الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة أبي بكر بلقايد –تلمسان–

كلية الحقوق والعلوم السياسية

قسم الحقوق

أمن المعلومات في بيئة الأعمال الإلكترونية

رسالة لنيل شهادة الدكتوراه في القانون العام

إعداد الطالب :

- مليانى عبد الوهاب

إشراف الأستاذ الدكتور:

* عبد القادر بن مرزوق

لجنة المناقشة :

الدكتور دلال يزيد	أستاذ محاضر "أ"	جامعة تلمسان.....	رئيسا
أ.الدكتور عبد القادر بن مرزوق	أستاذ محاضر "أ"	جامعة تلمسان	مشرفا و مقررا
الدكتور مراد قربيز	أستاذ محاضر "أ"	جامعة الأغواط	مناقشا
الدكتور لخضر بن عطية	أستاذ محاضر "أ".	جامعة الأغواط	مناقشا

السنة الجامعية : 2016– 2017

كلمة شكر وتقدير

الحمد لله رب العالمين حمدا يوافي نعمه ويدفع نقمه ويكافئ مزيده
لا ندعي أننا حققنا القصد وأشرفنا على الغاية فذلك طموح نسعى إليه ونسأل الله تحقيقه وبلوغ مرتبته، ولا شك أن دراستنا هاته لا تخلو من الملاحظات وشفيعنا في ذلك سلامة القصد وحسن النية وبذل الجهد.
أتقدم بالشكر الجزيل إلى الأستاذ الفاضل **الدكتور عبد القادر بن مرزوق** الذي لم يبخل علينا بنصائحه وإرشاداته العلمية والمنهجية في سبيل اتمام وإنجاز هذا العمل المتواضع.
كما لا يفوتني في هذا المقام أن أتوجه بالشكر الجزيل إلى أعضاء اللجنة المكلفة بمناقشة هاته الرسالة كل من :
الدكتور دلال يزيد، الدكتور مراد قريبيز، والدكتور لخضر بن عطية
وكذا الشكر الخاص إلى جميع أساتذة وإداريي قسم الحقوق بكلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد بتلمسان.

عبد الوهاب مليانى

قائمة أهم المختصرات المستعملة:

د.م.ج: ديوان المطبوعات الجامعية.

د.م: دون مكان النشر.

ب. س. ن: بدون سنة نشر.

ج.ر.ت: الجريدة الرسمية للمناقشات.

ج: الجزء.

ط : طبعة .

ب. ط : بدون طبعة .

د. ط : دون طبعة .

د. س : دون سنة .

Liste des principale abréviation utilisées:

ART: article.
a.d.s.l: asymmetrical digital sulocriber line.
b.d.r.i.j: des brigades clépartementales de recherche et d'investigation… judiciaire de la gendarmerie.
Bull: bulletin criminel.
Ch: chambre.
c.p.f: code pénale français.
c.p.p.f: code de procédure pénale français.
c.c.c: convention sur la cybercriminalité.
Corr: correctionnel.
c.a: cour d'appel.
c.p.t.e.f: code des postes et des communications électroniques… français.
Décis: décision.
Décr: décret.
Doc: documentation.
http: hypertext transfer protocol.
i.r.c.g.n: l'institut de recherché criminelle.
i.p: internet Protocol.
j.o.r.f: journal officiel de la république française.
Juris: jurisprudence.
j.c.p: juris- classeur périodique (semaine juridique).

l.c.e.n: loi pour la confiance dans l'économie numérique.
l.s.i.f: loi pour la sécurité intérieure en France.
n.c.p: nouveau code pénale.
N°: numéro.
Oecd: organisation de coopération et de développement économiques.
o.c.l.c.t.i.c: l'office central de lutte contre la criminalité liée aux technologies… de l'information et de la communication.
Op.cit: ouvrage précité.
P: page.
p.d.a: personale digital assistant.
Rapp: rapport.
r.s.c.p.c: revue de science criminelle étude droit pénale comparé.
r.s.c.p: revue de science criminelle et de droit pénale.
r.i.d.p: revue international du droit pénal.
s.t.r.j.d: service technique de recherche judiciaire et de documentation.
s.t.a.d: système de traitement automatisé de données.
Tcp/ip: transmission control Protocol/ internet Protocol.
Trib: tribunal correctionnel.
t.r.g: tribunal de grande instance.
Wi-fi: wireless fidelity.
www: the world wide web.

منذ قرن أو يزيد ، حينما توصل العالم لتقنية البرق و الهاتف إعتقدت الدول و الشعوب أن هذا هو ذروة الإبداع في مجال الإتصالات التي تساعد الأشخاص على التخاطب من مسافات متباعدة تقاس بآلاف الكيلومترات . و لم يكن بمقدورهم تصور أن العلم سيحقق إنجازات تختصر المكان و الزمان من خلال وسائل إتصالية لم تكن لتخطر لهم ببال ، و التي تجعل من الكرة الأرضية بقاراتها و بلدانها عبارة عن قرية صغيرة ، فلقد تطورت تلك الوسائل بالخصوص في إطار الإتصالات السلكية و اللاسلكية بشكل غير مسبوق ، فدخلت الأقمار الصناعية على خط الإتصالات ، على نحو أدى لظهور طفرة نوعية و كمية في حجم الإتصالات التي تتم عن طريق هذه الأقمار .

و صاحب ذلك التطور ظهور الحاسوب الذي تطور هو الآخر بشكل متسارع جدا نظرا لتقدم علم الإلكترونيات ، هذا ما نتج عنه تطور في إستخدامات الحاسوب و تطبيقاته .

و بظهور شبكة الأنترنت كوسيلة إتصالات عالمية ساهمت في تقارب الشعوب و الثقافات و ما زاد من قيمتها هو ظهور الهاتف المحمول و ما صاحبه من تطور حتى أصبح متعدد الإستعمالات بما في ذلك مميزات الحاسوب خاصة ان كان مرتبطا بشبكة الأنترنت ، و هو بهذا يقدم خدمة جليلة للبشرية ، فيكفي أنه يقدم خدمة إتصالية تواصلية بأي شخص و في أي وقت أيا كان مكانه و على مدار الساعة .

هذا التطور الهائل و السريع في تقنيات الإتصال الحديثة أدى إلى دخول العالم في عصر أطلق عليه إسم عصر المعلومات أو ثورة المعلوماتية أو غيرها من التسميات و التعبيرات الدالة على المعنى ذاته ، فقد إنسابت المعلومات من كافة مصادرها عن طريقها و بواسطتها نظرا لإلتفاف الأشخاص و الجماعات و الدول حولها و ذلك من مختلف القارات و البلدان و الأجناس حيث فعلت هذه التقنية ما لم تفعله السياسة في توحيد الشعوب و الثقافات .

فمن ثمانينات القرن الماضي أدت التطورات الحاصلة في تقنية المعلومات الى تدفق سيل من المعلومات التي يصعب إدراك حجمها و تنوعها و كثافتها ، خاصة بنماء هندسة البرمجيات و

صناعتها مع اندماجها بتكنولوجيا الإتصالات و الحواسيب المتطورة هي أيضا ، و التي وصلت بعملية الدمج إلى اخراج العمليات المختلفة في بيئة ذات طبيعة خاصة تسمى نظام المعالجة الآلية للمعلومات و الذي نطلق عليها في دراستنا هذه تسمية النظام المعلوماتي .

فلا ريب الآن أن تلك النظم عرفت إنتشارا واسعا خاصة لإرتباطها بالحواسيب و شبكة الأنترنت ذات الصبغة العالمية و التي تتحدد قيمتها لا من حيث مشتركيها فقط بل حتى من القدرة على تبادل المعلومات في تلك البيئة الإفتراضية ، فعادت من ضروريات الحياة اليومية سواء بالنسبة للاشخاص الطبيعية ام المعنوية العامة منها او الخاصة ، بل إن الدول و الحكومات في وقتنا الحالي إتجهت لتسيير أعمالها أساسا على إستخدام نظم المعلوماتية و هذا بالنظر لما تتميز به من سرعة و دقة في معالجة المعلومات الإلكترونية من تجميع لها و تخزين و استرجاع و تبادلها بين الأشخاص داخل الدولة أو خارجها ، لهذا أصبحت مكمن سرهم فيما تعلق بحياتهم الشخصية أو بطبيعة معاملاتهم المختلفة المالية منها على الخصوص و الإقتصادية بصفة عامة ، كما أنها مكمن أسرار الدولة و البنوك و المؤسسات الإقتصادية .

و بالرغم من المزايا المكتسبة بفضل التطور في تقنية المعلومات في شتى المجالات و الميادين إلا أن هذا التطور في ذات الوقت حمل معه بذورا للشر التي كانت تنتظر من يسقيها مياه الحياة ، و سرعان ما وجدت ساقيها المتمثل في المجرم المتميز بخصائص جد خاصة تميزه عن غيره من المجرمين العاديين و هو ما يطلق عليه تسمية المجرم المعلوماتي ، هذا الأخير الذي وجد ضالته التي كان يبحث عنها في تلك التقنية الحديثة للمعلومات التي أتاحت له فرصة إرتكاب الجريمة و الحصول من ورائها على أكبر قدر ممكن من النتائج الإجرامية التي يهدف إليها بأقل قدر ممكن من الخسارة و المخاطرة ، معتمدا على ما يمتلكه من مهارة فنية أو تقنية في هذا الصدد.

و صنفت الجرائم المرتبطة بتقنية المعلومات الى طائفتين من الناحية العامة ، طائفة أولى يعد فيها النظام المعلوماتي وسيلة لإرتكاب الجريمة ، بينما الطائفة الثانية يكون محل الإعتداء فيها هو النظام المعلوماتي و هي محور دراستنا على أساس أنها البيئة التي تتواجد فيها المعلومات الإلكترونية

و هو ما قصدناه في عنونة موضوع البحث لمّا وظفنا صيغة بيئة الأعمال الإلكترونية[1] و التي نعني بها كل عمل إلكتروني يكون محله النظام المعلوماتي مهما كان نوعه أو شكله او الجهة التي تقوم به ، و لا نقصد به المفهوم الضيق له المتعلق بإقتصاد المعرفة ، و لهذا ستكون دراستنا مبنية على الأعمال الإلكترونية التي محلها النظام المعلوماتي بإختلاف أشكالها و تصوراتها في حالة ما تم الإعتداء عليها و هو ما نقصده بالأمن لذى إخترناه كعنوان لموضوعنا من خلال توظيفه في إطار أمن المعلومات في بيئة الأعمال الإلكترونية .

فالخطورة التي تتجلى يوما بعد يوم لهذه الجرائم تتمثل بالخصوص في أنها سهلة الإرتكاب نتيجة الإستخدامات السلبية للتقنية المعلوماتية بما توفره من تسهيلات ، هذا بالإضافة الى أنها عابرة للحدود الدولية ، إضافة للميزات التي يمتاز بها المجرم المعلوماتي من ذكاء و معرفة تقنية ، هذا بالإضافة الى الطبيعة المتميزة لمحل الإعتداء و المتمثل في المعلومات المتواجدة في تلك البيئة المتميزة مع أننا سنتكل بصفة عامة و متواصلة طيلة الدراسة عن النظام المعلوماتي على أساس أنه خزان المعلومات الإلكترونية بل إنه يمثل أساس تداولها فلولاه لما كانت المعلومات الإلكترونية محل دراستنا فهو الثغرة او المكان الذي يجد فيه المجرم المعلوماتي ضالته المتمثلة في المعلومات الإلكترونية ، وذلك بإختراقه للنظام المعلوماتي ، الإطلاع عليها بطريق غير مشروع ، أو تخريبها ، أو إتلافها .....

و لمّا كان الحال كما ذكرناه أعلاه نجد أن المشرع الجنائي إتخذ موقفا حاسما في العديد من الدول بوضع نصوص خاصة لإضفاء حماية للنظام المعلوماتي من الأفعال التي تشكل تهديدا عليه فأضفى عليها الصبغة التجريمية .

[1] يستعمل مصطلح الأعمال الإلكترونية e-business. في جميع الأوجه الخاصة بالأعمال، من عولمة وتحسين للإنتاجية وإدارة لأوقات الانتظار وبحوث تسويقية وتقاسم للمعلومات مع المؤسسات والأفراد الآخرين. ويُعَدُّ الانتقال من نمط الأعمال التقليدية إلى نمط الأعمال الإلكترونية أمراً جديداً في عالم الأعمال، وهو أبرز مظهر لما يسمى اليوم (اقتصاد المعرفة). فالمعلومات والمعرفة في المنظمات اليوم تعدَّان أصلاً مهماً من أصولها، ولا يكفي أن تمتلك المنشآت أموالا سائلة وتجهيزات وأبنية لكي تؤدي أعمالها بكفاءة، بل إن قيمة المنشأة تقدر اليوم بأصولها المعرفية وما يتراكم لديها من معلومات. ولعل الأهم في المعلومات المتراكمة لدى المنشآت هو كيفية استخدامها لمصلحة المنشأة وتطوير موقعها التنافسي وزيادة أرباحها.

و هذا الذي قام به المشرع الجزائري لما عدّل قانون العقوبات بالقانون رقم 04-15[2] و الذي أفرد فيه قسما سابعا مكرر المتضمن لثمانية مواد من المادة 394 مكرر الى المادة 394 مكرر 7 و التي عالجت عدة جوانب تجريمية لأفعال مختلفة منها الدخول أو البقاء عن طريق الغش للمنظومة المعلوماتية ، تخريب النظام المعلوماتي ، إدخال أو إزالة تعديل المعطيات في النظام المعلوماتي ،...

و جاء هذا نظرا للعولمة التي لم تعد الجزائر بمنأى عنها و الخطورة المتزايدة للإجرام المعلوماتي ، إضافة الى أن الجزائر صادقة على إتفاقية الشراكة بينها و بين الإتحاد الأوروبي المنعقدة سنة 2002و الذي صادقت عليه الجزائر بموجب القانون رقم 2003-1144 المؤرخ في 02 ديسمبر 2003 و هو القانون الذي أجاز المصادقة على الإتفاق الأورومتوسطي المؤسس للشراكة بين الإتحاد الأوروبي و الجمهورية الجزائرية الديمقراطية الشعبية .

و عزز المشرع الجزائري أمن المعلومات الإلكترونية التي نقصد بها الحماية القانونية للمعلومات الإلكترونية في شقي القانون الجنائي أي الشق التجريمي و الإجرائي و هذا بالنظر للخطورة التي تعدت الأفراد الطبيعية و المعنوية الخاصة او العامة بل إن خطرها وصل الى الدولة و أمنها العام و على قاعدة البيانات و مختلف المجالات الحيوية ...، هذا ما تطلب منه التدخل من جديد بإصداره لقانون مستقل هذه المرة و هو القانون رقم 09-04[3] المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها .

فالتطورات التقنية الواقعة لم تؤثر على الشق الموضوعي للقانون الجنائي بل إمتد أيضا إلى الشق الإجرائي له ، حيث ان تلك التطورات أثارت العديد من الإشكالات كون النصوص الإجرائية الموضوعة سابقا وضعت لمواجهة الجرائم التقليدية و التي لا تثير إشكالا في نطاقها إلا أن هذه الجرائم المستحدثة و المتميزة بطابعها التقني خلقت صعوبات و تعقيدات إجرائية كثيرة وقفت الإجراءات التقليدية امامها عاجزة لا من حيث التحقيق -بمختلف مراحله من مرحلة الضبط الى

[2] القانون رقم 04-15 ،المتضمن لجرائم المساس بأنظمة المعالجة الألية للمعطيات ، المتمم للامر رقم 66-156 المتضمن لقانون العقوبات ، الصادر بتاريخ 10 نوفمبر2004 .

[3] القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها المرخ في 05 أوت 2009 .

مرحلة المحاكمة فيها- بل وصلت الى أدلة الإثبات و مبدأ حرية الإقتناع الشخصي للقاضي الجنائي ، هذا بالإضافة الى الإشكالات الموضوعية و التي لا تقل قيمة من سابقتها و المتمثلة في التحديد الموضوعي لحقيقة الجريمة و المجرم .

فالإشكالات في مجال هذه الظاهرة الإجرامية المستحدثة متعددة الا أننا سنحصرها في الشقين السباقي الذكر نظرا لما لهما من اهمية في المجال القانوني ، و من هذا المنطلق تظهر لنا **أهمية البحث** التي نوجزها أساسا في النقاط التالية :

- معرفة تلك المشكلات القانونية التي تواجه دراسة أمن المعلومات في بيئة الأعمال الإلكترونية كونها من الإشكالات لتي تعالج نمطا جديدا و مستحدثا من انماط الجرائم و هي الجرائم المتعلقة بالمعلوماتية و بالخصوص الإعتداءات الواقعة على النظام المعلوماتي ، حيث تعتبر من المستجدات التي لم تكن معروفة على الساحتين الوطنية و الدولية بدليل ما نتج من اتفاقيات دولية و اقليمية لمكافحتها والتي منها اتفاقية بودابست المنعقدة في 23 ابريل 2001 بإشراف المجلس الأوروبي .
- من خلال المحاولة التي نقوم بها لتحليل النصوص القانونية المتضمنة لتجريم الإعتداءات الواقعة على النظام المعلوماتي لإبراز العناصر التي تقوم عليها تلك الجرائم للوصول الى مدى توفيق المشرع الجزائري من عدمه في المسائل الموضوعية .
- الوقوف عند السياسة العقابية للمشرع الجزائري و مدى نجاحها في مواجهة تلك الظاهرة المستحدثة إجراميا للحد منها و الحد هنا لا يقصد منه المنع المطلق أو الكلي بل بالعكس نريد منه المنع الوقائي الذي يصل به المشرع الجنائي لإيصال رسالته الردعية العامة للكافة بأن السلوك مجرم و معاقب عليه ، هذا بالإضافة إلى الردع الخاص للجاني مرتكب الجريمة حال ارتكابه للجرم .
- من خلال تناول الجوانب الإجرائية خاصة فيما تعلق بالدليل التقني مشروعيته و مصداقيته ومختلف الإجراءات التقليدية و المستحدثة الخاصة بالبحث عن أدلة الإتهام والتي

سنستظهر من خلال دراستها لمدى ملاءمة تلك الإجراءات في مواجهة الخطورة الإجرامية لمختلف السلوكات المهددة لأمن المعلومات الإلكترونية ، هذا بالإضافة الى التعرف لكفاءة الدولة الجزائرية في التعامل مع تكنولوجيا المعلومات و إشكالية التطبيقات الإجرائية لها .

و نرمي من خلال دراستنا هذه للوصول الى تحقيق **الأهداف** التالية :

- حيث نهدف إلى الوقوف على مفهوم جرائم الإعتداء على النظام المعلوماتي و تحديد إستقلاليتها عن باقي الجرائم التقليدية الأخرى و الذي انعكس على التشريعات التقليدية ، هذا بالإضافة لشرح مسألة مهمة جدا و التي تدخل في صلب الدراسة و المتمثلة في عجز النصوص التقليدية للتعامل مع تلك الجرائم و التي كانت سببا لتكريس قوانين خاصة تتعلق بامن النظام المعلوماتي من الإعتداءت الواقعة عليه .
- تحديد جوانب القوة و الضعف في المعالجة التشريعية في جوانبها الموضوعية لجرائم الإعتداءات على نظم المعلوماتية و ما ينتج عن ذلك من سد للثغرات القانونية التي تمكن المجرم من أن يفلت من العقاب.
- تحديد الوسائل التي بواسطتها يتم تحقيق ملاءمة أدلة الإثبات بالأدلة المتحصلة من التقنية المعلوماتية .
- تحديد الآليات الخاصة بالتحري و التحقيق في هذه الجرائم و مدى إستعداد تلك الجهات خاصة في مجال التأهيل و التدريب و التسلح بالمعرفة التقنية .
- تحديد الأجهزة المساعدة للجهات التحقيقية في الكشف عن تلك الجرائم و مدى ضبطها تشريعيا لتتناسق الجهود مع بعضها البعض.

و مما سبق يمكننا تحديد **الهدف المرجو من هذا البحث** ،و الذي نحن بصدده ، فهو يتمحور حول تحليل ظاهرة **الجرائم الواقعة على النظام المعلوماتي بإعتباره البيئة التي تتم فيها كل الأعمال المتعلقة بالمعلومات الإلكترونية** إنطلاقا من **الدراسة التأصيلية لتلك الجرائم كسبب أصيل لصدور التشريعات الخاصة بأمنها** و هذا من خلال الغوص في جوانبها القانونية

و أبعادها المختلفة لنصل الى **تحليل الإستراتيجية التشريعة** المعمول بها **لتحقيق الأمن القانوني لها من الناحية الجنائية –ببعديه الموضوعي و الإجرائي – الذي ستتركز عليه دراستنا دون الفروع الأخرى من القانون إحتراما للتخصص.**

و من هنا يظهر جليا **سبب إختيارنا لهذا البحث** حيث أنه يعد من أهم المواضيع التي ينبغي توضيحها خاصة و نحن متجهون كدولة إلى ما يعرف برقمنة الإدارة أو الحكومة الإلكترونية التي تعتبر تحولا من إدارة المعلومات الورقية إلى إدارة المعلومات الإلكترونية ، الأمر الذي يشكل خطورة حقيقية على معلومات الأفراد و المؤسسات و حتى معلومات الدولة و يضعها في مواجهة الإعتداءات من حيث تأمينها القبلي و أمنها البعدي الذي نحن بصدد دراسته أي الحماية الجنائية لها من كل إعتداء يقع عليها .

حيث أنه يقع على المشرع واجب كبير في هذه المرحلة و هو مواكبة عصر العولمة و عصر الرقمنة و يغير من المفاهيم السائدة التي تعتبر تقليدية بالنسبة لهذا العصر ، و ذلك بأن يعدل المشرع نصوصه القانونية المتوفرة لتتماشى مع مستجدات هذا العصر ، كما عليه أن يستحدث منظومة قانونية تماشيا مع المتطلبات الواقعية و المستقبلية .

و من منطلق ما سبق من الطبيعي أن تطرح الأعمال الإلكترونية كما وضحناه أعلاه و التي نقصد بها في دراستنا هذه كل عمل إلكتروني يكون النظام المعلوماتي أساس له و بيئة لتداول المعلومات الإلكترونية ، فالتساؤلات القانونية تثير العديد من الإشكالات و التعقيدات خاصة في مجال أمنها القانوني و الذي نقصد به هنا الحماية الجنائية لها ، و من هنا يأتي هذا البحث لتوضيحها و الإجابة عنها لأن عدم الكشف عنها يجعل المسألة بمثابة الثغرة القانونية .

و من جهة أخرى لاحظنا أن غالبية الدراسات و البحوث التي أجريت حول الموضوع تناولت الفكرة إما من ناحية التجارة الإلكترونية أو في إطار المعاملات التجارية ذات الصيغة الإلكترونية أو تمت بدراسة الجريمة المعلوماتية بصفة عامة دون التطرق لمضمون المعلومات الإلكترونية و التعمق فيها كما أنها مقتصرة على الجوانب الموضوعية فقط دون الولوج للجوانب الإجرائية التي لا غنى

عنها في إطار أمن المعلومات الإلكترونية وهو الذي دفعنا الى إختيار فكرة الدراسة أي أن تكون في إطار متكامل أي الجمع بين الأطر الموضوعية لأمن المعلومات الإلكترونية و الأطر الإجرائية لها كي تكون الدراسة شاملة و متكاملة ، و هذا من خلال تأصيلنا للموضوع أولا و تحليل إستراتيجية المشرع التي إنتهجها لتوفير أمن المعلومات في بيئة الأعمال الإلكترونية .

و عليه إرتأينا أن تكون دراستنا لهذا البحث وفق **منهج** يتماشى مع موضوع الدراسة و مع المعطيات التي بيّناها أعلاه كي تتلاءم مع الأهداف المسطرة ، و نظرا لتشعب الموضوع و خصوصيته إخترنا مجموعة من المناهج المعتمدة في الدراسات القانونية و التي تكمل بعضها البعض للإلمام بكل جوانب الدراسة محل البحث لهذا إخترنا :

- **المنهج الوصفي** الذي يصف الظاهرة بتحليلها لجزئيات ندرسها و نتعمق فيها لنفهم أصل الظاهرة و حقيقيتها العلمية و القانونية .

- **المنهج التاريخي** الذي يعود بنا الى الجذور التاريخية للظاهرة محل الدراسة محاولة منا لمعرفة البدايات الأولى و مدى حداثتها بشيء من التفاصيل فيما يخص العنصر البشري و الموضوعي.

- **المنهج المقارن** و الذي من خلاله نقارن التشريع الجزائري بالتشريعات المقارنة بالخصوص الفرنسي الذي يعد أصلا و بيئة يتولد منها التشريع الجزائري ، هذا بالإضافة الى الإتفاقيات الدولية ذات الصلة بموضوع الدراسة .

- **المنهج الإستدلالي** و هذا من خلال قراءة النصوص القانونية و التعمق فيا حيث نستنتج منها مدى توفيق المشرع الجزائري في توفير الحماية المطلوبة من الناحية الجنائية للمعلومات الإلكترونية و إستخراج العيوب التي يجب تداركها و إصلاحها .

- **المنهج التحليلي** و هذا من خلال تحليل الإستراتيجية التشريعية المنتهجة لتوفير الحماية للمعلومات الإلكترونية و ذلك من خلال تفكيكها الى عناصر و تحليلها من خلال النصوص القانونية الموجودة .

و وفق ما سبق و بالنظر لأهمية الموضوع خاصة لمّا أصبحت المعلومات الإلكترونية المتداولة عبر النظام المعلوماتي تشكل حجرا أساسيا في التعاملات اليومية للجميع بما فيهم الدولة ، هذا الذي رافقه العديد من المسائل القانونية الموضوعية و التطبيقية التي واكبت الحركية الواسعة و السريعة و حتى المتطورة يوما بعد يوم بل يمكننا القول ان التطور يقاس بالثواني في هذا المجال اي مجال التقنية التكنولوجية ، و من بين تلك المسائل نجد مسألة الأمن القانوني للمعلومات الإلكترونية في بيئة الأعمال الإلكترونية بالتحديد في المجال الجنائي حيث تتطلب الدراسة البحث عن مضمون الجرائم التي بموجبها يتم الإعتداء على المعلومات الإلكترونية في تلك البيئة الخاصة و المتميزة الأمر الذي جعلها تستقل عن باقي الجرائم الأخرى و هذا الذي جعل المشرع يخصها بنصوص مستقلة عن النصوص الجنائية التقليدية، و من منطلق ما سبق يمكننا عرض **الإشكالية التي يطرحها الموضوع التي ترتبط أساسا بالمعالجة التشريعية لأمن المعلومات الإلكترونية في بيئة الأعمال الإلكترونية بالتحديد طبيعة الجرائم التي ترتكب عليها ، من حيث تمييزها عن غيرها وصولا إلى مدى إستقلاليتها عن غيرها من الجرائم ، و إنعكاس ذلك على النصوص التشريعية في المجال الجنائي ، و مدى توفيق المشرع في وضع إستراتيجية لمواجهة تلك الجرائم في الجانبين الموضوعي و الإجرائي .**

و لعرض كافة الأفكار المتصلة بالموضوع يترتب علينا دراسة البحث وفق **خطة منهجية** التي قسمناها الى بابين رئيسيين حيث خصصنا الباب الأول لجرائم الإعتداء على النظام المعلوماتي سبب لإصدار التشريعات الخاصة بأمنه – دراسة تأصيلية– ، حيث نتطرق في الفصل الأول منه للطبيعة القانونية الخاصة لجرائم الإعتداء على النظام المعلوماتي ، و في الثاني للواقع القانوني لأمن النظام المعلوماتي من أخطار الإعتداءات الواقعة عليه .

أما الباب الثاني فنعالج فيه تحليل الإستراتيجية التشريعية لأمن النظام المعلوماتي من الإعتداءات الواقعة عليه حيث نتطرق في الفصل الأول منه للجوانب الموضوعية لمواجهة جرائم

الإعتداء على النظام المعلوماتي ، في حين خصصنا الثاني منه للجوانب الإجرائية لمواجهة جرائم الإعتداء على النظام المعلوماتي .

من الطبيعي أن يصاحب ثورة المعلوماتية وجه آخر يتمثل في ظهور نمط مستجد و مستحدث من الجرائم المرتبطة بالمعلومات و هو ما يسمى بجرائم المعلوماتية التي يكون النظام المعلوماتي بيئة لإرتكابها.

و لقد شكلت هذه الجرائم تحديات واضحة على الصعيد الدولي و الوطني بسبب الفراغ التشريعي الذي تعانيه جل دول العالم ، فالتشريعات العقابية القائمة وجدت لمواجهة الجرائم التقليدية و هو ما يصعب تطبيقها على الجرائم محل الدراسة، التي تتصف بخصائص تختلف عن تلك التقليدية من حيث آلية إرتكابها و الوسط الذي تتم فيه ، و نوعية مرتكبيها .

كما أن مبدأ الشرعية الجنائية المتمثل في أن "**لا جريمة و لا عقوبة أو تدبير أمن بغير قانون** " الذي يحد من القياس في المواد الجنائية ، بل يعد من القيود التي تواجه تطبيق النص فوق ما كان يقصده المشرع الجنائي من خلاله فلا يحق تجاوز نية و إرادة المشرع .

هذا الأمر الذي تنبهت إليه الدول بعدما زادت و إنتشرت نسبة إرتكاب جرائم المعلوماتية و من هنا جاءت الإتفاقيات الدولية و الإقليمية لمواجهتها و ما استتبعه من تشريعات داخلية في إطار تلك المواجهة سدا للثغرات القانونية و ضمانا للحماية منها .

فالنصوص التقليدية وقفت عاجزة امام الظاهرة الجديدة و من هنا جاءت إستقلالية التنظيم التشريعي لها بنصوص خاصة تعالج التصورات المختلفة لمحال الإعتداءات على المعلومات الإلكترونية المتواجدة في بيئة النظام المعلوماتي الذي يتميز بمواصفات خاصة و متميزة جعلت من الجرائم الواقعة عليه كذلك تتميز عن غيرها من الجرائم . لهذا كانت المعالجة التشريعية لها تنعكس على نصوص القانون الجنائي إلا أن المعالجة إختلفت من دولة إلى أخرى ، و عليه ستكون دراستنا في هذا الباب في فصلين حيث خصصنا الأول منه للطبيعة القانونية الخاصة لجرائم الإعتداء على النظام المعلوماتي أما الثاني فنتطرق فيه الواقع القانوني لمواجهة الإعتداءات الواقعة على النظام المعلوماتي .

لم تعمد الأنظمة التشريعية لتعريف الجريمة و هو مسلك راجع لسببين الأول يتعلق بالمبدأ الأساسي المبنية على سياسة التجريم والعقاب في كافة التشريعات و هو المتمثل في مبدأ شرعية أو قانونية الجرائم و الجزاءات ، الذي يقتضي من المشرع أن ينص إبتداء على ما يعد من الأفعال أو التصرفات التي تشكل جرائم ، موضحا في صورة ما العناصر الخاصة التي تميزها عن غيرها ، و التي تكون في مقياس لمعرفة ما هو مجرم و ما لايعد ذلك .

بينما السبب الثاني فمرجعه أنه ليس من حسن السياسة التجريمية أن يعتمد المشرع على تعريف عام للجريمة ، فقد تظهر مقتضيات الظروف عدم دقته أو قصوره ، الأمر الذي يكون حائلا دون تطور التشريع الجنائي ، بما يتلاءم مع تطور ظروف المجتمع و حاجاته و هي بطبيعتها متغيرة متزايدة ، لذلك نجد أن أغلبية التشريعات الجنائية تخلو من تعريف عام للجريمة .

أما في الفقه الجنائي فقد عرفها شراحه بتعريفات متعددة و مختلفة بحسب الزاوية التي يختارها صاحب التعريف ، و عموما تعد جريمة من المنظور الجنائي" **كل سلوك إيجابي أو سلبي ، له مظهر و أثر خارجي يجرمه القانون و يضع له جزاء جنائي.**"

و على إثر ذلك و نحن بصدد دراسة جرائم الإعتداء على النظام المعلوماتي خاصة في ظل عجز النصوص التقليدية عن مواكبة عصر التقنية و مستجداتها التي أثرت في أسلوب إرتكاب الجرائم أو في محل الإعتداء المتمثل في تلك المعلومات ذات الطبيعة الخاصة و المتميزة الأمر الذي أصبغ على تلك الجرائم طبيعة خاصة مستقلة و متفردة عن غيرها و هو محل دراستنا في هذا الفصل الذي قسمناه الى مبحثين بحيث ندرس في الأول منه لإستقلالية جرائم الإعتداء على النظام المعلوماتي بينما نتطرق في الثاني منه لإنعكاس إستقلالية جرائم الإعتداء على النظام المعلوماتي على النصوص التشريعية التقليدية

المبحث الأول : إستقلالية جرائم الإعتداء على النظام المعلوماتي

إن تطور تكنولوجيا المعلومات و ما صاحبه من تأثير إيجابي على المعلومات التي تحولت من طبيعتها التقليدية إلى الطبيعة المستحدثة و التي يطلق عليها إصطلاح المعلومات الإلكترونية و ما صاحبها من نقلة نوعية في طريقة التعامل معها و بها ، إلا أن الأمر إنعكس سلبا عليها بالتحديد حيث أصبحت عرضة بواسطة نفس التكنولوجيا للإعتداء عليها بصور و أشكال مختلفة و متعددة مما إستحدث نوعا جديدا من الجرائم و هي محل دراستنا في هذ المبحث الذي نخصصه لدراسة إستقلالية تلك الجرائم فهي متفردة بخصوصيات تجعلها تتميز عن غيرها و بالتالي سنركز في هذا المبحث لتوضيح مفهومها و هذا في مطلب أول بينما نخصص المطلب الثاني لخصوصية جرائم الإعتداء على النظام المعلوماتي.

المطلب الأول : مفهوم جرائم الإعتداء على النظام المعلوماتي

لتوضيح مفهوم هذه الجرائم سنتطرق لتحديد مدلولها و هذا في الفرع الأول من هذا المطلب بينما نخصص الفرع الثاني للنظام المعلوماتي (البيئة الإلكترونية للمعلومات) محل الأمن من الإعتداء عليه، أي تحديد أصالة النظام المعلوماتي محل الأمن.

الفرع الأول : مدلول جرائم الإعتداء على النظام المعلوماتي

أولا : جرائم المعلوماتية بصفة عامة

يعد ظهور جرائم المعلوماتية حديثا نسبيا ، وهو مرتبط بتاريخ ظهور الكمبيوتر ، ومن الوجهة التاريخية ، طرح أول كمبيوتر للشراء في الأسواق التجارية عام 1954 بالولايات المتحدة الأمريكية.[1] ولم تمض فترة طويلة على ذلك حتى سجل وقوع أول جريمة معلوماتية في نفس البلد

[1] - Céline Castets-Renard ,droit de l'internet: droit français et européen, Montcherstien lextenso édition, 2eme édition ;2012, p 445.

عام 1958.[1] ومنذ ذلك الحين زادت نسبة هذه الجرائم يوما بعد يوم ، وتنوعت أساليب ارتكابها ، وتعددت اتجاهاتها ، كما زاد حجم الخسائر الناجمة عنها وأخطارها حتى غدت اليوم واحدة من أكثر وأخطر الأنشطة الإجرامية انتشارا في العالم.[2]ففي عقد الستينات من العقد المنصرم توسعت دائرة هذه الجرائم ، فإلتفتت إليها وسائل الإعلام ، حيث بدأت الصحف لأول مرة تنشر المقالات بصددها ، ومن ثم زادت حدة هذه الجرائم في فترة السبعينات بحيث بدأت ملامح ظاهرة الاجرام المعلوماتي تلوح في الأفق ، وبدأت الابحاث المعتمدة على الأسس العلمية ببحث هذه الجرائم في منتصف هذه الفترة.[3] وقد كان الإضرار بأجهزة الكمبيوتر وتخريب شبكات الهاتف من الصور الشائعة لهذه الجرائم في تلك الفترة.[4] في حين أن فترة الثمانينات والتسعينات ، سجلت قفزة في حجم هذه الجرائم من حيث الكم والنوع ، بحيث تحدد مفهوم وماهية هذه الجرائم وتبلور مفهوم ظاهرة الإجرام المعلوماتي بصورة واضحة تماما.[5]

وذلك بعد أن زاد نطاقها بشكل هائل بفعل ظهور شبكة "الإنترنت" واستخدامها من قبل عدد هائل من المستخدمين ، مما أدى إلى ظهور أنماط وصور جديدة من هذه الجرائم ، ففي الثمانينات أظهرت دراسة قام بها معهد كولفيلد للتكنولوجيا في استراليا عام 1985 ، بأن ما تزيد عن 900 جريمة معلوماتية تقع سنويا في استراليا ، وفي اليابان كشفت الشرطة المركزية بالعاصمة

[1] – محمد حماد مرهج الهيتي ، الجريمة المعلوماتية نماذج من تطبيقاتها دراسة مقارنة في التشريع الإماراتي والسعودي و البحريني والقطري والعماني، دار الكتب القانونية، ودار شتات للنشر والبرمجيات، مصر– الإمارات، ب.ط، 2014، ص 48.

[2] – سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية،بيروت، لبنان، ط1، 2011، ص 13.

[3] – ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، مطابع الحميضي الرياض السعودية، ط1، 1430هـ– 2009م، ص 30.

4 – رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية بيروت لبنان، ط1، 2012، ص 35.

5 – نائل عبد الرحمان صالح ،واقع جرائم الحاسب في التشريع الأردني ، بحيث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة (2000) بحوث مؤتمر القانون والكمبيوتر والأنترنت ، المجلد الأول ، الطبعة الثالثة ، كلية الشريعة والقانون جامعة (الإمارات العربية المتحدة ، 2004 ، ص 191.

طوكيو عام 1988 عن وقوع 1136 جريمة معلوماتية في اليابان خلال تلك السنة ، وفي التسعينات سجلت الشرطة الألمانية وقوع 5004 جريمة معلوماتية في المانيا خلال عام 1991 .[1] أما الألفية الجديدة فإنها شهدت تزايدا لا مثيل لها في حجم هذه الجرائم ، فبحسب الإحصاءات التي قام بها مركز (IC3) لتلقي الشكاوى عن الجرائم المعلوماتية عبر الأنترنت ،وهو مركز مؤسس بشراكة ما بين كل من مكتب التحقيقات الفدرالي في الولايات المتحدة الأمريكية (FBI)، والمركز الأمريكي لمكافحة جرائم الياقات البيضاء (NW3C) ، لتكون بمثابة وسيلة لتلقي الشكاوى عبر شبكة الأنترنت عن الجرائم المعلوماتية في العالم ، حيث بلغ عدد الشكاوى التي تلقاها المركز في عام 2001 ما مجموعة (4971) شكوى فيما بلغ عددها عام 2009 ما مجموعه (336655) شكوى.[2]

وهذا يعني بأن نسبة هذه الجرائم في تزايد مستمر ، مع الأخذ بعين الإعتبار أن النسب المذكورة تمثل فقط عدد جرائم المعلوماتية التي تم إكتشافها والإبلاغ عنها للمركز المذكور وليس العدد الكلي لها في العالم ، حيث أنه بمقتضى دراسة للمركز الأمريكي للإستراتيجيات والدراسات العالمية فإن حجم هذه الجرائم في العالم يبلغ ما يقارب 10 مليارات جريمة سنويا.[3]

تعرف الجريمة عموما ، في نطاق القانون الجنائي (الذي يطلق عليه أيضا تسميات قانون الجزاء أو قانون العقوبات و لكل تسمية حججها وأسانيدها التي لا يتسع هنا المقام لعرضها [4]) ، بأنها "فعل غير مشروع صادر عن ارادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا " [5] وعلى

[1] – للمزيد من التفصيل ينظر : نائلة عادل فريد قورة ، جرائم الحاسب الآلي الإقتصادية ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت 2005 ، ص 80-85.

[2] – حنان ريحان مبارك المضحكي، المرجع السابق، ص 14.

[3] – أيمن عبد الله فكري ، جرائم نظم المعلومات ، دار الجامعة الجديدة ، الإسكندرية ، 2007 ، ص 103.

[4] – انظر : كامل السعيد – شرح الاحكام العامة في قانون العقوبات الاردني والقانون المقارن ، الطبعة الثانية – دار الفكر للنشر والتوزيع – عمان 1983.

[5] – محمود نجيب حسني – شرح قانون العقوبات ، القسم العام – الطبعة السادسة – دار النهضة العربية – القاهرة 1989 – ص 40.

الرغم من التباين الكبير في تعريفات الجريمة بين الفقهاء القانونيين وبينهم وبين علماء الاجتماع ، إلا أننا نختار هذا التعريف استنادا إلى أن التعريف الكامل – كما يرى الفقه – هو ما حدد عناصر الجريمة إلى جانب بيانه لأثرها ، فلهذه القاعدة أهمية كبيرة في تعريف الجريمة ، فبيان عناصر الجريمة (السلوك ، والسلوك غير المشروع وفق القانون ، الإرادة الجنائية ، وأثرها ، العقوبة أو التدبير الذي يفرض القانون) من شأنه في الحقيقة أن يعطي تعريفا دقيقا لوصف الجريمة ، ويميز بينها وبين الأفعال المستهجنة في نطاق الاخلاق أو الجرائم المدنية أو الجرائم التأديبية.

أما الجريمة المعلوماتية فقد تعددت تعريفاتها بتنوع التعبيرات التي استخدمت للدلالة عليها ، وهو تعدد رافق سيرة نماء وتطور تكنولوجيا المعلوماتية ، ويمكننا أن نعزو السبب الرئيسي لهذا التعدد في التعريفات إلى كون الإطار أو البيئة الخاضعة لهذه الظاهرة الإجرامية ، كانت و لا تزال في طور النماء والتطور ، حيث أن عامل التطور الزمني الذي واكب تكنولوجيا المعلومات و تكنولوجيا الإتصالات ، ساهم بشكل مباشر في تعدد الإصطلاحات والتعريفات التي استخدمت للدلالة والتعريف بهذه الظاهرة التي بدأت بالظهور مع بدايات ثورة تكنولوجيا المعلومات والتي نمت وتطورت بتطورها إلى أن وصلنا إلى مرحلة اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات.

ولقد بذل المهتمون بدراسة نمط الاجرام المصاحب لإنتشار وسائط تكنولوجيا المعلومات ، جهدا كبيرا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعة هذه الجريمة ، إلا أن كثيرا من المحاولات قد باءت بالفشل حتى قيل أن هذه الجريمة تقاوم التعريف[1] ، من منطلق التعذر لإيجاد تعريف جامع شامل لها ، حيث نجد أن الفقهاء والدارسون قد أعطوا لها عددا ليس بالقليل من التعريفات تتمايز وتتباين تبعا لموضوع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته ، فالإختلاف وقع بين الباحثين في الظاهرة الاجرامية الناشئة عن استخدام تكنولوجيا المعلومات من الزاوية الفنية و الباحثين في ذات الظاهرة من الزوايا القانونية ، وفي الطائفة الاخيرة تباينت التعريفات تبعا

[1] – أنظر هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة – 1992 – ص 29.

لموضوع الدراسة ذاته وتعددت حسب ما اذا كانت الدراسة متعلقة بالقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية.

كما أنه قد أبانت التجربة أن كثير من الدول يعاني المحققون فيها من مصاعب جمّة في التصدي لجرائم المعلوماتية بسبب عدم وضع تعريف محدد لهذه الجرائم وعدم تحديد الأفعال الإجرامية المشكلة لهذه الجرائم بشكل واضح.[1]

فجرائم المعلوماتية أو كما يسميها البعض بالجرائم الإلكترونية أو جرائم الكمبيوتر أو جرائم الأنترنت أو جرائم السيبر أو جرائم الغش المعلوماتي وغيرها من المصطلحات [2] ، بذل الفقهاء جهودا حثيثة ، في محاولتهم لوضع تعريف جامع ومانع لها ، لكن دون أن يثمر ذلك بالوصول إلى النتيجة المرجوة ، وذلك بالنظر لإختلافهم إلى عدة اتجاهات حول المعيار الواجب الاعتماد عليه في تعريف هذه الجرائم ، وبصورة عامة يمكننا أن نصف هذه الإتجاهات إلى فريقين و هي كالآتي :

أ– الفريق الذي يعتمد على معيار واحد

وهم متفقون على ضرورة الاعتماد على معيار واحد في تعريف الجرائم المعلوماتية ولكنهم منقسمون حول ماهية هذا المعيار إلى اربعة اتجاهات :

1 – الإتجاه الأول : ويرى أصحابه بضرورة الاعتماد على معيار **أداة أو وسيلة** التي يستخدم فيها الكمبيوتر كوسيلة لإرتكابها.[3]من أنصار هذا الاتجاه الفقيه الالماني تاديمان (Teidemann) الذي عرف هذه الجرائم بأنها : "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي

[1] – محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، الطبعة الاولى ، مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004 ، ص 87 و 88.

[2] – اخترنا مصطلح الجرائم المعلوماتية بإعتباره المصطلح الاكثر شمولا من غيره من المصطلحات لأغلب صور هذه الجرائم التي لا يمكن حصرها ، فمصطلحا الجرائم الإلكترونية وجرائم السيبر يشملان فقط الجرائم المعلوماتية الواقعة عبر شبكة الأنترنت ، فيما أن مصطلح جرائم الكمبيوتر والانترنت قاصر عن شمول الجرائم المعلوماتية التي تقع عبر أجهزة الهاتف النقال أو المحمول (الموبايل)فيما يقصر مصطلح جرائم الغش المعلوماتي عن شمول جرائم الإتلاف المعلوماتي والتجسس المعلوماتي وصور أخرى كثيرة لهذه الجرائم.

[3] – أيمن عبد الله فكري ، المرجع السابق ، ص 83.

يرتكب بإستخدام الحاسب" ، والفقيه الإنجليزي ليزلي بول (Leslie D.Ball) الذي عرفها بأنها : "فعل اجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية" ، وكذلك الفقيه فإن دير ميروي (Van der Merwe) والذي عرفها بأنها : الفعل غير المشروع الذي يكون الحاسب داخلا في ارتكابه".[1] وكذلك الفقيه الإنجليزي توم فورستر (Tom Forester) الذي عرفها هو الآخر بأنها : "فعل اجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية " ، وكذلك الحال بالنسبة للفقيهين الإنجليزيين ريتشارد توتي وأنثوني هاركاسل (Richard Totty & Anthony Hardcastle) الذي عرفها بأنها : "تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسب ، وبعبارة أخرى ، تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا".[2]

ولكن يؤخذ على هذا الاتجاه ، أن الاخذ به لوحده ، سيجعل التعريف قاصرا وشاملا فقط للجرائم المرتكبة بواسطة الكمبيوتر دون الجرائم الواقعة على الكمبيوتر هذا من جهة ، ومن جهة أخرى فإن المشرع عندما يجرم سلوكا ما فإنه لا ينظر إلى الوسيلة أو الاداة المستخدمة في ارتكاب الجريمة انما ينظر إلى مدى خطورة السلوك.[3]

2 – الاتجاه الثاني : ويدعو اصحابه إلى الاعتماد على معيار **موضوع أو محل الجريمة** في تعريف هذه الجرائم ، فهم يرون بأن الجريمة تكون معلوماتية فيما إذا كان محلها هو الكمبيوتر أو

[1] – هشام محمد فريد رستم ، الجرائم المعلوماتية – أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي ، بحيث مقدم لمؤتمر القانون والكمبيوتر والأنترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة في الفترة (1-3/مايو/2000) ، بحوث مؤتمر القانون والكمبيوتر والأنترنت ، المجلد الثاني ، كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة ، 2004 ، ص 405 و 406.

[2] – أيمن عبد الله فكري ، المرجع السابق ، ص 83 و 84.

[3] – محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الأنترنت (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، بيروت لبنان، ط1، 2011، ص 29.

النظام المعلوماتي.[1] ومن أنصار هذا الاتجاه الفقيه روزمبلات (Rosenblatt) الذي عرف هذه الجرائم بأنها : "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".[2] وفي ذات الاتجاه يعرفها كل من الفقيهين فيفانت ولي ستانس (Vivant & Le Stains) بأنها : "مجموعة الأفعال غير المشروعة المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب".[3]

ولكن يعاب على هذا الاتجاه بأنه يضيق من نطاق الجرائم المعلوماتية وبشكل يجعلها تتمحور فقط على الجرائم الواقعة على الكمبيوتر أو المعطيات من دون الجرائم التي تقع بواسطة الكمبيوتر كالإحتيال المعلوماتي مثلا.[4]

3 – الإتجاه الثالث : ويعتمد أصحابه على معيار **معرفة الجاني بالتقنية المعلوماتية** كمعيار لتعريف الجرائم المعلوماتية ، وبمقتضى هذا الاتجاه تكون الجريمة معلوماتية فيما اذا توافرت لدى مرتكبها المعرفة والدراية الفنية بتكنولوجيا المعلومات ، ومن الفقهاء الذين أخذوا بهذا الاتجاه الفقيه البلجيكي ستين سيشيولبيرج (Stein Schiollberg) الذي عرفها بأنها : "الجرائم التي يتطلب فيها الماما خاصا بتقنيات الحاسب ونظم المعلومات ، لإرتكابها او التحقيق فيها ومقاضاة فاعليها". والفقيه ديفد ثومبسون (David Thompson) الذي عرفها بأنها : "أيه جريمة يكون متطلبا لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".[5] وقد تبنى معهد ستانفورد في الولايات المتحدة الامريكية في احدى دراساته هذا الاتجاه ، حيث عرفت الدراسة هذه الجرائم ، بأنها "أية

[1] – محمود أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان 2005 ، ص 15.

[2] – بنظر : هشام محمد فريد رستم ، المرجع السابق ، ص 407.

[3] - Vavant et le stainc, Lamy in Droit de l'informatique PUF éd 1989, No 2323 p1540.

[4] – نائلة عادل فريد قورة ، المرجع السابق ، ص 30.

[5] – عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي ، دار الكتب القانونية ، مصر ، المحلة الكبرى 2007 ، ص 25.

جريمة لفاعلها معرفة فنية بتقنية الحاسب تمكنه من ارتكابها".[1] ومن ثم تبنت وزارة العدل الأمريكية التعريف السابق بمقتضى دليلها الصادر عام 1979.[2]

ولقد انتقد الفقه هذا الاتجاه من كون أن الاخذ به يؤدي إلى البحث في الظروف الخاصة بالجاني للوصول إلى حقيقة وجود مثل هذه المعرفة من عدمها ،وهذا مما لا يتناسب مع القانون الجنائي الذي هو قانون موضوع ولا يعتد بالظروف الشخصية إلا على سبيل الإستثناء.[3] كما انه يؤدي إلى افلات بعض الجناة من العقاب ، مثلا كمن يقوم بإتلاف بيانات داخل الكمبيوتر من دون أن تكون لديه أية معرفة فنية بتكنولوجيا المعلومات بالرغم من أن هذا الفعل مجرم ومعاقب عليه في بعض القوانين حتى ولو لم تتوفر لدى الجاني أية معرفة فنية من هذا القبيل.[4] كما يؤخذ على هذا الإتجاه أنه أغفل التطورات الحاصلة في مجال الأجهزة التقنية كالكمبيوتر والهواتف النقالة التي ادت إلى تسهيل استخدام هذه الاجهزة حتى من قبل من هو جاهل للتقنية الحديثة للمعلوماتية.[5]

ب – الفريق الثاني الذي يعتمد على أكثر من معيار

وهم متفقون على ضرورة الاعتماد على أكثر من معيار واحد لتعريف الجرائم المعلوماتية ولكنهم اختلفوا فيما بينهم حول كم ونوع هذه المعايير ، ويمكن تصنيف اهم تعاريف هذه المجموعة في أربعة إتجاهات رئيسية :

1 – الإتجاه الأول : وهم يعتمدون في تعريفهم للجرائم المعلوماتية في معيارين معا هما **وصف السلوك والإتصال بالمعالجة الآلية للمعلومات أو نقلها**. فقد أخذ بهذا الإتجاه خبراء من

[1] – محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، ط2 ، دار النهضة العربية ، القاهرة ، 2009 ، ص 35.

[2] – نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف ، الإسكندرية ، 2008 ، ص 50.

[3] – أيمن عبد الله فكري ، المرجع السابق ، ص 91.

[4] – نائلة عادل فريد قورة ، المرجع السابق ، ص 91.

[5] – نسرين عبد الحميد نبيه ، المرجع السابق ، ص 59 و 60.

منظمة التعاون والإقتصاد والتنمية في إطار تعريف قدموه للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة بعنوان (الإجرام المرتبط بتقنية المعلومات) حيث تبنَّو التصنيف الثاني بأنها : "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و / أو نقلها "[1] وقد تبنت منظمة التعاون الإقتصادي والتنمية (DECD) نفسها أيضا هذا التعريف مع بعض التعديلات الطفيفة ، حيث أنها عرفت هذه الجرائم بأنها : "أي سلوك غير قانوني أو غير أخلاقي أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يعتبر إعتداء على الكمبيوتر ".[2] وهو ما أخذ به أيضا القانون العربي النموذجي الموحد في شأن مكافحة سوء استخدام تكنولوجيا المعلومات والإتصالات ، حيث عرفت المادة الأولى منه هذه الجرائم ، بأنها : "كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني".[3]

ولكن يؤخذ على هذا الاتجاه ، أنه يوسع من نطاق الجرائم المعلوماتية بصورة مبالغ فيها لتشمل حتى السلوك غير الأخلاقي بالرغم من أن دائرة الأخلاق تخرج عن نطاق التجريم بمقتضى القانون الجنائي.[4]

2 – الإتجاه الثاني : ويرى أصحاب هذا الاتجاه بضرورة الإستناد على معيارين معا هما **موضوع أو محل الجريمة و وسيلة أو أداة ارتكاب الجريمة** ، وكلا المعيارين السابقين يمثلان في الحقيقة وجهان لعملة واحدة هي الكمبيوتر ، فالكمبيوتر هنا يلعب دور الضحية ودور الوسيلة بحسب نوع الفعل الجرمي المرتكب.[5] ومن الفقهاء الذين تبنوا هذا الاتجاه نذكر الفقيهين جاك بولوجنا وروبرت لاندكويست (Jack Bologna & Robert J.Lindquist) الذين عرفاها بأنها : "جريمة

[1] – المرجع نفسه ، ص 63.

[2] – طارق ابراهيم الدسوقي عطية ، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية) ، دار الجامعة الجديدة ، الإسكندرية 2009 ، ص 159.

[3] – عبد الفتاح بيومي حجازي ، التزوير في جرائم الكمبيوتر والأنترنت ، دار الكتاب القانونية ، مصر – المحلة الكبرى ، 2005 ، ص 21.

[4] - Bart de Schuter. La criminalité liée à l'informatique, Rev DPC No 1 Avril 1985.p.390.

[5] – نسرين عبد الحميد نبيه ، المرجع السابق ، ص 63.

يستخدم الحاسب كوسيلة أو أداة لإرتكابها أو يمثل اغراء بذلك أو جريمة يكون الحاسب نفسه ضحيتها".[1]

ولقد أخذت منظمة الامم المتحدة في مؤتمرها العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فيينا سنة 2000م بهذا الإتجاه ، حيث أنها عرفت الجريمة المعلوماتية بأنها :" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي ، والجريمة تلك تشمل من الناحية المبدئية ، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".[2]

وقد أيد جانب من الباحثين هذا التعريف بإعتباره شاملا لكافة صور الجرائم المعلوماتية.[3]

3 – الإتجاه الثالث : وهم يرون بوجوب الإعتماد في تعريف الجرائم المعلوماتية على معيارين هما **الوسيلة** و **الربح**. أي أن جرائم المعلوماتية هي تلك التي يستخدم الكمبيوتر في ارتكابها وتهدف إلى تحقيق مكسب مادي ، وبناء على ذلك فقد عرف الفقيه الفرنسي ماس (Masse) هذه الجرائم بأنها "اعتداء غير مشروع ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".[4] ولكن يؤخذ على هذا الاتجاه قصوره عن شمول جرائم المعلوماتية التي لا تهدف إلى تحقيق ربح مادي مثلا كالتشهير بالآخرين عبر الأنترنت [5] ، وجرائم التخريب المعلوماتي.

4 – الإتجاه الرابع : ويرى المنادون بهذا الاتجاه وجوب الاعتماد على معيارين لتعريف الجرائم المعلوماتية وهما **إما تحقيق الربح أو الحاق الضرر** أي أن الجرائم المعلوماتية هي تلك التي ترتكب بواسطة الكمبيوتر وتهدف إما إلى تحقيق الربح للجاني أو إلى الحاق الضرر بالضحية المعلوماتية ، وبناء على ذلك فقد عرف الفقيه الأمريكي دون باركر (Donn Parker) هذه الجرائم بأنها "أي

[1] – هشام محمد فريد رستم ، المرجع السابق ، ص 408.

[2] – أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي والأنترنت ، ط1 ، دار وائل للطباعة والنشر ، عمان ، 2001 ، ص 77 و 78.

[3] – نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط1 ، دار الثقافة ، عمان ، 2008 ، ص 50 .

[4] - Masse (M) : Le droit pénal spécial et Travaux de scies criminelles de peintres 1984 Edjais, P.23.

[5] – محمود أحمد عبابنة ، المرجع السابق ، ص 18.

فعل متعمد مرتبط بأي وجه بالحاسبات يتسبب في تكبد أو امكانية تكبد المجني عليه لخسارة أو حصول أو امكانية حصول مرتكبه على مكسب".[1]

ثانيا : الوصول لتعريف جرائم الإعتداء على النظام المعلوماتي

والآن بعد أن أوردنا التعريفات السابقة نرى بأنه من الضروري ان نحاول بدورنا وضع تعريف لجرائم الإعتداء على النظام المعلوماتي ، وفي هذا الاطار فإننا نرى بأنه عند وضع أي تعريف للجريمة عموما و لهذه الجرائم خصوصا فإنه ينبغي الاعتماد في ذلك على ما يمكن من خلاله تحديد أركان الجريمة أي أن يتضمن التعريف جميع اركان الجريمة التقليدية عموما و التي تعرّف بأنها : **"كل سلوك خارجي ايجابيا كان أو سلبيا جرّمه القانون وقرر له عقابا اذا صدر عن شخص مسؤول"**[2] و قياسا على ذلك ، ولما كانت جرائم الإعتداء على النظام المعلوماتي لا تختلف عن الجرائم التقليدية إلا من حيث أن محلها هو دوما المعلومات أو البيانات الإلكترونية التي قد تكون متعلقة بالمال أو بالحياة الخاصة أو بالمصالح العامة وغيرها [3]، و عليه نخلص إلى القول أن جرائم الإعتداء على النظام المعلوماتي هي تعبير شامل يشير إلى كل نشاط اجرامي مرتبط بإستخدام تقنية المعلومات الحديثة ، بحيث أن غياب الارتباط بها يمنع ارتكاب مثل هذا العمل غير المشروع ،و لا يختلف الأمر سواء كانت وسيلة تقنية المعلومات الحديثة أداة لإتمام النشاط الإجرامي أم كانت محلا له أو هدفا للإعتداء عليها .

لهذا يمكننا تعريف جرائم الإعتداء على النظام المعلوماتي بأنها : **كل سلوك متعمد يشكل اعتداء على المعلومات المتواجدة ضمن بيئة إلكترونية ، يجرمه المشرع ويقرر له عقابا اذا صدر عن شخص مسؤول جنائيا .**

[1] – ايمن عبد الله فكري ، المرجع السابق ، ص 90 .

[2] – علي حسين الخلف وسلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، مطابع الرسالة ، الكويت ، 1982 ، ص 134.

[3] – خالد ممدوح ابراهيم ، الجرائم المعلوماتية ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2009 ، ص 91-92.

ولو قمنا بتحليل تعريفنا هذا نلاحظ فيه ما يلي :

1- أنه من حيث الركن المادي للجريمة ، يشمل جميع صور السلوك الإيجابية (فعل) والسلبية (الإمتناع).

2- أنه من حيث الركن المعنوي للجريمة يتعلق بالسلوك الصادر عن الشخص المسؤول جنائيا الذي يتوفر لديه القصد الجنائي بشقيه (العلم والإرادة) أو الخطأ غير العمدي . وهذا الشخص يستوي أن يكون شخصا طبيعيا أو معنويا.

3- أنه من حيث الركن الشرعي يشمل جميع صور السلوك الذي يجرمه المشرع في الحاضر والمستقبل ويفرض له عقابا ، فمهما كان السلوك لا يعتبر جريمة ما لم يجرمه المشرع فيجب مراعات أن جرائم الإعتداء على النظام المعلوماتي هي محصورة في النموذج الأمني ذي الأبعاد الثلاثة (سرية المعلومات ، سلامة المعلومات ، وجود و وفرة المعلومات) فهذه الجرائم لها صور متعددة تختلف بإختلاف الهدف المباشر في الجريمة ، بحيث أنها تنطوي على أنماط عديدة من السلوك الإجرامي ، وبالتالي تقتصر على كل فعل عمدي يتوصل فيه الجاني بغير وجه حق إلى نظام معلوماتي يتم الدخول إليه وترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات...الخ من صور الجرائم المنصوص عليها وفق قانون العقوبات. [1]

4- أنه من حيث صور وقوع هذه الجرائم فهي تشمل جميع صور الإعتداء (الحالية والمستقبلية) على المعلومات أو البيانات ضمن بيئة إلكترونية. وبناء على ذلك نستبعد من نطاق هذه الجرائم جميع صور السلوك التي تتعلق بالمكونات المادية للكمبيوتر أو التي تتعلق بالمعلومات أو البيانات في صورتها المادية ، لأنها تخضع للنصوص التقليدية الخاصة بالجرائم التقليدية من دون أن تثير أية مشكلة.

[1] – المرجع نفسه ، ص 92

5- ومن ناحية أخرى يجب توضيح خصوصية هذه الجريمة بحيث يبدوا واضحا الدور الذي تقوم به وسيلة تقنية المعلومات الحديثة في ارتكاب الجريمة ، ولا يعني ذلك في تقديرنا أن يصل هذا الدور إلى الحد الذي لا يمكن أن تتم الجريمة بدونه بل يكفي أن تسهل ارتكاب الجريمة ، أي أن يكون لها دور في اتمامها على النحو الذي تمت فيه.

و بناءا على ما سبق نجد أن المشرع الجنائي الجزائري قد تبنى تعريفا لجرائم الإعتداء على النظام المعلوماتي و ذلك بموجب الفقرة أ من المادة الثانية من الفصل الأول المعنون بالأحكام العامة فيما تعلق بالمصطلحات من القانون رقم (04/09)[1] " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية ".

و هذا التعريف نجده موفق جدا في الإحاطة بجميع الحالات او الصور التي تقع في إطارها الجريمة المعلوماتية سواء المتعلقة بالإعتداء على المنظومة المعلوماتية في حد ذاته و ما يحتويه من معلومات او معطيات إلكترونية في حالة ما إذا كان هدفا أساسيا من إرتكابها هو الحصول على المعلومات أو تشويهها أو تخريبها او تعطيل المنظومة ككل ، بل الأكثر من ذلك نجد أن هذا التعريف جاء بنظرة إستشرافية للمستقبل بأن نص مسبقا على الجرائم التي من الممكن أن تقع بواسطة النظام المعلوماتي تسهيلا لجرائم في صورتها التقليدية حيث اعتبر النظام هنا وسيلة مساعدة في ارتكاب الجريمة ، و بالتالي عدم وضع هذه الجريمة المستحدثة في اطار ضيق يجعلها محصورة في مجال محدد ، مما يسمح بإفلات مرتكبي الجريمة المعلوماتية من دائرة التجريم و من ثم خروجهم من دائرة العقاب .

[1] القانون رقم (04/09) ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، المؤرخ في 05 غشت 2009، الجريدة رسمية ، العدد 47 ، ص (05)

الفرع الثاني : أصالة النظام المعلوماتي

المعلومات الإلكترونية تشمل جميع المعلومات التي تمت معالجتها من نصوص أو صور أو أصوات أو رموز أو برامج ، و مهما كانت حالتها سواء معلومات مدخلة (معطيات) ، معلومات معالجة ، مخزنة عن طريق وجود ما يصطلح عليه بنظام المعلوماتية أو نظام المعالجة الآلية للمعطيات الذي يسمح بنقلها و تداولها أو يجعلها في حالة سكون هذا النظام الذي يتكون من مكونات أساسية . لهذا فإن دراسة النظام المعلوماتي يشكل أساسية في بحثنا كي نفهم الطبيعة الخاصة للجريمة المعلوماتية بحيث يعتبر بيئة لتواجد المعلومات الإلكترونية فهو محل حماية من السلوكات الإجرامية و حمايته من حماية تلك المعلومات المتواجدة فيه بل انها تمثل أصل الحماية و الأمن من أي إعتداء قد تتعرض له .

أولا : تعريف النظام المعلوماتي

نظام المعلومات **Information System** هو عبارة عن آلية و إجراءات منظمة تسمح بتجميع و تصنيف ، و فرز المعطيات و معالجتها ، و من ثمّ تحويلها إلى معلومات يسترجعها و يستخدمها الإنسان عند حاجته لها ، ليتمكن من إنجاز عمل أو إتخاذ قرار أو القيام بأية وظيفة ، عن طريق المعرفة التي سيتحصل عليها من المعلومات المسترجعة من النظام .[1]

و لقد عرفه قانون الأنستيرال النموذجي بشأن التجارة الإلكترونية بأنه" النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو إستلامها أو تخزينها أو لتجهيزها على أي وجه آخر".

في حين عرفته الإتفاقية الدولية الخاصة بالإجرام المعلوماتي المبرمة ببودابست من خلال المادة الأولى في فقرتها –أ– منها بأنه" أي جهاز أو مجموعة الأجهزة المتصلة ببعضها البعض أو

[1] – رشيدة بوكر، المرجع السابق، ص 49.

التي ذات صلة بذلك ، و يقوم أحدها أو أكثر من واحد منها ، تبعا للبرنامج ، بعمل معالجة آلية للبيانات" مع العلم انها قد أطلقت عليه تسمية منظومة الكمبيوتر.[1]

في حين نجد أن المشرع الجزائري قد عرفه بموجب المادة الثانية في فقرتها –ب– من القانون رقم (04/09)بأنه "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

الملاحظ على التعريفات السابقة أنها لم تحدد العناصر المكونة للنظام و إكتفت بذكر عنصر عملية المعالجة الآلية بإعتبارها تنطوي على مراحل سابقة و لاحقة (الإدخال ، التخزين ، النقل ...الخ) و هذا ما نلمسه من خلال إستعمال التعريفات السابقة الذكر لمصطلحي (...المتصلة....) و (...المرتبطة...) الذين يفسران أن هناك مراحل و مكونات للمعالجة الآلية للمعطيات كونها مسألة تقنية و فنية قد يقوم بها جهاز واحد أو مجموعة متضافرة و متشابكة مع بعضها البعض و هو المقصود بالإتصال و الإرتباط هنا.

أما المشرع الفرنسي فلم يتطرق لتحديد مفهوم النظام تاركا ذلك للفقه و القضاء و مع ذلك نجد أن مجلس الشيوخ الفرنسي كان قد إقترح تعريفا له بمناسبة تعديل قانون العقوبات على أنه "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة و التي تتكون كل منها من الذاكرة و البرامج و المعطيات و أجهزة الإدخال و الإخراج و أجهزة الربط و التي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضعا للحماية الفنية".[2]

[1] – سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2010-2011، ص 85.

[2] – المرجع نفسه، ص 85.

الملاحظ على هذا التعريف أنه إكتفى بتحديد بعض العناصر على سبيل المثال لا الحصر المتراوحة بين عناصر مادية و أخرى معنوية ، المرتبطة بينها لتحقيق هدف المعالجة الآلية للمعطيات الرقمية كحد أدنى للنظام حتى كي يكون محلا للحماية الجزائية ، كما أنه لم يحدد وسائل تحقيق المعالجة التي على رأسها الحاسوب مكتفيا بالإشارة أن تلك الوحدة أو الوحدات تؤدي في النهاية لتحقيق نتيجة معالجة المعطيات عن طريق مجموعة العلاقات رابطة بينها ، مما يفهم منه أن توافر هذه المكونات في أي جهاز أو آلة تقوم بالمعالجة الآلية ينطبق عليها مفهوم نظام المعالجة الآلية . [1]

و بتحليل ما سبق نجد أن النظام المعلوماتي مجموعة مكونة من حاسوب و عناصر أخرى مختلفة مرتبطة أو متصلة به و يشمل ذلك المعدات و البرمجيات، فتعريفه موجه ليشمل كل جهاز معزول أو مجموعة التجهيزات "المرتبطة عبر الشبكة" أو المتقاربة التي تضم عنصر أو مجموعة من العناصر و التي تضمن ، عن طريق تنفيذ برنامج المعالجة الآلية للبيانات ، كما أنه يشمل القيام بتسجيل المعطيات أو بوضعها في ذاكرة الحاسوب ، و كذا الإجراءات المتعلقة بتسجيل البيانات أو بوضعها في ذاكرة الحاسوب .

و عليه نخلص أن هذا النظام هو **مجموعة من العناصر المتداخلة و المتفاعلة مع بعضها و التي تعمل على جمع المعطيات و معالجتها لتشكل لنا المعلومات الإلكترونية و من ثمّ تخزينها و بثّها و توزيعها ، بغرض صناعة أو أخذ القرارات و تنسيقها ، إضافة إلى تحليل المشكلات و النظر في الموضوعات المعقدة** ، و عمله يمر وفق المراحل التالية:

- تأمين المدخلات المطلوبة من البيانات التي توضع في الحاسوب بوسائل خاصة .
- معالجة البيانات المدخلة و تحويلها من شكلها الأولي إلى نتائج مفهومة و قابلة للإستخدام تكون في شكل مخرجات أو معطيات

[1] - خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، رسالة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012، ص، 33- 37.

- تأمين المخرجات من المعلومات المطلوبة لمستخدميها أو لمن يحتاجها ، وهنا لابد أن تنقل تلك المعلومات من وحدة المعالجة المركزية إلى وسيلة إخراج مناسبة كشاشة الحاسوب ، أو الطابعة ...الخ
- التغذية الراجعة كون المعلومات المخرجة لنشاط محدد قد تكون بدورها مدخلات ثانية بغرض إعادة معالجتها مع بيانات أخرى من داخل ذاكرة الحاسوب ، و لأغراض و مخرجات أخرى.

و من هنا وجدنا أنه من الضروري التطرق لمكونات هذا النظام كي يتبين لنا مفهوم هذا النظام و عمله بصورة أكثر دقة .

ثانيا : مكونات النظام المعلوماتي

هو نظام يعتمد على الأفراد الذين يطلق عليهم العنصر البشري و الحاسب الآلي الذي يشمل على المكونات المادية أو مجموعة الأجهزة Hardware، و المكونات المنطقية أو البرمجية (التعليمات أو الأوامر) Software للحاسوب في معالجة المعطيات و إخراج المعلومات من خلال النشاط الذي يقوم به ، هذا بالإضافة إلى شبكة المعلومات ، و سنستعرضها وفق ما يلي:

أ – العنصر البشري

الذي يلعب دورا ضروريا و هاما في هذا النظام للقيام بالعمليات و الإجراءات فبدونه لا يستطيع النظام المعلوماتي العمل في جميع مراحله المختلفة فهو حلقة أساسية في مكونان النظام المعلوماتي ، و من مكونات العنصر البشري نجد المستخدمين النهائيين و الإختصاصيين الفنيين المسؤولين عن تشغيل و إدارة نظم المعلومات فنيا و منهم محللو النظم و مطورو البرمجيات و مشغلو النظام و مهندسو الصيانة و الإتصالات ....الخ.[1]

[1] – سليم الجبوري، المرجع السابق، ص 50.

ب – الحاسب الآلي

يعرّف الحاسب الآلي بأنه "عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها و توجيهها بإستخدام أوامر خاصة لمعالجة و إدارة المعلومات بطريقة ما ، و ذلك بتنفيذ ثلاثة عمليات أساسية هي : إستقبال المعطيات المدخلة إليه (الحصول على الحقائق المجردة) ، و معالجة المعطيات إلى معلومات (إجراء الحسابات و المقارنات و معالجة المدخلات) ، و إظهار المعلومات المخرجة (الحصول على النتائج)".[1]

و يمتاز الحاسوب بعدة خصائص و مميزات جعلت منه أداة رئيسية في حياتنا المعاصرة نوجزها وفق الآتي ذكره :

- السرعة في معالجة المعطيات و أداء الوظائف و القيام بالعمليات الحسابية فالحاسوب يقوم بوظائفه بسرعة مذهلة مقارنة بالبشر ، وهي ميزة وفرت على الإنسان الكثير من الوقت .[2]
- تخزين المعلومات و إستعادتها فالحاسوب يتمتع بقابليته لتخزين كمية كبيرة جدا من المعلومات و البيانات التي يمكن إستعادتها و الرجوع إليها للإستفادة منها في أي وقت يحتاج إليها الإنسان و تبقى هذه المعلومات مخزنة لفترة طويلة جدا دون أن يحدث لها أي تغيير .
- دقته في إستخراج النتائج من المعطيات المقدمة إليه لتكوين المعلومات النهائية .
- قابليته للبرمجة فتصميمه مبني على إمكانية أدائه لوظائف لا حدود لها و ذلك عن طريق البرامج التي يمكن تطويرها من أجل تحسين الأداء الوظيفي للحاسوب .
- إمكانية التعامل عن بعد و من أي مكان في العالم عن طريق وسائل الإتصال السلكية و

[1] – نعيم مغبغب، حماية برامج الكمبيوتر دراسة مقارنة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت لبنان، ب.ط، 2009، ص 32.

[2] – أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، د.ط، 2007، ص 134.

اللاسلكية و هذا بما يعرف بشبكة المعلوماتية .[1]

و للحاسوب مكونان رئيسيين هما :

1- المكونات المادية للحاسوب :

و هي الهيكل المادي للحاسوب أو الجسم المادي له و هو بدوره يتكون من وحدات تتمثل في وحدات الإدخال (In Put Units) التي تستعمل لإدخال البرامج أو المعطيات المراد معالجتها من الوسط الموجودة عليه إلى ذاكرة الحاسوب و هي مجموعة من الوسائل تتمثل في:

وسائل تسمح بالإتصال المباشر ON-LINE بين الوسط الخارجي (الإنسان) و بين وحدة المعالجة المركزية ، و من بين هذه الوسائل نجد لوحة المفاتيح ، ملتقطات الصوت و الصورة ،...الخ وكل وسيلة تقوم بإدخال معطيات مباشرة إلى وحدة المعالجة المركزية بالإضافة لوسائل تسمح بإدخال المعطيات بصورة غير مباشرة OFF-LINE ، بحيث يتم بواسطتها تهيئة البيانات المراد إدخالها ، و تشمل الفأرة و مشغلات الأقراص و الماسح ...الخ .[2]

كما نجد من بين المكونات المادية للحاسوب وحدة المعالجة المركزية (Central Processing Unit) و التي تعتبر العقل المفكر و المسيطر على عمل باقي الوحدات المكونة لجهاز الحاسوب بحيث تقوم بمعالجة المعطيات حسب التعليمات الواردة في البرنامج و فيها يتم جميع العمليات الحسابية أو المنطقية وهي تشتمل على وحدة التحكم و السيطرة (Control Unit) و هي عبارة عن دوائر إلكترونية تتحكم في عمليات تنفيذ التعليمات وفي عملية الإدخال و الإخراج و التخزين و المعالجة داخل الحاسوب بحيث تقوم بوظائف متعددة منها التنسيق و التحكم في البيانات الداخلة و المعلومات الخارجة من الذاكرة الرئيسية للحاسوب بتوجيهها إلى القنوات

[1] - نفس المرجع السابق، ص 134.

[2] - خليفي مريم، المرجع السابق ، ص، 22-23.

المختلفة ، وكذا قراءة و تفسير تعليمات البرامج ، إضافة إلى التحكم في توقيت العمليات المختلفة بفضل الساعة المنطقية.[1]

هذا بالإضافة لوحدة الحساب و المنطق (Arithmetic Logic Unit) و التي تقوم بجميع العمليات الحسابية و المنطقية ، مثل المقارنات التي تسمح للحاسوب بتقييم المواقف لتحويلها إلى الذاكرة و إخراجها حسب الطلب إلى وسط مناسب للمستخدم.

كما نجد وحدة الذاكرة و هي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو تخزين النتائج الآتية من وحدة المعالجة المركزية[2] و هي نوعان: وحدة الذاكرة الرئيسية التي تستخدم لتخزين المعطيات و البرامج التي يراد تنفيذها تكون سرعتها متفاوتة من جهاز لآخر كما يمكن تغييرها للجهاز الواحد بأخرى أقدر على الإستيعاب الأكثر للمعلومات و أسرع و هي قسمان الأول منها يسمى ذاكرة القراءة فقط المعروفة إختصارا بـ (Rom) محتوياتها تتكون من أوامر مخزنة في الجهاز من قبل الشركة المصنعة له ، ولا يمكن للمستخدم تعديلها ، بحيث تختص بالإحتفاظ بالبيانات و الأوامر المخزنة ، والتي تستخدم لقراءتها فقط ، و لا تقبل التخزين بعد التصنيع إلا بمعرفة جهة التصنيع أو المتخصصين بإستخدام أجهزة متخصصة ، أما القسم الثاني فيسمى الذاكرة العشوائية أو ذاكرة التوصيل العشوائي المعروفة إختصارا بـ (RAM) و تخزن فيها البيانات بصورة مؤقتة إستعدادا لمعالجتها أو لتخزينها في وسائط التخزين الدائمة كما تحتفظ بجميع الملفات الرئيسية للبرامج عند البدء بتشغيلها لذى كي يكون الجهاز ذو فعالية لابد أن تكون عالية السعة أو الحجم .[3]

[1] – نفس المرجع السابق، ص 23.

[2] – محمد مرسي الزهرة، الحاسي الإلكتروني والقانون، دار النهضة العربية، القاهرة، 2008، ص 20.

[3] – محمد عبد الظاهر حسين، الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، دار النهضة العربية، القاهرة، 2000، ص 12.

و وحدة الذاكرة المساعدة ، و هي الوحدة الثانوية لتخزين المعلومات و البرامج و التي تكون أقل ثمنا من الوحدة الرئيسية و أقل سعة منها إلا أنها تخزن المعلومات لفترة أطول تصل لأعوام وهي متمثلة في الأقراص المرنة و الصلبة و الأشرطة الممغنطة و القرص الضوئي و القرص الرقمي .

و من بين المكونات المادية للحاسوب نجد كذلك وحدات الإخراج و مهمتها إيصال المعلومة من الحاسوب إلى الوسط الخارجي ، و هي عكس وحدات الإدخال التي تؤدي دور إتصال الوسط الخارجي بالحاسوب ، فوحدات الإخراج تقوم بنقل النتائج المستخرجة من وحدات المعالجة المركزية إلى الخارج ، و أهم وحدات الإخراج نجد الشاشة (Screen) التي من خلالها يتمكن المستخدم من مشاهدة نتائج ما قام به من أعمال سواءا تلك المتعلقة بالأوامر أو النصوص المدخلة ، أو تلك المتعلقة بمشاهدة نتائج المعطيات بعد معالجتها داخل الجهاز .[1]

و من بين وحدات الإخراج نجد كذلك الطابعة (Printer) فهي من بين أهم الوحدات و الأكثر إستعمالا كونها تزود المستخدم بنسخ من المطبوعات للمعلومات و النتائج المخزنة داخل الحاسوب .[2]

2- المكونات المنطقية للحاسوب

تتمثل هذه المكونات في التطبيقات العملية التي تجري داخل الكيان المادي للحاسوب ، و التي تشمل المعطيات و المعلومات و البرمجيات ، هذه الأخيرة التي لها دورا مهما في معالجة البيانات المدخلة للجهاز و إستخراج النتائج المطلوبة التي تكون في صورة معلومات و ذلك عن طريق مجموعة الأوامر و التعليمات التي تحدد لجهاز الحاسوب طريقة عمله وفق خطوات محددة و متسلسلة.

1 – علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، 1997، ص 05.

2 – محمد عبد الظاهر حسين، المرجع السابق، ص 13.

و البرمجيات نوعان بحيث نجد برمجيات النظم التي تقوم بوظيفة إجرائية تسيطر من خلالها على الأداء الآلي للحاسوب ، و منها ماهو متواجد داخل الحاسوب و بعضها مخزن على الأقراص الممغنطة تشترى بشكل منفصل عن الحاسوب (مثالها لغات البرمجة و المترجمات و نظم التشغيل) ، أمّا النوع الثاني يتمثل في البرمجيات التطبيقية و هي برامج مصممة لتؤدي وظائف محددة تستجيب لإحتياجات العمل و متطلباته و بالتالي لا يمكن حصرها فمن أملثلتها البرامج المستخدمة في البنوك و المؤسسات المالية لتأدية وظائف معينة كمسك حسابات العملاء أو الربط بين البنوك .[1]

ج – المعلومات الإلكترونية

المعلومات لغة جمع معلومة و هي مشتقة من كلمة "علم" و دلالتها تتمحور بوجه عام حول المعرفة التي يمكن نقلها و إكتسابها ، علمت الشيء أعلمه أي عرفته ، و أعلم فلان الخبر أي أخبره به ، و أعلم فلان الأمر حاصلا أي جعله يعلمه ، و العلم نقيض للجهل ، و يقارب معنى المعلومة في اللغة الفرنسية مصطلح Information الدالة على عملية الإتصال التي تستهدف نقل و توصيل إشارة أو رسالة أو الإعلام عنها و إتخاذ وظيفتها في نقل المعارف Transfert de Connaissances، أما في اللغة الإنجليزية فنجد مصطلح Informatio اللاتينية الأصل و ترجمتها للعربية تدل على شيء قابل للإبلاغ و التوضيح أو على عملية الإبلاغ أو النقل و التوصيل للفكرة إلى الغير .[2]

أمّا إصطلاحا فقد تعددت التعاريف للمعلومات من طرف باحثين من تخصصات و ثقافات مختلفة حتى يكاد يستحيل إدراك المعنى المراد منها و في هذا يرى البعض أنها كالجاذبية و الكهرباء لا نستطيع وصفها بدقة ، و لكننا نعرف كيفية عملها . و ما يهمنا هنا هي التعريفات

[1] – زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 91.

[2] - سوير سفيان، المرجع السابق، ص 09.

الدائرة حول المعلومة المتخذة لشكل يجعلها قابلة للتوصيل إلى الغير بإعتبارها محل التأمين من الإعتداء عليها ، و التي نذكر بعضا منها وفق ما يلي :

فهي "الحقائق أو الرسائل أو الإشارات أو المفاهيم التي تعرض بطريقة صالحة للإبلاغ أو التوصيل Communication أو التفسير L'interprétation بواسطة إنسان أو أدوات أو معدات آلية".

أو هي "تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير بفضل علامة أو إشارة من شأنها أن توصّل المعلومة للغير" ، أو هي "صور الوثائق و البيانات أو الرسائل من أي نوع" .[1] و هي "الرسائل المعبّر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير" ، كما أنها "وسيلة للمعرفة قابلة لكي تحفظ أو تبلغ بواسطة الإصطلاحات" .

أمّا المعلومات الإلكترونية هي مصطلح مركب ناتج عن عملية الدمج و التزاوج بين الآلية و المعلومات بصفة عامة و التي أفرزت مفهوما جديدا لها الذي قام على تبادل مختلف أنماط المعلومات المعالجة آليا وفق ما يعرف بالمعلوماتية التي بدورها مكوّنة من مقطعين "مقطع أول المعلومات أمّا المقطع الثاني لآخر حرفين من مصطلح آلية"، و التي تعرف بأنها "المعلومات المعالجة بطريقة منطقية أو عقلية التي تعتبر بمثابة دعامة للمعارف الإنسانية والإتصالات في المجالات الفنية والإقتصادية والإجتماعية و ذلك بإستخدام معدّات آلية".[2]

كما ورد تعريف للمعلومات في الموسوعة العربية لمصطلحات علوم المكتبات بأنها "البيانات التي تمّت معالجتها لتحقيق هدف معين أو لإستعمال محدد لأغراض إتخاذ القرارات" بمعنى البيانات التي أصبحت لها قيمة بعد تحليلها أو تفسيرها أو تجميعها في شكل ذي معنى" .

[1] – نفس المرجع السابق، ص 10-11.

2 – أمال قارة، المرجع السابق، ص 102.

وعليه تتعدد التعاريف للمعلومات و لا يوجد تعريف مانع جامع شامل لحدّ الساعة إلا أننا نخلص بوجه عام إلى التعريف التالي :

"المعلومات هي الصورة المحمولة للبيانات المنظمة و المعالجة بطريقة تسمح بإستخلاص نتائج نهائية".

ولكي يتم إيضاح مفهومها بصورة أكثر دقة وجب التمييز بينها و بين بعض المصطلحات التي تتشابك معها ، فالمعطيات في اللغة تقابل "البيانات" وهي في اللغة من مشتقات كلمة "بين" من معانيها ما تبين به الشيء من الدلالة و غيرها ، و يقابل هذا في اللغة اللاتينية كلمة (datum) و تعني شيء معطى و مسلم به بصحته كحقيقة أو واقعة ، وجمعها (data) التي تستخدم في اللغة الإنجليزية أما في اللغة الفرنسية فيستخدم مقابلا لها كلمة (données) أما إصطلاحا فالتعاريف الموجهة لها تتعدد و منها نذكر : "تعبير عن مجموعة من الأرقام و الكلمات و الرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض" و لقد عرفتها الوكالة الفرنسية للتقييس (Afnor) بأنها "كل حادث مفهوم أو تعليمة تقدم في شكل متفق عليه ، قابلة للتبادل عن طريق البشر أو بوسائل أوتوماتيكية "كما عرفها البعض بأنها "جميع الحقائق و الأرقام و الرموز التي تشير أو تصف موضوعا ما أو فكرة معينة ، أو موقفا أو شرطا ، أو أي عامل آخر ، وتعني أيضا العنصر الأساسي للمعلومات التي تعالج بواسطة الحاسوب أو ينتجها الحاسوب و هي "مجموعة من الحقائق أو القياسات أو المعطيات التي تأخذ صورة أو أرقاما أو حروفا أو رموزا أو أشكالا خاصة و تصف فكرة أو موضوعا أو حدثا أو هدفا معينا و يتم تحويلها كمواد خام لغرض إستخراج معلومات معينة" .[1]

[1] – ميريام كومينر ، الإجرام البشري الإلكتروني ، جوانب استراتيجية وقانونية، مجلة الثقافة العالمية للمجلس الوطني للثقافة والفنون والآداب، الكويت ، العدد158 ، 2010، ص 64-65.

و في نفس الإتجاه عرّفت إتفاقية بودابست المعلومات في مادتها الأولى في فقرتها (ب) بأنها "كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل و تكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة و يجعل الحاسب يؤدي المهمة " كما أن المشرع الجزائري عرّفها وفق المادة 2 الفقرة الثالثة منها للقانون رقم (04/09) بأنها "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

و مما سبق يتبين لنا أن المعلومات هي المعنى المستخلص من تلك المعطيات ، و عليه فالمعطيات هي المعلومات في حالة كمون و المعلومات هي معطيات في حالة تبلور فهي كل نتيجة مبدئية أو نهائية مترتبة على تشغيل المعطيات أو تحليلها أو إستقرائها أو إستنتاج للدلالات الممكن إستنتاجها منها وحدها أو متداخلة مع غيرها أو تفسيرها على نحو يثري معرفة متخذي القرار و مساعدتهم على الحكم السديد على الظواهر المشاهدة أو يسهم في تطوير المعارف النظرية أو التطبيقية . أي أن المعلومات ترجمة للمعطيات الموجودة في الحاسب الآلي عند تشغيله و المعالجة بطريقة تسمح بتكوين محتوى معرفي يمكّن ذوي الشأن لإستخلاص نتائج معينة ، فهي تمثل في صورة مبسطة لها مجموعة المعطيات المعالجة آليا على جهاز الحاسب الآلي.[1]

وممّا لا شك فيه أنهما يتفقان في أن كلاّ منهما يحتوي في مضمونه فكرة معينة أو معرفة لكن ما يميزهما عن بعضهما الصورة المتواجدان عليهما في الواقع ، فالمعطيات تأخذ شكل أرقام و رموز و كلمات ...الخ وعن طريق المعالجة الآلية تتحول إلى نتائج تقرأ توصل لنا المعلومات المستنتجة منها تختلف عن الصورة الأولى المدخلة إلى الحاسب الآلي قبل المعالجة الآلية لها . [2]

[1] – محمد مرسي الزهر، المرجع السابق، ص 35.

[2] – محمد عبد الظاهر حسن، المرجع السابق، ص 14.

و من هنا يمكن التمييز بينهما من الناحية الفنية أو التقنية : فالمعطيات Data (données) هي المدخلات In Put إلى جهاز الحاسب الآلي بهدف تشغيلها Processing و معالجتها داخل الجهاز للحصول على المخرجات Out Put في صورة معلومات نهائية Information و عليه فالمعلومات المقصودة هنا في دراستنا هي المعطيات ذات الطبيعة الشكلية Formelالمدخلة إلى الحاسب الآلي بقصد معالجتها آليا لتأخذ صورتها النهائية بعد عملية معالجتها لتكوّن معلومات ذات طبيعة فكرية ذهنية ، و منه فالمعلومات هي المعطيات المعالجة آليا عبر أو بواسطة الحاسب الآلي.[1]

في حين نجد ان البرنامج هو مجموعة من التعليمات المعبّر عنها بشكل لفظي ، مرمّز بياني أو أي شكل آخر بحيث إذا أدرجت في جهاز للقراءة الآلية يمكنها أن تجعل الحاسوب أو أي جهاز إلكتروني آخر مشابه له بإمكانه إعداد معلومات ينفّذ مهمّة محددة أو يتحصل على نتيجة معينة .

والبرامج تعتبر مجموعة من التعليمات و الأوامر الصادرة من الإنسان إلى الآلة أو ما يعرف بالكيان المادي للحاسب ممّا يسمح لها بأداء مهمّة معينة و محدّدة ، فهو يتضمن كل المعطيات و المستندات الأخرى الملحقة به و المساعدة على تبسيط فهمه و تيسير تطبيقه لغاية محدّدة من حيث الوظيفة المقدمة من خلاله المتمثلة في القيام بمختلف العمليات التي يحتويها الحاسب و نظامه و من هنا فالحاسب الآلي لا يعمل دون وجود البرامج التي تعطي الأوامر للقيام بمختلف عملياته.

[1] – خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى، الجزائر، ط 2010، ص 17.

فبرامج المعلوماتية هي وسيلة إلكترونية تسمح بالقيام بعمل أو بالإجابة جزئيا أو كليا على رسائل المعطيات أو على عمليات دون أن يقوم شخص طبيعي بعملية الفحص أو بالتدخل في كل مرة ينفّذ فيها عمل أو تتم فيها الإجابة على رسالة المعطيات .[1]

لهذا فإدخال المعطيات إلى الحاسب الآلي و معالجتها يحتاج و يتطلب و جود البرامج التي تحولها إلى معلومات معالجة آليا و بدونها لن نحصل عليها فلا غنى للمعطيات المعالجة آليا عن البرامج المحولة لها من صورتها المبدئية الشكلية إلى الصورة النهائية الفكرية الذهنية.[2]

هذا و لم يتطرق المشرع الجزائري على غرار التشريعات المقارنة لتحديد مفهوم البرنامج إلا أننا نجده قد أورده محل حماية و هذا بموجب الأمر 05/03 المتعلق بحقوق المؤلف و الحقوق المجاورة و هذا من خلال المادة 04 الفقرة أ منها التي إعتبرت برامج الحاسوب من المصنفات الأدبية أو الفنية محل الحماية كما أستعمل نفس المصطلح في المواد 52 ، 53 ، 153 ، في حين أن المادة 05 الفقرة الثانية منها التي إعتبرت بعض الأعمال من قبيل المصنفات و التي تستدعي الحماية ذكرت "و قواعد البيانات سواء كانت مستنسخة على دعامة قابلة للإستغلال بواسطة آلة ..." فتعبير قواعد البيانات يقصد بها هنا برامج الحاسوب ، و من هنا نجد أن المشرع لم يتجه لإعطاء تعريف البرنامج و إكتفى بذكره تفاديا للتطورات التكنولوجية و الثورة العلمية في ميدان البرمجيات و تعقدها .

و بما أن البرامج هي في الأصل عبارة عن معلومات ممثلة في تعليمات و عبارات و التي عند تنفيذها داخل نظام المعالجة الآلية تؤدي إلى إنجاز وظيفة و بالتالي فإنها تدخل في إطار المعلومات من الناحية التقنية و القانونية ، و من ثم فإن العلاقة بينهما هي علاقة الجزء بالكل و بالتالي خضوعهما لنفس النظام القانوني و ما يدعم هذا الرأي هو تعريف المشرع الوطني

[1] – خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي ، دار الجامعة الجديدة، الإسكندرية، 2005، ص 17.

[2] – محمود حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، 1957، ص 06.

للمعطيات في المادة 02 الفقرة الثالثة منها الواردة في القانون (04/09) بقوله "...بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة المعلوماتية تؤدي وظيفتها" فالملاحظ هنا أن المشرع حسم موقفه حول الجدل الحاصل بين المعطيات و البرامج و ذلك لما أدرج البرامج ضمن مفهوم المعطيات بكل أنواعها.

1- الشروط الخاصة بالمعلومات الإلكترونية :

كون المعلومات الإلكترونية لها قيمة بوصفها نتاج نشاط إنساني ، فهذا يجعلنا نحدد شروطها كي تكون محل الحماية ضمانا لحقوق أصحابها و هذه الشروط نوجزها في العنصرين التاليين :

خاصية الوجود للمعلومة من حيث التحديد والإبتكار (Precise et Inventive):

كي نقول عن المعلومات الإلكترونية أنها موجودة يجب أن تكون محددة ، فالمعلومات لابد أن تأخذ شكلا معينا داخل النظام المعلوماتي ، و هذا الشكل هو المحدد لها ، و التحديد هنا يفرض نفسه ، و بإنعدامه تزول القيمة الحقيقية للمعلومات ، وفي هذا قال الأستاذ كاتالا(Gatala) "أن المعلومة قبل كل شيء تعبير و صياغة مخصصة من أجل تبليغ رسالة ، و يكون هذا التبليغ عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير" ،و من هنا و بإعتبار المعلومة فكرة للتبليغ فهذا يفترض فيها أن تكون محددة (**Precise**) ، ذلك أن التحديد بدوره يعتبر أمرا مطلوبا في مجال الحماية القانونية لأنه يحصر المعلومة في دائرة خاصة .[1]

ومن جانب آخر يجب أن تكون المعلومات مبتكرة (**Inventive**) ومعناه أن تكون المعلومة غير شائعة من قبل يسهل الوصول إليها من الكافة و بدونها لا تعد معلومة بالمعنى الفني الدقيق و تبعا لذلك فإن إستخدامها دون تدخل مصدرها يمثل إنتهاكا للحق في المعلومات و

[1] – أحمد الخليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص 75.

حالتها التقنية هي التي وضعها في متناول الناس المستفدين منها لكن هذا لا ينفي الحقوق الناشئة عنها .

– الجدة(Nouveauté) و الإستئثار(Exclusivité) :

الجدة هنا يقصد بها أن لا يكون قد سبق و أن وضع ذات المعلومة و التعريف بها ، ذلك أن المعلومة يجب أن تعبر عن شخصية من أوجدها و إبتدعها ، و إن لم يتحقق هذا تكون مجرد أفكار لا تستوجب الحماية ، و مما يجب ذكره أن الجدة يطلق عليها البعض مصطلح السرية (La Confidentialité) .[1]

و على كل بالنسبة للمصطلحين فالمقصود منهما واحد ، و هذا يمثل شرط لازم لحصر حركة المعلومات في دائرة محددة من الأشخاص ، فلا يمكن تصور الحماية لها بدون وجود هذا الشرط لأن المعلومات غير المحاطة به هي قابلة للتداول و من ثم بمنأى عن أي حيازة كالمعلومات المتعلقة بدرجة الحرارة في لحظة معينة أو الزلزال أو الفيضان الذي يضرب منطقة معينة فهي معلومات قابلة للنقل بسهولة بين كل الأشخاص و بسبب حرية تداولها المتعارضة مع الجدة أو السرية لا يمكن إعتبارها من قبيل المعلومات محل الحماية القانونية ،[2] ففي الواقع المعلومات تكتسب وصفها إما بالنظر لطبيعتها كإكتشاف شيء جديد كان مجهولا من قبل أو بالنظر إلى إرادة الشخص كإكتشاف مجال حديت لتسير الإدارة بواسطة رئيس شركة ما و إرادته بالإحتفاظ بسريته أو بالنظر إلى الأمرين معا كما هو الحال بالنسبة للرقم السري لبطاقة الإئتمان .

أما الإستئثار فيقصد به أن المعلومة في حيازة شخص معين الذي يحق له التصرف فيها دون غيره كإستئثار مؤلف المعلومة أو صاحبها بها ، كما يرد الإستئثار على المعلومة المخصصة لمجموعة من الأشخاص ، و هذا الشرط يستلزم :

[1] – محمد محمد شتا، فكرة الحماية الجنائية لبرامج الكمبيوتر، دار الجامعة الجديدة للنشر، الإسكندرية، 2001، ص 62.

[2] – خالد مصطفى فهمي، المرجع السابق، ص 14.

-أن ترد المعلومة على حقيقة أو حدث ، فيكون لكل شخص من حيث المبدأ حرية الحصول عليها أو حيازتها ، و هذه الحرية غير مطلقة إلا في مرحلتها الأولى للحيازة و ذلك فيما قام الشخص بتجميع و حفظ المعلومات ذاتها ، فهو ينشأ بهذه الصورة ، عن طريق التجميع و الحفظ معلومة جديدة يمكن أن يستأثر بها و يتصرف فيها لوحده و بمفرده .

-أن ترد المعلومة على فكرة أو عمل ذهني ، و من هنا وجب النظر لها من خلال مالكها أو مبتكرها لكن قبل ذلك لابد أن تكون في شكل معين كي يمكن حمايتها فالشكل هو الرداء الذي يستر الفكرة و هو المظهر الذي تخرج من خلال المعلومة إلى الغير .[1]

2- أنواع المعلومات الإلكترونية :

يمكن أن تظهر المعلومات في أنواع مختلفة و متعددة و هذه الأنواع يمكننا حصرها وفق الطوائف التالية:

- المعلومات الإسمية Informations Nominatives :

و تنقسم بدورها إلى معلومات شخصية و أخرى موضوعية :

*** المعلومات الشخصية Informations Subjectives :**

و يقصد بها تلك المعلومات المرتبطة بشخص المخاطب بها مثل إسمه ، موطنه ، صحيفة السوابق القضائية الخاصة به ، و حالته الإجتماعية فهي المعلومات اللصيقة بشخص صاحبها التي لا يجوز للغير الإطلاع عليها إلا بموافقة صاحبها شخصيا أو بأمر من السلطات المختصة .

[1] - سليم عبد الله الجبوري ، المرجع السابق ، ص 39-40 .

*** المعلومات الموضوعية Informations Objectives :**

و هي تلك المعلومات المنسوبة إلى شخص قصد الإدلاء برأيه الشخصي فيها و التي تكون في شكل مقالات و الملفات الإدارية للعاملين لدى الجهات الإدارية إذن هي معلومات موجهة إلى الغير بحسب الأصل .

– المعلومات الخاصة بالمصنفات الفكرية :

وهي عبارة عن معلومات متمثلة في مصنفات فكرية تخضع لقوانين الملكية الفكرية و التي قد تكون مصنفات أدبية أو فنية أو مصنفات صناعية .

– المعلومات المباحة :

و يقصد بها المعلومات المتاح الحصول عليها للجميع لأنها بدون مالك و مثالها تقارير البورصة اليومية و النشرات الجوية ...الخ ، فإذا تم تجميعها بغرض معالجتها لتشغيلها على الكمبيوتر و إسترجاعها بقصد خلق معلومات جديدة و عليه هذه الطائفة ممكن ان نجدها في صورتين هي :

*** المعلومات المعالجة Informations Traités :**

هي المعلومات المعالجة للتشغيل على جهاز الكمبيوتر بقصد تخزينها وحفظها فيه بقصد إسترجاعها وقت الحاجة إليها .

***المعلومات المتحصلة Informations Résultats :**

وهي تلك المعلومات الناتجة عن معالجة مجموعة معلومات والتي تقرر حق ملكيتها طبقا لقواعد حيازة المال المنقول .[1]

[1] – سليم عبد الله الجبوري، المرجع السابق، ص 36.

– المعلومات على أساس صورتها التي تظهر بها :

*** المعلومات المتحركة و الساكنة :**

المعلومات الساكنة هي معلومات تكون في شكل معطيات أولية أو نتائج نهائية متواجدة داخل جهاز الحاسوب أما المتحركة فهي تلك المتنقلة و المتداوللة عبر شبكات الإتصال من حاسب آلي إلى آخر .

*** المعلومات المشفرة و غير المشفرة :**

و يقصد بها المعلومات المحجوبة عن التداول العام عن طريق برنامج لمنعها عن الغير ممن ليس لهم الحق في الإطلاع عليها و التعامل معها ما لم يصرح لهم بذلك فالوصول إلى المعلومات المشفرة يكون أصعب بكثير من تلك غير المشفرة فالأمر يتطلب الحصول على الشفرة و الإذن بإستخدامها .[1]

د – شبكة المعلومات (الأنترنت) :

مصطلح أنترنت إنجليزي الأصل مختصر و مركب من شقين الأول(Inter) يمثل الحروف الأولى لكلمة (International و ترجمتها دولي) ، أما الشق الثاني (Net)كذلك مأخوذ من الحروف الأولى لكلمة (Network و ترجمتها شبكة عمل) ، و بجمع المختصرات يتكون المصطلح الذي يعني الشبكة العالمية للمعلومات المشار إليها بالأحرف (w.w.w) ، و التي تعني (word wid web) أي الشبكة الدولية الإلكترونية المتعددة الأبعاد و الخدمات .[2]

فالأنترنت تعتبر وسيلة تواصل و تبادل للمعلومات فهي نظام للتخاطب بين الحواسيب تسمح بنقل الملفات و البرامج و البيانات ، التي تكون مكتوبة أو أصوات أو صور المشكلة في مجموعها للمعلومات الإلكترونية بين حاسوب لآخر أو لحواسيب متعددة في أماكن متباعدة

[1] – نفس المرجع السابق، ص 37.

[2] – جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ب.ط، 2000، ص 04.

جغرافيا و في زمن ضئيل جدا من أجل الحصول و إستبيان المعلومات المتوفرة فيها و تبادل تلك المعلومات مهما كان حجمها أو بعد أو طريقة الإرتباط فهي تساعد على ربط الإتصالات بين الأفراد و الجماعات لتبادل الخبرات و إنجاز المهام عن بعد أو الإثراء و النقد و ذلك إعتمادً على توجيه المعلومات من المرسل إلى المستقبل .[1]

كما أنها أصبحت وسيلة معلومات تجارية تتميز بالسرعة الفائقة و المذهلة التي تربط مسؤولي الإنتاج بالباعة و الزبائن في مجتمع واحد أو مجتمعات مختلفة على الفور أو في أي وقت و في كل وقت .[2]

و عليه فالأنترنت هي وسيلة للتوسط في عملية نقل المعلومات المتواجدة في الملفات و الوثائق و المخزنة في جهاز الحاسوب إلى جهاز حاسوب آخر فمكان المعلومة ليس الأنترنت وإنما هو الحاسوب و الأنترنت هي وسيلة ربط بين الحواسيب هدفها نقل المعلومة من جهاز لآخر عن طريق الشبكة التي تربط بين شبكات منتشرة في العالم و من هنا وجب التفرقة بين أنواع شبكة الأنترنت و بينها و بين شبكة الأنترانت و الإكسترانت وفق ما يلي توضيحه :

1 – **أنواع شبكة الأنترنت** : و هي نوعان

– **الشبكات المحلية (LAN) Local Area Network**:

وهي الشبكات التي تربط بين مجموعة حواسيب قريبة من بعضها البعض و المشتركة في المعدات المادية و البرامج و البيانات فقد تربط بين إدارة مؤسسة أو شركة و بين فروعها المحلية عن طريق ربط الحاسوب المركزي(حاسوب مركزي واحد على الأقل) الذي يمتاز بالسرعة العالية و قدرة تخزينه الكبيرة و المتواجد في الإدارة الرئيسية و بين حواسيب فروعها المحلية في شبكة صغيرة

[1] – أحمد الخليفة الملط، المرجع السابق، ص 27.

[2] – عمر خالد زريقات، عقود التجارة الإلكترونية، عقد البيع عبر الانترنت، ط1، دار الحامد للنشر والتوزيع، الاردن، 2007، ص 36.

محلية تقع في نطاق منطقة جغرافية ضيقة و ذلك عن طريق قنوات الإتصال المحدودة النطاق التي تكون فيها الإشارات مقيدة و محدودة كالأسلاك المجدولة و المحورية و الألياف الضوئية .[1]

– الشبكات الموسعة أو العامة (WAN) Wide Area Network:

و هذه الشبكة تربط الحواسيب عبر العالم أي أنها منتشرة في مناطق جغرافية متباعدة كالمدن و الدول و حتى القارات و ذلك عن طريق قنوات إتصال غير محدودة النطاق كخطوط الهاتف و موجات الأثير المنتشرة عبر الفضاء و الهواء بواسطة الأقمار الصناعية .

كما تجدر الإشارة هنا أنه يمكن ربط الشبكة المحلية بالموسعة تحقيقا لتدفق المعلومات و تبادلها بكيفية تمكن من التواصل بين المستخدمين عن بعد و من مواقع مختلفة ، و عليه إذا كان إستخدام الشبكة بكيفية محلية أي في الإيطار الخاص بكل أو بعض موظفي المؤسسة أو الشركة و في حدود تبادل المعلومات الخاصة بالجانب الوظيفي و العملي لها ، و دون تبادل للمعلومات العامة ، أو إستخدامها من طرف مستخدمو الأنترنت العاديين فتسمى هنا الشبكة بشبكة الإنترانت أما إذا كان إستخدام الشبكة بكيفية تسمح بتداول المعلومات للعامة (من أشخاص خارج المؤسسة و فروعها) كالموزعين و العملاء ...الخ ، فتسمى الشبكة بشبكة الإكسترانت .[2]

ومنه إذا كانت الأنترنت هي شبكة شبكات المعلومات فالإنترانت هي شبكة محلية LAN خاصة بالمشروع أو المنشأة (المؤسسة أو الشركة) معلوماتها خاصة بها و بموظفيها ممن هم مسموح لهم بالإطلاع عليها و إستخدامها دون غيرهم ، أما الإكسترانت فهي شبكة موسعة WAN متميزة بحيث لا تكتفي بتدفق و تداول معلومات المؤسسة أو الشركة بين مجموعة محدودة بل يتعدى ذلك لمجموعات تتعدى حدود الوظيفة تحقيقا لسريان المعلومات داخلها و خارجها و تسهيلا لمزاولة أعمالها و نشاطاتها .

[1] – خليفي مريم، المرجع السابق، ص 17.

[2] – نفس المرجع السابق، ص 18-19.

