جامعة أحـــــــمد درايـــــة - أدرار
كلية الحقوق والعلوم السياسية
قسم الحقوق

الحماية القانونية للبيانات الشخصية في التشريع الجزائري

أطروحة مقدمة لاستكمال متطلبات الحصول على شهادة دكتوراه الطور الثالث في الحقوق
تخصص: حقوق وحريات

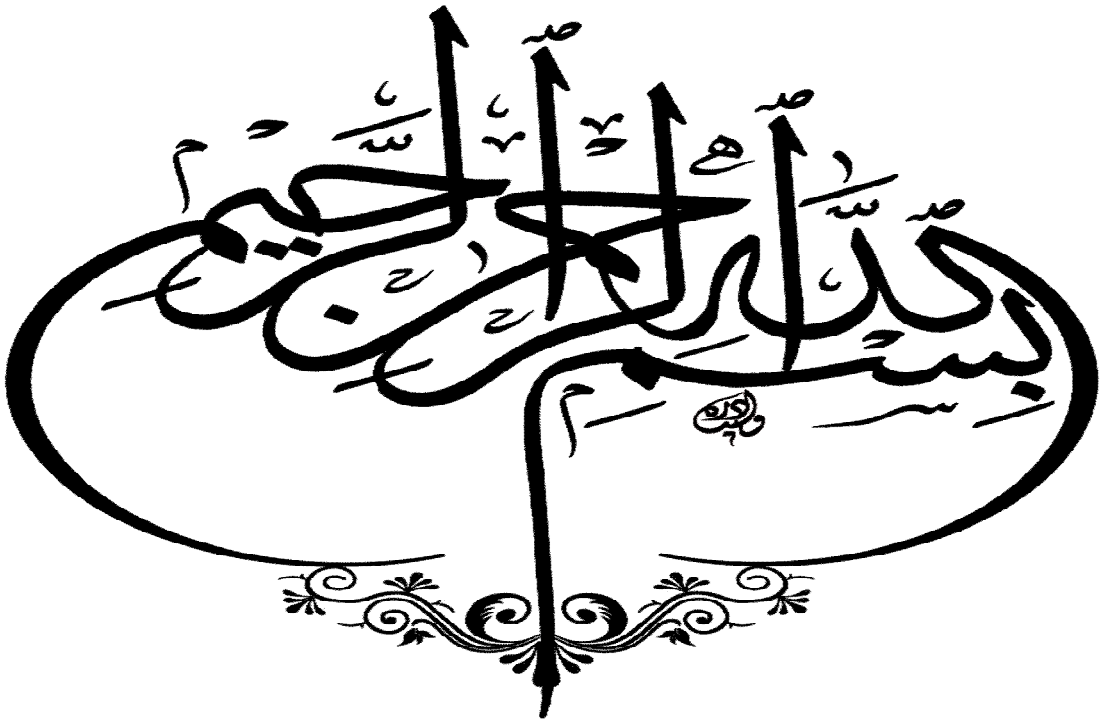
من إعداد الطالب:
كحلاوي عبد الهادي

الأستـــاذ المشـــــــرف:
أ.د/ بن زيطة عبد الهادي

لجنـــــــة المناقشة

أ.د يامة إبراهيـــــــــم	أستاذ التعليم العالي	جامعة أدرار	رئيســـــا
أ.د بن زيطة عبد الهادي	أستاذ التعليم العالي	جامعة أدرار	مشرفا ومقررا
أ.د رحمـــــــوني محمد	أستاذ التعليم العالي	جامعة أدرار	مناقشـــــا
د. كنتـــــاوي عبد الله	أستاذ محاضر .أ.	جامعة أدرار	مناقشـــــا
د. بركاوي عبد الرحمان	أستاذ محاضر .أ.	جامعة عين تموشنت	مناقشـــــا

السنة الجامعية: 2022/2021



{ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَا ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ (27) فَإِن لَّمۡ تَجِدُواْ فِيهَآ أَحَدٗا فَلَا تَدۡخُلُوهَا حَتَّىٰ يُؤۡذَنَ لَكُمۡ وَإِن قِيلَ لَكُمُ ٱرۡجِعُواْ فَٱرۡجِعُواْ هُوَ أَزۡكَىٰ لَكُمۡ وَٱللَّهُ بِمَا تَعۡمَلُونَ عَلِيمٞ (28) }

الآيتين 27 و28 من سورة النور برواية ورش عن نافع

إهداء

إلى والدي الشهم – رحمه الله رحمة واسعة-

إلى منبع الحنان وسر التوفيق، أمي الحبيبة –شفاها الله وبارك في عمرها.

إلى سكني ورفيقة دربي، زوجتي الغالية – أم الزهور.

إلى فلذات الكبد – رزان، أنس سعد ، سمية ومحمد أسامة- وفقنا الله لحسن تربيتهم.

إلى أختي العزيزة وإخوتي الكرماء بارك الله فيهم وفي ذريتهم

إلى أصدقائي الأعزاء، وكل من ساعدني حتى أتم هذا البحث.

إلى كل طالب علم أو محب للعلم وأهله..

الطالب

عبد الهادي كحلاوي

شكر وتقدير

الحمد لله أولاً وآخراً، ظاهراً وباطناً،

أما بعد:

قال المصطفى عليه الصلاة والسلام " لا يَشكُرُ اللّهَ من لا يَشكُرُ الناس"

رواه أبو هريرة/ صحيح أبي داود.

لايسعني في هذا المقام إلا أن أتقدم بالشكر الجزيل المقرون بالتقدير والاحترام لأستاذي الفاضل، الأستاذ الدكتور عبد الهادي بن زيطة، على كل ما شملني به من توجيه صائب، وتحفيز معين، وعلم غزير وخلق رفيع. فأقول جزاك الله عني كل خير وبارك في علمك ونفع بك ومتعك بلباس الصحة والعافية.

كما لايفوتني أن أتقدم بآيات الشكر والعرفان إلى جميع الأساتذة الكرام أعضاء اللجنة التكوينية، ومن خلالهم أعضاء لجنة المناقشة على قبولهم مناقشة هذه الأطروحة.

