جامعـــة أبوبكر بلقايد تلمسان
كليـــة الحقـــوق والعلـــوم السياسيـــة
قسم الحقوق

الحماية الجنائية للحكومة الإلكترونية
دراسة مقارنة

أطروحة مقدمة لنيل شهادة دكتوراه في العلوم ـ تخصص قانون عام

إعداد الطالبة:
بن قارة مصطفى عائشة

إشراف الأستاذ الدكتور:
بن طيفور نصر الدين

أعضاء اللجنة المناقشة:

د. قطاية بن يونس	أستاذ محاضر "أ"	جامعة تلمسان	رئيسا
أ/ د. بن طيفور نصر الدين	أستاذ التعليم العالي	جامعة تلمسان	مشرفا ومقررا
أ/د. باسم شهاب محمد	أستاذ التعليم العالي	جامعة مستغانم	مناقشا
أ/د. بن عزوز بن صابر	أستاذ التعليم العالي	جامعة مستغانم	مناقشا

السنة الجامعية: 2017 - 2018

قال الله تعالى:

"...وَمَا أُوتِيتُم منَ العلم إِلا قَليلا"

صدق الله العظيم

(سورة الإسراء ـ الآية 85)

شكر وتقدير

الحمد لله رب العالمين، على جلال فضله وعظيم نعمه، الحمد لله الذي أعطاني الصبر والعزيمة ويسر لي من الوقت والجهد والصحة لإتمام هذه الرسالة، إنه على كل شيئ قدير، والصلاة والسلام على أشرف الأنبياء والمرسلين.

إنطلاقا من قول النبي صلى الله عليه وسلم: "لا يشكر الله من لايشكر الناس"، فإني أتقدم بالشكر الجزيل وعظيم الامتنان:

إلى أستاذي الفاضل الأستاذ الدكتور بن طيفور نصر الدين لما كان له من سعة صدر وحرص تام في متابعة العمل من بدايته إلى نهايته؛

إلى أعضاء لجنة المناقشة على قبولهم مناقشة هذه الرسالة وعلى ما بدلوه من وقت وجهد في دراستها وتقويمها؛

إلى الذين أنارو لي طريق العلم والمعرفة إلى الأساتذة الأفاضل الذين تلقيت العلم على أيديهم؛

أخيرا إلى كل من ساعدني وقدم لي يد العون والمساعدة، ولو بالدعاء لإنجاز هذا العمل المتواضع.

فجازى الله عني الجميع خيرا.

الإهداء

أتشرف بتقديم هذا العمل المتواضع إلى روح أبي الذي أدعو الله أن يسكنه فسيح جنانه؛

إلى أمي الحبيبة أطال الله في عمرها؛

إلى زوجي الذي كان وما زال يشجعني ...يعينني على الحياة ...وكان له الفضل في إتمام هذه الرسالة؛

إلى أخوتي وأخواتي؛

إلى فلدات كبدي...بناتي شيماء كوثر ومريم؛

إلى كل أفراد عائلتي

قائمة أهم المختصرات(ABREVIATIONS)

أولا : باللغة العربية.

ج	.....	جزء؛
ج.ر	.....	الجريدة الرسمية؛
د.ج	.....	دينار جزائري؛
د.د.ن	.....	دون دار النشر؛
د.س.ن	.....	دون سنة النشر؛
ص	.....	صفحة؛
ط	.....	الطبعة؛
ع	.....	عدد؛
ف.ف	.....	فرنك فرنسي؛
ق.إ.ج.ج	.....	قانون الإجراءات الجزائية الجزائري؛
ق.إ.ج.ف	.....	قانون الإجراءات الجزائية الفرنسي؛
ق.ع.ج	.....	قانون العقوبات الجزائري؛
ق.ع.ف	.....	قانون العقوبات الفرنسي ؛
ق.م.ج	.....	قانون المدني الجزائري؛
ق.ع.ف	.....	قانون العقوبات الفرنسي.

ثانيا: باللغة الفرنسية.

Art	……..	Article ;
Bull. Crim	……..	Bulletin Criminelle ;
Cass. Crim	…….	Cassation Criminelle ;
C. P		Code Pénale ;
C. P. P	……..	Code Procédure Pénale ;
Crim	……..	Coure de cassation, chambre criminelle ;
D	……..	Recueil Dalloz ;
D.H	…….	Recueil Dalloz hebdomadaire
€	…….	Euro ;

Ed	……..	Edition ;
G. P	……..	Gazette du Palais ;
Ibid	……..	Meme Refrence ;
J. O	……..	Journal officiel ;
N°	……..	Numéro ;
OP. Cit	……..	Ouvrage cite ;
P	.....	Page ;
Rev. Dr. Pen. Crim	…….	Revus de droit pénal et de criminologie ;
Rev. Int. Dr . Pen	……..	Revus Internationale de droit pénale ;
R.S.C	……..	Revue de science criminel et de droit pénal compare ;
S	……..	Suivant ;
T	……..	Tome ;
Th.	……..	These .

مقـــدمـــــة

إنّ العالم بأسره دخل مرحلة متطورة ضمن آفاق عصر المعلومات بهدف الاستفادة من التقنيات المتاحة في مجال نظم وتقنية المعلومات والإتصالات، فأصبح المعيار الأساسي الذي تقاس به درجة تقدم الأمم في القرن الحادي والعشرين.

مند وقت ليس ببعيد ظهرت أهمّ الإختراعات البشرية وهو الحاسب الآلي. ذلك الجهاز المعقد في تركيبه، العظيم في إنجازاته، البسيط في تشغيله، المتميز بالسرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها.

مزايا الحاسب الآلي جعل تقبله كبيرا وكان اتساعه وانتشاره مذهلا، فقد تحول وخلال عشر سنوات فقط من ظهوره كجهاز تطبيقي إلى محور العمل والحركة في العديد من النشاطات المختلفة، سواء بالنسبة للأفراد، أم بالنسبة للدولة[1].

بقيت الدولة متواضعة إلى حد ما في تعاملها مع الحاسب الآلي، إلى أن أخذت الشبكة العالمية الإنترنت تتطور وتنتشر، حيث أصبحت أداة عصرية لازمة لا غنى عنها في كل المجالات، بل في كل بيت.

هذا التزاوج الحاصل بين الحاسب الآلي وشبكة الانترنت من جهة، والفرد العادي من جهة أخرى، واعتماد كل منها على الآخر، أدى بالدولة إلى الإستفادة من تقنيات نظم المعلومات والإتصالات في الأعمال الحكومية، فبرز حينها ما يعرف "بالحكومة الإلكترونية"[2].

---

[1] ــ أسامة أحمد المناعسة، جلال محمد الزعبي، الحكومة الإلكترونية بين النظرية والتطبيق، دار الثقافة للنشر والتوزيع، الأردن، الطبعة الأولى، 2013، ص 13.

[2] ــ تعددت التعاريف التي قيلت بشأن مصطلح ''الحكومة'' من الناحية الدستورية منها مايلي:

1 ــ يقصد بها كافة هيئات الحكم في الدولة، وهذا هو المعنى الذي يشير إليه الفقهاء بقولهم: إن للدولة ثلاثة عناصر هي: الحكومة والشعب والاقليم.

2 ــ ويقصد بها مجموع الهيئات الحاكمة أو المسيرة للدولة أي السلطات العامة في الدولة : التشريعية والتنفيدية والقضائية.

3 ــ والحكومة قد تعني السلطة التنفيدية بفرعيها (رئيس الدولة والوزارة)، وهذا هو المفهوم عندما يقال أن سلطات الدولة ثلاث هي: الحكومة والبرلمان والسلطة القضائية.

4 ــ والحكومة قد تعني أحد فرعي السلطة التنفيدية، وهي مجلس الوزراء والوزارة .عبد الفتاح بيومي حجازي، النظام القانوني للحكومة الالكترونية، الكتاب الأول، الحكومة الالكترونية،دار الكتب القانونية، المحلة الكبرى، مصر، 2007، ص 17 وما بعدها.

وانطلاقا من المعنى الدستوري لمصطلح "الحكومة " ومقارنته مع المعنى الحالي "للحكومة الالكترونية" يرى بعض الفقهاء مثل علي السيد الباز في بحثه حول: دور الأنظمة والتشريعات في تطبيق الحكومة الالكترونية، عدم إمكانية إطلاق مصطلح " الحكومة" على المعنى الحالي الذي يقصدونه للحكومة الالكترونية ــ أي تقديم السلطة الإدارية أو الإدارة العامة لخدماتها العامة بطرق الكترونية ــ فالحكومة بمعنى السلطة

.بمعنى بسيط انتقال تقديم الخدمات الحكومية من الصيغة الورقية إلى الصيغة الإلكترونية، وذلك باستخدام أجهزة الكمبيوتر وشبكات الإتصال والبرمجيات اللازمة لذلك[1]، يطلق على هذا التحول اسم "حكومة عصر المعلومات" أو "الحكومة الذكية أو الرقمية" وأيضا "الإدارة العامة الإلكترونية"[2] و"الإدارة الإلكترونية"[3].

فعلى المستوى الدولي عرفت منظمة التعاون الإقتصادي والتنمية (OECED) عام 2003 الحكومة الالكترونية بأنها "استخدام تكنولوجيا المعلومات والإتصالات وخصوصا الأنترنت للوصول إلى حكومات أفضل"[4]، كما عرفتها الأمم المتحدة عام 2002 بأنها "استخدام الأنترنت والشبكة العالمية العريضة لإرسال معلومات وخدمات الحكومة للمواطنين"[5].

أما على المستوى الوطني فإن أغلب التشريعات لم تتضمن تعريفا للحكومة الإلكترونية مكتفية فقط بتبيان الخطط التنموية لمشاريع الحكومة الإلكترونية، مما فتح المجال للفقه القانوني لبيان مدلول

التنفيدية اكبر بذلك بكثير لأنه من مهامها أيضا ومن باب أولى وضع السياسة العامة للدولة، وتحديد الأهداف العامة المراد إدراكها، وهي مهمة ذهنية لا يقوم بها سوى العقل البشري، أما الكمبيوتر فقد يساعد فقط في إعداد بعض البيانات أو المعلومات التي تساعد في رسم هذه السياسة في حين أن مهمة الإدارة هي التي تنفذ هذه السياسة من خلال الحاسب الآلي وشبكة المعلومات بدلا من أن تتم بالطريقة التقليدية.ماجد راغب الحلو، الحكومة الالكترونية والمرافق العامة، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات المصرفية الالكترونية، الجزء الرابع، المحور الأمني والإداري ، المنعقد في اكادمية شرطة دبي، الإمارات العربية المتحدة، في الفترة 26 ــ 28 ابريل 2003، مركز البحوث والدراسات، دبي، ط 1، 2003، ص10.

[1] ــ محمود القدوة، الحكومة الإلكترونية والإدارة المعاصرة، دار أسامة للنشر والتوزيع، الأردن، ط 1، 2010، ص 18.

[2] ــ يفضل البعض من الفقهاء مثل السيد باز وعبد الفتاح بيومي حجازي تسمية **"الإدارة العامة الالكترونية" أو المنظمة العامة الالكترونية"** تمييزا لها عن الحكومة بمفهومها العام في القانون الدستوري، وعن الإدارة الالكترونية الخاصة" ، التي تخدم القطاع الخاص في كافة مجالاته. عبد الفتاح بيومي حجازي، مرجع سابق، ص 45.

[3] ــ هناك ترابط وتداخل مفاهيمي بين الحكومة الإلكترونية والإدارة الإلكترونية على اعتبار أنهما يشتركان في استخدام الوسائل الإلكترونية ومختلف الشبكات في المنظمات الحكومية، في حين أن العلاقة بينهما هي علاقة الجزء بالكل، فالإدارة الإلكترونية هي الجزء وتعني تحويل جميع العمليات الإدارية ذات الطبيعة الورقية إلى عمليات ذات طبيعة إلكترونية باستخدام التطورات التقنية الحديثة "العمل الإلكتروني" أو الإدارة بل الأوراق، وتعمل الإدارة الإلكترونية على تطوير البنية المعلوماتية داخل المؤسسة، وبعبارة أخرى تطبيقها مقتصرة على حدود المنظمة فقط. أما الحكومة الإلكترونية تمثل الكل، وتعني بها العمليات الإلكترونية التي يتم من خلالها الربط بين المنظمات التي تطبق الإدارة الإلكترونية وذلك من خلال التشغيل الحاسوبي ذي التقنية العالية، مما يعني أن الإدارة الإلكترونية هي مرحلة سابقة من الحكومة الإلكترونية. أنظر: محمود القدوة، مرجع سابق، ص 23.

[4] – يوسف أبو فارة، دور إدارة أمن المعلومات في فاعلية الحكومة الإلكترونية، ورقة عمل مقدمة إلى مؤتمر ''أمن المعلومات والحكومة الإلكترونية'' المنعقد بكوالالمبور ــ ماليزيا، أبريل 2009، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، 2010، ص 106.

[5] ــ نفس المرجع، ص 107.

الحكومة الإلكترونية. وتتمحور مختلف التعاريف حول أتمتة وتحويل العمليات والأنشطة الحكومية إلى شكل الكتروني، يمكن من خلاله تقديم الخدمة عن بعد للمواطن وقطاع الأعمال باستخدام وسائل وشبكات الاتصال الحديثة كالانترنت والهواتف وغيرها، مع ضمان السرية والأمن للمعلومات، مما يكفل فعالية الخدمة وأدائها.

الحكومة الإلكترونية لا تقتصر على استخدام تكنولوجيا المعلومات لتقديم الخدمات للمواطنين، إنما هي فكر متجدد يعيد صياغة المؤسسات بشكل جديد، وأنّ الديموقراطية هي أحد الأهداف الرئيسية للحكومة الإلكترونية وهي العمل على مشاركة المستفيدين من خلال مشاركتهم عبر تلك الآليات، كما أن الحكومة الإلكترونية تمثل عقدا جديدا بين المؤسسات والمستفدين حيث يتحول المستفيد من متلق للخدمة إلى مشارك في صنع القرار[1].

لدى سعت مختلف الدول لتحقيق مفهوم الحكومة الإلكترونية في الواقع فعلا وتطبيقا، إلا أنّ مستوى الإستجابة في العمل الواقعي جاءت متفاوتة نظرا لعوامل وظروف، أهمها الدعم المادي بالنظر إلى التكاليف الباهضة التي يتطلبها تطبيق الحكومة الإلكترونية لاسيما البنية التحتية، وتأهيل الموارد البشرية...وغيرها. ولهذا كان التحوّل للحكومة الإلكترونية متدرّجا، يبدأ بأهم وأكثر القطاعات الحكومية خدمة، ووفقا لخطط إستراتيجية ترسمها كل دولة[2].

فالتحوّل إذن إلى الحكومة الإلكترونية كأسلوب جديد لتقديم الخدمات وتوفير المعلومات مطلب ملح لمختلف الدول، نظرا لأهميته في عالم اليوم، من خلال ما توفره من مزايا حيث أصبح الأداء الحكومي من خلال سرعة الخدمة وتقديمها من نافدة واحدة يوفر على المتلقي الوقت والجهد والنفقات، واعتماد نماذج إدارية تسهم في توحيد أسلوب العمل الإداري، وتحقيق العدالة، وبالتالي القضاء على البيروقراطية والفساد الإداري.

---

[1] ــ شعبان فرج، الحكومة الإلكترونية، إطارها النظري والمفاهيمي، بحث مقدم إلى الملتقى العلمي الدولي الأول حول"متطلبات إرساء الحكومة الإلكترونية في الجزائر: دراسة تجارب بعض الدول"، المنعقد بالجزائر بتاريخ: 13 و14 ماي 2014، جامعة سعد دحلب البليدة، بحث غير منشور، ص 3.

[2] ــ في الجزائر مثلا تم إطلاق موقع جديد بإسم "موقع البوابة الالكترونية لخدمات المواطن الجزائري"، يعتبر بمثابة نقطة وصل بين المواطن والإدارة، حيث يمكنه الاستعلام عن كل ما يشغله من وثائق وإجراءات إدارية، فيمكن من خلال هذا الموقع مثلا طلب الوثائق عبر الانترنت مثل وثيقة السوابق العدلية، وهذا الرابط هو:

www.elmouwatin.dz تاريخ الإطلاع:2016/02/12

لذلك سارعت العديد من الدول المتقدمة منها والنامية في تطبيقها[1] نتيجة لإدراكها بأهميتها في العصر الرقمي، ومن بين تلك الدول كانت الجزائر التي أولت إهتماما خاصا بتكنولوجيات الإعلام والإتصال ودمجها في المؤسسات العمومية بهدف تطوير الإدارة، وتحسين الخدمات المقدّمة للمواطنين، لتُطلق بعد ذلك وزارة البريد وتكنولوجيا الإعلام والاتصال برنامج "الجزائر الإلكترونية 2009 ــ 2013"، الذي تم فيه التشاور مع المؤسسات والإدارات العمومية والمتعاملين الإقتصادين العموميين والخواص والجامعات ومراكز البحث والجمعيات المهنية التي تنشط في مجال تكنولوجيا الإعلام والإتصال، إذ شارك أكثر من ثلاث مائة شخص في طرح الإفكار ومناقشتها خلال 6 أشهر، وتتضمن 13 محورا تحدد الأهداف الرئيسة التي كان مزعما إنجازها إلى غاية 2013 [2][3].

---

[1] ــ أفادت هيئة الأمم المتحدة ضمن تقرير ''الأمم المتحدة للحكومات الإلكترونية 2016'' بخصوص مؤشر تطور الحكومة الإلكترونية في دول العالم بأن المملكة المتحدة وايرلندا الشمالية تحتل المرتبة الأولى عالميا في مجال الجاهزية المعلوماتية تليها استراليا السويد ثم استراليا فكوريا الديموقراطية سنغفورا ثم فرلندا والسويد، وفي المقابل تأتي دول جنوبي آسيا الوسطى وأفريقيا في آخر قائمة الدول، واحتلت الجزائر في هذا التقرير المرتبة 150، في حين تتقدمها تونس برتبة 72 والمغرب 85 ومصر 108. لمزيد من التفاصيل انظر: استطلاع الأمم المتحدة للحكومة الإلكترونية بعنوان" الحكومة الإلكترونية لدعم التنمية المستدامة" المنشور على الموقع التالي:

https://publicadministration.un.org تاريخ الإطلاع: 12/08/ 2016

[2] ــ راجع مشروع الجزائر الإلكترونية 2013 المنشور على موقع وزارة البريد وتكنولوجيا الإعلام والإتصال: حيث تم الاطلاع عليه بتاريخ:2016/01/24.

http://www.premier-ministre.gov.dz/arabe/media/PDF/Dossier/Telecom/EAlgerie.pdf

[3] ــ فعلا تم بدأ تطبيق برنامج '' الحكومة الإلكترونية بالجزائر من قبل اللجنة الإلكترونية وتم تحقيق العديد من العمليات منها:

ــ تنصيب شبكة حكومية داخلية Intranet والتي اختصارها(RIG) وهي نظام شامل يتضمن مجموعة الوسائل الحديثة للإتصال على مستوى الحكومات العالمية.

ــ كذلك على مستوى الوظيف العمومي وعلى مستوى مصلحة الموارد البشرية تم وضع برنامج IDARA، أما فيما يخص التسيير التنبؤي لعمال الوظيف العمومي، قد تم تنصيب شبكة معلومات تربط الإدارات مع الهياكل المركزية والمحلية المكلفة بالوظيف العمومي.

ــ أتمتة العديد من المعلومات المتعلقة بمختلف الدوائر الحكومية عبر مواقع الويب مثل موقع إدارة الضرائب، موقع مجلس الدولة، موقع رئاسة الجمهورية، موقع الأمانة العامة للحكومة، موقع وزارة البريد وتكنولوجيا الإعلام والإتصال...إلخ.

ــ كما أخذت وزارة الداخلية والجماعات المحلية على عاتقها عملية تقنين الخدمات الإلكترونية بإطلاق ورشة كبرى لعصرة الإدارة المركزية والجماعات المحلية وذلك بالوضع التدرجي لنظام وطني للتعريف المؤمن يتمثل في ما يلي:

ــ إطلاق بطاقة التعريف الوطنية البيومترية والإلكترونية(CNIBe).

ــ إطلاق جوازات السفر الإلكترونية والبيومترية.

ــ إنشاء البريد الإلكتروني.

ــ إعداد نظام الدفع البنكي والحسابات البريدية، بالإضافة لإنشاء موزعات بنكية (CAB,TPE,DAB) وتوزيع بطاقات السحب والدفع الإلكتروني.

ــ شبكة للإطلاع على نتائج إمتحانات شهادتي الباكلوريا والتعليم المتوسط.

وعليه فتحول الإدارة الحكومية ومختلف أجهزة الدولة ومؤسساتها العامة إلى منظومة الحكومة الإلكترونية، واعتمادها على تقنية نظم المعلومات كأساس لتحقيق فعالية الحكومة الإلكترونية، يعني التحول من النطاق الورقي إلى النطاق الإلكتروني، حيث يزخر هذا النظام بالبيانات والمعلومات الرسمية والشخصية، وضمن شبكات إتصال مفتوحة ومتاحة للكافة. الأمر الذي يثير تخوفا كبيرا لدى متلقي الخدمة مواطنين أو قطاعات أعمال من الإستغلال غير المشروع، سواء من الغير أم من العاملين بها أنفسهم.

ذلك أنه قبل نشأة وظهور الحكومة الإلكترونية كان يتمّ الإحتفاظ بالبيانات والمعلومات في سجلات، وكان يتم الإحتفاظ بهذه السجلات في أماكن آمنة في المؤسسات الحكومية، حيث تعتمد على أسلوب الحماية المادية للوثائق، وتحديد من يسمح له بالوصول إلى هذه الوثائق. وقد تتطلب البعض منها الحصول على تصاريح وأذونات خاصة للإطلاع عليها وذلك لمنع التلاعب في هذه المعلومات والوثائق أو إستبدال النسخة الأصلية[1]، في حين أن التحول إلى الحكومة الإلكترونية يتطلب بالضرورة هجر الورق والدعائم المادية والإنطلاق في بيئة معنوية، قوامها أجهزة وإرساليات تقنية وشبكات اتصال مفتوحة ومتاحة للكافة، في كل زمان ومن أي مكان، مما تفقد ثقة المتعاملين بها لاسيما بعد إدراكم أنهم سيتعاملون مع الحكومة الإلكترونية من خلال رسائل بيانات متاحة على الشبكة، وأنهم قد يدفعون مبالغ مالية أيضا عبر هذه الشبكة التقنية، كل ذلك في غياب التوعية والتحضير المسبق، وقلة الثقافة بأمور التقنية، مما يؤدي إلى إحجام التعامل مع الحكومة الإلكترونية.

وتزداد المخاوف أكثر بسبب ظهور أنماط إجرامية مستحدثة كالجرائم المعلوماتية باعتبارها من الآثار السلبية التي خلفتها التقنية العالية، وأن هذه الجرائم تطال في اعتداءاتها قيما جوهرية تخص الأفراد والمؤسسات والدول في كافة نواحي الحياة، الإقتصادية، الثقافية، الأمنية[2].

ـــ التسجيل الأولي للحاملين الجدد لشهادة الباكالوريا.

[1] ـــ يوسف أبو فارة، مرجع سابق، ص 102.

[2]- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص 6.

لذلك ينبغي إيجاد الضوابط القانونية الكفيلة بحماية الحكومة الإلكترونية ضمن منظومة تشريعية تشمل الجوانب الجزائية فترصد السلوكات غير المشروعة التي يمكن أن تهدد العمل الحكومي الإلكتروني من جهة؛ ومن جهة أخرى، ونتيجة لخصوصية الجرائم الواقعة على الحكومة الإلكترونية من حيث سهولة ارتكابها، وأن تنفيذها لا يستغرق إلا دقائق معدودة، وأن محو آثارها وإتلاف أدلتها غالبا ما يلجأ إليه عقب ارتكاب الجريمة، وهي ليست محصور في نطاق إقليمي لدولة بعينها ممّا يجعلها من الجرائم العابرة للحدود، فضلا على أن مرتكبها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية للمعطيات، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام أجهزة إنفاذ القانون، لاسيما إثبات هذه الجرائم وآلية مباشرة إجراءات الاستدلال والتحقيق عبر البيئة الإفتراضيّة لتعقب المجرمين وتقديمهم للعدالة.

من هنا تأتي أهميّة موضوع البحث الذي حاولنا من خلاله مناقشة الآليات القانونية لحماية الحكومة الإلكترونية التي لم تكن معروفة للقانون الجزائي سواء الموضوعي أو الإجرائي، وهي موضوعات لا تزال بكرا و لم تنل حظها من البحث والتمحيص على مستوى الفقه الجنائي، إذ أغلب الدراسات المنشورة في مجال الحكومة الإلكترونية اقتصرت البحث فيه كوسيلة لتحقيق الإصلاح الإداري[1] دون محاولة الخوض في مسألة حماية التعاملات الإلكترونية الحكومية جزائيا.

وتتجلى أهمية الموضوع أيضا في بعث الثقة بالأمن المعلوماتي في التعاملات الحكومية الإلكترونية من خلال حماية البيانات والمعلومات من عمليات الوصول غير المرخصة والمشروعة، ويمنع أيضا إجراء تعديلات عليها في مراحلها المختلفة(في مرحلة المعالجة ومرحلة التخزين والنقل...)، كما أنّ الأمن المعلوماتي يتيح المجال للمستخدمين للوصول إلى البيانات والمعلومات للحصول على حاجاتهم منها.

---

[1] ــ كمثال على هذه الأبحاث والكتب لدينا على سبيل المثال:

ــ كتاب (دور الحكومة الإلكترونية في صناعة القرار الإداري والتصويت الإلكتروني) من تأليف الدكتور بشير علي الباز، ــ أيضا كتاب (الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام وأعمال موظفيه) لدواود عبد الرزاق الباز، ــ وكتاب (أثر الوسائل للإلكترونية على مشروعية تصرفات الإدارة) لأمل لطفي حسن جاب الله، بالإضافة إلى العديد من المؤتمرات كالتصدي للفساد الإداري من خلال التحول إلى الإدارة الإلكترونية، للدكتور هشام عبد المنعم عكاشة، بحث مقدم إلى مؤتمر الكويت الأول للقانون والحاسب الآلي، منشور في كتاب أبحاث المؤتمر، الطبعة الأولى1994. وبحث الحكومة الإلكترونية والمرفق العام للدكتور ماجد الحلو، بحث مقدم إلى المؤتمر العلمي الأول الذي نظمته أكاديمية شرطة دبي "الجوانب القانونية والأمنية للعمليات المصرفية" المنعقد في الفترة 26 ــ28 أبريل 2003.

وخلاصة القول أن أمن معلومات الحكومة الإلكترونية يهدف إلى حماية المصالح الثلاث[1]:

- سرية المعلومات: وذلك بجعلها متاحة فقط لفئات الأفراد والنظم المرخص لها بالوصول إلى هذه المعلومات وتسلمها؛
- سلامة المعلومات: بمعنى منع إجراء أي تعديل، وأن التغييرات التي قد تتم على المعلومات تجرى فقط بواسطة الأفراد المرخص لها بإجراء هذه التغييرات؛
- إتاحة المعلومات: حيث يتم التأكد من أن المعلومات تكون متاحة لفئة الأفراد المرخص لها بالحصول على هذه المعلومات، وأن تتمكن من الوصول إلى هذه المعلومات والحصول عليها في الوقت المناسب دون تأخير.

تهدف هذه الدراسة إلى تسليط الضوء على موضوع الحكومة الإلكترونية وحمايتها جزائيا، وهي من المواضيع إضافة إلى كونها مستحدثة، أيضا مبعثرة في تشريعات متفرقة تختلف طبيعتها وموضوعها، الشيئ الذي يصعب معه تجميعها وتنظيمها في إطار واحد، ولكنه مع صدور القانون رقم (15/04) المؤرخ في العشر من نوفمبر عام 2004 المتمم للأمر رقم (66 ــ 156) المتضمن قانون العقوبات الجزائري[2] حاولنا التركيز على الجرائم التي تناولها القانون الأخير بالتجريم، وبعض الجرائم المنصوص عليها في قوانين متفرقة.

نظرا لخصوصية الجرائم الواقعة على الحكومة الإلكترونية باعتبارها جرائم مستحدثة مرتبطة بالتقنية المعلوماتية، فإنها تثير العديد من المشكلات في نطاق قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم جرائم تقليدية لا توجد صعوبات كبيرة في إثباتها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ الإقتناع الشخصي للقاضي الجزائي.

---

(1) - Jaeger, Paul, and John Carlo, E –Government Education in Public Libraries : New Services Roles and Expanding Sosial Responsabililities, Journal of Education for Library and Information Science, vol 50 n° 1, 2009, p. 39.

(2) ــ قانون رقم 04 ــ 15 ، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66ــ 156 المؤرخ في 08 يونيو سنة 1966 المتضمن قانون العقوبات، ج.ر، عدد 71، لسنة 2004.

الأمر الذي كان عاملا حاسما لتدخل المشرع بنصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعمة بالتقنية ذاتها، ليُمكن من خلالها استنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم ووسائل ارتكابه، مما أدى إلى ظهور نوع جديد من الأدلة وهو الدليل الإلكتروني.

لأجل ذلك قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون رقم (22/06) المؤرخ في 20 ديسمبر 2006[1]، بالإضافة إلى إصداره للقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتّصال ومكافحتها[2]، ومن خلالها أوجد المشرع طرقا إجرائية حديثة تتفق والطبيعة التقنية للجريمة المعلوماتية.

بناء على ما تقدم، تتمحور إشكاليّة البحث حول: **ما مدى فاعلية التشريعات الجزائية الموضوعية منها والإجرائية في مواكبة التطور التكنولوجي والمعلوماتي الحاصل على نحو يحقق حماية جنائية للمعاملات الالكترونية الحكومية؟**

ويتفرع عن هذا الإشكال بعض التساؤلات أهمها:

أ. ماهي خطة التشريعات الجزائية في تجريم أفعال الاعتداء الواقعة على الحكومة الالكترونية؟

ب. هل تكفي القواعد الإجرائية المقررة للجرائم التقليدية في البحث والتحري لكي تسري على الجرائم الواقعة على الحكومة الالكترونية؟

ج. ماهو الدليل المناسب لإثبات الجرائم المستحدثة الواقعة على المعاملات الالكترونية الحكومية وآليات تنفيذها أمام القضاء، وكيف نضمن مصداقية هذا الدليل وأنه يعبر بالفعل عن الحقيقة التي تهدف إليها الدعوى الجنائية؟

إن البحث في الحماية الجنائية للحكومة الالكترونية، في الحقيقة يثير جملة من الصعوبات، ذلك أن موضوع البحث موضوعا حديثا لم يسبق بحثه بتعمق من الناحية الجزائية بالتحديد، ولو أن هناك

---

[1] – القانون رقم 06ـــ22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66 ـــ 155 المؤرخ في 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية الجزائري، ج.ر، ع 84، لسنة 2006.

[2] – القانون رقم 09 ـــ04 المؤرخ في 14 شعبان 1430هـــ ، الموافق لـــ 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتّصال ومكافحتها، ج.ر ع 47، الصادرة في 16 أوت لسنة 2009.

مجموعة من البحوث عالجت البحث من الناحية الإدارية، وحتى الجنائية ولكن بشكل جزئي، أو أنها عالجته بشكل سطحي.

فضلا عن ذلك، ارتباط الجرائم محل الدراسة بالحاسب الآلي، مما تتطلب الإحاطة بجانب التقنية كالحاسوب أو الشبكات ومختلف البرامج الأساسية، وكل ما يتعلق بالحكومة الالكترونية، وهذا يحتاج إلى جهد فني فضلا عن الجهد القانوني.

كما صادف البحث إشكال الحصول على اجتهادات المحكمة العليا، فهي جد قليلة، بل نادرة فيما يتعلق بجرائم الاعتداء الواقعة فعلا على الحكومة الالكترونية، لأنه غالبا ما تقع على الأفراد والمؤسسات الإقتصادية الخاصة، مما يتعذر معه الوقوف على موقف القضاء الجزائري من بعض المسائل الإجتهادية المتعلقة بموضوع الدراسة، لذلك كان لابد من التعرض إلى مواقف كل من القضاء الفرنسي وبعض التشريعات المقارنة من أجل تجاوز هذه الصعوبات.

حرصا على أن ننتهج في دراستنا هذه سبيلا منطقيا، تم اتباع منهج ذو ثلاث أبعاد، منهج تأصيلي، تحليلي ومقارن.

منهج تأصيلي أولا، من أجل رد الفروع والجزئيات إلى أصولها العامة الواردة في القانون الجنائي. وتحليلي ثانيا، من خلال إتباع طريق النصوص القانونية والأحكام القضائية بالتحليل مقتصرين على ما يتعلق مباشرة بالموضوع، فنحلل كل جريمة على حدى، أمّا المنهج المقارن فيظهر جليا من خلال مقارنة الحماية الجنائية للحكومة الإلكترونية في القوانين العربية كالتشريع الجزائري والمصري، السعودي، مع بعض التشريعات الأجنبية وبصفة خاصة في القانون الفرنسي، وفي الولايات المتحدة الأمريكية، وفي التشريع الإنجليزي.

ستتم معالجة هذا الموضوع من خلال البابين التاليين:

الباب الأول: الحماية الجنائية الموضوعية للحكومة الإلكترونية.

الباب الثاني: الحماية الجنائية الإجرائية للحكومة الإلكترونية.

الباب الأوّل

الحماية الجنائيّة الموضوعيّة للحكومة الإلكترونيّة

إن التطور الكبير الحاصل في مجال تكنولوجيا الإعلام والإتصال، والذي امتد أثره إلى كافة جوانب الحياة العامة، أحدث تغييرا جوهريا في شكل ودور الإدارات والأجهزة الحكومية وعلاقتها مع بعضها البعض ومع المواطنين، فكان الغرض من الاستعانة بهذه التقنية تحقيق دفعة تطويرية على أجهزة الدولة الخدمية منها والمعلوماتية، مما أدّى إلى التحول في تنفيذ المهام الحكومية من الطرق التقليدية إلى الطرق التقنية المستحدثة، وذلك باستخدام أجهزة الحاسب وشبكة المعلومات التقنية، وبالتالي ظهور ما يعرف بالحكومة الإلكترونية.

إذا كان التحول إلى الحكومة الإلكترونية في معناه هجر الورق والدعائم المادية والإنطلاق في بيئة تقنية معنوية، قوامها أجهزة وإرساليات تقنية وشبكات اتصال مفتوحة ومتاحة للكافة، في كل زمان ومن أي مكان، فإن هذا الأمر لا يزال يثير تخوفا كبيرا لدى المواطن العادي، الذي هو الهدف الأول للحكومة الالكترونية[1]، هذا التخوف يظهر حين يدرك هذا المواطن أنه سيتعامل مع الحكومة من خلال رسائل بيانات متاحة على الشبكة، وأنه سيؤدي مبالغ مالية أيضا، عبر هذه الشبكة التقنية، وأن ينتظر خروج ورقة أو أصول رسالة معنوية تخبره بإنجاز معاملته، أو بتمام تسديده للإلتزامات المالية المترتبة عليه، كل ذلك يتم في بيئة إفتراضية تسود فيها أنماط مستحدثة من الجرائم يصطلح على تسميتها بالجرائم المعلوماتية[2].

وقد عرف المشرع الجزائري هذه الجرائم من خلال المادة (2) من الفصل الأول من القانون رقم (09ـــ04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها المنوه عنه سابقا تحت عنوان "مصطلحات" بأنها: "جرائم المساس بأنظمة المعلجة الآلية

---

[1] ـــ أسامة أحمد المناعسة، مرجع سابق،، ص 14.

[2] ـــ لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة في البيئة الإفتراضية، فالبعض يستخدم الغش المعلوماتي، والآخر الإختلاس المعلوماتي، والبعض الآخر مصطلح الجريمة الإلكترونية...إلا أنه نرى أنها قاصرة الدلالة ويفضل مصطلح الجريمة المعلوماتية أو تقنية المعلومات وهو المصطلح المرادف نوعا ما لمصطلح " الجرائم المتصلة بتكنولوجيا الإعلام والإتصال" الذي آثر المشرع الجزائري استخدامه في القانون رقم (09 ـــ 04) المؤرخ في 14 شعبان الموافق لـــ 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على اعتبار أنه مصطلح عام يشمل التقنيات الحالية والمستقبيلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الأنترنت.

للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية". وهو تعريف حاول الإحاطة قدر الإمكان بجميع الجرائم الواقعة في البيئة التقنية سواء كان نظام المعالجة الآلية أداة أو محلا للجريمة.

هذه الجرائم تؤدي إلى خلل عام قد يهدد المجتمع كله في إقتصاده وسيادته وأمنه القومي، لاسيما وأن النظام المعلوماتي للحكومة الإلكترونية يتضمن بيانات رسمية، الأمر الذي يتطلب ضرورة إيجاد الضوابط القانونية الكفيلة بحماية الحكومة الإلكترونية من خلال توفير حماية موضوعية للحكومة الإلكترونية، بتحديد الجرائم الواقعة على المعاملات الالكترونية الحكومية وهو موضوع الفصل الأول، أما الفصل الثاني فسيخصص للجرائم الواقعة على وسائل إجراء وتنفيذ هذه المعاملات.

الفصل الأول: الجرائم الواقعة على المعاملات الحكومية الإلكترونية

الحكومة الالكترونية هي النّسخة الافتراضيّة للحكومة التقليديّة، غير أن مقرها الخوادم[1] الخاصة بمراكز حفظ البيانات للشبكة العالمية، وتمارس كل أعمال الحكومة في العالم الحقيقي سواء في علاقتها بالجمهور أو علاقاتها بجهات الأعمال أو علاقة مؤسساتها ببعضها البعض وحتى في علاقتها بموظفيها الذين يعدّون كزبائن داخليين.

وعادة ما يتمّ بناء بوابّة الكترونية موحّدة للدخول إلى تلك الخدمات التي يتمّ تنظيمها وتجميعها ضمن باقات خدمية عبر موقع الكتروني حكومي، تعكس من خلاله حاجات المواطن ومؤسسات الأعمال وليس الجهة الحكومية التي تقدمها[2].

ومن نماذج هذه الخدمات، تقديم الوثائق الرسمية مثل رخص قيادة السيارات والجوازات والوثائق المتعلقة بالحالة المدنية، وبطاقة السوابق العدلية، أيضا إبرام العقود الإدارية

---

(1) ــ الخادم أو المقلم أو المزود ويقال بالإنجليزية " Server "، وهو عبارة عن أجهزة كمبيوتر عادة ما تكون بمواصفات عالية تستخدم لاختزان ومعالجة ملفات المعلومات وقواعد بيانات الشبكة ومختلف البرامج. وتكون متصلة بالشبكة وتعمل على مدار 24 ساعة، ويقوم بتقديم خدمات للأجهزة الأخرى، فالمزود هو الجهاز الرئيسي في الشبكة وباقي الأجهزة المتصلة به عبارة عن عملاء "Client" لأنها تطلب خدمات معينة من الخادم. انظر:محمد محمد الهادي، الشارح لمصطلحات الكمبيوتر (إنجليزي ــ عربي)، دار المريخ للنشر، الرياض، 1988، ص 347.

(2) ــ عباس بدران، الحكومة الإلكترونية من الإستراتيجية إلى التطبيق، المؤسسة العربية للدراسات والنشر، بيروت، 2004، ص 46.

إلإلكترونية..إلخ[1]، وعليه ترتكز هذه المعاملات[2] على استخدام الإتصالات وتقنية المعلومات للقيام بالأعمال الحكومية، وهي لا تعتمد على الانترنت فقط بل أيضا على الفاكس والهاتف، حيث يمثلان عناصر من مكونات الإتصال في الحكومة الالكترونية[3].

المعروف أنّ أيّ جهاز حاسب آلي يتمّ توصيله بشبكة الانترنت يمكن اختراقه خلال ثلاث أيام لاسيما إذا كان خال من برامج الحماية، ونظرا لعدم وجود نظام معلوماتي كامل وخال من الإختراقات[4] سيؤدي ذلك إلى اختراق النظام بما في ذلك نظام الحكومة الالكترونية، وبالتالي الحصول على البيانات والمعلومات الرسمية، وهذا ما يفقد ثقة المواطنين بالحكومة الالكترونية.

من أجل بناء هذه الثّقة، ينبغي فرض حماية جزائية للنظام المعلوماتي للحكومة الالكترونية (المبحث الأول) على أساس أن أي اعتداء على المعلومات والبيانات الحكومية يتطلب الدخول إلى هذا النظام (المبحث الثاني).

---

(1) ــ للتوضيح أكثر يرجى زيارة أحد مواقع الالكترونية للحكومة الالكترونية مثل فرنسا وذلك على الموقع التالي:
https://www.service-public.fr/particuliers/vosdroits/services-en-ligne-et-formulaires

(2) ــ عرّف قانون المعاملات الالكتروني الأردني الجديد رقم (15) لسنة 2015، الصادر بتاريخ 15 أفريل 2015 المعاملات الالكترونية في مادته الثانية بأنها: "**أي إجراء يقع بين طرف أوأكثر لإنشاء التزام على طرف واحد أو التزام تبادلي بين طرفين أو أكثر سواء كان يتعلق هذا الإجراء بعمل تجاري أو التزام مدني أو يكون مع دائرة حكومية**، وأن هذه المعاملات تنفذ **بوسائل إلكترونية**". انظر في تفاصيل قانون التعاملات الالكتروني الأردني رقم (15) لسنة 2015 الموقع التالي:
http://www.lob.gov.jo/ تاريخ الإطلاع: 22/ 12/ 2015

أمّا قانون المعاملات الإلكتروني العماني رقم 96/ 2008 لسنة 2008 فقد عرف هوالآخر هذه المعاملات في المادة الأولى منه بأنها: "**إجراء أوعقد يبرم أو ينفذ كليا أو جزئيا بواسطة رسائل إلكترونية**".لمزيد من التفاصيل حول هذا القانون يرجى الإطلاع الموقع التالي:
http://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=1&PID=5&LID=7

أمّا المشرع السعودي فقد عرف المعاملات الإلكترونية من خلال ضوابط استخدام الحاسبات الآلية وشبكات المعلومات في الجهات الحكومية من خلال القرار رقم (81) المؤرخ في 19/ 03/ 1430هـــ، بأنها: "**أي تبادل أو تراسل أو تعاقد، أو أي إجراء آخر يبرم أو ينفذ بشكل كلي أو جزئي بوسيلة إلكترونية**". راجع في ذلك الموقع التالي:
http://www.yesser.gov.sa/ar/MechanismsAndRegulations/Regulations/Pages/control_computer_information_network-.aspx تاريخ الإطلاع: 22/ 12/2015

أمّا المشرع الجزائري لم يتطرق إلى هذه المعاملات الالكترونية بالتعريف بالرغم من استحداثه للبوابة الالكترونية المتعلقة بالصفقات العمومية عن طريق المرسوم الرئاسي رقم 10/ 263 المتعلق بتنظيم الصفقات العمومية، المؤرخ في 7 أكتوبر 2010، ج. ر عدد 58 لسنة2010 .

(3) ــ صفية بنت عبد الله أحمد بخيت، ضبط ومعايير أداء الحكومة الإلكترونية، ورقة عمل مقدمة ضمن بحوث مؤتمر " أمن المعلومات والحكومة الإلكترونية"، كوالالمبور، ماليزيا، أبريل 2009، مرجع سابق، ص 133. وانظر أيضا:

Samir Lahlou, E-Government ou Gouvernement Eléctronique, Bulletin d'information périodique (BIP), juin – 2002- n° 114, p 60.

(4) ــ محمود القدوة، مرجع سابق، ص 125.

المبحث الأول: جرائم الاعتداء على النظام المعلوماتي للحكومة الإلكترونية

من المعروف أنّ الحكومة الإلكترونيّة تعتمد على قاعدة بيانات[1] مخزنة في شبكات الحاسب الآلي أو تنساب خلالها عند التفاعل ما بين الجمهور وجهات الحكومة الإلكترونية، وأنّ النظام المعلوماتي للحكومة الإلكترونية معرض للعديد من التهديدات سواء كانت تقع بطريق مباشر على هذا النظام أو بطريق غير مباشر من خلال الخدمات الوسيّطة التي يقدمها الوسطاء ما بين العميل العادي في نطاق الحكومة الإلكترونية وما بين شبكة الأنترنت. ونظرا للدور الفنّي الكبير لهؤلاء، قامت التشريعات بحماية النظام المعلوماتي للحكومة الإلكترونية من خلال تحميل هؤلاء المسؤولية الجنائية.

وعليه سيتم التطرق إلى جرائم الإعتداء على النظام المعلوماتي للحكومة الإلكترونية بطريق مباشر وذلك في المطلب الأوّل، أمّا المطلب الثاني فسيخصص لجرائم الاعتداء غير المباشر على النظام المعلوماتي للحكومة الإلكترونية، وذلك على التفصيل الآتي:

المطلب الأول: جرائم الاعتداء المباشر على النظام المعلوماتي للحكومة الالكترونية

يتعرّض النظام المعلوماتي للحكومة الإلكترونية إلى الإختراق من قبل أفراد غير مصرّح لهم بالدخول إليه أو البقاء فيه، أو حتى إتلافه، وعلى الرغم من أن هذه الجرائم تعد مراحل سابقة وضرورية لارتكاب جرائم معلوماتية أخرى، مثل التزوير المعلوماتي أو الإعتداء على حرمة الحياة

---

[1] - يقابل قاعدة البيانات باللغة الفرنسية"Base de donnéés " وباللغة الإنجليزية "Data Base "، وهي عبارة عن مجموعة كبيرة من المستندات والوثائق تتناول موضوعا معينا (طب، هندسة، قوانين، الضرائب..)، يتم تنظيم وتصنيف محتوياتها ثم يقوم المتخصصون بتسجيل هذه المحتويات على أسطوانات متصلة بالحاسب، وتتميز هذه القاعدة بأنها تكون مرتبة ومصنفة بشكل يسهل عمليات البحث والإسترجاع لما ورد بها من معلومات. محمد سامي عبد الصادوق، حقوق مؤلفي المصنفات المشتركة،ا لمكتب المصري الحديث، ط 1، 2002، ص 456. وتدعى هذه قاعدة البيانات أيضا ببنك المعلومات، وهو مجموعة البيانات عن مجالات نشاط في المؤسسة مخزونة باستعمال إحدى وسائل التخزين المباشر. فاروق علي الحفناوي، قانون البرمجيات، دار الكتاب الحديث، القاهرة، 2002، ص 267.

والمشرع الجزائري تعرض لقاعدة البيانات في المادة 05 فقرة 02 من أمر رقم 05ـــ03 المتعلق بحقوق المؤلف والحقوق المجاورة الجزائري،حيث نص "...المجموعات والمختارات من مصنفات، مجموعات من مصنفات التراث التقليدي وقواعد البيانات سواء كانت مستنسخة من دعامة قابلة للإستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، والتي تأتي أصالتها من انتقاء موادها أو ترتيبها".الأمر رقم 05ـــ03 مؤرخ في 19جمادى الأولى عام 1424 الموافق 19 جويلية عام 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر،ع 44، لسنة 2003.

الخاصة وغير ذلك من الجرائم، إلا أن مرتكب هذا الفعل قد يقصده بحد ذاته دون أن يهدف إلى ارتكاب جرائم أخرى من ورائه.

والنظام المعلوماتي حسب المشرع الجزائري:" **هو نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيدا لبرنامج معين"**، وذلك ما جاء في الفقرة (ب) من المادة (2) من القانون رقم 09 ــ04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

وعليه يعد الاعتداء على النظام المعلوماتي لاسيما نظام الحكومة الالكترونية، من أهم جرائم المعلوماتية، كون هذا النظام يتم من خلاله العديد من عمليات المعالجة الآلية للمعطيات الحكومية، وتتمثل هذه الجرائم في الأساس على:

ــ جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي للحكومية الإلكترونية.

ــ والاعتداء على سير النظام المعلوماتي للحكومة الالكترونية.

ذلك ما سيتم تناوله على التفصيل الآتي في الفرعين التاليين:

الفرع الأول: جريمة الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي للحكومة الالكترونية.

أولت مختلف التشريعات اهتماما كبيرا بتجريم الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي للحكومة الالكترونية، ومن ذلك ما نصّ عليه المشرّع الفرنسي في المادة 323 ــ1 من قانون العقوبات[2] الصادر بالقانون رقم 19/88 والمعدل سنة 1994.

---

[1] - على الرغم من أن المشرع لم يحدد العناصر التي يتكون منها نظام المعالجة الآلية من مدخلات أو مخرجات وغيرها، وإنما اعتمد على عنصر عملية المعالجة الآلية في التعريف باعتبارها تنطوي على مراحل سابقة ولاحقة (الإدخال والخزن والنقل والتبادل...)، وهي تعتبر عناصر التبادل المتعلقة بالجوانب الاتصالية بالمعلومات ضمن مفهوم المعالجة، وما يبين ذلك عبارة "...المتصلة.."وكذا "...المرتبطة..." الواردتان ضمن نص المادة الثانية من قانون رقم (09ــ04) السابق الذكر.

[2] -Article 323-1de code pénal: « 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 60 000 € d'amende.

والمشرّع الأمريكي في قانون سنة 1984 الذي أقره الكونجرس الأمريكي بشأن تجريم الإتصال غير المرخص به، والغش وإساءة استعمال الكومبيوتر[1] والمعدل بموجب قانون إساءة استعمال الكمبيوتر لسنة 1994في المادة 1/1030، وغيرها من التشريعات الأجنبية منها والعربية كالمشرع السعودي مثلا وفقا لنظام مكافحة الجرائم المعلوماتية الصادر في 2007/3/26 في المادة الثالثة منه[2].

أمّا بالنسبة للمشرع الجزائري فقد حذا حذو المشرعين الفرنسي والأمريكي والسعودي ونص في المادة 394 مكرر فقرة أولى من قانون العقوبات الجزائري من خلال تعديله بالقانون رقم (04ـــ15) السابق ذكره على أنه: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أوجزء من منظومة للمعالجة الألية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتّب عن ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج " .

وعلى ذلك يلاحظ من خلال النصوص القانونية المتقدمة أنّ جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الألية تتخذ صورتين، الصورة الأولى تكون بارتكاب فعل الدخول أو البقاء بغش دون إحداث إتلاف أو تخريب للنظام وهي تمثل الصورة البسيطة، أما الصورة المشددة، فتتحقق

---

(1) - لمزيد من التفصيل حول هذا القانون " Computer Abus Amendment " يرجى الإطلاع على الموقع التالي: https://www.law.cornell.edu/uscode/text/18/1030 تاريخ الإطلاع:2016/12/13.

(2) ـــ تعتبر المملكة العربية السعودية خامس دولة عالميا من بين الدول الرائدة في استخدام "الخدمات الحكومية الرقمية"، حيث أنشات الحكومة الالكترونية في السعودية بموجب المرسوم الملكي رقم 7/ب/33181 بتاريخ 7 سبتمبر 2003، من قبل وزارة الاتصالات وتكنولوجيا المعلومات. ولتجسيد هذا المشروع فعليا سنت المملكة ترسانة قانونية في مجال المعاملات الإلكترونية وذلك بقرار مجاس الوزراء رقم 80 بتاريخ 7،3،1428 هـــ وتمت المصادقة عليه بموجب المرسوم الملكي رقم م/18 بتاريخ 1428/3/8 هـــ، وفي نفس التاريخ أصدر نظام مكافحة جرائم المعلوماتية بقرار مجلس الوزراء رقم 79. للإطلاع على هذه القوانين بالتفصيل أنظر هيئة الاتصالات وتقنية المعلومات بالمملكة العربية السعودية على الموقع التالي: .
http://www.citc.gov.sa/ar/Pages/default.aspx. تاريخ الإطلاع:2016/12/13.

بتوافر نتيجة عن فعل الدخول أو البقاء، ذلك ما سيتم تناوله بتفصيل من خلال دراسة كل صورة على حدة.

فالبحث إذن عن جريمة الدخول أو البقاء غير المشروع للنظام المعلوماتي للحكومة الإلكترونية، يقتضي تحديد أركان هذه الجريمة المتمثلة في الركن المادي (أولا) والركن المعنوي(ثانيا).

أولاـــ الركن المادي لجريمة الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي

يتكوّن الركن المادي في جريمة الدخول أو البقاء غير المشروع من مجرد سلوك الدخول أو البقاء في الجريمة في صورتها البسيطة، أو الدخول أو البقاء اللذان يؤديّان إلى نتيجة معينة في الجريمة في صورتها المشددة.

1 ـــ الصورة البسيطة لجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

يتمثّل الركن المادي لهذه الجريمة من نشاط اجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه، أو البقاء غير المصرح به كالآتي:

أ ـــ فعل الدخول غير المصرح به :

يقصد بالدخول غير المصرح به: الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام [1].

وقد عرفه نظام مكافحة الجرائم المعلوماتية السعودي لسنة2007[2] بأنه: "دخول شخص بطريقة متعمدة إلى حاسب ألي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها".

---

(1) -Bainbridge (David). Hacking the unauthorised access of computer system, the legal implication . M.L , Rev. March 1989 .vol 52 p. 237.

(2)ـــ صدر نظام مكافحة الجرائم المعلوماتية بقرار مجلس الوزراء رقم (79) بتاريخ 1428/3/7هـــ، وتمت المصادقة عليه بموجب المرسوم الملكي رقم م/17 بتاريخ 1428/ 3/8 هـــ الموافق لـــ 2007/3/27 م .

يتضح مما سبق أن فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الالكتروني[1].

فعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع وإنما يتخذ هذا الفعل وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق، بمعنى دون تصريح[2]، ويتحقّق الدخول غير المشروع إلى النظام المعوماتي بأحد الأمرين: أولهما ألا يكون هناك تصريح بالدخول بتاتا لدى من يقوم بالدخول، وثانيهما أن يوجد تصريح بالدخول، ولكن المصرح له يقوم بتجاوز الحدود التي رُسمت له في هذا التصريح، وسيوضح ذلك فيما يلي:

أ.1 ــ حالة عدم وجود تصريح إطلاقا:

يتم ذلك عن طريق اختراق النظام المعلوماتي، أي عن طريق الحصول على شفرات خاصة أو ادخال برنامج فيروس يتم دمجه في إحدى البرامج الأصلية للحاسب الآلي كي يعمل كجزء منه، ثم يقوم بتسجيل الشفرات التي يستعملها المستخدمون للدخول إلى الكمبيوتر، أو بأي وسيلة أخرى[3].

أ. 2 ــ حالة تجاوز التصريح:

في هذه الحالة يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له ويدخل إلى كامل النظام المعلوماتي أو إلى أجزاء أخرى يحظر عليه الدخول إليها، وهذا الفرض في الغالب يتمّ من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي[4].

ولا يعتد في هذه الجريمة بصفة مرتكب الفعل الاجرامي، وهو ما وضحته المادة 394 مكرر في فقرتها الأولى من قانون العقوبات الجزائري بقولها:"..كل من يدخل أو يبقى..."، سواء كان الفاعل

---

(1)ــ نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط 1، الأردن، 2008، ص 158.

(2) –Cour d'appel de Paris,,du 5 février 2014 , Bulltin crim 2015, n° 119. Disponible sur site suivante : https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000030635061

(3) ــ محمد مسعود محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، في القانون الجزائري والمقارن، رسالة ماجستير، كلية الحقوق، جامعة الاسكندرية، 2005، ص 115.

(4) - Cour , Cass, chombre crim, Lion, 03 Octobre, 2007. Arrét disponible sur site suivante: https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000017917792

يعمل في مجال الأنظمة أو لا علاقة له بنظام الكمبيوتر، سواء كان يستطيع الاستفادة من النظام أم لا، إنما يشترط أن لا يكون ممن لهم حق الدخول إلى النظام[1].

يتحقق الدخول غير المشروع متى كان مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه، من ذلك الأنظمة المتعلقة بأسرار الدولة أو التي تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة أو معلومات لا يمكن الاطلاع عليها[2].

لكي تقوم هذه الجريمة يجب ألا يكون النظام مفتوحا أمام الجمهور، لأنه لو كان كذلك فلا جريمة إذ يباح للجمهور الدخول والتجول في النظام[3].

لم يشترط المشرعين الجزائري والفرنسي لتوفر جريمة الاعتداء على نظام المعالجة الآلية على ضرورة توافر الحماية الفنية لهذا النظام، بل يكفي أن يكون غير مأذون له في ذلك. إلا أن هناك جانب من الفقه الفرنسي يرى ضرورة وجود نظام أمني لقيام الجريمة خاصة وأن توفر هذه الحماية الفنية والدخول بالرغم من ذلك إلى نظام المعالجة الآلية من شأنه أن يكون دليلا قاطعا على توفر القصد لدى الجاني، الذي لا يمكن أن يدخل صدفة، بل باستعمال طرق تقنية لخرق الحماية، غير أن هذا الاتجاه لم يتبن في فرنسا. وقد تأكد ذلك في حكم استئناف باريس الصادر في 5 أفريل 1994، تأكد من خلاله أنه ليس من اللازم لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول تمّ بمخالفة تدابير أمنية، وأنه يكفي لقيام الجريمة أن الدخول قد تم ضد إرادة المسؤول عن النظام[4].

الوضع في قانون العقوبات الجزائري مشابه للوضع في قانون العقوبات الفرنسي، إذ لم تبين المادة 394 مكرر إلى ضرورة أن يكون نظام المعالجة الآلية للمعطيات محمياً بجهاز أمان، وإنما جاء النص عاما، وعليه فان جميع الأنظمة سواء كانت محمية أو غيرمحمية تحظى بحماية هذا القانون.

---

(1)- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، الجزائر ، 2010، ص 11.

(2) ــ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999، ص 123.

(3) ــ محمد عبيد الكعبي، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة، 2010، ص 439.

(4)-Cour de cassation de Paris,chambre commercial,du 5 avril 1994, n° 91-21840 .disponible sur sit suivant: https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007032711

وتجدر الإشارة في الأخير إلى أن جريمة الدخول بدون تصريح إلى النظام المعلوماتي تعد من الجرائم الشكلية التي لا يتطلب لقيام الركن المادي فيها نتيجة ما، بالرغم من إمكانية حدوث أضرار معينة بالمعلومات سواء بمحوها أو بتعديلها أو إفساد نظام التشغيل نتيجة عملية الدخول غير المصرح له بالدخول إليه[1].

ب ــ فعل البقاء غير المشروع في نظام المعالجة الألية للمعطيات:

البقاء هو: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[2]، أو هو:"عدم وضع حد للتشعب داخل النظام مع الاعتقاد بأن ذلك يشكل خطأ"[3].

ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل نظام للمعالجة الآلية للمعطيات بدون قصد منه، كأن يكون الدخول قد تم عن طريق الصدفة بدون إرادة من الداخل، لكنه بعد اكتشافه بأنه داخل النظام يبقى فيه ولا يخرج منه في الوقت الذي كان يجب عليه مغادرته، فالبقاء هنا يبدأ من اللحظة التي يعلم فيها الجاني أنه داخل نظام غير مصرح له بدخوله ورغم ذلك لا يضع حدا لوجوده داخله ويبقى فيه[4].

والبقاء المعاقب عليه قد يتحقّق مستقلا عن الدخول إلى النظام وقد تجتمع الجريمتان كالتالي:

ب.1 ــ بالنسبة للبقاء المعاقب عليه كجريمة مستقلة:

يكون في حالة الدخول المشروع إلى النظام، سواء يكون مصرح به ولكن المتدخل تجاوز المدة المسموح له بالبقاء فيها داخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها بالرؤية أو الاطلاع فقط، أو يكون الدخول عن طريق الصدفة أو الخطأ، ويجب على المتدخل في هذه الحالة أن يقطع وجوده وينسحب فورا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي.

---

(1)- Cour d'appel de Lyon , du 17 janvier 2007.Bulletin criminel 2007, N° 236.disponible sur sit suivante : https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000017917792

(2)ــ علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون المنعقد :1 ــ3 مايو 2000، جامعة الامارات العربية المتحدة، العين، دولة الامارات العربية المتحدة، 2000، ص52.

(3) - Raymond Gassin, Fraude informatique, Dalloz 1995. n° 114 p. 19.

(4 -)Ib.id, n° 112, p, 19.

وما يجمع بين حالة البقاء بعد دخول مصرح به أو بعد دخول عن طريق الصدفة أو الخطأ أن الدخول في جميع هذه الحالات كان مشروعا، وبالتالي لا يمكن أن تطبق بشأنها أحكام جريمة الدخول غير المشروع، لأن هذه الأخيرة جريمة وقتية، لهذا تدخل المشرع الجنائي ليضيف سلوكا آخر إلى جانب الدخول غير المصرح به، وهو البقاء غير المشروع، والتي تعد جريمة مستمرة[1] وذلك في الفقرة الأولى من المادة 323 ــ 1 من قانون العقوبات الفرنسي بقوله" Ou de se maintenir" أي "أو البقاء"، ولقد طبق القضاء الفرنسي نص البقاء غير المصرح به في الحكم الشهير لمحكمة استئناف باريس الصادر في 5 ابريل 1994 وجاء في هذا الحكم أن القانون يجرم البقاء غير المصرح به داخل نظام الحاسب الآلي، سواء كان الدخول قد تم عن طريق الخطأ أو تم بطريقة مشروعة إلا انه اكتسب بعد ذلك صفة اللامشروعية كما لو فقد الفاعل حقه في البقاء نتيجة لخطأ من جانبه[2] .

ب.2 ــ وقد تجتمع جريمة البقاء غير المشروع مع جريمة الدخول غير المشروع:

وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام ويدخل إليه فعلا بالمخالفة لإرادة الشخص صاحب النظام أو من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك ويتحقق في هذا الفرض الاجتماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام[3].

وتجدر الاشارة إلى أن جريمة البقاء غير المشروع تعد من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة جرمية معينة، فيكفي البقاء غير المصرح به ليقوم الركن المادي لهذه الجريمة[4].

---

(1) -Raymond. Gassin .op. cit. n° 112, p, 19 .

وانظر أيضا نائلة عادل محمد فريد قورة، جرائم الحاسب الإقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، ط 2، القاهرة 2002، ص 361. وأيضا: جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، ط 1، دار النهضة العربية، القاهرة، 1992، ص 150.

(2) ــ محمد عيد الكعبي، مرجع سابق، ص 463.

(3) ــ علي عبد القادر القهوجي، الحماية الجنائية للبيانات...، مرجع سابق، ص 133.

(4) ــ نهلا عبد القادر المومني، مرجع سابق، ص 161.

2 ــ الصورة المشددة لجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

سبق الذكر أن المشرع يكتفي لقيام جريمة الدخول أو البقاء غير المشروع بمجرد وقوع فعل الدخول أو البقاء، دون أن يتطلب حدوث أيّ نتيجة معينة، لكن إذا نجم عن هذا الدخول أوالبقاء نتائج معينة ترتب على ذلك تشديد عقوبة هذه الجريمة، وليست كل النتائج محل اعتبار المشرع، بل هناك نتائج ثلاثة فقط يترتب عليها هذا الأثر القانوني، وهي حذف أو تغيير معطيات نظام المعالجة الألية للمعطيات، أو تخريب هذا النظام، وذلك حسبما أشارت إليها الفقرة الثانية والثالثة من المادة 394 مكرر من قانون العقوبات الجزائري[1]، بنصها: "...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة..."، وكذلك الفقرة الثانية من المادة 323ــ1 من قانون العقوبات الفرنسي، حيث تنص: "إذا نجم عن الدخول محو أو تعديل في المعطيات المخزنة في هذا النظام أو إتلاف تشغيل هذا النظام تكون العقوبة ثلاث سنوات وغرامة مقدارها 45000 يورو" [2].

ويكفي لتوافر الظرف المشدد أن تكون هناك علاقة سببية ما بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت وهي محو في النظام وعدم قدرته على أداء وظيفته أو تعديل البيانات، وهذه النتيجة هي التي اعتبرها المشرع ظرفا مشددا في هذه الجريمة[3].

كما لا يشترط أن تكون النتيجة الضارة مقصودة أي على سبيل الخطأ، فالظرف هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية وهي الدخول أو البقاء غير المشروع العلاقة السببية السابقة الذكر للقول بتوافره، إلا إذا أثبت الجاني انتفاء تلك العلاقة كأن يثبت أن التعديل أو محو المعطيات أو تخريب النظام يرجع إلى القوة القاهرة أو الحادث المفاجئ[4].

---

[1] ــ الأمر رقم 66 ــ 156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 04ــ 15 المؤرخ في 10 نوفمبر 2004، ج. ر ع 71 لسنة 2004.

[2] -Article 323-1 / 2 de code pénal constitue :" 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 100 000 € d'amende".

[3] ــ عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الالكترونية، الكتاب الثاني، الحماية الجنائية والمعلوماتية لنظام الحكومة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2003، ص 362.

[4] ــ أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط 1، 2007، ص 114.

ثانيا ــ الركن المعنوي لجريمة الدخول والبقاء في النظام المعلوماتي

جريمة الدخول أو البقاء داخل النظام بصورتيه البسيطة والمشددة جريمة عمدية ويستشف ذلك من نص المادة 394 مكرر من قانون العقوبات الجزائري بقولها: " كل من يدخل أو يبقى عن طريق الغش"، وهو ما نصت عليه المادة 323ــ01 من قانون العقوبات الفرنسي بقولها: "Frauduleusement"، وهذا التعبير يعني أن الفاعل يقدم على فعله أو امتناعه وهو يعلم بعدم شرعيته.

اذن جريمة الدخول أو البقاء داخل النظام المعلوماتي للحكومة الالكترونية جريمة عمدية لابد من توافر القصد الجنائي بعنصريه العلم والارادة، فيلزم أن تتجه نية الجاني إلى فعل الدخول أو البقاء في نظام الحكومة الالكترونية، وأن يعلم أنه ليس له الحق في الدخول إلى هذا النظام أو البقاء فيه[1].

ومن ثمة، فلا يتوافر القصد الجنائي إذا كان دخول الجاني داخل النظام مسموح به أي مشروع أو إذا وقع في خطأ كأن يجهل وجود حظر للدخول أو البقاء، ويكفي فيها توافر القصد الجنائي العام، ولا يشترط أيضا توافر قصدا جنائيا خاصا.

على خلاف التشريع الجزائري والفرنسي هناك بعض التشريعات تتطلبت نيّة خاصة لقيام جريمة الدخول أو البقاء غير المصرح بهما، فقانون إساءة استخدام الحاسبات الآلية لعام 1990 في المملكة المتحدة يتطلب لقيام جريمة الدخول أن ترتكب بنية ارتكاب جريمة أخرى كالسرقة أو التهديد أو النصب ...، وفي القانون البرتغالي للجرائم المعلوماتية لعام 1991 يشترط لقيام جريمة الدخول أن تكون لدى الفاعل نية الحصول لحسابه، أو لغيره على ربح أو فائدة غير مشروعة[2].

يمكن للقاضي الجنائي أن يستدلّ على توافر القصد الجنائي لدى الجاني إذا كان النظام المعلوماتي محاطا بنظام أمني وتم اختراقه، فنظام الأمن لا يعدو أن يكون وسيلة إثبات سوء النية من قام بانتهاك النظام ودخل بطريقة غير مشروعة.

---

(1) ــ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، 2007، ص 126.

(2) - Verguth (pascal),La répression des délits informatiques dans une perspectiveinternationale,Thèse de doctorat en Droit privé,à université de Montpellie, 1996,p p. 211. Disponible sur site suivant : ww.sudoc.abes.fr//DB=2.1/SET=1/TTL=1/CLK?IKT=1016&TRM=La+répression+des+délits+informatiques+dans+une+perspective+internationale.

وبالتالي فإذا توافر الركن المادي الذي يتخذ صور الفعل أو البقاء داخل النظام والركن المعنوي المتمثل في القصد الجنائي العام بعنصريه العلم والارادة قامت جريمة الدخول أو البقاء غير المشروع.

الفرع الثاني: جريمة الاعتداء على سير النظام المعلوماتي للحكومة الالكترونية.

لم يتعرض المشرع الجزائري لجريمة الاعتداء على سير النظام المعلوماتي للحكومة الالكترونية كجريمة مستقلة قائمة بذاتها، بل اكتفى بنتيجة إفساد النظام كظرف مشدد فقط لجريمة الدخول أو البقاء غير المشروع في المادة 394 مكرر/2 ، بخلاف المشرع الفرنسي الذي نص عليها بموجب المادة 323/ 2 ، وتنص على : "يعاقب كل من يقوم بتعطيل أو إفساد تشغيل نظام المعالجة الآلية للمعطيات بالحبس لمدة خمس سنوات وغرامة مقدارها 150000 يورو "[1].

ولذلك فإنه لتحقق هذه الجريمة يستلزم توافر الركن المادي والركن المعنوي، كالآتي:

أولا ــ الركن المادي لجريمة الإعتداء على سير النظام المعلوماتي للحكومة الالكترونية

يتمثل الركن المادّي إما في في تعطيل أو توقيف نظام المعالجة الآلية للمعطيات عن أداء نشاطه، وإما في فعل إفساد نشاط أو وظائف هذا النظام.

1 ــ تعطيل وتوقيف النظام: يقصد به كل فعل من شأنه أن يؤدي إلى إعاقة سير عمل نظام المعالجة الآلية للمعطيات، وذلك بإحداث عطب أو خلل بالشئ فيجعله لا يقوم بعمله بصورة طبيعية، مما يؤدي إلى الحد من سرعة النظام العلوماتي وجعله بطيئا أو يعطي نتائج غير مطلوبة[2].

ولا يشترط وقوع التوقف على كل عناصر النظام، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية (جهاز الكمبيوتر نفسه، شبكات الاتصال، أجهزة النقل...) أو المعنوية (البرامج والمعطيات....)[3]. ويحصل التعطيل أو التوقيف بأي وسيلة، فالمشرع لم يحدد وسيلة معينة، وتكون

---

(1) - Article 323 -2 /1de code pénal: "Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende".

(2) ــ محمد أمين محمد الشوابكة، جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط 1، عمان، الأردن، 1992، ص 223 ــ 224.

(3) ــ علي عبد القادر القهوجي، الحماية الجنائية للبيانات...، مرجع سابق، ص 139.

وسيلة التعطيل مادية إذا وقعت على الأجهزة المادية للنظام مثل تخريبها أو قطع شبكات الاتصال، وقد تكون وسيلة التعطيل معنوية إذا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات وذلك باتباع التقنيات التالية:

أ ــ إدخال برنامج فيروسي[1]؛

ب ــ استخدام قنابل معلوماتية[2]؛

ج ــ تعديل كلمة السر.

أو بأي وسيلة تؤدي إلى تباطؤ وارتباك في أداء النظام لوظيفته المعلوماتية. تطبيقا لذلك قضت إحدى المحاكم الفرنسية بتوافر جريمة الاخلال بالنظام من المتهم الذي قام بارسال رسائل كثيرة إلى أحد الأجهزة الخاصة بإحدى الشركات المنافسة ليتوهم هذا الجهاز أن الرسائل ترسل إليه من أجهزة متعددة، وتتضمن طلبيات شراء من الشركة، وقد كانت تلك الطلبات غير جدية وكان هدف المتهم منها أن يملأ الأجهزة الخاصة بهذه الشركة حتى تكون عاجزة عن تلقي طلبات جديدة، وبالتالي يحدث لها أضرار، لذا قضي بتوافر هذه الجريمة في تلك الحال.

2 ــ إفساد النظام المعلوماتي:

يقصد بالإفساد كل فعل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للإستعمال السليم، ذلك بأن يعطي نتائج غير تلك التي كان يجب الحصول عليها، أي أن الافساد يعني إعدام الشئ وجعله غير صالح للإستعمال مطلقا[3].

---

[1] ــ اشتق مصطلح الفيروس من العلوم البيولوجية، يعني به "السم"، وهو عبارة عن برنامج او جزء في الشفرة التي تدخل إلى الحاسب الآلي بهدف التخريب وتتميز بقدرتها على نسخ نفسها إلى نسخ كثيرة وقدرتها على الانتقال من مكان إلى مكان أو من حاسب إلى حاسب والاختفاء وتغطية محتوياته. انظر: رامي عبد العزير، الفيروسات وبرامج التجسس، دار البراء، الاسكندرية، 2005، ص 21 ــ 22.
وقد سجل أول اكتشاف للفيروس في مدينة "لاهور" في باكستان عام 1987، واطلق عليه اسم "Brain" إشتقاقا من الاسم الموقع على السطوانة التي يسكنها الفيروس. انظر: محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2004، ص 83.

[2] ــ القنبلة المعلوماتية "Bomb": هي نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخرى، فشكليا هي ليست ملفا كاملا وإنما شفرة تنظم إلى مجموعة ملفات يتم تقسيمهاإلى أجزاء متفرقة حتى لا يمكن التعرف عليها بحيث تتجمع فيما بينها بحسب الأمر المعطى لها في ساعة معينة أو في يوم معين أو عند حدوث واعقة معينة. أنظر: نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات، ورقة عمل مقدمة إلى المؤتمر الدولي حول أمن المعلومات "معا نحو تعامل رقمي آمن"، في 28 ــ2005/20،12، مسقط ــ سلطنة عمان، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، د.س.ن، ص 206.

[3] ــ أمال قارة، مرجع سابق، ص 116 ــ 119.

وعلى ذلك يختلف الافساد عن التعطيل، من حيث أن التعطيل يتيح فرصة إصلاح النظام المعلوماتي وارجاعه إلى حالته الطبيعية، إلا أن الافساد يترتب عنه انعدام صلاحية النظام المعلوماتي. كما ان الافساد يختلف عن التخريب المترتب عن فعل الدخول أو البقاء غير المشروع المنصوص عليه في المادة 394 مكرر/ 2 من قانون العقوبات الجزائري، في أن التخريب في حال الظرف المشدد لا يشترط فيه أن يكون قصديا، بينما يتطلب فيه هذا الشرط بالنسبة لجريمة الاعتداء على سلامة النظام المعلوماتي بما فيه نظام المواقع الحكومية الالكترونية[1].

ويتحقق الإفساد بأي وسيلة من شأنها أن تعوق سير النظام كالاعتداء المادي على النظام وذلك بتخريب الأجهزة المادية للنظام المعلوماتي أو قطع شبكات الاتصال أو بسكب أي مادة على الأجهزة، مما يترتب عليه تدمير النظام، أما الاعتداء المعنوي فيتم من خلال استعمال البرامج والفيروسات التي تؤدي إلى إعدام سير نظام المعالجة الآلية للمعطيات كنشر فيروسات بالنظام المعلوماتي.

وتجدر الإشارة إلى أن إتفاقية بودابست المتعلقة بالإجرام المعلوماتي الموقعة في 23 نوفمبر 2001[2] تطرقت إلى الاعتداء على سلامة النظام المعلوماتي في الفقرة الأولى من المادة 04 منها، إذ نصت على أنه: "يجب على كل طرف أن يتبنى الاجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية للتجريم تبعا لقانونه المحلي إذا أحدث ذلك عمدا ودون وجه حق، أي إضرار أو محو، أو تعطيل، أو إتلاف، أو طمس لبيانات الحاسب".

ومن بين الأهداف المقررة من هذا النص كما أشارت المذكرة التفسيرية لهذه الاتفاقية هو ضمان سلامة وحسن تشغيل المنظومة المعلوماتية[3].

---

[1] ــ هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية، معلقاعليها، دار النهضة العربية، القاهرة، 2007، ص 68.

[2] - Convention de Budapest sur la cybercriminalité, 23. XL.2001, disponible en ligne a l'adresse suivante :
http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf تاريخ الاطلاع: 2016/03/03

[3]- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني: الحماية الجنائية لنظام التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002، ص 41. وانظر أيضا: علي عبد القادر القهوجي، مرجع سابق، ص 141.

ثانيا: الركن المعنوي لجريمة الإعتداء على سير النظام المعلوماتي للحكومة الالكترونية

تعتبر جريمة الاعتداء على سير النظام المعلوماتي الحكومي بالتعطيل والافساد والتدمير جريمة عمدية، يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والارادة، إذ يجب أن تتخد إرادة الجاني إلى فعل الافساد، مع علمه بأن نشاطه الإجرامي يؤدي إلى الإعتداء على سلامة النظام المعلوماتي للحكومة الالكترونية[1].

فإذا قام شخص يتعامل مع النظام بطريقة مشروعة وبسبب إهمال منه بترتب تعطل أو افساد النظام نتيجة خطأ في التشغيل، ففي هذه الحالة لا تقوم الجريمة لانتفاء القصد الجنائي[2].

وهكذا إذا توافر الركن المعنوي بعنصريه العلم والارادة إلى جانب الركن المادي قامت الجريمة واستحق مرتكبها العقوبة المخصصة لهذه الجريمة، وتستخلص محكمة الموضوع توافر القصد الجنائي من عدمه من ظروف وملابسات الواقعة[3].

الفرع الثالث: العقوبات المقررة لجرائم الإعتداء المباشر على النظام المعلوماتي للحكومة الإلكترونية.

أقرّت مختلف التشريعات عقوبات لمرتكبي جرائم الاعتداء على النظام المعلوماتي بصفة عامة ونظام الحكومة الإلكترونية بصفة خاصة، وذلك من أجل بعث الثقة والأمان في نفوس متعاملي الحكومة الالكترونية، وذلك على النحو التالي:

أولا ــ عقوبة جريمة الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي :

تتخذ جريمة الدخول أو البقاء غير المشروع صورتان لكل واحد منهما عقوبتها، الأولى بسيطة والثانية مشددة، وسيتناول فيما يلي العقوبات الأصلية لهذه الجريمة في صورتيها، ثم يعرج على العقوبات التكميلية، وفيما بعد يبيّن عقوبة الإشتراك والشروع في هذه الجريمة.

---

(1) ــ خثير مسعود، مرجع سابق، ص 122.

(2) ــ عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، مرجع سابق، ص 43.

(3) ــ شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 130.

1 ــ العقوبات الأصلية:

تقرّر الفقرة الأولى من المادة 394 مكرر عقوبتين أصليتين على مرتكب جريمة الدخول أو البقاء غير المصرح بهما، وتشدد الفقرة الثانية من المادة نفسها عقوبة هذه الجريمة ، إذا نجمت عنها نتائج معينة، وسنتناول فيما يلي العقوبات في الجريمة البسيطة ثم في الجريمة المشددة.

أ ــ العقوبات الأصلية للجريمة البسيطة:

العقوبات الأصلية هي العقوبات التي قررها المشرع باعتبارها الجزاء الأساسي للجريمة. وقد عرفتها المادة 14 في فقرتها الثانية من قانون العقوبات الجزائري بأنها: "تلك العقوبات التي يجوز الحكم بها دون أن تقترن بها أية عقوبة أخرى". وفيما يلي سنوضح العقوبات الأصلية لجريمة الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي في صورتها البسيطة المقررة للشخص الطبيعي ثم للشخص المعنوي.

أ. 1 ــ بالنسبة للشخص الطبيعي:

نصّ المشرع الجزائري في المادة 394 مكرر من قانون العقوبات على عقوبة أصلية تتمثل في الحبس من ثلاثة اشهر(3) إلى سنة(1) والغرامة من خمسين ألف(50.000دج) إلى مائة الف دينار جزائري (100.000دج).

جعل المشرع للقاضي حدا أدنى وحدا أقصى للعقوبة حتى تكون له سلطة تقديرية في تفريدها بحسب ما تتطلبه الحالة المعروضة أمامه، ذلك أن بواعث ارتكاب هذه الجريمة كثيرة، وليس باعث الاكتشاف والفضول كباعث التجسس والربح، وغيرها كثير من الظروف الخاصة بكل فاعل وبكل جريمة مما يقتضي تفريد العقوبة. وهذه العقوبة التي قررها قانون العقوبات الجزائري تقترب كثيرا من العقوبة التي قررها قانون العقوبات الفرنسي لعام 1988، وهو أول قانون فرنسي يتناول جرائم المعطيات، وفي قانون العقوبات لسنة 1994 شدد من عقوبة تلك الجرائم وجعل لها حداً واحداً هو السنة (1) وألغي الحد الأدنى الذي جاء به قانون 1988 وهو الشهرين، ليسلب القاضي سلطته

التقديرية في التحكم بالعقوبة. وبالنسبة لعقوبة الغرامة فقد زادت أيضا في ظل قانون 1994 لتبلغ خمسة عشر ألف يورو (15000 يورو).

وفي تعديل آخر لقانون العقوبات الفرنسي في 21 جوان 2004 أصبحت العقوبة سنتين والغرامة ثلاثين ألف يورو (30.000 يورو). وقد احتفظ المشرع الفرنسي بالحد الواحد للعقوبة سواء كانت الحبس أو الغرامة، وضاعف كلا من العقوبتين، وهذا يعكس الرغبة القوية للمشرع الفرنسي في مواجهة هذه الجرائم.

ويلاحظ أنّ المشرع الفرنسي أولى إهتماما كبيرا بالمعطيات الشخصية التابعة للدولة، حيث شدد العقوبة في حالة ما إذا مس هذا الدخول أو البقاء غير المشروع هذه البيانات الشخصية في المادة 323 ــ3/1 من ق.ع.ف لتصبح العقوبة كالتالي الحبس لمدة 7 سنوات والغرامة(300.000 يورو)[1].

أ.2 ــ بالنسبة للشخص المعنوي:

أقرّ المشرع الجزائري مبدأ مساءلة الشخص المعنوي في القانون (04 ــ 15) المؤرخ في 11/10/ 2004 المعدل لقانون العقوبات السابق الذكر، وذلك في المادة 51 مكرر من هذا التعديل. كما حدّد في المادة 18 مكرر من نفس القانون العقوبات المطبقة على الأشخاص المعنوية والتي تتفق مع طبيعة هذه الأخيرة.

وبالنسبة لجريمة الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي يلاحظ أن المشرع حدد العقوبة الأصلية للشخص المعنوي في المادة 394 مكرر 04 من قانون العقوبات الجزائري، وهي الغرامة المضاعفة إلى خمس مرات عما هو مقرر على الشخص الطبيعي، وبالتالي تكون الغرامة المقررة عليه في جريمة الدخول والبقاء البسيطة تتراوح بين مائتين وخمسين ألف(250.000دج) وخمسمائة

(1) -Article 323-1/3 de code pénal : «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 150 000 € d'amende".

ألف (500.000دج)[1]، وفيما يخص القانون الفرنسي فقد نصّت المادة 323ـــ06 من قانون العقوبات بأن[2]:"الأشخاص المعنوية يمكن أن يحكم عليها بالمسؤولية الجنائية وفقا للشروط التي حدّدها المادة(121ـــ 02) وأنّ العقوبات المقررة عليها هي:

ـــ الغرامة وفق ما تنص عليه المادة 131 ـــ38 من قانون العقوبات.

ـــ العقوبات المحددة في المادة 131 ـــ39 من قانون العقوبات.

ـــ المنع المحدد في المادة 131 39 فقرة 02 بالنسبة للنشاط المهني الذي وقعت بمناسبته الجريمة".

ب ـــ العقوبات الأصلية للجريمة المشددة

سيفصل فيما يلي العقوبات الأصلية المشددة الموقعة على الشخص الطبيعي ثم الشخص المعنوي:

ب.1 ـــ بالنسبة للشخص الطبيعي:

تشدّد الفقرتان الثانية والثالثة من المادة 394 مكرر ق.ع جزائري عقوبة جريمة الدخول أو البقاء غير المصرح بهما إذا نجم عن هذا الدخول أو البقاء تخريب لنظام اشتغال منظومة المعالجة الآلية للمعطيات أو حذف أو تغيير لمعطياته فترفع العقوبة إلى ضعف تلك المقررة للجريمة المجردة أو البسيطة، سواء في حدها الأدنى الذي تضاعف من ثلاثة(3) اشهر إلى ستة (06) اشهر، أو في حدها الأقصى الذي تضاعف كذلك من سنة إلى سنتين، أما الغرامة فثبت حدها الأدنى عند خمسين ألف دينار جزائري (50000 د.ج) وارتفع حدها الأقصى إلى مائة وخمسين ألف دينار جزائري(150.000 د.ج) وذلك في حالة ما إذا أدى الدخول والبقاء إلى حذف أو تغيير

---

[1]ـــ والحكمة من مضاعفة الغرامة المقررة على الشخص المعنوي تتمثل في أنها لا تطبق لوحدها على الشخص الطبيعي، وإنما تطبق عادة إلى جانب عقوبة سالبة للحرية، كما أن المشرع راعى أيضا جانب الذمة المالية فهي لدى الشخص المعنوي أكبر منها لدى الشخص الطبيعي، مما جعله يضاعف الغرامة المفروضة على الأول.انظر محمد خليفة، مرجع سابق، ص 101.

[2]Article 323-6 de code pénal : «Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise".

للمعطيات أما إذا أدى الدخول أو البقاء إلى تخريب النظام فالغرامة تشدد للضعف أي تتراوح بين مائة ألف و مائتي دينار جزائري (100.000 دج إلى 200.000 د.ج).

وكذلك الشأن مع قانون العقوبات الفرنسي لسنة 2004 فقد رفع العقوبة إلى ثلاث سنوات (وسنتين للجريمة البسيطة) ورفع الغرامة إلى مائة ألف يورو (100.000 يورو)[1].

ب.2 ــ بالنسبة للشخص المعنوي:

تتمثّل العقوبة للشخص المعنوي عن الجريمة المشددة في الغرامة المضاعفة خمس مرات عما هو مقرر على الشخص الطبيعي، وتكون قيمتها في قانون العقوبات الجزائري بين مائتين وخمسين ألف (250.000دج) وسبعمائة وخمســـــين ألف دينار جزائري (750.000 د.ج)، وتكون قيمها في قانون العقوبات الفرنسي الجديد(2004) هي مائتين وخمس وعشرين ألف يورو (225.000 يورو).

تجدر الإشارة أن المشرع الجزائري شدد العقوبة في حالة الإعتداء على الجهات العامة وهو ما نصت عليه المادة 394 مكرر 3 من ق.ع بقولها: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أوالهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد". وعليه فالمشرع أولى اهتماما كبيرا بالمعطيات والنظام المعلوماتي التابع للدولة والجهات العامة، فشدد العقوبة إذا كانت المعطيات محل الاعتداء تتعلق بالدفاع الوطني وذلك نظرا لأهميتها ودورها في الحفاظ على سلامة التراب الوطني والأمن العام.

ولم تقصر المادة هذه الحماية على مؤسسة الدفاع الوطني، بل وسعتها لتشمل الهيئات والمؤسسات الخاضعة للقانون العام. والحكومة الالكترونية تعد إحدى هذه المؤسسات الرسمية ذات الطابع الخاص وذلك بما يمكن أن تحتويه أنظمتها المعلوماتية من بيانات ذات أهمية كبرى، فهي حكومة إفتراضية مقرها البيئة الإفتراضية، حيث تكون مستهدفة من طرف القراصنة ومجرمي المعلوماتية .

(1 -) Article 323-1/2 de code pénal :"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 100 000 € d'amende".

2 ــ العقوبات التكميلية:

نصت المادة 394 مكرر 6 من قانون العقوبات الجزائري[1] على مجموعة العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية وهي كالآتي:

أ ــ المصادرة[2]: تشمل الاجهزة والوسائل المستخدمة في ارتكاب الجريمة كالأقراص المضغوطة مثلا التي تبين طرق ارتكاب مثل هذه الجرائم، وذلك ببيعها أو حجزها، بشرط ألا تخل هذه المصادرة بحقوق الغير حسن النية. وهذا شرط يتعلق بالأشياء المملوكة لشخص غير المتهم، والغير وفقا لهذا هو كل أجنبي عن الجريمة تماما، أي كل من لا يسأل عنها و لم يكن قد أدين فيها بوصفه فاعلا أو شريكا، وتبثت ملكيته للشيء المضبوط[3].

ب ــ إغلاق المواقع: ويقصد بها مواقع الانترنت أو المواقع الإلكترونية[4] بصفة عامة والتي كانت وسيلة لإرتكاب هذه الجرائم أو ساهمت في إرتكابها. ولا يقصد المشرع هنا بالمواقع التي تكون محلا للجريمة تلك المواقع التي تتضمن أنظمة المعالجة الآلية للمعطيات والتي تم الاعتداء عليها بالدخول غير المشروع إليها، لأن هذه المواقع هي الضحية في تلك الجرائم، ومن تم فالتعبير الذي استعمله المشرع الجزائري في المادة 394 مكرر 6 غير سليم، وكان من الأولى أن يستعمل عبارة "المواقع التي تستعمل في ارتكاب الجريمة" بدل عبارة المواقع التي "تكون محلا لجريمة من الجرائم.."

---

(1) ــ حيث تنص المادة 394 مكرر 6 ما يلي: "مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

(2)ــ نصت على المصادرة المادة 15 من قانون العقوبات الجزائري بقوله: ''المصادرة هي الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الإقتضاء''. وهي عقوبة مالية، مادية أو عينية، تهدف إلى تمليك السلطات العامة أشياء ذات صلة بجريمة ما قهرا عن صاحبها وبغير مقابل. انظر: رؤوف عبيد، مبادئ القسم العام في التشريع العقابي، دار الفكر العربي، ط 1، القاهرة،2008 ، ص 868.

(3) ــ محمود نجيب حسني، شرح قانون العقوبات ــ القسم العام ــ النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، ط. 4، دار النهضة العربية ، 1977، ص 843.

(4) ــ عرّف مرسوم بقانون إتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات السابق الذكر في المادة الأولى منه أن الموقع الالكتروني هو:"مكان إتاحة المعلومات الالكترونية على الشبكة المعلوماتية، ومنها مواقع التواصل الإجتماعي، والصفحات الشخصية والمدونات".

ج ــ إغلاق المحل (المقهى الإلكتروني): وهو المكان الذي استعمله الجناة في ارتكاب جريمتهم، وكان يحوي الأجهزة التي استعملت في عملية الدخول أو البقاء غير المصرح بهما[1].ولا تطال هذه العقوبة (الغلق) الغير حسن النية.

أمّا بالنسبة لمدة عقوبة الغلق فلم تحدد المادة 394 مكرر 6 من قانون العقوبات الجزائري مدة معينة، وعليه بالرجوع للمادة 26 في الأحكام العامة لقانون العقوبات الجزائري، قد تكون مؤبدة أو مؤقتة.

وفي القانون الفرنسي تنص المادة 323 ــ 5 من قانون العقوبات على عقوبة الغلق في البند الرابع منها من بين العقوبات التكميلية المقررة للأشخاص الطبيعيين وقد حددت مدة الغلق لخمس سنوات أو أكثر، وتقع هذه العقوبة على المؤسسات أو على فروع المشروع الذي استخدم في ارتكاب الجريمة.

وفيما يخص العقوبات التكميلية لجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي في القانون الفرنسي نلاحظ أن قانون العقوبات الفرنسي لعام 1988 نص على عقوبة تكميلية واحدة هي المصادرة، أما قانون 1994 و 2004 فقد قدما في المادة 323 ــ 05 قائمة من العقوبات التكميلية كلها إختيارية، وتوقع على الشخص الطبيعي، وهي كالآتي[2]:

---

[1] ــ محمد خليفة، مرجع سابق، ص 97.

[2] -Article 323-5 de code pénal constitue:« Les personnes physiques coupables des délits prévus au présent chapitre encourent é galement les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 ".

ـــ الحرمان لمدة خمس سنوات أو أكثر من الحقوق الوطنية والحقوق المدنية وحقوق الأسرة وفق ما تقرره المادة 131 ـــ26.

ـــ الحرمان لمدة خمس سنوات أو أكثر من ممارسة وظيفة عامة، أو ممارسة نشاط مهني أو إجتماعي في المجال الذي ارتكبت فيه الجريمة.

ـــ مصادرة الأشياء التي استخدمت في الجريمة أو كامت معدة لاستخدامها فيها، أو نتجت عن الجريمة باستثناء الأشياء القابلة للإعادة.

ـــ الغلق لمدة خمس سنوات أو أكثر للمؤسسات أو لواحد أو أكثر من فروع المشروع الذي استخدم في ارتكاب الجريمة.

ـــ الإقصاء لمدة خمس سنوات أو أكثر من الصفقات العمومية.

ـــ المنع لمدة خمس سنوات أو أكثر من إصدار شيكات، ولا يمنع هذا من استرداد شيكات السحب الموجودة لدى المسحوب عليه أو الشيكات المعتمدة.

ـــ نشر أو تعليق الحكم المعلن ضمن الشروط التي تنص عليها المادة 131 ـــ 35.

3 ـــ عقوبة الإشتراك والشروع في جريمة الدخول أو البقاء غير المصرح بهما في النظام:

سنبين من خلال التالي العقوبة المقررة في الإشتراك والشروع في جريمة الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي، وذلك على النحو التالي:

أ ـــ عقوبة الإشتراك:

نصّ المشرع الجزائري في المادة 394 مكرر 5 من قانون العقوبات: "كل من شارك في مجموعة أو إتفاق تآلف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

يلاحظ من المادة المذكورة أنّ المشرع خرج نوعا ما عن القواعد العامة لقانون العقوبات حيث أن المادة 176 من ق.ع[1]نصت على الاتفاق الجنائي العام في الجنايات والجنح المعاقب عليها

[1] ـــ تنص المادة 176 من قانون العقوبات الجزائري: "كل جمعية أو إتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر أو لجنحة أو أكثر، معاقب عليها بخمس سنوات على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، ولقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل".

بخمس سنوات على الأقل، في حين أن جريمة الدخول والبقاء غير المصرح بهما تتراوح مدة عقوبتها بين 3 أشهر في الصورة البسيطة لها ومدة 6 أشهر في الصورة المشدّدة للجريمة.

وقد اكتفت هذه المادة في تجريمها للإشتراك العام بتلاقي الإرادات على ارتكاب الجريمة. في حين أن المادة 394 مكرّر 5 من ق.ع لا تكتفي مجرد العزم وإنما تتطلب للعقاب على الإشتراك أن يكون مجسدا بفعل أو أفعال مادية كأن يقوم المتفقون باقتناء برامج خبيثة كالفيروسات أو برامج اختراق يتم من خلالها الدخول غير المشروع لأنظمة الحاسبات الآلية. كما أن جرائم المعطيات ومنها جرائم الدخول والبقاء غير المشروع لا تتطلب إجتماعا حقيقيا بين شخصين أو أكثر، وإنما يتصور الإتفاق الجنائي بمجرد انتقال كلمة السر من شخص إلى آخر وإن لم يكون بينهما معرفة سابقة[1].

وعليه رصد المشرع الجزائري للشريك نفس عقوبة الجريمة التامة سواء كانت جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة أو المشددة.

نفس الأمر بالنسبة للمشرع الفرنسي حيث نص في المادة 323 ــ 4 من قانون العقوبات الفرنسي[2] على العقاب على الإتفاق الجنائي المجسد بالأعمال المادية " **La réparation a un groupement"** بنفس العقوبة التامة لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات.

ب ــ عقوبة الشروع[3]:

نصت المادة 394 مكرّر 7 من ق.ع جزائري على: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

---

(1) ــ مسعود خثير، مرجع سابق، ص 129.

(2) - Article 323-4de code pénal : « La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

(3) ــ تعرضت المادة 30 من قانون العقوبات الجزائري للشروع تحت عنوان المحاولة، فنصت على أن:" كل محاولة لارتكاب جناية تبتدئ بالشروع في تنفيذ الجناية أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو يخب أثرها إلا نتيجة ظروف مستقلة عن إرادة مرتكبيها حتى ولو لم يكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها".

بالرجوع إلى القواعد العامة للقانون الجنائي نجد أن الشروع في الجنح لا يعاقب عليه إلا بنص، وهذا ما نصت عليه المادة 31 من ق.ع جزائري[1] وبذلك نجد أن المشرع الجزائري قد تبنى فكرة العقوبة على الشروع في ارتكاب الجنح الماسة بنظام المعالجة الآلية للمعطيات وذلك لخطورتها وما تسببه من أضرار فادحة.

من خلال استقراء نص المادة 394 مكرر 5 من ق.ع الجزائري نجد أنها مشمولة بهذا النص أي أن المشرع الجزائري أخذ بفكرة الشروع في جريمة الاشتراك الجنائي.

إلا أنّ المشرّع الفرنسي أخرج جريمة الاشتراك أو الإتفاق الجنائي من نظام الشروع، لأن التحضير للجرائم الذي يتم في إطار إتفاق أو مجموعة تشكل في حد ذاتها محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع في الشروع[2].

لذلك يرى البعض بضرورة الاقتداء بالمشرع الفرنسي وإخراج الشروع من الاتفاق الجنائي وجعل هذا الأخير جريمة قائمة بذاتها، لأن العقاب على مجرد الشروع في هذا الاتفاق أو العزم يعد تجريما في مرحلة متقدمة جدا، وهي وجود الإرادة، الإرادة التي لم تلتق مع إرادات أخرى لأنها لو التقت لكان الإتفاق مكتملا. وعليه يجدر بالمشرع الجزائري أن يحدد بالتفصيل جرائم المعطيات التي ينطبق عليها هذا النظام دون جريمة الاتفاق الجنائي أو ما يعرف بالإشتراك[3].

ثانيا ــ عقوبة جريمة الإعتداء على سير النظام المعلوماتي للحكومة الالكترونية:

بما أنّ المشرع الجزائري لم يتعرض لهذه الجريمة، بل اكتفى بالنص على جريمة الدخول أو البقاء غير المصرح بهما في النظام، سنتعرض للعقوبة التي قررها المشرع الفرنسي بموجب الفقرة الأولى من المادة 323 ــ2 من قانون العقوبات الفرنسي على مرتكب جريمة إعاقة وإفساد نظام سير المعالجة

---

(1) ــ تنص المادة 31 من قانون العقوبات الجزائري على أن: "المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون. والمحاولة في المخالفة لا يعاقب عليها إطلاقا".

(2) ــ أمال قارة، مرجع سابق، ص 133.

(3) ــ محمد خليفة، مرجع سابق، ص 93.

اللآلية للمعطيات بما في ذلك الاعتداء على سلامة النظام المعلوماتي الحكومي من الاتلاف والتدمير بالحبس لمدة 5 سنوات والغرامة 150000 يورو[1].

كما رفع المشرع الفرنسي من عقوبة الحبس لمدة سبع (7) سنوات، وضاعف مقدار الغرامة إلى 300000 يورو[2]، في حالة ارتكاب هذه الجريمة (اي تعطيل وتعييب النظام) ضد نظام معالجة المعطيات الآلية للبيانات الشخصية التي تنفدها الدولة، ويرجع سبب تشديد عقوبة الحبس والغرامة في هذه الحالة حسب تقديرنا إلى دعم الثّقة في التعامل الرقمي واستخدام تكنولوجيا المعلومات وتشجيع التعامل بها دون تخوف من أي فعل إجرامي قد يكون من شأنه هدم التعامل الالكتروني بصفة عامة والحكومي بصفة خاصة.

المطلب الثاني: جرائم الاعتداء غير المباشر على النظام المعلوماتي للحكومة الالكترونية

يعتمد نظام الحكومة الالكترونية على قاعدة بيانات مخزنة في شبكات الحاسب الآلي تتضمن معلومات حكومية تكون محل الطلب من قبل العملاء أثناء إجراء المعاملات الحكومية الإلكترونية عبر مختلف الوسائط أهمها شبكة الانترنت، وهذا النظام يشارك في إعداده العديد من الأشخاص يساعدون العميل أو المستفيد في الوصول إلى شبكة الانترنت، يطلق عليهم "الوسطاء في تقديم خدمة الانترنت" وهم:

متعهّد خدمة الوصول، متعهد الايواء، والمنتج وناقل المعلومات، ومتعهد الخدمات، ومورد المعلومات، ومؤلف الرسالة.

نظرا لتشعب أدوار مقدمّي الخدمة الوسيطة عبر الانترنت سنوضح مدى مسؤولية بعض المهمين منهم كمتعهد خدمة الوصول، متعهد الايواء ومورد المعلومة من خلال ما جاء في بعض

(1) -Article 323-2/1 de code pénal:«Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende".

(2) -Article 323-2/2 de code pénal :« Lorsque cette infraction a été commise 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 sept ans d'emprisonnement et à 300 000 € d'amende".

التشريعات المقارنة وذلك في مطلب أول، أمّا المطلب الثاني سنخصّصه لدراسة المسؤولية الجنائية لمقدمي خدمات الانترنت في التشريع الجزائري.

الفرع الأول: مسؤولية مقدمي الخدمات الوسيطة في التشريعات المقارنة

إنّ طبيعة الدور الفنيّ الذي يقوم به الوسطاء له أثر كبير في تحديد مسؤوليتهم، ولا تثور صعوبة في تحديد المسؤولية العقدية لأنّ هؤلاء الوسطاء يرتبطون مع غيرهم بعقود إشتراك أو توريد، ولكن الصعوبة تثور بشأن تحديد المسؤولية الجنائية لهؤلاء.

وقد اختلفت التشريعات فيما يتعلق بالمسؤولية الجنائية لمقدمي خدمات الانترنت، فبعضها تنطبق عليها القواعد العامة للقانون الجنائي مثل القانون الأمريكي والبعض الآخر نظمها بتشريعات خاصة كالتوجيه الأوربي رقم 2000 ــ 31 الخاص بالتجارة الإلكترونية[1]، والقانون الفرنسي والقانون الألماني.

أولا ــ متعهد خدمة الوصول:

يطلق على متعهّد خدمة الوصول عدة تسميات منها: مزود الخدمة أو مقدم الخدمة، وهو أي شخص طبيعي أو معنوي يقوم بدور فني لتوصيل المستخدم إلى شبكة الانترنت، وذلك عن طريق عقود اشتراك تضمن توصيل العميل إلى المواقع التي يريدها[2].

فمتعهّد الوصول يقدّم خدمات ذات طبيعة فنية، تتمثل في ربط المشتركين بالمواقع أو المستخدمين الأخرين بالشبكة، وذلك عن طريق وضع الحاسب الخادم الخاص به (الذي يرتبط بصفة دائمة بالانترنت) تحت تصرف المشتركين، بحيث يسمح لهم بأن يتجولوا في هذه الشبكة، أو يدخلو إلى المواقع ويتبادلون الرسائل الالكترونية[3].

---

[1] ــ التوجيه الأوربي رقم 2000 ــ 31 الصادر بالإجماع في 8 حزيران (جوان) 2000، والمتضمن الأوجه القانونية لخدمات شركات المعلومات، لاسيما التجارة الإلكترونية.

[2] ــ مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، ط 1، 2000، ص 100.

[3] ــ جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2001، ص 116.

يتبّين ممّا سبق أن متعهد خدمة الوصول لا علاقة له بالمادة المعلوماتية أو بمضمونها أو بمضمون الرسائل المتبادلة على الشبكة، ودوره يتسم بالحياد، ومن ثم ليس له الاطلاع أو التعرف على مضمون الرسائل التي تمرّ من خلاله، وبالتالي فلا يمكن مساءلته عن طبيعة المادة المعلوماتية المقدمة[1].

هذا ما أكّدته أغلب التشريعات المقارنة سواء في الدول الأجنبية والعربية وسنوضح البعض منها على النحو التالي:

1ــ التوجيه الأوربي رقم 2000ــ31 الخاص بالتجارة الالكترونية الصادر بتاريخ: 2000/06/8[2]:

تضمن المبحث الرابع من هذا التوجيه لاسيما المواد من 12 ــ 15 مسؤولية المؤديين المهنيين، وقد أعفت المادة 12 /1 مزود الخدمة الوسيطة للأنترنت من المسؤولية عن الأعمال غير المشروعة التي يتضمنها الموقع إذا توافرت الشروط الآتية:

1 ــ ألا يكون مصدر الضرر (لم يبدأ النقل).

2 ــ ألا يكون قد اختار المرسل إليه الذي ينقل إليه المعلومات.

3 ــ ألا يختار المعلومات التي يقوم بنقلها أو يعدل فيها.

وتنص الفقرة الثانية من ذات المادة أن عمل مزود الخدمة يتضمن تخزين مؤقت للمعلومات التي يقوم بنقلها، إلا أن هذا التخزين المؤقت لا يجعله مسؤولا، ولا يجعل عمله يرقى إلى عمل متعهد الايواء. ومن ثمة لا يجب مساءلته.

كما تجيز الفقرة التالثة من المادة 12 من هذا التوجيه للدول الأعضاء أن تنص في قوانينها الداخلية على التزام مزود الخدمة بأن يوقف الخدمة ويستبعد المحتوى غير المشروع للموقع.

---

(1) ــ محمد حسين منصور، المسؤولية الالكترونية في مجال شبكات الانترنت، دارالنهضة العربية، القاهرة، 2002، ص 39.

(2)- Directive 2000/31/CE du Parlement européen et du Conseildu 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment de commerce électronique, dans le marché intérieur ("directive sur le commerce électronique").Disponible en ligne a l’adresse suivante:
http://www.wipo.int/edocs/lexdocs/laws/es/eu/eu107es.pdf :تاريخ الإطلاع:2016/12/09

يتضح من هذا التوجيه أنه يلزم مزودي خدمات الانترنت باتخاذ إجراءات سريعة لإزالة أو تعطيل الوصول إلى المعلومات غير المشروعة، وذلك بعد تحقق معرفته الفعلية.

كما أنّ هذا التوجيه يفرض بموجب المادة 15 منه الدول الأعضاء واجب الرقابة على مقدمي الخدمات أثناء تقديم الخدمات التي تشملها المواد 12 و13 و14 دون التعرض للإلتزامات العامة والقرارات الادارية الصادرة من السلطات الوطنية وفقا للتشريعات الوطنية[1].

ومع ذلك، فإن الدول الأعضاء قد تنشئ التزامات على مزودي الخدمات بإبلاغ السلطات العامة المختصة على وجه السرعة عن الأنشطة غير المشروعة من تلقاء نفسها أو بناء على طلبها[2].

2 ــ التشريع الفرنسي: نظّم المشرّع الفرنسي المسؤولية الجنائية لمقدمي خدمات الانترنت من خلال القانون رقم 2000 ــ 719 المتعلق يتعديل أحكام قانون حرية الإتصالات، والقانون رقم 2004 ــ 575 المتعلق يالثقة في الاقتصاد الرقمي.

أ ــ القانون رقم 2000 ــ 719 الصادر في 01 / 08 / 2000:

أصدر المشرّع الفرنسي بتاريخ 2000/08/01 القانون رقم 2000 ــ 719 بشأن تعديل بعض أحكام القانون المتعلق بحرية الاتصالات رقم 86 ــ 1067، والصادر في 30 سبتمبر 1986[3]، وقد أعفت المادة 8/43 من هذا القانون مزودي خدمات الانترنت من المسؤولية المدنية والجنائية عن محتوى الخدمات والمعلومات غير المشروعة، باستثناء الحالات التالية:

---

(1) - Le secret des communications est garanti par l'article 5 de la directive 97/66/CE. Conformément à cette directive, les États membres doivent interdire tout type d'interception illicite ou la surveillance de telles communications par d'autres que les expéditeurs et les récepteurs, sauf lorsque ces activités sont légalement autorisées.

(2)- أكمل يوسف السعيد يوسف، المسؤولية الجنائية لمقدمي المواد الإباحية للأطفال عبر الأنترنت، مجلة العلوم القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، العدد 14، 2011، ص19 .

(3) -LOI no 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication. Disponible en ligne a l'adresse suivante : ttps://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000402408 تاريخ الإطلاع: 09/12/ 2015

1 ــ اذا كان يقدم خدمات إضافية إلى جانب عمله الأصلي ــ توصيل العميل بشبكة الانترنت ــ كتخزين المعلومات، وفي هذه الحالة يسأل طبقا لأحكام الدور الجديد الذي يقوم به بصفته متعهد الايواء[1].

2 ــ إذا كان على علم بمحتوى البيانات غير المشروعة، خاصة إذا اتسمت بالطابع الاجرامي، و لم يقم باتخاذ الاجراءات الازمة لوقف إذاعتها عبر الانترنت، أو منع الوصول إليه[2].