ومن هنا فالأنترنت وسيلة إتصالات عامة عابرة للحدود الدولية لا تملكه أي دولة أو أي جهة أو أي مؤسسة تكمن غايتها في تسهيل الإتصال و الربط بين وسائل الإتصال العادية (الحواسيب) لتبادل المعلومات مع بعضها البعض في شتى المجالات وفق شبكة معلومات بمحاكاتها لأية شبكة حاسبات إلكترونية على أن تكون متصلة و قادرة على العمل متى توقفت أية شبكة كومبيوترية أخرى في صورة إتصالات تشابكية تبادلية مشكلة لبيئة تفاعلية للمعلومات ببعد عالمي .[1]

2- خصائص الأنترنت :

تنفرد الأنترنت عن غيرها من وسائل الإتصال الأخرى من حيث مزاياها أو بمستلزماتها وآلية الإتصال بها أو من حيث إستخدامها و تطبيقاتها و هذا ما سنوضحه وفق ما يلي:

- **مزايا الأنترنت :**

تمتاز الأنترنت إجمالا بأنها تسمح لمستخدميها الإتصال بأية جهة معلوماتية (شركات المعلومات العالمية و بنوك المعلومات) للتزود بالمعلومات التي يرغبون في الحصول عليها .

كما أنها أقل كلفة في نقل البيانات و تحليلها و إعطاء المعلومات بشأنها عن باقي نظم الإتصالات الأخرى و ذلك لإختلاف التعامل فيها بين المجهز و المستفيد .

هذا بالإضافة للسرعة و الدقة الهائلة التي توفرها في تبادل المعلومات (أفكار ، رسائل ، عقود ...الخ) .

مع إمكانية الحصول على المعلومات من مختلف المراجع العلمية و غيرها لأي شخص أو باحث الذي يمكنه التواصل مع غيره و الإرتباط به في أي وقت و من أي مكان حتى و لو كانت المسافة التي تفرق بينهما تعد بآلاف الأميال و في قارات متعددة .

[1] - نفس المرجع السابق، ص 18-19.

ضم الشبكة لكمية كبيرة جدا من الوثائق و المعلومات في حواسيب الشبكات المحلية المرتبطة بها ، و التي أصبحت مبوبة ومصنفة بشكل يسهل الوصول إليها بالرغم من أنها مخزونة في عدد لا حصر له من الحواسيب و موزعة في كثير من الدول و المؤسسات ذات الأهداف و الأغراض المختلفة .[1]

كما تعتبر الأنترنت شبكة إتصال بين المشترك و بين مراكز المعلومات في العالم ، سواء منها المراكز الشخصية أو التابعة للدول ، بحيث يكون الإتصال بهدف الإطلاع على معلومات محددة أو بهدف فتح حوار مع أشخاص غير محددين أو مؤسسات ، كما يستطيع المستخدم نقل تلك المعلومات التي لديه إلى العالم بعد إدخالها إلى حاسوبه الشخصي و ربطه بالشبكة العالمية (الأنترنت) و من ثم وضعها في نطاق الخدمة العامة للشبكة ليأتي من يستقبلها عبر حاسوبه .[2]

3- إستخدامات الأنترنت :

تستخدم الأنترنت في عدة خدمات إلكترونية نستعرض أهمها:

- **خدمة البريد الإلكتروني (E-Mail) :**

تعتبر من أشهر و أقدم خدمات الشبكة التي توفر إمكانية الإتصال بالغير كبديل للبريد التقليدي بكيفية أسرع و أقل تكلفة ، بحيث يمكن من خلالها إرسال و إستقبال للرسائل و المتضمنة للنصوص المكتوبة و الملفات أو للصور أو الوثائق من و إلى المرسل إليه ، و ذلك بمعرفة عنوان البريد الإلكتروني للطرفين ، و ذلك من خلال برامج خاصة مرافقة للمتصفحات .

و بهذا أصبحت خدمة البريد الإلكتروني بديلا للطرود البريدية العادية التي تنطوي على كتيبات أو أوراق أو مستندات و وثائق ، و بالرغم من هذه الأهمية التي تقدمها هذه الخدمة إلا أنه من ممكن أن تشكل تهديدا على عملاء هذه الخدمة و مصالحهم فيما لو أسيء إستخدامها

[1] - حنان ريحان مبارك المضحكي، المرجع السابق، ص 14.

[2] - نفس المرجع السابق، ص 15.

كالدخول إلى البريد الإلكتروني من غير صاحبه و هذا مما يؤدي إلى فضح أسرار الناس و إصابتهم بأضرار جسيمة ، هذا بالإضافة إلى الرسائل المزعة و التهديدات...الخ و كلها أمور تتم عبر هذه الخدمة .[1]

- **خدمة الويب العالمية (World Wide Web)** :

هذه الخدمة معروفة إختصارا ب (WWW) و هي نظام فرعي من الأنترنت مشكلة لنظام معلوماتي عالمي، و هو مؤلف من كم هائل من النصوص و الصور و العينات الصوتية و لقطات الفيديو ...الخ ، و من خلال هذه الخدمة بإستخدام برامج خاصة تسمى متصفحات و التي تسهل عملية وصول مستخدمي الشبكة إلى المواقع و معاينتها و التنقل بينها و التي من أشهرها برنامج Navigator و برنامج Internet Exporer و بدونها لا تعمل هذه الخدمة فبواسطتها يستطيع مستخدمها تصفح محتويات هذا النظام ، عن طريق تتبع وصلات البحث أو إختيار المواقع المرغوب في زيارتها و القيام بنشاطات علمية (البحث الأكاديمي أو الجامعي) ، أو إجتماعية كالتعارف و التراسل ، أو ترفيهية كالألعاب و مواقع التسلية ، أو قراءة الصحف و المجلات ، أو إقتصادية كالتسوق و شراء الأسهم ...الخ ، و لكل موقع من مواقع الويب عنوانه الخاص به .[2]

- **محركات البحث (Search Engines)** :

و هي عبارة عن برامج مساعدة للبحث و الحصول عن المعلومات و هي متعددة و كل منها يستخدم بطريقة معينة و خاصة لإجراء عملية البحث بحيث يتم إخبار هذه الخدمة بإسم

[1] - خليفي مريم، نفس المرجع السابق، ص 29.
[2] - نفس المرجع السابق، ص 27.

موضوع المراد البحث فيه و من ثم يتم تزويد المستخدم بقائمة المواقع المتطابقة مع المعلومات المراد الحصول عليها .[1]

- **التخاطب و الإستشارات و المجموعات الإخبارية و المجلات و الكتب :**

بحيث أصبح بإمكان مستخدمي الأنترنت التخاطب (أو ما يعرف ب Chat) مع غيرهم مباشرة من مستعملي الشبكة عن طريق الرسائل المكتوبة أو صوتا و صورة و الرد عليها بنفس الكيفية ، و من أشهر و أقدم أنظمة هذه الخدمة نجد نظام IRC المعروف كإختصار ل Internet Relay Chat ،كما يمكن عن طريق الشبكة اللقاء و التحادث بين مستخدميها من ذوي الإهتمامات المشتركة بحيث يشكلون مجموعات للنقاش و تبادل للمعلومات و الأفكار(المختلفة العلمية ، الثقافية ، السياسية ، الإقتصادية...الخ)، كما أنها أضحت وسيلة للحصول على الأخبار من المواقع الإخبارية فقد تحولت الصحف و المجلات و حتى التلفزيونية أو الإذاعية إلى النشاط الإلكتروني عبر الأنترنت و هذا ينطبق على الكتب التي أصبحت تسمى الكتب الإلكترونية .[2]

- **خدمة تحويل و إسترجاع الملفات و المعلومات :**

فالأنترنت تحتوي على العديد من المعلومات و بالتالي يمكن لمستخدميها الرجوع للملفات الموجودة على مستوى الشبكة و إستخدامها بتحويلها و إسترجاعها من حاسوب إلى آخر و هذا عن طريق نسخ تلك الملفات بشرط أن تكون أجهزة الحاسوب مرتبطة بالشبكة .

4- مستتلزمات و برتوكولات آلية الإتصال بالأنترنت :

للإتصال بالشبكة لابد من توافر العديد من العوامل التي تنحصر في : جهاز الحاسوب الكاشف (Modem) الذي يربط بين جهاز المستخدم بالشبكة و يقترب عمله من عمل جهاز الهاتف العادي فهو يحول المعلومات الرقمية من الحاسوب إلى أصوات أو إشارات يمكن حملها عبر

[1] - حنان ريحان مبارك المضحكي، المرجع السابق، ص 17.

[2] - خليفي مريم، المرجع السابق، ص 30.

خط الهاتف ، و من المستلزمات أيضا نجد كذلك حساب الإشتراك المتمثل في شكل عقد إشتراك مع الشبكة و هذا بعد إختيار و الإتفاق مع مزود الخدمة على الإرتباط عبر خطه الهاتفي الخارجي و ينصب العقد هنا على تحديد تكلفة الإشتراك (رسوم الإشتراك) بالشبكة و توصيف الخدمات الممنوحة من المزود و المطلوبة من المستفيد ،[1] هذا إضافة إلى إسم الدخول و كلمة المرور (pass word) فالإسم وسيلة للتعرف على المتصل (المستفيد و طالب الخدمة) بالشبكة و بدونه لا يمكنه الدخول و الحصول على المعلومات من حاسوب آخر ، أما كلمة المرور فهي تعبر عن هوية المستفيد التي تشمل على عدد من الرموز (initiales) أو الحروف (letters) المخصصة له عند إبرامه عقد الإشتراك بالشبكةمع الجهة المعنية ، و أخيرا نجد من بين مستلزمات الإتصال بالشبكة ما يسمى مجهز خدمات الأنترنت (on line servise) و المقصود به الشركات التي تقدم إستعدادها لتجهيز خدمات الأنترنت فهي تسمى بالوسيط بين مدخل المعلومات و المستفيد بحيث تتم الوساطة هنا بالإتفاق بين المستفيد و طالب الخدمة (المتمثلة في الحصول على المعلومة المطلوبة) ، حصول الوسيط على مقابل (رسوم مقررة لفترات زمنية معينة كشهر مثلا أو أكثر) مالي كعوض مقابل الحصول على الخدمة المطلوبة .

و لكي تنظم مسألة الإنتشار الواسع للأنترنت كان لابد من التحكم فيها عن طريق ما يسمى بالبرتوكولات (Protocol) التي هي عبارة عن مجموعة القواعد و القوانين التي تتحكم ببث البيانات و تسمح للحواسيب بتبادل المعلومات فيما بينها ، كما يعرّف كذلك بأنه "لغة موحدة تسمح لأي جهاز مهما كان اللغة التي يستخدمها بإمكانية تبادل المعلومات مع الأجهزة الأخرى المتواجدة على الشبكة ، و ربط الشبكات المنعزلة مع بعض ، من خلال قنوات وصل ، و بالتالي يتم نقل معلومات كل شبكة إلى أخرى"[2] ، و من بين البرتوكولات المنظمة لنقل المعلومات نجد :

[1] – منير محمد الجمبيهي، محمود محمد الجمبيهي، الطبيعة القانونية للعقد الإلكتروني، دار الفكر الجامعي، د.س.ن، د.ط، ص 09.

[2] - Lionel Bochorberg : Internet et commerce électronique , Delmas, paris , 2001.

برتوكول (Internet Protocol)/(Transmission Protocol Control) TCP/IP

و هما برتوكولان ينظمان نقل المعلومات و البيانات من الحاسب الآلي إلى الأنترنت ، و يعدّان من أهم برتوكولات الأنترنت يقومان بربط و توصيل الشبكات ببعضها البعض ، فهما أساس الربط بين الأجهزة المختلفة على شبكة الأنترنت ، و ذلك من خلال منح كل جهاز أو موقع على الشبكة رقما معينا ، حتى يتواصل مع بقية أطراف الشبكة ، وعليه أي شبكة لا تستخدم البرتوكولين لن تتصل بالأنترنت .[1]

فبرتوكول TCP الذي هو برتوكول التحكم في نقل المعلومات مهمته نقل المعلومات ما بين جهازين متواجدين على شبكة الأنترنت عن طريق تقسيم تلك المعلومات إلى حزم فيعطي لكل حزمة رقم تعريفي حتى يمكن التعرف عليها ، بحيث تحوي كل حزمة على طاقة هوية تتضمن عدّة معلومات ، من بينها عنوان جهاز المرسل إليه .

بينما برتوكول الأنترنت IP فهو محدد للطريق الذي تسلكه تلك الحزم ، و محدد لسرعتها القصوى في نقل المعلومات ، و هو الذي يعطي للحزمة بطاقة هويتها ، التي تشمل عنوان جهاز الإرسال و عنوان جهاز الإستقبال.

وبتوافر تلك الآلية الإتصالية بين مجموع مستخدمي الشبكة العالمية للمعلومات عن طريق ربط حواسيب المستخدمين لها في كل مكان ، و بهذا يمكنهم التعامل مع بعضهم البعض في الحصول و تبادل المعلومات المرغوبة .

في الأخير نخلص أن النظام المعلوماتي تعبير فني يصعب على القانونيين إدراك طبيعته كما أنه تعبير متطور خاضع للتطورات التقنية الواقعة في البيئة الرقمية المتسارعة و المتلاحقة .

[1] – خالد ممدوح إبراهيم، إبرام العقد الإلكتروني دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2008، ص 22.

و عليه نستطيع القول هنا ان المشرع الجزائري كغيره من التشريعات أدرك هذه الحقيقة العلمية و إكتفى بذكر المقصود منه وفقا للدلالة العلمية .

و بالتالي فالنظام المعلوماتي هو "أي نظام مهما كان و كيفما كانت عناصره المرتبطة ببعضها البعض لتحقيق المعالجة الآلية للمعلومات من تجميعها و تخزينها و معالجتها و نقلها و تبادلها ...الخ من خلال برنامج أو مجموعة برامج معلوماتية" . و بهذا يكون النظام المعلوماتي نتاج دمج وسائل المعالجة (الحواسيب) مع وسائل الإتصال (الأنترنت) ، وفق المفهوم الشامل له .

و عليه و نظرا للتطور التكنولوجي الذي آلت إليه مسألة المعلومات بوصفها ذات طبيعة إلكترونية خاصة النظام المعلوماتي الذي حولها من طبيعتها التقليدية إلى ما آلت إليه في وقتنا الحالي و جعلها تمتاز بخصائص ميزتها عن صورتها التقليدية نذكرها وفق الآتي :

- أنها قائمة بذاتها و مستقلة عن الخدمة التي تؤديها ، فلا علاقة لها بالمكونات المادية المكونة للآلية التقنية التي تشكل أحد مكونات نظام المعلوماتية أو بالخدمة التي تكون محلا لها .
- أنها ذات قيمة إنسانية بوصفها نتاج إنساني .[1]
- أنها ملك فكري و نتاج مالكها سواء كان مبتدعها شخص طبيعي أو معنوي ، فالأنترنت لا تخول لأي مستفيد منها إمتلاك المعلومات ما لم يكن هناك إتفاق صريح و واصح بذلك و هذا تطبيقا للقواعد القانونية العامة المتعلقة بحقوق الملكية الفكرية و الأدبية .
- تمثل المعلومات لمالكها مصالح شخصية و إقتصادية في آن واحد، فلها آثارها بالنسبة للأشخاص المستفيدة منها .

انها فكرة أو أفكار مجالها و ميدانها لا حدود له فميدانها عام يعود للجميع كالهواء الذي يمكننا من الحياة ، فكل شخص يتنفس الهواء بطريقة آلية و متكررة فهو حق إنساني للجميع ، لهذا فإن المعلومات الإلكترونية تستلزم تنظيما قانونيا خاصا يحميها من أي إعتداء يقع عليها.

[1] – محمود السيد عبد المعطي خيالي، الأنترنت وبعض الجوانب القانونية، دار النهضة، القاهرة، 1998، ص 15.

المطلب الثاني : خصوصية جرائم الإعتداء على النظام المعلوماتي

خصوصية تلك الجرائم تتعدد من حيث مميزاتها و من حيث مرتكبيها بالإضافة الى تميزها من حيث أخطارها الناجمة عنها هو ما سنعالجه وفق الفروع الثلاثة التاليين :

الفرع الأول : خصوصية جرائم الإعتداء على النظام المعلوماتي من حيث مميزاتها

تتميز هذه الجرائم عن الجرائم التقليدية بمجموعة من الخصائص الفريدة و المتميزة ، بحيث تكمن أهمية تبيان تلك الخصائص في تحديد طبيعتها الخاصة التي تميزها عن غيرها من الجرائم كما أنها تحدد آثارها التي تنسحب على التحقيق فيها و على أطرافها ، وهي كالآتي :

أولا : أنها متعدية أو عابرة للحدود

بالنظر لإرتباط المجتمع المعلوماتي بالشبكة المعلوماتية (خاصة شبكة الأنترنت) التي تعبر الأزمنة والأماكن من دون أن تخضع في ذلك للحراسة ونقاط التفتيش، فقد ترتب على ذلك عدم اعتراف هذا المجتمع بالحدود الجغرافية للدول.[1] وهذه الخاصية مكنت مجرمي المعلوماتية من ارتكاب جرائم عن بعد ، فهناك في الغالب تباعد كبير بين الجاني والمجني عليه في هذه الجرائم، وبالتالي بين الفعل الإجرامي والنتيجة الجرمية حيث تتحقق الأخيرة في الغالب خارج حدود الدولة التي وقع فيها الأول.[2]

فجرائم الإعتداء على النظام المعلوماتي وإن كانت لا تنفرد بهذه الخاصية ، لوجود بعض الجرائم التقليدية التي تتميز هي الأخرى بهذه الخاصية ، مثلا كجرائم الإرهاب الدولي والإتجار بالمخدرات وغسيل الأموال والجرائم المنظمة عموما ، إلا انها مع ذلك تختلف عنها في ذلك من حيث أنها ترتكب في أغلب الأحوال من دون حاجة إلى الحركة والتنقل ما بين الدول.[3] هذا

[1] – نهلا عبد القادر المومني ، مصدر سابق ، ص 50.

[2] – نسرين عبد الحميد نبيه ، مصدر سابق ، ص 133.

[3] – محمود أحمد عبابنة ، مصدر سابق ، ص 34.

بالإضافة إلى أن هذه الجرائم تكون خاصيتها العالم الإلكتروني بعكس الجرائم التقليدية التي تكون خاصيتها في العالم المادي ، ومثل هذه الخاصية تزيد من مصاعب اكتشاف هذه الجرائم والتحقيق فيها.[1]

يمكن القول أن أهم الخصائص التي تميز جريمة الإعتداء على النظام المعلوماتي هي تخطيها الحدود الجغرافية ، ومن ثم اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود.

مجتمع التقنية الحديثة لا يعترف بالحدود الجغرافية ، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع للحدود ، فهي تربط بين دول لا تحدها حدود الطبيعة أو حدود السياسة وتسمح لمستخديها بالتنقل المعنوي أو الإفتراضي بين الدول والقارات بدون تعقيدات أو صعوبات أو عوائق ، فهي عالم ضخم متنوع متجدد خالي من الحدود والعوائق.

حيث أن أماكن متعددة في دول مختلفة قد تتأثر بجريمة تكنولوجيا المعلومات الحديثة الواحدة في أن واحد [2]، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب الجريمة عن طريق نظام معلوماتي إلكتروني موجود في دولة معينة ، بينما يتحقق الفعل الإجرامي في دول أخرى.

هذه الطبيعة التي تتميز بها تكنولوجيا المعلومات الحديثة كونها جريمة عابرة للحدود خلقت الكثير من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة ، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى اشكاليات تتعلق بإجراءات الملاحقة القضائية وبالتالي

[1] – رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، د.ط، 2013، ص 27.

[2] – محمد حسين ، المسؤولية القانونية في مجال شبكات الانترنت ،ط1 ، دار النهضة العربية ، القاهرة 2002، ص 08.

فإن الوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى [1] ، فجريمة تكنولوجيا المعلومات الحديثة لا تعرف بعنصر المكان أو الزمان ، حيث يلعب البعد الزماني (اختلاف المواقيت بين الدول) والمكاني (امكانية تنفيذ الجرمية عن بعد) والقانوني (أي قانون يطبق) دورا مهما في تشتيت التحري والتنسيق الدولي لتعقبها ، فالجرائم هنا لا تقتصر على دولة بعينها ، ومن الممكن أن يكون العالم كله مسرحا لها ، حيث يمكن للفرد أن يرتكب جريمة من أي مكان في العالم وفي أي زمان.

ومن القضايا التي لفتت النظر إلى البعد الدولي لهذه الجرائم ، فضيحة عرفت بإسم مرض نقص المناعة المكتسبة (الإيدز) وتتلخص وقائعها عام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج هدف في ظاهره إلى اعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة ، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة) ، إذ كان يترتب على تشغيله تعطيل جهاز الحاسب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطل مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس ، وفي الثالث من فبراير من عام 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية ، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي ، حيث إن ارسال هذا البرنامج قد تم من داخل المملكة المتحدة ، وبالفعل وافق القضاء الامريكي على تسليم المتهم ، وتم توجيه احدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة ، إلا أن اجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية.

[1] – محمود صالح ، "الجرائم المعلوماتية" ماهيتها ، صورها – ورقة عمل مقدمة إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الافتراضية والمنعقدة بسلطنة عمان، 2-4 ابريل 2006 ، ص 17.

ومهما كان الامر فإن لهذه القضية أهميتها من ناحيتين :

الأولى : أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية .

الثانية : أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة اعداد برنامج خبيث (فيروس).

ونتيجة لهذه الطبيعة الخاصة لجريمة المعلوماتية نظرا للخطورة التي تشكلها على المستوى الدولي تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم.[1]

والتعاون الدولي يتمثل في المعاهدات والإتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء ، الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء.

ثانيا : سهلة الإركاب

فهذه الجرائم يرتكبها الجاني في الغالب لوحده من دون ان يحتاج في ذلك للإستعانة بشخص أو أشخاص آخرين ، بعكس الجرائم التقليدية التي يحتاج الجاني في ارتكابها في الغالب لمثل هذه الإستعانة ، فالجرم المعلوماتي قادر على تنفيذ مخططه الإجرامي لوحده وهو جالس أمام الكمبيوتر في منزله أو مكتبه أو مقهى للأنترنت ضد ضحية موجودة في دولة أخرى تبعد عنه آلاف الأميال . ذلك أنه اذا كان الجاني يحتاج غالبا في ارتكابه للجرائم التقليدية إلى بذل جهود عضلية بحسب طبيعة كل جريمة منها.[2] من مثل كسر الأبواب أو الاقفال في جريمة السرقة ، فإنه لا يحتاج إلى مثل هذا الجهد العضلي في ارتكابه الجرائم المعلوماتية ، وإنما يحتاج فقط إلى قدر معين

[1] – تجدر الاشارة في هذا المجال إلى مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاقبة المجرمين والذي عقد في هافانا عام 1990 ، وفي قراره المتعلق بالجرائم ذات الصلة بالحاسب ، ناشد المؤتمر الدول الأعضاء أن تكثف جهودها ، كي تكافح بمزيد من الفعالية عمليات اساءة استعمال الحسب ، والتي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني ، بما في ذلك النظر إذا دعت الضرورة في تحديث القوانين والاجراءات الجنائية ، بما في ذلك اتخاذ تدابير من أجل ضمان الجزاءات والقوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الاجراءات القضائية تنطبق على جرائم تكنولوجيا المعلومات ، وادخال تغيرات مناسبة عليها اذا دعت الضرورة ، كما حث المؤتمر الدول الأعضاء على مضاعفة الانشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات ، بما في ذلك دخولها حسب الاقتضاء اطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل المرتبطة بالجرائم ذات الصلة بالرحاسب .

[2] – أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي والانترنت،دار وائل للطباعة والنشر عمان، 2001، ص 107.

من التفكير الذهني وبعضا ضغطات الأزرار.[1] كما وأنها تتطلب إلى اللجوء إلى القسوة أو الأفعال القاسية كالضرب والقتل ، ولا تكلف الجاني شراء الاسلحة والذخائر وغيرها من الأدوات الصعبة المنال من أجل تنفيذ عمليته الإجرامية ، وإنما تتطلب منه الحصول فقط على بعض الاجهزة والبرامج التقنية للتعامل مع النظام المعلوماتي والشبكة المعلوماتية ، لذا فهذه الجرائم تمنح الجناة في الغالب فرصة سانحة لتخفيض تكاليف ارتكاب جرائمهم.2وتكون مغرية للمجرمين عموما ، لأنها تحقق لهم أكبر قدر ممكن من الأرباح بأقل قدر ممكن من التكلفة والجهد والخوف.[3] وهذه الخاصية بدورها تقلل من امكانية تخلف آثار مادية عن الجريمة الواقعة ، وهو ما يصعب بدوره من مهمة اكتشاف هذه الجرائم والتحقيق فيها.

ثالثا : مكلفة للضحايا

فإذا كانت هذه الجرائم مربحة للجناة فإنها في ذات الوقت مكلفة للضحايا حيث أنها تتسبب عموما في الحاق أضرار مالية بليغة بضحاياها مقارنة بما يمكن أن تتسبب فيه الجرائم التقليدية. فبينما أن معدل خسائر البنوك من الجرائم التقليدية كالسطو المسلح هي (10000) دولار ، فإن معدل خسائرها المالية نتيجة هذه الجرائم المستحدثة تتراوح ما بين (100000) و (500000) دولار أمريكي .[4] لذا فإن لهذه الجرائم خطورة كبيرة في اقتصاديات الدول ، حسبما سنأتي إلى تفصيلها فيما بعد لدى تطرقنا لخطورة هذه الجرائم من الناحية الإقتصادية ، كما وأن مثل هذه الخسائر تدفع ضحايا هذه الجرائم (وهم في الغالب من المؤسسات والشركات التجارية والمالية) إلى النأي من الأخبار عن هذه الجرائم ، خوفا من أن يترتب عن ذلك أضرار اخرى تلحق

[1] – محمد حماد مرهج الهيتي ، جرائم الحاسوب – ماهيتها – موضوعها – أهم صورها – والصعوبات التي تواجهها ، ط1 ، دار المناهج ، عمان ، 2006 ، ص 144.

[2] –.نفس المرجع السابق، ص 107.

[3] – محمد بن حميد المزمومي ، جريمة الإعتداء على الأموال عن طريق الحاسب الآلي، دار النهضة العربية، الإسكندرية، 2007،، ص 32.

[4] – رشاد خالد عمر، المرجع السابق، ص 60.29

بهم وبسمعتهم كما سنأتي على تفصيلها فيما بعد في الفصل القادم ، ومثل هذا الامر يشكل بلا شك عائقا آخر أمام اكتشاف هذه الجرائم والتحري والتحقيق فيها.

رابعا : قليلة المخاطرة

فنسبة مخاطرة الجاني الناجمة عن ارتكاب مثل هذه الجرائم ، قليلة نسبيا بالمقارنة مع تلك الناجمة عن ارتكابه للجرائم التقليدية ، فهو غير معرض لخطر المواجهة المباشرة مع المجني عليه او غيره ولا لخطر المواجهة المسلحة من الشرطة ، كما وأن نسبة اكتشافه وتعرضه للإدعاء في مثل هذه الجرائم هي فقط 1 من 22000 حالة. وذلك بالنظر إلى صعوبة تتبع اثره على شبكة الأنترنت ، خصوصا وان هذه الجرائم لا تكتشف في الغالب إلا بعد مرور زمن طويل على ارتكابها ، وكل هذا بدوره يشكل عائقا آخر أمام اكتشاف هذه الجرائم والتحري والتحقيق فيها.

خامسا : خفية عن الأنظار

هذه الجرائم ترتكب بخفة وفي خفة شديدة ، بحيث أنها ترتكب في الغالب من دون أن يرى طرفا الجريمة (المجرم المعلوماتي والضحية المعلوماتية) بعضها البعض ، فهي نادرا ما تكتشف مباشرة من الضحية أو غيره ، وتقع في الغالب من دون أن يدرك المجني عليه نفسه بوقوعه ضحية للجريمة المرتكبة.[1] ولعل مما يزيد من خفاء هذه الجرائم هو أن أغلب ضحاياها لا يتوسلون ببرامج وأنظمة الحماية الفنية لحماية انظمة المعلوماتية غالبا ما يتوسل في ارتكاب هذه الجرائم ببرامج وتقنيات تمكنهم من العمل في الخفاء من اختراق جدران الحماية الأمنية تلك ، وكل هذا بدوره يصعب في امكانية اكتشاف الضحايا لهذه الجرائم والتبليغ عنها ، وهذا بدوره يشكل عائقا آخر أمام اكتشاف هذه الجرائم والتحقيق فيها.

[1] – أحمد المناعسة وآخرون، المرجع السابق، ص 108.

سادسا : وقوعها في بيئة الكترونية

فهذه الجرائم تقع في بيئة الكترونية ، وأن الأدلة التي تخلفها تكون في الغالب أدلة الكترونية ، وكل هذا بدوره يترتب عليه جملة من المشاكل والصعوبات التي تعوق اكتشاف هذه الجرائم والتحقيق فيها ، على أننا سنؤجل الكلام عن هذه المشاكل والصعوبات للفصل الثاني لدى تطرقنا لصعوبات اكتشاف الجرائم المعلوماتية الراجعة إلى الجريمة المعلوماتية في ذاتها.

سابعا : أنها ترتكب من خلال الوسائل التقنية

فهذه الجرائم تقع في بيئة الكترونية يستلزم التعامل معها استعانة الجاني بوسائل أجهزة تقنية تتمثل في الغالب بالكمبيوتر وملحقاته الأساسية من مثل أجهزة الطبع والمسح الضوئي وكذلك أجهزة الربط بالشبكات وغيرها.[1] ولكن مع ذلك يمكن ارتكاب مثل هذه الجرائم أيضا من خلال وسائل تقنية أخرى كأجهزة الهاتف (المحمول) المتطورة ، وغيرها من الأجهزة و التقنيات التي يمكن أن تظهر إلى الوجود في أي لحظة.

وهذه الخاصية بدورها تصعب من مهمة اكتشاف هذه الجرائم والتحقيق فيها إذا ما أخذنا بنظر الإعتبار أن مجرمي المعلوماتية غالبا ما يكونون على دراية واسعة بكيفية التوسل بهذه التقنيات بعكس جهات الإستدلال والتحقيق ، خصوصا التقليدية منها ، التي تكون في الغالب جاهلة بكيفية التعامل معها.

الفرع الثاني: خصوصية جرائم الإعتداء على النظام المعلوماتي من حيث مرتكبيها

ما من شك أن المدى الزمني لنشأة وتطور العلوم الجنائية وما نتج في نطاقها من دراسات وتحديدا في ميدان علم الإجرام أمكن في ظلها بلورة سمات عامة للمجرمين عموما ، وسمات خاصة يمكن استظهارها لطائفة معينة من المجرمين تبعا للجرائم التي يرتكبونها ، فعلى سبيل المثال : افرزت

[1] – نسرين عبد الحميد نبيه، المرجع السابق، ص 134.

الجرائم الاقتصادية ما يعرف بإجرام ذوي الياقات البيضاء ، وبالتالي كان طبيعيا ان تحمل ظاهرة الاجرام عبر تكنولوجيا المعلومات الحديثة في جنباتها والدة طائفة جديدة من المجرمين ، اصطلح جانب من الفقه على تسمية من ينتمي إليها بالمجرم المعلوماتي.[1]

ومن جهتنا يمكننا القول أن المجرم المعلوماتي "تعبير " ينطوي على قدر من التجاوز في القول ، فالصحيح أنه لا يوجد نموذج محدد للمجرم المعلوماتي ، بل هناك عدة نماذج للمجرمين قد يستخدمون نظام المعلومات الإلكتروني (أيا كان الجهاز الذي يحتوي مزايا هذا النظام) في جرائمهم وقد يقومون بأفعال جرمية ضد نظام المعلومات الإلكتروني نفسه ، هناك من يقتل أو يسرق عن طريق الإستعانة بالوسيط الإلكتروني ، وهناك من يعتدي على سمعة الآخرين أو على حرمة حياتهم الخاصة أو على الاخلاق والقيم عبر الوسيط الالكتروني ، وهناك من يرتكب جريمة التزوير عن طريق الاستعانة بالوسيط الإلكتروني وهناك من يرتكب جريمة تزوير عن طريق الاستعانة بنظام المعلومات الالكتروني ، وهكذا الأمر بالنسبة لصور أخرى من الجرائم ، وبالتالي فإن تعدد جرائم تكنولوجيا المعلومات الحديثة وتنوعها التي تغطي صورا عديدة من الانشطة ، أدى إلى عدم اتضاح الصورة بشكل جلي في شأن تحديد سمات مرتكبيها ، بحيث اختلف الباحثون في هذا الخصوص كما اختلفوا أيضا فيما اذا كان المجرم المعلوماتي ينتمي إلى الإجرام الطبيعي (المجرم بطبيعته أو ما يسمى بذي الياقات الزرقاء) أو إلى الاجرام الاصطناعي المكتسب (المجرم النظيف أو ما يسمى بذي الياقة البيضاء).[2]

ويرى عدد كبير من الباحثين الذين عنوا بالمجرم في جريمة المعلوماتية ، أن هذا المجرم وان كان يتميز ببعض السمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل اجرامي يتطلب

[1] –ناصر ين محمد البقمي، المرجع السابق، ص 43.

[2] – غنام محمد غنام ، عدم ملاءمة القواعد التقليدية لقانون العقوبات لمكافحة جرائم الكمبيوتر ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت ،كلية الشريعة والقانون ، جامعة الإمارات ، ماي، 2004 ، ص 02.

توقيع العقاب عليه . فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتهم من جرائم ذوي الياقات البيضاء ، من حيث انتماء المجرم في أكثر الحالات إلى وسط اجتماعي حسن ، وتميزه بدرجة من العلم والمعرفة [1]، وليس معنى ذلك أنهم اقل خطورة من الناحية الاجرامية عن المجرمين ذوي الياقات الزرقاء (المجرم بطبيعته) . ويرمز بعض الباحثين بكلمة SKRAM إلى مجموعة الخصائص التي تميز المجرم في جريمة تكنولوجيا المعلومات الحديثة بصفة عامة عن غيره من المجرمين ، وهي تعني المهارة Skils ، المعرفة Knowledge ، الوسيلة ,Ressources ، السلطة Authority ، الباعث Motive.[2]

ويرى الاستاذ باركر أن المهارة هي ابرز خصائص مجرم تكنولوجيا المعلومات الحديثة ، فتنفيذ جريمة تكنولوجيا المعلومات الحديثة يتطلب قدرا من المهارة يتمتع بها الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال و عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات الحديثة أو بمجرد التفاعل الإجتماعي مع الآخرين .[3]

إلا أن ذلك لا يعني ضرورة أن يكون مرتكب جريمة تكنولوجيا المعلومات الحديثة على قدر كبير من العلم في هذا المجال أو أن تكون لديه خبرة كبيرة فيه ، بل ان الواقع العملي قد اثبت أن بعض انجح مجرمي تكنولوجيا المعلومات الحديثة لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طريق التعليم أو الخبر المكتسبة من العمل في هذا المجال كما أننا نرى أن عددا لا بأس به من صور جرائم تكنولوجيا المعلومات الحديثة التي ترتكب عبر وسيلة تقنيات المعلومات الحديثة أي عندما لا يكون نظام المعلومات الإلكتروني هو هدف الجريمة ، لا يتطلب سوى قدر جد بسيط من توافر المهارة لدى المجرم.[4]

[1] – قورة نائل عادل، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي لبنان، ط1، 2005، ص 39.

[2] – أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، 2010، ص 20.

[3] – هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية القاهرة، 2009، ص 49.

[4] – مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة القاهرة، 2008، ص 144.

أما المعرفة فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها ، وامكانية نجاحها واحتمال فشلها ، فالجناة عادة يمهدون لإرتكاب جرائمهم بالتعرف على المحيط الذي تدور فيه ، حتى لا يواجه بأشياء غير متوقعة من شأنها افشال افعالهم أو الكشف عنهم .[1]

وتميز المعرفة بمفهومها السابق مجرمي تكنولوجيا المعلومات الحديثة ، حيث يستطيع مجرم التقنية الحديثة أن يكون تصورا كاملا لجريمته ، ويرجع ذلك إلى ان المصرح الذي تمارس فيه جريمة تكنولوجيا المعلومات الحديثة هو نظام الحاسب الشامل ، فالفاعل يستطيع أن يطبق جريمته على انظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.[2]

أما الوسيلة فيراد بها الامكانيات التي يتزود بها الفاعل لإتمام جريمته ، فمجرمو تكنولوجيا المعلومات الحديثة يتميزون بالقدرة على الحصول على ما يحتاجون إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الاجرامي. والحقيقة أنه كلما كان نظام المعالجة الآلية المستهدف غير مألوف ، كانت الوسائل المتطلبة اكثر صعوبة في الحصول عليها ، لإقتصارها على عدد قليل من الأفراد هم عادة القائمون على تشغيل النظام. ومن جهتنا فإننا نرى أن هذه السمة يتمتع بها المجرم في صور جرائم تكنولوجيا المعلومات الحديثة عندما يكون نظام المعلومات الإلكتروني هو هدف الجريمة.

أما السلطة فيقصد بها الحقوق او المزايا التي يتمتع بها المجرم في جريمة تكنولوجيا المعلومات الحديثة والتي تمكنه من ارتكاب جريمته ، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى نظام المعالجة الآلية، وقد تتمثل هذه السلطة في الحق في استعمال الجهاز الذي يحوي مزايا نظام المعلومات الإلكتروني أو اجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على انظمة المعلومات الإلكترونية.

1 – هلال بن محمد بن حارب البوسعيدي، المرجع السابق، ص 48.

2 – أحمد محمود مصطفى، المرجع السابق، ص21.

وقد تكون السلطة التي يتمتع بها الجاني غير حقيقية ، كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر. وبالنسبة لهذه السمة فإننا نرى أيضا أن غالبية صور جرائم المعلوماتية التي ترتكب عبر وسيلة تقنية المعلومات الحديثة أي عندما لا يكون نظام المعلومات الإلكتروني هو هدف الجريمة ، لا تتطلب توافر السلطة لكي يتمكن من ارتكاب جريمته.

أما الباعث – الدافع أو الغرض أو الغاية و كلها تعبيرات لها دلالاتها الإصطلاحية في القانون الجنائي– فيتصل بما يعرف بالقصد الخاص في الجريمة ، وهي مسألة تثير جدلا فقها وقضائيا واسعا ، ذلك أن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي [1] وأن الباعث لا أثر له في وجود القصد الجنائي [2] للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية.

فالباعث هو "العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والإنتقام"[3] وهو اذن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو " يختلف من جريمة إلى أخرى ، تبعا لإختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات كما يختلف بالنسبة للجريمة الواحدة من شخص إلى آخر".[4]

أما الغرض "فهو الهدف الفوري المباشر للسلوك الإجرامي ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات" [5] أما الغاية ،

[1] – محمود نجيب حسني ، شرح قانون العقوبات القسم العام النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الإحترازي، ط5، دار النهضة العربية القاهرة، 1988 ، ص 1052.

[2] – أحمد فتحي سرور ، الوسيط في قانون العقوبات، القسم العام ، ط5 ، دار النهضة العربية ، القاهرة ، 1991 ، ص 427.

[3] – محمود زكي أبو عامر ، قانون العقوبات القسم العام ، الدار الجامعية للطباعة و النشر ، بيروت ، 1990، ص 226.

[4] – فوزية عبد الستار، شرح قانون العقوبات – القسم العام – ، دار النهضة العربية ، القاهرة، 1992 ، ص 479.

[5] – محمود زكي ابو عامر، المرجع السابق ، ص 226.

"فهي الهدف البعيد الذي يرمي إليه الجاني بإرتكاب الجريمة كإشباع شهوة الإنتقام أو سلب مال المجني عليه في جريمة القتل".

والأصل أن الباعث والغاية ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين ،علم الجناية بعناصر الجريمة ،واتجاه ارادته إلى تحقيق هذه العناصر أو إلى قبولها. ولا تاثير للباعث أو الغاية "على قيام الجريمة أو العقاب عليها ، فالجريمة تقوم بتحقق عناصرها سواء كان الباعث نبيلا أو رذيلا وسواء كانت الغاية شريفة أو دنيئة ، وإذا كانت القاعدة أن الباعث أو الغاية لا أثر لهما على قيام الجريمة ، فإن القانون يصيغ عليها في بعض الاحيان أهمية قانونية خاصة".[1]

وبالنسبة لجرائم التقنية الحديثة ، فثمة دوافع عديدة تحرك الجناة لإرتكاب أفعال الاعتداء المختلفة المنضوية تحت هذا المفهوم ، ويمكننا من خلال الحالات التطبيقية تبين الدوافع الرئيسية التالية : السعي إلى تحقيق الكسب المالي ، الإنتقام من الشخص المستهدف والحاق الأذى به ، الرغبة في قهر النظام و التفوق على تعقيد وسائل التقنية ، الدوافع السياسية و الإيديولوجية [2]. والحقيقة أنه أيا ما كان الباعث وراء ارتكاب الجريمة المعلوماتية ، فإنه يوجد شعور دائم لدى مرتكب الفعل بأن ما يقوم به لا يدخل في عداد الجرائم ، ويرى الأستاذ "باركر" أن اغلب هؤلاء المجرمين غير قادرين على اقتراف الجرائم التقليدية وخاصة تلك التي تتطلب مواجهة مع المجني عليه، فالمجرم المعلوماتي لا يستطيع الإعتداء على المجني عليه بطريقة مباشرة إلا أنه لا يرى غضاضة في أنه يكون هذا الاعتداء عن طريق وسائل التقنية الحديثة.

[1] – محمود نجيب حسني ، المرجع السابق ، ص 480.

[2] – سامي الشوا ، الغش المعلوماتي كظاهرة اجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة 25-28 تشرين أول / أكتوبر 1993.

وبناء على ما تقدم يتضح لنا أن مجرمي المعلوماتية ، تتوافر فيهم سمات عامة بغض النظر عن الفعل المرتكب ، وسمات خاصة تبعا للطبيعة المميزة لبعض جرائم المعلوماتية ، والأغراض المراد تحقيقها ، لذا فإن تصنيف هؤلاء المجرمين وبيان السمات الأساسية لكل فئة يشكل أنجع الوسائل لردع هذه الفئات أو الحد من نشاطها بإعتبار ذلك من المسائل الموضوعية اللازمة لتحديد اتجاهات المكافحة ، وبالفعل فإن العديد من دراسات علم الإجرام الحديثة في ميدان إجرام التقنية تسعى في الوقت الحاضر إلى ايجاد تصنيف منضبط لمجرمي التقنية ، لكنها تجد صعوبة في تحقيق ذلك بسبب التغير السريع الحاصل في نطاق هذه الظاهرة والمرتبط أساسا بالتسارع الرهيب في ميدان التقنية الحديثة ، فالمزيد من الوسائل والمخترعات التقنية يساهم في احداث تغيرات على السمات التي يتصف بها مجرمو التقنية ، على الأقل السمات المتصلة بالفعل نفسه وليس بالشخص ، ولهذا يتجه الباحثون مؤخرا إلى الإقرار بأن افضل تصنيف لمجرمي التقنية وهو التصنيف القائم على أساس أغراض الإعتداء وليس على أساس التكتيك الفني المرتكب في الاعتداء أو على أساس الوسائط محل الاعتداء أو المستخدمة لتنفيذه.

وهناك العديد من الدراسات التي قامت بوضع تصنيف لمرتكبي جرائم تكنولوجيا المعلومات الحديثة ، ويعد من أهمها دراسة الأستاذ (Donn B Parker) مختلفة ، وأيضا دراسة الأساتذة (David Icove, Karl Seger & William) التي أوردوها في مؤلفهم جرائم الكمبيوتر[1] حيث قسموا مجرمي التقنية إلى ثلاث طوائف : المخترقون ، والحاقدون.

[1] –قورة نائلة عادل ، المرجع السابق ، ص 57 .

الدراسة الأولى : دراسة (Donn B Parker)

ذهبت في تصنيف مجرمي التقنية الحديثة إلى سبعة أنماط مختلفة هي كالتالي :

الطائفة الأولى : وتدعى Parkstar وتظم الأشخاص الذين يرتكبون جرائم المعلوماتية يقصد التسلية والمزاح مع الأخرين بدون أن يكون في نيتهم احداث أي ضرر بالمجني عليهم.

وكمثال على ذلك المراهق الكندي الذي تسبب في احداث حالة من الفوضى الشديدة على شبكة الأنترنت ، حيث تعرضت عدة مواقع لإزدحام مروري عبر الشبكة عندما انهال عليها هذا المراهق بالالاف منالرسائل المزعجة وقدررت الخسائر المادية بملايين الدولارات.[1]

الطائفة الثانية : تدعى Hackers وتظم في جنباتها أشخاص يرتكبون جرائم الاختراق والدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف التعلم واكتساب الخبرة أو بهدف هزم السلطة والتحدي أو بدافع الفضول أو لمجرد اثبات الذات والقدرة على التعامل مع هذه الأنظمة والتغلب عليها أوالتسبب بالإرباك للآخرين.[2]

الطائفة الثالثة : وتدعى Maliciaus Hackers وتضم أشخاص يكون هدفهم من ارتكاب الجريمة فقط الحاق خسائر بالمجني عليهم مادية أو معنوية ، دون أن يكون الحصول على مكاسب مادية من ضمن هذه الأهداف ويندرج تحت هذه الطائفة الكثير من مخترعي الفيروسات وموزعيها.[3]

الطائفة الرابعة :**Personal Problem Solvers** وهي الطائفة الاكثر شيوعا وهي تظم ببين جنباتها أشخاصا يعانون من مشاكل مادية ولا يستطيعون حلها ومواجهتها بالوسائل الأخرى بما

[1] – خبر منشور على الموقع الإلكتروني :(Web.fares.net/w/ee7ebaz(7/9/2001

[2] – مصطفئ محمد موسئ ، أساليب إجرامية بالتقنية الرقمية ، ماهيتها ،مكافحتها ، دراسة مقارنة، دار الكتب القانوينة ، مصر ، 2005، ص 25 .

[3] – نفس المرجع السابق ، ص 26 .

فيها اللجوء إلى الجريمة التقليدية. لذا فهم يرتكبون هذا النوع المستحدث من الجرائم بدافع ايجاد حلول لتلك المشاكل.[1]

الطائفة الخامسة : Career Criminals وتتضمن هذه الطائفة مجرمي التقنية الحديثة الذين يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة. ويعمل المنتمون إلى هذه الطائفة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على افعالهم وصف الجريمة المنظمة ، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل ، ويقترب المجرم المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.[2]

الطائفة السادسة :**Exterme Advocates تدخل** في عدادها الجماعات الإرهابية أو المتطرفة ، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي ، ويتركز نشاطها بيصفة عامة في استخدام العنف ضد الاشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه. ولقد بدأ اهتمام الجماعات الإرهابية ، وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو جريمة التقنية الحديثة. فإعتماد المؤسسات المختلفة داخل الدول على انظمة تكنولوجيا المعلومات الحديثة في انجاز اعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الاحوال قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات.[3]

الطائفة السابعة :**The Criminally Negligent** والتي تظم واحدة من أهم المشكلات التي تتصل بإساءة استخدام انظمة المعلومات الإلكترونية ألا وهي الإهمال. ولا شك في أن الأهمال في انظمة المعلومات الإلكترونية يمكن أن يترتب عليه في كثير من الأحيان نتائج خطيرة قد تصل إلى

[1] - نفس المرجع السابق ، ص 27 .
[2] - نفس المرجع السابق ، ص 28 .
[3] - نفس المرجع السابق ، ص 29 .

حد ازهاق الروح. ففي نيوزيلندا ، على سبيل المثال ، قام اثنان من مبرمجي أنظمة الحاسبات بتغيير في أحد البرامج التي تحدد خط سير أحد الطائرات ولم يتمكنوا من ابلاغ الطائرة بهذا التغيير مما يترتب عليه تحطم الطائرة لإصطدامها بأحد الجبال وقتل 60 راكبا كانوا على متنها ، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ.[1]

الدراسات الثانية : دراسة الأساتذة (David Icove , Karl Seger & William Vonstorch)

ذهبت في تصنيف مجرمي المعلوماتية إلى ثلاث طوائف :

المخترقون ، المحترفون ، الحاقدون.

الطائفة الأولى : المخترقون أو المتطفلون :Hackers & Crackers

وتضم هذه الطائفة بين جنباتها فئتين الأولى تدعى الهاكرز HacKers وهم متطفلون يتحدون اجراءات أمن النظم والشبكات ، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي واثبات المقدرة مثل ما حصل عندما حاول أحد المتخصصين في تقنية المعلومات اختراق إحدى موردي الانظمة الامنية لشبكة الانترنت البريطانية (رودهوتانت) بهدف كشف الفجوات الأمنية بها بالفعل نجح في الحصول على أسماء وعناوين وكلمات السر والمعلومات الخاصة بالبطاقات الإئتمانية لأكثر من 24 الف شخص. والفئة الاخرى تدعى الكراكرز Crackers أو الهاكرز ذو النوايا الإجرامية ، فإن اعتداءاتهم تعكس ميولا جرمية خطرة تنبئ عنها رغباتهم في احداث التخريب [2].

الطائفة الثانية : المحترفون

يتميز أفراد هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية بالتنظيم والتخطيط للأنشطة المركبة ، لذا فإن هذه الطائفة تعد الأخطر من بين الفئات الأخرى وتهدف اعتداءات

[1] - نفس المرجع السابق ، ص 30 .
[2] - نفس المرجع السابق ، ص 31.

أفرادها في الأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم ارتكاب جرائم التقنية الحديثة ، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي. وأفرادها يتم تصنيفهم وتقسيمهم إلى مجموعات متعددة إما تبعا لتخصصهم في نوع معين من الجرائم أو تبعا للوسيلة المتبعة من قبلهم في ارتكاب الجرائم : فمثلا نجد طائفة محترفي التجسس بكافة أنواعه الاقتصادي والسياسي والعسكري والأمني والصناعي ، ونجد مثلا طائفة مجرمي الاحتيال والتزوير ، وهؤلاء هم الطائفة التي تكون اغراضها متجهة إلى تحقيق كسب مادي والاستيلاء على أموال الآخرين وضمن هذه الطائفة أيضا ثمة تصنيفات عديدة ، وحتى في الطائفة الفرعية قد تتوفر تخصصات لبعضهم كأن يوجه الشخص أنشطته الإحتيالية إلى قطاع مزادات البضاعة والمنتجات على الأنترنت أو في ميدان الاستيلاء على بطاقات الإئتمان والاتجار بها.

وإلى جانب المعرفة التقنية المميزة والتنظيم العالي والتخطيط للأنشطة المنوي ارتكابها ، فإن أفراد هذه الطائفة يتسمون بالتكتم ، فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولن ما أمكن عدم كشف طرقهم التقنية لإرتكاب جرائم وحول الأعمال الغالبة على هذه الطائفة فإن الدراسات تشير إلى أنهم من الشباب الأكبر سنا من الطائفة الأولى وأن معظمهم تتراوح أعمارهم ما بين – 40 عام.[1]

الطائفة الثالثة : الحاقدون

أفراد هذه الطائفة يسعون إلى اثبات مقدرتهم ومهارتهم ولا يسعون في نفس الوقت إلى تحقيق مكاسب مادية أو سياسية أو غيرها من المكاسب ، وإنما يرتكبون انشطتهم الإجرامية بدافع الرغبة في الإنتقام والثأر ، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم على علاقة ما بالنظام محل الجريمة ، وإلى غرباء من النظام تتوفر لديهم أسباب الإنتقام من الشخص المستهدف

[1] – نفس المرجع السابق ، ص 32 .

في نشاطهم ، وأقرب مثال على ذلك أحد الطلبة عندما أراد أن يثأر من صديقته التي هجرته فخزن على موقعها الشخصي بشبكة الانترنت بدون علمها بعضا من صورها ذات الطابع الإباحي مصحوبة بتعليقات سيئة عن اخلاقها وسلوكها.[1]

وقد يكون الهدف من شن حرب عبر وسائط تكنولوجيا المعلومات الحديثة تقوم به دولة أو جماعة ارهابية في مواجهة دولة أخرى عادية لها ، تسعى من خلاله إلى تدمير المواقع الخدماتية التي تقدم خدمات للمواطنين في ظل ما يعرف بالحكومة الإلكترونية ، مثل ما حصل عندما قامت مجموعة اسرائيلية تطلق على نفسها لقب Lapoosh بالسطو على موقع مصرف لبنان على شبكة الأنترنت و إحتلته و وضعت على صفحته الرئيسية عبارة (ملك لشعب اسرائيل) . و مثال أخر كذلك عندما قامت المخابرات الاسرائيلية بإختراق موقع حركة حماس على شبكة الانترنت ونشر صور اباحية عليه في محاولة منها لتشويه صورة الإسلام.[2]

و أيا ما كانت درجة الدقة في رسم حدود كل طائفة من الطوائف التي ينتمي إليها مجرمو المعلوماتية ، فإننا نرى أن البواعث الرئيسية على ارتكاب الجريمة المعلوماتية والتي تحدد الطائفة التي ينتمي إليها مجرم المعلوماتية لا تخرج عن ثلاثة بواعث تحركه. أما الباعث الأول فتشترك فيه جريمة المعلوماتية مع غيرها من الجرائم التقليدية ، كتحقيق الربح المادي في جرائم الاعتداء على الأموال والحاق الأذى المادي أو المعنوي بالشخص المستهدف في جرائم الاعتداء على الأشخاص. في حين يميز الباعث الثاني جريمة تقنية المعلومات الحديثة عن غيرها ويتمثل في الرغبة في الدخول في انظمة المعلومات الإلكترونية والمعلومات التي تحتويها لا لغرض سوى التسلية أو اثبات الخبرة التقنية التي يتمتع بها الفاعل أو غير ذلك من الأغراض التي لا يكون السعي إلى تحقيق ربح مادي أو الإضرار بهذه الانظمة من بينها. وأخيرا يأتي الباعث الثالث والذي يتمثل في الرغبة في الأضرار

[1] - نفس المرجع السابق ، ص 33 .
[2] – نفس المرجع السابق ، ص 34 .

بهذه الأنظمة ، سواء كانت هذه الرغبة بدافع الإنتقام أو لمجرد الإضرار بها أو غير ذلك ، وينتمي إلى هذه الطائفة مستخدمو فيروسات الحاسبات الآلية.

الفرع الثالث : خصوصية جرائم الإعتداء على النظام المعلوماتي من حيث اخطارها

فيما يلي نسلط الضوء على مدى خطورة جرائم المعلوماتية من حيث الكم والنوع على مجالات الحياة الرئيسية (الإقتصادية و الإجتماعية و النفسية و الصحية و العسكرية و الأمنية والسياسية و أخيرا الجوانب الإدارية) لذا سنتناول هذا الأمر في خمسة نقاط ، ندرس في الأول منها الاخطار الإقتصادية لجرائم المعلوماتية فيما نبحث في النقطة الثانية أخطارها الاجتماعية في حين نناقش في النقطة الثالثة اخطارها النفسية والصحية واخيرا نتطرق في الرابعة إلى اخطارها العسكرية والأمنية والسياسية أما النقطة الأخيرة فمخصصة للأخطار في الجانب الإداري

أولا : أخطارها الاقتصادية

للجرائم المعلوماتية اخطار لا توصف من الناحية الإقتصادية ، لوقوعها في معظم الأحوال على معلومات وبرامج ذات قيمة اقتصادية عالية ، سواء في ذاتها أو لإرتباطها بأموال قيمة ، مما يؤدي في الغالب إلى خسائر مالية فادحة ، إذ أنه وبمجرد حصول المجرم المعلوماتي على الوقت والوسيلة الكافيتين لتنفيذ جريمته فإنه قد لا يتردد في القضاء على أكبر المؤسسات الإقتصادية في العالم.[1] فالمجرم المعلوماتي يختلف عن المجرم العادي ، من حيث أنه يستخدم العقل والتقنية في عمليته الإجرامية بدلا من الأسلحة ليستولي في الغالب على مبالغ طائلة تفوق بكثير عما يستولي عليه المجرم الإعتيادي ، فمثلا أن معدل ما يسرق اللص العادي في الولايات المتحدة الامريكية هو ما دون الـ (10) آلاف دولار ، بينما أن معدل ما يسرق المجرم المعلوماتي هو حوالي (45) الف

[1] – محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة و القانون الجنائي ، دار الثقافة ، عمان ، 2004 ، ص 40 .

دولار.[1] وتعتبر الولايات المتحدة الامريكية الدولة الأكثر تضررا من الجرائم المعلوماتية من الناحية الاقتصادية ، حيث أنها تخسر سنويا ما مقداره (67.2) مليار دولار من جراء هذه الجرائم.[2]

أما على صعيد الدول الأخرى ، فإنه قد سبق وأن قدرت دراسة أجريت في بريطانيا عام 1990 حجم الخسائر المالية الناجمة عن هذه الجرائم في ذلك البلد بـ (400) مليون جنيه استرليني سنويا ، وفي فرنسا قدرت الخسائر المالية الناجمة عن هذه الجرائم فيها بـ (12.720) مليار فرنك فرنسي سنويا ، وذلك بمقتضى دراسة قامت بها الجمعية الفرنسية لأمن المعلومات عام 1996.[3] واما على صعيد الدول العربية فإنه وبمقتضى دراسة أجرتها منظمة (Softwar Alliance Business) في الشرق الأوسط تبين أن مجموع الخسائر المالية الناجمة عن هذه الجرائم في كل من المملكة العربية السعودية والإمارات العربية المتحدة معا تقدر بـ (30) مليون دولار سنويا ، وفي لبنان بـ (1.400.000) دولار سنويا.[4]

ثانيا : أخطارها الاجتماعية

ان خطورة جرائم المعلوماتية لا تتوقف عند حدود الإقتصاد بل تتخطاها لتشمل أيضا النواحي الإجتماعية للأفراد والمجتمعات وكالآتي :

1- المساس بالآداب والأخلاق العامة للمجتمع من خلال نشر الصور واللقطات والأفلام الجنسية (الإباحية) على شبكة الأنترنت، فعالمنا المعاصر يعيش ثورة جنسية طاغية ، تجاوزت كل الحدود والقيود ، بحيث أصبحت تشكل تهديدا كبيرا للمجتمعات البشرية ، فهي كما يقول (جيمس ريستون) الصحفي في جريدة نيويورك تايمز سيكون في النهاية أشد فتكا من الطاقة النووية في خطورتها على المجتمعات البشرية "، وأبرز سبب لهذه الثورة هو ظهور شبكة الأنترنت التي

[1] – قحطان محمد صالح الجميلي ، آلة العصر (الكمبيوتر) ، منشورات مكتبة الشعب ، بغداد ، 1985 ، ص 29.

[2] – عبد الرحمان جلهم حمزة ، جرائم الانترنت من منضور شرعي وقانوني ، ظافرة للتصميم والطباعة ، بغداد ، ب ، س ، ن، ص 22.

[3] – نائلة عادل فريد قورة ، المرجع السابق ، ص 80.

[4] – عبد الرحمان جلهم حمزة ، مرجع سابق ، ، ص 20-21.

ربطت العالم بأسره مع بعضه البعض ، وجعلته (بالأخص أمريكا وأروبا) يعيش جنونا جنسيا محموما في عالم الأزياء والافلام والصور الجنسية الفاضحة ، حتى أمسى الجنس هو الشغل الشاغل لعقول أغلب أفراد المجتمع البشري.[1] فتمثل هذه الشبكة واحدة من أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية وبشكل يقتحم على الجميع بيوتهم ومكاتبهم ، ولذلك فقد لجأ مروجوا تجارة الجنس إليها بغية الحصول على ارباح طائلة بأقل قدر ممكن من المخاطر ، حتى باتت توجد على هذه الشبكة اليوم طوفان من هذه الصور والأفلام ، بشكل لم يسبق له مثيل في تاريخ البشرية.[2]

وكل هذه المواقع والمواد الإباحية ، بلا شك لها آثارها السلبية على المجتمع وأفراده ، فمن يتعرض لمشاهدة هذه المواد ، فغنه في بادئ الامر قد يرتاد على هذه المواقع من حيث الفصول أو الخطأ ومن ثم يبدأ بالإدمان عليها إلى أن يصل اخيرا إلى مرحلة لا يعتبر فيها الإغتصاب جريمة ويسهل عليه ارتكاب الجرائم الجنسية ، والأخلاقية ولهذا فقد ذهب رأي من الباحثين إلى أن هناك علاقة طردية ما بين مشاهدة هذه المواد وارتكاب بعض الجرائم التقليدية. فكثيرا ما يؤدي الإدمان على مشاهدة هذه المواد إلى اعتداء الآباء على أولادهم جنسيا أو إلى اعتداء الازواج على زوجاتهم بإعتداءات لا أخلاقية ولا انسانية ولا دينية.[3]

ولعل ما يزيد خطورة الأمر هو أن كل مستخدم للأنترنت ، صغيرا كان أم كبيرا معرض اليوم لمشاهدة هذه المواد فالوصول إلى المواقع الاباحية قد أصبح سهلا في الوقت الحاضر بشكل

[1] – عارف خليل أبو عيد ، جرائم الأنترنت ، بحث منشور في مجلة جامعة الشارقة للعلوم الشرعية والقانونية ، المجلد الخامس ، العدد الثالث ، شوال /1429 هـ (أكتوبر /2008)، الشارقة ، ص 91.

[2] – حسن طاهر داود ، جرائم نظم المعلومات ، الطبعة الأولى ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2000 ، ص 93.

[3] – عبد الله عبد العزيز اليوسف ، التقنية والجرائم المستحدثة ، بحث منشور ضمن كتاب (الظواهر الإجرامية المستحدثة وسبل مواجهتها)، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الامنية الرياض ، 2004 ، ص 227.

يمكن معه حتى للمراهقين والأطفال الوصول إليها مع كل ما يحمله ذلك من أخطار لا توصف على هؤلاء الأبرياء.

2- المساس بخصوصيات حياة الأفراد ، نتيجة اختراق اجهزة الكمبيوتر واختراق البريد الإلكتروني وغيرها ، فمثل هذه الجرائم تشكل بلا شك تهديدا جسميا لخصوصيات وأسرار حياة الأفراد الشخصية والعائلية ، وسواء أحدث الاختراق من قبل الهاكرز أو الكراكرز.[1] أم من قبل جهات حكومية ، فإنها بلا شك تعتبر خرقا لأحد المبادئ الدستورية الراسخة ، ألا وهي مبدأ حق الانسان في الخصوصية.

3- المساس بسمعة وشرف وإعتبار الأفراد ، عن طريق نشر صور مشينة لسمعتهم وشرفهم ، سواء اكانت تلك الصور حقيقية أم مزيفة ومعدلة من خلال برامج تعديل الصور أو عن طريق السب والقذف والتشهير عبر الأنترنت ونشر الأقوال والتهم الملفقة ضد الافراد وبالأخص الذين يمثلون رموزا دينية أو سياسية في مجتمعهم.[2]وكثيرا ما تتسبب مثل هذه الجرائم في حدوث نتائج خطيرة كارثية تهدد استقرار الاسر والمجتمع ، فكم هي حالات الطلاق والضرب والقتل التي وقعت على ضحايا أبرياء نتيجة مثل هذه التهم الملفقة وبالأخص قذف النساء بتهمة الزنا .

ثالثا : أخطارها النفسية والصحية

إن للجرائم عموما أثارها السلبية على نفسية الضحايا ، إلا أن الآثار السليبة التي توقعها الجرائم المعلوماتية على نفسية ضحاياها تكون في الغالب أشد وقعا من تلك التي توقعها الجرائم التقليدية ، وبصورة عامة يمكن اجمال هذه الاثار بما يلي :

[1] – الهاكرز (Hackers) : هم من يقومون بالاختراق المجرد لنظم المعلومات ، وذلك على سبيل التحدي أو التسلية أو المغامرة ، من دون ان يتوافر لديهم النية في الاضرار بالنظام المخترق ، وأما الكراكرز (Crackers) : فهم لا يتوقفون عند حدود الاختراق المجرد ، وإنما يهدفون من وراء الاختراق إلى ارتكاب جريمة أخرى أو الإضرار بالنظام المعلوماتي المخترق ، وللمزيد من التفصيل ،ينظر : نسرين عبد الحميد نبيه ،ا لمرجع السابق ، ص 40-41.

[2] – علي بن عبد الله العسيري ، الآثار الأمنية لإستخدام الشاب للأنترنت ، ط1 ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004 ، ص 47-48.

1- ان المجني عليه في مثل هذه الجرائم ، يشعر بصورة مستمرة بعدم الارتياح النفسي لشعوره الدائم بضياع حقوقه وعدم امكانية استرجاعها ، لان الجاني في الغالب يكون مجهولا ، ويصعب اكتشافه ، كما ويشعر دوما بعدم الأمان والطمأنينة النفسية لا في حاضره ولا مستقبله ، حيث يشعر دوما بأنه معرض لخطر هذه الجرائم الخفية ، وأن خصوصياه واسرار حياته الشخصية والعائلية ومستوراته عموما معرضة للخطر الافشاء والانكشاف للملايين من مستخدمي الشبكة العنكبوتية ، وأن أمواله ونقوده الإلكترونية عرضة للسرقة والاختلاس ، واستمرار مثل هذا الشعور يخلق لديه في النهاية شعور آخر ، يتمثل بفقدان للثقة فيمن حوله من أصدقائه وأقربائه وزملائه في العمل أو الدراسة ، ممن يستعملون الكمبيوتر والانترنت.

2- إن اغلب ضحايا الجرائم المعلوماتية وبالأخص جرائم المواقع الإباحية يعانون في كثير من الأحيان من الإدمان على ارتياد هذه المواقع ، وبلا شك فإن مثل هذا الادمان لا يقل خطرا على الادمان على أقوى أنواع المخدرات ، بل انه قد يكون أشد منه خطرا وفتكا.

3- ان خطورة هذه الجرائم ، لا تقف عند الحدود النفسية ، بل تتعداها لتنتج عنها أخطار صحية قد تؤدي أحيانا بحياة الأبرياء ، ولعل أبرز مثال على ذلك هو ما حدث وان قام به أحد المجرمين المعلوماتيين (الكراكرز) لدى إختراق النظام المعلوماتي لإحدى المستشفيات في الولايات المتحدة الامريكية ، حيث أنه أقدم على العبث بملفات النظام ، مما أدى بالنتيجة إلى وفاة احد المرضى الراقدين في المستشفى.[1]

رابعا : أخطارها العسكرية والأمنية والسياسية

إذا كانت الدول فيما مضى تقاوم الجرائم التقليدية التي تقع على مصالحها العسكرية و الامنية والسياسية ، فإن عليها اليوم ان تواجه الجرائم لمعلوماتية الاكثر خطورة في هذا الصدد من الجرائم التقليدية ، نظرا لصعوبة اكتشافها ، فهذه الجرائم تعتبر كالشبح بالنسبة للدول وبالأخص

[1] - نفس المرجع السابق، ص 48-49.

الدول النامية التي لا تملك ما يكفي من التقنية لمواجهتها وإكتشافها ، وأهم المخاطر في هذه المجالات يمكن اجازها بما يلي :

1- على صعيد المخاطر العسكرية ، فإن الخطر الحقيقي لهذه الجرائم يتمثل في جرائم التجسس المعلوماتي ، حيث باتت بإمكان الكثير من الدول التي تملك التكنولوجيا ان توم بالتجسس على المواقع المنشآت العسكرية (السرية وغير السرية) للدول الأخرى من خلال أقمار صناعية وأجهزة تقنية متطورة ومعدة خصيصا لذلك ، واضحى بإمكان هذه الدول الوصول إلى معلومات ما كان ليصل إليها الجاسوس الاعتيادي إلا بطريقة مميزة.

2- على صعيد المخاطر الأمنية ، فإن بعضا من الجرائم المعلوماتية كالإرهاب الإلكتروني وجرائم غسيل الاموال عبر الانترنت وغيرها من الجرائم المنظمة امست تشكل تهديدا حقيقيا للأمن القومي للدول المعاصرة، خصوصا بعد أن أصبح هناك نوع من الإرتباط الطبيعي ما بين الجريمة المنظمة وشبكة الانترنت ، والذي هو ارتباط قابل للإزدهار والتطور يوما بعد يوم ، ذلك أن هذه الشبكة توفر للجريمة المنظمة القنوات والاهداف في آن واحد ، وكذلك توفر لها أيضا أفضل الفرص لإستغلال هذه القنوات والاهداف ، في سبيل تحقيق أكبر قدر ممكن من الأرباح ، بأقل قدر ممكن من الخسائر والمخاطرة ، وهذا ما تربو إليه جماعات الجريمة المنظمة دوما.[1]

وعلى وجه العموم فإن جرائم الإرهاب الإلكتروني تعد من أخطر هذه الجرائم ، فوسائل الاتصال الحديثة كالهواتف المحمولة والهواتف التي ترتبط بالأقمار الصناعية ، وأنظمة المعلومات الإلكترونية الحديثة كالكمبيوتر والأنترنت والفاكس والبريد الإلكتروني وغيرها كلها قدمت خدمة غير مقصودة للإرهابيين وباتت هذه الوسائل شائعة الإستعمال من قبل الجماعات الإرهابية ، ومنحتها مساحات شاسعة في مرونة العمل ، وساعدتها على زيادة أنشطتها ، كما وأدت إلى

[1] – عبد الله عبد الكريم عبد الله ، جرائم المعلومات والإنترنت (الجرائم الإلكترونية) ، ط1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007 ، ص 42.

زيادة ملحوظة في نطاق الإرهاب العابر للحدود ، وذلك من خلال ضمانها لعنصر السرية الضرورية لأعمال هذه الجماعات ، وعنصر الديمومة الضرورية لنقل أفكارها ، وعنصر تسهيل اتصالها بالجماهير.[1]

الجماعات في تجنيد الاشخاص على وجه الخصوص الاحداث والمراهقين الابرياء لإيقاعهم في مستنقع الإرهاب ، كما وساعدتها على نشر عملياتها بالصوت والصورة ، وفي التحريض على القتل والارهاب ، وفي الحصول على التمويل اللازم لإدامة عمليتها.[2]

وأما المخاطر السياسية لهذه الجرائم ، فإنها تتمثل في جرائم التشهير برؤساء ومسؤولي الدول ورموزها السياسية والقيادية ، وذلك من خلال نشر أقوال واشاعات بذيئة ومسيئة لسمعتهم ، أو نشر صور مشينة لهم سواء أكانت هذه الصور حقيقة أم مزيفة ، وذلك من اجل اضعاف مواطني دولهم بهم ، واضعاف نفوذهم على الصعيد الوطني والدولي.[3]وكذلك من اجل زرع الفتن والإضطرابات والإخلال بالإستقرار السياسي في دول الضحايا ، حتى باتت هناك مواقع الكترونية متخصصة بالسب والقذف والتشهير عبر شبكة الانترنت.

خامسا: أخطارها الإدارية

لم يعد أمام أي دولة سوى الاتجاه نحو المجتمع الإلكتروني والتكنولوجيا الرقمية فقد جعلت وسائل الإتصال الحديثة العالم يشبه المدينة الواحدة في تقارب أجزائه.

[1] – محمد أنور البصول ، الأنترنت واسهامه في عمليات الإرهاب ، بحث منشور ضمن (كتاب الإرهاب والعولمة) ط 1 ، مركز الدراسات والبحوث – جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2002 ، ص 279-285.

[2] – سامي علي حامد عياد ، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2006 ، ص 55-64.

[3] – منير محمد الجنبيهي وممدوح محمد الجنبيهي ، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، الإسكندرية ، 2006 ص 34-36.

ولقد أدت التقنيات الحديثة للمعلومات والاتصالات إلى إحداث تطورات هائلة في الحياة العامة سواءً على مستوى الأفراد الذين يرغبون في الحصول على خدماتهم بصورة أكثر تطورا وسرعة ودقة عالية، أو على مستوى الهيئات والمؤسسات القائمة على تقديم تلك الخدمات.

ولقد أصبح إدخال تكنولوجيا المعلومات في كافة الأعمال الحكومية هو هدف العديد من الدول التي تسعى للتقدم والرقي والتي منها الجزائر بحيث سعت إلى إستخدام تكنولوجيا المعلومات في الأجهزة الحكومية .

أدى إرتباط إستخدام تكنولوجيا المعلومات في الأجهزة الحكومية لظهور مصطلح جديد أطلق عليه الحكومة الإلكترونية الذي من خلاله تسعى الإدارة إلى تبسيط وتسهيل التعاون بينها وبين الأفراد وتوفير المعلومات بشكل متكامل وسريع للجميع لتحسين أداء الإدارة وتسهيل حصول المواطن على الخدمة بأقل تكلفة .

في وقتنا هذا طرح في ميدان الفكر مصطلح الحكومة الإلكترونية[1] الذي يشد الإنتباه باعتباره مصطلح حديث مرتبط بالمعلوماتية وتقنياتها المرتبطة بتكنولوجيا المعلومات.

فمع تطور تكنولوجيا المعلوماتية سارعت الحكومات الرشيدة إلى بحث تنفيذ نظام يغير من أسلوب تقديم وكيفية الحصول على الخدمات التي تقدمها الإدارات الحكومية والمجالس البلدية والإقليمية وأجهزة الحكم عموما بصورة أمثل تختصر الوقت والجهد والمال أيضا مع تحسين الأداء والكفاءة و الفعالية.

بحيث يرى البعض أنها تعني إستخدام وسائل الإتصال التكنولوجية المتنوعة والمعلومات في تسيير سبل أداء الإدارات الحكومية خدماتها العامة الإلكترونية ذات القيمة، والتواصل مع طالبي

[1] – لفظ الحكومة الإلكترونية متعلق بالصفات و المعاني التي توصف بها من حيث كونها سلطة عامة وركن في الدولة او الوزارة أو الهيئة التي تقوم بتنفيذ القوانين وإدارة المرافق العامة وغير ذلك.

إستخدام وسائل الإتصال الإلكترونية عبر بوابة واحدة وكذلك إستخدام المعلومات بطرق تعتمد على الآلية الالكترونية.

وهذا يعني أن الحكومة الإلكترونية تتبنى التغيير أو التعديل في العلاقات الأساسية بين الحكومة من ناحية، ولجمهور المواطنين ورجال الأعمال من ناحية أخرى من خلال طريقتين:

-تقديم الخدمات بطريقة مختلفة عن طرق التقليدية بواسطة تكامل المعلومات وتميز الأفراد من الوصول إليها عن طريق الأنترنت.

- التحول في طبيعة ممارسة السلطة عن طريق العمل على تحسين العلاقات وإقامة جسور الثقة بين الدولة ومواطنيها التي تعمل على الإستفادة من إمكانات تكنولوجيا الإتصال لتطوير الأداء الإداري والحكومي، وتحسين علاقة القائمين على المرفق العام بجمهور المتعاملين معه، وتحقيق الديمقراطية الإدارية بإتاحة الفرصة للجمهور لإبداء رأيه في مستوى أداء المرفق لخدماته وأخذه في حسبان القائمين على إدارة المرفق[1].

بينما يرى البعض الآخر أن الحكومة الإلكترونية تعرّف في مدلولها بمعنيين أحدهما واسع و الأخر ضيّق فالمعنى الواسع للحكومة الإلكترونية وفقا له تعني الإستخدام الأوسع للتكنولوجيا الحديثة في تنظيم الأعمال الحكومية وتطوير البنية التحتية المحلية اللازمة لذلك، بشكل يؤدي إلى إستفادة الحكومة من الإنترنت والمعلومات واتصالات التكنولوجية لإنجاز معاملات الأفراد بسهولة وسرعة، وتبعا لهذا المعنى فالحكومة الإلكترونية ليست مقصورة على بتوفير الخدمات للمواطنين عن طريق الأنترنت فحسب بل تشمل المحاولة الدائمة للحصول على أجود الخدمات الحكومية في

[1] ماجد الحلو ، الحكومة الإلكترونية والمرافق العامة، بحث مقدم إلى المؤتمر العلمي الأول الذي نظمته أكاديمية شرطة دبي حول " الجوانب القانونية والأمنية لعلميات الإلكترونية من 26-28 أفريل 2003. ص 6-10.

العلاقات الداخلية والخارجية من خلال الطرق الإلكترونية دون إعتبار للمكان والزمان أو تمييز أو إخلال تكافؤ الفرص.

أما المعنى الضيق للحكومة الإلكترونية فيعني مجموعة الأنشطة الحكومية التي تعتمد على الأنترنت والإتصالات الإلكترونية عبر مجموع طبقات ومستويات الحكومة لتقديم الخدمات والمعاملات للأفراد والحصول على المعلومات في شتى المجالات بيسر وسهولة.

فالإجراءات الإدارية الإلكترونية تكمن في التبادل غير المادي للبيانات بين المرافق العامة و الجمهور، هذا التبادل يتطلب عدم الإقتصار على وضع نماذج الإجراءات الإدارية على شبكة الأنترنت وإنما يجب أن يسمح بإمكانية القيام بجميع المراحل اللازمة لإنهاء الإجراء الإداري من خلال إستخدام نظم معلومات تؤدي إلى إنشاء مواقع تفاعلية تتيح للمستخدم طلب الخدمة و تلقي جواب على طلبه.[1]

بينما إتجه آخرون لتعريف الحكومة الإلكترونية من خلال المدول الجامع لها والإدارة ، حيث ذهب أنصار هذا الإتجاه إلى أن مفهوم الحكومة الإلكترونية يجب أن يراعى فيها:

– تحول أعمال القطاع العام إلى الإدارة الإلكترونية خصوصا وأن التجارة الإلكترونية كانت الأصل الذي تفرعت منه الحكومة الإلكترونية.

– أن يستوعب الخدمات التقليدية للحكومة بصرف النظر عن السلطة التي تقدمها سواء كانت السلطة التشريعية أو التنفيذية أو القضائية.

وفي هذا الإتجاه تعرّف الحكومة الإلكترونية بأنها قدرة القطاعات الحكومية على تبادل المعلومات وتقديم الخدمات فيما بينها وبين المواطنين وبين قطاعات الأعمال بسرعة ودقة عالية،

[1] – عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، الكتاب الأول، دار الفكر الجامعي، الإسكندرية، 2004، ص 07-08.

وبأقل تكلفة عبر شبكة الأنترنت أو وسائل الإتصال الأخرى مع ضمان سرية وأمن المعلومات المتناقلة في أي وقت أو أي مكان[1].

أخيرا يمكننا القول أن الحكومة الإلكترونية هي أداة لتطبيق نظام المعلوماتية المرتبطة بتكنولوجيا الحديثة في أعمال الحكومة لتحقيق أهدافها في تلبية احتياجات الأفراد وجعل الدولة أكثر تفاعلا مع مواطنيها دون أن تجعلهم يتكبدون مشقة الذهاب بأنفسهم للإدارات الحكومية[2].

و من منطلق أن الوسائل الإلكترونية فرضت على الأفراد والإدارات مواكبة علوم العصر وتقنياته بحيث لم يعد مقبولا التخلف عن ركب المعرفة التكنولوجية وهو أمر يبين أثر الإدارة العامة الإلكترونية في التطابق مع مبدأ التغير فمن حق الإدارات القائمة على سير المرافق العامة أن تطلب من أشخاص القانون الخاص المتعاقد معها لأداء عمل حكومي لها، أن تستخدم أحدث الوسائل العلمية والإبتكارات التكنولوجية في تطوير خدمة المرافق وإلا أنهت عقودها بإدارة منفردة.

لهذا أطلق في فرنسا عليها اللامركزية الفنية كونها الأكثر تجاوبا مع متطلبات مشروع نظام الحكومة الإلكترونية من خلال إنشاء هيئات متخصصة خاضعة لمجلس الوزراء و من خلالها سيسمح بتحويل إدارة المرفق العام من النظام التقليدي إلى الإلكتروني بصرف النظر عن طريقة الإدارة سواء أكانت مباشرة او غير مباشرة .

و إذا ما رأينا الواقع في الجزائر إلاّ و نجد أن الحكومة الإلكترونية بدأت ملامحها تظهر للعيان إنطلاقا من برنامج الجزائر الإلكترونية 2013 الذي كان مشروعا الذي بدأ يتجسد من خلال عصرنة الإدارة في قطاعاتها المختلفة تماشيا مع التوصيات و التأكيدات التي نادى بها

[1] وسيلة واعر ، دور الحكومة الإلكترونية في تحسين جودة الخدمات الحكومية حالة وزارة الداخلية و الجماعات المحلية – الجزائر- ، مداخلة ألقيت بالملتقى الدولي حول الجودة الشاملة بقطاع الخدمات بكلية العلوم الإقتصادية و علوم التسيير ، جامعة منتوري ، قسنطينة.

[2] محمد حسين النيلي، العلاقة بين القانون والحكومة الإلكترونية، ورقة عمل قدمت لمؤتمر الكويت حول الحكومة الإلكترونية في الفترة 13-15 أكتوبر 2003. ص 25-30.

السيد رئيس الجمهورية على ضرورة النهوض و الإرتقاء إلى مجتمع بلا أوراق و عالم الإقتصاد الرقمي من خلال خطوات رئيسية للوصول إلى الهدف المنشود المتمثل أساسا في المواطن الإلكتروني و ذلك عن طريق تطوير الأجهزة الإدارية و سن القوانين اللازمة التي تسمح بالوصول إلى تبسيط الإجراءات و العدالة الإلكترونية ، التربية و التعليم ، التعليم العالي ، الصحة ،...الخ ، من أجل ربط الإدارة بالمواطن و كذا المؤسسات.

و في هذا السياق نجد أن الحكومة تسعى جاهدة في تنفيذ برنامج السيد رئيس الجمهورية من خلال العمل على عصرنة كل القطاعات الإدارية و تحديث منظومتها المعلوماتية وتطويرها ، مع تكوين العنصر البشري لإعداده من أجل التعامل الجيد ذو النوعية المطلوبة في ذلك و في اطار ذلك قامت وزارة العدل بتطوير شبكة المعلومات لديها تماشيا مع متطلبات العصر و خدمة للمواطن[1] ، و هذا ما سنشرحه وفق ما يلي :

- **الشبكة القطاعية لوزارة العدل**

تشكل الشبكة القطاعية لوزارة العدل قاعدة مادية ضرورية للتوسع في التطبيقات المعلوماتية التي تجري تنميتها .الهدف منها تزويد قطاع العدالة بوسيلة مؤمنة لضمان تسيير آلي عن طريق إستخدام تطبيقات الإعلام الآلي كذلك توفير أساليب جديدة لتداول المعلومات والاتصالات والتبادل الفوري للمعطيات عبر مختلف مصالح العدالة، مع التمكين من الإطلاع على قواعد البيانات المنشأة من طرف قطاع العدالة والقضاء على العزلة لبعض الجهات القضائية والمؤسسات النائية عن طريق:

Visio *conference* المحاضرات عن بعد

-***Reunions à distance*** الاجتماعات عن بعد

-**Audition de détenus à distance** سماع واستجواب المحبوسين عن بعد

[1] إصلاح العدالة الحصيلة والآفاق، وزارة العدل، فيفري 2005 ، موقع الواب لوزارة العدل ، ص 34

Télé- formation-التكوين عن بعد

يتكون النظام من:

–ربط الشبكات فيما بينها.

–مركز معلوماتي يتكون من مجموعة من الملقمات للقيام بتسيير وإدارة الشبكة القطاعية وإيواء قواعد بيان قطاع العدالة.

- **المشاريع المسطرة في المخطط الخاص بعصرنة قطاع العدالة**

*** الخريطة القضائية الجديدة : la nouvelle carte judiciaire**

الشبكات المحلية في كل المستويات المجالس القضائية (المحاكم المديريات العامة لوزارة العدل مقر وزارة العدل) ، فيهتم هذا المشروع أساسا بإنجاز أداة تساعد على اتخاذ قرار إعداد خريطة قضائية جديدة وتسيير تطوراتها ، كما يطمح إلى إضفاء عقلانية أكثر على سياسة إنشاء جهات قضائية جديدة، تكوين وتعيين القضاة . هذا البرنامج بدء العمل به في شهر **جويلية 2004** و هو متواصل لإتمام إنجازه بالتعاون مع اللجنة الأوربية .

*** تسيير أوامر القبض : la gestion des mandats d'arrêt**

يرمي هذا المشروع الذي يتم مع الاشتراك مع الشرطة القضائية إلى تسهيل تسيير الأوامر بالقبض على مستوى الجهات الفضائية وضمن آفاق أفضل لضمان الحريات الفردية.

*** ترقيم الأرشيف القضائي : la numérisation des archives judiciaires**

يهدف هذا المشروع إلى تحسين ظروف حفظ الأرشيف القضائي وتسييره، من خلال الاستعانة بالأدوات الحديثة التي تضمن في نفس الوقت حماية أكبر ضد تلف وضياع الوثائق، وكذا جعل عمليات البحث والاسترجاع تتم بسرعة وفعالية[1].

علاوة على هذا الطرح الغالب اليوم المتمثل في مسايرة الالتزامات القانونية في مجال المحافظة على الأرشيف، ستتمكن مصلحة الأرشيف القضائي من أداء خدمتها العمومية على أحسن وجه بالدرجة الأولى إتجاه المواطن الذي يساعده في الحصول على وثيقة أو استكمال ملف قضائي.

[1] - إصلاح العدالة الحصيلة والآفاق، وزارة العدل، فيفري 2005 ، موقع الواب لوزارة العدل ، ص 34

هذه العملية تتسم بآثار آنية لكنها تبقى تشكل مسعى أساسيا للمحافظة على الذاكرة الوطنية.

*** إنشاء جدول وطني للهوية**

إنها عملية طويلة المدى تستدعي مشاركة وزارة الداخلية، تمر أولا بمرحلة ترقيم سجلات الحالة المدنية ووضع برنامج تسيير آلي.

هذه العملية تؤدي في الأجل القريب إلى إنشاء جهاز وطني للتعريف، وتنتهي بإنشاء جدول وطني للهوية .وستكون لها آثار إيجابية على الحياة الإدارية اليومية وذلك بتسهيلها الحصول على بعض الوثائق مراقبتها مثل :شهادة الجنسية، بطاقة التعريف الوطنية وجواز السفر.

و تماشيا مع ما سبق ذكره قد قامت الجزائر بإعداد ترسانة من القوانين كي تضمن توافق المنظومة التشريعية مع التحولات القائمة في هذا المجال ، إنطلاقا من تعديل قانون العقوبات بإدراج القسم السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم (15/04)المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات ، و الذي عزز بالقانون رقم (04/09) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، كما تم إصدار القانون رقم (03/15) الصادر في 01 فبراير 2015 و المتعلق بعصرنة العدالة ، كما أنه في نفس اليوم و السنة أي في 01 فبراير 2015 تم إصدار القانون (04/15) المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين ، و في 23 يوليو 2015 صدر الأمر رقم (02/15) المتضمن تعديل و تتميم قانون الإجراءات الجزائية و صدور إستدراك له في 29 يوليو 2015.[1]

[1] - إصلاح العدالة الحصيلة والآفاق، وزارة العدل، فيفري 2005 ، موقع الواب لوزارة العدل ، ص 34

المبحث الثاني: إنعكاس إستقلالية جرائم الإعتداء على النظام المعلوماتي على النصوص التشريعية التقليدية

على ضوء ما سبق و بعد أن توضحت لنا إستقلالية تلك الجرائم و تفردها عن غيرها من الجرائم نتجه الآن لتوضيح إنعكاس تلك الإستقلالية على النصوص التشريعية التقليدية إنطلاقا من المبدأ الأساسي الذي يقوم عليه القانون الجنائي و هو مبدأ الشرعية الجنائية في الشقين التجريمي و العقابي فلا يجوز القول عن أي سلوك أنه مجرم ما لم ينص المشرع الجنائي على تلك الصفة بنص صريح واضح يزيل اللبس و الغموض حيث أن تزايد مظاهر الإعتداء على نظم المعلومات و ما تحتويه من معلومات جعل القانون الجنائي يشوبه الثغرات و هو ما أطلق عليه بأزمة مبدأ الشرعية في نطاق جرائم الإعتداء على نظم المعلومات و هو ما سنتطرق إليه في المطلب الأول من هذا المبحث بينما نخصص المطلب الثاني منه لمدى عجز المواجهة الجنائية التقليدية ضد الإعتداءات على النظام المعلوماتي .

المطلب الأول : مبدأ الشرعية الجنائية و أزمته في جرائم الإعتداء على النظام المعلوماتي

لا تختلف جرائم الإعتداء على النظام المعلوماتي عن أية جريمة أخرى تقليدية مقررة عن طريق قانون العقوبات من حيث أنها تتطلب لتحقيقها الأركان المتفق على ضرورة تحقيقها في أية جريمة أخرى للتواجد على أرض الواقع ، فبالإضافة إلى ضرورة تواجد الشرط المبدئي في كل جريمة ونقصد هنا الركن الشرعي ، فإنه لابد من وجود ركن مادي ملموس يعبر عن ارادة الفاعل بشكل جلي يمكن اثباته ، ومن ثم لابد أيضا من ركن معنوي يعبر عن ارادة مجرم تقنية المعلومات الحديثة ، فالجريمة بشكل عام ، ليست ظاهرة مادية خالصة ، قوامها الفعل وأثاره ، ولكنها كذلك كيان نفسي ، ومن ثم استقر في القانون الجنائي الحديث ذلك المبدأ الذي يقضي بأن ماديات الجريمة

تنشئ مسؤولية ولا تستوجب عقاب ، ما لم تتوافر إلى جانبها العناصر النفسية التي يتطلبها كيان الجريمة.

وبلا شك ، فإن هذا المنطق يسري أيضا على الجرائم محل الدراسة ، بمعنى أنها لا تختلف عن أية جريمة يحتويها القانون العقابي ، فلابد و أن ترتكب من شخص قادر على تحمل تبعات أعماله ، فلا يسأل عن هذه الجريمة من لا يعترف لهم قانون العقوبات بهذه الصفة كالمجنون والمعتوه أو المصاب بمرض عقلي.

فالفقه يرى بأن الركن الشرعي لا يعدو كونه علاقة تربط بين ماديات الجريمة ، وشخصية الجاني ، وهذه العلاقة تتمثل في سيطرة الجاني على الفعل وآثاره ، وجوهرها الإرادة ، ومن ثم كانت ذات طبيعة نفسية [1]، ولاشك أن هناك تقسيم للجرائم بشكل عام يستند على أساس الركن المعنوي فتقسم إلى جرائم عمدية وأخرى غير عمدية ، ويعتمد هذا التقسيم على أن الفاعل في الجرائم العمدية قد قام بإقتراف فعله قاصدا ارتكاب السلوك المجرم وتحقيق النتيجة المجرمة ، بينما نجد أن الفاعل في الجريمة غير العمدية لم يقصد سوى ارتكاب السلوك دون ارادة تحقيق النتيجة المجرمة عن طريق النص الجزائي ، وإذا كان من المتصور غالبا أن لا تقع جريمة التقنية الحديثة إلا بصورة جريمة عمدية سبقها التفكير في الحصول على المعلومة أو اختراق شبكة نظام حاسب آخر من أجل الحصول على المنفعة أو تحقيق الهدف المرسوم له ، إلا أن هذا لا يعني أنها لا تحقق إلا عن طريق عمدي ، بل أنه من الممكن أيضا أن نتصور امكانية ارتكابها أيضا بشكل جريمة غير عمدية في بعض الأحوال المحتملة الحدوث.

[1] – محمود نجيب حسني ، النظرية العامة للقصد الجنائي (دراسة تأصيلية مقارنة في الجرائم العمدية) ، الطبعة الثالثة 1988 ، دار النهضة العربية ، القاهرة، ص 08.

وكون الجريمة عمدية هو الأصل إلا ما استثنى المشرع بنص على أنها غير عمدية ، فقد استقر في غالبية قوانين الجزاء تلك القاعدة التي تقضي بأنه إذا سكت الشارع عن بيان صورة الركن المعنوي في جريمة من الجرائم ، كان معنى ذلك أنه يتطلب القصد الجنائي العمدي فيها.

أما الركن المادي للجريمة فيعرف بأنه يتمثل في سلوك اجرامي معين يتطلب القانون كمناط للعقاب على هذه الجريمة ، على أن تحقق نتيجة ضارة لهذا السلوك الإجرامي كشرط بذاته يتعين قيامه حتى يعاقب على الجريمة ، وفضلا عن ذلك يجب أن يرتبط النشاط أو السلوك الإجرامي ونتيجته الضارة بعلاقة سببية ، وهو ما يطلق عليه "الإسناد المادي"[1]،وعليه فالركن المادي في الجريمة التامة يقوم على ثلاثة عناصر هي السلوك الاجرامي الذي يقع من الجاني ، والنتيجة الضارة أو الخطورة المترتبة على هذا السلوك سواء كان مقصود أم لا ، وأخيرا علاقة السببية بين سلوك الجاني والنتيجة التي تحققت.[2]

ويقصد بالسلوك الاجرامي (النشاط الخارجي الذي يقوم به الجاني ، ويبرز في العالم الخارجي مكونا لماديات الجريمة ومسببا لما قد يترتب عليها من ضرر أو خطر ، وسواء قصد الجاني من هذا السلوك الإجرامي تحقيق نتيجة معينة أم تحققت النتيجة دون أن تنصرف ارادته إليها"[3]. أي أن السلوك الإجرامي لابد أن يخرج الجريمة من كونها مجرد فكرة تجيش في نفس الجاني إلى فعل يظهر أثره في العالم الخارجي ويدركه الغير بإستخدام حواس الإدراك.

ويحدد السلوك الإجرامي في كل جريمة من قبل المشرع ضيقا واتساعا على نحو يمكن القاضي من تكييف السلوك الإجرامي أو فعل الجريمة ورده إلى القاعدة القانونية أو النص التجريمي

[1] – رؤوف عبيد ، مبادئ القسم العام من التشريع العقابي، طبعة ثالثة ، 1966 ،دار الفكر العربي ،ص 188.

[2] – يرى البعض أن عناصر الركن المادي هي اثنين فقط ، أولهما تطابق السلوك الإجرامي في النموذج المنصوص عليه قانونا ، والثاني عدم اقتران سلوك بظرف مباح.

[3] – أحمد عبد العزيز الألفي ، شرح قانون العقوبات (القسم العام) ، مكتبة النصر الزقازيق ،1995 ، ص 256.

الذي يحكمه[1]، معنى ذلك أنه للعقاب على الجريمة لابد أن يتطابق السلوك الإجرامي للجاني مع ذات النموذج الإجرامي الوارد في قاعدة قانون العقوبات على نحو من الدقة والوضوح ، بحيث لا يدع مجالا لإختلاف الرأي في مضمونه.

وبالكلام عن طبيعة السلوك الإجرامي في جريمة الإعتداء على النظام المعلوماتي ، فإن هذا السلوك يرتكب عن طريق إستخدام الأساليب الفنية ، و هو الأمر الذي إقتضي تدخل القانون الجنائي لمواجهتها ، لسد الفراغ او النقص التشريعي ، حيث لا يمكن أن تبقى بدون عقاب أفعال اجرامية جديدة رغم خطورتها.

ولكن حتى يتدخل المشرع فلا مناص سوى تطبيق النصوص القائمة على قانون العقوبات حتى لا تترك أفعال الإعتداء دون عقاب ، ولكن حتما دونما المساس بمبدأ الشرعية الجنائية ، بحيث تفسر النصوص القائمة على نحو أوسع من الذي وضعت لأجله ، كما من المتصور أيضا تطبيق النصوص القائمة في أية قوانين خاصة أخرى معمول بها ، الأمر الذي يبرر الحاجة للحماية الجنائية وعليه سنتعرض لمبررات الحماية من خلال التطرق لمبدأ الشرعية الجنائية الفرع الأول ، ثم ابراز قصور الجزاءات الجنائية التي تقررها التشريعات المدنية ذات الصلة الفرع الثاني .

الفرع الأول : مكونات مبدأ الشرعية .

أولا : مبدأ الشرعية الجنائية

أ – مقتضى مبدأ الشرعية الجنائية

من المبادئ الأساسية في اغلب التشريعات أنه لتشريع مظهر من مظاهر النشاط الإنساني (فعلا كان أم امتناعا)، أي لإعتبار تصرف ما بأنه جريمة معاقبا عليها ، لابد من تدخل المشرع بالنص و الذي يوضح لنا أن هذا التصرف أو ذلك المظهر أنه غير مشروع بما يفيد النهي عن فعل

[1] – في هذا المعنى : السعيد مصطفى السعيد، الأحكام العامة في قانون العقوبات، الطبعة الثانية، مكتبة النهضة المصرية، مصر، 1953، ص 50 وما بعدها.

وتقرير الجزاء لمن يخالف ذلك النهي (بالإرتكاب) أو لمن يخالف الأمر (بالإمتناع). وذلك ما يعرف بأنه مبدأ شرعية الجرائم و العقوبات أو مبدأ الشرعية الجنائية (Principe de légalité des délites et des peines) ، حيث :

- ان التجريم لا يكون إلا من قبل الشارع أي بنص قانوني صادر عن سلطة ممثلة للشعب ومختصة بالتشريع ، بيد أن استقلال المشرع بسلطة التجريم لا يمنعه من تفويض هذه السلطة في حدود معلومة للسلطة التنفيذية ، وغالبية الدساتير تجيز هذا التفويض، ويترتب على هذا المعنى أن القاضي محروم من سلطة التجريم ، وأيضا يمتنع عن القاضي الخروج عن نصوص التجريم والعقاب عند نفسيرها وتطبيقها[1] ، خلافا لما كانت عليه الحال في تشريعات العصور الماضية . كما أن الشخص يتمتع بحرية كاملة في تصرفاته فله أن يقوم بكل ما يشاء من تصرفات دون مساءلة أو متابعة من أي شخص إلا اذا قام بالتصرفات المحددة التي جرّمها القانون [2]، لذلك نلاحظ أن القوانين الجنائية ألزمت القاضي على ذكر النص القانوني الذي يطبقه على المسائل المطروحة أمامه ، كما لا يمكن له أن ينطق بعقوبة غير محددة بطبيعتها ومقدارها بنص القانون[3]، الأمر الذي يلزم القاضي بالإمتثال لنص عند النطق بالعقوبة ويبعده عن خطر خلق العقوبات.[4]

- انه يتعين على المشرع – أو من يفوض من السلطات التنفيذية – أن ينص مقدما على ما يعده من الأفعال أو التصرفات جرائم معاقبا عليها ، وأن يجهد في جعل ما يصوغه من هذه النصوص موضحا لخصائص أو مميزات كل جريمة ، فلا يكفي صدور نص التجريم فقط ، بل لابد

[1] – الأصل أن تتولى السلطة التشريعية مهمة إصدار القوانين ، غير أنه كإستثناء قد تمنح تفويض تشريعي في نطاق بعض المسائل الضيقة التي تحتاج إلى خبرة ومسائل فنية لا تملكها السلطة التشريعية ، وعليه فالنصوص التشريعية التي تعتبر مصدرا للتجريم والعقاب ، تكون صادرة عن السلطة التشريعية في الدولة حيث في الجهة الوحيدة التي تتولى ذلك كأصل عام ، كما قد تكون صادرة عن سلطة أخرى تختص بالتشريع كإستثناء وفق ما يعرف بالتفويض التشريعي ، كالقرارات الإدارية الصادرة وفقا للقوانين واللوائح ، مشار إليه لدى الدكتور محمد حماد مرهج الهيتي مرجع سابق ، ص 118.

[2] - P.Pouzat,J.Pinatel:Traité de droit criminel – Dalouz 2eme édition 1967 – p 143.No 77.

[3] - G. Stefant, G. Levasseur, B.Bouloc : Droit pénal général – Précis Dalloz 1980 – P132. N=17.

[4] - Pouzat, J.Pinatel : ouvrage précité – P 143.Numero 17.

من تحديد الجريمة تحديدا دقيقا وذكر عناصرها ماهية العقوبات المقررة لها ومقدارها أو كيفية تقديرها. وإذا ركان تدخل الشارع لازما على هذا الوجه ، فالمعنى الذي يستفاد من ذلك هو أن التجريم لا يكون إلا بنصوص مكتوبة ، وينبني على هذا أن النصوص المكتوبة هي المصدر الوحيد في تحديد الجرائم وتقرير العقوبات ، وبهذا يتميز القانون الجنائي في الكثير من فروع القانون الأخرى التي لا تقتصر مصادرها على القانون المكتوب بل قد تستمد من غير ذلك المعرفة مثلا.

- ان التجريم لا يكون إلا للمستقبل ، أي أن القوانين التي تصدر بتجريم التصرفات لا تسري على ما وقع من هذه التصرفات سابقا على تاريخ صدورها ونفاذها. وهذا مفهوم بداهة ، إذ أن العقاب على افعال أو تصرفات وقعت قبل نفاذ القانون وهو في حقيقة الأمر تجريم لها بغير قانون ما دام الغرض أنه وقت وقوعها لم يكن هناك قانون ينص على عقابها أي تجريمها. ذلك هو مقتضى قاعدة (عدم رجعية القوانين الجنائية) ، وهي في هذا المعنى ليست نتيجة فحسب لمبدأ الشرعية الجنائية بل انها أصل هذا المبدأ و مقتضاه. [1]

على أن مفهوم مبدأ الشرعية لا يتوقف على ما سلف ذكره بل يتجاوز ذلك لكي يشمل الإجراءات الجنائية التي يتطلبها القانون بالنسبة للمتابعة من يوم ارتكاب الجريمة لحين المحاكمة. لذلك يطلق الفقه على هذا مبدا (لا جريمة ولا عقوبة ولا تدابير أمن و لا إجراءات إلا بنص قانوني) ، ولكن هذه الصيغة غير لازمة لان الإجراءات مسألة مفترضة ، إذ هي تسبق دائما النطق بالعقوبة فهي مندمجة بصفة ضمنية في عنصر شرعية العقوبة.

ومن الواضح أن الغرض الاول من مبدأ الشرعية هو كفالة لحرية الأفراد في افعالهم وتصرفاتهم ، لأنه لو ترك أمر التجريم للقاضي كما كان الحال في تشريعات العصور الماضية لأضحى الأفراد في حيرة من أمرهم لا يدرون بصفة قاطعة ما هو مباح لهم وما هو محظور عليهم

[1] – عبد الله سليمان، شرح قانون العقوبات الجزائري (القسم العام) الجزء الأول الجريمة، ط6، د.م.ج، الجزائر،2005، ص 25.

فتتعطل بذلك حرياتهم ويشل نشاطهم بفعل الخوف والحذر تارة وبفعل ما يحتمل من تعسف القاضي واستبداده تارة أخرى.

و المبدأ فوق ذلك مما تقتضيه العدالة والمنطق ، اذ أن العقاب أخطر ما تملكه الدولة من الحقوق في مواجهة الأفراد لما يتهددهم من انواع الإيذاء في حرياتهم وأموالهم بل وفي أرواحهم تبعا لما تقتضيه مختلف العقوبات ، ومن ثم فإن الأمر يتطلب عدالة ومنطقا انذار الأفراد مقدما وفي صورة واضحة لا لبس فيها بما يتعرضون له إذا ما صدرت عنهم أفعال أو تصرفات معينة ، أي أن الأمر يتطلب النص مقدما على الجرائم وعقوباتها ، واخيرا فإنه مبدأ تقتضيه المصلحة العامة أو مصلحة الجماعة ، وذلك بإعتبار أن فيه ضمانا لوحدة القضاء الجنائي وعدم أو تفاوته تفاوتا يذهب بهذه الوحدة.[1]

ب – نتائج مبدأ الشرعية الجنائية

لا نزاع في ان مهمة القاضي الجنائي هي تطبيق القانون ، لأن هذا هو عمل القاضي بصفة عامة ولما كان مقتضى مبدأ شرعية الجرائم والعقوبات قصر سلطة التجريم على المشرع أو ما يفوضه من الهيئات التنفيذية أو الإدارية ، وحرمان القاضي الجنائي من تلك السلطة ، فإنه يجب على هذا الأخير أن يمتنع في تطبيقه للقانون الجنائي عن كل ما من شأنه أن يوصله إلى التجريم في صورة ما فلا ينبغي له انشاء جرائم جديدة لم ينص عليها ، أو توقيع عقوبات غير مقررة قانونا ، او الزيادة في العقوبات المقررة ، أو الحكم في جريمة لعقوبة مقررة لجريمة أخرى.

ومعنى كل ذلك أن القاضي ملزم بتطبيق القانون الجنائي كما هو ، أو كما وضعه أو أراده الشارع ، وهذا المعنى هو ما يعبر عنه بقاعدة التفسير الضيق (Interprétation étroite ou restrictive). وإذا كان مبدأ قانونية الجرائم والعقوبات يقتضي من جهة أخرى تقييد سلطة المشرع نفسه بقصر التجريم على المستقبل دون الماضي ، فلا شك في أن هذا القيد يجد صداه في عمل

[1] – المرجع نفسه، ص25.

القاضي كذلك ، فيحتم عليه الإمتناع عن تطبيق النصوص الجنائية المتضمنة للتجريم تطبيقا من شأنه أن يجعلها تسري على الماضي و عليه نستخلص نتائج هذا المبدأ و هي :

- حالة انعدام النص : اذا عرض على القاضي الجنائي أمر لا جريمة فيه ، أي لم يرد نص قانوني بتجريمه ، فإنه يتعين عليه أن يقضي بالبراءة مهما كان ذلك الأمر مستهجنا أو معيبا ، بل مهما كان فيه من اعتداء على حق فردي أو على مصلحة الجماعة.[1]

وأبرز النتائج المترتبة على ضرورة التزام التفسير الضيق تتلخص في أن القاضي الجنائي لا يملك أن يطبق القانون بطريقة القياس (raisonnement par analogie) ، كان يوقع العقوبة المقررة لفعل معين على متهم بفعل آخر مشابه ، ولكن لا عقاب عليه بنص صريح ، قياسا لهذه الحالة الأخيرة على الحالة الأولى. وهذه القاعدة هي نتيجة مباشرة لمبدأ الشرعية الجنائية ، لأن اباحة تطبيق القانون الجنائي بطريق القياس يعني تخويل القاضي الجنائي سلطة التشريع في بعض الاحوال مادام يستطيع عن طريق القياس أن يعاقب على أفعال لم يرد نص صريح بتجريمها. وفي هذا يختلف القاضي الجنائي بطبيعة الحال عن القاضي المدني الذي يستطيع أن يحكم بمقتضى قواعد العدل في حالة انعدام النص ، ويملك من باب أولى اللجوء إلى طريق القياس في تطبيقه للقانون.

واذا كان انعدام النص جزئيا ، بأن كان القانون يوجب فعلا معينا دون أن يقرر عقوبة يجازي بها من يمتنع عن أدائه ، فلا يعتبر هذا النص تجريما للفعل المذكور ومن ثم فإن القاضي لا يملك أن يحكم بعقوبة ما على من يمتنع القيام به. كذلك الشأن اذا كان القانون ينص على عقوبة دون أن يعرف الجريمة المستوجبة لها ، فلا يحق للقاضي أن يوقع هذه العقوبة حتى على من يبدوا له

[1] – وفي هذا يختلف عمل القاضي الجنائي اختلافا جوهريا من عمل القاضي المدني ، لأن هذا الاخير يملك في حالة انعدام النص أن يحكم بمقتضى (العرف) أو بمقتضى قواعد العدالة. لذا فإن غالبية القوانين المدنية تنص على أنه إذا لم يوجد نص تشريعي يمكن له أن يحكم بتطبيق العرف فإذا لم يوجد ، فبمقتضى مبادئ القانون الطبيعي وقواعد العدالة وهذا يقابل المادة الأولى من القانون المدني الجزائري مع تميز خاص لدى المشرع الجزائري أنه سبق العرف بالشريعة الإسلامية، أنظر المادة: 01 من القانون المدني الجزائري.