والشكر موصول كذلك لكل من أعانني على إنجاز هذا العمل بصورة مباشرة أوغير مباشرة، ولو بكلمة طيبة، فأسأل الله الكريم أن يجزيهم الجزاء الأوفى.

الطالب عبد الهادي كحلاوي

قائمة أهم المختصرات

الاختصار	الكلمة
السلطة الوطنية	السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي
ج. ر.ج.ج	الجريدة الرسمية للجمهورية الجزائرية
ح.م.ذ.ط.ش	حماية المعطيات ذات الطابع الشخصي
د.ب.ن	دون بلد النشر
د.ت.ص	دون تحديد الصفحة
د.د.ن	دون دار النشر
د.س.ط	دون سنة الطبع
ط	الطبعة
مج	المجلد
ع	العدد
C N I L	الهيئة الوطنية للمعلوماتية والحريات
G D P R	النظام الأوربي العام لحماية البيانات
Ed	Edition
N^0	Numéro
Op.cit	Ouvrage précédent cité
Vol	Volume
P	Page

مقدمة

مقدمة:

بادئ ذي بدء نحمد الله عزوجل الذي أرشدنا إلى حفـظ الخصوصية في أدق تفاصيلها، إذ أنها جزء لا يتجزء من حفظ نفس الإنسان وكرامته، كأولى الكليات الخمس حفظا، بعد حفظ الدين.

ولا يكاد يسلم أحد- في الوقت الراهن- من آثار المخاطر التي تهدد بيانات الأشخاص بفعل تأثير العالم التكنلوجي المنفتح وسرعة التطور الرقمي في مختلف المجالات المرتبطة بالأشخاص، لاسيما في مجال التواصل الإجتماعي، بالنظر للحجم الهائل لتدفق المعلومات التي تشتمل عليها، والمخزنة ضمن تطبيقات تشتمل على حجم أمان نسبي، ويمكن الوصول إلى جزء كبير منها ومعالجتها في بضع لحظات أو أقل من ذلك بكبسة زرعلى جهاز رقمي.

حيث اهتم التشريع الدولي بتكريس حماية الحياة الخاصة بموجب مختلف المواثيق الدولية على غرار الإعلان العالمي لحقوق الإنسان[1]، الذي أكد على حماية خصوصية الفرد بصفة عامة من خلال ما نصت عليه مادته الثانية عشر[2].

كما لاننكر الجانب الإيجابي للتطور التكنلوجي في مجال التواصل، لاسيما بفعل تأثير شبكة الإنترنت التي أسهمت في تقديم خدمات عالية المستوى في ظرف وجيز، إلا أن هذا الأثر الإيجابي يقتضي البحث عن إطار يضبط ويحمي حرمة البيانات الشخصية، بحيث تتأكد حماية هذه الأخيرة بفعل الاستعمال المفرط للوسائل التكنولوجية الحديثة والاعتماد عليها في مختلف مناحي الحياة ، الأمر الذي أثر من نواحي عدة على الخصوصية، من حيث رصد تنقلات الأفراد، أعمالهم وحركاتهم ، وتجميع وتحليل البيانات الشخصية

[1] الإعلان العالمي لحقوق الإنسان لسنة 1948، موقع منظمة الأمم المتحدة، منشور على الموقـــــع الالكتروني " "www.un.org/ar/universal-declaration-human-refights/index.htmail

[22] نصت المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"

المتعلقة باستعمال مختلف الوسائل التكنولوجية الحديثة في مجال الاتصال، على وجه الخصوص، على غرار تقنيات المراقبة بالكاميرات الرقمية، ومراقبة وسائل التواصل وغيرها. وهذا ما قد يؤثر سلبا على خصوصية البيانات المتداولة لاسيما إذا استغلت المعلومات والبيانات المجمعة لغايات وأغراض مختلفة تعود بالسلب على أصحابها.

كما أن البيانات الشخصية المحفوظة يدويا، يمكنها أن تواجه خطر المعالجة غير المشروعة، مما دفع بالعديد من التشريعات الدولية إلى الاهتمام بمجال حماية البيانات الشخصية بمختلف كيفيات معالجتها، آلية أو غير آلية.

وتزامنا مع ظهور الإنترنت والانتشار الواسع لاستعمالها باعتماد مختلف تقنيات الحاسوب والتطبيقات الحديثة، لاسيما تلك المتعلقة بالتواصل الاجتماعي، وانعكاساتها السلبية على خصوصية البيانات المجمعة أو المعالجة، دفع بالعديد من الدول والمنظمات الإقليمية والعالمية إلى سن تشريعات تكفل التقليل من خطر مختلف التقنيات الحديثة والسريعة التطور، على البيانات الشخصية، داخل الدول، أو على المستويين الإقليمي و الدولي. حيث برز دور كل من منظمة الأمم المتحدة، من خلال العديد من المؤتمرات والقرارات المتعلقة بمجال حماية البيانات الشخصية، هذا إلى جانب منظمة التعاون الاقتصادي والتنمية، والعديد من المنظمات الإقليمية ، لاسيما الإتحاد الأوروبي والدور البارز لمجلس أوروبا، من خلال تبني العديد من الاتفاقيات والتوصيات، إلى جانب سن قواعد إرشادية ونظام موحد للحماية الإقليمية للبيانات الشخصية.

كما اهتمت بعض المنظمات الإقليمية الأخرى، على غر ار الجامعة العربية والاتحاد الإفريقي، بمجال حماية البيانات الشخصية سواء بسن اتفاقيات تخص مجال حماية البيانات الشخصية بصفة مباشرة، أو بتكريس اتفاقيات لمكافحة الجرائم المرتبطة بالتقنيات الحديثة، والتي تكرس بصورة غير مباشرة حماية البيانات الشخصية، المعالجة آليا من الجرائم المرتبطة بتقنية المعلومات.

