جامعة عمار الثليجي الاغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق

حماية الخصوصية في ظل تنامي الاجرام المعلوماتي

مذكرة تخرج ضمن مقتضيات نيل شهادة الماستر
تخصص: قانون جنائي وعلوم جنائية

إعداد الطلبة:
دودو عبد العزيز
جنح حمزة

إشراف:
أ د النحوي سليمان

أعضاء لجنة المناقشة:

أ د. عمران عائشة	**رئيسا**
أ د. النحوي سليمان	**مشرفا ومقررا**
د. بلحسن حسام الدين	**مساعد المشرف**
د. تركي محمد السعيد	**ممتحننا**

السنة الجامعية: 2024/2023

شكر وتقدير

الحمد لله حمدا يوافي نعمه ويكافئ مزيده، الحمد لله على الذي بنعمته تتم الصالحات

أشكر أساتذتي الدكتور النحوي سليمان الذي تفضل بالإشراف على هذه المذكرة ولم يبخل علينا، بتوجيهاته ونصائحه، فله منا كل التقدير والاحترام.

كما أتقدم بجزيل الشكر والامتنان إلى السادة أعضاء لجنة المناقشة الكرام كل واحد منهم باسمه ومركزه، الذين شرفونا بقبول عضوية لجنة المناقشة متحملين عناء الاطلاع على هذا البحث وتقييمه وإثرائه وإتمام أوجه القصور فيه ومصوبين لنا أخطائنا.

الشكر موصول إلى كل الأساتذة وكل الأسرة الجامعية لكلية الحقوق والعلوم السياسية مع حفظ الألقاب والمناصب.

جعل الله جهودكم في ميزان حسناتكم، ورحم الله من قضى نحبه واسكنهم فسيح جناته

إهداء

إلى كم كان سندا وعونا عند الشدائد طوال عمري، إلى الرجل الأبرز في حياتي

أبي العزيز

إلى القلب المعطاء والصدر الحاني

أمي الغالية

إلى كل من ساعدني ولو بكلمة طيبة ودعاء طيلة حياتي الدراسية

إلى هؤلاء جميعا: اهديكم هذا العمل

مقدمة

مقدمة

يشهد العالم اليوم طفرة نوعية في مجال المعاملات السيبرانية، أحدثت تحولا جذريا في كافة ميادين الحياة، سيما التعاملات الاقتصادية والتجارية والإدارية والثقافية، وسهل الانفتاح على عالم بلا حدود، مما مكن من التواصل بين الأشخاص والمؤسسات، فأصبح العالم كقرية صغيرة يسهل فيها التعامل والتواصل باستمرار، فأصبحت المنظمات تستخدم شبكة الأنترنت في إنجاز معاملاتها وأعمالها، لتسهيل الحصول على البيانات والمعلومات لاتخاذ القرارات المناسبة وتقديم خدماتها للمستفيدين بكفاءة وفعالية وبأقل تكلفة وبأسرع وقت ممكن.

وأمام هذه النقلة في تبادل المعلومات وحفظها ونقلها والاسترجاع، بفضل قدرة الحاسوب على القيام بتلك العمليات، بسرعة ودقة وتكلفة منخفضة مقارنة بالطرق اليدوية، فضلا عن إمكانية تبادل المعلومات وربطها بغيرها، بواسطة شبكات الاتصال المحلية و الدولية، حيث أفرزت هذه الثورة في المعلومات و الاتصالات نوعا جديدا من الجرائم، ووصفة مثالية لتنفيذ العديد منها، وساحة إجرام نموذجية على رأسها الجريمة المعلوماتية التي ترتبط بالتقنيات الإلكترونية الحديثة، وتستهدف الاعتداء على البيانات والمعلومات والبرامج بكافة أنواعها، بل تعدى ذلك إلى الاعتداء على حق الخصوصية المعلوماتية من خلال جرائم اختراق الحسابات الخاصة وسرقة بياناتها والتشهير بها وما يترتب عن ذلك من انتهاك لحرمة الإنسان وحرمة أسرته.

يعتقد البعض أن صور الاعتداء على الحياة الخاصة تقتصر على إفشاء المعلومات و التنصت عليها والاعتداء على حرمة الاتصالات و المراسلات وسريتها، بل تعد هذه الصورة التي ركزت عليها أغلب التشريعات في قوانين العقوبات، حيث أن الاعتداء على الحق في الحياة الخاصة من خلال الأنظمة المعلوماتية يأخذ أبعادا وأشكالا أخرى مستحدثة، أبرزها مواجهة المخاطر المتعلقة بجمع المعطيات ذات الطابع الشخصي، ومعالجتها الاستغلالية من قبل القطاعين العام و الخاص، حيث يتم جمع عدد كبير من هذه المعطيات الشخصية – بنوك المعلومات – وتخزينها من قبل الدولة أو الجهات الأمنية والمصارف أو شركات التأمين أو الجامعات وغير ذلك من الهيئات الحكومية والخاصة، في حين يجهل الشخص ما يخزن عنه من معطيات شخصية، والفترة التي تخزن فيها والهدف من هذا التخزين وهنا تظهر جسامة وخطورة هذه البيانات و المعطيات خاصة ما تعلق منها بالمعتقد الديني والانتماء العرقي والسياسي والحالة الصحية، وغير ذلك من المعطيات التي يوثر الإفصاح عنها، حيث يفقد الشخص

السيطرة على معطياته الشخصية، ويظهر خطر ذلك جليا في استغال بنوك المعلومات لهذه البيانات الشخصية من خلال بيع هذه المعلومات لشركات أو مؤسسات أخرى للتربح المادي.

انتشرت هذه الجرائم بشكل واسع فتخطت حدود الدول، فأصبحت ظاهرة عالمية تهدد كيان المجتمعات نظرا لخطورتها، على الصعيد القانوني والاجتماعي والاقتصادي والأمني، مما يستدعي بالضرورة إصدار قوانين خاصة بالجريمة الالكترونية تتماشى مع خصوصيتها، لضمان الأمن المعلوماتي داخل إدارة المنظمات وخارجها، كما أن هذا التطور الكبير في التقنية والتكنولوجية المعلوماتية وضع الحق في الخصوصية موضعا حساسا وأكثر عرضة للانتهاك والاستغلال، الامر الذي جعل مسؤولية وضع الضمانات والسياسيات القانونية التي تجابه هذا الخطر الواقع على الحق في الخصوصية يقع على عاتق الدول الهيئات المختصة.

أهمية الموضوع:

تكمن أهمية العلمية لهذه الدراسة في إبراز أهم المخاطر التي يمكن أن تهدد الخصوصية، انطلاقا من أثر التقنية المعلوماتية لمعالجة المعطيات ذات الطابع الشخصي، لما للحواسيب من قدرة هائلة في تخزين وتجميع أكبر قدر ممكن من البيانات الشخصية واسترجاعها في أقصر وقت ممكن، والاحتفاظ بها لفترة طويلة من الزمن وتصنيف وتوثيق هذه البيانات، مما يهدد أسرار خصوصية الأفراد وسكينتهم، سواء بالاستخدام الخاطئ لمثل هاته البيانات كالإفشاء غير المشروع أو دمج هذه البيانات أو حذفها أو مسحها أو التلاعب بها أو سرقتها عبر مواقع الأنترنت بفعل الالتقاط غير المشروع لها،

في الاثراء القانوني حول الحق في الخصوصية وتأثيرها بالجريمة المعلوماتية، من خلال انتهاكها لكرامة الفرد وكيانه، على غرار أخلقة برامج التقنية الجديدة من خلال توجيه المجتمع التقني إلى ضرورة مراعاة واحترام الحق في الخصوصية المعلوماتية، فضلا عن الوسائل الردعية للحد من الجرائم الماسة بحرمة الحياة الخاصة.

أسباب اختيار الموضوع:

رغم صعوبة هذا الموضوع ودقة وسعة وجدية البحث لارتباطه بجانب علمي وتقني مرتبط بالتكنولوجيا الحديثة واستخداماتها المتطورة، غير ذلك لم يثنينا عن المضي فيه، نظرا لأهميته ولكونه من أهم المواضيع المطروحة على النطاق الدولي والوطني نتيجة التحول الرقمي في العالم، فضلا عن التحول

الكبير الذي تشهده الجزائر في الآونة الأخيرة في رقمنة القطاع الحكومي، والانتقال نحو إدارة بصفر ورقة، الأمر الذي يتطلب جهودا كبيرة في حماية البيانات من مخاطر المعالجة الالكترونية لها، مما يجعل منه موضوعا مستجدا ومستحدثا للدراسة، والبحث بشكل دائم ومستمر، وهو ما يجعل من أمر تطوير وتحديث النصوص القانونية الإجرائية، والدراسة والبحث الأكاديمي، أمرا واجبا في ظل التهديدات التي تشكلها الجريمة المعلوماتية.

صعوبات البحث:

لم يكن بالسهولة بمكان وضع خطة متوازنة ومعالجة فعالة ودقيقة لمثل هذا الموضوع، بالنظر إلى ازدواجية طبيعته (القانونية والفنية)، مما يستدعي ضبطا للمصطلحات والمفاهيم التقنية والقانونية منها، والتي يصعب التحكم فيها، وتوظيفها بالشكل المطلوب، من دون تغليب أي طابع على طابع آخر، تحت طائلة فقدان البحث لازدواجية المعالم.

كما أن انعدام احصائيات وأرقام حول موضوع الجريمة المعلوماتية وانتهاكات الخصوصية، نظرا لانعدام قنوات اتصال مع المصالح الأمنية والقضائية المختصة في متابعة أعمال البحث والتحقيق في هذه الجرائم جعل من الموضوع جافا في لغة الأرقام والاحصائيات والتعليق عليها، واستقراء النتائج والتحليلات.

إشكالية البحث:

موازاة مع الانتقال والتحول الرقمي، تفاقمت الاعتداءات على الخصوصية المعلوماتية عبر وسائل التقنية، الأمر الذي تطلب إيجاد الوسائل القانونية إلى جانب الوسائل التقنية التي تضمن الحماية الفعالة للحق في الخصوصية في العصر المعلوماتي، الأمر الذي جعل المشرع الجزائري قد استجاب لذلك بسن تشريعات جديدة لمواجهة آثار وانعكاسات التقنية المعلوماتية على معالجة المعطيات ذات الطابع الشخصي من خلال قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، فهل استطاع المشرع الجزائري وضع نظام قانوني يضمن حماية الحق في الخصوصية المعلوماتية في ظل تنامي الجريمة المعلوماتية ؟

تساؤلات الدراسة

تتفرع عن مشكلة الدراسة تساؤلات سيتم الإجابة عنها خلال الدراسة وهي:

1- ماهي السلوكيات التي تأخذ طابع الجريمة المعلوماتية؟

2- فيما تتمثل خصوصية الجريمة المعلوماتية التي تهدد التحقيق فيها؟

3- هل يمكن أن يكون للضحية دور في إعاقة التحقيق في الجريمة الالكترونية؟

4- ماهي المعطيات ذات الطابع الشخصي التي تعتبر جوهر الحق في الخصوصية المعلوماتية ويمثل الاعتداء عليها اعتداء على هذا الحق؟

5- فيما تتمثل القيود والضوابط – كإجراء وقائي – والإجراءات الجزائية التي وضعها المشرع في مواجهة الأجهزة الادارية العمومية والمؤسسات الخاصة، عند إنشائها أنظمة معلوماتية لمعالجة معطيات ذات طابع شخصي.

منهجية البحث:

للإلمام بجوانب هذا الموضوع بالنظر لخصوصيته وتشعبه وارتباطه بالجوانب التقنية، اعتمدنا على مناهج تتكامل فيما بينها:

المنهج التحليلي: وذلك من خلال تحليل بعض المفاهيم والغوص في جزئياتها، وطرحها بشكل مفصل، لاسيما النصوص القانونية والاستعانة بالآراء الفقهية للوصول لمعناها الحقيقي.

منهج وصفي: وهو المطلوب مع مشكلة البحث وذلك من خلال وصف الجزئيات والمفاهيم التي تم التطرق لها مثل بعض الانتهاكات والأفعال الماسة بالحق في الخصوصية.

المنهج المقارن: حيث النظام القانوني للدول مختلف عن بعضها، فمن باب الاستنارة بهذه التشريعات ومقارنة كيفية معالجتها لموضوع الحق في الخصوصية، والذي يعد دون شك ذو طبيعة عالمية.

خطة البحث

للوصول للهدف المنشود من هذه الدراسة تم انتهاج خطة مقسمة إلى فصلين، نتناول في الفصل الأول الإجرام المعلوماتي وصعوبة التحقيق، حيث نعالج فيه مفهوم الإجرام المعلوماتي وأركانه في المبحث الأول، لنعرج في المبحث الثاني إلى صعوبة التحقيق في ظل وجود جريمة معلوماتية من خلال انعكاسات خصوصية الجريمة المعلوماتية على إجراءات التحقيق فضلا عن دور الضحية في إعاقة سير التحقيق في هذه الجرائم.

أما الفصل الثاني فخصصناه للحق في الخصوصية وأوجه حمايته، من خلال تعريف الحق في الخصوصية المعلوماتية ونطاق الاعتداء عليها في المبحث الأول، أما البحث الثاني فتناولنا فيه حماية سرية المراسلات والاتصالات الالكترونية وحماية الأشخاص الطبعيين في المعالجة الآلية للمعطيات.

وفي آخر هذه الدراسة خلصنا إلى مجموعة من النتائج والاقتراحات، تم التوصل لها من خلال هذه الدراسة تم ادراجها في خاتمته.

الفصل الأول

الإجرام المعلوماتي وصعوبة التحقيق

شهد العالم في الآونة الأخيرة تطورا ملحوظا في مجال التقنية، نتج عنه استعمالا للحاسب الآلي وشبكة الأنترنت في جميع الميادين، إذ قد يُستخدم هذه الوسائل بطرق غير مشروعة، الأمر قد ينجر ارتكاب له علاقة بهذا المجال، وهو ما يُعرف بالجريمة الإلكترونية، ولحداثة هذه الجريمة، فقد اختلف الفقهاء في وضع تعريف موحد لها، حيث اتسمت بمجموعة من الخصائص، سنحاول في هذا الفصل التطرق إلى مفهوم الإجرام المعلوماتي وأركانه في المبحث الأول، لنتطرق إلى صعوبة التحقيق في الجريمة المعلوماتية بالنظر إلى خصوصيتها وخصوصية الضحية فيها في المبحث الثاني.

المبحث الأول: مفهوم الإجرام المعلوماتي وأركانه

سنتطرق في هذا المبحث إلى تعريف الإجرام المعلوماتي – الضيق والموسع وموقف المشرع الجزائري (المطلب الأول)، وتحديد أركانها (المطلب الثاني).

المطلب الأول: تعريف الإجرام المعلوماتي

استعصى على رجال الفقه ورجال القانون الجنائي التوصل إلى اتفاق حول مصطلح دقيق للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فنجد من يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، بينما يفضل آخرون تسميتها بالجريمة المعلوماتية.[1]

وأمام هذا الفراغ القانوني، بذل الفقه محاولات متعددة لإيجاد تعريف لهذه الجرائم، فانقسم في ذلك إلى اتجاهين رئيسيين، الاتجاه الأول المضيق لمفهوم الجريمة المعلوماتية، الاتجاه الثاني الموسع لمفهوم الجريمة المعلوماتية، سنحاول في هذا المطلب التطرق إلى هاذين الاتجاهين في تعريف الجريمة الالكترونية.

أولا: التعريف الضيق للجريمة المعلوماتية

اختلف أنصار هذا الاتجاه في تعريف الجريمة المعلوماتية، من حيث المعيار المعتمد، فمنهم من عرّف الجريمة المعلوماتية أنها: " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر لازما لارتكابه من ناحية ولملاحقته من ناحية أخرى"[2]. من خلال التعريف يتبين لنا أنه أُخذ بمعيار وسيلة ارتكاب الجريمة وهي الكمبيوتر إذ اعتبرها فعلا غير مشروع، فلا يكفي أن تتوافر المعرفة بتكنولوجيات الحاسبات الآلية بدرجة كبيرة من أجل ارتكاب الجريمة بل من أجل ملاحقتها أيضا، فأنتقد هذا التعريف كونه يحصر الجريمة المعلوماتية في الجرائم التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها[3].

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، طبعة الأولى، عمان، 2008، ص 46.

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الإسكندرية، 2005، ص 97.

[3] سوير سفيان، جرائم المعلوماتية، مذكرة مقدمة لنيل شهادة ماجستير في العلوم الجنائية، جامعة أبو بكر بلقايد، كلية الحقوق وعلوم السياسية، قسم الحقوق، سعيداني تلمسان، 2010، ص 12.

وأخذ البعض الآخر من أنصار هذا التجاه، بمعيار النتيجة، حيث عرّفها الأستاذ الفرنسي ماس بأنها: " تلك الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح "[4]، الغاية من الجريمة المعلوماتية حسب التعريف مادية تتمثل في تحقيق ربح، وبذلك فقد ركز على معيار النتيجة.

كما أن البعض الآخر زاوج بين المعيارين: معيار موضوع الجريمة وهو محاولة الوصول إلى المعلومات بطريقة غير مشروعة، على غرار معيار وسيلة ارتكاب الجريمة وهي الحاسوب أو الكمبيوتر، كتعريف الفقيه روزملات بأنها:" نشاط غير مشروع موجه للنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب او تغييرها، أو حذفها أو التي تحل عن طريقه"، ما يُعاب على هذا التعريف أن الكثير من الأفعال المشروعة، والتي يُستخدم فيها الحاسب الآلي كأداة لارتكابها كالاحتيال المعلوماتي، لا تدخل في نطاق الجريمة المعلوماتية.[5]

ثانيا: التعريف الموسع للجريمة المعلوماتية

يرى فريق من الفقهاء ضرورة توسيع مفهوم الجريمة المعلوماتية، تفاديا للقصور الذي شاب تعريفات الاتجاه الضيق في الاحاطة بأفعال الاجرام المعلوماتي.

فمنهم من عرفها بأنها:" كل أشكال السلوك غير المشروع الذي يُرتكب باستخدام الحاسوب "[6]، وعرفها البعض الآخر على أنها: " كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنيّة المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية "[7].

أُنتقد هذا التعريف في إضفاء وصف الجريمة المعلوماتية بمجرد مشاركة الحاسب الآلي في السلوك الإجرامي، حيث نجد صعوبة قبول هذا التوجه، فجهاز الحاسب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأقراص أو الأسطوانات الممغنطة أو اللواحق على سبيل المثال، ومن ثم لا يمكن إعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، حاله في ذلك حالة الاعتداء على أجهزة الحاسوب التي لم تدخل حيز الخدمة أو في حالة التجربة، أو الأنظمة المعلوماتية التي خرجت عن الخدمة[8]، أو كمن يقوم

[4] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، دون طبعة، الاسكندرية، مصر، 2004، ص 43.
[5] نهلا عبد القادر المومني، المرجع السابق، ص 46.
[6] سوير سفيان، المرجع السابق، ص 14.
[7] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الأولى، القاهرة، 1994، ص 04.
[8] قارة أمال، الجريمة المعلوماتية، رسالة ماجستير تخصص القانون الجنائي والعلوم الجنائية، كلة الحقوق، جامعة الجزائر، 2005، ص 28.

بالاتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السرقة أو السطو على بنك أو لارتكاب أي جريمة أخرى.