تطبيقا لذلك قضت المحمكة العليا الفرنسية بتاريخ 22 ماي 2000 في قضية اتحاد طلاب اليهود التي رفعها ضد شركة Yahoo باعتبارها مزود الخدمة، أنها مسؤولة عن عدم مشروعية الاعلانات والأعمال التي تمت عبر موقعها المخصص لبيع أشياء تتعلق بالنازية بالمزاد العلني، ومسؤوليتها تنشأ فقط منذ العلم بالمحتوى غير المشروع للموقع[3].

ب ــ القانون رقم 2004 ــ575 المتعلق بالثقة في الاقتصاد الرقمي الصادر في: 2004/06/21[4]:

خصّص هذا القانون المواد من 05 إلى 06 من الفصل الثاني منه لتنظيم عمل مقدمي خدمات الانترنت" المؤديين الفنيين" " Préstataires Technique" أي **مقدمي الخدمات الفنية**، ووفقا للمادة 1/6 الأشخاص الذين يقتصر عملهم على تقديم خدمة الاتصال عبر الانترنت (أي مزود الخدمة) يجب أن يخطرو المشتركين في الخدمة عن وجود وسائل تقنية تسمح بغلق الخدمة أو توقع جزاءات عليهم إذا توافرت شروط توقيعها[5]. وأكدت الفقرة السابعة من هذه المادة أن مزودي

---

(1) ــ انظر فيما سيأتي ص 43.

(2) ــ محمد حسين منصور، مرجع سابق، ص 177.

(3) - TGI Paris, référé, 22 mai 2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France.
لمزيد من التفاصيل حول قضية إتحاد طلاب اليهود وشركةyahoo راجع الموقع الخاص بالمجلة العلمية الخاصة بقانون تكنولوجيا المعلومات والإتصالات " **Juriscom** " في الموقع التالي:
http://juriscom.net/2000/05/tgi-paris-refere-22-mai-2000-uejf-et-licra-c-yahoo-inc-et-yahoo-france/ تاريخ الإطلاع: 2017/09/25.

(4) - Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Disponible en ligne a l'adresse suivante:
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164
تاريخ الإطلاع: 12/12/ 2015

(5) - Article 6/1 de loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.: «. Les personnes dont l'activité est d'offrir un accès à des services de

الخدمة ليس عليهم التزام بالاشراف والرقابة على مضمون البيانات التي يقومون بنقلها كما أنهم غير ملتزمين بالبحث عن الوقائع التي تشير إلى الأنشطة غير المشروعة[1].

وقد تمّ تعديل المادة السادسة من هذا القانون بموجب المادة 57 من القانون رقم 2014 ــ 873 والصادر في: 2014/08/04 المتعلق بالمساواة الحقيقية بين المرأة والرجل[2]، وقد تضمن التعديل إضافة فقرة تتعلق بالتزام مزود الخدمة بتقديم الوسائل الفنية في حال الانتهاكات الواردة على حقوق الملكية الفكرية[3].

3 ــ التشريع الألماني: يعدّ القانون الألماني أوّل تشريع أوربي يحدّد مسؤولية الوسطاء في الانترنت وذلك بمقتضى قانون خدمات المعلومات والاتصال الصادر في 1 أوت 1997، ويطلق عليه " TDG" ويعد هذا القانون نقطة البداية التي انطلق منها التوجيه الأوربي للتجارة الالكترونية الصادر في 2000، في تنظيمه لمسؤولية الوسطاء الفنيين عبر الشبكة[4].

وقد جاء في المادة الأولى في فقرتها الخامسة (5/01) ما يلي: "لا يعد مزود الخدمة مسؤولا عن المحتوى غير المشروع إلا إذا كان عالما بعدم مشروعية هذا المحتوى، وكان يستطيع من الناحية الفنية تجنب الوصول إليه أو كان من العدل أن يطلب منه ذلك[5].

---

communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens".

(1) – Article 6/7 de loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. : « Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites".

(2) - LOI n° 2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les homes, JORF n°0179 du 5 août 2014.Disponible en ligne a l'adresse suivante: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029330832&categorieLien=id

(3) - Article 6 / Modifié par LOI n°2014-873 du 4 août 2014 - art. 57 dispose «Les personnes visées à l'alinéa précédent les informent également de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle et leur proposent au moins un des moyens figurant sur la liste prévue au deuxième alinéa de l'article L. 331-26 du même code ».

(4) - Strowel (A) et Ide(N), responsabilité des intermédiaires actualités, législatives et jurisprudentielle, droit et nouvelles technologies, p. 16.10/10/2000 en: : -http:/www.droitTechnologies.org.

(5)-Itéanau, les contras des commerces électronique, droit et patrimoine, dec 1977,p. 310.

أمّا الفقرة الثالثة من المادة الخامسة (3/05) من هذا القانون فنصت على إعفاء مزود الخدمة الذي يقتصر دوره على مجرد توفير وسيلة الاتصال بالموقع من المسؤولية عن عدم مشروعية البيانات والمحتوى غير المشروع للموقع.

4 ــ قانون المعاملات الالكترونية العماني رقم 96/ 2008: تضمن في المادة 14 منه على مايلي: "لا يسأل وسيط الشبكة مدنيا أو جنائيا عن أية معلومات واردة في شكل سجلات الكترونية ــ تخص الغير ــ إذا لم يكن وسيط الشبكة هو مصدر هذه المعلومات واقتصر دوره على مجرد توفير إمكانية الدخول إليها. و لم يضع هذا القانون أي إلتزام قانوني على عاتق وسيط الشبكة يفرض عليه القيام بالمراقبة على المعلومات الواردة على شكل سجلات الكترونية تخص الغير[1].

ثانيا ــ متعهد الإيواء:

يطلق على متعهد الإيواء تسميات كثيرة منها: المورد المستضيف ومورد الإيواء، وهو كل شخص طبيعي أو معنوي يعرض إيواء صفحات الـ WEB على حاسباته الخادمة العملاقة، وذلك مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة للتاجر ــ الناشر ــ والذي ينشر عليه ما يريد من نصوص، ووثائق، أو صور أو فيديو، أو ينشئ روابط معلوماتية من المواقع الأخرى[2].

وعليه فعمل متعهد الإيواء يتشابه إلى حد كبير بعمل مدير التحرير في الصحف المكتوبة الذي يخصص مساحة إعلانية لإعلانات شركة معينة وأن متعهد الإيواء ليس هو مالك الموقع التي تبث عليه الإعلانات، بل هو الذي يقوم بتثبيته أو إيواء الموقع على الشبكة[3].

فالشخص المسؤول عن الإيواء يقوم بخدمة تخزين المعلومة وإدارة محتواها بشكل يسمح لمورد المعلومة بعرضها على الجمهور، بمعنى أن هذا الشخص يجعل المعلومات التي يزوده بها المنتج أو المورد

---

[1] ــ مرسوم سلطاني رقم 2008/96 المتعلق بإصدار قانون المعاملات الالكترونية الصادر في 27 جمادى الأولى 1429، الموافق لـ 17 مايو سنة 2008، السابق الذكر.

[2] محمد حسين منصور، مرجع سابق، ص 187.

[3] ــ شريف محمد غنام، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، 2008، ص 171.

في متناول الجمهور من خلال إعداد مكان للجمهور يمكنه من الاتصال بشبكة الانترنت والاطلاع على المواقع المتاحة، والحصول على المعلومات المطروحة[1].

ومن أوائل التشريعات التي كانت سباقة في معالجة مسؤولية متعهد الايواء هي:

1 ــ التشريع الألماني: وكان ذلك من خلال قانون " الخدمات الآلية Teléservices " الذي أصبح نافذا في 1997/08/01، وألحق بقانون خدمات الإعلام والإتصال.

وقد تضمّن هذا القانون إعفاء متعهد الايواء ــ والذي أطلق عليه تسمية " مضيف المواقع"ــ من المسؤولية ما لم يثبت علمه بالمحتوى الضار، أو إذا عجز عن توفير الوسائل التقنية اللازمة لمنع الوصول إلى هذا المحتوى[2].

2 ــ التشريع الأمريكي: من خلال القانون الصادر في 28/ 10/ 1998 قانون الألفية الأمريكي حول حق المؤلف "DMCA"، وقد جاء هذا القانون معدلا لقانون حق المؤلف الصادر في عام 1976، وطبقا لهذا القانون فإن المضيف للمعلومات والمواقع يعفى من المسؤولية المباشرة "Liability Direct" ومن المسؤولية غير المباشرة " Liability Vicariuos" إذا توافرت مجموعة من الشروط، كأن يكون مقدم الخدمة يجهل عدم مشروعية المحتوى، وعدم إستفادته ماديا من المحتوى غير الشرعي، وقام بسحب المضمون غير القانوني فور إخطاره بذلك من المضرور[3].

3 ــ التوجيه الأوربي: وفقا لنص المادة 14 من التوجيه الأوربي رقم 2000 ــ 31 الصادر في 8 يونيه 2000 بشأن التجارة الالكترونية، فقد أوجبت على الدول الأعضاء عدم إقامة مسؤولية متعهد الايواء إلا بشروط معينة هي:

أ ــ تبوث علمه الفعلي بالمضمون غير المشروع للمعلومات التي ينقلها عبر أجهزته التقنية، أو أن يكون النشاط غير المشروع ظاهرا.

---

(1) - حسين منصور محمد، مرجع سابق، ص 28.

(2) ــ طوني ميشال عبسى، التنظيم القانوني لشبكة الانترنت، صادر ناشرون، بيروت، لبنان، ط 1، 2001، ص 405.

(3) ــ لمزيد من التفاصيل حول أحكام القانون الأمريكي انظر:

Sedaillan,Valérie, la responsabilité des prestataires techniques sur internet, dans le digitale millénium copyrient act Américan et le projet de directive européenne sur le commerce éléctronique, Cahiers Lamy, janvier 1999,n’ 110,p.1 et s.

ب ــ أن يكون لديه الوسائل والتقنيات الفنية التي تمكنه من التحكم في المعلومات التي يبثها عبر تقنياته.

ج ــ وقف بث المعلومات غير المشروعة فور علمه بالمحتوى غيرالمشروع.

ووفقا لأحكام المادة 15 من ذات التوجيه، فإنه ينبغي لقوانين الدول الأعضاء في الاتحاد الاوربي أن تفرض على متعهد الايواء إلتزاما عاما بمراقبة المعلومات التي يقوم بنقلها، أو تخزينها، أو البحث النشط عن الوقائع والظروف التي تظهر الأنشطة غير المشروعة.

4 ــ التشريع الفرنسي: تم تناول مسؤولية متعهد الايواء من خلال القانون رقم 2000 ــ 719 المتعلق بتعديل بعض أحكام القانون الخاص بحرية الاتصالات رقم 86 ــ 1067، والصادر في 30/ 09/1986، والقانون **رقم 2004 ــ 575 المتعلق بالثقة في الاقتصاد الرقمي الصادر في 21/ 06/ 2004.**

أ ــ القانون رقم 2000 ــ 719 الصادر في 01 / 08 / 2000 [1]:

أصدر المشرع الفرنسي بتاريخ 01 / 08 / 2000 القانون رقم 2000 ــ 719 بشأن تعديل بعض أحكام القانون المتعلق بحرية الاتصالات. ووفقا لنص المادة 43 ــ 8 منه: "فإن الأشخاص الطبيعين أو المعنويين الذين يتعهدون بشكل مجاني أو بمقابل التخزين المباشر والمستمر للمعلومات من أجل أن يضعوا تحت تصرف الجمهور إشارات أو كتابات أو صورا أو أغاني أو رسائل وكل ما من طبيعته إمكان استقباله فإنهم يكونون غير مسؤولين جنائيا أو مدنيا عن مضمون هذه المعلومات أو الخدمة إلا إذا أصبحوا مختصين برقابتها بأمر من السلطة القضائية وامتنعوا على أن يوقفوا بث أو نشر هذه المعلومات عبر مواقع الانترنت[2].

---

(1) - LOI no 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication. Disponible sur l'adresse ssuivante: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000402408 تاريخ الإطلاع: 15/12/2016

(2) - « Art. 43-8.de lOI no 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication.Et ainsi rédigé - Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :

كما أوجبت الفقرة التاسعة من المادة 43 السابقة الذكر على متعهد الايواء أن يزود عملائه بالوسائل الفنية التي تسمح بتحديد هوية كل من يسهم في وضع مضمون المعلومات على الانترنت، حتى يمكن تحديد الشخص المسؤول عن المعلومات غير المشروعة[1].

يتميز القانون الفرنسي إذن عن القانونين الألماني والأمريكي، وكذا التوجيه الأوربي، أنه لم يكتف تأكيد مبدأ عدم مسؤولية متعهد الايواء فحسب، بل ذهب إلى أبعد من ذلك حيث حصر مسؤوليته المحتملة في حالة وحيدة هي عدم مبادرة هذا المتعهد إلى إزالة المشكو منه بناء على طلب السلطة القضائية وحدها، فلا يسأل بالتالي إذا ورد مثل هذا الطلب إليه من غير السلطة القضائية، مثلا من قبل المتضرر أو من قبل الغير.

كما أنّ الفقرة الحادية عشر من المادة المذكورة لا تجيز أن يفرض على متعهد الايواء إلتزام عام بمراقبة المعلومات التي يقوم بنقلها أو تخزينها ولا إلتزام عام بالبحث عن الوقائع أو الظروف التي تكشف الأنشطة غير المشروعة.

ب ــ القانون رقم 2004 ــ 575 المتعلق بالثقة في الاقتصاد الرقمي الصادر في: 21/ 06/ 2004[2].

نصّت الفقرة الثانية من المادة السادسة من هذا القانون على أن الشخص الطبيعي أو المعنوي الذي يقدم خدمة تخزين الرسوم والنصوص والأصوات والبريد الالكتروني غير مسؤول عن الأنشطة أو المعلومات غير المشروعة التي يتم تخزينها بناء على طلب ذوي الشأن إذا لم يكن قد علم فعليا بعدم مشروعيتها.

وقد أدخلت تعديلات جديدة على هذا القانون وبصفة خاصة على المادة السادسة منه وذلك بموجب المادة 57 من القانون رقم 2014 ــ873 والصادر في: 2014/08/04 المتعلق بالمساواه

« - si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu ;"

(1)- « Art. 43-9. Cet article dispose que: Les prestataires mentionnés aux articles 43-7 et 43-8 sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires.

(2) - Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

الحقيقية بين المرأة والرجل[1]، وقد نصت على أن الأشخاص الطبيعين أو المعنويين الذين يتعهدون بشكل مجاني أو بمقابل من خلال خدمات الاتصالات إلى الجمهور عبر الانترنت تخزين إشارات، كتابات، صور غير مسؤولين مدنيا ولا جنائيا عن الأنشطة أو المعلومات المخزنة بطلب من المستفيد من هذه الخدمات إذا لم يكن قد علم بها فعليا بعدم مشروعيتها، أو أنه منذ لحظة علمه تصرف بشكل مناسب لسحبها أو لجعل الوصول إليها غير متاح[2].

والملاحظ أنّ هذه المادة السادسة بعد التعديل تتشابه إلى حد كبير مع المادة 14 من التوجيه الأوربي رقم 2000ـــ31 والصادر في 8 يونيو 2000 بشأن التجارة الالكترونية، ذلك أنّ مسؤولية متعهد الايواء مرهونة بعلمه الحقيقي بالمضمون غير المشروع للبيانات والمعلومات التي يقوم بتخزينها أو نقلها، وأنه تصرف بسرعة لمنع وصول هذه المعلومات غير المشروعة بواسطة التقنيات الفنية المتوفرة لديه.

ومن التطبيقات الحديثة لهذه المادة، الحكم الصادر عن محكمة باريس الابتدائية في 17 جانفي سنة 2003، حيث أمر القاضي متعهد الايواء بسحب لعبة على هيئة صورة لرجل السياسة المعروف "Marie le Pen" وأكدت المحكمة بوضوح في هذا الحكم أن متعهد الايواء ليس مسؤولا عن

---

(1)- LOI n° 2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les homes.

(2) Article 06 modifié par artile 57 de loi **n° 2014-873** les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.
L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.
3 - Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.

محتوى الموقع أو مضمونه إذا تصرف بشكل مناسب لسحب المحتوى غير المشروع منذ علمه بوجوده[1].

ثالثا ــ مورد المعلومات: المورّد " Le fournisseur d'information ": هو شخص طبيعي أو معنوي يقوم ببثّ المعلومات المتعلقة بموضوع معين على الانترنت، حيث يتمكن مستخدم هذه الشبكة من الحصول عليها مجانا أو بمقابل مادي[2]، ويعتبر بمثابة القلب النابض لبث الحياة في هذه الشبكة وتدفق المعلومات إليها، ويعد هو المسؤول الأول عن هذه المعلومات، وبالتالي فإن له دورا رئيسيا في إطار المسؤولية عنها، لأنه هو الذي يملك سلطة رقابة مشروعية هذه المعلومات، والتحكم في بثها عبر الانترنت، ذلك لأنه هو الذي يقوم بتحميل النظام المعلوماتي التي قام بتأليفها أو جمعها حول موضوع معين وهو الذي يتولى الاختيار والجمع والتوريد للمادة المعلوماتية حتى تصل إلى الجمهور عبرالشبكة[3].

وقد عرفه البعض: أنه الشخص الذي يزود الوسطاء الآخرين بالمعلومات والبيانات التي تبث على الموقع فهو الذي يحدد مضمون ما يبث على الموقع، والبيانات التي يحددها هذا المورد قد تكون في شكل نصوص مكتوبة أو صور أو قطع موسيقية أو علامات تجارية يعلن عنها[4].

وقد تطرقت مختلف التشريعات المقارنة لتحديد مسؤولية مورد المعلومات كالتالي:

1 ــ التوجيه الأوربي: طبقا لأحكام التوجيه الأوربي رقم 2000ــ31 بشأن التجارة الالكترونية، فإن مورد المعلومات يعتبر هو المسؤول الأول عن مضمون المعلومات التي يتم بثها عبر تقنيات الاتصال الحديثة. ووفقا لنص المادة 14 من هذا التوجيه تنتفي مسؤولية مورد المعلومات إذا أثبت أنه لا يعرف مضمون هذه المعلومات غير المشروعة، ولا الوقائع أو الظروف التي نشرت فيها

---

(1) ــ لمزيد من التفاصيل حول هذا الحكم انظر الموقع التالي:
http:/www.légalis.net,jurisprudence et actualité de droit de l'internet. تاريخ الإطلاع: 12/25/ 2016

(2) -Feral- Schuhl Christiane, Cyber droit, le droit à l'épreuve de l'internet, 3ém Edition, Dunod, Paris, 2002, p. 129.

(3) ــ محمد حسين منصور، مرجع سابق، ص199.

(4) - Strowel (A) et Ide(N) , op. cit, p 1.

هذه المعلومات، وأن يوقف بث أو نشر هذه المعلومات فور علمه بعدم مشروعيتها، أو منع الاتصال بها أو الحصول عليها.

2 ــ القانون الفرنسي: إذا كان المورد شخصا معنويا فإن مديره هو المسؤول بصفته مديرا للنشر طبقا للمادة 42 من قانون حرية الصحافة الفرنسي الصادر بتاريخ 29 جويلية 1881 والتعديلات اللاحقة عليه آخرها في 4 سبتمبر 2011.

3 ــ القانون الألماني: يعتبر القانون الالماني المتعلق بخدمات الاتصالات والمعلومات الصادر في 10 أوت 1997 القانون الوحيد الذي تعرض مباشرة لمسؤولية مورد المحتوى عند معالجة مسؤولية مزود الخدمة [1].

وقد قرر في الفقرة (2) من المادة الخامسة منه مسؤولية مضيفي المواقع (متعهد الإيواء) عن مضمون البيانات المخزنة إذا توافرت شرطان هما:

ــ العلم بمحتوى المواقع التي يتولى إيوائها.

ــ إستطاعة متعهد منع نشر أو بث المضمون غير المشروع من الناحية الفنية.

الفرع الثاني: المسؤولية الجنائية لمقدمي خدمات الانترنت في التشريع الجزائري.

عرّف المشرع الجزائري لأوّل مرّة مقدمي خدمات الانترنت في المادة الثانية فقرة د (02/د) من القانون رقم(09ــ04) المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، بالرغم من صدور المرسوم التنفيدي رقم (98ــ257) المؤرخ في 25 أوت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها، حيث تطرق المشرع من خلاله مباشرة إلى تحديد شروط وكيفيات إقامة خدمات "الانترنت" واستغلالها دون تحديد مفهوم مقدم الخدمة، وقد عرفه القانون رقم (09 ــ 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها السالف الذكر بأنه:

---

[1] - انظر نصوص القانون الالماني المتعلق بخدمات الاتصالات والمعلومات باللغة الانجليزية على الموقع التالي:
- http:/www.iid,de/rahmen/rahmen/jukdgebt.htlm تاريخ الإطلاع: 30/12/ 2016

" 1 ــ أيّ كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام الاتصالات،

2 ــ وأيّ كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها."

يتّضح من خلال هذا التعريف أنّ المشرع الجزائري حصر الوسطاء في خدمة الانترنت في شخصين هما متعهد الوصول ومتعهد الايواء، بالرغم من تعدّد الاشخاص الذين يساعدون المستخدم في الدخول إلى شبكة الانترنت والتجول فيها والاطلاع على ما يريد، مثل منتج الخدمة، مورد المعلومات، متعهد الخدمات و مؤلف الرسالة.

وعليه دراسة المسؤولية الجنائية لمقدمي الخدمات، ستتم من خلال بيان شروط استغلال خدمات الانترنت والتزامات مقدمي خدمات الانترنت في التشريع الجزائري.

أولا ــ الشروط القانونية لإقامة خدمات الانترنت:

يمثل المرسوم التنفيذي رقم (98ــ257) المؤرخ في 25 أوت 1998، الذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها، والتعديلات اللاحقة عليه بموجب المرسوم التنفيذي رقم (2000 ــ307) المؤرخ في 14 أكتوبر 2000[1]، التنظيم الأساسي الذي يضبط الشروط القانونية للدخول لنشاط استغلال خدمات الانترنت، والتي تتمثل في شروط موضوعية وأخرى شكلية.

أ ــ الشروط الموضوعية: يقصد بها تحديد الاشخاص الذين لهم حق إقامة واستغلال خدمات الانترنت، وبالرجوع للمرسوم السابق الذكر المنظم لهذا النشاط نجد المادة الرابعة منه قبل التعديل كانت تنص على " لا يرخص بالدخول لنشاط الانترنت إلا للأشخاص المعنويين الخاضعيين للقانون الجزائري، المدعوون أدناه مقدم الخدمات، وبرأس مال يملكه فقط أشخاص معنويون خاضعون للقانون العام، و/ أو أشخاص طبيعيون من جنسية جزائرية".

---

[1] - المرسوم التنفيذي 2000ــ307 المؤرخ في 14 أكتوبر سنة 2000، يعدل المرسوم التنفيذي 98 257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات الانترنت، ج.ر.ج، ع 60، لسنة 2000.

يتبين من خلال هذه المادة بأن كل شخص معنوي خاضع للقانون الجزائري يمكنه الدخول لممارسة هذا النشاط، سواء كان هذا الشخص عام أو خاص، وحتى الاجانب الذين يقبلون الخضوع للقانون الجزائري، غير ان المشرع يشترط أن يكون رأس مال هذا الشخص المعنوي مملوك لأشخاص معنويون خاضعون للقانون العام و/ أو أشخاص من جنسية جزائرية.

بذلك يقصي المشرع الأجانب من الاستثمار في نشاط الانترنت، غير أن المشرع الجزائري تراجع بعد ذلك عن هذا التمييز وهذه التفرقة، وذلك بعد تعديل المادة الرابعة من المرسوم التنفيدي رقم (98ـــ257)، بمقتضى المادة الرابعة من المرسوم التنفيدي رقم (2000ـــ307) التي صارت تنص على أنه: "لا يرخص بإقامة خدمات الانترنت واستغلالها لأغراض تجارية ضمن الشروط إلا للأشخاص المعنويين الخاضعين للقانون الجزائري ، الذين يدعون مقدمي خدمات الانترنت".

وبالتالي فتح المشرع الجزائري باب الاستثمار أمام الأشخاص المعنويين الخاضعيين للقانون الجزائري، و"الخضوع للقانون الجزائري" لا يعني التمتع بالجنسية الجزائرية.

ب ـــ الشروط الشكلية: نصت المادة الخامسة من المرسوم التنفيذي رقم (2000ـــ307) المحدد لشروط الدخول لنشاط استغلال خدمات الانترنت، على ضرورة الحصول على ترخيص من الوزير المكلف بالاتصالات.

ويقصد بالترخيص (**Autorisation**) عمل تسمح بموجبه السلطة الادارية للمستفيد بممارسة نشاط أو التمتع بحق ممارسته، ويمكن هذا الاجراء الادارة من ممارسة رقابتها على الأنشطة الاقتصادية التي تشكل خطر على الأشخاص أو الاقتصاد الوطني[1].

أمّا من حيث الطبيعة القانونية للترخيص فهو عبارة عن تصرف قانوني في صورة قرار اداري اتفرادي[2]، وهذا القرار منشئ للحق وليس كاشف له[3].

---

[1] ـــ أعراب احمد، السلطات الادارية المستقلة في المجال المصرفي، رسالة ماجستير، كلية الحقوق، جامعة بومرداس، 2007/2006، ص64.

[2] ـــ نفس مرجع ، ص 66.

[3] - André CHAMINADE ? poste et communications électroniques 'Régime' Juridique des autorisations d'utilisation des préquences radioélectriques, JCP, la semaine juridique N°43,24 Octobre 2007, II10177, P36.

وللحصول على ترخيص إقامة خدمات الانترنت واستغلالها يجب على الطالب أن يقدم عرض مفصل عن الخدمات التي يقترح تقديمها وكذلك شروط وكيفيات النفاذ إلى هذه الخدمات، كذلك يشترط دراسة تقنية حول الشبكة المقترحة وحول التجهيزات والبرامج المعلوماتية التابعة لها مع تحديد هيكلها وكذلك صيغ الوصول بالشبكة العمومية للاتصالات، كذلك يجب على المستثمر أن يقدم التزام من المصالح المختصة في الوزارة المكلفة بالاتصالات يثبت إمكانية إقامة الوصلة المخصصة، الضرورية لنقل خدمات الانترنت، وهذا ما نصت عليه المادة الخامسة من المرسوم التنفيدي رقم (98ـ257).

ولا يسلم الترخيص بالاستغلال إلا بعد تحقيق تأهيلي يأمر به وزير الاتصلات، وذلك طبقا للمادة الرابعة من المرسوم التنفيدي رقم (98 ـ 257)، وكذلك بناء على موافقة اللجنة المذكورة[1]، ويسلم الترخيص لمدة غير محددة المدة ولا يمكن التنازل عنه. (المادة 8 من نفس المرسوم).

ثانيا ـ التزامات مقدمي خدمات الانترنت:

فرض المشرع الجزائري على مقدمي الخدمات عدة التزامات قد تكون عامة مثل مساعدة السلطات العامة وحفظ المعطيات المتعلقة بحركة السير وهو ما نص عليه القانون رقم (09 ـ 04) السالف الذكر، ومنها التزامات خاصة، تتفق وطبيعة عمل الاشخاص الوسيطة في خدمة الانترنت وهي كالتالي:

1 ـ الالتزامات العامة:

أ ـ مساعدة السلطات العامة: يلتزم مقدم الخدمات حسب المادة 10 من القانون رقم (09ـ 04) بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات، ووضع المعطيات التي تم حفظها تحت تصرف تلك السلطات.

[1]ـ المادة 16 من المرسوم التنفيدي رقم (98 ـ 257) المعدل بالمادة 6 من المرسوم التنفيدي رقم (2000 ـ 307)، حيث تتشكل اللجنة من الأعضاء الآتي ذكرهم: ـ ممثل الوزير المكلف بالمواصلات السلكية والاسلكية، رئيسا. ـ ممثل وزير الدفاع الوطني. ـ ممثل وزير الداخلية.

كما يتعيّن على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذلك المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[1].

ب ــ حفظ المعطيات المتعلقة بحركة السير: طبقا للمادة 11 من القانون رقم (09 ــ 04)، يلتزم مقدمو الخدمات بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال، والخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال، بالاضافة إلى المعطيات التي تسمح بالتعرف على المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

تحدّد مدة حفظ المعطيات المتعلقة بحركة السير بسنة واحد ابتداء من تاريخ التسجيل.

2 ــ الالتزامات الخاصة: نص المشرع الجزائري على التزامات مقدمي خدمات الانترنت في المرسوم التنفيدي(98 ــ 257) الذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها، وفي القانون رقم (09 ــ04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، وذلك على النحو التالي:

أ ــ الإلتزامات المستمدة من المرسوم التنفيدي رقم (98 ــ 257) الذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها:

طبقا للمادة 14 من المرسوم التنفيدي(98 ــ 257)، يلتزم مقدم خدمات الانترنت خلال ممارسة نشاطاته بما يأتي:

ــ تسهيل النفاذ إلى خدمات الانترنت، حسب الامكانيات المتوفرة إلى كل الراغبين في ذلك باستعمال أنجع الوسائل التقنية.

ــ إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات الانترنت وصيغة مساعدتهم كلما طلبوا ذلك.

---

[1] ــ راجع الفقرة الثانية (02) من المادة 10 من القانون رقم (09 ــ04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها السابق الذكر.

ـــ عرض أي مشروع خاص باستعمال منظومات الترميز على اللجنة.

ـــ تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها ويأويها، طبقا للأحكام التشريعية المعمول بها.

ـــ إعلام مشتركيه بالمسؤولية المترتبة عليهم فيما يتعلق بمحتوى الصفحات التي يستخرجها ويأويها، طبقا للأحكام التشريعية المعمول بها.

ـــ احترام قواعد حسن السيرة بالامتناع خاصة عن استعمال أية طريقة غير مشروعة سواء تجاه المستعملين أو تجاه مقدمي خدمات الانترنت الآخرين.

ـــ المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الادلاء بها إلا في الحالات المنصوص عليها في القانون.

ـــ اتخاذ كل الاجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه، قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق.

ومن ثم نلاحظ وجود نوع من التنوع في طبيعة الالتزامات الخاصة المفروضة على مقدمي خدمات الانترنت، من التزمات تقنية إلى التزامات أخلاقية ومهنية تتفق وطبيعة عمل وسطاء شبكة الانترنت.

ب ـــ الإلتزامات المستمدة من القانون رقم (09 ـــ04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها:

نصّ المشرع الجزائري في المادة 12 من القانون رقم (09ـــ04) المؤرخ في 05 أوت 2009 على أنه زيادة على الالتزامات المنصوص عليها في المادة 11 (والتي تتضمن الالتزامات العامة لمقدمي خدمات الانترنت وهي مساعدة السلطات العامة، وحفظ المعطيات المتعلقة بحركة السير)، يلتزم مقدمو خدمات الانترنت بما يأتي:

- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب الهامة وإخبار المشتركين لديهم بوجودها.

ثالثا ــ تحديد المسؤولية الجنائية لمقدمي خدمات الانترنت:

تقوم المسؤولية الجنائية لمقدمي خدمات الانترنت في حالتين، هما جريمة إفشاء أسرار التحري والتحقيق المنصوص عليها في المادة 10 من قانون(09ــ04) السابق الذكر، وجريمة عدم حفظ المعطيات المتعلقة بحركة السير والمنصوص عليها في المادة 4/11 من نفس القانون (09ــ04) المنوه عنه، وذلك على النحو التالي:

1 ــ جريمة إفشاء أسرار التحري والتحقيق:

نظّم المشرّع الجزائري هذه الجريمة في المادة 2/10 من القانون رقم (09 ــ 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، والتي تنص على أنه:" يتعين على مقدمي خدمات الانترنت كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لافشاء أسرار التحري والتحقيق".

يلاحظ من خلال هذه المادة أن هذه الجريمة جزء من جريمة إفشاء الموظف العام لأسرار وظيفته المنصوص عليها في المادة 301 من قانون العقوبات الجزائري[1]، وعليه لقيام هذه الجريمة يتطلب توافر ركنين المادي والمعنوي.

أ ــ الركن المادي: يتمثّل الركن المادي لهذه الجريمة في إفشاء مزود الخدمات لأسرار التحري والتحقيق، أي إذاعتها ونقلها واطلاع الغير عليها بعد أن كان العلم بها قاصرا على أصحابها أو الذين أئتمنوا عليها بحكم وظيفتهم[2].

---

[1] ــ تنص المادة 301 من قانون العقوبات الجزائري " يعاقب بالحبس من شهر إلى 6 أشهر وبغرامة من 20 ألف إلى 200 ألف دج الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين عليهم بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى بها إليهم وأفشوها في غير الحالات التي يوجب عليهم القانون لإفشاءها ويصرح لهم بذلك".

[2] ــ صالح شنين، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان أبوبكر بلقايد، 2012 ــ 2013، ص 125.

وبتكون الركن المادي لهذه الجريمة من العناصر التالية هي:

✓ صفة الجاني أو من أوتمن عليه السر: يأخد مزود خدمات الانترنت في هذه الحالة صفة المؤتمن على أسرار البحث والتحقيق، لاسيما أن إجراءات التحقيق والتحري سرية وفقا للمادة 11 من قانون الاجراءات الجزائية الجزائري.

✓ فعل افشاء السر: يقصد بالإفشاء اطلاع الغير على السر بأي طريقة كانت سواء كانت بالكتابة أوالاشارة أوالشفاهة . أما السر فهوعبارة عن واقعة أو صفة ينحصر نطاق العلم بها في عدد محدود من الأشخاص بحكم وظيفتهم، وكان في إفشائه حرج لغيره ولو لم يشترط كتمانه صراحة، ولا يشترط أن يكون السر قد أدلى به إلى الأمين، أو ألقي إليه على أنه سر وطلب منه كتمانه[1].

يشمل محل هذه الجريمة إفشاء العمليات التي ينجزها مقدم الخدمات وكذا المعلومات المتصلة بها، والمتعلقة بالتحري والتحقيق.

ب ــ الركن المعنوي: جريمة إفشاء مزودي الخدمات أسرار التحري والتحقيق هي جريمة عمدية لا بد من توافر القصد الجنائي العام بعنصريه العلم والارادة، فيجب أن يعلم الجاني بأنه يرتكب جريمة إفشاء الأسرار المتعلقة بالتحري والتحقيق، وأن تتجه إرادته إلى ارتكاب هذه الجريمة[2].

يجب الإشارة إلى أن جريمة إفشاء أسرار التحري والتحقيق تخضع للقاعدة العامة التي تقضي بأن البواعث ليست من عناصر القصد، بحيث تقوم هذه الجريمة بمجرد توافر القصد الجنائي العام ــ حتى وان كانت هذه البواعث نبيلة ــ إلى جانب الركن المادي للجريمة.

ج ــ العقوبة: لم يحدد المشرع الجزائري عقوبة لجريمة إفشاء مزودي الخدمات لأسرار التحري والتحقيق في المادة 2/10 من القانون رقم (09 ــ 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، بل أحال إلى العقوبات المقررة

(1) ــ عز الدين الديناصوري، عبد الحميد الشواربي، المسؤولية المدنية في ضوء الفقه والقضاء، دار الفكر العربي، 2012، مصر، ص144.

(2) ــ أحمد بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، دار هومة، الجزائر، 2014، ص 280 ــ 281.

لجريمة الافشاء، والمبينة في المادة 301 من قانون العقوبات الجزائري والتي تعاقب كل من أفشى بسر المهنة بالحبس من شهر إلى ستة (6) أشهر، وبغرامة 500 دج إلى 5.000 دج على إفشاء السر المهني.

هذا فيما يتعلق بالعقوبات المقررة للشخص الطبيعي، أما بالنسبة للشخص المعنوي[1]، فتطبق عليه عقوبة الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر، وفي المادة 18 مكرر 2 عند الاقتضاء.

كما قد يتعرض لواحدة أو أكثر من العقوبات التكميليّة وهي محددة في المادة 18 مكرر/2 من قانون العقوبات الجزائري كالتالي:

ـــ حل الشخص المعنوي، ـــ غلق المؤوسسة أو فرع من فروعها لمدة لاتتجاوز خمس (5) سنوات، ـــ الاقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات، ـــ المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات، ـــ مصادرة الشئ الذي استعمل في ارتكاب الجريمة أو نتج عنها، ـــ نشر وتعليق حكم الادانة، ـــ الوضع تحت الحراسة القضائية لمدة لا تتجاوزخمس(5) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

2 ـــ جريمة عدم حفظ المعطيات المتعلقة بحركة السير:

نصّ عليها المشرّع في المادة 4/11 و5 من القانون رقم (09ـــ04) المتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، والتي جاء فيها: "دون الاخلال بالعقوبات الادارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات

[1]ـــ تنص المادة 303 مكرر3 من قانون العقوبات الجزائري: " يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم المحددة في الأقسام 3 و4 و5 من هذا الفصل، وذلك طبقا للشروط المنصوص عليها في المادة 51 مكرر.
وتطبق على الشخص المعنوي عقوبة الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر، وفي المادة 18 مكرر 2 عند الاقتضاء.
ويتعرض أيضا لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر."

القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج، يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات." وحتى تقوم هذه الجريمة يجب توافر الركن المادي والمعنوي على النحو التالي:

أ ــ الركن المادي:

يتمثل الركن المادي لهذه الجريمة في عدم احترام الالتزامات المنصوص عليها في المادة 11 من القانون رقم (09ــ04)، وهي عدم حفظ مزودي الخدمات للمعطيات المنصوص عليها في المادة 11 أو عدم حفظها للمدة المحددة قانونا، وهي السنة ابتداء من تاريخ التسجيل وفقا للمادة 11.

- وعليه يتمثل النشاط الاجرامي لهذه الجريمة في عدم حفظ مزودي الخدمات المعطيات المتعلقة بحركة السير أصلا، و عدم حفظها في المدة القانونية ، أمّا محل الجريمة فيتمثل في المعطيات المتعلقة بحركة السير المنصوص عليه في المادة 11 من هذا القانون[1].

ولا تقوم هذه الجريمة بمجرد توافر النشاط الاجرامي، بل يتطلب المشرع الجزائري لقيامها نتيجة معينة، وهي أن يؤدي عدم حفظ تلك المعطيات إلى عرقلة حسن سير التحريات القضائية.

ب ــ الركن المعنوي:

حتى تقوم هذه الجريمة لابد من توافر القصد الجنائي العام بعنصريه العلم والارادة، فيجب أن يعلم بأن نشاطه مجرم، وأنه يتسبب في عرقلة حسن سير التحريات القضائية بسبب عد حفظه المعطيات المتعلقة بحركة السير .

كما يجب أن تتجه إرادته إلى ارتكاب هذه الجريمة، وتحقيق النتيجة الاجرامية المتمثلة في عرقلة حسن سير التحريات القضائية.

---

[1]ــ وفقا للمادة 11/ 1 من القانون رقم (09ــ04) تتمثل المعطيات محل الحفظ: المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال، والخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال، بالاضافة إلى المعطيات التي تسمح بالتعرف على المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

لم يتطلب المشرع في هذه الجريمة القصد الجنائي الخاص، فلا عبرة بالباعث والغرض من الجريمة، بل تقوم بمجرد توافر القصد الجنائي العام إلى جانب الركن المادي[1].

ج ــ العقوبة: طبقا للمادة 4/11 و5 من القانون رقم (09 ــ 04)، يعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج، أما الشخص المعنوي فيعاقب بالغرامة المقررة في المادة 18 مكرر من قانون العقوبات وهي من مرة إلى خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

نستنتج أن جرائم الخدمة الوسيطة في الاتصال بشبكة الانترنت هي من الجرائم التي تهدد نظام الحكومة الالكترونية، والتي يجب مواجهتها على نحو حاسم بنصوص تشريعية قاطعة لا لبس فيها، وهذا ما قام به المشرع الجزائري وأغلب التشريعات المقارنة.

المبحث الثاني: جرائم الاعتداء على بيانات المعاملات الحكومية الالكترونية

أصبحت الانترنت أداة أساسية للتعاملات الالكترونية لاسيما التعاملات الالكترونية الحكومية، والتي تتمثل أساسا في تقديم الخدمات من خلال الاتصال الالكتروني بين مقدم الخدمة (الحكومة) والمستفيد منها، لذلك فإن سرية وأمن المعلومات التي يجرى تبادلها عند إجراء هذه التعاملات خصوصا عندما يتعلق الأمر بالبيانات الشخصية أو بقضايا مالية (أرقام بطاقات الائتمان) من القضايا المهمة والضرورية جدا لنجاح الحكومة الالكترونية.

عرّف المشرع الجزائري البيانات (المعطيات) بموجب الفقرة (ج) من المادة (2) من الفصل الأول من القانون رقم (09 ــ 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها 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".

[1] ــ صالح شنين، مرجع سابق، ص 129.

بهذا التحديد، فإن صور الإعتداء المعلوماتي على بيانات التعاملات الالكترونية الحكومية يصعب حصرها، لأنها متطورة ومرتبطة بالتطور المتسارع لتكنولوجيا المعلومات باستمرار. لذا يمكن الإشارة إلى أبرز الانتهاكات الواقعة على البيانات الحكومية على ضوء النصوص القانونية في التشريعين الفرنسي والجزائري وأحيانا تشريعات أخرى. وعليه يمكن تقسيم أبرز هذه الجرائم إلى جرائم ضد سلامة البيانات الحكومية (المطلب الأول)، وأخرى جرائم ضد سريتها (الفرع الثاني).

المطلب الأول: جرائم الاعتداء ضد سلامة البيانات

تتعدد أشكال الجرائم الماسة بسلامة البيانات بتعدد أنماط السلوك الذي يؤدي إلى الاعتداء على المعلومات أو المعطيات حيث تأخذ شكل التلاعب في البيانات، وجريمة التزوير المعلوماتي.

الفرع الأول: جريمة التلاعب في البيانات

نصت المادة الرابعة من الإتفاقية الدولية حول الإجرام المعلوماتي "بودابست" المنعقدة بتاريخ 23 نوفمبر 2001 السابقة الذكر، على الإعتداءات الواقعة ضد تكاملية المعطيات (سلامتها) كالتالي: "على كل طرف تبنى التدابير التشريعية وغيرها التي تعتبر ضرورية لتجريم الأفعال التالية طبقا لقانونه الداخلي إذا ارتكبت عمدا ودون وجه حق إتلاف أو محو أو إفساد أو تعديل أو حذف المعطيات".

يقصد بالتلاعب بالبيانات إدخال بيانات غير مصرح بها أو تعديل بيانات موجودة أو إلغاء بيانات موجودة بالنظام، وهي تتعلق بمعطيات النظام، حيث تؤدي إلى تغيير من حالة هذه المعطيات وبالتالي المساس بسلامتها وتكاملها، على خلاف جريمة الاخلال بسير النظام والتي تتعلق أساسا بالنظام ذاته.

نظم المشرع الفرنسي هذه الجريمة بموجب المادة 323 ــ3 من قانون العقوبات، والتي تنص على أنه: "يعاقب كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات، أو محى، أو عدل بطريق الغش، بعقوبة الحبس ثلاث (3) سنوات وبغرامة 150000 يورو" [1].

[1] - Article 323 – 3/1 de code penal dispose que : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amande .

الوضع في قانون العقوبات الجزائري مشابه للوضع في قانون العقوبات الفرنسي حيث نصّت المادة 394 مكرر1 من قانون العقوبات الجزائري على ما يلي: "يعاقب بالحبس من من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها" .

حتى تقوم هذه الجريمة يجب أن يتوافر ركناها المادي والمعنوي، على التفصيل الآتي:

أولا ــ الركن المادي لجريمة التلاعب في البيانات

يقوم الركن المادي لجريمة التلاعب في المعطيات على النشاط الاجرامي الذي يتكون حسب نص المادة 394 مكرر1 من ق.ع.ج السابق الذكر من ثلاثة أفعال هي الادخال أو الإزالة (المحو) أو التعديل.

1 ــ فعل الإدخال: يقصد به" إضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم يوجد عليها معطيات من قبل، سواء كانت الدعامة محل الإعتداء فارغة ــ غير مشغولة ــ أوكانت تحتوي على خصائص ممغنطة قبل هذا الإدخال"[1].

هذه الجريمة تقع غالبا بمعرفة المسؤول عن القسم المعلوماتي والذي يسند إليه وضائف المحاسبة والمعاملات المالية لأنه يكون في وضع أفضل يؤهله لارتكاب هذا النمط من التلاعب غير المشروع[2].

يتحقق هذا الفعل في حالة الاستخدام التعسفي لبطاقات السحب والائتمان من حاملها الشرعي (كتسديد النقود أكثر من المبلغ المسموح به لصاحب البطاقة)، أم من غيره في حالات السرقة والفقد أو التزوير، كما يتحقق فعل الادخال أيضا بإدخال برامج خبيثة إلى نظام المعالجة الآلية بهدف إتلاف المعلومات وتشويهها وتدميرها باستخدام الفيروسات والقنبلة المعلوماتية بصفة خاصة، وهو ما قضت به محكمة "ليموج" عام 1994، حيث أدانت شخصا بتهمة إتلاف المكونات المنطقية للحاسب الآلي لقيامه بإدخال برنامج خبيث هو "حصان طروادة" إلى نظام الحاسب الآلي مما ترتب عليه إتلاف

(1) ـ نائلة عادل محمد فريد قورة، مرجع سابق، ص 473.

(2) ــ محمد سامي الشوا، ثورة المعلومات وإنعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998، ص 71.

للمعطيات فضلا عن إعاقة النظام عن أداء وظيفته[1]، وفي حكم لمحكمة النقض الفرنسية سنة 1996 ذهب فيه إلى أن إدخال البرامج الخبيثة إلى نظام الحاسب الآلي هو سلوك معاقب عليه وفق الفقرة الثانية من المادة 323[2].

2 ــ فعل التعديل: يقصد بهذا الفعل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، وغالبا ما يتم إجراء التعديل عن طريق برامج خبيثة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها[3].

3 ــ فعل المحو أو الإزالة: يقصد بفعل المحو إزالة كل أو جزء من المعطيات الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة[4]. وعملية الإزالة هي مرحلة لاحقة على عملية إدخال المعطيات، فالازالة تفترض الوجود السابق لعملية الادخال[5].

ويعتبر المحو جريمة إتلاف طالما وقع ثمة إتلاف الشئ بأي وسيلة، وذلك ما أكّده المؤتمر الخامس عشرة (15) للجمعية الدولية لقانون العقوبات المنعقد بالبرازيل في تشرين الأول سنة 1994 بشأن جرائم الكمبيوتر في مقرراته وتوصياته أنّ الادخال أو التعديل أو المحو يشكل جريمة تزوير، كما اعتبر المحو للبرامج أو لمعلومات جريمة إتلاف[6].

ثانيا ــ الركن المعنوي لجريمة التلاعب في البيانات

جريمة التلاعب بالبيانات المعلوماتية الحكومية جريمة عمدية تتطلب لقيامها القصد الجنائي العام المتمثل في العلم والإرادة، ويجب أن ينصرف كلاهما إلى كافة العناصر التي يتألف منها الركن المادي

---

(1) -Cass. Crim. 5 Janvier 1994, J. C.P. Edition General. 1994, IV,n° 856 corr. De Limoges, 14 mars 1994, p. 238 – 248.

(2) -Cass. Crim. 12 Décembre 1996, Bull Crim n° 465.

(3) -علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا..، مرجع سابق، ص 59 .

(4) ــ عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني..، مرجع سابق، ص 365.

(5)- R. Gassin .op. cit. n°. 201, p. 32.

(6) ــ نص المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر في شقه الموضوعي الموسوم بالجرائم في فقرته الثالثة تحت عنوان "تزوير الكمبيوتر أو التزوير المعلوماتي"بأنه يشمل إدخال أو إتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد ــ فيما لو ارتكبت بغير هذه الطرق ــ من قبيل أفعال التزوير المنصوص عليها في القانون الوطني. أما الفقرة الرابعة منه تنص على أن الإضرار بالبيانات والبرامج (الإتلاف) : ــ وتشمل المحو والإتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه. انظر: وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الإتصالات، دار المطبوعات الجامعية، 2007، الإسكندرية، ص 221.

للجريمة، فلابد أن يعلم الجاني أنه يقوم بإدخال أو تعديل أو إزالة معطيات معلوماتية، وأن هذه الأفعال تؤدي إلى نتيجة هي تغيير حالة المعطيات، سواء تؤدي إلى نتائج سلبية أو إيجابية قد تساعد على تحسين النظام[1].

لايشترط أن يكون القصد محددا بمعطيات معينة أو غير محدد، فالمعطيات كلها مشمولة بالحماية سواء في القانون الجزائري والفرنسي، بخلاف بعض القوانين تبسطها على أنواع معينة دون غيرها كالتشريع الأمريكي[2].

ولا يشترط لقيام الركن المعنوي في جريمة التلاعب بالمعطيات توافر القصد الجنائي الخاص وذلك ما يظهر جليا من خلال المادة 394 مكرر 01 من قانون العقوبات الجزائري، والأمر نفسه عند القانون الفرنسي في مادته 323 ــ 1/3 ق. ع. ف.

وعليه إذا توافر القصد الجنائي العام بعنصريه العلم والإرادة إلى جانب الركن المادي تقع جريمة الإعتداء القصدي على بيانات النظام المعلوماتي بما في ذلك نظام الحكومة الالكترونية، وبالتالي يستحق مرتكبوها العقوبة المقررة لها.

ثالثا ــ العقوبة المقررة لجريمة التلاعب ببيانات النظام المعلوماتي:

يرتّب قانون العقوبات الجزائري في مادته 394 مكرر01 على مرتكب جريمة التلاعب بالمعطيات عقوبة أصلية تتمثل في الحبس والغرامة، في حين يرتب عليه المادة 393 مكرر 06 عقوبة تكميلية يشترك فيها مع باقي جرائم المعطيات.

وهو النهج المتبع عند المشرع الفرنسي، حيث قرر عقوبة هذه الجريمة في المادة 323 ــ3 من ق.ع.ف، وفيما يلي تفصيل ذلك:

---

[1] ــ محمد مسعود محمد خليفة، مرجع سابق، ص 139.

[2] ــ حيث نصت المادة 1030 (أ) من التشريع الفيدرالي الأمريكي لسنة 1986. والتي تجرم الإتلاف العمدي وغير المصرح به لمعلومات يحتوي عليها حاسب آلي تابع لحكومة الولايات المتحدة الأمريكية أو ادارتها أو حاسب آلي غير تابع للحكومة إلا انه يستخدم من قبلها أو لصالحها ، ووسع قانون حماية بنية المعلومات القومية لعام 1986 من دائرة المعلومات محل الحماية فاضاف إلى ما سبق المعلومات الموجودة بالحاسبات المستخدمة من طرف المؤسسات الاقتصادية التابعة للحكومة وتلك المستخدمة في التجارة والاتصالات بين الولايات أو بين الولايات والدول الأخرى . أنظر: نائلة قورة، مرجع سابق، ص356.

1 ــ العقوبات الأصلية:

العقوبة الأصلية التي تقررها المادة 394 مكرر01 من قانون العقوبات الجزائري على مرتكب جريمة التلاعب بالمعطيات هي عقوبة الحبس من ستة(06) اشهر إلى ثـــــلاث (03) سنوات، وعقوبة الغرامة التي تتراوح من خمسمائة ألف (500.000 دج) إلى مليوني دينار جزائري (200.0000 دج). وفيما يخص عقوبة هذه الجريمة في قانون العقوبات الفرنسي، فقد كان قانون 1988 يعاقب عليها بالحبس من ثلاثة اشهر إلى ثلاث سنوات وبالغرامة من ألفي فرنك (2000) إلى خمسمائة ألف فرنك فرنسي (500.000 ف)، أمّا قانون 1994 فقد جعل حداً واحداً لهذه العقوبة، إذ أزال الحد الأدنى لها وثبتها عند الحد الأقصى وهو ثلاث سنوات، أما عقوبة الغرامة فجعلها خمسا واربعين ألف يورو (45.000 يورو)، أما قانون 2004 فقد شدد أكثر في العقوبة إذ رفع عقوبة الحبس إلى خمس سنوات وعقوبة الغرامة إلى خمس وسبعين ألف يورو (75.000 يورو)، وفي سنة 2015 أدخلت تعديلات على المواد الخاصة بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب المادة 04 من القانون رقم 2015ـــ912 المتعلق بالمعلوماتية، وشدّدت فيه عقوبة الغرامة فقط مع الابقاء بعقوبة الحبس ــ وهي خمس سنوات ــ وأصبحت بالنسبة لجريمة التلاعب 150.000 يورو [1]. كما أنه شدد العقوبة أيضا إذا كانت جريمة التلاعب تقع على المعطيات الشخصية التابعة للدولة لتصبح العقوبة سبع (7) سنوات حبس والغرامة إلى 300.000 يورو[2] .

الملاحظ أنّ عقوبة جريمة التلاعب بالمعطيات هي الأشد من بين العقوبات المقررة على باقي الأفعال المجرمة لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي للتلاعب، بينما لا يتوافر هذا

[1]- Article 323 – 3/1 de code pénaldispose que : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amande .

[2]- Article 323 – 3/2 de code pénal dispose «Lorsque cette infraction a été commise 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 sept ans d'emprisonnement et à 300 000 € d'amende".

القصد لدى مرتكب جريمة الدخول أو البقاء إلى نظام المعالجة الآلية للمعطيات المشددة. فالموقف النفسي لكل واحد منهما اتجاه التلاعب مختلف، حيث يريده الأول ولا يريده الثاني[1].

بالنسبة للعقوبة الموقعة على الشخص المعنوي فهي كما سلف ذكره الغرامة المضاعفة إلى خمس مرات عما هو مقرر على الشخص الطبيعي، وبالتالي تكون قيمتها في جريمة التلاعب بالمعطيات متراوحة بين مليونين وعشرة ملايين (2.000.000 إلى 10.000.000)دينار جزائري، وبالنسبة لقيمتها في القانون الفرنسي فهي ثلاث مائة وخمسة وسبعون ألف (375000) يورو، والغرامة هي العقوبة الأصلية الوحيدة التي نصت عليها المادة 394 مكرر 04.

2 ــ العقوبات التكميلية:

العقوبات التكميلية المقررة على جريمة التلاعب بالمعطيات هي نفسها العقوبات التكميلية المقررة بالنسبة لباقي جرائم المعطيات سواء في القانون الجزائري أو الفرنسي على النحو الذي سبق بيانه [2].

الفرع الثاني: جريمة التزوير المعلوماتي

ساهمت ثورة تكنولوجيا المعلومات والإتصال في تغيير طبيعة الوثائق الرسمية الإدارية، حيث بدأ العمل بالمعاملات الإلكترونية الحكومية، والتي تستند أساسا على الوثيقة المعلوماتية، لكن هذه الطبيعة المستجدة للوثيقة حملت معها العديد من التحديات، أبرزها أن تكون محلا للإعتداء عليها بتغيير حقيقتها بقصد الغش في مضمونها، إلا أن الضمانة الأبرز لحماية هذه الوثيقة من عملية التزوير المعلوماتي هي التشريعات، فماذا يقصد بجريمة تزوير الوثيقة المعلوماتية، ومدى قدرة التشريعات الحالية على بسط حماية لها؟

لمعالجة ذلك سيتم التطرق بداية إلى تعريف التزوير المعلوماتي وتحديد محله، ثم بيان الأركان الخاصة بهذه الجريمة وذلك على النحو التالي:

---

[1] ــ محمد خليفة، مرجع سابق، ص 145.

[2] ــ انظر فيما سبق ، ص32 وما بعدها.

أولا ــ مفهوم تزوير الوثيقة المعلوماتية: لتحديد مفهوم تزوير الوثيقة المعلوماتية بصفة عامة والوثيقة الإدرية الرسمية المعلوماتية بصفة خاصة، ينبغي الرجوع إلى صيغة نصوص قانون العقوبات الفرنسي كنموذج لتوسيع مفهوم التزوير، وإلى بعض القوانين العربية التي تناولت التزوير المعلوماتي في قوانين مستقلة.

1 ــ مفهوم التزوير في قانون العقوبات الفرنسي: توسّع المشرّع الجنائي الفرنسي في تجريم التزوير ليمتد إلى الوثيقة المعلوماتية ونظم ذلك في القسم الأول ضمن الكتاب الرابع من قانون العقوبات تحت عنوان"الإعتداءات ضد الثقة العامة" في المادة 1/441 المعدلة في 14 ماي1993[1].

طبقا لنص المادة 1/441 من قانون العقوبات الفرنسي[2]" التزوير هو كل تغيير بطريق الغش في الحقيقة ويكون من شأنه إحداث ضرر ويرتكب بأي طريقة كانت، سواء كان ذلك بالكتابة أو بأي سند آخر للتعبير عن الفكر والذي يكون الغرض منه أو كنتيجة له شأنا في إثبات حق أو واقعة لها آثارها القانونية".وعليه يمكن الاستنتاج أن الوثيقة تشمل إلى جانب الشكل التقليدي لها ــ وثيقة ورقية ــ كل وسيط آخر للتعبير عن فكرة معينة شرط أن يكون لها قيمة تبوثية، بمعنى أنها تصلح قانونا لإستخدامها كدليل إثبات حق أو واقعة لها آثار قانونية.

لما كان التزوير هو تغيير للحقيقة في الوثيقة، وهذه الأخيرة لها مفهوم أوسع طبقا للنص السابق " dans un écrit " و" support d'expression de la pensée "، وبالتالي فقد

---

(1) ــ أفرد المشرع الفرنسي نصا مستقلا في قانون العقوبات لمواجهة تزوير الوثائق المعلوماتية من خلال المادة 5/462 من قانون الغش المعلوماتي رقم 19/88 المؤرخ في 5 يناير 1988، لكن بعد تعديل قانون العقوبات الفرنسي سنة 1994 لم يأخذ المشرع بالمادتين 5/462 والمادة 6/462 المتعلقتين بتزوير الوثيقة المعالجة آليا واستعمالها باعتبار أن المادة 1/441 وسعت من مفهوم الوثيقة، خاصة والهاتين المادتين لاقتا اعتراضا من مجلس الشيوخ عند مناقشة هذا القانون، لما يترتب عليهما من مساواة بين المعطيات المعلوماتية بصفة عامة وبين المحررات من حيث القيمة القانونية، لذلك غيرالمشرع الفرنسي خطته بشأن تجريم تزوير الوثيقة المعلوماتية باعتبار أن المصلحة المحمية في جرائم المساس بالأنظمة المعلوماتية أو المعطيات مختلفة عن تلك المتعلقة بتزويرالوثائق المعلوماتية التي تتعلق بحماية الثقة العامة فيها. وبذلك الغيت المادتان من الباب الثالث (المتعلق بالجرائم المعلوماتية)، وأضافها إلى جريمة التزوير العادية بعد تطويع نصوصها بما يتلاءم وتلك المستندات. انظر: أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بتاريخ 09 ــ 11 ربيع الأول 1424 هـ الموافق لـ 10 ــ 12 مايو 2003 م، الإمارات العربية المتحدة، مرجع سابق، ص 539.

(2) - Article 441-1 de code pénal : "Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques."

شمل هذا المعنى كل الأشكال الحديثة التي نتجت عن استخدامات المعلوماتية والتي تحمل هذه الأفكار، ومن بينها الدعامات المادية كالأقراص الإلكترونية، أو البطاقات أو الشرائح المغناطيسية وغيرها، ولا يكون التزوير معتبرا إلا إذا كانت الوثيقة لها قيمة قانونية.

2 ــ تحديد مفهوم تزوير الوثيقة المعلوماتية بنصوص خاصة: من بين الإتجاهات التشريعية التي جرمت تزوير الوثيقة المعلوماتية بنصوص مستقلة عن قانون العقوبات منها التشريع المصري، وذلك من خلال قانون التوقيع الإلكتروني من جهة والأحوال المدنية من جهة أخرى، وذلك على النحو التالي:

أ) قانون التوقيع الإلكتروني: نصّت المادة 23 من قانون التوقيع الإلكتروني على :"مع عدم الإخلال بأية عقوبة أشد منصوص عليها في المادة قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من: ــ أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر".

المشرع المصري قد جرم التزوير في توقيع أو وسيط أو محرر إلكتروني عن طريق التقليد أو عن طريق التعديل في معلومات موجودة أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة. والملاحظ أنّ هذا النص لم يبين أركان جريمة التزوير بدقة بل اكتفى بالإشارة إلى بعض صور السلوك المادي كالاصطناع والتعديل[1].

ب) ــ قانون الأحوال المدنية[2]: جرّم المشرّع المصري في قانون الأحوال المدنية تزوير الوثائق الإدارية الرسمية ذات الطبيعة المعلوماتية المخزنة بالكمبيوترات الموجودة بمراكز الأحوال المدنية من خلال المادة 72 التي تنص على: "في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات

[1] - هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بتاريخ 09 ــ 11 ربيع الأول 1424 هـ الموافق لـ 10 ــ 12 مايو 2003 م، الإمارات العربية المتحدة، مرجع سابق، ص 57.

[2] - قانون الأحوال المدنية المصري رقم 143 لسنة 1994 في شأن الأحوال المدنية متاح على الموقع التالي:
https://groups.google.com/forum/#!topic/hamdy11/tzbzKpM2ri0 تاريخ الاطلاع: 2016/05/12.

المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومراكزا لإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية.

فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات".

وما يلاحظ على هذا النص أنه خاص بوثائق الأحوال المدنية ولا يسري على غيرها من الجرائم، وبالتالي تبقى هذه النصوص المتفرقة قاصرة عن استيعاب جريمة التزوير المعلوماتي من حيث موضع النص الخاص بها، أو من حيث تحديد أركانها، خاصة في ظل عدم تعديل قانون العقوبات فيما يتعلق بالتزوير ليشمل تزوير الوثيقة المعلوماتية[1].

أمّا بالنسبة للمشرع الجزائري فيعد من التشريعات التقليدية التي أبقت نصوصه الجنائية من غير تعديل بالرغم من استحداثه لنصوص تعاقب الإعتداء على نظام المعالجة الآلية للمعطيات(المواد من394 مكرر إلى 394 مكرر 7 من قانون العقوبات) والتي تضمنت بعض طرق التزوير كالتعديل والمحو والإدخال، بالإضافة إلى دخول الجزائر المجتمع المعلوماتي وتبني مشروع الحكومة الالكترونية سنة 2013، حيث بدأت بوادرها من خلال بطاقات السحب والدفع لبريد الجزائر كونها من البطاقات الذكية، وإطلاق العمل بجواز السفر البيومتري وبطاقة التعريف الوطنية البيومترية، يتبعها ذلك عصرنة الإدارة الإلكترونية من خلال تسهيل تقريب المواطن من الإدارة وصدور وثائق الأحوال المدنية بطريقة إلكترونية. كل ذلك يعد من العوامل الرئيسة التي تدفع المشرع الجزائري إلى ضرورة الاسراع إمّا:

ـــ بإضافة نص إلى باب التزوير في المحررات، بحيث يتناول هذا النص تعريف جريمة التزوير وأساسها ألا وهو المحرر وذلك على الشكل التالي: "المحرر هو كل مركب يتكون من حروف أو علامات تدل على فكرة معينة بالنظر إليها مباشرة أو بالإستعانة بتقنية أخرى"، وبذلك يشمل هذا النص المحررات التقليدية والمعلوماتية معا كالمستندات الموجودة على الأقراص والأشرطة.

[1]ـــ أشرف توفيق شمس الدين، مرجع سابق، ص 541 ـــ 542.

ـــ أو بإدراج نص خاص بالتزوير المعلوماتي[1].

ثانيا ـــ محل جريمة التزوير المعلوماتي

تنطوي جريمة التزوير على تغيير الحقيقة في محررات، وبظهور وانتشار تكنولوجيا المعلومات والإتصال ظهرت المحررات الالكترونية كمحل لجريمة التزوير المعلوماتي.

ولبيان مفهوم هذه المحررات[2] ينبغي أن نتطرق إلى تعريفها وفق ما جاءت به التشريعيات وتوصل إليه الفقه.

1) **التعريف التشريعي للمحررات (الوثيقة) الإلكترونية:** من بين التشريعات التي عرفت المحررات الالكترونية التشريع الإنجليزي في المادة 1/8 من قانون التزوير والتزييف لسنة 1981 بأنها تشمل كل شريط ممغنط أو صوتي أو كل وسيلة توجد بها بيانات مسجلة بطريقة ميكانيكية أو إلكترونية أو أي وسيلة أخرى".

كما عرفها القانون الكندي لسنة 1985 بأنها كل ورقة أو أي مادة أخرى سجلت عليها كلمات يمكن للشخص أو لجهاز الكمبيوتر أو أي وسيلة أخرى قراءتها أو فهمها"[3].

ومن بين الدول العربية التي كانت سبّاقة في تبني مشاريع الحكومة الالكترونية، ونظّمت كيفيات التعامل بالوثيقة المعلوماتية في المعاملات الإدارية الحكومية لدينا: الأردن، والإمارات العربية المتحدة ومصر.

ـــ حيث عرّف المشرع الأردني الوثيقة المعلوماتية في المادة 10 من قانون المعاملات الإلكترونية رقم 85 لسنة 2001[4]، بأنه: "رسالة معلومات يتم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بالوسائل الإلكترونية أو بوسائل مشابهة بما في ذلك تبادل البيانات أو البريد الإلكتروني أو الفاكس أو النسخ الرقمي"

---

[1] ـــ أشرف توفيق شمس الدين، مرجع سابق، ص 534.

[2] ـــ وذلك ما نصت عليه العديد من التشريعات وحصرته في ذلك السياق كالمشرع الجزائري، وتناوله في كل من القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد من 214 إلى 229.

[3] ـــ شيماء عبد الغني، مرجع سابق، ص 84.

[4] ـــ قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001، أنظر في تفاصيل هذا القانون: وائل أنور بندق، مرجع سابق، ص 373 وما بعدها.

ـــ في حين عرّف المشرع الإماراتي المحرر الإلكتروني في قانون التجارة الإلكترونية لإمارة دبي رقم (02) لسنة 2002، وذلك في الفقرة السابعة من المادة الثانية منه[1] بأنه: "سجل أو مستند إلكتروني يتم إنشاؤه أو تخزينه أو استخدامه أو نسخه أو إرساله أو إبلاغه أو إستلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلا للإسترجاع بشكل يمكن فهمه".

ـــ أمّا المشرّع المصري بين مفهوم الوثيقة المعلوماتية من خلال مصطلح المحرر الإلكتروني أولا، كما بين مفهوم المحرر الإلكتروني الرسمي من خلال قانون التوقيع الألكتروني. فبالنسبة لتعريف الوثيقة الأولى جاء ذلك في نص المادة الأولى من قانون التوقيع الإلكتروني رقم 15 لسنة2004[2] بأنه: "رسالة تنشأ أو تدرج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية، أو رقمية، أو ضوئية أو بأي وسيلة أخرى مشابهة".

أمّا بالنسبة للوثيقة الرسمية الإدارية المعلوماتية فقد أشارت إليها المادة 15 من قانون التوقيع الإلكتروني السابق الذكرعند بيان الحجية التي يتمتع بها المحرر الإلكتروني، حيث اعتبره ذلك المحرر الإلكتروني الصادر عن جهة إدارية والذي يحمل توقيعا إلكترونيا من موظف مختص[3].

ـــ تناول المشرّع الجزائري موضوع الوثيقة الإلكترونية لأول مرة سنة 2005 بموجب صدور قانون رقم (10/05) المعدل والمتمم للقانون المدني الجزائري[4]، حيث أصبح للكتابة في الشكل الالكتروني مكانا ضمن قواعد الإثبات في القانون المدني، وذلك طبقا لنص المادة 323 مكرر مدني جزائري على أنها: "كتابة تتكون من تسلسل حروف أو أوصاف أو أرقام أو أي علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها".

---

(1)ـــ قانون إمارة دبي رقم (02) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية، متاح بتاريخ 9 /2016/3 على الموقع التالي:
lhttp://www.aauopil.org/2012/02/2-2002.htm

(2)- القانون رقم 15 لعام 2004 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، المؤرخ في 21 أبريل 2004، الصادر في 23 أبريل 2004. انظر في تفاصيل القانون الموقع التالي: تاريخ الإطلاع 12 ديسمبر 2016.
http://www.wipo.int/wipolex/ar/details.jsp?id=13546

(3)ـــ وقد أشارت المذكرة الإيضاحية لهذا القانون إلى أن الإعتراف بحجية المحررات الالكترونية سواء كانت رسمية أو عرفية تشجع تعامل الأفراد والجهات الحكومية بها، فتحقق بذلك فكرة الحكومة الالكترونية. وبذلك يمكن كل فرد الحصول على الوثائق الرسمية إلكترونيا، ويعد ذلك مكسبا مهما حيث يسهل ذلك آداء الخدمات للجميع.

(4) ـــ القانون رقم (10/05) المؤرخ في 20 جوان 2005 المعدل والمتمم للأمر 75 ـــ 58 المتضمن القانون المدني، ج.ر.ج، ع 44، الصادر في 12 جوان 2005.

هكذا يتضح مما سبق أن المشرع الجزائري اعتمد المفهوم الواسع للكتابة سواء الكتابة على الورق أو على دعائم غير مادية، بشرط أن تكون الكتابة مفهومة.

2) التعريف الفقهي للمحررات (الوثيقة) الإلكترونية:

اختلف الفقهاء في تعريف الوثيقة المعلوماتية حيث ارتكز البعض منهم على الجانب المادي، أما البعض الآخر فتناول مفهومها من جانب موضوعي.

بالنسبة للإتجاه الأول: استخدم مصطلح الوثيقة المعلوماتية للدلالة على الوعاء أو الدعامة الالكترونية[1]، ويقصد بهذه الأخيرة الأجسام المادية المعدة سلفا لاستقبال المعلومات عن طريق طبعها بصورة أو بأخرى بشرط أن تكون سجلت عليها المعلومات بأحد الأساليب المعلوماتية[2].

أمّا الإتجاه الثاني، عرّف الوثيقة المعلوماتية بأنها "رسالة بيانات تتضمن معلومات تنشأ أو ترسل أو تستلم أو تخزن باستخدام وسائل إلكترونية".

تقديرنا في هذا أنّ الاتجاه الأول المستند رأيه حول الطبيعة الشكلية للمستند محل نظر: ذلك أن فكرة المستند الالكتروني في حد ذاتها لم تزل حتى الآن عرضة للتطور التقني، ومن تم لا يجوز التسليم باستقرار المعاملات الالكترونية، مدام المستند الالكتروني في تطور مستمر، لذلك يكون الاتجاه الموضوعي أقرب إلى الواقع والقانون.

---

[1] ــ تتعدد أشكال الدعامات الإلكترونية وذلك بحسب ما تفرزه تكنولوجيا المعلومات، ومن بين هذه الأشكال: القرص الصلب، القرص المضغوط والقرص الوميض.

القرص الصلب (Disque dur): هو قرص معدني رقيق مطلي بمادة مغناطيسية، له قدرة عالية على تخزين المعلومات وسرعة فائقة في تسجيل البيانات واسترجاعها، فهو ذاكرة تخزين موجودة عادة داخل الكمبيوتر حيث تعمل على تخزين معلومات متعددة منها نظام التشغيل، التطبيقات، المعطيات المدخلة.

أمّا القرص المضغوط (Compact Disque): هو قرص بصري أو ضوئي مسطح ودائري تخزن فيه البيانات في شكل إشارات رقمية، حيث تطلى الجهة التي تخزن عليها المعلومات بطبقة من الألمنيوم النقي، وتستخدم أشعة الليزر في تسجيل البيانات كفجوات محفورة على مسارات حلزونية ضيقة جدا غير منظورة على سطحه.

في حين أن القرص الوميض: هو قرص خارجي بحجم صغير،ي مكن حمله، ويتصل بمأخذ للكمبيوتر، وهو مثلا لقرص الصلب حيث تخزن عليها لمعلومات، كما يسهل عملية نقل هذه المعلومات من كمبيوتر لآخر. أنظر: محمد بلال الزعبي، أحمد الشرايعة، منيب قطيشات، سهير عبد الله فارس، خالدة محمد صايل الزعبي، مهارات الحاسوب، دار وائل للنشر والتوزيع، إعادة الطبعة الخامسة، 2008، ص 50 وما بعدها.

[2] ــ علي عبد القادر القهوجي، مرجع سابق، ص 38.

ومن نماذج الوثيقة الالكترونية والأكثر تداولا في مجال المعاملات الالكترونية الحكومية لدينا العقد الإداري الالكتروني، والبطاقات الإلكترونية (بطاقة التعريف الإلكترونية، جواز السفر الإلكتروني، بطاقة الوفاء...إلخ).

قضت محكمة النقض المصرية أن البطاقات الممغمطة يسري عليها وصف المحرر في مفهوم جريمة التزوير باعتبارها ورقة من أوراق البنوك[1].

ثالثا ــ أركان جريمة التزوير المعلوماتي:

تتعدّد أركان جريمة تزوير الوثيقة ذات الطبيعة المعلوماتية كباقي الجرائم بين ركن مادي ومعنوي، لكنها تتميز بخصوصية الأفعال المكونة لركنها المادي باعتبارها جريمة تقع في بيئة افتراضية غير ملموسة، ممّا يجعل أشكال وطرق التزوير مختلفة عن تلك المعروفة في جريمة التزوير التقليدية.

1 ــ الركن المادي لجريمة التزوير المعلوماتي

يتكوّن هذا الركن من عدة عناصر تتمثل في: تغيير الحقيقة في الوثيقة المعلوماتية عن طريق التلاعب في محتواها باتباع طرق مختلفة على نحو يسبب ضرر للغير.

أ ــ تغيير الحقيقة في نطاق المعلوماتية:

تغيير الحقيقة هو جوهر جريمة التزوير، والسلوك الإجرامي فيها هو الفعل الواقع على المحرر والذي يتمثل في تغيير الحقيقة على نحو مخالف للحقيقة، وبغير تغيير الحقيقة لا تقوم جريمة التزوير[2]. والمحرر في مجال المعاملات الإلكترونية يراد به المستند المعلوماتي، وهو كل شيء مادي متميز (قرص أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات ويستوي بعد ذلك أن يكون هذا الشئ قد خرج من الماكينة وتم تصنيفه أو تخزينه أم أنه مازال بداخلها انتظارا لاستخراجه أو تعديله[3] .

---

[1]- نقض مصري، الدائرة الجنائية، يوم الثلاثاء 15 مارس 2016، رقم 39505 لسنة 77 القضائية، لمزيد من التفاصيل حول هذا القضية يرجع الاطلاع على البوابة القانونية لمحكمة النقض المصرية في الموقع التالي:
http://www.cc.gov.eg/Courts/Cassation_Court/Criminal/Cassation_Court_Criminal.aspx. تاريخ الإطلاع: 2016/01/02

[2]- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة،2010 ، ص 931.

[3] ــ علي عبد القادر القهوجي، مرجع سابق، ص 150.

وفي إطار التعامل بالوثائق المعلوماتية في مجال الحكومة الالكترونية، يمكن إنجاز المعاملات الإدارية دون إخراجها على ورق ـــ لأنها مخزنة على الشبكة أو في النظم المعلوماتية ـــ، ودون مرورها بصورة مخرجات ضمن أية صورة تقليدية ممكنة، ولذلك يصبح فعل التغيير في الحقيقة الثابتة في هذه الوثيقة واقعا داخل النظام المعلوماتي أو على الشبكة، حيث يتعلق بتغيير معلومات معالجة آليا، وفي حالة إخراج هذه المعلومات بشكل ورقي عن طريق مخرجات الجهاز فتتمتع حينها المعلومات بالحماية القانونية من خلال نصوص التزير التقليدية[1].

وقد عالج المشرع الفرنسي جريمة التزوير في محررات النظام المعلوماتي وذلك من خلال قانون العقوبات الفرنسي الجديد الذي بدأ العمل به في الفاتح من مارس سنة 1994، واستحدث في باب التزوير نصا جديدا، هو نص المادة 441 ـــ1[2]، والملاحظ أن المشرع الفرنسي أحكم صياغته من ناحيتين:

الأولى: أنه قد حسم الخلاف حول المحرر المعلوماتي حيث قرر أن تغيير الحقيقة قد يتم في محرر أو في أي وعاء آخر، بمعنى أي دعامة آخرى غير المحرر.

الثانية: أنّ نص المادة 441 ـــ1 قد أطلق طرق تغيير الحقيقة، فلم تعد محددة قانونا على سبيل الحصر، كما كان عليه الحال في القانون الفرنسي القديم، حيث جاءت عبار نص المادة 441 ـــ1 كما يلي: ''يعد تزويرا كل تغيير بطريق الغش في الحقيقة من شأنه أن يحدث ضررا وأيا ما كانت الطريقة التي اجرى بها في محرر أو في دعامة (وعاء) أخرى تعبر عن فكر يهدف أو يمكن أن يرتب عليه إقامة الدليل على ثبوت حق أو واقعة ذات آثار قانونية''.

---

[1] ـــ براهمي جنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة محمد خيضر بسكرة، 2014 ـــ 2015، ص 204.

[2]-Article 441-1 de nouveau code penal, de 1 mars 1994:''Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.
Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 300 000 F : :d'amende''.valable a l'adresse suivante
https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=2818625CB6B4A1CC6C C068570B7.تاريخ الإطلاع: 2016/02/20

فمتى تم تغيير الحقيقة التي يحتويها المستند المعلوماتي وبأي طريقة شرط أن يكون محتوى ذلك المستند يثبت حقا أو واقعة ذات آثار قانونية يتحقق لنا بذلك جوهر جريمة التزوير وهو فعل تغيير الحقيقة.

ب ــ طرق التزوير المعلوماتي:

يمكن التلاعب في محتوى الوثيقة المعلوماتية بعدة أشكال فقد تكون بطرق مادية أو معنوية، وقبل التطرق إلى هذه الطرق تجدر الإشارة إلى أن الطرق المادية يجب أن تتم على مستند أصلي حقيقي، بينما طرق التزوير المعنوية لا تتحقق إلا أثناء تكوين المستند، ومن أهم طرق التزوير المادية[1]:

1. الحذف: وذلك بإزالة كلمة أو رقم أو رمز من شأنه التغيير في مضمون المستند.
2. الإدخال: وذلك بإضافة معطيات إلى المستند تغير محتواه.
3. التعديل: وذلك بحذف معطيات من المحرر وإضافة آخر مكانه.

هذه الطرق عاقب عليها المشرع الجزائري في نص المادة 394 مكرر 1 من قانون العقوبات. ما يلاحظ أن هذه الطرق تجعل جريمة تزوير الوثيقة المعلوماتية تشتبه بجريمة الإعتداء العمدي على النظام المعلوماتي التي تتم بأفعال مشابهة عن طريق الإدخال والمحو والتعديل، غير أن الفرق بينهما يكمن في طبيعة المعلومات التي يتم الإعتداء عليها، حيث تكون تلك المعلومات وثيقة في جريمة التزوير إذا كانت تثبت حقا أو مركزا قانونيا معينا أي لها آثار قانونية بالنسبة للغير.

يحدث هذا الفرض كثيرا في نطاق المعاملات الالكترونية خاصة في مجال المعاملات المالية حيث أنه في ظل انتشار التحويل الالكتروني للأموال من بنك لآخر قد يلجأ المجرم إلى تزوير الرسالة (الوثيقة) ليتم الدفع لحسابه هو[2] أو ما يقوم به الجاني من استبدال رقم القيد الخاص به برقم القيد الخاص بأحد الأشخاص[3].

---

[1] - براهمي جنان، مرجع سابق، ص 203.

[2] ــ أحمد الخليفة الملط، الجريمة المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، الاسكندرية، 2006، ص 467.

[3] ــ محمد عبيد الكعبي، مرجع سابق، ص 563.

كما توجد طرق مادية أخرى للتزوير م ينص عليها المشرع وهي تناسب الطبيعة المعلوماتية للوثيقة وذلك كتزوير الصورة، حيث يقع هذا التزوير بتغيير الصورة الموجودة في الوثيقة[1]، إذا كانت الصورة عنصرا جوهريا لا يقل أهمية عن بعض بيانات الوثيقة، كالبطاقات الشخصية ورخص القيادة وبطاقة التأمين وغيرها. ويتم هذا التزوير بالاستبدال باستخدام الماسح الضوئي، حيث توجد برامج متخصصة بتركيب الصور، وبالتالي لا يعد تغيير الصورة فعلا معاقبا عليه إلا إذا كانت الصورة جزءا مكملا لمحرر على أساس أن استبدالها يؤدي إلى تغيير في حقيقة معناه أو مضمونه[2].

أما أهم طرق التزوير المعنوي[3]في نطاق المعاملات الالكترونية تتمثل في:

1. تغيير إقرار أولي الشأن: ويحدث هذا الفرض عند قيام الموظف المشرف على تحرير الوثيقة بتغيير المعلومات التي طلب تدوينها عند إنشاء الوثيقة، وذلك بتحريف مضمونها ابتداء[4].

2. جعل واقعة غير صحيحة في صورة واقعة صحيحة: مثل قيام موظف الحالة المدنية بتغيير الحقيقة في شهادة الميلاد أو الوفاة إثباتا لوقائع غير صحيحة، سواء بتدوين بيانات معينة أو بترك تدوين بيانات لها أثرها من الناحية القانونية[5] .

وعليه إمكانية وقوع التزوير المعلوماتي بالطرق المعنوية وارد بصورة أكبر من التزوير المادي، والسبب في ذلك أن هذا التزوير ينصب على تغيير مضمون أو دلالة المحرر ذاته، فضلا عن أنه لا يتضمن آثار مادية تشير بجلاء إلى العبث بالمحرر، ولذلك لا يستدل عليه إلا إذا تم التوصل إلى حقيقة ما كان يجب إثباته وذلك للوصول إلى أن ما تم مخالف للحقيقة، هذا فضلا عن أن التزوير المعنوي

---

(1) ــ عبد الفتاح بيومي حجازي، الحكومة الالكترونية، الكتاب الثاني...، مرجع سابق، ص 203.

(2) ــ براهمي حنان، مرجع سابق، ص 206.

(3) ــ يقوم التزوير المعنوي في الوثيقة الورقية على تغيير الحقيقة في مضمونها دون وجود أي أثر مدرك على التغيير في ظاهرها حيث تبقى هذه الوثيق محافظة على شكلها وسلامتها ودون المساس بطبيعتها.فالاعتداء لا يقع على الوثيقة بل على مضمونها، حيث ما يذكر فيها من بيانات لا يتفق مع الحقيقة.

(4) ــ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، القاهرة، 2005، ص 223.

(5) ــ برا هيمي حنان، مرجع سابق، ص 217.

مصاحب لإنشاء المحرر المزور ذاته[1]، لأن هذه الوثيقة يتم إنشاءها من طرف الموظف العام المكلف قانونا بذلك ما يمنحه فرصة تغيير المعطيات التي تلقاها من ذوي الشأن خلال مرحلة الإدخال.

تجدر الإشارة أنّ الطرق المذكورة في التزوير ليست على سبيل الحصر في الجريمة المعلوماتية، لأن هذه التكنولوجيا متطورة وأشكالها متغيرة بشكل سريع، لذلك لا ينبغي حصر طرق التزوير عند صياغة النصوص التشريعية في مجال تجريم تزوير الوثيقة المعلوماتية.

ج ــ الضرر في جريمة التزوير المعلوماتي: لا يكفي لقيام جريمة التزوير قيام الركن المادي بتغيير الحقيقة في الوثيقة بل يكون من شأن ذلك إحداث ضرر للغير، وقد يكون هذا الضرر محققا أي واقعا فعلا أو محتملا بمعنى من الممكن تحققه في المستقبل وفقا للمجرى العادي للأمور[2].

يتميز الضرر في جريمة تزوير الوثيقة المعلوماتية بخصوصية معينة جعلت مدلوله يختلف بين أمرين:

الأول: يستند على مدى إمكانية المساس بالقيمة القانونية للوثيقة كدليل إثبات، حيث لا وجود للضرر إلا إذا أصاب القيمة التبوثية لهذه الوثيقة، بمعنى أن التزوير المعلوماتي مرتبط بتزوير معطيات لإستخدامها في إنتاج آثار قانونية، أي أن هذه الوثيقة معدة ابتداء كدليل إثبات، فإذا تخلف هذا المضمون، ووقع التزوير فإن الأمر يكيف على أساس جريمة إتلاف معطيات معلوماتية[3].

أمّا المدلول **الثاني:** فيرتبط بمعيار الخسارة المترتبة عن التزوير، فالضرر قائم حتى ولو لم يكن المحرر قد أعد أصلا للإثبات[4].

إلا أنه قد يؤخذ في جريمة تزوير الوثيقة المعلوماتية خاصة الوثيقة الرسمية الإدارية بتحقق الضررمتى كانت الوثيقة المعلوماتية تتمتع بقيمة قانونية في الإثبات ابتداء أي منذ نشوئها، والضرر في هذه الحالة مفترض من الناحية القانونية باعتبار هذه الوثيقة تنبعث منها ثقة عامة عند الأفراد.

---

(1) - عبد الفتاح بيومي حجازي، مرجع سابق، ص 222

(2) ــ إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2008، ص 57.

(3) - عبد الفتاح بيومي حجازي، الدليل الجنائي ..، مرجع سابق، ص248.

(4) ــ براهمي حنان، مرجع سابق، ص223.

2 ــ الركن المعنوي لجريمة التزوير المعلوماتي:

لا تكتمل جريمة التزوير في وثيقة معلوماتية إلا إذا توافر الركن المعنوي إلى جانب الركن المادي على غرار باقي الجرائم، وتعتبر هذه الجريمة من الجرائم العمدية، حيث لابد من توافر القصد الجنائي، غير أنه لا يكفي وجود القصد العام فقط، وإنما لابد من توافر قصد خاص، وذلك ما سنبينه في التالي:

1. **القصد العام:** يقوم القصد العام في جريمة التزوير المعلوماتي بانصراف إرادة الجاني إلى تغيير الحقيقة في وثيقة معلوماتية، مهما كانت الطريقة التي استخدمها لإيقاع هذا التغيير حيث لم تعد هذه الطرق محصورة كما هي في جريمة التزوير في وثيقة ورقية، كما يجب أن يرتبط علم الجاني بأنه يغير الحقيقة في وثيقة لها قيمة قانونية وهي محمية قانونيا. وهذا العلم مفترض فلا يدفع مسؤوليته عن ذلك بجهله[1].

2. **القصد الخاص:** هو نية إضافية أو قصد إضافي يتمثل في اتجاه نية الجاني إلى استعمال الوثيقة المزورة فيما زورت من أجله[2]. فإذا تخلفت هذه النية انتفى القصد الجنائي.

وتعتبر صيغة النص الجنائي الفرنسي في تجريم التزوير المعلوماتي من الصيغ التشريعية الأكثر وضوحا لنية الغش، مما يعني أن المشرع الفرنسي يتطلب في الجريمة توافر القصد العام إلى جانب القصد الخاص الذي قوامه غرض الجاني التأثير في إثبات حق أو واقعة قانونية[3]، وذلك ما يستشف بوضوح من نص المادة 441 ــ 1 من قانون العقوبات الفرنسي[4]،

أمّا المشرع المصري لم يحدد نوع القصد الذي يتطلبه لدى الجاني، وما إذا كان يكتفي بالقصد العام أم أنه يتطلب إضافة قصد خاص، ويتضح ذلك من نص المادة 23 من قانون التوقيع الالكتروني

---

(1) ــ فتوح الشاذلي وعفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار الثقافة للطباعة والنشر، القاهرة، 2000، ص 258.

(2) ــ علي عبد القادر القهوجي، الحماية الجنائية ...، مرجع سابق، ص 152.

(3) ــ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، دار النهضة العربية، ط 1، القاهرة، 2006، ص 114.

(4) - Article 441-1de code pénal français: " Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques".

المصري السالف الذكر في الفقرة ب، حيث جرم الاعتداء على المحرر الالكتروني بالتزوير، لكنه لم يبين نية الغش، إذ نصت هذه المادة على "أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا، أو زوّر شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر".

3 ــ العقوبات المقررة لجريمة التزوير المعلوماتي:

إنّ بيان العقوبات المقرّرة في جريمة تزوير الوثيقة المعلوماتية ذات الطبيعة الرسميّة الإدارية يقتضي الرجوع إلى الصيغ التشريعية المجرمة لهذا الفعل، سواء كان هذا الفعل مجرما بنصوص قانون العقوبات، أو بنصوص خاصة.

والمشرع الجزائري لم ينص ــ بنص خاص ــ على جريمة التزوير المعلوماتي مما أثير بشأنه جدلا فقهيا في مدى مساواته بالتزوير التقليدي ومن تم تطبيق العقوبات المقررة للتزوير التقليدي على المحررات المعلوماتية.

3 ــ 1 العقوبات المقررة في قانون العقوبات الفرنسي: صنّف المشرع الفرنسي العقوبات المقررة لجريمة التزوير إلى عدة أصناف وذلك ما يظهر جليا في نص المادة 441 من قانون العقوبات حيث جاءت في عدة فقرات، فالعقوبة تختلف بحسبما ما إذا كانت الوثيقة محل التزوير وثيقة رسمية إدارية أو وثيقة عرفية، كما تختلف حسب صفة الشخص مرتكب التزوير.

- بالنسبة للعقوبة المقررة في حال تزوير وثيقة صادرة عن إدارة عامة: تطبق على المخالف عقوبة أصلية تتمثل في السجن لمدة خمس (5) سنوات، وغرامة قدرها 7500 يورو، وذلك طبقا للمادة 441 ــ 1 من قانون العقوبات الفرنسي[1].

كما يمكن أن تلحق بها عقوبات تكميلية مثل المنع من ممارسة الحقوق المدنية، والأسرية، وكذا المنع من شغل الوظائف العامة.

---

[1] - Article 441-2 de code pénal françaisconstitue :" Le faux commis dans un document délivré par une administration publique aux fins de constater un droit, une identité ou une qualité ou d'accorder une autorisation est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende."

- العقوبة المقررة في حال تزوير وثيقة عامة أو رسمية: قرر المشرع الفرنسي طبقا للمادة 441 ــ 4 فقرة 1 من قانون العقوبات الفرنسي عقوبة السجن لمدة عشر (10) سنوات، وغرامة مالية تقدر بـــ 150.000 يورو كل من يقوم بتزوير الوثائق العامة الصادرة عن الجهات الحكومية، وكذا الوثائق القضائية بمعنى الأحكام والقرارات[1].

- اختلاف العقوبة حسب صفة المزور: رفع المشرع الجنائي الفرنسي العقوبة في حال تزوير وثيقة رسمية إدارية معلوماتية من طرف موظف عام أو مكلف بخدمة عامة، وذلك بمقتضى المادة 441 ــ 4 فقرة 3 من القانون الجنائي إلى عقوبة السجن لمدة (15) سنة، وغرامة مالية تقدر بـــ: 225.000 يورو[2] .

يرجع سبب ارتفاع العقوبة في جريمة التزوير المعلوماتي من طرف الموظف العام إلى سهوله ارتكابها من طرفه لما يملكه من سلطة والتي خولها له القانون لتحرير مثل هذه الوثائق، حيث سيكون لهذا الشخص المرخص له أو المسموح له قانونا بالدخول إلى النظام المعلوماتي; ومن تمّ إجراء عملية التزوير عليها.

3 ــ 2 العقوبات المقررة بنصوص خاصة:

انتهجت بعض تشريعات الدول، لاسيما العربية منها كالتشريع المصري والإماراتي منهجا معينا في تجريم جريمة التزوير المعلوماتي، حيث جرما هذا الفعل في قوانين منفصلة عن قانون العقوبات.

ــ بالنسبة للمشرع المصري، عاقب على فعل تزوير الوثيقة المعلوماتية في قانون التوقيع الالكتروني من خلال المادة 23 منه بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه (10.000) ولا تجاوز مائة ألف جنيه (100.000) أو بإحدى هاتين العقوبتين، إلا أنه يجب مراعاة العقوبة الأشد

(1) - Article 441-4de code pénale français: "Le faux commis dans une écriture publique ou authentique ou dans un enregistrement ordonné par l'autorité publique est puni de dix ans d'emprisonnement et de 150 000 euros d'amende"

(2)- Article 441-4/ 3; " Les peines sont portées à quinze ans de réclusion criminelle et à 225 000 euros d'amende lorsque le faux ou l'usage de faux est commis par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions ou de sa mission."

المنصوص عليها في قانون العقوبات أو أي قانون آخر[1].وفي مقابل ذلك نص المشرع المصري في المادة 72 من قانون الأحوال المدنية السابق الذكر عقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات (5) كل من قام بتزوير وثائق الحالة المدنية والتي لها طبيعة معلوماتية.

وعليه نستنتج أنّ عقوبة تزوير المستند الالكتروني تختلف في مصر على حسب نوع المستند الالكتروني المزور، فالتزوير في الوثيقة المعلوماتية الرسمية الإدرية يعاقب عليه بعقوبة أشد، بخلاف تزوير مستند إلكتروني عادي[2].

ـــ أمّا المشرع الإماراتي، فهو بدوره انتهج نفس أسلوب المشرع المصري فيما يتعلق بتجزأة عقوبة تزوير الوثيقة المعلوماتية الرسمية الإدارية، حيث قرر في المادة السادسة من المرسوم بقانون إتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الإماراتي[3] عقوبة السجن المؤقت والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم كعقوبةأصلية كل من زور مستندا إلكترونيا حكوميا هذا بالاضافة إلى عقوبة المصادرة كعقوبة تكميلية حيث نصت المادة 41 من هذا المرسوم بقانون على :"مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من

---

[1]ـ نصت المادة 23 من قانون التوقيع الإلكتروني على :" مع عدم الإخلال بأية عقوبة أشد منصوص عليها في المادة قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من: أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر".

[2] ـــ والملاحظ أن المشرع المصري جزأ عقوبة جريمة تزوير الوثيقة المعلوماتية، فليس هناك نصا جنائيا واحد يبين تدرج العقوبة حسب طبيعة الوثيقة المعلوماتية المزورة.

[3] ـــ نصت المادة 06 من مرسوم بقانون الإتحادي رقم (05) لسنة2012 بشأن مكافحة جرائم تقنية المعلومات على: يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائة وخمسون ألف درهم ولا تجاوز سبعامئة وخمسون ألف درهم كل من زور مستندا إلكترونيا من مستندات الحكومة الإتحادية أو المحلية أو الهيئات أو المؤسسات العامة الإتحادية.

وتكون العقوبة الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو إحدى هاتين العقوبتين إذا وقع التزوير في مستندات جهة غير تلك المنصوص عليها في الفقرة الأولى من هذه المادة.."لمزيد من التفاصيل حول هذا المرسوم بقانون يرجى الإطلاع في الموقع التالي:

http://www.wipo.int/wipolex/ar/text.jsp?file_id=316910 تاريخ الإطلاع: 2015/02/12.

الجرائم المنصوص عليها في هذا المرسوم أو الأموال المتحصلة منها.."، سواء تعلق الأمر بوثيقة صادرة عن الحكومة الإتحادية أو المحلية باعتبارها تتمتع بقيمة قانونية.

من خلال هذا المرسوم بقانون إتحادي نفسه نص المشرع الإماراتي في المادة 48 منه :"لا يخل تطبيق العقوبات المنصوص عليها في هذا المرسوم بقانون بأية عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر".

بذلك يكون مرسوم بقانون رقم(05) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات قد أحال لقانون العقوبات الإتحادي في تطبيق العقوبة متى كانت أشد من تلك الواردة فيه.

هذا في ما يتعلق بالجرائم الماسة بمصلحة سلامة البيانات المعلوماتية وهي من أولى المصالح اللازمة للتعاملات الالكترونية فهي التي تبعث الثقة في متعاملي الحكومة الالكترونية. وفيما يلي سيتم التعرض لمصلحة أخرى وهي الحفلظ على سرية البيانات الشخصية، وذلك على النحو التالي بيانه.

المطلب الثاني: جرائم الاعتداء ضد سرية البيانات الخاصة (الشخصية)

إنّ اللجوء إلى أتمتة العمل الاداري عن طريق الاعتماد على الحاسب الآلي وشبكات الانترنت في تقديم الخدمات العامة للجمهور تتطلب تجميع بيانات خاصة بالأفراد، من ذلك بيانات المتعاملين المخزنة في الأنظمة المعلوماتية لمصلحة الحالة المدنية، وهي بيانات تتعلق بالفرد منذ ولادته حتى وفاته، وكافة مفردات حالته المدنية محفوظة في هذا الأرشيف الالكتروني، وهي بطبيعة الحال عرضة للاعتداء سواء بالتلاعب فيها أو بانتهاك سريتها ونشرها بدون إذن صاحب الشأن نفسه[1].

وتجدر الاشارة أن هذه الاعتداءات لا تقتصر فقط على البيانات المخزنة في النظام المعلوماتي للحكومة الالكترونية، بل حتى البيانات التي يتم تبادلها إلكترونيا وذلك أثناء إجراء المعاملة الالكترونية الحكومية بين الحكومة الالكترونية نفسها وبين المتعامل معها، بغض النظر عن طبيعة المعاملة

[1] ـــ سيف عبد الله الجابري، أمن المعلومات والخصوصية الفردية، ورقة بحث مقدمة إلى المؤتمر الدولي لأمن المعلومات الإلكترونية "معا نحو تعامل رقمي آمن"، المنعقد بتاريخ 18ـــ20 ديسمبر 2005 بمسقط، سلطة عمان، مرجع سابق، ص 239.

الالكترونية سواء كانت عبارة عن تقديم خدمة عمومية أو إبرام صفقة في إطار التجارة الالكترونية الحكومية.

يمكن تعريف البيانات الخاصة بأنها معلومات تتعلق بالشخص ذاته كإنسان مثل الاسم والعنوان رقم الهاتف وغيرها من المعلومات التي تأخذ شكل بيانات وثيقة الارتباط والالتصاق بكل شخص طبيعي معرف أو قابل للتعريف[1].

تتعدّد صور هذه البيانات الشخصّية، منها ما يتعلق بالحالة الصحية للأشخاص، أو التي تتعلّق بالحالة المدنية، وحتى بالشؤون المالية كرقم الحساب البنكي ومركزه المالي ..إلخ[2].

نظرا لحساسية هذه البيانات وزيادة المخاطر المستمرة في استخدام الوسائل التقنية في جمع ومعالجة البيانات الشخصية من قبل الدولة، خاصة وتبني نظام الحكومة الالكترونية واعتمادها قاعدة البيانات المعلوماتية، لذا تظافرت الجهود الدولية لحماية البيانات الشخصية كإتفاقية مجلس أوربا الخاصة بحماية البيانات من مخاطر المعالجة الآلية في 17 سبتمبر 1980 السارية المفعول سنة 1985، وعلى دليل منظمة التعاون الاقتصادي والتنمية لعام 1980، ودليل الأمم المتحدة عام 1990 المتعلق باستخدام المعالجة الآلية للبيانات الشخصية، وفي خلال السنوات الخمس اللاحقة أصدر الاتحاد الأوربي في عام 1995 دليلا شاملا ملزما لدول الإتحاد الأوربي، يطلق عليه " الأمر التشريعي المتعلق بحماية خصوصية المعلومات وتنظيم نقل المعلومات خارج الحدود"[3].

إلى جانب هذه الجهود الدولية لحماية البيانات الخاصة، اهتمت تشريعات الدول بحماية هذا النوع من البيانات وفي مقدمتها التشريع الفرنسي بموجب القانون رقم 78/ 17 المتعلق **"بالمعلوماتية**

---

[1] ــ بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية، بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، جامعة الدكتور مولاي الطاهر بسعيدة، ع 6، جوان 2016، ص 273.

[2] ــ نفس المرجع، ص 274.

[3] - علي كريمي، تأثير التطور التكنولوجي على حقوق الإنسان ، الحياة الخصوصية وحماية البيانات الشخصية "نمودجا"، مجلة أبحاث الفعل الإحتجاجي بالمغرب، مقاربة الإنسان والسلوكيات والقيم، العدد 61 ــ 62 لسنة 2015، المغرب، ص 86.

والحريات"[1]، كما اهتمت أيضا بعض تشريعات الدول العربية بحماية الحق في الحياة الخاصة في مجال المعلوماتية[2].

فهل يوجد تنظيم قانوني خاص بجرائم التعدي على البيانات الخاصة في التشريع الجزائري؟.

الفرع الأول: جرائم الاعتداء على البيانات الخاصّة في التشريع الفرنسي

يتطلّب بيان مختلف أشكال وصور الجرائم الواقعة على البيانات الخاصّة تحديد أركانها ومن تم بيان العقوبات المقررة على مرتكبي هذه الجرائم وذلك على النحو التالي:

أولا ـــ تحديد أركان جرائم الاعتداء على البيانات الشخصية في التشريع الفرنسي:

تعتبر فرنسا من الدول الرائدة في ميدان حماية حقوق وحريات المواطنين في مواجهة مخاطر وتطورات تكنولوجيا المعلومات، حيث أصدرت بتاريخ 1978/01/06 قانون "المعلوماتية والحرّيات"، والذي تمّ تعديله عدّة مرات وتتميمه بعدة مراسيم خلال السنوات: 1988[3]ـــ و1992[4]وفي سنة 1996 [5]، وفي سنة 1999[6].

---

(1) -Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés .

(2) - كالتشريع التونسي من خلال القانون الأساسي المتعلق بحماية المعطيات الشخصية المؤرخ في 27 جويلية 2004، ج. ر عدد 63 لسنة 2004، حيث نص في الفصل الأول منه" لكل شخص الحق في حماية المعطيات الشخصية المتعلقة بحياته الخاصة باعتبارها من الحقوق الرئسسية المضمونة بالدسنور..."، وأصدر في ذات الإتجاه الأمر الخاص بتحديد وضبط طرق سير الهيئة الوطنية لحماية المعطيات الشخصية المؤرخ في 27 نوفمبر، الأمر عدد 3003 لسنة 2007. كما أصدر في نفس السنة من خلال الأمر المتعلق بشروط وإجراءات التصريح والترخيص لمعالجة المعطيات الشخصية، عدد 3004 لسنة 2007 المؤرخ في 27 نوفمبر. كما أصدر المشرع المغربي قانون رقم (08 ـــ 09) المتعلق بالأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، منشور في الجريدة الرسمية عدد 5711 بتاريخ 23 فبراير 2009.

(3) -Loi n° 88-227 du 11 mars 1988 relative à la transparence financière de la vie politique.

(4) - Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur.

(5) - Ordonnance n° 96-267 du 28 mars 1996 relative à l'entrée en vigueur du nouveau code pénal dans les territoires d'outre-mer et dans la collectivité territoriale de Mayotte ainsi qu'à l'extension et à la modification de certaines dispositions législatives rendues nécessaires par cette entrée en vigueur.

(6) -LOI n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle.

وأهم تعديل سنة 2004[1]، تم تلاه فيما بعد تعديل سنة 2006[2]، وقد أنشأ هذا القانون سلطة إدارية مستقلة هي "الجنة الوطنية للمعلوماتية والحريات". ثم أجرى عليه المشرع الفرنسي فيما بعد بعض التعديلات على القانون الجنائي ومسّ هو الآخر بالقانون رقم 78ـ 17 وتعديلاته، و لم يقم بتغيير روح قانون المعلوماتية والحريات، وقد تضمن التشريع الجنائي الفرنسي الحديث المواد 41 ـ 44 من قانون 1978 في الفصل الخاص بحماية ـ الشخصية ـ وتناول الجرائم المتعلقة بالبيانات الاسمية والأحكام الخاصة بالعقاب في المواد 226 ـ 16 والمادة 226 ـ 24 من قانون العقوبات الجديد، وقد ادخل المشرع الفرنسي الأفعال التالية ضمن الجرائم وذلك على النحو التالي:

1 ـ عدم اتخاذ الإجراءات الأولية لمعالجة البيانات، المادة 226 ـ 16 .

2 ـ عدم إتحاد الاحتياطات اللازمة لحماية البيانات، المادة 226 ـ 17 .

3 ـ المعالجة غير المشروعة للبيانات المادة 226 ـ 18 .

4 ـ معالجة بيانات اسمية محظورة دون موافقة أصحابها (ذوي الشأن) المادة 226 ـ 19.

5 ـ حفظ بيانات اسمية خارج الوقت المسموح به وفقا للطلب أو الإعلان المادة 226 ـ20.

6 ـ تغيير الغرض المحدد لجمع البيانات الاسمية المادة 226 ـ 21 .

7 ـ إفشاء البيانات الاسمية بما يضر بصاحب الشأن المادة 226 ـ 22. (الافشاء غير المشروع للبيانات الاسمية).

وفي ما يلي تفصيل لهذه الجرائم:

(1) -LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) -LOI n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

1 ــ جريمة عدم اتخاذ الاجراءات الاولية لمعالجة البيانات:

نصّت المادة 226ــ16 من قانون العقوبات الفرنسي على أن "كل من قام ولو بإهمال بمعالجة آلية للبيانات الاسمية دون مراعاة الاجراءات الأولية للقيام بها، والمحددة بالقانون يعاقب بالحبس لمدة ثلاث سنوات وبغرامة 300 أورو"[1].

يتّضح من خلال المادة 226 ــ 16، أنّ هذه الجريمة تتوافر على ركنين مادي ومعنوي وذلك على النحو التالي:

أ ــ الركن المادي:

لقيام الركن المادي لهذه الجريمة يجب أن تتم المعالجة الآلية للبيانات الشخصية دون اتخاذ الاجراءات القانونية الواردة بالمادتين 15و16 من قانون المعلوماتية والحريات رقم (17/78).

يرى جانب من الفقهاء أنّ نص التجريم يمتد ليشمل أيضا عدم مراعاة الاجراءات المنصوص عليها بالمادة 17 من قانون1978[2].

طبقا لنص المادة 15 فإنه يتعين بالنسبة لمعالجة البيانات الاسمية لحساب الدولة أو لحساب الهيئات المحلية أو الأشخاص المعنوية الخاصة التي تقوم بإدارة وخدمة عامة أن يتم تنظيم معالجة البيانات بلائحة، بناء على موافقة اللجنة الوطنية للمعلوماتية والحريات.

أمّا المادة 16 من قانون المعلوماتية والحريات، فتنص على أنه عندما يتعلق الأمر بمعالجة البيانات لحلاف الجهات المحددة بالمادة 15، فإنه يتعين إخطار اللجنة الوطنية للمعلوماتية والحريات، قبيل إجراء معالجة البيانات ويجب أن ينطوي هذا الاخطار على إقرار بأن المعالجة تتفق ومتطلبات القانون، وعند استلام الجهة الطالبة ما يفيد العلم بوصول الاخطار للجنة، كان في إمكانها البدأ في معالجة البانات، علما بأن هذا لا يعفيها من مسؤوليتها القانونية.

---

(1) - Articl 226-16 de code penal francais constitue: “Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.”

(2 -)Gabriel Roujou de Bourée, Bernard Bouloc, Jacque Francillon, Yeves Mayaud, code pénale comenté,Dalloz, 1996 P . 415 ets s. .

كما نصّت المادة 17 من هذا القانون على أنه فيما يتعلق بصور معالجة البيانات العامة أو الخاصة الجارية والتي لا تمس بالحياة الخاصة أو الحريات.يكتفي المشرع بشأنها بإخطار مبسط للجنة الوطنية للمعلوماتية والحريات، ويتم تسليم الإحطار بيان علم الوصول ويكون للجهة البدء فورا في معالجة البانات.

يتضح من خلال ما سبق أن المعالجة الآلية للبيانات الاسمية التي تتم لصالح الحكومة تتطلب ترخيصا، والمعالجة التي تتم لصالح أشخاص القانون الخاص تتطلب إخطار اللجنة الوطنية للمعلوماتية والحريات، ويكفي فقط إخطار مبسط للجنة طبقا للمادة 17 من القانون رقم (78ـــ17) المتعلق بالمعلوماتية والحريات، إذا كانت المعالجة لحساب أشخاص القانون العام أو الخاص ولا تنطوي على المساس بالحياة الخاصة أو الحريات، وكانت متسقة مع الضوابط التي وضعتها اللجنة حسب ما جاء في المادة 17 .

