.الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

المركز الجامعي أفلو

Ministry of Higher Education
and Scientific Research

Aflo University Center

معهد الحقوق والعلوم السياسية

قسم: الحقوق

مطبوعة بيداغوجية بعنوان :

محاضرات في
الجرائم المعلوماتية

المستوى: السنة الثانية ماستر

التخصص: القانون الجنائي والعلوم الجنائية

السداسي : الثالث

إعداد الدكتور: بن دراح علي إبراهيم

الرتبة : أستاذ محاضر قسم – ب

السنة الجامعية : 2021/2020

المركز الجامعي آفلو ص ب 306 – آفلو – الأغواط
البريد الإلكتروني: cu-aflou@cu-aflou.edu.dz
الهاتف: 76 11 16 029 / الفاكس: 11 11 029 16

Aflo University Center P O Box 306
Aflou-Laghouat
E-mail : cu-aflou@cu-aflou.edu.dz
Tel: 029 16 11 76 / Fax : 16 029 11 11

مقدمة

حاول الإنسان منذ بدء الخليقة البحث عن تدوين حضارته بشتى الطرق والوسائل محاولا نقل المعلومة من جيل إلى جيل، فكانت الرموز والكتابات على الحجر خير دليل على نقل تلك الصورة الإنسانية.

يندرج نقل المعلومة ضمن عملية التواصل الإنساني التي سعى إلى تجسيدها الإنسان،حيث أنه مع ظهور جهاز الحاسوب الآلي سنة 1946 بفضل مجهودات العالمين J.Presper Ecket و Jhon William Mauchy المنتميان إلى جامعة بنسلفانيا بالولايات المتحدة الأمريكية، والذي سبقته عهد الثورة الصناعية وظهور الآلة ، تمهيدا لما صار يعرف بعصر العولمة.

وقد قزّمت هذه التكنولوجيا المصاحبة لها عمر المسافة بين الشعوب، فأصبح العالم قرية صغيرة وألغت بذلك صعوبة التواصل الإنساني بين الشعوب.

لكن لما هذه التكنولوجيا من امتيازات فان لها كذلك مساوئ عديدة، حيث صاحب استعمالها نشوء ما يعرف بالسلوك الإجرامي المعلوماتي أو الجريمة المعلوماتية، والتي مسّت مستعملي هذه التقنية الحديثة في أشخاصهم وأموالهم نتيجة سوء استعمال هذه التقنية المحدثة ، وذلك كون جهاز الحاسوب كان له الضلع البارز في عديد التحولات

الاقتصادية والاجتماعية والصناعية والإدارية، محدثا معه ما صار يعرف بالجرائم الفنية (TECHNOCRIMES)[1].

وعليه نطرح التساؤلات التالية :

ما هي الجريمة المعلوماتية ؟ وما مدى فعالية التشريعات الدولية والداخلية لردعها؟

ستكون الإجابة على هذه التساؤلات هو جوهر دراستنا في هذا المقياس خلال هذا السداسي إن شاء الله ، وذلك من خلال التطرق إلى المحاور التالية :

الفصل الأول : الأحكام العامة للجريمة المعلوماتية

سنتطرق فيه إلى ماهية الجريمة المعلوماتية ستناول فيه التعريف والخصائص إضافة إلى أركانها.

الفصل الثاني : مكافحة الجريمة المعلوماتية على مستوى المجال الدولي

ويمثل الإطار الموضوعي لهذه المحاضرات من خلال التعرض إلى مختلف المواثيق والمعاهدات الدولية التي عالجت هذا الموضوع، وكذلك الآليات المتاحة لذلك.للجريمة المعلوماتية مع التعرض لأهم الصعوبات الإجرائية .

الفصل الثالث : مكافحة الجريمة المعلوماتية في نطاق القانون الداخلي

والذي تم تقسيمه إلى مبحثين :

المبحث الأول : مكافحة الجريمة المعلوماتية في مجال قانون العقوبات الجزائري

---

[1] قارة آمال ، الجريمة المعلوماتية ، ماجستير تخصص القانون الجنائي والعلوم الجنائية ، كلية الحقوق بجامعة الجزائر ،2005 ،ص 1 .

والذي سنتطرق فيه إلى الجرائم المعلوماتية الماسة بأنظمة المعالجة الآلية للمعطيات، ثم الجرائم المعلوماتية الواقعة على الأشخاص(القذف و الإهانة والسب والاعتداء على حرمة الحياة الخاصة للأفراد عبر الانترنت- الاستغلال الجنسي للأطفال عبر الانترنت- انتهاك الآداب العامة)، وكذلك الجرائم المعلوماتية الواقعة على الأموال (النصب الالكتروني- السرقة الالكترونية – استغلال بطاقات الائتمان) و الجرائم المعلوماتية الواقعة على الهيئات العامة.

المبحث الثاني: مكافحة الجريمة المعلوماتية خارج نطاق قانون العقوبات الجزائري

والذي تم تخصيصه إلى مكافحة الجريمة المعلوماتية في إطار حماية حقوق الملكية الفكرية و الشخصية وأخيرا الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال.

الفصل الأول : الأحكام العامة للجريمة المعلوماتية

سنتناول من خلال هذا المحور الأحكام العامة للجريمة المعلوماتية ، وذلك بالتطرق إلى تعريف الجريمة المعلوماتية وخصائصها **(المبحث الأول)** وأركانها **(المبحث الثاني)**.

المبحث الأول : ماهية الجريمة المعلوماتية

سيتم التطرق من خلال هذا المبحث إلى تعريف الجريمة المعلوماتية **(المطلب الأول)** ومن ثم استعراض أهم خصائصها **(المطلب الثاني)**.

المطلب الأول : تعريف الجريمة المعلوماتية

مع تطور وسائل الاتصال والمعلوماتية في العصر الحديث ، وارتباطها بأجهزة الكمبيوتر والانترنت ، فبمقدار استعمال هذه الوسائل بنوع جديد من الجرائم ، لم يكن معروفا في السابق ، جعل من الفقه يبحث عن إعطاء مفهوم محدد لهذه الجرائم .

أولا : تطور مفهوم الجريمة المعلوماتية لاقترانه بتطور جهاز الكمبيوتر

تزامنا مع تطور صناعة الحاسبات الالكترونية أصبحت الطريقة الميكانيكية المتبعة سابقا غير قادرة على القيام بالعمليات المتطورة ، وعليه تم تطوير هذا الجهاز ، والذي شمل تغيير وحدة المعالجة المركزية والذاكرة [2].

[2] بعقيقي عبير ، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي – دراسة مقارنة – ، أطروحة دكتوراه في الحقوق ، تخصص النظام الجزائي والسياسة الجزائية المعاصرة ، كلية الحقوق بجامعة محمد خيضر ببسكرة ، الجزائر ، 2018، ص 11.

وصولا إلى صناعة حاسب آلي يتوافق والتطور التكنولوجي ، صاحبه ظهور شركات عملاقة متخصصة .[3]

ثانيا : تعريف الجريمة المعلوماتية انطلاقا من اختلاف معالمها

عرفها الفقيه ميراو Merew على أنها الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية ، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات.[4]

كما عرفها الفقيه باركر Parkerعلى أنها كل فعل غير مشروع يكون العلم بتكنولوجيا الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى .[5]

غير أن اتجاها من الفقه أعطى للجريمة المعلوماتية معنى واسعا لتشمل كل أشكال السلوك أو الفعل غير المشروع والذي يرتكب بواسطة جهاز الحاسوب.[6]

في حين يعتبر بعض الفقه أن التعريف الذي تبنته منظمة الأمم المتحدة في مؤتمرها العاشر لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته الذي انعقد بفيينا بتاريخ 10 إلى 17 أفريل 2000، يمكن اعتباره كخلاصة تعريفية لما سبق حيث عرفتها بأنها "جريمة

---

[3] بعقيقي عبير، مرجع سابق ، ص11.

[4] طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة ، مصر، 2015 ، ص 153.

[5] نفس المرجع ، ص154.

[6] لورنس سعيد الحوامدة ، الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية مقارنة ، مجلة الميزان ، المجلد 4 ، العدد1، جامعة العلوم الإسلامية العالمية ، الأردن ، 2017، ص 189.

يمكن ارتكابها بواسطة نظام حاسوبي أوشبكة حاسوبية أو داخل نظام حاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية ".[7]

وعليه بالرغم من عدم الوصول إلى تعريف جامع ومانع لمفهوم الجريمة المعلوماتية،إلا أن الاتفاق انصب على انه كل فعل غير مشروع يستهدف تغيير بيانات أومعلومات،كيفما كان هذا التغيير، سواء كان بواسطة جهاز الحاسوب ، كما يمكن أن يكون باستخدام جهاز تكنولوجي آخر ، وهذا يطرح إشكالا جديدا.

إن حصر الجريمة المعلوماتية بجهاز الكمبيوتر لم يكن إلى حد قريب محل جدل فقهي في ظل تطور هذا الجهاز، ولكن بتدخل أجهزة أخرى أفرزها هذا التطور التكنولوجي والتقني الجارف، أكد على ضرورة شمول الجريمة المعلوماتية كل ما له علاقة باستخدام غير شرعي لأي وسيلة تكنولوجية ناقلة للمعلومة وعدم حصرها في جهاز الكمبيوتر.

ثالثا: تعريف الجريمة المعلوماتية بالتركيز على موضوعها

اشتغل كثير ممن الفقه على موضوع الجريمة المعلوماتية دون التركيز على الأداة المستخدمة لذلك ، ومن أمثال هؤلاء الفقهاء Rosamblatt حيث اعتبر جريمة الحاسب بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أوالوصول إلى المعلومات المخزنة داخل الحاسوب أو التي عن طريقه.

[7] زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى ، الجزائر ، 2011، ص 43.

المطلب الثاني : خصائص الجريمة المعلوماتية

تمتاز الجريمة المعلوماتية بعدة خصائص تميزها عن باقي الجرائم التي تصنف في خانة الجرائم الكلاسيكية ، أهمها :

أولا : جريمة عابرة للأوطان

نظرا للوسيلة المستعملة فيها وهي أجهزة الكمبيوتر ، جعل من هذه الجريمة عابرة للحدود ، لا ترتبط بإقليم جغرافي معين ، تكفي توفر جهاز حاسوب في أي مكان في الكرة الأرضية ، يكون مزودا بالشبكة المعلوماتية لارتكاب جريمة معلوماتية.

هذا الوضع جعل أمام الدول اللجوء إلى حتمية التعاون والتنسيق الدوليين من أجل مكافحة هذه الجرائم بكافة الوسائل المتاحة بداية من خلال إبرام اتفاقيات ومعاهدات دولية، وفتح المجال واسعا للقيام بإجراءات التحري والتدقيق اللازمين لكشف مرتكبي هذه الجرائم من خلال تحديد القانون الواجب التطبيق في هذه الحالات، وتحديد الدولة صاحبة الاختصاص القضائي.[8]

ثانيا : جريمة يصعب إثباتها

ما يميز هذا النوع من الجرائم هو صعوبة إيجاد الدليل المادي لإدانة مرتكبيها بسهولة ويسر، لأن محو الدليل إجراء بسيط ، خاصة مع ما يوفره العالم من مجرمين معلوماتيين محترفين برعوا في هذا المجال وتفنّنوا في علم القرصنة والمعلومات، لذا يصعب معهم إثبات الفعل الجنائي المرتكب، على عكس الجرائم العادية المرتكبة.

---

[8] بعقيقي عبير ، مرجع سابق ، ص 21.

كما ساهم في صعوبة اكتشاف هذه الجرائم واثبات مرتكبيها هو عدم توفر مختصين لدى رجال الأمن والمحققين، يضاهي مستوى هؤلاء المجرمين المعلوماتيين المحترفين في هذا النوع من الإجرام ، وذلك بالرغم من تطور وسائل الإثبات الجنائية المختلفة ووجود فرق جنائية مختصة في مكافحة هذا النوع من الجرائم .

ثالثا : جريمة آثارها وخيمة على الصعيد الاقتصادي

نظرا لشمول شبكة الانترنت والكمبيوتر أجهزة اقتصادية حساسة شملت أغلب معاملاتها، حيث تسببت الجرائم المعلوماتية بتكبيد هذه المؤسسات والشركات خسائر مالية ضخمة نتيجة اختراق أنظمتها المعلوماتية من طرف مجرمين مختصين في هذا المجال إضافة إلى سرقة أموال كبيرة من عديد البنوك باختراق حسابات الزبائن ، وتدمير نظام التشغيل أو نشر فيروسات أو إفشاء بيانات، حيث قدرت الخسائر المادية في نهاية القرن الماضي ما يقارب 500 مليون دولار في السنة حسب إحصائيات المركز الوطني لجرائم الحاسوب بالولايات المتحدة الأمريكية (NCCCD) [9].

رابعا : جريمة ناعمة : لا يحتاج هذا النوع من الجرائم إلى بذل مجهود عضلي أو جهد بدني معين المستخدم في الجرائم الأخرى كالقتل أو السرقة مثلا ، بل يحتاج إلى مجهود ذهني يستخدمه المجرم المعلوماتي ، كما لا يحتاج إلى سن محدد، فكثير من هذه الجرائم يرتكبها قصر لم يبلغوا سن الرشد ، ولا تقتصر على جنس الرجال ، فكثير من النساء من تورطن في هذا النوع من الجرائم، لذلك وصفت بالناعمة.

[9] بعقيقي عبير ، مرجع سابق ، ص22.

المبحث الثاني : أركان الجريمة المعلوماتية

كل الجرائم تتكون من الركن الشرعي والمادي والمعنوي ، لكن الجريمة المعلوماتية إضافة إلى الأركان الثلاث السابقة فإنها تمتاز بتوفر ركن آخر هو الركن الافتراضي، كل هذه الأركان ستكون محور دراستنا في هذا المبحث.

المطلب الأول : الركن الافتراضي للجريمة المعلوماتية

لتوفر قيام جريمة معلوماتية فانه يستلزم وجود نظام المعالجة الآلية للمعطيات، فما هو مفهوم هذا النظام ؟

أولا : تعريف نظام المعالجة الآلية للمعطيات

عرفه البعض من الفقه على أنه عبارة عن آلية وإجراءات منظمة ، تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثمّ تحويلها إلى معلومات ، يسترجعها الإنسان عند الحاجة للتمكين من انجاز عمل أو اتخاذ قرار أو القيام بأي وظيفة عن طريق المعرفة التي تحصل عليها من المعلومات المسترجعة من هذا النظام .[10]

ومن هنا طرح الإشكال عن مفهوم التعدد الذي يحمله هذا النظام ، وعند وقوع الاعتداء على عنصر بمفرده داخل هذا النظام ، هل نكون أمام الاعتداء على النظام بأكمله ؟

اعتبر عديد الفقه أنه يتم الرجوع إلى علاقة هذا الجزء بالنظام ، فإذا كان مستقلا عنه ، ومنه لا نكون أمام جريمة معلوماتية إذا ما تم الاعتداء العناصر الفردية ، حاله في ذلك

---

[10] سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية ، جامعة الحاج لخضر باتنة ، الجزائر ، 2013، ص 42.

حال الاعتداء على البرامج المعروضة للبيع ، أو أجهزة الحواسيب التي لم تدخل حيز الخدمة أو في حالة تجربة ، أو تلك الأنظمة المعلوماتية التي خرجت عن الخدمة [11].