كما أقر المجلس الأوروبي بقيام المخالفة – الجريمة – في كل حالة يتم فيها " تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها؛ وتبعا لذلك تسبب في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر"، وقد عرفها مؤتمر الأمم المتحدة العاشر المنعقد في بفيينا بتاريخ 10 إلى 17 أبريل 2000، بأنها: " أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي[9] أو شبكة حاسوبية، أو داخل نظام حاسوب الكترونية، والجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية "، تبنى الدكتور نهلا عبد القادر المومني هذا التعريف كونه حاول الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية سواء التي قد تقع بواسطة النظام المعلوماتي أو لك التي تكون داخل هذا النظام على المعطيات والبرامج والمعلومات، كما أنه شمل على جميع الجرائم الممكن وقوعا في بيئة الكترونية، فهذا التعريف لم يركز على فاعل الجريمة وقدرته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية، بل حاول عدم حصر الجريمة في نطاق ضيق يتيح المجال أمام إفلات العديد من صور الجريمة من دائرة العقاب. [10]

ثالثا: موقف المشرع الجزائري

أخذ المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح " الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال "[11] بحيث أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية يعد " محلا للجريمة " ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن القول بتوفر أركان الجريمة، وبالعودة إلى قانون العقوبات الجزائري نجد أن المشرع الجزائري اكتفى بالنص على العقوبة لبعض الأفعال الماسة بنظام المعالجة الآلية للمعطيات، في المواد من 394 مكرر إلى المادة

[9] أمام هذه الثورة التكنولوجية والتقنية الجارفة، أفرزت أجهزة أخرى الأمر الذي يستدعي ضرورة شمول الجريمة المعلوماتية كل ما له علاقة بالاستخدام غير الشرعي لأي وسيلة تكنولوجية ناقلة للمعلومة وعدم حصرها في جهاز الكمبيوتر.

[10] نهلا عبد القادر المومني، المرجع السابق، ص 49.

[11] المادة الثانية من القانون 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر عدد 47، الصادرة سنة 2009، المعدل والمتمم، تنص على انه: يقصد في مفهوم هذا القانون ما يأتي: الجرائم المتصلة بتكنولوجيا الاعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أة نظام الاتصالات الالكترونية "

394 مكرر 7 منه، دون أن يأتي لتعريف جرائم الانترنت، وترك ذلك للفقه والاجتهاد القضائي، مستأنسا بتجربة نظيره الفرنسي الذي لم يقم هو الآخر بذلك[12].

وبالرجوع إلى القانون رقم 04/09 نجد أن المشرع الجزائري نص بالإضافة إلى الجرائم المساس بأنظمة المعالجة الآلية المعطيات المحددة في المواد السالف ذكرها من قانون العقوبات، " أي جريمة أخرى تُرتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام الاتصالات الالكترونية "، وبذلك يكون المشرع الجزائري قد أعطى تعريفا موسعا للجريمة المعلوماتية، إذ لم يعد مفهوم الجريمة المعلوماتية مقتصرا على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء، بل تعدى ذلك للأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها.

من جهة أخرى نجد المشرع الجزائري تطرق أيضا للجرائم الالكترونية والعقوبات المقررة لها المتعلقة بالتجارة الالكترونية في القانون رقم 05/18[13]، في الفصل الثاني من الباب الثاني تحت عنوان: الجرائم والعقوبات، في المواد من 37 إلى 48، غير أن هذا القانون لم ينص هو كذلك على تعريف للجريمة الالكترونية.

من خلال ما سبق يتضح أن المشرع الجزائري:

- اعتمد عدة معايير للدلالة على الجريمة الالكترونية، منها معيار وسيلة ارتكاب الجريمة ويتمثل في نظام الاتصالات الإلكتروني، ومن جهة أخرى اعتمد المشرع معيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات، على غرار معيار القانون الواجب التطبيق أو ما يصطلح عليه بالركن الشرعي المنصوص عليه في قانون العقوبات، كما اعتمد المشرع الجزائري على معيار رابع يتمثل في نطاق الجريمة الالكترونية أو ما يسمى بالركن المفترض على اعتبار أن الجريمة ترتكب في النظام المعلوماتي أو نظام الاتصالات الالكترونية[14].
- بالرجوع إلى نص المادة 02 من القانون 04/09 – السالف الذكر استعمل عبارة " أي جريمة أخرى "، التي قد أُريد منها عدم الافلات من المسؤولية الجزائية أو العقاب، غير أنها تتنافي ومبدأ شرعية التجريم والعقاب، أذ أن هذه الجريمة تتطور يوما بعد يوما بتطور التكنولوجيا ونظام

[12] قارة أمال، المرجع السابق، ص 28.
[13] القانون 05/18 المؤرخ في 10 مايو 2018، المتعلق بالتجارة الالكترونية، ج ر، عدد 28، الصادرة في 16 مايو 2018.
[14] أنظر المادة 2 من القانون 04/09 السالف الذكر.

المعلومات، إذا أن النصوص القانونية الموضوعية والتي تجرم كل فعل بعينه وتحدد أركانه والعقوبة المقررة له قاصرة أو غائبة في ذلك، كما لا يمكن القياس لمتابعة أي شخص جزائيا في حال لو ارتكبت جريمة تقليدية بواسطة منظومة معلوماتية في ظل غياب النص الجزائي الذي يجرّم هذا الفعل إذا ارتكب بواسطة منظومة معلوماتية صراحة، مما يستدعي بالمشرع الجزائري أن يعمل على تعديل النصوص القائمة بما يتماشى مع التطور الحاصل في تكنولوجيا المعلومات من جهة، ومن جهة اخرى حتى تستوعب الصور المتطورة للجريمة التقليدية التي يمكن حسب طبيعتها أن تُرتكب في منظومة معلوماتية[15].

- وفكرة حصر الجريمة في تعريف شامل هو مساس بمفهوم النظام نفسه، إذ أنه في تطور مستمر لارتباطه بعناصر تقنية محضة، فترك مهمة تعريفه للفقه والقضاء فكرة جديرة بالاهتمام، وهذا ما يراه بعض الفقه.[16]

المطلب الثاني: أركان الإجرام المعلوماتي

للجريمة الالكترونية ثلاثة أركان مثلها مثل الجريمة الكلاسيكية، غير أن الجريمة المعلوماتية تتمثل بخصوصيات تختلف عن الجرائم الاخرى، وهذا ما سنتناوله بالتفصيل في هذا المطلب، وتتمثل في الركن الشرعي والمادي والمعنوي على غرار الركن المفترض.

أولا: الركن الشرعي

يقوم الركن الشرعي على مبدأ " لا جريمة ولا عقوبة أو تدبير أمن من غير قانون "، فإذا انتفى التجريم انتفت المسؤولية الجزائية لمرتكبها، فهذا المبدأ يعد ضمانا لمصلحة الأفراد وهو الحامي لحقوقهم وكفالة للحريات الفردية، فملاحقة الأفعال وتوقيع العقاب يكون ناتجا من قوانين صادرة من السلطة التشريعية، السلطة الوحيدة التي يخول لها تجريم الأفعال ومعاقبة مرتكبيها

يعد نص المواد 144 مكرر و146 مكرر و144 مكرر 2 و146 من قانون العقوبات رقم 01-09 المؤرخ في 26 جويلية 2001 أو نص تشريعي في مجال الإجرام المعلوماتي، والمتعلق بجريمة القذف والسب والإهانة إزاء رئيس الجمهورية أو فيما يخص كل ما هو معلوم بالضرورة بالدين أو ضد الهيئات

[15] صليحة بوجادي، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، الجزائر، 2021، ص 2531.

[16] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة، الجزائر، 2013، ص 43.

أو المؤسسات العمومية، إذ أدرج المشرع الجزائري لأول مرة مصطلح " .... وسيلة إلكترونية أو معلوماتية .... " وهو ما يجرم بالأفعال السالفة الذكر في محيط المعلومات والانترنت[17].

في حين خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال، تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات[18]، ويشمل على 8 مواد تتناول كل جرائم الاعتداءات على الأنظمة المعلوماتية، الذي تم تعديله بموجب القانون 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها[19].

تجدر الإشارة إلى أن المشرع واجه عدة عراقيل عند تنظيمه لمجال الحماية الجنائية من مخاطر جرائم المعلوماتية، وكانت أول العراقيل هو إمكانية تطبيق النصوص التقليدية على هذا النوع الجديد من الجرائم، أم أن ذلك يعد إخلالا بمبدأ الشرعية؟ ووقوع في التفاسير المخلة بمبادئ القانون الجنائي؟

اختلف المشرعين في ذلك بين من يرى ضرورة وضع نصوص خاصة بالجرائم الالكترونية وبين من يرى بتكييف النصوص القديمة مع هذه الجرائم الحديثة، وطرف ثالث يرى أنه لا فائدة من تطبيق التشريع الخاص بجرائم عادية ترتكب بوسائل تقنية متطورة، على النقيض يرى البعض أن في ذلك إخلال بالبنيان القانوني حيث أن المشرع يتطلب في الجرائم التقليدية سلوكا محددا وتتحقق مع الركن المادي للجريمة تختلف عن السلوكيات المطلوبة في الجرائم الإلكترونية، وهناك من يرى أن الجرائم المعلوماتية ماهي إلا جرائم عادية ترتكب بواسطة الحاسب الآلي، فالمطلوب من المشرع توقيع العقاب على ارتكاب هذه الجرائم بنصوص تقليدية.[20]

طرح هذا الاختلاف بين المشرعين اشكاليتين أساسيتين هما: إشكالية الموقع وإشكالية المصطلحات

---

[17] شلاخ لطيفة، انتشار الجريمة الالكترونية الماسة بالأشخاص في الهيئة الجزائرية، دراسة ميدانية لبعض مستخدمي مقاهي النت بمدينة المسيلة، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام الآلي والاتصال تخصص صحافة مكتوبة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف، المسيلة، ماي 2017، ص 14.

[18] أنظر القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، ج ر 71، يتضمن المواد من 394 مكرر إلى 394 مكرر 7.

[19] القانون 09/04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ج ر 47.

[20] معتوق عبد اللطيف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير علوم جنائية، جامعة العقيد الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة 2011-2012، ص 25.

1- إشكالية الموقع

إذ فالسؤال المطروح في هذا أين يمكن إدماج النصوص القانونية الجديدة في قانون العقوبات التقليدي؟ أم في قانون خاص؟ هناك من يقول بإمكانية إدماجها في جرائم الأموال باعتبار إمكانية إضفاء صفة المال على الكيانات المادية والمعنوية للحاسوب، والبعض الآخر يفضل إدماجها في إطار خاص بالجرائم ضد الملكية، باعتبار أن الكيان المادي للحاسوب عناصر مادية قابلة للتملك، وهناك من يرى إضافة جزء آخر خاص بالجرائم المعلوماتية مستقل عن الجرائم التقليدية كونها تتعلق بقيمة اقتصادية، جديدة لها طابع خاص.

وهناك من يرى بإلحاق كل جريمة معلوماتية بما يقابلها في قانون العقوبات التقليدي، جريمة التزوير المعلوماتي في باب تزوير المحررات، أفعال الاعتداء على المحررات يلحق بجرائم الاتلاف... إلخ.[21]

2- إشكالية المصطلحات

تتميز الجريمة المعلوماتية بالطابع التقني، الذي يطرح مشكل المصطلحات التقنية نظرا لغموض مفهومها باعتبارها مصطلح غريب عن لغة القانون.

فالإشكالية التي يطرحها الركن الشرعي للجريمة المعلوماتية يختلف عن مواقف التشريعات في تحديد تعريف للمصطلحات التقنية في الدول الانجلوسكسونية التي تعتمد على القانون في إعطاء التعريفات، على غرار الطريقة الفرنسية التي توكل مهمة تحديد التعريفات والمعاني للقضاء وهي الطريقة المفضلة نظرا لسرعة تطور تقنيات الاعلام الآلي في إمكانية مواكبة التطورات الحاصلة في هذا المجال. [22]

ثانيا: الركن المادي

يعتبر الركن المادي للجريمة المظهر الخارجي وكيانه المادي الظاهر، أو الماديات المحسوسة في العالم الخارجي، غير أن الركن المادي في الجريمة المعلوماتية له خصوصية عن الجرائم التقليدية كونه يقوم على صور في فعل الاعتداء والمتمثلة في:

[21] علي عبد القادر لقهوجي، الحماية الجنائية لبرنامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، د ط، 1999، ص 24.
[22] المرجع نفسه، ص 24.

ا. الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك

نصت المادة 394 مكرر من قانون العقوبات على أن الدخول أو الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك يشكل فعلا إجراميا ولهذا الفعل حسب هذه المادة صورتين هما:

1- الصورة البسيطة

يتمثل هذا النشاط الإجرامي في الأفعال التالية:

أ- **فعل الدخول:** وتحقق بمجرد الوصول إلى المعلومات المخزنة داخل النظام دون علم ورضا صاحبه، لأن هذا النظام لا يسمح للدخول فيه إلا الأشخاص المعينين أو يسمح بالدخول لكن مقابل نفقات.

كما أن المشرع الجزائري لم يحدد وسيلة الدخول أو الطريقة التي يتم بها الدخول إلى النظام، فتقوم الجريمة بأي وسيلة أو طريقة تمت بها عملية الدخول، فيستوي أن يكون الدخول مباشر أو غير مباشر، كما الجريمة تقوم ضد أي شخص مهما كانت صفته، وكفاءته المهنية والفنية، فليست من جرائم ذوي الصفة، بشرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو خطأ.[23]

تجدر الإشارة أن جريمة الدخول إلى النظام المعلوماتي هي جريمة شكلية، أي أنها تتحقق بمجرد الدخول إلى النظام المعلوماتي ولا يشترط فيها الوصول إلى المعطيات التي يحتويها النظام أو إحداث ضرر بالمعطيات أو بصاحبها.[24]

ب- **البقاء:** ويعني التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له حق السيطرة على هذا النظام، او تجاوز المدة المسموح له البقاء فيها، أو عدم الانسحاب فورا وقطع وجوده في نظام البيانات أو يطبع معلومات يسمح له برؤيتها أو الاطلاع عليها فقط.[25]

---

[23] جمال براهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، جامعة مولود معمري، تيزي وزو، الجزائر، المجلد 11، العدد 02، نوفمبر 2016، ص 124-155، ص 127.

[24] نسمة بطيحي، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، جامعة سطيف 02، المجلد 01، العدد 01، جوان 2019، ص 78.

[25] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه، الجزائر، الطبعة الثانية، 2007، ص 100.

2- الصورة المشددة:

نصت عليها المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات، حيث تُشدد العقوبة على فعل الدخول والبقاء غير المشروع عندما ينتج عنها محوٌ أو تحويل للمعطيات التي يحتويها النظام، أو تخريب نظام اشتغال المنظومة بحيث يؤدي ذلك إلى عدم صلاحيته لأداء وظائفه، فتربط بهذين الظرفين علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع والنتيجة الضارة وإن لم تكن مقصودة، إلا أثبت الجاني انتفاء تلك العلاقة السببية واثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ.

وقد اتجه غالبية الفقه إلى اعتبار أن هذه الجريمة جريمة سلوك مجرد أو السلوك المحض، أن أنها تقع وتكتمل بمجرد الانتهاء من السلوك المكون لها سواء تعلق بالدخول أو البقاء، أو بهما معا، أي أن الركن المادي لتلك الجريمة لا يشترط فيه بالضرورة التقاط معلومات بأي شكل من الأشكال، فلم يشترط المشرع في نموذجها القانوني أي نتيجة إجرامية.[26]

إلا أن الفقه لم يتفق ما إذا كانت هذه الجريمة وقتية او مستمرة أو متتابعة الأفعال، غير أن الرأي الراجح في هذا الصدد ذهب إلى اعتبار جريمة البقاء جريمة مستمرة كون الفترة الزمنية التي تستمر فيها جريمة الدخول قصيرة نسبيا بحيث يمكن اعتبارها مستمرة أو وقتية ذات أثر ممتد من دون أثر. [27]

II. الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات

لم يورد المشرع الجزائري نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء العمدي لمعطيات الموجودة داخل النظام، وهذا راجع إلى تفسير أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام ووظائفه، كما أن برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية،[28] على خلاف المشرع الفرنسي في قانون العقوبات فقد نصت المادة 2/323 على أنه بمجرد إعاقة أو إفساد اشتغال نظام المعالجة الآلية للمعطيات.[29]

اختلف الفقه في هذا الشأن فيما إذا كان هذا الاعتداء وسيلة أم غاية؟

---

[26] أمال قارة، المرجع السابق، ص 114.

[27] جميل عبد الباقي الصغير، جرائم التكنولوجيا الحديثة، دار النهضة العربية، الطبعة الأولى، القاهرة، 2001 ص 108.

[28] تنص المادة 3/02 من القانون 09-04 في تعريفها للمعطيات المعلوماتية بانها: " أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، **بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها "**

[29] أمال قارة، المرجع نفسه، ص 113.

فإذا كان الاعتداء مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا الاعتداء غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

وتتشكل صورة الاعتداء العمدي على سير النظام فعلين يتمثلان في:

1- التعطيل (العرقلة):

لم يشترط المشرع الجزائري أن يتم التعطيل بوسيلة معينة فيستوي أن يتم التعطيل بواسطة مادية مثل كسر الأجهزة المادية للنظام أو تحطيم أسطوانة، أو عن طريق وسيلة معنوية مثل تلك التي تتم بواسطة زراعة برنامج فيروسي (حصان طروادة)، قنابل منطقية مؤقتة، مما يجعل النظام يتباطأ في أدائه، كما يستوي أن يقترن التعطيل بالعنف أو من دونه.

2- الإفساد:

وذلك بإحداث خلل في نظام سيره وفقدان صلاحية أدائه لوظائفه، كأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، أو أنه يحول دون تحقيقه لوظائفه بشكل صحيح، حيث يصبح النظام غير صالح للاستعمال.

ويستوي أن يكون هذا التعييب كلي أو جزئي للنظام، وهو الذي يعتبر مشددا لجريمة الدخول والبقاء غير المشروع، غير أن الفرق يكمن في أن الافساد لا يشترط أن يكون عمديا في جريمتي الدخول والبقاء، بينما يكون شرطا بالنسبة لجريمة الاعتداء العمدي على نظام المعالجة الآلية للمعطيات.

في هذا الخصوص كان من الأجدر على المشرع الجزائري إضافة نص خاص بتجريم الاعتداء على سير النظام لرفع اللبس والحرج عن القاضي الجزائي الذي تفرضه قاعدة التفسير الضيق للنص الجزائي.[30]

تجدر الإشارة إلى أن المشرّع الجزائري قد جرّم كلا من الاشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية المذكورة، وجعل العقوبة لهما تساوي العقوبات المقرّة للجريمة ذاتها.

[30] ونوغي نبيل،زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، المجلد 04، العدد 03، الجزائر، 2019، ص ص 127-139، ص 13.