كما كرس المؤسس الدستوري الجزائري إلى جانب حماية الحق في الخصوصية، التأكيد على حماية المعطيات الشخصية من خلال التعديل الدستوري لسنة 2016، بموجب

أحكام المادة 46 منه[1]، كما نص على ذلك ضمن التعديل الدستوري الأخير بتاريخ نوفمبر 2020، وفق ما نصت عليه المادة 47 منه، والتي تضمنت فقرتها الأخير تين ما يلي "حماية الأشخاص الطبيعيين عند معالجة معطياتهم ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق"[2]

ومن الجدير بالذكر أن المشرع الجزائري نص في العديد من النصوص القانونية على تكريس حماية خصوصية البيانات الشخصية، بصورة غير مباشرة، من خلال تعديل العديد من النصوص القانونية على غرار قانون العقوبات، قانون الإجراءات الجزائية، و القانون المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية ..

كما تكللت الجهود التشريعية في مجال حماية المعطيات الشخصية وطنيا بإصدار القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[3]. والذي تضمن العديد من التدابير المتعلقة بحماية المعطيات ذات الطابع الشخصي المتعلقة بالأشخاص الطبيعيين، والذي سيتم تفصيل مختلف مضامينه والوقوف على مدى تكرسيه، إلى جانب مختلف النصوص القانونية الأخرى، لحماية البيانات ذات الطابع الشخصي وطنيا، في ظل الانتشار الواسع لاستعمال التكنولوجيات الرقمية، من قبل الأفراد والهيئات على حد سواء.

وعليه فإن المجال المحدد لموضوع دراستنا هذه يشمل مختلف الجوانب المتعلقة بحماية البيانات الشخصية في التشريع الجزائري، انطلاقا من مضمون مختلف النصوص القانونية بغض النظر عن المصطلحات المستعملة، على غرار مصطلح المعطيات ذات الطابع

---

[1] نصت الفقرة الأخيرة من المادة 46 من الدستور الجزائري، المعدل سنة 2016 على أن " حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه".

[2] دستور الجمهورية الجزائرية الديمقراطية الشعبية، المعدل سنة 2016 و 2020 ب:

- القانون رقم 16-01 المؤرخ في 6 مارس 2016 – ج.ر.ج.ج، عدد 14 المؤرخة في 2016/03/7.
- المرسوم الرئاسي رقم 20-442 المؤرخ في في 30 ديسمبر 2020، ج.ر.ج.ج، عدد 82، المؤرخة في 30 ديسمبر 2020.

[3] القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج، عدد 34، المؤرخة في 10 يونيو 2018.

الشخصي، مع التطرق إلى مضامين أهم المواثيق الدولية، مع توضيح موقف المشرع الجزائري من حيث الانضمام من عدمه.

وعليه حاولنا، من خلال هذه الدراسة، عرض مختلف الجرائم الماسة بالبيانات الشخصية والجزاءات المترتبة لمكافحتها، مع الوقوف على مضامين النصوص القانونية التي تتناول مجال البيانات الشخصية بصفة مباشرة، على غرار القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

كما أن أهمية موضوع هذه الدراسة تتجلى من خلال إسهام الاستعمال المفرط للوسائل التكنولوجية في مجال التواصل، ومعالجة مختلف المعلومات رقميا، في بروز العديد من الجرائم الماسة بحرمة المعطيات الشخصية، وأسهمت بصورة كبيرة في كشف جوانب متعددة من الخصوصية، مما أدى إلى دق ناقوس الخطر، ودفع بمختلف الباحثين القانونيين، إلى محاولة ضبط إطار إجرائي وجزائي لكبح الآثار السلبية لانتشار التكنولوجيات الرقمية على خصوصية البيانات، لاسيما تلك المتداولة عبر الحواسيب الآلية المربوطة بشبكة الإنترنت.

كما أن أغلب التعاملات في الوقت الحالي ترتكز على استعمال التكنولوجيات الرقمية، سواء في المجال التجاري، البنكي، الدراسي، الصحي، وغيرها، مما يستدعي توفير بيئة آمنة تتوفر على جميع الضمانات المناسبة، ليقوم الفرد بمختلف معاملاته بكل ثقة، ومسؤولية، سواء أكان معنيا بمعالجة معطياته، أو كان في حد ذاته معالجا أو مسؤولا عن المعالجة، إذا أدرك حقوقه المكرسة قانونا في الأولى، وواجباته ومسؤولياته المدنية والجنائية في الثانية.

وعليه تتجلى أهمية هذه الدراسة في بحث الضمانات المقررة من قبل المشرع الجزائري، والوقوف على مواطن الخلل، والاستلهام من التجارب التشريعية الدولية الرائدة في مجال حماية البيانات الشخصية المتعلقة بالأشخاص الطبيعيين.

ومن خلال كل ما سبق توضيحه، فإن الدافع الأساس لاختيار الموضوع هو الجانب الموضوعي، والمتجسد في استفحال ظاهرة استغلال البيانات الشخصية المتعلقة بالأشخاص الطبيعيين على وجه الخصوص، من أجل أغراض شتى، هدفها الرئيس هو المساس بحقوق الشخص المعني بالبيانات، كما قد يتعدى ذلك إلى المساس بالتركيبة المجتمعية وتماسكها، عند استهداف بيانات شخصية تخص فئات خاصة في المجمتع، كالأطفال مثلا. كما أن الضرورة التي تقتضيها التطورات التكنولوجية للتماشي مع مختلف التغيرات، التي بالرغم من آثارها السلبية، إلا أنها تحمل الكثير من الإيجابيات وتقريب المسافات وتوفير الجهد، مما يقتضي وضع إطار مناسب يكرس المعالجة الشرعية الموضوعية للبيانات الشخصية ويجرم كل انتهاك لخصوصية هذه البيانات .

وفي السياق ذاته، لا أنكر الميل الشخصي إلى بحث المواضيع المتعلقة بحماية الحقوق والحريات المرتبطة بالمجالات الرقمية المستجدة، بالنظر لما يحيط بهذا المجال من مسائل هامة ومتجددة تلامس اهتماماتي الشخصية والوظيفية، وكذا تمس تفاصيل شخصية لفئات كبيرة من المجتمع.