لم يقم المشرع الجزائري من خلال تعديله لقانون العقوبات لسنة 2004، وإضافته للقسم 7 مكرر الموضوع تحت مسمى" المساس بأنظمة المعالجة الآلية للمعطيات"،[12] حين نص على النوع من الجرائم بمهمة التعريف ، وترك ذلك للفقه والاجتهاد القضائي ، مستعرضا صور الاعتداءات على هذا النظام ، مستأنسا بتجربة نظيره الفرنسي الذي لم يقم هو الأخر بهذه المهمة ، بعد أن تم التخلي عنها من طرف الجمعية الوطنية التي رفضت نهائيا وأسقطت اقتراح مجلس الشيوخ بمناسبة تعديل قانون العقوبات الفرنسي ، لذا عدّ من الأعمال التحضيرية التي عرفت هذا النظام.[13]

وبالعودة إلى التعريف المقترح من قبل مجلس الشيوخ الفرنسي ، فانه يحمل مجالات محددة ، حيث اعتبر أن نظام المعالجة الآلية للمعطيات هو " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة ، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات ، على أن يكون هذا المركب خاضعا للحماية الفنية ".[14]

---

[11] قارة آمال ، مرجع سابق ، ص 28.

[12] وذلك بموجب القانون 04-15 المتضمن تعديل قانون العقوبات ، الجريدة الرسمية عدد 71 المؤرخة في 2004/11/10 ، ص 8.

[13] قارة آمال ، مرجع سابق ،ص 26.

[14] سعيداني نعيم ، مرجع سابق ، ص 43.

من الملاحظ أن هذا التعريف أدق أشمل من التعريف السابق ، كما أنه إضافة إلى تحديد عناصر المعطيات بدقة ، اشترط توفر الحماية الفنية اللازمة لهذه المعطيات ، وإلا لم تعد جريمة معلوماتية .

وعليه من الممكن أن يكون شمول المشرع فكرة التعريف أصلا هو مساس بمفهوم النظام نفسه ، كون هذا النظام في تطور مستمر لارتباطه بعناصر تقنية محضة ، وعليه فان ترك مهمة تعريفه للفقه والقضاء فكرة جديرة بالاهتمام ، وهو يراه بعض الفقه.[15]

ثانيا: الحماية الفنية للنظام المعلوماتي كشرط لقيام المسؤولية الجزائية

اختلف الفقه القانوني في مدى اعتبار الحماية الأمنية لنظام المعالجة الآلية للمعطيات كشرط ضروري كي يحظى هذا النظام بالحماية الجزائية من عدمها ، فقد اعتبر جزء من الفقه الفرنسي إلى عدم اشتراط توفر الحماية الفنية للنظام المعلوماتي لقيام الجريمة المعلوماتية [16]، وذلك راجع كون نظام الأمن والحماية الفنية أو التقنية لا يكون له سوى دور إيجابي ، وأن ثبوت سوء نية المنتهك لهذا النظام ودخوله إليه بطريقة غير شرعية هي متوفرة أساسا[17].

في حين قسم اتجاه آخر من الفقه المتمسك بضرورة وجود نطاق كاف من الحماية الأمنية للمختلف الأنظمة المعلوماتية المعالجة آليا، مقسما هذه الأخيرة إلى 03 أصناف:

- أنظمة مفتوحة للجمهور.

---

[15] سعيداني نعيم، مرجع سابق ، ص 43.

[16] نفس المرجع ، ص 45.

[17] احمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي–دراسة مقارنة –، ط1، دار النهضة العربية للنشر والتوزيع، مصر،2000، ص 264.

- أنظمة قاصرة على أصحاب الحق فيها، ولكن دون حماية فنية .
- أنظمة قاصرة على أصحاب الحق فيها، مع توفرها على حماية فنية لها .

حيث اعتبر هذا الفقه أن النوع الأخير من الأنظمة المعلوماتية هو الذي يتمتع بالحماية الجنائية، وحجتهم في ذلك أن الحماية الجنائية يجب أن تقتصر على الأنظمة المحمية فنيا، لأنه من الطبيعي أن يقوم باستغلالها أي شخص ، لذا فأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم وبتوفر الحماية الأمنية ولو بقدر أدنى [18].

لكن التساؤل المطروح في هذه الحالة حول إمكانية عدم توفر نظام معلوماتي على نظام حماية فنية على قدر ما ولو كان بسيطا، ومنه من الناحية العملية أصبح من غير المعقول تقبل فكرة وجود نظام معلوماتي لا يحتوي على عنصر الحماية الفنية له ، لذا فان وجود هذه الحماية له دور كبير في تحديد القصد الجنائي لدى المجرم المعلوماتي ، ومنه لم يصبح توفر هذا الشرط محلا للنقاش في الفترة الأخيرة.

المطلب الثاني : الأركان العامة للجريمة المعلوماتية

تخضع الجريمة لنفس أركان الجرائم العامة وهي الركن الشرعي والمادي والمعنوي .

أولا : الركن الشرعي للجريمة المعلوماتية

بعد توفر الشرط الافتراضي و الأساسي للجريمة المعلوماتية ،ألا وهو نظام المعالجة الآلية للمعطيات ، يظهر الركن الشرعي لها ، وهو وجود نصوص قانونية تواجه الزحف الذي عرفته الجرائم التي مست شبكة الانترنت و الاعتداءات التي شملت خصوصية

[18] قارة أمال ، مرجع سابق ، ص 29.

الأفراد والهيئات ، حيث لجأت أغلب التشريعات الوطنية إلى فرض رقابتها وتجريمها على أوجه مختلفة للجريمة المعلوماتية .

ففي الولايات المتحدة الأمريكية نص قانونها الفدرالي على مكافحة هذه الجرائم ، كما نصت على ذلك أغلبية ولايتها ، و ألحقت كندا تجريمها بقانون العقوبات ، في حين في فرنسا تم إصدار تشريع مستقل لها بموجب القانون رقم 17/78 المؤرخ في 1978/01/16 المتعلق بقانون الإعلام الآلي والحريات " Loi sur l'informatique et la liberté".[19]

بينما في الجزائر فقد نص المشرع على مكافحة الجرائم المعلوماتية من خلال تعديله لقانون العقوبات لسنة 2004، وإضافته للقسم 7 مكرر الموضوع تحت مسمى " المساس بأنظمة المعالجة الآلية للمعطيات "" Des atteintes aux systèmes de traitement automatisé des donnes"، كما سبق وتمت الإشارة إليه .

هذه النقاط التي سنعالجها بالتفصيل من خال المحور الثالث من هذه المحاضرات.

تصدر موضوع المال المعلوماتي وحمايته موضوع هذه النصوص ، وهو ما استقر عليه الاجتهاد القضائي والفقه على ضرورة اعتبار حماية أنظمة المعالجة الآلية للمعطيات أولوية تشريعية لدى غالبية الدول.

[19] Journal officiel français du 25/01/1978.

ثانيا: الركن المادي للجريمة المعلوماتية

عرفه الفقهاء على انه كل فعل ينتج عنه توقيف نظام المعالجة الآلية للمعطيات عن أدائه الطبيعي ، وبالرغم من الجدل الفقهي الذي صاحب مفهوم النظام المعلوماتي ، حول شموله جل عناصره من عدمه ، إلا أن غالبية الفقه ترى بضرورة عدم الاشتراط أن يقع فعل التعطيل أو الإضرار للنظام جملة ، بل يكفي أن يؤثر على أحد من عناصره فقط ، كجهاز الحاسوب نفسه أو تمتد إلى شبكات الاتصال أو البرامج والمعطيات.[20]

وعليه نكون أمام الركن المادي للجريمة المعلوماتية إذا تم الاعتداء على النظام المعالجة الآلية للمعلومات أو سلامته ، كما نكون في حالة الدخول والبقاء غير المشروع في هذا النظام أو الحذف أو التغيير أو في المعطيات ، كما يمكن اعتبار التخريب أو أي إتلاف في نظام الاشتغال اعتداءات مادية (المادة 394 مكرر ق ع ج).

كل تلك الصور تضمنها المشرع الجزائري من خلال قانون العقوبات المعدل لسنة 2004، أضاف إليها عديد صور المادية الكافية لقيام الركن المادي للجريمة المعلوماتية كإدخال معلومات في نظام المعالجة الآلية أو إزالتها (المادة 394 مكرر) .

ثالثا: الركن المعنوي للجريمة المعلوماتية

يعتبر قيام الركن المعنوي لأي جريمة عنصرا ضروريا لقيام المسؤولية الجنائية ، وهو القصد الجنائي ، ولكن لخصوصية الجرائم المعلوماتية ، خاض الفقه في خصوصية كل

[20] قارة آمال ، مرجع سابق ، ص 41.

جريمة على حدى ، من أجل التأكد من وجود هذا الركن من عدمه ، في حين طرح بعض الفقه الآخر إمكانية فصل القصد الجنائي الخاص عمن العام لهذه الجرائم.

يرى اتجاه من الفقه أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الانترنت ، من حيث مدى تحديد إذا كانت تتطلب قصدا عاما أم خاصا ، فالقصد الخاص يتوافر في بعض الجرائم المعلوماتية ، خاصة وأن الجرائم المعلوماتية تقوم بتوافر القصد العام ، أي علم الجاني بمضمون فعله أنه يقوم بعمل غير مشروع ، وارتباط هذا العلم بالإرادة [21]، ومثال عنها ما حكمت به محكمة النقض الفرنسة بتوافر نية التملك الوقتي في جريمة سرقة المعلومات من جهاز الحاسوب ، ويكفي ليقام تحقق هذه النية هو سلب وحيازة المستندات خلال وقت معين بدون إرادة صاحبها الشرعي أو الحائز عليها بصفة دائمة أو مؤقتة ، أي توفر نية المشاركة في الانتفاع بها.[22]

وكذلك الحال بالنسبة لجريمة التزوير المعلوماتي ، بتوفر نية إضافية لدى الجاني ترمي إلى استعمال المستند المزور ولم يستعمل من الناحية الفعلية ، فنكون في الحالة الأخيرة أمام قصد احتمالي عند العلم بإمكانية إحداث ضرر.[23]

كل ذلك يجعلنا أمام حالة صعوبة إثبات القصد الجنائي الخاص ، وبالتالي صعوبة إثبات الركن المعنوي للجريمة المعلوماتية ، وهو من أهم الخصائص التي أوردناها سابقا.

---

[21] لورنس سعيد الحوامدة ، مرجع سابق ، ص 207.

[22] نفس المرجع ، ص 208.

[23] قارة آمال ، مرجع سابق ، ص 57.

الفصل الثاني : الجريمة المعلوماتية على مستوى المجال الدولي

نظرا للتزايد المضطرد لعدد الجرائم المعلوماتية، وما أصبحت تشكله من تهديدات حقيقية على استقرار اقتصاداتها، بات من الضروري إعادة النظر في الأجهزة الدولية المكافحة للجريمة ومدى فعاليتها.

إن محاربة الجريمة المعلوماتية ومع تطور التكنولوجيا أصبح لا يمكن تجسيده عمليا بأيادي واحدة ، فالتطور التشريعي الداخلي مهما وصل إلى ذروته يبقى قاصرا إذا لم تكن هناك تكتلات دولية وإقليمية لمحاربة هذه الظاهرة .

لذلك سعت أغلب الدول إلى الإسراع في إبرام اتفاقيات دولية ، تضمن الحماية القانونية للحد من اتساع رقعة الجريمة المعلوماتية .

لذا فإننا سنتناول في هذا المحور أهم الاتفاقيات الدولية المكافحة للجريمة المعلوماتية **(المبحث الأول)**، وكذلك على الصعيد الإقليمي **(المبحث الثاني)** .

المبحث الأول : الجريمة المعلوماتية في إطار الاتفاقيات الدولية

سنتعرض إلى الجريمة المعلوماتية في إطار اتفاقية برن بشأن الحماية المصنفات الأدبية والفنية لسنة 1886 **(المطلب الأول)** وكذلك من خلال اتفاقية تريبس للجريمة المعلوماتية لسنة 1994 **(المطلب الثاني)**.

المطلب الأول :اتفاقية برن بشأن الحماية المصنفات الأدبية والفنية (1886)

أولا : إبرام الاتفاقية وأهم تعديلاتها

تتناول اتفاقية برن حماية المصنفات وحقوق مؤلفيها،وتعتبر من أهم وأعرق الاتفاقيات الدولية التي تناولت حق المؤلف وكرست مفهوم الحماية له، وقد أبرمت هذه الاتفاقية في برن سنة 1886 وتم تنقيحها في باريس سنة 1896، وفي برلين سنة 1908، واستكملت في برن سنة 1914، وتم تنقيحها في روما سنة 1928، وفي بروكسل سنة 1948، وفي استوكهولم سنة 1967، وفي باريس سنة 1971، وجرى تعديلها سنة1979[24].

ثانيا : المبادئ التي تقوم عليها الاتفاقية

تستند هذه الاتفاقية على ثلاثة(03) مبادئ أساسية وتشمل مجموعة من الأحكام المتعلقة بالحد الأدنى للحماية الواجب منحها وبعض الأحكام الخاصة التي وضعت لمصلحة البلدان النامية، هذه المبادئ هي :

[24] الموقع الرسمي للمنظمة العالمية للملكية الفكرية WIPO: https://www.wipo.int/treaties/ar/ip/berne/summary_berne.html

1- مبدأ "المعاملة الوطنية: المصنفات الناشئة في إحدى الدول المتعاقدة (أي المصنفات التي يكون مؤلفها من مواطني تلك الدولة، أو التي نشرت للمرة الأولى في تلك الدولة) يجب أن تحظى في كل دولة من الدول المتعاقدة الأخرى بالحماية نفسها التي تمنحها لمصنفات مواطنيها[25].

2- مبدأ الحماية التلقائية: والذي يقضي بأن يجب ألا تكون الحماية مشروطة باتخاذ أي إجراء شكلي[26].

3- مبدأ "استقلال الحماية: بمعنى أن لا تتوقف الحماية هذه على الحماية الممنوحة في بلد منشأ المصنف. ومع ذلك، إذا حدد تشريع أية دولة متعاقدة مدة للحماية أطول من الحد الأدنى المنصوص عليه في الاتفاقية وتوقفت حماية المصنف في بلد المنشأ، جاز رفض الحماية عند انتهاء مدتها في بلد المنشأ.[27]

ثالثا : معايير الحماية المطلوبة

تتعلق المعايير الدنيا للحماية بالمصنفات والحقوق الواجب حمايتها ومدة الحماية:

- بالنسبة إلى المصنفات، يجب أن تشمل الحماية "كل إنتاج في المجال الأدبي والعلمي والفني، أيا كانت طريقة أو شكل التعبير عنه" كما تنص المادة 2(1) من الاتفاقية.

---

[25] الموقع الرسمي للمنظمة العالمية للملكية الفكرية، مرجع سابق.

[26] نفس المصدر.

[27] نفس المصدر.

– مع مراعاة بعض التحفظات أو التقييدات أو الاستثناءات المسموح بها، تدخل الحقوق تالية الذكر ضمن الحقوق التي يجب الاعتراف بها كحقوق تصريح استئثارية:

- حق الترجمة،
- حق تحوير المصنفات وتعديلها،
- حق الأداء العلني للمسرحيات والمسرحيات الموسيقية والمصنفات الموسيقية،
- حق تلاوة المصنفات الأدبية علنا،
- حق نقل أداء تلك المصنفات للجمهور،
- حق الإذاعة (مع جواز النص في تشريع الدولة المتعاقدة على مجرد الحق في الحصول على مكافأة عادلة بدلا من حق التصريح)،
- حق الاستنساخ بأية طريقة أو شكل كان (مع جواز نص الدولة المتعاقدة على السماح في بعض الحالات الخاصة بالاستنساخ دون أي تصريح شرط ألا يخل الاستنساخ بالاستغلال العادي للمصنف، وألا يسبب أي ضرر لا داعي له للمصالح المشروعة للمؤلف، ومع جواز النص على الحق في الحصول على مكافأة عادلة عن التسجيلات الصوتية للمصنفات الموسيقية)،
- حق استعمال مصنف ما لإنتاج مصنف سمعي بصري، وحق استنساخ ذلك المصنف أو توزيعه أو أدائه علنا أو نقله للجمهور.