III. الاعتداء العمدي على المعطيات

نص عليها المشرع الجزائري في المادة 394 مكرر 01، والمادة 394 مكرر 02 من قانون العقوبات، حيث جرّم في الفقرة الأولى الاعتداء العمدي على المعطيات الموجودة داخل النظام المعلوماتي، بينما جرّم في الثانية المساس العمدي بالمعطيات الموجودة خارج النظام، وهذا ما سنبيّنه فيما يلي:

1- الاعتداءات العمدية للمعطيات الموجودة داخل النظام المعلوماتي

تتجسد هذه المعطيات العمدية على المعطيات في ثلاث أفعال هي: الادخال والمحو والتعديل، ولا يشترط اجتماع هذه الأفعال، بل يكفي أن يصدر من الجاني إحدى هذه الأفعال لتوفر الركن المادي.[31]

أ- الإدخال:

يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة الخاصة به سواء أكانت خالية أم أن عليها معطيات من قبل،[32] ويتجسد ذلك في حالة الاستخدام التعسفي لبطاقات السحب والائتمان مثلا، سواء من صاحبها الشرعي أو من غيره كحالة السرقة والتزوير.[33]

ب-المحو:

ويقصد به إزالة جزء من معطيات مسجلة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.[34]

ج- التعديل:

وهو تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، إذ قد يكون التلاعب في المعطيات عن طريق استبدالها أو عن طريق التلاعب في البرنامج، بإمداده بمعطيات مغايرة تؤدي إلى نتائج مغايرة عن تلك التي صُمم البرنامج لأجلها، وقد يكون بالتلاعب في المعطيات سواء بالمحو الكلي أو الجزئي وعادة ما تكون ببرامج الفيروسات وهي مختلفة الأنواع والأشكال.[35]

---

31 أمال قارة، المرجع السابق، ص 120.

32 على عبد القادر لقهوجي، المرجع السابق، ص 60.

33 أمال قارة، المرجع نفسه، ص 120.

34 علي عبد القادر لقهوجي، المرجع نفسه، ص 60.

35 لمعيني محمد، محاضرات ألقيت على طلبة السنة ثانية ماستر جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر ، بسكرة، الجزائر، 2015، 2016.

كما أن أفعال الإدخال والمحو والتعديل وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمنت اعتداء على المعطيات الموجودة داخل نظام كما أن أفعال الإدخال والمحو والتعديل وردت على سبيل الحصر، ومنه لا يقع تحت طائلة التجريم أي فعل آخر غيرها، ولو تضمن ذلك اعتداء على المعطيات الموجودة داخل نظام.[36]

2- الاعتداءات العمدية للمعطيات الموجودة خارج النظام المعلوماتي

نصت عليها أحكام المواد 394 مكرر 2 من قانون العقوبات، والتي كرّس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها، إذ لم يشترط أن تكون تلك المعلومات داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، حيث نصت هذه المادة على أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو معالجة آلية أو مرسلة عن طريق منظومة معلوماتية، مادامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

على غرار الفقرة الثانية من المادة 394 مكرر 2 جرمت أفعال الحيازة، الإفشاء، النشر، الاستعمال، أيا كان الغرض من هذه الأفعال التي ترد على المعلومات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات، إذ قد تكون منافسة غير مشروعة، ابتزاز، جوسسة، إرهاب، ..... إلخ.[37]

ثالثا: الركن المعنوي

يختلف الركن المعنوي للجريمة الالكترونية باختلاف أشكالها، وتأخذ صورة القصد الجنائي إضافة إلى نية الغش، سنحاول فيما يلي التعرض للركن المادي لكل جريمة على حدا.

1- جريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات

إلزامية توافر الركن المعنوي تقتضي اتجاه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء مع علمه بعدم أحقيته في الدخول إلى النظام والبقاء فيه، إذ أنه ينتفي الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به أو مشروع، أو إذا وقع الجاني في الخطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو البقاء، أو في نطاق هذا الحق بأن يجهل وجود الخطر من

[36] سوير سفيان، المرجع السابق، ص 94.
[37] نائلة عادل محمد فريد قورة، المرجع السابق، ص 366.

جراء الدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول، فضلا عن ذلك ففي حالة توافر القصد الجنائي بعنصريه العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء، فيضل قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام، في حين تبرز نية الغش من خلال الطريقة التي يتم بها الدخول عن طريق خرق الجهاز الرقابي الذي يحمي النظام، على غرار البقاء فتستنتج من خلال العمليات التي تمت داخل النظام.

2- جريمة الاعتداءات على سير نظام المعالجة الآلية للمعطيات

تعد هذه الجرائم عمدية بطبيعتها، فالمفروض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء غير المشروع داخل النظام.[38]

فالقصد الجنائي يُستنتج من طبيعة الأفعال المجرمة، ويظهر من خلال الأفعال المشكلة لهذه الجريمة، فلا يتصور أن يقوم الفاعل بالاعتداء على سير نظام المعالجة الآلية للمعطيات بعرقلته أو تعطيله أو إفساده من غير قصد.[39]

3- جريمة الاعتداءات العمدية على المعطيات

تعد هذه الجريمة بدورها من الجرائم العمدية، التي تتطلب لقيامها توافر القصد الجنائي بنوعيه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بخطورة النشاط الإجرامي الذي يقوم به وما يترتب عنه من عقاب، كما أنه بفعله يعتدي على صاحب الحق في السيطرة على تلك المعطيات دون موافقته، كما أن الضرر قد يتحقق في الواقع نتيجة للنشاط الاجرامي ولكن ليس عنصرا في الجريمة.

كما يجب أن تتجه إرادة الفاعل إلى فعل الإدخال أو المحو أو التعديل، فلا يُسأل من قام بذلك خطأ أو عن غير قصد، بل يُسأل طبقا لأحكام المادة 394 مكرر 3/2 التي تتناول الصورة المشددة لجريمتي الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية للمعطيات، إذ تعاقب الفاعل عن الحذف والتغيير المترتب عن الدخول والبقاء غير المشروعين ولو خطأ، إذ نصت المادة 394 مكرر 01 من قانون العقوبات على شرط ارتكاب هذه الأفعال " بطريق الغش "، ولا تتطلب قصد جنائيا خاصا، عكس بعض التشريعات المقارنة التي اشترطت القصد الخاص

[38] أمال قارة، المرجع السابق، ص 124.
[39] علي عبد القادر القهوجي، المرجع السابق، ص 142.

إلى جانب القصد العام، ويتمثل في اتجاه نية المتهم إلى الاضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير، وهو ما كان عليه النص الفرنسي القديم قبل تعديله، ثم تراجع عن ذلك واستبعده.[40]

4- جريمة استخدام المعطيات كوسيلة لارتكاب الجرائم الماسة بالأنظمة المعلوماتية

وتتم بإحدى الأفعال المنصوص عليها في المادة 394 مكرر 2 من قانون العقوبات والمتمثلة في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو استعمال لأي غرض المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، فلا يتصور أن تتم من دون علم وإرادة الفاعل مما يجعلها عمدية، غير أن المشرع اشترط أن يكون ذلك بطريق الغش، فاشترط القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش في هذه الصورة كذلك.

رابعا: الركن المفترض:

الركن المفترض هو أمر يطلبه القانون في الجريمة لقيام النموذج القانوني لتلك الجريمة، ففي الجريمة المعلوماتية فيستلزم لقيامها وجود نظام المعالجة الآلية للمعطيات، فما هو هذا النظام؟

1- تعريف نظام المعالجة الآلية للمعطيات

عرفه بعض الفقه على أنه عبارة ع 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.[41]

بناء على ذلك طُرح الإشكال عن مفهوم التعدد الذي يحمله هذا النظام، عند وقوع الاعتداء على عنصر بمفرده داخله، هل نكون أمام اعتداء على النظام بأكمله؟

اعتبر العديد من الفقهاء، أن العبرة تكون باستقلالية أو ارتباط هذا الجزء بالنظام، فإذا كان مستقلا عنه، لإننا لا نكون بصدد جريمة معلوماتية، حاله حال البرامج المعروضة للبيع، أو أجهزة

[40] نائلة عادل محمد فريد قورة، المرجع السابق، ص 368.
[41] سعيداني نعيم، المرجع السابق، ص 42.

الحاسوب التي لم تدخل حيز الخدمة أو في حالة التجربة، أو تلك الأنظمة المعلوماتية التي خرجت من الخدمة، – مثل ما أشرنا إليه سابقا –[42]

وبالرجوع إلى التعريف المقترح من قبل مجلس الشيوخ، فإنه يحمل مجالات محددة، حيث عرّف نظام المعالجة الآلية للمعطيات بأنه: " 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 الفنّية ".[43]

يعد هذا التعريف أدق وأشمل من التعريف السابق، إلا أنه بالإضافة إلى تحديد عناصر المعطيات بدقة، اشترط توفر الحماية الفنية اللازمة لهذه المعطيات، وإلا لم تعد جريمة معلوماتية.

2- الحماية الفنية للنظام المعلوماتي كشرط لقيام المسؤولية الجزائية

اختلف الفقه القانوني في مدى اعتبار الحماية الأمنية لنظام المعالجة الآلية للمعطيات كشرط ضروري ليحظى بالحماية الجزائية من عدمها، إلا أن جانبا من الفقه الفرنسي لم يشترط توفر الحماية الفنية النظام المعلوماتي لقيام الجريمة المعلوماتية،[44] وذلك أن نظام الأمن والحماية الفنية والتقنية لا يكون له سوى دور إيجابي، فثبوت نية المنتهك لهذا النظام ودخوله إليه بطريقة غير شرعية هي متوفرة أساسا.[45]

في حين اعتبر جانب من الفقه بضرورة وجود نطاق كاف من الحماية الأمنية لمختلف الأنظمة المعلوماتية المعالجة آليا، مقسما هذه الأجهزة إلى 03 أصناف:

- أنظمة مفتوحة للجمهور
- أنظمة قاصرة على أصحاب الحق فيها، ولكن دون حماية فنيّة
- أنظمة قاصرة على أصحاب الحق فيها، مع توفرها على حماية فينة لها.

حيث يرى هذا الجانب من الفقه أن هذا النوع الأخير من الأنظمة المعلوماتية هو الذي يتمتع بالحماية الجنائية، وحجتهم أن الحماية الجنائية يجب أن تقتصر على الأنظمة المحميّة فنيا، لأنه من الطبيعي

---

[42] قارة امال، المرجع السابق، ص 28

[43] سعيداني نعيم، المرجع السابق، ص 43.

[44] المرجع نفسه، ص 45.

[45] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، - دراسة مقارنة -، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، مصر، 2000، ص 264.

أن يستغلها أي شخص، فالقانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم وبتوفر الحماية الأمنية ولو بقدر أدنى.[46]

لكن السؤال المطروح في هذه الحالة حول إمكانية عدم توفر نظام معلوماتي على نظام حماية فنية على قدر ما ولو كان بسيطا، إذ أنه من الناحية العملية أصبح من غير المعقول تقبل فكرة وجود نظام معلوماتي لا يحتوي على عنصر الحماية الفنيّة له، لذ فإن وجود هذه الحماية له دور كبير في تحديد القصد الجنائي لدى المجرم المعلوماتي، فلم يعد توفر هذا الشرط محلا للنقاش في الآونة الأخيرة.[47]

[46] قارة امال، مرجع سابق، ص 29.

[47] بن دراح علي ابراهيم، محاضرات ألقيت على طلبة السنة ثانية ماستر جنائي، كلية الحقوق والعلوم السياسية، المركز الجامعي آفلو، الجزائر، 2020-2021، ص 12.

المبحث الثاني: صعوبة التحقيق في ظل وجود جريمة معلوماتية

لاشك أن ثورة المعلومات كان لها الأثر الإيجابي على حياة الأفراد والمجتمعات، فأصبحت عنصرا لا يمكن الاستغناء عنها، إلا أنها على النقيض أصبحت رقما صعبا في زيادة نسبة الجريمة المعلوماتية، تنعكس على خصوصيتها على إجراءات التحقيق الجنائي، كما أنها تعتبر عنصرا لا غنى عنه لمباشرة الإجراءات الجزائية، ومن ناحية ثانية قد يستصعب الوصول إليها لطبيعتها غير الملموسة، وللدليل المستمد منها، كما يتميز مرتكبي هذه الجرائم الذكاء والقدرة التقنية على إخفاء معالم الجريمة، وهو ما يؤدي إلى صعوبة وصول الجهات المكلفة بالتحقيق إلى الدليل الذي يفيد في كشف الجريمة، فضلا عن إمكانية تعارض إجراءات التحقيق مع مبادئ قانونية مثل مبدأ قرينة البراءة والحق في الخصوصية، واشكالية الاثبات الجزائي في الجرائم المعلوماتية وهذا ما سنتطرق إليه في المطلب الأول، كما يساهم الضحية نفسه في إعاقة سير إجراءات التحقيق، وهذا ما سنتناوله في المطلب الثاني

المطلب الأول: انعكاس خصوصية الجرائم المعلوماتية على إجراءات التحقيق

رغم وجود جرائم معلوماتية فقد تقف خصوصيتها كحجر عائق أمام السلطات المكلفة بالتحقيق في تمحيص الأدلة والوصول إلى الحكم القضائي.

أولا: خصوصية الجريمة أنها عابرة للحدود

ساهمت الانترنت في ذلك بطبيعتها العالمية، فكل نشاط اجرامي يتم من خلالها إلا ويحمل هذه الصفة، خاصة في قضايا الجريمة المنظمة، مثل الإرهاب، تبيض الأموال والاتجار بالمخدرات، فيقوم المجرمون عبر شبكات الأنترنت بتطوير آليا معقدة لمثل هذه النشاطات عبر التحويل الإلكتروني من بنك إلى آخر أو من بلد إلى بلد آخر، يصعب من خلالها تتبع هذه العمليات على الشبكة، على غرار ضعف التشريعات القانونية في مثل هذه الجرائم المعقدة.[1]

تثير هذه الخاصية العديد من المشاكل المتعلقة بالسيادة، الاختصاص القضائي، والقانون الواجب التطبيق، وفي قبول الأدلة المتحصل عليها في دولة ما أمام دولة أخرى، على غرار متطلبات التحقيق، الملاحقة والتفتيش والضبط.

[1] صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، الموسم الجامعي 2013/2012، ص 127.

فقواعد القانون الجنائي (بشقيه الموضوعي والإجرائي)، تخضع في تطبيقها من حيث المكان إلى المبدأ المعروف بالإقليمية، وهو خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، إذ تكون محاكمها صاحبة الولاية في الدعاوى الناشئة عنها، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي، في المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقا لحدودها المعترف بها في القانون الدولي، إلا في حالات استثنائية اقتضتها المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام العابر للدول.[2]

فمن بين القضايا المثارة في هذا الخصوص قضية الاعتداء على سيتي بنك (City Bank) في نيويورك بواسطة vladimirlevin وأعضاء من المافيا الروسية وبستراسبورغ، قد خلق مشكلة قانونية لمكتب التحقيقات الفيدرالي، حيث كان على المحققين فحص نظام البنوك في سبع دول مختلفة، أين تم الإيداع الالكتروني للنقود، وكان تطبيق أوامر التفتيش والتتبع الزمني لهذا الحدث تحديا بالنسبة لمعظم المحققين، وتم القبض على المتهم وحُكم عليه بالسجن لمدة ثلاث سنوات وإلزامه بدفع مبلغ 240 ألف دولار لسيتي بنك.[3]

وحدث أن قام المبرمج الإنجليزي Thompson RN يعمل في بنك الكويت بالتلاعب في معطيات نظام الحاسب الآلي للبنك، عن طريق الخصم من أرصدة العملاء والايداع في حسابه الخاص ثم بعد عودته لبلاده طلب من البنك تحويل الحساب الخاص إلى عدة حسابات في إنجلترا، حيث حكم عليه بالسجن بتهمة الحصول على أموال الغير بالاحتيال، فقام بالطعن على الحكم مستندا إلى عدم اختصاص القضاء الإنجليزي، فسلوك السحب والايداع كان بالكويت، غير أن محكمة الاستئناف رفضت طعنه على أساس أن النشاط الاجرامي للمتهم لم يكتمل إلا بعد طلب التحويل ثم حصوله على الأموال محل النشاط الاجرامي، وبالتالي فالمكافحة تتطلب تعاونا كثيفا بين الدول وتوافقا كبيرا بين تشريعاتها.[4]

إن اختلاف وتباين المعايير الوطنية فيما يتعلق بتحديد الاختصاص، يصعّب من عملية البحث والتحري ويفضي إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم، وحتى ولو افترض إيجاد حل

---

[2] عبد الحليم بن بادة، اجراءات البحث والتحري عن الجريمة المعلوماتية – الخصوصية والأركان، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 23، المجلد، جوان 2015، ص 94.

[3] طاهر محمود أبو القاسم، الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، 2019، ص 159.

[4] محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، المجلد 01، العدد 01، الجلفة، 2009، ص 376.

لهذه المشكلة من الزاوية القانونية، فإنها تظل تصطدم بعقبات عملية بالنظر إلى الإجراءات المعقدة والطويلة التي الواجب متابعتها لمحاكمة الجاني، عند ارتكاب الجاني إحدى هذه الجرائم، بالنظر إلى إقامته وجنسيته والبلاد التي تتم فيها محاكمته، الأمر يسري على تنفيذ الأحكام الصادرة بالخارج، وما يتعارض مع مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد مرتين وكذلك تسليم الوطنيين – مثال عن ذلك قضية الهاكر الجزائري حمزة بن دلاج – [5]

ثانيا: خصوصية عدم ترك الجريمة المعلوماتية لأثر خارجي

إذ أن الجريمة المعلوماتية لا تترك جثث وقتلى ولا آثار دمار، أو عنف مثل ما هو في الجرائم التقليدية، فالجريمة المعلوماتية باستخدام تقنيات تكنولوجية عالية تعتمد على نقل البيانات والمعلومات المعالجة آليا بالنبضات الالكترونية.[6]

بالإضافة إلى أن مرتكب الجريمة المعلوماتية يلجأ في غالب الأحيان إلى بذل أقصى احتياطاته لعدم ترك أثار لفعلته، ويتعلق الأمر في هذا على الجرائم التي تتم دون ان يشعر بها القائمون على تشغيل الأجهزة المعلوماتية، مثل برامج التجسس والتي تتم ببرامج خاصة، دون علم أو دراية مستعملي المعلوماتية ببرامجها، فيساهمون بجهلهم في مساعدة مرتكبي تلك الجرائم بطريقة غير مباشرة، من خلال تثبيت هذه البرامج أو البرامج الضارة بالجهاز، والتي تكون عادة كروابط مفخخة، بالإضافة على كوننا نتعامل أمام عالم افتراضي مسرحه هو المواقع والأجهزة الالكترونية التي يمكن فيها الحذف والزيادة و التعديل والنقصان، بخلاف الوثائق والمستندات الملموسة، تقول الدكتورة نهلا عبد القادر مومني بأن الجريمة المعلوماتية:" تتميز بصعوبة اكتشافها وإذا اكتشفت فإن ذلك من باب الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية "[7]

ثالثا: خصوصية ضخامة وحجم البيانات والملفات

إذا كانت سلطة التحقيق في الجرائم التقليدية أمم مسرح الجريمة واضحة ومعلومة المعالم، فإنهم في حالة الجريمة المعلوماتية سيكونون أمام عالم افتراضي لا متناهي متباعد الأطراف متصل ببعضه البعض، من

[5] عبد الحليم بن بادة، المرجع السابق، ص 95.
[6] طاهر محمود أبو القاسم، المرجع السابق، ص 158.
[7] نهلا عبد القادر المومني، المرجع السابق، ص 54.