أنه ارتكب عملا يستأهلها ، ذلك بأن مبدأ قانونية الجرائم والعقوبات يقتضي أن التجريم لا يكون إلا بتدخل الشارع لتحديد الجريمة وعقوبتها على السواء ، فإذا نص على أحد هذين الامرين دون الآخر لا يقوم التجريم لنص أحد عنصريه ، وهو نقص لا يملك القاضي الجنائي أن يكمله لأنه لا يملك التجريم كما نقول.

- حالة وجود النص : واذا وجد النص الجنائي الذي يجرم سلوكا ، فإما أن يكون واضحا وإما أن لا يكون ، فإن كان النص واضحا ، بأن كانت عبارة مفصحة بذاتها عن غرض الشارع بغير تأويل ، التزم القاضي بتطبيقه كما هو أي وفقا لمدلوله وبغير تجاوز لما تحتمله عبارته.

وأما إذا كان النص غامضا ، فإن القاضي الجنائي مطالب بتطبيق القانون على كل حال ومن ثم فإنه يملك بل يجب عليه أن يسعى إلى تأويل النص الغامض ، أي أن يسعى إلى استجلاء حقيقة غرض الشارع ، ومن المتفق عليه من الفقهاء ، أن له في هذا السبيل أن يستعين بكل أساليب التفسير ، منطقية كانت أو لغوية أو تاريخية ، بما سبق النص أو من الأعمال التحضيرية والمذكرات التفسيرية والوثائق الرسمية ، وبمقارنة النص الغامض بالنصوص الاخرى التي لها صلة[1].غير أن قاعدة التفسير الضيق تحتم عليه في كل ذلك أن لا يذهب إلى أبعد من استخلاص غرض المشرع ، أي تحديد المعنى الصحيح للألفاظ التي ورد بها النص حسبما قصده واضع القانون ، دون أن يكون في ذلك تعارض مع النص المذكور أو تحميل لعبارته أكثر مما تحتمل. لهذا فليس من حق القاضي إنشاء الجرائم والعقوبات وأيضا يمنع القاضي من الخروج عن نصوص التجريم والعقاب عند تفسيرها وتطبيقها[2] .

[1] – علي أحمد راشد ، مبادئ القانون الجنائي ،منشأة المعارف ، ب. س. ن ، ص 232.

[2] – الأصل أن تتولى السلطة التشريعية مهمة إصدار القوانين ، غير أنه كإستثناء قد تمنح تفويض تشريعي في نطاق بعض المسائل الضيقة التي تحتاج إلى خبرة ومسائل فنية لا تملكها السلطة التشريعية ، وعليه فالنصوص التشريعية التي تعتبر مصدرا للتجريم والعقاب ، تكون صادرة عن السلطة التشريعية في الدولة حيث في الجهة الوحيدة التي تتولى ذلك كأصل عام ، كما قد تكون صادرة عن سلطة أخرى تختص بالتشريع كإستثناء وفق ما يعرف بالتفويض التشريعي ، كالقرارات الإدارية الصادرة وفقا للقوانين واللوائح .

لأن الاخذ بالقياس في نصوص التجريم من شأنه أن يؤدي إلى خلق عقوبات لم يرد بشأنها نص.[1].

وتطبيقا لذلك يجب في حالة اذا بلغ النص من الغموض على نحو يتعذر معه استخلاص حقيقة غرض المشرع بيقين ، أي في حالة ما اذا ثار بشأن النص شك جدي ، أن يمتنع القاضي عن تكملة ما يعتقد أنه ينقص النص المذكور أو عن اللجوء إلى طريق القياس ، بمعنى أن المتهم يستفيد من الشك في مثل هذا الغرض.

يتبين مما تقدم أنه مع التسليم بأن القوانين الجنائية يجب أن تخضع لقاعدة التفسير الضيق فإن الحقيقة أن هذه القاعدة يكاد يتعذر احترامها في غير حالتي انعدام النص أو وجوده واضحا لا حاجة لتفسيره ، إذ قد رأينا أنه في حالة غموض النص فمن المتفق عليه أن للقاضي الجنائي أن يعمد إلى تأويله سعيا إلى استخلاص غرض المشرع مستعينا في ذلك بوسائل شتى ، والواقع أنه يتعذر في هذه الظروف وضع ضابط دقيق لتطبيق فكرة التفسير الضيق ، اللهم إلا في حالة ما اذا بلغ النص من الغموض درجة تجعله كما لوكان عاطلا ، فعند ذلك تكون الحال أقرب في الواقع إلى حالة انعدام النص كليا أو جزئيا حيث يسهل تطبيق قاعدة التفسير الضيق في معنى مطالبة القاضي بأن يمتنع عن تطبيق نص آخر على الواقعة بطريق القياس أو عن تكملة ما يراه ناقصا في النص.

وبناء على ما تقدم لا يتصور ان يكون هناك جريمة أو عقوبة بغير قانون الذي لا يخلو أي تشريع من الحديث منه[2] ، حصر مصدر التجريم والعقاب في التشريع ، فالتشريع هو المصدر الوحيد لقانون العقوبات وبالأخص القواعد الخاصة بإنشاء الجرائم والعقوبات وأيضا يمتنع عن

[1] – محمد حماد مرهج الهيتي ،المرجع السابق، ص 118.

[2] – تنص على المبدأ معظم التشريعات العقابية ونجد تطبيقا لذلك في التشريع العقابي الجزائري ما تنص عليه المادة الأولى من قانون العقوبات " لا جريمة و لا عقوبة أو تدابير أمن بغير قانون "

القاضي الخروج عن نصوص التجريم والعقاب عند تفسيرها وعليه وبشكل عام يمكن عكس مضمون مبدأ الشرعية الجنائية فيما يلي :

- أي فعل لا يمكن اعتباره جريمة ما لم يوجد تشريع يقضي بذلك.
- الفعل الذي يقرر له التشريع عقابا يجب أن يكون منصوص عليه صراحة.

التطبيق العلمي للمبدأ يمنع على القاضي أمرين ، التفسير الواسع وإعمال القياس في نطاق نصوص التجريم.

أما بالنسبة للجرائم التي تقع نتيجة الاستخدام غير المشروع للنظام المعلوماتي ، فالأمر جديد على مسامع المشرع ، مما قد يمس من قريب أو بعيد بمبدأ الشرعية الذي اصبح ملازما للإنسانية .

و برغم امكانية تطبيق النصوص التقليدية على بعض من جرائم المعلوماتية ، إلا أننا لا نعتقد بإستطاعة القانون الجنائي في نصوصه التقليدية مواجهة جرائم الإعتداء على النظام المعلوماتي ، وذلك لأن النصوص التقليدية قد وضعت لتطبق وفق معايير معينة لا تتناسب مع العديد من صور تلك الجرائم نظرا لطبيعتها الخاصة التي تتميز بها هذه الجرائم[1]، وبالتالي فإن تطبيق النصوص التقليدية عليها من شأنه المساس بمبدأ الشرعية الجنائية ، اذا ترك الأمر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله. لذا اختلف الفقهاء ازاء تطبيق النصوص القائمة على الجرائم الناشئة في التقنية الحديثة بين مؤيد ومعارض لتطبيق تلك النصوص على جرائم الإعتداء على النظام المعلوماتي.

فكما رأينا سابقا أن ما يترتب على مبدأ الشرعية هو سد المنافذ أمام التحايل على النصوص القانونية العقابية ، والذي من شأنه أن يؤدي إلى وضع صور من أنماط السلوك المباح تحت طائلة

[1] – جميل عبد الباقي الصغير ، المرجع السابق ، ص 12.

التجريم والعقاب ، من قبل سلطة لا تمتلك هذا الحق ، حيث تنحصر مهمتها في تطبيق النصوص دون زيادة أو تكلف .[1]

فمن المستقر قانونا أن قانون العقوبات لا تسري أحكامه وقوانينه إلا على المستقبل ، فهو لا يحكم ما وقع قبل صدوره ، فعدم رجعية القانون الجنائي على الماضي تطبق على الاحكام المتعلقة بخلق الجرائم والعقوبات ، وهو مضمون المادة الثانية من قانون العقوبات الجزائري :" يسري قانون العقوبات على الماضي إلا ما كان منه أقل شدة".

إن القاضي الجنائي ملزم على ضوء مبدأ الشرعية بأن يرد واقعة الدعوى إلى نص قانوني يجرمها بما يعرف بالتكييف اذ من خلاله تمنح الواقعة المكونة للجريمة تسميتها التي منحها إياها القانون.

الفرع الثاني :أزمة مبدأ الشرعية الجنائية سبب في تجريم الإعتداءات على النظام المعلوماتي

تعتبر جرائم الإعتداء على النظام المعلوماتي من الجرائم حديثة النشأة ، لذلك اعتراها نوع من الغموض في تكييف افعال الإعتداء غير المشروعة المصاحبة لها ، لدرجة أنها أعتبرت في بادئ الأمر مجرد جرائم عادية تقنية متطورة ، تستوعبها النصوص التقليدية.

إلا أن التسليم بتطبيق النصوص التقليدية على تلك الجرائم يثير العديد من النقاط القانونية الهامة أولها أن نصوص قوانين العقوبات التقليدية وضعت في وقت لم تكن تكنولوجيا المعلومات موجودة ، وبالتالي كانت مستندة إلى مفاهيم فقهية تقليدية ، تأخذ مادية المال او

[1] – شهد مبدأ الشرعية الجنائية تطورا حيث منح للقاضي بعض المرونة من خلال سلطته التقديرية فيما يتعلق بتقدير العقوبة، النصوص القانونية تجعل للعقوبة حد أقصى وحد أدنى ليحكم القاضي بما يراه مناسبا وفقا لظروف الجريمة ، كما قد يمنح النص العقابي لكثير من الجرائم عقوبات تخييرية حيث للقاضي أن يتخير من بينها ما يعتبره أكثر ملائمة ، والملاحظة أن التخفيف من الجمود لا يمس سوى الجزء الخاص بتقدير العقوبة فقط دون الجزء الخاص بخلق الجريمة.

وسيطه المادي بعين الإعتبار لإيقاع التجريم[1]، بينما غيرت المعلوماتية بشكل كبير المفاهيم القانونية نظرا لظهور قيم حديثة ذات طبيعة خاصة ، محلها بيانات ومعطيات ذات طبيعة غير مادية.

ثانيها إختلاف المواقف الفقهية والقضائية في معالجتها لهذه الجرائم ، ففي حين وجدت اجتهادات فقهية وأحكام قضائية حاولت تفعيل القواعد العقابية الكلاسيكية ، وجعلها مرنة و متوافقة والطبيعة الخاصة للمعلوماتية ، اعتبرتها أحكام أخرى سلوكا مباحا لم يرد بشأنه نص تجريمي التزاما بمبدأ الشرعية الجنائية والذي يقضي بأن لا جريمة ولا عقوبة بغير قانون .

و من جانب آخر يصعب التسليم بتخلف القانون الجنائي عن مواكبة الاستعمال الغير مشروع للمعلوماتية في ظل عدم تنظيم أحكام تلك الجرائم ، مما قد يترتب عنه افلات الجاني من العقاب عملا بمبدأ الشرعية الجنائية ، وهو ما يدفع بشكل أو بآخر إلى تطور النصوص التقليدية التي يعرفها قانون العقوبات ، ولكن دونما المساس بإحدى المبادئ المستقرة في القانون الجنائي وهو مبدأ شرعية التجريم والعقاب ، فجهد القاضي يجب أن لا يضع النصوص الكلاسيكية خارج اطارها ، كما لن يتعدى إلى مرتبة التفسير الذي يتجاوز حدود النص وغايته ولا يصل إلى حد إعماله القياس.

مما سيق يتضح أن الحاجة إلى حماية جنائية خاصة بجرائم الإعتداء على النظام المعلوماتي ، خلقتها بالدرجة الأولى دواعي مبدأ الشرعية الجنائية ، كون تلك الجرائم نوع متفرد من الفعل الجرمي ، وهو ما برر بضرورة التدخل وإصدار نصوص قانونية مصاغة بدقة لمعالجة هذه الظاهرة الإجرانية.

[1] – فريد منعم جبور ، حماية المستهلك عبر الأنترنت ومكافحة الجرائم الإلكترونية دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت ، لبنان ، 2010 ، ص 216.

المطلب الثاني : مدى عجز المواجهة الجنائية التقليدية ضد الإعتداءات على النظام المعلوماتي

أثرت الرؤى المتعددة و المختلفة في تحديد لطبيعة القانونية للمعلومات الإلكترونية في ضمان حماية في ظل النصوص القائمة هذا من جهة و من جهة أخرى عجزت تلك النصوص في مواجهة الجرائم المستحدثة و هذا ما سنتطرق إليه وفق الفرعين التاليين :

الفرع الأول : تباين الرؤى في تحديد الطبيعة القانونية للمعلومات الإلكترونية :

إنقسم الفقه في تحديد الطبيعة القانونية للمعلومات الإلكترونية كي يمكن حمايتها ، مما إنجر عليه تأثيرا على التشريعات المتعلقة بها ، و هذا ما سنتطرق إليه وفق ما يلي :

أولا: الإتجاه التقليدي القائل بأن المعلومات ذات طبيعة خاصة :

و يرى أصحابه أن المعلومات ليس لها طبيعة مادية كونها ليست من قبيل الأشياء المحسوسة و لغياب الكيان المادي لها ، فهو لا يجعلها محلا لحق مالي من بين الحقوق المالية المتعارف عليها قانونا ، و التي ترد على الكيانات المادية ، و هو ما يستلزم إستبعادها من طائفة الأموال .

و يرتكز أصحاب هذا الإتجاه على بديهية مسلم بها ، مؤداها أن الأشياء الموصوفة بالقيم (biens أو المال) ، هي تلك الأشياء القابلة للتملك و يمكن حيازتها و الإستئثار بها ، و نضرا لكون المعلومات طبيعة معنوية فمن غير المعقول أن تكون قابلة للحيازة و الإستئثار و فقا لهذا الإتجاه إلا عن طريق حقوق الملكية (الفكرية أو الصناعية) ، مما ينتج عنه أن المعلومات التي لا تنتمي إلى المواد الفكرية أو الصناعية لا يمكن إدراجها في مجموعة القيم المحمية .[1]

و ما يجب إبداءه هنا أن هذا الإتجاه لا يستبعد الحماية القانونية للمعلومات ، فحسبه ما دام أن هناك خطأ موجود عند الإستيلاء غير المشروع على معلومات الغير فهذا مبرر و يسمح

[1] – سليم عبد الله الجبوري، المرجع السابق، ص 44.

برفع دعوى المنافسة غير المشروعة ، فطالما أن الخطأ لا يجد أساسه في الإستيلاء على معلومة الغير فهو يجد أساسه في الظروف المقترنة به و هو تحليل يستند إلى المبدأ الذي تبنته محكمة النقض الفرنسية في حكمها القاضي بأن "الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق إستئثاري"

(L'action en Concurrence Déloyale Apour Objet D'assurer La Protection De Celui Qui Ne Peut Se Prévaloir D'un Droit Privatif) .[1]

إلا أن هذه الإحالة وفق المبدأ الذي إنتهجته محكمة النقض لم يعتمد من قبل غرفة التجارة الفرنسية و ذلك لعدم توافر الشروط التقليدية لدعوى المنافسة غير المشروعة ، و هذا ما أدى لبلورة تأسيس جديد للخطأ المعترف به من بعض الفقهاء الذين أسسوه وفق التطبيق الموسع لنظرية التصرفات الطفيلية . (La Théorie Des Agissement Parasitaire) و محاولة للتوفيق بين الرأيين السابقين بإعتبارهما يتجهان لنتيجة واحدة مع إختلاف التصور (منافسة غير مشروعة و تصرف طفيلي) ، طرح الفقيه لوكاس (Lucas) فكرة إسناد الخطاء إلى نظرية الإثراء بلا سبب (La Théorie Des Enrichissement Sand Cause) بوصف الخطاء هنا تطبيقا خاصا لها.

و لأجل الوصول إلى تبرير دقيق للخطاء في هذه الحالة انتهى الفقيه ديبوا (Desbois) على الرغم من عدائه لفكرة الإقرار بوجود الحق الإستئثاري للمعلومات إلا أنه من المقبول على حدّ رأيه الإعتراف كذلك بوجود خطاء على أساس دعوى المسؤولية المدنية عقدية كانت أو تقصيرية وفقا لما نص عليه القانون المدني الفرنسي .

هذا الرأي كان أكثر واقعية في تبرير الحماية القانونية للمعلومات بوجود الخطاء على أساس المسؤولية المدنية ، الذي كان له الأثر الواضح في ظهور الإتجاه الفقهي الحديث الذي يرى بأن المعلومات في مصاف القيم .[2]

[1] – محمد سامي شوا، المرجع السابق، ص 180.

[2] – سليم عبد الله الجبوري، المرجع السابق، ص 46.

ثانيا : الإتجاه الحديث القائل بأن المعلومات مجموعة مستحدثة من القيم :

يتزعم هذا الإتجاه كلا من الفقيهين كاتالا (Catala) و فيفانت (Vivant) و لكل منهما منهجه الخاص لكن للوصول إلى نفس النتيجة . فالفقيه كاتالا يعتبر المعلومات مشتقة عن دعامتها المادية (أي الشيء الذي يحتويها) ، و بكونها قيمة قابلة للإستحواذ مستقلة عن دعامتها المادية ((Un Bien Susceptible D'appropriation و يوضح رأيه قائلا "أن المعلومة تقوم وفقا لسعر السوق متى كانت غير محظورة تجاريا و أنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه و هي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما". و هنا يستند الفقيه كاتالا في رأيه على حجتين لإضفاء وصف القيمة على المعلومة : الحجة الأولى ترتكز على القيمة الإقتصادية للمعلومة و ذلك لما إعتبرها منتوج تجاري قائم على سعر السوق متى كان غير محظور ، و الحجة الثانية متمثلة في وجود علاقة تبني تجمع بين المعلومة و بين مؤلفها .[1]

و مع صحة هاتين الحجتين إلا أنهما لا تعدان من قبيل الحجج المألوف إستعمالها لتبرير الإعتراف بقيمة من القيم العلمية أو الفكرية...الخ .

أما الفقيه فيفانت الذي يعتمد نفس الإتجاه الذي ذهب إليه الفقيه كاتالا ، إلا أنه أسس رأيه و موقفه على حجتين الأولى مستوحات من الفقيهين بلانيول و روديبير المتمثلة في "أن فكرة الشيء أو القيمة لها صورة معنوية ، و أن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع إقتصادي و أن تكون جديرة بحماية قانونية" . أما الحجة الثانية قدمها الأستاذ فيفانت نفسه الذي رأى " أن كل الأشياء المملوكة ملكية معنوية ، و التي يعترف بها القانون ، و ترتكز على الإعتراف بأن للمعلومة قيمة ، عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو التحصيلات الضرورية أو حق المؤلف و الإنسان الذي يقدم و يكتشف و يطلع الجماعة على

[1] – سليم عبد الله الجبوري، المرجع السابق، ص 46.

شيء ما بصرف النظر عن الشكل أو الفكرة ، فهو يقدم لهم معلومة بالمعنى الواسع و لكنها خاصة به ، و يجب أن تعامل هذه الأخيرة بوصفها قيمة تصبح محلا لحق ، فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية". و لذلك فهو يرى أن القيمة المعلوماتية ليست بالشيء المستحدث إذ أنها موجودة من قبل في مجموعة ما .[1]

و عليه مما تقدم تعتبر المعلومات مالا قابلا للتملك أو الإستغلال و ذلك على أساس قيمته الإقتصادية و ليس على كيانه المادي و بذلك و لأجله فهي تستحق حمايتها القانونية . و تتمثل أهمية هذا الوصف أن المعلومات تدخل في عداد الأموال التي يحميها القانون الجنائي من الإعتداء عليها .

و نجد أن المشرع الجزائري قد أدرج في تعديله لقانون العقوبات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 و ذلك من خلال إدراجه للقسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات(من المادة 394 مكرر إلى المادة 394 مكرر 7) تحت الفصل الثالث المعنون ب "الجنايات و الجنح ضد الأموال" ، و هذا دلالة على أن المشرع الجزائري تفادى النقاش الفقهي الدائر حول الطبيعة القانونية للمعلومات و فصل في أمرها مباشرة لما أدرجها تحت الفصل الثالث السابق الذكر و من هنا سهل الأمر على الجهات القضائية و الباحثين متفاديا بذلك إيقاعهم في اللبس و الغموض حول موقفه من تكييف و تحديد طبيعة المعلومات الإلكترونية ، و من هنا نخلص أن المشرع أنه فصل في الأمر تسهيلا لعمل الجهات المختصة غالقا لباب التأويل .

[1] - سليم عبد الله الجبوري، المرجع السابق، ص 47.

الفرع الثاني : إعتبار البرنامج المعلوماتي حق من حقوق المؤلف

لا شك أن أولى بوادر الإهتمام بالحماية القانونية للمعلوماتية في بادئ الامر في محاولة لسد الفراغ كان في قوانين ذات طبيعة غير جنائية ، عن طريق يالاستعانة بالقواعد المتوفرة التي تراعي طبيعتها كمصنف معلوماتي قوانين حماية حقوق المؤلف.

وتظهر العلاقة بين حماية المعلوماتية عن طريق قوانين حقوق المؤلف ، في كون النظام المعلوماتي ما هو إلا ابتكار جديد لإحدى تطبيقات برامج الحاسب الآلي ومعطياته وبياناته واعتباره من قبيل المصنفات الفكرية.[1]

أولا : فكرة عامة عن الملكية الأدبية و الفنية

تعتبر الملكية الأدبية والفنية الصورة الثالثة من صور الملكية الفكرية، وبالرغم من اعتبار البعض أن تعبير الملكية الفكرية يشتمل على نوعين من الملكية الفكرية هما: الملكية الصناعية والملكية الأدبية والفنية، وإدخال ما يتعلق بالملكية التجارية ضمن الملكية الصناعية .

إلا أن الواقع أن هناك استغلال نسبي و لو أن هناك حقيقة صعوبة في الفصل لكل من الملكية الصناعية عن الملكية التجارية وكذلك الشأن بالنسبة للملكية الأدبية و الفنية[2] .

وتشمل الملكية الأدبية و الفنية القصص و الكتابات العملية و غيرها ، و النصوص المسرحية والأفلام والتأليف الموسيقي والرسوم وأعمال النحت والنجارة وما أشبه ذلك، ويستخدم اصطلاح حق المؤلف للدلالة على الملكية الأدبية والفنية ، حيث جاءت تحت طائلة حق المؤلف لتجعل له نطاق واسع يشمل كل المفردات والابتكارات الذهنية والفكرية التي تشكل كل واحدة

[1] – محمد حماد مرهج الهيتي، المرجع السابق، ص 122.

[2] – نواف كنعان، حق المؤلف ، النماذج المعاصرة لحق المؤلف ووسائل حمايته ، الطبعة الثالثة 2000 ، ص.47 وما بعدها

منها مصفا فكريا يمنح الحماية المقررة للمصنفات الفكرية وفقا لما جاء في ظل الاتفاقات الدولية والقوانين الداخلية لحماية حق المؤلف[1] .

وتعد اتفاقية "برن" بشأن المصنفات الأدبية و الفنية من أهم المعاهدات التي خضعت لعدة تطورات و تعديلات نظرا للتطورات التي شهدتها الحياة الاجتماعية و التكنولوجيا ، حيث ظهرت إبداعات و إختراعات الى حيز الوجود لم تكن تخطر ببال أهله أنفسهم.

و أوجبت عدة حقوق من شانها الانسجام مع الأعمال الجديدة التي تستوجب الحياة وتوفير النصوص التشريعية الجديدة أو الإضافية أو المعادلة في طل هاته التغيرات الإقتصادية والإجتماعية والسياسية التي شهدها النصف الاخير من هذا القرن.

و بالرغم من ان اتفاقية "برن" تمت على أساس التصور أو المفهوم أو النظام اللاتيني بدلا من النظام الأنجلوسكسوني لحق الاستنساخ ، إلا أنها مع ذلك تعتبر حجر أساس في إرسال اللبنة الأساسية لبناء الاتفاقية العالمية لحق المؤلف و التي شملت من بين ما نصت على حماية برامج الحاسب الآلي وفق شروط ومعايير سيتم التطرق إليها لاحقا ، كما أنه يرجع لاتفاقية "برن" بشأن حماية الصفقات الأدبية والفنية ، الفضل الأكبر في إرساء عددا من المبادئ الخاصة لصالح البلدان النامية –والتي ستأخذها اتفاقات لاحقة بالحسبان– لردم الهوة بين الدول المتقدمة والنامية ،

[1] – محمد حماد مرهج الهيتي، المرجع السابق، ص 123.

وكذا مراعاة ظروف هاته البلدان ووضعها الاقتصادي[1] .

وقد جاءت الإتفاقية العالمية لحقوق المؤلف لتعزز الجهود الدولية المبذولة في ميدان حماية مفردات الملكية الأدبية و الفنية ، و كذا مواكبة التطور على أرض الواقع من حيث نوعية النشاط الإبتكاري و حدوده ، لذا وجدنا و لعل في هاته إشارة واضحة على إلتزام المجتمع الدولي بمواكبة التطورات التي تعرفها الحياة الإقتصادية الدولية ، و إدخال كل ما هو جديد ضمن سلسلة الإهتمامات التي تبذلها المنظمات الإقتصادية و الجهات المعنية بمواكبة هاته التطورات في مختلف الإتجاهات و في شتى الميادين .

و يعتبر التطور الهيكلي الذي عرفته الإتحادات الدولية ، و بناء و إنشاء المنظمات الإقتصادية و خصوصا منها المعنية بحقوق الملكية الفكرية ، دلالة واضحة على حقيقة الإهتمامات التي يبذلها المجتمع الدولي على أرض الواقع.

من خلال ما سبق ، نكون قد ألقينا نظرة سريعة على مفردات الملكية الفكرية و ذلك نظرا للعلاقة التي تربط هاته الأخيرة ببرامج الحاسب الآلي ، حيث أنه في ميدان حماية برامج الحاسب

[1] – إتفاقية برن بشأن حماية المصنفات الأدبية و الفنية : Bern Convention for the Protection of Literary and Artistic Works، تعد أول الإتفاقات الدولية المتعلقة بحق المؤلف ، حيث و قعت في سبتمبر 1886 م، و يشار إليها بإتحاد "برن" أو إتحاد حق المؤلف ، و قد جرى تنقيحها عدة مرات، و تستند الإتفاقية إلى ثلاثة مبادئ أساسية ، و تشمل مجموعة من الأحكام المتعلقة بالحد الأدنى للحماية و كذلك بعض الأحكام الخاصة التي وضعت لصالح البلدان النامية، و المبادئ الأساسية التي إستنفذت إليها هاته الإتفاقية.

أ – مبادئ المعاملة بالمثل أو معاملة الأجانب معاملة الوطنيين : (National Treatment or Assimilation)

و هذه المساواة تعني أن المصنفات التي تكون بلدها الأصلي إحدى الدول الأعضاء (سواء كان مؤلف المصنف أو صاحبه من مواطني هذه الدولة ، أو التي يكون المصنف قد نشر للمرة الأولى بها) يجب أن تحظى هذه المصنفات في كل من الدول الأعضاء الأخرى بنفس الحماية التي تمنحها لمصنفات رعاياها.

ب– تلقائية الحماية : (Automatic Protection) و يعني ذلك عدم تعليق الحماية على إجراءات محددة (أي ألا تكون مشروطة).

ج– استقلالية الحماية : (Independence Protection) بمعنى أن تكون هذه الحماية مستقلة من سريان الحماية في البلد الأصلي للمصنف ، و مع ذلك فإنه يجوز رفض الحماية حين توقفها في البلد الأصلي إذا ما نص تشريع بلد ما على مدة حماية أطول من الحد الأدنى المنصوص عليه في الاتفاقية ، وإذا ما توقفت حماية الصنف من البلد الأصلي (الذي تم فيه التسجيل لأول مرة) ينظر في هذا ، محمد حسام محمود لطفي ، الشروط الجوهرية لحماية حق المؤلف ، موسوعة الفكر القانوني ، الجزء الثالث ، الجزائر ، 1993 ، ص 212 و ما بعدها .

الآلي سوف نعود بالنظر إلى موقع هاته البرامج داخل مفردات الملكية الصناعية ، و علاقتها ببراءات الإختراع ، و كذلك موقعها من مفردات الملكية الفنية و الأدبية (حقوق المؤلف) ، حيث نجد أن هناك ازدواجية في الحماية من خلال الاتفاقات الدولية التي سنطرق لها في هذا الميدان ، الشيء الذي أفرز معه ازدواجية في المعايير التي ترتئيها المنظمات الإقتصادية في ميدان حماية البرامج على ما سوف نرى لاحقا.

ثانيا : إعتماد برامج الحاسوب كمصنف محل حماية فكرية:

تعتبر برامج الحاسوب ابداعات فكرية ذات طبيعة تقنية[1]، هذه الطبيعة المزدوجة هي ما جعلت المشرع في العديد من الدول يستند إلى قانون حماية حق المؤلف كسبيل لحماية برامج الحاسب الآلي.[2]

ويقصد بحق المؤلف ، حقه في حماية القانون لإبتكاره الذهني ، بحيث يستطيع استعمال حقه هذا في مصنفه والاستئثار به واستغلاله كما هو مخول له بمقتضى القانون ، والوقوف في وجه كل معتد عليه ، بإلزام الغير بإحترام حقه.[3]

وعلى غرار التشريعات التي نصت على شمول برامج الحاسب الآلي بالحماية القانونية التي تقررها قوانين حماية حق المؤلف ، أدمج المشرع الجزائري برنامج الإعلام الآلي ضمن المصنفات الأصلية بموجب الأمر رقم 10/97 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة.[4]وكذا بموجب الأمر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق

[1] – خثير مسعود ، المرجع السابق ، ص 80.

[2] – برامج الحاسب الآلي هي عبارة عن تعليمات مثبتة على دعامة ، يمكن قراءتها لأداء واجب معين عن طريق نظام معالجة هذه المعلومات وقراءتها بواسطة الحاسب الآلي.

[3] – عبد الله بن محمد النجار ، الحماية المقررة لحقوق المؤلفين الأدبية ، دار النهضة العربية ، القاهرة ، 1990، ص 141.

[4] – نص المادة 04 من الأمر 10/07 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة على أنه :" تعتبر على الخصوص كمؤلفات فيه أو فنية محمية ما يأتي ، المصنفات الأدبية المكتوبة مثل المحاولات الادبية والبحوث العلمية التقنية والروايات والقصص والقصائد الشعرية ومصنفات و قواعد بيانات" .

2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة ، حيث نصت المادة الرابعة منه الفقرة أ على أن : "تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي :

أ –المصنفات الأدبية المكتوبة مثل : المحاولات الأدبية والبحوث العلمية والتقنية ، والروايات والقصص والقصائد الشعرية و برامج الحاسوب و المصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي تماثلها".

ب –وعلى إثر النص السابق يدخل البرنامج ضمن نطاق الحماية التي توفرها النصوص للمؤلفات ، فبات الاعتداء على برامج الحاسب الآلي بمثابة الإعتداء على مصنف أو مؤلف ، ومنه وبشكل طردي يعتبر الموقع الإلكتروني من المصنفات المحمية بموجب قانون حماية المؤلف.

ثالثا : مدى ملاءمة الجزاءات لحماية البرامج في قانون حماية المؤلف

على ضوء نصوص قانون حماية حق المؤلف ، فلهذا الاخير حقه الخالص على المصنف ، يمكنه استعماله واستغلاله والتصرف فيه وقتما يشاء وكيفما يشاء دون اعتداء أو تعرض من أحد.

أ) فلصاحب هذه المصنفات الحق في نسب المصنف إليه ووضع اسمه على مصنفه ، أو وضع اسم مستعار وله الحق في أن يقرر هل سينشر مصنفه أم لا ، ومتى وكيف سينشر المصنف وله الحق في تعديل مصنفه متى رأى الحاجة في ذلك ، وبناء على حقه في نشر مصنفه فيمكنه كذلك سحب المصنف من التداول إن كان في ذلك مصلحة له. ومن أهم الحقوق المخول للمؤلف حقه في دفع الاعتداء على المصنف واتخاذ الإجراءات التي وضعها القانون لحماية مصنفه.[1]

تبعا لذلك وبوصف النظام المعلوماتي أحد عناصره برامج الحاسب الآلي ، وبإدارج البرامج المعلوماتية ضمن المصنفات المحمية ، فلصاحب النظام المعلوماتي كامل الحق في تقرير نشر وتحميل وتخزين المعلومات على الحاسوب ، كما له الحق في نسبتها إليه ، والحق في دفع أي اعتداء قد يقع

[1] – أمجد حسان ، الفيروسات ارهابا يهدد انظمة المعلومات ، ملتقى الإرهاب في العصر الرقمي ، جامعة الحسين بن طلال ، 10–12 جويلية 2008 ، عمان ، ص 199.

عليها ، وله كذلك الحق في سحبها وشطبها من التداول عبر الحاسوب وعبر شبكة الأنترنت ، أو منح الآخرين رخصا بإستعمالها أو استغلالها.[1]

إلا أن الحماية التي يعطيها القانون المتقدم لبرامج الحاسب بإعتبارها كبقية المصنفات التي يحميها ، لم تسلم من أن ينسب إليها الفقه بعضا من مظاهر القصور :

– فطبيعة المؤلف تختلف عن طبيعة البرامج المعلوماتية ، الأمر الذي يستوجب التمييز بينها لا المساواة. من جانب آخر جرائم الإعتداء على حق المؤلف تختلف عن جرائم الإعتداء على برامج الحاسب الآلي كون الجرائم الأخيرة تفضي إلى خسائر أكثر بكثير من الخسائر الناجمة عن جرائم الاعتداء على حق المؤلف.[2]

– كما أن خوارزميات برنامج الحاسوب وأفكاره لا تتمتع بالحماية القانونية بمقتضى قانون حق المؤلف بإعتبارها ملكا عاما ، يمكن للجميع استعمالها واستخدامها ولو بدون ترخيص من مؤلفها حيث يمكن إعادة استخدام الخوارزم ذاته في عدد لا محدود من البرامج.[3] فالخوارزميات على أساس أنها مجرد اجراءات منطقية تأخذ حكم الفكرة التي تخرج بطبيعتها عن نطاق الحماية التشريعية.

– اضافة إلى ما سبق وبشكل عام فإن النصوص التي يتضمنها قانون حماية المؤلف ، لا تحمي البرامج المعلوماتية بإعتبارها من المصنفات إلا من صور الاعتداءات التي تشكل اعتداء على حق المؤلف دون الإعتداءات الأخرى التي قد تتعرض لها البرامج المعلوماتية.

– واذا كان القانون المتقدم قد منح الحماية المدنية لأصحاب الحقوق ، من خلال التعويض المدني عن أي صورة من صور الاعتداء على حق المؤلف الأدبي او المالي[4] فمتى أثبت المؤلف وقوع

[1] – خثير مسعود ، المرجع السابق ، ص 81 .

[2] – محمد حماد مرهج الهيتي : مرجع سابق ، ص 122.

[3] – خثير مسعود ، المرجع السابق ، ص 82.

[4] – تنص المادة 142 من الامر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة على أنه:" تكون الدعوى القضائية لتعويض الضرر الناتج عن الإستغلال الغير مرخص به لمصنف المؤلف والآداء لمالك الحقوق المجاورة من اختصاص القضاء المدني".

الاعتداء فيمكن الحكم له بالتعويض المناسب والعادل ، فإن هذه الحماية المدنية غير كاقية لوحدها لردع المعتدين فلابد أن تقرن المسؤولية الجزائية. وأكثر الأوصاف قربا من هذه الإعتداءات هي جريمة التقليد ، والتي تعرف بأنها " كل اعتداء مباشر أو غير مباشر على حقوق المؤلف في المصنفات الواجبة حمايتها أيا كانت طريقة الاعتداء أو صورته.[1]

ومادام المشرع الجزائري قد أدمج برامج الحاسب الآلي ضمن قائمة المصنفات المحمية عن طريق القانون المتعلق بحماية المؤلف ، فإن أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج يشكل فعلا من أفعال التقليد،[2] وهو ما تضمنه نص المادة 151 من الأمر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة.[3]

وعليه فالإستعمال غير المشروع للبرنامج المعلوماتي يشكل اعتداء تتبعه المسؤولية القانونية ، فكل من يقوم بإستيراد مصنفات محمية أو تصديرها دون اذن صاحبها ، يكون معتدى وتتشكل جريمة التقليد ويدخل في اطار هذه الجريمة كل من يقوم بالكشف الغير مشروع عن المصنف أو المساس بسلامته ، كما يعد مرتكبا لجنحة التقليد تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو آداء.

ولا تقتصر جرمية التقليد على من يعتدي على الحقوق الأدبية للمؤلف ، بل يشمل كذلك كل من يعتدي على حقوق المؤلف المالية ، حيث اعتبر المشرع الجزائري أن كل استنساخ للمصنف مهما كان نوعه أو طريقة أدائه ومهما كانت الوسيلة المعتمدة في النسخ ، يعتبر اعتداء

[1] – أمجد حسان ، المرجع السابق ، ص 10.

[2] – لابأس بأن نشير إلى أن الحق الأدبي للمؤلف يمنح لصاحب هذه المصنفات الحق في نسب المصنف إليه. أما الحق المالي للمؤلف يمكنه من الإستفادة من مصنفه ماليا سواء عن طريق أداء المصنف علانية أمام الجمهور أو عن طريق نشر المصنف وتوزيعه أو عن طريق التنازل عن الحقوق المالية التي أقرها القانون له ، أو عن طريق تأجير هذه الحقوق ، مشار إليه لدى د أمجد حسان : نفس المرجع ، ص 12.

[3] – المادة 151 من الامر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة .

على حقوق المؤلف.[1] خذا الصنف من جرائم التقليد هو أكثر شيوعا في المجال المعلوماتي أي عملية استنساخ البرامج النسخ غير الشرعي.

– إضافة إلى ما سبق ، ومن أجل استظهار قانون حماية حق المؤلف في حماية المصنف وبالتالي البرنامج المعلوماتي الذي تثبت له تلك الصفة و الذي يعتبر أحد مكونات النظام المعلوماتي ، عن طريق بيان ما أقره من جزاءات على الإعتداءات التي يمكن أن يتعرض لها البرنامج بإعتباره مصنفا حاله حال أي مصنف آخر ، فللقاضي أن يطبق كعقوبة أصلية الحبس في ستة أشهر إلى ثلاث سنوات وغرامة قدرها خمسمائة الف دينار جزائري إلى مليون دينار جزائري سواء تمت عملية النشر في الجزائر أو في الخارج.[2]

– وله سلطة تقرير عقوبات تكميلية ، تتمثل في مصادرة المبالغ المساوية لأقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف (البرنامج وبالتالي الموقع) وكل النسخ المقلدة والمصادرة .[3]

– كما للقاضي أن يضاف العقوبات المقررة وذلك في حالة العود ، مع امكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة اشهر ، واذا اقتضى الحال تقرير الغلق النهائي.[4]

---

[1] – أمجد حسان : المرجع السابق ، ص 11.

[2] – نص المادة 153 من الأمر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة على أن : " يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادتين 151 و 152 أعلاه بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من خمسمائة الف دينار (500000 دج) سواء كان النشر قد تم في الجزائر أو في الخارج.

[3] – نص المادة 157 من الأمر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المرجاورة على تقرير الجهة القضائية المختصة:

– مصادرة المبالغ التي تساوي مبلغ الإيرادات أو اقساط الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو آداء محمي.

– مصادرة أو اتلاف كل عتاد الشيء خصيصا لمباشرة النشاط غير مشروع وكل النسخ المقلدة.

[4] – نص المادة 156 من الامر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة على أن :"تضاعف في حالة العود العقوبات المنصوص عليها في المادة 151 من هذا الأمر.

كما يمكن للجهة 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.

ويمكن من جهة أخرى لمؤلف البرنامج المحمي أو ذوي حقوقه المطالبة بحجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد ، وذلك حتى في غياب ترخيص قضائي ، وقد يتم عن طريق الحجز الناتج عن التقليد ايقاف لأية عملية جارية ترمي إلى الاستنساخ الغير مشروع للبرنامج أو حجز الدعائم المقلدة والإيرادات المتولدة عن الاستغلال غير المشروع للمصنفات.[1]

من خلال استقراء النصوص السابقة يتضح أن الحماية الجنائية التي تقررها لا تتوافق مع خطورة الإعتداءات التي يتعرض لها النظام المعلوماتي. فهذه النصوص لا تنال بالتجريم جميع الاعتداءات التي لا تمس البرامج بل فقط تلك التي تتعرض لها المصنفات كون البرنامج جزءا منها.[2] فالمعايير التقليدية التي تحدد حصول الإعتداء لا تحمي البرنامج إلا بصورة الإعتداء المباشر الذي يتمثل بالنسخ المجرد ، فيجري التحقيق من الإعتداءات في مدى التشابه الظاهر بين العمل الأصلي والعمل المنسوخ. لكن برامج الحاسب قد تكون بصورة قد تظهر تظهر متطابقة تمام التطابق ، ولكنها تؤدي إلى نتائج تختلف عن بعضها كما أن هناك برامج تكتب بصورة قد تظهر أنها مختلفة تماما ولكنها تأتي بنفس النتائج.[3]

إلا أن الحماية الجزائية للبرامج وبالتالي للنظام المعلوماتي من خلال حق المؤلف تنصب بصفة أساسية على شكل البرنامج أو مضمونه الإبتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج ، مما يجعلها قاصرة على مد الحماية القانونية المأمولة.

مما سبق نجد أنه من اللازم إضافة نصوص قانونية جديدة لجرائم الإعتداء على النظام المعلوماتي شريطة أن تصاغ النصوص وفقا لمبدأ الشرعية الجنائية ، بحيث تكون نصوص وافية تنطبق على الصور والوقائع الجديدة التي تفرزها ثورات التقنية المتسارعة ، تتماشى مع الواقع الحالي والمستقبل ، بحيث تكون النصوص المجرمة للإعتداء على النظام المعلوماتي تتسم ببعد النضر والأخذ بمعياري التوقع والإحتمال.

[1] – آمال قارة : المرجع السابق ، ص 66.

[2] – محمد حماد مرهج الهيتي ، المرجع السابق ، ص 126.

[3] – أمال قارة ، المرجع السابق ، ص 126.

هناك صراع مرير قائم بين العدوان على المعلومات الإلكترونية بشتى السبل ومختلف الوسائل، وبين البرامج المضادة له والتي هدفها الكشف عنها وتحديد مكانها[1].

وبالرغم من أن هذا الصراع الدائم و المتواصل، إلا أن زيادة حدتها قللت من أهمية الوسائل الفنية أو التقنية التي يتم اللجوء إليها لحماية المعلومات الإلكترونية.

فقبل الحديث عن الإطار القانوني لحماية المعلومات الإلكترونية من أخطار الإعتداءات الواقعة عليها ، ارتأينا الحديث عن مواطن الخلل في نظام الحماية الفنية من مخاطر الإعتداء على المعلومات الإلكترونية كمبحث أول، و من ثم نعرض للحلول القانونية الملائمة التي في ضوء العمل بها قد يتسنى للقطاعات والشركات ومختلف الأجهزة الإدارية والسياسية وغيرها من الإدارات التي تلجأ إلى تكنولوجيا المعلومات في تعاملاتها، حيث يصبح من الممكن حماية البيانات والمعطيات المدرجة في النظام المعلوماتي، وبالتالي إتاحة الفرصة لمزيد من الإبداع والتقدم التكنولوجي في ميدان تكنولوجيا المعلومات والاتصال على السواء وهذا من خلال المبحث الثاني.

[1] – ستيف غيلمور، تبادل المعلومات باستخدام لغة الترميز الموسعة (XML)، بحث منشور في إطار الكتاب المتعلق بـ: حلول التجارة الالكترونية، مقدم من مايكروسوفت، إعداد Micro Modeling Associates، ترجمة: مركز التعريب والبرمجة، الدار العربية للعلوم ، الطبعة الأولى، 2000م، ص593 وما بعدها.

المبحث الأول : إشكالية الحماية الفنية –التقنية– لأمن النظام المعلوماتي في مواجهة الإعتداءات الواقعة عليها

شكلت الإعتداءات الواقعة على نظم المعلومات معضلة قانونية على أساس أن الحماية الفنية أو التقنية لم تعد كافية في إطار أمن المعلومات الإلكترونية و لهذا سنتطرق في هذا المبحث للإجراءات التقنية لأمن المعلومات الإلكترونية من مخاطر الإعتداء عليها و هذا كمطلب أول بينما نخصص المطلب الثاني لتسوية المشاكل القانونية المتعلقة بالحماية من مخاطر الفيروسات.

المطلب الأول: الإجراءات التقنية لأمن المعلومات الإلكترونية من مخاطر الإعتداء عليها

سنتطرق في هذا المطلب إلى التهديدات الأمنية للمعلومات الإلكترونية في النظام المعلوماتي وهذا كفرع أول بينما في الفرع الثاني منه نخصصه للوسائل الفنية الوقائية من التهديدات الأمنية للمعلومات الإلكترونية

الفرع الأول : التهديدات الأمنية للمعلومات الإلكترونية في النظام المعلوماتي

يمكن تعريف التهديدات بطرق مختلفة تنطوي جميعها على بعض القواسم المشتركة التي تجسد الإطار العام للتهديد بمفهومه الواسع، وفيما يأتي نستعرض نماذج هذه التعريفات:

– هو الشخص، المنظمة، الآلية، أو الحدث الذي يمكن أن يلحق الضرر بالموارد المعلوماتية للمنظمة.

– أي ظرف أو حدث من المحتمل أن يؤثر سلبا على العمليات التنظيمية (بما في ذلك مهمة، وظيفة، صورة أو سمعة)، الأصول التنظيمية والأفراد والمنظمات الأخرى، أو للأمة من خلال تعديل المعلومات، و/أو الحرمان من الخدمة.[1]

[1] – ممدوح الشحات صقر، ورقة عمل مقدمة في ندوة أمن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، جوان 2007. مأخوذ من الموقع www.arado.org.eg أطلع عليه بتاريخ 20 نوفمبر 2014 على الساعة 22h00

– أنه "الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصيا كالمتجسس أو المجرم المحترف والقرصان المخترق أو شيئا يهدد الأجهزة والبرامج والمعطيات أو حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية". [1]

وفقا للتعاريف أعلاه يمكننا تحديد أهم أبعاد مفهوم التهديدات لأمن المعلومات على النحو التالي:

- توجد التهديدات متى وجدت نقاط الضعف ويمكن أن يكون هناك عدد من التهديدات لكل نقطة ضعف.
- تتبع التهديدات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء والتي قد تأتي من مصادر داخلية أو خارجية، كما أنها قد تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلى عدم الكفاءة اليومية المتوقعة. وقد تتبع أخطاء النظام من سوء استخدام الأجهزة والبرمجيات، التحميل الزائد أو المشكلات التشغيلية وغير ذلك.
- قد تتسبب المشكلات الفنية نتيجة للهجمات المختلفة التي يتعرض لها النظام، فغالبا تدخل الفيروسات في النظام من خلال البرمجيات المصابة، المتطفلين، الديدان، أو القنابل المنطقية،...الخ. والتي تمثل بعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويهه وعرقلة وظائفه المختلفة، إتلاف أو تحريف بياناته.[2]
- يمكن تصنيف التهديدات في أنواع مختلفة بطرق مختلفة مثل التهديدات البشرية / غير البشرية، التهديدات المعتمدة / غير المعتمدة، تهديدات المهرة / غير المهرة، التهديدات الداخلية / الخارجية. الفيروس على سبيل المثال، هو تهديد غير بشري متعمد، عموما (في البداية على الأقل) وخارجي،

[1] - محمد محمد الالفي، ورقة عمل مقدمة في ندوة أمن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، جوان 2007. مأخوذ من الموقع www.arado.org.eg أطلع عليه بتاريخ 20 نوفمبر 2014 على الساعة 22h00

[2] - ممدوح الشحات صقر، المرجع السابق.

ويمكن أن يكون تهديد المهرة أو غير المهرة (اعتمادا على مطور الفيروس). من ناحية أخرى، يوصف تهديد مدير النظم الساخط بأنه بشري، متعمد، ومهرة، وداخلي.[1]

- التهديدات هي الأشياء التي يمكن أن تسبب الضرر، أو هي الأشياء السيئة المحتملة التي يمكن أن تحدث لأحد الأصول، ومن ثم يمثل خطرا ممكنا على النظام. وقد يكون هذا الخطر شخص يقوم بالتجسس أو التخريب، أو شيء يحدث مشكلة في الحاسب وملحقاته، أو حدثا مثل الحريق أو الفيضان، أو يستغل به نقطة ضعف النظام.

أولا : أنواع التهديدات الأمنية للمعلومات الإلكترونية

تتجسد أهمية تحديد أنواع التهديدات الأمنية للمعلومات الإلكترونية في مساعدتنا لرسم ما يصطلح عليه "بخارطة التهديدات لأمن المعلومات"، ومن ثم تقييم مصادر التهديد، حيث أن المهم النظر في جميع مصادر التهديدات المحتملة التي يمكن أن تسبب ضررا لموارد المعلومات في النظام المعلوماتي وفي كيفية التعامل معها خاصة في الجوانب التي تخدم دراستنا للموضوع محل البحث على النحو الذي يسهل معرفة وتحديد أي التهديدات الأكثر خطورة وبالتالي تركيز الرقابة على النشاط المرتبط به ومن ثم السعي إلى تقليل الآثار السلبية المحتملة له. حيث يمكن استخدام أسس مختلفة في تصنيف التهديدات، وأهم هذه الأسس هي:

- نوع الهجوم المحتمل: يصنف الخبراء المختصين بالقضايا الأمنية عبر الشبكات والانترنت

[1] – محمد محمد الالفي، المرجع السابق.

التهديدات لأمن المعلومات[1] إلى نوعين من أنواع الهجوم المحتملة وهما: الهجوم التقني والهجوم غير التقني.

– حسب المصادر التي تنبع منها التهديدات تصنف التهديدات حسب المصادر التي تتبع منها إلى نوعين وهما: مصادر تهديدات داخلية ومصادر تهديدات خارجية.

– حسب طبيعة التهديدات يتم تصنيف التهديدات حسب طبيعتها إلى ثلاث أنواع " تهديدات طبيعية، تهديدات بشرية، تهديدات بيئية".

–نوع الحدث الحاصل تقسيم أنواع التهديدات على أساس ما الذي يحدث مباشرة لأنظمة المعلومات و هي: الفضح و الكشف ، الوصول غير المصرح له للمعلومات ، الخداع ، التحكم غير الشرعي لأجزاء من النظام .[2]

و عليه سنوضح بإيجاز أهم أنواع التهديدات المحتملة لأمن المعلومات من خلال تصنيفها إلى تهديدات ، داخلية و أخرى خارجية ، و هي تهديدات بشرية صرفة فلا يهمنا التصنيفات الأخرى لها لأنها لا تمس بصلة لبحثنا هذا فالتهديدات البشرية نعرفها بأنها: أي أحداث تتم عن طريف أخطاء البشر، مثل أعمال غير مقصودة (إدخال بيانات غير مقصودة) أو إجراءات متعمدة مثل (الهجوم على الشبكة، تحميل البرمجيات الخبيثة، الوصول غير المصرح به إلى المعلومات السرية) وبالتالي يكون هذا التهديد هو محل دراستنا و يمكن تصنيف التهديدات البشرية إلى نوعين رئيسيين هما:

[1] – لكي نتمكن من استيعاب مفهوم أمن المعلومات لابد أن نرجع إلى اواخر السبعينات حيث كان آن ذاك معروف باسم أمن الاتصالات والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة الامريكية بأنه "المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات" . حيث تضمنت النشطات المحددة لأمن الاتصالات أربعة أجزاء تتمثل في: أمن التشفير، أمن النقل، أمن الإشعاع، أمن الفيزيائي .كما تضمنت أمن الاتصالات خاصيتان تتعلقان بموضوع هذه الوحدة وهي السرية والتحقق من الهوية للمزيد أنظر: ممدوح الشحات صقر، المرجع السابق.

2 – هيثم حمود الشبلي، إدارة مخاطر الإحتيال في قطاع الاتصالات، دار صفاء للنشر والتوزيع، عمان، ط1، 2009، ص 94.

أ- المهاجمون من الداخل:

إن المتسبب للتهديدات الأمنية هو الخطأ البشري، و المعني بذلك هم الموظفون والعاملون في إطار المنظومة المعلوماتية ، إذ يشكل الموظفون ما نسبته (75_80%) من مصادر التهديدات الداخلية في المنظومة وتشمل هذه الفئة الموظفين الحاليين والسابقين. المهاجمون من الداخل هم **"أولائك الأفراد الذين ينتمون للجهة المستهدفة، غير أنهم يقومون بأعمال تصادم جهود الجهة الرامية إلى حماية أنظمة المعلومات التي تستخدمها تلك الجهة".**

فالتهديدات الداخلية يمكن أن تكون بقصود أو غير قصود، من أشخاص معتمدين للوصول إلى نظم المعلومات ، و هم دوما "الخطر الذي تواجهه أي جهة"، مهما كانت سواء كانت تلك الجهة شركة أو منظمة أو حتى دولة. ومع استخدام الحاسوب والتقنيات زاد الخطر الناجم عن الهجمات التي يقوم بها المهاجمون من الداخل ضد الجهة التي ينتمي إليها.[1]

ويؤكد المتخصصون أن الهجوم الداخلي لا يحصل دون أسباب حقيقية، حيث أن هناك أسباب مختلفة للهجوم ضد نظم المعلومات، وهذه الأسباب يمكن إيجازها كالآتي:

- حالة عدم الرضا التي تظهر عندما يشعر الموظف بعدم الرضا ومن ثم يقوم بمهاجمة نظم المعلومات للانتقام.

- إثبات الشخص مهاراته الفنية وقدراته على تنفيذ هجوم إلكتروني، حيث هناك بعض الأفراد يشعرون بالفخر والاعتزاز بنفسهم.

- تحقيق مكاسب مالية، حيث يهاجم شخص ما أنظمة معلومات الجهة التي يعمل فيها لسرقة معلومات سرية يستخدمها لاحقا لابتزاز الجهة لدفع فدية مالية.

[1] - محمد محمد الألفي، الجريمة والمجرم عبر الأنترنت، ورقة عمل مقدمة في ندوة مكافحة الجريمة عبر الأنترنت على المستوى العربي، شرم الشيخ، مصر ، أفريل 2008. مأخوذ من الموقع www.arado.org.eg أطلع عليه بتاريخ 20 نوفمبر 2014 على الساعة 22h00

و هناك العديد من تلك الأخطاء التي تشكل تهديدا كبيرا على أمن المعلومات، وتشكل الأخطاء التقنية والتي حظيت بأكبر حصة، من بين أسوأ الأخطاء التي يرتكبها المستخدمون لأنظمة المعلومات ومنها:

- عدم الاحتفاظ بنسخ احتياطية واختبارها.
- التصريح بكلمات مرور المستخدمين عبر الهاتف أو تغيير كلمات المرور بناء على طلب الأفراد عبر الهاتف ومن قبل أفراد لا يتم التحقق من هويتهم.
- عدم القيام بتحديث الأنظمة عند اكتشاف فجوات (ثغرات) أمنية فيها.
- ربط الأنظمة بالإنترنت قبل تشغيل أنظمة الحماية.

فالإستهانة بالمخلفات التقنية أمر بالغ الخطورة، إذ يقوم المهاجم بتفتيش المخلفات التقنية بحثا عن أي شيء يساعده في اختراق النظام، مثل الأقراص الصلبة بعد استبدالها، أو الأوراق التي دون عليها كلمات السر أو أسماء الملفات والبرامج. وتشمل في المقام الأول الخروقات الأمنية العرضية الحاصلة من قبل الموظفين بسبب الإهمال أو غير المطابقة وسوء سلوك الموظف . فالتهديدات الداخلية المحتملة تحتوي على اختراق بيانات النظام المعلوماتي ، و الاستخدام غير المشروع لها .

ب– المهاجمون من الخارج

وهم الأشخاص من خارج النظام المعلوماتي والذين يطلق عليهم "القراصنة Haker" والذين لديهم بواعث مختلفة للهجوم على الأنظمة، وهم اكثر خطورة من الموظفين الساخطين كما رأينا سابقا من خلال تطرقنا للمجرم المعلوماتي و دوافعه أو بواعثه .[1] ففي المقام الأول نجد أن العملية تتم وفق تهديدات الفيروسات، وهجمات القراصنة ، والهجمات الإرهابية، هجمات الحرمان من الخدمة الموزعة، هجمات الاحتيال والبريد المزعج.

[1] – محمد الصاعدي، جرائم الأنترنت وجهود المملكة العربية السعودية في مكافحتها، ورقة عمل مقدمة في ندوة مكافحة الجريمة عبر الأنترنت ، شرم الشيخ مصر، أفريل 2008. مأخوذ من الموقع www.arado.org.eg أطلع عليه بتاريخ 20 نوفمبر 2014 على الساعة 22h00

فالتهديدات الخارجية غالبا ما تلقى الكثير من الاهتمام عند إثارتها من قبل وسائل الإعلام وتصبح معروفة جيدا، مما يجعل من السهل التركيز عليها والتعامل معها . و تم تصنيف حصان طروادة وديدان الانترنت كأكبر التهديدات. وجاء بالمرتبة الثانية التهديد المرتبط بسوء سلوك الموظف.

و عليه فإن فعل الإنسان الذي يشارك مباشرة، من خلال السلوكات المتعمدة و مثالها التخريب، الالتقاط المتعمد للبيانات غير الصحيحة، التعديل غير المبرر أو حذف البيانات، سرقة النسخة الاحتياطية والابتزاز والتخريب، الهجمات على الشبكة، تحميل البرمجيات الخبيثة، و الوصول غير المصرح به إلى المعلومات السرية أو من فعل غير مباشر و مثاله التخريب، إطلاق سراح البرمجيات الخبيثة يجعلنا نستعرض بعضا من التهديدات الأكثر شيوعا التي تواجهها المعلومات والتي تقع ضمن فئة القراصنة، المقنعون (masqueraders)، نشاط المستخدم غير المصرح به، التحميل دون حماية الملفات، وشبكات المناطق المحلية (LAN) وأحصنة طروادة.[1]

ثانيا : أساليب التهديدات الأمنية للمعلومات الإلكترونية

أ – القرصنة: القرصان هو الشخص الذي يتجاوز عناصر التحكم في الوصول إلى النظام من خلال الاستفادة من نقاط الضعف الأمنية التي تركها مطوري الأنظمة في النظام. وبالإضافة إلى ذلك، العديد من المتسللين هم بارعون في اكتشاف كلمات السر للمستخدمين المرخص لهم الذين يفشلون في اختيار كلمات المرور التي يصعب تخمينها أو تلك غير المدرجة في القاموس. تمثل أنشطة القراصنة تهديدات خطيرة للمعلومات السرية في أنظمة الحاسوب. حيث أنشأ العديد من المتسللين نسخ من الملفات ذات الحماية غير الكافية وتم وضعها في مجالات النظام والتي يمكن الوصول إليها من قبل الأشخاص غير مخولين.

[1] - محمد الصاعدي، جرائم الأنترنت وجهود المملكة العربية السعودية في مكافحتها، المرجع السابق .

ب – الإختفاء : المختفي أو المقنع هو المستخدم المصرح به للنظام والذي حصل على كلمة مرور مستخدم آخر، على النحو الذي يمكنه الوصول إلى الملفات المتاحة للمستخدم الآخر. وهؤلاء المتخفون غالبا ما يكونوا قادرين على قراءة ونسخ الملفات السرية. والتكرار أمر شائع في الشركات التي تسمح للمستخدمين لتبادل كلمات السر.

ج – نشاط المستخدم غير المصرح : هذا النوع من النشاط يحدث عندما يحقق مستخدمي النظام المخولين للوصول إلى الملفات التي لا يحق لهم الوصول إليها. وضعف التحكم في الوصول غالبا ما يمكن من الوصول غير المصرح به، والتي يمكن أن تمس الملفات السرية.

د – التحميل للملفات دون حماية: يمكن تحميل الملفات السرية إذا تم في عملية التحميل، نقل الملفات من بيئة آمنة في الحاسبة المضيف إلى الحاسبات الصغيرة غير المحمية لغاية المعالجة المحلية. حيث يمكن الوصول إلى المعلومات السرية غير المراقبة من قبل المستخدمين المصرح لهم على الحاسابات الصغيرة.[1]

هـ – شبكات المناطق المحلية: تشكل الشبكات المحلية تهديدا خاصا للسرية بسبب أن البيانات التي تتدفق من خلال LAN يمكن مشاهدتها في أي عقدة في الشبكة، بغض النظر عما إذا كانت هذه البيانات معنونة أم لا إلى تلك العقدة. وهذا أمر بشكل خاص لأن معرفات المستخدمين غير المشفرة وكلمات المرور السرية للمستخدمين الذين يسجلون الدخول إلى المضيف تخض لتقديم تنازلات كلما تحولت هذه البيانات من عقدة المستخدم ومن خلال LAN إلى المضيف. أي معلومات سرية غير مخصصة للعرض في كل عقدة يجب أن تكون محمية من خلال التشفير.

[1] – أشرف صلاح الدين، طرق الحماية التكنولوجية بأنواعها واشكالها المختلفة، ورقة عمل مقدمة في ندوة امن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، مصر، جوان 2007. مأخوذ من الموقع www.arado.org.eg أطلع عليه بتاريخ 20 نوفمبر 2014 على الساعة 22h00.

و – أحصنة طروادة: يمكن برمجة أحصنة طروادة لنسخ الملفات السرية إلى المناطق غير المحمية من النظام عندما يتم تنفيذ أية عملية من قبل المستخدمين الذين يؤذن لهم بالوصول إلى تلك الملفات. وحالما يتم التنفيذ، يصبح حصان طروادة مقيما في نظام المستخدم، ويمكن نسخ الملفات السرية بشكل روتيني على الموارد غير المحمية .

ي –الأجهزة المحمولة: و هذا من التحديات الجديدة التي تتزايد خطورتها يوما بعد يوم و هذا من خلال البرمجيات الضارة التي تستهدفه، وسرقة البيانات، وفقدان أو سرقة الأجهزة، وبشكل متزايد، وقضايا أخرى تظهر في كل وقت، مثل القدرة على تحديد الموقع الجغرافي للفرد من خلال أجهزتهم بحيث يخلق أنواع من المخاطر التي لا تزال غير مفهومة.

الفرع الثاني : الوسائل الفنية الوقائية من التهديدات الأمنية للمعلومات الإلكترونية

ما من وشك أن للوسائل الفنية –التي تعمل على الوقاية من اثار التهديدات الأمنية– أثر بالغ الأهمية في تحديد موقع ونوع الفيروس وتعقب آثاره وبالتالي الوقاية من الأخطار الممكن وقوعها في حال غياب هاته الإجراءات.

ويمكن تلخيص هاته الإجراءات الواجب العمل بها من طرف مالك البرنامج أو من طرف الجهات المنتجة أو غيرها من الجهات الصلة بالنقاط التالية:

أولا: أن تكون النسخة التي يحصل عليها مقتني البرنامج مغلفة بغلاف الشركة المنتجة تغليفا محكما وهذا لا يعني أن البرامج المغلفة مؤداه خلوها تماما من الفيروس، لكن هذا الاجراء يقلل من احتمالات الإصابة بالفيروس بدرجة كبيرة.[1]

ثانيا: عمل نسخة احتياطية باستخدام القرص الاصلي برنامج ثم حماية القرص الاحتياطي أيضا[2].

[1] – محمد محمد الالفي، المرجع السابق، ص 95.

[2] – محمد فهمي طلبة وآخرون ، فيروسات الحاسب وأمن البيانات، مرجع سابق، ص98.

وتجدر الإشارة إلى أن مسألة عمل نسخة احتياطية للبرنامج لاقت اعتراضا واسع النطاق من طرف المبرمجين والشركات المنتجة بحجة أن العديد من الأفراد غالبا من يلجئون إلى قرصنة البرامج تحت ذريعة أن هذه النسخة لا تمثل سوى نسخة احتياطية لبرنامج هذا فضلا عن أن أغلب الأشخاص الذين يحصلون على هاته النسخ غالبا ما يتواجدون في أماكن خاص بهم يصعب الوصول إليها أو معرفة أنهم قاموا –مثلا– بعملية قرصنة لبرامج الحاسب الالي.

لذا برزت معارضة حادة لمسألة عمل نسخة احتياطية للبرنامج إلا أن هاته المعارضة لم ترق –في الواقع– إلى مستوى منع الأفراد أو الجهات من الاحتفاظ بنسخة احتياطية كإجراء وقائي يتم اللجوء في حال تعرض برامجهم لهجمات فيروسية.

ثالثا: تحميل البرنامج على القرص الصلب من القرص الأصلي للبرنامج.

رابعا: العمل على مقارنة الملفات المخزنة على القرص الأصلي بنفس الملفات المخزنة على القرص الاحتياطي.

إذ أنه في حال تواجد أي اختلاف، يصبح هناك شك في تواجد الفيروس[1].

خامسا: العمل على اختبار كل برنامج موجود على القرص والتأكد من أنه يؤدي وظائفه بصورة طبيعة، وملاحظة أي أشياء غريبة قد تحدث من أي برنامج.

سادسا: العمل على اختبار البرامج المخزنة مع تغيير التاريخ في ساعة النظام (**SYSTEM CIOCK**) إدخال التواريخ التي تستخدمها بعض الفيروسات والتي تبدأ عملها وفق تاريخ أو توقيت محدد، إذ يتم بهذه الطريقة الكشف عن هذه الفيروسات –إذا كانت موجودة– وبالتالي إمكانية التخلص منها[2].

[1] تتم المقارنة باستخدام الأمر (Disk comp) أو الأمر (Comp) في نظام التشغيل (DOS).

[2] فهمي محمد طلبة، المرجع السابق، ص98.

سابعا: العمل على اختبار البرامج للبحث عن سلاسل حرفية معينة ترتبط بوجود أنواع معينة من أنواع الفيروسات، وبالتالي إمكانية التخلص منها.

ثامنا: مرقبة ملفات الأوامر المجمعة (**Batch Files**) ذات الامتداد (**BAT**) بين الفينة والأخرى، وكذلك ملف المواصفات (**Config. Sys**) وملاحظة أي تغيير يطرأ على الأوامر الموجودة فيها، حيث أن الفيروس يحتاج إلى الارتباط بأي ملفات منفذة حتى يتم تشغيله، لذلك فإنه في بعض الأحيان يكتب سطورا في ملف الأوامر المجمعة أو في المواصفات حتى يضمن تنفيذه[1].

تاسعا: تعقب آثار الفيروس، وذلك باستخدام أسلوب التوقيع الرقمي.

حيث يمكن —عن طريق أسلوب التوقيع الرقمي- تعقب آثار الفيروس إلى مصدره-وذلك عندما يكون الفيروس موجها عبر شبكات الاتصال- إذ يمكن عن طريق استخدام (**Audit Trail**) أن يتم تتبع هذا الفيروس، الشيء الذي يمكن عن طريقه أن يحجم مروجو الفيروسات عن الإنتاج لها وترويجها عبر الشبكات[2].

عاشرا: إتاحة الإمكانية للبرامج للقيام بعملية الدفاع الذاتي.

حيث يستطيع كل مبرمج تصميم نظام دفاعي ضد الفيروسات، وهناك أبحاث تقترح أن تضاف هذه الإمكانية لمترجمات البرامج وذلك حتى تقوم بتزويد البرامج في مرحلة الترجمة بهذا النظام الدفاعي.

وتكمن ميزة هذا الأسلوب في سهولة وسرعة تطبيقه، إلا أنه يعاب عليه أنه لا يستطيع اتخاذ إجراء ضد الفيروس المهاجم إلا بعد تعرفه عليه، وربما يكون الوقت عندئذ قد فات وبدأ الفيروس نشاطه الهدام[3].

---

[1] – محمد فهمي طلبة، المرجع السابق، ص98-99.

[2] – عوض الحاج علي أحمد، عبد الامير خلف حسين، امنية المعلومات وتقنيات التشفير، دار الحامد للنشر والتوزيع، الأردن، 2004، ص 128 وما بعدها.

[3] – المرجع نفسه ، ص 128 وما بعدها.

الحادي عشر: استخدام أحد البرامج المساعدة في عرض أسماء الملفات المختفية (hidden Files)، وعند ملاحظة أي أسماء جديدة أكثر من أسماء الملفات المستخدمة في نظام التشغيل يكون هناك شك في تواجد الفيروس الذي يجب العمل على التخلص منه.

الثاني عشر: العمل على تسجيل بيانات كل برنامج مثل طول الملف والتاريخ والوقت ومصدر البرنامج، وعند ظهور الفيروس في أي وقت، تصبح هذه البيانات في منتهى الأهمية.

حيث يمكن من خلال تاريخ اكتشاف هذا الفيروس استنساخ النسخ الاحتياطية التي تم عملها قبل هذا التاريخ خالية من الفيروس، ويكون هناك شك فقط في باقي النسخ التالية لهذا التاريخ.

كما أن هذه البيانات قد تقود المستخدم في النهاية إلى المجرم الذي قام بوضع هذا الفيروس[1].

الثالث عشر: وضع برنامج عازل للفيروسات في الجهاز الذي يصل بين الشبكات الداخلية والعالم الخارجي (مثل الوسيط Proxt) لمنع وصول الفيروسات إلى الشبكة المحلية أو إلى أجهزة المستفيدين.

الرابع عشر: التأكد من أن جميع الاتصالات التي تتم من خلال الحاسبات الشخصية للمستفيدين بخارج المؤسسة تتم عن طريق الشبكة وليس عن طريق "مودم" قد يتم تركيبه خلسة في أحد الحاسبات الشخصية للاتصال (بإنترنت) مثلا[2].

الخامس عشر: استخدام ما يطلق عليه "بالتوقيع الرقمي" (Digital Signature).

فلما كان تداول البيانات داخل الشبكات والبريد الالكتروني هما من المصادر الهامة للإصابة بالفيروسات، فلابد من التركيز على هذا القطاع للحد من تأثير الفيروسات وذلك بالعمل على اكتشاف وجوده قبل أن تبدأ عملها.

[1] – محمد فهمي طلبة وآخرون، فيروسات الحاسب وأمن البيانات، مرجع سابق، ص90.

[2] – عوض الحاج علي أحمد، عبد الامير خلف حسين، المرجع السابق، ص 128 وما بعدها.

ويعتبر أسلوب "التوقيع الرقمي" من الأساليب الهامة التي يمكن عن طريقها تحقيق هاته النتيجة.

كما يختلف أسلوب "التوقيع الرقمي"-في عمله- عن أسلوب البرمجيات التي تستخدم للكشف عن وجود الفيروس، حيث يسمح بكشف أي تغيير قد يتم إجراؤه على أي برنامج أو ملف، ذلك لأنه –ببساطة- يشبه توقيع مرسل الرسالة عليها ولا يمكن تزويده أو انتقاله.

وقد قامت بعض الشركات الصانعة للبرمجيات بتقديم العديد من المقترحات بهدف تعميم استخدام "التوقيع الرقمي" في جميع معاملات البريد الالكتروني في شبكة الانترنت، وكذا في شبكات (إنترانت)[1].

ومن بين هذه المقترحات أن تقوم الشركات الصانعة للبرمجيات (بالتوقيع) رقميا على منتجاتها، مما يسمح لمستخدم البرنامج بالتعرف على أي تعديل قد يكون ألحق بالبرنامج بعد إنتاجه.

وفي حالة تلوث البرنامج بأحد الفيروسات، يمكن-من خلال التوقيع الرقمي- تتبع هذا الفيروس حتى مصدره، مما يشكل حافزا قويا لمطوري البرامج لتوخي الحذر عند تطوير وإنتاج برامجهم.

ومن خلال التوقيع الرقمي يمكن أن يتحقق نظام التشغيل من صحة التوقيعات على البرامج قبل السماح بتشغيلها، وبذلك تتضاءل فرص النجاح أمام أي فيروس، ولو أن هذا قد يؤدي إلى سوء الأداء في الحاسبات البطيئة، ولكن بعد ازدياد سرعات الحاسبات الشخصية والوصول إلى سرعة 1"جيجا بايت"، فإن ذلك يجعل هذه العملية ذات تأثير لا يكاد يذكر على الأداء[2].

[1] – شبكات إنترانت: هي شبكات محلية داخلية تقوم بين المنشآت التي تستخدم تقنية (إنترنت) من برمجيات مثل (HTML) وصفحات (WEP) و(متصفح browse) وغير ذلك.

[2] – عوض الحاج علي أحمد، عبد الامير خلف حسين، المرجع السابق، ص 128 وما بعدها.

من خلال ما تقدم نكون قد استوضحنا لعدد من الوسائل والإجراءات التقنية التي يلزم العمل بها لتحقيق الأمنية على مستوى البرامج والحيلولة دون ولوج أو دخول الغير إليها وتسريب الفيروسات العدوانية التي غالبا ما يكون دورها تحطيم البيانات وإتلاف البرامج والتجسس على القطاعات الهامة، والتي تدفع الكثير من جراء هاته الهجمات وما تخلفه من آثار.

ومع ذلك نقول أنه بقراءة الواقع نجد أن هذه الإجراءات لم تقف حائلا دون تمكن العديد من الفيروسات من اختراق الشبكات و النفاذ إلى البرامج والبيانات في العديد من القطاعات .

المطلب الثاني: تسوية المشاكل القانونية المتعلقة بالحماية من مخاطر الفيروسات

ما من شك أن تفعيل السبل القانونية وبناء النصوص الموضوعية في موضوع الحماية من مخاطر التهديدات الأمنية مؤداه تقليص حجم المخاطر وتقليص مستوى الجريمة المرتكبة بحق المعلومات عن طريق الإعتداء عليها .

وقد جاءت أغلب الجرائم الالكترونية الواقعة عن طريق النظام المعلوماتي نتيجة علم الجناة بحقيقة النقص والفراغ القانوني الذي يعد مشجعا لهم بالدرجة الأولى على ارتكاب مثل هاته الأفعال ما دام أن هؤلاء الجناة على قناعة مسبقة بإمكانية إفلاتهم من العقوبة التي افتقرت إلى مبدأ الشرعية الجنائية الذي يضمن الحد من مستوى الجريمة في هذا الميدان.

وفي الواقع توجد هناك عدد من الأسباب التي تمثل موانع أمام تطبيق القانون والتي تحتاج إلى حلول جدية وموضوعية للحيلولة دونها.

الفرع الأول : المعوقات التطبيقية القانونية

في الواقع، يواجه تطبيق القانون في موضوع الفيروس عددا من الصعوبات والموانع التي يمكن تلخيصها فيما يلي:

1- في إطار الإعتداءات التي أساسها الفيروس نجد أنه-في الغالب- لا يتمكن الضحية من معرفة المجرم الذي صمم هذا الفيروس، وأنه في حال معرفته بذلك، فإنه غالبا ما يتحمل تكاليف باهظة للوصول إلى هاته الحقيقة ومتابعة الجاني[1].

2- رغبة العديد من ضحايا الفيروس وقد سبق الإشارة إلى ذلك من الشركات والقطاعات الاقتصادية الكبرى -وخصوصا في ميدان البنوك- في عدم الكشف عن إصابة نظامهم بالفيروس، وذلك حتى لا يتسبب ذلك في اهتزاز ثقة العملاء إذ يؤدي الكشف -مثلا- عن هاته الفيروسات -في قطاع البنوك- إلى قيام العديد من العملاء باللجوء إلى سحب أرصدتهم كإجراء حال علمهم بذلك.

3- جهل أو عدم معرفة الضحية أن نظامه قد أصيب بالفيروس لمدة طويلة وعندما يكتشف ذلك يصعب عليه تحديد وقت وسبب الإصابة

4- صعوبة قياس أو تقدير الخسائر -خصوصا عندما تكون مادية- ومثال ذلك أن بعض الفيروسات يتسبب في إتلاف أحد البرامج مما يؤدي إلى إصابة مخطط هذا البرنامج بكثير من الاحباط نتيجة ذلك دون حدوث خسائر مادية محددة مع العلم أن أهمية هاته المخططات قد تفوق بكثير التقديرات المادية المتوقعة.

5- قدرة الفيروس على إخفاء أي آثار وكذا إمكانية بعض الفيروسات مسح نفسها تماما من ذاكرة البرنامج بعد تنفيذها لأعمالها التدمرية وبالتالي صعوبة الوصول إلى المخرب الذي قام بتصميم هذه الفيروسات أو إدخالها إلى النظام.

6- جهل المستخدم للمعلومات الكافية عن الفيروس وبالتالي لا يعرف أن هناك مخربا وراء هذا الفيروس الذي يجب الإبلاغ عنه حتى يتم الوصول إلى مدبره ومعاقبته.

[1]- محمد فهمي طلبة، المرجع السابق، ص206.

وفي الواقع هذا الجهل –إلى حد ما– أصبح متجاوزا بالنظر إلى كون الفيروسات في المرحلة الراهنة أصبحت تمس عددا غير محدود من أجهزة النظام المعلوماتي وتخلف عددا من الأضرار لذا فإنه في حال جهل البعض بحقيقة وجود الفيروس داخل البرامج أو النظام الخاص بهم فإن ذلك ليس معناه جهل الجميع الذين تنال منهم الفيروسات تخلف أضرار بالغة بقطاع البرامج لديهم.

7– عدم توفر الخبرة الكافية لدى المشرعين بالجوانب الفنية المختلفة لموضوع الفيروس أو في مجال الحاسب بصفة عامة الشيء الذي انعكس مباشرة على البناء القانوني الذي يستدعي معرفة دقيقة بالطرق بالوسائل التي يتم من خلالها اعداد الفيروس وكذا الوسائل التي يتم عبرها تنفيذه لمخططة وبالتالي إمكانية تدخل المشرع كلما أتيحت له الفرصة لذلك لسد مختلف القنوات التي يمكن من خلالها أن تفلت الجريمة من العقاب.

8– قدرة الفيروس –ومع التطور الهائل لوسائل الاتصال– على الانتقال واختراق الحدود الجغرافية المتعارف عليها بحيث أن اغلب الفيروسات لم تعد تهم دولة واحدة أو قطاع معين وإنما أصبحت تطول آثارها الآلاف بل الملايين من الأجهزة والنظم في عدد كبير من البلدان دون استثناء.

وتعد هذه أخطر المراحل التي وصل اليها الفيروس –وإن كانت هناك بعض الدراسات والتنبؤات عن مستقبل الفيروس والإمكانات أمامه يطور نفسه في ضوئها.[1]

وعليه سنعرض للمقترحات والضمانات الواجبة التطبيق، والتي في حال الأخذ بها قد يتم تخطي هذه العقبات البالغة التعقيد في إطار مرحلة أصبحت فيها العولمة حديث الساعة، وأخذت في إطارها الدول تتجه نحو بناء مفهوم التجارة الالكترونية والحكومة الالكترونية وغيرها من المظاهر التي طبعت حياة الفرد والجماعات في كل مكان.

[1]– محمد فهمي طلبة ، فيروسات الحاسب وأمن البيانات، المرجع السابق، ص206.

الفرع الثاني : ضرورة صدور نظام تشريعي خاص بأمن المعلومات من الإعتداءات الواقعة عليها

لما كان النظام المعلوماتي و المسائل المتصلة به [1] ، تسمح لمستخدميه الدخول إلى النظام من أي مكان في العالم، و هذا لكون بنية الانترنت التحتية المتمثلة بأنظمة الكمبيوتر والاتصالات تمتد إلى العديد الدول، وأن مكان ممارسة العمل الفعلي للشخص قد لا يكون هو المكان الذي تقدم من خلاله خدمة إطلاق الموقع على الشبكة، ولما كان الاعتماد على الانترنت أصبح يمثل محور حياة الفرد والجماعة، لذا فقد كان لظهور التحديات القانونية والتنظيمية الصفة المباشرة نتيجة هاته التطورات المتلاحقة.

وبالتالي فقد وجدنا أنه من المناسب الحديث عن بعض الحلول التي تهم موضوعنا والمتمثل في امن المعلومات الإلكترونية و النظم من الفيروسات —بالتحديد– التي تروج شبكات الاتصال وتمتد آثارها إلى أكثر من جهة أو أكثر من قطاع.

حيث يجمع الباحثون أن تحديد الموقف من مسائل القانون المتصلة بالأنترنت يجب أن ينطلق ابتداء من فهم الطبيعة التقنية لهذه الواسطة المعقدة من وسائط تكنولوجيا المعلومات، وأنه بدون

[1] – مواقع الإنترنت يمكن أن تدار أو تستضاف من أي مكان من العالم بغض النظر عن مكان صاحب الموقع، إذ أن الوسائط التقنية تتيح الدخول إلى الكمبيوتر وإدخال المعلومات والتحكم بالمحتوى من أي مكان في العالم.

كما أن المستخدم يمكنه أن يدخل إلى الخط الخادم من أي مكان بغض النظر عن موقع الكمبيوتر المستخدم في الدخول، هذا بالإضافة إلى أن إدارة موقع الإنترنت يهدف مالكه أن يكون مميزا من جهة تقنية تدفعه لاستضافة موقعه في أكثر الدول تقدما من حيث البنية التحتية والكفاءة والتقنية وأكثرها تسهيلا بالنسبة لمشاريع الاستثمار المعلوماتي، وقواعد تنظيمها القانوني، وهو ما أدى إلى أن يشيع وجود النظام الخام للموقع في دولة غير دولة مالك الموقع مع توفر القدرة التقنية للدخول إلى موقعه في أي وقت يشاء، وإدارة موقعه بالشكل الذي يريد. حيث من المعلوم أن وسائل إدارة المواقع عن بعد قد تكون عاملة في وقت، وقد تتوقف عن العمل تبعا للوضع التقني الذي يسود في وقت الدخول إلى الموقع:

أنظر: يونس عرب: جرائم الكمبيوتر والإنترنت أطلع عليه http//www.arablaw.org بتاريخ 2015/01/15 على الساعة 23h20

إدراك هذه الطبيعة يتخلف الشرط الموضوعي لتقييم مدى ملائمة القواعد القانونية القائمة، ومدى الحاجة إلى إيجاد قوانين خاصة تنظم مسائل عصر المعلومات، بما فيه الإنترنت.[1]

وعليه فإن أولى المقترحات والحلول التي نوليها اهتمامنا هي تلك التي تهم الكيفية التي يتوجب من خلالها تسوية الإجراءات الشكلية المتعلقة بتنازع القوانين والاختصاص التي تحكم جرائم الحاسب الآلي –وتحديدا- الفيروسات الالكترونية المروجة عبر شبكات الاتصال.

ولتوضيح الصورة الميدانية نسوق المثال التالي:

فلو فرضنا أن شخصا متواجد في الولايات المتحدة أو في الباكستان مثلا، وقام بزرع فيروس معلوماتي عبر الشبكة المعلوماتية (الإنترنت) الذي زار عددا من المواقع على هاته الشبكة، وعمل على اختراق مجموعة من الأنظمة على الشبكة، وأحدث إتلاف بياني معلوماتي في البرامج والنظم، وقد طال هذا الأثر عددا من البلدان منها الجزائر ومس الآلاف من الحاسبات الالكترونية، بحيث خلف خسائر يصعب حصرها، فما هو الإجراء الواجب إتباعه لتفادي هذا الإشكال ؟ وهنا –بالتحديد- نتساءل: ما هو القانون واجب التطبيق ؟ و فيما يخص موضوع حماية الأنظمة من مخاطر الإعتداءات كان لابد من وضع تشريع خاص بحماية الانظمة المعلوماتية من الإعتداءات الواقعة عليها يضمن الآتي توضيحه:

أولا: خلق أجهزة دولية متخصصة هدفها مراقبة شبكات الاتصال، ومهمتها الكشف عن الفيروسات التي تروج عبر الشبكات والعمل على ضبط المخالفات في هذا الميدان، وكذا –في حال انتشار فيروس عبر شبكات الاتصال- هذا الفيروس ومعرفة مصدره، والعمل على الكشف عن الشخص أو الجهة المروجة له وتقديمها للجهات المكلفة بالمحاكمة.

[1] – نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات، المؤتمر الدولي حول أمن المعلومات –نحو تعامل رقمي آمن-، 18-2005/12/20، مسقط، سلطنة عمان.

وعليه فإنه يمكن القول أن عمل هذه اللجان يشبه-إلى حد ما- عمل اللجان الدولية، إلا أن هاته اللجان تمتاز بكونها تشتمل على عناصر فنية متخصصة في ميدان النظم وتكنولوجيا المعلومات، الشيء الذي يتيح لها إمكانية العمل-وبحرية- للتمكن من حماية المعلومات الإلكترونية من الانتهاكات التي ترتكب عبر شبكات الاتصال، والتي يتم من خلالها تحقيق الاعتداء على الأنظمة.[1]

ثانيا: إنشاء قانون خاص و مستقل، وذلك لتفادي الإشكالات الناجمة عن مشاكل الفيروسات المروجة عبر شبكات الاتصال.

ومما ينبغي الإشارة إليه هو أن التشريع المستقل الذي أشرنا إليه هنا المتعلق بالحماية من مخاطر الإعتداءات على المعلومات ، وليس كل صور الاعتداءات أو المشاكل الأخرى المثارة -خصوصا- في إطار الإعتداءات على النظام المعلوماتي[2].

[1] - جميل زكرياء محمود، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات، المؤتمر الدولي حول أمن المعلومات –نحو تعامل رقمي آمن-، 18-2005/12/20، مسقط، سلطنة عمان.

[2] - يعد من الطبيعي في بيئة التجارة الالكترونية، أن تظهر المنازعات-تماما كما هو الحال في العالم غير الالكتروني- وأن من بين هاته المنازعات ما يتصل بإبرام العقد وتنفيذه وتفسيره، وأخرى تتصل بالعناصر المرتبطة بالتجارة الالكترونية، ومنازعات الملكية الفكرية-وتحديدا- بالنسبة للعلامات التجارية واتصالها بأسماء المواقع التجارية الالكترونية على شبكة الإنترنت.

ومن المعلوم أن هذه المنازعات التي غالبا ما تتضمن طرفا أجنبيا لقيامها ابتداء بين أطراف خارج النطاق الإقليمي الواحد، تثير العديد من التساؤلات بالنسبة للمحكمة المختصة بنظر النزاع، والقانون واجب التطبيق على النزاع، ومدى قوة وحجية الأحكام الأجنبية الصادرة في مثل هذه النزاعات للنفاذ في إقليم آخر.

لم ينجز الكثير في حقل التصدي الجماعي لمشكلات الاختصاص وتنازع القوانين في بيئة التجارة الالكترونية، حيث يتصل بهذا الموضوع أيضا مسألة مدى فعالية وأهمية الاعتماد على طرق التقاضي البديلة وتحديد التحكيم لفض منازعات التجارة الالكترونية.

ويختلف الوضع فيما يخص ميدان الفيروسات عنه في ميدان التجارة الالكترونية، حيث أن التجارة الالكترونية تحمل في مضمونها علاقات متبادلة قد يشوبها بعض القصور أو يعترضها بعض الصعوبات التي تثير المشاكل القانونية من حيث تطبيق أي من قوانين الأطراف والمحاكم المختصة بالنظر في النزاع القائم بين أطراف العلاقة في حال اختلاف جنسيات الأطراف.

أما الفيروسات فهي لا تمثل علاقات بين أطراف، ولا تعد بيئة مناسبة لقيام علاقات، بل هي برامج عدوانية تهاجم النظم و البيئة الالكترونية التي يستخدمها أصحابها في قيام وتنفيذ علاقاتهم التجارية والقانونية...الخ. ولهذا فإن مسألة التنازع في القوانين في ميدان الفيروسات تستوجب البت فيها بطرق مغايرة عن تلك المتمثلة في ميدان التجارة الالكترونية. ينظر في ذلك يونس عرب، المرجع السابق.

ومما ينبغي قوله أن القضاء في ميدان تكنولوجيا المعلومات والمتعلق بحماية أنظمة المعلومات وشبكات الاتصال، ينبغي أن يملك حجية الإلزام وآليات التنفيذ لأحكامه ضمانا للحفاظ على المكتسبات التي وصلت إليها الحياة البشرية، وكذا إتاحة الفرصة للإبداع والمبدعين لتقديم المزيد في عالم يسوده الأمن والاستقرار وليس في بيئة محفوفة بالمخاطر أخذت فيها معظم الشركات والقطاعات تعزل نفسها عن شبكات الاتصال مخافة الهجمات الفيروسية التي تتزايد حدتها يوما بعد يوم.

ثالثا: توضيح الأعمال التي تشكل جرائم نتيجة الأضرار التي يحدثها الإعتداء على النظام المعلوماتي.

حيث سبق وأن قلنا أن الفيروس –في الواقع– يحدث أضرارا مختلفة تبعا للهدف الموجه لأجله. وبالتالي فإنه لتحقيق مبدأ الشرعية، يستوجب التعاون بين رجال القانون لتجريم كافة مظاهر وأشكال الاعتداء التي يلجأ إليها الفيروس في تحقيق الضرر، هذا دون إغفال الإشارة إلى ضرورة الاستعانة بأصحاب الخبرة الفنية في هذا الميدان[1].

رابعا: العمل على ترتيب إجراءات هيكلية يكفل من خلالها المتضررون من الهجمات الفيروسية الحصول على تعويضات مالية في حال كان الضرر الذي لحق بهم مادي، حيث من المعلوم أن بعض الفيروسات قد تطول الآلاف من الأفراد الذين تلحق بهم أضرار جسيمة من جراء هاته الفيروسات، ففي هاته الحالة هل من المعقول أن الشخص الذي تسبب في هذا الفيروس أو الجهة التي قامت بزرعه قادرة على تعويض هؤلاء المتضررين جميعا ؟

[1] لقد عمل البعض على تناول أشكال الاعتداء التي يلجأ إليها الفيروس الالكتروني ودعا إلى تجريمها وذلك بالنظر إلى النتيجة المحتمل إحداثها من طرف الفيروس حيث حدد هاته الأعمال فيما يلي:

أ–تحطيم أو تعديل بيانات الغير. ب–تحويل بيانات الغير إلى بيانات ليس لها معنى. ج–التدخل واعتراض الغير عند استخدامهم القانوني للبيانات. د–تغيير وظائف برامج الغير بما يسبب أضرار مادية أو معنوية.و–تحطيم أجزاء من مكونات الحاسب أو جعلها غير قادرة على أداء وظائفها. ي–نسخ البرامج دون إذن الحصول على تصريح من الشركة المنتجة لهذه البرامج: ينظر في ذلك محمد فهمي طلبة وآخرون، فيروسات الحاسب وأمن البيانات، مرجع سابق، ص208-209.

بالطبع لا يمكن تحقيق ذلك، لذا فإنه يتوجب على المجتمع الدولي إيجاد وسائل بديلة وذلك عن طريق إنشاء شركات تأمين عالمية متخصصة ترتبط مباشرة مع الأجهزة الدولية المكلفة بضبط ومتابعة مبرمجي الفيروسات الالكترونية، ووظيفتها هو التعويض للمتضررين عن الأضرار التي خلفها الفيروس ببرامجهم وأنظمتهم الالكترونية.

المبحث الثاني: الإطار التشريعي لأمن النظام المعلوماتي من الإعتداءات الواقعة عليه

بناء على ما تقدم نتناول الإتجاهات القانونية المتعلقة بالتعامل مع هذه الظاهرة وفق تأثرها إما بالإتجاه الفقهي القائل بعدم الحاجة لإصدار تشريع خاص و مستقل لحماية الأنظمة المعلوماتية [1]، أو الإكتفاء بالحماية الأمنية ذات الطبيعة الفنية[2]، أو الإتجاه الذي ينادي بضرورة صدور خاص و مستقل عن قانون العقوبات كتنظيم تشريعي يتعلق بكل ما يتعلق بالنظاام المعلوماتي[3]. لهذا سنتطرق لها ليس كدراسة تحليلية لنصوص وقواعد هذه القوانين ، بل مجرد استعراض عام لإتجاهات التشريع والمعالم الرئيسية في تحديد تلك الجرائم في صورة اقرب ما تكون إلى استظهار مرتكزات السياسة التشريعية للقوانين المقارنة و القوانين الوطنية بشأن هذه الجرائم لنلمس مدى اختلاف الأنظمة القانونية للدول في التعامل معها ، ولعل مرد ذلك يرجع إلى اختلاف تجربة كل منها مع الجريمة المعلوماتية ، حسب درجة التطور التقني وجسامة الخسائر الناتجة عن أفعال الاعتداء التي تمس هذا القطاع ، ومدى تأثير النتائج الإقتصادية التي ترتب عن ذلك.

و عليه فإن الأساليب والأشكال التي تلجأ إليها الدول في صياغة النصوص القانونية بهدف الحماية الجنائية للأنظمة المعلوامتية ، في هذا الصدد يمكن إجمالها فيما يلي :

- تتجه بعض الدول عند صياغتها للنصوص الجنائية التي تحمي النظم المعلوماتية إلى انتهاج أسلوب الإضافة ، حيث تقوم بإضافة نصوص تنظيم الحالات التي يرتكب فيها الجاني النشاط

[1] – يرى مناصرو الاتجاه بأنه لا داعي للذعر ، فلا جديد فيما يتعلق بأجهزة الكمبيوتر ، وبوسع الأجهزة القضائية أن تستعمل الأنظمة القانونية القائمة لضبط وتنظيم الأوجه المختلفة لإستخدام أجهزة الكمبيوتر ، ويدعي أنصار هذا الاتجاه أنه قد أفلح في التعامل مع جميع الوسائل الاخرى مثل التلفون والفاكس ، ويقولون أيضا أن جميع الجرائم التي تتم من خلال أجهزة الكمبيوتر أو بواسطته يمكن التعامل معها بواسطة الأنظمة القانونية القائمة ، مشار إليه لدى إيهاب ماهر السمباطي ، الجرائم الإلكترونية الجرائم السيبيرية قضية جديدة أم فئة مختلفة التناغم القانوني هو السبيل الوحيد ، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ، المملكة المغربية ، 19-20 يونيو ، 2007 ، ص 03.

[2] – نائلة عادل محمد فريد قورة : مرجع سابق ، ص 306.

[3] – ايهاب ماهر السمباطي ، الجرائم الإلكترونية الجرائم السيبيرية قضية جديدة أم فئة مختلفة التناغم القانوني هو السبيل الوحيد ، مرجع سابق ، ص 16.

الإجرامي المتصل بالنظم المعلوماتية إلى النصوص القائمة والموجودة بالفعل ، ومن هذا القبيل ما قام به المشرع الجزائري في ظل نصوص قانون العقوبات.[1]

– فيما تقوم دول أخرى بوضع نصوص جديدة قياسيا على نصوص تقليدية قائمة بالفعل ، ففي هذه الحالة يصاغ نص جديد يتفق مع أحد الاشكال التقليدية للسلوك الإجرامي ، حيث يتم تحويل السلوك في صورته التقليدية إلى صورة أخرى ترتبط بالحاسب الآلي ونظامه ، بإعتبارها المحل الجديد للسلوك الإجرامي ، وعادة ما تتبع أغلب الدول هذه الطريقة.[2]

– وفي بعض التشريعات يتم افراد قانون يعاقب فيه على الجرائم المعلوماتية بكل صورها، ويكون ذلك إما بإصدار تشريع مستقل أو تجميع كل ما يتعلق بالجريمة المعلوماتية في قسم مستقل ملحق بالتشريع الجنائي ، وهذه الطريقة تسمح بتوضيح الطبيعة الخاصة للجريمة المعلوامتية ، كما تسمح بوضع عقوبات خاصة لهذه الجرائم بما يتوافق معها[3] ، ومن أمثلة التشريعات التي تبنت هذه الخطة تشريعات الولايات المتحدة الأمريكية والقانون الإنجليزي.[4]

كما ان بعض الأنظمة القانونية في سبيل توفير الحماية الجنائية للمعلوماتية ، قامت بجمع اكثر من أسلوب من أساليب الصياغة التشريعية المتقدمة ، ويرجع سبب ذلك إلى مدى تأثير هذه الجرائم ووقت تدخل المشرع لمواجهتها ، وتعد السويد من التي واجهت بداية الجريمة المعلوماتية بوضع نص عام يتعلق بالجريمة المعلوماتية ، وبعد ذلك قامت بتعديل قانون العقوبات واضافت نصوص جديدة تنظم الجريمة المعلوماتية قياسا على نصوص قائمة بالفعل في القانون ، مع الإحتفاظ بالنص الاول المتعلق بالجريمة ذاتها . ولهذا الغرض قسمنا هذا المبحث إلى مطلبين :

[1] – لاحظ المشرع الجزائري خطورة افعال الاعتداء على أجهزة الحاسب ونظم المعلومات ، وتدخل لتوفير حماية جنائية لها في ظل القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات ، بإدماج أحكام خاصة بالإجرام المعلوماتي في صلب قانون العقوبات ، فإستحدث نصوص خاصة بالجرائم والإعتداءات الماسة بالانظمة المعلوامتية.

[2] – نائلة عادل أحمد فريد قورة ، مرجع سابق ، ص 311.

[3] – نائلة عادل محمد فريد قورة ، نفس المرجع ، 311.

[4] – أشرف شمس الدين ، الحماية الجنائية للمستند الإلكتروني ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2006 ، ص 09.

مطلب أول نعرض فيه الاطار التشريعي الدولي الأجنبي لجرائم الإعتداء على النظام المعلوماتي . و مطلب ثان نعرض فيه للإطار التشريعي الداخلي لتجريم الإعتداءات على النظام المعلوماتي

على أن تكون هذه المطالب في شكل وصفي للأطر القانونية تاركين التحليل للباب الثاني من هذه الدراسة.

المطلب الأول : نماذج لتشريعات دولية و داخلية في إطار جرائم الإعتداء على النظام المعلوماتي

نتطرق في هذا المطلب لنماذج تشريعية ذات بعد دولي هذا كفرع أول بينما نخصص الفرع الثاني نماذج تشريعية غربية داخلية.

الفرع الأول : نماذج تشريعية دولية لجرائم الإعتداء على النظام المعلوماتي

أولا : قانون الأونستيرال النموذجي بشأن التجارة الإلكترونية

وضعت اللجنة الأممية للقانون التجاري – و هي التي يختصر في تسميتها بالأونسيترال – في اعتبارها أن هذا القانون سيكون أداة فعالة للدول المعنية بتحديث تشريعاتها في اطار التعاملات المرتبطة بتقنية الإتصالات الحديثة[1] ، و لقد طرأ على هذا القانون عدة عمليات تشريعية لتكملته وفق المستجدات الواقعة و لكي يكون قانونا متكاملا ينصح به من طرف اللجنة الأممية للتجارة الإلكترونية للدول للأخذ به دون إلزام منها .

[1] - نظرا لما تتميز به جرائم الاعتداء على النظام المعلوماتي خاصة في أنها عابرة للحدود الدولية، لذلك كان لزاما على المجتمع الدولي توحيد جهوده لمكافحة هذه الجريمة، نظرا لارتكابها من أشخاص قد يكونون منظمين تنظيما إجراميا هذا بالإضافة للخطورة الإجرامية المتزايدة في إطار المساس و الإعتداء على نظم المعلومات، و بتقصي تلك الجهود نجد أنه على المستوى الإقليمي أو الدولي تم عقد عدة مؤتمرات في إطار مواجهة تلك الجرائم التي على إثرها صدر الكثير من التوصيات و من ذلك : المؤتمر السابع للأمم المتحدة الخاص بمكافحة جرائم الحاسب الآلي وفي 1995م عقد المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين في هافانا كانت الجريمة الإلكترونية أحد الموضوعات التي تم بحثها من خلال وضع الأطر القانونية لمكافحتها، كما دعت الوكالات والمؤسسات ذات الطابع الدولي إلى التدخل لحماية المعلومات وعدم الإعتداء عليها، وفي مقدمتها نجد منظمة التنمية والتعاون الاقتصادي.

فالقانون الأول من حيث الصدور كان في 16 ديسمبر 1996 في الجلسة العامة رقم 85 ، و هو يحتوي على 17 مادة حيث عالجت تلك المواد الأتي توضيحه :

– نطاق تطبيق القانون النموذجي بحيث يغطي كل الحالات التي تنشأ فيها المعلومات أو تخزن أو تبلغ بوسائل إلكترونية أو ضوئية أو وسيلة مشابهة ، و المستخدمة في سياق الأنشطة التجارية[1]. كما تم كذلك التعريف بكل المصطلحات ذات الصلة بالموضوع الذي شرع لأجله هذا القانون ،[2] و هي : رسائل البيانات[3] ، و التبادل الإلكتروني لها[4] ، المنشئ و المرسل إليه[5] ، الوسيط[6] ، نظام المعلومات[7] .

– التفسير بحيث يقصد منها أن تقوم المحاكم و غيرها من السلطات الوطنية أو المحلية توفير الإرشاد الى تفسير هذا القانون[8] .

– التغيير بالإتفاق و المقصود منه ألا تنطبق فقط بين المنشئ و المرسل إليهم رسائل البيانات لكن أيضا تشمل الوسطاء ، و عليه يمكن تغيير الفصل الثاني من الجزء الأول من هذا القانون

[1] المادة الأولى من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية .

[2] وائل أنور بندق ، موسوعة القانون الإلكتروني و تكنولوجيا الإتصال و المعلومات ، الطبعة الأولى (2007) ، دار المطبوعات الجامعية ، الإسكندرية ، ص 42-48

[3] الفقرة أ من المادة الثانية من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية الجمعية العامة للامم المتحدة أنظر في ذلك ، فؤاد بنصغير، التجارة الإلكترونية ،النجاح الجديدة ، الطبعة الأولى ، 2011، ص133

[4] الفقرة ب من المادة الثانية من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص133

[5] الفقرتين ج و د من المادة الثانية من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص134

[6] الفقرة هـ من المادة الثانية من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص134.

[7] الفقرة و من المادة الثانية من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص134.

[8] المادة الثالثة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص134

بموجب اتفاقية ثنائية أو متعددة الأطراف ، و إما بموجب قواعد للنظم يتفق عليها الأطراف ، مع تقييد صراحة إستقلالية الأطراف بالحقوق و الإلتزامات الناشئة بينهم[1] .

– الإعتراف القانوني برسائل البيانات بحيث لا ينبغي التمييز بين رسائل البيانات و المستندات الورقية بصرف النظر عن أية إشتراطات قانونية تقتضي وجود "كتابة" أو "محرر أصلي" و هو يمثل مبدأ أساسي عام لا ينبغي قصره على الأدلة القانونية[2] .

– الكتابة التي تيسر الإطلاع على المعلومات أي بشكل مقروء و قابلة للتفسير كضمانة لوجود الدليل الملموس و الذي يؤكد نية الإلتزام لدى الأطراف ، و مساعدة الأطراف على إدراك تبعات إبرامهم للعقد ، فإمكانية قراءته للجميع تكفل بقاء المستند بلا تحريف بمرور الزمن و يوفر سجلا دائما للمعاملات كما أنه يتيح المجال للإستنساخه و لتوثيقه ، و بهذا يكفل أن يكون في شكل مقبول لدى السلطات العامة و المحاكم[3] .

– التوقيع المعترف به في بيئة قائمة على التعاملات الرقمية و هو يقوم مقام التوقيع في التعاملات الورقية و لهذا حددت وظائفه المتمثلة في : تحديد هوية الشخص ، تحديد ما يؤكد يقينا مشاركة ذلك الشخص بالذات في فعل التوقيع ، الربط بين الموقع و المستند . لهذا أعتمد للدلالة على نية الطرف الموقع في الإلتزام بمضمون العقد محل الإبرام ، و على نيته في الإقرار بتحرير النص ، و نية الشخص ربط نفسه بمضمون مستند قد كتبه شخص آخر ، واقعة و زمان وجود شخص في مكان معين[4] .

[1] المادة الرابعة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص135

[2] المادة الخامسة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص135

[3] المادة السادسة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص ص135-136.

[4] المادة السابعة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص136

– الأصل بوصفه واسطة يتم فيها تثبيت المعلومات للمرة الأولى و هي ذات صلة بمستندات الملكية و الصكوك القابلة للتداول ، التي تتسم فكرة الطابع الفريد للأصل ، مع العلم ان مستندات الملكية و الصكوك القابلة للتداول ليست هي الوحيدة التي يتطلب فيها الأصل و من أمثلة الوثائق التي تتطلب الأصل نجد الوثائق التجارية و التي منها وثائق التصديق على الوزن ، و الشهادات الزراعية ، و تقارير التفتيش ،و شهادات التأمين ، ...الخ ، حيث أن إرسالها دون تغيير أي في شكلها الأصلي أمر لابد منه لأطراف التجارة الدولية لتكون التقة في محتوياتها للتقليل من إمكانية حدوث تغيير فيها[1] .

– قبول رسائل البيانات و حجيتها الإثباتية بحييث تعتبر كدليل إثبات في الإجراءات القانونية و أنها ذات قيمة بغض النظر عن شكلها الإلكتروني و هذا في مجال الإختصاص القضائي مع أنها تتميز بالتعقيد و هذا تبعا لما اذا كانت قد انشئت او خزنت أو ابلغت بطريقة يعول عليها[2].

– الإحتفاظ برسائل البيانات بواسطة مجموعة من القواعد البديلة للمقتضيات القائمة بشأن تخزين المعلومات لأغراض مثل المحاسبة أو الضرائب و التي قد تشكل عقبات أمام تطوير التبادل التجاري الحديث ، و هذا من خلال الكتابة[3] ، مع التأكيد على انه لا حاجة للاحتفاظ بالرسالة دون تعديل ما دامت المعلومات التي تم تخزينها تعكس بدقة رسالة البيانات على النحو الذي ارسلت به ، مع تناول جميع المعلومات التي تدعو الحاجة لتخزينها[4] .

[1] المادة الثامنة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص 136 – 137

[2] المادة التاسعة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص 137– 138

[3] المادة العاشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص 138– 139

[4] المادة العاشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص 138– 139

– تكوين العقود و صحتها من خلال تشجيع التجارة الدولية بتوفير المزيد من اليقين القانوني في اطار ابرام العقود بالوسائل الالكترونية ، من خلال توافر العرض و القبول بالوسائل الالكترونية سواءا كانا مجتمعين في رسالة واحدة او منفصلين ، مع امكانية الدولة المشرعة استثناء تطبيق ذلك[1] .

– اعتراف الاطراف برسائل البيانات التي لا تتعلق بأبرام العقود و مثالها الاشعار بالبضائع المعيبة و عروض الدفع و الاشعار بالمكان الذي سينفذ فيه العقد و الاعتراف بالدين ...الخ ، و هذا في اطار اثبات صحة استعمال الوسائل الالكترونية في هذا الصدد[2] .

– اسناد رسائل البيانات بإقامة افتراض بان رسالة البيانات تعتبر في ظروف معينة رسالة من المنشئ ، مع تقييد ذلك الافتراض في حالة ما اذا كان المرسل اليه قد علم او كان ينبغي ان يكون على علم ، بان الرسالة ليست رسالة المنشئ[3] .

– الاقرار بالاستلام و هو قرار تجاري يتخذه مستعملو وسائل التجارة الإلكترونية و هذا لا ثبات استلام رسالة البيانات [4].