وتنص الاتفاقية على بعض "الحقوق المعنوية"، أي الحق في المطالبة بنسب المصنف إلى مؤلفه والحق في الاعتراض على أي تشويه أو تحريف أو تعديل أو تقييد للمصنف من شأنه الإضرار بشرف المؤلف أو بشهرته.

رابعا: مدة الحماية الممنوحة

تستوجب القاعدة العامة منح الحماية حتى انقضاء خمسين (50) سنة من وفاة المؤلف. بيد أن هناك بعض الاستثناءات لتلك القاعدة العامة. ففي حالة نشر مصنف مغفول اسم مؤلفه أو تحت اسم مستعار، تنقضي مدة الحماية بعد 50 سنة من إتاحة المصنف قانونا للجمهور، ما لم تتضح تماما هوية المؤلف من الاسم المستعار، أو ما لم يكشف المؤلف عن هويته خلال تلك الفترة. وفي الحالة الأخيرة، تطبق القاعدة العامة. وبالنسبة إلى المصنفات السمعية البصرية (السينمائية)، تبلغ المدة الدنيا للحماية 50 سنة اعتبارا من تاريخ إتاحة المصنف للجمهور (أي عرضه) وإلا اعتبارا من تاريخ ابتكاره. وبالنسبة إلى مصنفات الفنون التطبيقية والمصنفات الفوتوغرافية، تبلغ المدة الدنيا للحماية 25 سنة اعتبارا من تاريخ ابتكارها[28].

وتسمح اتفاقية برن ببعض التقييدات والاستثناءات للحقوق المالية، وهي الحالات التي يجوز فيها الانتفاع بالمصنفات المشمولة بالحماية بدون تصريح مالك حق المؤلف، وبدون دفع أي مكافأة. ويشار إلى هذه التقييدات عادة بعبارة "الانتفاع المجاني" بالمصنفات

[28] الموقع الرسمي للمنظمة العالمية للملكية الفكرية WIPO: https://www.wipo.int/treaties/ar/ip/berne/summary_berne.html

المشمولة بالحماية، وتنص عليها المواد 9(2) (الاستنساخ في بعض الحالات الخاصة)، و10 (الاقتباس والانتفاع بالمصنفات على سبيل التوضيح لأغراض التعليم)، و10 ثانيا (استنساخ جريدة أو مواد مشابهة والانتفاع بالمصنفات بغرض الإبلاغ بالأحداث الجارية)، و11 ثانيا(3) (التسجيلات المؤقتة لأغراض البث).

ويسمح ملحق وثيقة باريس الخاصة بالاتفاقية أيضا للدول النامية بإنفاذ تراخيص غير طوعية لترجمة المصنفات واستنساخها في بعض الحالات، فيما يتعلق بالأنشطة التعليمية. وفي هذه الحالات، يُسمح بالانتفاع المشار إليه بدون ترخيص مالك الحق، بشرط دفع المكافأة التي ينص عليها القانون.

المطلب الثاني : الجرائم المعلوماتية في اتفاقية تريبس (1994)

أولا : الإطار العام لإبرام اتفاقية تربيس

هي اتفاقية دولية تديرها منظمة التجارة العالمية (WTO) الذي يحدد المعايير الدنيا للقوانين المتعلقة بالعديد من أشكال الملكية الفكرية، كما تنطبق على أعضاء منظمة التجارة العالمية .

تم التفاوض عليها في نهاية جولة الأوروغواي من الاتفاق العام بشأن التعريفات الجمركية والتجارة (القات) في ديسمبر1993، حيث تم التوقيع عليها في مدينة مراكش المغربية بتاريخ 1994/04/15.

ثانيا : أهم الشروط التي تضمنتها هذه الاتفاقية

احتفظ هذه الاتفاقية بنفس المبادئ التي تناولتها اتفاقية برن ، حيث فرصت عدة شروط تفضي إلى تعزيز عنصر الحماية للملكية الفكرية ، والتي من أهمها:

- يجب أن تمتد حقوق التأليف والنشر إلى 50 سنة بعد وفاة المؤلف.(المادتان 12 و 14)
- يجب أن تمنح حقوق المؤلف تلقائياً وليس استناداً إلى أي "شكلية"، مثل التسجيل أو التجديد.
- يجب أن يعتبر القانون برامج الحاسب الآلي "كأعمال الأدبية" تحت حقوق التأليف والنشر وأن تلقى نفس شروط الحماية.
- يجب أن تمنح براءات الاختراع في جميع "مجالات التكنولوجيا"، رغم أن بعض الاستثناءات لبعض المصالح العامة مسموح بها (المادة 27-2 و 27-3) ويجب أن تكون قابلة للتنفيذ لمدة 20 عاماً على الأقل (المادة 33).
- عدم السماح بالمساس غير المعقول بالمصالح المشروعة لأصحاب الحقوق من برامج الكمبيوتر وبراءات الاختراع و البضائع المختلفة المصنعة .
- عدم السماح بالمساس غير المعقول بالمصالح المشروعة لأصحاب العلامات التجارية , بما في ذلك استخدام العلامة التجارية دون العودة إلى مالك العلامة التجارية بشكل مباشر لانجاز اي تعامل تجاري.[29]

[29] https://ar.wikipedia.org/wiki

- على الدول الأعضاء ضمان حقوق الملكية الفكرية من العلامات التجارية و براءات الاختراع وغيرها, و ضمان عدم انتقال البضائع , البرامج او غيرها بين الدول الأعضاء بدون موافقة المالك المباشر او وكيله في المنطقة بموافقة من المالك المباشر.

ثالثا : تكريس الحماية الجنائية من الجريمة المعلوماتية في اتفاقية تريبس

تضمن القسم الخامس من هذه الاتفاقية ما اصطلح على تسميتها بالإجراءات الجنائية، حيث يقتضي الاتفاق أن تنص الأعضاء في قوانينها على إجراءات وعقوبات جنائية تطبق على الأقل في حالات التقليد المتعمد للعلامات التجارية المسجلة أو انتحال حقوق المؤلف على نطاق تجاري ، وأن تنص الأعضاء أيضا على الجزاءات كالحبس أو الغرامة المالية والحجز ومصادرة وإتلاف السلع المتعدية أو أية مواد ومعدات تستخدم بصورة رئيسية في ارتكاب الجرم.[30]

وطالما أن هذه الاتفاقية قد ساوت بين برامج الحاسب الآلي و الأعمال الأدبية وتمتعهما بنفس شروط الحماية ، فان المساس بالأنظمة المعلوماتية يعد من الجرائم التي تناولها القسم الخامس من هذا الاتفاقية ، حتى و لم يتم التصريح المباشر بها.

[30] القسم الرابع من اتفاقية التريبس المتعلقة بإنفاذ حقوق الملكية لفكرية – الجزء الثالث–

المبحث الثاني : الجريمة المعلوماتية في الإطار الإقليمي

سنحاول التطرق إلى المجهودات المبذولة على الصعيد الأوروبي والذي يبرز من خلال اتفاقية بودابست 2001(**المطلب الأول**) وكذلك على صعيد الدول العربية من خلال القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصال لسنة 2004 (**المطلب الثاني**) .

المطلب الأول : اتفاقية بودابست بشأن جرائم الانترنت لسنة 2001

Convention sur la cybercriminalité

تظهر الجهود الإقليمية بشكل بارز من خلال مساعي مجلس أوروبا الذي تأسس سنة 1949 بعد نهاية الحرب العالمية الثانية ، بهدف القضاء على الأفكار الديكتاتورية المرتبطة بالأنظمة الشمولية ، والبالغ عدد أعضائها 41 عضوا منذ سنة 1997[31].

سعى هذا المجلس نحو مكافحة الجريمة مع المحافظة على حرمة الحياة الخاصة، وفي هذا السياق يرى مؤسسو هذه الهيئة أن عقوبة الإعدام لا مكان لها في المجتمعات الديمقراطية. حيث تم في أبريل 1983 ، اعتماد البروتوكول رقم 6 الملحق بالاتفاقية الأوروبية لحقوق الإنسان ، الذي يلغي عقوبة الإعدام في وقت السلم ، وفي مايو 2002،

[31] الموقع الرسمي لمجلس أوروبا : https://www.coe.int/fr/web/about-us/achievements

البروتوكول رقم 13 بشأن الإلغاء في جميع الظروف، ووصل به الأمر إلى اعتبار فرض إلغاء عقوبة الإعدام شرطا مسبقا للانضمام لهذه الهيئة .[32]

ومع تطور مفهوم الجريمة المعلوماتية سعت الهيئة المذكورة آنفا إلى إبرام معاهدة ساهم في صياغتها عدد كبير من الخبراء القانونيين وبمساعدة دول أخرى لاسيما الولايات المتحدة الأمريكية ، كما تمت إثرها القيام بعديد المشاورات بين حكومات أعضاء المجلس و أجهزة الشرطة والمشرفين على القطاعات المعنية بأجهزة الكمبيوتر، مما ساهم في توقيع 30 دولة بتاريخ 23 نوفمبر 2001في العاصمة المجرية بودابست، لمكافحة الاستخدام غير المشروع للحسابات وشبكات المعلومات[33] .

أولا : مضمون اتفاقية بودابست

تناولت الاتفاقية في مقدمتها الإشارة إلى ثورة تكنولوجيات المعلومات المجتمعية بشكل جوهري، وتأثيرها على مستقبل فئات المجتمع، واجتياح تكنولوجيا المعلومات بشكل أوبآخر تقريبا كل جوانب الأنشطة البشرية، [34] التي تجاوزت الاتصالات الهاتفية المنطوية على نقل صوت الإنسان إلى تبادل كميات هائلة من البيانات، بما في ذلك الصوت، والنص، والموسيقى والصور الثابتة والمتحركة، والتي لم يعد هذا التبادل محصورا فيها بين البشر، حيث تعدتها بين البشر والحواسيب، وبين أجهزة الكمبيوتر نفسها، بغض النظر عن بعد

---

[32] الموقع الرسمي لمجلس أوروبا، مرجع سابق.

[33] محمد علي العريان، الجرائمالمعلوماتية ، دار الجامعة الجديدة ،جامعةالإسكندرية ، ،مصر ،2011، ص25.

[34] التقرير التفسيري لاتفاقية الجريمة الالكترونية، انظر الموقع الرسمي لمجلس أوربا https://www.coe.int/fr/، مرجع سابق.

المسافات الجغرافية، ومنه حدوث نمو هائل في حجم المعلومات المتاحة والمعرفة التي يمكن استخلاصها من منها.[35]

و تعرضت المقدمة إلى التطورات التي شملت مختلف الجوانب الاقتصادية والاجتماعية التي صاحبها تدفق للمعلومات والاتصالات بسهولة أكبر من جميع أنحاء العالم لاغية لمفهوم الحدود ، لذا تظل القوانين الوطنية محصورة بشكل عام في إقليم معين، ومنه فمهمة القانون الدولي هي إيجاد الحلول للمشاكل المتعلقة بامتداد رقعة الجريمة المعلوماتية مع المحافظة على احترام حقوق الإنسان في مجتمع المعلومات الجديد.[36]

ثانيا : بنود الاتفاقية Les chapitres du convention

تضمنت الاتفاقية أربعة فصول:

- **الفصل الأول** : وضع تحت مسمى "استخدام المصطلحات"
- **الفصل الثاني** : وشمل التدابير الواجب اتخاذها على الصعيد المحلي بموجب القوانين الموضوعية وكذا الإجرائية
- **الفصل الثالث** : خصّص لمجال التعاون الدولي
- **الفصل الرابع** : فتناول الأحكام الختامية للاتفاقية

1- استخدام المصطلحات كآلية طوعية لتوضيح المفاهيم : سعت الاتفاقية إلى ضرورة الوصول إلى مقاربة في توحيد المصطلحات المرتبطة بالجريمة المعلوماتية ، ولكن على

[35] التقرير التفسيري لاتفاقية الجريمة الالكترونية.

[36] نفس المرجع.

أساس طوعي وليس إلزامي ، وهذا ما ما نستشفه من خلال المادة الأولى من الاتفاقية ، والتي تنص على أنه : " لأغراض هذه الاتفاقية ، فإن التعبير ..."[37] ، والذي صرحت به من خلال الفقرة د من المادة الأولى حيث نصت على أن " **يترك التعريف للمجالس التشريعية الوطنية القدرة على إدخال تمييز في الحماية القانونية لبيانات الحركة وفقا لحساسيتها**،" هذه المفاهيم شملت 04 عناصر هي :

العنصر الأول : نظام الكمبيوتر système informatique

عرفت الاتفاقية نظام الكمبيوتر بأنه :" **يعني أي جهاز واحد أو مجموعة من الأجهزة مترابطة أو ذات صلة ، والتي تضمن أو تمنح أي عنصر أو أكثر معالجة آلية للبيانات في تنفيذ البرنامج** "، ويقصد بمصطلح "آلي" أي دون تدخل بشري مباشر.

العنصر الثاني : بيانات الكمبيوتر données informatiques

عرفت اتفاقية بودابست بيانات الكمبيوتر على أنه " **تعني أي تمثيل للحقائق أوالمعلومات أو المفاهيم في شكل يفسح المجال لمعالجة الكمبيوتر ، بما في ذلك برنامج للتأكد من أن نظام الكمبيوتر يؤدي وظيفة**" ، و لتوضيح أن البيانات الواردة في هذه الاتفاقية يجب أن تُفهم على أنها بيانات في شكل إلكتروني أو أي شكل آخر قابل للمعالجة الآلية ، تم إدخال مفهوم "بيانات الكمبيوتر"، ويمكن أن تكون بيانات الكمبيوتر التي تتم معالجتها آليا

[37]L'article 1 de la convention stipule que " aux fins de la présente convention, l'expression:..."

موضوع إحدى الجرائم الجنائية المحددة في هذه الاتفاقية وكذلك موضوع تطبيق أحد تدابير التحقيق المحددة في هذه الاتفاقية.[38]

العنصر الثالث : مزوّد الخدمة fournisseur de service

تضمنت الفقرة د من المادة 1 من الاتفاقية تعريفا لمزود الخدمة على أنه " **يعني أي كيان عام أو خاص يقدم لمستخدمي خدماته القدرة على التواصل باستخدام نظام الكمبيوتر**" ، ومنه بموجب هذا التعريف يتضح لنا أن جميع مشمولة بموجب هذا التعريف سواء كانت عامة أو خاصة التي توفر للمستعملين القدرة على التواصل فيما بينهم .

العنصر الرابع : بيانات المرور données relatives au trafic

تضمنت المادة 1 من الاتفاقية في فقرتها د إعطاء تعريف لبيانات المرور ، حيث عرفتها بأنها ""**بيانات المرور" تعني أي بيانات تتعلق بالاتصال من خلال نظام الكمبيوتر ، التي تنتجها هذه الأخيرة كجزء من قناة اتصال ، تشير إلى الأصل والوجهة والطريق والوقت والتاريخ ، حجم ومدة الاتصال أو نوع الخدمة الأساسية** "

يظهر من خلال هذا التعريف أن بيانات المرور فرعية ومساعدة للاتصال في حد ذاته، ففي في حال التحقيق في جريمة جنائية ارتكبت من خلال نظام كمبيوتر، تكون هنالك حاجة إلى بيانات المرور لتعقب مصدر الاتصال كنقطة انطلاق من أجل جمع أدلة إضافية أوكجزء من الأدلة على الجريمة،لكن ولأن بيانات المرور معرضة للزوال، مما

[38] التقرير التفسيري لاتفاقية الجريمة الالكترونية، انظر الموقع الرسمي لمجلس أوربا https://www.coe.int/fr/ ، مرجع سابق.