حيث الكم الهائل والضخم من البيانات والمعطيات، أمام هذا وقلة الإمكانيات المادية والبشرية، فإنه من الصعب بمكان تحديد الملفات والبيانات المجرمة، مما يؤدي في الغالب إلى اصطدام مهمة الاكتشاف والتحقيق بحق الفرد في الخصوصية الشخصية من جهة، ومن جهة أخرى في المسار الصحيح في التحقيق في المعلومات المحصل عليه من الجريمة المعلوماتية، في ظل غياب آليات لفرز هذه المعلومات.[8]

كما أن البحث في ملفات الحاسب الآلي تقابله صعوبات كثيرة وغير عادية، حيث أن الجاني باستطاعته تحريك الملفات من جهاز لآخر بسرعة فائقة واخفائها في مساحة ضئيلة جدا على ذاكرة الحاسوب، أو تخزينها في سيرفر (serveur) يقع في دولة ذات اختصاص قانوني مختلف في تجريم هذه الجرائم، فضلا عن صعوبة تتبع المعلومات داخل الجهاز كدليل تسعى الجهات الأمنية لملاحقته وذلك بسبب وجود كم هائل من المعلومات والبرامج والملفات المخزنة التي يتعين فحصها ولها ارتباط بالجريمة لكشف أدلة الجريمة، تكمن الصعوبة إما في طبيعة المعلومات أو في نقص الخبرة الفنية.[9]

رابعا: خصوصية المجرم المعلوماتي

من الصعوبات التي تواجه السلطات المختصة في التحقيق قدرة الجاني على محو الأدلة القائمة ضده، أو تدميرها في زمن قصير.[10]

حيث يسعى المجرمون الالكترونيين إلى إخفاء جرائمهم وتمويهها، بإحداث أعطال أو أخطاء في أنظمة التشغيل أو إزالة أثار الجريمة عن طريق التلاعب بقواعد البيانات والقوائم في جهز الحاسوب والبرامج، لاسيما ما يتعلق بالتخزين الالكتروني غير المرئي والبيانات الكثيرة وهي مكتوبة بلغات رقمية – البايثون مثلا – وهي لغة لا تفهمها إلا الآلة والمبرمجون، باستخدام رموز وتشفيرات، إذ قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف لأفعالهم، على غرار إخفاء الهويّة وانتحال شخصيات أخرى.

[8] سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 98.

[9] طاهر محمود أبو القاسم، المرجع السابق، ص 159، 160.

[10] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الطبعة الأولى، عمان، 2011، ص 223.

وما يزيد تعقيدا في مجال البحث والتحقيق المعلوماتي، استخدام المجرم المعلوماتي أسلوب التخفي غبر الشبكة من خلال استعمالهم ما يُعرف بالشبكة الخفية للنت أو يصطلح عليه باللغة الإنجليزية " The Darknet "،[11] فالمستعمل لهذه الشبكة يظهر تارة متصلا من الولايات المتحدة الأمريكية، وتارة من اليابان وتارة من انجلترا، وهو ما يجعل من أمر اقتفاء أثر المجرم المعلوماتي غاية في التعقيد إن لم يكن مستحيلا.[12]

خامسا: خصوصية الأصالة في الدليل الالكتروني

فالدليل الالكتروني له طابع افتراضي لا يرقى إلى مستوى الأصالة بالنسبة للدليل المادي الذي يعبر عن وضع مادي ملموس، في حين أن الدليل الرقمي يقوم على النظام الثنائي، ويعتمد على رقمين هما الواحد والصفر لتمثيل أي عدد (1. 0)[13] وهو عبارة عن نبضات متواصلة الايقاع تستمد حيويتها وتفاعلها من الطاقة، وقد أثارت مسألة الأصالة في الدليل الالكتروني إشكالية مدى قبولها في مجال الإثبات الجنائي على اعتبار افتقادها للمظهر المادي للملموس.[14]

المطلب الثاني: الضحية ودوره في إعاقة سير التحقيق في الجرائم

يعد الضحية في الجريمة المعلوماتية هو كل من أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع للتقنيات الالكترونية الرقمية.[15]

ويرجع زيادة ارتكاب الجريمة المعلوماتية، خاصة جرائم السب والشتم، والابتزاز الالكتروني، وسرقة المعلومات الشخصية والاعتداء على حرمة الحياة الخاصة، إلى قلة خبرة الضحايا، وكشفهم لبعض المعلومات الشخصية عن حياتهم اليومية واستعمالاتهم المفرطة لوسائل التواصل الاجتماعي.

---

[11] شبكة موازية لشبكة الأنترنت العادية، وقد ظهرت للوجود أول مرة سنة 1970في الولايات المتحدة الأمريكية ، لأجل تأمين المعلومات العسكرية المتنقلة عبر شبكة، "ARPANET " ثم دخلت عالم المعلوماتية سنة 2002، يكفي لولوج الشبكة الخفية والإبحار عبرها تحميل تطبيق معلوماتي متوفر على شبكة الانترنت، و تفعيله على جهاز الحاسوب، و لعل أشهره هو تطبيق، " TOR" "The Onion Router " يعمل على هذا الأخير على تغيير العنوان الإلكتروني للحاسوب " IP" المتصل بالشبكة الموازية الخفية عدة مرات في الساعة الواحدة.

[12] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في الحقوق تخصّص – قانون العقوبات والعلوم الجنائية، جامعة باتنة، كلية الحقوق والعلوم السيّاسية، قسم الحقوق، الجزائر 2015، 2016، ص 287.

[13] طه زروقي، بنية الآلة، محاضرات وتمارين ألقيت على طلبة السنة الأولى، كلية الاعلام الآلي جامعة البويرة، الجزائر، 2021، ص 15.

[14] عائشة بن قارة، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، الطبعة الأولى، مصر، 2010، ص 252.

[15] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، الطبعة الأولى، القاهرة، مصر، 2009، ص 158.

كما يؤدي امتناع الضحايا عن التبليغ أو ما يصطلح عليه بمصطلح " الرقم الأسود " للجرائم المعلوماتية سببا في عدم مباشرة اجراءات التحقيق في الجرائم المعلوماتية، ويرجع ذلك إلى:

- الجهل بالقانون من حيث عدم الإدراك بوجود نصوص تُجرم وتعاقب على أشكال الجرائم المعلوماتية، سواء فيما يتعلق بعلمه بأن هذه الافعال التي يعاقب عليها القانون، أو بجهله بالإجراءات الواجب اتباعها كمعرفة الجهة التي يلجأ إليها للتبليغ أو في كيفية التبليغ.
- امتناع الشركات والمؤسسات عن التبليغ خوفا على سمعتها وكيانها، أو أن يكون ذلك فرصة للمجرمين المعلوماتيين في معرفة ثغرات ونقاط ضعف النظام المعلوماتي للمؤسسة من جهة ثانية، كما قد تكون الشركة ضالعة في جرائم الكترونية ضد شركات منافسة لها في السوق، فتلجأ إلى توظيف مهندسين في التجارة الالكترونية أو في المعلوماتية من أجل المحافظة على الميزة التنافسية في السوق من خلال معرفة الخطط الإستراتجية الاستثمارية أو التنافسية للشركات الأخرى من خلال قرصنة حواسيبها أو هواتف مدراءها.
- تخوف المؤسسات التجارية من استغراق فترة زمنية طويلة في التحقيق، مع احتمالية احتفاظ جهات التحقيق بأجهزة الحاسوب مما يؤثر سلبا على سير العمل بتلك الشركات والمؤسسات.
- وتمتنع المؤسسات المالية والبنوك، عن التبليغ، خشية اهتزاز ثقة المتعاملين معها، وبالتالي سحب ودائعهم واستثماراتهم، ولا يقف الأمر عند هذا الحد، بل يتعدى ذلك إلى الامتناع عن تقديم أي مساعدة لجهة التحقيق أثناء علمها بالجريمة، الامر الذي يشكل صعوبة في اكتشاف الجريمة من جهة واثباتها من جهة أخرى.[16]

ففي أحدى الوقائع المماثلة تعرض بنك **Marchant Bank City** في بريطانيا إلى سرقة 08 مليون جنيه استرليني من أحد أرصدته إلى رقم حساب في سويسرا، تم بعد ذلك ضبط الفاعل متلبسا بسحب المبلغ المسروق، وبدلا بالتبليغ عن الجريمة ومتابعة الجاني قضائيا، قام البنك بدفع مليون جنيه له شرط التزام الفاعل بالصمت وعدم الإدلاء بأي تصريح أو حتى أن يُعلم عن جريمته، وإعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام أمن الحاسوب الرئيسي أو المركزي للبنك.[17]

[16] فهد عبد الله العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الطبعة الأولى، الاسكندرية، مصر، 2016، ص 130.
[17] حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، ط 01، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، ص 34.

- خوف الموظفين وفي حال الإبلاغ عن الجرائم المعلوماتية، من اتخاذ الجهة المسئولة عن تشغيل النظام المعلوماتي من حرمانهم من خدمة الانترنت أو تحديد المواقع التي يسمح لهم بزيارتها[18]، كما قد يكون الموظف متورطا لإحدى الجرائم المعلوماتية – مهندس في البرمجيات – تحت غطاء المؤسسة أو الشركة التي يعمل فيها، فبتبليغه عن الجريمة قد يكون التحقيق ضده أثناء تفتيش أو البحث في الجريمة المبلغ عنها.

وقد اجتهد الفقه في وضع مجموعة من التدابير للحد من تضخم الرقم الأسود للجريمة المعلوماتية، غير أن تنفيذها على أرض الواقع مرتبط بكفاءة وقدرة جهاتها الأمنية المتخصصة في رصد هذه الجرائم من جهة ومن جهة أخرى على وعي المواطنين، ومن هذه التدابير:

- تكوين رجال أمن محترفين في مجال الأمن المعلوماتي وبرامج وعلوم الحاسوب.
- تخصيص وحدات أمنية أو ما يسمى بشرطة أو بوليس الجريمة المعلوماتية، تكثف من جهودها ونشاطها وتواجدها في رصد الاعتداءات الالكترونية على مستوى البنوك والمؤسسات التجارية والمالية ومصالح البريد والهاتف، على غرار أسواق الحاسوب والبرمجيات باعتبارها ملتقى مجرمي المعلوماتية.[19]

[18] حسين ربيعي، المرجع السابق، ص 292.

[19] عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكومبيوتر والتزوير، دارسة معمقة في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، الطبعة الأولى، مصر،2002، ص 72، 73.

الفصل الثاني

الحق في الخصوصية المعلوماتية وأوجه حمايتها

عمدت المواثيق الدولية والاقليمية إلى الاعتراف بالحق في الحياة الخاصة في العديد من المواضيع، ليصبح في مصاف حقوق الإنسان، التي اتفقت غالبية الدساتير في الدول الحديثة على احترامها، وجاءت التشريعات العقابية للتصدي لمختلف الانتهاكات التي يتعرض لها هذا الحق، بتجريم السلوكيات التي تنتهك حرمة الحياة الخاصة، أو تمس بإحدى عناصرها، سنتناول في المبحث الأول مفهوم الحق في الخصوصية، من خلال تعريف الفقهي للحق في الخصوصية في المطلب الأول، ونطاق الاعتداء على الحق في الخصوصية المعلوماتية في المطلب الثاني، أما في المبحث الثاني فسنعمد للحديث عن أوجه الحماية الجزائية للحق في الخصوصية المعلوماتية، من خلال الحديث عن حماية سرية المراسلات والاتصالات الالكترونية في المطلب الأول، أما المطلب الثاني فخصصناه للحديث عن حماية الأشخاص الطبيعيين في مجال المعطيات المعلوماتية.

المبحث الأول: مفهوم الحق في الخصوصية المعلوماتية ونطاقها

إن المعاملات التي يقوم بها المستهلك على شبكة الأنترنت قد تحمل معلومات تتعلق بحياته الخاصة كاسمه وكنيته ومقر إقامته وطبيعة عمله، وأرقام حساباته البنكية وغير ذلك، وغير ذلك مما لا يطلع عليه غيره، وجاءت التشريعات والتنظيمات تمنع وتعاقب كل من يعتدي على هذه الخصوصية، ولمعرفة أهمية هذا الحق لابد من فهم ماهية هذا الحق، ونطاق الاعتداء عليه.

المطلب الأول: تعريف الحق في الخصوصية المعلوماتية

يعتبر حق الانسان في الخصوصية عموما جوهر الحقوق والحريات الشخصية، ويعد الاعتراف بهذا الحق مجرد كاشف له وليس منشئ له، كونه من الحقوق اللصيقة بالإنسان، ويعد هذا الحق من الحقوق المثيرة للجدل بين فقهاء القانون الوضعي، وقد كان هناك اختلاف حول مفهومها خصوصا في ظل التطورات والتعقيدات التي طرأت وتطرأ على صعيد واقع الأفراد بغض النظر عن المراكز القانونية التي يحتلونها والتي تتغير وفقها مقومات الحق في الخصوصية، لذلك لابد من الالتزام بالموضوعية عند إخضاعه لأي تعريف.[1]

أولا: التعريف الفقهي للحق في الخصوصية

ويعود الفضل في توجيه الانتباه لمفهوم الخصوصية إلى المؤلفين الامريكيين في هذا المجال هما:

الأول: الخصوصية والحرية Privacy and Freedom لصاحبه Alan Westin سنة 1967، الذي عرف خصوصية المعلومات على أنها: " حق الفرد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين." حيث أن مفهوم الخصوصية يتمحور حول الحد من سيطرة الحكومة على الاستقلال الجسدي للأفراد. لكن مع موجة التطور التقني، تصاعدت التحديات التي تواجه خصوصية الأفراد وتغير مفهوم الخصوصية بناء على ذلك.[2]

[1] رامز محمد عمار، نعمت عبد الله مكي، حقوق الإنسان والحريات العامة، الطبعة 01، 2010، من دون دار نشر، ص 347.

[2] رؤى سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية، مشروع رسالة مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في تخصص الأنظمة، جامعة الملك عبد العزيز، المملكة العربية السعودية، مجلة كلية الدراسات الاسلامية والعربية بدمنهور العدد السادس الاصدار الثاني، الجزء الأول 2021، ص 1053.

وقد ظهرت الخصوصية في الأنظمة قانونية كوسيلة لتحديد الخطوط الفاصلة بين حق الفرد المطلق وحق المجتمع بالتعرض لشؤونه، وفي أنظمة قانونية أخرى كانت الخصوصية هي الحرية في مواجهة كل اعتداء أو انتهاك،[3] فهذا التباين كان سببا وعاملا في نشوء العديد من التعريفات للحق في الخصوصية، والتي كانت إما تتوسع في تعريفها إلى درجة اقترانها بالحرية عموما، أو تعمد إلى تضييق نطاقها لتصل إلى حد الحق في العزلة والسرية وفي أن يُترك وحيدا.[4]

الثاني: الاعتداء على الخصوصية The Assult On Privacy لمؤلفه Raphael Miller Arthr سنة 1971، والذي عرفها على أنها: " قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم." حيث يرى أن أجهزة الكمبيوتر وبنوك البيانات والملفات تسهم بشكل بارز في مجال حماية الخصوصية بعيدا عن التعميمات والأفكار المبتذلة المليئة بالعاطفة والبعيدة عن المنطق فيما يخص التعامل مع الحق في الخصوصية.[5]

إلى جانب الدراسة التي قام بإعدادها Michel James سنة 1994 تحت إشراف اليونسكو بعنوان الخصوصية وحقوق الانسان Privacy And Human Rights، والتي تعد إحدى أوسع الدراسات بشأن المسائل المتصلة بالخصوصية وحقوق الانسان في ضوء التطورات التقنية الحديثة، حيث استعرض الصعوبات والتباينات الثقافية في استخدام المصطلح واختلاف المفهوم القانوني للخصوصية في المعلومات بين النظم القانونية.[6]

وعلى الرغم من اختلاف الفقهاء في تعريف الحق في الخصوصية المعلوماتية، إلا أن النقاط المشتركة بينهم تتمثل في السعي وراء الحد من السلطة الممنوحة للحكومات أو الأفراد فيما يتعلق بعملية الاطلاع على البيانات الشخصية للأفراد واستعمالها بغض النظر عن الأسباب، مع تسليط الضوء على النقص التشريعي القانوني حول حماية الأفراد من الانتهاك الشخصي الالكتروني من مخاطر التقنية بشكل عام.[7]

---

[3] بولين أنطونيوس أيوب، الحامية القانونية للحياة الشخصية غي مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي، الطبعة 01، 2009، ص 09.

[4] سعيداني نعيم، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في القانون، قانون جنائي، جامعة باتنة 01، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020،2021، ص 13.

[5] صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار، عنابة، كلية الحقوق والعلوم السياسية المجلد 24، العدد 02، 2018، ص ص 123-145، ص 126.

[6] صبرينة جدي، المرجع نفسه، ص 126.

[7] عائشة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون، المجلد 2، العدد 6، المغرب، 2016، ص 75.

ومن أهم التعريفات التي ساقها الفقه للخصوصية المعلوماتية: " أنها قدرة الأفراد في السيطرة على معلوماتهم الشخصية وحريتهم أن تضل في سرية "، أو هي:" حق الفرد في أن يقرر متى وكيف وإلى أي مدى يمكن تبادل المعلومات التي تخصه مع الآخرين "، أو هي: " رغبة الشخص في التحكم أو على الأقل التأثير بشكل كبير في كيفية التعامل مع بياناته الشخصية "[8]

كما عرفت على أنها: " قدرة الشخص على التحكم في سرية بياناته ومعلوماته الشخصية والتحكم كذلك فيمن يمكنهم الوصول إلى هذه المعلومات. سواء كانوا أفراد آخرين أو حكومات أو حواسيب "، وعرفها آخرون بأنها: " حق الأفراد أن يحددوا لأنفسهم متى وكيف وإلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين، وبأن يضبطوا عملية جمع المعلومات الشخصية عنهم، وكيفية معالجتها آليا وحفظها وتوزيعها واستخدامها في صنع القرار الخاص بهم أو المؤثر فيهم."[9]

من خلال هذه التعاريف يبدو واضحا أن الحفاظ على حق الشخص في خصوصيته المعلوماتية يقوم بالأساس على حماية البيانات الشخصية له، إذ لا يمكن التفريق بين المصطلحين، فالخصوصية المعلوماتية تعني بشكل أساسي المحافظة على السرية منع التدخل فيما يعتبر حميمية الشخص وأسراره عبر حماية بعض البيانات ذات الطبع الشخصي، بشكل يمنع انتشار المعلومات التي تكشف عن الحياة الخاصة وتجعلها عرضة للانكشاف سواء عند عملية جمع المعلومات أو عند تخزينها أو عند معالجتها.[10]

يمكننا القول إذن أن الخصوصية المعلوماتية هي حماية البيانات الشخصية، لكن الخصوصية ليست حماية البيانات ذلك أن هذه الأخيرة هي فرع من الخصوصية تتعلق بمواجهة الاعتداءات على البيانات الشخصية، وتنظم الحق في حماية هذه البيانات وسيطرة صاحبها عليها في مواجهة القوى الرقابية المحتملة لأنظمة الكمبيوتر من خلال قواعد معينة تحكم جمع ومعالجة البيانات الشخصية في عصر المعلوماتية،[11] وبالتالي فإن هناك ترادفا بوجه عام قائم بين اصطلاح الخصوصية المعلوماتية وحماية البيانات الشخصية وليس بين الخصوصية وحماية البيانات.