ويندرج الهدف الأساس لبحث هذا الموضوع ضمن معرفة مدى تكريس المشرع الجزائري لحماية البيانات الشخصية، مقارنة بالجهود التشريعية الدولية الجماعية والإقليمية، وحتى الوطنية على مستوى الكثير من الدول الغربية منهاو العربية، لاسيما تلك التي كان لها السبق في تكريس الحماية القانونية للبيانات الشخصية، هذا إلى جانب التنبيه على مخاطر التقنيات الحديثة على المعطيات الشخصية، مع الوقوف على ضوابط معالجة هذه المعطيات، والجزاءات المترتبة في حالة الإخلال بالالتزامات.

كما يمكن تلخيص أهم الدراسات السابقة المرتبطة بموضوع بحثنا هذا كما يلي:

- أطروحة دكتوراه موسومة ب" الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الإتفاقي والقانون الوطني، لمؤلفتها " الدكتورة مروة زين العابدين صالح، تاريخ المناقشة 2014، تطرقت الدراسة إلى الآليات الدولية لحماية البيانات الشخصية من خلال التطرق لمخاطر شبكة الإنترنت على البيانات الشخصية

والحماية الجنائية لهذه البيانات المتداولة عبر شبكة الإنترنت، ولم تتطرق لدور الاتفاقيات الدولية الإقليمية العربية والإفريقية في حماية البيانات الشخصية باستثناء التطرق لبعض نماذج حماية بعض التشريعات الوطنية العربية للخصوصية ومكافحة الجريمة المعلوماتية .

- أطروحة دكتوراه موسومة ب" الحماية الجنائية لنظام المعالجة الآلية للمعطيات – دراسة مقارنة-، لمؤلفها " الدكتور الطيبي البركة، المناقشة خلال السنة الدراسية 2020-2021، تم التطرق فيها إلى إبراز دور التشريعات الدولية والتشريع الجزائري في تكريس الحماية الجنائية لنظام المعالجة الآلية للمعطيات، والتي تطرق فيها لجرائم المعالجة الآلية للمعطيات الشخصية في التشريع الجزائري، إلا أنه بالرغم لتفصيله لمختلف أحكام القوانين المتعلقة بحماية المعطيات الشخصية، إلا أنه أدرجها ضمن الحماية الجنائية فقط وفق ما يتماشى وموضوع الدراسة. بينما توجد العديد من الجوانب والتدابير الوقائية الإجرائية والمؤسساتية لحماية معالجة المعطيات الشخصية في القانون الجزائري، قبل اتخاذ مختلف الإجراءات الجزائية المقررة. وهو ماسيتم التفصيل فيه ضمن موضوع هذه الأطروحة.

- مقال علمي موسوم ب "الحماية القانونية للبيانات الشخصية – دراسة في القانون الفرنسي (القسم الأول)" منشور شهر سبتمبر 2011، و(القسم الثاني)، منشور شهر ديسمبر 2011، صاحب البحث: "الدكتور سامح عبد الواحد التهامي" ، حيث تلخصت محاور هذه الدراسات حول تقديم مفهوم البيانات الشخصية، وضوابط معالجتها في التشريع الفرنسي، مع الوقوف على مدى فعالية هيئة (CNIL)، كسلطة مكلفة بحماية البيانات الشخصية، في فرنسا، وهي تعد دراسة هامة ومرجعية حول موضوع حماية البيانات الشخصية في التشريع الفرنسي، الذي وضع أول قانون لحماية البيانات الشخصية وكرس إنشاء أول سلطة إدارية مستقلة لحماية البيانات منذ سنة 1978.

- مقال علمي موسوم ب" ضرورة إنشاء سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة استخدامات المعلوماتية" لمؤلفه " الدكتور بن زيطة عبد الهادي، المنشور بمجلة الحقيقة، جامعة أدرار، العدد 39، ديسمبر 2016" ، والذي

استشرف فيه تكريس آلية إدارية مؤسساتية لحماية البيانات الشخصية، في ظل الاستعمال المفرط للوسائل التكنلوجية في معالجة البيانات المتعلقة بالأفراد، لاسيما عند تشكيل بنوك معلومات مخزنة على مستوى الإدارات والمؤسسات المعنية، مما يعرضها لخطر الاستغلال غير المشروع، الأمر الذي يستدعي توفير ضمانات فعلية، وهوما تم تكريسه لاحقا بإنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، بموجب القانون 18-07، والتي سيتم التفصيل في مدى نجاعتها، والوصول إلى ما استشرفه الباحث، من عدمه، في العنصر المخصص حسب خطة بحثنا هذا.

و عليه تم طرح الإشكالية التي يدور حولها موضوع دراستنا هذه، على النحو التالي:
مامدى فعالية الحماية القانونية المكرسة من قبل المشرع الجزائري للبيانات الشخصية ؟

يندرج تحت هذه الإشكالية عدة أسئلة فرعية، تم صياغة الأساسية منها كما يلي:

- ما المقصود بالبيانات الشخصية؟
- فيم تتجسد أهم الضمانات والآليات القانونية الدولية لحماية البيانات الشخصية؟
- ماهي الضمانات القانونية الإجرائية، المؤسساتية والجزائية المكرسة من قبل المشرع الجزائري لحماية البيانات الشخصية؟

وللإجابة على هذه الإشكالية، تم اعتماد المنهج الوصفي من خلال التطرق لمضامين مختلف النصوص القانونية المتعلقة بحماية البيانات الشخصية، والوقوف على مدى نجاعتها وفعاليتها. كما تم الاستعانة بالمنهجين التحليلي والتاريخي، لتحليل مضامين مختلف النصوص القانونية وكذا مختلف الآليات المكرسة وتوضيح فعاليتها وانعكاساتها الإيجابية على مجال حماية البيانات الشخصية، بدراسة مختلف النصوص القانونية المتعلقة بمكافحة جرائم تقنية المعلومات. مع البحث في التشريعات الدولية والعربية، على وجه الخصوص، حول آليات تكريس هذه الحماية، مع مراعاة الترتيب الزمني لإصدار مختلف التشريعات، وصولا إلى إبراز موقف المشرع الجزائري لبيان مساهمة كل منها في إيجاد الاقتراحات والحلول الملائمة لما يثيره موضوع البحث من إشكالات.