يدعو إلى الأمر بالتعجيل بحفظها، ونتيجة لذلك،قد يكون من الضروري الكشف السريع عنها بغية تحديد طريق الاتصال من أجل جمع المزيد من الأدلة قبل حذفها أو بغية التعرف على المشتبه به. [39]

حدد هذا التعريف فئات بيانات المرور التي تخضع معالجتها لنظام خاص في هذه الاتفاقية وهي:

- منشأ الاتصال- وجهة الاتصال – طريقة الاتصال – وقت الاتصال – تاريخ الاتصال و حجمه- مدته ونوع الخدمة التي ينطوي عليها.

ومن الضروري أن نقف عند مصطلح "**المنشأ**" الذي يشير إلى رقم الهاتف أو عنوان بروتوكول الإنترنت (IP) أو ما شابه ذلك من هوية هيئة الاتصالات التي يزودها مزود الخدمة بخدماته، ويقصد بمصطلح "**الوجهة**" العنوان المماثل لهيئة الاتصالات التي تنقل إليها الاتصالات.[40]كما تشير عبارة "**نوع الخدمة التي ينطوي عليها**" إلى نوع الخدمة التي يتم استخدامها داخل الشبكة، مثل نقل الملفات، أو البريد الإلكتروني أو الرسائل الفورية.[41]

2- التدابير الواجب اتخاذها على الصعيد الوطني

[39] التقرير التفسيري لاتفاقية الجريمة الالكترونية ، مرجع سابق.

[40] نفس المرجع.

[41] نفس المرجع.

تضمن الفصل الثاني من اتفاقية بودابست (من المادة 2 إلى المادة 22) ثلاثة أقسام وهي: القانون الجنائي الموضوعي (المواد من 2 إلى 13)،والقانون الإجرائي (المواد من 14 إلى 21) والولاية القضائية (المادة 22).

2-1 خصص القسم الأول من الفصل 2 للقانون الجنائي الموضوعي Droit pénal matériel

والذي تناول عدة مواضيع هي :

أ-الجرائم ضد سرية وسلامة وتوفر بيانات وأنظمة الكمبيوتر

Infractions contre la confidentialité ,l'intégrité et la disponibilité des données et systèmes informatiques

تطرقت المواد من 2 الى 6 من الاتفاقية للجرائم التي وصفت بأنها لها علاقة بسرية وسلامة وتوفر بيانات وأنظمة الكمبيوتر ، والمتمثلة في الجرائم التالية :

أ-1- النفاذ غير الشرعي "Accès illegal " "المادة 2": عرفته اتفاقية بودابست على أنه " **الوصول المتعمد وغير القانوني إلى جزء من نظام الكمبيوتر.**" كما اعتبرت نفس المادة أنه يجوز لأي طرف أن يطلب ارتكاب الجريمة لخرق التدابير الأمنية ، بقصد

الحصول على بيانات الكمبيوتر أو في توافر نية إجرامية أخرى ، أو فيما يتعلق بنظام كمبيوتر متصل بنظام الكمبيوتر الآخر.[42]

يتألف "النفاذ" من الدخول الكامل أو الجزئي إلى نظام الكمبيوتر **(المعدات، والمكونات والبيانات المخزنة في النظام المثبت، والدلائل، وبيانات الحركة، والبيانات ذات الصلة بالمحتوى)**. ومع ذلك، لا يتضمن مجرد إرسال رسالة عن طريق البريد الإلكتروني أو ملف إلى هذا النظام. ويشمل "النفاذ" الدخول إلى نظام كمبيوتر آخر، حيث يتم ربطه عبر شبكات الاتصالات العامة، أو بنظام كمبيوتر على نفس الشبكة، مثل شبكة اتصال محلية LANأو شبكة إنترانت داخل منظمة[43].

أ-2- الاعتراض غير الشرعي "Interception illégale " "المادة 3" : عرفته على أنه " **الاعتراض المقصود وغير القانوني الذي تم تنفيذه بالوسائل التقنية ، وبيانات الكمبيوتر ، أثناء الإرسال غير العام أو من أو داخل نظام الكمبيوتر ، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام كمبيوتر يحمل مثل هذه البيانات ."**[44] والمقصود

---

[42] L'article 2 de la convention stipule que " ..l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique."

[43] التقرير التفسيري لاتفاقية الجريمة الالكترونية، مرجع سابق.

[44] L'article 3 de la convention stipule que " .. l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y

بالإرسال غير العام أي غير الموجه للجمهور، والمقصود هنا طبيعة عملية الإرسال، وليس طبيعة البيانات المرسلة، فيمكن أن تكون البيانات التي يتم إرسالها معلومات متاحة للجمهور، ولكن الأطراف ترغب في التواصل بشكل سري، كما يمكن الاحتفاظ بسرية البيانات لأغراض تجارية حتى يتم دفع مقابل الخدمة، كما هو الحال في خدمة التلفزيون المدفوع [45].

ينطوي الاعتراض بواسطة "وسائل تقنية أو فنية" على التنصت على محتوى الاتصالات أو رصده أومراقبته، أو شراء محتوى البيانات سواء بطريقة مباشرة من خلال الولوج إلى نظام الكمبيوتر واستخدامه، أو بطريقة غير مباشرة عن طريق استخدام أجهزة اختلاس السمع أو التنصت الإلكترونية. ويمكن أن ينطوي الاعتراض أيضا على التسجيل، كما تشمل الوسائل التقنية الأجهزة التقنية المثبتة على خطوط النقل وكذلك أجهزة جمع وتسجيل الاتصالات اللاسلكية، ويمكن أن تشمل استخدام البرمجيات وكلمات المرور والرموز.[46]

- المساس بسلامة المعطيات " Atteinte à l'intégrité des données "

المادة4: الذي عرفته بأنه "**كل عمل متعمد وبدون حق يهدف إلى الإضرار أوالتخريب**

---

compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques .."

[45] التقرير التفسيري لاتفاقية الجريمة الالكترونية، مرجع سابق.

[46] نفس المرجع.

أوالحذف أو الإتلاف أوالتغيير في البيانات" [47]، وفي هذه الأفعال المجرمة بهدف حماية بيانات وبرامج الكمبيوتر المخزنة الكمبيوتر وفي تشغيلها واستخدامها ، يرتبط "**الإضرار**" و"**التخريب**" عملان متداخلان، وكلاهما بهدف الى التغيير السلبي في سلامة البيانات والبرامج أو محتواها الإعلامي. بينما يعتبر "**حذف**" البيانات مطابقا لتدمير الشيء المادي، حيث يتم تدميرها وجعلها غير قابلة للتعرف. [48]

ويقصد **بـ"إتلاف"** بيانات الكمبيوتر كل عمل يمنع أو ينهي توافر البيانات للشخص الذي لديه حق المرور إلى الكمبيوتر أو لوسيلة حفظ البيانات التي تم تخزين البيانات عليها، بينما يعني مصطلح "**التغيير**" تعديل البيانات القائمة، ومنه فإن إدخال رموز خبيثة، مثل الفيروسات وأحصنة طروادة، مشمولة في هذه الفقرة، كما هو الحال بالنسبة للتعديل الناجم عن البيانات.[49]

- المساس بسلامة النظام " Atteinte à l'intégrité du système " المادة 5:

والتي تعني تجريم العرقلة المتعمدة للاستعمال المشروع للأنظمة المعلوماتية بما في ذلك المرافق المسؤولة عن عملية الاتصالات من خلال استخدام بيانات الكمبيوتر أو التأثير عليها ، وكمثال توضيحي عن هذه الجرائم، البرامج التي تولد هجمات "الحرمان من الخدمة"، و"الرموز الخبيثة" مثل الفيروسات التي تمنع أو تبطئ بشكل كبير تشغيل النظام،

---

[47] L'article 4 de la convention stipule que " .. le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques".

[48] التقرير التفسيري لاتفاقية الجريمة الالكترونية، مرجع سابق.

[49] نفس المرجع.

أو "البرامج التي ترسل كميات هائلة من البريد الإلكتروني إلى المتلقي" من أجل إعاقة وظائف الاتصال في النظام.[50]

– **إساءة استخدام الأجهزة "Abus de dispositifs " المادة 6** وتعني كل فعل متعمد وغير قانوني يتم ارتكابه ويكون متعلقا بأجهزة معينة أو ببيانات المرور التي يساء استخدامها لغرض ارتكاب الجرائم المذكورة أعلاه ضد سرية وسلامة وتوافر أنظمة أو بيانات الكمبيوتر، والتي غالبا ما يتطلب حيازة وسائل المرور المتمثلة في أدوات القراصنة.

ب– الجرائم المعلوماتية Infractions informatiques

حددت الاتفاقية جريمتين مرتبطتين بالكمبيوتر نفسه وهما :

–جريمة التزوير المعلوماتي "Falsification informatique " المادة 7والتي عرفتها بأنها "**الأفعال التي تكون مقدمة أو مسببة إلى تغيير أو محو أو حذف متعمد وبدون وجه حق لبيانات الكمبيوتر لاستخدامها لأغراض قانونية كما لو كانت صحيحة.**" كما تركت الاتفاقية السلطة التقديرية للتشريعات الداخلية في مدى اعتبار توفر نية احتيالية أو نية جنائية كشرط لقيام المسؤولية الجنائية، مما تعني اختيارية اعتماد توفر القصد الجنائي في هذه الجريمة لدى الدول الأعضاء.

[50] التقرير التفسيري لاتفاقية الجريمة الالكترونية، مرجع سابق.

- **جريمة الاحتيال المعلوماتي "Fraude informatique** " "المادة 8" ، والذي عرفته بأنه "**الفعل المتعمد وغير القانوني الذي يتسبب في فقدان ممتلكات لدى الآخرين عن طريق:**

- **إدخال أو تغيير أو محو أو حذف بيانات الكمبيوتر ،0**

- **أي شكل من أشكال التدخل في تشغيل نظام الكمبيوتر ، بتوفر نية احتيالية أوجنائية للحصول بدون وجه حق ، على منفعة اقتصادية للذات أو للآخرين."[51]**

وفي هذا يظهر الفرق بين جريمة التزوير المعلوماتي التي لم يشترط توفر القصد الجنائي لإقرارها بعكس الحالة الثانية المرتبطة بالاحتيال الالكتروني التي اشترطت توفر النية الاحتيالية ، كما اشترطت نفس المادة المساس بضرر اقتصادي من أجل تحقيق منفعة اقتصادية سواء للمرتكب الفعل أو لغيره.

ج- الجرائم التي لها علاقة بمحتوى الكمبيوتر Infractions se rapportant au contenu

- **الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية" Infractions se rapportant à la pornographie enfantine " المادة 9 :** حيث عالجت

[51] [51] L'article 8 de la convention dispose que " .. le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par: a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques, b. toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui."

هذه المادة مختلف الجرائم المتعلقة بالإنتاج الإلكتروني والحيازة والتوزيع للمواد الإباحية التي تعرض صورا للأطفال. و محاربة كل أشكال الاستغلال الجنسي للأطفال وتعريضهم للخطر، والتي تندرج ضمنها:

- **إنتاج المواد الإباحية** المتعلقة بالأطفال لأغراض التوزيع عن طريق نظام الكمبيوتر- **فقرة أ-**

- **عرض المواد الإباحية** المتعلقة بالأطفال عن طريق نظام الكمبيوتر-**فقرة ب-**

- **توزيع أو بث** المواد الإباحية المتعلقة بالأطفال عن طريق نظام الكمبيوتر-**فقرة ج-**

- **شراء** أو **الشراء للآخرين** المواد الإباحية المتعلقة بالأطفال.-**فقرة د-**

- **حيازة** مواد إباحية للأطفال في نظام كمبيوتر أو أي وسيلة تخزين بيانات الكمبيوتر- **فقرة هـ-** مثلا عن طريق تحميلها.

د- الجرائم الانتهاكات المتعلقة بالمساس بحقوق الملكية الفكرية والحقوق المجاورة" Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes المادة 10

هـ- جرائم تترتب عليها أشكال أخرى من المسؤولية والعقوبات Autres formes de responsabilité et de sanctions المادة 11-12 ، والتي تناولت التواطؤ (م11) ومسؤولية الأشخاص المعنويين (م 12).

و- اختتم هذا القسم بالمادة 13 التي تضمنت مجموعة من العقوبات والتدابير: حيث ألزمت كل طرف باعتمادها كتدابير تشريعية وتدابير أخرى تبعا للمخالفات الجنائية المرتبطة بالمواد من 2 – 11 بحيث تكون قابلة لعقوبات فعالة ومتناسبة ورادعة ، بما في ذلك أحكام الحبس.

كما يجب على كل طرف التأكد من أن الأشخاص الاعتباريين المسؤولين بموجب أحكام المادة 12 يخضعون لعقوبات أو تدابير جنائية أو غير جنائية تكون فعالة ،متناسبة ورادعة ، بما في ذلك العقوبات المالية.

2-2 خصص القسم الثاني من الفصل 2 للقانون الجنائي الإجرائي Droit procédural

تناول هذا القسم عديد الجوانب التي لها علاقة بمختلف الجوانب الإجرائية في مجال مكافحة الجريمة المعلوماتية ، حيث تم التطرق إلى نطاق تطبيق تدابير القانون الإجرائي (م 14) ، والى النسخ الاحتياطي (م15) وكذلك تم التطرق إلى حفظ النسخ والحفظ السريع لمعطيات الكمبيوتر المخزنة(م16)، كذا تقاطع المنتوج " Injonction de produire " (م18).

3-2 خصص القسم الثالث من نفس الفصل إلى الاختصاص Compétence

3- التعاون الدولي : Coopération internationale

اخضعت هذه الاتفاقية شروط إبرامها إلى مجموعة من المبادئ بين دول الأعضاء ، منها:

- **مبادئ عامة** : والتي منها

أ- المبادئ المتعلقة بتسليم المجرمين "Principes relatifs à l'extradition (م24)"

ب- المبادئ المتعلقة بالمساعدة المتبادلة " Principes généraux relatifs à l'entraide "(م25)

ج- مبدأ سرية وتقييد الاستخدام " Confidentialité et restriction d'utilisation "(م28)

- **مبادئ نوعية** : أهم هذه المبادئ

أ-المساعدات المتبادلة للتدابير المؤقتة " Entraide en matière de mesures provisoires "(م29)

ب-المساعدات المتبادل مع سلطات التحقيق " Entraide concernant les pouvoirs d'investigation ": وذلك في مجال الوصول إلى البيانات المخزنة(م31) وفي مجال **الوصول عبر الحدود إلى البيانات المخزنة ، بموافقة أوهل هي في متناول الجمهور**" **Accès transfrontière à des données stockées, "avec consentement ou lorsqu'elles sont accessibles au public** **م 32.**

4- الأحكام الختامية للاتفاقية : تناولت الاتفاقية في أحكامها الختامية شروط توقيعها من قبل أعضاء مجلس أوروبا ، كما منحت حق التوقيع إلى الدول التي ساهمت في إعدادها ، في حين حددت تاريخ دخولها حيز التنفيذ في اليوم الأول من الشهر التالي لانتهاء مدة ثلاثة أشهر بعد التاريخ الذي شمل توقيع 5 دول ،3 على الأقل يكونون من مجلس أوروبا، كما تنص المادة 36-3، كما حددت المادة 39 من الاتفاقية آثار هذه الاتفاقية ، وشروط تعديلها(م44) .

