الفيدرالية مفهوما واسعا للمال ليشمل كل شيء ينطوي على قيمة، بما فيها الأموال المعنوية و البيانات المعالجة و منها قانون عقوبات ولاية كاليفورنيافي القسم 502[1]. و قانون إيداهو في القسم 2202- 18[2] و قانون عقوبات مونتانا في القسم 31- 6- 45[3].

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally، without authorization to access any nonpublic computer of a department or agency of the United States، accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or، in the case of a computer not exclusively for such use، is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;....."

[1] -CALIFORNIA PENAL CODE 502(c)"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.(2) Knowingly accesses and without permission takes, copies, ormakes use of any data from a computer, computer system, or computernetwork, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.(3) Knowingly and without permission uses or causes to be used computer services.(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damage or causes damage to a computer, computer system, or computer network". mandreptla.org

[2] -18-2202. Computer crime : "(1) Any person who knowingly accesses, attempts to access or uses, or attempts to use any computer, computer system, computer network, or any part thereof for the purpose of: devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; or committing theft; commits computer crime."
www.legislature.idaho.gov

[3] -45-6-311. Unlawful use of a computer: "(1) A person commits the offense of unlawful use of a computer if the person knowingly or purposely:

(a) obtains the use of any computer, computer system, or computer network without consent of the owner; (b) alters or destroys or causes another to alter or destroy a computer program or computer software without consent of the owner; or (c) obtains the use of or alters or destroys a computer, computer system, computer network, or any part thereof as part of a deception for the purpose of obtaining money, property, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other

2/ موقف التشريع الانجليزي:

تناول المشرع الانجليزي من خلال قانون السرقة Theft act الصادر في سنة 1978 جريمة النصب في المادة 16 و الناصة على عقاب كل من حصل على نحو غير مشروع و بأي وسيلة خداع سواء لنفسه أو للغير على منفعة مالية[1]. و من خلال التفسير الواسع لهذا النص فإن جريمة النصب يمكن أن تشمل التلاعب في البيانات من أجل الحصول على منفعة مادية. و قد أدان القضاء الإنجليزي المتهم Thomson.VR بجرم الاحتيال، وذلك في واقعة تتلخص في قيام ذلك الأخير بتدبير برنامج أمر الكمبيوتر بموجبه بتحويل كميات من حسابات بعض الزبائن المحفوظة على الكمبيوتر والتي لم يجر عليها أي صفقات مالية لمدة من الزمن ثم قام بالكتابة إلى مدير البنك آمرا إياه بتحويل الأرصدة من حساباته في الكويت. و قد تم ذلك بالفعل و عندما كشف أمره تمت ادانته بتهمة الحصول على أموال بطريق الخداع. وقد جرم المشرع الانجليزي مسألة غش الكمبيوتر بعد تصديقه لقانون إساءة استخدام الكمبيوتر عام 1990.[2]

الفرع الثاني: موقف التشريعات العربية من جريمة النصب عبر الانترنت.

و سنحدد في هذا الفرع موقف التشريعات العربية بصفة عامة حيال هذه الجريمة المستحدثة، و الذي ينقسم إلى قسمين الأول يخص التشريعات العربية التي صمتت حيال مواجهة هذا الاجرام المستحدث. أما الثاني فيتعلق بالتشريعات التي عالجت هذا الاجرام بنصوص خاصة. لنتطرق بعد ذلك إلى موقف التشريع الجزائري من هذه الجريمة.

أولا: موقف التشريعات العربية من جريمة النصب عبر الانترنت بصفة عامة.

لقد صمتت معظم التشريعات العربية عن مواجهة جريمة النصب عبر الانترنت، حيث اكتفت بتطبيق النصوص التقليدية عليها و منها **التشريع المصري** و الذي تناول جريمة النصب في المادة 336 من قانون العقوبات[3] و التي يتطلب لتوافرها أن يكون ثمة احتيال وقع من المتهم على المجني عليه بقصد خداعه و

---

person.(2) A person convicted of the offense of unlawful use of a computer involving property not exceeding $1,500 in value shall be fined not to exceed $1,500 or be imprisoned in the county jail for a term not to exceed 6 months, or both. A person convicted of the offense of unlawful use of a computer involving property exceeding $1,500 in value shall be fined not more than 2 1/2 times the value of the property used, altered, destroyed, or obtained or be imprisoned in the state prison for a term not to exceed 10 years, or both".policy.mofcom.gov.cn

[1]- نقلا عن محمد سامي الشوا، المرجع السابق، ص126.

[2]- و في كندا فإن المادتين 387 -388 من قانون العقوبات يسهل تطبيقهما على النصب المعلوماتي، حيث أدان القضاء الكندي في قضية Regina.V. marin Ressource Analysed Limited المتهمين في جريمة الشروع في النصب لاستخدامهم رقم حساب شخص آخر للولوج في النظام المعلوماتي، و كذلك الأمر بالنسبة لأستراليا التي تبنت تفسيرات واسعا لمفهوم الاحتيال مستوحى من القانون الانجليزي . نقلا عن محمد أمين أحمد الشوابكة، المرجع السابق، ص187-188.

[3]- تنص المادة 336 من قانون العقوبات المصري على أنه:"يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات مخالصة أو أي متاع منقول و كان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها باستعمال طرق

الاستيلاء على ماله فيقع المجني عليه ضحية هذا الاحتيال الذي يتوافر باستعمال طرق احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة أو التصرف في مال الغير ممن لا يملك التصرف فيه.

و على عكس التشريعات العربية السابقة، قامت بعض الدول العربية بسن قوانين خاصة إلى جانب قوانينها العقابية تجرم و تعاقب على جريمة النصب على عبر الانترنت. و منها **التشريع الإماراتي الاتحادي** رقم 02 لسنة 2006 بشأن مكافحة جرائم المعلوماتية في المادة 10 .[1] كما تناولها **المشرع السعودي** من خلال نظام مكافحة جرائم المعلوماتية السعودي في مادته 1/4.[2]

و كذلك عالجها **قانون جرائم المعلوماتية السوداني** في فصله الثالث المعنون بالجرائم الواقعة على الأموال و البيانات و الاتصالات في المادة 11 منه.[3] أما **التشريع الأردني** فقد جرمها في قانون المعاملات الإليكترونية رقم 85 لعام 2001، حيث جرمت نصوص مواده أي استخدام للمعلوماتية بغرض القيام بأفعال احتيالية و ذلك في المواد 35-38 من ذات القانون[4].

احتيالية من شأنها ايهام الناس بوجود مشروع كاذب أو واقعة مزورة أو احداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطريق الإحتيال أو ايهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور و إما بالتصرف في مال ثابت أو منقول ليس مالكا و لا له حق التصرف فيه.

و إما باتخاذ اسم كاذب او صفة غير صحيحة و العقوبة تصل إلى ثلاث سنوات. أما من شرع في نصب و لم يتمه فيعاقب بالحبس مدة لا تتجاوز سنة. و يجوز وضع الجاني في حالة العود تحت ملاحظة البوليس مدة سنة على الأقل و سنتين على الأكثر."

[1]- تنص المادة 10 من التشريع الإماراتي الاتحادي رقم 02 لسنة 2006 بشأن مكافحة جرائم المعلوماتية على:"كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند و ذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه يعاقب بالحبس مدة لا تقل عن سنة و بالغرامة التي لا تقل عن ثلاثين ألف درهم أو بإحدى هاتين العقوبتين".

[2]- تنص المادة 1/4 من نظام مكافحة جرائم المعلوماتية السعودي على:"يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا كان الجرائم المعلوماتية الآتية:
الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، و ذلك عن طريق الاحتيال، أو اتخاذ اسم كان أو انتحال صفة غير صحيحة".

[3]- تنص المادة 11 من قانون جرائم المعلوماتية السوداني على :" كل من يتوصل عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة ، بغرض الاستيلاء لنفسه أو لغيره على مال أو سند أو توقيع للسند ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً ".

[4]- تنص المادة 35 من قانون المعاملات الاليكترونية الأردني على "يعاقب كل من يقوم بإنشاء أو نشر أو تقديم شهادة توثيق لغرض احتيالي أو لأي غرض غير مشروع بالحبس مدة لا تقل عن ثلاثة أشهر و لا تزيد عن سنتين أو بغرامة لا تقل عن 300 دينار ولا تزيد على 1000 دينار أو بكلتا هاتين العقوبتين"

ثانيا: موقف التشريع الجزائري من جريمة النصب عبر الانترنت.

تناول المشرع الجزائري على غرار غيره من المشرعين العرب جريمة النصب في المواد 372 إلى 375 من قانون العقوبات في القسم الثاني من الفصل الثالث تحت عنوان النصب و اصدار شيك بدون رصيد[1]. حيث عرفت المادة 372[2] من ذات القانون جريمة النصب .

ومن خلال استقرائنا لهذه المادة نجد أن المشرع الجزائري لم يعترف صراحة بامكانية وقوع جريمة النصب عبر الانترنت، و لكننا نلاحظ أنه لا يوجد ما يحول دون وقوع المعلومات و البيانات الوهمية المنشورة عبر الانترنت تحت طائلة هذا النص سواء باعتبارها أموالا أو منقولات. و بهذا أصبح من المتصور أن يقوم أحد الأشخاص بالتلاعب في هذه البيانات و يحولها كلها أو بعضها لصالحه لسلب كل ثروة الغير أو بعضهاإما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو باحداث الأمل في الفوز بأي شيء أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها.

و تعاقب المادة 36 من ذات القانون "كل من يقدم إلى جهة تمارس أعمال توثيق المستندات معلومات غير صحيحة بقصد إصدار شهادة توثيق أو وقف سريانها أو إلغائها بالحبس مدة لا تقل عن شهر و لا تزيد على ستة أشهر أو بغرامة لا تقل عن 1000 دينار و لا تزيد عن 5000 دينار أو بكلتا هاتين العقوبتين"

و كذلك فإن المادة 37 من ذات القانون تضفي الحماية للأشخاص الطبيعية أو الإعتبارية من أية ممارسات احتيالية من أي جهة تمارس أعمال توثيق المستندات سواء بتقديم معلومات غير صحيحة في طلب التسجيل أو من إفشاء أسرار عملائها أو بمخالفة الأنظمة و التعليمات التي تصدر استنادا إلى هذا القانون و يعاقب على هذه الأفعال بغرامة لا تقل عن 50.000دينار.و تنص المادة 38 من ذات القانون على أن "يعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الاليكترونية بالحبس مدة لا تقل عن ثلاثة أشهر و لا تزيد على سنة أو بغرامة لا تقل عن 3000 دينار و لا تزيد على 10.000 دينار أو بكلتا العقوبتين، و يعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون".

[1]– لمزيد من التفاصيل حول جريمة النصب في القانون الجزائري ينظر د/ محمد صبحي نجم، المرجع السابق، من ص141 إلى ص154.

[2]– تنص المادة 372 من قانون العقوبات الجزائري على: "كل من توصل إلى إستلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو ابراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك و كان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو باحداث الأمل في الفوز بأي شيء أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر و بغرامة من 500 إلى 20000 دج.

و اذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد اصدار أسهم أو سندات أو أذونات

أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات و الغرامة إلى 200000 دج".

و في جميع الحالات يجوز أن يحكم علاوة على ذلك على الجاني بالحرمان من جميع الحقوق الواردة في المادة 14 أو من بعضها و بالمنع من الاقامة و ذلك لمدة سنة على الأقل و خمس سنوات على الأكثر."

و تجدر الاشارة هنا بأن المشرع الجزائري نص على النصب المعلوماتي الواقع على المعطيات من خلال المادة 394 مكرر 1 و مكرر 2 من قانون العقوبات[1]. و ذلك من خلال جريمة الإعتداءات العمدية على المعطيات.[2]

ومن أشهر القضايا الواقعية حول النصب عبر الانترنت ما يلي:

– وقوع العديد من الجزائريين و منهم من يملك شهادات جامعية و شهادات عليا في كمين جهات مجهولة تغريهم بوعود كاذبة و الحصول على هدايا معتبرة و مناصب عمل. ومن بين ضحايا هذا النوع الإجرامي المستحدث محامي؛ إذ تلقى رسالة اليكترونية عبر بريده الاليكتروني من طرف شركة البرمجيات الشهيرة "ميكروسوفت" تعلمه بفوزه في إحدى المسابقات التي شارك فيها من خلال عملية القرعة التي أجرتها الشركة، و قد تمثلت الجائزة التي تحصل عليها بمليون جنيه إسترليني. و لكن حصوله على تلك الجائزة واقف على اتخاذ عدة إجراءات من بينها إعطائه رقم حسابه البنكي و إرساله مبلغ 2000 يورو، غير أن فطنة وذكاء المحامي الذي روى لأصدقائه ما حدث له جعله يتفطن أن المسابقة وهمية خاصة و أن من بين أصدقائه من تعرض لهذه الخدعة و ما هي إلا مسابقة وهمية.

– و في مثال آخر تعرض الطالب محمد من ولاية الشلف نتيجة للبطالة التي يعيشها للاحتيال عبر الانترنت حينما لجأ إليها للبحث عبر مواقعها عن عمل له لعله يحقق فرصة أحلامه. و في كل موقع كان يعرض فيه مسابقة أو وظيفة كان يشارك فيها. و في أحد الأيام تلقى رسالة بقبول ملفه و بالتالي حصوله على وظيفة بإحدى المؤسسات بإفريقيا. و لكن يشترط عليه إرسال مجموعة من الوثائق عبر البريد الاليكتروني للشركة التي كان يحمل رقم هاتفها و شعارها، الأمر الذي طمأنه، و لاستكمال الإجراءات عليه إرسال مبلغ 500 دولار لحساب الشركة. غير أنه لم يستطيع تحويل المال من الجزائر فسافر إلى تونس، ولم يستطيع كذلك فعل ذلك فاتصل بشقيقه المغترب بفرنسا الذي قام بتحويل المبلغ. و بعد فترة تلقى رسالة اليكترونية أخرى تطالبهالشركة فيها بإرسال مبلغ 300 دولار. مما جعل الشكوك تراوده و قرر بذلك عدم

---

[1]– تنص المادة 394 مكرر 1 على :" يعاقب بالحبس من ستة أشهر إلى ثلاث(3) سنوات و بغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها." أما المادة 394 مكرر2 فينص فيها على:" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج كل من أدخل عن طريق الغش بما يأتي:

1– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2– حيازة أو افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم."

[2]– لمزيد من التفاصيل حول هذه الجريمة ينظر ص280 من هذه الرسالة.

إرسال المبلغ و انتظار رد الشركة الوهمية. غير أنه لا حياة لمن تنادي. خاصة أنه أرسل جميع مدخراته من عمله كمستخلف في مؤسسة وطنية[1].

– و في قضية مغايرة تم اكتشاف موقع وهمي لأحد البنوك العاملة في الإمارات العربية المتحدة يشبه إلى حد بعيد الموقع الأصلي للبنك و تم إنشاؤه من قبل قراصنة للحصول على معلومات و رموزهم السرية مما حدا بالبنك إلى توجيه رسائل لعملائه يحذرهم من ذلك.

و كذلك تلقى بعض عملاء أحد البنوك رسائل تفيدهم بوجود عرض بقروض شخصية أو تمويل سيارات بفائدة منخفضة من هذا البنك و يطلب منهم إتباع إجراءات معينة و من ثم يتم توصيلهم إلى موقع غير صحيح بغرض الحصول على بيانات حساباتهم.[2]

– و في قضية أخرى تعرض الممثل المصري المشهور خالد النبوي للنصب عبر الانترنت[3].

– وفي قضية أخرى استخدمت شركتان يابانيتان الانترنت عن الاعلان لمسابقة لليانصيب(Loterie) والفائز فيه سيتحصل على مبلغ 9.000.000 فرنك. و هذا ما أدى إلى جلب مئات المهتمين بتلك المسابقة. غير أنه و في حقيقة الأمر كانت مجرد مسابقة وهمية. إذ بمجرد الإعلان عن أرقام الفائزين فيها اختفى الموقع الذي كان مخصصا لها[4].

المبحث الثالث:

جرائم الإعتداء على الملكية الفكرية عبر الإنترنت

يقصد بالملكية الفكرية [5] Propriété intellectuelle ":"حق المؤلف أو المبدع لمصنفات أدبية أو فنية، في أن تحظى أعمالها بحماية كاملة تحفظها من الاستغلال المادي أو الإساءة إليها"[6]. أو بأنها: "الحقوق الممنوحة للأفراد نظير ابتكارات عقولهم"[7]. أو هي: "شكل من المعارف أو التعابير الموضوعة بذكاء إنساني والمحفوظة بحماية كاملة و شرعية"[8]. أو هي: "حق المؤلف في حماية المبتكرات الفنية و المؤلفات التي

---

[1] – مليكة حراث: المسابقات و الوظائف الوهمية، أحدث جرائم الإنترنت، مقال منشور عبر الإنترنت على: http:// www.akhbarelyoum-dz.com.

[2]– د/ عمر فاروق فحل، المرجع السابق، ص 318

[3] – نشرة الأخبار الفنية لقناة روتانا سينما، ليوم 2010/12/10.

[4] – Dr/ Mohamed BUZABAR, opcit, p24

[5]– تسمى هذه الملكية كذلك الملكية الفنية و الأدبية Propriété artistique et littéraire ينظر إبراهيم نجار، أحمد زكي بدوي، يوسف شلالا: القاموس القانوني، فرنسي– عربي،الطبعة 8، مكتبة لبنان، 2002 ، ص232.

[6] – وليد الزيدي، المرجع السابق، ص52.

[7]– ينظر تعريف منظمة التجارة العالمية الموجود على موقعها: http: //www.wato.org

[8]– La propriété intellectuelle (DI) « est définit comme toute forme de connaissance ou d'expression crée en partie ou en tout par l'intelligence humaine et pouvant bénéficier d'une protection légale »

Association canadienne pour les études supérieures: Propriété intellectuelle ،un guide pour étudiants de cycle supérieur ،p3.http:// www.acpes.ca.

يضعها في الآداب و الفنون و العلوم أيا كان نوع هذه المصنفات أو طريقة التعبير عنها أو أهميتها أو الغرض من تصنيفها، و ذلك من خلال وقت معين و طبقا لبعض الإجراءات التي يحددها القانون"[1].

و يعتبر حق الملكية الفكرية أحد الحقوق المعنوية أو الأدبية التي تعرف بأنها: "قدرة يقرها و يحميها القانون لشخص على إنتاجه الفكري أو الذهني أو الأدبي أو الفني أيا كان نوعه، فيكون له الاحتفاظ بنسبة ذلك الإنتاج إليه دائما و يحتكر المنفعة المالية التي تنتج من استغلاله"[2]. أو هي:" الحقوق التي يتمتع بها الأشخاص للانتفاع الحصري من نتاج أفكارهم لفترة محددة من الزمن."[3]

هذا من جهة و من جهة أخرى، فهي تعتبر من طبيعة مزدوجة إذ تعطي من ناحية لصاحبها سلطة مباشرة على الشيء الواردة عليه هذه الملكية من استعمال لهذا الشيء و استغلاله و التصرف فيه و هو ما يطلق عليه بالشق المادي. و من ناحية أخرى، فإن المالك يرتبط شخصيا بما أبدعه، فيكون له حق الحماية من اعتداء الغير على ما أنتجه، كما يتمتع بأن ينسب إليه إنتاجه الذهني باعتبار ما أنتجه امتدادا لشخصيته. و هذا الشق يطلق عليه الجانب المعنوي.[4]

و ترد الملكية الفكرية بهذا على أشياء غير مادية لا تدرك إلا بالفكر، فهي تمثل في حقيقة الأمر إنتاج الذهني و تسمى الحقوق الواردة عليها بالحقوق الذهنية[5].

و تنقسم حقوق الملكية الفكرية إلى قسمين كبيرين هما:

- الملكية الأدبية و الفنية و الحقوق المرتبطة بها أو المجاورة لها.
- الملكية الصناعية و الحقوق المرتبطة بها أو المجاورة لها[6].

و سوف نقتصر دراستنا هذه في هذا المبحث على الملكية الأدبية و الفنية،و ذلك بالتفصيل في الجرائم التي تكون تلك الأخيرة محلا لها عبر الإنترنت.و ذلك من خلال تقسيمه إلى مطلبين كما يلي:

المطلب الأول: جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت

المطلب الثاني: موقف التشريعات المقارنة من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت.

---

[1]- القاموس القانوني، مرجع سابق، الموضع السابق.

[2]- د/ إسحاق إبراهيم منصور، المرجع السابق، ص297.

[3]- أحمد عبد الله مصطفى: حقوق الملكية الفكرية و التأليف في بيئة الإنترنت، دورية الكترونية محكمة Cyberarians Journal، العدد 21، ديسمبر 2009،http:// Cyberarian.org

[4]- يحي مفرح الزهراني: الإنترنت و حقوق المؤلف،http://artnews.com

[5]- د/ فاضلي إدريس:المدخل إلى الملكية الفكرية، الملكية الأدبية و الفنية و الصناعية، جامعة الجزائر، دار هومة، 2004/2003، ص23-35؛ فرحة زراوي

[6]- حق الملكية الصناعية و الحقوق المرتبطة بها هي الحقوق المعنوية التي تشمل استغلال براءات الاختراع و الرسوم والنماذج الصناعية. لمزيد من التفاصيل ينظر د/ فرحة زراوي صالح: الكامل في القانون التجاري الجزائري، الحقوق الفكرية، حقوق الملكية الصناعية و التجارية- حقوق الملكية الأدبية و الفنية، إبن خلدون للنشر و التوزيع، وهران، 2006، ص3 و ما بعدها. و كذا د/ محمد ياسر الفتوح: الملكية الفكرية و الجريمة المعلوماتية، http:// www.knal. Com

المطلب الأول:

جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت

يقصد بالملكية الأدبية و الفنية نظام الحماية المقرر بشأن المصنفات في حقل الآداب و الفنون و الذي بدأ وجوده التنظيمي بإبرام اتفاقية برن لحماية المصنفات الأدبية و الفنية في 1886/09/09،وبموجبه تحمي المواد المكتوبة كالكتب، و المواد الشفهية كالمحاضرات و المصنفات الفنية الأدائية كالأشرطة السينمائية والمواد الإذاعية السمعية و الفنون التطبيقية كالرسم و النحت و الصور التوضيحية و الخرائط والتصميمات و المخططات و الأعمال المجسمة المتعلقة بالجغرافيا و الخرائط السطحية للأرض، و برامج الحاسوب وقواعد البيانات و طبوغرافيا الدوائر المتكاملة وفق الاتجاه الغالب و بموجب اتفاقيات لاحقة على اتفاقية برن.

و يعرف هذا القسم من الملكية الفكرية أيضا بحقوق المؤلف، ويلحق به ما أصبح يطلق عليه الحقوق المجاورة لحق المؤلف و المتمثلة بحقوق المؤدين والعازفين والمنتجين في حقل الفونجرامات (التسجيلات الصوتية) و حقل الإذاعة[1]. ولقد تأثرت الملكية الفكرية بصفة عامة والملكية الأدبية والفنية بصفة خاصة بالتطور التكنولوجي الذي شهده عالمنا من خلال بروز ثورة معلوماتية قوامها استغلال التقنية العالية من حاسبات آلية و إنترنت، إذ أفرزت هذه التقنية العالية أنماطا و أنواعا جديدة من مصنفات الإبداع الفكري تسمى بمصنفات تقنية المعلومات.

هذا من جهة و من جهة أخرى، أصبحت الإنترنت وسيلة فعالة لنقل الآلاف من الملفات سواء تمثلت في صور أو موسيقى أو أفلام، أو كتب إذ أنه ووفقا لـ Albarto MANGUEL باتت هذه الشبكة تتيح فرصة سهولة تصفح الكتب و المؤلفات من أكبر مكتبات العالم كمكتبة الإسكندرية مثلا والإطلاع على الكتب الموجودة فيها وذلك باستخدام محركات البحث[2]. كما أن مكتبة Amazon.com تقدم عبرها إمكانية الإطلاع و الحصول على أكثر من 3 ملايين عنوان كتاب. ضف إلى ذلك فإن هذه الأخيرة تتيح القدرة على نسخ كتاب يحتوي عن 600 صفحة في أقل من دقيقة واحدة[3]. الأمر الذي سهل و يسر إمكانية سرقتها و تقليدها من أي فرد بدون بذل أدنى جهد و بدون موافقة من صاحبها. بل الأمر من ذلك أصبح بإمكان العامة اقتناء المصنفات عبر العالم الإفتراضي و ليس مجرد الاكتفاء بالإطلاع عليها فقط[4].

---

[1]– يونس عرب: نظام الملكية الفكرية لمصنفات المعلوماتية، http:// www.arablawinfo.com

[2]– Alberto Manguel écrit: "je me repose avec confiance sur les possibilités que m'offre l'informatique que de traquer dans des bibliothèques plus vaste que celle d'Alexandrie un renseignement inaccessible ،et mon ordinateur personnel peut "accéder" à toutes sortes de livre". Voir M.Gabriel DE BORGLIE :Le droit d'auteur et l'internet,rapport du groupe de travail et de l'academie des sciences morales et politiques, cahiet des sciences morales et politiques, PUF, 2001, p18.

[3]– Voir M. Gabriel DE BORGLIE , ibid, p20.

[4]– Sophie HEIN: La circulation des œuvres littéraires sur les info routes, http://www.lex-electronica.or

وبالتالي أصبح طريق الإعتداء على الملكية الفكرية عموما، والملكية الأدبية والفنية خاصة سهل للغاية عن طريق استخدام ما تتمتع به هذه التقنية من خصائص وأساليب فريدة من نوعها. و على هذا فإنه إلى جانب الوجه المشرق لهذه الشبكة هناك الوجه المظلم المليء بجرائم مستحدثة و منها: جريمة الإعتداء على الملكية الأدبية و الفنية. و لقد تم تخصيص هذا المطلب لإبراز ماهية جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت و ذلك بالتطرق إلى تعريفها وبتبيان أركانها، و ذلك في الفرعين التاليين:

الفرع الأول: تعريف جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت.

الفرع الثاني: أركان جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت.

الفرع الأول: تعريف جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت

ويمكن تعريفها بأنها كل فعل غير مشروع يقع على حق المؤلف[1] و المبدع لمصنفات أدبية أو فنية عن طريق استخدام تقنية الإنترنت مثل قيام شخص بإنزال نسخة من مقال أو كتاب عبر الإنترنت ثم قيامه بترويجها عبر مجموعة إخبارية أو قيام الغير بالترويج لفكرة ما كان غيره قد تناولها معه بالنقاش عبر الإنترنت و قيامه بنسبتها لنفسه. أو أن يتم تداول البريد الخاص عبر المجموعات الإخبارية. أو أن يتم النسخ باستخدام الماسح (Scaner) لمقالة أو جزء من مقالة أو عمل أو برمجية مملوكة للغير أو وثيقة أو فيلم سينمائي أو ملف موسيقي، ثم القيام بوضع أي من تلك النسخ عبر الإنترنت". و تعتبر جريمة التقليد عبر الإنترنت أو ما يطلق عليها جريمة العدوان على حقوق النسخ عبر الإنترنت من أخطر و أشهر هذه الجريمة.و يمكن تعريفها بأنها قيام الشخص بإنزال نسخة من مصنف رقمي(مقال، أو كتاب، أو قطعة موسيقية، أو رسم أو فيلم) عبر الانترنت دون موافقة مؤلفها. أو قيامه بترويج و استخدام بأي شكل كان، نسخ من الماديات التي تتكون منها الصفحة أو الموقع عبر الانترنت بقصد تحقيق أغراض تجارية خاصة دون موافقة مالكها.

الفرع الثاني: أركان جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت

إذا كانت الجريمة عموما لا تقوم ما لم تتوافر أركانها، لاسيما الركن المادي على وجه التحديد، فإنه في جريمة النسخ الإلكتروني ينبغي لقيام هذا الركن توافر عدة أمور من حيث ضرورة العدوان على الابتكار ولزوم العلنية و المدة. ذلك أن العدوان في جرائم انتهاك حقوق النسخ يتخذ أبعادا جديدة حقا، فتقنية المعلومات أفاءت علينا بسهولة كبيرة في التعامل مع المعلومات، و من ثم لم يعد هناك صعوبة حتى في ارتكاب عدوان عليها. بل إن كل ما يمكن أن يعد استيلاء أو حيازة في إطار هذه الجرائم يمكن أن يتم بمجرد النقر بأقل مجهود ممكن و من دون خسائر مالية. فيكون العدوان على هذه الشاكلة ذا سهولة

---

[1]– يقصد بحق المؤلف: كل حق استئثاري يمنحه القانون لمؤلف أي مصنف للكشف عنه كابتكار له أو استنساخه أو توزيعه أو نشره على الجمهور بأي طريقة أو وسيلة و كذلك الإذن للغير باستعماله على وجه محدد. د/ عفيفي كامل عفيفي، المرجع السابق، ص61.

خاصة، مكنت كل من يرغب في انتهاك حقوق المؤلف من القيام دون تكبد عناء الجريمة و بذل الجهد اللازم لارتكابها. و مثل هذا الأمر يسم ارتكاب جريمة الانتهاك العمدي لحقوق المؤلف عبر الإنترنت وعلى الأخص حقوق النسخ، بالخطورة الخاصة. إذ أن لها طبيعة إجرامية معقدة، كما هو الشأن في جرائم ذوي الباقات البيضاء التي ترتكب من قبل طائفة معينة من المجرمين[1]. و على هذا يتطلب لقيام جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت أركانا ثلاثة تتمثل في الركن الشرعي، و الركن المادي، و الركن المعنوي.

أولا: الركن الشرعي.

و الذي يمثل النص الجنائي المجرم لهذه الأفعال و سيتم التطرق اليه بالتفصيل في موقف التشريعات المقارنة من هذه الجريمة.[2]

ثانيا: الركن المادي.

1/ و يأخذ السلوك الإجرامي المكون للركن المادي في جرائم النسخ عبر الانترنت الصور الثلاثة الآتية:

أ- العرض عبر الانترنت لإعلان مبتكر ثم إعداده للبث بطرق تقليدية معتادة:

و يكون ذلك عن طريق قيام الجاني بالعدوان بتقليد المصنفات الرقمية المتواجدة عبر الانترنت و التي لها أصل مادي و بممارسة حقوق المالك دون موافقته، وذلك عن طريق ممارسته للاستنساخ المحظور و الذي يكون برفع النسخة المستنسخة على الإنترنت وإعادة وضعها مثلا على الصفحة الخاصة به عبر الإنترنت عن طريق استخدام تقنية قص/لصق (Copie/Coller)[3]. و يستوي في ذلك أن يكون النسخ قد وقع كاملا أو جزئيا[4].

و الإشكال المطروح هنا يدور حول شكل النسخ، فهل يشترط أن يكون النسخ هنا حرفيا كاملا Literal لقيام جريمة الإعتداء على حقوق النسخ؟ أم يستوي في ذلك النسخ الحرفي الجزئي Non-Literal أو ما يسمى بالمحاكاة imitation و الذي يعدل فيه المصنف المعتدى عليه (دون أن يطأ ذلك التعديل شكله وطريقة كتابته و منهجه) كأن يتم اقتباسه مثلا أو حذف أجزاء منه ليظهر بمظهر المصنف الجديد؟.

---

[1]- نقلا عن د/عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص528.

[2]- ينظر ص220 من هذه الرسالة.

[3]- M. Gobriel DE BORGLIE, op cit, p20.

[4]- و يكون النسخ كاملا في الحالة التي توضع فيها الصفحة بأكملها بشكل مصغر مثلا. أما الجزئي فيكون في حالة التي يكون فيها الموضوع على صفحة جزء من الصفحة المعتدى عليها أو تكون في مجرد الإشارة إلى ملكية المجني عليه الأدبية كعنوان مصنفه المادي أو اسمه الأدبي. ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص533.

والإجابة على ذلك تتمثل في أن مسألة التمييز بين الحرفية و غير الحرفية ترجع إلى قاضي الموضوع فهي تعتبر مسألة تقديرية. إذ أن ذلك الأخير هو الوحيد دون غيره يملك سلطة تحديد ما إذا كان النسخ حرفيا نقليا أو لم يكن كذلك. و بالتالي وقوع الجريمة من عدمها[1].

ب- الإنزال و التحصل:

و يتضمن إنزال مصنف أو جزء منه ثم تحميله في مواقع عبر الإنترنت بقصد الاستخدام التجاري- الخاص- سواء عبر الإنترنت أو في العالم المادي. و ليس هناك مفارقة في كيفية نشر النسخ غير المشروع عبر الانترنت، إذ يمكن أن يكون نشرا عبر الإنترنت ذاتها. و تتم عملية الإنزال و التحصيل (téléchargement) عن طريق إعادة تركيب النسخة بسهولة (facilité de mixage) بواسطة تقنية الربط المتن(hypertexte).[2] فقد قضي بإدانة شركة "software publishing" و رئيسها " Andrew kasanicky" لأنه نسخ أعدادا من مجلة "Play Boy" و أعاد نشرها على قرص مدمج CD-ROM وقام بتوزيعها. و لقد رفضت المحكمة إدعاء المدعى عليه بأن تلك الأعداد كانت في موقع عام[3].

ج- التحول إلى الرقمية:

يتخذ هذا الشكل تحويل مصنف ورقي أو أحد أركانه إلى الشكل الرقمي دون إذن المؤلف.

و تعد عملية التراسل أو تحويل الملف الذي يحوي مصنفا منشورا عبر الإنترنت من جرائم انتهاك حقوق النسخ. فالتراسل يعطي صلاحية التوزيع التي تدخل ضمن حقوق المؤلف على مصنفه. و من الأمثلة على خطورة التراسل مما يتعلق بالمصنفات الفنية و الموسيقية التي يتم تسجيلها فيتم تراسلها عبر الإنترنت في شكل ملفات يمكن بعد ذلك استنساخها و توزيعها بطرحها للتداول ماديا على أقراص ممغنطة أو مضغوطة CDS أو عبر الإنترنت في هيئة ملفات. و ينبغي أن يرتبط التحويل هنا بالإنزال أو النسخ المباشر، و من ثم بالتوزيع التجاري لما تم نسخه أو إنزاله. كما قد يأخذ شكل التحويل تحويل المصنف بالترجمة أي نقله إلى لغة أخرى (لغة كوبول إلى لغة فوتران) بدون ترخيص[4].

هذا من جهة و من جهة أخرى، يعد من جرائم العدوان على حقوق النسخ جلب أو استيراد نسخ من مؤلف معتدى عليه بالنسخ غير المشروع و ذلك عن طريق الحصول على نسخ من مواقع مسجلة في دول أخرى.

و لا يكفي لقيام الركن المادي في جريمة النسخ عبر الإنترنت توافر إحدى الصور الثلاث السابقة للسلوك الإجرامي، بل يجب إلى جانب ذلك توافر شرط آخر و مهم و هو عدم موافقة المؤلف أو مالك الصفحة أو الموقع على ذلك النسخ.

---

[1]- د/ عمر محمد أبو بكر بن يونس، المرجع السابق، الموضع السابق.

[2]- M. Garbriel DE BORGLIE, op cit,p19.

[3] - د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص534.

[4]- د/ أسامة عبد الله قايد: الحماية الجنائية لحق المؤلف، مركز البحوث و الدراسات القانونية بكلية الحقوق، جامعة القاهرة، دار النشر هاتيه، القاهرة، 1990، ص143 و ما بعدها.

2/ **عدم موافقة المؤلف أو مالك الصفحة أو الموقع على النسخ:** أي عدم وجود إذن من المؤلف أو خلفائه و يجب أن يكون هذا الإذن سابقا على أفعال الإعتداء أو على الأقل معاصرا لها.

و تجدر الإشارة هنا إلى أن رضا المؤلف لا يعد سببا من أسباب الإباحة، بل هو أحد عناصر الركن المادي الذي يتخلف بتخلفه[1].

هذا من جهة و من جهة أخرى، يجب أن يفرغ هذا الإذن في قالب مكتوب. و الكتابة هنا شرط وجود لا شرط إثبات فقط[2].

ضف إلى ذلك فإذا كان المصنف أو الموقع أو الصفحة المعتدى عليها مشتركة، كالمصنف المشترك[3] الموجود تحت عنوان "Afrique Virtuelle" و المتواجدة على موقع www.olets.org، أو المعارض الفنية المشتركة المنشورة عبر الإنترنت كما هو الشأن بالنسبة لـ "Art Entertainment network" لـ Walker Art center de Minnea polis المتواجد على موقع www.walkerart.org [4] فيجب أن يصدر الإذن كتابة من جميع الشركاء.و إذا كان جماعيا[5]، فالموافقة تصدر عن الشخص الطبيعي أو ممثل الشخص المعنوي[6]. و لعل أشهر قضية تضرب كمثال هنا هي قضية الشاعر الفرنسي Raymond Queneau في فرنسا، حيث تم نسخ مصنفه من على موقع عبر الإنترنت دون إذن منه، مما أدى بالمحكمة الابتدائية بالقضاء و تكييف الإعتداء بأنه جريمة العدوان على حقوق نسخ ذلك الأخير. و كذا الشأن بالنسبة لقضية الموسيقى الفنان الفرنسي Jaques Brel، و الذي تم نشر مصنفه الموسيقي بدون إذنه[7].

و في جميع الأحوال يجوز أن تصدر الموافقة من المؤلف أو المالك نفسه أو من أحد خلفائه كأن تكون صادرة من المتنازل له في حدود الحق المتنازل عنه[8].

---

[1]– لمزيد من التفاصيل ينظر د/ علي عبد القادر القهوجي،(الحماية الجنائية لبرامج الحاسب) مرجع سابق، ص27–28.

[2]– لمزيد من التفاصيل ينظر د/علي عبد القادر القهوجي، نفس المرجع، ص28 و د/ كامل عفيفي، المرجع السابق، ص64–65.

[3]– يقصد بالمصنف المشترك "œuvre collaboration": كل مصنف يشارك في إبداعه و/او إنجازه عدة مؤلفين مثل المصنف السمعي البصري، لمزيد من التفاصيل ينظر د/ فاضلي إدريس، المرجع السابق، ص92 و ما بعدها.

[4]– M. Gabriel DE BORGLIE, Op cit, p22.

[5]– يقصد بالمصنف الجماعي "œuvres collectives"كل مصنف يشارك في إبداعه عدة مؤلفين بمبادرة شخص طبيعي أو معنوي و إشرافه بنشره باسمه مثل المعاجم و الموسوعات و دوائر المعارف و الصحف و المجلات. ينظر د/ فاضلي إدريس، المرجع السابق، ص91.

[6]– آمال قارة، المرجع السابق، ص87.

[7]–Voir M. Gabriel DE BORGLIE,op cit, p34 .

[8]– د/ علي عبد القادر القهوجي،(الحماية الجنائية لبرامج الحاسب) مرجع سابق، ص28.

و الجدير بالذكر أن جريمة النسخ عبر الإنترنت أو التقليد يقع الإعتداء فيها على مصنف رقمي محمي. أي أن محل النشاط الإجرامي فيها هو المصنف الرقمي. و يقصد به "أي عمل إبداعي من بيئة تكنولوجيا المعلومات"[1].أو هو "كل مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات".[2]

و تشمل هذه المصنفات ثلاث أنواع: البرمجيات، قواعد البيانات و طبوغرافيا الدوائر المتكاملة.

البرمجيات: تعد برامج الحاسوب أول و أهم مصنفات المعلوماتية التي حظيت

باهتمام كبير من حيث وجوب الاعتراف و توفير الحماية القانونية لها، و البرمجيات كما أسلفنا هي من الكيان المعنوي لنظام الكمبيوتر. و هي تشمل:

برنامج المصدر: و هي مجموعة الأوامر التي يضعها المبرمج أو مؤلف البرنامج، و تكون مدركة له وغير مدركة للآلة، و يستخدم في تأليفها أو وضعها لغات البرمجة.

برنامج الآلة: و هو عكس مفهوم برنامج المصدر تماما، إذ تدركه الآلة و تستطيع التعامل معه و تشغيله.

الخوارزميات: و هي العناصر و الرموز الرياضية التي يتكون منها بناء البرنامج.

قواعد البيانات Database: و هي تجميع مميز للبيانات يتوافر فيه عنصر

الابتكار أو الترتيب أو التبويب عبر مجهود شخصي بأي لغة أو رمز و يكون مخزنا بواسطة الحاسوب ويمكن استرجاعه بواسطته أيضا.

و مناط حماية قواعد البيانات– بوجه عام – هو الابتكار كما عبرت عنه الاتفاقات الدولية في هذا الحقل، فالمادة 2/10 من اتفاقية تربس نصت على أنه: "تتمتع بالحماية البيانات المجمعة أو المواد الأخرى سواء كانت في شكل مقروء آلي أو في أي شكل آخر إذا كانت تشكل خلقا فكريا نتيجة انتقاء و ترتيب محتواها"

طوبوغرافيا الدوائر المتكاملة topographie of integrated circuit:

مثلت شبكة المواصلات فتحا جديدا و مميزا في حقل صناعة الالكترونيات و تطوير وظائف التقنية العالية، و مع تطور عمليات دمج الدارات الإلكترونية على الشريحة للقيام بمهام ووظائف إلكترونية أصبح التميز و الخلق الإبداعي يتمثل في آليات ترتيب و تنظيم الدوائر المدمجة على شريحة شبه الموصل، بمعنى أن طبوغرافيا الشريحة ينطوي على جهد إبداعي مكن من تطوير أداء نظم الحواسيب بشكل متسارع و هائل[3].

ثم ظهرت أنماط جديدة من المصنفات الرقمية تثير مسألة الحاجة إلى الحماية القانونية و هي: أسماء النطاقات أو الميادين أو المواقع على الشبكة، و عناوين البريد الإلكتروني، و قواعد البيانات على الخط التي تضمها مواقع الإنترنت و مادة أو محتوى موقع الإنترنت من نصوص و رسوم و أصوات و مؤثرات حركية تعرف باسم الوسائط المتعددة[4].

---

[1]– عبد الرحمن ألطاف: تحديات حماية الملكية الفكرية للمصنفات الرقمية، http:// Arabia.bitsnips.com

[2]– أمير فرج يوسف، المرجع السابق، ص54.

[3]– لمزيد من التفاصيل ينظر أمير فرج يوسف، المرجع السابق، ص60.

[4]– يقصد بأسماء نطاقات (عناوين) الإنترنت: Domaine names لكل موقع على شبكة الإنترنت عنوان دال عليه يمكن للمستخدم بمجرد وضعه في مكان العناوين بعد الدخول للشبكة أن يصل إلى موقع أيا كان،موقع أنظمة الكمبيوتر المستضيفة

و يعد العدوان على برمجيات الحاسوب عبر الإنترنت من أحد التطبيقات الحديثة للعدوان على حقوق النسخ ومن الجرائم الخطرة على اقتصاديات هذه البرمجيات. إذ يوجد عبر هذه الشبكة مواقع هكرة تحتوي ربط بمواقع قراصنة أكثر ظلاما، يمكن من خلالها جلب برمجيات غير مرخصة متواجدة في دول مثل الولايات المتحدة و تايوان و تشيكيا و سلوفاكيا و ترويجها بقصد تسهيل للغير ارتكاب عدوان على برمجيات مشروعة. و قد يأخذ الترويج هذا شكل الربط على الصفحات أو عن طريق إرسال رسالة بالبريد الالكتروني إلى عدد غير معروف تحتوي في موضوعها عناوين الصفحات التي عليها برمجيات مملوكة للغير يمكن ارتكاب قرصنة ضدها.

و لقد كانت أولى القضايا التي نظرها القضاء الأمريكي في محاكمة علنية، هي قضية Christian MORLEY (28 عاما) ، حيث أدين بتهمة التأمر لاستنساخ 5 آلاف من البرمجيات المخفاة في مواقع عبر الانترنت تابعة لإحدى الجامعات في كيبيك كندا[1].

و يشترط القانون في المصنف الرقمي شروطا لكي يكون محلا لجريمة العدوان على حقوق النسخ و هي:

– **الابتكار:** يعد الابتكار جوهر حماية حقوق النسخ، و هو تعبير عن الأصالة

و الإبداع. و يأخذ الابتكار طابع الجدة الذي يتناول أركان المصنف، مجتمعه أو منفردة. فهو الأثر الذي تحدثه فكرة المصنف في طور تنفيذها أو تحويلها إلى الواقع العملي (التداول).

و يعرف الابتكار بأنه: "جهد البحث و الانتقاء و التخليق" أو أنه "تركيبة من الروح الإختراعية والجدة"[2]. وقد قضت محكمة نانت التجارية الفرنسية في عام 1998 بأن الابتكار الذي يتعلق بقاعدة البيانات على الإنترنت يقتضي توافر جهد جاد في البحث و الاختيار و التحليل. أما قضاء محكمة النقض المصرية فإنه يتوسع في مفهوم الابتكار، فقد قضت محكمة النقض المصرية عام 1964 بأن: "فهرسة إحدى كتب الأحاديث النبوية يعد عملا ابتكاريا لأنه يكفي أن يكون عمل واضعه حديثا في نوعه و يتميز بطابع

له أو الموقع الجغرافي الفعلي لصاحب الموقع أو مزودات الموقع بالمواد المنشورة.و تتميز عناوين المواقع بسمات معينة، فالمواقع التجارية بوجه عام تنتهي بالاختصار (com) أما عناوين مواقع المنظمات فتنتهي بالاختصار (org) و المواقع الحكومية بالاختصار (gov) و الجامعات بالاختصار (edu) و بالنسبة للعناوين المرتبطة بدول معينة فتنتهي برمز أو اختصار الدولة مثالها بريطاني uk و مصر EG و الأردن JO و غيرها.

وتعمل شركات عالمية في حقل تسجيلها المواقع إضافة إلى خدمات استضافتها و تصميمها، أما المواقع التي تنتهي باسم الدولة فتختص بها جهة واحدة إضافة إلى هيئة معينة في الدولة. و قد أنشأ في أمريكا عام 1998 منظمة غير ربحية (إيكان) بهدف تنظيم مسائل أسماء النطاقات، مع أن الغرض الأكيد الواضح من تسجيلها التمهيد لخلق ما يسمى حكومة الإنترنت التي ستسيطر على مقدرات طريق المعلومات السريع و تتحكم بمصادر المعلومات في العالم. لمزيد من التفاصيل ينظر يونس عرب، (نظام الملكية الفكرية لمصنفات المعلوماتية) مرجع سابق، http:// www.arablawinfo.com

[1]– لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص553 وما بعدها، و حول وقائع قضية Christian Morley ص559.

[2]– د/ عمر محمد أبو بكر بن يونس، نفس المرجع ، ص535.

شخصي خاص، و أنه يعتبر من قبيل الابتكار في الترتيب أو التنسيق أو بأي مجهود آخر أن يتسم بالطابع الشخصي[1].

فبالتالي الابتكار يعني أن المصنف يتميز بطابع أصيل، أي يكون المؤلف قد أضاف عن عبقريته إلى فكرة سابقة ما يجعل لها طابعا جديدا يسمح بتمييز المصنف عما كان عليه من قبل سواء تعلق ذلك بجوهر الفكرة (مضمونها) أم بطريقة عرضها أم بالتعبير عنها (أيا كانت وسيلة التعبير) أم بترتيبها أو تبويبها (أي تسلسلها)[2]. واعتبار المصنف مبتكرا أو عدم اعتباره كذلك مسألة موضوعية يستقل بتقديرها قاضي الموضوع[3]. وعليه تعد مشمولة بحقوق النسخ، الأعمال التي تتضمن هدفا جماعيا و تحتوي تصنيفا و ترتيبا و فهرسة لغرض ما كالقواميس و الموسوعات، فهذه الأخيرة تعتبر مصنفات مبتكرة. فإذا أضيفت إلى برمجيات الحاسوب و تم كذلك تحميلها عبر الإنترنت فإنها تخضع للحماية و تسري عليها حماية القانون[4].

والابتكار قد يكون كليا أو جزئيا بحيث تخرج أحد العناصر المكونة للمصنف عن الابتكار كما هو الشأن في المؤلفات المدرسية أو الجامعية من حيث العنوان، فهي مشمولة في جزئية منها بالحماية في حين ليست مشمولة في جوانبها الأخرى. فمثلا إذا كان المؤلف تحت عنوان شرح قانون العقوبات و بالضبط كانت على شكل مطبوعة (polycopie) فإن ذلك الأخير ليس محلا للحماية لكونه ليس مبتكرا و إنما لحقته صفة الدارج، إلا أن ذلك لا يمنع من شمول عناصره الأخرى، كمادة المصنف و اسم المؤلف بالحماية القانونية الكاملة لكون المادة لحقها الابتكار هنا[5].

و عليه تعد الجدة من الأمور اللازمة التي يقوم عليها الابتكار. و الجدة المقصودة هنا هي التي تجعل المصنف، بمجرد ذكر عنوانه منسوبا إلى شخص بذاته كأن يكون المصنف هنا وضعه شخص ما و حقق بذلك خدمة ذات طابع عام. فمثلا مؤلف الفقيه العلامة السنهوري: الوسيط في شرح القانون المدني فإذا قام شخص باستخدام عنوان هذا الكتاب على صفحته عبر الإنترنت، يعد معتديا و متعديا على حقوق صاحب الكتاب[6]. ويشمل الابتكار عدة مظاهر تلحق بالمصنف الرقمي، مثل ابتكار تنظيم النصوص و الرسومات المنجزة على الحاسوب و الألحان الموسيقية و الصوتيات و برمجيات الحاسوب و أعمال تصنيف و تجميع و فهرسة البيانات. [7]

---

[1]– نقلا عن عبد الرحمن ألطاف، المرجع السابق، http:// Arabia.bitsnips.com .

[2]– د/ علي عبد القادر القهوجي، (الحماية الجنائية لبرامج الحاسب) مرجع سابق، ص11.

[3]– ينظر د/ عفيفي كامل عفيفي، المرجع السابق، ص61.

[4]– د/ أحمد كمال أحمد صبري: الحماية القانونية لحقوق المؤلف الرقمية على شبكة الإنترنت، المركز القومي للبحوث الاجتماعية و الجنائية، ص36.

[5]– د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة استخدام الإنترنت) مرجع سابق، ص537.

[6]– د/ عمر محمد أبو بكر بن يونس، نفس المرجع، ص536.

[7]– د/ عمر محمد أبو بكر بن يونس، نفس المرجع، ص537.

وعليه يشكل الابتكار شرطا أساسيا للقول بوجود مصنف مشمول بحقوق النسخ. أي يجب أن يتصف المصنف باستقلالية الابتكار و الإبداع.

- العلنية:

و هي تعني – وفق قانون النسخ- ضرورة بروز المصنف أو العمل على الهيئة أو الشكل التي يمكن للجمهور الإطلاع عليه. و لعل أبلغ صورة لهذا، هي عملية طرح المصنف للجمهور ببثه بأي شكل عبر الإنترنت[1] لما تتوافر فيها من إمكانيات قد لا تتوافر في العالم المادي. كإعداد جزء من موقع أو صفحة له عبر الإنترنت. و لا يشترط أن يرتبط البث هنا بلغة HTML، و إنما يقبل حتى و لو كان في صيغة برمجية إنزال مثل ملفات (PDF أو TIFF image من كوداك kodak)، و بما يعني إمكانية قيام الغير من الإطلاع عليه، و من شموله بحماية القانون كذلك. كما حدث في قضية دكتور Gubler في فرنسا إذ قام أحد أصحاب مقاهي الإنترنت بنسخ مذكرات دكتور Gubler و نشرها عبر الإنترنت بما شكل انتهاكا لحقوق النسخ فضلا عن الحق في الخصوصية[2]. و في قضية Jacques BREL و Michel SARDOU في فرنسا،إذ قام طالبين في المدرسة العليا ببث مصنف للمطريين على الموقع الخاص بهما على شبكة الإنترنت دون موافقة و إذن المؤلف، مما أتاح الفرصة لمستخدمي الإنترنت في نسخ المصنف الموسيقي. و قد أدانتهما المحكمة الابتدائية لباريس تأسيسا على أن البث الرقمي للمصنف عبر الإنترنت بدون إذن المؤلف يشكل جريمة تقليد المصنف[3]. و الشأن كذلك ينطبق إذا قام شخص بنسخ صور الفنانين أثناء سير رواية سينمائية أو مسلسل درامي من على موقع عبر الإنترنت و إعادة بثها على صفحته أو إنزالها في حاسوبه الخاص، إنما يعد انتهاكا لحقوق النسخ. و هو اتجاه يأخذ به المشرع الكندي و كذا القانون الأمريكي منذ عام 1993 في قضية Play boy Entertainment.v.frene معتبرا أن النشر على الإنترنت هو نشر علني[4].

هذا من جهة و من جهة أخرى يعد كذلك انتهاكا لحقوق النسخ في القانون المقارن حالة العدوان على الحق في الدعاية عبر الإنترنت. و هي الحالة التي يقوم فيها الغير بانتحال اسم و شهرة شخص مشهور عبر الإنترنت، بتضمينه لصفحة أو تداول البريد الإلكتروني أو الاتصال المباشر. ففي هذه الحالة فإن كلا من القانونين (الأمريكي و الكندي) السابقين يعتبرها عدوانا على الحق في الشهرة عبر الإنترنت مما يندرج في إطار قانون النسخ. و مرد ذلك لاعتبار الحق في الشهرة ذا مردود اقتصادي[5].

---

[1]– د/ علي عبد القادر القهوجي، (الحماية الجنائية لبرامج الحاسب) مرجع سابق، ص11.

[2]–M.Gabriel DE BROGLIE,op.cit, p101.

[3]– TGI Paris ،14/08/1996، La mise à disposition d'œuvres de Jacques BREL et de Michel Sardou sur un site internet reproduites sans autorisation ،constitue une contrefaçon ،Art Music/ ENST et ECP. Sté ،Edition Pouchenel/ F. X. Bergot Brel ,http:// juriscom.net .

[4]– د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص542.

[5]– ينظر د/عمر محمد أبو بكر بن يونس، نفس المرجع، نفس الموضع.

- الغرض التجاري أو المكسب المالي الخاص:

قد يتطلب القانون[1] شروطا اقتصادية لاكتمال الجريمة، أو تشديد العقاب على ارتكابها. و يقصد بهذا الشرط أن يكون الغرض من النسخ هو غرض اقتصادي، أو الحصول على مكاسب مالية خاصة، كأن يقوم الجاني ببيع و تداول النسخ المسروقة و المقلدة، أو أن يقصد الحصول على جوائز أو اجتياز اختبارات[2].

- المدة:

و نقصد بالمدة هنا أن القانون لا يتولى الحماية الأبدية للمصنفاتالمشمولة بحقوق النسخ، و إنما تكون الحماية قائمة خلال مدة معينة، تحسب من تاريخ صدور أول طبعة من النسخة. أي أن المصنفات المشمولة بحقوق النسخ تكون في ظل حماية قانونية طوال هذه المدة، فإذا انتهت تلك الأخيرة أصبح المصنف حرا طليقا من كل قيد، إلا بالنسبة لملكيته فتبقى حكرا على مالكه الذي يستطيع دون غيره إدعاءها. و كل ما هنالك أن عبء الإثبات يفرض على المالك إذا لم يقم بتسجيله[3].

و يختلف القانون في تحديد هذه المدة، إذ تحددها اتفاقية برن لحماية الحقوق الفنية و الأدبية بمدى حياة مؤلف المصنف مضافا إليها 25 عاما ما لم يكن هناك فرضية ارتباط المصنف بالطبعة الأولى. كما هو الشأن في التنازل المادي لصاحبه إلى الطابع أو الناشر. و كذا القانون الأمريكي الذي يحددها لمدى حياة المؤلف مضافا إليها 50 عام بعد وفاته (الباب 17 القسم (a) 302 من تقنين الولايات المتحدة تعديل 1994)[4].

أما بالنسبة لكندا فتحدد هذه المدة بمدى حياة المؤلف المقدرة بأكثر من 70 عاما على عكس القوانين المقارنة الأخرى[5].

أما بالنسبة للجزائر فالمدة المقررة لحماية المصنف هي بصفة عامة هي مدى حياة المؤلف المقدرة بـ50عاما- تماشيا مع اتفاقية برن- يبدأ في حسابها من سنة بعد وفاته[6].

---

[1]- يتطلب القانون الأمريكي مثل هذا الشرط.

[2]- لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، المرجع السابق، ص543.

[3]- Voir Association canadienne pour les études supérieures,(Propriété intellectuelle) , op cit, p9.

[4]- كان القانون الأمريكي الصادر في 1790/05/31 في القسم الأول منه الفقرة الأولى يقرر حماية قانونية للمصنف مدتها 14 عاما، يمكن تحديدها إلى 14 عاما أخرى إذا كان مؤلف المصنف حيا.

[5]- Voir Association canadienne pour les études supérieures,(Propriété intellectuelle) , opcit,meme page.

[6]- ينظر المادة 54 من الأمر رقم 05/03 المتعلقة بحماية حقوق المؤلف و الحقوق المجاورة.

أما بالنسبة للمصنف السمعي البصري (Œuvre audiovisuelle) المندرج تحته برامج الحاسب (Programmes d'ordinateur) فالمدة محددة بـ 50 عاما تبدأ في الحسبان من تاريخ أول سنة تم نشرها[1].

ثانيا:الركن المعنوي في جريمة النسخ عبر الإنترنت.

على الرغم من أن المشرع الجزائي لم ينص صراحة على ضرورة توافر هذا الركن إلا أن الفقه و القضاء يسلمان بضرورة توافره[2]. و لما كانت جريمة التقليد بصفة عامة هي جريمة عمدية أي يلزم لقيامها توافر القصد الجنائي و بالضبط العام من علم و إرادة[3]، فالأمر مطابق بالنسبة لجريمة التقليد عبر الإنترنت فهي عمدية تقوم على القصد الجنائي العام من علم و إرادة. فيكفي أن يعلم الجاني بأن نشاطه الإجرامي يرد على مصنف رقمي ينسب إلى شخص آخر، أي يعلم أن ما ينشره أو يذيعه أو يستعمله أو يقتبس منه من مصنفات رقمية موجودة في البيئة المعلوماتية بدون وجه حق، و أن تتجه إرادته إلى الإذاعة أو النشر أو الاستعمال أو الاقتباس حتى يتوافر القصد الجنائي. [4]

و تجدر الإشارة إلى أنه من المتفق عليه في الفقه و القضاء الفرنسيين أن القصد الجنائي في جريمة التقليد مفترض، بمعنى أن تحقق إحدى صور النشاط الإجرامي السابقة يعد قرينة تكفي في نفس الوقت للقول بتوافر القصد الجنائي أي أن حسن النية لا يفترض في هذه الجريمة[5].

المطلب الثاني:

المعالجة القانونية لجريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت.

يعتبر حق الملكية الفكرية من أكثر الحقوق التي يتم انتهاكها يوميا على شبكة الإنترنت أو على كافة شبكات الاتصالات والمعلومات على مستوى العالم. فالإنترنت بوصفها طريق اتصال يتيح تبادل المعلومات و نقلها بكافة صورها، مكتوبة و مرئية و مسموعة، و باعتبارها ليست مجرد صفحات للمعلومات بل مكانا للتسوق و موضعا للأعمال و الخدمات وفضاء غير متناه من الصفحات لنشر الأخبار و المعالجات

---

[1]– ينظر المادة 58 من الأمر السابق.

[2]– كان يوجد رأي في الفقه أصبح الآن مهجورا لا يشترط أن يتوافر لدى الجاني قصد جنائي لكي تتوافر جريمة التقليد في جانبه، و بالتالي اكتفي هذا الرأي بتوافر الركن المادي لدى الجاني حتى يعتبر مرتكبا لجريمة التقليد. إلا أن الفقه الحديث وسايره كذلك القضاء اشترط أن يتوافر لدى الجاني القصد الجنائي أي الركن المعنوي و لا يكتفي بتوافر الركن المادي حتى يسوغ القول بتوافر هذه الجريمة في جانبه،بالرغم من عدم اشتراط المشرع لتوافره في حق الجاني. لمزيد من التفاصيل ينظر د/ عفيفي كامل عفيفي، المرجع السابق، ص65.

[3]– ذهب اتجاه في الفقه إلى أنه يلزم توافر قصد جنائي خاص إلى جانب القصد العام و يتمثل في سوء نية الجاني. لمزيد من التفاصيل ينظر د/علي عبد القادر القهوجي، (الحماية الجنائية لبرامج الحاسب) مرجع سابق، ص30 و كذا د/ عفيفي كامل عفيفي، المرجع السابق، ص66.

[4]– لمزيد من التفاصيل ينظر د/ علي عبد القادر القهوجي، نفس المرجع ، ص30.

[5]– لمزيد من التفاصيل ينظر د/ علي عبد القادر القهوجي، نفس المرجع، ص31.

والمؤلفات و الأبحاث و المواد، هيئت أو أتاحت الفرصة لقراصنة المعلوماتية لانتهاك مثل هذه الحقوق لاسيما فيما يتعلق بحق الملكية الأدبية و الفنية. و عليه فوجود معاهدات دولية تمنع مثل تلك الانتهاكات وإصدار كل دولة قوانين خاصة بها تعمل على حماية الملكية الفكرية أصبح من الأمور الضرورية لتوفير الحماية القانونية للمصنفات المتصلة بالتقنية العالية و الموضوعة من قبل مؤلفيها ضمن جهدهم الفكري. ولقد خصصنا هذا المطلب لتوضيح التكييف القانوني لهذه الجريمة المستحدثة الواقعة عبر الانترنت، من خلال تقسيمه إلى فرعين نتطرق في أولهما إلى موقف المعاهدات التي تم إبرامها في هذا المجال ثم نسلط الضوء في ثانيهما لإبراز موقف التشريعات المقارنة من هذه الجريمة. و ذلك كمايلي:

الفرع الأول: المعالجة القانونية الدولية لجريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت.

الفرع الثاني: موقف التشريعات المقارنة من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت.

الفرع الأول: المعالجة القانونية الدولية لجريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت.

من أهم المعاهدات التي تم إبرامها في هذا المجال معاهدات ثلاث هم على التوالي:

- معاهدة برن.
- معاهدة تريبس.
- معاهدة الويبو.

أولا: معاهدة برن لحماية المصنفات الأدبية و الفنية:

تعتبر معاهدة بيرن التي تم التوقيع عليها في 1886/09/09 في سويسرا حجر الأساس في مجال الحماية الدولية لحق المؤلف و قد وقعت هذه الاتفاقية 120 دولة من بينها الجزائر[1]. و تعتبر المادة 09 منها الأساس لأنها تنص على منح أصحاب حقوق المؤلف حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة و بأي شكل كان. وفي أن يرخص أو يمنح أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه. و كذلك تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنيا أو أجنبيا[2]. و إلى جانب اتفاقية بيرن التي شهدت تعديلات عديدة آخرها تعديل باريس 1971 الشهير بصيغة باريس، توجد على الصعيد الدولي 4 اتفاقيات في حقل حق المؤلف (الاتفاقية العالمية بحقوق المؤلف المبرمة بجنيف عام 1952، اتفاقية التسجيل الدولي للمصنفات السمعية و البصرية –جنيف 1989، اتفاقية تفادي الازدواج الضريبي على عائدات حقوق المؤلف –مدريد 1979، اتفاقية الدوائر المتكاملة – واشنطن 1989) و ثلاث اتفاقيات بخصوص الحقوق المجاورة لحق المؤلف (اتفاقية حماية

---

[1]– صادقت الجزائر على هذه الاتفاقية بموجب المرسوم الرئاسي رقم 341/97 المؤرخ في 1997/09/13. إذ تضمن هذا المرسوم انضمام الجزائر مع التحفظ لهذه الاتفاقية. ينظر الجريدة الرسمية، العدد 61 المؤرخة في 1997/09/14.

[2]– منير محمد الجنبيهي، ممدوح محمد الجنبيهي،(جرائم الإنترنت و الحاسب الآلي) مرجع سابق، ص117.

فناني الأداء و منتجي التسجيلات الصوتية و هيئات الإذاعة- روما 1961، اتفاقية حماية منتجي التسجيلات الصوتية -جنيف 1970، اتفاقية توزيع الإشارات حاملة عبر التوابع الصناعية- بروكسل 1947)[1].

ثانيا: معاهدة تريبس.

معاهدة تريبس هي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطو عليها خصوصا مع انتشار عمليات السطو الإلكتروني على الأعمال الفنية دون إعطاء مالكيها أيا من حقوقهم المادية أو المعنوية.و تم التوقيع عليها عام 1994 ومن قبل الدول الأعضاء بها و هي تعد إطارا شاملا لموضوعات الملكية الفكرية، فهي تنظم حقوق المؤلف و من بينها حقوقه على المصنفات الرقمية بتوفيرها الحماية لبرامج الحاسوب و قواعد البيانات في مادتها العاشرة، و نظمت الحقوق المجاورة لحق المؤلف و العلامات التجارية و المؤشرات الجغرافية و التصميمات الصناعية، و براءات الاختراع و الدوائر المتكاملة و الأسرار التجارية و الممارسات غير التنافسية في الرخص[2].

هذا من جهة و من جهة أخرى، ربطت هذه الاتفاقية بين المعايير الدولية و المعايير المحلية و تضمنت العديد من الإجراءات الهامة و الفعالة لردع الإعتداءات على حقوق الملكية الفكرية. كما أنها و من جهة ثانية فرضت على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع و منها على سبيل المثال لا الحصر إعطاء الحق للسلطات في إصدار الأوامر بشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة والتي عادة ما تكون سهلة التخلص منها لو لم تكن هناك سرعة في محاولة ضبطها و كذلك التحفظ على أدوات ارتكاب الجرائم و ذلك فضلا على فرض عقوبات جنائية رادعة [3].

ثالثا: معاهدة الويبو: (المنظمة العالمية للملكية الفكرية)[4]

و تضم هذه المعاهدة ثلاث معاهدات و هي:

-معاهدة الويبو بشأن حق المؤلف.

- معاهدة الويبو بشأن الأداء و التسجيل الصوتي.

---

[1]- ينظر يونس عرب، (نظام الملكية الفكرية لمصنفات المعلوماتية) مرجع سابق، الجدول الأول، http:// www.arablawinfo.com.

[2]- يونس عرب، (نظام الملكية الفكرية لمصنفات المعلوماتية)مرجع سابق ، المنشور على الموقع السابق.

[3]- لمزيد من التفاصيل ينظر منير محمد الجنبيهي ممدوح محمد الجنبيهي،(جرائم الإنترنت و الحاسب الآلي) مرجع سابق، ص118.

[4]- أنشأت هذه المنظمة عام 1967 في مدينة استوكهولم و أصبحت إحدى وكالات هيئة الأمم المتحدة المتخصصة في 1974/12/17 و كذا الجهة الدولية التي تدير سائر اتفاقيات الملكية الفكرية. لمزيد من التفاصيل ينظر يونس عرب،(نظام الملكية الفكرية لمصنفات المعلوماتية) مرجع سابق، المنشور على الموقع السابق.

-معاهدة الويبو بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة[1].

كما أن الاتفاقية الأوربية حول الإجرام المعلوماتي المنعقدة في بودابست قد نصت هي الأخرى على هذه النوعية من الجرائم و ذلك لأن الانتهاكات الواقعة على الملكية الفكرية هي أحد أشكال الإجرام المعلوماتي الأكثر شيوعا، و الذي بازدياد نسبته يزداد قلق و انشغال العالم بأسره، بهذا التيار الإجرامي المتقدم. إذ خصصت له المادة العاشرة و العنوان الرابع.[2] و كذا الشأن بالنسبة لنظيرتها العربية و الخاصة بمكافحة جرائم تقنية المعلومات في المادة 17.[3]

---

[1]- لمزيد من التفاصيل ينظر منير محمد الجنبيهي ممدوح محمد الجنبيهي، (جرائم الإنترنت و الحاسب الآلي)مرجع سابق، ص118 و ما بعدها.

[2]- العنوان الرابع: الجرائم المتصلة بالإعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة.

تنص المادة العاشرة على:" 1- يجب على كل طرف أن يتبنى الإجراءات التشريعية، و أية إجراءات أخرى يرى أنها ضرورية لتجريم-تبعا لقانونه الداخلي- انتهاكات الملكية الفكرية المعرفة في قانون ذلك الطرف، وفقا للالتزامات التي تم التوقيع عليها في ظل الاتفاقية لحق المؤلف الموقعة في باريس في 24 جويلية 1971، و اتفاقية برن لحماية الأعمال الأدبية و الفنية، واتفاقية المنظمة العالمية للملكية الفكرية (OMPI). باستثناء أي حق معنوي ممنوح بواسطة هذه الاتفاقيات إذا ما ارتكبت هذه الأفعال عمدا، و على نطاق تجاري و بواسطة نظام معلوماتي.

2- يجب على كل طرف يتبنى الإجراءات التشريعية، و أية إجراءات أخرى، يرى أنها ضرورية من أجل تجريم – تبعا لقانونه الداخلي- انتهاكات الحقوق المجاورة المعرفة في قانون هذا الطرف، وفقا للالتزامات التي تم التوقيع عليها في ظل الاتفاقية الدولية لحماية الفنانين، المؤدين أو العازفين و منتجي الصوتيات و منظمات البث المبرمة في روما (اتفاقية روما)، و اتفاقية الجوانب التجارية لحقوق الملكية الفكرية و اتفاقية المنظمة الدولية للملكية (OMPI) بالنسبة للأداء، العزف، و البث. وباستثناء أي حق معنوي منصوص عليه بواسطة هذه الاتفاقيات إذا تم ارتكاب هذه الأفعال عمدا، و على نطاق تجاري، أو بواسطة نظام معلوماتي.

3- يمكن لأي طرف، في ظل ظروف محددة للغاية، أن يحتفظ بالحق في عدم تطبيق المسؤولية الجنائية، بالنسبة للفقرتين الأولى و الثانية من هذه المادة، بشترط توافر طرق أخرى فعالة و جاهزة، و أن لا يكون في هذا التحفظ ما يحمل اعتداء على الالتزامات الدولية المفروضة على هذا الطرف، في تطبيق الاتفاقيات الدولية المشار إليها في الفقرتين الأولى و الثانية من هذه المادة. لمزيد من التفاصيل ينظر د/ هلالي عبد اللاه أحمد، (الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية) مرجع سابق، ص332.

[3]- تنص المادة 17 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على:" إنتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، و ذلك إذا إرتكب الفعل على قصد و لغير الإستعمال الشخصي، و إنتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، و ذلك إذا إرتكب الفعل عن قصد و لغير الإستعمال الشخصي."

الفرع الثاني: موقف التشريعات المقارنة من جريمة الإعتداء على الملكية الأدبية والفنية عبر الإنترنت.

و نعرض تحت هذا الفرع إلى موقف التشريعات الغربية من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت أولا، ثم نخصص النقطة الثانية لتحديد موقف التشريعات العربية من هذه الجريمة. و ذلك كمايلي:

أولا: موقف التشريعات الغربية من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت

لقد وضعت الدول الغربية قوانين خاصة[1] لتوفير الحماية للملكية الأدبية و الفنية من الإعتداءات التي تتعرض لها من خلال الانترنت.و من هذه الدول فرنسا و الولايات المتحدة الأمريكية. و التي سيتم الطرق إليها كمايلي:

1/ موقف التشريع الفرنسي من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت:

---

[1]– ومن بين هذه الدول:الفلبين سنة 1972من خلال المرسوم الرئاسي رقم 49 تاريخ 1972/11/14، إيطاليا سنة 1981من خلال القانون رقم 407 تاريخ 1981/07/29. المتعلق بالإجراءات العاجلة ضد النسخ غير المشروع و إعادة الإنتاج (برمجيات و قواعد البيانات)،النصوص المتعلقة بحماية تصميم أشباه الموصلات لسنة 1987.السويد سنة 1982من خلال القانون رقم 284 لسنة 1982 – قواعد معلومات، قانون حماية تصاميم دوائر أشباه الموصلات رقم 1425 لسنة 1986، قانون حق المؤلف المعدل لسنة 1989– برمجيات. هنجاريا سنة 1983من خلال مرسوم وزارة الثقافة رقم 15 لسنة 1983 –البرمجيات.أستراليا سنة 1984من خلال القانون المعدل لقانون حق المؤلف لسنة 1984 المتعلقة بالمعلوماتية – الربمجيات.الهند من خلال القانون المعدل لقانون حق المؤلف لسنة 1984 – برمجيات.المكسيك من خلال القانون المعدل لقانون حق المؤلف رقم 114 لسنة 1984 – البرمجيات.فنلندا من خلال قوانين حق المؤلف المعدلة لقانون الأعمال الأدبية و الفنية لسنة 1984 ذوات الأرقام 34 لعام 91 و 418 لعام 93 و 446 لعام 1995 البرمجيات و قواعد المعلومات، قانون حماية طوبوغرافية أشباه الموصلات رقم 2 لسنة 91. تشيلي سنة 1985 من خلال قانون الملكية الفكرية لعام 85 برمجيات. ألمانيا من خلال القانون المعدل لقانون حق المؤلف لعام 85 و المعدل مرة أخرى عام 93 – برمجيات، قانون حماية طبوغرافية الشرائح الإلكترونية لأشباه الموصلات لعام 87 المعدل عام 90، المادة السابعة من قانون خدمات المعلومات و الاتصالات لعام 1997.اليابان من خلال قانون معدل لقانون حق المؤلف لعام 1985، قانون الدوائر المتكاملة و أشابه الموصلات لعام 1985. تايوان من خلال قانون حق المؤلف لعام 1987. البرازيل سنة 1987من خلال القانون رقم 646 لسنة 1987.كندا من خلال القسم 42 من قانون حق المؤلف المعدل لسنة 1987 –قواعد معلوماتية.إسبانيا من خلال قانون رقم 22 لسنة 87 المتعلق بالملكية الفكرية وفق آخر تعديل لعام 1996،قانون الحماية القانونية لطبوغرافية أشباه الموصلات لعام 1988 ،المادة 270 من القانون الجنائي لعام 1995.هولندا من خلال قانون 1987 لحماية الطبوغرافيا الأصلية لمنتجات أشباه الموصلات،قانون حق المؤلف لعام 1994 –برمجيات و قواعد معلومات.الدانمارك من خلال قانون حماية إنتاج أشباه الموصلات رقم 778 لسنة 1987،القانون رقم 153 لسنة 1988.إسرائيل سنة 1988 من خلال أمر/ تعليمات حق المؤلف رقم 1911 كما عدلت عام 1988.النمسا من خلال قانون حماية أشباه الموصلات رقم 372 لسنة 1988،قانون حق المؤلف رقم 93 لسنة 1993 المعدل رقم 151 لسنة 1996. (برمجيات و قواعد معلومات) النرويج سنة 1990 من خلال قانون حق المؤلف المعدل لعام 1990.لوكسمبورج من خلال قانون 1995 المعدل لقانون حق المؤلف لعام 1972.

تناول المشرع الفرنسي جريمة الإعتداء على الملكية الأدبية و الفنية في قانون الملكية الفكرية من خلال المادة 335-2 و الناصة على جريمة التقليد أو الاستنساخ لكتب أو ألحان موسيقية أو رسم أو رسم ألوان، سواء أكان ذلك عن طريق النسخ الكلي (بالطباعة الكلية) أو الجزئي (بالطباعة الجزئية). و على جريمة جلب أو تصدير مثل هذه المواد المستنسخة. حيث قررت لهما عقوبة الحبس لثلاث سنوات(3) و غرامة 300.000 يورو[1]. أما فيما يخص جريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت فقد عالجها المشرع الفرنسي من خلال المادة 335-3 من قانون الملكية الفكرية و التي تعاقب على استنساخ أو نشر أو بث بأية وسيلة كانت لمصنف فكري عدوانا على حقوق المؤلف. كما نظمها من خلال قانون حماية نشر الاختراعات عبر الانترنت الصادر بتاريخ 28 أكتوبر 2009 و المسمى ب HADOPI2 و الذي عدل و تمم قانون HADOPI و المحدد للعقوبات المقررة للتحميل غير المشروع المراقب من طرف السلطة العليا لحماية نشر المصنفات عبر الانترنت.[2]

2/موقف المشرع الأمريكي:

تناول المشرع الفدرالي الأمريكي هذه الجريمة سنة 1980 من خلال:

قانون حق المؤلف لبرامج الحاسوب لسنة 1980 المعدل لقانون حق المؤلف لسنة 1974. و قانون القرصنة و التقليد المعدل لعام 1982. و قانون حق المؤلف المعدل لسنة 1980.وقانون حماية شرائح أشباه الموصلات لعام 1994.[3]

ثانيا: موقف التشريعات العربية من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت

و سيتم التطرق من خلال هذه النقطة لتبيان موقف التشريعات العربية عامة من هذه الجريمة، لنوضح فيما بعد موقف التشريع الجزائري. و ذلك كمايلي:

---

[1]– Article L335-2 du code de la prpriété intellectuelle : « Toute édition d'écrits، de composition musicale، de dessin، de peinture ou de toute autre production، imprimée ou gravée en entier ou en partie، au mépris des lois et règlements relatifs à la propriété des auteurs، est une contrefaçon et toute contrefaçon est un délit.

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Seront punis des mêmes peines le débit، l'exportation et l'importation des ouvrages contrefaisants.

Lorsque les délits prévus par le présent article ont été commis en bande organisée، les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende. »

2 –Voir Loi relative à la protection pénale de la propriété littéraire et artistique sur internet , http:// Wikipedia.org.

- Anthoni BEM :Ordonnance relative à la loi HADOBI 2، la protection pénale de la propriété intéllectuelle et protection des données،http:// admin.ch.

- Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet،http:// www.legifrance.gouv.fr.

[3] –Voir Mercel DUBE :La protection et exploitation de la propriété intéllectuelle، p17،http:// archipel.uquan.com.

1/موقف التشريعات العربية عامة من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت

و لما كان هذا النوع من الجرائم المرتكب عبر الانترنت يهدد كلا من الدول الأجنبية و العربية على السواء فقد قرر مشرعو الدول العربية كغيرهم في الدول الأجنبية وضع قوانين خاصة تجرم و تعاقب على كل اعتداء عبر الانترنت على الملكية الأدبية و الفنية.و من بين هذه الدول:

الأردن من خلال القانون رقم 22 لسنة 1992 و المتعلق بقانون حماية حق المؤلف المعدل بالقانون 14 لسنة 1998 و 29 لسنة 1999 و يشمل حماية البرمجيات و قواعد البيانات.**الإمارات العربية المتحدة** من خلال القانون الاتحادي رقم 40 لسنة 1992 و لائحته التنفيذية و يتضمن حماية برامج الحاسوب.**البحرين** من خلال القانون رقم 10 لسنة 1993 و الذي وفر الحماية القانونية لبرامج الحاسوب . **مصر** من خلال قانون 29 لسنة 1994 المعدل لقانون 1954 و تضمن حماية برامج الحاسوب و قواعد البيانات.تونس من خلال القانون 36 سنة 1994. **قطر** من خلال قانون 25 لسنة 1995 والذي تضمنت قواعده حماية لبرامج الحاسوب.عمان من خلال قانون 47 لسنة 1996. **لبنان** من خلال قانون 75 لسنة 1999 و الذي يوفر الحماية لكلا من برامج و قواعد البيانات و كذلك الشأن بالنسبة **للكويت** من خلال المرسوم رقم 99/64.[1]

2/ موقف التشريع الجزائري من جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت:

نظم المشرع الجزائري جريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت في الأمر 05/03 المتعلق بحق المؤلف و الحقوق المجاورة[2] و ذلك بعد اعترافه الصريح على اعتبار برامج الحاسب الآلي هي من المصنفات المحمية في المادة 1/4[3]، بحيث يشكل أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج فعلا من أفعال التقليد. اذ نص على تلك الجريمة من خلال الفصل الثاني من هذا الأمر المعنون في المادة 151 و المادة 152.[4]

---

[1]– ينظر يونس عرب،(نظام الملكية الفكرية لمصنفات المعلوماتية) مرجع سابق، http:// www.arablawinfo.com

[2]– صدر الأمر 05/03 بتاريخ 2003/07/19 و المتعلق بحق المؤلف و الحقوق المجاورة ولقد عدل هذا الأمر و تمم الأمر رقم 10/97 المؤرخ في 1997/03/06 المعدل و المتمم للأمر رقم 14/73 المؤرخ في 1973/04/03.

[3]– تعدد المادة 4 و 5 من هذا الأمر المصنفات المحمية. حيث تنص المادة 1/4 منه على:" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية مايأتي:

أ) المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية، و البحوث العلمية و التقنية، و الروايات، و القصص، و القصائد الشعرية، و برامج الحاسوب، و المصنفات الشفوية مثل المحاضرات و الخطب و المواعظ و باقي المصنفات التي تماثلها."

و تجدر الاشارة إلى أن الأمر 14/73 لم يذكر في مادته 2 صراحة برامج الحاسوب ضمن المصنفات المحمية . ينظر لمزيد من التفاصيل مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا في أكتوبر 2009، كلية الحقوق و العلوم السياسية، جامعة زيان عاشور، الجلفة،ص 15 و مابعدها. و كذا آمال قارة، المرجع السابق، ص76 و ما بعدها. مقال في غياب خاص بالمعلوماتية في التشريع الجزائري، ص 136، http:// www.facebook.com

[4]– تنص المادة 151 من ذات الأمر على:" يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

– الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف،

و يتضح من خلال استقراء هاتين المادتين:

أ- أن الحالات التي تمثل جنحة التقليد وردت على سبيل الحصر لا المثال و التي يمكن تصنيفها إلى ثلاث أصناف:

الصنف الأول: و يتعلق بالجنح التي تمس بالحق المعنوي للمؤلف[1] و تضم فعلي الكشف غير المشروع عن مصنف أدبي أو أداء فني[2]، و كذا المساس بسلامة المصنف أو الأداء الفني.[3]

الصنف الثاني: و يتعلق بالجنح التي تمس بالحق المالي للمؤلف[4] و تضم فعلي استنساخ مصنف بأي أسلوب من الأساليب في شكل نسخ مقلدة، و ابلاغ المصنف أو الأداء الفني للجمهور عن طريق التمثيل

- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة،
- استيراد أو تصدير نسخ مقلدة من مصنف أو أداء،
- بيع نسخ مقلدة لمصنف أو أداء،
- تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أداء."

و تنص المادة 152 على:" يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداءالعلني، أو البث الاذاعي السمعي أو السمعي البصري، أو التوزيع بواسطة الكبل أو بأية وسيلة نقل أخرى لاشارات تحمل أصواتا أو صورا أو أصواتا أو بأي منظومة معالجة معلوماتية."

[1]- يقصد بالحق المعنوي للمؤلف:هو أن تنسب الفكرة الابتكارية إلى الشخص المبتكر وله وحده الحق في الكشف للكافة، أذن فالحق الأدبي يتعلق بالشخص المخترع في اسمه وسمعته وشهرته ونطاق هذا الحق زمنيا حق دائم عنها من الحقوق اللصيقة بشخص مؤلفها وبالتالي لا تخضع للتصرفات القانونية. وتتمثل الحقوق المعنوية بمايلي:

وهي الحق في أن ينسب إليه مصنفه وأن يذكر اسمه على جميع النسخ المنتجة الحق في تقرير نشر مصنفه وفي تعيين طريقة النشر وموعده

الحق في إجراء أي تعديل على مصنفه سواء بالتغيير أو التنقيح أو الحذف أو الإضافة.

الحق في دفع أي اعتداء على مصنفه وفي منع أي تشويه أو تحريف أو أي تعديل أخر عليه أو أي إضافة أو مساس به من شأنه الإضرار بسمعته وشرفه على أنه إذا حصل أي حذف أو تغيير أو أو أي تعديل آخر في ترجمة المصنف.

وجدت أسباب جدية ومشروعة لذلك ويلزم المؤلف في هذه الحالة بتعويض من آلت إليه حقوق الاستغلال المالي الحق في سحب مصنفه من التداول إذا تعويضاً عادلا. مقال حقوق الملكية الفكرية في البيئة الرقمية،http:// alyaseer.net

[2]- تنص المادة 22 من الأمر 05/03 على:" يتمتع المؤلف بحق الكشف عن المصنف الصادر باسمه الخاص أو تحت اسم مستعار.و يمكنه تحويل هذا الحق للغير.

يعود الكشف عن المصنف بعد وفاة مؤلفه إلى ورثته ما لم تكن هناك وصية خاصة

تفصل الجهة القضائية التي يختارها المبادر بكشف المصنف في حالة نزاع بين الورثة....."

3- تنص المادة 25 من ذات الأمر:" يحق للمؤلف اشتراط احترام سلامة مصنفه و الاعتراض على أي تعديل يدخله عليه أو تشويهه أو افساده اذا كان ذلك من شأنه المساس بسمعة المؤلف أو بشرفه أو بمصالحه المشروعة."

[4]- يقصد بالحق المالي للمؤلف: هي الحق بالاستغلال المادي وتتمثل في الإفادة مالياً من الإنتاج الفكري والإبداعي، ، فهو حق مؤقت، ويجوز لمالك الحق بعد ذلك أن يتصرف به كيفما يشاء، حيث أن للمؤلف الحق في استغلال مصنفه بأي طريقة يختارها و لايجوز للغير القيام بأي تصرف مما هو مبين أدناه دون اذن كتابي من المؤلف أو من يخلفه.

وتتمثل الحقوق المادية فيما يلي:

أو الأداء العلني، أو البث الاذاعي السمعي أو السمعي البصري، أو التوزيع بواسطة الكبل أو بأية وسيلة نقل أخرى لاشارات تحمل أصواتا أو صورا أو أصواتا أو بأي منظومة معالجة معلوماتية.

الصنف الثالث: و يضم الجنح المشابهة لجنحة التقليد و المتمثلة في خمس جنح مشابهة للتقليد و التي يطلق عليها جنح البيع بالمفرق[1] و تي يمكن حصرها في:

استيراد النسخ المقلدة و تصديرها سواء بالنقل المادي لها أو النقل المعنوي و الذي يتحقق في حالتنا هذه عن طريق شبكات الحاسوب التي تربط العديد من الدول أي عن طريق الانترنت[2]، بيع نسخ مزورة من المصنف، تأجير مصنف مقلد أو عرضه للتداول[3]، و الجنحتين المتعلقتين بالمساعدة و المشاركة في المساس بحقوق المؤلف و الرفض عمدا دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف.[4]

ب–تستوجب جريمة التقليد لقيامها أركان. ركن شرعي يتمثل في النصوص القانونية التي توفر الحماية الجنائية لحق المؤلف و الحقوق المجاورة و التي خصها المشرع بالفصل الثاني المعنون بالأحكام الجزائية وفي المواد من 151 إلى غاية 160 من ذلك الأمر. و ركن مادي و الذي يتمثل النشاط المادي فيه في الإعتداء على حق من حقوق المؤلف التالية:

الإعتداء على الحق في الكشف عن المصنف و يكون هذا عندما ينشر أو يذاع هذا المصنف في غير الوقت المناسب و المحدد من قبل مؤلفه أو بطريقة غير الطريقة التي يراها ملائمة له. فمثلا يمكن نشر

الحق في استنساخ المصنف بأي طريقة أو شكل سواء كان بصورة مؤقتة أو دائمة بما في ذلك التصوير الفوتوغرافي أو السينمائي أو التسجيل الرقمي الالكتروني والحق في طباعة المصنف وإذاعته وإخراجه

الحق في ترجمة المصنف إلى لغة أخرى أو اقتباسه أو توزيعه موسيقيا أو إجراء أي تحوير عليه

الحق في التأجير التجاري للنسخة الأصلية من المصنف أو نسخة منه إلى الجمهور

الحق في توزيع المصنف أو نسخه عن طريق البيع أو أي تصرف أخر ناقل للملكية

الحق في استيراد نسخ من المصنف وان كانت هذه النسخ قد أعدت بموافقة صاحب الحق فيه

و الحق في نقل المصنف إلى الجمهور عن طريق التلاوة أو الإلقاء أو العرض أو التمثيل أو النشر الإذاعي أو التلفزيوني أو السينمائي أو أي وسيلة أخرى سلكية كانت أو لاسلكية بما في ذلك إتاحة هذا المصنف للجمهور بطريقة تمكنه من الوصول إليه في أي زمان ومكان يختاره أي منهم. مقال حقوق الملكية الفكرية في البيئة الرقمية، المنشور على الموقع السابق.

[1]– آمال قارة، المرجع السابق، ص84.

[2]– تنص المادة 153 من الأمر05/03 على:"يعاقب مرتكب جنحة التقليد مصنف أو أداء، كما هو منصوص عليه في المادتين 151 و 152 أعلاه، بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات و بغرامة من خمسمائة ألف دينار (500.000 دج) إلى مليون دينار (1.000.000 دج) سواء كان النشر قد حصل في الجزائر أو في الخارج".

[3]– تنص المادة 154 من ذات الأمر على:"يعد مرتكبا الجنحة المنصوص عليها في المادة 151 من هذا الأمر و يستوجب العقوبة المقررة في المادة 153 أعلاه، كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة."

[4] – تنص المادة 154 من ذات الأمر على:"يعد مرتكبا لجنحة التقليد و يستوجب نفس العقوبة المقررة في المادة 153 أعلاه، كل من يرفض عمدا دفع المكافأة المستحقة للمؤلف لأي مالك حقوق مجاورة آخر خرقا للحقوق المعترف بها بموجب الحقوق المنصوص عليها في هذا الأمر."

المصنف من قبل دور النشر الالكترونية دون إذن المؤلف أو المتنازل إليه يعد تعدياً على حق المؤلف.أو بث الأغاني وتوزيعها عبر شبكة الانترنت دون ترخيص .

الإعتداء على الحق في سلامة المصنف و ذلك من خلال تعديل و تحوير أو تغيير أو حذف أو اضافة ترد على المصنف من شخص آخر و دون اذن من المؤلف. فمن يقوم بانزال معلومات رقمية من كتاب أو برنامج عبر الانترنت و يقوم بتغيير مصدر محتويات المعلومة باضافة أو حذف أو تحوير في تلك المحتويات بغير علم مؤلفها و رغبته يكون قد ارتكب جريمة التقليد الناتجة عن اعتدائه الواقع على الحق في سلامة المصنف المنشور عبر الانترنت.

الإعتداء على الحق في النسخ و الذي يكون عن طريق النسخ الحرفي الكامل للمصنف أو الجزئي أو بطريق الاقتباس أو التشويه عن طريق حذف أجزاء من البرنامج. و سواء تم ذلك النسخ باسم مؤلفه الحقيقي أم الخيالي الذي يخلقه الناسخ.[1]

الإعتداء على حق المؤلف في ابلاغ المصنف أو الأداء إلى الجمهور: ويعتبر الإبلاغ عموميا حينما يبقى خارج الإطار العائلي بالمفهوم الدقيق ويحتوي حق الإبلاغ على كل إبلاغ سواء كان مباشرا أو غير مباشر عن طريق تثبيتات كالأسطوانات أو الفيلم أو الفيديو....الخ. [2]

و يشترط القانون ان تكون تلك الإعتداءات بدون رضا المؤلف، أي بدون اذن من المؤلف أو من خلفه.أما فيما يخص للركن المادي في الجنح المشبهة بالتقليد فتتمثل صوره في:

استيراد أو تصدير النسخ المقلدة من الجزائر أو في الخارج، بيع و تأجير نسخ مقلدة، عرض نسخ مقلدة للتداول، المساعدة و المشاركة في المساس بحق المؤلف و الرفض العمدي لدفع المكافأة المستحقة.

أما بالنسبة للركن المعنوي لهذه الجريمة فالقصد الجنائي فيها مفترض و على الجاني اثبات العكس.[3]

أما فيما يتعلق بالعقوبات المقررة لمثل هذه الجريمة فقد حددتها المواد من 153 إلى غاية 159[4] من ذلك الأمر و قد تم التشديد في هذه العقوبات عما كانت عليه سابقا. و ذلك على النحو التالي:

-للقاضي أن يطبق كعقوبة أصلية الحبس من 6 أشهر إلى 3 سنوات وغرامة قدرها 500.000 دج إلى 1000.000 دج سواء تمت عملية النشر في الجزائر أو في الخارج.[5]

-للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لأقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف (البرنامج) وكل النسخ المقلدة والمصادرة تدبير تكميلي

- وتأمر الجهة القضائية بتسليم العتاد أو النسخ المقلدة أو قيمــة دلك وكذلك الإيرادات موضوع المصــادرة

---

[1]- ينظر لمزيد من التفاصيل آمال قارة، المرجع السابق، ص 86 و مابعدها.

[2] - مقال في غياب خاص بالمعلوماتية في التشريع الجزائري، ص 41، http:// www.facebook.com

[3]- ينظر لمزيد من التفاصيل آمال قارة، المرجع السابق ، ص88.

[4]- كانت هذه العقوبات في السابق منظمة في قانون العقوبات الجزائري في المواد390 إلى 394.

[5]- ينظر المادة153 السابقة الذكر.

للمؤلف أو أي مالك حقوق آخر لتكون عند الحاجة بمثابة تعويض.[1]

– يمكن للقاضي بناء على طلب الطرف المدني الأمر بنشر أحكام الإدانة على نفقة المحكوم عليه على ألا تتعدى المصاريف قيمة الغرامة المحكوم بها.[2]

– للقاضي أن يضاعف العقوبات المقررة وذلك في حالة لعود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر، وإذا اقتضى الحال تقرير الغلق النهائي[3].

تجدر الإشارة إلى إجراء هام يتم اثر اكتشاف جريمة التقليد وهو ما يسمى بالحجز الناتج عن التقليد اذ يمكن لمؤلف المصنف الرقمي المحمي أو ذوي حقوقه المطالبة بحجز الوثائق و النسخ الناتجة عن الاستنساخ غير المشروع أو التقليد، وذلك حتى في غياب ترخيص قضائي أو المطالبة بإيقاف لأية عملية جارية ترمي إلى الاستنساخ غير المشروع للمصنف الرقمي أو حجز الدعائم المقلدة والإيرادات المتولدة عن الاستغلال غير المشروع للمصنفات المعلوماتية.

على أن من اختصاص ضباط الشرطة القضائية معاينة انتهاك حقوق المؤلف وهم مؤهلون بصفة تحفظية بحجز النسخ المقلدة من المصنف أو من دعائم المصنفات ولكن بشروط أن تكون النسخ المقلدة موضوعة تحت الحراسة من طرف الديوان الوطني لحقوق المؤلف والحقوق المجاورة. و أن على المحضر الذي يثبت بان النسخ المقلدة المحجوزة التقدم لرئيس الجهة القضائية المختصة إقليميا [4].

كما يختص بعملية الحجز الأعوان المحلفون التابعين للديوان الوطني لحقوق المؤلف والحقوق المجاورة لكن بشروط :

وضع النسخ المقلدة تحت حراسة الديوان الوطني لحقوق المؤلف والحقوق المجاورة.

---

[1] – تنص المادة 157 من الأمر السابق على:"تقرر الجهة القضائية المختصة:
مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الإستغلال غير الشرعي لمصنف أو أداء محمي.
مصادرة و اتلاف كل عتاد أنشئ خصيصا لمباشرة النشاط غير المشروع و كل النسخ المقلدة."

[2]– تنص المادة 158 من الأمر السابق على:" يمكن الجهة القضائية المختصة، بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزأة في الصحف التي تعينها، و تعليق هذه الأحكام في الأماكن التي تحددها و من ضمن ذلك على باب مسكن المحكوم عليه و كل مؤسسة أو قاعة حفلات يملكها، على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها."

[3]– تنص المادة 156 من الأمر السابق على:"تضاعف في حالة العود، العقوبة المنصوص عليها في المادة 153 من هذا الأمر.
كما يمكن الجهة القضائية المختصة أن تقرر الغلق المؤقت مدة لا تتعدى ستة (6) أشهر للمؤسسة التي يستغلها المقلد أو شريكه أو أن تقرر الغلق النهائي عند الاقتضاء."

[4]– تنص المادة 145 من الأمر السابق على:"يتولى ضباط الشرطة القضائية أو الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف و الحقوق المجاورة معاينة المساس بحقوق المؤلف أو الحقوق المجاورة."

الإخطار الفوري لرئيس الجهة القضائية المختصة إقليميا بمحضر مؤرخ و موقع قانونيا يثبت النسخ المقلدة (المحجوزة). [1]

الفصل الثاني:

جريمة غسل الأموال والمخدرات عبر الإنترنت

لقد أصبحت شبكة الإنترنت في عصرنا هذا أداة فعالة وقناة اتصالية ممتازة ومجالا رحبا لانتشار أخطر وأبشع الجرائم التي تهدد عالمنا هذا والتي كانت سابقا – في العالم المادي– يحسب لها ألف حساب ومن بينها جريمتي غسل الأموال التي تعتبر ظاهرة إجرامية ومشكلة عالمية وصورة من الصور الحديثة للجرائم الاقتصادية وبالضبط الجريمة المنظمة، والتي ساهمت الإنترنت في تغذيتها وكثرتها لا سيما مع ظاهرة المدفوعات الإفتراضية (cyber – payement)[2]. و جريمة المخدرات التي تهدد جميع فئات المجتمع والتي ساهمت تلك الشبكة في ترويجها وكيفية تعاطيها وزرعها... إلخ.

وعليه سيتم تناول هاتين الجريمتين بنوع من التفصيل في المبحثين التاليين:

المبحث الأول: جريمة غسل الأموال عبر الإنترنت.

المبحث الثاني: جريمة المخدرات عبر الإنترنت.

---

[1]– تنص المادة 146 من الأمر السابق على:" فضلا عن ضباط الشرطة القضائية، يؤهل الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف و الحقوق المجاورة للقيام بصفة تحفظية بحجز نسخ دعائم المصنفات أو الأداءات المقلدة شريطة وضعها تحت حراسة الديوان.

يخطر فورا رئيس الجهة القضائية المختصة بناء على محضر مؤرخ و موقع قانونا يثبت النسخ المقلدة المحجوزة.