كما أن أي باحث علمي لا بد وأن تواجهه صعوبات عند إعداد بحثه، قد تدفعه لشحذ همته والعمل بجهد أكبر للوصول إلى الغاية المرجوة. ومن أبرز الصعوبات المسجلة أثناء

معالجة موضوع دراستنا هذه هو تشعب موضوع البحث وقلة المراجع المتخصصة- عند بداية البحث-، لاسيما في السنتين الأوليين من اختيار موضوع البحث (2017 و2018)، تزامنا مع فرض إجراءات الحجر لمجابهة وباء كورونا، على غرار غلق المكتبات، وتأجيل أو صعوبة التنقل إلى المعارض الدولية للكتاب.

وقد تم اعتماد خطة من بابين أساسيين للإحاطة بمختلف جوانب إشكالية البحث.

حيث تم تخصيص الباب الأول لبسط الإطار المفاهيمي للبيانات الشخصية، مع الوقوف على الدوافع الملزمة لتكريس حماية هذه البيانات، ويتجلى ذلك من خلال تقسيم هذا الباب إلى فصلين، تم التطرق في الفصل الأول إلى مفهوم البيانات الشخصية، وعالج الفصل الثاني الدوافع الملزمة لحماية هذه البيانات.

أما موضوع الباب الثاني فتم تخصيصه للتدقيق في الآليات القانونية الدولية والوطنية لحماية البيانات الشخصية، وذلك بتقسيمه إلى فصلين، تم التطرق في الفصل الأول إلى الحماية الدولية للبيانات الشخصية، والثاني للحماية الوطنية للبيانات الشخصية. كما تناولت خاتمة هذا البحث أهم النتائج المتوصل إليها والتوصيات المتعلقة بها.

الباب الأول:
مفهوم البيانات الشخصية والدوافع الملزمة لحمايتها

الباب الأول: مفهوم البيانات الشخصية والدوافع الملزمة لحمايتها

يشكل مفهوم البيانات الشخصية المفتاح الأساس لضبط وتدقيق مجال الحماية لهذه البيانات، نظرا لاختلاف تنوع هذه المفاهيم بالرجوع إلى عاملي الزمن والبيئة التشريعية المعنية، لاسيما وأن هذه البيانات يمكن أن تتأثر بتطور مختلف المجالات الرقمية، مما يقتضي تكيف التشريع مع هذا التطور.

كما أن دوافع حماية البيانات تعد المنطلق الرئيس لتحيين وتكييف التشريعات الوطنية والدولية مع مختلف ما يعترضها من مساس بمجال خصوصيتها، لاسيما بتأثير شبكة الإنترنت على معالجة مختلف البيانات، وكنتيجة لاستقراء النتائج العلمية لمختلف الدراسات التقييمية لتأثير هذه الشبكة على المعلومات بصفة عامة والبيانات الشخصية بصفة خاصة، اهتم القانون الجنائي بجزء كبير من المجالات المعالجة للجانب السلبي لتأثير الإنترنت وما تسببه من جرائم معلوماتية، والتي لا يمكن ضبط حدودها بصفة دقيقة، لاسيما وأن مخرجاته تتجدد وتتغير بصورة سريعة جدا.

هذا في حين أن ضبط النص التشريعي يتم بعد ملاحظة نتائج هذا التطور على المجتمع بصفة عامة، وعلى البيانات الشخصية بصفة خاصة، لكونها موضوع دراستنا هذه. وعليه سيتم التطرق من خلال هذا الباب إلى عرض تفاصيل مختلف جوانب الخصوصية وعلاقتها بالبيانات الشخصية، مع التدقيق في تعاريف وأنواع البيانات الشخصية في الفصل الأول . ثم تخصيص الفصل الثاني لعرض وتدقيق مختلف الدوافع الملزمة لحماية البيانات الشخصية بالرجوع إلى آثار مختلف التكنولوجيات الرقمية وما لها من مخاطر على البيانات الشخصية، لاسيما تلك المتصلة بفضاء الإنترنت.

الفصل الأول: مفهوم البيانات الشخصية

لقد برز الاهتمام ببحث مصطلح البيانات الشخصية تزامنا مع الانتشار الواسع للإنترنت، وكذا تأثير الحواسيب ومختلف الأجهزة الرقمية على مجال سير ومعالجة المعلومات، لاسيما تلك المتعلقة بخصوصيات الأفراد، صورهم، توجهاتهم الفكرية والعقدية، مراسلاتهم، أبحاثهم، أرقامهم التعريفية السرية وغير السرية..الخ، كلها من جملة

الأسباب الدافعة إلى اهتمام المنظمات الدولية كذلك والتشريعات الوطنية بوضع مفهوم للبيانات الشخصية، يمكن من خلاله جمع مختلف التصورات لهذه البيانات المرتبطة بأمور دقيقة من شخصية الإنسان المعقدة.

وفي إطار موضوع دراستنا هذه، حاولنا جمع مختلف المفاهيم المقترحة للبيانات الشخصية، انطلاقا من الأساس اللغوي، الاصطلاحي الفقهي ثم التشريعي، وقبل كل ذلك عرجنا على الجانب التاريخي المتتبع لنشأة وتطور هذه الفكرة وعلاقتها بالخصوصية (المبحث الأول)، ثم التطرق إلى مختلف المفاهيم الفقهية والقانونية للبيانات الشخصية (المبحث الثاني).