المطلب الثاني : القانون العربي النموذجي الاسترشادي لمكافحة الجريمة المعلوماتية لسنة 2004

أولا : حتمية توحيد الجهود العربية في نص اتفاقية لمكافحة الجريمة المعلوماتية

بعد اتساع رقعة الجريمة المعلوماتية ، وفرض سيطرتها على الصعيد العالمي ، وبعد أن تجسيد محاصرة مجلس أوروبا لهذا التوغل بموجب اتفاقية بودابست وجدت الدول العربية نفسها مجبرة على توقيع اتفاقية إقليمية نحارب كل أشكال هذه الجريمة ، حيث قد صدر ما اصطلح على تسميته **بالقانون العربي النموذجي الاسترشادي بخصوص مكافحة الجريمة المعلوماتية** نتيجة عمل مشترك بين وزراء الداخلية العرب ومجلس الوزراء العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن قدم كلا المجلسين مشروعا

بخصوص مكافحة الجريمة المعلوماتية[52]، اعتمد هذا القانون من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بموجب القرار رقم 495 المؤرخ في 2003/10/08 ، ومن قبل مجلس وزراء الداخلية العرب في دورته الحادية والعشرين.[53]

ثانيا :الجرائم الواردة في القانون العربي النموذجي الاسترشادي لسنة 2004

تضمن هذا القانون مجموعة من الجرائم المرتبطة بإساءة استخدام مختلف تقنيات المعلومات ، وهي :

1- جريمة غسل الأموال عبر الوسائط الإلكترونية: وهي الجريمة التي نصت عليها المادة 19 من هذا القانون ، حيث اعتبرت أن كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه للمصدر غير المشروع لها أو إخفائه أو قام باستخدام أو اكتساب أوحيازة الأموال، مع العلم أن مصادرها غير مشروعة عن طريق استخدام الحاسب الالكتروني أو شبكة المعلومات الدولية بقصد إضفاء الصفة المشروعة على هذه الأموال ، يتعرض إلى العقوبة مع ترك تقدير العقوبة المناسبة لكل دولة.

ما يمكن استنتاجه هو أن نص هذا القانون حدد صور هذه الجريمة في ما يلي :

- تحويل الأموال غير المشروعة أو نقلها

- تمويه للمصدر غير المشروع لها أو إخفائه

---

[52] بدري فيصل، مكافحة الجريمة في القانون الدولي والداخلي ، أطروحة دكتوراه في القانون العام ،كلية الحقوق ، جامعة الجزائر ، 2018، ص33-34.

[53] نفس المرجع، ص34.

- القيام باستخدام أو اكتساب أو حيازة الأموال، مع العلم أن مصادرها غير مشروعة

كما ربط استخدام هذه الصور وفق آلية ليست بالتقليدية، بل عن طريق استخدام الحاسب الالكتروني أو شبكة المعلومات الدولية.

نجد من هذه الجرائم المنتشرة على الصعيد الدولي والإقليمي :

- **استخدام بطاقات الائتمان لشراء الأشياء الثمينة:** كالأعمال الفنية ، حيث يتم تسديدها لاحقا بالأموال الناتجة عن تبييض الأموال.
- **استخدام البطاقات البلاستيكية في جرائم غسل الأموال :** وذلك عن طريق استخدام البطاقات الممغنطة بعدة عمليات تسهل عملية غسل الأموال.[54]
- **أعمال الصيرفة الالكترونية :** الناجمة عن عملية امتلاك مصرف وإدارته عن طريق استخدام الصيرفة الالكترونية (سويفت SWIFT) ، وهي خدمة خاصة بنقل الأموال وتقديم خدمات مالية الى الوسطاء وتجار السندات وشركات المقاصة والشركات المالية الكبرى .[55]

2- جريمة التزوير المعلوماتي : وذلك بالرجوع إلى أحكام المادة الرابعة من القانون التي اعتبرت أن كل من زور المستندات المعالجة آليا أو البيانات المسجلة في ذاكرة الحاسوب أو على شريط أو أسطوانة ممغنطة أو غيرها من الوسائط ، يتعرض للعقوبة، وكذلك على

---

[54] طرشي نورة ، مكافحة الجريمة المعلوماتية ، ماجستير في القانون الجنائي ، كلية الحقوق ، جامعة الجزائر ، 2012، ص 84.

[55] نفس المرجع ، ص 83.

مستخدمي هذه المستندات مع العلم بتزويرها الذي توقع عليه نفس العقوبة ، مع انتهاج نفس ما تبناه هذا النص مع الجريمة السابقة وذلك بترك تقدير العقوبة المناسبة للدول الأعضاء.

3- جريمة السرقة المعلوماتية : تضمنت المادة 14 من القانون النموذجي تجريم كل أشكال السرقة العلمية المرتبطة بعمليات نسح ونشر المصنفات الفكرية والأدبية والأبحاث العلمية ، عند ارتكابها دون وجه حق ، حيث تعرض مرتكبوها للعقوبة ، مع ترك تقدير العقوبة للقوانين الداخلية في ظل احترام قوانين الملكية الفكرية للدول الأعضاء .

4- جريمة اختراق النظم المعلوماتية : نصت المادة الثالثة من القانون النموذجي على أن كل من توصل بطريقة التحايل لاختراق المعالجة الآلية للبيانات يعاقب بالحبس والغرامة ، حيث تركت تقدير العقوبة للدولة ، كما أضافت نفس المادة في فقرتها الثانية اعتبار انه إذا نتج عن هذا الفعل محو أو تعديل البيانات المخزنة بالحاسب أو تعطيل تشغيل النظام بسبب تسريبات للفيروسات أو غيرها من الأساليب المعلوماتية ، يكون معرضا صاحبها إلى العقوبة والحبس .

يظهر تأثر واضعو هذا النص الواضح باتفاقية بودابست مع تم اعتماده من مفاهيم في كيفية التعامل مع فكرة أنظمة المعالجة الآلية للمعطيات.

المطلب الثالث : الصعوبات الإجرائية في مكافحة الجريمة المعلوماتية على الصعيد الدولي

بالرجوع إلى الأعمال التحضيرية التي سبقت اتفاقية بودابست والى ما تم التطرق إليه من خلال مختلف الاتفاقيات الدولية و الإقليمية ، يمكن تخليص أهم الصعوبات الإجرائية التالية :

1- **التزايد المضطرد لمختلف الجرائم المتعلقة بالفضاء الإلكتروني:** لا سيما الجرائم المرتكبة من خلال استخدام شبكات الاتصالات السلكية واللاسلكية عن طريق الإنترنت، والتي من أهمها المعاملات المالية غير المشروعة، أو تقديم خدمات غير قانونية، وانتهاك حقوق التأليف والنشر، علاوة على الجرائم التي تنتهك كرامة الإنسان وحماية القاصرين.[56]

2- **صعوبة تبني مقاربة مشتركة لأغراض التعاون الدولي في مجال القوانين الجنائية الموضوعية** : هذه المسائل تخاطب مباشرة إشكالية التعريف بكل جريمة والعقوبات المناسبة لها ومسؤولية الفاعلين في الفضاء الإلكتروني، بما في ذلك مزودو خدمات الإنترنت.[57]

3- **استخدام سلطات قسرية قليلة الفعالية** : تظهر هذه الصعوبة بشكل واضح في مجال الاستخدام العابر للحدود، وقابلية تطبيقها في بيئة تكنولوجية، مثل اعتراض الاتصالات

---

[56] التقرير التفسيري لاتفاقية الجريمة الالكترونية ، مرجع سابق.

[57] نفس المرجع.

السلكية واللاسلكية والمراقبة الإلكترونية لشبكات المعلومات، لاسيما عن طريق شبكة الإنترنت، لذا يستلزم البحث في نظم معالجة المعلومات ومصادرتها ، بما في ذلك مواقع الإنترنت، مما يجعل مواد غير قانونية غير قابلة للنفاذ ويتطلب من مقدمي الخدمات الامتثال لالتزامات خاصة، مع مراعاة المشاكل الناجمة عن تدابير خاصة بسلامة المعلومات، كالتشفير مثلا.[58]

4- **الصعوبات المرتبطة بالاختصاص القضائي للجرائم المعلوماتية :** تظهر أهمية تحديد المكان الذي ارتكبت فيه الجريمة من أجل تحديد القانون الواجب تطبيقه ، لذا تظهر مشكلة " عدم جواز المحاكمة على ذات الجرم مرتين " في حال تعدد الاختصاصات القضائية، ومسألة كيفية حل تنازع الاختصاص الإيجابي وطريقة تفادي النزاعات السلبية المرتبطة بالاختصاص القضائي[59]، كل تلك الإشكاليات المرتبطة بتحديد الاختصاص القضائي ظلت ولا زالت تشكل هاجسا لدى خبراء القانون الدولي في مجال مكافحة هذه الجريمة .

فكيف تعامل المشرع الجزائري مع هذه الجريمة في مجال مكافحتها موضوعيا واجرائيا ، فعليه ستكون الإجابة على التساؤل هو محور دارستنا اللاحق و المتعلق بمكافحة الجريمة المعلوماتية في نطاق القانون الداخلي.

---

[58] التقرير التفسيري لاتفاقية الجريمة الالكترونية، مرجع سابق .

[59] نفس المرجع .

الفصل الثالث : الجريمة المعلوماتية في نطاق القانون الداخلي

سنتناول من خلال هذا المحور الجريمة المعلوماتية في مجال قانون العقوبات الجزائري **(المبحث الأول)**، وخارج مجال قانون العقوبات **(المبحث الثاني)**

المبحث الأول : الجريمة المعلوماتية في مجال قانون العقوبات الجزائري

وذلك من خلال التطرق إلى الجرائم المعلوماتية الماسة بأنظمة المعالجة الآلية للمعطيات **(المطلب الأول)** والجرائم الواقعة على الأشخاص و الأموال **(المطلب الثاني)** وكذا الواقعة على الهيئات العامة **(المطلب الثالث)**.

المطلب الأول: الجرائم المعلوماتية الماسة بأنظمة المعالجة الآلية للمعطيات

خطى المشرع الجزائري خطوات كبيرة في مجال مكافحة الجريمة المعلوماتية ، يعتبر القانون الجزائري سباقا في مجال مواكبة التشريعات الغربية التي سعت إلى هذا النوع من التجريم كالأمريكي والفرنسي،[60] وذلك بعد أن أقر بتجريم صور الاعتداء على شبكة الانترنت والمساس بالبيانات المعالجة آليا ، في إطار أحكام التعديل الذي شمل قانون العقوبات لسنة 2004 ، بموجب القانون رقم 04-15 المؤرخ في 2004/11/10[61] ، في

[60] زبيحة زيدان ، مرجع سابق ، ص48.

[61] الجريدة الرسمية عدد 71 المؤرخة في 2004/11/10، ص 8.

إطار أحكام القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات ، هذه المواد هي من 394 مكرر إلى 394 مكرر 7 ، والمتمثلة في الجرائم التالية :

أولا : جريمة الدخول في كل أو جزء من منظومة للمعالجة الآلية لمعطيات (م 394 مكرر/1) أو محاولة ذلك

تنص المادة 394 مكرر على أنه " **يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الإلية للمعطيات أو يحاول ذلك.** " لقد جرم المشرع فعل الدخول بطريق غير شرعية إلى أي منظومة معلوماتية دخولا غير شرعي ، وذلك حين عبر عنه بطريق الغش ، كما أن المشرع لم يفرق بين الدخول إلى جزء من المنظومة أوكلها.

وهنا سيتخلص من نص المادة ما يلي :

- التسليم بتوفير القصد الجنائي بمجرد الدخول إلى نظام معلوماتي عن طريق الغش.
- عدم الاعتداد بنتائج هذا الدخول حتى ولو يسبب أي تخريب أو إضرار بالبيانات ، لكون اعتبارها جريمة وقتية .
- مجرد المحاولة يعتبر في حد ذاته جريمة حتى وان لم يتحقق فعلا.

ثانيا: جريمة البقاء (م 394 مكرر/1)

بالرجوع إلى نفس المادة السابقة وفي نفس الفقرة 1 فان المشرع قد فرق بين فعل الدخول غير الشرعي والبقاء فيه ، وذلك باعتبار كل فعل يعتبر مجرما ، فالبقاء قرينة على توفر القصد الجنائي ، كما تعتبر جريمة مستمرة ، على عكس الجريمة الأولى، غير أن المشرع لم يفرق بين البقاء غير الشرعي أو مجرد المحاولة على غرار الجريمة الأولى.

ثالثا: جريمة حذف أو تغيير في معطيات المنظومة (م394مكرر/2) كنتيجة للدخول غير الشرعي أو البقاء واعتبارهما كجريمتين مضاعفتين

تنص المادة 394 مكرر في فقرتها الثانية على أنه " **تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة**" وعليه فان المشرع الجزائري فرق بين عملية حذف البيانات وعملية تغييرها ، اللذين يعتبرهما كنتيجة لفعل الدخول غير الشرعي أوالبقاء كما اعتبرهما جريمة مضاعفتين وذلك نتيجة لخطورة النتائج المترتبة عنهما.

رابعا: جريمة تخريب نظام الاشتغال كنتيجة للدخول غير الشرعي أو البقاء (م394مكرر/3)

نصت المادة 394 مكرر/3 على أنه " **وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج**" وعلى أساس ذلك لم يعتبر المشرع الجزائري جريمة تخريب نظام

الاشتغال جريمة مستقلة بذاتها على غرار الدخول غير الشرعي أو البقاء ، بل باعتبارها نتيجة للجرائم السابقة، وذلك يرجع إلى أنه من الممكن حدوث تخريب لهذا النظام ابتداء دون توفر القصد الجنائي إلا عندما يكون كنتيجة لجريمة سابقة .

خامسا: جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها عن طريق الغش(م 394 مكرر1)

نصت المادة 394 مكرر 1 على أنه "**يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل** " ومنه فان المشرع قد اعتبر أن إدخال معطيات مغشوشة في نظام المعالجة الآلية جريمة معلوماتية تستوجب عقوبة ، والتي ضاعفها إذا ما قورنت بالعقوبات السابقة ، وذا كان قد ربط فعل الحذف بالنتيجة المترتبة عن الدخول غير الشرعي أو البقاء ، فقد اعتبر جريمة الإزالة جريمة مستقلة في حد ذاتها تستوجب نفس العقوبة السابقة بالرغم من اتفاقية بودابست وكذا المشرع الفرنسي استعمل مصطلح "**الحذف**" لاستخدامه ضمن نفس المعنى .

وان ذهبنا إلى المعنى اللغوي فان معنى الحذف هو الإسقاط بينما يعني مصطلح الإزالة هو الإبعاد من المكان ، ومنه فان المشرع قد يكون فرق في الآثار بين الفعلين ، فحذف بيانات الكترونية معينة بكون بإسقاطها من موقعها في النظام المستهدف ، ولو كان بصفة مؤقتة ، مما يعني ظرفيتها وبذلك تكون قابلة للاسترجاع عن طريق برامج

خاصة "Logiciel de récupération de données électroniques" بالرغم من صعوبتها، ولكن إزالة البرامج تهدف إلى التخلص نهائيا منها وبشكل كامل ، لذلك يكون المشرع قد فرق بين الفعلين الإجراميين واعتبر الفعل الأخير أشد وطأة ، لذا فرق بين عقوبة كل فعل مجرم منهما.