تفصل الجهة القضائية في طلب الحجز التحفظي خلال ثلاثة (3) أيام على الأكثر من تاريخ اخطارها." كما تنص المادة 147 على:" يمكن رئيس الجهة القضائية المختصة بأن يأمر بناء على طلب من مالك الحقوق او ممثله بالتدابير التحفظية الآتية:

ايقاف كل عملية صنع جارية ترمي إلى الإستنساخ غير المشروع للمصنف أو للأداء المحمي أو تسويق دعائم مصنوعة بما يخالف حقوق المؤلفين و الحقوق المجاورة.

القيام و لو خارج الأوقات القانونية بحجز الدعائم المقلدة و الإيرادات المتولدة من الإستغلال غير المشروع للمصنف أو للأداء المحمي أو تسويق دعائم مصنوعة بما يخالف حقوق المؤلفين و الحقوق المجاورة.

حجز كل عتاد استخدم أساسا لصنع الدعائم المقلدة.

يمكن رئيس الجهة القضائية المختصة أن يأمر بتأسيس كفالة من قبل المدعي."

[2]– عمر محمد أبو بكر بن يونس و د/ يوسف أمين شاكر: غسل الأموال عبر الإنترنت، الطبعة الأولى، أقاقوس، القاهرة، 2004، ص31.

المبحث الأول:

جريمة غسل الأموال عبر الإنترنت

تعد ظاهرة غسل الأموال[1] وكما يسميها البعض تبييض الأموال[2] أو جريمة التسعينات[3] إحدى الظواهر الإجرامية المعاصرة المصنفة ضمن الجرائم الاقتصادية الحديثة المرتبطة بالجريمة المنظمة التي أثارت قلق الأنظمة السياسية في مختلف دول العالم خاصة في الآونة الأخيرة التي تشهد تطورا تكنولوجيا وتقنيا زاد من خطورتها الاقتصادية، بخلقه لكيانات اقتصادية قد تمتد عبر الحدود الدولة الواحدة بهدف تدمير اقتصاديات تلك الدول لاسيما مع ظهور الإنترنت وتزايد استخدامها كوسيط تجاري، إذ ساهمت وسهلت بطاقات الدفع وطرق التسديد الأخرى عبر تلك الشبكة في الكثير من عمليات غسل الأموال. وتحولت بذلك تلك الجريمة من تقليدية إلى مستحدثة تستخدم لارتكابها التقنية العالية كالحاسب الآلي والإنترنت فظهر بذلك ما يسمى جريمة غسل الأموال عبر الإنترنت أو جريمة للتبييض الإليكتروني[4].

الأمر الذي دفع بالعديد من المشرعين و الفقهاء إلى التدخل للإيجاد طرق لمكافحة هذه الظاهرة ذات المخاطر الاقتصادية والسياسية والاجتماعية وذلك بتحديدها[5] وتبيان طبيعتها وخصائصها والمراحل التي تمر بها.

وفي هذا انقسم هؤلاء إلى فئتين، فئة تعرف تلك الظاهرة تعريفا ضيقا وذلك بحصرها في الأموال غير المشروعة الناتجة عن جرائم معنية ومحددة على سبيل الحصر نذكر منها: جريمة الاتجار بالمخدرات، أو جريمة تمويل الإرهاب، جرائم الإعتداء على البيئة، جرائم استيراد الأسلحة والذخائر والمفرقعات، جرائم سرقة الأموال واغتصابها جرائم الفجور و الدعارة و جرائم الواقعة على الآثار وجرائم الاتجار بالأشخاص

---

[1]– لقد استعمل المشرع الجزائري مصطلح تبييض الأموال بدلا من مصطلح غسل الأموال. لمزيد من التفاصيل ينظر لعشب علي: الاطار القانوني لمكافحة غسل الأموال، ديوان المطبوعات الجامعية، الجزائر، بدون سنة نشر، ص16.

[2]– لمصطلح غسل الأموال مسميات أخرى نجدها في بعض الكتابات كتطهير الأموال، تنظيف الأموال ولكنها كلها تؤدي إلى نفس المعنى لعشب علي: نفس المرجع، نفس الموضع. والمصطلح غسل الأموال يقابله باللغة الفرنسية Blanchiment d'Argent، وفي اللغة الإنجليزية Money Laudring يرجع أصل هذا المصطلح لعام 1973 محمد سامي الشوا: السياسية الجنائية في غسل الأموال، دار النهضة العربية، القاهرة، بدون سنة الطبع، ص14.

[3]– د/ محمد الأمين البشري، (التحقيق في الجرائم المستحدثة) مرجع سابق، ص 181.

[4]–Voir Blanchiment des capitaux : nouvelle tendance de la Cybercriminalité en 2006, http://www.zdnet.fr

[5]– جاء في منجد اللغة والإعلام بأن غسل: "غسلا وغسلا الشيء: طهره بالماء وأزال وسخه والغسل، الاسم من غسل وجمعه أغسال والغسالة ما يغسل من ثوب. المنجد في اللغة والإعلام، الطبعة السابعة والعشرون، دار المشرق، بيروت، 1984، ص550.

والأطفال والاتجار غير المشروع بالأعضاء البشرية، جرائم الرشوة والابتزاز وغيرها من جرائم المنظمة المعاصرة [1].

أما أصحاب الفئة الثانية، فضلوا وضع تعريف واسع لها، وذلك بعدم حصر مصادرها في جرائم محددة، وإنما تتسع لتشمل الأموال القذرة الناتجة عن جميع الجرائم والأعمال غير المشروعة بدون استثناء[2].

إذن فجريمة غسل الأموال تعني إخفاء طبيعة أو مصدر الأموال غير المشروعة المتحصلة من الجرائم المنظمة المعاصرة التي لا تقع تحت سبيل الحصر، أي أنها من الجرائم المركبة[3] التي تستلزم وجود جريمة

---

[1]– من التشريعات و الآراء الفقهية التي أخذت بهذا التعريف نجد:

اتفاقية فيينا لسنة 1998 الخاصة بمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، الاتفاقية الدولية لقمع وتمويل الإرهاب المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة ليوم: 1990/12/09، قانون مكافحة تبييض الأموال اللبناني، رقم 318 لسنة 2001 ورقم 547 لسنة 2003، قانون مكافحة غسل الأموال الليبي الصادر لسنة 2002، قانون مكافحة غسل الأموال وتمويل الإرهاب سوري رقم 59 لسنة 2003، قانون مكافحة غسل الأموال السوداني لسنة 2003، قانون غسل الأموال المصري رقم 80 لسنة 2002.

أما بالنسبة للفقه الجنائي فنجد أن المستشار عمرو عيسى الفقي قد عرفها بأنها "عملية يلجأ إليها من يعمل بتجارة المخدرات والجريمة المنظمة أو غير المنظمة لإخفاء المصدر الحقيقي للدخل غير المشروع والقيام بأعمال أخرى للتمويه كي يتم إضفاء الشرعية على الدخل لذي تحقق " وكذلك الأستاذ وليد حجاج إسماعيل حيث عرفها بأنها: " إخفاء طبيعة الأموال المتحصلة من الجرائم المنصوص عليها بالمادة (2) من قانون مكافحة غسل الأموال المصري رقم 80 لسنة 2002، وإظهارها بمظهر الأموال المستمدة من مصادر مشروعة (نظيفة) كما لو كان قد بذل صاحبها من أجل حصدها الوقت والعرق وحرص بالعمل المتواصل على تكوينها". ينظر على التوالي المستشار عمرو عيسى الفقي: الجرائم المعلوماتية، جرائم الحاسب والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث،الإسكندرية، 2006، ص140. وليد حجاج إسماعيل: قانون مكافحة غسل الأموال رقم 80 لسنة 2002، دار أبو المجد للطباعة، مصر 2002، ص12.

[2]– ومن مؤيدي هذا التعريف: القانون الأمريكي لسنة 1986، قانون تبييض الأموال الفرنسي رقم 96 – 392 المعدل والمتمم لقانون العقوبات الفرنسي. القانون المتعلق بدعم المجهود الدولي لمكافحة الإرهاب ومنع لغسل الأموال التونسي رقم 75 الصادر لسنة 2003، تعليمات مكافحة غسل الأموال لسنة 2001 الصادرة عن البنك المركزي الأردني، القانون رقم 04–05 المعدل والمتمم لقانون العقوبات الجزائري في مادته 389 مكرر وكذا القانون رقم:01/05 المؤرخ في 2005/02/06 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها. أما فيما يخص الفقه، ينظر كلا: د/ محمد الأمين البشري، مرجع سابق ص185 و188 د/ هدى حامد قشقوش: جريمة غسل الأموال في نطاق التعاون الدولي، دار النهضة العربية، القاهرة، 2001، ص7.د/ إبراهيم عيد نايل: المواجهة الجنائية لظاهرة غسل الأموال في القانون الجنائي الوطني والدولي، بدون دار النشر، 1997، ص635، منير محمد الحنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص79، لعشب علي، المرجع السابق،ص24–25 حيث تتفق كلها بأن جريمة غسل الأموال: "هي أية عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسب منه الأموال أيان كان مصدرها".

[3]– يقصد بالجرائم المركبة: الجرائم التي يشترط فيها القانون وقوع فعل إلى جانب الجريمة الأصلية بحيث يصبح عنصرا من عناصر هذه الجريمة أو ظرفا مشددا لعقوبة: أو هي تلك الجرائم التي يتطلب المشرع لتمام ركنها المادي حدوث أكثر من واقعة. ينظر عبد الله سليمان،المرجع السابق، ص355.

أصلية أو أولية يتحصل منها على الأموال القذرة كالاتجار في المخدرات ثم تليها جريمة غسل الأموال كجريمة لاحقة.

وغسل الأموال مصطلح حديث نسبيا، بدأ استخدامه في الولايات المتحدة الأمريكية نسبة إلى مؤسسات الغسل التي تمتلكها المافيا، وهي مؤسسات نقدية كان يتاح فيها مزج الإيرادات غير المشروعة إلى حد تظهر فيها وكأنها محصلة من مصدر مشروع[1].

وهي كغيرها من الجرائم لها ثلاثة أركان ركن شرعي، وركن مادي[2]، وركن معنوي[3]. وتمر هذه الظاهرة بثلاثة مراحل تشكل في حقيقة " دورة غسل الأموال" منذ نشأة الأموال عن إحدى الطرق الإجرامية مرورا بمرحلة الإيداع ثم التعميم ومرحلة الإدماج[4]. وتتكون عناصر هذه العملية من الغاسل و الغسول والمغسول[5].

ولقد أدى النمو المتسارع لاستخدام الإنترنت كوسيط تجاري إلى تزايد انتشار الجريمة على تلك الشبكة وتنوع أشكالها وطرق ارتكابها بصورة مطردة، بداية من سرقة بيانات الحسابات المصرفية وبطاقات الائتمان من قبل الهاكرز مرورا ببيع صور الأطفال على المواقع الإباحية، وحتى قيام عصابات غسل الأموال بإخفاء الأموال غير المشروعة وتمويهها عبر متاهات من الحسابات المصرفية على الشبكة الأم. وبالتالي بروز فجر جريمة مستحدثة تستخدم فيها التقنية الحديثة في ارتكابها كالإنترنت والحواسب أصطلح عليها تسمية: غسل الأموال عبر الإنترنت Cyber Laundering أو التبييض الإليكتروني. وفي هذا يصف أحد الباحثون علاقة الإنترنت بظاهرة غسل الأموال بأنها: " حركة سريعة لا تتوقعها الحدود الجغرافية والجودة

1- لعشب علي، المرجع السابق ص 16 ويرجع ظهورها للمرة الأولى لمبتكرها Capme. د/ محمد سامي الشوا، المرجع السابق ص 15.

2- لمزيد منالتفاصيل حول الركن الشرعي والركن المادي لجريمة غسل الأموال ينظر لعشب علي، المرجع السابق، ص102 وما بعدها.

3- لقد انقسمت حيال صورة هذا الركن الآراء الفقهية إلى اتجاهين: اتجاه يتطلب القصد الجنائي فقط وأخر يضاف إلى الجانب القصد الجنائي الخطأ. لمزيد من التفاصيل ينظر لعشب علي، نفس المرجع، ص108 وما بعدها.

4- هناك اتجاه حديث يرى أن المرور بمراحل الغسل الثلاث المشار إليها أعلاه ليس أمرا حتميا، ويفضل تقسيم عملية غسل الأموال إلى ثلاثة أنواع رئيسية للغسل وهي: الغسل البسيط، الغسل المتوسط، الغسل المتقن، لمزيد من التفاصيل ينظر عبد الفتاح سليمان: مكافحة غسل الأموال، الطبعة الأولى، دار علاء الدين للطباعة والنشر، القاهرة، 2004، ص140 وما بعدها. وتجدر الإشارة إلى أن د/ محمد الأمين البشري ضاف مرحلة رابعة وهي مرحلة النشاط غير المشروع. لمزيد من التفاصيل ينظر د/ محمد الأمين البشري،المرجع السابق، ص 190 وما بعدها. وكذلك عمرو عيسى الفقي، المرجع السابق، ص204 -205.

5- الغاسل هو الشخص أو المنظمة أو المؤسسة التي تحوز أو تمتلك أموال غير المشروعة وتسعى إلى غسلها.

الغسول: وهو المؤسسة أو المصرف الذي يقوم بالإجراءات المخالفة للقانون ويلحق بهم فئات السماسرة والعملاء والوسطاء والمساعدين.

المغسول وهو عبارة عن الأموال أو المتحصلات أو غيرها.

ذاتها تجعل الإنترنت و البطاقات الذكية محل ترحيب من الجمهور وكذلك محل جاذبية من المجرمين الذين هم في شوق لغسل أموالهم بهدوء وسرعة. فالنقود الإليكترونية وسيلة سهلة في التحويل والنقل من مكان لأخر "[1].

والإشكال المطروح هنا هو ماذا نعني بهذه الجريمة المستحدثة؟ وما هي خصائصها؟ وما هي المراحل التي تمر بها؟وما هي الأساليب الحديثة التي ترتكب بواسطتها؟.

اشكالات سيتم الإجابة عليها وفقا للمطلبين التاليين:

المطلب الأول: تعريف جريمة غسل الأموال عبر الإنترنت و مراحلها.

المطلب الثاني: طرق ووسائل غسل الأموال عبر الإنترنت و التكييف القانوني لها.

المطلب الأول

تعريف جريمة غسل الأموال عبر الإنترنت ومراحلها.

نتناول في هذا المطلب تعريف جريمة غسل الأموال عبر الإنترنت و كذا المراحل التي تمر بها هذه الجريمة، و ذلك في الفرعين التاليين:

الفرع الأول: تعريف جريمة غسل الأموال عبر الإنترنت.

الفرع الثاني: مراحل عملية غسل الأموال عبر الإنترنت.

الفرع الأول: تعريف جريمة غسل الأموال عبر الإنترنت

إن لمصطلح غسل الأموال عبر الإنترنت العديد من التعريفات، إلا أن جميعها تصب في نفس الهدف. ومن هذه التعريفات أنها عبارة عن :"إظهار الأموال المتحصلة من جرائم الاتجار بالتجارة غير المشروعة مثل المخدرات و الإرهاب والقمار وغيرها بصورة تتمتع بقانونية المصادر وشرعيتها عبر استخدامها لشبكة الإنترنت كأداة لإخفاء هذا المصدر غير المشروع أو ذاك الذي تحصلت منه هذه الأموال"[2].

و من خلال التعريف السابق يمكن استخلاص ما يلي:

– أن غسل الأموال عبر الانترنت هو جريمة ناتجة عن أعمال أو أنشطة إجرامية حققت عوائد مالية ضخمة، يعاد ضخها في الاقتصاد الدولي عبر شبكة الانترنت باستخدام النقود الاليكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الانترنت أو تداول الأسهم و ممارسة الأنشطة التجارية عبر هذه الشبكة.

---

[1]– د/ عبد الفتاح بيومي حجازي: جريمة غسل الأموال بين الوسائط الإليكترونية ونصوص التشريع، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2005، ص 23.

[2]– د/ عبد الله عبد الكريم عبد الله: جرائم غسل الأموال على شبكة الإنترنت، دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، 2008، ص 21

– أن فكرة جريمة غسل الأموال عبر الانترنت يعود إلى عصابات الجريمة المنظمة من حيث المصدر، والتي فضلت لحل مشاكل سيولتها و عدم قدرتها بالاحتفاظ بالأموال القذرة في البنوك و مشاكل اكتشاف أنشطتها في غسل الأموال بصورتها التقليدية[1]. إضفاء صفة الشرعية على مصادر أموالها غير المشروعة من خلال غسلها عبر شبكة الانترنت، مما نتج عنه تسهيل ارتكاب هذه الجريمة بسرعة تختلف عن مثيلاتها التي ترتكب بالصورة التقليدية و جعلها تنتشر بشكل واسع النطاق متعدية للحواجز الحدودية الموجودة بين الدول، لدرجة أنه بفضل هذه الشبكة أصبحت أو تحولت تلك الجريمة إلى أخطر الجرائم الاقتصادية التي ظهرت في عصرنا الحالي.

– لم يبق مصدر الأموال غير المشروعة محصورا أساسا في تجارة المخدرات كما هو الشأن في غسل الأموال بصورتها التقليدية، بل و نتيجة الانفتاح العالمي و ارتباط الأسواق الدولية بعضها ببعض، اتسعت مصادر هذه الجريمة بصورتها المستحدثة لتضم أعمال التجارة بالأسلحة و تجارة الرقيق و الدعارة التي تتم من خلال شبكة الانترنت و عبر الكمبيوتر و آلياتهاالاليكترونية. فأصبحت بذلك الجريمة تتم و تنظم اليكترونيا، و تحقق بذلك أرباحا طائلة إلى جانب تجارة المخدرات.

– لا تقتصر هذه الجريمة على مرتكبها فقط، و إنما تتعداه إلى كل من شارك فيها من مساهمين ومتدخلين و مستفيدين و كل من أخفى معلومات أو أنكر حقائق تتعلق بطبيعة المصدر أو بعلاقة الملكية[2].

– تتميز هذه الجريمة بنفس الخصائص التي تتميز و تنفرد بها جرائم الانترنت، و ذلك لكونها مجرد نوع منها. و تتلخص هذه الخصائص في سهولة ارتكابها نظرا لاستخدام الوسائل ذات الطابع التقني، و كذا إخفاء معالمها و صعوبة تتبع مرتكبيها ذي الحرفية و الذكاء الخارق إضافة إلى سرعة ارتكابها لاعتمادها على وسائل اتصال حديثة[3].

هذا من جهة و من جهة أخرى، فإنها تهدد الأمن القومي و السيادة الوطنية و إبداع العقل البشري و تشيع فقدان الثقة بالتقنية[4].

---

[1]– المقصود بغسل الأموال بصورتها التقليدية أي لما ترتكب هذه الجريمة باستخدام أساليب تقليدية و التي نعني بها تلك الأساليب الشائعة و المألوفة التي لا تتطلب تدخل آليات أو تقنيات متطورة للوصول إلى الهدف المنشود، بل تعتمد أساسا على الانسان و من بين هذه الأساليب: تهريب و تبادل العملات، استخدام الشركات أو الصفقات الوهمية، استغلال ديون السمسرة و كذا دور القمار و الكازينوهات، شراء الأصول المادية و الوسائل النقدية، لمزيد من التفاصيل ينظر لعشب علي، المرجع السابق، ص 31

[2]– د/ عبد الله عبد الكريم عبد الله، المرجع السابق، الموضع السابق.

[3]– ينظر خصائص جرائم الإنترنت في الفصل التمهيدي من هذه الرسالة.

[4]– ينظر لمزيد من التفاصيل عياد عبد العزيز: تبييض الأموال و القوانين و الاجراءات المتعلقة بالوقاية منها ومكافحتها في الجزائر، الطبعة الأولى، دار الخلدونية، 2007، ص 36

– تستهدف عمليات غسل الأموال عبر الانترنت نقل التحصيلات من الدوائر التابعة لأنشطة القمار والمخدرات و البغاء و تجارة السلاح عبر مصارف و مؤسسات مالية قانونية،و ذلك باستخدام الانترنت[1].

– إن ما يسهل عمليات تبييض أو غسل الأموال عبر الإنترنت، هو أن شروط التعامل على الشبكة الدولية لا تتطلب إجراءات معقدة، إنما فقط تدوين الاسم و رقم بطاقة الائتمان الخاصة بالتعامل،الذي من اليسير جدا – من الناحية التقنية –سرقته عبر الشبكة .

– تحدث هذه الجريمة المرتبكة عبر الانترنت آثار سلبية ضارة في مجال التبادلات المالية و التجارية الإلكترونية، إذ تسببت الأموال الضخمة المسحوبة بطرق غير شرعية خسائر فادحة لاقتصاديات دول كبرى و شركات و مؤسسات عالمية معروفة.

ضف إلى ذلك، فإنه و تبعا لتقارير مجموعة المهام الدولية في مجالات التعاملات المالية، فإن إجمالي الأموال التي يتم غسلها سنويا في مختلف أرجاء العالم تصل إلى حوالي 155 ترليون دولار، أي ما يعادل 55 من إجمال الناتج المحلي في العالم. و هذا ما نتج عنه صعوبة عمل المحققين و رجال القانون في التحليل أو تتبع مصادر غسل الأموال عبر الشبكة الدولية. [2]

– إن جريمة غسل الأموال عن طريق الإنترنت كجريمة منظمة تجد نفسها في عمليات الصيرفة الإلكترونية و التي تمثل المجال الخصب لها، لسرعة ارتكابها و ضعف الوقاية و لسهولة انتقال رؤوس الأموال ما بين الحسابات[3].

و تجدر الإشارة إلى أن ظاهرة غسل الأموال عبر الانترنت برزت مع نهاية القرن العشرين، لتشكل معضلة كبيرة للنظم القانونية المعاصرة. و لعل السبب الرئيسي في استجلاء هذه الظاهرة هي المدفوعات الإفتراضية Cyber-payment[4].

الفرع الثاني: مراحل عملية غسل الأموال عبر الإنترنت

تمر جريمة غسل الأموال عبر الإنترنت أو التبييض الإلكتروني بنفس المراحل التي تمر بها تلك الجريمة في صورتها التقليدية، و هي ثلاث مراحل مرحلة الإحلال (Placement)، و مرحلة التجميع (Empilage)، و مرحلة اللإدماج (Intégration). إلا أن الفرق بينهما يكمن في استخدام الإنترنت في تلك الدورة.

---

[1]– وليد الزيدي، المرجع السابق، ص 63

[2]– وليد الزبدي، المرجع السابق، الموضع السابق.

[3]– و في هذا يقول خبراء إقتصاديون أن البنوك السويسرية يها ما تتراوح بين ترليون و ترليوني دولار من الأموال جاءت من مصادر محرمة.ذكرت تقارير صادرةعن الأمم المتحدة أن سويسرا تحتل مرتبة متقدمة في الدول المستقبلة للأموال المغسولة والتي تصل إلى 750 مليون دولار سنويا.وتتقاسم بقية الكمية كل من لوكسمبورغ و إمارة موناكو و النمسا و جمهورية التشيك و أخيرا إسائيل. ينظر كلا من عبد الفتاح سليمان، المرجع السايق، ص14 وما بعدها. د/أكرم عبد الرزاق المشهداني: 600 مليار دولار سنويا حجم غسل الأموال في العالم، http:// www.alwatan-news.com

[4]– عمر محمد أبو بكر بن يونس و د/يوسف أمين شاكير، المرجع السابق، ص31.

أولا: مرحلة الإحلال (الإيداع أو التوظيف)

تعد هذه المرحلة من أصعب المراحل إذ تكون الأموال فيها غير النظيفة عرضة للاكتشاف.،وعليه يقتضي التخلي عن كمية هذه الأموال غير النظيفة في هذه الأخيرة و التي يكون في صورة قيام غاسل الأموال بمحاولة إدخال الأموال الناتجة عن نشاطه غير مشروع إلى النظام الإلكتروني و ذلك من خلال توظيفها في صورة إيداع بالمؤسسات المالية أو المصارف أو بمحاولة إجراء عمليات بيع و شراء و إلكتروني لأسهم أو لمؤسسة مالية أو تجارية.أي بتحويل تلك الأموال الطائلة التي تكون في صورة أرصدة إلى مشتريات[1].

ثانيا: مرحلة التغطية (التعميم،التمويه، الترقيد)

وفي هذه المرحلة يقوم غاسل الأموال بعمليات معقدة يهدف من ورائها لفصل الأموال المشبوهة عن مصدرها الأصلي،وذلك باخفاء طبيعتها الغير مشروعة وبطمس علاقتها مع مصادرها غير المشروعة من خلال القيام بالعمليات المالية و المصرفية المتتالية عبر الإنترنت. و تعتبرهذه المرحلة من أهم المراحل التي تمر بها جريمة غسل الأموال عبر الإنترنت، و الأصعب بالنسبة للسلطات المكلفة بمكافحة غسل الأموال[2].

و من صورها نقل الأموال بسرعة فائقة من دولة لأخرى لاسيما صوب المرافئ و الملاذات المالية الآمنة، التواطؤ مع المصارف الوطنية و الأجنبية و استخدام بطاقات الدفع الإلكتروني و الحسابات الرقمية المتغيرة، الاستفادة من خدمات نوادي القمار في تغيير العملة وإصدار الشيكات و تحويل الأموال[3].

ثالثا: مرحلة الدمج (التكامل، التجفيف، العصر)

و هي آخر مراحل عملية غسل الأموال بصفة عامة، و هي تهدف لإضفاء طابع الشرعية على الأموال القذرة ذات الأصل الإجرامي، و ذلك بارجاعها مرة أخرى في دورة و في شكل عوائد نظيفة وغير خاضعة للضريبة،لتبدو في النهاية و كأنها عوائد طبيعة لصفقة تجارية. ويتم من خلال هذه المرحلة –في غسل الأموال عبر الإنترنت – دمج الأموال المغسولة في الاقتصاد المتداول عبر الإنترنت و الذي يشكل نسبة كبيرة من التجارة الدولية بحيث يصبح من الصعوبة التمييز بينها و بين الأموال من مصادر مشروعة. [4]

وتجدر الإشارة هنا أنه من الممكن أن تتم كل مرحلة بشكل مستقل عن الأخرى، كما يمكن حصولها مرة واحدة. ولكي يكتب النجاح لعملية الغسل عبر الإنترنت لابد من إخفاء مصدر المال الحقيقي وترتيب عملية الغسل بدقة مع ضرورة تعدد آليات الغسل عبر الإنترنت بحيث تتم تارة عبر عملية بيع عن طريق الإنترنت أو شراء، أو أن يكون هناك تحويل إلكتروني أو أي نشاط تجاري أو مالي عبر الإنترنت[5].

---

[1]– د/ عبد الله عبد الكريم عبد الله، المرجع السابق، ص26

[2]– لعشب علي، المرجع السابق، ص30

[3]– د/ عبد الفتاح بيومي حجازي، (جريمة غسل الأموال بين الوسائط الإليكترونية...) مرجع سابق، ص 47.

[4]– وتسمى هذه المرحلة بمرحلة التجفيف للأموال القذرة و بمرحلة العصر نسبة إلى المرحلة النهائية في عملية غسيل الثياب. ينظر لمزيد من التفاصيل حول هذه المرحلة عبد الفتاح سليمان، المرجع السابق ص141.

[5]– د/عبد الله عبد الكريم عبد الله،المرجع السابق،ص 26.

المطلب الثاني:

طرق ووسائل غسل الأموال عبر الإنترنت و التكييف القانوني لهذه الجريمة

و على غرار المطلب الأول سنبين في هذا المطلب طرق ووسائل غسل الأموال عبر الإنترنت ثم نتطرق إلى المعاجة الجنائية لهذه الجريمة، و ذلك في الفرعين التاليين:

الفرع الأول: طرق ووسائل غسل الأموال عبر الإنترنت.

الفرع الثاني: موقف التشريعات المقارنة من جريمة غسل الأموال عبر الإنترنت.

الفرع الأول:طرق ووسائل غسل الأموال عبر الإنترنت

من أبرز الوسائل التكنولوجية المتقدمة في غسل الأموال عبر الإنترنت:

أولا: الخدمات المصرفية الإلكترونية

شهدت أعمال المصاريف في الآونة الأخيرة تقدما ملحوظا في مجال السماح لعملاء البنوك باجراء العمليات المصرفية من خلال شبكات الاتصال الإليكترونية كاستخدام شبكة الإنترنت في تقديم تلك الخدمات المصرفية.

وتعرف الخدمات المصرفية الإلكترونية أو ما تسمى العمليات المصرفية الإلكترونية بأنها:" قيام البنوك بتقديم الخدمات المصرفية التقليدية أو المبتكرة من خلال شبكات اتصال إلكترونية،و تقتصر صلاحية الدخول إليها على المشاركين فيها وفقا لشروط العضوية التى تحددها البنوك. و ذلك أحد المنافذ على الشبكة كوسيلة لاتصال العملاء"[1].

و تهدف هذه الخدمات إلى خدمة زبائن تلك البنوك و تسهيل تنفيذ العمليات المختلفة، كتحويل الأموال ودفع الالتزامات و الفواتير، و الاستفسار عن الحسابات و أرصدة الشيكات، و شراء الأوراق المالية و فتح أو إغلاق الحسابات.

ومن مزايا هذه الخدمات:

– استخدام تكنولوجيا الانترنت في مجال الخدمات البنكية يخفض من التكاليف الكبيرة التي يتحملها البنك لإجراء عمليات مختلفة تؤكد المعطيات الدولية أن تكلفة إجراء المعاملات المصرفية بواسطة الانترنت تشكل نحو 2% من تكلفتها في حالة الاعتماد على فرع البنك التقليدي و 3.6% في حالة استخدام خدمة التليفون بينما تشكل 8% من تكلفتها في حالة استخدام جهاز الصرف الآلي ATM.

– تقديم خدمات مصرفية جديدة مثل دفع فواتير إليكترونيا بدون رسوم في حين أن البنوك التقليدية يقدم هذه الخدمة مقابل حصولها على رسوم عالية .

– زيادة كفاءة أداء البنوك و تحسين مستوى الخدمة .

---

[1]– د/ عبد الفتاح بيومي حجازي،(جريمة غسل الأموال)مرجع سابق، ص41

– توفير الوقت و الجهد للعميل و كذلك لموظفي البنك فضلا عن توافر الخدمة على مدار 24 ساعة بما فيها أيام العطلة الرسمية.

– إحكام الرقابة على العمليات المصرفية.

– إرسال و استقبال مستندات بسرعة فائقة مما يسهل عمليات التجارة الخارجية.

– زيادة القدرة التنافسية للبنوك و المؤسسات المالية الوطنية مع نظيرتها العالمية، و فتح باب أمام تواجد أكبر للبنوك الوطنية في الأسواق الخارجية .

– تسهيل الحصول على البيانات المالية الخاصة بالعميل ذلك أن العملاء الذين يتعاملون مع بنوك الانترنت يمكنهم استخدام تطبيقات برامج الكمبيوتر الخاصة بإدارة الأموال من خلال حساباتهم على الانترنت في نقل المعلومات المالية الخاصة بهم من حساباتهم الإليكترونية إلى ملفات على الكمبيوتر الخاص بهم. [1]

و لا شك أن المزايا السابقة التي تصاحب تلك الخدمات أو العمليات المصرفية الإليكترونية تغري العاملين في حقل غسل الأموال على تسخير هذه التكنولوجيا في نقل الودائع و التحويلات من حساباتهم إلى حسابات أخرى داخل أو خارج الدولة عن طريق وسائط إليكترونية.

ثانيا: بنوك الانترنت Cyber Banking.

إن دخول الانترنت على الأعمال التجارية، أدى إلى بروز ظاهرة البنوك الاليكترونية و حصول تطور كبير في مجال الأعمال المصرفية حتى انتهى الأمر إلى وجود كامل للبنك على شبكة الانترنت سمي بمصطلحات مختلفة إلا أن جميعهايصب في نفس المعنى كبنوك الانترنت و البنوك الاليكترونية والبنوك الإفتراضية.

ولقد أدى ظهور هذا النوع من البنوك إلى تغيير المفهوم التقليدي للبنك. و كذلك لنوعية و طريقة الخدمات التقليدية التي تقدمها البنوك، بل أنه غير النقود بمفهومها التقليدي الذي نعرفه. و هي تعد من أخطر و أهم الوسائل التكنولوجية الحديثة في غسل الأموال. إذ أنها في الواقع لا تعكس المعنى الفني الشائع و المألوف للبنوك، بل هي عبارة عن وسيط في القيام ببعض العمليات المالية و عمليات البيوع، حيث يقوم المتعامل مع هذا النظام بإدخال الشفرة السرية من أرقام أو خلافه و طباعتها على الكمبيوتر، ومن ثم يستطيع تحويل الأموال بالطريق التي يأمرها بها الجهاز. و هو مجسد في موقع تجاري إداري استشاري شامل له وجود قائم و مستقل على الخطتتميز بأنها رخيصة التكلفة[2].

ومن مخاطر هذا النظام تمكين الجناة في جريمة غسل الأموال القيام بمرحلتي التغطية والدمج ، بطريقة أكثر يسرا و سهولة . فهذه الوسيلة التكنولوجية الحديثة تمكن غاسلو الأموال من تحويل أرصدتهم عدة

---

[1]– د/ عبد الفتاح بيومي حجازي، نفس المرجع ، ص 42–43

[2]– د/ حسين الغافري، محمد الألفي، المرجع السابق، ص132. و من أمثلة هذه البنوك الإفتراضية بنك المسمى "بنت بنك" و عنوانه B@nkwww.netbank.com و لمزيد من التفاصيل حول هذا البنك ينظر د/ عبد الفتاح بيومي حجازي، (جرائم غسل الأموال) مرجع سابق، ص44–45

مرات يوميا في أكثر من بنك حول العالم.و ما يزيد من خطورة هذا الأمر أن البنوك عبر الإنترنت يمكن أن تعمل لفترات طويلة مع الانتقال دوريا خارج الحدود الوطنية و دون أن تتوقف، وذلك من خلال بعض الوسائل الإلكترونية السريعة و بهدف تجنب أي ملاحقة أو انفضاح أمرها[1].

ولقد أشار فريق عمل «F.A.T.F »[2] في تقرير لعام 2001/2000 إلى الإمكانيات الضخمة التي يمكن أن تقدمها بنوك الانترنت لمرتكبي جرائم غسل الأموال، و أشار كذلك إلى أن مواجهة عمليات غسل الأموال التي تتم عبر الانترنت تحتج إلى جهد فائق و كبير وقد يكون من الصعوبة بمكان الوصول إلى نتائج إيجابية شأنه في فترة زمنية قصيرة[3].

ثالثا: أجهزة الصرف الآلي (ATM).

تستخدم أجهزة الصرف الآلي في عمليات إيداع أو سحب الأموال القذرة من الحسابات المصرفية للتخلص من الإجراءات المتعلقة بتعبئة النماذج الخاصة بعمليات الإيداع و الصرف التي تعد أدلة إثبات يمكن الرجوع إليها في حالة الشك في مصدر الأموال. و يجري استعمال الآلات في عمليات غسل الأموال بإجراء العديد من عمليات الإيداع و السحب للأموال المراد غسلها في يوم واحد و من عدة أماكن دون أن تلفت نظر السلطات المختصة واكتشافها.وخصوصا أن استخدام هذه الآلات لا يخضع للالتزامات القانونية المترتبة على عاتق البنوك بخصوص الإبلاغ عن العمليات المصرفية التي تتجاوز مبالغ محددة قانونا للسلطات المختصة . [4]

رابعا:البطاقات الذكية أو ما يسمى بالكارت الذكيSmart card.

وهو أسلوب تكنولوجي في صرف النقود، و هو شبيه بكارت الدين debit card و يقوم بصرف النقود التي كان قد سبق تحميلها من العميل مباشرة إلى القرص المغناطيسي عن طريق ماكنة الصرف الآلي (ATM) أو عن طريق تليفون معد لهذا الغرض[5].

---

[1]– د/ عبد الفتاح بيومي حجازي،نفس المرجع، ص 75.

[2]–FATF : هي منظمة تم تأسيسها من مجموعة السبعة G7 في قمة باريس عام 1989 بقصد إعداد إجراءات مكافحة غسل الأموال و لقد أصدرت هذه المنظمة سنة 1990 40 توصية بشأن مكافحة غسل الأموال و في عام 2001 أضيفت ثماني توصيات تتعلق بالتحويلات الإليكترونية و تمويل الإرهاب. لمزيد من التفاصيل ينظرعبد الفتاح سليمان، المرجع السابق، ص 291

[3]– د/ حسين الغافري، محمد الألفي، المرجع السابق، ص 134.

[4]– د/ حسين الغافري، محمد الألفي، نفس المرجع ، ص 136.

[5]– لمزيد من التفاصيل حول هذه البطاقة ينظر كلا من صبايحي ربيعة: التطور التكنولوجي و جريمة تبييض الأموال، المجلة الجزائرية للعلوم القانونية و الاقتصادية و السياسية، العدد 2009/04، ص 391. و د/ عبد الفتاح بيومي حجازي، (جرائم غسل الأموال) مرجع سابق، ص 78 وما بعدها.

و تعتبر تكنولوجيا الكارت الذكي مكملة لنظام بنوك الانترنت، فضلا عن أنه يتفرد بسمات تميزه عن بطاقات الائتمان، الأمر الذي أغرى غاسلي الأموال باستخدامها و سهل ووفر لهم الأساليب المحكمة للقيام بعملياتهم المشبوهة. و تتلخص بعض هذه السمات في:

تشبه هذه البطاقات الذكية حافظة النقود الحقيقة التي يحملها الشخص و تضم أوراقا نقدية و عملة حقيقة. كما يمكن لحامل البطاقة سحب اعتمادات مالية ورقية إذ يمكنه أن يسحب اعتمادات مالية إليكترونية، وعندما تتم عمليات الشراء فإن ما يدفعه مستعمل البطاقات يخصم من النقود الموجودة قيمتها في البطاقة. فإذا ما قاربت على النفاذ فمن الممكن إعادة شحنها في أي منفذ إليكتروني. ومما لا شك فيه أن هذه الوسيلة سهلة لغسل الأموال إذ يمكن لحامل البطاقة استهلاك قيمة الكارت الذكي في مشتريات باهظة القيمة، ثم يقوم بإعادة شحنها بأموال مودعة لدى مصرفه الإليكتروني، و ذلك بالمال الذي يرغب في تدويره و غسله[1].

ويمكن للبطاقة الذكية أن تؤدي في وقت واحد أدوارا متعددة يمكن للكارت الذكي أن يقوم بدور الشيك، ذلك أن المصارف ليست هي المستفيدة من هذه البطاقات، بل هناك المستهلك الذي يمكنه التعامل بهذه البطاقات بوصفها نقدا أو شيكا. إذ أنها تفي بالوظائف ذاتها التي يقدمها الشيك. و تبرز هذه السمة دور البطاقة الذكية في جريمة غسل الأموال من خلال تحرير شيكات مسحوبة عليها ثم سحب قيمة الشيك من النقود المخزنة فيها و إعادة شحنها مرة أخرى من قبلالمصرف الإليكتروني الخاص بساحبها و ذلك بأموال يرغب صاحبها في غسلها أو تدويرها و يجعلها أموال مشروعة بعد أن كانت متحصلة من مصدر غير مشروع[2]. و يلحق بالبطاقة الذكية حافظة النقود الإليكترونية و هي عبارة عن بطاقة سابقة الدفع، أي تختزن مبلغا من النقود مدفوع مسبقا، و متعدد الاستعمالات. و تستخدم هذه الحوافظ في غسل الأموال عن طريق إيداع المال غير المشروع المطلوب غسله بطريقة تقليدية أو إليكترونية، ثم يقوم المصرف المودع لديه هذه الأموال بطريقة شرعية بإصدار حوافظ نقدية في صورة هواتف تيليفون أو غيرها من صور هذه النقود الاليكترونية بعد إيقافها يتم غسل الأموال أو تدويرها كما أراد الجاني. و مثال ذلك بأن يقوم صاحب الحساب بالتحصيل على بطاقة ممغنطة صالحة الاستعمال في أي دولة من دول العالم وبالتالي يضع ماله غير المشروع بعملة محلية ثم يقوم بمرحلة لاحقة باللجوء إلى الدول التي تتعامل بالعملات الأجنبية ذات الغطاء النقدي كالدولار و اليورو و يسحب أمواله بطريقة إليكترونية منها[3].

---

[1]– د/عبد الفتاح بيومي حجازي، (جرائم غسل الأموال...) مرجع سابق، ص 80.

[2]– د/ عبد الفتاح بيومي حجازي، نفس المرجع ،ص82.

[3]–النقود الإليكترونية (e–cash) أو (Cybercash) هي تلك النقود التي يتم تداولها من خلال أجهزة الحساب الآلي وشبكاته. و هي نتيجة حتمية على ظهور التجارة الاليكترونية – ويؤدي استخدامها إلى سرعة و سهولة تسوية المدفوعات وتقليص الحاجة إلى الاحتفاظ بالنقود السائلة. الأمر الذي يساعد في التبادل التجاري. لمزيد من التفاصيل ينظر شيماء فوزي أحمد: التنظيم القانوني للنقود الإلكترونية، مجلة الرافدين، المجلد 14،العدد 50،السنة 16، كلية الحقوق، جامعة الموصل، ص9 و ما بعدها.

و تجدر الإشارة إلى أن النقود الاليكترونية تعد إحدى أكثر أنظمة النقد و الصرف إغراء لغاسلي الأموال لاستحالة تعقبها و لسريتها و سرعتها، إذ يمكن تحويل أي مبلغ كان من خلالها في فترة وجيزة جدا من الزمن و دونما إعاقات أو حواجز جغرافية أو مصرفية أو قضائية. حيث يجري تمريرها بين أي طرفين على الشبكة و بصورة فورية و مباشرة و دونما الحاجة إلى وسيط مالي كالبنوك. و بالتالي عدم وجود آثار ورقية تدل على وقوع العملية أو تسهيل اقتفاء أثرها[1].

خامسا: الشيكات الاليكترونية.

الشيكات الاليكترونية أو الآلية هي شيكات تصدرها الحسابات الآلية أو الاليكترونية (الكمبيوتر)، تعتمد على الاستغناء عن التوقيع الكتابي عليها من مصدرها، أي الأمر بسحبها و إحلال رقم سري محل هذا التوقيع الذي يقوم مقام التوقيع و بواسطته يمكن التعرف على مصدر الشيك. و قد لجأت المصارف إلى هذا النوع من الشيكات توفيرا للوقت و الجهد الذي يبذل في كتابات الشيكات العادية[2].

و الحقيقة أن علاقة الشيك الاليكتروني بجريمة غسل الأموال هي علاقة وثيقة ومباشرة، فالشيك الاليكتروني يعتمد على وجود حساب عادي للعميل أو محرر الشيك لدى إحدى البنوك ثم يقوم العميل بتحويل هذا الحساب و تداوله عبر شبكة الانترنت في صفقات تجارية يكون طرفا فيها و يكون الشيك الاليكتروني هو وسيلة التداول، و قبل ذلك العميل هو الوسيط بين مصدر الشيك أو محرره و بين المستفيد، و لذلك فمتى كان لدى (أ) من الأشخاص حساب يقدر بمليون دولار لدى أحد البنوك، و كان المال غير مشروع المصدر بأن كان محصلا من تجارة المخدرات أو الاختلاس أو غيرها، و يرغب في غسله عن طريق الشيك الاليكتروني، فما عليه سوى الدخول في معاملات مع (ب) و (جـ) و (د) و غيرهم عن طريق الشبكة، و هذه المعاملات قد تكون بيعا أو إيجارا أو قروضا أو غيرها، المهم أن يخرج (أ) المال غير المشروع من ذمته إلى هؤلاء مقابل عقارات أو منقولات يقو م بشرائها أو استئجارها و غيرها من المعاملات حتى يتم تدوير المال أو غسله كما يرغب (أ)[3].

سادسا: البورصة عبر الانترنت.

تعتبر البورصة المحرك الأساسي لاقتصاديات السوق فهي إحدى أكبر مساحات النزاع الاقتصادي بين المؤسسات و الشركات العالمية، و هي من ناحية أخرى مصدرا ثروة و إفلاس في الوقت نفسه بالنسبة للمتعاملين فيها.

---

[1]– ينظر حسن طاهر داود، المرجع السابق، ص 117 و ما بعدها. د/ ابراهيم الدسوقي أبو الليل: الجوانب القانونية عبر وسائل الاتصال الحديثة، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الإنترنت، كلية الشريعة و القانون، جامعة الإمارات، ماي 2000، ص 36. د/ عصام عبد الفتاح مطر، المرجع السابق، ص 91.

[2]– ابراهمي الدسوقي أبو الليل، (الجوانب القانونية للتعاملات الاليكترونية) مرجع سابق، ص 32.

ينظر المزيد من التفاصيل حول هذه الشيكات ينظر د/ عبد الفتاح بيومي حجازي، (جريمة غسل الأموال....) مرجع سابق، ص82 و ما بعدها.

[3]– د/عبد الفتاح بيومي حجازي، نفس المرجع ، ص 90

و يوجد عدد كبير من المواقع على شبكة الانترنت و التي تشكل بورصات افتراضية يمكن من خلالها شراء و بيع الأسهم و السندات، بالاضافة إلى وجود مواقع على شبكة الانترنت و التي تشكل بورصات افتراضية يمكن من خلالها شراء و بيع الأسهم و السندات، بالإضافة إلى وجود مواقع على شبكة الانترنت للسمسرة في سوق البورصة تساعد المبتدئين على الدخول إلى هذه الأسواق و التعامل معها[1]. و هناك بعض المواقع المتخصصة في تقديم دروس و إرشادات حول الاستثمار في البورصة عبر شبكة الانترنت.

و مما لا شك فيه أن البورصة و سوق الأوراق المالية من الاستثمارات الجاذبة لغاسلي الأموال نظرا لتداول رأس المال بسرعة و بسهولة، سيما لو كان ذلك بوسيلة إليكترونية هي شبكة انترنت حيث يلجأ غاسل المال إلى شراء مجموعة كبيرة من الأسهم و السندات بأموال ذات مصدر غير مشروع أو مضاربة في البورصة على سلعة أو معدن نفيس، ثم يقوم بتحريك السلعة أو المعدن أو الأسهم والسندات و بيعها و إعادة شرائها حتى يتم تدويرها و غسلها و ذلك ممكن و سهل لو استخدمت شبكة الانترنت[2].

سابعا: التجارة الاليكترونية.

أما عن علاقة التجارة الاليكترونية بعملية غسل الأمول فهي علاقة وثيقة، ذلك أن طريق الوفاء أو السداد في معاملات التجارة الاليكترونية، فتحت الأبواب لغاسلي الأموال بتكريس طريق الوفاء أو السداد في هذه المعاملات الاليكترونية لأجل غسل الأموال المشروعة التي لديهم بوسيلة اليكترونية، وبعد ذلك دخولهم في صفقات هذه التجارة الاليكترونية[3].

ومن أخطر الوسائل التي قد يستخدمها الجناة في غسل الأموال عن طريق التجارة الاليكترونية هي عملية فتح الاعتماد المستندي[4] بطريقة اليكترونية و التي يتم فيها تبادل الوثائق و المستندات الاليكترونية من خلال البريد الاليكتروني. بل أن النقود في هذا النظام تنتقل بطريقة اليكترونية من بنك فاتح الاعتماد إلى المستند. و في هذه الحالة يمكن تمويل المصدر الذي يتم فيه سداد بأموال غير مشروعة من قبل فاتح الاعتماد، و الذي يرغب في غسل أمواله المتحصلة من طرق غير مشروعة. كالاتجار في المخدرات مثلا، حيث يقوم بعمل إيداعات مبالغ مالية كبير غير مشروعة لدى البنك الخاص به، و يقوم بفتح الاعتمادات المستندات الاليكترونية لصالح مستفيد أو مستفيدين يدخل معهم في صفقات بيع و شراء و غيرها من صور

---

[1]– ومن المواقع التي تقدم مثل تلك الخدمة: www.shaanb.cm، www.ndb.com

[2]– د/عبد الفتاح بيومي حجازي، (جريمة غسل الأموال...) مرجع سابق، ص 98

[3]– د/ ابراهيم الدسوقي أبو الليل،(الجوانب القانونية عبر وسائل الاتصال الحديثة) مرجع سابق، ص5.

[4]– يقصد بالاعتماد المستندي "تعهد كتابي غير قابل للإلغاء صادر من البنك فاتح الاعتماد بناء على تعليمات طالب الاعتماد لصالح المستفيد بالدفع أو بقبول كمبيالات مستندية مسحوبة عليه من قبل المستفيد، و قد يفوض البنك فاتح الاعتماد بنكا آخر في بلد المستفيد ليتولى الدفع نيابة عنه أو قبول تلك الكمبيالات المستندية و ذلك مقابل مستندات منصوص عليها في الاعتماد المستندي و بشرط أن تكون مطابقة تماما لشروطه و مقدمة خلال مدة صلاحيته.د/حسين الغافري، محمد اللألفي، المرجع السابق، ص143

المعاملات المالية الاليكترونية على نحو يقتضي فتح هذه الاعتمادات التي تتداول فيها عشرات الآلاف أو الملايين من الجنيهات دون إمكانية الكشف عن مصدر هذه الأموال[1].

ثامنا: بطاقات الائتمان.

بطاقات الائتمان هي أداة دفع إلكترونية وسحب حديثة، تستخدم في بيئة إلكترونية أوجدها كثرة استخدام الحاسبات الآلية لا سيما في مجال القطاع المصرفي، أي أنها وسيلة من وسائل الدفع الجديدة. الأمر الذي سهل ويسر لغاسلي الأموال الطريق المنشود لهدفهم، حيث يقوم صاحب المال الملوث باستخدام بطاقته الائتمانية لصرف ماله من أي جهاز صرف آلي في بلد أجنبي ثم يعمد الفرع الذي جرى الصرف من جهازه إلى طلب تحويل المال إليه من فرعه الذي سبق وأصدر بطاقة الائتمان، فيستجيب هذا الفرع تلقائيا ويحول المال ثم يخصم قيمته من حساب عميله الذي يكون بذلك قد تهرب من القيود التي تفرض عادة على التحويلات.كما قد يتم استخدام بطاقات الائتمان لشراء مجوهرات يتم سداد الفاتورة الخاصة بها فيما بعد بالنقد العائد من عملية التجارة في المخدرات أو استخدام تلك البطاقات المسروقة لشراء أشياء ثمينة[2].

تاسعا: نوادي القمار عبر الانترنت.

ومن الطرق والوسائل الجديدة التي تتبعها هذه الظاهرة – والتي بدأت منذ عامين – الاستخدام المتنوع للمواقع الالكترونية التي تخفي أنشطة غسل الأموال كنوادي الانترنت المستخدمة للقمار والنشاطات المصرفية المقترنة بها والتي أصطلح على تسميتها الكازينوهات الإفتراضية.Virtuel Casino الشبيهة بكازينوهات لاس فيجاس الموجودة في العالم المادي.و تشير أصابع الإتهام لدى الجهات الحكومية الأمريكية وكذا الأوروبية إلى أن معظم هذه النوادي والتي تعلن عبر الإنترنت موجودة فيزيائيا في منطقة حوض الكاريبي. وفي هذا الشأن قامت شرطة المباحث الفيدرالية (FBI) بنيويورك بتعقب المواقع التي تقوم بنشاطات تغطي غسل الأموال، مركزة في ذلك على المواقع التي تدار فيها عمليات المقامرة وعلى لاعبيها، وتبين لها أن جل هذه المواقع موجودة في كاركار وجزر الإنتيل وجزيرة أنتيجوا، وجمهورية الدومينيكان. وبعد خمسة أشهر من العمل المكثف والشائك، أصدرت عدة اتهامات وجرى اعتقال العديد من مديري هذه المواقع[3].

وهناك أساليب أخرى تساعد في عمليات غسل الأموال عبر الإنترنت ومنها: [4]

– **نظام فيدواير:** وهو نظام داخلي للمصرف الاحتياطي الاتحادي في أمريكا، إذ يجري غاسل الأموال اتصالا هاتفيا، ويعطي له التعليمات وفق شفرة خاصة به، وتدخل الرسالة في الجهاز الالكتروني لمعالجتها وإرسالها إلى الجهة المستلمة ويتم التحويل للمال عن طريق هذا النظام على أوراق المصرف المذكور.

---

[1]– د/حسين الغافري، محمد اللألفي، نفس المرجع ، ص 142.

[2]– د/ عبد الفتاح بيومي حجازي، (الأحداث والإنترنت) مرجع سابق، ص84

[3] – د/ ممدوح عبد الحميد عبد المطلب: جرائم استخدام الكومبيوتر وشبكة المعلومات العالمية، مكتبة دار الحقوق، الشارقة، 2001، ص70.

[4] – د/ عبد الله عبد الكريم عبد الله، المرجع السابق، ص27 وما بعدها.

– **نظام شيبس:** وهو نظام المدفوعات بين المصارف التابعة لهيئة المقاصة في الولايات المتحدة الأمريكية ويمثل مصارف عملاقة في أمريكا وبلدان أخرى، حيث يتم إرسال الأموال بين البنوك كدائن ومدين عن طريق نظام المقاصة.

– **نظام سويفت Swift:** وهو نظام مقره في بلجيكا لنقل رسائل التحويلات عبر الحدود.

– **شراء المواقع الإلكترونية أو المنتديات على شبكة الإنترنت:** والتي تكون خاسرة أو متعثرة والمعروضة للبيع بغية تمويلها ثم تعويمها.

– **إقدام غاسلي الأموال على إنشاء أو شراء مؤسسات تجارية:** في كل من بلد تحصيلها أو بلد إيداعها بحيث يجري غسلها من خلال شراء وبيع السلع والخدمات بطريقة صورية كشراء سلع من الشركة التي يرغب في تحويل المال إليها. على أن تتم عمليات البيع أو الشراء عبر الإنترنت.

– **المزادات التي تجري عبر الإنترنت**

وتجدر الإشارة إلى أنه يجب الاعتراف بأن غاسلي الأموال عبر الإنترنت يتمتعون بخصائص تميزهم عن غيرهم من المجرمين العاديين تتمثل في الخطورة والذكاء والبراعة وقمة في الحرفية في استخدام التقنية، وهم يتطلعون دوما ويعمدون على ابتكار طرق جديدة لتعجيز السلطات وكذا خداعهم. ومن بين هذه الطرق اللجوء إلى تقنية **موندكس الشهيرة Mondex** [1] – ضمن تقنيات البطاقة الذكية – التي تسهل لغاسلي الأموال إمكانية تحويل أموالهم مع تشفير عملية التحويل عبر جهاز مودم أو عبر الإنترنت. وبالتالي لا يمكن تتبعه أو معرفة مضمون العملية[2].

الفرع الثاني: موقف التشريعات المقارنة من جريمة غسل الأموال عبر الانترنت.

نالت قضية مكافحة غسل الأموال اهتماما كبيرا من دول العالم للحيلولة دون إثراء مرتكبي تلك الجرائم من أعمالهم الإجرامية. وتعد جريمة غسل الأموال من الجرائم الإقتصادية المستحدثة ومن المشاكل العالمية التي تواجه الدول[3] والتي ساعد على تقدمها وتناميها ما أفرزته التكنولوجيا الحديثة من أدوات وآليات فرضت العديد من القيود والصعوبات على اكتشاف تلك الجرائم أو الوصول إلى مرتكبيها و تعقبهم، فضلا عن تسارع وتعقد ظاهرة العولمة الاقتصادية.ولهذا قامت العديد من الدول (سواء العربية أو الأجنبية) بوضع قوانين لمكافحتها وردع مرتكبيها وذلك إما بتعديل نصوصها لتستوعب تجريم تلك الجريمة الجديدة أو بسن تشريعات أو نصوص خاصة وجديدة تجرمها.و سيتم تبيان موقف هذه التشريعات المقارنة بتقسيم هذا الفرع إلى موقفين نتعرض في الأول منهما موقف التشريعات المقارنة الغربية منها و العربية من هذه الجريمة. وذلك كما يلي:

---

[1]– تقنية موندكس وهي بطاقة ذات القيمة المخزنة يمكن شحنها مجددا عبر وضعها في فتحة معينة بالصرف الآلي. د/ عبد الفتاح بيومي حجازي،(جريمة غسل الأموال:...)، مرجع سابق، ص 38.

[2]– د/ عبد الفتاح بيومي حجازي، (الأحداث والإنترنت)، مرجع سابق، ص89.

[3]– لمزيد من التفاصيل ينظر د/ زياد علي عربية: غسل الأموال، أثاره الاقتصادية والاجتماعية ومكافحتها دوليا وعربيا، مجلة الأمن والقانون، العدد (1) السنة 12، يناير 2004، ص 96 وما بعدها.

أولا: موقف التشريعات الغربية من جريمة غسل الأموال عبر الانترنت .

و سنبين موقف هذه التشريعات حيال هذه الجريمة من خلال تقسيمها إلى موقفين الأول نخصصه لموقف التشريع الفرنسي و الثاني نتطرق فيه إلى توضيح موقف التشريع الأمريكي من هذه الجريمة المستحدثة. وذلك كمايلي:

1/ موقف التشريع الفرنسي من جريمة غسل الأموال عبر الانترنت.

عالج المشرع الفرنسي جريمة غسل الأموال من خلال عدة قوانين[1] آخرها قانون 96-392 المؤرخ في 13 ماي 1996، و المتعلق بمكافحة تبييض الأموال و المتاجرة في المخدرات و المعدل و التمم لقانون العقوبات الفرنسي، و الذي عرف المشرع الفرنسي من خلاله غسل الأموال و ذلك في المادة 324- 1 من قانون العقوبات الفرنسي بأنه "تسهيل التبرير الكاذب بأي وسيلة كانت بمصدر أموال أو دخول لمرتكب جناية أو جنحة تحصل منها على فائدة مباشرة أو غير مباشرة أو تقديم المساعدة في عمليات ايداع أو إخفاء أو تحويل العائد المباشر لجنحة أو جناية ".[2] كما تضمن النص على العقوبة المقررة لهذه الجريمة و التي هي السجن لمدة خمس سنوات (في الحالة البسيطة) و الغرامة المالية التي تقدر ب 375000 يورو.

و بعشرة سنوات اذا كانت مرتكبة بطريق الإعتياد أو باستعمال التسهيلات التي تمنحها له ممارسة نشاط مهني أو في إيطار جماعة منظمة، و بغرامة مالية قدرها 750000 يورو(الحالة المشددة).[3]

2/ موقف التشريع الأمريكي من جريمة غسل الأموال عبر الانترنت

تعتبر الولايات المتحدة الأمريكية الدولة الرائدة في مجال إصدار تشريعات لمكافحة غسل الأموال. اذ صدر في سنة 1970 قانون يعرف بقانون سرية االحسابات. و في سنة 1986 قانون الرقابة و السيطرة على غسل الأموال و تلته قوانين أخرى تنظم هذه الآفة الإقتصادية إلى حين صدور قانون قمع غسل الأموال لسنة 1994. أما فيما يتعلق بجريمة غسل الأموال عبر الانترنت فقد قام المشرع الفدرالي بتعديل قانون سرقة أعمال المصارف لسنة 1970 ليضاف إلى

---

[1]- لمزيد من التفاصيل ينظر لعشب علي، المرجع السابق، ص 62 و ما بعدها.

[2] -Art 324-1 :" Le blanchiment est le fait de faciliter، par tout moyen، la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect.
Constitue également un blanchiment le fait d'apporter un concours à une opération de placement، de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit.
Le blanchiment est puni de cinq ans d'emprisonnement et de 375000 euros d'amende".

[3] -Art 324-2 :" Le blanchiment est puni de dix ans d'emprisonnement et de 750000 euros d'amende :
1° Lorsqu'il est commis de façon habituelle ou en utilisant les facilités que procure l'exercice d'une activité professionnelle ;
2° Lorsqu'il est commis en bande organisée".

التقنين الأمريكي باسم قانون مراقبة غسل الأموال لسنة 1986 والذي ميز فيه المشرع الأمريكي بين العمليات المالية التي تتم عبر الإنترنت وتلك التي تتم في العالم المادي وذلك بمقتضى القانون Electronic Fund Transfer Act. [1]

ثانيا: موقف التشريعات العربية من جريمة غسل الأموال عبر الانترنت

شاركت الدول العربية بفاعلية الجهود الدولية لمكافحة عمليات غسل الأموال حيث أصدرت معظم الدول العربية تشريعات وطنية لمكافحة عمليات هذه الظاهرة، كما تم تأسيس مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال إفريقيا (مينا فاتف) لمكافحة هذه الظاهرة بالدول العربية، بالإضافة إلى عقد المؤتمرات والتوصل إلى الاتفاقيات التي تسهم في دعم سبل التعاون الأمني والمالي في مجال مكافحة غسل الأموال و منها الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 1/16[2]. و على هذا سنبين أولا موقف التشريعات العربية بصفة عامة من جريمة غسل الأموال عبر الانترنت، لنعرض بعد ذلك موقف التشريع الجزائري من هذه الجريمة. و ذلك كمايلي:

1/ موقف التشريعات العربية بصفة عامة من جريمة غسل الأموال عبر الانترنت.

تعتبر جريمة غسل الأموال من الجرائم الإقتصادية، و هي ترتبط في الغالب بالجريمة المنظمة كجرائم المخدرات و الإرهاب و تهريب السلاح. و لقد انقسمت التشريعات العربية في تحديد موقفها من جريمة غسل الأموال عبر الانترنت إلى قسمين. **قسم اكتفى بتطبيق نصوص قوانينه العقابية التقليدية**، كما هو الشأن في **مصر** مثلا اذ تم فيها تشريع قانون جديد سمى "بقانون مكافحة غسل الأموال رقم 80 لسنة 2002" يجرم جريمة غسل الأموال ويعاقب عليها بأشد العقوبات نظرا لما تسببه من سمعة سيئة للبلاد وتفويض الاقتصاد الوطني المصري[3]. و قسم آخر فضل مواجهة هذه الجريمة الاقتصادية الخطيرة والأخطر لارتكابها عبر الانترنت باستحداث نصوص خاصة تجرمها و تعاقب عليها. **ومن الدول التي استحدثت تشريعاتها** نصوصا

---

[1]– لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة....)، مرجع سابق، ص 665.وذات الشأن بالنسبة للقانون الكندي الذي انتبه فيه مشرعه إلى عملية غسل الأموال عبر الإنترنت مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال. و لمزيد من التفاصيل حول مكافحة جريمة غسل الأموال في الدول الغربية ينظر.

Jacqueline RIFFAULT: Le blanchiment de capitaux en droit comparé,RSC ، n°2 Avril – Juin 1999 ،p 233 – 249.

[2]–تنص المادة 1/16 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على:" الجرائم المتعلقة بالجرائم المنظمة و المرتكبة بواسطة تقنية المعلومات:

1– القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال."

[3]– لمزيد من التفاصيل ينظر: وليد حجاج إسماعيل، المرجع السابق ص 6 وما بعدها، و كذاعبد الفتاح سليمان: مكافحة غسل الأموال،الطبعة الأولى، ص 55 و ما بعدها.

لمواجهة و منها **الإمارات العربية المتحدة** فلقد جرم المشرع الإماراتي تلك الظاهرة في صورتها المستحدثة وذلك في القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات إضافة إلى قانون غسل الأموال الصادر عام 2002 وذلك في المادة 19 منه.[1]

2/ موقف التشريع الجزائري جريمة غسل الأموال عبر الانترنت

أما بالنسبة للجزائر فقد صادقت كنظيرتها من القوانين العربية على كل الاتفاقيات المتعلقة بمكافحة ظاهرة غسل الأموال.[2] كما قام المشرع الجزائري بإصدار عدة نصوص قانونية[3] لها علاقة بمراقبة و مكافحة غسل الأموال ومنها:

– المرسوم التنفيذي رقم 02–127 المؤرخ في 2002/04/07 يتضمن إنشاء خلية معالجة الاستعلامات وتنظيمها وعملها.

---

[1]– تنص المادة 19 من القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على: "يعاقب بالحبس مدة لا تزيد على سبع سنوات وبالغرامة التي لا تقل عن ثلاثين ألف درهم ولا تزيد على مئتي ألف درهم، كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير المشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعا لارتكاب أي من هذه الأفعال".

[2]– تعد الجزائر من بين الدول السباقة إلى المصادقة على الاتفاقيات الدولية المتعلقة بالجريمة المنظمة التي ليس لها حدود جغرافية أو اتجاهات إيديولوجية أو عقائدية. و لقد صادقت الجزائر على ثلاث اتفاقياتدولية ذات الصلة بالجريمة المنظمة وهي:

اتفاقية فيينا لسنة1988 الخاصة بمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية وذلك بموجب المرسوم الرئاسي رقم 95– 45 المؤرخ في 1995/01/28.

اتفاقية قمع تمويل الإرهاب لسنة 1995 وذلك بموجب مرسوم رئاسي رقم 2000– 445 المؤرخ في 2002/12/23.

اتفاقية الجريمة المنظمة عبر الوطنية لسنة 2000 بموجب مرسوم رئاسي رقم 02–55 المؤرخ في 2002/02/25. ينظر لعشب علي، المرجع السابق، ص 67.

[3]– الأمر رقم 96–22 المؤرخ في 1996/07/09 المتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال من و إلى الخارج. الأمر 77–03 المؤرخ في 19 مارس 1977 المتعلق بمنع الجمع غير الشرعي للأموال. الأمر 11/03 المؤرخ في 2003/08/26 المتعلق بالنقد والقرض و الذي ألزم المشرع في المادة 8 منه مجلس النقد و القرض بضرورة اجراء تحقيق حول مصدر أموال الشخص المترشح لإنشاء بنك. و في هذا الاطار لا يجوز منح الاعتماد لهذا المترشح اذا ارتكب جرائم متصلة بتجارة المخدرات أو تبييض الأموال. كما ألزمت المادة 9 من نفس القانون هذا الشخص بتبرير مصدر المال.و تجدر الاشارة هنا إلى أن هذه النصوص لاتستوعب في حقيقة الأمر نشاط غسل الأموال بل يمكن أن تصنف بأنها من جرائم الكسب غير المشروع أو مخالفة لتنظيم حركة رؤوس الأموال أو جرائم مالية أخرى مشابهة. لمزيد من التفاصيل ينظر عجة الجيلالي: الاصلاحات المصرفية في القانون الجزائري في ايطار التسيير الصارم لشؤون النقد والمال، مجلة اقتصاديات شمال افريقيا،العدد 4،جامعة الشلف، ص 25. صالحي نجاة: الآليات الدولية لمكافحة تبييض الأموال و تكريسها في التشريع الجنائي الجزائري، مذكرة مكملة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، السنة الجامعية 2010–2011، ص 103.

– القانون رقم 11/02 المؤرخ في 2002/12/24 المتضمن قانون المالية لسنة 2003.

– القانون رقم 01/05 المؤرخ في 2005/02/06 المتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحتها والذي ألغى أحكام المواد 104 إلى 110 من قانون 02-11-127 المتعلق بقانون المالية لسنة 2003[1].

– القانون رقم 01/06 المؤرخ في 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته.

– القانون رقم 06-22 المؤرخ في 2006/12/20 المعدل والمتمم لأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية.

– القانون رقم 06-23 المؤرخ في 2006/12/20 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات. و يقصد بجريمة تبييض الأموال في كل من قانون العقوبات الجزائري و القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها: "اخفاء المصدر الاجرامي للممتلكات لا سيما المال القذر". وباستقرائنا لنص المادتين389 مكرر[2] من قانون العقوبات الجزائري والمادة 2 من القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها نستخلص أن لهذه الجريمة أركان. فأما الركن المادي فيتمثل في أربعة صور وردت على سبيل الحصر وهي:

أ- تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته.

ب- إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها مع العلم بأنها من عائدات إجرامية .

ج- اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها بأنها تشكل عائدات إجرامية.

---

[1]- لمزيد من التفاصيل حول هذه النصوص القانونية ينظر عياد عبد العزيز، المرجع السابق، ص 35 و ما بعدها.

[2]- تنص المادة 389 مكرر من قانون العقوبات و المادة 2 من القانون رقم 05-05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها على:" يعتبر تبييضا للأموال:

أ- تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته.

ب- إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها مع العلم بأنها من عائدات إجرامية

ج- اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها بأنها تشكل عائدات إجرامية.

د- المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة أو التواطؤ أو تآمر على ارتكابها و محاولة ارتكابها و المساعدة

و التحريض على ذلك و تسهيله و إسداء المشورة بشأنه".

د- المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة أو التواطؤ أو تآمر على ارتكابها و محاولة ارتكابها و المساعدة و التحريض على ذلك و تسهيله و إسداء المشورة بشأنه .

و أما فيما يخص الركن المعنوي فالمشرع الجزائري يكيف هذه الجريمة ضمن الجرائم العمدية الذي يقتضي فيها توافر القصد الجنائي للجاني. أي يشترط أن يكون الجاني على علم من أن الممتلكات محل سلوكه هي عائدة من جريمة .

و أما فيما يخص الركن الشرعي، فالمشرع الجزائري ميز من حيث العقوبة بين التبييض البسيط و التبييض المشدد. فأما بالنسبة للنوع الأول فيقرر له عقوبة الحبس من 5 سنوات إلى 10 سنوات و بغرامة 1000000 دج إلى 3000000 دج[1]. أما النوع الثاني فيقرر له عقوبة الحبس من 10سنوات إلى 15 سنوات و بغرامة 4000000 دج إلى 8000000 دج.[2]

و تعاقب المادة 389 مكرر3 من قانون العقوبات على محاولة ارتكاب الجريمة بالعقوبات المقررة للجريمة التامة. هذا فيما يخص العقوبات الصلية الموقعة على الشخص الطبيعي. أما العقوبات التكميلية الموقعة عليه فتتمثل في الحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 9 من قانون العقوبات،[3] مصادرة الأملاك محل الجريمة و الوسائل و المعدات المستعملة في ارتكاب جريمة تبييض الأموال.[4]

كما قرر المشرع الجزائري عقوبات للشخص المعنوي و ذلك في المادة 389 مكرر 7 عقوبات و هي الغرامة التي لا تقل عن أربع مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، مصادرة الممتلكات و العائدات التي استعملت في ارتكاب الجريمة، المنع من مزاولة نشاط مهني أو اجتماعي لمدة 5 سنوات، حل الشخص المعنوي.

و عليه نستخلص مما تقدم أن المشرع الجزائري لم ينص على جريمة غسل الأموال عبر الانترنت و اكتفى بتجريم هذه الجريمة التي تتم بطرق تقليدية.

---

[1]- ينظر المادة 389 مكرر 1 من قانون العقوبات الجزائري.

[2]- ينظر المادة 389 مكرر 2 من قانون العقوبات الجزائري. و تعتبر من الظروف المشددة للعقوبة:الاعتياد، استعمال التسهيلات التي يوفرها نشاط مهني، ارتكاب الجريمة في اطار جماعة إجرامية.

[3]- ينظر المادة 389 مكرر 6 من قانون العقوبات الجزائري.

[4]- ينظر المادة 389 مكرر 4 من قانون العقوبات الجزائري و المادة 389 مكرر 5 من ذات القانون.

المبحث الثاني:

جريمة المخدرات عبر الإنترنت

تعتبر المخدرات[1] من المواد السامة، وإن كان قليلا منها قد يكون فيه علاج وشفاء للناس إلا أن الإدمان على تناولها فيه خطر وضرر لمن يتعاطها سواء على شخص المدمن أو عائلته وأسرته. وبهذا لم يكن أمام المشرع إلا الحد من قاعدة أن الإنسان حر يتصرف في نفسه كما يرغب، فأجمعت غالبية التشريعات على

---

[1]– يصعب وضع تعريف جامع مانع للمواد المخدرة خصوصا بعد أن اتسع مدلولها بسبب التقدم الهائل في العلوم الكيميائية ليشمل المواد النفسية أو تلك التي تؤثر في النشاط العقلي أو التي تسبب الهلوسة والأوهام أو هي كل العقاقير المستخلصة من النباتات أو المركبات الكيميائية و التي تغير من حالة الإنسان المزاجية، و مع تكرار تناولها تخلق نوعا من التسمم في جسمه و يصبح مدمنا عليها عاجزا عن التخلي عنها. وهي تقسم بالنظر إلى أصلها إلى ثلاثة أنواع: المخدرات الطبيعية وهي عبارة عن نباتات تحتوي أوراقها و أزهارها و ثمارها أو أية أجزاء منها على مادة فعالة لها تأثير على الجهاز العصبي مثل نبات القنب (الحشيش) ونبات الخشخاش والكوكا والقات....

المخدرات المصنعة وهي التي تصنع من نتاج المخدرات الطبيعية مثل المورفين والهيروين.

المخدرات التخليقية: وهي التي يتم تخلفها ابتداء من المعامل من تركيبات كيميائية، ومنها العقاقير المهبطة و المنومة (الاربتيورات) مثل أموباربيتال Amobarbital وسيكوباربيتال Secobarbital

وجلوتثميدGlutethmidوميثاكوالونMethaqualone و كذلك العقاقير المنشطة أو المنبهة (الأمفيتامينات) مثل الامفيتامينAmphetamine و ديكساميفيتامينDexamphetamine و ميثامفيتامينMethamphetamine و كذلك عقاقير الهلوسة مثل (LSD) و المسكالينMescaline و غيرها. سيدهم مختار: المخدرات و المؤثرات العقلية، مجلة المحكمة العليا، العدد2، السنة 2010، ص 29 و لمزيد من التفاصيل عن تصنيفات أخرى من المخدرات، ينظر د/إدوار غالي الذهبي: جرائم المخدرات، الطبعة الثانية، مكتبة غريب، القاهرة، 1988، ص 22 و23.

Les différents types de drogues:

Le cannabis (herbe ،résine ،huile)

La cocaïne (poudre)

Le crack (mélange de cocaïne ،bicarbonate de soude et ammoniaque)

L'opium (plante ressemblant au coquelicot)

La morphine (extraite de l'opium)

Les substances psychotropes (des centaines de variétés)

Dépresseurs – Hallucinogènes

Stimulants – Inhalants

Les drogues locales.

Les colles

Les solvant (éther ،acétone ،trichloréthylène)

Les carburants (essence à moteur)

Les gaz (propulseurs des bombes aérosols)

Aissa KASMI: situation actuelle du phénomène de la drogue en Algérie, séminaire national d'information et de sensibilisation sur les dangers de la drogue, office National de lutte contre la drogue et la Toxicomanie, Ministère de la justice, Tlemcen: 20-21 Novembre 2006, p6.

مكافحة الإدمان على المخدرات بتوقيع العقوبة على من يتعاطاها ويتاجر بها وقد يودع المدمن في مصحات علاجية للعلاج من عادة الإدمان.

وتجدر الإشارة إلى أن تجارة المخدرات تعد من أهم وأخطر أنواع التجارة المحرمة عالميا، ولم تفلح كافة الجهود المبذولة على منعها نهائيا،بل اقتصرت تلك الأخيرة على تقليلها نظرا لوجود بعض البلدان المصنعة و المهربة لتلك المخدرات إلى باقي دول العالم.ولما تدره تلك التجارة على العاملين فيها من ربح وفير. وقد كان تجار المخدرات يلاقون صعوبات كثيرة في الاتفاق على عمليات التهريب. إلا أنه وبعد التطور التكنولوجي الكبير الذي شهده عالمنا والمتمثل في انتشار وغزو شبكة الإنترنت، فقد استغل مصنعي ومهربي المخدرات الشبكة واستخدموها كوسيلة مسهلة في الاتفاق على عمليات تهريب المخدرات من بلد إلى أخر. إذ برزت مواقع أشد خطورة تبث صورا زائفة للمخدرات والمؤثرات العقلية تنقل متعاطيها إلى جنة الأحلام. فأصبحت بذلك الشبكة مسرحا حيويا وملائما لتعاطي تلك المواد السامة وترويجها، وتحولت إلى قناة اتصالية ممتازة ومجالا رحبا لإدخال المخدرات والمؤثرات العقلية في نطاق العالم الإفتراضي، لدرجة سهل وأمن التعامل غير المشروع لمستهلكيها (سواء المروج أوالمدمن عليها).

وهذا ما أثبته تقرير لجنة البلدان الأمريكية، حيث أشير فيه إلى أن نصف الكرة الأرضية لعامي 1999-2000 أصبحت تستخدم الإنترنت في زيادة إنتاج المخدرات المصنعة واتساع رقعته، وأن الجماعات الإجرامية المنظمة توظف العولمة والاتصالات الفورية والتحويلات المالية الالكترونية في تحسين كفاءة أنشطة الاتجار بالمخدرات[1]. و نتيجة لهذا برزت مصطلحات مستحدثة في هذا المجال كتكنلجة المخدرات (Drug'sTechnecality) [2] وسيبر دروق(cyber drugs) وجريمة تكنلجة المخدرات والمؤثرات العقلية.[3] والإشكال المطروح هنا: هو هل يساعد الإنترنت في انتشار المخدرات إنتاجا أو تهريبا أو ترويجا أو تعاطيا؟ وكيف استطاع سادة العالم السفلي استغلال المجتمع الجديد؟ وماذا نعني بجريمة تكنلجة المخدرات والمؤثرات العقلية؟ وهل تخضع هذه الجريمة للعقوبات المنصوص عليها في القوانين التقليدية؟.

و سيتم الاجابة على مجموع هذه الاشكالات وفق المطلبين التاليين:

المطلب الأول: تعريف جريمة تكنلجة المخدرات وطرق نشرها عبرها.

المطلب الثاني: المعالجة القانونية لجريمة تكنلجة المخدرات.

---

[1]- د/ محمد فتحي عيد: الإنترنت ودوره في انتشار المخدرات الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 7.

[2]- د/ عمر محمد بن يونس: المخدرات والمؤثرات العقلية عبر الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2003، ص15.

[3]- يقصد بالمؤثرات العقلية هي كل مادة طبيعية أو اصطناعية أو كل منتوج طبيعي مدرج في الجداول 1-2-3-4 من إتفلقية المؤثرات العقلية لعام 1971 و هي تؤثر على العقل كالأمفيتاميتات و الباربيتورات و عقاقير الهلوسة. المهبطة أو النومة (الباربتيورات) مثل أموباربيتال.ينظر سيدهم مختار، المرجع السابق، ص 29.

المطلب الأول:

تعريف جريمة تكنلجة المخدرات وطرق نشرها عبر الإنترنت.

و سنحدد في هذا المطلب ما المقصود من "جريمة تكنلجة المخدرات عبر الانترنت" في الفرع الأول، ثم نتطرق إلى الطرق التي تنتشر بها عبر هذه الشبكة في الفرع الثاني. و ذلك كمايلي:

الفرع الأول:تعريف جريمة تكنلجة المخدرات.

الفرع الثاني: طرق نشر ثقافة المخدرات و المؤثرات العقلية عبر الانترنت.

الفرع الأول: تعريف جريمة تكنلجة المخدرات

لا يمكن لأحد إنكار مدى خطورة انتشار الجوانب السلبية للمخدرات والمؤثرات العقلية في أوساط مجتمعاتنا، لا سيما وأنها تمثل أعتى مظاهر الجريمة المنظمة. ولقد ازداد هذا الأمر خطورة لما برزت الإنترنت واستخدمت كوسيلة لتوسيع دوائر الطلب على تلك المواد السامة والخطيرة، حتى أصبحت خريطة حركة عرض المخدرات والمؤثرات العقلية محليا وإقليميا وعالميا لا يكتب لها النجاح ما لم تأخذ في الحسبان العالم الإفتراضي. وبذلك برز نوع مستحدث من إجرام الانترنت يعرف "بإجرام تكنلجة المخدرات والمؤثرات العقلية" والذي هو:"عبارة عن تعبير يشمل اجتماع التعامل بالمخدرات والمؤثرات العقلية بتكنولوجيا المعلومات/ الإنترنت وذلك باستخدام وسائلها"[1]. أو هي: "استخدام الإنترنت لتسهيل التعامل بالمخدرات والمؤثرات العقلية (نشر + الاتجار+ الترويج + التعاطي)".

وتتنوع جرائم تكنلجة المخدرات والمؤثرات العقلية، شأنها شأن مثيلتها التقليدية وتتراوح بين الاتجار أو الحيازة أو التعاطي أو الاحراز أو الوساطة.إذ تستخدم الإنترنت في تسهيل التعامل غير المشروع بالمؤثرات العقلية والمخدرات، فهي تستعمل في الاتجار غير المشروع لتلك المواد السامة وفي الترويج لها والتوزيع أيضا. وتقوم بفتح أسواق جديدة، وتساهم على التعرف على مستهلكين جدد.هذا وتقوم منظمات غير مشروعة في العديد من الدول في أيامنا هذه باستخدام الإنترنت للترويج غير المشروع محليا وإقليميا وعالميا للمخدرات والمؤثرات العقلية. بل أكثر من ذلك فإن هناك مواقع ذات خطورة بالغة تمنحها الإنترنت تتخصص في التدريب على زراعة المخدرات وكذا تبين طرائق وعمليات تحويلها خطوة بخطوة، وكذلك كيفية التعاطي لأول مرة والجرعات والمدة بين الجرعة والأخرى.

هذا من جهة ومن جهة أخرى، أدى الاستعمال السيئ للإنترنت إلى خلق أو ظهور أنواع جديدة من المخدرات والمؤثرات العقلية وعلى شرح طرق الحصول على تراخيص إنتاجها باستخدام التكنولوجيا، كما لو استخدم الحاسوب في تأهيل نظم الإنتاج واختيارات البدائل المختلفة في تصنيفها أو زراعتها.

---

[1]– د/ عمر محمد بن يونس،(المخدرات والمؤثرات العقلية عبر الإنترنت) مرجع سابق، ص17.

ولقد سجلت الإحصائيات أن أكثر الدول التي بها حركة اتجار في المخدرات والمؤثرات العقلية عبر الانترنت في عام 2000 هي كل من هولندا وسويسرا [1].

وتجدر الإشارة إلى أن علة التجريم هذا النوع من الجرائم بصفة عامة(سواء التقليدية أو التي تستخدم فيها تكنولوجيا المعلومات) تختلف من دولة لأخرى، فهناك من يعتبرها خطرا عاما يهدد كيان المجتمع ويمس مصالحه[2]، وهناك من يصنفها ضمن جرائم الإرهاب، وآخرون يساوونها بأسلحة الدمار الشامل[3].

الفرع الثاني: طرق نشر ثقافة المخدرات والمؤثرات العقلية عبر الإنترنت

تتنوع الأساليب والطرق المستخدمة في نشر ثقافة المخدرات والمؤثرات العقلية عبر الإنترنت وذلك كما يلي:

أولا:الترويج غير المشروع عبر الانترنت للمخدرات والمؤثرات العقلية:

ويقصد به إغواء الناس وإغرائهم وتحريضهم معنويا للوصول إلى إقناعهم بها وبجدواها وجدوى التعاطي، ومن ثم فتح الطريق إلى الإدمان عليها والاعتماد عليها. ويكون ذلك عن طريق الترويج للعرض أي بقيام أيا كان بالتعرف على كيفية زراعتها وتنميتها وتطويرها وتخليقها معمليا أو إعدادها للتعاطي وكيفية تعاطيها والمدة اللازمة بين الجرعة والأخرى. ولا أهمية في ذلك لطريقة الترويج فقد تكون على الصفحة أو الموقع عبر الإنترنت بتقديم شروحات وافية ومباشرة، وقد تكون ملفات مضغوطة يتم إنزالها في الحاسوب المتصل بالشبكات وبالتالي الإطلاع عليها في أي وقت.والترويج لهذه المواد السامة عبر الإنترنت قد يقوم به شخص واحد كاستخدامه الصفحات المجانية عبر شبكة المعلومات الدولية. أو أن يتولى إقناع الغير بمسألة العرض أو الطلب عبر غرف المحادثات أو حلقات النقاش أو باستخدام نظام حثالة البريد الإلكتروني (spam). كما قد يقوم به عدة أشخاص وذلك عن طريق البث عبر الإنترنت من طرف أشخاص يتصفون بصفات معينة. كأن يكون الشخص معد الصفحات[4] أو معد البرمجية[5] أو وسيط الكتروني[6].

---

[1]– ينظر هذه الإحصائيات على موقع: www.lawmg.co.sehttp://

[2]– كالقانون الليبي القديم(قبل عام 1994)

[3]– كالقانون الليبي المعاصر(يعد 1994) حيث استند في مقوماته إلى الإعلان الليبي لمكافحة المخدرات والمؤثرات العقلية الذي يقرر بان المخدرات والمؤثرات العقلية من أسلحة الدمار الشامل وتجدر إلى ان اعتبارها نوعا من تلك الأسلحة سوف يساعد كثيرا في مواجهة تكنلجة جرائم المخدرات والمؤثرات العقلية لتأخذ حظها من المواجهة الدولية، فمثلا إن وضعية المصلحة المحمية على هذا النحو تسمح بتقرير التجريم والعقاب حتى في تلك الدول التي تسمح بقدر من التعاطي والحيازة والإحراز لمزيد من التفاصيل ينظر د/ محمد بن يونس، (المخدرات...) مرجع سابق، ص49.

Aissa KASMI ,opcit,p9.

[4]– يقصد بمعد الصفحات وهو الشخص الذي يتولى إعداد الصفحات لتتخذ شكلها الذي يبرز عند استخدام متصفحات شبكة الإنترنت فيضع في الصفحات البيانات اللازمة بها والتي تحقق القيمة الاسترادادية للمعلومات المطلوبة في شكل كلمات وجمل و اعلانات وأيقونات.

[5]– يقصد بمعد برمجيات الترويج: هو كل شخص ساهم في إعداد وتطوير البرمجية تقنيا وهو يضم كل من المبرمج والمطور أو المؤهل لها، ولا يشترط في ذلك الاخير ان يكون مؤهلا لإعداد البرمجيات د/ عمر محمد بن يونس،(المخدرات..) مرجع سابق، ص66

[6]– يقصد بالوسيط الإلكتروني هو وفقا للمشروع الليبي في مادته(1/5) كل شخص طبيعي او إعتباري يملك الوسائل اللازمة للتعامل كحلقة وصل او كشبكة بقصد تقديم خدمات تكنولوجيا المعلومات/الإنترنت د/ عمر محمد بن يونس، نفس المرجع،ص67

ثانيا:الاتجار غير المشروع عبر الإنترنت للمخدرات والمؤثرات العقلية:

المقصود بالاتجار في المخدر تقديمه للغير بمقابل أو احتراف الفاعل التعامل فيه واتخاذه نشاطا معتادا مستمرا له. وهنا سنتطرق إلى الاتجار غير المشروع للمخدرات والمؤثرات العقلية بنظام البريد الإلكتروني ثم الاتجار الإلكتروني غير المشروع لتلك المواد.

1/ الاتجار بنظام البريد الإلكتروني

يحقق البريد الإلكتروني انتشارا ترويجيا للمادة المخدرة وعرضا مستمرا لحركة التوزيع، إذ يعد وسيلة للتعرف على الطلب على المخدرات والمؤثرات العقلية. أو بصيغة أخرى هو وسيلة لمعرفة المستهلك النهائي وهو المصاب بالاعتمادية أي الضحية.

2/ الاتجار الإلكتروني غير المشروع للمخدرات والمؤثرات العقلية

ونعني به استخدام التجارة الإلكترونية بقصد الاتجار غير المشروع بالمخدرات والمؤثرات العقلية. والاتجار المجرم هنا يشمل علاقات العرض الذي تقام خارج إطار الطلب، فعلى سبيل المثال يمكن أن يكون العرض مؤسسا على تبادل المخدرات والمؤثرات العقلية بواسطة أرقام بطاقات الاعتماد المصرفية carte de crédit عبر الانترنت. كما يمكن ان تمتد حركة الاتجار الالكتروني غير المشروع لتلك المواد السامة إلى بيع التقنية ذاتها كبيع موقع الكتروني متطور ومشهور بكثرة الطلب أو الالتزام بدفع مقابل مادي حال الاشتراك في غرف المناقشة التي يتم من خلالها التعامل غير المشروع بتلك المواد الخطيرة، او القيام بإعداد تقنية خاصة لمحركات البحث مهمتها المساعدة في الانتقال والبحث على مواقع العرض الخاصة بطوائف أو أنواع معينة ومخصصة للمخدرات والمؤثرات العقلية، او استخدام تقنية تشفير خاصة يتم تقنينها وتوزيعها على العملاء والتجار عبر الانترنت، او تأسيس وسيط الكتروني متكامل كمزود خدمات الانترنت أو شبكة اتصالات متكاملة مهمتها الترويج عبر الانترنت.[1]

ثالثا: التعاطي عبر الانترنت للمواد المخدرة والمؤثرات العقلية:

يحفل الانترنت بغرف دردشة متخصصة في تعاطي[2] شتى أنواع المخدرات، من غرف تعاطي الهيروين وغرف تعاطي عقار النشوة[3] و الاكستازي[4]، وتقوم هذه الأخيرة بتقديم نصائح للمتعاطين الجدد وتدعوهم إلى

---

[1]– د/عمر محمد بن يونس،(المخدر...)مرجع سابق،ص 69 و ما بعدها.

[2]– ويقصد بالتعاطي تناول المادة المخدرة وإدخالها الجسم بأي وسيلة كانت لتؤثر على الأجهزة الموجودة بالجسم. وهو نوعان تعاطي بالصدفة وآخر تعاطي للمناسبة، لمزيد من التفاصيل ينظر أحمد أبو الروس: مشكلة المخدرات والإدمان،دار المطبوعات الجامعية، الاسكندرية، بدون سنة طبع، ص85.

[3]– يقصد بعقار "النشوة" هو أدوية جديدة ظهرت مع تطور الكيمياء وهي تشير إلى جزئ كيميائي معين يرمز له بMDMA وهي المسؤولة عن إحداث آثار نفسية(EFFETS PSYCHOACTIFS).

[4]– "الاكستازي "L'ecstasy هي عبارة عن حبوب ملونة ذات أشكال مختلفة تحمل بعض الرسومات المختلفة. وكانت تستخدم في بداية الأمر ونظرا لخطورتها لأغراض عسكرية في عام 1912 و اخترعتها مخابر مارك. مقال:"L'ecstazy" http:// www.doctissimo.fr.،

عدم تعاطي أي عقار آخر من المخدرات أو المؤثرات العقلية أو الكحوليات مع هذا العقار.ويبدو التعامل مع المخدرات من خلال اعترافات رواد غرف الدردشة ضربا من المرح والتسلية والفكاهة. فعن طريق المحادثات في هذه الغرف يمكن معرفة أساليب زراعة الماريجوانا ومعالجتها وتعاطيها، بل يمكن صناعاتها منزليا عن طريق المعلومات الموجودة في بعض المواقع بمواد بسيطة وأولية موجودة في بلدان كثيرة. إذ يمكن تصنيعها من الموز والفول السوداني. وفي هذا يقول أحد المختصين في مكافحة المخدرات من العاملين في البيت الأبيض الأمريكي:" أن ما تقوم به شبكة الانترنت العالمية يقوض الجهود والسياسات التي تبذلها الحكومة لمكافحة المخدرات، وذلك لأن الشبكة تنشر معلومات تؤدي إلى زرع بذور معاداة قوانين المخدرات[1]". وتبدو المشكلة المترتبة على تبادل الحديث في غرف الدردشة عبر الانترنت سلبية من زاويتين:

– جهل أولياء الأمور لثقافة تكنولوجيا المعلومات

– أن طبيعة الحديث في غرف الدردشة هي عبارة عن حديث عادي بين المشاركين حيث تتداول فيه معلومات تتعلق بأي شيء بما فيها المخدرات[2].

وتجدر الإشارة إلى أن أكثر الفئات تأثرا بانتشار تلك السموم الناجمة عن تعاطي تلك المواد الخطيرة هي فئة الشباب الثروة البشرية للدول. وهذا ما اثبته خبراء الحاسب الآلي والانترنت، إذ قدر عدد الاطفال الذين يبحرون في المواقع المخصصة للاستعمال غير المشروع للمخدرات عام 2000إلى 4ملاين طفل وسيرتفع العدد إلى 15مليون طفل، تتراوح أعمارهم بين العامين وسبعة عشرة عاما[3]. كما اكد تقرير الهيئة الدولية لمراقبة المخدرات عام 2001 في صفحته الخامسة على وجود دليل واضح على استعمال الانترنت كوسيلة لتبادل الرسائل والمعلومات التي تشجع الشباب خاصة على تعاطي المخدرات، ويؤكد مكتب الامم المتحدة المعني بالمخدرات والجريمة في نفس السياق على ان غرف الدردشة التي تنتشر على شبكة الانترنت من الروافد التي تغذي ثقافة تعاطي إدمان المخدرات بين الشباب عبر الانترنت والتي تمجد موسيقى البوب والتي على نغماتها يحلو لهؤلاء الآخرين تعاطي المخدر، وكذا إتباع خطى مطرب من أكثر مطربي البوب وملحنيها، الذي يلعب دور الداعية لتعاطي الحشيش[4] في المناسبات الاجتماعية والترفيهية والدينية. ويرى

---

[1]– أشار اليه د/ ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 74.

[2]– د/ عبد الفتاح بيومي حجازي،(الأحداث والإنترنت) مرجع سابق،ص112.

[3] – د/ عبد الفتاح بيومي حجازي،نفس المرجع، ص111–112

[4]– يعرف الحشيش وفقا للاتفاقية الدولية التي انتهى إليها مؤتمر الأفيون المنعقد في جنيف في 1925/02/19 هو:"الرؤوس المجففة المزهر أو المثمرة من السيقان لإناث لنبات الكنابيساتيفا الذي لم تستخرج مادته الصمغية أيا كان الاسم الذي يعرف به في التجارة ".أوهو:" الناتج او المحضر أو المستخرج من ازهار واوراق او سيقان او جذور راتنج نبات القنب الهندي ذكرا كان او انثى." والطريقة الشائعة لتعاطي الحشيش في البلاد العربية هي تدخينه في الجوزة او السجائر والبعض يتعاطاه أكلا بغير طهي او بعد طهيه مع الحلوى او وضعه في القهوة او الشاي، والبعض الآخر يبتلعه على شكل حبيبات صغيرة تشبه

المكتب أن الانترنت يروج لثقافة قيم الجنس والمخدرات وموسيقى الروك اندرول، وان هناك من نجوم غناء البوب من يقدم للشباب عبر الإرسال التلفيزيوني وشبكة الانترنت صورا زائفة عن الحالة المترتبة على تعاطي المخدرات، تتمثل في جعل المتعاطي جذابا وخلاقا وذا شخصية قيادية. وهي صورة تشجع الشباب على القدوم على التعاطي وكذا الاستمرارية فيه.[1]

ففي الدردشة يبدو تعاطي عقار الهلوسة (LSD)[2] لطالب في المرحلة الثالثة(مرحلة ثانوية) من أروع العمال التي قام بها في حياته وتبدو شمة الكوكايين بالنسبة لطالب آخر مثل قهوة الصباح التي تنعشه والتي يستطيع الحصول عليها بسهولة بمجرد اتصال هاتفي.[3]

رابعا:الزراعة غير المشروعة للقنب عبر الانترنت:

استفاد المجرمون من التقنيات الحديثة في مجال زراعة النباتات المخدرة[4] سواء أكانت تلك الاخيرة مشروعة أوغير مشروعة. إذا أصبحوا يستخدموا التكنولوجيا الحديثة لاسيما الانترنت في تلك الزراعة للنباتات المخدرة ومن بينها زراعة القنب الهندي[5] ، والتي تزايدت داخل البيوت خاصة في الولايات المتحدة الأمريكية وكندا وهولندا. ولقد ساعد على زيادة انتشار زراعتها في أوروبا الغربية البيع غير المقيد لبذور القنب ومعدات الزراعة فيما يعرف باسم دكاكين القنب، إضافة إلى وجود نوافذ عبر شبكة الانترنت يملكها موردون في كندا وهولندا لبيع بذور القنب بالإضافة إلى تقنيات متقدمة لاستنبات القنب. وتجدر الاشارة إلى

حبات الفول،ولذلك يطلق عليها اسم الفولة. كذلك قد يخلط الحشيش ببعض الاعشاب الجافة، ويطلق عليه اسم المنزول.لمزيد من التفاصيل ينظر د/ إدوار غالي الذهب، المرجع السابق، ص 23 وما يليها.

[1]– د/ محمد فتحي عيد، المرجع السابق، ص66 وما بعدها.

[2]– عقار "الهلوسة (LSD)" هو مركب من حمص ليسارجيك وعقاقير مسالكينور بتالينوبنتاز و سينوميثاكوالون وغيرها. وقد أقبل الشباب على تعاطي هذه العقاقير بصورة مفزعة واشتهرت بينهم باسم عقاقير الهلوسة بالنظر لما تحدثه في متعاطيها من احلام اليقظة وتهيؤات غير صحيحة وتصورات غريبة وخداعات بصرية، ويتم تعاطيها في شكل كبسولات بداخلها المسحوق المخدر او أقراص صغيرة أو سائل توضع نقطة منه على قطعة من السكر. وقد يعطى على شكل حقنه في العضل او في الوريد، وأقل كمية منه حتى ولو كانت مثل ذرة التراب تسبب للشخص حالة من الهلوسة والخيالات الغريبة تستغرق ثماني ساعات أو أكثر. د/إدوار غالي الذهب،المرجع السابق، ص32.

[3]– د/ ممدوح عبد المطلب، المرجع السابق، ص75.