– زمان و مكان ارسال و تلقي رسائل البيانات عن طريق تحديد وقت الارسال بدخول الرسالة في النظام المعلوماتي و متى كانت متوفرة للمعالجة داخله و لا يهم ان كانت مفهومة او قابلة

[1] المادة الحادية عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة)، نفس المرجع السابق، ص139

[2] المادة الثانية عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة)، نفس المرجع السابق، ص139

[3] المادة الثالثة عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة)، نفس المرجع السابق، ص 140-141

[4] المادة الرابعة عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة)، نفس المرجع السابق، ص 142-143.

للاستعمال من جانب المرسل اليه ام لا . كما تم تناول مكان تلقي الرسالة كأن يكون مكان العمل الرئيسي او مكان اخر[1] .

- الأفعال المتصلة بنقل البضائع و مستندات النقل[2] .

ثانيا : قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001

يطبق هذا القانون حيثما تستخدم التوقيعات الإلكترونية في سياق الأنشطة التجارية و هذا لا يلغي أي قاعدة قانونية يكون القصد منها حماية المستهلكين حيث عرفت المادة الأولى منه الفقرة أ، التوقيع الإلكتروني بأنه "بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة اليها أو مرتبطة بها منطقيا و التي يجوز أن تستخدم لتعيين هوية الموقع بالنسبة الى رسالة البيانات و لبيان موقفه و لبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات ".

كما يعرف الشهادة بانها رسالة بيانات او سجلا اخر يؤكد ان الارتباط بين الموقع و بيانات انشاء التوقيع ، في حين تعرف رسالة البيانات بانها معلومات يتم انشاؤها او ارسالها او استلامها او تخزينها بوسائل الكترونية او ضوئية او بوسائل متشابهة ، بما في ذلك على سبيل المثال لا الحصر ، التبادل الالكتروني للبيانات او البريد الالكتروني او البرق او التلكس او النسخ البرق . أما الموقع فهو الشخص الحائز على بيانات انشاء التوقيع و يتصرف اما بالأصالة عن نفسه و اما بالنيابة عن من يمثله ، بينما مقدم خدمة التصديق هو الشخص المصدر للشهادات و يجوز ان يقدم خدمات اخرى ذات صلة بالتوقيعات الالكترونية .

[1] المادة الخامسة عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة)، نفس المرجع السابق، ص 144- 145

[2] المادتين السادسة عشرة و السابعة عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص 146-148

و الطرف المعول هو الشخص الذي يجوز له ان يتصرف استنادا الى شهادة او الى توقيع الكتروني[1].

[1] المادة الثانية (الفقرات ب- ج – د – هـ – و) من القانون الاونسيترال النموذجي بشان التوقيعات الالكترونية لسنة 2001 حيث تتعدد صور التوقيع الإلكتروني ما بين التوقيع البيومتري والتوقيع الرقمي والتوقيع بالقلم الإلكتروني وتعتبر الصورة الأولى طريقة التحقق من الشخصية عن طريق الاعتماد على الخواص الفيزيائية و السلوكية للأفراد وتستخدم للتحقق من الشخصية عن طريق الاعتماد على الخواص الفيزيائية و السلوكية للأفراد وتستخدم هذه التقنيات بواسطة أجهزة الأمن والمخابرات وتتمثل هذه الطرق البيومترية الآتية: البصمة الشخصية ، مسح العين البشرية ، التحقق من ميزة للصوت ، التعرف على الوجه البشري ، خواص اليد البشرية ، التوقيع الشخصي...الخ. بينما التوقيع الرقمي : بأنه قيمة عددية تعمم بها رسالة البيانات حيث تجعل من الممكن استخدام إجراء رياضي معروف يقترن بمفتاح الترميز الخاص بمنشئ الرسالة والقطع بأن هذه القيمة العددية قد تم الحصول عليها باستخدام ذلك المفتاح،في حين التوقيع بالقلم الإلكتروني يتم باستخدام قلم إلكتروني يمكن بواسطته الكتابة على شاشة الحاسوب مباشرة باستخدام برنامج معين ، ويقوم هذا البرنامج بوظيفتين الأولى خدمة التقاط التوقيع والثانية خدمة التحقق من صحته وعندما يقوم المستخدم بتحريك القلم على الشاشة وكتابة توقيعه يلتقط البرنامج حركة البدء ويظهر هذا التوقيع على الشاشة لتمييز صفة الموقع كما هو الأمر في الكتابة العادية. هذا بالإضافة إلى التأكيد على أنه لا ينبغي أن يكون إختلاف في المعاملة بين الرسائل الموقعة إلكترونيا و المستندات الورقية التي تحمل توقيعا خطيا تطبيقا لمبدأ عدم التمييز. و في اطار إستخدام التوقيع الإلكتروني و لضمان سرية التعاملات تم تفعيل التشفير لتأمين التوقيع و عدم المساس أو الإعتداء على المعلومات الإلكترونية، الذي يعني عملية تحويل المعلومات إلى رموز غير مفهومة تبدو غير ذات معنى بحيث يمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومة أو فهمها و هي تنطوي على تحويل النصوص العادية لنصوص مشفرة للحفاظ على سلامتها من عبث القراصنة. ويسمح هذا النظام لتحييد المخاطر المتوقعة من استخدام الطرق الإلكترونية في المعاملات التجارية حيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها ، فالتشفير يساعد على حفظ سرية المعلومات والتوقيع الإلكتروني الذي يتطلب الحفاظ على الأرقام و الرموز لحمايته داخل التجارة الإلكترونية لكي لا يستطيع أي شخص الاطلاع على هذه البيانات غير المتعاقدين أو من يصرح له قانونا بذلك كما يهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات ومن تم منع وصولها مشوهة للطرف الآخر في المعاملات التجارية على نحو يعرقلها، وهو نوعان :نظام التشفير المتماثل أو المتناظر وهو أسلوب يستخدم فيه مفتاح سري لتشفير رسالة ما وفك تشفيرها ويسمى بالمفتاح المتناظر لأن المفتاح الذي يستخدم لتشفير الرسالة هو نفسه المستخدم لفك تشفيرها ، لكن هذه الطريقة تتطلب إحالة المفتاح بين الأطراف بطريقة يجب أن تضمن سلامته وتعطي هذه التقنية حماية أكثر في الشبكة المغلقة أما النوع الثاني و هو نظام التشفير اللامتماثل و اللامتناظر وهو أسلوب يتم فيه تشفير البيانات باستخدام مفتاح ما وفك تشفيرها باستخدام مفتاح آخر ولهذا السبب يسمى باللامتناظر فالتشفير المتناظر تشفر الرسالة أو التوقيع باستخدام الرقم العام وفي نفس الوقت يتم فك الشفرة وإرجاع المعلومات إلى وضعها الأصلي باستخدام نفس الرقم العام ولو حصل أن شخص آخر يعرف هذا الرقم أو توصل إليه عن طريق الدليل العام فبإمكانه فك الشفرة وقراءة الرسالة أو التوقيع. أما إذا تم تشفير المعلومات بأسلوب التشفير اللامتناظر فإن المعلومات يتم تشفيرها بالرقم العام ولكن لا يمكن فك الشفرة والوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تم على أساسه التشفير.

ثالثا : الاتفاقية الدولية الخاصة بالإجرام المعلوماتي المبرمة ببودابست 2001

– تطرقت هذه الاتفاقية للتعاريف الخاصة بأغراض هذه الاتفاقية فعرفت منظومة الكمبيوتر بأنه أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات الصلة بذلك ويقوم أحد أو أكثر منها عن طريق البرامج بعمل معالجة آلية للبيانات .

– بينما يقصد ببيانات الكمبيوتر أي عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج الذي يؤدي لتأدية المهام داخل المنظومة .

– في حين يقصد بجهاز الخدمة أي كيان عام أو خاص لمستخدمي الخدمة الحاصة بهم والذي له القدرة على الاتصال بواسطة منظومة الكمبيوتر، أو أي كيان آخر يقوم بمعالجة أو تخزين بيانات الكمبيوتر نيابة عن خدمة الاتصالات أو مستخدمي هذه الخدمة.[1]

– كما تقوم كل دولة طرف في هذه الاتفاقية بإقرار الإجراءات التشريعية وغيرها من الإجراءات كلما كان ذلك ضروريا لإصدار نصا قانونيا أو تشريعيا الذي يشكل قاعدة لتجريم سلوكات الإعتداء على البيانات في إطار إذا ما تعلق بإتلافها أو إلغائها أو إفسادها أو تغييرها أو تدميرها دون وجه حق [2] .

– و تم تعريف التدخل غي المشروع في منظومة المعالجة الآلية للمعطيات بأنه أي سلوك من السلوكات السابقة الذي يرتكب عن قصد للإعاقة الخطية دون وجه حق لعمل منظومة الكمبيوتر[3].

[1]– المادة 1 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[2]– المادة 4 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[3]– المادة 5 من الاتفاقية الدولية للإجرام المعلوماتي 2001

– في حين تطرقت هاته الإتفاقية لإقرار الإجراءات التشريعية وغيرها من الإجراءات الاخرى كلما كان ذلك ضروريا من خلال النصوص التشريعية أو القانونية التي تصدر من طرف المشرعين الوطنيين وذلك في إطار تجريم الإنتاج أو البيع أو الحصول بغرض الإستخدام أو التوفير لجهاز يشمل برنامج كمبيوتر يتم تصممیه أو تطويعه أساسا بغرض إرتكاب أية من الجرائم المنصوص عليها في إطار المادة الثانية من هاته الإتفاقية و المواد ثلاثة وأربعة وخمسة منها، كذلك كلمة السر الخاصة بالكمبيوتر أو الكود الشيفري للدخول أو بيانات مماثلة تمكن الدخول لمنظومة المعلومات بأكملها أو أي جزء منها بقصد استخدام الجهاز في أغراض خاصة لارتكاب أية من الجرائم الواردة بالمواد من إثنان إلى خمسة، كذلك حيازة إحدى القطع المشار إليها سابقا بقصد استخدامها في أغراض الخاصة بارتكاب جرائم الواردة في المواد أعلاه [1] .

– و تقوم كل دولة طرف في هذه الاتفاقية بإقرار النصوص القانونية التي تشرع تجريم التزوير المتعلق بالكمبيوتر و تجريم التدليس المتعلق بالكمبيوتر كذلك الأعمال الإباحية وصور الأطفال الفاضحة، الإنتهاكات الخاصة بحقوق الطبع والنشر والحقوق المتعلقة بهما[2].

– وتقوم كل دولة طرف في هذه الاتفاقية كذلك بإقرار النصوص القانونية التي تجرم المساعدة أو التحريض أو الشروع في ارتكاب أية جريمة من الجرائم السابقة الذكر عن قصد، دون إغفال تجريم الشخص المعنوي الذي يرتكبها بموجب سلطة تفويض أو سلطة ممارسة السيطرة والتحكم طبقا للمبادئ والأسس القانونية الخاصة للدولة [3].

– وعليه تضمن كل دولة من خلال إقرارها للإجراءات التشريعية المعاقبة على الجرائم السابقة الذكر بموجب عقوبات فعالة ومتناسبة تدعو للعدول عنها والتي قد تشمل الحرمان من الحرية وأي

[1]– المادة 6 من الاتفاقية الدولية للإجرام المعلوماتي 2001، يجوز لكل دولة طرف في هذه الإتفاقية التحفظ على الفقرة 1 من هذه المادة ى بشرط ألا يكون هذا التحفظ متعلق بعمليات البيع أو التوزيع .

[2]– المواد 6،7،8،9،10 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[3]– المادتين 11، 12 من الاتفاقية الدولية للإجرام المعلوماتي 2001

إجراء جنائي أو غير جنائي يتوافق مع متطلبات الردع في إطار السياسة الجنائية الحكيمة والراشدة المنتهجة في كل دولة[1].

– وفي هذا الإطار تم النص على مجموعة من الإجراءات بما في ذلك تجميع الأدلة الخاصة بالجريمة في صورتها الإلكترونية من خلال ضبط الإجراءات التحقيقية وفق إمكانية كل دولة كما أنه تم الاعتماد على الإجراءات الوقائية[2]، كما تم التأكيد على سرعة المحافظة على بيانات الكمبيوتر المخزنة و إصدار الأوامر من خلال منح السلطات المختصة وحق التفويض في توجيه الأوامر التي يمكن من خلالها التوصل لنوعية خدمة الاتصال أو المراسلة المستخدمة والشروط الفنية التي يتم اتخاذها في ذلك والفترة الزمنية للخدمة، بالإضافة إلى ذلك البيانات الشخصية للمشترك، عنوانه البريدي أو الجغرافي...الخ، وأي معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الإتصالات.

– كما أنه تم إقرار الصلاحيات القانونية للبحث ومصادرة بيانات الكمبيوتر المخزنة تجميعها في الوقت الصحيح.[3]

– ولتقوية مجال الإجراءات وتوضيحه لكي تكون كل دولة طرف في هاته الاتفاقية على بينة من أمرها تم إقرار حق كل دولة طرف في الاتفاقية بإصدار الإجراءات التشريعية ليشمل أي جريمة ترتكب على أراضيها أو على متن إحدى السفن التي تحمل تلك الدولة الطرف أو بإحدى الطائرات المسجلة بموجب قوانينها أو بمعرفة أحد مواطنيها.[4]

– في حين ختمت هاته الاتفاقية بمبادئ عامة تتعلق بالتعاون الدولي في إطار تسليم المجرمين والمساعدات المتطلبة في إطار الإجراءات.[5]

[1]– المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[2]– المادتين 14، 15 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[3]– المواد 16، 21 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[4]– المادة 22 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[5]– المواد 22– 48 من الاتفاقية الدولية للإجرام المعلوماتي 2001

الفرع الثاني : نماذج تشريعية غربية داخلية في إطار جرائم الإعتداء على النظام المعلوماتي

أولا: النظام القانوني الأمريكي لمكافحة جرائم المعلوماتية

ينظم جرائم المعلوماتية في الولايات المتحدة الأمريكية مجموعة من التشريعات على المستوى الفدرالي وكذلك على المستوى المحلي في مختلف الولايات.

أ – على المستوى الفدرالي

يمثل الفصل (18) من قانون الولايات المتحدة التشريع الرئيس لجرائم التقنية الحديثة ، فقد استجاب الكونغرس لمشكلة جرائم تقنية المعلومات من خلال سن العديد من القوانين الفدرالية كان أولها قانون الاحتيال واساءة استخدام الكمبيوتر (Computer Fraud and Abuse Act)(CFAA) عام 1984 وتم تعديله عام 1986 ومن ثم عدل عام 1994 من أجل التعامل مع مشكلة (الشيفرة الخبيثة) وغيرها من البرامج والتي تهدف إلى تغيير أو اتلاف أو تدمير البيانات على نظام الحاسب.

وينص القسم (1030) من الفصل (18) من قانون الولايات المتحدة على اعتبار الافعال التالية مجرمة :

- التوصل غير المصرح به (الدخول) إلى أحد أنظمة الحاسب للحصول على معلومات أمنية وطنية مع وجود نية لضرر للولايات المتحدة أو لمنفعة دولة أجنبية.
- التوصل غير المصرح به (الدخول) إلى أحد انظمة الحاسب للحصول على معلومات خاصة بأموال محمية.
- التوصل غير المصرح به (الدخول) إلى نظام خاص بالحكومة الفدرالية الأمريكية.
- الدخول غير المصرح به إلى اي نظام مع نية الاحتيال.

- الدخول غير المصرح به إلى اي نظام محمي[1] مع تعمد الحاق اضرار به.

- الاتجار الاحتيالي في كلمات السر الحاسوبية وغيرها من المعلومات التي يمكن استخدامها لإكتساب الوصول إلى نظام محمي.

- الاتجار الاحتيالي في كلمات السر الحاسوبية وغيرها من المعلومات التي يمكن استخدامها لإكتساب الوصول إلى نظام محمي.

- بث أو تهديد بإرتكاب ضرر لأي نظام محمي عبر الولايات أو للتجارة الأجنبية بغرض ابتزاز أموال أو منافع من أي شخص طبيعي أو معنوي.

- ويحضر القسم (1462) من الفصل (18) من قانون الولايات المتحدة ، استخدام نظام الحاسب لإستيراد مواد مخلة بالآداب إلى داخل داخل الولايات المتحدة الامريكية، ويحضر القسم (1463) نقل أية مواد فاحشة عبر الولايات أو الجهات الخارجية.

ويجرم القسم (2251) من الفصل (18) توظيف أي قاصر أو اغرائه في المشاركة في أنشطة جنسية بما فيها خلق وتصوير مواد وبثها لجهات خارجية ، أو استخدام نظام الحاسب للإخلال برعاية قاصر بقبول استغلاله مع العلم في انتاج مواد تنطوي على استغلال جنسي . أما القسم (1028) من الفصل (18) من قانون الولايات المتحدة فإنه يعتبر انتاج أو نقل ادارة جهاز يتضمن نظام حاسب يقصد استخدامه بتزوير الوثائق أو انتاج وثائق تعريف مزورة جريمة تعتبر المادة (2319) من ذات القسم الاخلال بحق المؤلف جريمة فدرالية.

كما أصدر الكونغرس عام 2003 قانون مكافحة البريد الإلكتروني غير المرغوب فيه (Anti Spam Law) (The CAN-SPAM ACT of 2003) الذي دون في قسم (1037) من الفصل ((18) من قانون الولايات المتحدة. ويحظر هذا القانون ارسال الرسائل غير المرغوب فيها

[1] – عرف مصطلح نظام الحاسب المحمي في القانون الفدرالي الأمريكي بأنه الإصطلاح يطلق على نظام الحاسب الذي يستخدم في مؤسسة مالية أو تستخدمه حكومة الولايات المتحدة الامريكية أو يستخدم في التجارة فيما بين الولايات أو في التجارة الخارجية أو الاتصال.

كما ينص على أنه يجب أن تشمل رسائل البريد الإلكتروني آلية تتيح للمتلقي الإشارة إلى أنه لا يريد استقبال هذه الرسائل من المستقبل ، ويهدف هذا القانون أيضا إلى القضاء على عادة الحصول على عناوين البريد الإلكتروني من مواقع الأنترنت.

ب – على مستوى الولايات

ان الاطار العام لتشريعات الولايات المتحدة في حقل جرائم المعلوماتية يمثل بما يلي :

– كل ولاية من الولايات الخمسين تملك حرية التشريع الخاص بها وليس هناك آلية على مستوى الولايات أو المستوى الفدرالي تتطلب تبني الولايات شكلا أو محتوى محددا لقوانينها بالرغم من وجود مشاريع توحيد ومحاولات تصريحات تهدف إلى توحيد التدابير التشريعية ، وقد سنت جميع الولايات قوانين خاصة أو عدلت قوانين العقوبات لديها بما يكفل النص على تجريم أنشطة جرائم تكنولوجيا المعلومات الحديثة ، مع تباين فيما بينها سواء من حيث صور النشاط المجرم ، أو من حيث آلية التعامل مع محل الاعتداء .[1]

– ان الاطار العام لتوحيد قوانين جرائم تقنية المعلومات يعتمد على مشروع قانون نموذجي (Model state computer crimes code) تم وضعه من قبل هيئة أكاديمية عام 1998 ، وفي نطاقه تم تقسيم جرائم التقنية الحديثة إلى الجرائم الواقعة على الاشخاص ، والجرائم الواقعة على الاموال عدا السرقة ، وجرائم السرقة والاحتيال ، وجرائم التزوير ، وجرائم المقامرة والجرائم ضد الآداب عدا الجرائم الجنسية ، والجرائم ضد المصالح الحكومية

[1] – رشاد خالد عمر، المرجع السابق، ص 44-45.

وهذا التقسيم يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدف الاعتداء.[1]

وبإستعراض مواقف التشريعات القائمة والنافذة في الولايات الأمريكية ، نجد أن عددا قليلا من الولايات تعاملت مع الجرائم التي تستهدف الاشخاص من غير الجرائم المتعلقة بالمحتوى النفسي ، فلا يوجد أية ولاية نصت على جريمة تقنية حديثة تتعلق بقتل الاشخاص. أما ولايتا (فرجينيا) (وكاليفورنيا) فقد اعتبرا استخدام نظام المعلومات الإلكترونية بدون تصريح بنية الحاق الضرر المادي بالأفراد جريمة من بين جرائم التقنية الحديثة.[2]

وقد اعتبر 16 ولاية من بين الولايات الامريكية أن كل التهديدات والمواد التي تثير الاحقاد من قيل الافعال الجرمية ومن معظمها تتطلب أن يكون الجاني قد نقل تهديدا ممكن تطبيقه وممكن تصديقه لإلحاق اصابة بشخص أو ضرر به أو بعائلته أو بأي شخص آخر. وبعضها اعتبر من بين جرائم السلوك أو المساهمة في ارتكاب سلوك قد يؤدي بالشخص العادي
(A reasonable Person) للمعاناة من التهديد أو التعرض لإزعاج حقيقي أو أي ضرر أخر وكذلك الخوف من الإصابة أو الموت على نفسه أو أي من أفراد عائلته. بعضها جرم الإتصالات التي تتضمن مواد بذيئة بأية واسطة الكترونية تستهدف تهديد شخص أو الحاق ضرر به أو بعائلته

[1] – الجرائم الجنسية التي تستهدف الاشخاص : وتشمل حض وتحريض القاصرين على انشطة جنسية غير مشروعة وافساد القاصرين بأنشطة جنسية عبر الرسائل الإلكترونية وتلقي أو نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة والتحرش الجنسي بالقاصرين عبر الكمبيوتر والرسائل التقنية ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام وللقاصرين تحديدا ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الأنترنت وتصوير أو اظهار القاصرين ضمن أنشطة جنسية واستخدام الانترنت لترويج الدعارة بصورة قسرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم والحصول على الصور والهويات بطريقة غير مشروعة لإستغلالها في انشطة جنسية ، وبإمعان النظر في هذه الاوصاف نجد أنها تجتمع جميعا تحت صورة واحدة وهي استغلال تقنية المعلومات الحديثة لترويج الدعارة وإثارة الفحش واستغلال الأطفال القصر في أنشطة جنسية غير مشروعة.

طائفة جرائم الأموال – عدا السرقة – أو الملكية المتضمنة أنشطة الإختراق والإتلاف: وتشمل أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة إما مجردا أو لجهة ارتكاب فعل أخر ضد البيانات والبرامج والمخرجات .....

[2] – المادة 15207 –1802 من قانون عقوبات ولاية فرجينيا (VA. CODE. ANN). والمادة 502 من قانون عقوبات ولاية كلفورنيا.

ويشمل ذلك استخدام لغة فاحشة ، وقد اعتبر محكمة نيويورك أن هذا النص ينطبق على رسائل التهديد والذم التي ترسل عبر الانترنت.

بالإضافة إلى الافعال الجرمية سابقة الذكر ، فإن معظم الولايات الأمريكية تضمنت قوانينها موادا تتعلق بالأفعال التي تستهدف استغلال أو اغواء القصر أو تتعلق بدعارة الأطفال.

وقد اهتمت كافة الولايات الامريكية بشكل أساسي بجرائم تقنية المعلومات المتصلة بالإختراق والحاق رالضرر بالنظم والشبكات والمعطيات جراء هذه الانشطة ، وتنقسم التدابير التشريعية المتصلة بالإختراق إلى طائفتين : طائفة تشريعات انتهاك الحرمة (Trespass) ، وطائفة الهاكرز (Hackers) التي تقوم بأنشطة اختراق وانتهاك الحرمة دون تصريح (Hacking) ، وطائفة الكريكرز (Crackers) التي تقوم بهجمات التدمير انطلاقا من دوافع الحقد (Cracking).

ومعظم الولايات تتوفر لديها تشريعات تعتبر الدخول إللى نظم الكمبيوتر أو الشبكات بدون ترخيص جريمة ، وهي ما تعرف بتشريعات الـ (Hacking) ، وكذلك فإن معظم الولايات وضعت تشريعات تحضر هجمات التدمير وتعتبرها أكثر خطورة من أنشطة الدخول غير المصرح به ، وبعض الولايات مثل ولاية نيويورك تعتبر مجرد اختراق نظام الحاسب بنية ارتكاب أو محاولة ارتكاب أي جريمة بمثابة جريمة معاقب عليها.

وأكثر من ذلك اعتبرت بعض الولايات جرائم تقنية المعلومات انكار أو قطع أو اعاقة خدمة نظام حاسب أو التسبب في تعطيل هذه الخدمة أو منع الدخول للنظم.

واعتبرت ولاية شمال كارولينا أن التهديد بتدمير نظام الحواسب بقصد الحصول على مال أو أية منفعة للشخص أو لشخص آخر أو التسهيل له ارتكاب أي فعل ارتكابا لجريمة تقنية المعلومات.[1]

[1] -نعيم مغبغب ، المرجع السابق، ص 270 .

كما جرمت معظم الولايات استخدام نظام المعلومات الكتروني يقصد الاعتداء على خصوصية البيانات أو الرقابة أو جميع المعلومات عن الموظفين أو السجلات الوظيفية عن الموظفين أو السجلات الطبية أو الرواتب او القروض أو أي معلومات مالية شخصية. كما جرمت غالبية الولايات الأمريكية استخدام تقنية المعلومات الحديثة لإرتكاب الاحتيال ، كما يلاحظ اعتماد بعض الولايات ادماج احتيال تكنولوجيا المعلومات ضمن نصوص الإحتيال التقليدية المقررة في قوانين هذه الولايات بدل وضع نصوص تشريعية مستقلة بشأن احتيال تقنية المعلومات الحديثة.

أما بالنسبة للأفعال الأخرى التي تستهدف الأخلاق والآداب العامة ، فإن ولاية أمريكية واحدة فقط جرمت المقامرة على الخط وهي ولاية (Louisiana) فقد اعتبرت هذه الولاية المقامرة بواسطة نظام الحسب جريمة ، ويتضمن ذلك القيام بأي سلوك أو المشاركة بسلوك يتضمن اللعب كالمضاربات بأنواعها تحت خطر خسارة ذلك الشخص أي قيمة ، وذلك بإستخدام أي من وسائط تقنية المعلومات الحديثة.

وبالنسبة للجرائم ضد الحكومة ، اعتبرت العديد من الولايات الأمريكية من قبيل جريمة تقنية المعلومات الحديثة استخدام أي من وسائط لتعطيل تطبيق القانون أو تعطيل خدمة حكومية ، فعلى سبيل المثال حظر استخدام نظام الحاسب للتسبب بتعطيل أو قطع أي خدمة أو أية عملية أو اجراءات حكومية محلية أو انشطة المؤسسات العامة. والعديد من الولايات جرمت استخدام نظام الحاسب لتعطيل أو قطع أي خدمة أساسية، ويشمل ذلك خدمات المؤسسات العامة والخاصة ذات النفع العام والخدمات الطبية وخدمات الاتصال وكافة خدمات الحكومية، ويشمل أيضا تعريض الأمن العام للخطر.[1]

واعتبرت بعض الولايات استخدام نظام الحاسب للحصول على معلومات تعتبرها الدولة أو أي دائرة سياسية من قبيل المعلومات السرية ، جريمة من جرائم تقنية المعلومات الحديثة،

[1]- نفس المرجع السابق ، ص 271 .

والعديد من الولايات جرمت الدخول غير المصرح به إلى أية معلومات مخزنة داخل نظام حاسب مملوك أو متصل بجهات التشريع بالولاية. كذلك جرمت العديد من الولايات استخدام نظام الحاسب لتدمير أي دليل بقصد تعطيل أي تحقيق رسمي ، كما اعتبرت غالبية الولايات الأمريكية عدم ابلاغ عن جريمة تقنية المعلومات بمثابة جريمة. [1]

ثانيا : النظام القانوني الفرنسي لمكافحة جرائم المعلوماتية

ان التجربة الفرنسية في مجال مكافحة جرائم المعلوماتية ليست أقل نضجا من التجربة الامريكية بل هي كذلك تعتبر من أوائل الدول التي تعاملت مع جرائم تقنية المعلومات تعاملا واقعيا ، بحيث استجابت مبكرة لما تتطلبه مكافحة هذه الظاهرة من خلال التدابير التشريعية[2].

أ – الجرائم التي تقع مباشرة على تكنولوجيا المعلومات والاتصال

نص المشرع الفرنسي على الجرائم التي تقع مباشرة على تكنولوجيا المعلومات والاتصال ، وهي الجرائم المتعلقة بأنظمة المعالجة الآلية للبيانات وسرية وسلامة وتوافر البيانات والمعلومات المعالجة آليا. وبهذا الخصوص جرم المشرع الفرنسي الافعال التالية :

---

[1] - نفس المرجع السابق ، ص 271 .

[2] وقد تقدم وزير العدل الفرنسي سنة 1985م بمشروع قانون عقوبات جديد أضاف إلى الكتاب الثالث منه بابًا تحت عنوان " les infractions en matière informatique" يتكون من 8 مواد تتعلق بتجريم الاعتداء على البرامج أو المعطيات أو أي عنصر أخذ من النظام المعلوماتي أو استخدام أو نقل أو إنتاج برامج أو معطيات أو أي عنصر آخر من نظام المعالجة عن طريق الاستخدام غير القانوني لهذه الأنظمة ، ولكن هذا المشروع لم ير النور...، وفي سنة 1986 تقدم بعض النواب بمشروع قانوني حول الغش المعلوماتي Fraude de Informatique و دارت حوله مناقشات مطولة دامت قرابة عام و نصف ليخرج في الأخير في شكل مختلف عن مقترح النواب و بصورة مشابهة للمشروع الذي قدمه وزير العدل سنة 1985. وقد تم دمج هذا المشروع في قانون العقوبات الفرنسي ليشكل الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات و بذلك نص على الجرائم المعلوماتية في المواد 462/2-9/462 و قد تضمنت هذه المواد تجريم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو حتى جزء منه، وتشدد العقوبة في حالة محو أو تعديل المعطيات الموجودة داخل النظام أو إفساد وظيفته...، كما جرم كل من أدخل معطيات في النظام أو محو أو تعديل المعطيات الموجودة أو في طرق معالجتها أو نقلها أو المساس بأداء النظام لوظيفته، وكذا تزوير المستندات المعالجة آليا أو إستعمالها....،لتفاصيل أكثر أنظر عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، 2004، ص19-20 ..ينظر أيضا، عبد القادر القهوجي، المرجع السابق، ص39-41.

1- الهجمات على النظم المؤتمتة لمعالجة البيانات :

حيث جرم كل من :

- الدخول غير المشروع أو الوصول الاحتيالي إلى نظام آلي لمعالجة البيانات (المادة 323-1 من قانون العقوبات الفرنسي الجديد).

- فعل عرقلة أوتشويه وظيفة النظام الآلي لمعالجة المعلومات.[1]

-ادخال أو حذف أو التعديل الاحتيالي للبيانات الموجودة في نظام آلي لمعاجلة البيانات.[2]

- المشاركة في مجموعة أو الاتفاق على ارتكاب فعل من الأفعال المعاقب عليها في المواد السابقة.[3]

- بالإظافة إلى ذلك نص قانون العقوبات على معاقبة محاولة ارتكاب فعل من الافعال سابقة الذكر[4] ، وعلى المسؤولية الجنائية للأشخاص الإعتباريين.[5]

2 – انتهاك حقوق الاشخاص الناشئة من الملفات أو البيانات الشخصية المعالجة معلوماتيا

حيث نجده جرم كل من الأفعال التالية :

- فعل معالجة بيانات شخصية آليا من دون أخذ الاحتياطات اللازمة للحفاظ على أمن هذه المعلومات [6].

- جمع البيانات الشخصية عن طريق الاحتيال أو باية وسيلة غير مشروعة[7] .

[1] - المادة 323-2 من قانون العقوبات الفرنسي الجديد.

[2] - المادة 323-3 من قانون العقوبات الفرنسي الجديد.

[3] - المادة 323-4 من قانون العقوبات الفرنسي الجديد.

[4] - المادة 323-7 من قانون العقوبات الفرنسي الجديد

[5] - المادة 323 -6 من قانون العقوبات الفرنسي الجديد.

[6] - المادة 226-17 من قانون العقوبات الفرنسي الجديد.

[7] - المادة 226-18 من قانون العقوبات الفرنسي الجديد.

– فعل انشاء أو حفظ بيانات شخصية في شكل الكتروني دون موافقة صريحة من الشخص ؤالمعني ، بحيث أن هذه البيانات تكشف عن الأصول العرقية أو الآراء السياسية أو الفلسفية أو الدينية أو النقابية أو عادات الاشخاص [1].

– الإبقاء على معلومات في شكل الكتروني لمدة تتجاوز المدة المستوجبة لطلب اذن أو تصريح مسبق لتنفيذ المعالجة الآلية[2].

– اساءة استخدام المعلومات اثناء تسجيلها أو تصنيفها أونقلها أو أي شكل آخر من أشكال المعالجة الآلية[3].

– الكشف عن البيانات الشخصية المعالجة آليا التي تؤثر على اعتبار الشخص أو خصوصيته[4].

3– خرق قواعد التشفير (قانون 29 كانون الأول 1990)

ب– الجرائم الواقعة بإستخدام تكنولوجيا المعلومات والإتصالات :

نص المشرع الفرنسي على الجرائم الواقعة بإستخدام تكنولوجيا المعلومات والإتصال أي الجرائم التي تتم من خلال استخدام غير مشروع لتقنية المعلومات الحديثة.

1– الجرائم الواقعة ضد الاشخاص :

– الإعتداء على القصر : أصدر المشرع الفرنسي بعض النصوص لمكافحة وضع الاعتداءات الجنسية وحماية القصر ضحايا هذه الجرائم ، وذلك عندما تستخدم في ارتكاب الجريمة وسائل تكنولوجيا المعلومات والإتصالات (تقنية المعلومات الحديثة) ، فنصت المادة 227–23 من قانون

[1] - المادة 226–19 من قانون العقوبات الفرنسي الجديد.

[2] - المادة 226–20 من قانون العقوبات الفرنسي الجديد.

[3] - المادة 226–21 من قانون العقوبات الفرنسي الجديد.

[4] - المادة 226–22 من قانون العقوبات الفرنسي الجديد.

العقوبات الفرنسي الجديد على تجريم افعال نشر أو تثبيت أو تسجيل أو نقل الصور الإباحية للقاصرين.[1]

كما نصت المادة 225-7 من قانون العقوبات الفرنسي الجديد على تجريم فعل القوادة Proxenetisme المتعلقة بالقاصرين بإستخدام وسائل تكنولوجيا المعلومات والإتصالات.

و هذا بالإضافة لما نصت عليه المادة 227-4 من قانون العقوبات الفرنسي الجديد على تجريم فعل تعريض القصر للخطر ؤعبر تصنيع أو نقل او تثبيت أو تداول اي محتوى ذو صفة عنيفة أو إباحية أو ذو طبيعة تسبب ضررا خطيرا لطرامة الانسان ، من المحتمل أن يشاهدها أو يتداولها قاصر بإستخدام تقنيةالمعلومات الحديثة.

- جرائم التهديد و الإعتداء على حرمة الحياة الخاصة .[2]

- الإعتداء على السمعة والتشهير ، القذف Diffamation غير العلني [3] ، السب Injure غير العلني .

- جريمة افشاء الاسرار (المادة 226-13 من قانون العقوبات الفرنسي الجديد).

2- الجرائم الواقعة على الأموال :

- جرائم الاحتيال المادة 313-1 وما يليها من قانون العقوبات الفرنسي الجديد

- جريمة الإتلاف المادة 322-12 من قانون العقوبات الفرنسي الجديد.

3- الجرائم الواقعة بإنتهاك قانون الصحافة (قانون 29 تموز 1881 بصيغته المعدلة).

- التحريض على الجرائم والمخالفات (مادة 23 و 24)

- الدفاع عن ارتكاب جرائم ضد الإنسانية (مادة 24)

[1] - المادة 216-2/1 من قانون العقوبات الفرنسي الجديد .

[2] - المادة 217-7 من قانون العقوبات الفرنسي الجديد

[3] - المادتين 226-10 و 624-3 من قانون العقوبات الفرنسي الجديد

- التمجيد والتحريض على الإرهاب (مادة 24).
- التحريض على الكراهية العرقية (مادة 24).
-التشهير والإهانة (المواد 30 ، 31 ، 32).

4 – الواقعة بإنتهاك قانون الملكية الفكرية.

- عمل الفكري بما في ذلك البرمجيات والصوت والضصورة (مادة 335-3/2).
- التعدي على تصميم أو نموذج (مادة 521-4)
- التعدي على العلاقات التجارية (مادة 716-9)

5– هتك أو ادارة أو المشاركة في مشروع قمار عبر شبكة الأنترنت.

(مادة 1 من قانون 12 تموز 1983 المعدل بقانون 16 كانون الأول 1992).

6– الجرائم المرتكبة بإنتهاك قانون الصحة العامة

- الإتجار بالمخدرات عبر وسائل تقنية المعلومات الحديثة.
- بيع الأدوية عبر وسائل تقنية المعلومات الحديثة دون الحصول على إذن.

المطلب الثاني : نماذج تشريعية عربية في إطار جرائم الإعتداء على النظام المعلوماتي

على المستوى العربي ، سنقتصر في دراسة الحركة التشريعية في شأن مواجهة جرائم المعلوماتية ، على نماذج تشريعية نبدأها بالقانون العربي الاسترشادي لمكافحة جرائم تقنية المعلموات وما في حكمها ومن ثم نتطرق إلى النظام القانوني لمكافحة الجرائم المعلوماتية لدولة الإمارات العربية المتحدة والمملكة العربية السعودية حيث أصدرت دولة الإمارات القانون الإتحادي رقم 2 لسنة 2006 الخاص بمكافحة جرائم تقنية المعلومات الحديثة ، وهذا القانون هو القانون الريادي الأول في العالم العربي الذي يعنى بجرائم المعلوماتية ، ، كذلك اصدار المملكة العربية

السعودية بتاريخ 2008/01/24 نظامها الخاص بمكافحة جرائم تقنية المعلومات و نختمها بالتنظيم التشريعي الجزائري في إطار تجريم الإعتداء على المنظومة المعلوماتية

الفرع الأول: القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها (2004/417)

بناء على مشروع قانون تقدمت به دولة الإمارات العربية المتحدة بخصوص مكافحة جرائم تقنية المعلومات الحديثة في نطاق الأمانة العامة الحديثة في نطاق الأمانة العامة لجامعة الدول العربية صدر القانون العربي النموذجي أو الإسترشادي لمكافحة تقنية أنظمة المعلومات وما في حكمها والذي إعتمده مجلس وزارة العدل العرب في دورته التاسعة عشر بالقرار رقم 495-د 19 - 2003/10/8 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين ، و على إثر ذلك صدر هذا القانون النموذجي و الذي يتضمن القانون العربي الإسترشادي (النموذجي) لمكافحة جرائم تقنية أنضمة المعلومات وما في حكمها ، تجريم الأفعال التالية :

1- الدخول العمد وبغير وجه حق إلى موقع أو نظام معلوماتي.[1]الدخول غير المشروع بقصد الغاء أو حذف أو تدمير أو انشاء أو اتلاف أو تغيير أو بإعادة نشر بيانات أو معلومات شخصية.[2]

2- الدخول غير المشروع بقصد الغاء أو حذف أو تدمير او انشاء أو اتلاف او تغيير أو بإعادة نشر بيانات أو معلومات شخصية.

3- تزوير في أحد المستندات المعالجة في نظام معلوماتي.[3]

[1] - المادة الثالثة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمه الصادر عن الأمانة العامة لجامعة الدول العربية (قرار رقم 2004/417) .ا .

[2] - المادة الثالثة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[3] - المادة الرابعة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

4- الإدخال عن طريق شبكة معلومات أو أحد أجهزة الحاسب الآلي وما في حكمها وما من شأنه ايقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو اتلاف أو تعديل البرامج أو البيانات أو المعلومات.[1]

5- اعاقة أو تشويش أو تعطيل العمد وبأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها والوصول إلى الخدمة أو الدخول إلى أجهزة أو البرامج أو مصادر البيانات أو المعلومات.[2]

6- التنصت والإلتقاط أو الاعتراض بدون وجه حق لما هو مرسل عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الالي أو ما في حكمها.[3]

7- استعمال الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها من تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه ، ولول كان هذا الفعل أو الإمتناع مشروعا.[4]

8- التوصل عن طريق الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي وما في حكمها إلى الإستيلاء على مال منقول أو على سند أو توقيع هذا السند وذلك بالإستعانة بطريقة احتيالية أو بإتخاذ إسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.[5]

9- استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في الوصول بدون وجه حق إلى ارقام أو بيانات بطاقة ائتمانية وما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله.[6]

---

[1] – المادة الثالثة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[2] – المادة السابعة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[3] – المادة الثامنة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[4] – المادة التاسعة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[5] – المادة العاشرة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها

[6] – المادة الحادية عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها

10- الانتفاع بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي في حكمها بخدمات الإتصالات.[1]

11- انتاج أو اعداد أو ارسال أو خزن ما من شأنه المساس بالنظام العام أو الآداب العامة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.[2]

12- نشر أو نسخ مصنفات فكرية أو أدبية أو ابحاث علمية أو ما في حكمها بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها.[3]

13- الدخول بدون وجه حق إلى موقع خاص لشركة أو مؤسسة أو غيرها لتغيير تصاميم هذا الموقع أو الغاء أو اتلاف أو تعديل أو شغل عنوانه.[4]

14- الإعتداء على أي من المبادئ ، أو القيم الدينية أو الاسرية أو حرمة الحياة الخاصة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها.[5]

15- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الاتجار بالجنس البشري أو تسهيل التعامل فيه.[6]

16- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الإتجار أو الترويج أو التعاطي بالمخدرات أو المؤثرات العقلية وما في حكمها أو تسهيل التعامل فيها.[7]

[1] – المادة الثانية عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[2] – المادة الثالثة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[3] – المادة الرابعة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[4] – المادة الخامسة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[5] – المادة السادسة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[6] – المادة السابعة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[7] – المادة الثامنة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حاكمها .

17- القيام بتحويل الأموال غير المشروعة أو نقلها أو تمويه بالمصدر غير المشروع لها أو اخفائه ، أو القيام بإستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو تحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع ، وذلك عن طريق استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها وبقصد اضفاء الصفة المشروعة على تلك الأموال أو انشاء أو نشر موقع لإرتكاب أي من هذه الأفعال.[1]

18- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي وما في حكمها لتسهيل وترويج برامج وأفكار مخالفة للنظام العام.[2]

19- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما فيحكمها لجماعة ارهابية تحت مسميات تمويهية لتسهيل الإتصالات بقياداتها أو اعضائها او ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة او المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية.[3]

20- الدخول العمد بغير وجه حق إلى موقع أو نظام مباشر أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الامن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو بث أفكار تمس ذلك.[4]

[1] – المادة التاسعة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[2] – المادة عشرين من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[3] – المادة واحد وعشرون من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[4] – المادة الثانية والعشرون من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

الفرع الثاني: نظام مكافحة جرائم تقنية المعلومات الحديثة في الإمارات العربية المتحدة والمملكة العربية السعودية.

أولا: نظام مكافحة جرائم تقنية المعلومات الحديثة في الإمارات العربية المتحدة

نص القانون الإتحادي رقم 2 لسنة 2006 على تجريم الأفعال التالية :

أ- إختراق المواقع والأنظمة الإلكترونية :

عاقب هذا القانون على جريمة اختراق المواقع وأنظمة المعلومات ، وفرد لتلك الجريمة أنواعا من العقوبة تتدرج وفقا لحالات أربع : حالة القيام بفعل دون ترتب نتيجة ، حالة القيام بالفعل مع ترتب نتيجة متعلقة بإلغاء أو حذف أو تدمير معلومات ، حالة القيام بالفعل مع ترتب نتيجة متعلقة بإنتهاك معلومات شخصية ، حالة القيام بالفعل أثناء أو بسبب العمل أو تسهيل للغير مهمة القيام بهذا الفعل.[1]

ب- تزوير مستندات معترف بها في نظام معلوماتي :

حيث يعاقب هذا القانون كل من زور مستندا من مستندات الحكومة الإتحادية او المحلية أو الهيئات أو المؤسسات العامة الإتحادية والمحلية المعترف به قانونا في نظام معلوماتي.[2]

[1] – المادة الثانية من القانون الإتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات ، منشور في العدد رقم (442) من الجريدة الرسمية لدولة الإمارات العربية المتحدة.

[2] – المادة الرابعة من القانون الإتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات .

ج– التعطيل او العبث :

من خلال تعطيل الوصل إلى الوسائل أو البرامج أو المعلومات أو الشبكات المتعلقة بتقنية المعلومات [1] أو العبث بالشبكة المعلوماتية أو احدى وسائل التقنية التي يترتب عليها ضرر موصوف .[2]العبث بالفحوص الطبية بإستخدام الانترنت أو احدى وسائل تقنية المعلومات.[3]

د – التنصت أو التهديد :

بإستخدام الأنترنت أو إحدى وسائل تقنية المعلومات .[4]التهديد بإستخدام الإنترنت أو بإحدى وسائل تقنية المعلومات .[5]

و– السرقة و الاحتيال :

بإستخدام الانترنت أو احدة وسائل تقنية المعلومات والاستيلاء على البطاقات الإلكترونية بإستخدام الأنترنت أو احدى وسائل تقنية المعلومات .[6]

هـ– المساس بالآداب العامة والتحريض عليها و المساس بالأديان و انتهاك حرمة الحياة الخاصة و الاتجار بالبشر أو بالمخدرات و غسل الاموال و الأفعال الإرهابية و والحصول على معلومات حكومية او التحريض على ارتكاب اي جريمة من هذا القانون :

تجريم الدعارة بإستخدم الأنترنت أو احدى وسائل تقنية المعلومات ،[7] أو العبث بالمواقع الإلكترونية على الانترنت [8] ، أو المساس بالأديان بإستخدام الانترنت أو احدى وسائل تقنية

[1] – المادة الخامسة من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[2] – المادة السادسة من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[3] – المادة السابعة من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[4] – المادة الثامنة من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[5] – المادة التاسعة من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[6] – المادة العاشرة و الحادية عشر من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[7] – المادة الثانية عشر والثالثة عشر من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[8] – المادة الرابعة عشر من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

المعلومات [1] ، أو انتهاك حرمة الحياة الخاصة عن طريق الانترنت أو احدى وسائل تقنية المعلومات[2] ، أو الاتجار بالبشر عبر الانترنت والاتجار بالمخدرات وغسل الاموال عبر الانترنت [3] ، أو انشاء مواقع الكترونية مخالفة للنظام العام والآداب أو استخدام وسائل تقنية المعلومات لهذه الغاية [4] ، أو الأفعال الإرهابية عبر أو بإستخدام وسائل تقنية المعلومات والحصول على معلومات حكومية عبر أو بإستخدام وسائل تقنية المعلومات [5] ، أو التحريض أو التدخل في الجرائم السابق ذكرها في هذا القانون.[6]

ثانيا : نظام مكافحة جرائم تقنية جرائم المعلومات في المملكة العربية السعودية (القانون الصادر بتاريخ 2008/01/24)

نص قانون مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية على تجريم الافعال التالية :

- التنصت على ما هو مرسل عن طريق وسائط التقنية أو التقاطها أو اعتراضه .[7]
- الدخول غير المشروط لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو امتناع عنه والدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو الغائه أو اتلافه أو تعديله أو شغل

[1] – المادة الخامسة عشر من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات .

[2] – المادة السادسة عشر من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات .

[3] – المادة السابعة عشر والثامنة عشر والتاسعة عشر من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات ، منشور في العدد رقم 442 ، من الجريدة الرسمية لدولة الإمارات العربية المتحدة

[4] – المادة عشرون من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات ، منشور في العدد رقم 442 ، من الجريدة الرسمية لدولة الإمارات العربية المتحدة.

[5] – المادة الواحد والعشرون والثانية والعشرين من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات ، منشور في العدد رقم 442 ، من الجريدة الرسمية لدولة الإمارات العربية المتحدة

[6] – المادة الثالثة والعشرين من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات ، منشور في العدد رقم 442 ، من الجريدة الرسمية لدولة الإمارات العربية المتحدة.

[7] – المادة الثالثة من نظام مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 2008/01/24 أنظر في هذا فؤاد بن صغير ، مرجع سابق ،ص 102.

عنوانه والمساس بالحياة الخاصة بالآخرين أو التشهير بالأخرين والحاق الضرر بهم عبر وسائل تقنية المعلومات المختلفة .[1]

- انشاء المواقع للمنظمات الإرهابية على الشبكة العنكبوتية والدخول إلى نظام معلوماتي للحصول على معلومات وبيانات تمس الامن الداخلي والخارجي للدولة أو اقتصادها الوطني.[2]

- الإستيلاء على مال منقول أو على سند أو توقيع هذا السند عن طريق الاحتيال أو انتحال شخصية غير صحيحة ، أو الوصول إلى بيانات بنكية وائتمانية أو بينات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال ، عبر استخدام وسائل وتقنية المعلومات أو الدخول غير المشروع إلى نظام معلوماتي ، والدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو اعادة نشرها وايقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير او نسخ البرامج أو البيانات الموجودة والمستخدمة فيها أو حذفها أو تسريبها أو اتلافها أو تعديلها أو اعاقة الوصول إلى الخدمة او تشويشها أو تعطيلها بأي وسيلة كانت من وسائل التقنية .[3]

- انتاج ما يمس بالنظام العام أو الآداب العامة أو حرمة الحياة الخاصة أو اعداده أو ارساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو انشاء موقع على الشبكة المعلوماتية أو نشره للإتجار في الجنس البشري أو تسهيل التعامل به ، أو انشاء المواد المتعلقة بالشبكات الاباحية أو انشطة الميسر المخلة بالآداب العامة ونشرها أو ترويجها أو إنشاء موقع للإتجار بالمخدرات او المؤثرات العقلية أو ترويجها أو طرق تعاطيها أو تسهيل العامل بها .[4]

[1] – المادة الثالثة من نظام مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية ، نفس المرجع السابق ، ص 102 .

[2] – المادة السابعة من نظام مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية ، نفس المرجع ، ص (102) .

[3] – المادة الرابعة والخامسة من نظام مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية نفس المرجع ، ص (103).

[4] المادة السادسة من نظام مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية ، نفس المرجع ، ص (104) .

الفرع الثالث : الإطار القانوني الوطني المتعلق بجرائم الإعتداء على النظام المعلوماتي

و يشمل هذا الإطار نصوص قانونية مختلفة نحصرها فيما يلي :

أولا: القانون رقم 15/04 المعدل و المتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

بحيث احتوى على جرائم مختلفة تستهدف النظام المعلوماتي و هي :

أ– الجرائم المنصوص عليها بالمادة 394 مكرر :

– الدخول غير المشروع و عن طريق الغش للأنظمة المعلوماتية .

– البقاء غير المشروع في الانظمة المعلوماتية .تعديل او حذف معطيات المنظومة نتيجة الدخول غير المشروع .

– الإضرار (الإتلاف او التخريب) بنظام التشغيل للمنظومة على اثر الدخول او البقاء غير المشروع .

ب – الجرائم المنصوص عليها في المادة 394مكرر 1:

– ادخال معطيات في منظومة معلوماتية خلسة .

– ازالة او تعدي معطيات في منظومة معلوماتية خلسة .

ج – الجرائم المنصوص عليها في المادة 394 مكرر 2 :

– القيام عمدا و خلسة بتصميم او تجميع او توفير او نشر او البحث عن معطيات تمكن من ارتكاب الجرائم السابقة الذكر .

– حيازة او افشاء او نشر او استعمال معطيات متحصل عليها من جرائم المساس بانظمة المعالجة الالية للمعطيات .

د – تجريم المساعدة و التحريض على ارتكاب الجرائم السابقة الذكر

ثانيا : القانون رقم 15-03 المتعلق بعصرنة العدالة

أ – حيث أنه جاء لعصرنة سير قطاع العدالة من خلال وضع منظومة معلوماتية مركزية لدى وزارة العدل تتعلق بنشاط الوزارة و المؤسسات التابعة لها و مختلف الجهات القضائية و التي تكون محمية بواسطة برنامج يرخص لاستعمال معطيات المنظومة المركزية ، الذي يسمح بتبادل المعلومات بطريقة الكترونية كتابة و قراءة ، و استخدام تقنية المحادثات المرئية عن بعد في الاجراءات القضائية

- **التصديق الإلكتروني**
- **ارسال الوثائق و الاجراءات القضائية بالطريق الالكتروني**
- **استعمال المحادثة المرئية عن بعد اثناء الاجراءات القضائية**
- **الاجراءات**
- **الاحكام الجزائية**

ثالثا: القانون رقم 15-04 المحدد للقواعد العامة المتعلق بالتوقيع و التصديق الالكترونيين

أ – حيث يقصد في مفهوم هذا القانون بالتوقيع الالكتروني بانه بيانات في شكل الكتروني مرفقة او مرتبطة منطقيا ببيانات الكترونية اخرى تستعمل كالرموز او مفاتيح التشفير الخاصة كوسيلة توثيق عبر جهاز او برنامج معلوماتي معد لتطبيق بيانات انشائه من اجل التحقق منها و التي تمنح عبر وثيقة الكترونية تسمى شهادة التصديق الالكتروني تثبت الصلة بين الموقع و هو شخص طبيعي يحوز بيانات انشاء التوقيع الالكتروني و يتصرف لحسابه الخاص او لحساب الشخص الطبيعي او المعنوي الذي يمثله ، و بين البيانات . تلك الشهادة تمنح من مؤدي الخدمات في مجال الترخيص .

ب – مبادئ المماثلة و عدم التمييز اتجاه التوقيع الالكتروني .

ج – اليات انشاء التوقيع الالكتروني الموصوف و التحقق منه.

د – شهادة التصديق الالكتروني الموصوفة و سلطات التصديق.

هـ – النظام القانوني لتأدية خدمات التصديق الالكتروني.

ي– العقوبات الادارية و المالية و الاحكام الجزائية.

بعد أن فرغنا من الدراسة التأصيلية لجرائم الاعتداء على النظام المعلوماتي كسبب رئيسي لإصدرا التشريعات الخاصة بأمنها ، فقد تبين لنا أن النظام المعلوماتي تتهدده مخاطر قانونية عديدة في العالم الافتراضي، ومما لاشك فيه أن مواجهة تلك المخاطر تتطلب صياغة خطة لها ابعادها ومحاورها الاستراتيجية[1] التي تتميز بالعموم[2] و التكامل[3] و المسايرة لتطور الإختيارات السياسية[4] و قيام الوسائل[5] و المرونة[6] ، كما انها تعتمد على منطلقات ومقومات تشريعية وتنظيمية (مادية و بشرية) لا غنى عنها حتى تحقق أهدافها المرصودة لها، أي بشكل يكفل في النهاية الحيلولة دون وقوع الجريمة، أو انجاحها في السيطرة عليها حال تحقق نتيجتها الاجرامية، أو بعبارة أخرى موجزة نعني "تطبيق آلية وقائية و ردعية".

ونقصد بالآليات الوقائية الشق التجريمي لمسائل الاعتداء على نظم المعالجة الآلية، ذلك ان تحديدها بصفة مسبقة تماشيا مع مبدأ الشرعية يحمل معنى الإنذار، وبالتالي يضع للأفراد حلولا واضحة تفصل بين المشروع وغير المشروع، فإذا ما سلكه الفرد يكون محل لوم ، هذا بالإضافة للعقوبة التي تعتبر الإطار القانوني الوقائي الرادع سواء في الجرائم التقليدية والمستحدثة، إلا أن الطبيعة الخاصة لجرائم الاعتداء على نظم المعالجة الآلية والخسائر الناجمة عنها قد تجعل المشرع الجنائي يعيد النظر في مسألة انفراد تلك الأخيرة في تحقيق الوقاية، وقد يكون من نتائج ذلك استحداثه قواعد وتدابير وقائية أكثر ملاءمة وانسجام مع طبيعتها الخاصة. وإن كان كذلك فماهي هذه القواعد والتدابير؟.

---

[1] الإستراتيجية كلمة يونانية عرفت في دراسة الحرب بمعنى قيادة الجيش ثم انتقلت نهاية القرن القرن الماضي لمجال العلوم الإجتماعية و الإقتصادية كما أصبحت متداولة في علم التخطيط و التنفيذ و وصفت بالعلم لتزويدها الإنسان بالمعرفة القادرة على تطوير مفاهيمه وفنه و أدائه تحقيقا لأهدافه كما وصفت بالفن بإعتبارها دراسة في استعمال العلم ، و مجمل القول هنا في إطار دراستنا الجنائية و بخصوص موضوعنا هذا يمكننا القول أن الإستراتيجية هي مجموعة من الأساليب و الوسائل التي توصل إلى أهداف السياسة الجنائية عن طريق خطوات عملية تمثلها الى واقع ملموس .

[2] و نعني بها انطباقها على جميع صور الجرائم و تشمل جميع عناصر السياسة الجنائية و فروعها من تجريم و عقاب و منع.

[3] لأن ارتباطها بالأهداف السياسية و الإجتماعية و الإقتصادية يستلزم إتفاقها معها .

[4] و لن يتحقق ذلك الا في مدى طويل نسبيا يتيح الفرصة لظهور النتائج و نضج الافكار السياسية المستقبلية

[5] و الفاعلية و مدى تحقيق النتائج التي تضعها على المنهج العلمي القائم على التجربة

[6] لأن المعطيات الأساسية التي تبعث على رسم الإستراتيجية كثيرا ما تتغير في مرحلة التنفيذ

فإذا فشلت الوقاية و وقعت الجريمة وفق النموذج القانوني المحدد لها، فبوقوعها ينشأ للدولة حق معاقبة الجاني إنما تقوم بذلك مستخدمة آليات إجرائية مقررة قانونا بحيث لا يمكن تجاوزها، فالتجاوز سيهدم مقومات الإدانة ليشيد هيكل البراءة فتكون النتيجة تبرئة المجرم حال لزوم معاقبته.

والواقع أن طبيعة جرائم الاعتداء على نظم المعالجة الآلية بعناصرها ووسائل ارتكابها قد تدفع المشرّع الجنائي لإعادة النظر في كثير من المسائل الإجرائية، ذلك أن طبيعة هذا النوع من الاجرام قد يتسبب في أزمة حقيقية لقانون الإجراءات الجزائية في صورته المعروفة ، خاصة فيما يتعلق بالإثبات باعتباره من أهم الموضوعات في هذا القانون التي تثير اشكالات ، فنحن أمام جرائم يكون فيها الدليل من ذات طبيعتها، وهو الأمر الذي لن تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل التقليدي قادرة على القيام به.

ولا يقف الأمر عند هذا الحدّ بل يتجاوزه إلى مشكلة أكبر تتعلق بمسألة قبول هذا الدليل أمام القضاء، فكما نعلم فإنّ القضاء يلعب دورا لا يمكن إنكاره في تطبيق القانون وردع كل من تسوّل له نفسه الاعتداء على المصالح الاجتماعية والاقتصادية محل الحماية القانونية، ولن يتجلّى ذلك إلا من خلال حكم حائز لقوة الشيء المقضي فيه ، وعملية تقدير الأدلّة تشكل جوهر هذا الحكم، حيث لا يمكن الوصول إليه وإدراكه ما لم يمارس القاضي سلطته التقديرية على الأدلة محل الوقائع، وفي مجال جرائم الاعتداء على النظام المعلوماتي يكون الدليل التقني السمة المميزة للعملية التحقيقية، خاصة أن الحكم هو الكلمة النهائية للقضاء ، وسلامة هذا الحكم يتوقف بدرجة كبيرة على سلامة تقدير الأدلة.

ولما كان الدليل التقني ليس كالأدلة المادية وإنما عبارة عن معلومات مكمنها هو النظام المعلوماتي أي البيئة الإلكترونية للمعلومات ، و هذه الحقيقة تضعنا أمام مشكلة مشروعية الاخذ بالدليل التقني أو مدى قبوله كوسيلة من وسائل الاثبات الجزائي ؟

بل حتى مع قبول القانون واعترافه بهذا الدليل فإن عملية البحث عنه يشكل صعوبة في حد ذاتها ، من منظور الجهات التحقيقية اللازمة بل نقول هنا المتخصصة في مجال المعلوماتية حيث ان تلك الجهات يجب ان تكون متصفة بالتقنية او الفنية كي تكون في مستوى الدليل محل البحث .

وتماشيا مع تسلسل الأفكار على النحو السابق ذكرها ستكون دراستنا في هذا الباب وفق القواعد المعترف بها من قبل المشرع الجزائري و المتعلقة بمواجهة هذه الظاهرة مع الاستنارة في ذلك كله مع بعض الفقه المقارن . و هذا يقتضي منا تقسيم الباب الثاني من دراستنا إلى فصلين كما يلي:

الفصل الأول : الجوانب الموضوعية لمواجهة جرائم الإعتداء على النظام المعلوماتي

المبحث الأول : تحديد الشق التجريمي لمسائل الاعتداء على النظام المعلوماتي

المبحث الثاني : مدى ملاءمة العقوبة في جرائم الاعتداء على النظام المعلوماتي .

الفصل الثاني : الجوانب الإجرائية لمواجهة جرائم الإعتداء على النظام المعلوماتي

المبحث الأول: الدليل التقني بين الإشكالات الإجرائية و قبول مشروعيته و مصداقيته

المبحث الثاني : الاتجاه نحو تنظيم الإطار التشريعي للأدلة التقنية كرهان مستقبلي

مع الإنتشار الواسع و المتزايد للإستعمالات المختلفة و المتعددة للنظم المعلوماتية ، هذا الذي أدى إلى تزايد عدد مستخدميها في مختلف التعاملات اليومية ، الأمر الذي كبرت معه المصالح المرتبطة بها و بالمعلومات من إدخال و تخزين أو نقل و تداول لها أو معالجتها ، هذا الذي أستغل في أغراض غير مشروعة فأصبح النظام المعلوماتي محلا للعديد من الإعتداءات التي تشكل خطرا على المعلومات الإلكترونية المتواجدة فيه ، خاصة بعد دمج النظام المعلوماتي بالأنترنت التي شكلت عالما إفتراضيا غير مادي أو محسوس تتواجد فيه تلك المعلومات ، و التي ساهمت في تفشي جرائم وصفناها بأنها مستحدثة و مستقلة عن الجرائم التقليدية لهذا تدخل المشرع الجنائي لحمايتها جنائيا بنصوص مستقلة عن النصوص التقليدية التي وقفت عاجزة عن توفير تلك الحماية و هو ما سنعالجه في هذا الفصل من خلال التطرق للجوانب الموضوعية التي خصها المشرع لحماية النظام المعلوماتي من الجرائم التي تشكل اعتداء عليه و ذلك بتوفير نصوص تجريمية لمواجه تلك الإعتداءات توضح شكل الإعتداء و المصالح محل الحماية هذا بالإضافة الى وضع جزاءات لكل من قام بالإعتداء على النظام المعلوماتي وفق ما هو منصوص عليه بالتشريع العقابي .

و لتوضييح تلك الجوانب الموضوعية المكرسة للمواجهة جرائم الإعتداء على النظام المعلوماتي إرتأينا ان يكون هذا الفصل مقسم الى مبحثين حيث خصصنا المبحث الأول منه لتحديد الشق التجريمي لمسائل الاعتداء على النظام المعلوماتي بينما نتطرق في المبحث الثاني لمدى ملاءمة العقوبة في جرائم الاعتداء على النظام المعلوماتي .

المبحث الأول : تحديد الشق التجريمي لمسائل الاعتداء على النظام المعلوماتي

لم يكن المشرع الجزائري بمعزل عن الحركية التشريعية التي واجهت الإعتداءات على نظم المعلوماتية حيث نجده قد إستعد لتلك الظاهرة و مواجهتها وفق رؤية موضوعية عالجت الشق التجريمي في حالة الإعتداء على النظام المعلوماتي في نسق متكامل أعطى فيه المشرع الجزائري تصوره التشريعي لمجابهة الفراغ القانوني و ضمان لسد الثغرة التشريعية التي تمكن المجرم من الإفلات من العقاب و هذا وفق القانون رقم 04-15 المعدل و المتمم لقانون العقوبات في اطار القسم السابع مكرر الذي خصصه المشرع الجزائري لجرائم المساس بنظام المعالجة الآلية للمعطيات من المادة 394 مكرر الى المادة 394 مكرر 7 . و هذا ما سندرسه في المبحث وفق المطلبين التاليين :

المطلب الأول : الجرائم المتعلقة بالإعتداء على النظام المعلوماتي

حدّث المشرع الجزائري نصوصه التجريمية بموجب تعديل قانون العقوبات بالقانون رقم 15/04 في المواد من 394 مكرر إلى 394 مكرر7 تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" لتتماشى مع متطلبات أمن المعلومات في البيئة الإلكترونية ، كما عززها بنصوص تشريعية في المجال الجنائي بعد ذلك بقانون مكافحة جرائم تكنولوجيا الإعلام والاتصال رقم 04/09[1].

وبرجوعنا للتشريعين السابقي الذكر نجد أن الصور التجريمية الأصلية التي عالجها المشرع الجزائري و المتعلقة بالإعتداء على النظام المعلوماتي متغيرة بتغير السلوك المرتكب و النتيجة الواقعة و هذا ما سنتناوله وفق الفروع التالية :

[1]- القانون رقم 04/09 الصادر بتاريخ 5 أوت 2009 جريد رسمية عدد 47.و هو قانون اجرائي بالأصل.

الفرع الأول: الجريمة المنصوص عليها بالمادة 394 مكرر

أولا جريمة الدخول أو البقاء عن طريق الغش

تعتبر الأنشطة التي تستخدم في إطار تبادل المعلومات الالكترونية[1] عن طريق النظام المعلوماتي ، و ما نتج عنها من إشكالات قانونية في إطار أمنها من الإعتداءات الواقعة عليها ، وهذا الأمر الذي جعل المشرع يتجه لإدخال تشريعات جديدة تحمي المعلومة داخل النظام المعلوماتي ، و التي منها تجريم الدخول في نظام الحاسب الآلي فضلا عن إتلاف المعلومات المبرمجة أو الموجودة داخل هذا النظام، وهو ما نص عليه المشرع بنص المادة 394 مكرر[2].

أ- الركن المادي لجريمة الدخول أو البقاء عن طريق الغش

بالرجوع إلى نص المادة 394 مكرر السالف الذكر يتضح أن الركن المادي لهذه الجريمة يتكون من عنصرين هما الدخول إلى نظام المعالجة أو البقاء فيه بعد الدخول وسنتناول هذين العنصرين بشيء من التفصيل.

1- الدخول إلى نظام المعالجة الآلية للمعطيات

الدخول هو الولوج إلى المعلومات والمعطيات المخزنة داخل النظام المعلوماتي بدون رضا المسؤول عنه[3]، وقد حصل نقاش واسع في الولايات المتحدة الأمريكية حول عبارة " الدخول " وذلك سنة 1996 أمام محكمة كانساس العليا في قضية allen، وتتلخص وقائع القضية في قيام المتهم allen بإستخدام حاسبه الآلي للإتصال بحاسب شركة الهاتف الجنوبية الغربية التى تتحكم في تحويل الإتصالات البعيدة المدى، حيث تلاعب المتهم بنظامها بطريقة تسمح بالإتصال الهاتفي

---

[1]- سليم عبد الله الجبوري، المرجع السابق، ص318.

[2]- ذكرنا سابقا أن المشرع استحدث هذه الجرائم بموجب تعديل قانون العقوبات بالقانون رقم 15/04 المؤرخ في 2004/11/10، ج ع 71 حيث تنص المادة 394 مكرر من قانون العقوبات أنه "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..." تقابلها المادة 1/67 من قانون المعاملات والتجارة الإلكترونية القطري[2]، الفصل 48 من القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية[2] رقم 83 لسنة 2000، والمادة 02 من إتفاقيت بودابيست..، .

[3] - حيث تشير المذكرة التفسيرية لإتفاقية بودابيست أن الولوج غير القانوني يجب أن يكون دون حق وذلك يعني ألا عقاب على الولوج المصرح به أو كان الولوج متاحا للجمهور..،

مجاناً، وقد إتضح للمحققين أن allen إخترق النظام عن طريق فك كلمته السرية، ومن ثمة إزالة الدليل على نشاطه بإلغاءه للسجلات ، وقد دافع المتهم عن نفسه أمام المحكمة بأنه لا يوجد دليل على دخوله إلى الحاسب الآلي للشركة، إلا أن الإدعاء إعتمد على تعريف التشريع الواسع لعبارة "الدخول access " والتى تقر بأن الدخول يعني الإقتراب أو إصدار أمر أو الإتصال بـ..**أو أية أشياء أخرى تؤدي إلى إستخدام مصادر الحاسوب** ، لكن المحكمة أجابت بأن هذا التعريف كان واسعا بحيث يؤدي إلى القول بعدم دستورية التشريع لغموضه، وإنتهت المحكمة إلى أن المعنى الكامل والعادي يجب أن يطبق عوضا عن الترجمة المشوهة للتعريف المتوافر ، وأن القول بأن دخول المتهم إلى النظام يظهر في قيامه بالبحث عن كلمة العبور الخاصة بنظام الشركة المذكورة للوصول إلى المعلومات قول لا دليل عليه، وهو ما يؤدي إلى القول بعدم دخول المتهم إلى حاسابات الشركة[1].

ويتحقق هذا السلوك المجرم عن طريق قيام الجاني الإلكتروني بإختراق أنظمة المعلوماتية الذي يمكننا أن نتصور الدخول إليها وفق فرضيات نوجزها وفق الآتي توضيحه :

– الدخول عن طريق تشغيل حاسب آلي مغلق:

حيث يقوم الجاني في هذه الحالة بفتح جهاز الكمبيوتر وتشغيله ثم يدخل إلى النظام ، غير أن العبرة ليست بتشغيل الكمبيوتر ولكن بالتمكن من الدخول إلى النظام إذ يستطيع الجاني أن يدخل إلى النظام والجهاز مغلق، وقد يتمكن من تشغيل الجهاز دون أن يصل إلى الملفات ويمكن اعتبار هذه الحالة شروعا ويعاقب عليه ، و هنا يثار تساؤل في حالة النظام المفتوح وقام الجاني بالإطلاع عليه عن طريق شاشة الجهاز؟ ، و لقد أجاب جانب من الفقه بأن مجرد الإطلاع على

[1]– خليفة محمد، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة، 2011/2010، ص 140 وما بعدها.

تلك المعلومات الظاهرة على شاشة الجهاز لا يعد دخولاً للنظام ، إنما يكون الدخول إذا كان الجاني هو من قام بتشغيل الجهاز و الولوج إلى النظام[1].

– الدخول بإستعمال حاسب آلي مفتوح :

في هذه الحالة يكون جهاز الحاسوب قيد الاستعمال ثم قام الجاني بإستغلال ذلك ودخل إلى إحدى أنظمة المعالجة أو الملفات المتواجدة فيه..، وعليه فإن ذلك يعد دخولاً غير مشروع ويعاقب عليه.

– الدخول عن طريق الإختراق

في كثير من الأحيان يتم ربط أجهزة الحاسب الآلي بشبكة خاصة أو يكون موصولا بالانترنيت ، فيتمكن المتهم في هذه الحالة من الدخول إلى الكمبيوتر عن طريق جهازه الخاص ويتم ذلك غالبا بإستخدام وسائل تقنية حديثة كبرامج التجسس والاختراق ويتطلب مهارة عالية.

– الدخول عن طريق خطوط الاتصالات

وفي هذه الحالة يعمد الجاني إلى العبث بخط من خطوط الهاتف المتصل بالنظام المعنى من أجل إعطاء تعليمات إلى هذا النظام لتحقيق غرض معين [2]، وقد قضي في فرنسا بوقوع هذه الجريمة ممن تمكن من الدخول إلى أجهزة الهواتف الخاصة بإحدى المؤسسات واستطاع من خلال ذلك إجراء اتصالات تليفونية على حساب تلك المؤسسة[3].

– الدخول إلى نظام الحاسب الآلي بإستعمال بطاقة الغير: في هذه الحالة يقوم المتهم بإستعمال بطاقة الغير للدخول إلى نظام الحاسب الآلي التابع لإحدى الجهات من أجل الحصول

[1]– وما تجدر الإشارة إليه أن الدخول لا يكون محققا إذا كان برضا صاحب النظام..، لذلك يعتبر البعض أن عدم الرضا ركن في هذه الجريمة فإذا توفر الرضا انتفت الجريمة حتى ولو استعمل الجاني النظام في غير الأغراض التي أرادها صاحب النظام... ينظر لمزيد من التفصيل ، عبد الفتاح بيومي حجازي، التجارة الالكترونية.... المرجع السابق، ص30.

[2]– وقد تم اتهام مهندسين يعملون في شركة إتصال فرنسية لإستعمالهم خط التليفون المركب على أجهزة عارضة للألعاب الالكترونية...، وتمكنوا من جراء ذلك من الحصول على جوائز على اعتبار أنهم فازوا بالألعاب التي قاموا بها..، في حين أنهم تحايلوا على الجهاز الخاص باللعبة وتحصلوا على معلومات ساعدتهم على الفوز...، ينظر، شيماء عبد الغني محمد عطا الله، المرجع السابق، ص108.

[3]– كما قضي بأنه يعد شريكا في الجريمة التقني الذي كان مكلفا بصيانة النظام الكهربائي و الذي ساهم مع الفاعل في الحصول على الأرقام السرية التي من خلالها استطاع الجاني أن يدخل إلى نظام الكمبيوتر...ينظر، شيماء عبد الغني محمد عطا الله، المرجع السابق، ص112.

على أمر معين أو بيانات معينة أو معلومات هي مقتصرة على أصحاب البطاقات، وقد قضي في فرنسا بوقوع هذه الجريمة على من استخدم بطاقة السحب مع الرقم السري الخاص بشخص آخر دون موافقته وعد ذلك من قبيل الدخول[1].

و في هذا الإطار ثارت إشكالية الدخول الذي يتم عن طريق التقاط الإشعاعات والإشارات الصادرة عن الكمبيوتر ومدى خضوعه لهذه الجريمة ؟ ، حيث إعتبر الفقه أن الدخول بهذه الطريقة يعد تداخلاً و ليس دخولا ، وما يعزز هذه الإشكالية أن كثيراً من القوانين جرمت السلوكين معا " التداخل والدخول " ومن ذلك ما نص عليه قانون جرائم الكمبيوتر الأمريكية حيث "**عاقب كل من يتداخل أو يسبب تداخل الغير أو يحاول التداخل – مع علمه بذلك – في برامج كمبيوتر أو البيانات التي يحتويها أو في نظام الكمبيوتر أو شبكته**".

هذا ما دفعنا لتوضيح معنى الدخول بصورة اكثر دقة تحديدا لعناصر السلوك محل التجريم ، وعليه يقصد بالدخول في هذه الجريمة الدخول الإلكتروني عن طريق الأساليب والوسائل التقنية المتاحة كالدخول إلى مركز النظام المعلوماتي ، غير أن المشرع لم يحدد وسيلة معينة يتم بها الدخول وعلى هذا الأساس فإن الدخول إلى نظام المعالجة الآلية للمعطيات يتعلق بأي وسيلة تقنية سواء كان ذلك بإستعمال البرامج المخصصة لإختراق الأنظمة أو بإستعمال طريقة يطلق عليها "الفخ La Trappe"، وهو عبارة عن منفذ يجهز به النظام مسبقا من قبل مصمم البرنامج ليسمح له لاحقا بتحميل برامج تعيق سير عمله[2]، ومن الوسائل المستعملة في هذا المجال أيضا نجد أسلوب "التخفي Déguisement"، ويقصد انتحال صفة من له الحق في الدخول إلى النظام....، غير أن أخطر وسيلة تعرف بالقناة المتخفية "canal cache"، وهي طريقة جد معقدة يعمد فيها الجاني

[1] – محمد أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003، ص1150.

[2] – وعليه يعد الدخول بهذه الوسيلة تهديدا حقيقيا لأمن المعلومة ويخلق العديد من المشاكل التقنية، حيث يؤدي إلى هدم بيانات سرية مثل كلمة المرور ومعلومات سرية خاصة بالبرنامج...، ثم المساس بالمعاملات التجارية التي تتم عن طريق هذا النظام أو الموقع، بل ويفتح الباب أما ارتكاب جرائم أخرى ... ينظر، التقرير التفسيري لاتفاقية بودابست المتعلقة بجرائم الكمبيوتر خاصة المواد 3 إلى 6 .

لإختراق نظام الحماية المعتمد من طرف صاحب النظام ، ومن الجناة الالكترونيين من يعتمد على وسيلة التسلل "Faufilement" وتتم عن طريق تتبع مستعمل رخصة الدخول إلى النظام[1].

وعليه فإن الدخول بهذا المفهوم يختلف عن التقاط الإرسالات أو الإشارات عن بعد ذلك أن المتهم لا يدخل إلى نظام معين، لذلك يرى البعض و نميل إلى رأيهم أنه يجب تخصيص نص يعاقب على التجسس على تلك الرسائل والبيانات المرسلة ، وإن كان هذا الفعل يمكن أن يدخل في نطاق المادة 303 مكرر من قانون العقوبات والتي تعاقب على المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية ومنها التقاط الصور أو تسجيل أو نقل المكالمات التي تدخل في إطار المعلومات الإلكترونية إن تم إستخدامها في نطاق نظام معلوماتي [2].

ومن التطبيقات القضائية لجريمة الدخول إلى نظام المعالجة الآلية للمعطيات ما قضت به إحدى محاكم الجنح الفرنسية بإدانة شخص كان مكلف بالرقابة والإشراف على سنترال تليفوني في شركة فرنسا للاتصالات، وذلك بتهمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات حيث قام هذا المتهم بإيصال جهاز المنتيل[3] Minitel بخط التجارب والألعاب "التيلماتيك" التى تمنح جوائز للفائزين..، حيث تزيد الجوائز تبعا لمدة الاتصال أو الاستعمال وقد أحيل المتهم إلى المحكمة بتهمة السرقة إلا أن المحكمة غيرت التكييف حيث اعتبرت أن الاتصالات التليفونية خدمة لا يمكن أن تكون محل للحيازة، واعتبرت الفعل جريمة دخول إلى نظام المعالجة الآلية للمعطيات[4].

[1]– رامي عبد الحليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجموعة الملتقى الدولي حول التنظيم القانوني للانترنيت، مجلة دراسات، 2009، ع 1، ص17-18

[2]– وما نلاحظه أن المادة 303 مكرر1 جرمت الاحتفاظ للتصور أو التسجيلات المتحصل عليها بالأفعال المذكورة في المادة 303 مكرر..
وأضافت عنصرا آخر وهو الوثائق مع أن المادة 303 مكرر لم تأتي على ذكر الوثائق و إنما ذكرت المكالمات والأحاديث و الصور...وهذا نقص في المواد نرجو من المشرع تداركه.

[3]– المنتيل، جهاز شبيه بجهاز الكمبيوتر المحمول لكنه صغير الحجم وله جميع خصائص الحاسب المحمول بالإضافة إلى أنه وسيلة اتصال.

[4]– وانتهت المحكمة إلى إدانة المتهم بمبلغ 750000 فرنك عن هذه الجريمة ....ينظر، عبد الفتاح بيومي حجازي، التجارة الالكترونية.، المرجع السابق، ص34.

كما قضت محكمة جنح باريس بإدانة أحد المتهمين بنفس الجريمة الذي كان يقدم نفسه على أنه مندوب المجموعة الفيدرالية (FBI) من أجل الحصول على خدمات الهاتف من بعض الشركات[1].

ومن خلال التبيان السابق لعنصر الدخول إلى نظام المعالجة الآلية للمعطيات بصفة غير شرعية يتضح أن هذه الجريمة تقع بمجرد إتيان النشاط فمجرد الدخول يعد جريمة بغض النظر عن الأفعال اللاحقة له[2].

2 – البقاء بالغش داخل نظام المعالجة

يتحقق هذا السلوك المجرم بتواجد الجاني داخل النظام المعلوماتي بدون رضا من له الحق في التحكم بالنظام[3]، ويكون ذلك إما بعد الدخول غير المشروع في النظام، أو في حالة البقاء داخل النظام بعد نفاذ الوقت المحدد للبقاء داخله وكثيرا ما يحدث ذلك إذا كان استعمال النظام بمقابل محدد بمدة زمنية..، وهو ما جعل البعض يطلق على هذا الفعل المجرم بسرقة وقت الآلة[4]، وقد تتحقق جريمة البقاء داخل النظام دون جريمة الدخول وذلك في الحالة التي يكون فيها الدخول إلى النظام عن طريق الخطأ أو الصدفة[5]، ومحل التجريم في هذه الحالة هو بقاء الجاني داخل النظام، إذ كان يجب عليه في هذه الحالة أن يقطع وجوده و ينسحب فورا[6].

---

[1]– عبد الفتاح بيومي حجازي، التجارة الالكترونية،المرجع السابق، ص34.

[2]– فبمجرد الدخول إلى النظام المعلوماتي تقوم الجريمة حتى لو لم يترتب على فعل الدخول ضرر، أو لم يحقق الجاني فائدة من الدخول سواء كان الدخول إلى النظام كله أو جزء منه..، كما يعد مرتكبا للسلوك المجرم كل شخص مسموح له بالدخول إلى جزء معين من النظام لكنه تعداه أجزاء أخرى.... ينظر، علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، الدار الجامعية للطباعة والنشر، بيروت، 1999، ص130-133.

[3]– رامي عبد الحليم، المرجع السابق، ص17.

[4]– شيماء عبد الغني محمد عطا لله، المرجع السابق، ص121، ينظر أيضا أمال قارة، المرجع السابق، ص111.

[5]– ويرى البعض أن هذه الجريمة كثيرا ما تتحقق من طرق العاملين في الشركات والمؤسسات الذين يبقون في النظام مع أن الوقت المحدد لهم قد انتهى، وبالتالي فإن تجريم البقاء داخل النظام هو موجه إليهم بالدرجة الأولى فاستعمال النظام بعد انتهاء الوقت المحدد يعد دخولا وبقاء في النظام، غير أن أحكام القضاء الفرنسي في هذا المجال تؤكد على ضرورة توافر القصد الجنائي.. وهو البقاء في النظام بغرض إستعمال في أغراض شخصية للمتهم، فمستخدموا الشركات الذين يستعملون أجهزة الحاسوب غالبا ما يستعملونها في ألعاب التسلية الأمر الذي يكلف الشركة مبالغ طائلة نظير استعمالهم لخطوط الهاتف... ينظر، شيماء عبد الغني محمد عطا لله، المرجع السابق، ص124.

[6]– أمال قارة، المرجع السابق، ص110.

كما يعد البقاء متحققا في الحالة التي ينسخ فيه الجاني معلومات مسموح بالإطلاع عليها فقط[1]، وقد يجتمع الدخول غير المشروع وعنصر البقاء غير المشروع وذلك عندما لا يكون للجاني الحق في الدخول إلى النظام ومع ذلك يدخل إليه و يبقى داخله، ويكفي أحدهما لقيام الجريمة حسب المادة 394 مكرر.

وقد ثار جدل فقهي حول الفاصل الزمني بين فعلي الدخول و البقاء[2]، والراجح أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني بالتجول داخل النظام أو يستمر في ذلك بعد انتهاء الوقت المحدد له، فإذا دخل الجاني إلى النظام وظل ولم يحرك ساكنا كانت الجريمة جريمة دخول فقط.

ويكفي لتحقق عنصر البقاء مجرد التواجد داخل كل أو جزء من النظام فمجرد التجول يكفي لقيام هذا السلوك المجرم[3] دونما أن يشترط لذلك المحو أو الإتلاف أو التعديل للمعلومات المتواجدة في النظام المعلوماتي ، و يرى البعض من الفقهاء أن الاستعمال التعسفي لنظام المعالجة الآلية للمعطيات لا يعد من قبيل الدخول أو البقاء، إذ أن المتهم في جريمة الدخول أو البقاء في النظام ليس له الحق في الدخول أو البقاء..، في حين أن المستعمل المتعسف له الحق في الدخول والبقاء غير أنه يستعمل الجهاز أو النظام في غير الغرض المخصص له، كأن يقوم بتشغيل برنامج خاص بالألعاب أو التسوق .

ب: الركن المعنوي لجريمة الدخول أو البقاء عن طريق الغش

جريمة الدخول إلى النظام المعلوماتي أو البقاء فيه من الجرائم العمدية التي تقوم بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، حيث يتوجب أن يكون الجاني عالما بعدم أحقيته في

[1]- يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور كخدمة الهاتف والتي يحصل فيها الجاني على الخدمة لكن دون دفع الثمن أو يحصل على الخدمة مدة أطول من المدة الممنوحة له.

[2]- ذهب رأي فقهي إلى القول بأن الدخول يتحقق منذ اللحظة التي يتم فيها الدخول فعلا إلى النظام و ذلك بعد فترة قصيرة من الدخول و تبدأ بعدها جريمة البقاء، وتنتهي بانتهاء حالة البقاء.. والعبرة بعلم الجاني أن بقاءه في النظام غير مشروع، و ذهب رأي آخر أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع، فإذا لم يستجب يعد عندها مرتكبا بجريمة البقاء داخل النظام بصفة غير مشروعة... ينظر، أكثر تفاصيل... أمال قارة، المرجع السابق، ص112.

[3]- علي عبد القادر القهوجي، المرجع السابق، ص134-136.

الدخول أو البقاء في النظام المعلوماتي ، وأن هذا الفعل مخالف لإرادة صحاب النظام، ومع ذلك يقوم بالدخول الى النظام أو البقاء فيه[1]، وأن يقوم بذلك الفعل بإرادته الحرة السليمة من أي عيب ، إذ قد ترتكب الجريمة من شخص واقع تحت الإكراه أو التهديد ... الخ ، بإستغلال مهاراته التقنية في الدخول لهذه الأنظمة وهذا يكون نافيا للمسؤولية الجنائية .

والملاحظ أن المشرع اشترط في المادة 394 مكرر السالفة الذكر أن يتم الدخول أو البقاء بطريقة الغش "...**كل من يدخل أو يبقى عن طريق الغش**"، ويقصد بطريق الغش في هذه الحالة سوء نية الجاني حيث يعلم بأن دخول النظام أو البقاء فيه ليس من حقه ومع ذلك يقوم بالدخول، وتستخلص سوء نيته باختراقه لنظام الحماية الخاص بنظام المعالجة[2]، وبالنسبة للبقاء فيستنتج من خلال العمليات والتصرفات التي قام بها الجاني داخل النظام ، ومع ذلك فإن الغش لا يظهر فقط من خلال عمليات خرق نظام الحماية وإنما أيضا من خلال الدخول أو البقاء دون وجه حق، وما نظام الحماية إلا وسيلة لإثبات سوء النية أو الغش[3]، أما بالنسبة للدخول بالصدفة او عن طريق السهو او الخطأ فالفقه يرى أن الدخول لا يوصف بعدم المشروعية ، وما على الشخص في هذه الحالة إلا أن يخرج متى إكتشف أنه دخل دون وجه حق ، فإن بقى و لم يخرج يتوافر في حقه القصد الجنائي وظهرت نية الغش لديه[4]، كما لا يتوفر القصد الجنائي إذا كان دخول الجاني أو بقاؤه مسموح به أصلا أو وقع الجاني في خطأ بشأن حقه في الدخول أو البقاء سواء من حيث النطاق أو الزمان[5].

[1]- عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام الكمبيوتر ، دار الفكر الجامعي، الإسكندرية، 2004، ص350.

[2]- وقد جاء في المادة 2 من إتفاقية بودابيست للإجرام المعلوماتي أنه يحق للدول الأعضاء أن تشترط بأن الجريمة ترتكب عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة داخله.

[3]- أمال قارة، المرجع السابق، ص123-124.

[4]- هذا وإن كان البعض يرى أن الدخول بطريق السهو أو الخطأ هو فعل غير مشروع لكن المشرع لا يعاقب عليه لإنتقاء القصد الجنائي ينظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام الكمبيوتر، المرجع السابق، ص35.

[5]- مدحت عبد الحليم رمضان، المرجع السابق، ص51-53

ومن خلال تحليلنا للنص المتعلق بجريمة الدخول والبقاء غير المشروع للنظام المعلوماتي نلاحظ أن المشرع قد أحسن صنعا في صياغة هذه المواد ولكن ما يعاب عليه هو عدم النص على فعل التداخل الذي يختلف عن فعل الدخول للنظام .

ثانيا : الظروف المشددة بموجب المادة 394 مكرر

تكملة لجريمة الدخول أو البقاء في النظام بحيث يمتد فيها إجرام الجاني إلى إحداث تغييرات داخل نظام عمله مما يؤدي إلى حذف أو تغيير معطيات متواجدة داخلة النظام المعلوماتي أو تخريب لسيره ، لهذا نجد أن المشرع الجزائري قد ربط بينها و بين جريمتي الدخول أو البقاء غير المشروع في النظام المعلوماتي بإعتبارها ظرف تشديد لها[1] ، بينما المشرع الفرنسي أورد نصين أحدهما عبارة عن ظرف تشديد لجريمة البقاء أو الدخول داخل نظام المعالجة، والآخر ينص على فعل إعاقة سير النظام المعلوماتي و الإخلال به بصفة مستقلة[2].

و الملاحظة التي يمكننا إبداؤها هنا أن المشرع الفرنسي نص على هذه الجريمة كظرف تشديد لجريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات بنص المادة 1/323 من قانون العقوبات الفرنسي، ثم نص على نفس الجريمة تقريبا بصفة مستقلة بنص المادة 2/323، أما المشرع الجزائري فقد اكتفى بالنص على هذه الجريمة كظرف تشديد لجريمة الدخول أو البقاء في نظام المعالجة، و الفرق بين الحالتين يكمن في أن تعطيل النظام المعلوماتي المقترن بجريمة الدخول أو البقاء

[1] – المادة 394 مكرر في فقرتها الثانية أنه "...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة ...".

[2] "النص المتعلق بظرف التشديد فهو ما جاء في المادة 1/323 التي تشدد عقوبة الحبس إلى ثلاث سنوات والغرامة إلى 45 ألف أورو إذا ترتب على فعل الدخول البقاء إلغاء أو تعديل بيانات مبرمجة في النظام أو الإخلال بسيره وهي تقابل المادة 394 مكرر في فقرتها الثانية..، أما النص الثاني فهو ما جاء في المادة 2/323 التي تنص على أنه "يعاقب على إعاقة أو الإخلال بسير نظام معالجة المعلومات بالحبس لمدة لا تزيد عن 5 سنوات والغرامة التي لا تزيد عن 75 ألف أورو"[2].

– 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.
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 œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende".

يكون بغير قصد، أما جريمة تعطيله المنصوص عليها بصفة مستقلة في المادة 2/323 من قانون العقوبات الفرنسي هي جريمة عمدية ، و عليه فان ضابط التفرقة بينهما يكمن في القصد و لتبيان تلك الظروف المشددة و ضابط التفرقة بينهاسنقوم بتحليلها وفق ما يلي:

أ – الحذف أو التغيير في معطيات النظام المعلوماتي

بناءً على المادة 394 مكرر في فقرتها الثانية[1] منها نجد أن الظرف المشدد لهذه الجريمة يشمل الحذف أو التغيير وهو ما سنتناوله فيما يلي:

1 – الحذف: قد يترتب على دخول الجاني أو بقائه في نظام المعالجة الآلية للمعطيات حذف لمعطيات هذه المنظومة أي أن يحدث نقص في معطياتها، ولا يشترط أن ينصب الحذف على جميع المعطيات المتعلقة بنظام المعالجة وإنما يكفي أن يحدث حذف جزئي لها، و التساؤل المطروح هنا حول هل يشترط أن يؤدي الحذف إلى تعطيل النظام؟ **و** بالرجوع إلى نص المادة المذكور سلفا نجد أن المشرع لم يشترط أن ينتج عن هذا الحذف تعطيل أو ضرر للنظام وبالتالي فمجرد وقوع حذف في معطيات المنظومة كاف لتشديد العقوبة.

2 – التغيير: يختلف التغيير عن الحذف فهو يفترض استبدال معطيات مكان أخرى نتيجة الدخول أو البقاء في النظام، فيبقى النظام في هذه الحالة سليما لكن بوجود معطيات مغايرة، كما أن التغيير لا يشترط أيضا تعطيل النظام أو فساده إنما مجرد التعديل يجعل السلوك المجرم قائما، فمصطلح "تغيير" مجرم لذاته تجريم الدخول أو البقاء داخل نظام المعالجة هو تجريم وقائي حتى لا يحدث تعطيل لهذا النظام أو المساس بالمعطيات الموجودة فيه و هذا احتراما لمبدأ الشرعية الجنائية فلا يهم بعدها إن حدث معه تعطيل للنظام أو تحسين أدائه بسبب ذلك التغيير، غير أن البعض يرى خلاف ذلك ويذهب إلى أن جريمة الدخول أو البقاء في صورتها المشددة تتحقق إذا نتج عن التغيير أو الحذف أو الإتلاف تعطيل لسير النظام أو عدم قدرته على أداء وظائفه بأكمل وجه .

[1] تنص المادة 394 مكرر في فقرتها الثانية".. تضاعف العقوبة إذا ترتب على الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة ."وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة...

ب : تخريب النظام المعلوماتي : كما نجد أن المادة 394 مكرر في فقرتها الثالثة [1]نصت على ظرف مشدد مستقل عن الظرفين السابقين وهو مجرم لذاته ،فالتخريب يقصد به هنا أن يترتب على الدخول أو البقاء داخل النظام إتلافه ، وبالتالي تعطيله عن أداء مهامه فمصطلح التخريب يشتمل على جميع الأوصاف المؤدية لعرقلة أو إفساد لوظائف النظام ، و الذي يحدث من خلال العبث في معطيات النظام المتعلقة بنظام سيره ، لهذا فالتخريب أكثر ضرر من فعل التغيير غير أن المشرع ربط بينه و بين نتيجته المتمثلة في تعطيل النظام فالجريمة هنا من الجرائم المادية التي يتطلب لقيامها تحقق النتيجة و إلا بغيابها سينعدم الظرف المشدد و تكون محل المتابعة فيها بموجب الدخول او البقاء عن طريق الغش للنظام المعلوماتي .

ومما لا شك أن فيه أن ظرف التشديد أتى هنا للعقاب على تخريب سير النظام المعلوماتي ، فإن كان النظام مخربا قبل الدخول أو البقاء فلا ظرف تشديد، غير أنه يكفي لقيام ظرف التشديد هذا أن يكون جزء من نظام تشغيل المنظومة مخرب والجزء الآخر سليم إذا وقع عليه التخريب.

و ما يجدر بنا الإشارة إليه هنا أن جريمة التخريب لسير النظام يستعمل فيها وسائل متعددة منها تخريب الجهاز ، أو بإستخدام الفيروسات ، أو القنابل المنطقية ، أو التغيير في الرقم السري ، أو تخريب أو إتلاف برنامج الدخول ينتج عنها تتوقف كامل أو جزئي للنظام أو إستحالة مطلقة لإستخدام النظام المعلوماتي و هو ما سنوضحه وفق ما يلي :

1 – الإعاقة أو العرقلة: وهي كل الأعمال التي من شأنها منع النظام بصفة كلية أو جزئية عن العمل وقد ترد الإعاقة على برنامج من البرامج التي يحتويها النظام[2]، ولا يشترط وسيلة معينة لحصول الإعاقة أو العرقلة فقد تتم مادياً عن طريق إتلاف أجهزة الحاسب الآلي أو شبكة الاتصال بتخريبها وكسرها أو حرقها، وقد يتم ذلك معنوياً وذلك عن طريق إدخال فيروسات داخل النظام أو تغيير كلمة السر أو تغيير نظام سيره ، لكن هل يشترط أن تقع هذه الجريمة بوجود تعطيل

[1]فتنص المادة 394 مكرر في فقرتها الثالثة".. وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة..."

[2]– شيماء عبد الغني محمد عطا لله، المرجع السابق، ص128.

بسيط أو بعبارة أخرى تعطيل غير مستمر؟ ، و بالرجوع إلى التقرير التفسيري المتعلق بشرح اتفاقية بودابست للإجرام المعلوماتي نجد أنها تشترط أن تكون العرقلة على درجة من الخطورة بحيث يُحرم صاحب النظام من الاستعمال العادي لنظامه، ويدخل في ذلك منع الخدمة أو التشفير بسوء نية، غير أن القانون الفرنسي[1] ،لم يفرق بين حالة الإعاقة الدائمة أو المؤقتة أو على فترات ، فأي توقف بسيط للنظام المعلوماتي قد يحدث خللا مما يتسبب في خسائر فادحة ، فيتحقق هذا السلوك المجرم عن طريق استخدام ما يعرف بالقنابل المعلوماتية ، أو بطاقات الوقف[2]، ولا يشترط في التعطيل أو العرقلة أن تكون إيجابية بل يمكن أن يتحقق ذلك عن طريق الامتناع كأن يمتنع الجاني عن القيام بعمل يفرضه عليه القانون أو الاتفاق.

ويشير التقرير التفسيري لإتفاقية الإجرام المعلوماتي أن العرقلة أو الإعاقة يجب أن تكون بدون وجه حق حتى تتحقق الجريمة، حيث الأنشطة العادية المتعلقة بإصلاح شبكات الاتصال أو تجربة نظام الحماية أو إدخال أنظمة متطورة داخل نظام المعالجة من قبيل الأفعال التي تتم بوجه حق ولا تعد سلوكاً مجرماً، كونها صادرة برضا صاحب النظام ، كما يتيح التقرير التفسيري السالف الذكر للأطراف الموقعة اختيار نظرية محددة لمعنى العرقلة أو الإعاقة في قوانينها الداخلية وذلك بتحديد إلى أي مدى يمكن اعتبار الأفعال من قبيل العرقلة[3].

وما ينبغي الإشارة إليه أن الأفعال المكونة لهذه الجريمة وصفت بأنها "عرقلة أو إعاقة" لسير النظام المعلوماتي في سيره و التي قد تكون في شكل كلي للنظام المعلوماتي أو في جزء منه فقط و متى تحقق ذلك تكون الجريمة قائمة في حق مرتكبها .

2 – الإخلال: وهو كل الأعمال التي تمس بحسن سير النظام المعلوماتي فهذا النوع من السلوك يجعل النظام غير قادر على أداء مهامه بصفة عادية، كالتقليل من سرعته أو عدم إتمامه للمهمة

[1]– حيث تنص المادة 2/323 من قانون العقوبات الفرنسي الجديد يعاقب على الأفعال التي تعوق أو تخل بسير نظام المعالجة الآلية للمعطيات أو البيانات بالحبس لمدة لا تزيد عن خمس سنوات والغرامة التي لا تزيد عن 100.000 أورو

[2]– أمال قارة، المرجع السابق، ص118.

[3]– عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام الكمبيوتر، المرجع السابق، ص41.

التي برمجَ لأجلها أو حتى الزيادة في سرعته بشكل يخل بالعمل به....، وبعبارة أخرى يقصد بالإخلال تعييب النظام الذي يؤدي إلى حصول نتائج غير تلك التي كان من الواجب الحصول عليها ، مما يؤدي الى ارباكه [1].

وعليه فإن الإخلال المتعلق بنظام المعالجة بالمفهوم السابق يختلف عن العرقلة أو التعطيل فهو لا يؤدي إلى توقف عمل نظام المعالجة أو إتلافه لكنه يجعل هذا النظام غير قادر على الاستعمال السليم والصحيح، وهذا النوع من الارتباك تتأثر به أجهزة الحاسب الآلي وكذا البرامج والأنظمة على حد سواء، ويتم هذا النوع من التعطيل إن صح التعبير بعدة تقنيات وأساليب هي نفسها تقنيات وأساليب الإعاقة أو العرقلة لكن النتيجة تختلف بإختلاف السلوك المجرم و نذكر منها:

* القنبلة المعلوماتية: بحيث يتم إدخال بعض المعطيات بواسطتها فتتكاثر داخل النظام وتحد من استعماله.

* استخدام فيروس: وتتمثل وظيفته في القيام بتغيير غير واضح داخل النظام فتجعل مخرجات النظام غير تلك التي كان من المفترض أن تخرج[2].

ب – مدى لزوم القصد الجنائي في الظروف المشددة بموجب المادة 394 /2 مكرر

تعتبر الظروف المشددة المنصوص عليها في الفقرة الثانية من المادة 394 مكرر نتيجة غير مقصودة من الجاني حالة ما اذا ارتكب الجريمة الأصلية في صورتها البسيطة و هي إما بموجب الدخول أو البقاء قبيل الجرائم غير العمدية فالحذف أو التغيير إعتبرهما المشرع نتائج غير إرادية صادرة عن الجاني ، و التي وقعت نتيجة تواجده الإرادي في النظام بموجب الجريمة الأصلية المرتكبة من قبله عن ارادة و علم ، وبالتالي فهي تقوم على أساس الخطأ غير العمدي ، فالظرف المشدد

[1] – شيماء عبد الغني محمد عطا لله، المرجع السابق، ص129.

[2] – عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام المرجع السابق، ص41-42

هنا ظرف مادي ذو طبيعة موضوعية هو نفسه النتيجة محل الظرف المشدد و المرتبط بالجريمة الأصلية – وهي جريمة الدخول أو البقاء غير المشروع – للقول بتوافره[1].

أما بالنسبة للظرف المشدد المتعلق بالتخريب و المنصوص عليه بموجب الفقرة الثالثة من المادة 394 مكرر فالمشرع كذلك لم يؤكد على القصد الجنائي و بالتالي اعتبرها غير عمدية معتمدا على المسؤولية الموضوعية لصاحبها اي انه اعتبره مسؤولا عن النتيجة المحققة جراء ارتكابه للجريمة الأصلية و هي جريمة الدخول او البقاء غير المشرووع للنظام المعلوماتي او غير المصرح او المرخص له و ما على المتهم هنا ان اراد نفي التهمة عنه ان يثبت ان النتيجة الواقعة لم يكن لتصرفه دخل في حدوثها و انما له علاقة بسبب آخر[2] ، و حينها لا يتابع متى تم التأكد من صحة إدعائه إلا بالجريمة في صورتها البسيطة اي بموجب الفقرة الأولى من المادة 394 مكرر .

إلا اننا نجد أن المشرع الجزائري قد خالف المشرع الفرنسي الذي نص على التعطيل أو الإفساد لنشاط نظام معلوماتي من خلال المادة 323-2[3] من قانون العقوبات الفرنسي التي تتطلب تخريب النظام المعلوماتي فالتعطيل او الإفساد يقابلهما التخريب الذي حسب المشرع الفرنسي لا يكون إلا مقصودا و نستشهد هنا بالقضاء الفرنسي الذي قضي بتوافر العمد في حق المتهم الذي زرع فيروسا على قرص ممغنط، حيث أن زرع الفيروس بهذه الطريقة يدل أن الجاني يعلم بأن القرص سوف يستعمل في عمل الجهاز وأن هذا الفيروس سوف ينتقل إليه[4].

[1]– أمال قارة، المرجع السابق، ص114.

[2]حالة القوة القاهرة أو الحادث المفاجئ مثلا .

[3]Art 323-3 du C.P.F
Dispose que "le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de donné est puni .. "
و هو ما تنص عليه المادة الخامسة من الإتفاقية للاجرام المعلوماتي في اطار الاعتداءات على سلامة النظام

[4]– وتعتبر الجريمة قائمة حتى ولو كان جهاز الحاسوب مزود ببرنامج ضد الفيروسات ذلك أن عدم استخدام هذه البرامج الحمائية لا ينفي توافر الركن المادي للجريمة... ينظر، شيماء عبد الغني محمد عط الله، المرجع السابق، ص130.

الفرع الثاني : جريمة التلاعب بالمعطيات المتواجدة داخل النظم المعلوماتي

نص المشرع على هذه الجريمة في المادة 394 مكرر1 من قانون العقوبات[1] و تقابلها المادة 323-3 من قانون العقوبات الفرنسي و الملاحظ هنا أن الإطار العام للنص جاء غير مميز لنوعية المعلومة بل جاء حماية لها على العموم و شاملا لكل أنواع التلاعبات بمختلف الوسائل التي قد تمس بها .

أولا : الركن المادي لجريمة التلاعب بالمعطيات داخل النظام المعلوماتي

يتضح من خلال المادة 394 مكرر1 من قانون العقوبات المادة 3/323 من قانون العقوبات الفرنسي و المادة 4 من إتفاقية الإجرام المعلوماتي أن السلوك المجرم ينحصر في أفعال الإدخال أو المحو أو التعديل ويكفي لتقويم هذه الجريمة توفر أحد الأفعال السالفة الذكر ، و على هذا الأساس فإن النص الجنائي هنا يحمي المعلومة المعالجة داخل النظام أو تلك التي مازالت في إطار المعالجة[2] و لا يتناول المعلومات المتواجدة خارج النظام المعلوماتي ، وسنتناول فيما يلي الأفعال المكونة للركن المادي لهذه الجريمة :

أ – الإدخال: حيث يعاقب المشرع كل من أدخل معطيات في النظام المعلوماتي بطريق الغش[3] حيث يعرف بأنه تغذية النظام بالمعلومات المراد معالجتها او بتعليمات لازمة لعملية المعالجة ويتحقق الإدخال عن طريق إضافة معطيات جديدة في نظام المعالجة الآلية[4]، وفعل الإدخال بيتم عن طريق إستخدام البرامج الخبيثة بغرض التعديل في البيانات الأمر الذي يؤثر على صحتها أو

---

[1] تنص المادة 394 مكرر 1"...كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"...، والتي تقابلها المادة 3/323 من قانون العقوبات الفرنسي التي تنص على : "كل من أدخل بسوء نية بيانات في نظام معالجة البيانات أو قام بسوء نية بإلغاء أو تعديل هذه البيانات يعاقب حتى 5 سنوات حبس و غرامة قدرها 75.000 أورو."، و تقابلها كذلك المادة 4 من اتفاقية بودابست لمكافحة الإجرام المعلوماتي في إطار الإعتداء على سلامة المعلومات.

[2] – لذلك يرى البعض أن الحماية الجنائية بخصوص هذه الجريمة تظل مستمرة طالما أن المعلومة داخل النظام في طريقها إلى المعالجة.. ينظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام... المرجع السابق، ص45.

[3] – عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الأنترنت ، المرجع السابق ، ص 378، أنظر علي عبد القادر القهوجي، المرجع السابق ص144 .

[4] – يصنف الفقهاء هذا النوع من السلوك ضمن الغش المعلوماتي الذي يتم عن طريق التلاعب وإدخال بيانات جديدة مصطنعة بغرض تغيير الحقيقة... ينظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام الكمبيوتر، المرجع السابق، ص46.

نسبتها أو قيمتها كما أنه يكون بغرض إتلافها او تشويهها أو تدميرها ، و هو أمر سهل القيام به خاصة في المراحل الأولى لتشغيل النظام و هي مرحلة إدخال المعلومات و بالتالي يكن من السهل تغذية النظام بمعلومات مغلوطة أو زائفة لم تكن موجودة فيه من قبل ، الأمر الذي يؤثر سلبا على المعلومات الموجودة فيه من حيث سلامتها و قيمتها .

كما يتميز فعل الإدخال أنه يقع في غالب الأحيان بمعرفة المسؤول عن قسم المعلومات المسند إليه وظائف المحاسبتية و التعاملات المالية على أساس الوضعية المتواجد فيها التي تؤهله للتلاعب غير المشروع بالمعلومات . فمن الصور التي يمكن للمسؤول القيان بإدخال معلومات مغلوطة نجد إدخال أسماء وهمية في كشوف المرتبات الأمر الذي يترتب عنه صرف مرتبات لموظفين وهميين ، كذلك التلاعب في معلومات التعاملات المالية كإدخال فواتير وهمية تحت إسم أحد الموردين .