سادسا: جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات عمدا وعن طريق الغش (م 394 مكرر1/2)

نصت المادة 394 مكرر 2 في فقرتها الأولى على انه "**يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا ، وعن طريق الغش :1- تصميم أو بحث أو تجميع أو توفير أو نشر أوالاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.**" وعليه فإننا نكون أمام توفر عدة شروط لقيام هذه الجريمة المعلوماتية ، وهي :

أ- **توفر القصد الجنائي لدى الجاني** : في هذه الحالة ابتداء لأقر المشرع كشرط أساسي لإقرار هذا الفعل المجرم توفر القصد الجنائي لارتكابه، لان علمية تصميم برنامج معين أوبحث في برنامج معين آخر أو نشره وحتى الاتجار فيه لا يعتبر جرما في حد ذاته ، إذا لم يسبقها توفر نية مسبقة لارتكاب جريمة معلوماتية تعتمد بالأساس على توفر علم مسبق لدى الجاني بان هذا البرنامج مغشوش .

ب–**أن يكون هذا الجرم مرتبطا بأفعال محددة وهي :** تصميم أو بحث أو تجميع أو توفير أو نشر أوالاتجار في المعطيات ، وعليه فان أي فعل آخر يمس هذه المعطيات لا يندرج ضمن هذا الإطار.

ج– **أن تكون المعطيات محل الجرم مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية:** وهنا يكون المشرع قد اعترف ضمنا بضرورة أن تكون المعطيات تتوفر على قدر كاف من الحماية ، لأن المساس بالمعطيات المتاحة والمتوفرة للجمهور لا يمكن أن تكون محل متابعة جزائية ، وبذلك يكون المشرع قد تأثر بالاتفاقيات والقانون المقارن الذي سعى إلى هذا الاتجاه لاسيما اتفاقية بودابست.

كما يمكن إن يكون هذه الجرائم سببا غير مباشرا في ارتكاب الجرائم المعلوماتية السابقة، وعليه فان المشرع قد قرر لها نفس العقوبة السابقة.

سابعا: جريمة حيازة أو إفشاء أو نشر أو استعمال معطيات المتحصل عليها من الجرائم المذكورة سابقا عمدا وعن طريق الغش (م 394 مكرر2/2)

فكما أقرّ المشرع جرمية الانفعال المذكورة سابقا ، فان حيازة معطيات أو إفشائها أونشرها أو استعمالها يعتبر جريمة يعاقب عليها القانون .

المطلب الثاني: الجرائم المعلوماتية الواقعة على الأشخاص و الأموال

سنتطرق الى الجرائم المعلوماتية الواقعة الأشخاص **(أولا)** والجرائم المعلوماتية الواقعة على الأموال **(ثانيا)**.

أولا : الجرائم المعلوماتية الواقعة الأشخاص

والمتمثلة في الجرائم التالية :

1-القذف و الإهانة والسب والاعتداء على حرمة الحياة الخاصة للأفراد عبر الانترنت:

تضمنت المواد 296و298،297 من قانون العقوبات المساس بشرف واعتبار الأشخاص والسب والقذف ، لكن لم يتناول إلى استعمال مختلف الوسائل المعلوماتية للقيام بهذه الجرائم .

كانت بداية تجريم هذه الأفعال من قبل المشرع بداية بموجب القانون رقم 01-09المؤرخ في 26 جوان2001 الذي أضاف المادة 144 مكرر التي نصت على العقوبة بالحبس من 3أشهر إلى 12 شهرا وبغرامة من 50.000 دج إلى 250.000دج أو بإحدى هاتين العقوبتين فقط كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أوالتصريح أو بأية آلية لبث الصوت أوالصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى. تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا.في حالة العود، تضاعف عقوبات الحبس والغرامة المنصوص عليها في هذه المادة، والتي عدلت بموجب القانون رقم 11-14المؤرخ في 2أوت2011، والتي تم من خلالها التخلي عن فكرة مضاعفة عقوبة الحبس والاكتفاء بمضاعفة الغرامة.

إذا فإذا كانت هذه العقوبات حصرها المشرع في الأفعال المرتبطة ببعض الشخصيات في الدولة ، فانه يمكن استعمالها قياسا في الجرائم المرتكبة على باقي الأشخاص هذا من

جهة ، كما أن نصوص المواد الثلاث المذكورة سابقا جاءت بصيغة العموم ،ولا لم تأت تفصيلا .

ما تجدر الإشارة إليه أن الجرائد الالكترونية وشبكات التواصل الاجتماعي تعد مجالا خضا لهذا النوع من الجرائم ، ومن الواضح أن قيام هذه الجرائم مكتملة الأركان لكونه يبقى ثابتا من خلال الكتابات التي تظهر أو التعليقات التي يمكن الاحتفاظ بها والتي تشكل مساسا أو قذفا لبعض الأشخاص ومنه توفر القصد الجنائي لدى المتهم، فاستعمالها من طرف الغير يعد من قبيل النشر الافتراضي.

2-الاستغلال الجنسي للأطفال عبر الانترنت: على عكس الجريمة السابقة المتعلقة بالسب والقذف غبر الانترنت فقد سارع المشرع بموجب القانون رقم 14-01 المؤرخ في 04 فيفري 2014 المتضمن تعديل قانون العقوبات على إضافة مادة خاصة تجرم كل استغلال جنسي للأطفال القصر بكل الوسائل ، والتي تندرج من ضمنها الوسائل المعلوماتية بكافة أنواعها ، وهي المادة 333مكرر والتي على نصت على العقوبة بالحبس من 5 سنوات إلى 10 سنوات وبغرامة من 500.000دج إلى 1.000.000دج، لكل من صور قاصرا لم يكمل 18سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أوقام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر.

كما أضافت نفس المادة وحماية لحقوق الأطفال الضحايا انه في حالة الإدانة تأمر الجهة القضائية بمصادرة الوسائل المستعملة لارتكاب الجريمة والأموال المتحصل عليها بصفة غير مشروعة مع مراعاة حقوق الغير حسن النية .

وكذلك من صور الاستغلال الجنسي للأطفال القصر هو التحريض على الفسق والدعارة وهو الأمر الذي تناوله القسم السابع من الفصل الثاني المتعلق بالجنايات والجنح ضد الأسرة والآداب العامة والمخصص لتحريض القصر على الفسق والدعارة، فقد نصت المادة 342 المعدلة على أنه من حرض قاصرا لم يكمل 18سنة على الفسق أو فساد الأخلاق أو تشجيعه عليه أو تسهيله له ولو بصفة عرضية، يعاقب بالحبس من 5سنوات إلى 10سنوات وبغرامة من 20.000دج إلى 100.000دج.ويعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات المقررة للجريمة التامة، حيث فتحت المادة 343 المجال واسعا في مجال الآليات المستعملة لذلك ، حين نصت على امتداد العقوبة لكل شخص ساعد أو عاون أو حمى دعارة الغير أو أغرى الغير على الدعارة بأية طريقة كانت.

3- انتهاك الآداب العامة عبر الانترنت: ما يقال عن جرائم السب والقذف عبر الانترنت يقال على هذا النوع من الجرائم لأنه لا يوجد نص واضح باستثناء جرائم استغلال الأطفال جنسيا التي أدرجها المشرع ضمن مجال انتهاك الآداب العامة ، وعليه فان كل الجرائم التي نتدرج ضمن هذا الباب وتم فيها استخدام وسائل معلوماتية فإنها تكون مدعاة لقيام جريمة معلوماتية.

ثانيا : الجرائم المعلوماتية الواقعة على الأموال

حيث سنتعرض إلى عديد الجرائم التي تناولها المشرع الجزائري ، والمتمثلة فيما يلي :

1-النصب الالكتروني : تعتبر الجرائم المعلوماتية التي تستهدف المال من أشهر الجرائم وأخطرها خاصة مع انتشار وسائل الانترنت والحواسيب ، فأصبح المجرم المعلوماتي يبحث عن كل الطرق للبحث عن المال المعلوماتي في محاولة منه للوصول إليه مستعملا طرقا غير مشروعة ، وعليه طرح التساؤل بداية عن المال المعلوماتي المعني بالحماية القانونية ؟

يعتبر المال المعلوماتي المعني بالحماية القانونية" **كل مال الكتروني قابل للنقل والتملك**" كما يمكن تعريفه "**بأنه المال الموجود في الحاسوب سواء في صورة معلومات أو بيانات الكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أودعامات تخزين خارجية ، فهو بذلك كل المدخلات الالكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية**".[62]

عرف الأستاذ الأمريكي سكويرز جريمة النصب الالكتروني على أنها" إساءة استخدام نظام الحاسوب بحيث ينطوي سلوك على حيلة أو خدعة مظللة ."[63] كما يمكن تعريفه على انه التحويل غير الشرعي للأموال المعلوماتية.

---

[62] ناير نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية ،دار الجامعة الجديدة ، مصر ، 2012، ص32.

[63] ربيعي حسين، مرجع سابق ، ص 70.

وبالرجوع إلى تعريف المشرع الجزائري لجريمة النصب من خلال ما تضمنته المادة 372 ق ع فنجده عرفها على صيغة العموم ، ولم يحدد جريمة النصب الالكتروني في حد ذاتها ، حيث عرف جريمة النصب على أنها " كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أوتصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أوصفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500إلى 20.000دينار. وإذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أذونات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات والغرامة إلى 200.00 دج."

وعليه فان كان المشرع لم يربط جريمة النصب بالجريمة المعلوماتية ، ولم يحدد وسيلة بعينها ، ولكن يمكن إسقاطها إذا ما تم توفر شروطها ، والمتمثلة في ما يلي :

أ-تحديد هوية مرتكب جريمة النصب الالكتروني: أن يكون مرتكب الجرم شخصا معينا ، لأنه لا يمكن للبعض تصور أن يقوم بهذه الجريمة جهاز الحاسوب بنفسه ، لكن الأنظمة الانجلوسكسونية وكذلك جانب من الفقه الفرنسي قبل بفكرة تطبيق العقوبة على الأنظمة المعلوماتية ، في حين طبقت بعض التشريعات الأخرى كالولايات

المتحدة الأمريكية القواعد الخاصة بالاحتيال في مجال البريد والتلغراف والبنوك على حالة النصب الالكتروني .

ب- أن نكون أمام تعامل قانوني للمال المعلوماتي : بحيث تشمل تصرفات ومعاملات حددها القانون وهي : استلام أو تلقى أموال أو منقولات أو سندات أوتصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها ، كما لم يفرق المشرع بين الحصول على هذه المعاملات وبين الشروع فيها.

ج- استعمال وسائل احتيالية : حدد المشرع صور الجرائم الاحتيالية وهي :

-استعمال أسماء أو صفات كاذبة

-استعمال سلطة خيالية

-استعمال اعتماد مالي خيالي

- إحداث الأمل في الفوز بأي شيء

-زرع الخوف في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها .

د- ان يكون الهدف منها سلب كل ثروة الغير أو بعضها : وهو ما يعبر عن الركن المعنوي أي القصد الجنائي لدى المجرم المعلوماتي ، كما أن المشرع اعتبر عملية الشروع معاقبا عليها هي كذلك.

هـ- تشديد العقوبة إذا تعلق الأمر بتعاملات تخص شركات أو مشروعات تجارية أوصناعية : نصت المادة 372 ق ع في اخر فقرة 1 على أنه إذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أذونات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أوصناعية فيجوز أن تصل مدة الحبس إلى 10 سنوات والغرامة إلى 200.000 دج.

و- أن تتم هذه التصرفات بواسطة استخدام أنظمة معلوماتية : وهو ما يعبر عن توفر الركن الافتراضي للجريمة المعلوماتية ، أي يتم استخدام هذا الجرم بواسطة نظام معلوماتي متوفر على نظام المعالجة الآلية للمعطيات.

ومن أبرز الأمثلة الخاصة بالنصب الالكتروني نجد:

- من أبرز القضايا التي حكمت عليها محكمة النقض الفرنسية حول شخص دخل ساحة انتظار السيارات، ولكنه عوض وضع النقود الأصلية في الآلة الالكترونية وضع قطعة

نقدية عديمة القيمة، فترتب عن ذلك تشغيل الآلة وتحرك العقارب ، حيث اعتبرتها جريمة نصب الكتروني، حتى وان كان المعني لم يحصل على أي شيء مادي[64].

– الاحتيال على الطريقة النيجيرية حيث اشتهرت هذه الطريقة على أساس استعمال رسائل الكترونية توهم الأشخاص أن المعني يحوز على أموال تصل ملايين الدولارات في بلده الأصلي وانه بحكم معاناته من مشاكل سياسية أنه يحتاج إلى فتح حساب باسم الضحية مع تقديم نسبة من 10 إلى 15 ٪ من مبلغ العملية، شريطة تقديم تسبيق مبلغ أولي، حيث تعرض الكثير من الضحايا إلى هذه الجريمة.[65]

2- السرقة الالكترونية : إذا كانت تعرف السرقة في مفهومها التقليدي فقها بأنها اختلاس لمال منقول بنية تملكه والذي تعود ملكيته للغير ،[66] فالسرقة الالكترونية أو المعلوماتية لا تختلف في مفهومها التقليدي من حيث توفر عنصري الاختلاس والتملك غير المشروع للمال المملوك للغير ، ولكن الاختلاف في الطريقة للحصول على هذا المال ،وهي استعمال وسائل معلوماتية ، حيث عرفها البعض على أنها " كل فعل يأخذ صور الاختلاس ويمس ببيانات المجني عليه".[67]

و بالرجوع إلى النص التشريعي الجزائري فالبرّغم من تعديله لقانون العقوبات لسنة 2004 وتطرقه لنظام المعالجة الآلية للمعطيات كما سبق وان تم التطرق إلى ذلك، إلا

---

[64] ربيعي حسين ، آليات البحث والتحري عن الجرائم المعلوماتية ، دكتوراه في الحقوق تخصص قانون العقوبات والعلوم الجنائية جنائي ،جامعة باتنة 1،الجزائر،2016 ، ص 100.

[65] نفس المرجع ، ص 74.

[66] بعقيقي عبير ، مرجع سابق ، ص 80.

[67] نفس المرجع، ص 81.

انه لم يتعرض إلى جريمة السرقة المعلوماتية أو الالكترونية بشكل صريح ، وعليه فإنها تخضع في أحكامها إلى أحكام وقواعد السرقات بالمفهوم التقليدي ، حالها في ذلك حال جريمة النصب الالكتروني ، وذلك بخضوعها إلى أحكام نص المادة 350 من ق ع التي تنص على انه " **كل من اختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة إلى 5 سنوات وبغرامة من 100.000دج إلى 500.000دج.**"

إن عدم تحديد المشرع للشيء المختلس يجعل من إمكانية إدراج المعلومات والبيانات الواردة في الحواسيب طرحا ممكنا، ومنه قبولها كركن مادي لجريمة السرقة المعلوماتية في غياب الركن الشرعي الصريح.

3-استغلال بطاقات الائتمان بطريقة غير شرعية :

أ- **مفهوم بطاقة الائتمان** : تعرف بطاقات الائتمان على أنها تلك البطاقات التي تستعمل للدفع والتي تصدرها المؤسسات المالية والتي تسمح لصاحبها بسحب أوتحويل الأموال ، كما عرفتها المادة 132 من قانون النقد الفرنسي .