[4]– ويقصد بزراعة النباتات المخدرة وفقا لمحكمة النقض المصرية بانها لا تعني مجرد إلقاء البذور في جوف الأرض او غرس شتلات النبات في باطنها، ولكنها تتجاوز هذا المدى لتشمل كل أفعال التعهد اللازمة للزرع سواء انصبت هذه الأفعال عليه مباشرة كأفعال التسميد والتقليم او وقعت على الأرض ذاتها كأعمال الري والغرق واستئصال النباتات الطفيلية، د/ إدوار غالي الذهبي، نفس المرجع، ص63

[5] – يعرف "القنب الهندي الحقيقي" علميا باسم كنابيسساتيفا(Cannabissativa) وتمتاز شجيراته عن شجيرات القنب الأخرى بقصر ساقها وكثرة فروعها، وهو يكثر في الهند وبعض أجزاء الجزيرة العربية و إفريقيا وبعض دول البحر الأبيض المتوسط ولكن أشد الشجيرات أثرا في تخديرها هي التي تنمو في اجواء تمتاز بحرارتها وجفافها النسبي ويستخرج منه ما يسمى بالحشيش لمزيد من التفاصيل ينظر/د إدوار غالي الذهبي، نفس المرجع ، ص23 وما يليها

أن السلطات البريطانية قد أعلنت خلال عام 2000 عن وجود أكثر من 1000 موقع على الانترنت تعرض مختلف أنواع المخدرات للبيع وخاصة القنب بالإضافة إلى الاكستازي والهيروين والكوكايين[1].

خامسا: الصنع غير المشروع للعقاقير المخدرة عبر الانترنت

ساهمت التكنولوجيا الحديثة لاسيما الانترنت في تطوير بحوث المخدرات وخاصة في مجال الصنع غير المشروع للعقاقير، ومنها المنشطات الأمفيتامينية[2] التي تحتل المرتبة الثانية لدى المتعاطين. ويعتبر عقار الاكستازي(النشوة) أكثر هذه العقاقير رواجا وانتشارا بين فئة الشباب وخاصة في الحفلات الصاخبة في أوروبا وأمريكا والكاريبي. حيث تقدم مواقع على الانترنت كيفية صنعه وتعاطيه بأمان وذلك إما باستخدام الحاسوب في معالجة جزئيات العقاقير الخاضعة للرقابة أو عن طريق الأدلة المعنونة(اصنعها بنفسك) التي تمتلئ بها شبكة الانترنت والتي تمكن قراءها من تحضير وتعاطي العقاقير الخاضعة للرقابة[3] أو عن طريق المواقع التي تقدم الكتب التي تتناول كيفية الحصول على السلائف الكيميائية المستخدمة في صنع المخدرات والمؤثرات العقلية، والتعرف على أسلوب تشغيل مختبرات العقاقير غير المشروعة خاصة وانها لا تتطلب فيها كيميائيا يحمل مؤهل جامعيا[4].كما تساهم تلك الشبكة في اقناع فئة الشباب بان ذلك العقاريعد البديل الممتاز لكل من الكراك والكوكايين والهروبين وعقار الهلوسة (LSD). ولقد شهد عاما 2000-2001حركة نشطة لضبط كميات كبيرة من عقار النشوة في اسرائيل وتركيا وكذا لمادة MDP-2-P-3.4[5]

وتجدر الاشارة إلى ان بعض تنظيمات الاتجار وغير المشروع بالمخدرات هي التي تتحكم في عمليات صنع المنشطات الأمفيتامينية التي يتزايد تعاطيها في جميع دول العالم. ففي تايلاند على سبيل المثال حل الميتامفياتين محل الهيروبين كأكثر العقاقير تعاطيا منذ أواخر التسعينيات.ضف إلى ذلك فإن الانترنت تساهم في انتشار التجارة الالكترونية للمنومات والمهبطات الخاضعة للرقابة عبر مواقعها إذ تقوم الصيدليات بإرسال كميات من هذه العقاقير بالبريد إلى من يطلبونها دون مراعاة الشروط التي وضعها القانون لضبط تجارة العقاقير الخاضعة للرقابة.

---

[1]- د/محمد فتحي عيد، المرجع السابق، ص 98.

[2]- المنشطات الأمفيتامينية: هي نوع من العقاقير الاصطناعية والتي تصنف ضمن المؤثرات العقلية

[3]- تجدر الإشارة إلى ان الكثير من هذه الأدلة تقع ملقماتها في كندا والولايات المتحدة الأمريكية

[4]- والدليل على ذلك نسبة الكيميائين الجامعيين المقبوض عليهم في قضايا صنع غير المشروع للامفيتامينات تقل عن 10% وهو ما يفسر وقوع العديدمن حوادث الحرائق والانفجارات والاصابات في المختبرات غير المشروعة. د/ محمد فتحي عيد، المرجع السابق، ص137.

[5]- مادة (MDP-2-P-3.4)هي مادة تصنع بصورة مشروعة في الصين لاستعمالها في صنع مستحضرات صيدلانية وتهرب من الصينومن القنوات المشروعة لاستخدامها في تصنيع عقار الاكستازي.

المطلب الثاني

المعالجة القانونية لجريمة المخدرات عبر الانترنت.

تعد جريمة الاتجار في المخدرات إحدى أقدم الجرائم المنصوص على تجريمها في كافة قوانين دول العالم.بل و الأكثر من ذلك أن تصنيعها أو زراعة أحد النباتات التي تستخرج منها أو توزيعها أو إخفائها أو أن القيام بأي عمل من الأعمال المتصلة بما تم ذكره، هو عمل مجرم ومشددة عقوبته.

و لقد خصص هذا المطلب للتطرق إلى موقف التشريعات الدولية و الممثلة في الاتفاقيات و المعاهدات الدولية من جريمة المخدرات عبر الانترنت، و كذا موقف التشريعات المقارنة من تلك الجريمة. و ذلك من خلال الفرعين التاليين:

الفرع الأول: الجهود الدولية المبذولة في قمع و الوقاية من المخدرات و المؤثرات العقلية عبر الانترنت.

الفرع الثاني: موقف التشريعات المقارنة من جريمة تكنلجة المخدرات و المؤثرات العقلية.

الفرع الأول: الجهود الدولية المبذولة في قمع و الوقاية من المخدرات والمؤثرات العقلية عبر الانترنت:

اعترف المجتمع الدولي بهذا النوع من الإجرام منذ عام 1961،إذ أخذ موضوع المخدرات و المؤثرات العقلية الطابع الدولي تماما بصدور الاتفاقية الوحيدة للمخدرات المؤرخة 1961//03/30 بنيويورك ثم بانعقاد لجنة الأمم المتحدة لمكافحة المخدرات في العاصمة النمساوية.أما اتفاقية المؤثرات العقلية فهي اتفاقية فيينا المؤرخة في 1971/02/21. ولقد اعترف المجتمع الدولي بأن المخدرات و المؤثرات العقلية تهدد الأمن القومي للدول و سيادتها كما تهدد كرامة وآمال الملايين وأسرهم و تسبب خسائر لا تعوض في أرواح البشر[1] و أكد في ذلك على ضرورة زيادة وتعزيز التعاون الدولي، وكذا تبادل المعلومات بما فيها تبادل الخبرات الوطنية للكف على تشجيع إساءة استعمال المخدرات والاتجار غير المشروع بها بواسطة استخدام الإنترنت وفي المقابل لاستخدام هذه التقنية الحديثة كوسيلة لخفض الطب على المخدرات.[2] وقد

---

[1]– لمزيد من التفصيل ينظر د/مصطفى طاهر:المواجهة التشريعية بظاهرة غسل الأموال المتحصلة من جرائم المخدرات، الطبعة الثانية، مطابع الشرطة، 2004، ص28 وما بعدها.

[2]– يقصد بخفض الطلب على المخدرات إتخاد التدابير و الإجراءات اللازمة لتقليص عدد متعاطي المخدرات إلى أدنى حد ممكن فيقل الطلب على المخدرات و تبور تجارتها.وهو مصطلح حديث نسبيا دخل لغة المهتمين بمعالجة مشكلة المخدرات في عقد الثمانينات. و كان أول استعمال له في سياق علمي دولي في المخطط الشامل المتعدد التخصصات للأنشطة المقبلة في ميدان مكافحة إساءة استعمال العقاقير الذي اعتمده المؤتمر الدولي المعني بإساءة استعمال العقاقير و الاتجار غير المشروع فيها. ثم استعمال المصطلح بعد ذلك في برنامج العمل العالمي الذي اعتمدته الجمعية العامة للأمم المتحدة في دورتها الاستثنائية السابعة عشرة و في اجتماع القمة الوزاري العالمي لخفض الطلب على المخدرات و مكافحة خطر الكوكايين المعقود في لندن. و اعتبارا من 1994 أصبح المصطلح بندا ثابتا في جدول أعمال لجنة المخدرات في دورتها

جاء ذلك في قرار الجمعية العامة للأمم المتحدة رقم 132/45 المؤرخ في فبراير 2000 بشأن أهمية التعاون الدولي في مكافحة مشكلة المخدرات العالمية، وفي قرارها رقم 65/55 بشأن التعاون الدولي لمكافحة المخدرات المؤرخ في 2001/01/26 وكذا في تقرير اللجنة الثالثة للجمعية العامة للأمم المتحدة حول المراقبة الدولية للمخدرات المؤرخ في 2001/11/14[1].

هذا من جهة و من جهة أخرى، فقد جرمت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في مادتها 16[2] الترويج للمخدرات و المؤثرات العقلية أو الإتجار بها و المرتكبة بواسطة تقنية المعلومات و منها شبكة الإنترنت.

والجدير بالذكر أن الهيئة الدولية لمراقبة المخدرات[3] هي أول من نبه العالم إلى الدور السلبي للإنترنت في الانتشار السريع والرهيب للمخدرات والمؤثرات العقلية عبر العالم (في تقريرها لعام 1992)،من خلال توفير كم هائل من المعلومات القيمة والخطيرة التي تسهل الوصول إليها في زمن متناه القصر، وتبين كيفية إنتاجها (الإنتاج الزراعي أو الإنتاج الصناعي). وكذا سهولة تخفي متعاطيه وهروبهم من قبضة أجهزة مكافحة المخدرات[4].

هذا من جهة ومن جهة أخرى، فإن أول إساءة لاستخدام الإنترنت في مجال الاتصال المادي والقانوني بالمخدرات والمؤثرات العقلية تعلقت بموضوع الدعوة إلى تعاطي المخدرات والحض عليها. وكانت للجماعة الأمريكية التي يتزعمها "ديفيد بوردين" وتطلق على نفسها اسم " شبكة تنسيق الاستخدام المرشد للمخدرات[5]"

السنوية وفي جدول اللجان الفرعية المنبثقة عن اللجنة. د/ محمد فتحي عيد،(الإنترنت و دوره في إنتشار المخدرات) مرجع سابق، ص42.

[1]– د/ عمر محمد بن يونس،(المخدرات...) مرجع سابق، ص19.

[2]– تنص المادة 16 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على :" الجرائم المتعلقة بالجرائم المنظمة و المرتكبة بواسطة تقنية المعلومات:

2– الترويج للمخدرات و المؤثرات العقلية أو الإتجار بها."

[3]– الهيئة الدولية لمراقبة المخدرات هي هيئة تحل محل اللجنة الرئيسية الدائمة ومحل هيئة الإشراف على المخدرات. وهي تتكون من 13 عضوا ينتخبهم المجلس الاقتصادي والاجتماعي من بين الخبراء في مجال الطب والصيدلة والقانون، ويختار ثلاثة أعضاء من قائمة أشخاص ترشحهم منظمة الصحة العالمية من ذوي الخبرة في الطب أو علوم العقاقير أو الصيدلة. بينما يختار العشرة الباقين من قائمة أشخاص ترشحهم الدول الأعضاء في الأمم المتحدة والدول غير الأعضاء في الأمم المتحدة. وأهم ما تقوم به الهيئة: * لفت انتباه الحكومات إلى الثغرات ومواطن الضعف في المراقبة الوطنية وفي التقيد بأحكام المعاهدات.

لها أيضا أن توصي بتقديم المساعدات التقنية أو المالية أو كليهما إلى الدول التي تحتاجها وتطلبها. د/محمد فتحي عيد، (الإنترنت....) مرجع سابق، ص 6.

[4]– والسبب في ذلك يرجع إلى تمتع الإنترنت باللامركزية و اللا ملكية.

[5]– تعمل هذه الجماعة عبر الإنترنت منذ عام 1993، وهي تدعو إلى ضرورة تغيير قوانين المخدرات وضرورة النص على إباحة حيازتها.

Drug Reform coordination Network قصب السبق في هذا الخصوص.ضف إلى ذلك فهناك مجلة شهرية أمريكية تدعى High times تروج لمخذر الماريجوانا في الولايات المتحدة الأمريكية منذ 20 عاما. والتي أنشئ لها موقع على الإنترنت منذ 4 سنوات. وفي هذا الشأن يرى مالكها أنه يمكن لأي شخص أن يطلق موقعا على الشبكة فضلا عن وجود مئات المواقع التي تروج لثقافة الماريجوانا ويصعب متابعتها[1].

الفرع الثاني: موقف التشريعات المقارنة من جريمة تكنلجة المخدرات و المؤثرات العقلية.

و بعد أن بينا الجهود الدولية المبذولة للوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها من خلال أبرام المعاهدات و الإتفاقيات، سنحدد في هذا الفرع موقف التشريعات المقارنة حيال هذه الأفعال غير المشروعة من خلال تقسيمها إلى موقفين نوضح في الأول منها موقف التشريعات الغربية من جريمة تكنلجة المخدرات و المؤثرات العقلية، أما الموقف الثاني فنخصصه للتشريعات العربية من هذه الجريمة المستحدثة. و ذلك كمايلي:

أولا: موقف التشريعات الغربية من جريمة تكنلجة المخدرات و المؤثرات العقلية:

لقد خصت كل الدول الغربية قوانين خاصة لمواجهة مثل هذا الاجرام المستحدث و الذي أفرزه التطور التكنولوجي الذي شهدته. و نذكر من هذه الدول فرنسا و أمريكا.

1/ موقف التشريع الفرنسي من جريمة تكنلجة المخدرات و المؤثرات العقلية:

عالج المشرع الفرنسي جريمة تكنلجة المخدرات و المؤثرات العقلية من خلال المادة 222-37 في فقرتها الثانية من قانون العقوبات الفرنسي و التي تعاقب كل من سهل بأي وسيلة كانت الإستعمال غير المشروع للمخدرات و المؤثرات العقلية بالحبس لمدة 10 سنوات و بغرامة مالية قدرها 7500000 يورو[2]، و على هذا الأساس قامت محكمة الإستئناف Douai بادانة موقع انترنت Proselyt.com لأنه قام بنشر معلومات حول كيفية تعاطي مخدر القنب و أماكن بيعه....[3]

---

[1]- بحث رائحة الماريجوانا تتبعث من أوكار الإنترنت، http:// www. Cadac.og

[2] -222-37 : « Le transport, la détention, l'offre, la cession, l'acquisition ou l'emploi illicites de stupéfiants sont punis de dix ans d'emprisonnement et de 7 500 000 euros d'amende.

Est puni des mêmes peines le fait de faciliter, par quelque moyen que ce soit, l'usage illicite de stupéfiants, de se faire délivrer des stupéfiants au moyen d'ordonnances fictives ou de complaisance, ou de délivrer des stupéfiants sur la présentation de telles ordonnances en connaissant leur caractère fictif ou complaisant. »

[3]-Voir Abbas JABER : Les infractions commises sur internet، L'Harmattant، Paris، p 100.

-Ivana OBRADOVIC(OFDT) : Legislations relatives à l'usage et à la detention de cannabis : définitions et état des lieux en Europe , Note n°2011-19, Saint-Denis, p 4, http://www.ofdt.fr.

2/ موقف التشريع الأمريكي جريمة تكنلجة المخدرات و المؤثرات العقلية:

أما فيما يخص المشرع الأمريكي فقد جرم جريمة تكنلجة المخدرات والمؤثرات العقلية من خلال القانون الصادر في عام 1999 والمسمى The Methamphetamine Anti Proliferation Act والذي جرم من خلاله المشرع الفدرالي الأمريكي إستخدام الخطوط النشطة الدالة عبر الإنترنت للإتصال والولوج على مواقع الأدوية والعقاقير والسموم والمخدرات والمؤثرات العقلية[1].

ثانيا: موقف التشريعات العربية من جريمة تكنلجة المخدرات و المؤثرات العقلية:

و سنقسمها إلى موقفين، موقف نخصصه لتبيان موقف التشريعات العربية بصفة عامة، لنعرض بعد ذلك لابراز موقف التشريع الجزائري من جريمة تكنلجة المخدرات و المؤثرات العقلية، و ذلك كمايلي:

1/ موقف التشريعات العربية بصفة عامة من جريمة تكنلجة المخدرات و المؤثرات العقلية:

إنقسمت التشريعات العربية في موقفها حيال تكييفها لجريمة تكنلجة المخدرات و المؤثرات العقلية إلى تشريعات **إكتفت بتطبيق نصوص قوانينها العقابية التقليدية** كما هو حال **التشريع المصري**، اذ جرم المشرع المصري الاتجار في المخدرات وشدد العقوبة لمن يجلب المخدرات من الخارج محاولا إدخالها مصر بالإعدام شنقا حتى تثبت التهمة في حقه.[2] و على عكس ذلك قامت بعض التشريعات العربية الأخرى **بسن قوانين خاصة** تستوعب هذه المستجدات الإجرامية التي طرأت على جريمة الإستعمال و الإتجار غير المشروع للمخدرات و المؤثرات العقلية و منها:

التشريع الليبي، إذ طرحت الجمعية الوطنية الليبية لمكافحة المخدرات والمؤثرات العقلية، إدارة فرع بنغازي مشروع قانون مؤرخ في 2000/4/22 من ستة مواد يتضمن طرحا لفكرة التعديل القانون رقم 7لسنة 1990 بشأن المخدرات والمؤثرات العقلية بما يتوافق ونظم تقنية المعلومات والإنترنت.

و كذا **التشريع الإماراتي** من خلال القانون الاتحادي رقم(6) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، حيث تضمنت المادة 18[3] منه تجريم ترويج المخدرات او المؤثرات العقلية عبر الانترنت. كما جرم **المشرع السعودي** التعامل بالمخدرات والمؤثرات العقلية عبر الإنترنت في المادة(06) /4 [4] من نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية.

-Drogues، Savoir plus،Livret juridique، INPES، Avril 2004،p 18.

[1]- د/ عمر محمد أبو بكر بن يونس، (المخذرات...) مرجع سابق، ص 73.

[2]- د/ عمر محمد أبو بكر بن يونس، (المخذرات...) نفسمرجع سابق، ص 72.

[3]- تنص المادة 18 من القانون الاتحادي رقم(6) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات على:"كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد ترويج المخدرات أو المؤثرات العقلية وما في حكمها او تسهيل التعامل فيها وذلك في غير الأحوال المصرح بها قانونا، يعاقب بالسجن المؤقت".

[4]- تنص المادة (06) /4 من نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية حيث نص على:"يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من

2/ موقف التشريع الجزائري من جريمة تكنلجة المخدرات و المؤثرات العقلية:

عالج المشرع الجزائري جريمة المخدرات من خلال عدة قوانين[1] فمثلا جاء الأمر رقم 75-9 المؤرخ في 17 /04/ 1975 يتضمن قمع الاتجار والاستهلاك المحظورين للمواد السامة والمخدرات ثم تلاه القانون رقم 04- 18 المؤرخ في 2004/2/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها. حيث خص الفصلين الأول والثاني إلى الأحكام العامة والتدابير الوقائية والعلاجية، أما الفصل الثالث والذي يهمنا فخصه للأحكام الجزائية وذلك من خلال المواد من 12 إلى 31. فجرم و عاقب بذلك استهلاك وحيازة وتسليم وعرض المخدرات أو المؤثرات العقلية بهدف الاستعمال والاستهلاك الشخصي من خلال المادة 12 و 13 من هذا القانون[2]. وكذا إنتاج أو صنع أو حيازة أو عرض أو بيع أو وضع للبيع أو حصول وشراء قصد البيع أو التخزين واستخراج أو تحضير أو توزيع أو تسليم بأية صفة كانت أو سمسرة أو شحن أو نقل عن طريق العبور أو نقل المواد المخدرة أو المؤثرات العقلية[3] وكذا تصدير واستيراد هذه المواد السامة[1] أو زراعتها[2] او تصنيعها ونقلها وتوزيعها[3]. كما عاقب

الجرائم المعلوماتية الآتية:... 4/ إنشاء موقع على الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي أو نشره للإتجار بالمخدرات أو المؤثرات العقلية أو ترويجها او طرق تعاطيها أو تسهيل التعامل بها."

[1]- إنضمت الجزائر للإتفاقية الدولية الوحيدة لسنة 1961 بموجب المرسوم الرئاسي رقم 63-343 المؤرخ في 1963/9/11 كما إنضمت أيضا إلى البروتوكول المتعلق بتعديل الإتفاقية المذكورة و الموقع بجنيف يوم 1971/3/25 بموجب مرسوم رئاسي مؤرخ في 2002/2/5 و أخيرا إتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع بالمخدرات و المؤثرات العقلية لعام 1988 بموجب مرسوم رئاسي مؤرخ في 1995/2/28. لمزيد من التفاصيل ينظر سيدهم مختار،المرجع السابق، ص 31.

[2]- نصت المادة 12 من القانون رقم04-18 على مايلي: "يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 5000إلى 50000دج أو بإحدى هاتين العقوبتين كل شخص يستهلك أو يحوز من اجل الاستهلاك الشخصي مخدرات أو مؤثرات عقلية بصفة غير مشروعة". وتنص المادة 13 من نفس القانون على: "يعاقب بالحبس من سنتين إلى عشر سنوات و بغرامة من 100000إلى 500000دج كل من يسلم او يعرض بطريقة غير مشروعة مخدرات او مؤثرات عقلية على الغير بهدف الاستعمال الشخصي.

يضاعف الحد الأقصى للعقوبة إذا تم تسليم او عرض المخدرات او المؤثرات العقلية حسب الشروط المحددة في الفقرة السابقة على قاصر او معوق او شخص يعالج بسبب إدمانه أو في مراكز تعليمية او تربوية او تكوينية او صحية أو اجتماعية او داخل هيئات عمومية."

[3]- تنص المادة 17 من ذات القانون على:"يعاقب بالحبس من عشر سنوات إلى عشرين سنة وبغرامة من 5000.000إلى 50.000.000 دج كل من قام بطريقة غير مشروعة بإنتاج أو صنع أو حيازة أو عرض او وضع للبيع أو حصول وشراء قصد البيع أو التخزين أو استخراج أو تحضير أوتوزيع أو تسليم بأية صفة كانت أو سمسرة أو شحن او نقل عن طريق العبور أو نقل المواد المخدرة أو المؤثرات العقلية.

ويعاقب على الشروع في هذه الجرائم بالعقوبات ذاتها المقررة للجريمة المرتكبة ويعاقب على الأفعال المنصوص عليها في الفقرة الأولى أعلاه بالسجن المؤبد عندما ترتكبها جماعة إجرامية منظمة".

على تسهيل الإستعمال غير المشروع لتلك المواد المخدرة أو المؤثرات العقلية سواء أكان ذلك بمقابل أو مجانا و مهما كانت الوسيلة المستخدمة في ذلك [4]و التي يمكن أن تكون عن طريق الانترنت وذلك بنشر إحدى المواقع المتخصصة في هذا المجال معلومات تعلم و تشرح لمتعاطي هذه المواد السامة كيفية إستعمالها و عنوين الأماكن التي تباع فيها. و إضافة إلى ذلك فقد عاقب كل من حرض أو شجع أو حث بأية وسيلة كانت على إرتكاب الجرائم السابقة بالعقوبات المقررة لها.

و من هذا نستخلص أن المشرع الجزائري و إن لم ينص صراحة على جريمة تكنلجة المخدرات و المؤثرات العقلية ولكن يمكن القول بتطبيق المواد الواردة في القانون رقم 04- 18 المؤرخ في 2004/2/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها و لا سيما المادة 15 و 17 و 22 من ذلك القانون و كذلك يمكن تطبيق المادة 394 مكرر2 من قانون العقوبات.

ويقصد بالنقل عن طريق العبور وفق المادة 2 من ذات القانون النقلعن طريق دولة العبور والتي هي الدولة التي يجري عبر إقليمها نقل المواد غير المشروعة والمخدرات والمؤثرات العقلية والمواد الواردة في الجدول الأول والجدول الثاني غير المشروعة والتي ليست مكان منشئتها الأصلي ولا مكان مقصدها النهائي.

[1]- تنص المادة 19 من ذات القانون على: "يعاقب بالسجن المؤبد كل من قام بطريقة غير شرعية بتصدير أو استيراد مخدرات أو مؤثرات عقلية".

[2]- تنص المادة 20 من ذات القانون على: "يعاقب بالسجن المؤبد كل من زرع بطريقة غير مشروعة خشخاش الأفيون أو شجيرة الكوكا اونيات القنب".

ويقصد بنبات القنب وفقا للمادة 2 منه أي نبات من جنس القنب أما خشخاش الأفيون فهو كل شجيرة من فصلية الخشخاش المنوم، أما شجيرة الكوكا فهي كل نوع من أنواع الشجيرات من جنس اريتروكسيلون

[3]- تنص المادة 21 من ذات القانون على:"يعاقب بالسجن المؤبد كل من قام بصناعة او نقل او توزيع سلائف أو تجهيزات او معدات إما بهدف استعمالها في زراعة المواد المخدرة او المؤثرات العقلية وإما مع علمه بأن هذه السلائف أ و التجهيزات او المعدات ستستعمل لهذا والنقل وفقا للمادة 2 من ذات القانون هو نقل المواد الموضوعة تحت المراقبة داخل الإقليم الجزائري من مكان إلى آخر أو عن طريق العبور أما السلائف فيقصد بها جميع المنتجات الكيميائية التي تستخدم في عمليات صنع المواد المخدرة والمؤثرات العقلية".

[4]- تنص المادة 15 من ذات القانون في فقرتها الأولى على:" يعاقب بالحبس من خمس (5) سنوات إلى خمس عشرة سنة و بغرامة من 500000 دج إلى 1000000 دج، كل من:

1- سهل للغير الإستعمال غير المشروع للمواد المخدرة أو المؤثرات العقلية بمقابل أو مجانا، سواء بتوفير المحل لهذا الغرض أو بأية وسيلة أخرى، وكذلك المر بالنسبة لكل من الملاك و المسيرين و المديرين و المستغلين بأية صفة كانت لفندق او منزل مفروش او نزل أو حانة أو مطعم أو ناد او مكان عرض أو أي مكان مخصص للجمهور أو مستعمل من الجمهور، الذين يسمحون باستعمال المخدرات داخل هذه المؤسسات أو ملحقاتها او في الأماكن المذكورة."

و من القضايا الواقعية التي تظهر دور الانترنت في نشر ثقافة المخدرات:

القضية الأولى: حيث قامت السلطات الاتحادية والمحلية في عدد من الولايات المتحدة الأمريكية بجملة تعقب واسعة لمروجي المخدرات عبر الإنترنت لاسيما عقار GHB [1]، وألقت القبض على العشرات في مختلف المدن الأمريكية وفي هذا الشأن قامت هيئة المحلفين العليا بالمقاطعة الوسطى لولاية فلوريدا باتهام إحدى الشركات في 30 سبتمر 1999 بالقيام بالإعلان والترويج على ذلك العقار خلال المدة 1996إلى 1998 عبر المجموعات الإخبارية والبريد الإلكتروني[2].

القضية الثانية: حيث قامت هيئة المحلفين العليا بولاية فيرجينيا في 17ماي 2000 بتوجيه الاتهام إلى مالك موقع عبر الإنترنت بقيامه بالترويج لعقار NITROXS OXIDE وعقاقير أخرى -وهو عقار مسبب للوفاة – للعملاء في المقاطعة الغربية لولاية فيرجينيا عبر الموقع Bongmant.com الذي يديره المتهم[3].

وفي أول حملة من نوعها قام المحققون بما يزيد عن 150حملة تفتيش في أكثر من 70مدينة أمريكية. اعتقل فيها العديد من موزعي المخدرات الذين يستخدمون تكنولوجيا العصر الإنترنت لتوزيع بضائعهم المخدرة[4].

القضية الثالثة: حيث أدين كارل ديفيد روبرت بالسجن لمدة 4 سنين و9 أشهر بتهمة استعماله لتكنولوجيا المعلومات الإنترنت بغرض الاتجار غير المشروع بالمخدرات (عرض مواصفات المخدرات للبيع وكذا شرح كيفية الحصول عليها وكذا على بعض الأدوية المراقبة).[5]

القضية الرابعة: وفي قضية متشابهة أدين KIMBALL بالسجن لمدة 13 سنة بتهمة الشروع في عرض المخدرات للاتجار عبر الإنترنت[6] .

وتجدر الإشارة إلى انه ووفقا لإحصائيات الإنتربول يقوم أكثر من ألف موقع إنجليزي بالإتجار غير المشروع بالمخدرات والمؤثرات العقلية عبر الإنترنت مثل الاتجارcannabis seeds and derivatives وكذلك الاتجار بعقار MDMA والمعروف في التداول باسم ecstasy وكذلك الكوكايين والهيروبين.[7]

---

[1]– عقارGHB هو عقار مخدر عبارة عن خليط يتكون من مواد كيميائية صناعية ويعمل هذا العقار ومشتقاتهBD 1K4 وGBL كعامل مؤثر على النظام المركزي للأعصاب مما يتسبب في الشعور بالدوران والغثيان والدوخة وعدم القدرة على التركيز وقد يتسبب في الوفاة فحسب إحصائية تبين أن هذا العقار أدى إلى وفاة اكثر من 72 شخصا. عمروعيسى الفقي، المرجع السابق، ص142.

[2]– مقال منشور على الموقع http:// www. cnn.com

[3]– عمروعيسى الفقي، المرجع السابق، ص143

[4]– عمرو عيسى الفقي،نفس المرجع، ص 137

[5]– عمر محمد بن يونس،(المخدرات...) مرجع سابق، ص33

[6]– عمر محمد بن يونس، المرجع السابق، ص34

[7]– عمر محمد بن يونس، المرجع السابق ، ص46

هذا من جهة ومن جهة أخرى فإن الإحصائيات والدراسات الشرطية في بريطانيا تشير إلى وجود علاقة متينة جدا بين تجارة البرمجيات المقلدة counterefeit software والاتجار غير المشروع بالمخدرات والمؤثرات العقلية فقد تبين عند مهاجمة أوكار تجار المخدرات Derbyshire و Chesterfield في بريطانيا وجود أعداد ضخمة من برمجيات مقلدة جاهزة للتوزيع[1].

ويصرف النظر عن تقاعس الدول في مواجهة ظاهرة المواقع التي تروج للمخدرات عبر شبكة الإنترنت رغم اهتمام الحكومات بمواجهة المواقع الإباحية على الشبكة فهناك تحالفات مناهضة لتعاطي وإدمان المخدرات لها مواقع على الشبكة[2] منها تجمع لنتحد[3]. وإلى جانب ذلك هناك من المواقع التي تطالب بإباحة تعاطي المخدرات والمؤثرات العقلية إذانها تجعل من تعاطاها ينقلك إلى عالم الأحلام والراحة وذلك عن طريق بثها لشخصية كرتونية تمثل شخصا مدمنا للمخدرات يصرخ يجب جعل حيازة المخدرات مشروعة، إنها تجعل اليوم العادي أكثر متعة وحيوية. ويطلق على هذه المواقع اسم مواقع الثقافة المضادة وأشهرها موقع Paranoia.com.[4]

[1]– عمر محمد بن يونس،(الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص661

[2] – ينظر لمزيد من التفاصيل د/عبد الفتاح بيومي حجازي، (الأحداث والإنترنت)، مرجع سابق، ص109

[3]– ينظر د/ محمد فتحي عيد، المرجع السابق، ص68. و كذلك موقع http:// www.drugstrategies.com

[4]– لمزيد من التفاصيل ينظر د/ محمد فتحي عيد، نفس المرجع، ص68 وما بعدها

الفصل الثالث:

جرائم الإعتداء على التجارة الإلكترونية عبر الإنترنت

تعتبر التجارة الإلكترونية إحدى إفرازات ثورة التكنولوجيا، فهي من المتغيرات الجديدة التي فرضت نفسها بقوة خلال الحقبة الأخيرة من القرن العشرين، حيث أصبحت تمثل أحد دعائم النظام الاقتصادي العالمي الجديد و أحد الآليات الهامة التي تعتمد عليها عولمة المشروعات التجارية و الإنتاجية.

و لقد تعددت و اختلفت مفاهيمها (سواء فقها أو قانونا)[1] بين التعريفات الموسعة و المنتقاة و الضيقة[2]. الأمر الذي أدى إلى صعوبة استحداث تعريف موحد شامل لها[3].

---

[1]– تناولت وثائق الأمم المتحدة تعريفا لهذه التجارة، من خلال تعريف تبادل المعلومات الإلكترونية. و أوردت القوانين المقارنة في أوربا لها تعريفات كتلك الصادرة في لوكسمبورغ (قانون التجارة الإلكترونية لدوقية) و إيطاليا و فرنسا. أما بالنسبة للتشريعات العربية فنجد أن المادة الأولى من مشروع التجارة الإلكترونية المصري قد عرفها و كذلك قانون التجارة الإلكترونية التونسي في مادته الثانية و كذا قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات و التجارة الإلكترونية و القانون الأردني. لمزيد من التفاصيل ينظر على التوالي: د/ عبد الفتاح بيومي حجازي، (الأحداث و الإنترنت) مرجع سابق، ص258. د/ مدحت عبد الحليم رمضان : الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص12 و ما بعدها. د/ عمربن يونس، (الجرائم الناشئة عن...) مرجع سابق، ص140. إيهاب صلاح الدين: الإطار القانوني للتجارة الإلكترونية، مجلة القضاء العسكري، العدد 16، المجلد الثاني، ديسمبر 2006، ص73.

–**Le commerce électronique** peut être définit comme l'ensemble des échanges électroniques liés aux activités commerciales. Il recouvre toute opération de vente de biens et de services via un canal électronique.

puf، 1ere éd،: Que sais-je? Le commerce électronique François Leslé Nicolas Macarez 2001. ،p4.

Boubaker Nobel El Houssine: Travaux pratiques de commerce électronique, Institut des université de hautes études commerciales de Sousse, année universitaire 2004/2005,Sousse ،p5, http://www.web2-com.com

–Henri ISAAC, Pierre Volle: E– Commerce ،de la stratégie à la mise en œuvre opérationnelle, Pearson éducation France, Paris,2008, p12–13.

–Vincent VIGNEAU: Commerce électronique et Protection des consommateurs, Master 2, droit des nouvelles technologies de l'information et de la communication , université de Versailles– Saint– Quentin en Yvelines, année universitaire 2010/2011, p7.

Olivier AUZON: Le droit de Commerce électronique,édition du puit fleuri, 2007,p13.

[2]– فأما بالنسبة لأصحاب التعريف الموسع فيعرفون التجارة الإلكترونية بأنها: "مجموعة الخدمات المتبادلة و العمليات التجارية و الصفقات الناجمة عن استعمال الشبكة و المتعلقة بالعالم الأعمال".

أما التعريف المنتقى فيمثله الفقيه الفرنسي CAPRIOLI و مقتضاه أن التجارة الإلكترونية: "هي ذلك العمل الذي تقوم به المنشأة باستخدام المعلوماتية و المرتبط بشبكات الاتصالات بقصد التعامل مع بيئتها التجارية".

و أما التعريف المضيق فيذهب أنصاره إلى أن التجارة الإلكترونية "ما هي إلا مجموعة العلاقات التجارية بين مستخدمي الإنترنت". د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن...) مرجع سابق، ص141.

[3]– و لقد كانت الصعوبة في مجال استحداث تعريف للتجارة الإلكترونية ينبثق من مسألة تبادل الإرادة و ذلك لسببين: الأول يتعلق بعدم التواجد المادي للمتعاقدين، و الثاني موضوع الجنسية التي قد تتفق و قد تتخلف. و في هذه الحالة نجد أنفسنا أمام تنازع في القوانين الواجبة التطبيق. د/ عمر محمد أبو بكر بن يونس، نفس المرجع، نفس الموضع.

و لكن و بالرغم من ذلك يمكن تعريف التجارة الإلكترونية بأنها "كافة الأنشطة التجارية للبضائع و الخدمات التي تتم باستخدام تكنولوجيا المعلومات و عبر شبكة اتصال دولية و باستخدام التبادل الالكتروني للبيانات لتنفيذ العمليات التجارية سواء تمت بين الأفراد أو بين الأفراد و الهيئات"[1]. ولذلك لا يقصد بالتجارة الالكترونية تلك التجارة في الأجهزة الالكترونية، بل يقصد بها أن تتم التجارة الالكترونية بين المتعاملين فيها، بممارستهم لأعمالهم التجارية من خلال استخدام أجهزة و وسائل إلكترونية مثل الإنترنت و غيرها من الأدوات[2]. و عليه يمكن تشبيهها بسوق إلكتروني يتقابل فيه البائعون و الموردون و الوسطاء و المستهلكون، و تقدم فيه المنتجات و الخدمات في صورة رقمية أو افتراضية، و يتم دفع ثمنها بالنقود الإلكترونية.فهي بذلك لا تختلف عن التجارة التقليدية إلا في تنفيذ تلك الفعاليات، إذ أنها تتم بأسلوب غير تقليدي في الوصول إلى المستهلكين في كافة أنحاء العالم، و ذلك بتحقيقها عائدات ضخمة يقابلها انخفاض كبير في التكاليف[3]. و هي بذلك تتميز بالمميزات التالية:

– ارتباطها بالأنشطة التجارية ذات المفهوم الواسع الذي لا يقتصر على المعاملات التجارية و حسب بل يشمل جميع الأنشطة الاقتصادية كالاستثمارات و عمليات البنوك.

– و تمتاز بكونها ذات طبيعة دولية دائمة نظرا لعالمية شبكة الإنترنت.ضف إلى ذلك فإنه يشترط تواجد أطراف العقد في المواجهة،و لا يشترط تنفيذ التزامات العقد في ذات المكان[4]. و هي تمر بثلاث مراحل أساسية:

مرحلة بناء المواقع التجارية على شبكة الإنترنت و التسوق خلالها، و يطلق عليها مرحلة ما قبل إبرام العقد الإلكتروني، مرحلة إبرام العقد الإلكتروني،مرحلة تنفيذ الالتزامات المترتبة على العقد الإلكتروني[5].

و لعل من المظاهر التجارية الجديدة عبر التجارة الإلكترونية هو المركز التجاري الإفتراضي ، و هو عبارة عن خدمة إلكترونية يتم الدخول إليها عبر الإنترنت بالنظام المفتوح تسمح بالعرض والطلب من خلالها[6].

ولما كانت الإنترنت هي إحدى وسائل التجارة الإلكترونية، و كانت هذه الأخيرة عبارة عن نظام معلوماتي عبر هذه الشبكة يضم بيانات و معلومات و أموال تتدفق عبرها،الأمر الذي جعل منها مجالا خصبا

---

[1]– د/ خالد ممدوح إبراهيم:إبرام العقد الإلكتروني، دراسة مقارنة، الدار الجامعية، مصر، 2007، ص58.

[2]– و من الأدوات نذكر التسوق عبر التليفون أو عبر الأجهزة المحمولة كالهاتف النقال أو الكمبيوتر المحمول أو جهاز الاستدعاء أو التتبع و الأجهزة اليدوية المختلفة مثل الكمبيوتر اليدوي. و عن طريق خاصية الرد الآلي على المكالمات الهاتفية و هو ما يطلق عليه بالتجارة الإلكترونية الصوتية. لمزيد من التفاصيل ينظر د/ عصام عبد الفتاح مطر، المرجع السابق، ص29–30.

[3]– لمزيد من التفاصيل ينظر د/ عصام عبد الفتاح مطر، نفس المرجع، ص32–33.

[4]– د/ حسين الغافري، محمد الألفي، المرجع السابق، ص142.

[5]– لمزيد من التفاصيل ينظر د/ عصام عبد الفتاح مطر، المرجع السابق، ص133 و ما بعدها.

[6]– لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن...) مرجع سابق، ص143.

لمرتكبي الجرائم، إذ سهلت لهم جميع صور الإعتداءات التي يمكن أن تكون هذه الأخيرة محلا لها، و ذلك من خلال الإعتداء على بياناتها و موقعها على شبكة الإنترنت، و كذا الإعتداء على بطاقات الائتمان كوسيلة سداد للتجارة الإلكترونية و كذا الإعتداءات الواقعة على التوقيع الإلكتروني كوسيلة للإثبات في هذا النوع من التجارة. و عليه قسمنا فصلنا هذا إلى ثلاث مباحث كالتالي:

المبحث الأول: جرائم الإعتداء على مواقع و بيانات التجارة الإلكترونية

المبحث الثاني: جرائم الإعتداء على بطاقات الائتمان

المبحث الثالث: جريمة العدوان على التوقيع الإلكتروني

المبحث الأول:

جرائم الإعتداء على مواقع و بيانات التجارة الإلكترونية

تعبر التجارة الإلكترونية الواقعة عن طريق الإنترنت عن نظام معلوماتي يحوي بيانات و معلومات و أموال تتدفق عبر تلك الشبكة. لكنه و لسوء الحظ أصبحت هذه الأخيرة عرضة لاعتداءات غير مشروعة من قبل مريضي الأنفس، و منها تلك الإعتداءات التي تقع على المواقع الإلكترونية و بيانات تلك التجارة. وهذا ما شعر به المجتمع الأوربي و أكده و خاصة بعد الإعتداءات الحديثة التي شهدتها مواقع الإنترنت التجارية أمازون دوت كوم. الأمر الذي فطن ذلك المجتمع بوجود مخاطر تواجهها تلك الشبكة و شبكات الكمبيوتر إلى جانب ضرورة تصنيفهم لجرائم الكمبيوتر باعتبارها تهدد التجارة والمصالح الحكومية[1].

و أمام هذه المخاطر التي تهدد التجارة الإلكترونية و تعيق تقدمها و ازدهارها تدخل المشرع الجنائي للحد منها،و حرص على توفير حماية جنائية لمواقع التجارة الإلكترونية، و ذلك من ناحيتين: الأولى تتبلور في تجريم الدخول العمدي و البقاء غير المشروع في نظام معالجة البيانات. و أما الثانية فتتمثل في تجريم الإعتداء على نظام معالجة البيانات التي يحتويها النظام أو التلاعب بها أو إعاقة أو تحريف تشغيل النظام.

و تجدر الإشارة إلى أن السلوك الإجرامي في هذه الجريمة يتمثل في الدخول غير المشروع على نظم معالجة البيانات و كذلك إعاقة أو تحريف تشغيل نظم معالجة البيانات، و كذلك التلاعب في بيانات نظم معالجة هذه البيانات. و هذه الصور للسلوك الإجرامي تندرج ضمن جريمة يطلق عليها "جرائم الإعتداء على نظم المعالجة الآلية للبيانات" و التي تقع على مواقع التجارة الإلكترونية أو غيرها من المواقع على شبكة الإنترنت. أما جرائم الإعتداء على بيانات التجارة الإلكترونية فتشمل جريمة التعامل في البيانات بدون ترخيص، جريمة انتهاك سرية و خصوصية البيانات، جريمة التصريح عمدا بمعطيات خاطئة.

---

[1]– د/ مدحت رمضان: الحماية الجنائية لموقع الإنترنت... و محتوياته، مجلة التشريع، السنة الأولى، العدد الثاني، جويلية 2004، ص39.

و سيتم تناول ذلك من خلال تقسيم هذا المبحث إلى المطلبين التاليين كمايلي:

المطلب الأول: جرائم الإعتداء على مواقع التجارة الالكترونية.

المطلب الثاني: الجرائم المتعلقة بتداول البيانات الخاصة بالتجارة الالكترونية.

المطلب الأول:

جرائم الإعتداء على مواقع التجارة الإلكترونية

حرص المشرع المعاصر على حماية مواقع التجارة الإلكترونية و ذلك من ناحيتين: الأولى تجريم الدخول العمدي (الاختراق) أو البقاء غير المشروع في نظام معالجة البيانات. و الثانية تجريم الإعتداء على نظام معالجة البيانات.و سيتم تفصيل ذلك في الفرعين التاليين:

الفرع الأول: جريمة الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات.

الفرع الثاني:جريمة الاخلال بنظام المعالجة الآلية.

الفرع الأول: جريمة الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات.

وسنتطرق تحت هذا الفرع إلى تعريف هذه الجريمة ثم إلى تحديد أركانها فتوضيح موقف التشريعات المقارنة منها. و ذلك على النحو التالي":

أولا: تعريف جريمة الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات.

لقد حرصت التشريعات الجنائية على تجريم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات، فجرم الدخول العمدي غير المصرح به إليها، كما جرم البقاء فيها بغير تصريح و هو الذي قد حصل بعد دخول مشروع. و هذا التجريم يشمل الدخول و كذا البقاء في كل أو جزء من هذا النظام، و بصرف النظر عن الغاية التي يهدف إليها الجاني. و كذلك بصرف النظر عما إذا كان النظام محميا بجهاز للأمن أم لا. وتعرف نظم معالجة البيانات حسب تعريف مجلس الشيوخ الفرنسي بأنها: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، و التي تتكون كل منها من الذاكرة و البرامج و المعطيات و أجهزة الإدخال والإخراج و أجهزة الربط،و التي يربط بينها مجموعة من العلاقات التي يتم عن طريقها تحقيق نتيجة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام المعالجة الفنية"[1].

وتتحقق هذه الجريمة سواء نتج عن هذا التواجد غير المشروع داخل النظام ضرر من نوع معين كالتخريب مثلا أم لم ينتج[2]. و هذا ما أقرته أغلبية نصوص التشريعات الجنائية المقارنة، اذ صنفت جريمة الدخول أو

---

[1]– د/ عبد الفتاح بيومي حجازي: الحماية الجنائية للتجارة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، 2001، ص329.

[2]– لمزيد من التفاصيل ينظر د/ عبد الفتاح بيومي حجازي، نفس المرجع، ص342 وما بعدها.

البقاء غير المشروع في نظام معالجة البيانات ضمن الجرائم الشكلية (جرائم الخطر) و الوك المؤثم و هو هنا الدخول أو البقاء غير المشروع في النظام بطريقة عرضية و غير مقصودة. [1]

هذا من جهة و من جهة أخرى، يشترط لقيام هذه الجريمة أن يقع الدخول أو البقاء غير المصرح بهما من أشخاص لا يملكون حق الدخول إلى هذه الأنظمة.[2]

ثانيا: أركان جريمة الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات

وعلى أية حال فإن هذه الجريمة تتكون كغيرها من الجرائم من أركان نتناولها كالتالي:

1/ الركن الشرعي، و الذي يتمثل في النصوص العقابية التي تجرم مثل هذه السلوكات غير المشروعة و الذي سيتم التفصيل فيا فيما بعد. [3]

2/ الركن المادي ويأخذ فيه السلوك الإجرامي صورتي الدخول والبقاء غير المشروع.

أ- **الدخول بدون وجه حق إلى النظام:** و يعني به ولوج الجاني إلى الحاسب بصورة غير مشروعة،أو هو إساءة استخدام الحاسب الآلي و نظامه عن طريق شخص غير مرخص له باستخدامه. و الدخول إليه للوصول إلى المعلومات و المعطيات المخزنة بداخله للإطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي[4]. و يعتبر الدخول على النظام من الجرائم الوقتية (infractions instantanées) ، أي من الجرائم التي تستلزم قيام الجاني بسلوك آني يبدأ و ينتهي في الحال[5]. و تقع الجريمة من أي شخص رجل، امرأة، طفل(بالغ أو حدث) محترف أو غير محترف، عامل في المؤسسات الضخمة أو غير عامل بها، و مهما كان قصده سواء أكان الدخول للقيام بعمل غير مشروع أو لمجرد الفضول و حب الاستطلاع[6]. ويتحقق الدخول غير المشروع متى كان مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه. كتلك الأنظمة المتعلقة بأسرار الدولة أو دفاعتها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة، والتي لا يجوز الإطلاع عليها. و يكون كذلك في الحالة التي يضع فيها مالك النظام قيودا للدخول إلى ذلك الأخير ولم يحترم الجاني ذلك، أو تعلق الأمر بسداد مبلغ من النقود لم يسدده ذلك الأخير، وقام بالدخول غير المشروع لهذا النظام[7]. كما يتحقق متى دخل الجاني إلى النظام كله أو جزء منه. كالدخول إلى طرفية الحاسب أو شبكة الاتصال أو البرامج. وكذلك يتحقق الدخول غير المشروع متى كان مسموحا للجاني بالدخول لجزء معين في البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له

---

[1]- د/ شيماء عبد الغني محمد عطا الله: الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص97. و ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة...) مرجع سابق، ص331.

[2]- محمد سامي الشوا: ثورة المعلومات و انعكاستها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998، ص71 .

[3]- ينظر ص 272 من هذه الرسالة.

[4]- د/ عصام عبد الفتاح مطر، المرجع السابق، ص307-308.

[5]- د/ مدحت عبد الحليم رمضان، (الحماية الجنائية للتجارة الإلكترونية) مرجع سابق، ص51.

[6]- Hemy ALTERMAN: la fraude informatique، GP ،p530

و ينظر د/ عصام عبد الفتاح مطر، المرجع السابق، ص308.

[7]- د/ علي عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون و الكومبيوتر والإنترنت، كلية التشريعية و القانون، جامعة الإمارات، دولة الإمارات العربية، 2000، ص50-51.

بالدخول فيه. و لذلك فلو فرض أن الجاني دخل على موقع "أمازون دوت كوم" و الذي يعتبر موقع للبيع الإلكتروني معد للجمهور، لكنه تجاوز الموقع إلى البيانات الخاصة بإعداد الموقع و تنظميه، في صفحة "Home Borg" و التي تنطوي على معلومات لا يجوز للجمهور الدخول عليها، و بالتالي يكون فعل الجاني مكونا لجريمة الدخول غير المشروع، رغم انفتاح ذلك الموقع على الجمهور[1]. و لذلك يخرج من نطاق الدخول غير المشروع، الدخول إلى برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه. كما لا تتوافر الجريمة إن اقتصر دور الجاني على مجرد قراءة الشاشة، إذ بهذه الأفعال لا تقوم جريمة الدخول غير المشروع إلى النظام المعلوماتي[2].

هذا من جهة و من جهة أخرى، فإن الدخول إلى النظام يجوز بأي وسيلة تقنية كالدخول عن طريق استخدام كلمة السر الحقيقية- إذا لم يكن للجاني الحق في استخدامها- أو باستخدام برنامج أو شفرة خاصة[3]، أو عن طريق استخدام الرقم الكودي لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول، و سواء تم ذلك عن طريق شبكات الاتصال التليفونية أو لطرفيات محلية أو عالمية[4].

و تجدر الإشارة هنا أنه من أكثر التقنيات استخداما لارتكاب جريمة الدخول غير المشروع للنظام:

- استخدام البرامج المخصصة لتخطي أنظمة الحماية الفنية في الحالات الطارئة،إذ على الرغم من ضرورة تزويد الحاسبات ببعض أنظمة الحماية الفنية للحيلولة دون الاتصال غير المشروع بالبرامج و البيانات المخزنة،إلا أن إدارة و تشغيل البيانات و الحاسبات بطريقة آمنة خاضعة للتحكم و السيطرة تقتضي وجود نوع من البرامج يمكن استخدامه لتجنب تخطي حواجز الحماية الفنية لمنظومات الحاسب في الحالات الطارئة و حالات اختلال وظائف الحاسب أو توقفه عن العمل.[5]

-أبواب المصيدة (Trap-Doors): من الأمور الشائعة التي يقوم بها واضعي البرامج أن يتركوا فواصل في البرامج أثناء إعدادها تسمى أبواب المصيدة تستخدم في إضافة ما يحلو لهم من أوجه التلاعب، و يتم ذلك أثناء قيامها بالمعالجة النهائية على اعتبار أن هذا شيء عادي.[6]

---

[1]- د/ مدحت عبد الحليم رمضان، (الحماية الجنائية للتجارة الإلكترونية.)مرجع سابق، ص53.

[2]- د/ عبد الفتاح بيومي حجازي، (الحماية الجنائية لنظام التجارة الإلكترونية) مرجع سابق، ص338.

وتجدر الإشارة إلى أن الدكتور مدحت عبد الحليم رمضان قد أضاف حالة أخرى للدخول غير المشروع و هي حالة الدخول بطريق الصدفة أو الخطأ أو السهو، و إن كان القانون الجنائي لا يعاقب سوى على الدخول العمدي، على عكس ما يراه جانب من الفقه إذ يعتبرون أن هذا النوع من الدخول هو مشروع، بشرط أن يكون من واجب الفاعل عندئذ أن يقطع تواجده وينسحب فورا فإذا بقي رغم ذلك يعاقب. د/ مدحت عبد الحليم رمضان، (الحماية الجنائية للتجارة الإلكترونية) مرجع سابق، ص52.

[3]- د/ مدحت عبد الحليم رمضان،نفس المرجع، ص51.

[4]- د/ علي عبد القادر القهوجي،(الحماية الجنائية للبيانات المعالجة إلكترونيا) مرجع سابق، الموضع السابق.

[5]- لمزيد من التفاصيل ينظر آمال قارة، المرجع السابق، ص108.

[6]- لمزيد من التفاصيل ينظر د/جميل عبد الباقي الصغير:جرائم التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، ص 54.

– **صناديق القمامة (Poubelle)**:تلقى عادة في سلة المهملات أوراق الكربون أو أوراق عادية تحتوي على بيانات أو حتى أشرطة مغناطيسية من قبل العاملين في أقسام الخلية الالكترونية بواسطة مهندس الصيانة الدورية للأجهزة و طبيعي لذلك استخدام هذه الملحقات أول بأول.

– **طريقة المختصرات (le raccourci)**: و تتمثل هذه التقنية في استغلال نقاط الضعف الخاصة بالنظام الداخلي للرقابة.

– طريقة القناع (le déguisement): و ذلك بأن يقوم القرصان بإقناع الحاسوب بأنه شخص مرخص له بالدخول.

– **طريقةActe Asynchrone**: و تتمثل هذه التقنية في استعمال نقاط الضعف الموجودة على مستوى نظام الاستغلال.[1]

ب– البقاء بدون وجه حق في النظام: و يقصد به بقاء المتهم داخل نظام للكمبيوتر بعد دخوله إليه عرضا و بطريق الخطأ[2]. ويعني أيضا دخول المتهم النظام بطريق مشروع ولكنه يستمر بعد الوقت المحدد لبقائه فيه، أو هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[3]. فالبقاء هنا يتمثل في عدم قطع الفاعل الاتصال بالنظام عند إدراكه بأن وجوده غير مشروع؛ فهو يبدأ من اللحظة التي كان يجب على الشخص فيها أن يغير وضعه بالخروج من النظام. وكثيرا ما يحدث ذلك إذا كان استعمال النظام محددا بوقت معين نظير أجر مالي، و يتخطى الفاعل هذا الوقت. أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والإطلاع فقط. ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التليفونية، و التي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه، أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة[4]. و البقاء داخل النظام يفترض

---

[1]– لمزيد من التفاصيل ينظر آمال قارة، المرجع السابق، الموضع السابق.

[2]– د/ شيماء عبد الغني محمد عطا الله، المرجع السابق، ص121.

[3]– د/ علي عبد القادر القهوجي،(الحماية الجنائية للبيانات المعالجة إلكترونيا) مرجع سابق، ص52.

[4]– و قد أعمل القضاء الفرنسي تجريم البقاء في النظام في قضية تتلخص وقائعها في قيام بعض العاملين في شركة الخطوط التليفونية باستعمال تلك الخطوط– دون دفع المقابل المالي– للقيام بألعاب "الفيديوجيم" للحصول على جوائز مقررة لمن يستمر في اللعب مدة معينة. و قد أعمل هذا القضاء وصف البقاء في النظام بطريق الغش، و ليس وصف الدخول في النظام، حيث أن هؤلاء العاملين كان من حقهم الدخول في النظام أصلا لمراقبته و الإشراف عليه و إصلاح أعطاله.
كما أنزل القضاء الفرنسي هذا الوصف على من عمد إلى إرسال وسائل وهمية إلى شركة من الشركات التي تتولى تقديم خدمات التيليماتيك بغرض شغل شبكة التليفونات التي يستعملها زبائن تلك الشركة، إضرارا بمصالحها. كما أدى تدخل المتهمين إلى خلق ازدحام في صناديق بريدها الإلكتروني بهذه الرسائل الفارغة أو المضللة، مما تسبب في اضطراب علاقة تلك الشركة بزبائنها. و قد قصد المتهمون إلى تحقيق الغاية سعيا إلى حمل زبائن تلك الشركة إلى شركتهم التي تعمل في نفس المجال أيضا. و قد جاء انتهاء القضاء الفرنسي إلى وقوع جريمة البقاء في النظام بنية الغش و ليس إلى وقوع جريمة

اختلاس وقت النظام و يتخذ صورة الجريمة المستمرة[1]. و يمكن أن يكون البقاء لاحقا على دخول غير مشروع و ذلك في الفرض الذي لا يكون للجاني فيه الحق في الدخول إلى النظام، و يدخل إليه فعلا ضد إرادة من له حق السيطرة عليه ثم يبقى داخل النظام بعد ذلك. و يتحقق في هذا الفرض الاجتماع المادي بين الجريمتين[2]. و يكفي لقيام هذه الجريمة، البقاء داخل النظام كله أو في جزء منه بذات المعنى السابق. فلا يشترط أن يضاف إليه ضرورة التقاط معلومات أو أي شكل من أشكال الضرر[3]. و يرجع السبب في تجريم هذه الجريمة إلى أن النص الذي يتضمن تجريمها يعتبر نصا احتياطيا بالنسبة لتجريم الدخول غير المشروع إلى النظام، فلا تنسب جريمة البقاء إلى من قام بالدخول إلا إذا بقي داخل النظام و انصرفت إرادته إلى ذلك. و ذات الحكم ينصرف إلى من هو مسموح له بالدخول إلى جزء من النظام ثم يدخل إلى جزء آخر غير مصرح له الدخول فيه[4]. و الأمر في ذلك يتماثل مع تجريم إخفاء الأشياء المسروقة بالنسبة لجريمة السرقة نفسها، فالفاعل في جريمة السرقة الذي يحتفظ بالمسروقات لا ينسب إليه أنه قام بجريمة أخرى هي إخفاء المسروقات[5]. و إذا كانت هذه الجريمة تهدف أساسا إلى حماية نظام المعالجة الآلية بصورة مباشرة،إلا أنها تحقق أيضا و بصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها. بل يمكن من خلالها تجريم سرقة وقت الآلة، و ذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له حق السيطرة على النظام، و يقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج[6].

الدخول في النظام بدون وجه حق، استنادا إلى أن الجمهور من حقه أن يدخل في النظام للاتصال بمراكز هذه الخدمات. د/ شيماء عبد الغني محمد عطا الله، المرجع السابق، ص121-122.

[1]- د/ جميل عبد الباقي الصغير، (القانون الجنائي و التكنولوجيا الحديثة) مرجع سابق، ص150.

و تجدر الإشارة إلى أن الفقه قد اختلف حول طبيعة هذه الجريمة من وقيته أو مستمرة أو متتابعة الأفعال. لمزيد من التفاصيل ينظر آمال قارة، المرجع السابق، ص112. و كذا د/عصام عبد الفتاح مطر، المرجع السابق، ص315. و د/ شيماء عبد الغني محمد عطا الله، المرجع السابق، ص123. فيما يخص أهمية طبيعة هذه الجرائم.

[2]- هناك من الفقه من يرى بوجود تعدد معنوي في فعلي الدخول غير المشروع و البقاء غير المشروع، و هناك من يرى بعدم وجود التعدد المعنوي. لمزيد من التفاصيل ينظر د/ عبد الفتاح بيومي حجازي، (الحماية الجنائية لنظام التجارة الإلكترونية) مرجع سابق، ص340.

[3]- د/ علي عبد القادر القهوجي، (الحماية الجنائية. للبيانات المعالجة إلكترونيا)مرجع سابق، ص53.

[4]- و لذلك هناك في الفقه من يرى أن هذه الجريمة تقوم بسلوك سلبي، فرغم دخول الجاني مصادفة، و رغم علمه بأن ذلك غير مشروع فهو يرفض الخروج من النظام، و بمعنى آخر يمتنع عن الخروج من النظام. لذلك قال جانب من الفقه بقيام الجريمة بسلوك سلبي، ينظر د/ أحمد حسام طه تمام، المرجع السابق، ص299.

[5]- Roger MERLE ،André Vitu: Traité de droit criminel, droit pénal spécial,éd Cujas,1982 ، p2001.

[6]- آمال قارة، المرجع السابق، ص111.

3/ الركن المعنوي

تعتبر جريمة الدخول أو البقاء غير المصرح بهما في صورتهما البسيطة أو المجردة جريمة عمدية تقوم على القصد الجنائي العام و لا تتطلب قصدا خاصا. و على ذلك فيجب أن يشمل علم الجاني كل واقعة تدخل في تكوين جريمة الدخول و البقاء، فيتعين أن ينصرف علمه إلى أن فعله ينصب على نظام للمعالجة الآلية للمعطيات و البيانات. و كذا إلى أن دخوله هذا و بقاءه في هذا النظام يكتسي الصفة غير المشروعة.ضف إلى ذلك فلا بد من توافر الإرادة المقتصرة على إرادة السلوك الإجرامي المكون للجريمة بكل مقوماته. [1]

ثالثا: موقف التشريعات المقارنة من جريمة الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات.

و نظرا لخطورة هذه الجريمة فقد تدخلت مختلف التشريعات و عاقبت عليها. فأما فيما يخص موقف الاتحاد الأوروبي من هذه الجريمة، فلقد أكد ذلك الأخير على أن الإعتداءات الحديثة على مواقع الإنترنت التجارية مثل أمازون دوت كوم amazon.com هي التي وجهت نظر المجتمع الدولي إلى المخاطر التي يواجهها الإنترنت و شبكات الكمبيوترات و أن جرائم الكمبيوتر تهدد التجارة و المصالح الحكومية، و قد أخذ المجلس الأوروبي زمام المبادرة و وضع مشروعا لاتفاقية تتعلق بجرائم الكمبيوتر مع الأخذ في الإعتبار الطابع الدولي الغالب لمثل هذه الجرائم.و لقد وجه المشروع الدول المتعاقدة على المستوى الداخلي إلى أن تجرم أفعال الإعتداء على سرية و تكامل بيانات الكمبيوتر و أنظمته و الاتصال بها، و حدد المشروع من هذه الأفعال الدخول العمدي غير المشروع على نظام الكمبيوتر بصورة كلية أو جزئية. و أعطى المشروع للدول المتعاقدة خيار أن تضيف شرطا للعقاب، و هو أن يكون الدخول باختراق إجراءات تأمين النظام أو بنية الحصول على بيانات معينة أو لأي غرض آخر غير مشروع (المادة 2 من المشروع)[2].

أما **بالنسبة للتشريعات الغربية** و التي نبتدؤها **بالمشرع الفرنسي** فقد عالج جرائم أنظمة معالجة البيانات في المواد 323-1 إلى 323-7، و تعاقب المادة الأولى منه (323-1) على الدخول بطريق الغش أو التدليس على نظام للمعلومات أو ابقاء الاتصال بطريقة غير مشروعة بالحبس لمدة سنتين و بغرامة 30 ألف يورو. وتكون العقوبة الحبس لمدة ثلاث سنوات و غرامة 45 ألف يورو إذا ترتب على نشاط الجاني إلغاء أو تعديل البيانات الموجودة بالنظام أو تعديل أو تشغيل النظام[3].

---

[1]- آمال قارة، المرجع السابق ، ص 115.

[2]- لمزيد من التفاصيل ينظر د/ مدحت عبد الحليم رمضان،(الحماية الجنائية..) مرجع سابق، ص38 و ما بعدها.

[3]-323-1 : " Le fait d'accéder ou de se maintenir، frauduleusement، dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

و الحال ذاته بالنسبة **للمشرع الأمريكي** و الذي كان السباق في تقرير العقاب على هذه الجريمة و ذلك منذ عام 1984 عند صدور قانون تزييف آليات الدخول و الإساءة و الاحتيال عبر الحاسوب. ثم قرر عام 1986 استثناء على ما هو مقرر في المادة 1/4 القسم "1030"[1] من التقنين الأمريكي –فيما يتعلق باستخدام الحاسوب– أن مسالة استهلاك وقت الحاسوب يشكل انتهاكا يمكن أن يصل إليه الاتهام الجدي في هذا الإطار. ثم في عام 1994 وسع في جريمة الدخول غير المصرح به لتطأ المسائلة العاملين داخل المؤسسة و المستخدمين غير المصرح لهم. أما في عام 1996 فقد مس التعديل الأفعال التي يعدها القانون الأمريكي أشكالا للاختراق من خلال حاسوب مستخدم في مؤسسة مالية أو من قبل الحكومة. أما في عام 2001 فقد جيء بتعديل استخدم من خلاله المشرع الأثر السيئ للإرهاب في سياسته التشريعية، من خلال تعديل نص القسم 1030 لكي يأخذ في الإعتبار قوة الهجمات الإرهابية عبر الإنترنت، و لقد تضمن هذا التشريع صلاحيات للسلطات على الحصول على الأدلة تتجاوز تلك التي كانت لهم سابقا.

و من ثم فإنه وفقا للقسم 1030 في شكله النهائي يعاقب على الأفعال التالية:

أ–الدخول على جهاز كمبيوتر يستخدم في التجارة أو الاتصال بين الولايات و القيام عمدا بنقل برنامج أو معلومة أو كود كمبيوتر أو نظام كمبيوتر.

ب–ارتكاب أفعال يكون من شأنها المنع أو التسبب في منع أو حرمان الغير من استعمال كمبيوتر أو خدمات كمبيوتر أو نظام أو شبكة أو معلومات أو بيانات أو برنامج.

ج–اختلاس مكونات لبرامج أو معلومات أو كود أو أمر دون موافقة من المسؤولية على الكمبيوتر المستقبل للبرنامج أو المعلومات أو الكود أو الأمر إذا أدى هذا النقل إلى خسائر لشخص أو أكثر تبلغ ألف دولارا أو أكثر خلال فترة سنة من ارتكاب الفعل، أو إذا أدت إلى تعديل أو إفساد كلي أو جزئي لكشف طبي أو تقرير طبي أو علاج طبي أو الرعاية الصحية لشخص أو أكثر.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système ،soit une altération du fonctionnement de ce système، la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat، la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende".

أما المشرع البلجيكي فقد جرم في المادة 1/550 من القانون الصادر في 2000/11/28 (المعدل لقانون العقوبات البلجيكي) فعل الدخول غير المصرح به في النظام المعلوماتي. و في اليابان، أصدر المشرع الياباني قانون الدخول غير المشروع إلى الحاسوب رقم 128 لسنة 1999، و خص المواد 3،4،8 و 9 من القسم الثالث منه لمعالجة موضوع العدوان على وسائل الاتصال بالإنترنت. لمزيد من التفاصيل ينظر د/ عصام عبد الفتاح مطر، المرجع السابق، ص312–313.

[1]– ينظر نص القسم 1030 من التقنين الأمريكي ص463 من هذه الرسالة.

د-اختلاس برامج أو معلومات أو كود أو أمر بطريق الكمبيوتر لجهاز يستخدم في التجارة أو الاتصال بين الولايات، و يشكل الفعل خطورة ان النقل أو الاختلاس أضر او تسبب في الإضرار لكمبيوتر أو نظام كمبيوتر أو شبكة أو معلومة أو بيان أو برنامج، و كان ذلك بدون تصريح من الجهات المسؤولة.

و-غش كلمات المرور بما يسمح بالدخول على نظام الكمبيوتر، دون تصريح بما يؤدي إلى الإضرار بالتجارة بين الولايات أو بالتجارة الخارجية[1].

أما بالنسبة **للتشريعات العربية** فسارت على ذات النهج في تقرير التجريم و العقاب على هذه الجريمة ومنها نظام مكافحة الجرائم المعلوماتية لسنة 2007 في **المملكة العربية السعودية** إذ نص على تلك الجريمة في مادته 3/3[2].

أما في **الإمارات العربية المتحدة** فقد جرم المشرع الإماراتي تلك الأفعال في المادة 1/2[3] من القانون الاتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات. أما في **الجزائر** فقد نص المشرع الجزائري على هذه الجريمة في المادة 394 مكرر من قانون العقوبات.[4]

و من خلال استقرائنا لنص هذه المادة يتضح لنا أن المشرع الجزائري قسم جريمة الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات إلى صورتين، صورة بسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع و صورة مشددة تتحقق بتوافر الظرف المشدد لها[5]، و يكون في الحالة التي ينتج

---

[1]- ينظر د/ عصام عبد الفتاح مطر، المرجع السابق، ص310-311 و كذا د/مدحت عبد الحليم رمضان، (الحماية الجنائية...) مرجع سابق، ص41 و ما بعدها

[2]- تنص المادة 3/3 من نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2007 على :" يعاقب بالسجن مدة لا تزيد على سنة و بغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:.....

3- الدخول غير المشروع إلى موقع إلكتروني أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه، أو تعديله أو شغل عنوانه".

[3]- تنص المادة 1/2 من القانون الاتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات علي: "كل فعل عمدي يتواصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به يعاقب عليه بالحبس و بالغرامة أو بإحدى هاتين العقوبتين".

[4]- تنص المادة 394 مكرر من قانون العقوبات الجزائري على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 دج إلى 150000دج".

[5]- الظرف المشدد الذي يشترطه المشرع الجزائري لقيام جريمة الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات في صورتها المشددة هو ظرف مادي يكفي أن توجد بينه و بين الجريمة العمدية الأساسية علاقة سببية للقول بتوافره إلا إذا أثبت الجاني إنتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ. آمال قارة، المرجع السابق، ص 114.

فيها عن الدخول أو البقاء غير المشروع إما محو أو تغير في المعطيات الموجودة في النظام أو تخريب لنظام أشغال المنظومة و قرر لها عقوبات في صورتيها. فأما البسيطة فعقوبتها الحبس من ثلاثة أشهر إلى سنة و بغرامة مالية تقدر ما بين 50000 إلى 100000دج[1]. وأما العقوبات المقررة لها في صورتها المشددة هي الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 دج إلى 15000دج[2].

الفرع الثاني: جريمة الإخلال بنظام المعالجة الآلية.

و على غرار الفرع الأول سيتم تعريف هذه الجريمة و تبيان أركانها، ثم تحديد موقف التشريعات المقارنة منها، و ذلك كمايلي:

أولا: تعريف جريمة الإخلال بنظام المعالجة الآلية وبيان أركانها.

و إلى جانب جريمة الدخول و البقاء غير المشروع في نظام المعالجة الآلية كنمط من أنماط السلوك الإجرامي الواقع على التجارة الإلكترونية، هناك اعتداءات تقع على محتوى البرامج التي تشمل المعلومات وذلك بإتلافها أو تعديلها أو حذفها. و هذا ما يطلق عليه "جريمة الإخلال بنظام معالجة البيانات[3] "

أو "جريمة الإعتداء العمدي على المعطيات"[4]. و الذي يأخذ فيها السلوك الإجرامي المكون لركنها المادي ثلاثة أفعال أو صور و هي: الإدخال غير المصرح به للمعطيات داخل نظام المعالجة الآلية للمعطيات (Intrusion) أو إزالة هذه المعطيات عن طريق محوها (l'effacement) أو تعديلها بغير تصريح (modification)، مع العلم بأن كل هذه الأفعال تؤدي إلى نتيجة واحدة تتمثل في المساس بسلامة وتكامل هذه البيانات.

هذا من جهة و من جهة أخرى، فإنه لا يشترط اجتماع هذه الصور لقيام الجريمة، بل يكفي لقيامها وقوع إحداهما. و أفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل.

و هذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد و هو المعطيات أو المعلومات التي تمت معالجتها آليا و التي أصبحت مجرد إشارات أو رموز تمثل المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة. كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزء منه.

و تجدر الإشارة هنا إلى أن الجريمة هذه لا تقع على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام، أي تلك التي دخلت و لم يتخذ حيالها إجراءات المعالجة الآلية. أما تلك التي في طريقها إلى المعالجة حتى

---

[1]– ينظر نص المادة394 مكرر/1 من قانون العقوبات الجزائري.

[2]– ينظر نص المادة394 مكرر/3 من قانون العقوبات الجزائري.

[3] – د/ عصام عبد الفتاح مطر، المرجع السابق، ص317.

[4]– آمال قارة، المرجع السابق، ص 120.

و لو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، و يكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال[1].

و عموما التلاعب في المعطيات الموجودة داخل النظام يتخذ إحدى الأشكال التالية:

1/ الإدخال (Intrusion):

و يقصد به إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أو كان يوجد عليها معطيات من قبل[2]. و تقع هذه الجريمة غالبا بمعرفة المسؤول عن القسم المعلوماتي و الذي يسند إليه وظائف المحاسبة و المعاملات المالية، لأنه يكون في أفضل وضع يؤهله لارتكاب هذا النمط من التلاعب غير المشروع.

و يصنف الفقه هذه الجريمة ضمن جرائم الغش المعلوماتي، الذي يتم فيه التلاعب بالبيانات و ذلك إما بإدخال معلومات مصطنعة، كقيام المسؤول المعلوماتي في المنشأة بضم مستخدمين غير موجودين بالفعل أو قيامه بالإبقاء على مستخدمين تركوا الوظيفة فعلا، أو إتلاف المعلومات الموجودة في النظام[3].و يتحقق فعل الإدخال – بصفة عامة– في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق في كل حالة يتم فيها إدخال برنامج غريب (كفيروس حصان طروادة أو أي قنبلة معلوماتية) يؤدي إلى إضافة معطيات جديدة[4]. كما قد يتم ارتكاب هذا الفعل في أولى مراحل تشغيل نظام معلومات الحاسوب، و قد يرتكب بعد بداية التشغيل[5].

2/ المحو (l'effacement):

و يقصد به إزالة جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[6]. و يمكن للمسؤولين عن حفظ البيانات – و بصورة مبسطة– أن يضيروا و يتلفوا المعلومات المكلفين بحفظها داخل جهاز الحاسب الآلي، و ذلك عن طريق إتلاف المعلومات أو محوها[7]. كذلك يرى جانب من الفقه الجنائي، أن محو البيانات المعالجة قد يتم عن طريق التلاعب في الشرائط الممغنطة. ففي فرنسا أخفقت عملية نصب قدرت بحوالي

---

[1]– آمال قارة، المرجع السابق، ص120–121.

[2]– د/ عبد القادر القهوجي،(الحماية الجنائية للبيانات الإلكترونية) مرجع سابق، ص59.

[3]– لمزيد من التفاصيل ينظر د/ محمد سامي الشوا، المرجع السابق، ص71 و ما بعدها.

[4]– لمزيد من التفاصيل ينظر د/ عبد الفتاح بيومي حجازي،(الحماية الجنائية لنظام التجارة الإلكترونية) مرجع سابق، ص355–356.

[5]– د/ عصام عبد الفتاح مطر، المرجع السابق، ص321.

[6]– د/ علي عبد القادر القهوجي،(الحماية الجنائية للبيانات الإلكترونية) مرجع سابق، الموضع السابق.

[7]– لمزيد من التفاصيل ينظر د/ محمد سامي الشوا، المرجع السابق، ص75.و د/ جميل عبد الباقي الصغير،(القانون الجنائي و التكنولوجيا الحديثة) مرجع سابق، ص34.

21 مليون فرنك فرنسي بسبب خطأ لمعلوماتي مبتدأ[1]. و من القضايا التي تتعلق بهذا الفعل قضية شركة Credit Company Data TRW الأمريكية.[2]

و تجدر الإشارة إلى أن فعل المحو هو مرحلة لاحقة على عملية إدخال المعطيات، فالمحو يفترض الوجود السابق لعملية الإدخال[3].

3/ التعديل (Modification):

و يقصد به تغيير المعطيات الموجودة داخل النظام و استبدالها بمعطيات أخرى[4]. أو هو تغيير لحالة المعطيات الموجودة بدون تغيير الطبيعة الممغنطة لها[5]. أو هو كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي[6].وقد يتم التلاعب في المعطيات عن طريق استبدال هذه المعطيات، أو عن طريق التلاعب في البرنامج و ذلك بإمداده بمعطيات مغايرة يؤدي لنتائج مغايرة عن تلك التي صمم البرنامج لأجلها[7]. و كقاعدة عامة يتحقق فعلي المحو و التعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديلها و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات – و سواء أكانت منطقية أو زمنية– و كذلك عن طريق برنامج الممحاة Gomme

---

[1]– ينظر لمزيد من التفاصيل عن وقائع القضية د/ عبد الفتاح بيومي حجازي،(الحماية الجنائية الإلكترونية) مرجع سابق، ص358.

[2]– تتلخص وقائع هذه القضية في أن هذه الشركة قامت تزويد عملائها (بنوك، شركات، متاجر) بمعلومات من خلال حاسباتها الآلية تتعلق بالمركز الائتماني لأفراد الجمهور نظير اشتراك يدفعه هؤلاء العملاء، و كانت هذه الشركة تضم في أنظمة حاسباتها معطيات تتعلق بحوالي 50 مليون شخص (عام 1976). و قد استغل موظف بالشركة يعمل كاتبا بقسم علاقات المستهلكين هذا النشاط و قام ببيع مراكز ائتمانية جديدة، و ذلك عن طريق محو المعطيات المتعلقة بالمراكز الائتمانية الرديئة و تعديلها و استبدالها بمعطيات يمليها أصحاب تلك المراكز لتحسن من مركزهم الائتماني، ليحصلوا على سجل ائتماني نظيف.و تجدر الإشارة إلى أن هذه العملية تضمنت مختلف أشكال التلاعب بالمعطيات (الإدخال، المحو، التعديل)، فهذا الموظف كان يزيل بعض المعطيات و يدخل محلها أخرى و يعدل معطيات ثالثة. و كانت نتيجة هذه التلاعبات أن تورط العديد من عملاء الشركة في معاملات مالية و تجارية مع أشخاص ذوي سمعة ائتمانية سيئة، و لو يتم اكتشاف هذه الجريمة إلا بعد تبليغ تقدم به أحد الأشخاص إلى مكتب التحقيقات الفيدرالي fbi بعدما تلقى عرضا من ذلك الموظف بتحسين سجله الائتماني مقابل مبلغ معين. د/ هشام فريد رستم،(قانون العقوبات و مخاطر..) مرجع سابق، ص187.

[3]– Raymond GASSIN: Fraude informatique, Rép.Pénal. Dalloz,1995, n°201, p32.

[4]– د/ علي عبد القادر القهوجي، (الحماية الجنائية للبيانات المعالجة إلكترونيا) مرجع سابق، ص59.

[5]– Raymons Gassin ،op cit ،n°202 ،p32.

[6]– د/ نائلة عادل فريد قورة: جرائم الحاسب الاقتصادية، دراسة نظرية و تطبيقية، دار النهضة العربية، القاهرة، 2004، ص220.

[7]– د/ عبد الفتاح بيومي حجازي، (الحماية الجنائية لنظام التجارة الإلكترونية) مرجع سابق، ص359.

d'effacement أو برنامج الفيروسات بصفة عامة[1]. و من الفيروسات التي تساهم في تعديل أو إتلاف النظام "حصان طروادة" و فيروس الدودة أو ما يسمى "بدودة موريس"[2].

و يجب التنويه في هذا الوضع إلى أن الصور الثلاثة المكونة للركن المادي لجريمة الإعتداء العمدي على المعطيات و ردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات. فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق[3]. وتصنف جريمة التلاعب بالمعطيات ضمن الجرائم المادية على عكس جريمة الدخول أو البقاء غير المصرح بهما، إذ لا يكفي أن تهدد سلامة المعطيات بخطر المحو أو التعديل و الإدخال، و إنما لابد أن يقع ضرر فعلي على هذه المعطيات يتمثل في تغيير حالتها. فالمشرع في مثل هذه الجريمة يتطلب نتيجة معينة من خلال السلوك الإجرامي فيها وهي تغيير حالة المعطيات[4]. و نتيجة جريمة التلاعب بالمعطيات بالنسبة للتعديل و المحو هي نفسها النتيجة التي يترتب عليها تشديد العقوبة في جريمة الدخول و البقاء غير المصرح بهما. و ما يميزهما أن هذه الأخيرة تتم دائما بعد دخول أو بقاء غير مصرح بهما كما أنها تكون غير عمدية، على عكس النتيجة في جريمة التلاعب التي قد تتم بعد دخول أو بقاء مصرح بهما أو غير مصرح بهما، و إنها دائما عمدية يقصد الجاني أحداثها[5].

وتعد هذه الجريمة من الجرائم العمدية التي تقوم على القصد الجنائي العام بعنصرية العلم و الإرادة و هي لا تتطلب قصدا جنائيا خاصا. فلابد أن يعلم الجاني أنه يقوم بإدخال أو محو أو تعديل غير مصرح به على معطيات للحاسب الآلي، و أن من شأن أفعاله هذه أن تؤدي إلى نتيجة هي تغيير حالة المعطيات، ولابد من إرادة الجاني لهذه النتيجة و ذاك السلوك[6].

ثانيا: موقف التشريعات المقارنة من جريمة الإخلال بنظام المعالجة الآلية

قررت التشريعات الجنائية باختلافها الحد من تلك الجريمة التي تؤثر سلبا في التجارة الإلكترونية و تعيق تطورها سواء الغربية أو العربية. فأما فيما يخص **التشريعات الغربية**، فقد نص **المشرع الفرنسي** على هذه

---

[1]– د/ علي عبد القادر القهوجي، (الحماية الجنائية للبيانات...) مرجع سابق، ص60.

[2]– د/ أحمد حسام طه تمام، المرجع السابق، ص360.

[3]– Voir CHAMOUX : la loi sur la fraude informatique ،de nouvelles incriminations ، JCP،1988، Doct 3321

[4]– Raymond Gassin ،op cit ،n°199 ،p32.

[5]– Xavier LINANT De BELLEFOND et Allan HOLLANDE :Pratique du droit de l' informatique et de l'internet, 6ème éd, Delmas, 2008, p239.

[6]– تتطلب بعض التشريعات توافر القصد الجنائي الخاص إلى جانب العام في جريمة التلاعب بالمعطيات كقصد الإضرار بالغير و قصد تحقيق ربح غير مشروع للجاني أو للغير كما هو الوضع في القانون البرتغالي و الفنلندي و التركي. لمزيد من التفاصيل ينظر د/ نائلة عادل قورة، المرجع السابق، ص228.

الجريمة بعد جريمة إعاقة و إفساد أنظمة المعالجة الآلية. فوفقا للمادة 2/323 من قانون العقوبات الفرنسي الجديد فإنه يتم تطبيق عقوبة الحبس لمدة خمس سنوات و غرامة 75000 يورو على كل من يعمل على إعاقة أو إفساد تشغيل نظام معالجة البيانات. كما تعاقب المادة 3/323 على كل إدخال بيانات في نظام معالجة البيانات أو إلغاء أو تعديل البيانات المثبة فيه[1].

أما فيما يتعلق **بانجلترا** فقد أصدر المشرع البريطاني قانون إساءة استخدام الحاسوب عام 1990 و جرم في المادة الأولى من القسم الثالث منه كل نشاط يسبب تعديل غير مصرح به في محتوى أي حاسوب[2].

أما فيما يتعلق **بالتشريعات العربية**، فقد عالجها **القانون الاتحادي الإماراتي** رقم 02 لسنة 2006 المتعلق بمكافحة جرائم تقنية المعلومات و ذلك من خلال نص المادة 2/2[3]. و الشأن ذاته بالنسبة **لنظام مكافحة الجرائم المعلوماتية لعام 2007 السعودي** و ذلك في مادته 3/3 و 1/5[4].

---

[1]-323-2 : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat، la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende ».

323-3: « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »

و في ذات المنوال أضاف المشرع البلجيكي بمقتضى القانون الصادر في 12/28 (200) مادة جديدة إلى قانون العقوبات البلجيكي برقم 210 مكرر نصت على أنه: "كل من يرتكب خطأ في نظام معلوماتي بإدخال أو تعديل أو إحداث أثر في معطيات متواجدة أو معالجة أو محولة بموجب نظام معلوماتي أو بإحداث تعديل بكل وسيلة تقنية في الاستخدام الممكن للمعطيات المتواجدة في نظام معلوماتي أو بتعديل المحتوى لهذه المعطيات، يعاقب بالسجن من ستة أشهر إلى 5 سنوات وبغرامة من 65 ألف فرنك إلى 100 ألف فرنك أو بالعقوبتين معا." د/ عصام عبد الفتاح مطر، المرجع السابق، ص319..

[2]- تنص المادة الأولى من القسم الثالث من قانون إساءة استخدام الحاسوب على أن: "كل شخص يعد مذنبا بجريمة إذا ارتكب أي نشاط يسبب تعديل غير مصرح به في محتوى أي حاسوب، في الوقت الذي يقوم فيه بذلك يكون لديه النية الضرورية و العلم الضروري".

[3]- تنص المادة 2/2 من القانون الاتحادي الإماراتي رقم 02 لسنة 2006 المتعلق بمكافحة جرائم تقنية المعلومات على: "إذا ترتب على فعل الدخول في نظام معلوماتي إلقاء أو حذف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب مرتكبها بالحبس مدة لا تقل عن ستة أشهر و بالغرامة أو بإحدى هاتين العقوبتين".

[4]- تنص المادة المادة الثالثة من نظام مكافحة الجرائم المعلوماتية لعام 2007 السعودي على: "يعاقب بالسجن مدة لا تزيد على سنة و بغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب فعل الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه". وتنص

و تعتبر جريمة التلاعب بالمعطيات الجريمة الثانية التي ينص عليها **قانون العقوبات الجزائري** بعد جريمة الدخول و البقاء غير المصرح بهما و ذلك من خلال نص المادة 394 مكرر1 قانون عقوبات جزائري[1] والمادة 394 مكرر2 .[2]

و باستقرائنا لنص هاتين المادتين نستخلص أن المشرع الجزائري ميز بين صورتين في الإعتداءات العمدية على المعطيات. فأما الصورة الأولى و الناصة عليها المادة 394 مكرر1 فالإعتداء فيها يقع على المعطيات الموجودة داخل النظام و الذي يتمثل النشاط الاجرامي فيها على ثلاث الصور التي تم تفصيلها سابقا. و هي: الادخال، المحو، التعديل. أما الصورة الثانية و الناصة عليها المادة 394 مكرر2 فيقع الإعتداء فيها على المعطيات الموجودة خارج النظام .

و تجدر الاشارة هنا أن المشرع الجزائري في الفقرة الأولى من هذه المادة استهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات. بينما نجده في فقرتها الثانية يجرم أفعال الحيازة أو الإفشاء أو النشر أو الاستعمال للمعطيات بغض النظر عن الهدف المبتغى من ذلك.

المطلب الثاني:الجرائم المتعلقة بتداول البيانات الخاصة بالتجارة الإلكترونية

ممارسة التجارة الإلكترونية يعني ممارسة العمليات التجارية عن طريق الوسائل الإلكترونية، و هذا يعني تبادل البيانات إلكترونيا و استخدام الوثائق الإلكترونية عن طريق مورد الخدمات الإلكترونية.

المادة 1/5 من ذات القانون على: "يعاقب بالسجن مدة لا تزيد على أربع سنوات و بغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب فعل الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها".

[1]– تنص المادة 394 مكرر1 من قانون العقوبات الجزائري على: "يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات و بغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

[2]– تنص المادة 394 مكرر2 من قانون العقوبات الجزائري على: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات و بغرامة 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

1 –تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2–حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم."

لذلك قد تتعرض عمليات التجارة الإلكترونية فيما يتعلق بتداول البيانات لاعتداء يتمثل في التعامل في البيانات بدون ترخيص أو انتهاك سرية و خصوصية البيانات أو جريمة التصريح عمدا بمعطيات خاطئة وسيتم التطرق إلى ذلك في الفروع التالية:

الفرع الأول: جريمة التعامل في البيانات بدون ترخيص.

الفرع الثاني: جريمة انتهاك سرية و خصوصية البيانات.

الفرع الثالث: جريمة التصريح عمدا بمعطيات خاطئة.

الفرع الأول: جريمة التعامل في البيانات بدون ترخيص

تعتبر جريمة التعامل في البيانات بدون ترخيص من الجرائم الشكلية التي تقوم كأي جريمة على ركنين ركن مادي و آخر معنوي. فأما الركن المادي لهذه الجريمة فيتوافر بمجرد تداول البيانات بدون ترخيص مسبق حتى و أن لم يترتب على ذلك أي نتيجة إجرامية. أي أن يتم تداول هذه البيانات بدون موافقة الجهة المختصة بمنح الترخيص و لشخص آخر أجنبي عن هذا التعامل. وأما فيما يخص الركن المعنوي فإن جريمة عدم الحصول على ترخيص من الجهة المختصة لتداول البيانات جريمة غير عمدية، لأن الشخص قد يخطئ في تداول ذلك البيانات بدون حصوله على الترخيص اللازم و بذلك يكون قد خالف اللوائح و القوانين في رصد صور الخطأ غير العمدي، و لكن قد يتعمد تداولها بدون ترخيص و هو على علم بذلك[1].

الفرع الثاني: جريمة انتهاك سرية و خصوصية البيانات

تعتبر هذه الجريمة كنظيرتها من الجرائم الشكلية التي يتحقق الركن المادي لها بمجرد إتيان السلوك الإجرامي دون اشتراط تحقق النتيجة. و هي بذلك تقوم على ركنين ركن مادي و ركن معنوي. فأما الركن المادي فيتحقق بمجرد انتهاك سرية البيانات و خصوصيتها، و السرية هنا تعني عدم معرفة الغير من غير المتعاقدين ببيانات العملية التجارية. أما الخصوصية فتعني بها ارتباط هذه البيانات بالمتعاقدين أطراف العملية التجارية مما يحتم عدم إطلاع الغير عليها.و تجدر الإشارة إلى أن الغرض من التجريم في هذه الجريمة هو الحفاظ على سرية و خصوصية البيانات. أما الركن المعنوي لهذه الجريمة فيتمثل في القصد الجنائي العام بعنصريه الإرادة و العلم أي أن هذه الجريمة تصنف ضمن الجرائم العمدية. [2]

الفرع الثالث: جريمة التصريح عمدا بمعطيات خاطئة

جريمة التصريح عمدا بمعطيات خاطئة تقتضي إعطاء معطيات غير صحيحة من جانب أي شخص، وتتعلق هذه المعطيات بالطبع بعملية التجارة الإلكترونية محل البحث سواء كان التصريح بهذه المعطيات الخاصة قد صدر إلى مورد خدمات التوثيق الإلكتروني أو إلى أطراف عملية التعاقد أو أي طرف آخر – كبنك– و كان يتعين على هذا الشخص الالتزام بصحة المعطيات التي صرح بها لثقة مورد الخدمة

---

[1]– د/ هدى حامد قشقوش، (الحماية الجنائية للتجارة الالكترونية عبر الإنترنت) مرجع سابق، ص39.

[2]– لمزيد من التفاصيل ينظر د/ هدى حامد قشقوش،(الحماية الجنائية للتجارة الالكترونية) مرجع سابق ، ص42.

الإلكترونية و كذلك الأطراف في توقيعه على غير ما صدر عنه. و هي كغيرها من الجرائم تقوم على ركن مادي يكفي لتوافره التصريح من جانب الجاني بمعطيات خاطئة بدون أن تتحقق النتيجة باعتبارها جريمة شكلية، يشكل النشاط الإجرامي في حد ذاته فيها جريمة دون الحاجة لاشتراط تحقق النتيجة. و ركن معنوي يتمثل في القصد الجنائي العام القائم على عنصري العلم و الإرادة، فلا يتصور أن تتحقق هذه الجريمة بصورة غير عمدية. إذ أن الإعطاء في حد ذاته يفيد معنى الإرادة و السعي و العلم معا[1].

العقوبات المقررة لهذه الجرائم:

لقد قرر التشريع التونسي على عكس التشريعات الأخرى معالجة موضوع التجارة الإلكترونية معالجة تفصيلية غطى بها كافة جوانب الموضوع و من ضمنها اهتمامه بتجريم الإعتداء على تداول البيانات بدون ترخيص و ذلك في نص المادة 46 منه و عاقب كل من تسول له نفسه فعل ذلك بعقوبة السجن مدة تتراوح بين الشهرين و ثلاث سنوات و غرامة من 1000 الى 10000 دينار أو احداهما.كما نصت المادة 4 منه على معاقبة كل من لم يراع قواعد كراسة الشروط المنصوص عليها بالقانون بالغرامة من 1000 الى 10000 دينار،وأضاف ذات القانون في المادة 44 منه على سحب الترخيص من مورد خدمات الوثائق الالكترونية و ايقاف نشاطه اذا أخل بواجباته التي نص عليها هذا القانون.

و كذا جرم فعل انتهاك سرية و خصوصية البيانات في نص المادة 52 منه و عاقب مزود أو مورد الخدمات الالكترونية و أعوانه الذين يفشون أو يحثون أو يشاركون في افشاء المعلومات التي عهدت اليهم. و كذاعاقب على جريمة التصريح عمدا بمعطيات خاطئة في المادة 47 منه و ذلك كالآتي:"يعاقب كل من صرح عمدا بمعطيات خاطئة لمورد خدمات التوثيق الالكتروني و لكافة الأطراف التي طلب منها أن تثق بامضائه بالسجن لمدة تتراوح بين 6 أشهر و عامين و بغرامة تتراوح بين 10000،1000 دينار أو احدى هاتين العقوبتين" [2].

---

[1]– د/ هدى حامد قشقوش، نفس المرجع ، ص45.

[2]– لمزيد من التفاصيل ينظر د/ هدى حامد قشقوش،(الحماية الجنائية للتجارة الالكترونية) مرجع سابق ، ص40–44–46.

المبحث الثاني:

جرائم الإعتداء على بطاقات الائتمان عبر الإنترنت.

لقد انتشر استخدام بطاقات الائتمان[1] في عصرنا هذا المعروف بعصر المعلوماتية و أصبحت تحتل مساحة كبيرة في تعاملات الأفراد على حساب باقي وسائل الدفع التقليدية الأخرى، إذ أصبح هؤلاء الأخيرين يعتمدون عليها تماما في حياتهم اليومية، لاسيما مع ظهور الإنترنت التي حولت العالم إلى قرية صغيرة والتي ساهمت في تسهيل معاملاتهم التجارية و المصرفية من بيع و شراء... عبرها[2]. و لكنها و في المقابل أتاحت الفرصة للمجرمين و العصابات الدولية لإساءة استخدام هذه البطاقات؛ إذ أصبحت تلك الشبكة تستعمل كأداة للاحتيال على نظام الدفع الإلكتروني الخاص بها بقصد تحقيق أرباح غير مشروعة. هذا ما أدى إلى ميلاد جرائم مستحدثة محلها تلك البطاقات و بيئتها الإنترنت تختلف عن نظيرتها التقليدية، لاعتبارها ظاهرة إجرامية ذات طبيعة خاصة يصعب كشفها و إثباتها و القبض على مرتكبها ذوي المهارات التقنية العالية و الذكاء الخارق، و لكونها متعدية الحدود فقد يتم سرقتها من هونكونج من شخص آمن موجود في أوربا دون الحاجة إلى الالتقاء بالضحية، و دون أن يدخل ذلك الجاني بيته أو يفتح خزانته، ودون أن يحمل سلاحا أو يريق قطرة دم.فكما يقول السيد آجون نيوتن فهي "جريمة سرقة عن بعد و في عالم الريموت كنترول تأتي السرقة بالريموت و لكن دون كنترول"[3]. وعليه قسمنا مبحثنا هذا إلى المطالب الآتية:

المطلب الأول: ماهية بطاقات الائتمان.

المطلب الثاني: ماهية جرائم الإعتداء على بطاقات الائتمان عبر الإنترنت.

المطلب الثالث:موقف التشريعات المقارنة من جرائم الإعتداءعلى بطاقات الائتمان عبر الإنترنت.

---

[1]– إذ أنه يوجد في الولايات المتحدة حوالي 185 مليون بطاقة أي بنسبة 63% من إجمالي عدد السكان. أما في الصين فإن حجم التعاملات المالية باستخدام بطاقات الائتمان قد تعدى الـ 169 مليار دولار أمريكي عام 2001 ، بحث الجريمة عبر الإنترنت، www.f-law.net //:http.

[2]– إذ أثبتت شبكة (MSNBC) عمليا سهولة الحصول على أرقام بطاقات الائتمان من الإنترنت، بحيث قامت بعرض قوائم على أكثر من 2500 رقم بطاقة ائتمان حصل عليها من سبعة مواقع للتجارة الإلكترونية باستخدام قواعد بيانات متوفرة تجاريا، و لم يكن يصعب على أي متطفل استخدام ذات الوسيلة البدائية للاستيلاء على أرقام تلك البطاقات و استخدامها في عمليات شراء يدفع قيمتها أصحابها الحقيقيين. محمد محمد عبد الله المنشاوي، بحث سابق، www.minshawi.com //:http.

[3]– لمزيد من التفاصيل ينظر د/ عماد على خليل، المرجع السابق، ص5.

المطلب الأول:

ماهية بطاقات الائتمان

و نتطرق تحت هذا المطلب إلى تعريف بطاقات الائتمان أولا، ثم نبين الخصائص التي تتميز بها هذه الوسيلة للدفع. و ذلك في الفرعين التاليين:

الفرع الأول: تعريف بطاقات الائتمان.

الفرع الثاني: خصائص بطاقات الائتمان.

الفرع الأول: تعريف بطاقات الائتمان.