---

[8] فهد عبد العزيز سعيد، دور تقنية المعلومات في حماية خصوصية البيانات، مركز التميز لأمن المعلومات، المقالات العلمية، جامعة الملك سعود، الرياض، 2010، ص 02.

[9] سوزان عدنان، انتهاك حرمة الحياة الخاصة عبر الأنترنت، مقال منشور في مجلة جامع دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث، 2013، ص 433.

[10] منى الأشقر، محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، الطبعة الأولى، 2018 بيروت، لبنان، ص 22.

[11] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الاتفاقي والقانون الوطني، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2016، ص 41.

ويرجع استخدام اصطلاح الخصوصية منفردا دون إلحاقه بالبيانات في البيئة الالكترونية للدلالة على حماية البيانات الشخصية، فيرجع إلى أن تعبير الخصوصية شاع بهذا الوقع في ظل تزايد مخاطر التقنية إلى حد ارتباطها بهذه المخاطر في الاستخدام، كأنه ينحصر في نطاقها وبيئتها ذلك أن أشد ما يمكن ان يمثل توغلا، على هذا الحق وانتهاكا له هي الوسائل التقنية ومخاطر المعالجة الآلية للبيانات الشخصية.[12]

يمكننا القول إذن أن الفقه قد ساهم في إثارة مسائل نظام خصوصية المعلومات وتوضيح ملامحه، في ظل التطورات الحاصلة في مجال تقنية المعلومات، وتحديدا إنشاء بنوك المعلومات وإجراء عمليات المعالجة والتحليل للبيانات الشخصية بواسطة الكومبيوتر.[13]

وكخلاصة للدراسات الاكاديمية، فإنه قد جرى التعامل مع الخصوصية من حيث مفهومها كحق لمنع إساءة الحكومة والإدارات وحتى الشركات الخاصة للبيانات الشخصية التي يصار إليها معالجتها آليا أو الكترونيا، أو تقييد استخدامها وفقا للقانون فقط.[14]

لهذا الأساس يمكن القول أنه إذا كان الحق في الخصوصية بمفهومه التقليدي يعني حق الفرد في أن يقرر بنفسه متى وكيف وإلى أي حد يمكن للغير أن يطلع على شؤونه الخاصة مثلم سبق إيراده، وفي ظل الاعتداءات التي تطال الحياة الخاصة بواسطة التقنيات المعلوماتي الحديثة فأصبح يعني حق الفرد أن يقرر بنفسه متى وإلى أي مدى يمكن أن تصل بياناته الشخصية للآخرين.[15]

ثانيا: موقف المشرع الجزائري من الحق في الخصوصية

يعتبر المشرع الجزائري من بين التشريعات التي توجهت نحو الاعتراف بالحق في الخصوصية بمفهومه الشامل، واعتباره حقا مستقلا شأنه شأن المشرع الفرنسي، إذ يرى أن الحماية المباشرة للحق في الحياة الخاصة تعد مكملة للحماية غير المباشرة والموجودة قبلها في نصوص قانونية أخرى.

[12] منة تركي الموسومي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلكين، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية 2013، ص 5.

[13] سعيداني نعيم، المرجع السابق، ص 109.

[14] بولين أنطونيوس أيوب، المرجع السابق، ص 57.

[15] محمد حسين منصور، المسؤولية الالكترونية، الطبعة الأولى، منشأة المعارف الإسكندرية، مصر، 2006، ص 59.

ويعد الدستور في مقدمة النصوص القانونية التي اعترفت بالحق في الحياة الخاصة في التشريع الجزائري، ففي أول دستور جزائري سنة 1963، لا نجد نص صريح حول الحياة الخاصة، إلا نص المادة 11 منه التي تمنح الجزائر فيها موافقتها للإعلان العالمي لحقوق الانسان، الذي تتمن المادة 12 منه على عدم جواز تعرض أي أحد لتدخل تعسفي في حياته الخاصة، ثم جاء دستور 1976،[16] أين نص المشرع على الحياة الخاصة في المادة 49 فقرة 01، حيث نصت على أنه:" لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه يحميها القانون"، بالإضافة لنص المادة 60 منه التي نصت على: " يمارس كل مواطن جميع حرياته في إطار احترام الحقوق المعترف بها للغير في الدستور ولاسيما احترام الحق في الشرف وستر الحياة الخاصة ... "، وفي دستور 1996[17] اهتم المشرع الدستوري أيضا بالحق في الحياة الخاصة، ورد فيه نصين أولهم في المادة 39 ضمن عنوان الحقوق والواجبات، والتي نصت على أنه: " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه يحمها القانون " والنص الثاني يتمثل في المادة 63، والتي تنص على أنه: " يمارس كل واحد جميع حرياته في إطار احترام الحقوق المعترف بها للغير، لاسيما احترام الحق في الشرف وسر الحياة الخاصة .... "، وبصدور دستور مارس 2016،[18] اعترف المشرع الجزائري لأول مرة في المادة 46 منه بالخصوصية المعلوماتية، أين نص صراحة على حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

أما بالنسبة للتشريع العادي فيعد المرسوم رقم 88-13 المؤرخ في 1988/07/04 المنظم للعلاقة ين الإدارة والمواطن،[19] أول نص قانوني ورد فبه مصطلح الحياة الخاصة، إذ نصت المادة 11 منه على أنه: " لا يجوز للإدارة المسيرة أن تنشأ أو تسلم أي وثيقة أو أي خبر(معلومة) مهما يكن سندها في ذلك. إذا كانت الوثيقة والخبر يتصلان بحياة الفرد الخاصة أو يرتبطان بحياة الفرد الخاصة أو يرتبطان بوضعيته الشخصية بصرف النظر عن أحكام المادة 10 من هذا القانون، ما لم يرخص بذلك التنظيم المعمول به أو تكون ثمة موافقة من المعني.

[16] أمر 76-97 مؤرخ في 22 نوفمبر 1976 يتضمن إصدار دستور الجمهورية الجزائرية الديموقراطية الشعبية، الجريدة الرسمية رقم 94، الصادرة بتاريخ 24 نوفمبر 1976.

[17] مرسوم رئاسي رقم 96-438 مؤرخ في 07 ديسمبر 1996 يتعلق بإصدار نص تعديل الدستور، المصادق عليه في استفتاء 28 نوفمبر 1996ن الجريدة الرسمية رقم 76، الصادرة بتاريخ 08 ديسمبر 1996.

[18] قانون رقم 16-01 مؤرخ في 06 مارس 2016 يتضمن التعديل الدستوري، الجريدة الرسمية رقم 14، الصادرة بتاريخ 07 مارس 2016.

[19] مرسوم 88-131 مؤرخ في 04 يوليو 1988 ينظم العلاقة بيم الإدارة والمواطن، الجريدة الرسمية رقم 27، الصادرة بتاريخ 06 يوليو 1988.

وفي قانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها،[20] أين نصت الفقرة السابعة من المادة 04 منه على ضرورة أن تكون الترتيبات التقنية الموضوعة موجهة فقط وحصريا لتجميع وتسجيل المعطيات ذات الصلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها وعدم المساس بالحياة الخاصة للغير.

ثم جاء القانون 15-03 المؤرخ في 2015/02/01 المتعلق بعصرنة العدالة،[21] أن بدأ المشرع الجزائري يولي أهمية بالغة بالمصطلح الخصوصية ويتعلق الأمر بمسألة الخصوصية المعلوماتية، لينص في المادة 05 من هذ القانون على وجوب أن تتواجد على التراب الوطني كل المعطيات والمعطيات ذات الطابع الشخصي التي تم جمعها من طرف مؤدي خدمات التصديق الالكتروني، على غرار القانون 16-03 المؤرخ في 2016/06/19 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص[22].

ويعد القانون 24-06 المؤرخ في 2024/04/28 المعدل والمتمم لقانون العقوبات،[23] النص القانوني الذي وفر من خلاله المشرع الجزائري حماية جزائية فعلية ونوعية للحق في الحياة الخاصة، حيث نصت المادة 303 مكرر منه على أنه: " يعاقب بالحبس من شهر إلى 03 سنوات وبغرامة من 50.000 دج إلى 100.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت."

فبالرغم من هذا الزخم الكبير من النصوص القانونية التي صاغها المشرع الجزائري بخصوص الحياة الخاصة، إلا أنه لم يضع تعريفا لهذا الحق في أي من هذه النصوص، ويبدو أن هذا السكوت مرده الطبيعة المعقدة لهذا المصطلح، فلا يمكن حصره في تعريف واحد يغطي كل جوانبها، وذلك بسبب تعدد وتنوع الأشكال التي تغطيها هذه العبارة، فضلا عن أن المفهوم يعد نسبيا، فيختلف باختلاف الأخلاق وتطورها فما كان يعتبر خارج الحياة الخاصة في زمن ما، لم يعد اليوم كذلك ودخل في حيز

[20] القانون رقم 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. جريدة رسمية عدد 47، الصادرة بتاريخ 16 غشت 2009

[21] القانون رقم 15-03 المؤرخ 1 فبراير سنة 2015، المتعلق بعصرنة العدالة، الجريدة الرسمية رقم 06، الصادرة بتاريخ 10 فبراير 2015.

[22] القانون 16-03 المؤرخ في 2016/06/19 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، الجريدة الرسمية رقم 37، الصادرة بتاريخ 22 يونيو 2016.

[23] قانون رقم 24-06 مؤرخ في 28 أبريل 2024، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية رقم 30، الصادرة بتاريخ 10 أبريل 2024.

الخصوصية، كما أن مسائل كانت دقائق الحياة الخاصة أصبحت اليوم مسائل عادية، وعليه يكون من الصعب وضع تعريف واحد للحق في الخصوصية يصلح تطبيقه على الكافة وعلى مر الأزمنة.[24]

المطلب الثاني: نطاق الاعتداء على الحق في الخصوصية المعلوماتية

يرتبط مصطلح الخصوصية بشكل جوهري مع حماية البيانات والمعلومات التي تكشف عن هويته وحياته الخاصة وحالته الصحية أو الاجتماعية، والمتداولة عبر الأنترنت، والممثلة تمثيلا رقميا، وتسمى بالبيانات الشخصية، وهي المحل الذي ينصب عليه نطاق الحق في الخصوصية الرقمية.

أولا تعريف البيانات الشخصية

يشار لها أيضا بالمعطيات ذات الطابع الشخصي، أو البيانات الإسمية، وهو ما يصطلح عليه باللغة الانجليزية Personal Data، وباللغة الفرنسية Les Données Personnelles، والذي يقصد به من الناحية الفنيّة، كل تمثيل يمكن أن تُخزن فيه المعلومة، والذي يمكن أن يكون نصا أو جدولا أو رسما بيانيا، كما يمكن أن يكون موديلا أو لونا أو إشارة أو أية رموز أخرى، تكون ذات دلالة ومعنى لدى معالج المعلومة.[25]

ومن الناحية القانونية فقد أورد المشرع الجزائري تعريفا للبيانات الرقمية، والذي عبر عنها بـ: " المعطيات المعلوماتية " وعرفها 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"،[26] أما البيانات الشخصية فلم يورد لها تعريفا خاصا بها، حيث عرفتها اللجنة الوطنية للمعلوماتية والحريات (CNIL) [27] بأنها:" كل معلومة تتعلق بشخص طبيعي معروف الهوية أو ممكن التعرف على هويته بصفة مباشرة أو غير مباشرة بالرجوع إلى رقم تعريفي أو إلى واحد أو مجموعة من العناصر التي تخصه .... " [28]

---

[24] نويري عبد العزيز، الحماية الجزائية للحياة الخاصة دراسة مقارنة بين القانون الجزائري والفرنسي، دار هومه للطباعة والنشر والتوزيع، الطبعة الأولى، الجزائر، 2015، ص 63.

[25] كيث دفلين، الإنسان والمعرفة في عصر المعلومات، ترجمة: شادن اليافي، مكتبة العبيكان، السعودية، ط 1، 2001، بتصرف

[26] القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47.

[27] Abréviation du : Commission Nationale De L'informatique Et Libérés

[28] المادة الثانية من قانون 06 جانفي 1978 المتعلق بالمعلوماتية، الملفات والحريات.

ثانيا: أنواع البيانات الشخصية

من خلال التعاريف السابقة، فإن البيانات الشخصية تنقسم إلى نوعين أساسيين: البيانات المحددة للهوية، والبيانات الخاصة.

1- البيانات المحددة للهوية

بالنظر إلى الوسائل والتقنيات المعلوماتية المتعلقة بتحديد هوية الأشخاص، نجد أن البيانات المحددة للهوية تنقسم إلى نوعين من البيانات: يتمثل النوع الأول في الحروف والأرقام والرموز، والتي تتمثل في كلمات المرور التي تسمح أو تمنع المستخدم من الولوج إلى الحاسوب أو قاعدة البيانات أو الولوج إلى مختلف أنواع البريد أو مواقع التواصل الاجتماعي، أو تسجيل الدخول إلى منتدى أو حساب شخصي على موقع إلكترون، فيما يتمثل النوع الثاني في القياسات الحيوية، على غرار بصمة الأصبع، بصمة القزحية، البصمة الصوتية، بصمة أبعاد الكف، خط اليد (التوقيع)، بصمة الوجه، .... إلخ[29]

2- البيانات الشخصية الخاصة

يتعلق هذا النوع من البيانات بالحياة الخاصة للأفراد وتشمل كل البيانات التي من شأنها الكشف عن الأصل العرقي أو الآراء السياسية أو المعتقدات الدينية أو غيرها، وكذلك البيانات الشخصية المتعلقة بالصحة أو الحياة الجنسية، أو السوابق العدلية، المخزنة لدى المؤسسات العامة والخاصة في شكل قواعد بيانات، أو في خوادم الشبكات المعلوماتية، وتعتبر قواعد البيانات لمختلف المنظمات مصدرا هاما لهذا النوع من البيانات، كذاك المواد الاعلامية المنشورة على صفحات شبكات التواصل الاجتماعي، والبيانات التي تقوم وكلات التحقيق والاستخبارات بتقصيها وجمعها.[30]

ويتحدد نطاق هذه البيانات الشخصية الخاصة في عدة مواضع:

[29] منصور بن محمد الغامدي، البيانات الحيوية، البصمة الصوتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ط 01، 2005، ص 06.

[30] مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، قسنطينة، الجزائر، المجلد 07، العدد 01، 2018 ص 464.

أ- شبكات التواصل الاجتماعي:

تحوز شبكات التواصل الاجتماعي مثل: (Facebook Twitter Linkedin Intagram) عدة معلومات حول الأشخاص المستخدمين، زمن بينها معلوماتهم الشخصية من هوية، إقامة، منطقة، أصدقاء، ميول، أفكار، توجهات، نشاطات، تفاعلات، وكذا أدوات الاتصال والمراسلة من رسائل على التطبيقات أو ربط للبريد الإلكتروني، وكذا الهاتف، واستخدام تقنيات الهاتف، وتعد نقاط الاتصال والدخول إلى هذه الشبكة عملية مراقبة مستمرة وتسجيل دائم يتبع المستخدم.[31]

ولا يزال موضوع الخصوصية عبر مواقع ووسائل التواصل الاجتماعي يثير العديد من الإشكالات ولم يستقر الاجتهاد حول العديد من المسائل، خاصة ما تعلق بالملكية والقيمة التجارية للبيانات الشخصية المتداولة عبر هذه المواقع والوسائط، مع إمكانية تعارض الحق في الخصوصية مع حرية التعبير والحق في الوصول إلى المعلومة.[32]

وتأتي أرباح شركات شبكات التواصل الاجتماعي، من خلال جمع بيانات الأفراد وبيعها عادة إلى شركات دعاية، فكب المعلومات التي يقوم الفرد بإنزالها تكون معرضة لمخاطر الخصوصية، والسبب في ذلك الخوادم التي تحفظ أرقام IP، والكوكيز (COOKIES) التي تحفظ المعلومات حول المستخدم، على غرار مزود خدمة الأنترنت التي تمر كل المعلومات القادمة والمرسلة من المستخدم عبره.[33]

ب-وسائل الاتصال الالكترونية:

يعتبر البريد الالكتروني أحد الوسائل الحديثة في المعاملات الالكترونية التي تقدمها شبكة الانترنت، عن طريق التبادل الفوري للرسائل، ويعد اختراق البريد الالكتروني من اهم المخاطر التي تواجه الحق في الخصوصية، حيث يتعرض الفرد لانتهاك سرية المعاملات والمراسلات التي تدخل في شتى المجالات، لذلك لابد من تكريس ضمانات لحماية سرية المراسلات وفقا للقواعد

[31] عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية، دار الخلدونية، الجزائر، 2017، ص 123.
[32] مفيدة مباركية، المرجع السابق، ص 477.
[33] محمد ناصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية – دراسة مقارنة -، الطبعة الأولى، مركز الدراسات العربية، مصر، 2016، ص 52.

العامة، وهذا في حدود ضوابط معينة بغض النظر ما إذا كانت الأساليب المستخدمة تقليدية او حديثة.[34]

ج- محركات البحث:

تلجأ معظم الشركات إلى جمع البيانات الشخصية عبر مواقعها على شبكة الأنترنت، دون التصريح عن الغرض من ذلك، كما أنها لا تلتزم بإشعار المستخدمين بالتجميع عن طريق بيان سياسة الخصوصية الذي يُفترض أن يكون في الموقع، كما تقوم محركات البحث – Google مثلا – بجمع أكبر قدر ممكن من المعلومات والبيانات الشخصية من عناوين البروتكولات IP، وطلبات البحث، التي يمكن من خلالها تحديد هوية ومعتقدات الشخص أو ميوله، حيث قضت محكمة الدرجة الأولى بباريس بتاريخ 06 نوفمبر 2013 في هذا الخصوص، بالزام Google، بالاستناد إلى الحق في حرمة الحياة الخاصة، بوقف عرض صور تكشف الحياة الجنسية لأحد الأشخاص.[35]

د- المعاملات التجارية الالكترونية:

مع انتشار المعاملات التجارية الالكترونية كبيع وشراء وعرض للخدمات والمعلومات قد تشكل مساسا بالحق في الخصوصية، فهي تتطلب ثقة بين التاجر والزبون، خاصة عند تقديم رقم الاعتماد أو معلومات شخصية أو عنوان البريد، في حين قد يتم الاستيلاء والاستغلال غير المشروع لهذه البيانات، مما يجعل هذه المعاملات مصدرا آخر للخطر الذي يهدد الحياة الخاصة، كما ان وسائل الدفع الالكتروني هي الأخرى تعد أكبر مصدر خطر، لما يقابل سرعة المعاملات المالية من تهديد لسرية هذه المعاملات، إذ قد تُستخدم البيانات الشخصية للمتعامل لأغراض إجرامية من خلال تداولها مع مؤسسات مالية ومقدمي السلع والخدمات والوسطاء حيث يتم الاستلاء عليها.[36]

[34] خديجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الالكترونية – دراسة مقارنة -، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 29، العدد 03، 2013، ص 149.
[35] مفيدة مباركية، المرجع السابق، ص 468.
[36] صبرينة جدي، المرجع السابق، ص 130.