يتحقّق الركن المادي لهذه الجريمة بأي معالجة آلية للبيانات الاسمية دون اتخاذ الاجراءات الأولية التي يتطلبها القانون (سواء ترخيص أو إخطار أو إخطار مبسط للجنة الوطنية للمعلوماتية والحريات)، ولا يشترط توافر نتيجة اجرامية معينة.

نلاحظ أنّ المشرّع الفرنسي أولى عناية خاصة بالبيانات الإسمية، حيث فرض إجراءات وقائية تحول دون المساس بهذه البيانات (عن طريق الترخيص والإخطار)، فهذه الحماية لا تقتصر على البيانات الخاصة، بل مدد الحماية حتى في البيانات التي لا تمس الحياة الخاصة واشترط فيها الحصول على إخطار مبسط من اللجنة الوطنية للمعلوماتية والحريات.

ب ـــ الركن المعنوي:

يتّخذ الركن المعنوي لهذه الجريمة في إحدى الصورتين الأولى، القصد الجنائي أو الخطأ غير العمدي (الخطأ الجنائي)، ويتحقق القصد الجنائي العام بعلم الجاني بالواجبات التي كان يفرضها عليه القانون والتي تتمثل في القيام باتخاذ بعض الاجراءات الأولية قبل إجراء أي معالجة آلية للبيانات الاسمية كالحصول على ترخيص أو إخطار من اللجنة الوطنية للمعلوماتية والحريات، ويجب أن تتجه

إرادة الجاني إلى إجراء المعالجة الألية دون مراعاة للإجراءات الأولية التي يتطلبها القانون، ولا عبرة بالبواعث[1].

كما يأخذ الركن المعنوي أيضا صورة الخطأ إذا كان نتيجة إهمال أو رعونة الفاعل حسب نص المادة 226 ــ16 من قانون العقوبات الفرنسي، وبالتالي يعاقب المشرع على هذه الجريمة سواء اتخذ الركن المعنوي القصد الجنائي أو الخطأ[2].

2 ــ جريمة عدم اتخاذ الاحتياطات اللازمة في حماية البيانات المعالجة.

نصّ المشرّع الفرنسي على هذه الجريمة في المادة 226 ــ 17 من قانون العقوبات الفرنسي على أنّ: "كل من أجرى أو حاول إجراء معالجة آلية لمعلومات إسمية، دون اتخاذ التدابير المنصوص عليها في المادة 34 من القانون رقم (78 ــ 17) الصادر في 6 يناير 1978 يعاقب بالحبس خمس سنوات وغرامة تقدر بثلاثمائة (300) ألف أورو" [3].

يتضح من خلال هذه المادة أنه لقيام هذه الجريمة توافر ركنين أولهما مادي والثاني معنوي.

أ ــ الركن المادي:

يتحقّق الركن المادي لهذه الجريمة بإجراء أو محاولة إجراء المعالجة الآلية للبيانات الاسمية دون اتخاذ التدابير المنصوص عليها في المادة 34 من القانون رقم (78 ــ 17) الصادر في 6 يناير 1978، وتتمثل فيما يلي[4]:

ــ في حالة خرق أو اعتداء لأمن البيانات الاسمية سواء بطريق عرضي أو غير قانوني إلى تدمير أو فقدان أو تعديل أو الكشف عنها أو الوصول غير المصرح به للبيانات الاسمية المعالجة في إطار الخدمات الاتصالات الالكترونية العامة.

---

(1)- اعتبرت محكمة النقض الفرنسية الجريمة المنصوص عليها بالمادة 41 من قانون 1978 وهي التي تقابل المادة 226 ــ 16من قانون العقوبات الفرنسي الجديد من الجرائم المادية التي يفترض توافر القصد الجنائي فيها بمجرد ارتكاب الفعل، ولا عبرة بالبواعث. انظر:

Crim 3 décembre 1987, Bull Crim, n°381, J C,P,p 323 .

(2) -Gabriel Roujou de Bouréeet autres, op .cit, p. 416.

(3) – Article 226-17de code pénale francais constitue:"Le fait de procéder ou de faire procéder à un traitement de données à caractèrepersonnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.".

(4) – Alain Bensoussan, le multimédia et le droit, Hermes, 1996, n° 226.

مشار إليه عند: أيمن عبد الله فكري، مرجع سابق، ص 689.

ـــ في حالة عدم تبليغ مزود خدمة الاتصالات الالكترونية اللجنة الوطنية للمعلوماتية والحريات عن الاعتداءات الحاصلة للبيانات الشخصية.

ـــ يلتزم كل مزود خدمة الاتصالات الالكترونية بحفظ قائمة الانتهاكات الحاصلة على البيانات الاسمية، بما في ذلك شروطها وآثارها والتدابير المتخذة ويبقيها تحت تصرف اللجنة.

ب ـــ الركن المعنوي:

يتخذ الركن المعنوي لجريمة عدم اتخاذ الاحتياطات اللازمة في حماية البيانات المعالجة صورة القصد الجنائي أو الخطأ، وعليه تقع الجريمة سواء اتخذ الركن المعنوي صورة القصد الجنائي أو الخطأ.

3 ـــ جريمة المعالجة غير المشروعة للبيانات:

نصّت المادة 226 ـــ 18 من قانون العقوبات الفرنسي على: " كل من قام بجمع البيانات الاسمية بطريق الاحتيال، أو بصورة غير مشروعة يعاقب بالحبس مدة خمس سنوات وغرامة تقدر بثلاثمائة (300) ألف أورو" [1].

يتضح من خلال هذه المادة أنه لقيام هذه الجريمة توافر ركنين مادي وآخر معنوي.

أ ـــ الركن المادي:

يتمثّل الركن المادي في جمع البيانات الاسميّة بطريق الاحتيال أو بصورة غير مشروعة إذا تم الحصول على هذه المعلومات بطريقة لا تخلو من الاحتيال والغش، وذلك ما نصت عليه المادة 25 من القانون رقم (78 ـــ 17) المتعلق بالمعلوماتية والحريات، التي تحظر الحصول على المعلومات بوسائل إحتيالية أو بطرق غير مشروعة، مما يؤدي إلى ترتيب المسؤولية الجنائية للجهة القائمة على الحاسب الآلي[2].

---

[1]-Article 226-18 code pénal francais constitue: ”Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyalou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende”.

[2] - عبد الفتاح بيومي حجازي، مرجع سابق، ص 75.

ب ــ الركن المعنوي:

جريمة المعالجة غير المشروعة للبيانات الاسمية جريمة عمدية، لا بد فيها من توافر القصد الجنائي بعنصريه العلم والارادة، لذلك يجب أن يعلم الجاني بأن فعل جمع البيانات الاسمية بطريق الغش معاقب عليه جنائيا ومع ذلك تنصرف إرادته إلى ارتكاب هذا الفعل، وبالتالي لا تقوم الجريمة إذا كانت المعالجة غير المشروعة ناتجة عن خطأ أو إهمال.

إذا ما توافر الجريمة بركنيها المادي والركن المعنوي، قامت المسؤولية للجاني وهو من يقوم بفعل المعالجة أو يأمر بالقيام بها فكلاهما فاعلا أصليا في الجريمة.

4 ــ جريمة معالجة بيانات إسمية محظورة دون موافقة أصحابها:

تنص المادة 226 ــ 19 على أنه " كل من قام في غير الحالات المستثناة قانونا، بحفظ بيانات إسمية في ذاكرة إلكترونية، دون موافقة صريحة من صاحب البيانات، متى كانت هذه البيانات تظهر بصورة مباشرة أو غير مباشرة الأحوال العرقية، أو الآراء السياسية أو الفلسفية أو الدينية، أو الانتماءات النقابية أو تتعلق بالصحة أو التوجه أو الهوية الجنسية، يعاقب بالحبس مدة خمس (5) سنوات وغرامة تقدر بثلاثمائة (300) ألف أورو" [1].

يتبيّن من خلال نص المادة المبينة أعلاه أنه لقيام هذه الجريمة يجب توافر ركنين أحدهما مادي والثاني معنوي وذلك على النحو التالي:

أ ــ الركن المادي:

يتحقّق الركن المادي لهذه الجريمة بوضع أو حفظ بيانات شخصية محظرورة دون موافقة صريحة من صاحب الشأن وكانت متعلقة بالأصول العرقية أو الآراء السياسية أو الفلسفية

[1] –Article 226-19 de code pénale francais constitue:" Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoireinformatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui,directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques,philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives àla santé ou à l'orientation ou identité sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

أو الدينية، أو الانتماءات النقابية أو تتعلق بالصحة أو التوجه أو الهوية الجنسية[1]. ويرجع السبب في تجريم هذه الأفعال إلى استبعاد أي تمييز يقوم على الأصل العرقي أو الدين أو السياسة مما يخل بمبدأ المساواة، وذلك من أجل حماية الفكر والرأي والعقيدة والانتماء النقابي، فضلا عن أن هذه البيانات تدخل في نطاق الحياة الخاصة، والتي يحظر معالجة البيانات الخاصة بها[2].

ب ــ الركن المعنوي

تعد جريمة معالجة بيانات إسمية محظورة دون موافقة أصحابها من الجرائم العمدية، يتحقق الركن المعنوي فيهاب توافر القصد الجنائي العام بعنصريه العلم والارادة، ولذلك يجب أن يعلم الجاني أنه يعالج بيانات شخصية متعلقة بالمعتقدات الدينية أو الاتجاهات السياسية أو الفلسفية وحتى الصحية دون موافقة صريحة من صاحب الشأن، وأنّه يعلم بأن القانون يحظر ذلك، ومع ذلك تتجه إرادته إلى ارتكاب السلوك الإجرامي. وهذه البيانات تتعلق بالبيانات التي يحظر الغير معالجتها وحتى الاطلاع عليها نظرا لخصوصيتها.

لا عبرة بالباعث والغرض من ارتكاب هذه الجريمة، ولا حتى بالقصد الجنائي الخاص حيث اكتفى المشرع الفرنسي بالقصد الجنائي العام.

5 ــ جريمة حفظ بيانات إسمية خارج المدة المحددة:

نصّت المادة 226 ــ 20 من قانون العقوبات الفرنسي على أنه: "كل من قام من دون موافقة اللجنة الوطنية للمعلوماتية والحريات بحفظ معلومات إسمية ولمدة تجاوز الوقت المحدد في طلب الموافقة أو الإخطار السابق، يعاقب بالحبس مدة خمس (5) سنوات وغرامة تقدر بثلاثمائة (300) ألف أورو، ما لم يتم هذا الحفظ لأغراض تاريخية، أو إحصائية أو علمية ضمن الشروط التي ينص عليها القانون"[3].

---

[1] - كان قانون المعلوماتية والحريات الفرنسي الصادر عام 1978، ينص في المادة (31) منه قبل صدور قانون العقوبات الجديد، على حظر تخزين المعلومات الاسمية التي تتعلق بالأصل العرقي أو الآراء السياسية أو الفلسفية أو الدينية أو الانتماء النقابي للشخص.

[2] ــ عمر أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة، دار النهضة العربية، القاهرة، 2000، ص 112.

[3] -226-20 de code penal: Le fait de conserver des données à caractère personnel au-delà

يتّضح من خلال نص المادة 226 ــ20 من قانون العقوبات الفرنسي أنه يتعين لقيام هذه الجريمة توافر ركنين المادي والمعنوي، على النحو التالي:

أ ــ الركن المادي:

يتحقّق الركن المادي لهذه الجريمة بحفظ البيانات الشخصية خارج المدة المحددة في الطلب أو الإخطار، ودون موافقة اللجنة الوطنية للمعلوماتية والحريات، ذلك أنه من ضوابط تخزين المعلومات الاسمية تأقيت عملية التخزين[1] وهو ما نصت عليه المادة (28) من قانون المعلوماتية والحريات الفرنسي بقولها: "لا يجوز الاحتفاظ بالمعلومات الاسمية إلا للمدة المحددة في طلب إقامة نظم المعلومات أو لمدة تزيد على المدة اللازمة لتحقيق الغرض من تجميع البيانات واحتياجات البرنامج، إلا إذا وافقت اللجنة الوطنية للمعلزماتية والحريات بالإحتفاظ بهذه المعلومات أكثر من المدة المحددة".

بناء على ذلك تقع الجريمة إذا كان حفظ البيانات الاسمية لمدة تجاوز المدة المطلوبة للحفظ، وفي غير الاحوال الاستثنائية التي نص عليها القانون صراحة في المادة 226ــ 20 السابقة الذكر وهي لأغراض تاريخية، أو إحصائية أو علمية فيجوز في هذه الحالات تجاوز المدة المقررة في الطلب أو الاخطار المسبق.

كما يرى البعض أن هذا الاستثناء ينطبق أيضا على البيانات الصحيحة التي يحتفظ بها إلى ما لا نهاية كإسم الشخص، تاريخ ميلاده، واسم والديه[2].

---

de la durée prévue parla loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable addresseeà la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement etde 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiquesou scientifiques dans les conditions prévues par la loi .

(1) -Pierre Sagos et Michel Mass, l'informatique et droit pénal, journée d'études de 15 novembre 1980, CUJAS 1890, P. 19.

(2) -W.JARRAYA, La protection des données personnelles dans le commerce électronique, mémoire pour l'obtention du Master en droit privé, Université de Sfax, Faculté de droit de Sfax, 2004-2005, p. 1. Disponible sur site : http://droitdu.net/fichiers/elloumi_protection_donnees_caractere_personnel_internet**Pdf.**

ب ــ الركن المعنوي:

جريمة حفظ البيانات الاسمية خارج المدة المحددة من الجرائم العمدية، التي يقوم فيها الركن المعنوي على القصد الجنائي العام بعنصريه العلم والارادة، ولا يعاقب على هذا الفعل إذا تم الحفظ عن طريق الخطأ ، فلابد أن يكون الجاني عالما بأنه يحتفظ ببيانات إسمية لمدة تتجاوز الوقت المحدد في طلب الموافقة أو الاخطار السابق، وأن يعلم أيضا أن ذلك الاحتفاظ يتم بغير موافقة اللجنة الوطنية للمعلوماتية والحريات ، وأن الغرض من عملية الحفظ المجاوز للمدة المحددة بما لا ينص عليه القانون، ومع ذلك تنصرف إرادته لهذا الفعل[1] .

6 ــ جريمة تغيير الغرض من المعالجة الآلية للبيانات الإسمية:

نصّت المادة 226 ــ21 من قانون العقوبات الفرنسي على أن" كل من حاز على بيانات إسمية، بمناسبة تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة الآلية، وقام بتغيير الغرض منها المحدد بالقانون، أو اللائحة التنظيمية بالموافقة على المعالجة أو بقرار اللجنة الوطنية للمعلوماتية والحريات، يعاقب بالحبس مدة خمس (5) سنوات وغرامة مالية تقدر بثلاثمائة (300) ألف أورو"[2].

يتبين من خلال نص المادة أنه لقيام هذه الجريمة يشترط توافر ركنيها الأساسيين وهما الركن المادي والركن المعنوي وذلك فيما يلي:

أ ــ الركن المادي:

يتحقّق الركن المادي لهذه الجريمة بتغيير الغرض من المعالجة الآلية للبيانات الاسمية، ذلك أن تسجيل البيانت الشخصية لا بد وأن يكون له هدف أو غرض معين، ويجب الالتزام به دون تغيره

---

(1) -لا يتطلب المشرع الفرنسي توافر القصد الجنائي الخاص، فلاعبرة بالبواعث التي دفعت الجاني إلى ارتكاب فعلا لحفظ غير المشروع للبيانات الشخصية. أسامة قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1998، ص 91.

(2) - Article 226-21 de code penal: "Le fait, par toute personne détentrice de données à caractère personnel à l'occasion deleur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement,de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acteréglementaire ou la decision de la Commission nationale de l'informatique et des libertés autorisant letraitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est punide cinq ans d'emprisonnement et de 300 000 euros d'amende.

فعلى سبيل المثال لا يجوز تغيير الغرض من المعلومات الخاصة بالحالة الصحية، والتي تفيد في التأمين الصحي أو الاجتماعي لغرض الأبحاث الطبية .

المشرّع كان يهدف من تجريمه لهذا الفعل هو منع أي استخدام غير مشروع من قبل حائز البيانات الاسمية، وذلك باستخدامها في غير الغرض الذي خصصت له[1]، ومن تمّ بعث الثّقة في نفوس المتعاملين مع الجهات المعنية التي احتفظت بهذه المعلومات.

حدّد المشرع الفرنسي في المادة 226 ــ 21 معيار الانحراف عن الغرض المحدد للبيانات الاسمية وذلك من خلال الطلب المقدم مسبقا للجنة الوطنية للمعلوماتية والحريات، حيث يحدد فيه غرض معالجة هذه البيانات وذلك بمناسبة تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة.

ب ــ الركن المعنوي:

جريمة تغيير الغرض من المعالجة الآلية للبيانات الاسمية جريمة عمدية، يقوم الركن المعنوي فيها على القصد الجنائي العام، ومن تم لا يعاقب عنها إذا كانت نتيجة خطأ، وبالتالي يتعين على الجاني أن يعلم بأن فعله يشكل إنحرافا عن الغرض من المعالجة الآلية للبيانات الاسمية، وأن إرادته تتجه نحو تحقيق هذا السلوك الإجرامي.

ولا عبرة بالبواعث التي تدفع الجاني لارتكاب هذه الجريمة أو غايته، سواء تمثلت في غنم الجاني، أو دفع ضرر عنه، أو بدافع الانتقام أو تحقيق مصلحة للغير[2] وذلك لغلق باب الإحتجاج من استخدام هذه المعلومات في غير الغرض المحدد لها.

7 ــ جريمة الإفشاء غير المشروع للبيانات الاسمية:

تنص المادة 226 ــ 22 من قانون العقوبات الفرنسي على أنه " كل من تلقى بمناسبة التسجيل أو التصنيف أو النقل أو أي شكل آخر من أشكال معالجة البيانات الإسمية والتي يترتب

[1] ــ عبد الحليم مدحت رمضان، مرجع سابق، ص 103.

[2] ــ صالح شنين، مرجع سابق، ص 195.

على إفشاءها الاعتداء على إعتبار صاحب الشأن أو حرمة حياته الخاصة، عن هذه المعلومات، وقام بنقلها من دون موافقة المعني بها إلى الغير، يعاقب بالحبس مدة خمس (5) سنوات وغرامة مالية تقدر بثلاثمائة (300) يورو. وإذا وقعت الجريمة السابقة نتيجة عدم الاحتياط أو الإهمال تكون العقوبة الحبس مدة ثلاث (3) سنوات وغرامة مالية تقدر بمائة (100) ألف يورو.

لا تحرك الدعوى العمومية وفقا للفقرتين السابقتين إلا من خلال المجني عليه أو ممثله القانوني، أو من له صفة في ذلك"[1].

يتبين من خلال نص المادة أنّ قيام هذه الجريمة يتطلب توافر ركنين المادي والمعنوي وذلك من خلال التالي:

أ ـــ الركن المادي:

يشترط لقيام الركن المادي لجريمة الإفشاء غير المشروع للبيانات الشخصية ضرورة أن تكون هذه البيانات بحيازة مالك النظام أو من له حق السيطرة عليه وتحصل عليها بمناسبة تصنيفها أو نقلها أو علاجها تحت أي شكل من أشكال المعالجة، وأن يكون من شأن إفشاء هذه البيانات الإضرار باعتبار صاحب الشأن (المجني عليه)، أو حرمة حياته الخاصة[2].

كما يجب أن يتم الإفشاء دون رضا صاحب البيانات، لأن ذلك يصبغ عليها صفة التجريم، بعكس الموافقة التي تكون سببا لإباحة فعل الإفشاء للبيانات الاسمية، وأن يتم إفشاء هذه البيانات

---

(1) -Article226-22 de code penal:" Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, deleur classement, de leur transmission ou d'une autre forme de traitement, des données à caractèrepersonnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou àl'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissanced'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 eurosd'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte dela victime, de son représentant légal ou de ses ayants droit"

(2)-Décocg (A), chronique législative, Rev.S.C, 1978, p. 658.

للغير الذي لا يكون له حق الإطلاع عليها. ومثال ذلك قد تسجل بيانات طبية بهدف الاستفادة منها للتأمين الصحي ثم يقوم الجاني(سواء مالك النظام أو من له حق السيطرة عليه) بنقل هذه المعلومات إلى جهة معينة تجري أبحاثا بخصوص أمراض معينة، وذلك بدون موافقة صاحب الشأن، إذن فالغير الذي تحصل على هذه المعلومات لا علاقة له بالبيانات المعالجة، و لم يكن من الأشخاص الذين لهم علاقة بالنظام المعلوماتي التي تمت المعالجة من خلاله.

باعتبار جريمة الإفشاء غير المشروع للبيانات الاسمية تتشابه إلى حد كبير مع جريمة إفشاء الأسرار المهنية والمنصوص عليه في المادة 226 ــ 13 من قانون العقوبات الفرنسي ــ والتي تتضمن تجريم كل كشف للمعلومات السرية من طرف الأشخاص بحكم مهنتهم أو وظيفاهم سواء كانت دائمة أو مؤقتة ــ وذلك من خلال العلة من التجريم وهو حماية الأسرار من الإفشاء ومنع الغير بالإطلاع عليها، إلا أنه في حقيقة الأمر أن كلا الجريمتين تختلف عن بعضهما من حيث الأركان والموضوع[1].

من حيث الأركان: المشرع في جريمة إفشاء الأسرار المهنية والمعاقب عليها بالمادة 226 ــ 13 لا يتطلب لوقوعها أن يحدث إعتداء على الشرف أو الاعتبار أو الحياة الخاصة، بخلاف جريمة إفشاء البيانات الإسمية[2].

أمّا من حيث موضوع الجريمة فجريمة إفشاء الأسرار المهنية تشمل المعلومات السرية فقط والتي يتم العلم بها بمناسبة صفته، في حين جريمة الإفشاء غير المشروع للبيانات الاسمية تشمل البيانات الاسمية السرية وغير السرية[3].

ب ــ الركن المعنوي:

يتمثل الركن المعنوي لجريمة الإفشاء غير المشروع للبيانات الاسمية في صورة القصد الجنائي أو الخطأ، ويستشف ذلك في صريح الفقرة الثانية من المادة 226 ــ22 من قانون العقوبات

[1]-Pierre Sagos et Michel Mass, op.cit., P , 20.

[2]ــ صالح شنين، مرجع سابق، ص 197.

[3] ــ عبد الفتاح بيومي حجازي، مرجع سابق، ص 87.

الفرنسي بنصه: "وإذا وقعت الجريمة السابقة نتيجة عدم الإحتياط أو الإهمال تكون العقوبة الحبس مدة ثلاث سنوات وغرامة مالية تقدر بمائة ألف يورو".

ـــ ويتحقق القصد الجنائي بتوافر عنصريه العلم والإرادة، دون الحاجة إلى القصد الخاص، فيجب أن يعلم الجاني أنه يقوم بتسريب بيانات شخصية تشكل اعتداء على اعتبار أو الحياة الخاصة للأفراد، وأنه يفشيها للغير الذي لا يحق له الاطلاع عليها، ومع ذلك تتجه إرادته للسلوك الاجرامي ويقبل النتيجة المترتبة عليه ويريدها.[1]

ـــ أمّا الركن المعنوي في صورة الخطأ فقد يتحقق إذا كان فعل الإفشاء قد وقع نتيجة عدم إحتياط أو إهمال من طرف الجاني، ومثال ذلك: قيام موظف النظام المعلوماتي في المستشفى بالإفضاء للغير بطريق الخطأ عن معلومات صحية تخص المريض (أ) في حين كان يجب عليه الإفضاء عن معلومات للمريض(ب)، فهنا تقوم المسؤولية الجنائية على أساس الخطأ من قبل الجاني.

تجدر الإشارة أن تحريك الدعوى العمومية في الجريمتين السابقتين، لا تتمّ إلا من خلال المجني عليه أو ممثله القانوني، أو من له صفة في ذلك.

ثانيا ـــ العقوبات المقررة لجرائم الاعتداء على البيانات الشخصية في التشريع الفرنسي:

قرّر المشرع الفرنسي عقوبات على مرتكبي هذه الجرائم وذلك على التفصيل الآتي:

1 ـــ عقوبة الحبس لمدة تلاث سنوات وغرامة مالية تقدر بثلاثمائة (300) ألف أورو لمرتكبي جرائم:

ـــ عدم اتخاذ الإجراءات الأولية لمعالجة البيانات وذلك طبقا للمادة 226 ـــ 26 من قانون العقوبات الفرنسي[2].

---

(1) - Sami FEDAOUI, La protection des données personnelles face aux nouvelles exigences de sécurité, mémoire fin d'étude mastere 2, université de ROUEN, 2007- 2008, p 102. En ligne sur site suivant: http://www.memoireonline.com/10/08/1573/m_la-protection-des-donnees-personnelles-face-aux-nouvelles-exigences-de-securite.html تاريخ الاطلاع: 2017/01/01

(2) - ويرى بعض الفقهاء "kaysserpiterre " أنه لا يقتصر العقاب على هذه الجريمة من ارتكب السلوك الاجرامي المكون للجريمة بل يمتد ليشمل أيضا كل من أمر بإجراء المعالجة كفاعل أصلي في الجريمة حسب القواعد العامة في القانون الجنائي لمسؤولية الفاعل. انظر: عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الحماية الجنائية لنظام التجارة الالكترونية، الكتاب الثاني، دار الفكر الجامعي، 2002 ، ص 73.

ـــ ونفس العقوبة قررتها المادة 226 ـــ17 من قانون العقوبات الفرنسي في جريمة عدم اتخاذ الاحتياطات اللازمة في حماية البيانات المعالجة.

ـــ أما بالنسبة لجريمة المعالجة غيرالمشروعة للبيانات فيعاقب المشرع الفرنسي بذات العقوبة السابقة الذكر، وهو ما قررته المادة 226 ـــ 18 من قانون العقوبات الفرنسي.

ـــ وهي العقوبة ذاتها قررتها المادة 226 ـــ20 من قانون العقوبات الفرنسي لجريمة حفظ بيانات إسمية خارج المدة المحددة.

2 ـــ عقوبة السجن لمدة خمس (5) سنوات وغرامة تقدر بثلاثمائة (300) ألف أورو حسب المادة المادة 226 ـــ19 من قانون العقوبات الفرنسي كل من قام بمعالجة بيانات إسمية دون موافقة صاحبها وكانت متعلقة بالأصول العرقية والدينية أو بالأحوال الصحية أو الهوية الجنسية.

ـــ أمّا المادة 226 ـــ21 من قانون العقوبات الفرنسي يعاقب المشرع الفرنسي كل من يرتكب جريمة تغيير الغرض من المعالجة الآلية للبيانات الاسمية، بنفس العقوبة السالفة الذكر.

ـــ أمّا بالنسبة لجريمة الإفشاء غير المشروع للبيانات الاسمية، وطبقا لنص المادة 226 ـــ 22 من قانون العقوبات الفرنسي، فقد شدّد المشرع الفرنسي العقوبة على هذه الجريمة في صورته العمدية، حيث عاقب عليها بالسجن خمس (5) سنوات وغرامة مالية تقدر بثلاثمائة (300) ألف أورو، أمّا إذا ارتكبت هذه الجريمة في صورة الخطأ نتيجة عدم إحتياط أو إهمال، فيعاقب المشرع عليها بالحبس ثلاث سنوات وغرامة تقدر بمائة (100) ألف أورو.

بعد عرض هذه العقوبات نلاحظ أنّ المشرع الفرنسي قد أدرك خطورة الإستعانة بالتقنيات المعلوماتية في العمل الحكومي أو على مستوى الخاص، وأثار ذلك في التعدي على البيانات الاسمية، التي أصبحت مصدر قلق لدى أصحابها، لذلك شدد العقوبات لمرتكبي هذه الجرائم وجعلها ردعية بدرجة أولى تتراوح بين ثلاث إلى خمس سنوات، و خاصة العقوبات المالية.

الفرع الثاني: الحماية الجنائية للبيانات الشخصية في التشريع الجزائري

لم يقنن المشرع الجزائري بعد تشريع خاص يهدف إلى حماية البيانات الشخصية تحديدا، رغم أن دستورها أكد على حرمة كل ما يتعلق بالحياة الخاصة وعلى ضمانتها الموكلة إلى الدولة[1].

ومع ذلك نلاحظ من خلال العديد من النصوص القانونية حماية البيانات الشحصية، من خلال تجريم الاعتداء على نظام المعالجة الآلية للمعطيات، وذلك من خلال التعديل الذي أدخله على قانون العقوبات بمقتضى القانون رقم (04ـــ15) المؤرخ في 10 نوفمبر2004[2]، وأيضا القانون رقم(06ـــ23) المؤرخ في 20 ديسمبر 2006[3]، وأخيرا من خلال تجريم الاعتداء على التوقيع الالكتروني بموجب القانون رقم (15ـــ 04) المؤرخ في أول فبراير 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين[4].

وفيما يلي عرض تفصيلي لمختلف النصوص التجريمية:

أولاـــ حماية البيانات الشخصية من خلال حماية نظام المعالجة الآلية للمعطيات:

تأثرت الجزائر على غرار الدول الأخرى بما أفرزته الثورة المعلوماتية، ممّا دفع المشرع الجزائري إلى تعديل قانون العقوبات وذلك لمواجهة الاشكال المستحدثة من الاجرام، وكان بموجب القانون رقم (04 ـــ 15) المؤرخ في العاشر من نوفمبر عام 2004 المتمم للأمر رقم (66 ـــ 156) المتضمن قانون العقوبات، والذي أفرد القسم " السابع مكرر" منه تحت عنوان: **"المساس بأنظمة المعالجة الآلية للمعطيات"**، والذي تضمن ثمانية مواد (من المادة 394 مكرر وحتى المادة 394 مكرر7) ونص على عدة جرائم هي[5]:

---

[1] ـــ المادة 23 و39 و40 من دستور 1996 الجزائري المعدل بموجب القانون 08 ـــ 19 المؤرخ في 15 نوفمبر 2008.

[2] ـــ قانون رقم (04 ـــ 15) مؤرخ في 27 رمضان عام 1425 الموافق لـــ 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66 ـــ 156 المؤرخ في 18 صفر عام 1386الموافق لـــ 8 يونيو 1966 والمتضمن قانون العقوبات الجزائري، ج.ر عدد 71 لسنة 2004.

[3] ـــ قانون رقم (06 ـــ23) مؤرخ في 29 ذي القعدة عام 1427 الموافق لـــ 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66 ـــ 156 المؤرخ في 18 صفر عام 1386الموافق لـــ 8 يونيو 1966 والمتضمن قانون العقوبات الجزائري، ج.ر عدد 84 لسنة 2006.

[4] ـــ قانون رقم (15 ـــ 04) مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج. ر ع 06 لسنة 2015.

[5] ـــ تفاديا لتكرار هذه الجرائم انظر في تفاصيل أركانها ص 14 وما بعدها.

ـــ الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك (المادة 394 مكررف1)، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة (المادة 394 مكرر فقرة 2).

ـــ الدخول أو البقاء المؤدي إلى تخريب نظام تشغيل المنظومة (المادة394 مكرر فقرة 3).

ـــ إدخال أو إزالة أو تعديل ـــ بطريق الغش ـــ معطيات في نظام المعالجة الآلية (المادة395 مكرر1).

ـــ تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أومراسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم(م394 مكرر2).

ـــ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم (م 394 مكرر2).

تجدر الإشارة أن هذا التعديل لم يورد صراحة ذكر الحياة الخاصة، فمن خلال استقراء نصوص التجريم السابقة الذكر، وأن المتابعة الجزائية في هذا الشأن لا تتم بمناسبة تجريم المساس بالحياة الخاصة للأشخاص، بل استنادا على قاعدة المادة 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري، بجنحة المساس بأنظمة المعالجة الآلية للمعطيلت التي تتحق بمجرد المساس سواء كانت تلك المعطيات تتصف بصفة الخصوصية أم لا، فالجنحة تقوم بمجرد إتيان أحد الأفعال المحددة بنصوص المواد السالفة الذكر.

وعليه فإن ممارسة الشخص لخصوصياته من خلال تلك المعطيات محمية بشكل غير مباشر من خلال حماية أنظمة المعالجة الآلية لتلك المعطيات.

ثانيا ـــ حماية البيانات الشخصية من خلال القانون رقم (06ـــ23) المعدل لقانون العقوبات الجزائري:

قرّر المشرع الجزائري حماية جزائية خاصة[1] للبيانات الإسمية من خلال التعديل الذي أدخله على قانون العقوبات، وذلك بموجب القانون رقم (06ـــ23) المؤرخ في 20 ديسمبر 2006،

[1] - هذه الحماية الخاصة للبيانات الشخصية ليست بالحماية الجزائية لهذه البيانات كونها لا تتضمن كل الجرائم الماسة بالبيانات الشخصية مثلها مثل التشريع الفرنسي أو حتى التشريع المغربي من خلال القانون رقم 09 ـــ 08 المتعلق بحماية الأشخاص الداتيين تجاه معالجة المعطيات

وذلك في القسم الخامس من الفصل الأول من الباب الثاني في الكتاب الثالث منه تحت عنوان "الإعتداءات على شرف إعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار"، وذلك في المواد من 303 مكرر إلى المادة 303 مكرر3 [1].

التعرض لهذه الحماية وفقا لما قرره المشرع العقابي يكون على النحو التالي:

1 ــ جريمة إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة:

حرص المشرع الجزائري على حماية الحياة الخاص للأشخاص ضد وسائل التجسس عليها ومحاولة كشفها، وذلك من خلال نص المادة 303 مكرر فقرة أولى رقم 1 بنصها: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة للأشخاص بأي تقنية كانت وذلك:

1 ــ بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه".

بالرجوع إلى نص المادة 303 مكرر من قانون العقوبات يمكن تحديد الأركان الواجب توافرها في هذه الجريمة، وهي كالتالي:

أ ــ الركن المادي:

يتحقق الركن المادي لهذه الجريمة بإحدى صور النشاط الإجرامي بالتنصت عن طريق التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاص أو سرّية، من دون موافقة صاحب الشأن، وبأي وسيلة كانت.

لقيام هذه الجريمة لا بد من توافر شروط معينة تتمثل في[2]:

ذات االطابع الشخصي ، بل تتضمن هذه الحماية بعض الجرائم الماسة بالحياة الخاصة والتي من الممكن ان ترتكب وسائل التقنية وتقع على حرمة شرف واعتبار الأشخاص وحياتهم الخاصة.

[1] - هذه الحماية الخاصة للبيانات الشخصية ليست بالحماية الجزائية لهذه البيانات كونها لا تتضمن كل الجرائم الماسة بالبيانات الشخصية مثلها مثل التشريع الفرنسي أو حتى التشريع المغربي من خلال القانون رقم 09 ــ 08 المتعلق بحماية الأشخاص الداتيين تجاه معالجة المعطيات ذات االطابع الشخصي ، بل تتضمن هذه الحماية بعض الجرائم الماسة بالحياة الخاصة والتي من الممكن ان ترتكب وسائل التقنية وتقع على حرمة شرف واعتبار الأشخاص وحياتهم الخاصة.

[2] - بن ذياب عبد المالك، حق الخصوصية في التشريع العقابي الجزائري، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013، ص 238.

1 ــ القيام بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث: جرم المشرع الجزائري التنصت وتسجيل الأحاديث الصادرة بين شخصين أو بين الشخص ونفسه.

ويقصد بالتنصت أو الالتقاط (captation) الاستماع سرا إلى كلام له صفة الخصوصية أو السرية صادر من شخص ما أو متبادل بين شخصين أو أكثر دون رضاه، وبمجرد الاستماع يتحقق الركن المادي للجريمة، ولا يشترط تسجيله أو نقله أو وضعه في دعامة إلكترونية أو غيرها.

أما التسجيل (enregistrement) فهو حفظ الحديث على جهاز أو أي وسيلة أخرى معدة لذلك بقصد الاستماع إليه فيما بعد.

أما النقل(transmition)، فيقصد به نقل الحديث الذي تم الاستماع إليه أو تسجيله من المكان الذي يتم فيه الاستماع أو التسجيل إلى مكان آخر[1].

ويمكن أن يقوم شخص واحد وهو الجاني بهذا الاعتداء في صوره الثلاث (الالتقاط، التسجيل والنقل)، كما يمكن أن يقوم بها أكثر من شخص واحد معتدي، وفي هذه الحالة تكون المسؤولية على كل واحد منهم منفصلا عن الآخر.

2 ــ أن تكون هذه المكالمات أو المحادثات خاصة أو سرية: أخذ المشرع الجزائري بالمعيار الشخصي المتعلق بخصوصية وسرية الحديث أو المكالمة، فالعبرة ليست بطبيعة المكان بل بطبيعة الحديث موضوع الجريمة، فمتى كان الحديث خاصا يحتوي على أسرار، تقوم الجريمة بصرف النظر عن المكان الذي الذي يتم فيها إجراء الحديث، سواء كان عام أو خاص[2].

3 ــ أن يستخدم في ذلك أي أسلوب كان (أية تقنية): لم يحدد المشرع وسيلة بذاتها، بل استعمل عبارة "بأية تقنية كانت"، ما يعني اتساع نطاق استعمال أية أجهزة قد تظهر في المستقبل وهو ما يعكس مسايرة المشرع للتطور العلمي في مجال الاتصالات.

---

[1] ــ آدم عبد العبيد حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة الأزهر، دار المتحدة للطباعة، مصر، 2000، ص 538.

[2] - بن ذياب عبد المالك، مرجع سابق، ص 97 .

4 ــ عدم رضا الضحية: يشترط لتجريم فعل الإلتقاط أو التسجيل أو النقل المكالمات أو الأحاديث الخاصة أن تتم من دون رضا صاحب الشأن، لأن رضا المجني عليه يبيح الفعل المجرم الذي ينفي قيام هذه الجنحة.

ب ــ الركن المعنوي:

تعتبر جريمة إلتقاط أو تسجيل أو نقل المكالمات أو الأحاديث الخاصة أو السرية من الجرائم العمدية، فلا تقوم عن طريق الخطأ غير العمدي أو الإهمال، وهذا ما يتجلى بصريح عبارات المادة 303 مكرر التي جاءت في فقرتها الأولى أنّ:"كل من تعمّد المساس بحرمة الحياة الخاصة للأشخاص..."، ويجب أن يتوافر القصد الجنائي بعنصريه العلم والإرادة[1].

يجب أن يعلم الجاني أن هذا الفعل لا يسمح به القانون، وأنه بإتيانه يكون معتديا على حرمة الحياة الخاصة للغير، ومع ذلك تتجه إرادته إلى ارتكاب هذا الفعل المجرم[2].

ج ــ العقوبة:

قرّر المشرّع العقابي في المادة 303 مكرر فقرة أولى عقوبة أصلية لمن يرتكب هذه الجنحة تتراوح بين ستة (6) أشهر إلى ثلاث سنوات وغرامة مالية من 50.000 دج إلى 300.000 دج، هذا متى كان الجاني شخصا عاديا.

كما قرّرت المادة 303 مكر 2 من قانون العقوبات جواز توقيع عقوبة تكميلية وهي منع المحكوم عليه من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 من القانون

(1) -Merle (R) et Vitu (A), traité de droit criminel, droit pénal, T2 , p. 231.

(2) ــ فلو كان شخص في مكالمة هاتفية مع أحد أقاربه وفجأة تداخلت مكالمة أخرى بسبب خلل فني في الإتصالات، وتمكن هذا الشخص من استراق السمع لما يجري في المكالمة التي تداخلت مع مكالمته، فلا مجال لقيام وتبوث الجريمة في جانبه لأنه لم يقصد القيام بهذا الفعل.

نفسه[1]، وذلك لمدة لا تتجاوز خمس (5) سنوات، كما يجوز للمحكمة أن تأمر بنشر حكم الإدانة، طبقا للكيفيات المبينة في المادة 18 من قانون العقوبات[2].

كما لا يفلت الشخص المعنوي من المسؤولية الجزائية إذا ارتكبت الفعل المنصوص عليه في المادة 303 مكرر وذلك وفقا لما نصت عليه المادة 51 مكرر. إلا أنّ مسؤولية هذا الأخير، لا تمنع من مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في الأفعال نفسها[3].

2 ــ جريمة إلتقاط أو تسجيل أو نقل الصورة:

نصّت على هذه الجنحة المادة 303 مكرر نقطة 2 من قانون العقوبات على أنه: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت، وذلك:

بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه".

وبالرجوع إلى هذا النص يتبين لقيام هذه الجريمة ضرورة توافر الركنين، المادي والمعنوي فضلا عن الجزاء المقرر لها وذلك من خلال ما يأتي:

أ ــ الركن المادي:

إعمالا لنص المادة 303 مكرر من قانون العقوبات، فإن الركن المادي لجريمة إلتقاط أو تسجيل أو نقل صورة شخص في مكان خاص، يتحقق من خلال قيام المتهم بالنشاط الإجرامي الذي يتخذ صورة من الصور الثلاث المبينة بهذا النص وهي: الالتقاط أو التسجيل أو النقل لصورة

---

[1] ــ إذ تنص الفقرة الأولى من المادة 9 مكرر على أنه:" يتمثل الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية في: 1 ــ العزل أو الإقصاد من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة، 2 ــ الحرمان من حق الانتخاب أو الترشح ومن حمل أي وسام، 3ــ عدم الأهلية لأن يكون مساعدا محلفا، أو خبيرا، أو شاهدا على أي عقد، أو شاهدا أما القضاء إلا على سبيل الاستدلال، 4 ــ الحرمان من الحق في حمل الأسلحة، وفي التدريس، وفي إدارة مدرسة للتعليم بوصفه أستاذا أو مدرسا أو مراقبا، 5 ــ عدم الأهلية لأن يكون وصيا أو قيما، 6 ــ سقوط حقوق الولاية كلها أو بعضها".

[2] ــ وتنص الفقرة الأولى من المادة 18 من قانون العقوبات على أنه : " للمحكمة عند الحكم بالإدانة أن تأمر في الحالات التي يحددها القانون بنشر الحكم بأكمله أو مستخرج منه في جريدة أو أكثر بعينها، أو بتعليقه في الأماكن التي يبينها، وذلك كله على نفقة المحكوم عليه، على ألا تتجاوز مصاريف النشر المبلغ الذي يحدده الحكم بالإدانة لهذا الغرض وألا تتجاوز مدة التعليق شهرا واحد".

[3] ــ المادة 51 مكرر من قانون العقوبات الجزائري (المستحدثة بالقانون رقم 04 ــ 15 المؤرخ في 2004/11/10) فقرة 2 منها.

شخص يتواجد في مكان خاص من دون رضاه، وذلك بأي تقنية كانت، الأمر الذي يجعل من الركن المادي يتكون من أربعة عناصر وهي:

1 ــ نشاط إجرامي يتخذ صورة التقاط أو التسجيل أو نقل الصورة: التقاط الصورة يعني أخذها لشخص أو لعدة أشخاص، وتعتبر الجنحة قد تحققت كاملة بمجرد إلتقاط الصورة، ولو لم يواصل المعتدي في تجسيد الصورة وإظهارها إلى العالم الخارجي.

أما تسجيل الصورة، هو تثبيت الصورة ، وهذه العملية تحدث في الأجهزة الأكثر تطورا من آلة التصوير العادية كالكاميرا والهاتف النقال والحاسب الألي، وهنا تزداد خطورة هذه التقنيات من حيث الاعتداء على حرمة الحياة الخاصة للأشخاص.

ونقل الصورة فهو تحويلها وإرسالها من موضع لآخر بغرض تمكين شخص موجود في مكان مختلف عن المكان الذي يوجد فيه المعتدي على حرمة حياته الخاصة بواسطة الصورة.

2 ــ وسيلة ارتكاب الفعل الإجرامي: لم يحدد المشرع الجزائري في قانون العقوبات وسيلة معينة يرتكب بها الجاني هذه الجنحة، إذ نص في الفقرة الأولى من المادة 303 مكرر منه على "...أية تقنية كانت..."، وعليه أي أسلوب يؤدي إلى التقاط أو تسجيل أو نقل صورة شخص يحقق الجنحة، وذلك بدءا من آلة تصوير إلى أكثر الوسائل تقدما تكنولوجيا.

3 ــ ارتكاب الجريمة في مكان خاص: على عكس جريمة التقط أو تسجيل أو نقل المكالمات أو الأحاديث، فقد اشترط المشرع لقيام جريمة التقاط أو تسجيل أو نقل صورة شخص، أن يتم هذا الفعل في مكان خاص.

3 ــ ارتكاب الجريمة من دون رضا المجني عليه: بشترط لقيام هذا الفعل هو عدم رضا المجني عليه، فإذا تخلفت المعارضة لا تقوم الجريمة ويصبح الفعل مشروعا[1].

ب ــ الركن المعنوي:

تعتبر جريمة التقاط أو تسجيل أو نقل صورة شخص في مكان خاص من الجرائم العمدية، فلا تقوم عن طريق الخطأ غير العمدي أو الاهمال، فيتحقق ركنها المعنوي بتوافر القصد الجنائي بعنصريه

[1] - صفية بشاتن، الحماية القانونية للحياة الخاصة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص 412.

العلم والإرادة، فلا بد أن يكون الفاعل عالما بأن ما عمد على إيتانه من أحد الأفعال المحددة في المادة 303 مكرر من قانون العقوبات المشكلة لعناصر النشاط الاجرامي من التقاط أو تسجيل أو نقل صورة الشخص في مكان خاص من دون رضاه، فضلا على توجه إرادته الحرة إلى القيام بتلك الأفعال من دون رضاء صاحب الصورة[1].

ج ــ العقوبة:

قرّر المشرع العقابي لهذه الجنحة عقوبة الحبس من ستة أشهر إلى ثلاث سنوات، وغرامة مالية تتراوح بين 50.000 دج و 300.000 دج كعقوبة أصلية وردت في المادة 303 مكرر من قانون العقوبات.

ــ كما أنّ الشروع في ارتكاب هذه الجنحة الواردة في هذه المادة، يعاقب عليها بنفس العقوبات المقررة للجنحة التامة.

كما أجازت المادة 303 مكرر 2 فقرة 1 من قانون العقوبات، أنه للمحكمة أن تحظر على المحكوم عليه من أجل هذه جريمة التقاط أو تسجيل أو نقل صورة لشخص ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر لمدة لا تتجاوز 5 سنوات، كما يجوز لها أن تأمر بنشر حكم الإدانة طلقا للكيفيات المبينة في المادة 18 من قانون العقوبات.

كما يتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب هذه الجريمة، وذلك وفق ما نصت عليه المادة 303 مكرر 2 فقرة 2.

ــ كذلك يكون الشخص المعنوي مسؤولا جزائيا عن ارتكابه هذه الجنحة وذلك طبقا للشروط المنصوص عليها في المادة 51 مكرر سالفة الذكر. وتطبق عليه عقوبة الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر، وفي المادة 18 مكرر2 عند الإقتضاء، كما يتعرض لأحدى العقوبات التكميلية المنصوص عليها في المادة 18 مكرر السابقة الذكر.

---

[1] - آدم عبد العبيد حسين، مرجع سابق، ص 550 .

3 ــ جريمة الاحتفاظ، نشر واستخدام التسجيل أو الصور أو الوثائق:

بعد ارتكاب المعتدي لإحدى الجنحتين المنصوص عليهما في المادة 303 مكرر، لا يتصور الاحتفاظ بموضوعهما احتفاظا سلبيا، وإنما كان ذلك بغرض استعمالها بطرق غير مشروعة ولأجل ذلك جرم المشرع الجزائري كل احتفاظ أو نشر أو استخدام التسجيل أو الصورة المتحصل عليها بإحدى طرق انتهاك حرمة الحياة الخاصة من خلال عليها المادة 303 مكرر 1 في فقراها الأولى من قانون العقوبات.

بناء على ذلك يمكن تحديد الأركان الواجب توافرها في الجريمة المنصوص عليها في المادة 303 مكرر 1 من قانون العقوبات، وهي الركن المادي والمعنوي بالاضاف إلى تحديد العقوبة المقررة لها وذلك في ما يلي:

أ ــ الركن المادي:

يتحقق الركن المادي لهذه الجريمة بالاحتفاظ أو الوضع أو السماح بالوضع في متناول الجمهور أو الغير ــ بما يفيد الإعلان ــ أو استعمال تسجيل أو وثائق متحصل عليها بإحدى الطرق المبينة في المادة 303 مكرر من قانون العقوبات، ومن تم تكون عناصر هذا الركن كما يلي:

1 . نشاط إجرامي يتخذ صورة الاحتفاظ أو الإعلان أو تسهيل الإعلان أو الاستعمال: يتحقق هذا النشاط الإجرامي من خلال إتيان الفاعل إحدى الصور الأربعة المنصوص عليها بالمادة 303 مكرر 1 من قانون العقوباتوهي: الاحتفاظ، أو الوضع في متناول الجمهور أو الغير، أو السماح بالوضع في متناولهم أو الاستخدام.

يقصد **بالاحتفاظ:** إمساك الجاني لتسجيل أو صورة أو مستند خاص بشخص أو أشخاص آخرين عن قصد، مع علمه بمحتوى التسجيل أو المستند، مع ضرورة أن يكون قد تم الحصول على التسجيل أو الصورة أو الوثيقة عن طريق الالتقاط أو التسجيل أو النقل للمكالمات أو الأحاديث الخاصة أو السرية أو لصورة المجني عليه في مكان خاص[1].

[1] ــ بن ذياب عبد المالك، مرجع سابق، ص 127.

أمّا **الوضع في متناول الجمهور أو الغير**: فيقصد به إعلان الغير عن محتوى التسجيل أو الصورة أو الوثيقة، بأي وسيلة كانت.

السماح بالوضع في متناول الجمهور أو الغير: يتخذ هذا السلوك مظهرا سلبيا بعدم الاعتراض على النشر والإذاعة للصور أو المكالمات والمحادثات الخاصة، كما يتخذ أيضا مظهرا إيجابيا من خلال تسليم وتقديم جسم الجريمة لغرض الإعلان عنه أو تسهيل ذلك[1].

تتجسد الصورة الرابعة في **فعل الاستعمل،** ويتمثل في استخدام التسجيل أو الوثيقة لتحقيق غرض ما، أي النشاط الذي يسعى الجاني من خلاله إلى تحقيق الغاية التي يرغب فيها. ويشترط لقيام هذا الاستخدام شرطين، أولهما أن تتوافر صفة إرادية، وثانيهما أنه يلزم إبراز التسجيل أو الصورة أو المستند.

2 . موضوع النشاط الاجرامي يتمثل في التسجيل أو الصور أو الوثيقة المتحصل عليها بإحدى الطرق المبينة في المادة 303 مكرر من قانون العقوبات.

ب ــ الركن المعنوي:

تعتبر الجريمة المنصوص والمعاقب عليها بالمادة 303 مكرر 1 من قانون العقوبات جريمة عمدية، يتطلب لقيامها توافر القصد الجنائي بتوافر عنصري العلم والإرادة.

فيجب أن يعلم الجاني بمصدر الحصول على التسجيل أو الصورة أو الوثيقة، وأنه يقوم بالاحتفاظ به أو وضعه أو السماح بوضعه في متناول الجمهور أو الغير أو استخدامه، كما ينبغي أن تتجه إرادته إلى إتيان الأفعال المادية للجريمة بالاحتفاظ أو الوضع أو السماع بالوضع في متناول الجمهور أو الغير أو الاستخدام للتسجيل أو الصورة أو المستند موضوع الجريمة.

ولا يعتد بالباعث في اكتمال عناصر القصد الجنائي، سواء كان بغرض التشهير أو الحصول على منفعة مادية أو معنوية.

---

[1] ــ هشام محمد فريد رستم، الحماية الجنائية لحق الانسان في صورته، مكتبة الآلات الحديثة، أسيوط، د. س. ن، ص 103.

ج ــ العقوبة:

تعاقب المادة 303 مكرر 1 على جريمة الاحتفاظ أو الوضع أو السماح بالوضع في متناول الجمهور أو الغير أو استخدام التسجيل أو الصورة أو الوثيقة بالعقوبات الواردة بالمادة 303 مكرر، كما يجوز للمحكمة أن تحظر على المحوم علي مما يجعل هذه الجريمة تخضع للعقوبات الواردة بالمواد: 303 مكرر و303 مكرر 1 و303 مكرر 2 من قانون العقوبات بالنسبة للفاعل كشخص طبيعي، وبالمواد: 303 مكرر 3 إذا كان الفاعل شخصا معنويا.

وعندما ترتكب الجريمة عن طريق الصحافة فتخضع للجرائم المحددة في قانون الإعلام وذلك بالرجوع إلى القانون العضوي رقم 12 ــ 05 المؤرخ في 12 يناير سنة 2012 المتعلق بالإعلام، لاسيما المادة 115 منه المتعلقة بالمسؤولية[1].

كما يعاقب على الشروع في ارتكاب هذه الجريمة سواء من الشخص الطبيعي أو من الشخص المعنوي، بناء على نص الفقرة الثانية من المادة 303 مكرر 1 من قانون العقوبات بالعقوبات ذاتها المقررة للجريمة التامة.

ثالثا ــ حماية البيانات الشخصية من خلال تجريم الاعتداء على التوقيع الالكتروني:

قرّر المشرع الجزائري حماية البيانات الشخصية من خلال جرائم الاعتداء على التوقيع الالكتروني وذلك بموجب القانون رقم (15ــ04) المؤرخ في أول فبراير 2015، المحدد للقواعد العامة للتصديق والتوقيع الالكتروني السابق الذكر، حيث خصص الفصل الثاني من الباب الرابع منه للأحكام الجزائية، وقد جرم من خلاله عدة أفعال تمثل إعتداء على التوقيع الالكتروني من بينها جرائم الاعتداء على البيانات الشخصية وذلك في المادتين 70 و71 من هذا القانون. وفيما يلي شرح لهذه الجرائم:

---

(1) - تنص المادة 115 من القانون العضوي رقم 12 ــ 05 المؤرخ في 12 يناير سنة 2012 المتعلق بالإعلام، مايلي:

"يتحمل المدير مسؤول النشرية أو مدير جهاز الصحافة الالكتروني، وكذا صاحب الكتاب أو الرسم مسؤولية كل كتابة أو رسم يتم نشرهما من طرف نشرية دورية أو صحافة إلكترونية.

ويتحمل مدير خدمة الاتصال السمعي البصري أو عبر الانترنت وصاحب الخبر الذي تم بثه من قبل خدمة الاتصال السمعي البصري أو عبر الانترنت"، القانون العضوي رقم 12 ــ 05 المؤرخ في 12 يناير سنة 2012، يتعلق بالإعلام، ج.ر، ع02، الصادرة قي 15 يناير 2012.

1 ــ جريمة إفشاء البيانات الشخصية:

نصّت عليها المادة 70 من القانون (15 ــ 04) المحدد للقواعد العامة للتصديق والتوقيع الالكتروني، بقولها " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق أخل بأحكام المادة 42 من هذا القانون".

ويتضح من خلال هذا النص أنه لقيام جريمة إفشاء البيانات الشخصية توافر ركنين أحدهما مادي والآخر معنوي، فضلا عن تحديد الجزاء المقرر لهذه الجريمة وذلك على التفصيل الآتي:

أ ــ الركن المادي:

يتمثل الركن المادي لهذه لجريمة في الإخلال بأحكام المادة 42 من القانون رقم (15 ــ04) المتعلق بتحديد القواعد العامة للتصديق والتوقيع الالكتروني، وبالرجوع إلى نص المادة 42 السالفة الذكر[1] نجد أن المشرع يلزم مؤدي خدمات التصديق الالكتروني بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكترونية الممنوحة".

يقصد بشهادة التصديق الالكتروني حسب الفقرة السابعة (7) من المادة الثانية (2) من القانون السابق الذكر، أنها " وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع" ، فهذه الشهادة تمنح من قبل طرف ثالث موثوق أو مؤدي خدمات تصديق إلكتروني، وتمنح للموقع دون سواه، وتتضمن على بيانات خاصة لهذا الأخير (الموقع) كإسمه أو الاسم المستعار الذي يسمح بتحديد هويته، رمز تعريف شهادة التصديق الالكتروني، فضلا عن بعض المعلومات الخاصة بالوثيقة ذاتها كحدود استعمال هذه الشهادة، وقيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الالكتروني، كما تشير إلى تمثيل شخص طبيعي أو معنوي آخر عند الاقتضاء وهذا ما حددته المادة 15 من القانون رقم (15 ــ 04) .

---

[1] ــ تنص المادة 42 من قانون التصديق والتوقيع الالكتروني رقم (15 ــ 04) أنه: "يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكترونية الممنوحة".

فكل إفشاء للبيانات والمعلومات الخاصة بشهادة التصديق الالكترونية من قبل مزودي خدمات التصديق الالكتروني يشكل ركنا ماديا لجريمة الافشاء غير المشروع لمزودي خدمات التصديق.

ب ــ الركن المعنوي:

يأخذ الركن المعنوي لجريمة الإفشاء غير المشروع للبيانات والمتعلقة بشهادة التصديق الالكترونية صورة العمد بتوافر القصد الجنائي العام الذي يقوم يتوافر العلم والإرادة، يتعين أن يكون الجاني (مزودي خدمات التصديق الالكتروني) ملزما بالحفاظ على البيانات الخاصة بشهادة التصديق الالكترونية ومع ذلك يقوم بإفشاءها، وأن تتجه إرادته نحو هذا السلوك غير المشروع.

ج ــ العقوبة:

قرّر المشرع الجزائري من خلال المادة 70 من القانون (15 ــ 04) المحدد للقواعد العامة للتصديق والتوقيع الالكتروني، عقوبة أصلية للشخص الطبيعي تتمثل في الحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط.

أما بالنسبة للشخص المعنوي وطبقا للمادة 75 من نفس القانون يعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، بمعنى يعاقب على هذه الجريمة بغرامة تقدر بـــ: خمس ملايين دينار (5.000.000 دج).

2 ــ جريمة الجمع غير المشروع للبيانات الشخصية:

تنص المادة 71 يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة 43 من هذا القانون".

لقيام هذه الجريمة لابد من توافر ركنين مادي ومعنوي على النحو الآتي:

أ ــ الركن المادي:

طبقا للفقرة الأولى من المادة 43 من القانون الخاص بالتصديق والتوقيع الالكتروني: "لا يمكن مؤدي خدمات التصديق الالكتروني جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة".

يتحقق الركن المادي لهذه الجريمة بجمع البيانات الشخصية من قبل مزودي خدمات التصديق الالكتروني للمعني وبغير موافقته الصريحة . ونظرا لحساسية هذه البيانات الخاصة اشترط المشرع موافقة صريحة من المعني سواء كانت شفهية أو كتابية المهم أن تكون صريحة، وغير ضمنية.

ب ــ الركن المعنوي:

يتخذ الركن المعنوي لهذه الجريمة في صورة القصد الجنائي العام بعلم الجاني (مزودي خدمات التصديق الالكتروني) بالصفة الشخصية للبيانات المراد جمعها، وأن يعلم أيضا بجمع بيانات شخصية دون الحصول على موافقة صريحة من صاحب الشهادة المعني، ويتعين أيضا أن تتجه إرادته إلى إجراء هذا الجمع غير المشروع للبيانات الشخصية.

ولم يتطلب المشرع الجزائري القصد الجنائي الخاص، ولا عبرة بالباعث من ارتكاب هذه الجريمة.

ج ــ العقوبة:

يعاقب المشرع الجزائري على جريمة الجمع غير المشروع للبيانات الشخصية من قبل مزودي خدمات التصديق الالكتروني بعقوبة أصلية تتمثل في الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، هذا إذا كان الجاني شخص طبيعي، أما إذا كان شخص معنوي فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، بمعنى يعاقب على هذه الجريمة بغرامة تقدر بـــ: خمسة ملايين دينار (5.000.000 دج) وذلك طبقا للمادة 75 من نفس القانون.

3 ــ جريمة استعمال البيانات الشخصية لغير الغرض المحدد له:

نصت على هذه الجريمة المادة 71 من القانون رقم (15 ــ04) المتضمن القواعد العامة للتصديق والتوقيع الالكتروني.

لقيام هذه الجريمة يشترط توافر ركنيها الأساسين، المادي والمعنوي، بالاضافة إلى تحديد العقوبة المقررة لها وذلك في التفصيل التالي:

أ ــ الركن المادي:

بالرجوع إلى نص المادة 71 من القانون السابق الذكر نلاحظ أنها تحيل إلى الفقرة الثانية من المادة 43 من نفس القانون وذلك من خلال الاخلال بأحكامها، حيث تنص هذه المادة الأخيرة بأنه: "ولا يمكن مؤدي خدمات التصديق الالكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الالكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى".

يتحقق الركن المادي لهذه الجريمة بتغيير الغرض من جمع البيانات الشخصية، ذلك أن عمليه الجمع لا بد وأن يكون لها هدف معين، ويجب الالتزام به دون تغييره، وغرض مزودي خدمات التصديق الالكتروني هو إصدار الشهادة.

لم يحدد المشرع الجزائري معيار الانحراف عن الغرض المحدد لجمع البيانات الشخصية، بخلاف المشرع الفرنسي في المادة 226 ــ 21 من قانون العقوبات الفرنسي، حيث يلزم تحديد الغرض في الطلب المقدم مسبقا للجنة الوطنية للمعلوماتية والحريات، حيث يحدد فيه غرض معالجة هذه البيانات وذلك بمناسبة تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة.

ب ــ الركن المعنوي:

جريمة استعمال البيانات الشخصية لغير الغرض المحدد لها جريمة عمدية، يقوم الركن المعنوي فيها على القصد الجنائي العام، ومن تم لا يعاقب عنها إذا كانت نتيجة خطأ، وبالتالي يتعين على مزودي خدمات التصديق الالكتروني أن يعلم بأن فعله يشكل إنحرافا عن الغرض من جمع البيانات الشخصية ، وأن إرادته تتجه نحو تحقيق هذا السلوك الإجرامي.

لم بشترط المشرع الجزائري القصد الجنائي الخاص، بل يكفي توافر القصد الجنائي العام إلى جانب الركن المادي لتقوم الجريمة. ولا عبرة بالبواعث التي تدفع الجاني لارتكاب هذه الجريمة أو غايته.

ج ــ العقوبة:

تعاقب المادة 71 من قانون رقم (15 ــ 04) المتضمن القواعد العامة للتصديق والتوقيع الالكتروني على جريمة استعمال مزودي خدمات التصديق الالكتروني للبيانات الشخصية لغير الغرض المحدد لها، بعقوبة الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة مالية تقدر من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000دج) أو بإحدى هاتين العقوبتين فقط، هذا بالنسبة للجاني إذا كان شخص طبيعيا، أما إذا كان شخص معنويا فتعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، بمعنى يعاقب على هذه الجريمة بغرامة تقدر بـــ: خمسة ملايين دينار (5.000.000 دج).

عند مقارنة هذه العقوبات مع العقوبات التي قررها المشرع الفرنسي في حالة الاعتداء على البيانات الاسمية نلاحظ أنها متقاربة نوعا ما، وهذا ما يستفاد أن المشرع الجزائري قد اهتم بهذه البيانات الخاصة وأدرك مدى أهميتها في عصر تقنية المعلومات، وأن أي اعتداء عليها يؤدي إلى اهتزاز الثقة في أصحابها وبالتالي في الدولة وفي نظامها المعلوماتي المثمثل في الحكومة الالكترونية.

بعد رصد أهم الجرائم الواقعة على المعاملات الالكترونية الحكومية، يتعين حماية آليات نتفيذ هذه المعاملات والتي بدورها تنطبق على جميع أنواع المعاملات الحكومية منها والعادية التي تتم بين الخواص، وتتمثل في التوقيع الالكتروني باعتباره وسيلة توثيق هذه المعاملات التي تتم في الفضاء الافتراضي، وأيضا التسديد الالكتروني. وتتم هذه الحماية من خلال تجريم أفعال الاعتداء على التوقيع الالكتروني والدفع الالكتروني، هذا ما سيكون محل دراسة الفصل الثاني.

الفصل الثاني: الجرائم الواقعة على وسائل إجراء المعاملات الالكترونية الحكومية

إنّ الثّقة والأمان يأتيان في مقدمة الضمانات التّي ينبغي توافرها لازدهار المعاملات الالكترونية وانتشارها والأخذ بها كوسيلة أمثل لتبادل المعاملات الإدارية والاقتصادية والسياسية...إلخ[1]، وذلك من معرفة الأفراد واطمئنانهم لما تتمتع به المعاملات الإلكترونية من القوة الثبوتيّة التّي تحفظ بها حقوقهم، سواء تعلّق ذلك بالخدمات التي تقدّمها الحكومة للأفراد أو غيرها من المعاملات كالتّجارة الإلكترونية وعقود البيع والشراء التي تتمّ بواسطة المراسلات الالكترونية، وعليه فأوّل خطوة لإجراء هذه المعاملات هي ثوتيقها على نحو يبعث الاطمئنان لدى المتعاملين بها ويتوافر لهم الثقة والأمان، وبعد ذلك تأتي ثاني خطوة. وهي مرحلة السّداد أو الدفع الالكتروني لإتمام تنفيذ هذه المعاملات.

وعليه ينبغي توفير حماية قانونية لاسيما الجنائية لرصد مختلف السلوكات غير المشروعة التي تهدّد وسائل إجراء المعاملات الالكترونية الحكومية من خلال تجريم الاعتداء على التوقيع الإلكتروني (المبحث الأول)، وبطاقة الائتمان (المبحث الثاني).

المبحث الأول: جرائم الاعتداء على التوقيع الالكتروني

تؤدّي الحكومة الإلكترونية خدماتها لجمهور المتعاملين معها بطريقة سهلة ميسرة من خلال استخدام تقنية المعلومات وتطور الاتصالات وذلك في شكل محررات إلكترونية.

لكي تكون لهذه المستندات أو المحررات الحجية في الإثبات والصفة الرسميّة فلا بدّ أن تحمل توقيعا للمسؤول في الحكومة الإلكترونية أو شفرة معينة حتّ نضمن فاعلية الحكومة الإلكترونية[2]. وينبغي أن يكون هذا التوقيع يتناسب والبيئة الالكترونية، بمعنى يكون هو أيضا إلكترونيا.

---

[1] ــ حسن بن محمد المهدي، القوة الثبوتية للمعاملات الإلكترونية، مجلة البحوث القضائية، الجمهورية اليمنية، ع 7، جوان 2007، ص 07.

[2] ــ بشير علي الباز، دور الحكومة الإلكترونية في صناعة القرار الإداري والتصويت الإلكتروني، دار الكتب القانونية، مصر، 2009، ص 38.

للتوقيع الإلكتروني أهميّة كبرى في نطاق الحكومة الالكترونية، ذلك أنّ المعاملات الإداريّة الحكوميّة وتقديم الخدمات للمواطنين تتمّ كلها عن طريق المحررات الالكترونيّة، سواء عند صدور شهادة ميلاد أو إذن استيراد أو تصدير أو رخصة بناء أو غيرها من الوثائق والشهادات، بغض النظر عن الجهات التي تصدرها كمصلحة الأحوال المدنية أو الجمارك أو الضرائب، فيتمّ توقيعها من قبل الموظفين العموميين في هذه الجهات[1]، مما يساعد في تحديد هوية الموقِّع.

لذلك حاولت الجزائر إرساء نظام قانوني للتوقيع الإلكتروني، فقامت بإصدار القانون رقم (15ــ04) المحدّد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، المؤرخ في أوّل فبراير 2015[2]، وقرّر المشرّع من خلاله حماية جزائية خاصّة للتوقيع الالكتروني في الفصل الثاني منه، وهو ما سيتم تبيانه من خلال التعرّض أوّلا إلى تحديد مفهوم التوقيع الالكتروني، ومدى حجيّته كأداة ضمان للحكومة الإلكترونية وذلك في مطلب أوّل، أمّا الثاني فنخصّصه لصور الاعتداء على التوقيع الالكتروني.

المطلب الأول: توثيق المعاملات الالكترونية الحكومية

يُقصد بالتوثيق في المعاملات الالكترونية (Authentification) التحقُق من هُوية الموقع، وأنّ الرسالة الموقّعة منه تنسب إليه، ذلك أنّ المعاملات الالكترونية تتمّ على دعامة إلكترونية غير ملموسة، يصعب التحقُق من شخصية المتعامل مع الطرف الآخر، لذا أوجدت القوانين المقارنة هذا الأسلوب للحفاظ على صحّة هذه المعاملات وسلامتها القانونية وكذلك الحفاظ على سريتها[3].

لهذا فإنّ معرفة توثيق المعاملات الالكترونية يتطلّب البحث في ماهيّة التوقيع الالكتروني وحجيته في الإثبات، وذلك في الفرعين التاليين:

---

[1] ــ عبد الفتاح بيومي حجازي، النظام القانوني للحكومة الالكترونية، الكتاب الثاني، مرجع سابق، ص 147.

[2] ــ القانون رقم (15 ــ04) المؤرخ في أول فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج. ر. ج ، ع 6 ، لسنة 2015.

[3] - خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية، الدار الجامعية، الإسكندرية، 2008، ص 116.

الفرع الأول: ماهية التوقيع الالكتروني

سيتم التطرق في هذا الفرع إلى ماهية التوقيع الالكتروني من خلال تعريفه، تحديد الجهة المعنية بالتصديق، ثم بيان أنواع التصديق الالكتروني، وذلك على التفصيل التالي:

أولا ــ تعريف التوقيع الالكتروني:

تعدّدت التعاريف التي أعطيت للتوقيع الإلكتروني بحسب النظم القانونية السائدة، حيث تمّ تعريفه من خلال المنظمات الدولية، ومن خلال التشريعات المقارنة، وكذا في التشريع الجزائري.

من بين المنظّمات الدوليّة التي اهتمت بموضوع التوقيع الالكتروني: منظّمة الأمّم المتّحدة للتجارة الدولية المعروفة باليونسيترال، ومنظمة الإتحاد الأوروبي.

1) تعريف لجنة الأمم المتحدة للتجارة الدولية المعروفة باليونسترال للتوقيع الالكتروني:

وضعت منظمة الأمم المتحدة للتجارة الدولية "اليونسيترال"[1]، في القانون النموذجي بشأن التجارة الإلكترونية الصادر بتاريخ 16 ديسمبر 1996، اللبنات الأساسيّة لتعريف التوقيع الإلكتروني وعرفته في المادة 2/ ب بأنه: "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[2].

كما هو واضح من النّص، لم يقيّد قانون اليونسترال مفهوم التوقيع الالكتروني، بل إن النص يمكن أن يستوعب أية تكنولوجيا تظهر في المستقبل تفي بإنشاء توقيع إلكتروني، تاركا بذلك حرية اختيار الطريقة للفرد أو الدولة، ما دامت تلك الطريقة تسمح بتعيين هوية الموقع وبموافقته على المعلومات الواردة في الرسالة.

---

(1) - اليونسترال هي لجنة قانون التجارة الدولية التابعة للأمم المتحدة، وتضم في عضويتها غالبية دول العالم الممثلة لمختلف النظم القانونية الرئيسية، وغرضها الرئيس تحقيق الانسجام والتوائم بين القواعد القانونية المنظمة للتجارة الإلكترونية وتحقيق وحدة القواعد المتبعة وطنيا في التعامل مع مسائل التجارة العالمية. انظر: فرح مناي، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجديد، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009، ص 29.

(2) ـ قانون اليونسترال النموذجي بشأن التوقيعات الالكترونية 2001، منشورات الأمم المتحدة، نيويورك، 2002، منشور على الموقع: htttp://uncitral org. تاريخ الإطلاع: 25 ــ 02 ــ 2016

2) تعريف الإتحاد الأوربي للتوقيع الإلكتروني:

أصدر التوجيه رقم 93/1999 الصادر عن البرلمان الأوربي بتاريخ 13 ديسمبر 1999 المتعلق بالتوقيعات الالكترونية[1]، ويتكوّن هذا التوجيه من 28 حيثية و15 مادة و04 ملاحق، حيث جاء في مادته الأولى أنّ الهدف منه هو تسهيل استخدام التوقيعات الالكترونية والمساهمة في الاعتراف القانوني بها كدليل إثبات[2].

أمّا الفقرة الأولى من المادة الثانية منه عرّفت التوقيع الالكتروني على أنه عبارة عن: "بيان أو معلومة معالجة إلكترونيا، ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرىـــ كرسالة أو محرّرـــ وتصلح لتمييز الشخص وتحديد هويته"[3].

كما ميّز في الفقرة الثانية من نفس المادّة بين التوقيع الإلكتروني المتقدم أو المعزز "signature électronique avancée" والتوقيع الإلكتروني البسيط، فالتوقيع الإلكتروني المتقدم هو الذي يكون معتمدا من أحد مقدمي خدمات التصديق الإلكتروني ويمنح شهادة تفيد صحة التوقيع الإلكتروني بعد التحقق من نسبة التوقيع إلى صاحبه.

وحدّد في نفس المادة السابقة شروط التوقيع الالكتروني المتقدم وهي أن يكون[4]:

---

(1) Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques , Journal officiel n° L 013 du 19/01/2000 , publiésur le site :http://eur-lex.europa.eu/ a la date : 25/02/2016.

(2) Article premier de Directive 1999/93/CE du Parlementeuropéen et du Conseil, consiste: "L'objectif de la présente directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur".

(3) Article 2 de Directive 1999/93/CE du Parlementeuropéen et du Conseil: "signature électronique", une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification;

(4) -Article 2/2de Directive 1999/93/CE du Parlement européen et du Conseil:
"signature électronique avancée" une signature électronique qui satisfait aux exigences suivantes:
a) être liée uniquement au signataire;
b) permettre d'identifier le signataire;

(أ) مرتبط ارتباطا فريدا مع صاحب التوقيع،

(ب) قادر على تحديد صاحب التوقيع والتعرف عليه باستخدامه.

(ج) يتم إنشاؤه باستخدام وسائل يضمن فيها صاحبه السرية التامة.

(د) مرتبط مع المعلومات المضمنة في الرسالة حيث أنه يكشف أي تغيير في المعلومات".

إلى جانب هذه التعاريف التي قدّمت من طرف بعض المنظمات الدولية، نجد كذلك بعض التشريعات المقارنة والعربية قد أعطت تعريفا للتوقيع الإلكتروني.

1) بالنسبة للتشريع الفرنسي: إعترف المشرع الفرنسي بالتوقيع الإلكتروني من خلال إصداره للقانون رقم 2000ـــ230 المؤرخ في 13 مارس 2000 في شأن تعديل قانون الإثبات في مجال تكنولوجيا المعلومات والمتعلق بالتوقيع الالكتروني[1]، الذي تطرق فيه إلى التوقيع التقليدي والإلكتروني، مركزا على وظائف التوقيع المعروفة في المادة 4/1316 من القانون المدني الفرنسي بعد تعديلها حيث نص على أن: "التوقيع الذي يحدد هوية صاحبه والذي يفصح عن قبوله بمضمون المحرر الذي يرتبط به وبالالتزامات الواردة فيه".

تبنّى المشرّع الفرنسي هذا التعريف حتى يكون تعريفا عاما للتوقيع، أمّا التوقيع الإلكتروني فقد عرّفه المشرع في الفقرة الثانية من التعديل بأنه: "التوقيع الذي ينتج عن استخدام أية وسيلة مقبولة موثوق بها، لتحديد هوية الموقع وتكفل اتصال التوقيع بالعمل أو المستند المرتبط به"[2].

---

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif

etd) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit detectable.

(1) LOI n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique JORF n°62 du 14 mars 2000 page 3968 .

(2) - Art. 1316-4.de la loi n' 2000 – 230: - dispise que « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cetacte. Quand elle est apposée par un officier public, elle confèrel' authenticité à l'acte.« Lorsqu'ellees télectronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'act eau quell elle s' attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la

تجدر الإشارة أنّ هذه المادّة لا تطبق فقط على العقود الالكترونية المدنية، بل يمكن تطبيقها على العقود الالكترونية الإدارية، حيث أن الفقرة من المادة الثالثة (3) من المرسوم رقم 2002 ــ 692، تؤكد أنّ التوقيعات والطلبات التي يتمّ إرسالها عن طريق وسيط إلكتروني، يجب أن يتم توثيقها وفقا للشروط المنصوص عليها في المادتين 1316 و 4/1316 من القانون المدني[1].

2) في التشريع الأمريكي: وقد حظي التوقيع الالكتروني بنصيب وافر من الأهمية في التشريع الأمريكي، وبهذا عرفه القانون الأمريكي الصادر في 30 يونيو 2000 بأنه: "شهادة رقمية تصدر عن إحدى الهيئات المستقلة وتميز كل مستخدم يمكن أن يستخدمها في إرسال أي وثيقة أو عقد تجاري أو تعهد أو إقرار"[2]. هذا ما يتعلق بالتشريعات الدولية والمقارنة، وفي نفس السياق سايرت أغلب الدول العربية التطورات الحاصلة على مختلف وسائل الاتصال الحديثة، الشيء الذي دعى إلى إصدار ترسانة قانونية جديدة تساير هذه التطورات، منها مايلي:

المشرع الأردني: عرّفه في قانون المعاملات الالكترونية رقم (15) لسنة 2015 في المادة 02 المخصصة لتحديد المصطلحات والعبارات المتعلقة بالمعاملات الالكترونية على أن التوقيع الالكتروني هو: "البيانات التي تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو أي وسيلة أخرى مماثلة في السجل الإلكتروني أو تكون مضافة عليه أو مرتبطة به بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامه وتميزه عن غيره"[3].

أصدر **المشرّع المصري** في نفس السياق قانونا خاصا بالتوقيع الإلكتروني، وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم (15) لسنة 2004، حيث خصّص المادة الأولى منه لتعريف بعض

---

signature électroniquee stcréée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

(1) - Article 3 /2 de décret n° 2002-692 du 30 avril 2002 pris en application du 1° et du 2° de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics, ditque Les candidatures et les offres transmises par voie électronique doivent être envoyées dans des conditions qui permettent d'authentifier la signature du candidat selon les exigencies posées aux articles 1316 à 1316-4 du code civil.

(2) ــ عبد الفتاح بيومي حجازي، النظام القانوني للحكومة الالكترونية، الكتاب الثاني، مرجع سابق، ص 115.

(3) ــ اقانون رقم (15) لسنة 2015 المتعلق بالمعاملات الإلكترونية، منشور على موقع التشريعات الأردنية:

http://www.lob.gov.jo/ تاريخ الإطلاع: 26 ــ 02 ــ 2016.

المصطلحات القانونية، منها التوقيع الإلكتروني والذي عرفه بأنه: "ما يوضع على المحرر الالكتروني ويتخذ شكل حروف أو أرقام أو رسوم أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد الموقع وتمييزه عن غيره" [1].

أمّا بالنسبة **للمشرع الجزائري**: استخدم مصطلح التوقيع الالكتروني لأوّل مرّة في نص المادة 327/ 2 من القانون المدني المعدل سنة 2005 بموجب القانون رقم 05 ــ10 والتي تنص على: ''يعتدّ بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرّر أعلاه''.

فلم يعرف التوقيع الالكتروني في هذه المادة، وإنما جاء التوقيع الالكتروني وسيلة إثبات في القانون المدني.

حيّ في المرسوم التنفيذي رقم 07ــ 162 المتعلق بنظام الاستغلال المطبق على كل أنواع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، المؤرخ في 30 ماي 2007[2]، لم يضع المشرع تعريفا للتوقيع الالكتروني، وإنما ذكر الصور التي قد يظهر من خلالها، حيث ميز بين التوقيع الالكتروني العادي، والتوقيع الالكتروني المؤمن، فجاء ذكر النوع الأول (التوقيع الالكتروني العادي) في المادة 1/3 من المرسوم التنفيذي 07 ــ 162 إذ تنص على:" التوقيع الالكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و 323 مكرر 1 من الأمر رقم 74 ــ 58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر 1975 والمذكور أعلاه".

أمّا التوقيع الإلكتروني المؤمّن فوضحه في الفقرة الثانية من المادة الثالثة من المرسوم التنفيذي السابق الذكر أن: "التوقيع الالكتروني المؤمن: هو توقيع إلكتروني يفي بالمتطلبات الآتية:

1 ــ يكون خاصا بالموقع،

2 ــ يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصريّة،

---

[1] - القانون رقم 2004 ــ 15 المتعلق بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، الجريدة الرسمية المصرية، العدد 17 تابع (د)، 22 أبريل 2004.

[2] ــ المرسوم التنفيذي رقم 07 ــ 162 المؤرخ في 30 مايو سنة 2007، والمتعلق بنظام الاستغلال المطبق على كل أنواع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر.ج، ع 37، الصادر في 07 يونيو 2007.

3 ــ يضمن مع الفعل المرتبط به، صلة بحيث يكون له كل تعديل لاحق للفعل قابلا للكشف عنه" .

هذا التعريف يكاد يتطابق مع التعريف الوارد في التوجيه الأوربي ــ المذكور سابقا ــ إلا أنه خالفه في المصطلح باستعماله التوقيع الالكتروني المؤمن"électronique sécurisée signature "

في حين استخدم التوجيه الأوربي التوقيع الالكتروني المتقدم"éléctroni que avancée signature".

بصدور القانون رقم (15ــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين السابق الذكر[1]، جاء في الفصل الثاني منه المخصص للتعاريف وبصفة خاصة الفقرة الأولى من المادة الثانية إلى تعريف التوقيع الالكتروني على أنه: ''بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق''[2].

وعليه يلاحظ من نص الفقرة1 من المادة 2 من القانون رقم (15ــ 04) السابق الذكر أنه قام بتعريف التوقيع على أساس وظيفة التوثيق أما في الفقرة الثالثة من نفس المادة 2 قام بتعريف البيانات المكونة للتوقيع الالكتروني التي تدل على الجانب التقني الذي يتخذه شكل التوقيع من رموز أو مفاتيح تشفير حيث جاءت هذه الأشكال على سبيل المثال وليس على سبل الحصر.

من خلال مختلف التعريفات نلاحظ أنّ القوانين السابقة لم تحدّد أنواع التوقيع الالكتروني، وهذا نظرا لإمكانية استيعاب هذه التعريفات لما يستجد من توقيعات إلكترونية قد يفرزها هذا التطور التكنولوجي الهائل والمتسارع، بالإضافة أنها ركزت على الوظائف التي ينبغي أن يؤديها في مجال التبادلات الإلكترونية.

---

[1] ــ يعتبر القانون (15ــ04) المحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، أوّل نص تشريعي اهتم بشكل مباشر بالتوقيع الالكتروني، إذ جاء لإرساء النظام القانوني له وضبط المفاهيم المرتبطة به، فحدد القواعد التي تحكمه من خلال تخصيص باب كامل من أحكامه. فصل الجزء منه المبادئ المماثلة وعدم التميز تجاه التوقيع الإلكتروني وفي الثاني آليات إنشاء التوقيع الالكتروني الموصوف وكيفية التحقق منه، ولكنه أحال بشأن حفظ الوثائق الموقعة إلكترونيا للتنظيم ولذلك اعتمد تطبيقا له المرسوم التنفيذي رقم (16ــ142)، فوضح قواعد حفظ هذه الوثائق حتى يعتد بها وتكون دليلا للإثبات.

[2] ــ المادة 2 /1 من القانون رقم (15 ــ04) المؤرخ في أول فبراير 2015،المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر.ج، ع 6، لسنة 2015.

ثانيا ــ المصادقة على التوقيع الالكتروني: جهة التصديق الالكتروني

تعدّ جهة التصديق الالكتروني الطرف الثالث في المعاملة الالكترونية، وتكمن وظيفتها في التأكد من صحة التوقيع وبيانات الشخصية للأفراد عن طريق حرصها ــ جهة التصديق ــ من عدم الحصول أي تعديل أو تحريف في المعاملة الالكترونية حيث تعمل على توثيق المعاملات عن طريق إصدار شهادات التصديق الالكترونية التي تؤكد على هوية المتعاملين وصحة وسلامة البيانات الواردة في المعاملة الالكترونية، ويطلق على هذا الطرف الثالث المحايد مصطلح ''مقدم خدمات التصديق'' أو ''مؤدي خدمات التصديق''.

وقد عرّف **قانون اليونسترال النموذجي بشأن التوقيع الالكتروني 2001** السابق الذكر مقدم خدمات التصديق الالكتروني بأنه: "شخصا يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية".

في حين استخدم **المشرع التونسي** مصطلح مزود خدمات المصادقة الالكترونية، وعرّفه في الفصل الثاني من قانون المبادلات والتجارة الإلكترونية بأنه " كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني" [1].

يلاحظ تطابق مضمون هذا التعريف مع التعريف السابق المتعلق بقانون اليونسترال النموذجي للتجارة الالكترونية.

أمّا **المشرع الجزائري** عرّف مؤدي خدمات التصديق الالكتروني في القانون رقم (15 ــ 04) المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين والمؤرخ في أول فبراير 2015، وذلك في الفصل الثاني منه تحت عنوان ''التعاريف '' في المادة 2 /12 بأنه: "شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الالكتروني" [2].

---

[1] ــ قانون رقم 2000/ 83 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية، الرائد الرسمي للجمهورية التونسية، ع 64 لسنة 2000.

[2] ــ المادة 2 / 12 من القانون رقم (15 ــ04) المؤرخ في أول فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، السابق الذكر.

إنطلاقا ممّا سبق نجد أنّ المشرع الجزائري لم يخالف التشريعات السابقة بخصوص الشخص الذي يقدم خدمات تسليم الشهادات الالكترونية.

تجدر الإشارة أنّ جهة التصديق الالكتروني المقدمة لخدمات التصديق الالكتروني تشبه في مهامها مع مهام الموثق فتصدر الجهة شهادات إلكترونية تدعى بشهادة التصديق الإلكتروني، حيث تؤكد هذه الأخيرة صحة الكتابة ومصداقية التوقيع ومعرفة أطراف المعاملة.

عرّف المشرّع الجزائري شهادة التصديق الإلكتروني في الفقرة السابعة من المادة الثانية من القانون رقم (15 ــ 04) السابق الذكر بأنها: "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع". في حين خصص الفصل الثالث منه والمعنون تحت عنوان النظام القانوني لتأدية خدمات التصديق الالكتروني، حيث حدد في القسم الأوّل من هذا الفصل شروط حصول مؤدي خدمات التصديق الالكتروني على ترخيص لتأديّة خدمات التصديق الالكتروني، فضلا عن الالتزامات والواجبات التي تقع على عاتقه بمجرد حصوله على هذا الترخيص وذلك من خلال الفرع الأول من القسم الثاني والمخصص لواجبات مؤدي خدمات التصديق الالكتروني ومسؤولياته.

إجمالا فإن للتصديق الإلكتروني أهمية كبيرة في مجال المعاملات الالكترونية الإدارية أو التجارية وذلك لتوفير الثقة والأمان لأطراف المعاملة الالكترونية.

ثالثا ــ أنواع التوقيع الالكتروني

على غرار قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية، وأغلب التشريعات المقارنة، لم يحدّد القانون الجزائري صور التوقيع الإلكتروني، بل ترك المجال مفتوحا كي يتسع هذا المفهوم لكل ما يستجد من تطورات تكنولوجية قد تقرر أشكالا وصورا جديدة من التوقيعات الالكترونية، إلا أنه أشار بشكل غير مباشر لبعض هذه الصور من خلال تحديده للمفاهيم المرتبطة بها مثل مفتاح التشفير الخاص ومفتاح التشفير العمومي المرتبطان بالتوقيع الرقمي.

وفيما يلي الصور الأكثر شيوعا للتوقيع الإلكتروني وهي كالتالي:

1 ــ التوقيع الإلكتروني الرقمي:

يسمّى أيضا التوقيع بواسطة المفتاح، وسمي "رقميا" لأنه يحتوي على رقم سري لا يعرفه سوى صاحبه ويشيع استخدامه في التعاملات المالية والبنكية وبواسطة بطاقة الائتمان، ويقوم هذا التوقيع على وسائل التشفير الرقمي[1] الذي يعتمد على معادلات رياضية لضمان سريّة المعلومة والاتصال بطريقة آمنة عبر تحويله إلى شكل غير مفهوم إلاّ من أطراف العلاقة، فيتمّ التوقيع الرقمي باستعمال مفتاح معين لتشفير الرسالة الالكترونية، ثمّ يعمد مستقبلها لفك التشفير بمفتاح آخر للحصول على المعلومات المرسلة، فإذا ظهرت الرسالة بعد فك التشفير واضحة مقروءة، كان التوقيع المرسل صحيحا[2].

هذا النوع من التوقيع الأوسع نطاقا والأكثر استخداما لكونه يعتمد على تقنية التشفير، مما يجعله يحقق نوعا من الثقة والأمان لدى الدول والشركات.

والمشرع الجزائري من خلال القانون رقم (15 ــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين تطرق إلى تقنية التشفير، واعتبر مفاتيح التشفير الخاصة من أهم بيانات إنشاء التوقيع الالكتروني، وهو خاص بالموقع فقط، أما مفاتيح التشفير العمومية تعد من بيانات التحقق من التوقيع الالكتروني، وتكون في متناول الجميع[3]للتأكد من موثوقية التوقيع، والتأكد من هوية وشخصية الموقع.

---

[1] - يقصد بالتشفير استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها. الفصل 05/02 من القانون 2000ــ 83 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية، الرائد الرسمي للجمهورية التونسية، ع 64 ، لسنة 2000.

[2]- منابي فراح، مرجع سابق، ص 98.

[3] ــ عرف المشرع الجزائري مفتاح التشفير الخاص في المادة 2 / 8 من القانون رقم (15 ــ04) السابق الذكر أنه: "عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا التشفير بمفتاح التشفير العمومي.

أما مفتاح التشفير العمومي فيعرف طبقا للمادة 9/2 من القانون السابق الذكك رأنه: "عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني، وتدرج في شهادة التصديق الالكتروني".

2 ــ التوقيع الإلكتروني البيومتري:

يعتمد هذا النوع من التوقيع على طرق التحقّق من الشخصيّة التي تعتمد على الخواص الفيزيائية والطبيعية والسلوكية للأفراد، فلكل إنسان صفات وسمات تميزه عن غيره مثل: مسح قرنية العين، أو بصمة الأصابع، بصمة الشفاه أو نبرة الصوت، أو ملامح الوجه...، فيجب أوّلا أخذ صورة لأحد أجزاء الجسم عم طريق تقنية مخصصة لذك، بعد ذلك تحفظ بشكل شفرة داخل الحاسوب، فتتكوّن قاعدة بيانات للشخص بواسطة برنامج تقني، عند رغبة صاحب الشأن استعمال هذه المعلومة يرجع إليها ويوثّق تصرفه، فتقارن الصورة المحفوظة مع الصورة الملتقطة، فإذا تطابقت تمكن الشخص من توثيق تصرفه[1].

يحتاج التوقيع البيومتري إلى توثيقه من جهة مختصة معتمدة بشكل رسمي تقوم بتوثيق التوقيع وتصديقه وتربط بينه وبين الموقع وذلك لزيادة الموثوقيّة وتحقيق الأمان في التعامل الإلكتروني وحماية المتعاملين من التقنيات الإحتيالية المتبعة لفك رموز التشفير[2].

وعليه يتشابه كل من التوقيع الرّقمي والتوقيع البيومتري في أن كلا منهما يقوم على التشفير ومعالجة البيانات المتبادلة إلكترونيا بوجود سلطة التوثيق التي تعمل على توثيق التوقيع الإلكتروني وتصديقه[3].

3 ــ التوقيع بالقلم الالكتروني:

تعتمد هذه الطريقة في استعمال قلم إلكتروني خاص (Pen Op)، إذ يقوم الشخص بالتوقيع على لوحة إلكترونية تابعة للحاسوب ويتم التحقق من صحة التوقيع بواسطة برنامج خاص، وذلك

---

(1)- عيسى غسان ريضي، القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة للنشر والتوزيع، ط 1، الأردن، ص 62.
وتجدر الإشارة أن التوقيع البيومتري المبني على الخواص الذاتية للإنسان يعتبر وسيلة موثوق بها لتمييز هوية الشخص، نظرا لارتباط الخواص الذاتية به، غير أن هذه الطريقة منتقدة من حيث ارتفاع التكلفة التي يتطلبها وضع نظام آمن في شبكات المعلومات باستخدام وسائل البيومترية، مما حددت من انتشاره، وجعلته قاصرا على الدول المتقدمة وفي مجالات محدودة تقتصر بالخصوص على الجوانب الأمنية ولا تصل في الغالب إلى المعاملات التجارية والمالية.

(2) ــ عبد اللطيف بركات، مرجع سابق، ص 36.

(3) ــ حنان مليكة، النظام القانوني للتوقيع الالكتروني في ضوء قانون التوقيع الالكتروني السوري رقم 04 ــ 2009، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثاني، المجلد 26 ، 2010، ص 365.

بالاستناد إلى حركة القلم والأشكال التي يتخذها من دوائر وانحناءات فيتم مطابقتها مع التوقيع المحفوظ مسبقا في ذاكرة الحاسوب[1]. وقد يتم الخلط بين التوقيع بالقلم الالكتروني والتوقيع الممسوح ضوئيا "scannérisée" عبر جهاز الماسح الضوئي (Scanner)، إذ أنّ هذا الأخير لا صلة له بالتوقيع الالكتروني ولا قيمة قانونية في الإثبات، هذا ما أكدته محكمة الاستئناف الفرنسية في 20 أكتوبر 2000، مضمون ما جاء في القضية:" ....استخدام محامي التوقيع الممسوح ضوئيا في عريضة الاستئناف، وقد رفضت في هذه الحالة محكمة الاستئناف التوقيع الممسوح ضوئيا كوسيلة لإثبات الهوية الموقع والموثوقية، الأمر الذي نستنتجه هو أن الطريق الوحيد الأمن هو التوقيع الالكتروني أو الرقمي[2].

4 ــ التوقيع بالبطاقة والرقم السري:

يستخدم هذا النظام في التعاملات البنكية والمعاملات المالية، وهي جزء من الحكومة الالكترونية لهاته الأشخاص المعنوية، ومثال على ذلك بطاقة الائتمان التي تحتوي على رقم سري لا يعرفه سوى صاحب البطاقة[3]، ويتم هذا التوقيع عبر إدخال بطاقة ممغنطة في جهاز إلكتروني مخصص لذلك ثم إدخال الرقم السرّي والضغط على زر الموافقة لإتمام العملية المطلوبة، وهذا النوع من التواقيع يشيع في أجهزة الصرف الآلي لدى المصارف للحصول على كشف الحساب أو سحب الأموال أو تحويلها[4]. وينبغي الإشارة أنّ هذه البطاقات مزودة بشريحة إلكترونية، بمثابة ذاكرة تخزن فيها المعلومات الخاصة بالشخص، وتطبقها الجزائر في مجال المعاملات المالية والضمان الاجتماعي مثل بطاقة الشفاء.

---

(1) ــ عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية (دراسة مقارنة)، المكتب الجامعي الحديث، الاسكندرية، 2009، ص22.

(2) M, Guével, le développement de la signature électronique, thèse de mastère 2, recherche droit des affaires, université Paris Nord 13, France, 2010/2011, disponible en ligne sur: http://www.cngtc.fr/ à la date : 25 – 02 - 2014 .

(3) - هدى حامد قشقوش الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية للطبع والنشر والتوزيع، القاهرة، 2005، ص 218 و219.

(4) ــ مناني فراح، مرجع سابق، ص 191.

الفرع الثاني: القيمة القانونية للتوقيع الالكتروني في الإثبات

يتمّ استخدام تقنية التوقيع الالكتروني في العديد من المجالات أهمّها: المعاملات الإدارية الحكومية في مختلف الخدمات التي تقدّم للمواطنين، مما يهدف إلى بعث الثّقة والأمان في مثل هذه التعاملات، بما يسمح منح هذه المحررات القوّة في الإثبات (أولا)، وبشروط معينة (ثانيا)، وعليه كيف تعامل المشرع الجزائري مع مثل هذه المحررات، فهل اعترف بحجيتها في الإثبات بما يفيد الاعتماد عليها كأداة ضمان للتعاملات الحكومية الإلكترونية؟

أولاـــ حجية التوقيع الالكتروني كأداة ضمان للحكومة الإلكترونية.

اعترف القانون الجزائري لأوّل مرة بالتوقيع الإلكتروني في القانون المدني ضمن المواد المتعلقة بإثبات الإلتزام من خلال نص المادة 2/327 منه على ما يلي" ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1" [1].

وبذلك ساير المشرع الجزائري معظم التشريعات المقارنة كالقانون الفرنسي[2]، والقانون المصري[3]... ، وكذا قانون اليونسترال النموذجي الخاص بالتوقيع الإلكتروني "Loi type de la

---

[1] ـــ قام المشرع الجزائري بتعديل القانون المدني بموجب القانون رقم (05 ـــ 10) المعدل والمتمم للأمر 75 58 المتضمن القانون المدني، ومن خلاله تم استحداث المادتين 323 مكرر و323 مكرر 1، وعلى أساسه انتقل المشرع الجزائري من النظام الورقي في الإثبات إلى النظام الالكتروني.

[2]- اعترف المشرع الفرنسي بحجية التوقيع الإلكتروني في الإثبات في نص المادة 1316ـــ 1 من القانون المدني المعدل بموجب المرسوم رقم 2000 ـــ 230 المؤرخ في 13 مارس 2000: "الكتابة المتحدة في شكل إلكتروني معترف لها بذات الحجية في الإثبات التي للكتابة المدرجة على الورق بشرط إمكانية بيانها للشخص الصادر عنه وأن تنشأ وتحفظ في أحوال من طبيعتها ضمان كمالها وحدها". كما نص في الفقرة الثالثة من نفس المادة ما يلي: "أن الكتابة على وسيط إلكتروني ذات القوة في الإثبات كالكتابة على ورق". وقد أشارت المادة 1316 من القانون المدني الفرنسي أن اقتران المحرر بتوقيع إلكتروني لموظف عام يضفي الصبغة الرسمية على المحرر، كما صدر المرسوم رقم 973/2005 الخاص بالمحررات الموثقة المؤرخ في 10 أوت 2005، حيث وضع هذا المرسوم إنشاء وحفظ هذه المحررات التي يمكن أن تنشأ على دعامة إلكترونية ثم تقتضى المادة 1317 من القانون المدني المتعلقة بالمحررات الرسمية.

[3] - نصّ المشرّع المصري في المادة 18 من القانون رقم 15 لسنة 2004، المتعلق بتنظيم التوقيع الإلكتروني، وبإنشاء هيئة تنمية تكنولوجيا المعلومات: "يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بحجية في الإثبات إذا توافرت فيها الشروط الآتية:

أ ـــ ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.

ب ـــ سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

ج ـــ إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني".

"CNUDCI sur les signatures électroniques (2001)" [1] وكذا التوجيه الأوربي بشأن التوقيعات الإلكترونية "Parlement européen et du Conseil pour les signatures électroniques"[2].

أقرّ بمبدأ التعادل الوظيفي ما بين التوقيع الإلكتروني والتوقيع اليدوي أو التقليدي وساوى بينهما في الحجية، وجعل للتوقيع الإلكتروني نفس وظائف التوقيع العادي من حيث تحديد هوية موقعه وتمييزه عن غيره والتعبير عن إرادته ورضاه بمضمون التصرف القانوني الذي تضمنه المحرر طالما استوفى الشروط المحددة في المادة 223 مكرر 1 والمتمثلة في: أن يكون التوقيع توقيعا شخصيا ومميزا لموقعه وأن يكون متصلا بالمحرر الإلكتروني ولا يقبل الانفصال عنه[3].

لكن بعد اعتماد القانون الخاص بالتوقيع الإلكتروني قلّص المشرّع الجزائري من نطاق حجية التوقيع الإلكتروني، وجعل التوقيع **الإلكتروني الموصوف** وحده يكون مماثلا للتوقيع المكتوب، أي يكون له نفس حجيته سواء كان هذا التوقيع لشخص طبيعي أو معنوي[4]، إلا أنه لم ينفِ الحجيّة على التوقيع الإلكتروني العادي بدليل ما نصت عليه المادة 9 من القانون الخاص بالتوقيع الإلكتروني والتي جاء فيها ما يلي: "بغض النظر عن أحكام المادة 8 أعلاه، لا يمكن تجريد التوقيع الإلكتروني من

---

(1) - اعترفت لجنة الأمم المتحدة للتجارة الدولية المعروفة باليونسترال، في القانون النموذجي بشأن التجارة الإلكترونية الصادر في 16 ديسمبر 1996، بحجية التوقيع الالكتروني وساوت بينه وبالتوقيع العادي، وذكرت الشروط الواجب توافرها فيه في الفقرة الأولى من المادة السابعة منه:" عندما يشترط القانون وجود توقيع من شخص، يعد ذلك الاشتراط مستوفيا فيما يتعلق برسالة البيانات، إذا استخدم توقيع إلكتروني يعول عليه بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات..". وائل أنور بندق، مرجع سابق، ص 55.

(2)ـــ اعترف التوجيه الأوربي بشأن التوقيعات الالكترونية والصادر عن البرلمان الأوربي بتاريخ 13/ 12/ 1999 بالتوقيع الإلكتروني من خلال المادة 1/5 منه، وحث الدول الأعضاء على تسهيل استعماله من أجل حسن سير العمل في السوق الأوربي . Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques , Journal officiel n° L 013 du 19/01/2000 , publié en 20-05-2016 sur le sitesuivant : http://eur-lex.europa.eu/

(3) - حابت أمال، التجارة الإلكترونية في الجزائر، رسالة دكتوراه في العلوم القانونية، جامعة مولود معمري، تيزي وزو، 2015،ص 106.

(4) - أوباية مليكة،خصوصيات التوقيع الإلكتروني في القانون الجزائري، مداخلة مقدمة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد في 7 ــ 8 فبراير 2017 بالمركز الجامعي، غليزان، ص 12.

فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب: شكله الإلكتروني، أو أنه لا يعتمد على شهادة تصديق إلكتروني، أو أنه لم يتم إنشاؤه بواسطة آلة مؤمنة لإنشاء التوقيع الإلكتروني".

عرّف التوقيع الإلكتروني المؤمن في المرسوم التنفيذي رقم 07 ــ 162 على أنه هو التوقيع الذي يفي بالمتطلبات الآتية: يكون خاصا بالموقع، يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصريّة، يضمن مع الفعل المرتبط به صلة، بحيث يكون كل تعديل لاحقا للفعل قابلا للكشف عنه[1].

من أجل حفظ الوثيقة الموقعة إلكترونيا، ألزم المشرّع الجزائري إتباع مجموعة من الإجراءات التقنيّة التي تسمح بتخزين الوثيقة الموقعة إلكترونيا لضمان سلامتها، فقام بإصدار مرسوم تنفيذي رقم (16ــ142) بتاريخ 5 ماي 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا[2].

ثانيا ــ الشروط الواجب توافرها في التوقيع الإلكتروني:

من خلال ما سبق يمكن استنتاج الشروط الواجب توافرها في التوقيع الالكتروني للاعتداد به كالتوقيع العادي، فهناك شروط بعضها مرتبط بإنشاء التوقيع، وأخرى مرتبطة بالموقع، وبعضها الآخر متعلق بالبيانات الخاصة بالتوقيع. وذلك ما نبيّنه تباعا:

أ ــ الشروط المرتبطة بإنشاء التوقيع:

نصّت المادة 07 من القانون رقم (15ــ04) على هذه الشروط ضمن الفقرة الأولى والرابعة منها، وتتمثل في إنشاء التوقيع على أساس شهادة تصديق الإلكتروني موصوفة (أ)، وأن يكون مصممّا بواسطة آليّة مؤمنة خاصة بإنشاء التوقيع الإلكتروني (ب).

(1) ــ إنشاء التوقيع على أساس شهادة تصديق الإلكتروني موصوفة:

تطلب القانون ضرورة استخدام تقنيّة آمنة في التوقيع الإلكتروني تسمح بالتعرف على شخصية الموقع وتضمن سلامة المحرر من العبث، وهي تدخل طرف آخر يضمن توثيق التوقيع[3].

---

(1) - الفقرة الثانية من المادة الثالثة من المرسوم التنفيذي رقم 07 ــ 162 السالف الذكر.

(2) - المرسوم التنفيذي رقم 16 ــ142 مؤرخ في 27 رجب عام 1437 الموافق 5 مايو 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا، ج.ر.ج ع 28، الصادر بتاريخ 08 ماي 2016.

(3) ــ أباية مليكة، مرجع سابق، ص8.

هذا الطرف إمّا يكون طرف ثالث موثوق[1]، وإمّا مؤدي خدمات التصديق الإلكتروني[2]، يمنح لهذا الموقع شهادة تصديق إلكتروني موصوفة.

يتعين أن تتضمن هذه الشهادة أساسا[3]:

1 ــ إشارة تدل على أنها شهادة تصديق إلكتروني موصوفة.

2 ــ تحديد هوية مصدرها وتوقعه الإلكتروني الموصوف.

3 ــ إسم الموقع مع إمكانية إدراج صفة من صفاته.

4 ــ بيانات تتعلق بالتحقق من التوقيع.

5 ــ تحديد تاريخ بداية ونهاية صلاحيتها.

6 ــ حدود استعمالاتها، وحدود قيمة المعاملات التي ستستخدم لأجلها.

(2) ــ أن يكون التوقيع مصمّما بواسطة آليّة مؤمنة خاصة بإنشاء التوقيع الإلكتروني:

ينشأ التوقيع الإلكتروني بوجه عام بواسطة آلية إنشاء التوقيع الإلكتروني، وهي جهاز أو برنامج معلوماتي معد لتطبيق بيانات الإنشاء[4]، بينما يشترط في التوقيع الالكتروني الموصوف أن ينشأ بواسطة آلية إنشاء مؤمنة خاصة، ولا تكون كذلك إلا إذا استوفت المتطلبات التالية[5]:

ــ يجب أن تضمن هذه الآلية بواسطة الوسائل التقنية والإجراءات المناسبة، على الأقل ما يلي:

ــ عدم مصادقة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة.

---

(1) ــ عرّفته المادة 11/02 من القانون رقم (15ــ04) السابق الذكر بأنه: ''شخص معنوي يقوم بمنح شهادات التصديق الإلكتروني الموصوف، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي''.

(2) - هو شخص طبيعي أو معنوي منحته السلطة الاقتصادية للتصديق الإلكتروني الترخيص ليقوم بمنح شهادات التصديق الإلكتروني الموصوف وخدمات أخرى في مجال التصديق الإلكتروني. انظر المادة 12/02 من القانون رقم (15ــ04) السالف الذكر.

(3) - انظر المادة 15 من القانون رقم (15ــ04)، مرجع سابق.

(4) - انظر المادة 4/2 من انفس لقانون .

(5) - المادة 11 من القانون رقم (15 ــ 04).

ـــ ضمان سرية تلك البيانات.

ـــ عدم الوصول إلى تلك البيانات عن طريق الإستنساخ.

ـــ حماية التوقيع بشكل كافي من أي تزوير وضمان عدم استعمال بيانات التوقيع من قبل الغير.

ـــ كما يجب أن تضمن تلك الآلية عدم تعديل بيانات التوقيع وأن لا تمنع من عرض هذه البيانات على الموقع قبل عملية التوقيع.

ب ـــ الشروط المرتبطة بالموقع: وهي كالتالي:

(أ) أن يمكن التوقيع من خلال تحديد هوية الشخص الموقع:

يعتبر تحديد هويّة الموقِّع الذي أبرم تصرفا معينا أمرا ضروريا في مجال الإثبات، ولهذا حتى يكتسب التوقيع الموثوقية ينبغي أن يكون قادرا على تحديد هوية الموقع بسهولة أيّا كانت الصورة التي تمّ بها التوقيع[1].