و من التطبيقات القضائية في اطار ادخال معلومات مغلوطة داخل النظام المعلوماتي ما قضى به قضاء المحكمة العليا الفرنسية عام 1994 و هذا لما أيدت حكم بالإدانة لأحد الأشخاص المدان بتهمة إتلاف المعلومات لقيامه بإدخال معلومات مغلوطة متعلقة بالنسب الضريبية الخاصة بضريبة المبيعات في نظام معالجة آلية ، و ذلك في الإستمارة الخاصة بذلك ثم قام بإدخال بعض هذه المعلومات إلى النظام المعلوماتي . كما قضت محكمة جنح باريس بأن بتطبيق المادة 323-3 على واقعة أنطوت على إدخال برنامج " sniffer " ، و هو البرنامج الذي يعمل على شبكة الكمبيوتر القادر على الجمع التلقائي للمعلومات و التي يرسلها عبر الشبكة وهو برنامج و لس معلومة حيث انه ان اضيف للمعلومات داخل النظام المعلوماتي فلا يؤثر فيه بل مهمته هو تجميع المعلومات فقط ، و بناءا على تفسير نص المادة 323-3 رأت المحكمة انها تنطبق على هذه الواقعة[1].

[1]- لدى رشيدة بوبكر ، المرجع السابق، ص 252-253.

وبالرجوع إلى التقرير التفسيري لاتفاقية الإجرام المعلوماتي نجدها تفسر المادة 4 منها على أساس أنها جريمة غش معلوماتي، وقد ورد في التفسير أيضا أن فعل الإدخال يتضمن إدخال معلومات غير صحيحة على الحاسوب وكذا التلاعب في البرامج الموجودة فيه، وكل التدخلات في معالجة البيانات، وأضاف التقرير أن العقوبة تطال كل تلاعب تعسفي خلال معالجة البيانات بغرض الحصول دون وجه حق على منفعة إقتصادية له أو للغير.

لكن المشرع لم يشر إلى وجوب وقوع ضرر أو حتى بقصد وقوع ضرر أو تغيير، وبالتالي فإن مجرد إدخال معلومات على معطيات نظام المعالجة يشكل السلوك المجرم لهذه الجريمة، كما لا يهم صحة المعلومات المدخلة من عدمه فالعبرة بالإدخال لا بمدى صحة هذه المعلومات.

ب – الإزالة: وهو السلوك الثاني المنصوص عليه في المادة 394 مكرر1 من قانون العقوبات ويقصد بالإزالة المحو الجزئي أو الكلي للمعلومات المتواجدة داخل النظام أو النقل و التخزين لها في منطقة خاصة .

و على إثر ذلك تكون الإزالة عملية لاحقة عن عملية الإدخال للمعلومات المغلوطة ، فهي تفترض الوجود السابق لها ، فالمسؤول عن الحفظ يمكنه تدمير إتلاف المعلومات المكلف بحفظها داخل النظام.

و من القضايا ذات الصلة نجد قضية TRW Company Credit data التي كانت تعمل على تزويد عملائها من بنوك وشركات و متاجر –من خلال أنظمة المعلومات– بمعلومات تتعلق المركز الإئتماني لإفراد الجمهور نظير إشتراك يدفعه هؤلاء العملاء بحيث كان لها 50 مليون شخص معلوماتهم لدى الشركة ، فإستغل موظف بقسم علاقة المستهلكين و قام ببيع مراكز إئتمانية جديدة مختلقة لذوي المراكز الإئتمانية الضعيفة مقابل مبلغ مالي يدفعه هؤلاء ، فعمل الموظف على محو المعلومات المتعلقة بمركزيتهم الضعيفة و استبدلها بمعلومات تحسن من مركزهم [1].

[1] عبد الفتاح بيومي حجازي ، الحماية الجنائية للتجارة الإلكترونية ، المرجع السابق ، ص49

و هذه العملية شملت صور متعددة للتلاعب بالمعلومات و هي الإزالة ، المحو ، و التعديل و لم يتم كشف هذه الجريمة إلا بعد تقدم احد الأشخاص ببلاغ إلى مكتب التحقيقات الفيدرالي "FBI" بعدما تلقى عرضا من الموظف بتحسين سجله الإئتماني مقابل مبلغ معين .

ج – التعديل: وهو سلوك يدخل كذلك في تكوين الركن المادي لجريمة التلاعب بالمعلومات داخل النظام المعلوماتي ويقصد بالتعديل تغيير المعلومات الموجودة داخل النظام و استبدالها بمعلومات أخرى[1]، كما أنه يدخل في إطاره كذلك التلاعب في البرنامج بإمداده بمعلومات مغايرة تؤدي لنتائج غير تلك التي صمم لأجلها . وإستخدام الجاني هذا السلوك في جريمة التلاعب بالمعلومات نجده بكثرة في جرائم الإحتيال المعلوماتي بمجالاته المختلفة بما في ذلك أنظمة التحويل الإلكتروني للأموال أو بطاقات الإئتمان و أجهزة الصرافة الآلية نظرا لما تتميز به من سهولة عن طريق إحتجاز الأمر بالدفع الموجه من المصرف الآلي إلى نظام الحاسب الآلي ثم يُزور هذه الرسالة حتى يتم دفع المبلغ إلى حسابه الخاص، ويكفي الجاني أن يتوجه إلى شباك التوزيع بالبنك ليسحب الأموال بسرعة قبل اكتشاف الحقيقة[2].

ثانيا : الركن المعنوي لجريمة التلاعب بالمعطيات داخل نظام المعالجة

هذه الجريمة من الجرائم العمدية طبعا لا تقوم إلا بتوافر القصد الجنائي العام من علم وإرادة، والملاحظ أن المشرع أورد مصطلح "...بطريق الغش" أي أن هذه الأفعال يجب أن تتم بطريق الغش، وبالتالي يجب توفر سوء النية لدى الجاني عند إدخاله لمعطيات جديدة أو محو أو تغيير هذه المعطيات..، لأن ذلك قد يتم برضا صاحبها وعلمه أو عن طريق الخطأ وهنا تنتفي المسؤولية، وتطبيقا لذلك قضي في فرنسا ببراءة المتهم الذي باع مجلة ملحقة بشريط ممغنط يحمل فيروس مما أدى إلى تدمير جميع المعطيات في النظام التابع للمشتري، لكن محكمة الاستئناف

[1]– وتطبيقا لذلك قضي في فرنسا بتوافر هذه الجريمة في حق المتهم الذي قام بتعديل الفيشات الورقية الخاصة بالشركة التي تعمل بها ثم قامت بإدخالها في جهاز الكمبيوتر بالشركة... ينظر، شيماء عبد الغني محمد عطا لله، المرجع السابق، ص135.

[2]– ومن التطبيقات العملية لهذا السلوك قيام أحد المجرمين في ألمانيا بزرع فيروس في شبكة المعلومات متعلق بمستخدمي نظام خاص وذلك من أجل جمع معلومات شخصية لمستعملي هذا النظام بالإضافة إلى تعديل بعض البيانات المتعلق بهم. ينظر، رامي حليم، المرجع السابق، ص17.

استندت في قرار التبرئة على أساس أن المتهم لم يكن يعلم بوجود فيروس داخل القرص المرفق أي عدم توفر نية الغش لديه[1].

وعليه يجب في هذه الجريمة أن تتجه إرادة الجاني إلى فعل الإدخال أو الإزالة أو التعديل ثم يعلم أن نشاطه غير مشروع وأنه يعتدي على صاحب الحق في المعطيات ومع ذلك تتجه إرادته إلى ارتكاب الفعل، وفي هذه الحالة يتوفر القصد الجنائي[2]..، وترى محكمة النقض الفرنسي أن نية الغش يمكن استخلاصها من واقعة الإدخال مثلا فإستعمال قنبلة معلوماتية أو فيروس يدل على نية الغش لدى المتهم[3].

الفرع الثالث : جريمة التعامل غير الشرعي في معطيات النظام المعلوماتي

بواسطة المادة 394 مكرر2 [4]و التي تقابلها المادة 1-3/323 من قانون العقوبات الفرنسي[5] ، حيث نلمس أن المشرع مراده حماية المعطيات خارج النظام المعلوماتي ، فهو لم يشترط أن تكون المعطيات متواجدة داخل النظام ، و عليه التجريم شمل المعطيات في أي شكل كانت عليه .

أولا : الركن المادي لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي

يتمثل الركن المادي لهذه الجريمة في نوعين من السلوكات المجرمة تضمن المجموعة الأولى منها الأفعال المتعلقة بالتعامل غير الشرعي في معطيات يمكن أن يرتكب بها أحد الجرائم المنصوص

[1]- شيماء عبد الغني محمد عطا لله، المرجع السابق، ص138.

[2]- مدحت رمضان عبد الحليم، المرجع السابق، ص59-61.

[3]- شيماء عبد الغني محمد، المرجع السابق، ص138

[4]- نص المشرع على هذه الجريمة في المادة 394 مكرر2 من قانون العقوبات حيث جاء فيها "يعاقب بالحبس من شهرين إلى ثلاث سنوات و بغرامة مالية من 1000.000دج إلى 5.000.000دج كل من يقوم عمداً و عن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

[5] - " Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

عليها سابقا ، وتعد المجموعة الثانية بمثابة التعامل غير الشرعي بالمعطيات المتحصل عليها من الجرائم السابقة وسنتناول كلا المجموعتين وفق ما يلي :

أ – التعامل في معطيات صالحة لإرتكاب جريمة ماسة بنظام المعلومات:

ويكون التعامل وفق مجموعة من الأفعال التي عددتها المادة 394 مكرر2 في فقرتها الأولى و التي تقابلها المادة 323-3-1 من قانون العقوبات الفرنسي و هاته الأفعال هي:

1- التصميم la conception :

و الذي يتمثل في إعداد معلومات صالحة في إرتكاب الجريمة ، و هو عمل يقوم به المختصون في مجال البرمجيات و هم المبرمجون أو مصممي البرامج ، و من ذلك تصميم برنامج لأهداف تخريبية – البرامج الخبيثة les programmes virus أو البرامج المصممة من أجل الوصول للنظام المعلوماتي.

2– البحث la recherche :

البحث حول ماذا أو في ماذا ؟؟ فما المقصود بالبحث هنا هل البحث في كيفية تصميم المعلومات أي إجراء أبحاث فيما تعلق بإيجاد المعلومات حولها ؟ أم البحث في المعلومات التي تمكن من إرتكاب الجريمة؟

فالبحث في إطار الخدمات الإلكترونية المقدمة بواسطة الشبكة العنكبوتية و هو ما يسمى ب "محركات البحث" ، وهي عبارة عن برامج مساعدة للحصول على المعلومة على اساس ان الأنترنت بها كم هائل ومعتبر جدا من المعلومات ، فالباحث لديه هدف محدد من خلال بحثه وبالتالي فمحرك البحث يساعده لبلوغ هدفه المنشود من خلال تزويده بالمواقع المتخصصة ذات الصلة بموضوع بحثه ، ومن بين المحركات نجد yahoo و Google ومن هنا يظهر لنا أن البحث بهذه الكيفية يتعلق بحق الأفراد في الحصول على المعلومات و من منظورنا هو لا يدخل في إطار المعنى المقصود في المادة 394مكرر2 وبالتالي فالبحث هو البحث عن كيفية تصميم المعلومات و إعدادها .

3- التجميع le rassemblement:

وهو القيام بجمع قدر من المعلومات التي بإجتماعها مع بعضها تؤدي لإرتكاب الجريمة على النظام المعلوماتي و من هنا جاء النص عليها بصيغة الجمع بينما المشرع الفرنسي فقد إصطلح عليها الحيازة Détenir بينما إتفاقية الإجرام المعلوماتي فضلت مصطلح الحصول من أجل الإستخدام ، إلا ان المصطلح المعتمد من طرف المشرع الجزائري نراه اكثر دقة على أساس ان التجميع يقتضي وجود الحيازة لأكبر قدر من المعلومات دون وجود نية إستخدامها فبمجرد توافرها لدى الجاني يكون قد إرتكب الجريمة المعاقب عليها بالمادة 394 مكرر 2 .

4- التوفير disposition à Mettre :

لابد من الإشارة هنا أن المشرع الفرنسي في المادة 323-3-1 نص على "التوفير أو الوضع تحت التصرف" ، و في نفس السياق نجد أن إتفاقية الإجرام المعلوماتي نصت على عبارة أي "أشكال أخرى للوضع تحت التصرف" .

و مصطلح التوفير يشير إلى عرض المعلومات و إتاحتها و جعلها في متناول الغير ، بل وتحت تصرفه و حيازته ، و من ذلك نجد كلمة المرور ، الشفرة او الكود أو اي بيانات تسمح بالدخول لكل او جزء من النظام المعلوماتي و يدخل في اطارها كذلك ليشمل الكشف او الإفشاء العلني للثغرات الأمنية في النظام المعلوماتي و هو ما اشارت اليه المذكرة التفسيرية لإتفاقية الإجرام المعلوماتي ، كما يضم كذلك وضع اجهزة على الخط ليتم استخدامها بواسطة الغير تجميع الروابط بين الخطوط المتشعبة من أجل تسهيل الوصول لتلك الأجهزة ، و ذلك بالإحالة لبرنامج متصل ببرامج مصممة للإتلاف او هدم المعلومات أو للتدخل في عمل النظام المعلوماتي والذي يكون بواسطة الفيروسات .

و نلمس خطورة التوفير وفق المعنى السابق عن التجميع كون الأخير هو المستفيد منها بينما الأول فالمستفيدون من التوفير يكون عددهم كبير و تتسع دائرته و عليه فكلما كثر عددهم كانت الخطورة أكبر.

5- النشر la diffusion:

و يقصد به إذاعة المعلومات و التي مهما كان نوعها أو طبيعتها ، و تمكين الغير من الإطلاع عليها ، و للإشارة فالتشريع الفرنسي جاء خاليا من هذا السلوك و نجد الإشارة اليه في اتفاقية الإجرام المعلوماتي بموجب المادة 6 الفقرة 2 و بالرجوع للمذكرة التفسيرية نجد أنه ينبغي أن يمتد ليشمل كل النشاط من شأنه نقل المعلومات الى الآخرين .

و تكمن خطورة هذا السلوك في اتساع دائرة المذاع اليهم المعلومات مما يؤدي الى احتمالية اكبر ان تستعمل تلك المعلومات في الجرائم لذى احسن المشرع لما نص على تجريم هذا السلوك نظرا للخطر الكبير و الاحتمالية الاكبر لحدوث جرائم جراء اذاعة او نشر تلك المعلومات .

6-الإتجار a commercialisation :

الإتجار المقصود بالمادة 394 مكرر 2 ليس ذلك المقصود في القانون التجاري ، بل يشمل كافة التصرفات التي تكون بمقابل سواءا كان عينيا او نقديا ، حتى و لو لم ينص عليها القانون التجاري في اطار الاعمال التجارية المنظمة من خلاله .

و وفق هذا فأن الإتجار يختلف عن التوفير على اساس ان الأخير قد يكون بدون مقابل ، لهذا فالإتجار قد يكون جزء من التوفير لأنه يشمل تقديم المعلومات بمقابل او بدون مقابل .

إلا اننا نجد ان المشرع الفرنسي استعمل مصطلحا آخر و هو الإستيراد D'importer فهو يعتبر تقديم المعلومات سلوكا مجرما سواء كان بمقابل او بدونه، في حين اتفاقية الاجرام المعلوماتي تضمن البيع و الإستيراد ، بينما الإتجار يتصور وقوعه بالبيع و الإستيراد و الشراء لهذا نقول ان المشرع الجزائري يتجه نحو التوسع في تجريم التعامل في المعلومات التي يمكن ان ترتكب بها الجرائم مضوع دراستنا و هذا رغبة منه في الوقاية المسبقة او القبلية للحد من هذه الجرائم و ضمان لغياب النص التشريعي الذي يستفيد منه المجرم و افلاته من العقاب .

ب– التعامل في معطيات متحصلة من جريمة ماسة بنظام المعلومات:

وهي الصور الثانية لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي ، الواردة في نص المادة 394 مكرر2 الفقرة الثانية منها ، وتتم هذه الجريمة عن طريق الحيازة ، الإفشاء ، النشر الإستعمال ، و تلك السلوكات تعتبر فريدة من حيث النص لأن المشرع الفرنسي و حتى اتفاقية الإجرام المعلوماتي لم ينصا عليها وسنحاول شرحها وفق ما يلي :

1–الحيازة la Détention :

تعتبر الحيازة في إطار القانون الجنائي سيطرة الشخص على مال منقول بنية التملك والإحتباس و التي تكون مستقلة أي أن يمارس الشخص أي عمل مادي على المال بدون رقابة من شخص آخر له على المال سلطة قانونية أعلى بمقتضى حق من الحقوق ، و لهذا لا يعتبر حائزا العامل المرتبط بعلاقة عمل بالمعلومات لإنعدام السيطرة عليها بنية التملك و لا يمكنه ممارسة أي عمل عليها بدون تصريح من رب العمل ، و عليه فالحيازة من وجهة نظر القانون الجنائي لا تعد حقا او مركزا قانونيا ، بل هي مركز واقعي قد تكون مشروعة مستندة لسبب صحيح ، كما قد تكون غير مشروعة .

لهذا فحيازة المعلومات تكون بالسيطرة عليها سيطرة مطلقة يستطيع معها الحائز إتلاف المعلومات او تعديلها او الإنتفاع بها أو إستعمالها أو توجيهها ، كما انها قد تكون سيطرة محدودة تمكنه فقط من الانتفاع بالمعلومات او استغلالها في وجه محدد .

و لا تكفي السيطرة لقيام الحيازة ، بل لابد من توافر الإرادة القائمة على نية التملك و السيطرة على المعلومات ، مع العلم بذلك ، فهي ركن أصيل من اركان الحيازة .

2– الإفشاء la Révélation:

يفترض الإفشاء إنتقال المعلومات من حيازة الجاني الى الغير و هذا هو الفرق بين الإفشاء و الحيازة حيث ان الأخيرة ينحصر وجود المعلومات لدى الحائز دون تقديمها للغير في حين ان

الثانية نجد ان المعلومات يتم انتقالها من يد الحائز لها الى الغير و لا يشترط في الغير ان يكون من فئة معينة .

3- النشر :

لم يحدد المشرع وسيلة للنشر و على اثر ذلك يستوي ان يتم النشر عن طريق الأقراص المضغوطة او بالكتابة او بالطريقة الورقية او اي سيلة اخرى خاصة أن الوسائل التقنية الحديثة ساهمت في النشر السريع و بكفاءة عالية للمعلومات المتحصل عليها من جرائم الإعتداء على النظام المعلوماتي .

4- الإستعمال :

نجد أن المشرع قد توسع في دائرة التجريم حتى يصل الى الإحاطة الكلية بهذه الجرائم و من بين مظاهر توسعه نجد تجريمه لسلوك الإستعمال لأي غرض كان للمعلومات المتحصل عليها من الجرائم محل الدراسة، و نلمس مدى توفيق المشرع الجزائري فيما ذهب اليه خاصة ان الإستعمال غير المشروع للمعلومات يعد مجرما مهما كان الهدف منها ، و مهما كان نوع الإستعمال ، وباية وسيلة كان ذلك الإستعمال ، و لو لمرة واحدة فقط .

ثانيا : الركن المعنوي لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي

تعتبر هذه الجريمة من الجرائم العمدية التى يتطلب قيامها إثبات القصد الجنائي بعنصريه العلم والإرادة لدى الجاني أي علمه بأنه يقوم بإحدى السلوكات المنصوص عليها بالمادة 394 مكرر2 ، و أن سلوكه يكون وسيلة لارتكاب الجرائم الماسة بنظام المعالجة الآلية للمعطيات ، وأن يقوم بهذه الأعمال بإرادته الكاملة، ولكن إتفاقية الإجرام المعلوماتي في مادتها السادسة إشترطت صراحة توافر قصد إستعمالها في الجرائم المذكورة آنفا، وهو قصد خاص في هذه الجريمة وهو نية إسعمال هذه المعطيات في إرتكاب إحدى الجرائم الماسة بالنظام المعلوماتي .

و بالرجوع الى المشرع الجزائري نجده لم يتوقف عند اشتراط الغش للدلالة على القصد الجنائي العام كما هو الحال في المادتين 394 مكرر و 394 مكرر 1 ، بل نص كذلك على

العمد صراحة في الفقرة الأولى من المادة 394 مكرر2 التي جاء نصها "...عمدا و عن طريق الغش .." فهل يفهم منه ان المشرع تطلب قصدا خاصا لقيام هذه الجرائم ؟ حيث ان هناك راي يقول ان المشرع يتطلب القصدان العام و الخاص و هذا واضح من المصطلحان المستخدمان في الفقرة الاولى من المادة المذكورة اعلاه و المراد بالغش هنا هو القصد الخاص لوجود مصصطلح العمد الدال على القصد العام ، و ما يفند هذا الطرح هو نص الفقرة الثانية من المادة 394 **مكرر2** فلو كان المشرع يتطلب بقوله ""عن طريق الغش" قصدا خاصا ، فما حاجته ان يتراجع في المادة نفسها مقررا أن الجريمة تقوم "لأي غرض كان" اي مهما كان القصد لدى الجاني والوقائع التي انصرف اليها السلوك في اطار التعامل بالمعلومات ، و هو الأمر الذي يجعلنا نقول ان المشرع لم يتطلب قصدا خاصا يؤدي لوقائع محددةغير الوقائع التي تدخل في ما حدده المشرع و هذا هو القصد العام ، و من هنا فمصطلح عن طريق الغش لم تدل على قصد خاص لدى الجاني و إنما هي للتأكيد على العمد المطلوب في هذه الجريمة .

المطلب الثاني: تجريم الإتفاق و الشروع في ارتكاب جرائم الإعتداء على نظام معلوماتي

للمعاقبة على الجريمة لابد من وقوع الجريمة التامة وهو ما يتطلب البدء في النشاط الاجرامي الذي يهدف لتحقق النتيجة الإجرامية محل الحماية منها ، ولكن قد يضطر الجاني للتوقف لسبب خارج عن ارادته يؤدي به للتوقف او عدم اتمام الجريمة و بالتالي عدم تحقق النتيجة الاجرامية و في هذه الحالة لا تكن محل مساءلة جزائية ما لم ينص عليها المشرع صارحة في اطار الجنح اما في الجنايات فهي مجرمة لذاتها دون الحاجة لنص في ذلك الخروج و وضعت هذه القاعدة بغرض تقرير نوع من الحماية الوقائية المتقدمة في بعض الجرائم ذات الخطورة و لهذه الوضعية وما ينجر عنها نجد أن المشرع الجزائري جرم الإتفاق الجنائي في اطار جرائم الإعتداء على النظام المعلوماتي كما جرم الشروع فيها بنصوص صريحة و هذا ما سنتناوله وفق الفرعين التاليين :

الفرع الأول : الإتفاق الجنائي في إطار جرائم الإعتداء على النظام المعلوماتي

أولا : تعريف الإتفاق الجنائي

تنص المادة 394 مكرر5 من قانون العقوبات الجزائري على أنه: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة او اكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة افعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

تناول المشرع الجزائري تجريم الإتفاق بموجب المادة176 كما يلي: **"كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الاعداد لجناية أو أكثر معاقب عليها بخمس سنوات حبس على الاقل ضد الاشخاص أو الاملاك تكون جمعية أشرار وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل"** ، و تقابلها في التشريع الفرنسي المادة 145- 1من الباب 5 من الكتاب الرابع المعنون ب "**المشاركة في جمعيات الاشرار**" La participation à une association de malfaiteurs كما يلي:

"يشكل جمعيات الاشرار كل مجموعة او اتفاق تألف بغرض الاعداد لجنحة أو أكثر أو جناية أو أكثر معاقب عليها بـ 5 سنوات حبس وكان هذا التحضير مجسد بفعل أو عدة أفعال مادية فانه يعاقب على الاقل ب5 سنوات حبس.

واذا كانت الجريمة المعد لها جناية أو جنحة معاقب عليها ب 10 سنوات فان المشاركة في جمعيات الاشرار يعاقب عليها ب10 سنوات و 150000يورو غرامة.

واذا كانت الجريمة المعد لها جنحة معاقب عليها على الاقل ب 5 سنوات حبس فان المشاركة في جمعيات الاشرار يعاقب عليها ب5 سنوات حبس و 75000 يورو."

فمن خلال قانون العقوبات نلمس أن لم يتم التطرق للمقصود بالاتفاق أو الجمعية غير أن المسلم به أن الجمعية أو الاتفاق يقضي انعقاد ارادتين أو أكثر على ارتكاب الجريمة أو على

الاعمال المجهزة أو المسهلة لارتكابها ولا يهم مدة تشكيل الجمعية أو تأليف الاتفاق ، إلا أن الجمعية أكثر هيكلة من الاتفاق [1] .

و بعدم تطرق القانون لتعريفه نتطرق لبعض من الآراء الفقهية التي أثارت جدلا حول مدى ملائمة تجريم المشرع له و التي نوجزها في اتجاهين كما يلي:

ويرى أصحاب الإتجاه الأول أن الاتفاق الجنائي إن كان مبني على عقد العزم لإرتكاب الجريمة، الا أن المعاقبة عليه لا يعد استثناء على القاعدة المطردة التي لا استثناء لها التي تقضي بـ "عدم العقاب على مجرد العزم على ارتكاب الجرائم" ، و هذا يستند إلى أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها وانما يعاقب عليه في حد ذاته كجريمة خاصة تامة وحجة المعاقبة عليه أن العزم الاجرامي الجماعي ظاهر بمظهر مادي لأن كل عضو في الإتفاق الجماعي يعلنه عزمه للبقية فتتحد ارادتهم في مجال إتفاقهم ، فالاتفاق يكون هنا معلوما مثبتا بالإضافة إلى أنه ظاهرة تهدد الامن العام ، فهو يمتاز بوجهة الوقاية فنتيجته احباط الاتفاق الجنائي ليحال بين الجناة وبين تحقيق خططهم .

بينما الإتجاه الثاني يرى ان حجج الإتجاه الأول غير قويمة من خلال المقارنة بين خطورة الاتفاق الجنائي وبين خطورة الأعمال التحضيرية التي تصدر عن شخص يسعى لإرتكاب الجريمة بمفرده ، فالاتفاق الجنائي مرحلة مبكرة بالنسبة للتحضير للجريمة فهي ترد على المرحلة النفسية أي لمرحلة اتخاذ القرار وعقد العزم على ارتكاب الجريمة ، فلو صحت خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة لوجب على المشرع ان يجرم مرحلة التحضير للجريمة من باب أولى[2].

و بالرجوع الى التشريع نجد ان المشرع لم يتوسع في تجريم الاتفاق وتحديد نطاقه في اطار الاعمال التحضيرية ، فالمشرع الجزائري يعاقب على الاتفاق الجنائي معتمدا في ذلك على معيار خطورة الجريمة ومعيار جسامة العقوبة، حيث حدد في المادة 176 الجرائم الجائز في الاتفاق

[1] – أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة للطباعة والنشر، الجزائر، 2009، ص 472.

[2] – عبد الفتاح مصطفى الصيفي، قانون العقوبات، النظرية العامة، دار الهدى للمطبوعات، الاسكندرية، دس، ص247

الجنائي وهي الجنايات والجنح التي يعاقب عليها بـ (5) سنوات حبسا على الاقل ، و هو بهذا يأخذ بالإنتقادات السابقة حيث نجده لم يقم بتجريم مجرد العزم والتصميم على الاعداد للجرائم بل جرّم التحضير لها .

و هذا ما نلمسه في الجرائم موضوع الاتفاق فيما يتعلق بالاعتداء على النظام المعلوماتي كما سبق وأن رأينا عبارة عن جنح معاقب عليها بأقل من (5) سنوات حبس ، بل اشترط في الإتفاق أن يكون مجسدا بفعل أو عدة افعال مادية وهو ما يظهر بوضوح من خلال المادة 394 مكرر 5 من خلال عبارة : "... **وكان هذا التحضير مجسدا بفعل أو عدة افعال مادية** ..." فالمشرع الجزائري لم يتوقف عند حد المرحلة النفسية بل رفعه الى المرحلة المادية أي عملية البدء في التنفيذ.

وما قيل بخصوص المشرع الجزائري يقال أيضا بخصوص المشرع الفرنسي إذ لم يكتف بمجرد العزم بل تطلب تجسيده بأعمال مادية وهو ما يستفاد بوضوح من عبارة "... **وكان هذا التحضير مجسدا بفعل أو عدة افعال مادية، يعاقب** ..." الواردة بالمادة (323 - 4) التي تناولت بالتجريم الاتفاق الجنائي في نطاق المعالجة الآلية للمعلومات.

و عليه سندرس الاتفاق الجنائي في نطاق جرائم الاعتداء على نظم المعالجة الآلية شأنه شأن أي جريمة يتكون من اركان ويقرر له المشرع جزاء وهذا ما سنحاول دراسته وفق الآتي تبيانه :

ثانيا: أركان الاتفاق الجنائي

بإستقراء نص المادة 394 مكرر 5 نجد أن الإتفاق الجنائي لإرتكاب جرائم الاعتداء على النظام المعلوماتي مبني على ثلاثة أركانا: أ – المشاركة في الاتفاق، ب– الاعداد لجريمة من جرائم الاعتداء على النظم المعلوماتي ، ج – ركن معنوي هو القصد الجنائي وهو ما سيتم تفصيله فيما يلي:

أ- المشاركة في الاتفاق الجنائي

بالرجوع الى المادة 176 من قانون العقوبات الجزائري السالف ذكرها نجده العبارة التالية : "... **كل جمعية أو اتفاق مهما كانت مدته أو عدد أعضائه ... وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل**" ، بحيث يسير أطراف الإتفاق عن علم و بارادتهم في اتجاه واحد لتنصب في موضوع واحد و محدد ، و لا يهم الطريقة التي يعبر بها عن الارادة ، كالقول أو الكتابة أو الايماء ، و يقوم الإتفاق مهما كان الوقت المستغرق لانعقاد الارادات طال ام قصر، وسواء كان منظما أم كان عارضا من دون تعيين لكيفية التنفيذ أو تحديد للأدوار [1].

وهذا بالإضافة لإشتراط تجريم الاتفاق في الجرائم محل الدراسة أن يكون مجسدا بفعل أو عدة أفعال مادية ،أي أن المشرع الجزائري وان اكتفى بوجود العزم في ظل المادة 176 ، فإن المادة 394 مكرر5 الخاصة بالاتفاق ، تتطلب أن يكون مجسدا بفعل أو عدة أفعال مادية ، أي أن المشرع الجزائري تطلب فضلا عما سبق توضيحه وجود مرحلة أخرى بعد الإرادة أو العزم وهي مرحلة الأعمال التحضيرية التي تتجسد في أعمال أو أفعال مادية يكون القصد منها التحضير والاعداد لارتكاب إحدى جرائم الاعتداء على النظام المعلوماتي ، و هذا ما يتوافق مع ما اشترطه المشرع الفرنسي في ذلك مع بعض من الإختلاف من جانب هذا الاخير الذي نجده وان كان قد اشترط تجسيد هذا الاتفاق في أعمال مادية ، فانه قد عمم ذلك بموجب المادة 450-1 أو بالمادة 323-4 من قانون العقوبات الفرنسي .[2]

كما أن الاتفاق يشترط أكثر من عضوين كحد أدنى لعدد اعضاء الاتفاق[3] ، فلا يكفي لقيام الاتفاق تعدد الارادات وانما يتعين أن تتجه الى نفس جرائم الاعتداء على النظام المعلوماتي

---

[1] د. محمود نجيب حسني، شرح قانون العقوبات القسم العام النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، ط6 دار النهضة العربية القاهرة، 1989، ص485.

[2] – ومن امثلة التحضير المادي المعاقب عليه اقتناء شخصين برامج معدة خصيصا لاختراق نظم المعالجة الآلية تبادل المعلومات الهامة لارتكاب الجريمة كإعلان عن كلمة المرور أو رمز الدخول، أنظر آمال قارة، المرجع السابق، ص 132

[3] – عز الدين الديناصوري، عبد الحميد الشواري، المسؤولية الجنائية من قانون العقوبات والاجراءات الجنائية، ط3 منشأة المعارف، الاسكندرية، 1988 ص369.

بمعنى الإتحاد لإرتكاب نفس الجريمة ، و هو ما نلمسه من الالفاظ التي استخدمها المشرع الجزائري الواردة بنص المادة 394 مكرر5 " ...**مجموعة أو إتفاق**..." أو نص المادة 176 ".... **أو عدد أعضائه** ... " فعبارة **مجموعة** جاءت عامة اذ لم يقيدها بعدد معين وهو ما يفترض ضرورة وجود شخصين فأكثر وبمفهوم المخالفة اذا ارتكب العمل التحضيري المادي شخص واحد بمفرده وبمعزل عن غيره فلا يعاقب في هذه الحالة فالعقاب لا يتقرر الا في حالة **اجتماع شخصين فاكثر**.

ب- موضوع الاتفاق الجنائي:

يكفي أن يكون موضوع الإتفاق هو الاعداد لجريمة واحدة فحسب وهو ما يستفاد بوضوح من عبارة "...**لجريمة أو اكثر** ..." الواردة بالمادة 394 مكرر5 ، و **دون تعيين أو تحديد للموضوع الإتفاقي**[1] ، إذ يقوم الاتفاق بمجرد الاعداد والتحضير لها فحسب ، فمتى كان الاتفاق يتمثل في أعمال التحضير والاعداد لتلك الجرائم فان الاتفاق يكتسب صفته الاجرامية ولو كانت الأعمال في ذاتها غير ذات صفة اجرامية فالاتفاق على تعلم كيفية تصميم المعلومات التي تساعد على الاختراق مثلا يعتبر عمل مشروع لكنه يصبح غير مشروع إذا كان بنية استعماله في الجرائم التي تنص عليها المادة 394 مكرر وما بعدها.

و ما ينبغي الإشارة اليه هنا أن المادة 176 من قانون العقوبات تجرم الإتفاق الجنائي بغرض الاعداد لجناية أو أكثر أو جنحة أو أكثر ضد الاشخاص أو الأملاك و التي تشمل في نطاقها جرائم الاعتداء على نظم المعلومات بوصفها جنح ترتكب ضد الاملاك ، و هو ما يدفعنا للإشادة هنا بموقف المشرع الجزائري الذي قرر تجريم الاتفاق لإرتكاب جنحة الإعتداء على النظام المعلوماتي بنص خاص و التي لا يتجاوز حدها الاقصى عن 3 سنوات حبس مما حذا بالمشرع الى تخصيصها بأحكام خاصة لتفادي الثغرة القانونية او التناقض التشريعي وصولا الى حماية متكاملة

[1] – وبهذا تفترق جريمة الاتفاق الجنائي عن جريمة الاشتراك بالاتفاق في الجريمة، إذ يجب أن يقع الاشتراك على جريمة معينة أو على جريمة مكملة لجريمة معينة، ولكن الاتفاق الجنائي يقع على جريمة مقصودة غير معينة إذ ان قصد الشرع من ذلك واضح فهو يريد توسيع في دائرة جريمة الاتفاق الجنائي حتى لا يفلت المجرم من العقاب ومن اية ناحية. عز الدين الديناصوري، عبد الحميد الشواري، المرجع السابق، ص373.

للجرائم محل الدراسة ،كون المادة 176 تستهدف الاعداد للجنح المعاقب عليها ب5 سنوات حبس على الأقل .

ج- الركن المعنوي للاتفاق الجنائي

جريمة الاتفاق الجنائي جريمة مقصودة لا بد لقيامها من توافر القصد وهذا الاخير القائم على العلم والارادة وهو ما سيتم تناوله فيما يلي:

1- العلم:

يقصد بالعلم هنا أن يعلم كل طرف في الاتفاق الجنائي بماهية الدور المنوط له فيما تعلق بموضوع الاتفاق الجنائي وبما له من خصائص ، فالمشرع في اضفائه للصفة الاجرامية للأدوار يتجه لتحديد نوعية العلم بالدور و مكانته في تنفيذ الجريمة محل الدراسة و لا يبحث مجال العلم المسبق بالصفة الإجرامية للدور ذاته لأن ذلك أمر مفترض على نحو لا يقبل اثبات العكس ، و يترتب على ذلك ان من يجهل الغرض من الاتفاق وهو ارتكاب جنح الاعتداء على نظام المعلومات أو التحضير لها لا يعد القصد متوفرا لديه.

فمن يعتقد أنه انضم لمجموعة تتاجر تجارة عادية في برامج نظام المعلومات عادية في حين أن الإتجار كان في برامج خبيثة كالفيروس ، أو برامج الاختراق...الخ ، لا يعد القصد متوافر لديه و قد يكون كذلك إذا علم بعد دخوله الاتفاق بموضوعه غير المشروع الا أنه بالرغم من ذلك بقي فيه.

2-الارادة : لا يكفي مجرد الاشتراك في الاتفاق الجنائي مع العلم بموضوعه ، بل لابد من توافر الارادة لشخصين على الأقل لإرتكاب احدى الجرائم محل الدراسة مع نية القيام بالدور الذي سيعهد به اليهم ، فإذا لم تكن الارادة على هذا النحو، فغياب الجدية في النية كالهزل او العبث أو السعي الى الوشاية بأعضاء الاتفاق أو يريد مجرد استطلاع أمرهم دون الانضمام اليهم ي، هذا ما يجعل القصد ينتفي لانتفاء الإرادة الجادة.

الفرع الثاني: جريمة الشروع في ارتكاب جريمة اعتداء على نظام معلوماتي

أولا : مكانة الشروع

تمر الجريمة قبل تمامها بعدة **مراحل**، حيث يبدأ الجاني بالتفكير فيها و عقد العزم عليها وهي **مرحلة نفسية** تكون الجريمة عبارة عن فكرة أو مجرد إرادة، ولا عقاب عليها، لأنها مجرد أفكار ليس لها أي مظهر خارجي ملموس يوحي بخطورتها ، إلا إذا نص القانون على غير ذلك، ومن قبيل ذلك نجد المادة 176 من قانون العقوبات التي نصت على تجريم و معاقبة التصميم المشترك على القيام بالفعل.[1]

ثم تأتي بعد ذلك **مرحلة الأعمال التحضيرية**، وهي المرحلة الإنتقال لمرحلة وسطى بين التفكير في الجريمة والبدء في تنفيذها ، حيث تتصف بالمادية التي تقتضي من الجاني مباشرة أعمال استعدادا لتنفيذ جريمته ، منها إعداد أدوات التنفيذ أو تهيئة المناخ اللازم لارتكابها ، كاقتناء كالفيروسات، أو تصميم برامج اختراق يتم من خلالها الدخول غير المشروع للنظام ، فالمشرع لا يولي اهتماما للأعمال التحضيرية إلا اذا كانت تشكل خطر على المصالح و الحقوق التي يتوجب عليه حمايتها[2]، هنا يتدخل المشرع للحماية وفق نص تجريمي مستقل بذاته ، وفي نطاق الجرائم محل الدراسة راعى المشرع عند صياغته نصوص مواد الإعتداءات للنظام المعلوماتي بالعقاب على بعض الأعمال التحضيرية بوصفها جرائم مستقلة، ومن قبيل ذلك ما جاءت به 394 مكرر2 من الأفعال بوصفها جرائم مستقلة كالبحث والتصميم، كذلك المادة 394 مكرر 5 التي تعاقب على مجرد الأعمال التحضيرية في الصورة الاتفاق الجنائي.

و أخيرا نجد **مرحلة الشروع** ، أو مرحلة إنصراف إرادة الجاني لتنفيذ الركن المادي إلا أنها لا تكتمل لسبب لا دخل لإرادته فيه ، فالشروع بإعتباره جريمة ناقصة او غير تامة ، هذا النقصان لا يعتري الركن المعنوي فيها لأن القصد ثابت لدى الفاعل، وإنما يعتري الركن المادي، فالفاعل

[1]- وتقابلها في قانون العقوبات السوري المادة (325) تحت عنوان "جمعية الأشرار" الواردة ضمن الفصل الثالث بعنوان "في الجمعيات غير المشروعة".

[2]- عبود السراج، المرجع السابق، ص 307.

يقدم على أفعال تعتبر بدء في التنفيذ لكنه لا يتمكن من تحقيق النتيجة ، و هذه المرحلة تكون محل معاقبة من قبل المشرع فالمادة 30 من قانون العقوبات التي تنص على "**كل محاولات التي لإرتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى إرتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى و لم يكن بلوغ الهدف المقصود بظرف مادي يجهله مرتكبها** ." ، فالمشرع جرم الشروع في الجنايات بالمطلق و نص على ان الشروع في الجنح لا يكون مجرما الا بنص خاص و هذا ما ورد التأكيد عليه بموجب المادة 31 من قانون العقوبات التي تنص على " **المحاولة في الجنح لا يعاقب عليه الا بنص صريح في القانون** .

و المحاولة في المخالفة لا يعاقب عليها الاطلاق ."

لهذا نجد ان المشرع نص على تجريم الشروع في اطار الجرائم محل الدراسة على أساس أنها توصف بالجنحة التي تستلزم نصا خاصا بها ، و هو أقرته المادة 394 مكرر 7 التي جاء فيها " **يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها**"، و التي يقابلها في التشريع الفرنسي المادة 323-7 من قانونه العقابي حيث تنص على " **يعاقب على الشروع في الجرائم المنصوص عليها بالمواد من 323-1 الى 323-3-1 بالعقوبات المقررة للجريمة نفسها** ." و النص على تجريم الشروع في اطار الإعتداءات على النظام المعلوماتي نلمس منه رغبة المشرع في الإحاطة قدر الإمكان بالجرائم محل الدراسة .

ثانيا : أركان الشروع:

قرر المشرع تجريم الشروع في جرائم الاعتداء على نظم المعلوماتية و هي مسألة لزوم كي تتوافق مع تجريمه للاتفاق الجنائي فيها و من هنا نجد ان المشرع يمتلك نظرة متكاملة موصوفة بالشمولية في اطار الشق التجريمي للجرائم محل الدراسة ، و من هنا تكون دراستنا تنصب حول تحديد اركانه وفق الآتي توضيحه :

أ- الركن المادي:

لقيام الركن المادي في محاولة المساس بالنظام المعلوماتي لا بد من اجتماع عنصرين اثنين:

1- البدء بالتنفيذ:

اختلف الفقه في تحديد معيار هذا التمييز بين البدء في التنفيذ و الأعمال التحضيرية وانقسموا إلى مذهبين شخصي ومادي ، فيرى أصحاب المذهب المادي conception objective الذي يمثله الفقيه "فيلي" أن الفعل لا يدخل في دائرة التنفيذ إلا إذا أصاب به الفاعل الركن المادي للجريمة كما عرفها القانون، وهكذا فإن الأخذ بهذا المذهب يؤدي إلى إفلات أعمال كثيرة من العقاب بالرغم من أنها تتم عن قصد جنائي لدى الفاعل، أما المذهب الشخصي conception subjective فيبحث أنصاره في إرادة الجاني الإجرامية أي في مدى دلالة أفعال الشخص على قصده، ويرى الأستاذ "جارو" رائد المذهب أن الجاني يبدأ في التنفيذ إذا أتى عملا من شأنه في نظر الجاني أن يؤدي حالا ومباشرة إلى النتيجة المقصودة، وهو ما يعبر عنه بالفعل الذي لا يحتمل إلا تأويل واحد ويقابله الفعل القابل للتأويل.[1]

و يتلخص موقف المشرع الجزائري في اعتماده على المذهب الشخصي لتحديد البدء في التنفيذ، متأثرا في ذلك باتجاه المشرع الفرنسي، كما استفاد من تطور الاجتهاد القضائي الفرنسي الذي كرس عبارة "**الفعل الذي يؤدي مباشرة إلى ارتكاب الجريمة**" وهي العبارة نفسها التي استعملها المشرع الجزائري في المادة 30 من قانون العقوبات ، كما أنه لم يشترط أن يؤدي حالا إلى النتيجة لأن الشروع قد يستغرق مدة طويلة قبل أن تمامها ، إلا أنه لم يأخذ بالمذهب الشخصي بالمطلق ، بل أخذ كذلك بالمذهب الموضوعي و ذلك حينما ميز بين البدء بالتنفيذ والفعل الذي لا لبس فيه المؤدي مباشرة إلى ارتكاب الجريمة في ذات المادة السابقة الذكر ،كما يلي "... **الشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها**..." فباستعماله "**الشروع في التنفيذ**" إنما إشارة إلى **البدء بالتنفيذ** حسب المذهب المادي، وباستعماله "**الفعل**

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص 95، وعبود السراج، المرجع السابق، ص 310 إلى 313،

الذي لا لبس فيه المؤدي مباشرة إلى ارتكاب الجريمة" إشارة إلى البدء بالتنفيذ حسب المذهب الشخصي[1] .

وإن كان موقف المشرع الجزائري يبدو جليا على النحو السابق بيانه، إلا أنه ليس كذلك فيما يخص جرائم الاعتداء على النظم التي جرم المشرع أغلبية الأعمال التحضيرية لهذه الجرائم إدراكا منه لخطورتها باعتبارها جرائم مستقلة مقصودة قائمة بذاتها في المادة 394 مكرر 2.

ومع ذلك تعتبر المحاولة في ارتكاب بعض الجرائم كمحاولة إرسال كم كبير من الرسائل دفعة واحدة إلى النظام شروعا في جريمة إعاقة أنظمة المعلوماتية التي لم يجرمها المشرع الجزائري كجريمة مقصودة، و يعد كل فعل ماس بمعلومات النظم كمحاولة تغييرها أو تخريب محوها بدءا في تنفيذ جريمة التلاعب غير المصرح به بالمعلومات.

غير أن ذلك لا يعني تصور الشروع في جميع جرائم الاعتداء على نظم المعالجة الآلية، ففي جريمة الدخول غير المصرح به مثلا لا يتصور فيها الشروع لأنها –إعمالا للقواعد العامة– من الجرائم الشكلية أو من جرائم السلوك المحض، وبالتالي لا يكون هناك مجال للحديث عن الشروع، فلكي يكون هناك مجال للقول بخيبة الأثر لا بد أن يكون للفعل نتيجة، أو عدم تحققها لظروف خارجة عن إرادة الفاعل، وعلى ذلك فالجرائم الشكلية إما أن تقع بوقوع الفعل فتعد جريمة تامة وإما أن لا تقع أبدا.[2]

وتطبيقا على جريمة الدخول غير المصرح به، فحيازة كلمة المرور من قبل من ليس له الحق فيها لا يعد شروعا في هذه الجريمة، وإذا ما بدأ استخدامها وذلك باتصاله بالأنترنت عبر مزود اتصال بالأنترنت الذي ولج به إلى مواقع الكترونية في العالم الافتراضي ، كان ولوجه غير مصرح بالدخول إليها ، حينها يكون قد استغرق السلوك كاملا ، وهو ما يكفي لكي تقوم عليه جريمة الدخول التامة.

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي العام، المرجع السابق، ص 96.

[2]– عبود السراج، المرجع السابق، ص 254.

وفي هذا الصدد أشارت المذكرة التفسيرية لاتفاقية بودابست على صعوبة تصور الشروع في بعض عناصر الجرائم التي تستهدف عناصر أمن المعلومات، وتأسيسا على ذلك ألزمت الاتفاقية الأطراف بتجريم الشروع إلا في جرائم التلاعب غير المصرح به بالمعلومات، التعامل في معلومات غير مشروعة، فضلا عن اعتراض نظم المعالجة الآلية وإعاقتها، وهو ما يعني استبعاد الشروع في جريمة الدخول غير المصرح به، ومع ذلك نجد المشرع الجزائري يختم المادة 394 مكرر المتعلقة بالدخول أو البقاء غير المصرح بهما إلى نظام المعالجة الآلية كما يلي "... **أو يحاول ذلك**".

بل وحتى على فرض التسليم بقبول فكرة الشروع في جريمة الدخول غير المصرح به فإن الأمر تكتنفه صعوبات لا يمكن التغلب عليها، لعل أبرزها معرفة أو تحديد الأفعال التي تدخل في نطاق البدء في التنفيذ، وتمييزها عن الأعمال التحضيرية الغير معاقب عليها عند محاولة الدخول إلى النظام.

2- عدم إتمام الجريمة لظروف خارجة عن إرادة الفاعل:

إن البدء في التنفيذ غير كاف لتكوين الشروع إذا لم يتوفر العنصر الثاني وهو وقف التنفيذ أو خيبة أثر الأفعال نتيجة لظروف مستقلة عن إرادة مرتكبها أي بمعنى آخر لسبب اختياري.

- **الشروع الناقص:**

نص المشرع الجزائري في المادة (30) من قانون العقوبات الجزائري "إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها" وهو ما يعني أنه إذا كان عدم تمام الجريمة راجع إلى إرادة الفاعل فإن الشروع ينعدم، ويوصف تراجعه هذا على أنه عدول اختياري تميزا له عن العدول الإجباري الذي يتحقق معه الشروع في الجريمة، ويكون العدول اختياريا إذا كانت هناك أسباب نفسية خالصة دفعت الجاني إلى عدم المضي في إتمام الجريمة، أي لا يكون العدول ثمرة عوامل خارجية واجهت إرادة الفاعل إلى عدم إتمام الجريمة وإلا كان هذا العدول الاختياري يدخل بالفعل في دائرة الشروع.[1]

[1]- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، المرجع السابق، فقرة 397، ص 376.

وبتطبيق ذلك على جرائم الاعتداء على نظم المعالجة الآلية فإنه إذا دخل الجاني لأحد نظم المعالجة الآلية ثم بدأ بالتلاعب بالمعلومات ثم عدل عن إتمام الجريمة لعدم رغبته في إتمام النشاط الإجرامي أيا كان الباعث وراء هذا العدول فلا شك أن العدول في هذه الحالة منتجا لأثره في عدم توقيع العقاب طالما لم يكن مرجعه أسبابا خارجية، أما إذا توافرت هذه الأسباب كما لو دخل الجاني بطريق الصدفة المحضة إلى نظام المعالجة الآلية وأراد أن يستمر في البقاء على هذا الاتصال مع النظام بالرغم من أنه ليس له الحق في هذا الاتصال أو البقاء على الاتصال مع النظام، وحدث أن قام العاملين على نظام المعالجة الآلية باكتشاف دخوله إلى النظام فقام بقطع الاتصال عليه[1]، فإن الجريمة هنا قد وقفت عند حد الشروع.

وغني عن البيان أن العدول الاختياري لا ينتج آثاره إذا تمت الجريمة، كما أنه من ناحية أخرى يجب أن يكون سابقا على اللحظة التي تكتمل فيها عناصر الشروع، ويترتب على العدول الاختياري خروج الفعل من دائرة العقاب بوصفه شروعا في ارتكاب الجريمة، إلا أن الفعل قد ينطوي على تكييف قانوني آخر من ذلك الدخول غير المشروع متى توافرت أركانه وهي الصورة الغالبة.

- **الشروع التام:**

ويطلق على هذه الصورة بـ: "الجريمة الخائبة"، ذلك أن الجاني يأتي كل ما باستطاعته من سلوك ويفرغ منه، غير أن النتيجة لا تحقق لأسباب تتعلق بالظروف لا بالسلوك ولا بالوسيلة، وعبر المشرع الجزائري عن هذه الصورة بقوله "إذا لم يوقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة".

ولا أهمية للتمييز — من الناحية القانونية– بين الجريمة الخائبة والموقوفة وعلى الخصوص بالنسبة للتشريعات الجزائية التي تعاقب على الشروع بأنواعه بالعقوبة نفسها المقررة للجريمة التامة، ونعني بالذكر على وجه الخصوص القانون الجزائري والفرنسي والسوري.

[1]– محمد أمين الرومي، المرجع السابق، ص 107.

الجرائم الخائبة في مجال نظم المعالجة الآلية كثيرة، ومن صور ذلك إدخال برنامج فيروسي لأحد نظم المعالجة الآلية بغرض تخريب بعض المعلومات التي يحتويها إلا أن النتيجة لم تتحقق بسبب من أن النظام مشمول بحماية تدابير أمنية حالت دون ذلك.

- **إستحالة الجريمة :**

يقصد بها الحالات التي لا يتمكن فيها الجاني من تحقيق النتيجة الإجرامية على الرغم من إتيانه كل النشاط اللازم لتحققها، وذلك لأسباب كانت قائمة وقت ارتكاب الفعل، ولقد ثار خلاف في الفقه حول هذه الجريمة من حيث العقاب عليها، وما إذا كانت تلحق بالشروع المعاقب عليه أم أن الاستحالة تحول دون العقاب عليه.[1]

قرر المشرع الجزائري في نص المادة 30 "... **ولو لم يكن بلوغ الهدف المقصود لسبب ظرف مادي يجهله مرتكبها**"، ويلاحظ من خلال هذا النص أن المشرع قد أخذ بالرأي الفقهي التصالحي الذي يميز بين الاستحالة المادية والقانونية إذ يعاقب على الشروع في الجريمة وإن كان سبب عدم بلوغ الهدف ظرفا ماديا يجهله مرتكب الجريمة.

ومن أمثلتها في اطار الجرائم محل الدراسة استخدام الجاني شفرة غير صحيحة للدخول إلى نظام مدفوع الأجر قد قام صاحبها بإنهاء تعاقده مع المؤسسة المالكة للنظام.

[1] – وانقسم الفقهاء فريقين: فريق يقول بعدم العقاب وفريق يقول بالعقاب فيما ذهب فريق ثالث مذهبا وسطا (تصالحيا)، فالرأي الذي يرى عدم العقاب على الجريمة المستحيلة يستند إلى حجتين أولهما: البدء بالتنفيذ، ثانيهما: انعدام الاضطراب الاجتماعي الذي يترتب على الجريمة التامة وحتى أن وجد في الجريمة المستحيلة فإنها أقل بكثير عما يحدثه ارتكاب جريمة، أما الاتجاه الذي رأى وجوب العقاب على الجريمة المستحيلة بكافة صورها على سند من القول أو وقوع الشروع لا يتوقف على البدء في تنفيذ الفعل، وإنما يكفي لكي يقوم الشروع في القتل مثلا أن يأتي الفاعل من الأفعال ما يعد في نظره موصلا للقتل، ولو كانت هذه الأعمال لا تشكل بدءا في التنفيذ، ما دام هو نفسه يعتقد بأن من شأن أعماله إيقاع القتل الذي خاب، ولا أهمية بعد ذلك لمصدر استحالة الجريمة ولا لنوعها أو مداها، أما الفريق التصالحي فقد أخذ باتجاهين الأول: قسم الاستحالة إلى استحالة مطلقة واستحالة نسبية ورأوا ضرورة العقاب على الفعل في الثانية بوصفه شروعا دون الأولى، والثاني: قسمها إلى استحالة مادية واستحالة قانونية، للمزيد من التفاصيل حول هذه الآراء أنظر: أحسن بوسقيعة، الوجيز في القانون الجزائي العام، المرجع السابق، 97 وما بعدها، عبود السراج، المرجع السابق، ص 324 وما بعدها.

ب- الركن المعنوي:

الشروع جريمة مقصودة دائما يتخذ فيها الركن المعنوي صورة القصد الجرمي بعنصريه العلم والإرادة، وهو ما يعني ضرورة اتجاه الإرادة إلى ارتكاب الجريمة تامة لا إلى مجرد الشروع فيها، ويتطلب القصد الجرمي اتجاه الإرادة إلى نتيجة محددة، ويترتب على ذلك أنه إذا لم تتجه إرادة الجاني إلى إحداث نتيجة إجرامية محددة فلا محل للشروع، طالما أن الإرادة اقتصر مضمونها على الأفعال المرتكبة فقط، ويعاقب الجاني في هذه الحالة على ما حققه من أفعال إذا كانت بذاتها جريمة مستقلة[1]، ويترتب على ذلك أن مجرد الدخول إلى النظام المعلوماتي فلا يعني ذلك أن المتهم يحاول ارتكاب جريمة التلاعب بالمعلومات مثلا ما لم يتجه قصده إلى إتمام هذه الجريمة، وإنما قد يسأل عن دخول غير مصرح به متى توافرت أركانه.

كما نجد ان المشرع الجزائري اتجه إلى ذكر كل جرائم الاعتداء على نظم المعالجة الآلية بما فيها جريمة الاتفاق الجنائي، ثم أورد نصا خاصا بالشروع في الجرائم السابقة بقوله في المادة 394 مكرر 7 "**يعاقب على الشروع... المنصوص عليها في هذا القسم...**"

وهو ما يعني توسيع نطاق الشروع ليشمل الاتفاق الجنائي[2]، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي، إلا أنه للأسف توسع في نطاق العقوبة وحبذا لو يحذو المشرع الجزائري حذو المشرع الفرنسي الذي أخرج جنحة الاتفاق الجنائي للتحضير

[1]- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، المرجع السابق، فقرة 390، ص 373.

[2]- لقد ثار خلاف فقهي حول تجريم الشروع في الاتفاق الجنائي بين مناد به ومعارض، وفيما يلي سنبين هذا الاختلاف :

حيث ذهب فريق إلى القول بأنه لا يوجد شروع في الاتفاق على سند من القول أن الاتفاق حالة نفسية تقع عند الجناة في لحظة واحدة ولا تحتمل البدء ولا الانتهاء فهو لا يقع إلا كاملا ولا يتصور فيه البدء في التنفيذ.

وعلى نقيض الاتجاه السابق ذهب اتجاه إلى القول بإمكانية تصور الشروع في الاتفاق، محتجا بأنه طالما كانت أركان الشروع متصورة، ولم يكن القانون متضمنا نصا خاصا يقضي بعدم العقاب عليه فلا وجه للقول بالرأي السابق، فليس صحيحا أن الشروع في الاتفاق غير متصور، إذ الدعوى إليه أو الحمل عليه بدء في التنفيذ، فإذا توافر القصد الجرمي ولم يتم لأسباب لا دخل لإرادة الجاني فيها فالعقاب على الشروع متعين إذا كان الاتفاق جناية إذ لا يتطلب العقاب عليها نصا خاصا، وإذا كان الاتفاق جنحة فلا بد من وجود هذا النص.

لجرائم الاعتداء على نظم المعلومات من نطاق الشروع وذلك بموجب المادة 323-7 كما يلي "**يعاقب على الشروع في الجرائم المنصوص عليها 323-1 إلى 323-3-1**".

المبحث الثاني : مدى ملاءمة العقوبة في جرائم الاعتداء على النظام المعلوماتي

من أهم التوصيات التي أسفرت عنها الدراسات التي ناقشت ظاهرة جرائم الاعتداء على نظم المعلوماتية هي ضرورة إيجاد جزاء قانوني رادع يتم تعميمه على كل من يشارك في ارتكاب حالات الاعتداء على نظم المعلوماتية ، وتنبع أهمية العقوبة من كونها تشكل الإطار التنظيمي الوقائي الرّادع الذي يحيط بهذه النظم، فتكريس عقوبات رادعة يجعل التفكير بالاعتداء على هذه النظم من قبل العابثين أمرا في غاية الصعوبة، كما يضمن أمن المعلومات وعناصرها.

ولذا أشارت المذكّرة التفسيرية لاتفاقية بودابست على ضرورة أن يكون كل فعل مجرّم تم النص عليه في هذه الاتفاقية مستحق لجزاءات جزائية التي يجب أن تكون فعالة وملائمة ورادعة وذلك للحيلولة دون حدوث نتائج خطيرة، وهو ما أقرّته بموجب المادة 13 بعنوان "الجزاءات والإجراءات" كما يلي "يجب على كل طرف أن يتخذ الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية من أجل اعتبار الجرائم الجنائية المشار إليها في المواد 2-11 تستأهل جزاءات فعالة وملائمة ورادعة بما في ذلك عقوبات سالبة للحرية.

ويجب على كل طرف أن يضمن الأشخاص المعنوية يمكن أن تكون مسؤولة وفقا للمادة 12 وأن تكون محلا لجزاءات أو إجراءات جنائية أو غير جنائية فعالة وملائمة ورادعة، بما في ذلك جزاءات ماليّة".

فالاتفاقية تؤكد على ضرورة تكريس عقوبات فعالة وملائمة ورادعة تتناسب وخطورة هذه الأفعال، وادراكا لأهمية المسألة فضلا عن ازدياد الوعي بخطورة هذا النوع المستحدث من الاجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى رغم المجال الواسع الذي لا حدود له إذ أصبح كل فرد له كل القدرة في أن يصبح عدوا شرسا لأي اقتصاد بأكمله، واقترافه ليس من الطبقة المثقفة فحسب بل من قبل الجميع بمختلف الأعمار ومستويات التعليم، نتيجة تبسيط وسائل تكنولوجيا المعلومات وانتشار الانترنت كوسيلة نقل المعلومات، ولذلك ألحق المشرّع الجزائري تعديلا على القسم السابع مكرر من قانون العقوبات المتضمّن المساس بنظم المعالجة

الآلية، وذلك بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 ومسّ به تشديد عقوبة الغرامة دون المساس بالنصوص التجريمية الواردة في هذا القسم سابع مكرر من القانون رقم04-15 .

وإلى جانب المشرع الجزائري، نجد أيضا المشرع الفرنسي الذي قام – وبناء على توجيهات اللجنة الأوربية رقم 2000/31/ec حول بعض الأوجه القانونية لخدمات مجتمع المعلوماتيّة وخاصة التجارة الالكترونية في السوق الداخلية – بتعديل قانون العقوبات وذلك بموجب القانون رقم (2004 - 575) المؤرخ في 21 جوان 2004 والمتعلق بالثقة بالاقتصاد الرقمي

La LOI n° 2004 – 575 du 21 juin 2004 pour la confiance dans l'économie numérique (len) destine a transposer la directive européène 2000/31/ec du 18 juin 2000 (directive sur le commerce éléctronique).

حيث مسّ هذا التعديل القسم الخاص بالجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات وذلك بتشديد عقوبة الحبس والغرامة المقررة لهذه الأفعال وذلك بموجب المادة (45) من الفصل الثاني منه بعنوان La Lutte contre la cybercriminalité.

من منطلق أن العقوبة تمثل إحدى آليات الإستراتيجية القانونية الوقائية ذات الوصف الردعي و التي اعتمدها المشرع الجزائري وغيره من التشريعات الجزائية المقارنة في سبيل الحماية من وقوع جرائم لو وقعت لسببت خسائر اقتصادية فادحة بل وقد تستهدف أمن و إستقرار الدولة الى غير ذلك من النتائج محل الإعتبار في الحماية الجنائية ، لذى نجد أن قانون العقوبات الجزائري تبنى مبدأ المسؤولية الجزائية للأشخاص الطبيعية في اطار الجرائم محل الدراسة إلى جانب المسؤولية الجزائية للأشخاص المعنوية ، وسنفصل ذلك فيما يلي:

المطلب الأول: العقوبات المقررة على الشخص الطبيعي.

المطلب الثاني: العقوبات المقررة على الشخص المعنوي .

المطلب الأول: العقوبات المقررة على الشخص الطبيعي

بالرجوع إلى نصوص قانون العقوبات الجزائري والفرنسي نجدهما ينصان أساسا على العقوبات الأصلية المطبقة على مختلف الجرائم المرتكبة في مجال الجنوح التقني، وطبقا للمبادئ والاتجاهات الحديثة المتعلقة بالعقوبات يتضمنان إضافة للعقوبات الأصلية قائمة للعقوبات التكميلية.

الفرع الأول: العقوبات الأصلية:

يحدد القانون لكل جريمة عقوبة أو أكثر أصلية، وهذا هو شأن جرائم الاعتداء على نظم المعالجة الآلية، وهذه العقوبة قد تكون بسيطة (عادية)عندما لا تقترن بأي ظرف من ظروف التشديد، كما قد تكون مشدّدة عندما تقترن بظرف من ظروف التشديد.

أولا : العقوبات البسيطة:

لكي تكون الأمور واضحة فضّلنا أن نبين العقوبة التي تخضع لها كل جريمة على حدى كما يلي:

أ – عقوبة جريمة الدخول أو البقاء غير المصرح بهما (البسيطة):

إذا لم ينجم عن الدخول أو البقاء غير المصرح بهما إعاقة أو إفساد النظام أو إزالة أو تعديل للمعلومات فإن العقوبة تكون:

1 – في التشريع الجزائري:

الحبس من (3) أشهر إلى سنة والغرامة من (50000) إلى (200000) دينار جزائري.

وذلك بموجب المادة (394 مكرّر) المعلة بموجب القانون رقم (06-32) المؤرخ في 20 ديسمبر سنة 2006 بعدما كانت عقوبة الغرامة في حدها الأقصى مائة ألف دينار جزائري (100000دج)، والملاحظ أن تشديد عقوبة الغرامة كان الهدف منه الحدّ من تفشي ظاهرة الاجرام في نطاق المعالجة الآلية للمعلومات ونتيجة لما ارتآه المشرع من خطورة قيام الأشخاص بالدخول رغما لما لها من سرّية، الأور الذي يعرض الشركات والادارات التي تعتمد في تسيير

شؤونها على نظم المعالجة الآلية إلى الانتهاك خاصة بعدما خطت الحكومة الجزائرية مؤخرا خطوات خجولة نحو إرساء مشروع الحكومة الالكترونية المنتظر تطبيقه عام 2013. هذا وقد جعل المشرع للقاضي حدّا أدنى وحدّا أُقصى للعقوبة حتى تكون له سلطة تقديرية في تفريدها بحسب ما تتطلبه الحالة المعروضة أمامه.

2 – في التشريع الفرنسي:

الحبس لمدة سنتين وغرامة تقدر بـ: (30000 يورو).

لم تكن العقوبة في وقت ليس بالبعيد كما هي عليه الحال الآن، ذلك أن المشرع الفرنسي عندما سنّ اول قانون تناول فيه بالتجريم جرائم الاعتداء على نظم المعالجة الآلية، وهو القانون رقم (88 -19) المؤرخ في 5 جانفي 1988 المتعلق بالغش المعلوماتي، كان الحدّ الأدنى وكذا الأقصى منخفضًا[1]، وهو بهذا يقترب كثيرا من العقوبة التي قررها المشرع الجزائري، ولعل أن تفسير ذلك أنه من المنطقي أن يسمح المشرع بفترة تحذير للناس بلغة يفهمها الجميع حوا المستهدف من القانون وردّة الفعل حال تخطي حدوده، ولكي يمكن القيام بالتحذير فإنه يجب ان يكون ذلك بشكل واضح، فأساس المبادئ المقررة لأغلب الجرائم الخطرة كالقتل والسرقة تعود إلى مئات السنين كما أنها لم يصاحبها تغيير كبير عبر الزمن[2].

والظاهر أن المشرع الفرنسي قد تخطى هذه الفترة بما يقرب (6) سنوات من إقراره أول قانون يجرّم العدوان على المعلومات ونظم معالجتها، ليأتي بقانون العقوبات لسنة 1994 ليجعل من عقوبة هذه الجرائم حدّا واحدا سواء كانت بالحبس (الشهرين) أو بالغرامة (خمسة عشر ألف يورو "15000 يورو") ليسلب القاضي سلطته التقديرية في التحرّك بالعقوبة.

---

[1] Art 462-2 du A.C.P.F dispose que : «quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2000 f à 50000 f ou de l'une de ces deux peines..».

[2] أورين كير، المرجع السابق، ص15.

ولأن الجرائم في تطور مستمر تبعا لتطور تقنية المعلومات وما ينجم عن ذلك من نموّ دائم للخسائر الناجمة عنها، فقد قام المشرع الفرنسي مرة أخرى بتشديد العقوبة وذلك بموجب المادة (45) من الفصل الثاني من القانون رقم (2004 - 575) المؤرخ في 21 جوان 2004 المتعلق بالثقة بالاقتصاد الرقمي، وذلك بعد عشر (10) سنوات أخرى على تعديل سنة 1994 وستة عشر (16) سنة على أول قانون، لتصبح العقوبة سنتين والغرامة ثلاثين ألف (30000 يورو)، وقد احتفظ المشرع الفرنسي بالحدّ الواحد للعقوبة سواء كانت الحبس أو الغرامة وضاعف كلا من العقوبتين.

نستخلص مما سبق أن المشرع الفرنسي لا يألوا جهدا في محاولته لمواجهة جرائم تقنية المعلومات عامة، وجريمة الدخول أو البقاء بصفة خاصة، فقد بدأ مبكرا في مواجهة هذه الجرائم، ولم يتأخر في إجراء التعديلات التشريعية متى رأى ضرورة لذلك.

وإن كان ذلك كذلك، فإن جريمة الدخول أو البقاء تبقى في أسفل سلم العقوبات المقررة على الجرائم الواقعة على المعلومات ونظم معالجتها في القانون الفرنسي[1].

ب – عقوبة جريمة التلاعب غير المصرح به بالمعلومات:

1 – في التشريع الجزائري:

الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وغرامة (4000000دج).

أخضع المشرع الجزائري المتلاعب بنظم المعالجة الآلية سواء في صورتها البسيطة أو المشددة –كما سنرى–، وهو واضح بدليل المادة (394 مكرر1)[2] من قانون العقوبات كما يلي "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000دج إلى 4000000دج كل من أدخل..".

ولعلّ هذا التشديد له ما يبرّره، لأن جريمة الدخول والبقاء غير المصرح بهما في صورتها البسيطة لا تؤدي إلى أضرار معينة بالمعلومات أو النظام، بل حتى في صورتها المشددة، وإن أدت

[1] Voir : Raymons gassin. Op. Cit ; p 36.

[2] المعدلة بموجب القانون رقم (06 - 32) المؤرخ في 20 ديسمبر 2006.

إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعلومات (إزالة – إدخال – تعديل)، ذلك أن هذه الأخيرة جريمة يتوافر لدى مرتكبها القصد الجرمي للتلاعب في حين ينتفي لدى الدّاخل أو الماكث في صورتها المشددة، مما يمكن القول على ضوئه أن الجني في الجريمة الأولى أشد خطرا من الجاني في الجريمة الثانية في صورتيها، الأمر الذي يستوجب التفريق بينهما في نطاق العقوبة وهو ما تفطّن له المشرع الجزائري.

هذا وتأتي عقوبة الحبس في جريمة التلاعب في أعلى سلّم العقوبات المقررة على جرائم الاعتداء على النظم المعلوماتية، فهي تزيد على عقوبة جريمة الدخول والبقاء غير المصرح بهما في حدّها الأدنى، وتتساوى معها في حدّها الأقصى، بينما تأتي جريمة التلاعب في وسط السلّم من حيث عقوبة الغرامة، فغرامة هذه الجريمة والمقررة بأربع ملايين (4000000دج) أكبر من غرامة جريمة الدخول أو البقاء غير المصرح بهما التي تتراوح بين خمسين ألف (50000) ومئتا ألف (200000)دج، وأقل من غرامة جريمة التعامل في معلومات غير مشروعة والتي تتراوح بين مليون (1000000) وعشرة ملايين (10000000)دج.

2- التشريع الفرنسي:

الحبس (5) سنوات وغرامة تقدر بقيمة (75000يورو).

بالعودة إلى المادة (462 – 4) من قانون 1988 نجد أن المشرع الفرنسي كان يعاقب المتلاعب بالمعلومات بالحبس من ثلاثة (3) أشهر إلى ثلاثة (3)سنوات والغرامة من ألفي (2000 فرنك) إلى خمسمائة ألف (500000 فرنك)، إلا أنه وبعد تعديله لقانون العقوبات بموجب القانون رقم (92 – 1336) المؤرخ في 16 ديسمبر 1992 فقد جعل حدّا واحدا لهذه العقوبة، إذ أزال الحد الأدنى لها وثبتها عند الحد الأقصى وهو ثلاث (3) سنوات، أما عقوبة الغرامة فجعلها خمسا وأربعين ألف (45000 يورو).

والملاحظ أن عقوبة جريمة التلاعب غير المصرح به بالمعلومات تفوق عقوبة جريمة الدخول أو البقاء غير المصرح بهما، ورغم عدم تساوي عقوبتي التلاعب والدخول أو البقاء غير المصرّح بهما

فإنهما متقاربتان كثيرا مما أدى بالفقه إلى انتقاد هذا الوضع[1]، وهو تقارب العقوبة بين جريمة مقصودة وأخرى غير مقصودة (بالنسبة لظرفها المشدد).

ولقد استجاب المشرع الفرنسي لهذا النقد وقام بتعديل نصوص جريمة التلاعب وكذا الدخول أو البقاء بالقانون رقم (575 - 2004) المؤرخ في 21 جوان 2004، حيث قام برفع عقوبة جريمة الدخول أو البقاء إلى ثلاث (3) سنوات بينما رفع عقوبة جريمة التلاعب إلى خمس (5) سنوات لتصبح المادة (323 - 2) كالتالي "...يعاقب بالحبس 5 سنوات وغرامة تقدر بـ 75000 يورو...".

وقد كانت عقوبة جريمة التلاعب في القانون الفرنسي مساوية دائما لعقوبة جريمة إعاقة وإفساد نظم المعالجة الآلية، وقد فسر ذلك في الجمعية الوطنية الفرنسية بالتقارب الكبير بين الجريمتين، وتعذّر التمييز بينهما في بعض الأحيان كما فسّر أيضا بأن فعل إعاقة النظام يكون بالضرورة عن طريق إدخال المعلومات، وهي صورة من صور التلاعب بالمعلومات[2].

ج – عقوبة جريمة التعامل في المعلومات غير المشروعة:

1 - في التشريع الجزائري:

الحبس من شهرين (2) إلى ثلاث (3) سنوات والغرامة من (1000000) إلى (10000000) دج.

وذلك بموجب الفقرة (1) من المادة (394 مكرر 2)[3] كما يلي "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000دج إلى 10000000دج كل من..."، وبذلك يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول أو البقاء غير المصرح بهما سواء في صورتيها البسيطة أو المشددة، وبين جريمة التلاعب بالمعلومات (غير أن حدها الأدنى يقل عن كلتا الجريمتين) ذلك أن التعامل في معلومات غير مشروعة يزيد عن الحد

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية، 2007، ص 191.

[2] المرجع نفسه، ص 192.

[3] المعدلة بموجب القانون رقم 06 – 32 المؤرخ في 20 ديسمبر 2006.

الأقصى لجريمة الدخول أو البقاء في صورتيها (سنة أو سنتين)ويتساوى مع الحدّ الأقصى لجريمة التلاعب بالمعلومات (3 سنوات)غير أن حدها الأدنى يقل عن الجريمتين معا لأنه في جريمة الدخول أو البقاء البسيطة هو ثلاث (3) أشهر بينما في صورتها المشددة ستة (6) أشهر، أما في جريمة التلاعب هو ستة (6) أشهر.

غير أن ترتيب هذه الجريمة من حيث عقوبة الغرامة يأتي في المرتبة الأولى، فالغرامة في هذه الجريمة تفوق كثيرًا مقدار الغرامة في جريمة الدخول أو البقاء غير المصرح بهما والمقدر من خمسين ألف (50000) ومئتا ألف (200000) دينار جزائري، وكذلك في جريمة التلاعب بالمعلومات والمقدر مقدار الغرامة فيها من خمسمائة ألف (500000) إلى أربع ملايين (4000000) دج.

2 – في التشريع الفرنسي:

بالعقوبة المقررة للجريمة نفسها.

بالعودة للمادة (323 – 3 – 1) نجد أن المشرع الفرنسي عاقب على جريمة التعامل في معلومات غير مشروعة بالعقوبة المقررة للجريمة نفسها، بما يعني لعقوبة جريمة الدخول أو البقاء غير المصرح بهما أو جريمة التلاعب بالمعلومات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية التي يمكن أن تؤدي البرامج والأجهزة والوسائل المتعامل فيها إلى ارتكابها وذلك كما يلي "يعاقب بالعقوبة المقررة للجريمة نفسها...".

وبرأينا حسناً فعل المشرع الفرنسي بعقابه الجناة بعقوبة الجريمة نفسها، ذلك أنه ليس من مقتضيات العدالة ولا المنطق المعاقبة على جريمة معينة بصفتها أعمال تحضيرية لجريمة أخرة بعقوبة أشد من عقوبة تلك الأخيرة.

فجريمة التعامل في معلومات غير مشروعة هي من الجرائم الشكلية أو جرائم الخطر، والغاية من تجريمها هو سدّ الطريق أمام كل من يريد ارتكاب جرائم الدخول أو التلاعب، وإذا كان الأمر على ما سلف، فإن الأفعال الممثلة للنشاط الجرمي فيها تعد – وعلى حدّ قول بعضهم

وبحق[1] – من قبيل الأعمال التحضيرية لجريمتي الدخول أو البقاء غير المصرح بهما وجريمة التلاعب بالمعلومات، من ثم لا يصح في نظر المنطق القانوني ولا العقلي أن يقرر للأعمال التحضيرية لجريمتي الدخول أو البقاء والتلاعب عقوبة أشد من عقوبة الجريمة ذاتها !! وهو المنطق الذي سار عليه المشرع الفرنسي وخالفه المشرع الجزائري.

وفيما يتعلق بالنصوص الحالية وفي انتظار تدخل المشرع الجزائري يمكن للقاضي استعمال سلطته التقديرية في التحرك بين حدّي العقوبة الأدنى والأقصى بالنسبة لجريمة التعامل في معلومات غير مشروعة وجريمة الدخول أو البقاء غير المصرح بهما وجريمة التلاعب بالمعلومات بحيث يحول دون أن تكون العقوبة المقررة لجريمة التعامل أكثر من عقوبة الجرائم المقررة لارتكابها.

ثانيا : الظروف المشددة:

تأثرا بنظرية تفريد العقاب، قد يجد المشرع أن العقوبة التي قررها أصلا كجزاء للجريمة المرتكبة تصبح غير كافية في ظروف أو حالات محددة، فيرتب على تحققها تشديد العقوبة، وهو ما رآه المشرع في جرائم الاعتداء على نظم المعالجة الآلية، والظروف المشددة في هذه الأخيرة قد تكون إما تبعا لصفة المجني عليه، أو تبعا للنتيجة المترتبة.

أ – التشديد تبعا لصفة المجني عليه:

قد تأخذ بعض التشريعات عند تجريمها للعدوان على المعلومات بالاعتبار الجهة التي تتبعها وتولي اهتماما أكبر بالمعلومات التي تتبع الدولة والجهات العامة، ولذلك نجد بعض المشرعين يقصر الحماية على تلك المعلومات فقط دون المعلومات المتعلقة بالأفراد إلا إذا كانت هذه الأخيرة تمسّ مصالح الدولة، ويمكننا أن نلمح هذا الاتجاه بوضوح في القانون الفدرالي الأمريكي لجرائم الحاسب الآلي، فالمادة (1030) (أ) (3) منه لا تعاقب على الدخول المجرد إلا إذا كان محلّه الحاسبات

[1] محمد خليفة، المرجع السابق، ص 220.

الآلية التي تعمل داخل الحكومة الفدرالية أو الحاسبات التي ترتبط بها مصالح هذه الأخيرة، وكذلك الأمر بالنسبة لجريمة إتلاف المعلومات والبرامج[1].

والأمر نفسه نجده في قانون إساءة استخدام الحاسبات الآلية في المملكة المتحدة وفي اليابان، إذ لا تشمل هذه القوانين الحماية من جريمة التلاعب بالمعلومات إلا تلك المعلومات التي تستخدمها مؤسسة عامة، أو معلومات الأفراد التي تنطوي على التزام أو حق، وفي أستراليا تقتصر الحماية على المعلومات التي تحتويها الحاسبات الآلية التابعة للكومنولث أو تعمل لحسابه، أما غيرها من المعلومات فيشترط أن تكون أفعال الاتلاف التي تصيبها قد ارتكبت بواسطة إحدى الخدمات التي يقدمها، أو يديرها الكومنولث أي بواسطة شبكات الاتصال[2].

وقد أخذ المشرع الجزائري هذا الأمر بعين الاعتبار، فهو وإن بسط حمايته الجزائية على المعلومات بمختلف أنواعها بغض النظر عن الجهات التي تنتمي إليها فقد شدد العقوبة إذا كانت تلك المعلومات التي تم العدوان عليها تتعلق بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام نظرا للخطورة البالغة التي تنجم عن الاعتداء عليها، وهذا ما نصت عليه المادة (394 مكرر) كما يلي: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ودون الاخلال بتطبيق عقوبات أشدّ".

وكما هو ملاحظ فإن المشرع الجزائري يجعل من صفة المجني عليه ظرفا مشددا لعقوبة جرائم الاعتداء على النظم، إذ شدد العقوبة لتصبح ضعف العقوبة المقررة لجرائم الاعتداء على النظم التابعة للأفراد العاديين وأشخاص القانون الخاص.

وإذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة فتضاعف الغرامة مرتين، إذ تضاعف إلى خمس مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من طرف شخص معنوي – كما سنرى – ، ومن ثم يضاعف ذلك إلى ضعفين

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 217.

[2]– نفس المرجع السابق، ص 224.

لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة إلى عشر أضعاف عمّا هو مقرر على الشخص العادي.

وبرأينا أن المشرع الجزائري أحسن عملا بتشديده العقوبة إذا استهدفت معلومات حساسة كتلك المتعلقة بالدفاع الوطني، ذلك أن الجاني الذي يخرج عن أصوله وقوميته ويأتي عملا من شأنه النيل من النظم المتعلقة بالمؤسسات العامة والدفاع الوطني فإنه نذالة وإجرام في حق نفسه وفي حق وطنه مما يستدعي أخذه بمنتهى القسوة، فضلا عما يتطلبه الأمر من وجوب العمل على سلامة وأمن القوة العسكرية التي حفظها وسلامتها حفظ وسلامة للدولة بأكملها.

وبالرجوع لقانون العقوبات الفرنسي فلا نجد أي نص يشدد الحماية على المعلومات ونظمها والمتعلقة بالجهات العامة، وبالتالي فإن العقوبة المقررة للجاني الذي يستهدف المعلومات المتعلقة بالدفاع الوطني والمؤسسات والهيئات الخاضعة للقانون العام هي نفسها المقررة للجرائم التي تستهدف المعلومات المتعلقة بالأفراد والجهات الخاصة.

ب – التشديد تبعا للنتيجة المترتبة:

نصّت الفقرة الثانية والثالثة من المادة (394 مكرر)[1] من قانون العقوبات الجزائري على أنه: "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من (50000 دج) إلى (300000 دج).

وكما هو ملاحظ فإن المشرع الجزائري قد جعل من النتيجة المترتبة ظرفا مشدّدا للعقوبة في جريمة الدخول أو البقاء غير المصرّح بهما، فإذا كان المشرع الجزائري أخضع الجاني في جريمة الدخول أو البقاء لعقوبة بسيطة تتراوح من 3 أشهر الى سنة وغرامة من (50000) الى (200000) دج فان العقوبة تشدد وهذا في حالتين وهما:

[1] المعدلة بموجب القانون رقم (06 – 32) المؤرخ في 20ديسمبر سنة 2006.

الحالة الاولى: اذا نجم عن هذا الدخول أو البقاء حذف او تغيير لمعلومات المنظومة: فترفع العقوبة الى ضعف تلك المقررة للجريمة المجردة او البسيطة سواء في حدها الادنى الذي يضاعف الى ستة أشهر أو في حدها الاقصى الذي يضاعف الى سنتين. أما الغرامة فترفع للضعف أي تتراوح من 100000 الى اربعمائة الف 400000دج

الحالة الثانية: اذا نجم عن هذا الدخول أو البقاء تخريب لنظام اشتغال المنظومة فترفع عقوبة الحبس من 6 اشهر الى سنتين، أما الغرامة فيثبت حدها الادنى عند خمسين الف 50000دج في حين يرتفع حدها الاقصى عند ثلاثمائة الف 300000دج.

والى جانب المشرع الجزائري نجد ان المشرع الفرنسي الذي . بدوره . جعل من جسامة النتيجة ظرفا مشددا لعقوبة جريمة الدخول او البقاء غير المشروع إذ ترتفع العقوبة متى نجم عن الدخول او البقاء حذف او تغيير او تخريب اشتغال المنظومة، وهذا ما نصت عليه الفقرة الصانية (2) من المادة (323. 1)[1] كمايلي "... إذا ترتب على الافعال المذكورة حذف او تغيير لمعطيات المنظومة أو تخريب اشتغال هذا النظام تصل العقوبة الى 3 سنوات حبس وغرامة 45000يورو غرامة ".

أما في ظل قانون 1988 رفع المشرع عقوبة الحبس في حدها الاقصى من سنة الى سنتين، بينما ترك الحد الادنى كما عليه وهو شهرين، كما رفع الغرامة في حديها الادنى والاقصى[2]

وكذلك الشأن مع قانون العقوبات لسنة 1994 الذي احتفظ بنفس عقوبة الحبس ورفع عقوبة الغرامة الى ثلاثين الف (30000) يورو، اما قانون العقوبات الفرنسي لسنة 2004 فقد رفع عقوبة الحبس الى ثلاث سنوات للجريمة البسيطة، ورفع الغرامة الى خمس وأربعين الف يورو 45000 يورو.

[1] المعدلة بموجب المادة (45) من الفصل الثاني من القانون رقم (2004. 575) المؤرخ في 21 جوان 2004 المتعلق بالثقة بالاقتصاد الرقمي.

[2] Art_ 462- 2 alinéa 2 du A.C.P .F dispose que ; Lorsqu'il en sera résulté soit la suppression ou la modification de données continues dans le système ; soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois a deux ans l'amende de 10000 f à 100000f

ويلاحظ على المشرع الفرنسي أنه قد شدد العقوبة الا أنه لم يرفعها الى الضعف كما فعل المشرع الجزائري ولعل ذلك راجع الى سببين:

1 – ان عقوبة الجريمة البسيطة تضاعفت ولا يمكن مضاعفتها مرة أخرى بالنسبة للجريمة المشددة.

2 – هو استجابة لانتقاد الفقه بوجود فارق كبير بين العقوبة البسيطة والمشددة.[1]

الفرع الثاني : العقوبات التكميلية

تتمثل هذه العقوبة في المصادرة والغلق وهو ما سيتم تناوله فيما يلي:

أولا : المصادرة

ان تجريم السلوك الذي يهدد نظم المعالجة الآلية في سريتها أو سلامتها واتاحتها ووفرتها ليس كافيا لمعاقبة أو ردع الجناة، فبعض هؤلاء المجرمين حتى وان تم توقيفهم وادانتهم سوف يكون بوسعهم حيازة الاشياء التي استخدموها في ارتكاب جرائم لاستخدامها لأغراض اجرامية او أغراض أخرى، وعلى الرغم من توقيع بعض العقوبات سوف يظل الشعور باقيا بأن الجريمة مثمرة في مثل هذه الظروف، لهذا كان من الضروري اتخاذ آليات أو تدابير عملية للحيلولة دون افادة المجرمين من الاشياء التي استخدموها في تحقيق سلوكياتهم الاجرامية، ومن أهم الوسائل للقيام بذلك هو ضمان توافر أنظمة تقضي بمصادرة الاشياء التي استخدمت في ارتكاب الجريمة وهذا ما نصت عليه المادة (394 مكرر 6) بقولها "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الاجهزة والبرامج والوسائل المستخدمة " وهذا مسلك حسن لأثره الشخصي (في نفسية الفاعل) والموضوعي في فعالية مواجهة هذا النوع من الجرائم.

ويتضح من خلال عبارة "يحكم بمصادرة " الواردة في المادة اعلاه أن المصادرة وجوبية متى تعلق الامر بالأجهزة والبرامج والوسائل المستخدمة هذا من جهة.

ومن جهة اخرى يفهم من عبارة الوسائل المستخدمة ان موضوع المصادرة لا يقتصر على وسيلة معينة وانما يتسع ليشمل أي وسيلة تستجد مهما كان نوعها أو طبيعتها إذ لا يهم فيما إذ

[1] محمد خلفية، المرجع السابق، ص 174.

كانت هذه الوسيلة معلوماتية او تقليدية، مادية او معنوية معدة خصيصا لارتكاب تلك الجرائم أو ذات طابع مزوج فضلا عن ذلك يلزم ان تكون الاشياء التي يحكم بمصادرتها قد استخدمت في ارتكاب الجريمة وهو ما يستشف صراحة من عبارة "المستخدمة" الواردة بالمادة (394 مكرر 6) وفي كل الاحوال فان عقوبة المصادرة يجب الا تخل بحقوق الغير حسن نية، وعرفت المادة (15. 2) من قانون العقوبات حسن نية بأنه "يعتبر من الغير حسن النية الاشخاص الذين لم يكونوا شخصيا محل متابعة أو ادانة من أجل الوقائع التي أدت إلى المصادرة ولديهم سند ملكية أو حيازة صحيح ومشروع على الاشياء القابلة للمصادرة".

واحترام المشرع لحسن النية يأتي منسجما مع مبدأ الشرعية وحسن النية هذا يشير الى الشخص الذي يجهل حقيقة العلاقة بين المال الذي له حق عليه والجريمة المرتكبة، وكذا من يعلم بهذه العلاقة دون جدوى.[1] ومن امثلة الغير حسن النية في هذا الاطار مالك نظام للمعالجة الآلية (وليكن حاسوب محمول مثلا) الذي سرقه الجاني واستخدمه في تخريب نظام للمعالجة الآلية تابع لحد الشركات التجارية، ففي هذه الحالة يتعين مراعاة حقوق هذا الشخص حسن النية بحيث تمتنع المصادرة أو ينتقل موضوعها الى الدولة محملا بهذه الحقوق، وهذا ما نص عليه المشرع الفرنسي بموجب الفقرة الاخيرة من المادة (131- 21) من قانون العقوبات الفرنسي كما يلي: ان الشيء المصادر- ما عدا الحكم الخاص بالأشياء المتوقع تلفها- تؤول ملكيته الى الدولة لكن تبقى محملة بالحقوق العينية المكونة شرعا لمصلحة الغير.

والى جانب المشرع الجزائري نجد المشرع الفرنسي الذي بدوره قد نص على عقوبة مصادرة الاشياء التي استخدمت او كان من شأنها ان تستخدم في ارتكاب الجريمة أو نتج عنها وذلك بموجب الفقرة الثالثة من المادة (232- 5) من قانون العقوبات.[2]

[1] باسم شهاب، مبادئ القسم العام لقانون العقوبات وفقا لأحدث التعديلات بالقانون رقم 23 لسنة 2006، د.م.ج، وهران، 2007، ص279

[1] Voir. Art 323-5 alinéa 3du C.P.F

ثانيا :الغلق

الى جانب عقوبة المصادرة نص المشرع على عقوبة تكميلية وجوبية اخرى هي عقوبة الغلق وذلك بموجب المادة (394مكرر6) كما يلي: "مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على اغلاق المحل أو مكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالكها".

فكما هو ملاحظ ان المشرع الجزائري قد جعل لعقوبة الغلق محلين الاول هو المواقع محل الجريمة والثاني هو محل أو مكان الاستغلال.

فبالنسبة للأول، فلو تأملنا قليلا في التعبير الذي استخدمه المشرع الجزائري في المادة السابقة لوجدناه غير سليم، إذ أنه يستعمل عبارة المواقع التي تكون محلا للجريمة ما يعني المواقع التي تتضمن نظم المعالجة والتي تم الاعتداء عليها وبعبارة أدق المواقع الضحية والقول بذلك يجعل من المجني عليه جانبا وهو قول غير صحيح لذلك كان اولى بالمشرع الجزائري أن يستعمل عبارة "المواقع التي تستعمل في ارتكاب الجريمة "بدل عبارة المواقع التي تكون محلا للجريمة

أما المحل الثاني الذي تقع علي عقوبة الغلق أيضا فهو محل أو مكان الاستغلال وهو المكان الذي استعمله الجناة في ارتكاب جريمتهم، وكان يحوي الوسائل الالكترونية التي استعملت في عملية الدخول غير المصرح به أو في عملية التلاعب أو في عملية التعامل في عمليات غير مشروعة بل كانت تحوي هذه الوسائل كما هو الحال في مقهى الانترنت أو يتم التعامل فيها بواسطة هذه الوسائل داخل هذا المحل.

فضلا عن ذلك. يمكن أن يحوي هذا المحل أو المكان المعلومات الصالحة لارتكاب الجريمة أو المعلومات المتحصلة من جريمة دون أن يحوي تلك الوسائل.[1]

بل يكفي في هذا المكان كما وصفته المادة (394مكرر6) أن يكون مكان استغلال lieux d'exploitation

[1] محمد خليفة، المرجع السابق، ص 123.

هذا ولم تحدد المادة (394 مكرر 6) مدة معينة للغلق وعليه وعملا بالقواعد العامة من قانون العقوبات تكون عقوبة مؤبدة أو مؤقتة وذلك وفقا للمادة (16- 1)[1] من قانون العقوبات بقولها يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة بمناسبته، ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر سنوات في حالة الادانة لارتكاب جناية أو خمس سنوات في حالة الادانة لارتكاب جنحة...

والى جانب المشرع الجزائري نجد المشرع الفرنسي بدوره قد نص على عقوبة الغلق كعقوبة تكميلية تشترك فيها جميع جرائم الاعتداء على نظم المعالجة الآلية وذلك بموجب البند الرابع 4 من المادة (323-5) كما يلي **"غلق لمدة 5 سنوات أو اكثر المؤسسات او لواحد أو أكثر من فروع المشروع الذي استخدم في ارتكاب الجريمة"**.

لكن مما يجدر الاشارة اليه أن المشرع الفرنسي وفضلا عن عقوبة الغلق والمصادرة كان قد نص على غيرها من العقوبات التكميلية الوجوبية سعيا منه لتحقيق مبدأ تفريد العقوبة[2]
وذلك بموجب المادة ذاتها(232-5)[3]

وأهماها مايلي:

- الحرمان لمدة 5 سنوات أو اكثر من ممارسة وظيفة عامة، أو ممارسة نشاط مهني أو اجتماعي في المجال الذي ارتكبت فيه الجريمة.
- الاقصاء لمدة 5 سنوات أو أكثر من الصفقات العمومية
- المنع لمدة 5 سنوات أو أكثر من اصدار شيكات، ولا يمنع هذا من استرداد شيكات السحب الموجودة لدى المسحوب عليه والشيكات المعتمدة
- نشر الحكم أو تعليقه ضمن الشروط التي تنص عليها المادة (131- 35)

[1] المعدلة بموجب القانون رقم (06- 23) المؤرخ في 20 ديسمبر 2006

[2] فيما يخص العقوبات التكميلية لجرائم الاعتداء على نظم المعالجة الآلية في القانون الفرنسي نميز بين وضعين: الاول في قانون 1988 والثاني بعد تعديل 1994 فالمادة (462- 9) من قانون 1988 لم تكن تقرر الا عقوبة تكميلية واحدة هي المصادرة أما المادة (323- 5) من قانون العقوبات لسنة 1994 والمادة نفسها من قانون العقوبات لسنة 2004 فقد قدمت قائمة بالعقوبات التكميلية.

[3] Voir. Art 323- 5 du C P F

- والملاحظ أن ما قام به المشرع الفرنسي ينسجم ومبدأ تفريد العقوبة ذلك ان من شأن تنويع العقوبات التكميلية وضع خيارات عديدة امام القاضي الجزائي تمكنه من اختيار ما يتناسب منها والقضية المعروضة أمامه ولذلك فحبذا لو ينتهج نهجه المشرع الجزائري بدل من تضييق نطاقها وحصرها في المصادرة والغلق مما يمكنه على ضوئها من اصدار عقوبات تكميلية مختلفة تختلف باختلاف الوقائع الاجرامية وتنوعها وتعدد الظروف وتلونها وتفاوت مستويات السلوك الانساني وتباينها واختلاف الظروف والاحوال.

المطلب الثاني: العقوبات المقررة على الشخص المعنوي

في ظل التقدم العلمي والاقتصادي الذي نشهده الآن قد يحدث كثيرا أن يكون مرتكب الجريمة قد تصرف ليس لحسابه الخاص ولكن لحساب شركة أو مؤسسة معينة كأن يقوم ممثل هذه الشركة باستخدام الوسائل المعلوماتية المتاحة بالدخول الى نظم المعالجة المتاحة بالدخول الى نظم المعالجة الآلية التابعة لإحدى الشركات المنافسة دخولا غير مصرح به والاطلاع على ملفاتها وخططها ومنافستها في ذلك وربما يصل الامر الى التلاعب بمعلومات تلك الشركة. أو ما شابه ذلك من الافعال التي تدخل في اطار الحرب الاقتصادية والتكنولوجية التي تحدث كثيرا بين الشركات والمؤسسات الكبرى التي تعمل في مجال واحد وتحكمها قواعد المنافسة، لهذا كان من الضروري التوجه نحو فرض العقاب على الشركات التجارية والمؤسسات وغيرها من الكيانات المعنوية للحيلولة دون خلق حالة من اللاإدانة في ضورة الاعتداء على نظم المعالجة الآلية من طرف الاشخاص المعنوية ولعل السبيل الوحيد للقيام بذلك هو تقرير مبدأ المسؤولية الجزائية للشخص المعنوي في نطاق الجرائم محل الدراسة.

وهذا ما نص عليه المشرع الجزائري في المادة (394 مكرر6) كما يلي: "**يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي**".

والى جانب المشرع الجزائري نجد المشرع الفرنسي يقر بدوره مسؤولية الشخص المعنوي في مجال المعالجة الآلية للمعلومات وذلك بموجب المادة (323-6) كما يلي: **"يمكن أن يحكم على الاشخاص المعنوية بالمسؤولية الجزائية وفقا للشروط المحددة في المادة 121-2...."**[1]

وهو ما دعت اليه اتفاقية بودابست بموجب المادة 12 تحت عنوان مسؤولية الاشخاص المعنوية responsabilité des personnes morales كما يلي: **"يجي على كل طرف أن يتخذ الاجراءات التشريعية وأية اجراءات اخرى يرى أنها ضروري من اجل اعتبار الاشخاص المعنوية مسؤولة عن الجرائم المشار اليها في الاتفاقية اذا ارتكبت لمصلحتها عن طريق أي شخص طبيعي يتصرف بشكل فردي أو بوصفه عضوا في مؤسسة الشخص المعنوي"**[2]

الفرع الأول: حقيقة المسؤولية الجزائية للشخص المعنوي

اذا كان الاعتراف بوجود الأشخاص المعنوية قد اصبح أمرا مسلما به في القوانين الوضعية والتي تتجسد في مجموعة أشخاص أو اموال ترمي الى تحقيق غرض معين ويعترف لها القانون بالشخصية القانونية التي تجعلها اهلا لتحمل الالتزامات وأداء الواجبات واكتساب الحقوق، ويكون لها كيانها المستقل عن شخصية المكونين لها. وعن من قام بتخصيص الاموال فان الحال ليس كذلك فيما يخص امكانية تحميلها المسؤولية الجزائية حيث ثار خلاف فقهي كبير بشأن مدى مساءلة الاشخاص المعنوية وكانت الآراء تدور حول بين مؤيد ومعارض لذلك.

فذهب الاتجاه المعارض الى عدم إقرار المسؤولية الجزائية للشخص المعنوي على سند من القول أن الشخص المعنوي مكون خيالي لا ارادة له وبالتالي فان الاسناد المعنوي لا يمكن تصوره بالنسبة له، علاوة على ذلك أن العقوبات الجزائية وهي عقوبات اما سالبة للحرية أو مقيدة لها لا يمكن قبول توقيعها الا على الشخص الطبيعي، دون الشخص المعنوي كما أن توقيع هذه العقوبات على الشخص المعنوي من شأنه ان يصيب بالتبعية الأشخاص الطبيعيين الذين لهم صفة

[1] Art « 323 – du C P F dispose que Les personnes morales peuvent par l'artiche déclarées responsables pénalement, dans les conditions prévues l'article 121-2

1- Art 12 du C C C disbonsible en lingne à l'adresse suivante ; htt convention coe intèè_treaty en treaties html 185 htm

الاعضاء في الشخص الاعتباري وهذا لا يستقيم لأن هؤلاء الاعضاء قد لا يكون لهم باعا في المخالفة المنسوبة الى الشخص الاعتباري مما يؤدي الى الخروج على أحد المبادئ الاساسية في قانون العقوبات وهو مبدأ شخصية العقوبة الذي يقضي بالا يسأل الشخص الا عن أفعاله الذاتية دون الافعال التي يرتكبها غيره.

وعلى النقيض من ذلك نادى رأي آخر بضرورة اقرار المسؤولية اجزائية للشخص المعنوي، بسبب أن الاشخاص المعنوية لم تعد أشخاصا وهمية ولكنها أصبحت تمثل حقائق قانونية كما تتوافر لها الارادة الخاصة بها والمستقلة عن ارادة أعضائها.[1]

وهي ترجمة لإرادة جماعة متميزة عن ارادة الاعضاء المكونين له فهذه الارادة الجماعية ليست بإرادة أسطورية، بل هي ارادة حقيقية مجسدة في كل مرحلة من مراحل حياة هذا الشخص، والتي يعبر عنها كل يوم بواسطة الاجتماعات والمداولات وانتخاب الجمعية العامة لأعضائها أو مجالس ادارتها فهذه الارادة الجماعية قادرة على ارتكاب الجرائم مثلها مثل الارادة الفردية، وليس هناك ما يمنع من ابتداع عقوبات تتلاءم وطبيعة هذا الشخص وعليه فان الاستحالة المادية لتطبيق بعض العقوبات الجنائية على الشخص المعنوي مثل السجن أو الحبس هي حجة واهية وذلك أنه إذا كان لا يمكن تطبيق العقوبات السالبة للحرية على الشخص المعنوي يمكن على الاقل مادام له ذمة مالية توقيع عقوبات مالية عليه مثل الغرامة والمصادرة كما أن هناك من العقوبات ما يمكن تطويعها لتتلاءم مع ماهية هذا الشخص كالحكم عليه بعقوبة الحل – وهي ما تقابل عقوبة الاعدام- الذي يضع نهاية لوجوده القانوني، أو الحكم عليه بعقوبة المنع من ممارسة النشاط أو الغلق الى غير ذلك من العقوبات الملائمة لطبيعة هذا الشخص، واذا تعذر تطبيق بعض العقوبات المالية في بعض الاحيان والتي تتعلق بحالة عدم دفع الغرامة (حالة العسر) وهو الامر الذي يقرر معه الشرع اللجوء الى الاكراه البدني، فان فكرة تدابير الامن يمكن ان تقدم حلولا بديلة.

[1] أحمد حسام طه تمام، المرجع السابق، ص 180- 181.

فضلا عن ذلك فان احكام القضاء قد أقرت بذلك صراحة[1].

ولم يكن المشرع الجزائري بمعزل عن ذلك حيث أقر من جهته واستجابة لمتطلبات الواقع في أول خطو تشريعية له المسؤولية الجزائية للشخص المعنوي وقد كان ذلك بموجب القانون رقم (04-15) المؤرخ عام 10-11 2004 وذلك بنص عام هو نص المادة (18 مكرر) ليعزز هذه الحماية التي أقرتها أحكام هذا القانون بالقانون المعدل لقانون العقوبات رقم (23)لسنة 2006 في جوانب عدة سواء في اطار القسم العام لقانون العقوبات أو في اطار القسم الخاص لقانون العقوبات[2].

تنص المادة 51 مكرر من قانون العقوبات على انه: "**باستثناء الدولة والجماعات المحلية والاشخاص 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.**"

ويتضح من خلال هذا النص أن المشرع استثنى الاشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة في حماية المصالح العامة الجماعية والفردية، ولكونها المكلفة بملاحقة المجرمين ومعاقبتهم.

وبالرجوع لقانون العقوبات الفرنسي نجده بدوره قد أقر مسؤولية الشخص المعنوي وذلك عند تعديله لقانون العقوبات لسنة 1994 وذلك بموجب المادة (121-2) كما يلي: "**باستثناء الدولة، فان الاشخاص المعنوية تعد مسؤولة جزائيا على حسب ما هو وارد في المادة 121-4 121 -7 عن الجرائم المرتكبة لحسابها بواسطة اعضائها أو ممثليها**".

[1] فقد سجلت محكمة النقض الفرنسية في بداية الامر اعتراضها على توقيع عقوبة الغرامة على الشخص المعنوي باعتبارها من الجزاءات الجزئية لا المدنية ثم أيدت دفع للغرامات المفروضة على ممثليه بالنسبة للجرائم المادية délits matériels التي لا تتطلب اثبات الخطأ وأقرت مسؤوليته عن فعل الغير، أنظر: د. باسم شهاب المرجع السابق، ص307 كذلك: د. حسام طه تمام، المرجع السابق، ص 183.

[2] أنظر في عرض بقية الحجج بالتفصيل: بشوش عائشة، المسؤولية الجنائية للأشخاص المعنوية، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الجزائر، 2001، 2002. ص 27 وما بعدها للمزيد حول مسؤولية الشخص المعنوي أنظر: عبد الرؤوف مهدي، المسؤولية الجزائية عن الجرائم الاقتصادية، منشأة المعارف الاسكندرية، 1976.

وقد استثنى هو الآخر ولاعتبارات خاصة بعض الاشخاص المعنوية من مجال تطبيق المادة السابقة وهي الدولة والجماعات الاقليمية، مع جواز مساءلة الاخيرة عن الجرائم التي ترتكب بمناسبة تنفيذ مرفق عام يصح تفويض الغير بإرادته، ويشترط لإمكان المسؤولية وجود تفويض اتفاقي، مع ضرورة تعلق النشاط بمرفق عام.[1]

الفرع الثاني: أنواع العقوبات المطبقة على الشخص المعنوي

أسلفنا القول أن المشرع الجزائري قد أقر المسؤولية الجزائية للأشخاص المعنوية وقد عنون الباب المخصص لها ب"العقوبات المطبقة على الاشخاص المعنوية " des peines applicable aux personnes morales وقد عددت المادة 18 مكرر مجموعة من العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح كما يلي:

1- الغرامة التي تساوي مرة الى خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة

2- واحدة أو اكثر من العقوبات التكميلية الآتية:

- حل الشخص المعنوي
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات
- الاقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات
- المنع من مزاولة نشاط أو عدة انشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا لمدة لا تتجاوز خمس سنوات
- مصادرة الشيء الذي ارتكب في الجريمة أو نتج عنها
- نشر وتعليق حكم الادانة
- الوضع تحت التصرف لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى الى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

[1] Voir . Art 121 -2 du C.P.f

ومما تجدر الاشارة اليه في هذا المقام أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب، بل توقع على كل الجرائم التي يرتكبها الشخص المعنوي وان كانت الغرامة المحددة وفق المادة (394 مكرر 4) هي ذات حد واحد حيث أوجبت الأخذ بالحد الأقصى لهذه العقوبة وهو خمس سنوات فيما يتعلق بالجرائم محل الدراسة.

أما فيما يتعلق بالمشرع الفرنسي فتتمثل بعض العقوبات المقررة على الشخص المعنوي عملا بالمادة (323- 6) هي:[1]

1-الغرامة البالغة خمس اضعاف ما يفرض على الشخص الطبيعي بموجب القانون الذي يعاقب على الجريمة (المادة 131- 38)[2]

2-اذا نص القانون على جناية أو جنحة يسأل عنها الشخص المعنوي فانه يمكن أن يعاقب بعقوبة أكثر من العقوبات الواردة في المادة (131-39)ومنها: [3]

- المنع من مزاولة نشاط أو عدة انشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا ولمدة خمس سنوات أو اكثر
- الاغلاق بصفة نهائية أو لمدة خمس سنوات أو أكثر المحلات أو واحدة أو أكثر من مؤسسات المشروع التي استخدمت في ارتكاب الوقائع الاجرامية.
- الاقصاء من الصفقات العمومية بصفة نهائية أو لمدة تتجاوز خمس سنوات
- الوضع لمدة خمس سنوات أو أكثر تحت الحراسة القضائية
- مصادرة الاشياء التي استخدمت أو كان من شأنها أن تستخدم في ارتكاب الجريمة
- نشر أو تعليق حكم الادانة

3-المنع المحدد في المادة (131- 39) فقرة 2 بالنسبة للنشاط المهني الذي وقعت الجريمة بمناسبته.