المبحث الأول: المقصود بالخصوصية

من خلال عنوان هذا المبحث يتضح شقا الدراسة الخاصة بالجانب التاريخي لبروز فكرة البيانات الشخصية بدءاً بالتطور التاريخي للخصوصية، وهذا ما تم الوقوف عليه من خلال الدراسة المرجعية الخاصة بهذا الجانب، الذي لا يكاد ينفك عن المفاهيم العامة للخصوصية، سواء العلمية الفقهية منها، أو التشريعية، لاسيما تلك الواردة في المواثيق الدولية الخاصة بمجال تكريس حقوق الإنسان، والتي تعد حماية الخصوصية من بين أهم هذه الحقوق، وهو ما سيتم التطرق له في المطلب الأول من هذا المبحث. ليتم استخلاص جملة من النتائج التي تحدد العلاقة الموجودة بين الخصوصية والمعلومات أو البيانات ذات الطابع الشخصي، في إطار ما عنونا به المطلب الثاني ألا وهو خصوصية البيانات الشخصية.

المطلب الأول: تعريف الخصوصية وتطورها التاريخي

نظرا لكون الإطار الأول لحماية البيانات الشخصية هو الخصوصية فهي تعد حاضنة البيانات الشخصية ولذا كان من المناسب لمعالجة هذا الموضوع التطرق إلى مختلف التعاريف الاصطلاحية، الفقهية، الشرعية والتشريعية للإحاطة بمختلف جوانبها، وهو ما

سيتم تفصيله في الفرع الأول. كما سيتم دراسة تطورها التاريخي وصولا إلى خصوصية المعلومات والمعطيات الشخصية في الفرع الثاني من هذا لمطلب.

الفرع الأول: تعريف الخصوصية

سيتم التطرق إلى كل من التعريف اللغوي والاصطلاحي الفقهي والقانوني للخصوصية كما سيتم تفصيله أدناه:

أولا: التعريف اللغوي

الخصوصية لغة يقابلها العموم وهي من مصدر الفعل خص، فنقول اختصه بالشيء خصا و خصوصا وخصوصية وخصيصي[1]. كما أن لفظ الخصوصية ينصرف إلى الحصر وشدة الإطلاق، واستخصه استخصاصا طلب أن يكون خاصا به، والخاص ضد العام، يقال خاص لفلان أي منفرد له.[2]

ثانيا: التعريف الاصطلاحي

إن مصطلح الخصوصية في التشريعات الأنجلوساكسونية يتمحور في كل ما يخص شيئا دون غيره[3]، بينما ذهب المشرع الفرنسي إلى اعتماد مصطلح "الحياة الخاصة" باحترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي، حيث اتفق جانب من الفقه الأمريكي على أن الحق في الخصوصية يفسر ببقاء الشخص مجهولا، بعيدا عن فضول الناس،فهو أميل إلى الخلوة والوحدة[4].

وللإحاطة بهذا المفهوم سوف نتطرق له من مختلف الجوانب الشرعية، الفقهية والتشريعية على النحو التالي:

---

[1] القاموس المحيط، محمد الدين محمد بن يعقوب الفيروز آبادي، دار الحديث، القاهرة، ص 471.

[2] معجم محيط المحيط، تأليف المعلم بطرس البستان، مكتبة لبنان ناشرون، 1998، ص235.

[3] شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية –دراسة مقارنة، دار الفكر والقانون، المنصورة، سنة 2015، ص03.

[4] جليلة بنت صالح نعمان، حق الخصوصية دراسة مقارنة بين القانون الإسلامي والقانون الوضعي- القانون الجزائري أنموذجا، مجلة الشريعة والاقتصاد، جامعة الإخوة منتوري – قسنطينة، عدد10، المجلد05، سنة 2016، ص220.

أ- في فقه الشريعة:

لقد كفلت الشريعة الإسلامية الحماية لمختلف الحقوق والحريات المتعلقة بصون كرامة الإنسان، لاسيما تلك التي تدخل ضمن أسراره وخصوصياته، فهي من آكد الحقوق المكفولة شرعا، والتي تجسدها الخصوصية، باعتماد النظرة الشاملة لجميع جوانبها، من خلال مراعاة آداب الاستئذان قبل الدخول لأي مسكن[1]. كذلك تم النهي عن التجسس بأي صورة كانت حفاظا على خصوصية الأفراد[2]. إلا أنه ولعدم ورود تعريف مباشر للخصوصية في الشريعة الإسلامية فإن هناك اجتهادات لبعض الفقهاء قياسا بمواضيع ذات صلة بموضوع الخصوصية، حيث عرفت ب" صيانة الحياة الشخصية والعائلية للإنسان بعيدا عن الانكشاف أو المفاجأة من الآخرين بغير رضاه، والحرص على أن تكون بعيدة عن كل أشكال وصور تدخل الغير، ويستوي بذلك أن يكون من الأقارب المقربين أم من الغير الذين ليست لهم صلة إطلاقا به، داخل بيته أو خارجه، وضمان قدر من الزمن يخلو فيه إلى نفسه، ويتصرف في أثنائه بحرية هو وأهل بيته إلى درجة يستطيع معها رد الاعتداء الواقع على هذه الحرمة دون أدنى مسؤولية، وتكليف الغير بمراعاة ذلك، وا لا تعرض للجزاء الشرعي"[3].

ومن خلال التفاصيل التي جاء بها هذا التعريف فإننا نرى أنه ألم بمختلف جوانب الخصوصية، وقيدها كذلك بالقيود الشرعية، حتى في حالة ما كان الغير المتدخل من أقرب الأقربين.

---

[1] كما جاء في الآية الكريمة رقم 27 من سورة النور ، يقول الله عز وجل " يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَا ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ".

[2] ودليل ذلك قول الله عز وجل في الآية 12من سورة الحجرات " يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرٗا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡمٞۖ وَلَا تَجَسَّسُواْ وَلَا يَغۡتَب بَّعۡضُكُم بَعۡضًاۚ أَيُحِبُّ أَحَدُكُمۡ أَن يَأۡكُلَ لَحۡمَ أَخِيهِ مَيۡتٗا فَكَرِهۡتُمُوهُۚ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ تَوَّابٞ رَّحِيمٞ".

[3] حسني الجندي، ضمانات حرمة الحياة الخاصة في الإسلام، دار النهضة العربية، ط1، سنة 1993، مصر، القاهرة ص46، نقلا عن جليلة بنت صالح نعمان، المرجع السابق، ص217-218.