وفي هذا الصدد نصّ المشرّع الجزائري في المادة السادسة من القانون (15ـــ04) المتعلق بالقواعد العامة بالتوقيع والتصديق الإلكترونيين على أنه: "يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع..."، ويتم ذلك بالرجوع إلى جهات إصدار التوقيعات الإلكترونية، وشهادة التصديق المعتمدة، التي تمكن من تبيان هوية ذلك الموقع.

الشخص الذي يقوم بتوقيع مستند إلكتروني من خلال التوقيع البيومتري يتمّ التحقق من هويته من خلال الخصائص البيولوجية التي تميزه عن غيره[2].

الأمر ذاته بالنسبة للتوقيع الرقمي الذي يتم باستخدام المفتاحين العام والخاص، حيث يمكن من التعرف على هوية الموقع، إضافة إلى الاستعانة بسلطات التصديق[3].

---

(1) - علي أبو مارية، التوقيع الإلكتروني ومدى قواه في الإثبات دراسة مقارنة، مجلة جامعة الخليل للبحوث، العدد 02، 2010، ص 119.

(2) ـــ فرح مناني، مرجع سابق، ص 192.

(3) ـــ علي أبو مارية، مرجع سابق، ص 119.

(2) ــ سيطرة الموقع على منظومة التوقيع:

لابدّ من سيطرة الموقّع على الوسيط الإلكتروني على النحو الذي يطمئن إلى سلامة توقيعه وعدم تعرضه في صورته السرية لآي تزوير أو تلاعب، كي نضمن نسبة التوقيع إلى صاحبه وارتباطه بمضمون المحرر[1]. لذلك فرض القانون أن ينفرد هذا الموقع بالتحكم بالوسيلة التي أنشأ بها التوقيع.

وقد عرف المشرع الجزائري هذه الوسيلة على انها جهاز أو برنامج معلوماتي معد لتطبيق بيانات أنشاء التواقيع الإلكترونية[2]، من دون أن يحدد هذه الأجهزة والبرامج بشكل دقيق، وذلك لترك المجال لإمكانية إقرار التكنولوجيا لوسائل إلكترونية جديدة يمكن من خلالها إنشاء التواقيع الإلكترونية[3]، من هذه الأجهزة نذكر أجهزة تسجيل البصمات، أجهزة وأنظمة التشفير...

(3) إرتباط التوقيع بالموقع دون سواه:

يعتبر التوقيع الإلكتروني روح المحرر الإلكتروني، وتعبيرا واضحا عن شخصية موقعه[4].

لذلك ينبغي أن يرتبط التوقيع بهذا الموقع دون سواه، وأن ينسب لشخص معين بالذات، والذي عرفه المشرع الجزائري (الموقع) في نص المادة الثالثة من المرسوم التنفيذي رقم (07 ــ 162) السابق الذكر على أنه شخص طبيعي ينصرف لحسابه الخاص أو لحساب الشخص طبيعي آخر أو الشخص المعنوي الذي يمثله...

كما عرّفه في نص الفقرة الثانية من المادة الثانية من القانون رقم (15ــ04) المحدّد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين على أنه شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني، ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله.

---

(1) ــ نبيل صقر ومكاري نزيهة، الوسيط في القواعد الإجرائية والموضوعية في الإثبات في المواد المدنية، دار هدى للطباعة والنشر والتوزيع، الجزائر، ص 257.

(2) ــ أنظر المادة 4/2 من القانون رقم (15،04) السالف الذكر.

(3) ــ حابت أمال، مرجع سابق، ص 112.

(4) ــ علي أبو مارية، مرجع سابق، ص 119.

ج ــ الشروط الخاصة ببيانات التوقيع:

لابدّ من ارتباط التوقيع الالكتروني ارتباطا وثيقا بالبيانات الخاصة به، وذلك ما فرضته المادة 6/7 من القانون رقم(15ــ04) المنوه عنه سابقا، بحيث يمكن الكشف عن التغيرات اللاحقة لهذه البيانات.

يستلزم هذا ضرورة تكامل البيانات المتعلقة بالتوقيع الإلكتروني، بحيث يعتبر أي تعديل أو تغيير في رسالة البيانات أو المحرر بعد توقيعه قابلا للكشف عنه، مما ينزع عنه صلاحيته للإثبات، والغاية من هذا الشرط هو حماية سلامة المحرر الإلكتروني من أي تغيير[1].

يشترط في المحرر الإلكتروني سلامة المحتوى أو حفظ المعلومات كما هي منذ إنشائه طوال مدة التقادم التي يخضع لها التصرف المحفوظ، ولذلك يلاحظ أن عملية الحفظ لها دور هام في مجال الإثبات، فلذلك يجب حفظ المعلومات والمعطيات على دعامات إلكترونية ضد التلف والتعديل أو أي صورة من صور الهلاك[2]، و ذلك بإتباع مجموعة من التدابير التقنية المحددة في المرسوم التنفيذي رقم (16ــ142) المحدد لكيفيات لحفظ الوثيقة الموقعة إلكترونيا السالف الذكر.

بذلك يمكن القول أن التوقيع الالكتروني يمكنه في ظل ضمانات معينة أن يقوم بذات الدور الذي يؤديه التوقيع التقليدي، بل أن هذا التوقيع الأخير قد لا يجد مكانا له في ظل المعالجة الالكترونية للمعلومات. وبالتالي المشكلة التي تثار في شأن حجية التوقيع الالكتروني في الإثبات ليس لها وجود في ظل صراحة النصوص التي تؤكد هذا التوقيع.

---

(1) ــ سكيل رقية، الإثبات بالتوقيع الإلكتروني بين التقنية المعلوماتية والنصوص القانونية، مداخلة مقدمة في الملتقى الوطني حول النظام القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، مرجع سابق، ص 12.

(2) ــ حنان براهيمي، مرجع سابق، 144.

المطلب الثاني: صور الاعتداء على التوقيع الالكتروني

يتناول هذا المطلب بيان صور الأفعال الإجراميّة التيّ تمسّ التّوقيع الإلكتروني، وذلك من خلال بيان منهج المشرّعين الفرنسي والجزائري في كفالة الحماية الجنائية له، وبيان مدى كفاية هذه الخطة في تجريم الأفعال التيّ تهدّد العمل بالتوقيع الالكتروني في مختلف المعاملات الإلكترونية خاصة الحكوميّة منها.

وعليه سنخصص الفرع الأوّل لجرائم الاعتداء على التوقيع الالكتروني في التشريع الفرنسي، أمّا الفرع الثاني يتضمّن جرائم الاعتداء على التّوقيع الالكتروني في التّشريع الجزائري.

الفرع الأول: جرائم الاعتداء على التوقيع الالكتروني في التشريع الفرنسي

أصدر المشرّع الفرنسي بتاريخ 13 مارس 2000 قانونا خاصا بالتوقيع الإلكتروني رقم 230 سنة 2000 في شأن تعديل قانون الإثبات في مجال تكنولوجيا المعلومات والمتعلق بالتوقيع الالكتروني السالف الذكر[1]، وقد أدرج هذا التعديل في نص المادة 1316 من القانون المدني الفرنسي في ست فقرات.

الملاحظ من خلال هذه النصوص أنه لم يورد قواعد خاصة بالحماية الجنائية للتوقيع الإلكتروني بل تركها للنصوص العامة، وبالرجوع إلى هذه الأخيرة تطبق عليها جرائم الإعتداء الواقعة على النظام المعلوماتي وبياناته الواردة في المواد 323 ــ1 ــ 323 ــ7 من قانون العقوبات الفرنسي، وجريمة التزوير المعلوماتي في المادة 441 من نفس القانون، وفيما يلي تفصيل لهذه الجرائم:

أولا ــ الاعتداء على النظام المعلوماتي للتوقيع الإلكتروني وبياناته:

من أبرز صور الإعتداء على النظام المعلوماتي للتوقيع الالكتروني هو الدخول إلى النظام والبقاء فيه بدون إذن، فضلا عن جريمة الإعتداء العمدي على النظام المعلوماتي الخاص بالتوقيع الإلكتروني.

---

[1] ــ انظر فيما سبق ص118 .

1 ــ جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي للتوقيع الإلكتروني:

نصّ المشرع الفرنسي على هذه الجريمة في المادة 323ــ1 من قانون العقوبات الفرنسي، ولقيامها ينبغي توافر ركنيها، المادّي يتمثّل في الدخول أو البقاء غير المشروع في قاعدة بيانات تتعلق بالتوقيع الإلكتروني، وتصنف هذه الجريمة من جرائم الخطر حيث يتمّ تجريم السلوك دون توقف ذلك على نتيجة معينة، فهي ليست من جرائم الضرر التي يشترط فيها إلحاق ضرر بالمجني عليه[1].

وتعدّ هذه الجريمة من الجرائم العمدية، وبالتالي لا يتصوّر وقوعها بطريق الخطأ، وصورة الركن المعنوي فيها هو القصد الجنائي العام.

2 ــ جريمة الإعتداء العمدي على النظام المعلوماتي للتوقيع الإلكتروني:

نصّ عليها المشرع الفرنسي في المادة 323ــ 2، ويتمثل الركن المادي لهذه الجريمة في التعطيل والتوقيف، أو بإفساده بأي وسيلة، ويعد ذلك أمرا منطقيا بالنظر لتعدد الوسائل وتميز الصبغة التقنية عليها حيث يصعب حصرها، وهي من الجرائم العمدية يتطلب فيها الأمر توافر القصد الجنائي العام بعنصرية العلم والإرادة، وهو ما يستفاد من نص المادة 323 ــ 2 فقرة 2 من قانون العقوبات الفرنسي.

وبالتالي إذا ترتب إفساد أو تدمير سير النظام عن خطأ أو إهمال، فلا وجود لجريمة، وكمثال لذلك الشخص الذي يستعمل أسطوانة تحتوي على فيروس مدمر، دون علمه بوجوده.

ثانيا ــ الإعتداء على بيانات التوقيع الإلكتروني:

نصّ المشرع الفرنسي على جريمة التلاعب ببيانات النظام المعلوماتي بموجب المادة 323 ــ2 من قانون العقوبات الفرنسي، ويتمثّل الركن المادي لهذه الجريمة في النشاط الإجرامي الذي يتكون من ثلاث أفعال هي الإدخال أو المحو أو تعديل بيانات التوقيع الإلكتروني.

أمّا الركن المعنوي لهذه الجريمة فيتمثل في القصد الجنائي العام، بعنصريه العلم والإرادة، ولا يشترط توافر القصد الخاص، بل يكفي القصد الجنائي العام لتحقق الركن المعنوي.

---

[1] ــ انظر فيما سبق ص 22.

ثالثا ــ تزوير التوقيع الإلكتروني:

جاء النّص على هذه الجريمة في المادة 441 من قانون العقوبات التي نصت على أنه: "يعد تزويرا كل تغيير تدليسي للحقيقة، يكون من شأنه إحداث ضررا، ويقع بأي وسيلة كانت، سواء وقع في محرر أو سند أيا كان موضوعه والذي أعد مسبقا كأداة لإنشاء حق أو ترتيب أثر قانوني معين".

لقيام هذه الجريمة لا بد من توافر ركنين مادي ومعنوي على النحو التالي:

يقوم **الركن المادي** لهذه الجريمة في فعل تغيير الحقيقة في توقيع إلكتروني بأي وسيلة، ومن أشهر وسائل تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة كسر الشفرة[1].

يرى بعض الفقهاء[2] أن التوقيع الإلكتروني لا يمكن تقليده، وإنما يمكن استعماله دون علم مالكه باعتباره يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، فيما يتم تزوير التوقيع التقليدي بتقليد توقيع شخص آخر مما يعني أن التوقيع ذاته مختلف عن التوقيع الخاص بصاحبه، وذلك لأن التوقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي وبالتالي لا يمكن أن يكون مماثل معه[3].

أمّا **الركن المعنوي**: يتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، فجريمة تزوير التوقيع الإلكتروني من الجرائم العمديّة، فيجب أن يعلم الجاني بوقائع الجريمة وكونها من المحظورات، ومع ذلك تتجه إرادته إلى الفعل المجرم.

---

(1) ــ شنين صالح، مرجع سابق، ص 239.

(2) ــ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص 554.

(3) ــ أمّا في جريمة تزوير التوقيع الإلكتروني فإنه يتم الحصول على منظومة التوقيع الإلكتروني الخاصة بشخص آخر، وبالتالي التوقيع الإلكتروني في حد ذاته صحيح لم يطرأ عليه تعديل أو تغيير، بل تم استخدامه دون رضا مالكه، حيث يكون الجاني قد تحصل على منظومة التوقيع الإلكتروني بطريق غير مشروع بنية استخدامها في توقيع وثائق معلوماتية. انظر: براهيمي حنان، مرجع سابق، ص 239.

الفرع الثاني: جرائم الاعتداء على التوقيع الالكتروني في التشريع الجزائري.

نظرا للانتشار الواسع للتوقيع الالكتروني في إطار المعاملات الإلكترونية التجارية، كان لابد من إقرار حماية جزائية ضدّ الاعتداءات التيّ يتعرّض لها التوقيع الالكتروني، لذا نظّم المشرع الجزائري حماية جنائية خاصة للتوقيع الالكتروني بموجب القانون رقم (15 ــ 04) المؤرخ في أول فبراير 2015، الذي يحدد القواعد العامة لتوقيع والتصديق الالكترونيين[1].

انطلاقا من المادتين 70 و71 من القانون رقم (15ــ04) السابق الذكر، يتضح أنّ هناك طائفة من الجرائم تقع اعتداء على التوقيع الالكتروني وهي محددة في المادتين، منها ما يمس بالبيانات الشخصية، فعملنا على إدراجها بصفة مستقلة في إطار الحماية الجنائية للبيانات الشخصية في التشريع الجزائري[2]، وفيما يلي سنتناول دراسة جرائم الاعتداء على التوقيع الالكتروني على النحو التالي:

أولاــ جريمة التصريح بإقرارات كاذبة:

تنصّ المادة 66 من قانون رقم (15 ــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين ما يلي: "يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفةّ .

يتطلب لقيام هذه الجريمة وفقا للمادة 66 من القانون السابق الذكر توافر ركنين، ركن مادي، وركن معنوي، فضلا عن تحديد الجزاء المقرر لمرتكب هذه الجريمة، وذلك على النحو الآتي:

أ ــ الركن المادي:

تتحقّق هذه الجريمة بالتصريح بإقرارات كاذبة، أي إعطاء معطيات غير صحيحة لمؤدي خدمات التصديق الالكتروني بغرض الحصول على شهادة تصديق إلكتروني موصوفة، ذلك أن هذه

---

(1) - خصّص المشرع الجزائري الفصل الثاني من الباب الرابع للأحكام الجزائية وذلك في المواد من 66 إلى 75 من القانون رقم (15 ــ04) المتضمن القواعد العامة المحددة للتوقيع والتصديق الالكترونيين السابق الذكر.

(2) ــ انظر فيما سبق ص 98 وما بعدها .

الأخيرة عبارة عن "**وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع**" [1]، وهي تمنح من قبل مؤدي خدمات التصديق الالكتروني لصاحبها بعد التحقق من بيانات التحقق الالكتروني[2]، أي بعد التأكد من هوية صاحب التوقيع الالكتروني وذلك بعد التصريح الصحيح بالبيانات الالكترونية التي تثبت علاقته بالتوقيع الالكتروني.

وعليه بمجرد التصريح بإقرارت كاذبة تقوم الجريمة، فهي من قبيل جرائم السلوك المجرد، وليست من جرائم الضرر، بمعنى أن المشرع لا يشترط لقيام الركن المادي فيها حلول ضرر معين، وإنما يكفي تحقق النشاط الإجرامي وهو التصريح بإقرارات كاذبة[3].

ب ــ الركن المعنوي:

جريمة التصريح بإقرارات كاذبة هي جريمة عمدية، تتطلب لقيامها القصد الجنائي العام بعنصريه العلم والارادة، فيجب أن يعلم الجاني أن ذلك الفعل محظورا قانونيا، ومع ذلك تنصرف إرادته إلى التصريح بإقرارات غير صحيحة، ومع ذلك يتقبل النتيجة المترتبة عن فعله، ولهذا لا يتصور وقوع الجريمة بطريق الخطأ لأن فعل الإعطاء ناتج عن قصد[4].

ولا تتطلّب هذه الجريمة لقيامها قصدا جنائيا خاصا، ولا حتى باعثا معينا من ارتكابها، سواء كان ذلك الإدلاء بإقرارات كاذبة لمؤدي خدمات التصديق الالكتروني بغرض العبث أو حتى من أجل الحصول على شهادة تصديق الكتروني موصوفة.

ج ــ العقوبة:

هدف المشرّع من تجريم هذا الفعل هو حماية المعاملات الالكترونية بمختلف أنواعها وفي مقدمتها التجارة الالكترونية، لاسيما الثقة المفترضة في هذه التجارة، وبالتالي فالعقاب عليها يؤدي إلى زيادة التعامل الالكتروني، لما يزرع الثقة لدى المتعاملين في هذه التجارة والحفاظ على

---

(1) ــ راجع الفقرة السابعة من المادة الثانية (2) من القانون رقم (15 ــ 04) المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

(2) ــ يقصد ببيانات التحقق من التوقيع الالكتروني وفق المادة الثانية (2) فقرة 5 من القانون رقم (15 ــ 04) بأنها: " رموز أو مفاتيح التشفير العمومية، أو أي بيانات أخرى، مستعملة من أجل التحقق من التوقيع الالكتروني".

(3) ــ شنين صالح، مرجع سابق، ص 181.

(4) ـ هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص 45.

حقوقهم[1]. لذلك وطبقا للمادة 75 من القانون رقم (15 ــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين السابق ذكره، عاقب على هذه الجريمة من خلال المادة 75 من القانون رقم (15ــ04) السالف الذكر، بعقوبة أصلية تتمثل في الحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة مالية تقدر من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، هذا إذا كان الجاني شخص طبيعي، أمّا إذا كان شخص معنوي فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، بمعنى يعاقب على هذه الجريمة بغرامة تقدر بـــمليون دينار (1.000.000 دج).

ثانيا ــ جريمة عدم إعلام السلطة الاقتصادية بوقف نشاط تأدية خدمات التصديق الالكتروني.

تنص المادة 67 من قانون رقم (15 ــ 04) السالف الذكر بأنه: "يعاقب بالحبس من شهرين (2) إلى سنة واحدة (1) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون".

يتطلب لقيام هذه الجريمة توافر ركنين، ركن مادي والثاني معنوي، وذلك وفق التفصيل التالي:

أ ــ الركن المادي:

يتمثّل السلوك الإجرامي في هذه الجريمة بتوقف مؤدي خدمات التصديق الالكتروني عن نشاط تأدية خدمات التصديق الالكتروني في الآجال المحددة في المادتين 58 و59 من القانون رقم (15 ــ 04) السابق الذكر، وبالرجوع للمادة 58 السابقة الذكر نلاحظ أنها تلزم مؤدي خدمات التصديق الالكتروني إعلام السلطة الاقتصادية للتصديق الالكتروني[2]، في الآجال المحددة في سياسة التصديق

[1] ــ عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية...، مرجع سابق، ص 290.

[2] - وهي إحدى سلطات التصديق المحددة قانونا بعد السلطة الوطنية والحكومية للتصديق الالكترونيين، يتم تعيينها من قبل السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية، وتتولى تأدية عدة مهام من أهمها: منح التراخيص لمؤدي خدمات التصديق الالكتروني بعد موافقة السلطة الوطنية للتصديق الالكتروني، التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الالكتروني بنفسها أو عن طريق مكاتب

لهذه السلطة، برغبته في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الالكتروني أو بأي فعل قد يؤدي إلى ذلك، أما المادة 59 من القانون السابق الذكر تلزم مؤدي خدمات التصديق الالكتروني الذي يوقف نشاطه لأسباب خارجة عن إرادته أن يعلم السلطة الاقتصادية للتصديق الالكتروني بذلك فور توقفه.

وبالتالي تقع هذه الجريمة بمجرد توقف مؤدي خدمات التصديق الالكتروني سواء بإرادته أو بغير إرادته عن نشاطه من دون تبليغ السلطة الاقتصادية للتصديق الالكتروني في الآجال المحددة لذلك، السبب في تجريم هذا الفعل هو الآثار الخطيرة المترتبة على وقف نشاط مؤدي خدمات التصديق الالكتروني، لأن ذلك يؤدي بالضرورة توقف المعاملات التجارية الالكترونية بسبب عدم إمكانية إصدار شهادة التصديق الالكتروني، الذي تعتبر ضرورية للتحقق من صفة الموقع وبالتالي إعطاء المصداقية للوثيقة أو المحرر الالكتروني.

ب ــ الركن المعنوي:

جريمة عدم إعلام السلطة الاقتصادية بوقف نشاط تأدية خدمات التصديق الالكتروني من الجرائم العمدية، لابد فيها من توافر القصد الجنائي العام، وذلك بأن يعلم الجاني وهو مؤدي خدمات التصديق الالكتروني أنه أخل بإلتزام إعلام السلطة الاقتصادية للتصديق الالكتروني بوقف نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون، ومع ذلك تتجه إرادته إلى هذا السلوك.

ج ــ العقوبة:

قرّر المشرع العقابي لمرتكبي هذه الجريمة إذا كان شخصا طبيعيا عقوبة الحبس من شهرين (2) إلى سنة واحدة (1) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط، أما بالنسبة للشخص المعنوي فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وهو ما

تدقيق معتمدة...، لمزيد من التفاصيل راجع المادة 30 وما بعدها من القانون رقم (15 ــ 04) المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

نصت عليه المادة 75 من هذا القانون، بمعنى يعاقب على هذه الجريمة بغرامة تقدر بـــ: خمسة (5) ملايين دينار (5.000.000 دج).

بالاضافة إلى هذا الجزاء الجنائي هناك جزاء إداري آخر وهو مانصت عليه الفقرة الثالثة من المادة 58 من القانون رقم (15 ــ 04) السابق الذكر[1]، يتمثل في سحب الترخيص، ويوقع على كل مؤدي خدمات التصديق الالكتروني لم يعلم السلطة الاقتصادية للتصديق الالكتروني في الآجال المحددة في سياسة التصديق لهذه السلطة، برغبته في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الالكتروني.

ثالثا ــ جريمة التعامل غير المشروع ببيانات إنشاء توقيع إلكتروني .

تنص المادة 68 من القانون الخاص بالتوقيع والتصديق الالكترونيين رقم (15 ــ 04) ما يلي: ''يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000 دج) إلى خمسة ملايين دينار (5.000.000 دج)، أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير''.

يتضح من خلال المادة 68 من القانون السالف الذكر أنه يتطلب لقيام هذه الجريمة توافر ركنين مادي يتمثل في حيازة، أو إفشاء، أو استعمال بيانات إنشاء توقيع إلكتروني، كما يتطلب فيها أيضا ركنا معنويا، وفيما يلي تفصيل ذلك:

أ ــ الركن المادي:

يتمثّل الركن المادي في هذه الجريمة في إتيان أحد الأفعال التالية: حيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير. ويقصد ببيانات إنشاء التوقيع الالكتروني حسب المادة 2 / 2 من قانون (15 ــ04) السالف ذكره أنها: "بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الالكتروني"، ومن المعلوم أن

[1] - تنص المادة 58 /3 من قانون (15ــ04) السابق الذكر ما يلي: " يترتب وقف النشاط سحب الترخيص"

هذه البيانات سرية لا يعلمها إلا صاحب التوقيع وهي مؤمنة من قبل آلية إنشاء التوقيع الالكتروني، باعتباره جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الالكتروني.

وعليه يتخذ السلوك الإجرامي إحدى الصور الآتية: حيازة أو إفشاء أو إستعمال بيانات التوقيع الالكتروني وذلك كما يلي:

ـــ **حيازة بيانات إنشاء التوقيع الالكتروني:** من المعلوم أن هذه البيانات سرية لا يعلمها إلا صاحبها وهو الموقع الشرعي، فبمجرد حيازة هذه البيانات من طرف الجاني سواء كان موظفا أو من غير ذلك، تقوم الجريمة حتى و لم يستعملها بطريق غير مشروع، وعليه هذه الجريمة من جرائم الخطر أو جرائم السلوك المجرد لا يشترط قيام الركن المادي فيها تحقيق نتيجة معينة.

أمّا فعل إفشاء بيانات التوقيع الالكتروني، يقصد بها نشر هذه البيانات واطلاع الغير عليها، بعد أن كان العلم بها قاصرا على من ائتمنوا عليها بحكم وظيفتهم، وانتهاك سرية هذه البيانات لا يقتصر على هذه الفئة بل بصفة عامة أي حتى مالم تقدم إليه أو اتصل بها بحكم عمله، وهي الأخرى من جرائم الضرر، حيث يتحقق الركن المادي للجريمة بمجرد انتهاك سرية البيانات، حتى ولو لم يترتب على الفعل نتيجة إجرامية معينة.

تتجسّد الصورة الثالثة في **فعل الاستعمال،** وهو استخدام الجاني لهذه البيانات بغرض استعمالها فيما بعد للحصول على شهادة التصديق الالكترونية من أجل إجراء معاملاته كالتجارة الالكترونية مثلا.

ب ـــ الركن المعنوي:

جريمة التعامل غير المشروع ببيانات التوقيع الإلكتروني من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصريه العلم والإرادة، فيجب أن يعلم الجاني بأن فعل حيازة أو إفشاء أو استعمال بيانات التوقيع الالكتروني محظور ومعاقب عليه قانونا، وأن تتجه إرادته للفعل المجرم.

لا تتطلّب هذه الجريمة قصدا خاصا، وإنما يكتفي بشأنها القصد الجنائي العام.

ج ــ العقوبة:

شدّد المشرّع الجزائري العقوبة في جريمة التعامل غير المشروع في بيانات إنشاء التوقيع الالكتروني، فهي تعدّ أشدّ الجرائم جزاء من بين جرائم الاعتداء على التوقيع الالكتروني، ويرجع سبب ذلك إلى غرس الثقة في التوقيع الالكتروني وبالتالي الثقة في المعاملات الالكترونية، ولذلك نصت المادة 75 من القانون (15ــ04) السابق الذكر بعقوبة الحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000 دج) إلى خمسة ملايين دينار (5.000.000 دج)، أو بإحدى هاتين العقوبتين فقط إذا كان الجاني شخصا طبيعيا، أمّا بالنسبة للشخص المعنوي فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، بمعنى يعاقب على هذه الجريمة بغرامة تقدر بـــ:خمسة وعشرون مليون دينار (25.000.000 دج).

رابعا ــ جريمة الإخلال بالتزام تحديد هوية صاحب شهادة التصديق الالكتروني:

تنصّ المادة 69 من القانون السالف الذكر أنه: ''يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة''.

لقيام هذه الجريمة يشترط توافر ركنيها الأساسين، المادي والمعنوي، بالإضافة إلى تحديد العقوبة المقررة لها وذلك في التفصيل التالي:

أ ــ الركن المادي:

بالرجوع إلى المادة 69 من القانون السابق الذكر، يتبين أن الركن المادي لهذه الجريمة يتحقق نتيجة عدم التحقق من هوية طالب شهادة التصديق الالكتروني، وهذا إلتزام يقع على عاتق مؤدي خدمات التصديق الالكتروني، حسب الفقرة الثانية من المادة 44 من القانون رقم (15ــ04) الذي يحدد القواعد العامة للتوقيع والتصديق الالكترونيين، فيجب على مؤدي خدمات التصديق الإلكتروني

أن يتحقق من هوية طالب التصديق الالكتروني، وحتى من صفاتها الخاصة عند الاقتضاء، وذلك قبل منح شهادة التصديق الالكتروني لطالبها أي لصاحبها، هذا إذا كان هذا الأخير شخصا طبيعيا، أما إذا كان شخصا معنويا ففي هذه الحالة يحتفظ مؤدي خدمات التصديق الالكتروني بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الالكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الالكتروني، وهو ما نصت عليه المادة 2/44 من القانون رقم (15 ــ 04) السابق الذكر.

يرجع السبب في تجريم المشرع لهذا الفعل، حتى لا تقع شهادة التصديق الالكتروني في يد أشخاص غير أصحابها ويستعملونها في معاملاتهم الالكترونية بطريقة غير مشروعة، لذلك يجب على مؤدي خدمات التصديق الالكتروني أن يتحقق من هوية طالب هذه الشهادة حتّى يتأكد من الهوية الحقيقية لصاحبها وذلك قبل منح شهادة التصديق الالكتروني.

تجدر الإشارة أن هذه الجريمة من جرائم السلوك المجرد، يكفي فيها تحقق السلوك المجرم وهو عدم التحقق من هوية طالب شهادة التصديق الالكتروني، بغض النظر عن النتيجة المترتبة بعد هذا الفعل أي استعمالها بصفة شرعية أم لا.

ب ــ الركن المعنوي:

جريمة الإخلال بالتزام تحديد هوية صاحب شهادة التصديق الالكتروني جريمة عمدية يقوم الركن المعنوي فيها على القصد الجنائي العام، فيتعين على مؤدي خدمات التصديق الالكتروني أن يعلم بأنه يمنح شهادة التصديق الالكتروني من غير التحقق من هوية طالبها، وأن هذا الفعل مجرم قانونا، ومع ذلك تتجه إرادته نحو ذلك السلوك.

ج ــ العقوبة:

تعاقب المادة 69 من القانون رقم (15 ــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين على جريمة الإخلال بالتزام تحديد هوية صاحب شهادة التصديق الالكتروني بعقوبة الحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20.000دج) إلى

مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، هذا بالنسبة للجاني إذا كان شخص طبيعيا، أما إذا كان الشخص معنويا فتعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، بمعنى يعاقب على هذه الجريمة بغرامة تقدر بـــ: مليون دينار (1.000.000 دج).

خامسا ـــ جريمة مباشرة خدمات التصديق الالكتروني دون الحصول على ترخيص:

جاء النص على هذه الجريمة في المادة 72 من القانون الخاص بالتوقيع والتصديق الالكترونيين على: "يعاقب بالحبس من سنة (1) واحدة إلى ثلاث (3) سنوات وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليوني دينار (2.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الالكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه. تصادر التجهيزات التي استعملت لارتكاب الجريمة طبقا للتشريع المعمول به".

من خلال نص المادة 72 من القانون السابق الذكر، يتبين أنه لقيام هذه الجريمة توافر ركنين، ركن مادي، والآخر معنوي، وذلك على نحو التفصيل الآتي:

أ ـــ الركن المادي:

يتمثل السلوك الإجرامي في هذه الجريمة، في انتحال الجاني صفة مؤدي خدمات التصديق الالكتروني المرخص له بخلاف الحقيقة، ويصدر شهادات تصديق الكتروني دون ترخيص بذلك من السلطة الاقتصادية للتصديق الالكتروني.

كما تقع الجريمة أيضا في حالة استئناف مؤدي خدمات التصديق الالكتروني أو مواصلة نشاطه بالرغم من سحب الترخيص. ذلك لأن ممارسة مؤدي خدمات التصديق الالكتروني لنشاطه في تأدية خدمات التصديق الالكتروني مرهون بضرورة حصوله على ترخيص من طرف السلطة الاقتصادية للتصديق الالكتروني، وهو ما نصت عليه المادة 33 من القانون رقم (15ـــ04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين[1].

[1] - تنص المادة 33 من القانون رقم (15 ـــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين على: "يخضع نشاط تأدية خدمات التصديق الالكتروني إلى ترخيص تمنحه السلطة الالقتصادية للتوقيع الالكتروني".

السبب في تجريم هذا الفعل هو الآثار الخطيرة المترتبة على شهادة التصديق الالكتروني في حق الغير، حيث يكون مضمونها التسليم بصحة بيانات التوقيع الالكتروني أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها[1].

جريمة مباشرة خدمات التصديق الالكتروني بدون الحصول على ترخيص من جرائم الخطر، حيث يكتمل الركن المادي فيها بمجرد إتيان الجاني لسلوك إصدار شهادة تصديق الكتروني بدون ترخيص، دون تطلب حصول ضرر بجهة ما أو شخص ما[2].

ب ــ الركن المعنوي:

هذه الجريمة من الجرائم العمدية، لابد فيها من توافر القصد الجنائي العام، وذلك بأن يعلم الجاني سواء كان من الغير بأن يقوم بإصدار الشهادة دون ترخيص، أما إذا كان مؤدي خدمات التصديق الالكتروني فيجب أن يعلم باسئناف أو مواصلة نشاطه بالرغم من سحب الترخيص، ومع ذلك تتجه إرادته نحو هذا السلوك المجرم قانونا.

ومن ثمة لا يتصور وقوع هذه الجريمة بطريق الخطأ بل يجب أن تنصرف إرادة الجاني إلى هذا الفعل، إنطلاقا من المادة 1/72 من القانون رقم (15 ــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين السالف الذكر.

ج ــ العقوبة:

قرّر المشرّع الجزائري لهذه الجريمة عقوبة أصلية تتمثل في الحبس من سنة (1) واحدة إلى ثلاث (3) سنوات وبغرامة من مائتي ألف(200.000) دينار إلى مليوني (2.000.000) دينار أو بإحدى هاتين العقوبتين فقط، هذا إذا كان الجاني شخصا طبيعيا، أما إذا كان شخصا معنويا وطبقا للمادة 75 من القانون السابق الذكر، فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى

---

[1] ــ شنين صالح، مرجع سابق، ص 173.

[2] ــ سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت، دار النهضة العربية، القاهرة، 2007، ص 167.

للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وبالتالي يعاقب في هذه الجريمة بغرامة تقدر بـــ : عشرة ملايين دينار (10.000.000 دج).

كما تصادر التجهيزات التي استعملت لارتكاب الجريمة وذلك طبقا للتشريع المعمول به.

سادسا ـــ جريمة الكشف عن معلومات سرية :

وُرِد النص على هذه الجريمة في المادة 73 من القانون السابق الذكر أنه:" يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق".

أ ـــ الركن المادي:

يشترط لقيام الركن المادي لجريمة الكشف عن معلومات سرية ضرورة أن يتم كشفها من قبل الشخص المكلف بالتدقيق وذلك أثناء قيامه بعملية التدقيق، حيث تلزم المادة 52 من القانون رقم (15 ـــ 04) السلطة الاقتصادية للتصديق الالكتروني بمراقبة مؤدي خدمات التصديق الالكتروني من خلال عمليات تدقيق دورية ومراقبات فجائية طبقا لسياسة التصديق للسلطة الاقتصادية ودفتر الأعباء الذي يحدد شروط وكيفيات تأدية خدمات التصديق الالكتروني، من أجل التحقق من مدى مطابقة أعماله مع ما يفترض الالتزام به والمحدد في دفتر الشروط، وتتم عملية التدقيق من خلال الاطلاع على المعلومات والتي تعد سرية خاصة بمؤدي الخدمات وأصحاب شهادة التصديق الالكتروني.

وعليه تقوم هذه الجريمة بمجرد كشف الشخص المكلّف بالتدقيق بانتهاك سرية البيانات التي قام بالاطلاع عليها بموجب تأدية وظيفته.

وعليه يمكن إدراج جريمة الكشف عن المعلومات السريّة من قبل الأشخاص المكلفين بالتدقيق مع جريمة الكشف عن الأسرار المهنية والمنصوص عليها في المواد من 311 إلى 303 قانون العقوبات الجزائري، حيث أنها تتضمن كشف معلومات سرية من طرف أشخاص تحصلوا عليها بمقتضى مهنتهم أو وظيفتهم.

ب ــ الركن المعنوي:

هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثّل في القصد الجنائي العام بعنصريه العلم والإرادة، فيجب أن يعلم الجاني وهو في هذه الجريمة الشخص المكلف بالتدقيق بأن كشف المعلومات السرية التي قام بالاطلاع عليها أثناء قيامه بالتدقيق محظور ومعاقب عليه قانونا، وأن تتجه إرادته للفعل المجرم.

لا تتطلب هذه الجريمة قصدا خاصا، وإنما يكتفي بشأنها القصد العام فقط، وبالتّالي متى تحقق الركن المادي والركن المعنوي وجب إنزال العقوبة على الجاني دون النظر إلى الباعث الذي دفعه إلى كشف معلومات سرية.

ج ــ العقوبة:

طبقا لنص المادة 75 من القانون رقم (15 ــ 04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين، يعاقب على هذه الجريمة بعقوبة أصلية تتمثل في الحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة مالية تقدر من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، أما إذا كان الشخص المكلف بالتدقيق شخصا معنويا فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وبالتالي يعاقب في هذه الجريمة بغرامة تقدر بـــ: عشرة مليون دينار (10.000.000 دج).

سابعا ــ جريمة إساءة استخدام شهادة التصديق الالكتروني:

تنصّ المادة 74 من القانون السالف الذكر أنه: "يعاقب بغرامة من ألفي دينار (2.000 دج) إلى مائتي ألف دينار (200.000 دج) كل شخص يستعمل شهادته للتصديق الالكتروني الموصوفة لغير الأغراض التي منحت من أجلها."

إذن يتطلب لقيام هذه الجريمة طبقا للمادة 74 من قانون رقم (15 ــ04) المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين السالف الذكر، توافر ركنين مادي يتمثل في استخدام شهادة التصديق الالكتروني في غير الغرض الذي قدمت من أجله.

كما يتطلب فيها أيضا ركن معنوي، فضلا عن تحديد الجزاء المقرر من طرف المشرع العقابي ضد مرتكب هذا السلوك الإجرامي، وذلك على التفصيل الآتي:

أ ــ الركن المادي:

يتمثل الركن المادي في هذه الجريمة في استعمال شهادة التصديق الالكتروني في غرض آخر غير ما قدمت من أجله، واقتصر المشرّع الجاني على صاحب شهادة التصديق الالكتروني دون غيره ممن يتصل بها بحكم عمله. ومعيار الغرض من استخدام شهادة التصديق الكتروني محدد في الشهادة ذاتها حيث تتوفر على عدة معطيات من بينها حدود استعمال شهادة التصديق الالكتروني، وحدود قيمة المعاملات التي قد تستعمل من أجلها هذه الشهادة وذلك وفق المادة 15 من قانون رقم (15 ــ 04).

ب ــ الركن المعنوي:

جريمة إساءة استخدام شهادة التصديق الالكتروني جريمة عمديّة، يلزم لقيامها القصد الجنائي العام، وذلك بعلم الجاني في استعمال شهادة التصديق الالكتروني لغير الغرض المخصص لها، ومع ذلك تتجه إرادته نحو هذا السلوك الإجرامي ويتقبل النتائج المترتبة عليه، ولا عبرة بالباعث الذي دفع الجاني إلى إساءة استخدام شهادة التصديق الالكتروني.

ج ــ العقوبة:

قرّر المشرع الجزائي عقوبة نوعا ما أخف مقارنة مع بقية الجرائم، حيث عاقب فقط بالعقوبة المالية دون عقوبة سالبة للحرية، وهي الغرامة من ألفي دينار (2.000 دج) إلى مائتي ألف دينار (200.000 دج)، هذا بالنسبة للجاني إذا كان شخصا طبيعيّا أما إذا كان شخصا معنويّا وطبقا للمادة 75 من القانون السابق الذكر، فيعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، والتالي يعاقب في هذه الجريمة بغرامة تقدر بـــ: مليون دينار (1.000.000 دج).

المبحث الثاني: جرائم الاعتداء على بطاقات الدفع الالكتروني

لم يقتصر دور الانترنت على استخدامه في الحكومة الالكترونية كوسيلة للإعلان عن الأنشطة الحكومية، وذلك بتوفير هذه المعلومات للمتعاملين معها، ونشر مختلف القوانين واللوائح على شبكة الانترنت، بل تعدت ذلك لتصبح طريقة سداد رسوم الخدمات الحكومية، حيث يمكن للشخص سداد المصاريف والرسوم كالضرائب مثلا عن طريق الوفاء الالكتروني.

تعدّ بطاقات الدفع من وسائل الدفع الحديثة التي ابتدعتها البنوك، فكانت بدايتها في الولايات المتحدة الأمريكية في مطلع القرن العشرين عام1913[1]، وتطوّرت فكرتها ونظامها حتى أصبح لها مكانة مهمّة بين أدوات الدفع الأخرى، لذا فمن الأهمية بمكان تعريفها، حيث إنّ بيان ماهية بطاقة الدفع يعد من المسائل الأولية التي يجب حسمها حتى يمكن تحديد نطاق حمايتها جنائيا في ظل النصوص الحالية لقانون العقوبات أو القوانين الخاصة بذلك، وعليه سيتم تقسيم هذا المبحث إلى مطلبين كالتالي:

المطلب الأول: ماهية بطاقة الدفع الالكتروني.

المطلب الثاني: مضمون الحماية الجنائية الخاصة لبطاقة الدفع الالكتروني.

المطلب الأول: ماهية بطاقة الدفع الالكتروني

تطوّرت وسائل الدفع الالكترونية في إطار إجراء المعاملات الإلكترونية بمختلف أنواعها الإداريّة منها والتجاريّة نتيجة استخدام الحاسبات الآليات والانترنت في القطاع المصرفي، نظرا لما توفّره من سرعة وسهولة تسويّة المدفوعات وتقليص الحاجة إلى الاحتفاظ بالنقود السائلة[2] .

---

[1] ــ وذلك عندما أصدرت بعض الشركات الأمريكية العاملة في مجال البترول بطاقات معدنية لعملائها لتشويه مشترياتهم من منتجات هذه الشركات بواسطتها في نهاية كل مدة محددة، كانت هذه العملية داخلية إلى غاية 1950، وبعد ذلك توسعت دائرة استخدامها حيث أتيح لهم الحق في استعمالها لشراء كل احتياجاتهم المتنوعة، وكانت أول البنوك الأمريكية التي قامت بإصدارها هو بنك ناسيونال فرانكلين ــ بنيويورك. انظر: الخليل عماد علي، الحماية الجزائية لبطاقة الوفاء، دار وائل للطباعة والنشر، الطبعة الأولى، عمان، الأردن، 2000، ص 07.

[2] ــ فاطمة شعران، النظام القانوني لبطاقات الدفع الإلكتروني، مداخلة مقدمة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، مرجع سابق، ص 3.

بناء على ذلك سوف نتناول في هذا المطلب تعريف بطاقة الدفع الإلكتروني في الفرع الأول، وإلى أنواعها في الفرع الثاني.

الفرع الأول: تعريف بطاقة الدفع الالكتروني

تعدّدت التعاريف التيّ أعطيت لبطاقة الدفع الإلكتروني سواء من الناحيّة الشكليّة[1] أو القانونيّة وحتى الفقهيّة، وما يهمّنا في هذا المقام التعريف القانوني من خلال مختلف التشريعات وما ورد عن الفقهاء من مفاهيم، ذلك ما سنبينه فيما يلي:

أولاـــ التعريف القانوني لبطاقة الدفع الإلكتروني:

لقد تطرّق المشرّع الجزائري إلى بطاقة الدفع والسحب في المادة 543 مكرر23 من القانون التجاري الجزائري المعدل والمتمم بموجب قانون رقم 05 ــ 02 والتي تنصّ على ما يلي: "تعتبر بطاقة دفع كل بطاقة صادرة على البنوك أو الهيئات المالية المؤهّلة قانونا وتسمح لصاحبها فقط بسحب أو تحويل أموال، أمّا بطاقة السحب تعتبر كل بطاقة صادرة عن البنوك والهيئات الماليّة المؤهلة قانونا وتسمح لصاحبها فقط في سحب الأموالّ[2].

يؤخذ على هذه المادّة أنها جاءت سطحية، فالمشرّع لم يعرّف بطاقة الدفع والسحب، بل اعتبرها بطاقة صادرة عن البنوك أو مؤسسة مالية مؤهلة قانونا. كما نصّ في المادة 543 مكرر24 من القانون التجاري الجزائري السابق الذكر على أن الالتزام بالدفع المعطي بموجب بطاقة الدفع لا رجوع فيه ولا يمكن الاعتراض عليه إلا في حالة ضياع أو سرقة البطاقة المصرح بها قانونا أو في حالة

---

[1] ــ تتميز التعاريف الشكلية ببيان الخواص الشكلية التي تتميز بها جميع البطاقات الالكترونية ومنها بطاقة الدفع الالكتروني، فهي "مصنوعة من مواد بلاستيكية لها مواصفات كيميائية محددة، مادة كلوريد الفينيل غير المرئي ..غير المرن، مستطيلة الشكل أبعادها هي 8.572 سم للطول و5.403 سم للعرض ويبلغ سمكها حوالي 0,76ــ 0,80 ملم يطبع على وجهها بشكل بارز رقمها واسم حاملها وتاريخ صلاحياتها واسم شعار المنظمة العالمية الراعية للبطاقة والبنك المصدر لها، يوضع عليها غالبا صورة حاملها كوسيلة لضمان التعرف عليه حين استعمالها مع نموذج البطاقة وهو ذاته التوقيع المعتمد في البنك وذلك بخلفية البطاقة المخصصة للتوقيع الخاصة بصاحب البطاقة، بالإضافة إلى صاحب البطاقة والبطاقة ذاتها سواء رصيدها أو تاريخ انتهائها أو بداية استعمالها ورقم الهاتف البنك مصدر البطاقة". انظر: زرقان هشام، النظام القانوني لبطاقات الدفع الإلكتروني، مذكرة ماجستير، تخصص قانون أعمال، جامعة محمد خيضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، بسكرة، 2015ــ2016، ص 13.

[2] ــ الأمر رقم 75ــ59 المؤرخ في 26 سبتمبر 1975، المتضمن القانون التجاري الجزائري المعدل والمتمم بالقانون رقم 05 ــ 02 المؤرخ في 06 فيفري 2005، ج. ر.ج. ع 11، لسنة 2005 .

التسوية القضائية أو إفلاس المستفيد. أمّا عن الطبيعة القانونية لهذه البطاقات اعتبرها المشرّع الجزائري أوراقا تجارية إضافية إلى الأوراق التجارية الكلاسيكية كالسفتجة، الشيك...إلخ [1].

كما نجد أن المشرّع الجزائري تطرّق أيضا إلى وسائل الدفع الإلكتروني في قانون النقد والقرض رقم 03ـــ11، حيث نصت المادة 69 منه" تعتبر وسائل دفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل" [2].

وما يلاحظ على هذا النص أنه جاء واسعا ليشمل جميع وسائل الدفع سواء التقليدية أو الحديثة.

ممّا سبق، يتّضح أنّ التشريع الجزائرّي يفتقر لتعريف صريح ودقيق لوسائل الدفع الإلكتروني. وهو النهج المتبع عند بعض التشريعات المقارنة، كالتشريع التونسّي مثلا نجده قد اكتفى فقط بالإشارة إلى وسائل الدفع الإلكتروني، دون إعطاء تعريف لبطاقة الدفع الإلكتروني بحيث نصت المادة 2 من قانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية التونسي على أنه: "وسيلة الدفع الإلكتروني هي وسيلة التي تمكن صاحبها من القيام بعمليات الدفع المباشر عن بعد عبر الشبكات العمومية للاتصالات"[3].

نفس الشيء بالنسبة للمشرّع الأردني اكتفى هو الآخر بالإشارة إلى وسائل الدفع الإلكتروني دون إعطاء تعريف لبطاقة الدفع الإلكتروني، حيث نصّت المادة 21ـــ أ من قانون رقم (15) لسنة 2015 المتعلق بالمعاملات الإلكترونية على أنّه: "يعتبر تحويل الأموال بوسائل الكترونية مقبولة لإجراء الدفع "[4]، محددا في نفس المادة فقرة ‘‘ب’’ منه على أن البنك المركزي الأردني يحدد إجراءات عمل أنظمة الدفع الإلكتروني ومتطلباتها الفنية والنقدية.

---

[1] ـــ حابت أمال، مرجع سابق، ص117.

[2] ـــ الأمر رقم 03ـــ11 المؤرخ في 26 أوت 2003 المتعلق بالنقد والقرض المعدل والمتمم، ج.ر.ج، ع 52، لسنة 2003.

[3] ـــ القانون التونسي رقم 85 لسنة 2001 المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية. وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، مرجع سابق، ص 651 وما بعدها.

[4] ـــ قانون المعاملات الالكترونية الأردني رقم (15) لسنة 2015 المتعلق بالمعاملات الإلكترونية، راجع الموقع الالكتروني الخاص التتشريعات الأردنية، مرجع سابق.

أمّا المشرّع الفرنسي تطرّق إلى البطاقات الإلكترونية في المادة الرابعة (4) من القانون المتعلق بعمليات ومراقبة مؤسسات الائتمان رقم (84ـــ 46) المؤرخ في 1984/01/24 كوسيلة دفع[1]، وإلى غاية سنة 1991 أين صدر قانون رقم 91 ـــ 1382 بتاريخ 30 ديسمبر 1991 الخاص بحماية الشيكات وبطاقات الدفع المعدل للمرسوم الصادر في 30 ديسمبر سنة 1935.[2].

عرّف القانون السالف الذكر (91ـــ1382) بطاقة الدفع في المادة الثانية منه بأنها أداة تصدر من إحدى مؤسسات الائتمان، أو إحدى الجهات المنصوص عليها في المادة 08 من القانون رقم 84ـــ46 والصادر في 24 يناير 1984 الخاص بنشاط ورقابة مؤسسات الائتمان، وتسمح لحاملها بسحب أو تحويل النقود من حسابه[3]. وبعد إلغاء هذه المادة بموجب المادة الرابعة من المرسوم رقم2000 ـــ 1223 الصادر في 14 ـــ 12 ـــ 2000 ، لتُعرّف بطاقة الدفع فيما بعد في المادة L132-1 من قانون النقد والمالية سنة 2000 كالتالي: "أي بطاقة صادرة عن مؤسسة ائتمانية أو مؤسسة أو إحدى الجهات المنصوص عليها في المادةL.518-1، وتسمح لحاملها بسحب أو تحويل الأموال" [4].

ثانيا ـــ التعريف الفقهي لبطاقات الدفع الإلكتروني:

نظرا لتعدّد أطراف العلاقة التعاقدية الناشئة عن استخدام بطاقة الدفع الإلكترونية، تعدّدت في مقابل ذلك التعاريف التيّ قدّمها الفقهاء لهذه البطاقة[5].

---

(1) - Loi n° 84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de crédit

(2) ـــ بن عيمور أمينة، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة ماجستير، تخصص قانون الأعمال، جامعة قسنطيمة منتوري، كلية الحقوق، 2004ـــ 2006، ص 8 و9.

(3) - Article 2/1 de Loi n° 91-1382 du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement: « Constitue une carte de paiement toute carte émise par un établissement de crédit ou par une institution ou un service mentionné à l'article 8 de la loi n° 84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de crédit et permettant à son titulaire de retirer ou de transférer des fonds".

(4)- Article L132-1 de code monétaire et financier :"Constitue une carte de paiement toute carte émise par un établissement de crédit ou par une institution ou un service mentionné à l'article L. 518-1 et permettant à son titulaire de retirer ou de transférer des fonds".

(5) ـــ تتميز بطاقة الدفع الإلكترونية بأنها ثلاثية الأطراف، الطرف مصدر البطاقة، حامل البطاقة والتاجر ولكل طرف إلتزامات خاصة في هذه العلاقة الثلاثية. لمزيد من التفاصيل انظر: خشة حسيبة، وسائل الدفع الحديثة في القانون الجزائري، مذكرة ماجستير، تخصص قانون أعمال، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، قسم الحقوق، مسيلة، 2015ـــ2016، ص 19 وما بعدها.

حيث عرفها البعض[1] بأنها بطاقة خاصة يصدرها المصدر لعميله، تمكنه من الحصول على السلع والخدمات من محلات وأماكن معينة عند تقديمه لهذه البطاقة، ويقوم بائع السلع أو الخدمات بتقديم الفاتورة الموقعة من العميل إلى المصرف مصدر الائتمان فيسدد قيمتها له، ويقدم المصدر للعميل كشفا شهريا بإجمالي القيمة لتسديدها أو خصمها من حسابه الجاري طرفه.

كما يعرفها المجمع الفقهي لمنظمة المؤتمر الإسلامي[2] "بأنها مستند يعطيه مصدره لشخص طبيعي أو اعتباري بناء على عقد بينهما، يمكنه من شراء السلع والخدمات، ممن يعتمد المستند، دون دفع الثمن حالا، لتضمنه التزام المصدر بالدفع، ومن أنواع هذا المستند ما يمكن من سحب النقود من المصارف".

وبشأن الطبيعة القانونيّة لبطاقة الدفع، اختلف الفقهاء حولها: فهناك من يعتبرها نوع من النقود الإلكترونية لتتمّ تداولها إلكترونيا، وذهب رأي آخر إلى فكرة الوكالة، حيث يقوم بموجبها حامل البطاقة بتوكيل البنك في دفع ثمن السلعة أو الخدمة التي حصل عليها خصما من حسابه لديه، واتجه جانب آخر من الفقه إلى اعتبارها أداة وفاء بطبيعتها مثل الشيك[3].

الفرع الثاني: أنواع بطاقات الدفع الالكتروني

تتعدّد وسائل الدفع الالكترونية المستخدمة في المعاملات الالكترونية فهناك من تقوم على استخدام البطاقات اللدائنية (البلاستيكية)، ومنها ما تستند إلى مفهوم النقود الإلكترونية.

أولا ــ البطاقات اللدائنية (البلاستيكية):

يطلق على هذه الوسيلة المستحدثة في التعامل المالي عدة مسمّيات، فقد سمّيت ببطاقات الدفع الالكترونية وبطاقات الائتمان وبطاقة الاعتماد والنقود البلاستيكية، ويقصد بها البطاقة البلاستيكية

---

[1] ــ عبد الوهاب أبو سليمان، البطاقات البنكية الافتراضية والسحب المباشر من الرصيد، دار القلم، دمشق، دون تاريخ النشر، ص 27.

[2] ــ القرارات والتوصيات الصادرة عن المجمع الفقهي لمنظمة المؤتمر الإسلامي في دورته السابعة بجدة في المملكة العربية السعودية، من 07 ــ 12 ذي القعدة 1412هـ الموافق 09 ــ 14 أيار (مايو) 1992م، مجلة مجمع الفقه الإسلامي، الدورة السابعة، الجزء الأول، جدة، 1992، ص 543.

[3] ــ جهاد رضا الحباشنة، الحماية الجزائية لبطاقة الوفاء، دار الثقافة عمان، الأردن، 2008، ص 23.

التي تصدرها البنوك أو شركات متخصصة لعملائها كوسيلة بديلة للنقود[1]، وذلك بناء على عقد بينهما بهدف استعمالها بشكل متكرر في تسديد ثمن السلع ومقابل الخدمات للموردين، كما يتمكن بها حامل البطاقة أيضا من سحب النقود من المصارف[2]. ويتخذ هذا النوع من الوفاء بواسطة البطاقات البلاستيكية عدة تقسيمات: فمن حيث العلاقة التعاقدية إلى بطاقات إئتمانية (Credit Card) وبطاقات غير إئتمانية (Debit Card)[3]، ويمكن تقسيمها من حيث المزايا والإمتيازات التي تقدمها للعميل إلى البطاقة العادية (Classic Card) والبطاقة الذهبية (Gold Card).

من أحدث صور البطاقات البلاستيكية البطاقة الذكيّة (Smart Card)، وهي بطاقة لا تحتوي على النقد فقط بل تحتوي أيضا على المعلومات الشخصية الخاصة بالمستخدم كبيانات التأمين الصحي وبيانات رخصة القيادة وبيانات بطاقة الإئتمان ومعلومات الرصيد في البنك، ويمكن شحن هذا النوع من البطاقات عن طريق الصراف الآلي وكذلك الحاسب الشخصي[4]، ومن أحدث صورها بطاقة الموندكس (Mondex Card) ظهرت عام 1990 وأنتجتها مؤسسة ماستر كارد العالمية[5].

ثانيا ــ النقود الالكترونية:

تقوم فكرة النقود الالكترونية على محاولة خلق وتطوير نظام للدفع يمكن أن يقدم نموذجا بديلا عن للنقود السائلة، فهي نقود لا وزن لها ولا ثقل، وقد عرفها القرار الإرشادي الصادر عن البرلمان

---

(1) ــ خالد ممدوح إبراهيم، مرجع سابق، ص 137.

(2) ــ عدنان إبراهيم سرحان، الوفاء (الدفع) الالكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد في دبي في الفترة ما بين 10 ــ 12 مايو 2003، المجلد الأول، ص 275. منشور في الموقع التالي:

http://slconf.uaeu.ac.ae/prev_conf/2003/1.pdf تاريخ لإطلاع: 2017/09/26

(3) ــ فالبطاقة الائتمانية تعطي لصاحبها إئتمانا فعليا من البنك المصدر للبطاقة بحيث لا يلزم فورا بالسداد، وإنما له الحق في تسهيلات إئتمانية يتفق على شروطها من حيث وقت الخصم والمبلغ المسموح به ومواعيد الوفاء وغيرها، ومن أشهر هذا النوع بطاقة الفيزا، ماستر كارد، وأمريكان اكسبرس. في حين أن البطاقة غير الإئتمانية تسمح لحاملها بالوفاء بقيمة السلع والخدمات التي يحصل عليها بدلا من الوفاء النقدي، وذلك في حدود مبلغ معين دون أن يمنحه إئتمانا، ومن ذلك البطاقة الزرقاء في فرنسا، وبطاقة الفيزا إلكترون في دولة الإمارات. خالد ممدوح ابراهيم، مرجع سابق، ص 138.

(4) ــ دحية رباب، دراسة تحليلية لأداء أنظمة الدفع، حالة نظام الدفع المكثف في الجزائر، مذكرة ماجستير تخصص علوم قانونية، جامعة المسيلة، 2011ــ2012، ص 29

(5) ــ خالد ممدوح إبراهيم، مرجع سابق، ص 138.

والمجلس الأوربيين في 2000/09/18، بأنها: "كل قيمة نقدية تمثل دينا على مصدرها وتخزن على دعامات إلكترونية" [1].

يعرفها البعض بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدما وغير مرتبطة بحساب بنكي، وتحظى بقبول واسع من غير من قام بإصدارها، وتستعمل كأداة للدفع لتحقيق أغراض مختلفة" [2].

وعليه تقوم النقود الرقمية على فكرة قيام البنك بتحويل جزء من حساب أحد عملائه إلى عملات إلكترونية ذات أرقام وعلامات خاصة وبوحدات عملة صغيرة بعد تشفيرها على جهاز الكمبيوتر الخاص بالعميل من خلال برامج السوفت وير والذي يسمى المحفظة، وعند رغبة العميل في استخدام نقوده الرقمية يصدر أمر لجهاز الكمبيوتر الخاص به بتحويل قيمة السلع المشتراه إلى البائع، وعند وصول هذا الأمر عبر الانترنت إلى البنك مصدر النقود الرقمية، يقوم بخصم المبلغ من حساب العميل وتحويله للبائع سدادا لثمن المشتريات[3].

المطلب الثاني: مضمون الحماية الجنائية الخاصة لبطاقات الدفع الالكتروني

القانون الجزائري لم يتضمّن نصوصا خاصة ببطاقات الدفع، وبالتالي فإن المرجع في ذلك للقواعد العامة الواردة في قانون العقوبات سواء باعتبارها مالا أو محررا، بخلاف بعض التشريعات المقارنة حيث تضمّن التشريع الجنائي الأمريكي منذ عام 1984 نصّا خاصا تناول الاستعمال غير المشروع لبطاقات الدفع وذلك في المادة (1029) من القانون الفدرالي والمعدل عام 1994.

كما قرّر المشرّع الفرنسي حماية جنائيّة خاصّة لهذه البطاقات بموجب القانون رقم (91 ــ 1381) المؤرخ في 30/ 12/ 1991 السابق الذكر، حيث تضمنت نصوصه الإشارة إلى ثلاث جرائم تتعلق بالبطاقات الائتمانية هي: تقليد أو تزوير بطاقة وفاء أو سحب، والثانية استعمال

---

[1] ــ انظر القرار الإرشادي (0CE/46/200) المتعلق بنشاط مؤسسات النقد الإلكتروني، الجريدة الرسمية للمجموعة الأوربية بتاريخ 2000/10/27.

[2] ــ محمد إبراهيم محمود الشافعي، **النقود الإلكترونية (ماهيتها، مخاطرها وتنظيمها القانوني)**، مجلة الأمن والقانون، الصادرة عن شرطة دبي، العدد الأول، يناير، السنة الثانية، 2004، ص 75.

[3] ــ خالد ممدوح ابراهيم، مرجع سابق، ص 143,

أو محاولة استعمال لبطاقة وفاء أو سحب مقلدة أو مزورة مع العلم بذلك، والثالثة قبول الدفع عن طريق الوفاء ببطاقة مقلدة أو مزورة وهو على علم بذلك[1].

من القوانين العربية التي تصدّت لجرائم بطاقات الدفع القانون العماني، حيث نص في مدونته العقابية بالمادة (276) مكرر (3) على عقوبة السجن مدة لا تزيد على خمس سنوات وبغرامة لا تجاوز ألف ريال[2] على نفس الجرائم المنصوص عليها في التشريع الفرنسي.

كما تضمّن نظام مكافحة جرائم المعلوماتية السعودي في المادة الرابعة منه في الفقرة الثانية على عقوبة السجن لمدة لا تزيد على ثلاث سنوات، وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب فعل الوصول ـــ دون مسوغ قانوني ـــ إلى بيانات بنكية أو إئتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات[3].

وعليه إنّ دراسة الجرائم الواقعة على بطاقة الدفع الالكتروني تتطلّب بيان مختلف صور هذه الجرائم (الفرع الأول)، مع أخذ نموذج تشريعي تصدى لمثل هذا النوع المستحدث من الإجرام وهو التشريع الفرنسي (الفرع الثاني).

الفرع الأول: صور الجرائم الواقعة على بطاقات الدفع الالكتروني

إنّ التزايد المستمر في استعمال بطاقات الدفع، كبديل عن حمل النقود والشيكات، أصبحت ظاهرة قياسية في الوقت الحاضر، وأمام هذا الوضع تزايد الاستعمال الخاطئ الاحتيالي لهذه البطاقة، سواء من قبل الحامل الشرعي للبطاقة أو من طرف الغير خارج أطراف العلاقة التعاقدية.

على هذا الأساس سنتطرق في هذا الفرع إلى: مسؤولية حامل البطاقة الجنائية (أولا)، ثم مسؤولية الغير عن الجرائم التي يرتكبها (ثانيا).

---

[1] ـــ عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، 2014، ص 326.

[2] ـــ قانون مكافحة الجرائم الإلكترونية (مواد مستحدثة ضمن أحكام قانون الجزاء العماني) بسلطنة عمان2001، وذلك بموجب المرسوم السلطاني رقم(72) لسنة 2001، بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي.

[3] ـــ نظام مكافحة الجرائم المعلوماتية السعودية (2007)، الصادر بالمرسوم الملكي رقم م/ 17 وتاريخ 1423/03/08، بناء على قرار مجلس الوزراء رقم (79) وتاريخ 03،07/ 1423.

أولا ــ الاستعمال غير المشروع لبطاقة الوفاء من قبل حاملها:

يتحقّق ذلك عن طريق استعمالها بعد انتهاء مدة صلاحيتها، أو إلغاءها من البنك المصدر لها، أو بتجاوز حد السحب المسموح به.

ثار خلاف فقهي بخصوص تكييف أفعال الإساءة من قبل الحامل الشرعي لبطاقة الوفاء وذلك ما سنوضحه فيما يلي:

1 ــ استعمال بطاقة الدفع بعد انتهاء مدة صلاحيتها:

من المعلوم أن علاقة البنك مصدر البطاقة بالعميل علاقة عقدية، تنقضي بانتهاء المدة المتفق عليها، وعليه يجب على حامل البطاقة تسليمها لمصدرها، لكن قد يحتفظ بها ويستخدمها في السحب أو الوفاء بمشترياته على الرغم من انتهاء صلاحيتها[1].

في هذا الفرض، نجد اتجاه في الفقه لا يقر بتحقق جريمة النصب بحق من يستعمل بطاقة انتهت مدة صلاحيتها، حيث أن الكذب الصادر من الحامل ينصب على مدى صلاحية البطاقة لا الاقتناع بوجود دين وهمي، وتقديم البطاقة لا يكفي لتحقيق المناورة التي تقوم بالطرق الإحتيالية، ويمكن اكتشافه من التاجر بكل سهولة وذلك من خلال الإطلاع على تاريخ صلاحية البطاقة المدون عليها[2].

لذا يتحمل التاجر الضرر في حالة قبوله الوفاء باستخدام بطاقة منتهية الصلاحية[3].

أمّا في حالة التواطؤ بين التاجر وحامل البطاقة الشرعي على قبول الوفاء بالبطاقة منتهية الصلاحية وذلك للإضرار بالبنك، كأن يقوم التاجر بتقديم تاريخ عمليات الوفاء المنفذة، فهنا تتوافر الطرق الاحتيالية اللازمة لقيام جريمة النصب، فيسأل العميل بصفته فاعلا أصليا، ويعاقب التاجر كشريك له في جريمة النصب[4].

---

(1) ــ جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، مصر، 2003، ص 53.

(2) ــ عادل يوسف الشكري، الحماية الجنائية لبطاقات الدفع الالكترونية، مركز دراسات الكوفة، مجلة تصدر عن كلية القانون جامعة الكوفة، العدد 11 لسنة 2008، ص،90.

(3) ــ جهاد رضا الحباشنة، مرجع سابق، ص 131.

(4) ــ عمر سالم، الحماية الجنائية لبطاقة الوفاء، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، 1995، ص 79.

وقد ذهبت محكمة النقض الفرنسية في حكم صادر في 19 مارس 2014 إلى اعتبار تصرف استعمال الحامل لبطاقة منتهية الصلاحية سلوك مكونا لجريمة خيانة الأمانة على أساس "أن البطاقة بمثابة محرر يتم تسليمها إلى العميل على سبيل عارية الاستعمال ومن اجل وظيفة محددة وان استمرار التعامل بها على الرغم من إخطاره بسحبها من قبيل الاختلاس الذي يضر بالبنك"[1].

أمّا بالنسبة لموقف المشرّع الجزائري فلم تتضمن نصوص قانون العقوبات حكم استعمال حامل بطاقة الدفع والسحب منتهية الصلاحية، لكن يرى البعض أن هذه الواقعة ترتب المسؤولية العقدية كأصل عام، والمسؤولية الجنائية في حالة عدم ردها للبنك مصدر البطاقة، رغم مطالبته بردها كجريمة خيانة أمانة، وفي حالة تواطوءه مع التاجر فيسألان كلاهما عن جريمة نصب[2].

2 ــ الاستعمال غير المشروع لبطاقة الإئتمان الملغاة :

قد يحدث أن تصدر الجهة مصدرة بطاقة الائتمان قرارها بإلغاء بطاقة الائتمان السابق إصدارها لعميلها نتيجة تعسفه في استخدامها سواء بالسحب أو بالوفاء، أو نتيجة لعدم تسديده لمديونياته في الموعد المتفق عليه في العقد، **فما هو التكييف القانوني لهذه الجريمة ؟**

في هذه الحالة يجب التمييز بين الفرضين التاليين:

الفرض الأول: الإمتناع عن رد بطاقة الائتمان المنتهية صلاحيتها:

إذا انتهت صلاحية البطاقة سواء لإلغائها أم لانتهاء مدتها وطلب المصدر (البنك) من حامل البطاقة الإئتمانية تسليم البطاقة التزم حاملها بردها إلى مصدرها لأنها سلمت إليه كعارية استعمال، وهو أحد عقود الأمانة، ويكفي لتوافر الاختلاس أن ينكر حامل البطاقة وجود هذه البطاقة في حيازته لكي يتخلص من التزامه بالرد، ولا يشترط استعمالها رغم مطالبته البنك بها أو سحبها[3].

---

(1) -Arrêt n° 1193 du 19 mars 2014 (12-87.416) de la Chambre criminelle disponible en ligne cour de cassation : https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/dite_societe_28730.html

(2) - شنين صالح، مرجع سابق، ص 145.

(3) ــ جميل عبد الباقي الصغير، مرجع سابق، ص 78.

وهو ما نصّت عليه المادة (3/2) من الشروط العامة لعقد البطاقة المصرفية الصادرة عن اعتماد ليون بنصها على أن " تبقى البطاقة ملكا للمؤسسة المصدرة لها التي تملك حق سحبها في أي لحظة أو عدم تجديدها...ويلتزم حامل البطاقة بناء على ذلك بردها بمجرد أول طلب لها، ويتعرض للجزاءات إذا استمر في استعمالها بعد إعلانه بسحب البطاقة بخطاب عادي"[1]

في حين يرى البعض عدم تحقق أي جريمة في هذه الحالة، لأن إظهار البطاقة ليس كافيا بتحقق طرق إحتيالية، وهي تحتاج إلى مظاهر خارجية مدعمة للقول بصحة الأكاذيب، وتتحقق هذه الأخيرة في حالة تواطؤ التاجر مع حامل البطاقة في النشاط الإجرامي، مثل وجود فواتير غير سليمة التاريخ أو مذيلة بتوقيع غير مطابق[2] .وهو ما قضت به محكمة استئناف باريس في حكم لها صادر بتاريخ 17 أكتوبر عام 1991، حيث أدانت التاجر للإشتراك في جريمة النصب بمساعدة الفاعل الأصلي على الوفاء ببطاقات إئتمانية غير صالحة مع علمه بذلك[3].

الفرض الثاني: استخدام الحامل الشرعي للبطاقة بعد إلغائها:

هذا الفرض يمكن أن يتحقق في الحالتين:

الأولى وهي استخدام بطاقة الإئتمان الملغاة في سحب النقود، وهذا لا يشكل أية جريمة أو حتى الشروع فيها، لوجود استحالة مادية تتمثل في عدم استجابة جهاز الصراف الآلي لطلبه، إما بسحب البطاقة من قبل الصراف الآلي أو عدم إتمام العملية[4].

أما الحالة الثانية: تتمثل في استخدام بطاقة الإئتمان الملغاة في الوفاء، وذلك في حالة في قيام الحامل الشرعي للبطاقة بعد علمه بالغائها من قبل البنك بشراء سلع أو خدمات عبر شبكة

---

(1) - لمزيد من التفاصيل انظر: Conditions Générales CIC Clients particuliers **في الموقع التالي:**

https://www.cic.fr/fr/banques/telechargements/CIC_Convention-de-comptes_Conditions-generales_07-2014.pdf تاريخ الاطلاع: 2016/05/01

(2) - عمر سالم، مرجع سابق، ،ص 61.

(3) - Chambre commerciale, 26 février 2008 (Bull. n° 42, pourvoi n° 07-10.761) disponible sur site suivant:
https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2008_2903/quatrieme_partie_jurisprudence_cour_2922/activites_economiques_commerciales_financiers_2952/droit_bancaire_12230.html تاريخ الاطلاع: 2016/05/01

(4) ــ جهاد رضا الحباشنة، مرجع سابق، ص 129.

الانترنت،واستخدام البطاقة الملغاة في الوفاء للتجار يشكل جريمة نصب حيث أنّ مجرد تقديم البطاقة إلى التاجر يهدف إلى الإقناع بوجود ائتمان وهمي لا وجود له في الواقع وليس مجرد كذب، خاصة وانّ إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان بالإضافة إلى تحقق عنصر التسليم الذي يتمثل في قيام التاجر بتسليم المشتريات إلى الحامل الشرعي للبطاقة[1].

وقد أخذت محكمة جنح باريس بهذا الرأي، في حكم لها صادر في 16 أكتوبر 1984 وقضت بإدانة الحامل الشرعي لبطاقة الإئتمان بتهمة جنحة النصب لقيامه بتقديم بطاقة مجردة من أي قيمة، لأنها ملغاة بواسطة البنك مصدرها، وذلك بهدف الإقناع بوجود دين وهمي، والحصول من البنك على الوفاء للتاجر الذي قدم سلعا لحامل البطاقة مما يشكل إستيلاء على بعض ثروة الغير[2].

3 ــ تجاوز حامل البطاقة الرصيد المسموح به:

يتحقّق هذا الفعل غير المشروع في حالة تعسّف حامل البطاقة لاستعمالها، ويتخذ ذلك إحدى الصورتين: السحب من جهاز توزيع العملة رغم عدم وجود رصيد كاف له، أو الحصول على سلع وخدمات تتعدى المبلغ الذي حدده مصدر البطاقة. وفيما يلي تفاصيل ذلك:

أ ــ الصورة الأولى: السحب من جهاز توزيع العملة رغم عدم وجود رصيد كاف له، وفي هذه الحالة تضاربت آراء الفقهاء في إسناد المسؤولية الجنائية بين مؤيد لذلك ورافضا لها نهائيا.

ــ بالنسبة لإقرار المسؤولية الجنائية لحامل بطاقة الائتمان: اختلفت آراء الفقهاء حول تكييف النشاط الذي صدر من حامل بطاقة الائتمان، فهناك من يرى معاقبته عن جريمة السرقة، وهناك من يرى مساءلته عن جريمة النصب، والبعض الآخر يرى مساءلته عن جريمة خيانة الأمانة[3].

نظرا لعدم تصور تطبيق هذه الصورة في الواقع العملي، بسبب التطور الحاصل في المجال الإلكتروني في برمجة الأجهزة الآلية لتوزيع النقود، حيث برمجت على سحب البطاقة في حالة ما إذا

---

(1) ــ سليمان أحمد فاضل، مرجع سابق، ص 174 ــ 175.

(2) -T.corr ,Paris16 octobbre 1974,J .C.P , ed 1967, p . 129.

(3) ــ أحمد سفر، أنظمة الدفع الإلكترونية، منشورات الحلب الحقوقية، ط 1، لبنان، 2008، ص 170.

أصبحت غير صالحة للاستعمال، وكذلك الامتناع عن صرف نقود تتعدى الرصيد المسموح به لصاحبها[1].

ـــ وفيما يتعلق بالاتجاه الرافض لإقرار مسؤولية حامل البطاقة جنائيا: فيرى هذا الجانب أن هذا الفعل لا يتعدى كونه إخلالا بأحد الاتتزامات التعاقدية التي قد تمنح مصدر البطاقة الحق في اتخاذ إجراءات إدارية كسحب البطاقة، أو ترتب مساءلته مدنيا إذا توافرت شروطها[2].

ب ـــ الصورة الثانية: الوفاء بقيمة السلع والخدمات رغم عدم وجود رصيد كاف، في هذه الحالة لا يوف المشتري بقيمة السلع والخدمات التي حصل عليها نقدا بل عن طريق بطاقة الائتمان الخاصة به، وفي هذه الحالة يحل المصدر لها محله في الوفاء بقيمة عملياته هذه ليقوم بعد ذلك بالسداد إلى البنك مستفيد من الفترة الممنوحة له على سبل الائتمان، وبعد ذك يكتشف التاجر والبنك عدم وجود رصيد كاف لحامل البطاقة لتغطية قيمة هذه العملية التجارية. فهل ينطوي هذا الفعل على جريمة ؟ في هذه الحالة نميز بين إتجاهيين[3]:

ـــ الأول: يرى مساءلة حامل البطاقة جنائيا عن جريمة نصب، بينما يرى الاتجاه الثاني: عدم انطواء هذه الواقعة عن جريمة في ضوء نصوص قانون العقوبات، وأنها لا يتعدى كونها مجرد إخلال بالتزاماته التعاقدية مع مصدر البطاقة.

ثانيا ـــ الاستعمال غير المشروع لبطاقة الدفع من قبل الغير:

يقصد بالغير هنا من لم تصدر البطاقة باسمه من الجهة المختصة بإصدارها، فإذا استعملها كان استعماله هذا غير مشروعا، ويتحقق ذلك إما باستخدام بطاقة مسروقة أو مفقودة، أو تزوير البطاقة واستخدامها على نحو غير مشروع، وذلك على التفصيل الآتي:

---

[1] ـــ محمود أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الإئتمان، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، مرجع سابق، ص1132.

[2] ـــ محمد أبو العلاء عقيدة، القانون الجنائي في مواجهة إساءة استخدام بطاقة الإئتمان، موجز للتقرير المقدم بالفرنسية للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25 ـــ 28 اكتوبر 1993، ص 7.

[3] ـــ محمود أحمد طه، مرجع سابق، ص 1133.

1 ــ الاستعمال غير المشروع لبطاقة مسروقة أو مفقودة:

تتمثل هذه الحالة في قيام شخص بسرقة هذه البطاقة من مالكها الأصلي أو العثور عليها في حال فقدها من مالكها الشرعي.

يتعيّن على حاملي البطاقات في حالة سرقتها أو ضياعها إخطار الجهة المصدرة لها وأيضا إخطارها عند ضياع أو سرقة الرقم السري الذي لا يمكن استعمال البطاقة بدونه إن حدث ذلك[1].

فإذا قام صاحب البطاقة بإخطار الجهة المصدرة للبطاقة بضياعها أو سرقة الرقم السري الخاص بها أصبحت هذه الجهة مسؤولة بعد الإخطار. وفي هذه الحالة تقوم الجهة مصدرة البطاقة بوقف تشغيل البطاقة والرقم السري[2]. ولكن المشكلة تثور بشأن تكييف السلوك الذي يرتكبه الغير.

في هذه الحالة يجب التمييز بين الفروض التالية:

الفرض الأول: استعمال الغير بطاقة مسروقة أو مفقودة لسحب النقود:

عمليا يصعب تصور هذه الصورة نتيجة برمجة الأجهزة الآلية لحماية بطاقة الائتمان من استعمالها من غير صاحبها حيث تمنحه ثلاث فرص لتجربة الرقم السري، فإذا جربت المرة الثالثة و لم يكن الرقم صحيحا قامت الآلة بسحب البطاقة.

و لم تثر هذه الحالة خلافا حول التكييف القانوني لها، حيث استقرّ الرأي أنّ الواقعة تشكل جريمة نصب، واستبعدت السرقة إلا في حالة قيام الجاني بعملية سرقة البطاقة ورقمها السري، وبالتالي يكون الجاني قد ارتكب جريمتين مستقلتين وهما السرقة كجريمة وسيلة والنصب كجريمة غاية[3].

الفرض الثاني: استعمال بطاقة مسروقة أو مفقودة كأداة وفاء:

إنّ استعمال البطاقة في هذه الحالة أيسر من الحالة السابقة، حيث لا يقتضي الأمر في كثير من الحالات معرفة الرقم السري للبطاقة، بل تتم المعاملة بتوقيع حامل البطاقة على فاتورة الشراء، ومن ناحية أخرى لا يمكن اكتشاف تزوير التوقيع من قبل البائع لعدم خبرته.

---

[1] ــ محمد سامي الشوا، المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية للكتاب، القاهرة، 2003، ص 118.

[2] ــ نائلة عادل محمد فريد قورة، مرجع سابق، ص539.

[3] ــ نفس المرجع، ص 541.

وقد استقرّت العديد من الأحكام القضائية الفرنسية على معاقبة من يستخدم بطاقة مسروقة أو مفقودة في الوفاء بجريمة النصب، على أساس انتحال الجاني اسما كاذبا مما يسوغ القول معه أنه استخدم وسيلة إحتيالية يتوسل بها لإقناع المجني عليه (التاجر) بأن هناك إئتمانا موجودا[1].

أمّا إذا سُرقت البطاقة مع الرقم السريّ الخاص بها و لم يُبلّغ صاحبها بضياعها أو سرقتها، فإنّه يتحمّل مسؤولية المبالغ التّي يتمّ سحبها بموجب هذه البطاقة[2].

2 ــ تزوير بطاقة الإئتمان:

الفرض هنا أن الجهة المختصة بإصدار بطاقة الإئتمان التي استعملت سواء في السحب أم في الوفاء لم تصدرها، وإنما قام الغير بتزويرها أو بتقليدها، **فما هو التكييف القانوني لهذه الجريمة؟**

ــ لقد ثار خلاف فقهي بشأن تطبيق أحكام جريمة التزوير على بطاقات الإئتمان، بين اتجاه رافض لتطبيق النصوص التقليدية لجريمة تزوير البيانات الإلكترونية، ومنها بيانات بطاقة الإئتمان، بحجة عدم إمكانية القراءة البصرية لمحتويات هذه المحررات الإلكترونية إلا بواسطة الحاسوب والتزوير يفترض تغييرا في علامات أو رموز مرئية[3]. أمّا الاتجاه الثاني، فيرى أصحابه قيام جريمة التزوير في حالة تغيير بيانات بطاقة الإئتمان، استنادا إلى أن المعلومات المعالجة إلكترونيا متى دونت على اسطوانات أو شريط ممغنط تعتبر محررا، وإن كان من غير الممكن قراءته بصريا، إلا أنه يمكن قراءته عن طريق الحاسوب، وبالتالي فإن تغيير الحقيقة في هذه المحررات الالكترونية يؤدي إلى قيام الركن المادي لجريمة التزوير[4].

وقد حسم هذا الخلاف الفقهي التدخّل التشريعي، حيث نصّت بعض القوانين على التزوير المعلوماتي بتعديل نصوصها القائمة، كما هو الحال في التشريع الكندي الصادر عام 1985، والتشريع الاسترالي لعام 1983، أو بإصدار نصوص خاصة، كما هو الحال بالنسبة للمشرع

---

(1) Cass, crim,3 fevr 1970, Bull, crim, 1970, n° 47, p. 109.

(2) ــ فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق، ص 159.

(3) ــ حماد رضا الحباشنة، مرجع سابق، ص 72.

(4) ــ نائلة قورة، مرجع سابق، ص 586.

الفرنسي[1]، الذي استحدث قانون أمن الشيكات وبطاقات الوفاء رقم (1382/91) لسنة 1991، والتعديلات اللاحقة التي أدخلت عليه بموجب قانون رقم 2007 ــ 1544، حيث كفل حماية جنائية خاصة لبطاقة الوفاء عن التقليد والتزوير، واستعمال البطاقة المقلدة أو المزورة، وقبول الدفع ببطاقة الوفاء على الرغم من علمه بتقليد البطاقة أو تزويرها، بموجب المادة 1331/67 من القانون السابق ذكره[2].

3 ــ استعمال بطاقة إئتمان مزورة:

في إطار غياب النصوص القانونية الناظمة للجرائم التي تتعرض لها بطاقة الإئتمان بشكل عام في كثير من البلدان والعربية على وجه الخصوص[3]، واستنادا إلى ما تتطلبه استعمال البطاقة في الوفاء بالمشتريات والحصول على الخدمات، اختلف الفقه حول نوع الجريمة التي يسأل عنها، فهناك من يرى مساءلته عن جريمة سرقة باستعمال مفتاح مصطنع، وهناك من يرى مساءلته عن جريمة نصب، وهناك من يرى مساءلته عن جريمة استعمال محرر مزور، وذلك على النحو التالي[4]:

أ ــ جريمة سرقة باستعمال مفتاح مصطنع:

يرى هذا الاتجاه أن هذه الواقعة تشكل جريمة سرقة مشددة باستعمال مفتاح مصطنع، لأن المال خرج من ذمة صاحبه دون رضاه، والمفتاح المصنع في هذه الحالة هو البطاقة المزورة، على أساس أن هذا الأخير هو كل أداة تقوم بذات الوظيفة التي يقوم بها المفتاح بغض النظر عن شكلها أو حجمها أو المادة المصنوع منها، خاصة وأن البطاقة في حقيقتها مجرد أداة للوصول إلى سحب النقود من الحساب[5].

---

[1] ــ أنظر فيما سيأتي، ص 169.

[2] ــ صالح شنين، مرجع سابق، ص 149.

[3] ــ تدخلت بعض تشريعات الدول بنصوص صريحة، يجعل من تزوير بطاقة الائتمان واستعمالها جرائم كما فعل المشرع الفرنسي في المادة 2/67 من قانون رقم (1382/91) المتعلق بأمن الشيكات وبطاقة الوفاء سابقا والمادة 3/163 من قانون النقد والمالية لسنة 2000. وكذا المشرع العماني في المرسوم السلطاني رقم (72) لسنة 2001، بشأن تعديل بعض أحكام قانون الجزاء العماني في مادته 276 مكرر3.

[4] ــ جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الإئتمان، مرجع سابق، ص 109.

[5] ــ هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992، ص 134.

وقد اعترض غالبية الفقه ـــ وهو ما نؤيده ـــ على اعتبار أن هذه الواقعة (استعمال بطاقة إئتمان مزورة) سرقة باستعمال مفتاح مصطنع، واستندوا في ذلك إلى أن تسليم النقود تم إراديا من قبل الجهاز الآلي لتوزيع النقود بمجرد إدخاله البطاقة في الآلة وكتابة الرقم السري لها. فضلا عن أن البطاقة لا تعد مفتاحا مصطنعا لأن هذا المفتاح هو الذي يستخدم للدخول في المكان الذي يرتكب فيه جريمة السرقة، هو ما لا يتوافر في بطاقة الإئتمان، وإنما هي فقط أداة الجريمة نفسها، كما لا يجوز القياس في النصوص التجريمية[1].

ب ـــ جريمة نصب:

إذا قام أحد الأفراد باستعمال بطاقة إئتمان مزورة في سحب النقود من الجهاز الآلي أوفي الوفاء بقيمة عملياته التجارية، فإنه يعد مرتكبا لجريمة نصب، وهو ما ذهب إليه بعض الفقه والقضاء مستندين في ذلك إلى استعمال البطاقة المزورة بمثابة استخدام طرق إحتيالية لخداع الجهاز الآلي الذي يقوم بسحب النقود أو لإيهام التاجر بوجود إئتمان بهدف الحصول على السلع والخدمات[2].وهو ما قضت به محكمة (sRenne) بأن استخدام البطاقة المزورة يشكل جريمة نصب[3]، وعلى عكس ذلك قضت محكمة (Lille) بأنّ هذا الفعل لا يشكل جريمة نصب، لأن الطرق الإحتيالية تتم بين شخصين الجاني والمجني عليه، بينما في هذه الحالة العلاقة بين شخص وشئ وهو الجهاز[4].

ولكن قضت محكمة النقض الفرنسية بأن الجهاز الآلي لتوزيع النقود يمكن خداعه لأنه يوجد خلف كل جهاز صاحبه (موظف البنك)[5].

---

[1] ـــ عمر سالم، مرجع سابق، ص 38.

[2] ـــ جميل عبد الباقي، مرجع سابق، ص 955.

[3] -Jeandidier Wilfrid, les truquage et usages frauduleux de carte magnétique, J.C.P , doctr 3229, 1986. مشار إليه عند محمد نائلة قورة، مرجع سابق، ص 537.

[4] - Crim, cass, 16 juin 1986, Revue de droit intrnational des systemes éléctronique de paiment, 1987, n° 18, p. 9.

[5] ـــ جميل عبد الباقي، مرجع سابق، ص 111.

ج ــ جريمة استعمال محرر مزور:

يرى جانب من الفقه أنّ هذه الواقعة تعد جريمة استعمال محرر مزور وفقا لنصوص قانون العقوبات[1].

أخذ بهذا الرأي المشرّع الفرنسي، حيث عاقب على جريمة استعمال محرر مزور في قانون الغش المعلوماتي لعام 1988 بموجب المادة 6/462، وفي قانون العقوبات الجديد المعمول به حاليا سنة 1994 بموجب المادة 1/441، وجاءت هذه الحماية الجنائية عامة، على خلاف قانون 1382/91 الصادر عام 1991 المتعلق بأمن الشيكات وبطاقة الوفاء، والذي جاء بحماية جنائية خاصة لبطاقات الوفاء من التزوير واستعمال محرر مزور، حيث عاقب على جريمة استعمال محرر مزور في المادة 2/67 سابقا والمادة 3/163 من قانون النقد والمالية لسنة 2000[2].

يصادف في هذه الجريمة أن الذي قام بتزوير بطاقة الإئتمان هو نفسه الذي قام باستعمالها فيما زورت من أجله (سواء بالسحب أم بالوفاء). في هذه الحالة نكون إزاء تعدد في الجرائم، جريمة تزوير وكذلك جريمة استعمال المحرر المزور. وهذا التعدد قد يكون معنويا وذلك إذا تم التزوير والاستعمال بفعل واحد، كأن يوقع المتهم على الفواتير لدى أحد التجار، فالتوقيع تزوير واستعمال للبطاقة في نفس الوقت، وفي هذه الحالة يعاقب على الجريمة ذات الوصف الأشد. كما قد يكون تعددا ماديا متى ارتكب الجريمة بفعلين مستقلين. وهذا التعدد قد يكون مرتبطا ارتباطا غير قابل للتجزئة وذلك متى ارتكبت الجريمتين لغرض واحد مثل تغير اسم صاحب البطاقة واستعمالها، كما يكون ارتباطا بسيطا، إذا لم يكن لغرض واحد كاستعمال البطاقة المزورة لتحقيق أغراض لم تكن في ذهنه وقت تزويره البطاقة[3].

---

(1) ــ عمر سالم، مرجع سابق، ص 37. وانظر أيضا:

Gavala (c), le droit pénal des cartes magnétique ,et/ou crédit,p,1994 ,dalloz 94 .92 .

(2) ــ انظر في تفاصيل الجريمة ص 169 وما بعدها .

(3) ــ كيلاني محمود، النظام القانوني لبطاقة الوفاء والضمان، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1996، ص 856 ــ 857.

الفرع الثاني: الحماية الجنائية لبطاقة الدفع الالكتروني في التشريع الفرنسي

نصّ المشرّع الفرنسي على حماية جنائية خاصة لبطاقة الدفع في المادة الحادية عشر من قانون (91 ــ 1882) والتي عدلت المادة 67 من المرسوم بقانون 30 أكتوبر 1935، المحدد لقواعد التعامل بالشيك والمرتبط ببطاقات الدفع، إذ تنص هذه المادة على إدخال المادتين 1/67، و2/67 بعد المادة 67 من هذا القانون الأخير.

وفقا للمادة 1/67 من القانون السابق الذكر، يعاقب بالعقوبات المنصوص عليها في المادة 67 (الحبس من سنة واحدة إلى سبعة سنوات والغرامة من 3600 فرنك حتى 5000000 فرنك، أو بإحدى هاتين العقوبتين فقط:

1 ــ كل من قام بتقليد أو تزوير بطاقات الوفاء أو السحب.

2 ــ كل من استعمل أو حاول استعمال البطاقة المقلدة أو المزورة وهو عالم بذلك.

3 ــ كل من قبل الدفع ببطاقة الوفاء على الرغم من علمه بتقليد البطاقة أو تزويرها.

أمّا المادة 2/67 فإنه في الحالات السابقة يتعين مصادرة وتدمير الشيكات والبطاقات المقلدة أو المزيفة، وكذلك مصادرة المواد والماكينات والمعدات أو الأدوات التي استخدمت أو التي كانت متجهة إلى الاستخدام في التزييف أو التقليد، إلا إذا استخدمت بدون علم المالك.

بصدور قانون النقد والمالية سنة 2000 أدخل تعديل آخر على المواد 67 و1/67 و2/67 حيث ألغيت هذه المواد من قانون 30 أكتوبر 1935 بموجب الأمر رقم (2000 ــ 1223) المحدّد لقانون النقد والمالية، ونصّت على هذه الجرائم بموجب المادة الرابعة منه، حيث اقتصر التعديل على الشق الجزائي دون المساس بالأفعال الثلاث المنصوص عليها في القانون القديم (قانون 30 أكتوبر 1935)، ومن تم أصبحت المادة 1/67 من القانون السابق الذكر هي المادة 4/163 من الأمر رقم (2000 ــ 1223) المتعلق بالنقد والمالية، أما المادة 2/67 من القانون القديم هي المادة 163/ 5 من الأمر رقم (2000 ــ 1223) السالف الذكر.

وعليه نفصل تباعا الجرائم الخاصة ببطاقات الوفاء ثم العقوبات المقررة لها.

أولا ــ الجرائم الخاصة ببطاقة الوفاء (الدفع) في التشريع الفرنسي:

نصّ المشرّع الفرنسي في المادة (3/163) من قانون النقد والمالية لسنة 2000 المعدل بالقانون رقم 2007 ــ1544 الصادر في 29 أكتوبر 2007 من خلال المادة 14 منه على ثلاث جرائم هي[1]:

ــ جريمة تقليد أو تزوير بطاقة الوفاء.

ــ جريمة استعمال أو محاولة استعمال البطاقة المزورة أو المقلدة.

ــ جريمة قبول التعامل بالبطاقة على الرغم من العلم بتزويرها أو تزويرها.

يتّضح من خلال هذه المادة أنّ محل الجرائم الثلاث السابقة الذكر هي بطاقة الوفاء أو السحب وهي بدورها الموضوع الذي ينصب عليه نشاط الجاني في الأفعال الثلاث، والمشرع الفرنسي عرف بطاقة الوفاء في المادة1/57 من القانون رقم 91 ــ 1382 الصادر في 30 ديسمبر 1991 الخاص بتأمين الشيكات وبطاقات الوفاء، بأنها:" أداة تصدر من إحدى مؤسسات الإئتمان، أو إحدى الجهات المنصوص عليها في المادة 08 من القانون رقم 84 ــ 46 والصادر في 24 يناير 1984 والخاص بنشاط ورقابة مؤسسات الإئتمان، وتسمح لحاملها بسحب أو تحويل النقود من حسابه"[2].

وعليه يتّضح بمفهوم المخالفة أنّ كل الأنواع الأخرى للبطاقات كبطاقة الاعتماد أو البطاقات الخاصة لا تصلح أن تكونا موضوعا للجرائم الثلاث، وإن كان يمكن أن تخضع

---

(1) - Article L163-3 Modifié par Loi n°2007-1544 du 29 octobre 2007 - art. 41 JORF 30 octobre 2007, consiste « Est puni des peines prévues à l'article L. 163-3 le fait pour toute personne :
1. De contrefaire ou de falsifier une carte de paiement ou de retrait ;
2. De faire ou de tenter de faire usage, en connaissance de cause, d'une carte de paiement ou de retrait contrefaisante ou falsifiée ;
3. D'accepter, en connaissance de cause, de recevoir un paiement au moyen d'une carte de paiement contrefaisante ou falsifiée."

(2) ــ أما بطاقة السحب فقد عرفها المشرع الفرنسي في المادة 2/57 من القانون ذاته، وهي تصدر من ذات جهات إصدار بطاقة الوفاء، ولكن يقتصر دورها على سحب النقود فقط من أجهزة التوزيع الآلي.

للنصوص العامة في التزوير المعلوماتي[1]. وبعد تحديد محل جرائم بطاقة الوفاء نتطرق فيما يلي تفصيل هذه الجرائم.

1 ــ جريمة تقليد أو تزوير بطاقة الوفاء:

نصّ المشرّع الفرنسي على هذا الفعل في المادة 3/163 من قانون النقد والمالية لسنة 2000 وذلك في الفصل الخامس المتعلق بالجرائم المرتبطة بالشيكات ووسائل الدفع، وذلك بقوله: "يعاقب بالعقوبات المنصوص عليها في المادة 3/163 كل من قام بتقليد أو تزوير بطاقة وفاء أو سحب..". وعلى الرغم من أن المشرع لم يوضح في هذا النص كافة الأركان التي تقوم عليها هذه الجريمة إلا أنه استنادا إلى نص المادة 1/441 من قانون العقوبات الفرنسي الجديد يمكن تحديد أركانها.

أ ــ الركن المادي:

يتخذ الركن المادي لهذه الجريمة إحدى الصورتين: التقليد أو التزوير فضلا عن بيان الآثار التي يرتبها وهي إحداث الضرر.

➢ **التقليد:** يقصد به عموما صناعة شيء على غرار شيء آخر[2]، ويقصد به في مجال بطاقة الوفاء، صناعة بطاقة وفاء على غرار بطاقة أخرى، ويستلزم الأمر في هذه الحالة معرفة الرقم السرّي الخاص بها عند استخدام البطاقة المقلدة. وقد يحدث أن يتم اصطناع بطاقة وفاء جديدة دون أن تكون على غرار بطاقة لأخرى، وفي هذه الحالة يدخل الاصطناع تحت مدلول التزوير[3].

➢**التزوير:** جاء لفظ التزوير عاما دون تحديد طرق خاصة به، وذلك يتوافق مع ما نص عليه المشرع في المادة 1/441 من قانون العقوبات الفرنسي الجديد، حيث جاء لفظ تغيير الحقيقة مطلقا غير محدد على سبيل الحصر، ومفاده أن أي تغيير في بطاقة الوفاء ذاتها سواء بتغيير بعض أرقامها، أو الإمضاء الموقع عليها، أو الإسم المدون فوق ظهرها، أو أي تعديل على البيانات الالكترونية، بأي

---

[1] ــ انظر فيما سبق بخصوص جريمة التزوير المعلوماتي ص 72 وما بعدها.

[2] ــ محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، وفقا لأحدث التعديلات، دار النهضة العربية، القاهرة، 2012، ص 238.

[3] ــ محمد عبيد الكعبي، مرجع سابق، ص 686.

طريقة من طرق التزوير المادي(سواء بالإدخال، التعديل أو الحذف) يتحقق الركن المادي لهذه الجريمة.

أما بالنسبة للتزوير المعنوي، فهناك صعوبة وقوعه نظرا لأن بطاقة الوفاء تصدر من إحدى المؤسسات المالية، ويتبعها رقم سري، وتفترض وجود حساب خاص بالعميل الذي صاحب البطاقة، فإذا انتحل شخص شخصية صاحب حساب في أحد البنوك بشرط أن يعلم بأنه لم يحصل على بطاقة وفاء من البنك، ثم طلب هذه البطاقة فصدرت باسم صاحب الحساب الحقيقي، وحصل المتهم عليها، ففي هذه الحالة نكون بصدد تزوير معنوي اتخذ صورة جعل واقعة مزورة في صورة واقعة صحيحة، وذلك بانتحال شخصية الغير[1].

- **الضرر:** لا يكفي لقيام جريمة تقليد أو تزوير بطاقة وفاء قيام الركن المادي بتغيير الحقيقة في البطاقة، وإنما أن يكون من شأن ذلك إحداث ضرر للغير، والملاحظ أن المشرع لم يذكر الضرر صراحة في نص المادة 3/163 من قانون النقد والمالية لسنة 2000، إلا أن المستقر عليه فقها وقضاء ضرورة توافر هذا الركن ويكفي أن يكون ضررا إحتماليا يمس الأفراد أو المؤسسات المالية. ويستوي في الضرر أن يكون ماديا أو معنويا، ومسألة توافر الضرر من المسائل الموضوعية التي يقدرها قاضي الموضوع حسب ظروف كل دعوى[2].

ب ــ الركن المعنوي:

جريمة تقليد أو تزوير بطاقة الوفاء جريمة مقصودة، ومن ثم يتخذ ركنها المعنوي صورة القصد الجنائي العام بشقيه العلم والإرادة، بأن يعلم الجاني أن ما يرتكبه هو فعل مجرم قانونا، ومع ذلك تتجه إرادته لتنفيذ هذه النتيجة.

إلى جانب هذا القصد يلزم لقيام الركن المعنوي توافر قصدا خاصا، يتمثل في اتجاه نية الجاني إلى استعمال بطاقة الوفاء المزوّرة فيما زُوّرت من أجلـــه، وإضافة المتحصل منها إلى ممتلكاته[3]. فإذا

---

[1] ــ محمد عبيد الكعبي، مرجع سابق، ص 687.

[2] ــ عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة 2010، ص 930.

[3] ــ عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 940.

تخلفت هذه النية انتفى القصد الجنائي، ومتى توافر للقصد الجنائي عناصره فلا عبرة بالبواعث التي قد تدفع الجاني على ارتكاب جريمة تقليد وتزوير بطاقة الوفاء.

2 ــ جريمة استعمال أو محاولة استعمال البطاقة المزورة أو المقلدة:

طبقا للفقرة الثانية من المادة 3/163 من قانون النقد والمالية لسنة 2000، نص المشرع الفرنسي على هذه الجريمة بقوله: "كل من استعمل أو حاول استعمال بطاقة وفاء أو سحب مقلدة أو مزورة وهو يعلم ذلك.".

وعليه لا تقوم هذه الجريمة إلا بتوافر ركنيها المادي والمعنوي وفيما يلي تفصيل ذلك[1]:

أ ــ الركن المادي:

يتمثل الركن المادي في جريمة استعمال بطاقة وفاء مقلدة أو مزورة في فعل الاستعمال، أي إحراز البطاقة والاحتجاج بها على أنها صحيحة، ومؤدى ذلك أن مجرد وجود البطاقة المزورة في حيازة المتهم دون إحرازها لا يقوم به فعل الاستعمال[2]،فيتعين أن يقوم المتهم بإحرازها والاحتجاج بها على أنها صحيحة، ويكون ذلك عندما يستخدمها في الوفاء لدى أحد التجار أو يستخدمها في السحب من إحدى آلات التوزيع الآلي[3].

ب ــ الركن المعنوي:

يتخذ الركن المعنوي لهذه الجريمة صورة القصد الجنائي العام، أي العلم بتزوير البطاقة أو تقليدها، وإرادة استعمالها (في الوفاء أو السحب)، والاحتجاج بها على أنها صحيحة، وينتفي القصد وبالتالي الجريمة إذا تبث جهل المتهم بتقليد أو بتزوير بطاقة الوفاء، حتى ولو ضبطت معه[4].

---

(1) ــ هناك صعوبة تحديد طبيعة جريمة استعمال بطاقة الوفاء المقلدة أو المزورة، حيث اعتبرها البعض من الجرائم المستمرة والبعض الآخر من الجرائم الوقتية، وذلك على أساس الوقت التي تستغرقه الجريمة في تحقيق كافة عناصرها، وعليه تعتبرجريمة استعمال بطاقة وفاء مقلدة أو مزورة جريمة وقتية إذا كان تقديم البطاقة كوسيلة وفاء أو سحب من آلات توزيع النقود لا يستغرق إلا برهة قليلة من الزمن، والعكس صحيح.

(2) ــ محمد عبيد الكعبي، مرجع سابق، ص 691.

(3) - Gavalda (c), op cit, p 92.

(4) -Ibid p. 92.

تجدر الإشارة أنّه من خلال نص المادة 4/163 من القانون السابق الذكر أن المشرع الفرنسي عاقب على الشروع في جريمة الاستعمال للبطاقة المقلدة أو المزورة، وذلك من خلال عبارة "من حاول استعمالها"، ويتحقق ذلك عندما يفشل المتهم في تحقيق النتيجة الإجرامية المترتبة على هذا الإستعمال، وهي الحصول على الخدمة أو السلعة عندما يستخدمها كوسيلة للوفاء، أو الحصول على النقود إذا استخدمها كوسيلة للسحب. والحقيقة أن الاستعمال أو محاولة الإستعمال تبدو قليلة الأهمية مادام المشرع ساوى في العقاب بين الجريمة التامة ومجرد المحاولة[1].

3 ــ جريمة قبول التعامل ببطاقة مقلدة أو مزورة:

نصّ المشرّع على هذه الجريمة في المادة 4/163 من قانون النقد والمالية الفرنسي لسنة 2000، حيث جاء فيها: "كل من قبل الدفع عن طريق بطاقة وفاء مقلدة أو مزورة وهو يعلم بذلك"، فالجريمة تقوم هنا في حالة استخدام البطاقة كوسيلة وفاء فقط دون السحب، بحيث يسأل التاجر أو صاحب الخدمة في حالة توافر ركني هذه الجريمة، وهما ركن مادي وآخر معنوي.

أ ــ الركن المادي:

يتمثّل الركن المادي في هذه الجريمة في قيام شخص بقبول الوفاء عن طريق البطاقة على الرغم من علمه بتقليدها أو تزويرها، ويكون هذا الشخص في العادة تاجرا أو مقدم خدمة معينة، وعليه تثور في هذه الحالة إشكالية تطبيق القواعد العامة للمسؤولية الجنائية على أساس أن التاجر في هذه الحالة هو الجاني والمجني عليه قد يكون البنك المسحوب عليه، أو صاحب الحساب الذي تم تقليد بطاقته.

لحل هذه الإشكالية ينبغي التمييز بين ثلاث فروض:

الفرض الأول: أن يقوم حامل البطاقة المقلدة أو المزورة بتقديمها إلى التاجر ويفصح له عن طبيعتها، ويقوم هذا الأخير بالاتفاق مع حامل البطاقة بقبولها ويتم الوفاء بواسطتها، في هذا الفرض فإن حامل البطاقة لا يسأل عن جريمة استعمال، لأنه لم يحتج بالبطاقة على أنها صحيحة، وإنما يسأل

[1] ــ محمد عبيد الكعبي، مرجع سابق، ص 693.

كشريك للتاجر الذي يحتج بها على البنك بأنها بطاقة صحيحة، ولا يغير من ذلك التكييف أن التاجر سوف يحتج على البنك بصورة من البطاقة المزورة[1].

الفرض الثاني: أن يقوم حامل البطاقة المزورة بتقديمها للتاجر على أنها صحيحة، ويعلم هذا الأخير أنها مزورة ولا يفصح لحاملها عن ذلك، ويقبل الوفاء بواسطتها، في هذا الفرض يعد حامل البطاقة مرتكبا لجريمة الاستعمال، ويعد التاجر كذلك مرتكبا للجريمة ذاتها، وقد يحتج التاجر بصورة هذه البطاقة لدى البنك لاستيفاء حقه وهو يعلم أن البطاقة مزورة، وهذه الصورة تكفي لقيام جريمة الاستعمال إذا توافرت بقية أركانها[2].

الفرض الثالث: وهو نادر الوقوع، يكون فيه حامل البطاقة غير عالم بأن البطاقة مقلدة أو مزورة ويقدمها للتاجر، ويعلم هذا الأخير بالتقليد أو التزوير، وعلى الرغم من ذلك يقوم بقبولها، في هذه الحالة لا يسأل حامل البطاقة عن جريمة الاستعمال لانتفاء القصد الجنائي، ولكن يسأل التاجر عن جريمة الاستعمال إذا استخدمها واحتج بها في مواجهة البنك.

ب ــ الركن المعنوي:

يتّخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام بشقيه العلم والإرادة، ويتمثل وفقا للقواعد العامة في علم المتهم (التاجر) بأن بطاقة وفاء مقلدة أو مزورة، واتجاه إرادته إلى قبولها كوسيلة وفاء.

ثانيا ــ العقوبات المقررة للجرائم الواقعة على بطاقة الوفاء (الدفع) في التشريع الفرنسي:

قرّر المشرّع الفرنسي لهذه الجرائم نوعين من العقوبات، عقوبتين أصليتين، وأخرى عقوبة تكميليّة وجوبية تتمثّل فيما يلي:

أ ــ العقوبات الأصلية:

عاقب المشرع الفرنسي مرتكب جرائم بطاقة الوفاء الثلاث السابقة الذكر بعقوبة الحبس لمدة سبع (7) سنوات، وغرامة مالية تقدر بـــ 750.000 يورو، وذلك ما نصت عليه المادة 3/163

(1) ــ محمد عبيد الكعبي، مرجع سابق، ص 695.

(2) - نقض 26 يونيو 1956، مجموعة أحكام محكمة النقض، السنة السابعة، رقم 25، ص91.

من قانون النقد والمالية الفرنسي لسنة 2000[1]، ويلاحظ أن المشرع الفرنسي لم يترك للقاضي سلطة تقديرية في تقرير العقاب في هذه الجرائم حيث ساوى بين مقلد أو مزور البطاقة ومع من يستعملها للوفاء أو السحب، ومع من يقبلها للوفاء بها، ويستوي أن يكون المبلغ بسيط أو كبير، ولعل الغاية من ذلك هو حماية البطاقة في حد ذاتها حيث أصبحت من أكثر وسائل الوفاء في العصر الحالي، وذلك بخلاف القانون القديم الملغى وهو قانون 30 أكتوبر 1935، المحدد لقواعد التعامل بالشيك والمرتبط ببطاقات الدفع، حيث حدد من خلال المادة 67 منه على عقوبة الحبس التي لا تقل مدتها عن سنة (1) ولا تزيد على سبع (7) سنوات، والغرامة التي لا تقل عن 3.600 فرنك ولا تزيد عن 5.000000 فرنك، أو إحدى هاتين العقوبتين.