لقد أدى التطور التكنولوجي الكبير في مجال الاتصالات و ظهور التجارة الإلكترونية و انتشارها الكبير واعتماد الكثير من الأفراد في شراء حاجاتهم عن طريق شبكة الإنترنت إلى امتداد نشاط بطاقات الائتمان[1] إلى هذه الشبكة باعتبارها وسيلة جديدة من وسائل الدفع التي أوجدها كثرة استخدام الحاسبات الآلية لاسيما في مجال القطاع المصرفي[2]، إذ تعتبر أداة دفع إلكترونية و سحب حديثة، تستخدم في بيئة إلكترونية، وظيفتها تحريك النقود التقليدية بين حسابات أطراف التعامل بها عبر شبكات الحاسب الآلي،أي أنها تقوم بتسوية المعاملات التجارية و البنكية بين الأفراد و البنوك طبقا لنظام التحويل الآلي للنقود، فهي عبارة عن بطاقة مستطيلة من البلاستيك تحمل اسم المؤسسة المصدرة لها و شعارها و توقيع حاملها[3]. و تقوم هذه

---

[1]– هناك الكثير من المصطلحات التي تطلق على هذه البطاقات كبطاقات الدفع الإلكتروني و النقود الائتمانية، و النقود البلاستيكية، و بطاقات الوفاء الحديثة و بطاقات الضمان، و النقود الإلكترونية و الحافظة الإلكترونية و الكروت ذات القيمة المحفوظة و النقود البولمرية و النقود الخاصة،ولكن المصطلح الأكثر شيوعا و الأشمل معنى بالنسبة لهذه البطاقات هو بطاقات الائتمان.

[2]– لقد ظهرت البطاقات الائتمانية لأول مرة في الولايات المتحدة الأمريكية قبل الحرب العالمية الأولى أي سنة 1914،ثم انتقلت بعد ذلك إلى أوروبا في عام 1963 عن طريق مؤسسة الأمريكان إكسبريس، والداينرز كلوب. أما بالنسبة للعالم العربي فإن دخول البطاقات لأسواقها جاء متأخرا. ينظر لمزيد من التفاصيل حول تطور بطاقات الائتمان د/ إيهاب فوزي السقا: الحماية الجنائية و الأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية،2007، ص30 و ما بعدها.

JAUFFRET.Alfred :Droit Commercial, 20 ème éd,LGDJ, Paris,1991,n°882,p 572.

[3]– د/ جميل عبد الباقي الصغير: المسؤولية الجنائية في مجال المعاملات الالكترونية، ورقة عمل مقدمة إلى دورة الجوانب القانونية و الفنية في المعاملات الالكترونية المنعقدة في الفترة من 8-2012/4/12، مركز البحوث و الاستشارات القانونية، كلية الحقوق، جامعة القاهرة، ص 5. و لقد اختلفت التعريفات الخاصة ببطاقات الائتمان و يمكن تقسيمها إلى ثلاثة أنواع (من حيث الشكل و اللغة و المضمون). لمزيد من التفاصيل ينظر د/ إيهاب فوزي السقا، المرجع السابق، ص11 و ما بعدها.

الأخيرة على فكرة الائتمان[1] الذي يحكمه مبدأ الحماية من جرائم السرقة بالإكراه[2] لافتراض وجود فاصل زمني بين تقديم مانح الائتمان لوسائل الوفاء لعملية الشراء و بين استرداد تلك الوسائل[3].

الفرع الثاني: خصائص بطاقات الإئتمان.

وتتصف بطاقات الائتمان بالعديد من الخصائص التي تميزها عن غيرها من وسائل الدفع والوفاء الأخرى[4] ومنها:

---

[1]– أصل كلمة الائتمان مأخوذة من كلمة الأمانة و هي الوفاء أو الوديعة و من مشتقاتها الاستئمان أي ائتمن فلانا، آمنه جعله أمينا على الشيء. و عرف بعض الفقهاء الائتمان بأنه:"التزام يقطعه مصرف لمن يطلب منه أن يجيز له استعمال مال معين نظرا التي يشعره بها نحوه." أو بأنه:"إعطاء حرية التصرف الفعلي و الحالي في مال عيني أو قوة شرائية في مقابل الوعد برد نفس الشيء أو مال معادل له خلال فترة زمنية معينة، نظير مقابل الخدمة المؤداة".أو هو:"مقايضة مال حاضر بمال مستقبل."ينظر على التوالي: د/ سليمان أحمد فضل، المرجع السابق، ص 168. د/ إيهاب فوزي السقا، المرجع السابق، ص13.

[2]– لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة...) مرجع سابق، ص418.

[3]– د/ عصام عبد الفتاح مطر، المرجع السابق، ص352.

[4]– و المقصود بوسائل الدفع الأخرى و الوفاء النقود و الشيك إلى جانب مجموعة من البطاقات المخصصة للتعاملات المالية. فهي تختلف عنهما في نقاط عديدة و لكن في المقابل تشترك معهما في:

كلا من النقود و بطاقات الائتمان وسيط للتبادل، فهما وسيلتان لنقل ملكية السلع و الخدمات من طرف إلى آخر.

و كلا من الشيك و بطاقات الائتمان يتم استخدامه في تداول نقود الودائع و نقل ملكيتها من شخص لآخر. كما أن كلاهما يشتركان في عدد أطراف التعامل بها.فالأولى هناك: مصدر للبطاقة و الحامل و التاجر و الثاني هناك: الساحب والمسحوب عليه و المستفيد.

هذا من جهة و من جهة أخرى فهي تختلف عنهما في:

أ- بالنسبة للنقود:

1- تعد النقود قيمة نقدية ذاتية: إذ يتخلى عنها صاحبها نهائيا للبائع مقابل السلع أو الخدمة التي يحصل عليها على عكس بطاقات الائتمان التي لا يستطيع حاملها التخلي عنها نهائيا للتاجر، فهي مجرد وسيلة تمكن البائع من الحصول على نقوده مقابل بيعه للخدمة أو السلعة لحامل البطاقة.

2- النقود هي أداة تخزين للقيمة إذ يستطيع حائزها الاحتفاظ بها مدة طويلة و اكتنازها لاستخدامها في المستقبل. فهذا ما يمكن تصوره في بطاقات الائتمان في المرحلة الحالية من مراحل تطورها.

3- تتمتع النقود بالقبول العام لدى المجتمع و تستمد سيادتها من الدولة، فلا يستطيع أحد التجار أن يرفض التعامل بالنقود الورقية، و العكس قد يرفض التاجر التعامل بالبطاقة.فضلا عن أن البطاقات تصدر من مؤسسات و جمعيات مالية هي الضامنة لها، و بالتالي فلا ينطبق على العديد منها جرائم التزييف و التزوير و التقليد للعملة المعدنية أو الورقية المنصوص عليها في قوانين العقوبات.

4- تتمثل النقود بصكوك محددة القيمة متساوية المقدار. و هذا لا يتفق مع طبيعة بطاقات الائتمان، لأنها تتعلق بحجم الائتمان و مدته الممنوحة لها، و هذا يبين مدى التباين في قيمتها.

5- تحكم ملكية النقود قاعدة مدنية معروفة ألا و هي الحيازة في منقول سند الملكية و هذا ما لا ينطبق على بطاقات الائتمان إذ لا يمكن نقل ملكيتها بل و حتى التنازل عنها.

1- بطاقات الائتمان تقوم على ثلاثية الأطراف: البنك المصدر و حامل البطاقة و التاجر.

2- البطاقة تعتبر أداة لوظيفة الائتمان.

3- التزام مصدر البطاقة بالوفاء نيابة عن حامل البطاقة للتاجر.

4- عدم خضوع البطاقة للنظام القانوني الخاص بوسائل الدفع الأخرى.

5- التعامل بالبطاقة يلزمه وجود أجهزة إلكترونية مساعدة تقرأ بياناتها مثل أجهزة السحب الآلي ATM ونقاط البيع بالتجزئة POS.

6-الصفة العالمية لهذه البطاقات بحيث يقبل التعامل بها في معظم أنحاء التصدر البطاقات مؤسسات مالية كالبنوك و المؤسسات المالية و التجارية.

7-تصدر البطاقات مؤسسات مالية كالبنوك و المؤسسات المالية و التجارية.

8- لا يفرض التعامل بهذه البطاقات على خلاف وسائل الدفع التقليدية الأخرى التي تقوم بإصدارها و يكون التعامل بها إجباريا بين المتعاملين.

6- تخضع النقود لنظام قانوني للإصدار، ورقابة مباشرة من البنك المركزي و الحكومة، أما البطاقات فتخضع لنظام تجاري.

7- النقود هي متاحة للجميع أما بطاقات الائتمان فيلزم شروطا و ضمانات معينة لإصدارها.

ب-بالنسبة للشيك:

1- من أهم خصائص الشيك أنه يتم تداوله بالطرق التجارية بين الأفراد و المؤسسات على عكس البطاقة. ضف إلى ذلك فإن محرر الشيك يتخلى عنه للمستفيد، الذي يقوم بتقديمه للبنك المسحوب عليه للحصول على قيمته أو إضافته لحسابه لدى البنك. أما حامل البطاقة فكما سبق ذكره في النقود لا يستطيع التخلي عنها نهائيا، و لكن يقدمها فقط للتاجر ثم يستعيرها مرة أخرى.

2- يعد البنك المسحوب عليه الشيك مدين لعميله دون أن يلتزم بالدفع عنه في حالة عدم وجود رصيد يكفي لسداد قيمته. أما في البطاقة فإن مصدرها يضمن الوفاء للعميل ما دام قد احترم حامل البطاقة و التاجر إجراءات التعامل وشروط العقد.

3- يتم استعمال الشيك في عملية تجارية واحدة ينتهي دوره بعدها، كما أنه محدد بقيمة محددة من النقود و تاريخ استحقاق. أما البطاقة فتستعمل أكثر من مرة، و تتمتع بضمان البنك المصدر.

4- يستخدم الشيك على المستوى المحلي أو المستوى الدولي في نطاق محدد جدا، أما في البطاقة فالمنظمات الراعية تضمن لها العالمية و القبول الدولي لدى جميع دول العالم. أما بالنسبة للبطاقات المخصصة للتعاملات المالية، فلكل منها آلية خاصة في التعامل و أهداف و منها: بطاقات الحساب و بطاقات الصرف الآلي و بطاقات ضمان الشيكات و البطاقة الذكية. ينظر على التولي: د/ إيهاب فوزي السقا، المرجع السابق، ص61 و ما بعدها، و أسامة أحمد المناعسة، جلال الزعي، صايل الهواوشة، المرجع السابق، ص173.

و تحمل بطاقات الائتمان العديد من المعلومات و البيانات المطبوعة بطريقة بارزة و متغلغلة في جسم البطاقة[1] و تتمثل في:

اسم حامل البطاقة: و يطبع على الوجه الأمامي للبطاقة بالحروف الانجليزية البارزة.

صورة حامل البطاقة: و ذلك للتأكد من شخصيته و منع الغير من استعمالها.

رقم البطاقة و رقم البنك المصدر لدى المؤسسة الدولية الراعية للبطاقة: و عادة ما يتكون من 14-18 رقما.

مدة الصلاحية: أي تحديد و إثبات تاريخ أول بدء التعامل بالبطاقة و تاريخ انتهاء البطاقة.

شريط التوقيع: و هو موجود على خلفية البطاقة، و يلزم البنك المصدر أن يوقع حامل البطاقة على هذا الشريط عند استلام البطاقة.

شريط الممغنط: و يدخل على هذا الشريط جميع البيانات الخاصة بالبطاقة.

المطلب الثاني:

ماهية جرائم الإعتداء على بطاقات الائتمان عبر الإنترنت.

لقد سبق القول بأن الانترنت ونظرا لما تتمتع به من سمات، قد أتاحت الفرصة للمجرمين و العصابات الدولية لإساءة استخدام هذه البطاقات. إذ أصبحت تلك الشبكة تستعمل كأداة للاحتيال على نظام الدفع الإلكتروني الخاص بها بقصد تحقيق أرباح غير مشروعة. هذا ما أدى إلى ميلاد جرائم مستحدثة محلها تلك البطاقات و بيئتها الإنترنت تختلف عن نظيرتها التقليدية،تسمى بجرائم الإعتداء على بطاقات الائتمان.فماذا نعني بهذا الاجرام؟ و ما هي أركانه؟ و ما هي الأساليب المعتمدة للاستيلاء على تلك البطاقات. أسئلة سيتم الاجابة عليها بتقسيم المطلب إلى فرعين كالتالي:

الفرع الأول: تعريف الجرائم الواقعة على بطاقات الائتمان عبر الإنترنت و أركانها.

الفرع الثاني: الأساليب المعتمد عليها في الجرائم الواقعة على بطاقات الائتمان عبر الانترنت .

الفرع الأول: تعريف الجرائم الواقعة على بطاقات الائتمان عبر الانترنت و أركانها

و سنتطرق في هذا الفرع إلى تعريف الجرائم الواقعة على بطاقات الائتمان عبر الانترنت أولا ثم نتناول أركانها. و ذلك كمايلي:

أولا: تعريف الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

و يمكن تعريف هذا النمط الإجرامي التقني المستحدث بأنه: "عبارة عن الاستيلاء غير المشروع على الأرقام و المعلومات الخاصة بالبطاقات الائتمانية المملوكة للغير من خلال الاعتماد على تقنية شبكة المعلوماتية العالمية (الإنترنت) بهدف الحصول على أثمن السلع و الخدمات من ملايين المواقع التجارية

[1] –الهدف من البطاقة البارزة و المتغلغلة في جسم البطاقة يكمن في تأمين البطاقة ضد التزوير و التقليد.

المنتشرة عبر الشبكة العنكبوتية و التي يقبل عليها الوفاء بالبطاقات الممغنطة"[1].وعليه تنحصر جرائم الإعتداء على بطاقات الائتمان عبر الإنترنت في إمكانية التقاط أرقام هذه البطاقات والسطو عليها عبر قنوات الإنترنت المفتوحة و استخدامها بطريقة غير مشروعة في عمليات التسوق عبر الشبكة، بحيث يتم خصم قيمة السلع من العملاء الشرعيين لهذه البطاقات. ويتم ذلك السطو إما عن طريق سرقتها و الاستيلاء عليها أو عن طريق النصب و الاحتيال.

وتجدر الإشارة إلى أن أشهر صور النصب و الاحتيال هي النصب ببطاقات الائتمان[2].

ثانيا:أركان الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

يتطلب القانون لقيام الجرائم الواقعة على بطاقات الائتمان عبر الانترنت أركان، تتمثل في الركن الشرعي والركن المادي و الركن المعنوي. فأما الركن الشرعي فهو النص القانوني الذي يضفي الصفة غير الشرعية على الفعل فيخرجه من دائرة الاباحة إلى دائرة التجريم و الذي سنفصل فيه عند الكلام على موقف التشريعات المقارنة من هذه الجريمة[3]. و أما الركن المادي فكما هو معروف يتكون من ثلاث عناصر ألا وهي سلوك اجرامي و الذي يتمثل في النشاط المادي الصادر عن الجاني، و ذلك سواء باختراق خطوط الاتصال العالمية أو انشاء المواقع الوهمية أو عن طريق التجسس و غيرها من الأساليب التي تتطور يوما بعد يوم. و نتيجة و التي تتحقق بحصول الجاني على هذه الأرقام. و أخيرا رابطة السببية التي تربط هذا السلوك الاجرامي بالنتيجة.

و يذهب بعض الفقهاء إلى ضرورة وجود نشاط مادي بعد الاستيلاء على المال المعلوماتي كبيعه أو استعماله[4]. أما فيما يخص الركن المعنوي لهذه الجرائم فيمكن القول أن هذه الأخيرة من الجرائم العمدية التي تقوم على توافر القصد الجنائي العام بعنصريه الارادة و العلم، فالجاني لما يقوم بعملية السطو على أرقام البطاقات الائتمانية لا بد و أن يكون عالما بأن هذه المعطيات مملوكة للغير و لا يجوز الاستيلاء عليها ومع ذلك يسعى بارادته إلى الاستحواذ عليها بقصد تملكها أو استعمالها فيما بعد بصورة غير شرعية[5]. و إلى جانب ذلك القصد يجب توافر قصد جنائي خاص و المتمثل في توافر نية الإضرار بأصحاب بطاقات الائتمان الحقيقيين و تحقيق الاستفادة الكبرى و الربح من خلال استغلال بطاقات الائتمان[6].

---

[1]– د/ عماد على خليل، المرجع السابق، ص2.

[2]– وليد الزيدي، المرجع السابق، ص65.

[3]– لمزيد من التفاصيل ينظر ص 298 من هذه الرسالة.

[4]– أشار اليها د/ حسين بن سعيد بن سيف الغافري: الجرائم الواقعة على التجارة الالكترونية، 2006، ص 47.

[5]– د/ حسين بن سعيد بن سيف الغافري، نفس المرجع، نفس الموضع.

[6]– د/ عصام عبد الفتاح مطر، المرجع السابق، ص361.

الفرع الثاني: الأساليب المعتمد عليها في الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

إن الاستخدام غير المشروع عبر الإنترنت لأرقام بطاقات الائتمان لا يقتصر فقط على الغير، و لكن قد يستخدمها حاملها الشرعي بطريقة غير مشروعة عبر الإنترنت. و لهذا فإن التلاعب في أرقام بطاقات الائتمان قد يقع من الغير أو من قبل حاملها الشرعي. و فيمايلي تفصيل الأساليب و الطرق التي يتم من خلالها الإعتداء على أرقام بطاقات الائتمان.

أولا:أساليب التلاعب في بطاقات الائتمان عبر الانترنت التي تقع من الغير:

يقصد بالغير في هذه النقطة كل الأشخاص الذين لا صلة لهم بأطراف بطاقة الإتمان (الحامل الشرعي للبطاقة، البنك، التاجر)، أي هم قراصنة المعلوماتية.و هناك أساليب و طرق مختلفة و متعددة لا تقع تحت الحصر يستخدمها هؤلاء في الحصول على أرقام و بيانات بطاقات الائتمان عن طريق الإنترنت لاستخدامها بطريقة غير مشروعة في الحصول على السلع و الخدمات عبر تلك الشبكات، يتمثل أشهرها في الأساليب التالية:

1/ الاختراق غير المشروع لمنظومة خطوط الاتصالات العالمية: أو ما يعرف باسم illegal acces أو التجسس،و يعد هذا الأسلوب من أخطر الأساليب التي تهدد فكرة التجارة عبر الإنترنت. إذ يربط جهاز الحاسوب الخاص بالمشتري بذلك الخاص بالتاجر حيث يستخدم قراصنة المعلوماتية برامج تتيح لهم الإطلاع على البيانات و المعلومات الخاصة بالشركات التجارية و الكبرى و الأفراد على شبكة الإنترنت. وعلى ذلك يتمكنون من الحصول على بيانات بطاقة الائتمان المستخدمة في التجارة الإلكترونية عبر تلك الشبكة. و لعل الدافع الأساسي وراء اللجوء إليه يتمثل في الرغبة الكامنة في نفوس محترفي إجرام التقنية في قهر نظام التقنية و التفوق على الحماية و تعقيلها[1].

2/ أسلوب الخداع: و يتحقق هذا الأسلوب بإنشاء مواقع وهمية على شبكة الإنترنت المشابهة تماما لمواقع الشركات و المؤسسات التجارية الأصلية الموجودة على هذه الشبكة بحيث يظهر بأنه الموقع الأصلي المقدم لتلك الخدمة[2].

ولإنشاء هذا الموقع يقوم القراصنة بالحصول على كافة بيانات الموقع الأصلي من خلال شبكة الإنترنت مع تعديل بياناته السابقة بالشبكة، بحيث لا يكون هناك غير موقع واحد بنفس العنوان و هو الموقع الوهمي والذي يصبح يستقبل كافة المعاملات المالية و التجارية التي يقدمها الموقع الأصلي لأغراض التجارة الإلكترونية و من بينها البيانات الخاصة ببطاقات الائتمان و الرسائل الإلكترونية الخاصة بالموقع الأصلي

---

[1]– د/ عماد على خليل، المرجع السابق، ص3.

[2]– د/ جميل عبد الباقي الصغير: الحماية الجنائية و المدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، القاهرة،1999، ص37.

و الإطلاع عليها و من ثم الاستفادة غير المشروعة من المعلومات المتضمنة فيها، و ذلك على نحو يضر بالشركات و المؤسسات صاحبة الموقع الأصلي و يدمر ثقة المستخدمين في التجارة الإلكترونية[1].

3/ تقنية تفجير الموقع المستهدف: و يوجه هذا الأسلوب عادة إلى الحواسب المركزية للبنوك والمؤسسات المالية و المطاعم و الفنادق و وكالات السفر بهدف تحصيل أكبر عدد ممكن من أرقام بطاقات الإئتمان. و يستند هذا الأسلوب أساسا على مئات آلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص إلى الجهاز المستهدف بهدف التأثير على سعته التخزينية. بحيث يؤدي شكل هذا الكم الهائل من الرسائل الإلكترونية في نهاية المطاف إلى إغراق الموقع العامل على الشبكة و تفجيره و تشتيت المعلومات والبيانات المخزنة فيه، لتنقل بعد ذلك للجهاز الخاص بالمجرم أو تمكنه من حرية التجول في الموقع المستهدف بسهولة و يسر، فيستولي بذلك على ما يشاء من أرقام و بيانات خاصة ببطاقات إئتمانية مملوكة لغيره[2].

4/الإستدراج أو الصيد: و يقوم هذا الأسلوب على نسخ موقع من مصدر موثوق به كالمصرف على سبيل المثال ثم يقوم المحتالون بإرسال وصلة إلى موقع إلكتروني آخر مخادع يطلبون فيه بعض المعلومات المهمة كالإسم و رقم الحساب و الرقم القومي و اسم المستخدم و كلمة المرور من المستهلكين و يقوم المستهلكون بالرد مقدمين تلك المعلومات ليتم استخدامها بعد ذلك من قبل المحتالين في فتح حسابات مصرفية أو شراء مجوهرات و مواد إلكترونية[3].

5/ تخليق أرقام البطاقات: و يعرف هذا الأسلوب باسم Card Math و هو يعتمد بالدرجة الأولى على إجراء معادلات رياضية و إحصائية بهدف تحصيل أو تخليق أرقام بطاقات ائتمانية مملوكة للغير، و هي كل ما يلزم للشراء عبر شبكة الإنترنت[4]. حيث يتوافر في الأسواق برامج تشغيل باسطة و خاصة تتيح امكانية تخليق أرقام بطاقات بنك معينة من خلال تزويد الحاسوب بالرقم الخاص بالبنك المصدر للبطاقات[5]. و عادة ما يقوم مجرموا البطاقات بنشر هذه المعادلات و بيان الكيفية التي يمكن من خلال اتباعها خطوة بخطوة الحصول على أرقام البطاقات الائتمانية المملوكة للغير عبر مواقعهم المنتشرة على

---

[1]– د/ نائلة عادل محمد فريد قورة،المرجع السابق، ص562.

[2]– د/ عماد على خليل، المرجع السابق، ص4، د/ عصام عبد الفتاح مطر، المرجع السابق، ص359.

[3]– د/ عصام عبد الفتاح مطر، نفس المرجع، ص359.

[4]– علي حسن عباس: مخاطر استخدام بطاقات الدفع الالكتروني عبر شبكة الإنترنت (المشاكل و الحلول)، ورقة عمل مقدمة إلى ندوة "الصور المستحدثة لجرائم بطاقات الدفع الالكتروني" الت نظمها مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة، 1998/12/14، ص17.

[5]– د/ سليمان أحمد فضل، المرجع السابق، ص171.

شبكة الانترنت. و من الأمثلة على هذه المواقع www.drak-secrets.com و www.hacker.secrets/credit3txt.[1]

و تجدر الإشارة إلى أن تخليق أرقام بطاقات الائتمان الخاصة بالغير أو المستخدمة من قبل الآخرين تشكل تعدادا معنويا للجرائم، حيث أنه ينصب عليها وصف تزوير و استعمال المزور و كذلك ينطبق عليها وصف الاحتيال و ذلك إذا ما استخدمت في الولوج إلى النظام المعلوماتي بغية الحصول على السلع والخدمات التي توفرها الشبكة.و قد قضت محكمة Rennes بأن استخدام البطاقة المزورة يعد من قبيل الطرق الاحتيالية التي تقوم بها جريمة النصب. و قد اكتشفت بعض البنوك تكرار اعتراض بعض حاملي بطاقات الدفع الإلكتروني على عمليات لم يقوموا بإجرائها و تبين لها أنها عمليات تم إجراؤها عن طريق شبكة الإنترنت، بواسطة بعض الهواة المتطفلين (hackers) و المخربين(crachers) الذين تمكنوا من التقاط و تخليق أرقام بطاقات الدفع الإلكتروني الخاصة ببعض العملاء على الشبكة، و استغلالها في الحصول على السلع و الخدمات. و لاسيما أنه لا توجد شيفرة خاصة باستخدام بطاقات الفيزاكارد والماستركارد[2].

هذه باختصار أشهر و أهم الطرق و الأساليب التي يهدف مجرمو البطاقات الائتمانية من خلالها إلى تحصيل الأرقام و البيانات المتعلقة بالبطاقة الائتمانية المملوكة للغير، لتستخدم في نهاية المطاف في تحقيق الإثراء غير المشروع على حساب أصحاب تلك البطاقات 1/6 و البنوك المصدرة لها، و التي أصبحت هي الأخرى ضحية من ضحايا هذا النمط الإجرامي التقني المستحدث.

هذا من جهة و من جهة أخرى، فإن القضاء الفرنسي يسانده بعض الفقه يعتبر أن سرقة الأرقام و البيانات السرية الخاصة ببطاقات الائتمان و استخدامها بصورة غير مشروعية من الغير جريمة نصب، على أن المتهم قد انتحل اسما كاذبا. و من ثم يكون قد استخدم وسيلة احتيالية لإقناع المجني عليه بوجود ائتمان. بينما يذهب جانب آخر من الفقه على اعتبار أن هذا الفعل هو في حقيقة الأمر يشكل جريمة سرقة باستعمال مفتاح مصطنع و المتمثل في بطاقات الائتمان[3].

ثانيا:أساليب التلاعب في بطاقات الائتمان التي تقع من قبل حاملها الشرعي:

تكون بطاقات الائتمان في بعض المرات عرضة للاستخدام غير المشروع حتى من قبل أطرافها و لا سيما التلاعب الذي يقع من العميل الحامل الشرعي للبطاقة.و يقصد بالعميل هنا الشخص الذي يحصل على البطاقة من البنك المصدر لها بغرض استخدامه الشخصي لها كوسيلة دفع للحصول على السلع والخدمات المختلفة. و غالبا ما يتحقق ذلك في حالتين:

الحالة الأولى: تجاوز حامل البطاقة للرصيد خلال فترة صلاحيتها

---

[1]– أشار اليها د/ حسين بن سعيد بن سيف الغافري، (الجرائم الواقعة على التجارة الالكترونية) مرجع سابق، الهامش 3،ص45.

[2]– محمد أمين أحمد الشوابكة، المرجع السابق، ص201–202.

[3]– د/ عماد على خليل، المرجع السابق، ص5. و ينظر كذلك محمدأمين أحمد الشوابكة، المرجع السابق، ص200.

ويتم ذلك بأن يقوم حامل البطاقة الشرعي بشراء سلع أو خدمات التي تقدمها الشبكة- بملء الاستمارة الإلكترونية- رغم علمه بأن رصيده بالبنك غير كافي لتغطية هذه المبالغ. أو أن يقوم بإجراء تحويل إلكتروني من رصيد لآخر متجاوز رصيده في البنك مصدر البطاقة.و قد انقسم الفقه و القضاء بشأن التكييف القانوني لمثل هذه الحالة إلى اتجاهين:

الاتجاه الأول: و يرى أن العميل لا يعد مرتكبا لجريمة نصب في مواجهة التاجر، و ذلك لكونه يعلم تماما بموجب العقد الذي يوجد بينه و بين الجهة المصدرة للبطاقة الأقصى الذي يلتزم به البنك و يضمن سداده إليه،فالتاجر يعد متصرفا في هذه الحالة على مسؤوليته. كذلك لا يمكن القول بأن حامل البطاقة قد استخدم طرقا احتيالية من شأنها الإيهام بوجود ائتمان وهمي، حيث أن مجرد تقديم البطاقة لا يشكل طرقا احتيالية مما تقوم به جريمة النصب. و قد ذهبت محكمة الاستئناف Angers بفرنسا على اعتبار أن استيلاء حامل البطاقة على مبالغ تتجاوز رصيده عند وضعها في أحد أجهزة التوزيع الآلي المعد لذلك لا يشكل أية جريمة جنائية[1].

الاتجاه الثاني: و على عكس الاتجاه الأول يكيف أنصار هذا الاتجاه حامل البطاقة للرصيد خلال فترة صلاحيتها بجريمة النصب،و ذلك لأن مجرد تقديم العميل – الذي ليس له رصيد في البنك – البطاقة إلى التاجر يعتبر في حد ذاته وسيلة احتيالية من شأنها الإقناع بوجود ائتمان وهمي. و يستند أنصار هذا الرأي إلى حكم محكمة Dovai الذي أدان حامل البطاقة بتهمة النصب، لأنه استخدمها و دفتر الشيكات في سحب أوراق البنكنوت من فرع آخر للبنك خلافا للفرع القائم بمسك حساب العميل.

و يؤيد بعض الفقه هذا الرأي لكون أنه من غير المنطق و العدالة أن يسأل الشخص و يعاقب إذ أصدر شيك بدون رصيد، بينما لا يسأل جنائيا إذا قام بتسديد مشترياته عن طريق بطاقة الوفاء على الرغم من علمه بعدم وجود رصيد له. الأمر الذي يستوجب تدخل المشرع الجنائي بتجريم مثل هذا الفعل بنص يحدده و يحدد عقوبته[2].

الحالة الثانية: استخدام الحامل الشرعي للبطاقة بعد إلغائها أو انتهائها

في حالة إلغائها: و ذلك بقيام البنك مصدر البطاقة بإلغائها كجزاء لسوء استخدامها من طرف العميل. وفي هذه الحالة يلتزم ذلك الأخير بإرجاع البطاقة إلى البنك مصدرها و لكن قد يحدث أن يمتنع عن ردها مستخدما بياناتها في شراء لسلع أو خدمات عبر شبكة الإنترنت، بالتالي إلزام البنك بالوفاء بهذه المبالغ للتاجر.

في حالة انتهائها: فهنا يجب التمييز بين حالتين: حالة استخدام بطاقات الائتمان بعد انتهاء مدة صلاحيتها، و في هذه الحالة لا يشكل ذلك جريمة نصب. و بين ما إذا اتفق الحامل الشرعي مع التاجر على قبول الوفاء ببطاقة منتهية الصلاحية إضرارا بالبنك المصدر، و ذلك بأن يقوم التاجر بتزوير تاريخ

---

[1]- د/ جميل عبد الباقي الصغير،(المسؤولية الجنائية في مجال المعاملات الالكترونية) مرجع سابق، ص9.

[2]- د/ سليمان أحمد فضل، المرجع السابق، ص 172-173.

انتهاء مدة صلاحية البطاقة على الفاتورة، أو يقوم بتقديم تاريخ عمليات الوفاء المنفذة. فهنا يسأل الحامل الشرعي جنائيا بارتكابه لجريمة نصب و كذا التاجر[1].

المطلب الثالث:

موقف التشريعات المقارنة من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

نظرا لما للاعتداء على بطاقات الائتمان من أثر سيء على الاقتصاد المحلي والعالمي، بات توفير الحماية الجنائية لها أمر يفرضه الواقع و المستقبل على حد السواء، و لا سيما بعد ظهور الانترنت الشبكة العالمية و انتشارها و استخدامها في الاستلاء بطريقة غير شرعية على أرقام بطاقات الائتمان. و على هذا كان لزاما على التشريعات المقارنة أن تواجه هذه الظاهرة الإجرامية المستحدثة بسنها لقوانين خاصة لمكافحة إساءة استخدام بطاقات الائتمان عامة، و إساءة استخدامها عبر الإنترنت خاصة و رادعة في الوقت ذاته بفرضها لعقوبات على من يقوم باصطناع أو تزوير أو سرقة أو النصب باستخدام تلك البطاقة. و لقد تقسيم هذا المطلب إلى الفرعين التاليين:

الفرع الأول: موقف التشريعات الغربية من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

الفرع الثاني: موقف التشريعات العربية من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت

الفرع الأول: موقف التشريعات الغربية من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

و سنحدد في هذا الفرع كلا من موقف التشريع الفرنسي ثم التشريع الأمريكي من الجرائم الواقعة على بطاقات الإئتمان عبر الانترنت كما يلي:

أولا: موقف التشريع الفرنسي من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

نص المشرع الفرنسي على تجريم مجموعة من الأفعال التي يكون محلها بطاقة اليكترونية ، إذ نصت المادة (11) من القانون رقم 19-1382 الصادر في 30 ديسمبر 1991 والتي عدلت المادة 67 من المرسوم بقانون الصادر في 30 أكتوبر 1935 لكي تضيف المادتين 1/67 ،2/67 بعد المادة 67 من المرسوم بقانون سالف الذكر، إذ نصت المادة 1/67 على تجريم ثلاثة أفعال يكون محلها بطاقة اليكترونية الأول يتمثل بجريمة تزوير أو تقليد بطاقة الوفاء والثاني جريمة استعمال أو محاولة استعمال بطاقة مقلدة أو مزورة أما الثالث فهو جريمة قبول الوفاء بواسطة بطاقة مقلدة أو مزورة.

---

[1]- د/ سليمان أحمد فضل، نفس المرجع ، ص175، إيهاب مصطفى عبد الغني: الحماية الجنائية للأعمال البنكية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011، ص 300.

وتجدر الاشارة إلى أن المشرع الفرنسي اقتصر في تجريمه لمثل هذه الأفعال على جرائم تزوير وتقليد البطاقات دون التطرق إلى الأفعال التي تمثل إساءة استخدام البطاقة الاليكترونية وكان من المفترض أن ينص على تجريم الأفعال التي تعد اساءةً لاستخدام البطاقة من قبل حاملها والتي من ضمنها إساءة استخدام بطاقة الائتمان الملغاة .[1]

ثانيا: موقف التشريع الأمريكي من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

جرم التشريع الجنائي الأمريكي النشر غير المشروع لأرقام بطاقات الائتمان و البيانات و المعلومات الخاصة بها عبر شبكة الإنترنت. و ذلك من خلال القانون الفدرالي للاحتيال عبر وسائل الاتصال،الذي جرم النقل غير المصرح به للمعلومات أو الإشارات أو العلامات أو الصور أو التسجيلات الصوتية عبر أي من وسائل الاتصال[2].

الفرع الثاني: موقف التشريعات العربية من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.

و سنركز في هذا الفرع على موقف التشريع الجزائري ممثلا للتشريعات العربية [3] من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت.و ذلك كمايلي:

---

[1] – حسن حماد حميد،جاسم خريبط خلف: إساءة إستخدام بطاقة الائتمان الإليكترونية الملغاة، مجلة جامعة بابل للعلوم الإنسانية، المجلد 18، العدد 2 ، 2010، ص 11-12.

[2]– لمزيد من التفاصيل ينظر د/ عصام عبد الفتاح مطر، المرجع السابق، ص353 و ما بعدها.

[3]– جرمت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات كل إستخدام غير مشروع لأدوات الدفع الإلكترونية و من بينها بطاقة الإئتمان و ذلك في المادة 18 و الناصة على:" الإستخدام غير المشروع لأدوات الدفع الإلكترونية:

1- كل من زور أو إصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت.

2- كل من إستولى على بيانات أي أداة من أدوات الدفع و إستعملها أو قدمها للغير أو سهل للغير الحصول عليها.

3- كل من إستخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام بيانات أي أداة من أدوات الدفع.

4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك." كما جرمت التشريعات العربية ذلك السلوك غير المشروع الواقع عبر الإنترنت و منها: القانون الاتحادي الإماراتي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات في مادته 11 و الناصة على أنه :"كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول من دون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية بقصد الحصول على أموال الغير أو ما تتيحه من خدمات،يعاقب بالحبس مدة لا تقل عن ستة أشهر و بالغرامة. أو باحدى هاتين العقوبتين و تكون العقوبة الحبس مدة لا تقل عن سنة و الغرامة التي لا تقل عن ثلاثين ألف درهم أو احدى هاتين العقوبتين اذا توصل ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير."

تعتبر بطاقات الائتمان وسيلة سهلة و ميسرة لابرام الصفقات من بيع و شراء عبر شبكة الانترنت و هي تعتبر كنتيجة ايجابية للتجارة الالكترونية. و يعتبر القانون 03-15[1] المتعلق بالنقد والقرض أول قانون جزائري تضمن التعامل الإلكتروني الحديث في القطاع المصرفي، ويتضح ذلك من خلال المادة 69 التي تضمن نصها " تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكون السند أو الأسلوب التقني المستعمل".و يتبين من خلال هذا النص نية المشرع الجزائري الانتقال من وسائل الدفع الكلاسيكية إلى وسائل دفع حديثة إلكترونية. ويتضح ذلك جليا بصدور الأمر 05-06 المؤرخ بتاريخ 23 أوت 2005 المتعلق بمكافحة التهريب[2]، وفي المادة الثالثة حيث استعمل صراحة مصطلح " وسائل الدفع الإلكتروني" باعتبرها من بين التدابير والإجراءات الوقائية لمكافحة التهريب. وبذلك انتقل المشرع من مصطلح مهما يكن السند أو الأسلوب التقني المستعمل الوارد في نص المادة (69) من القانون 03-15 المتضمن الموافقة على الأمر 03-11 المتعلق بالنقد والقرض [3] إلى مصطلح أكثر دقة المتمثل في وسائل الدفع الإلكتروني الوارد في النص 03 من الأمر المذكور[4] . وبموجب القانون رقم 05-02 المؤرخ في 06 فيفري 2005 المعدل و المتمم للقانون التجاري أضاف فقرة ثالثة للمادة 414 في وفاء السفتجة نص فيها على أنه".. يمكن أن يتم التقديم أيضا بأية وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما" ولقد تم إضافة نفس هذه الفقرة إلى المادة 502 بمناسبة تقديم الشيك للوفاء.كما أضاف باب رابع إلى الكتاب الرابع من القانون التجاري والمعنون بالسندات التجارية، إذ تضمن فصله الثالث بطاقات السحب والدفع وذلك في المادة 543 مكرر 23[5]. و لقد اعتبر المشرع الجزائري وسائل الدفع الالكتروني أوراقا تجارية جديدة إضافة إلى الأوراق التجارية الكلاسيكية وهي السفتجة والشيك والسند لأمر.

أما فيما يخص موقف المشرع الجزائري من الجرائم الواقعة على بطاقات الائتمان، فيمكن القول بتطبيق المواد التي تحكم كل من جريمة خيانة الأمانة و كذا جريمة السرقة و جريمة النصب و جريمة التزوير وذلك كمايلي:

و قد سايره المشرع السعودي، و جرم و عاقب في المادة 2/4 من نظام مكافحة المعلوماتية لعام 2007 حيث تنص على:" يعاقب بالسجن مدة لا تزيد على ثلاث سنوات و بغرامة لا تزيد على مليوني ريال، أو باحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:.....

2-الوصول -دون مصوغ نظامي صحيح - إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية بقصد الحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات".

[1]-الجريدة الرسمية، العدد 52.

[2]-الجريدة الرسمية، العدد 59.

[3]- الجريدة الرسمية، العدد 64.

[4]- الأمر 05-06 المؤرخ بـ 23 أوت 2005 المتعلق بمكافحة التهريب، ج ر ع، 59.

[5]- تنص المادة 543 مكرر23 من القانون التجاري الجزائري على:"تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك و الهيئات المالية المؤهلة قانونا و تسمح لصاحبها بسحب أو تحويل أموال.

تعتبر بطاقة سحب كل بطاقة صادرة عن البنوك او الهيئات المالية المؤهلة قانونا و تسمح لصاحبها فقط بسحب أموال".

فأما بالنسبة لجريمة خيانة الأمانة و بما أن المشرع الجزائري يعتبر وسائل الدفع الالكتروني و من بينها بطاقات الائتمان من الأوراق التجارية فيمكن تطبيق المادة 376 [1] من قانون العقوبات الجزائري و التي تجرم و تعاقب كل من اختلس أو بدد بسوء نية أوراقا تجارية بقصد الاضرار بمالكيها أو حائزيها بعقوبات أصلية تتمثل في الحبس من ثلاثة أشهر إلى ثلاث سنوات و بغرامة من 500 إلى 20000 دج. وبعقوبات تكميلية تتمثل في الحرمان من حق أو أكثر من القوق الواردة في المادة 14 و بالمنع من الاقامة و ذلك لمدة سنة على الأقل و خمس سنوات على الأكثر.

و أما بالنسبة لجريمة السرقة فيمكن تطبيق نص المادة 350[2] قانون العقوبات في حالة التي يسحب فيها الحامل الشرعي لتلك البطاقة مبالغ مالية تتجاوز الحد المسموح سحبه خلال فترة صلاحيتها أو استخدامه لها بعد إلغائها أو انتهائها.

و أما فيما يخص جريمة النصب فيمكن تطبيق نص المادة 372[3] من قانون العقوبات في الحالة الذي يقوم فيها الغير بالتقاط رقم بطاقة الإئتمان عند اجراء معاملة بين شخصين عبر شبكة الإنترنت ويقوم بسحب مبلغ مالي من حساب صاحب البطاقة. ففي هذه الحالة ينطبق وصف النصب على هذا الفعل وذلك بإستعمال طريقة احتيالية و المتمثلة في ادعاء صفة غير صحيحة بأنه صاحب الحساب أو وكيل عنه عندما استعمل الرقم السري للكارت الذي يوهم بذلك.

و يمكن تصور وقوع التزوير في هذا النوع من البطاقة بإستعمال إحدى طرق التزوير المادي أو المعنوي والمعروف أن طرق التزوير المادي تتمثل في الإضافة والحذف والاصطناع لألفاظ أو أرقام أو إمضاءات أو أختام أو بصمات. كما يعد وضع صورة شخصية لغير صاحب البطاقة عليها من طرق التزوير، فتنص المادة 216[4] عقوبات جزائري على وقوع التزوير بانتحال شخصية الغير أو الحلول محلها كوضع " صور أشخاص آخرين مزورة".

والمعروف أن طرق التزوير المعنوي تتمثل في تغيير موضوع المحررات من الشخص المكلف بكتابته عند تحريرها أو تغيير إقرارات أولي الشأن أو جعل واقعة في صورة واقعة صحيحة أو واقعة غير معترف بها في شكل واقعة معترف بها (مادة 1/216 و 2 و3 عقوبات جزائري). وتتحقق الطريقة الأولى (تغيير موضوع المحررات) في حالة بطاقة الائتمان إذا أصدرها الموظف المسؤول لصالح شخص معين مع أنها باسم شخص آخر، ويمكن أن يتحقق ذلك إذا كان الإسم المدون عليها لا يعود إلى صاحب الصورة المسجلة عليها. وفي الفرض السابق يسأل الموظف عن تزوير البطاقة ما دام أن القصد الجنائي يتوافر لديه. بيد ان التزوير قد ينسب إلى صاحب الشأن الذي يقدم بيانات كاذبة إلى موظف البنك. في هذه الحالة الأخيرة يعد صاحب الشأن شريكا بالتحريض مع فاعل حسن النية في جناية تزوير محررات البنوك.

---

[1]- ينظر المادة 376 من قانون العقوبات الجزائري .

[2]- ينظر المادة 350 من قانون العقوبات الجزائري .

[3]- ينظر المادة 372 من قانون العقوبات الجزائري .

[4]- ينظر المادة 216 من قانون العقوبات الجزائري .

وعلى أي حال فإن مجرد التقاط أرقام بطاقة الائتمان لا يشكل جريمة سرقة أو نصب أو خيانة أمانة، ذلك أن الأمر لا يتعلق بمال منقول ولكن بمعلومة ذات طبيعة معنوية، بينما ترد جرائم المال على مال ذي طبيعة محسوسة وفقا لما استقر عليه التفسير القانوني لتلك الجرائم في التشريعات المختلفة . ومن هنا نجد أن المواد 394 مكرر و 394 مكرر1 التي نص عليها المشرع في القسم السابع مكرر تنطبق على الجرائم الواقعة على بطاقات الائتمان.[1]

و لتفادي ما سبق بيانه من إساءة استخدام بطاقات الائتمان عبر شبكة الإنترنت، طالبت شركات بطاقات الائتمان عملائها بعدم استخدام رقم البطاقة في المعاملات عبر الإنترنت إلا بعد تشفيرها،هذا و يعد "نظام المعاملات التجارية الإلكترونية المؤمنة" المعروف بالنظام "Set" أحدث نظام لحماية المتعاملين عبر الإنترنت[2].

بالإضافة إلى ظهور صور جديدة للسداد عبر الإنترنت كالنقود الرقمية[3]، و كذا إصدار بطاقات ائتمانية مدفوعة مسبقا أو بحد ائتمان بسيط[4].

---

[1]- يجب الإشارة أن المشرع الجزائري نظم الجرائم التي تقع على البطاقات الإلكترونية للمؤمن له إجتماعيا و ذلك في القانون 08-01 المؤرخ في 2008/01/23 و المتمم للقانون رقم 83-11 و المتعلق بالتأمينات الإجتماعية في المواد 93 مكرر2 و مكرر3 و مكرر4، إذ جرم و عاقب على الأفعال التالية:

- الإستعمال غير المشروع لتلك البطاقة الإلكترونية للمؤمن له إجتماعيا أو للمفتاح الإلكتروني لهيكل العلاج أو المهني الصحة.(الحبس من سنتين إلى خمس سنوات و الغرامة المالية المقدرة ب 100.000دج إلى 200.000 دج).

- الغش بالتعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية و / أو الإدارية المدرجة في البطاقة الإلكترونية أو للمفتاح الإلكتروني لهيكل العلاج أو المهني الصحة. (الحبس من سنتين إلى خمس سنوات و الغرامة المالية المقدرة ب 500.000 دج إلى 1.000.000 دج)

- الإعداد أو التعديل أو النسخ بطريقة غير مشروعة للبرمجيات التي تسمح بالوصول أو بإستعمال المعطيات المدرجة في البطاقة الإلكترونية أو للمفتاح الإلكتروني لهيكل العلاج أو المهني الصحة.(الحبس من سنتين إلى خمس سنوات و الغرامة المالية المقدرة ب 500.000 دج إلى 1.000.000 دج).

- النسخ أو الصنع أو الحيازة أو التوزيع بطريقة غير مشروعة لتلك البطاقة الإلكترونية للمؤمن له إجتماعيا أو للمفتاح الإلكتروني لهيكل العلاج أو المهني الصحة. .(الحبس من سنتين إلى خمس سنوات و الغرامة المالية المقدرة ب 500.000 دج إلى 5.000.000 دج). لمزيد من التفاصيل ينظر المادة 93 مكرر2 و مكرر3 و مكرر4 من القانون 08-01 المؤرخ في 2008/01/23 و المتمم للقانون رقم 83-11 و المتعلق بالتأمينات الإجتماعية.

[2]- وليد الزيدي، المرجع السابق، ص66.

[3]- حيث يتم تخزين مبلغ إلكتروني على القرص الصلب للحاسب الآلي الخاص بالمشتري - تأخذ شكل حافظة نقود- ليستخدمها في سداد مشترياته. ينظر محمدأمين أحمد الشوابكة، المرجع السابق، ص202.

4- و هذه البطاقات خاصة للاستعمال عن طريق الإنترنت، بحيث إذا تعرضت للاستيلاء و للاستخدام من قبل الغير كانت الخسائر محدودة. ينظر د/ إيهاب فوزي السقا، المرجع السابق، ص205.

و من القضايا الواقعية لإساءة استخدام بطاقات الائتمان عبر الإنترنت:

– قيام شخص ألماني بالدخول غير المشروع إلى أحد مزود الخدمات و استولائه على أرقام بطاقات ائتمانية الخاصة بالمشتركين و من ثم تهديده مزود الخدمة بإفشاء أرقام تلك البطاقات ما لم يستلم فدية.وقد تمكنت الشرطة الألمانية من القبض عليه[1].

– قيام شخصان بإنشاء موقع على الإنترنت مخصص لشراء طلبات يتم بعثها فور تسديد قيمتها إلكتروني، و لم تكن الطلبات لتصل إطلاقا حيث كان الموقع وهمي قصد منه النصب و الاحتيال. و قد تم القبض على مؤسسه لاحقا[2].

– قيام مهندس حاسبات آسيوي بعمل العديد من السرقات المالية و بشراء العديد من السلع و الخدمات عبر شبكة الإنترنت مستخدما بيانات بطاقات الائتمان و الحسابات الشخصية لعدد كبير من الضحايا[3].

– قيام المتطفل كيفن ميتنك باستخدام وسيلة الاحتيال على الكمبيوتر من أجل الحصول على (20.000) بطاقة ائتمانية من شركة (Netcom) للاتصالات في سان جوس في كاليفورنيا[4].

– إلقاء إدارة المعلومات و التوثيق و جرائم الحاسبات القبض على شخص استغل أرقام بطاقات الائتمان الشخصية للشراء عبر الإنترنت[5].

---

[1]– محمد عبد الله المنشاوي، (جرائم الإنترنت....)، http:// www.minshawi.com.

[2]– محمد عبد الله المنشاوي،نفس المرجع.

[3]– الجريمة عبر الإنترنت، http:// www.f–law.net.

[4]– محمد أمين أحمد الشوابكة، المرجع السابق،ص 201.

[5]– الجريمة عبر الإنترنت، بحث منشور على الموقع السابق. و من الأمثلة الأخرى نذكر منها:

– إلقاء مباحث الأموال العامة بالإسكندرية القبض على تشكيل عصابي يضم 5 أشخاص من بينهم 3 طلاب بالأكاديمية العربية للعلوم و التكنولوجيا تخصص في استخدام الحاسبات الآلية للاستيلاء على حسابات الفيزاكارت "الخاصة لعملاء البنوك".

كما تمكنت إدارة مباحث جرائم الحاسبات و شبكات المعلومات بوزارة الداخلية من ضبط عصابة تضم ثلاثة طلاب لكليات الهندسة و التجارة و الألسن يقومون بالاستيلاء وسرقة أرصدة كروت بطاقات الائتمان الخاصة ببعض المواطنين المقيمين خارج البلاد و ذلك باستخدام مواقع مشبوهة على شبكة الإنترنت.واستطاعوا الحصول على كميات كبيرة من المنتجات الإلكترونية و أعداد كبيرة من التليفونات المحمولة و أجهزة كمبيوتر و سيارات بعد شرائها بأرقام البطاقات المملوكة للغير.

وقد ألقي القبض على الطلاب الثلاثة بعد جهود مضنية. حيث كانوا يستخدمون مقاهي إنترنت عامة بمناطق حدائق القبة والزيتون و الوايلي، و أحيلوا إلى النيابة التي أمرت بحبس الطلاب أربعة أيام على ذمة التحقيق.و تمت عمليات الضبط في اطار توجيهات السيد وزير الداخلية بالتصدي للجرائم المستحدثة التي تشكل خطرا على أمن المواطن، حيث تلقى اللواء بلاغا لمدير إحدى شركات الإنترنت الكبرى يفيد تلقيه إخطارا من البنك الأهلي يؤكد أن أحد العملاء لديه قام بشراء عدة أجهزة إلكترونية ببطاقات ائتمانية لشخص أمريكي.

أما في الولايات المتحدة استطاع الحدث جستن بترس اختراق شبكة وكالة (TRW) لخدمات بطاقات الائتمان و سرقة بيانات لمجموعة بطاقات الائتمان من أجهزة الحاسب الآلي الخاصة بالوكالة.

المبحث الثالث:

جريمة العدوان على التوقيع الإلكتروني عبر الإنترنت.

تستلزم عقود التجارة الإلكترونية لصحة تمامها و إثباتها و توثيقها توقيع الأطراف المتعاقدة عليها كما هو الشأن في عقود التجارة التقليدية. و يسمى ذلك الأخير "بالتوقيع الإلكتروني" الذي ظهر بديلا عن التوقيع اليدوي التقليدي. و للتوقيع الإلكتروني فائدة كبيرة عبر الإنترنت و بصفة خاصة في نشاط التجارة الإلكترونية، لكونه أداة فعالة في حركة المعاملات التجارية و المدنية، فهو يخفف من حدة الاستخدام الورقي في الاتفاقات ثم أنه يسمح بقدر من المرونة في المعاملات، كما أنه يختصر المسافات و الزمن إذ يكفي أن يضع الشخص توقيعه لكي تتم المعاملات دون حاجة لانتقاله إلى الأماكن الأخرى لكي يقوم بمعاملاته. ضف إلى ذلك فهو يفيد و يسهل كثيرا العمليات المصرفية[1]. و لكنه هو الآخر لم يسلم من المجرمين، حيث أصبح محلا لاعتداءاتهم، فظهر بذلك اجرام مستحدث يسمى بجريمة العدوان على التوقيع الالكتروني.و عليه تم تقسيم هذا المبحث الى المطالب الآتية:

المطلب الأول:تعريف التوقيع الالكتروني.

المطلب الثاني: ماهية جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

المطلب الثالث: موقف التشريعات المقارنة من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

كما قام بعض الهاكرز من الحصول على بيانات لأكثر من 2 مليون بطاقة للفيزاكارد و الماستركارد، بعد الدخول إلى الأنظمة التي تدير عمليات التحويل الإلكتروني، و الإضرار بخمس ملايين بطاقة ائتمان. مما دعا شركة سيتي بنك المصرفية إلى إغلاق 8800 حساب مصرفي من حسابات العملاء، لعدم استخدام بيانات و أرقام البطاقات مستقبلا.

أما الهاكرز إبراهيم عبد الله فتمكن في غضون ستة أشهر فقط من الاستيلاء على 22 مليون دولار من المشاهير و الشركات الاستثمارية الكبرى. و كانت هوايته تزوير بطاقات الائتمان البنكية و استطاع سرقة أرقام 800 كارت ائتمان و حوالي مائة ألف دولار، كما قام بسرقة أرقام بطاقات الائتمان من زبائنه في المطعم الذي يعمل به.

كما قام الحدث الذي لقب نفسه ماكسوس بالاستيلاء على بطاقات الائتمان و تحويل الأرصدة و الحسابات من خلال شبكة الإنترنت حيث أن يستولي على ثلاثمائة ألف بطاقة استخدمها بالفعل في الشراء. حيث خصصت منها قيمة بمبلغ مالي كبير. و تعد هذه العملية من أوسع عمليات السطو عبر شبكة الإنترنت. لمزيد من التفاصيل ينظر على التوالي: عمرو عيسى الفقى، المرجع السابق، ص214 و 216. د/ عبد الفتاح بيومي حجازي، (الأحداث و الإنترنت) مرجع سابق، ص 210 و ما بعدها و 213 و ما بعدها. د/ايهاب فوزي السقا، المرجع السابق، الهامش رقم2، ص 204. د/ عبد الفتاح بيومي حجازي، (جريمة غسل الأموال) مرجع سابق، الهامش رقم 2، ص24 و مابعدها. د/ عبد الفتاح مراد، المرجع السابق، ص 403. د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن استخدام الإنترنت) مرجع السابق،ص 427.

[1]– د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت)مرجع سابق، ص427.

المطلب الأول:

تعريف التوقيع الالكتروني.

تتباين التعريفات التي أعطيت للتوقيع الإلكتروني فيما يخص الفقه و التشريع. و سنتطرق في هذا المطلب إلى تعريف التوقيع الالكتروني من خلال الفرعين التاليين:

الفرع الأول: التعريف القانوني للتوقيع الإلكتروني.

الفرع الثاني: التعريف الفقهي للتوقيع الإلكتروني.

الفرع الأول: التعريف القانوني للتوقيع الإلكتروني.

إن شيوع عمليات التجارة الالكترونية عبر شبكة الانترنت و تنامي استخدام السندات و العقود الالكترونية التي تفرض تقنية التوقيع الالكتروني، حتم تدخل التشريعات الدولية و الوطنية لتنظم هذه المفاهيم الحديثة وبيان شروطها و آثارها. و قد تم تعريف التوقيع الالكتروني على **المستوى التشريعي الدولي** كمايلي:

عرفت المادة 1/2 من **قانون الأمم المتحدة النموذجي بشأن التوقيعات الإلكترونية لعام 2001** التوقيع الإلكتروني بأنه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا يجوز أن تستخدم لتعيين هوية الموقع بالنسبة لرسالة البيانات و لبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات. و وفقا للمادة 1/2 من **التوجيه الأوربي رقم 99-1993** الصادر بتاريخ 13 ديسمبر بشأن التوقيع الإلكتروني، فإنه يقصد بالتوقيع الإلكتروني "بيان أو معلومة معالجة إلكترونيا، ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرى (كرسالة أو محرر) و التي تصلح كوسيلة لتمييز الشخص و تحديد هويته."و أضافت الفقرة الثانية من ذات المادة بأن ينبغي أن يتوفر في التوقيع المتقدم المتطلبات التالية:

أ- أن يكون قادرا على تحديد شخصية الموقع، و مميزا له عن غيره من الأشخاص.

ب- أن ينشأ باستخدام وسائل و إجراءات تقنية تقع تحت سيطرة الموقع.

ت- أن يرتبط بالمعلومات التي يتضمنها المحرر الإلكتروني بطريقة تسمح بكشف أية محاولة لتعديل هذه البيانات. و متى توافرت هذه الشروط يكون للتوقيع المتقدم الحجية القانونية الكاملة في الإثبات.

أما على **المستوى التشريعات الوطنية** فقد عرف المادة 1316-4 من **القانون المدني الفرنسي** التوقيع بأنه التوقيع الضروري لاكتمال التصرف القانوني، و الذي تحدد هوية من يحتج به عليه و يعبر عن رضاء الأطراف بالالتزامات الناشئة عن هذا التصرف و عندما يكون التوقيع إلكترونيا، ينبغي استخدام وسيلة آمنة لتحديد الشخص بحيث تضمن صلته بالتصرف الذي وقع عليه."[1]

---

[1] – 1316-4: " La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose.Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public، elle confère l'authenticité à l'acte. Lorsqu'elle est électronique، elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé

كما عرف **القانون الفيدرالي الأمريكي للتجارة الإلكترونية لعام 2000** التوقيع الإلكتروني بأنه: "أصوات أو إشارات أو رموز أو أي إجراء آخر يتصل منطقيا بنظام معالجة المعلومات إلكترونيا، و يقترن بتعاقد أو مستند أو محرر و يستخدمه الشخص قاصدا التوقيع على المحرر أو المستند". و عرفته المادة الثانية من **القانون الفيدرالي السويسري** الخاصة بتقديم خدمات الشهادات في مجال التوقيع الإلكتروني الصادر بتاريخ 19 ديسمبر عام 2004 بأنه:" المعطيات الإلكترونية مجتمعة أو مرتبطة منطقيا بمعطيات إلكترونية أخرى و تستخدم في التحقق من مصداقيته". و التوقيع الإلكتروني في التعريف الأكثر تطورا هو الذي يعنى بالمتطلبات الآتية:

1- أن يرتبط فقط بصاحبه

2- يسمح بالتعرف على الموقع

3- أن يكون قد أنشئ بوسائل يحفظها الموقع تحت رقابته المنفردة

4- يرتبط بالمعطيات التي يتعلق بها بحيث أن كل تغيير لاحق عليها يمكن اكتشافه.

و يلاحظ أن **القانون التونسي رقم 83 لسنة 2000 بشأن المبادلات و التجارة الإلكترونية** لم يتضمن تعريفا للتوقيع الإلكتروني و لكنه أشار إلى العناصر المكونة له حيث عرفت المادة 6/2 منظومة إحداث الإمضاء بأنها مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات المهيأة خصيصا لإحداث إمضاء إلكتروني. و أضافت الفقرة "7" من ذات المادة أن منظومة التدقيق في الإمضاء هي مجموعة من عناصر التشفير العمومية أو مجموعة من المعدات التي تمكن من التدقيق في الإمضاء الإلكتروني.

بينما عرف **القانون الأردني رقم 85 لسنة 2001 بشأن المعاملات الإلكترونية** في المادة الثانية منه التوقيع الإلكتروني بأنه:"الأصوات الإلكترونية أو الرموز أو المعالجة أو التشفير الرقمي التي تبين هوية الشخص المعني الذي وضع هذه الإشارات على المستند من أجل توقيعه و بغرض الموافقة على مضمونه". ووفقا للمادة الأولى من **مشروع قانون التجارة الإلكترونية في مصر لعام 2001** فإن التوقيع الإلكتروني هو:" حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع و تمييزه عن غيره".أما وفقا للمادة 3/1 من القانون المصري رقم 15 لسنة 2004 بشأن تنظيم التوقيع الإلكتروني فإن التوقيع الإلكتروني هو:" ما يوضع على محرر إلكتروني و يتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها و يكون له طابع منفرد يسمح بتحديد شخص الموقع و يميزه عن غيره". وقررت الفقرة 5. من ذات المادة بأن الموقع هو: "الشخص الحائز على بيانات إنشاء التوقيع، ويوقع عن نفسه أو عمن ينيبه أو يمثله قانونا".

---

est présumée، jusqu'à preuve contraire، lorsque la signature électronique est créée، l'identité du signataire assurée et l'intégrité de l'acte garantie، dans des conditions fixées par décret en Conseil d'Etat".

وتقرر المادة الثانية من **القانون الإماراتي رقم 2 لسنة 2006 بشأن المعاملات و التجارة الإلكترونية** بأن التوقيع الإلكتروني هو:" توقيع مكون من حروف أو أرقام أو رموز أو أصوات معالجة ذي شكل إلكتروني و ملحق أو مرتبط منطقيا برسالة إلكترونية و ممهور بنية توثيق أو اعتماد تلك الرسالة".

وعرف **المشرع السعودي في نظام التعاملات الإلكترونية لعام 2007** في المادة 14/2 التوقيع الإلكتروني بأنه: "بيانات إلكترونية مدرجة في تعامل إلكتروني أو مضافة إليه أو مرتبطة به منطقيا تستخدم لإثبات هوية الموقع و موافقته على التعامل الإلكتروني و اكتشاف أي تعديل يطرأ على هذا التعامل بعد التوقيع عليه". وتضيف الفقرة 16 بأن الموقع هو:" شخص يجري توقيعا إلكترونيا على تعامل إلكتروني باستخدام منظومة توقيع إلكتروني".

و كذلك الشأن بالنسبة **للقانون الجزائري** حيث إعتمد المشرع الجزائري بالتوقيع الإلكتروني لأول مرة في نص المادة 2/327 مدني جزائري المعدلة بالقانون 05-10[1] والتي تنص على " ... يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر أعلاه.." وذلك من أجل إضفاء الحجية على المحررات الإلكترونية.

أما عن تعريف التوقيع الإلكتروني، فإن القانون الجزائري يميز بين التوقيع الإلكتروني المؤمن وذلك بموجب المادة 3 من المرسوم التنفيذي 07-162[2] و الناصة على: " التوقيع الإلكتروني هو أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر 1[3]. كما يعتبر القانون 03-15[4] المتضمن الموافقة في الأمر 03-11 [5] المتعلق بالنقد والقرض أول قانون جزائري تضمن التعامل الإلكتروني الحديث في القطاع المصرفي، ويتضح ذلك من خلال المادة 69 التي تضمن نصها " تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكون السند أو الأسلوب التقني المستعمل"و يتبين من خلال هذا النص نية المشرع الجزائري الانتقال من وسائل الدفع الكلاسيكية إلى وسائل دفع حديثة إلكترونية. كما نظم ممارسة نشاط التصديق الإلكترونيمن قبل مقدمي خدمات التصديق الإلكتروني بموجب المرسوم التنفيذي 07- 162 و الذي يشترط فيه الحصول على ترخيص تمنحه سلطة البريد والمواصلات السلكية واللاسلكية، وهذا الترخيص يكون مرفق بدفتر الشروط يحدد حقوق وواجبات مؤدي الخدمات والمستعمل.

---

[1]- القانون 05-10 المعدل والمتمم للامر 75-58 المتضمن القانون المدني

[2]- المرسوم 07-162 يعدل ويتمم المرسوم 01-123 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.

[3]- المادة 323 مكرر و323 مكرر 1 من القانون المدني الجزائري تعرف الكتابة الإلكترونية.

[4]- الجريدة الرسمية، العدد 52.

[5]-الجريدة الرسمية، العدد 64.

أما عن الأشخاص الذين يجوز لهم قانونا ممارسة هذا النشاط، يجب أن تتوفر فيهم نفس الشروط لممارس نشاط تقديم الانترنت في الجزائر. [1]

و تجدر الاشارة إلى أن نشاط مقدمي خدمات التصديق الإلكتروني يعتبر نشاطا اقتصاديا يخضع للقيد التجاري طبقا للقانون التجاري.وبذلك تكون جهة التوثيق الالكتروني[2] مسؤولة عن توثيق العقد الإلكتروني، الأمر الذي يجعل الوضع تطبيقا لمهمة الموثق العادي.

الفرع الثاني: التعريف الفقهي للتوقيع الالكتروني.

و في نطاق التعريفات الفقهية، يرى البعض بأن تعريف التوقيع الإلكتروني هو: "مجموعة حروف أو أرقام أو رموز أو أصوات إلكترونية أو تشفير رقمي أو أي نظام معالجة إلكتروني آخر، بحيث يمكن أن يعبر عن رضاء أطراف التصرف القانوني و أن يميز و يحدد هوية شخص موقعه، بحيث يمكن ارتباطه بمضمون المحرر الثابت على أية دعامة إلكترونية".

و يذهب اتجاه آخر إلى تعريفه بأنه:" رمز سري أو شفرة خاصة مما لا يفهم معناه، إلا صاحبه و من يكشف له عن مفتاحه، و بالتالي فهو يختلف عن شكل التوقيع التقليدي".

و يذهب اتجاه ثالث لتعريفه بأنه: "كل إشارات أو رموز أو حروف مرخص بها في الجهة المختصة باعتماد التوقيع و مرتبطة ارتباطا وثيقا بالتصرف القانوني، تسمح بتمييز شخص صاحبها و تحديد هويته، و تتم دون غموض عن رضائه بهذا التصرف القانوني".

و يعرفه اتجاه أخير بأنه: "مجموعة الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات و قبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته[3]."

---

[1]–المادة 3 من المرسوم 07–162 .

[2]– الموثق الإلكتروني هو طرف ثالث محايد يتمثل في أفراد أو شركات أو جهات مستقلة محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية. والوظيفة الأساسية للموثق الإلكتروني أو لجهة التوثيق الإلكترونية هي تحديد هوية المتعاملين في التعاملات الإلكترونية وتحديد أهليتهم القانونية في التعامل والتحقق من مضمون هذا التعامل وسلامته وكذلك جديته وبعده عن الغش والاحتيال. ينظر ناجي الزهراء: التجربة التشريعية الجزائرية في تنظيم المعاملات الالكترونية المدنية و التجارية، ورقة مقدمة إلى المؤتمر العلمي المغاربي الأول حول المعلوماتية و القانون المنعقد في الفترة من 28 إلى 29 أكتوبر 2009، ص 13.

[3]– ينظر على التوالي: د/عصام عبد الفتاح مطر، المرجع السابق، ص211 و ما بعدها.د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص422 و ما بعدها. د/ إبراهيم الدسوقي أبو الليل، المرجع السابق، ص162 و ما بعدها.د/عبد الفتاح بيومي حجازي:التوقيع الالكتروني في النظم القانونية المقارنة،الطبعةالأولى،دار الفكر الجامعي، الاسكندرية،2005،ص14 و ما بعدها.عجابي الياس:الطبيعة القانونية للتوقيع الالكتروني،بحث مقدم في مجلة دراسات وأبحاث ضمن أعمال الملتقى الدولي الخاص بالتنظيم القانوني للانترنت و الجريمة الالكترونية يومي 27–2009/04/28، العدد 2009/01،جامعة الجلفة، ص 25.أزرو محمد رضا: التوقيع الالكتروني و مقتضيات الآمان القانوني، دراسة مقارنة، بحث مقدم في مجلة دراسات وأبحاث ضمن أعمال الملتقى الدولي الخاص بالتنظيم القانوني للانترنت و الجريمة الالكترونية يومي 27–2009/04/28، العدد 2009/01،جامعة الجلفة، ص 7.

و عليه يعتبر التوقيع الالكتروني وحدة قصيرة من البيانات، تحمل علاقة رياضية مع تلك البيانات الموجودة في الوثيقة. مع العلم أنها ترتب عليه نفس الآثار المترتبة عن التوقيع المادي.و هو يهدف إلى حفظ مستويات الأمن و الخصوصية للمتعاملين مع الشبكة من حيث الحفاظ على سرية المعلومات أو الوسائل، و إلى منع أي شخص آخر على الإطلاع أو تحريف أو تعديل الرسالة، كما أنه يحدد هوية المرسل والمستقبل و يتم عن طريقه التأكد من صحة المعلومات عن عدمها[1]. و هو نوعان:

التوقيع الرقمي أو الكودي:و يكون عن طريق استعمال أرقام يتم تركيبها لتكون في النهاية" كودا يتم التوقيع به".و هناك التوقيع البيومتري و يسمى التوقيع بطريقة Pen-on.[2]

المطلب الثاني:

ماهية جريمة العدوان على التوقيع الالكتروني عبر الإنترنت:

نعرض في هذا المطلب لتعريف جريمة العدوان على التوقيع الالكتروني و أركانها. و ذلك في الفرعين التاليين:

الفرع الأول: تعريف جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

الفرع الثاني: أركان جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

الفرع الأول: تعريف جريمة العدوان على التوقيع الالكتروني عبر الإنترنت:

يمكن تعريف جريمة العدوان على التوقيع الالكتروني بأنها:"هي كل جريمة تستعمل فيها شبكة المعلومات العالمية (الانترنت) و يكون محلها التوقيع الالكتروني و ذلك اما باتلافه أو استساخه أو تزويره و تقليده أو استعماله و هو مزورا مع علمه بذلك أو إفشاء بياناته أو استعمالها في القرض المقدم من أجله". و تصنف هذه الجريمة ضمن الجرائم الشكلية، أي أنها تعد من جرائم الخطر أو جرائم السلوك المجرد التي لا يتوقف تجريم السلوك فيها المتمثل في الحصول على التوقيع الالكتروني على تحقق نتيجة معينة.و انما يكفي تمام صناعة البرنامج أو النظام المعلوماتي اللازم لذلك [3].

-Didier GOBERT:Cadre juridique pour les signatures électroniques et les services de certificats، analyse de la loi du 9/07/2001،p3, http:// www.consultandraining.com.

-Djamel ADUCH: Signature électronique, aspects techniques,réglementaires et organisationnels, p 3-4-5&16.

[1]- د/ سليمان أحمد فاضل، المرجع السابق، ص159.

[2]- لمزيد من التفاصيل ينظر د/ هدى حامد قشقوش،(الحماية الجنائية للتجارة الالكترونية...) مرجع سابق، ص75.

-Dr/ Ahmad A.AL-GHADYA : Digital Signatures and Liability Issues Arising Out of Their Certification، Journal of Law,n°2، Vol 28,June 2004,p74.

[3]- لمزيد من التفاصيل ينظر د/عبد الفتاح بيومي حجازي،(التوقيع الالكتروني....) مرجع سابق، ص574.

هذا من جهة و من جهة أخرى، فان المشرع يجرم نوعين من الانتهاكات الواقعة ضد التواقيع و المستندات الإلكترونية، الأول و هو الإتلاف و التزوير في المجال المعلوماتي.و الثاني هو الحصول بدون وجه حق على المستندات و التواقيع الإلكترونية.

الفرع الثاني: أركان جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

و هي كغيرها من الجرائم تقوم على ثلاث أركان: ركن شرعي و ركن مادي و ركن معنوي.

أولا: الركن الشرعي

و الذي هو النص الجنائي الذي يجرم و يعاقب على الفعل غير المشروع و المتمثل هنا في جريمة العدوان على التوقيع الإلكتروني، و من بين القوانين التي تحوي نصوصا تجرم هذا السلوك القانون الفرنسي في المادة 444-1 قانون العقوبات الفرنسي و قانون العقوبات العماني في المادة 276 مكرر5 و قانون التوقيع الإلكتروني رقم 15 لسنة 2004 المصري في المادة 23[1].

ثانيا: الركن المادي

فأما الركن المادي فيأخذ إحدى الصور الآتية:

1/ إتلاف التوقيع الإلكتروني:و هو يتحقق بافقاد البرنامج المعلوماتي الخاص بالتوقيع الالكتروني قدرته على العمل، عن طريق نشر فيروس معلوماتي أو سكب الماء أو السائل على الوسيط الالكتروني المحفوظ عليه[2].

2/ استنساخ التوقيع الإلكتروني: حيث يقوم الجاني باختراق أحد المواقع من خلال معرفة الخادم المشترك فيه ذلك الشخص ثم يقوم بالبحث عن الهوية الإلكترونية الخاصة بذلك الشخص، و عندما يتوصل إليها يقوم باستنساخ التوقيع الإلكتروني الخاص به[3].

3/استعمال توقيع المزور مع علمه بذلك: و يقصد باستعمال التوقيع الإلكتروني المزور أو المعيب إبرازه و الاحتجاج به فيما زور من أجله و ذلك على اعتبار أنه صحيح.

و هذه الجريمة مستقلة عن جريمة التزوير، و تقوم على أركان ثلاثة: هي فعل الاستعمال و محل يقع عليه هذا الفعل و هو التوقيع الإلكتروني المزور أو المعيب أو الوسيط الإلكتروني المزور أو المحرر الإلكتروني المزور، ثم القصد الجنائي.و على ذلك إذا تحقق فعل الاستعمال فيما أعد التوقيع لأجله، قامت جريمة إساءة استعمال التوقيع الإلكتروني المزور في حق الجاني و عوقب بعقوبتها طالما أنه يعلم بتزويره وانصرفت إرادته إلى فعل الاستيلاء، و هكذا الحال بشأن استعمال محرر أو وسيط إلكتروني مزور. وجريمة استعمال التوقيع الإلكتروني المزور هي جريمة عمدية، صورة الركن المعنوي فيها هو القصد

---

[1]- لمزيد من التفاصيل ينظر ص 307 و ما بعدها من هذه الرسالة.

[2]- د/عبد الفتاح بيومي حجازي، المرجع السابق، ص542.

[3]- د/عصام عبد الفتاح مطر، المرجع السابق، ص366.

الجنائي بعنصريه العلم و الإرادة. فيجب أن يعلم الجاني أن التوقيع الإلكتروني أو المحرر الإلكتروني أو الوسيط الإلكتروني مزورا أو معيبا، و مع ذلك تتصرف إرادته إلى استعماله فيما أعد له[1].

4/ تزوير[2] و تقليد التوقيع الإلكتروني: و يتم هذا الفعل باستخدام برامج حاسوبية و أنظمة معلوماتية خاصة بذلك يتم تصميمها على غرار البرامج و الأنظمة المشروعة. أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، و استخدامها في تحقيق أغراضه[3].

5/ إفشاء بيانات التوقيع الإلكتروني أو استخدامها في غير الغرض المقدم من أجله: و يقصد بإفشاء البيانات نشرها على كثيرين على نحو يتحقق سماعهم اياه في وقت واحد، بصورة جماعية سواء كان ذلك بالقول أو بطريقة ميكانيكية كالميكروفون أو موجات الراديو.....، أي كل الوسائل التي تتحقق بها العلانية[4].

ثانيا: الركن المعنوي

هذا فيما يخص الصور التي تأخذها جريمة العدوان على التوقيع الإلكتروني و المكونة للركن المادي. أما فيما يخص الركن المعنوي فهذه الجريمة تعد من الجرائم العمدية التي يستلزم فيها القصد الجنائي العام أي علم و إرادة. فيجب أن يعلم الجاني بأنه يرتكب إحدى الصور المكونة للجريمة و التي سبق ذكرها. بالإضافة إلى علمه بالنتائج المرتبة عنها، و أن تتجه إرادته إلى ارتكاب هذه الأفعال.[5]

المطلب الثالث:

موقف التشريعات المقارنة من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت:

و نظرا لأهمية التوقيع الإلكتروني باعتباره البديل عن التوقيع اليدوي التقليدي في عصر المعلوماتية، فقد جرم المشرع – من خلال قوانين العقوبات الداخلية و بعض التشريعات الخاصة – شتى أنواع الانتهاكات الواقعة ضد التوقيع و المستندات الإلكترونية سواء في الدول الغربية أو العربية. و سيتم تفصيل موقف هذه التشريعات في الفرعين التاليين:

الفرع الأول: موقف التشريعات الغربية من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

الفرع الثاني: موقف التشريعات العربية من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

---

[1]– د/ سليمان أحمد فاضل، المرجع السابق، ص165.

[2]– يقصد بالتزوير تغيير الحقيقة بقصد الغش في محرر بطريقة بينها القانون تغييرا يؤدي إلحاق الضرر بالغير. د/ محمد صبحي نجم، المرجع السابق، ص30.

[3]– د/عصام عبد الفتاح مطر، المرجع السابق، الموضع السابق.

[4]– د/عبد الفتاح بيومي حجازي،(التوقيع الالكتروني....) مرجع سابق، ص591.

[5]– د/عبد الفتاح بيومي حجازي، نفس المرجع، ص544 و 548 و 552 .

الفرع الأول: موقف التشريعات الغربية من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت.

و سنحصر التكييف القانوني لجريمة العدوان على التوقيع الالكتروني في التشريعات الغربية على **التشريع الفرنسي فقط** و ذلك على النحو الآتي:

لقد استحدث القانون الفرنسي نصوصا تشريعية وسعت في مجال التزوير بحيث أصبح لا يقتصر على ما يصدق عليه وصف المحرر المكتوب فقط،بل امتد ليشمل أيضا أي دعامة أو جزء بما في ذلك الدعامات المستخدمة في مجال الحاسب الآلي. أي أن التزوير يمتد ليشمل المستندات المعلوماتية. و هذا ما قرره المشرع الفرنسي في المادة 444-1 قانون العقوبات الفرنسي و الناصة على:"يعتبر تزويرا كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر، و يعاقب على ذلك بالحبس لمدة ثلاث سنوات و بغرامة مالية قيمتها45000 يورو ."[1]

الفرع الثاني: موقف التشريعات العربية من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت. و سنحصر التكييف القانوني لجريمة العدوان على التوقيع الالكتروني في التشريعات العربية[2] على **التشريع الجزائري فقط** و ذلك على النحو الآتي:

---

[1] – 441-1 :" Constitue un faux toute altération frauduleuse de la vérité، de nature à causer un préjudice et accomplie par quelque moyen que ce soit، dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende".

و تجدر الاشارة إلى أن المشرع الفرنسي قد نص في المادة 5/452 من القانون رقم 19 لسنة 1988 على معاقبة كل شخص قام بتزوير مستندات آلية أيا كان شكلها و أدى ذلك إلى إحداث ضرر للغير بالحبس مدة تتراوح ما بين سنة و خمس سنوات.

[2]– انقسمت التشريعات العربية في تكييفها لهذه الجريمة قسمين: قسم اعترف بهذه الجريمة و عاقب على ارتكابها، و قسم آخر صمت و لم يبين موقفه حيالها. و من **التشريعات التي تعاقب على هذه الجريمة قانون العقوبات العماني** في المادة 276 مكرر 5 و التي تنص على: "يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر و لا تزيد عن سنتين و بغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب تزوير بيانات أو وثائق مبرمجة أيا كان شكلها". و كذا المادة 380 من قانون العقوبات القطري المعدل بالقانون 11 سنة 2004 والناصة على:" يعاقب بالحبس مدة لا تتجاوز خمس سنوات كل شخص ارتكب تزويرا في المستندات المعالجة آليا، أيا كان شكلها، ترتب عليه الإضرار بالغير أو استعمل هذه المستندات المزورة مع علمه بذلك." و المادة 23 من قانون التوقيع الإلكتروني رقم 15 لسنة 2004 المصري على: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس و بغرامة لا تقل على عشرة ألاف لا تقل عن عشرة آلاف جنيه و لا تتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

أ- أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر.

ب- استعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بذلك.

لم يوفر المشرع الجزائري الحماية الجنائية لذلك التوقيع على عكس نظيره التوقيع اليدوي الذي وفر له الحماية الجنائية من خلال تجريمه للتزوير في المحررات الرسمية و العمومية في المادة 214 من قانون العقوبات الجزائري في فقرتها الأولى.[1] فهناك غياب لنص جنائي يجرم و يعاقب على جريمة العدوان على التوقيع الالكتروني.

و باستقرائنا لنص هذه المادة نجد أن المشرع الجزائري نظم التزوير التقليدي الذي يكون بوضع توقيعات مزورة على محرر عادي رسمي أو عمومي، أي أنه وفر الحماية الجنائية للتوقيع التقليدي فقط .إلا أنه كان من الواجب عليه أن يوسع مفهوم المحرر من أجل ادماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير للكلام عن التوقيع الالكتروني. و عليه يمكن القول أن المشرع الجزائري لم يستحدث نصوصا عقابية لمواجهة جريمة العدوان على التوقيع الالكتروني و التي تكون إما بتزويره أو بإفشاء بياناته أو استخدامها في غير الغرض المقدم من أجله إلى غيرها من السلوكيات الاجرامية التي يمكن أن يكون محلا لها، و التي لايمكن التحدث عنها إلا إذا كان المحرر هو عبارة عن مستند معلوماتي.

ت- توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكترونيا أو اخترق هذا الوسيط أو اعترضه أو عطله من أداء وظيفته."

و تجدر الإشارة هنا أن المشرع المصري قد اقتصر التجريم في هذه الجريمة على البيانات و الوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص بإصدار شهادات التصديق الإلكتروني أو اتصل بها بحكم عمله". و المادة 4 من القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات على: " يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية و المحلية معترف به قانونا في نظام معلوماتي.

و تكون العقوبة الحبس و الغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر".

كما ورد في المادة 16 من الباب الثاني المعنون التجارة و المعاملات الإلكترونية من مشروع القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات و الاتصالات إذ نصت على:" للتوقيع الإلكتروني نفس القيمة في الإثبات المقررة للتوقيع التقليدي، و يتمتع بالحماية الجنائية المقررة للتوقيع التقليدي في حالة التزوير وفقا للنصوص المقررة في قانون العقوبات.

و يعاقب بالعقوبة المقررة لجريمة التزوير حسب الأحوال من استعمل المستند المزور مع علمه بتزويره".

[1] – تنص المادة 1/214 من قانون العقوبات الجزائري على: " يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته:

1– إما بوضع توقيعات مزورة."

[2] – المستند المعلوماتي: و هو ذلك المستند غير المعالج آليا و تعتبر مستندات معلوماتية الأوراق المعدة لتسيطر المعلومات عليها، و الأقراص الممغنطة التي لم يسجل عليها أي شيء بعد، و الملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرنامج، و كذلك أيضا البطاقات البنكية التي لم تدخل الخدمة بعد، و هذه و إن كان مسجلا عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة، إلا أنه لم يتم معالجتها بعد، إذ أنها ما زالت في مرحلة الاعداد فقط. آمال قارة ، المرجع السابق، ص 135.

خلاصة الباب الثاني

لقد أدى سوء استخدام شبكة الإنترنت الى ظهور طائفة جديدة من الجرائم المستحدثة و التقليدية التي تطال الذمة المالية للأشخاص سميت بجرائم الإعتداء على الأموال عبر الإنترنت، و التي تضم جريمة السرقة والنصب و الإعتداء على الملكية الفكرية كجرائم تقليدية قديمة في اسمها و حديثة في طريقة تنفيذها، وجريمة غسل الأموال و المخدرات و الإعتداء على التجارة الإلكترونية كجرائم مستحدثة، وبذلك يمكن الوقوف على النتئج التالية:

أولا– فيما يخص جريمة السرقة عبر الإنترنت ، فهي نوع من السرقة المعلوماتية، التي تعرف بأنها ختلاس للمعلومات و نقلها من حيازة صاحبها (و ان لم تكن حيازة كاملة) الى الغير باستخدام الإنترنت. حيث تختلف السرقة عبر الإنترنت عن تلك الواقعة في العالم المادي في كون أن محل الإعتداء هو المعلومات، و التي اختلف الفقه حولها.

تقوم السرقة عبر الإنترنت على ثلاث أركان تتميز بطبيعة خاصة نظرا للوسط الذي ترتكب فيه، و هي موضوع أو محل الإعتداء و يتمثل في المعلومات التي تأخذ شكل نبضات إليكترونية وهي ذات طبيعة معنوية أو بالأحرى المال المعلوماتي و ركن مادي و يتمثل في فعل الاختلاس المعلوماتي و ركن معنوي ويتمثل في القصد الجنائي.

ثانيا–أما فيما يخص جريمة النصب عبر الإنترنت، فانها تعبر من أشد و أكثر جرائم الأموال المتداولة والمنتشرة عبر الشبكة،فهي تحتل المرتبة الأولى في العالم الإفتراضي على عكس ما هو متعارف عليه في العالم المادي أين تتسيد جريمة السرقة جرائم الأموال، لكونها سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي.

ثالثا– أن جرائم الإعتداء على الملكية الفكرية عبر الإنترنت و بالضبط الملكية الأدبية و الفنية و الحقوق المرتبطة بها أو المجاورة، قد تأثرت بالتطور التكنولوجي المعتمد خاصة على الحواسيب و شبكة الإنترنت، اذ أفرزت أنماطا و أنواعا جديدة من مصنفات الإبداع الفكري تسمى بمصنفات تقنية المعلومات و التي كانت في المقابل محلا للاعتداء باستخدام تلك الشبكة.

و تتحقق عن طريق كل فعل غير مشروع يقع على حق المؤلف و المبدع لمصنفات أدبية أو فنية عن طريق استخدام تقنية الإنترنت .

رابعا–أما فيما يخص جريمتي غسل الأموال و المخدرات عبر الإنترنت، فقد خلصنا الى النتائج التالية:

–أن جريمة غسل الأموال عبر الإنترنت، تتحقق في إظهار الأموال المتحصلة من جرائم الاتجار بالتجارة غير المشروعة مثل المخدرات والإرهاب والقمار وغيرها بصورة تتمتع بقانونية المصادر وشرعيتها عبر استخدامها لشبكة الإنترنت كأداة لإخفاء هذا المصدر غير المشروع أو ذاك الذي تحصلت منه هذه الأموال، وتعود فكرة جريمة غسل الأموال عبر الانترنت إلى عصابات الجريمة المنظمة من حيث المصدر.

–في حين أن جريمة المخدرات عبر الإنترنت، تكون بتكنلجة المخدرات والمؤثرات العقلية، وهو تعبير يشمل اجتماع التعامل بالمخدرات والمؤثرات العقلية بتكنولوجيا المعلومات/ الإنترنت وذلك باستخدام وسائلها في تسهيل التعامل غير المشروع بالمؤثرات العقلية والمخدرات، فهي تستعمل في الاتجار غير المشروع لتلك المواد السامة وفي الترويج لها والتوزيع أيضا. وتقوم بفتح أسواق جديدة، وتساهم على التعرف على مستهلكين جدد.

خامسا–أما بالنسبة لجرائم الإعتداء على التجارة الإلكترونية عبر الإنترنت ، وتتحقق عن طريق عدة صور تتمثل في: جرائم الإعتداء على مواقع و بيانات التجارة الإلكترونية و جرائم الإعتداء على بطاقات الإئتمان و جريمة الإعتداء على التوقيع الإلكتروني.

الباب الثالث:

جرائم العدوان على أمن الدولة عبر الإنترنت

تحتل جرائم العدوان على أمن الدولة أو ما يسمى بالجرائم الماسة بأمن الدولة و شخصيتها مكانة هامة في كل من التشريع المقارن[1] كجرائم جنائية بالدرجة الأولى –حتى و لو تم إضفاء الطابع السياسي عليها في بعض التشريعات– و كذا في المعاهدات الدولية و ذلك على الرغم من أن مرتكبيها من الأفراد، نظرا لما تتميز به هذه الطائفة من الجرائم بخصائص خطيرة تميزها عن نظيرتها من الجرائم الواقعة على الأشخاص و تلك الواقعة على الأموال من أبرزها اتخاذها الطابع الدولي.

و يمكن تعريف جرائم العدوان على أمن الدولة بأنها:"تلك الجرائم التي ترتكب ضد الدولة بصفتها شخصا من أشخاص القانون العام الداخلي أو شخصا من أشخاص القانون الدولي العام"[2].و عليه فهي تصنف إلى صنفين اثنين: جرائم ماسة بأمن الدولة الداخلي و جرائم ماسة بأمن الدولة الخارجي.

و تعرف الأولى بأنها:"تلك التي ترتكب ضد الدولة بصفتها شخصا من أشخاص القانون العام الداخلي، وتستهدف إلحاق الضرر بها بصفتها سلطة عليا، أو تستهدف السيطرة عليها، و تغيير أحكام الدستور أو تعديلها بصفتها غير شرعية، أو إثارة العصيان المسلح ضد السلطات القائمة ومنعها من ممارسة وظائفها، أو غصب أو الشروع في غصب سلطة سياسية أو مدنية أو قيادة عسكرية "[3]. و القاعدة الجنائية في هذا النوع من الجرائم تهدف إلى حماية نظام الحكم، و شكل الحكومة و دستور البلاد العام و نشاطات السلطات في مواجهة المحكومين.

أما الجرائم الماسة بأمن الدولة الخارجي فهي:"تلك الجرائم التي ترتكب ضد الدولة بصفتها شخصا من أشخاص القانون العام، و التي تستهدف المساس بشخصية الدولة أو المساس باستقلالها أو بسيادتها

---

[1]– أخذت الجرائم المخلة بأمن الدولة مكان الصدارة بين كل الجرائم التي تنص عليها التشريعات المعاصرة و منها: قانون العقوبات المصري إذ تأتي الجرائم المخلة بأمن الدولة في المواد 77–105 و هي النصوص التي تشكل الباب الأول من القسم الأول من هذا القانون. و كذلك قانون العقوبات الليبي في المواد 165–217 و في القانون المغربي في المواد 175–216، و في القانون السوري في المواد 260–311 و في القانون اللبناني في المواد 174–215 و في القانون الجزائري في المواد 61–101. أما في القانون الايطالي فتأتي الجرائم المضرة بأمن الدولة التي يصطلح عليها "الجرائم الواقعة على شخصية الدولة" في المواد 241–294 قانون العقوبات (قانون روكو 1930) و في القانون الفرنسي فتأتي المواد المتعلقة بأمن الدولة في المواد 410–1 إلى 433–2 تحت عنوان الجرائم المضرة بالمصالح الأساسية للأمة و في القانون الإسباني في المواد 58–77 قانون العقوبات وفي القانون الألماني في المواد80–101عقوبات وفي القانون النمساوي في المواد 58–77عقوبات و في البلجيكي المواد73– 124عقوبات.

[2]– د/محمد سليمان موسى:الجرائم الواقعة على امن الدولة، دراسة مقارنة في التشريعات العربية والقانونين الفرنسي والايطالي في ضوء المفاهيم الديمقراطية الدستورية المعاصرة ومبادئ حقوق الانسان، دار المطبوعات الجامعية، الإسكندرية، 2009، ص8.

[3]– د/ عبد القادر عدو،المرجع السابق، ص272

ووحدتها و سلامة أراضيها"[1]. و من أمثلتها جرائم الخيانة و التجسس، و جرائم التعاون مع أعداء الدولة و حمل السلاح في صفوفهم.

و في كل الأحوال فإن المشرع في كل دولة يلتزم بسن التشريعات التي تحمي الدولة كشخص معنوي قانوني و سياسي، قائم بذاته محافظة على الاستقرار فيها، إذ أن ذلك يؤدي إلى استمرار مكانتها في المجتمع الدولي، أي ثبات مكانة الدولة كمجموع واحد[2]. و هو في هذا يتجه إلى رصد نصوص خاصة في مدونته العقابية لأحكام كيفية التعامل مع هذه النوعية من الجرائم، سواء من حيث القاعدة الموضوعية أو الإجرائية.

و لقد تأثرت هذه الجرائم كغيرها من الجرائم الواقعة على الأشخاص و كذا الواقعة على الأموال بالتطور التكنولوجي و ما أفرزه من تقنيات عالية من بينها تقنية الإنترنت التي فتحت الباب أمام مجرمي المعلوماتية في ارتكاب جرائمهم بكل سهولة و ارتياح، خاصة و أن العالم الإفتراضي هو عالم لا يعترف بالدولة بل حتى بوجود حدود إقليمية، و ليس به سلطة مركزية تحكمه، كما أن لا أحد يستطيع الإدعاء بملكيته. الأمر الذي ساهم في انتشار الجرائم التي كانت صعبة الارتكاب في العالم المادي عبر الإنترنت كقيام الدول بإعداد العدة لمواجهة بعضها البعض. كما هو شأن في الولايات المتحدة في مفاوضاتها المستمرة للتحكم في قدرة الشركات على إعداد برمجيات يمكنها اختراق أجهزة الحاسوب حول العالم. و كذلك ما تقوم به آلة الحرب العسكرية The defense Agency في اليابان من إعداد أسلحة تستخدم في العالم الإفتراضي Cyberweapon تتكون من فيروسات مضادة للاختراق و كذلك برمجيات اختراق ذاتية. و الحقيقة أن مثل هذا الأمر ليس بغريب، إذا علمنا أن مثل هذه النوعية من الأسلحة يمكن إعدادها بطريقة بناء الأنظمة الحاسوبيةComputer system[3].

و لهذا خصصنا هذا الباب لدراسة الجرائم الماسة بأمن الدولة و التي تمثل الإنترنت فيها تربة خصبة وأرضية ممتازة لارتكابها بكل سهولة و بدون بذل أي جهد عضلي كان لازما في السابق لارتكاب مثل هذه الجرائم و تحقيق أكبر عدد من الضحايا. و من أبرز و أشهر هذه الجرائم التي ترتكب عبر الإنترنت جريمتي الإرهاب و التجسس. و لقد تم التطرق إليها في الفصلين التاليين:

الفصل الأول: جريمة الإرهاب عبر الإنترنت

الفصل الثاني: جريمة التجسس عبر الإنترنت

---

[1]– د/ عبد القادر عدو، نفس المرجع ، ص273.

[2]– د/ مأمون سلامة:قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، الجزء الأول،، دار الفكر الجامعي، القاهرة، 1988، ص74.

[3]– د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن استخدام الإنترنت.....) مرجع سابق، ص646.

الفصل الأول:

الإرهاب عبر الانترنت

يعتبر الإرهاب الهاجس والشبح المرعب الذي تعيشه كل الدول وتتخوف منه، إذ أصبح جزء من الحياة اليومية فلا يكاد يمر يوما دون أن تقع عملية إرهابية في مكان ما من العالم، وتتناقلها وسائل الإعلام المرئية والسمعية بنوع من الإثارة والتضخيم.

ورغم أن الإرهاب قديم قدم التاريخ المكتوب ؛إلا انه و منذ الستينات في القرن الماضي اتخذ بعدا جديدا مثيرا للقلق.وذلك بسبب:

-انتشاره في بعض القارات الأخرى خاصة الشرق الأوسط بعد أن كان مقتصرا فقط على الدول الأوروبية.

-اتخاذه مساحة مرعبة في السنوات الأخيرة.

-إجتياح هذه التقنية الحديثة عالمنا هذا بصورة مذهلة مما يمكن الإرهابيون من تنفيذ عملياتهم الدموية المدمرة بأقل مجهود، ودون تمكن الجهات الأمنية من منعهم ابتداء أو من ضبطهم بعد ذلك[1].

ولقد كان لظهور شبكة المعلومات دور كبير في تنفيذ تلك العمليات؛الأمر الذي أدى إلى بروز نوع آخر من جرائم الانترنت يهدد امن الدولة ونظامها، سواء السياسي أو الاقتصادي أو الاجتماعي أو الأمني، باستتبابه الفوضى واللااستقرار، يسمى بالإرهاب الإلكتروني أو الإرهاب عبر الإنترنت.والذي سيتم تناوله بالتفصيل في المبحثين التاليين كالآتي:

المبحث الأول:الأحكام العامة للإرهاب.

المبحث الثاني:ماهية الإرهاب عبر الانترنت.

المبحث الأول:

الأحكام العامة للإرهاب.

شهد العالم خلال النصف الثاني من القرن الماضي تطورا كبيرا في النشاطات الإرهابية التي أصبحت تهدد استقرار الدول وامن المواطن وتؤثر على جهود التنمية الاقتصادية وعلى التطور في جميع الميادين.وقد تجاوزت الأعمال الإرهابية حدود الإقليم الواحد، وتجاوزت أثارها وأضرارها الحدود الإقليمية إلى الدولية ؛واكتسبت بذلك طابعا دوليا. وهذا ما جعلها جريمة خطيرة ضد النظام الدولي، ضد مصالح الشعوب الحيوية، ضد الأمن والسلام في العالم وضد حقوق وحريات الأفراد الأساسية، فجريمة الإرهاب بالمفهوم المعاصر للارهارب[2] بدأت منذ ثلاثينات القرن الماضي مع مقتل الملك اليوغوسلافي ووزيرا لخارجية

---

[1] – د/حسنين المحمدي بوادي، المرجع السابق، ص 15 .

[2] – لقد أطلق مصطلح الإرهاب للمرة الأولى، لوصف الأعمال التي يقوم بها "روسبير ورفاقه" من خلال المحكمة التي شكلتها حكومة الثورة لمحاكمة المناهضين، وقد اقترن الإرهاب بالحكومات في الحقبة الأولى للثورة الفرنسية 1789-1794. ولهذا عرف الحكم الذي أعقب قيام الثورة الفرنسية بحكم "الإرهاب "، ولهذا السبب أيضا نلاحظ أن قاموس لاروس الفرنسي

الفرنسي عام 1934 بمرسيليا. وتطورت خلال السبعينات والثمانينات، حيث عرف العالم العديد من عمليات اختطاف الطائرات وحجز الرهائن. إلا أنها وصلت مع بداية التسعينات إلى مرحلة من الوحشية لم تعرفها من قبل؛ فبدأت عمليات التخريب المأساوية تحدث على أوسع نطاق وكذا الاغتيالات الجماعية والفردية، واختطاف الأشخاص واحتجازهم كرهائن. ولم يسلم من الأعمال الإرهابية لا الشيوخ ولا النساء ولا الأطفال ومن كل الفئات[1] والسؤال الذي يطرح هنا هو: ماذا نعني بالإرهاب؟ وما هي صوره وخصائصه؟ وما هو الفرق بين الجريمة الإرهابية وغيرها من الجرائم المتشابهة لها؟ وما هي العوامل التي ساعدت في انتشار هذه الظاهرة الإجرامية الخطيرة؟ أسئلة سيتم الإجابة عليها في االمطالب التالية كالآتي:

المطلب الأول: ماهية الإرهاب.