هـ-قواعد بيانات الحاسوب

بظهور الحكومة أو الإدارة الالكترونية، أو الرقمنة، أصبح تسيير المؤسسات يتم عبر الأنظمة المعلوماتية، مما يتطلب قواعد تبني قواعد البيانات التي تحتوي على بيانات شخصية تعود للعمال أو الموظفين أو التلاميذ، أو المرضى، أو المتابعين قضائيا في المحاكم، كلها بيانات تستوجب الحماية.[37]

كشفت الانترنت عن كثير من المخاطر والتحديات الأمنية التي قد تستهدف الكثير من الأجهزة والأنظمة الأساسية، على غرار أنظمة التشغيل والاتصالات، لذا من الضروري إيجاد تقنيات حديثة ومبتكرة لأمن الشبكات والأجهزة المتصلة لحمايتها من الهجمات التي تستهدف البيانات والمعلومات، من خلال تشفير جميع الاتصالات للتصدي للتحديات الجديدة المتمثلة في انتحال الهوية، أو الهجمات التي تستنزف استهلاك البطاريات، فمن المتوقع في الرؤى المستقبلية ظهور تحديات جديدة وهو ما يحتم تحديث البرمجيات والهاردوير الخاص بهذه الأجهزة حتى تعمل بكفاءة طول مدة خدمتها.[38]

[37] مفيدة مباركية، المرجع السابق، ص 466.

[38] أحمد محمد عبد الباقي، الأنترنت – التكنولوجيا وجرائم المستقبل، دار النهضة العربية، الطبعة الأولى، القاهرة، 2017، ص 551.

المبحث الثاني: أوجه الحماية الجزائية للحق في الخصوصية المعلوماتية

في ظل تزايد خطر التعدي على خصوصية مراسلات واتصالات الانسان، بسبب ما أنتجه التقدم العلمي والتكنولوجي من أجهزة التنصت والتسجيل الحديثة، فإن الأمر يستدعي تحقيق توازن بين الحق في حماية سرية المراسلات والاتصالات وعدم انتهاكها، وبين حق الدولة في الحفاظ على سلامتها الداخلية والخارجية ومراقبة كل ما من شأنه المساس بأمنها وأمن مواطنيها، وضع المشرع الجزائري آليات احترازية للحفاظ على سرية المراسلات والاتصالات الالكترونية من جهة – المطلب الأول – ، على غرار حماية المعطيات أثناء معالجتها – المطلب الثاني –.

المطلب الأول: حماية سرية المراسلات والاتصالات الالكترونية

يقصد بالحق في حرمة أو خصوصية الحق في الاتصالات الهاتفية: " حق الشخص في عدم الاعتداء على الاتصالات أو المحادثات الشخصية التي يجريها بواسطة استخدام جهاز هاتف التلفون، سواء أكان الاتصال سلكيا أو لاسلكي سواء تم ذلك بالتنصت أو المراقبة أو التسجيل في غير الأحوال التي يجيزها القانون "[1]

وينصرف مفهوم الحق في المحادثات والمكالمات الخاصة إلى تلك الأحاديث المباشرة التي تتم بين شخصين أو أكثر شفويا دون استخدام أجهزة الاتصال، وتلك الأحاديث التي تنم بين شخصين أو أكثر غير متواجدين في مكان عام باستخدام أجهزة الاتصال.[2]

أحاط المشرع الجزائري سرية المراسلات الالكترونية بحماية جزائية، تستهدف فرض عقوبات ردعية وقيام مسؤولية جزائية، لكل من تسول له نفسه انتهاك سرية المراسلات الالكترونية للغير، بغض النظر عن شكل الانتهاك سواء أكان بقصد الاطلاع على المراسلات أو نشر مضمونها أو استعمالها من دون ترخيص من صاحب الشأن أي المرسل أو المرسل له.[3]

---

[1] محمد نور الدين، الحماية الجنائية للحق في خصوصية المكالمات الهاتفية، دراسة تحليلية نقدية للقانون الكويتي والإماراتي، كلية القانون، جامعة الشارقة، عمادة البحث العلمي، مجلد رقم 43، 2016، ص 692.

[2] محمد أمين خرشة، جرائم الاعتداء على الحياة الخاصة، مجلة الحقوق، الأردن، العدد 08، 2012، ص 383.

[3] القانون رقم 18-04 مؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية رقم 27، صادرة بتاريخ 13 مايو 2018.

أولا: الحماية الدستورية للسرية المراسلات والاتصالات الالكترونية

تناول الدستور الجزائري[4] حماية حرمة الاتصالات ولم يسمح بالمساس بها إلا في الحالات المحددة قانونا وتحت رقابة السلطة القضائية،[5] فقد نصت المادة 46 منه على أنه: " لا يجوز انتهاك حرمة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون، أنا المادة 47 فقرة 01 فنصت على أنه: " لكل شخص الحق في حماية حياته الخاصة وشرفه. " كما نصت الفقرة الثانية منه على أن: " لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في شكل كانت.

حيث يُلاحظ من خلال المادة 47 من الدستور الجزائري مدى ارتباط الوثيق بين حق حماية الحياة الخاصة وحق حماية سرية المراسلات والاتصالات الخاصة، حيث بعدما أشار المشرع لحرمة الحياة الخاصة في الفقرة الأولى جاء في الفقرة الثانية وأشار لحرمة المراسلات والاتصالات الخاصة.

ثانيا: الحماية الجزائية لسرية المراسلات والاتصالات الإلكترونية

كما أقر قانون العقوبات الجزائري[6] حماية جزائية لحرمة الحياة الخاصة من أي تعدي، لاسيما من الاستعمالات غير المشروعة لتكنولوجيا المعلومات والاتصالات الحديثة، ذلك أن كل من النشر والتصوير والاستراق السمعي البصري والاطلاع على المراسلات المكتوبة والهاتفية تشكل صور الاعتداء على حرمة الحياة الخاصة.[7]

فالمشرع الجزائري بموجب المادة 303 من قانون العقوبات جرم بصفة عامة التعدي على الرسائل والمراسلات، ودون التقيد بشكل هذه المراسلات، فهو لا يتعلق بالرسائل الورقية بل يشمل أيضا رسائل البريد الالكتروني والرسائل النصية بأي تقنية كانت.[8]

---

[4] المرسوم الرئاسي رقم 20-442 مؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء نوفمبر 2020، جريدة رسمية رقم 82/ مؤرخة في 30 ديسمبر 2020.

[5] نصت المادة 65 مكرر 5 من قانون الاجراءات الجزائية: " إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة عبر الحدود المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الارهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أ يأذن بما يأتي: اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية اللاسلكية، وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط تثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية .... "

[6] قانون رقم 24-06 مؤرخ في 28 أبريل 2024، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية رقم 30، الصادرة بتاريخ 10 أبريل 2024.

[7] ذنون يونس صالح المحمدي ومهمدي صالح شحادة العبيدي، التعويض الناشئ عن الاعتداء على حرمة الحياة الخاصة، مجلة جامعة تكريت للحقوق، العراق، 2018، المجلد 02، العدد 03، الجزء الأول، ص 167.

[8] مفيدة مباركية، المرجع السابق، ص 475.

كما شدد المشرع الجزائري إذا كان مرتكب الفعل موظف أو مستخدم أو مندوب عن مصلحة البريد أو البرق، حيث نصت المادة 137 من قانون العقوبات على معاقبة كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها بالحبس من 03 أشهر إلى 05 سنوات وغرامة000 30 دج إلى 000 50 دج، يعاقب بذات العقوبة كل مستخدم أو مندوب في مصلحة البرق.

أما بالنسبة للمراسلات الالكترونية تقضي المادة 303 مكرر من قانون العقوبات أنه: " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 000 50 دج إلى 000 300 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية وذلك: 1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه .... "

كما تنص المادة 303 مكرر 1 من قانون العقوبات أنه: " يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 من هذا القانون .... "

يُلاحظ أن الشرع الجزائري جرم وعاقب في قانون العقوبات كل تعدي على حرية المراسلات والاتصالات سواء عن طريق نقل المكالمات أو الأحاديث الخاصة أو السرية دون وجه حق.

ثالثا: حماية سرية الاتصالات والمراسلات في مجال البريد

أصدر المشرع الجزائري قانون 2000-03 المتضمن القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية المعدل والمتمم،[9] يهدف إلى تحديد الشروط العامة للاستغلال في الميادين المتعلقة بالبريد والمواصلات السلكية واللاسلكية، وكيفية ضبطها، فحدد في المواد من 127 إلى 137 عدة عقوبات جزائية تترتب على الاعتداء على سرية المراسلات من قبل من الموظفين لدى مصالحها.[10]

[9] قانون رقم 2000-03 مؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية رقم 48، الصادرة بتاريخ 06 أوت 2000.

[10] أوقاسي خليدة، حرمة الحياة الخاصة في القانون الجنائي – دراسة مقارنة في التشريع الجزائري والفرنسي -، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة الجزائر 01، 2013-2014، ص 54.

وأمام الطفرة التكنولوجية والعلمية التي شهدها ويشهدها العالم في مجال الاتصالات، واستعمالات الهاتف النقال، كان لزاما على المشرع الجزائري مواكبة هذا التطور، فألغى القانون 2000-03 السالف الذكر وصدر بدلا عن القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية،[11] فقد نصت المواد من 164 إلى المادة 188 من القانون 18-04 على عدة عقوبات جزائية تفرض على المتعاملين في هذا المجال، إذ تنص المادة 164 على عقوبة تتراوح بين الحبس من سنة إلى خمس سنوات وبغرامة من 500 000 دج إلى 1 000 000 دج كل شخص ينتهك سرية المراسلات المرسلة عبر البريد أو الاتصالات الالكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها، على غرار نص المادة 165 من نفس القانون التي تعاقب كل متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال بالحبس من سنة إلى ثلاثة سنوات وبغرامة من 1 000 000 دج إلى 5 000 000 أو بإحدى هاتين العقوبتين، وتطبق نفس الأحكام على كل متعامل للاتصالات الالكترونية بحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الالكترونية أو أمر أو ساعد في ارتكاب هذه الأفعال.

وبما أنه من السهل على المستخدم لدى هيئة البريد أن يطلع على محتواها، فإنه طبقا لأحكام المادة 166 يعاقب كل عون مستخدم من طرف متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال في إطار ممارسة مهامه بعقوبة الحبس من ستة أشهر إلى سنتين وبغرامة من 500 000 إلى 1 000 000 دج.

ويعاقب بنفس العقوبات كل شخص مستخدم لدى متعامل الاتصالات الالكترونية يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الالكترونية أو أمر أو ساعد في ارتكاب هذه الأفعال، ويعاقب كل شخص غير الأشخاص المذكورين في المادتين السابقتين حسب نص المادة 167 بالحبس من شهرين إلى سنة واحدة وبغرامة من 200 000 دج إلى 500 000 دج.

[11] القانون 18-04 مؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات اللاسلكية، الجريدة الرسمية رقم 27، صادرة بتاريخ 13 مايو 2018.

من خلال ما سبق نجد أن جريمة الاعتداء على المراسلات والاتصالات تتم باطلاع الشخص على الرسائل أو المحادثات بصفة غير مشروعة كما تتعدد الجرائم الواقعة على البريد الالكتروني بتعدد غرض المجرم المعلوماتي، فيكفي أن يتم الاختراق حتى نكون بصدد انتهاك سرية المراسلات والاتصالات.[12]

رابعا: الاستثناءات الوارد على هذا القيد

إن تحديد نطاق الحق في حرمة الحياة الخاصة يحكمه عاملان أساسيان ومتنازعان، العامل الأول هو المصلحة الفردية في حرمة الحياة الخاصة وإضفاء السرية على نشاطاتها، والعامل الثاني هو حق المجتمع في توجيه سلوك أفراده ومعرفة بعض المعلومات عنهم، في حدود معينة وبوسائل مشروعة ومطابقة للقانون من أجل حماية مصالح المجتمع المختلفة، وعلى رأسها حماية الأمن والنظام العام،[13] فالقاعدة العامة تقتضي عدم مشروعية التنصت على المراسلات والمحادثات الخاصة بكافة أنواعها، إلا أن هناك استثناء يرد عليها حيث يُباح مراقبة المحادثات الخاصة، إذا كان بأمر من الجهة الخاصة المخولة لها إصدار الإذن بذلك وبصفة قانونية.[14]

وبالرجوع لقانون الاجراءات الجزائية المعدل والمتمم في الفصل الرابع في المواد 65 مكرر 5 إلى المادة 65 مكرر 10 والمعنون بـ: " اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، فقد سمحت بالتنصت في بعض الجرائم أهمها جرائم المخدرات والجرائم العابرة للحدود الوطنية جرائم تبيض الأموال ....، ومما يُضفي صفة المشروعية على عملية التنصت، صدور الإذن من جهة قضائية، وهي إما وكيل الجمهورية أو قاضي التحقيق.[15]

فقد رخص المشرع الجزائري للسلطات القضائية المختصة بموجب نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، حيث جاء فيها أنه: " إذا اقتضت ضرورات التحري في الجرائم المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات أو الجرائم

[12] سهير إيمان، الإعتداء على الحياة الخاصة في الوسط الافتراضي، مذكرة ماجستير، كلية الحقوق والعلوم السيتسية، جامعة البليدة 2، 2014-2015، ص 128.

[13] صوادقية هاني، حرية الحياة الخاصة في الأنظمة الوضعية المقارنة والشريعة الاسلامية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة البليدة 02، 2014 – 2014، ص 442.

[14] أوقاسي خليدة، المرجع السابق ص 32.

[15] العاقب عيسى، حماية الحياة الخاصة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة البليدة 2، 2014، ص 98.

المنظمة عبر الحدود والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية و اللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة وعمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

وبالرجوع للمواد من 08 والمادة 65 مكرر من قانون الإجراءات الجزائية تشمل شروط إباحة التنصت فيما يلي:

- أن تكون الجريمة قد وقعت فعلا،
- ظان تكون هذه الاجراءات استثنائية مفيدة في كشف الحقيقة،
- أن تكون الجريمة جناية أو جنحة بشرط أن يعاقب عليها بمدة تزيد عن 3 أشهر،
- أن يصدر الأمر أو الإذن من القضاء بمراقبة المحادثات،
- أن يكون الإذن مسببا،
- أن تكون المراقبة محددة بمدة لتفادي التعسف فيها، وأن تذكر هذه المدة في الأمر.

كما نصت المادة 56 من القانون[16] المتعلق بالوقاية من الفساد ومكافحته، على أنه من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى تسليم المراقب أو اتباع أساليب خاصة كالترصد الالكتروني والاختراق، على النحو المناسب بإذن من السلطة القضائية المختصة، تكون للأدلة المتوصل إليها بهذه الأساليب حجيتها وفقا للتشريع والتنظيم المعمول بهما.

كما نصت المادة 03 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتهما[17] على أنه: " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام والآداب العامة أو لمستلزمات التحريات أو التحقيقات

[16] قانون 06-01 مؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، جريدة رسمية رقم 14، صادرة بتاريخ 08 مارس 2006.
[17] القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، صادرة بتاريخ 16 أوت 2009.

الجارية ..... وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المعلوماتية.

كما نصت المادة 04 فقرة 03 من نفس القانون أنه: " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية:

لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية ..... لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.... "

وتطبيقا لنص المادة 13 من القانون السالف الذكر، صدر المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما،[18] حيث تكلف هذه الهيئة بموجب المادة 04 منه بضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحث سلطة القاضي المختص وباستثناء أي هيئات وطنية.

من خلال النصوص القانوني السابقة الذكر نلاحظ أن المشرع الجزائري ضيق من نطاق الحق في حرية المراسلات والاتصالات الالكترونية بهدف مكافحة بعض الجرائم التي تتسم بخطورتها الإجرامية، كجرائم المخدرات، الجرائم المنظمة العابرة للحدود الوطنية، جرائم الإرهاب، الجرائم الماسة بأمن الدولة، جرائم تبيض الأموال، الجرائم الماسة بأنظمة المعالجة للمعطيات، الجرائم الخاصة بالتشريع الخاص بالصرف وجرائم فساد.[19]

حيث منح المشرع الجزائري صلاحيات للسلطة القضائية المختصة وضباط الشرطة القضائية تمكنهم من مراقبة الاتصالات الالكترونية، وإلزام مقدمي خدمت الانترنت بحفظ بيانات المستخدمين التي تمكن من التعرف عليهم، كمكان المرسل والمرسل له وعناوين المواقع الالكترونية المطلع عليها، الأمر الذي قد يتعارض مع الحق في الخصوصية، لأن هذه القواعد تسمح بمراقبة الاتصالات الالكترونية وجمع البيانات

[18] المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما، الجريدة الرسمية رقم 53، صادرة بتاريخ 08 أكتوبر 2015.

[19] بن حيدة محمد، مكانة الحق في الحياة الخاصة في ظل التعديل الدستوري 16-01، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، 2018، العدد 10، المجلد 01، ص 41.

سواء من طرف السلطات الداخلية والأجنبية في إطار التعاون الدولي والمساعدة القضائية، إلا أن اهتمام المشرع الجزائري بحماية الحق بالخصوصية ليس مغيبا، إذ نلمسه من خلال إرادته في التوفيق بين تبني قواعد إجرائية ناجعة لمكافحة الجرائم والوقاية منها وبين تكريس هذا الحق المهم.[20]

المطلب الثاني: حماية الأشخاص الطبيعيين في مجال معالجة المعطيات

أدرج المشرع الجزائري القسم السابع مكرر في الفصل الثالث من الباب الثاني من الكتاب الثاني من القانون رقم 24-06 مؤرخ في 28 أبريل 2024، يعدل ويتمم الأمر 66-156 بتاريخ 08 يونيو 1966، المتضمن قانون العقوبات المواد 394 إلى 394 مكرر7، بعنوان المساس بأنظمة المعالجة الآلية للمعطيات، كما أصدر القانون 09-04 بتاريخ 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فعاقب المشرع على كل تخريب لمحتويات نظام المعالجة الآلية للمعطيات أو إعاقة تشغيله، أو تخريب الحماية الفنية للمعطيات التي تتمثّل في الإجراء الوقائي للمحافظة على خصوصية البيانات المتناقلة عبر الشبكات، وبالأخص عبر الأنترنت، للوصول إلى سرية الرسائل الالكترونية والبيانات المتناقلة.

أولا: تعريف المعطيات ذات الطابع الشخصي

يقصد بالمعطيات ذات الطابع الشخصي: كل معلومة، بغض النظر عن دعامتها، متعلقة بشخص معرّف أو قابل للتعرّف عليه، والمشار إليه أدناه، الشخص المعني بصفة مباشرة أو غير مباشرة، لاسيّما بالرجوع إلى رقم التعريف أو عنصر أو عدّة عناصر خاصة بهويّته البدنية أو الفيزيولوجية أو الجينية أو البيو مترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.[21]

أما معالجة المعطيات ذات الطابع الشخصي فقد عرّفها المشرع الجزائري بأنها: " كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها، على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الايصال عن طريق الارسال أو النشر، أو أي شكل من أشكال الإتاحة أو التقريب أو الرّبط البيني، وكذا الإغلاق أو التشفير

[20] مفيدة مباركية، المرجع السابق، ص 482.

[21] المادة 03 من القانون 18-07 مؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34، صادرة بتاريخ 10 يونيو 2018.