[1] Voir. Art 323- 6du C P F
[2] Voir. Art 131- 38du C P F
[3] Voir. Art 131- 6du C P F

الفرع الثالث: تشديد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية:

من أهم العقوبات المطبقة على الشخص المعنوي هي عقوبة الغرامة ويقصد بها الزام المحكوم عليه بدفع مبلغ من النقود يقدره الحكم القضائي الى خزينة الدولة وبالتالي فهي تختلف عن التعويض الناشئ عن الجريمة الذي يمثل حقا للمجني عليه.

وإذا كانت الغرامة المطبقة على الشخص المعنوي تتراوح بين واحد الى خمس أضعاف الغرامة المقررة على الشخص الطبيعي كما حددت ذلك المادة 18 مكرر فان المداة 394 مكرر4 من القانون ذاته، والمتعلقة بعقوبة الشخص المعنوي عن ارتكاب جرائم الاعتداء على نظم المعالجة الألية عند وضعها تقيد سلطة القاضي في تخفيض قيمة الغرامة المقررة إذ الزمته بالحد الاقصى لهذه الغرامة وهو خمس أضعاف ما قررته للشخص الطبيعي[1]

حيث نصت كما يلي: "... بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي" أما اذا ارتكبت احدى الجرائم السابقة من شخص معنوي على احدى الجهات العامة فتتضاعف الغرامة في التشريع الجزائري مرتين، إذ تضاعف خمس مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي وثم يضاعف ذلك الى ضعفين لأن الجريمة ارتكبت ضد احدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة الى عشر 10 أضعاف عما هو مقرر على الشخص العادي

أما بخصوص المشرع الفرنسي فنجده قد ضاعف الغرامة الى خمس (5) أضعاف quintuple ما يفرض على الشخص الطبيعي وذلك بموجب الفقرة الأولى (1)من المادة (323-6) التي أحالت الى المادة (131- 38)[2]من قانون العقوبات

"La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines".

[1] محمد خليفة المرجع السابق، ص 126

[2] Voir. Art 323- 6du C P F voir aussi Art 131 -38 du C P F

طبقا لنظرية تبادل الآثار التي تؤكد تبادل جزئيات من المواد أو الأجسام التي تتلامس أو تحتك، ونظرا لأن الجريمة –الإيجابية– هي فعل يقتضي بالضرورة حركة، والحركة لا بد وأن تصاحبها ملامسة أو احتكاك فلا بد أن يتخلف عن كل جريمة آثار[1]، والآثار المتخلفة عن النشاط الجرمي تعتبر مصادر الدليل الجنائي، ولما كانت الاعتداءات التي تنال من نظم المعالجة الآلية جرائم كبقية الجرائم التقليدية والمستحدثة الأخرى، لها أركانها وعناصرها كما سبق وأن تم دراستها وتمر بذات المراحل التي تمر بها الجريمة، ولعل أبرزها مرحلة التنفيذ ومحاولة التخلص من آثارها، ولذلك تثور هنا مسألة استخلاص الدليل الذي تثبت به هذه الجرائم.

وإذا كان الاعتراف هو سيد الأدلة يليه شهادة الشهود فضلا عن القرائن والآثار الناجمة عن النشاط الإجرامي بما لها من دور في إثبات الجريمة وكشف الحقائق فيها بالنسبة لجرائم قانون الجزاء التقليدية، فإن قواعد هذا القانون تبدو قاصرة إزاء ملاحقة مرتكب الجريمة لإثبات هذا النوع من الجرائم المتطورة من حيث ارتكابها ومن حيث الاستفادة من التقنية العلمية في هذا التطور وهو ما ولد الحاجة للبحث عن وسيلة تصلح أن تتطور بتطورها وذلك لكي تقوى على إثباتها فظهر ما يسمى بـ:

[1] – طبقا لأشهر نظريات العلوم الجزائية المفيدة في إعادة تكوين عناصر الجريمة وعلاقة الجناة بالجريمة، نظرية لوكارد للتبادل التي تقول "كل شيء أو أي شخص يدخل مكانا أو مسرحا للجريمة يأخذ معه شيئا ويترك خلفه شيئا منه عند مغادرته".

« any one, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they depart », charles E.O.hara, fundamentals of criminal investigation, 3rd, ed springfield : charles tomas, 1973, p95.

محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 249.

الدليل الرقمي[1] أو الإلكتروني حسبما أطلق عليه المشرع الأوروبي أو التقني –وهو المصطلح الذي سنعتمده في دراستنا تماشيا مع تسمية جرائم تقنية المعلومات– لينظم بجدارة إلى المفاهيم التقليدية للدليل.

والدليل التقني طبيعة خاصة اكتسبها من موضوعه، فالدليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ولذلك فإن طبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها، فدليل التزوير مثلا يأتي من إثبات تغيير الحقيقة في المحررات التي يقع عليها، ودليل جريمة القتل المقصود قد يولد من فحص الأداة التي استخدمت في القتل وطلقات الذخيرة التي استعملت فيها، ويمكن تطبيق ذلك أيضا على إثبات جرائم الاعتداء على نظم المعالجة الآلية، فإثبات جريمة الدخول غير المصرح به يمكن أن تثبت بأدلة تقنية ناتجة أيضا عن الوسائل التقنية.

وهذه الذاتية أثرت بدورها على إجراءات طرق الحصول عليه بحيث لم يعد يكفي الاعتماد على الإجراءات التقليدية لجمعه كالتفتيش والضبط، إذ حتى لو تم تعديل القواعد التي تنظمها فإن ذلك يبدو غير ذي معنى إذا لم يكن مدعما بالتقنية ذاتها أي بالمعالجة الآلية للمعلومات في جمع الدليل التقني.

وهو ما أيقظ الدافع لدى المشرع الجزائري، حيث تدخل بموجب القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم (66-155) المتضمن قانون الإجراءات الجزائية فاستحدث بموجبه إجراءين هما: عملية التسرب واعتراض المراسلات وتسجيل الأصوات والتقاط الصور، كما تدخل بموجب القانون رقم (009-04) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فنظم الوضع القانوني للتفتيش في البيئة التقنية فضلا

[1]– يرجع أصل مصطلح الدليل الرقمي digital evidence إلى استخدام النظام الرقمي الثنائي (0،1) وهي الصيغة التي تسجل بها كل المعلومات أشكال وحروف ورموز وغيرها (داخل الحاسب الآلي، حيث يمثل (0) وضع الإغلاق off، والواحد (1) وضع التشغيل (on)، ويمثل الرقم صفر (0) أو الرقم واحد (1) ما يعرف بالبيت bit، ويشكل عدد 8 بت 8 bits ما يعرف بالبايت byte، أنظر: بيل جيتس، المعلوماتية بعد الانترنت: طريق المستقبل، ترجمة عبد السلام رضوان الكويت، المجلس الوطني للثقافة والفنون والآداب، 1998، ص 41-63 فما أن يتم تحويل المعلومات إلى أرقام، فإنه يصبح في الإمكان تخزينها في أجهزة الكمبيوتر كصفوف طويلة من bits، وهذا النظام هو نوع من الشفرة أو الكود، ويعتبر أبجدية الحاسبات الإلكترونية أي أساس اللغة التي بها تتم ترجمة وتخزين واستخدام المعلومات داخل الكمبيوتر، السيد عاشور، ثورة الإدارة العلمية والمعلوماتية، دار الشروق، القاهرة، 2000، ص 24.

عن الضبط، كما استحدث إجراءين تستعمل فيهما الوسائل التقنية في التحري والتحقيق هما: المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة المرور، ولكن هل بالفعل هذه القواعد وحدها كافية لتغطية الجوانب القانونية والعملية المتصلة بهذه الظاهرة أم لا بد من تكريس قواعد أخرى؟

وللإجابة على هذا الإشكال سنتطرق بالدراسة للدليل التقني بين الإشكالات الإجرائية و قبول مشروعيته ومصداقيته كمبحث أول و من ثم نتطرق في المبحث الثاني لدراسة الإتجاه نحو تكريس تنظيم الإطار التشريعي للأدلة التقنية كرهان مستقبلي.

المبحث الأول : الدليل التقني بين الإشكالات الإجرائية و قبول مشروعيته و مصداقيته

أثرت تقنية المعلومات على نوعية الجرائم المصاحبة لها ، كما أثرت على الإثبات إذ أصبحت الأدلة التقليدية غير قادرة على إثبات هذا النوع من الجرائم، حيث أصبح الجناة يستخدمون وسائل متطورة تمكنهم من إخفاء سلوكاتهم كاستخدام كلمات السر والتشفير والتلاعب ، وتخريبها و اتلافها ،وذلك بواسطة طرق إلكترونية ، في وقت قياسي قد تكون جزء من الثانية، كل ذلك في إطار بيئة غير مادية هي بيئة النظام المعلوماتي، وهو ما يضعف بكثير من قوة الأدلة التقليدية المعروفة من حيث كفايتها في إقامة بناء الإدانة في هذه الجرائم التي تتم في عالم افتراضي كاعتراف الفاعل بارتكابه للجريمة، والحصول على أدلة مادية عن طريق التفتيش، أو الحصول على أداة الجريمة ،هذا بالإضافة إلى أن إكتشاف هذا النوع من الجرائم يحتاج لطرق إلكترونية متناسبة مع طبيعة الوسيلة المتستخدة بحيث يمكنها فك رموزها وترجمتها إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة، وهو ما يعرف بالدليل التقني .

المطلب الأول: الإشكالات الإجرائية للدليل التقني

نتطرق في هذا المطلب لمفهوم الدليل التقني كفرع اول ومن ثم الى مشروعيته ومصداقيته كفرع ثاني.

الفرع الأول : مفهوم الدليل التقني

حيث يعرف الدليل التقنيي بأنه "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه"[1]، أو أنه "الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي

[1]- محمد الأمين البشري، المرجع السابق، ص 969.

لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.[1]

الملاحظ على التعريفات السابقة أن منها من اعتبر الدليل التقني كل معلومات يتم إعدادها أو تخزينها بشكل رقمي كما لو كانت محملة على وسيط معين يمكن قراءته عن طريق الآلة والتي عند تنفيذها في نظام المعلومات تؤدي إلى إنجاز وظيفة ما ، و هو بهذا يتلاقى مع البرنامج أي لا وجود لتفرقة بين الدليل التقني و البرنامج ، فبالرغم من أن كلا المكونان يتفقان في مسألة الالتصاق بتقنية المعلومات من حيث تكوينهما، فهما عبارة عن آثار معلوماتية يتركها مستخدم الانترنت، ويظهران في شكل رئيسي هو الشكل الرقمي، فالمعلومات داخل النظام المعلوماتي و مهما كان شكلها فهي تتحول إلى طبيعة رقمية، من خلال تقنية الترقيم التي تتعلق بترجمة أو تحويل أي مستند معلوماتي مؤلف من نصوص أو صور أو أصوات أو بيانات إلى نظام ثنائي في تمثيل الأعداد قوامه الرقمان الواحد و الصفر ، إلا أن الفرق بين الدليل التقني والبرنامج يكمن في الوظيفة التي يؤديها كل واحد منهما، فالأخير له دور في القيام بمختلف العمليات التي يحتويها النظام ، ذلك أنه لا يقوم بعمله إلا عن طريق مجموعة من البرامج عن طريق إعطاء أوامر بذلك، أما الدليل التقني فدوره يكمن في معرفة كيفية حدوث جرائم الاعتداء على النظام المعلوماتي، لإجل نسبتها إلى مرتكبها[2].

في حين ذهب التعريف إلى إعتبار الدليل التقني للأدلة المستخلصة من الكمبيوتر، و عليه فالمعلومات التي تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية أي التي لا زالت لم تفصل عن أجهزة الحاسب الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها... لا تصلح لأن توصف بالدليل التقني وهو قول غير دقيق في نظرنا ، هذا بالإضافة الى ان الكمبيوتر ليس وحده من يقوم بالمعالجة الآلية للمعلومات حيث أن الهواتف المحمولة و البطاقات الذكية كبطاقة الذاكرة

[1] – خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الموقع التالي:
http://kenanaonline.com/users/khaledmamdouh/posts/79345 .أطلع عليه بتاريخ 2015/02/25 على الساعة 20h25

[2] – عائشة بن قارة مصطفى، المرجع السابق، ص 31.

الخارجية تقوم بالدور ذاته و لهذا فان قصر الدليل التقني في الكمبيوتر و اجهزته يعد تعريفا يشوبه النقصان .

ولما سبق نقدم تعريفنا للدليل التقني بأنه "المعلومات المخزنة في النظام المعلوماتي بجميع مكوناته ، أو المتنقلة عبره بأي طريقة إلكترونية ، و التي من ممكن تجميعها وتحليلها باستخدام تكنولوجيا خاصة لتظهر في شكل مخرجات ورقية أو إلكترونية أو معروضة على شاشة النظام أو غيره من الأشكال، لإثبات وقوع الجريمة في إطار الإجراءات المعمول بها ".

و لما كان هذا الدليل يتكون من معطيات ومعلومات في شكل إلكتروني غير ملموس وغير محسوس متواجدة في الأجهزة و المعدات ، فهو يحتاج إلى جوانب تقنية للتعامل معه، و كدليل يحتاج إلى بيئته التقنية للبحث عنه و استخراجه ، و لذلك فهو دليل يخضع للمنطق العلمي[1]، وسنتناول اهم مميزاته وفق ما يلي :

– يمتاز الدليل التقني بالسعة التخزينية العالية:

يمكن تخزين آلاف الصور، مجموعةكتب ، منشورات ، محادثات....إلخ.[2]

– سهولة التلاعب بالدليل التقني:

بالتعديل أو الإتلاف أو وضع المعلومات في ملفات رقمية أخرى بسرعة قصوى .

– الدليل التقني يرصد و يحلل معلومات عن الجاني :

من خلال تسجيل تحركات الفرد، عاداته ،سلوكاته ، الأمور الشخصية الخاصة، لذا فهو أيسر من الدليل المادي من حيث إستخدامه في مجال البحث الجنائي.

– الدليل التقني مستوحى من بيئته التقنية:

الدليل التقني مستنبط من بيئته الإفتراضية المتكونة من أجهزة الحاسوب والخوادم والمضيفات والشبكات ويتم تداوله عبرها.

[1]– عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 977.

[2]– ممدوح عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في: 10-12 مايو 2003، ص 2241.

– قابليته للنسخ:

حيث يستخرج منها نسخ مطابقة للأصل، التي لها نفس القيمة العلمية، مما يشكل ضمانة فعالة للحفاظ عليه وحمايته من الفقدان والتغيير عن طريق نسخ طبق الأصل منه.[1]

– صعوبة التخلص منه:

على عكس الأدلة التقليدية[2] التي يمكن بسهولة التخلص منها ، من الأوراق والأشرطة المسجلة التي تحتوي على إقرارا بارتكاب شخص للجرائم وذلك بتمزيقها وحرقها، أو مسح بصمات الأصابع من موضعها، أو بقتل الشهود أو تهديدهم بعدم الإدلاء بالشهادة...الخ .

و بالنسبة للأدلة التقنية فإن الحال غير ذلك ، حيث يمكن استرجاعها بعد محوها ، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منها، لأن هناك العديد من البرمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها مثل foremost، recoverjpeg، وphotorec المستخدمة باسترجاع الصور والملفات المحذوفة من الهارد وذواكرUSB[3] .

ولا مشكلة تثار فيما إذا تم ذلك الإلغاء بالأمر[4] delete أو عن طريق إعادة تهيئة أو تشكيل القرص الصلب hard disk باستخدام الأمر format وسواء كانت هذه المعلومات صورا أو رسومات أو كتابات أو غيرها، كل ذلك يشكل صعوبة إخفاء الجاني لجريمته طالما علم رجال البحث والتحقيق بوقوع الجريمة، بل أن نشاط الجاني لمحو الدليل (فعل الجاني لمحو الدليل)

[1]– عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الانترنت، ندوة الدليل الرقمي بمقر جامعة الدول العربية بجمهورية مصر العربية، في الفترة من 5-8 مارس 2006، ص 17.

[2]– يتشابه كل من الدليل التقني والدليل الجيني أو ما يطلق عليه DNA وبالعربية الحمض النووي، وذلك لاتحاد كليهما في هذه الخصيصة وهي صعوبة التخلص منهما من ناحية، ومن ناحية أخرى يمكن إحداث تعديل في تكوينهما معا.

[3]– للمزيد من التفاصيل حول هذه البرامج أنظر الموقع التالي:

[2]– http://www.isecur1ty.org/articles/digital-forensics/221-photorec-recoverjpeg-foremost.html USA, v, EDWARD m. stulock, app. 8th cir.no.02- 1401OCTOBER 25, 2002.

مشار إليه لدى: عمر محمد بن يونس، أشهر المبادئ المتعلقة بالانترنت في القضاء الأمريكي، الطبعة الأولى، دار أكاكوس، 2004، ص 817.

يشكل دليلا، فنسخة من هذا الفعل يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا كدليل إدانة ضده.[1]

– **الطبيعة ديناميكية للدليل التقني** : فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان.

– **عالمية مسرح الدليل التقني**: يمكن لمستغلي الدليل من تبادل المعرفة الرقمية بمناطق مختلفة من العالم، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبيا.

– **تطور الدليل التقني بطبيعته**: التي لا تتصف بالجمود بالتبعية للتطور المتواصل في البيئة التقنية.

– **الطبيعة الرقمية الثنائية (1–0) للدليل التقني**:

ليس للدليل التقني هيئة واحدة، وإنما له خصيصة الالتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه، إذ يتكون من تعداد غير محدود لأرقام ثنائية موحدة في الصفر و الواحد (1–0)، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكتابة مثلا في العالم الرقمي ليس لها الوجود المادي الذي نعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء في العالم الرقمي يتكون من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة[2]، وأما تكوين معطياته فإنها تختلف من حيث الحجم والموضوع، إذ كمية الـ (1–0) في ملف يمكن أن تختلف عن الحجم في ملفات أخرى.

الفرع الثاني: معوقات الدليل التقني.

تعد المشكلات المثارة أثناء تطبيق قاعدة الدليل التقني في البيئة الافتراضية و التي حتى ولو إذا ما تدخل المشرع كما هو حال المشرع الجزائري الذي عدل أحكام تشريعه الإجرائي بل واستحدث البعض الآخر فإن ذلك لا يقدم حلا متكاملا للمعضلة العملية ما لم يقابل ذلك

[1]– ممدوح عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، المرجع السابق، ص 2240.

[2]– عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 971.

بحلول أخرى تعمل على القضاء أو التقليل من الصعوبات التي تواجهها أثناء مباشرتها[1] ، وهو أمر غاية في الاهمية لمواجهة هذا النوع المستحدث من الجرائم وذلك لكي نمنع ما يمكن أن يقال من ان صعوبة إثبات واكتشاف هذه الجرائم و التي نوجزها في النقاط التالية:

أولا: المعوقات الخاصة بطبيعة تكوين الدليل التقني

و يقصد بها المشاكل الداخلية فيه والمتعلقة به تحديدا، وذلك بسبب الطبيعة النابعة من تكنولوجيا المعلومات التي يتكون منها هذا الدليل ، و التي تعود على إجراءات الحصول عليه فتضعف من قيمتها إن لم يتم إيجاد حلول بشأنها، و سنفصل فيها كما يلي :

أ: طبيعته غير المرئية و المختلطة :

الشكل المجالي أو النبضاتي المغناطسي أو الكهربائي للمعلومات الرقمية تفقد الرجل العادي إدراكها بالحواس الطبيعية، فهي متواجدة في عالم افتراضي مبني على جانب معنوي غير ملموس في مكون رقمي مختلط، نتيجته عدم إمكانية وجود فرز، ذاتي في إطار التخزين الرقمي، فمسألة اختلاط الملف المجرم موضوع الدليل الجنائي الرقمي بالملف البريء أمر وارد في البيئة

[1]– التحديات التي تعترض الدليل الرقمي تم التطرق لها في المؤتمرات الدولية، ولعل أهمها مؤتمر الإنتربول السادس لجرائم تقنية المعلومات الذي شهدته القاهرة في الفترة ما بين 13 إلى 15/ 4 / 2005 حيث تم تناول هذه التحديات من خلال الورقة التي قدمها وفد مصر ومدير إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، فيتمثل**التحدي الأول**: ويتمثل في انتشار مقاهي الانترنيت التي يستطيع أي فرد من خلالها أن يتعامل مع شبكة الشبكات، بما فيه المجرم الذي يستخدمها لارتكاب جرائمه، وهو ما يؤدي إلى صعوبة التوصل لمرتكبها، نظرا إلى إمكانية تنتقل المجرم بين أكثر من مقهى خلال اليوم الواحد مما يؤدي إلى صعوبة التوصل بصورة دورية لأدلة الإثبات لقيام تلك المقاهي بإعادة تشكيل الأجهزة، أما **التحدي الثاني** فيتمثل في تكنولوجيا A.D.S.L أو ما يعرف باسم " الانترنيت فائق السرعة" والذي لم يسلم هو الأخر من يد المجرمين، إذا استخدموه لتنفيذ مخططاتهم الإجرامية وذلك عن طريق اشتراكهم إلى جانب أشخاص آخرين في جهاز واحد عن طريق موزع خطوط، مما يؤدي إلى صعوبة التوصل إليهم، أما **التحدي الثالث** فيرجع إلى ظهور الانترنيت اللاسلكي، والذي سهل لهم الانتقال إلى عدة أمكنة في اليوم الواحد[1]، أما فيما يخص **التحدي الرابع** عمليات التخفي PROXY أثناء التجوال عبر الشبكة التي تؤمنها بعض المواقع، التي استغلت من طرف القراصنة بل أن مصممي الفيروسات المدمرة من خلال تلك المواقع قاموا بإطلاق فيروساتهم المدمرة عبر العالم الأمر الذي بات يشكل ظاهرة خطيرة، ولذلك فإننا نقترح إلزام مسؤولي المواقع التي تستخدم البر وكسيات بالاحتفاظ بالمعطيات الأساسية والحقيقية لمستخدمي مواقعهم على الشبكة.

التخزينية في العالم الرقمي[1]، فعلى سبيل المثال ملفات الولوج LOG FILLE تبدو مشابهة للملفات العادية، وممكن جمعها مثل أي ملف آخر وهي تحتوي على كمية هائلة من المعلومات التي قد تفيد البحث والتحقيق الجنائي، إلا أن الصعوبة في جمع هذه المعلومات الجنائية أنها عادة ما تكون مختلطة بغيرها من معلومات مستخدمي الكمبيوتر الابرياء، مما قد يشكل تهديدا لخصوصية هؤلاء[2].

وبالتالي يختلف الدليل التقني عن الأثار المادية الناتجة عن الجرائم التقليدية، فلا تنتج التقنية الشعر والدماء وبصمات الأصابع وآثار الأقدام وما إلى ذلك وإنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة الي تشكل نظام المعالجة الآلية على أية شاكلة يكون عليها لا تفصح عن شخصية معينة، فضلا عن ذلك غالبا ما يكون الدليل التقني مرمرا أو مشفرا مع وضع عناوين مضللة لها وتخزينها في شكل ملفات غير تقليدية.

فلا مرية أن المجرمين الذين يرتكبون جرائم الاعتداء على نظم المعالجة الآلية من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب، فهم قد يزيدون من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التي قد تدينهم بترميز أو تشفير المعلومات المخزنة إلكترونيا أو المنقولة عبر الشبكات الاتصال، بحيث قيد يستحيل على غيرهم الاطلاع عليها وبذلك يشكل هذا الدليل عائقا أمام سلطات البحث والتحقيق أثناء تطبيقها للقواعد الإجرائية المقررة لاستخلاصه.

ب: ديناميكية الدليل التقني:

فالأدلة التقنية أدلة ليست أقل من مادية من الأدلة المادية فحسب بل تصل إلى درجة التخيلية في حجمها وشكلها ومكان تواجدها غير المعلن فيهي ذات طبيعة ديناميكية فائقة السرعة إذا تتنقل عبر شبكات الاتصال بسرعة فائقة، بمعنى إمكانية تخزين المعلومات le stockage des

[1] – عمر بن يونس، الإجراءات الجنائية عبر الانترنيت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصلا إلى الدليل الإلكتروني في التحقيقات الجنائية، المرجع السابق، ص 24.

[2] ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP/IP) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق، ص 19.

données في الخارج – على خادم server – بواسطة شبكة الاتصال عن بعد وهو ما قد يثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط الأدلة التقنية والبحث عنها، لأنه يستلزم القيام بها خارج حدود الدولة في نطاق دولة أخرى حيث ارتكبت الجريمة أو جزء منها[1]، وهذا كله يصطدم بمشاكل الحدود والولايات القضائية، لما ينطوي عليه من مساس بسيادة هذه الدولة، وهذه المشكلة تظهر بصورة جلية حين اتخاذ اجراءات التفتيش لضبط هذه الجرائم عندما يكون نظام المعالجة الآلية متصلا ينظم أخرى خارج الدولة، ويكون تفتيش هذه النظم ضروريا لإماطة اللثام عما تشمله من جرائم.

وهو ما يفرض الحاجة إلى الحصول على إذن الدولة التي يتم إجراء البحث في مجالها الإقليمي أو إبرام اتفاقية ومعاهدات دولية ثنائية أو متعددة الأطراف في مجال التعاون الدولي[2] التي تستهدف من وزراء ذلك التقريب بين القوانين الجزائية الوطنية من أجل جمع هذا النوع من الأدلة العابرة للحدود.

وتعد معاهدة المجلس الأوروبي حول جرائم تقنية المعلومات الموقعة في 2001/11/23، والتي أيدتها الولايات المتحدة بقوة هي أول خطوة رئيسية في هذا الاتجاه ويمكن اعتبارها بداية لعمل وضع القواعد والمعاير التي يتوقع من البلدان المعنية أن تتبعها في نهاية الأمر في جهودها.

خصصت اتفاقية بودابيست الباب الثالث منها لدراسة التعاون الدولي coopération internationale ومن خلال نصت المادة (23) على ضرورة تعاون الأطراف فيما بينها وفق لأحكام هذا الفصل، ومن خلال تطبيق الوسائل الدولية الملائمة بنسبة لتعاون الدولي في المسائل الجزائرية والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بنسبة لقوانين المحلية، إلى أقصى مدى ممكن، بغرض التحقيقات والإجراءات الجزائية المتعلقة بالجرائم ذات الصلة بالنظم الحاسوبية، والبيانات المعلوماتية، أو لجمع الأدلة ذات الشكل الإلكتروني لمثل هذه الجرائم".

[1] Dans ce sens. Voir ;Fiche de l AWT. La criminalité informatique. Disponible en ligne à l adresse suivante ; http;//www.awt.be/contenu/tel/sec/sec,fr,fic,140.000.pdf.

[2] Emmanuelle L'amandé – Maga Secours , législations et dispositifs de lutte contre la cybercriminalité ; un besoin d'harmonisation internationale, disponible en ligne à l'adresse suivante ;http ;// www.mag – secours com / spip. php ? article 7842.

وفي هذا الصدد نجد أن المشرع الجزائري قد خصص الفصل السادس من القانون رقم (09-04) لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها " للتعاون والمساعدة القضائية الدولية " وما يستنتج ذلك من ضرورة أن تطلب الجزائر الدعم من الدول التي سبقتنا في هذا المجال على غرار اتفاق التعاون الذي وقعته الجزائر بتاريخ 25 أكتوبر 2003 مع فرنسا لمحاربة الإجراء المنظم وبالخصوص الإجرام التقني والمتضمن التعاون الأمني والدعم التقني للشرطة الجزائرية لمحاربة المجرمين الإلكترونيين إذا يجب إذا اقتضت الضرورة وضع قانون يسهل هذا التعاون بين الجزائر والدول الأخرى[1].

ج: إمكانية تعديل أو محو الدليل التقني :

تتم جرائم الاعتداء على نظم المعالجة الألية في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت ويطلق عليها " البيئة التقنية " هذه الأخيرة تعكس على طبيعة الدليل الذي تتجه مما تجعله غير مرئي، وهو ما يجعل أمر طمسه ومحوه كليا من قبل الفاعل أمرا في غاية السهولة وفي زمن قصيرا جدا. وهكذا على سبيل المثال فإن المستخدم الذي يحكم في المعلومات يمكن أن يستعمل نظاما معلوماتيا من اجل محو تلك المعلومات التي تعد موضوعا للتنقيب الجنائي، وبالتالي تدمير كل الأدلة.

وعلى ذلك نرى أنه يمكن الحفاظ على الأدلة ومن ثم ضمان أن الإجراءات التقليدية لجمع الدليل التقني كالتفتيش والضبط لا تزال فعالة في بيئة تكنولوجية تتميز بالتلاشي أو التبخير – وذلك فظلا عن البرمجيات التي يمكن بمقتضاها استرداد كافة الملفات التي تم إلغائها أو إزالتها- إتباع نظام إلزام مزودي الخدمات بالتحفظ على المعطيات المخزنة لديهم حيث أنه إذا لم تتوافر الأدلة على الاتصال وعن عناوين الأشخاص المشتركين في الجريمة فإنها تكون عرضة للاختفاء وهذا ما نصت عليه اتفاقية بودابيست في المادة 16 من ضرورة السماح لكل طرف لسلطاته المختصة

[1] ج-ر-م، الفترة التشريعية السادسة، الدورة العادية الرابعة، الجلسة العلنية المنعقدة يوم السبت 27 يوليو 2009، السنة الثالثة، رقم 122، ص19.

أن تأمر أو تفرض بطريقة أخرى مزود الخدمة التحفظ على المعطيات المعلوماتية المخزنة بما في ذلك المعطيات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي.

وحتى تستوضح الصورة لنا عن هذا الإجراء نعطي المثال عليه: قد يعلم رجال الضبط القضائي بوجود فيروسات في اليوم الأول فيقومون باتخاذ إجراءات الحصول على إذن التفتيش في اليوم التالي، وفي اليوم الثالث يحصلون على الإذن ثم يصل عملهم أن المزود قام بشطب السجلات كالمعتاد في اليوم الثالث المذكور.

إذا التحفظ على المعطيات يعتبر إجراء أولي أو تمهيدي الهدف منه هو الاحتفاظ بالمعطيات قبل فقدانها، وهي المبررات التي حددتها المذكرة التفسيرية لاتفاقية بودابيست والتي تدعو إلى اتخاذ مثل هذا الإجراء وذلك كما يلي:

1- قابلية المعطيات المعلوماتية للتلاشي، حيث تكون محلا للمحو أو التغيير سواء كان ذلك بدافع إجرامي – بهدف طمس معالم الجريمة أو أي عنصر إثباتي لشخصية المجرم – أو بدافع غير إجرامي وذلك في إطار الحذف الروتيني للمعطيات التي لم تعد الحاجة إليها.

2- غالبا ما يتم ارتكاب جرائم الاعتداء على نظم المعالجة الآلية عن طريق نقل الاتصالات عبر نظم الحاسوب، حيث يمكن أن تتضمن هذه الاتصالات محتويات غير مشروعة مثل الفيروسات، فتحديد مصدر هذه الاتصالات يمكن أن تساعد في تحديد هوية مرتكبي الجريمة.

3- تأمين الدليل التقني من الصياغ، حيث يتم نسخ دليل على نشاط جنائي من قبل مزودي الخدمات، مثل المراسلة الإلكترونية التي تم إرسالها أو استقبالها، ومن تم يمكن الكسف عن دليل جنائي للجرائم المرتكبة.

كما نصت عليه التشريعات الأجنبية كالتشريع الأمريكي، إذا نص على هذا الإجراء في القسم (f) 2703 U.S.C 18 من قانون خصوصية الاتصالات الإلكترونية الأمريكي ECPA[1].

[1] "A gent may direct providers to preserve existing record pending the issuance of however, compulsory legal process. Such requests have no prospective effect " .

يلاحظ مما سبق أن إجراء التحفيظ على المعطيات المخزنة يعد لبعض الدول العربية- كسوريا- سلطة قانونية جديدة فهو أداة تحقيق مستحدثة في إطار مكافحة جرائم تقنية المعلومات، في حين نجد المشرع الجزائري قد نص في القانون رقم (09- 04) لسنة 2009 بشان الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على إجراء الحفظ وذلك في المادة (10) منه.

وباستقرائنا لنص المادة السابقة الذكر نلاحظ أنها بالرغم من أهميتها خاصة إذا تعلق الأمر بتتبع مصدر أو مكان وصول الاتصالات الإلكترونية وبالتالي تحديد هوية الجناة، إلا أن نطاق تطبيق هذه المادة لا يمتد إلى التحفظ على المعطيات، وعليه إذا كان الامر متعلقا بحفظ معطيات سبق وجودها وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها فإن السعي لدى مزود الخدمة بقصد التحفظ عليها فإن الخدمة إلى غطاء من المشروعية يبرر له قيامه بذلك، وعلى ذلك نرى أنه يتعين على المشرع الجزائري أن يتدخل لسن قاعدة قانونية إجرائية ينظم فيها الوضع القانوني للتحفظ على المعطيات المخزنة تحت السيطرة مزود الخدمات وذلك على نحو ما فعلت اتفاقية بودابيست .

ثانيا : المعوقات الخاصة بالعامل البشري

ويتعدد هذا النوع من المعوقات على النحو التالي:

أ: نقص المعرفة التقنية لدى رجال القانون:

لا شك في أن أجهزة العدالة على رأسها الشرطة تلعب دورا رئيسيا إن لم نقل يتوقف عليها أمر تطبيق القانون بصورة كلية.

وإذا كانت لهذه الأجهزة بما لها من خلفية قانونية أهمية كبيرة في التحري عن الجرائم وتحقيقها والبحث عن مرتكبيها في إطار الجرائم التقليدية إلا أن وظيفتها في مكافحة جرائم الاعتداء على نظم المعالجة الآلية لا ترقى إلى نفس الدرجة من الأهمية، ذلك أن الطبيعة الخاصة للبيئة التي تتعامل معها فضلا عن ذاتية الدليل التقني الذي يعيش فيها انعكس على عمل الجهات

المكلفة بالبحث والتحري، حيث يتطلب الكشف عن هذه الجرائم إتباع استراتيجيات خاصة تتعلق باكتسابهم مهارات خاصة على نحو يساعدهم على مواجهة التقنيات المعلوماتية وهو ما تفتقر إليه الجهات المكلفة بالتحري والتحقيق في العالم المادي.

فإذا أضفنا إلى نقطة الدراية الرقمية مسألة التعامل مع الأدلة التقنية وهي التي تشكل عقبة كبيرة أمام سلطات التحقيق، فإننا نكون أمام معضلة أكبر من مجرد الحصول على الدليل التقني، إذا أخذنا في الاعتبار أن مكمن الدليل التقني غالبا هو الحاسوب والخوادم والمضيفات والشبكات ولعل المثال التقليدي التوظيفي الملائم دائما هو قيام رجل الشرطة بوضع حقيبة كاملة تحتوي على اسطوانات الكمبيوتر المصادرة وذلك في صندوق السيارة بالقرب من جهاز الإرسال والاستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية قد تسببت في تدميرها جميعا[1].

لذلك كان من الضروري إعداد إدارة خاصة لمواجهة هذا الاعتداء التقني تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها تتلقى البلاغات وتلاحق مجرمي التقنية وتبحث عن الأدلة ضدهم وتقدمهم للمحاكمة، وذلك كله ضمانا للنوعية لمواجهة التحديات الأمنية الناتجة عن هذا الإجرام. سيما وأن متطلبات العدالة تقتضي أن تتحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه اكتشاف كافة جرائم تقنية المعلومات، وهذا ما دعت إليه الاتفاقية الأوروبية لجرائم تقنية المعلومات[2]، وكذلك المؤتمر المنعقد في السوربون بباريس 2005/1/19 والذي كان موضوعه الشرطة والانترنيت، وكذا المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة في الفترة ما بين 13 إلى 2005/4/15.

[1] عبد الله حسين علي محمود، المرجع السابق، الهامش رقم(1)، ص 355.

[2] جاء في المذكورة التفسيرية لاتفاقية بودابيست بيانا لضرورة إنشاء وحدات خاصة كما يلي: "كل طرف في الاتفاقية تكون ملزمة بتبني الإجراءات التشريعية وأية إجراءات أخرى ترى أنها ضرورية وفق قانونها الداخلي والأطر القانونية من اجل إنشاء وتأسيس سلطات .... مقررة داخل القسم الحالي بغرض التنقيبات أو الإجراءات الجنائية النوعية.

وهو ما حدث فعلا، حيث بادرت مختلف الدول سواء الأجنبية أو العربية بإنشاء وحدات متخصصة لمكافحة الإجرام التقني بصفة عامة[1].

[1] لم يتوقف الأمر على المستوى الوطني فحسب فالبعد الدولي لهذه الجرائم باعتبارها من الجرائم العبرة للحدود، بما يمكن أن تتعدى آثارها عدة دول، مما يستحيل على الدولة القضاء عليها بمفردها لذلك فإن الحاجة تدعو إلى ضرورة التعاون فيما بينها باعتبارها إحدى الضرورات اللازمة لمواجهة هذه الأنشطة الإجرامية المستحدثة، ويعد التعاون الشرطي الدولي " la coopération policière internationale" من أهم صور التعاون الدولي في مكافحة الإجرام بصفة عامة والإجرام العابر للحدود لاسيما إجرام تقنية المعلومات بصفة خاصة، ويتحقق هذا التعاون من خلال عدة أجهزة من أهمها: المنظمة الدولية للشرطة الجنائية، وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين اجهزة الشرطة في الدول الأطراف على نحو فعال في مكافحة الجريمة، وذلك عن طريق تجميع المعلومات المتعلقة بالمجرم والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة إليها، وتبادل هذه المعلومات فيما بينها.

وهذا وقد أكد سكرتير الانتربول الدولي « Raymond Kendall » في مؤتمر جرائم الانترنيت المنعقد في لندن في 2000/10/9 على ضرورة تعاون الدول في مكافحة جرائم التقنية المعلومات بصفة عامة باعتبار هذه الأخيرة تبرز كظاهرة دولية، وقد أكد على أنه يجب على المجتمع الدولي عدم الانتظار إلى حين عقد معاهدات واتفاقيات في هذا الإطار بل يجب الشروع ويشكل فوري في مكافحة هذه الجرائم ويقوم الانتربول بوضع استراتيجية جديد لمواجهة جرائم الاعتداء على نظم المعالجة الآلية بالتعاون مع الأمم المتحدة.

وتجدر الإشارة إلى أنه يوجد منظمات أخرى لها دور لا يقل عن دور الإنتربول في مواجهة هذا النوع المستحدث من الإجرام عل المستوى الدولي ونخص بالذكر منظمة التعاون الاقتصادي والتنمية oecd ومجموعة الثمانية الاقتصادين G-8 GOUPE OF EIGHT حيث قامت بإعداد ملتقى دولي في نهاية نوفمبر 2000 في طوكيو لتكوين قوة دولية أطلق عليها digital opprtunity task force تتمثل مهامها في تحقيق أمن تكنولوجيا المعلومات.

وعلى غرار هذه المنظمة أنشا المجلس الأوروبي في لوكسمبورغ في عام 1991 شرطة أوروبية " الإنتربول " والتي تتخذ من لاهاي – هولندا –مقرأ لها، لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة وملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال جرائم الاعتداء على نظم المعالجة الآلية.

في 28 / 2/ 2002 تم إنشاء " الأور جست " من قبل مجلي الاتحاد الأوروبي كجهاز يساعد على التعاون القضائي والشرطي في مواجهة الجرائم الخطيرة، حيث يعد دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية، خصوصا فيما يتعلق بالأنشطة المرتبطة بجرائم الاعتداء على نظم المعالجة الآلية. إلى جانب الانتربول والا ورجست تم انشاء فضاء جماعي من غير حدود سمي بشجن وذلك من خلال التوقيع على معاهدة في 1986/6/14 وعلى اتفاقية تطبيق تلك المعاهدة في 1990/6/19 وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الاوربي لمواجهة التحديات المنية التي تفرضها الظروف الجديدة، منها جرائم الاعتداء على نظم المعالجة الآلية وتتمثل هاتين الوسيلتين في مراقبة المشتبه فيهم عبر الحدود وملاحقة المجرمين.

فضلا عن ذلك قام مركز التدريب الوطني عن الجرائم التقنية " nslec "وهو أحد المؤسسات التابعة للاتحاد الاوربي بإعداد المشروعات والبرامج التي تهدف الى مكافحة الجرائم عالية التقنية، ومن اهم هذه المشروعات مشروع فالكون 2001، وأيضا برنامج اجيس 2004/2003 اللذان يهدفان الى التدرب على مكافحة جرائم الاعتداء على نظم المعالجة الآلية . اما على المستوى العربي نجد أن مجلس وزراء الداخلية العرب انشا المكتب العربي للشرطة الجنائية مجاله مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والانظمة المعمول بها في كل دولة للمزيد من التفاصيل انظر على التوالي :

عمر محمد ابو بكر بن يونس ، الجرائم الناشئة عن استخدام الانترنيت، المرجع السابق .ص814.

Nadine adine L. C thwaites; Eurojust. autre brique dans l édifice de 1 coopération judiciaire en matière pénale ou solide mortier?.R.s.c.c ;n1. Janvier-mars 2003.p45.

L harmonisation des moyens de lutte contre la cybercriminalité. Revue de web réalise le 22/4/2004. Disponible en lingne à l adresse suivante :htt://www.finances-gouv.fr.

عفيفي كامل عفيفي، المواجهة الشرطية لجرائم الكمبيوتر والانترنيت، منشور على الموقع التالي:

http; // www. Wamadani. Com /vb/ showthread. Php?t= 26760.

ولعل النموذج المعتاد والأكثر شهرة هو " الإدارة المخصصة لمتابعة جرائم تقنية المعلومات بمكتب التحقيقات الفدرالي FBI [1] في الولايات المتحدة الأمريكية والتي نالت الاعتراف بها كواحدة من أنجح هيئات مكافحة الإجرام التقني، وإلى جانبها نجد إسبانيا التي أنشأت " وحدة التحريات المركزية المعنية بمعلومات جرائم تقنية المعلومات " بصفة عامة وجرائم الاعتداء على النظم بصفة خاصة التي تعمل مع الإدارة المركزية في وزارة الداخلية الاسبانية على مراقبة مرتكبي تلك الجريمة المستحدثة والعمل على إحباط مخططهما الاجرامي، كما نجد أيضا فرنسا إذ لم تسلم هي الأخرى من مخاطر هذا الإجرام ونتيجة لذلك قرر وزير الداخلية الفرنسي السابق Dominique de Villepin بعد اطلاعه على التقرير المقدم له من قبل وزير المالية والاقتصادThierry Breton والذي أكد فيه تضاعف كم جرائم تقنية المعلومات بمختلف أشكالها[2]، على ضرورة اتباع مخطط محكم لتحقيق الأمن المعلوماتي، ويتضمن هذا المخطط ما يلي:

– دعم قوات الشرطة والدرك المتخصصين في هذه المكافحة، وذلك عن طريق زيادة عددهم.

Le doublement du nombre des enquêteurs spécialise.

– تكوين شبكة خبراء من الشرطة والدرك.

Réseau d’experts police-gendarme

والى جانب الاقتراحات لسابقة، يضيف الوزير السابق ضرورة تطوير التعاون مع مراكز البحوث المتواجدة في الجامعات والمؤسسات الكبيرة بغرض تسهيل مسايرهم للتطورات

[1] والذي يضم بداخله مجموعة اشخاص مدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتم تحصيله من أداة.

[2] كلف وزير الداخلية الفرنسي السابق Dominique de Villepin وزير الاقتصاد والمالية Thierry breton في يوليو2004، بتقديم تقرير حول نوعية جرائم تقنية المعلومات الكثر انتشارا في الوسط الفرنسي، واعطاء نسبة المتضررين منها إضافة الى الاقتراحات اللازمة والمناسبة لمكافحة ذلك الاجرام، ولقد حددت نسبة ذلك الاجرام بحوالي 600000 جريمة سنة 2004 حسب الاحصائيات المقدمة من المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات، ومعظم تلك الجرائم تتعلق بالقرصنة المعلوماتية(الدخول غير المصرح به)،انظر:

Rapp. Présenté par Thierry breton et remis à monsieur le ministre de l intérieure et de des libertés locales ;Chantier sur la lutte contre la cybercriminalité ,25/02/2005 , disponible en ligne à l’adresse suivante : http : //www.lesechos.fr

-la gendarmerie et la lutte contre la cybercriminalité .disponible en ligne à l adresse suivante http://www.libertysecurity.org/article226.html.

التكنولوجية، أضف الى ذلك ضرورة وضع شهادة مواطن[1] مسندة الى مزودي الخدمات أو الدخول الى الأنترنيت.

كما قامت فرنسا وسعيا الى مكافحتها هذا الاجرام المستحدث بجميع صوره بإنشاء عدة وحدات ومراكز متخصصة وغير متخصصة ضمن الشرطة والدرك لمكافحة هذا الاجرام، وهذا ما اشارت اليه الاتفاقية الاوربية لمكافحة جرائم تقنية المعلومات والتي وقعت وانضمت اليها فرنسا وصادقت على سريانها على ارضها، ومن ذلك المكتب المركزي لمكافحة الاجرام المرتبط بتكنولوجيا المعلومات والاتصالات المعروف اختصارا ب: (OCLCTIC)[2]، قسم الانترنيت التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف اختصارا ب: (STRJD)، القسم المعلوماتي الالكتروني التابع لمعهد البحوث الجزائية للدرك الوطني المعروف اختصارا ب: (IRCGN)، وحدات أقسام الاستعلامات والتحقيقات القضائية المعروفة اختصارا ب: (BDRIJ)[3].

---

[1] شهادة مواطن: وضعت هذه الشهادة من أجل معرفة الجهود المبذولة من قبل مزودي الخدمات والدخول إلى الإنترنت لمكافحة الإجرام عبر تلك الشبكة لمزيد من التفاصيل أنظر:

Rapp. Présenté par Thierry , diponible en ligne à l' adresse précédent.

[2] يعتبر هذا المكتب سلاح الدولة الفرنسية في مكافحة جرائم تقنية المعلومات بصفة عامة بما فيها جرائم الاعتداء على نظم المعالجة الآلية، إلى جانب وحدات أخرى، ولقد تم إنشاءه بموجب مرسوم وزاري رقم (2000- 405) المؤرخ في 15- 5 – 2000 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية.

Décri. n° 2000 – 405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

وتجدر الاشارة في هذا المقام أن المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال يمثل لفرنسا نقطة الاتصال le point de contact international dans le domaine de la cyber- criminalité المركزية التبادلية الدولية، فهو من جهة يشارك على المستوى الوطني، في تحريك وتنسيق الأعمال التحضيرية اللازمة ومن جهة أخرى، فهو يشارك في نشاطات المنظمات الدولية، كما أنه يحافظ على الروابط العلمية بين المصالح المختصة في البلدان الأخرى ومع المنظمات الدولية (ومن بين تلك المنظمات الدولية التي تسهر على مكافحة جرائم تقنية المعلومات بصفة عامة والجرائم التي تستهدف نظم المعالجة الآلية بصفة خاصة: مجموعة الثمانية G8 و أربول Europol والانتربول Interpol والجنة الأوروبية commotion European)، وذلك مع مراعات الاتفاقية الدولية – في بحثها – على المعلومات المرتبطة بتلك الجرائم المميزة وكذا المتعلقة بالتعرف وتحديد مرتكبيها، أنظر المادة (7) من نفس المرسوم، وأنظر كذلك:

la police nationale ; la lutte contre la cybercriminalité et les fraudes aux cartes bancaires, disponible en ligné à l' adresse suivante ; http //www. intérieur. goun. Fr.

[3] للمزيد من التفاصيل حول هذه الأقسام، مهامها، أنظر ما يلي:

- Rapp. présenté par Thierry Bereton .disponible en ligne à l'adresse précédente.
- La gendarmerie et la lutte contre la cybercriminalité disponible en ligne à l'adresse suivante http ; //www. libertysecurity.org/ artichl 226. html

وهذا ما قامت به مصر أيضا حيث أنشأت إدارة مكافحة جرائم الحاسبات وشيكات المعلومات وذلك بموجب القرار رقم 13507 الصادر عن وزرارة الداخلية المصرية[1] أيضا الأردن التي نشأت مديرية الأمن العام قسم خاص يعني بجرائم تقنية المعلومات بصفة عامة ويتولى إجراءات المكافحة والاستدلال والتحقيق في الجرائم التي ترتكب بواسطة النظم هدفا أو بيئة لها وذلك عام 1998[2] أما والحال بالجزائر فقد تم إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته تتولى تنشيط وتنسيق عملية الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم[3]، ونذكر على سبيل المثال الدرك الوطني الذي كان السباق في إنشاء مركز لمكافحة جرائم تقنية المعلومات ببئر مراد رايس، وأوضح العقيد بالدرك الوطني – معمري – أن هذا المركز الذي سيباشر عمله بعد أشهر قليلة يعنى بتطوير أساليب التعامل مع هذا النوع من الجرائم[4].

[1] وهذه الإدارة جديدة في تكوينها ونوعيتها تختص بمكافحة مثل تلك الجرائم، وهي في الأصل تابعة للإدارة العامة للمعلومات والتوثيق، وتخضع للإشراف المباشر لمدير الإدارة، وتشرف عليها فنيا مصلحة الأمن العام، ويشمل البناء التنظيمي لهذه الإدارة على ثلاث أقسام وهي: قسم العمليات، وقسم التأمين وقسم البحوث والمساعدات الفنية وتجدر الإشارة إلى أن إدارة مكافحة جرائم الحسابات و شبكات المعلومات ليست الإدارة الوحيدة المختصة بمكافحة هذه الجرائم بل هناك عدة جهات تسعى إلى تحقيق هذا الهدف، ومن قبيل ذلك الإدارة العامة لمباحث الأموال العامة/ الإدارة العامة للمعلومات والتوثيق، وتعد هذه الأخير من أكثر الإدارات بوزارة الداخلية تعاملا مع الجرائم المعلوماتية، وهي تختص بعملية المتابعة الفنية من خلال التحري عن الجرائم المبلغ عنها من الإدارات الأخرى، كما تقوم بتحديد شخص المتهم من خلال عملية التتبع باستخدام عنوان الانترنيت IP الذي يتعامل من خلاله الشخص مع شبكة الانترنت

[2] وقد تم تزويد هذا القسم بمختصين في مجال علوم وهندسة الكمبيوتر وكما تم تزويده بما يلزم من اجهزة ومعدات وبرمجيات تساعده في عمليات التحقيق في جرائم الكمبيوتر وفي فحص الأجهزة المضبوطة في الجريمة والمحافظة على الادلة فيها، وضاح محمود الوضاح، نشأت مفضي المجالي، المرجع السابق، ص 113.

[3] أنظر المادة (13) و (14) من لقانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[4] أطلع عليه على الموقع الإلكتروني التالي:

http ; //www. sawt – alahrar. net/ online/ modules. PHP? Name= News & file= article & Sid= 858.

أما من حيث التكوين والتأهيل فقد قامت الجزائر يبعث إطارات من الدرك الوطني للتكوين والتخصص في البحث والتنقيب، وفي ملاحقة مجرمي المعلوماتية إلى بلدان أجنبية مثل فرنسا والولايات المتحدة الأمريكية وفق اتفاقيات ثنائية للتعاون بين البلدتين[1] كما قامت وزارة العدل الجزائرية وفي تاريخ 2008/12/13 وبالتعاون مع المدرسة الوطنية للقضاء الفرنسية بمقر المدرسة العليا للقضاء بالعاصمة بتنظيم دورة تكوينية لضباط الشرطة القضائية التابعين للمديرية العامة للأمن الوطني وقيادة الدرك الوطني والأمن العسكري والتي كانت بحضور الخبير الفرنسي برنارد سيسمي، نائب الرئيس المكلف بالتحقيق القضائي الجهوي المتخصص بران بفرنسا، وقد نظمت هذه الدورة وعلى حد قول مدير التكوين بوزارة العدل بهدف تعزيز قدرات ضباط الشرطة القضائية خلال التحقيقات الامنية والقضائية في هذا النوع من الجرائم وتكثيف معارفهم القانونية مع عرض تجربة فرنسا في هذا المجال، خاصة وأن الجريمة ظاهرة جديدة في الجزائر[2].

يتضح لنا من خلال ما سبق ذكره أنه مهما نجح المشرع في وضح النصوص القانونية ومجاراته للتطورات التي تشهدها التقنية المعلوماتية يوما بعد يوما إلا أن ذلك يعدو غير كافي ما لم يتبع بإنشاء أجهزة فنية متخصصة يناط بها عملية تطبيق هذه القوانين، وما يطلبه الأمر من إتباع تكوين متعمق في ميدان تكنولوجيات الإعلام والاتصال، ذلك أن توفر استراتيجية تدريبية تعد أفضل وسيلة لتنمية وعي الثقافة المعلوماتية للعاملين يسيرون في خطوات متناسقة مع التطورات السريعة التي صاحبت هذه التكنولوجيا ومواجهتها، لذلك يجب على الجهات المعنية أن تولي التأهيل والتدريب اهتمام خاصا، وذلك بالاعتماد على الكوادر الوطنية داخل وخارج الوطن ومتابعة ذلك بالبحث عن كل جديد حول هذه التقنية وأخذ ما يلزم من الدورات المتعلقة بهذا

[1] la gendarmerie étudie les expériences étrangères afin de combattre la cybercriminalité. disponible en ligne à l'adresse suivante ;
http ; // www. Alegria. Com/ forums / computer – internet / 21325 – cybercriminalité –en – alg – rie- 4. html.

[2] كما يضيف مدير التكوين أنه " تم تنظيم دورة من تأطير خبراء أجانب لحداثة الجريمة على اعتبار أن المجتمع الجزائري حيث الإدراك بالتكنولوجيا والجريمة تفرض تكوين ضباط الشرطة القضائية وتمكينهم من اكتساب تجربة معالجة القضايا باحترافية مستقبلا، واعتبر مدير التكوين أن مثل هذه الملتقيات هي بمثابة تمرين ميداني للمحققين، أنظر أكثر تفاصيل حول هذه الدورة على الموقع التالي:
http ; // www. echoroukonline . com/ara/national/30039.html.

المجال، فضلا عن الاحتكاك بالكوادر العربية والاجنبية والإفادة من خبرات الدول التي لها تجارب ناجحة في المجال التقني [1] لاسيما أمام الفجوة الرقمية[2] التي يعيشها سكان العالم.

ب: إحجام المتضررين عن التبليغ:

إن الطبيعة الخاصة التي تتميز بها الجرائم الاعتداء على نظم المعالجة الآلية، جعلتها تثير العديد من المشكلات، أهمها صعوبة اكتشاف هذه الجرائم وإن اكتشفت فإن ذلك يكون بمحض الصدفة ولا نتحدث من واقع التقنية بالجزائر إذا المتتبع لها يلاحظ ندرة إن لم نقل انعدام القضايا الأمنية والقضائية المنشورة والموثقة المتعلقة بها، إلا أن هذا الواقع من وجهة نظرنا لا يعكس حقيقة الأمور فقلة هذه الجرائم يعود- فيما نرى – إلى عدم اكتشافها والسبب في ذلك هو ذاتية هذه الجرائم من حيث كونها مجهولة ومستترة تتم في بيئة تقنية لا تترك وراءها أي أثر خارجي وذلك عن طريق تلاعب الفاعل غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل المعلومات عن طريقها لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها[3]

والأسوأ من ذلك أنه إذا ما تصادف واكتشفها فإنه يعمد في أغلب الأحوال إلى التستر عليها والصمت بدل استدعاء الشرطة والاعتراف بأنه من ضحايا جرائم الهاكرز.

فقد دلت دراسة أجريت في فرنسا على أن جرائم تقنية المعلومات التي تم اكتشافها لم تمثل إلا (1%) فقط من الجرائم المرتكبة، أما التي تم الإبلاغ عنها فلم تتعد (15%) من النسبة الثانية[4] مما يزيد من الصعوبة لا في مجال اكتشاف وإثبات جرائم الاعتداء على نظم المعالجة الآلية

---

[1] هذا ما أكد عليه الدكتور بشار حافظ الأسد – رئيس الجمهورية العربية السورية – بقوله: " علينا أن نول التأهيل والتدريب اهتماما خاصا في كل المجالات وعلى كل المستويات... وذلك بالاعتماد على الكوادر الوطنية في سورية وخارجها إضافة إلى الاحتكاك بالكودار العربية والأجنبية والإفادة من خبرات الدول التي لها تجارب ناجحة في مجالات محددة ..." أنظر نص الكلمة القومية الشاملة للرئيس بشار الأسد لدى أدائه القسم الدستوري في مجلس الشعب، مؤسسة تشرين للصحافة والنشر، بتاريخ 2000/07/17، ص 20.

[2] " الفجوة الرقمية " هو تعبير أصبح شائعا خلال السنوات القليلة الماضية، يستخدم للدلالة على الهوة التي تفصل بين من يمتلكون المعرفة والقدرة على استخدام تقنيات المعلومات والكمبيوتر والإنترنيت، وبين من لا يمتلكون مثل هذه المعرفة أو هذه القدرة ذلك أن المجتمع أصبح ينقسم على هذا النحو، بالإضافة إلى اقتساماته التقليدية الأخرى، رأفت نبيل علوه، المرجع السابق، ص171.

[3] ومن أمثلة ذلك إدخال فيروس إلى الجهاز عن طريق الاتصال بشبكة الانترنت ويظل الفيروس كامنا حتى لحظة معينة ثم يقوم بتدمير المعلومات.

[4] – سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الاولى، دار النهضة العربية، القاهرة، 1999، ص95.

فحسب، بل وفي دراسة الظاهرة برمتها، وهو ما يعبر عنه العلماء الإجرام بالرقم الأسود chiffre noire [1] حيث يعوق رسم السياسة الجزائرية السليمة لمواجهة الظاهرة الإجرامية المستجدة واختيار أفضل الوسائل لمواجهتها.

فكثيرا من الجهات التي تتعرض أنظمتها للانتهاك تعمد إلى عدم الكشف عنها حتى تبين موظفيها لما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة، تجنبا للإضرار بسمعتها وماكنتها واهتزاز ثقة عملائها فيها [2]، لاسيما أن هذه الجرائم تقع بصفة كبيرة على المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة.

إلى جانب ذلك فإن المجني عليه يتردد احيانا في الابلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكاب هذه الأخيرة قد يؤدي الى تكرار وقوعها بناء على تقليدها من قبل الخرين، كما أنّ الاعلام عنها يؤدي أحيانا الى الكشف عن مواطن الضعف في نظام المجني عليه مما يسهل عملية اختراقه.

وفي هذا الصدد أوصى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات والذي عقد في ريودي جانيرو بالبرازيل في الفترة من 4-9سبتمبر 1994 على ضرورة تشجيع المجني غليهم غلى الابلاغ عن الجرائم والشهود، وغيرهم من مستخدمي تكنولوجيا المعلومات كذلك القرار الصادر عن الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء من ضرورة اتباع تدابير لتشجيع الضحايا على ابلاغ السلطات المختصة بهذه الجرائم. من الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض

[1] محمود صالح العادلي، الجرائم المعلوماتية ماهيتها وصورها، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية بتاريخ 2- 4 أبريل 2006، مسقط، عمان، ص8.

[2] محمد عبد الله ابو بكر سلامة ، المرجع السابق، ص97.

النصوص المتعلقة بجرائم تقنية المعلومات التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم على الجهة مع تقدير جزاء عن الاخلال بهذا الالتزام[1].

ويثير مسألة الابلاغ عن الجرائم الاعتداء على نظم المعالجة الآلية مسائل تتعلق بمدى ما هو متاح من نصوص في التشريعيات الجزائية التي توجب الإبلاغ وترتب عقوبة على ذلك، وبالرجوع الى قانون العقوبات الجزائري وفيما يتعلق بالجرائم التي يعلق القانون تحريك الدعوى فيها على شكوى أو طلب من المجني عليه يكون التبليغ عن الجريمة حقا لكل شخص، وهذه هي القاعدة العامة في حق كل مواطن في الابلاغ طالما أن الجريمة ليست ممن يلزم لتحريك الدعوى عنها شكوى أو طلب من الجهة التي حددها القانون.

ولكن هناك حالات يكون فيها الإبلاغ عن الجريمة واجبا على كل من علم بوقوعها ويترتب على الإخلال بهذا الواجب جزاء جزائيا، كالجريمة المنصوص عليها في المادة (91) من قانون العقوبات الجزائري التي تنص على" مع عدم الاخلال بالواجبات التي يفرضها سر المهنة، يعاقب بالسجن المؤقت لمدة لا تقل عن عشر سنوات ولا تتجاوز عشرين سنة في وقت الحرب وبالحبس من سنة الى خمس سنوات وبغرامة من 3000الى 30000دج في وقت السلم، كل شخص علم بوجود خطط أو أفعال لارتكاب جرائم الخيانة أو التجسس أو غيرها من النشاطات التي يكون من طبيعتها الاضرار بالدفاع الوطني ولم يبلغ عنها السلطات العسكرية او الإدارية أو القضائية فور علمه بها..." والجريمة المنصوص عليها في المادة (32) من قانون الإجراءات الجزائية الي تنص على ما يلي "يتعين على كل سلطة نظامية وكل ضابط أو موظف عمومي يصل إلى علمه أثناء مباشرته مهام وظيفته خبر جناية او جنحة إبلاغ النيابة العامة بغير ثوان، وأن يوافيها بكافة المعلومات ويرسل إليها المحاضر والمستندات المتعلقة بها".

من هذه الزاوية يجب على أي سلطة عامة وكل ضابط أو موظف عمومي، وذلك حسب النص أن يبلغ بأي جريمة من الجرائم محل الدراسة وصل علمها إليه، إلا تعرض للمساءلة

[1].- هشام محمد فريد رستم، المرجع السابق، ص25-27.

التأديبية، لكن ذلك مرتبط برفع ثقافة رجل الأمن أو الموظف فيما يتعلق بهذه الجريمة نظرا لخصوصيتها وطبيعتها الخاصة التي تختلف تماما عن الجريمة التقليدية، ذلك أن أثار الجريمة ودليلها لا يظهران غالبا، وإن ظهرت فلا يستوضحها إلا خبير أو متخصص في المعالجة الآلية وعلى معرفة بنظم الاتصالات وشبكة المعلومات الدولية، فضلا عن ذلك فإن واجب الإبلاغ المقرر بنص المادة (32) لا يمتد إلى اولئك العاملين في القطاع الخاص وشركاته ومؤسساته وهي الكثرة الغلبة من الجهات التي تستخدم نظم المعالجة الآلية مثل المؤسسات المالية والشركات والمصانع الكبرى التي ليست مملوكة للحكومة[1].

لهذا يجب على المشرع الجزائري أن يسارع إلى تكريس قاعدة قانونية موضوعية يعاقب من خلالها على كل من يعلم بوقوع الجريمة ولا يبلغ عنها ولو لم يكن متضررا منها أو ذا مصلحة، ولا شك أن ذلك كله يصب في مصلحة الدعوى الجزائية وإمكانية استجماع الأدلة التقنية في شأن جرائم الاعتداء على نظم المعالجة الألية وبالتالي مساعدة السلطات العامة على كشف ستر هذا النوع من الجرائم والوصول غلى الحقيقة تحقيقا لصالح المجتمع وأفراده، ولصالح المتهمين أنفسهم لكي لا يدان إلا المسيء ويبرأ البريء، مع ضرورة تفادي البلاغات الكيدية.[2]

إلا أن ما يسجل في هذا الإطار أنه في معظم البلاغات عن جرائم الاعتداء على نظم المعالجة الالية خاصة الرقمية منها فإن إمكانيات توافر الجهالة عبرها أكثر حدة مما هي عليه الحال في العالم المادي، أو بمعنى أخر فإن البلاغات التي تصل إلى الجهات المختصة بالتحقيق كثيرا ما تكون مقيدة ضد مجهول وإذا كان الامر على ما سلف، فهل يمكن التعرف على هوية الجاني الحقيقي؟

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 77 – ص 78.

[2] – عوض بن غلاب الوذاني، تقنيات تحديد الهوية في مواجهة التحديات الأمنية ، دار الحامد للنشر والتوزيع، عمان الأردن، د س ن، د.ط، ص 127

– صعوبة تحديد شخصية مرتكب الجريمة:

ويعد هذا التحدي على حد ما في المذكرة التفسيرية لاتفاقية بودابست من إحدى المشاكل التي تطرح للكفاح ضد الإجرام في عالم الشبكات إن لم يكن في نظرنا أهمها وإن كان يمكن معرفة النظام – أي هوية الحاسوب والخادم والمضيف والشبكات – الذي ارتكبت من خلاله ومثل هذا الأمر أوجد اتجاهات في الفقه المقارن تقضي باعتبار مزود الدخول أو خدمات الأنترنت – حسب الأحوال – مسؤولا عن الجريمة حال عدم معرفة شخصية الجاني الأصلي على أساس مبدأ افتراض مسؤولية الغير[1]

فقد أثير في المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلوا / النرويج في الفقرة ما بين 29 – 31 /5/ 2000 موضوع عدم إمكانية البنية التحتية للإنترنت من التوصيل إلى تحديد شخصية مرتكبة الجريمة، أو المصدر الحقيقي لها، وموقعه على وجه التحديد، وإن كانت توفر إمكانية التعرف على عنوان ورقم الحاسوب فقط المرتبط بالأنترنت والمستعمل كوسيلة لارتكاب الجريمة أي ما يعرف اختصارا في النظام التقني (IP) الذي يشير إلى رقم يعين الحاسوب الموصل على الانترنت مثل هذا الرقم الذي يحدد هوية الحاسوب الذي استخدم في ارتكاب جرائم الاعتداء على نظم المعالجة الآلية إنما يفيد حال التوصيل إليه اتخاذ اجراءات التحفظ بقصد ضبط ولكن في مقابل ذلك، فإن هذا الرقم ليس موحدا على المستوى العالمي، إذا أن هناك أقلية من الدول التي تتبعه دون غيرها وخاصة الدول العربية، ففي الولايات المتحدة أو كندا وبعض الدول الأخرى يمكن للشخص فيها اقتناء (IP) خاص به يشير إلى كونه أحد أعضاء الانترنيت ومن ثم يمكن تحديد هذا الشخص بكل سهولة لتبدأ بعد ذلك سلسلة إثبات ارتكابه للجريمة من عدمه.

إلا أنه في دول الاخرى مثل أغلب الدول العربية فإن مصداقية الهوية عبر الانترنت (IP) تتقلص كثيرا إذا علمنا أن كل خط هوية على الانترنت يصادفه عدد من الهويات التي يمكن أن

[1] عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 835.

تكون محل للتغاير بين أعضاء الانترنت المشتركين في مزود انترنت واحد[1] وهنا يمكن القول أن مجرد وجود شخص في الجزائر أو في سوريا فإنه يملك فورا هوية رقمية محددة حقا حال وجوده على الانترنت، إلا أنه إذا حدث وانقطع الإرسال فإن الشخص إذا عاد من جديد إلى الانترنت فإن الهوية السابقة لن تكون له وإنما لغيره، إذا من الممكن جدا – بل وهو الامر المعتاد هنا- أن يتواجد بهوية (IP) أخرى.

ونتفق فيما يذهب إليه البعض[2] من ان الأمر هنا يترك بعد ذلك لفطنة عضو الضابطة العدلية وكيفية تعامله مع الحدث، وهو هنا يستند إلى مسالة الدلائل الكافية وما ينبثق عنها من شبهات كما لو كان الحاسوب الذي تم عبره ارتكاب جريمة الاختراق هو حاسوب شخصي يخص شخص بعينه، وفي هذه الحالة فإن ضبط الحاسوب ذاته يستدعي بالضرورة سؤال صاحبه فيما إذا كان قد استخدم احد غيره الحاسوب المذكور أو يكون الحاسوب المذكور موضوعا في الغرفة الشخصية سيما وأن العادة قد جرت على أن يحتفظ الأشخاص صغار السن بمقتنياتهم الشخصية في غرفهم ولا يسمحون لأحد غيرهم باستعمالها، ومن ثن فإنه ما يتم تحديد هوية الحاسوب (IP) حتى يتمكن في الغالب من الأحوال تعيين المتهم طالما أن الأمر يتعلق بحاسوب موضوع في منزل أو في شركة أو مكتب أو هيئة، إلا أن الامر يزداد صعوبة حين يكون الحاسوب في مكان شبه عام معد لتقديم خدمة للجمهور كما هو الشأن في مقاهي وإن كانت تقوم في العادة بالاستعلام عن اسم عضو الانترنت الذي استخدم الحاسوب فيها فقط كل ما يمكن الحصول عليها معطيات حول هيئته وزمن استعماله للحاسوب ... ومطابقة ذلك مع زمن حدوث الواقعة.[3]

لكن ماذا لو كانت المعلومات المحملة في عناوين IP غير حقيقة أو زائفة؟ وهذا ممكن حينما تحدث حزم معلوماتية Pocket باستخدام مصدر زائف لمصدر عنوان (IP) بحيث يظهر

[1] – نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي-دراسة مقارنة-، دار هومة للطباعة والنشر والتوزيع، 2008، ص17.

[2] – عمر أبو بكر بن يونس، المرجع السابق، ص 833.

[3]- عوض بن محمد غلاب الوذاني، المرجع السابق، ص 222.

أن المعلومات جاءت من نظام معالجة محدد بينما في الحقيقة جاءت من كمبيوتر آخر، ومثال ذلك حينما يقوم برنامج خبيث بإدخال معلومات كاذبة أو غير حقيقية عن حقيقية عنوان (IP) في Pocket الإرسال وقبل الولوج في الشبكة المعلوماتية ويحدث ذلك حينما يقوم البرنامج الخبيث بإغراق الشبكة بالمعلومات أو إرسال العديد من الرسائل أو حث الماكينة الرئيسية في مزود الخدمة أو الشبكة على الإسراع أو التعجيل في العمل، إلا أنه لحسن الحظ معظم المجرمين لا يعلمون كيف يزيفون عناوين (IP) ولا يعرفون أي من عناوين (IP) يمكن أن تكون دالة على شخص المجرم في الجريمة المحددة[1].

وبعد دراستنا للقواعد المنظمة لاستخلاص الدليل التقني، توضح لدينا مدى الصعوبات والتعقيد التي تكتنف الحصول عليه، وهو ما يفتح الباب لمناقشة مسألة مشروعية الأخذ بهذا النوع من الأدلة ومصداقيتها في إطار نظرية الإثبات الجزائي، وهو ما سنتناوله في المطلب التالي.

المطلب الثاني : مشروعية الدليل التقني و مصداقيته

يعتبر الدليل التقني من الأدلة الحديثة التي أفرزها التطور التقني، وهو ايضا ذو طبيعة خاصة من حيث الوسط الذي ينشأ فيه والطبيعة التي يبدو عليها وهذا يثر التساؤل حول مشروعية الأخذ به، إذا أنه يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده والحصول عليه، فمشروعية الوجود تقتضي أن يكون الدليل قد قبله المشرع ضمن أدلة الإثبات الجنائي المعمول بها في قانونا الإجرائي.[2]

كما أن الدليل التقني في تعبيره عن الحقيقة التي تهدف إليها الدعوى العمومية ، لا سيما من خلال الصعوبات المصاحبة لاستخلاصه إضافة للتطور في مجال التقنية مما يتيح العبث بها مما يؤثر في مضمونها مما يجعلها مخالفة للحقيقة ، و هو ما سنحاول تحديده على النحو التالي:

[1] –ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (tcp/IP) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق، ص 18.

[2]- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية دراسة تحليلية، دار الكتب القانونية مطابع مصر الكبرى، د.ط، 2011، ص 195

الفرع الأول : مشروعية الدليل التقني

إن قبول الدليل يتسع ويضيق تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة، فيما إذا كانت تجنح إلى تقييده ، أم كانت تطلق حريته.

ويتيقن القاضي الجزائي في هذه المرحلة أساسا من مدى مراعاة الدليل الجنائي أساسا لقاعدة مشروعية إن منطق الحديث لدراسة مشروعية الدليل التقني يقتضي منا تناول مشروعية وجوده ومن ثم مشروعية الحصول عليه.

أولا :مشروعيته من حيث الوجود

يقصد بمشروعية الوجود أن يكون الدليل معترف به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة[1]، ويمكن القول أن طبيعة نظام الإثبات السائد في الدولة هو المعيار الذي يتحدد على أساسه موقف القوانين المقارنة فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل التقني.

وفي هذا الإطار نجد أن نظم الإثبات لا تخرج عن ثلاث فئات:

الفئة الأولى:

وتأخذ بنظام الأدلة القانونية، حيث تحدد الأدلة التي يجوز للقاضي الجنائي قبولها.

الفئة الثانية: وهي القوانين الأنجلوساكسونية حيث تقيد من حرية الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة، أما في مرحلة تحديد العقوبة فسيود مبدأ حرية الإثبات.

الفئة الثالثة: وهي القوانين ذات الصياغة اللاتينية، حيث تبنى مبدأ حرية الإثبات، ومنها سلطة القاضي في قبول جميع الأدلة وهنا تكون جميع طرق الإثبات مقبولة، ما لم يستبعد المشرع بعضها صراحة[2] وينتمي إلى هذه الفئة القانون الفرنسي (المادة 427 من قانون الإجراءات الجزائية) والقوانين الاخرى التي تأثرت به كالقانون الجزائري (المادة212 من قانون الإجراءات الجزائية) وهو النظام الذي سيكون محل دراستنا على اعتبار اعتناقه من قبل المشرع الجزائري .

[1] طارق محمد الجملي، المرجع السابق، ص 11.

[2]- نجيمي جمال ، المرجع السابق، ص 70 وما بعدها.

وفي هذا الصدد لم نجد المشرع الجزائري وكغيره من التشريعات المنتمية إلى العائلة ذات الأصل اللاتيني أنه قد أفرد نصوصا خاصة تحظر على القاضي مقدما قبول أو عدم قبول أية دليل بما في ذلك الدليل التقني، وهذا أمر منطقي على اعتبار أن الجزائر تستند لمبدأ حرية الإثبات الحر حيث أصبح هذا الأخير القانون العام في الإجراءات الجزائية في التشريعات اللاتينية، وتتمثل خصائص هذا النظام في أنه لا يرسم للقاضي طرقا محددة للإثبات يقيده بها، بل يترك الخصوم أحرار يقدمون الادلة التي يستطيعون إقناع القاضي بها، ويترك القاضي حرا في تكوين اعتقاده من أي دليل يقدم إليه وهو حر في وزن وتقدير كل دليل، وفي التنسيق بيم الأدلة التي تتمثل في الحكم بالإدانة أو البراءة، دون أن يقيده في هذا الإطار بأي نوع من الشروط سوى تلك التي يتعين عليه تطلبها فيه – أي في الدليل –.

وعليه فإنه في مثل هذا النظام لا تثور مشكلة مشروعية الدليل التقني من حيث الوجود على ، فالأساس هو حرية الأدلة ولذلك فمسألة قبول الدليل التقني لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي، إلا أن الطبيعة الخاصة للدليل التقني قد اقتضت منا توسيع نطاق بحث مشروعية الوجود إلى مسالة هامة تتعلق بأصالة الدليل التقني.

أ: قبول الدليل التقني في التشريع على أساس مبدأ حرية الإثبات الجزائي:

تعتبر حرية الإثبات في المسائل الجزائرية من المبادئ المستقرة في نظرية الإثبات الجزائي ويقصد بهذا المبدأ أنه لجميع الأطراف لحرية في اللجوء إلى كافة وسائل الإثبات للتدليل على صحة ما يدعونه، فلسلطة الاتهام أن تلجأ إلى أية وسيلة لإثبات وقوع الجريمة على المتهم، ويستظهر القاضي الحقيقة بكل ذلك أو بغيره من طرق الإثبات[1].

وقد أقر المشرع الجزائري مبدأ حرية الإثبات الجزائي في المادة (212) من قانون الإجراءات الجزائية حيث نصت على أنه " **يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا**

[1] أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجزائية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1982، ص240.

الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي" .

بينما نص عليه المشرع الإجرائي الفرنسي بالمادة (427) من قانون الإجراءات الجزائية الحالي والتي جاء فيها " **ما لم يرد نص مخالف، إثبات الجرائم بجميع طرق الإثبات، بحكم القاضي بناء على اقتناعه الشخصي"**[1] وهذا النص وإن كل مخصصا لمحاكم الجنح، إلا أن مبدأ حرية الإثبات يطبق أمام جميع أنواع المحاكم الجزائية، إلا إذا نص القانون على خلاف ذلك. وهناك العديد من الاسباب التي تبرز الأخذ بمبدأ حرية الإثبات في نطاق نظرية الإثبات الجزائي منها أن حرية الإثبات تعد نتيجة منطقية لمبدأ قضاء القاضي بمحض اقتناعه الذاتي والتي تستلزم بالضرورة منح الحرية للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها حتى يتسنى له أداء رسالته في إرساله العدالة بين المتقاضين.

كما أنه ومن العلم أن الإثبات في الدعوى الجزائية يرد على وقائع قانونية مادية كانت أو نفسية ، التي يصعب الحصول على دليل مسبق لها وذلك بعكس الدعوى المدنية التي يرد الإثبات فيها على تصرفات وأعمال يسهل إعداد دليل مسبق بشأنها[2].

و من بين المبررات الداعية للإخذ بحرية الإثبات ظهور الادلة العلمية الحديثة التي كشف عنها العلم الحديث في إتيان الجريمة ونسبتها إلى المتهم كبصمة الصوت، والبصمة الوراثية D.N.A

ولا يختلف الأمر في الجزائر بالنسبة للدليل التقني حيث لم يتضمن قانون (09 – 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها أية وأوضاع خاصة بهذا الصدد، ومن ثم فإن الدليل التقني سيكون مشروعا من حيث الوجود استصحابا للأصل – أي الاصل في الأدلة مشروعية وجودها – وذلك باعتباره من الاساليب العلمية الحديثة في الإثبات الجزائي.

[1] ART 427 du C.P.PF dispoose que « hors les cas àu la loi en dispose autrement, les infractions peuvent etre établies par tout mode de preuve et le juge décide d' après son intime convicition »

[2] – محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988، ص 409 وما بعدها.

إن أعمال مبدا حرية الإثبات على النحو السابق ذكره يجعل من دور القاضي الجزائي دور إيجابي في كشف الحقيقة الفعلية في الجرائم التقليدية منها والمستحدثة كالجرائم محل الدراسة، ويبدو هذا الدور من ثلاث جوانب:

الأول: له الحرية في توفير الدليل المناسب والضروري للفصل في الدعوى بما في ذلك الدليل التقني.

الثاني : له الحرية في قبول اي دليل ، يمكن ان تتولد منه قناعته بما في ذلك الدليل التقني .

الثالث : انه يتمتع بالحرية نفسها في تقدير قيمتها الاقناعية حسبما تنكشف لوجدانه .

و بالرغم من ان النيابة العامة عليها اقامة الدليل على الادانة و المتهم عليه نفيه بكل الإمكانيات، إلا أن ذلك ليس معناه عدم تدخل القاضي، فدوره ليس سلبيا يقتصر على موازنة الأدلة مع بعضها البعض و ترجيح الأقوى منها كدور القاضي المدني بل دوره ايجابي ، فمن حقه و واجبه ان يتحرى وينقب عن الحقيقة باتخاذ الاجراء الذي يراه مناسبا ، ويقتنع بمنتهى الحرية ذلك في إطاره مسعاه لإكتشاف الحقيقة .

وهكذا فان القاضي الجزائي سواء بناءا على طلبات الاطراف او بموجب مقتضيات سلطته ان يأمر باتخاذ الاجراء الذي يراه مناسبا وضروريا للفصل في الدعوى، فيمكنه سماع الشهود او استدعاء الخبراء اذ واجهتها مسالة فنية ،كما لها ان تسال او تستجوب المتهم حول اساس الاتهام الموجه اليه (المادتان (442) و (536) من قانون الاجراءات الجزائية) .

اما في مواد الجنايات فقد خول القانون الاجرائي الفرنسي لرئيس محكمة الجنايات بموجب نص خاص وهو المادة (310) من قانون الاجراءات الجزائية سلطة تفويضية بمقتضاها يمكن ان يتخذ كافة الاجراءات التي يعتقد انها مفيدة في الكشف عن الحقيقة حيث لا قيد عليه سوى شرفة وضميره .

وتطبيقا على جرائم الاعتداء على نظم المعالجة الالية ، فان للقاضي الجزائي وفي سبيل الوصول الى الحقيقة له ان يوجه امرا الى مزود الخدمة بتقديم المعطيات التي تسمح بالتعرف على المرسل اليهم الاتصال وكذا عناوين المواقع المطلع عليها ... الخ .[1]

ومن ابرز مؤشرات او دلائل الدور الايجابي للقاضي الجزائي في البحث عن الدليل التقني ايضا ، ان للقاضي الجزائي سلطة الامر باعتراض الاتصالات السلكية و اللاسلكية متى ما قدر فائدة الاجراء وجديته وملائمته لسير الدعوى .

كما للقاضي الجزائي ندب الخبراء وكذا اعلانهم ليقدموا ايضاحات عن التقارير المقدمة منهم ، لما للخبرة في مجال المساعدة القضائية من الدور الكبير ، فهي تعد من اقوى مظاهر تعامل قاضي الموضوع من الواقعة الاجرامية الموضوعة وهذا الاخير يملك تعيين الخبراء سيما ان الاصل يظل للتحقيق الذي تجريه الامحكمة في الجلسة ، وهذا ما اكدته المادة (143) من قانون الاجراءات الجزائية الجزائري حينما نصت " **لجهات التحقيق او الحكم عندما تعرض لها مسالة ذات طابع فني ان تامر بندب خبير اما بناء على طلب النيابة العامة واما من تلقاه نفسها او من الخصوم .....**"

وفي مجال البحث عن الدليل التقني نجد ان الخبرة التقنية في مجال المساعدة القضائية تعد اقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات ازاء نقص المعرفة القضائية الشخصية لها ، فمما لا شك فيه ان عملية الحصول على الادلة الجنائية التقنية امر صعب الوصول اليه لما تتطلبه من خبرة ومهارة كبيرة في مجال تقنية المعلومات ، ويرجع ذلك لتعدد صور و اشكال الإجرام الواقع على نظم المعلوماتية ، مابين مهاجمة المعلومات بغرض تدميرها او الاستيلاء عليها او قد يكون المقصود بالهجوم هو الاجهزة كنشر الفيروس يعمل على اتلاف وحداته الرئيسية مثلا او قد يكون الامر مجرد اختراق لكلمة سر خاصة ببنك او مؤسسة كبرى بغرض الاحتيال

[1]- سامي جلال فقي حسين، المرجع السابق، ص 73.

والحصول على الاموال ، وقد تكون بمجرد اثبات الذات وإظهار المقدرة العالية في مجال نظم المعلوماتية .[1]

ولما كانت عملية تجميع الادلة التقنية الجزائية في الجرائم محل الدراسة ، تعد من اهم واصعب الامور التي تواجه عملية الاثبات الجزائي لذا كان لزامان يتم اللجوء الى خبير قضائي تقني او رقمي ، متخصص ، لاستخلاص الدليل التقني .

تعد مرحلة قبول الدليل التقني المرحلة او الخطوة الثانية التي تلي البحث عن الدليل وتقديمه من قبل جميع الاطراف (سلطة الادعاء، المتهم ، القاضي).

و في هذا الصدد طبقا لمبدأ الشرعية الاجرائية التي يتحصل من خلالها الدليل الجزائي بما يتضمنه من ادلة مستخرجة من وسائل الكترونية كالكمبيوتر المحمول مثلا ، لا يكون الدليل مقبولا في عملية الإثبات والتي يتم من خلالها إخضاعها للتقدير ، إلا إذا كان مشروعا بأن تم البحث عنه والحصول عليه وفقا لطرق مشروعة[2].

ب– مدى تأثير الأصالة الرقمية في الدليل التقني على مبدأ قبوله:

وهذه المسألة لا يمكن المرور دون بحثها ، فهناك تميز حقيق بين الأصالة في طابعها المادي وبين الأصالة في طابعها الرقمي ، من حيث أن الأولى إن هي سوى تعبير عن وضعية مادية ملموسة ، كما هو الشأن في الورق المكتوب أو بصمة الأضبع أو الحدوث العيني للواقعة ، فهذه كلها لها طابعها المادي المتميز ، في حين أن الثانية ليست سوى تعداد غير محدود لأرقام ثنائية موحدة في الصفر والواحد ، فطبيعة الدليل التقني لا تعبر عن قيمة أصلية بمجرد رفع محتواه على الأنترنت حيث يتواجد في كل مكان يتم استدعاءه منه[3].

وتبرز هذه المشكلة بصورة جلية عندما يقوم المتهم بإزالة الدليل التقني عن بعد ، فكما هو معلوم يكون ما تبقى منه هو نسخة فقط قد تم التوصل إليها عن بعد أيضا بطريق المراقبة

[1] – عمر الشيخ الأصم، نظام الرقابة النوعية في المختبرات الجنائية في الدول العربية، دار الحامد للنشر والتوزيع، عمان، الاردن، 2006، ص 57.

[2] – عائشة بن قارة مصطفى ، المرجع السابق ، ص125.

[3] – عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، المرجع السابق ، ص973.

الإلكترونية مثلا ، ومن ثم فهل يكفي ناتج المراقبة الإلكترونية وحده للقول بأن الدليل هنا هو دليل أصلي وبالتالي يقبل طرحه على القضاء؟ وذات السؤال ينطبق على حالة الدليل المسترد بعدما تم حذفه باستخدام خاصية الإلغاء؟

والواقع من الأمر أن بحث موضوع الأصالة على المستى القانوني جعل المشرع المقارن يعتمد منطق افتراض أصالة الدليل التقني ، حيث نص قانون.

الإثبات الأمريكي في المادة (3/1003) على أنه ، « إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة فإن أية مخرجات طابعة مشا أو مخرجات مقروءة برؤية العين تبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية».

وإن كان ذلك كذلك، فإنها دعوة إلى المشرع الجزائري لكي يأخذ حظه في تقنين هذا النوع من المسائل وأهميته، وتبرز أهمية التسليم بمنطق افتراض الأصالة في الدليل التقني على المستوى القانوني هو في حالة رفضها، إذ لا نكون أمام دليل إدانة، وهو ما يؤدي في النهاية إلى رفض منطق التعامل مع هذه النوعية من الأدلة حال كونها لازمة.

إذا كان مبدأ حرية الإثبات يجيز للقاضي حرية الاستعانة بكافة وسائل الإثبات اللازمة بما في ذلك الدليل التقني لتكوين عقيدته، إلا أن هذا الإطلاق ليس بلا قيد وبلا حدود، وإلا لوصل الأمر إلى درجة الفوضى، بل لكان الأمر قد وصل إلى درجة التساهل بارتكاب جرائم تحت ستار البحث عن الأدلة والتحقيق فيها، لذا كان من الضروري رسم ضوابط وأطر معينة يتعين أن تمارس في نطاقها بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من وراءها، وهو الوصول إلى الحقيقة الفعلية في الدعوى، وإذا كانت هذه الحقيقة تمثل الهدف الأسمى لقانون الإجراءات الجزائية.

ونتيجة لذلك جنحت أغلب التشريعات إلى تحديد الأدلة التي تقبل في إثبات عينة من الجرائم إذ لا يجوز الإثبات بغيرها كأدلة إثبات جريمة الزنا[1].

[1] حيث اقتصر المشرع الجزائري على ثلاثة أنواع من الأدلة فحسب لإثبات جريمة الزنا وذلك ما نصت عليه صراحة المادة (341) من قانون العقوبات الجزائري، على أن الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة (339) يقوم إما على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة التلبس، وإما بإقرار وارد في رسائل أو مستندات صادرة من المتهم وإما بإقرار قضائي.

كما يلزم المشرع أحيانا القاضي الجزائي بإتباع طرق الإثبات الخاصة في بعض المسائل غير الجزائية التي يتوقف على الفصل فيها الفصل في الدعوى الجزائية – أي إثبات المسائل الأولية خاصة المدنية والتجارية منها مثل إثبات عقد الأمانة في جريمة خيانة الأمانة[1]، إلا أن هناك قيدا عاما يحد من حرية القاضي في قبول الدليل بما في ذلك الدليل التقني وهو قيد المشروعية، حيث يشترط في الدليل الذي يبني عليه حكمه أن يكون قد تم الحصول عليه بطريقة مشروعة والقول بغير ذلك يهدر قيمة الدليل وتشوب قضاءه بالبطلان انطلاقا من القاعدة التي تقول: « ما بني على باطل فهو باطل ».

ثانيا : مشروعيته من حيث طريقة الحصول عليه

طبقا لمبدأ المشروعية الذي تخضع له قواعد الإثبات الجزائي فإن الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية، لا يكون مشروعا إلا إذا تم الحصول عليه و تقديمه إقامته أمام القضاء، بالطرق المطلوبة قانونا ، ومتى ما تم الحصول على الدليل خارجها فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، ومن قبيل ذلك حصوله من تفتيش لنظام معلوماتي باطل، كما لو لم تكن جريمة من جرائم الاعتداء على النظم محل الإذن قد وقعت بعد .

ولقد وضعت الدساتير الوطنية[2]، والقوانين الإجرائية المختلفة[3]، نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية ومن تم مخالفة هذه النصوص في استخلاص الدليل الجزائي يصبغ هذا الدليل باللامشروعية .

ومشروعية طريقة الحصول على الدليل بصفة عامة لا تعني بالضرورة اتفاق الإجراء مع القواعد القانونية المكتوبة أو التي ينص عليها المشرع فحسب، بل يجب أن تتعدى ذلك إلى مراعاة إعلانات حقوق الإنسان والمواثيق والاتفاقيات الدولية وقواعد النظام العام وحسن الآداب السائدة

[1] و في ذلك نصت المادة (177) من قانون أصول المحاكمات الجزائية السوري صراحة ،إذا كان وجود الجريمة مرتبطا بوجود حق شخصي وجب على القاضي إتباع قواعد الإثبات الخاصة به .

[2] راجع المواد (46)- (48) – (32) – (34) فقرة (2 – 35) من الدستور الجزائري لسنة 1996، والمواد (28)-(29)-(31) – من الدستور السوري لسنة 1973 المعدل بالقانون رقم 6 لعام 2000 .

[3] راجع المواد (41) و (44) من قانون الإجراءات الجزائية الجزائري.

في المجتمع وبالإضافة إلى المبادئ التي استقرت عليها محكمة النقض وبصفة عامة مع الأنظمة الثابتة في وجدان المجتمع المتحضر.

ويترتب على ذلك أن إجراءات جمع الأدلة المتحصلة من الوسائل الإلكترونية إذا خالفت تلك القواعد والمبادئ التي تنظم كيفية الحصول عليها، فإنها تكون باطلة وبالتالي بطلان الدليل المستمد منها لأنه ما بني على باطل يكون باطل، ولهذا الموضوع أهمية بالغة لما يترتب على بطلان الدليل آثار فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد عليه في إدانة المتهم.

فمشروعية الدليل تتطلب صدقه في مضمونه، وان يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث طرق الحصول عليه.

والحقيقة أن هذا القيد يحظى أهمية كبرى نتيجة التطور الكبير الذي تحقق مؤخرا في شأن تطويع التقنية لكي تعمل في بيئة الرقابة والبحث والتحقيق كالمراقبة الإلكترونية مثلا التي استحدثها المشرع الجزائري بموجب القانون رقم (04-09) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإذا كانت هذه الأخيرة تفيد في الكشف عن الجريمة وإقامة الدليل على الجاني، فإنها قد تعصف أكثر فأكثر بحقوق الأفراد وحرياتهم إذا لم يحسن استخدامها، وهو ما قد ينجر عنه الإضرار بالعدالة .

والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراء والإجراءات اللاحقة له مباشرة، غير أن هذه القاعدة تثير مسألة في غاية الأهمية تتعلق بماهية المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له حتى يمتد إليها البطلان، وقد تعددت المعايير التي قال بها الفقه المقارن والمعيار الراجح والسائد في الجزائر هو أن العمل اللاحق يعتبر مرتبطا بالإجراء السابق إذا كان هذا الأخير مقدمة ضرورية لصحة العمل اللاحق، فإذا أوجب القانون مباشرة إجراء معين قبل آخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه كان الإجراء، الأول شرطا لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه[1].

[1] أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجزائية، رسالة دكتوراه كلية الحقوق، جامعة القاهرة، 1959، ص382،

أما موقف القاضي من الدليل التقني غير المشروع ومدى الأخذ به سواء كان ذلك في إدانة المتهم أو براءته سوف نتعرض له فيما يلي .

أ- الدليل التقني غير المشروع :

في إطار بحث مشروعية الدليل التقني أثيرت مسألة قيمة الدليل التقني غير المشروع في الإثبات الجنائي ؟

ومثل هذا التساؤل سوف يقود حتما إلى بحث قيمة كل من دليل الإدانة ودليل البراءة للوقوف على ما إذا كان هناك فرق بين الحالتين أم لا، وذلك كل في فقرة مستقلة على التوالي:

– بالنسبة لدليل الإدانة :

انطلاقا من قاعدة أن الأصل في الإنسان البراءة فإن المتهم يجب أن يعامل على أساس أنه بريء في مختلف مراحل الدعوى إلى أن يصدر بحقه حكم بات (نهائي)، وهذا يقتضي أن تكون الأدلة التي تؤسس عليها حكم الإدانة مشروعة[1] ولا يهم في ذلك إن كانت أدلة تقليدية أو مستخلصة من الوسائل الإلكترونية.

وأي دليل إدانة يتم الحصول عليه بطريقة غير مشروعة أو بوسيلة مخالفة للقانون يعتبر غير مشروع ومن ثم غير مقبول في عملية الإثبات، لأنه إذا ما سمح بقبول الأدلة التي تكون وليدة إجراءات باطلة، فإن الضمانات التي كفلها القانون لحماية حقوق المواطن أو كرامته لا قيمة لها، كما أن القواعد التي يسنها المشرع لا أهمية لها متى ما أمكن إهدارها وعدم الالتزام بها .

وبناء على ذلك لا يجوز القبول بدليل تقني جرى الحصول عليه من تسرب، جرى القيام به دون مراعاة الشروط الشكلية والموضوعية للإذن بمباشرة التسرب، أو عن طريق إكراه المتهم المعلوماتي من أجل فك شفرة الدخول إلى النظم المعلوماتية، أو كلمة السر اللازمة للدخول إلى ملفات المعلومات المختزنة، وتتسم بعدم المشروعية أيضا أعمال التحريض على ارتكاب الجريمة من قبل أعضاء الضابطة العدلية، التنصت والمراقبة الإلكترونية عن بعد دون مسوغ قانوني .

[1] – محمد راغب، النظرية العامة للإثبات في التشريع العربي المقارن، الطبعة الأولى، مطبعة المعرفة،القاهرة،1960،ص177،

فإذا ما حصل دليل تقني وفق الطرق السابقة يتم إبطاله، وعدم إنتاج الإجراء الباطل الآثار التي تترتب عليه مباشرة، حيث نصت المادة (191) من قانون الإجراءات الجزائية الجزائري على أنه: «تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها..» .[1]

ب – بالنسبة لدليل البراءة:

بينا في الفقرة السابقة أن حكم الإدانة يجب أن يكون مستندا على دليل تقني مشروع، ولا يجوز أن تبنى الإدانة على دليل باطل، إلا أنه في دليل البراءة نلمس اختلافا حول مدى اشتراط المشروعية بوجه عام في دليل البراءة ويمكن رد هذا الخلاف إلى ثلاثة اتجاهات كما يلي :

الاتجاه الأول[2]: يرى أن المشروعية لازمة في كل دليل سواء أكان إدانة أو براءة، على سند من القول أن القضاء ليس له أن يقر قاعدة أن الغاية تبرر الوسيلة كمبدأ قانوني صحيح، فالمفروض أن تكون السبل القانونية المشروعة كفيلة وحدها بإثبات براءة البريء في أي تشريع إجرائي قويم وإلا فإن البنيان الإجرائي كله يكون مختلا متداعيا، إذا كان يسمح بإدانة البريء، أو بالأدق إذا كان لا يسمح ببراءة البريء إلا بإهدار مبدأ الشرعية من أساسه. وينتهي هذا الاتجاه إلى إثبات البراءة – كالإدانة – لا يون إلا من خلال سبل مشروعة ولا يصح أن يفلت إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أي تشريع لكل اقتناع سليم .

[1] – وفي ذلك أوصى المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، والذي عقد في ريو دي جانيرو بالبرازيل في الفترة من 4-9 سبتمبر سنة 1994 في مجال حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان بمجموعة من التوصيات، منها التوصية رقم (18) التي تنص على أن «كل الأدلة التي تم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة، ولا يمكن التمسك بها أو مراعاتها، في أي مرحله من مراحل الإجراءات، وقد أشار هذا المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب .

[2] – رؤوف عبيد ، مبادئ الإجراءات الجنائية في القانون المصري ، دار الفكر العربي ، القاهرة ، ص747-741، محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، المرجع السابق ، ص426 هامش رقم (2).

الاتجاه الثاني[1] : يرى أن المشروعية لازمة في دليل الإدانة دون البراءة على سند من القول أن الأصل في الإنسان البراءة ولا حاجة للمحكمة بأن تثبت براءته، وكل ما تحتاج إليه هو أن تشكك في إدانته، ويضيف هذا الاتجاه إلى أن بطلان دليل الإدانة الذي تولد من إجراء غير مشروع لم نما شرع لضمان حرية المتهم، فلا يجوز أن ينقلب هذا الضمان وبالا عليه .

بينما يبرز اتجاه ثالث وسط[2]، مفاده أن أداة البراءة غير المشروعة تقبل في حالات دون أخرى، فإذا كان الدليل قد تم التوصل إليه بوسيلة تعد جريمة جنائية، فإن هذا الدليل لا يعول عليه ويجب استبعاده.

أما إذا كانت الوسيلة لا تصل إلى حد الجريمة وإنما تتضمن مخالفة قاعدة إجرائية، ففي هذه الحالة لا يهدر الدليل المتحصل عليه بل يمكن الاستناد إليه .

وفي إطار الترجيح بين هذه الاتجاهات نجد أنفسنا نؤيد الاتجاه الثاني والذي يقصر المشروعية على دليل الإدانة دون البراءة، وذلك لأننا لو تمسكنا بعدم قبول دليل البراءة بحجة أنه غير مشروع، فإننا سوف نصل إلى نتيجة خطيرة للغاية وهي إدانة بريء، وفي هذه الحالة يتحمل المجتمع ضررين: الضرر الأول عقاب بريء قام الدليل على براءته، أما الضرر الثاني هو إفلات مجرم يستحق العقاب من العقاب .

أما التعليل بأن التشريع القانوني كفيل وحده بإثبات براءة البريء، فليس على إطلاقه، لأنه وعلى حد قول البعض من الفقه[3] وبحق- ما من تشريع في العالم من منع البشر إلا وتعتريه فجوات وعيوب كثيرة، تجد س الناس من يستطيع خرق هذه القوانين، بحجة إتباع القانون نفسه وذلك بطرق غير مباشرة، ولذلك فالقوانين الوضعية مرشحة للتعديل والتجديد في أي وقت .

---

[1] – محمود محمود مصطفى، شر قانون الإجراءات الجنائية، الطبعة الثانية، مطبعة دار النشر الثقافة، القاهرة، 1974، ص174. د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الجزء الثالث، دار النهضة العربية، القاهرة، 1980 ص388.

[2] – سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، القاهرة، دار النهضة العربية 1972، ص471-473.

[3] – عوض بن محمد غلاب الوذناني، المرجع السابق، ص 108.

وإذا كان الأمر على ما سلف، فإنه لا يكفي لاعتماد هذا الدليل كدليلا للإدانة، إذ الطبيعة الفنية الخاصة للدليل التقني تمكن من العبث بمضمونه على نحو يحرف الحقيقة أو لوجود خطأ في الحصول عليه، وهو ما يفتح الباب لمناقشة مسألة مصداقيته في إطار نظرية الإثبات الجزائي.

الفرع الثاني : مصداقية الدليل التقني

السائد فقهيا أن سلطة القاضي الجزائي في تقدير الدليل يحكمها مبدأ حرية القاضي الجزائي في تكوين قناعته مما يستتبع ذلك حتميا نتيجة هامة ألا وهي « حرية القاضي في تقدير الأدلة» ، ذلك أن مسألة قيمة الدليل لإثبات الحقيقة هي مسألة موضوعية محضة للقاضي أن يمارس سلطته التقديرية فيها، بل هي المجال الطبيعي لهذه السلطة حيث أنها تتعلق بقيمة الدليل في الإثبات وصولا للحقيقة[1] .

إلا أنه في الوقت الذي منح القانون للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لاقتناعه الشخصي، فإنه في المقابل لم يطلق حريته ليقضي كيفما شاء وفقا لهواه الشخصي بل قد أحاطه بقيود و ضوابط تشكل في مجموعها شروطا لضمان الوصول إلى الحقيقة الفعلية في الدعوى من دون الانتقاص من الحقوق والحريات .

وهو ما كرسه المشرع الجزائري صراحة بموجب المادة (212) من قانون الإجراءات الجزئية حيث نصت " **يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي....**" و هذا يعني أن الأدلة الجزائية لا تحضى أمام القاضي الجزائي بقوة ثبوتية ، مما ينتج عنه أن القاضي يؤسس اقتناعه على أي دليل كما يصح أن يهدمه تبعا لقناعته الشخصية ، فلا يجوز مطالبة أو إلزام القاضي بالاقتناع بأي دليل ولو لم تكن في الدعوى أدلة سواه .

[1] – فاضل زيدان محمد، المرجع السابق ،ص ص 92 – 94 .

و في إطار الجرائم محل الدراسة خاصة فيما تعلق بالطبيعة الخاصة للدليل التقني التي تمكن من العبث بمضمونه على نحو يؤدي لتحريف الحقيقة أو التغيير في مضمونها ، و مع نقص المعرفة المعلوماتية للقاضي الجزائي فإن الأمر على القاضي الإستعانة بالخبرة لإستخراج الدليل ويبحث مصداقيته في مجال المعلومات، مما قد يقوي من قيمته على نحو لا يقبل العكس، الذي من شأنه إضفاء حجية قاطعة وقوة على الدليل التقني بما لا يمكن للقاضي الجزائي أن يعمل سلطته التقديرية لقبوله .[1]

أولا : مصداقية الدليل التقني بوصفه يعبر عن حقيقة علمية

يعتبر الدليل التقني تطبيق من تطبيقات الدليل العلمي، بل أكثر منه حجية في الإثبات وذلك بما يتميز به من موضوعية وحياد وكفاءة ، محكم وفق قواعد علمية حسابية قاطعة لا تقبل التأويل يقوي يقينيته، ويساعد القاضي من التقليل من الأخطاء القضائية، والاقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة.

فالفقه الفرنسي يتناول حجية الدليل التقني في المواد الجزائية ضمن مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل الرادارات الأجهزة السينمائية، أجهزة التصوير، أشرطة التسجيل، أجهزة التنصت، وتطبيقا لذلك قضي في فرنسا بخصوص قوة المحررات الصادرة عن الآلات الحديثة في الإثبات بأنه إذا كانت التسجيلات الممغنطة لها قيمة الدلائل يمكن الاطمئنان إليها، ويمكن أن تكون صالحة في الإثبات أمام القضاء الجزائي[2]، وفي حكم آخر قررت محكمة النقض الفرنسية بأنه إذا اطمأنت محكمة الموضوع وفقا لاقتناعها الذاتي والقواعد العامة إلى ما استندت إليه النيابة العامة من قرائن بشأن خطأ سائق سيارة منسوب إليه تجاوز السرعة، وقد ثبت

[1] – سامي جلال فقي حسين، المرجع السابق، ص 237.

[2] Crim 24 avril 1987, Bull. n" 173. Cité par: Francillon (Jacques), les crimes informatiques et d'autres crime dans le domaine de la technologie informatique en France. r.i.d.p, 1993. p.308.

ذلك من خلال جهاز آلي التقط صورة السيارة المتجاوزة للسرعة، ودون أن يكون السائق قد سئل فإنها لا تكون ملزمة بتحديد من استندت إليه من عناصر الواقعة في تبرير اقتناعها[1].

ومما سبق يتبين لنا أن ظهور الدليل التقني قد زاد من دور الإثبات العلمي واستتبعه ذلك تعاظم دور الخبراء في القيام بدور فعال في إبداء خبرتهم الفنية، بالنضر إلى أن الكثير من الجرائم التي ترتكب ستقع على مسائل إلكترونية آية في التعقيد. وبالنظر إلى تطور مجالات الخبرة فإنه سوف تتسع مجالات اللجوء إليها. كذلك فقد توفر التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة علمية قد يصعب إثبات عكسها.

وإذا كان للخبرة التقنية أهمية كبرى في استخلاص الدليل التقني فإن دورها في بحث مصداقيته في مجال المعالجة الآلية للمعلومات تغدو أعظم، فالدليل التقني وبحكم طبيعته العلمية يمثل إخبارا صادقا عن الواقع من منظور علمي ذو كفاءة بيّنة ، إلا أن هذا لا ينفي استبعاده للشك في سلامته من العبث من ناحية و صحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى، ولا شك أن الخبرة تحتل في هذه الحالة دورا مهما في التثبت من سلامة هذا الدليل.

التقنية الحديثة تمكن من العبث بالدليل التقني بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة . أما الثانية وان كانت نسبة الخطأ الفني في الحصول على الدليل التقني نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل التقني لسببين[2]: الخطأ في استخدام الأداة المناسبة في الحصول على الدليل التقني، ويرجع ذلك للخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة أما الثانية تكمن في الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن 100 % ويحدث هذا غالبا بسبب وسائل اختزال المعطيات أو بسبب معالجة المعطيات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها .

[1] Crim 3janvier 1978,bull,n°1,D.c.p.p.1991-1992,p413.Crime.20janvier977,J.C.P.1977,n° 11.

[2] -ممدوح عبد الحميد عبد المطلب، مرجع سابق،ص2253.

فمثلما يخضع الدليل التقني لقواعد معينة تحكم طرق الحصول عليه، فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية من الناحية العلمية، وذلك يرجع للطبيعة الفنية لهذا الدليل، فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه[1]، وسوف نحاول فيما يلي تناول بعض هذه الوسائل من حيث سلامته من العبث، ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالي :

يمكن التأكد من سلامة الدليل التقني من العبث بعدة طرق نذكر منها :

- يلعب علم الكمبيوتر دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون وكينونة الدليل التقني[2]، وهذا العلم يستعان به في كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظري الرقمي من الوسائل المهمة للكشف عن مصداقية الدليل التقني، ومن خلالنا تتم مقارنة الدليل التقني المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا[3].

- حتى في حالة عدم الحصول على النسخة الأصلية للدليل التقني أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي الإمكان التأكد من سلامة الدليل التقني من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات.