المطلب الثاني: الفرق بين الإرهاب و بين ما يشابه من جرائم.

المطلب لثالث: الأسباب و العوامل المساعدة على انتشار الإرهاب..

المطلب الأول:

ماهية الإرهاب

نتناول في هذا المطلب تعريف الإرهاب و الخصائص التي يتمتع بها، و كذا أشكاله و نتائجه في الفروع التالية:

الفرع الأول: تعريف الإرهاب و خصائصه.

الفرع الثاني: أشكال الإرهاب و نتائجه.

الفرع الأول: تعريف الإرهاب و خصائصه.

نتطرق في هذا الفرع إلى تعريف الإرهاب من حيث اللغة والفقه و القانون ، ثم نبين الخصائص و المميزات التي يتميز بها هذا النوع من الاجرام الماس بأمن الدولة. و ذلك كمايلي:

أولا: تعريف الإرهاب

1/ لغة: رهب، يرهب، ترهيبا أي خوف والإرهابي هو من يلجأ إلى الإرهاب لإقامة سلطته.والحكم الإرهابي هو نوع من الحكم الذي يقوم على الإرهاب والعنف [2].

يعرف الإرهاب بأنه:" نظام من العنف تؤسسه الحكومات والحركات السياسية" د/محمد سليمان موسى، المرجع السابق، الهامش رقم 1، ص628.

[1] – بوحنة محمد: الأدوات القانونية لمكافحة الإرهاب، مجلة الشرطة، العدد 71، فيفري 2004، ص3.

[2] – قاموس المنجد في اللغة والإعلام، ص282.

2/ فقها: من المتعارف عليه أن مهمة تعريف الجريمة وتحديد عناصرها وبيان أركانها عمل قانوني يضطلع به عادة فقهاء القانون والمفكرين ورجال العدالة الجنائية.ولكن ومنذ أن ظهرت الجريمة الإرهابية بشكلها المعاصر تصدى لها السياسيون بالتعريف والوصف. دون الرجوع إلى الفقه والقضاء أو الشرائع السماوية. وكانت النتيجة دخول المجتمع الدولي في خلاف طويل حول تعريف الإرهاب[1]. فلحد الآن لم يتفق ذلك الأخير على تحديد مفهوم شامل و موحد للإرهاب، تلك الآفة التي لا تعرف حدودا ولا دينا ولا جنسية. فقد تباينت التعريفات بين من يعتبرها عمل نضالي مشروع ومباح ضد العدو ومن يعتبرها عمل إجرامي تجرمه كل القوانين والشرائح.وفي هذا الصدد اجتهد بعض فقهاء الفقه الجنائي والباحثين في إعطاء بعض التعريفات للإرهاب. وكانت أولى تلك المحاولات هي تلك التي بذلت في أثناء المؤتمر الدولي الأول لتوحيد قانون العقوبات الذي عقد في "وارسو" سنة 1930.وعلى هذا عرف الفقه الإرهاب بأنه: " عنف منظم ومتصل بقصد خلق الرعب والتهديد العام الموجه إلى دولة أو جماعة سياسية وترتكبه منظمة بقصد تحقيق أهداف سياسية "[2].

أوبأنه: " إستراتجية تتسم بعنف دولي الطابع تدفعها إيديولوجية صممت لإدخال الرعب في فئة من مجتمع لتحقيق مكاسب سلطوية أو دعاية لحق أو ضرر بصرف النظر عن الجهة المستفيدة، سواء كان المنفذون يعملون لمصلحتهم أو مصلحة الغير".[3]

أو بأنه: " الاستخدام غير المشروع للعنف أو التهديد به بواسطة فرد أو مجموعة أو دولة ضد فرد أو جماعة أو دولة ينتج عنه رعبا يعرض للخطر أرواحا بشرية أو يهدد حريات أساسية و يكون الغرض منه الضغط على الجماعة أو الدولة لكي يغير سلوكها اتجاه موضوع ما"[4].

---

[1]– إذ ظلت الأمم المتحدة نتيجة ذلك تتردد لأكثر من نصف قرن في اتخاذ التدابير اللازمة لمكافحة الإرهاب. ويتضح ذلك جليا من توصيات مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المذنبين، والتي اعتمدت بواسطة الجمعية العامة للأمم المتحدة عام 1992 في فقرتها الأولى والثانية.حيث جاء في الفقرة الأولى منها: " منذ أن أعدت الأمم المتحدة عام 1972 أول دراسة عن الإرهاب الدولي، لم يتمكن المجتمع الدولي من تحديد معنى متفقا عليه عالميا لما تشمله عبارة الإرهاب الدولي أ و الإرهاب، كما أنه لم يتوصل إلى اتفاق كاف بشأن التدابير اللازم اتخاذها لمنع مظاهر العنف الإرهابي المؤذية ومكافحتها ". وجاء في الفقرة الثانية منها: " ودون المساس بمناقشة الموضوع في الجمعية العامة للأمم المتحدة وريثما يتم الاتفاق على تعريف مقبول عالميا للإرهاب الدولي، من المفيد العمل على تعريف السلوك الذي يعتبره المجتمع الدولي غير مقبول ويرى أن تطبق بشأنه تدابير وقائية وقمعية فعالة تكون متمشية مع مبادئ القانون الدولي المتعارف عليه ".

د /محمد الأمين البشري، المرجع السابق، ص136

[2]– د/محمود سليمان موسى، المرجع السابق، ص 630.

[3]– ينظر علاء الدين راشد: المشكلة في تعريف الإرهاب، دار النهضة العربية، القاهرة، 2006، ص31.

[4] – ينظر د/محمد الأمين البشري، المرجع السابق، ص138–139.

و الإرهاب في نظر الفقيه "سوتيل " هو عبارة: "عن عمل اجرامي مصحوب بالرعب أو العنف أو الفزع بقصد تحقيق هدف معين "[1].

و عرفه الفقيه " بيمكن" بأنه: "كل فعل يقوم على تخويف الناس عن طريق استخدام العنف". ويذهب "هيفانوفيتش " إلى أن الإرهاب هو عبارة عن:"أعمال من طبيعتها أن تثير لدى الناس، الإحساس بالتهديد ومن ثم ينتج عنها الإحساس بالخوف من الخطر على أي صورة "[2].

ويرى البعض أن للإرهاب مفهومين أو تعريفين، احدهما واسع يشمل كل جريمة سياسية يترتب على وقوعها أو التعبير عنها، إثارة الفزع العام لما لها من طبيعة خاصة. أما المفهوم الضيق فيتمثل في:" الأعمال الإجرامية التي يكون هدفها الأساسي هو نشر الخوف والرعب وذلك باستخدام وسائل تصلح لخلق حالة من الخطر العام [3].

أما الإرهاب في نظر الفقيه Niko GRUNZBURG فهو:" الاستعمال العمدي للوسائل القادرة على إحداث خطر عام يهدد الحياة أو السلامة الجسدية أو الصحية أو الأموال العامة." كما يعرف بأنه:"الاستخدام المنظم للعنف لتحقيق هدف سياسي و بصفة خاصة جميع أعمال العنف (حوادث الإعتداءات الفردية أو الجماعية أو التخريب) الذي تقوم به منظمة سياسية بممارستها على المواطنين لخلق جو من عدم الأمن وهو ينطوي على طوائف متعددة من الأعمال أخطرها احتجاز الرهائن و اختطاف الأشخاص و قتلهم ووضع المتفجرات أو العبوات الناسفة في أماكن تجمع المدنين أو وسائل النقل العامة و التخريب و تغيير مسائر الطائرات بقوة[4]".

3/ قانونا: عرفت اتفاقية جنيف لقمع ومعاقبة الإرهاب لعام 1937م، في مادتها الأولى على أن الأعمال الإرهابية هي "الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف، أو يقصد بها، خلق حاله من الرعب في أذهان أشخاص معينيين، أو مجموعة من الأشخاص، أو عامة الجمهور".

– أما الاتفاقية الأوروبية لعام 1977م، فلم تأت بتعريف محدد للإرهاب فقد عددت مجموعة من الأفعال، منها ما كان قد حرم سابقا باتفاقيات دولية سابقة، أو كان التعامل الدولي حرمها، وأضاف إليها كل الأفعال الخطرة التي تهدد حياة الأشخاص أو أموالهم، ومن المأخذ على هذا التعريف عدم إرضائه الدول المشاركة، وذلك لعدم مصادقة أية دولة على الاتفاقية، وبحصر هذا التعريف بالإرهاب في بث الرعب بين الأشخاص أي بين العامة، لكن الحقيقة تشير إلى أن للإرهاب اهدافا ابعد واشمل.

---

[1]– Reuven YOUNG : Defining Terrorism، The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation, Boston College International and Comparative Law Review، Volume 29, Issue 1, Article 3, p3, http:// lawdigitalcommons.bc.edu

[1] – مؤنس محب الدين: الإرهاب، مجلة الأمن العام المصرية، العدد 94، السنة 24، جويلية 1981، ص 81.

[3]– ينظر لمزيد من التعريفات حول الإرهاب د/محمود سليمان موسى، المرجع السابق، ص230 وما بعدها

[4]– ينظر لمزيد من التعريفات بوحنة محمد، المرجع السابق، ص 4

– أما الاتفاقية العربية لعام 1998، فقد عرفت الإرهاب في مادتها الأولى فقرة 2 بأنه:"كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إفشاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر"[1].

كما تعد من الجرائم الإرهابية الجرائم المنصوص عليها في الاتفاقيات التالية (عدا ما استثنته منها تشريعات الدول المتعاقدة أو التي لم تصادق عليها):

– اتفاقية طوكيو والخاصة بالجرائم والأفعال التي ترتكب على متن الطائرات والموقعة بتاريخ 1963/9/14.

– اتفاقية لاهاي بشأن مكافحة الاستيلاء غير المشروع على الطائرات والموقعة بتاريخ 1970/12/16.

– اتفاقية مونتريال الخاصة بقمع الأعمال غير مشروعة الموجهة ضد سلامة الطيران المدني والموقعة بتاريخ 1971/9/23، والبروتوكول الملحق بها والموقع في مونتريال في 1974/8/10.

– اتفاقية نيويورك الخاصة بمنع ومعاقبة الجرائم المرتكبة ضد الأشخاص المشمولين بالحماية الدولية بمن فيهم الممثلون الدبلوماسيون و الموقعة في 1973/12/13.

– اتفاقية اختطاف و احتجاز الرهائن و الموقعة 1979/12/17.

– اتفاقية الأمم المتحدة لقانون البحار سنة 1983، وما تعلق منها بالقرصنة البحرية[2].

أما فيما يخص **التشريعات الداخلية** فقد اتجهت معظم التشريعات الجنائية إلى وضع نصوص جديدة تتعلق بمكافحة ظاهرة الإرهاب للتغلب على هذه الظاهرة على المستوى الوطني، وذلك تلبية للحاجات المحلية من جهة، وللوفاء بالالتزامات التي اضطلعت بها الدول بمقتضى اتفاقيات دولية من جهة أخرى. ومن هذه التشريعات:

– القانون رقم 82 لسنة 1982 في فرنسا و الخاص بمكافحة الإرهاب وطبقا للمادة الأولى منه فان الإرهاب:" يتمثل في خرق القانون، يقدم عليه فرد من الأفراد أو تنظيم جماعي بهدف إثارة اضطراب جسيم في النظام العام عن طريق التهديد بالترهيب.

و كذا **قانون العقوبات الفرنسي الجديد** اذ تضمن بابا كاملا لجرائم الإرهاب و ذلك في المواد من 421-1 إلى 422 -5. بحيث عرف المشرع الفرنسي الإرهاب في المادة 421-1 بأنه: " هو كل نشاط يرتبط

---

[1]– ينظر محمد عبد المحسن سعدون:مفهوم الإرهاب و تجريمه في التشريعات الجنائية الوطنية و الدولية، ص 138– 139، http:// www.iasj.net

[2]– د/ محمد الأمين البشرى، المرجع السابق، ص 142-143.

بمشروع فردي أو جماعي يهدف إلى إحداث اضطراب جسيم في النظام العام بواسطة التخويف و بث الرعب[1].

و بذلك يكون المشرع قد حدد معيار الجريمة الإرهابية بناء على الباعث أو الغرض الخاص، و المتمثل في أن تكون هذه الجرائم على علاقة بمشروع فردي أو جماعي يهدف إلى الإخلال الخطير بالنظام العام عن طريق التفزيع أو الرعب.[2]

– أما بالنسبة **للتشريع الأمريكي** فقد عرف المشرع الأمريكي ظاهرة الإرهاب في المادة 2656 من القانون الأمريكي بأنه: " عنف له دوافع سياسية و موجه ضد أهداف مدنية من قبل منظمات سرية بقصد التأثير على الرأي العام".

– **قانون العقوبات السوري**، إذ عرف تلك الظاهرة الخطيرة في المادة 304 و ذلك كالأتي: " يقصد بالإعمال الإرهابية، جميع الأفعال التي ترمي إلى إيجاد حالة ذعر وترتكب بوسائل كالأدوات المتفجرة والأسلحة الحربية و المواد الملتهبة و المنتجات السامة أو المحرقة والعوامل الوبائية أو الجرثومية التي من شأنها أن تحدث خطرا عاما."

– القانون رقم 97 لسنة 1992 المعدل و المتمم **لقانون العقوبات المصري**، إذ تضمنت المادة 86 منه تعريف ظاهرة الإرهاب و ذلك كما يلي:"يقصد بالإرهاب في تطبيق أحكام هذا القانون كل استخدام للقوة أو العنف أو التهديد أو الترويع، يلجأ إليه الجاني لتنفيذ مشروع إجرامي فردي أو جماعي بهدف الإخلال بالنظام العام و تعريض سلامة المجتمع و أمنه للخطر، إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو الاتصالات أو المواصلات أو بالأموال أو بالمباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو وضع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها، أو تعطيل تطبيق الدستور أو القوانين أو اللوائح ".

– **القانون الجزائري** من خلال الأمر رقم 95–11 المؤرخ في 1995/12/25 الذي ألغى المرسوم التشريعي رقم 95–03 المؤرخ في 1995/12/30 و المتعلق بمكافحة أعمال التخريب و الإرهاب في الجزائر والتي أدمجت أحكامه في قانون العقوبات(المواد 87 مكرر– 87 مكرر10). فإلى غاية سنة 1991 عاشت الجزائر بعيدا عن الظاهرة إلى أن حلت سنة 1992 بظهور الإرهاب في أبشع صوره والذي سميت بالعشرية

---

[1] – Art.421–1: « constituent des actes de terrorisme، l'orsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes..... ».

وتجدر الإشارة إلى إن المشرع الفرنسي قد صنف الجرائم الإرهابية ضمن جرائم القانون العام وهي تضم الجرائم التالية: المساس بالحياة، المساس الإرادي بسلامة الشخص، الخطف والاحتجاز وتحويل وسائل النقل وكذا السرقة وأعمال التخريب والهدم والنصب وكذا جرائم المعلوماتية بالإضافة على صناعة وحيازة الأسلحة وذخيرتها ومتفجرات....

[2]– د/ أحسن بوسقيعة:الوجيز في القانون الجزائي العام، الطبعة الرابعة، دار هومة، الجزائر، 2006، ص 48.

السوداء، والذي نزفت منها جميع فئات الشعب الجزائري و عانت منها[1]. ولقد عرف المشرع الجزائري الفعل الإرهابي أو التخريبي في المادة 87 مكرر على النحو الأتي: " يعتبر فعلا إرهابيا أو تخريبا كل فعل يستهدف أمن الدولة و الوحدة الوطنية والسلامة الترابية واستقرار المؤسسات و سيرها العادي عن طريق أي عمل غرضه ما يأتي:

– بث الرعب في أوساط السكان و خلق جو انعدام الأمن من خلال الإعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو المس بممتلكاتهم.

– عرقلة حركة المرور أو حرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية.

– الإعتداء على رموز الأمة و الجمهورية ونبش أو تدنيس القبور.

– الإعتداء على وسائل المواصلات والنقل والملكيات العمومية و الخاصة والاستحواذ عليها واحتلالها دون مسوغ قانوني.

– الإعتداء على المحيط و إدخال المادة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الانسان أو الحيوان أو البيئة الطبيعية في خطر.

– عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة و الحريات العامة وسير المؤسسات المساعدة للمرفق العام.

– عرقلة سير المؤسسات العمومية أو الإعتداء على حياة أعوانها أو ممتلكاتها أو عرقلة تطبيق القوانين و التنظيمات"

ويأخذ وصف الجريمة الإرهابية أو التخريبية إنشاء أو تأسيس أو تنظيم أية جمعية أوتنظيم أو جماعة أو منظمة يكون غرضها القيام بفعل إرهابي أو تخريبي. وكذا كل انخراط أو مشاركة مهما يكن شكلها، في الجمعيات أو الجماعات أو المنظمات المذكورة آنفا مع معرفة غرضها أو أنشطتها.[2]

كما يأخذ وصف الجريمة الإرهابية أو التخريبية الإشادة بالأفعال الإرهابية أو التخريبية أو تشجيعها أو تمويلها بأية وسيلة كانت[3]. وكذا إعادة طبع أو نشر الوثائق أو المطبوعات أو التسجيلات التي تشيد تلك الأفعال[4].

ويعتبر كذلك إرهابيا كل جزائري ينشط أو ينخرط في الخارج في جمعية أو جماعة أو منظمة إرهابية أو تخريبية مهما كان شكلها أو تسميتها،حتى وان كانت أفعالها غير موجهة ضد الجزائر[5].

---

[1]– ينظر المزيد من لتفاصيل حول ظاهرة الإرهاب في الجزائر أحمد أبو الروس: الإرهاب والتطرف والعنف في الدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2001، ص 200

[2]–المادة 87 مكرر 3 من قانون العقوبات الجزائري.

[3]– المادة 87 مكرر 4 من قانون العقوبات الجزائري

[4]– المادة 87 مكرر 5 من قانون العقوبات الجزائري

[5]– المادة 87 مكرر 6 من قانون العقوبات الجزائري

وتأخذ كذلك وصف الجريمة الإرهابية أو التخريبية حيازة أسلحة ممنوعة أو ذخائر أو استيلاء عليها أو حملها أو الاتجار فيها أو استيرادها أو تصديرها أو وصنعها أو تصليحها أو استعمالها دون رخصة من السلطة المختصة.

وكذا بيع عن علم أسلحة بيضاء، أو شرائها أو توزيعها أو استيرادها أو صنعها لأغراض مخالفة للقانون[1].

و أخيرا أضاف القانون 01-09 المؤرخ في 2001/6/26 فعلين آخرين يأخذان وصف تلك الجريمة وهما: انتحال صفة إمام مسجد و استعمال المسجد مخالفة لمهمته النبيلة[2].

وبرغم من تعريف الدول لأعمال الإرهاب في تشريعاتها الداخلية، فان هذا غير كاف. إذ انه لم تسلم تلك الأخيرة من النقد، و يرجع ذلك أساسا إلى عدم توصل المجتمع الدولي إلى الاتفاق على تعريف موحد لتلك الأعمال ضمن اتفاقية مخصصة لمثل هذه الأعمال[3].

وتجدر الإشارة إلى إن الجريمة الإرهابية هي كأي جريمة (سواء أكانت تامة أو ناقصة) ، ترتكب تنفيذا لغرض إرهابي في أي من الدول المتعاقدة، أو على رعاياها أو ممتلكاتها أو مصالحها يعاقب عليها قانونها الداخلي.

ثانيا:خصائص الإرهاب.

تتمتع الجريمة الإرهابية بخصائص تجعلها فريدة و مغايرة لغيرها من الجرائم، و هذا ما يمكن استخلاصه من التعريفات المذكورة أعلاه. و يمكن تلخيصها في:

1/ الجريمة الإرهابية هي جريمة منظمة من حيث العضوية والانضباط والطاعة.ولكن في المقابل ليست كل جريمة منظمة حدثا إرهابيا[4].

2/تعتبر الجريمة الإرهابية عملا غير مشروع يمتاز بالتنظيم والتخطيط المحكم و المستخدم فيه القوة و العنف و التهديد و الترويع. و هو يقع ضمن دولة واحدة أو يكون عابرا للحدود من طرف فرد واحد أو من قبل جماعة سواء برا أو بحرا أو جوا.

فأما فيما يخص القوة: فيكون بالاستخدام الفعلي لها أو بمجرد التلويح باستخدامها.فلا يعتبر عملا إرهابيا مجرد حمل السلاح (سواء كان ناريا أو ابيضا) حتى لو كان ظاهرا أو إمساكه باليد دون التلويح باستعماله و لو ضمنيا. واستخدام القوة لا يقتصر فقط على استخدام السلاح، فقد تكون بدونه مثل تنظيم مظاهرة شعبية و تحريكها كوسيلة من وسائل الضغط على الحكومة[5].

---

[1]- المادة 87 مكرر7 من قانون العقوبات الجزائري

[2]- المادة 87 مكرر 10 من قانون العقوبات الجزائري

[3]- لمزيد من التفاصيل ينظرد/ محمود سليمان موسى، المرجع السابق، ص 632 وبوحنة محمد، المرجع السابق، ص 5 وما بعدها و محمد عبد المحسن سعدون، المرجع السابق ، ص 137، http:// www.iasj.net

[4]- ينظر د/ أحمد فاروق زاهر، المرجع السابق، ص 20 و ما بعدها.

[5]- ينظر د/أحمد فتحي سرور: الوسيط في قانون العقوبات، القسم الخاص، دار الطباعة الحديثة، الطبعة الرابعة، 1999، ص85.

وأما فيما يخص العنف: فهو عبارة عن ممارسة الإرهابيين الضغط على السلطة السياسية لتحقيق غرض معين.وقد يتنوع هذا الآخر بين العسكري أو السياسي أو الفكري[1].

أما التهديد فنعني به: الضغط على إرادة شخص ما و تخويفه من أن ضررا سيصيبه هو أو سيصيب أشخاصا أو أشياء له بها صلة، مثل الاختطاف أو هتك العرض. وهو يهدف إلى زرع الخوف في النفوس[2].

أما الترويع: فهو اشد وأعلى درجات زرع الخوف.فهو يخلق ويبث الرعب لدى مجموع أفراد الشعب أو غالبيتهم، بجعلهم يعيشون في جو يسوده الرعب والقلق والخطر الدائم والمستمر. مثل وضع مواد متفجرة في الأماكن المزدحمة كالسوق أو المستشفيات أو اختطاف الطائرات واحتجاز المسافرين على متنها و طاقمها.

وتجدر الإشارة أن الترويع يختلف عن التهديد في كونه يحدث رعبا غريزيا أكثر من الثاني؛ أو بصيغة أخرى الترويع له مفهوم فسيولوجي على عكس التهديد الذي له مفهوم نفسي[3].

وفي جميع الأحوال يلزم أن يكون من شأن استخدام القوة والعنف والتهديد والترويع إحداث الإعتداء على النظام العام أو تعريض سلامة المجتمع وأمنه للخطر.

3/ توجه الجريمة الإرهابية عادة ضد المدنين الأبرياء –من المارة والمتفرجين – فهي نمط حديث من العنف الأعمى الذي لا يفرق بين الضحايا والأهداف المادية ؛فلم يسلم منه لا الشيوخ ولا النساء ولا الأطفال و من كل الفئات[4].

4/ الجريمة الإرهابية أيا كان نوعها أو دوافعها تؤدي إلى نتائج معروفة مثل التسبب في الموت والتفجير وإتلاف الأموال و الممتلكات و التسبب في خسائر مادية و بشرية[5].

5/ الجريمة الإرهابية تستقطب الإعلام للدعاية و لفت انتباه أكبر عدد من الناس؛ فلا يمر أسبوع لا تتناقل فيه وكالات الأنباء ووسائل الإعلام خبر إرهابي حدث في منطقة ما من العالم، و هذا ما جعل معدلات الإرهاب تزداد من حيث الكم ومن حيث الحجم[6].

6/ الإرهاب ظاهرة عالمية[7] يعاني منها العالم كله، فلقد أدرك العالم بعد التفجيرات التي شهدتها الولايات المتحدة الأمريكية في 11 سبتمبر 2001، أن الإرهاب لا يهدد دولا معينة بل يهدد جميع الدول حتى تلك

---

[1]– لمزيد من التفاصيل ينظر د/ رمسيس بهنام: قانون العقوبات، القسم الخاص، العدوان على أمن الدولة الداخلي، منشأة المعارف، الاسكندرية،1982، ص184.

[2]– ينظر د/ رؤوف عبيد: جرائم الإعتداء على الاشخاص و الاموال، الطبعة الثامنة، دار الفكر العربي، 1985، ص 421 و ما بعدها.

[3]– ينظر د/ إبراهيم عيد نايل: السياسة الجنائية في مواجهة الإرهاب، دار النهظة العربية، 1992، ص 19.

[4]– ينظر د/ محمد الامين البشرى، المرجع السابق،ص 144

[5]– ينظر د/ محمد الامين البشرى، نفس المرجع ، ص 145.

[6]– ينظر د/ محمد الامين البشرى، نفس المرجع ، ص146.

[7]– ينظر د/ أحسن بوسقيعة ، المرجع السابق، ص 45.

التي كانت تعتبر نفسها في وقت سابق في منأى عنه.وهذا ما جعل جميع دول العالم تعطي أهمية بالغة لمكافحة الإرهاب وتنضم إلى الاتفاقيات المبرمة في هذا الإطار و تصادق عليها و تتحالف مع دول أخرى للوقاية من هذه الآفة.

7/ الجريمة الإرهابية هي من جرائم الخطر ليس من جرائم الضرر، فلا يشترط حدوث فيها ضرر فعلي بل يكفي تعريض المصالح الاجتماعية التي أضفى عليها المشرع حمايته لخطر الضرر[1].

الفرع الثاني: أشكال الإرهاب و نتائجه.

تعد الجرائم الإرهابية أهم أنواع الجرائم الماسة بأمن الدولة، اذ تتضمن اعتداء على سلطة الدولة و على سير المؤسسات الدستورية فيها. وهي تتنوع وفقا للهدف و الغرض المقصود منها، كما أنها إلى نتائج وخيمة تمس بالنظام العام و المصلحة العامة. و سيتم تفصيل ذلك كمايلي:

أولا:أشكال الإرهاب.

يعتبر الإرهاب ظاهرة إجرامية عالمية تعاني و تنزف جميع الدول باختلاف أنظمتها و مختلف شعوبها دون التمييز بين الصغير والكبير، الغني و الفقير، الجاهل والمتعلم و هو على أشكال: فهناك إرهاب دولي و إرهاب داخلي و ارهاب فردي وآخر جماعي و ارهاب مشروع و آخر غير مشروع.

1/ الإرهاب الدولي: يعرف الإرهاب الدولي بأنه:" الإعتداء على الأرواح و الممتلكات العامة أو الخاصة بالمخالفة لأحكام القانون الدولي بمصادره المختلفة". كما يعرف بأنه: " استخدام أو التهديد باستخدام العنف ضد أفراد ويعرض للخطر أرواحا بشرية بريئة أو يودي بها أو تهديد الحريات الأساسية للأفراد لأغراض سياسية بهدف التأثير على موقف أو سلوك مجموعة مستهدفة بغض النظر عن الضحايا المباشرين"[2].

باستقرائنا لهذين التعريفين للإرهاب الدولي يمكن استخلاص بأنه عبارة عن جريمة دولية تتجاوز إقليم الدولة، أساسها مخالفة القانون الدولي، هدفها الإعتداء على الأرواح البشرية أو تعريضها للخطر و كذا الإعتداء على الممتلكات سواء العامة أو الخاصة، يرتكبها فرد أو جماعة أو دولة.كما تجدر الإشارة إلى أن الإرهاب الدولي يشمل أيضا أعمال التفرقة العنصرية التي تباشرها بعض الدول.

2/ الإرهاب الداخلي: وهو عكس الإرهاب الدولي إذ يقع داخل حدود دولة معينة، أي يعتبر جريمة داخلية وطنية تهدف امن الدولة و الوحدة الوطنية و السلامة الترابية و استقرار المؤسسات وسيرها العادي.اي انها جريمة وطنية تهدد النظام العام و السكينة العامة للدولة، و يطبق على مرتكبها (سواء أكان فردا أو جماعة

1- ينظر د/حسنين المحمدي بوادي، المرجع السابق،الهامش رقم 2، ص 23.

2- لمزيد من التفاصيل ينظر بوحنة محمد، المرجع السابق، ص 4، و كذا محمد عرب الموسوي: مفهوم الإرهاب الدولي،http:// www.ahwar.org. الإرهاب الدولي و إشكالية مكافحته،http:// www.djelfa.info و كذا حسن عزيز نور الحلو:الإرهاب في القانون الدولي، دراسة قانونية مقارنة، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، الأكاديمية العربية المفتوحة في الدانمارك، هلسنكي- فنلندا،2007،.http:// scrib.com

) قانون العقوبات الخاص بالدولة التي حدث فيها الإعتداء الإرهابي[1]. وينقسم هذا النوع بدوره إلى إرهاب الدولة أو الحكم وهو الذي تمارسه السلطة الحاكمة على المواطنين و هناك الإرهاب الذي يقوم به فرد أو جماعة ضد السلطة القائمة في الدولة[2].

3/ الإرهاب الفردي: هو الذي يقوم بوضع خطته و تنفيذها شخص واحد. و يطلق عليه كذلك الإرهاب غير السلطوي، لكونه يوجد ضد الدولة من طرف بعض العناصر المناوئة لها من أجل زعزعة النظام السياسي القائم و إحداث تغيير كامل و شامل في التركيبة السياسية و الإجتماعية طبقا لمنظور إيديولوجي معين.[3]

4/ الإرهاب الجماعي: فهو عكس الأول إذ يقوم بوضع خطته عدة أشخاص. ولكن لا يهم ما إذا كان تنفيذها بمعرفة جميع الأشخاص أو بعضهم أو حتى بمعرفة واحد منهم.[4]

و تجدر الإشارة إلى انه و بالرغم من اختلاف أنواع الإرهاب إلا أن هناك سمة واحدة تشترك بينهم و هي انه تعبير عن بث الرعب والخوف الذي يقوم به فرد او جماعة سواء كان ذلك لأغراض سياسية أو شخصية أو غيرها.

ثانيا: أغراض الإرهاب و نتائجه:

1/ أغراض الإرهاب:

من استقرائنا للتعريفات السابقة التي قيلت بشأن الإرهاب يمكن تحديد غرض الإرهاب في الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر.

أ- الإخلال بالنظام العام:

يقصد بالنظام العام مجموعة المصالح الجوهرية للمجتمع أو مجموعة الأسس التي يقوم عليها كيان الجماعة سواء كانت سياسية أو اجتماعية أو اقتصادية أو خلقية. ومن الأسس الجوهرية التي تعد في المجتمعات المعاصرة من مقومات النظام العام:

-الأسس التي يقوم عليها نظام الدولة والتي تتحدد على أساسها طريقة ممارستها في المجتمع عن طريق السلطات العامة، و التي تحدد علاقاتها وواجباتها إزاء المواطنين.

-الأسس التي يقوم عليها نظام الأسرة كالمجتمعات التي تعترف بتعدد الزوجات و تبيح الطلاق و أخرى يكون المبدأ فيها هو وحدة الزواج و تحريم الطلاق.

---

[1] – لمزيد من التفاصيل ينظر عبد القادر زهير النقوزي:المفهوم القانوني لجرائم الإرهاب الداخلي و الدولي، الطبعة الأولى، منشورات الحلبي الحقوقية، 2008، ص30.

[2]– لمزيد من التفاصيل ينظر عصام مفلح: مفهوم الإرهاب و الموقف الدولي، إرهاب الدولة و إرهاب المنظمات، ص5، http:// www.reefnet.gov.sy

[3]– ينظر الإرهاب الدولي و إشكالية مكافحته، المنشور على الموقع السابق. و كذا أشكال الإرهاب http:// saeed.com،

[4]–د/جميل حزام يحيى الفقية: مفهوم الإرهاب في القانون الدولي العام، ص20 و ما بعدها، http:// ycsr.org

-الأسس التي يقوم عليها النظام الاقتصادي.

-الأسس الخلقية التي يقرها المجتمع في زمن معين للحفاظ على القيم التي يؤمن بها، وهي تختلف من شعب لآخر وتتأثر بعوامل مختلفة أهمها الدين والتقاليد والفلسفة السائدة في المجتمع [1].

وفكرة النظام العام هي فكرة مجردة و نسبية تختلف من مكان لآخر ومن زمان لآخر.

والإخلال بنظام العام لدولة ما يكون مثلا عن طريق تعريض امن الدولة و مؤسساتها للخطر، أو الإعتداء على احد رموز الأمن أو الدولة، أو تعطيل تطبيق الدستور كاستخدام القوة لمنع الرئيس من ممارسة سلطاته الدستورية.

وتجدر الإشارة إلى أن الإخلال بالنظام العام والآداب العامة لا يشترط فيه أن يكون هذا الأخير خطيرا أو على درجة كبيرة من الجسامة[2].

ب-تعريض سلامة المجتمع وأمنه للخطر:

ويقصد بذلك تعطيل مظاهر الحياة العادية في الدولة كما تحددها القوانين و اللوائح والأنظمة،وكذا زعزعة السكينة لدى الأفراد في المجتمع ومن أمثلها: التهديد بإحراق أماكن العبادة غير الإسلامية أو عرقلة إقامة الشعائر في المناسبات الدينية أو تعطيل ممارسة الناس حقهم في السياحة أو الاشتغال بالفن.....

وتجدر الإشارة في هذه النقطة انه يكفي تعريض سلامة المجتمع وأمنه للخطر دون ضرورة تحقق التعريض الفعلي لهذا الخطر وذلك لكون أن الجريمة الإرهابية وكما سبق ذكره من جرائم الخطر لا من جرائم الضرر[3].

2/نتائج الإرهاب:

الجريمة الإرهابية هي نمط حديث من العنف الأعمى الذي لا يفرق بين الضحايا و الأهداف المادية، وأيا كان نوعها أو دوافعها فهي تؤدي إلى النتائج التالية:

أ- إيذاء الأشخاص:

و يقصد بالإيذاء هنا هو كل فعل يمس سلامة المجني عليه وصحته أيا كانت جنسيته (سواء السلامة الجسدية أو السلامة النفسية). و مثال ذلك:إطلاق النار على سائح أجنبي من قبل إرهابي و القيام بعملية انتحارية أمام ثكنة عسكرية، أو مدرسة عسكرية، كما حدث في آخر الأحداث في الجزائر والذي كانت عبارة عن عملية انتحارية أمام مدرسة عسكرية "شرشال" التي أوردت ب18 قتيلا.[4]

---

[1]- د/ حبيب ابراهيم الخليلي: المدخل للعلوم القانونية، النظرية العامة للقانون، الطبعة الثامنة، ديوان المطبوعات الجامعية، الجزائر، 2006، ص 110.

[2]- د/ حسنين المحمدي بوادي، المرجع السابق، ص 23

[3]- د/ حسنين المحمدي بوادي، نفس المرجع ، الموضع السابق.

[4]- نشرة أخبار الثامنة، القناة الجزائرية.

ب-إلقاء الرعب بين الأشخاص أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر:

يقصد بذلك إحداث الفزع والخوف والذعر في نفوسهم من جراء استخدام القوة أو العنف أو التهديد أو الترويع، وكذلك يقصد بذلك تعريض حريات الأشخاص للخطر، ومثال ذلك منع دخول السائحين الأجانب إلى منطقة معينة أو كإكراههم على ارتداء زي معين[1] أو كإكراه الفتيات على ارتداء الحجاب ومنعهم من الخروج من المنازل و الذهاب إلى المدارس و الجامعات و العمل[2].

ومن جهة أخرى يقصد به تعريض الأشخاص للخطر، كأن تقوم جماعة إرهابية بتسميم الماء الصالح للشرب أو بتفجير أنبوب الغاز أو بوضع متفجرات في وسائل المواصلات العامة[3].

ج- الإضرار بالاتصالات أو المواصلات أو الملكيات العمومية أو الخاصة:

ويقصد بالاتصالات هنا وسائل الاتصال السلكية واللاسلكية مثل التليفونات وأجهزة الراديو والتلفزيون والأقمار الصناعية و شبكة المعلومات "الانترنت".

أما المواصلات التي يقصد الإضرار بها، فهي وسائل النقل والمواصلات العامة كالحافلات والقطارات والسقف و الطائرات.والإعتداء يكون عليها سواء بالكسر أو الحرق أو التخريب أو القيام بتفكيكها في قطع وسرقتها و الاستحواذ عليها ووضع المتفجرات في السكك الحديدية أو الجسور. كما قد يقع الإضرار بالملكيات العامة[4] والخاصة[5] سواء كانت منقولات أو عقارات أو معدات أو آلات.ويتم الإعتداء عليها بالاستحواذ عليها والسيطرة عليها عنوة أو بشغلها أو احتلالها بدون وجه حق أو ترخيص من السلطة المختصة أو صاحب الحق عليها[6].

د- الاضرار بحركة التنقل والمرور:

و يكون ذلك بوضع الحواجز و المتاريس في الطرق العمومية لإعاقة و منع حركة السير و المرور أو تفجير الجسور أو الرادارات.ويعد التجمهر والاعتصام في الساحات العمومية من قبل هذه الإعتداءات التي قد تلحق في الغالب ضرر بالمجتمع[7].

---

[1]- د/ ابراهيم عيد نايل، المرجع السابق، ص 24.

[2]- د/ حسنين المحمدي بوادي، المرجع السابق، ص 25.

[3]- د/ حسنين المحمدي بوادي، المرجع السابق، الموضع السابق.

[4]- الأملاك العامة: هي تلك الأملاك المملوكة للدولة أو الأشخاص الإدارية. وتكون مخصصة للنفع العام. ينظر د/ ماجد راغب الحلو :القانون الاداري، دار الجامعة الجديدة، 2004، ص90 و مابعدها.

[5]- الأملاك الخاصة: هي تلك الأملاك المملوكة ملكية خاصة للدولة أو الأشخاص الإدارية بغرض استغلالها والحصول على ما ينتج عنها من موارد مالية. ينظر د/ ماجد راغب الحلو، نفس المرجع،نفس الموضع.

[6]- د/ حسنين المحمدي بوادي، المرجع السابق، ص 26-27.

[7]- د/ ابراهيم عيد نايل، المرجع السابق، الموضع السابق.

هـ- إلحاق الضرر بالبيئة:

ويقصد بالبيئة المحيط المادي الذي يعيش فيه الإنسان، بما يشمل من ماء وهواء وفضاء و تربة وكائنات حية و منشآت أقامها لإشباع حاجاته. أو يقصد بالبيئة كل من:

أ- البيئة الطبيعية: وقوامها الماء و الهواء و الفضاء و التربة وما عليها أو بها من كائنات حية.

ب- البيئة الوضعية: بما وضعه الإنسان في البيئة الطبيعية من مرافق ومنشآت لإشباع حاجاته. [1]

و يتم الإضرار بالبيئة بإدخال مواد سامة أو خطرة فيها من شأنها إحداث ضرر وخطر كبيرين على صحة الإنسان أو الحيوان أو النبات على حد سواء[2].

و- منع أو عرقلة عمل السلطات العمومية أو حرية ممارسة الشعائر الدينية و الحريات العامة:

يقصد بالسلطات العمومية السلطات الثلاثة في الدولة – حسب الدستور- السلطة التشريعية والسلطة التنفيذية والسلطة القضائية.ويقصد بالعرقلة الحيلولة أو المنع بين إحدى السلطات في ممارستها لأعمالها في الوقت والمكان المحددين لذلك. فيعد من قبل العرقلة تفجير محكمة مما يقف ذلك دون عقدها لجلساتها للنظر في القضايا المطروحة أمامها. وكذا يعد من قبل العرقلة الإعتداء على أحد أعضاء السلطة (احد النواب).

كما يعد من قبيل العرقلة الحيلولة دون ممارسة حرية الشعائر الدينية سواء في المساجد أو الكنائس أو المعابد وأداء الواجبات الدينية في هذه الأمكنة أو التردد إليها[3].

ضف إلى ذلك فان عرقلة تسيير المؤسسات المساعدة للمرفق العام تصنف ضمن هذا العنوان ويقصد بها تلك المؤسسات التي تهدف إلى تقديم خدمة أو منفعة عامة مثل البلدية والدائرة والولاية...الخ.وتكون العرقلة بالقيام بأعمال تقف حائلا بين هذه المرافق ونشاطها العادي والمألوف، مثل إحداث تفجيرات في هذه المؤسسات أو لصق مناشير أو رسائل تهديدية بتفجير هذه المرافق أو وجود قنبلة بداخلها.[4]

كذلك يتحقق الإرهاب في حالة منع أو عرقلة معاهد العلم لأعمالها، سواء أكانت جامعات أو معاهد أو مدارس. وأيا كان نوع هذه المعاهد العلمية أو تبعيتها، فيستوي أن يكون المعهد خاضعا للإشراف الإداري المباشر للدولة أم يكون معهد خاص.وعلى ذلك يتحقق الإرهاب إذا قامت مجموعة من الأشخاص بمنع احد الأساتذة بالقوة من إلقاء محاضرة، أو تقوم بإغلاق مدرسة بحجة عدم جواز اختلاط البنين مع البنات[5].

---

[1]- لمزيد من التفاصيل حول تعريف البيئة ينظر د/ماجد راغب الحلو: قانون حماية البيئة في ضوء الشريعة، دار الجامعة الجديدة، الإسكندرية، 2004، الهامش رقم 5، ص39.

[2]- لمزيد من التفاصيل ينظر القانون رقم 83-03 المؤرخ في 5 فيفري المتعلق بحماية البيئة الصادر بموجب الجريدة الرسمية عدد رقم 6 بتاريخ 1983/2/5.

[3]- د/محمود سعيد: جرائم الإرهاب، أحكامها الموضوعية واجراءت ملاحقتها، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 1995، ص 22 .

[4]- د/محمود سعيد، المرجع السابق، ص 23.

[5]- د/ حسنين المحمدي بوادي، المرجع السابق، ص 27-28.

ي- عرقلة سير المؤسسات العمومية أو الإعتداء على أعوانها أو عرقلة تطبيق القوانين والتنظيمات:

ويقصد بالمؤسسات العمومية كافة المؤسسات سواء كانت اقتصادية أو تجارية أو إدارية، بحيث تهدف العرقلة هنا والحيلولة دون سيرها العادي وممارستها لنشاطها المألوف التجاري أو الإداري، سواء كانت بالتفجير أو التهديد بالتفجير أو باحتلالها أو التخريب لبعض أملاكها الضرورية لنشاطها، كحرق وسائل النقل المخصصة لها أو الإعتداء على أعوانها سواء على حياتهم كالقتل أو الضرب والاحتجاز أو حتى على ممتلكاتهم كحرق وتخريب منازلهم أو وسائل نقلهم[1].

بينما عرقلة تطبيق القوانين والتنظيمات فيقصد به تعطيل تطبيقها أو المنع من الخضوع لها، كاستخدام القوة لمنع رئيس الجمهورية من ممارسة سلطاته الدستورية أو لمنع إجراء انتخابات أعضاء السلطة التشريعية في الموعد المحدد في القانون أو منع التحقيق مع احد الموظفين العموميين الذي ارتكب جريمة تأديبية تستوجب العقاب[2].

المطلب الثاني:

الفرق بين الإرهاب و بين ما يشابهه من جرائم.

تتشابه الجريمة الإرهابية مع مجموعة من الجرائم(الجريمة السياسية، العنف السياسي، الجريمة المنظمة، جريمة احتجاز الرهائن)، في كونها ذات طابع دولي و يستخدم فيها العنف و القوة و التهديد، كما أنها تستهدف الاخلال بالنظام العام و المساس بالصالح العام. غير أنها في المقابل تختلف عنها في نقاط جوهرية. و سيتم تناول كل جريمة من الجرائم المشابهة للجريمة الإرهابية في الفرعين التاليين كمايلي:

الفرع الأول: الإرهاب و الجريمة السياسية و العنف السياسي.

الفرع الثاني: الإرهاب و الجريمة المنظمة و جريمة احتجاز الرهائن.

الفرع الأول: الإرهاب و الجريمة السياسية و العنف السياسي.

و في هذه النقطة نتطرق بداية إلى الفرق بين الإرهاب و الجريمة السياسية ثم نعرج إلى تبيان الفرق الموجود بين الإرهاب و بين العنف السياسي. و هذا كمايلي:

أولا: الإرهاب و الجريمة السياسية:

ويقصد بالجريمة السياسية "délit politique ": تلك الجرائم التي تنطوي على النظام السياسي للدولة سواء من جهة الخارج، أي المساس باستقلال الدولة و سيادتها، أو من جهة الداخل، أي المساس بشكل

---

[1]- مسلم خديجة: الجريمة الإرهابية، رسالة ماجستير في القانون الجنائي و العلوم الجنائية، معهد الحقوق بن عكنون، الجزائر، 1996-1997،ص 18.

[2]- د/ حسنين المحمدي بوادي، المرجع السابق، ص 28.

لاحكومة أو نظام السلطات فيها أو الإعتداء على حقوق الأفراد السياسية[1].أو هي الجريمة التي ترتكب بباعث سياسي أو تقع على الحقوق السياسية العامة أو الفردية[2]. ومن أمثلتها إصدار المنشورات والبيانات النافذة ؛ولكن وبرغم من اشتراك الجريمة الإرهابية مع الجريمة السياسية في أنهما يهدفان إلى المساس بالنظام العام والسكينة العامة، أي أنهما تصنفان ضمن الجرائم البالغة الخطورة التي تمس سلامة الدول سواء من الداخل أو الخارج.الا أن الجريمة السياسية لا تتوفر أحيانا على عنصر العنف والرعب والمفاجأة التي تتميز بها الجريمة الإرهابية. وعلى هذا فقد استبعد الإرهاب من نطاق الجرائم السياسية منذ المؤتمر الدولي لتوحيد قانون العقوبات العام 1935.[3]

ثانيا: الإرهاب و العنف السياسي:

العنف السياسي هو ذلك العنف الذي يبعث الخوف والرعب في نفوس الناس ويخل بالأمن والنظام لدرجة التأثير على الطمأنينة العامة وزعزعة الثقة في نظام الدولة؛ و من أمثلته: اغتيال المسئولين الحكوميين ومحاولة الاستيلاء على السلطة عن طريق الانقلابات العسكرية.ويشترك هذا الأخير مع الإرهاب في نقطة أنهما يبعثان الخوف والرعب في نفوس الكافة، ويلحقان أضرار جسمانية أو تخريب الممتلكات. ويختلفان في كون أن العنف السياسي يصبح عملا مقبولا في حالة نجاحه وتحقق أهدافه السياسية[4]، على عكس الإرهاب الذي هو دائما وسيظل عملا تنبذه كل الأمم والشعوب.

الفرع الثاني: الإرهاب و الجريمة المنظمة و جريمة احتجاز الرهائن.

و نتطرق في هذه النقطة إلى تبيان الفرق بين الإرهاب و الجريمة المنظمة بداية ثم بين الإرهاب و جريمة احتجاز الرهائن. و هذا كمايلي:

أولا: الإرهاب و الجريمة المنظمة:

تعتبر الجريمة المنظمة شكل من الأشكال الحديثة للإجرام المنظم المتطور؛ فهي مشروع إجرامي يحوي أنشطة إجرامية متعددة يقوم عليها أناس محترفون في الإجرام يعملون داخل تنظيمات أو جماعات، ويخضعون لقواعد صارمة و دقيقة.

ومن جهة أخرى فإن الجريمة الإرهابية تعتبر نوعا من أنواع الجريمة المنظمة، ولكنه وبالرغم من ذلك وفي المقابل ليست كل جريمة منظمة حدثا إرهابيا[5]، وذلك لان هناك بعض من جرائم الإرهاب التي لا يتوفر فيها عنصر الهدف الاقتصادي الذي يعد من أحد وأهم خصائص الجريمة المنظمة.

---

[1]– د/ علي حسين الخلف، سلطان عبد القادر الشادي: المبادىء العامة في قانون العقوبات العراقي، وزارة التعليم العالي والبحث العلمي، العراق، 1982، ص 297

[2]– ينظر المادة 21 من قانون العقوبات العراقي

[3]– لمزيد من التفاصيل ينظر د /محمد الامين البشري، المرجع السابق، ص 146

[4] – د/محمد الأمين البشرى، المرجع السابق، الموضع السابق.

[5]– د/ محمد الأمين البشرى، نفس المرجع ، ص 146.

هذا من جهة ومن جهة أخرى، فان الجماعات أو المنظمات الإرهابية كثيرا ما تميل إلى استخدام وسائل الإعلام في الإعلان عن أهدافها،على عكس الجريمة المنظمة التي تسهر أن تحقق أهدافها الاقتصادية في سرية تامة لكي تتمكن بالهروب بعائدات الجريمة من مكان الحدث[1].

ومن جهة ثالثة، فان الجاني في جريمة الإرهاب لا يعبأ بالحياة في سبيل تنفيذ المهام الموكلة إليه، بينما يسعى مرتكب الجريمة المنظمة إلى البقاء حيا للاستمتاع بعائدات جريمته.

ولكن وفي المقابل، تجدر الإشارة إلى أن الجماعات الإرهابية قد تعتمد على الأموال المستمدة والناتجة عن الجريمة المنظمة لدعم عملياتها الإرهابية خاصة التي تحتاج إلى مبالغ مالية كشراء السلاح...[2]

ثانيا: الإرهاب و جريمة احتجاز الرهائن:

تعرف جريمة أخذ الرهائن واحتجازهم بأنها: "اختطاف الأشخاص واحتجازهم و التهديد بقتلهم أو إيذائهم أو استمرار احتجازهم من أجل إكراه طرف ثالث سواء كان هذا الطرف دولة أو منظمة دولية أو حكومية أو شخصا طبيعيا أو اعتباريا أو مجموعة من الأشخاص على القيام أو الامتناع عن القيام بفعل معين كشرط صريح أو ضمني للإفراج عن الرهينة"[3]. ولهذا فهناك من يعتبرهما وجهان لعملة واحدة، لاشتراكهما في الهدف؛ إذ يسعى كلاهما إلى إفشاء الرعب والخوف. كما أنهما يتفقان في أسلوب العمل والتنظيم.وقد يكون أعضاء المنظمات الإرهابية هم أساسا من محترفي الجرائم المنظمة حيث يسعون للاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ، فهناك صلة وتعاون وثيق بينهما[4].

و تعد جريمة اختطاف واحتجاز الرهائن من أخطر الجرائم الإرهابية التي تعاقب عليها كل التشريعات الوطنية،وهي إحدى الجرائم المنصوص عليها في اغلب الاتفاقيات الدولية المتعلقة بمكافحة الإرهاب.[5]

ولكن تجدر الإشارة إلى أن احتجاز الرهائن لا يكون دائما لتحقيق أهداف إرهابية، إذ يتم دون استعمال العنف وعن طريق الغش والاحتيال ويكون ذلك بقصد الحصول على الأموال أو إجبار الأفراد و المؤسسات الخاصة على اتخاذ قرار معين[6].

---

[1]– محمد محمد علي ابراهيم: الجوانب الاقتصادية لغسيل عوائد الجريمة المنظمة، ورقة مقدمة إلى أعمال ندوة الجريمة المنظمة و أساليب مواجهتها في الوطن العربي، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2003، ص91 و ما بعدها.

[2]– ينظر د/محمد ابراهيم زيد: الجريمة المنظمة، تعريفها،أنماطها و جوانبها التشريعية، ورقة مقدمة إلى أبحاث حلقة علمية حول الجريمة المنظمة و أساليب مكافحتها المنعقدة ما بين 14–18 نوفمبر 1998 بأبوظبي، أكاديمية نايف العربية للعلوم الأمنية، الرياض،1998، ص 37.

[3] – التعريف الذي جاء في الاتفاقية الدولية لمناهضة أخذ الرهائن والذي أقرتها الجمعية العامة للأمم المتحدة في 1979/12/17.

[4]– محمد عبد الله المنشاوي، البحث السابق،http:// www.minshawi.com

[5]– د/محمد الأمين البشرى، المرجع السابق، ص 147.

[6]– د/محمد الأمين البشرى، نفس المرجع ، ص 148.

هذا من جهة ومن جهة أخرى، فان أمر معالجة العملية الإرهابية يتوقف على قرار الدولة والقيادة السياسية، بينما تعتمد معالجة عملية احتجاز الرهائن – أحيانا – على قرار الأسرة أو المؤسسة المالية التي ينتمي إليها الفرد[1].

المطلب الثالث:

الأسباب و العوامل المساعدة على انتشار الإرهاب:

جريمة الإرهاب كغيرها من الجرائم التقليدية تساعد على قيامها عوامل مختلفة، تتفاعل فيما بينها لدفع المجرم إلى ارتكاب جرمه الشنيع.و هذه العوامل تكون سياسية أو اقتصادية أو اجتماعية أو نفسية أو دينية أو عرقية. وعلى هذا فهي تقسم إلى قسمين: القسم الأول ويضم أسبابا غير مباشرة، وتتمثل في الأسباب الاجتماعية والاقتصادية و النفسية.و القسم الثاني يضم أسباب مباشرة، وتتمثل في الأسباب السياسية والدينية.

وتقترن هذه الأسباب (المباشرة و غير المباشرة) بعوامل أخرى مشتركة تلعب دورا بارزا في نتائج تلك العوامل و الأسباب و هي: الجهل، التعلم من الرفاق، الإحساس بالظلم، إهمال المجتمع و الدولة لبعض الفئات التي تختلف معها في الرأي، طريقة تعامل السلطة الرسمية للمواطنين، الأجهزة الأمنية (استغلالها واستفزازها للإرهابيين)، وسائل الإعلام[2]. وسيتم التفصيل في هذه الأسباب في الفرعين التاليين:

الفرع الأول: الأسباب المباشرة.

الفرع الثاني: الأسباب غير المباشرة.

الفرع الأول:الأسباب المباشرة:

الأسباب المباشرة المساعدة على انتشار جرائم الإرهاب هي مجموع العوامل و الدوافع المساعدة بصورة مباشرة في انتشار هذه الجرائم. و تتميز هذه العوامل بأنها الأكثر حساسية و تأثيرا في هذه الجرائم، وتتمثل هذه الأخيرة في الأسباب السياسية و الاسباب الدينية. و التي سنتناولها كمايلي:

أولا: الأسباب السياسية

وهي تعود إلى الاستعمار القديم و التنافس المتواصل والنزاع الدائم بين الدول الصناعية الكبرى ذات المصالح الاقتصادية غير المحدودة.وهي تعتبر الأكثر عنفا وقوة وتطرفا متى ما قورنت بالوطنية و الثورية. وتعد العمليات الانتحارية التي قام بها الجنود اليابانيون ابان الحرب العالمية الثانية خير مثال على الروح الوطنية. [3]

ضف إلى ذلك العمليات الانتحارية التي يقوم بها الفلسطينيون لتحرير بلادهم من الاستعمار الإسرائيلي.

---

[1]– د/محمد الأمين البشرى، نفس المرجع، ص 147.

[2] – د/ محمد الامين البشرى، نفس المرجع ، ص149.

[3]– لمزيد من التفاصيل ينظر د/محمد الامين البشري،المرجع السابق، ص 150

ثانيا: الأسباب الدينية

تخاطب الأديان مهما كان نوعها في الإنسان الروح والعقل، وهي بذلك الأكثر نفاذا و تأثيرا في الانسان. ويجد استغلال الأديان نجاحا في المناخات الاقتصادية المتردية والظروف السياسية المضطربة و الظروف الاجتماعية غير المتوازنة. و تتضاعف آثار الدين على العمل الإرهابي في المجتمعات التي ينتشر فيها الجهل و الفقر و الظلم و مخالفة أوامر الدين و نواهيه[1].

الفرع الثاني:الأسباب غير المباشرة.

وتتمثل في:

أولا: الأسباب الاقتصادية

إذا كان الاقتصاد الضعيف للدولة يهيء التربة الخصبة والمسرح الحيوي للإرهاب لإثارة الكراهية ضد الدولة وتشجيع الطبقات الدنيا على الثورة ضد نظام الدولة،بخروجها وقيامها بأعمال شغب وعنف وإرهاب ضد النظام العام،ومن اجل ذلك أيضا تسعى المنظمات الإرهابية إلى ضرب الاقتصاد القومي وتعطيل المرافق الإنتاجية أو الاستثمارية حتى تتمكن من التأثير على الدولة والدعوة لأهدافها السياسية[2].

هذا من جهة ومن جهة أخرى، فان العامل الاقتصادي يلعب دورا في تدعيم العمليات الإرهابية و تمويلها، و خاصة تلك التي تحتاج إلى المال لشراء الأسلحة[3].

ثانيا: الأسباب الاجتماعية

تؤدي العوامل الاجتماعية كالتخلف والتدهور الصحي وتدهور خدمات الدولة في بعض المناطق و التمييز الاجتماعي بين فئات المجتمع الواحد و انتشار البطالة إلى فتح باب نشر الفكر الإرهابي، و ذلك عن طريق الانخراط في الصفوف الإرهابية و مساندتهم أدبيا و ماديا في العمليات التي يقومون بها[4].

ثالثا: العوامل النفسية و العقلية

تشكل العوامل النفسية و العقلية حجر الزاوية في عملية صناعة الإرهابي؛ فالإرهابي عادة ليس مريضا عقليا و يعاني من حالة نفسية غير عادية، خاصة و هو قادر على استيعاب الخطط الإرهابية و متماسك في مرحلة التنفيذ وقوي بعد العملية.و هو يواجه إجراءات التحقيق و المحاكمة بثبات و يصمد إلى ما بعد المحاكمة، ويعود أحيانا إلى ممارسة نشاطه أكثر من مرة. إلا أن الثابت أن الأسباب النفسية و العقلية تلعب دورا في الحدث الإرهابي و تصبح محور التحقيق والشكوك في كل حدث إرهابي ويعزى ذلك إلى:

1- تستخدم الجوانب النفسية والعقلية بخبرة ودراية علمية في صناعة الإرهابي و استقلاله.

2- تساعد العوامل النفسية و العقلية في السيطرة على الإرهابي و توجيهه وفق مخطط معلوم.

---

[1]- ينظر د/محمد الأمين البشرى، المرجع السابق ، ص 151.

[2]- ينظر د/محمد الأمين البشرى، نفس المرجع ، ص 150.

[3]- ينظر د/ أسماء بنت عبد العزيز الحسين: أسباب الإرهاب و العنف و التطرف، دراسة تحليلية، 2002،ص 10.

[4]-ينظر د/ أسماء بنت عبد العزيز الحسين، نفس المرجع،ص 18. د/ مصطفى محمد موسى: التكدس السكاني العشوائي و الإرهاب، الطبعة الاولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص 88.

3- تستخدم العوامل النفسية والعقلية لاستيعاب الشبهة أو علاقة الإرهابي بأطراف المنظمة الأخرى و يؤكد ذلك درجة جنونية الأحداث الإرهابية التي توجب فور تناقل أخبارها بأنها أعمال لا يأتي بها إلا مجنون أو معتوه.

4- توجد حالات نفسية وعقلية حقيقية تساهم أحيانا في الأعمال الإرهابية بطريقة أو أخرى يصعب التأكد منها،خاصة في العمليات الانتحارية.[1]

المبحث الثاني:

ماهية الإرهاب عبر الانترنت

في الماضي كان الإرهاب يعني قيام بعض الإرهابيين بتفجير قنبلة في مكان ما أو اغتيال شخصية ما أو تفجير طائرة في الجو وما إلى ذلك من عمليات روتينية اعتاد رجال الأمن في جميع الدول على مواجهتها. وكانت تلك العمليات تتم بغرض نشر الإرهاب في الدولة التي ينتمي إليها الإرهابيين أو حق في دولة لا ينتمون إليها لتحقيق أغراضهم، والتي كان معظمها يتمثل في معارضة النظام الحاكم وما يمثله من رموز أو تحجيم الحركة السياحية أو اغتيال رموز فكرية تتناقض أفكارها مع فكر الإرهابيين، الذين يقومون بتنفيذ تلك العمليات وما إلى ذلك من أهداف.أما الآن ومع التقدم التقني وكذا تقدم وسائل الاتصالات الذي نعيشه ونكاد نلمسه، فقد تغيرت و تطورت تلك الأساليب التي يحاول الإرهابيون بها الوصول إلى أهدافهم وأصبح الإرهاب الإلكتروني هو السائد حاليا، وأصبح اقتحام المواقع وتدميرها و تغيير محتوياتها و الدخول على شبكات الاتصال بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائيا هو أسلوب الإرهاب حاليا في محاولة الوصول إلى أغراضهم.ففي جلسة خاصة عقدها الكونجرس الأمريكي لمناقشة العلاقة بين الانترنت و بين الحادث الإرهابي- في أوكلاهوما- استنسخ عضو الكونجرس "ادوارد كيندي" نسخة من كتاب من الانترنت يتضمن إرشادات للإرهابيين، وحث أعضاء الكونجرس على ضرورة وضع ضوابط حول الاستخدام السيئ للشبكة خاصة فيما يتعلق بالإرهاب والإباحية. كذلك فقد حذر خبراء الحاسب الآلي من أن المعلومات الأساسية لتصنيع القنابل الذرية يمكن الحصول عليها بسهولة من خلال شبكة الانترنت.[2]

والإشكال المطروح هنا: هو ماذا نعني بالإرهاب عبر الإنترنت وما هي خصائصه؟ وما الفرق بينه وبين نظيره التقليدي وما هي أشكاله؟ أو كيف يتم استخدام الانترنت في نقل العنف والتهديد والترويج التي يبنى عليها الإرهاب من العالم الإفتراضي إلى العالم المادي؟ وسيتم الإجابة على هذا الإشكال وفقا للمطالب التالية:

المطلب الأول: تعريف الإرهاب عبر الانترنت و خصائصه.

المطلب الثاني: الفرق بين الإرهاب عبر الانترنت و بين الإرهاب التقليدي و العوامل المساعدة في انتشاره.

---

[1]- ينظر د/ أسماء بنت عبد العزيز الحسين، المرجع السابق،ص 19.

[2]- د/عبد الفتاح بيومي حجازي،(الأحداث والإنترنت) مرجع سابق، ص185.

المطلب الثالث: أشكال الإرهاب عبر الانترنت وموقف التشريعات المقارنة من هذه الجريمة.

المطلب الأول:

تعريف الإرهاب عبر الانترنت و خصائصه.

نتناول تحت هذا المطلب تعريف هذا النوع الجديد و الخطير من الإرهاب و الذي ساهمت في انتشاره شبكة الانترنت، لنتطرق بعد ذلك لتبيان الخصائص التي يتميز بها هذا الاجرام المستحدث. و ذلك في الفرعين التاليين:

الفرع الأول: تعريف الإرهاب عبر الانترنت.

الفرع الثاني: خصائص الإرهاب عبر الانترنت.

الفرع الأول: تعريف الإرهاب عبر الانترنت.

أدى ظهور الحاسبات الآلية وانتشار استخدام الانترنت إلى تغيير شكل الحياة في العالم، إذ أصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوما بعد يوم في إدارة معظم الأنشطة الحياتية بما فيها مشروعات البنى التحتية الأساسية و الحساسة للدول.الأمر الذي وفر المجال الخصب والملائم للإرهابيين الإلكترونيين ومكنهم من ارتكاب جرائمهم وتحقيق أهدافهم بكل ارتياح وطمأنينة ضد نظم السيطرة والتحكم التي تؤثر في توزيع الكهرباء والمياه والاتصالات وشبكات البنوك والتجارة وغيرها. إذ يقوم الإرهابي بارتكاب عمله الإرهابي وهو جالس في منزله ووراء مكتبه أو في مقهى يحتسي فيها قهوته أو مشروبه المفضل أو من غرفته في احد الفنادق و ذلك بمجرد الضغط على زر واحد في لوحة مفاتيح الحاسب الآلي المتصل بشبكة الشبكات.

ولقد اختلفت وتباينت تعريفات الإرهاب عبر الانترنت أو كما يسمى الإرهاب الالكتروني أو الإرهاب الرقمي " electronic or digital terrorism " كالتالي:

فهناك من يعرفه بأنه:" هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا، توجه من اجل الانتقام أو الابتزاز أو الإجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة"[1].

و هناك من يعرفه بأنه: " تعبير يشمل مزج مصطلح التهديد بنظم المعالجة الآلية للمعلومات باستخدام تقنية الاتصالات الحديثة"[2]. أو بأنه: " العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل

---

[1]– سلطانة بنت فهد بن دغيليب العتيبي: الإرهاب الالكتروني، التهديد الجديد في نظام الصحة الالكتروني عن بعد، مقال منشور على الإنترنت على الموقع: http:// .www.crime-research.org

[2] – الإرهاب الالكتروني، http:// www.knal-google.com

الإلكترونية، الصادر من الدول أو الجماعات أو الأفراد على الانسان في دينه أو نفسه أو عرضه أو عقله أو ماله، بغير حق بشتى صنوفه و صور الإفساد في الأرض"[1]. أو أنه: "عبارة عن منتديات مجهولة تقوم بنشر دورات تعليمية عن تصنيع المتفجرات والسموم"[2]. أو بأنه: " تعبير يشمل مزج مصطلح التهديد بنظم المعالجة الآلية للمعلومات لاستخدام تقنية الاتصالات الحديثة / الانترنت."[3] أو بأنه:" استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية ".[4]

أو بأنه:" جريمة العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية سواء كان صادرا من الدول أو الجماعات أو الأفراد على الإنسان بشكل عام. و على سبيل المثال الأعمال غير المشروعة التي يكون فيها الكمبيوتر إما وسيلة أو هدفا أو كليهما و يمكن إعطاء أمثلة عامة تشمل نطاق الإلكتروني و منها:

-الأنشطة التخريبية، أو التهديد بها، في عالم الإنترنت، مع نية تحقيق المزيد من الأهداف الاجتماعية والدينية و السياسية و نحوها،أو لتخويف أي شخص.

-وضع بعض مستخدمي الإنترنت في حالة خوف.

-التأثير الإلكتروني السلبي على الانسجام بين الأديان، الأعراق، الأقاليم، الجماعات أو الطوائف.

-تهديد سيادة ووحدة الدولة."[5]

و لقد تفطن الغرب في قضية الإرهاب الإلكتروني و مخاطره في منتصف العام الماضي، حيث قام الرئيس الأمريكي السابق " بيل كلينتون " في عام 1996 بتشكيل لجنة حماية المنشآت التحتية الحساسة، والذي كان من أول استنتاجاتها: " أن مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة الأمريكية، وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف امن الولايات المتحدة الأمريكية ". و في أعقاب ذلك قامت كافة الوكالات الحكومية في الولايات المتحدة الأمريكية بإنشاء هيئاتها ومراكزها الخاصة للتعامل مع احتمالات الإرهاب الإلكتروني. فقامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية، ووظفت ألفا من خبراء امن المعلومات وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني. وقامت القوات الجوية الأمريكية باتخاذ نفس الخطوات، وكذا الشأن بالنسبة للمباحث

---

[1]- مفهوم الإرهاب الإلكتروني ، http:// www.Mahawar el-islam.com

[2]- الإرهاب و الإنترنت، htttp:// www.aljazeera.com

[3]- د/ عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن استخدام الإنترنت)مرجع سابق، ص 649.

[4] -Business information systèmes، 2ème édition ،2003،p 14.

[5]- د/محمد بن عبد الله آل فايع العسيري، د/حسن بن أحمد الشهري: استعمال الإنترنت في تمويل الإرهاب و تجنيد الإرهابيين، الإرهاب الإلكتروني و بعض وسائله و الطرق الحديثة لمكافحته،جامعة نايف العربية للعلوم الأمنية، الرياض،2012،ص225.

الفدرالية وكذلك الدول الأوروبية، لاسيما تلك التابعة للحلف الأطلسي.[1] وعقب أحداث 11 سبتمبر في الولايات المتحدة الأمريكية تصاعدت التهديدات والمخاوف من حدوث هجمات إرهابية الكترونية،خاصة بعد عمليات ناجحة كبدت المستهدفين خسائر ضخمة و فادحة ؛ الأمر الذي دعا 30 دولة إلى التوقيع على الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الانترنت في بودابست عام 2001.[2]

وتجدر الإشارة إلى انه لاعتبار الشخص إرهابيا عبر الانترنت (إرهابي الكتروني) و ليس فقط مخترق، فانه يجب أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، وعلى الأقل أن تحدث أذى كافي من اجل نشر الخوف و الرعب.[3]

الفرع الثاني:خصائص الإرهاب عبر الإنترنت:

تتميز جريمة الإرهاب عبر الانترنت أو الإرهاب الإلكتروني بمجموعة من الخصائص، يمكن حصرها في النقاط التالية:

أولا: استخدام التقنية الرقمية العالمية لارتكاب هذه الجريمة

إذ يلجأ الإرهابيون إلى استخدام التقنية الرقمية من حاسب آلي و انترنت بهدف إخافة و ترويج و ترهيب الآخرين – سواء أكانوا أشخاصا طبيعة كالأفراد أو أشخاصا معنويا كالدولة – أو لمهاجمة نظم المعلومات كبث الفيروسات أو تدمير المواقع...

حيث وجدت بعض المنظمات الإرهابية ضالتهم المنشودة في ابتكار آلاف المواقع[4] لنشر أفكارهم ومعتقداتهم والتخطيط والتجهيز لعمليات إرهابية وتنسيق وتبادل الخبرات الميدانية العملية فيما بينهم. حيث كشفت مواقع لتعليم صناعة المتفجرات والألغام والأسلحة الكيماوية الفتاكة وطرق تسميم مياه المدينة أو تفجير سوق أو مبنى.وأخرى توضح آلية اختراق و تدمير المواقع و البيانات والنظم المعلوماتية واختراق البريد الإلكتروني؛ وكيفية الدخول على المواقع المحجوبة وبث الفيروسات.ومن هذه المواقع: موقع مشاور وموقع جنة القناص (http://www.snuperspanelise.com) وموقع سرايا الجبل[5]. ناهيك عن مواقع مخصصة لشن حملات نفسية على الدول و المجتمعات التي تقوم بترويجها حيث تعرض الرهائن والأسرى وكيفية إعدامهم[6]. و لهذا

---

[1]– الحماية من الإرهاب الالكتروني ، http:// www.mpc.gov

[2]– د/ سليمان أحمد فضل، المرجع السابق، ص 124.

[3]– د/ سليمان أحمد فضل، نفس المرجع ، ص3 12

[4] – إذ انه ووفقا لبعض التقديرات فانه في عام 1995 كان هناك ما لا يقل عن 100 موقع من المواقع التي تدعم الإرهاب بينما في يومنا هذا يزيد عدد هذه المواقع عن 5000 موقع، ينظر كلا من " الإنترنت والإرهاب " المنشور على الموقع التالي http:// :www.arwikipédia.org

و "إرهاب الإنترنت الخطر الوافد.....، http:// www.maltaqui.com

[5]– عبد الحفيظ سعد، أحمد عبد المقصود: الإرهاب الإليكتروني ووصفات مجانية لتصنيع قنبلة هيدروجينية، جريدة صوت الأمة، العدد 228،2005/04/11، ص 5.

[6]– مفهوم الإرهاب الإلكتروني، مقال سابق منشور على http:// www.Mahawar el-islam.com.

فان ووفقا لآراء الخبراء و الباحثون فان امن البشرية سيصبح في المستقبل القريب مهددا ليس بالصواريخ وإنما بأجهزة الحواسيب وعن طريق برامج متقدمة تؤدي إلى تدمير البنية الأساسية في بلد من البلدان ومعدات الدفاع وتخريب الاتصالات و قوى الطاقة والأنظمة العسكرية.[1]

ثانيا: خطورة الإرهاب الإلكتروني

تعتبر هذه الخاصية مكملة للخاصية السابقة، إذ أن الاستخدامات السيئة و الضارة لهذه التقنيات الحديثة المعتمد عليها في جميع مجالات الحياة أفرزت فجر إجرام مستحدث وخطير يهدد العالم بأسره يسمى الإرهاب الإلكتروني لا سيما وان المنشآت التحتية الحساسة للدول (وبالأخص الغربية) تعتمد بشكل كبير على المعلومات الرقمية مما يجعلها الهدف الأول لأية هجمات إرهابية. فالإرهاب عبر الانترنت كما يقول المستشار محمد الألفي يمكن أن يتسبب في إلحاق الشلل كأنظمة القيادة و السيطرة و الاتصالات وإلى قطع شبكات الاتصال بين الوحدات و القيادة أو تعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها أو اختراق النظام المصرفي أو إرباك حركات الطيران المدني شل مخططات الطاقة الحرارية أو النووية.[2]

وبهذا أصبح الإرهاب الإلكتروني من اخطر ما يواجه العالم اليوم، أصبح بإمكان الإرهابي من خلال ضغط على احد أزرار الكمبيوتر، اختزال 90 ٪ من العمليات الإرهابية، و كذا الحصول على قنبلة حقيقية وهو جالس في بيته و بأقل التكاليف من خلال المواقع المخصصة لذلك. ويرى د/ سليمان احمد فضل أن من أسباب خطورة الإرهاب الإلكتروني انه يعتمد على البرمجيات كسلاح له، وتلك البرمجيات يسهل الحصول عليها عبر الانترنت من خلال إعداد برمجي لبرمجة إرهابية، كما انه يمكن توزيعها بصورة عشوائية، فيمكن لأحد الهكرة القيام بإعداد برمجية وتحميلها عبر الانترنت عبر مواقع مجهولة ثم يقوم بالدعاية لها أيضا، مما يدفع العديدين للولوج إلى تلك المواقع للتعرف عليها.[3]

المطلب الثاني:

الفرق بينه وبين الإرهاب التقليدي و العوامل المساعدة في انتشاره

سيتم من خلال هذا المطلب تبيان أهم الفروق بين الإرهاب التقليدي والإرهاب عبر الانترنت، وحصر لمختلف العوامل التي من شأنها المساعدة على انتشارهذا النوع من الإرهاب، وذلك من خلال الفرعين التاليين:

الفرع الاول: الفرق بينه و بين الإرهاب التقليدي.

الفرع الثاني: العوامل المساعدة في انتشارالإرهاب الالكتروني.

---

[1]- ينظر د/ عبد الفتاح بيومي حجازي، (الاحداث والإنترنت) مرجع سابق، ص 189.

[2].- الحماية من الإرهاب الالكتروني،http://www.Mahawar el-islam.com

[3]- د/ سليمان أحمد فضل، المرجع السابق، ص 130.

الفرع الأول: الفرق بينه و بين الإرهاب التقليدي.

باستقرائنا لمختلف التعاريف السابقة لكل من الإرهاب التقليدي و كذا الإرهاب عبر الإنترنت يمكننا أن نستخلص أن هناك مجموعة من نقاط التشابه و الاختلاف بين هذين النوعين من الإرهاب، يمكن حصرها في التالي:

أولا: نقاط التشابه بين الإرهاب الالكتروني و الإرهاب التقليدي

ففيما يخص نقاط التشابه فهي تتمثل في أن القاعدة الأساسية التي يستند إليها الإرهاب التقليدي هي ذاتها التي يستند إليها الإرهاب عبر الإنترنت ألا و هي: التهديد وما يثيره من فزع وخوف و ترويع يؤدي إلى عدم الاستقرار النفسي لدى المجني عليه. ضف إلى أن كلاهما الغرض منهما الإخلال بالنظام العام وتعويض سلامة المجتمع وأمنه للخطر.

هذا من جهة ومن جهة أخرى، فان كلاهما يقومان على خلفية دوافع سياسية أو عرقية او دينية.

ثانيا: نقاط الاختلاف بين الإرهاب الالكتروني و الإرهاب التقليدي

و بالرغم من تشابهما في النقاط المذكورة أعلاه إلا أنهما في المقابل يختلفان في مجموع النقاط التالية:

1/ الوسيلة المستخدمة في ارتكاب الجريمتين:

تختلف الوسيلة المستخدمة في ارتكاب جريمة الإرهاب التقليدي عن نظيرتها الواقعة عبر الإنترنت.فأما الأولى فيلجأ الإرهابيون إلى استعمال الوسائل التقليدية العادية في تنفيذ عملياتهم الإرهابية كاستخدام السلاح أو القنابل على عكس الثانية أين تعتمد على التقنية الرقمية العالية من حاسب آلي وانترنت.

2/ المكان الذي ترتكب منه و فيه الجريمتين:

فالإرهاب التقليدي يرتكب من/ في العالم المادي الملموس و المرئي اين تسهل فيه معاينة مسرح الجريمة[1]. مثل وضع الإرهابي لمواد متفجرة في الأماكن المزدوجة أو تفجير نفسه (عملية انتحارية) أو خطف طائرة و المسافر على متنها و طاقمها. أما الإرهاب عبر الإنترنت فيرتكب من/ في العالم الإفتراضي اي عبر الانترنت، أين يصعب فيها اكتشاف مدبرها و منفذها وأين يختفي فيها مسرح الجريمة للمعاينة، فالإرهابي في هذا النوع من الإرهاب يستطيع أن يقوم بعملياته الإرهابية انطلاقا من بيته و هو جالس وراء حاسوبه الخاص ومن خلال الضغط على احد أزرار هذا الأخير.كما انه يحقق الفضاء الإلكتروني ملاذا آمنا لنشر أفكاره العنصرية و المتطرفة.

3/ محل الجريمتين:

يقع الإعتداء و العنف في الإرهاب التقليدي على الأشخاص – سواء أكانوا طبيعيين كالأفراد أو معنويين كالدول – وعلى الممتلكات– سواء كانت خاصة أو عامة – ولكن الشأن يختلف في الإرهاب عبر

---

[1]– لمزيد من التفاصيل حول موضوع اجراءات التحقيق في الحدث الإرهابي، ينظر د/ محمد الأمين البشري، المرجع السابق، ص 154 و ما بعدها.

الإنترنت، فبالإضافة إلى ما سبق ذكره في النوع الأول، فان ذلك الأخير يطال الإعتداء فيه نظم المعلومات وذلك عن طريق تدمير المواقع وتخريبها وكذا اختراق المواقع الرسمية أو الشخصية، اختراق وإغراق البريد الإلكتروني بالرسائل الغير مرغوب فيها، أو بإطلاق الفيروسات. [1]

4/ أهداف الجريمتين:

الإرهاب عبر الإنترنت يهدف إلى ضرب البنى التحتية و الأساسية للدول و التي أصبحت في فجر المعلوماتية تعتمد كليا و بشكل كبير على المعلومات الرقمية: فهو يمكن أن يتسبب في إلحاق الشلل بأنظمة القيادة و السيطرة و الاتصالات أو قطع شبكات الاتصال بين الوحدات و القيادة أو تعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها أو اختراق النظام المصرفي أو إرباك حركة الطيران أو قطع الكهرباء و الغاز و مثل مخططات الطاقة الحرارية أو النووية.على عكس الإرهاب التقليدي الذي يهدف إلى هز أمن الدولة و استقرارها بالقيام بتفجيرات أو احتجاز الرهائن أو تلويث المياه الصالحة للشرب أو قتل احد الأشخاص الرسمية في الدولة.

5/ خطورة الإرهاب عبر الإنترنت مقارنة بذلك التقليدي[2].

الفرع الثاني:العوامل المساعدة في انتشار الإرهاب عبر الإنترنت

في الواقع أن الإرهاب الإلكتروني يتمثل في إمكان النفاذ إلى شبكات التحكم في المرافق العامة، مما يتسبب في الشلل التام للبنى التحتية الأساسية، بل و احتمال تدميرها بالكامل. فالدول أصبحت معرضة لما يمكن أن نطلق عليه: أسلحة الخراب و الفوضى في أرجاء البنية المعلوماتية ولعل أهم عامل مساعد في انتشار

---

[1]– نظم المعلومات هو اصطلاح نشأ منذ السبعينات من القرن الماضي بهدف وصف الحالة التي نشأت باندماج تقنية عملاقة هي تقنية نظم المعلومات، وتقنية الاتصالات عن بعد وهندسة التحكم، وقد أدى هذا التزاوج إلى اختراع تقنيات باهرة ساعدت بشكل كبير على تطوير أنظمة معالجة البيانات بمختلف أشكالها وأنواعها، وأصبحت بالفعل عاملا حاسما في تحديد مصير عالمنا بدوله وأفراده،وأثرت ولا تزال تأثر في شتى مناحي الحياة المعاصرة. بشكل كبير على تطوير أنظمة معالجة البيانات بمختلف أشكالها وأنواعها، وأصبحت بالفعل عاملا حاسما في تحديد مصير عالمنا بدوله وأفراده. وقد عرفها احد المتخصصين في مجال نظم المعلومات بأنها: " اخضاع المعلومات في حصرها وتبويبها وتحليلها إلى مجموعة من نظم التشغيل والمعالجة الحسابية والمنطقية لاستخلاص النتائج ". وفي تعريف اخر بأنها: " مجموعة من الاجراءات التي يتم من خلالها تجميع واسترجاع أو تشغيل وتخزين ونشر المعلومات بغرض دعم عمليات صنع القرار وتحقيق الرقابة داخل الجهة الادارية أوايا كانت شكل تلك المنظمة ". وقد عرف قانون "الاونيسترال" النموذجي بالمادة 6/2 بشأن التجارة الإلكترونية نظم المعلومات بأنها: " النظام الذي يستخدم لانشاء رسائل البيانات،أو ارسالها أو استلامها أو تخزينها أو تجهيزها على اي وجه اخر". لمزيد من التعريفات ينظر د/ايمن عبد الله فكري، المرجع السابق، ص 25 وما بعدها .

[2]– تقرير مؤسسة راند في 1999/12/15 بعنوان نحواستيراتجية قومية لمكافحة الإرهاب عبر الإنترنت.المنشور على الموقع الإلكتروني: http:// www.rand.org. وقد اشار هذا التقرير إلى خطورة الإرهاب عبر الإنترنت، كما اعتبر التقرير ان العدوان من قبل الإرهابيين عبر الإنترنت كذلك العصابات الاجرامية من اخطر أشكال العدوان، وتصل درجة خطورته إلى ابعد من العدوان الإرهابي الحادث في العالم المادي، ولذلك جاء في احد توصياته ضرورة قيام فر تنفيذي ولجان تشريعية لاعداد العدة مواجهة الإرهاب عبر الإنترنت وتحمل المسؤولية الكاملة عن ذلك.

الإرهاب الالكتروني التطور التكنولوجي و كثرة الاعتماد على وسائل التقنية العالية من حواسيب و شبكة انترنت في تسيير شؤون الحياة. فكلما ارتقت الدول في استخدام شبكات نظام المعلومات و زاد الترابط بين هذه الشبكات، زاد تعرضها بالتالي لهذا النوع من التهديد،و هو الوضع الذي يثير أشد القلق لدى الدول المتقدمة التي يتزايد اعتمادها على شبكات المعلومات في ادارة معظم شؤون حياتها. فالتطور الكبير في الاعتماد على تكنولوجيا المعلومات في ادارة مشروعات البنى الأساسية يعد مجالا خصبا للارهابيين الالكترونيين –كما سبق ذكره – لممارسة جرائمهم ضد نظم السيطرة والتحكم التي تؤثر في توزيع الكهرباء والمياه و الاتصالات و شبكات البنوك والتجارة وغيرها. [1]

ولهذا يرى الخبراء والباحثين أن ما يهدد البشرية في المستقبل ليس الصواريخ بل أجهزة الكمبيوتر في ظل شن حرب فضاء الكترونية بين الدول تؤدي إلى تدمير البنية الأساسية في بلد من البلدان ومعدات الدفاع وتخريب الاتصالات وقوى الطاقة والأنظمة العسكرية. ونظرا لاستشعار بعض الدول الخطورة على أمنها القومي من اختراق شبكة الانترنت، فقد سارعت برصد مبالغ مالية هائلة لمواجهة و مكافحة إرهاب الانترنت، كما هو الشأن في الولايات المتحدة الأمريكية (مخطط الرئيس السابق بيل كلنتون لحماية البنية التحتية للدولة الأمريكية من هجمات الإرهاب الإلكتروني).

وإلى جانب ذلك فهناك عوامل أخرى ساعدت على انتشار الإرهاب عبر الإنترنت ومنها: انفتاح الشبكة الغير محكوم أخلاقيا ولا سياسيا ولا ثقافيا ولا قانونيا وتجاريا، – عدم ارتباطها بدولة معينة، صعوبة رقابة أو محاسبة ما ينشر فيها، السرية في تبادل المعلومات وقلة التكلفة، لكل هذه الأسباب أصبح الإرهاب عبر الانترنت هو المقر المختار للحركات والمنظمات المتطرفة والإرهابية، مثل منظمات التطرف الديني أو التمييز العنصري. [2]

المطلب الثالث:

أشكال الإرهاب عبر الإنترنت و موقف التشريعات المقارنة منها

ان المراد من هذا المطلب هو تعداد الصور التي تتخذها هذه الجريمة عبر الانترنت، وكذا موقف مختلف التشريعات المقارنة منها، وذلكمن خلال الفرعين التاليين:

الفرع الاول: أشكال الإرهاب عبر الانترنت.

الفرع الثاني: موقف التشريعات المقارنة من الإرهاب عبر الإنترنت.

---

[1]– محمد محمد الالفي:العوامل الفاعلة في انتشار جرائم الإنترنت، ورقة مقدمة في المؤتمر الدولي الاول حول حماية امن المعلومات والخصوصية في قانون الإنترنت، القاهرة، جوان 2008/4/2، http:// www.f– law.net

2– محمد محمد الالفي، المرجع السابق، الموضع السابق.

الفرع الأول: أشكال الإرهاب عبر الإنترنت

في عصر الازدهار الإلكتروني وفي زمن قيام حكومات الكترونية، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها أنماط الجريمة، والتي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة الإرهاب الإلكتروني أوكما يسميها البعض جريمة إرهاب الانترنت والتي أخذت أشكالا حديثة تتماشى مع التطور التقني، وتغير وتطور الأساليب التي يحاول المفسدين الوصول بها إلى أهدافهم و منها تحقيق أضرارا جسيمة من خلال تنفيذهم لتلك الجريمة.ومن الأشكال التي تتخذها هذه الجريمة:

أولا: قيادة الجماعات الإرهابية و نشر الأفكار المتطرفة:

لقد أصبح الفضاء الإلكتروني ملاذا أمنا لدعاة التطرف والعنصرية مثل " النازية الجديدة " وتفوق الجنس الأبيض " و" معاداة السامية "، وقد تبلورت أساليبهم الإلكترونية الرقمية التي تخدم أفكارهم بالإضافة إلى فعاليتها في تجنيد العناصر الشبابية لصالح معتقداتهم المتطرفة والإرهابية. حيث يمكن من خلال شبكة الانترنت بث الأفكار المتطرفة سواء كانت سياسية أو دينية أو عنصرية، وبالتالي السيطرة على وجدان الأفراد وخاصة منهم الشباب واستغلال طموحاتهم واندفاعهم وقلة خبرتهم و سطحية تفكيرهم في إفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مأرب خاصة تتعارض مع مصلحة الوطن واستقرار المجتمع[1].

لقد أصبحت الانترنت مجالا خصبا لنشر المواقع المعادية الموجهة ضد سياسة دولة محددة أو عقيدة أو مذهب معين أو طائفة معينة، وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد المستهدف.فأما المواقع السياسية المعادية ففيها يتم الإساءة إلى بلد معين وإلى قادته السياسيين عن طريق نشر الأخبار الملفقة والمعلومات المزورة والفاسدة التي تنشر الفرقة بين أفراد الشعب ونظامه السياسي. وهم غالبا ما يكونون من معارضي النظام السياسي السائد في بلد ما.

هذا من جهة ومن جهة أخرى، فهم يعملون في الغالب على إنشاء قاعدة بيانات بعناوين أشخاص يحصلون عليها من الشركات التي تبيع تلك القواعد أو بطرق أخرى ومن ثم يضيفون تلك العناوين قسرا الى قائمتهم البريدية ويبدؤوا في اغراق تلك العناوين بمنشوراتهم، وهم عادة يلجأ ون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولإيصال أصواتهم إلى اكبر قدر ممكن[2]. ومثال ذلك ما جرى في الجزائر، إذ قامت مجموعة مجهولة[3] باستحداث صفحة خاصة على "الفايس بوك " منتحلين صفات شباب جزائريين، يحاولون تحريض الشباب على الانتفاضة والاحتجاج على الأوضاع الاقتصادية والاجتماعية التي آلت إليها

---

[1]– مقال منشور من مركز البحوث والدراسات بشرطة دبي بعنوان الامن والإنترنت، http://www.dubaipolice.gov

[2]– د/عبد الفتاح مراد، المرجع السابق، ص 399

[3]– لقد كشفت التحقيقات الامنية بأنه من بين المنخرطين في موقع التواصل الاجتماعي التي تدعو إلى الثورة في الجزائر يوم 17 سبتمبر، يوجد عرب من بعض الدول المجاورة. نوارة باشوش: مصالح الامن تضع يدها على المخططين والمحرضين عبر الفايس بوك واليوتيوب، جريدة الشروق، 2011/09/17، العدد 3417، ص 04.

البلاد من بطالة وحقرة وأزمة سكن، و القيام بثورة على غرار تلك التي قامت في تونس و مصر وليبيا..." ؛ حيث ورد في نفس الصفحة أنه: " تم اختيار يوم 17 سبتمبر كيوم رسمي لاندلاع الثورة الجزائرية ضد النظام والاحتجاج لوقف الفساد " و في نفس السياق وجدت مجموعة من الشباب أطلقوا على أنفسهم " الشباب القيادي للتجمع الوطني الديمقراطي " باستغلال موقع يدعون و يحرضون فيه غيرهم من الشباب الجزائري للخروج ضد النظام يوم 17 سبتمبر على الساعة التاسعة و النصف صباحا في ساحة البريد المركزي (كمكان للتجمع). ضف إلى ذلك ووفقا لتحقيقات وجدت مقاطع فيديو تم بثها في موقع اليوتوب تدعو للثورة في الجزائر، منها عدد من الفيديوهات لسيدات منقبات، يرتدين نظرات شمسية يحرضن الشباب على الثورة ويشجعنه على اللحاق بإخوانهم من الثوار في مصر وتونس و ليبيا للتخلص من الورم الذي زرعته فرنسا في المغرب العربي ممثلا في نظام الجزائر على حد وصفهن[1].

كما قامت مجموعة في مصر طلقت على نفسها " حزب التحرير" بالدعوة إلى مكافحة وتعطيل أحكام الدستور والقانون، ومنع مؤسسات الدولة مباشرة عملها و الترويج لأفكارها عبر منشورات. ومن خلال موقع الانترنت تم إنشاؤه لهذا الغرض وكذا بغرض تغيير النظام الحاكم.وقد أصدرت محكمة امن الدولة العليا حكما يدين أفراده بتقرير عقوبة السجن الذي يتراوح مابين سنة إلى 7 سنوات[2].

أما المواقع المعادية للعقيدة فمنها ما يكون موجها من قبل أعداء حاقدين من أتباع الديانات الأخرى،كالمواقع التي تنشئها الجاليات اليهودية أو النصرانية تحت مسميات إسلامية بقصد بث معلومات خاطئة عن الإسلام والقرآن، أو بهدف الدعاية للأديان الأخرى ونشر الشبهة والافتراءات حول الإسلام.

أما القسم الثاني منها فيكون أفرادها من ذات العقيدة و لكنهم يختلفون في المذاهب. ويكون الغرض من تأسيس هذه المواقع بصفة عامة:

أ- الإساءة إلى دين من الأديان السماوية ونشر الأفكار السيئة عنه وحث الناس على الابتعاد عنه.

ب- بث الشقاق بين أفراد الشعب الواحد و المعتنقين لأكثر من دين فيحاولون إثارة الفتنة فيما بينهم عن طريق نشر الأخبار الكاذبة والمظللة في محاولة منهم لتحقيق هدفهم الخبيث[3]. و كمثال على ذلك، قيام بعض الغربيين المتعاطفين مع المرتد الكويتي المدعو " حسين قمر " - والذي غير اسمه إلى "روبرت قمر" بعد أن دخل المسيحية – بنشر عبر الانترنت التماسا بمساعدة دولية له. كما قام عدد من العلمانيين بتأييد حق المذكور بالارتداد عن دين الإسلام استنادا إلى حرية الانسان في العقيدة، وحقه في تغيير ديانته التي تفرض عليه لصغر سنه بسبب ولاية أسرته، و حقه في اختيار الدين الذي يناسبه عند بلوغه سن الرشد و التمييز. ولاشك أن هذا التفلسف في تبرير ما يخالف العقيدة و القيم الراسخة في المجتمع قد يكون

---

[1]- نوارة باشوش، المرجع السابق ، الموضع السابق.

[2]- محمد محمد الالفي،(العوامل الفاعلة في انتشار جرائم الإنترنت) مرجع سابق،

http:// www.f -law.net

[3]- منير محمد الجنبهي و ممدوح محمد الجنبهي،(جرائم الإنترنت.....) مرجع سابق، ص 81.

له تأثير سلبي عميق على الفرد لاسيما صغير السن، وهو الأمر الذي يتسبب في زعزعة ثوابت المجتمع وخلخلة مرتكزات استقراره.[1]

وأما المواقع العنصرية فهي تروج للعنف العرقي الذي يؤدي إلى محاولة الإيقاع بين الأعراق المختلفة وأصحاب الديانات المختلفة، كما في صراع العرقيات في أفغانستان.

وتجدر الإشارة إلى أن الترويج للكراهية والعنصرية عبر الانترنت قد عرف بدايته في الولايات المتحدة الأمريكية عام 1995 حينما أقدمت جماعة عنصرية بيضاء على إنشاء موقع لها عبر شبكة الانترنت تحت عنوان " ستورم فرونت ". و قد أسس هذا الموقع شخصا يدعى " دون بلاك"[2]. ومنذ ذلك الوقت شهدت شبكة المعلومات الدولية انطلاق آلاف المواقع العنصرية، قدرت وقفا لإحصائية أعدها مركز متخصص عن مواقع الكراهية على تلك الشبكة بثلاثة آلاف موقع[3] ومنها موقع المنظمة النازية العنصرية "مافيا ترنشكوت" "trench coot " [4] والذي يمتاز أعضاؤها بخبرة و ذكاء في مجال المعلوماتية (الكمبيوتر). وهو ما كشفته تحقيقات الشرطة الأمريكية اثر الجريمة التي ارتكبها طالبان امريكيان ينتميان إلى هذه المنظمة يدعيان " إيريك هارس " و " ديلان كيلبوله " الذين قاما باطلاق النار على زملائهم بمدرستهم الثانوية في مدينة " لتيلتون " التابعة لولاية " كولورادو" في الولايات المتحدة الأمريكية فأردوا على الفور 15 قتيلا. ثم اختبآ في مكتبة المدرسة إلى ان عثرت عليهما الشرطة منتحرين بعد ساعات من الإعتداء، وعقب تفكيك عدد من العبوات الناسفة في إحدى السيارات المجاورة للمدرسة. ولقد أسفرت التحريات بأن الطالبان كانا يعلنان صراحة قبل الحادث أنهما " سيجعلان من شهر ابريل يوما مؤثرا لا ينساه الأمريكيون"[5]. ولعل

---

[1]– د/عبد الفتاح بيومي حجازي، (الاحداث والإنترنت) مرجع سابق، ص 182.

[2]– دون بلاك هو خبير في الكمبيوتر وعضو سابق في جماعة كوكلوكس كلان العنصرية البيضاء. هذه الجماعة يدعو مؤسسوها إلى ضرورة تفوق الجنس الأبيض عن باقي الاجناس.وهي موجودة على الموقع www.kkk.com وتمثل عددا من الجمعيات العنصرية تحمل أسماء عرقية مثل: امريكا أولا America first، والجنس الأبيض the white race ايجابية المسيحية، positif christianity والعهود والمواثيق the constitution وتضم صفحات هذا الموقع بيانات ومعلومات عن اسم زعيم هذه المنظمة "توماس روب" ورقم هاتفه وعنوان موقعه. ولقد تم حجب موقع المنظمة من شبكة الإنترنت بناء على طلب من الحكومة الأمريكية بسبب التطرف الديني لأعضاء هذه المنظمة وعنصريتهم السياسية وتطرفهم في التمييز للون الأبيض. لمزيد من التفاصيل ينظر د/ حسنين المحمدي بوادي، المرجع السابق، ص 88

[3]– ويقول العاملون ضد العنصرية ان مواقع الإنترنت والبريد الإلكتروني ومساحات الحوار التي تجري على الشبكة أصبحت وسائل لتجنيد انصار جماعات الكراهية والعنصرية وجمع التبرعات لها. ينظر بحث مكافحة عنصرية الإنترنت http:// news.bbc.co.uk،

[4]– هذه المنظمة تضم في صفوفها طلبة يكنون الكراهية للمواطنين خصوصا للسود والاسبان ولغيرهما من الاقليات ويرتدون زيا خاصا مكونا من المعاطف السوداء الطويلة ويطلقون شعارات دموية مثل:" ينبغي قتلهم جميعا". د/حسنين المحمدي بوادي، المرجع السابق، ص 89.

[5]– ولقد تم حجب موقع هذه المنظمة من قبل شركة امريكان اون لاين بناء على ضغوط الرأي العام والحكومة الأمريكية. د/ حسنين المحمدي بوادي، المرجع السابق، الموضع السابق.