ب- عند فقهاء القانون:

أعطى الفقهاء اهتماما متفاوتا، في الدقة والإحاطة، لتعريف الخصوصية، بحيث عرفها الفقيه الفرنسي **بادينتر** بأنها" كل ما ليس له علاقة بالحياة العامة، أو هي كل مالا يعتبر من الحياة العامة"[1].

كما ذهب الفقية **ميشال** إلى تو يف الحق في الخصوصية بأنه" حق في الخلوة أي أنها رغبة الإنسان في الوحدة والألفة والتخفي والتحفظ"[2].

وعرفها **لبرنديسو وارن** بأنها " مفهوم يرتبط بكيان الإنسان أو بحيزه الخاص الذي يسعى من خلاله إلى حماية مشاعره وأفكاره وأسراره الخاصة تجسيداً لكينونته الفردية "[3].

وقد ذهب رأي من الفقه الأمريكي إلى تعريف الحق في الخصوصية بأنها " الحق في الخلوة، فمن حق الشخص أن يستلزم من الغير أن يتركوه وشأنه ولايعكر عليه أحد صفو خلوته"[4].

وعرف **روبرسون** الحق في الخصوصية بأنه "الحق في أن يعيش الإنسان بعيدا عن العلانية "[5].

كما أشار الفقيه **نيرسون** في تعريفه الخصوصية بكونها " الالتزام بالتحفظ الذي يمكن الشخص المعني من عدم تعريض شخصيته للغير بدون موافقة، حيث تمكنه هذه الطريقة

---

[1] مقتبسة عن سليم جلاد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، المرجع نفسه، ص13.

[2] مقتبسة عن سليم جلاد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، المرجع نفسه، ص14

[3] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط1 ، بيروت،2017 ، ص22.

[4] مقتبسة عن: ماروك نصر الدين، الحق في الخصوصية، مجلة كلية العلوم الإسلامية- الصراط-، السنة الرابعة، العدد السابع، ربيع الثاني 1424هـ، جوان 2003م، ص108، رابط المقال" "https://www.asjp.cerist.dz/en/downArticle/412/5/1/84523

[5] عبد العزيز محمد سرحان،الاتفاقية الأوروبية لحقوق الإنسان، دار النهضة العربية، القاهرة، 1966، ص326.

بأن يترك وشأنه متمتعا بالسلم المطلوب، كما باستطاعته الاعتزال عن الناس والخلوة مع نفسه "[1].

ومن وجهة نظر القاضي الأمريكي **دوغلاس** فإنها تعني "حق الفرد في اختيار نمط سلوكه وتصرفاته الفردية في الحياة في ظل اختلاطه ومشاركته مع مختلف تركيبات المجتمع، حياته الاجتماعية الخاصة "[2].

ومن جهته **ألن ويستين** عرف الخصوصية بأنها رغبة بشرية مميزة، تجسد حق الأفراد أو الجماعات في أن يقرروا بأنفسهم زمن ومدى وكيفية مشاركة المعلومات الشخصية مع الآخرين، و تم التركيز على المشاركة الاجتماعية، بإبراز قدرة الفرد على الانسحاب الطوعي والمؤقت من المجتمع العام عبر وسائل مادية أو نفسية قصد تحقيق التوازن بين الخصوصية والمشاركة[3]

كما صدر عن مؤتمر رجال القانون المنعقد بعاصمة السويد " ستوكهولم " سنة 1967 تعريفا للخصوصية بأنها: " حق الفرد في أن يعيش بعيدا عن جملة من الأفعال تشمل:

- الاعتداء على مكانته، سمعته، اعتباره وشرفه.
- المساس بالكيان البدني أو المعنوي للفرد والتدخل في حريته الأخلاقية العامة.
- التدخل في حياته الخاصة.
- إفشاء معلوماته المتحصل عليها بطبيعة مهامه أو مهنته وكذا هامش الأمان والثقة التي يحظى بهما.
- التدخل في مراسلاته واتصالاته الشخصية، بالاستخدام غير الشرعي لوسائل الاتصال المتنوعة.

---

[1] آدم عبد البديع آدم حسن، الحق في الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2000، ص 170

[2] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، سنة 2016، ط1، ص38.

[3] ريموند واكس، الخصوصية مقدمة قصيرة جدا، ترجمة ياسر حسن، مراجعة هاني فتحي سليمان، مؤسسة هنداوي للتعليم والثقافة، القاهرة، مصر، ط01، سنة 2013، ص44.

- الاستعمال التعسفي لصورته أو اسمه وانتهاك حقه في السرية عن طريق التجسس والتلصص والملاحظة.
- بث الوقائع المتعلقة بأموره وتصرفاته ومعلوماته الشخصية"[1].

وورد ضمن توصية الجمعية الاستشارية للمجلس الأوروبي بتاريخ 23 يناير 1970، تعريف الخصوصية ب: " استطاعة الفرد توجيه حياته كيف شاء مع أدنى حد من التدخل، ويعتبر من الحياة الخاصة: الحياة العائلية، ما يتعلق بسلامة الجسم، الشرف والاعتبار، إعطاء صورة غير صحيحة عن الشخص والكشف عن وقائع غير مفيدة من شأنها أن تسبب الحيرة والحرج للشخص، نشر الصور الفوتوغرافية دون إذن الشخص، الحماية ضد التجسس والفضولية غير المقبولة والتي تكون بدون مبرر، الحماية ضد استعمال الاتصالات الخاصة والحماية ضد كشف أي معلومة خاصة التي قد يبلغ بعض الأشخاص العلم بها"[2].

ج. في التشريع:

تضمنت المادة 15 من الإعلان العالمي لحقوق الإنسان تعريفا للخصوصية بأنها " لا يُعرض أي شخص لأي تدخل في حياته الخاصة، رسائله، أسرته أو مسكنه، بصورة تعسفية أو القيام بشن حملات تستهدف شرفه وسمعته، كما يتاح الحق لكل شخص في أن يطلب الحماية القانونية له ضد كل أنواع التدخلات والحملات ".