ب ــ العقوبة التكميلية: طبقا للمادة 5/163 من قانون النقد والمالية الفرنسي لسنة 2000، أضاف المشرع الفرنسي عقوبة تكميلية وجوبية هي المصادرة[2]، ويتمثّل موضوعها في البطاقات المقلدة أو المزورة وذلك بغرض تدميرها، وأيضا المواد والماكينات والمعدات والأدوات التي استخدمت في التقليد أو التزوير أو التي كان مقررا استخدامها في هذا الغرض إلا إذا كان ذلك بدون علم المالك[3].

---

(1) - Article L163-3 **de** Code monétaire et financier francais dispose :" Est puni d'un emprisonnement de sept ans et d'une amende de 750 000 euros le fait pour toute personne:
1. De contrefaire ou de falsifier un chèque ou un autre instrument mentionné à l'article L. 133-4 ;
2. De faire ou de tenter de faire usage, en connaissance de cause, d'un chèque ou un autre instrument mentionné à l'article L. 133-4 contrefaisant ou falsifié ;
3.D'accepter, en connaissance de cause, de recevoir un paiement au moyen d'un chèque ou d'un autre instrument mentionné à l'article L. 133-4 contrefaisant ou falsifié.

(2) - Article L163-5 **de** Code monétaire et financier francais dispose "La confiscation, aux fins de destruction, des chèques et autres instruments mentionnés à l'article L. 133-4 contrefaits ou falsifiés est obligatoire dans les cas prévus aux articles L. 163-3 à L. 163-4-1. Est également obligatoire la confiscation des matières, machines, appareils, instruments, programmes informatiques ou de toutes données qui ont servi ou étaient destinés à servir à la fabrication desdits instruments, sauf lorsqu'ils ont été utilisés à l'insu du propriétaire".

(3) ــ العقوبة التكميلية المنصوص عليها في المادة 67/ 2 من قانون 30 أكتوبر 1935، المحدد لقواعد التعامل بالشيك والمرتبط ببطاقات الدفع ــ هي نفسها المنصوص عليها في المادة 163 /5 من قانون النقد والمالية الفرنسي لسنة 2000.

أخيرا فإننا نلاحظ أن الحماية الجنائية لبطاقة الوفاء في التشريع الفرنسي اقتصرت فقط على تجريم تقليد أو تزوير البطاقة واستعمالها، أو قبول التعامل بها كوسيلة وفاء، دون أن تمتد للأفعال غير المشروعة التي يرتكبها حامل البطاقة مثل استخدام البطاقة على الرغم من انتهاء صلاحيتها أو إلغائها من الجهة التي أصدرتها، أو استخدامها كوسيلة وفاء أو سحب على الرغم من عدم وجود رصيد دائن لحاملها لدى البنك.

وعليه في الحالات غير المنصوص عنها في المادة 4/163 من قانون النقد والمالية الفرنسي لسنة 2000، تطبق عليها القواعد العامة في قانون العقوبات، سواء تم تكييف نشاط المتهم على أنه سرقة أو نصب أو خيانة أمانة[1].

هذا ما يخص موضوع الباب الأول الخاص بالأحكام الموضوعية لحماية الحكومة الالكترونية جزائيا، وعليه فإن رصد هذه الجرائم غير كافي، بل لابد من متابعة قضائية لمعاقبة مرتكبي هذه الجرائم، كل ذلك محل بحث الباب الثاني من الدراسة المعنون بـــ " الحماية الجنائية الإجرائية للحكومة الالكترونية".

(1) -Etienne Madrranges, la loi du 30 décembre 1991, relative à la sécurité des chèque et des cartes de poiment , vers un denengorgement des tribunaux, la nouvelle pénalité libératoire, G. P ,doc, p. 3.

الباب الثاني

الحماية الجنائيّة الإجرائيّة للحكومة الإلكترونيّة

تعدّ الجرائم الواقعة على الحكومة الالكترونية من الأنماط الإجرامية التي فجرتها حديثا ثورة تقنية المعلومات والإتصالات عن بعد، حيث تعتبر من المستجدات التي لم تكن معروفة للقانون الجزائي الإجرائي، وبالتالي فأيّ محاولة للتعامل إجرائيا مع هذا النمط الإجرامي في إطار عملية البحث والتحقيق، سوف يخلق إشكالات في نطاق قانون الإجراءات الذي وضعت نصوصه لتحكم إجراءات متعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، بل أن هذه الطرق التقليدية أصبحت عقيمة بالنسبة لإثبات هذا النوع المستحدث من الإجرام، لهذا ظهر نوع خاص من الأدلة يمكن الإعتماد عليه في إثبات الجرائم الواقعة على الحكومة الالكترونية، ومن تم نسبتها إلى فاعليها، وهذا الدليل يطلق عليه "الدليل الإلكتروني"[1].

بناء على ما سبق، سنتناول إجراءات جمع الأدلة عن الجرائم الواقعة على الحكومة الإلكترونية من خلال الفصل الأول، وتخصيص الفصل الثاني للقواعد الخاصة بالمحاكمة في هذا النوع المستحدث من الإجرام الواقع على الحكومة الإلكترونية.

الفصل الأوّل: إجراءات جمع الأدلة عن الجرائم الواقعة على الحكومة الالكترونية

إنّ الطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية، من حيث حداثة أساليب إرتكابها، وسهولة إخفائها وسرعة محو آثارها، بل أن هذه الآثار ليست محصورة في النطاق الإقليمي لدولة بعينها، بل تتعداه إلى دول أخرى، فضلا عن أن مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية للمعطيات، ليس هذا فحسب بل إنها تستهدف محلا من طبيعة خاصة ونعني بذلك المعلومات، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة، لاسيما

[1]ـــ يرجع أصل مصطلح الدليل الرقمي أو الدليل الإلكتروني Digital evidence إلى استخدام النظام الرقمي الثنائي (0، 1) وهي الصيغة التي تسجل بها كل البيانات (أشكال وحروف ورموز وغيرها)داخل الحاسب الآلي، حيث يمثل(**الصفر**) وضع الإغلاقOff، والواحد (1)وضع التشغيلOn، ويمثل الرقم **صفر**(0) أو الرقم **واحد**(1) ما يعرف بالبيت (Bit)، ويشكل عدد بيت (Bit)ما يعرف بالبايتByte. انظر: بيل جيتس، المعلومة بعد الانترنت: طريق المستقبل، ترجمة عبد السلام رضوان، الكويت، المجلس الوطني للثقافة والفنون والآداب، 1998، ص 41 ـــ 63.

عملية إثبات هذه الجرائم وآلية مباشرة عمليات الاستدلال والتحقيق عبر البيئة الإفتراضية لتعقب المجرمين وتقديمهم للعدالة[1].

كل هذه التحديّات دفعت بالمشرّع الجزائي إلى إعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون. ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد وأن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام به. مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة المعلوماتية الإعتماد عليها في الوصول إلى الدليل المناسب في إثبات الجرائم الواقعة على الحكومة الإلكترونية منها الجرائم المعلوماتية.

وعليه تتمحور الإشكاليّة في هذا الإطار حول: **ما مدى تخصيص المشرع الجزائري قواعد إجرائية خاصة بالتعامل مع الجرائم الواقعة على الحكومة الالكترونية ومنها الجرائم المتصلة بتكنولوجيات الإعلام والإتصال؟ وما مدى فاعليتها في الحصول على الدليل الالكتروني؟**

المبحث الأول: خصوصيّة التحرّي والتحقيق عن الجرائم الواقعة على الحكومة الالكترونية

الثابت أنّ الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمرّ عملية التحقيق أيضا بمرحلتين، مرحلة التحقيق الأولي ومرحلة التحقيق الإبتدائي، فالمرحلة الأولى هي مرحلة جمع الإستدلالات، التي يباشرها أعضاء الضبط القضائي[2]، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق.

---

(1) - عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في التشريع الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية،2010، ص 14.

(2)ـــ حسب المادة 15 من قانون الإجراءات الجزائية المعدلة بالمادة الرابعة من الأمر رقم 15ـــ02 المؤرخ في 23 جويلية 2015 المتضمن قانون الإجراءات الجزائية: "يتمتع بصفة ضابط الشرطة القضائية:

1 ـــ رؤساء المجالس الشعبية البلدية،

2 ـــ ضباط الدرك الوطني،

3 ـــ الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني،

إذا كانت الجهات المكلفة بالتحري والتحقيق عن الجريمة والمجرمين معتادة التعامل مع الجريمة بصورتها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية في مسرح الجريمة من بصمات وآثار أقدام أو بقع دم...، فإن أهم مشكلة ستواجه هذه الجهات عند تعاملها مع الجريمة المعلوماتية تبدأ من طبيعة البيئة الافتراضية التقنية التي ترتكب فيها[1].

وعليه فإنّ المكافحة الفاعلة قد تنطوي أوّلا على تخصيص ضبطية قضائية مختصة بالبحث والتحري عن الجرائم المعلوماتية (المطلب الأوّل)، ثم بحث متطلبات التحقيق الإبتدائي وما تتمتع به من أصول فنيّة في التعامل مع هذه الجرائم وذلك في المطلب الثاني. في حين يخصص المطلب الثالث للدليل المناسب لإثبات هذه الجرائم، والذي يتميّز من ذات الطبيعة التقنيّة.

المطلب الأوّل: الضبطيّة المختصّة بالبحث والتحرّي عن الجرائم الواقعة على الحكومة الالكترونية

تعدّ مرحلة التحقيق الأولي (جمع الإستدلالات) من المراحل الخطرة في إطار عملية بناء الدعوى الجنائية، ذلك لما لها من أهمية في البحث والتحري عن الجرائم وعن مرتكبيها، وجمع المعلومات عنها، وتحضير المادة اللازمة لتحريك الدعوى العمومية، وبعبارة أخرى تهيئة القضية وتقديمها للنيابة العامة[2].

---

4 ــ ذوو الرتب في الدرك، ورجال الدرك الذين أمضوا في سلك الدرك ثلاث سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع، مفتشوا الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل وعينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني، بعد موافقة لجنة خاصة،

5 ــ الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضوا ثلاث(3) سنوات على الأقل بهذه الصفة والذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل". أمر رقم 15 ــ02 مؤرخ في 23 يوليو سنة 2015، يعدل ويتمم الأمر رقم 66ــ155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج. ع 40 ، الصادر في 23 يوليو 2015.

[1] ــ سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص 95 وما بعدها.

[2] ــ عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر، الجزائر، 2003، ص 184.

خوّل القانون مهمة البحث والتحري لأجهزة الضبط القضائي[1]، وتتميز هذه الفئة بقوة الملاحظة وسرعة البديهة، حيث يحاول ضابط الشرطة القضائية بكل جهد متابعة الجريمة والبحث فيها وعن الأدلة وصولا لإظهار الحقيقة.

وعليه تعدّ هذه المرحلة من أبرز المراحل التي يستعان بها لمواجهة الإجرام المستحدث، كالجرائم المعلوماتية، غير أنّ التحرّي في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطوير أجهزة الضبط القضائي لتواكب التطوّر الحاصل في مجال الجريمة.

نتيجة لهذا قامت معظم الدول بإحداث أجهزة متخصّصة بمكافحة هذا النوع المستحدث من الإجرام تتولى مهمة التحري عن جرائم العالم الإفتراضي وكشف النقاب عنها، وقد حملت هذه الأجهزة تسميات مختلفة منها مثلا شرطة الأنترنت أو فرقة التحرّي عن جرائم المعلوماتية إلى غير ذلك من التّسميات(الفرع الأوّل).

لا يقتصر الأمر على إحداث أجهزة مختصة بالبحث والتحري عن الجرائم الواقعة على الحكومة الالكترونية كالجرائم المعلوماتية مثلا، بل يتطلب أيضا منح هذه الأجهزة أساليب تحري خاصة تتماشى وهذا النوع من الإجرام وذلك في إطار مكافحة هذه النوعية من الجرائم (الفرع الثاني).

الفرع الأوّل: وحدات الضبط القضائي المختصة في الجرائم الواقعة على الحكومة الإلكترونية

بالنظر إلى الطبيعة التقنيةّ التي تتميّز بها الجريمة المعلوماتية ذهبت أغلب الدول إلى استحداث أجهزة متخصصة لها من الكفاءة والتدريب والوسائل البشرية ما يؤهلها للتعامل مع هذه النوعية الخاصة من الإجرام، في هذا الإطار نعرض وحدات الضبط القضائي في الجرائم الواقعة على الحكومة الالكترونية بما فيه جرائم معلوماتية أو كما يطلق عليها المشرع الجزائري جرائم تكنولوجيا الاعلام والاتصال على المستوى الداخلي (أولا) ثم على المستوى الدولي(ثانيا).

---

[1] ــ حسب المادة 14 من قانون الإجراءات الجزائية الجزائري، يشمل الضبط القضائي:

1 ــ ضباط الشرطة القضائية.

2 ــ أعوان الضبط القضائي.

3 ــ الموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي.

أوّلاـــ وحدات الضبط القضائي المختصة في الجرائم الواقعة على الحكومة الإلكترونية على المستوى الداخلي:

بادرت مختلف الدول بإنشاء أجهزة متخصصة في مجال الجريمة المعلوماتية في إطار مكافحتها والبحث والتحري عنها وعن مرتكبيها، وذلك لما تتمتع به من كفاءة وتدريب يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام. وسنحاول إلقاء الضوء على هذه الأجهزة الموجودة في بعض الدول ثم نعرج على الوضع في الجزائر.

أ ـــ الأجهزة المختصة في الدول الأجنبية:

كانت الدول المتقدمة سباقة في مكافحة الجرائم المعلوماتية، وهي تحاول جاهدة في إحداث أجهزة متخصصة في ذلك، وعلى درجة عالية من التقنية، ومن هذه الدول الولايات المتحدة الأمريكية، بريطانيا وفرنسا، وذلك فيما يلي:

1. في الولايات المتحدة الأمريكية:

تعدّ الولايات المتحدة الأمريكية من أولى الدول التي قامت بتقديم خدمات القطاع الإداري عن بعد وكان ذلك في بداية التسعينات وبالضبط في سبتمبر من عام 1935، حين أصدر نائب الرئيس الأمريكي السابق آل جور تقريرا حمل عنوان "من البيروقراطية إلى الإنتاج: نحو حكومة تعمل أكثر وتكلف أقل"[1]، هذا من جهة.

ومن جهة أخرى تعد الولايات المتحدة الامريكية هي الأخرى من أولى الدول التي واجهت الجرائم المعلوماتية[2]، وذلك بالنص على مواجهتها تشريعيا بإنشاء إدارة متخصصة لمتابعة الجرائم المعلوماتية بمكتب التحقيقات الفدرالي(F.B.I) Federal Burau of Investigation،

---

[1] ـــ خالد ممدوح ابراهيم، مرجع سابق، ص 16.

[2] ـــ تعد الولايات المتحدة الأمريكية ثاني دولة بعد السويد سنت قانونا خاصا بحماية أنظمة الحاسب الآلي، وكان ذلك في (1976 ـــ 1985)، وفي سنة1985 حدد معهد الأدلة القومي خمسة أنواع رئيسية للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، وجرائم التلاعب بالحاسب الآلي، أيضا دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب الآلي. وفي سنة 1986 صدر قانونا تشريعيا يحمل الرقم (1213) عرف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت جميع المتطلبات الدستورية اللازمة لتطبيقه، وعلى إثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ، من ذلك قانوان ولاية تكساس لجرائم الحاسب الآلي. انظر: مصطفى محمد موسى، الجهاز الالكتروني لمكافحة الجريمة، الطبعة الأولى، مطابع الشرطة للطباعة والنشر والتوزيع، مصر، 2001، ص 95.

والذي يضمّ داخله مجموعة من الأشخاص المدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتمّ تحصيله من أدلة[1].

بالإضافة إلى إدارة مكافحة جرائم المعلوماتية في ألـــ(F.B.I)، هناك مراكز أخرى لها نفس أهداف هذا الجهاز المتخصص في تعقب مجرمي المعلوماتية، تتمثل فيما يلي:

- **قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية:** تم إنشاء هذا القسم سنة 1991، ويختص بالتعريف بهذه الجرائم والكشف عنها وعن مرتكبيها[2].

- **المركز الوطني لحماية البنية التحتية:** وهو تابع للمباحث الفدرالية الأمريكية، ويتقاسم مهامه مع وزارة الدفاع الأمريكية، ويتكون من فريق سري يصل أعضاءه إلى 125 رجلا حكوميا.

- **مركز تلقي الشكاوى جرائم الانترنت"ICCC "[3]:** تمّ إنشاؤه من طرف مكتب التحقيقات الفدرالي"FBI" في سنة 2000، وفي عام 2003 ثم دمج مركز شكاوي الإحتيال عبر الانترنت المعروف بـــ "IFC"[4] مع هذا المركز، ويعمل مركز بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء "NWC"[5]، حيث يقوم بالربط بين معلومات يتلقاها من ضحايا جرائم الانترنت فيعد منها ملف يسلمها لرجال تطبيق القانون[6].

- **شرطة الواب "Webpolice":** تعتبر نقطة مراقبة على الانترنت، إضافة إلى أنها تتلقى الشكاوي من مستخدمي الشبكة وملاحقة الجناة والقراصنة والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[7].

---

[1] ـــ سليمان أحمد فاضل، مرجع سابق، ص 404.

[2] ـــ كان هذا القسم تابعا لوزارة العدل الأمريكية وفي عام 1996 أصبح قسما مستقلا نتيجة تضخم عمله، لمزيد من التفاصيل أنظر: عمر يونس بن عرب، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، مصر، 2004، ص 814.

[3] - وهو إختصار لـــ: " Internet Centre Complaint Crime "

[4] ـــ وهو إختار لـــ: "Internet Fraude compcenter"

[5] ـــ وهو إختصار لـــ: "National White coller center"

[6] ـــ حسن بن سعيد سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007، ص 350.

[7] ـــ جميل عبد الباقي الصغير، الجوانب الإجرائية لجرائم الانترنت، دار الفكر العربي، القاهرة، 2001، ص 77.

• **وحدة جرائم الانترنت:** وهي وحدة متخصصة بالتحقيق في جرائم الملكية الفكرية وجرائم الانترنت، ويترأسها مدير مساعد مكتب التحقيقات الفدرالي ولها ذات مرتبة وحدة التفتيش[1].

2. في بريطانيا: قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتحري عن الجرائم المعلوماتية، بدأت نشاطها سنة 2001 وتضم نحو 80 مفتشا، 40 منهم متمركزا في لندن ضمن الوحدة الوطنية لمكافحة جرائم التقنيّة العالية، و40 موزعين على الوحدات المحلية الأخرى.

تتلخّص مهام هذه الوحدة في متابعة مرتكبي الجرائم الجنسية عبر الانترنت، خصوصا تلك الواقعة على الأحداث، وكذلك قراصنة المعلومات، وجرائم نشر الفيروسات[2].

3. في فرنسا: قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية، سواء ما كان منها تابعا للأمانة العامة للدفاع الوطني، ووزارة الداخلية، ووزارة الدفاع، وخلية مراقبة التجارة الالكترونية ومعالجة البريد الالكتروني التابعة للمديرية العامة للمنافسة والاستهلاك وزجر الغش بوزارة الاقتصاد والمالية والصناعة. وذلك على النحو التالي:

أ ــ على مستوى الأمانة العامة للدفاع الوطني: تتكوّن هذه المؤسسة من الأجهزة الرئيسية التالية:

• **المديرية المركزية لتنظيم أمن أنظمة المعلومات:**

تمّ إحداث هذه المديرية بتاريخ 31 يوليو 2001[3]، وهي تحت سلطة الكاتب العام للدفاع الوطني، وتتكون من عدة أجهزة فرعية تتمثل فيما يلي:

ــ مركز الخبرة الحكومي للرد على الاعتداءات المعلوماتية ومعالجتها: قامت الحكومة الفرنسية بإحداث جهاز إنداروسمساعدة على شبكة الانترنت، وأُنيطت به مهمة اليقظة التكنولوجية والرد على الاعتداءات المعلوماتية. وهو يعمل بتنسيق مع المصالح المكلفة بأمن المعلومات في مختلف الادارات[4].

---

(1) ــ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت قي مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2007، ص108 ــ 109.

(2) ــ نبيلة هبة هروال، مرجع سابق، ص 111.

(3) -Décret n°2001-693 du 31 juillet 2001 créant au secretariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information.

(4) - عبد الكريم دحو الإدريسي، أمن مجتمع المعلومات بين المؤسسات الأمنية والمدنية وشبه الأمنية، الجزءالأول: التجربة الفرنسي، مطبعة النجاح الجديدة، الطبعة الأولى، الدار البيضاء، المغرب، 2003، ص 12.

ـــ مركز التدريب على أمن أنظمة المعلومات: أُحدث هذا المركز بموجب المرسوم المؤرخ في 3 مارس 1986، ويعتبر الفاعل المركزي لشبكة التحسيس بالمشاكل المرتبطة بأمن أنظمة المعلومات وهو الجهاز المتخصص في تكوين مختلف الخبراء المؤهلين في هذا الشأن[1].

وعليه فمهمة المركز تندرج في إطار الأهداف التي تتابعها المديرية المركزية لتنظيم أمن أنظمة المعلومات، لاسيما ما يتعلق بتأمين أنظمة معلومات الدولة.

- **مديريّة الوقاية وأمن الدولة:** تسهر هذه المديرية على تأمين حرية وأمن إتصالات السلطات العمومية، ووقاية أمن الأفراد على تراب الجمهورية[2].
- **مديريّة التكنولوجيا ونقل التكنولوجيا الحسّاسة:** من المهام الرئيسية لهذه المديرية المشاركة في دعم المحافظة على التراث التقني والعلمي الفرنسي، مع اليقظة العامة (البشرية والتكنولوجية)[3].
- **لجنة الاستخبارات المشتركة بين الوزارات:** تتولّى هذه اللجنة المهام التالية[4]:

ـــ مهمة الأمانة العامة لإجتماعات الوزارات المتعلقة بالاستخبارات.

ـــ وتُعد تقارير استخبارية ومذكرات توقعية واستنفارية.

ـــ وتنظم وتنشط مجموعات العمل التي نص عليها المخطط الوطني للإستخبارات الذي تنسق عملية إعداده.

ب ـــ على مستوى وزارة الداخلية: سنخصّص المجال للشرطة وما تشمله من مراكز متخصّصة على مستوى الشّرطة الفرنسّية وذلك على النحو التالي:

---

(1) - عبد الكريم دحو الإدريسي، مرجع سابق، ص 14.

(2) - لمزيد من التفاصيل حول مديرية الوقاية وأمن الدولة اتظر الموقع الالكتروني الخاص بها:

http://www.sgdsn.gouv.fr/site_article58.html

(3) - عبد الكريم دحو الإدريسي، مرجع سابق، ص 17.

(4) -Commission de Sécurité ,Guide Pratique à l'usage des Élu,france, 2011,disponibl en ligne, leM 02-23-2017:

http://www.gard.gouv.fr/content/download/3391/22881/file/Guide_maires_2011.pdf

- **القسم الوطني لقمع جرائم المساس بالأموال والأشخاص:**

بدأ هذا القسم مهامه سنة 1997 وتلقى حوالي 3000 بلاغ خلال عام 2004، ويتألّف من 6 محققين مختصين في التحقيق في الجريمة المعلوماتية، ويقوم هذا القسم بمعالجة الجرائم مع إحالة القضايا الأخرى التي يكون المشتبه فيه معروفا إلى الجهات القضائية المختصة[1].

- **المكتب المركزي لمكافحة جرائم تكنولوجيا المعلومات والإتصالات:**

تمّ إنشاء هذا المركز الوطني بموجب مرسوم وزاري رقم (405/2000) بتاريخ 2000/05/15[2]، وذلك بالإدارة العامة للشرطة الوطنية داخل المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية.

يتمتّع هذا المكتب باختصاص وطني لمكافحة هذه الجرائم المستحدثة، ويمارس عمله من خلال وحدة العمليات ووحدة المساعدة التقنية ووحدة التحليل والتوثيق العملي[3].

يكلف هذا المكتب الوطني وفقا للمادة الثالثة من المرسوم السابق ذكره بملاحقة مرتكبي الجرائم المتعلقة بتكنولوجيا المعلومات والإتصالات، إضافة إلى تقديم يد المساعدة للشرطة القضائية في إجراءات التحقيق لهذه النوعية من الجرائم[4].

---

(1)ـــ عبد الكريم دحو الإدريسي، مرجع سابق،، ص 122.

(2)-Décret n°2000-405 du 15 mai 2000 portant création d'un office central de luttecontre la criminalitéliée aux technologies de l'information et de la communication.

(3)ـــ نافد ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، رسالة دكتوراه في الحقوق، جامعة عين شمس، 2007، ص 460.

(4) -Article 3 de décret n°2000-405 du 15 mai 2000 portant création d'un office central de luttecontre la criminalité liée aux technologies de l'information et de la communication D'animer et de coordonner, au niveau national, la mise en oeuvre opérationnelle de la lute contre les auteurs et complices d'infractions spécifiques à la criminalitél iée aux technologies de l'information et de la communication ;
2° De procéder, à la demande de l'autorité judiciaire, à tous actes d'enquête et de travaux techniques d'investigations en assistance aux services chargés d'enquêtes de police judiciaire sur les infractions dont la commission est facilitée par ouliée à l'utilisation des technologies de l'information et de la communication, sans préjudice de la compétence des autres offices centraux de police judiciaire ;
3° D'apporter assistance aux services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects, de la direction générale de la concurrence, de la consommation et de la répression des fraudes et de tout autre service, en cas d'infractions visées à l'alinéa 2 de l'article 2, quant ils en font la demande. Cette assistance ne dessaisit pas les services demandeurs ;

بالإضافة إلى ذلك، تُوكل للمكتب مهمتان رئيسيتان[1]:

الأولى: تتعلق بالجانب الميداني في المكافحة، وهي:

ـــ مباشرة تحقيقات قضائية ذات مستوى تقني عال، وهي تحقيقات تباشر بمبادرة أو بطلب من القضاة.

ـــ تقديم المساعدة التقنية بمناسبة إنجاز تحقيقات قضائية من طرف مصالح أخرى(مثل المصالح المعنية بتجارة المخدرات).

أما المهمة الثانية: ترتبط بالنشاط الاستراتيجي، وتتمثل في:

ـــ التكوين والتنشيط وتنسيق عمل باقي المصالح المختصة في ميدان مكافحة الجرائم المرتبطة بالتقنيات المعلومات والاتصال.

ـــ والتعاون الدولي، حيث أن هذا المكتب المركزي يعتبر نقطة الاتصال الوطنية بالنسبة لفرنسا في ميدان التعاون الشُرطي الأوربي والمؤسّسي.

ج ـــ على مستوى مصالح الدرك الوطني: ينعقد الإختصاص لرجال الدرك الوطني في مكافحة الجرائم المعلوماتية على مستويين: على مستوى الإختصاص الوطني، وعلى مستوى الإختصاص الإقليمي، على النحو الآتي:

1 ـــ على مستوى الإختصاص الوطني: نجد على مستوى هذا الاختصاص المراكز الآتية:

- **قسم الانترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية:**

تم إنشاؤه عام 1998، ويختص بجمع الأدلة الرقمية (Preuves numiriques) ويصل عدد أفراده إلى 14 شخص مختصين في مجال تقنية المعلومات فيهم 8 مهندسين و6 تقنيين.

4° D'intervenir d'initiative, avec l'accord de l'autorité judiciaire saisie, chaque foisque les circonstances l'exigent, pour s'informer sur place des faits relatifs aux investigations conduites.

[1] - عبد الكريم دحو الإدريسي، مرجع سابق، ص 31ـــ32.

- **المركز الوطني لتحليل الصور الإباحية:**

تمّ إنشاؤه في أكتوبر 2003، ويختص بجمع وترتيب الصور التي يتم ضبطها أثناء التحقيق القضائي في قاعدة بيانات، كما يقوم بالمشاركة في التحقيقات وإجراءات الضبط الهامة[1].

- **القسم المعلوماتي الالكتروني التابع لمعهد البحوث الجنائية للدرك الوطني:**

لقد تم إنشاؤه عام 1992، ويختص بتحليل بيانات الحاسوب في إطار التحقيقات القضائية المتعلقة بالأعمال الإقتصادية والمالية، وبالتالي يقوم بتقديم المساعدة التقنية للدرك الوطني.

2 ــ **على مستوى الإختصاص الإقليمي:** كما نجد على مستوى هذا الاختصاص أيضا المراكز التالية:

- **الوحدات الإقليمية ووحدات البحوث:**

إذ تساهم هذه الوحدات إلى جانب الوحدات المركزية السابقة في مكافحة جرائم الانترنت على المستوى الإقليمي.

- **وحدات أقسام الاستعلامات والتحقيقات القضائية:**

وتتركز أعمال هذه الوحدات على تبادل الخبرات التقنية وتبادل الإختصاصات بين رجال الدرك الوطني. وإلى جانب وحدات الشرطة والدرك المختصة بمكافحة جرائم المعلوماتية، توجد خلية استقبال وتحليل الانترنت والتي تم إنشاؤها سنة 1998 من قبل المديرية العامة للجمارك.

د ــ خليّة مراقبة التجارة الإلكترونية ومعالجة البريد الإلكتروني:

أنشئت هذه الخلية في 12 ديسمبر 2001 بموجب قرار رقم 2001 ــ1179[2]، حيث قررت الحكومة إنشاء خلية تابعة للمديرية العامة للمنافسة والاستهلاك، وزجر الغش بمورلي، وقد كلفت هذه الخلية بمراقبة التجارة الالكترونية والتوجيه والتدبير ــ إلكترونيا ــ للطلبات والشكايات الصادرة عن المستهلكين أو المقاولات[3].

---

(1) ــ نبيلة هبة هروال، مرجع سابق، ص 123.

(2) -Décret n°2001-1179 du 12 décembre 2001 relatif aux services déconcentrés de la direction générale de la concurrence, de la consommation et de la répression des fraudes.

(3) - عبد الكريم دحو الإدريسي، مرجع سابق، ص 33.

وبصفة هذه الخليّة تشرف على شبكة المراقبة فهي تتولى المهام التالية[1]:

ـــ مراقبة مواقع الانترنت التجارية وممارساتها: في حالة الاشتباه بوجود مخالفات لقانون الاستهلاك، فإنه يمكن للخلية أن تباشر معاينات عن بعد لتوافي المديريات أو الوزارات المختصة ترابيا بتقارير في هذا الشأن، وذلك لإنجاز تحقيقات معمقة ومتابعة هذه المخالفات.

أمّا بالنسبة لباقي المخالفات التي لا تختص بها، ترسل المعلومات الضرورية إلى المصالح المعنية مثل المديرية العامة للضرائب والدرك والشرطة.

ـــ يسمح نشاط موقع مورلي بالحصول على مجموعة من المعلومات التي توضح بالخصوص المشاكل التي يقع فيها الأفراد، والمشاكل المحتملة لتطبيق قانون الاستهلاك، وبالتالي تتطلع الخلية على كل المسائل القانونية في ميدان التجارة الالكترونية.

وفيما يتعلق بالدول العربية فقد خصّصت هي الأخرى أجهزة متخصصة لمكافحة هذه الجرائم ونذكر منها على سبيل المثال:

1. **مصر:** قامت وزارة الدخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم خلال الشبكة المعلوماتية من خلال الاعتماد على التقنيات الحديثة، تتمثل هذه الجهات فيما يلي:

- **الإدارة العامة للمعلومات والتوثيق:** تعد هذه الإدارة من أكثر الإدارات تعاملا مع الجرائم المعلوماتية بوزارة الداخلية، حيث أنها تختص بعمليات المتابعة الفنية لعديد من الجرائم، وذلك من خلال التحري عن الجرائم التي تبلغ إلى الإدارة من الإدارات الأخرى، وذلك من خلال استخدام شبكة الانترنت وتحديد شخص المتهم[2].
- **إدارة مكافحة جرائم الحاسبات وشبكات المعلومات:** أنشأت هذه الإدارة سنة 2002 بموجب قرار وزاري رقم 13507 لسنة 2002 ، وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة، وتشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثلاث أقسام رئيسية هي[3]:

---

(1) - عبد الكريم دحو الإدريسي، مرجع سابق، ص 34.

(2)- سليمان أحمد فاضل، مرجع سابق، ص 398.

(3) ـــ نفس المرجع، ص 398.

ـــ قسم العمليات، ـــ قسم التأمين، ـــ وقسم البحوث والمساعدات الفنيّة. وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية، فهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحاسبات والشبكات وتختص بمكافحة جرائم الأنترنت على مختلف أنواعها[1].

2. **قسم مكافحة جرائم الحاسبات وشبكات المعلومات:** وقد أنشئ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي ويخضع من حيث الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جرائم عليها باستخدام الأساليب والتقنيات العلمية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات[2].

2. **في الأردن:** قامت الحكومة الأردنية في سبيل مواجهة تلك الجرائم والحد من خطورتها وضبط مرتكبيها وتقديمه للعدالة بتأسيس قسم خاص في مديرية الأمن العام للتعامل مع تلك القضايا باسم **قسم جرائم الحاسوب التابع لإدارة المختبرات والأدلة الجرمية** وذلك في سنة 1998[3]، ويختص هذا القسم بما يلي[4]:

ـــ معالجة واستخراج الأدلة الرقمية من مختلف الأجهزة الإلكترونية ووسائط التخزين والحواسيب بكافة أنواعها، والأجهزة الخلوية..

---

[1] ـــ نبيلة هبة هروال، مرجع سابق، ص 141.

وضعت هذه الادارة عدة طرق للإبلاغ عن جرائم الانترنت أهمها تخصيص الخط الساخن (108)، وتشير الاحصائيات ألى أنه في عام 2010 تم تلقي عدد 1912 بلاغا من بينهم 1378 عبرهذا الخط، وقد كشف مديرإدارة جرائم الحاسبات وشبكات المعلومات عن نجاح ضباط الادارة خلال سنة 2016 في ضبط 2372 قضية سب، 1623 قضية إساءة، و193 قضية نصب من خلال الانترنت، و77 قضية اختراقات حسابات شخصية. حسام محمد نبيل الشنراقي، دور أجهزة البحث الجنائي في مكافحة جرائم المعلومات، ورقة عمل مقدمة في ندوة "الاستخدام الآمن لشبكة الانترنت، جامعة طنطا، بتاريخ 15/5/10، ص 14.

[2] ـــ نبيلة هبة هروال، مرجع سابق، ص 142.

[3] ـــ مرنيز فاطمة، الإعتداء على الحق في الحياة الخاصة عبر شبكة الانترنت، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2012 ـــ 2013، ص 195.

[4] ـــ جلال محمد الزغبي، مكافحة جرائم تقنية المعلومات في الأردن، المؤتمر الدولي لمكافحة جرائم تقنية المعلومات، أبوظبي بدولة الإمارات العربية المتحدة، بتاريخ : 14 ـــ 12 ـــ 2011، ص 7. ،

ـــ تتبع البريد الإلكتروني والـــ " IP Adress " وتحديد مصدر الجهاز الذي تم من خلاله ارتكاب عمل جرمي معين(سرقة كلمات المرور، سرقة أرقام بطاقات الإئتمان..).

ـــ كما يقوم هذا القسم بتحليل الأشرطة المرئية وتفصيل الصور والفديو فيها في قضايا السرقات والصراف الآلي، وغيره من القضايا التي يتم تصويرها بكاميرات المراقبة.

ـــ ويقوم ايضا بتوثيق كل ذلك يتقارير مخبرية تسلم للجهات الطالبة ومنها القضائية .

كما تم تأسيس قسم الإسناد الفني في عام 1997 في كل من إدارة الأمن الوقائي وإدارة البحث الجنائي، ويقوم هذا القسم باستقبال الشكاوى وإجراء التحقيق الأولي مع المشتبه بهم وإرسال الأجهزة والمعدات والعينات المضبوطة إلى قسم جرائم الحاسوب في إدارة المختبرات والأدلة الجرمية وذلك لاستخراج الأدلة الرقمية[1] .

بالاضافة إلى ذلك تم إنشاء مديرية أمن المعلومات وحوادث الشبكات بمركز تكنولوجيا المعلومات الوطني، حيث يقدم العديد من الخدمات المتعلقة بأمن وسلامة معلومات الحكومة الالكترونية كما يلي[2]:

ـــ خدمة حماية المعلومات والشبكات، وذلك من خلال القيام بـــ: استقبال التبليغات والتقارير عن حوادث تكنولوجيا المعلومات، التعامل مع الأدلة الرقمية الخاصة بأمن المعلومات والتعاون مع الجهات المعنية.

ـــ خدمة الفحص الأمني للمواقع الالكترونية الحكومية وذلك من خلال: الكشف المبكر لحالات الإختراق التي قد تتعرض لها الأنظمة والمواقع الالكترونية الحكومية، وتبليغ الجهات المعنية.

ـــ خدمة التدقيق على أمن المعلومات وذلك للتأكد من أفضل الممارسات لحماية المعلومات الحكومية.

---

[1]ـــ مرنيز فاطمة، مرجع سابق، ص 196.

[2]ـــ مركز تكنولوجيا المعلومات الوطني بالمملكة الهاشمية الأردنية متاح بتاريخ: 12 / 04/ 2016 ، على الموقع التالي:
http://www.nitc.gov.jo/

ـــ خدمة إصدار الشهادات الرقمية (Certificates SSL) للمواقع الالكترونية الحكومية، وذلك لضمان الدخول الآمن على هذه المواقع من خلال تشفير الاتصال بين العميل ومواقع المؤسسات الإلكترونية للحصول على الخدمات المقدمة بشكل آمن وموثوق.

ـــ نشر التوعية في مجال أمن المعلومات وذلك من خلال: عقد الدورات الخاصة بأمن وسلامة المعلومات، إرسال رسائل نصية إرشادية تحذيرية وتوجيهية، التوعية بمخاطر الأنترنت على الأفراد والمؤسسات.

ثانيا ـــ وحدات الضبط القضائي المختصة في الجرائم الواقعة على الحكومة الإلكترونية على المستوى الوطني:

تأثرت الجزائر على غرار الدول الأخرى بمخاطر الجريمة المعلوماتية، خاصة وهي في إطار تطبيق مشروع "الجزائر الالكترونية 2013"، مما تطلب الأمر توفير أجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة المعلوماتية، وكان ذلك فعلا حيث خصّصت الدولة آليات على مستوى جهاز الشرطة، وأخرى على مستوى الدرك الوطني، بالإضافة إلى إنشاء هيئة متخصصة في مكافحة هذه الجرائم وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

لتسهيل عمل هذه الأجهزة قام المشرّع بتوسيع إختصاص أعضاء الضبط القضائي لمسايرة الوضع المستجد للجريمة المعلوماتية وذلك على النحو التالي[1]:

❖ **الأجهزة المختصة على مستوى جهاز الشرطة:** أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية والتقنية بالجزائر العاصمة[2] و4 مخابر جهوية موزعة على التراب

---

[1] ـــ سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2012 ـــ 2013، ص 107.

[2] ـــ المخبر المركزي للشرطة العلمية والتقنية أو المعهد الوطني للشرطة الجنائية: هو أحد مراكز تكوين الشرطة الجزائرية تم إنشاؤه سنة 1999، لتلبية الحاجات التكوينية التخصصية للشرطة الجزائرية بالجزائر العاصمة، بمصالحه 15، يحل المرتبة الثانية إفريقيا والأولى عربيا بين مخابر الشرطة.

سجلت المديرية العامة للأمن الوطني أكثر من 1055 جريمة إلكترونية خلال سنة 2016، والتي تورط فيها أكثر من 946 شخص، وهذه الجرائم تتعلق بالمساس بالأشخاص عبر الانترنت، الإعتداء على سلامة الأنظمة المعلوماتية، الإحتيال عبر الانترنت. ولأجل الحد من هذه الظاهرة تشارك المديرية لعامة للأمن الوطني كل سنة الحملة التوعوية العالمية المصادفة لليوم العالمي للأنترنت الآمن في 7 فبراير،

الوطني بكل من قسنطينة، وهران، بشار وتمنراست، تحتوي هذه المخابرعلى فروع تقنية من بينها خلية الإعلام الآلي[1]، بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر.

❖ **الأجهزة المختصة على مستوى الدرك الوطني:** يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام (ببوشاوي) التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية[2] . هذا بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها (ببئر مراد رايس) والتابع لمديرية الأمن العمومي للدرك الوطني[3].

وكان شعار سنة 2017 هو" كن أنت التغيير: لنتحد من أجل شبكة انترنت أفضل".انظر: الموقع الرسمي للشرطة الجزائرية: بتاريخ: 2017/02/10. http://www.dgsn.dz/

(1) ــ انظر في تفاصيل ذلك الموقع الرسمي للشرطة الجزائرية: بتاريخ 2017/02/10.

http://www.dgsn.dz

(2)- أحدث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني بموجب المرسوم الرئاسي رقم 04 183 المؤرخ في 8 جمادى الأولى عام 1425هـ الموافق 26 جوان سنة 2004 م، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي. ج.ر.ج. ع 41 الصادرة في 27 جوان 2004.

ومن مهام المعهد حسب المادة 6 من المرسوم الرئاسي المنوه عنه سابقا ما يلي:

- ✓ إجراء، بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، الخبرات و الفحوص العلمية التي تخضع لإختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية، بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح؛
- ✓ تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة بإستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع و تحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة؛
- ✓ المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام؛...إلخ.

(3)-وهو هيكل متخصص تابع لقيادة الدرك الوطني، يقع مقره بالجزائر العاصمة بالدائرة الادارية لبئر مراد رايس، ولممارسة صلاحياته، تم تقسيمه إلى ما يلي: قسم (01) اليقظة المعلوماتية؛ قسم (01) التحقيقات المعلوماتية، قسم (01) الأمن الرقمي؛ مصلحة (01) التقنية والاستغلال؛ مصلحة (01) الإدارة والوسائل.

ومن صلاحيات مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ما يلي:

- ✓ ضمان يقظة عامة ومستمرة على شبكة الانترنيت؛
- ✓ الوقاية من كل أنواع الجرائم المرتبطة بتكنولوجيات الإعلام والإتصال و مكافحتها؛
- ✓ مساعدة السلطات القضائية وإجراء الخبرة التقنية المتعلقة بالجرائم المرتبطة بتكنولوجيات الإعلام والإتصال؛
- ✓ تقديم المساعدة للتنظيمات العمومية الوطنية، في ما يتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والإتصال ومكافحتها؛
- ✓ تقديم المساعدة لوحدات الدرك الوطني المكلفة بالشرطة القضائية لمعاينة الجرائم التي سهل إرتكابها أو المرتبطة باستعمال أنظمة الإعلام الآلي وتكنولوجيات الإعلام والإتصال، جمع أدلتها والبحث عن مرتكبيها؛
- ✓ إعداد و تفعيل الاستراتيجية الرقمية للدرك الوطني؛

كما تمّ إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الإستعلام والأمن: وذلك على مستوى مديرية الأمن الداخلي بدائرة الاستعلام والأمن بوزارة الدفاع الوطني، بموجب المرسوم الرئاسي رقم (14ـــ183)، المؤرخ في 11 يونيو سنة 2014، المتضمن إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الإستعلام والأمن[1]، ويُسيرها ضابط سام يعين طبقا للأحكام التنظيمية المعمول بها في وزارة الدفاع الوطني، وذلك طبقا للمادة الثانية(2) من هذا المرسوم الرئاسي، وقد حددت مهامها بصفة دقيقة وعلى سبيل الحصر[2] وفق المواد 4 و5 و6 و8 من المرسوم أعلاه، حيث تقوم في إطار مهامها وطبقا للقوانين المعمول بها، بضبط الإجراءات القضائية اللازمة لجمع الأدلة المعنوية والمادية المرتبطة بالجرائم والجنح التابعة لاختصاصها المنصوص عليها في المادتين الخامسة(5) والسادسة (6) من هذا المرسوم[3].

كما تقوم هذه المصلحة أيضا بمعالجة الآثار القضائية للقضايا المتصلة بأمن الإقليم، الإرهاب، التخريب والجريمة المنظمة، هذا بالإضافة إلى المساهمة في الوقاية من أي شكل من أشكال التدخل الأجنبي، وفي قمعه، كما تساهم في الوقاية من أعمال الإرهاب أو الأعمال التي تمس بأمن

- ✓ المشاركة في إعداد وتفعيل الاستراتيجية الرقمية الوطنية؛
- ✓ التمكن والتحكم في قواعد أمن التكنولوجيات وأنظمة الإعلام؛
- ✓ المشاركة في تقوية أمن أنظمة الإعلام الوطنية وحماية فضاء المعلومات الوطني؛
- ✓ المشاركة في إعداد القوانين والنظم المسيرة لمجال تكنولوجيات الاعلام والاتصال؛
- ✓ إنشاء علاقات تنسيق وتعاون مع مختلف المتدخلين في مجال تكنولوجيات الإعلام والاتصال.الرائد حلاب منير، دور الدرك الوطني في ميدان محاربة جرائم المعلوماتية، مداخلة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، السابق الذكر، ص 3. وفي هذا الإطار صرح الرائد من خلال المداخلة على عدد القضايا المعالجة من طرف مركز الوقاية من الجرائم المعلوماتية للدرك ا لوطني، من سنة 2009 إلى 2016 وهي تتراوح مابين 18 قضية إلى 465 قضية في سنة 2016، وهذه الجرائم تنصب على: التهديد، جرائم المساس بالنظام العام، الإرهاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات(الإختراق)، تحرض الفصر على الفسق والدعارة، الإعتداء على الحياة الخاصة.

[1] ـــ المرسوم الرئاسي رقم 14ـــ183 المؤرخ في13 شعبان عام 1435 الموافق لـــ 11 يونيو سنة 2014، يتضمن إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الإستعلام والأمن ومهامها وتنظيمها، ج.ر.ج ع 32، الصادر في 12 يونيو 2014.

[2] ـــ انظرالمادة الخامسة والسادسة من نفس المرسوم.

[3] ـــ محمد بكرارشوش، الإختصاص القضائي في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة، العدد الرابع عشر، جانفي 2016، ص 317.

الدولة...كما تساهم في الوقاية من الإجرام المتصل بالتكنولوجيات الجديدة للإعلام والإتصال، وفي قمعه.

وعليه خصّص المشرّع الجزائري مهام خاصة لأعضاء الضبطية القضائية في إطار القواعد العامة للإجراءات الجزائية، فضلا وجود هيئة أخرى متخصصة في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

❖ **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:**

استحدث المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بموجب قانون رقم 09ـــ04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والإتصال ومكافحتها، في المواد 13 و14 من هذا القانون.

تتولّ هذه الهيئة وفقا للمادة 14 تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، وأيضا تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وتحديد مكان تواجدهم.

وبتاريخ 8 أكتوبر سنة 2015 أصدر مرسوم رئاسي رقم 15ـــ261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافتها[1]، وتعد هذه الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي، توضع لدى الوزير المكلف بالعدل، ويحدد مقرها بمدينة الجزائر(المادة 3 من المرسوم الرئاسي السابق الذكر)، وفي إطار تشكيل الهيئة وتنظيمها نجد المادة 6 من المرسوم الرئاسي رقم 15ـــ261 السالف الذكر تضم ما يلي: ـــ لجنة مدبرة، ـــ مديرية عامة، ـــ مديرية للمراقبة الوقائية واليقضة الإلكترونية، ـــ مديرية للتنسيق التقني، ـــ مركز للعمليات التقنية، ـــ ملحقات جهوية.

[1] ـــ مرسوم رئاسي رقم 15ـــ 261 مؤرخ في 24 ذي الحجة عام 1436 الموافق لـــ 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج. ر ع 53 لسنة 2015.

ما يهمّنا في هذه التشكيلة هو اللّجنة المدبّرة باعتبارها تتشكّل من الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيا الإعلام والإتصال، **قائد الدرك الوطني، المدير العام للأمن الوطني،** ممثل عن رئاسة الجمهورية، وممثل عن وزارة الدفاع الوطني، وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وعليه نلاحظ من خلال ما سبق أن هذه الهيئة تتوفر على تشكيلة متنوعة من مختصين في مجال التقنية لذلك تساهم في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والإتصال وهومانصت عليه المادة الرابعة من هذا المرسوم الرئاسي، وبالتالي التخفيف من ميزانية الدولة، فعوض أن تبعث الدولة إطارات من الدرك الوطني إلى بلدان أجنبية مثل فرنسا والولايات المتحدة الأمريكية تكتفي بتكوينهم وتأهيلهم في هذه الهيئة الوطنية، وبالتالي تطوير كفاءات سلك الدرك الوطني، حتى تكون أكثر عملية في مكافحة الجرائم المعلوماتية.

من أجل التجسيد الفعلي وتسهيل مهام الأجهزة المنوه عنها سابقا(ضباط الشرطة القضائية بصفة عامة)، وفي إطار مكافحة الجريمة المعلوماتية والتي تتطلب كفاءة مهنية عالية، تناسب وخصوصيات هذه الجرائم المستجدة، قام المشرع الجزائري بإدخال تعديلات جوهرية على قانون الإجراءات الجزائية بالقانونين 14/04[1]، و22/06[2] حيث وسّع بموجبهما الإختصاص الإقليمي لأعضاء الضبطية القضائية[3]، كلما تعلق الأمر ببحث ومعاينة إحدى الجرائم المنصوص عليها في المادة 16/ 7 من ق.إ.ج.ج وحصرتها فيما يلي: "جرائم المخدرات والجريمة المنظمة عبر الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف".

---

[1]- قانون رقم 04ـــ14 مؤرخ في 27 رمضان عام 1425، الموافق لـــ 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66ـ155 المؤرخ في 18 صفر 1386 الموافق لـــ 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج.ر.ج. ع 71 ـــ الصادرة في 10 نوفمبر 2004.

[2]- قانون رقم 06ـــ 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق لـــ 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66ـــ 155 المؤرخ في 18 صفر 1386 الموافق لـــ 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج.ر.ج ع 84 الصادرة في 24 ديسمبر 2006.

[3]- طبقا لنص المادة 1/16 ق.إ.ج. ج يتحدد الإختصاص المحلي لأعضاء الضبطية القضائية العامة في الجرائم العادية، بالحدود التي يباشرون ضمنها وظائفهم المعتادة.

بناء على المواد 16 و16 مكرّر من ق.إ.ج.ج فإن الإختصاص الإقليمي لنشاط ضباط الشرطة الفضائية، اتسع إقليميا فيما يخص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ليشمل كامل الإقليم الوطني.

كما أنه طبقا للمواد من 40 مكرر 1 إلى 40 مكرر3 ق.إ.ج، فإن الإختصاص الإقليمي لنشاط ضباط الشرطة القضائية اتسع إقليميا ليشمل اختصاص إقليمي لمحاكم أخرى غير المحكمة التي يباشرون معامهم في دائرة اختصاصها، حيث حدد هذا الإختصاص الإقليمي الموسع وفقا لأحكام المرسوم التنفيذي رقم (06ـــ348) المؤرخ في 05ـــ10ـــ2006، المتضمن تمديد الإختصاص المحلي لبعض المحاكم، ووكلاء الجمهورية وقضاة التحقيق[1].

هذا بالإضافة إلى أن ضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، يمارسون مهامهم في كامل التراب الوطني طبقا للقانون رقم 09ـــ04 المنوه عنه سابقا، والنصوص التنظيمية الصادر لتطبيق أحكامه، لاسيما المرسوم الرئاسي رقم 15ـــ261 المحدّد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها[2].

ثالثا: الأجهزة المتخصصة بالبحث والتحري عن الجرائم الواقعة على الحكومة الالكترونية على المستوى الدولي والإقليمي.

من المعلوم أن الجرائم المعلوماتية بما في ذلك جرائم الإعتداء على الحكومة الالكترونية تتميز بأنها عابرة للحدود الوطنية، حيث يمكن أن يتعدى أثرها عدة دول، لذا كان لابد من وجود تعاون دولي لمكافحة هذا النوع من الإجرام، ومن أساليب التعاون الدولي التعاون الأمني الذي يمكن أن يحقق أهداف لايمكن للشرطة الإقليمية تحقيقها، ومن أبرز هذه الأجهزة نذكر ما يلي:

---

[1]- مرسوم التنفيذي رقم (06ـــ348) المؤرخ في 15 رمضان 1427 الموافق لـــ 05ـــ10ـــ2006، بتضمن تمديد الإختصاص المحلي لبعض المحاكم، ووكلاء الجمهورية وقضاة التحقيق، ج..ر.ج، ع 63، الصادر في 8 اكتوبر 2006.

[2]ـــ علالي بن زيان، معيار الإختصاص في الجرائم المعلوماتية على ضوء التشريع الإجرائي الجزائري، مداخلة مقدمة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، مرجع سابق، ص 5.

1 ــ على المستوى الدولي: تعد **المنظمة الدولية للشرطة الجنائية "الأنتربول"**[1]من أهمّ الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم المعلوماتية[2] الواقعة على الحكومة الالكترونية، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المستحدث. وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين[3]:

الأولى: تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الموجودة في أقاليم الدول الأطراف.

الثانية: التعاون في ملاحقة المجرمين الفارين والقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

تعمل المنظمة الدوليّة للشرطة الجنائيّة في مجال الجرائم المعلوماتية بوضع قائمة إسمية لضباط متخصصين يمكن الإستعانة بهم في مجال البحث والتحري في مثل هذه القضايا، كما توفر هذه المنظمة للدول الأطراف المعلومات الازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين. ولقد أنشأت هذه المنظمة وحدة متخصصة في الجرائم المعلوماتية تقوم لتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته[4].

---

(1) ــ تم إنشاء هذه المنظمة سنة 1923، تحت إسم اللجنة الدولية للشرطة الجنائية وذلك للتنسيق بين أجهزة الشرطة في الدول الأوربية في مجا مكافحة الجريمة، ونم إيقاف نشاطها إبان الحرب العالمية الثانية، ثم أعيد فتحها خلال مؤتمر فينا تحت إسم " منظمة الشرطة الجنائية الدولية" سنة 1956، وهي تظم 177 دولة عضوا وتظم أجهزة هي: الجمعية العامة، اللجنة التنفيدية، الأمانة العامة، وجهاز المستشارين والمكاتب المركزية الوطنية. لمزيد من التفاصيل راجع: علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة "دراسة للاستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات"، إيتراك للنشر والتوزيع، القاهرة، 2000، ص 174 وما بعدها.

(2) ــ وقد أكد سكرتير الأنتربول الدولي" Raymond Kendall " في مؤتمر جرائم الأنترنت المنعقد بـــ"لندن" بتاريخ:09ــ 10ــ 2000، على ضرورة تعاون الدول في مكافحة جرائم الأنترنت، باعتبار هذه الأخيرة تبرز كظاهرة دولية، وقد أكد على أنه يجب على المجتمع الدولي عدم الانتضار إلى حين عقد معاهدات دولية وإتفاقات في هذا الإطار، بل يجب الشروع وبشكل فوري في مكافحة هذه الجرائم.انظر: عمر محمد أبوبكر يونس، الجرائم الناشئة عن استخدام الانترنت..، مرجع سابق، ص 814.

(3) ــ علاء الدين شحاتة، مرجع سابق، ص 14.

(4) ــ سعيداني نعيم، مرجع سابق، ص 108.

إلى جانب الأنتربول، هنالك منظمات لها دور فعال في مواجهة هذا النوع المستحدث من الإجرام على المستوى الدولي، **كمنظمة التعاون الإقتصادي والتنمية "OECD" ومجموعة الثمانية الإقتصادية (G8)**، حيث قامت بإعداد ملتقى دولي في نهاية نوفمبر 2000 في طوكيو لتكوين قوة دولية، تتمثل مهامها في تحقيق أمن تكنولوجيا المعلومات[1].

2 ــ على المستوى الإقليمي:

- **الشرطة الأوربية أو الأوروبول:** وهو جهاز على مستوى الإتحاد الأوربي تم إنشاؤه عام 1992 ومقره في مدينة لاهاي بهولندا لكي يكون حلقة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة لملاحقة الجناة في الجرائم العابرة للحدود[2]، ومنها جرائم الاعتداء الالكتروني على الحكومة الالكترونية.

بمبادرة من الشرطة القضائية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه إسم "ICROS" [3]في سنة 2010، بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء[4].

- **الأورجست:** وهو جهاز يعمل على المستوى الأوربي إلى جانب الأوربول في مجال مكافحة الجرائم الخطيرة، تم إنشاؤه عام 2002، وينعقد إختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الإتحاد الأوربي أو دولة عضو مع دولة أخرى من غير الإتحاد الأوربي. ويعد الأورجيست دعامة في فعالية التحقيقات والمطاردات المتبعة من قيل السلطات القضائية الوطنية، وخصوصا فيما يتعلق بالجرائم المعلوماتية[5].

---

[1]ــ جميل عبد الباقي الصغير، مرجع سابق، ص 80.

[2]ــ نفس المرجع ، ص 79.

[3] - Internet Crime Repportinge Online System.

[4]ــ جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالانترنت، مرجع سابق، ص 72 وما بعدها.

[5] -Harmonisation des moyens de lute contre la cybercriminalité, revue de web, réalise le 22-04- 2004, disponible en ligne à l'adresse suivante://www.finances.gouv.fr

الفرع الثاني: أساليب التحري الخاصة عن الجرائم الواقعة على الحكومة الالكترونية

إنّ التطوّر العلمي والتكنولوجي في مختلف المجالات أدى إلى ظهور أشكال إجراميّة لم تكن معروفة من قبل كالجرائم المعلوماتية مثلا، ونظرا للطبيعة اللاماديّة لهذه الجريمة والخصوصيات التي تتميز بها، فهي تثير صعوبات عملية عديدة بالنسبة للسلطة المكلفة بالبحث والاستدلال، حيث لم تعد أساليب البحث والتحري التقليدية كافية وفعالة لمواجهة هذه الأشكال الإجرامية الجديدة، ممّا استدعى الأمر ضرورة إعتماد إجراءات حديثة تتماشى والطرق الإجرامية، وتبعا لذلك قام المشرع الجزائري بتبني أساليب خاصة للتحري[1] عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات بصفة عامة وجرائم الإعتداء الإلكتروني على الحكومة الإلكترونية بصفة خاصة. وذلك من خلال تعديل قانون الإجراءات الجزائية الجزائري بموجب القانون رقم 06 ــ 22 المؤرخ في 20 ديسمبر 2006.[2] وتتمثل هذه الإجراءات في عملين:

ــ الأول: هي عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

ــ أمّا الثانية: فهي عملية التسرب.

عند استقراءنا لهذين الإجرائين بداية يتضح أنهما يتميزان بالمساس بحق الإنسان في الخصوصية، وهي مصلحة تتعارض مع مصلحة الدولة في العقاب، وهي تمس بذلك مبادئ دستورية تتعلق بحقوق الأفراد ومصالحهم، غير أن المشرع الجزائري بعد إقراره بمشروعية هذه الإجراءات حدد نطاقها الموضوعي، حيث لا يتم اللجوء إليها إلاّ في ظروف استثنائية تحدّد في الجرائم الخطيرة، ووفق شروط صارمة لضمان حماية الحياة الخاصة للمشتبه فيها. إذن فماهي شروط اللجوء إلى هذه الأساليب

---

[1] ــ لم يعط المشرع الجزائري تعريفا محددا لعبارة " أساليب التحري الخاصة"، وإن نص صراحة على إمكانية اللجوء إلى هذه الأساليب في قانون مكافحة الفساد رقم 06 ــ01 المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته. وقد عرفا البعض أنها تلك العمليات أو الإجراءات والتقنيات التي تستخدمها الضبطية القضائية تحت الرقابة والإشراف المباشرة للسلطة القضائية، بغية البحث والتحري عن الجرائم الخطيرة المقررة في قانون العقوبات، وجمع الأدلة عنها والكشف عن مرتكبيها وذلك دون علم ورضا الأشخاص المعنيين. لوجاني نور الدين، أساليب البحث والتحري الخاصة وإجراءاتها، يوم دراسي حول: علاقة النيابة العامة بالشرطة القضائية احترام حقوق الإنسان ومكافحة الجريمة"، أمن ولاية إليزي، المديرية العامة للأمن الوطني، وزارة الداخلية، الجزائر، 12 ديسمبر، 2007، ص4.

[2] ــ قانون رقم 06ــ22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66ــ155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الاجراءات الجزائية، ج.ر.ج. ع 84، الصادرة في 34 ديسمبر2006.

الخاصة لاسيما أسلوبي اعتراض المراسلات وتسجيل الأصوات والتقاط الصور (أولا). وأسلوب التسرب (ثانيا).

أولا ــ عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: نصّ المشرع الجزائري على هذه الأساليب في المواد من65 مكرر 5 إلى غاية 65 مكرر10 من قانون الإجراءات الجزائية، وفيما يلي سنحاول تحديد مفاهيم هذه الآساليب (أ)، ومن تمّ بيان الشروط أو الضمانات القانونية اللازمة لتطبيق هذه العمليات (ب).

(أ) ــ **تحديد مفهوم عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:**

- **اعتراض المراسلات:**

لم يتطرق المشرع إلى تحديد مفهوم إعتراض المراسلات، في حين عرفه المشرع الأمريكي في الباب الثالث من القانون الفدرالي الأمريكي لسنة1968 بأنه:"**الإكتساب السمعي أو أي إكتساب لمحتويات أية أسلاك أو أي إتصالات شفوية باستخدام أي جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر**" [1]، فهو إجراء تحقيقي ومن أهم وسائل البحث والتحري يباشر خلسة وينتهك فيه سرية الأحاديث الخاصةــ تأمر به السلطة القضائية في الشكل المحدد قانونا، بهدف الحصول على دليل غير مادي للجريمة، يتمثل مضمونه في المراسلات.

يقصد بالمراسلات قانونا: "**كل إتصال مجسد في شكل كتابي يتم عبر مختلف الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو يطلب منه. ولاتعتبر الكتب والمجلات والجرائد واليوميات كمادة مراسلات**" [2].

بالرجوع لنص المادة 65 مكرّر 5 من قانون الإجراءات الجزائية التي تنص على ما يلي: "إذا اقتضت ضرورة التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو ...، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي: اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية

[1] ــ شيماء عبد الغني، مرجع سابق، ص 305 وما بعدها.

[2] ــ المادة 09 فقرة 6 من قانون رقم 2000 ــ 03 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

واللاسلكية.."، وعليه نلاحظ أن المشرع عندما ذكر عن اعتراض المراسلات فإنه حدد نوع هذه المراسلات، وهي التي تتم بواسطة وسائل الإتصال السلكية واللاسلكية وبالتالي استبعد المراسلات العادية أي الخطابات الخطية التي تتم عن طريق البريد.

عرّف المشرّع الجزائري الإتصالات السلكية واللاسلكية في المادة الثامنة فقرة 21 من قانون رقم 2000 ــ 03 المؤرخ في 6 غشت سنة 2000، المحدّد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية بأنها: "**كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية**"[1].

باعتبار أنّ المشرّع لم يعرّف اعتراض المراسلات التي تتم بوسائل سلكية واللاسلكية، وبالرجوع للمادة 65 مكرر 05 السالفة الذكر نلاحظ أن مجال الاتصال جاء موسعا أي لم يقتصر على الاعتراض على المكالمات الهاتفية فقط، بل وسعه لمختلف أنواع الاتصالات السلكية واللاسلكية (كالمراسلات التي تتم عبر جهاز التلكس(Télex)، أو جهاز التلغراف (Télégraphe)، وعبر الفاكس(Fax)، بالإضافة للمراسلات التي تتم عبر جهاز الكمبيوتر والتي تتخذ شكل البريد الإلكتروني(Email)[2].

- **تسجيل الأصوات:**

لم يعرّف المشرع الجزائري التسجيل الصوتي، وإنما أشار إليه في المادة 65 مكرر 05 فقرة 03 من قانون الإجراءات الجزائية فيما يلي:"..وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط

---

[1] ــ القانون رقم 2000 ــ 03 مؤرخ في 5 غشت سنة 2000، المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج.ر.ج.ج، ع 48 ، الصادرة في 6 غشت 2000.

[2] ــ عرف المشرع الجزائري البريد الالكتروني في المادة 02 فقرة 2 من المرسوم التنفيذي رقم 98 ــ 257 المؤرخ في 25 غشت 1998 المتعلق بضبط شروط وكيفيات إقامة خدمات الأنترنت بأنها:" خدمة تبادل رسائل إلكترونية بين المستعملين". ج.ر ج. ج ، ع 63، الصادرة في 26 غشت 1998.

أما الرسائل الالكترونية: "فهي بمثابة تبادل وقراءة وتخزين معلومات في شكل رسائل معطيات بين الموزعات الموجودة في مواقع متباعدة. ويمكن المرسل إليه(أو المرسل إليهم) قراءة الرسالة المبعوثة في وقت حقيقي أو في وقت مؤجل".

وتثبيت وبت وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية...".

يقصد بعمليّة تسجيل الأصوات بأنها حفظ الحديث الخاص على أشرطة مخصصة لهذا الغرض، لإعادة سماعها فيما بعد، للوقوف على ما تحتويه من تفصيلات وأقوال يعول عليها كدليل من أدلة الإدانة بعد التأكد من صحة نسبتها إلى قائلها وعدم إدخال أي تغيير أو تعديل عليها[1].

بالرجوع إلى الفقرة الثالثة من نص المادة 65 مكرر5 من قانون الاجراءات الجزائية، يلاحظ أن المشرع أخذ بطبيعة الكلام كمعيار لإجراء عملية التصنت إذ أنّه لم يولي اهتمام لطبيعة المكان الذي يجرى فيه الحديث، إذ أنه سوّى بين المكان العام والمكان الخاص، فلايهم طبيعة المكان بقدر مايهم طبيعة الحديث وسريته. وعليه فقد ترك المشرع الأمر للسلطة التقديرية للقاضي في تحديد طبيعة الحديث حسب ظروف كل حالة [2].

- **إلتقاط الصور:**

تعتبر عملية التقاط الصور الفوتوغرافية من التقنيات المستحدثة التّي جاء بها المشرّع الجزائري فيما يخص البحث والتحري عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات بأسلوب التصور بمختلف أنواعه، وقد عبر عن عملية التصوير أو التقاط الصور في قانون الإجراءات الجزائية في نص المادة 65 مكرر 5 بعبارة الإلتقاط.

يقوم هذا الإجراء أساسا على معاينة مادية مرئية لحالة شخص أو عدة أشخاص مشتبه في امرهم، على الحالة التي كانوا عليها وقت التصوير لغرض استخدام محتوى الفيلم كمادة إثبات ودليل مادي. ويتم ذلك سواء عن طريق الصورة الفردية أو عن طريق شريط الفديو يعرض الصوت وصورة

---

[1] ــ عمار التركي السعدون الحسيني، الحماية الجنائية للحرية الشخصية في مواجهة السلطة العامة، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص 188.

[2] ــ ركاب أمينة، أساليب التحري الخاصة في جرائم الفساد في التشريع الجزائري، مذكرة ماجستير، في قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2014 ــ 2015، ص 65.

متتالية تبرز الوقائع المرتكبة بصفة فعلية وحقيقية تمكن من الوقوف على الفاعلين الحقيقين دون شك، من خلال استعمال وسيلة تكنولوجية معينة[1] تفيد في إجلاء الحقيقة وتسجيلها[2].

بالرجوع إلى نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية والتي تنص على ما يلي:"...التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ..."، يلاحظ أنّ المشرّع الجزائري أخذ بطبيعة المكان لا بحالة الخصوصية التي يكون عليها الأشخاص كمعيار لتحديد مفهوم المكان الخاص، على خلاف إجراء تسجيل الأصوات الذي أعتمد فيه على طبيعة الحديث. وعليه يتضح أن المشرع سمح أن يمد عين الكاميرا إلى الأماكن الخاصة التي تعد مستودعات أسرار المعنيين بالمراقبة في سبيل اكتشاف الحقيقة واستبيان المجرم[3].

(ب) ــ الضمانات القانونية لإجراء عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

نظرا لخطورة عمليات **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور** على حقوق وحريات الأفراد، فقد أورد المشرع العديد من الضمانات والإجراءات التي تعتبر بمثابة قيود ترد على السلطة التي تأمر بإجراء هذه العمليات، وتحول دون تعسفها سواء كانت هي بنفسها أو السلطات التي تتولى تنفيدها، وذلك ببيان هذه الضمانات كالآتي:

1 ــ الضمانات الموضوعية لإجراء عملية اعتراض المراسلات وتسجيل لأصوات والتقاط الصور: تتمثل هذه الضمانات في:

أ ــ وقوع جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات: حدّد المشرع الحالات التي يجوز فيها منح الإذن باعتراض المراسلات وتسجيل الأصوات والتقاط الصور على سبيل الحصر

---

[1] ــ وعليه لا يعد من قبيل التقاط الصور استعمال وسيلة البصر الطبيعية وحدها مثل النظر إلى شخص أو تتبع أفعاله وحركاته في أبسط تفاصيلها، أو باستعمال منظار مقرب للمشاهدة، أو رسم صورة شخص على ورق لأن هذه الوسائل لا تستطيع نقل الصورة أو تسجيلها. انظر: نويري عبد العزير، الحماية الجزائية للحياة الخاصة ــ دراسة مقارنة ــ رسالة دكتوراه في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2010 ــ2011، ص 130 وما بعدها.

[2] ــ راجع حكم جنائي لمحكمة الجنايات، مجلس قضاء تلمسان، قضية رقم 00015/ 08، بتاريخ 03/ 03/ 2008، غير منشور ، الملحق رقم 2، ص 155.

[3] ــ ركاب أمينة ، مرجع سابق، 68.

وذلك في المادة 65 مكرر5 من قانون الإجراءات الجزائية[1]، ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا أنه قد تكتشف عرضا جرائم غير تلك الواردة في الإذن أثناء إجراء عمليات اعتراض المراسلان وتسجيل الأصوات والتقاط الصور، فإن ذلك لا يكون سببا لبطلان الإجراءات وفق نص المادة 65 مكرر6 فقرة 2 من قانون الإجراءات الجزائية.

ب ــ وجود دلائل كافية تقتضي اللجوء لعمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: لا يكتفي وقوع جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، بل يجب فضلا عن ذلك أن تقتضي ضرورة التحري والتحقيق ذلك، بأن يكون الإذن له فائدة في إظهار الحقيقة. وبالنالي لا تعدّ العمليات السابقة مشروعة إذا استهدفت مجرد التلصص على المتهم أو التشهير به .

2 ــ الضمانات الشكليّة لإجراء عملية اعتراض المراسلات وتسجيل لأصوات والتقاط الصور:

تتمثل هذه الضمانات في:

أ ــ الجهة المختصة بإصدار الإذن: اعطى المشرع صلاحية منح الإذن لجهة قضائية محايدة وذلك ضمانا لحماية المصلحة المختصة، وهي السلطة القضائية المختصة وذلك استنادا لنص المادة 65 مكرر 5 من قانون الإجراءات الجزائية وهي تتمثل في:

- **وكيل الجمهورية:** بالإضافة إلى الإختصاصات المخولة لوكيل الجمهورية وفق المادة 12 الفقرة 2 والمادة 36 فقرة 1 من قانون الإجراءات الجزائية، أضاف إليه المشرع سلطة الإذن باعتراض المراسلات السلكية واللاسلكية والتقاط وتسجيل المحادثات الخاصة أو التقاط صور في أماكن خاصة، إذا اقتضت ضرورات البحث والتحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
- **قاضي التحقيق:** الى جانب وكيل الجمهورية أعطى المشرع لقاضي التحقيق في حالة فتح تحقيق قضائي سلطة إصدار إذن بإجراء عمليات اعتراض المراسلات وتسجيل الأصوات

[1] ــ حيثت ورد فيها مايلي: " إذا اقتضت ضرورات التحري والتحقيق في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة العابرة للحدود الوطنية أو**الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يلي: ...."

والتقاط الصور، وتحت مراقبته المباشرة في الجرائم السابقة الذكر[1]،وهو ما نصت عليه المادة 65 مكرر 5 بقولها: ''في حالة فتح تحقيق قضائي، تتم العمليات المذكورة، بناء على إذن من قاضي التحقيق، وتحت مراقبته المباشرة'' .

3 ــ الجهة المكلفة بتنفيذ الإذن: نظرا للطبيعة الخاصة التي تتميز بها عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، فقد أوكل المشرع مهمة مباشرتها لضابط الشرطة القضائية المأذون له من قبل وكيل الجمهورية أو المناب من قبل قاضي التحقيق[2]، وبالتالي فقد استثنى المشرع أعوان الشرطة القضائية من إجراء هذه العمليات، وهذا نظرا لحساسية وخطورة لما فيها من مساس بحرية وحرمة الأفراد الخاصة.

كما أجازت المادة 65 مكرر 08 من قانون الإجراءات الجزائية الجزائري تنفيذ هذه العمليات من قبل أي عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالإتصالات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات المطلوب إنجازها[3].

يشترط القانون على ضابط الشرطة القضائية أن يحرر محضرا ينقل فيه تفاصيل العمليات التي قام بها منذ بدايتها إلى نهايتها، ويرسله إلى وكيل الجمهورية أو قاضي التحقيق الذي أنابه للقيام بذلك وذلك مانصت عليه المادة 65 مكرر 09 من قانون الإجراءات الجزائية الجزائري.

ب ــ العناصر التي يتطلبها الإذن بإجراء عمليات اعتراض المراسلات وتسجيل لأصوات والتقاط الصور: يشترط في الإذن حتى يكون صحيحا أن يتوافر على عدة عناصر منها ما يتعلق بالشكل، ومنها ما يتعلق بالمضمون، ومنها ما يتعلق بالمدة المحددة لإجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

---

[1] ــ وذلك بعد أن يقوم وكيل الجمهورية بإخطار قاضي التحقيق بموجب طلب افتتاحي أو بناء على شكوى مصحوبة بإدعاء مدني، وذلك وفقا للمواد 67، 36 فقرة 5 والمادة 72 من قانون الإجراءات الجزائية.

[2] ــ باستثناء رؤساء المجالس الشعبية البلدية بالرغم من تمتعهم بصفة ضابط الشرطة القضائية، إلا أن الواقع العملي يمنعه من مباشرة هذه العمليات، وذلك راجع لافتقارهم الخبرة والمؤهلات والتكوين اللازمين لهذه النوعية من العمليات.

[3] ــ تنص المادة 65 مكرر 8 من قانون الاجراءات الجزائية على: " يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل مكلف بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5 أعلاه".

- **شكل الإذن:** يجب أن يصاغ الإذن في شكل عبارة صحيحة، يستفاد منها اتجاه إرادة مصدر الأمر (وكيل الجمهورية أو قاضي التحقيق) إلى إجازة المراقبة مثل عبارة تأمر أو نأذن ...، كما يجب أن يكون الإذن مكتوبا وذلك طبقا لنص المادة 65 مكرر 7 الفقرة 2 من قانون الإجراءات الجزائية.
- **مضمون الإذن:** يشترط في الإذن الخاص بإجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور أن يتضمن عدة بيانات، وحددها المشرع في نص المادة 65 مكرر 7 الفقرة 1 من قانون الإجراءات الجزائية، منها كل العناصر التي تسمح بالتعرف على الصور المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير، بالإضافة إلى أن يكون الإذن محددا لمدة نفاذه.
- **مدّة الإذن:** يسلم الإذن بإجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور لمدة أربعة أشهر قابلة للتجديد حسب مقتضيات البحث والتحري أو التحقيق، وبنفس الشروط التي صدر بها الإذن الأصلي، وذلك تطبيقا لنص المادة 65 مكرر7 الفقرة 2 من قانون الإجراءات الجزائية، والهدف من تحديد المدة هو تضيق مجال الإعتداء على الحياة الخاصة للأفراد ومنعا للتعسف في استعمال السلطة.

ثانيا ــ عملية التسرب:

أدرج المشرع الجزائري عمليّة التسرب بموجب القانون رقم 06ــ 22 المؤرخ في 20 ديسمبر 2006، المعدّل و المتمّم للأمر رقم 66ــ 155 المتضمن قانون الإجراءات الجزائيّة، والذي أفرد الفصل الخامس منه تحت عنوان: "**في التسرب**" والذي تضمّن ثمانية مواد(من المواد 65 مكرر11 حتّى المادة 65 مكرر18). وتناول من خلالها تحديد مفهوم هذه العملية، وشروط إجراءها، الأفعال المبررة التي يقوم بها العنصر المتسرب، وأخيرا الحمايّة الجنائية للقائم بعمليّة التسرب. وسنحاول تفصيل ذلك من خلال التالي:

1ـــ مفهوم التسرب:

التسرب **لغة** مشتق من الفعل تسرب تسربا أي دخل وانتقل خفية وهي الولوج والدخول بطريقة أو بأخرى إلى مكان أو جماعة[1].

يعتبر أسلوب التسرب أو الإختراق تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط الشرطة القضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية، ويقدم لمتسرب نفسه على أنه فاعل أو شريك[2].

أما من **الناحية القانونية**، عرفه المشرع الجزائري في المادة (65 مكرر 12) بأنه: **"قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلّف بتنسيق العمليّة بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنّه فاعل معهم أو شريك أو خاف..."**[3].

من خلال التعريف السابق يتضح أن التسرب هو عبارة عن عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية وكذا الإحتكاك شخصيا بالمشتبه بهم والمتهمين وهذا ينطوي على خطورة بالغة تحتاج إلى دقة وتركيز وتخطيط سليم[4].

يلجأ إلى هذا الإجراء عادة عندما تقتضي عمليّة التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر من هذا القانون وهي: ـــ جرائم المخدرات ـــ الجريمة المنظمة عبر

---

(1) ـــ سهيل حسيب سماحة، معجم اللغة العربية، الطبعة الأولى، مكتبة سمير،1984، ص 130.

(2) ـــ حريزي ربيحة، إجراءات جمع الأدلة ودورها في الكشف عن الجريمة، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2011، ص 451.

(3) ـــ ذكر المشرع الفرنسي التسرب(Infiltration) في المواد 81/706 إلى 87/706 وكذا المادتين 7/694 و9/694 من تعديل الإجراءات الجزائية بموجب القانون رقم 297/2007 المؤرخ في 2004/03/09.

(4) ـــ يلاحظ أن المشرع سمى هذه العملية **بالتسرب** في قانون الإجراءات الجزائية في حين استخدم مصطلح **الإختراق** في المادة 56 من القانون رقم 06 ـــ 01 المتعلق بالوقاية من الفساد ومكافحته، وهما مسميان لمسمى واحد ولهما نفس المدلول.

الحدود الوطنيّة ـــ الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ـــ جرائم تبييض الأموال والإرهاب ـــ وأيضا الجرائم المتعلّقة بالتشريع الخاص بالصرف .

يمكن تجسيد عملية التسرب في نطاق الجرائم الالكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الإفتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها أو بث فيروسات، فيتّخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل مثلهم.

2ـــ شروط صحة عمليّة التسرب: التسرب كممارسة غير مألوفة لضابط أو عون الشرطة القضائيّة، بل يعد من أخطر الإجراءات مساسا بحرمة الحياة الخاصة للمشتبه فيه، لذلك اشترط المشرع ضمانات معيّنة يتعيّن مراعاتها عند اللجوء إلى هذا الإجراء ويتمثل ذلك في نوعين من الشروط وذلك كما يلي:

- **الشروط الموضوعية:** تتمثل هذه الشروط وفق الأحكام التي نظمها المشرّع الجزائري في شرطين أساسين:

ـــ الأول يتمثل في تحديد نوع الجريمة ويجب ألا تخرج عن الجرائم التي حددها على سبيل الحصر في المادة 65 مكرر 05 في سبعة أنواع وهي: جرائم المخدرات، الجريمة المنظنة العابرة للوطنية، جرائم تبييض الأموال، الجرائم الإرهابية،جرائم الفساد، الجرائم المتعلقة بالتشريع الخاص بالصرف والجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات.

يرجع سبب تحديد هذه الجرائم دون غيرها إلى الخطورة الإجرامية لهذه الأفعال وأثرها على السياسة العامة في الدولة واقتصادها، فهي جرائم سريعة الإنتشار وعابرة للحدود الوطنية، وهي جرائم قائمة على التخطيط واستخدام كل الوسائل محو آثار الجريمة وطمس معالمها.

ما يهمنا في هذا المجال جرائم المساس بأنظمة المعالجة الآلية للمعطيات والتي تعد من أهم الجرائم الواقعة على المعاملات الالكترونية الحكومية.

ـــ أما الشرط الموضوعي الثاني فهو أن يكون الإذن بالتسرب مسببا، فمن خلال التسبيب تتبين العناصر التي أقنعت الجهات القضائية المختصة بمنح الإذن وكذا العناصر التي دفعت الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن.

- **الشروط الشكلية:** تنحصر الشروط الشكلية لهذا الإجراء في صدور إذن التسرب من وكيل الجمهريّة أو قاضي التحقيق بعد إخطار وكيل الجمهوريّة، وهذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية"....يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن...حسب الحالة بمباشرة عملية التسرب"[1].

ويجب أن يكون الإذن مكتوبا وإلا كان الإجراء باطلا، وهذا ما نصت عليه المادة 65 مكرر 15 بقولها:" يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 مكتوبا تحت طائلة البطلان"، كما يجب أن يتضمن الإذن مجموعة من الشروط يتوقف على تحديدها صحة الإجراء في حد ذاته كذكر هوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، بالإضافة إلى تحديد المدة المطلوبة في عملية التسرب والتي يجب ألاّ تتجاوز أربعة (4) أشهر ويمكن أن تجدّد حسب مقتضيات التحرّي والتحقيق ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي أذن بهذا الإجراء أن يأمر في أي وقت بوقفه قبل انتهاء المدة المحددة[2].

---

[1] ـــ نلاحظ مما سبق ذكره أن المشرع الجزائري أسند مهمة إصدار إذن التسرب إلى وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهوريّة، بمعنى أن المشرع خرج عن الأصل العام في التحقيق القائم على الفصل بين سلطتي الاتهام والتحقيق، ذلك أن وكيل الجمهورية مهمته الأساسيّة هي تقديم المتهم إلى العدالة، ومن الصعوبة أن يتجرد من صفته الاتهاميّة عندما يقوم بإصدار الترخيص بالتسرب، خاصة وأن طبيعة عمليّة التسرب فيها نوع من الخطورة على حرمة الحياة الخاصة للأفراد لاسيما الحق في الخصوصيّة، لذلك فالأفضل منح هذه المهمة إلى قاضي التحقيق لما له من استقلالية وحسن التقدير ما يطمئن معه الأفراد. هذا من جهة.

ومن جهة أخرى، بالرغم من أهميّة هذا الإجراء في الكشف عن الفكرة الإجرامية والتي قد لا تظهر للوجود دون اللجوء إلى عملية التسرب، إلاّ أنه يطرح انتقادات كالتي يطرحها التحريض البوليسي،حيث يلعب المتسرب دورا ايجابيّا أثناء القيام بالأعمال الإجرامية، وذلك شيء ضروري حتى يكتسب ثقة المشتبه فيهم، خاصة وأنّ طبيعة هذا الأخير دو نسبة عالية من الذكاء. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي، مرجع سابق، ص 122.

[2] ـــ نفس المرجع، ص 121.

تجدر الإشارة أنّ مهمة تنفيذ عملية التسرب تسند طبقا لأحكام المادتين 65 مكرر 12 الفقرة 1 و65 مكرر فقرة 13 من قانون الإجراءات الجزائية إلى ضباط الشرطة القضائية وأعوانهم بشكل عام والمسخرون بشكل خاص[1]، ويستثنى عمليا رؤساء المجالس الشعبية، وذلك راجع لكونهم أشخاص معروفة، وهذا يتعارض مع الطابع السري للأسلوب.

أمّا بالنسبة للعناصر الواجب توافرها في إذن عملية التسرب فهي نفسها الواجب تضمينها في إذن عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور سواء ماتعلق منها بشكل الإذن و مضمونه بالإضافة إلى مدة الإذن .

3 ــ الأفعال المبرّرة في عمليّة التسرب: نص المشرع صراحة في المادة 65 مكرر 14 على أنّه:"يمكن لضباط وأعوان الشرطة القضائيّة المرخص لهم بإجراء عمليّة التسرّب والأشخاص الذين يسخرون لهذا الغرض القيام بما يلي[2]:

ــ اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات تحصّل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

ــ استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال".

يتضح من خلال هذا النص أن طبيعة هذه الأفعال تستوجب من القائمين بها مشاركة إيجابيّة، كحيازة متحصلات الجريمة أو وسائل ارتكابها، وهذا النوع من الأفعال له تأثير على المسؤوليّة

---

[1] ــ في الحالة التي يتم فيها تنفيذ عملية التسرب من خلال أحد أعوان ضباط الشرطة القضائية، يقتضي الأمر هنا ضرورة وجود ضابط شرطة منسق للعملية تنفذ العملية تحت مسؤوليته وإشرافه.

[2] ــ تجدرالإشارة أن صياغة هذه الأفعال مأخوذة من المادة 706ــ 32 من قانون الإجراءات الجنائية الفرنسي، وذلك في إطار مكافحته جريمة الاتجار غير مشروع للمخدرات، والتي تنص ما يلي:

Article 706-32 du CCP francais dispose que " …les agents de police judiciaire peuvent, avec l'autorisation du procureur de la République ou du juge d'instruction saisi des faits qui en avise préalablement le parquet, et sans être pénalement responsables de ces actes :
1- Acquérir des produits stupéfiants ;
2- En vue de l'acquisition de produits stupéfiants, mettre à la disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication. "

الجزائيّة، إلاّ أن القانون أعفاهم من هذه المسؤولية وذلك بنصه صراحة على ذلك في المادة 65 مكرر 14 بقولها :" ...دون أن يكونوا مسؤولين جزائيا...". ويمتد هذا الإعفاء لظروف أمنية للمتسرب حتى بعد انقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها أو في حالة تقرير وقف العمليّة، بشرط ألاّ يتجاوز ذلك مدة أربعة (4) أشهر سواء من تاريخ انقضاء المدة المحددة في الإذن أو من تاريخ صدور قرار وقفها من قبل القاضي الذي رخص بإجرائها.

وحتى تحقق عمليّة التسرب الأهداف المنشودة منه، ينبغي أن تتم بكل سريّة تامّة حتى يكون المتسرب في مأمن من انكشاف هويّته الحقيقيّة من قبل المجرمين، لذلك منحه المشرع نوع من الحماية الجنائيّة، فقرّر بنص المادة 65 مكرر 16 من ق.إ.ج.ج. عقوبة الحبس من سنتين(2) إلى خمس(5) سنوات وغرامة من 50.000دج إلى 200.000 دج لكل من يكشف هويّة ضباط أو أعوان الشرطة القضائيّة.

إذا تسبب الكشف عن الهويّة في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس(5) سنوات إلى(10) سنوات والغرامة من 200.000دج إلى 500.000دج .

وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر(10) سنوات إلى عشرين(20) سنة والغرامة من 500,000دج إلى 1,000,000دج دون الإخلال عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات.

ينبغي الإشارة في هذا المقام أن المشرع أدرج قواعد موضوعيّة والخاصة بالقواعد القانونية المتعلقة بالتجريم والعقاب ضمن القواعد الإجرائية والمتمثلة في مجموعة من القواعد التي تنظم وسائل التحقيق من وقوع الجريمة ومحاكمة مرتكبيها وتوقيع الجزاء الجنائي عليهم، لذلك ينبغي على المشرع أن ينقل الأحكام الخاصة بالقواعد الموضوعية إلى قانون العقوبات حتى يكون لنا نظام قانوني جنائي منتظم ولا يلتبس على القاضي عند تطبيقه لإحدى هذه العقوبات.

في نهاية الفصل الخاص بإجراء التسرب قام المشرع بتكيف عمل المتسرّب على أنه شاهد حيث نص في المادة 65 مكرر 18 على أنّه :"يجوز سماع ضابط الشرطة القضائية الذي تجرى عمليّة التسرب تحت مسؤوليته دون سواء بوصفه شاهدا عن العمليّة".

المطلب الثاني: فنيّة التحقيق عن الجرائم الواقعة على الحكومة الإلكترونية

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة.

هذه القواعد إمّا قانونية أو فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والإمتثال. أما الثانية فتتميّز بالمرونة التيّ يضفي عليها المحقق من خبرته وفطنته ومهاراته الكثيرة[1].

مع تزامن ظهور أنماط مستحدثة من جرائم تقنية المعلومات كان لابدّ من استحداث أسلوب التحقيق لما يوافق طبيعة هذه الجرائم ذات الطبيعة الخاصة. وعليه سنعرض من خلال التالي صعوبات التحقيق في الجرائم الواقعة على الحكومة الالكترونية ذات الخصّيصة التقنية، باعتبارها لا توافق مع فكر المحقق الجنائي وذلك من خلال الفرع الأول، وبعد ذلك سنعرض للحلول والمتمثلة في الأصول الفنية التي تتطلب للتحقيق في الجرائم الواقعة على الحكومة الالكترونية وذلك في الفرع الثاني.

الفرع الأول: صعوبات التحقيق في الجرائم الواقعة على الحكومة الإلكترونية

يتسم التحقيق في الجريمة المعلوماتية وملاحقة مرتكبيها جنائيا بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق، بل يمكن أن تؤدي إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون. ومن أهمّ الصعوبات التي تواجه القائمين على مكافحة الجرائم المعلوماتية والتحقيق ما يلي:

---

[1] ــ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي، الطبعة الأولى، 2009، ص56.

أولا ــ صعوبات تتعلق بالجريمة ذاتها:

كخفاء الجريمة، وغياب الدليل المرئي الممكن بالقراءة فهمه، وافتقاد أكثر الآثار التقليدية وإعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها، أيضا سهولة محو الدليل أو تدميره في زمن قصير جدا مما يعرقل السلطات من كشف الجريمة إذا علمت بها[1]. بالإضافة إلى ذلك الضخامة البالغة لكم البيانات والمعلومات المتعين فحصها، وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية[2].

ثانيا ــ صعوبات تتعلق بإجراءات الحصول على أدلة الجريمة:

إذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع، فإنه قد يصعب عليها القيام بهذا التحري بالنسبة للجريمة المعلوماتية، حيث أن مرتكبي هذه الجرائم من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة وذلك باستخدام كلمات السر مما يستحيل على جهات التحقيق الحصول على الأدلة التي تدينهم[3].

أيضا من معوّقات التحقيق تعذر اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلا بحاسبات أخرى خارج الدولة[4]، وعليه قد يثير التفتيش عبر الحدود مشكلات عديدة تتعلق بخرق سيادة الدولة على إقليمها.

ثالثا ــ صعوبات تتعلق بجهات التحقيق "عدم توافر الكفاءة البشرية المؤهلة للتحقيق":

بعض هذه الصعوبات ترجع إلى شخصية المحقق، مثل التهيب من استخدام الحاسب الآلي وشبكة الانترنت، بالإضافة إلى عدم الإهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية، والبعض الآخر يتعلق بالنواحي الفنية المطلوبة بالتحقيق في هذا النوع من الجرائم، كنقص معرفة الجوانب الفنية

---

(1) ــ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994، ص16 وما بعدها.

(2) ــ عبد الرحمن بحر، معوقات التحقيق في جرائم الأنترنت، دراسة مسحية على ضباط الشرطة بدولة الكويت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999، ص 46.

(3) ــ حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009، ص 529.

(4) ــ هشام محمد فريد رستم، مرجع سابق، ص 22.

والتقنية لأجهزة الحاسوب والانترنت، وعدم توفر المعرفة بأساليب ارتكاب الجرائم المعلوماتية، ذلك أن افتقار جهات التحقيق للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل[1].

الفرع الثاني: الأصول الفنية الواجب مراعاتها للتحقيق في الجرائم الواقعة على الحكومة الإلكترونية

وهي مجموع من المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المعلوماتية، ولا يقصد بها المهارات التقليدية التي يتمتع بها كل محقق[2]، بل المهارات التي تتسم بالجدة والحداثة وتعتبر إفرازا للتطور الإنساني في مجال تقنية الإتصال والحوسبة. إلاّ أنّ هذه المهارات غير كافية مالم يتبعها تدريب للجهات القائمة بالتحري والتحقيق، ذلك ما سنبينه من خلال النقاط المتقدمة.

أولاـــ العناصر الأساسية للتحقيق في مجال الجريمة المعلوماتية:

يقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق قبل البدء في عمليات التحقيق الإبتدائي وإجراءات أخرى ينبغي مراعاتها أثناء هذا التحقيق[3].

1/ الإجراءات الواجب مراعاتها قبل البدء في التحقيق: تتمثل هذه الإجراءات فيما يلي:

ـــ تحديد نوع نظام المعالجة الآلية للمعطيات فهل هو كمبوتر معزول أم متصل بشبكة معلومات.

ـــ وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.

ـــ إذا وقعت الحريمة على شبكة الانترنت فإنه يجب مراعاة طرفيات الإتصال.

ـــ مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

ـــ مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

---

[1] ـــ هلال بن محمد بن حارب البويعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة،2009، ص 240.

[2] ـــ وهي مهارات أساسية يفترض بداهة توافرها في المحقق بالضرورة، كمهارة التعامل مع مسرح الجريمة والتحفظ على الأدلة المادية ومناقشة الشهود وغيرها.

[3] ـــ جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص 119. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي ...، مرجع سابق، ص 84.

ـــ يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الإستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته.

ـــ تصوير الأجهزة المستهدفة (التي وقعت بها أو عليها الجريمة) من الأمام والخلف وذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.

2/ الإجراءات الواجب مراعاتها أثناء التحقيق: عند البدء في عملية التحقيق لا سيما عند القيام بعملية تفتيش جهاز الحاسوب فإنه على رجال التحقيق مراعاة ما يلي:

ـــ عمل نسخة إحتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل استخدامها والتأكد فنيا من دقة النسخ عن طريق الأمر(Disk comp).

ـــ نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

ـــ العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة إختلاس معلوماتي.

ـــ العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

ـــ حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

ثانيا ـــ ضرورة تدريب وتأهيل المحقق المعلوماتي:

في إطار مكافحة الجرائم المعلوماتية لابد من وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، لهذا كان من الضروري إعداد المحققين، باعتبارهم يواجهون أنشطة إجرامية معقدة وتنفذ بطرق ذكية ودقيقة. وليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيرا في النظم المعلوماتية، بل لابد من الإلمام ببعض المسائل التي تمكنه من التفاهم

مع خبراء التقنية، كما ينبغي أن يكون ملما بالإجراءات الإحتياطية التي ينبغي اتخاذها على مسرح الجريمة والتدابير اللازمة لتأمين الأدلة[1].

لأجل ذلك بدأت بعض الأجهزة الأمنية بإعداد كوادراها دورات تدريبية للضبط والتحقيق في الجرائم المعلوماتية حتى تكون مسايرة للتطورات السريعة التي تشهدها التقنيات، ويجب أن يشمل منهج التدريب خصوصا تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة أو الأساليب التي تتعلق بالكشف عنها وكيفية إثباتها ومعاينتها والتحفظ عليها وكيفية فحصها فنيا[2].

المطلب الثالث: الدليل المناسب لإثبات الجرائم الواقعة على الحكومة الإلكترونية

تختلف الجرائم الواقعة على الحكومة الالكترونية كالجرائم المعلوماتية عن الجرائم التقليدية في كون الأولى تتم في بيئة غير مادية أو ما تعرف بالوسط الإفتراضي، حيث يمكن للجاني عن طريق نبضات إلكترونية رقمية لا ترى أن يبعث في بيانات الحاسوب أو برامجه وذلك في وقت قياسي قد يكون جزءا من الثانية، كما يمكن محوها في زمن قياسي قبل أن تصل يد العدالة إليه إذا ما استخدمت برامج خاصة في ذلك، مما يصعب الحصول على دليل مادي في مثل هذه الجرائم.

وعليه فإن كشف ستر هذا النوع من الجرائم يحتاج إلى أدلة ذات طبيعة خاصة، ومختلفة عما ألفناه في الجرائم التقليدية، حيث تستخدم ذات الطبيعة التقنية الناجمة عن الحاسوب والانترنت، وتتمثل في **الدليل الالكتروني (Electronic evidence)**. بمعنى آخر ترتكز عمليّة الإثبات الجنائي للجرائم الالكترونيّة على الدليل الالكتروني باعتباره الوسيلة الوحيدة لإثبات هذه الجرائم،

---

[1] ــ يرى البعض أن من المستحسن أن تُوكل مهمة التحقيق في الجرائم المعلوماتية إلى بيوت الخبرة المتخصصة في هذا المجال لا سيما مع وجود شركات عالمية متخصصة في تحقيق الجرائم المعلوماتية وحققت النجاح في كثير من الحالات، في حين أن جانب آخر يرى أن متطلبات العدالة الجنائية تقتضي تحمل الأجهزة الأمنية الحكومة مسؤوليتها تجاه اكتشاف كافة الجرائم ومن بينها الجرائم المعلوماتية، وحتى تكتمل قدرات تلك الأجهزة لابد من الاستعانة بالنخبة المتخصصة في مجال التقنية في جميع مراحل الدعوى الجنائية ، ومن تم لابد من إيجاد أسلوب خاص للتحقيق في هذه الجرائم يجمع بين الخبرة الفنية والكفاءة المهنية. انظر: محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2004، ص124.

[2] ــ سرحان حسن المهيبي، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، المجلد العشرون، العدد الرابع، العدد رقم (97)، أكتوبر 2011، ص 37.

لذا سنتناول في هذا المطلب تحديد مفهوم الدليل الالكتروني(الفرع الأول)، فضلا عن دراسة أهم تقسيمات هذا الدليل (الفرع الثاني) وذلك من خلال الفروع التاليّة:

الفرع الأول: مفهوم الدليل الألكتروني

سنحاول في هذا الفرع توضيح مفهوم الدليل الإلكتروني(أولا)، ثم بيان أهم الخصائص التي تتميز بها وذلك لبيان أهم الفرقات بينه وبين الدليل في الجرائم التقليدية (ثانيا).

أولا ـــ تعريف الدليل الإلكتروني:

تعدّدت التعريفات التي قيلت بشأن الدليل الالكتروني وتباينت بين التوسع والتضييق، ويرجع ذلك لموضع العلم الذي ينتمي إليه هذا الدليل، فاختلفت بين أولئك الباحثين في مجال التقنية، والباحثين في المجال القانوني، وسنحاول فيما يلي عرض أهم هذه التعريفات :

عرّف البعض الدليل الالكتروني بأنه "**كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما** "[1] . وهناك من يعرفه بأنه " **الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة** "[2]. أو أنّه "**معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتمّ الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه**" [3]. أو: "**هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصال من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميّا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة لتقرير البراءة**

---

(1) - Christin Sgarlata and David J Byer , The Electronic paper Trail: Evidentiary Obstaclesto Discovery of electronic Evidence. Journal of Science and Technology Law .22 September 1998 .p 4 .

مشار إليه عند: عمر محمد أبوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت...، مرجع سابق، ص 969.

(2)ـــ عمر محمد أبوبكر بن يونس، مرجع سابق، ص 969.

(3)ـــ محمد الأمين البشري، مرجع سابق، ص 234 .

أو الإدانة فيها [1] . أما الأستاذ كيسي (Casey) فيعرّف الأدلة الجنائية الرقمية بأنها "**تشمل جميع البيانات الرقمية التي يمكن أن تثبت أنّ هنالك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني أو بين الجريمة والمتضرر منها. والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات، بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت و الصورة** [2]. أما التعريف المقترح للدليل الالكتروني من قبل المنظمة الدولية لأدلة الحاسوب(International Organization (IOCE) of Computer Evidence) [3] بأنه " **المعلومات المخزنة أو المتنقلة في شكل ثنائي، ويمكن أن يعتمد عليها في المحكمة** "[4]. وهو نفس المعنى تقريبا المتبني من قبل الفريق العلمي العامل على مستوى الأدلة الرقمية Standard Working Group on Digital Evidence (SWGDE)[5]، باعتبار هذا الأخير أنشئ من أجل توحيد الجهود التي تقوم بها المنظمة الدولية لأدلة الحاسوب (IOCE)، وتطوير مختلف التخصصات والمبادئ التوجيهية من أجل استرداد، المحافظة ودراسة الأدلة الرقمية بما فيها الصوتية والمصورة [6].

---

[1] ــ عبد الناصر محمد محمود فرغلي وعبيد سيف سعيد المسماري، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، ''الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية''، دراسة تطبيقية مقارنة، الرياض، المنعقد في الفترة: 02ــ1148/11/04/04 هــ الموافق لــ12 ــ 2007/11/14، ص 13.

[2] - "Digital Evidence encompasses any and all digital data that ran establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator . This Digital Data is a combination of numbers that represent information of various kinds , including text , images , audio ,and video . By EoghanCasey , Digital Evidence and Computer Crime—Forensic Science, Computers and the Internet , Second Edition , Academic Press *An imprint of Elsevier* , London , 2004 , p 260 .

[3] – المنظمة الدولية لأدلة الحاسوب (IOCE) هي: تنظيم دولي تمّ اعتماده في نسيان/ أبريل 1995، مقره الولايات المتحدة الأمريكية، وتسعى هذه المنظمة إلى توفير منتدى دولي لوكالات أنفاذ القانون لتبادل المعلومات بشأن التحقيق في جرائم الحاسوب وغيرها من قضايا الطب الشرعي، ويتألف من أجهزة إنفاذ القانون والوكالات الحكومية المعنية بالتحقيق الرقمي وتحقيقات الطب الشرعي، وذلك بناء دعوة من المجلس التنفيذي بالمنظمة . لمزيد من التفصيل حول المنظمة يرجى العودة للموقع الخاص بها وهو كالتالي :

Http: //www.ioce.org/ index? php id =15

[4]- Electronic evidence is" information stored or transmitted in binary form that may be relied upon in court " . Eoghan Casey ،ib id , p 261.

[5] ــ عرّف الفريق العلمي العامل على مستوى الأدلة الرقمية الدليل الرقمي بأنه" **المعلومات المخزنة أو المتنقلة في شكل ثنائي، ذات قيمة اثباتية**".

"Digital Evidence is any information of probative value , that is either stored or transmitted in a digital form" .

[6] ــ لمزيد من التفصيل حول الفريق العامل حول مستوى الأدلة الرقمية, انظر الموقع التالي:

www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

بعد استعراضنا للتعريفات التي قيلت بشأن الدليل الالكتروني نلاحظ في البداية أنها متقاربة من بعضها البعض، وأنّها حاولت استيعاب هذا النوع المستحدث من الدليل بالرغم من حداثته وارتباطه بالتقنية الرقمية، إلاّ أنّ هناك بعض الملاحظات ينبغي الإشارة إليها في هذا المقام تتمثل فيما يلي:

1 ــ هناك خلط في تعريف الدليل الالكتروني بمفهوم برامج الحاسب الآلي عند بعض الفقهاء[1]، حيث تمّ اعتبارها بيانات يتمّ إدخالها إلى جهاز الحاسوب، وذلك لانجاز مهمة ما، وهذا التعريف ينطبق تماما مع مفهوم برامج الحاسب الآلي[2].

صحيح قد يتفق المصطلحين في أنّ كيلهما يعدّ آثارا معلوماتية أو رقمية، حيث يتركهما كل مستخدم للنظام المعلوماتي، وتتخذ شكلا واحدا هو الشكل الرقمي، لأن البيانات داخل الكمبيوتر سواء كانت في شكل نصوص أم أحرف، أرقام، رموز، أصوات أو صور تتحوّل إلى طبيعة رقمية، لان تكنولوجيا المعلومات الحديثة ترتكز على تقنية الترقيم، التي تعني ترجمة أو تحويل أي مستند معلوماتي مؤلف من نصوص أو وصور ..إلى نظام ثنائي في تمثيل الأعداد يفهمه الكمبيوتر قوامه اللرقمان [صفر]، واحد] [3]. بل أكثر من ذلك قد تعد بعض البرامج لوحدها دليلا إلكترونيا مثل برنامج الاختراق (**asylu_014_fe**)[4] .

---

[1]- عند ChristinSgarlata and David J Byer.انظر فيما سبق ص4 .

[2] ــ تعد برامج الحاسوب من أهم المكونات المنطقية للحاسوب وهي بمثابة العمود الفقري له، ولها مفهومان أحدهما ضيق والآخر واسع فالمدلول الضيق ينصرف إلى" مجموعة التعليمات الموجهة من الإنسان إلى الآلة والتي تسمح لها بتنفيذ مهمة معينة". أما المدلول الواسع فيشمل فضلا عن المفهوم الضيق للبرامج، التعليمات والأوامر الموجهة للعميل مثل بيانات استعمال البرنامج وكيفية المعالجة الالكترونية للمعلومات، أي كافة البيانات الأخرى الملحقة بالبرنامج والتي تساعد على سهولة فهم تطبيقه، وهذه البيانات عبارة عن تعليمات موجهة من المبرمج الذي يتولى إعداد البرنامج إلى العميل الذي يتعامل مع الآلة. انظر: محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر،2002، ص 33 ومابعدها. وانظر كذلك: علي أحمد الفرجاني، جريمة القرصنة المعلوماتية، دراسة مقارنة من الجانبين الموضوعي والإجرائي، مجلة التشريع ، السنة الثانية ،العدد السابع ، أكتوبر 2005 ، ص 19 .

[3] ــ النظام الثنائي الرقمي(Binary)، أعتمد أساسا للكمبيوتر الرقمي ويمكن من هذا النظام تحول كافة الأرقام العشرية والحروف والأشكال إلى نظام ثنائي، ويمكن من جهة أخرى الاعتماد على المكافئ له سواء كان نظام ثنائي أو نظام الست عشر. مشار إليه عند: ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، المجلة الكبرى، 2006، ص 22 .

[4] – والمشكلة في الوقت الحالي أنّه يمكن لأي شخص تحميل هذه الأنواع من البرامج الخطرة وبالمجان من الانترنت، مثلا يحمّل برنامج (asylu_014_fe) من الموقع التالي: :
http://upload.9q9q.net/file/ghc7b6yZ...14_fe.zip.html

إلا أنّ الفرق بين الدليل الالكتروني وبرامج الحاسوب يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في تشغيل الحاسوب وتوجيهه إلى حلّ المشاكل ووضع الخطط المناسبة، وبدونها لا يعدو أن يكون مجرد آلة صماء كباقي الآلات، بل انه توجد برامج خاصة تساهم في استخلاص الدليل الالكتروني مثل: برنامج معالجة الملفات مثل X tree Pro Gold[1]، وبرنامج النسخ مثل Lap Link [2] .

أمّا الدليل الجنائي الرقمي له أهمية كبرى ودور أساسي في معرفة كيفية حدوث الجريمة الالكترونية، بهدف إثباتها ونسبتها إلى مرتكبيها، لاسيما في البيئة الافتراضية، غير محسوسة (intangible)، حيث يمكن تفتيش محتوى القرص الصلب لمعرفة كل المراحل التي مرّ بها المجرم وهو في سبيل تحقيقه للهدف الإجرامي.