- هناك نوع من الأدلة التقنية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل التقني المقصود من حيث عدم حصول تعديل أو تغيير في النظام المعلوماتي.

فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل التقني ومطابقته للواقع .

عادة تتبع جملة من الإجراءات الفنية للحصول على الدليل التقني وقد قدمنا أن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشك في سلامة نتائجها، ولذا فإنه يمكن في هذا

[1] –طارق محمد الجملي، المرجع السابق،ص 26.

[2] – ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص2241.

[3] – نفس المرجع السابق ص 2246-2247.

الشأن اعتماد ما يعرف باختبارات (داو بورت)[1] كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل التقني من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ولذا فإننا سنعرض باختصار للخطوات التي تتبع للتأكد من سلامة هذه الإجراءات من الناحية الفنية[2]، وذلك بإتباع اختبارين رئيسين هما :

* **اختبار السلبيات الزائفة:** ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل التقني، وأنه لا يتم إغفال معطيات مهمة عنه .

* **اختبار الايجابيات الزائفة:** ومفاد ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل التقني لاختبار فني يمكن من التأكد من أن هذه الأداة لا تعرض معطيات إضافية جديدة .

وبذلك يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل التقني وفى ذات الوقت لم تضف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق تلك الآلة مصداقية في التدليل على الواقع.

حيث تدل البحوث المنشورة في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل التقني، وفى المقابل أثبتت تلك الدراسات الأدوات المشكوك في كفاءتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[3].

ومن خلال ما تقدم نخلص إلى أنه يمكن التغلب على مشكلة الشك في مصداقية الدليل التقني من الناحية العلمية من خلال إخضاعه لاختبارات تمكن من التأكد من صحتها، لكن ما موقف القاضي الجزائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم ؟

[1] – ترجع أصول هذا الاختبار (اختبارات داو برت) للحكم الذي أصدرته المحكمة العليا الامريكية في قضية داو بورت ضد ميريل دو للصناعات الدوائية 1993 ، نفس المرجع السابق ، ص 2248.

[2] – نفس المرجع السابق، ص2294 ومابعدها.

[3] طارق محمد الجملي، المرجع السابق، ص 26 .

يخضع الدليل التقني شأنه شأن الدليل الجزائي بشكل عام للمبدأ العام في الإثبات الجزائي وهو حرية القاضي الجزائي في الاقتناع، والقاضي في ظل هذا المبدأ يملك حرية واسعة في تقييم عناصر الإثبات، ووزن الأدلة وتقديرها بالكيفية التي تمكنه من تكوين عقيدته في الدعوى المطروحة عليه، ولا يخضع في ذلك إلا إلى صوت ضميره وما يقتنع به شخصيا، ولا يستشير في ذلك سوى وجدانه، فهو وحده الذي يملي عليه الحكم الذي يصدره والرأي الذي يتوصل إليه.

ولقد تعاظم دور الإثبات العلمي مع بروز الدليل التقني إلى حقل الأدلة الجنائية كأفضل دليل لإثبات الجرائم محل الدراسة إن وجد، مما ألزم القاضي أن يتعامل معه في مقابل نقص الثقافة المعلوماتية من جهة، وشروط السلامة التي يتمتع بها من العبث والخطأ من جهة أخرى فهل من شأن ذلك أن القاضي يسلم ويبني اقتناعه بالدليل التقني على أساس أن أمره محسوم علميا.

حيث يعد مبدأ الاقتناع القضائي أحد أهم المبادئ التي تقوم عليها نظرية الإثبات في المواد الجزائية، وعنه تتفرع معظم القواعد التي تحكم هذا الإثبات[1]، وقد تعددت الآراء فيما يتعلق ببيان مدلوله[2]، وأيا كان التعريفات الموضوعة له إلا أنها تصبو إلى معنى واحد وهي: أن للقاضي أن يستمد من أي دليل تطمئن إليه نفسه، ويسكن إليه وجدانه، دون أي قيد يقيده في ذلك إلا ما تقتضيه العدالة ذاتها من قيود، ويتصل بذلك سلطته في إستبعاد أي دليل لا يقتنع به إذ لا وجود لدليل يفرض عليه أن يستمد منه اقتناعه سواء تلك الأدلة التي طرحت عليه من قبل الخصوم أو النيابة العامة، بل حتى التي يرى بنفسه تقديمها، والحرية هذه التي يتمتع بها القاضي الجزائي في هذا المجال ليست مقررة بهدف توسيع الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجزائية.

[1] محمود نجيب حسني، شرح قانون الإجراءات الجنائية، المرجع السابق، 2241

[2] حيث عرفه د. محمود مصطفى بأنه «التقدير الحر المسبب لعناصر الإثبات في الدعوى وهو البديل عن نظام الأدلة القانونية» وفي رأي د. علي راشد بأنه «تلك الحالة الذهبية والنفسية أو ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة اليقين بحقيقة واقعة أم تحدث تحت بصره بصورة عامة». .

ومبدأ الاقتناع القضائي وفق هذا المعنى يتيح للقاضي حرية واسعة في تقدير القيمة الدامغة للأدلة المقامة أمامه على حسب اقتناعه، بل لعله أهم نتيجة تترتب على هذا المبدأ .

ويعد التشريع الجزائري في طليعة التشريعات التي أكدت هذا المبدأ وذلك من خلال المادة (307) من قانون الإجراءات، و التي تقابلها المادة (353) من قانون الإجراءات الفرنسي حيث تنص على " ... **إن القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت أن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي**". كما أن الاقتناع القضائي كرسته أيضا صراحة المادة (212) من قانون الإجراءات الجزائية الجزائري .

وما تجدر الإشارة إليه هنا أن مبدأ إقتناع القاضي هو عام يسري في كافة أنواع المحاكمات الجزائية بإختلاف التصنيفات للجرائم محل المتابعة الجزائية ، سواء كانت محاكم الجنايات أو أقسام للجنح أو للمخالفات[1].

[1]: وان كان المشرع الجزائري لم يجد ذلك صراحة في المواد المقررة لهذا المبدأ (راجع المواد 307و212 من قانون الإجراءات الجزائية) بخلاف المشرع الفرنسي، فقد صرح ذلك صراحة، حيث خصص المادة (353-1) من قانون الإجراءات لتطبيق المبدأ أمام محكمة الجنايات، كما نصت المادة (427) من ذات القانون على تطبيق هذا المبدأ بالنسبة لمحاكم الجنح، أما المادة (ط 55) من نفس القانون فهي مخصصة بالنسبة لمحاكم المخالفات. وما يقيل بخصوص المشرع الفرنسي يقال بالنسبة للمشرع السوري، حيث نجد هذا الأخير قد أدرج نص المادة (75 – 1) السابقة ضمن الكتاب الثاني تحت عنوان – المحاكمات –، فضلا عن ذلك فإن هذه المادة قد أقرت للقاضي حرية الاستعانة بكافة وسائل الإثبات لتكوين قناعته حول حقيقة الوقائع المرفوعة عنها الدعوى، وأعمتها في ذلك على الجنايات والجنح والمخالفات بصريح العبارة.

و هذا لا يعني أن نطاقه محدد فقط على مرحلة المحاكمة ، بل يمتد كذلك ليشمل مرحلة التحقيق الابتدائي حيث يطبقه قضاة التحقيق[1].

و مما سبق نجد أن مبدأ الاقتناع الشخصي للقاضي الجزائي يعد أساسا في العمل القضائي لإصدر الأحكام الجزائية ، وعليه فإن ظهور الدليل التقني بكل مميزاته يجب أن لا يغير شيئا من هذا المبدأ . ومن ثم فإن الدليل التقني لا يحظى بقوة حاسمة في الإثبات تماشيا مع الأصل. فهو مجرد دليل لا تختلف قيمته و حجته الثبوتية عن بقية الأدلة ، فيصح للقاضي أن يبني قناعته عليه كما يصح أن يطرحه إذا تطرق الشك إليه بخصوصه .

فالدليل التقني بوصفه تطبيقا من تطبيقات الدليل العلمي لا يمكن أن ينازع القاضي في قيمة ما يتمتع به من قوة استدلالية قد استقرت بالنسبة له وتأكدت من الناحية العلمية، فإذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل التقني بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنهما برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا توافرت في الدليل التقني الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية وفقاً للمادة لـ(212) والمادة (307) من قانون الإجراءات الجزائية الجزائري، ولكن يقتصر دور القاضي على الظروف والملابسات التي وجد فيها الدليل فهي من يدخل في نطاق تقديره الذاتي فهي من صميم وظيفته القضائية، بعيث يكون في مقدوره أن يطرح مثل هذا الدليل – رغم

[1]: فقضاء التحقيق يملك حرية التصرف في الدعوى وتحديد مصيرها حسب تقديره غير أن مهمة هذا الأخير لا تعدو أن تكون مقصورة فقط على تقدير مدى كفاية الأدلة أو عدم كفايتها للاتهام، وهي بذلك تختلف عن وظيفة قضاة الحكم الذين عليهم تقدير الأدلة القائمة من حيث كفايتها أو عدم كفايتها للحكم بالإدانة. وإذا صح التعبير يمكن القول بأن الأولى تسعى إلى ترجيح الظن بينما الثانية تسمى إلى توكيد اليقين، وشتان بين الاثنان. يترتب على ذلك نتيجة هامة وهي إن الشك في مرحلة الاتهام يفسر ضد مصلحة المتهم، مما يستوجب إحالة الدعوى إلى المحكمة المختصة، بخلاف الشك في مرحلة الحكم فهو كما هو معلوم – يفسر لمصلحة المتهم.

وبالتالي يظهر لنا أن نطاق تطبيق مبدأ حرية القاضي في مرحلة التحقيق محدود، إذ يكاد يقتصر على مجرد الموازنة بين الأدلة المثبتة للتهمة وتلك النافية لها، لترجيح مدى كفايتها أو عدم كفايتها للاتهام. بينما في المقابل نجد أن نطاق تطبيق المبدأ المذكور أمام قضاء الحكم يتسع الى حد كبير باعتباره يتصل بوقائع كل دعوى على حدة بحس نظر: عبد الله بن صالح بن الرشيد الربيش، المرجع السابق، ص 80.

قطيعته من الناحية العلمية – إذا تبين بأنه لا يتفق مع ظروف الواقعة وملابستها، حيث تولد الشك لدى القاضي، ومن تم يقضي في إطار تفسير الشك لصالح المتهم .

ذلك أن مجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أم بالبراءة، دون بحث الظروف والملابسات، فالدليل العلمي ليس آلية معدة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة[1]

و عليه فإنه يجب الإبقاء على السلطة التقديرية للقاضي التقديرية في تقديره للأدلة التقنية لضمان تنقيتها من الشوائب العلمية لأن الحقيقة العلمية لابد ان تتشكل وفق حقيقة قضائية فهو المسيطر على هذه الحقيقة لأنه من خلال سلطته التقديرية يستطيع تفعيل الشك لصالح المتهم، بأن يستبعد الأدلة التي يتم الحصول عليها بطرق غير مشروعة[2].

ثانيا : مصداقية الدليل التقني بوصفه يعبر عن الحقيقة التي تهدف إليها الدعوى العمومية

إن تأثير التطور العلمي لا يقف عند مضمون الدليل بل يجب أن يمتد إلى الإجراءات المعمول بها للحصول عليه ، لذلك لابد أن تكون تلك الإجراءات متطورة تماشيا مع طبيعة الدليل و ان تكون مشروعة للحفاظ على شرعية الدليل المتولد منها ، وأن تكون مطروحة أمام القاضي في الجلسة ضمن أوراق الدعوى لإيتاحتها للخصوم بشكل يمكن من مناقشته والرد عليه، كما يجب أن تكون يقينية .

فالقانون و إن ترك للقاضي الجزائي الحرية في أن يستمد اقتناعه من أي دليل وبأية وسيلة يراها موصلة إلى الحقيقة[3] ، إلا أن هذه الحرية لا تعني أن القاضي الجزائي يستطيع بناء عقيدته على أي دليل يحصل عليه مهما كان مصدره ووسيلة البحث عنه، فهو ملزم بضرورة أن يكون الدليل المستند عليه في الحكم مقبولا في الدعوى بمراعاة قاعدة مشروعية الحصول عليه وفق النظام الإجرائي المعمول به ، بل إن مخالفة هذا الشرط قد يهدر قيمة الدليل و يقضى في النهاية الى

[1]- جميل عبد الباقي الصفير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص 22.

[2]- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إحلال نظرية الإثبات الجنائي، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، أكاديمية شرطة دبي، الفترة من 26 إلى 48-4-2003، دبي ، ص15.

[3]- موسى مسعود رحومة عبد الله، حرية القاضي الجنائي في تكوين عقيدته، المرجع السابق، ص86.

بطلان، فالخصومة الجزائية قائمة على ضمان حرية المتهم لا على سلطة الدولة في العقاب، وبالتالي يتعين على القاضي ألا يثبت توافر هذه السلطة تجاه المتهم إلا من خلال دليل يتم الحصول عليه من إجراءات مشروعة احترمت فيها الحريات و الضمانات المعمول به قانونا[1]، و لهذا لا يجوز الإعتماد على دليل يتصف بالبطلان و لابد أن يكون مطابقاً للنصوص المقررة لضمانات الحرية الفردية وكذا القواعد العامة للإجراءات الجزائية والمبادئ القانونية العامة كالقواعد والمبادئ التي توجب احترام قيم العدالة وأخلاقياتها والنزاهة في الحصول على الأدلة واحترام حقوق الدفاع .

و الأمر نفسه ينطبق على الدليل التقني الذي يشترط فيه هو الآخر أن يكون مشروعا في ذاته وغير مخالف للقواعد القانونية وللمبادئ القانونية العامة.

و متى تأكد القاضي من الأدلة أنها مقبولة قانونا، حينئذ يستكمل عمله بمناقشته و هذا بحضور الخصوم، فمن القواعد الأساسية في الإجراءات الجزائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعرف"بوضعية الدليل" بما يعني أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الإطلاع عليه ومناقشته وذلك احتراماً لحقوق الدفاع .

وبمقتضى هذا فإن القاضي لا يجوز له أن يبني حكمه على دليل لا صلة له في الأوراق، فالدليل الذي لا يتحقق فيه هذا الشرط يكون منعدما في نظر القانون وذلك استناداً إلى قاعدة وجوب تدوين كافة الإجراءات الاستدلال والتحقيق. وغاية ذلك حتى يكون الخصوم على بينة مما يقدم ضدهم من أدلة، وأن تتاح لهم إمكانية مناقشتها والرد عليها[2]

و هو ما كرسته الفقرة الثانية (2) من المادّة (212) من قانون الإجراءات الجزائية الجزائري إذا تنص " **ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه**" و التي تقابلها المادة (427) في فقرتها الثانية من

[1]- فتحي محمد أنور عزت، المرجع السابق، ص 44

[2]- إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية – دراسة قانونية نفسية – الطبعة الأولى رسالة دكتوراه،عالم الكتاب، القاهرة،1980، ص 646.

قانون الإجراءات الجزائية الفرنسي التي نصت على أنه "**لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الخصوم**"[1].

و بمقتضى هذا فإن القاضي في تقديره للأدلة سواء كانت تقليدية أو مستخرجة من الوسائل الإلكترونية لا يكتفي بالمحاضر التحقيق و ما دوّن فيها ، بل عليه إعادة الإستماع للشهود الذين قد سبق سماعهم شهاداتهم أثناء التحقيق الابتدائي، فضلا عن اعتراف المتهم نفسه وكذا تقارير الخبراء وذلك بمناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة ، ويطرح جميع الأدلة الأخرى للمناقشة الشفوية، فلا يكون بين الدليل والقاضي وسيط، والغرض من ذلك أن يتاح لكل طرف في الدعوى أن يواجه خصمه بما يحوزه من أدلة ضده ، مما يفيد القاضي في تكوين قناعته من نتيجة هذه المناقشات التي تجري أمامه في الجلسة[2].

فضلا عن ذلك فإن هذا من شأنه أن يحقق رقابة فعالة على جدية الأدلة التي تكون قد حصلت في مرحلة التحقيق فتعرض مجدداً، وهو ما يتيح في المقابل مراقبة التقدير الذي كانت سلطة التحقيق قد خلصت إليه.

و هو ما عبرت عنه المحكمة العليا الجزائرية في قضاء لها بقولها "**لا يمكن لقضاة الموضوع أن يؤسسوا قرارهم إلا على الأدلة المقدمة لهم أثناء المرافعات والتي تتم مناقشتها حضورياً**"[3]

ولا يختلف الأمر بالنسبة للدّليل التقني بوصفه دليل من أدلّة الإثبات، مهما كانت الحالة التي يكون عليها سواء كان على شكل مخرجات ورقية أو إلكترونية أو معروضة بواسطة الكمبيوتر على الشاشة الخاصة به. كل أولئك سيكون محلاً للمناقشة عند الأخذ بها كأدّلة إثبات أمام المحكمة.

[1] -Art 427 alinéa 2 du C.P.P.F dispose que : «Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui».

[2]– فاضل زيدان محمد، المرجع السابق، ص 259 .

[3]– قرار نقض جنائي صادر بتاريخ 21 جانفي 1982 ، الاجتهاد القضائي، ص 66 ، غير منشور اطلع عليه لدى تقنين الإجراءات الجزائية، تحت إشراف د. أحسن بوسقيعة، ص 73 .

و عليه فإن القاضي الجزائي له الحرية الكاملة في أن يستمد اقتناعه من الدليل التقني طالما اطمئن إليه وكان متضمنا في أوراق ملف الدعوى ، وعرض عليه أثناء المرافعات وناقشها أطراف الدعوى ، فلا يجوز للقاضي أن يبني اقتناعه على هذه المعلومات الشخصية، وذلك حماية للخصوم من أي تأثير خاطئ على القاضي، يكون ناتجاً عما وصله من معلومات خارج إطار الدعوى، وإلا يكون قد جمع في شخصه صفتين متعارضتين صفة الشاهد وصفة القاضي، وهذا ما لا يجيزه القانون ويرتب عليه بطلان الحكم. لأن الخصوم ليس بإمكانهم مناقشة شهادته، والرد عليها بحرية مما يشكل مساساً بحق الدفاع.بل باعتماده على معلوماته الشخصية يكون عرضة للتهمة، وسوء الظن به وهو الشيء الذي يجب أن ينزه عنه القضاء عموماً.[1]

وإن كان ذلك كذلك، فإن المعلومات العامة المستقاة من خبرة القاضي بالشؤون العامة المفروض إلمام الكافة بها لا تعد من قبيل المعلومات الشخصية المحذورة على القاضي أن يبني حكمه عليها، ومن قبيل ذلك الثقافة المعلوماتية فيما يتعلق بأساسيات الكمبيوتر .

لكن يلاحظ أنه وإن كان يجب أن يصدر الحكم من عقيدة للقاضي يستقيها هو مما يجريه من التحقيقات مستقلاً في تحصيل هذه العقيدة بنفسه لا يشاركه فيها غيره إلا أن ذلك لا يعني حرمان القاضي بصفة مطت من الأخذ برأي الغير، لم في يجوز له ذلك متى كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متولدا من عقيدته هو وليس من تقرير الخبير.

و في نطاق الأدلة التقنية يتطلب من القاضي الجزائي أن يكون مؤهلا التأهيل الفني والتقني على كيفية التعامل مع الدليل التقني، لأنه سيكون محلاً للمناقشة الحضورية بين الأطراف عند الأخذ بها كأدلة إثبات في الدعوى الجزائية، فهذا التأهيل يضمن نجاح مهمة القاضي الذي تناط به مهمة المناقشة العلمية لهذه الأدلة والهيمنة على الدعوى الجزائية ولن يتحقق ذلك إلا بعقد

[1]– موسى مسعود رحومة عبد الله، حرية القاضي الجنائي في تكوين عقيدته، المريع السابق، ص 114

دورات تدريبية مكثفة لهؤلاء القضاة على كافة مستوياتهم ودرجاتهم في تقنية المعلومات، وإذا كان قد تم وضع حذا المفهوم وتطويره من قبل المجلس الأدبي بشأن جرائم تقنية المعلومات، وصدقت عليه شبكة لشبونة للمجلس الأوروبي في سبتمبر 2009[1]، فإنه برأينا لا حرج لو كان هناك دور عربي يعمل على مساعدة مؤسسات التدريب القضائي لوضع برامج تدريب على الأدلة التقنية للقضاة، وإدماج هذا النوع من التدريب ضمن أساس التدريب الأولي والتدريب أثناء الخدمة .

ثالثا: يقينية الأدلة التقنية

لما كان هدف التشريعات الإجرائية هو إصابة القاضي الحقيقة الواقعية في حكمه، لذا وجب على القاضي قبل تحريره لحكمه أن يصل إلى الحقيقة مؤكدة بأن تكون لديه يقينا مؤكدا بحدوثها، لا بمجرد الظن والاحتمال، إذ أن الشك يفسر لصالح المتهم بحسبان أن الأصل في الإنسان البراءة .

وشرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستخلص منها هذا اليقين أدلة تقليدية أو مستحدثة كالدليل التقني.

و يقصد باليقين **لغة** : بأنه **العلم وإزاحة الشك، وتحقيق الأمر، وقد أيقن يوقن إيقانا فهو موقن، أو يقن ييقن يقنا، فهو يقن، واليقين نقيض الشك، والعلم نقيض الجهل**[2].

أما اصطلاحا : فاليقين هو **كل معرفة لا تقبل الشك، ومنه حدسي كاليقين ببعض الأوليات أو استدلالي غير مباشر يتنبأ إليه المرء بعد البرهنة، ومنه ذاتي يسلم به المرء ولا يستطيع نقله إلى غيره، أو موضوعي يفرض نفسه على العقول كاليقين العلمي، وقد يسمى التسليم بأمر ظاهر أو راجح يقينا اقتناعا، أو شبه يقين .**

[1] أنظر في ذلك: الفريق العامل للأصحاب المصلحة المتعددين في إطار المشروع المعني بالجريمة المعلوماتية ومن قبل شبكة لشبونة، التدريب على الجريمة المعلوماتية للقضاة وأعضاء النيابة العامة، ورقة عمل معدة لمؤسسات التدريب القضائي التابعة للمجلس القضائي، قسم مجتمع المعلومات والعمل على مكافحة الجريمة، المديرية العامة لحقوق الإنسان والشؤون القانونية، المجلس الأوروبي، سترانسبورغ، فرنسا، 8 أكتوبر2009.

[2] ابن منظور، لسان العرب، المرجع السابق، ص 4934

والعلم اليقيني هو الذي ينكشف فيه المعلوم انكشاف لا يبقى معه ريب ولا يقاربه إمكان الغلط أو الوهم[1].

أما **اليقين في الاصطلاح القانوني فقد عرفه البعض من الفقهاء[2] على أنه «عبارة عن اقتناع مستمد إلى حجج ثابتة وقطعية»** أو أنه عبارة عن «**حالة ذهنية أو عقلانية تؤكد وجود الحقيقة»[3]، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة ثقة عالية من التوكيد** . "

ومتى ما تكامل اليقين بأن وصل القاضي إلى درجة القطع ينشأ ما يسمى بالاقتناع اليقيني وهو أساس الحقيقة القضائية التي ينشدها القاضي في حكمه .

في الوقت الذي يعود فيه لقاضي الموضوع تقدير الأدلة وموازنتها وفقاً لما يمليه عليه وجدانه، ودون أن يخضع في ذلك لرقابة لمحكمة العليا، إلا أنه مع ذلك مقيد في ذلك بضرورة تأسيس قناعته على الجزم واليقين لا على الظن والترجيح وذلك لاستبعاد قرينة البراءة اللاصقة بكل إنسان استنادا إلى أن الأصل في الإنسان البراءة .

وإذا كانت هذه هي الأحكام العامة التي تحكم اليقين في الأدلة الجزائية في الجزائر وفي الدول ذات الصياغة اللاتينية، فإن الأمر لا يختلف بالنسبة للدليل التقني، إذ يشترط أن يكون هو الآخر يقيني حتى يمكن الحكم بالإدانة .

ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من أدلة تقنية، وهكذا يستطيع القاضي من خلال ذلك وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة جريمة من جرائم الاعتداء على نظم المعالجة الآلية إلى شخص معين من عدمه .

---

[1] إبراهيم مدكور، المعجم الفلسفي، دار الكتاب، القاهرة، 1983 ، ص216.

[2] موسى مسعود رحومة عبد الله، حرية القاضي الجنائي في تكوين عقيدته، المرجع السابق، ص131.

[3] RACHED (a-a) de l’intime conviction du juge , thèse paris ;1942, p3.

فكأن اقتناع القاضي يصل إلى الجزم واليقين عن طريق نوعين من المعرفة: أولهما المعرفة الحسية التي تدركها الحواس، والآخر المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها.

إلا أنه في نطاق الجزم بوقوع جرائم الاعتداء على نظم المعلوماتية ونسبتها إلى المتهم يستدعي نوعا آخر من المعرفة ألا وهي المعرفة العلمية في مجال المعلوماتية[1]، وهو ما يلقي المزيد من الأهمية على تدريب القضاة، وتكمن خطورة هذه الأخيرة في كون الجهل بها قد يؤدي في بعض الأحيان إلى التشكيك في قيمة الدليل التقني وما يستتبعه ذلك من القضاء بالبراءة، على اعتبار أن الشك يجب أن يستفيد منه المتهم في مرحلة المحاكمة، بل حتى لإعمال هذه الأخيرة يلزم أن يكون هناك ما يرقى لمستوى التشكيك في الدليل وهو ما قد لا يتوافر لدى القاضي .

تحدثنا فيما سبق عن كيفية الوصول إلى درجة اليقين والقطع وتبين كيف أن القاضي يصل إليها إلا من خلال ثلاث أنواع من المعارف حسية عقلية ومعلوماتية، حتى يبنى عليها حكمه بالإدانة في نطاق جرائم الاعتداء على نظم المعلوماتية، وذلك لاستبعاد قرينة البراءة اللاصقة بكل إنسان استنادا إلى أن الأصل في الإنسان البراءة .

أما إذا لم تقدر الأدلة التقنية على إحداث القطع أو اليقين بوقوع الجريمة ونسبتها إلى المتهم يلزم حينئذ استمرار حالة البراءة التي يكفي لتأكيد وجودها مجرد الشك في ثبوت تلك الإدانة استنادا إلى القاعدة التي تقول بأن الشك يفسر في مصلحة المتهم[2].

ويبنى على ذلك، أن حكم الإدانة يكون معيبا إذا ما تأسس على ترجيح ثبوت التهمة أو إذا كان قد بني على مجرد افتراضات أو استنتاجات لا يؤيدها الواقع .

[1] عائشة بن قارة مصطفى، المرجع السابق، ص181.

[2] د. هلالي عبد الله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 87.

المبحث الثاني : الإتجاه نحو تنظيم الإطار التشريعي للأدلة التقنية كرهان مستقبلي

حتى يحقق دليل الإثبات هدفه في إثبات أركان الجرائم محل الدراسة حسبما يحددها القانون وإيجاد العلاقة بين تلك الأركان والشخص المتهم بتنفيذها، لا بد من جمع عناصر التحقيق والدعوى وتقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو أدلة ترجح معها إدانة المتهم قدمته إلى المحكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي لإدانة المتهم وإلا قضي ببراءته.

إلا لأنه نظرا للتطور التقني الذي لحق نظم المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل التقني فسيقود دون شك إلى تغيير كبير إن لم يكن كليا في المفاهيم السائدة حول إجراءات الحصول إليه، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم لمنهج بعض الإجراءات التقليدية كالتفتيش والضبط ككل في قانون الإجراءات الجزائية على ضوء ما أسفرت عنه تطورات العلم والتقنية لا سيما في مجال ثورة المعلومات، فضلا عن استحداث نوع من القواعد الإجرائية تتلاءم وطبيعة البيئة التقنية، فتطوير الإثبات وطرقه أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الإجرام وذلك لكي نمنع ما يمكن أن يقال من "صعوبة هذا الإثبات قد يؤدي إلى عدم التجريم".و هذا ما سنتناوله وفق :

المطلب الأول : مدى كفاية القواعد الإجرائيية العامة لإستخلاص الدليل التقني

المطلب الثاني: تكريس قواعد إجرائية و تنظيمية خاصة لإستخلاص الدليل التقني

المطلب الأول : مدى كفاية القواعد الإجرائية العامة لإستخلاص الدليل التقني

مما لا شك فيه أن المشرع لم يجز استخلاص الدليل من غير ضوابط تحكم ذلك، بل نظم ذلك عن طريق قواعد إجرائية معينة، وأهم هذه القواعد تلك المتعلقة بالتفتيش والضبط والتسرب، ومما لا شك فيه أن هذه القواعد عامة النطاق تنظم استخلاص الدليل في جميع الجرائم تقليدية كانت أو مستحدثة، إلا أنها في الثانية قد تكون في حاجة إلى تطوير لكي تتناسب مع طبيعتها

الخاصة وطبيعة الدليل الذي يصلح لإثباتها، وهذا ما سنلاحظه مع جرائم الاعتداء على نظم المعلومات فيما يلي:

الفرع الأول: التفتيش لضبط الدليل التقني:

التفتيش[1] هو عبارة عن إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة ونسبتها إلى المتهم، تحقق وقوعها في محل يتمتع بحرمة وذلك وفقا للضمانات والقيود القانونية المقررة . فهو إجراء يهدف لضبط أشياء مادية قد تساعد في إثبات وقوع الجريمة وإسنادها إلى المتهم المنسوب إليه ارتكابها، وعلى ذلك فتفتيش نظام المعلومات يعد من أخطر المراحل حال اتخاذ الإجراءات ضد مرتكب جرائم الاعتداء عليه ، لكون محل التفتيش هو محل جدل فقهي ، فهو لا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي

فمن المعروف لدينا الآن أن نظم المعلوماتية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها بشبكات اتصال بعدية على المستوى المحلي أو الدولي.

فمحل التفتيش قد يرد على المكونات المادية لنظام معلوماتي وأوعيته المختلفة بحثا عن شيء يتصل بالجرائم المرتبطة به وتفيد في كشف الحقيقة عنها وعن مرتكبيها، وهذه لا خلاف يذكر حول خضوعها للتفتيش ، وذلك تبعا لطبيعة المكان الموجودة فيه سواء من الأماكن العامة، أو الأماكن الخاصة، فلصفة المكان أهمية في مجال التفتيش، فإذا كانت خاصة كمسكن[2] المتهم أو أحد ملحقاته كانت لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا في أغلب التشريعات الجزائية ، حيث نصت المادة (64) من

[1]- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج2، د.م.ج، الجزائر، 1999، ص 40، عبد الله أوهايبيه، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومه للنشر والتوزيع، الجزائر، 2008، ص 266.

[2]- ويقصد بالمسكن كل مكان يرتبط بالحياة الخاصة لصاحبه، ويقتصر الانتفاع به عليه، فهو كل مكان يقيم فيه الشخص بصفة دائمة أو مؤقتة، وكذلك توابع ذلك المكان كالحديقة والحظيرة والمخزن، وكذلك عيادة الطبيب ومكتب المحامي والسيارة الخاصة، بل وحتى المحل العام تصبح له حصانة المسكن عند إغلاقه ذلك أن العبرة في تحديد المكان الخاص هي بسماح الشخص للغير بدخول منزله دون تمييز أو لا. أنظر: د. أحمد شوقي الشلقاني، المرجع السابق، ص 242.

قانون الإجراءات الجزائية على أنه "**لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه.**"

وتطبق فضلا عن ذلك أحكام المواد من 44 إلى 47 من هذا القانون"

إلا أنه وإذا كان المشرع الجزائري قد أورد القاعدة في المادة (64) من ذلك القانون، رجع وأورد عليها استثناء بموجب الفقرة الثالثة (3) من نفس المادة[1]، حيث استثنى المشرع تطبيق هذه الضمانات على طائفة من الجرائم محيلا في ذلك إلى أحكام المادة (47) في فقرتها الثالثة (3) التي تنص "**وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص**".

والملاحظ أن المشرع في هذه الحالة قد غلب مصلحة تحقيق المصلحة العامة على الحرية الفردية ، و مرد ذلك إلى اعتبارين:

- ذاتية جرائم الاعتداء على نظم المعلومات فهي جريمة قابلة للاختفاء بسرعة.
- افتراض كون الدليل التقني هو الدليل الوحيد في الدعوى العمومية، وارتكاز عملية الإثبات على وجوده.

وفي المقابل لم يجز المشرع إجراء تفتيش منزل المتهم في مثل هذه الظروف بدون قيد بل أباحه في حالة واحدة وهي حالة صدور إذن من وكيل الجمهورية المختص.

[1]- جاء في الفقرة الثالثة من المادة (64) من قانون الإجراءات الجزائية: "غير أنه عندما يتعلق الأمر بتحقيق في إحدى الجرائم المذكورة في المادة 47 (الفقرة 3) من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر".

أما إذا كانت المكونات المادية للنظام متواجدة في أماكن عامة كمحلات بيع وصيانة الحاسبات الآلية، وبحوزة شخص كما لو كان عامل صيانة فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس القيود والضمانات المنصوص عليها في هذه الحالة.

قد يرد التفتيش وما في حكمه على الجانب غير المادي لنظام المعلومات ، المتمثل في المعلومات المعالجة إلكترونيا، ولعل الصورة المعتادة والمثال العلمي الذي يمكن تقريره هنا هو فحص البرمجيات الذي يعد من الوسائل الرئيسية في الكشف عن أكثر جرائم الاعتداء على نظم المعالجة الآلية ضراوة مثل جرائم الدخول غير المشروع إلى نظم الغير، فوجود برمجيات غير مصنفة تعمل في بيئة الاختراق أو تساعد عليه كما هو الشأن في برمجيات المسح للكشف عن الأبواب المفتوحة scan ports prog يمكن أن يشكل منطقة استفهام ودلالة كافية أيضا على ارتكاب الشخص لجريمة دخول غير مشروع لنظام المعالجة الآلية إذا استتبع ذلك اعترافا شفويا بارتكاب الجريمة وعليه فإن صلاحية مكونات النظام المعلوماتي غير المادية كمحل يرد عليه التفتيش ، ذلك أن المشرع الجزائري يميل إلى هذا الاتجاه، حيث أنه استجاب للتغييرات التقنية فأجاز تفتيش المعلوماتية وذلك بموجب المادة (5) من القانون رقم (09-04) لسنة 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أجازت هذه المادة للسلطات القضائية المختصة وكذا لضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة (4) من هذا القانون ومن بين هذه الحالات: توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وللوقاية من الجرائم الماسة بأمن الدولة، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين معلوماتية.

وإلى جانب المشرع الجزائري نجد كذلك المشرع الفرنسي الذي قدر هذه التغييرات إذ قام بتعديل نصوص التفتيش، حيث قام بإضافة عبارة "المعطيات المعلوماتية" في المادة (94) من قانون

الإجراءات الجزائية وذلك بموجب المادة (42)[1] من القانون رقم (545-2004) المؤرخ في 21 جوان 2004 المتعلق بالثقة في الاقتصاد الرقمي لتصبح المادة على النحو التالي "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة"[2].

وفي هذا الصدد صرحت الاتفاقية الأوروبية في شأن جرائم تقنية المعلومات بحق الدول الأعضاء في تفتيش النظم في إطار الإجراءات الجزائية، وذلك من خلال الفقرة الأولى (1) من المادة (19) من القسم الرابع حيث نصت على "أن لكل طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى:

- نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة فيه.
- الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزنة في إقليمها[3].

ولكن، ماذا لو كان نظام المعالجة الآلية مزودا بنظام حماية يمنع من ولوجه دون تدخل القائم على هذه المنظومة ومساعدته؟ فهل يا ترى يجوز إجبار المتهم مثلا على تزويد السلطات المختصة بالتحقيق بمفاتيح المرور إلى نظام المعالجة الآلية؟ أو بالأحرى هل يمكن إكراهه على الإفصاح عن كلمة السر وما في حكمها من أجل تسهيل الولوج إلى البيئة التقنية؟

هنا تباينت الآراء بصدد هذه المسألة، فثمة رأي يرفض إجبار المتهم على تقديم المعلومات اللازمة لتسهيل ولوج النظام المعلوماتي، والحجة التي يستند إليها هذا الرأي تتجسد في قاعدة معروفة ومستقرة أن المتهم لا يجوز إجباره على الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته، إذ من حقه الاعتصام بالصمت دون أن يفسر ذلك الصمت ضد مصلحته.

[1]- art 42 du L.C.E.N dispose que : « a l' article 94 du code de procédure pénale, après les mots : « des objets », sont insérés les mots : « ou des données informatiques ».
[2]- art 94 du C.P.P.F dispose que : « les perquisitions sont effectuées dans tous les lieux ou peuvent se trouver des objets ou des données dont la découverte serait utile a la manifestation de vérité ».
[3]- art 19 alinéa 1 du C.C.C disponible en lingne a l' adresse suivante : http://convention.coe.int/treaty/en/treaties/html/185.htm.

وهذا الاتجاه اعتنقته بعض التشريعات الحديثة، ومنها القانون الياباني الذي يحظر على الأجهزة المختصة إكراه مالك نظام المعالجة الآلية على الإفصاح عن كلمة المرور أو السر password، والنهج ذاته كان قد تبناه مشروع قانون الإجراءات الجزائية البولندي.

وفي المقابل، ذهب رأي آخر إلى القول بأنه، وإن كان لا يجوز إجبار الشخص على الإدلاء بأقواله ضد نفيه، بيد أن ذلك لا ينبغي أن يكون حائلا دون إجباره على تقديم معلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة، متى كانت هذه المعلومات بحوزته، قياسا على إجبار الشخص على تسليم مفتاح الخزنة الذي بحوزته[1].

وقد رد أنصار الرأي الأول[2] على ذلك بالقول –ونحن نؤيده في ذلك– أن قياس المعلومة (المتمثلة في كلمة السر وما في حكمها) هي أمر معنوي بخلاف المفتاح الذي هو شيء مادي محسوس قابل للتسليم، هذا من ناحية، ومن ناحية أخرى فإن هذا الرأي الأخير لا يتفق مع الأصول المستقرة في الإثبات الجزائي، ويتنافى مع مقتضيات حق الدفاع أمام القضاء الجزائي، ومن ناحية ثالثة، وحتى على فرض التسليم بجواز إكراه المتهم أو المشتبه به على تقديم مفاتيح الشفرة التي تمكن من ولوج النظام المعلوماتي، فإن الأمر تكتنفه صعوبات عملية لا يمكن التغلب عليها، لعل أبرزها أن المتهم يستطيع التذرع بنسيان المعلومة أو عدم إمكان تذكرها أو ما شابه ذلك.

وهذا يعني ببساطة أن الرأي الأول أدعى إلى القبول، وللاستدلال على ذلك أكثر ما يستخلص ضمنا من نص المادة (100) من قانون الإجراءات الجزائية الجزائري كما يلي "**يتحقق قاضي التحقيق حين مثول المتهم لديه لأول مرة من هويته ويحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه وينبهه بأنه حر في عدم الإدلاء بأي قرار...**".

[1] – عطية عثمان محمد بوحويش، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة ماجستير، مقدمة إلى أكاديمية الدراسات العليا، فرع بنغازي، 2009، ص 70. مشار إليه لدى: موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المرجع السابق، ص 9.

[2] – موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المرجع السابق، ص 9.

وعلى خلاف ذلك يجوز إجبار الغير على تقديم المعلومة التي من شأنها تيسير الدخول إلى المنظومة كمقدم الخدمة مثلا، بتقديم بعض معطيات المرور للتمكن من تحديد المصدر أو مكان الوصول للاتصالات، وهذا ما نصت عليه المادة (10) و(11) من القانون رقم (09-04) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لأن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع خلافا للوضع بالنسبة للمتهم.

إلا أن هناك مسألة خطيرة متعلقة بالتفتيش عن بعد وذلك نتيجة لطبيعة تكنولوجيا الإتصالات التي تسمح بتوزيع المعلومات المحتوية لأدلة عبر الشبكات في أماكن بعيدة عن الموقع المادي للتفتيش، تلك المواقع تدخل في إختصاص قضائي آخر أو في بلد آخر فهل التفتيش يمتد اليها مع انها خارج الإختصاص القضائي للحاجة الإجرائية ام انه يتوقف ؟ اثيرت هذه المشكلة العملية فقهيا ، و وجدت بعض التشريعات حلا لهذه المشكلة كما في التشريع الجزائري، حيث نصت الفقرة الثانية (2) من المادة (5) من القانون رقم (09-04) لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه "**في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة[1]، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك...**".

و في نفس الإتجاه نجد أن المشرع الفرنسي حسم هذه المسألة أيضا، وذلك بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون رقم (239-2003) بشأن الأمن الداخلي الصادر في 18 مارس سنة 2003، حيث أضاف المادة (57-1) من قانون الإجراءات الجزائية وذلك بموجب المادة (17-1) منه والتي أجازت لرجال الضبط القضائي الدخول من الجهاز الرئيسي على المعلومات التي تهم عملية البحث والتحري، فتنص المادة (17-1) منه على أنه "**يجوز**

[1] – أي حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

لضباط الشرطة القضائية أو تحت مسؤولياتهم أعوان الشرطة القضائية، وفي إطار التفتيش المنصوص عليه، الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر بما أن هذه المعطيات يتم الدخول إليها أو تكون متاحة انطلاقا من النظام الرئيسي".

وتسمح الاتفاقية الأوروبية لجرائم المعلوماتية لعام 2001 للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش، فتنص الفقرة الثانية (2) من المادة (19) من القسم الرابع على أنه من حق السلطة القائمة بتفتيش الكمبيوتر المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلي محل التفتيش[1].

كما قد تكون المعلومات غير المشروعة جرى تخزينها في نظام معالجة آلية خارج إقليم الدولة من أجل إخفاء الدليل و إعاقة الوصول اليه لإعاقة سير العدالة ، و نتيجة لذلك أجاز المشرع الجزائري بتفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، حيث أجازت الفقرة (3) من المادة (5) من القانون المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لسنة 2009 "**الحصول على المعطيات المبحوث عنها والمخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل.**" ، و هو نفس الأمر بالنسبة للمشرع الفرنسي الذي أجاز بموجب الفقرة الثانية (2) من المادة (57-1) من قانون الإجراءات الجزائية المضافة

- art 19 alinéa 2 du C.C.C, disponible en lingne à l'adresse suivante : http://vonvention.coe.int/treaty/en/treaties/html/185.htm.

بموجب المادة (17) الفقرة (2) من قانون الأمن الداخلي رقم (239-2003) لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم فنصت **"إذا تبين مسبقا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليمي الوطني، وأنه يمكن الدخول إليها أو أنها متاحة انطلاقا من النظام الرئيسي، فإنه يمكن الحصول عليها من طرف ضابط الشرطة القضائية مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية.**[1]"

كما نجد أن المجلس الأوروبي أصدر المجلس توصيات تجيز بإمتداد التفتيش للانظمة المعلوماتية ، ولو كانت تقع خارج إقليم الدولة، فتنص التوصية رقم (13) لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات على أنه: **"لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال التفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط المعطيات المتواجدة فيها، ما دام أنه من الضروري التدخل الفوري للقيام بذلك".**

كما أشارت المادة (32) من إتفاقية الإجرام المعلوماتي "الأوروبية لعام " 2001، بجواز و إمكانية الدخول لأجل التفتيش و ضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في **حالتين: إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، والثانية إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش**[2].

و من منطلق أن التفتيش وسيلة إجرائية يهدف منها الحصول على دليل مادي يساعد لإثبات وقوع الجريمة مع إسنادها للمتهم المنسوب إليه ارتكابها ، فإنه يقتضي للقيام به لابد من

[1]- art 17-1/2 du L.S.I.F dispose que : « s' il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l' officier de police judiciaire, sous réserve des conditions d' accès prévues par les engagements internationaux en vigueur… ».

[2]- art 32 du C.C.C dispose que : « une partie peut, sans l' autorisation d' une autre partie : a accéder à des données informatiques stockées accessible… ».

وقوع الجريمة بصورة الجناية أو الجنحة فالمخالفات مستبعدة لعدم تواجد الخطورة الإجرامية ، هذا بالإضافة لوقوعها تامة مكتملة [1]، ضف الى ذلك إستخراج جميع الأمارات الكافية لترجيح نسبة جريمة من جرائم الاعتداء على نظم المعلوماتية إلى شخص معين سواء بوصفه فاعلا أو شريكا، كما لو كان الحاسوب المحددة هويته (IP) الذي تم بواسطته ارتكاب جريمة الدخول غير المصرح به هو حاسوب يمتلكه شخص محدد بعينه ، هنا نقول أن التفتيش يسبقه تحريات جدية ، إذ لا يكفي لحث السلطة التحقيقية لإصدار أمرها أو إذنها أو قرارها بالتفتيش مجرد وقوع جريمة من جرائم الاعتداء على نظم المعلوماتية واتهام شخص معين بارتكابها، بل يجب أن تتوافر لديها أسباب كافية بوجد لدى الشخص المراد تفتيشه أدوات استخدمت في الجريمة أو أشياء متحصلة منها، منها مثلا وجود مستندات إلكترونية أو دعامات تفيد في نسبة الفعل لصاحبها .

والتفتيش في مجال دراستنا قائم على محل يودع و يحتفظ فيه الشخص المعلومات السرية الخاصة به ، وهو محل له حرمة، ونتيجة لذلك نجد أن المشرع الإجرائي الجزائري كغيره من التشريعات ومن قبيل ذلك التشريع الفرنسي ، قد حرص على كفالة الحقوق والحريات وتضمنها والتي منها الحق في الخصوصية و حرمة الحياة الخاصة ، لذلك جعل الأمر بيد سلطة محددة وفق اجراءات محددة ، والتي حددها بقاضي التحقيق باعتباره صاحب السلطة الأصلية ، إلا أنه يمكن للضبطي القضائية القيام بذلك استثناء في **حالة التلبس**[2] والتي من المتعارف عليه في التشريعات الإجرائية ومنها الجزائري أنها تعتبر إحدى الحالات التي تتسع فيها سلطات الضبطية القضائية حيث تباشر لاختصاصات في الأصل من اختصاص قاضي التحقيق و التي منها التفتيش بحثا عن أدلة إرتكاب الجريمة وتحديد الفاعل، وذلك مهما كان محل التفتيش المسكن[3] أو الشخص ، عند وقوع جناية أو جنحة داخل المنزل واستدعائهم من قبل صاحبه لإجراء التحقيق.[4]

[1]- نبيلة هبه هروال، المرجع السابق، ص 233.

[2]- راجع المادة (44) و(45) من قانون الإجراءات الجزائية الجزائري.

[3]- راجع المادة (45) من قانون الإجراءات الجزائية والمادة (1/56) من قانون الإجراءات الجزائية الفرنسي.

[4]- راجع المادة (46) و(42) من قانون أصول المحاكمات الجزائية السوري.

وبالنظر إلى ضرورات عملية تعود للحرص على سرعة إنجاز أعمال التحقيق وتيسيره والاستفادة من قدرات رجال الضبطية القضائية في تنفيذ بعض إجراءاتها، أجيز لها تكليف هؤلاء تنفيذ بعض أعمالها وعلى رأسها التفتيش.

ولا يختلف الأمر في حالة جرائم الاعتداء على نظم المعلوماتية ، فالأصل أن يقوم قاضي التحقيق بتفتيش النظم بنفسه أو ندب أحد أعضاء الضبطية وفقا للقواعد الإجرائية المنصوص عليها وفق هذه النصوص[1]، وفي هذه الحالة يجب تحديد في إذن بالإنتدابنوع المهمة و هو التفتيش مع تحديد المكان والشخص والأشياء المراد تفتيشها وضبطها كتحديد الجهاز الإلكتروني، برامج الاختراق برامج فيروسات،...الخ ،إضافة الى وجوب حضور المعني(المتهم في الأصل كما قد يكون غيره) محله بالتفتيش ،و ينص التشريع الإجرائي الجزائري على وجوب حضور شاهدين في كلا الحالتين سواء كان القائم بالتفتيش قاضي التحقيق أو ضابط الشرطة القضائية، ويعد حضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية إحدى الأشخاص الواجبة الحضور وقت إجراء تفتيش مسكن المتهم، وذلك بعد تعذر حضور المتهم وقت ذلك الإجراء وامتناعه عن تعيين ممثل له أو هروبه، والأمر نفسه بالنسبة للتشريع الإجرائي الفرنسي[2].

إلا أن المشرع أقر بالطبيعة المستقلة و المتفردة لجرائم الاعتداء على نظم المعلوماتية وما تتطلبه التحقيقات من سرية أثناء جمع الدليل التقني في إطار الجرائم محل الدراسة عاد بموجب الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية[3] ،إستثنى تطبيق الأحكام السابقة (فيما يتعلق بحضور الأشخاص المحددين في الفقرة الأولى من هذه المادة) على عدة جرائم التي من بينها **جرائم المساس بنظم المعالجة الآلية للمعلومات**.

[1]- راجع المواد (138)، (139)، (140)، (141)، (142) من قانون الإجراءات الجزائية الجزائري.

[2]- أنظر المادة (45) من قانون الإجراءات الجزائية الجزائري، والتي هي ترجمة حرفية للمادة (56) إجراءات فرنسي.

[3]- تنص الفقرة الأخيرة من المادة (45) من قانون الإجراءات الجزائية على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني...".

و يذهب المشرعان الجزائري والفرنسي إلى حضر تفتيش المنازل وما في حكمها في وقت معين، فقد حدد المشرع الجزائري **وقت التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا**، وذلك من خلال المادة (47) إجراءات جزائية[1]، أما بالرجوع إلى القانون الفرنسي فنجده يحدده من الساعة السادسة صباحا إلى الساعة التاسعة مساءا، وذلك من خلال المادة (59) إجراءات جزائية[2].

إلا أن هناك حالات استثنائية يجوز الخروج عن تلك القاعدة، فيصح فيها إجراء التفتيش **ليلا أو نهارا**، أهمها : **حالة طلب صاحب المنزل أو جهت نداءات من الداخل أو في الأحوال المستثناة قانونا**[3]**، أو حالة الجرائم المعاقب عليها في المواد (342) إلى (348) من قانون العقوبات الجزائري وذلك في داخل كل فندق أو منزل مفروش أو فندق عائلي أو محل لبيع المشروبات أو نادي أو منتدى أو مرقص أو أماكن المشاهدة العامة وملحقاتها وغيرها.**[4]

هذا بالإضافة للجرائم المنصوص عليها في الفقرة الثالثة (3) من المادة (47) من نفس القانون و التي منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إذ جاء فيها "**وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص**".

[1]- تنص المادة (47) إجراءات جزائية جزائري على "لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساءا، إلا إذا طلب صاحب المنزل أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا".

[2]- Voir : art 59 alinéa 1 du C.P.P.F.

[3]- أنظر المادة (47-1) من قانون الإجراءات الجزائية الجزائري.

[4]- أنظر المادة (47-2) من قانون الإجراءات الجزائية الجزائري.

والملاحظ أن في إقرار المشرع الجزائري التفتيش في اطار الجرائم محل الدراسة ليلا أو نهارا يكون قد أدرك الطبيعة المميزة لهذه الجرائم وخصوصيتها من حيث أنه يمكن ارتكابها في أي وقت، وأن أدلة الإدانة فيها سهلة الإخفاء او التدمير ، وبالتالي فإن التأخير في إجراء التفتيش من شأنه عرقلة سير مجريات التحقيق،

و لما كان التفتيش عملا تحقيقيا فإنه يتطلب ذلك تحرير محضر لإثبات ما تم من إجراءات، وما نتج عن التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما، والتي تقضي بأن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[1] ، لهذا فإن الأمر ذاته يكون فيما يخص محضر تفتيش نظم المعلوماتية وإن كان يستلزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة القائم بالتفتيش بتقنية المعلومات فضلا على استعانته في مجال الخبرة الفنية الضرورية وفي صياغة مسودة محضر التفتيش بشخص يرافقه يكون متخصص في الحاسوب والانترنت[2].

أما في الجزائر فقد تدخل المشرع الجزائري لاستكمال ما تبقى من فراغ تشريعي في المنظومة التشريعية، وذلك بموجب القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث استحدث المادة (6) التي تنص على أنه "**عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز، والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية...**".

[1]- قدري عبد الفتاح الشهاوى، المرجع السابق، ص 160.

[2]- نبيلة هبة مولاي علي هروال، المرجع السابق، ص 263.

وإلى جانب المشرع الجزائري نجد المشرع الفرنسي الذي قام بإدخال تعديل على قانون الإجراءات الجزائية الفرنسي لسد هذا الفراغ التشريعي وذلك بموجب قانون الأمن الداخلي رقم (239) لسنة 2003 حيث استحدث الفقرة الثالثة (3) من المادة (57-1) التي تنص على أن "**المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة، يتعين نسخها على دعامات، ودعامات التخزين المعلوماتية هذه يتعين تحريزها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون**"[1]، وهذا الأمر مسلك طبيعي باعتبار أن فرنسا من الدول الموقعة على اتفاقية بودابست لعام 2001، حيث نصت هذه الأخيرة على الضبط في الفقرة الثالثة (3) من المادة (19) من القسم الرابع منها على أنه" **من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزءا منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر، وأن تحافظ على سلامة تلك المعلومات المخزنة**"[2].

أما بخصوص المكونات المادية للنظام فلا يثير ضبطها أي صعوبات، فيمكن ضبط المدخلات بما تشمله من مفردات كلوحة المفاتيح، نظام الفأرة، نظام القلم الضوئي...

هذا وقد يرد الضبط على عناصر تقنية منفصلة مثل الديسكات والأسطوانات الممغنطة... وهنا لا إشكال قانوني يطرح عند القيام بالضبط، في حين قد تثور الصعوبة عندما يلزم ضبط النظام كله أو الشبكة كلها، وتظهر هذه المسألة بصورة جلية في حالة ما إذا كان الحاسوب المتورط في الاتهام مثلا ليس حاسوبا شخصيا pc وإنما جزء من شبكة معقدة، فإن الدمار المصاحب

[1]- art 17-1/3 du L.S.I.F dispose que « les données auxquelles il aura été permis d' accéder dans les conditions prévues le present article peuvent être copiées sur tout support, les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code ».
(voir aussi : art 57-1 alinéa 3 du C.P.P.F).
[2]- art 19 alinéa 3 du C.C.C disponible en ligne à l' adresse suivante :
http://convention.coe.int/treaty/en/treaties/html/185.htm.

لذلك والمشكلات العملية التي يمكن أن تبرز جراء ضبط الشبكة بالكامل غالبا ما تواجه إجراء الضبط.[1]

وعلى أية حال فإن طريقة ضبط المعلومات المعالجة آليا تختلف عما هي عليه عند ضبط المكونات المحسوسة كالأقراص المرنة والمودم والخادم...، ونتيجة لذلك يفضل البعض فضلا عن المصطلح التقليدي "الضبط" saisir استخدام مصطلح الحصول بطريقة مشابهة obtenir par un moyen similaire وذلك من أجل الأخذ في الاعتبار الطرق الأخرى لرفع المعلومات غير المادية، وهو ما يستفاد بوضوح من الفقرة (3) من المادة (19) من الاتفاقية الأوروبية لجرائم تقنية المعلومات.

فهناك أسلوب النسخ و حاليا يتم استخدام برامج متخصصة في النسخ مثل برنامج lap link[2]، كما يوجد أسلوب تجميد التعامل بنظام المعلوماتية أو إحدى القطع المكونة له التي استخدمت في ارتكاب الجريمة، ويتخذ هذا الأسلوب عدة مظاهر، من أبرزها: نظام ضغط محتويات القرص الصلب، وكذلك نقل المحتويات إلى أقراص صلبة متعددة أو ممغنطة، ومثل هذا الإجراء يصلح أن يتخذ في مواجهة الحاسبات الخادمة التي تحتوي على مواقع الهاكر أو ملفات فيروسية، كما يصلح أيضا إذا كان القرص الصلب يحتوي مثلا على ملفات مشفرة، وتحتاج إلى فك شفرتها[3].

من الطبيعي أن يتبع عملية ضبط الأدلة الجنائية عامة عملية تحريزها، وهو ما ينطبق على الأدلة التقنية إلا أن هذه الأخيرة ونظرا لطبيعتها الخاصة فإن مسألة تأمين ضبطها يتطلب –فضلا

[1]– فعلى سبيل المثال إذا قام مدير نظام لشبكة حاسوب بتخزين معلومات تم التقاطها مسجلة في مكان ما في الشبكة، فإن الشبكة تصبح أداة لجريمة مدير نظام الشبكة، ومن الناحية الفنية فإن أعضاء الضابطة العدلية ربما يمكنهم الحصول على إذن بضبط الشبكة بالكامل، ومع ذلك فإن تعطيل الشبكة كلها يعوق أعمال قانونية عملية ويزعج حياة مئات الأشخاص.

[2]– برامج النسخ مثل lap link: وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي parallet port أو على التوالي serial port وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم، أنظر: حسن طاهر داود، المرجع السابق، ص 229. و ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (tcp/ip) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق، ص 10.

[3]– عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 871 وما بعدها.

على الإجراءات التي وضعها المشرع للمحافظة على سلامة المنقولات عامة[1]- اتخاذ بعض الإجراءات الخاصة للحفاظ عليها وصيانتها من العبث وذلك على النحو التالي:[2]

1- ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها.

2- عدم ثني القرص لأن ذلك قد يؤدي إلى تلفه وفقدان المعلومات المسجلة عليه.

3- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة، مع الإشارة إلى أن درجة الحرارة المسموح بها تتراوح ما بين (2-32) درجة مئوية، إما بالنسبة للرطوبة المسموح بها فتتراوح ما بين 20% إلى 80%.

4- منع الوصول إلى المعلومات التي تم ضبطها، وذلك عن طريق ترميزها أو تقييدها عن طريق وسيلة إلكترونية أخرى تمنع الدخول إلى هذه المعلومات، ونص على هذا الإجراء المشرع الجزائري وذلك في المادة (7) من القانون رقم (09-04) لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أوجبت هذه المادة على **السلطات المختصة في حالة استحالة إجراء حجز المعطيات بنسخها دون ضرورة حجز كل المنظومة لأسباب تقنية، استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة،** كما نصت على هذا الإجراء الفقرة الثالثة (3) من المادة (19) من اتفاقية بودابست الموقعة في 23 نوفمبر 2001 كما يلي " **rendre inaccessibles ou enlever ces données informatique du système informatiques consulté".**

ووفق المذكرة التفسيرية للاتفاقية فإنه يتم اللجوء إلى هذا الإجراء في حالة ما إذا كانت المعطيات تتضمن خطرا أو ضررا بالمجتمع ومثال ذلك: البرامج التي تحتوي على فيروسات أو تقدم نموذجا لعمل الفيروسات، أو قنابل.

[1]- راجع في ذلك المواد التالية (45) و(84) من قانون الإجراءات الجزائية الجزائري، والمادة (1/35) من قانون أصول المحاكمات الجزائية السوري.

[2]- هشام محمد فريد رستم، المرجع السابق، ص 130-131.

الفرع الثاني : الخبرة التقنية:

و التي يقصد بها "أنها إجراء يهدف لاستخدام القدرات الفنية أو العلمية لشخص والتي لا تتوافر لدى رجل القضاء أو المحقق، من أجل الكشف عن دليل أو قرينة تفييدهم في المعرفة الحقيقة بشأن وقوع الجريمة أو نسبتها إلى المتهم أو تحديد ملامح شخصيته الإجرامية[1]"، و عليه ما هي إلا وسيلة إثبات تهدف لكشف بعض الدلائل أو تحديد مدلولها بواسطة المعلومات العلمية غير المتوافرة لدى المحقق أو القاضي.

وتكمن أهميتها في المساعدة لسائر السلطات المختصة (سلطات الإستدلال و التحقيق والمحاكمة) بالدعوى العمومية لتحقيق العدالة ، لذا فقد اهتم المشرع الجزائري بالخبراء ومساعدتهم لجهات التحقيق المختلفة ، خاصة في مجال استخلاص دليل إثبات جرائم الاعتداء على نظم المعلوماتية، فهي تتعلق بمسائل فنية معقدة ، والتطور في أساليب ارتكابها سريع ومتطور، والتي لا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز في مجال تخصصه.

ولعل أن هذه الأهمية هي التي جعلت المشرع اثر تعديله لقانون الإجراءات الجزائية بموجب الأمر 15-02 فالمادة 35 مكرر منه كرست المساعدة المتخصصة في المسائل الفنية و التي من بينها الجرائم التقنية ، حيث نصت المادة 35 مكرر من الأمر السابق الذكر : " يمكن للنيابة العامة الإستعانة في مسائل فنية ، بمساعدين متخصصين.

يساهم المساعدون المتخصصون في مختلف مراحل الإجراءات تحت مسؤولية النيابة العامة التي يمكنها ان تطلعهم على ملف الإجراءات لإنجاز مهامهم .

يؤدي المساعدون المتخصصون اليمين أمام المجلس القضائي الذي يعينون بدائرة إختصاصه لأول مرة ، وفق الصيغة الآتية :

(أقسم بالله العظيم أن أقوم بأداء مهامي على أحسن وجه و أن أحافظ على سرية المعلومات التي أطلع عليها بمناسبة أداء عملي .)

[1]- أحمد شوقي الشلقاني، المرجع السابق، ص 259.

تنجز الأعمال التي يقوم بها المساعدون المتخصصون في شكل تقارير تلخيصية أو تحليلية يمكن أن ترفق بالتماسات النيابة العامة.

تحدد شروط و كيفيات تعيين المساعدين المتخصصين و كذا قانونهم الأساسي و نظام تعويضاتهم عن طريق التنظيم."

كما نجد في نفس السياق المادة 147من قانون الإجراءات الجزائية التي كرست حق قضاة التحقيق في انتداب خبير او خبراء.

و بقراءة المادة 35 مكرر أعلاه نلمس أن الخبراء يتم إختيارهم من قبل النيابة العامة وهذا على سبيل الجواز متى دعت الضرورة لذلك ، و هذا نظرا للمسألة الفنية المعروضة عليهم ، و التي تخرج عن نطاق معارفهم ، كما ان القانون ترك لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعددين وذلك بموجب المادة 147 من قانون الإجراءات الجزائية وفق الإجراءات المنصوص عليها باللمواد من 143 الى 146 من قانون الإجراءات الجزائية ، والذي نراه يتجاوب مع الحال الذي عليه الخبرة التقنية.

و لصحة قيام الخبير بأداء مهامه يقع عليه واجب تأدية اليمين و إلا كان عمله باطلا ، و هذا لحمله على الصدق والأمانة في عمله، وبث الطمأنينة في آراءه التي يقدمها سواء بالنسبة لتقدير الجهات التحقيقية، لذلك فلقد أوجب المشرع الجزائري بموجب المادة (145)[1] و الفقرة الثالثة من المادة 35 مكرر المذكورة أعلاه من قانون الإجراءات الجزائية ، و يستوي أداء اليمين يوم تسليمه العمل أو أداه قبل العمل المطلوب[2].

فالخبير يتولى مهمته تحت رقابة القاضي الذي أمر بإجراء الخبرة ولا يستلزم ذلك حضوره فعلا أثناء قيامه بإعماله بل يكفي أن يبقى على اتصال معه بهدف إحاطته علما بكل

[1] – تنص المادة (145) من قانون الإجراءات الجزائية الجزائري على أنه "يحلف الخبير اليمين المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتي بيانها:

–أقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال–

ولا يجدد هذا القسم ما دام الخبير مقيدا في الجدول".

[2] عبد الناصر محمد محمود فرغلي ود. عبيد سيف سعيد المسماري، المرجع السابق ص24

المستجدات التي تطرأ عليه في مجال عمله[1] على اعتبار أن الخبير هو مساعد متخصص للقاضي ، وفي حدود ما نص عليه أمر أو حكم الندب أثناء إجراء أعمال الخبرة، ومن ذلك تكليف الخبير بإجراء أبحاث معنية أو سماع أي شخص معينة باسمه قد يكون قادرا على مدهم بالمعلومات ذات الطابع الفني[2]. بأمر أو حكم الندب فإذا لم يودع تقريره جاز للقاضي في الحال استبداله بغيره، وعليه إذا ذاك أن يقدم نتائج ما قام به من أبحاث، كما عليهم أيضا أن يردوا في ظرف ثمان وأربعين ساعة جميع الاشياء والاوراق التي تكون في عهدتهم على ذمة إنجاز مهمتهم أكثر من ذلك يجوز أ تتخذ ضدهم تدابير تأديبية قد تصل إلى شطب أسمائهم من جداول الخبراء بقرار من وزير العدل إذا نسب إليهم إهمال ما[3] . فالخبير يحرر لدى انتهاء أعمال الخبرة في شكل تقارير تلخيصية او تحليلية كما نصت عليه الفقرة الرابعة من المادة 35 مكرر المذكورة اعلاه و التي يجب أن تشمل على وصف ما قام به من أعمال ونتائجها[4] و هذا طبقا للمادة (215) من قانون الإجراءات الجزائية تكون هذه التقارير مجرد استدلالات لإنارة القاضي، وذلك لكون رأي الخبير يعطي دائما بصفة استشارية ولا يقيده فهو ليس بحكم وليست له قيمة قضائية أكثر من شهادة الشهود، وعليه فيجوز للقاضي أن يأخذ بالخبرة أو يطرحها، وأن يفاضل بين تقارير الخبراء، ويأخذ منها بما يرتاح إليه ويطرح ماعداه, وله أن يأمر بإجراء خبرة إضافية إذا كان هذا التقرير ناقص أو غير كامل [5].

وهذا يؤدي بحكم المنطق العقلي إلي التأكيد علي أن كل ما يتعلق بالدعوي يجب أن ينتهي عند قاض الموضوع لكي يتولى الفصل فيه. فالكلمة الاخيرة لمحكمة الموضوع حتى ولو كان الرأي الذي استندت إليه هو الرأي الخبير.

---

[1] راجع الفقرة الخامسة من المادة (143)) من قانون الاجراءات الجزائية الجزائري .

[2] راجع المادة (152) من قانون الاجراءات الجزائية الجزائري .

[3] راجع المادة 148 من قانون الاجراءات الجزائية الجزائري.

[4] راجع المادة (153 /1) من قانون الاجراءات الجزائية الجزائري.

[5] وما يحصل في الواقع العملي أن القاضي غالبا ما يسلم بما خلص اليه الخبير في تقريره، ويبني حكمه على أساسه، وهذا التصرف منطقي من القاضي فلا شك في أن رأي الخبير ورد في موضوع فني لا اختصاص للقاضي به ، وليس في شأن ثقافته أو خبرته القضائية أن تتيح له الفصل فيه، بالإضافة الى ذلك هو الذي انتدب الخبير ووثق فيه وراي أنه مناسب لمهمته.

وذات الأمر يسري هنا على الناتج من الخبرة في إطار المعلوماتية ، حيث أن القاضي يظل الخبير الأعلى، حتى ولو كانت المسألة الفنية في مجال تقنية المعلومات قد عرض لها خبير تقني وأخذ القاضي برأيه، ومثل هذا المنطق لا يجعل الخبير في مستوى عمل القاضي، بل يظل دور القاضي قائما في المفاضلة بين التقارير الفنية المقدمة إليه [1] .

وإذا كان الأمر على ما سلف فما هي أذن أساليب الخبير التقني في تحري الحقيقة سيما إذا كان بصدد مسالة من المسائل الجديدة على العمل والتقنية، مثلما هو الحال في تكنولوجيا المعالجة الآلية للمعلومات.

لما كانت عملية تجميع الأدلة التقنية، تعد من أهم وأصعب الأمور التي تواجه الخبير التقني كان لزاما عليه أن يتبع عدة خطوات من أجل اشتقاق هذا النوع المستحدث من الدليل، وتتمثل هذه الخطوات في **– المراحل التالية :**

– التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها.

– التأكد من صلاحية وحدات النظام للتشغيل.

– تسجيل معطيات وحدات المكونات المضبوطة كالنوع والطراز والرقم المسلسل...

– استكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز.

– عمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب hard d'ISK لإجراء عملية الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برامجية.

– تحديد أنواع وأسماء المجموعات البرامجية، برامج النظام (برامج التشغيل)، وبرامج التطبيقات وبرامج الاتصالات.... وما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة.

– إظهار الملفات المخبأة، والنصوص المخفية داخل الصور.

[1] – عمر ابو بكر بن يونس ،الجرائم الناشئة عن استخدام الانترنيت، المرجع السابق ص1028.

-استرجاع الملفات التي تم محوها من الأصل وذلك باستخدام أحد برامج استعادة المعلومات وكذلك بالنسبة للملفات المعطلة أو التالفة، مثل برنامج Recovrecov4all Professional Easy Recover.

- تخزين هذه الملفات، أو المعطيات وعمل نسخ طبق الأصل أخرى من الأسطوانة أو القرص المحتوي لها ولفحصها عن طريق تطبيق الخطوات سالفة الذكر[1].

- يتم إعداد قائمة يجرد فيها الخبير كل الأدلة التقنية التي تم الحصول عليها في الديسك الخاص به مع إجراء مراجعة لكل صورة محتفظ بها في الديسك في كمبيوتر آخر للتأكد من سلامة القائمة[2].

- تحويل الدليل التقني إلى هيئة مادية وذلك عن طريق طباعة الملفات، أو تصوير محتواها إذا كانت صور أو نصوص، أو وضعها في أي وعاء أخر حسب نوع المعطيات المكونة للدليل[3].

في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط، والدليل التقني في شكله المادي، ومن تم الربط بينهما مما يكسب الدليل الموثوقية واليقينية، اللتان تؤديان إلى قبوله لدى جهة التحقيق والحكم.

حيث يتم إعداد تقرير بجميع خطوات وإجراءات البحث ويرفق به في الغالب الملاحق الإيضاحية المصورة أو المسجلة وغيرها لاعتمادها ثم تسلم إلى جهة الحم والقضاء.

الفرع الثالث : التسرب:

من المقومات التشريعية المكرسة من قبل المشرع الجزائري لمكافحة الجرائم المستحدثة[4] و التي من بينها جرائم الاعتداء على نظم المعالجة الألية نجد إجراء التسرب، وتم تنظيم هذا الإجراء وفق ثمانية مواد من المواد (65 مكرر 11) حت المادة (65 مكرر 18).

[1] عبد الناصر محمد محمود فرغلي وعبيد سيف المسماري المرجع السابق. ص36.

[2] عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر المرجع السابق. ص2265.

[3] عبد الناصر محمد محمود فرغلي ود. عبيد سيف المسماري المرجع السابق. ص35

[4] - وقد كان ذلك بموجب القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم (66-155) المتضمن قانون الإجراءات الجزائية والذي أفرد الفصل الخامس منه تحت عنوان: " في التسرب ".

حيث عرف المشروع الجزائري التسرب بموجب المادة (65 مكرر 12) من قانون الإجراءات الجزائية على انه: " **قيام ضابط أو هون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف**" .

كما حدد المشرع نطاقه بالجرائم المذكورة في المادة (65 مكرر) التي عددها على سبيل الحصر وهي: **جرائم المخدرات، الجريمة المنظمة، الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، جرائم تبييض الأموال والإرهاب، وأخيرا الجرائم المتعلقة بالتشريع الخاص بالصرف.**

ويمكن تصور عملية التسرب في نطاق جرائم الاعتداء على نظم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى البيئة الافتراضية واشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش والاتصال المباشرة في كيفية قيام أحدهم باختراق شبكات أو بث الفيروسات مستخدما في ذلك أسماء وصفات هيئات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سعيا منه الاستفادة منهم حول كيفية اقتحام الهاكر لموقع ما مثلا.

لما كان التسرب ممارسة غير مألوفة للضابط أو عون الشرطة القضائية بل يعد من أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمتهم نجد أن المشرع أحاطه بجملة من الضمانات يتعين مراعاتها عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة اللجوء إليه، فكما سبق ذكره وعملا بمبدأ الشرعية يجب أن تتوفر في هذا الإجراء الإذن وهذا ما نصّت عليه المادة(65مكرر11) من قانون الإجراءات الجزائية كما يلي " .... **يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت ...**" فالجهة المختصة لإصداره كما هو مبين من نص المادة إما وكيل الجمهورية أو قاضي التحقيق وذلك حماية للحقوق الأساسية المكرسة دستوريا، وعليه لا يمكن بأي حال من الأحوال أن قوم ضابط الشرطة القضائية بالعملية بفرده دون المرور على الجهاز القضائي ، والذي يجب ان يكون مكتوبا وهو ما نصت

عليه المادة (65 مكرر 15) من قانون الإجراءات الجزائية بقولها " **يجب أن يكون الإذن المسلم طبقا للمادة (65 مكرر 11) أعلاه مكتوبا ... تحت طائلة البطلان"** وذلك أن الأصل في العمل الإجرائي الكتابة، وإذا صدر في إطار إنابة قضائية ينبغي مراعاة الشروط الشكلية والموضوعية للإنابة القضائية التي نصت عليها المادة (138)، (139) من قانون الإجراءات الجزائية مع تحديد المشرف على العملية وهويته الكاملة ، مع تحديد مدته حسب نص المادة (65 مكرر 15) الفقرة الثالثة من قانون الإجراءات الجزائية على ان **لا تتجاوز أربعة أشهر**، ويمكن أن تجدد حسب مقتضيات التحري أو التحقيق، ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة.

كما أن المشرع الإجرائي نص في المادة (65 مكرر 17) من قانون الإجراءات الجزائية، بأنه يمكن **للعون المتسرب أن يواصل نشاطه غير القانوني الوارد في نص المادة (65 مكرر 14) من قانون الإجراءات الجزائية مع إعفائه من المسؤولية الجزائية لمدة لا تتجاوز (4) أشهر على أن يخطر القاضي مصدر الرخصة في أقرب الآجال، أما إذا لم يتمكن العون المتسرب من إيقاف نشاطه خلال المدة المذكورة في ظروف تضمن أمنة يمكن للقاضي أن يرخص بتمديدها لمدة (4) أشهر أخرى.**

و حفاظا على السرية المطلوبة حصر المشرع إجراء التسرب بين القاضي الآمر بها (وكيل الجمهورية أو قاضي التحقيق) وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب حيث نلمس من نص المادة (65 مكرر 12) والمادة (65 مكرر 14)[1] من قانون الإجراءات الجزائية أن المخولين قانونيا للعمل بنظام التسرب هم **ضابط وكذا أعوان الشرطة القضائية وكذا الأشخاص المسخرين لذلك**

[1] تنص المادة(65 مكرر 12) على أنه يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية ..."وتنص المادة (65 مكرر 14) على أنه " يمكن لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عمليات التسرب والأشخاص الذين يسخرون لهذا الفرض ..."

هذا و يكون الإذن مكتوب بشكل مفصل لاطلاع القاضي بشكل تام عن ظروف القضية ومتطلباتها فالتسبيب أساس العمل القضائي ومن ثم كان لزاما عند إصدار الإذن بالتسرب سواء من طرف وكيل الجمهورية أو قاضي التحقيق إظهار جميع الأدلة بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية (المادة 65 مكرر 15) من قانون الإجراءات الجزائية).

وقد حصرتها المادة (65 مكرر5) في سبعة أنواع هي: **جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبيض الأموال، الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائد الفساد.**

و بعد صدور الإذن بالتسرب من طرف القضاء يباشر العون المتسرب عمله حسب المقتضيات المطلوبة منه ومن تم هناك أثارا ستترتب عن ذلك منها:

قد نصت على ذلك المادة (65 مكرر 14) من قانون الإجراءات الجزائية على أنه يمكن:

اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

وكذا **استعمال أو وضح تحت تصرف مرتكبي هذه الجرائم الوسائل ذات طابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.**

وبالتالي يمكن للعون المتسرب استعمال الأموال المتحصل عليها من ارتكاب الجرائم المذكورة بنص المادة (65 مكرر 5) من قانون الإجراءات الجزائية ومن تم فإن المتسرب يمكنه تسخير الوسائل المادية لفائدة الخلية الإجرامية من نقل، تسليم، حيازة، إيواء .... أما بخصوص الوسائل القانونية فالمقصود منها توفير الوثائق الرسمية إن كان هناك ضرورة لذلك كاستخراج بطاقة تعريف أو رخصة سياقة أو بطاقة رمادية وبالتالي يحتاج إلى جهاز خاص لتزوير الوثائق الرسمية دون المرور على الإدارة المختصة لإبقاء أعماله ضمن السرية المطلوبة.

لو تأملنا قليلا في طبيعة الأفعال السابقة لوجدناها تستوجب من القائمين بها مشاركة إيجابية كحيازة متحصلات الجريمة أو وسائل ارتكابها، وغني عن البيان أن هذا الصنف من الافعال

يوجب المسؤولية الجزائية وإدراكا من المشروع لهذا الوضع قام بإعفائهم صراحة من هذه المسؤولية وهو ما يستفاد بوضوح من عبارة " ... **دون أن يكونوا مسؤولين جزائيا**..."الواردة بالمادة (65مكرر14) من قانون الاجراءات الجزائية، بل وقد مدّد نطاق هذا الاعفاء لظروف أمنية للمتسرّب حتى بعد انقضاء المدة المحددة في رخصة التسرب، وفي حالة عدم تمديدها أو في حالة تقريره وقف العملية، بشرط ألا يتجاوز ذلك مدة أربعة (4)أشهر سواء من تاريخ انقضاء المدة المحددة في الإذن أو من تاريخ صدور قرار وقفها من قبل القاضي الذي رخّص بإجرائها [1].

وهذه الحالة ما هي إلا تكريسا للمادة (39) من قانون العقوبات التي نصت على أنه «لا جريمة إذا كان الفعل قد أمر أو أذن به القانون .

إذا كان الفعل قد دفعت إليه الضرورة الحالة للدفاع المشرع عن النفس أو عن الغير أو عن مال مملوك للشخص أو للغير بشرط أن يكون الدفاع متناسبا مع جسامة الاعتداء."

وعليه يمكن إدخال نظام التسرب ضمن أسباب الإباحة باعتبار أن القانون امر بذلك مما يجعل المتسرب معفي من المسؤولية الجزائية، من جهة .

كما عملية التسرب تتطلب إحاطتها بالسرية التامة وذلك لتحقيق الأهداف المتوخاة منها ولذلك قرر المشرع الجزائري جزاءات عقابية مشددة في حالة إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية.

[1] تنص المادة (65 مكرر 17) من قانون الإجراءات الجزائية على أنه : " إذا تقرر وقف عملية التسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر 14 اعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا يتجاوز ذلك مدة اربعة أشهر.

يخبر القاضي الذي أصدر الرخصة المنصوص عليها في المادة 65 مكرر 11 أعلاه، في أقرب الآجال، إذا انقضت مهلة الأربعة (4) أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، يمكن هذا القاضي أن يرخص بتمديدها لمدة اربعة (4) أشهر على الأكثر".

بل أن ذلك الأخير قد وسع من نطاق الحماية لتشمل أفراد عائلة المتسرب، وتتراوح هذه العقوبات من سنتين إلى عشرين سنة حبس وغرامة من خمسين ألف إلى مليون دينار حسب الحالات الثلاث المذكورة بالمادة (65مكرر16)[1]من قانون الإجراءات الجزائية بل أكثر من ذلك و بالرجوع إلى المادة (65 مكرر 18) من قانون الاجراءات الجزائية نجدها تمنع سماع الضابط المتسرب واجازت سماع الضابط المشرف على العملية بصفته شاهدا.

المطلب الثاني : تكريس قواعد إجرائية و تنظيمية خاصة لإستخلاص الدليل التقني

ذكرنا سلفا مجموعة من القواعد الإجرائية التقليدية لجمع الدليل التقني الذ يكفي لإثبات هذا النوع الجديد من الجرائم وتبين لنا مدى التعقيد الذي أحدثته ثورة الاتصالات في مسألة استخلاصه وفقها وصعوبته، وهو ما يؤدي إلى إفلات العديد من المجرمين من العقاب، وعلى ذلك كان لزاما أن يلحق التطور طرق الحصول على هذا الدليل الجنائي وذلك من خلال تكريس قواعد قانونية إجرائية غير تقليدية تتناسب والطبيعة التقنية لهذه الجرائم وللدليل التقني الذي يصلح لإثباتها لكي يمكن عن طريقها الوصول إليه ونقصد بذلك تكريس تقنية المعلومات لجمع الدليل التقني.

وهو ما تفطن له المشرع الجزائري، فنجده وإيمانا منه بضرورة تدعيم الحصول على الدليل التقني بتقنية المعلومات تدخل بموجب القانون رقم (06 – 22) المؤرخ في 20 ديسمبر 2006 فاستحدث الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور " فأجاز بموجبه لوكيل الجمهورية أن يأذن باعتراض الاتصالات السلكية واللاسلكية، ليطل بعد مرور ثلاثة سنوات منى هذا التعديل بإطلالة أخرى وذلك بموجب القانون رقم (09- 04) بشأن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكافحتها

[1] تنص المادة (65 مكرر 16) لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات.

يعاقب كل من يكتشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 50000دج إلى 200000دج.

وإذا تسبب الكشف عن الهوية في اعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس إلى عشر سنوات والغرامة من 2000000دج إلى 500000دج.

وإذا تسبب هذا الكشف في وفاة أحد هؤلاء لأشخاص فتكون لعقوبة الحبس من عشر سنوات إلى عشرين سنة والغرامة 500000دج إلى 100000دج من دون الإخلال، عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات".

فاستحدث بموجبه إجراءين: الأول: وهو المراقبة الإلكترونية والثاني: حفظ المعطيات المتعلقة بحركة السير ، وسنتناولها وفق ما يلي :

الفرع الأول: المراقبة للاتصالات الإلكترونية

يقول خبراء أمن المعلومات أن المقولة –الوقاية خير من العلاج– التي اعتاد الناس تداولها في الأوساط الصحية لا يمكن تطبيقها بدقة في مجال جرائم الاعتداء على نظم المعالجة الآلية أو الفضاء الإلكتروني، ومع ذلك فإن من الحماقة أن يترك الفرد منزله غير مغلق عند ذهابه إلى العمل صباحا، ومن الحماقة كذلك أن يترك نطاقه المعلوماتي دون حماية بحيث يسهل الوصول إليه.[1]

انطلاقا من هذه العبارات يتضح لنا أن المنع الجنائي وتحديد عقوبات جرائم الاعتداء على النظم محل الدراسة بصفة مسبقة بما يتماشى ومبدأ الشرعية وإن كان يوفر حماية أساسية للنظام وللمعلومات في وقت مبكر جدا ضد المخاطر والأضرار الناجمة عن هذه الجرائم من إتلاف وتدمير باهظ التكلفة في حالة إعادة البناء، أو الوصول إلى معلومات شرعية من ذلك كلمات المرور أو معلومات عن النظام الهدف وأسرار تستخدم باستخدام النظام مجانا وغيرها كثير، إلا أنه غير كافي لوحده، فحتى تكون هناك الفعالية في الحركة والأداء لا بد أن نعززها بحماية فنية تعمل على الحيلولة دون وقوع هذه الجرائم أو التخفيف من آثارها إذا وقعت.

وهذا ما أكدت عليه المذكرة التفسيرية لاتفاقية بودابست حينما ذهبت إلى القول من أن الوسيلة الأكثر فعالية لمنع الولوج غير المصرح به تتمثل بطبيعة الحال في التهديد بقانون العقوبات ومع ذلك فإن هذا العرض لا يكون مكتملا بدون تبني ووضع إجراءات أمنية فعالة. [2]

ووسائل أمن المعلومات كثيرة ومتنوعة حيث لا يمر يوم دون وجود منتج جديد، ولا يمر أيضا دون إعادة تقييم لوسائل الأمن، ولا نبالغ إن قلنا أنسوق وسائل الأمن أصبح يتقدم في عدد منتجاته على سوق الأجهزة ذاتها والحلول، لأن كل منتج وكل برنامج جديد يتطلب قدرا معينا من

[1] – عبد الفتاح بيومي حجازي، الأحداث والانترنت، المرجع السابق، ص 292.

[2] – إن أهمية الحماية الفنية دعت واضعي مشروع الغش المعلوماتي الفرنسي إلى إدراج شرط للتجريم المتمثل في تمتع نظام المعالجة الآلية بنظام الأمان، لكن ذلك لم يظهر في الصياغة النهائية للنص.

وسائل الحماية، بل أن سوق الأمن قد انتقل إلى التخصصية فنشأت شركات عملاقة تعمل في حقل أمن المعلومات، ووسائله وحلوله، واتجهت الدراسات البحثية والإستراتيجية والعملية وحتى القانونية إلى التعامل مع وسائل الأمن على استقلال، فثمة أدلة ودراسات شاملة في ميدان الفيروسات ووسائل مكافحتها وثمة مثلها في ميدان التشفير وحلوله وغيرها كثير.

هذا وتتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة المعالجة الآلية للمحافظة على المعلومات بشكل آمن، كما تتعدد أغراضها ونطاقات الاستخدام فنجد على سبيل المثال: التحكم بالوصول من خلال الاستخدام الأمثل لكلمات السر وأنظمة التحقق البيولوجي كقارئات بصمات الأصابع والتعرف الصوتي، تقنيات التشفير سواء التشفير المتناظر أو التشفير غير المتناظر (التشفير باستخدام المفتاح العام)، الجدران النارية، وفضلا عما تم ذكره توجد هناك العديد من وسائل الأمن الفنية التي تستخدم في الحماية المبكرة من الاعتداءات المحتملة مثل الترميز، والتوقيع الإلكتروني، والتحديثات والبرامج المطورة للحماية من عمليات الاختراق والمخترقين مثل:

[1] internet alert 99 jammer

[1]– حسن طاهر داوود، جرائم نظم المعلومات، المرجع السابق، ص 159، جبريل العريشي، أمن المعلومات عن طريق الجدار الناري والتشفير وغيرها...، الرياض، الخميس 5 نوفمبر 2009، منشور على الموقع التالي: http://www.almarfeh.org.

وليد أبو سعد، أمن المعلومات، الموسوعة العربية للكمبيوتر والانترنت، 2005، منشور على الموقع الالكتروني التالي: http://www.c4arab.com/showlesson.php?lesid=1758.

وباللغة الفرنسية أنظر:

Philipe rosé. La criminalité informatique. Edition dahlab. Collection que sais- je ? paris. 1998. P8. Voir aussi : nidal el chaer, la criminalité informatique devant la justice pénale, édition juridiques, Beyrouth, Liban, p178.

كذلك الأساليب التقليدية للأمن بالأجهزة والمنشآت أو ما تسمى في الحقل التقني "بالحماية المادية".[1]

فضلا عما تقدم هناك وسائل أخرى تخرج عن نطاق المجالات التقنية منها إرشادات ونصائح الخبراء الدوليين في مجال الأمن المعلوماتي...

إذا جميعها هي وسائل لتحقيق أمن معلوماتي أفضل، والتي ينبغي إجراء عملية تقييم وتغيير منتظمة للآثار الناجمة عنها من أجل الوقوف على مدى نجاحها في تحقيق النتائج المرجوة، ذلك أنه مع كل جديد ثمة جديد في ميدان الثغرات الأمنية، لأننا ببساطة وفي كل يوم أمام جديد من التقنيات والبرمجيات والبروتوكولات، وفي كل يوم نحن أمام مبرمج يتقيظ ذهنه عن جديد في عالم الكمبيوتر والانترنت، وهو إما جديد إيجابي يستخدم في رخاء البشرية وضمن الاستخدام الإيجابي للإبداع العقلي، أو جديد سلبي يستثمر لتحقيق أغراض غير مشروعة، وبالتالي فإن تحديد المخاطر والثغرات والاعتداءات والخطط والإستراتيجيات عملية مستمرة، يوما بعد يوم، هذا من جهة.

ومن جهة أخرى، ونظرا لوقوع هذه الجرائم ضمن فضاء افتراضي يتم فيه تبادل المعلومات الرقمية وتجري عبره كل أنواع المعاملات والخدمات الإلكترونية بكيفية لا يمكن للسلطات العمومية التحكم فيها بطرق الرقابة التقليدية، من هنا ظهرت الحاجة إلى تكريس إطار قانوني أكثر ملاءمة

[1] – ومن هنا نجد كل منشأة وكل هيئة طريقتها الخاصة في توفير الأمن الفني من المخاطر محل التحديد وبحدود متطلبات حماية المعلومات التي تم تحديدها وبحدود إمكانياتها المادية والميزانية المخصصة للحماية، فلا تكون إجراءات الأمن –الفني– رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغا بها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية، فمثلا تعقيد الحماية على المعلومات لدرجة يصعب فيها حتى على المخولين الوصول إليها قد تدفع لاحقا إلى إهمال كل الإجراءات الأمنية مما يجعل المعلومات عرضة للخرق وهذا ما يسمى لدى الخبراء التقنيين في مجال أمن المعلومات "التأثير على صحة الأداء وفعاليته"، ففي بيئة المعلومات فمن الطبيعي مثلا أن نضع على جهاز كمبيوتر شخصي كلمة سر للدخول إلى الملفات الهامة أو حتى للنظام كله وأن لا نعطي الكلمة لأحد، وأن نضع برنامجا أو أكثر لمقاومة الفيروسات الإلكترونية الضارة، فإذا كان الكمبيوتر خاص بدائرة أو منشأة ويضم معلومات هامة ومصنفة أنها سرية، كان لزاما علينا إجراءات الأمن، فمثلا يضاف للنظام جدران نارية تحد من دخول أشخاص من الخارج وتمنع اعتداءات منظمة قد يتعرض لها النظام، وإذا كانت النظام يتبادل رسائل إلكترونية يخشى على معلوماتها من الإفشاء، تكون تقنيات التشفير مطلوبة بالقدر المناسب، لكن يقبل مثلا على جهاز كمبيوتر خاص غير مرتبط بشبكة عامة أن توضع أنواع متعددة من الجدران النارية أو أن يوضع على أحد الأنظمة وسائل تعريف متعددة لشخص المستخدم، ككلمة السر والبصمة الإلكترونية، وأن يخضع النظام إلى عدد مبالغ فيه من الفلترات والجدران النارية، وتشفير طويل المدى لكافة المعلومات الموجودة أو المتبادلة عبره، بمعنى أن إجراءات الحماية تنطلق من احتياجات الحماية الملائمة فإذا زادت عن حدها أمست ذات أثر سلبي على الأداء، فأصبح النظام بطيئا وغير فاعل في أداء مهامه الطبيعية، وإن نقصت عن الحد المطلوب ازدادت نقاط الضعف وأصبح أكثر عرضة للاختراق الداخلي والخارجي.

وانسجاما مع خصوصية وخطورة جرائم الاعتداء على النظم يتضمن القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها ولعل أهم قاعدة لذلك وهو المراقبة الإلكترونية.[1]

والذي يهمنا في جزئيتنا هذه "المراقبة الإلكترونية" على اعتبار أن اعتماد وسائل الأمن تخرج نوعا ما عن نطاق الدراسات القانونية.

وفي هذا الصدد يمكن القول أن إقرار "نظام الرقابة الوقائية عبر الوسائل الإلكترونية" يعد من بين أهم آليات واستراتيجيات مكافحة جرائم الاعتداء على نظم المعالجة الآلية والوقاية منها على اعتبار أن الفضاء الافتراضي الذي نحن جزء منه هو أرضية لشبكات عديدة من الجرائم محل الدراسة، وهذا ما نادت به اتفاقية بودابست في المادة (21) تحت عنوان "اعتراض معطيات المحتوى" interception de données relatives au contenu كما يلي "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي – المكنات التالية:

أ- جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.

ب- إلزام مقدم الخدمات، في نطاق قدراته الفنية المتوافرة على:

1-على أن يجمع أو يسجل عن طريق تطبيق وسائل فنية موجودة على أرضه، أو:

2-أن يمنح السلطات المختصة عونه ومساعدته من أجل تجميع أو تسجيل، في الوقت الفعلي، المعطيات المتعلقة بمحتوى اتصالات معينة على أرضه، منقولة عن طريق نظام معلوماتي...".

وهذا ما أكد عليه المشرع الجزائري بموجب المادة (3) من القانون رقم (09-04) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كما يلي "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون

[1]- هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية للنشر، القاهرة، 2000، ص 60

الإجراءات الجزائية وفي هذا القانون، وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها...".

وفي هذا الإطار نجد اتفاقية بودابست قد ميزت بين نوعين من المعطيات المعلوماتية محل الاعتراض، بين المعطيات المتعلقة بالمرور والمعطيات المتعلقة بمحتوى الاتصال، وبالنسبة للنوع الأول فقد عرفتها بموجب المادة الأولى (1) بأنها "كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال مع تعيين المعلومات التالية: أصل الاتصال، مقصد الاتصال أو الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال، أو نوع الخدمة[1]"، أما بالنسبة للنوع الثاني: المعطيات المتعلقة بالمحتوى فلم يأت تعريف لها في الاتفاقية، لكنها تشير إلى المحتوى الإخباري للاتصال، بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا المعطيات المتعلقة بالمرور.

والملاحظ أنه وإن كان من المقبول أن كلا النوعين من المعطيات يمكن أن تمس مصالح ذات طبيعة خاصة، إلا أنه بالنسبة لمعطيات المحتوى فإن المصالح الفردية تعد أعلى، نظرا لطبيعة محتوى المعطيات أو الرسالة، ومن هذا المنظور يمكن فرض قيود على تجميع محتوى المعطيات أشد من تلك الخاصة بمعطيات المرور، وقد أكدت اتفاقية بودابست هذا التمييز حيث أدرجت كل إجراء على حدى تحت عنوان خاص، فخصت تجميع حركة المعطيات بعنوان "التجميع في الوقت الفعلي لمعطيات المرور" collecte en temps réel des données relative au traffic (المادة 20)، أما تجميع محتوى المعطيات فجاء تحت عنوان "اعتراض معطيات المحتوى" interception de données relatives au contenu (المادة 21).

وما قيل بشأن اتفاقية بودابست يقال بالنسبة للمشرع الجزائري، حيث أنه وبالرجوع إلى القانون رقم (09-04) بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها، نجده

[1]- art 1 du c.c.c, disponible en lingne à l' adresse suivante : http:// convention .coe .int/treaty en/treaties/html/185.htm.

يفرق هو الآخر بين اعتراض المعطيات المتعلقة بالمحتوى وتجميع المعطيات المتعلقة بحركة السير من وجهة نظر مزدوجة للشروط القانونية التي ينبغي بداءة أن تكون متوافرة من أجل الإذن بمثل هذا الإجراء والجرائم التي يمكن اللجوء حيالها، فقد أشار بشكل معياري في عناوين هاتين الإجراءين إلى تجميع المعطيات المتعلقة بحركة السير تحت مسمى "حفظ المعطيات المتعلقة بحركة السير" (المادة 11)، وتجميع المعطيات المتعلقة بالمحتوى تحت مسمى "مراقبة الاتصالات الإلكترونية" (المادة 4).[1]

ومما لا شك فيه أن المراقبة الإلكترونية إجراء ماس بالحق في الخصوصية، إلا أن هذا الأخير ليس حق مطلق، بل مقيد بالمصلحة العامة، إلا أنه قد تتعارض خصوصية الإنسان مع مصلحة المجتمع في كشف الحقيقة في شأن الجريمة والحيلولة دون وقوعها والتصدي لها بحزم بكل الوسائل المتاحة، مما يستلزم وجود توازن مناسبun équilibre approprié ودقيق بين حق الإنسان في الخصوصية وحق المجتمع في مقاومة الجريمة، ولإقامة هذا النوع من التوازن ينبغي إحاطة هذه المراقبة بجملة من الضمانات، وذلك منعا للتعسف في جميع صوره.

إذا فالمسألة تحكمها قاعدة عامة تحظر المراقبة الإلكترونية، ويرد عليها استثناء تمليه الضرورة، وهذا ما ستناوله فيما يلي على أن يسبق ذلك من جانبنا تحديد ما المقصود بالمراقبة الإلكتروني.

[1]– مصطفاوي عبد القادر، الشرطة الوطنية ومكافحة الجريمة المعلوماتية، الملتقى الدولي لمحاربة الجريمة المعلوماتية، 5-6 ماي 2010، منشور في مجلة مركز البحوث القانونية والقضائية، ص 121.

أولا: المقصود بمراقبة الاتصالات الإلكترونية

لم يتطرق المشرع الجزائري شأنه شأن أغلب التشريعات المقارنة إلى تحديد ما المقصود بمراقبة الاتصالات الإلكترونية مكتف في ذلك بتحديد مفهوم الاتصالات الإلكترونية فحسب[1]، غير أن الفقه قد تصدى إلى هذه المهمة، وفي هذا الإطار تم تعريفها على أنها "مراقبة شبكة الاتصالات"[2]، أو هو "العمل الذي يقوم به المراقب (بكسر القاف) باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا، أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض أمني أو لأي غرض آخر".[3]

يتبين من خلال استقرائنا لهذان التعريفان أن المراقبة الإلكترونية تعتبر من بين التدابير الماسة بحق الإنسان في سرية مراسلاته واتصالاته الخاصة وما يتفرع عنها من حق سرية مراسلاته الالكترونية، ومن ثم وجب تحديد استخداماتها في نطاق الاتصالات المنطوية على خطورة التهديدات المحتملة بالنظر إلى أهمية المصالح المحمية، وفي هذا الإطار نجد أن المشرع الجزائري قد حددها —من بين ما حددها– فيما لو كانت هناك معلومات كافية عن احتمال اعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ((المادة 2/4) من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها) هذا من جهة.

---

[1]– عرف المشرع الجزائري الاتصالات الإلكترونية بموجب الفقرة (و) من المادة الثانية (2) من القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تحت عنوان المصطلحات بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، كما عرفها قانون البريد والاتصالات الإلكترونية الفرنسي لسنة 1980 بأنها "كل انتقال أو إرسال أو استقبال لإشارات أو علامات أو كتابة أو صور أو أصوات عن طريق النظام الكهرومغناطيسي".

Art L32 1° du C.P.T.E.F dispose que « communications électroniques.

On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d' écrits, d' images ou de sons, par voie électromagnétique ».

[2]– la cyber surveillance : « est la surveillance des réseaux de télécommunication… », Maximilien dosté amégée : la cyber surveillance et le secret Professionnel, paradoxes ou contradictions ?,les mémoire D.E.A, université paris, Nanterre, 2002, p50.

[3]– مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، 2003، ص 3.

ومن جهة أخرى فإن التقنية المستخدمة في هذه المراقبة هي التقنية الإلكترونية، والتي تعني "مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة"[1]، ومن بين تلك التقنيات نجد برنامج كارنيفور[2] وتقنية مراقبة البريد الإلكتروني[3]، وقد أكدت التجارب في الولايات المتحدة الأمريكية أن لهذه الأساليب الأثر الفعال في الرصد المبكر للاعتداءات المحتملة.

الفرع الثاني: حظر مراقبة الاتصالات الإلكترونية الخاصة

مما لا شك فيه أن مراقبة الأحاديث والاتصالات الخاصة تمس بحق الإنسان في الخصوصية ذلك الحق الذي حضي بحماية دستورية في مختلف التشريعات الحديثة[4] لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معا، والحق في الخصوصية وما يتفرع عنه من حرية المراسلات وسرية الأحاديث الخاصة، أضحى تحت رحمة وتهديد وسائل تنصت حديثة اخترقت الحجب ونفذت من خلال السياج المنيع الذي يحيط بالحياة الخاصة[5]، ولم تقتصر هذه الوسائل على التصنت على الاتصالات السلكية (مثل الهاتف الثابت) واللاسلكية (مثل الهاتف المحمول) فحسب[6]، بل امتدت بقدرتها الفائقة إلى التقاط الاتصالات التي تتم بطريق الانترنت (مثل البريد الإلكتروني)، مما أفقد الإنسان أكثر وأكثر حريته وخصوصيته.

---

[1]- نفس المرجع السابق، ص 205.

[2]- تقنية برنامج كارنيفور: التي طورتها إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفدرالي (F.B.I) وذلك من أجل تعقب وفحص رسائل البريد الإلكتروني المرسلة والواردة عبر أي حاسب خادم تستخدمه أي شركة تقوم بتوفير خدمة الانترنت، ويشتبه في أن تيار الوسائل المار عبر خدماتها يحمل معلومات عن جرائم جنائية، ويتم تنفيذ عمليات التعقب والفحص بوضع أجهزة الشركة الموفرة للخدمة تحت المراقبة، وقد حققت هذه التقنية نجاحات كبيرة في تعقب المجرمين، ولقد أصبح يطلق على هذه التقنية بعد 11 سبتمبر 2001 تقنية dcs 1000 وأصبحت تختص بمتابعة القضايا المتعلقة بالأمن القومي والتصدي لأي محاولة لتنفيذ هجومات داخل الولايات المتحدة الأمريكية.

[3]- تقنية مراقبة البريد الإلكتروني: هو برنامج صممه الأمريكي "ريتشارد أتوني"، من أجل سبر محتوى البريد الإلكتروني موضوع المراقبة وقراءة الرسائل التي قام صاحبها بإتلافها أو تلك التي لم يقم بتخزينها أساسا، ولقد استخدمت أجهزة الاستخبارات الأمريكية هذا البرنامج لكشف مشتبه فيه من الجنسية الروسية حاول اختراق مواقع على شبكة الانترنت.

[4]- فقد كفل الدستور الجزائري الحقوق والحريات الفردية في الفصل الرابع في المواد (35)-(36)-(39)-(40).

[5]-محمد أبو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، 2008، ص 5.

[6]- مصطفاوي عبد القادر، المرجع السابق، ص 122.

وهو ما أيقظ الدافع لدى المشرع الجزائري بسن نصوص قانونية تعمل على توفير قدر كبير من الحماية الجزائية على سرية الاتصالات الخاصة للأفراد، حيث عاقب لأول مرة متأثرا في ذلك بنظيره الفرنسي[1] على اعتراض الاتصالات دون إذن بذلك، وذلك بإضافته المادة (303 مكرر) بموجب القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات، حيث تنص تلك الأخيرة على أنه: "يعاقب بالحبس من 6 أشهر إلى ثلاث سنوات وبغرامة من 50000 دج إلى 30000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأي تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.[2]

وتجدر الإشارة في هذا الإطار أن بعض الفقهاء[3] يرى أن المادة (303 مكرر) تخص المحادثات الخاصة أو التي تتم في مكان خاص، وأيضا التي تتم عن طريق خط تلفوني، دون المحادثات التي تتم عن طريق الوسائل الإلكترونية، والتي تتخذ شكل البريد الإلكتروني أو شكل المحادثة الفورية وهي الصورة المعتادة.

إلا أن هذا الرأي مهما كانت مبرراته التي يقوم عليها لا يمكن القبول به، بسبب من أن المشرع لم يحدد وسيلة نقل المحادثات أو تسجيلها إن كانت بخط تلفوني بصريح العبارة كما فعل

[1]- راجع المواد (226-1)، (226-2)، (226-8) من قانون العقوبات الفرنسي.

[2]- في حين لازال هذا الأمر في غيبة عن بعض التشريعات الجزائية الحديثة وعلى رأسها التشريع السوري، إذ لم يتدخل هذا الأخير إلى حد الآن شأنه شأن الكثير من التشريعات العربية- لوضع نص خاص يتناول فيه بالتجريم الاعتداءات المنصبة على الاتصالات العادية منها أو إلكترونية وإنما اكتفى بالنصوص الخاصة بحماية الأسرار، مما يدع المجال مفتوحا للانتهاكات المتعددة للحق في الخصوصية وما يتفرع عنها من سرية الأحاديث الخاصة الجاري قيامها عبر الوسائل الإلكترونية.

[3]- عائشة بن قارة مصطفى، الدليل الإلكتروني في مجال الإثبات الجنائي، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009، ص 108.

المشرع المصري[1] مثلا، أو كانت وفق البريد الإلكتروني أو غرف الدردشة أو غيرها، بل استخدم مصطلحات عامة مرنة تشمل صور الاعتداء على الحياة الخاصة بمختلف التقنيات، ونستدل على ذلك بقوله في مطلع المادة "... بأي تقنية كانت..."، هذا من ناحية.

ومن ناحية ثانية، وحتى على فرض التسليم بتحديده لها بخط التلفون فإن الأمر لا يخلو من النقض والتعارض مع ما وصل إليه التطور التقني وعمليات الدمج التي حصلت بين نطاق الحوسبة والاتصال، ولا ندل على ذلك من حالة التكامل بين أجهزة الهاتف الخلوي وتقنيات تبادل واستعراض المعلومات وعلى رأسها الانترنت.[2]

بل ويغدو هذا الرأي غير صحيح البتة إذا ما علمنا أن الخطوط التليفونية هي الوسيلة الرئيسية المستخدمة للاتصال بشبكة الانترنت.

ثانيا: مشروعية مراقبة الاتصالات الإلكترونية

رأينا فيما تقدم أن الحماية الجزائية للاتصالات السلكية واللاسلكية بما فيها تلك التي تتم عبر الوسائل الإلكترونية بات أمر مؤكدا، وإذا كان المشرع قد أباح مراقبة الاتصالات الإلكترونية إذا اقتضت ضرورة الوقاية من بعض الجرائم، فإن إحاطة هذه المراقبة ببعض الضمانات القانونية[3] الفعالة تعد أمرا ضروريا لحماية الحرية الفردية ولحماية حق الإنسان في سرية اتصالاته ولعل أهمها:

أ – أن يتم تنفيذ الإجراء تحت سلطة القضاء وبإذن منه قبله وخلاله وبعده:

فالسلطة القضائية هي المختصة عموما بإصدار هذا الإذن ويعد ذلك ضمانة لازمة لمشروعية الاعتراض على الاتصالات الإلكترونية، بل هو من مظاهر تكريس دولة الحق والقانون وإضفاء الشرعية على كل الإجراءات المتخذة في هذا الشأن من طرف الضابطة العدلية، وهذا ما

[1] – حيث جاء في الفقرة (أ) من المادة (303) من قانون العقوبات المصري كما يلي: "استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التلفون...".

[2] – لكون الانترنت تعمل بنظام استعمال الحاسوب، على أية شاكلة يكون عليها، كالحاسب الشخصي pc أو النقال أو الشبكات networks وأيضا الهواتف النقالة التي يدخل عليها الحاسوب فيجعلها تتصل بالأنترنت.

[3] - Le FBI, mission et stratégie de lutte contre la cybercriminalité, Delecki Zachary
,مداخلة ألقيت في الملتقى الدولي لمحاربة المعلوماتية ، 5-6 ماي 2010 بالجزائر، منشور في مجلة مركز البحوث القانونية والقضائية ،ص 133

أكد عليه المشرع الجزائري بموجب الفقرة الأخيرة من المادة الرابعة (4) من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كما يلي: "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة".

ب: أن تكون ثمة ضرورة قصوى تدعو إليه:

بالرجوع إلى نص المادة (4) من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووفقا للمناقشات التي دارت خلال الأعمال التحضيرية لهذا القانون يتضح[1] أن ضابط الوقاية من وقوع بعض الجرائم يعتبر السند الشرعي المبرر للمراقبة، ومن قبيل ذلك أن تكون هناك معلومات كافية تنذر باحتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو أن هناك معلومات تنتقل فضائيا تنذر بوقوع اعتداء على أم الدولة، وفي هذه الحالة يتم الترخيص بالمراقبة الإلكترونية.