أو المسح أو الاتلاف"،[22] ولم يحصر المشرع الجزائري المسؤول عن المعالجة الآلية في الشخص الطبيعي، بل أدج أيضا الشخص المعنوي كالشركات والهيئات العمومية، وعرّفه بأنه: " شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر، يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها."[23]

ثانيا: حقوق الشخص المعني بالمعالجة

سنتعرّض فيما يلي إلى الحقوق المتصلة بالإعلام والولوج والحق في التصحيح والحق في الاعتراض

1- الحق في الإعلام

نصّت المادة 32 من القانون 18-07 المتعلّق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي إلى وجوب إعلام – مسبقا – كل الأشخاص المعنيين الذين يتم الاتصال بهم لجمع المعطيات، وذلك قبل القيام بهذا التّجميع وليس أثناءه، على أن يكون الاعلام صريحا ولا يتحمّل اللُّبس، ولا يسقط إلا في حالة التي يكون فيها الشخص المعني على علم مسبق بالعناصر اللاّزم إخباره بها.[24]

وحددت المادة المذكورة سلفا العناصر التي يُلزم أن يُخطر بها الشخص المعني وهي:

- هوية المسؤول عن المعالجة وعند الاقتضاء هويّة ممثّله
- أغراض المعالجة
- كل المعلومات المفيدة

غير أن إلزامية الإعلام المذكور في المادة 32 من هذا القانون لا تطبق إذا:

- تعذّر إعلام الشخص المعني، لاسيما في حالة معالجة المعطيات ذات الطابع الشخصي لأغراض إحصائية أو تاريخية أو علمية، يجب على المسؤول عن المعالجة في هذه الحالة إشعار السلطة الوطنية باستحالة إعلام الشخص المعني، وتقديم سبب الاستحالة لها.
- في حالة ما إذا تمت المعالجة تطبيقا لنص قانوني.
- إذا تمّت المعالجة حصريّا لأغراض صُحفية أو فنيّة أو أدبية.

[22] المادة 03 من القانون 18-07 السالف الذكر

[23] المادة 03 فقرة 12 من القانون 18-07 السالف الذكر.

[24] يحي تومي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07، دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 1525.

2- الحق في الولوج

نصّت المادة 34 من القانون 18-07 السالف الذكر بأنه:" يحق للشخص المعني أن يحصل من المسؤول عن المعالجة على:

- التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، وأغراض المعالجة وفئات المعطيات التي تنصبُّ عليها والمرسل لهم.
- إفادته وفق شكل مفهوم بالمعطيات الخاصة به التي تخضع للمعالجة، وكذا بكل معلومة متاحة حول مصدر المعطيات، كما يحقّ للمسؤول عن المعالجة أن يطلب من السُّلطة الوطنية تحديد آجال الإجابة على طلبات الولوج المشروعة، ويمكنه الاعتراض على الطلبات التعسفية لاسيما من عددها وطابعها المتكرّر، ويقع على عاتقه إثبات الطابع التعسفي لهذا الطّلب.

3- الحق في التصحيح

نصت المادة 35 من القانون 18-07، أنه يحق للشخص المعني بعد تقديم ما يّثبت هويته أن يحصل مجانّا من المسؤول عن المعالجة، على تحيين أو تصحيح أو مسح أو إغلاق الولوج إلى المعطيات ذات الطابع الشخصي، والتي تكون معالجتها غير مطابقة للقانون، فعلى المسؤول على المعالجة القيام التصحيحات اللاّزمة ودون مقابل، وذلك في أجل عشرة أيام كاملة من تاريخ إخطاره، وفي حالة عدم الرّد يمكن اللجوء إلى السلطة الوطنية عن طريق إيداع طلب، إذ تقوم بتكليف أحد أعضائها من أجل القيام بكل التحقيقات المفيدة والعمل على إجراء التصحيحات اللاّزمة في أقرب الآجال، كما يمكن بناء على الفقرة من هذه المادة استعمال حق التصحيح من قبل ورثة الشخص المعني.

4- الحق في الاعتراض

يعد من بين الحقوق الأساسية التي منحها القانون 18-07 للشخص بغية حماية حياته الخاص، من خلال مواجهة استعمال معطياته الخاصة من قبل المسؤول عن المعالجة أو الغير، حيث جاءت المادة 36 من هذا القانون بالنصّ: " يحق للشخص المعني أن يعترض لأسباب مشروعة على معالجة معطياته ذات الطابع الشخصي، وله الحق في الاعتراض على استعمال المعطيات المتعلقة به لأغراض دعائية ولاسيما التجارية منها من طرف المسؤول الحالي للمعالجة أو مسؤول عن معالجة لاحقة ... " وعليه يمكن أن تتم ممارسة الحق في الاعتراض لحظة جمع البيانات،

غير الفقرة الأخيرة من هذه المادة رفعت هذا الحق إذا كانت المعالجة تستجيب لالتزام قانوني أو إذا كان تطبيق هذه الأحكام قد أُستبعد بموجب إجراء صريح في المحرر الذي يرخص بالمعالجة.

ثالثا: الحماية الإدارية والجزائية في معالجة المعطيات الشخصية

نظرا لأهمية المعطيات ذات الطابع الشخصي وجب وضع قواعد لحمايتها من المخاطر التي تهدّدها، لذلك أقر المشرع الجزائري في الفصل الثالث 18-07 أحكاما جزائية بموجب المواد من 54 إلى غاية المادة 74 منه، فوضع نصوصا تجرم الانتهاكات الماسّكة بالمعطيات الشخصية أثناء معالجتها، وأقر جملة من العقوبات على الجهات التي لا تحترم مقتضيات هذا القانون، وقبل التطرّق إلى الحماية الجزائية لابد من التعرُّض إلى الحماية الإدارية كأجراء وقائي.

1- الحماية الإدارية للمعطيات الشخصية

السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

نصت المادة 22 فقرة 01 من القانون 18-07 على أنه :" تنشأ لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي"،

فحسب مقتضيات المادة 25 من القانون 18-07 السالف الذكر، تسهر اللجنة على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، وضمان عدم انطواء استعمال تكنولوجيا الاعلام والاتصال على أيّ أخطار تجاه حقوق الأشخاص والحرّيات العامّة والحياة الخاصة، ومن بين مهامها ما يلي:

- منح التراخيص وتلقّي التّصريحات المتعلّقة بمعالجة المعطيات ذات الطابع الشّخصي
- إعلام الأشخاص المعنيّين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
- الترخيص بنقل البيانات ذات الطابع الشخصي نحو الخارج، وفقا للشروط المنصوص عليها في هذا القانون.
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي للمعالجة.
- الأمر بالإغلاق كعطيات أو سحبها أو إتلافها.
- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.
- إصدار عقوبات إدارية وفقا للمادة 46 من القانون 18-07 السالف الذكر.

كما تتوفر السلطة الوطنية على صلاحية البحث والتحري التي تمكّن أعوانها المفوّضين لهذا الغرض من القيام بالتحريّات المطلوبة.

تتخذ السلطة الوطنية إجراءات إدارية في حق المسؤول عن المعالجة في حال خرقه لأحكام القانون 18-07 من خلال المواد 46 و47 و48 وتتمثّل في:

الإنذار – الإعذار- السّحب المؤقّت لمدّة لا تتجاوز سنة أو السحب النهائي لوصل التصريح أو الترخيص.

توقيع عقوبة غرامة مالية ضد كل مسؤول إمّا:

- يرفض دون سبب شرعي حقوق الاعلام والولوج أو التصحيح أو الاعتراض المنصوص عليه في هذا القانون، أو لا يقوم بالتبليغ.

في حالة العود تطبق العقوبات المنصوص عليها في المادة 64ن وتكون قرارات الهيئة قابلة للطعن لدى مجلس الدولة.

يتعيّن على الرئيس وأعضاء اللجنة الالتزام بالطابع السرّي للمعطيات بعد الانتهاء من مهامّهم، على أن يستفيدوا من حماية الدولة ضد التهديدات أو الإهانات أو الاعتداءات التي يتعرضون لها خلال مزاولة العمل خلال عهدتهم لمدة 05 سنوات.

2- الحماية الجزائية للمعطيات الشخصية

ضمانا لحقوق الأفراد في الحياة الخاصة، تضمّن القانون رقم 18-07 المتعلّق بحماية المعطيات الشخصيّة، قواعد جزائية متعلقّة بحماية المعطيات ذات الطابع الشخصي، وتم تقسيمها إلى: جرائم ماسة بالقواعد الموضوعية، جرائم ماسة بالقواعد الاجرائية.

أ- الجرائم الماسة بالقواعد الموضوعية للمعالجة

جرّم المشرع الجزائري جملة من الأفعال التي تشكّل خرقا للقواعد التي يلزم مراعاتها عند القيام بمعالجة المعطيات ذات الطابع الشخصي، على غرار العقوبات المقررة للشخص المعنوي في مخالفته للقواعد المنصوص عليها في قانون العقوبات، فضلا عن العقوبات التكميلية التي

تطال الذين يخالفون أحكام هذا القانون والمنصوص عليها في قانون العقوبات، وتشمل نوعين من الجرائم: جريمة المعالجة غير المشروعة، وجريمة الاستعمال غير المشروع للمعطيات.

1- جريمة المعالجة غير المشروعة للمعطيات ذات الطابع الشّخصي

يقع على المسؤول على المعالجة وضع تدابير تقنية وتنظيمية ملائمة لحماية المعطيات ذات الطابع الشّخصي من الاتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخّصين، خصوصا عندما تستوجب المعالجة إرسال معطيات عبر شبكة معيّنة وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة، كما يجب أن تضمن هذه التدابير مستوى ملائما من السّلامة بالنّظر إلى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها.[25]

فقد نصت المادة 57 من القانون 18-07 السالف الذكر، على أنه: " يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000 دج إلى 500.000 دج كل من قام دون الموافقة الصريحة للشخص المعني، وفي غير الحالات المنصوص عليها في هذا القانون، بمعالجة المعطيات الحساسة"

أما المادة 58 من نفس القانون فنصت على أنه: " يعاقب بالحبس من 06 أشهر وبغرامة من 60.000 دج إلى 100.000 دج إلى 300.000 دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدلسية أو بطريقة غير نزيهة أو غير مشروعة "

أما المادة 68 من فقرتها الثانية فتنصّ أنّه " يُعاقب بنفس العقوبة كل من قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدّة المنصوص عليها في التشريع الساري المفعول، أو تلك الوارد في التصريح أو الترخيص."

2- جريمة الاستعمال غير المشروع للمعطيات

نصّت المادة 69 من القانون 18-07 على أنه: " يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100.000 دج إلى 500.000 دج كل مسؤول عن المعالجة وكل معالج من الباطن وكل شخص مكلّف بالنظر إلى مهامه بمعالجة معطيات ذات طابع

[25] حسب أحكام المادة 38 الواردة في الفصل الأول بعنوان: سرية وسلامة المعالجة، الباب الخامس، حول التزامات المسؤول عن المعالجة في القانون 18-07 السالف الذكر.

شخصي يتسبّب أو يسّهل – ولو عن إهمال – الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك."

3- جرائم تتعلق بحقوق الشخص المعني

منح المشرع الجزائري للأشخاص المعنيين بمعالجة المعطيات ذات الطابع الشخصي مجموعة من الحقوق في مواجهة المسؤول عن المعالجة، بهدف حماية حياتهم الخاصة من كل اعتداء، حيث خصها المشرّع في الباب الرابع من القانون 18-07 ... كل اعتداء على الحقوق يشكل فعلا مجرما، كإجراء المعالجة رغم اعتراض الشخص المعني، أو رفض حقوق الإعلام أو الولوج أو التصريح أو الاعتراض، ومن بين الجرائم المتعلقة بحقوق المعني كل معالجة يجريها المسؤول دون أخذ الموافقة الصّريحة من الشخص المعني، ودون أن تكون هذه المعالجة مدرجة ضمن الحالات الضرورية المنصوص عليها قانونا.

ب- الجرائم الماسة بالقواعد الإجرائية الشكلية للمعالجة

يقتضي القيام بمعالجة المعطيات ذات الطابع الشخصي ضرورة احترام جملة من القواعد الإجرائية التي نص عليها المشرّع بهدف حماية الأشخاص الطّبيعيين، حيث يلتزم المسؤول عن المعالجة قبل إجرائها بضرورة ببعض الشكليات، إذ أن مخالفتها يعدّ جريمة معاقب عليها، وهذا بهدف حفظ أمن هذه المعطيات.

1- الجرائم المتعلّقة بالإجراءات المسبقة عن المعالجة

يجب على المسؤول عن المعالجة ان يحصل على تصريح أو ترخيص من قبل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من قبل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وهذا ما نصّت عليه المادة 12 من القانون 18-07 السالف الذكر، ويعد غياب التصريح أو الترخيص جريمة يعاقب عليها وفق المادة 56 من القانون هذا القانون، أو في حالة تقديم تصريحات كاذبة لمواصلة نشاط معالجة المعطيات رغم سحب التصريح أو الترخيص الممنوح له.

2- نقل المعطيات ذات طابع شخصي نحو دولة أجنبية

من بين المخاطر التي تهدد حق الأفراد في حماية حياتهم الخاصة، والتي يتم فيها مخالفة القواعد الشكلية لمعالجة المعطيات الشخصية دون ترخيص من السلطة الوطنية،

نقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية، وهي من الجرائم العمدية يعاقب عليها طبقا لأحكام المادة 67 من نفس القانون.

ويعد كذلك من الجرائم المتعلقة بالإجراءات المسبقة للمعالجة، من غير الحالات المنصوص عليها قانونا، كل من قام بوضع أو حفظ في الذاكرة الآلية للمعطيات ذات الطابع الشخصي بخصوص جرائم وإدانات أو تدابير أمن، إذ يتعلق الأمر بالمعطيات الشخصية المتعلقة بالجنايات أو الجنح أو المخالفات المرتكبة من قبل شخص معين، وبالإدانات الصادرة بشأنها من القضاء، وكذا التدابير الوقائية المتّخذة من قبله، فكل معالجة بهذه المعطيات تُعدّ جريمة معاقب عليها بموجب المادة 68 من هذا القانون، فهذا النوع من المعالجة ممنوع في القطاع الخاص، ولا تخصّ معالجتها إلا الهيئات القضائية.[26]

[26] عائشة بن قارة، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الطبعة الأولى، الاسكندرية، مصر، 2010، ص 755.

خاتمة

خاتمة

نعيش في الآونة الأخير طفرة وتطورا غير مسبوق في تكنولوجيات الاعلام والاتصال على مستوى جميع الأصعدة، فبقدر إيجابيات ذلك هناك العديد من السلبيات لعل أبرزها وأهمها ما أفرزته هذه النقلة والتطور في خلق تهديدات لجوانب أخلاقية من هوية الفرد، كالخصوصية والكرامة والاحترام، حيث أصبحت منصات ووسائل التقنية التي تقدم خدمات للأفراد، تعمل على جمع ومعالجة المعلومات والبيانات الشخصية للأفراد، والتي كانت محلا لكثير من الجرائم المعلوماتية مثل السرقة والانتحال والمتاجرة أو الاستعمال المسيء لها، مما قد يهدد خصوصية الفرد، فأصبحت هذه الجرائم تشكل تحديا لجميع العاملين والمستهلكين وحتى المستثمرين في هذا القطاع، خاصة وانها جريمة يصعب تقفي آثارها أو وقفها كونها عابرة لحدود الدول.

فقد حاولنا من خلال هذا الدراسة معالجة الموضوع من خلال فصلين أساسيين، تعرضنا للفصل الأول إلى الإجرام المعلوماتي وصعوبة التحقيق، بالتطرق إلى مفهوم الأجرام المعلوماتي من خلال الاتجاه الضيق والموسع وكذا موقف المشرع الجزائري من ذلك، ثم بيان أركان الجريمة المعلوماتية، حيث تناولنا الأركان العامة للجريمة من ركن شرعي ومادي ومعنوي، بالإضافة إلى الركن المفترض في هذه الجريمة، أما المبحث الثاني لهذا الفصل فخصصناه لصعوبة التحقيق في هذا الجريمة ، فتحدثنا في المطلب الأول عن صعوبة التحقيق بالنظر إلى خصوصية هذه الجريمة التي جعلها تنفرد عن الجريمة التقليدية، سواء بالجريمة ذاتها أو بالمجرم الالكتروني، لنبين في المطلب الثاني من هذا المبحث دور الضحية في إعاقة سير التحقيق خاصة فيما يتعلق بالرقم الأسود لهذه الجرائم.

أما الفصل الثاني فخصصناه للحديث عن الخصوصية المعلوماتية، من خلال تعريفها الفقهي والقانوني وموقف المشرع الجزائري من التعريفات، في المبحث الأول ، على غرار نطاق الاعتداء على الحق في الخصوصية من خلال بيان ماهية البيانات الشخصية وانواعها ومحل الاعتداء الذي يكون في وسائط ومنصات التواصل الاجتماعي، وفي محركات البحث وقواعد بيانات الحاسوب، أما المبحث الثاني فقد تناولها حماية الجزائية لهذه البيانات من خلال حماية سرية المراسلات والاتصالات الالكترونية في المطلب الأول، أما المطلب الثاني فتناولنا فيه حماية الشخص الطبيعي في مجال معالجة البيانات.

فمن خلال هذه الدراسة، تم التوصل في نهايتها إلى جملة من النتائج، نذكر أهما فيما يلي:

1- بالنظر لحداثة وتطور للجريمة الالكترونية، فلا يوجد لحد الآن إجماع فقهي، حيث تباينت التعريفات بين من المفهوم الواسع والضيق لهذه الجريمة، أو في صياغة موحدة للدلالة عليها بين يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي، أو من يسميها بالجريمة الالكترونية أو السيبرانية.

2- على غرار المشرع الجزائري الذي لم يستقر على تسمية واحدة للجريمة المعلوماتية، فأسماها بـ: المساس بأنظمة المعالجة الآلية للمعطيات وذلك في قانون 04-15، في حين عمد على تسميتها بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال في القانون 09-04، غير أنه رغم اختلاف التسميتين إلا أن الهدف واحد هو مكافحة الجريمة المعلوماتية.

3- تتميّز الجريمة المعلوماتية بعدة خصائص تميزها عن الجريمة التقليدية جعل من التحقيق فيها صعبا، على غرار الضحية في هذه الجريمة الذي أصبح رقما أسودا في إعاقة سير التحقيق وفي ارتفاع نسبة الجريمة الالكترونية.

4- هناك معطيات تكون متفرقة ومشتتة بين مختلف قواعد البيانات، لكن بفعل ما أنتجه التقنية المعلوماتية يمكن جمع المعطيات ومعالجتها، فإنها تتحول إلى معلومات ذات طبع شخصي قد تشكل تهديدا حقيقيا لخصوصية الأفراد، حيث تصبح نوعا من البيان التفصيلي عن حياة الفرد وانشطته وخبايا أسراره.

5- كرّس المشرع الجزائري مبادئ يتوجب احترامها عند كل معالجة للمعطيات ذات الطابع الشخصي، بهدف عدم الإساءة إلى أصحابها، وهو مبدأ مشروعية المعالجة الذي يقتضي أن تكون العمليات التي تتم آليا بهدف استغلال المعطيات الشخصية صحيحة ودقيقة عن طريق ربط ودمج معطيات شخصية مع معطيات أخرى، وتحليلها للحصول على معطيات ومعلومات ذات دلالة خاصة.