حيث يستطيع صاحب هذه البطاقة تسديد التزاماته مباشرة حتى ولو لم يكن يملك حسابا او رصيدا لدى البنك مصدر البطاقة ، ولكن يلتزم بتسديد تلك الالتزامات في اجل معين ، من اشهر هذه البطاقات Visa وMaster card [68]، كما ساهمت هذه البطاقات في

[68] ربيعي حسين، مرجع سابق، ص 79.

تشجيع التسوق عبر شبكة الانترنت في مقابل زيادة حجم التخوف من الجرائم المرتبطة من استغلال هذه البطاقات بطريقة غير شرعية .

وعلينا أن نميز بين وبطاقات الائتمان وبطاقات الدفع الالكتروني الأخرى:

- **بطاقات الوفاء** : والتي تدعى بطاقة الخصم الشهري وتستخدم في الوفاء مقابل السلع او الخدمات من طرف المتعاملين التجاريين حيث يتم خصمها من قبل المؤسسة المالية التي أصدرت هذه البطاقة ، فتعتبر هذه البطاقات أكثرها شيوعا لعمليتها.[69]

- **بطاقات الصرف الآلي** : نجد هذا النموذج متوفرا في الجزائر وهي البطاقات التي تمنحها المؤسسات البنكية أو بريد الجزائر لزبائنها والتي يتم بموجبها سحب مبالغ مالية مع تحديد سقف أعلى لعملية السحب.

2- **صور الاعتداءات التي تطال بطاقات الائتمان** : تتمثل هذه الاعتداءات في صورتين :

- **الاعتداءات التي تطال البطاقة في حد ذاتها** : كسرقتها أو ضياعها واستعمالها على نخو غير مشروع.

- **الاعتداءات التي تطال البيانات الموجودة في البطاقة:** وذلك بتزوير البيانات الموجودة في البطاقة.

[69] ربيعي حسين، مرجع سابق، ص 79.

وبالرجوع إلى قانون العقوبات الجزائري فانه لم يتضمن تعريفا لهذه الجريمة وترك أمرها لبعض القوانين الخاصة كقانون التأمينات الاجتماعية لسنة 1983 المعدل والمتمم ، وكذا قانون التأمينات والبريد ..الخ .

المطلب الثالث الجرائم المعلوماتية الواقعة على الهيئات العامة

خص المشرع الجزائري من خلال تعديله لقانون العقوبات لسنة 2004 بعض الهيئات العامة والمؤسسات الخاضعة للقانون العام بحماية جنائية لمعطيتها المعلوماتية، لذلك سنحاول التطرق إلى الأركان الجريمة المعلوماتية المرتبطة بهذه الهيئات .

1- الركن الشرعي : نص المادة 394 مكرر 3 على "انه تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".

ومنه فان الجرائم السابقة المتعلقة بنظام المعالجة الآلية للمعطيات جهات الدفاع الوطني أو المؤسسات الخاضعة للقانون العام فان عقوبتها تكون مضاعفة ، وذلك لما تحتويه أنظمة هذه المؤسسات من أهمية ذات بعد امني واستراتيجي ، له انعكاسات على امن الدولة ككل ، لذا أخضعه المشرع إلى قواعد حماية خاصة .

2-الركن المادي : لقد حددت المادة 394 مكرر 3 الركن المادي لجريمة المعلوماتية التي تطال هذه المؤسسات والهيئات ، وذلك بالإحالة إلى المواد التي سبقتها ، والتي تكون بتوفر إحدى صور الجرائم التي تم التطرق إليها بالتفصيل سابقا، وهي :

- الدخول في كل أو جزء من منظومة للمعالجة الآلية لمعطيات أو محاولة ذلك
- البقاء
- حذف أو تغيير في معطيات المنظومة كنتيجة للدخول غير الشرعي أو البقاء
- تخريب نظام الاشتغال كنتيجة للدخول غير الشرعي أو البقاء
- إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها عن طريق الغش
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات عمدا وعن طريق الغش
- جريمة حيازة أو إفشاء أو نشر أو استعمال معطيات المتحصل عليها من الجرائم المذكورة سابقا عمدا وعن طريق الغش .

1-**الركن المعنوي** : وهو توفر القصد الجنائي العام والخاص معا بغرض المساس بأنظمة المعالجة الالكترونية لهذه الهيئات والمؤسسات الخاضعة للقانون العام .

2- **الركن الافتراضي** : وفي الأصل كذلك موجود كون هذه الجرائم تمس أنظمة المعالجة الآلية للمعطيات .

المبحث الثاني : الجريمة المعلوماتية خارج مجال قانون العقوبات الجزائري

بعد استعراضنا من خلال الفصل السابق للجريمة المعلوماتية في إطار قانون العقوبات الجزائري ، سنتناول من خلال هذا الفصل الجريمة المعلوماتية خارج مجال قانون العقوبات، حيث سنتناول هذا الموضوع في إطار حماية حقوق الملكية الفكرية والمعطيات

الشخصية **(المطلب الأول)** والانتقال إلى الجريمة المعلوماتية المتعلقة بتكنولوجيات الإعلام والاتصال**(المطلب الثاني)**.

المطلب الأول : الجريمة المعلوماتية في إطار حماية حقوق الملكية الفكرية و المعطيات الشخصية

سنتطرق الجريمة المعلوماتية في إطار حماية حقوق الملكية الفكرية من خلال **الفرع الأول** وفي إطار حماية المعطيات الشخصية من خلال **الفرع الثاني** من نفس المطلب .

الفرع الأول : الجريمة المعلوماتية في إطار حماية حقوق الملكية الفكرية

1- النص القانوني باعتبار المعلوماتية ضمن حقوق المؤلف في التشريع المقارن والجزائر : وقع الجدل الفقهي في البداية حول اعتبار المعلوماتية حقا للمؤلف وكانت بداية الاعتراف بذلك من خلال موافقة حقوق المؤلف الأمريكية copyright office لسنة 1964 على إيداع البرامج لديه كمصّنفات ، وكذلك الحال في فرنسا بموجب القانون 86-66 المؤرخ في 1986/07/03 حيث أضيفت برامج الكمبيوتر ضمن حقوق المؤلف .[70] وفي الجزائر لم ينص الأمر 73-14 المؤرخ في 1973/04/03 المتعلق بحق المؤلف[71] ولا الأمر 97-10 المؤرخ في 1997/03/06 المتعلق بحقوق المؤلف والحقوق المجاورة[72] صراحة على اعتبار حقوق المؤلف معلوماتية .

---

[70] بدري فيصل ، مرجع سابق ، ص 133.

[71] الجريدة الرسمية عدد 29 المؤرخة في 1974/04/10 ، ص 434.(ملغى)

[72] الجريدة الرسمية عدد 13 المؤرخة في 1997/03/12 ، ص 03. (ملغى)

لكن الأمر 03-05 المؤرخ في 2003/07/09 المتعلق بحقوق المؤلف والحقوق المجاورة[73] اعتبر صراحة من خلال نص المادة 4 منه على أن برامج الحاسوب تعتبر كمصنفات محمية .

2- الجرائم المعلوماتية في نطاق حق المؤلف والعقوبات المقررة عليها : تضمنت المواد من 151 إلى 160 من الأمر 03-05 العقوبات المقررة في مجال حق المؤلف والمتمثلة في :

أ- جنحة التقليد : يعد مرتكبا لهذه الجنحة من يقوم بالأعمال التالية :

- الكشف غير المشروع للمصنف أو المساس بسلامته أو الأداء لفنان مؤد أوعازف.
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة .
- استيراد أو تصدير نسخ مقلدة لمصنف أو أداء .
- بيع لنسخ مقلدة لمصنف أو أداء.
- تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء.
- كل من ينتهك الحقوق المحنية قانونا فيبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني أو البث الإذاعي السمعي أو السمعي البصري أو التوزيع بواسطة الكبل أو بأي وسيلة نقل أخرى لإشارات تحمل أصواتا فقط أو صورا وأصواتا أوبأي منظومة معالجة معلوماتية .[74]

---

[73] الجريدة الرسمية عدد 44 المؤرخة في 2003/08/23 ، ص 03.

[74] كما تنص المادة 152 من الأمر 03-05 .

- كل من يشارك بعمله او بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة .[75]
- كل من يرفض عمدا دفع المكافأة المستحقة للمؤلف أو أي مالك حقوق مجاورة آخر للحقوق المعترف بها قانونا.[76]

ب- العقوبة المقررة لجريمة التقليد : نصت المادة 153 من الأمر 03-05 على العقوبة المقررة لجريمة التقليد للمصنف أو الأداء بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج ، مع مضاعفة هذه العقوبة في حالة العود [77].

الفرع الثاني : الجريمة المعلوماتية في إطار حماية المعطيات الشخصية

تناول المشرع بشكل مفصل حماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية وذلك بموجب القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[78].

والملاحظ هو التأخر في إصدار هذا القانون بالرغم من أهميته ، حيث يسجل فارق ما يفوق 14 سنة عن صدور أول نص تشريعي يتناول الحماية الجنائية لنظام المعالجة الآلية للمعطيات في إطار قانون العقوبات لسنة 2004.

---

[75] طبقا لما تنص عليه المادة 154 من الأمر 03-05.

[76] كما نصت المادة 155 من الأمر 03-05.

[77] طبقا لما نصت عليه المادة 156 من الأمر 03-05.

[78] القانون 18-07 المؤرخ في 2018/06/10 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34 المؤرخة في 2018/06/10، ص 11.

أولا : ضبط دقيق للمصطلحات

ما يلاحظ على هذا النص الشريعي هو العناية الفائقة بمسألة التعريف ، وعدم ترك أي مجال للتأويل أو التفسير ، ومنه أي غلق مجال الاجتهاد في هذا الباب، وهذا ما يتبين لنا من خلال الخوض في التعاريف التي تطرق إليها هذا النص القانوني .

1 – المعطيات ذات الطابع الشخصي: عرفت المادة من القانون 18-07 بأنها كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه .

وتكون لتلك المعطيات علاقة بصفة مباشرة أو غير مباشرة بـ "الشخص المعني" ، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أوالفيزيولوجية أوالجينية أوالبيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

لقد وسّع في مجال شمول عناصر هوية الأشخاص، من البدنية إلى الفيزيولوجية ..الخ، وهذا ما يبين نية المشرع في عدم تضييق نطاق التعريف لهذه المعطيات .

2- الأشخاص الذين لهم علاقة بالمعطيات : حدد القانون 18-07 الأشخاص والفئات الذين لهم علاقة بالمعطيات الشخصية وهم :

أ- الشخص المعني : عرفت الفقرة 2 من المادة 3 الشخص المعني بأنه كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة.

ب- المسؤول عن المعالجة: شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها.

ج- معالج من الباطن : هو كل شخص طبيعي أو معنوي، عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة.

د- الغير: كل شخص طبيعي أو معنوي، عمومي أو خاص أو أي كيان آخر غير الشخص المعني والمسؤول عن المعالجة والمعالج من الباطن والأشخاص المؤهلون لمعالجة المعطيات الخاضعون للسلطة المباشرة للمسؤول عن المعالجة أو المعالج من الباطن.

هـ- المرسل إليه: الشخص الطبيعي أو المعنوي أو السلطة العمومية أو المصلحة أوأي كيان آخر يتلقى معطيات ذات طابع شخصي.

و- مقدم الخدمات : ويكون في صورتين:

- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

- أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو للمستعملين.

ي- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: هي سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي تابعة لرئيس الجمهورية و مقرها الجزائر العاصمة، تتمتع بالشخصية المعنوية والاستقلال المالي والإداري .

تتشكل اللجنة من عضوية 03 شخصيات يعينهم رئيس الجمهورية يكونون ذوي اختصاص في عمل السلطة ، و 03 قضاة يقترحهم المجلس الأعلى للقضاء وعضو عن كل غرفة برلمانية ، وممثلا واحدا عن كل من : المجلس الوطني لحقوق الإنسان ووزارة الدفاع الوطني، و وزارة الشؤون الخارجية، ووزارة الداخلية و وزارة العدل ووزارة البريد والمواصلات السلكية واللاسلكية و وزارة الصحة، ووزارة العمل والتشغيل والضمان الاجتماع،[79]حيث يؤدي أعضاء السلطة اليمين القانونية قبل تنصيبهم أمام مجلس قضاء الجزائر.

تزوّد السلطة بأمانة تنفيذية تساعدها على تأدية وظائفها يسيّرها أمين تنفيذي بمساعدة مستخدمين ، حيث يقوم أعضاء هذه الهيئة كذلك بتأدية اليمين القانونية أمام مجلس قضاء الجزائر .

يلتزم أعضاء السلطة بالمحافظة على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها ، ولو بعد انتهاء مهامهم .

كما تضطلع السلطة بعدة مهام أهمها :

[79] كما تنص المادة 23 من القانون 18-07.

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
- إضافة إلى تقديم الاستشارات في هذا المجال تتلقى السلطة الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للقواعد والإجراءات التي سنتطرق إليها لاحقا.
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.
- الأمر بإغلاق معطيات أو سحبها أو إتلافها.

3- معالجة المعطيات : كما عرّف المشرع من خلال الفقرة 3 من نفس المادة من القانون 18-07 مصطلح المعالجة واعتبره كل عملية أو مجموعة عمليات منجزة بطرق أوبوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أوالتنظيم أوالحفظ أو الملاءمة أو التغيير أوالاستخراج أو الاطلاع أو الاستعمال أوالإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أوالمسح أو الإتلاف.

وقرن المشرع تعريف المعالجة بـ "موافقة الشخص المعني" الذي عرّفه على انه " كل تعبير عن الإرادة المميزة يقبل بموجبه الشخص المعني أو ممثله الشرعي معالجة المعطيات الشخصية المتعلقة به بطريقة يدوية أو إلكترونية".

وإذا كان المشرع لم يتناول تعريف المعالجة الآلية للمعطيات في إطار قانون العقوبات، فقد تناولها في إطار هذا القانون وعرفها على أنها العمليات المنجزة كليا أوجزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها.

ومنه بالرغم من تناول المشرع لتعريف المعالجة الآلية للنظام إلا أنه لم يستخدم مصطلح "نظام" الذي قرنه بالمعالجة الآلية للمعطيات في قانون العقوبات، مما يثير عديد التساؤلات .

ثانيا: تصنيف المعطيات

فرّق القانون 18-07 بين أنواع المعطيات، من حيث طبيعتها أو مضمونها وهي :

أ- **معطيات حساسة** : معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أوالآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أوتكون متعلقة بصحته بما فيها معطياته الجينية.

ب- مضمون غير شرعي : كل مضمون مخالف للقوانين السارية لاسيما مضمون ذو طابع تخريبي أو من شأنه المساس بالنظام العام والمضمون ذو الطابع الإباحي أو المنافي للآداب العامة.

ج- معطيات جينية : كل معطيات متعلقة بالصفات الوراثية لشخص أو عدة أشخاص ذوي قرابة.

د- معطيات في مجال الصحة : كل معلومة تتعلق بالحالة البدنية أو العقلية للشخص المعني، بما في ذلك معطياته الجينية.

هـ- ملف : كل مجموعة معطيات مهيكلة ومجمعة يمكن الولوج إليها وفق معايير محددة.

و- الاتصال الإلكتروني : كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها، عبر الأسلاك أوالألياف البصرية أو بطريقة كهرومغناطيسية.

ثالثا : حقوق الشخص المعني والتزامات المسؤول عن المعالجة

يتمتع الشخص المعني بالمعطيات الشخصية بمجموعة من الحقوق ، كما يقع المسؤول عن المعالجة مجموعة من الالتزامات .