2 ــ حصرت التعريفات السابقة مصادر الأدلة الالكترونية في أجهزة الحاسب الآلي وملحقاتها أو ما تعرف عند التقنيين **بفُتح النظم الحاسوبية**[3]، ونظم الاتصال، إلاّ أن العلم أثبت أن هناك نظم أخرى مدمجة بالحواسيب قد تحتوي على العديد من الأدلة الرقمية كالهواتف المحمولة (Mobile

---

[1] ــ برنامج معالجة الملفات مثل(X tree Pro Gold): برنامج يُمكّن المحقق من العثور على الملفات في أيّ مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يُمكّن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

[2] ــ برنامج 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 Parallel Port أو على التوالي Serial Port وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أيّ محاولة لتدميرها من جانب المتهم. انظر: ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP / IP) في بحث وتحقيق الجرائم على الكمبيوتر، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية ، المنعقد في 26 ــ 28 نيسان 2003، بدبي ــ الإمارات العربية المتحدة ــ ، ص 10. متاح على الموقع التالي :

http://www.arablawinfo.com/research_search.asp?validate=articles&ArticleID=133

[3] ــ**فُتح النظم الحاسوبية** تتألف من محركات الأقراص الصلبة ولوحة المفاتيح ورصد مثل الحواسيب المحمولة وشاشات الحاسوب وغيرها من النظم التي تحتوي على المعلومات المخزنة . أما نظم الاتصال فتشمل جميع أنواع الشبكات بما فيها شبكة المعلومات الدولية ــ الانترنت ــ فهي ثرية جدا من معلومات مثل صفحات المواقع المختلفة (Web Page) والبريد الالكتروني(Email)، غرف الدردشة والمحادثة Logs of (Synchronous Chat Sessions). انظر :

Casey Eghan ، op –cit ، p12-13.

Telephone) والبطاقات الذكية(Smart Cards)[1] والمساعد الرقمي الشخصي (personal digital assistants) [2].

وتأسيسا على هذه الملاحظات، واسترشادا بما سبق عرضه من تعريفات للدليل الالكتروني، يمكننا تعريفه بأنّه : "**معلومات مخزنة في أجهزة الحاسوب وملحقاتها ــ من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات كالطبعات والفاكس ــ أو متنقلة عبر شبكات الاتصال، والتي يتمّ تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها** "[3].

ثانيا ــ خصائص الدليل الإلكتروني:

تنعكس البيئة الرقمية على طبيعة الدليل الالكتروني، باعتبارها المحل الذي يعيش فيه، مما جعله يتصف بخصائص ميزته عن الدليل الجنائي التقليدي وهي كالتالي:

1 ــ **الدليل الالكتروني دليل علمي:** يتكوّن هذا الدليل من بيانات ومعلومات ذات هيئة الكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات، وأدوات الحاسبات الآلية، واستخدام نظم برامجية حاسوبية، فهو يحتاج إلى مجال تقني يتعامل معه، وهذا يعني أنه كدليل يحتاج إلى بيئته التقنية التي يتكوّن فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فان ما ينطبق على الدليل العلمي ينطبق على الدليل الالكتروني. فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القانون المقارن(**إن القانون مسعاه العدالة أما العلم**

---

[1]ــ البطاقة الذكية :بطاقة بلاستيكية تحتوي على شريحة إلكترونية يمكن أن يتم تخزين أي نوع من البيانات عليها سواء كانت بيانات مكتوبة أو صورا، وكذلك يمكن تحميل عدة برامج على البطاقة، ويمكن حماية المعلومات على الشريحة بعدة مستويات من السرية ابتداء من القراءة المباشرة إلى استخدام كلمة سر خاصة بحاملها أو استخدام برامج خاصة تتحكم فيها جهة الإصدار، كما تتميز البطاقة بإمكانية تغيير البيانات المخزنة على الشريحة ودون الحاجة إلى إصدار بطاقة جديدة، ولها عدة تطبيقات وذلك لتنوع البيانات التي يمكن تخزينها، مثل رخص السياقة ، مفاتيح غرف الفنادق والجوازات ..الخ . لمزيد من التفصيل انظر: محمد محمد عنب، موسوعة العلوم الجنائية، تقنية الحصول على الآثار والأدلة المادية، الجزء الأول، مركز بحوث الشرطة، الشارقة، الطبعة الأولى،2007، ص 701 و ما بعدها.

وانظر الموقع التالي: :

http://www.alsharq.com/PrintPage.aspx?xf=2008،February,article_20080220_685&id=ocal&sid=localnewsl

[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 61.

فمسعاه الحقيقة)، وإذا كان الدليل العلمي له منطقه الذي لا يجب أن يخرج عليه،إذ يستبعد تعارضه مع القواعد العلمية السليمة، فانّ الدليل الالكتروني له ذات الطبيعة، فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه [1].

3 ــ **الدليل الالكتروني دليل تقني:** فهو مستوحى من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية، وتتمثل هذه الأخيرة في إطار الجرائم الالكترونية في العالم الافتراضي، وهذا العالم كامن في أجهزة الحاسب الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها. فالأدلة الرقمية ليست مثل الدليل العادي، فلا تنتج التقنية سكينا يتمّ به اكتشاف القاتل أو اعترافا مكتوبا أو بصمة أصبع ..الخ، وإنّما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان.

4 ــ **الدليل الرقمي دليل متنوع ومتطور:**حيث يشمل كافة أشكال وأنواع البيانات الممكن تداولها رقميا، بحيث يمكن أن يظهر على شكل وثيقة (Document) معدة لنظام المعالجة الآلية، كما من الممكن أن يكون صورة ثابتة أو متحركة (أفلام رقمية) أو معدة بنظام التسجيل السمعي البصري أو يكون مخزنا في البريد الإلكتروني .. إلخ.

وأمّا عن كون الدليل الإلكتروني دليلا متطورا فهي خاصية تكاد تكون تلقائية، نظرا لارتباطه الوثيق بالطبيعة التي تتمتع بها حركة الإتصال عبر الانترنت والعالم الإفتراضي اللذان لا يزالان في بدايتهما و لم يصلا بعد إلى منتهاهما ولن يكون من السهل إحتواؤهما[2].

5 ــ **الدليل الالكتروني صعب التخلص منه:** وتعدّ من أهم خصائص الدليل الالكتروني، بل يمكن اعتبار هذه الخاصية ميزة يتمتّع بها الدليل الرقمي عن غيره من الأدلة التقليدية، حيث يمكن التخلص بكل سهولة من الأوراق والأشرطة المسجلة إذا حملت في ذاتها إقرار بارتكاب شخص لجرائم وذلك بتمزيقها وحرقها، كما يمكن التخلص من بصمات الأصابع بمسحها من موضعها، كما انه في بعض الدول الغربية يمكن التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة، هذا الأمر بالنسبة للأدلة التقليدية ،أمّا بالنسبة للأدلة الرقمية فان الحال غير

---

[1] ــ عمر محمد ابوبكر بن يونس، مرجع سابق، ص 977. وانظر أيضا: Eoghan Casey ، op –cit , p. 9

[2] ــ سعيداني نعيم، مرجع سابق، ص 124.

ذلك، حيث يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، ممّا يؤدي إلى صعوبة الخلاص منها، لان هناك العديد من البرامج الحاسوبية وظيفتها استعادة البيانات التي تمّ حذفها أو إلغائها مثل**O&O Rescue Box v4.0**, **Recover Lost Data**[1]، سواء تمّ هذا الإلغاء بالأمر(Delete) أو عن طريق إعادة تهيئة أو تشكيل للقرص الصلب (Hard Disk) باستخدام الأمر (Format)، سواء كانت هذه البيانات صور أو رسومات أو كتابات أو غيرها، كل ذلك يشكل صعوبة أخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة، طالما علم رجال البحث والتحقيق الجنائي بوقوع الجريمة . بل إن نشاط الجاني لمحو الدليل يشكل كدليل أيضا، فنسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا كدليل إدانة ضده [2].

6 ــ **الدليل الالكتروني قابل للنسخ:** حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى (التقليدية)، ممّا يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق نسخ طبق الأصل من الدليل[3]. ومثل هذا الأمر لاحظه المشرع البلجيكي فقام بتعديل قانون التحقيق الجنائي (Code d'instruction Criminelle) بمقتضى القانون المؤرخ في(28 نوفمبر 2000 م)، حيث تمّ إضافة المادة (39 bis) التي سمحت بضبط الأدلة الرقمية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية [4].

---

[1] ــ لمزيد من التفصيل حول هذه البرامج انظر الموقع التالي:

http://edu.arabsgate.com/showthread.php?t=502020

[2] ــ ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في: 10 ــ 12 مايو 2003 ، ص 2240 .

[3] ــ عبد الناصر محمد محمود فرغلي وعبيد سيف سعيد المسماري، مرجع سابق ، ص 15 .

[4] ــ عمر محمد ابوبكر بن يونس، مرجع سابق، ص 978 .

الفرع الثاني: تقسيمات الدليل الإلكتروني

يتخذ الدليل الإلكتروني عدة صور وأشكال، وفي هذا الإطار قامت وزارة العدل الأمريكية سنة 2002 عرض تقسيم لهذا الدليل إلى ثلاث مجموعات وهي كالتالي [1]:

1 ــ السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت .

2 ــ السجلات التي تمّ إنشاؤها بواسطة الحاسوب، وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل (Log Files) وسجلات الهاتف وفواتير أجهزة السحب الآلي (ATM).

3 ــ السجلات التي تمّ حفظ جزء منها الإدخال وجزء آخر تمّ إنشاءه بواسطة الحاسوب، ومن أمثلتها: أوراق العمل المالية التي تحتوي على مدخلات تمّ تقليمها إلى برامج أوراق لعمل مثل Excel، ومن تمّ تمّت معالجتها بإجراء العمليات الحسابية عليها .

وهو نفس التقسيم الذي أخد به القضاء الأمريكي، فسجلات الحاسوب Computer (Records المقبولة استثناء أمام القضاء الأمريكي إذا كانت معدة في هيئة نصوص Text تتخذ أحد هذه الأشكال : **سجلات الحاسوب المتوالدة (Computer-generated records)وسجلات الحاسوب المخزنة (Computer-stored records)** والفرق بينهما يتوقف على ما إذا كان الشخص أو الآلة تنشئ محتويات هذه السجلات أي(مصدر هذه السجلات)، فسجلات الحاسوب المخزنة تشير إلى الوثائق التي تحتوي على كتابات (Writings) شخص أو بعض الأشخاص وحدث وان صارت في شكل الكتروني، مثل رسائل البريد الالكتروني .(E-mail messages)

أمّا سجلات الحاسوب المتوالدة فالكمبيوتر هو الذي يصدرها، وهي تحتوي على مخرجات (Output) برامج الحاسوب التي لم تمسّها أيدي البشرية مثل سجلات الدخول على الانترنت(Log-in records) ومصدرها مزود خدمة الانترنت، فهذه السجلات لا تحتوي على

[1] ــ سلطان محي الديحاني، الجرائم المعلوماتية،على الموقع التالي :

http://www.atsdp.com/forum/zbmszjg-zbgbjgzkni-4377.html

بيانات بشرية، فهي مجرد مخرجات كان لابد من وجود مدخلات (Input) لها ممثلة في لوغاريتمات البرمجة [1].

وهناك نوع ثالث من السجلات يجمع بين التدخل الإنساني ومعالجة الكمبيوتر، كما لو أدخل متهم بيانات معينة وطلب من الكمبيوتر أن يقوم بمعالجتها توصلا إلى نتائج يسمح بها البرنامج المستخدم، كمن يتهرب من الضرائب فيقوم بتسجيل بيانات غير صحيحة عن دخله وربحه طالبا من الكمبيوتر حساب الضريبة المستحقة[2]. ونشير أن هذه الطبيعة الخاصة بكل نوع تنعكس على قيمته الاثباتية، فهي ليست على درجة واحدة من القوة و القبول أمام المحاكم الأمريكية [3] .

ويؤخذ على هذه التقسيمات أنّها ليست شاملة للدليل الالكتروني بل اقتصرت على نوع محدد منه، وهي سجلات الحاسوب التي تحتوي على نص، بالرغم من أن الدليل الرقمي يشمل كافة البيانات الرقمية الممكن تداولها رقميا كالصور والأصوات والرسوم وغيرها، بل تستخدم حاليا بروتوكولات الاتصالات والتطبيقات المعلوماتية في تحقيق الجرائم الالكترونية، ويعتبر نظام TCP/IP[4] من أكثر البروتوكولات المستخدمة في شبكات الإنترنت فهي جزء أساسي منه،

---

(1)- Department of Justice in United States," Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" July 2002 ,available at: http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm

ـــ وانظر أيضا في نفس المعنى: عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي ، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، دون دار نشر، 2006، ص 420 و ما بعدها . كذلك انظر لنفس المؤلف، الجرائم الناشئة عن استخدام الانترنت..، مرجع سابق ، ص 981 .

ـــ **اللوغاريتمات أو الخوارزميات** هي مجموعة من التعليمات التي ممكن أن تتبع لانجاز عمل ما بعدد محدد من الخطوات وذلك عبر تجزئة المسألة البرمجية المراد حلها إلى أجزاء صغيرة بسيطة و بتجميع هذه الأجزاء يمكن التوصل إلى الحل الصحيح . انظر: ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت.، مرجع سابق ، ص91 .

(2)ـــ شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 409.

(3)ـــ انظر فيما سيأتي في الفصل الثاني، ص 291.

(4) ـــ بروتوكول التحكم بالنقل ـــ بروتوكول الانترنت TCP/IP: هي عائلة بروتوكولات الاتصالات بين عدة أجهزة من الكمبيوتر طورت أساسا لنقل البيانات بين أنظمة (UNIX) ثم أصبحت المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الانترنت بواسطة الاتصال الهاتفي وهما في الأصل بروتوكولين مستقلين في شبكة الانترنت، ويعملان معا وبشكل متزامن حيث يرتكزان على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Packet) بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصلة فيما بينها. لمزيد من التفاصيل بروتوكول TCP/IP، انظر: ممدوح عبد الحميد عبد المطلب ، استخدام بروتوكول TCP / IP في بحث وتحقيق الجرائم على الكمبيوتر ،المؤتمر سابق الذكر.

حيث تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحدّد الأجهزة التي أصابها الضرر من الفعل الإجرامي وتحديد نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة.

من خلال ها العرض، نقول أنه أية محاولة لتقسيم الدليل الالكتروني ينبغي أن يراعى فيها اعتبار مهم ألا وهو التطور المستمر الذي يطرأ على البيئة الرقمية التي يعيش فيها الدليل الرقمي، ممّا تجعله من الأدلة المتطورة بطبيعتها، فتطور هذه البيئة يكاد يكون تلقائي هنا، حيث تتسع لإمكانية شمول مظاهر رقمية جديدة [1].

المبحث الثاني: القواعد الإجرائية لاستخلاص الدليل الإلكتروني

ممّا لا شك فيه أنّه لا يوجد ما يسمّى بالجريمة الكاملة مهما حاول الجاني إخفاءها، وذلك استنادا إلى قاعدة " **لوكا رد لتبادل المواد**" التّي تنص على أنّه عند احتكاك جسمين بعضهما ببعض فانّه لابّد وأن ينتقل جزء من الجسم الأوّل إلى الثاني وبالعكس[2]، وبالتالي ينتج عن هذا الاحتكاك ما يعرف بالدليل الجنائي، وفي مجال الجريمة الالكترونيّة لدينا الدليل الالكتروني، وحتّى يتحقّق هذا الدليل لاثبات هذا النوع المستحدث من الإجرام، فإنّه لابد من جمع عناصر التحقيق والدعوى، وتقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو ترجّح معها إدانة المتّهم قدمته إلى المحكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي لإدانة المتهم وإلا قضي ببراءته.

إلا أنّ خصوصيّة الجريمة الالكترونيّة وذاتيّة الدليل الالكتروني سوف يقود دون شك إلى تغيير كبير إن لم يكن كليّا في المفاهيم السائدة حول إجراءات الحصول على هذا الدليل، وذلك نتيجة لضئالة دور بعض الإجراءات التقليديّة في بيئة تكنولوجيا المعلومات، وبالتالي يقودنا إلى إتباع نوع مستحدث من الإجراءات يتلاءم وطبيعة هذه البيئة .

---

[1] ــ عمر محمد ابوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت..، مرجع السابق، ص 980.

[2] ــ خالد حمد محمد الحمادي، الثورة البيولوجية، ودورها في الكشف عن الجريمة، دار الجامعة الجديدة، 2005، ص 19.

وعلى ذلك سنتناول في هذا المبحث الإجراءات التقليدية لإستخلاص الدليل الالكتروني أولا، ثم يليه الإجراءات الحديثة لإستخلاص هذا الدليل.

المطلب الأول: القواعد الإجرائيّة التقليديّة لاستخلاص الدليل الالكتروني

نظم المشرع كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا إلى هذه الغاية، وأهم هذه الإجراءات كما بيّنها القانون، هي: المعاينة، التفتيش، وضبط الأشياء، سماع الشهود وندب الخبراء، وهي تستخدم بصفة عامة لجمع الدليل في جميع الجرائم التقليديّة منها والمستحدثة، إلا أن دورها في الثانية يكون بحاجة إلى تطوير لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها، وهو ما سوف نلاحظه في الفروع المتقدّمة من هذا المطلب.

الفرع الأول : التفتيش وضبط الدليل الالكتروني

إنّ التفتيش في الجرائم التقليدية ما هو إلا وسيلة للإثبات المادي، ذلك لأنه إجراء يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وغايته دوما هي الحصول على الدليل المادي، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي والشبكات، فهي مجرد نبضات ليس لها أي مظهر مادي محسوس في العالم الخارجي، فلا سبيل لأن يرد عليها تفتيش أو ضبط[1]، ومن الأجدر إخضاعها لأحكام مستقلة تتلاءم وطبيعتها الخاصة.

ولعل الإشكال الذي يطرح نفسه يتمحور **حول موقف المشرع الجزائري من هذه الإشكالية، بعبارة أخرى هل خصص أحكام خاصة تتعلق بالتفتيش والضبط في البيئة الإفتراضية؟**

---

[1]ـــ يرى جانب من الفقه أن الإصطلاح الواجب إطلاقه على عملية البحث عن أدلة الجريمة في العالم الإفتراضي هو" الولوج أو النفاذ" باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، بينما مصطلح التفتيش فيعني البحث ، القراءة والتدقيق في البيانات وهو مصطلح تقليدي أكثر، وهناك من يستخدم المصطلحين معا بغرض التنظيم والتنسيق بين المفاهيم التقليدية والحديثة، وهذا ما نستشفه من المادة 19 من الإتفاقية الأوربية لجرائم الانترنت والتي تنص:"1 ـــ كل طرف يتبنى الإجراءات التشريعية وغيرها من الإجراءات اللازمة من أجل أن تكون سلطاته المختصة مؤهلة قانونا لتفتيش أو للولوج بإحدى الطرق ..."، انظر: مرنيز فاطمة، مرجع سابق، ص 238.

أولا: التفتيش في البيئة الالكترونية

التفتيش[1] إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهمّ إجراءات التحقيق في كشف الحقيقة لأنّه غالبا ما يسفر عن أدلّة مادية تؤيد نسبة الجريمة إلى المتهم.

التفتيش ليس غاية في حدّ ذاته، وإنّما هو وسيلة لغاية تتمثّل فيما يمكن الوصول من خلاله إلى أدلّة ماديّة تساهم في بيان وظهور الحقيقة[2]. ونتيجة لذلك يعدّ تفتيش نظام الحاسوب والانترنت من أخطر المراحل حال اتخاذ الإجراءات الجنائية ضد مرتكب الجريمة الالكترونية، لكون محلّ التفتيش هنا ـــ وهو الحاسوب والشبكات ـــ محلّ جدل فقهي متزايد يوما بعد يوم خاصة بالنسبة للكيان المعنوي للحاسوب فهو مجرد برامج وبيانات الكترونية ليس لها أيّ مظهر مادي محسوس.

فما مدى صلاحية مكونات وشبكات الحاسوب كمحلّ يرد عليه التفتيش، وما هي الضوابط التي يجب إتباعها في ذلك؟ وهذا ما سوف نتناوله على النحو التالي:

أ ـــ مدى قابلية مكونات وشبكات الحاسوب للتفتيش: تتكوّن نظم الحاسوب من مكوّنات مادية(Hardware)[3] ومكوّنات منطقيّة (Software)[4]،كما أنّه تربطه بغيره من الحاسبات شبكات اتصال بعدية[5] على المستوى المحلّي أو الدولي.

---

[1]ـــ يقصد بالتفتيش "إجراء من إجراءات التحقيق يقوم به موظّف مختص، طبقا للإجراءات المقررة قانونا، في محلّ يتمتّع بحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقّق وقوعها لإثبات ارتكابها أو نسبتها إلى المتّهم ". لمزيد من تعريفات أخرى للتفتيش انظر: عوض محمد عوض، قانون الإجراءات الجنائي، الجزء الأول، مؤسسة الثقافة الجامعية، 1989، ص 475. محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الجزء الثاني، التفتيش و الضبط، الطبعة الأولى، مطبعة جامعة القاهرة، 1978، ص 14. أحمد فتحي سرو ر، الوسيط في قانون الإجراءات الجنائية دار النهضة العربية، القاهرة ، الطبعة الثانية، 1981، ص 544. قدري عبد الفتاح الشهاوي، مرجع سابق، ص 15. أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، طبعة 1999، الجزائر، ص 40.

[2]ـــ حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، منشأة المعارف، الإسكندرية، 1982، ص 385.

[3] ـــ المكونات المادية هي مجموعة من الوحدات لكل منها وظيفة محددة وتتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، وتسمى بمعدات الحاسوب، وهي: وحدات الادخال، وحدة الذاكرة الرئيسية،وحدة ذاكرة القراءة، وحدة الحاسب والمنطق والشاشة، وحدة التحكم، وحدة الذاكرة المساعدة، وحدة الإخراج، والطابعة. انظر في تفاصيل ذلك: محمد خليفة، مرجع سابق، ص 8.

[4]ـــ يعرف الكيان المنطقي للحاسب بأنه: مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات. عفيفي كامل عفيفي، مرجع سابق، ص 78.

[5]ـــ علاء الدين محمد فهمي وآخرون، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، القاهرة مطابع المكتب المصري الحديث، 1991، ص 10 .

1 ــ تفتيش مكوّنات الحاسوب الماديّة:

الواقع أنّ تفتيش المكوّنات الماديّة للحاسوب بأوعيّتها المختلفة بحثا عن شيء يتّصل بجريمة الكترونيّة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، يدخل في نطاق التفتيش طالما تمّ وفقا للإجراءات القانونية المقرّرة، بمعنى أنّ حكم تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء من الأماكن العامة أو الأماكن الخاصة، إذ أنّ لصفة المكان أهميّة خاصّة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتّهم أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلاّ في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقرّرة قانونا في أغلب التشريعات الجنائية كالقانون المصري[1]، إلا أن المشرع الجزائري بمناسبة التعديل الذي أدخله على قانون الإجراءات الجزائية بالقانون رقم (06ــ 22) المؤرخ في 20 /2006/12، استثنى المشرع تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في (الفقرة الثالثة من المادة 47)[2]) ومن بينها الجرائم **الماسة بأنظمة المعالجة الآلية للمعطيات**، حيث نصّ في المادة 64 فقرة الثالثة على أنه: "غير أنّه عندما يتعلّق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 47 (الفقرة 3) من هذا القانون، تطبّق الأحكام الواردة في تلك المادّة وكذا أحكام المادة 47 مكرّر".

يفهم من استقراء هذه المواد أن المشرع لا يشترط حضور الشخص الذي يشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه، وأنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل ودون الحاجة إلى رضائه عند القيام بهذه الإجراءات[3].

---

[1] – يشترط المشرع المصري لصحة تفتيش منزل المتهم صدور الأمر القضائي المسبب ولو في حالة التلبس، وذلك بعد الحكم بعدم دستورية المادة 47من قانون الإجراءات الجنائية المصري، فضلا عن شروط التفتيش العامة. لمزيد من التفصيل انظر: عوض محمد عوض، مرجع سابق، ص 311 وما بعدها، وانظر أيضا: سامي حسن الحسني، النظرة العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1996، ص 163.

[2] ــ تنص (**المادة 3/47 من قانون الاجراءات الجزائية المعدل بالقانون رقم 06ــ 22** على: "عندما يتعلّق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنيّة أو **الجرائم الماسّة بأنظمة الحاسب** والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنّه يجوز إجراء التفتيش والمعاينة والحجز **في كل محلّ سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص..**".

[3] ــ الفقرة الثانية من المادة 64 : " .....وتطبق فضلا عن ذلك أحكام المواد 44 إلى 47 من هذا القانون" أي عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بجرائم المعلوماتية.

الملاحظ أن المشرع في هذه الحالة قد غلب المصلحة العامة على حريات الأفراد، ومرد ذلك إلى اعتبارين[1]:

ـــ ذاتية الجريمة المعلوماتية المتمثلة في إمكانية اختفائها بسرعة فاقة.

ـــ افتراض كون الدليل الالكتروني هو الدليل الوحيد في الدعوى الجزائية ومن تم ارتكاز كل العملية الإثباتية على وجوده.

أمّا بالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكوّنات الحاسب سالفة الذّكر أو كان مسيطرا عليها أو حائزا لها فإنّ تفتيشها لا يكون إلاّ في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.بمفهومه على الأشياء المادية

2 ـــ تفتيش المكونات المعنوية لنظام المعالجة الآلية: لقد ثار خلاف تشريعي وفقهي بشأن مدى جواز تفتيش المكوّنات المعنوية للحاسوب تمهيدا لضبط الأدلة الالكترونية .

ذهب الرأي الأوّل إلى عدم جواز تفتيش نظم الحاسوب، على أساس أن هدف التفتيش هو البحث عن الأشياء وضبطها، وهذا الشئ ء يقتصر على المال ذي الحيز المادي المحسوس ولا يمتد إلى الكيانات المنطقية، وقد عملت الدول التي أخذت بهذا الإتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية[2].

على النقيض من ذلك هناك رأي آخر يرى أن المنظومة المعلوماتية بما تشمله من برامج الحاسوب يمكن أن تنطبق عليها خصائص وسمات المادة، وبالتالي تدخل في نطاق الأشياء المادية، مستندين في ذلك إلى أن المادة هي كل ما يشغل حيزا ماديا في فراغ معين، وأن هذا الحيز يمكن قياسه والتحكم فيه وذلك بمقياس البايت(Byte) والكيلوبايت(Kb) والميغابيت(MB)[3].

---

[1] ـــ سعيداني نعيم، مرجع سابق، ص 145.

[2] ـــ علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، ، عالم الكتب الحديثة، مصر، 2004، ص 31.

[3] ـــ هلال بن محمد بن حارب البوسعيدي، مرجع سابق، ص 250.

وقد استجاب المشرع الفرنسي لهذه التغيرات وقام بتعديل النصوص التي تحكم التفتيش من خلال المادة 42 من االقانون رقم 2004/545 المؤرخ في 2004/06/21 المتعلق بالثقة في الاقتصاد الرقمي حيث أضاف عبارة "**المعطيات المعلوماتية**" في المادة 94 من قانون الإجراءات الجزائية الفرنسي ليصبح نص المادة على النحو التالي: " يباشر التفتيش في جميع الأماكن التّي يمكن العثور فيها **على أشياء أو معطيات معلوماتية** يكون كشفها مفيدا لإظهار الحقيقة"[1].

أمّا المشرّع الجزائري فقد ساير نهج المشرّع الفرنسي من خلال القانون رقم 09/ 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، حينما أجاز صراحة تفتيش المنظومة المعلوماتية، وذلك بموجب المادة 05 منه التي نصت على أنه: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية ....الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين معلوماتية".

في هذا الصدد صرّحت المادة 2/19 من إتفاقية بودابست لمكافحة الجرائم المعلوماتية الموقعة قي 23 نوفمبر 2001 المشار إليها سابقا بحق الدول الأعضاء في تفتيش أجهزة الكمبيوتر في إطار الإجراءات الجنائية، على" أنّ لكل دولة طرف الحق في أن تسنّ من القوانين ما هو ضروري لتمكين السلطات المختصّة بتفتيش أو الدخول إلى:

ـــ نظام الكمبيوتر أو جزء منه أو المعلومات المخزّنة به.

ـــ الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزّنة في إقليمها[2]".

---

[1]-Article 94 du C.P.P.F، dispose que :" Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver**des objetsou des données informatiques** dont la découverte serait utile à la manifestation de la vérité".

[2] ـ هلالي عبد الله أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية...، مرجع سابق، ص239.

3 ــ تفتيش الشبكات المعلوماتية المتصلة بالحاسوب[1] "التفتيش عن بعد":

إنّ طبيعة التكنولوجيا الرقميّة قد عقّدت من التحدّي أمام أعمال التفتيش والضبط، وذلك بسبب امتداد الأدلة الالكترونيّة عبر شبكات الحاسوب في أماكن بعيدة عن الموقع المادي للتفتيش، وان كان من الممكن الوصول إليها من خلال الحاسوب المأذون بتفتيشه، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتّى في بلد آخر. لذلك يثار التساؤل حول أثر تفتيش الأنظمة المعلوماتية المتصّلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة. ونستطيع أن نميز في هذه الصورة بين الفرضين على النحو التالي:

الفرض الأوّل: اتصال حاسب المتهم بحاسب آخر موجود في مكان آخر داخل الدولة:

في هذه الحالة وجدت بعض التشريعات الإجرائية حلاّ لهذه المشكلة من خلال نصها على إجازة تفتيش نظم المعلومات المتصلة بالحاسوب الذي يجرى تفتيشه (أي الشبكة وما يتصل بها).

ويعتبر المشرع الجزائري من بين هذه التشريعات حين نصت الفقرة الثانية من المادة 05 من القانون(04/09) بأنه: "في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للإعتقاد 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" .

وإلى جانب المشرع الجزائري نجد المشرع الألماني في المادة 103 من قانون الإجراءات الجزائية الألماني ينص على إمكانية إمتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر. وكذلك الحال بالنسبة للمشرع البلجيكي في المادة 88 من قانون تحقيق الجنايات البلجيكي التي تنص على ''إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو في جزء منه فإن البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي''[2].

---

[1]ــ تعرف الشبكة المعلوماتية بأنها مجموعة مكونة من إثنين فأكثر من أجهزة الحاسوب والمتصلة ببعضها إتصالا سلكيا أو لا سلكيا. وقد تكون الأجهزة متواجدة في في نفس الموقع وتسمى الشبكة المحلية (Intranet)، وقد تكون موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف وتسمى بالشبكة بعيدة المدى(Internet). ومع التطور التكنولوجي لثورة الإتصالات وظهور شبكة الانترنت، والتي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لا مركزية.

[2]ــ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 203.

أما المشرع الفرنسي حسم هذه المسألة أيضا بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون رقم (239 لسنة 2003) بشأن الأمن الداخلي الصادر في 18 مارس سنة 2003 الذي أجازت المادة 17 لرجال الضبط القضائي من درجة ضباط و غيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتمّ فيها التفتيش على البيانات التي تهمّ التحقيق والمخزنة في النظام المذكور أو في أيّ نظام معلوماتي آخر مادامت هذه البيانات متّصلة في شبكة واحدة مع النظام الرئيسي أو يتمّ الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسي"[1].

تسمح الاتفاقيّة الأوربيّة لجرائم الانترنت لعام 2001 للدول الأعضاء أن تمدّ نطاق التفتيش الذي كان محلّه جهاز كمبيوتر معيّن إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به معلومات يتمّ الدخول إليها في هذا الجهاز من خلال الجهاز محلّ التفتيش[2].

على العكس من ذلك، هناك من التشريعات المقارنة ما تقصر أثر إذن التفتيش على الأجهزة الموجودة في مكان محدّد دون امتدادها إلى الأجهزة المرتبط مثل بلجيكا وسويسرا.

الفرض الثاني: اتصال حاسب المتّهم بحاسب آخر موجود في مكان آخر خارج الدولة:

من المشاكل التّي تواجه سلطات التحقيق في جمع الأدلة الالكترونية قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنيّة خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية وذلك بغرض عرقلة التحقيق ومن تمّ سير العدالة.

---

[1]ـــ قام المشرع الفرنسي بتعديل قانون الإجراءات الجنائية الفرنسي بموجب القانون رقم (239 لسنة 2003) بشأن الأمن الداخلي الصادر في 18 مارس سنة 2003، حيث أضاف المادة 57ـــ1 من قانون الإجراءات الجناية والتي حسمت النزاع القائم حول مدى إمكانية تفتيش النظام الرئيسي و الأنظمة المتّصلة به في الداخل و الخارج.

- Article**17-1du LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France** dispose que:"Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

[2]ـــ تنص المادة 2/19 من القسم الرابع على أنه من حق السلطة القائمة بالتفتيش الكمبيوتر المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمدّ نطاق التفتيش إلى أيّ جهاز آخر إذا كانت المعلومات المخزّنة يتمّ الدخول إليها من الكمبيوتر الأصلي محلّ التفتيش"

لمواجهة هذا الإحتمال نجد أن المشرع الجزائري قد أجاز تفتيش الأنظنة المتصلة حتى ولو كانت متواجدة خارج الإقليم الوطني، وهو الوارد بالفقرة الثالثة من نص المادة 05 من القانون رقم (04/09) السابق الذكر " .....إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل". ولعل هذه الفقرة مأخوذ نصها من الفقرة الثانية من المادة 57ـــ1 من قانون الإجراءات الجزائية الفرنسي [1][2].

في نفس الاطار أصدر المجلس الأوربي توصيّات تجيز أن يمتدّ تفتيش الكمبيوتر إلى الشبكة المتّصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة. فتنص التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتّصلة بتقنية المعلومات على أنّه" لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقا لضوابط معيّنة أن تقوم بمدّ مجال تفتيش كمبيوتر معيّن يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة مادامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها، مادام أنّه من الضروري التدخل الفوري للقيام بذلك"[3].

كما نصّت التوصية رقم (17) على أنه "يمكن أن يمتدّ نطاق تفتيش الكمبيوتر إلى النظام المتواجد في الخارج، إذا كان من الضروري اتخاذ إجراءات عاجلة في هذا الشأن. ويتعيّن أن يوجد أساس قانوني

---

[1]ـــ المادة 57 ـــ ½ من قانون الإجراءات الجزائية الفرنسي مضافة بموجب المادة (17 فقرة 2) من قانون الأمن الداخلي رقم (239 لسنة 2003)" إذا تبين مسبقا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني وأنه يمكن الدخول إليها وأنه متاحة إنطلاقا من النظام الرئيسي فإنه يمكن الحصول عليها من طرف ضباط الشرطة القضائية مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية ."

[2]- Article**17-1/2 du LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France** 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".

[3] - عمر الفروق الحسيني، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25ـــ28 اكتوبر 1993، حول "الجرائم الواقعة في مجال تكنولوجيا المعلومات"، دار النهضة العربية، القاهرة،1993 ، ص 461.

لامتداد مجال هذا النوع من التفتيش، حتّى لا يشكل ذلك الإجراء مخالفة لسيادة دولة أجنبيّة لذلك فإنّه من الضروري الحصول على موافقة الدولة التي يمتدّ التفتيش إلى نظام يتواجد على إقليمها".

أجازت المادة (32) من الاتفاقية الأوربية بشأن جرائم الانترنت الموقعة عام2001، إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: الأولى إذا تعلّق التفتيش بمعلومات أو بيانات مباحة للجمهور، والثانيّة إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش[1].

وعلى ذلك، إذا كان امتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي(التفتيش الالكتروني العابر للحدود) له أهميته في إمكانية الحصول على الدليل عن بعد وفي بضع ثواني، إلا أنّ بعض الفقه يتحفظ على القيام بذلك لأنّه يعتبر انتهاك لسيادة الدولة الأجنبيّة، وإذا اقتضت ضرورة التحقيق القيام به ينبغي مراعاة العديد من الضمانات يكون متفق عليها سلفا عن طريق اتفاقيات ومعاهدات في هذا المجال، وهذا ما يؤكد أهميّة التعاون الدولي في مكافحة الجرائم الالكترونيّة.

ب ــ شروط التفتيش في البيئة الالكترونية:

تضمّنت معظم التشريعات الإجرائية على ضوابط معيّنة يجب إتباعها عند التعرّض للحريّات الشخصية بإجراء من الإجراءات الماسّة بالحريّة كالتفتيش و تنقسم الشروط العامّة للتفتيش إلى نوعين من الشروط، شروط موضوعيّة وأخرى شكليّة وذلك على النحو التالي:

1 ــ الشروط الموضوعية لتفتيش نظم الحاسوب: يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث شروط أساسية هي: السبب، المحل، السلطة المختصة بالقيام به. وفيما يلي تفصيل كل شرط على حده:

---

[1] ــ تنص المادة 32 من إتفاقية بودابست لمكافحة جرائم المعلوماتية ما يلي: يمكن لأي طرف دون تصريح من الطرف الآخر :

أ ــ أن يصل إلى البيانات المعلوماتية المخزنة والمتاحة للجمهور(مصدر مفتوح) بغض النظر عن موقعها الجغرافي،

ب ــ أو أن يصل، أو أن يتلقى عبر نظام معلوماتي يقع على إقليمه، بيانات معلوماتية مخزنة في دولة أخرى، إذا حصل هذا الطرف على موافقة قانونية وإرادية من شخص لديه سلطة قانونية للكشف عن هذه البيانات إلى هذا الطرف من خلال هذا النظام المعلوماتي". هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية...، مرجع سابق، ص 378.

أ ــ **سبب التفتيش في البيئة الالكترونية:** سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث[1]، ويتمثل في وقوع جريمة ما جناية أو جنحة واتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، وتوافر قرائن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المتّهم أو في مسكنه أو بشخص غيره أو مسكنه، وهو ما ينطبق على الجريمة الالكترونية على النحو التالي:

أوّلا: وقوع جريمة من الجرائم الالكترونية بالفعل سواء كانت جناية أو جنحة:

لابدّ لصحّة إجراء التفتيش في بيئة تكنولوجيا المعلومات أن نكون بصدد جريمة الكترونية واقعة بالفعل سواء كانت جناية أو جنحة، وتستبعد المخالفات لضآلة خطورتها. وقد عرّف المشرع الجزائري جرائم المتصلة بتكنولوجيا الإعلام والإتصال في الفقرة الأولى من المادة 02 من قانون 09 السابق الذكر بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية ".

تطبيقا لمبدأ شرعيّة الجرائم والعقوبات، فلا محلّ لإصدار الإذن بتفتيش نظم الحاسوب إلا إذا كان المشرّع قد نصّ صراحة على الأفعال التي تشكل جرائم من هذا النوع، وذلك ما فعلته المشرع الجزائري من خلال تعديله قانون العقوبات سنة 2004 بالقانون رقم (04ــ15) المؤرخ في 10نوفمبر سنة 2004، حيث أدرج فصلا خاص ــ الفصل السابع ــ بجرائم المساس بأنظمة المعالجة الآلية للمعطيات (المواد من 394 مكرر إلى 394 مكرر 7 من ق.ع.ج)[2].

الملاحظ أن المشرع الجزائري لا يشترط وقوع جريمة فعلا حتى يتم هذا الإجراء بل أجاز تفتيش النظام المعلوماتي إما للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة الرابعة من نفس القانون، وهو الأمر الذي يفهم صراحة بقراءة نص المادتين معا.

---

[1] ــ قدري عبد الفتاح الشهاوي، مرجع سابق، ص 53.

[2] ــ عائشة بن قارة مصطفى، مرجع سابق، ص 100.

ثانيا ــ اتهام شخص أو أشخاص معيّنين بارتكاب الجريمة أو المشاركة فيها:

ينبغي أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية تدعو للاعتقاد بأنه قد ساهم في ارتكاب الجريمة الالكترونيّة أو شريكا فيها ممّا يستوجب اتهامه فيها، وبالتالي إمكانية تفتيش حاسوبه الشخصي وبرامجه الخاصة . و لم تتعرّض قوانين الإجراءات الجنائية لتعريف الدلائل، وإنّما اكتفت بالنص على تطلب الدلائل القوية والمتوافقة مع الاتهام[1].

إلاّ أنّ الفقه تصدّى لتحديد مفهومها حيث عرّفها بأنّها "مجموعة الوقائع الظاهرة والملموسة التي يستنتج منها أنّ شخصا معيّنا هو مرتكب الجريمة"[2].

أمّا الدلائل الكافية في الجرائم الالكترونيّة، يقصد بها "مجموعة المظاهر أو الأمارات المعيّنة القائمة على العقل والمنطق والخبرة الفنيّة والحرفيّة للقائم بالتفتيش والتي تؤيد نسبة الجريمة الالكترونية إلى شخص معيّن بوصفه فاعلا أو شريكا"[3]، ومن أمثلتها: ارتباط عنوان انترنت بروتوكول الخاص بجهاز الحاسوب الذي يحتوي على صور فاضحة مع رقم حساب المتّهم لدى مزوّد الخدمات، ووجود رقمين للتلفون لديه يستخدمان في ذلك[4].

ثالثا ــ توافر أمارات قويّة أو قرائن على وجود بيانات أو معدّات معلوماتيّة تفيد في كشف الحقيقة لدى المتّهم المعلوماتي أو غيره:

من المستقرّ عليه في التشريعات المقارنة أنّ الإذن بالتفتيش يلزم أن يصدر بناء على تحريّات جدية، فلا يكفي لحث سلطة التحقيق إلى إصدار قرارها بالتفتيش مجرد وقوع جريمة من الجرائم الالكترونيّة، واتهام شخص معيّن بارتكابها، بل يجب أن تتوافر لدى المحقق أسباب كافية أنّه يوجد في

---

(1) ــ أنظر المواد (34، 350، 134) من قانون الإجراءات الجنائية المصري، والمواد(2ــ 63، 105، 176 ، 177، 211، 212) من قانون الاجراءت الجنائية الفرنسي.

(2) ــ أحمد فتحي سرور، مرجع سابق، ص 755. وانظر أيضا في نفس المعنى:

Roger Merle et AndreVitu، Traité de droit criminel, tome 2, dexieme édition, édition Cujas, p. 757.

(3) ــ هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1997، ص 121.

(4) ــ شيماء عبد لغني، مرجع سابق، ص 282.

مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في الجريمة الالكترونيّة، أو أشياء متحصّلة منها، أو أيّ أدلّة الكترونيّة يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتّهم أو غيره[1].

ب: محل التفتيش:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء الماديّة التي تتضمّن سرّه، و السّر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة كالمسكن أو الشخص و الرسائل [2]. ومحل التفتيش في الجريمة الالكترونيّة هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الإتصال .

لكي يتمّ التفتيش على هذه المحال، فإنّه ينبغي الإشارة أنّ هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إمّا موضوعة في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو هاتف نقال.

سبق أن أشرنا إلى مدى قابليّة المكونات المادية والمعنوية للحاسوب فضلا عن شبكات الاتصال الخاصّة به، وموقف التشريعات المقارنة من ذلك[3].

1ـــ الإذن بالتفنيش:

من الضمانات المقررة في التشريعات القضائية الإجرائية أنه لا يجوز تفتيش المساكن أو الشروع في تفتيشها إلا بإذن مكتوب من السلطة القضائية المختصة.

وغالبا ما يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يتواجد في المسكن، ومن تم فهل يجوز بمقتضى هذا الإذن لضابط الشرطة القضائية الولوج إلى البيئة الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن الأدلة الإثباتية التي يمكن أن تكون محل الضبط؟

من المستقر عليه في التشريعات المقارنة كالقانون الأمريكي مثلا لا يجيز تفتيش جهاز الكمبيوتر إلا بناء على إذن وفقا للأصل العام، أما المشرع الجزائري فإنه لم يقدم حلا لهذه المسألة بصورة صريحة، ذلك أن القواعد الخاصة بإجراء التفتيش المذكور في قانون الإجراءات الجزائية تتعلق بالتفتيش

(1) USA v. Raymond Wong, App. 9th Cir, No. 02 -10070 CR-00-40069-CW,June 26, 2003.

(2)ـــ قدري عبد الفتّاح الشهاوي، مرجع سابق، ص 110 و ما بعدها.

(3)ـــ انظر فيما سبق، ص 229.

التقليدي الذي محله المساكن وملحقاتها، وأن القواعد الخاصة بإجراء التفتيش المعلوماتي الوارد بالقانون(09 ــ04) السالف الذكر لا نجد المشرع ينص على هذا الشرط إطلاقا، باستثناء إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.

إلا أنه طبقا لمعيار الخصوصية التي يحميها المشرع فإن النظام المعلوماتي وما يحويه من أسرار الأشخاص فإنه يخضع بالتبعية لمبدأ عدم جواز الدخول إلى هذا النظام المعلوماتي وتفتيشه دون إذن من السلطة القضائية المختصة أو دون إذن صاحبه، ومؤدى ذلك أنه من أجل تفتيش منظومة معلوماتية يحتاج ضابط الشرطة القضائية إلى إذنين بالتفتيش، الأول يخص بالمسكن الذي يتواجد به الحاسوب، والثاني يتعلق بتفتيش المنظومة المعلوماتية في حد ذاتها أو على الأقل إذنا واحدا يجيز تفتيش جهاز الكمبيوتر الخاص بالمتهم إلى جانب تفتيش المسكن[1].

تجدر الإشارة في هذه الحالة أنه يجب أن يحدد في إذن اتفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها(أجهزة الحاسوب، صور جنسية الكترونيّة خاصة بالأطفال، مصنّفات الكترونية مقلّدة..)، والهدف من هذا التحديد هو تجنب التفتيش الاستكشافي، بحيث لا يترك للمأذون بالتفتيش أي سلطة تقديرية في ذلك. إلاّ أنّ هناك صعوبة في احترام هذا الشرط أثناء الممارسة العمليّة في تفتيش أجهزة الكمبيوتر، ويرجع ذلك إلى الطبيعة الخاصة لهذه الأخيرة الذي يحتوي بدوره على عدد كبير من الملفات، بالإضافة إلى أنّ أسماء هذه الملفات لا تدلّ بالضرورة على ما تحتويها، فقد يعمد المتهم إلى وضع أسماء مستعارة لملفات تحتوي على مواد غير مشروعة. كما تثار صعوبة قانونية أثناء تنفيذ إذن التفتيش على هذه الملفات، **فهل يعتبر كلّ ملف" صندوقا مغلقا " يحتاج كل واحد منها إلى إذن قضائي مستقل عن الآخر؟.**

والمشرع الجزائري كأغلب التشريعات لا يقدم حلا لهذه المسألة وما نجده على المستوى القضائي في الولايات المتحدة الأمريكية، وجود تضارب بين الأحكام القضائية بخصوص هذه المسألة، حيث اعتبرت من جهة أنّ الديسك بما فيه من ملفات وجهاز الكمبيوتر بما يحتويه من ملفات صندوقا مغلقا واحدا، ومن ثمّ لا يشترط صدور إذن قضائي مستقل لكل ملف على حده[2].

---

[1] ــ عائشة بن قارة مصطفى، مرجع سابق، ص 106.

[2]-USA v. Raymond Wong, 275 F .3d 449, 464-65 (5th Cir. 2001).

وعلى خلاف ذلك اتجهت أحكام أخرى للقضاء الأمريكي إلى أنّ كل ملف في الكمبيوتر يتطلّب إذنا خاصا لتفتيشه، وبناء على ذلك فإنّها اعتبرت أنّ الملف الواحد صندوقا مغلقا، ويرجع أساس هذا الحكم إلى اعتبار أنّ الكمبيوتر يحتوي على الكثير من المعلومات التي تتعلّق بالحياة الخاصة لصاحب هذا الجهاز، بمعنى اختلاط الملفات المجرمة مع البريئة، وإذا أجزنا لرجال الضبط القضائي فتح الملفات الأخرى الموجودة داخل الجهاز فإنّ ذلك سوف يؤدي بالفعل إلى الاعتداء على الحياة الخاصة للأفراد[1]

2 ــ الشروط الشكلية للتفتيش:

بالإضافة إلى الشروط الموضوعيّة لصحة إجراء تفتيش نظم الحاسوب وشبكات الاتصال الخاصة به، هناك شروط أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريّات الفرديّة من التعسّف أو الانحراف في استخدام السلطة، وتتمثل هذه الشروط في التالي:

أ ــ إجراء التفتيش بحضور أشخاص معينين بالقانون: يعتبر هذا الشرط من أهم الشروط الشكليّة التّي يتطلّبها القانون في الجرائم التقليديّة، وذلك لضمان الإطمئنان إلى سلامة الإجراء وصحة الضبط.

وعليه من خلال استطلاعنا على التشريعات الإجرائية المقارنة نجد أن بعضها أوجب حضور عملية التفتيش الذي تجريه الضبطية القضائية المشتبه فيه أو شهودا[2]، وأوجبت تشريعات أخرى حضور أشخاص معينين في القانون في حالات معينة، وأجازت في أحوال أخرى إجراء التفتيش دون حضور أحد.

---

(1) -USA v. Walser275 F .3d 675, 986(10th Cir. 2001).

(2) ــ بالنسبة لتفتيش المساكن وما في حكمها، نجد أنّ المشرع المصري قد غاير في الشروط المقرّرة وفق الشخص القائم به، حيث اشترط حضور شاهدين في حالة ما إذا كان التفتيش يباشر بمعرفة أحد مأموري الضبط القضائي، وعلى أن يكون هذان الشاهدان بقدر الإمكان من أقارب المتّهم البالغين أو من القاطنين معه بالمنزل أو من الجيران (المادة 51 من قانون الإجراءات الجنائية المصري). أما إذا كان القائم بالتفتيش هو قاضي التحقيق أو عضو النيابة العامة فيصحّ اتخاذ هذا الإجراء دون حاجة لاستدعاء شهود (المادة 92 إجراءات جنائية مصري)، ويستوي الأمر عند قيام مأمور الضبط القضائي بمباشرة التفتيش بناء على ذلك من سلطة التحقيق، فلا يلتزم باستدعاء شهود لأنّ المندوب يحلّ محل النائب تماما.

وإن كان المشرع الجزائري من التشريعات الإجرائية التي أوجبت ضرورة حصول التفتيش المتعلق بالمساكن وملحقاتها حضورالمشتبه فيه عندما يتم تفتيش مسكنه من طرف الضبطية القضائية، وإن تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا، استدعى ضابط الشرطة القضائية لحضور تلك العمليّة شاهدين من غير الموظفين الخاضعين لسلطته[1].

إلا أنه وبموجب التعديل الذّي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم (06ـــ 22) مسّ المادة 45 منه حيث استغنى المشرع عن ضمانة حضور الأشخاص المحدّدين في الفقرة الأولى من هذه المادة في جرائم معيّنة منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات. والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السريّة أثناء جمع الدليل الالكتروني، خاصة وأنّ هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله و التلاعب فيه حتى عن بعد. كما أنّ هذه الضمانة بدأت تتضاءل أهميّتها في الدول التي بدأت تأخذ بإجراء "التفتيش عن بعد"[2]، أو ما يطلق عليها في الفقه الفرنسي مصطلح "التفتيش على المباشر" (Perquisition en ligne)[3] .

ب ـــ ميقات إجراء التفتيش في الجرائم الالكترونيّة: يقصد بضمانة الميقات في التفتيش أن يجريه القائم به خلال فترة زمنيّة عادة ما يحدّدها المشرّع، وذلك حرصا على تضييق نطاق الاعتداء على الحريّة الفردية وحرمة المسكن، في حين نجد بعض التشريعات الإجرائية تركت أمر تحديد ذلك الوقت للقائم بالتفتيش ومن ثمّ يقوم به في كل الأوقات سواء ليلا أو نهارا، ومن بين تلك التشريعات قانون الإجراءات الجنائية المصري.

وعلى العكس من ذلك نجد القانونين الجزائري والفرنسي يحظران تفتيش المنازل وما في حكمها في وقت معيّن، وهو محدّد في القانون الجزائري فيما عدا من الساعة الخامسة صباحا إلى

---

[1] ـــ انظر المادة 45 من قانون الإجراءات الجزائية الجزائري، والتي هي ترجمة حرفية للمادة 56 إجراءات جنائية فرنسي.

[2] ـــ يقصد بالتفتيش عن بعد: قيام مأمور الضبط القضائي بالتفتيش وهو قاعد في مكتبه باستخدام برامج خاصّة تحمل في طابعها قاعدة التفتيش عن الجريمة، ويثير هذا الإجراء العديد من المشكلات القانونية، أبرزها:

ـــ التعدي على الخصوصيّة. ـــ التعدّي على سيادة دول أخرى، ذلك لأنه يعدّ من قبيل التجسس وانتهاك حواسيب وخوادم لهذه الدول, خاصة إذا كانت من الدول التي لا تعترف بمشروعيّة هذه البرمجيات.

[3] -Yann Padova, un aperçu de lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénale, n^0 4, Dalloz,2002, p. 770.

الساعة الثامنة مساء، وذلك من خلال المادة 47 من قانون الإجراءات الجزائية الجزائري[1]، أمّا في القانون الفرنسي فنجده محدّدا من الساعة السادسة صباحا إلى الساعة التاسعة مساء، وذلك من خلال المادة 59 إجراءات جنائية[2].

إلاّ أنّ هناك حالات استثنائية يصح فيها إجراء التفتيش ليلا أو نهارا، تتمثل فيما يلي:

- حالة رضا صاحب المنزل رضا حرا، صريحا وعن علم بالسبب.
- حالة الضرورة وتتمثّل في حالة الاستغاثة من داخل المنزل، وحالتي الحريق والغرق[3] أو ما شابه ذلك.
- التحقيق في جميع 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، وفي أي مكان مفتوح للعموم أو يرتاده الجمهور، إذا تحقّق أنّ أشخاصا يستقبلون فيه عادة لممارسة الدعارة.
- بالإضافة إلى جريمتي المخدرات والإرهاب التي أجاز فيهما المشرع الجزائري مأمور الضبط القضائي إجراء التفتيش في كل ساعة من ساعات النهار أو الليل، أضاف قائمة من الجرائم وذلك من خلال المادة 10 من القانون رقم(06ــ 22)المعدّل والمتمّم للأمر رقم (66ــ 155) والمتضمن قانون الإجراءات الجنائيّة، وتتمثل هذه الجرائم في: الجريمة المنظّمة عبر الحدود الوطنية، **الجرائم الماسّة**

---

[1] ــ تنص المادة 47 من قانون الإجراءات جزائية الجزائري على: "لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساء، إلاّ إذا طلب صاحب المنزل أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقرّرة قانونا".

[2]-Article 59 alinéa 1 du C.P.P.F, dispose que :" Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, l**es perquisitions et les visites domiciliaires ne peuvent être commencéesavant 21 6 heures et après 21 heures**.

[3] ــ تجدر الإشارة أنّه في هذه الحالات إذا كان يجوز فيها لمأمور الضبط القضائي الدخول الليلي في المسكن، إلاّ أنّه لا يجوز تفتيشه، بل له الحق فقط في إلقاء النظر على محتوياته دون معاينتها وفحصها، ولما كان دخول المسكن عملا مشروعا، وكانت حالة التلبس قائمة فيه، فله أن يباشر سلطاته المقرّرة في القانون، وهي القبض على المتّهمين وتفتيشهم وضبط كل ما يفيد في كشف الحقيقة. انظر: محمود نجيب حسني، شرح قانون الإجراءات الجنائية ، الطبعة الثانية، دار النهضة العربة، القاهرة، 1988، ص87.

بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال وكذا الجرائم المتعلّقة بالتشريع الخاص بالصرف[1].

يلاحظ أنّ المشرّع الجزائري عندما استثنى الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات من حظر التفتيش ليلا، يكون قد أدرك فعلا ميزة هذه الجرائم، من حيث قابلية الدليل الالكتروني فيها للمحو والتدمير في أقل من ثانية، لذلك أنّ إرجاء التفتيش في الموعد القانوني قد يعرقل السير الطبيعي لمجريات التحقيق.

أمّا بالنسبة للتشريعات التي لم تنصّ صراحة على مواعيد خاصة لإجراء التفتيش في الجرائم الالكترونيّة، فتسري عليها القواعد العامة التي تحدّد الميقات الزمني لإجراء التفتيش في الجرائم التقليديّة.

2 ــ **محضر التفتيش في الجرائم الالكترونية:** باعتبار أنّ التفتيش عمل من أعمال التحقيق، فينبغي تحرير محضر به يثبت فيه ما تمّ من إجراءات، وما أسفر عنه التفتيش من أدلة، و لم يتطلّب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنّه لا يشترط لصحّته سوى ما تستوجبه القواعد العامة في المحاضر عموما، والتي تقتضي بأن يكون مكتوبا باللغة الرسميّة وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمّن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.

الأمر نفسه بالنسبة لمحضر تفتيش نظم الحاسوب، فإنّه يستلزم بالإضافة إلى الشكليّات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة بتقنيّة المعلومات، ثمّ ينبغي بعد ذلك أن يكون هناك شخص متخصّص في الحاسوب والانترنت يرافقه للاستعانة به في مجال الخبرة الفنيّة الضروريّة، وفي صياغة مسودّة محضر التفتيش.

هذا فيما يخص بالتفتيش كأهم إجراء من إجراءات جمع الأدلة في مجال البيئة الالكترونية، وسنتناول فيما يلي الضبط كإجراء مستقل عن التفتيش على الرغم من أنّ التشريعات الإجرائية عادة

---

[1] ــ تنص المادة 3/47المعدلة بالمادة 10من القانون رقم(06ــ 22)المعدّل والمتمّم للأمر رقم (66ــ 155) والمتضمن قانون الإجراءات الجنائيّة ما يلي:" وعندما يتعلّق الأمر بجرائم المخدرات أو الجريمة المنظّمة عبر الحدود الوطنية، **الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات** وجرائم تبييض الأموال و الإرهاب وكذا الجرائم المتعلّقة بالتشريع الخاص بالصرف فإنّه يجوز إجراء التفتيش و المعاينة والحجز في كل محل سكني أو غير سكني **في كل ساعة من ساعات النهار أو الليل** وذلك بناء على إذن مسبق من وكيل الجمهوريّة المختص".

ما تجمع بينهما باعتبار أنّ ضبط الأشياء المتعلقة بالجريمة هي الأثر المباشر للتفتيش، إلاّ انّه من الممكن أن يكون الضبط نتيجة لمعاينة، كما يجوز للمحقق أن يطالب أحد الأفراد بتقديم شيء موجود في حيازته إليه و يلزمه بذلك، و يطلق على الإجراء " الالتزام بالعرض".

ثانيا ــ الضبط المعلوماتي

يختلف الضبط[1] في الجريمة الالكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل، وذلك بسبب أنّ الأوّل يرد على أشياء ذات طبيعة معنويّة وهي البيانات، المراسلات والاتصالات الالكترونية، أمّا الثاني فيرد على أشياء ماديّة، منقولة كانت أم عقارات، و قد أثارت هذه الطبيعة المعنوية للبيانات جدل فقهي واختلاف تشريعي حول مدى إمكانية ضبطها خاصة إذا كانت مجردة من الدعامة المادية المثبّتة عليها، ويرجع السبب في ذلك أنّ الضبط ــ حسب الأصل ــ لا يرد إلاّ على الأشياء المادية[2].

إذا كان الأمر قد انتهى بنا إلى ضرورة أن يشمل التفتيش المكونات المعنوية للحاسوب، وذلك طبقا للمادة الخامسة (5) من قانون (04/09) السابق ذكره، فانّه من الضروري أن يترتب على ذلك إباحة ضبطها.

من التشريعات التي نصت صراحة على إمكانية ضبط المعطيات المخزنة آليا التشريع الجزائري وذلك بموجب القانون رقم (09ــ 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، أين استحدث المادة 06 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 الازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية ....'' .

---

[1]ــ يقصد بالضبط في قانون الإجراءات الجنائية: "وضع اليد على شيء يتصل بجريمة وقعت و يفيد في كشف الحقيقة عنها و عن مرتكبها ". انظر: مأمون سلامة، شرح قانون الإجراءات الجنائية، دار الفكر العربي، 1998، ص 358.

[2]ــ لمزيد من التفصيل حول هذه الاختلافات انظر: هشام محمد فريد رستم، مرجع سابق، ص 93 و ما بعدها. وانظر أيضا: هلالي عبد الله أحمد، مرجع سابق، ص 199 و ما بعدها. أيضا عبد الفتاح بيومي حجازي، مرجع سابق، 218 وما بعدها.

إلى جانب المشرع الجزائري نجد المشرع الفرنسي حيث تمّ إدخال تعديلات على قانون الإجراءات الفرنسي لسدّ هذا الفراغ التشريعي وذلك بموجب قانون الأمن الداخلي رقم 239 لسنة 2003حيث استحدث المادة (76ـــ 1 فقرة 3)التي تنص على أنّ البيانات التي يتم الحصول عليها من جراء تفتيش النظام المعلوماتي يتعين نسخها على دعامات، ثمّ يتم تحريز هذه الدعامات في أحراز مختومة بالشمع الأحمر [1]، وهذا الأمر شيء طبيعي كون فرنسا من الدول الموقعة على اتفاقية بودابست لعام 2001، ونصت هذه الأخيرة على الضبط في المادة(19) من القسم الرابع منها الخاص بالتفتيش وضبط البيانات المعلوماتية المخزنة[2]، حيث تنص على أنّه" من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: ـــ 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"[3].

تجدر الإشارة إلى أنّ الضبط قد يرد على عناصر معلوماتية منفصلة مثل الديسكات والاسطوانات الممغنطة .. ، وهنا لا تثور أيّ مشكلة قانونية عند القيام بالضبط، ولكن الصعوبة تثار عندما يلزم ضبط النظام كله أو الشبكة كلها، ذلك لأنّها تحتوي على عناصر لا يمكن فصلها، ومع ذلك يتعيّن ضبطها لأنّها تتضمّن عناصر للإثبات في الجريمة، لذلك يتّم إعمال مبدأ التناسب[4] من أجل إقامة التوازن بين مصلحتين، مصلحة الدولة في كشف الحقيقة و مصلحة صاحب النظام في تسيير أعماله وعدم ضياع فرص الربح خاصة في المشروعات الاقتصادية، وقد قضت المحكمة الفدرالية

---

(1)-Article**17-1/3 du LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France** dispose que:" - « Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent 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. ».

(2)-Perquisition des données informatiques stockées.

(3)ـــ هلالي عبد اللاه أحمد، إتفافية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص240 .

(4)ـــ يقصد بهذا المبدأ Principe de proportionnalité :"اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة، بحيث لا يؤدي الضبط إلى تعطيل كل العمل في النظام و الشبكات المتصل بها". انظر:شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 358.

الألمانية بإلغاء قرار الضبط الذي ورد على 220 دسك بالإضافة إلى الوحدة المركزية وذلك اثر مخالفة مبدأ التناسب[1].

أمّا بالنسبة للمكونات المادية للحاسوب فلا يثير ضبطها أيّ مشكلات، فيمكن ضبط الوحدات المعلوماتية الآتية: وحدة المدخلات بما تشمله من مفردات كلوحة المفاتيح، نظام الفأرة، نظام القلم الضوئي..، وضبط وحدة المخرجات وما تشمل عليه من وسائل كالشاشة، الطابعة، الرسم والمصغرات الفيلمية.. ، أيضا وحدات التخزين كالأقراص الصلبة والمرنة وأُقراص الليزر .

من الطبيعي أن تختلف طريقة ضبط البيانات المعالجة آليّا عمّا هو متّبع عند ضبط الأشياء المحسوسة كجهاز الحاسب الآلي وملحقاته كالأقراص المرنة و المودم و الخادم ..[2]، ويرجع ذلك إلى الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة، لأن محل تلك الجرائم هو جوانب معنوية تتعلق بالمعالجة الآلية للمعطيات والتي تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحواسيب التي تحفظها.

لذلك نجد المشرع الجزائري من خلال القانون رقم (09ــ 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السابق الذكر وضع طريقتين لضبط الأدلة الإلكترونية:

❖ **الأولى:** تكون عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية، تكون هذه الأخيرة قابلة لحجزها ووضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليه في قانون الإجراءات الجزائية.

---

(1)-Verguchi Pascal, la répression de délit informatique dans une perspective international, thèse, Montpellier 1996, p. 365.

مشار إليه عندشيماء عبد الغني محمد عطا الله، مرجع سابق، نفس الموضع.

(2)ــ 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 الاعتبارالطرق الأخرى لرفع البيانات غير المادية، وهو ما نستشفه في الفقرة 3 من المادة 19 من الاتفاقية الأوربية لجرائم الانترنت.

❖ أما **الثانية:** تكون باستعمال التقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيات وفق الطريقة الأولى.

ـــ والمعروف أنّه بعدما يتمّ ضبط البيانات الالكترونية و تأمينها فنيّا[1]، و أمام غياب الثقافة المعلوماتية عن المحقق الجنائي ممّا يجعل تلك الأدلة عرضة للإتلاف و الإفساد، لذلك يتعيّن اتخاذ بعض الإجراءات الخاصة للحفاظ عليها وصيانتها من العبث، وذلك على النحو التالي[2]:

1. أخذ نسخة إحتياطية عن المعطيات والعمل عليها لضمان عدم المساس بالدليل الأصلي.
2. ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها.
3. عدم ثني القرص لأن ذلك يؤدي إلى تلفه وفقدانه للمعلومات المسجلة عليه.
4. عدم تعريض الأقراص و الأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة، مع الإشارة إلى أنّ درجة الحرارة المسموح بها تتراوح مابين (2ـــ 32) درجة مئوية، أما بالنسبة للرطوبة المسموح بها تتراوح ما بين (20% إلى 80%).

الفرع الثاني:لخبرة التقنية

الخبرة القضائية عموما هي الاستشارة الفنيّة التّي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علميّة خاصة لا تتوافر لديه[3] فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلميّة والفنيّة و التي لا تتوافر سواء لدى المحقّق أو القاضي.

---

[1] – وذلك ما نوه عليه المشرع الجزائري في المادة السادسة الفقرة الثالثة من القانون رقم 09ـــ 04 حينما أوجبت على السلطات التي تقوم بعملية ضبط الدليل الإلكتروني أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، وأن لاتؤدي إستعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات.

[2] ـــ هشام محمد فريد رستم، مرجع سابق، ص129 وما بعدها.

[3] ـــ أمال عثمان، الخبرة في المسألة الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1964، ص 68 وما بعدها. وانظر أيضا: عادل حافظ غانم، الخبرة في مجال الإثبات الجنائي، مجلة الأمن العام، العدد 43، سنة 1968، ص 19 وما بعدها.

وتقدّم الخبرة عونا ثمينا لجهة التحقيق والقضاء ولسائر السلطات المختصّة بالدعوى الجنائيّة في أداء رسالتها، فبدونها يتعذّر الوصول إلى الرأي السديد بشأن المسائل الفنيّة التي يكون على ضوئها كشف جوانب الحقيقة المبنيّة على الأصول والحقائق العلميّة[1]. لذا فقد اهتمّ المشرع في الجزائر بتنظيم أعمال الخبرة، حيث أجاز قانون الإجراءات الجنائية الجزائري الاستعانة بالخبراء لكل من مأمور الضبط القضائي والنيابة العامة وقاضي التحقيق[2].

الخبرة التقنية في أغلب التشريعات شأنها في ذلك شأن الخبرة القضائية في الجرائم التقليدية من حيث القواعد القانونية التي تحكم الخبرة عموما سواء من خلال اختيار الخبراء أو من حيث عمليات الخبرة في حدّ ذاتها باختلاف الأمور الفنيّة التي تحكم عمل الخبير التقني، إلاّ أنّ هناك بعض التشريعات نظّمت أعمال الخبرة في مجال الجرائم الالكترونيّة مثل القانون البلجيكي الصادر في 23 نوفمبر سنة 2000[3].

وقد نصّت المادة 88 من القانون البلجيكي المذكور على أنّه "يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفيّة الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة، على أن يتمّ ذلك بالطريقة التي تريدها جهة التحقيق"[4].

المشرع الجزائري لم يتخلف عن هذه التشريعات حينما أشار في المادة 05 الفقرة الأخيرة من القانون رقم 09/ 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها السابق الذكر أنه: ‘‘يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية

---

[1]ـــ حسن بن سعيد سيف الغافري، مرجع سابق، ص 440.

[2]ـــ حيث تنص المادة 143 من قانون الإجراءات الجزائري على:"لجهات التحقيق أوالحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبيرا إما من تلقاء نفسها أو بناء على طلب من النيابة العامة وإما بطلب من الخصوم...".

[3]Meunier(C), op.cit. p. 611.

[4] Meunier(C), op.cit, p. 681.

تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

الإشكال المطروح هنا هو: هل يلتزم القاضي دائما برأي الخبير التقني باعتباره رأيا فنيّا محضا، أم أنّه مازال للقاضي الفسحة في تلك الدعوى في أن يطرح رأي الخبير ويعتبر نفسه الخبير الأعلى؟

في ظل دراستنا للخبرة التقنيّة، ارتأينا التطرق إلى هذا النوع المستحدث من الخبرة، من خلال الإشارة إلي القواعد القانونية والفنيّة التي تحكم أعمال الخبير التقنيّ، وذلك فيما يلي:

أولاـــ القواعد القانونيّة التي تحكم الخبرة التقنيّة: سنتناول من خلالها طرق اختيار الخبراء، وواجبات الخبير التقني فضلا عن تحديد مدى حجيّة تقرير الخبير، وذلك من خلال ما يلي:

1 ـــ اختيار الخبراء: حدّد كل من المشرّع الجزائري والمصري طرق اختيار الخبراء، حيث نصّت المادة 144 من قانون الإجراءات الجزائيّة الجزائري على أنّه:" يختار الخبراء من الجدول الذي تعدّه المجالس القضائيّة بعد استطلاع رأي النيابة العامة. وتحدّد الأوضاع التي يجري بها قيد الخبراء أو شطب أسماءهم بقرار من وزير العدل. ويجوز للجهات القضائيّة بصفة استثنائيّة أن تختار بقرار مسبّب خبراء ليسوا مقيّدين في أي من هذه الجداول"، وذلك كحالة عدم وجود الخبرة المطلوبة ضمن هذه الجداول.

ترك القانون لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعدّدين (المادة 147 قانون الإجراءات الجزائيّة الجزائري)، وهذا التعدد ضروري في مجال الخبرة التقنية، ذلك أنّه من الصعوبة وجود متخصّص منفرد له الدراية الكاملة بتقنيات الحاسوب ونظمه، حتّى وإن كان يملك القدرات الماليّة على الظهور بمظهر المتفرّد في مجال الخبرة القضائيّة، هذا من جهة، ومن جهة أخرى، لم يحدّد المشرع طبيعة شخص الخبير سواء كان شخصا طبيعيّا أو شخصا معنويّا كمؤسسة متخصّصة تعمل في مجال المحاسبة مثلا، وان كان الواقع العملي للخبرة الاستعانة بالشخص الطبيعي، إلاّ انّه في مجال الجريمة الالكترونيّة يتعيّن الاستعانة بشركات ومنظمات أو مؤسسات متخصّصة، حيث تملك موارد

ماديّة من برامج وأجهزة حديثة، وموارد بشرية من مهندسين متخصّصين في الحاسوب والانترنت، ومن أمثلة هذه الشركات، مختبر الخبرة والبحث عن البصمات (الآثار) المعلوماتية في فرنسا "Lerti"[1].

وتجدر الإشارة في هذا الإطار أنّ بعض الفقه[2] يرى أنّه لا يشترط في الخبير المنتدب أن يكون متخرّج من معاهد أو جامعات متخصّصة في دراسات الحاسوب والانترنت، بل يكفي اكتسابه مهارة وموهبة استعمال الحاسوب والانترنت والتعامل مع تقنيّة المعلومات، إذ أنّ أمهر مبرمجي نظم التشغيل حتّى الآن مثل (Bill Gates)، لم يكن تحصيله العلمي يتجاوز المرحلة الثانويّة، وذات الأمر ينطبق على عتاة الهكرة ومخترقي الأنظمة فإنّ أعمارهم لا تتجاوز مرحلة التعليم الثانوي.

وعلى ذلك، بالرغم من صحة قول الرأي السابق ـــ إمكانية القضاء الاستعانة بخبير غير دارس ـــ، إلاّ أنه يؤخذ عليه بأنه يتعارض مع الواقع القانوني، ذلك أنّه عادة ما يحرّر الخبير في نهاية أعمال الخبرة تقريرا، ويلزم هذا الأخير أن يكون متكاملا لعناصره الشكليّة والموضوعيّة[3]، وبالتالي لا يمكن لشخص دو دراية فنيّة فحسب أن يُعدّ هذا التقرير. فضلا على أنّ هذا الرأي من شأنه جعل جميع أفراد المجتمع بمختلف الأعمار خبراء تقنيّة نتيجة الانتشار الواسع لمعرفة تقنية الحاسوب والانترنت في أواسط هذه المجتمعات.

---

(1) ـــ "Le laboratoire d'expertise et de recherche de traces informatique "Lerti: تمّ إنشاء هذا المختبر سنة 2004من قبل اشتراك خمسة خبراء تقنية من أعلى مستوى في فرنسا، وهذا المختبر مختص في التحقيق الرقمي واستعادة البيانات والبحث عن الآثار المعلوماتية على جميع أنواع الوسائل المعلوماتيّة (كالقرص الصلب، مفاتيح USB وأجهزة المساعد الرقمي الشخص(PDA) ، البطاقات الذكيّة المصرفيّة وأيضا الهواتف المحمولة). وتمّ تعيين هذا المخبر كأوّل شخص معنوي في مجال الخبرة القضائية في فرنسا، حيث أدى هذا المخبر اليمين القانونيّة في 29 يناير، أمام محكمة استئناف Grenoble ، وتمّ تسجيله في قائمة جدول الخبراء. لمزيد من التعريف حول "Lerti"، انظر الموقع الخاص به.

www.Lerti.fr

(2) ـــ عمر بن يونس، مرجع سابق، ص 1025.

(3) ـــ لمزيد من التفاصيل حول كيفية كتابة تقرير فنّي انظر: برهامي أبوبكر عزمي، الشرعيّة الإجرائيّة للأدلة العلميّة، دراسة تحليليّة لأعمال الخبرة، دار النهضة العربيّة، القاهرة، 2006 ، ص 396 وما بعدها.

2 ــ واجبات الخبير التقني: تتمثل هذه الواجبات فيما يلي:

1 ــ حلف اليمين: أوجب القانون[1] على الخبير حلف اليمين قبل أداء مأموريته، وإلاّ كان العمل باطلا، فهو إجراء جوهري قصد منه المشرع حمل الخبير على الصدق والأمانة في عمله وبثّ الطمأنينة في آراءه التي يقدّمها، سواء بالنسبة لتقدير القاضي أو لثقة بقيّة أطراف الدعوى[2].

ولقد استقر الفقه والقضاء على أنّ أداء الخبير لليمين يوم تسليمه العمل يغني عن أداءه اليمين عند مباشرة كل مأموريّة[3]، وهو ما نصت عيه المادة 3/145 من ق.إ،ج،ج، حيث إذا كان الخبير من غير خبراء وزارة العدل المعينين بالقانون، أو كان اسمه غير مقيّد في الجدول، يجب في هذه الحالة استحلافه اليمين بأن يؤدي عمله بالصدق والأمانة.

2 ــ أداء الخبير لمأموريّته بنفسه وفي حدود ما نصّ عليه أمر أو حكم الندب[4][5].

3ــ خضوع الخبير للرقابة القضائية:يتعين على الخبير أن يتولى مهمته تحت رقابة القاضي الذي عينه، وأن يبقى على اتصال دائم به لأجل إحاطته علما بتطورات الأعمال التي يقم بها، فالخبير هو مساعد للقاضي ومعاون فنّي لا أكثر[6].

4ــ استجابة الخبير للطلبات التي قد يوجهها الأطراف أثناء تنفيذ عمليّة الخبرة وهو ما جاء في المادة 152 من قانون الإجراءات الجزائري ، كتكليف الخبير بإجراء أبحاث معيّنة أو سماع أي شخص معيّن باسمه قد يكون قادرا على مدّهم بالمعلومات ذات الطابع الفنّي.

---

[1] – نصّت المادة 145 من قانون الإجراءات الجزائية الجزائري على " يحلف الخبير اليمين المقيّد لأول مرّة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتي بيانها:

ــ أقسم بالله العظيم بأن أقوم بأداء مهمّتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال ــ

ولا يجدّد هذا القسم مادام الخبير مقيّدا في الجدول...".

[2] ــ أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، بحث منشور في بالمركز العربي للدراسات الأمنية والتدريب بالرياض، 1993، ص 28 .

[3] ــ برهامي أبوبكر عزمي، مرجع سابق، ص 383 . نقض 21 4 1959 س 10 ص 479 طعن رقم 483 سنة 29 قضائية.

[4] ــ إلا أنه باستطاعة الخبير الاستنارة في مسألة خارجيّة عن تخصّصه بفنيّن آخرين (المادة 149إجراءات جزائية جزائري) ويتعيّن على هؤلاء أن يحلفوا اليمين وفق الشروط المنصوص عليها في المادة 145 إجراءات جزائري.

[5] ــ وفي ذلك نصّت محكمة النقض المصرية في إحدى القضايا المعروضة عليها ما يلي: " ..للمحكمة في حدود مالها من حق استظهار عناصر الجريمة ألاّ تتقيّد بما قد يعرض له الطبيب في تقريره من توفر نيّة القتل إذ إن مأموريّته قاصرة على حد إبداء رأيه الفنّي في وصف الإصابات وسبب القتل .." . طعن رقم 1354 لسنة 26 ق جلسة 14/ 1/ 1957، مجموعة الأحكام، ص 651.

[6] -J- Michaud، le juge d' instruction et l'expert , R. S. C , 1975 , p. 791.

5 ــ تقديم التقرير الفنّي خلال المدّة المحدّدة بأمر أو حكم الندب، وإذا لم يودع تقريره في المهلة المحدّدة فإنّه يجوز للقاضي استبداله في الحين مع إلزامه بردّ جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها إليه في ظرف ثمان وأربعين ساعة ،ذلك ما نصّت عليه المادة 148 من قانون إجراءات جزائري، وقد يتعرّض الخبير المقصّر إلى عقوبات تأديبيّة وحتّى جزائيّة[1] .

3 ــ مدى حجيّة تقرير الخبير التقني:

بعد انتهاء الخبير من أبحاثه وفحوصاته، يتعيّن عليه أن يعدّ تقريرا يضمنه خلاصة ما توصّل إليه من نتائج بعد تطبيق الأسس والقواعد العلميّة الفنيّة على المسائل محل البحث[2]. ويخضع هذا التقرير شأنه شأن باقي وسائل الإثبات لتقدير القاضي، فالقانون لم يضف عليه أيّة قوة ثبوتيّة خاصّة، فهو لا يلزم القاضي، ولهذا الأخير مطلق الحريّة في تقديره، فله أن يأخذ بنتائج الخبرة أو استبعادها كما يشاء، وله كذلك أن يأمر بإجراء خبرة تكميليّة[3] أو القيام بخبرة مضادة أو مقابلة[4] لاسيما إذا تعارضت النتائج التي توصّل إليها الخبراء حول نفس المسألة أو تعارض تقرير الخبير مع شهادة أحد الشهود.

تجدر الإشارة إلى أنّه وإن كان من المقرّر أن القاضي يملك سلطة تقديريّة بالنسبة لتقدير الخبير الذي يرد إليه، إلاّ أنّ ذلك لا يمتدّ إلى المسائل الفنيّة فلا يجوز له تفنيدها إلاّ بأسانيد فنيّة[5].

---

(1) -J- Bradel, la responsabilite' pénale de l'expert , R.S.C, 1986, p. 24.

(2)ــ تنص المادة 153/ 1 من قانون الإجراءات الجزائية الجزائري: " يحرّر الخبراء لدى انتهاء أعمال الخبرة تقريرا يجب أن يشتمل على وصف ما قاموا به من أعمال ونتائجها، وعلى الخبراء أن يشهدوا بقيامهم شخصيّا بمباشرة هذه الأعمال التي عهد إليهم باتخاذها ويوقعوا على تقاريرهم...".

(3)ــ يقصد بالخبرة التكميليّة:"الخبرة التي تأمر بها المحكمة عندما ترى نقصا واضحا في الخبرة المقدّمة إليها أو أنّ الخبير لم يجب عن جميع الأسئلة و النقاط الفنيّة المعيّن من أجلها أو أنّها لم تستوف حقّها من البحث أو التحرّي، فتطلب المحكمة باستكمال النقص الملحوظ في تقرير الخبرة وتسند الخبرة التكميليّة إلى الخبير الذي أنجزها أو إلى خبير آخر". انظر: مولاي ملياني بغدادي، الخبرة القضائيّة في المواد المدنيّة، مطبعة حلب، الجزائر، 1992، ص 15 .

(4)– كرّست المحكمة العليا الخبرة المضادة في قرارها الصادر بتاريخ 18/ 11/ 1998، تحت رقم 155373، بقولها:"إذا تبث وجود تناقض بين خبرة وأخرى وتعذّر فضّ النزاع بين الطرفين، وجب الاستعانة بخبرة فاصلة وعدم الاقتصار على خبرة واحدة أو خبرتين تماشيّا مع متطلّبات العدل ".

(5)ــ نقض 29/ 5/ 1967، مجموعة أحكام النقض، السنة 18، ص 143. ونقض 11/27/ 1967، السنة 18، ق 251. وقضت في هذا المعنى بأنّ:" رأي الخبير الفنّي لا يصحّ تفنيده بشهادة الشهود، فإذا كانت المحكمة قد أطرحت رأي مدير مستشفى الأمراض العقليّة في

في رأينا، أنّه من الضرورة إعطاء قوّة إلزاميّة لتقرير الخبير التقني، وذلك على أساس أن القاضي إذا رفض رأي الخبير فقد تعارض مع نفسه، إذ يعني ذلك أنّه أراد أن يفصل بنفسه في مسألة سبق أن اعترف في بادئ الأمر بأنّ الخبير يتمتّع فيها بمعرفة ودراية تفوق معرفته الشخصيّة.

وما يحدث عمليّا أنّ القاضي غالبا ما يسلم بما خلص إليه الخبير في تقريره، ويبني حكمه على أساسه، وهذا التصرّف منطقي من القاضي فلا شك في أنّ رأي الخبير ورد في موضوع فنّي لا اختصاص للقاضي به، وليس في شأن ثقافته أو خبرته القضائية أن تتيح له الفصل فيه، بالإضافة إلى ذلك هو الذي انتدب الخبير ووثق فيه ورأى أنّه مناسب لمهمّته[1].

ثانيا ــ القواعد الفنيّة التي تحكم عمل الخبير التقني: بالإضافة إلى القواعد القانونيّة السابقة الذكر والمتوفّرة في جميع التخصصات في مجال الخبرة، وجود قواعد خاصّة تنفرد بها الخبرة التقنية وقبل الشروع في تبيان هذه القواعد يتعيّن علينا تحديد أهم المسائل التي يستعان فيها بالخبرة التقنيّة وهي كالتالي[2]:

1 ــ وصف تركيب الحاسوب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعيّة التي يستخدمها بالإضافة إلى الأجهزة الملحقة به وكلمات المرور أو السر ونظام التشفير.

2 ــ وصف طبيعة بيئة الحاسب أو الشبكة من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائل الاتصالات وتردّد موجات البث وأمكنة اختزانها.

3 ــ وصف الوضع المحتمل لأدلة الإثبات والهيئة التي تكون عليها.

4 ــ التمكن من نقل أدلة الإثبات غير المرئيّة وتحويلها إلى أدلّة مقروءة، أو المحافظة على دعامتها بغير أن يلحقها تدمير أو إتلاف، مع إثبات أنّ المخرجات الورقيّة لهذه الأدلة تطابق ما هو مسجّل على دعائمها الممغنطة.

5 ــ بيان كيفية عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

الحالة العقليّة لشخص واستندت في القول بسلامة عقله إلى أقوال الشهود، فإنّها تكون قد أخلت بحقّ الدفاع وأسّست حكمها على أسباب لا تحمله" . نقض 11/12/ 1951، مجموعة القواعد القانونيّة، ج 1، ق 44، ص 541.

[1] ــ محمد مروان، وسائل الإثبات في المواد الجنائيّة في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعيّة، الجزائر، 1998، ص 404.

[2] ــ هشام فريد رستم، الجوانب الإجرائيّة للجرائم المعلوماتيّة، مرجع سابق، ص 142 و 143 .

6ــ إجراء الإختبارات التكنولوجية على الدليل الإلكتروني للتحقق من أصالتهومصدره كدليل يمكن تقديمه لأجهزة إنفاذ القانون.

1 ــ خطوات اشتقاق الدليل الالكتروني:

وضعت وزارة العدل الأمريكية إطارا عمليا يحدد خطوات أساسية لجمع الأدلة الألكترونية ثم فحصها ومن ثم تحليلها وأخيرا كتابة النتائج المتوصل إليها في تقرير، ويمكن إيجاز هذه الخطوات في المراحل التالية[1]:

أولاّــ خطوات ما قبل التشغيل والفحص:

أ ــ التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدوّن عليها.

ب ــ التأكد من صلاحية وحدات النظام للتشغيل.

ج ــ تسجيل بيانات الوحدات المكوّنات المضبوطة، كالنوع والطراز، والرقم التسلسلي.

ثانيا ــ خطوات التشغيل والفحص:

أ ــ استكمال تسجيل باقي بيانات الوحدات من خلال قراءات الجهاز.

ب ــ عمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب (Hard Disk)، لإجراء عمليّة الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير، سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برامجيّة.

ج ــ تحديد أنواع وأسماء المجموعات البرامجيّة، برامج النظام(برامج التشغيل)، وبرامج التطبيقات، وبرامج الاتصالات..، وما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة، برامج إنشاء ومعالجة الصور في جرائم دعارة الأطفال مثلا.

د ــ إظهار الملفات المخبّأة، والنصوص المخفيّة داخل الصور.

---

[1] ــ عمر محمد بن يونس، الحقوق والحريات والالتزامات الرقمية في القانون الوطني الأمريكي، ورقة عمل مقدمة في المؤتمر الدولي حول أمن المعلومات، المنعقد بتاريخ: 18ــ2005/12/20، مسقط ــ سلطنة عمان، ص 428. وانظر أيضا: ممدوح عبد الحميد عبد المطلب، **استخدام بروتوكول(TCP/IP) في بحث وتحقيق الجرائم على الكمبيوتر..، مرجع سابق، ص 9.**

هـ ــ استرجاع الملفات التي تمّ محوها من الأصل وذلك باستخدام أحد برامج استعادة البيانات، وكذلك بالنسبة للملفات المعطلة أو التالفة، مثل برنامج Recover4all Professional، Easy Recover). وبعد ذلك تخزّن هذه الملفات أو البيانات، ويعمل لها نسخ طبق الأصل أخرى من الأسطوانة أو القرص المحتوي لها لفحصها عن طريق تطبيق الخطوات سالفة الذكر .

و ــ يتم إعداد قائمة يجرّد فيها الخبير كل الأدلة الالكترونيّة التي تمّ الحصول عليها في الديسك الخاص به مع إجراء مراجعة لكل صورة محتفظ بها في الديسك في كمبيوتر آخر للتأكد من سلامة القائمة[1].

ي ــ تحويل الدليل الالكتروني إلى هيئة ماديّة وذلك عن طريق طباعة الملفات، أو تصوير محتواها إذا كانت صور أو نصوص، أو وضعها في أيّ وعاء آخر حسب نوع البيانات والمعلومات المكوّنة للدليل.

ثالثا: تحديد مدى الترابط بين الدليل المادي والدليل الالكتروني:

في هذه المرحلة يتمّ فحص كل من الدليل المادي المضبوط، و الدليل الالكتروني في شكله المادي، ومن تمّ الربط بينهما ممّا يكسب الدليل الموثوقيّة واليقينيّة، اللتان تؤديان إلى قبوله لدى جهة التحقيق والحكم.

رابعا: مرحلة تدوين النتائج وإعداد التقرير:

حيث يتمّ إعداد تقرير بجميع خطوات وإجراءات البحث، ويرفق به في الغالب الملاحق الإيضاحيّة المصوّرة أو المسجّلة وغيرها لاعتمادها ثمّ تسلّم إلى جهة الحكم و القضاء.

2 ــ أدوات جمع الدليل الالكتروني:

يقوم الخبير التقني في سبيل تحري الحقيقة الاستعانة بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله قد يستخدم العديد من الأدوات والبرمجيات التي تمكّنه الحصول على الدليل

[1] ــ ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، مرجع سابق، ص 265.

الالكتروني، وتعتبر هذه الأدوات في نفس الوقت أساسية لأجهزة البحث والتحري والتحقيق بصفة عامة، ومن بين هذه البرمجيات المستخدمة في جمع الأدلة الالكترونيّة كالتالي[1]:

أ ــ برنامج أذن التفتيشComputer Scorch Warrant Program

هو برنامج قاعدة بيانات، يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

ب ــ قرص بدء تشغيل الكمبيوتر (Bootable Diskette)[2]: وهو قرص يُمكن المحقق من تشغيل الكمبيوتر، إذا كان نظام التشغيل فيه محمياً بكلمة مرور ويجب أن يكون القرص مزوداً ببرنامج مضاعفة المساحة Double space فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

ج ــ برنامج معالجة الملفات مثل (X tree Pro Gold)

هو برنامج يُمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يُمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

د ــ برنامج النسخ مثل (Lap Link)

هو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي Parallel Port أو على التوالي Serial Port وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

---

[1] ــ فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دون ناشر، الطبعة الثانية، 2010، القاهرة، ص 109ــ 110.

[2] ــ حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية ، 2000، ص 228 وما بعدها.

هـــ ــ برامج كشف الديسك مثل (AMA Disk, View disk)

يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة[1].

و ــ برامج اتصالات مثل (LANtastic)

يستطيع هذا البرنامج ربط جهاز حاسب الخبير أو المحقق بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

هذه هي أهم الطرق العامة لجمع الأدلة الرقمية، والتي يجب أن يقوم بها خبراء في هذا المجال نظراً لعلمية ودقة هذه الأدلة.

بعد دراستنا لأهم القواعد القانونية والفنية للخبرة التقنية ينبغي علينا التنويه بأن الدولة مهما كانت قوية تكنولوجيا إلاّ أنّها لا تقدر وحدها على مواجهة الإجرام الالكتروني، بل لابد من تعاون دولي في مجال الخبرة التقنية، وذلك من خلال عقد المؤتمرات وحضور الندوات، والاستفادة من تجارب الدول الأخرى، كما ينبغي تخصيص ميزانيّة معينة لتأهيل الخبراء إلى مستوى معين حتى يصبحوا قادرين على التعامل مع هذا النوع المستحدث من الأدلة الالكترونية.

المطلب الثاني: القواعد الإجرائية المستحدثة في استخلاص الدليل الالكتروني

ذكرنا سلفا من خلال المطلب الأول مجموعة من الإجراءات التقليدية للحصول على الدليل الالكتروني, وتبيّن من خلالها مدى الصعوبات التي تحيط بها في ذلك، وهذا ما يسهّل للكثير من المجرمين الإفلات من العقاب، لدى فمن الضروري أن تواكب التشريعات المختلفة هذا التطوّر الملحوظ وذلك من خلال خلق قواعد قانونية إجرائيّة غير تقليدية لهذا الإجرام غير التقليدي، لذلك يكون من الضروري الاعتماد على تقنية تكنولوجية المعلومات في جمع الدليل الالكتروني، وذلك إمّا من أجل تيسير التجميع التقليدي للدليل الالكتروني كالتفتيش والضبط، ومن تمّ تضل هذه الإجراءات فعالة إزاء التغيير في بيئة تكنولوجيا المعلومات، أو تبني إجراءات حديثة مستقلة قائمة بذاتها.

[1]ــ ممدوح عبد الحميد، زبيدة محمد جاسم وعبد الله عبد العزيز، مرجع سابق، ص 2243 وما بعدها.

بما أنّ البيانات في بيئة التكنولوجيا ليست دائما ساكنة، بحيث يمكن أن تكون متحركة عبر شبكة من الشبكات، لذلك ينبغي أن يتلاءم الإجراء وطبيعة البيانات محل هذا الإجراء. فبالنسبة للبيانات الساكنة (الفرع الأول) يتم اللجوء إلى حفظ المعطيات المتعلقة بحركة السير، والأمر بتقديم بيانات معلوماتية متعلقة بالمشترك. أما بالنسبة للبيانات المتحركة (الفرع الثاني) يتم اللجوء إلى مراقبة الاتصالات الالكترونية.

الفرع الأول: الإجراءات المتعلقة بالبيانات الساكنة

إنّ الإجراءات الخاصة بالبيانات الساكنة أو المتحركة[1] كلها مستقاة من اتفاقية بودابست المنعقدة في (23 نوفمبر 2001 م) [2]، وهي أولى المعاهدات الدولية التي تكافح تلك الجرائم الالكترونيّة وهذه الاتفاقية تمت تحت إشراف المجلس الأوربي، ووقع عليها ثلاثون دولة بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوربي المشاركة في إعداد هذه الاتفاقية وهي كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية حيث صادقت عليها هذه الأخيرة في 22 ديسمبر 2006 ودخلت بالفعل حيز النفاد في الأول من يناير 2007 . وهي مفتوحة لانضمام دول أخرى حتى يمكن أن تساهم في ضبط وتنظيم مجتمع المعلومات والاتصالات بشكل أفضل.

---

(1) - البيانات الساكنة هي بيانات موجودة داحا حاسب ألي، وهذا الأخير غير متصل بأي شبكة من الشبكات المعلوماتية سواء المحلية منها كالانترانت أو الدولية كالانترنت، ولذلك فإن الإعتداء على هذه البيانات يتطلب تواجد المعتدي في مركز الحاسب. وعليه لا تحتاج البيانات الساكنة لحمايتها إلا إجراءات أمنية محدودة. بعكس البيانات المتحركة التي تنتقل عبر شبكات الإتصال إذ تحتاج إلا إجراءات أمنية أكبر، لأنها تتعرض للعديد من المخاطر خلال انتقالها من حاسب لآخر، فهي مجودة في عالم إفتراضي غير محدود. انظر: محمد خليفة، مرجع سابق، ص 69 ـ70..

(2)ـ للاطلاع على النص الكامل لاتفاقية بودابست ، يرجى مراجعة الموقع الخاص بالمجلس الأوربي :

http://www.convention .coe.int/treaty/EN/treaties/htm1/185.htm

وقد جاء في ديباجة اتفاقية المجلس الأوربي حول الإجرام السيبيري بيانا لمخاطر انتشار شبكة المعلومات على ما يلي :

ـ " اقتناعا من الدول أعضاء مجلس الاتحاد الأوربي بضرورة منح الأولوية للسعي من اجل تنفيذ سياسة جنائية مشتركة تهدف إلى حماية المجتمع من إخطار جرائم الانترنت ، وهي التي تشمل أمورا من بينها تبني التشريع المناسب ودعم التعاون الدولي .

ـ و إدراكا لعمق التغيرات التي أحدثها التحول إلى الرقمية وارتباط شبكات الكمبيوتر مع بعضها البعض مع استمرار عولمتها .

ـ و انشغالا بمخاطر احتمال استخدام شبكات الكمبيوتر و المعلومات الالكترونية أيضا في ارتكاب جرائم جنائية ....." .

تتمثل الإجراءات المتعلقة بالبيات الساكنة في التحفظ العاجل على هذه البيانات أو كما يسميها المشرع الجزائري حفظ المعطيات المتعلقة بحركة السير (أولا)، ثم الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك(ثانيا).

أولا ــ حفظ المعطيات المتعلقة بحركة السير:

نصت إتفاقية بودابست في المادة 16 منها على ضرورة كل طرف السماح لسلطاته المختصة أن تأمر أو تفرض بطريقة أخرى مزود الخدمة **التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي،** وذلك عندما تكون هناك أسباب تدعو للإعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير. وهو ما أكده المشرع الجزائري بموجب المادة 10 من الفصل الرابع في القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال مكافحتها[1]، حيث ألزم مقدمي الخدمات[2] بحفظ المعطيات[3]وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ووضعها في ترتيب معين في انتضار إتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره، فالتحفظ إجراء أولي أو تمهيدي الهدف منه هو محاولة الإحتفاظ بالبيانات فبل فقدها.

وما تجدر الإشارة إليه في هذا الإطار أنه ليس أي معطيات معلوماتية محل إعتبار من المشرع، بل حصر المشرع الجزائري المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة في المعطيات المتعلقة بحركة السير (معطيات المرور)، وهي كما عرفها في المادة الثانية من القانون رقم (09/ 04) تلك المعطيات المتعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الإتصالات، توضح مصدر الإتصال، الوجهة المرسل إليها والطريق الذي

---

(1) ــ أورد المشرع الجزائري في المادة 10 أنه في إطار تطبيق أحكام هذا القانون (04/09) يتعين على مزودي الخدمة تقديم المساعدات للسلطات المكلفة بالتحريات القضائية...بوضع المعطيات التي يتعين عليهم حفظها وفقا لأحكام المادة 11 أدناه تحت تصرف هذه السلطات"

(2) ــ عرف المشرع الجزائري مزود الخدمة (مقدم الخدمة) بموجب الفقرة 06 من المادة الثانية في القانون 09،04 بأنه:

1/ كل كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الإتصال بواسطة منظومة معلوماتية و،أو نظام الإتصالات.

2/ أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها.

(3) ــ تجدر لإشارة إلى أن هناك فرق بين التحفظ على البيانات"la conservation des données" والاحتفاظ أو أرشفة البيانات"l'archivage des données" ويقصد بالأول حفظ بيانات سبق وجودها في شكل مخزن، وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة. أما الثاني فيقصد به تجميع البيانات والاحتفاظ بها في المستقبل بدون ضمان سلامتها وسريتها، فهو عملية تخزين لا غير. عائشة بن قارة مصطفى، مرجع سابق، ص 159.

يسلكه ووقت وتاريخ وحجم ومدة الإتصال، ونوع الخدمة. وقد حصر المشرع معطيات المرور التي ألزم في المادة 11 مزودي الخدمة بحفظها في:

1 ــ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

2 ــ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

3 ــ الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.

4 ــ المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

5 ــ المعطيات التي تسمح بالتعرف على المرسل إليه الإتصال وكذا عناوين المواقع المطلع عليها.

عرفت إتفاقية بودابست في مادتها ألأولى الفقرة ''د'' هذا النوع من المعطيات بأنها'' محلا لنظام قانوني محدّد، حيث يتمّ توالد هذه البيانات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة، وبذلك فهي تشمل طائفة من البيانات تتمثل في: مصدر الاتصال ووجهته المقصودة، خط السير ووقت أو زمن الاتصال وفقا لتوقيت غرينتش، حجم الاتصال ومدته ونوع الخدمة المؤداة(مثل نقل الملفات أو بريد الكتروني أو مراسلات فوريّة). وفي الغالب ما يحوز مقدم.

بما أن حفظ المعطيات إجراء وقتي واحتراما للحق في الخصوصية فإن المشرع الجزائري وضع إلتزاما على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها بعد سنة من تاريخ التسجيل[1]، وعلى غرار المشرع الجزائري نجد المشرع الفرنسي حرص بدوره في نطاق التخزين التلقائي للمعطيات المتعلقة بالإتصالات الإلكترونية وذلك بموجب المادة 32 من قانون البريد والإتصالات الإلكترونية المضافة بموجب المادة 29 من القانون رقم 2001/ 1062 والمعدلة بالمادة 20 من القانون 2003/ 239 المؤرخ في 03/18/ 2003 المتعلق بالأمن الداخلي على ضرورة مسح المعطيات المخزنة بعد الإحتفاظ بها لمدة أقصاها سنة إذا دعت مقتضيات البحث والتحقيق والمتابعة القضائية ذلك.

[1] ــ تنص المادة 11 من القانون رقم 09 /04 " ...تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة إبتداء من تاريخ التسجيل..."

ثانيا ــ الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك:

البيانات الشخصيّة المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصيّة التي تحميه الاتفاقيّة الأوربية لحقوق الإنسان والحريات الأساسية (بتاريخ 4 نوفمبر 1950)، فلا يجوز لمزود الخدمات أو غيره أن يقوم بإفشاء ما لديهم من معلومات إلى الغير. إلا أنّ بعض التشريعات المقارنة تسمح لرجال الضبط القضائي أن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات والتي يطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزودو الخدمات، وهو ما يلزمه القانون الفرنسي رقم 719 لسنة 2000 المعدل للقانون رقم 1067 لسنة 1986 الخاص بحريّة الاتصالات، حيث تنص المادة(43ــ9) منه على" أنّه يتعيّن على مزودي خدمات الدخول المحافظة على بيانات مستعملي خدماتهم وذلك تمهيدا لطلب السلطات منهم تلك البيانات التي قد تفيد كدليل في جريمة معيّنة وقعت بالفعل[1].

أمّا بالنسبة للقانون الأمريكي المعروف بقانون خصوصية الاتصالات الالكترونيّة (ECPA)، فقد أجاز لرجال الضبط القضائي في إطار ما يقومون به من جمع الاستدلالات الاطلاع على البيانات الموجودة في حوزة مزودي الخدمات والتي تخص مستخدمي شبكة الانترنت، وذلك من خلال توجيه تكليف إلى مزود الخدمات بتقديم تلك المعلومات، وتتمثل هذه الأخيرة في ثلاث طوائف هي[2]:

أولا ــ المعلومات الشخصية الخاصة بالمشترك مثل اسمه ورقم تلفونه وعنوانه.

ثانيا ــ المعلومات الشخصية الخاصة بالمتعامل مع المشترك (أي كل من يتّصل به أو يدخل معه في صفقة).

---

(1)- Art. 43-9. LOI n° 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication)
"Les prestataires mentionnés aux articles 43-7 et 43-8 sonttenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services don't ells sont prestataires".

(2) ــ شيماء عبد الغني، مرجع سابق، ص216.

ثالثا ــ المعلومات المتعلقة بمحتوى البيانات (مضمون المحادثات ــ مضمون الملفات).

المشرع الجزائري لم ينص على هذا الإجراء في قانون 04/09 السابق الذكر بل اكتفى بعملية حفظ المعطيات المتعلقة بحركة السير في إطار إلتزامات مقدمي الخدمات.

أما بالنسبة لاتفاقية بودابست فقد نصت في المادة 18 منها على "أنّه يجوز للدول الأطراف في تلك الاتفاقية تمكين السلطات المختصة من إلزام مقدمي الخدمات تقديم البيانات المتعلقة بالمشترك، سواء كانت في حيازته المادية أو تحت سيطرته" حيث تكون هذه البيانات مخزنة بعيدا عن الحيازة المادية لمزود الخدمة، ولكن يمكن السيطرة عليها، ومثال ذلك أن تكون البيانات مخزّنة في وحدة تخزين عن بعد ويتم تقديمها عن طريق شركة أخرى. ويشترط في هذه البيانات أن تكون مخزّنة، حيث يستثنى منها أية معلومات متعلقة بحركة ومحتوى البيانات ذات العلاقة باتصالات مستقبلية، لأنّها تكون محل دراسة الفرع الثاني من هذا المطلب والخاص بالإجراءات المتعلقة بالبيانات المتحركة[1].

حدّدت الاتفاقية المقصود بتلك البيانات بقولها أنها تتعلّق:

ــ بنوع خدمة الاتصال التي اشترك فيها الشخص والوسائل الفنية لتحقيقها.

ــ العنوان البريدي أو الجغرافي ورقم تلفون المشترك.

ــ رقم دخول المشترك للحصول على تلك الخدمة والفواتير التي ترسل إليه، وأي معلومات تتعلق بطريقة الدفع (مثل رقم بطاقة الائتمان أو حسابه البنكي)، أو أي معلومات أخرى تتعلق بأداء الخدمة أو بالاتفاق بين هذا المشترك ومزود الخدمة.

[1] ــ هلالي عبد اللاه، اتفاقية بودابست لمكافحة الجرائم المعلوماتية..، مرجع سابق، ص 223.

الفرع الثاني: الإجراءات المتعلقة بالبيانات المتحركة(اعتراض الإتصالات الإلكترونية)

استحدث المشرع الجزائري إجراء المراقبة الإلكترونية بموجب المادة الثالثة من القانون رقم (04/09) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلحة بتكنولوجيات الإعلام والإتصال ومكافحتها حينما أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها. وفيما يلي سنتناول مفهوم مراقبة الإتصالات الإلكترونية (أولا)، ثم عرض ضمانات هذه المراقبة الإلكترونية (ثانيا).

أولاـــ المقصود بمراقبة الإتصالات الإلكترونية:

لم يتطرّق المشرّع الجزائري إلى تحديد مفهوم مراقبة الإتّصالات الإلكترونيّة[1]، مكتفيا بذلك تحديد مفهوم الإتصالات الإلكترونية فحسب، حيث عرفها في المادة الثانية فقرة "و" من القانون رقم (04/09) السالف الذكر بأنها: " **أي تراسل أو إرسال أو استقبال علامات أو إشارات**

---

[1]ـــ تجدر الإشارة أن إتفاقية بودابست قد ميزت بين نوعين من البيانات المعلوماتيّة محلّ الاعتراض (المراقبة الإلكترونية)، بين **البيانات المتعلقة بالمرور** و**البيانات المتعلقة بمحتوى الاتصال**، وبالنسبة للنوع الأوّل فإنّ المادة الأولى(1) من الاتفاقيّة قد عرّفتها بأنّها" كل البيانات التي تعالج الاتصالات التي تمرّ عن طريق نظام معلوماتي، والتي يتمّ إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال، مع تعيين المعلومات التاليّة: أصل الاتصال، مقصد الاتصال أو الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ، حجم وفترة الاتصال، أو نوع الخدمة.

أمّا بالنسبة للنوع الثاني: **البيانات المتعلقة بمحتوى الاتصال** فإنّه لم يأت تعريف لها في الاتفاقيّة لكنّها تشير إلى المحتوى الإخباري للاتصال، بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

ويلاحظ ممّا سبق ذكره أنّ هناك نوع من التقارب بين هذين النوعين من البيانات، من حيث المعنى إلاّ أنهما مختلفين تماما من حيث درجة المساس بالحق في الخصوصيّة، حيث يكون ذلك أكثر أهميّة بالنسبة لمراقبة محتوى الاتصال أو المراسلة، ومن ثمّ تفرض ضمانات أكبر عند تجميع محتوى البيانات في الزمن الفعلي عن حركة البيانات سواء من حيث الجرائم التي من أجلها يتمّ توظيف هذا الإجراء، أو من حيث السلطة المختصة بإصدار أمر المراقبة.

وقد أكّدت اتفاقية بودابست هذا التمييز حيث أدرجت كل إجراء على حدا تحت عنوان خاص، فخصّت تجميع حركة البيانات بعنوان" **التجميع في الزمن الفعلي لبيانات المرور**"[1] (المادة 20)، أما تجميع محتوى البيانات فجاء تحت عنوان " **اعتراض محتوى البيانات**"[1] (المادة 21).

وعلى العكس من ذلك تضع بعض الدول مفهوما موحدا لكل من تجمع حركة البيانات ومراقبة محتوى البيانات ومن ثمّ يسري عليهما نفس الضمانات الخاصة عند اتخاذ احد الإجراءين، دون أخذ في الاعتبار إلى الحساسيّة التي تحيط بموضوع مراقبة محتوى البيانات. ويرجع السبب في ذلك إلى عدم وجود تمييز في القانون الذي لا يوجد فيه اختلافات حول المصلحة في الخصوصيّة أو لتشابه إجراءات التجميع التقني ومن هذه الدول فرنسا والجزائر.

أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية''، في حين عرّفها المشرّع الأمريكي في الباب الثالث من القانون الفدرالي الأمريكي لسنة 1968 بأنه: ''**الإكتساب السمعي أو أي إكتساب لمحتويات أية أسلاك أو أي إتصالات شفوية باستخدام أي جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر**''[1]. أما الفقه فقد عرفها بأنها '' مراقبة شبكة الإتصالات''، أو العمل الذي يقوم به المراقب (بكسر القاف) باستخدام التقية الإلكترونية لجمع بيانات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر[2].

الملاحظ أن التقنية المستخدمة في هذه المراقبة هي التقنية الإلكترونية، والتي تعني مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات الداخلة وفق برنامج موضوع مسبقا لتحديدهم من أجل ضبطهم وتفتيشهم وجمع الأدلة قبلهم لإثبات إدانتهم وتقديمهم إلى المحاكمة[3]، ومن بين تلك التقنيات نجد برنامج كارنيفور[4]وتقنية مراقبة البريد الإلكتروني[5].

من الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الالكتروني فقط، بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية، وهو ما قررته المادة الرابعة من القانون رقم (09/ 04) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتهاالمنوه عنه سابقا بنصها: ''**يمكن القيام بعمليات المراقبة الإلكترونية للإتصالات للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب**

---

(1) ــ شيماء عبد الغني، مرجع سابق، ص 305 وما بعدها.

(2) ــ مصطفى محمد مرسى، المراقبة الإلكترونية عبر شبكة الأنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، الطبعة الأولى ، دار الكتب والوثائق القومية المصرية، 2003، ص 192.

(3) ــ نفس المرجع، ص 205.

(4) ــ قامت إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفدرالي (FBI) بتطوير هذه التقنية، 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 الرسائل المار عبر خدماتها يحمل معلومات عن جرائم جنائية، ويتم تنفيذ عمليات التعقب والفحص بوضع أجهزة الشركة الموفرة للخدمة تحت المراقبة، ولقد أصبح يطلق على هذه التقنية بعد أحداث 2011/09/11 تقنية (C/ SC 1000). مصطفى محمد مرسي، مرجع سابق، ص 202.

(5) ــ هي برنامج صممه الأمريكي "**ريتشارد داتوني** " من أجل سير محتوى البريد الإلكتروني موضوع المراقبة وقراءة الرسائل التي قام صاحبها بإتلافها أو تلك التي لم يقم بتخزينها أساسا، وقد استخدمت أجهزة الإستخبارات الأمريكية هذا البرنامج لكشف مشتبه فيه من الجنسية الروسية حاول اختراق مواقع على شبكة الانترنت. مصطفى محمد مرسي، مرجع سابق، ص217.

أو الجرائم الماسة بأمن الدولة وكذا في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني".

ثانيا ـــ شروط المراقبة الإلكترونية للإتصالات:

باعتبار أن الأحاديث الشخصية والإتصالات الخاصة حرمة تستمد من حرمة الحياة الخاصة لصاحبها، فقد أحاط المشرع الجزائري إجراء المراقبة الإلكترونية للإتصالات مجموعة من الشروط أهمها:

ـــ أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء وبإذن منه، وهو ما كرسته المادة الرابعة (4) من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها بنصحها على أنه لا يجوز إجراء عمليات المراقلة إلا بإذن من السلطات القضائية المختصة.

ـــ أن تكون هناك ضرورة تتطلب هذا الإجراء وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية وهو ما أكده المشرع في الفقرة "ج" من المادة الرابعة في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السابق الذكر.

وعليه يتضح أن المعلوماتية بقدر ما أسعدت البشرية ويسرت لها سبل الحياة، وبرزت الحكومة الالكترونية كأهم تطبيق لها، إلا أنه قد أتعستها بارتكاب جرائم قد تمس ثقة المتعاملين معها، ما يترتب عليه إعاقة تقدم مشاريع الحكومة الالكترونية، مما تطلب الأمر تدخل تشريعي لمختلف الدول ومنها المشرع الجزائري، ليس فقط على مستوى تجريم أفعال الاعتداء الواقعة عليها، بل أيضا على المستوى الإجرائي، من خلال تخصيص ضبطية خاصة للبحث والتحري عن الجرائم المستحدثة الواقعة على الحكومة الالكترونية، وأيضا البحث عن الدليل المناسب لإثباتها، وهو الدليل الالكتروني.

نتيجة للطبيعة الفنية والعلمية للدليل الالكتروني، كان من الضروري اتباع إجراءات خاصة لاستخلاصه، وهي إجراءات تقليدية وأخرى مستحدتة.

بعد الحصول على الدليل الالكتروني، تأتي المرحلة التالية وهي مرحلة المحاكمة، والتي تكون محل دراسة الفصل الثاني.

الفصل الثاني: القواعد الخاصة بالمحاكمة في الجرائم الواقعة على الحكومة الالكترونية

تمثل المحاكمة المرحلة الأخيرة للدعوى العمومية، لذا تعرف باسم التحقيق النهائي، ويقصد بها مجموعة الإجراءات المتخذة بهدف تمحيص جميع أدلة الدعوى سواء كانت لمصلحة المتهم أو ضده، وذلك بهدف استقصاء الحقيقة الواقعية والقانونية المتعلقة بالدعوى، ومن تم الفصل فيها[1].

إلا أن الأحكام الإجرائية المتعلقة بمرحلة المحاكمة في الجرائم الواقعة على الحكومة الالكترونية قد تعتريها بعض الصعوبات، لاسيما مجال تحديد المحكمة المختصة بالفصل في هذه النوعية من الجرائم، والتي يترتب على أساسها تحديد القانون الواجب التطبيق، ولأن الجرائم المعلوماتية ذو طبيعة عالمية[2]، حيث تتجاوز آثارها الحدود الوطنية لتمس الجماعة الدولية، وأن خطورتها غير محصورة في النطاق الإقليمي لدولة بعينها، مما قد يتنازع فيه أكثر من دولة، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام أجهزة العدالة الجنائية المعنية بمكافحة الجريمة.

كما تثير هذه الجرائم مسألة سلطة المحكمة الجنائيّة في قبول وتقدير الدليل الإلكتروني، لاسيما وأن هذا الدليل ذو طبيعة خاصة، ويتطلب خطوات معقدة لتحصيله، لذا فإن قبوله في الإثبات قد يثير هو الآخر العديد من المشكلات، وذلك بخلاف الدليل في الجرائم التقليدية.

هذا ما سنحاول دراسته في هذا الفصل من خلال الاختصاص القضائي الجنائي لنظر الجرائم الواقعة على الحكومة الالكترونية (المبحث الأول)، وسلطة القاضي الجنائي في تقدير الدليل الالكتروني (المبحث الثاني).

---

[1] ــ مأمون سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الطبعة الثانية، دار الفكر العربي، القاهرة، ص 160.

[2] ــ هناك فرق بين الجريمة الدولية والجريمة العالمية، فالجريمة الدولية هي تصرف غير مشروع يعاقب عليه القانون الدولي بحسبان أنه يشكل اعتداء على العلاقات الانسانية في الجماعات الدولية، في حين أن الجريمة العالمية هي جرائم تمس النظام العام الداخلي للدول وتخضع لتجريم قانون العقوبات الوطني، ولا تثير مسؤولية دولية، وإنما يسأل عنها الفرد كأي جريمة عادية، ويثبت الإختصاص بالمحاكمة في شأنها للمحاكم الوطنية لا لمحاكم دولية، وعادة ما تأخذ صورة "الجرائم المنظمة"، كالمتاجرة بالمخدرات وجريمة الإرهاب وجريمة القرصنة المعلوماتية...إلخ. انظر: فتوح عبد الله الشاذلي، القانون الدولي الجنائي، الكتاب الأول: أوليات القانون الدواي الجنائي، دار المطبوعات الجامعية، الاسكندرية، 2001، ص 23 ــ 24.

المبحث الأول: الإختصاص القضائي لنظر الجرائم الواقعة على الحكومة الإلكترونية

إنّ الطبيعة الخاصة التي تتميز بها الجرائم التي تقع على نظام الحكومة الإلكترونية ومنها جرائم المعلوماتية لا تقف عند الطبيعة الخاصة بالأفعال التي تتحقّق بها الجرائم، وإنّما تمتدّ هذه الطبيعة لتشمل أيضا البعد العالمي لهذا النوع من الإجرام.

وعليه تعدّ الجريمة المعلوماتية تبعا لذلك شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية[1]، ولا شك في أن الطبيعة العالمية التي تتميز بها الجرائم التي تتصل بنظم المعالجة الآلية للمعطيات قد تثير مشكلات كثيرة تتعلق بتحديد جهة الإختصاص المحلي لهذه الجرائم، وبقواعد سريان القانون الوطني من حيث المكان[2].

هذا ما يطرح إشكاليّة حول موقف المشرع الجزائري من مسألة الإختصاص القضائي في مجال الجرائم الواقعة على الحكومة الالكترونية، فهل تطبق عليها نفس القواعد المطبقة على الجرائم التقليدية، أم استحدث قواعد خاصة تتلاءم وخصوصيّة هذه الجرائم؟

ذلك ما سنبينه في المطالب المتقدمة من هذا البحث، حيث يتضمّن الأوّل منه قواعد الإختصاص القضائي المطبقة على هذه الجرائم إذا ارتكبت في الحدود الوطنية لدولة الجزائر، أمّا إذا تجاوزت الجريمة الحدود الإقليمية للدولة فتمتد لتمسّ دول أخرى، وهو ما يكون محل دراسة المطلب الثاني.

المطلب الأول: الإختصاص القضائي الجنائي الوطني

يتحدّد الإختصاص المحلي للجهات القضائية بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم في دائرته القبض على هؤلاء الأشخاص، غير أنه نتيجة تطور الجريمة وظهور جرائم خطيرة، دفع المشرع الجزائري إلى تطور سبل مكافحة هذه

---

[1] ــ محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25ــ28 اكتوبر 1993، مرجع سابق، ص 360.

[2] ــ عمر الفاروق الحسيني، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25ــ28 اكتوبر 1993، مرجع سابق، ص 464.

الجرائم، عن طريق إدخال تعديلات على قانون الإجراءات الجزائية بالقانونين الأول رقم (04 ــ14) المؤرخ في 10 نوفمبر 2004، والثاني القانون رقم (06ــ348) المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، حيث وسع بموجبهما الإختصاص الإقليمي لكل من وكيل الجمهورية وقاضي التحقيق وبعض المحاكم[1] على النحو التالي:

الفرع الأول: الإختصاص الإقليمي الموسع لوكيل الجمهورية وقاضي التحقيق

سنبيّن فيما يلي القواعد العامة التي تحكم الاختصاص الاقليمي لوكيل الجمهورية وقاضي التحقيق كأصل عام، ثم التغيرات التي أدخلها المشرع الجزائري عليهما من حيث الاختصاص المكاني وذلك بموجب التعديلات التي أدخاها المشرع الجزائري على قانون الإجراءا الجزائية الجزائري، وذلك فيما يلي:

أولا ــ الإختصاص الإقليمي الموسع لوكيل الجمهورية:

كقاعدة عامة يتحدد الإختصاص المحلي لوكيل الجمهورية في الجرائم العادية طبقا للمادة 2/37 من ق.إ.ج.ج بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر.

غير أن المشرع الجزائري وسع الإختصاص المحلي لوكيل الجمهورية بموجب التعديل الذي أدخله على قانون الإجراءات الجزائية قانون رقم (04ــ 14) طبقا للفقرة الثانية من المادة 37 منه،

[1] ــ قام المشرع الجزائري بإدخال بعض التعديلات على المرسوم التنفيذي رقم رقم(06ــ348) المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، وذلك موجب مرسوم تنفيذي رقم (16 ــ 267) المؤرخ في 17 أكتوبر من سنة 2016، ولكن هذا التعديل مس ثلاث مواد فقط المادة 3و4و5 من المرسوم التنفيذي رقم 06 ــ 348 السابق الذكر، وهي مواد تتعلق بالولايات التي يمتدإليها الاختصاص المحلي لمحكمة قسنطينة، ووهران وورقلة، دون المساس بالأحكام الأخرى. مرسوم تنفيذي رقم (16 ــ 267) مؤرخ في 15 محرم عام 1338، الموافق لــ 17 أكتوبر من سنة 2016، يعدل ويتمم المرسوم التنفيذي رقم 06ــ348 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج، عدد 62، الصادر في 23 أكتوبر 2016.

ليشمل اختصاص محاكم أخرى تحدد عن طريق التنظيم[1]، وهذا كلما تعلق البحث والتحري والمتابعة في جرائم محددة على سبيل الحصر، ومنها الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات[2].

هذا ما يتعلق بالإطار القانوني المحدّد لتوسيع الإختصاص لوكيل الجمهورية.

أمّا فيما يخص طرق إخطار المحكمة ذات الإختصاص الموسع بالملف، فقد أوجبت المادة 40 مكرر 1 من ق.إ.ج.ج على ضابط الشرطة القضائية الإبلاغ الفوري لوكيل الجمهورية لدى المحكمة التي ارتكبت في دائرة اختصاصها الجريمة ـــ ومنها الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات[3] ـــ وموافاته بأصل ونسختين من إجراءات البحث والتحري في هذه الجريمة، والذي يقوم بدوره بإرسال النسخة الثانية من هذه الإجراءات بصفة فورية إلى النائب العام لدى المجلس القضائي الذي يتبع له القطب الجزائي المتخصص.

إذا اعتبر النائب العام لدى المجلس القضائي أن الجريمة تدخل ضمن اختصاصه، يطالب طبقا للمادة 40 مكرر 2 بالإجراءات كاملة فورا[4].

كما يجوز للنائب العام لدى المجلس القضائي التابعة له الجهة القضائية المختصة، أن يطالب بالإجراءات في جميع مراحل الدعوى[5].

---

[1] ـــ وهو المرسوم التنفيذي رقم (06ـــ348) بتضمن **تمديد الاختصاص المحلي لبعض المحاكم، ووكلاء الجمهورية وقضاة التحقيق**، السابق الذكر.

[2] ـــ تنص المادة 2/37 من ق.إ.ج.ج ما يلي: " يجوز تمديد الإختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطياتوجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

[3] ـــ يلاحظ من نص المادة 40 مكرر ق.إ.ج أن المشرع الجزائري حدد مجموعة من الجرائم التي بموجبها يوسع الإختصاص لوكيل الجمهورية منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات في القسم السابع مكرر من المواد 394 مكرر إلى 394 مكرر7، وفي مقابل ذلك عرف المشرع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في القانون رقم (09ـــ04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بقوله: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية"، وبالتالي مفهوم الجرائم المعلوماتية كان أوسع في الثاني بخلاف التحديد الأول الوارد في قانون العقوبات، ولذلك كان على المشرع في نص المادة 40 مكرر ق.إ.ج أن يستعمل مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال عوض جريمة المساس بأنظنة المعالجة الآلية للمعطيات وذلك لاستعاب جرائم معلوماتية أخرى غير المنصوص عليها في قانون العقوبات موازاة مع التطور الحاصل في مجال المعلوماتية والإتصال.

[4] ـــ راجع المادتين 40 مكرر 1 و40 مكرر 2 من القانون رقم (04ـــ14) المعدل والمتم لقانون الإجراءات الجزائية الجزائري.

[5] ـــ راجع المادة 40 مكرر 3 من القانون رقم (04ـــ 14) المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

ثانيا ــ الإختصاص الإقليمي الموسع لقاضي التحقيق:

لقد وُرد في المادة 40 /2 من ق.إ.ج المعدل بالقانون 14/04 توسيع الإختصاص الإقليمي لقاضي التحقيق لدى القطب الجزائي المتخصص، ليمتدّ اختصاصه لمحاكم إقليمية أخرى محدّدة بموجب المرسوم التنفيذي رقم(06ــ348) المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، وذلك في إطار مكافحة الجرائم المحددة في المادة 2/40 من ق.إ.ج ج[1].

بذلك ألزمه بعض الأحكام الخاصة، كلما تعلق الأمر بالجرائم المنوه عنها سابقا، ومنها الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات، ولذلك أنه طبقا للمادة 40 مكرر 2/3 من ق.إ.ج.ج، يصدر قاضي التحقيق العادي في حالة فتح تحقيق قضائي بصدد تلك الجرائم، أمر بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى القطب الجزائي المتخصص، وفي هذه الحالة يصبح ضباط الشرطة القضائية العاملون بدائرة اختصاص المحكمة التي وقعت بدائرتها الجريمة يتلقون التعليمات مباشرة من قاضي التحقيق لدى القطب الجزائي المتخصص[2].

كما نصّت المادة 40 مكرّر 4 من ق.إ.ج.ج، على أنه يحتفظ الأمر بالقبض، أو الأمر بالحبس المؤقت الذي صدر ضد المتهم بقوة تنفيذية، إلى أن تفصل فيه محكمة القطب الجزائي المتخصص مع مراعاة أحكام المادة 123 وما يليها من هذا القانون.

أيضا نصت المادة 40 مكرّر5 من ق.إ.ج.ج، أنه يجوز لقاضي التحقيق لدى القطب الجزائي المتخصص، تلقائيا أو بناء على طلب النيابة العامة، وطوال مدة الإجراءات أن يأمر باتخاذ كل إجراء تحفظي أو تدبير أمن، زيادة على حجز الأموال المتحصل عليها من الجريمة، أو التي استعملت في ارتكابها.

---

[1] ــ علالي بن زيان، معيار الإختصاص في الجرائم المعلوماتية على ضوء التشريع الإجرائي الجزائري، مداخلة مقدمة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المركز الجامعي أحمد زبانة، غليزان، بتاريخ 07 ــ08 فبراير 2017، ص 8.

[2] ــ جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الطبعة الثانية، الجزائر، 2013، ص 74.

الفرع الثاني: الإختصاص الإقليمي الموسع للأقطاب الجزائية المتخصصة

يقصد بالأقطاب الجزائية المتخصصة تركيز إختصاصات إقليمية لجهات قضائية متفرقة على عديد المناطق في يد جهة قضائية واحدة، شريطة أن يتعلق الأمر بتشكيلة من الإختصاصات النوعية المحددة على سبيل الحصر[1]، وكانت البداية الحقيقية والرسمية لظهور هذه الأقطاب[2] سنة 2004، في إطار إختصاص إقليمي موسع، من خلال تعديل قانون الإجراءات الجزائية بموجب القانون رقم (04ـــ 14) المؤرخ في 10 نوفمبر 2004 حيث وسع المشرع الجزائري الإختصاص المحلي لكل من وكيل الجمهورية، قاضي التحقيق والمحكمة إلى دائرة اختصاص محاكم أخرى تحدد عن طريق التنظيم، كلما تعلق الأمر بمتابعة جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

في هذا الإطار صدر المرسوم التنفيذي رقم (06ـــ348) المؤرخ في 05 أكتوبر 2006، حيث تمّ بموجبه تحديد أربعة محاكم على المستوى الوطني وتوسيع اختصاصها الإقليمي ليشمل دوائر اختصاص محاكم أخرى موزعة على جهات الوطن الأربع، شرقا، وسطا، غربا وجنوبا[3]، وفي سنة 2016 أدخل المشرع الجزائري بعض التعديلات على هذا المرسوم، وكان ذلك بالمرسوم التنفيذي رقم (16 ـــ 267) المؤرخ في 17 أكتوبر سنة 2016، هذا التعديل مسّ ثلاث مواد الثالثة، الرابعة والخامسة وهي المواد المعنية بتمديد الاختصاص المحلي للمحاكم التالية قسنطينة، ورقلة ووهران، مع الابقاء على القطب الجزائي لسيدي امحمد بالعاصمة دون تعديل، وهذا كما يلي:

1ـــ القطب الجزائي لسيدي امحمد بالعاصمة:

طبقا للمادة الثانية من المرسوم التنفيذي رقم (06ـــ 348) ، يمتد الإختصاص الإقليمي لهذا القطب ليشمل محاكم تقع في دائرة اختصاص مجالس قضائية لكل من الجزائر، شلف، الأغواط،

---

[1] ـــ محمد بكراروش، مرجع سابق، ص305.

[2] ـــ إنّ لفظ "قطب" أو "أقطاب متخصصة " ظهر رسميا لآول مرة ضمن نصوص قانون الإجراءات المدنية والإدارية الصادر سنة 2008، بالرغم من أن المحاولة الأولى كانت في سنة 2005 عند تقديم مشروع القانون العضوي المتعلق بالتنظيم القضائي. الذي لم يحض بقبول المجلس الدستوري، وذلك من خلال المادة 24 منه. انظر: رأي المجلس الدستوري رقم 01/ر.ق.ع/م.ع/ 05 مؤرخ في 10 جمادى الأولى عام 1426 الموافق 17 يونيو سنة 2005، المتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي للدستور.

[3] ـــ محمد بكراروش، مرجع سابق، ص 316.

البويرة، تيزي وزو، الجلفة، المدية ، المسيلة، بومرداس، تيبازة، عين الدفلى، البليدة، وهي تشمل اثنا عشر مجلسا قضائيا، تشمل إداريا ولايات تقع جغرافيا في وسط شمال الجزائر.

2 ــ القطب الجزائي المتخصّص لقسنطينة:

يمتدّ الإختصاص المحلي لهذا القطب وفقا للمادة الثانية من المرسوم التنفيدي رقم (16ــ267)[1]، ليشمل محاكم المجالس القضائية التالية: قسنطينة وأم البواقي وباتنة وبجاية وتبسة وجيجل وسطيف وسكيكدة وعنابة وقالة وبرج بوعريريج والطارف وخنشلة وسوق أهراس وميلة.

3 ــ القطب الجزائي المتخصّص لورقلة:

طبقا لنص المادة الثانية من المرسوم التنفيدي (16ــ 276)[2]، يمتد الإختصاص الإقليمي لهذا القطب إلى محاكم المجالس القضائية لــ: ورقلة وأدرار وتامنغست وإيليزي وبسكرة والوادي وغرداية.

4 ــ القطب الجزائي المتخصّص لوهران:

يمتدّ الإختصاص الإقليمي لهذا القطب حسب المادة الثانية من المرسوم التنفيدي (16ــ276) المنوه عنه سابقا، إلى محاكم المجالس القضائية التالية: وهران، بشار، وتلمسان وتيارت، تندوف،سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، وتيسيمسيلت، النعامة، عين تموشنت وغليزان.[3]

تجدر الإشارة أن المشرع الجزائري قد نصّ في نفس المرسوم السابق الذكر على أحكام أخرى تتعلق بعمل هذه الأقطاب من ذلك مانصت عليه المادة السادسة منه على أنه يختص رئيس المجلس

---

[1] ــ في المرسوم التنفيدي القديم رقم (06ــ 348) كان الإختصاص الإقليمي لهذا القطب يمتد وفقا للمادة الثالثة ليشمل اختصاص محاكم تابعة للمجالس القضائية التالية: قسنطينة، أم البواقي، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، باتنة، سوق أهراس، ميلة، الطارف، الوادي.

[2]- أضيفت الولايتين بسكرة والوادي إلى القطب الجزائي المتخصص لوررقلة بعد إن كانتا تابعتان إلى القطب الجزائي المتخصص لقسنطينة، أما تندوف فأصبحت من اختصاص القطب الجزائي المتخصص لوهران.

[3] ــ في إطار المرسوم التنفيذي رقم 06ــ 348 السابق الذكر، كان الاختصاص المحلي لمحكمة وهران ووكيل الجمهورية وقاضي التحقي في المادة الالخامسة منه يمتد إلى محاكم المجالس القضائية التالية:وهران، بشار، وتيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، وتيسيمسيلت، النعامة، عين تموشنت وغليزان.

القضائي الذي تقع في دائرة اختصاصه المحكمة التي تم تمديد اختصاصها للفصل بموجب أمر في الإشكاليات التي يثيرها تطبيق أحكام المرسوم، على أن يكون هذا الأمر نهائي غير قابل لأي طعن[1].

المطلب الثاني: الإختصاص القضائي الجنائي الدولي

سبق الإشارة أنّ الجرائم المعلوماتية قد تتعدّى الحدود الوطنية للدولة، وأن الحدود الجغرافية فقدت كل أثر لها في بيئة إلكترونية متشعبة العلاقات، يتجاوز فيها السلوك الإجرامي المكان بمعناه التقليدي، مما يخلق صعوبة في تحديد الدولة صاحب الإختصاص القضائي بنظر هذه الجرائم.

بناء على ما سبق سنتطرق في هذا المطلب لضوابط الإختصاص القضائي من بيان قواعد تحديد القانون الواجب التطبيق في الفرع الأول، وإشكالية الإختصاص القضائي من حيث الجدل الفقهي الثائر في هذا المجال مع تحديد موقف المشرع الجزائري منه.

الفرع الأول: ضوابط الإختصاص القضائي

إنّ قواعد القانون الجنائي بشقيه (الموضوعي والإجرائي) تعدّ مظهرا من مظاهر سيادة الدولة لذلك فإن تطبيقها من حيث المكان يخضع لمبدأ مستقر ألا **وهو مبدأ الإقليمية،** الذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها ولا تخضع لسلطان أي قانون أجنبي، وفي المقابل فلا مجال لأن يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقا لحدودها المعترف بها، حيث يصطدم بسيادة غيرها من الدول، إلا في أحوال إستثنائية تقتضيها حماية المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام[2] .

الأصل أنّ عناصر الركن المادي للجريمة تكتمل في نطاق إقليم دولة واحدة، حيث يقع السلوك الإجرامي وتترتب عليه آثاره في إقليم دولة واحدة، هذا ما يتعلق بالجريمة الفورية حيث لا تثير

---

[1] ــ بن كثير بن عيسى، الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاء، العدد63، مديرية الدراسات القانونية والوثائق، وزارة العدل، الجزائر، 2008، ص 82.

[2] ــ عدنان الخطيب، موجز القانون الجزائي، الكتاب الأول، المبادئ العامة في قانون العقوبات، مطبعة جامعة دمشق، 1963، ص 79.

مشكلات قانونية من حيث تحديد مكان وقوع الجريمة غير أن بعض الجرائم كالجريمة المتتابعة يتجاوز مداها أحيانا حدود الدولة، حينما ينجزأ ركنها المادي أو يتوزع على أكثر من مكان، بحيث يمكن وقوع السلوك في إقليم دولة بينما تتحقق النتيجة للجريمة في إقليم دولة أخرى، ويتجلى ذلك في عدد من الجرائم ذات الطبيعة العابرة للحدود الوطنية كالجريمة المعلوماتية مثلا وهو ما سنعالجه بالتفصيل في الفرع الثاني.

وعليه إذا وقعت الجريمة كلّها أو في جزء منها على إقليم الجزائر فإن الأثر المترتب على ذلك يتمثل في سريان نصوص القوانين الجنائية الجزائرية وفي اختصاص القضاء الجزائري بمحاكمة المتهم بتلك الجريمة، هذا ما نصت عليه المادة الثالثة من قانون العقوبات التي أكدت على أنه: "يطبق قانون العقوبات الجزائري على كافة الجرائم التي ترتكب في أراضي الجمهورية"، كما نصت المادة 586 من قانون الإجراءات الجزائية أنه "تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها قد تم في الجزائر".

بالإضافة إلى **مبدأ الإقليمية** فإن القانون الواجب التطبيق يمكن أن يتحدد أيضا وفقا لمعايير أخرى كمبدا الشخصية أو مبدأ العينية أو مبدأ العالمية وغالبا ما تأخذ بها التشريعات الجنائية كمبادئ مكملة لمبدأ الإقليمية.

المقصود **بمبدأ الشخصية** هو تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكب الجريمة خارج إقليمها[1]، فيخضع حسب هذا المبدأ لقانون بلاده أينما وجد. والمشرع الجزائري أخذ بهذا المبدأ من خلال نص المادة 582 من قانون الإجراءات الجزائية التي نصت على أن كل واقعة موصوفة بأنها جناية معاقب عليها في القانون الجزائري ارتكبها جزائري خارج إقليم الجمهورية يجوز أن يتابع ويحاكم في الجزائر.

أمّا **مبدأ العينيّة** فيقصد به تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة والمرتكبة خارج إقليمها أيّا كانت جنسية مرتكبها[2].

---

[1] ــ جلال ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة، الاسكندرية، 2003، ص 317.

[2] ــ عبد الله سليمان، شرح قانون العقوبات، (القسم العام)، الجزء الأول: الجريمة، دار الهدى للطباعة والنشر والتوزيع، 2003، ص 89 ــ90.

وقد اعتمد المشرع الجزائري هذا المبدأ في المادة 588 من قانون الإجراءات الجزائية والتي تنص على أن كل أجنبي ارتكب خارج الإقليم الجزائري بصفته فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية... تجوز متابعته ومحاكمته وفقا للقانون الجزائري إذا ألقي عليه القبض في الجزائر أو حصلت الدولة على تسليمه لها.

في حين أنّ **مبدأ العالمية** هو أن تختص الدولة بتطبيق قانونها الجزائي على أجنبي ارتكب جريمة في الخارج وتم توقيفه أو إلقاء القبض عليه بأراضيها. والمشرّع الجزائري لم يأخذ به منبها في ذلك خطة معظم التشريعات العقابية مقتصرا على المبادئ السالفة الذكر[1]

الفرع الثاني: إشكالية الإختصاص القضائي المعلوماتي

يتحدّد السريان المكاني للقانون الجنائي والجهة المختصة طبقا للمبادئ المشار إليها في الفرع الأول، وهو أمر لا يخلو من صعوبات بالنظر لخصوصية الجريمة المعلوماتية باعتبارها جريمة عابرة للحدود، إن كان ارتكابها فقط تم داخل النطاق الإقليمي لدولة معينة، وكانت آثارها محصورة في حدوده، الأمر الذي لا يثير أي خلاف في اختصاص المحاكم الجزائرية مكانيا طبقا لأحكام المادة الثالثة من قانون العقوبات الجزائري، والإستثناءات الواردة عليه.

غير أن الصعوبة تكمن في الحالات التي يتوزع فيها السلوك المادي للجريمة في أكثر من دولة كأن يقع السلوك الإجرامي في دولة، في حين تتحقق النتيجة الإجرامية في دولة أخرى، ويكون بالتالي قانون كل دولة تحقق فيها أحد عناصر الركن المادي للجريمة قابلا للتطبيق، مما يؤدي إلى تنازع إيجابي في الإختصاص بين أكثر من تشريع وطني، وبين أكثر من دولة لملاحقة نفس النشاط الإجرامي[2]، فمثلا في حالة تعطيل نظام معلوماتي عن طريق إدخال فيروس مما يؤدي إلى إفساد النظام وعدم تشغيله، فيرتكت الفعل المادي في بلد ونظام الضحية في دولة أخرى بعد أن تمر في كثير من الأحيان بأكثر من دولة قبل وصولها إلى بلد الإستقبال، ومثل هذه الظاهرة تفرض تنازعا في الإختصاص،

[1] ـــ علي عبد الله سليمان، شرح قانون العقوبات الجزائري: الجريمة، ديوان المطبوعات الجامعية، 2002، ص 115.

[2] - سليمان أحمد فاضل، المواجهة التشريعية والأمنية...، مرجع سابق، ص 234.

وبالتالي هل يمكن أن تخضع الجرائم الواقعة على الحكومة الإلكنرونية ومنها الجريمة المعلوماتية للمبادئ القانونية السالفة الذكر التي تحكم القانون الواجب التطبيق وتحديد جهة الإختصاص المكاني؟

هذا ما نجم عنه خلاف فقهي حول تحديد القانون الواجب التطبيق ومن تم تحديد المحكمة لمحاكمة مرتكبيها دون غيرها من المحاكم، وهو ما سنوضحه في التالي، في حين حسم هذا الخلاف الفقهي التدخل التشريعي للعديد من الدول مع بيان موقف المشرع الجزائري فيما يتعلق بالمحاكم المختصة للنظر في هذه الجرائم المرتكبة خارج التراب الوطني.

أولا ــ موقف الفقه من تنازع الإختصاص الجنائي المعلوماتي:

حاول الفقه إيجاد حل لمشكلة التنازع الإيجابي للإختصاص القضائي في الجرائم المعلوماتية، وانقسم في ذلك إلى ثلاث إتجاهات: مذهب النشاط الإجرامي، مذهب تحقق النتيجة، والمذهب المختلط على النحو التالي:

1 ــ مذهب السلوك أو النشاط الإجرامي:

يستند هذا الرأي على المكان الذي وقع فيه السلوك واعتبره مكان وقوع الجريمة وذلك بصرف النظر على المكان الذي تحققت فيه النتيجة، أو من المفترض تحققها فيه، ومن المبررات التي يمكن إعتمادها أساسا للأخذ به أنه يسهل عملية الإثبات وجمع أدلة الجريمة، كما أن المحكمة المختصة للنظر في الدعوى تكون قريبة من مسرح الجريمة وتسهل بالتالي عملية البحث والتحري، والحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة[1].

2 ــ مذهب مكان تحقق النتيجة:

يرى أصحاب هذ الاتجاه أن المكان الذي تحققت فيه النتيجة أو كان من المفترض تحققها هو الضابط لتحديد مكان وقوع الجريمة والقانون الواجب التطبيق والجهة المختصة بنظرها، لكنه لم يسلم بدوره من النقد بداعي أن اعتماده يؤدي إلى عدم تجريم الشروع إذا لم تتحقق النتيجة وعدم العقاب على ما يعرف بجرائم السلوك[2].

---

[1] ــ نور الدين الواهلي، الإختصاص في الجريمة الالكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص 137.

[2] ــ موسى مسعود ارحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، دراسة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون المنظم بأكادمية الدراسات العليا، طرابلس، خلال الفترة 28 ــ 29/ 10/ 2009 منشور بتاريخ 2016 /07/22 على الرابط التالي: com.aiefpedi تاريخ الاطلاع:2017/04/12.

3 ــ المذهب المختلط:

أمام الانتقادات التي طالت كلا المعيارين السابقين، ظهر معيار ثالث يذهب إلى أن الجريمة تعتبر واقعة في مكان حصول النشاط وأيضا في مكان تحقق النتيجة أو الذي من المنتظر أن تتحقق فيه، ووفقا لهذا المعيار فالإختصاص ينعقد لمحاكم الدولة التي وقع فيها التنفيذ المادي للجريمة وأيضا لمحاكم الدولة التي تحققت فيها آثار الجريمة، وللتغلب على مشكل تنازع الإختصاصيتم تغليب قانون محل تحقق النتيجة الإجرامية إذا كانت الجريمة تامة، وتغليب قانون محل مكان تحقق النشاط أو السلوك إذا وقعت الجريمة عند حدود الشروع أو كانت من قبيل جرائم السلوك المجرد.

لذلك نرى من الضروري إيراد نص خاص يحدد معيار الإختصاص القضائي لمحاكمة الجرائم المعلوماتية لاسيما التي تقع بطريق الانترنت، هذه الشبكة التي لا تخضع لرقابة أو سيطرة دولة معينة ولا يوجد قانون جنائي يحكمها، بل على العكس تتعد القوانين التي تطبق عليها بتعدد الدول المرتبطة بها، أين تكمن المشكلة هنا، حيث تختلف التشريعات المقارنة في تكييف الفعل بين الاباحة والتجريم في كل دولة، فما يعد مخلا بالحياء في بعض الدول الإسلامية، يعد مباحا في دول أخرى، الأمر الذي يدعو إلى ضرورة تدويل الجرائم المرتكبة عليها.

ثانيا: موقف التشريعات المقارنة من إشكالية الاختصاص القضائي المعلوماتي

تنوعت خطة التشريعات المقارنة في تحديد المحكمة المختصة بالفصل في الجرائم المعلوماتية، حيث تبنت البعض منها تطبيق مبدأ العالمية، في حين مددت دول أخرى قواعد الاختصاص، وفيما يلي بيان ذلك:

الموقف الأول: وهو تطبيق مبدأ العالمية في تحديد إختصاص القضاء الوطني مثل بلجيكا، وهو ما نصت عليه المادة الرابعة من قانون العقوبات البلجيكي، وكرسته أيضا المادة 12 مكرر من قانون التحقيقات الجنائي البلجيكي[1]، حيث تختص المحاكم الوطنية لمحاكمة مرتكبي بعض الجرائم ذات

[1]- Article 12bis du Titre préliminaire du Code d'instruction criminelle : « Hormis les cas visés aux articles 6 à 11, les juridictions belges sont également compétentes pour connaître des infractions commises hors du territoire du Royaume et visées par une règle de droit international conventionnelle ou coutumière ou une règle de droit dérivé de l'Union européenne liant la Belgique, lorsque cette règle lui impose, de quelque manière que ce soit, de soumettre l'affaire à ses autorités compétentes pour l'exercice des poursuites » .

الطبيعة الدولية مثل جرائم المخدرات والارهاب والقرصنة والجرائم الجنسية الواقعة على الأطفال، ومنها ما يتم بالوسائل الالكترونية، بالرغم من وقوعها خارج إقليم الدولة وأن المتهمين ليس من مواطني تلك الدولة.

يلقى مبدأ العالمية تطبيقه أيضا في بعض الجرائم المنصوص عليها في قانون العقوبات لدولة الإمارات العربية المتحدة، وهو ما نصت عليه المادة 21 منه، وتتمثل هذه الجرائم في:

ـــ جريمة تخريب أو تعطيل وسائل الإتصال الدولية، ويقصد بذلك عادة جرائم خطف الطائرات. ـــ جريمة الإتجار بالمخدرات. ـــ جريمة الاتجار بالرقيق الأبيض (النساء). ـــ جريمة الاتجار بالصغار أو الرقيق. ـــ جرائم القرصنة. ـــ جرائم الإرهاب الدولي.

أما الحل الثاني: يتمثل في امتداد قواعد الاختصاص، أي باختصاص القانون الإقليمي (أي باختصاص القضاء الوطني) على الجرائم المعلوماتية، وطبقه القانون الفرنسي في المادة 113 ـــ6 إلى غاية الفقرة 13 من نفس المادة، حيث فرق المشرع الفرنسي بفي قانون العقوبات بين الجرائم التي ترتكب داخل فرنسا أين ينعقد الاختصاص للقضاء الفرنسي، وبين الجرائم التي تقع خارجها ويختص فيها أيضا القضاء الفرنسي، وذلك في حالة اتصال ظروف الواقعة المرتكبة ما يجعل لفرنسا مصلحة في تطبيق القانون الفرنسي، والملاحظ أن المشرع الفرنسي حاول توسيع نطاق تطبيق المادة 113ـــ2 من قانون العقوبات (المجسدة لمبدأ الإقليمية) لتشمل جرائم ترتكب خارج إقليم الجمهورية الفرنسية.

تطبيقا لذلك قضت المحكمة الابتدائية بباريس باختصاص المحاكم الفرنسية، وبالتالي تطبيق القانون الفرنسي إذا كان مركز البث موجودا في خارج الإقليم الفرنسي. وبناء عليه إذا كان الجهاز الخادم موجودا في أمريكا بينما تظهر الرسائل التي يقوم ببثها هذا الجهاز في فرنسا، فإن المحاكم الفرنسية ينعقد لها الاختصاص[1].

---

(1) -Cass,13 non 1998, Dalloz, 1999,p 106.

مشار إليه عند: شيماء عبد الغني، مرجع سابق، ص 371.

تعد الولايات المتحدة الأمريكية أيضا من التشريعات التي تعطي الإختصاص لمحاكمها الجنائية إذا حدثث آثار الجريمة على إقليمها، فقد استندت على مبدأ الإختصاص بالنتيجة كمعيار للإختصاص الوطني[1].

تم تطبيق مبدأ النتيجة في قضية (مينيسوتا ضد جرانتي جات ريسورت)، بشأن بث ألعاب القمار عبر الانترنت من لاس فيغاس بولاية نيفادا، والذي وصل إلى ولاية (مينيسوتا) التي يحظر قانونها مثل هذه الألعاب، وتكرس هذا الاتجاه القضائي فيما انتهت إليه الدائرة الخامسة الاستئنافية في قضية قمار ومراهنات عبر الانترنت[2].

وتجدر الإشارة أن هذا المبدأ لا ينطبق على جميع المحاكم الأمريكية، بل يختلف من ولاية إلى أخرى، فولاية فرجينيا مثلا تأخد بمكان البث كمعيار للإختصاص الوطني، لذلك رفضت ـــ محام فرجينياـــ اختصاصها بنظر دعوى قذف وُردت عبارات القذف فيها في جريدة صغيرة تظهر في ولاية "كونيتيكت" على الرغم من أنه قد تم وضعها على شبكة الانترنت[3].

أما المشرع الإنجليزي فقد حدد اختصاص القضاء الانجليزي بالجريمة المعلوماتية بمقتضى المادة الخامسة من قانون إساءة استخدام الحاسوب المؤرخ في 1990، حتى ولو لم يحدث الفعل المجرم على الإقليم الإنجليزي أو توادج المتهم على هذا الإقليم، وإنما يكفي أن يكون هناك ارتباط وثيق بين الجريمة وبين الإقليم الانجليزي[4].

---

[1] ـــ يتضمن مبدأ النتيجة الإجرامية في القانون الأمريكي: الأثر الإمتدادي للنتيجة الإجرامية، إذا كانت نتيجة إجرامية قد بدأت وانتهت في إقليم معن، إلا أن نتيجتها الإجرامية كأحد عناصر الركن المادي امتدث إلى إقليم آخر. هذا ما يبرر سلوك الدولة في متابعة المتهم. ومن أولى= ==القضايا التي طبقت فيها هذا المبدأ في الجرائم المرتكبة عبر الانترنت، هي قضية الولايات المتحدة الأمريكية ..ضد أل توماس. لمزيد من التفاصيل حول هذه القضية. انظر: عمر بن يونس، مرجع سابق، ص 908.

[2] ـــ حيث قررت الدائرة الخامسة الاستئنافية " أنه على الرغم من عرض ألعاب القمار قد تم من خلال مكاتب في الكاريبي إلا أن قبول القمار والمراهنة قد تم في الولايات المتحدة، ومن تم تنطبق القوانين الأمريكية". انظر:عمر بن يونس، مرجع سابق، ص 910.

[3] ـــ شيماء عبد الغني، مرجع سابق، ص 375.

[4] ـــ ويقصد هنا بالارتباط الوثيق (أو العلاقة القوية) بين الجريمة وبين الإقليم الانجليزي أن يتواجد المتهم الذي نفذ الجريمة المعلوماتية في إقليم الدولة مادام أنه قد قام باستعمال جهاز الكمبيوتر في انجلترا، كما يؤول الاختصاص للقضاء الانجليزي إذا كا الجهاز الذي دخل عليه المتهم بدون وجه حق متواجدا في الإقليم الانجليزي (أي النتيجة امتدت إلى بيريطانيا).نفس المرجع، ص 379.

ثالثا: موقف المشرع الجزائري

لا يثار أي إشكال بخصوص مسألة الإختصاص عندما ترتكب الجرائم الواقعة على الحكومة الإلكترونية ومنها جرائم المساس بأنظمة المعالجة الآلية لمعطيات الحكومة داخل الإقليم الوطني، وإنما تبرز الصعوبة عندما ترتكب هذه الجرائم خارج التراب الوطني من قبل أشخاص أجانب، بمعنى يكون لها إمتداد خارجي أو دولي[1].

في هذه الحالة تدخل المشرع الجزائري فعلا وحسم هذه الإشكالية ـــ الإختصاص القضائي الجنائي المعلوماتي ـــ من خلال نص المادة 15 من القانون رقم 09/ 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث نصت المادة 15 منه على أنه "فضلا عن الإختصاص المنصوص عليه في قانون الإجراءات الجزائية، فإن المحاكم الجزائرية تكون مختصة أيضا بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني".

وعليه نستنتج أنّ الإختصاص القضائي المعلوماتي ينعقد للمحاكم الجزائرية للفصل في الجرائم التي لها صلة بتكنولوجيا الإعلام والإتصال والتي يكون مرتكبوها شخصا أجنبيا أو خارج أرض الوطن، عندما يكون غرضها مستهدفا مؤسسات الدولة الجزائرية وهيئات الدفاع الوطني والمصالح الإستراتيجية للإقتصاد الوطني.

هذا بالإضافة إلى المساعدة القضائية الدولية المتبادلة المنصوص عليها في المادة 16 من القانون (09ـــ04) المنوه عنه سابقا، فإن المشرع الجزائري أوكل مهمة تبادل المعلومات التي من شأنها جمع المعطيات التي تفيد في التعرف على مرتكب هذه الجريمة، إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، حيث حول لهذه الأخيرة العمل مع نظيرتها في الخارج على تسيير السبل لسير التحريات بقصد الوصول إلى مرتكب الجرائم والتعرف على أماكن تواجدهم، ومن تم

[1] ـــ علالي بن زيان، مرجع سابق، ص 10.

تسهيل متابعتهم وجلبهم إلى المثول أمام المحاكم الجزائرية في إطار الإتفاقيات والمساعدة القضائية الدولية، ومبدأ المعاملة بالمثل[1].

ما تجدر الإشارة إليه أنّ نص المادة 15 السابق الذكر ما هو إلا تكرار لقاعدة الإختصاص العيني المنصوص عليها بالمادة 588 من قانون الإجراءات الجزائية وليس بالإضافة الجديدة إلى قواعد الإختصاص مثلما استهل به نص المادة 15 من القانون 09/ 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال السابق الذكر.

إن الجرائم المعلوماتية العابرة للوطنية تستعصي في كثير من الأحيان على الخضوع للقوالب القانونية التي تحكم مسألة الإختصاص المكاني، ومن ثمة فإن الطبيعة الخاصة لهذه الجرائم تتطلب تجاوز المعايير التقليدية بخصوص مسألة تنازع الإختصاص والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها وآلية اقترافها والتخلص من آثارها وغيرها من خصوصيات يفرضها الطابع التقني.

المبحث الثاني: القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجزائي

نظرا للطبيعة الخاصة للجرائم الواقعة على الحكومة الإلكترونية فإن دليل إثباتها يختلف ويتميز عن الدليل التقليدي، فالدليل الإلكتروني يعيش في بيئة متطورة بطبيعتها وتشمل على أنواعا متعددة من البيانات الرقمية التي تصلح مجتمعة أو منفردة لكي تكون دليلا للبراءة أو للإدانة، وبالتالي يعتبر الدليل الإلكتروني الوسيلة الوحيدة والرئيسية في الإثبات الجنائي للجرائم المعلوماتية[2].

إلا أنّ مجرد وجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يكف للتعويل عليه، إذ يلزم أن تكون لهذه الأدلة قيمة قانونية، فما مدى حجية الدليل الإلكتروني في الإثبات الجنائي؟

الإجابة على هذا الإشكال تكون من خلال البحث عن:

---

[1] ــ يوسف قجاج، الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون، العدد 28 لشهر فيفيري 2015، ص 190.

[2]- Eoghan Cassy,op. cit, p.5.

ـــ سلطة القاضي الجنائي في قبول الدليل الالكتروني وذلك في المطلب الأول، وفيه نتناول أساس قبول الدليل الالكتروني في الإثبات الجنائي(الفرع الأوّل)، تمّ القيود التي ترد على حريّة القاضي الجنائي في قبول الدليل الالكتروني(الفرع الثاني).

ـــ أمّا في المطلب الثاني سنخصصه لسلطة القاضي الجنائي في تقدير الدليل الالكتروني، وذلك من خلال فرعين يتمثل الأول في الطبيعة العلمية للدليل الإلكتروني وأثرها على اقتناع القاضي الجزائي أمّا الفرع الثاني سيكون مخصص لموقف المشرع الجزائري من الدليل الإلكتروني في الإثبات الجنائي.

المطلب الأول: سلطة القاضي الجزائي في قبول الدليل الإلكتروني

يعدّ قبول الدليل الخطوة الإجرائيّة الأوليّة التّي يمارسها القاضي تجاه الدليل الجنائي بصفة عامة والدليل الالكتروني بصفة خاصة، وذلك قبل البدء في تقديره، للتأكد من مدى صلاحيته، وملائمته لتحقيق ما قدم من أجله، وقبول القاضي الجنائي الدليل الالكتروني في الإثبات لابدّ وأن يستند على أساس، وهذا الأخير يختلف من نظام إلى آخر سواء كان نظام لاتيني أو نظام أنجلوسكسوني.

وبهذا فالقاضي الجنائي يهدف في هذه المرحلة إلى التيقن من مدى مراعاة الدليل الجنائي أساسا للضوابط التي لا يمكن بدونها أن يترتب على الدليل أي آثار قانونيّة.

على ضوء ما سبق بيانه سنتناول هذا المطلب في الفرعين التاليين:

الأوّل يتضمن أساس قبول الدليل الالكتروني في الإثبات الجنائي، أما الثاني يتضمن ضوابط قبول الدليل الإلكتروني في الإثبات الجنائي.

الفرع الأول: أساس قبول الدليل الإلكتروني في الإثبات الجزائي

الواقع أنّ موقف القوانين المقارنة فيما يتعلّق بسلطة القاضي الجنائي في قبول الدليل الالكتروني تخضع إلى طبيعة نظام الإثبات السائد في الدولة، وتنقسم هذه النظم إلى ثلاث فئات:

الفئة الأولى: تتبنى مبدأ حريّة الإثبات، و منها سلطة القاضي في قبول جميع الأدلة، وهنا تكون جميع طرق الإثبات مقبولة، مالم يستبعد المشرّع بعضها صراحة، كاستبعاد المراسلات بين المتهم

ومحاميه مثلا، وينتمي إلى هذه الفئة القانون الفرنسي المادة (427) من قانون الإجراءات الجنائيّة والقانون الجزائري، المادة(212) من قانون الإجراءات الجنائيّة والقانون المصري (291) من قانون الإجراءات الجنائيّة .

الثانية: وتأخذ بنظام الأدلة القانونيّة، حيث تحدّد الأدلة التي يجوز للقاضي الجنائي قبولها، كالقانون الهولندي(المادة 339) من قانون الإجراءات الجنائيّة والقانون الألماني الذي يحدّد على سبيل الحصر وسائل الإثبات التي يتعيّن على القاضي قبولها[1]، وإن كان التطبيق العملي لهذين القانونين يتّجه نحو نظام حريّة الإثبات[2].

أما الفئة الثالثة والأخيرة: وهي القوانين الأنجلوسكسونيّة، حيث تقيّد من حريّة الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة، أمّا في مرحلة تحديد العقوبة فيسود مبدأ حريّة الإثبات[3].

وعلى ذلك، سنحاول من خلال التالي أن نبيّن موقف النظم القانونيّة من الدليل الالكتروني كدليل إثبات، ومن البديهي أن يكون هذا الموقف مبنيّا على أساس قانوني لقبول هذا النوع المستحدث من الأدلة.

أولاـــ في النظام اللاتيني:

لم تفرد التشريعات المنتميّة إلى العائلة ذات الأصل اللاتيني مثل فرنسا[4]، وغيرها من الدول المتأثرة بها كالجزائر و مصر، نصوصا خاصّة فيما يتعلق بقبول الدليل الالكتروني، وذلك على أساس

---

(1)ـــ وهذه الوسائل هي: سماع أوسؤال المتهم(der Angeklagte)، وشهادة الشهود(die Zeugen)، وتقارير الخبراء die (Schachverstandigen)، الانتقال للمعاينة (der Augenschein)، والمستندات (die Urkunden).

(2) -Pradel, la preuve en procédure pénale comparé, rapport général, in, revus international de droit pénal, 1992, p. 18.

(3)ـــ أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائيّة المقارنة، الطبعة الثانيّة، دار النهضة العربيّة، القاهرة، 2006، ص14.

(4) ـــ أقرّ المشرع الفرنسي صراحة مبدأ حرية الإثبات الجنائي في المادة (427) من قانون الإجراءات الجنائية الفرنسي حيث تنص: "ما لم يرد نص مختلف، يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخصي".

أنّ هذه الدول تستند لمبدأ حريّة الإثبات في المسائل الجنائيّة[1]، هذا المبدأ الذي يمثل لُبّ نظام الإثبات الحر[2]، حيث أصبح هذا الأخير القانون العام في الإجراءات الجزائيّة في التشريعات اللاتينيّة، وبمقتضاه يحكم القاضي في الدعوى حسب العقيدة التي تكوّنت لديه بكامل حريّته، و تتمثل خصائص هذا النظام في عدم تحديد الأدلّة ، بمعنى أنّ الخصوم لهم الحريّة في الالتجاء إلى أيّ دليل يمكنه ممن إثبات ادعائهم، كما أنّ هذا النظام يخوّل القاضي سلطة تقييم الأدلة دون أن يفرض عليه قيدا أو شرطا، فالقاضي حرّ في أن يستعين بكل طرق الإثبات للبحث عن الحقيقة، وهو حرّ في وزن و تقدير كل دليل، و في التنسيق بين الأدلة التي تتمثل في الحكم بالإدانة أو البراءة[3].

انطلاقا مما سبق ذكره يتّضح لنا مبدئيّا أنّه يجوز للقاضي الجنائي الاستناد إلى الدليل الالكتروني لإثبات الفعل الجنائي في سائر الجرائم والجرائم المعلوماتية على وجه الخصوص. وهو ما سوف نبيّنه بالتفصيل في التالي، من خلال دراسة أساس قبول هذا النوع المستحدث من الدليل في التشريعات ذات الأصل اللاتيني، ثمّ نبينّ أهم النتائج المترتبة على الأخذ بهذا الأساس.

1 ــ مبدأ حريّة الإثبات الجنائي كأساس لقبول الدليل الالكتروني:

تعتبر حريّة الإثبات في المسائل الجنائيّة من المبادئ المستقرّة في نظريّة الإثبات الجنائي، وذلك بخلاف المسائل المدنيّة حيث يحدّد القانون سلفا وسائل الإثبات وقواعد قبولها وقوّتها. ويقصد بهذا المبدأ: حريّة جميع الأطراف في اللجوء إلى كافة وسائل الإثبات للتدليل على صحّة ما يدّعونه،

---

[1] ــ أقر المشرع الجزائري مبدأ حرية الإثبات الجنائي في المادة (212) من قانون الإجراءات الجزائية الجزائري حيث نصت على أنه: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لإقتناعه الشخصي"، أما المشرع المصري فقد أخذ هو الآخر بمبدأ حرية الإثبات من خلال المادة (291) من قانون الإجراءات الجنائية المصري حيث تنص على أن :" للمحكمة أن تأمر ولو من تلقاء نفسها أثناء مظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة".

[2] ــ يطلق عليه البعض نظام (الأدلة الأدبيّة) ، أمّا البعض الآخر يطلق عليه نظام (الأدلة الاقناعيّة) ، أو نظام (الاقتناع الشخصي أو الذاتي) (Système de l'intime conviction de juge)، وهناك من يسميه (حرية القاضي الجنائي في الاستسلام لنداء ضميره). لمزيد من التفصيل حول هذا النظام: انظر: احمد فتحي سرور. أصول الإجراءات الجنائيّة، دار النهضة العربية، القاهرة، 1969، ص 343. وانظر كذلك: مفيدة سويدان، نظرية الاقتناع الذاتي للقاضي الجنائي، دكتوراه في الحقوق، جامعة القاهرة، 1985، ص 109. محمود نجيب حسني، مرجع سابق، ص 421.

[3] ــ عائشة بن قارة مصطفى، مرجع سابق، ص 183.

فلسلطة الاتهام أن تلجأ إلى أيّة وسيلة لإثبات وقوع الجريمة على المتّهم، ويدفع المتّهم كذلك بكل الوسائل، ويستظهر القاضي الحقيقة بكلّ ذلك أو بغيره من طرق الإثبات[1]. إذن فجميع الأدلة متساوية لا تفاضل بينها إلا بمقدار ما تحدثه من أثر في نفس القاضي من ارتياح واطمئنان[2].

وقد استقرّ مبدأ حريّة الإثبات الجنائي منذ القديم على الرغم من أنّ " تقنين التحقيقات الجنائيّة الفرنسي" لم يكرّسه صراحة، وإنّما أشير إليه في بعض النصوص، خاصّة التعليمة المقرّرة للمحلفين لدى محكمة الجنايات[3].

في الوقت الحالي، فإنّ قانون الإجراءات الجنائيّة الفرنسي قد أقرّ مبدأ حريّة الإثبات الجنائي صراحة بمقتضى المادة(427) منه حيث تنص: " ما لم يرد نص مخالف، يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخصي" [4]، وهذا النص وإن كان مخصّصا لمحاكم الجنح، إلاّ أنّ مبدأ حريّة الإثبات يطبق أمام جميع أنواع المحاكم الجنائيّة، إلاّ إذا نصّ القانون على خلاف ذلك[5]. وتأييدا لذلك تفرض محكمة النقض الفرنسيّة على محاكم الموضوع تطبيقا صارما لهذا المبدأ بحيث تفرض في النهاية حريّة كاملة للإثبات، فهي تشدّد في العديد من أحكامها على حريّة قضاة الموضوع في الاستعانة بأي دليل يكون لازما لتكوين عقيدتهم، وأنّ الفقرة (2 من المادة 427) تطبق على وسائل الدفاع[6]، بيد أنّ الدائرة الجنائيّة

---

(1)ـــ أحمد ضياء الدين محمد خليل، مرجع سابق، ص 240.

(2)ـــ يجب التمييز بين مبدأ حريّة الإثبات وحريّة القاضي في الاقتناع، وعدم الخلط بينهما، حيث يقصد بالأوّل الطريق الإثباتي المرسوم لكل أطراف الدعوى بما فيهم القاضي في اختيار وسائل الإثبات الملائمة للواقعة محل الإثبات، بينما يتعلّق الثاني بنطاق سلطة القاضي في تقدير وتقييم الدليل، بحيث يمثّل المبدأ الثاني الأساس الذي يسيطر على آخر مرحلة من مراحل تقدير الدليل الجنائي منذ نشأته حتى تحقيق غايته. انظر: أحمد ضياء الدين محمد خليل، مشروعيّة الدليل في المواد الجنائيّة، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعيّة في مجال الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة عين شمس، 1982 ص 248 .

(3)ـــ المادة 342 من قانون التحقيقات الجنائيّة الفرنسي (Code d'instruction francais).

(4) Article 427 du (C.P.P) , dispose que :" Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction".

(5) Merle et Vitu, op. cit, p. 165.

(6)Cass;Crim 12avril 1995, B, n° 156. Cass;Crim 15 juin 1993, B, n° 210, Cass ;Crim 25 septembre 1987, B, n° 316 .

لمحكمة النقض الفرنسيّة ذهبت أكثر من ذلك في احترام مبدأ حريّة الإثبات، فهي ترى أنّه طالما لا يوجد نص قانوني يستبعد صراحة دليلا ما فلا يجوز للمحكمة عدم قبول هذا الدليل ولو كان ذلك الدليل غير مشروع بل لو كان عدم المشروعيّة ناتجة عن ارتكاب جريمة [1]، غير أنّها تشترط فحسب أن يكون هذا الدليل قد خضع للمناقشة الحضوريّة في الجلسة أي احترام حقوق الدفاع.

كذلك أقرّ المشرع الجزائري مبدأ حريّة الإثبات الجنائي في المادة(212) من قانون الإجراءات الجزائيّة الجزائري حيث نصّت على أنّه: " يجوز إثبات الجرائم بأيّ طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي"[2].

نفس الشيء كرّسته المادة (291) من قانون الإجراءات الجنائيّة المصري حيث تنص على أنّ "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى، بتقديم أيّ دليل تراه لازما لظهور الحقيقة"، وقد أكّدت محكمة النقض المصريّة [3] هذا المبدأ في العديد من أحكامها، بقولها" أنّ القانون ـــ فيما عدا ما إستلزمه من وسائل خاصة للإثبات ـــ فتح بابه أمام القاضي الجنائي على مصراعيه

---

(1) -Cass;Crim 15 juin 1993, B, n° 210. Cass;Crim 6avril 1993, J.C.P, édition générale, n° 43, note Mme Rassat, p. 415.

(2) ـــ من الملاحظ أنّ المشرّع الجزائري أدرج نص المادة(212) من قانون الإجراءات الجزائيّة الجزائري ضمن الأحكام المشتركة والمتعلقة بطرق الإثبات أمام جهات الحكم مما لا يدع أيّ شك في تطبيقها أمام كل الجهات القضائيّة الجزائيّة، في حين أنّ المشرع الفرنسي أورد نص المادة(427) قانون الإجراءات الفرنسيّة التي تقابل المادة(212) جزائري، ضمن أحكام الجنح، ممّا أثار جدلا فقهيّا حول تطبيقه أمام الجهات الأخرى إلاّ أنّ الكثير من الفقهاء يعتبرون أنّ حكم المادة(427) هو حكم عام، انظر في هذا الشأن:

G. Lauvasseur, La juridiction correctionnelle depuis l'application du code de procédure pénal, revus du science criminelle,1959, p. 577.

(3) ـــ تجدر الإشارة أنّ المحاكم المصريّة كانت قد استقرّت ـــ قبل صدور قانون الإجراءات الجنائيّة الحالي (رقم 150 لسنة 1950) الصادر في سنة 1950 ـــ على تطبيق مبدأ حريّة الإثبات، واستقرّت على أنّ للقاضي الجنائي حريّة الاستعانة بكافة وسائل الإثبات لتكوين اقتناعه حول حقيقة الوقائع المرفوعة عنها الدعوى. انظر على سبيل المثال: نقض 12 يونيه سنة 1939 ، مجموعة القواعد القانونيّة، الجزء الرابع، رقم 406، ص 575. نقض 11 يناير سنة 1943، مجموعة القواعد القانونيّة، الجزء السادس، رقم 68، ص 64.

يختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة ويزن قوّة الإثبات المستمدّة من كل عنصر[1].

2 ــ النتائج المترتبة على تطبيق مبدأ حريّة الإثبات الجنائي:

على ضوء ما تقدّم، فإنّ إعمال مبدأ حرية الإثبات يجعل القاضي الجنائي يتمتّع بدور إيجابي في توفير وقبول وتقدير الدليل الجنائي بما في ذلك الدليل الالكتروني.

وسوف نتناول من خلال التالي، دور القاضي الجنائي في توفير وقبول الدليل الالكتروني أمّا مسألة التقدير نتركها للمطلب الثاني والخاص بسلطة القاضي الجنائي في تقدير الدليل الالكتروني.

أ ــ الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني:

يؤدي القاضي الجنائي دورا هاما، بل لعله أكثر الأدوار أهميّة في الدعوى الجنائيّة، وبصفة خاصة في شأن عمليّة الإثبات، و لم يكن منح القاضي الجنائي هذا الدور سوى أحد مظاهر اعتناق المشرّع لمبدأ حريّة الإثبات، وحتّى يتّضح لنا هذا الدور المهم للقاضي الجنائي يتعيّن لنا أن نقوم بتحديد مفهوم هذا الدور بداية، ثم نعرض لأهم مظاهر الدور الايجابي للقاضي الجنائي.

1ــ مفهوم الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني: يقصد به عدم التزام القاضي بما يقدّمه له أطراف الدعوى من أدلة، وإنّما له سلطة بل وواجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعليّة فيها[2]، ذلك أنّ الحقيقة لا تظهر من تلقاء نفسها، وإنّما في حاجة دوما إلى من يبحث وينقب عنها، وليس له أن يقنع بما يقدمه إليه أطراف الدعوى وإنّما عليه أن يبحث بنفسه عن الأدلة اللازمة لتكوين عقيدته على الوجه الصحيح لأنّه يسعى إلى اكتشاف الحقيقة الموضوعيّة أي الحقيقة في كل نطاقها[3].

---

[1] ــ نقض 25 يناير 1965، مجموعة أحكام محكمة النقض، س 16 رقم 21، ص 87. نقض 20 يناير 1969، س 20 رقم 35، ص 164. وانظر كذلك: نقض 24 أبريل 1978، س 29 رقم 84 ، ص 442. وانظر أيضا: 25 نوفمبر 1984، س 29 رقم 185، ص 821.

[2] ــ محمود محمد مصطفى، شرح قانون الإجراءات الجنائيّة، مطبعة دار النشر الثقافة، الطبعة الثانية القاهرة، 1953، ص 360.

[3] ــ محمود نجيب حسني، مرجع سابق، ص 78.

وفي ذلك يختلف دور القاضي الجنائي عن دور القاضي المدني، فإذا كان عمل هذا الأخير مجرّد قبول الأدلة المقدمة من الخصوم في الدعوى، فليس له أن يبادر من تلقاء نفسه إلى البحث عن أيّ دليل أو تقديمه وأن يوجّه أحد الأطراف إلى تقديم دليل بعينه، بينما القاضي الجنائي لا يتخذ هذا الدور السلبي[1]، فمن حقّه بل من واجبه أن يتحرّى ويبحث عن الحقيقة بجميع الوسائل، سواء نصّ عليها القانون أم لم ينص عليها كالدليل الالكتروني مثلا، وقد أكّدت هذا المعنى المادة(212) من قانون الإجراءات الجزائيّة الجزائري والمادة 291من قانون الإجراءات الجنائيّة المصري[2].

2 ــ مظاهر الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني: إذا كانت مهمّة البحث عن الأدلة وتقديمها في مرحلة المحاكمة تقع بصفة أساسيّة على عاتق الإدعاء والدفاع، فلا يعني ذلك أنّ القضاة لا يتحمّلون جانبا من هذه المسؤوليّة. بل يلقى عليهم عبء الإثبات شأنهم في ذلك شأن سلطة الاتهام، وللاستدلال على ذلك نلاحظ أنّ المحاكم الفرنسيّة في مواد الجنح والمخالفات يمكنها أن تتخذ جميع الإجراءات الضروريّة لتكوين اقتناعها[3]، فلها أن تسأل أو تستجوب المتهم حول أساس الاتهام الموجه إليه(المادتان 442 و536) من قانون الإجراءات الجنائيّة الفرنسي، ويمكنها سماع الشهود أو استدعاء الخبراء إذا واجهتها مسألة فنيّة.

أمّا في مواد الجنايات فقد أفرد القانون الإجرائي الفرنسي نصّا خاصّا منح بموجبه رئيس محكمة الجنايات سلطة تقديريّة خاصّة للقيام بجميع الإجراءات التي يقدّر فائدتها في كشف الحقيقة (المادة 310) من قانون الإجراءات الجنائيّة الفرنسي.

---

[1] ــ وتكمن العلّة في الفرق بين دور كل من القاضي الجنائي والقاضي المدني في البحث عن الأدلة، إلى اختلاف طبيعة المصالح التي تحميها كل من الدعوى الجنائيّة والدعوى المدنيّة، فالأولى تحمي مصلحة عامة هي مصلحة المجتمع، أمّا الدعوى المدنيّة فإنّها تحمي مصالح خاصّة بأطرافها. انظر: محمد زكي أبو عامر، الإجراءات الجنائيّة، دار الجامعة الجديدة، الطبعة الثانية، الاسكندرية، 2002، ص 851.

[2] ــ وفي ذلك قضت محكمة النقض المصريّة " أنّ القانون قد أمدّ القاضي في المسائل الجنائيّة بسلطة واسعة وحريّة كاملة في سبيل تقصي تبوث الجرائم أو عدم تبوثها والوقوف على حقيقة علاقة المتهمين ومقدار اتصالهم بها ففتح له باب الإثبات على مصراعيه يختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة ويزن قوّة الإثبات المستمدّة من كل عنصر بمحض وجدانه فيأخذ بما تطمئن إليه عقيدته ويطرح ما لا ترتاح إليه غير ملزم بأن يسترشد في قضائه بقرائن معيّنة بل له مطلق الحريّة في تقدير ما يعرض عليه منها ووزن قوّته التدليلية في كل حالة حسبما يستفاد من وقائع كل دعوى وظروفها، بغيته الحقيقة التي ينشدها إن وجدها ومن أي سبيل يجده مؤديا إليها ولا رقيب عليه في ذلك غير ضميره وحده. نقض 12 يونيه 1936، مجموعة القواعد القانونيّة، الجزء الرابع، رقم 406، ص 575. نقض 20 يناير 1969، مجموعة أحكام النقض، س 20، رقم 35، ص 164.

[3] ــ السيد محمّد حسن شريف، النظريّة العامة للإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 2002، ص 213.

لا يختلف الوضع في ذلك عن القانون المصري، فقد نصّت المادة 291 من قانون الإجراءات الجنائيّة على أنه "للمحكمة أن تأمر، ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة"، ولهذا أجيز للمحكمة أن توجه إلى الشهود أيّ سؤال ترى لزومه لظهور الحقيقة في أيّة حالة كانت عليها الدعوى[1]، وسمح لها أن تسمع شهادة أيّ شخص يحضر من تلقاء نفسه لتقديم ما لديه من معلومات في شان الدعوى المعروضة[2]. وأن تأمر ولو من تلقاء نفسها بإعلان الخبراء ليقدموا إيضاحات بالجلسة عن التقارير المقدّمة منهم في التحقيق الابتدائي أو أمام المحكمة[3].

تطبيقا لذلك فالقاضي الجنائي أن يوجه أمرا إلى مزود خدمة الانترنت بتقديم بيانات معلوماتيّة المتعلّقة بمستخدم الانترنت، كعناوين المواقع التي زارها ووقت الزيارة والصفحات التي اطلع عليها والملفات التي جلبها والحوارات التي شارك فيها والرسائل الالكترونيّة التي أرسلها أو استقبلها وغيرها من المعلومات المتعلقة بكل أفعال المستخدم عندما يتّصل بالشبكة[4].

من مظاهر الدور الايجابي للقاضي الجنائي في البحث عن الدليل الالكتروني، أنّه بإمكان القاضي الجنائي أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح عن كلمات المرور السريّة والشفرات الخاصة بتشغيل البرامج المختلفة، أو تكليفه بحل رموز لبيانات مشفّرة داخل ذاكرة الحاسب الآلي، كذلك للقاضي الجنائي سلطة الأمر بتفتيش نظم الحاسب الآلي بمكوناته الماديّة والمعنويّة وشبكات الاتصال متى ما قدّر ضرورة وملائمة هذا الإجراء.

ب ــ الدور الايجابي للقاضي الجنائي في قبول الدليل الالكتروني:

تحدّثنا فيما سبق عن الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني، من حيث ماهيته ومظاهره، وتبيّن كيف أنّ القاضي الجنائي على خلاف القاضي المدني، حيث لا يجوز له أن

(1) ــ المادة 273 من قانون الإجراءات الجنائيّة المصري.

(2) ــ المادة 277 من قانون الإجراءات الجنائيّة المصري.

(3) ــ المادة 293 من قانون الإجراءات الجنائيّة المصري.

(4) ــ عائشة بن قارة مصطفى، مرجع سابق، ص 193.

يقنع بما يقدمه له الأطراف في الدعوى من أدلّة، وإنّما عليه أن يبحث بنفسه عن الأدلّة ذات الأثر في تكوين عقيدته، وأن يستثير الأطراف إلى تقديم ما لديهم من أدلّة، وتعدّ مرحلة قبول الدليل الالكتروني الخطوة الثانيّة بعد البحث عن الدليل وتقديمه من قبل كلّ من سلطة الادعاء والمتهم والقاضي في حالة ما إذا تطلب أنّ الفصل في الدعوى يتطلب تحقيق دليل بعينه، وذلك من أجل خلق حالة اليقين المطلوبة لدى القاضي كأساس لإصدار حكمه بالإدانة أو لتأكيد حالة البراءة[1].

ثانيا ــ في النظام الأنجلو أمريكي:

نظام الإثبات في التشريعات ذات الأصل الأنجلوأمريكي يختلف عن غيره من التشريعات التي تأخذ بالنظام اللاتيني، فالدليل في النظام الأوّل تحكمه قواعد خاصة لقبوله أمام المحاكم، سواء تعلّقت هذه القواعد بمضمون أو فحوى الأدلة، أو بكيفيّة تقديم الأدلة.

فمن القواعد المتعلقة بمضمون الأدلة:قاعدة استبعاد **شهادة السماع(The Hearsay Rule)**[2]، وهي قاعدة متعلقة بمضمون الدليل، ومادام الدليل الالكتروني في أصله يمثّل شهادة سماع على أساس أنّه يتكوّن من جمل وكلمات أدخلها شخص إلى جهاز الكمبيوتر، سواء تمّ معالجة تلك البيانات أو لم يتمّ ذلك[3].

ومن شأن ذلك أن يثير اعتراضا على قبول المستندات المطبوعة التي يخرجها الحاسوب في الإثبات أمام القضاء الجنائي.

أمّا بالنسبة للقواعد المتعلقة بكيفيّة تقديم الأدلة إلى القضاء، وتحديد مدى قبولها، كأدلة إثبات في المواد الجنائيّة، تلك القاعدة المعروفة **بقاعدة الدليل الأفضل (The Best Evidence Rule)، أو قاعدة المحرّر الأصلي(Original Document Rule)**، ولو طبّقنا هذه القاعدة من حيث المبدأ على الدليل الالكتروني لكان مستبعدا كوسيلة إثبات في هذا النظام. وهو ما أدّى إلى قلق رجال

---

(1) ــ عائشة بن قارة مصطفى، مرجع سابق، ص 195.

(2) - Thomas J. Gardner, TerryM. Anderson, Criminal Evidence, Principles and cases, (5) fifth edition, Thompson Wadsworth Publisher, 2004, p.140.

(3) ــ شيماء عبد الغني، مرجع سابق، ص 404.

الضبط القضائي والمدّعيين العموميين من أنّ مجرّد مخرجات طابعة ملف الكتروني مخزّن على الحاسوب لا يعدّ أصليّا[1].

الإشكال الذي ينبغي طرحه في هذا المقام هو: **ما موقع الدليل الالكتروني من هذه القواعد، فهل يتمّ رفضه ومن تمّ استبعاده كدليل إثبات جنائي، أم يتمّ قبوله، وعلى أيّ أساس يكون هذا القبول؟.** ذلك ما سنحاول بيانه فيما يلي:

1 ــ الدليل الالكتروني مقبول استثناء من قاعدة استبعاد شهادة السماع:

الشهادة قد تكون عن رؤية (حضوريّة)، وقد تكون شهادة سماعيّة[2] يشهد فيها الشاهد بما سمعه ممّن رأى الواقعة، والحقيقة أنّ بعض التشريعات كالولايات المتحدة الأمريكيّة و انجلترا وكندا واستراليا لا تعتدّ بالشهادة السماعيّة في الإثبات الجنائي. وبما أنّ الدليل الالكتروني يعدّ شهادة سماع[3]، فيظهر من أوّل وهلة أنّه دليل غير مقبول، إلا أنّه في الحقيقة غير ذلك، لأنّ المشرع في الأنظمة الأنجلوأمريكية وضع قائمة من الاستثناءات على قاعدة شهادة السماع ومن بينها البيانات والمعلومات التي يتمّ الحصول عليها من الكمبيوتر(Evidence from Computer) أو (Computer Printouts)، حيث يكون هذا الأخير مقبولا في الإثبات شأنه شأن غير من الأدلة[4].

---

[1] ــ عمر محمّد بن يونس، الإجراءات الجنائيّة عبر الانترنت في القانون الأمريكي، مرجع سابق، ص 440.

[2] ــ يقصد بشهادة السماع أو كما يطلق عليها البعض التسامع عن الغير أو الشهادة النقليّة وبالإنجليزيّة، "Hearsay" ، بيان أو تقرير شفوي أو كتابي يحدث خارج المحكمة، ويقدم إليها من أجل الحقيقة وبعبارة أخرى من أجل إثبات أمر حدث خارج الجلسة وكان صادقا. انظر: رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة، دار المهضة العربية، الطبعة الأولى، 2010، ص 33.

[3] ــ انظر فيما سيأتي، ص294 .

[4] ــ وتجدر الإشارة إلى أنّ قبول الدليل الالكتروني على أساس استثناء قاعدة شهادة السماع لا ينطبق على جميع أنواع سجلات الحاسوب، ذلك أنّه سبق ذكرنّ هذه الأخيرة تمّ تقسيمها من قبل المحاكم الفدراليّة الأمريكيّة إلى ثلاث أنواع، **سجلات الحاسوب المخزنة(Computer-stored records)، وسجلات الحاسوب المتوالدة (Computer-generate records)**، وهناك نوع ثالث من السجلات يجمع **بين التدخل الإنساني ومعالجة الكمبيوتر.**

ففي النوع الأوّل، حيث تحتوي سجلات الحاسوب المخزّنة على بيانات بشريّة، مثل المخرجات من برنامج الكتابة من الكمبيوتر(Word). فهي تعتبر شهادة سماعيّة مثلها في ذلك مثل الكلماتأو التقريرات التي يسجّلها الإنسان على الأجهزة المختلفة.

وتجدر الإشارة أن القضاء الانجليزي يناقض أساس قبول الدليل الالكتروني في الاثبات الجنائي، حيث وإن كان المشرع الانجليزي يقبله في الاثبات الجنائي على أساس أنّه استثناء شهادة السماع، إلاّ أنّ القضاء قد قبل هذا الدليل على أساس أنّه شهادة مباشرة، ويظهر ذلك جليّا في العديد من القضايا المعروضة أمامها، ففي قضيّة (R.v.Wood)[1] تمّ العثور في حيازة المتّهم على بعض المعادن التي قد سرقت وكانت تركيبة المادة الكيميائيّة لهذه المعادن مسجّلة في كمبيوتر المجني عليه، وقد قدّمت ورقة مخرجة من الكمبيوتر كدليل، والسؤال الذي طرح في هذه القضيّة هل تعتبر هذه الورقة الناتجة عن الكمبيوتر دليلا سماعيّا، وبالتالي لا نأخذ به؟ ـــ أجابت عن ذلك المحكمة معتبرة أنّ الورقة الناتجة عن الكمبيوتر مقبولة وفقا للشريعة العامة، وتصلح للإثبات فهي ليست من قبيل الشهادة السماعيّة. كما قبلت المحكمة الجزئيّة في قضيّة (Castle v. Cross)[2] الدليل المستخرج من جهاز قياس نسبة الكحول في الدم باعتباره دليلا مباشرا وليس من قبيل الشهادة السماعيّة.

في نفس الاتجاه أيضا قضت محكمة الاستئناف في انجلترا بقبول الدليل المستخرج من الكمبيوتر في قضيّة (R.v.Pettigrew)[3] بوصفه شهادة مباشرة وليست سماعيّة والتي تخلص وقائعها في أنّه وجد في حيازة المتّهم الذي قام بالسطو على البنك أرقام النقود المسروقة والتي كانت مسجّلة في كمبيوتر البنك في انجلترا، وقد قبلت المحكمة في هذه القضيّة مخرجات الكمبيوتر الورقيّة باعتبارها دليلا مباشرا وليس من الأدلة السماعيّة.

أمّا النوع الثاني، فإنّ الجهاز هو الذي يقوم بتدوين البيانات التي تصلح أن تقدّم مباشرة إلى المحكمة، فهي ليست من قبيل شهادة السماع، وتتوقف قيمته الثبوتيّه على ما إذا كان جهاز الكمبيوتر يعمل بطريقة أم لا.

أمّا بالنسبة للنوع الثالث، والذي يجمع بين التدخل الإنساني ومعالجة الكمبيوتر، وإن كان جزء منها يعد شهادة السماع وهو الصادر عن الإنسان إلا أنه لا يعدّ هذا النوع من السجلات شهادة سماع، حتّى وإن كان يجب توافر لصحّة المستند الالكتروني شرطين: فمن ناحية يجب توافر الشرط اللازم لصحة الشهادة السماعيّة، كما أنّه يجب التأكد من عمل الجهاز نفسه على نحو صحيح. عمر بن يونس، مرجع سابق، ص 437 وما بعدها. وانظر أيضا: شيماء عبد الغني، مرجع سابق، ص 403.

(1) -R.v.Wood, 1983, 76 Cr. App. R 23, Steve Uglow, evidence, text and materials, London, Sweet and Maxwell, 1997, p. 514

مشار إليه عند: شيماء عبد الغني, مرجع سابق, ص 391.

(2) -Castle v. Cross, 1985, 1 All E.R,87 SteveUglow, ibidem, p.515.

(3) -وقائع هذه القضيّة مستمدّة من: SteveUglow, op. cit, p. 514

2 ــ الدليل الالكتروني مقبول استثناء من قاعدة الدليل الأفضل:

تذهب قواعد الإثبات في التشريعات ذات الأصل الأنجلوأمريكي إلى تطبيق قاعدة الدليل الأفضل والتي يقصدها: لأجل إثبات محتويات كتابة أو سجل أو صورة، فإنّ أصل الكتابة أو السجل أو الصورة يكون مطلوبا[1].

هذا يعني لا يجوز تقديم الصورة لإثبات محتوى الأصل[2].

القانون الأمريكي أقر هذه القاعدة بموجب المادة (1002) من قانون الإثبات الأمريكي و التي تقضي على أنّ حجيّة الكتابة أو التسجيل أو الصورة رهن بتقديم الأصل إلاّ إذا نصّ على خلاف ذلك [3].

ومع انتشار الجرائم المعلوماتية وتوسع انتشارها بتقنيات متطورة، استدعى الأمر إلى تغيير هذه القاعدة لكي تتلاءم مع عصر المعلومات، وقد استجابت بعض التشريعات(كالقانون الأمريكي والانجليزي) لهذه المستجدات، وقام بحسم هذه المسألة لصالح الدليل الالكتروني، وذلك من خلال تعديل قانون الإثبات الفدرالي الأمريكي[4]، والدليل على ذلك أنّه تمّ تطوير المادة (1/101) من قانون الإثبات الأمريكي[5] لكي تشمل الدليل الالكتروني بشكل موسّع، حيث سمحت بالاعتراف

---

(1) ــ عمر محمّد بن يونس، مرجع سابق، ص 440.

(2) - Amoury (B) et Poullet (Y)، le droit de la preuve face à l'informatique et télématique، revue internationale de droit comparé، n° 2، avril - juin، 1985، p. 339.

(3) ــ جاء نصّها الحرفي كالتالي:" باستثناء ما هو مقرّر في هذا القانون أو بقانون خاص يصدر عن الكونجرس، فإنّه عند إثبات مضمون الكتابة والتسجيل والصورة فإنّه يلزم توافر **أصل الكتابة والتسجيل والصورة**"، والنص بالإنجليزية كالتالي:

Rule (1002).of FEDERAL RULES OF EVIDENCE,providesthat:"To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress"

(4) – ينبغي التنبيه أنّ التطور الذي حصل في مجال التشريع لا يقتصر فقط على قواعد الفدراليّة للإثبات الأمريك ي، بل يشمل فضلا عن ذلك القوانين الخاصة بالولايات كتلك القائمة في ولاية **كاليفورنيا، وايوا**، حيث تنص المادة (5/1500) من قانون الإثبات الكالفوربي، على أنّ:" المعلومات المسجّلة بواسطة الحاسب أو برامج الحاسب، أو نسخ أيّهما لا يجب وصفها أو معاملتها على أنّها غير مقبولة بمقتضى قاعدة "أفضل الأدلّة" ". وكذلك جاءت المادة (16/716) من القانون الجديد لجريمة الحاسب لسنة 1984 بولاية ايوا(Iowa)، قاعدة إثبات جديدة تقضي بأنّه :" في أحوال الاتهام بمقتضى هذا الفصل، تكون مخرجات الحاسب مقبولة كدليل على الكيان المنطقي أوالبرنامج أو البيانات التي يحتويها حاسب أو البيانات التي تؤخذ منه، بغض النظر عن تطبيق قاعدة لإثبات تقضي بخلاف ذلك".

(5)- **Rule (1001/1). of FEDERAL RULES OF EVIDENCE**،provides that:" Writings and recordings.—‘‘Writings’’ and ‘‘recordings’’ consist of letters، words، or numbers، or their equivalent، set down by handwriting، typewriting، printing، Photostatting، photographing، magnetic impulse، mechanical or electronic recording، or other form of data compilation"

بالمواد المكتوبة (Writings) والمسجّلة (Recording) والالكترونيّة (Electronic)، لكي تحظى بذات الاهتمام الذي تحظى به الأدلّة الأخرى في المحاكم، وبالتالي قام المشرّع الأمريكي باستخدام مدلول موسع للكتابة والتسجيلات ليشمل كل من الحروف أو الكلمات أو الأرقام أو ما يعادلها، مكتوبة على اليد أو منسوخة على الآلة الكاتبة أو مطبوعة أو تمّ تصويرها أو اتخذت شكل نبضات مغناطيسيّة بتسجيل ميكانيكي أو الكتروني أو أيّ شكل آخر من تجميع المعلومات[1].

لذلك يتمّ اعتبار الكتابة الموجودة داخل الجهاز في صورة كهرومغناطيسيّة من قبيل النسخة الأصليّة وبالتالي لا نصطدم بقاعدة الدليل الأفضل، ونعتبر أنّ المحرّرات الالكترونيّة نسخة أصليّة.

ولقد ذهب القانون الأمريكي أبعد من ذلك حال توسّعه في مدلول عرض الدليل الالكتروني، إذ تنص المادة(1001/ 3 من قانون الإثبات الأمريكي) على أنّه:" **إذا كانت البيانات مخزّنة في حاسوب أو جهاز مماثل فإنّ مخرجات الطابعة أو أيّة مخرجات أخرى يمكن قراءتها بالنظر إلى ما تمّ إظهارها وتبرز انعكاسا دقيقا للبيانات، تعدّ بيانات أصليّة**"[2].

يفهم من خلال هذه المادة أنه يقبل الدليل الالكتروني المستخرج من الطابعة كدليل أصلي كامل، من غير جلب الحاسوب إلى قاعة المحكمة لتأكيد تلك الأصالة.

الفرع الثاني: ضوابط قبول الدليل الإلكتروني في الإثبات الجزائي

إذا كان من المسلم به أنّ للقاضي الجنائي حريّة الاستعانة بكافة وسائل الإثبات اللازمة بما في ذلك الدليل الالكتروني لتكوين عقيدته، فإنّه يثور التساؤل حول نطاق هذه الحريّة، وما إذا كانت حريّة مطلقة أو نسبية.

الواقع أنّ حريّة القاضي الجنائي في هذا الشأن لا يمكن أن تكون مطلقة من كل قيد، لأنّ السلطة المطلقة مفسدة مطلقة. لذا كان من الضروري رسم ضوابط وأطر معيّنة يتعيّن أن تمارس هذه

---

(1) ــ شيماء عبد الغني، مرجع سابق، ص 388.

(2) - **Rule(1001/ 3). of FEDERAL RULES OF EVIDENCE**،provides that:"If data are stored in a computer or similar device، any printout or other output readable by sight، shown to reflect the data accurately، is an **''original''**.

السلطة في نطاقها بحيث لا تنحرف عن الغرض الذي يسعى إليه المشرع، وهو الوصول إلى الحقيقة الفعلية في الدعوى[1].

على ضوء ما تقدم، سوف نبين فيما يلي ضوابط قبول الدليل الإلكتروني من وجهة نظر النظام اللاتيني والأنجلو أمريكي وذلك وفق التفصيل التالي:

أولاـــ ضوابط القبول في النظام اللاتيني:

يوجد قيدا عاما يحد من حرية القاضي في قبول الدليل الإلكتروني، هو قيد المشروعية، بالإضافة إلى قيد ثاني هو وجوب يقينية هذا الدليل فضلا عن ضرورة مناقشته من قبل القاضي ومن كل طرف له مصلحة في ذلك.

1 ـــ قيد مشروعية الحصول على الدليل الإلكتروني:

تخضع قواعد الإثبات الجنائي لمبدأ المشروعيّة ومقتضاه أنّ الدليل الجنائي بما يتضمّنه من أدلة مستخرجة من وسائل إلكترونيّة كالكمبيوتر مثلا، لا يكون مشروعا ومن ثمّ مقبولا في الإثبات، إلاّ إذا جرت عملية البحث عنه والحصول عليه وإقامته أمام القضاء في إطار أحكام القانون واحترام قيم العدالة وأخلاقياتها التي يحرص على حمايتها[2]، فإذا كان المشرع يلقي على كاهل المحقق مهمة كشف الحقيقة في شأن الجريمة وجمع أدلتها فإنّ عمله مشروط بأن يتمّ في رحاب الشرعيّة، وذلك باحترام حقوق الأفراد وعدم المساس بها إلا في الحدود التي يقررها القانون، فإن تجاوز المحقق هذه الحدود وتمكّن من الحصول على دليل يثبت وقوع الجريمة، وجب طرح هذا الدليل وعدم قبوله في الإثبات[3].

---

[1] ـــ جميل عبد الباقي الصغير، مرجع سابق، ص 101.

[2] Djavad (F), le fardeau de la preuve en matière pénale essai d'une théorie générale, thèse Paris, 1977, p. 26.

[3] ـــ وفي ذلك تقرر محكمة النقض بأنّه لا يجوز إدانة المتهم إلى دليل ناشئ عن إجراء باطل (نقض 1/2/ 1990) مجموعة أحكام النقض س 40 رقم 2 ص 27.

ولقد وضعت الاتفاقيات الدوليّة[1]، والدساتير الوطنيّة[2] والقوانين الإجرائيّة المختلفة[3] نصوصا تتضمّن ضوابط لشرعيّة الإجراءات الماسة بالحريّة ومن تمّ فإنّ مخالفة هذه النصوص في تحصيل الدليل الجنائي يصمّ هذا الدليل الجنائي بعدم المشروعيّة، ومن هنا فإنه لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم دليلا الكترونيا تمّ حصوله من تفتيش لنظام معلوماتي باطل، وذلك إثر صدور إذن من جهة غير مختصّة، أو لم تكن الجريمة الالكترونية محل الإذن قد وقعت بعد .. .

وعليه يكتسب هذا القيد أهميّة كبرى نتيجة التقدم الهائل الذي تحقّق في السنوات الأخيرة في شأن الوسائل الفنيّة للبحث والتحقيق والتي تسمح أكثر فأكثر باختراق مجال الحياة الخاصة للأفراد، وإن كان في مقابل ذلك يرضي أو يلبي مقتضيات العدالة الجنائيّة على مكافحة الجريمة بصفة عامة والجريمة الالكترونيّة بصفة خاصة. ومما يثار بحثه في هذا الصدد هو قيمة الدليل غير المشروع في الإثبات الجنائي، فهل يتم استبعاده لمخالفته القواعد العامة للإجراءات الجنائيّة والمبادئ القانونيّة العامة[4]، أم يتم قبوله وذلك حماية للمصلحة العامة على حساب المصلحة الخاصة للأفراد؟

فيما يلي سنتناول قيمة الدليل غير المشروع، سواء كان دليل إدانة أودليل براءة.

أ ــ بالنسبة لدليل الإدانة:

انطلاقا من قاعدة أنّ الأصل في الإنسان البراءة فإنّ المتهم يجب أن يعامل على أساس أنّه برئ في مختلف مراحل الدعوى إلى أن يصدر بحقّه حكم بات(نهائي)، وهذا يقتضي أن تكون الأدلة التي يؤسّس عليها حكم الإدانة مشروعة سواء كانت أدلة تقليدية أو ناتجة عن الوسائل الالكترونيّة بصفة

---

[1] ــ راجع على سبيل المثال المواد:(5 ــ 11ــ 12) من الإعلان العالمي لحقوق الإنسان لسنة 1948. والمواد (3 ــ 8ــ 38) من الاتفاقية الأوربيّة لحقوق الإنسان والحريات الأساسيّة لسنة 1950. وكذلك الاتفاقيّة الدوليّة ضد التعذيب وسائر المعاملات غير الإنسانيّة والحاطة من الكرامة البشريّة لسنة 1984. وأيضا الاتفاقيّة الأوربيّة لمنع التعذيب والمعاملة غير الإنسانيّة أو المهينة لسنة 1987.

[2] – راجع المواد: (46ــ 48ــ 32ــ 34 فقرة 2ــ 35) من الدستور الجزائري لسنة 1996.

[3] ــ راجع المواد:(34ــ 35ــ 91ــ 94 ــ 95ــ 141ــ 206) من قانون الإجراءات الجنائيّة المصري. كذلك المادتين (41 و 44) من قانون الإجراءات الجزائيّة الجزائري.

[4] ــ قضت محكمة النقض البلجيكيّة بأن وصف الدليل غير المشروع لا يقتصر فقط على الفعل الذي يحظره القانون صراحة بل يشمل كل فعل يتعارض مع القواعد الجوهريّة للإجراءات الجنائيّة أو المبادئ القانونيّة العامة. انظر: جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة...، مرجع سابق، ص 110.

عامة، ومن أمثلة الطرق غير المشروعة التّي يمكن أن تستخدم في الحصول على الدليل الالكتروني، إكراه المتهم المعلوماتي من أجل فك شفرة الدخول إلى النظم المعلوماتيّة، أو كلمة السر اللازمة للدخول إلى ملفات البيانات المختزنة، وتتسم بعدم المشروعيّة أيضا أعمال التحريض على ارتكاب الجريمة الالكترونيّة من قبل رجال الضبط القضائي، كالتجسس المعلوماتي أو المراقبة الالكترونيّة عن بعد دون مسوّغ قانوني[1].

انطلاقا من ذلك فأيّ دليل يتمّ الحصول عليه بطريقة غير مشروعة يتمّ إبطاله بما في ذلك الدليل الالكتروني[2]، وعدم إنتاج الإجراء الباطل للآثار التّي تترتّب عليه مباشرة، وهو ما نصت عليه نصّت المادة (157 فقرة 1) من قانون الإجراءات الجزاية الجزائري على أن " تراعى الأحكام المقرّرة في المادة المتعلقة باستجواب المتهمين والمادة (105) المتعلقة بسماع المدعي المدني وإلاّ ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه إجراءات ..". ونصّت أيضا المادة (191) من قانون الإجراءات الجزائيّة الجزائري على أن "تنظر غرفة الاتهام في صحّة الإجراءات المرفوعة إليها وإذا تكشّف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها..".

وهي نفس القاعدة المتبعة في قانون الإجراءات الجزائيّة المصري، حيث نصت المادة (336) من قانون الإجراءات الجنائيّة المصري على أنّه" إذا تقرّر بطلان أي إجراء، فإنّه يتناول جميع الآثار التي تترتب عليه مباشرة، ويلزم إعادته متى أمكن ذلك".

---

[1] ــ عائشة بن قارة مصطفى، مرجع سابق، ص 217.

[2] ــ وفي ذلك أوصى المؤتمر الدولي الخامس عشر للجمعيّة الدوليّة لقانون العقوبات، والذي عقد في ريودي جانيرو بالبرازيل في الفترة من 4ــ 9 سبتمبر سنة 1994 في مجال حركة إصلاح الإجراءات الجنائيّة وحماية حقوق الإنسان بمجموعة من التوصيات، منها التوصيّة رقم (18) التي تنص على أنّ كل الأدلة التي يتمّ الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة، ولا يمكن التمسك بها أو مراعاتها، في أيّ مرحلة من مراحل الإجراءات، وقد أشار هذا المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي والجرائم التقليدية في بيئة تكنولوجيا المعلومات، وإلاّ ترتب عليه بطلان الإجراء فضلا عن تقرير المسؤوليّة الجنائيّة لرجل السلطة العامة الذي انتهك القانون. لمزيد من التفصيل حول هذا المؤتمر انظر:

-XV(15eme) Congrès International de droit pénal, Rio de Janeiro, Brésil, 4-9 septembre 1994, Association Internationale de droit pénale, R. I. D.P, 1er et 2eme trimestres 1995, p.38.

إذا كانت القاعدة أنّ الإجراء الباطل يمتدّ بطلانه إلى الإجراء والإجراءات اللاحقة له مباشرة، غير أنّ هذه القاعدة تثير مسألة في غاية الأهميّة تتعلّق بماهية المعيار الذي يبيّن مدى العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له حتى يمتدّ إليها البطلان. وقد تعدّدت المعايير التي قال بها الفقه المقارن[1]، والمعيار الراجح والسائد في مصر والجزائر هو أنّ العمل اللاحق يعتبر مرتبطا بالإجراء السابق إذا كان هذا الأخير مقدمة ضروريّة لصحة العمل اللاحق، فإذا أوجب القانون مباشرة إجراء معيّن 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[2] .

ب ــ بالنسبة لدليل البراءة:

هناك اختلاف حول مدى اشتراط المشروعيّة بوجه عام في دليل البراءة ويمكن ردّ هذا الخلاف إلى اتجاهات ثلاثة، الأوّل: يتمسّك باعتبار المشروعيّة شرطا لازما في كل دليل والاتجاه الثاني: يقصر المشروعيّة على دليل الإدانة وحده وهو ما تأخذ به محكمة النقض، والاتجاه الثالث: يذهب إلى التفرقة بين ما إذا كانت طريقة الحصول على الدليل غير المشروع ترقى إلى مرتبة الجريمة من عدمه.

ــ الاتجاه الأوّل[3]: يرى أنّ المشروعيّة لازمة في كل دليل سواء أكان إدانة أو براءة، وذلك تأسيسا على نص المادة (336) من قانون الإجراءات الجنائية المصري التي تقرر بطلان جميع الآثار المترتبة على الإجراء الباطل دون تفرقة بين دليل إدانة ودليل براءة، أضف إلى أنّ قصر المشروعية على دليل الإدانة فقط دون البراءة فيه وبالا على الفرد والمجتمع، لأنّه يؤدي إلى اعتبار التزوير وشهادة الزور وإرهاب الشهود حتى يعدلوا عن أقوالهم مشروعة لإثبات البراءة، وينتهي هذا الاتجاه إلى أن إثبات البراءة ــ كالإدانة ــ لا يكون إلا من خلال سبل مشروعة ولا يصح أن يتلف إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أيّ تشريع لكل اقتناع سليم.

---

(1) ــ أحمد فتحي سرور، نظريّة البطلان في قانون الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1959، ص 182.

(2) ــ أحمد فتحي سرور، نفس المرجع ، ص 382 وما بعدها.

(3) – انظر في هذا الاتجاه: رؤوف عبيد، مبادئ الإجراءات الجنائيّة في القانون المصري، دار الفكر العربي، 2006، ص 740. محمود نجيب حسني، مرجع سابق، ص 437.

ـــ **الاتجاه الثاني**[1]: يرى أنّ المشروعية لازمة في دليل الإدانة دون البراءة تأسيسا على أنّ المحكمة لا تحتاج إلى اليقين في إثبات البراءة بل يكفي في ذلك الشك وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع، أضف إلى ذلك أنّ للمتهم الحريّة الكاملة في اختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى وما تحيط نفسه من عوامل الخوف والحذر وغيرها من العوارض الطبيعيّة لضعف النفوس البشريّة والإصرار على تطلب مشروعيّة دليل البراءة أسوة بدليل الإدانة يعرقل حق المتهم في الدفاع عن نفسه الذي يعلوا على حق المجتمع في استيفاء العقاب.

وتعتنق محكمة النقض هذا الاتجاه وقد عبّرت عنه بقولها :"إن كان يشترط في دليل الإدانة أن يكون مشروعا إذ لا يجوز أن تبنى إدانة صحيحة على دليل باطل في القانون، إلاّ أنّ المشروعيّة ليست بشرط واجب في دليل البراءة ، ذلك أنّه من المبادئ الأساسيّة في الإجراءات الجنائيّة أنّ كل متهم يتمتع بقرينة البراءة حتى يحكم بإدانته نهائيّا[2].

ـــ **الاتجاه الثالث**[3]: ويرى ضرورة التفرقة بين ما إذا كان دليل براءة قد تمّ الحصول عليه نتيجة سلوك يعدّ جريمة جنائيّة وما إذا كان قد تمّ الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة إجرائيّة، فإن كان الأول وجب إهدار الدليل وعدم الاعتداد به، لأنّ القول بغير ذلك مفاده استثناء بعض الجرائم من العقاب، والدعوى إلى ارتكابها وهو ما لا يجوز وتأباه الشرائع القويمة، أما إذا كان الحصول على الدليل يخالف قاعدة إجرائيّة فحسب فهنا يصح الاستناد إلى هذا الدليل في تبرئة المتهم تحقيقا للغاية من تشريع البطلان، ولأنّ الفرض أنّ البطلان الذي شاب وسيلة التوصل إلى الدليل إنما يرجع إلى فعل من قام بالإجراء الباطل ، وبالتالي لا يصح أن يضار المتهم بسبب لا دخل له فيه.

---

(1) – انظر في هذا الاتجاه محمود محمود مصطفى، شرح قانون الإجراءات الجنائيّة، مرجع سابق، ص 424. أحمد فتحي سرور، مرجع سابق، ص 752. وانظر أيضا: مأمون سلامة، مرجع سابق، ص 174. محمد زكي أبو عامر، مرجع سابق، ص 117. هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1984، ص 584.

(2) – نقض 31 يناير 1967، مجموعة أحكام النقض، س 18، رقم 24، ص 128. نقض 15 فبراير سنة 1984، مجموعة أحكام النقض، س 35، رقم 31 ، ص 153.

(3) ـــ انظر في هذا الاتجاه: سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، مرجع سابق، ص 471 وما بعدها. محمد عيد الغريب، حريّة القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائيّة، النسر الذهبي للطباعة، 1996ـــ 1997، ص 62.

في إطار الترجيح بين الاتجاهات الثلاثة نجد أنفسنا نؤيد الاتجاه الثاني والذي يقصر المشروعيّة على دليل الإدانة دون البراءة وذلك لعدّة أسباب:

1 ــ أنّ القاعدة هي افتراض البراءة في المتهم ومن تمّ فإنّ أيّ دليل يساعد على تأكيد هذه القاعدة يجب قبوله دون الالتفات لأي اعتبار آخر.

2 ــ قيد المشروعيّة ذاته وهو احترام حقوق الدفاع ممّا يستتبع قصر هذا القيد على دليل الإدانة هو وحده الذي يمسّ حق الدفاع أما قيد البراءة فلا يخضع لهذا القيد[1].

3 ــ كذلك فإنّ العدالة لا تضار إذا أفلت مجرم من العقاب استنادا إلى دليل غير مشروع، لأنّه لا يضير العدالة إفلات مجرم من العقاب بقدر ما يضيرها إدانة برئ.

2 ــ شرط يقينية الدليل الإلكتروني وغير قابليته للشك :

تهدف الخصومة الجنائيّة إلى معرفة الحقيقة المطلقة، ممّا يقتضي أن يصدر حكم القاضي عن اقتناع يقيني بصحّة ما ينتهي إليه من أدلة، لا بمجرّد الظن والاحتمال، إذ أنّ الشك يفسّر لصالح المتّهم، أخذا بقاعدة أساسيّة أنّ الأصل في الإنسان البراءة.

شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستقى منها هذا اليقين تقليديّة أو مستحدثة كالدليل الالكتروني.

بناء على ذلك سوف نتعرض إلى هذا الضابط من خلال أخذ فكرة عامة عن اليقين، ثمّ كيفيّة وصول اقتناع القاضي الجنائي إلى هذا اليقين.

أ ــ فكرة عامة عن اليقين:

إنّ تعريف اليقين في اللّغة هو العلم وزوال الشك وعدم وجود أدنى ريبة[2]. أمّا في الاصطلاح فقد عرّفه الفقهاء بأنّه اعتقاد القاضي بأنّ ما وصل إليه هو الحقيقة[3]. أو هو حالة ذهنيّة وعقليّة

---

(1) ــ ياسر الأمير فاروق محمد، مرجع سابق، ص 655.

(2) ــ مختار الصحاح، مرجع سابق، ص 743.

(3) ــ مفيدة سويدان، مرجع سابق، ص 183.

تؤكد وجود الحقيقة[1]، والوصول إلى ذلك اليقين يتمّ عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال وقائع الدعوى وما يرتّبه ذلك في ذهنه من تصورات ذات درجة عالية من التوكيد وعندما يصل القارئ إلى هذه المرحلة من اليقين، فإنه يصبح مقتنعا بالحقيقة.

ب ــ كيفية الوصول إلى اليقين :

يلتزم القاضي أن يبني اقتناعه على سبيل اليقين والجزم، بمعنى أن تكون هذه الأدلة غير قابلة للشك، والمطلوب عند الاقتناع ليس اليقين الشخصي للقاضي فحسب، وإنّما هو اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قوّتها في الإقناع [2]، وهو بهذا المفهوم يقوم على عنصرين، أحدهما شخصي، ويلخص في ارتياح ضمير القاضي واطمئنان نفسه إلى إدانة المتّهم على سبيل الجزم واليقين، والثاني موضوعي، ويخلص في ارتكان هذا الارتياح والاطمئنان على أدلّة من شأنها أن تفض لذلك وفقا لمقتضيات العقل والمنطق[3]. بحيث لا يكون عمل القاضي ابتداعا للوقائع وانتزاعا من الخيال[4].

تكمن العلّة من وراء اقتضاء هذا القيد في أنّ الحكم بإدانة شخص أمر جدّ خطير، وتترتّب عليه آثار جسيمة، ويمكن أن ينال من حريّته أو شرفه أو ماله، بل قد يكون حقّه في الحياة[5]. فضلا عن أنّ القانون قد جعل الأحكام الباتّة عنوانا للحقيقة، لذلك وجب أن تكون تلك الأحكام مبنيّة على الجزم واليقين[6].

---

(1) Rached (A.A), de l'intime conviction du juge, thèse Paris, 1942, p. 3.

مشار إليه عند: هلالي عبد ألاله أحمد، حجيّة مخرجات الكمبيوتريّة في المواد الجنائيّة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، ص 78.

(2) ــ أحمد فتحي سرور، مرجع سابق، ص475.

(3) ــ محمد عيد غريب، مرجع سابق، ص 130.

(4) ــ نقض 9 يناير سنة 1930، مجموعة القواعد القانونيّة، الجزء الأوّل، رقم 368، ص 416.

(5) ــ حسن صادق المرصفاوي، أصول الإجراءات الجنائيّة في القانون المقارن، منشأة المعارف، الاسكندرية، 1982، ص 624.

(6) ــ السيد محمد حسن شريف، النظرية العامة للإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص 364. وانظر أيضا: محمّد علي السالم عياد الحلبي، حريّة القاضي الجنائي في الاقتناع في قوانين مصر والأردن والكويت، مجلة الحقوق، العدد الثالث، السنة الحادية والثلاثون، سبتمبر 2007، الكويت، ص 376.

إذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالأدلة التقليديّة عن طريق المعرفة الحسيّة التي تدركها الحواس، أو المعرفة العقليّة التي يقوم بها القاضي عن طريق التحليل والاستنتاج، فإنّ الجزم بوقوع الجريمة الالكترونيّة ونسبتها إلى المتّهم المعلوماتي تتطلّب نوعا جديدا من المعرفة وهي المعرفة العلميّة للقاضي بالأمور المعلوماتيّة لاسيما وأن القاضي الجنائي يلعب دورا إيجابيّا في الإثبات، وقد يؤدي الجهل في بعض الأحيان إلى التشكك في قيمة الدليل الالكتروني ومن تمّ يقضي بالبراءة، لاسيما أنّ الشك يستفيد منه المتّهم المعلوماتي في مرحلة المحاكمة، وهذا ما يؤدي إلى إفلات المجرمين من تطبيق القانون[1].

لذلك نتيجة نقص الثقافة المعلوماتية لدى القاضي الجنائي، فنادرا ما يتحقق له اليقين باللأدلة الإلكترونية، يجب عليه أن يخضع هذا الدليل إلى التقييم الفني من قبل الخبيرالتقني للتأكد من سلامته من العبث وذلك باستعمال طرق علمية خاصة [2] وبالتالي البحث عن مصداقية الأدلة الألكترونية والتحققق من يقينية هذه الأدلة.

3 ــ قيد مناقشة الدليل الإلكتروني:

من القواعد الأساسيّة في الإجراءات الجنائيّة أنّه لا يجوز للقاضي أن يبني حكمه على أدلّة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبّر عنه بوضعيّة الدليل، ومقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته، وكلا الأمرين ينبغي توافرهما. وقد أرست هذا الضابط المادة(212 فقرة 2) من قانون الإجراءات الجزائيّة الجزائري إذ تنص :" ولا يسوغ للقاضي أن يبني قراره إلاّ على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريّا أمامه" [3] .

---

[1]ــ عائشة بن قارة مصطفى، مرجع سابق، ص 279.

[2]ــ نفس المرجع ، ص217.

[3]ــ كذلك نصت على هذه القاعدة المادة (427) من قانون الإجراءات الجنائيّة الفرنسي في فقرتها الثانيّة بقولها: "لا يجوز للقاضي أن يؤسّس حكمه إلاّ على أدلّة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الخصوم".

- Article 427 alinéa 2 du (C.P.P) dispose que :" Le juge ne peut fonder sa décision que sur des preuves [*appréciation*] qui lui sont apportées au cours des débats et contradictoirement discutées devant lui" .

نصّت عليها أيضا المادة (302) من قانون الإجراءات الجنائيّة المصري بقولها" ومع ذلك لا يجوز له (أي القاضي) أن يبني حكمه على أيّ دليل لم يطرح أمامه في الجلسة".