6- وضع المشرّع الجزائري مجموعة من الضوابط الموضوعية القانونية التي تحكم المعالجة السليمة والمشروعة للمعطيات ذات الطابع الشخصي، وترتبط أساسا بحقوق المعني بالمعالجة، والتي يهدف المشرع من خلالها إعطاء المعني السيطرة على معطياته الشخصية، وتتمثل في الحق في الإعلام، الحق في الولوج، الحق في التصحيح والحق في الاعتراض.

7- كما أحاط المشرع الجزائري معالجة المعطيات الشخصية بمجموعة من الإجراءات المسبقة، والتي ينبغي على كل شخص طبيعي أو معنوي ينتمي إلى القطاع العام أو الخاص، احترامها قبل البدء

في إنشاء معالجة معلوماتية، وتنحصر أساسا في التصريح لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو الترخيص منها قبل القيام بهذه المعالجة، مالم تكن المعالجة تنصب على حالة من الحالات التي استثنى فيها المشرع الخضوع لهذه الإجراءات.

8- تتعرض المعلومات ذات الطابع الشخصي لجملة من المخاطر خلال تجميع وتخزين المعلومات ذات الطابع الشخصي في أجهزة الكمبيوتر، إلى الوصول إليها من دون إذن وبطرق التحايل، مما يفتح مجالا واسعا لإساءة استخدامها أو توجيهها توجيها منحرفا أو استخدامها في غير الغرض الذي جُمعت لأجله، مما يؤدي للمساس بخصوصية أصحاب هذه المعطيات.

9- أرود المشرع الجزائري آليات قانونية لمواجهة التحديات الناشئة عن أثر التقنية المعلوماتية على خصوصية الأفراد عند معالجة معطياتهم الشخصية، وذلك من خلال الحماية الإدارة المجسدة في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصية لها دور الاشراف والرقابة على عمليات معالجة المعطيات ذا الطابع الشخصي، أو عن طريق آلية الردع الجزائي من خلال العقاب على الانتهاكات والاعتداءات التي تطال الحق في الخصوصية المعلوماتية.

10- تنامي طاهرة الجريمة المعلوماتية، وزيادة حجم النشاط الإجرامي بشكل مفرط، وتحولت إلى نشاط يستهف تحقيق الربح من خلال مساومة الضحية في خصوصيته أو كرامته، على غرار تحولها للواقع الحالي كالإرهاب الالكتروني، والنشاط الإجرامي المنظم، إذ أصبحت الجماعات الإجرامية والارهابية تستغل شبكات الأنترنت لأجل حصد موارد مالية ونشر أفكارها.

الاقتراحات:

1- نرى أنه من الأحسن وتفاديا للبس أن يذكر المشرع خصائص المعلومة (التحديد – الابتكار – الرية – الاستئثار) محل الحماية لتفادي أي لبس قانوني، حيث تعد هذه المعلومة مستهدفة من خلال الجرائم المعلوماتية، على غرار تعديل النصوص القائمة لتستوعب الصور المتطورة للجرائم المعلوماتية.

2- نص القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات ذات الطابع الشخص على تمكين المعني بالمعالجة مجموعة من الحقوق كحق الإعلام والتصحيح وغيرها، إلا أن المشرع لم يصدر مرسوم تنظيمي لتطبيق أحكما هذ القانون، خاصة فيما يتعلق بكيفية

ممارسة الشخص بالمعالجة حقوقه، أو بخصوص كيفية ممارسة السلطة الوطنية لصلاحياتها وسلطاتها، خاصة ما تعلق بمهام البحث والمعاينة لجرائم الاعتداء على المعطيات الشخصية، إما عن طريق أعوانها أو عن طريق أعوان آخرين تلجأ إليهم السلطة، اقتداء بالمشرع الفرنسي في هذا الخصوص، على غرار إدراج صور التجريم الناشئة عن أفعال الاعتداء على المعطيات ذات الطابع الشخصي.

3- ضرورة إدراج مقاييس لها علاقة بالتقنية الجديدة في الكليات والمعاهد القضائية، مثل ادراج الجريمة الالكترونية في مقياس قانون العقوبات، الإدارة الالكترونية في مقياس القانون الإداري، المحكمة الالكترونية في مقياس الإجراءات الجزائية، على غرار التكثيف من الدورات التحسيسية والتثقيفية لفائدة مستخدمي التقنية او موظفي الشركات والمؤسسات وخاصة المالية منها، بهدف وضعهم أمان واقع الجريمة المعلوماتية، وتلقينهم صور وأنواع وأساليب الجريمة المعلوماتية، وسبل التصدي للهجمات الالكترونية وكيفية التعامل معها.

4- التحسيس والرفع من مستوى الوعي لدى الافراد بالأمن المعلوماتي والجريمة المعلوماتية وأنها أعمال غير مشروعة تعرض مرتكبيها لعقوبات مشددة، وأن التبليغ عنها يعد من صميم التشاركية في التصدي ومواجهة هذه الجرائم.

5- ضرورة تأهيل وتدريب الأفراد في مجال البحث والتحري والتحقيق، مع هذا النوع الجرائم والتقنيات الحديثة في الكشف عن هذه الجرائم قبل وقوعها أو أثناء أو بعد وقوعها، وتحقيق تعاون إقليمي ودولي سواء فيما يتعلق بالتقنية أو في التكامل القانوني لتصدي لهذه الجرائم، فضلا عن تأهيل القضاة وتكوينهم حتى يتسنى له الالمام بكافة النصوص والإجراءات المتبعة في هذا النوع من الجرائم خاصة ما يتعلق بالأحكام المستحدثة، في حين هناك من يرى ان التخصص القضائي يعد ناجعا لمجابهة خطر الجريمة المعلوماتية من خلال قضاة متخصصين في الجريمة المعلوماتية ومحاكم متخصصة بها.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

المراجع

الكتب العامة:

1) د. رامز محمد عمار، نعمت عبد الله مكي، حقوق الإنسان والحريات العامة، الطبعة الأولى، 2010، من دون دار نشر.

2) د. عائشة بن قارة، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، مصر، 2010.

الكتب الخاصة:

3) د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، – دراسة مقارنة –، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، مصر، 2000.

4) د. أحمد محمد عبد الباقي، الأنترنت – التكنولوجيا وجرائم المستقبل، دار النهضة العربية، الطبعة الأولى، القاهرة، 2017.

5) د. جميل عبد الباقي الصغير، جرائم التكنولوجيا الحديثة، دار النهضة العربية، الطبعة الأولى، القاهرة، 2001.

6) د. حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، دون سنة نشر.

7) د. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الطبعة الأولى، عمان، 2011.

8) د. طاهر محمود أبو القاسم، الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، 2019.

9) د. عائشة بن قارة، حجية الدليل الالكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الطبعة الأولى، الاسكندرية، مصر، 2010.

10) د. عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكومبيوتر والتزوير، دارسة معمقة في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، الطبعة الأولى، مصر، 2002.

11) م. عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية، دار الخلدونية، الطبعة الأولى، الجزائر، 2017.

12) بولين أنطونيوس أيوب، الحامية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي، الطبعة الأولى، 2009.

13) أ.د. علي عبد القادر لقهوجي، الحماية الجنائية لبرنامج الحاسب الآلي، من دون طبعة، الدار الجامعية للطباعة والنشر، بيروت، د ط، 1999.

14) د. فهد عبد الله العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، الطبعة الأولى، 2016.

15) د. محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، الطبعة الأولى الإسكندرية، مصر، 2007.

16) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الأولى، دار النهضة العربية، القاهرة، 1994.

17) د. محمد ناصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية – دراسة مقارنة –، مركز الدراسات العربية، الطبعة الأولى، مصر، 2016.

18) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الإسكندرية، بيروت 2005.

19) د. محمد علي العريان، الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الاسكندرية، 2004.

20) د. نهلا عبد القادر المومني، الجرائم المعلوماتية، طبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.

21) د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، مصر، الطبعة الأولى، 2009.

22) د. مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، مصر، 2016.

23) د. منى الأشقر، د. محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، الطبعة الأولى، بيروت، لبنان، 2018.

24) أ د. منصور بن محمد الغامدي، البيانات الحيوية، البصمة الصوتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، الطبعة الأولى، 2005.

25) د. نويري عبد العزيز، الحماية الجزائية للحياة الخاصة دراسة مقارنة ين القانون الجزائري والفرنسي، دار هومه للطباعة والنشر والتوزيع، الطبعة الأولى، الجزائر، 2015.

الرسائل العلمية:

أطروحات الدكتوراه

1) د. العاقب عيسى، حماية الحياة الخاصة، أطروحة دكتوراه، جامعة البليدة 2، كلية الحقوق والعلوم السياسية، قانون خاص، 2014.
2) د. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في الحقوق تخصّص – قانون العقوبات والعلوم الجنائية، جامعة باتنة، كلية الحقوق والعلوم السيّاسية، قسم الحقوق، الجزائر 2015، 2016.
3) د. سعيداني نعيم، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه العلوم في القانون، قانون جنائي، جامعة باتنة 01، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2020،2021.
4) د. صوادقية هاني، حرية الحياة الخاصة في الأنظمة الوضعية المقارنة والشريعة الاسلامية، أطروحة دكتوراه، جامعة البليدة 02، كلية الحقوق والعلوم السياسية، قانون عام، 2014–2015.

رسائل الماجستير

1) أوقاسي خليدة، حرمة الحياة الخاصة في القانون الجنائي – دراسة مقارنة في التشريع الجزائري والفرنسي –، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق، جامعة الجزائر 01، 2013–2014.
2) سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
3) رؤى سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية، مشروع رسالة مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في تخصص الأنظمة، جامعة الملك عبد العزيز، المملكة العربية السعودية، مجلة كلية الدراسات الاسلامية والعربية بدمنهور العدد السادس الاصدار الثاني، الجزء الأول 2021.
4) سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، الجزائر، 2012–2013.
5) سهير إيمان، الاعتداء على الحياة الخاصة في الوسط الافتراضي، مذكرة مقدمة لنيل شهادة الماجستير، جامعة البليدة 2، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014–2015.

6) سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2010.
7) د. شلاخ لطيفة، انتشار الجريمة الالكترونية الماسة بالأشخاص في الهيئة الجزائرية، دراسة ميدانية لبعض مستخدمي مقاهي النت بمدينة المسيلة، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام الآلي والاتصال تخصص صحافة مكتوبة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف، المسيلة، ماي 2017.
8) صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، الموسم الجامعي 2013/2012.
9) قارة أمال، الجريمة المعلوماتية، رسالة مقدمة لنيل شهادة الماجستير تخصص القانون الجنائي والعلوم الجنائية، جامعة الجزائر 01، كلية الحقوق، 2005.
10) معتوق عبد اللطيف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير علوم جنائية، جامعة العقيد الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة، 2011-2012.

المقالات والمجلات العلمية:

1) د. بن حيدة محمد، مكانة الحق في الحياة الخاصة في ظل التعديل الدستوري 16-01، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، العدد 10، المجلد 01، 2018.

2) ذنون يونس صالح المحمدي ومهمدي صالح شحادة العبيدي، التعويض الناشئ عن الاعتداء على حرمة الحياة الخاصة، مجلة جامعة تكريت للحقوق، العراق، 2018، المجلد 02، العدد 03، الجزء 01.

3) د. جمال براهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، جامعة مولود معمري، تيزي وزو، الجزائر، المجلد 11، العدد 02، نوفمبر 2016.

4) د. خديجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الالكترونية – دراسة مقارنة –، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 29، العدد 03، 2013.

5) أ. سوزان عدنان، انتهاك حرمة الحياة الخاصة عبر الأنترنت، مقال منشور في مجلة جامع دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث، 2013.

6) د. صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار، عنابة، كلية الحقوق والعلوم السياسية المجلد 24، العدد 02، 2018.

7) د. صليحة بوجادي، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، الجزائر، 2021.

8) د. عبد الحليم بن بادة، اجراءات البحث والتحري عن الجريمة المعلوماتية – الخصوصية والأركان، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 23، المجلد، جوان 2015.

9) د. عائشة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون، المجلد 2، العدد 6، المغرب، 2016.

10) أ. فهد عبد العزيز سعيد، دور تقنية المعلومات في حماية خصوصية البيانات، مركز التميز لأمن المعلومات، المقالات العلمية، جامعة الملك سعود، الرياض، 2010، ص 02.

11) د. محمد أمين خرشة، جرائم الاعتداء على الحياة الخاصة، مجلة الحقوق، الأردن، العدد 08، 2012.

12) د. محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، المجلد 01، العدد 01، الجلفة، 2009.

13) د. محمد نور الدين، الحماية الجنائية للحق في خصوصية المكالمات الهاتفية، دراسة تحليلية نقدية للقانون الكويتي والإماراتي، كلية القانون، جامعة الشارقة، عمادة البحث العلمي، مجلد رقم 43، 2016.

14) د. مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، قسنطينة، الجزائر، المجلد 07، العدد 01، 2018.

15) د. منة تركي الموسومي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلكين، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية 2013.

16) د. نسمة بطيحي، مجلة الفقه القانوني والسياسي، جامعة سطيف 02، الجزائر، المجلد 01، العدد 01، جوان 2019.

17) د. ونوغي نبيل، د. زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، المجلد 04، العدد 03، الجزائر، 2019.

18) د. يحي تومي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07، دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019.

المحاضرات

1) د. بن دراح علي ابراهيم، محاضرات ألقيت على طلبة السنة ثانية ماستر جنائي، كلية الحقوق والعلوم السياسية، المركز الجامعي آفلو، الجزائر.

2) أ. طه زروقي، بنية الآلة، محاضرات وتمارين ألقيت على طلبة السنة الأولى، كلية الاعلام الآلي جامعة البويرة، الجزائر، 2021.

3) د. لمعيني محمد، محاضرات ألقيت على طلبة السنة ثانية ماستر جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2015، 2016.

القوانين:

1) دستور سنة 1796، صادر بموجب الأمر 76-97 مؤرخ في 22 نوفمبر 1976 يتضمن إصدار دستور الجمهورية الجزائرية الديموقراطية الشعبية، الجريدة الرسمية رقم 94، الصادرة بتاريخ 24 نوفمبر 1976.
2) دستور 1996، صادر بموجب المرسوم رئاسي رقم 96-438 مؤرخ في 07 ديسمبر 1996 يتعلق بإصدار نص تعديل الدستور، المصادق عليه في استفتاء 28 نوفمبر 1996ن الجريدة الرسمية رقم 76، الصادرة بتاريخ 08 ديسمبر 1996.
3) دستور 2016، صادر بموجب القانون رقم 16-01 مؤرخ في 06 مارس 2016 يتضمن التعديل الدستوري، الجريدة الرسمية رقم 14، الصادرة بتاريخ 07 مارس 2016.
4) دستور 2020 صادر بموجب المرسوم الرئاسي رقم 20-442 مؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء نوفمبر 2020، جريدة رسمية رقم 82، صادرة بتاريخ في 30 ديسمبر 2020.

5) قانون رقم 2000-03 مؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية رقم 48، الصادرة بتاريخ 06 أوت 2000.
6) قانون 06-01 مؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، جريدة رسمية رقم 14، صادرة بتاريخ 08 مارس 2006.
7) القانون رقم 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. جريدة رسمية عدد 47، الصادرة بتاريخ 16 غشت 2009.
8) القانون رقم 15-03 المؤرخ 1 فبراير سنة 2015، المتعلق بعصرنة العدالة، الجريدة الرسمية رقم 06، الصادرة بتاريخ 10 فبراير 2015.
9) القانون 16-03 المؤرخ في 2016/06/19 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، الجريدة الرسمية رقم 37، الصادرة بتاريخ 22 يونيو 2016.
10) القانون رقم 18-04 مؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية رقم 27، صادرة بتاريخ 13 مايو 2018.
11) القانون 18-05 المؤرخ في 10 مايو 2018، المتعلق بالتجارة الالكترونية، ج ر، عدد 28، الصادرة في 16 مايو 2018.
12) القانون 18-07 مؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34، صادرة بتاريخ 10 يونيو 2018
13) قانون رقم 24-06 مؤرخ في 28 أبريل 2024، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية رقم 30، الصادرة بتاريخ 10 أبريل 2024.

المراسيم

1) مرسوم 88-131 مؤرخ في 04 يوليو 1988 ينظم العلاقة بيم الإدارة والمواطن، الجريدة الرسمية رقم 27، الصادرة بتاريخ 06 يوليو 1988.
2) المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما، الجريدة الرسمية رقم 53، صادرة بتاريخ 08 أكتوبر 2015.

فهرس
المحتويات

محتوى الفهرس	الصفحة
مقدمة	**01**
الفصل الأول: الإجرام المعلوماتي وصعوبة التحقيق	**08**
المبحث الأول: مفهوم الإجرام المعلوماتي وأركانه	**09**
المطلب الأول: تعريف الإجرام المعلوماتي	**09**
أولا: التعريف الضيق للجريمة المعلوماتية	**09**
ثانيا: التعريف الموسع للجريمة المعلوماتية	**10**
ثالثا: موقف المشرع الجزائري	**11**
المطلب الثاني: أركان الإجرام المعلوماتي	**13**
أولا: الركن الشرعي	**13**
ثانيا: الركن المادي	**15**
ثالثا: الركن المعنوي	**20**
رابعا: الركن المفترض	**22**
المبحث الثاني: صعوبة التحقيق في ظل وجود جريمة معلوماتية	**25**
المطلب الأول: انعكاس خصوصية الجريمة المعلوماتية على إجراءات التحقيق	**25**
المطلب الثاني: الضحية ودوره في إعاقة سير التحقيق في الجرائم	**29**
الفصل الثاني: الحق في الخصوصية المعلوماتية وأوجه حمايتها	**33**
المبحث الأول: مفهوم الحق في الخصوصية المعلوماتية ونطاقها	**34**
المطلب الأول: تعريف الحق في الخصوصية المعلوماتية	**34**
أولا: التعريف الفقهي للحق في الخصوصية	**34**
ثانيا: موقف المشرع الجزائري من الحق في الخصوصية	**37**
المطلب الثاني: نطاق الاعتداء على الحق في الخصوصية المعلوماتية	**40**
أولا: تعريف البيانات الشخصية	**40**
ثانيا: أنواع البيانات الشخصية	**41**
المبحث الثاني: أوجه الحماية الجزائية للحق في الخصوصية المعلوماتية	**45**
المطلب الأول: حماية سرية المراسلات والاتصالات الالكترونية	**45**
أولا: الحماية الدستورية لسرية المراسلات والاتصالات الإلكترونية	**46**
ثانيا: الحماية الجزائية لسرية المراسلات والاتصالات الإلكترونية	**46**
ثالثا: حماية سرية المراسلات والاتصالات في مجال البريد	**47**

رابعا: الاستثناءات الواردة على هذا القيد	**49**
المطلب الثاني: حماية الأشخاص الطبيعيين في مجال معالجة المعطيات	**52**
أولا: تعريف المعطيات ذات الطابع الشخصي	**52**
ثانيا: حقوق الشخص المعني بالمعالجة	**53**
ثالثا: الحماية الإدارية والجزائية لمعالجة المعطيات ذات الطابع الشخصي	**55**
خاتمة	**61**
قائمة المصادر والمراجع	**66**
فهرس المحتويات	**75**