1-**حقوق الشخص المعني** : هذه الحقوق هي :

أ- **الحق في الإعلام** : حددت المادة 32 من القانون 18-07 شروط نيل هذا الحق لدى الشخص المعني لم يكن على علم مسبق بها، فيجب على المسؤول عن المعالجة أومن يمثله إعلام مسبقا وبصفة صريحة ودون لبس كل شخص يتم الاتصال به قصد تجميع معطياته ذات الطابع الشخصي.

وتشمل العناصر المرتبطة بالحق في الإعلام فيما يلي :

- هوية المسؤول عن المعالجة أو هوية ممثله.

- أغراض المعالجة.

- كل معلومة إضافية مفيدة، لاسيما المرسل إليه ومدى إلزامية الرد والآثار المترتبة عن ذلك وحقوقه ونقل المعطيات إلى بلد أجنبي.

ب- **الحق في الولوج** : منح القانون 18-07 للشخص المعني هذا الحق وذلك من خلال التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، وأغراض المعالجة وفئات المعطيات التي تنصّب عليها والمرسل إليهم، وإفادته وفق شكل مفهوم بالمعطيات الخاصة به التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات.

ج- **الحق في التصحيح** : كما منح القانون للشخص المعني هذا الحق بصفة مجانية من قبل المسؤول عن المعالجة سواء تعلق الأمر:

– تحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة للقانون.

– وكذلك لو تعلق الأمر تبليغ الغير الذي أوصلت إليه المعطيات الشخصية بكل تحيين أو تصحيح أو مسح أو إغلاق للمعطيات ذات الطابع الشخصي.

د– الحق في الاعتراض : منح القانون للشخص المعني حق الاعتراض وذلك عند توفر أسباب مشروعة على معالجة معطياته ذات الطابع الشخصي، كاستعمال معطياته ضمن أغراض دعائية او تجارية ..الخ.

هـ– الحق في منع الاستكشاف المباشر : حيث يمنع القانون 18–07 الاستكشاف المباشر بواسطة آلية اتصال أو جهاز الاستنساخ البعدي أو بريد إلكتروني أو أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة، باستعمال بيانات شخص طبيعي، في أي شكل من الأشكال، لم يعبر عن موافقته المسبقة على ذلك.

وفي المقابل منح القانون استثناء عن هذه الوضعية فيتم الترخيص بالاستكشاف المباشر عن طريق البريد الإلكتروني، إذا ما طلبت البيانات مباشرة من المرسل إليه، بمناسبة بيع أو تقديم خدمات، إذا كان الاستكشاف المباشر يخص منتجات أو خدمات مشابهة يقدمها نفس الشخص الطبيعي .

2–التزامات المسؤول عن المعالجة : يلتزم المسؤول عن المعالجة بالالتزام بعدة قواعد وإجراءات ضرورية ضمانا لسلامة المعطيات وهي :

أ- **سرّية وسلامة المعالجة** : وذلك بأن يقوم المسؤول عن المعالجة باتخاذ التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أوغير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين، خصوصا عندما تستوجب المعالجة إرسال معطيات عبر شبكة معينة وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة[80].

ب- معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التصديق والتوقيع الإلكترونيين: باستثناء حالة الموافقة الصريحة، يجب الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني، من الأشخـاص المعنيين بها مباشرة، ولا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها وفقا لنصت عليه المادة 42 من القانون 18-07.

ج-معالجة المعطيات ذات الطابع الشخصي في مجال الاتصالات الإلكترونية : ففي حالة إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الاتصالات الالكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، يعلم مقدم الخدمات فورا السلطة الوطنية والشخص المعني، إذا أدى ذلك إلى المساس بحياته الخاصة.

[80] كما تنص المادة 38 من القانون 18-07.

د- نقل المعطيات نحو دولة أجنبية : حيث منع القانون 18-07 القيام بهذا الإجراء إلا بموجب ترخيص من طرف السلطة الوطنية ، شريطة أن تكون هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها[81].

رابعا : الجوانب الإجرائية لحماية المعطيات الشخصية

وهي المصنفة ضمن الإجراءات المسبقة للمعالجة وتشمل نظامين هما : التصريح والترخيص .

1- التصريح : يودع التصريح المسبق الذي يتضمن الالتزام بإجراء المعالجة لدى السلطة الوطنية ويمكن تقديمه بالطريق الإلكتروني، في مقابل تسليم وصل الإيداع أو بإرساله بالطريق الالكتروني فورا أو في أجل أقصاه 48 ساعة.

كما يمكن أن تكون المعالجات التابعة لنفس المسؤول عن المعالجة والتي تتم لنفس الغرض أو لأغراض مرتبطة محل تصريح واحد . كما يمكن له تحت مسؤوليته أن يباشر في عملية المعالجة بمجرد استلامه الوصل .

ولقد وضعت المادة 14 من القانون مجموعة من الشروط الشكلية يجب أن يتضمنها التصريح وهي :

- اسم وعنوان المسؤول عن المعالجة وعند الاقتضاء اسم وعنوان ممثله.

[81] طبقا لما نصت عليه المادة 44 من القانون 18-07.

– طبيعة المعالجة وخصائصها والغرض أو الأغراض المقصودة منها.

–وصف فئة أو فئات الأشخاص المعنيين والمعطيات أو فئات المعطيات ذات الطابع الشخصي المتعلقة بهم.

–المرسل إليهم أو فئات المرسل إليهم الذين قد توصل إليهم المعطيات.

– طبيعة المعطيات المعتزم إرسالها إلى دول أجنبية.

– مدة حفظ المعطيات.

-المصالحة التي يمكن الشخص المعني أن يمارس لديها الحقوق المخولة له .

– وصف عام يمّكن من تقييم أولي لمدى ملاءمة التدابير المتخذة من أجل ضمان سرية وامن المعالجة .

– الربط البيني أو جميع أشكال التقريب الأخرى بين المعطيات، وكذا التنازل عنها للغير أو معالجتها من الباطن، تحت أي شكل من الأشكال، سواء مجانا أو بمقابل.

2- الترخيص : تقرر السلطة الوطنية إخضاع المعالجة المعنية لنظام الترخيص المسبق عندما يتبين لها عند دراسة التصريح المقدم لها أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

كما اشترطت المادة 17 من نفس القانون أن يكون قرار السلطة مسببا وأن يبّلغ إلى المسؤول عن المعالجة في أجل 10 أيام التي تلي تاريخ إيداع التصريح.

خامسا : العقوبات المتعلقة بالمساس بالمعطيات الشخصية

إضافة إلى العقوبات الإدارية تجاه المسؤول عن المعالجة في حالة خرقه لأحكام القانون والمتمثلة في :

- الإنذار
- الاعذار
- السحب المؤقت لمدة لا تتجاوز سنة أو السحب النهائي لوصل التصريح أوللترخيص
- الغرامة

حيث تتخذ هذه العقوبات بموجب قرارات قابلة للطعن أمام مجلس الدولة [82].

تضمن القانون 18-07 كذلك عقوبات جزائية وذلك من خلال المادة 54 منه والمتمثلة في العقوبات المتعلقة بالأطر الخاصة باحترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وعدم المساس بحقوق الأشخاص وشرفهم وسمعتهم وهي بالحبس من سنتين إلى 5 سنوات وبغرامة مالية من 200.000 دج إلى500.000 دج .

وحدد القانون 18-07 لكل جريمة ما يقابلها من عقوبة و التي أبرزها:

[82] كما تنص المادة 46 من القانون 18-07.

- الحبس من سنة إلى 3سنوات وبغرامة من 100.000 دج إلى 300.000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7من هذا القانون وهي كل ما تعلق بالموافقة المسبقة .
- الحبس من سنة إلى 3سنوات وبغرامة من 100.000 دج إلى 300.000 دج في حالة معالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة، لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب شرعية .
- العقوبة بالحبس من سنتين إلى 5 سنوات وبغرامة من 200.000 دج إلى 500.000 دج لكل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12من هذا القانون، ويعاقب بنفس العقوبة كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له .

المطلب الثاني: الجريمة المعلوماتية المتعلقة بتكنولوجيات الإعلام والاتصال

بعد التعديل الذي طال قانون العقوبات لسنة 2004 والنص على الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، أصبحت الضرورة ملحة لإصدار قانون يتوافق وهذا التعديل في مجال تكنولوجيات الإعلام والاتصال .

أولا: التعريف القانوني لهذه الجرائم

بصدور القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[83] الذي حاول المشرع من خلاله تعريف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حيث اعتبرها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، لكن أضاف إليها الجرائم الأخرى التي ترتكب أويسهل ارتكابها عن طريق منظومة أو نظام للاتصالات الالكترونية .

ومنه فإن هذا القانون يكون قد شمل مواضيع ومجالات أخرى أوسع نطاقا من التي أوردها قانون العقوبات .

ثانيا : عناصر الجريمة المعلوماتية في إطار القانون 09-04

هذه العناصر المتمثلة فيما يلي:

أ- **منظومة معلوماتية** : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر لمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

ب- **معطيات معلوماتية:** 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.

[83] الجريدة الرسمية عدد 47 المؤرخة في 2009/08/16 ، ص05.

ج- **مقدمو الخدمات** : ويتخذ صورتين:

- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.
- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

د- **المعطيات المتعلقة بحركة السير**: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات توضح مصدر الاتصال والوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

هـ- **الاتصالات الإلكترونية:** أي تراسل أو إرسال أو استقبال علامات أوإشارات أوكتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[84].

ثالثا: مكافحة الجريمة المعلوماتية في ظل القانون 09-04

نص المشرع على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته تتولى تنشيط وتنسيق عملية الوقاية من هذه الجرائم .

[84] المادة 02 من القانون 09-04.

كما تتولى دور مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات في الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال ، وكذلك تبادل المعلومات مع نظيراتها في الخارج من اجل جمع المعلومات وانجاز الخبرات القضائية .

خاتمة

مع تطور وسائل الاتصال والمعلوماتية في العصر الحديث، وارتباطها بأجهزة الكمبيوتر والأنترنت، وبمقدار الإفراط في استعمال هذه الوسائل ظهر نوع جديد من الجرائم المقترنة بهذه الثورة التكنولوجية لم يكن معروفا في السابق، جعل من الفقه يبحث عن إعطاء مفهوم محدد لهذه الجرائم والتي اصطلح على تسميتها بـ"الجريمة المعلوماتية".

والجزائر على غرار دول عديدة سعت بكل جهودها من أجل مكافحة هذه الجرائم المستحدثة مع أنها فرضت نوعا من الخصوصية، بحيث أصبحت لصيقة بهذه الجرائم نظرا لشمولها مجالات عديدة ونظرا كذلك لخطورة آثارها.

وإن كان لم يتفق الفقه حول إعطاء مفهوم محدد للجرائم المعلوماتية فإن غالبية الدول والتي من بينها الجزائر سعت إلى إرساء أرضية حقيقية من أجل مكافحة هذه الجرائم بالرغم من كل الصعوبات المقترنة بها.

تمتاز الجريمة المعلوماتية بعدة خصائص تميّزها عن باقي الجرائم التي تصنف في خانة الجرائم الكلاسيكية بين ما هي خصائص عامة ومنها ما ارتبط بها بصفة خاصة الأمر الذي جعلها تحتل موقعا هاما في المنظومات الجنائية الدولية والوطنية، وهو الذي نتج عنه القيام بإنشاء معاهدات واتفاقيات دولية وإقليمية لمحاربة هذه الظاهرة الجديدة على العالم بالاعتماد على تظافر الجهود الدولية والتعاون الدولي .

كما انعكس نفس الأمر على السياسة التشريعية في الجزائر من خلال تعديل قانون العقوبات لسنة 2004 وكذلك خارج هذا القانون من خلال حماية حقوق الملكية الفكرية وكذا حماية المعطيات الشخصية والجريمة المعلوماتية المتعلقة بتكنولوجيات الإعلام والاتصال.

وعليه ومن أجل حماية فعلية لمجابهة الجرائم المعلوماتية في الجزائر لابد من العمل على تجسيد حقيقي للحماية الجنائية للمعطيات عبر تطوير أنظمة الحماية التقنية في إطار المعالجة الآلية للمعطيات، كما يجب العناية بالعنصر البشري المتخصص في مكافحة هذه الجرائم سواء من ناحية التكوين أو من ناحية المتابعة ومواكبة مختلف الأنظمة الجنائية المقارنة، وكذلك تطوير عملية تبادل الخبرات والكفاءات بين مختلف الدول لاسيما المجاورة .

كما حان الأوان للعمل على توحيد النصوص القانونية وضمّ القواعد الواردة في قانون العقوبات مع كل القوانين الأخرى المتعلقة بمكافحة الجرائم المعلوماتية في نص واحد تحت مسمى قانون مكافحة الجرائم المعلوماتية،على غرار القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي والقانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

قائمة المراجع

1- الكتب :

- احمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي–دراسة مقارنة –، ط1، دار النهضة العربية للنشر والتوزيع، مصر ،2000.

- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى ، الجزائر، 2011.

- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية،دار الجامعة الجديدة ، مصر، 2015 .

- محمد علي العريان، الجرائمالمعلوماتية ، دار الجامعة الجديدة ،جامعةالإسكندرية ، ،مصر ،2011.

- ناير نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة ، مصر، 2012 .

2- المجلات والدوريات :

- لورنس سعيد الحوامدة ، الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية مقارنة ، مجلة الميزان ، المجلد 4 ، العدد1، جامعة العلوم الإسلامية العالمية ، الأردن ، 2017.

3- الرسائل والمذكرات :

- بدري فيصل ، مكافحة الجريمة في القانون الدولي والداخلي ، أطروحة دكتوراه في القانون العام ،كلية الحقوق ، جامعة الجزائر ، 2018.

- بعقيقي عبير، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي – دراسة مقارنة –، أطروحة دكتوراه في الحقوق، تخصص النظام الجزائي والسياسة الجزائية المعاصرة ، كلية الحقوق بجامعة محمد خيضر، بسكرة ، الجزائر ، 2018.

- ربيعي حسين، آليات البحث والتحري عن الجرائم المعلوماتية ، دكتوراه في الحقوق تخصص قانون العقوبات والعلوم الجنائية جنائي ،جامعة باتنة 1،الجزائر،2016 .

- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر، باتنة ، الجزائر، 2013.

- طرشي نورة، مكافحة الجريمة المعلوماتية ، ماجستير في القانون الجنائي ، كلية الحقوق، جامعة الجزائر ، 2012

- قارة آمال ، الجريمة المعلوماتية ، ماجستير تخصص القانون الجنائي والعلوم الجنائية ، كلية الحقوق بجامعة الجزائر ،2005 .

4- النصوص القانونية :

- الأمر رقم 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات، الجريدة الرسمية 49 المؤرخة في 1966/06/11، وتعديلاته لاسيما القانون رقم 04-15، الجريدة الرسمية عدد 71 المؤرخة في 2004/11/10 .

- الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 44 المؤرخة في 2003/08/23.

- القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 المؤرخة في 2009/08/16.

- القانون رقم 18-07 المؤرخ في 2018/06/10 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34 المؤرخة في 2018/06/10.

5- المواقع الالكترونية الرسمية :

- الموقع الرسمي للمنظمة العالمية للملكية الفكرية WIPO:
https://www.wipo.int/treaties/ar/ip/berne/summary_berne.html

- الموقع الرسمي لمجلس أوروبا : https://www.coe.int/fr/web/about-us/achievements

الفهرس