ما حدث على شبكة الانترنت في خصوص مؤتمر "ديربان " بجنوب إفريقيا عن العنصرية لخير دليل على وجهة النظر هذه.[1]

وإضافة إلى ذلك فهناك عدة قضايا عرضت على المحاكم يشجع المتهمون فيها فكرة العنصرية و التطرف باستعمال الانترنت. ومنها القضية التي أدانت فيها محكمة جنح بروكسل- بلجيكا أثناء أعياد – شرطيا بالضبط القضائي وشخصا آخر معه، كونهما قاما بإدلاء بأقوال متنوعة في حلقات النقاش عبر الانترنت، تشير إلى فكر عنصري.ولقد اعتبرت المحكمة حلقات النقاش بالرغم من أنها تتمتع بالخصوصية إلا أنها مفتوح لاستقبال الأشخاص. ومن ثم فهي مشمولة بما هو مقرر بالمادة 444 عقوبات بلجيكي.كما أدانت محكمة ستراسبورغ في 1999/8/27 قيام احد الأشخاص بالحث على التمييز العنصري العلني ضد العرب عبر حلقات النقاش،حيث ورد في وقائع الحكم أن المدعو "R "قام بتوجيه قذف إلى العنصر العربي. كما اعترف بنزاهيته وكرهه للأجانب المتفرنسين.[2]

ثانيا: القصف الإلكتروني:

القصف الإلكتروني[3]هو أسلوب يستخدمه الإرهابيون للهجوم على شبكات المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات، مما يزيد الضغط على قدرتها على استقبال الرسائل من المتعاملين معها.مما يؤدي إلى تعطل الشبكة و عدم إمكانية استقبال أي رسائل، فضلا عن إمكانية انقطاع الخدمة و خاصة إذا كانت الجهة المضرورة من ذلك هي مقدمة خدمة الانترنت مثلا، حيث يتم ملء منافذ الاتصال (communication- Ports) وكذلك قوائم الانتظار (Queues)مما ينتج عنه انقطاع الخدمة، و بالتالي تكبد خسائر مادية و معنوية غير محدودة[4].منها زعزعة ثقة الناس في سوق الانترنت أو تقصف الخوادم بدودة الانترنت كالشفرة الحمراء والتي تؤدي إلى إغراقها DOS[5] . وقد وصف أحد خبراء الكمبيوتر والانترنت هذه الهجمات بأنها شبيهة بتكديس أكوام القمامة أمام مكتب شركة ما في الصباح الباكر بحيث يمنع المتعاملون مع الشركة من الوصول إلى أبوابها للتعامل معها.[6]

---

[1]– لم تكن شبكة المعلومات الدولية بعيدة عن اجندة المؤتمر العالمي حول العنصرية والذي عقد في ديربان جنوب افريقيا في سبتمبر 2001 وبحضور مائة وخمسين دولة. ينظر بحث " مكافحة عنصرية الإنترنت" المنشور على الموقع السابق.

[2]– ينظر في ذلك د/عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص 686-687.

[3]– يطلق على القصف الالكتروني كذلك مصطلح التشبع Saturation أو الهجوم المعلوماتي أو الاغراق بالرسائل والذي هو نوع من الإعتداء ضد الجهوزية او قابلية عمل النظام المعلوماتي، ويقضي بملء نظام معلوماتي بكم هائل من البيانات إلى حد لا يعود بالامكان استعماله بشكل صحيح. وليد الزيدي، المرجع السابق، ص47.

[4]– تكون تلك الرسائل محملة

[4]–لمزيد من التفاصيل حول هذه الدودة ينظر د/عمر محمد أبو بكر بن يونس،(الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص370.

[5]– د/ مصطفى محمد موسى: أساليب إجرامية بالتقنية الرقمية، دراسة مقارنة، دار الكتب والوثائق العربية، القاهرة، 2003، ص203.

و تجدر الإشارة إلى أنه تم تسمية هذا الهجوم بالقصف الإلكتروني تشبيها له بالقصف المدفعي بالقنابل أثناء الحروب[1].

وقد ازدادت في الآونة الأخيرة حوادث تعرض مواقع الشركات المهمة على شبكة الانترنت لهجمات مكثفة من قبل القراصنة، إذ يقوم هؤلاء بإمطار المواقع المذكورة بفيض لا متناهي من البيانات الموجهة إلى عنوانها الإلكتروني –مستخدمين في ذلك عناوين وهمية للرد على رسائلهم الموجهة لمهاجمة هذه المواقع وذلك إلى درجة لا يعود فيها الموقع قادر على الاستيعاب المزيد من البيانات مما يؤدي إلى توقفه عن العمل[2].

وفي ظل اعتماد الدول الكلي على التقدم التكنولوجي أصبح أمر تنفيذ الهجمات المعلوماتية أي القصف الإلكتروني أمرا حتميا يهدد بنيتها التحتية و أهدافها الحيوية و أمنها القومي و ذلك بشن هجمات معدة بطريقة محكمة تدمرها في لحظة واحدة و في اقل من دقيقة واحدة. ومن المواقع التي تعرضت لهجمات معلوماتية أدت إلى خسائر مادية و معنوية:

– المواقع الأمريكية العالمية:

إذ تعرضت كلا من "فراد أي بي دوت كوم "، و " أمازون دوت كوم "، و " سي أن أن دوت كوم"، و" دي دي نت " لسلسلة من أعمال التخريب يوم 2000/02/09 بعد تعرض موقعي "ياهو" و"دوت كوم" العالميتين لذات أعمال التخريب.وحدث الهجوم بقيام المخربين بإرسال ألاف الرسائل التي تشغل الموقع عن التعامل برسائل الزبائن العادية في توقيت واحد و بالغ الحرج[3] تقدر مدته 72 ساعة متواصلة[4] مما أدى إلى توقفها عن العمل عدة ساعات[5].

– موقع وكالة الأنباء الروسية(اتارتاس):

---

[1]– د/ حسنين المحمدي بوادي، المرجع السابق، ص97.

[2]– وليد الزيدي، المرجع السابق، ص47.

[3]– إن توقيت ارتكاب الهجمات تم في وقت بالغ الحرج إذ كانت شركة أي بي دوت كوم تعرض أسهمها للبيع في اسواق الأسهم العالمية، واما الهجوم على موقع شركة إي بي فقد تزامن مع الاعلان عن مشروع مشترك بينها وبين موقع شركة والت ديزني المعروف ب جودوت كوم لتطوير مواقع على الإنترنت لبيع الاعلانات السينمائية وباقي أنواع الدعاية والترويج.ينظر مقال ملاحقة مخربي الإنترنت،http:// news.bbc.co.uk

[4]– /د حسنين المحمدي بوادي، المرجع السابق، ص 100.

[5]– إذ توقف موقع "ياهو" نتيجة القصف الإلكتروني لمدة ثلاث ساعات وعندما عاد للعمل الا بنسبة 70 ٪ من قدرته.كما ان موقع" سي ان ان" الاخبارية قد تعرض هو الاخر لهجوم دام ساعتين تقريبا. اما موقع " دي دي نت " وهو موقع إلكتروني جديد مهم لأخبار شركات التكنولوجيا والكمبيوتر فكمثيله تعرض لهجوم سبب في تعطيل لاكثر من ساعتين ونصف الساعة، ينظر مقال ملاحقة مخربي الإنترنت ، المنشور على الموقع السابق .

إذ اقتحم متسللون معارضون للحملة العسكرية الروسية على الشيشان هذا الموقع تاركين رسالة مضمونها: " إننا هنا لمقاتلة الشيطان و قواتنا لازالت تكبر " ، مما أدى إلى تعطله لأكثر من ساعة في الوقت الذي قام فيه الفنيون بإصلاح الأعطال الناتجة عن عمليات التسلل[1].

– مواقع حكومية اسرائلية:

فقد نشر بتاريخ 2000/10/26 أن مواقع حكومية اسرائلية منها موقع البرلمان الإسرائيلي وموقع وزارة الخارجية الاسرائيلية و موقع لرئيس الوزراء الاسرائيلي ووزارة الدفاع وموقع وزارة الخزانة الاسرائيلية، قد تعرضت لهجمات تخريبية واسعة على شبكة الانترنت من جماعات إسلامية من جميع أنحاء العالم انتقاما، لما قام به مراهقين اسرائيليين من تخريب لموقع لحزب الله في لبنان وكذا الاضطهاد الذي يعاني منه الشعب الفلسطيني. مما أدى إلى شلها تماما وتعطيلها تقنيا عن العمل لساعات عديدة.إذ بعث هؤلاء المهاجمون بوابل من الرسائل الإلكترونية المتلاحقة والمتضمنة عبارات مثل: " الموت لكل اليهود " بهدف تخريب المواقع الاسرائيلية[2].

وتجدر هنا إلى أن هذا الإرهاب الذي يمارس عبر الانترنت لا يقتصر على الكبار بل قد يتعداه إلى الأحداث.فالتسلل إلى مواقع الشبكة المختلفة و العبث بها ليس حكرا على مجموعات منظمة، وإنما قد يكون مجرد محاولات فردية من صبية يستخدمون أسماء وهمية أو حركية لإدخال الروع في نفوس الآخرين، ومنهم صبي المافيا[3] والذي استطاع ان يخترق الشبكة وعطل مواقع خاصة بالشبكة الإخبارية CNN وموقع Yahoo وكذلك مواقع أخرى على الانترنت عن طريق إدخال كميات كبيرة من المعلومات فيها. وكمثال ثاني يتمثل في إحباط محاولة تعطيل شبكة المعلومات الدولية على مستوى دول العالم كلها عشية رأس السنة الميلادية 2001 من قبل مكتب التحقيقات الفدرالي الأمريكي.حيث خطط قراصنة شباب (بالغين و مراهقين) من عدة دول لتنفيذها[4].

---

[1]– مقال روسيا في الشيشان امام معركة الإنترنت ، news.bbc.co.uk . http://

[2]– لقد سهلت مجموعات اسلامية الحصول على برامج متخصصة تتيح ارسال سيلا ضخما من الرسائل الإلكترونية بهدف تخريب المواقع الاسرائيلية ولذلك حولت وزارة الدفاع الاسرائيلية– محاولة تفادي هذه الحرب– مزود خدماتها في الإنترنت من مزود خدمة اسرائيلي محلي إلى اخر يتبع شركة ATNT الأمريكية للاتصالات. وقد قالت صحيفة يدعوت احرنوت الاسرائيلية ان الامن الاسرائيلي تمكن من متابعة مصدر بعض تلك الرسائل، والذي تبين بأنها مرسلة من معاهد بحث اكاديمية في القاهرة بالاضافة إلى مهاجمين اخرين من الولايات المتحدة الأمريكية واوروبا، مستخدمين في ذلك التسهيلات التي توفرها شركات الإنترنت المعروفة مثل "yahoo، hotmail ".

لمزيد من التفاصيل ينظر مقال مواجهات اسرائلية فلسطنية على شبكة الإنترنت، news.bbc.co.uk http:// و د/عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص 688 وما بعدها.

[3]– صبي المافيا هو حدث كندي اطلق على نفسه هذا الاسم للايحاء بخطورته. لمزيد من التفاصيل عن صبي المافيا ينظر د/ عبد الفتاح بيومي حجازي (الاحداث والإنترنت) مرجع سابق، ص 188.

[4]– لمزيد من التفاصيل ينظر مقال مراهقون تآمروا لتعطيل الإنترنت مطلع العام الجديد ، http://www.aljazeera.net

ثالثا: تدمير أنظمة المعلومات

قد يستخدم الانترنت في شن هجمات إرهابية لتدمير وإتلاف أنظمة المعلومات التي تعتمد عليها الدول لاسيما المتقدمة في إدارة شؤونها السياسية والاقتصادية والاجتماعية ويكون ذلك عن طريق اقتحام أو التسلل للمواقع الشخصية والرسمية أو اختراق الأجهزة الشخصية واختراق البريد الإلكتروني أو الاستيلاء عليه... وهي أفعال أصبحت تنشر يوميا في الصحف والاخبار، فكثيرا ما تتداول الصحف والدوريات العلمية أنباء كثيرة عن الاختراقات الأمنية المتعددة في أماكن كثيرة من العالم ليس آخرها اختراق أجهزة الحاسب الآلي في البنتاجون (وزارة الدفاع الأمريكية) [1].

ولكي تتم عملية الاختراق لا بد من برنامج يتم تصميمه ليتيح للمخترق الذي يريد اختراق الحاسب الآلي لشخص آخر أن يتم ذلك الاختراق. وقد صممت العديد من تلك البرامج التي تتيح عملية الاختراق وتجعلها سهلة، إلا أن معظم تلك البرامج كان بها نقطة ضعف أساسية تقلل كثيرا من إمكانيتها[2]، فيما عدا برنامج واحد تمكن مصممو من التغلب على نقطة الضعف التي منها كافة برامج الاختراق الأخرى إلا وهو برنامج " حصان طرواده " [3] البرنامج الأخطر و الأشهر في مجال اختراق أجهزة الحاسبات الآلية. والذي هو عبارة عن تغطية أوامر الحاسب الآلي لتمكين الحاسب الآلي من إتيان بوظائف غير مصرح له بها مع ترك البرنامج على حاله للاستثمار في تحقيق أهدافه[4].

---

[1]– محمد عبد الله المنشاري، المرجع السابق، http:// www.minshawi.com

[2]– وتتمثل نقطة الضعف في امكانية الشعور بتلك البرامج على الجهاز الذي تم اختراقه وعليه يكون ومن الممكن متابعة تلك البرامج والقضاء عليها.

[3]– حصان طروادة بالفرنسية cheval de troie وبالانجليزية trojan horse و هو عبارة عن برمجية اختراق من حيث الطبيعة التقنية ولها وجهان.الوجه الاول هو ا لزبون client أما الوجه الثاني فهو الخادم surfer ينفصلان بارسال الخادم إلى حاسوب الغير المقصود ويتم التعامل معه بعد ذلك ولقد صمم هذا البرنامج في البداية بغرض حسن ومفيد وهو ما يقوم به الأبناء غلى جهاز الكمبيوتر وفي غياب الوالدين أو معرفة ما يقوم به الموظفون على جهاز الكمبيوتر في غياب المدراء، الا انه تم تطوير هذا البرنامج بعد ذلك تطويرا سيئا ومدمرا. وذلك بنسخ ذاته إلى الملفات الأخرى، كما انه يتيح للمخترق امكانية الدخول إلى الأماكن السرية والمشفرة فينتشر فيها ليحقق غرضه في اتدمير والتخريب. ويعتبر المبرمج (backorfice) من ابرز الامثلة المعروفة من حصان طراودة، إذ يصفه احد خبراء الحاسوب الأمريكان، بانه: "...يمكنه ان يدمر الكاميرا التي تملكها ويمكنه ان يفتح جهاز الميكروفون الخاص بك، ويمكنه ان ينسخ ملفات وان ينقل كل ما يراه ويسمعه ويقرأه ويعيد ارساله " وتجدر الإشارة إلى ان ما يميز حصان طروداة عن باقي الفيروسات انه لا يستطيع تنشيط نفسه وتحقيق معدلات غير محددة للانتشار، وانما يحتاج إلى من يقوم بتنشيطه ويعني ذلك انه لا يصيب الحاسوب الا مرة واحدة.ينظر على التوالي: عمر محمد أبو بكر بن يونس، (الجرائم الناشئة.....) مرجع سابق، ص 366–367. وليد الزيدي، المرجع السابق، ص46 . منير محمد الجنبيهي، ممدوح محمد الجنبيهي، (جرائم الإنترنت...) مرجع سابق، ص 48.

[4]– د/ محمد الامين البشري، المرجع السابق، ص 96.

وتبرز الخطورة الخاصة في هذا النوع من الفيروسات في أن مبرمج هذا الفيروس لا يحتاج إلى إحداث تدوير له عبر الانترنت، وإنما كل ما يقوم به هو وضعه في حاسوب يكون على اتصال بالشبكة و يتكفل الفيروس بالباقي. كما لو يقوم معد هذا الفيروس بإلصاقه بوثيقةDoc ثم يقوم بإلصاقها attachement برسالة الكترونية ويرسلها إلى غيره، وعند فتح الغير للرسالة المذكورة فان الفيروس يهبط في حاسوبه دون أن يشعر به في الغالب، أو أن يتم وضعه في الحاسوب عن طريق تحميل برمجيات عبر الانترنت أو تحميل برمجيات مستنسخة أو غير ذات ثقة. [1]

هذا من ومن جهة أخرى، فان هذا البرنامج لا يمكن كشفه بواسطة البرامج المتخصصة في كشف الفيروسات.وعليه فانه لا يمكن في الأغلب الأعم من الأحوال معرفة وجود مثل هذا البرنامج على جهاز الكمبيوتر أو الإحساس بوجوده للقضاء عليه.[2]

ولتتم عملية الاقتحام يجب زرع حصان طروادة في جهاز الصحية بعدة طرق منها:

– يرسل عن طريق البريد الإلكتروني كملف ملحق حيث يقوم الشخص باستقباله و تشغيله و قد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى.

– عند استعمال برنامج المحادثة الشهير المنتج من إسرائيل المعروف ب (ICQ).

–عند تحميل برنامج من احد المواقع غير الموثوق بها.

–مجرد كتابة كوده على الجهاز نفسه.

– في حالة اتصال الجهاز بشبكة داخلية أو شبكة الانترنت.

– يمكن نقل الملف أيضا بواسطة برنامج (FTP) أو (Telnet) الخاصة بنقل الملفات.

– كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجودة في برامج معالجة النصوص بصفة عامة فان برامج القرصنة تعتمد كليا على بروتوكول(TCP/IP) و هناك أدوات (Activex) مصممة و جاهزة لخدمة التعامل بهذا البروتوكول ومن أشهرها (winsock.ocx) لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الأدوات، ويحتاج الأمر إلى برنامجين خادم في جهاز الضحية وعميل في جهاز المتسلل حيث يقوم الخادم بفتح منفذ في جهاز الضحية و يكون هذا المنفذ معروفا من قبل العميل أصلا.حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية حيث يتعرف برنامج الخادم (serveur) على إشارات البرنامج المخترق ويتم الاتصال ومن ثم يتم عرض محتويات جهاز الضحية كاملة لدى المخترق حيث يتمكن العبث بها أو الاستيلاء على ما يريد منها[3].

---

[1]– د/عمر محمد أبو بكر بن يونس، (الجرائم الناشئة.....) مرجع سابق، ص467.

[2]– منير محمد الجنبيهي، محمود محمد الجنبيهي، (جرائم الإنترنت....) مرجع سابق، الموضع السابق.

[3]– لمزيد من التفاصيل ينظر محمد عبد الله المنشاوي، البحث السابق،www.minshawi.com http://

وإلى جانب برنامج حصان طروادة يستخدم المهاجم في هجومه لتدمير النظام المعلوماتي ما يسمى بالقنبلة المنطقية المعروفة بالشفرة المعيقة أو المعوقة Disabling code [1]، والتي هي عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة و مخفية مع برامج أخرى، وتهدف إلى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو في فترة زمنية منتظمة، بحيث تعمل على مبدأ التوقيت فتحدث تدميرا وتغييرا في المعلومات و البرامج عند انجاز أمر معين في الحاسب الآلي أو برنامج معين[2]. وهي من حيث الشكل ليست ملفا كاملا وإنما شفرة تنظم إلى مجموعة ملفات البرمجية بتقسيمها إلى أجزاء هنا و هناك حتى لا يمكن التعرف عليها.بحيث تجتمع فيما بينها بحسب الأمر المعطى لها في زمن وحيد و يؤدي اجتماعها هذا إلى انعدام القدرة على تشغيل البرمجية عبر الحاسوب.وأما من حيث الموضوع فهي تؤدي إلى خلل في البرمجية ونظامها و قد يطال ذلك نظام عمل الحاسوب لاشتماله على برمجيات من ذات الطبيعة التقنية لمجموعة البرمجية، أو أن تكون ملفات هذه البرمجية من النوعية التي ترتبط بنظام التشغيل حال إنزالها على الحاسوب.وأكثر ما تبرز القنابل المنطقية في البرمجيات المؤقتة Bita version التي تشتمل عليها الحملات الاعلانية للبرمجيات. وفي البرمجيات المؤجرة التي لا يفقد مالكها حقوق الملكية فهو يقوم بتأجيرها فقط[3].

وإلى جانب هذه القنبلة هناك قنبلة أخرى تسمى بالقنبلة الزمنية[4] و التي تستخدم كمثيلتها في التخريب بإثارتها لحدث في لحظة زمنية محددة بالساعة و اليوم و السنة والوقت اللازم. كأن يضع المبرمج هذه القنبلة على اسم معين في قائمة موظفي الشركة، بحيث يكون البرنامج قابلا للانفجار بمجرد إزالة ذلك الاسم. و الذي بانفجاره يقضي على جميع البرامج والمعلومات المرتبطة بذات البرنامج و غيره محدثا خسائر انتقامية للشركة.ومن الأمثلة الواقعية على هذه القنابل المعلوماتية:

– تمكن احد العاملين بإدارة المياه و الطاقة في الولايات المتحدة الأمريكية –ولاية لوس انجلاس–من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها، مما أدى إلى تخريب هذا النظام عدة مرات.

– قيام محاسب خبير في نظام المعلومات بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة التي يعمل بها بدافع الانتقام منها (لفصله منها)، حيث انفجرت بعد مضي ستة أشهر من رحيله من المنشأة، وترتب على ذلك الإتلاف الكلي للبيانات المتعلقة بها[5].

---

[1]– كما تسمى تلك القنبلة بالقنبلة الموقوتة Date bomb ويصطلح عليها باللغة الفرنسية bombe logique وباللغة الانجليزية logic bomb .

[2]– محمدأمين أحمد الشوابكة، المرجع السابق، ص 240.

[3]– لمزيد من التفاصيل، ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص 371

[4]– القنبلة الزمنية time bomb سميت كذلك لقيامها بالعمل التخريبي في وقت يحدد سلفا وهي تعتبر إلى جانب القنبلة المنطقية أنواعا من القنابل المعلوماتية.

[5]– محمد أمين أحمد الشوابكة، المرجع السابق، ص 241

كما قد يستخدم المهاجم لتخريب نظم المعلومات ما يعرف ببرنامج الدودة (worm software) والذي يقوم باستغلال أية فجوة في نظم التشغيل كي ينتقل من حاسب إلى آخر، ومن شبكة إلى أخرى عبر الوصلات التي تربط بينهما. وتتكاثر أثناء عملية انتقالها بإنتاج نسخ منها و بدون حاجة لتدخل إنساني في تنشيطها (التنشيط الذاتي) [1]. وتهدف هذه البرامج إلى العمل على تقليل خفض كفاءة الشبكة، أو إلى التخريب الفعلي للملفات والبرامج ونظم التشغيل، وذلك بإشغال أي حيز ممكن من سعة الشبكة.فهي تتسبب في تعطيل الحاسوب بتجميد لوحة المفاتيح والشاشة و تعبئة الذاكرة وتبطئة الحاسوب.[2] ولقد ظهرت الدودة لأول مرة في 1988/12/2 على يد العبقري "روبرت موريس" Robert MORRIS"؛ اذ صممها ذلك الأخير خصيصا لكي يثبت عدم ملائمة أساليب وسائل الأمان في شبكة الكمبيوتر، ولكنه تسبب في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة الأمريكية، بالإضافة إلى إعاقة طريق ومسلك الشبكات، بالإضافة إلى خسائر مالية كبيرة في مواجهة دودة الانترنت (Worm Internet).[3] ولقد تم إدانة موريس بالحكم عليه بالحبس لمدة ثلاث سنوات و بالعمل 400 ساعة في الخدمة الاجتماعية و غرامة قدرها 10500 دولار، بالإضافة إلى تكاليف المراقبة، ففي عام 1999 ظهرت هناك دودة Explore.zip وكذلك دودة ميليسا Melissa.[4]

ولعل من أشهر أشكال الدودة عبر الانترنت هي ما يسمى بدودة الحب " love bug" التي ابتكرها الفيليبيني " أونال دوقزمن" Onel De Guzman في عام 2000، بحيث تعمل كملصق على مراسلة الكترونية تهبط في الجهاز بمجرد فتح الرسالة المعنونة بعبارات حب و اغراء. وقد تسببت في خسائر تقدر بملايين الدولارات في العديد من المؤسسات مثل "Nasa" وإدارة الأمن القومي SCA وقطاع عريض من المواقع التجارية.كذلك برزت أشكال أخرى للدودة كتلك التي أعلنت عنها مؤسسة نورتن "Norton " المتخصصة في مكافحة الفيروسات في نوفمبر 2000 وهي نوعان: أولهما W32.hllw.bymerworm و التي هي عبارة عن دودة تنتشر عبر محرك الشبكات المشتركة فتقوم بالبحث عن الملفات المشتركة في الشبكة ثم تطبع نفسها في ملف النظام في برمجية النوافذ

---

[1]– وبهذا فهي تختلف عن حصان طروادة الا انها لا تلتصق بنظم التشغيل في الحاسوب الذي تصيبه، ومن هنا فهي تختلف عن الفيروس الذي يصيب نظم التشغيل وغيرها.

[2]– ينظر وليدالزيدي، المرجع السابق، ص 45.

[3]– لمزيد من التفاصيل عن قضية موريس ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة.....) مرجع سابق، ص368.

[4]– تقوم دودة Explore.zip بتدمير الملفات الإلكترونية مع تهبيط قدرة عمل الشبكات وتسبيب عطل في خدمة ملقمات أو خوادم البريد الإلكتروني. اما دودة ميليسا Melissa فهي تصل عبر البريد الإلكتروني (Outlock–Edoura) لتعطي الملفات وتحطم أنظمة الحاسوب، وهي عبارة عن دودة تنتمي إلى طائفة Macro Virus لمزيد من التفاصيل ينظر:

– Michel BORDERA: the computer virus war، is the legal system fighting or surrending?, http://wings.biffalo.edu

Windows/system folder/. والدودة الأخرى w95. hybris.gen worm والتي تم اكتشافها في سبتمبر 2000 وتنتشر حين إرسال ملف ملصق بالرسالة الإلكترونية المرسلة. وعندما تعمل هذه الدودة فان ملف wsock32.dll المكتبي يحدث تعديلا أو يتغير مكانه، وهو ما يجعلها تلتصق من جديد بكل رسالة الكترونية يتم إرسالها. وفي فبراير 2001 ظهرت دودة أطلق عليها اسم لاعبة التنس الشهيرة Cornickova Anna أو Anna Virus ، و في مطلع عام 2001 تم الإعلان عن دودة جديدة تسمى Nacked wife. ESC.[1]

وقد كثرت حالات الاختراق عبر شبكة الانترنت، ولم تعد قاصرة على المحترفين فقط بل تعدت إلى بعض الهواة أيضا من باب إثبات الذات والقدرة على القيام بتلك المحاولات بنجاح مثلهم في ذلك مثل المحترفين.فقد قدرت وكالة المباحث الفدرالية الأمريكية في عام 1997 أن حوالي 43 ٪ من الشركات التي تستخدم خدمة الانترنت تعرضت لمحاولات اختراق تتراوح بين 3-5 مرات خلال سنة واحدة.أما في سنة 1999 زاد العدد إلى 800 حالة وهو ضعف عدد الحوادث التي قامت بالتحري عنها في عام 1998. أما الهجوم على شبكات الحاسب الآلي على الانترنت فقد تضاعف هو الآخر إذ بلغت نسبة الزيادة300٪ في ذلك العام أيضا وهي زيادة رهيبة ومرعبة.وقد أكدت وحدة الخدمات السرية الأمريكية (the us secret service) أن الجرائم المنظمة قد بدأت في الاتجاه نحو استغلال التسلل للحصول على المعلومات اللازمة لتنفيذ مخططاتها الإجرامية. و قد أوضحت دراسة أجريت عام 1979 على 581 طالب جامعي أمريكي، أن نسبة (50 ٪) منهم قد اشترك في أعمال غير نظامية أثناء استخدام الانترنت خلال ذلك العام، وان(47) طالب أو ما نسبته (7.3 ٪) سبق وان قبض عليه في جرائم تتعلق بالحاسب الآلي، وأن (75)طالبا منهم أو ما نسبته (13.3 ٪) منهم قبض على أصدقائهم في جرائم تتعلق أيضا بالحاسب الآلي[2].

ومن الأمثلة الواقعية لحالات تدمير إرهابي لشبكة المعلومات نذكر:

- قيام مراهقة في الخامسة عشر من عمرها بمحاولة اختراق إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة، وتمثل تبريرها في أنها ملت من مشاهدة التلفزيون ففكرت في شيء آخر تقوم به يبدد ما تشعر به من ملل.[3]

- وفي حادثة أخرى و أثناء حرب الخليج، قام مراهقان بالتسلل عن طريق جهاز الكمبيوتر من منزلهما إلى الصفحة العنكبوتية الخاصة بإحدى القواعد العسكرية الأمريكية.

- وفي عام 1997 قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار (Massachusetts)، مما أدى إلى تعطيل نظام الملاحة الجوية لمدة ستة ساعات[4].

---

[1]- لمزيد من التفاصيل ينظر د/ عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص369-370

[2]- ينظر منير محمد الجنبيهي، ممدوح محمد الجنبيهي، (جرائم الإنترنت...) مرجع سابق، ص 54 وما بعدها.

[3]- حسنين المحمدي بوادي، المرجع السابق، ص74.

[4]- محمد محمد عبد الله المنشاوي، البحث السابق ، http:// www.minshawi.com

– كما تعرضت شبكة الانترنت الإماراتية للتخريب من قبل شبكة قراصنة عالميين تسببوا ليس في تخريب خدماتها فحسب بل العديد من الأنظمة العالمية الأخرى[1].

– كما تمكن احد القراصنة في الولايات المتحدة الأمريكية من السيطرة على نظام الكمبيوتر في مطار أمريكي صغير وأطفأ مصابيح اضاءة ممرات الهبوط مما هدد بحصول كارثة· وفي ايطاليا هوجمت عدة وزارات و جهات حكومية و مؤسسات من قبل احد الإرهابين. [2]

– أما في استراليا و بالضبط في عام 2000 تمكنت المنظمات الإرهابية من تدمير شبكة الصرف الصحي في إحدى المدن مما نجم عنها أضرار صحية و اقتصادية فادحة أصابت الأهال والمؤسسات والأجهزة الحكومية.

– وفي اليابان وبالتحديد في مارس سنة 2000 أعلنت دوائر الشرطة، المتروبولتيانية عن أن جماعة " آدم هيزكو" الإرهابية أفلحت في اختراق نظام البرمجة المتحكمة في نظام أو أنشطة مائة و خمسون سيارة من سياراتها، بالرغم من أن معظمها لم يكن يحمل أية علامات مميزة. واستطاعت تلك الجماعة أن تتحكم في عمل تلك السيارات و توجيهها حسب التعليمات التي كانت تصدرها لها، بما يحقق نجاح بعض العمليات الخاصة التي أرادت الجماعة تنفيذها. و المعروف أن هذه المنظمة الإرهابية هي التي ارتكبت عملية إطلاق الغاز السام بمحطة مترو الإنفاق في طوكيو عام 1995، و كذلك أفلحت في التلاعب بأنظمة الكمبيوتر والانترنت في أكثر من خمسين شركة من الشركات الكبرى في اليابان وفي اختراق أنظمة عشر إدارات حكومية وتوجيهها لصالحها الخاص[3].

كما أن المواقع الفلسطينية تتعرض بصفة مستمرة من الإسرائيليين إلى الاقتحام والعبث بمحتوياتها وإزالة ما عليها من معلومات و عرض صورة العلم الإسرائيلي على الصفحة الرئيسية بالمواقع المقتحمة[4].

رابعا: التهديد الإرهابي

تعددت الأساليب الإرهابية في التهديد عبر الانترنت من التهديد بالقتل لشخصيات سياسية إلى التهديد بتفجيرات المراكز السياسية أو التجمعات الرياضية ثم التهديد بإطلاق فيروسات لإتلاف الأنظمة المعلوماتية في العالم. ومن الأمثلة الواقعية عن التهديد الإرهابي:

– التهديد بقتل الشخصيات السياسية:

ففي أمريكا و بالضبط في شهر أكتوبر 1999 قام شخص كندي يدعى " تيموثي أندرد " ببث رسالة الكترونية نصها " سوف أقتل الرئيس" من بريده الإلكتروني عبر الانترنت إلى الرئيس الأمريكي " بيل كلنتون"[1].

---

[1]– لمزيد من التفاصيل حول موضوع تخريب شبكة الإنترنت الاماراتية ينظر د/ عبد الفتاح مراد، المرجع السابق، ص 398.

[2]– مقال الإرهاب الإليكتروني، http:// www.crime-research.org

[3]– د/ حسنين المحمدي بوادي، المرجع السابق، ص102-103.

[4]– لمزيد من التفاصيل ينظر منير محمد الجنبيهي وممدوح محمد الجنبيهي، (جرائم الإنترنت...) مرجع سابق، ص 91.

ومن ناحية أخرى فقد أدانت محكمة NANTERRE " بفرنسا قيام أحد الجناة ببعث رسالة تهديد عبر الانترنت عن طريق البريد الإلكتروني إلى احد رجال السياسة يهدده فيها بالقتل وحكمت عليه بالحبس لمدة شهرين مع الإيقاف[2].

وفي كولومبيا وفي نوفمبر 1999 أرسل صبي لم يتجاوز عمره 12 عاما رسالة تهديد عبر الكمبيوتر الخاص بالعائلة إلى الرئيس الكولومبي " باسترانا" يهدد فيها بنسف موكبه الرئاسي وبقتله[3].

أما فيما يخص الشيشان، فوجدت مواقع تدعم ظاهرة أنشطة الجهاد عبر الانترنت وتدعو إلى اغتيال الرئيس الروسي "بوتين "[4].

- التهديد بتفجير المراكز السياسية:

ففي مناسبات أعياد الميلاد لسنة 2001 استغل أربعة تلاميذ بريطانيين من بلدة " جيراردكروس" في مقاطعة بكنجهام شاير في وسط بريطانيا هذه المناسبة في إرسال عبر شبكة الانترنت برقية تهنئة إلى الرئيس الامريكي "كلينتون "، الا أنهم تمادوا في كتابتها إذ أضافوا إلى رسالتهم تلك عبارة: " أرسل مليون دولار والا سنفجر البيت الأبيض "[5].

- التهديد بتفجير التجمعات الرياضية:

ففي 2001/09/12 أرسل الأمريكي االمسمى "كينيث هاريل" رسالة تهديد الكترونية على احد المواقع الرياضية الشهيرة، يهدد فيها بتفجير نهائيات بطولة البيسبول وقتل ما لا يقل عن ستين ألف متفرج كان من المقرر ان يشاهدوا المباراة النهائية في الملعب وكان نص الرسالة كالتالي " المهمة لم تنتهي بعد.....نستعد لتفجير نهائي بطولة البيسبول و قتل ستين ألف أمريكي آخرين "[6].

- التهديد بإطلاق الفيروسات:

هددت مجموعة تطلق على نفسها اسم (بانتس/هاجيس) بإطلاق فيروس[7] يخرب الانظمة المعلوماتية في العالم، ان لم يتم إطلاق سراح صديقهم القرصان المعلوماتي المشهور " كيفن ميتنيك" الذي حكم عليه

---

[1]- تم الإشارة إلى الإحالة في الباب الأول من هذه الرسالة ص145.

[2]- ينظر د/جميل عبد الباقي صغير، (القانون الجنائي والتكنولوجيا الحديثة) مرجع سابق، ص41 وما بعدها.

[3]- ينظر د/ حسنين المحمدي بوادي، المرجع السابق، ص 93.

4- ينظر تقرير " روسيا في الشيشان امام معركة الإنترنت "، http://.news.bbc.co.uk

[5]- ينظر لمزيد من التفاصيل د/حسنين المحمدي بوادي، المرجع السابق، ص 92

[6]- وتجدر الإشارة إلى أن الجاني قد استخدم الإرسال ذلك التهديد اسما حركيا عند التوقيع على الرسالة الا وهو" إليك أمان".

[7]- يقصد بالفيروس: برنامج أو شفرة ذات غرض تعديلي للمعلومات يملك قدرة الالتصاق ببرنامج مؤهل وتكرار نفسه في البرمجيات الأخرى في الحاسوب. ومن النتائج التي تترتب على هذا الفيروس تعديل البرامج والتنقل بواسطتها إلى برامج أخرى، نسخ اوامر بدلا عن اوامر البرنامج، إلحاق أضرار بالغة بالبرامج، تقليل سرعة الحاسب. ومن أخطر الفيروسات المنتشرة عبر شبكة الإنترنت، فيروس "Nimada " وفيروس القمة وفيروس " w32Mytob.u.@.mm أو w32Mytob.x وفيروس RTA. ينظر لمزيد من التفاصيل على التوالي: د/عمر محمد أبو بكر بن يونس، (الجرائم الناشئة.....) مرجع سابق، ص 364. د/عادل عبد الجواد محمد: اجرام الإنترنت، مجلة الامن والحياة، العدد 21، السنة 20، ديسمبر

بالحبس لمدة 5 سنوات و الوضع تحت الرقابة لمدة 3 سنوات مع الإجبار على البقاء بعيدا على الوسائل الإلكترونية و شبكات المعلوماتية. و لقد ظهر هذا التهديد لفترة قصيرة على صفحة موقع " yahoo " على الانترنت خلال شهر ديسمبر سنة 1997.

ولقد كان نص رسالة التهديد كالتالي: " يوم عطلة الميلاد 1997 سيتحرك القسم المتفجر من هذا الفيروس لينشر الفوضى في جميع شبكات العالم سيكون بالإمكان تأمين "مضاد" لهذا الفيروس في حال أطلق سراح "كيفين ميتنيك"[1].

- التهديد بقطع الكهرباء:

حيث هدد خبير كمبيوتر بلجيلكي عن طريق إرساله لرسالة الكترونية عبر موقع البريد الإلكتروني بصحيفة "هيت لانيست نيوز" بكسر شفرة كمبيوتر محولات الكهرباء في بلجيكا يوم الأربعاء 1999/12/29 في الفترة المسائية الممتدة بين 13h 30 إلى 15h30، و قطع الكهرباء على بلجيكا برمتها واصفا إياه بالأمر الهين و السهل[2].

- التهديد بتفجير مؤسسات مالية:

هدد شاب أمريكي يدعى " جاها برج ويل " كل من مدير شركة ميكروسوفت و المدير التنفيذي لشركة MPI بنسف الشركة إذا لم تدفع له مبلغ 5 ملايين دولار أمريكي[3].

إضافة إلى ما سبق ذكره من أشكال الإرهاب الإلكتروني، فان الانترنت ذلك العالم الإفتراضي تقوم بمد الشخص بخبرات ضارة فيما يتعلق بالمعلومات التي تتعلق بالإرهاب، فهي تبين للشخص كيفية الحصول على بعض أنواع المتفجرات من الانترنت مباشرة مثل: C4 و TNT وRDX و NAPALM وExplosive وعلى المتفجرات البلاستيكية، و كذلك كيفية تصنيع الصواريخ البسيطة. بل أكثر من ذلك فهي تقوم بشرح الأساليب المفصلة في كيفية لبس الاحزمة الناسفة و إخفاء الأسلحة وتيسير تهريبها ومن ثم إعادة تركيبها وما تسمى "بعملية التبشيم ". ضف إلى ذلك فهو يشرح أساليب تمويه العبوات و الإسعافات

2000، يناير 2001، ص 81، د/ نعيم مغبغب: مخاطر المعلوماتية والإنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون لمقارن، بدون دار نشر، 1998، ص215 وما بعدها. مقال فيروس القمة يتحكم في الحاسبات عن بعد، لغة العصر، مجلة الاهرام للكمبيوتر والإنترنت و الاتصالات، العدد الثالث والخمسون للسنة الخامسة، ماي 2005، ص 92. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، (امن المعلومات الإلكترونية) مرجع سابق، ص 48 و ما بعدها.

- la cybercriminalité ،www.astrosurf.com

[1]- لمزيد من التفاصيل ينظر د/حسنين المحمدي بوادي، المرجع السابق، ص94.

[2]- ينظر د/حسنين المحمدي بوادي، نفس المرجع ، ص95.

[3]- ينظر د/حسنين المحمدي بوادي، المرجع السابق، ص96.

لمعالجة الإصابات، إضافة لنشر المنشورات و المجلات الإلكترونية التي تمتلئ بها الشبكة مثل: مجلة صوت الجهاد التي لا تزال صفحاتها عالقة رغم محاولات الحجب[1]، **ومن الأمثلة الواقعية عن ذلك:**

– أن فتاة تنتمي إلى إحدى الجماعات المتطرفة تدعى " أنجيلا ناركان" من برلين تحصلت على موقعها الخاص على الانترنت على معلومات مفصلة عن كيفية القيام بعمليات التخريب وكيف يمكن العبث بأسلاك صناديق الإشارات الكهربائية في السكك الحديدية لتعطيل حركة القطارات.[2]

– و في مثال آخر و بالضبط ما حصل في مصر في الآونة الأخيرة أي "حادثة الأزهر"، عندما اهتزت مصر على انفجار قنبلة وضعها طالب في كلية الهندسة، و الذي حصل على معلومات عن كيفية صنع قنبلة من خلال الانترنت[3].

ويسعى الأحداث بشكل خاص إلى الحصول على خبرات ضارة تساهم في زيادة عدوانيتهم من خلال الشبكة، ففي ولاية " أركنساس " الأمريكية انفجرت قنبلة على طفل في العاشرة من عمره و أودت بحياته. وقد تبين أن الطفل كان يحاول تصنيع القنبلة و انه حصل على المعلومات الخاصة بتصنيعها من خلال شبكة الانترنت. وفي هذا تشير الإحصائيات الأمريكية إلى أن نسبة حوادث الوفاة بالقنابل المنزلية قد زادت بمعدل 20 ٪ خلال فترة 1990–1993.كما حذرت الأوساط الأمنية هناك من لجوء بعض مشجعي الرياضة من المشاكسين الى تصنيع العاب نارية وصواريخ لإطلاقها خلال المباريات وذلك بحصولهم على المعلومات من الانترنت تمكنهم من تصنيعها وتطويرها[4].

كذلك فقد حذر خبراء الحاسب الآلي من أن المعلومات الأساسية لتصنيع القنابل الذرية يمكن الحصول عليها بسهولة من خلال شبكة الانترنت[5].

وقد ورد في تقرير بعنوان " مراهقون يحصلون على معلومات نووية " أن المسؤولين في ولاية كاليفورنيا بالولايات المتحدة الأمريكية أفادوا بان مراهقين أحداث وشباب استولوا عبر شبكة الانترنت على آلاف الشفرات الخاصة بالدخول إلى مواقع خاصة وتمكنوا من التسلل إلى شبكات معلوماتية تابعة لمختبرين أمريكيين (مختبر ساندیا و مختبر أرك ريدج) [6] ، يعملان في إطار برنامج الأسلحة النووية[7].

---

[1]– مقال الإنترنت والإرهاب، http:// .news.bbc.co.uk

[2] – خبر منشور في جريدة الاهرام المصرية يوم 1997/8/4، ص10.

[3]– رأفت رضوان: الإنترنت والإرهاب، جريدة الاهرام المسائي، 4/21 /2005، ص 7.

[4]– يستخدم مختبر ساندیا لتصميم كافة المكونات غير نووية للاسلحة النووية الأمريكية في حين انشأ مختبر ارك ريدج عام 1943 لانتاج البلوتنيوم الذي استعمل في انتاج اولى الأسلحة النووية الأمريكية.

[5]– لمزيد من التفاصيل ينظر د/ عبد الفتاح بيومي حجازي، (الاحداث والإنترنت) مرجع سابق، ص 187.

[6]– د/ عبد الفتاح بيومي حجازي،نفس المرجع ، ص 185– 186.

[7]– ينظر مقال المنشور من مركز البحوث والدراسات بشرطة دبي بعنوان: الأمن والإنترنت، http:// www.dubaipolice.gov

هذا وقد حث عضو الكونجرس الأمريكي "ادوارد كيندي " أعضاءه على ضرورة وضع ضوابط حول الاستخدام السيئ للشبكة خاصة فيما يتعلق بالإرهاب والإباحة، وذلك اثر الجلسة الخاصة التي عقدها الكونجرس في "أوكلاهما" لمناقشة العلاقة بين الانترنت و الحادث الإرهابي، حيث استنتج ذلك الأخير نسخة من كتاب يتضمن إرشادات للإرهابيين من شبكة الانترنت[1].

هذا من ومن جهة أخرى، فلقد أتاح برنامج Google earth[2] الشهير الموجود على الانترنت فرصة للإرهابيين لمراقبة العالم عبر الانترنت،حيث أصبح يستغل في مجال الاستخدام العسكري و كشف مناطق أمنية كانت في السابق سرية للغاية. الأمر الذي أثار الرعب في إسرائيل وفقا لتقرير صحفي في صحيفة " يديعوت احرنوت" الإسرائيلية، حينما أشار إلى أن هذا البرنامج المطور الذي يتضمن أرشيفا لصور ملتقطة بالأقمار الصناعية يكشف مواقع عسكرية و أمنية إسرائيلية هامة و بالغة الحساسية، كمقر وزارة الدفاع في تل أبيب وقواعد أساسية تابعة للسلاح الجوي الإسرائيلي والمفاعل النووي السري المثير للجدل في مدينة " ديمونة " بالصحراء الجنوبية.كما تعرف مستخدمو الانترنت على موقع سري آخر ترددت مزاعم انه مقر وكالة الموساد للاستخبارات الإسرائيلية.

وحذرت الصحيفة من أن البرنامج جعل من هذه المواقع أهدافا سهلة محتملة لمن يريد مهاجمتها؛ مضيفة أن جوجل طورت صور الأقمار الصناعية الخاصة بإسرائيل، وضاعفت تقريبا من درجة وضوحها ودقتها خلال الأيام الأخيرة، ووصفت البرنامج بأنه يمثل "نقطة قوة " للدول الأعداء على حد تعبيرها و"كنزا"للفصائل المسلحة. و أشارت الى أن الصور تتكون من بيكسل واحد لكل 10–20 مترا مربعا على الأرض. وفي سياق متصل أظهر تقرير اخباري آخر نشر في جريدة " Daly Telegraph البريطانية" أن المقاومة في العراق تستخدم هذا البرنامج لتنفيذ هجمات ضد المعسكرات البريطانية و الأمريكية. وتجدر الإشارة إلى ان هذه المعلومات لم تأت من فراغ و لكن تم العثور عليها من خلال المستندات المضبوطة أثناء مهاجمة عدد من المنازل التي كان يختبئ فيها المسلحون.

وأشارت الصحيفة استنادا على دوائر استخبارية أن عناصر المقاومة قد استخدمت هذا البرنامج في تحديد المناطق المستهدفة.و يظهر ذلك جليا في الصور الذي تم العثور عليها و التي تظهر محيط مدينة البصرة الجنوبية، و كانت تحتوي على مباني تفصيلية داخل المعسكر البريطاني، بالإضافة إلى أهداف يمكن

---

[1]– عبد الفتاح بيومي حجازي، (الاحداث والإنترنت) مرجع سابق، ص 185

[2] – جعل هذا البرنامج الدول إلى كتاب مفتوح من خلال عرض صور للكرة الارضية وخرائط الدول بتفاصيل دقيقة جدا تصل إلى حد عرض اسماء الشوارع والحواري والأزقة بأسمائها الشعبية احيانا. اي انه سهل من عملية تحديد الاماكن بصورة دقيقة ومتناهية وبسرعة فائقة، فما على مستخدم الإنترنت سوى الضغط على منطقة ذات دلالة معينة، وحينئذ ستنبثق إحدى نوافذ ديسكفري التي تضم روابط لكل ملفات الفيديو ومعلومات الموسوعة حول هذه المنطقة وعرض صور لها بما فيها المناطق العسكرية ايضا. وهي الخدمة التي أحدثت هزة في العالم نتيجة خوضها في المحضور. وكانت شركة جوجل قد طرحت هذا البرنامج بهدف تزويد مستخدميها بمعلومات جغرافية، ومساعدة السائحين والمسافرين على معرفة البلاد التي يتوجهون اليها. مقال الإنترنت يسهل الحروب والعمليات الإرهابية،www.amjad68.jeera.com http://

قصفها مثل الخيام و أماكن الغسيل والمراحيض. كما أن خطوط الطول ودوائر العرض لهذه الأهداف كانت محددة على ظهور الصور .كما أوضح ضابط مخابرات بريطاني في تصريحات أوردتها ذات الجريدة أنهم يستخدمون برنامج Google earth لتحديد أكثر الأهداف سهولة،وان المعسكرات البريطانية في البصرة تتعرض بشكل يومي تقريبا لقذائف الهاون بفضل هذا البرنامج[1].

الفرع الثاني:موقف التشريعات المقارنة من جريمة الإرهاب عبر الانترنت

إن الفكر القانوني يعيش مع أوائل القرن الحادي والعشرين مرحلة انتقالية اتجاه ظاهرة إجرامية عالمية حديثة، جرائم ذكاء بامتياز، عابرة للحدود الوطنية وجرائم تقنية ومصرفية، جماعية وفردية، منظمة مافيوية، ذات مهنية عالية و إعداد جيد ترتكبها جماعات إجرامية منظمة، جماعات إرهابية أو دول عملاقة يسوده إغفال الهوية،السرية والغموض تستعمل الترغيب والترهيب دوافعها زعزعة استقرار البلدان، تجميع الثروات الطائلة وتعزيز نفوذ المنظمات الإجرامية والإرهابية.وسائلها الفضلى لإخفاء عائدات هذه الجرائم، تتم من خلال خرق قوانين النقود المحلية والدولية وبتبييض الأموال مستغلين التغطية التي يؤمنها هذا النظام السري. مع الإشارة إلى أن هذه الجرائم تمارس من طرف أشخاص متمتعين بكامل صحتهم الجسدية، حاملي الشهادات، ميسورين وذوي المكانة الاجتماعية المرموقة، يعتمدون على تكوينهم الذهني ويستمتعون بكامل قواهم العقلية، وليسوا أشخاصا ذوي عيوب خلقية وأولئك البربريين، الأميين، الفقراء، الشاذين عن المجتمع، الذين يشكون من ضعف دماغي أو تشويش عقلي،يستخدمون التكنولوجيا المتطورة للانترنت لتوسيع مسرح عملياتهم الإرهابية. وبالتالي أصبح من الصعب اصطياد هذا الأخطبوط الإلكتروني الجديد.

و في ظل ازدياد خطورة هذا النوع الجديد و الخطير من الإرهاب، أصبح من اللازم على الدول مواجهته ومكافحته وذلك بسن قوانين خاصة إلى جانب قوانينها العقابية علها تتلاءم مع هذا النوع المميز من الإرهاب الإلكتروني. و هذا ما سنبينه في فرعنا هذا من خلال التطرق إلى موقف الدول الغربية ثم العربية. و ذلك كمايلي:

أولا: موقف التشريعات الغربية من جريمة الإرهاب عبر الانترنت.

و سنبين هنا موقف التشريع الفرنسي ثم موقف التشريع الأمريكي من جريمة الإرهاب عبر الانترنت. و ذلك كمايلي:

1/ موقف التشريع الفرنسي من جريمة الإرهاب عبر الانترنت:

عالج المشرع الفرنسي جريمة الإرهاب عبر الانترنت من خلال الفصل الأول من الباب الأول المعنون بالإرهاب في المادة 421-1 من قانون العقوبات الفرنسي الجديد في الفقرة الثانية و الناصة على:" تعد أعمالا ارهابية حين تكون تلك الأعمال ذات علاقة بمشروع فردي أو جماعي يهدف إلى الاخلال بشكل خطير بالنظام العام بالترويع أو بالرعب، الأعمال الإجرامية الآتية:

[1]– مقال الإنترنت يسهل الحروب والعمليات الإرهابية،الموجود على الموقع السابق.

ب- السرقة، الابتزاز، التدمير، التجريد، الاتلاف، و كذلك الجرائم في مجال المعلوماتية حسبما هي معرفة في الكتاب الثالث من هذا القانون "[1]. و الأفعال المقصودة في هذه العبارة الأخيرة هي تلك التي حددتها المادة 323-1 من قانون العقوبات الفرنسي الجديد و التي تتناول العدوان على نظم المعالجة الآلية للمعطيات، و التي تعد أفعالا ارهابية إذا ترتب على ارتكابها إخلالا خطيرا بالنظام العام سواء ارتكبها أشخاص طبيعية أو معنوية.

2/ موقف التشريع الأمريكي من جريمة الإرهاب عبر الانترنت.

أما بالنسبة للتشريع الأمريكي فتغير الوضع في مكافحة و قمع الإرهاب تنظر عن ذي قبل، لاسيما عقب هجمات الحادي عشر من سبتمبر التي شهدتها تلك الأخيرة، إذ تقدم وزير العدل الأمريكي "جو اشكروفت" بمشروع قانون يوسع من سلطات متابعة الإرهابيين ومعاقبتهم، كما انه يكيف التسلل الكمبيوتري بأنه جريمة إرهابية تصل عقوبتها إلى السجن مدى الحياة. كما انه يوسع من صلاحيات الاحتجاز والمصادرة لسلطات التحقيق قبل الإدانة، ويشرك في المسؤولية الجنائية كل من يساعد المتسللين أو يأويهم، حتى ولو كانت الأضرار الناجمة عن الجريمة محدودة الأثر.

وتجدر الإشارة إلى أن هذا الأخير (مشروع القانون) يطبق بأثر رجعي على الجرائم الإرهابية، مما يعني انه سيؤثر على المتسللين ومصممي برامج الفيروس السابقين الذين لم يكن القانون يعاقبهم بأكثر من تحذير أو عقوبة طفيفة[2].

هذا من جهة ومن جهة أخرى، فانه يجب الإشارة بان الرئيس الأمريكي بوش الابن قام بإصدار قرار رئاسي 13231 مؤرخ في 16/ 2001/10 بشأن حماية البنية التحتية الحساسة في عصر المعلومات، والذي تم بموجبه إنشاء مجلس يضم ثلاثين رئيسا لشركات مساهمة مهمته منح الرئيس منشورة حول امن النظام المعلوماتي في الدولة.

ولقد قام المشرع الأمريكي بإصدار قانون جديد، وهو القانون الوطني 2001 المؤرخ في2001/10/26[3]. و الذي كان له تأثير امتد إلى استحداث تعديلات في التشريعات النافذة المفعول على المستوى الفدرالي في الولايات المتحدة التالية:

---

[1]-421-1 : « Constituent des actes de terrorisme، lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur، les infractions suivantes : 1°.....،

2° Les vols، les extorsions، les destructions، dégradations et détériorations، ainsi que les infractions en matière informatique définis par le livre III du présent code،..... »

[2]- لمزيد من التفاصيل ينظر تقرير امريكا: متسللوا إرهابين، news.bbc.co.uk . http://

[3]- سمي هذا القانون بباتريوت اختصارا لتوحيد و تعزيز أمريكا من خلال توفير الأدوات الملائمة المطلوبة لاعتراض وعرقلة الإرهاب، و يكمن الغرض المنشود من هذا القانون في ردع و معاقبة الأعمال الإرهابية في الولايات المتحدة الأمريكية أو حول العالم، لتعزيز أدوات لتحقيق تنفيذ القانون و أغراض أخرى كتعزيز الاجراءات و كشف و ملاحقة غسل الأموال الدولية

Title 18, section 1030.The Computer Fraud and Abuse Act.
Title 18, section 1961. Rico predicate offenses.
Title 18, section 2331. Definition of domestic and international terrorism.
Title 18, section 2510. The Wiretap Statue.
Title 18, section 2702 et seq. The Electronic Communications Privacy Act.
Title 18, section 3056. Secret Service Jurisdiction.
Title 18, section 3177. Definition of Terrorism Offenses.
Title 18, section 3103 (a).Delayed notice warrants.
Title 18, section 3121. The open register and trap and trace statute.
Title 18, section 3286. Statue of limitations for terrorism offenses.
Title 47, section 551. The cable Act.
Federal Prule of criminal procedure 6(e). sharing grand jury information.
Provisions Not Amending United States Code or Federal Rules[1].

ثانيا : موقف التشريعات العربية من جريمة الإرهاب عبر الانترنت.

بعد أن بينا موقف الدول الغربية من جريمة الإرهاب عبر الانترنت، سنحدد هنا موقف الدول العربية من تلك الجريمة[2]، و التي انقسمت بشأنه هذه الدول إلى قسمين. فهناك دول عربية صمتت في معالجة هذا النوع من الإرهاب الالكتروني و الأخطر من نظيره التقليدي، على عكس دول عربية أخرى و التي خصصت لها قوانين تكافحها إلى جانب قوانينها العقابية. و على هذا سنوضح موقف الدول العربية كمايلي:

1/ موقف التشريعات العربية بصفة عامة من جريمة الإرهاب عبر الانترنت

قامت بعض التشريعات بوضع قوانين خاصة في مواجهة جريمة الإرهاب عبر الانترنت. و من هذه التشريعات **التشريع المصري** و الذي جرم الإرهاب عبر الانترنت في المادة 86 مكرر عقوبات مصري من خلال عبارة "بأية وسيلة".[3] و كذا **القانون الاتحادي رقم 6 لسنة 2006** في الإمارات العربية المتحدة

و تمويل الإرهاب. لمزيد من التفاصيل حول مضمون هذا القانون ينظر :USA Patriot Act،www.fincen.gov http://

[1] – د/عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن استخدام الإنترنت) مرجع سابق، ص659.

[2]– لقد نصت المادة 15 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على الجرائم المتعلقة بالإرهاب و المرتكبة بواسطة تقنية النعلومات:

1– نشر أفكار و مبادئ جماعات إرهابية و الدعوة لها.

2– تمويل العمليات الإرهابية و التدريب عليها و تسهيل الإتصالات بين التنظيمات الإرهابية.

3– نشر طرق صناعة المتفجرات و التي تستخدم خاصة في عمليات إرهابية.

4– نشر النعرات و الفتن و الإعتداء على الأديان و المعتقدات."

[3]– تم تعديل للمادة 86 **عقوبات مصري و ذلك باضافة** المادة 86 مكرر و الناصة على:" يعاقب بالسجن كل من انشأ او اسس او نظم او ادار ، على خلاف احكام القانون جميعة او هيئة او منظمة او جماعة او عصابة ، يكون الغرض منها

بشأن مكافحة جرائم تقنية المعلومات حيث جرم ارتكاب هذه الأفعال الخطيرة أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية وذلك في المادة 21 منه.[1] و كذا **المملكة العربية السعودية** و التي خصصت مادة في نظام مكافحة جرائم المعلوماتية لتجريم ذلك النوع من الإرهاب الفريد من نوعه و الخطير، و ذلك في المادة 7 منه.[2]

2/ موقف التشريع الجزائري من جريمة الإرهاب عبر الانترنت.

سارعت الدولة الجزائرية التي عانت الكثير والكثير من ويلات الإرهاب الى مواجهة جريمة الإرهاب عبر الانترنت بوضع القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والمتمم لقانون العقوبات وذلك في المادة 4[3] و التي تسمح باللجوء إلى المراقبة الإلكترونية وذلك في أربع حالات أوردتها على سبيل الحصر من بينها:

–الوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب والجرائم الماسة بأمن الدولة، وفي حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة، أو الدفاع الوطني

الدعوة باية وسيلة إلى تعطيل احكام الدستور او القوانين او منع احدى مؤسسات الدولة او احدى السلطات العامة من ممارسة اعمالها ، او الإعتداء على الحرية الشخصية للمواطن او غيرها من الحريات والحقوق العامة التى كلفها الدستور والقانون ، او الاضرار بالوحدة الوطنية او السلام الاجتماعى ويعاقب بالاشغال الشاقة المؤقتة كل من تولى زعامة او قيادة ما فيها او امدها بمعونات مادية او مالية مع علمة بالغرض الذى تدعوا اليه."

[1]– تنص المادة 21 من القانون الاتحادي رقم 6 لسنة 2006 على: " كل من انشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعات إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها أو ترويج أفكارها، يعاقب بالحبس مدة لا تزيد على خمس سنوات ".

[2]– تنص المادة 7 من نظام مكافحة جرائم المعلوماتية على: " يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال،أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1)– إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو احد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو أيا من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أداة تستخدم في الأعمال الإرهابية.

2)– الدخول غير مشروع إلى موقع إلكتروني أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو احد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني."

[3]– تنص المادة 4 في فقرتها (أ) و (ب) من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والمتمم لقانون العقوبات على:" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:

أ– للوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب و الجرائم الماسة بأمن الدولة؛

ب– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدولة أو الدفاع الوطني أو النظام العام."

أو النظام العام. و كذا من خلال المادة87 مكرر 4 من قانون العقوبات الجزائري[1] و التي تجرم فعل تشييد الأفعال المذكورة في المادة 87 مكرر أو التشجيع على ارتكابها أو تمويلها بأية وسيلة كانت. و على هذا فعبارة أية وسيلة كانت تتسع لتضم شبكة الانترنت فكل من اقترف عمدا هذه الأفعال و كانت عبر الانترنت يعاقب بعقوبة السجن المؤقت من 5 سنوات إلى 10 سنوات و بغرامة مالية من 100.000 دج إلى 500.000 دج. و كذا من خلال المادة 394 مكرر3 من قانون العقوبات الجزائري إذ شدد المشرع الجزائري العقوبات إذا إستهدفت هذه الجرائم المعلوماتية الدفاع الوطني أو الهيئات و المؤسسات المتعلقة بالقانون العام .[2] كما نص في المادة 394 مكرر2 في فقرتها الثانية[3] على أنه يعاقب كل من بحث أو جمع أو وفر أو نشر أو حاز أو إستعمل معطيات مخزنة لأي غرض كان و ليكن في هذه الحالة نشر الفكر التطرفي الإرهابي.

---

[1]– تنص المادة 87 مكرر4 على:" يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات و بغرامة مالية من 100.000 دج إلى 500.000 دج، كل من يشيد بالأفعال المذكورة في المادة 87 مكرر أعلاه أو يشجعها أو يمولها بأية وسيلة كانت".

[2]– تنص المادة 394 مكرر3 من قانون العقوبات الجزائري على: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضع للقانون العام، دون الاخلال بتطبيق عقوبات أشد".

[3]– تنص في المادة 394 مكرر2 في فقرتها الثانية على:"يعاقب بالحبس من شهرين (2) إلى ثلاث(3) سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا أو عن طريق الغش بما يأتي:

2– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

الفصل الثاني:

التجسس عبر الإنترنت

تعد عمليات التجسس من العمليات القديمة قدم البشرية و قدم النزاعات البشرية، فمنذ تقدم العصور كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم و الخطط التي يعدونها لمهاجمته. و لهذا كان للتجسس أهمية كبيرة على كافة مستويات النزاعات الإنسانية التي مر بها البشر منذ بدء الخليقة. و قد تطورت عمليات التجسس طبقا لما يسود المجتمع من تطورات علمية و تكنولوجية. فمثلا اخترع الإنسان جهاز الرادار ليتجسس على أعدائه و معرفة تحركاتهم، ثم حدث تطور كبير ألا و هو اختراع الأقمار الصناعية[1] التي تقوم بتصوير الإنسان و الآلات الحربية و المدنية و المباني و كل ما هو فوق الأرض يتم تصويره كل فترة زمنية معينة لمعرفة التحركات التي تتم. كما طورت الولايات المتحدة الأمريكية طائرات للتجسس بدون طيار[2]. و الآن و في ظل التطور التقني الهائل الذي نعيشه فقد أصبح هناك ما يعرف بالتجسس الإلكتروني[3] خاصة ذلك الذي يتم عبر الإنترنت.

---

[1]– حيث قاموا بتطوير جيل جديد من أقمار التجسس. وفي هذا تؤكد بعض المصادر أن ثلاثة أقمار من طراز "كيهول" موضوعة في مدار فضائي حاليا و تستطيع التقاط صور عن الأرض لا تتجاوز قياساتها 15 سم أي ما يكفي للتمييز بين شاحنة و دبابة، بالإضافة إلى أنه توجد أقمار من طراز "لاكروس" تستعمل تقنية التصوير المعروفة بـ: "رادار الفتحة التركيبية " SynthenticApertineتبث موجات صفرية باتجاه الأرض ثم تلتقط انعكاساتها المرتدة إلى القمر. و يمكن تحليل هذه الصور الرادارية بواسطة برامج كمبيوتر خاصة لتحويلها إلى صورة مفهومها و الميزة الرئيسية لهذه التقنية هي أنها تسمح بتخطي الغيوم و الأمطار و الغبار و أنها تصلح للاستعمال أثناء الليل. د/ عفيفي كامل عفيفي، المرجع السابق، الهامش رقم 04، ص306.

[2]– إذ حدث ذلك بعد حادثة سقوط إحدى طائراتها فوق الإتحاد السوفياتي –سابقا– "لوكهيد" و أسر طيارها لمدة سنتين قبل أن يتم تبادله مع جاسوس سوفياتي كان مسجونا في الولايات المتحدة الأمريكية. و كانت أولى الطائرات الأمريكية دون طيار هي Tagoard و كانت تتم الملاحقة فيها بواسطة برنامج كمبيوتري حددت فيه مساراتها الجوية ذهابا و إيابا و كانت الطائرات تقوم بتصوير المناطق و في نهاية المهمة يتم إلقاء آلة التصوير و الصور و نظام التوجيه في مكان محدد بواسطة مظلة ليلتقطها الفريق المشرف على العملية في حين بتم تدمير بقية الطائرة بصورة ذاتية. إلا أن استخدام هذه الطائرات لم يحقق النجاح المطلوب، الأمر الذي دفع الولايات المتحدة إلى صنع طائرات صغيرة و اقتصادية دون أطقم قيادة و ذلك منذ العقد الثامن من هذا القرن. و قد استخدمت إسرائيل هذه الطائرات أثناء عملياتها في لبنان في العام 1982. و تعد الطائرة "داركستان" Darkstan من النماذج الشديدة التعقيد وهي مصنوعة وفق هندسة الطائرات الخفية Stealth air التي تمتص الموجات الرادارية. و بالتالي تحول دون أن تكتشفها الرادارات العادية، و تتم عملية الملاحة في هذه الطائرات بواسطة برنامج كمبيوتري خاص. كما تستخدم الولايات المتحدة الآن لأعمال الاستصلاح في أجواء البوسنة طائرة تعمل ذاتيا دون طيار من طراز "بريداتيور" Predatar. و هذه الطائرة تحلق على ارتفاع 4/5 كلم و تلتقط صورا رادارية حتى حجم 30كلم. و لا تتأثر بالظروف المناخية مثل الغيوم و الظلام، و تستطيع كذلك أن تعمل لمدة 24 ساعة بصورة متواصلة، د/ عفيفي كامل عفيفي، نفس المرجع ، نفس الهامش ، ص306–307.

[3]– منير محمد الجنيهي، ممدوح محمد الجنيهي، (جرائم الإنترنت و الحاسب الآلي) مرجع سابق، ص86–87.

وعليه سيتم التعرض لهذه الجريمة المستحدثة المهددة لأمن الدولة وفقا للمبحثين التاليين:

المبحث الأول: الأحكام العامة للتجسس.

المبحث الثاني: ماهية التجسس عبر الإنترنت.

المبحث الأول:

الأحكام العامة للتجسس .

تعد جرائم التجسس من أهم الجرائم التي تقع على كيان الدولة و أكثرها خطرا و أفدحها ضررا، إذ تشكل اعتداء مباشرا ومؤثرا على الوجود السياسي للدولة. وهي تعتبر أحد الأنواع و السبل الملتوية في الحروب القديمة و الحديثة.و السؤال الذي يطرح هنا: هو ماذا نعني بالتجسس؟ و ما هي الطبيعة القانونية لمثل هذه الجريمة ؟و ما هي أنواعه؟... أسئلة سيتم الإجابة عنها وفقا للمطلبين التاليين كالآتي:

المطلب الأول: ماهية التجسس.

المطلب الثاني: الفرق بين التجسس و الخيانة.

المطلب الأول:

ماهية التجسس.

نتناول في هذا المطلب تعريف جريمة التجسس و كذا تطورها التاريخي،كما نبين طبيعتها القانونية و نحدد أنواعها. و هذا في الفرعين التاليين:

الفرع الأول: تعريف التجسس و تطوره التاريخي

الفرع الثاني: الطبيعة القانونية للتجسس و أنواعه.

الفرع الأول: تعريف التجسس و تطوره التاريخي.

و لقد خصصنا هذا الفرع لتعريف جريمة التجسس لغة ثم فقها فقانونا، لنعرج بعد ذلك إلى تبيان تطوره التاريخي. و ذلك كمايلي:

أولا: تعريف التجسس.

1/ لغة: جس و تجسس و اجتس الأخبار و الأمور، بحث عنها و فحصها.

و الجسيس جمعه أجسة و الجاسوس جمع جواسيس. و الجساس: الذي يتجسس الأخبار ثم يأتي بها. والجاسوسية هي مهنة الجاسوس[1].

[1]– قاموس المنجد في اللغة والإعلام، مرجع سابق، ص90.

2/ فقها: يبدو من العسير وضع تعريف جامع شامل للتجسس بسبب تعدد أفعال التجسس واختلافها مما يحول دون وضعها جميعاً في قالب واحد، إذ تشكل كل حالة جريمة خاصة ومميزة عن سواها. و لهذا لم يتفق الفقهاء حول تعريف واحد لجريمة التجسس، بل انقسموا في ذلك إلى ثلاث اتجاهات رئيسية و ذلك بحسب تطور المراحل الزمنية التي مرت بها ظاهرة التجسس و ذلك على النحو التالي:

الاتجاه الأول: التعريف القديم للتجسس.

و يقوم على أساس من الأفكار السائدة في القانون الدولي و القانون العسكري في مرحلة ما قبل نشوب الحرب العالمية الأولى. حيث يعرف أصحاب هذا الاتجاه التجسس بأنه: "البحث عن أي نوع من المعلومات، خفية عن دولة معينة بهدف إيصالها لدولة أجنبية و ذلك بنية الإضرار بالدولة المتجسس عليها"[1].أو بأنه: "يتمثل في العمل خفية أو تنكرا أو تحت حجج مزيفة لجمع الوثائق أو المعلومات السرية حول الموارد العسكرية، التنظيم الهجومي أو الدفاعي و الوضع العسكري و الاقتصادي، أو البحث عنها بنية تسليمها إلى حكومة أخرى مجانا أو بمقابل"[2].

الاتجاه الثاني: التعريف التقليدي للتجسس.

وعلى عكس الاتجاه الأول يقوم هذا الاتجاه على أساس مراعاة الخصائص الذاتية للقانون الجنائي و التي تميزه عن غيره من فروع القانون. و عليه يعرف التجسس وفقهم بأنه:"فعل إعطاء أو الحصول أو نشرأو البحث عن الأشياء أو مكتوبات أو وثائق أو معلومات سرية عن الوضع العسكري، الدبلوماسي، الاقتصادي التي تهم الدفاع الوطني أو الأمن الخارجي للدولة بقصد إيصالها إلى شخص ليست له صفة أو إلى عميل دولة أجنبية"[3]، و يكون متهما بالتجسس كل شخص، الذي بعد أن يتعرف أو يتحصل على أشياء، وثائق، بيانات سرية تهم الدفاع الوطني، و كذلك التنظيمات و الاكتشافات الصناعية أو خطط التعبئة الاقتصادية و الصناعية للبلاد، يقوم بإعطائها أو توصيلها أو إفشائها، سواء بهدف الربح أو لأي هدف آخر، لأي عميل لجهة أجنبية، أو لأي شخص له حق التعرف عليها"[4]. أو بأنه "نقل أو إفشاء خبر أو أي أمر من الأمور التي تعتبر سرا من أسرار الجمهورية العراقية و كان من شأن ذلك الإضرار بالمصلحة الوطنية و القومية للقطر العراقي و الأمن العربية إلى جهة خارجية أو داخلية، سواء كان ذلك لقاء منفعة أو بدونها"[5].

---

[1]– لقد تم نقد هذا التعريف من عدة وجوه لمزيد من التفاصيل ينظر، د/محمود سليمان موسى، المرجع السابق، ص92 و ما بعدها.

[2]– و هو كالتعريف الأول قد انتقد لمزيد من التفاصيل حول النقد ينظر، د/ محمود سليمان موسى، نفس المرجع، ص95 وما بعدها.

[3]– ينظر نقد هذا التعريف د/ محمود سليمان موسى، نفس المرجع، ص100–101.

[4]– ينظر د/ محمود سليمان موسى، المرجع السابق، ص102–103.

[5]– سعد الأعظمي: التجسس في التشريع العراقي، دار الكتب للطباعة و النشر، الموصل، 1981، ص19.

الاتجاه الثالث:التعريف الحديث للتجسس.

و على عكس الاتجاهين السابقين اتجه أصحاب هذا الاتجاه إلى تعريف التجسس من خلال الإحاطة بجوانبه المتعددة في ضوء التطورات التي لحقت التشريع الجنائي حول تحديد مضمون التجسس.و عليه فيعرف التجسس وفقا لهذا الاتجاه بأنه "كل نشاط يقوم به أجنبي و يؤدي إلى وقوع ضرر بأحد المقومات الأساسية لوجود الدولة، و ذلك بقصد تحقيق مصلحة جهة أجنبية"[1].

3/ قانونا: القاعدة العامة في معظم التشريعات الجنائية[2]، تتمثل في عدم وجود تعريف للتجسس، إذ تركت تلك المهمة للقضاء و الفقه اعتمادا على أن التجسس ذو طبيعة متجددة و متغيرة و متشعبة.

---

[1]– إن أهم التعريفات التي تدخل في هذا الصدد هي تعريف بيير هوغني و كلود ديفيس و ريمون جوليه لمزيد من التفاصيل ينظر د/ محمود سليمان موسى، المرجع السابق، ص 108 و ما بعدها. و كذا عثمان بن علي بن صالح: جريمة التجسس و عقوبتها في الشريعة الاسلامية و القانون الوضعي، رسالة ماجستير، تخصص التشريع الجنائي الاسلامي، جامعة نايف العربية للعلوم الامنية، الرياض، 2006، ص20.

[2]– فمثلا لم يتطرق المشرع الفرنسي بصورة مباشرة للتعريف بالتجسس، و ذلك خشية أن يؤدي ذلك إلى عدم خضوع صور أو أفعال تجسسية جديدة لمثل هذا التعريف، إن هي لم تتطابق مع مؤدى ذلك التعريف و مواصفاته. و لكنه ترك أمر ذلك للقضاء و الفقه لكونهما أكثر قدرة على مواكبة التطورات و التغيرات التي تستجد في هذا المجال. غير أن المشرع الفرنسي مع ذلك قد وضع مبادئ أساسية يمكن أن تساهم في تشكيل تعريف التجسس، وتساعد القضاء و الفقه في معرفة أو تحديد المضمون القانوني له، و ذلك من خلال المواد من 1–411 إلى غاية 11–411 من قانون العقوبات الفرنسي. و هو الشأن ذاته بالنسبة للتشريع الجزائري و التشريعات الجنائية العربية فلقد نص ذلك الأخير على تلك الجريمة في المادة 64 عقوبات جزائري و ذلك كالآتي: "يرتكب جريمة التجسس و يعاقب بالإعدام كل أجنبي يقوم بأحد الأفعال المنصوص عليها في الفقرات 2 و 3 و 4 من المادة 61 و في المادتين 62 و 63. و يعاقب من يحرض على ارتكاب إحدى الجنايات المنصوص عليها في هذه المادة و المواد 61 و 62 و 63 أو يعرض ارتكابها بالعقوبة المقررة للجناية ذاتها". وتنص المادة 61 في فقراتها 2 و 3 و 4 على:".....

2/ القيام بالتخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر أو تقديم الوسائل اللازمة لذلك سواء بتسهيل دخول القوات الأجنبية إلى الأرض الجزائرية أو بزعزعة ولاء القوات البرية أو البحرية أو الجوية أو بأية طريقة أخرى.

3/ تسليم قوات جزائرية أو أرض أو مدن أو حصون أو منشآت أو مراكز أو مخازن أو مستودعات حربية أو عتاد أو ذخائر أو مبان أو سفن أو مركبات للملاحة الجوية مملوكة للجزائر أو مخصصة للدفاع عنها إلى دولة أجنبية أو إلى عملائها.

4/ إتلاف أو إفساد سفينة أو سفن أو مركبات للملاحة الجوية أو عتاد أو مؤن أو مبان أو إنشاءات من أي نوع كانت و ذلك بقصد الإضرار بالدفاع الوطني أو إدخال عيوب عليها أو التسبب في وقوع حادث و ذلك تحقيقا لنفس القصد.

أما المادة 62 فنصت في فقراتها على:".....

2/ القيام بالتخابر مع دولة أجنبية أو مع أحد عملائها بقصد معاونة هذه الدولة في خططها ضد الجزائر.

3/ عرقلة مرور العتاد الحربي.

4/ المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو للأمة يكون الغرض منه الإضرار بالدفاع الوطني مع علمه بذلك.

أما المادة 63 فنصت في فقراتها على:

وعليه يمكن تعريف التجسس بأنه جناية يقوم بها شخص أجنبي تتمثل في سلسلة من الأفعال و التصرفات التي تستهدف المساس بسلامة التراب و الإضرار بمصالح الدفاع الوطني[1].

ثانيا: تطوره التاريخي و أهميته:

1/ تطوره التاريخي:

إن ظاهرة التجسس ليست بظاهرة حديثة، بل هي ظاهرة قديمة قدم البشرية نشأت مع نشأة أولى المجتمعات البشرية و أيا كانت صورة هذا المجتمع، أسرة، عشيرة، قبيلة، قرية، مدينة...إلخ. إذ أنه منذ أن وجد الإنسان وجدت معه الحرب كوسيلة من وسائل الدفاع عن النفس، أمام هجمات الأعداء والطامعين، و منها استخدام الأسلحة المتوافرة و وسائل القتال المعروفة عند كل أمة من الأمم[2]. و نشأ بهذا التجسس. إذ أن كل تجمع بشري يسعى جاهدا لمعرفة ما لدى غيره من التجمعات الأخرى من أسرار أو معلومات. و قد ارتبطت هذه الظاهرة في الماضي البعيد بالقدرات الخارقة للآلهة و الأساطير، و كانت الوسيلة الأولى للحصول على المعلومات في هذا الزمن تتمثل في اللجوء إلى العرافين و الكمان و السحرة باعتبارهم وسطاء بين الشر و بين الآلهة، حيث يكون لهؤلاء حق معرفة نوايا و رغبات الآلهة و ما سيحدث فيما يتعلق بمصائر البشر، و غالبا ما يتم ذلك عن طريق الوحي أو الإلهام أو التنجيم أو الأحلام.ثم أخذ

2/ الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها.

3/ إتلاف مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد معونة دولة أجنبية أو ترك الغير يتلفها.

و على خلاف معظم التشريعات الجنائية، أورد قانون العقوبات في الاتحاد السوفياتي السابق، تعريفا للتجسس في المادة 58 منه و التي تقضي بأن التجسس: "يشمل كل فعل من أفعال تسليم أسرار الدولة التي يجب أن تبقى محجوبة أو متكتم عليها أو اختلاسها أو جمعها بقصد تسليمها إلى الدول الأجنبية أو المنظمات المناوئة للثورة أو الأشخاص العاديين و يعاقب على هذه الأفعال بالحرمان من الحرية منذ ثلاث سنوات على الأقل و بمصادرة الأموال كلها أو بعضها، و إذا نجم عن الفعل أو كان يمكن أن ينجم عنه نتائج خطيرة للغاية تؤذي مصالح الاتحاد السوفياتي، فإن العقوبة تبلغ حد أقصى تدبير للدفاع الاجتماعي، وهو الإعدام أو وصم الجاني بالصفة الشائنة "عدو الشغيلة"، والحكم بحرمانه من أن يكون مواطنا في جمهورية الاتحاد السوفياتي، وإبعاده نهائيا من إقليم الاتحاد، ومصادرة أمواله." أما في التشريع الدولي فقد وضعت المادة 29 من الاتفاق الدولي المعقود في لاهاي في 18 أكتوبر 1907 والمتضمن قوانين الحرب البرية وأعرافها تعريفا صريحا للتجسس إذ جاء فيها مايلي: "لا يجوز أن يعتبر جاسوسا إلا ذلك الذي يعمل في الخفاء، أو يتنكر، مستقصيا أو محاولا استقصاء المعلومات، في منطقة العمليات الحربية التابعة لأحد الفريقين المتحاربين، بقصد نقلها إلى الفريق الآخر". كما عرفت المادة 46 من بروتوكول 1977 الملحق لاتفاقية جنيف لعام 1949 الجاسوس بأنه ذلك الذي يجمع او يحاول جمع معلومات ذات قيمة عسكرية، في الخفاء أو باستعمال الغش.

ينظر على التوالي: د/ محمد صبحي نجم، المرجع السابق، ص 192، د/محمود سليمان موسى، المرجع السابق، الهامش رقم 02، ص117 . و كذا د/ محمد الفاضل، المرجع السابق، ص 296 و ما بعدها.

Jean LARGUIER ; droit pénal spécial, 8ème éd, cujas,1994, p225

[1]- ابتسام القزام، المرجع السابق، ص 122.

[2]- محمد راكان الدغمي: التجسس وأحكامه في الشريعة الإسلامية، الطبعة2، دار السلامة، بيروت، 1985، ص47.

التجسس بعد ذلك طابعا أكثر واقعية، فلم يعد مرتبطا بإرادة الآلهة أو الأرواح و لكنه ارتبط بقوة و مشيئة الحكام و الغزاة، و إرادة المحافظة على الجماعة السياسية تحت سلطان الملك. و قد عرفه كل من الفراعنة والبابليين واليهود والرومان والإغريق والقرطاجيين وغيرهم من شعوب العصور القديمة.[1]

2/ أهمية التجسس:

يمثل التجسس أهمية بالغة بالنسبة لكافة الدول في مختلف العصور، و قد تصل هذه الأهمية إلى درجة الضرورة خاصة إذا تعلق الأمر بحماية المصالح الأساسية للدولة أو بحقها في سلامة وجودها السياسي أو كيانها الوطني، و لذلك فهو يشكل نشاطا محتوما يجب القيام به. و من هنا تحرص كل دولة على ممارسة التجسس على غيرها من الدول الأخرى و تبيح لنفسها هذا النشاط. إلا أن هذه الدولة لا تجيز لغيرها من الدول حق ممارسة التجسس على مصالحها الوطنية، بل إنها تقاوم مثل هذا النشاط و تعاقب عليه بأشد ما يمكن من عقاب.[2]

الفرع الثاني: طبيعة التجسس القانونية و أنواعه.

وسنحدد في هذا الفرع الطبيعة القانونية للتجسس بداية، ثم نعرض أنواعه. و ذلك كمايلي:

أولا: طبيعة التجسس القانونية:

يعتبر التكييف القانوني للتجسس من أهم المسائل التي انشغل بها الفقه و القضاء و التشريع منذ القديم. إذ كان هذا الأخير يدخل في إطار الجرائم الماسة بالعظمة و الجلالة الملكية في ظل القانون القديم، أي أنها تصنف كجريمة من الجرائم السياسية الخطيرة. إلا أنه و في ظل النظام الجديد، حيث أصبح للدولة شخصيتها المستقلة و المنفصلة عن شخصية حكامها، اختلف هؤلاء حول طبيعتها القانونية. إذ اعتبرها البعض منهم بأنها جرائم ذات طبيعة سياسية مما يعطي مرتكبيها حق التمتع و الاستفادة بمزايا و حقوق المجرمين السياسيين.[3] غير أن هناك من ينتقد –و بشدة– هذا التكييف، و يجرد جرائم التجسس من أي طابع سياسي، و يعتبرها مثل أي جريمة عادية كالقتل و السرقة و خيانة الأمانة. و هذا ما يقتضي أن يعامل مرتكبيها معاملة المجرمين العاديين.[4] بل هناك من يرى بأن جرائم التجسس ليست بجرائم سياسية ولا عادية و إنما هي جرائم ذات طابع خاص تتكون من أفعال أكثر ضررا و خطرا تقع على الأمة في مجموعها. و لهذا يجب معاملة فاعلها أقسى معاملة و أعنفها مع تطبيق قواعد و أحكام استثنائية.[5]

---

[1]– لمزيد من التفاصيل ينظر كلا من د/ محمود سليمان موسى، المرجع السابق، ص 20 و ما بعدها و محمد راكان الدغمي، المرجع السابق، ص 47 و ما بعدها.

[2]– ينظر محمد راكان الدغمي، نفس المرجع، ص 32 و ما بعدها.

[3]– كالتشريع الفرنسي و كذا الجزائري، لمزيد من التفاصيل ينظر د/ محمود سليمان موسى، المرجع السابق، ص 149 و ما بعدها.

[4]– كالتشريع الليبي و السوري، لمزيد من التفاصيل ينظر د/ محمود سليمان موسى، المرجع السابق، ص175.

[5]– لمزيد من التفاصيل ينظر د/ محمود سليمان موسى، نفس المرجع، ص177.

ثانيا: أنواع التجسس.

تتعدد أنواع التجسس حسب طبيعة المعلومات التي تكون محل هذه الجريمة إلى:

1/ التجسس العسكري: و يهدف إلى الكشف عن أسرار الدفاع و الحصول على الخطط الحربية و معرفة أصناف الأسلحة و مقاديرها، و نظم التعبئة العامة، و عدد أفراد القوات المسلحة و ترتيباتها و تنظيماتها وتحركاتها. [1]

2/ التجسس السياسي: و يرمي إلى استطلاع مواقف زعماء البلاد و قادتها السياسيين و اتجاهاتهم ومبادئهم و آرائهم و تقدير القوى المعنوية أو الخلقية في الأمة، و مواطن الضعف و القوة في أبنائها، وعوامل الفرقة و الاتحاد بين الأحزاب و المنظمات و الطبقات و شتى الهيئات الرسمية و الخاصة، و طاقة جميع هؤلاء في مجالدة العدو و مقاومته.[2]

3/ التجسس الاقتصادي أو التجاري: تعتبر المعلومات الاقتصادية إحدى أهم الدعائم التي تستند عليها الدول في العصر الحديث. ذلك لأن الاقتصاد في يومنا هذا هو القوة و أساس حركة الدول و الحكومات. و عليه فإن التجسس عليها يقصد به الوقوف على حقيقة موارد البلاد و ثرواتها و حالة تموينها، و تجارتها الخارجية، و سلامة وضعها المالي و النقدي.

وتجدر الإشارة إلى أن هذا النوع من التجسس كان صانعا لأحداث التاريخ الاقتصادي للعالم، و كان هو الدافع و الحافز للتوسع الاستعماري و اقتسام العالم جغرافيا و سياسيا و اقتصاديا، و كان هو الوجهة نحو قيام الكتل الضخمة و إعادة هيكلة النظام الدولي من جديد. [3]

هذا من جهة و من جهة أخرى، فإن التجسس الاقتصادي لا يعتبر حكرا على الدول أو الحكومات، بل يمارس كذلك عن طريق الشركات أو المنظمات أو المؤسسات. و التي تقوم به علنا و دون أدنى محاولة من جانبها لإخفاء ذلك، و مثال ذلك أنشطة التجسس التي مارستها الحكومة الفرنسية ضد شركة (أ.ب.م).

و لقد أجري في عام 1996 استفتاء بين مسؤولية الأمن الصناعي في الشركات الأمريكية أظهر أن كثيرا من الدول قد حصلت بشكل غير مشروع على معلومات سرية عن أنشطة تجارية و صناعية في الولايات المتحدة. و تم ترتيب هذه الدول وفقا لحجم الانتهاكات على النحو التالي: الصين، كندا، فرنسا، الهند، اليابان، ألمانيا، كوريا الجنوبية، كومنولث الدول المستقلة (الاتحاد السوفياتي سابقا)، تايوان، المملكة المتحدة، إسرائيل، المكسيك، باكستان، سنغافورة، هونج كونج.

ومن بين الأساليب والوسائل التي أصبحت تستخدم بكثرة الآن في التجسس التجاري الدولي:

-إغراء بعض من لديهم المعلومات على البوح بها (سواء بمقابل أو بدون).

---

[1]- ينظر د/ نادر عبد العزيز شافي: جرائم التجسس، مجلة الجيش، العدد230، سبتمبر 2004، http:// lebany.gov.lb.

[2]- ينظر د/ محمد الفاضل، المرجع السابق، ص 294.

[3]- ينظر د/محمد الفاضل،نفس المرجع ، ص 254 و 255.

-الاستفادة من الشراكة التجارية بين الدول ومن الابحاث المشتركة، أو بشراء بعض المكونات الحساسة من الشركات الصانعة لها.

-استثارة النزاعات الدينية أو العرقية أو المذهبية أو السياسية للموظفين للحصول منهم على المعلومات سواء بالترغيب أو بالترهيب.

-استخدام أساليب أبحاث التسويق لجمع المعلومات عن المنافسين و استخدام الاستمارات التي يقوم بملئها طالبو الوظائف أو إخفاء بعض الأسئلة غير البريئة ضمن الاستبيانات.

-جمع المعلومات الاستخبارية من المعارض العامة و المؤتمرات و الرحلات السياحية و النوادي والمطاعم.

-شراء المعلومات من الأفراد، بما في ذلك سماسرة المعلومات الذين يتكسبون من التجسس و بيع المعلومات.

-استضافة الزوار الأجانب في دول أخرى و الحصول منهم على المعلومات المطلوبة في مقابل إكرام وفادتهم و تمويل زيارتهم لهذه الدولة و تجولهم فيها.[1]

4/ التجسس الصناعي و العلمي: تعتبر فكرة التجسس الصناعي فكرة حديثة و يقصد به كل إلمام بأسرار صناعات البلاد و كل إطلاع على المعلومات و الأبحاث و الدراسات المتصلة بالاختراعات العلمية أو الابتكارات الصناعية. [2]

و تجدر الإشارة إلى أن تحديد مضمون هذا النوع من التجسس ليس دائما بالأمر السهل، إذ توجد صور أخرى للتجسس غالبا ما تؤثر فيه أو تتأثر به، كالتجسس العسكري عندما يتعلق بصناعة أو اكتشافات حربية، و كالتجسس الاستراتيجي أو السياسي الاقتصادي الذي يمارس بهدف الإضرار بالمصالح الوطنية.[3]

5/ التجسس الديبلوماسي: و هو التجسس الذي يمارسه أفراد البعثات الديبلوماسية و يتمثل في جمع المعلومات بطريقة غير قانونية من دون أن يخفي القائمون به صفتهم الديبلوماسية، و هو يصنف ضمن التجسس في السلم. [4]

المطلب الثاني:

الفرق بين التجسس و الخيانة

سنتعرض في هذا المطلب إلى تبيان الفروق الموجودة بين جريمتي التجسس و الخيانة[5]، ولكنه و قبل تفصيل ذلك يجب الاشارة إلى أن هاتين الجريمتين تشتركان في كونهما من الجرائم الماسة بأمن الدولة الخارجي.و لكنهما في المقابل يختلفان في نقاط عديدة ثار الخلاف فيها حول ضابط التفرقة بينهما.

---

[1]- ينظر حسن طاهر داود، المرجع السابق، ص 65 و 66.

[2]- ينظر حسن طاهر داود، نفس المرجع، ص 61.

[3]- ينظر كلا من د/ محمد الفاضل، المرجع السابق، الموضع السابق، و د/ محمود سليمان موسى، المرجع السابق، ص 259.

[4]- ينظر د/ نادر عبد العزيز شافي، المرجع السابق، http:// lebany.gov.lb.

[5]- نعني بالخيانة التسليم فهي تتم غالبا بعمل من أعمال التسليم. إذ يقوم الجاني بتسليم الغير أو العدو شيء أو معلومات أو أسرار تتعلق بأمن و سيادة و استقلال الدولة. ينظر د/ محمد صبحي نجم، المرجع السابق، ص 191 .

و قد ذهبت في تحديد ذلك ثلاث مذاهب مختلفة و هي:

المذهب الموضوعي

المذهب الذاتي

معيار الجنسية، و التي سنتطرق اليها في الفروع التالية:

الفرع الأول: المذهب الموضوعي

و قد اشتق أنصارها معيار التفريق بين الخيانة و التجسس من طبيعة الفعل المقترف أي طبيعة الركن المادي للجريمة المرتكبة. فالخائن حسب رأيهم هو من يسلم ما في يديه من الأسرار إلى دولة أجنبية. و أما الجاسوس فهو من يسعى للحصول على ما ليس في حيازته من الأسرار. فعمل الأول التسليم، و عمل الثاني البحث و التنقيب و هذا أقل خطورة و أذى من الأول[1].

نقد هذا المذهب:

لقد أخذ أصحاب هذا المذهب بمعيار متموج و غير دقيق، و لا يثبت أمام وقائع السلوك الإجرامي وحقائق الحياة، فقد يسعى أحد الأشخاص للبحث عن الأسرار و استقصائها، ثم يقوم هو ذاته– بعد الحصول عليها – بتسليمها إلى دولة أجنبية، فماذا نعتبره و قد قام هو نفسه بالفعلين معا، فعل الاستقصاء+ فعل التسليم في آن واحد؟.[2]

الفرع الثاني:المذهب الذاتي.

و يبني أصحابه معيار التفريق على أساس الدافع أي العلة التي تحمل الفاعل على الفعل أو الغاية القصوى التي يتوخاها. فإذا ثبت أن الفاعل كان يهدف من وراء اقترافه الجرم إلى الإعتداء على سلامة الدولة و أمنها، أو تهديم كيانها، أو الانتقاص من استقلالها كمن يتصل بالدول الأجنبية رغبة في استعدائها على وطنه، فهو خائن و فعله خيانة. أما إذا لم تكن نفسية الفاعل تنطوي حين اقترافه الجرم على نية الغدر بالوطن، كأن يرتكب الفعل بدافع الطيش أو الخفة أو الجشع المادي فهو جاسوس و فعله تجسس.

وتجدر الإشارة إلى أن هذا المعيار في نظر أهل الفقه، يتصف بالعدل و الإنصاف لأنه من البداهة بمكان كبير أن يعاقب من يسعى إلى زج بلاده في أتون حرب قد تكون،ما حقه بأشد مما يعاقب به من يتجر بالأسرار طعما بالدراهم و الدينار.[3]

نقد هذا المذهب:

لم يسلم هذا المذهب هو الآخر من النقد بالرغم من المزايا التي يتصف بها، لأن تطبيقه يستلزم سبرغور النفوس و البحث عن دوافعها و اكتناف خفاياها، و يتطلب الدخول في تحليل ظروف كل فاعل أو شريك والبحث في نواياه و ملابسات جريمته، و هذا مطلب عسير و قد يبدو في بعض الأحيان مستحيلا. و قد لا

---

[1]– ينظر د/ محمد صبحي نجم، المرجع السابق، الموضع السابق.

[2]– لمزيد من التفاصيل ينظر د/محمد الفاضل، المرجع السابق، ص 317 و 318.

[3]– ينظر د/ محمد الفاضل، المرجع السابق ، ص 318 .

يقيم الخائن وسيلة يستر بها دوافعه، إذ يكفي أن يلتقي بعض المال ليقول أصحاب هذا المذهب أن الفعل يكون تجسس، لأن الدافع هو الحصول على المال. فالمعيار المبني على الدافع إذن صعب التطبيق، ويفتح أمام المجرم باب التمويه و التضليل على مصراعيه.[1]

الفرع الثالث: معيار الجنسية.

ساد رأي آخر يفرق بين الخيانة و التجسس على أساس معيار جنسية الفاعل. و تعليله أن المواطن المارق الذي يعق وطنه و يخفر واجب الولاء حياله، هو أشد إجراما و أكثر مضاضة على النفس من ذلك الأجنبي الذي قد يقدم على إيذاء سلامة الدول الأخرى خدمة لوطنه. فالأول خائن بلا جدال، و أما الثاني فيعتبر أهل هذا الرأي جاسوسا.

و يأخذ بهذا المعيار عدة تشريعات منها القانون المغربي و القانون الجزائري. ففي هذه القوانين، يميز المشرع الجنائي بين الخيانة و التجسس على أساس معيار الجنسية.[2]

---

[1]– ينظر د/ محمد الفاضل، المرجع السابق، ص 319.

[2]– تنص المادة 185 عقوبات مغربي على:" يعد مرتكبا لجناية التجسس و يعاقب بالإعدام كل أجنبي ارتكب أحد الأفعال المبينة في المادة 181 فقرة 2 و 3 و 4 و 5 و المادة 182." أما المادة 61 عقوبات جزائري فتنص على: "يرتكب جريمة الخيانة و يعاقب بالإعدام كل جزائري و كل عسكري أو بحار في خدمة الجزائر يقوم بأحد الأعمال الآتية:

حمل السلاح ضد الجزائر.

القيام بالتخابر مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر أو تقديم الوسائل اللازمة لذلك سواء بتسهيل دخول القوات الأجنبية إلى الأرض الجزائرية أو بزعزعة ولاء القوات البرية أو البحرية أو الجوية أو بأية طريقة أخرى.

تسليم قوات جزائرية أو أرض أو مدن أو حصون أو منشآت أو مراكز أو مخازن أو مستودعات حربية أو عتاد أو ذخائر أو مبان أو سفن أو مركبات للملاحة الجوية مملوكة للجزائر أو مخصصة للدفاع عنها إلى دولة أجنبية أو إلى عملائها.

إتلاف أو فساد سفينة أو سفن أو مركبات للملاحة الجوية أو عتاد أو مؤن أو مبان أو إنشاءات من أي نوع كانت و ذلك بقصد الإضرار بالدفاع الوطني أو إدخال عيوب عليها أو التسبب في وقوع حادث و ذلك تحقيقا لنفس القصد".

وتضيف المادة 62 من نفس القانون أنه: "يرتكب جريمة الخيانة و يعاقب بالإعدام كل جزائري و كل عسكري أو بحار في خدمة الجزائر يقوم في وقت الحرب بأحد الأعمال الآتية:

تحريض العسكريين أو البحارة على الانضمام إلى دولة أجنبية أو تسهيل السبيل لهم إلى ذلك و القيام بعمليات تجنيد لحساب دولة في حرب مع الجزائر.

القيام بالتخابر مع دولة أجنبية أو مع أحد عملائها بقصد معاونة هذه الدولة في خططها ضد الجزائر.

عرقلة مرور العتاد الحربي.

المساهمة في مشروع لإضعاف الروح المعنوية للجيش أو للأمة يكون الفرض منه الإضرار بالدفاع الوطني مع علمه بذلك."

أما المادة 63 فنصت على: "يكون مرتكبا للخيانة و يعاقب بالإعدام كل جزائري يقوم:

بتسليم معلومات أو أشياء أو مستندات أو تصميمات، يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الاقتصاد الوطني إلى دولة أجنبية أو أحد عملائها على أية صورة ما و بأية وسيلة كانت.

الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها.

إذا أنها تعتبر الجرائم المضرة بالأمن الخارجي أو الدفاع الوطني التي يرتكبها المواطن خيانة، أما إذا ارتكبها أحد الأجانب، فإنها تأخذ وصف التجسس. على أن جرائم التجسس في هذه التشريعات لا تقتصر على نقل أو إفشاء الأسرار المتعلقة بالأمن الخارجي للدولة إلى سلطة أجنبية. بل تشمل إلى جانب ذلك، جرائم أخرى كتخريب و إتلاف الآلات و التجهيزات المعدة للاستعمال لمصلحة الدفاع الوطني و كذلك تحريض العسكريين على الانضمام إلى سلطة أجنبية أو إضعاف الروح المعنوية للجيش أو الأمة.[1]

المبحث الثاني:

ماهية التجسس عبر الانترنت

لقد أصبحت تلك الشبكة الإنترنت بنكا زاخرا بالمعلومات و تحولت إلى بيئة صالحة و تربة خصبة لعمليات التجسس على المعلومات الخاصة بالهيئات الحكومية والخاصة. وهذا ما يسر الأمر على مرتكبي مثل هذه الجرائم سواء أكان هؤلاء من القوى الداخلية أو الخارجية المعادية للدولة.

و في هذا يقرر أحد الخبراء أنه: "لم تعد القوة النارية التي تملكها الجيوش وحدها التي تقرر مصير الحروب و رجحان كفة الأطراف المتقاتلة و إنما المعلومات التي يملكها كل طرف حول الطرف الآخر هذه الحقيقة ثابتة منذ فجر التاريخ ولقد أتت التطورات السياسية و العسكرية خلال السنوات الأخيرة لتؤكدها." ويؤكد آخر في هذا الصدد أن الحرب اليوم أصبحت " حربا كلية و هناك ثلاث خطوط رئيسية تدور حولها المعلومات: فهناك المعلومات السياسية و المعلومات العسكرية والمعلومات الاقتصادية ولا يمكننا تمييز هذه المعلومات عن بعضها فكلها معلومات حيوية يجب أن تحصل عليها من البلاد المعادية قبل و أثناء القتال لتتضح لنا صورة عن قوة العدو".[2] وهذا ما يسرته الثورة الرقمية التي قوامها الحواسيب والانترنت، إذ أصبحت مسألة الحصول على المعلومات–أيا كان نوعها – تأخذ أبعادا جديدة، حيث تطورت أساليب جمع هذه المعلومات ولم تعد تقتصر على الجاسوسات الفاتنات اللواتي يقمن بإغواء قادة الأعداء، إذ صارت تعتمد اعتمادا كبيرا على التكنولوجيا الإليكترونية و المعلوماتية أي على التقنية الرقمية، ومنها التجسس على المعلومات – أيا كان نوعها –عن طريق الانترنت الشبكة التي – بالرغم من ايجابياتها– فتحت بوابة الخطر،و تحولت إلى شبح يهدد مصالح المجتمعات المتقدمة والنامية على السواء، اذ باتت تشبه الخزائن بلا أبواب.

و لقد تم تقسيم هذا المبحث الثاني كنظيره الأول إلى المطلبين التاليين:

المطلب الأول: تعريف التجسس عبر الإنترنت و الأساليب المتبعة فيه.

المطلب الثاني: موقف التشريعات المقارنة من جريمة التجسس عبر الإنترنت.

إتلاف مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد معاونة دولة أجنبية أو ترك الغير يتلفها".

أما المادة 64 من نفس القانون و كما سبق ذكره فقد خصها المشرع الجزائري بجريمة التجسس.

[1] – د/ محمود سليمان موسى، المرجع السابق، ص 146.

[2] – د/عفيفي كامل عفيفي، المرجع السابق، ص 305– 306

المطلب الأول:

تعريف التجسس عبر الانترنت و الأساليب المتبعة فيه.

و سيتم التطرق في هذا المطلب إلى تعريف هذا النوع الجديد من الاجرام المهدد لامن الدولة و التي ساهم التطور التكنولوجي لا سيما الانترنت في ظهوره، و في زيادة حجمه، ثم نتناول بعد ذلك الأساليب الحديثة المستعملة في ارتكاب مثل هذه الجريمة. و ذلك في الفروعين التاليين:

الفرع الأول: تعريف التجسس عبر الانترنت.

الفرع الثاني:الأساليب المتبعة في التجسس عبر الانترنت.

الفرع الأول: تعريف التجسس عبر الانترنت

وعليه يمكن تعريف التجسس عبر الانترنت بأنه:"الحصول وتجميع المعلومات السرية المخزنة والمحفوظة داخل لحواسيب المربوطة بالانترنت و الخاصة بسياسة الدولة وبدفاعها و نظامها الاقتصادي والصناعي وكذا أبحاثها العلمية خاصة تلك المتعلقة بأبحاث الطاقة النووية وتسليمها إلى حكومة أجنبية أخرى أو تجميع معلومات شخصية عن مستخدمي الانترنت بغية استغلالها لأغراض معينة(والذي تطرقنا إليه في الإعتداء على حرمة الحياة الخاصة)".[1]

باستقرائنا للتعريف السابق يمكن استخلاص مايلي:

أن محل هذه الجريمة يكون إما على شكل:

1/ بيانات سياسية و عسكرية:

أكد أحد الخبراء أن حرب اليوم أصبحت " حربا كلية و هناك ثلاث مجالات رئيسية مستهدفة للتجسس: وهي المعلومات السياسية و المعلومات العسكرية والمعلومات الاقتصادية"[2].

ولقد سبق و أن عرفنا كلا من التجسس العسكري و التجسس السياسي اللذان ينصبان على البيانات العسكرية والسياسية الخاصة بالدولة المعادية باعتبارها المرآة العاكسة لقوة تلك الدولة قبل و أثناء القتال.والأمر ذاته يتكرر بالنسبة للتجسس على هذه البيانات عبر الانترنت، و هذا ما أكدته إحصاءات صادرة من مكتب التحقيقات الفدرالي الأمريكي (أف بي آي) إذ أن 80% من الثغرات الأمنية في النظم الكمبيوترية الأمريكية تحدث عن طريق شبكة الانترنت.و قد حذر هذا المكتب من تزايد هذا الخطر على الأمن القومي الأمريكي مع دفع الاتجاه إلى تشبيك الأجهزة الكمبيوترية[3].

---

[1]– تجدر الاشارة إلى أن النوع الأول المشار إليه في التعريف هو الذي يهمنا في هذا المطلب.

[2]– د/عفيفي كامل عفيفي، المرجع السابق،ص310

[3]– د/عفيفي كامل عفيفي، نفس المرجع ،ص311

2/ المعلومات الاقتصادية:

حيث يهدف التجسس في نطاق الأنشطة التجارية إلى الحصول على أسرار التسويق والتجارة كحساب التكلفة وكشف الميزانية و أحوال الأسواق و العناوين الخاصة بالعملاء. أما في مجال الأنشطة الصناعية فيهدف التجسس فيها إلى الحصول على نتائج الأبحاث العلمية التي تجرى لتطوير المنتجات و أسرارها وخاصة الشرائح الصغيرة من أشباه المواصلات[1]. و في هذا الصدد يؤكد أحد الخبراء في مجال مكافحة الجاسوسية أهمية المعلومات الاقتصادية التي يتم جمعها عن الطرف المعادي لما لها من أثر حيوي يمكن تعطيل الجيش المعادي في ثكناته قبل أن يتحرك و ذلك لتدبر مصادر المقاومة... وهي إمكانيات البلاد الزراعية و الصناعية،و للمعلومات الاقتصادية أهمية عظمى في بناء خطة السوق ضد البلاد المعادية والعمل بها حال ابتداء القتال.بل إن هذه المعلومات لا تمثل أهمية قط للدول المتنافسة حربيا بل أن الأمر يتعدى ذلك الى الدول المتنافسة تجاريا[2]، فمع توسع التجارة الاليكترونية عبر شبكة الانترنت تحولت الكثير من مصادر المعلومات الى وسائط يسهل اختراقها أي أصبحت تمثل أهدافا سهلة للتجسس التجاري. ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار الى زيادة نسبة التجسس على الشركات من 36%عام 1994 الى 45% عام 1999. كما أظهر استفتاء أجري عام 1996 بين مسئولية الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول و بشكل غير مشروع على معلومات سرية عن أنشطة تجارية و صناعية في الولايات المتحدة. وتم ترتيب هذه الدول وفقا لحجم الانتهاكات على النحو التالي: الصين،كندا، فرنسا، الهند، اليابان، ألمانيا، كوريا الجنوبية، كومنولث الدول المستقلة (الاتحاد السوفييتي سابقا)، تايوان، المملكة المتحدة، إسرائيل، المكسيك،باكستان، سنغافورة، هونج كونج[3].

الفرع الثاني: الأساليب الحديثة المتبعة في التجسس عبر الانترنت:

من الأساليب المستحدثة للتجسس عبر الانترنت:

أولا: أسلوب إخفاء المعلومات داخل المعلومات: وهو أسلوب شائع و أن كان ليس بالأمر السهل و هو يتلخص في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومة أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها والغير عادية في داخلها، وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها. فالجاسوس يخاطر كثيرا إذا لجأ إلى طباعة المعلومات التي يخطط لسرقتها أو حاول عرضها على شاشة الحاسب لان الضحية قد يلحظ هذه التصرفات و يوقفها، أو قد يقوم الحاسب بتسجيل هذه المحاولات. و لذلك يلجأ الجواسيس إلى وسائل غير تقليدية للحصول على المعلومات السرية،فقد يقوم الجاسوس مثلا بكتابة برنامج وتنفيذه خلسة على حاسب

---

[1]– د/هشام محمد فريد رستم،(قانون العقوبات.....)،مرجع سابق،ص150

[2]– د/عفيفي كامل عفيفي، المرجع السابق،ص310

[3]– حسن طاهر داود، المرجع السابق، ص65

الضحية حيث يفحص هذا البرنامج كل البيانات المخزنة على الحاسب ثم يومض أحد المصابيح الصغيرة الموجودة على لوحة الحاسب لفترة قصيرة إذا كان البيان (0)أو يومض لفترة أطول إذا كان البيان (1)، ثم يقوم بتسجيل شريط فيديو لهذه اللوحة عن طريق تسليط كاميرا الفيديو (المخفية بمهارة) على لوحة الحاسب لتسجيل عمليات الوميض المتتالية،و بإدارة هذا الشريط بعد ذلك ببطء يمكن قراءة البيانات المسجلة في الحاسب دون ترك أثر ينم عن الجاسوس. وتجدر الإشارة إلى أن الكشف عن المعلومات المخفاة بهذا الأسلوب أمر صعب إن لم يكن مستحيلا في بعض الأحيان. [1]

ثانيا: استخدام برنامج حصان طروادة: [2]

و الذي يتم إستخدامه بصورة خفية في البرامج التطبيقية و بالتالي يمكن الوصول إلى قاعدة بيانات الحاسب من بعد دون أن يشعر أحد[3]، كأن يرسل أحد الهاكر صورة أو ملف يحتوي على ذلك الفيروس عبر المحادثات أو الشات أو من خلال رسالة عبر البريد الالكتروني.أو يقوم بإنزال برامج أو ملفات من مواقع مشبوهة مثل المواقع الجنسية أو المواقع التي تساعد على تعليم التجسس.[4]

ثالثا: استعمال تقنية أبواب المصيدة[5]: أو الابواب الخفية او الخلفية للتوصل غير المصرح به و غير المحدد إلى بيانات الحاسب و برامجه و ملفاته. و قد تم استخدام هذه التقنية من قبل أحد المبرمجين الذي اعد بابا خفيا في البرنامج الذي تستخدمه احدى الشركات التي تستخدم حاسب للمشاركة الزمنية، مما سمح له بالحصول على برامج و بيانات مستخدمين آخرين.[6]

رابعا: استعمال هوائيات مع ربطها بحاسب خاص: حيث يمكن عن طريق هذه الهوائيات التقاط الموجات الكهرومغناطيسية المنبعثة من الحاسب خلال فترة تشغيله مع امكانية تسجيلها و معالجتها و ترجمتها إلى معلومات تتسم بالوضوح،حيث يمكن أن يتم هذا الالتقاط من مسافة تزيد على 300 قدم من الحاسب المستهدف.[7]

كما أن هناك تقنيات أخرى للتجسس على البيانات في حال انتقالها بين نهاية طرفية و أخرى، و يمكن حصرها فيمايلي:

– استعمال أجهزة اليكترونية بسيطة لالتقاط البيانات المنقولة عن طريق الاسلاك المعدنية أو خطوط الهاتف الخاصة لأنظمة الاتصالات الاليكترونية .

---

[1]–لمزيد من التفاصيل ينظر حسن طاهر داود، نفس المرجع ،ص67–68

[2]– ينظر تعريف هذا البرنامج في ص 351 من هذه الرسالة.

[3]–د/عفيفي كامل عفيفي، المرجع السابق،ص 312

[4]–مقال ما هي عملية الهاكينج أو التجسس ؟ ،http:// www. wikipedia.org

[5]– تقوم فكرة هذه التقنية على ترك ثغرات تسمح بالدخول إلى البرنامج مرة أخرى عند إعداده لتلافي ما قد يرد فيه من أخطاء.

[6]– ينظر د/ هشام محمد فريد رستم،(قانون العقوبات ومخاطر...) مرجع سابق، ص 142.

[7]– د/ عفيفي كامل عفيفي، المرجع السابق، ص 313.

– استعمال أجهزة التقاط خاملة لا تصدر أية اشارات لاسلكية لإعتراض وصلات الموجات القصيرة التي تحتوي على مجموعة من القنوات المحتوية على بيانات.[1]

المطلب الثاني:

موقف التشريعات المقارنة من جريمة التجسس عبر الانترنت.

تعتبر جرائم التجسس جرائم قديمة قدم البشرية و معاقب عليها بأشد العقوبات في كافة القوانين الغربية والعربية على السواء. و التجسس عبر الانترنت يعتبر أحد أشكال التجسس الحديث و بالضبط نوعا من التجسس الالكتروني (كالتجسس بواسطة الأقمار الصناعية و التجسس بواسطة طائرات الاستطلاع المتقدمة....) إلا أنه في معظم الأحيان لا تتمكن الدولة – رغم علمها باسم الدولة التي تتجسس عليها– من ضبط الشخص الذي يقوم بالتجسس إلا في أحوال معينة وهي إذا ما كان التجسس يتم بالشكل القديم و الذي يتم بإرسال شخص من الدولة إلى الدولة الأخرى للحصول على المعلومات من مصادره في تلك الدولة فيتم التمكن من ضبطه. الأمر الذي جعل نصوص القانون الجنائي قاصرة و عاجزة على مواجهة مثل هذا الاجرام المستحدث و الخطير المهدد لمصالح الدولة بما فيها زعزعة أمنها واستقرارها. و على هذا فالسؤال المطروح هنا هو: كيف عالجت التشريعات المقارنة هذه الجريمة المستحدثة؟. و للاجابة على هذا السؤال ارتأينا تقسيم هذا المطلب إلى فرعين. و ذلك كالآتي:

الفرع الأول:موقف التشريعات الغربية من جريمة التجسس عبر الانترنت.

الفرع الثاني: موقف التشريعات العربية من جريمة التجسس عبر الانترنت.

الفرع الأول: موقف التشريعات الغربية من جريمة التجسس عبر الانترنت.

سنبين من خلال هذا الفرع كلا من موقف التشريع الفرنسي حيال هذه الجريمة المستحدثة، ثم نتناول موقف التشريع الأمريكي. وذلك كالآتي:

أولا: موقف التشريع الفرنسي من جريمة التجسس عبر الانترنت.

لم يعرف المشرع الفرنسي كغيره من المشرعين جريمة التجسس تاركا ذلك للفقه و القضاء[2] ، و لكنه عالجها باعتبارها جريمة تمس أمن و سلامة الدولة في الباب الأول من الكتاب الرابع تحت عنوان" الجنايات و الجنح الواقعة على الوطن، الدولة و السلامة العامة"، حيث تناولها في القسم الأول المعنون بالخيانة و التجسس في المواد من 411-1 إلى غاية المادة 411- 11 من قانون العقوبات الفرنسي الجديد. إذ نص في المادة 411-1 من قانون العقوبات الفرنسي الجديد على: "تعتبر الأفعال الواردة في

---

[1]– ينظر د/ عفيفي كامل عفيفي، نفس المرجع ، ص 314.

[2]– ينظر في ذلك ص369 من هذه الرسالة.

المواد 411-2 إلى 411-11 خيانة إذا كانت مرتكبة من طرف فرنسي أو عسكري في خدمة فرنسا وتكون تجسس إذا ارتكبها أجنبي."[1]

و باستقرائنا لهذه المادة يمكن تعريف التجسس بأنه: "كل فعل يقوم به أجنبي و يؤدي إلى الإضرار بالمصالح الأساسية للأمة و الدولة الفرنسية، و التي تتألف من أمنها و استقلالها و سلامتها الإقليمية وشكل نظامها الجمهوري، و مؤسساتها ووسائل دفاعها، و علاقاتها الدبلوماسية و حماية الشعب داخل وخارج فرنسا و التوازن في وسطه الطبيعي ومحيطه و العناصر الأساسية في مقدراتها العلمية والاقتصادية و تراثها الحضاري. و لقد تناول المشرع الفرنسي التجسس عبر الانترنت في المادة 411-6 إلى غاية المادة411-9 من قانون العقوبات الفرنسي الجديد[2].حيث يتضح من خلال هذه المواد أن التجسس يمكن أن يحدث عن طريق الانترنت، و ذلك من خلال تسليم أو تسهيل تسليم أو جمع أو اتلاف بيانات معلوماتية من شأنها المساس بأمن و سلامة الدولة إلى دولة أجنبية أو إلى أحد عملائها.

---

[1] – 411-1:" Les faits définis par les articles 411-2 à 411-11 constituent la trahison lorsqu'ils sont commis par un Français ou un militaire au service de la France et l'espionnage lorsqu'ils sont commis par toute autre personne.

[2] –Article 411-6 :" Le fait de livrer ou de rendre accessibles à une puissance étrangère، à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements، procédés، objets، documents، données informatisées ou fichiers dont l'exploitation، la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225000 euros d'amende."

Article 411-7 :" Le fait de recueillir ou de rassembler، en vue de les livrer à une puissance étrangère، à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents، des renseignements، procédés، objets، documents، données informatisées ou fichiers dont l'exploitation، la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150000 euros d'amende".

Article 411-8 :" Le fait d'exercer، pour le compte d'une puissance étrangère، d'une entreprise ou organisation étrangère ou sous contrôle étranger ou de leurs agents، une activité ayant pour but l'obtention ou la livraison de dispositifs، renseignements، procédés، objets، documents، données informatisées ou fichiers dont l'exploitation، la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150000 euros d'amende".

Article 411-9 :" Le fait de détruire، détériorer ou détourner tout document، matériel، construction، équipement، installation، appareil، dispositif technique ou système de traitement automatisé d'informations ou d'y apporter des malfaçons، lorsque ce fait est de nature à porter atteinte aux intérêts fondamentaux de la nation، est puni de quinze ans de détention criminelle et de 225000 euros d'amende Lorsqu'il est commis dans le but de servir les intérêts d'une puissance étrangère، d'une entreprise ou organisation étrangère ou sous contrôle étranger، le même fait est puni de vingt ans de détention criminelle et de 300000 euros d'amende."

و من الأمثلة الحية عن جريمة التجسس عبر الانترنت في الدول الأوروبية:

– خلال صيف1994 قامت مجموعة من الهكرة بسرقة معلومات عسكرية تتعلق بالسفن التي تستعملها القوات العسكرية التابعة للدول الاعضاء في حلف شمال الاطلنطيNATO من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية.[1]

– تم رصد هجمات جاسوسية في ألمانيا استهدفت كلا من السلطات الحكومية الألمانية أو الشركات العاملة في القطاع الاقتصادي عبر الانترنت وبالضبط عبر البريد الالكتروني.

وتجدر الإشارة إلى أن عدد هذه الهجمات الالكترونية قد عرف تزايدا من عام 2009 الى عام 2010من 900هجمة الى 1600 هجمة و الذي كان مصدرها من الصين و روسيا لا سيما التجسس الاقتصادي.

هذا من جهة ومن جهة أخرى، فان إحدى الدراسات العلمية ترجح تكبد ألمانيا خسائر تقدر بما يتراوح بين 20–50 مليار يورو سنويا بسبب التجسس الاقتصادي أو التجسس على الشركات المنافسة في ألمانيا.وفي هذا يرى فريتشه (وكيل وزارة الداخلية) أن الهجمات في عالم المعلومات تزايدت خلال السنوات الماضية وأصبحت أكثر تعقيدا و خاصة تلك التي تستخدم برنامج "ستوكس نت " والذي هو عبارة عن دودة الكترونية تلعب دور فيروسات جاسوسية والتي ألحقت أضرارا جسيمة بالمنشآت النووية في إيران. ولقد أكدت بيانات وزارة الداخلية في ألمانيا أن عدد المواقع الالكترونية التي تصل عدوى البرامج الضارة يصل إلى 40 ألف موقع ثم تنتشر الفيروسات الضارة عبر هذه البرامج.[2]

ثانيا: موقف التشريع الأمريكي من جريمة التجسس عبر الانترنت.

عالج المشرع الأمريكي جريمة التجسس في قانون التجسس لسنة 1917 في القسم 50 من القانون الأمريكي[3] ، ثم تناولها في القسم 18USC Section793 من ذات القانون[4]. و تناول جريمة التجسس

---

[1]– د/ حسين الغافري، محمد الألفي، المرجع السابق،ص49.

[2]– مقال حرب التجسس عبر الإنترنت. يوزع بلانك. وكالة الأنباء الألمانية، http:// www.th3pro.com

[3]–لمزيد من التفاصيل ينظر مقال لويكيبدي:Espionnage Act de 1917، http:// en.wikipedia.org

[4] –18 USC §793:" (**a**)Whoever، for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States، or to the advantage of any foreign nation، goes upon، enters، flies over، or otherwise obtains information concerning any vessel، aircraft، work of defense، navy yard، naval station، submarine base، fueling station، fort، battery، torpedo station، dockyard، canal، railroad، arsenal، camp، factory، mine، telegraph، telephone، wireless، or signal station، building، office، research laboratory or station or other place connected with the national defense owned or constructed، or in progress of construction by the United States or under the control of the United States، or of any of its officers، departments، or agencies، or within the exclusive jurisdiction of the United States، or any place in which any vessel، aircraft، arms، munitions، or other materials or instruments for use in time of war are being made، prepared، repaired، stored، or are the subject of research or development، under any contract or agreement with the United States، or any department or agency thereof، or with any person on behalf of the United States، or otherwise on behalf of the United States، or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the

عبر الانترنت على بيانات معلوماتية تضم معلومات سرية تمس بسلامة و أمن الحكومة الأمريكية والموجودة في حواسيب تلك الأخيرة في القسم[1] 18 USC Section 1030(a)،حيث نص فيه على معاقبة

Army، Navy، or Air Force is being prepared or constructed or stored، information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(**b**)Whoever، for the purpose aforesaid، and with like intent or reason to believe، copies، takes، makes، or obtains، or attempts to copy، take، make، or obtain، any sketch، photograph، photographic negative، blueprint، plan، map، model، instrument، appliance، document، writing، or note of anything connected with the national defense; or

(**c**)Whoever، for the purpose aforesaid، receives or obtains or agrees or attempts to receive or obtain from any person، or from any source whatever، any document، writing، code book، signal book، sketch، photograph، photographic negative، blueprint، plan، map، model، instrument، appliance، or note، of anything connected with the national defense، knowing or having reason to believe، at the time he receives or obtains، or agrees or attempts to receive or obtain it، that it has been or will be obtained، taken، made، or disposed of by any person contrary to the provisions of this chapter; or

(**d**)Whoever، lawfully having possession of، access to، control over، or being entrusted with any document، writing، code book، signal book، sketch، photograph، photographic negative، blueprint، plan، map، model، instrument، appliance، or note relating to the national defense، or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation، willfully communicates، delivers، transmits or causes to be communicated، delivered، or transmitted or attempts to communicate، deliver، transmit or cause to be communicated، delivered or transmitted the same to any person not entitled to receive it، or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(**e**)Whoever having unauthorized possession of، access to، or control over any document، writing، code book، signal book، sketch، photograph، photographic negative، blueprint، plan، map، model، instrument، appliance، or note relating to the national defense، or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation، willfully communicates، delivers، transmits or causes to be communicated، delivered، or transmitted، or attempts to communicate، deliver، transmit or cause to be communicated، delivered، or transmitted the same to any person not entitled to receive it، or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(**f**)Whoever، being entrusted with or having lawful possession or control of any document، writing، code book، signal book، sketch، photograph، photographic negative، blueprint، plan، map، model، instrument، appliance، note، or information، relating to the national defense،…"

[1] – 18 USC § 1030:"(**a**)Whoever :

(**1**)having knowingly accessed a computer without authorization or exceeding authorized access، and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations، or any restricted data، as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954، with reason to believe that such information so obtained could be used to the injury of the United States، or to the advantage of any foreign nation willfully communicates، delivers، transmits، or causes to be communicated، delivered، or transmitted، or attempts to communicate، deliver، transmit or cause to

كل من اتصل عن علم بدون تصريح بحاسب أو اتصل به على نحو غير مصرح به و انتهز ذلك لتحقيق أغراض خارج نطاق التصريح المخول له و تمكن بهذا السلوك من:

1- الحصول على معلومات سرية لحكومة الولايات المتحدة الأمريكية بقصد استخدامها أو بسبب الاعتقاد في امكانية استخدامها للإضرار بالولايات المتحدة أو لفائدة دولة أجنبية.

2- الحصول على معلومات تتعلق بمؤسسة مالية أو بوكالة تقدم تقارير عن المركز الإئتماني للمستهلكين.

3- استخدام أو تعديل او اتلاف أو تدمير أو افشاء معلومات مخزنة في حاسب عن علم بذلك، أو منع الاستخدام المصرح به لحاسب متى كان هذا الحاسب يعمل أو يدار لأجل أو بالنيابة عن حكومة الولايات المتحدة الأمريكية و كان من شأن سلوك الفاعل التأثير في تشغيله.

و من الأمثلة الواقعية عن التجسس عبر الانترنت الواقع على حواسيب الحكومة الأمريكية أو الذي تقوم به تلك الحكومة للتجسس على غيرها من الدول:

- تمكن طالب من اختراق شبكة الحاسب لهيئة الأبحاث المتقدمة والتي تقوم بربط الشبكات المدنية بنظريتها العسكرية التابعة لوزارة الدفاع الأمريكية وذلك في عام 1984.[1]

- اختراق "ادوارد أوستن سبخ" البالغ من العمر 23عاما أنظمة 200حاسب في دول مختلفة خلال عام 1988، من بينها أنظمة حاسبات تابعة لوزارة الدفاع البريطانية ووكالة الناسا الأمريكية لأبحاث الفضاء وبعض الشبكات المعلوماتية العسكرية الأمريكية بما فيها شبكة ملينات، وذلك باستخدام بعض تسهيلات النظام المعلوماتي لإحدى الجامعات.

- اختراق الألماني الغربي "ماركوس هيس" البالغ من العمر 24عاما أنظمة 30حاسب بالولايات المتحدة الأمريكية تتعامل في معلومات عسكرية والحصول منها على معلومات لها هذه الصفة فضلا عن بيانات تتعلق بأبحاث علمية، وذلك عن طريق الاتصال البعدي.[2]

---

be communicated، delivered، or transmitted the same to any person not entitled to receive it، or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2)intentionally accesses a computer without authorization or exceeds authorized accessand thereby obtains;

(3)intentionally، without authorization to access any nonpublic computer of a department or agency of the United States، accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or، in the case of a computer not exclusively for such use، is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States."

- Charles DOYLE :Cybercrime،A sketch of 18 usc 1030 and related federal criminal laws، the librery of congress ,CRS, 25 february2008,p2 et suite.

- Computer Fraud and Abuse Act , http://cio.doe.gov

[1]- ينظر د/هشام محمد فريد رستم، (قانون العقوبات و مخاطر تقنية المعلومات) مرجع سابق،هامش رقم (2) ص 134

[2]- د/ عفيفي كامل عفيفي، المرجع السابق،ص309

– قيام خمسة متسللين من هولندا في الفترة ما بين عامي 1990–1991م من التسلل الى 43 نظاما من أنظمة الحاسب الآلي في مواقع الجيش الأمريكي على شبكة الانترنت، بما في ذلك المواقع التي كانت موجهة مباشرة لعملية عاصفة الصحراء، حيث استطاعوا الحصول على معلومات في غاية الأهمية عن مواقع دقيقة للقوات الأمريكية و أنواع الأسلحة التي تمتلكها تلك القوات، و قدرة صواريخ باتريوت، و حركة السفن الحربية في منطقة الخليج.

– ومن بين حالات التجسس الدولي (أي التجسس الذي تقوم به الأجهزة الاستخبارية للحصول على أسرار و معلومات الدولة و من ثم إفشائها لدولة أخرى معادية، أو استغلالها بما يضر المصلحة الوطنية للدولة) ما تم اكتشافه مؤخرا عن مفتاح وكالة الأمن القومي الأمريكية والتي قامت بزراعته في نظام التشغيل الشهير "ويندوز ".

هذا من جهة ومن جهة أخرى،كشف أخيرا النقاب عن شبكة دولية ضخمة للتجسس الالكتروني تعمل تحت إشراف هذه الوكالة بالتعاون مع أجهزة الاستخبارات و التجسس في كل من كندا وبريطانيا ونيوزيلندا ويطلق عليها اسم " أيشلون " لرصد المكالمات الهاتفية والرسائل بكافة أنواعها سواء ما كان منها برقيا أو تلكس أو فاكس أو الكترونيا.[1]

– كما نشرت صحيفة فرنسية ملفا واسعا عن خفايا موقع الفايسبوك والجهات الصهيونية و أكدت على أنه موقع استخباراتي صهيوني مهمته تجنيد العملاء والجواسيس لصالح الكيان الصهيوني.وتضمن الملف الذي نشرته مجلة لوما غازين ديسرائيل معلومات عن أحدث الطرق للجاسوسية تقوم بها كل من المخابرات الإسرائيلية و الأمريكية و ذلك بإيجاد جهاز استخباري اسمه مخابرات الانترنت عن طريق تجنيد أشخاص عاديين لا يعرفون أنهم يقومون بمثل هذه المهمة الخطيرة معتقدين بأنهم يتسلون أمام صفحات الدردشة الفورية واللغو في أمور قد تبدو غير مهمة.[2]

– كما كشف كتاب صدر في باريس تحت عنوان "عين واشنطن " النقاب عن فضيحة تورط جهازي المخابرات الأمريكية و الإسرائيلية في اختراق جميع المعلومات المسجلة على هذه الأجهزة،وذكر فيه أن الولايات المتحدة تقوم بعمل كمائن للنظم المعلوماتية لدى أعدائها و حلفائها على حد سواء بحيث تصبح لديها جميع المعلومات في مختلف المجالات، و أشار إلى أن هناك اتفاقا بين الولايات المتحدة وإسرائيل على أن يتم تصميم برنامج معلوماتي معين تبيعه الولايات المتحدة لخصوم إسرائيل و أعدائها مقابل قيام إسرائيل ببيع هذا البرنامج لخصوم الولايات المتحدة و أعدائها. كما أكد مؤلفا الكتاب أن إسرائيل في فترة الانتفاضة الفلسطينية أرادت أن تحصل على كل المعلومات المخزنة لدى الأردن عن الفلسطينيين فاتفقت

---

[1]– ينظر لمزيد من التفاصيل منير محمد الجنبيهي وممدوح محمد الجنبيهي،(جرائم الإنترنت...) مرجع سابق، ص88–87.

[2]– مقال التجسس عبر الإنترنت....أو مخابرات الإنترنت ، http:// www.almski. Com

مع شركة أمريكية على أن تبيع برنامج معلومات إلى الأردن للتجسس على كل المعلومات الموجودة لديها بسهولة عن الفلسطينيين والأرض المحتلة ونقلها إلى إسرائيل. [1]

– إضافة إلى وجود موقع يدعى ويكيليكس الذي يتجسس على أسرار السياسة العالمية و خاصة سياسة الحكومة الأمريكية و من بينها كشفه لخفايا القضية الفلسطينية والقضية العراقية .[2]

– قيام وكالة المخابرات الأمريكية (CIA) ووكالة التحقيقات الفيدرالية (FBI) من القبض على عملاء فرنسيين بعد اتهامهم بالتجسس على أحد كبريات الشركات الأمريكية في مجال الحاسب.[3]

الفرع الثاني: موقف التشريعات العربية من جريمة التجسس عبر الانترنت.

هذا فيما يخص موقف التشريعات الغربية، أما بالنسبة لموقف التشريعات العربية من جريمة التجسس عبر الإنترنت فيمكن أن نقسمه إلى موقفين، نتطرق في أولهما إلى تحديد الدول العربية التي وضعت قوانين خاصة في مواجهة هذه الجريمة الخطيرة ثم نعرج إلى الدول العربية التي التزمت الصمت حيال هذا الاجرام المستحدث الخطير و الجسيم المهدد لسلامة و أمن الدولة. أما الموقف الثاني فارتأينا تخصيصه للتشريع الجزائري.

أولا: موقف التشريعات العربية بصفة عامة عن جريمة التجسس عبر الانترنت.

انقسمت التشريعات العربية حيال مواجهة جريمة التجسس عبر الانترنت إلى تشريعات لم تعدل قوانينها لتتلاءم مع هذه الجريمة الخطيرة الماسة بأمن الدولة مكتفية بتطبيق قوانينها العقابية التقليدية، و من بينها **التشريع المصري** و الذي تناول جريمة التجسس في المادة 77 من قانون العقوبات المصري. و **التشريع السوري** و الذي تناولها في المواد 271 إلى 274 من قانون العقوبات السوري، و **التشريع المغربي** في المادة 185 من قانون العقوبات المغربي.

وعلى عكس التشريعات العربية السابقة عالجت بعض التشريعات العربية هذه الجريمة المستحدثة و خصتها بنصوص قانونية خاصة ضمن قوانين مخصصة لمكافحة الجريمة المعلوماتية، و منها **نظام مكافحة جرائم المعلوماتية والتعاملات الالكترونية السعودي** في المادة 7/ 2 منه.[4] و كذا **الامارات العربية المتحدة** من

---

[1]– لمزيد من التفاصيل حول هذا الكتاب ينظر د/ عفيفي كامل عفيفي، المرجع السابق،ص 311–312

[2]– ينظر لمزيد من التفاصيل موقع ويكيليكس الموجود على الإنترنتWikileaks.org مثلا كالموقع الذي يكشف أسرار الحرب الأمريكية على العراق الموجود على:Irak.arte.tv

[3]– ينظر د/ هشام محمد فريد رستم،(قانون العقوبات.....) مرجع سابق، ص 150

[4]– تنص المادة 2/7 من نظام مكافحة جرائم المعلوماتية والتعاملات الالكترونية السعودي على:" يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:.....

2–الدخول غير المشروع إلى موقع الكتروني، أو نظام معلوماتي مباشرة،أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة،أو اقتصادها الوطني."

خلال القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات في المادة 22.[1] كما جرم المشرع السوداني جريمة التجسس عبر الانترنت في **قانون جرائم المعلوماتية السوداني لسنة 2007** من خلال المادة 7 منه[2].

ثانيا: موقف التشريع الجزائري من جريمة التجسس عبر الانترنت.

تناول المشرع الجزائري جريمة التجسس في الباب الأول من الكتاب الثالث تحت عنوان الجنايات و الجنح ضد الشيء العمومي، و ذلك في المادة 64 من قانون العقوبات الجزائري.[3] أين يتضح من خلالها مايلي:

1- أن المشرع الجزائري يعتبر الجاسوس هو كل شخص أجنبي يجمع أو يحاول جمع معلومات تمس بأمن الدولة الخارجي لمدها لدولة أجنبية معادية.

2- أن المشرع الجزائري يحدد على سبيل الحصر الأفعال التي تكون جريمة التجسس لكونها جريمة خطيرة و هامة تهدد أمن الدولة و سلامة ترابها. و هي:

- القيام بالتخابر مع دولة أجنبية أو مع من يعملون لمصلحتها لمعاونتها في عملياتها الحربية للاضرار بالقوات الجزائرية و الذي يتم عن طريق تسريب معلومات سرية و هامة تمس بأمن الدولة. و يستوي في ذلك أن يكون هذا التخابر سريا أو علنيا، شفويا أو كتابيا، بصورة مباشرة أو غير مباشرة ، و لو لمرة واحدة، و لا يشترط في ذلك أن تتحقق النتيجة لقيام هذه الجريمة.

و تجدر الاشارة أن المشرع الجزائري لم يحدد صورا لمعاونة الدولة الأجنبية في عملياتها الحربية.

- تسهيل دخول القوات الأجنبية إلى الأرض الجزائرية أو تقديم الوسائل اللازمة لذلك، أو زعزعة ولاء القوات المسلحة الجزائرية عن طريق تحريضها بعدم ولائها للسلطة الجزائرية و التآمر عليها لمصلحة دولة أجنبية.

---

[1]- تنص المادة 22 من القانون الاتحادي رقم (2)لسنة 2006بشأن مكافحة جرائم تقنية المعلومات على:" يعاقب بالسجن كل من دخل و بغير وجه حق موقعا أو نظاما مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك".

[2]- تنص المادة 7من قانون جرائم المعلوماتية السوداني لسنة 2007 على:" كل من يدخل عمدا موقعا او نظاما مباشرة أو عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب و ما في حكمها بغرض:

- الحصول على بيانات أو معلومات تمس الأمن القومي للبلاد او الاقتصاد الوطني يعاقب بالسجن مدة لا تتجاوز 7 سنوات أو بالغرامة أو بالعقوبتين معا،

- الغاء بيانات أو معلومات معلومات تمس الأمن القومي للبلاد او الاقتصاد الوطني او حذفها او تدميرها أو تغييرها يعاقب بالسجن مدة لا تتجاوز 10 سنوات أو بالغرامة أو بالعقوبتين معا."

[3]- تنص المادة 64 من قانون العقوبات الجزائري على:"يرتكب جريمة التجسس و يعاقب بالاعدام كل أجنبي يقوم بأحد الأفعال المنصوص عليها في الفقرات 2 و3 و4 من المادة 61 و في المادتين 62 و 63.و يعاقب من يحرض على ارتكاب احدى الجنايات المنصوص عليها في هذه المادة و المواد 61 و 62 و 63 أو يعرض ارتكابها بالعقوبة المقررة للجناية ذاتها."

– تسهيل دخول العدو إلى البلاد عن طريق تعطيل القوات الجزائرية و انسحابها من موقع معين قصد تمكين قوات الجيش الأجنبية من الدخول إلى الاقليم الجزائري بكامل عناصره.

– تسليم العدو بعد دخوله إلى البلاد مدنا أو حصونا أو منشآت أو أراضي أو عتاد أو مستودعات حربية أو السفن أومبان أو طائرات سواء أكانت مملوكة للجزائر أو مخصصة للدفاع أو ذخائر.

– اتلاف أو افساد أو ادخال عيوب لسفينة أو طائرة أو عتاد أومبان أو مؤن أو انشاءات بقصد الاضرار بالدفاع الوطني.

– المساهمة في جريمة اضعاف الروح المعنوية للجيش أو للأمة وذلك بانزال الخوف و الفزع في قلب الجيش قبل و أثناء المواجهة فيدخلون المعركة و هم خائفون من نتيجتها كاشاعة معلومات تتعلق بجسامة سلاح العدو، أو باضعاف المقاومة الشعبية للشعب الجزائري كنقص في التموين مثلا.

– الاستحواذ بأية وسيلة كانت على أسرار الدفاع الوطني أو الاقتصاد الوطني بقصد تسليمها إلى دولة أجنبية أو أحد عملائها.

– اتلاف أسرار الدفاع الوطني أو الاقتصاد الوطني بقصد معاونة دولة أجنبية.

3– أن المشرع الجزائري اعتبر أن هذه الجريمة هي من الجرائم العمدية التي تتطلب قصدا جنائيا عاما وآخر خاصا يتمثل في الاضرار بمصالح الدولة و الدفاع الوطني.

4– قرر المشرع الجزائري عقوبة الاعدام على كل من يرتكب جريمة التجسس أو يحرض على ارتكابها .

هذا فيما يخصص جريمة التجسس بصفة عامة، أما عن موقف المشرع الجزائري من جريمة التجسس عبر الانترنت فإنه يمكننا استخلاصها من المادة 2/63[1] من خلال العبارة التالية: " الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات.....". و التي قد تتم عن طريق الانترنت بالولوج إلى حواسيب الجيش الوطني والحصول على أسرار الدفاع الوطني أو الاقتصاد الوطني. و كذا من خلال المادة 394 مكرر3 من قانون العقوبات الجزائري[2]. كما نص في المادة 394 مكرر2على أنه يعاقب كل من بحث أو جمع أو وفر أو نشر أو حاز أو إستعمل معطيات مخزنة لأي غرض كان و ليكن في هذه الحالة التجسس على أسرار الدفاع الوطني.[3] و على هذا يمكن أن نستخلص أن المشرع الجزائري يعترف و يجرم التجسس الواقع عن طريق الانترنت.

و من الأمثلة الحية عن هذا النوع من التجسس عبر الإنترنت في الدول العربية:

– كشفت مفكرة الإسلام –خلال الثورة الشعبية لمصر – عن عرض قدمته شركة بريطانية لتزويد النظام الحاكم في مصر سابقا قبل الإطاحة به في ثورة شعبية قبل شهور ببرامج للتجسس على اتصالات الانترنت

---

[1]– تنص المادة 2/63 من قانون العقوبات الجزائري على:".....2–الإستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها."

[2]– تنص المادة 394 مكرر 3 من قانون العقوبات الجزائري على:" تضاعف العقوبات المنصوص عليها في هذا القسم، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضع للقانون العام، دون الاخلال بتطبيق عقوبات أشد".

[3]– ينظر نص المادة 394 مكرر2 ص442.

لاستهداف الناشطين.وذكرت هيئة الإذاعة البريطانية أن وثائق عثر عليها داخل مقر جهاز "أمن الدولة " تشير إلى أن تلك البرامج التي زودت بها الشركة البريطانية الحكومة المصرية تم استخدامها لفترة تجريبية لمدة 5 أشهر نهاية العام.[1]

– كشف موقع بلومبورغ في سوريا –و نظرا لما يحدث فيها من ثورة شعبية على غرار الدول التي شهدتها –بأن شركة آريا الايطالية عقدت مع سوريا صفقة ب18مليون دولار تتضمن تمكينها من الحصول على برنامج للتجسس أطلق عليه اسم "أصفادور" من أجل تعقب الناشطين السياسيين عبر الانترنت ومراقبة المكالمات الهاتفية والرسائل النصية الواردة في البريد الالكتروني.إذ يتم فحص وتصنيف هذه بالرسائل وتجميعها في مكان رصد خاص لمراقبتها مراقبة حية و خاصة إذا تعلق الأمر بمظاهرات و تجمعات شعبية مثلا. [2]

[1]– مقالة التجسس الاقتصادي عبر الإنترنت ، http:// www. forexblogae.com

[2]– هذا البرنامج ما يزال في مراحله التجريبية اذ لم يكتمل تركيبه بعد وفقا وكالة بلومبورغ، و يشرف عليه مهندسون ايطاليون متواجدون في دمشق.تقرير أوردته قناة العربية في نشرتها "آخر ساعة " ،http:// www.youtube.com

خلاصة الباب الثالث:

تبين من خلال هذا الباب أن جرائم العدوان على أمن الدولة تعد من أخطر الجرائم التي تكون ضحيتها الرئيسية الدولة، سواء بصفتها شخصا من أشخاص القانون العام الداخلي أو شخصا من أشخاص القانوني الدولي العام. و لقد تأثرت كغيرها من الجرائم (الواقعة على الأشخاص و الواقعة على الأموال) بالتطور التكنولوجي، و ما نتج عنه من اجتياح و غزو الانترنت للعالم و كثرة الإعتماد عليها واستخدامها في كافة نواحي الحياة، و التي قلبت موازين هذا الكون برمته سواء بالإيجاب أو بالسلب. ولكن و لسوء الحظ فاق الجانب السلبي على الإيجابي و ذلك بسوء استغلال هذه الشبكة في ارتكاب أفعال غير مشروعة كانت في الماضي مستحيلة أو شبه مستحيلة، و من بينها جرائم العدوان على امن الدولة و لا سيما جريمتي الإرهاب و التجسس، و التي ساهمت هذه الشبكة بقدر كبير في ارتكابها بشكل سهل و سريع وفتاك اذ سهلت على مرتكبيها بما تتمتع به من خصائص تجعلها فريدة من نوعها طريقا كانت صعبة وشاقة و طويلة في الماضي.

- **فأما فيما يخص جريمة الإرهاب عبر الإنترنت:** فهو يعد من أحدث و أخطر أشكال الإرهاب اليوم الذي يواجه العالم، و هو يتمثل في استخدام الموارد المعلوماتية المتمثلة في شبكات المعلومات وأجهزة الكومبيوتر و شبكة الإنترنت، لأغراض التخويف أو الإرغام لأهداف سياسية. وهو يرتبط الى حد كبير بالمستوى المتقدم للغاية الذي تلعبه تكنولوجيا المعلومات في كافة مجالات الحياة في العالم. و يمكن أن يتسبب في الحاق الشلل لأنظمة القيادة و السيطرة و الإتصالات أو قطع شبكات الإتصالات بين الوحدات و القيادة أو تعطيل أنظمة الدفاع الجوي أو اخراج الصواريخ عن مسارها أو اختراق النظام المصرفي او ارباك حركة الطيران المدني أو شل محطات الطاقة الحرارية و النووية. اذ يعد نوعا من أنواع الإرهاب الإلكتروني أو الرقمي، فهي جريمة حديثة في طرقها و قديمة في اسمها.

- **أما فيما يخص التجسس عبر الإنترنت:** فهو يعتبر أحد أشكال التجسس الحديث و بالضبط نوعا من التجسس الالكتروني (كالتجسس بواسطة الأقمار الصناعية والتجسس بواسطة طائرات الاستطلاع المتقدمة.....).

ويكون بالحصول وتجميع المعلومات السرية المخزنة والمحفوظة داخل الحواسيب المربوطة بالانترنت والخاصة بسياسة الدولة وبدفاعها و نظامها الاقتصادي والصناعي وكذا أبحاثها العلمية خاصة تلك المتعلقة بأبحاث الطاقة النووية وتسليمها إلى حكومة أجنبية أخرى أو تجميع معلومات شخصية عن مستخدمي الانترنت بغية استغلالها لأغراض معينة.

خاتمة:

الآن وقد فرغنا من هذه الرسالة، نريد أن نتساءل عن النتيجة التي خلصنا إليها، والتي كان البحث في شتى مراحله مقدمة تؤدي إليها، والحق أن خاتمة بحث من الأبحاث يجب أن تحفل بإبراز الثمرة أو النتيجة التي أسفرت الرسالة عنها، لا أن نعيد موجز ما سبق عرضه.

وإذا كان الأمر كذلك، فإننا نستطيع القول أن النتائج التي أسفر البحث عنها تتمثل في:

1- جلب التطور العلمي الهائل للمعلوماتية عبر العالم عددا من المخاطر نجمت على إساءة استخدام الكمبيوتر عامة وشبكة الانترنت خاصة، وتطويعها لصالح المجرم المعلوماتي لممارسة نشاطاته الجرمية عبر الشبكة بكل طمأنينة وإرتياح. حيث سهلت تلك الأخيرة ظهور طائفة جديدة من الجرائم المستحدثة، تختلف عن نظيرتها التقليدية وتتميز عنها بحداثتها من حيث الأساليب و الأدوات المستعملة في تنفيذها و كذلك في أسلوب ذلك التنفيذ تعرف بجرائم الانترنت.

2- عدم وجود تعريف محدد لهذه الجرائم سواء قانونا أو فقها أو قضاء، و يرجع السبب في ذلك إلى أن التقدم التقني و العلمي في مجال الإتصالات و تكنولوجيا المعلومات و في شبكة الإنترنت أفرز مجموعة من الجرائم الجديدة و الفريدة من نوعها و المغايرة تماما لتلك التي إعتاد رجال القانون و الفقه الجنائي على التعامل معها و مكافحتها .

3- تصنف جرائم الانترنت ضمن جرائم التقنية العالية وهي نوع من الجرائم المعلوماتية و التي ترتكب غالبا في صورة سلوك إيجابي و المتميز بجملة من الخصائص ككونها عابرة للحدود وصعبة الاثبات وترتكب من قبل شخص على دراية فائقة بمجال الحوسبة يسمى بالمجرم التقني.

4- يمكن تعريف جرائم الإنترنت بأنها كل سلوك إرادي غير مشروع، صادر عن شخص مسئول جنائيا و ذا دراية فائقة بمجال الحوسبة، معاقب عليه قانونا بجزاء جنائي و تكون شبكة الإنترنت محلا له أو وسيلة لارتكابه.

5- وجوب الاتفاق على ضرورة اعتماد مصطلح سيبار كرايم للدلالة عن جرائم الإنترنت دون غيره من المصطلحات غير الدقيقة.

6- وجود فراغ تشريعي كبير في غالبية الدول العربية فيما يتعلق بجرائم الانترنت. وهذا ما ساعد مجرمي الانترنت و يسر لهم ارتكاب جرائمهم بكل راحة و هناء و بكل حرية.

7- مواجهة المشرع الجزائري للتطور التكنولوجي الذي إجتاح جميع نواحي الحياة لا سيما مجال الإتصالات السلكية و اللاسلكية من خلال القوانين التالية:

- **قانون العقوبات(المعدل بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004)**، و الذي تم بموجبه إحداث قسم جديد فيه تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات" و الذي احتوى أهم الجرائم التي تستهدف الأنظمة المعلوماتية و هي:

أ- الجرائم النصوص عليها في المادة 394 مكرر:

-الدخول خلسة للأنظمة المعلوماتية.

– البقاء غير المشروع في الأنظمة المعلوماتية.

–تعديل أو حذف معطيات المنظومة نتيجة الدخول غير المشروع.

– الإضرار بنظام تشغيل المنظومة على إثر الدخول أو البقاء غير المشروع.

ب– الجرائم المنصوص عليها في المادة 394 مكرر 1:

– إدخال معطيات في منظومة معلوماتية خلسة.

– إزالة أو تعديل معطيات في منظومة معلوماتية خلسة.

ج– الجرائم المنصوص عليها في المادة 394 مكرر 2:

– القيام عمدا و خلسة:

– بتصميم أو تجميع أو توفير أو نشر أو البحث عن معطيات تمكن من إرتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

– بحيازة أو إفشاء أو نشر أو إستعمال معطيات متحصل عليها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

د– الجريمة المنصوص عليها في المادة 394 مكرر 3:

إرتكاب الجرائم السالفة الذكر إضرارا بالدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام.

– **القانون رقم 09–04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها**، و الصادر في 05 غشت 2009 و الذي إحتوى قواعد للوقاية من الجرائم الإفتراضية و دعم وسائل مكافحتها من خلال وضع ترتيبات تسمح برصدها المبكر و جمع الأدلة عنها .

– **القانون 03–05 المتعلق بحقوق المؤلف و الحقوق المجاورة**، و الذي نص على تجريم إنتهاك حقوق المؤلف و الحقوق المجاورة عن طريق التقليد بأي وسيلة كانت بما فيها منظومة معالجة معلوماتية (المادة152).

– **القانون 2000–03 المؤرخ في 05 غشت 2000 المحدد للقواعد العامة المتعلقة بالبريد و بالمواصلات السلكية و اللاسلكية.** و الذي وضع القواعد التي تنظم مختلف شبكات المواصلات السلكية و اللاسلكية مهماكانت الوسيلة المستعملة.

و كذا **المرسوم التنفيذي رقم 98–256 المؤرخ في 25 أوت 1998 المعدل و المتمم للجزء التنظيمي من الأمر 75–89 المؤرخ في 1975/12/30 المتضمن قانون البريد و المواصلات و قانون الإجراءات الجزائية و القانون المدني و كذا قانون الإعلام....**

8– الإجرام غير المعلوماتي على شبكة الإنترنت هو نوع من جرائم الإنترنت تستخدم فيه تلك الشبكة كوسيلة لارتكاب الجريمة .أي كسلاح فتاك لارتكاب الجريمة سواء أكانت تقليدية أو مستحدثة.

9– ينقسم الإجرام غير المعلوماتي على شبكة الانترنت إلى ثلاثة أصناف، ويتمثل الصنف الأول في الجرائم الواقعة على الأشخاص ثم تليها الجرائم المقترفة ضد الأموال، وأخيرا الجرائم الماسة بأمن الدولة.

وتبعا لذلك قمنا بتقسيم دراستنا هذه إلى ثلاث أبواب تضمن كل باب جريمة من تلك الجرائم. ومن خلال دراستنا **للباب الأول** والذي تطرقنا فيه إلى الجرائم الواقعة على الأشخاص عبر الانترنت في ثلاث فصول تناولنا في كل منها الجرائم التالية جرائم البث العلني، وجرائم الإعتداء على حرمة الحياة الخاصة وجرائم المطاردة، والجرائم الأخلاقية.خلصنا فيها إلى النتائج التالية:

فيما يخص الفصل الأول:

1- تضم جرائم البث العلني الواقعة عبر الانترنت ثلاث أنواع من الجرائم هي الجرائم الماسة بسمعة الأشخاص وشرفه واعتباره عبر الإنترنت والمتمثلة في القذف والسب والتشهير الالكتروني، وجرائم الصحافة الاليكترونية والعنف عبر الانترنت. وهي جرائم في معظمها تقليدية والجديد فيها أنها ترتكب عبر الانترنت. فجرائم القذف والسب الالكتروني تتم عبر الإنترنت بواسطة إنشاء مواقع خاصة تنشر كتابات وألفاظ أو تعرض صورا أو رسومات تتضمن معاني مؤذية و خادشة لشرف وسمعة واعتبار شخص معين أو دولة من الدول أو دين من الأديان. والشأن ذاته بالنسبة لجرائم الصحافة الإلكترونية وخاصة مع ظهور مؤخرا مواقع التواصل الاجتماعي من التويتر والفايسبوك، والتي أصبحت تبث صورا نادرة وحصرية لا يستطيع التليفزيون الحصول عليها و بثها، تعمل على التحريض و على زعزعة استقرار الدول و تهديد أمنها الداخلي والخارجي على السواء ولاسيما العربية، و لعل ما يسمى بالربيع العربي خير دليل.

2- انعدام النصوص القانونية المواجهة لجريمة القذف والسب الالكتروني في معظم الدول العربية ومنها القانون الجزائري الذي اكتفى بتطبيق نصوص قانون العقوبات التقليدية و التي لا تتلاءم مع طبيعة هذه الجريمة ولا تتماشى مع المبدأ الجنائي المعروف بشرعية الجرائم و العقوبات و مع حظر القياس في الجنائي. على عكس جرائم الصحافة الالكترونية و التي عاقب المشرع الجزائري عليها من خلال قانون الإعلام رقم 05/12 وكذا في قانون العقوبات الجزائري.

فيما يخص الفصل الثاني:

1- أدى استخدام الحاسبات كبنوك معلومات إلى ظهور أخطار مستجدة غير مسبوقة لحياة الانسان الخاصة لما تحويه هذه المعلومات من أدق التفاصيل الخاصة بحياة الفرد في كافة المجالات الاجتماعية والصحية و التعليمية.

2- إن المخاطر الناجمة عن اختراق البيانات الخاصة والمعلومات السرية للأفراد (البيانات الاسمية) تشكل تهديدا مباشرا و جديا للحياة الخاصة وللحريات الفردية، وتدفع بالأفراد إلى الإحجام عن التعامل الصريح والدقيق في إعطاء المعلومات على الشبكة، بل وتقليص حجم التعامل عبرها. وهذا بلا شك سوف يعمل على تقليل فرص التطور والتقدم العلمي والتقني الذي تسعى الشبكة الدولية إلى تطويره وإنمائه.

3- تقوم جريمة الإعتداء على الحياة الخاصة عبر الانترنت أساسا على مبدأ التمركز في موقع معين داخل شبكة الإنترنت. وهي تعتبر من أخطر جرائم الإجرام غير المعلوماتي على شبكة الإنترنت، نظرا لعدم وجود

الحماية التقنية الفاعلة لما يتم تداوله من معلومات وأسرار ومراسلات بطريق الإنترنت و الذي يعد طريقا مطروقا يقصده كافة الناس، و تعتبر فيه حياة الفرد كالكتاب المفتوح يقرؤه كل الناس.

4- من الأساليب الإجرامية الشائعة في الإعتداء على حرمة الحياة الخاصة عبر الإنترنت: استعمال بيانات شخصية غير حقيقية، جمع أو معالجة بيانات حقيقية بدون ترخيص، إنشاء بيانات بصورة غير قانونية وإساءة استعمالها، عدم الالتزام بالقواعد الشكلية الخاصة بتنظيم عملية وجمع ومعالجة ونشر البيانات الشخصية.

5- حرصت كافة تشريعات الدول على صيانة الحياة الخاصة للأفراد من مخاطر بنوك المعلومات وذلك إما بالنص على حمايتها في صلب دساتيرها أو تشريعاتها الوطنية. ولقد تصدى المشرع الجزائري صراحة لذلك من خلال نصوص قانون العقوبات بدء من المادة 303 مكرر إلى 303 مكرر 3 من قانون 06- 23 المؤرخ في 2006/12/20 المعدل والمتمم لقانون العقوبات والتي جرمت كل أنواع المساس بحرمة الحياة الخاصة باستخدام وسائل التكنولوجيا الحديثة .

6- المطاردة عبر الإنترنت هي القيام بمجموعة أفعال تقوم على أساس فكرة الخوف من أفعال تجعل المجني عليه يعتقد اعتقادا جازما بأنه عرضة لنتائج إجرامية من نوع ما، و ذلك إما عن طريق استخدام البريد الإلكتروني أو حلقات النقاش وغرف الدردشة، أو عن طريق إنشاء موقع ويب خاص بالجاني. وتعتبر جريمة التهديد من أشهر جرائم المطاردة عموما.

7- انعدام النصوص القانونية المواجهة لجريمة المطاردة عبر الانترنت في غالبية الدول العربية ومنها القانون الجزائري الذي صمت واكتفى بتطبيق نصوص قانون العقوبات التقليدية.

فيما يخص الفصل الثالث:

1- تتم جرائم انتهاك الآداب العامة عبر الإنترنت عن طريق نشر وبث الصفحات الخادشة والمخلة بالحياء عبر مواقع الإنترنت، أو إنتاج أو إعداد أو تهيئة أو إرسال أو تخزين أو ترويج أي محتوى يخل بالحياء أو النظام العام والآداب عن طريق شبكة المعلومات. ويقصد بها كل فعل يتضمن مخالفة القواعد الأخلاقية الأساسية التي يبنى عليها المجتمع وكذا تعاليم كافة الأديان السماوية و ذلك باستخدام الانترنت.

2- غياب المواجهة القانونية لمثل هذه الجريمة التقليدية الواقعة عبر الانترنت في غالبية القوانين العربية ومن بينها القانون الجزائري.

3- تحميل بعض القوانين مثل القانون الأردني والجزائري المسؤولية الجنائية الكاملة لمقدمي ومزودي خدمات الإنترنت عن المادة المنشورة والمواقع التي يقومون باستضافتها،و ذلك إذا قاموا أو ساهموا بتقديم خدمات اتصال مخالفة للنظام العام والآداب العامة. في حين اكتفت غيرها بوضع برامج البروكسي لتلك المواقع من قبل المؤسسات المعنية بالاتصالات أو الهيئة المختصة بتزويد المشتركين بخدمات الإنترنت.

4- ترتكب الجرائم الجنسية عبر الإنترنت إما عن طريق تخصيص مواقع خاصة لذلك، تبث أفلاما خليعة أو مقالات فاضحة أو صورا ماجنة سواء كانت للكبار أو الصغار. أو عن طريق ما يسمى بالدردشة الإباحية والقوائم البريدية الجنسية.

5- تعتبر سهولة إنشاء هذه المواقع والوصول إليها وكذا تحميل الملفات الإباحية السبب الرئيسي والمباشر في انتشار هذه الجريمة.

6- الدافع الرئيسي وراء نشر الجنس و الإباحية عبر الإنترنت هو السعي وراء تحقيق الربح المادي.

7- تعتبر الفئة الشبابية الذين يتراوح أعمارهم ما بين 12-15 سنة أكثر ضحايا هذه الجريمة لاسيما الأطفال الصغار الذين يتم فيما بعد استغلالهم جنسيا.

8- حرصت غالبية التشريعات المقارنة على مكافحة هذه الجريمة الواقعة عبر الانترنت لا سيما تلك التي يستغل فيها الأطفال جنسيا. ولقد تناول التشريع الجزائري هذه الجريمة من خلال المادة 344 و394 مكرر2 قانون العقوبات الجزائري وإن أغفل توفير الحماية الجنائية للأطفال من الاستغلال الجنسي لهم عامة و عبر الانترنت خاصة.

أما فيما يخص **الباب الثاني** فخصصناه للجرائم الواقعة على الأموال عبر الإنترنت، وقسمناه كنظيره إلى ثلاث فصول تطرقنا في كل منها إلى جريمة السرقة و النصب و كذا جريمة الإعتداء على الملكية الفكرية الواقعة عبر الانترنت في الفصل الأول والتي تعتبر جرائم مالية تقليدية؛ وجريمة غسل الأموال والمخدرات في الفصل الثاني والجرائم الواقعة على التجارة الإلكترونية والتي تعتبر جرائم مالية مستحدثة. وخلصنا من خلالها إلى النتائج التالية:

فيما يخص الفصل الأول:

1- تعد جرائم السرقة والنصب والإعتداء على الملكية الفكرية جرائم تقليدية تقع على الأموال المنقولة سواء أكانت مادية أو معنوية.

2- أن السرقة عبر الإنترنت تعتبر نوعا من السرقة المعلوماتية، و هي تقع على المال المعلوماتي أين تستخدم فيها الإنترنت كأداة تخزين وحيازة و تعامل بهذا المال. وهي عبارة عن اختلاس للمعلومات ونقلها من حيازة صاحبها إلى الغير باستخدام الانترنت.

3- أدى التطور الذي حدث في مجال تكنولوجيا المعلومات إلى إعطاء الأموال المعنوية قيمة اقتصادية قد تفوق قيمة الأموال . وهذا التطور هو الذي أدى بالفقه الحديث إلى اعتماد معيار آخر غير معيار مادية المال أو طبيعة الشيء الذي يرد عليه الحق المالي ليصل من خلاله إلى إسباغ صفة المال على الشيء المعنوي و لجأ في ذلك إلى معيار القيمة الاقتصادية للشيء. حيث يعتبر الشيء مالا لا بالنظر إلى ماله من كيان مادي وإنما بالنظر إلى قيمته الاقتصادية. وهذا ما دفع بأغلبية التشريعات على تطبيق النصوص التقليدية لجرائم الأموال على جريمة السرقة عبر الانترنت.

4- يرجع السبب الرئيسي في الحيلولة دون تطبيق النصوص التقليدية لجريمة السرقة في مجال البرامج ولبيانات عبر الانترنت إلى كونها ذات طبيعة غير مادية أو معنوية و هذا ما أدى إلى

اختلاف الآراء الفقهية حول طبيعة المعلومات المتداولة عبر الإنترنت،أهي مال أم لا؟ وبالتالي هل يصح تكييف الاستيلاء عليها بالسرقة؟.

و في نظرنا تعتبر هذه المعلومات المتداولة عبر الإنترنت أموالا منقولة ذات طبيعة معنوية لها قيمة اقتصادية و تجارية، فهي تقبل التخزين و النقل و يمكن حبسها و إطلاقها.

هذا من جهة ومن جهة أخرى، فانه باستقرائنا للتعريف الذي وضعناه للسرقة عبر الإنترنت نستخلص أن هذه المعلومات قد تكون محلا للقرصنة المعلوماتية عن طريق نسخ الملفات أو نقل محتوى المعلومات باستخدام الفيروسات ودود لإنترنت.أي يتم الإعتداء فيها على المنتجات الفكرية أو ما يعرف بحق المؤلف، و في هذه الحالة تكيف الجريمة بأنها سرقة ويعاقب صاحبها بعقوبة السرقة دون الإخلال بالعقوبة الخاصة بالإعتداء على الملكية الأدبية والفنية والواردة في قانون حماية حقوق الملكية الفكرية.و في المقابل قد تكون تلك المعلومات محلا للاختلاس وذلك في حالة سرقة بطاقات الائتمان أو الدخول إلى حساب العملاء وسرقتهم. وفي هذه الحالة تكيف الجريمة بأنها سرقة و تطبق عليها النصوص الخاصة بالسرقة التقليدية.وهناك حالة ثالثة يتم فيها سرقة المعلومات الخاصة بالأفراد والدول، أي التعدي على حرمة الحياة الخاصة أو التجسس على الدول. وتكيف الجريمة هنا أيضا بأنها سرقة ويعاقب صاحبها بعقوبة السرقة دون الإخلال بالعقوبة المنصوص عليها في جريمة الإعتداء على الحياة الخاصة إلى جانب نصوص التجسس.

5- تحتل جريمة النصب المرتبة الأولى في الجرائم الواقعة على الأموال عبر الإنترنت في العالم الإفتراضي و أغلبها يقع على بطاقات الائتمان؛وهو نوع من الاحتيال المعلوماتي.

6- يأخذ النصب عبر الإنترنت عدة أشكال نذكر منها:إرسال رسائل غير مرغوب فيها عن طريق البريد الإلكتروني،إعداد مزادات خادعة عبر الإنترنت، الاستيلاء على متعلقات الهوية، الاحتيال في نقل الأموال إليكترونيا...

7- تعتبر جريمة التقليد عبر الإنترنت من أخطر و أشهر جرائم الإعتداء على الملكية الفكرية لاسيما جرائم الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت.

8- محل الإعتداء في هذه الجرائم هو المصنفات الرقمية المحمية التي يجب أن تتوفر فيها شروط معينة لاسيما شرط الابتكار.

9- يمكن حصر السلوك الإجرامي في جريمة النسخ الإلكتروني غير المشروع في ثلاث صور: العرض عبر الإنترنت لإعلان مبتكر ثم إعداده للبث بطرق تقليدية معتادة،الإنزال والتحميل، التحول إلى الرقمية.

10- تصدى المشرع الجزائري لجرائم الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت من خلال الأمر 05/03 المتعلق بحق المؤلف والحقوق المجاورة وذلك بعد اعترافه الصريح على اعتبار برامج الحاسب الآلي هي من المصنفات المحمية.

فيما يخص الفصل الثاني:

1- تعتبر جريمة غسل الأموال عبر الإنترنت جريمة حديثة تعود فكرتها إلى عصابات الجريمة المنظمة. وهي تجد نفسها في عمليات الصيرفة الإلكترونية بالخصوص، و هي عبارة عن إظهار الأموال المتحصلة من جرائم الاتجار بالتجارة غير المشروعة مثل المخدرات و الإرهاب والقمار وغيرها بصورة تتمتع بقانونية المصادر وشرعيتها عبر استخدامها لشبكة الإنترنت كأداة لإخفاء هذا المصدر غير المشروع أو ذاك الذي تحصلت منه هذه الأموال.

2- تستهدف عمليات غسل الأموال عبر الانترنت نقل التحصيلات من الدوائر التابعة لأنشطة القمار والمخدرات والبغاء وتجارة السلاح عبر مصارف ومؤسسات مالية قانونية،و ذلك باستخدام الانترنت.

3- إن ما يسهل عمليات تبييض أو غسل الأموال عبر الإنترنت، هو أن شروط التعامل على الشبكة الدولية لا تتطلب إجراءات معقدة.

4- تمر جريمة غسل الأموال عبر الإنترنت أو التبييض الإلكتروني بنفس المراحل التي تمر بها تلك الجريمة في صورتها التقليدية، و هي ثلاث مراحل مرحلة الإحلال و مرحلة التجميع و مرحلة الإدماج؛ إلا أن الفرق بينهما يكمن في استخدام الإنترنت في تلك الدورة.

5- لم يعالج المشرع الجزائري جريمة غسل الأموال عبر الإنترنت بنصوص صريحة و اكتفى بتجريم هذه الجريمة في صورتها التقليدية أي المرتكبة بالطرق التقليدية من خلال القانون رقم 06-23 المعدل و المتمم لقانون العقوبات و القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها.

6- تعتبر جريمة المخدرات عبر الإنترنت أو ما يصطلح عليه إجرام تكنلجة المخدرات والمؤثرات العقلية، إجرام حديث تستخدم فيه الإنترنت كوسيلة لتسهيل التعامل غير المشروع (و ذلك عن طريق الاتجار، الترويج، التوزيع، التعاطي، تبيان كيفية زراعة وصناعة تلك المواد السامة) بالمؤثرات العقلية و المخدرات.

7- أدى الاستعمال السيئ للإنترنت إلى خلق أو ظهور أنواع جديدة من المخدرات والمؤثرات العقلية وعلى شرح طرق الحصول على تراخيص إنتاجها باستخدام التكنولوجيا، كما لو استخدم الحاسوب في تأهيل نظم الإنتاج واختيارات البدائل المختلفة في تصنيفها أو زراعتها.

8- لم ينص المشرع الجزائري صراحة على جريمة تكنلجة المخدرات و المؤثرات العقلية ولكن يمكن القول بتطبيق المواد الواردة في القانون رقم 04- 18 المؤرخ في 2004/2/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها و لا سيما المادة 15 و 17 و 22 من ذلك القانون و كذلك يمكن تطبيق المادة 394 مكرر2 من قانون العقوبات.

فيما يخص الفصل الثالث:

1- تضم جرائم الإعتداء على التجارة الالكترونية عبر الانترنت: جرائم الإعتداء على نظم المعالجة الآلية للبيانات، والتي تقع على مواقع التجارة الالكترونية وغيرها من المواقع على شبكة الإنترنت عن طريق

الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات و إما عن طريق الإخلال بنظام المعالجة الآلية و ذلك بالإدخال أو المحو أو التعديل.
وجرائم تقع على بيانات التجارة الالكترونية وتشمل جريمة التعامل في البيانات بدون ترخيص،جريمة انتهاك سرية و خصوصية البيانات وجريمة التصريح عمدا بمعطيات خاطئة.

وجرائم تقع على بطاقات الائتمان و التي تكون من خلال إلتقاط أرقام هذه البطاقات و السطو عليها (إما عن طريق سرقتها و الإستيلاء عليها أو النصب و الإحتيال) عبر قنوات الإنترنت المفتوحة و استخدامها بطريقة غير مشروعة في عمليات التسوق عبر تلك الشبكة، و ذلك بخصم قيمة السلع من العملاء الشرعيين لها . و التلاعب بهذه البطاقات لا يقتصر على الغير فقط بل يتعدى إلى حاملها الشرعي و ذلك في حالتين: حالة تجاوز حامل البطاقة للرصيد خلال فترة صلاحيتها و حالة استخدام الحامل الشرعي للبطاقة بعد إلغائها أو انتهائها.
وأخرى يقع فيها الإعتداء على التوقيع الالكتروني، وذلك إما بإتلافه أو استنساخه أو تزويره أو تقليده أو استعماله و هو مزورا مع علمه بذلك أو إفشاء بياناته أو استعماله في القرض المقدم من أجله.

2-عالج المشرع الجزائري جرائم الإعتداء على نظم المعالجة الآلية للبيانات فجرم فعل الدخول العمدي أو البقاء غير المشروع في منظومة معلوماتية بغير وجه حق في المادة 394 مكرر قانون العقوبات. و جرم وعاقب على جريمة الإخلال بنظام المعالجة الآلية من خلال المادة 394 مكرر 1 و 394 مكرر 2 قانون العقوبات. كما عالج جرائم الإعتداء على بطاقات الائتمان من خلال القسم السابع مكرر من قانون العقوبات الجزائري في المواد 394 مكرر و 394 مكرر1 . أما فيما يخص جرائم الإعتداء على التوقيع الإلكتروني فلم يستحدث المشرع الجزائري نصوصا عقابية لمواجهة هذه الجرائم و التي تكون إما بتزويره أو بإفشاء بياناته أو استخدامها في غير الغرض المقدم من أجله إلى غيرها من السلوكيات الاجرامية التي يمكن أن يكون محلا لها و التي لايمكن التحدث عنها إلا إذا كان المحرر هو عبارة عن مستند معلوماتي.
3- أما فيما يخص **الباب الثالث** فتناولنا فيه الجرائم الواقعة على أمن الدولة عبر الإنترنت و التي هي جرائم مستحدثة،و حصرناها في فصلين وتطرقنا فيهما إلى جريمة الإرهاب عبر الإنترنت و جريمة التجسس عبر الإنترنت. و خلصنا من خلال تحليلهما إلى النتائج التالية:
1- يعد الإرهاب عبر الإنترنت نوع من أنواع الإرهاب الالكتروني أو الرقمي. و هو يعتمد أساسا على استخدام التقنية العالية في ارتكاب الجريمة.
2- الإرهاب عبر الانترنت هو تعبير يشمل مزج مصطلح التهديد بنظم المعالجة الآلية للمعلومات لاستخدام تقنية الاتصالات الحديثة / الانترنت
3- من أشكاله:قيادة الجماعات الإرهابية، القصف الإلكتروني،....
4- محل الإعتداء في الإرهاب عبر الإنترنت:الأشخاص+ الممتلكات+ نظم المعلومات.
5- الهدف الأول والأخير في الإرهاب عبر الإنترنت هو ضرب البنى التحتية و الأساسية للدول.

6- تصدت معظم التشريعات لظاهرة الإرهاب عبر الانترنت و من بينها التشريع الجزائري الذي عانى من ويلاته كثيرا من خلال قانون العقوبات والقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والمتمم لقانون العقوبات وذلك في المادة 4 التي تسمح باللجوء إلى المراقبة الإلكترونية و المادة 87 مكرر و 394 مكرر2 و 3 من قانون العقوبات الجزائري.

7- كان من نتيجة استخدام شبكة الانترنت والربط بينها عن طريق الخطوط الهاتفية و القمر الصناعي ووسائل الاتصال الحديثة إضعاف قبضة الأمن والتحكم والمراقبة على الكم الهائل من المعلومات التي تزخر بها و تقدمها، مما جعلها بيئة صالحة لعمليات التجسس من قبل قوى داخلية أو خارجية معادية للدولة على المعلومات الخاصة بالهيئات الحكومية والخاصة والتي يساء استخدامها. و يعتبر التجسس عبر الانترنت أحد أشكال التجسس الحديث وبالضبط التجسس الالكتروني.

8- من الأساليب الحديثة المستعملة في التجسس عبر الإنترنت:أسلوب إخفاء المعلومات داخل المعلومات، استخدام حصان طروادة.

9- يهدف التجسس عبر الإنترنت إلى جمع مجموعة من المعلومات تضم: معلومات اقتصادية وصناعية، بيانات سياسية و عسكرية و بيانات شخصية.....

10- لقد جرمت معظم التشريعات العقابية جريمة التجسس عبر الانترنت و منها التشريع الجزائري الذي تناولها من خلال قانون العقوبات في المادة 2/63 و 394 مكرر 3.

التوصيات

من خلال النتائج التي توصلنا إليها والسابق الانتهاء منها نود أن نوصي بعدد من التوصيات التي نرى أنها هامة. ولهذا نوصي بما يلي:

- ضرورة التدخل التشريعي لمواجهة القصور في التشريعات و القوانين الحالية، أو تحديثها بالنص صراحة على تجريم استخدام شبكة الإنترنت كتقنية علمية عالية و حديثة للإضرار بالأشخاص والأموال والدول.

- وضع قانون للإنترنت يشمل في أحد جوانبه تجريم جرائم الإنترنت بنوعيها المعلوماتي و غير المعلوماتي في شبكة الإنترنت (بشقيه الموضوعي والإجرائي).

استعمال أساليب التقنية لمواجهة جرائم الإنترنت (وإن كان بعضها قد تم الاستعانة به) ، كالتشفير واستخدام أسلوب تنقية المواقع في شبكة الإنترنت أو أسلوب الغفلية في هذه الشبكة أو استخدام تقنية الجدار الناري أو أسلوب استخدام المزايا البيولوجية في شبكة الإنترنت....

- ضرورة إنشاء مراكز قومية لآمان الحاسبات و المعلومات و الإنترنت.

- ضرورة تدريس مناهج خاصة بالحاسوب و المعلوماتية من قبل متخصصين في المراحل التعليمية المختلفة مع توفير معامل و مختبرات كاملة لعدد فصل دراسي أو فصلين يعملان على أجهزة الحواسيب المربوطة بالإنترنت.

- ضرورة تسجيل أسماء الأشخاص الذين يستخدمون الشبكة في مقاهي الإنترنت و المدة التي استغرقوها.

– ضرورة نشر الوعي والثقافة المطلوبة لدى مستخدمي الإنترنت حتى لا يكونوا صيدا لأعمال نصب واحتيال عن طريق الشبكة، وحتى لا يكونوا ضحايا لأي فعل غير مشروع تستخدم فيه تلك الشبكة.

– ضرورة تجريم استضافة المواقع الإباحية وكذا كل تداول للمواد الإباحية الخاصة بالأطفال بصفتها أسوء مجال في الإباحية الالكترونية، وتشديد العقاب عليها.

التنسيق و تبادل المعلومات والخبرات بين الأجهزة المعنية بمكافحة الإرهاب عبر الإنترنت في كافة دول العالم.

– التدريب و تبادل المعدات والأساليب الكفيلة بالتعامل مع المنظمات الإرهابية التي تتخذ من الإنترنت وسيلة لمباشرة نشاطها.

– ضرورة افتتاح العديد من المواقع التي توضح مدى خطورة التعامل مع الدعوات التي تطلقها بعض الجهات غير المعروفة، و توجيه الشباب إلى مواقع لها القدرة على الحوارات الترفيهية لإقناع من يكون لديه نزعة التطرف، و تشديد العقوبات الصارمة على بعض المواقع التي تؤيد أو تروج لمثل هذه المواقع عبر الإنترنت. و للوقاية من أي اتجاهات متطرفة، يجب تعويد الطفل منذ المرحلة الأولى في تنشئته على الحوار والمناقشة ثم تستكمل وقايته من أي اتجاهات متطرفة من خلال التعليم الرسمي بتحريك جو المدرسة إلى جو تفاعلي عوضا عن الاستسلام و القبول بالتلقين و الحقن، و طبعا لا يتم ذلك إلا في جو تربوي منفتح. و على المستوى المجتمعي يتطلب الأمر فكرا متقبلا للتسامح مروجا للوسطية في كل الأمور.

– تجنب الدخول إلى المواقع المجانية، لاسيما أثناء التصفح للمواقع،إذ أنها في الغالب تخفي وراءها شيئا ما.

– غلق المواقع التي تحتوي على تصميمات و صور لتجنب التعدي على حرمة الحياة الخاصة.

– الاستعانة بقراصنة المعلومات نظرا لأنهم يمتلكون خبرة و دراية في عمليات اختراق الشبكة ومهاجمتها وتوظيفهم كمراقبين و رجال أمن لحماية الشبكة. إضافة إلى تدريب كوادر جديدة لحماية الشبكة من الجريمة.

– إلزام مقدمي خدمة الإنترنت في جميع الدول العربية – كما هو متعامل به في المملكة العربية السعودية– بتطبيق عدد من الإجراءات الفنية لمنع أعمال المتسللين و إساءة استخدام البريد الإلكتروني وغيرها من المخالفات المتعلقة بالجوانب الأمنية لاستخدام شبكة الإنترنت.و من بين هذه الإجراءات:منع انتحال أرقام الإنترنت، العمل على منع إساءة استخدام البريد الإلكتروني أو ما يسمى البريد المهمل أو غير المرغوب فيه، الاحتفاظ بسجل استخدام مزود الاتصالات الخاص بالمشتركين، وسجل استخدام البر وكسي لمدة لا تقل عن السنة، الحصول على خدمة الوقت عن طريق وحدة البر وكسي و مزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات،تحديث سجلات منظمة رايب الخاصة بمقدمة الخدمة، ضرورة تنفيذ ما تتوصل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبة المخالفات الأمنية.

– ضرورة تفعيل التعاون الدولي لمكافحة جرائم الإنترنت، و ذلك عن طريق العمل على إيجاد قدر ممكن من التناسق و التطابق فيما بين قوانين الدول المختلفة و المتعلقة بمكافحة جرائم الإنترنت فلا يكون الفعل الذي يتم ارتكابه جريمة في بلد ما وغير معاقب عليه في قانون بلد آخر. فمن هنا يجد المجرمون الملاذ الآمن الذي يلجئون إليه دون أي اعتبار لما ارتكبوه من جرائم.
هذا من جهة و من جهة أخرى، تعاون جميع الدول على تسليم المطلوبين أمنيا إلى الدول التي تطالب بهم لارتكابهم جرائم إنترنت.

– ضرورة تعديل نصوص قانون العقوبات الجزائري باضافة مواد قانونية تجرم و تعاقب على جرائم الإنترنت و توقع أشد العقوبات على مرتكبيها و كل من يستعمل هذه الشبكة في غير نطاقها الإيجابي بتقرير جزاءات جنائية مشددة و صارمة و ذلك من خلال التصويت على مشروع القانون الخاص بتلك الأخيرة، فبالرغم من توفيره للحماية الجنائية لأنظمة المعالجة الآلية للمعطيات في القسم السابع مكرر من قانون العقوبات إلا أن هذا غير كاف فأنظمة المعالجة الآلية للمعطيات لا تعني بالضرورة الإنترنت .
هذا من جهة و من جهة أخرى، فان المشرع الجزائري بمعاصرته للتطور التكنولوجي الذي إجتاح جميع نواحي الحياة لا سيما مجال الإتصالات السلكية و اللاسلكية ومواجهته له من خلال القوانين 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، و قانون العقوبات و الإجراءات الجزائية و القانون المدني و كذا قانون الإعلام..... فهذا غير كاف لمكافحة و مواجهة جرائم الإنترنت، و ذلك لأن هذه القوانين تعالج في نصوصها الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و كذا عددت الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و التي تعتبر جزء من ظاهرة إجرامية حديثة و خطيرة تسمى بالجريمة المعلوماتية.....
– ضرورة إعتراف المشرع الجزائري بأن جرائم الإنترنت هي جرائم مستحدثة تنتمي إلى جرائم المعلوماتية تستوجب أحكام قانونية خاصة و صريحة سواء من الناحية الموضوعية أو الإجرائية، و التي حيرت كل رجال القانون من ضبطية قضائية و قضاة إذ يستوجب التعامل فيها بالتحلي بالخبرة العالية و الفطنة بالنسبة لأعضاء الضبطية القضائية، و يعتمد القاضي الجزائي في الحكم فيها على نصوص قانونية توائمها و تلائم المسرح المرتكبة فيه.
– ضرورة توفير الحماية الجنائية للأطفال و لا سيما الإستغلال الجنسي لهم عبر هذه التقنية في القوانين الجزائرية. فبالرغم من النظام الجديد لحجب المواقع الإرهابية و الإباحية و غير المرغوب فيها الذي أطلقته شركة إتصالات الجزائر تحت تسمية " في أمان" و الذي من خلاله يسمح للأولياء بمراقبة حركة تصفح الإنترنت لأبنائهم لحمايتهم من التأثيرات السلبية لتلك المواقع غير المرغوب فيها و كذا الإدمان على الإنترنت من خلال ضبط التوقيت الذين يرونه مناسبا فهذا غير كاف بل يجب حماية هذه الفئة الحساسة بقوانين عقابية تعاقب كل من تسول له نفسه المريضة بالإساءة إليها بعقوبات قاصية و شديدة نظرا لحساسية هذه الفئة و سهولة إعتبارها أسهل الأطعم.

– ضرورة إقامة مرصد مراقبة في الجزائر يعهد إليه بحفظ أمن الشبكة الالكترونية على الصعيدين الإقليمي والدولي على غرار تجربة فرنسا والولايات المتحدة الأمريكية وكوريا الجنوبية وبريطانيا.

– ضرورة التكثيف من الحملات الوطنية التحسيسية وعقد ندوات علمية تبين مدى الجانب السلبي للانترنت.

قائمة المراجع:

أولا: المراجع باللغة العربية:

الكتب:

المراجع العامة:

د/ إبراهيم عيد نايل:المواجهة الجنائية لظاهرة غسل الأموال في القانون الجنائي الوطني والدولي، بدون دار النشر، 1997.

د/ابراهيم عيد نايل:السياسة الجنائية في مواجهة الإرهاب، دار النهضة العربية، القاهرة، 1996.

د/ أحسن بوسقيعة:الوجيز في القانون الجزائي العام، الطبعة الرابعة، دار هومة، الجزائر، 2006.

أحمد أبو الروس: الإرهاب والتطرف والعنف في الدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2001.

أحمد أبو الروس: مشكلة المخدرات و الإدمان، دار المطبوعات الجامعية، الإسكندرية، بدون سنة طبع.

أحمد عبد الحكيم عثمان: الجرائم الدولية في ضوء القانون الدولي في الجنائي والشريعة الإسلامية، دار الكتب القانونية، مصر، 2009.

د/ أحمد شوقي أبو خطوة: شرح الأحكام العامة لقانون العقوبات الاماراتي، الطبعة الأولى، الجزء الأول، 1989.

د/ أحمد شوقي أبو خطوة: جرائم الإعتداء على الأموال، القسم الخاص، دار النهضة العربية، القاهرة،1994.

د/أحمد السيد عفيفي: الأحكام العامة للعلانية في قانون العقوبات، القاهرة، 2001.

د/أحمد فتحي سرور: الوسيط في قانون العقوبات، القسم الخاص، الطبعة الرابعة، دار الطباعة الحديثة، القاهرة، 1990.

د/ أحمد فتحي سرور: الوسيط في قانون العقوبات، القسم العام، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991.

د/ أسامة عبد الله قايد:الحماية الجنائية لحق المؤلف، مركز البحوث و الدراسات القانونية بكلية الحقوق، جامعة القاهرة، دار النشر هاتيه، 1990.

د/أسماء بنت عبد العزيز الحسين: أسباب الإرهاب و العنف و التطرف، دراسة تحليلية، 2002.

د/ إسحاق إبراهيم منصور: نظريتا القانون و الحق و تطبيقاتهما في القوانين الجزائرية، ديوان المطبوعات الجامعية، الجزائر، 1992.

د/ إدوار غالي الذهبي: جرائم المخدرات، الطبعة الثانية، مكتبة غريب، القاهرة، 1988.

د/ جلال ثروت: نظم القسم العام في قانون العقوبات، طبعة منقحة، دار الهدى للمطبوعات، الإسكندرية.

د/ جميل عبد الباقي الصغير: قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1998.

د/ حبيب إبراهيم الخليلي: المدخل للعلوم القانونية، النظرية العامة، الطبعة الثامنة، ديوان المطبوعات الجامعية، الجزائر، 2006.
د/ حسين فريجة: شرح قانون العقوبات الجزائري،جرائم الأشخاص – جرائم الأموال، ديوان المطبوعات الجامعية، الجزائر، 2006.
د/ حسن صادق المرصفاوي: قانون العقوبات الخاص، منشأة المعارف، الإسكندرية،1991.
د/دياب البدانية: مواجهة الجريمة المنظمة العابرة للحدود الوطنية،من المحلية إلى الكونية،جامعة المؤتة، الأردن.
د/دردوس مكي: القانون الجنائي الخاص في التشريع الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر، 2007.
د/رمسيس بهنام: قانون العقوبات، القسم الخاص، العدوان على أمن الدولة الداخلي، منشأة المعارف، الإسكندرية، 1982.
د/رؤوف عبيد: جرائم الإعتداء على الشخاص و الموال، الطبعة الثامنة، دار الفكر الجامعي، 1985.
سعد الأعظمي: التجسس في التشريع العراقي، دار الكتب للطباعة و النشر، الموصل، 1981.
د/ سليمان عبد المنعم: القسم العام من قانون العقوبات، دار الجامعة الجديدة، الإسكندرية، 2002.
د/ زكي أبو عامر،د/ سليمان عبد المنعم: القسم العام من قانون العقوبات، دار الجامعة الجديدة، الإسكندرية، 2002.
شريف سيد كامل: الجريمة المنظمة في القانون، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001.
شريف سيد كامل: جرائم الصحافة في القانون المصري، الطبعة الثانية، دار النهضة العربية، القاهرة،1997.
طارق سرور: قانون العقوبات، القسم الخاص، جرائم الإعتداء على الأشخاص، دار النهضة العربية، القاهرة،2000.
د/ عبد المجيد زعلاني: قانون العقوبات الخاص، الطبعة الثانية، دار هومة، الجزائر.
عبد الفتاح الصيفي: الأحكام العامة للنظام الجنائي في الشريعة الإسلامية و القانون، دار النهضة العربية، القاهرة، 2004.
عبد الله سليمان: شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول، "الجريمة"، ديوان المطبوعات الجامعية، الجزائر، 1996.
عبد الله سليمان: شرح قانون العقوبات الجزائري، القسم العام، الجزء الثاني، "الجزاء الجنائي"، الطبعة الرابعة، ديوان المطبوعات الجامعية، الجزائر، 2005.
علاء الدين راشد: المشكلة في تعريف الإرهاب، دار النهضة العربية، القاهرة، 2006.
عبد القادر زهير النقوزي: المفهوم القانوني لجرائم الإرهاب الداخلي و الدولي، الطبعة الأولى، منشورات الحلبي الحقوقية، 2008.

علي حسين الخلف، سلطان عبد القادر الشادي: المبادىء العامة في قانون العقوبات العراقي، وزارة التعليم العالي والبحث العلمي، العراق، 1982.

علي عبد القادر القهوجي: شرح قانون العقوبات، القسم العام، الكتاب الأول، دار المطبوعات الجامعية، الإسكندرية، 1997.

علي عبد القادر القهوجي: مبادئ علم الإجرام، مؤسسة الثقافة الجامعية،الإسكندرية، 1992.

عياد عبد العزيز: تبييض الأموال و القوانين و الاجراءات المتعلقة بالوقاية منها ومكافحتها في الجزائر، الطبعة الأولى، دار الخلدونية، 2007.

عبد الفتاح سليمان: مكافحة غسل الأموال، الطبعة الأولى، دار علاء للطباعة و النشر، القاهرة، 2004.

د/ عبد العزيز سعد: الجرائم الأخلاقية في قانون العقوبات، الشركة الوطنية للنشر و التوزيع، عمان،2005.

د/عدلي أمير خالد: المستحدث في جرائم الإعتداء على الأشخاص في ضوء المستحدث من القوانين وأحكام النقض و المحكمة الدستورية العليا، دار الفكر الجامعي، الإسكندرية، 2013.

د/ عوض محمد:جرائم الأشخاص و الأموال، دار المطبوعات الجامعية،الإسكندرية،1984.

د/ فاضلي إدريس:المدخل إلى الملكية الفكرية، الملكية الأدبية و الفنية و الصناعية، جامعة الجزائر، دار هومة، 2004/2003.

د/ فتوح عبد الله الشاذلي: قانون العقوبات، القسم العام، الكتاب الأول، دار المطبوعات الجامعية، الإسكندرية،1998.

د/ فوزية عبد الستار: شرح قانون العقوبات، القسم العام، دار النهضة العربية،القاهرة،1992.

فرحة زراوي صالح: الكامل في القانون التجاري الجزائري، الحقوق الفكرية، حقوق الملكية الصناعية والتجارية حقوق الملكية الأدبية و الفنية، إبن خلدون للنشر و التوزيع، وهران، 2006.

لعشب علي: الإطار القانوني لمكافحة غسل الأموال، ديوان المطبوعات الجامعية، الجزائر.

د/ محمد زكي أبو عامر:قانون العقوبات، القسم العام، دار الجامعة الجديدة، الإسكندرية، 2007.

محمد سامي الشوا: سياسية جنائية في غسل الأموال، دار النهضة العربية، القاهرة.

محمد راحي: جريمتا السرقة و الإبتزاز، دراسة مقارنة، دار الهدى،الجزائر، 2006.

د/ محمود صالح العادلي: الجريمة الدولية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2003.

د/ محمود نجيب حسني: شرح قانون العقوبات، القسم العام، الطبعة السابعة، دار النهضة العربية، القاهرة، 1989.

د/ محمود نجيب حسني: شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة،1988.

د/ مدحت رمضان: دروس في قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1998.

د/ معز أحمد محمد الحيارى: الركن المادي للجريمة، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2010.

معوض عبد التواب: القذف و السبب و البلاغ الكاذب و إفشاء الأسرار و شهادة الزور، دار المطبوعات الجامعية، الاسكندرية، 1988.

د/ ماجد راغب الحلو: قانون حماية البيئة في ضوء الشريعة، دار الجامعة الجديدة، الإسكندرية، 2004.

د/ ماجد راغب الحلو: القانون الإداري، دار الجامعة الجديدة، الإسكندرية، 2004.

د/ مأمون سلامة:قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، الجزء الأول، دار الفكر الجامعي، القاهرة، 1988.

د/ محمد الفاضل:الجرائم الواقعة على أمن الدولة، الطبعة الرابعة، المطبعة الجديدة، دمشق، 197هـ-1978.

محمد راكان الدغمي: التجسس وأحكامه في الشريعة الإسلامية، الطبعة2، دار السلامة، بيروت، 1985.

د/محمد سليمان موسى: الجرائم الواقعة على أمن الدولة، دراسة مقارنة في التشريعات العربية و القانونين الفرنسي و الإيطالي في ضوء المفاهيم الديمقراطية الدستورية و مبادئ حقوق الإنسان، دار المطبوعات الجامعية، الإسكندرية،2009.

د/محمد صبحي نجم: شرح قانون العقوبات الجزائري، القسم الخاص، ديوان المطبوعات الجامعية، الجزائر،2000.

د/ محمود سعيد: جرائم الإرهاب، أحكامها الموضوعية واجراءت ملاحقتها، الطبعة الأولى ، دار الفكر الجامعي، الإسكندرية، 1995.

مصطفى طاهر:المواجهة التشريعية بظاهرة غسل الأموال المتحصلة من جرائم المخدرات، الطبعة الثانية، مطابع الشرطة، 2004.

ممدوح خليل بحر: حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر و التوزيع، الأردن، 1996.

د/ منصور بن خضروان الداموك: مبادئ القانون الدولي و تطبيقاته في المملكة العربية السعودية، الطبعة الأولى، مكتبة الملك فهد الوطنية، الرياض، 1424.

نسرين عبد الحميد نبيه: الإجرام الجنسي، دار الجامعة الجديدة، الإسكندرية،2008.

د/ هدى حامد قشقوش:جريمة غسل الأموال في نطاق التعاون الدولي، دار النهضة العربية، القاهرة، 2001.

وليد حجاج اسماعيل: قانون مكافحة غسل الأموال رقم 80 لسنة 2002، دار أبو المجد للطباعة، مصر، 2002.

المراجع المتخصصة:

أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2000.

أمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، الجزائر، 2006.

أسامة أحمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة: جرائم الحاسب الآلى والإنترنت، دراسة مقارنة، ط 1، دار وائل للطباعة والنشر، الأردن، 2001.

أسامة أحمد المناعسة:جرائم الحاسب الآلي و الانترنت،دراسة تحليلية مقارنة، دار وائل للنشر، الأردن ، الطبعة الأولى، 2001.

د/ أسامة عبد الله قايد: الحماية الجنائية للحياة الخاصة و بنوك المعلومات،الطبعة الثالثة، دار النهضة العربية، القاهرة،1994.

أمير فرج يوسف: الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية.

د/ أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007.

د/ السيد عتيق: جرائم الانترنت، دار النهضة العربية، القاهرة، 2000.

د/ ايهاب فوزي السقا: الحماية الجنائية و الأمنية لبطاقات الإئتمان، دار الجامعة الجديدة، الإسكندرية،2007.

د/ جميل عبد الباقي الصغير: الانترنت و القانون الجنائي، الطبعة الأولى،دار النهضة العربية، القاهرة، 1996.

د/ جميل عبد الباقي الصغير: القانون الجنائي و التكنولوجيات الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، الكتاب الأول، الطبعة الأولى، دار النهضة العربية، القاهرة،1992 .

د/ جميل عبد الباقي الصغير: جرائم التكنولوجيا الحديثة، دار النهضة العربية، القاهرة.

د/ جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة،2002 .

د/ جميل عبد الباقي الصغير: الحماية الجنائية و المدنية لبطاقات الإئتمان الممغنطة، دار النهضة العربية، القاهرة،1999.

د/ حسين الغافري،أ/ محمد الألفي: جرائم الانترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة،2008.

د/ حسين بن سعيد بن سيف الغافري: الجرائم الواقعة على التجارة الإلكترونية،2006.

د/ حسنين المحمدي بوادي: إرهاب الانترنت، الخطر القادم، الطبعة الأولى، دارا لفكر الجامعي، الإسكندرية،2006.

د/ خالد ممدوح إبراهيم:إبرام العقد الإلكتروني، دراسة مقارنة، الدار الجامعية، مصر، 2007.