عبّرت محكمة النقض المصريّة عن هذا الضابط بقولها" من المقرر أنّ لمحكمة الموضوع أن تستخلص من جماع الأدلة والعناصر المطروحة أمامها على بساط البحث الصورة الصحيحة لواقعة الدعوى حسبما يؤدي إليه اقتناعها، وأن تطرح ما يخالفها من صور أخرى لم تقتنع بصحتها، ما دام استخلاصها سائغا مستندا إلى أدلّة مقبولة في العقل والمنطق ولها أصل في الأوراق[1].

علّة هذه القاعدة هي مبدأ الشفويّة[2] في المحاكمة الجنائيّة، وهو مبدأ أساسي في الإجراءات الجنائيّة، وتقتضيه أولى بديهيات العدالة[3]، حيث يجعل القاضي غير مكتف في تقديره للأدلة سواء كانت تقليدية أو مستخرجة من الوسائل الالكترونية، على ما دوّن بمحاضر التحقيق، وإنّما يتوجّب عليه أن يسمع الشهود واعتراف المتهم بنفسه وما يدلي به الخبراء ويطرح جميع الأدلة الأخرى للمناقشة الشفويّة، فلا يكون هناك وسيط بين الدليل والقاضي. وغاية ذلك حتّى يتاح لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة إزاءه ويبيّن موقفه منها، ممّا يفيد القاضي من تكوين قناعته من حصيلة هذه المناقشات التي تجرى أمامه في الجلسة[4].

لا يختلف الأمر بالنسبة للدليل الالكتروني، سواء كان على شكل بيانات معروضة على شاشة الكمبيوتر، أو مدرجة في حاملات البيانات أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئيّة أو مستخرجة في شكل مطبوعات، كل أولئك سيكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة[5].

---

(1) – نقض رقم 360 السنة 46، جلسة 1976/6/6، س 27. وكذلك نقض رقم 929، السنة 53، جلسة 10/13/ 1982. انظر: معوض عبد التوّاب ، الوسيط في أحكام النقض الجزائيّة، مركز الوثائق والدراسات الانسانية، دون سنة الطبع،، ص 24 وما بعدها.

(2) – إنّ مبدأ الشفويّة في القضاء الجنائي، في أساسه من قواعد النظام الاتهامي والذي ظهرت به الإنسانية منذ الثورة الفرنسية، وقد أقرّته الجمعيّة التأسيسية منذ 18/ 1/ 1791 من نظام الإثبات الجنائي المبني على حريّة القاضي الجنائي في تكوين قناعته، وقد استقرّ النظامان معا، شفويّة المرافعة وقضاء القاضي بمحض اقتناعه، في قانون تحقيق الجنايات الفرنسي الذي صدر في 24 نوفمبر سنة 1808. انظر في ذلك: رؤوف عبيد، المشكلات العمليّة الهامة في الإجراءات الجنائيّة، الجزء الأول، الطبعة الثانيّة، دار الفكر العربي،1963، ص 472.

(3) ــ محمود نجيب حسني، مرجع سابق، ص 427. وانظر أيضا : محمد مروان، مرجع سابق، ص 491.

(4) ــ فاضل زيدان محمد، مرجع سابق، ص 254.

(5) ــ هلالي عبد الله أحمد، حجيّة المخرجات الكمبيوترية في المواد الجنائيّة، مرجع سابق، ص 103.

يترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم المعلوماتية بناء على علمه الشخصي أو استنادا إلى رأي الغير إلا إذا كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر من قبله[1].

1ـــ عناصر قيد مناقشة الدليل الالكتروني: يقوم ضابط مناقشة الدليل الالكتروني على عنصرين أساسيين هما:

أ ـــ إتاحة الفرصة للخصوم للاطلاع على الدليل الالكتروني والرد عليه.

ب ـــ وأن يكون للدليل الالكتروني أصل في أوراق الدعوى.

بالنسبة للعنصر **الأوّل**، يجب على القاضي مبدئيا أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم حتّى يكونوا على بيّنة ممّا يقدّم ضدّهم من أدلة ليتمكّنوا من مواجهة هذه الأدلة والردّ عليها، وذلك احتراما لحقوق الدفاع، الذي يعدّ أحد المظاهر الأساسية لدولة القانون والنظم الديمقراطية[2]، ويتيح مبدأ المواجهة تجسيد هذا الأخير، حيث يقتضي المبدأ الأوّل حضور كل خصم في الدعوى، وأن يطّلع خصمه على ما لديه من أدلة، وأن يواجهه بها، وأن يناقش كل منهما أدلّة الطرف الآخر[3].

يتطلّب مبدأ المواجهة نوعين من الضمانات:

الأولى: منها سابق على عمليّة المواجهة ذاتها بين الأطراف في الجلسة، وهو يتضمّن ضرورة إحاطة المتهم علما بالتهمة المنسوبة إليه، وأن يمنح الوقت والوسائل اللازمة لتحضير دفاعه، وأن يسمح له بالاستعانة بمحام للدفاع عنه، وكذلك الاستعانة، عند الاقتضاء بمترجم[4].

---

(1)- Crim.,10 janvier 1995, pourvoi n° 94-84.687, *Bull.crim*. 1995, n° 13. disponible en ligne : sur site de la courdecassation francais: https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2013_6615/livre_4_jurisprudence_cour_6619/arrets_rendus_chambres_6675/droit_penal_procedure_penale_6682/procedure_penale_29254.html.

(2) -Nicol Opoulos (P), le procédure devant les juridictions répressives et le principe du contradictoire, revue de science criminel, N' 1 , 1989, p.3.

(3)ـــ محمود نجيب حسني، مرجع سابق، ص 815.

(4) ـــ محمد حسن شريف، مرجع سابق، ص 231.

أمّا النوع **الآخر** من الضمانات، فيتمّ أثناء عمليّة المواجهة ذاتها، وهي الأكثر تأثيرا في الدعوى الجنائيّة، إذ يلزم أن يسمح لكل طرف بتقديم ما لديه من مستندات، وسؤال شهود، والخبراء، وأن يطلب اتخاذ أي إجراء يقدر فائدته، وإثارة أي دفوع ، أو إيداع أي مذكرات[1]. ثمّ حق كل طرف في مناقشة أدلة الطرف الآخر وتفنيدها، كسؤال الشهود ومناقشتهم، ومناقشة تقرير الخبير ودحض ما ورد به.

وعلى ذلك، لا يجوز للقاضي الجنائي أن يبني اقتناعه على دليل قدّمه أحد أطراف الدعوى إلا إذا عرض هذا الدليل في جلسة المحاكمة بحيث يعلم به سائر الأطراف. إذ أنّ العدالة تقتضي أن يأتي حكم القاضي بعد مناقشة هادئة ومجادلة حرّة متكافئة من كل صاحب حق مشروع في الدعوى.

أمّا بالنسبة للعنصر **الثاني** والمتمثّل في ضرورة أن يكون للدليل الالكتروني أصل في أوراق الدعوى، وذلك حتى يكون اقتناع القاضي مبنيّا على أساس، وفي ذلك قالت محكمة النقض المصريّة في حكم حديث لها:" على المحكمة أن تبنى حكمها على الوقائع الثابتة بالدعوى، وليس إقامة قضائها على أمور لا سند لها من التحقيقات"[2]، وأنّ القاضي حرّ في استمداد اقتناعه من أي دليل يطمئن إليه، طالما أنّ له مأخذه الصحيح من الأوراق[3].

من أجل ذلك أوجب المشرّع تحرير محضر الجلسة لإثبات وقائع الدعوى الجنائيّة وأدلتها لكي يتمكّن القاضي الموضوع أو أيّ من الخصوم من الرجوع إلى هذا المحضر إذا ما رغبوا في استيضاح أيّ من الوقائع الثابتة به، وذلك منعا للتحكم وتحقيقا للعدالة.

بالإضافة إلى ذلك، فإنّ هذا التدوين يمكن المحكمة المطعون أمامها، من مراجعة الحكم المطعون فيه وتقديره من حيث الخطأ والصواب[4].

---

(1)-Nicol Opoulos (P),op.cit, p. 21 et s .

(2)ــ نقض 22 أكتوبر سنة 1990، مجموعة أحكام النقض، س 41،رقم 162، ص 929.

(3)– نقض 24 فبراير سنة 1975، مجموعة أحكام النقض، س 26، رقم 42، ص 188.

(4)ــ مأمون سلامة، الإجراءات الجنائيّة، مرجع سابق، ص 170ــ 175.

ثانيا ــ ضوابط القبول في النظام الأنجلو أمريكي:

خروجا عن الأصل العام الذي يتبنّاه القانون الانجليزي في عدم قبول الشهادة السماعيّة، إلاّ أنّ هذا القبول مقيّد بشروط معيّنة نصّت عليها المادة (69) من قانون الشرطة والإثبات الجنائي لسنة 1984 وهي كالتالي[1]:

1ــ عدم وجود أسباب معقولة للاعتقاد بأن ّالبيان يفتقر إلى الدقة بسبب الاستخدام غيرالمناسب أو الخاطئ للحاسب.

2 ــ الوفاء بأيّة شروط متعلّقة بالمستند محدّدة طبق القواعد المحاكمة (المتعلّقة بالطريقة أو الكيفيّة التي يجب أن تقوم به االمعلومات الخاصة بالبيان المستخرج عن طريق الحاسب).

3 ــ أنّ الحاسب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فإن ّأي ّجزء لم يعمل في هب صورة سليمة أو كان معطّلا عن العمل، لم يكن ليؤثّر في إخراج المستند أو دقّة محتوياته[2].

بناء عليه فإنّ النيابة العامة إذا استندت إلى مستند الكتروني في دعوى جنائيّة يتعيّن عليها أن تقدّم الدليل على أن ّالجهاز يعمل بطريقة صحيحة، ولا يلزم أن يتمّ إثبات هذه الأخيرة من جانب الخبير.

---

[1] ــ عمر محمد بن يونس، مرجع سابق، ص 428.

[2] –ويقيم القانون الكندي عدّة قرائن على سلامة عمل جهاز الكمبيوتر، تتمثل فيما يلي:

1 ــ إذا كانت الجهة صاحبة الجهاز تعتمد على الكمبيوتر في إدارة عملها اليومي، ومادام الجهاز يعمل بشكل صحيح فإنّ الملف الالكتروني يكون هو الآخر صحيحا، بل أكثر من ذلك فإنّ الملف يعتبر صحيحا أحيانا على الرغم من بعض الخلل في جهاز الكمبيوتر إذا كان هذا الخلل لا يؤثر في سلامة هذا الملف إذا لم توجد أسباب معقولة تدعو إلى التشكك في سلامة هذا الملف. (المادة 5 فقرة (a) من قانون الإثبات الالكتروني الموحّد في كندا).

2 ــ إذا تمّ تسجيل أو تخزين الملف الالكتروني من جانب شخص غير طرف في الدعوى القضائيّة في أثناء قيامه بأعماله المعتادة والذي لم يكن يعمل لحساب أحد أطراف تلك الدعوى الذي يحاول تقديمها في الدعوى.

3 ــ إذا قدّمها الخصم في دعوى أمام المحكمة وكان هذا المستند مستخرجا من جهازه، ذلك أنّه بتقديمه هذا المستند لصالحه إنّما يشهد بصحّته.

المطلب الثاني: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني

يخضع الدليل الالكتروني للمبدأ العام في الإثبات الجنائي وهو حريّة القاضي الجنائي في الاقتناع (L'intime conviction)، وحريّته في هذا المقام بالغة السعة، فهو وحده الذي يقدّر قيمة الدليل الالكتروني بحسب ما تحدثه من أثر في وجدانه من ارتياح واطمئنان، ومع تعاظم دور الإثبات العلمي مع ظهور الدليل الالكتروني المطلوب للإثبات في الجرائم الالكترونيّة، ممّا جعل القاضي أنّه يضطر للتعامل مع هذا النوع المستحدث من الأدلة الضرورية لكشف أنماط جديدة من الجرائم في مقابل نقص الثقافة المعلوماتية، **فهل من شأن ذلك أنّ القاضي يسلم ويبني اقتناعه بالدليل الالكنروني على أساس أن أمره محسوم علميا؟**

على ذلك، سنتناول في الفرع الأوّل، الطبيعة العلمية للدليل الالكتروني وأثرها على اقتناع القاضي الجنائي، ثمّ بيان مشكلات الدليل الالكتروني ومدى تأثيرها على اقتاع القاضي، وأخيرا موقف المشرع الجزائري من هذا الدليل في الإثبات الجنائي.

الفرع الأول: الطبيعة العلمية للدليل الإلكتروني وأثرها على اقتناع القاضي الجزائي

يقتضي الحديث عن الطبيعة العلميّة للدليل الالكتروني وأثرها على اقتناع القاضي الجنائي، بيان مضمون مبدأ الاقتناع القضائي وما يعنيه في مجال الإثبات الجنائي، ثمّ بيان قيمة الدليل الالكتروني في الإثبات الجنائي، ومادام أنّ الدليل الالكتروني يعدّ تطبيقا من تطبيقات الدليل العلمي، يتعيّن علينا أن تناوله بالدراسة بالإضافة إلى مدى تأثّر القاضي الجنائي به، ذلك ما سيتمّ تناوله في التالي على النحو الآتي:

أوّلاـــ مفهوم مبدأ الاقتناع القضائي:

يعدّ مبدأ الاقتناع القضائي أحد أهم المبادئ التي تقوم عليها نظريّة الإثبات في المواد الجنائيّة، وعنه تتفرّع معظم القواعد التي تحكم هذا الإثبات[1].

[1] ـــ محمود نجيب حسني، مرجع سابق، ص 774.

يعرف فقهاء القانون الجنائي الإقتناع بأنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنية ذو خاصية ذاتية نتيجة تفاعل ضمير القاضي وأدلة الإثبات المطروحة والتي يقيرها الخصوم إما لإثبات أو إنكار إتهام [1].

قد أقرت معظم التشريعات الحديثة[2] هذا المبدأ، حيث نصّ عليه المشرّع الفرنسي في المادة (353) من قانون الإجراءات الحالي الصادر في 1958[3]، التي تنص على ما يلي: " لا يطلب القانون من القضاة حسابا بالأدلة التي اقتنعوا بها، ولا يفرض قاعدة خاصّة تتعلّق بتمام وكفاية دليل ما، وإنّما يفرض عليهم أن يتساءلوا في صمت وتدبّر، وأن يبحثوا في صدق ضمائرهم أي تأثير قد أحدثتها لأدلة الراجحة ضد المتّهم ووسائل دفاعه..."[4].

أمّا المشرع الجزائري فإنّه كرّس مبدأ الاقتناع القضائي بموجب المادة (307) من قانون الإجراءات، وهي مستوحاة من المادة(353) من القانون الفرنسي حيث تنص على:" يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلّق فضلا عن ذلك بحروف كبيرة في أظهر مكان غرفة المداولة:(إنّ القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعيّن عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت أن يبحثوا بإخلاص ضمائرهم في

---

[1] ــ نصر الدين ماروك، النظرية العامة للإثبات الجنائي، الجزء الأول، دار هومة، 2004، ص 620.

[2] ــ لم يقتصر تطبيق مبدأ الاقتناع القضائي على التشريعات اللاتينية فحسب، بل يمتدّ حتى بالنسبة للتشريعات الانجلوأمريكيّة مع اختلاف طفيف في الصياغة، فهي لا تعرف تعبير الاقتناع القضائي، وإنّما تستخدم بدلا منه **تعبير ثبوت الإدانة بعيدا عن أيّ شك معقول** Proof) . beyond a reasonable doubt)انظر:

Spencer(John), la preuve en procedure pénale, droit englais, R.I. D. P, 1992, p. 101.

[3] - Stefani(Gaston), répertoire de prevue en droit pénal, et de procedure pénal, Dalloz tome v, 1969, p. 5.

[4] Article 535 du (C.P.P) ، dispose que :" La loi ne demande pas compte aux juges des moyens par lesquel sils se sont convaincu s،elle ne leur prescrit pas de règles des quelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interrogereux-mêmes dans le silence et le recueillement et de chercher،dans la sincérité de leur conscience ،quelle impression ont faite ،sur leur raison، les preuves rapportées contre l'accusé، et les moyens de sadéfense. La loi ne leur fait que cette seule question، qui renferme toute la mesure de leurs devoirs: "Avez-vous une intim econviction ?".

أي تأثير قدأحدثته في إدراكهم الأدلة المسندة إلى المتّهم وأوجه الدفاع عنها و لم يضع لهم القانون سوى هذا السؤال الذي يتضمّن كل مطاق واجباتهم: هل لديكم اقتناع شخصي؟''.

كما أنّ الاقتناع القضائي كرسته أيضا صراحة المادة (212) من قانون الإجراءات الجزائيّة الجزائري حيث تنص :" يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص..".

ثانيا ــ قيمة الدليل الالكتروني كدليل علمي:

في البداية ينبغي علينا الإشارة إلى أن الدليل الالكتروني لا يحظ أمام القاضي الجنائي بقوّة حاسمة في الإثبات، وإنّما هو مجرد دليل لا تختلف قيمته ولا تزيد حجّته عن سواه، وهذا أثر من آثار حريّة القاضي الجنائي في الاقتناع، وعلى هذا الأساس يصح للقاضي أن يؤسس اقتناعه على الدليل الالكتروني كما يصح أن يهدره تبعا لاطمئنانه، ولا يجوز مطالبة القاضي أو إلزامه بالاقتناع بالدليل الالكتروني ولو لم تكن في الدعوى أدلة سواه.

والفقه الفرنسي يتناول حجية مخرجات الكمبيوتر في المواد الجنائية ضمن مسألة قبول الأدلة المتحصلة عن الآلة أو ما يسمى بالأدلةالعلمية، سواء كانت بيانات مكتوبة أو صورا. وتطبيقا لذلك قضي في فرنسا بخصوص قوّة المحرّرات الصادرة عن الآلات الحديثة في الإثبات بأنّه إذا كانت التسجيلات الممغنطة لها قيمة الدلائل يمكن الاطمئنان إليها، ويمكن أن نكون صالحة في الإثبات أمام القضاء الجنائي[1]. وفي حكم أخر قرّرت محكمة النقض الفرنسيّة بأنه إذا اطمأنت محكمة الموضوع وفقا لاقتناعها الذاتي والقواعد العامة إلى ما استندت إليه النيابة من قرائن بشأن خطأ سائق سيارة منسوب إليه تجاوز السرعة، وقد ثبت ذلك من خلال جهاز آلي التقط صورة السيارة المتجاوزة

[1]- Crim 24avril 1987, Bull, n° 173.cité par Francillon (Jacques), les crimes informatiques et d'autre crime dans le domaine de la technologie informatique en France, revue internationale du droit pénale, 1993, p. 308 et s.

للسرعة، ودون أن يكون السائق قد سئل، فإنّها لا تكون ملزمة بتحديد من استندت إليه من عناصر الواقعة في تبرير اقتناعها[1].

من الجدير بالذكر أنّ أغلب التشريعات ذات الأصل اللاتيني وان كانت تتفق حول قبول الدليل الالكتروني استنادا إلى قاعدة الاقتناع الحر للقاضي الجنائي، إلاّ أنّها تختلف في طريقة تقديم هذا الدليل أمام المحكمة، حيث تشترط بعض التشريعات كالقانون اليوناني (المادة 324 من التقنين الإجرائي)[2] والياباني[3]، سويسري والنمساوي، قواعد معيّنة في هذا الخصوص، كأن يكون الدليل الالكتروني مقروءا سواء أكان مطبوعا على ورق بعد خروجه من الجهاز، أم كان مقروءا على شاشة جهاز الكمبيوتر ذاته.

بما أنّ الدليل الالكتروني تطبيق من تطبيقات الدليل العلمي، وذلك بما يتميّز به من موضوعيّة وحياد وكفاءة، ممّا يجعل اقتناع القاضي الجنائي أكثر جزما ويقينا، حيث يساعده على التقليل من الأخطاء القضائيّة، والاقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة. تلك السمات التي ربما تدفع البعض إلى الاعتقاد بأنّه بمقدار اتساع مساحة الأدلة العلميّة ومن بينها الدليل الالكتروني بمقدار ما يكون انكماش وتضاؤل دور القاضي الجنائي في التقدير، خاصّة أمام نقص الثقافة الفنيّة للقاضي وبالتالي فإنّ مهمّته تصبح شبه آلية، حيث يكون الدور الأكبر للخبير الذي يسيطر على العمليّة الإثباتيّة، و لم يبق أمام القاضي سوى الإذعان لرأي الخبير، دون أيّ تقدير من جانبه[4].

---

(1)- Crim 3 janvier 1978, Bul, n°1 ,Dalloz , code de procédure pénale, 1991- 1992, p. 413. Crim, 20 janvier 1977, J.C. P. 1977, n° 11.

مشار إليه عند: هشام محمد فريد رستم، الجوانب الإجرائيّة للجرائم المعلوماتية..، مرجع سابق، ص 156.

(2) – حيث تشترط المادة (364) من التقنين الإجرائي اليوناني قراءة المستندات والوثائق التي استخدمت كأدلة أثناء التحقيقات، مع العلم أنّه يسود مبدأ حريّة قبول الأدلة وحريّة تقييمها من طرف القاضي الجنائي (المادة 177ـــ 179 إجراءات يوناني)

(3) – ويجب التنويه بأنّ التسجيل الالكترومغناطيسي (Électro- magnétique) لا يصلح كدليل يستند منه القاضي اقتناعه بسبب أنه غير مرئي في حد ذاته، لدى يتم تحويلها إلى شكل مرئي مقروء عن طريق طباعتها، ومن تمّ قابليتها للتقدير. انظر: هشام محمد فريد رستم، مرجع سابق، ص 159.

(4)ـــ عائشة بن قارة مصطفى، مرجع سابق، ص 248.

وعليه يمكن الفصل في هذا الخلاف من خلال بيان دور الخبير في الدعوى الجنائية من جهة، ثم تقدير القاضي للدليل العلمي من جهة أخرى.

1 ــ دور الخبير في الدعوى الجنائيّة:

سبق الحديث عن الخبرة و بيان الدور البارز لها في عمليّة الإثبات القضائي نظرا لما شهده هذا العصر من تطور علمي و تكنولوجي[1]، لحد وصفه بعصر المعلومات. فالخبرة وسيلة إثبات تهدف إلى كشف بعض الدلائل و الأدلة، أو تحديد مدلولها بالاستعانة بالمعلومات العلميّة[2]، التي لا تتوافر لدى القاضي، حيث تتطلب بعض الحالات معرفة خاصّة لا يملك القاضي الأهلية اللازمة لها، ممّا استلزم أن يكون للخبير دور في الدعوى الجنائيّة، وذلك ماقضت به محكمة استئناف شونبري "Chambery "في 16 نوفمبر 2016، بتهمة موظف عام قام بالاعتداء على المراسلات الالكترونية بطريق الغش المعلوماتي ضد أحد العملاء، واستند القاضي في ذلك ذلك برأي الخبير. [3].

الدليل العلمي شأنه شأن باقي أدلة الإثبات يخضع لتقدير القاضي ومدى تأثيره في الاقتناع الذاتي للقاضي الجنائي، وأنّه لا يمكن للخبير مهما كانت دقّة نتائجه وموضوعيتها أن يحتل مكانة القاضي في إيجاد العدالة، والتي يستلزم إيجاد حسا مختصا لا يدركه غيره، ويتمّ هذا الحس من خلال التكوين العلمي و القضائي الرفيع، والذي تنهض به المؤسسات العلميّة القانونيّة بوجه عام و القضائيّة بوجه خاص، ليشكل أساسا رصينا في التقدير السليم للأدلة و الذي من خلاله يصل إلى قراره العادل الذي يكون عنوانا للحقيقة[4].

غير أنه ما يظهر في الواقع العملي أن القاضي غالبا ما يسلم بما خلص إليه الخبير في تقريره، ويبني حكمه على أساسه، وهذا التصرف منطقي من القاضي، فلا شك في أن رأي الخبير وُرد في

---

(1)ــ انظر فيما سبق، ص وما بعدها.

(2)ــ أحمد فتحي سرور، الوسيط في الإجراءات الجنائيّة، مرجع سابق، 494.

(3)- Cour d'appe Chanbery ، 16 novembre 2016. Disponile en ligne :

https://www.legalis.net/jurisprudences/cour-dappel-de-chambery-arret-du-16-novembre-2016/

(4)ــ عائشة بن قارة مصطفى، مرجع سابق، ص 249

موضوع فني لا اختصاص للقاضي به، وليس من شأن ثقافته أو خبرته القضائية أن تتيح له الفصل فيه، بالإضافة إلى ذلك فهو الذي انتدب الخبير ووُثق فيه ورأى أنه مناسب لمهمته[1].

في مقابل ذلك يرى بعض الفقه[2]ضرورة إعطاء قوة إلزامية لتقرير الخبير، وذلك على أساس أن القاضي إذا رفض رأي الخبير فقد تعارض مع نفس، ويعني ذلك أنه أراد أن يفصل بنفسه في مسألة سبق أن اعترف في بادئ الأمر بأن الخبير يتمتع فيها بمعرفة ودراية تفوق معرفته الشخصية.

في تقديرنا نرى أن الخبرة هي مجرد استشارة فنية، تستعين بها السلطات القضائية لمساعدتهم في تكوين عقيدتهم نحو المسائل الفنية، وإن أصبحت لها دور بارز في عملية الإثبات القضائي في العصر الحالي، عصر المعلومات، إلا أنه في الأخير ما هو إلا أحد الأدلة الجنائية التي تملك المحكمة حيالها التقدير، وهذا الرأي مطروح أيضا للمناقشة من قبل كافة خصوم الدعوى.

2 ــ تقدير القضاء للدليل العلمي:

يخضع الدليل العلمي كما سبق إلى تقدير القاضي الجنائي و بالتالي اقتناعه، وفي هذا الخصوص ينبغي أن نميّز بين أمرين:

ــ أوّلا: القيمة العلميّة القاطعة للدليل[3]:

ــ ثانيا: الظروف و الملابسات التي وجد فيها الدليل.

فتقدير القاضي لايتناول الأمر الأوّل، وذلك لأن ّقيمة الدليل تقوم على أسس علميّة دقيقة، وبالتالي لا حريّة للقاضي في مناقشة الحقائق العلميّة الثابتة[4]. أمّا الظروف والملابسات التي وجد فيها

---

(1) -Georges Cornu, Les rôlesrespectifs du juge et du techniciendansl'administration de la preuve , Xecolloque des institutsd'étudesjudiciaires, Poitiers, 26-28 mai 1975, Publication de la Faculté de droit et des sciences sociales de Poitiers ,1975,P. 67.

(2)ــ أمال عبد الرحيم عثمان، الخبرة في المسائل الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964، ص 307 وما بعدها.

(3)ــ جميل عبد الباقي الصغير، مرجع سابق، ص 22. وانظر أيضا: هلالي عبد الله، مرجع سابق، ص 46.

(4) – أصبح للبصمة الوراثية (D.N.A) نتائج قاطعة في تحديد الهويّة، فعلى سبيل المثال، إذا أثبت فحص الحمض النووي استحالة أن يكون الطفل (س) ابنا للأب (أ) التي تدعي الأم (ب) نسبته إليه، فما على القاضي سوى التسليم لهذه النتيجة دون مناقشة كيف تمّ التوصل إلى هذه النتيجة من الناحيّة العلميّة، ونتيجة لذلك أصبحت بعض التشريعات مثل القانون الفرنسي، القانون الألماني، والقانون الايرلندي تستخدم البصمة الوراثية في التعرف على شخصيّة الجناة، وذلك بضمانات تحمي السلامة الجسديّة وحرمة الحياة الخاصة للمتّهم. لمزيد من التفصيل حول

الدليل، فإنّها تدخل في نطاق تقديره الذاتي، فهي من صميم وظيفته القضائيّة، بحيث يكون في مقدوره أن يطرح مثل هذا الدليل رغم قطعيّته إذا تبيّنب أنّه لا يتفق مع ظروف الواقعة وملابساتها، حيث تولد الشبهة لدى القاضي، ومن تمّ يقضي في إطار تفسير الشكل صالح المتّهم.

ذلك أن مجرد توافر الدليل العلمي لا يعني أنّ القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أم بالبراءة، دون بحث الظروف والملابسات، فالدليل العلمي ليس آلية معدّة لتقريراقتناع القاضي بخصوص مسألة غير مؤكدة[1]، بل هو دليل إثبات قائم على أساس من العلم و المعرفة، وللقاضي النظر إليه على ضوء الظروف و الملابسات المحيطة.

وعلى ذلك، فإنّنا لانذهب مع الاتجاهات الفقهيّة القائلة بأنّ نظام الأدلة العلميّة سيكون نظام المستقبل وسيحل الخبير في القضاء، فيكون الدور له وليس للقاضي، فيجعل رأي الخبير هو الحاسم لاقتناع القاضي. ولأنّ التطور العلمي في مجال الأدلة لا يتعارض مع سلطة القاضي الجنائي في تقديرها، بل إنّ هذه الأدلة ستكفل للقاضي وسائل فعالة في كشف الحقيقة[2].

الفرع الثاني: مدى تأثير مشكلات الدليل الالكتروني على اقتناع القاضي

يثير الدليل الالكتروني العديد من المشكلات، وهي في الحقيقة تتعلق بطبيعته التكوينية من جهة وبإجراءات الحصول عليه من جهة أخرى، وهذه المشكلات تعود عليه بالسلب حيث تضعف من قيمته في مجال الإثبات الجنائي إن لم يتّم إيجاد حلول بشأنها. وسيكون تناولنا لهذه المشكلات من خلال نوعين من المشاكل أولها موضوعيّة وثانيها مشكلات إجرائيّة.

أوّلاــ المشكلات الموضوعيّة للدليل الالكتروني:

وهي غالبا ما تتعلّق بطبيعة الدليل ذاته، وذلك بسبب الخصائص الفيزيائية التي يتكوّن منها هذا الدليل، سواء بسبب الطبيعة غير المرئية له، أو بسبب مشكلة الأصالة، أو بسبب ديناميكيّته.

هذا الموضوع انظر: جميل عبد الباقي الصغير، مرجع سابق، ص 59. وانظر أيضا: وانظر أيضا: خالد محمد الحمادي، مرجع سابق، ص 29 وما بعدها .

[1] ــ جميل عبد الباقي الصغير، مرجع سابق، ص 23. وانظر أيضا: هلالي عبد الله، مرجع سابق، ص47.

[2] ــ فاضل زيدان، مرجع سابق، ص 155.

1 ــ الدليل الالكتروني دليل غير مرئي:

فهو عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي في شكل ثنائي[1]، وبطريقة غير منظمة، فعلى سبيل المثال تتضمن الأقراص الصلبة مزيجا من بيانات مختلطة فيما بينها والتي لن تكون كلها ذات صلة بالمسألة المطروحة [2]، بمعنى أنّ هناك اختلاطا بين الملفات البريئة مع تلك المجرمة التي تعدّ موضوعا للدليل الجنائي الرقمي ممّا تؤدي إلى خلق مشكلة التعدي على الخصوصية. وبالتالي يختلف الدليل الرقمي عن الآثار المادية الناتجة عن الجرائم التقليدية كالأعيرة والأسلحة النارية أو المحرر ذاته الذي تمّ تزويره، ممّا يسهل على رجال العدالة إثباتها، بعكس الجرائم الالكترونية حيث يكون ذلك في منتهى الصعوبة، بل الدليل فيها ــ الدليل الرقمي ــ عبارة عن نبضات الكترونية مكوّنة من سلسلة طويلة من الأصفار، لا تفصح عن شخصية معينة، وهذه المشكلة تظهر بصفة جلية مع شبكه الانترنت حيث تسمح لمستخدميها الاتصال بدون الكشف عن أسماءهم الحقيقية كإرسال رسائل البريد الالكتروني مجهولة المصدر.

فضلا عن ذلك غالبا ما يكون الدليل الرقمي مرمّزا أو مشفرا، كما يمكن تعديله والتلاعب فيه، مما يقطع الصلة بين المجرم وجريمته، ويحول دون كشف شخصيته، وبذلك يشكل هذا الدليل عائقا أمام رجال التحرّي والتحقيق خاصة أنهم اعتادوا على الإثبات المادي للجرائم.

2 ــ مشكلة الأصالة في الدليل الالكتروني:

إنّ الأصالة في الدليل الالكتروني لها طابع افتراضي لا يرتقي إلى مستوى الأصالة في الدليل المادي، فهذه الأخيرة تعبير عن وضعية ماديّة ملموسة، كما هو الشأن في الورق المكتوب أو بصمة الأصبع، في حين أن الدليل الرقمي عبارة عن تعداد غير محدود لأرقام ثنائية (Binary Digits) موحدة في الصفر و الواحد (0-1) فالصورة (Image) مثلا في العالم الرقمي ليس لها ذلك الوجود

(1) -Computer Forensics Procedures, Tools, and Digital Evidence , Bags Brett Pladna What They Are and Who Should Use Them. available at: http://www.infosecwriters.com/text_resources/pdf/BPladna_Computer_Forensic_Procedures.pdf

(2) -Johann Hershensohn,I.T. FORENSICS: THE COLLECTION AND PRESENTATION OF DIGITAL EVIDENCE, available at: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf

المادي الذي نعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فكل شيء في العالم الرقمي يتكوّن من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة. ولقد أثارت مسألة الأصالة العديد من المشكلات من حيث مدى الاعتداد بالنسخة التي تشكل دليلا كاملا هنا[1].

الواقع من الأمر أنّ بحث موضوع الأصالة على المستوى القانوني جعل المشرع المقارن يعتمد منطق **افتراض أصالة الدليل الالكتروني**، وقد تضمن قانون الإجراءات الجنائية الفدرالي في الولايات المتحدة الأمريكية نصا صريحا (القاعدة 1001بند (3)) حيث يسمح استثناء بقبول الدليل الالكتروني باعتباره مستندا أصليا مادام أن البيانات صادرة من كمبيوتر أو جهاز مماثل وسواء أكانت هذه البيانات مطبوعة أم مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبّر عن البيانات الأصلية بشكل دقيق[2]. ومنه تتساوى الكتابة الماديّة من حيث الأصالة مع مخرجات الحاسوب على الرغم من أنّ طبيعة الكتابة عبر الحاسوب تجعل من المخرجات مجرد نسخ للأصل الموجود رقميا في الحاسوب أو عبر الانترنت.

3 ــ الدليل الالكتروني ذو طبيعة ديناميكية:

فالدليل الالكتروني ينتقل عبر شبكات الاتصال بسرعة فائقة، حيث يمكن تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد، ويترتب على ذلك صعوبة تعقّب الأدلة الرقمية وضبطها، لأنّه يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها[3]، مثل معاينة مواقع الانترنت المخالفة، تفتيش نظم الحاسب الآلي، أو ضبط الأقراص الصلبة التي تحتوي على مواد غير مشروعة كالصور الإباحية مثلا، وهذا كله يصطدم بمشاكل الحدود والولايات القضائية، ويرجع السبب في ذلك إلى أنّ هذه الإجراءات تمثل مساسا بسيادة الدولة التي

---

(1)ــ عائشة بن قارة مصطفى، مرجع سابق، ص 252.

(2) -Pascal Vergucht , op. cit, p. 120.

(3) – Marthew. R .Zakaras, International Computer Crime , revue international de droit pénal, 3eme et 4eme trimestres 2001 , p 828 .

عبر من خلالها نشاط المجرم وهو في طريقه للهدف، أو حيث قد توجد أدلة الجريمة، وهو ما ترفضه الغالبية العظمى من الدول، لذلك أبرمت العديد من الاتفاقيات والمعاهدات الدولية في مجال التعاون الدولي[1] التي تستهدف من وراء ذلك التقريب بين القوانين الجنائية الوطنية من اجل جمع هذا النوع من الأدلة العابرة للحدود خاصة في إطار مكافحة الجرائم العالمية ومنها الجرائم الالكترونية .

ثانيا ــ المشكلات الإجرائيّة للدليل الالكتروني:

لا تقف مشكلة الدليل الالكتروني عند طبيعته التكوينية، بل تمتد لتشمل إجراءات الحصول عليه، وتتمثل هذه الأخيرة في حالتين هما: ارتفاع تكاليف الحصول عليه، ممّا أدى إلى القول بأنّ الدولة، على الرغم من أنّ مسعاها الحقيقي هو تحقيق العدالة، لن تلجأ إلى أسلوب الإنفاق في هذا الإطار[2]. أمّا المشكلة الثانية تتعلق بنقص الخبرة الفنية والتقنية لدى سلطات الاستدلال والتحقيق والقضاء بمجال تقنية المعلومات. كل ذلك سنتعرض له من خلال التالي:

1 ــ ارتفاع تكاليف الحصول على الدليل الالكتروني:

غالبا ما يتمّ اللجوء إلى الخبرة في مجال التعامل مع أيّ ظاهرة فنية، لاسيما في مجال تكنولوجيا المعلومات والانترنت، فهي تؤدي دور لا يستهان به إزاء نقص معرفة رجال إنفاذ القانون للجوانب

---

(1) ــ مثل الاتفاقية الأوربية للإجرام المعلوماتي (اتفاقية بودابست) الموقعة في 2001/11/23 , حيث تمّ تخصيص الباب الثالث لدراسة التعاون الدولي Coopération International ، ومن خلاله نصت **المادة 23** "على ضرورة تعاون الأطراف فيما بينها وفقا لأحكام هذا الفصل، ومن خلال تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المسائل الجنائية و الترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بالنسبة للقوانين المحلية، إلى أقصى مدى ممكن، بغرض التحقيقات والإجراءات الجنائية المتعلقة بالجرائم ذات الصلة بالنظم الحاسوبية والبيانات المعلوماتية، أو لجمع الأدلة ذات الشكل الالكتروني لمثل هذه الجرائم " .

Article 23 . General principles relating to international co-operation:

"The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence".

(2) ــ عمر محمد ابوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق ، ص 984 .

التقنية في الجرائم الالكترونية، إلاّ أنّ هذه الخبرة تشكل عبئا ثقيلا على العدالة الجنائية بالنظر إلى حجم وضخامة المصاريف التي يتمّ إنفاقها في سبيل الحصول على الدليل الرقمي، وان كان الإنفاق يتفاوت حسب ما إذا كانت الدولة تأخذ بالنظام الاتهامي أو بنظام التنقيب والتحري[1]، غير أن الإشكال الأساسي لا يتعلق بطبيعة النظام الإجرائي المتّبع في كل دولة، و إنّما ينحصر في طبيعة الدليل الرقمي وما يتطلب إثباته من تكاليف باهظة، خاصة أمام غياب منظمات متخصصة كالجامعات والمعاهد لاسيما في الدول العربية حيث يتطلب الأمر اللجوء إلى شركات أو منظمات أجنبية في الخارج، ممّا يجعل التكاليف تخضع للسعر العالمي المقرر في اللوائح المالية لتلك المنظمات .

لذلك نقترح إنشاء مخابر معتمدة تابعة للأجهزة العدالة الجنائية، تكون مجهزة بأحدث وسائل التقنية، مع ضرورة تبادل المعلومات مع المراكز والمؤسسات الأجنبية حكومية كانت أم خاصة حتى تستفيد من خبراتها في المجال التقني لاسيما تجربة الولايات المتحدة الأمريكية باعتبارها من الدول السباقة في هذا المجال، وذلك عن طريق الندوات والمؤتمرات، فضلا عن دورات تدريبية وذلك في إطار التعاون الدولي الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين الدول المختلفة.

2 ــ نقص المعرفة التقنية لدى رجال إنفاذ القانون:

إنّ الطبيعة الخاصة بالدليل في مجال الجريمة الالكترونية انعكس على عمل الجهات المكلّفة بالتحقيق والمحاكمة حيث يتطلّب الكشف عن هذه الجرائم وإثباتها إتباع استراتجيات خاصة تتعلق باكتسابهم مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته، بحيث تتعقد التقنيات المرتبطة بارتكاب تلك الجرائم لذا يجب استخدام تقنيات تحقيق جديدة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبيها و كيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجاني والحصول على أدلة إدانته[2]. لذا من المتصور أن تجد الجهات المكلفة بالقبض والتحقيق نفسها غير قادرة على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، فكثيرا ما تفشل جهات التحقيق في جمع الأدلة الالكترونية، بل أنّ المحقق نفسه قد يدمّر الدليل بخطأ منه

(1) ــ عمر محمد أبوبكر بن يونس، نفس المرجع، ص 987 .

(2)-YANN PADOVA ,op. cit. p ,772 .

أو بإهمال، كقيام رجال 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 تسببت في تدميرها جميعا [1].

لذا يجب أن تنشأ كل دولة إدارة متخصصة بهذا النوع من القضايا، وذلك لتلقي البلاغات وملاحقة المجرم الالكتروني والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة [2].

الفرع الثالث: موقف المشرع الجزائري من الدليل الإلكتروني في الإثبات الجزائي

نصّت المادة 212 من قانون الإجراءات الجزائية على أنه "يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لإقتناعه الخاص..." كما نصت المادة 307 من القانون ذاته " أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم...".

من خلال هذين النصين القانونيين يتضح جليا أن المشرع الجزائري قد تبنى كقاعدة عامة نظام الإقتناع الشخصي للقاضي الجزائي، واستثناء نجده أخذ أيضا بنظام الأدلة القانوية في إثبات بعض الجرائم[3].

بتحليل المادة 212 من قانون الإجراءات الجزائية تكرس قاعدتين تكمل إحداها الأخرى، قاعدة الإقتناع الجزائي من جهة وقاعدة حرية إختيار وسائل الإثبات الجزائي من جهة أخرى.

وإذا كان الدليل الإلكتروني إحدى تطبيقات الدليل العلمي، فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الإقتناع الشخصي حيال هذا الدليل طبقا لأحكام المادة 212 من قانون الإجراءات الجزائية؟.

---

[1] ــ عبد الله حسين محمد، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002، ص 355.

[2] ــ رأفت رضوان، شرطة الانترنت، بحث منشور بمجلة بحوث الشرطة، العدد 26، يوليو 2004، ص111.

[3] ــ أنظر المادتين 342، 339 من قانون العقوبات الجزائري.

لقد سبق الذكر أن الجريمة المعلوماتية في القانون الجزائري طبقا للمادة الثانية فقرة (أ) من قانون (09ـــ 04) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكمولوجيات الاعلام والاتصال ومكافحتها السابق الذكر، تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكذا كل جريمة آخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للإتصالات الإلكترونية، والقاضي في إطار تقديره للدليل الألكتروني ملزم باحترام ومراقبة القواعد العامة المنظمة لطرق استخلاص الدليل الإلكتروني سواء كانت هذه الطرق تقليدية أو حديثة، فبالنسبة للتفتيش المعلوماتي مثلا فالقاضي يتحقق من مدى صحة محاضر التفتيش من حيث الشكل، وأنه قد تم إعداده من طرف واضعه أثناء مباشرة وظيفته، ويكون مضمونه يدخل في اختصاصه[1].

أمّا بالنسبة لتقارير الخبرة فإن المحكمة العليا ذهبت للقول أن الخبرة شأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع[2]، وهذا ما تؤكده المادة 212 من قانون الإجراءات الجزائية التي تنص على أنه: ''لا تعتبر التقارير المتبثة للجنايات أو الجنح إلا مجرد إستدلالات...''

لكن الطبيعة العلمية والتقنية للجريمة المعلوماتية غالبا ما تفرض على القاضي الإستناد في تكوين إقتناعه على الخبرة الفنية والتقيد بالنتيجة المتوصل إليها من الخبير في تقرير خبرته ولا يمكنه طرحها وإستبعادها إلا إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلمية [3].

[1] ـــ أنظر المادة 214 من قانون الإجراءات الجزائية الجزائري.

[2] ـــ قرار المحكمة العليا المؤرخ في 11/ 07/ 1995 المنشور في نشرة القضاء رقم 58 لسنة 2006، ص 170.

[3] ـــ قرار المحمة العليا الغرفة الجنائية، مؤرخ في 04/ 06/ 2002، نشرة القضاء رقم 58 لسنة 2006، ص 255.

الخاتمة

في ختام هذه الدراسة، يظهر جليا أنّ المعاملات الإلكترونيّة الحكوميّة معرّضة للعديد من المخاطر، سيما وأنّ التقدم المعلوماتي في تطوّر مستمر، وأنّ وحدات الجهاز الإداري للدولة تتعامل في مستندات ووثائق حيويّة ذات أهمّية بالغة للدولة وللمواطنين معا، وأنّ إساءة استخدام هذه البيانات قد يفقد ثقة الجمهور بالحكومة الالكترونية ويزيد الفجوة النفسيّة القائمة بين المواطنين والحكومة، الأمر الذي يشكل عقبة أمام مخططات ومشاريع الحكومة الالكترونية بمختلف دول العالم ومنها الجزائر التّي بدأت تخطوا خطواتها الأولى نحو تطبيق مشروع الحكومة الإلكترونية والذي من خلاله يتمّ السعي إلى استخدام تقنيات المعلومات والإتصالات الإلكترونية في توفير وتقديم معلومات وخدمات حكومية للمواطنين وجعلها متاحة للجمهور.

وإذا كانت الدولة هي المعني الأوّل بأمن المعلومات والبيانات على الشبكة لأنها المزود الأكبر بهذه المعلومات وهي مقدم الخدمة للمواطنين ولقطاعات الأعمال، في مقابل ذلك هي من يتولّى تحديد وفرض قواعد التعامل التقني بالشبكة، بالإضافة إلى تفعيل نظم الحماية.

ولتحقيق الأمن المعلوماتي في نظام الحكومة الإلكترونية يتطلب الأمر:

أولا: صياغة تشريع على نحو يحدد السلوكات المحظورة فيبينها ويفرد لها العقاب، وهو ما يعرف بالحماية الجزائية الموضوعية.

أما الثاني: فيُرد إلى آليات التطبيق والمتابعة القضائية لمختلف صور الاعتداءات الواقعة على العمل الحكومي الإلكتروني، وذلك في إطار الحماية الإجرائية للمعاملات الحكومية الالكترونية وآليات تنفيدها.

فعلى **مستوى الشّق الموضوعي** من الحماية الجزائية، لم تخصّ التشريعات العقابية المقارنة حماية جنائية خاصّة للمعاملات الإلكترونية الحكوميّة، بل يمكن حمايتها في إطار القواعد العامة لقانون العقوبات، وهو النّهج المتّبع عند المشرّع الجزائري، حيث تدخل من خلال المواد 394 مكرر إلى المادة 394 مكرر 7 من قانون العقوبات، التي وردت في القسم السابع مكرر منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، بالإضافة إلى ذلك خصّص المشرع الجزائري أيضا بعض

القواعد الخاصة لحماية هذا النوع من المعاملات كالقانون رقم (15ـــ04) المتضمّن القواعد العامة للتوقيع والتصديق الالكترونيين .

ومن خلال البحث عن صور الاعتداء المعلوماتي على الحكومة الالكترونية والتي تمّ تقسيمها إلى جرائم واقعة على المعاملات الالكترونية، وأخرى واقعة على وسائل إجراء هذه المعاملات، يتّضح أنّ المشرّع الجزائري لم يتعرض لجريمة الاعتداء على سير النظام المعلوماتي للحكومة الإلكترونية كجريمة مستقلة قائمة بذاتها، بل اكتفى بإفساد النّظام كظرف مشدد فقط لجريمة الدخول أو البقاء غير المشروع في المادة 394 مكرر/2 من قانون العقوبات الجزائري، بخلاف المشرّع الفرنسي حيث نص عليه بموجب المادة 2/323 من قانون العقوبات الفرنسي.

ولهذا يتعيّن على المشرّع الجزائري استحداث نصّا خاصا بالاعتداء على سير نظام المعالجة الآلية للمعطيات بما في ذلك نظام الحكومة الالكترونية.

كما تبيّن أيضا أنّ المشرّع الجزائري نظّم عمل مقدمي خدمات الانترنت، باعتبارهم وسطاء في تقديم خدمة الانترنت للعميل في الوصول إلى شبكة الانترنت، وأقرّ قواعد خاصة فيما يتعلق بالمسؤولية الجنائية، في حالة اخلالهم بالالتزامات العامة منها أو الخاصة، غير أنّه لم يحدّد طبيعة المتدخل المهني الذي يكون عرضة للتجريم والمساءلة القانونية.

لذلك ينبعي تحديد مسؤولية كلّ متدخل مهني على حدا، من متعهّد خدمة الوصول إلى متعهّد الإيواء وصولا إلى مورد المعلومات، وذلك تماشيا مع التشريعات الأوربيّة، كالتشريع الفرنسي والألماني، وكذا التشريعات الأمريكية.

وكما هو معلوم أنّ التعامل في إطار نظام الحكومة الالكترونية يزخر بالبيانات الشخصية الرسمية وضمن شبكات اتصال مفتوحة، الأمر الذي يتطلب توفير حماية خاصّة لهذه البيانات، وهو ما فعله المشرع الفرنسي الذي حماها جنائيا بنصوص خاصة في إطار قانون العقوبات، بخلاف المشرّع الجزائري الذي لم يقنّن بعد تشريع خاص يهدف إلى حماية البيانات الخاصة، باستثناء بعض النصوص المجزأة بين قانون العقوبات وقانون التوقيع والتصديق الالكترونيين رقم(15 ــ 04).

لذلك يستحسن تدخل المشرع الجزائري لاستحداث نصوص قانونية ضمن قانون العقوبات في الباب الأول المتعلق بالجنايات والجنح ضد الأشخاص، وذلك في القسم الخامس مكرر 3 تحت إسم "الاعتداء على البيانات الشخصية"، حيث يرصد مختلف صور الاعتداء على البيانات الشخصية، وتحديد مختلف العقوبات الملائمة التّي من شأنها إحداث الردع العام والخاص.

ولتوفير ثقة أكبر في المتعاملين بالمحررات المعلوماتية الرسمية ينبغي تدخل تشريعي لحمايتها من جريمة التزوير المعلوماتي. وفي هذا الاطار تعددت الصيغ التشريعية في تجريم الوثيقة المعلوماتية بين اتجاه يوسع في الصيغة ليشمل كل تزوير في وثيقة ذات قيمة قانونية مهما كانت طبيعتها ورقية أو معلوماتية، وهي خطة المشرع الفرنسي من خلال المادة 1/441 من قانون العقوبات الفرنسي الجديد لسنة 1994. في حين أبقت بعض التشريعات ومنها الجزائر على نصوص التزوير التقليدي ليثار الجدل في مدى امتداد هذه النصوص ليشمل التزوير في الوثيقة المعلوماتية.

وبهذه يتعين على المشرع الجزائري الاسراع إمّا:

ـــ بإضافة نص إلى باب التزوير في المحررات، حيث يتناول هذا النص تعريف جريمة التزوير وأساسها ألا وهو المحرر وذلك على الشكل التالي: "المحرر هو كل مركب يتكون من حروف أو علامات تدل على فكرة معينة بالنظر إليها مباشرة أو بالإستعانة بتقنية أخرى"، وبذلك يشمل هذا النص المحررات التقليدية والمعلوماتية معا كالمستندات الموجودة على الأقراص والأشرطة.

ـــ أو بإدراج نص خاص بالتزوير المعلوماتي.

ولتحقيق أكبر قدر ممكن من سريّة وسلامة المعاملات والمعلومات التي تحويها وتأكيد هوية وشخصية صاحبها بدقة استعانت أغلب الدول بالتوقيع الالكتروني واعترفت به قانونا، حيث أصبح من أهم أدوات التعاملات الالكترونية، لما يوفّره من الأمان القانوني من خلال الإجراءات التقنية العالية التّي يعتمد عليها، وهو ما دفع المشرّع الجزائري إلى الإعترف بقيمته وصلاحيته للإثبات بنص صريح.

ومن أجل ضبط التعامل بالتوقيع الالكتروني قام المشرع الجزائري ولأوّل مرّة بتوفير حماية جنائية خاصة للتوقيع الالكتروني بموجب القانون رقم (15 ــ 04) الذي يحدّد القواعد العامة للتوقيع والتصديق الالكترونيين، بخلاف المشرّع الفرنسي الذي لازال يطبق القواعد العامة لقانون العقوبات، من خلال جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وجريمة التزوير.

كما أصبحت بطاقة الدفع الإلكتروني من أهم الآليات المستحدثة في إجراء المعاملات الحكومية الالكترونية، كونها تشكل دعامة قانونية على صعيد الوفاء والائتمان، نظرا لما تشهده هذه البطاقات من تطور سريع. ولأجل ذلك وفّرت أغلب التشريعات المقارنة حماية جنائية كالتشريع الكندي الصادر سنة 1985، أو التّشريع الفرنسي الذي استحدث قانون أمن الشيكات، وبطاقات الوفاء رقم 91/ 1382. بخلاف المشرع الجزائري الذي لازال يطبق القواعد العامة لقانون العقوبات على الجرائم الواقعة على هذه البطاقة. حيث لازال مصطلح الدفع الالكتروني غريبا عن التشريع الجزائري، ولذلك:

يجب على المشرع الجزائري التدخل لوضع قواعد قانونية صارمة تعمل على حماية بطاقات الدفع الالكتروني حتى تكون في مأمن من إساءة استخدامها.

وعلى الرغم من تجريم بعض أفعال الاعتداء التي تقع في مجال تقنية المعلومات ووضع العقوبات الرادعة لها، فهي لا تكفي لحماية نظام الحكومة الالكترونية وإنما يلزم وضع نظام وقائي متكامل يعرف بالأمن الإلكتروني، وذلك عن طريق:

ــ التحديث المستمر لأنظمة التشغيل للحاسبات الآلية، مرفقة في ذلك بالبرامج المضادة للفيروسات.

ــ تركيب جدار ناري (Firewall) بين المستفيدين ومصادر المعلومات المتواجدة في قاعدة البيانات الحكومة الالكتروني، فهذا الجدار عبارة عن برنامج خاص يتولى فحص كل البيانات والمعلومات الواردة من الأنترنت، ثم بعد ذلك يقوم بالسماح لها بالدخول إذا كانت متوافقة مع

إعدادات جدار الحماية، أو باستبعادها إذا كانت من البرامج الخبيثة مثل الفيروسات، وبرامج التجسس...إلخ.

ـــ عمل نسخ إحتياطية للمعلومات الهامة وحفظها في أماكن آمنة.

ـــ ينبغي أن تتكون كلمة المرور من ست خانات على الأقل. وأن تكون مزيجا من الأحرف والأرقام، ويفضل عدم التكرار.

ـــ تدريب الموظف العام حول وسائل حماية خصوصية وسرية بيانات المواطنين بشكل منتظم ومتواصل.

أما على **مستوى الشق الإجرائي** من الحماية، فقد تبيّن وجود صعوبة في إثبات الجرائم الواقعة على الحكومة الالكترونية ومنها الجرائم المعلوماتية، وذلك بالنظر إلى الطبيعة الفنيّة المعقّدة لهذه الجرائم، مما أضفى عليها نوعا من الخصوصيّة في كل مراحل الدعوى العمومية بدءا من مرحلة جمع الأدلة، التحقيق الإبتدائي، إلى مرحلة المحاكمة.

فيما يخص مرحلة جمع الأدلة (التحقيق الأولي) التي تعدّ من أهم المراحل التّي يستعان بها في مواجهة الجرائم المعلوماتية، تمّ تسخير ضبطية قضائية مختصة سواء على المستوى الدولي أو الداخلي وحتى الوطني، حيث خصص المشرع الجزائري ضبطية على مستوى جهاز الشرطة، وأخرى على مستوى الدرك الوطني، بالإضافة إلى إنشاء هيئة متخصصة في مكافحة هذه الجرائم وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب القانون رقم (09 ـــ04) المتعلق بالقواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وما يميّز هذه الضبطيّة عن الضبطية القضائية في الجرائم التقليدية، أنها لا تعتمد على التدريبات المادية والفيزيولوجية، وإنّما تعتمد على التكوين في مجال المعلوماتية وتكنولوجيات الاتصال.

ونظرا للطبيعة اللامادية لهذه الجرائم المستحدثة، لم تعدّ أساليب البحث والتحرّي التقليديّة كافية لمواجهة هذه الجرائم، مما استدعى بالمشرع الجزائري إلى استحداث أساليب تحرّي خاصّة عن الجرائم

الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك من خلال القانون رقم (06 ــ 22) المعدل لقانون الإجراءات الجزائية، وتتمثل هذه الإجراءات في عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وعملية التسرب.

كما تبّين أن الدليل المناسب في إثبات الجرائم الواقعة على الحكومة الكترونية هو الدليل الالكتروني، وهو عبارة عن معلومات مخزّنة في أجهزة الحاسوب وملحقاتها، أو متنقلة عبر شبكات الاتصال، والذي يتمّ تجميعه وتحليله باستخدام برامج وتطبيقات خاصّة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها.

لأجل الحصول على الدليل الالكتروني ثمة نوعين من القواعد الإجرائية لاستخلاصه، طرق إجرائية تقليدية تتمثّل في التّفتيش، الضبط والخبرة، وأخرى مستحدثة تتلاءم مع الطبيعة الفنيّة للدليل الالكتروني كحفظ المعطيات المتعلقة بحركة السّير، واعتراض الاتصالات الالكترونية، وهو ما قام به المشرع الجزائري فعلا بموجب القانون رقم(09 ــ04) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإتصال ومكافحتها.

فالجزائر إذن تعدّ من أولى الدول العربية في سن قواعد إجرائية خاصة في مواجهة ظاهرة الإجرام المعلوماتي، وإن كان الكثير من الدول لاتزال تخضع هذه الجرائم للنصوص الإجرائية التقليدية، وهو ما يترتب عليه إفلات الجناة من العقاب.

وعليه أصبح من المقرر في التشريع الجزائري جواز التفتيش لضبط المعلومات على الرغم من طبيعتها المعنوية، وذلك وفقا للمادة الرابعة من قانون (09 ــ04) السابق الذكر، وذلك في إطار ضمانات موضوعية وشكلية تحمي الحق في خصوصية الأفراد من الانتهاكات.

ويترتب على ذلك أن يكون مصدر الإذن بالتفتيش أو منفذه على دراية تامة بالأمور الفنية لأجهزة الحاسب الآلي، ولا يتحقق ذلك إلا من خلال عقد دورات تدريبية لرجال الضبط القضائي وكل أجهزة إنفاذ القانون بأساليب الضبط وجمع الأدلة والتحقيق في هذه النوعية من الجرائم وذلك بصفة دورية ومنتظمة لمواكبة التطور التكنولوجي.

وفي إطار التحقيق عن الجرائم الواقعة على الحكومة الالكترونية، تبيّن وجود صعوبات تعرقل المحقق عن عمله، بسبب خصوصية هذه الجرائم، مما تطلّب الأمر ضرورة تحديد الإجراءات الواجب اتباعها في التحقيق وتقنيات التحفظ على الأجهزة المستخدمة في ارتكاب هذه الجرائم، على أن يكون ذلك متاح في دليل خاص (un guide) بالبحث والتحقيق عن هذه الجرائم، يُعِده خبراء مختصين في مجال التقنية المعلوماتية.

ولأنّ الجرائم الواقعة على الحكومة الالكترونية هي جرائم عابرة للحدود الوطنية للدولة، بل القارات ممّا يجعل خطورتها غير محصورة في النطاق الإقليمي لدولة بعينها، الأمر الذي أصبح يثير العديد من التحديات القانونية المتمثلة في تحديد المحكمة المختصة بالفصل في هذه القضايا.

في هذا الإطار مدّد المشرّع الجزائري الاختصاص في هذه الجرائم بموجب القانون رقم (04 ــ14) المعدّل والمتمّم لقانون الإجراءات الجزائية الجزائري، والمرسوم التنفيدي رقم (06 ــ 348) المتضمّن تمديد الاختصاص المحلّي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق والتعديلات اللاحقة عليه بموجب المرسوم التنفيذي رقم (16 ــ 267). غير أن هذا الامتداد داخلي وليس خارجي، بمعنى لا يتعدى حدود دولة الجزائر، بخلاف بعض الدول مثل فرنسا والولايات المتحدة الأمريكية التي جعلت الإختصاص لمحاكمها الوطنيّة حتى ولو وقعت الجريمة المعلوماتية في الخارج، طالما تحققت آثارها في الداخل.

لذلك ينبغي على المشرع الجزائري وضع قواعد تُوسّع من اختصاص المحاكم حتى ولو وقعت الجريمة خارج الدولة، لأن تطبيق القواعد العامة في المواد 582 و589 من قانون الإجراءات الجزائية والمادة 15 من القانون رقم (09ــ 04) السابق الذكر غير كافية.

ومع ذلك نلاحظ توجه المشرع الجزائري نحو التخصص القضائي من خلال إنشاء هيئات قضائية متخصصة على مستوى النيابة العامة، التحقيق والمحاكمة تستأثر بالجرائم الخطيرة على غرار جرائم المساس بأنظمة المعالجة الآلية للمعطيات، في شكل أقطاب متخصصة توضع على مستوى المحاكم التي يتمّ توسيع اختصاصها المحلي ليشمل اختصاصا إقليميا لمحاكم أخرى محددة قانونا.

وفيما يخصّ مسألة مدى حجية الدليل الالكتروني في الإثبات الجنائي، اتضح أنّ مبدأ حرية الإثبات أساس قبول الدليل الإلكتروني في الإثبات الجنائي، عند الدول ذات الأصل اللاتيني وغيرها من الدول المتأثرة بها كالجزائر، وذلك بخلاف النظام الأنجلو أمريكي، الذي يتقيد فيه القاضي الجنائي بقاعدة الإثبات المقيد، ويُقبل فيه الدليل الالكتروني استثناء عن قاعدة عدم قبول الشهادة السماعيّة.

هذا وعلى الرغم من القيمة العلميّة القاطعة للدليل الالكتروني، يبقى هذا الدليل شأنه شأن باقي الأدلة يخضع للسلطة التقديريّة للقاضي الجنائي، للتحقق من ضمان احترام ضابط المشروعية في الحصول عليه، وبالتالي يظل القاضي هو المسيطر على هذه الحقيقة، ويّفسر الشك لصالح المتهم.

وعليه نفترح في الأخيرا ضرورة تدخل المشرع الجزائري لإحداث قانون خاص بالمعلوماتية، يكون شاملا، يتضمن مختلف القواعد الجزائية الموضوعية والإجرائية للجرائم المعلوماتية، وبالتالي يكون مرجعا أساسيا يهتدي به القاضي وكل السلطات القضائية عند معالجة هذا النوع المستحدث من الإجرام.

قائمة المراجع

أولاـــ المراجع باللغة العربية:

أ ـــ الكتب العامة

1. **أحمد شوقي الشلقاني**، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999.
2. **أحمد بوسقيعة**، الوجيز في القانون الجزائي الخاص، الجزء الأول، دار هومة، الجزائر، 2014.
3. **أحمد عوض بلال**، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائيّة المقارنة، الطبعة الثانيّة، دار النهضة العربيّة، القاهرة،2006.
4. **أحمد فتحي سرو ر**، الوسيط في قانون الإجراءات الجنائية دار النهضة العربية، القاهرة، الطبعة الثانية،1981.
5. **أحمد فتحي سرور**، أصول الإجراءات الجنائيّة، دار النهضة العربية، القاهرة، 1969.
6. **بيل جيتس**، المعلومة بعد الانترنت: طريق المستقبل، ترجمة عبد السلام رضوان، المجلس الوطني للثقافة والفنون والآداب، الكويت، 1998.
7. **حسن صادق المرصفاوي**، أصول الإجراءات الجنائيّة في القانون المقارن، منشأة المعارف، الاسكندرية، 1982.
8. **جباري عبد المجيد**، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الطبعة الثانية، الجزائر، 2013.
9. جلال ثروث، نظم الإجراءات الجنائية، دار الجامعة الجديدة، الاسكندرية، 2003.
10. **رؤوف عبيد**، المشكلات العمليّة الهامة في الإجراءات الجنائيّة، الجزء الأول، الطبعة الثانيّة، دار الفكر العربي، 1963.
11. **رؤوف عبيد**، مبادئ الإجراءات الجنائيّة في القانون المصري، دار الفكر العربي، الاسكندرية، 2006.
12. **رؤوف عبيد**، مبادئ القسم العام في التشريع العقابي، دار الفكر العربي، الطبعة الأولى، القاهرة، 2008.

13. **عبد الله أوهايبية**، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر، الجزائر، 2003.

14. **عدنان الخطيب**، موجز القانون الجزائي، الكتاب الأول، المبادئ العامة في قانون العقوبات، مطبعة جامعة دمشق، 1963.

15. **علاء الدين محمد فهمي وآخرون**، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، 1991.

16. **علي عبد الله سليمان**، شرح قانون العقوبات الجزائري: الجريمة، ديوان المطبوعات الجامعية، 2002.

17. **علي عبد الله سليمان**،، شرح قانون العقوبات، (القسم العام)، الجزء الأول: الجريمة، دار الهدى للطباعة والنشر والتوزيع، 2003،

18. **عوض محمد عوض**، قانون الإجراءات الجنائي، الجزء الأول، مؤسسة الثقافة الجامعية، 1989.

19. **عز الدين الدناصوري، عبد الحميد الشواربي**، المسؤولية المدنية في ضوء الفقه والقضاء، دار الفكر العربي، 2012، مصر.

20. **فتوح عبد الله الشاذلي**، القانون الدولي الجنائي، الكتاب الأول: أوليات القانون الدواي الجنائي، دار المطبوعات الجامعية، الاسكندرية، 2001

21. **مأمون سلامة**، شرح قانون الإجراءات الجنائية، دار الفكر العربي، 1998.

22. **محمد زكي أبو عامر**، الإجراءات الجنائيّة، دار الجامعة الجديدة، الطبعة الثانية، الاسكندرية، 2002.

23. **محمد محمد الهادي**، الشارح لمصطلحات الكمبيوتر (إنجليزي ـــ عربي)، دار المريخ للنشر، دون دار النشر، 1988.

24. **محمد مروان**، وسائل الإثبات في المواد الجنائيّة في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعيّة، الجزائر، 1998.

25. **محمود محمد مصطفى**، شرح قانون الإجراءات الجنائيّة، مطبعة دار النشر الثقافة، الطبعة الثانية، القاهرة، 1953.

26. **محمود محمود مصطفى**، الإثبات في المواد الجنائية في القانون المقارن، الجزء الثاني، التفتيش والضبط، الطبعة الأولى، مطبعة جامعة القاهرة، 1978.

27. **محمود نجيب حسني**، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988.

28. **محمود نجيب حسني**، شرح قانون العقوبات، القسم الخاص، وفقا لأحدث التعديلات، دار النهضة العربية، القاهرة، 2012

29. **محمود نجيب حسني**، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، ط. 4 ، دار النهضة العربية ، 1977.

30. **معوض عبد التوّاب**،الوسيط في أحكام النقض الجزائيّة، مركز الوثائق والدراسات الانسانية، دون سنة الطبع.

31. **مولاي ملياني بغدادي**، الخبرة القضائيّة في المواد المدنيّة، مطبعة حلب، الجزائر، 1992.

32. **نبيل صقر ومكاري نزيهة**، الوسيط في القواعد الإجرائية والموضوعية للإثبات في المواد المدنية، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009.

33. **نصر الدين ماروك**، النظرية العامة للإثبات الجنائي، الجزء الأول، دار هومة، 2004.

ب ــ الكتب المتخصصة:

1. **أحمد الخليفة الملط**، الجريمة المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، الاسكندرية، 2006.

2. **أحمد سقر**، أنظمة الدفع الإلكترونية، منشورات الحلب الحقوقية، الطبعة الأولى، لبنان، 2008.

3. **أسامة أحمد المناعسة**، جلال محمد الزعبي، الحكومة الإلكترونية بين النظرية والتطبيق، دار الثقافة للنشر والتوزيع،الطبعة الأولى، الأردن، 2013.

4. **أسامة قايد**، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1998.

5. **أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الالكتروني، دار النهضة العربية، الطبعة الأولى، القاهرة، 2006.

6. **أمال قارة**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الأولى، 2007.

7. **إيهاب فوزي السقا**، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2008.

8. **برهامي أبوبكر عزمي**، الشرعيّة الإجرائيّة للأدلة العلميّة، دراسة تحليليّة لأعمال الخبرة، دار النهضة العربيّة، القاهرة، 2006.

9. **بشير علي الباز**، دور الحكومة الإلكترونية في صناعة القرار الإداري والتصويت الإلكتروني، دار الكتب القانونية، مصر، 2009.

10. **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.

11. **جميل عبد الباقي الصغير**، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2001.

12. **جميل عبد الباقي الصغير**، الجوانب الإجرائية لجرائم الانترنت، دار الفكر العربي، القاهرة، 2001.

13. **جميل عبد الباقي الصغير**، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، مصر، 2003.

14. **جميل عبد الباقي الصغير**، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، 1992.

15. **جهاد رضا الحباشنة**، الحماية الجزائية لبطاقة الوفاء، دار الثقافة عمان، الأردن، 2008.

16. **حسن طاهر داود**، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000.

17. **حسين بن سعيد سيف الغافري**، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.

18. **خالد ممدوح إبراهيم**، أمن الحكومة الإلكترونية، الدار الجامعية، الإسكندرية، 2008.

19. **خالد ممدوح إبراهيم**، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009.

20. **خثير مسعود**، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، الجزائر، 2010.

21. **الخليل عماد علي**، الحماية الجزائية لبطاقة الوفاء، دار وائل للطباعة والنشر، الطبعة الأولى، عمان، الأردن، 2000.

22. **رامي عبد العزير**، الفيروسات وبرامج التجسس، دار البراء، الاسكندرية، 2005.

23. **رمزي رياض عوض**، سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية، الطبعة الأولى، 2010.

24. **سليمان أحمد فاضل**، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت، دار النهضة العربية، القاهرة،2007.

25. **شريف محمد غنام**، التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، 2008.

26. **شيماء عبد الغني محمد عطا الله**، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، 2007.

27. **طوني ميشال عبسى**، التنظيم القانوني لشبكة الانترنت، صادر ناشرون، بيروت، لبنان، الطبعة الأولى، 2001.

28. **عائشة بن قارة مصطفى**، حجية الدليل الالكتروني في مجال الإثبات الجنائي في التشريع الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية،2010.

29. **عادل رمضان الأبيوكي**، التوقيع الإلكتروني في التشريعات الخليجية (دراسة مقارنة)، المكتب الجامعي الحديث، الاسكندرية، 2009.

30.**عباس بدران**، الحكومة الإلكترونية من الإستراتيجية إلى التطبيق، المؤسسة العربية للدراسات والنشر، بيروت، 2004.

31.**عبد الفتاح بيومي حجازي**، الحكومة الإلكترونية بين الواقع والطموح، دراسة متأصلة في شأن الإدارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2008.

32.**عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، القاهرة، 2005.

33.**عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني: الحماية الجنائية والمعلوماتية لنظام التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002.

34.**عبد الفتاح بيومي حجازي**، النظام القانوني للحكومة الالكترونية، الكتاب الأول، الحكومة الالكترونية، دار الكتب القانونية، مصر، المحلة الكبرى، 2007.

35.**عبد الكريم دحو الإدريسي**، أمن مجتمع المعلومات بين المؤسسات الأمنية والمدنية وشبه الأمنية، الجزءالأول: التجربة الفرنسي، مطبعة النجاح الجديدة، الطبعة الأولى، الدار البيضاء، المغرب، 2003.

36.**عبد الله حسين محمد**، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002.

37.**عبد الوهاب أبو سليمان**، البطاقات البنكية الافتراضية والسحب المباشر من الرصيد، دار القلم، دمشق، دون تاريخ النشر.

38. **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية الحكومة الالكترونية، الكتاب الثاني، الحماية الجنائية والمعلوماتية لنظام الحكومة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2003.

39.**عصام عبد الفتاح مطر**، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، 2014.

40. **علاء الدين شحاتة**، التعاون الدولي لمكافحة الجريمة "دراسة للاستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات"، إيتراك للنشر والتوزيع، القاهرة، 2000.

41. **علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، عالم الكتب الحديثة، مصر، 2004.

42. **علي عبد القادر القهوجي**، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999.

43. **عمار التركي السعدون الحسيني**، الحماية الجنائية للحرية الشخصية في مواجهة السلطة العامة، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012.

44. **عمر أبو الفتوح عبد العظيم الحمامي**، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010.

45. **عمر أحمد حسبو**، حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة، دار النهضة العربية، القاهرة، 2000.

46. **عمر سالم**، الحماية الجنائية لبطاقة الوفاء، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، 1995.

47. **عمر محمد بن يونس**، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، دون دار نشر، 2006.

48. **عيسى غسان ريضي**، القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2009.

49. **فتحي محمد أنور عزت**، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، دون ناشر، الطبعة الثانية، القاهرة، 2010.

50. **فتوح الشاذلي، عفيفي كامل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار الثقافة للطباعة والنشر، القاهرة، 2000.

51.**فرح مناني**، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجديد، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009.

52.**محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2004.

53.**محمد أمين محمد الشوابكة**، جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 1992.

54.**محمد بلال الزعبي، أحمد الشرايعة، منيب قطيشات، سهير عبد الله فارس، خالدة محمد صايل الزعبي**، مهارات الحاسوب، دار وائل للنشر والتوزيع، إعادة الطبعة الخامسة، 2008.

55.**محمد حسين منصور**، المسؤولية الالكترونية في مجال شبكات الانترنت، دار النهضة العربية، القاهرة، 2002.

56.**محمد حسين منصور**، المسؤولية الالكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.

57.**محمد سامي الشوا**، المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية للكتاب، القاهرة، 2003.

58.**محمد سامي الشوا**، ثورة المعلومات وإنعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998.

59.**محمد سامي عبد الصادوق**، حقوق مؤلفي المصنفات المشتركة، المكتب المصري الحديث، الطبعة الأولى، **2002**.

60.**محمد عبيد الكعبي**، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة، 2010.

61.**محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، **2004**.

62.**محمد عيد الغريب**، حريّة القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائيّة، النسر الذهبي للطباعة، 1996ـــ 1997.

63.**محمد محمد شتا**، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، 2002.

64. **محمد محمد عنب**، موسوعة العلوم الجنائية، تقنية الحصول على الآثار والأدلة المادية، الجزء الأول، مركز بحوث الشرطة، الشارقة، الطبعة الأولى،2007.

65. **محمود القدوة**، الحكومة الإلكترونية والإدارة المعاصرة، دار أسامة للنشر والتوزيع،الطبعة الأولى، الأردن، 2010.

66. **مدحت عبد الحليم رمضان**، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، الطبعة الأولى، 2000.

67. **محمود أحمد عبابتة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2009.

68. **مصطفى محمد مرسى**، الجهاز الإلكتروني لمكافحة الجريمة، مطابع الشرطة للطباعة والنشر والتوزيع، الطبعة الأولى، مصر، 2001.

69. **مصطفى محمد مرسى**، المراقبة الإلكترونية عبر شبكة الأنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، الطبعة الأولى، دار الكتب والوثائق القومية المصرية، 2003.

70. **ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، المحلة الكبرى ، 2006.

71. **منير محمد الجنبيهي، ممدوح محمد الجنيهي**، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

72. **نائلة عادل محمد فريد قورة**، جرائم الحاسب الإقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، الطبعة الثانية، القاهرة، 2002.

73. **نبيلة هبة هروال**، الجوانب الإجرائية لجرائم الانترنت قي مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، **2007**.

74. **نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2008.

75.**هدى حامد قشقوش**، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية ،القاهرة، 1999.

76.**هدى حامد قشقوش**، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992.

77.**هشام محمد فريد رستم**، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994.

78.**هشام محمد فريد رستم**، الحماية الجنائية لحق الانسان في صورته، مكتبة الآلات الحديثة، أسيوط، دون سنة طبع.

79.**هلال بن محمد بن حارب البويعيدي**، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة،2009.

80.**هلالي عبد أللاه أحمد**، حجيّة مخرجات الكمبيوتريّة في المواد الجنائيّة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.

81.**هلالي عبد اللاه أحمد**، إتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، 2007.

82.**هلالي عبد الله أحمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1997.

83.**وائل أنور بندق**، موسوعة القانون الإلكتروني وتكنولوجيا الإتصالات، دار المطبوعات الجامعية، الإسكندرية، 2007.

ج ــ الرسائل والمذكرات الجامعية:

❖ **الرسائل العلمية:**

1. **أحمد فتحي سرور**، نظريّة البطلان في قانون الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1959.

2. **أحمد ضياء الدين محمد خليل**، مشروعيّة الدليل في المواد الجنائيّة، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعيّة في مجال الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق،جامعة عين شمس، 1982.

3. **آدم عبد العبيد حسين**، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة الأزهر، دار المتحدة للطباعة، مصر، 2000.

4. **براهمي جنان**، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة محمد خيضر بسكرة، 2014 ــ 2015.

5. **بن ذياب عبد المالك**، حق الخصوصيّة في التشريع العقابي الجزائري، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.

6. **حابت أمال**، التجارة الإلكترونية في الجزائر، رسالة دكتوراه في العلوم القانونية، جامعة مولود معمري، تيزي وزو، 2015.

7. **السيد محمّد حسن شريف**، النظريّة العامة للإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 2002.

8. **السيد محمد حسن شريف**، النظرية العامة للإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2002.

9. **صالح شنين**، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان أبوبكر بلقايد، 2012 ــ 2013.

10. **صفية بشاتن**، الحماية القانونية للحياة الخاصة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012.

11. **فتحي محمد أنور محمد عزت**، دور الخبرة في الإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة عين شمس، 2007.

12. **كيلاني محمود**، النظام القانوني لبطاقة الوفاء والضمان، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1996.

13. **مرنيز فاطمة**، الإعتداء على الحق في الحياة الخاصة عبر شبكة الانترنت، رسالة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2012 ــ 2013.

14. **مفيدة سويدان**، نظرية الاقتناع الذاتي للقاضي الجنائي، رسالة دكتوراه في الحقوق، جامعة القاهرة، 1985.

15. **نافد ياسين محمد المدهون**، النظام القانوني لحماية التجارة الإلكترونية، رسالة دكتوراه في الحقوق، جامعة عين شمس، 2007.

16. **نويري عبد العزير**، الحماية الجزائية للحياة الخاصة ــ دراسة مقارنة ــ رسالة دكتوراه في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2010 ــ2011.

17. **هلالي عبد الله أحمد**، النظرية العامة للإثبات في المواد الجنائية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1984.

❖ **المذكرات الجامعية:**

1. **أعراب احمد**، السلطات الادارية المستقلة في المجال المصرفي، مذكرة ماجستير، كلية الحقوق، جامعة بومرداس، 2007/2006.

2. **بن عيمور أمينة**، البطاقات الالكترونية للدفع والقرض والسحب، مذكرة ماجستير، تخصص قانون الأعمال، جامعة قسنطيمة منتوري، كلية الحقوق، 2004ــ 2006.

3. **حريزي ربيحة**، إجراءات جمع الأدلة ودورها في الكشف عن الجريمة، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2011.

4. **خشة حسيبة**، وسائل الدفع الحديثة في القانون الجزائري، مذكرة ماجستير، تخصص قانون أعمال، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، قسم الحقوق، مسيلة، 2015ــ2016 .

5. **دحية رباب**، دراسة تحليلية لأداء أنظمة الدفع، حالة نظام الدفع المكثف في الجزائر، مذكرة ماجستير تخصص علوم قانونية، جامعة المسيلة، 2011ـــ2012.
6. **عبد الرحمن بحر**، معوقات التحقيق في جرائم الأنترنت، دراسة مسحية على ضباط الشرطة بدولة الكويت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999.
7. **ركاب أمينة**، أساليب التحري الخاصة في جرائم الفساد في التشريع الجزائري، مذكرة ماجستير، في قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2014 ـــ 2015.
8. **سعيداني نعيم**، آليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2012 ـــ 2013.
9. **محمد مسعود محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي، في القانون الجزائري والمقارن، رسالة ماجستير، كلية الحقوق، جامعة الاسكندرية، 2005.

د ـــ المقالات العلمية والبحوث:

1. **أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بتاريخ 09 ـــ 11 ربيع الأول 1424 هـــ الموافق لـــ 10 ـــ 12 مايو 2003 م، الإمارات العربية المتحدة، المجلد الثاني، بحوث مؤتمر منشورة، دون دار نشر، 2003.
2. **أكمل يوسف السعيد يوسف**، المسؤواية الجنائية لمقدمي المواد الإباحية للأطفال عبر الأنترنت، مجلة العلوم القانونية، والإقتصادية، كلية الحقوق، جامعة المنصورة العدد الرابع عشر، 2011.
3. **أوباية مليكة**،خصوصيات التوقيع الإلكتروني في القانون الجزائري، مداخلة مقدمة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد في 7 ـــ 8 فبراير 2017 بالمركز الجامعي، غليزان.

4. **بن قارة مصطفى عائشة**، الحق في الخصوصية المعلوماتية، بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، جامعة د. مولاي الطاهر بسعيدة، العدد السادس، جوان 2016.
5. **بن كثير بن عيسى**، الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاء، العدد63، مديرية الدراسات القانونية والوثائق، وزارة العدل، الجزائر، 2008.
6. **جلال محمد الزغبي**، مكافحة جرائم تقنية المعلومات في الأردن، المؤتمر الدولي لمكافحة جرائم تقنية المعلومات، أبوظبي بدولة الإمارات العربية المتحدة، بتاريخ : 14 ــ 12 ــ 2011.
7. **حسام محمد نبيل الشنراقي**، دور أجهزة البحث الجنائي في مكافحة جرائم المعلومات، ورقة عمل مقدمة في ندوة "الاستخدام الآمن لشبكة الانترنت، جامعة طنطا، بتاريخ 2015/5/10.
8. **حسن بن محمد المهدي**، القوة الثبوتية للمعاملات الإلكترونية، مجلة البحوث القضائية، العدد السابع، الجمهورية اليمنية، جوان 2007.
9. **حنان مليكة**، النظام القانوني للتوقيع الالكتروني في ضوء قانون التوقيع الالكتروني السوري رقم 04 ــ 2009، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثاني، المجلد 26 ، 2010.
10. **رأفت رضوان**، شرطة الانترنت، بحث منشور بمجلة بحوث الشرطة، العدد 26، يوليو 2004.
11. **سرحان حسن المهيني**، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، المجلد العشرون، العدد الرابع، العدد رقم (97)، أكتوبر 2011.
12. **سكيل رقية**، الإثبات بالتوقيع الإلكتروني بين التقنية المعلوماتية والنصوص القانونية، مداخلة مقدمة في الملتقى الوطني حول النظام القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد في 7 ــ 8 فبراير 2017 بالمركز الجامعي، غليزان.
13. **سيف عبد الله الجابري**، أمن المعلومات والخصوصية الفردية، ورقة بحث مقدمة إلى المؤتمر الدولي لأمن المعلومات الإلكترونية "معا نحو تعامل رقمي آمن"، المنعقد بتاريخ 18ــ20 ديسمبر 2005 بمسقط، سلطة عمان.

14. **شعبان فرج**، الحكومة الإلكترونية، إطارها النظري والمفاهيمي، الملتقى العلمي الدولي الأول حول"متطلبات إرساء الحكومة الإلكترونية في الجزائر: دراسة تجارب بعض الدول"، المنعقد بالجزائر بتاريخ:13و14 ماي 2014،

15. **صفية بنت عبد الله أحمد بخيت**، ضبط ومعايير أداء الحكومة الإلكترونية، ورقة عمل مقدمة ضمن بحوث مؤتمر " أمن المعلومات والحكومة الإلكترونية"، كوالالمبور، ماليزيا، أبريل 2009.

16. **عادل حافظ غانم**، الخبرة في مجال الإثبات الجنائي، مجلة الأمن العام، العدد 43، سنة 1968.

17. **عادل يوسف الشكري**، الحماية الجنائية لبطاقات الدفع الالكترونية، مركز دراسات الكوفة، مجلة تصدر عن كلية القانون جامعة الكوفة،العدد 11 لسنة 2008 .

18. **عبد الناصر محمد محمود فرغلي وعبيد سيف سعيد المسماري**، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، ''الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية''، دراسة تطبيقية مقارنة، الرياض، المنعقد في الفترة:02ـــ11/04/04/ 1148 هـــ الموافق لـــ12 ـــ 2007/11/14.

19. **عدنان إبراهيم سرحان**، الوفاء (الدفع) الالكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد في دبي في الفترة ما بين 10 ـــ 12 مايو 2003.

20. **علالي بن زيان**، معيار الإختصاص في الجرائم المعلوماتية على ضوء التشريع الإجرائي الجزائري، مداخلة مقدمة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المركز الجامعي أحمد زبانة، غليزان، بتاريخ 07 ـــ08 فبراير 2017.

21. **علي أبو مارية**، التوقيع الإلكتروني ومدى قواه في الإثبات دراسة مقارنة، مجلة جامعة الخليل للبحوث، العدد الثاني، 2010.

22. **علي أحمد الفرجاني**، جريمة القرصنة المعلوماتية، دراسة مقارنة من الجانبين الموضوعي والإجرائي، مجلة التشريع ، السنة الثانية، العدد السابع ، أكتوبر 2005.

23. **علي عبد القادر القهوجي**، الحماية الجنائية للبيانات المعالجة الكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت المنعقد: 1ـــ3 مايو 2000، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، العين، دولة الامارات العربية المتحدة، 2000.

24. **علي كريمي**، تأثير التطور التكنولوجي على حقوق الإنسان ، الحياة الخصوصية وحماية البيانات الشخصية "نموذجا"، مجلة أبحاث الفعل الإحتجاجي بالمغرب، مقاربة الإنسان السلوكيات والقيم ـــ العدد 61 ـــ 62 لسنة 2015، المغرب.

25. **عمر الفاروق الحسيني**، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25ـــ28 اكتوبر 1993، حول "الجرائم الواقعة في مجال تكنولوجيا المعلومات"، دار النهضة العربية، القاهرة، 1993.

26. **عمر محمد بن يونس**، الحقوق والحريات والالتزامات الرقمية في القانون الوطني الأمريكي، ورقة عمل مقدمة في المؤتمر الدولي حول أمن المعلومات، المنعقد بتاريخ: 18ـــ2005/12/20، مسقط ـــ سلطنة عمان.

27. **فاطمة شعران**، النّظام القانوني لبطاقات الدفع الإلكتروني، مداخلة مقدمة في الملتقى الوطني حول الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري ، المنعقد في 7 ـــ 8 فبراير 2017 بالمركز الجامعي، غليزان.

28. **لوجاني نور الدين**، أساليب البحث والتحري الخاصة وإجراءاتها، يوم دراسي حول: علاقة النيابة العامة بالشرطة القضائية احترام حقوق الإنسان ومكافحة الجريمة"، أمن ولاية إليزي، المديرية العامة للأمن الوطني، وزارة الداخلية، الجزائر، 12 ديسمبر، 2007،

29. **ماجد راغب الحلو**، الحكومة الالكترونية والمرافق العامة، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، الجزء الرابع المحور الأمني والإداري ، المنعقد في اكادمية شرطة دبي، الإمارات العربية المتحدة ، في الفترة 26 ـــ 28 أبريل 2003، مركز البحوث والدراسات، دبي، ط 1، 2003.

30. **محمد إبراهيم محمود الشافعي، النقود الإلكترونية (ماهيتها، مخاطرها وتنظيمها القانوني)،** مجلة الأمن والقانون، الصادرة عن شرطة دبي، العدد الأول، يناير، السنة الثانية، 2004.

31. **محمد أبو العلاء عقيدة،** القانون الجنائي في مواجهة إساءة استخدام بطاقة الإئتمان، موجز للتقرير المقدم بالفرنسية للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25 ــ 28 اكتوبر 1993.

32. **محمد بكرارشوش،** الإختصاص القضائي في المادة الجزائية في التشريع الجزائري، مجلة دفاتر السياسة، العدد الرابع عشر، جانفي 2016.

33. **محمّد علي السالم عياد الحلبي،** حريّة القاضي الجنائي في الاقتناع في قوانين مصر والأردن والكويت، مجلة الحقوق، العدد الثالث، السنة الحادية والثلاثون، سبتمبر 2007، الكويت.

34. **محمد محي الدين عوض،** مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25ــ28 اكتوبر 1993.

35. **محمود أحمد طه،** المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الإئتمان، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بتاريخ 09 ــ 11 ربيع الأول 1424 هـ الموافق لـ 10 ــ 12 مايو 2003 م، الإمارات العربية المتحدة.

36. **ممدوح عبد الحميد عبد المطلب،** استخدام بروتوكولTCP / IP في بحث وتحقيق الجرائم على الكمبيوتر، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، المنعقد في 26 ــ 28 نيسان 2003، بدبي ــ الإمارات العربية المتحدة ــ

37. **ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز،** نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في: 10 ــ 12 مايو 2003 أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، بحث منشور في بالمركز العربي للدراسات الأمنية والتدريب بالرياض، 1993.

38. **موسى مسعود ارحومة**، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، دراسة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون المنظم بأكادمية الدراسات العليا، طرابلس، خلال الفترة 28 ــ 29/ 10/ 2009.

39. **نادية أمين محمد علي**، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات، ورقة عمل مقدمة إلى المؤتمر الدولي حول أمن المعلومات "محو تعامل رقمي آمن"، في 28 ــ2005/2012، مسقط ــ سلطنة عمان.

40. **نور الدين الواهلي**، الإختصاص في الجريمة الالكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014.

41. **هدى حامد قشقوش**، الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المنعقد بتاريخ 09 ــ 11 ربيع الأول 1424 هـ الموافق لـ 10 ــ 12 مايو 2003 م، الإمارات العربية المتحدة.

42. **يوسف أبو فارة**، دور إدارة أمن المعلومات في فاعلية الحكومة الإلكترونية، ورقة عمل مقدمة إلى مؤتمر "أمن المعلومات والحكومة الإلكترونية" المنعقد بكوالالمبور ــ ماليزيا 2009.

43. **يوسف قجاج**، الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون، العدد 28 لشهر فيفيري 2015.

هـ ــ النصوص القانونية:

❖ **النصوص القانونية الوطنية:**

أ ــ النصوص الدستورية:

ــ **الدستور الجزائري** لسنة 1996، ج.ر عدد77، المؤرخة في 8 ديسمبر 1996 والتعديلات اللاحقة عليه بالقانون (02 ــ03)، ج.ر.ج، رقم 25، المؤرخة في 14 أبريل 2002. والقانون رقم (08ــ19) ج.ر.ج، رقم 63، المؤرخة في15 نوفمبر 2008، وأخيرا القانون رقم(16ــ01)ج.ر.ج، رقم 14 المؤرخة في07 مارس 2016.

ب ــ النصوص التشريعية:

ــ الأمر رقم 66 ــ 155 المؤرخ في 18 صفر 1386، الموافق لــ 08 يونيو 1966، **المتضمّن قانون الإجراءات الجزائية** الجزائري المعدل والمتمم بالقانون رقم 06 ــ 22 المؤرخ في 21 ديسمبر 2006، ج.ر عدد 84 لسنة 2006.

الأمر رقم 66 ــ 156 المؤرخ في 18 صفر 1386، الموافق لــ 08 يونيو 1966، المتضمن **قانون العقوبات**، ج . الصادرة سنة 1966.

ــالأمر رقم 75 ــ 58 المؤرخ في 26 سبتمبر 1975المتضمن **القانون المدني** المعدل والمتمم بالقانون رقم 07 ــ 05 المؤرخ في 3 ماي 2007، ج.ر ج، عدد 31 لسنة 2007.

ــ القانون رقم 2000 ــ 03 مؤرخ في 5 غشت سنة 2000، المحدد **للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية**، ج.ر.ج.ج، عدد 48 ، الصادرة في 6 غشت 2000.

ــ الأمر رقم 03ــ11 المؤرخ في 26 أوت 2003 المتعلق **بالنقد والقرض** المعدل والمتمم، ج.ر.ج، العدد 52، لسنة 2003.

ــ القانون رقم 04ـــ14 مؤرخ في 27 رمضان عام 1425، الموافق لــ 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66ــ ــ155 المؤرخ في 18 صفر 1386 الموافق لــ 8 يونيو 1966، المتضمنقانون الإجراءات الجزائية، ج.ر.ج. عدد 71 ــ الصادرة في 10 نوفمبر 2004.

ــ قانون رقم 04 ــ 15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66ــ 156 المؤرخ في 08 يونيو سنة 1996 المتضمن **قانون العقوبات**، ج.ر عدد 71، لسنة 2004.

ــ الأمر رقم 05ــ03 مؤرخ في 19جمادى الأولى عام 1424 الموافق 19 جويلية عام 2003، يتعلق **بحقوق المؤلف والحقوق المجاورة**، ج.ر.ج، عدد 44 لسنة 2003.

ــ القانون رقم 05ــ10 المؤرخ في 20 جوان 2005 المعدل والمتمم للأمر 75 ــ 58 **المتضمن القانون المدني**، ج.ر.ج، عدد 44، الصادر في 12 جوان 2005.

القانون رقم 06ـــ22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66ـــ155 المؤرخ في 8 يونيو 1966 المتضمن **قانون الإجراءات الجزائية**، ج.ر.ج. عدد 84، الصادرة في 34 ديسمبر2006.

ـــ القانون رقم 06 ـــ23 مؤرخ في 29 ذي القعدة عام 1427 الموافق لـــ 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66 ـــ 156 المؤرخ في 18 صفر عام 1386 الموافق لـــ 8 يونيو 1966 والمتضمن **قانون العقوبات الجزائري**، ج.ر عدد 84 لسنة 2006.

ـــ القانون رقم 09 ـــ04 المؤرخ في 14 شعبان 1430هـــ ، الموافق لـــ 05 أوت 2009، يتضمن القواعد **الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها**، ج.ر عدد 47، الصادرة في 16 أوت لسنة 2009.

ـــ قانون عضوي رقم 12 ـــ 05 المؤرخ في 12 يناير سنة 2012، يتعلق بالإعلام، ج.ر، عدد 02، الصادرة قي 15 يناير 2012

ـــ الأمر رقم 15 ـــ02 مؤرخ في 23 يوليو سنة 2015، يعدل ويتمم الأمر رقم 66ـــ155 المؤرخ في 8 يونيو سنة 1966 والمتضمن **قانون الإجراءات الجزائية**، ج.ر.ج. عدد 40 ، الصادر في 23 يوليو 2015.

ـــ قانون رقم 15 ـــ 04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير 2015 **يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيي**ن، ج. ر عدد 06 لسنة 2015.

ج ـــ النصوص التنظيمية:

❖ **المراسيم الرئاسية:**

ـــ المرسوم الرئاسي رقم 10/ 263 المؤرخ في 728 شوال عام 1431 هـــ الموافق لـــ7 أكتوبر سنة 2010 المتضمن **تنظيم الصفقات العمومية**، ج. ر .ج ، عدد 58 لسنة 2010 .

ـــ المرسوم الرئاسي رقم 14ـــ183 المؤرخ في13 شعبان عام 1435 الموافق لـــ 11 يونيو سنة 2014، يتضمن **إنشاء مصلحة التحقيق القضائي لمديرية الأمن الداخلي بدائرة الإستعلام والأمن ومهامها وتنظيمها**، ج.ر.ج عدد 32، الصادر في 12 يونيو 2014.

ـــ المرسوم الرئاسي رقم 15ـــ 261 المؤرخ في 24 ذي الحجة عام 1436 الموافق لـــ 8 أكتوبر سنة 2015، **يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها**، ج. ر عدد 53 لسنة 2015.

❖ **المراسيم التنفيذية:**

ـــ المرسوم التنفيدي رقم 98 ـــ 257 المؤرخ في 25 غشت 1998 المتعلق **بضبط شروط وكيفيات إقامة خدمات الانترنت**، ج.ر ج. ج ، عدد63 ، الصادرة في 26 غشت 1998.

ـــ المرسوم التنفيذي رقم 2000ـــ307 المؤرخ في 14 أكتوبر سنة 2000، يعدل المرسوم التنفيذي رقم 98ـــ 257 المؤرخ في 25 أوت 1998 الذي **يضبط شروط وكيفيات إقامة خدمات الانترنت**، ج.ر.ج، عدد 60، لسنة 2000.

ـــ المرسوم التنفيذي رقم 06ـــ348 المؤرخ في 15 رمضان 1427 الموافق لـــ 05ـــ10ـــ2006، بتضمن **تمديد الاختصاص المحلي لبعض المحاكم، ووكلاء الجمهورية وقضاة التحقيق**، ج.ر.ج، عدد 63، الصادر في 8 أكتوبر 2006.

ـــ المرسوم التنفيذي رقم 07 ـــ 162 المؤرخ في 30 مايو سنة 2007، والمتعلق **بنظام الاستغلال المطبق على كل أنواع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية**، ج.ر.ج، العدد 37، الصادر في 07 يونيو 2007.

ـــ المرسوم التنفيدي رقم 16 ـــ142 مؤرخ في 27 رجب عام 1437 الموافق 5 مايو 2016، **يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا**، ج.ر.ج عدد 28 الصادر بتاريخ 08 ماي 2016.

ـــ المرسوم تنفيذي رقم 16 ـــ 267 مؤرخ في 15 محرم عام 1338، الموافق لـــ 17 أكتوبر سنة 2016، يعدل ويتمم المرسوم التنفيذي رقم 06ـــ348 المتضمن **تمديد الاختصاص المحلي**

لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج، عدد 62، الصادر في 23 أكتوبر 2016.

❖ **النصوص القانونية الأجنبية:**

ـــ قانون الأحوال المدنية المصري رقم 143 لسنة 1994 في شأن الأحوال المدنية.

ـــ قانون الإجراءات الجنائية المصري(طبقا لأحدث التعديلات بالقانون 95 لسنة 2003)، الصادر بالقانون رقم 150 لسنة 1950.

ـــ القانون رقم 15 لعام 2004 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، المؤرخ في 21 أبريل 2004، الصادر في 23 أبريل 2004.

ـــ التوجيه الأوربي رقم **2000 ـــ 31** الصادر بالإجماع في **8** حزيران (جوان)**2000**، والمتضمن الأوجه القانونية لخدمات شركات المعلومات، لاسيما التجارة الإلكترونية.

ـــ قانون رقم 2000/ 83 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية، الرائد الرسمي للجمهورية التونسية، العدد 64 لسنة 2000.

ـــ القانون الأساسي المتعلق بحماية المعطيات الشخصية المؤرخ في 27 جويلية 2004، ج. ر تونسية، عدد 63 لسنة 2004.

ـــ الأمر المتعلق بشروط وإجراءات التصريح والترخيص لمعالجة المعطيات الشخصية بالمغرب، رقم 3004 لسنة 2007 المؤرخ في 27 نوفمبر 2007.

ـــ قانون رقم 08 ـــ 09 المتعلق بالأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، منشور في الجريدة الرسمية بالمملكة المغربية، عدد 5711 بتاريخ 23 فبراير 2009.

ـــ القرار الإرشادي (CE/46/2000) المتعلق بنشاط مؤسسات النقد الإلكتروني، الجريدة الرسمية للمجموعة الأوربية بتاريخ 2000/10/27.

ـــ قانون التعاملات الالكتروني الأردني رقم (15) لسنة2015، الصادر بتاريخ 15 أبريل 2015.

ـــ قانون إمارة دبي رقم (02) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية.

ـــ مرسوم سلطاني رقم 2008/ 96 المتعلق بإصدار قانون المعاملات الإلكترونية العماني الصادر في 27 جمادى الأولى عام 1429، الموافق لـــ 7 مايو سنة 2008 .

ـــ القرار رقم (81) المتعلق بضوابط استخدام الحاسبات الآلية وشبكات المعلومات في الجهات الحكومية المؤرخ في 19/ 03/ 1430هـــ، بالمملكة العربية السعودية.

ثانيا: المراجع باللغة الأجنبية

1 ـــ باللغة الفرنسية

❖ **Ouvrages :**

1. **Amoury (B) et Poullet (Y)**, le droit de la preuve face à l'informatique et télématique, revue internationale de droit compare, n° 2, avril - juin 1985.
2. **Djavad (F),** le fardeau de la preuve en matière pénale essai d'une théorie générale, thèse Paris, 1977.
3. **Etienne Madrranges**, la loi du 30 décembre 1991, relative à la sécurité des chèque et des cartes de poiment , vers un denengorgement des tribunaux, la nouvelle pénalité libératoire, G. P ,doc. 2003.
4. **J- Bradel**, la responsabilite' pénale de l'expert , R.S.C, 1986.
5. **J- Michaud**, le juge d' instruction et l'expert , R. S. C , 1975.
6. **Jeandidier Wilfrid**, les truquage et usages frauduleux de carte magnétique, J.C.P ,doctr 3229, 1986.
7. **Lauvasseur**, La juridiction correctionnelle depuis l'application du code de procédure pénal, revus du science criminelle,1959.
8. **M, Guével**, le développement de la signature électronique, thèse de mastère 2, recherche droit des affaires, université Paris Nord 13, France, 2010/2011 .
9. **Raymond Gassin**, Fraude informatique, Dalloz 1995.
10. **Roger Merle et Andre Vitu**, Traité de droit criminel, tome 2, dexieme édition, édition Cujas. 2000.

11. **W.JARRAYA**, La protection des données personnelles dans le commerce électronique, mémoire pour l'obtention du Master en droitprivé, Université de Sfax, Faculté de droit de Sfax, 2004-2005.
12. **Gaval (C),** le droit pénal des cartes magnétique ,et/ou crédit,1994, dalloz.
13. **André CHAMINADE** ? poste et communications électroniques 'Régime' Juridique des authorisation sd'utilisation des préquences radioélectriques, JCP, la semaine juridique N°43,24 Octobre 2007, II10177.
14. **Décocg (A),** chronique législative, Rev.S.C, 1978.
15. **Feral- Schuhl Christiane**, Cyber droit, le droit à l'épreuve de l'internet, 3ém Edition, Dunod, Paris.
16. **Grats**, la résponsabillité penal d'internet, Dalloz, 1996.
17. **Itéanau**, les contras des commerces électronique, droit et patrimoine, dec 1977.
18. **Marthew. R .Zakaras**, International Computer Crime, revue international de droit pénal, 3eme et 4eme trimestres 2001 .
19. **Merle (R) et Vitu (A),** traité de droit criminel, droit pénal, T2. 1999.
20. **NicolOpoulos (P)**, le procedure devant les jurisdictions répressives et le Principe du contradictoire, revue de science criminel, N' 1 , 1989.
21. **Pierre Sagos et Michel Mass**, l'informatique et droit pénal, journée d'études de 15novembre 1980 , CUJAS 1890.
22. **Pradel**, la preuve en procedure pénale comparé, rapport général, revus international de droitpénal. 1992.
23. **Samir Lahlou**, E-Government ou Gouvernement Electronique, Bulletin d'information périodique (BIP), juin – 2002- n° 114.
24. Sami FEDAOUI, La protection des données personnelles face aux nouvelles exigences de sécurité, mémoire fin d'étude mastere 2, université de ROUEN, 2007- 2008.
25. **Sedaillan,Valérie**, la responsabilité des prestataires techniques sur internet, dans le digitale millennium copyrient act American et le projet de directive européennesur le commerce éléctronique, Cahiers Lamy, janvier 1999,n' 110.
26. **Stefani(Gaston)**, répertoire de prevue en droitpénal, et de procedure pénal, Dalloz tome v, 1969.

27. **Verguth (pascal),**La répression des délits informatiques dans une perspective internationale,Thèse de doctorat en Droitprivé, à université de Montpellie, 1996.
28. **YannPadova**, un aperçu de lute contre la cybercriminalité en France, revue de science criminelle et de droit pénale, n^0 4, Dalloz,2002.

❖ **Textes :**

1. **-**Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**.**
2. Loi n° 84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de credit.
3. Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques , Journal officiel n° L 013 du 19/01/2000 .
4. LOI n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique JORF n°62 du 14 mars 2000 .
5. Directive 2000/31/CE du Parlement européen et du Conseildu 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.
6. LOI no 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication.
7. Décret n°2001-693 du 31 juillet 2001 créant au secretariat général de la défense nationale une direction centrale de la sécurité des systèmesd'information**.**
8. Décret n°2001-1179 du 12 décembre 2001 relatif aux services déconcentrés de la direction générale de la concurrence, de la consommation et de la répression des fraudes.
9. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
10. LOI n° 2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les homes.

2 ــ باللغة الإنجليزية

1. Bainbridge (David) . Hacking the unauthorised access of computer system , the legal implication . M.L. Rev. March, vol 5 1989.
2. Eoghan Casey, Digital Evidence and Computer Crime—Forensic Science, Computers and the Internet , Second Edition , AcademicPress *An imprint of Elsevier* , London , 2004.
3. Jaeger, Paul, and John Carlo, E –Government Education in Public Libraries :New Services Roles and Expanding Sosial Responsabililities, Journal of Education for Library and Information Science, vol 50 n° 1, 2009.
4. Obstacles to Discovery of electronic Evidence. Journal of Science and Technology Law .22 September 1998 .
5. Thomas J. Gardner, Terry M. Anderson, Criminal Evidence, Principles and cases, (5) fifthe dition, Thompson Wadsworth Publisher, 2004

ثالثا ــ مواقع الأنترنت:

ــ الموقع الرسمي للقوانين الجزائرية: http://www.joradp.dz/HAR/Index.htm

ــ الموقع الرسمي للتشريعات الفرنسية: https://www.legifrance.gouv.fr/

ــ الموقع الرسمي لمحكمة النقض الفرنسية: https://www.courdecassation.fr

ــ مشروع الجزائر الإلكترونية 2013 المنشور على موقع وزارة البريد وتكنولوجيا الإعلام والإتصال.

http://www.premier-ministre.gov.dz/arabe/media/PDF/Dossier/Telecom/EAlgerie.pdf

ــ الموقع الرسمي للتشريعات الأردنية: http://www.lob.gov.jo/

ــ استطلاع الأمم المتحدة للحكومة الإلكترونية بعنوان" الحكومة الإلكترونية لدعم التنمية المستدامة" المنشور على الموقع التالي:

https://publicadministration.un.org

الفهرس

الملخص

الحكومة الالكترونية مفهوم جديد يعتمد على استغلال تكنولوجيا المعلومات الرقمية في إنجاز المعاملات الإدارية، وتقديم الخدمات المرفقية من خلال مواقع ويب حكومية توضع على الانترنت.

والتحول إلى الحكومة الإلكترونية يحوي جوانب إيجابية وميزات كبيرة، إلا أنه في الوقت ذاته لا يخلو من المخاوف والخطورة بسبب الاعتداءات الواقعة على المعاملات الالكترونية الحكومية، وآليات تنفيدها، مما يتطلب الأمر إيجاد منظومة تشريعية تشمل الجوانب الموضوعية والإجرائية لحماية الحكومة الالكترونية جزائيا.

الكلمات المفتاحية: الحكومة الالكترونية، النظام المعلوماتي، جرائم، التوقيع الالكتروني.

Résumé

Le gouvernement électronique, un nouveau concept se basant sur une bonne exploitation de la technologie de l'information numérique et de la communication, qui vise à réaliser des échanges dans le cadre de l'administration et le public, par le biais de sites Web du gouvernement affichés en ligne.

L'introduction d'un e-gouvernement et sa réussite sont conditionnées par la mise en place d'un cadre juridique afin de réduire les risques dû aux piratages informatiques visant à compromettre les transactions entre le e-administration et les citoyens, notamment sur l'aspect de la vie privée et de la confidentialité des données, ainsi que, les mécanismes pour son bon déroulement qui dépendra largement d'un environnement juridique adapté regroupant des textes de lois et la manière de les exécutées, afin de protéger et sécuriser l'administration électronique .

Les mots clés : Gouvernement Eléctronique, système informatique, les crimes, signature éléctronique.

Abstract

E-government is a new concept that relies on the exploitation of digital information technology in the execution of administrative transactions, also in the provision of the attached services through government web sites.

The transition to e-government has positive aspects and great features. At the same time, however, it is not without fear and seriousness because of the attacks on electronic government transactions and the mechanisms of their implementation. This requires a legislative system that includes the substantive and procedural aspects of the electronic protection of e-government.

Keywords: Electronic Government, Information System, Crimes, Electronic Signature.