ج: يراعى استخدام الوسيلة المذكورة في نطاق ضيق للغاية، بخصوص الوقاية من عدد محدود من الجرائم، وهي التي تمس حقوقا ذات أهمية كبيرة لاعتبارات يقدرها المشرع:

وفي هذا الإطار نجد أن المشرع الجزائري قد نص صراحة في المادة (4) على الحالات التي يجوز فيها مراقبة الاتصالات الإلكترونية، وقد تم ذكرها على سبيل الحصر، منها: احتمال اعتداء على منظومة معلوماتية تابعة لمؤسسات الدولة أو الدفاع الوطني أو النظام العام أو الاقتصاد، فضلا عن الوقاية من الجرائم الماسة بأمن الدولة، حتى يبنى على ذلك ضرورة صدور الإذن بالاعتراض والجرائم السابق ذكرها جرائم خطرة تمس أهم المجالات الحيوية المرتبطة ارتباطا وثيقا بكيان الدولة والاقتصاد الوطني وأمن المجتمع وسلامته.

إذا نخلص مما سبق إلى أن المشرع الجزائري لا يألو جهدا في محاولته مكافحة جرائم تقنية المعلومات بصفة عامة، وجرائم الاعتداء على نظم المعالجة الآلية بصفة خاصة، فقد بدأ منذ فترة ليس بالبعيدة بمواجهة هذه الجرائم، ولم يتأخر في إجراء التعديلات التشريعية في قانون العقوبات

[1] – أنظر: ج.ر.م، الفترة التشريعية السادسة، الدورة العادية الرابعة، الجلسة العلنية المنعقدة يوم السبت 27 يوليو 2009، السنة الثالثة، رقم 122، ص ص 14، 24.

في خطوة الهدف منها تطوير القاعدة القانونية لكحي تتفاعل مع العالم الافتراضي، ليصدر بعد ذلك القانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وذلك لتكييف المنظومة التشريعية بشكل كاف، ولتكريس إطار قانوني أكثر ملاءمة للجريمة التقنية، ولعل أهم ما استحدثه في هذا الإطار "عملية المراقبة الإلكترونية"، والتي إن صح اعتبارها خطوة جريئة منه على اعتبار أن هذا التدبير من أخطر الإجراءات في إطار النظام الإجرائي عبر العالم الافتراضي لكونه يمس مباشرة خصوصيات الإنسان ونظام المعالجة الآلية الذي يحتوي العالم الافتراضي مباشرة.

وبالرغم من أن البعض من الفقه[1] يرى أن المراقبة البرمجية لا تزال محل نظر في القانون من حيث ضرورة الالتزام بما هو مقرر في القانون والضمانات الدستورية للحق في الخصوصية، ذلك أن إعداد برمجيات تتولى بذاتها البحث عن الجرائم ومرتكبيها مثل برمجية كارنيفور أمر يحتاج إلى تطوير قد لا يتوافق مع الضمانات الدستورية المعاصرة، لما يشكله مثل هذا الإجراء من عدوان على الحق في الخصوصية، والذي يعد من أقوى مظاهر الحقوق الدستورية الفردية.

إلا أننا نرى وإن كانت المراقبة صح إجراء من شأنه العصف بالحريات الفردية خاصة إذا كان الأمر يخضع لمبدأ تطويع التقنية لكي تعمل في بيئة الرقابة لغرض الوقاية فقط دون أن تكون هناك جريمة قد وقعت فعلا، إلا أنه أصبح الآن ضروري في إجهاض الكثير من المشروعات الإجرامية الخطرة كتلك التي تستهدف المنظومات المعلوماتية التابعة للدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، إذ أن هذه التهديدات إن تحققت يغدو معالجة آثارها جد صعب.

وضرورة مراقبة الاتصالات الإلكترونية ترجع من ناحية إلى ازدياد معدلات الجريمة، فجرائم الاعتداء على نظم المعالجة الآلية قد سجلت في الجزائر في الآونة الأخيرة تطورات ملحوظة على حد تصريح مدير الدراسات القانونية لوزارة العدل —وإن لم يحدد نسبتها صراحة–، فإذا عزمنا على محاربتها فيجب ألا نتردد في تمكين رجال الشرطة من حمل سلاح المراقبة الإلكترونية، ومن

[1]–عمر أبو بكر بن يونس، المرجع السابق، ص 840.

ناحية أخرى إلى ازدياد استعمال المجرمين للتقنية المعلوماتية للإعداد لارتكاب اخطر الجرائم كتلك الماسة بالمجالات الحيوية المرتبطة ارتباطا وثيقا بكيات الدولة والاقتصاد الوطني وأمن المجتمع وسلامته، فإذا استخدم المجرمون الوسائل المعلوماتية ومنها البريد الإلكتروني لتسهيل ارتكاب جرائمهم، فيجب ألا نحرم الشرطة من استخدام نفس الوسيلة لمقاومة الجريمة وكشف مرتكبيها.

فالضرورة هنا تتعلق بمسألة حماية أمن البلاد والمواطن والاقتصاد الوطني من هذه الجريمة الخطيرة، وهي المسائل التي أخذها المشرع بعين الاعتبار، ومما لا شك فيه أن تلك الأخيرة تعلو على حق المشتبه فيهم في الحفاظ على حقهم في السرية أو حرمة حياتهم الخاصة المكفولة دستوريا خاصة عدم جواز انتهاك سرية المراسلات والاتصالات بمختلف أشكالها.[1]

والمسألة في النهاية تتوقف على قدرة المشرع على إقامة التوازن بين حق المجتمع في الأمن ومنع الجريمة، وحق الأفراد في السرية، وهو ما عمل على تجسيده المشرع الجزائري في القانون السابق الإشارة إليه، حيث نظم مراقبة الاتصالات الإلكترونية بقانون واضح يشمل جميع الضمانات التي تمنع تعسف القائمين عليها، ولعل ما يطمئن أكثر أن ممارسة هذه العملية تكون في ضمانة أهم الضمانات الإجرائية ألا وهي "سلطة القضاء" التي يقع عليها عاتق الالتزام بتكثيف استخدام الضمانات لصالح المتهم، ويعد ذلك ضمانة ضد افتئات أجهزة الدولة على حرمة الحياة الخاصة فغن تهاونت سلطات الضابطة العدلية في القيام بالمحافظة على هذه الضمانات حق على عملها البطلان ومن تم استبعد الدليل المستمد من هذه المراقبة، فإذا أضفنا إلى ذلك أن استخدام المعطيات المتحصل عليها جراء هذه المراقبة خارج الحدود الضرورية للتحريات يعرض صاحبها للمسؤولية الجزائية وفق ما جاء في المادة (9) من القانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والمشاهد للتوجهات التشريعية الآن يلاحظ أنها أصبحت في صف التقنية بعض الشيء في تتبع الجرائم الكبرى مثل الإرهاب وغسيل الأموال وغيرها، إذ يبدو أن نظام الرقابة الوقائية عبر الوسائل الإلكترونية بدأ يمتد

[1]- نجيمي جمال، المرجع السابق، ص 443 وما بعدها.

كنظام لإبراز قوة التقنية والتنافس في هذا المجال رغم كونه محاطا بكثير من القلق الذي يبديه رجال القانون دفاعا عن الحريات الخاصة، والحقيقة أن هذه الاعتراضات لم تكن حائلا اتجاه منطق التعامل مع نظم الرقابة الوقائية التقنية وهو ما حصل في الجزائر، لا بل أن بعض التشريعات قد تمادت في ذلك –إن صح القول– إلى حد منح مزود الخدمات صلاحية مراقبة النظام دون صدور إذن لذلك، وهو الموقف الذي جسده المشرع الأمريكي، وذلك إما في إطار المراقبة المعتادة لمزود الخدمة لتابعة عمل الشبكة (المادة (I) (A) (2) 2511§ 18U.S.C)، أو أن تكون بناءا على شكوى المشترك (القسم 18 (I) (2) 2511 .U.S.C.Sec)[1].

و مما تقدم نقول أن مراقبة وتسجيل الاتصالات الإلكترونية أمر محظور بحسب الأصل لأنه إجراء خطير يهدد حقوق وحريات الأفراد، ويفتح الباب للتعسف الذي قد يستحيل منعه واستثناء من هذا الأصل يبيح المشرع استخدام هذه الوسيلة لمنع الجريمة في حدود ضيقة تحاط بضمانات تمنع التعسف وتمكن المجتمع من الحفاظ على حقوق المجموع وإن أدى ذلك إلى التضحية بحقوق البعض الذين يفترض فيهم معاداتهم للنظام الاجتماعي.

الفرع الثالث: الإجراءات الخاصة باستخلاص الدليل التقني

أولا : اعتراض المراسلات السلكية واللاسلكية:

سبق البيان أن هذا الإجراء قد تم إدراجه من قبل المشرع الجزائري بموجب القانون رقم (06 -22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، فستحدث له الفصل الرابع تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" وقد ضمنه ستة مواد (من المادة (65 مكرر) حتى المادة (65 مكرر 10)) وتناول من خلالها مسألة السرية في استخدمها وضمانات استخدمها، وسنحاول تفصيل ذلك من خلال النقاط التالية على أن نسبق ذلك من جانبنا تحديد المقصود بهذا الإجراء.

[1] – عمر بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، د.م، 2008، ص 386 وما بعدها.

أ- المقصود باعتراض المراسلات السلكية واللاسلكية:

نستشف من نص المادة (65 مكرر 5)[1] من قانون الإجراءات الجزائية الجزائري أن المقصود باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهاته المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض.

وفي اجتماع لجنة الخبراء للبرلمان الأوروبي بستراسبورغ بتاريخ 2006/10/6 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية نجدها تعرف اعتراض المراسلات بأنها " عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم"[2].

ب- السرية في اعتراض المراسلات السلكية واللاسلكية:

إن العمليات المنصوص عليها في نص المادة (65 مكرر5) تتطلب عدم المساس بالسر المهني المنصوص عليه في المادة (45)[3] من قانون الإجراءات الجزائية المتعلق بالتفتيش، وهذا ما جاء به نص المادة (65 مكرر6) من قانون الإجراءات الجزائية وخاصة إذا تعلق الأمر بالأماكن التي يشغلها أشخاص ملزمون بكتمان السر، حيث أنه في اعتراض المراسلات لا توجد نصوص قانونية في التشريع الجزائي تشير إلى الأماكن والأشخاص الذين لا يجوز اتخاذ هذه الإجراءات في شانهم، لذلك فإنا نكتفي بالإشارة إلى الأماكن التي يشغلها أشخاص ملزمون بكتمان السر المهني والأشخاص الذين تخضع متابعتهم إلى إجراءات خاصة، في احترام السر المهني وليس استثنائها كمكتب المحامي[4] .

---

[1] أجازت الفقرة الأولى من المادة (65 مكرر 5) من قانون الإجراءات الجزائية لوكيل الجمهورية أن يأذن ب: اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية".

[2] مشار لهذا التعريف لدى: لوجاني نور الدين، أساليب البحث والتحري الخاصة وإجراءاتها وفقا لقانون رقم (22/66) المؤرخ في 2006/12/20 مداخله في يوم دراسي حول " علاقة النيابة العامة بالشرطة القضائية، " احترام حقوق الإنسان ومكافحة الجريمة" وزارة الداخلية المديرية العامة للأمن الوطني، المنعقد يوم 12 ديسمبر 2007 بإيليزي، الجزائر، ص8.

[3] راجع المادة (45) من قانون الإجراءات الجزائية الجزائري.

[4] طبقا لقانون تنظيم مهنة المحاماة تحت رقم (04/91) المؤرخ 1991/1/8 وذلك في نص المادة (80)، ونص المادة (151) من الدستور.

ومكتب الموثق[1] المحضر القضائي[2] ....

ونفس الشيء بالنسبة للأشخاص فإنه لا يوجد أشخاص مستثنون لكن نظرا لصفاتهم فإن القيام بهذه العمليات التقنية تتطلب إجراءات خاصة مثل أعضاء الحكومة، قضاة المحكمة العليا الولاة، رئيس أحد المجالس القضائية، النائب العام لدى المجلس القضائي[3]، كذلك أعضاء المجلس الشعبي الوطني ومجلس الأمة[4] أعضاء المنظمات الدولية[5]...

ومنه فإن تلك الأماكن وهؤلاء الأشخاص غير مستثنين من الإجراءات الخاصة للتحري وإنما يقتضي الأمر وجوب مراعاة الطابع السري، وتعامل خاص مع تلك الأماكن وهؤلاء الأشخاص.

ج- الضمانات المقررة لاعتراض المراسلات السلكية واللاسلكية:

مما لا شك فيه أن أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بنظام المعالجة الآلية فهو من جانب آخر يمثل انتهاكا لحرمة الحياة الخاصة للأفراد واعتداء على سرية مراسلاتهم واتصالاتهم التي كفلتها الدساتير والتشريعات العقابية، ورغبة من المشرع الجزائري لوضح حد لما قد يثار من جدال بشأنها فهو من ناحية أعطى سلطات التحقيق مكنة جديدة للبحث عن الدليل وخولها سلطة الاستعانة بوسيلة جد مهمة لا سيما في هذا العصر الذي لم يكن خافيا ما وصل إليه فيه الجناة من أساليب متطورة في تنفيذ جرائمهم وإخفاء أي أثر يدل عليهم أو يقودهم إلى قبضة العادلة، ومن ناحية أخرى، فهو لم يفتح الباب على مصراعيه في اللجوء إلى هذه الوسيلة بل كان قد أحاط استخدامها بعدد من الضمانات القانونية التي تعمل على منع تعسف السلطات العامة وتصون الحرية الفردية وتتمثل أهمها فيما يلي:

---

[1] وفقا للقانون (06/06)المؤرخ 2006/2/20 المتضمن تنظيم مهنة الموثق وذلك في نص المادة (4).

[2] بمقتضى القانون رقم (03/06) المؤرخ 2006/2/21 المتضمن تنظيم مهنة المحضر القضائي وذلك في نص المادة (7)منه.

[3] طبقا للمادة (573) من القانون الاجراءات الجزائية لا يكونون محل متابعة الا بقرار يصدر عن النائب العام لدى المحكمة العليا بعد تحقيق يجريه القاضي من أعضاء المحكمة العليا .

[4] طبقا للمواد (109)، (110)، (111) من الدستور الجزائري.

[5] جرى العرف الدولي على الاعتراف بنوع من الحصانة للمنظمات الدولية المعتمدة تدى أغلبية دول العالم.

1 – ترخيص السلطة القضائية ومراقبتها:

السلطة القضائية هي المختصة عموما بإصدار هذا الإذن وبعد ذلك ضمانة لازمة لمشروعية الاعتراض على المراسلات السلكية واللاسلكية في القانون الجزائري، فطبقا لنص المادة (65 مكرر 5) من قانون الإجراءات الجزائية لا يمكن لضابط الشرطة القضائية اللجوء إلى اجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي.

وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الترخيص أو الإذن تقدير فائدة الإجراء وجديته وملاءمته لسير الدعوى بعد الاطلاع على معطيات التحريات التي قامت لها مصالح الضبطية القضائية مسبقا في إطار تحقيق ابتدائي أو حالة جرم مشهود وعليه لا بد أن يشمل الإذن المسلم لضابط الشرطة القضائية جميع العناصر المتعلقة ب:

*** نوع الجريمة التي اقتضت ضرورة التحري أو التحقيق القضائي:**

وهي محددة على سبيل الحصر بنص المادة (65 مكرر 5) من قانون الإجراءات الجزائية ومن بينها المساس بنظم المعالجة الآلية للمعطيات.[1]

*** طبيعة المراسلة والاتصال:**

محل الاعتراض أو التصنت.

وإلى جانب المشرع الجزائري نجد المشرع الفرنسي قد كرس هذه الضمانة في المادة (100) من قانون الإجراءات الجزائية كما يلي " في المواد الجنائية والمواد الجناحية إذا كانت العقوبة تساوي أو تفوق سنتين حبس، يمكن لقاضي التحقيق إذا دعت مقتضيات البحث والتحري أن يأمر باعتراض تسجيل ونقل المراسلات التي تتم عن طريق وسائل الاتصال...."

2– فائدة الاعتراض في إظهار الحقيقة: تقرر التشريعات المعاصرة أنّ ضابط فائدة المراقبة في ظهور الحقيقة يعتبر السند الشرعي المبرر للاعتراض. ذلك بسبب هذا الاجراء يتضمن اعتداءات

[1]- سامي جلال فقي حسين، المرجع السابق، ص 283 وما بعدها.

جسيما على حرمة الحياة الخاصة وسرية الاتصالات. فيباح استثناء وفي حدود ضيقة وذلك للفائدة المنتظرة منه. والتي تتعلق بإظهار الحقيقة بكشف غموض الجريمة وضبط الجناة[1].

3- الجرائم التي يجوز فيها الاعتراض: بالرجوع إلى المادة (65 مكرر5) من قانون الإجراءات الجزائية نجد المشرع الجزائري قد نص صراحة على نوع الجرائم التي يجوز فيها مباشرة الاعتراض ومنها جرائم الاعتداء على نظم المعالجة الآلية وذلك ادراكا منه على عدم كفاية الوسائل التقليدية لجمع الدليل التقني نظرا لما تتمتع به هذه الجريمة المستحدثة من خصوصية.

3- مدّة الاجـراء:

وهي أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدرة الأمر وفقا لمقتضيات التحرّي والتحقيق. وذلك بموجب الفقرة الثانية (2) من المادة(65 مكرر) بقولها "يسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد..." وهي نفس المدة التي حددها المشرع الفرنسي في الفقرة الثانية من المادة (100)[2] .

ثانيا: حفظ المعطيات بحركة السير:

لمّا كان الدليل التقني قابع في البيئة ويتسم بخصائصها وهي خصائص تُبنى على أساس الطبيعة المرنة التي عليها العالم الافتراضي الذي هو عالم نظم المعالجة الآلية فإن للفاعل امكانية إزالته من على بعد باستخدام التقنية ذاتها، وإذا ما أضفنا إلى نقطة إزالة الدليل التقني مسألة الفوضى التي تعمّ مؤسسات تقديم الخدمات عن أرشفة المراسلات الإلكترونية لاستغلالها عند الحاجة. فإننا نكون أمام معضلة أكبر ألا وهي تخلّف الدليل نهائيا سيما حال التوصّل إلى أدلة تقليدية يمكن أن تساعد على نسبة الجريمة إلى المتهم كالاعتراف والتلبس...إلخ وما يستتبع ذلك من انتفاء الحديث عن المسؤولية الجزائية، وبالتالي لا مجال لإنزال العقاب، إذ لا أدلة ولا عقوبة

[1] -نجيمي جمال، المرجع السابق، ص 450.

[2] .Cette décision est prise pour une dur22 maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes quanditions de forme et de durée les méms conditions.

بدون إثبات. من هنا استلزم هذا الأمر وضع إطار قانوني لمعالجة هذه الفوضى، ولعل أحسن سبيل إلى ذلك هو «إتّباع نظام إلزام مزوّدي الخدمات بحفظ المعطيات".

وهذا ما تضمنه قرار الجمعية العامة الأمم المتحدة رقم (63/55) المؤرخ 22 يناير 2001 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية وذلك في الفقر " و" من المادة 1 منه والتي الزمت الدول أن تسمح بحفظ المعطيات الالكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الحصول عليها، وهو ما أكده المشرع الجزائري بموجب المادة (10) من الفصل الرابع من القانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها تحت عنوان" التزامات مقدمي الخدمات " كما يلي "في اطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية....وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أعلاه تحت تصرف السلطات المذكورة...".

وسنتناول فيما يلي تحديد مفهوم هذا الإجراء، وقبل ذلك نوضح المقصود بمزودي الخدمات باعتبارهم الحائزين لهذه المعطيات كما يلي:

أ – المقصود بمزودي الخدمات:

عرف المشرع الجزائري مزود أو مقدم الخدمة بموجب الفقرة(د) من المادة (2) من القانون رقم(09-04) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنّه:

1- أي كيان عام أو خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.[1]

1- عمر الشيخ الأصم، المرجع السابق، ص 69 وما بعدها.

2- و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعملها "[1].

وبناءاه عليه فإن المراسلة بالبريد الالكتروني والتي يتم استقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه والتي لم يطلع عليها بعد فإنها تستقر في حالة تخزين الكترونين ففي هذه المرحلة فإنّ النسخة من الاتصال المخزنة تتواجد فقط كإجراء أو وسيط مؤقت في انتظار استقبال المرسل إليه لها من مزود الخدمة، وبمجرد استلام المرسل إليه المراسلة بالبريد الالكتروني فان موقف مزود الخدمة يتراوح بين أمرين: إما أن يقوم بمسح تلك الرسالة أو أن يقوم بتخزينه، في هذا الفرض الأخير تعتبر الرسالة مخزنة لدى مزود خدمة الاتصالات الالكترونية.

وفي هذا المقام يجدر بنا الاشارة إلى أنه من الأهمية بمكان التفرقة بين مصطلحي "التحفظ على المعطيات LA conservation des données والاحتفاظ أو ارشفة المعطيات l'archivage des données، فرغم أن للكلمتين معنيين متجاورين في اللغة الشائعة لكن لهما معنى مختلف في اللغة المعلوماتية، إذ أن عبارة يتحفظ على المعطيات تعني حفظ معطيات سبق وجودها في شكل مخزن وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة، في حين أن عبارة الاحتفاظ بالمعطيات تعني حفظ المعطيات لدى حائزها بالنسبة لمستقبل المعطيات التي في طور الانتاج والتوالد، ومعنى ذلك أن أرشفة المعطيات عبارة عن عملية تخزين

[1] ويعرف قانون حماية الحياة الخاصة في مجال الاتصالات الالكترونية في الولايات المتحدة الأمريكية نوعين من مزودي الخدمات: النوع الأول" مزودو خدمة الاتصالات الإلكترونية" ويقصد به كل من يقدم خدمة الى مستخدمي الشبكة والتي تتمثل في تسهيل ارسال واستقبال الاتصالات السلكية والإلكترونية، فعلى سبيل المثال تعمل شركات الهاتف وشركات البريد الالكتروني بشكل عام كمزود خدمة اتصالات الإلكترونية، فقد لاحظ القضاء أن NETSCAPE كمزود حسابات بريد الكتروني عبر موقع NETSCAPE.NET تعد مزود خدمة اتصالات إلكترونية ECS.

والنوع الثاني هم: " مزود خدمة الحوسبة عن بعد " ويعرف حسبما جاء في القسم (2) من قانون خصوصية الاتصالات الإلكترونية الأمريكي بأنه " كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونية" عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، المرجع السابق، ص 279 وما بعدها.

وقد عرفته اتفاقية بودابست في المادة أولى(1)فقرة (ج) بأنه " كل من يقوم بخدمات الإيصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أو جهة خاصة، وقد يقدم خدماته للجمهور أو لمجموعة من المستخدمين الذين يشكلون مجموعة مغلقة".

للمعطيات على عكس التحفظ عليها الذي يعني النشاط الذي يضمن للمعطيات سلامتها وسريتها، ويبدو أن المشرع الجزائري لا يقيم أهمية لمسألة ضمان أمن المعطيات من خطر التغيير أو التجريد من صفتها أو حالتها الراهنة على عكس ما فعلت اتفاقية بودابست في المادة (16)[1]منها، ويبدو ذلك واضحا من عبارة "حفظ" التي استخدمها في المادة (11) من القانون السابق ذكره.

ب – مفهوم حفظ المعطيات المتعلقة بحركة السير:

استرشادا بما سبق ذكره يمكننا تحديد المقصود بحفظ المعطيات على أنه: "قيم مزود الخدمات بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل في انتظار اتخاذ اجراءات قانونية أخرى كالتفتيش وغيره".

لكن مما تجدر الاشارة إليه في هذا الاطار أنه ليس أي معطيات معلوماتية [2] محل اعتبار من المشرع، بل حدد المشرع الجزائري المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمات ب:معطيات المرور أو كما سماها "حركة السير"، وقد عرّف هذه الأخيرة بموجب الفقرة من المادة 2 من نفس القانون بأنّها "أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

والملاحظ على هذه الفقرة أنها قد تضمنت مصطلحات غريبة نوعا ما على القانون الجزائي، ومن ذلك(مصدر الاتصال)، ومما لاشك فيه أن هذا الأخير يشير إلى رقم التلفون مثلا، أو عنوان بروتوكول الأنترنت، أو بطريقة مماثله تحديد هوية جهاز الاتصال الدي يقوم مزود الخدمة بتقديم خدماته من خلاله. كذلك مصطلح (الوجهة المرسلة إليها) ويشير إلي جهاز الاتصال

[1] - Voir. Art 16 du C.C.C.

[2] مما تجدر الاشارة إليه أن المعطيات المعلوماتية محل التنقيب والبحث الجزائي ليست نوعا واحدا، بل لها نماذج متعددة بما في ذلك ثلاثة أنواع خاصة:1- المعطيات المتصلة بالمرور، 2-ومعطيات المحتوى، 3- ومعطيات المشترك.

الذي تتجه إليه الاتصالات المرسلة. مصطلح (نوع الخدمة) ويشير إلى نوع الخدمة المستخدمة داخل الشبكة مثل نقل ملف، بريد إلكتروني...

وبالرجوع إلي المذكرة التفسيرية لاتفاقية بودابست نجدها تشير هي الأخرى إلي شمول معطيات المرور المتعلقة باتصالات سابقة ضمن المعطيات المشمولة بإجراء التحفيظ المنصوص عليه في المادة (16) من الاتفاقية، وإن كانت هذه الأخيرة لا تتضمن ما يوجب الاحتفاظ بالمعطيات وكذا الجمع والاحتفاظ بكل او حتى بعض المعطيات المجمعة بواسطة مزود الخدمات وذلك – على حد ما جاء فيها – من أجل تحديد خط سير الاتصال بمعنى مصدر أو مكان وصول هذه الاتصالات والتي تعد من الامور الجوهرية للتعرف على هوية الأشخاص الذين أرسلوا الفيروسات مثلا أو النجاح في إتمام الوصول إلى نظام المعالجة الالية. وقد عرفت المادة الأولى فقرة (د) من اتفاقية بودابست هذا النوع من المعطيات بانها "صنف من بيانات الحاسوب التي تشكل محلا لنظام قانون محدد، حيث يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة"، وبذاك فهي تشمل طائفة من المعطيات تتمثل في مصدر الاتصال ووجهته المقصودة، خط السير ووقت أو زمن الاتصال وفقا لتوقيت غرينتش، حجم الاتصال ومدته ونوع الخدمة المؤدات.

وفي الغالب ما يجوز مزود الخدمة بمفرده معطيات المرور ما يكفي للتحديد بدقة مصدر أو نهاية الاتصال، بل إن كل واحد منهم(يحوز) يكون لديه أجزاء اللغز، ويتعين أن توضع هذه الأجزاء تحت الاختبار بقصد تحديد مصدرها والجهة المرسلة إليها[1].

[1] هذا وقد أشارت المذكرة التفسيرية لاتفاقية بودابست على ضرورة تكريس الحكومات لهذا لإجراء بما يسمح لهم من تقديم المساعدة على المستوى الدولي فيما يتعلق بالتحفظ العاجل على المعطيات المخزنة داخل حدوده، وهو ما يكفل ضمان عدم اختفاء المعطيات الجوهرية خلال الإجراءات المطلولة لطلب المساعدة القضائية المتبادلة أثناء قيام الطرف المقدم إليه الطلب من الحصول على المعطيات وإرسالها إلى الطرف مقدم الطلب أو الملتمس.

ومن ضمن معطيات المرور نجد أن المشرع الجزائري وفي المادة (11) قد حدد عدة طوائف منها، والتي تخضع لنظام قانوني واحد، بما يعني دخولها في نطاق الالتزام بالحفاظ من طرف مزود الخدمة وحصرها في:

1- المعطيات التي تسمح بالتعرف على مستعملي الخدمة

2- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

3- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

4- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

5- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

6- بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه....."

ج- التزامات مزودي الخدمات ومسؤولياتهم:

1- التزامات مزودي الخدمات بمدة معينة للتخلص من المعطيات:

بما أن حفظ المعطيات إجراء وقتي Mesure provisoire فقد لجا المشرع الجزائري واحتراما للحق في الخصوصية الى وضع التزاما على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها وذلك بعد سنة ابتداء من تاريخ التسجيل، وهو ما يستفاد بمفهوم مخالفة نص المادة (11) من القانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها كما يلي"....تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة من تاريخ التسجيل ...".

والى جانب المشرع الجزائري نجد الفرنسي الذي حرص هو بدوره على مسألة حرمة الحياة الخاصة في نطاق التخزين التلقائي للمعطيات المتعلقة بالاتصالات الالكترونية، وذلك بموجب

المادة (L1- 3 – 32) [1] من قانون البريد والاتصالات الالكترونية المضافة بموجب المادة (29) من القانون رقم (2001- 1062) المؤرخ في 15 نوفمبر 2001 المتعلق بالأمن اليومي والمعدلة بموجب المادة (20) من القانون رقم (2003 – 239) المؤرخ في 18 مارس 2003 والمتعلق بالمن الداخلي.

بل أن هذا القانون الأخير قد أورد عقوبات في حالة عدم مسح المعطيات المخزنة وذلك بموجب المادة (L3 – 39)[2] من قانون البريد والاتصالات الالكترونية المعدلة بموجب المادة (29) من قانون الأمن اليومي.

على أن الفقرة الثانية من المادة (L1 - 3- 32) من قانون البريد والاتصالات الإلكترونية اوردت استثناء على ذلك، إذ أجازت الاحتفاظ بتلك المعطيات لمدة أقصاها سنة إذا دعت مقتضيات البحث والتحقيق والمتابعة القضائية ذلك[3].

2– مسؤولية مزودي الخدمات عن التقاعس عن حفظ المعطيات:

إذا تلك هي الالتزامات المفروضة على مقدمي الخدمات التي كرسها المشرع الجزائري بموجب المادة (11) من القانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، وذلك فضلا عن الالتزامات المفروضة في دفتر الشروط، لأن مستعملي هذه الوسائل يتعاملون مع هيئات معينة ولديهم دفتر شروط يتضمن كل الالتزامات، إذن لا بد عليه أن يحترم ما نص عليه دفتر الشروط، وتقوم الادارة أو هذه الهيئة بفرض

[1] ART L32 – 3- 1 Alinéa 1 du C.P.T.E (Créé par Loi n° 2001 – 1962 du 15 novembre 2001 – art . 29 JORE 16 novembre 2001, Modifié par Loi n° 2003 – 239 du 18 mars 2003 – art. 20 JORF 19 mars 2003). dispose que ; « Les opérateurs de télécommunications, et notamment ceux mentionnés à l' article 43 – 7 de la loi n° 86 – 1076 DU 30septmbre 1986 précitée, sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dés que celle – ci est achevée, sous réserve des dispositions des II, III et IV ….. »

[2] ART L39 – 3 alinéa 1 du C.P.T.E (Modifié Loi n° 2001 – 1962 du 15 novembre 2001 – art . 29 JORE 16 novembre 2001, Modifié par Loi n° 2003 – 239 du 18 mars 2003 – art. 20 JORF 19 mars 2003). dispose que ; « Est puni d'un an d'emprisonnement et de 75000 euros d' amende (* taux *) le fait pour un opérateur de télécommunications ou ses agents ;
1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communication dans les cas opérations sont prescrites par la loi … ».

[3] Art L.32-3-1 Alinéa 2du c.p.t.e.f. dispose que. « Pour les besoins de la recherche. De la constatation et de la poursuite des infractions pénales. Et dans le seul but de permettre. En tant que de besoin. La mise à disposition de l'autorité judiciaire d informations. Il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques »

التزامات عملاقة نحو هؤلاء فاذا تخلوا عن هذه الالتزامات فالإدارة تطبق عقوبات كسحب الرخصة إضافة الى عقوبات إدارية، وإذا قصر او اهمل أحد مستخدمي هذه الوسائل الالتزامات المذكورة في دفتر الشروط بعد تطبيق العقوبات الادارية عليه تقوم بمتابعته جزائيا، لأنه في هذه الحالة يعرقل السير العادي للعدالة، وتتراوح العقوبة من 6 أشهر الى5 سنوات، إضافة الى غرامة مالية تتراوح من 50000دج الى500000دج، اما الشخص المعنوي فيعاقب بالغرامة وفقا للقواعد المقررة في قانون العقوبات[1].

والى جانب المشرع الجزائري نجد المشرع الفرنسي الذي أورد هو الآخر عقوبات على مزود الخدمات أو كما سماه " un opérateur de télécommunications"

وذلك حالة عدم حفظه المعطيات التقنية المفروض عليه تخزينها والمتعلقة بهوية المتصلين وساعة الاتصال، وذلك بموجب الفقرة الثانية من المادة (L 3 – 39)[2] من قانون البريد والاتصالات الإلكترونية.

ثالثا : تكريس هيئات للرقابة و المكافحة

لن يكون امن المعلومات الإلكترونية المتواجدة في بيئتها و المتمثلة في النظام المعلوماتي متكاملا الا من خلال تكريس هيئات للرقابة واخرى للمكافحة التي تعمل في تناسق لضمان أمن المعلوماتي سواء ا قبليا أي قبل وقوع جريمة الإعتداء عليه وفق ما تم التطرق اليه سابقا ، أو بعديا اي بعد وقوع الجريمة محل الدراسة.[3]

[1] – تنص الفقرة الأخيرة من المادة (11) من القانون رقم(09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها بانه" :دون الاخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة ن تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك الى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من 6اشهر الى 5 سنوات و بغرامة من 50000دج الى 500000دج. يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات"

[2] ART L 39 -3 ALIN2A 2 DU C.P.T.E.F DISPOSE QUE. ; « EST puni d'un an d'emprisonnement et de 75000 euros d' amende le fait pour un opérateur de télécommunications ou ses agents …
2° DE NE PAS PROCEDER à la conservation des données techniques dans les conditions ou' cette conservation est axgée par la loi ».

[3] – نعيم مغبغب ، المرجع السابق، ص 259 ما بعدها

حيث تكون تلك الحماية مستندة لهيئات خاصة او عامة، التي يوكل اليها درء كل ما من شأنه المس بالنظام المعلوماتي ، والتي نص عليها من خلال إتفاقية الإجرام المعلوماتي لسنة 2001 .

حيث تقوم السلطة المركزية بإنشاء هيئات او للرقابة يعهد اليها مراقبة جميع المؤسسات العامة في الدولة التي تستخدم أنظمة المعلوماتية و التي تنشأ بموجب قوانين تنظم كيفية انشائها وصلاحياتها .

فهي تمتع بصلاحيات واسعة في مجال عملها تمتد الى التنفيذ المباشر، فهي مستقلة في مجال عملها عن جميع السلطات وبالتالي يتوجب عليها تقديم تقارير إلى كل من السلطتين التنفيذية و التشريعية و التي لا يجوز نشرها إلاّ في الأبواب التي يحق للجمهور الإطلاع عليها .

و يعود الى هذه الهيئات أمر الترخيص للمؤسسات التي تطلب تخزين المعلومات في أنظمتها المعلوماتية، هذا ما يمكن من الرجوع إليها إذا ما تعرض النظام لإعتداء يمس به ،فهي تقوم بالعمل الرقابي بشكل مباشر، كما يقتصر دورها في أنها لجنة تقديم الشكاوى و التي تراجعها متى قدمت اليها بموجب الإعتداءات الواقعة على النظام المعلوماتي .

والحماية هنا تكون وفق تبعية تنظيمية للسلطة التنفيذية المركزية لضمان إستقلاليتها عن طريق ايجاد تشريع خاص ينظم امر تشكيل تلك الهيئة وتعيين صلاحياتها واسلوب عملها ويضمن لها استقلالية كاملة في نشاطها، ويفرض عليها تقديم تقارير دورية إلى كل من السلطتين التشريعية و التنفيذية ، من دون ان تكون خاضعة لأي ضغوط .

ويعود لهذه الهيئة تقديم الترخيص أو رفض تقديمه لمن لا تتوافر فيه الشروط اللازمة لتقديمه وتطبيق العقوبات الإدارية بحق كل من أخل بالتزاماته المعهودة اليه .

كما قد تلعب دورا استشاريا في اطار تقديمها الإرشاد والتوجيه ، أو تلقيها للشكاوى و التي تتخذ في اطارها الاجراءات المناسبة .

وبالرجوع الى الجوانب التشريعية المنظمة لتلك الهيئة نجد ان المشرع الجزائري اصدر القانون رقم 15-04 [1] بتاريخ 01 فبراير 2015 والمتعلق بتحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ومن خلال **المادة 16** من القسم الاول المعنون **بالسلطة الوطنية للتصديق الالكتروني** من الفصل الثاني المعنون **بسلطات التصديق الإلكتروني** من الباب الثالث منه المعنون ب **التصديق الإلكتروني**، قد نص من خلال المادة السابقة الذكر " **أنه تنشأ لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الإستقلال المالي، تسمى السلطة الوطنية للتصديق الإلكتروني و تدعى في صلب النص السلطة. تسجل الإعتمادات المالية اللازمة لسير السلطة ضمن ميزانية الدولة .**"

حيث يحدد مقر السلطة عن طريق التنظيم لاحقا المادة 17 . وتكلف هذه السلطة بترقية استعمال التوقيع و التصديق الإلكترونيين وضمان موثوقية إستعمالهما . وفي هذا الإطار تتولى السلطة الوطنية للتصديق الإلكتروني المهام الأتية المنصوص عليها بالمادة 18:

- إعداد سياستها للتصديق الإلكتروني ولاسهر على تطبيقها ، بعد الحصول على الرأي الإيجابي من قبل الهيئة المكلفة بالموافقة وهما السلطتين الحكومية و الإقتصادية للتصديق الإلكتروني
- إبرام إتفاقيات الأطراف المتبادل على المستوى الدولي.
- إقتراح مشاريع تمهيدية للنصوص التشريعية و التنظيمية المتعلقة بالتوقيع الإلكتروني أو التصديق الإلكتروني التي تعرض على الوزير الأول
- القيام بعمليات التدقيق على مستوى السلطتين الحكومية و الإقتصادية للتصديق الإلكتروني ععن طريق الهيئة الحكومية المكلفة بالتدقيق .
- تتم إستشارة السلطة عند إعداد أي مشروع تشريعي أو تنظيمي متصل بالتوقيع أو التصديق الإلكترونيين.

[1] القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين الصادر في 01 فبراير 2015 جريدة رسمية عدد 06 الصادرة في 10 فبراير 2015

كما نصت المادة 19 على أن السلطة تتشكل من مجلس ومصالح تقنية و إدارية حيث ألزمت المادة أعلاه تعيين أعضاء المجلس وعددهم 5 من بينهم الرئيس ، من قبل رئيس الجمهورية و يالذين يختارون على أساس كفاءاتهم ، لاسيما في مجال العلوم التقنية اللنتعلقة بتكنولوجيا الإعلام والإتصال ، وفي مجال قانون تكنولوجيا الإعلام و الإتصال ، وفي إقتصاد تكنولوجيا الإعلام و الإتصال.

كما يتمتع المجلس بجميع الصلاحيات اللازمة لأداء مهام السلطة ، وبهذه الصفة يمكن للمجلس الإستعانة بأي كفاءة من شأنها مساعدته في أشغاله .

وتحدد عهدة أعضاء المجلس بأربع سنوات قابلة للتجديد مرة واحدة .

كما تم إنشاء السلطة الحكومية للتصديق الإلكتروني و هي المنصوص عليها في القانون 15-04 ضمن القسم الثاني من الفصل الثاني المشار اليه اعلاه و هو ما نلمسه بالمادة 26 منه التي تنص على " **تنشأ لدى الوزير المكلف بالبريد و تكنولوجيا الإعلام و الإتصال سلطة حكومية للتصديق الإلكتروني تتمتع بالإستقلال المالي و الشخصية المعنوية.**"

تحدد طبيعة هذه السلطة وتشكيلها و تنظيمها و سيرها عن طريق التنظيم **المادة 27**.

وتكلف هذه السلطة بمتابعة ومراقبة نشاط التصديق الإلكتروني وتوفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي ، وهو ما نصت عليه **المادة 28** التي وضحت مهام السلطة الحكومية من خلال المهام التالية :

- إعداد سياستها التصديق الإلكتروني التي تعرض على السلطة الوطنية للموفقة عليها ، كما تسهر على تطبيق تلك السياسة .
- الموافقة على سياسات التصديق الصادرة عن الأطراف الثلاثة الموثوقة و السهر على تطبيقها .
- الإحتفاظ بشهادات التصديق الإلكترونية االمنتهية صلاحياتها، والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق ، بغرض تسليمها الى السلطات القضائية المختصة ، عند الإقتضاء طبقا للأحكام التشريعية و التنظيمية المعمول بهما .

- نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة الوطنية .
- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة الوطنية دوريا أو بناء على طلب منها .
- القيام بعملية التدقيق على مستوى الطرف الثالث الموثزق عن طريق الهيئة الحكومية المكلفة به طبقا لسياسة التصديق.

هذا بالاضافة الى انشاء السلطة الإقتصادية للتصديق الإلكتروني المنصوص عليها **بالمادة 29** من القسم الثالث من الفصل الثاني المشار اليه اعلاه حيث تنص على " **تعين السلطة المكلفة بضبط البريد و المواصلات السلكية و اللاسلكية في مفهوم هذا القانون ، سلطة اقتصادية للتصديق الإلكتروني.**"

حيث تكلف هذه السلطة بمتابعة ومراقبة مؤديي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع و التصديق الإلكترونيين لصالح الجمهور وهو ما نصت عليه **المادة 30** والتي أوكلت لها المهام التالية :

- إعداد سياستها للتصديق الإلكتروني التي تعرض على السلطة الوطنية للموافقة عليها ، والسهر على تطبيقها .
- منح التراخيص لمؤديي خدمات التصديق الإلكتروني بعد موافقة السلطة الوطنية .
- الموافقة على سياسات التصيق الصادرة عن مؤديي خدمات التصديق الإلكتروني والسهر على تطبيقها .
- الإحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها ، والبيانات المرتبطة بمنحها من طرف مؤديي خدمات التصديق الإلكتروني بغرض تسليمها إلى السلطات القضائية المختصة عند الإقتضاء طبقا للأحكام التشريعية والتنظيمية المعمول بها .
- نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة الوطنية .
- إتخاذ التدابير اللازمة لضمان إستمرارية الخدمات حالة عجز المؤدي للخدمة .

- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة الوطنية دوريا أو بناء على طلب منها .
- التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الإلكتروني بنفسها أو عن طريق مكاتب معتمدة .
- اسهر على وجود منافسة فعلية ونزيهة بين مؤديي خدمات التصديق الإلكتروني بإتخاذ كل التدابير اللازمة لترقية أو إستعادة تلك المنافسة .
- التحكيم في النزاعات القائمة بين مؤديي خدمات التصديق الإلكتروني.
- مطالبة مؤديي التصديق الإلكتروني أو كل شخص معني بأي وثيقة أو معلومة تساعدها في تأدية المهام المخولة لها .
- إعداد دفتر الشروط امحدد لشروط وكيفيات تأدية التصديق الإلكتروني وعرضه على السلطة الوطنية للموافقة عليه .
- إجراء كل مراقبة لسياسة التصديق الإلكتروني ودفتر الشروط .
- إصدار التقارير و الإحصائيات العمومية والتقرير السنوي المتضمن وصف نشاطاتها مع إحترام مبدأ السرية .
- القيام بتبليغ النيابة العامة بكل فعل ذي طابع جزائي يكتشف بمناسبة تأدية المهام .

قرارتها ذات صفة إدارية قابلة للطعن أمام السلطة الوطنية في أجل شهر واحد يبتدأ من تاريخ التبليغ به ، ولا يكون لهذا الطعن أثر موقف بينما القرارات المتخذة من طرف السلطة الوطنية فهي قابلة للطعن أمام مجلس الدولة في أجل شهر واحد يبتدأ من تاريخ التبليغ ولا يكون لهذا الطعن أثر موقف ، **المادتين 31 و 32** .

ب – هيائات المكافحة

المرسوم الرئاسي رقم 261-15[1] المحدد **لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها** الصادر بتاريخ 08 اكتوبر 2015

وهي الهيئة المنصوص عليها بالقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث أنها سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وتضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية. وتكلف بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال وضمان مراقبة الاتصالات الالكترونية .

وبخصوص مجال عملها و وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائرية و في هذا المرسوم و مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

[1] المرسوم الرئاسي رقم 261-15 المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها الصادر بتاريخ 08 اكتوبر 2015 الجريدة الرسمية عدد 53 الصادرة بتاريخ 08 اكتوبر 2015

و إذا كنا قد تطرقنا في بحثنا هذا لتأصيل جرائم الإعتداء على النظام المعلوماتي لأهم أشكال الجرائم المتعلقة بالمعلومات و التي تقع عليه ، و التي هي في إتساع و تزايد نتيجة للتطور في تكنولوجيا الإتصال و المعلومات ، لما للتقنية الحديثة من أثر على قيمة المعلومات المتداولة عبرها و هويتها ،حيث عاد اختراق الجوانب الأمنية للمعلوماتية وتكسير حواجزها التي تحمي المعلومة بشكلها الجديد، هذا الذي جعلت الرؤية تتغير للحذر من تلك الإعتداءات التي تمسها محاولة لفهم مضمونها و صبغتها بصبغة تشريعية لتوفير جانب وقائي في ظل عجز التأمين التقني لها .

حيث تغيرت المفاهيم التقليدية التي كانت سائدة، بدخول التكنولوجيا في مختلف المجالات ، كالصيرفة الإلكترونية ، والحكومة الإلكترونية والاقتصاد الرقمي والنقود الإلكترونية... مما جعلنا نعيش عصر الرقمنة .

وإذا كانت خطورة تلك الجرائم له أثره على الدول صاحبة التكنولوجيا ، إلا أن تلك الخطورة لم تسلم منها حتى الدول النامية التي إستخدمت تلك التكنولوجيا لمساعدتها في النمو ، فخطر تلك الجرائم يمكن أن يكون كبيرا إذا كانت الإستراتيجية الموضوعة لمواجهتها ليست بالمستوى المطلوب، ونتيجة لهذا الوضع كان لابد من اتخاذ مسألة أمن المعلومات ومكافحة هذا الإجرام أكثر جدية من طرف الحكومات، و لمسايرة هذه الممارسات قامت العديد من الدول بسن قوانين خاصة لمواجهة هذه الجرائم الجديدة، حيث نجد أن الجزائر كباقي الدول قامت هي الأخرى بسد الفراغ القانوني في هذا المجال بإصدارها القانون رقم (04-15) الصادر في 10 من نوفمبر 2004 ، المعدل والمتمم للأمر رقم (66-156) المتضمن قانون العقوبات الذي تناول فيه بالتجريم مختلف الاعتداءات على نظم المعالجة الآلية ومعلوماتها، و الذي عززه بالقانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و القوانين اللاحقة عليه كالقانون 15-03 و القانون 15-04 المتعلقين بالتصديق و التوقيع الإلكترونيين ، مسايرا في ذلك المشرع الجزائري للتطورات التكنولوجية والعلمية، مما يجعل الجزائر في صدارة البلدان التي تفاعلت مع تلك التطورات التقنية الجديدة .

و مع ذلك إن كانت القوانين الصادرة و المطبقة قد تضمنت الأنواع الجديدة من الجرائم المستحدثة ،فصعوبة إثبات جرائم الاعتداء على نظم المعلوماتية بالنظر إلى طبيعة الدليل الذي يتحصل منها، فضلا على الحاجة إلى المعرفة العلمية والفنية والتي قد لا تتوافر لدى رجال القانون فبرغم الجهود التي بذلت ولا تزال تبذل، فإن هذه التحديات تبقى عصية على الحل في كثير من الأحيان في غياب إستراتيجية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها لاسيما في الدول التي لم تبادر بعد إلى تعديل تشريعاتها بما يكفل تجاوز القوالب القانونية التقليدية التي لم تعد تتناسب هذا العصر .

وهكذا تحددت إشكالية هذا البحث في تأصيل تلك الجرائم و تحليل الإستراتيجية التي اتبعها المشرع الجزائري للحماية من هذه الجرائم ومكافحتها ومدى نجاحها بالمقارنة مع التشريعات التي أكست نظم المعالجة الآلية الحماية على غرار المشرع الجزائري .

ولقد توصلنا من خلال هذه الدراسة إلى النتائج والتوصيات التالية:

أولا، النتائج

1. أن جرائم الإعتداء على النظام المعلومات التذي يكون بيئة لتواجد المعلومات الإلكترونية بأنه "**كل سلوك متعمد ، يشكل اعتداء على المعلومات الإلكترونية ضمن بيئة إلكترونية ، يجرمه المشرع ويقرر له عقابا ، اذا صدر عن شخص مسؤول جنائيا .**"

2. إن محل جرائم الاعتداء على المعلومات هو نظام المعلوماتية بمكوناته غير المادية، أما مكوناته المادية فالاعتداء عليها مجرم بنصوص التجريم التقليدية .

حيث ينصرف مدلول تلك المكونات غير المادية للنظام إلى المعلومات بدلالتها الواسعة المنصرفة لتشمل جميع المعلومات التي تمت معالجتها من نصوص أو صور أو أصوات أو رموز أو برامج ومهما كانت الحالة التي تكون عليها سواء كانت معلومات مدخلة (معطيات) معلومات معالجة، مخزنة أو في طور النقل والتبادل ضمن وسائل الاتصال المندمجة مع نضام الحوسبة ».

أما مصطلح نظام المعلوماتية فيستخدم للدلالة على مفهومه العلمي «أي نظام مهما كان مسماة يتوافر له عدة عناصر مرتبطة ببعضها بعدد معين من الروابط لتحقيق المعالجة الآلية للمعلومات».

3. إن هدف التدابير التشريعية و وسائل امن المعلومات ضمان توافر ثلاثة عناصر أساسية للمعلومات ونظم معالجتها هي: الإستئثار، الجدية والسلامة .

4. أهم مميزات جرائم الاعتداء على نظم المعلوماتية هو استهدافها للمعلومات بأشكالها المتباينة في البيئة الإلكترونية وليست ذات الكيان مادي، وعلى ذلك لم تخلو الحماية الجزائية من صعوبة باعتبار أن جل النصوص الجزائية جاءت للتعامل مع وضعيات مادية ملموسة، وبالتالي فإن الاعتداء على هذه القيم المعنوية يخرجها من مناط الحماية الجزائية لا سيما وأن القياس محظور ولا يجوز التوسع في تأويل النص الجزائي ، خاصة و أن المصالح المرتبطة بها أغلبها جديدة.

وعلى ذلك فقد توصلنا إلى أن من أهم لدواعي هو تدخل المشرع لإصدار نصوص تحظر الاعتداء على نظم المعلوماتية في التشريع الجزائري القائمة على الإحاطة بكافة أشكال الاعتداءات التي تقع على مكوناتها غير المادية، خاصة مع العجز الذي كان يشوب التشريع في مواجهتها للجرائم التي كانت ستترتب عليه آثار خطيرة، نتيجة إرتكاب أفعال غير مشروعة ويفلت أصحبها من العقاب بسبب عدم وجود نصوص يجرمها ، أو قد يتوسع القضاء في تفسيره للنصوص العقابية القائمة بحيث يتم المساس بمبدأ شرعية الجرائم والعقوبات، لهذا فتدخل المشرع الجزائي لتوفير هذه الحماية ، تضمن أن تتم التعاملات الإلكترونية في أمان، وفي حالة حدوث إعتداء فإن التشريع يكفل حفظ حقوق المتضرر منه ، وإيقاع العقوبة بالمجرم .

5. أما بالنسبة لآلية التدخل التشريعي لمواجهة جرائم الاعتداء على نظم المعلوماتية ، فقد اختلفت التشريعات فيها، فبعضها ذهبت إلى إضافة حالات الاعتداء على نظم المعلوماتية إلى النصوص القائمة، أو تعديلها لتحتوي تلك الإعتداءات ، واتجهت تشريعات أخرى إلى وضع نصوص جديدة ضمن تشريع مستقل أو ملحق بالتشريع الجزائي، وكثيرا ما اعتمدت الوسيلتين معا ، حيث نجد أن المشرع الجزائري جرم الإعتداء على نظم المعالجة الآلية في قسم خاص في قانون

العقوبات وهو القسم السابع مكرر المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات" ، تماشيا مع الرؤية التشريعية التي إنتهجها المشرع الفرنسي حماية للمصالح المختلفة التي تتعلق بالمعلومات ونظمها .

6. يلزم الاستعانة في تحديد المقصود بالدخول بالتوسع في مفهوم «أي تفاعل ناجح مع النظام» دون أهمية لصغر هذا التفاعل، وذلك لتجنب حصر الدخول في إطار محدود في نطاق التشريعات التي جرمت الدخول غير المشروع من دون أن تتولى مسألة تحديد مدلولها، وهو الوضع في التشريع الجزائري والفرنسي .

7. يثير تحديد مفهوم الدخول إلى نظام المعالجة الآلية إشكالات عدة تتمحور حول عنصرين يعتبران مناط تجريم هذا الفعل بحيث يشكل تحديدهما على وجه الدقة بيانا للسلوك المجرم، يتجلى العنصر الأول في تحديد الأشخاص المخول لهم بالدخول إلى النظام أما العنصر الثاني فيتأتى من تحديد حالات عدم التصريح بالدخول .

8. تذهب بعض التشريعات الجزائية إلى النص على تجريم فعل الدخول الذي قد ينصرف إلى الدخول أو البقاء أو اعتراض النظم ، في حين تفرق تشريعات أخرى بين هذه الاعتداءات وتفرد لكل منهم نصا خاصا، و وجدنا أن المشرع الجزائري جمع المشرع فعلي الدخول والبقاء غير المشروعين داخل النظم في نص تجريمي واحد لم لا و أنه دل عليها بمصطلحين مختلفين ولم يشر إلى فعل الاعتراض منتهجا في ذللك درب المشرع الفرنسي، إلا أنه أعطى في المقابل مفهوم موسع لجريمة الدخول غير المشروع لنظم المعالجة الآلية ليمتد ليشمل الالتقاط غير المشروع والاعتراض غير المشروع للمعلومات أثناء انتقالها باعتبار أنها في النهاية تمثل انتهاك لاتصال معلوماتي بين النظم المختلفة أثناء عملها .

9. جرمت أغلب التشريعات المقارنة البقاء غير المصرح به إلى جانب الدخول غير المصرح به حتى لو لم يصحب إتيانهما أي مساس بمكونات النظام ، أي تم اعتبارها جريمة شكلية لا علاقة لها بالاعتداء على المعلومات، فبمجرد الولوج أو البقاء غير المشروع يعد فعلا مجرما إذ يمهد

للاعتداء على المعلومات، وهو الوضع السائد في كل من التشريع الجزائري والفرنسي، وتوصلنا إلى أن مفهوم البقاء ينصرف إلى الحالة التي يبقى فيها الجاني داخل النظام بصفة غير مشروعة بعدما تحقق دخوله عن طريق الصدفة أو الخطأ ليخرج من مفهومه ما دون ذلك من الحالات التي يكون فيها دخوله مشروطا بزمن محدد وحدث تجاوز لهذا الزمن وان كان ثمة مجال لأن تطبق على الجاني جريمة أخرى لم يتناولها المشرع الجزائري بالتجريم وهي جريمة الاستعمال غير المصرح به لنظام المعلومات.

10. بالنسبة لمحل الحماية الجزائية في جريمة الدخول أو البقاء غير المصرح بهما تبين لنا أن المشرع الجزائري قد وسع من نطاق الحماية وذلك حينما جرم فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من النظام وذلك بموجب المادة 394 مكرر، وهو ما يسمح باستيعاب المعلومات خلال مرحلة المعالجة والتخزين والاسترجاع، و التي يتضمنها فضلا عن الشبكات ذاتها أو المعلومات المنقولة عبرها وبالتالي يشمل تجريم الاعتراض غير المشروع للاتصالات سواء من خلال الدخول إلى هذه الشبكات أو من خلال التقاط الإشارات التي يحدثها جهاز إلكتروني من خلال وسائل التقاط إلكترونية. وهو نفس الاتجاه الذي سلكه المشرع الفرنسي.

11. لاحظنا من خلال دراستنا للاتجاه التشريعي المعتنق من قبل المشرع الجزائري جنوحا تشريعيا باتجاه التشدد في الحماية الجزائية لنظام المعلوماتي ، و نلاحظ ذلك في المصطلحات المرنة المعتمدة فضلا عن التوسع بالركن المادي للدخول والبقاء و الغاية من ذلك توسيع مجال الحماية.

12. بالنسبة لجريمة التلاعب غير المصرح به بالمعلومات التي جرمها المشرع الجزائري بعد جريمة الدخول أو البقاء بموجب المادة 394 مكرر1، فإن الإطار العام للنص لم يميز نوعية المعلومات وما إذا كانت معلومات تتصل بالشخص أو بمصالح اقتصادية أو مالية أو مسائل أمنية أو غير ذلك، ولعل مرد هذا الاتجاه السعي لتعميم حماية المعلومات بكافة أنواعها، كما أنه جاء شاملا لكل أنواع وسائل التلاعب بالمعلومات، أي قام بتجريم كل ما يؤدي إلى تغيير حالة المعلومات بغير

تصريح وذلك بإدخال معلومات جديدة عليها غير مصرح بإدخالها أو تعديل أو إزالة غير مصرح بها لمعلومات موجودة داخل نظام المعالجة الآلية .

13. بالنسبة لجريمة إفساد النظام المعالجة فقد آثر المشرع الجزائري عدم النص عليها كجريمة خاصة عمديه، وإنما اكتفى باعتبارها ظرف مشدد لجريمة الدخول والبقاء غير المصرح بهما، وذلك نتيجة للتشابه الكبير بينها وبين جريمة التلاعب بالمعلومات، بحيث يصعب في كثير من الأحيان التمييز بينهما وذلك لأن الأفعال التي تتضمنها جريمة التلاعب غير المصرح به للمعلومات تؤدي هي الأخرى إلى إعاقة النظام وإفساده بخلاف الأمر نجده في بعض التشريعات المقارنة مثل التشريع الفرنسي حيث وجدناه يجرم هذه النتيجة كظرف تشديد غير مقصود المادة 323-1من قانون العقوبات الفرنسي وكجريمة خاصة مقصودة هي إعاقة أنظمة المعالجة الآلية (والتي نصت عليها المادة 323-2 من قانون العقوبات الفرنسي).

14. أظهر البحث كذلك أن التلاعب بالمعلومات بالإدخال والإزالة والتعديل يعد من أهم الأساليب المستعملة في ارتكاب الاحتيال المعلوماتي بمجالاته المختلفة، بما في ذلك أنظمة التحويل الإلكتروني للأموال أو البطاقات الممغنطة وأجهزة الصرف الآلي، لم لا أن هذا التكييف لا يلعق مجرد التلاعب بالمعلومات بذاتها بل يجب أن يكون هدف الجاني من خلاله إلى استخدامه في تحقيق ربح مادي غير مشروع وهو ما يثير في هذه الحالة مسألة تعدد الجرائم، أما إذا ما تم مجرد التلاعب في القيم المالية في صورة إدخال أو إزالة أو تعديل للمعلومات فحسب، فلا يرتقي هذا السلوك إلى مستوى النصب، بل يشكل جريمة مستقلة موضوعها التلاعب في القيم المالية .

15. بالنسبة للمعلومات التي ينصب عليها السلوك الإجرامي في جرائم التلاعب غير المصرح به للمعلومات، فوجدنا أن تشريعات الجزائر وفرنسا تحدد محل محدد وهو المعطيات التي تمت معالجتها آليا والموجودة داخل نظام المعالجة الآلية، ليخرج بذلك من نطاقها مادون ذلك من المعلومات غير المعالجة، أو المنفصلة عن النظام، أو محررات النظام ، وإن كان في الحالة الأخيرة ثمة مجال لأن

يعاقب على جريمة «تزوير المستندات المعلوماتية واستعمالها متى توافرت أركانها» والتي لم يفرد لها المشرع الجزائري نصا خاصا وذلك على خلاف المشرع الفرنسي.

أما ما يخص المعلومات المنقولة عبر نظم المعالجة الآلية، فقد وجدنا أنه في حين ذهبت بعض التشريعات إلى الإشارة صراحة إلى حماية المعلومات من أفعال التلاعب في هذه الحالة، لم تتضمن تشريعات أخرى التحديد السابق، وإن كانت العبارات الوارد بها اتسمت بالعموم بما يسمح بإدراج المعلومات المنقولة عبر النظم ضمن مظلتها، وهي السياسة التي اتبعها المشرع الجزائري منتهجا في ذلك نهج المشرع الفرنسي.

16. بالنسبة لجريمة التعامل في معلومات غير مشروعة، فقد تبين لنا أن بعض التشريعات المقارنة ونعني بالذكر المشرع الفرنسي واتفاقية بودابست قد هدفت من خلال تجريمها إلى الحيلولة دون ارتكاب أي من جريمتي الدخول أو البقاء غير المصرح بهما أو جريمة التلاعب بالمعلومات وذلك من خلال تجريمها للتعامل في معلومات صالحة لارتكاب جريمة من الجرائم محل الدراسة، في حين وجدنا أن المشرع الجزائري قد انفرد عنهما بإضافته صورة أخرى للتعامل في المعلومات غير مشروعة وهي التعامل في معلومات متحصلة من جريمة، إذ لا نجد لهذه الصورة الأخيرة ذكرا لا في القانون الفرنسي ولا في اتفاقية بودابست.

ووجدنا أن هدفه من وراء تجريمها يتمثل في عدم استفادة الجاني من مشروعه الإجرامي وفي التقليل والتخفيف من الآثار ومن الضرر الذي يمكن أن يترتب على ارتكاب إحدى الجرائم السابقة.

17. بالنسبة للمحل الذي ينصب عليه السلوك الإجرامي في جريمة التعامل في معلومات غير مشروعة، فوجدنا أن المشرع الجزائري قد قرر أن يقع السلوك على المعلومات المخزنة، المعالجة والمرسلة، في حين اتضح لنا أن بعض التشريعات الجزائية المقارنة الأخرى كانت أكثر توسعا في ذلك عندما نصت على التجهيزات أو الأدوات (الوسائل المادية) والبرامج والعمليات (الوسائل غير المادية) وهو الوضع في التشريع الفرنسي، لكن في مقابل ذلك وجدنا أن هذا الأخير حد من هذا التوسع عندما تطلب أن تكون الوسائل مصممة خصيصا لارتكاب واحدة أو أكثر من جرائم

الاعتداء على نظم المعالجة الآلية في حين وجدنا أن المشرع الجزائري قد اكتفى فيها أن تكون صالحة أو قابلة لأن ترتكب بها الجريمة فحسب.

18. فيما يتعلق بأحكام العقاب على الجرائم معل البحث فقد وجدنا أن :

أ) كل من التشريع الجزائي الجزائري والمقارن (المشرع الفرنسي واتفاقية بودابست...) يجمع على فاعلية العقوبة بوصفها الإطار التنظيمي الوقائي الرادع الذي يحيط بهذه النظم، فتكريس عقوبات رادعة يجعل التفكير بالاعتداء، على هذه النظم من قبل العابثين أمرا في غاية الصعوبة، كما يضمن أمن المعلومات وعناصرها.

ب) العقوبات التي نص عليها المشرع الجزائري هي عقوبات ذات حدين حد أدنى وحد أعلى مما يعني هذا إمكان القاضي من إعمال السلطة التقديرية بين هذين الحدين وهذا على نقيض المشرع الفرنسي الذي نص على عقوبة ذات حد واحد وبالتالي إبعاد القاضي من إمكانية إعمال السلطة التقديرية.

ت) بالنسبة لظروف التشديد، فقد نص المشرع الجزائري على ظرف مشدد لعقوبة الاعتداء على نظم المعلوماتية وذلك تبعا لصفة المجني عليه، بحيث متى استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، تشدد العقوبة إلى الضعف لما يشكله هذا من تهديد لأمن الوطن والمؤسسات أو الهيئات العامة ، ولا نجد مثيلا لهذا الظرف المشدد لا في القانون الفرنسي ولا في اتفاقية بودابست.

أما الظرف المشدد الثاني فيكون تبعا للنتيجة المترتبة بحيث تشدد عقوبة جريمة الدخول أو البقاء غير المصرح به في التشريع الجزائري في حالتين:

الحالة الأولى: إذا نجم عن هذا الدخول أو البقاء حذف أو تغيير لمعلومات المنظومة.

الحالة الثانية: إذا نجم عن الدخول أو البقاء تخريب لنظام اشتغال المنظومة، أما بخصوص المشرع الفرنسي فقد جعل – بدوره – من جسامة النتيجة ظرفا مشددا لعقوبة جريمة الدخول أو البقاء،

غير المشروع، ولكنه لم يرفعها إلى الضعف كما فعل المشرع الجزائري وتوصلنا إلى أن ذلك راجع إلى سببين:

أولا: أن عقوبة الجريمة البسيطة تضاعفت ولا يمكن مضاعفتها مرة أخرى بالنسبة للجريمة المشددة.

ثانيا: هو استجابة لانتقاد الفقه بوجود فارق كبير بين العقوبة البسيطة والمشددة.

بدراسة هذه الظروف توصلنا إلى توحد نظرة التشريعات في تقدير جسامة الدخول أو البقاء غير المصرح به اخل نظم المعلوماتية، فالتشريع الجزائري اعتبرها جناية هذا حتى لو اقترنت بظروف التشديد، وكذلك هو الوضع في التشريع الفرنسي.

ت) تبنت معظم التشريعات الجزائية « مبدأ المسؤولية الجزائية للشخص المعنوي»، في نطاق جرائم الاعتداء على نظم المعالجة الآلية إلى جانب المسؤولية الجزائية للأشخاص الطبيعية وهذا في كل من التشريع الجزائري المادة 394 مكرر3، التشريع الفرنسي المادة 323-6 اتفاقية بودابست (المادة (12) تحت عنوان مسؤولية الأشخاص المعنوية)...

ج) بالنسبة لنطاق العقوبة، فقد تبين لنا أن المشرع الجزائري – على غرار المشرع الفرنسي- ورغبة منه في قطع دابر الجريمة والقضاء على الشر في شرنقته من جهة، وتقديرا لخطورة هذا النوع من الجنح من جهة أخرى وسع من نطاق العقوبة لتشمل من حيث الأفعال أعمال البدء بالتنفيذ، ومن حيث الأشخاص تشمل الأشخاص الذين يشاركون في التحضير لجنح نظام المعالجة الآلية في إطار اتفاق جنائي .

19. بالنسبة للعقوبات التكميلية فقد تبين لنا أن المشرع الجزائري قد نص على المصادرة والغلق كعقوبة تكميلية وجوبيه للعقوبة السالبة للحرية في جرائم الاعتداء، على نظم المعالجة الآلية، وهو مسلك حسن لأثره الشخصي (في نفسية الفاعل) والموضوعي في فعالية مواجهة هذا النوع من الجرائم، وهو نفس المسلك الذي اتبعته بعض التشريعات المقارنة كالتشريع الفرنسي، غير أن هذا الأخير وفضلا عن عقوبة الغلق والمصادرة كان قد نص على غيرها من العقوبات التكميلية الوجوبية سعيا منه لتحقيق مبدأ تفريد العقوبة .

20. لا بد من اتخاذ مسألة أمن المعلومات من الناحية التقنية بشكل أكثر جدية، والبحث عن طرق وأساليب جديدة لمكافحة الجريمة التقنية والحد من انتشارها، وهي وظيفة خبراء أمن المعلومات فضلا عن رجال الصناعة وهذا ما أكدت عليه المذكرة التفسيرية لاتفاقية بودابست، هذا من جهة .

ومن جهة أخرى تطويع التقنية لكي تعمل في بيئة الرقابة لفرض الوقاية، لكن بدون أن تتعرض حقوق الأفراد وحرياتهم للخطر، وهو ما تفطن له المشرع الجزائري، فقد وجدناه قد استحدث إجراء المراقبة الإلكترونية كوسيلة وقائية قانونية، وقد كان ذلك بموجب المادة 3 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

21. الدليل التقني عبارة عن معلومات مخزنة في النظم وملحقاتها، أو متنقلة عبرها، من الممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة لتظهر في شكل مخرجات ورقية أو الكترونية أو معروضة على شاشة النظم أو غيرها من الأشكال، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها .

22. التكنولوجيا أثرت على طبيعة الجرائم المرتكبة نتيجة لاستخدام تقنيتها العلمية و التي عقدت الدليل التقني وقواعد استخلاصه، بحيث أن ذلك قد أثر على القواعد الإجرائية التقليدية للحصول عليه فعجزت عن تنظيم الوضع القانوني للوصول إلى الدليل الذي يكفي لإثبات هذا النوع من الجرائم .

23. و من خلال الطبيعة الخاصة لجرائم الاعتداء على نظم المعلوماتية وإستقلاليتها لذى فالدليل التقني تطلب من المشرع إعادة تقييم منهجه الخاص بالقواعد الإجرائية التقليدية الموضوعة للتعامل مع وضعيات مادية كالتفتيش والضب في قانون الإجراءات الجزائية على ضوء ما أسفرت عنه تطورات العلم والتقنية سيما في مجال ثورة المعلومات فضلا عن استحداث نوع من القواعد الإجرائية تتلاءم والطبيعة التقنية والفنية التي عليها هذه الجرائم والدليل المستنبط منها، إذ وجدنا من خلال دراستنا أن المشرع الجزائري قد نظم الوضع القانوني للتفتيش والضبط في البيئة التقنية

إيمانا منه بقصور القواعد التقليدية في مواجهة هكذا جرائم، فضلا عن استحداثه إجراءين يتم الاعتماد فيهما على تقنية تكنولوجيا المعلومات في مجال استخلاص الدليل التقني، الأول: وهو المراقبة الإلكترونية والثاني: حفظ المعطيات المتعلقة بحركة السير، وقد كان ذلك بموجب القانون رقم 09-04 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

24. يضع المشرع الجزائري التزاما على مقدمي الخدمات بإزالة المعطيات لتي يتم تخزينها تلقائيا وذلك بعد سنة ابتداء من تاريخ التسجيل.

25. استحدث المشرع الجزائري لإجراء التسرب واعتراض الاتصالات السلكية واللاسلكية كوسيلة لمواجهة جرائم الاعتداء على نظم المعلوماتية ، وقد كان ذلك بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، وذلك بشأن ملاحقة هذه الجرائم.

26. إن الوسائل العلمية وإن كانت تفيد في كشف الحقيقة عن الجريمة وإقامة الدليل على الجاني، فإنها قد تعصف بعقوق الأفراد وحرياتهم إذا لم يحسن استخدامها...

27. تمثل الاتصالات الإلكترونية أحد أوجه الحياة الخاصة للإنسان، و لهذا عاقب المشرع الجزائري على اعتراض الاتصالات السلكية واللاسلكية دون إذن بذلك وذلك بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر2006 المعدل والمتمم لقانون العقوبات.

بينما تتمثل الثانية في إبطال التسجيلات التي تتضمنها وإهدار قيمة الدليل المستمد منها .

28. أظهر البحث كذلك عدم كفاية القواعد التقليدية أو المستحدثة لاستخلاص الدليل التقني إذ تعوق تطبيقها في كثير من الأحيان صعوبات قانونية وعملية عديدة وتضعف قيمتها في استنباطه، وهي في الحقيقة صعوبات تتعلق بالطبيعة التكوينية للدليل التقني وأخرى تتعلق بالعامل البشري.

29. منح المشرع الجزائي الجزائري القاضي الجزائي دورا ايجابيا من حيث قبول الدليل أو تقدير قيمته الإثباتية، إذ فسح له المجال أمامه لكي يستلهم عقيدته من أية وسيلة أو دليل يطمئن إليه

وجدانه ويرتاح إليه ضميره، ولم يختلف الأمر بالنسبة للدليل التقني حيث لم يتضمن القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها أية أوضاع خاصة بهذا الصدد، ومن ثم فإن الدليل التقني مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والإثبات في مجال الجرائم الاعتداء على النظم بصفة خاصة، وهذا مظهر من مظاهر اعتناق المشرع لمبدأ حرية الإثبات والاقتناع وهو ليس بالوضع السائد في التشريع الجزائري بل في جميع القوانين ذات الصياغة اللاتينية مثل القانون الفرنسي، وغيره من القوانين المتأثرة .

30. تتمتع الأدلة التقنية بقيمة علمية قاطعة في الدلالة على الحقائق التي تتضمنها، باعتبار علميتها وموضوعيتها وحيا<ها وكفاءتها، ويمكن التغلب على مشكلة الشك في مصداقيتها في مجال المعالجة الآلية للمعلومات من خلال إخضاعها لاختبارات تمكن من التأكد من صحتها .

31. أظهر البحث أن الدليل التقني مهما تقدمت طرقه وعلت قيمته العلمية والفنية في الإثبات فإنه يحتاج إلى قاضي يتمتع بسلطة تقديرية، لأن هذه السلطة التقديرية تكون لازمة لتنقية الدليل من شوائب الحقيقة العلمية، كما أنها ضرورية لكي تجعل الحقيقة العلمية حقيقة قضائية، فالحقيقة تحتاج دائما إلى دليل، وإذا كانت هذه الحقيقة قابلة للتطور فإن الدليل الذي تقوم به لا بد أن يكون هو الآخر متطورا لكي يقوى على إثباتها، ويجب ألا يقف هذا التطور عند طرق الحصول على الدليل، بل يلزم أن يتطور أيضا كل من يتعامل مع هذا الدليل من محققين وقضاة لأنه بهذا التطور الأخير تتطور الحقيقة القضائية ونستطيع أن نجعل الحقيقة العلمية حقيقة عادلة .

32. صعوبة تحديد شخصية فاعل الجريمة استنادا إلى الدليل التقني وإن كان يمكن معرفة عنوان ورقم الحاسوب فقط المرتبط بالانترنت والمستعمل كوسيلة لارتكاب الجريمة مما ساعد للتوصل إليه عبر إقامة الدليل التقليدي فيما بعد .

ثانيا : الحول المتوصل اليها :

على ضوء تلك النتائج فإننا توصلنا إلى الآتي :

1. ضرورة المراجعة الدورية للتشريعات الجزائية القائمة وإزالة أي غموض أو ثغرات فيها التي من الممكن أن يفلت منها الجاني ومن قبيل ذلك :

أ- بالنسبة لجريمة الدخول غير المصرح به إلى نظم المعالجة الآلية أيا كانت النتيجة التي أدت إليها فإننا نقترح تشديد عقوبتها في الحالات التالية :

*إذا كان مرتكب الجريمة عاملا بالمؤسسة الضحية، واستغل عمله هذا في الدخول غير المصرح به .

*إذا كان الدخول بنية ارتكاب جريمة لاحقة عليه .

*إذا تمت الجريمة اختراقا لنظم الأمن.

ب-حبذا لو يجرم المشرع الدخول غير المصرح به المتجاوز للغرض الذي منح من أجله التصريح بنص خاص و مباشر وذلك منعا لإفلات مرتكبيه من العقاب .

ت- حبذا لو يحذو المشرع الجزائري حذو المشرع الفرنسي وينص على جريمة إعاقة وإفساد نظام المعالجة الآلية كجريمة مقصودة قائمة بذاتها بما لا يتعارض مع جريمة التلاعب بالمعلومات .

ث- حبذا لو يحذو المشرع الجزائري حذو المشرع الفرنسي ويعاقب على جريمة التعامل في معلومات غير مشروعة بالعقوبة المقررة للجريمة نفسها، أي المقررة للجريمة التي يمكن أن تؤدي الوسائل المتعامل فيها إلى ارتكابها، لأنه من غير الممكن المعاقبة على جريمة التعامل في معلومات غير مشروعة بصفتها أعمال تحضيرية لجريمة الدخول أو البقاء غير المشروع أو التلاعب غير المشروع بالمعلومات بعقوبة أشد من عقوبات تلك الأخيرة .

ج- حبذا لو يحذو المشرع الجزائري حذو المشرع الفرنسي ويخرج جنحة الاتفاق الجنائي للتحضير لجرائم الاعتداء على نظم المعالجة الآلية من نطاق الشروع لتصبح المادة على النحو التالي: « يعاقب على الشروع في ارتكاب الجنح المنصوص عليها من 394 مكرر إلى 394 مكرر 2 بالعقوبات المقررة للجنحة ذاتها ».

ح- حبذا لو يحذو المشرع الجزائري حذو المشرع الفرنسي فيقرر تنويع العقوبات التكميلية بما يحقق مبدأ تفريد العقوبة بدل حصرها في المصادرة والغلق .

خ- تعديل المادة (394مكرر6) باستبدال عبارة «المواقع التي كانت محلا للجريمة» بعبارة «المواقع التي كانت وسيلة للجريمة »

د- الاقتصار على استعمال مصطلح «الغش» للدلالة على القصد في جرائم التعامل في معلومات غير مشروعة بدلا من استعمال مصطلح الغش والعمد معا لعدم وجود ضرورة تستوجب ذلك .

ذ- النص صراحة على ضرورة توافر القصد الخاص في جريمة التعامل في معلومات صالحة لارتكاب جريمة .

ر- تعديل المادة (395 مكرر5) المتعلقة بالاتفاق الجنائي في نطاق الجرائم محل الدراسة وذلك بإضافة عبارة « أو ارتكابها» بدل حصر موضوع الاتفاق في الإعداد لهذه الجرائم فحسب.

ز- بالرغم من أهمية القانون رقم (09 - 04) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها باعتباره يندرج ضمن إطار مساعي تعزيز العدة التشريعية الوطنية بما يجعلها تواكب الحداثة والعصرنة في مجال احتواء إسقاطات التقدم العلمي وتكنولوجيات الإعلام والاتصال الحديثة، وما أحرزت عليه الجزائر من تقدم وتطور في شتى الميادين والمجالات، إلا أنه باعتقادنا انه لم يكن هناك ضرورة تستدعي من المشرع الجزائري أن يقوم بسنه والتكفل به بعيدا عن المنظومة التشريعية الجزائية القائمة، وذلك لأن قانون الإجراءات الجزائية ليس عاجز على استيعاب مختلف القواعد الإجرائية المستحدثة منها (كحفظ المعطيات المتعلقة بحركة السير) والمعدلة في القانون الجديد السالف الذكر (كالتفتيش والضبط)، لذلك كان يستحسن بالمشرع الجزائري لو اكتفى بمجرد تعديل بعض أحكام قانون الإجراءات الجزائية وقانون العقوبات وإضافة بعض المواد إليها.

س- حبذا لو يتدخل المشرع الجزائري ويجرد السرقة المعلوماتية على أن يراعى في التجريم اعتبارين:

*أن يكون التجريم بنص عام يتسع ليشمل الصور المختلفة التي يمكن أن تنطوي عليها السرقة في البيئة التقنية أو الرقمية بدلا من إفراد نصوص خاصة لكل صورة من هذه الصور .

*تقوم الجريمة ولو لم يتم حرمان الحائز الشرعي منها، بل يكفي أن يقتصر الأمر على مجرد المشاركة في الحيازة والانتفاع فحسب .

ش- نهيب بالمشرع الجزائري تعديل قانون الإجراءات الجزائية وذلك بإضافة المادة التالية: « إذا صدر إذن بتفتيش نظام معالجة آلية معين، واكتشفت جرائم أخرى ضمن ملفات غير تلك التي ورد ذكرها في إذن التفتيش، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة .

2. يجدر بالمشرع عدم الاكتفاء بتطوير القواعد الإجرائية التقليدية بما يتماشى وطبيعة الدليل التقني، أو استحداث البعض الآخر إذ أن مشكلات الطبيعة التكوينية للدليل التقني والمعوقات الخاصة بالعامل البشري قد تحول أحيانا دون الوصول إلى حد تطبيقها، وعلى ذلك فحتى تكون الخطة متكاملة لابد من تدعيم تلك القواعد بإستراتيجيات وقواعد أخرى تكفل تحقيق الأهداف المرصودة ألا وهي استخلاص الدليل التقني، ولعل أهمها:

أ- إيلاء الاهتمام إلى موضوع التعاون الهيكلي والمنتظم بين أجهزة إنفاذ القانون وبين القطاع الخاص بما في ذلك مقدمي الخدمة في مجال الاتصالات الإلكترونية وذلك عبر منعهم دورا إيجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم والكشف عن مرتكبيها، وذلك من خلال تحديد التزاماتهم لاسيما التزامهم بالتحفظ على المعطيات المخزنة لديهم أسوة باتفاقية بودابست.

ب- ضرورة تنظيم نشاط مستعملي الخدمة على غرار مقدمي الخدمة، وذلك بإعادة النظر في تسيير مقاهي الانترنت من حيث إضفاء المسؤولية على المسيرين، وإخضاعهم لدفتر أعباء دقيق يحدد المسؤوليات فضلا عن الفضاءات الافتراضية الموجودة في المؤسسات العامة كالجامعات وغيرها وحتى الخاصة منها .

ت- إبرام اتفاقيات ومعاهدات دولية ثنائية أو متعددة الأطراف في مجال التعاون الدولي التي تستهدف من وراء ذلك التقريب بين القوانين الجزائية الوطنية من أجل جمع هذا النوع من الأدلة العابرة للحدود، خاصة في إطار مكافحة الجرائم العالمية ومنها جرائم الاعتداء على النظم.

فضلا عن ذلك تبين كيفية تسليم المجرمين، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بهذا النوع من الجرائم .

ث- تعميق التفكير حول فكرة إنشاء وحدات خاصة يناط بها مهمة التحري والتعتيق في البيئة التقنية سواء على المستوى الوطني أو على المستوى القاري كما هو الحال على المستوى الأوروبي، على أن يكون الاهتمام بالتوازي بتدريب وتكوين معمق لأعضاء الشرطة القضائية والمحققين على التعامل مع جرائم الاعتداء على نظم المعلوماتية ذات الطبيعة الفنية والعلمية المعقدة وتعزيز قدراتهم على التحقيق فيها وتأمين الأدلة التقنية، بحيث يمكن الوصول إلى الحقيقة .

3. بذل جهود خاصة لتمكين القضاة وأعضاء النيابة العامة لملاحقة ومقاضاة مرتكبي جرائم تقنية المعلومات والاستفادة من الأدلة التقنية من خلال التدريب والربط الشبكي (التواصل) والتخصص، وإذا كان قد تم وضع هذا المفهوم وتطويره من قبل المجلس الأوربي بشأن جرائم تقنية المعلومات، وصادقت عليه شبكة لشبونة للمجلس الأوروبي في سبتمبر 2009 وأوصت بنشره وتنفيذه على نطاق واسع من قبل مؤسسات التدريب القضائي، وتقريرها جعله في صلب اهتمام المجلس الاستشاري للقضاة الأوروبيين والمجلس الاستشاري للمدعين العامين الأوروبيين، فضلا عن اللجنة الأوروبية من أجل نظام قضائي فعال لضمان أكبر تأييد ممكن لهذا المفهوم، فإنه برأينا لا حرج لو كان هناك دور عربي يعمل على مساعدة مؤسسات التدريب القضائي لوضع برامج تدريب على أدلة جريمة تقنية المعلومات للقضاة وأعضاء النيابة العامة، وإدماج هذا النوع من التدريب ضمن أساس التدريب الأولي والتدريب أثناء الخدمة والمساهمة في تسهيل التواصل فيما بين القضاة وأعضاء النيابة العامة لتعزيز معارفهم، بالإضافة إلى الدعم بشكل منتظم، بدلا من دعم متخصص، لمبادرات التدريب التي توضع من قبل الشركاء المعنيين .

4. العمل على تكريس نصوص قانونية تعاقب على كل من يعلم بوقوع الجريمة ولا يبلغ عنها ولو لم يكن متضررا منها أو ذا مصلحة.

5. دعوة المؤسسات التعليمية المعنية بتأهيل الأطر القانونية إلى تضمين مادة مبادئ الحاسوب وتطبيقاته ضمن خططها الدراسية .

6. ضرورة إصدار دليل إرشادي تقني وقانوني حول صور جرائم تقنية المعلومات بصفة عامة والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة التقنية ومواصلة تحديث هذا الدليل بشكل دوري وكلما دعت الحاجة لذلك وتعميمه على العاملين في مجال التحقيق في الميدان وعلى أجهزة القضاء.

وتوصلنا من خلال دراستنا إلى ضرورة أن تتضمن مقومات استراتيجيات مواجهة جرائم الاعتداء ومحاربتها إلى جانب القوانين الجنائية الموضوعية قوانين إجرائية تتماشى وطبيعة البيئة الرقمية خاصة مسألة استخلاص الدليل التقني طبعا بدون أن تتعرض حقوق الإفراد وحرياتهم للخطر، ولهذا قيل بأن من يتقن وضع قانون العقوبات ثم يترك قانون الإجراءات الجنائية بدون لم إتقان كمن يبني قصرا في الهواء .

أكثر من ذلك، فإن القوانين الجزائية الموضوعية والإجرائية لا تكفي وحدها لمواجهة الجرائم محل الدراسة بل لا بد من إيجاد استراتيجيات مكملة على المستوى الفني التقني والقضائي وعلى مستوى التعاون القضائي الدولي وتسليم المجرمين .

أولا : المراجع باللغة العربية

أ–الكتب والمؤلفات :

1- إبراهيم مدكور، المعجم الفلسفي، دار الكتاب، القاهرة، 1983 .

2- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة للطباعة والنشر، الجزائر، 2009.

3- عبد الفتاح مصطفى الصيفي، قانون العقوبات، النظرية العامة، دار الهدى للمطبوعات، الاسكندرية، دس.

4- أحمد الخليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

5- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج2، د.م.ج، الجزائر، 1999.

6- أحمد عبد العزيز الألفي ، شرح قانون العقوبات (القسم العام) ، مكتبة النصر الزقازيق ،1995 .

7- أحمد فتحي سرور ، الوسيط في قانون العقوبات، القسم العام ، ط5 ، دار النهضة العربية ، القاهرة ، 1991.

8- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، 2010.

9- أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي والأنترنت ، ط1 ، دار وائل للطباعة والنشر ، عمان ، 2001.

- أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي والانترنت،دار وائل للطباعة والنشر عمان، 2001.

10- أشرف شمس الدين ، الحماية الجنائية للمستند الإلكتروني ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2006.

11- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، د.ط، 2006.

12- أيمن عبد الله فكري ، جرائم نظم المعلومات ، دار الجامعة الجديدة ، الإسكندرية ، 2007 .

13- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، ب.ط،2011، .

14- خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي ، دار الجامعة الجديدة، الإسكندرية، 2005.

15- خالد ممدوح ابراهيم ، الجرائم المعلوماتية ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2009.

- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2008.

16- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى، الجزائر، ط1 .

17- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، د.ط، 2013.

18- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية بيروت لبنان، ط1، 2012.

19- رؤوف عبيد ، مبادئ القسم العام من التشريع العقابي، طبعة ثالثة ، 1966 ،دار الفكر العربي .

20- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.

21- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية دراسة تحليلية، دار الكتب القانونية مطابع مصر الكبرى، د.ط.

22- سامي علي حامد عياد ، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2006.

23- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الاولى، دار النهضة العربية، القاهرة، 1999.

24- السعيد مصطفى السعيد، الأحكام العامة في قانون العقوبات، الطبعة الثانية، مكتبة النهضة المصرية، مصر، 1953.

25- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية،بيروت، لبنان، ط1، 2011.

26- طارق ابراهيم الدسوقي عطية ، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية) ، دار الجامعة الجديدة ، الإسكندرية 2009 .

27- عبد الفتاح بيومي حجازي ، التزوير في جرائم الكمبيوتر والأنترنت ، دار الكتاب القانونية ، مصر المحلة الكبرى ، 2005 .

- عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي ، دار الكتب القانونية ، مصر ، المحلة الكبرى 2007.

- عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، 2004،

- عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، الكتاب الأول، دار الفكر الجامعي، الإسكندرية، 2004.

- عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام الكمبيوتر ، دار الفكر الجامعي، الإسكندرية، 2004

28- عبد الله أوهابيبه، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومه للنشر والتوزيع، الجزائر، 2008.

29- عبد الله بن محمد النجار ، الحماية المقررة لحقوق المؤلفين الأدبية ، دار النهضة العربية ، القاهرة ، 1990.

30- عبد الله سليمان، شرح قانون العقوبات الجزائري (القسم العام) الجزء الأول الجريمة، ط6، د.م.ج، الجزائر،2005.

31- عبد الله عبد الكريم عبد الله ، جرائم المعلومات والإنترنت (الجرائم الإلكترونية) ، ط1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007 .

32- عز الدين الديناصوري، عبد الحميد الشواري، المسؤولية الجنائية من قانون العقوبات والاجراءات الجنائية، ط3 منشأة المعارف، الاسكندرية، 1988 .

33- علي حسين الخلف وسلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، مطابع الرسالة ، الكويت ، 1982.

34- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، الدار الجامعية للطباعة والنشر، بيروت، 1999.

- علي عبد القدر القهواجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، 1997.

35- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إحلال نظرية الإثبات الجنائي،

36- عمر الشيخ الأصم، نظام الرقابة النوعية في المختبرات الجنائية في الدول العربية، دار الحامد للنشر والتوزيع، عمان، الاردن، 2006، ص 57.

37- عمر بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، د.م، 2008.

38- عمر خالد زريقات، عقود التجارة الإلكترونية، عقد البيع عبر الانترنت، ط1، دار الحامد للنشر والتوزيع، الاردن، 2007.

39- عمر محمد بن يونس، أشهر المبادئ المتعلقة بالانترنت في القضاء الأمريكي، الطبعة الأولى، دار أكاكوس، 2004.

40- عوض الحاج علي أحمد، عبد الامير خلف حسين، امنية المعلومات وتقنيات التشفير، دار الحامد للنشر والتوزيع، الأردن، 2004.

41- عوض بن غلاب الوذاني، تقنيات تحديد الهوية في مواجهة التحديات الأمنية ، دار الحامد للنشر والتوزيع، عمان الأردن، د س ن، د.ط.

42- فريد منعم جبور ، حماية المستهلك عبر الأنترنت ومكافحة الجرائم الإلكترونية دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت ، لبنان ، 2010.

43- فوزية عبد الستار، شرح قانون العقوبات – القسم العام – ، دار النهضة العربية ، القاهرة، 1992.

44- قحطان محمد صالح الجميلي ، آلة العصر (الكمبيوتر) ، منشورات مكتبة الشعب ، بغداد ، 1985.

45- قورة نائل عادل، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي لبنان، ط1، 2005،.

46- كامل السعيد – شرح الاحكام العامة في قانون العقوبات الاردني والقانون المقارن ، الطبعة الثانية – دار الفكر للنشر والتوزيع – عمان 1983.

47- محمد أبو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، 2008

48- محمد بن حميد المزمومي ، جريمة الإعتداء على الأموال عن طريق الحاسب الآلي، دار النهضة العربية، الإسكندرية، 2007.

49- محمد حسين ، المسؤولية القانونية في مجال شبكات الانترنت ،ط1 ، دار النهضة العربية ، القاهرة 2002.

50- محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة و القانون الجنائي ، دار الثقافة ، عمان ، 2004 .

- محمد حماد مرهج الهيتي ، الجريمة المعلوماتية نماذج من تطبيقاتها دراسة مقارنة في التشريع الإماراتي والسعودي و البحريني والقطري والعماني، دار الكتب القانونية، ودار شتات للنشر والبرمجيات، مصر- الإمارات، ب.ط، 2014.

- محمد حماد مرهج الهيتي ، جرائم الحاسوب – ماهيتها – موضوعها – أهم صورها – والصعوبات التي تواجهها ، ط1 ، دار المناهج ، عمان ، 2006.

51- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية، 2007.

52- محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الأنترنت (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، بيروت لبنان، ط1، 2011.

53- محمد عبد الظاهر حسين، الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، دار النهضة العربية، القاهرة، 2000.

54- محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، ط2 ، دار النهضة العربية ، القاهرة ، 2009.

55- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الكمبيوتر، دار الجامعة الجديدة للنشر، الإسكندرية، 2001.

56- محمد مرسي الزهرة، الحاسي الإلكتروني والقانون، دار النهضة العربية، القاهرة، 2008.

57- محمود أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان 2005 .

58- محمود السيد عبد المعطي خيالي، الأنترنت وبعض الجوانب القانونية، دار النهضة، القاهرة، 1998.

59- محمود حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، 1957.

60- محمود زكي أبو عامر ، قانون العقوبات القسم العام ، الدار الجامعية للطباعة و النشر ، بيروت ، 1990.

61- محمود محمود مصطفى، شر قانون الإجراءات الجنائية، الطبعة الثانية، مطبعة دار النشر الثقافة، القاهرة، 1974.

62- محمود نجيب حسني – شرح قانون العقوبات ، القسم العام – الطبعة السادسة – دار النهضة العربية – القاهرة 1989 .

- محمود نجيب حسني ، النظرية العامة للقصد الجنائي (دراسة تأصيلية مقارنة في الجرائم العمدية) ، الطبعة الثالثة 1988 ، دار النهضة العربية ، القاهرة.

- محمود نجيب حسني ، شرح قانون العقوبات القسم العام النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الإحترازي، ط5، دار النهضة العربية القاهرة، 1988.

- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988.

- محمود نجيب حسني، شرح قانون العقوبات القسم العام النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، ط6 دار النهضة العربية القاهرة، 1989.

63- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة القاهرة، 2008.

- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، 2003

- مصطفئ محمد موسى ، أساليب إجرامية بالتقنية الرقمية ، ماهيتها ،مكافحتها ، دراسة مقارنة، دار الكتب القانوينة ، مصر ، 2005.

64- منير محمد الجمبيهي، محمود محمد الجمبيهي، الطبيعة القانونية للعقد الإلكتروني، دار الفكر الجامعي، د.س.ن، د.ط.

- منير محمد الجنبيهي وممدوح محمد الجنبيهي ، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، الإسكندرية ، 2006 .

65- نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي-دراسة مقارنة-، دار هومة للطباعة والنشر والتوزيع، 2008.

66- نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف ، الإسكندرية ، 2008.

67- نعيم مغبغب، حماية برامج الكمبيوتر دراسة مقارنة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت لبنان، ب.ط، 2009.

68- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط1 ، دار الثقافة ، عمان ، 2008.

69- نواف كنعان، حق المؤلف ، النماذج المعاصرة لحق المؤلف ووسائل حمايته ، الطبعة الثالثة 2000 .

70- هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية للنشر، القاهرة، 2000.

71- هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية القاهرة، 2009.

72- هيثم حمود الشبلي، إدارة مخاطر الإحتيال في قطاع الاتصالات، دار صفاء للنشر والتوزيع، عمان، ط1، 2009، .

73- هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة – 1992 .

74- وائل أنور بندق ، موسوعة القانون الإلكتروني و تكنولوجيا الإتصال و المعلومات ، الطبعة الأولى (2007) ، دار المطبوعات الجامعية ، الإسكندرية .

ب – رسائل الدكتوراه و مذكرات الماجستير:

I–رسائل الدكتوراه:

1- إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية – دراسة قانونية نفسية – الطبعة الأولى رسالة دكتوراه،عالم الكتاب، القاهرة،1980.

2- أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجزائية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1982.

3- خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، رسالة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012.

4- سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، القاهرة، دار النهضة العربية 1972.

5- سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، القاهرة، دار النهضة العربية 1972.

II- رسائل الماجستير :

1- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2010-2011،

2- عطية عثمان محمد بوحويش، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة ماجستير، مقدمة إلى أكاديمية الدراسات العليا، فرع بنغازي، 2009.

مقالات مداخلات وبحوث:

1- أشرف صلاح الدين، طرق الحماية التكنولوجية بأنواعها واشكالها المختلفة، ورقة عمل مقدمة في ندوة امن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، مصر، جوان 2007.

2- إصلاح العدالة الحصيلة والآفاق، وزارة العدل، فيفري 2005 ، موقع الواب لوزارة العدل .

3- أكاديمية شرطة دبي، الفترة من 26 إلى 48-4-2003، دبي.

4- أمجد حسان ، الفيروسات ارهابا يهدد انظمة المعلومات ، ملتقى الإرهاب في العصر الرقمي ، جامعة الحسين بن طلال ، 10-12 جويلية 2008 ، عمان

5- إيهاب ماهر السمباطي ، الجرائم الإلكترونية الجرائم السيبيرية قضية جديدة أم فئة مختلفة التناغم القانوني هو السبيل الوحيد ، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ، المملكة المغربية ، 19-20 يونيو ، 2007.

6- بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية.

7- جبريل العريشي، أمن المعلومات عن طريق الجدار الناري والتشفير وغيرها...، الرياض، الخميس 5 نوفمبر 2009.

8- جميل زكرياء محمود، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات، المؤتمر الدولي حول أمن المعلومات –نحو تعامل رقمي آمن-، 18-2005/12/20، مسقط، سلطنة عمان.

9- جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ب.ط، 2000.

10- حسن طاهر داود ، جرائم نظم المعلومات ، الطبعة الأولى ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2000.

11- خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية.

12- رامي عبد الحليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجموعة الملتقى الدولي حول التنظيم القانوني للانترنيت، مجلة دراسات، 2009، ع 1.

13- سامي الشوا ، الغش المعلوماتي كظاهرة اجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة 25-28 تشرين أول / أكتوبر 1993.

14- ستيف غيلمور، تبادل المعلومات باستخدام لغة الترميز الموسعة (XML)، بحث منشور في إطار الكتاب المتعلق بـ: حلول التجارة الالكترونية، مقدم من مايكروسوفت، إعداد Micro Modeling Associates، ترجمة: مركز التعريب والبرمجة، الدار العربية للعلوم ، الطبعة الأولى، 2000م.

15- عارف خليل أبو عيد ، جرائم الأنترنت ، بحث منشور في مجلة جامعة الشارقة للعلوم الشرعية والقانونية ، المجلد الخامس ، العدد الثالث ، شوال /1429 هـ (أكتوبر /2008)، الشارقة.

16- عبد الرحمان جلهم حمزة ، جرائم الانترنت من منضور شرعي وقانوني ، ظافرة للتصميم والطباعة ، بغداد ، ب ، س ، ن.

17- عبد الله عبد العزيز اليوسف ، التقنية والجرائم المستحدثة ، بحث منشور ضمن كتاب (الظواهر الإجرامية المستحدثة وسبل مواجهتها)، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الامنية الرياض ، 2004.

18- علي بن عبد الله العسيري ، الآثار الأمنية لإستخدام الشاب للأنترنت ، ط1 ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004 .

19- عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الانترنت، ندوة الدليل الرقمي بمقر جامعة الدول العربية بجمهورية مصر العربية، في الفترة من 5-8 مارس 2006.

20- غنام محمد غنام ، عدم ملاءمة القواعد التقليدية لقانون العقوبات لمكافحة جرائم الكمبيوتر ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت ، كلية الشريعة والقانون ، جامعة الإمارات ، ماي، 2004 .

21- ماجد الحلو ، الحكومة الإلكترونية والمرافق العامة، بحث مقدم إلى المؤتمر العلمي الأول الذي نظمته أكاديمية شرطة دبي حول " الجوانب القانونية والأمنية لعلميات الإلكترونية من 26-28 أفريل 2003.

22- محمد أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003.

23- محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، الطبعة الاولى ، مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004 .

24- محمد الصاعدي، جرائم الأنترنت وجهود المملكة العربية السعودية في مكافحتها، ورقة عمل مقدمة في ندوة مكافحة الجريمة عبر الأنترنت ، شرم الشيخ مصر، أفريل 2008.

25- محمد أنور البصول ، الأنترنت واسهامه في عمليات الإرهاب ، بحث منشور ضمن (كتاب الإرهاب والعولمة) ط 1 ، مركز الدراسات والبحوث – جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2002 .

26- محمد حسين النيلي، العلاقة بين القانون والحكومة الإلكترونية، ورقة عمل قدمت لمؤتمر الكويت حول الحكومة الإلكترونية في الفترة 13-15 أكتوبر 2003.

27- محمد محمد الألفي، الجريمة والمجرم عبر الأنترنت، ورقة عمل مقدمة في ندوة مكافحة الجريمة عبر الأنترنت على المستوى العربي، شرم الشيخ، مصر ، أفريل 2008.

28- محمد محمد الالفي، ورقة عمل مقدمة في ندوة أمن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، جوان 2007.

29- محمود صالح ، "الجرائم المعلوماتية" ماهيتها ، صورها – ورقة عمل مقدمة إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الافتراضية والمنعقدة بسلطنة عمان، 2-4 ابريل 2006 .

30- مصطفاوي عبد القادر، الشرطة الوطنية ومكافحة الجريمة المعلوماتية، الملتقى الدولي لمحاربة الجريمة المعلوماتية، 5-6 ماي 2010، منشور في مجلة مركز البحوث القانونية والقضائية،.

31- ممدوح الشحات صقر، ورقة عمل مقدمة في ندوة أمن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، جوان 2007.

32- ممدوح عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في: 10-12 مايو 2003.

33- ميريام كومينر ، الإجرام البشري الإلكتروني ، جوانب استراتيجية وقانونية، مجلة الثقافة العالمية للمجلس الوطني للثقافة والفنون والآداب، الكويت ، العدد158 ، 2010.

34- نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات، المؤتمر الدولي حول أمن المعلومات –نحو تعامل رقمي آمن-، 18-2005/12/20، مسقط، سلطنة عمان.

35- ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، مطابع الحميضي الرياض السعودية، ط1، 1430هـ-2009م.

36- نائل عبد الرحمان صالح ،واقع جرائم الحاسب في التشريع الأردني ، بحيث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة (2000) بحوث مؤتمر القانون والكمبيوتر والأنترنت ، المجلد الأول ، الطبعة الثالثة ، كلية الشريعة والقانون جامعة (الإمارات العربية المتحدة ، 2004.

37- هشام محمد فريد رستم ، الجرائم المعلوماتية – أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي ، بحيث مقدم لمؤتمر القانون والكمبيوتر والأنترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة في الفترة (1-3/مايو/2000) ، بحوث مؤتمر القانون والكمبيوتر والأنترنت ، المجلد الثاني ، كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة ، 2004 .

38- وليد أبو سعد، أمن المعلومات، الموسوعة العربية للكمبيوتر والانترنت، 2005،

ج- القوانين و الأوامر و المراسيم :

1- قانون العقوبات الصادر بموجب الأمر رقم 66-156 المؤرخ في 08-06-1966 جريدة رسمية عدد49.

2- أمر رقم 15-02 المؤرخ في 23-07-2015 المعدل و المتمم للامر رقم 66-155 المؤرخ في 08-06-1966 المتصمن لقانون الإجراءات الجزائية

3- الأمر 03-05 المتعلق بحق المؤلف والحقوق المجاورة المؤرخ في 2003/07/19 الجريدة الرسمية رقم 44.

4- القانون رقم 04-15 المتعلق بتعديل قانون العقوبات الجريدة الرسمية رقم 71

5- القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها الصادر بتاريخ 05 غشت 2009 الجريدة الرسمية عدد 47

6- قانون رقم 15-03 المتعلق بعصرنة العدالة الصادر بتاريخ 01 فبراير 2015 جريدة رسمية عدد06

7- القانون رقم 15-04 المحدد للقواعد الخاصة المتعلقة بالتوقيع و التصديق الإلكترونيين الصادر بتاريخ 01 فبراير 2015 جريدة رسمية عدد 06

8- المرسوم الرئاسي المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال الصادر بتاريخ 08-10-2015 جريدة رسمية عدد53

مواقع الأنترنت :

1- خبر منشور على الموقع الإلكتروني :(Web.fares.net/w/ee7ebaz(7/9/2001

2- موقع الويب لوزارة العدل

3- موقع arabelaw

http://kenanonline.com -4

www.maj-secours.com/spip.php -5

www.finonaces-gouv.fr -6

www.wamadani.com/vp/showthread.php?t=26760 -7

www.libartésecurité.org/artichle226.html -8

.www.interieur.gouv.fr -9

www.sawt-alhrar.net/onlinemodules . -10

www.algéria.com/forumse/computre -11

..inernet/21325-cibaiercriminamité-en-alg-rie-4.html

12- موقع جريدة الشروق اونلاين

ثانيا المراجع باللغة الفرنسية

- **Ouvrages** :

1- Bart de Schuter. La criminalité liée à l'informatique, Rev DPC No 1 Avril 1985.

2- Lionel Bochorberg : Internet et commerce électronique , Delmas, paris , 2001.

3- Masse (M) : Le droit pénal spécial et Travaux de sciences criminelles de peintres 1984 Edjais.

4- Philipe rosé. La criminalité informatique. Edition dahlab. Collection que sais- je ? paris. 1998. .

5- Nidal El Chaer, la criminalité informatique devant la justice pénale, édition juridiques, Beyrouth, Liban.

6- Vavant et le Ctainc, Lamy in Droit de l'informatique

matique PUF éd 1989.

7- Céline Castets-Renard ,droit de l'internet: droit français et européen, Montcherstien lextenso édition, 2eme édition ;2012.

- **Articles** :

1- G. Stefani, G. Levasseur, B.Bouloc : Droit pénal général – Précis Dalloz 1980 Paris .

2- P.Pouzat,J.Pinatel:Traité de droit criminel – Dalouz 2eme édition 1967 Paris .

الفهرس الصفحة

ملخص:

أحدثت المعلومات الإلكترونية –وبيئتها نظام المعالجة الآلية– تغيير جذري في المفاهيم القانونية السابقة، حيث أصبح من الضروري إعادة النظر في تلك المفاهيم لتتأقلم مع التطورات الحاصلة، ومن بين أهم المسائل القانونية المطروحة في هذا المجال هو وجوب الأمن القانوني لها، وهو موضوع يحتاج إلى دراسة تأصيلية له، ومن ثم دراسة للإستراتيجية التشريعية لمواجهة التهديدات الأمنية للمعلومات الإلكترونية.

لذلك فإن البحث يتجه إلى تحديد الإشكالات الموضوعية والإجرائية التي تواجه أمن المعلومات من الناحية القانونية والواقعية إضافة إلى تحديد الآليات المتوجه نحوها لتكريس أمن متكامل.

الكلمات المفتاحية: المعلومات الإلكترونية، النظام المعلوماتي، أمن المعلومات الإلكترونية.

Resume :

Les données éléctroniques leur champs et le système de traitement automatique ont provoquées un changement radical dans les anciens concepts législatifs. La révision de ces concepts devient indispensable de sorte qu' elles s' adaptent avec les évolutions constatées. Parmi les plus importants concepts législatifs invoqués dans ce domaine, l'obligation d'-imposer sa sécurité légal. ce sujet a besoin d' une étude approfondie, de ce fait il faut étudier la stratégie législative afin de contre-carrer les menaces sécuritaires des informations électronique. Donc la recherche doit être orienter vers la détermination problématique de l'objectif et les procédures que rencontre la sécurité des informations du coté légal, et la pratique en plus de la détermination du mécanisme vers lequel il faut consacrer une parfait sécurité.

Les mots clés : les informations électroniques. Système informatique. Les crimes informatiques. Sécurité des données électroniques.

Summary

The electronic information the mechanism system- has caused a radical change in the previous legal concept. Where it becomes necessary to consider those concepts to familiarize themselves with the current development. Thus, providing legal security is among the most important legal issues raised in this field. Nevertheless, this issue needs a fundamental study as well as a legislative and strategic study to confront security. Threats of electronic information. Therefore. All researches aimes at identifying substantive and procedural problems wich oppose information security on the legal and factual side. In addition, to identify the mechanism towards it to devote such an integrated security.

Key words, electronic information: information system. Computer crime. Electronic information security.