د/ خالد ممدوح إبراهيم:فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي،الإسكندرية،2010.
د/ خالد ممدوح ابراهيم: حجية البريد الالكتروني في الاثبات، دار الفكر الجامعي، 2005.
سامح محمد عبد الحكم: جرائم الانترنت الواقعة على الأشخاص في إطار التشريع البحريني، دراسة مقارنة بالتشريع المصري، دار النهضة العربية، القاهرة، 2007.
د/ سليمان أحمد فضل: المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة،2007.
د/ شيماء عبد الغني محمد عطا الله: الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.
طارق ابراهيم الدسوقي عطية: الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009.
د/عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004.
د/ عمر محمد بن يونس: المخدرات والمؤثرات العقلية عبر الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2003.
عمر محمد أبو بكر بن يونس و د/ يوسف أمين شاكر: غسل الأموال عبر الانترنت، الطبعة الأولى، أقاقوس القاهرة، 2004.
د/عبد الرحمن بن عبد الله السند: الأحكام الفقهية للتعاملات الإلكترونية" الحاسب الآلى وشبكة المعلومات (الإنترنت)"، الطبعة الأولى، دار الوراق، 2004.
د/ عفيفي كامل عفيفي: جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، الطبعة الثانية، 2000.
د/ عبد الفتاح بيومي حجازي: الحماية الجنائية للتجارة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، 2001.
د/ عبد الفتاح بيومي حجازي: الأحداث و الانترنت، دراسة متعمقة عن أثر الانترنت في انحراف الأحداث، دار الفكر الجامعي، الإسكندرية، 2004.
د/ عبد الفتاح بيومي حجازي: الدليل الجنائي في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي و الانترنت، دار الكتب القانونية، مصر.
د/ عبد الفتاح بيومي حجازي: جريمة غسل الأموال بين الوسائط الإليكترونية ونصوص التشريع، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2005.
د/ عبد الفتاح بيومي حجازي: نحو صياغة نظرية عامة في علم الجريمة و المجرم المعلوماتي،الطبعة الأولى، منشأة المعارف،الإسكندرية،2009.

د/ عبد الفتاح بيومي حجازي: التوقيع الإلكتروني في النظم القانونية المقارنة،الطبعة الأولى، دار الفكر الجامعي،الإسكندرية،2005.

د/ عبد الفتاح مراد: شرح جرائم الكمبيوتر و الانترنت، بدون دار النشر، بدون سنة نشر.

د/ عبد الله حسين علي محمود:سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية،دار النهضة العربية، القاهرة، 2002.

د/ عبد الله عبد الكريم عبد الله: جرائم غسل الأموال على شبكة الانترنت، دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، 2008.

عبد الله عبد الكريم عبد الله:جرائم المعلوماتية و الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية ، بيروت، 2007.

د/ علاء عبد الباسط خلاف: الحماية الجنائية لوسائل الاتصال الحديثة (الحاسب الإليكتروني "الكمبيوتر" الانترنت)،بدون دار نشر، 2004.

د/ علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، 1997.

د/ عصام عبد الفتاح مطر: التجارة الإلكترونية في التشريعات العربية و الأجنبية، دار الجامعة الجديدة، الإسكندرية، 2009.

عمرو موسى الفقي: الجرائم المعلوماتية،جرائم الحاسب و الإنترنت في مصر و الدول العربية، المكتب الجامعي الحديث، الإسكندرية،2006.

د/ عبد العزيز بن حمد الزومان: شبكة الانترنت، دليل تعريفي، مكتبة الملك فهد الوطنية، الرياض.

د/مدحت رمضان: جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000.

د/ مدحت عبد الحليم رمضان: الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001.

د/ محمد قطب: الجرائم المعلوماتية و طرق مواجهتها، الجزء الثاني، الاكاديمية الملكية للشرطة، البحرين، 2010.

د/مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، 2005.

د/ مصطفى محمد موسى: أساليب إجرامية بالتقنية الرقمية، دراسة مقارنة، دار الكتب والوثائق العربية، القاهرة، 2003.

د/ محمد سامي الشوا: ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994.

د/ ممدوح عبد الحميد عبد المطلب: جرائم استخدام الكومبيوتر وشبكة المعلومات العالمية، مكتبة دار الحقوق، الشارقة، 2001.

محمد أمين أحمد الشوابكة: جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة،عمان، 2004.

محمد الألفي: المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت،الطبعة الأولى، المكتب المصري الحديث، القاهرة،2005.

محمد أمين الرومي: جرائم الكمبيوتر و الانترنت، دار المطبوعات الجامعية، الإسكندرية،2004.

محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن، دار الجامعة الجديدة، الإسكندرية،2007.

محمود أحمد عبابنة:جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع، عمان، 2005.

منير محمد الجذبيهي، ممدوح محمد الجنبيهي: جرائم الانترنت، دار الفكر الجامعي، الاسكندرية، 2004.

منير محمد الجذبيهي، ممدوح محمد الجنبيهي: أمن المعلومات الإلكترونية، دار الفكر الجامعي، الاسكندرية، 2005.

د/ نائلة عادل فريد قورة: جرائم الحاسب الاقتصادية، دراسة نظرية و تطبيقية، دار النهضة العربية، القاهرة، 2004.

د/نعيم مغبغب:مخاطر المعلوماتية و الإنترنت، المخاطر على الحياة الخاصة و حمايتها، دراسة في القانون المقارن،1998.

د/ هلالى عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،دراسة مقارنة،الطبعة الأولى، دار النهضة العربية، القاهرة،1997.

د/ هلالي عبد اللاه أحمد: الجوانب الموضوعية و الاجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23-11-2001، الطبعة الأولى، دار النهضة العربية، القاهرة.

د/ هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1995.

د/ هشام فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994.

د/ هدى حامد قشقوش: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة،2000.

وليد الزيدي: القرصنة على الانترنت و الحاسوب، التشريعات القانونية، الطبعة الأولى، دار أسامة للنشر والتوزيع، الأردن، 2003.

وضاح محمود الحمود و نشأة مفضي المجالي: جرائم الإنترنت، دار المنار للنشر و التوزيع، عمان، 2005.

يونس عرب: قانون الكمبيوتر، النظرية و المشتملات، منشورات اتحاد المصارف العربية، 2001.

الأبحاث الجامعية:

مذكرات الماجستير:

حسن عزيز نور الحلو:الإرهاب في القانون الدولي، دراسة قانونية مقارنة، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، الأكاديمية العربية المفتوحة في الدانمارك، هلسنكي- فنلندا،2007،.scrib.com.

درابلة عمري: تنظيم المسؤولية الجنائية عن جرائم الصحافة المكتوبة، رسالة ماجستير، كلية الحقوق بن عكنون، جامعة الجزائر،2004.

زيتوني نصيرة: المسؤولية الجنائية عن جرائم الاعلام، بحث لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق بن عكنون، الجزائر، 2002.

صالحي نجاة: الآليات الدولية لمكافحة تبييض الأموال و تكريسها في التشريع الجنائي الجزائري، مذكرة مكملة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، السنة الجامعية2010-2011.

عثمان بن علي بن صالح: جريمة التجسس و عقوبتها في الشريعة الاسلامية و القانون الوضعي، رسالة ماجستير، تخصص التشريع الجنائي الاسلامي، جامعة نايف العربية للعلوم الامنية، الرياض، 2006.

محسن بن محسن بن باعث الرويلي: تجريم الأفعال الإباحية الاليكترونية و العقاب عليها، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض 2010.

مسلم خديجة: الجريمة الارهابية، رسالة ماجستير في القانون الجنائي و العلوم الجنائية، معهد الحقوق بن عكنون، الجزائر، 1996-1997.

يونس عرب: جرائم الحاسوب، دراسة مقارنة، رسالة مقدمة لنيل درجة الماجستير في الحقوق، كلية الدراسات العليا، الجامعة الأردنية،1994.

أطروحات الدكتوراه:

حسين بن سعيد بن سيف الغافري:السياسة الجنائية في مواجهة جرائم الانترنت، رسالة دكتوراه حقوق، جامعة عين شمس، 2005.

خالد حسين عبد التواب أحمد: جرائم القذف و السب العلني عبر الانترنت، رسالة دكتوراه، جامعة عين شمس، 2011.

شيرين الياس دبابنة: التأثير الاجتماعي و الاقتصادي لجرائم الانترنت في المجتمع الاردني،رسالة دكتوراه في علم الاجتماع، كلية الدراسات العليا، الجامعة الاردنية،2008.

محمد محمد حسن: جريمة القذف، دراسة مقارنة بين قانون الجنائي الوضعي والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، 1996.
الطيب بلواضح: حق الرد و التصحيح في جرائم النشر الصحفي و أثره على المسؤولية الجنائية في ظل قانون الإعلام الجزائري رقم 90-07، أطروحة لنيل شهادة الدكتوراه العلوم في الحقوق، تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2012-2013.

المقالات المنشورة و الدوريات و الحلقات العلمية:

أحمد عبد الكريم سلامة:الإنترنت والقانون الدولي الخاص "فراق أم تلاقى"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000.
د/ أحمد فاروق زاهر: الجريمة المنظمة، ماهيتها،خصائصها و أركانها، بحث مقدم إلى الحلقة العلمية جرائم الاحتيال و الاجرام المنظم،جامعة نايف العربية للعلوم الامنية، الرياض، 2008.
أمجد دخل الله: القرصنة الالكترونية، مجلة المحامون، العددان3و4، السنة 72، سوريا،عام 2007.
أسامة غربي: الاباحية الالكترونية،،مقال منشور ضمن أعمال الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية المنعقد بالجلفة ليومي2هـ-2009/04/28،مجلة دراسات و أبحاث، جامعة الجلفة،العدد2009/01.
د/ أسامة بن غانم العبيدي: جريمة الاستغلال الجنسي للأطفال عبر شبكة الانترنت، دراسة قانونية مقارنة، مجلة الشريعة و القانون، العدد 53، السنة 27، يناير 2013، كلية القانون، جامعة الإمارات العربية المتحدة،
أزرو محمد رضا: التوقيع الإلكتروني و مقتضيات الآمان القانوني، دراسة مقارنة، مقال منشور ضمن أعمال الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية المنعقد بالجلفة ليومي 27-28/0د/2009،مجلة دراسات و أبحاث، جامعة الجلفة،العدد2009/01.
أكمل يوسف السعيد يوسف: المسؤولية الجنائية لمقدمي المواد الاباحية عبر الانترنت، مجلة البحوث القانونية و الاقتصادية، كلية الحقوق، جامعة المنصورة،2011.
الأزرق بن عبد الله، أحمد عمراني: نظام المعلوماتية في القانون الجزائري، واقع و آفاق، ورقة مقدمة إلى المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، البيئة المعلومات الآمنة،المفاهيم و التشريعات و التطبيقات المنعقد بمدينة الرياض خلال الفترة 7 آبريل 2010.
ابراهمي الدسوقي أبو الليل، الجوانب القانونية للتعاملات الاليكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة، التراسل الاليكتروني"، الطبعة الأولى، مجلس النشر العالمي، الكويت، 2003.
إبراهيم الدسوقي أبو الليل: الجوانب القانونية للتعاملات الإلكترونية، كلية الشريعة والقانون، جامعة الأزهر، فرع دمنهور، العدد18، مجلس النشر العلمي، 2003.
ابراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات عبر وسائل الاتصال الحديثة، بحث مقدم إلى مؤتمر القانون والكمبيوتر و الانترنت، كلية الشريعة و القانون، جامعة الإمارات، ماي 2000.

إبراهيم أبو كامش: فضاء الانترنت في فلسطين تنخره السرقة و الابتزاز و الاحتيال و التشهير، مجلة الحياة و السوق، س2، العدد 56، 2012

إسماعيل عبد النبي شاهين: أمن المعلومات في الانترنت بين الشريعة والقانون، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000.

ايهاب صلاح الدين: الإطار القانوني للتجارة الإلكترونية،مجلة القضاء العسكري، العدد 16، المجلد2، ديسمبر 2006.

الأزرق بن عبد الله، أحمد عمراني: نظام المعلوماتية في القانون الجزائري، واقع و آفاق، ورقة مقدمة إلى المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، البيئة المعلومات الآمنة، المفاهيم و التشريعات و التطبيقات المنعقد بمدينة الرياض خلال الفترة 7 آبريل 2010 للمشكلات و استكشاف لسياسات المواجهة المنعقد بدار الضيافة، جامعة عين شمس 26-28 سبتمبر 2004، كلية الآداب، قسم علم الإجتماع، مركز الدراسات المعرفية، المعهد العالي للفكر الإسلامي.

بوحنة محمد: الأدوات القانونية لمكافحة الإرهاب، مجلة الشرطة، العدد 71، فيفري 2004.

جميل عبد الباقي الصغير: المسؤولية الجنائية في مجال المعاملات الالكترونية، ورقة عمل مقدمة الى دورة الجوانب القانونية و الفنية في المعاملات الالكترونية المنعقدة في الفترة من 8-2012/4/12، مركز البحوث و الاستشارات القانونية، كلية الحقوق، جامعة القاهرة.

جورج لبكي: المعاهدات الدولية للإنترنت، حقائق وتحدّيات، مجلة الدفاع الوطني، www.lebarmy.gov.lb،

حسن بن أحمد الشهري: استعمال الإنترنت في تمويل الإرهاب و تجنيد الإرهابيين، الإرهاب الإلكتروني وبعض وسائله و الطرق الحديثة لمكافحته،جامعة نايف العربية للعلوم الأمنية، الرياض،2012.

حسن طاهر داود: جرائم نظم المعلومات،الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2000.

د/ حسين بن سعيد الغافري: الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الإلكترونية العماني، ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت القاهرة 2-4 يونيو 2008، www.shaimaaatalla.com.

حسن حماد حميد، جاسم خريبط خلف: إساءة إستخدام بطاقة الإئتمان الإلكترونية الملغاة، مجلة جامعة بابل للعلوم الإنسانية، المجلد 18، العدد2، 2010.

ربحى مصطفى عليان: البريد الإلكترونى، مجلة الأمن والحياة، العدد 234، السنة الحادية والعشرون، 2003.

زياد علي عربية: غسل الأموال، آثاره الإقتصادية و الإجتماعية و مكافحتها دوليا و عربيا، مجلة الأمن و القانون، العدد1، السنة 12، يناير 2004.

سيدهم مختار: المخدرات و المؤثرات العقلية، مجلة المحكمة العليا، العدد2، السنة 2010.

شيماء فوزي أحمد: التنظيم القانوني للنقود الإلكترونية، مجلة الرافدين، المجلد 14، العدد 50، السنة16، كلية الحقوق، جامعة الموصل.

صبايحي ربيعة: التطور التكنولوجي و جريمة تبييض الأموال، المجلة الجزائرية للعلوم القانونية و الإقتصادية و السياسية، العدد04/2009.

د/صالح سليمان عبد العظيم: الأبعاد و التأثيرات الاجتماعية المرتبطة باستخدام الانترنت على الاسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الامارات العربية، ورقة مقدمة إلى مؤتمر واقع الاسرة في المجتمع: تشخيص للمشكلات و استكشاف لسياسات المواجهة المنعقد بدار الضيافة، جامعة عين شمس، 27-28 سبتمبر 2004، كلية الآداب، قسم علم الاجتماع، مركز الدراسات المعرفية، المعهد العالي للفكر الاسلامي.

د/ علي عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون و الكومبيوتر و الإنترنت خلال الفترة ما بين 1-3 ماي بجامعة الإمارات العربية ، كلية الشريعة و القانون، 2000.

علي حسن عباس: مخاطر إستخدام بطاقات الدفع الإلكتروني عبر شبكة الإنترنت (المشاكل و الحلول)، ورقة عمل مقدمة إلى ندوة " الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني" التي نظمها مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة، 1998/12/14.

عجابي الياس: الطبيعة القانونية للتوقيع الإلكتروني، مقال منشور ضمن أعمال الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية المنعقد بالجلفة ليومي2ه-2009/04/28،مجلة دراسات و أبحاث، جامعة الجلفة،العدد01/2009.

عبد العزيز النويري: المخاطر القانونية للانترنت على حرية التعبير و الحياة الخاصة، التواصل،العدد 26، جوان 2010، كلية الحقوق، جامعة الحاج لخضر، باتنة

علاء الدين محمد شحاتة: رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي،المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة ما بين 2و-1993/10/28، مشكلات المسؤولية الجنائية في مجال الجرائم الواقعة على البيئة، الجرائم الواقعة في مجال تكنولوجيا المعلومات، دار النهضة العربية، القاهرة،1993.

عماد علي الخليل: التكييف القانوني لاساءة استخدام أرقام البطاقات عبر شبكة الانترنت،بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، خلال الفترة من 1-3 ماي بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون.

عماد علي الخليل: التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الانترنت، دراسة عملية في ظل أحكام قانون العقوبات الأردني، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الانترنت، 2000.

عمر الفاروق: جرائم الكمبيوتر و الجرائم الأخرى في مجال تكنولوجيا المعلومات، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 28/25 أكتوبر 1993.

عمر فاروق فحل: خطر الجرائم المعلوماتية الالكترونية، دراسة مقارنة، مجلة المحامون،سوريا، العدد4/3، السنة 72.

د/عادل عبد الجواد: اجرام الإنترنت، مجلة الأمن و الحياة، العدد221، السنة20، ديسمبر 2000/يناير 2001، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

د/ عبد الفتاح الصيفي، د/ مصطفى عبد المجيد كاره، د/ أحمد محمد النكلاوي: الجريمة المنظمة، التعريف و الانماط و الاتجاهات،أكاديمية نايف العربية للعلوم الامنية،الرياض، 1999.

د/ غنام محمد غنام: عدم ملائمة القواعدالتقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر،بحث مقدم لمؤتمر القانون و الكمبيوتر و الانترنت، خلال الفترة من 1-3 ماي بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون.

فريد عبد المعز فرح: التعاقد عبر الإنترنت، مجلة البحوث الفقهية و القانونية، كلية الشريعة و القانون، جامعة الأزهر، فرع دمنهور، العدد18، 2003.

د/ كمال عبد الرشيد:جرائم العنف العائلي(رؤية أمنية)، دراسة مقدمة الى ندوة جرائم العنف العائلي بتاريخ 1992/2/9، كلية الحقوق، جامعة المنصورة.

د/ محمد فتحي عيد: الانترنت، ماهيته وخدماته، الأمن و الحياة، العدد 242، س 21، سبتمبر/ أكتوبر 2002.

د/محمد فتحي عيد: الانترنت و دوره في انتشار المخدرات، أكادمية نايف العربية للعلوم الأمنية، الرياض، 2003.

د/محمد الأمين البشيري:التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

د/محمد محمد الألفي: بعض أنماط جرائم الانترنت، ورقة عمل مقدمة في دورة الجوانب القانونية والفنية في المعاملات الالكترونية في الفترة من 08 – 2012/04/12 بكلية الحقوق، جامعة القاهرة.

د/محمد قطب: جرائم الاخلاق و الآداب عبر الشبكة الدولية للمعلومات(الانترنت) و دور التدريب في مواجهتها، مجلة الامن العام، العدد 199، س 49، أكتوبر 2007

محمد بن عبد الله آل فايع العسيري، د/ حسن بن أحمد الشهري: استعمال الإنترنت في تمويل الإرهاب و تجنيد الإرهابيين، الإرهاب الإلكتروني، و بعض وسائله و الطرق الحديثة لمكافحته، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

محمد محمد علي إبراهيم: الجوانب الإقتصادية لغسيل عوائد الجريمة المنظمة، ورقة مقدمة إلى أعنال ندوة الجريمة المنظمة و أساليب مواجهتها، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2003.

د/ محمد إبراهيم زيد: الجريمة المنظمة، تعريفها أنماطها و جوانبها التشريعية، ورقة مقدمة إلى أبحاث حلقة علمية حول الجريمة المنظمة و أساليب مكافحتها المنعقد ما بين 14-18 نوفمبر 1998 بأبوظبي، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1998.

د/ مصطفى محمد موسى: التكدس السكاني العشوائي و الإرهاب، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

ميلود بن عبد العزيز: الجرائم الإباحية وأثرها على المجتمع من منظور شرعي وقانوني،مقال منشور ضمن أعمال الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية المنعقد بالجلفة ليومي27-2009/04/28،مجلة دراسات وأبحاث، جامعة الجلفة،العدد2009/01.

د/ مدحت رمضان: الحماية الجنائية لموقع الإنترنت... و محتوياته، مجلة التشريع، العدد الثاني، السنة الأولى، جويلية 2004.

مصطفى إبراهيم عيسى: جرائم العصر، مجلة الأمن و الحياة، العدد340،السنة 29، أوت / سبتمبر 2010.

د/ ممدوح عبد الحميد: جرائم استخدام شبكة المعلومات العالمية، جرائم الإنترنت من منظور أمني، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة ، ماي 2000.

الحلقة العلمية: الدليل الرقمي و التحقيق في الجرائم الالكترونية، المنعقدة من 22 إلى 1429/12/27، كلية علوم الادلة الجنائية، جامعة نايف العربية للعلوم الامنية.

ميلود عبد العزيز: الجرائم الإباحية و أثرها على المجتمع من منظور شرعي و قانوني، مقال منشور ضمن أعمال الملتقى الدولي حول التنظيم القانوني للانترنت والجريمة الالكترونية المنعقد بالجلفة ليومي27-2009/04/28،مجلة دراسات وأبحاث، جامعة الجلفة،العدد2009/01.

محمد محمد الالفي:العوامل الفاعلة في انتشار جرائم الانترنت، ورقة مقدمة في المؤتمر الدولي الاول حول حماية امن المعلومات والخصوصية في قانون الانترنت، القاهرة، جوان 2008/4/2 موجودة على الموقع: www.f- law.net.

نوفل علي عبد الله، محمد عزت: جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، مجلة الرافدين للحقوق، المجلد 12، العدد 44، السنة 2010.

د/ نادر عبد العزيز شافي: جرائم التجسس، مجلة الجيش، العدد230، سبتمبر 2004،lebany.gov.lb .

ناجي الزهراء: التجربة التشريعية الجزائرية في تنظيم المعاملات الإلكترونية المدنية و التجارية، ورقة مقدمة إلى المؤتمر العلمي المغاربي الأول حول المعلوماتية و القانون المنعقد في الفترة من 28 إلى 29 أكتوبر.

هشام فريد رستم: جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، العدد17، جوان 1995.

د/ هشام محمد فريد رستم:الجرائم المعلوماتية، أصول التحقيق الجنائي الفني و آلية التدريب التخصصي للمحققين، مجلة الأمن و القانون، العدد الثاني، السنة7، 1999.

يونس عرب: جرائم الكمبيوتر و الانترنت، إنجاز في المفهوم و النطاق و الصور و القواعد الاجرائية للملاحقة والاثبات، ورقة عمل مقدمة إلى مؤتمر الامن العربي، تنظيم المركز العربي للدراسات . و البحوث الجنائية، أبو ظبي، 10-2002/2/12،arablaw.org.

مواجهة الجريمة النعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون و المعلوملتية المزمع عقده بأكاديمية الدراسات العليا في أكتوبر2009، كلية الحقوق و العلوم السياسية، جامعة زيان عاشور، الجلفة.

الجرائد و الشرائط و النشرات الإخبارية:

أحمد رزق رياض، عقوبة جريمة الازعاج على النت تصل إلى الحبس سنة، جريدة الجمهورية، 17 أوت 2010.

حسني عبد الصبور: قضية الساعة، الانترنت و فيروس الشفرة الحمراء، جريدة الأهرام،2001/8/11، س126، العدد 41886، المنشور على:ahram.org.eg.

رأفت رضوان: الإنترنت و الإرهاب، جريدة الأهرام المسائي،2005/04/21.

حوار د/ فايز عبد الله الشهري مع هداية نت،الجريدة اليومية الالكترونية للصحافة، السعودية،30 يناير2001، المنشور على الانترنت في الموقع التالي:www.hedayah.net

عبد الحفيظ سعد، أحمد عبد المقصود: الإرهاب الإليكتروني ووصفات مجانية لتصنيع قنبلة هيدروجينية، جريدة صوت الأمة، العدد 11،2005/04/228.

عطاف الشمري: عدد مستخدمي الانترنت في العالم العربي يتجاوزون ال38 مليون مستخدم، جريدة الرياض،العدد 14983، 2 يوليو 2009،alriyadh.com .

عادل راوتي : 60% من مستخدميها شباب، الانترنت تتفوق على مصادر الخبر،الاذاعة الجزائرية، radioalgérie.dz.

نوارة باشوش: مصالح الأمن تضع يدها على المخططين و المحرضين عبر الفايسبوك و اليوتيوب، جريدة الشروق،2011/09/17، العدد3417.

فيروس القمة يتحكم في الحاسبات عن بعد، لغة العصر، مجلة الأهرام للكمبيوتر و الإنترنت و الإتصالات، العدد53، السنة 5، ماي 2005.

18 مليار سنتيم قيمة نفقات تصفح الجزائريين على الانترنت،جريدة الفجر،2009/12/02.

مقاهي الانترنت في الجنوب فضاءات للانحلال و أخرى للتعارف و قليل منها للعلم، جريدة النهار،2010/08/02.

مقاهي الانترنت في تيزي وزو تتحول الى أوكار للدعارة و الجهاد دون مراقبة،جريدة النهار، 2010/08/02.

المواقع الإباحية تتصدر قائمة التصفح الإلكتروني لدى شباب بومرداس، جريدة النهار، 2010/08/02.
جريدة النهار،العدد1323، فيفري2012.
جريدة الأهرام،2009/04/17.
Un projet de loi en cours de prepration,lutte contre lacybercriminalité ،جريدة المجاهد
،2008/04/12.
الأمن يضبط47 جريمة إلكترونية، جريدة أخبار اليوم، 2013/03/11، .www.akhbarelyoum.dz
شريط التكنولوجيا الحديثة، بث على التليفزيون الجزائري، القناة الأولى يوم 2008/11/05.
التشهير عبر الإنترنت، برنامج 90 دقيقة، قناة المحور،2010/12/22.
نشرة أخبار الثامنة، القناة الجزائرية.
نشرة الأخبار الفنية لقناة روتانا سينما، ليوم2010/12/10.
غدا الحكم في دعوى مديرة التسويق للإساءة لشرفها عبر الانترنت، صحيفة الخبر الاليكترونية ،2010/09/26. منشورة على الموقع www.gn4me.com.
غدا الحكم في دعوى مديرة التسويق للإساءة لشرفها عبر الانترنت، خبر منشور على الانترنت من صحيفة الخبر الاليكترونية يوم 2010/09/26، على الموقع www.gn4me.com.
إتصالات الجزائر تطلق "في أمان" لمراقبة إستخدام الأطفال للإنترنت، جريدة المساء، www.el-massa.com.
حلول رقابة لفائدة الأولياء على الإنترنت، جريدة الأحداث الجزائرية،www.elahdath.net.
إتصالات الجزائر، خدمة مراقبة تصفح الإنترنت "في أمان" تدخل حيز الخدمة اليوم، الإذاعة الجزائرية، www.radioalgerie.dz.

البحوث و التقارير المنشورة على مواقع الإنترنت:

أحمد عاصم أحمد عجيلة: ورقة عمل في موضوع رؤية قانونية حول ثبوت جرائم السب و القذف عبر الانترنت في القانون المصري، المؤتمر الدولي الأول حول الخصوصية و أمن المعلومات في قانون الانترنت، جوان 2008، منشور على الانترنت على www.mohamoun-mountada.com
د/أكرم عبد الرزاق المشهداني: 600 مليار دولار سنويا حجم غسل الأموال في العالم، مقال منشور على الموقع : www.alwatan-news.com
د/جميل حزام يحي الفقيه: مفهوم الإرهاب في القانون الدولي العام،ycsr.org
د/ بوفليح سالم: محاضرات قيمة في القانون الجنائي، مقال منشور على الموقع: montada.elkhabar.com
حمزة نادي: ما هي الفروق القانونية بين جريمتي السب و القذف؟، مقال منشور على الانترنت على الموقع التالي: www.almoltaqa.com

حمادي الأسيوطي: جرائم النشر و الصحافة و حماية الصحافي، مقالة قانونية منشورة على الانترنت على الموقع:www.kafishokr.com.

د/ دياب البدانية: مواجهة الجريمة المنظمة العابرة للحدود الوطنية، من المحلية إلى الكونية، جامعة مؤتة، الاردن، مقال منشور على: www.mutah.edu.jo.

سماح خميلي:التكنولوجيا بين أيد غير أمينة في الجزائر(الانترنت وظاهرة الجنس الالكتروني)، مقال منشور على الانترنت:.www.chihab.net.

د/فؤاد جمال:جرائم الحاسبات والانترنت، بحث منشور على الانترنت على الموقع: www.tashreaat.com

سلطانة بنت فهد بن دغيليب العتيبي: الإرهاب الالكتروني، التهديد الجديد في نظام الصحة الالكتروني عن بعد، مقال منشور على الانترنت على الموقع: www.crime-research.org.

عبد الرحمن ألطاف: تحديات الملكية الفكرية للمصنفات الرقمية، مقال منشور على الموقع:arabica.bitsnips.com

د/ عبد الفتاح محمود كيلاني: مدى المسؤولية القانونية لمقدمي خدمة الانترنت، مقال منشور على الانترنت على الموقع: www.flaw.bu.eg

عصام مفلح: مفهوم الإرهاب و الموقف الدولي،إرهاب الدولة و إرهاب المنظمات، مقال منشور على الانترنت على الموقع: www.refnet.gov.sy .

د/عادل عمر: الجرائم الأخلاقية و أثرها على إنتشار الجريمة،news.elfagr.org

د/ محمد ياسر الفتوح: الملكية الفكرية و الجريمة المعلوماتية، مقال منشور على الموقع: www.knal.com.

محمد عبد المحسن سعدون: مفهوم الإرهاب و تجريمه في التشريعات الجنائية الوطنية و الدولية، مقال منشور على الموقع: www.iasj.net.

محمد عرب الموسوي: مفهوم الإرهاب الدولي، مقال منشور على الموقع: orgwww.ahwar.

محمد شوقي : جرائم الانترنت... من الإباحية للإرهاب، مقال منشور بتاريخ 2008/08/12 على الموقع التالي :www.moheet.com.

محمود صالح العادلي: الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية، بحث منشور على الانترنت الموقع : dreadly.com

محمد عبد الله المنشاوي: جرائم الإنترنت من منظور شرعي و قانوني، بحث منشور على الموقع:www.minshawi.com

د/ محمد عبد الله المنشاوي: جرائم الانترنت في المجتمع السعودي، بحث منشور على:www.minshawi.com

محمد محمود: الجريمة الإلكترونية و جرائم المعلوماتية في القانون السوداني، بحث منشور على الإنترنت على الموقع: www.smu.edu

د/مشعل عبد الله القدهي: المواقع الاباحية على شبكة الانترنت و أثرها على الفرد و المجتمع"، بحث منشور على الموقع : www.aljra.net

مليكة حراث:المسابقات و الوظائف الوهمية، أحدث جرائم الإنترنت، مقال منشور على الموقع:www.akhbar el youm-dz.com.

محمد فارس: أخطر 10 فيروسات في التاريخ، مقال منشور على الانترنت على الموقع: itwadi.com

حوار مجتمع المعرفة مع د/ عمر محمد أبو بكر بن يونس: جرائم الإنترنت و القوانين الدولية، مقالة منشورة على الموقع :www.mengo.net.

يونس عرب: نظام الملكية الفكرية لمصنفات المعلوماتية، بحث منشور على الموقع:www.arablawinfo.com

يونس عرب:جرائم الكمبيوتر و الانترنت، المعنى و الخصائص و الصور و إستراتيجية المواجهة القانونية،مقال منشور على الانترنت على الموقع التالي:www.arablaw. org.

يونس عرب: جرائم الكمبيوتر و الإنترنت، انجاز في المفهوم و النطاق و الصور و القواعد الإجرائية للملاحقة و الإثبات، ورقة عمل مقدمة الى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات و البحوث الجنائية، أبو ظبي، 10-2002/2/12، بحث منشور على الموقع:maktoubblog.com.

يونس عرب: المخاطر التي تهدد الخصوصية و خصوصية المعلومات في العصر الرقمي، بحث منشور على الموقع التالي:www.arablaw.com

وليد الرمزي:التعاون الدولي حاسم في حرب الجزائر ضد الجريمة السيبرانية، مقال منشور على الانترنت يوم 2010/05/11على الموقع التالي:magharebba.com

د/هيثم عبد الرحمن البقلي: الجريمة المعلوماتية، مقال منشور على الانترنت على الموقع:www.kennaoline.com

جرائم الانترنت،.djelfa.info

الانترنت يتحول مسرحا لارتكاب الجرائم الالكترونية و السعودية و الامارات في الصدارة، مقال منشور على الانترنت على:teknotel.info

دور الحاسوب في الجريمة المعلوماتية و محل الجريمة، المنشور على الموقع:feeds.feedburner.com

منتديات الجزائر: ما هو الجيل الثالث للهاتف النقال و ما الجديد فيه؟www.eljazayera.com ،

الدليل الجنائي و مشكلة تحصيله في الجرائم الالكترونية، بحث منشور على الانترنت على الموقع : www.arabipcenter.com

القذف الالكتروني بأسماء وهمية مقال منشور على الانترنت على الموقع: alryadh .com

الحكم بالسجن و الغرامة على شاب شتم موظفا عاما على الانترنت، قضية منشورة على الموقع: www.brzan.com.

ما هو مفهوم الصحافة الالكترونية؟ مقال منشور على الانترنت على الموقع التالي:itqanbs.com

تعريف الصحافة الالكترونية مقال منشور على الانترنت على الموقع التالي: forums.m7taj.org

الجريمة عبرالانترنت، مقال منشور على الانترنت على الموقع :www.meus.bbc.com و على:www.f-law.net

القانون الجنائي، جرائم الإعتداء على الأشخاص و على الأموال، بحث منشور على الانترنت على الموقع: ta3lam.mortadarabi.com

فيروسات الكمبيوتر و الانترنت، مقال منشور على الانترنت على الموقع: kenanaonline.com

جرائم الإعتداء على الأشخاص، بحث منشور على الانترنت على الموقع:www.alayam.com

جرائم الكمبيوتر و الانترنت (الجريمة الاليكترونية) بحث منشور على الانترنت على الموقع:.www.islamonline.net

الهاكرز.....لصوص برؤية عصرية. بحث منشور على الانترنت على الموقع التالي: www.kufur-kasem.com

من الجرائم الأكثر شيوعا السب و القذف، بحث منشور على الانترنت على الموقع: www.nooralislam.alafdal.net.

ما هي عملية الهاكينج أو التجسس ؟ مقال منشور على الموقع التالي: www.wikipedia.com

الإرهاب الالكتروني مقال منشور على الموقع:www.knal-google.com

مفهوم الإرهاب الإلكتروني مقال منشور على: .www.Mahawar el-islam.com

التجسس عبر الانترنت....أو مخابرات الانترنت، مقال منشور على الانترنت على الموقع التالي: www.almski.com

روسيا في الشيشان امام معركة الانترنت، مقال منشور على الانترنت على الموقع: news.bbc.co.uk.

التجسس الاقتصادي عبر الانترنت ، مقالة منشورة على الانترنت على الموقع التالي: www. forexblog.ae.

طبيعة جرائم الاعلام، مقال منشور على الموقع التالي:dc307.4shared.com

الإرهاب و الانترنت، مقال منشور عبر الانترنت على: www.aljazeera.com و على : www.arwikipédia.org.

رائحة الماريجوانا تنبعث من أوكار الإنترنت، مقال منشور على الموقع:www.cadac.org

الصين تغلق 60 ألف موقع إباحي، بحث منشور على الموقع:news.maktoob.com

تقرير شبكة CNN الإخبارية بعنوان:"سهولة الوصول إلى الملفات الإباحية"، المنشور على الموقع:www.cnn.com
الإنترنت، مقال منشور على الموقع:fr.wikipédia.com
جرائم الإنترنت.... من الإباحية إلى الإرهاب، مقال منشور على الموقع:www.moheet.com
الأمن و الإنترنت، مقال منشور على الموقع:www.dubaipolice.gov
إرهاب الإنترنت الخطر الوافد.....، مقال منشور على الموقع:www.mattaqui.com
من الإرهاب الحماية الإلكتروني، مقال منشور على الموقع:www.mpc.org
نحو استراتيجية قومية لمكافحة الإرهاب عبر الإنترنت، بحث منشور على الموقع:www.rand.org
مكافحة عنصرية الإنترنت، مقال منشور على الانترنت على الموقع: news.bbc.co.uk.
ملاحقة مخربي الإنترنت، مقال منشور على الانترنت على الموقع: news.bbc.co.uk.
مواجهات اسرائيلية فلسطينية على شبكة الإنترنت، مقال منشور على الانترنت على الموقع: news.bbc.co.uk.
مراهقون تآمروا لتعطيل الإنترنت مطلع العام الجديد، مقال منشور عبر الانترنت على: www.aljazeera.net
حرب التجسس عبر الإنترنت، يوزع بلانك، وكالة الأنباء الألمانية، مقال منشور عبر الانترنت على: www.th3pro.com
L'ecstazy، مقال منشور عبر الانترنت على: www.doctissimo.fr
أمريكا : متسللوا إرهابيين، مقال منشور على الانترنت على الموقع: news.bbc.co.uk.
الإنترنت يسهل الحروب و العمليات الإرهابية، مقال منشور عبر الانترنت على: www.amjad68.jeera.com
العنف تعريف و الإساءة، مقال منشور عبر الانترنت على: www.nfsp.org.sa
العنف تعريف، مقال منشور عبر الانترنت على: dr-alhassani.com
العنف تعريف، مقال منشور عبر الانترنت على:mawdoo3.com.
خبراء يثنون على سياسة حجب بعض المواقع و يشددون على أهمية التوعية، مقال منشور عبر الإنترنت على:up.graam.com.
عملية دولية تنقض خلالها أجهزة إنفاذ القانون على أفراد يستغلون الأطفال جنسيا و يتبادلون صورهم عبر الإنترنت، www.interpol.int.
حقوق الملكية الفكرية في البيئة الرقمية، alyassere.net.
الحماية من الإرهاب الإلكتروني،www.mpc.gov.
أشكال الإرهاب،saeed.com.
قائمة الدول حسب عدد مستخدمي الإنترنت،www.wikipedia.org.

عدد مستخدمي الإنترنت في الشرق الأوسط و شمال إفريقيا،.youtube.com .
غياب خاص بالمعلوماتية في التشريع الجزائري،www.facebook.com.
الإرهاب الدولي و إشكالية مكافحته،www.djelfa.info .
أشكال الإرهاب، saeed.com.
الحماية من الإرهاب الإلكتروني،www.Mahawar el-islem.com.
دودة الحاسوب،ar.wikipedia.org.
ديدان الإنترنت، www.4jam3a.net.
هكذا سيمنع الآباء أبناءهم من دخول المواقع الإرهابية و الإباحية،www.elbilad.net
جريمة التهديد في القانون الجزائري،www.startimes.com .
جريمة التهديد الشفوي،jurispedia.org.

القواميس و المعاجم:

ابتسام القرام: المصطلحات القانونية في التشريع الجزائري، قاموس باللغتين العربية و الفرنسية، قصر الكتاب، البليدة، 1998.
إبراهيم نجار، أحمد زكي بدوي، يوسف شلالا: القاموس القانوني، فرنسي- عربي،الطبعة 8، مكتبة لبنان، 2002.
د/صالح مسند: مصطلحات الانترنتfaculty.ksu.edu.sa .
القاموس الجديد للطلاب،معجم عربي مدرسي ألفبائي، الطبعة 7، المؤسسة الوطنية للكتاب، الجزائر،1991.
قاموس أطلس للطلاب، ط 1، دار أطلس للنشر، 2003.
المنجد في اللغة و الإعلام، الطبعة السابعة و العشرون، دار المشرق، بيروت.
مرشد الطلاب، المرشد الجزائري، قاموس مدرسي عربي.
معجم ا لحاسبات، الطبعة 3، مجمع اللغة العربية، القاهرة، 2003.

الإتفاقيات و الدساتير و القوانين والمراسيم:

اتفاقية بودابست الموقعة في 23-11-2001 ببودابست، و المتعلقة بجرائم الإنترنت.
الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
الدستور الجزائري.
الدستور الأردني.
الدستور البحريني.
الدستور المصري.
الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن لقانون العقوبات الجزائري المعدل و المتمم بالقانون رقم 09-01.

قانون العقوبات المصري.
قانون العقوبات الأردني.
قانون العقوبات البحريني.
قانون العقوبات الإتحادي رقم 06 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات.
قانون جرائم المعلوماتية السوداني.
نظام مكافحة جرائم المعلوماتية السعودي.
القانون رقم 01/05 المؤرخ في 2005/02/06 المتعلق بالوقاية من تبييض الأموال و تمويل الإرهاب و مكافحتها.
قانون مكافحة غسل الأموال رقم 80 لسنة 2002.
قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية و التجارة الإلكترونية الدولية لسنة 1996.
الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن لقانون الإجراءات الجزائية الجزائري المعدل و المتمم بالقانون رقم 06-22.
القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها.
قانون اساءة استخدام الحاسوب البريطاني.
قانون الإعلام الجزائري رقم 05/12.
قانون المعاملات الإلكترونية الأردني.
القانون التجاري الجزائري.
القانون 05-06 المعدل و المتمم للأمر 75-585 المتضمن القانون المدني الجزائري.
القانون 03-15 المتضمن الموافقة على الأمر 03-11 المتعلق بالنقد و القرض.
القانون 83-03 المؤرخ في 5 فيفري1983 المتعلق بحماية البيئة.
الأمر 05-06 المتعلق بمكافحة التهريب.
الأمر رقم 05/03 المتعلقة بحماية حقوق المؤلف و الحقوق المجاورة.
المرسوم التنفيذي رقم 98-256 المعدل و المتمم للجزء التنظيمي من الأمر 75-89 و المتضمن قانون البريد و المواصلات.
المرسوم رقم 07-162 يعدل و يتمم المرسوم 01-123 المتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية و على مختلف خدمات المواصلات السلكية و اللاسلكية.
القانون 08-10المتمم و المعدل للقانون 83-11و المتعلق بالتأمينات الإجتماعية.

Code pénal francais.

Loi relative à la protection pénale de la propriété littéraire et artistique.
Loi n°2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet,www.legifrance.gouv.fr.

Code civil francais.
Code de procedure penale francais.
California penale code.
USA patriot act,www.fincen.gov.
Computer fraud and abuse act,cio.doe.gov.

المواقع على الإنترنت:

.www.aljazeera.com
www.el-burhan.com
www.alex.com.
www.gn4me.com
www.aljazeera.net
. www.alwatan.com.sa
www.alsaha.com
www.youtube.com
www.alarabya.net
Wikipédia-a blogspot.com.
موقع منظمة التجارة العالميةwww.wato.org
www.nooralislam-alafdal.com
www.cnn.com
www.lawmg.co.se
.swma.net
.www.drugstrateegies.com
.www.legislature.idaho.gov
Policy.mofcom.gov.cn

لأحكام وقرارات المحاكم:

الطعن رقم 474 لسنة 55 ق،جلسة 1985/3/3.
جلسة 1975/02/17، س26.
مجموعة أحكام النقض، العدد 2 لسنة7 ق.
الطعن رقم 61341 لسنة 59 ق جلسة 1991/1/7.

باللغة الأجنبية:

Ouvrages:

OUVRAGES GENERAUX:

Drogues,savoir plus,Livret juredique,INPES,avril 2004.

Jean LARGUIES:Droit penal special,8ed,cujas,1994.

JAUFFRET.Alfred: Droit commercial,20ème éd,LGDJ, Paris,1991,n°882.

Roger MERLE ،André Vitu: Traité de droit criminal, droit pénal special, éd Cujas, 1982.

OUVRAGES SPECIAUX:

Adrian THAM : What is code red worm ?,Aug4,2001, SANS institute.

Abbas JABER:Les infractions commis sur internet, L'Harmattant, Paris.

Business information systèmes, 2ème édition, 2003.

Charles DOYLE :Cybercrime,a sketch of 18 usc 1030 and related federal criminal laws, the librery of congress,CRS , 25 february 2008.

Djamel ADUCH: Signature électronique, aspects techniques, réglementaires et organisationnels.

Direction des affaires criminelles et des graces : Le traitement judiciaire de la cybercriminalité, guide méthodologique,Ministère de la justice, Trait d'union le Mans, mai 2002

Henri ISAAC, Pierre Volle: E- Commerce , de la stratégie à la mise en œuvre opérationnelle,Pearson éducation France, Paris, 2008.

Henry AFTERMAN :la fraude informatique,GP.

J SOHIER :le guide d'exploration de l'internaute,éd logiques,Monteriel,1995.

Mohamed CHAWKI: Essai sur la notion de cybercriminalité, IEHEI, Juillet 2006.

M.CHAWKI :le vol d'information,quel cadre juridique aujourdhui !,droit-tic,juillet2006.

Nicolas MACAREZ, Francois LESLE :Que sais-je ?le commerce éléctronique,1ère éd,puf,2001.

Olivier AUZON: Le droit de Commerce électronique, édition du puits fleuri, 2007.

Paul BAY: Cyber stalking , harassment in the internet age and how to protect your family, British library ,2004.

Raymons GASSIN: Fraude informatique, Dalloz, 1995 , n°201et n°202.

Vincent FAUCHAUX,Pierre Depreg :Le droit de l'internaute loi, contrat et usage,litec,paris,2008.

Xavier LINANT DE BELLEFOND et Allan HOLLANDE : Pratique de droit informatique Pratique du droit de l' informatique et de l'internet, 6ème éd, Delmas, 2008,

M.Gabriel DE BORGLIE :Le droit d'auteur et l'internet,rapport du groupe de travail et de l'academie des sciences morales et politiques, cahiet des sciences morales et politiques, PUF, 2001 .

LES THESES ET SEMINAIRES :

Alexandra GREENWOOD :Le statut de l'hebergeur et le web 2,0,mémoire master 2 professionnel-droit de l'internet public,Université Paris,Sorbonne,Année universitaire 2008-2009.

Mohamed N.SALAM: Le piratage informatique, définition et problèmes- juridiques, mémoire pour l'obtention du diplôme d'études approfondies en droit interne et international des affaires, Université Libanaise, 2004

Vincent VIGNEAU: Commerce électronique et Protection des consommateurs, Master 2, droit des nouvelles technologies de l'information et de la communication ,université de Versailles- Saint- Quentin en Yvelines, année universitaire 201 0/2011.

Aissa KASMI: Situation actuelle du phénomène de la drogue en Algérie, séminaire national d'information et de sensibilisation sur les dangers de la drogue, office National de lutte contre la drogue et la Toxicomanie, Ministère de la justice, Tlemcen: 20-21 Novembre 2006.

ARTICLES :

Dr/ Ahmad A.Al-Ghadya : Digital signatures and liability issues arising out of their certification, Journal of Law, n°2, Vol 28, June 2004.

Chamoux: La loi sur la fraude informatique, de nouvelles incriminations,JCP, 1988.

Dr/ Mohamed BUZABAR: La Criminalité informatique sur l'Internet, journal of Law, No. 1, vol. 20, 2002.

Jurisclasseur,communication,2000.

Jacqueline RIFFAULT :Le blanchimant des capitaux en droit compare,RCS, n° 2,Avril-Juin ,1999.

Raymond GASSIN: Fraude informatique, Rép.Pénal. Dalloz,1995, n°201

Louise ELLISON and Yaman Akdeniz :Cyber-stalking,the rigulation of harassement on the internet,Criminal law Review,December 1998,special edition crime,Criminal Justice and the internet.

Nicolas DESURMONT :Vers une problémitique du harsselement criminel en résau,revue internationale de criminologie et de police technique,vol 49,juillet-septembre 2006.

De nouvelles incriminations,JCP , 1988,doct 3321.

ARTICLES ET RAPPORTS SUR INTERNET :

Association canadienne pour les etudes superieures : Propriété intellectuelle, un guide pour étudiants de cycle supérieur, www.acpes.ca.

Anthoni BEM : ordonnance relative a la loi HADOBI2,la protection penal de la proprieté intelectuelle et protexion des données , admin.ch.

Blanchiment des capitaux nouvelles tendances de la cybercriminalité en 2006,www.zdnet.fr.

Boij: Victims of cyber stalking, available at net on: www.firstmonday.dk

Boubaker NOBEL EL HOUSSINE: Travaux pratiques de commerce électronique, Institut des université de hautes études commerciales, de Sousse, année universitaires 2004/2005,Sousse,disponible à l'adresse: www.web2-com.com.

Brigite FILLON :La messagerie éléctronique sur internet,disponible à l'adresse suivante :www.priaf.asso.kr.

Carlo MORSELLI ,Thomas GABOR ,Jhon KIEDROWSKI,M.A :Les facteurs qui faconnent le crime organisé,Rapport n° 007,Canada,2010,www.mutah.edu.jo.

Centre canadien de la statistique juridique, collection.nlc-bnc.ca.

Cyberstalking laws ,www.haltabuse.org.

Cyberstalking, www.wikipedia.org.

Carlo MORSELLI, Thomas GABOR, Jhon KIEDROWSKI,M.A :Les facteurs qui façonnent le crime organise, Rapport n° 007, Canada, 2010 ,publications.gs.ca.

Diffinition de banque de données sur web, dictionnaire-sensageat.com.

Definition of internet,www.futura-sciences.com;

Department of computer science: A Brief history of the internet ,www.sc.ucsb.edu.and djelfa.info.

Didier GOBERT :Cadre juridique pour les signatures éléctroniques et les services de certificats,analyse de loi du 09/07/2001, www.consultandraining.com.

Deuxieme congrés des nations unies,à vienne,sous le titre « la prévention du crime et le traitement des délinquants »,10-17/04/2000, www.uncjin.org.

M le député Jean Marc NESME : Assemblée Nationale, rapport fait au nom de la commission des affaires étrangéres sur le projet de loi n°905 autorisant l'approbation de la convention sur la cybercriminalité,17/12/2004, www.assemblée-nationale.fr.

Michel BORDERA: the computer virus war, is the legal system fighting or surrending?, wings.biffalo.edu

G8 :cybercriminalité, www.finance disponible.fr.

Harassement statistic, www.haltabuse.org.

Ivana OBRADOVIC (OFDT) : legislations relatives a l'usage et a la detention de cannabis: définitions et état des lieux en Europe , Note n°2011-19, Saint-Denis, http://www.ofdt.fr.

Jean-chrysostome BOLOT,Walid DABBOUS :L'internet,historique et évolution.quel avenir prévisible ?, planéte.inria.fr.

Jed ALL: Une cyber-patrouille de police sur internet , publié le 25 mars 2005, aliquid.free.fr

Joao GODOY : Computer and international criminal law: High tech crimes and criminals,New England International and Comparative Law Annal, 2000,Lexisnexis.com.

Josselyne ABADI:Du harsselement au reseau au harcelement global .21 octobre 2011,conscience-vraie.info.

Lyes AFLOU : Le gouvernement algérien révise le Code pénal pour protéger la vie privée, 15/05/2006, Magharebia.com.

La definition de l'internet,www.lyceeb.com.

La définition du ministre de l'intérieure français ،vsabouni.free.fr et sur le site: www.interieur.gouv.fr

L'harmonisation des moyens de lutte contre la cybercriminalité, revue de web réalisé le 22/04/2004, www.finances.gouv.fr

L'impossible définition universel de la cybercriminalité, disponible à l'adresse :www.village-justice.com.

Les cybercriminels,rarement attrapés, faute de plainte, publier le 09/09/2010, disponible à l'adresse :génération.t.com.

La violation des droits de l'homme sur internet, www.educnet.education.fr.

Marcel DUBE :la protection et l'exploitation de la propriété intellectuelle,archipel.uquan.com.

Michel BORDERA :the computer virus war,is the legal system fighting or surrending ?, wings.biffalo.edu.

Margaret BEARE :les femmes et le crime organisé, rapport n° 013,Canada,2010, publications.gs.ca.

MITONGO KALONI Tresor-Ghautier : Notion de cybercriminalite، Praxis d'une penalisation delinquance electronique en droit penal Congolais, Université de Lubumbashi, 2010 , p 17, www.leganet.cd.

Quest-ce qu'une tablette tactile ? Définition, www.maisondunumérique.com.

PASEAL Alix : virtualegis,le droit de l'entreprise,3/8/2009,virtualegis.com.

Premiere sanction d'un vol de données numeriques par un tribunal,article du 3/10/2011,le figaro,lefigaro.fr.

Richmond VA:Internet Fraud Center, 9/4/03, www.ifccfbi.gov.

Sandy RIHANA :Introduction a l'internet,www.nachez.info.

Sophie HEIN: La circulation des œuvres littéraires sur les inforoutes, www.lex-electronica.or

Stalking, fr.wikipédia.org.

Service de presse nationale de fbi :Internet Fraud Center, www.ifccfbr.gov.

Thibault VERBIES:Pornographique et internet, comment réprimer ? , www.droit-technologie.org.

The Federal Networking Council: Resolution dated, October 24, 1995, definition of internet, www.Fnc.gov.

Une histoire de l'e-mail, www.arobase.org.

Us département of justice, www.justice.gov.

Vocabulaire de l'informatique et de l'internet, www.oc-money-metz.fy

Yanis DELMAS :Histoire de l'informatique,d'internet et du web,delmas-rigoutsas.nom.fr.

Y.AKDEMY et J.BELL:la vie privée et l'internet perspective du Royaume-Uni , chapitre 8, Asmp.fr

Yaman AKDENIZ: International Developments Section Of Regulation Of Child Pornography on the internet , www.cyber-righs.org.

JUGEMENTS ET DECISIONS DES TRIBUNAUX ETRANGERS:

T.G.I PARIS,réf 30 Avril 1997, d 1998, somm convenentes.

T.G.I PARIS, 14/08/1999 , La mise à disposition d'œuvres de Jacques BREL et de Michel Sardou sur un site internet reproduites sans autorisation ،constitue une contrefaçon ،Art Music/ ENST et ECP. Sté ،Edition Pouchenel/ F. X. Bergot Brel ,http:// juriscom.net6.

T.G.I Paris, 1 CH.Correctionelle, Jugement du 16 Decembre 1996, www.legalis.net.

T.G.I de Clermont-Ferrand, Chambre Correctionelle, Jugement du 26 Septembre 2011, www.legalis.net.

United States Cour of Appeal: USA V.Abraham Jacob Alkhabaz, January 29,1997, 104f.3d, 1492, en.wikipedia.org.

CA Anvers, 13/12/1984, Paris,RDIT, 1986.

Cass.Crim, 12/01/1989,Bull.Crim,n°4.

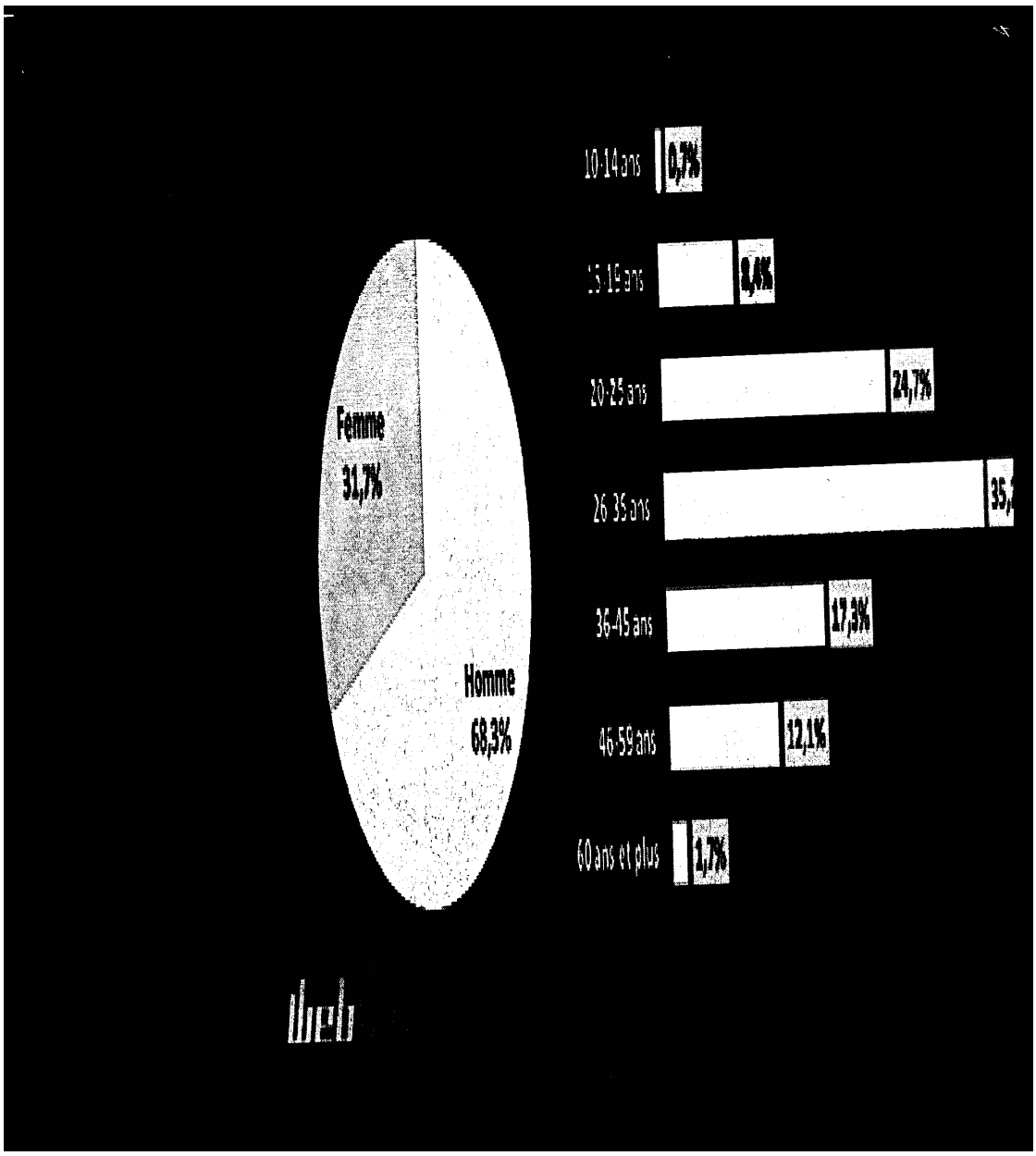
Diffamation et injures sur l'internet : le Tribunal de grande instance est déclaré compétent, Ordonnance du 22 janvier 2003 du TGI Paris , http:// www.foruminternet.org,

Décision n°2004-496 DC, 10 juin2004 du conseil constitutionnel, www.droit-tic.com

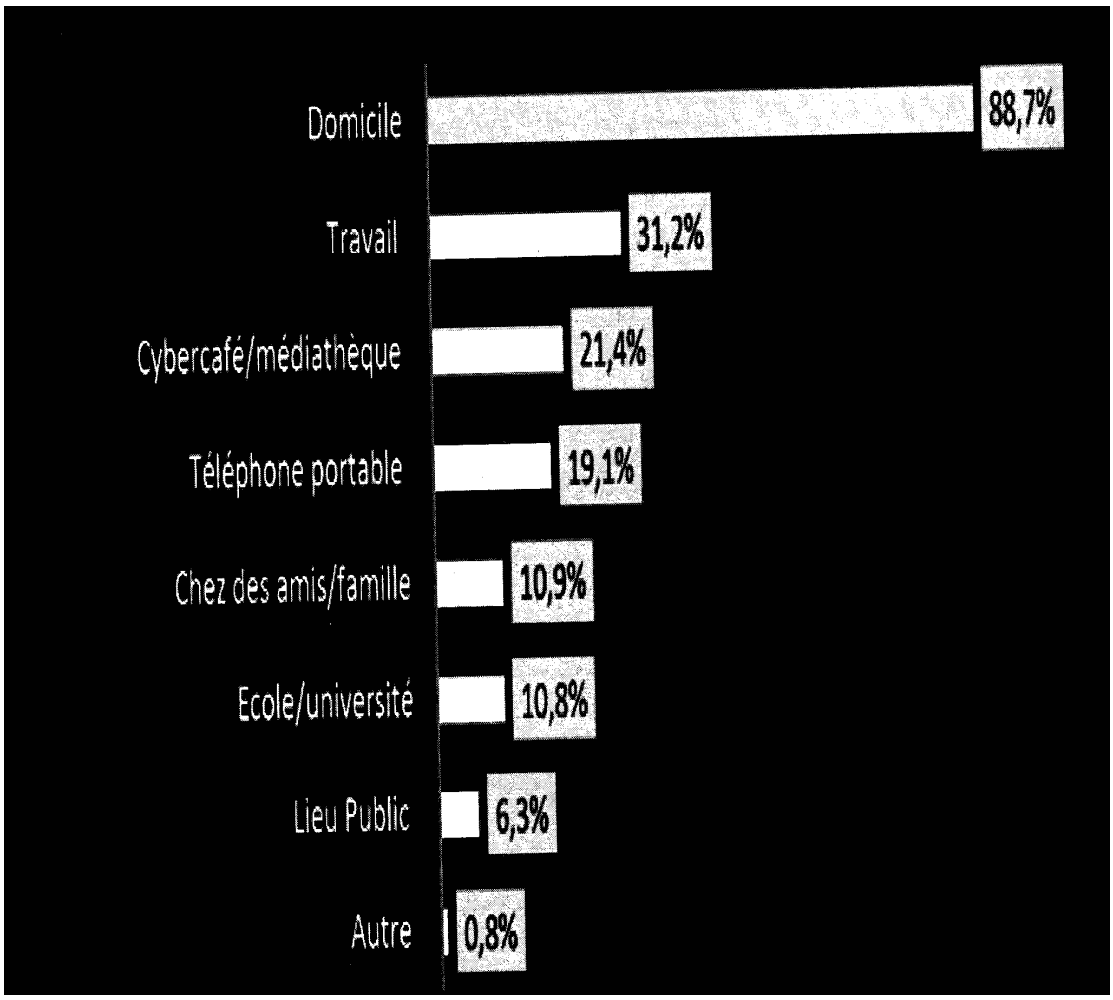
الملاحق

الملحق الأول

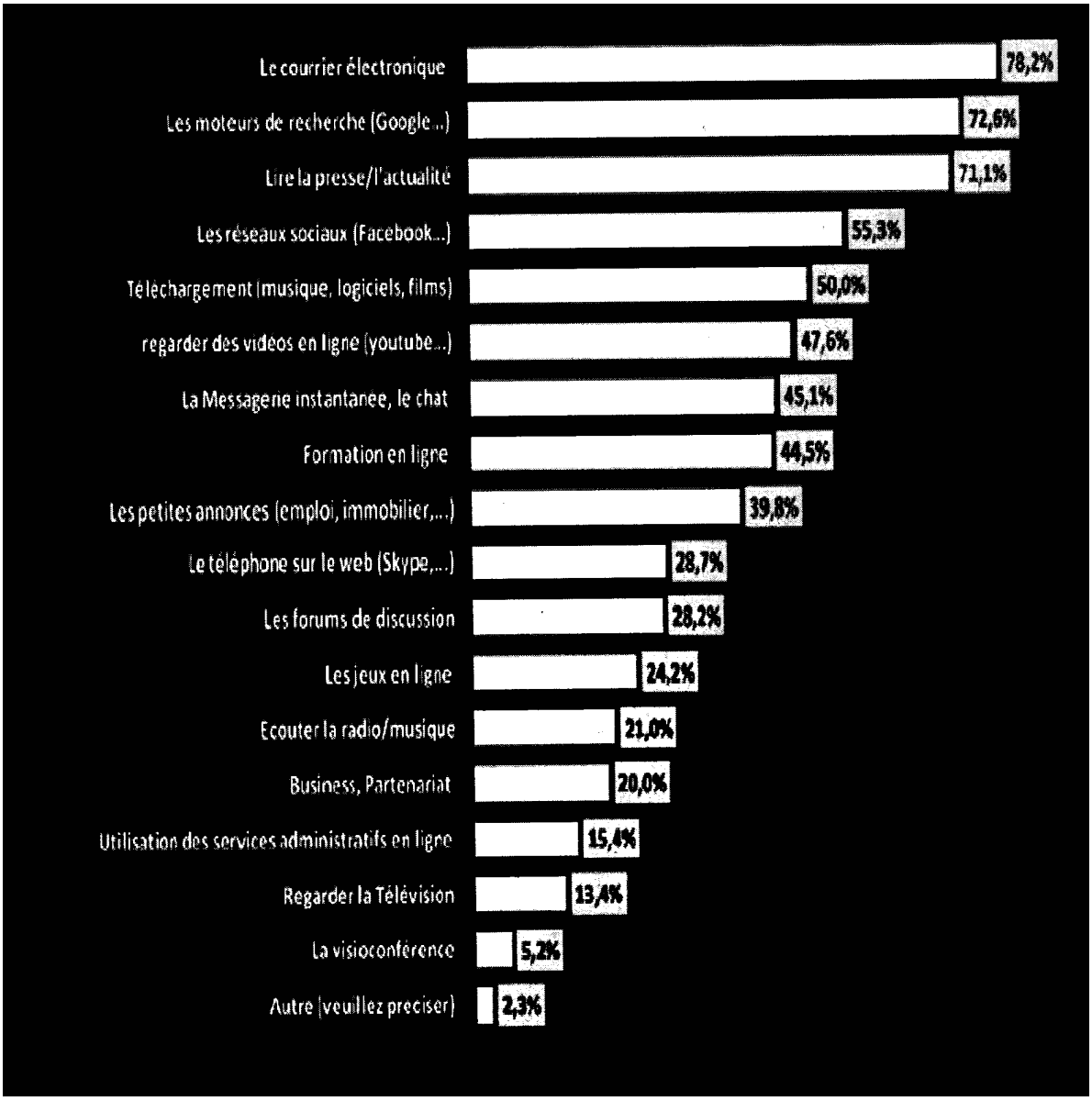
1. إحصائيات حول مستخدمي الانترنت في الجزائر
2. إحصائيات عدد مستخدمي الانترنت في الجزائر وفق الجنس (ذكر أو أنثى) والسن
3. إحصائيات حول نسبة الجزائريين المتصلين بالانترنت وفقا للأماكن المتواجدين فيها
4. إحصائيات حول اهتمامات المستخدم الرئيسية عبر ارتباطه بالانترنت في لجزائر
5. إحصائيات حول اهتمامات الجزائريين فيما يخص الخدمات التي تقدمها الانترنت من التوظيف و البيع عبرها



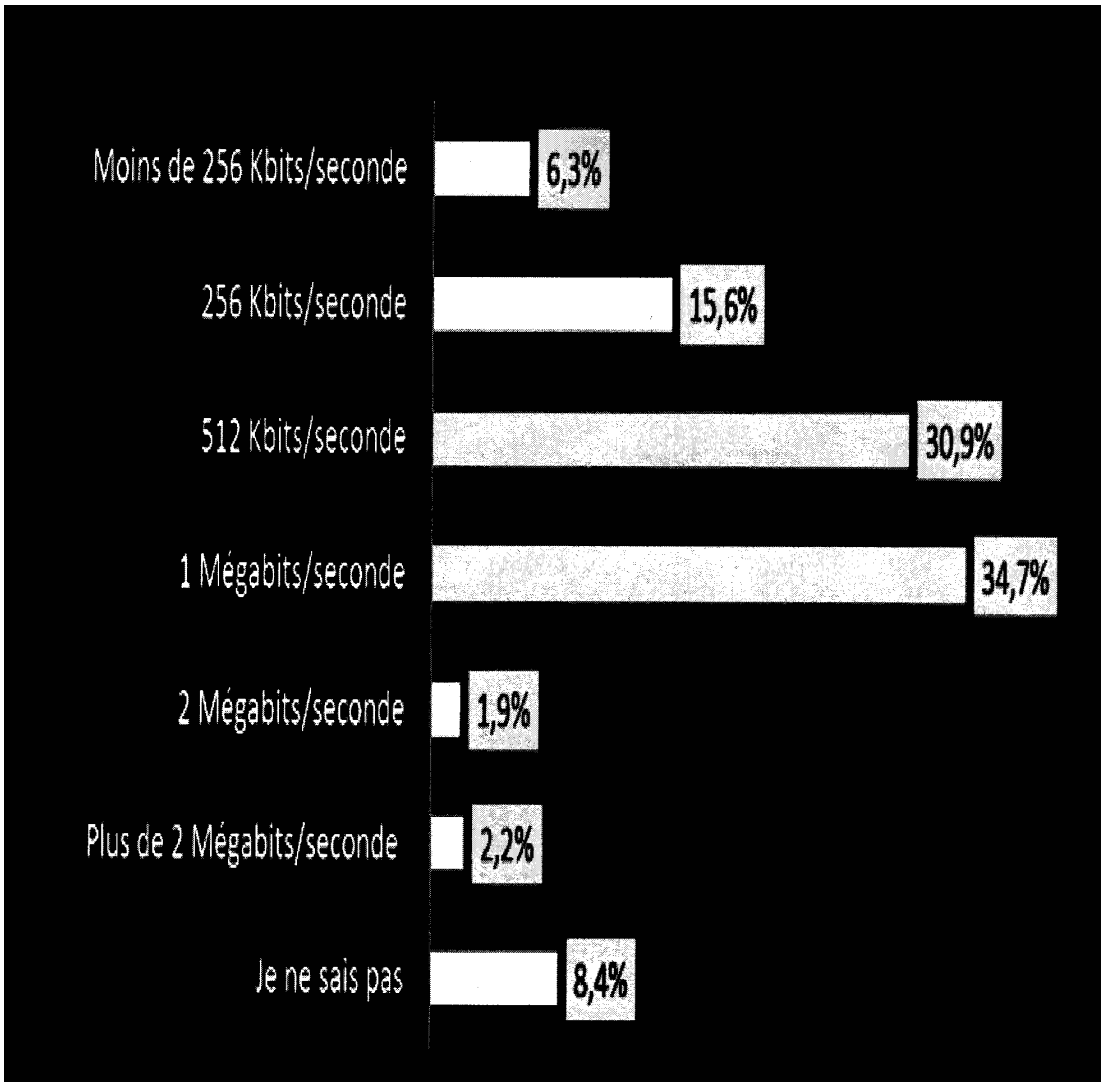
إحصائيات حول عدد مستخدمي الانترنت في الجزائر



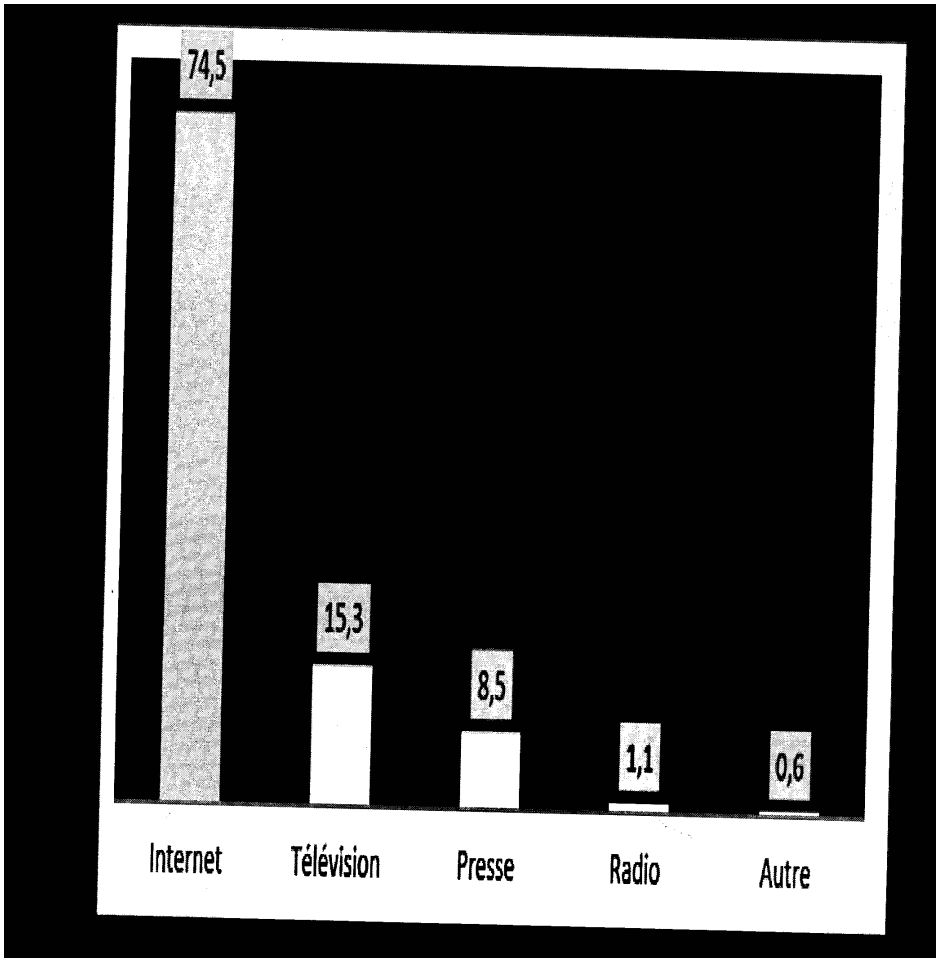
إحصائيات حول نسبة الجزائريين المتصلين بالانترنت وفقا للأماكن المتواجدين فيها



إحصائيات حول اهتمامات المستخدم الرئيسية عبر ارتباطه بالانترنت في الجزائر



إحصائيات حول اهتمامات المستخدم الرئيسية عبر ارتباطه بالانترنت في الجزائر



إحصائيات حول اهتمامات الجزائريين فيما يخص الخدمات التي تقدمها الانترنت
من التوظيف و البيع عبرها

الملحق الثاني

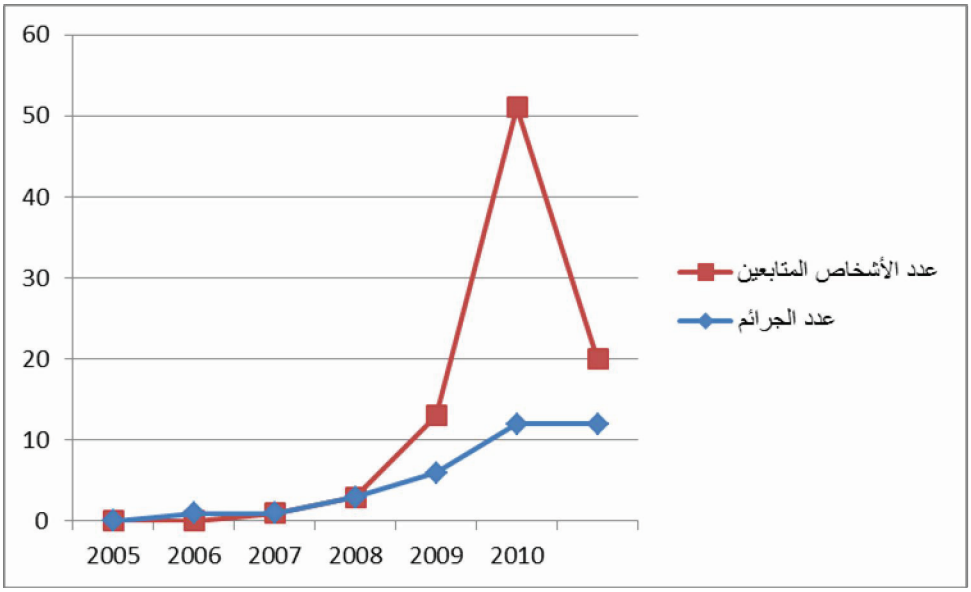
1- قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم وعدد الأشخاص التابعين (إلى غاية 30 أفريل 2010)

2- قضايا المساس بأنظمة المعالجة الآلية للمعطيات مفصلة حسب نوعها (2005 - أفريل 2010)

3- معلومات عن ضحايا جرائم المساس بأنظمة المعالجة الآلية للمعطيات

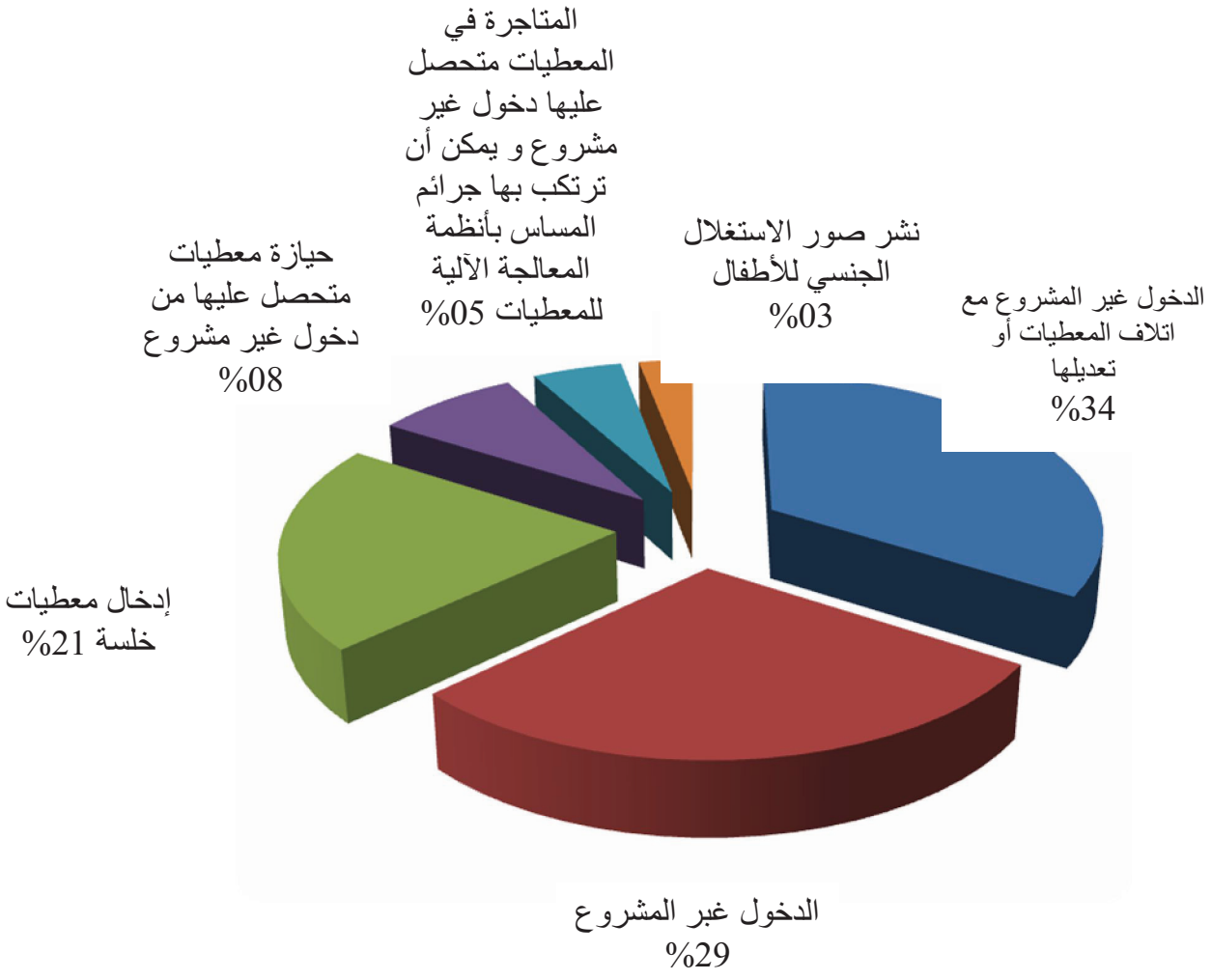
قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم وعدد الأشخاص التابعين (إلى غاية 30 أفريل 2010)

السنة	2005	2006	2007	2008	2009	2010	المجموع
عدد الجرائم	01	01	03	06	12	12	35
عدد الأشخاص المتابعين	00	01	03	13	51	20	88



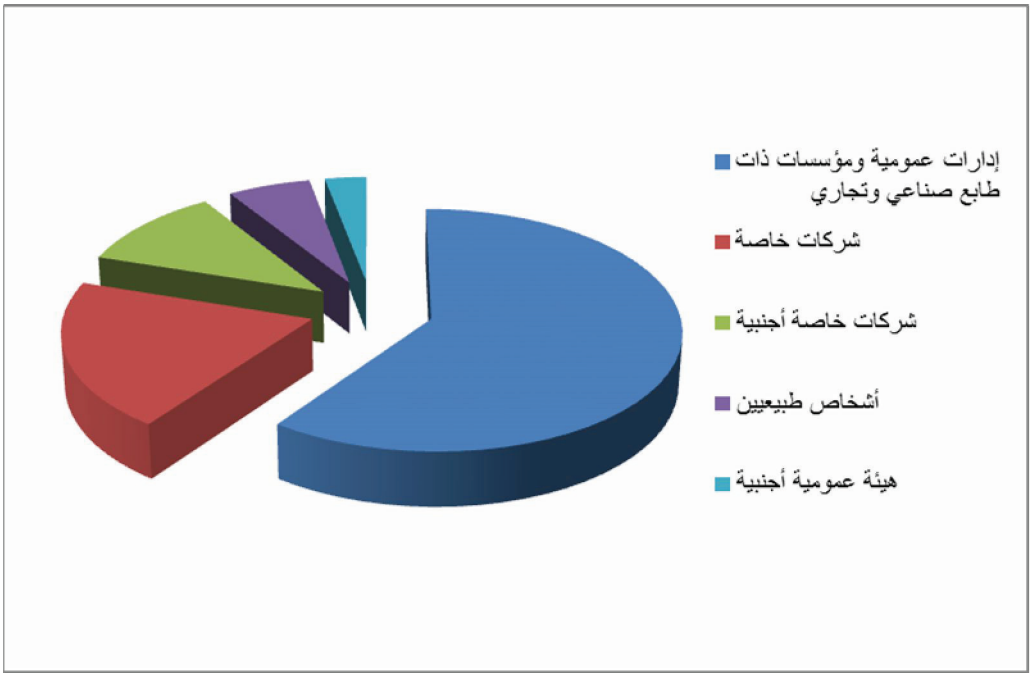
قضايا المساس بأنظمة المعالجة الآلية للمعطيات مفصلة حسب نوعها (2005 - أفريل 2010)

نوع الجريمة	العدد	النسبة المئوية
الدخول غير المروع مع اتلاف المعطيات أو تعديلها	13	%34
الدخول غبر المشروع	11	%29
إدخال معطيات خلسة	08	%21
حيازة معطيات متحصل عليها من دخول غير مشروع	03	%08
المتاجرة في المعطيات متحصل عليها دخول غير مشروع و يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات	02	%05
نشر صور الاستغلال الجنسي للأطفال	01	%03
المجمـــــــــــــــوع	38	100



معلومات عن ضحايا جرائم المساس بأنظمة المعالجة الآلية للمعطيات

الضحية	العدد	النسبة المئوية
دارات عمومية ومؤسسات ذات طابع صناعي وتجاري	21	%60
شركات خاصة	07	%20
شركات خاصة أجنبية	04	%11
أشخاص طبيعيين	02	%06
هيئة عمومية أجنبية	01	%03
المجمـــــــــــــــوع	35	100



الملحق الثالث

1. الاتفاقية الأوروبية لجرائم الانترنت
2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الملحق الرابع

1. القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها
2. المرسوم التنفيذي رقم 98-256 المتضمن قانون البريد والمواصلات
3. الأمر رقم 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة

الفهرس

المقدمة..... 01

الفصل التمهيدي:ماهية جرائم الانترنت..... 12

المبحث الأول: تعريف جرائم الانترنت و تطورها التاريخي..... 13

المطلب الأول:تعريف جرائم الانترنت. 14

الفرع الأول: تعريف جرائم الانترنت قانونا. 14

الفرع الثاني: تعريف جرائم الانترنت فقها..... 18

الفرع الثالث: النقد الموجه لهذه التعريفات..... 23

المطلب الثاني:التطور التاريخي و إحصائيات حول جرائم الانترنت 28

الفرع الأول: التطور التاريخي لجرائم الانترنت و العوامل التي ساعدت في انتشارها..... 28

الفرع الثاني: الإحصائيات التي أجريت حول جرائم الانترنت..... 30

المبحث الثاني:خصائص جرائم الانترنت و الفرق بينها وبين غيرها من الجرائم..... 36

.المطلب الأول: خصائص جرائم الانترنت. 37

الفرع الأول: جرائم الانترنت جرائم محلها، وسيلتها شبكة الانترنت وأداة ارتكابها الحاسوب..... 37

الفرع الثاني: جرائم الانترنت عابرة للحدود و صعبة الاكتشاف. 39

الفرع الثالث: مرتكب جرائم الانترنت شخص ذو خبرة فائقة بمجال الحوسبة. 45

المطلب الثاني:الفرق بين جرائم الانترنت وغيرها من الجرائم. 55

الفرع الأول: الفرق بين جرائم الانترنت والجرائم التقليدية..... 56

الفرع الثاني: الفرق بين جرائم الانترنت و الجرائم المستحدثة المشابهة لها..... 60

خلاصة الفصل التمهيدي..... 71

الباب الأول:جرائم الإعتداء على الأشخاص عبر الانترنت..... ..... **73**

الفصل الأول:جرائم البث العلني عبر الإنترنت..... 74

المبحث الأول:الجرائم الماسة بالشرف و الاعتبار عبر الإنترنت..... 74

المطلب الأول:الأحكام العامة للجرائم الماسة بالشرف و الاعتبار..... 75

الفرع الأول:تعريف القذف والسب و التشهير..... 75

الفرع الثاني:أركان جريمة القذف و السب. 77

المطلب الثاني: جريمة القذف و السب و التشهير الواقعة عبر الانترنت..... 81
الفرع الأول: ماهية الجرائم الماسة بالشرف و الإعتبار الواقعة عبر الانترنت..... 81
الفرع الثاني: موقف التشريعات المقارنة من جريمة القذف و السب و التشهير الواقعة عبر الانترنت..... 85
المبحث الثاني:جرائم الصحافة الالكترونية و العنف عبر الانترنت..... 92
المطلب الأول:جرائم الصحافة الالكترونية. 93
الفرع الأول: الأحكام العامة لجرائم الصحافة. 93
الفرع الثاني:تعريف جرائم الصحافة الالكترونية و أركانها..... 94
الفرع الثالث: موقف التشريعات المقارنة من جرائم الصحافة الالكترونية..... 95
المطلب الثاني: جرائم العنف عبر الانترنت..... 98
الفرع الأول:تعريف جرائم العنف..... 98
الفرع الثاني: بعض النماذج الواقعية عن جرائم العنف التي تكون الانترنت سببا في وقوعها..... 100
الفصل الثاني: جرائم الإعتداء على حرمة الحياة الخاصة و جريمة المطاردة عبر الإنترنت. 103
المبحث الأول: جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت..... 104
المطلب الأول:ماهية جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت 107
الفرع الأول: تعريف جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت..... 107
الفرع الثاني: طرق الإعتداء على الحياة الخاصة عبر الانترنت..... 108
المطلب الثاني: أنواع جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت و التكييف القانوني لها..... 111
الفرع الأول: أنواع جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت..... 112
الفرع الثاني: موقف التشريعات المقارنة من جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت..... 114
المبحث الثاني:جريمة المطاردة عبر الإنترنت..... 130
المطلب الأول:الفرع الأول: تعريف جريمة المطاردة عبر الإنترنت..... 132
الفرع الثاني: الأساليب المتبعة في ارتكاب جريمة المطاردة عبر الانترنت. 133
المطلب الثاني:موقف التشريعات المقارنة من جريمة المطاردة عبر الانترنت 135
الفرع الأول: موقف التشريعات الغربية من جريمة المطاردة عبر الانترنت. 135

الفرع الثاني: موقف التشريعات العربية من جريمة المطاردة عبر الانترنت..... 139
الفصل الثالث:الجرائم الأخلاقية عبر الانترنت..... 143
المبحث الأول:جرائم انتهاك الآداب العامة الواقعة عبر الإنترنت. 144
المطلب الأول:ماهية جريمة انتهاك الآداب العامة الواقعة عبر الانترنت..... 144
الفرع الأول: تعريف جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت. 144
الفرع الثاني: أركان جريمة انتهاك الآداب العامة الواقعة عبر الإنترنت. 145
المطلب الثاني:موقف التشريعات المقارنة من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت. 147
الفرع الأول: موقف التشريعات الغربية من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت. 147
الفرع الثاني: موقف التشريعات العربية من جريمة انتهاك الآداب العامة الواقعة عبر الانترنت. 149
المبحث الثاني:الجرائم الجنسية عبر الانترنت. 153
المطلب الأول:ماهية الجرائم الجنسية عبر الانترنت. 155
الفرع الأول: تعريف الجرائم الجنسية الواقعة عبر الانترنت. 155
الفرع الثاني:أسباب انتشار الجرائم الجنسية الواقعة عبر الانترنت. 156
الفرع الثالث: طرق و أساليب نشر الجرائم الجنسية الواقعة عبر الانترنت..... 159
المطلب الثاني:التكييف القانوني للجرائم الجنسية الواقعة عبر الانترنت. 160
الفرع الأول: الجهود الدولية في مكافحة الجرائم الجنسية الواقعة عبر الانترنت. 160
الفرع الثاني: موقف التشريعات المقارنة من الجرائم الجنسية الواقعة عبر الانترنت..... 163
خلاصة الباب الأول..... 174
الباب الثاني:جرائم الإعتداء على الأموال عبر الانترنت..... ..... **176**
الفصل الأول:جريمة السرقة والنصب والإعتداء على الملكية الفكرية عبر الانترنت...... **177**
المبحث الأول:جريمة السرقة عبر الانترنت..... 177
المطلب الأول:ماهية السرقة عبر الانترنت. 178
الفرع الأول: تعريف السرقة عبر الانترنت..... 178
الفرع الثاني: أركان السرقة عبر الانترنت. 179
المطلب الثاني:موقف التشريعات المقارنة من جريمة السرقة عبر الانترنت..... 187
الفرع الأول: موقف التشريعات الغربية من جريمة السرقة عبر الانترنت. 187

الفرع الثاني: موقف التشريعات العربية من جريمة السرقة عبر الانترنت. 189
المبحث الثاني:جريمة النصب عبر الانترنت..... 191
المطلب الأول:تعريف النصب عبر الانترنت و أشكاله. 192
الفرع الأول: تعريف جريمة النصب عبر الانترنت..... 192
الفرع الثاني: أشكال النصب عبر الانترنت. 194
المطلب الثاني:موقف التشريعات المقارنة من جريمة النصب عبر الانترنت..... 196
الفرع الأول: موقف التشريعات الغربية من جريمة النصب عبر الانترنت. 197
الفرع الثاني: موقف التشريعات العربية من جريمة النصب عبر الانترنت. 200
المبحث الثالث:جرائم الإعتداء على الملكية الفكرية عبر الإنترنت..... 204
المطلب الأول:جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت..... 206
الفرع الأول: تعريف جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت..... 207
الفرع الثاني: أركان جريمة الإعتداء على الملكية الأدبية و الفنية عبر الإنترنت..... 207
المطلب الثاني:المعالجة القانونية لجريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت... 216
الفرع الأول: المعالجة القانونية الدولية لجريمة الإعتداء على الملكية الأدبية و الفنية عبر الانترنت. 217
الفرع الثاني: موقف التشريعات المقارنة من جريمة الإعتداء على الملكية الأدبية والفنية عبر الإنترنت. 220
الفصل الثاني:جريمة غسل الأموال والمخدرات عبر الإنترنت..... 227
المبحث الأول: جريمة غسل الأموال عبر الإنترنت..... 228
المطلب الأول:تعريف جريمة غسل الأموال عبر الإنترنت ومراحلها. 231
الفرع الأول: تعريف جريمة غسل الأموال عبر الإنترنت..... 231
الفرع الثاني: مراحل عملية غسل الأموال عبر الإنترنت 233
المطلب الثاني: طرق ووسائل غسل الأموال عبر الإنترنت و التكييف القانوني لهذه الجريمة... 235
الفرع الأول:طرق ووسائل غسل الأموال عبر الإنترنت..... 235
الفرع الثاني: موقف التشريعات المقارنة من جريمة غسل الأموال عبر الانترنت..... 242
المبحث الثاني:جريمة المخدرات عبر الإنترنت..... 248
المطلب الأول:تعريف جريمة تكنلجة المخدرات وطرق نشرها عبر الإنترنت..... 250
الفرع الأول: تعريف جريمة تكنلجة المخدرات 250
الفرع الثاني: طرق نشر ثقافة المخدرات والمؤثرات العقلية عبر الإنترنت..... 251

المطلب الثاني:المعالجة القانونية لجريمة المخدرات عبر الانترنت..... 256
الفرع الأول: الجهود الدولية المبذولة في قمع و الوقاية من المخدرات والمؤثرات العقلية عبر الانترنت..... 256
الفرع الثاني: موقف التشريعات المقارنة من جريمة تكنلجة المخدرات و المؤثرات العقلية. 258
الفصل الثالث:جرائم الإعتداء على التجارة الإلكترونية عبر الإنترنت..... **264**
المبحث الأول:جرائم الإعتداء على مواقع و بيانات التجارة الإلكترونية..... 266
المطلب الأول:جرائم الإعتداء على مواقع التجارة الإلكترونية..... 267
الفرع الأول: جريمة الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات..... 267
الفرع الثاني: جريمة الإخلال بنظام المعالجة الآلية. 278
المطلب الثاني:الجرائم المتعلقة بتداول البيانات الخاصة بالتجارة الإلكترونية..... 280
الفرع الأول: جريمة التعامل في البيانات بدون ترخيص..... 284
الفرع الثاني: جريمة انتهاك سرية و خصوصية البيانات..... 284
الفرع الثالث: جريمة التصريح عمدا بمعطيات خاطئة..... 284
المبحث الثاني: جرائم الإعتداء على بطاقات الائتمان عبر الإنترنت. 283
المطلب الأول:ماهية بطاقات الائتمان..... 284
الفرع الأول: تعريف بطاقات الائتمان. 284
الفرع الثاني: خصائص بطاقات الإئتمان. 285
المطلب الثاني:ماهية جرائم الإعتداء على بطاقات الائتمان عبر الإنترنت..... 287
الفرع الأول: تعريف الجرائم الواقعة على بطاقات الائتمان عبر الانترنت و أركانها..... 287
الفرع الثاني: الأساليب المعتمد عليها في الجرائم الواقعة على بطاقات الائتمان عبر الانترنت. 289
المطلب الثالث: موقف التشريعات المقارنة من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت. 293
الفرع الأول: موقف التشريعات الغربية من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت. 293
الفرع الثاني: موقف التشريعات العربية من الجرائم الواقعة على بطاقات الائتمان عبر الانترنت. 294
المبحث الثالث:جريمة العدوان على التوقيع الإلكتروني عبر الإنترنت. 299

المطلب الأول:تعريف التوقيع الالكتروني. 300
الفرع الأول: التعريف القانوني للتوقيع الإلكتروني. 300
الفرع الثاني: التعريف الفقهي للتوقيع الالكتروني. 303
المطلب الثاني:ماهية جريمة العدوان على التوقيع الالكتروني عبر الإنترنت..... 304
الفرع الأول: تعريف جريمة العدوان على التوقيع الالكتروني عبر الإنترنت..... 304
الفرع الثاني: أركان جريمة العدوان على التوقيع الالكتروني عبر الإنترنت..... 305
المطلب الثالث:موقف التشريعات المقارنة من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت..... 306
الفرع الأول: موقف التشريعات الغربية من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت. 307
الفرع الثاني: موقف التشريعات العربية من جريمة العدوان على التوقيع الالكتروني عبر الإنترنت. 307
خلاصة الباب الثاني..... 309
الباب الثالث:جرائم العدوان على أمن الدولة عبر الإنترنت..... 311
الفصل الأول: الإرهاب عبر الانترنت..... 313
المبحث الأول:الأحكام العامة للإهاب. 313
المطلب الأول:ماهية الإرهاب..... 314
الفرع الأول: تعريف الإرهاب و خصائصه. 314
الفرع الثاني: أشكال الإرهاب و نتائجه. 322
المطلب الثاني:الفرق بين الإرهاب و بين ما يشابهه من جرائم. 327
الفرع الأول: الإرهاب و الجريمة السياسية و العنف السياسي. 327
الفرع الثاني: الإرهاب و الجريمة المنظمة و جريمة احتجاز الرهائن. 328
المطلب الثالث:الأسباب و العوامل المساعدة على انتشار الإرهاب..... 330
الفرع الأول:الأسباب المباشرة..... 330
الفرع الثاني:الأسباب غير المباشرة. 331
المبحث الثاني:ماهية الإرهاب عبر الانترنت..... 332
المطلب الأول:تعريف الإرهاب عبر الانترنت و خصائصه..... 333
الفرع الأول: تعريف الإرهاب عبر الانترنت. 333
الفرع الثاني:خصائص الإرهاب عبر الإنترنت..... 335

المطلب الثاني:الفرق بينه وبين الإرهاب التقليدي و العوامل المساعدة في انتشاره..... 346
الفرع الأول: الفرق بينه و بين الإرهاب التقليدي..... 337
الفرع الثاني:العوامل المساعدة في انتشار الإرهاب عبر الإنترنت..... 338
المطلب الثالث:أشكال الإرهاب عبر الإنترنت و موقف التشريعات المقارنة منها 339
الفرع الأول: أشكال الإرهاب عبر الإنترنت 340
الفرع الثاني:موقف التشريعات المقارنة من جريمة الإرهاب عبر الانترنت 356
الفصل الثاني:التجسس عبر الإنترنت **361**
المبحث الأول:الأحكام العامة للتجسس..... 362
المطلب الأول:ماهية التجسس. 362
الفرع الأول: تعريف التجسس و تطوره التاريخي. 362
الفرع الثاني: طبيعة التجسس القانونية و أنواعه. 366
المطلب الثاني:الفرق بين التجسس و الخيانة 368
الفرع الأول: المذهب الموضوعي 369
الفرع الثاني:المذهب الذاتي. 369
الفرع الثالث: معيار الجنسية. 370
المبحث الثاني:ماهية التجسس عبر الانترنت 371
المطلب الأول:تعريف التجسس عبر الانترنت و الأساليب المتبعة فيه. 372
الفرع الأول: تعريف التجسس عبر الانترنت. 372
الفرع الثاني: الأساليب الحديثة المتبعة في التجسس عبر الانترنت: 373
المطلب الثاني:موقف التشريعات المقارنة من جريمة التجسس عبر الانترنت. 375
الفرع الأول: موقف التشريعات الغربية من جريمة التجسس عبر الانترنت. 375
الفرع الثاني: موقف التشريعات العربية من جريمة التجسس عبر الانترنت..... 381
خلاصة الباب الثالث..... 385
خاتمة..... 386
المراجع..... 398
الملاحق
الفهرس