كما ورد في القرارات الصادرة عن المحاكم في الولايات المتحدة تعريفا للخصوصية بأنها " التدخل غير المبرر في عزلة الغير، واستغلال اسم المرء، أو شكله، والدعاية وتسليط الضوء الزائف على المرء، والدعاية غير المبررة لحياة المرء الخاصة".[3]

---

[1] الشافعي محمد بشير، قانون حقوق الإنسان- مصادره وتطبيقاته الوطنية والدولية، مصر – منشأة المعارف، ط05، 2005، ص157-158.

[2] حسين إبراهيم خليل، تطبيقات قضائية على جريمة الإزعاج المعتمد عن طرق وسائل الاتصال الحديثة، مصر- دار الفكر والقانون للنشر والتوزيع، ط1، 2015، ص6.

[3] ريم بلحسن، أحمد بولباري، الحق في خصوصية المعطيات الشخصية في التشريع الجزائري –دراسة في ظل القانون رقم 18-07، مجلة العلوم القانونية والاجتماعية، المجلد الخامس، العدد الثالث، سبتمبر 2020، ص242.

لكن بتأثير التحول التكنولوجي والحواسيب الآلية، بدأ مفهوم الخصوصية في التحول من الخصوصية المادية إلى الخصوصية المعلوماتية ليشمل "حق الفرد في التحكم في تداول المعلومات المتعلقة به أو له، هذا التعريف الذي ينطوي على علاقة وثيقة بين الخصوصية والمعطيات الشخصية، على الرغم من أن حماية المعطيات الشخصية ليست مطابقة لحماية الخصوصية"[1].

وانطلاقا من هذه التعاريف نستخلص أن الخصوصية تتجسد في ذلك الحيز الشخصي الخاص بكل إنسان ينفرد فيه بنفسه في سكينة وسرية تامتين، قصد ضمان كتمان أسراره وكبح أي تدخل يستهدف الكشف عن معلومات حساسة سرية تكشف تفاصيل الحياة الخاصة[2].

وقد حدد بعض الفقهاء أركانا للخصوصية تتجسد في التحلي بالسرية والألفة، فأما التحلي بالسرية فيشمل جميع الأمور التي يخفيها الشخص عن الغير، والسكينة تشتمل على عدم التدخل في شؤون الغير وتركهم وشأنهم، أما الألفة فتشتمل الهدوء الممزوج بالبعد عن الآخرين في عزلة معينة[3].

ثالثا: الطبيعة القانونية للحق في الخصوصية:

أيد الفقيه بيكور الجانب الفقهي القائل بأن الحق في الخصوصية حق ملكية لا يمكن الاعتداء عليه في حين يحق لمالكه التصرف فيه تحت مبرر ضمان أكثر حماية، وما

---

[1] Ruth Gavison, Privacy and the limits of the law, in Michel J.Gorr and Sterling Harwood, eds, Crime and Punishment: Philosophic Explorations (Bwl;ontm CA: wadsworth, Publishing Co. 2000. Formerly Jones and Bartlett Publishers, 1996), pp 46-68

نقلا عن: مروة زين العابدين صالح، المرجع السابق، ص50-51.

[2] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية –الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت لبنان، سنة 2018، ص22.

[3] كريمة بوحجة، حماية البيانات الطبية الخاصة في العصر الرقمي –دراسة وصفية وتحليلية-، أطروحة دكتوراه، سنة 2014، ص 28-29.

يسجل في هذا الجانب الاتجاه التقليدي والنظرة المادية لحق الخصوصية والذي يتعارض مع خصائص الحق في الملكية في الكثير من الجوانب[1].

هذا في حين ذهب الفقيهين هوريو وبيني إلى اعتبار الحق في الحياة الخاصة بما في ذلك الحق في سرية المراسلات يدخل ضمن الحقوق الشخصية[2].

ومن جانبه جرم التقنين الجنائي الفرنسي منذ سنة 1804 إفشاء بعض الأسرار، حماية للحياة الخاصة للأفراد لاسيما في مواجهتهم للموظفين الأمناء على أسرار المواطنين بحكم وظيفتهم، كما أشار مضمون المادة 378 من قانون العقوبات الفرنسي القديم المذكور على "معاقبة الأطباء والجراحين، ومسؤولي الصحة والصيادلة والحكيمات وكل شخص مؤتمن بحكم حالته أو وظيفته على أو صفته المؤقتة على سر وقام بإفشائه في غير الحالات التي نص عليها القانون يعاقب بالحبس من شهر إلى ستة أشهر، والغرامة من 1200 إلى 6000 فرنك فرنسي" [3].

وقد تضمن قرار الجمعية العامة للأمم المتحدة بتاريخ 17 ديسمبر 2018، في دورتها الثالثة والسبعين تكريس الحق في الخصوصية الرقمية، حيث تم حث الدول الأعضاء على تكييف وتحيين تشريعاتها بصورة فعالة تكرس جزاءات مناسبة تتماشى وحماية هذا الحق وما يتطلبه كل ذلك من إنشاء مراصد وسلطات إدارية مستقلة تسند لها مهمة متابعة تكريس الحماية لكل الجوانب المتعلقة بالخصوصية، لاسيما عند معالجة المعطيات الشخصية، مع منح هذه السلطات مختلف المستلزمات المادية وكذا تكريس جملة من الصلاحيات لتوقيع الغرامات، والمتابعة القضائية، عند التعذر، وفق ما تقتضيه الالتزامات الدولية في هذا الجانب[4].

---

[1] جليلة بنت صالح نعمان، المرجع السابق، ص 222-224.

[2] سعد منور سعد البشتاوي، الحماية الدستورية للخصوصية المعلوماتية، المجلة الأردنية للمكتبات والمعلومات، مج(52)، ع2، الجامعة الأردنية مايو 2017، ص 110.

[3] شريف يوسف خاطر، حرية تداول المعلومات بين المنع والإباحة – دراسة مقارنة، دار الفكر والقانون، المنصورة-مصر، سنة 2015، ص32.

[4] تبينة حكيم، آليات الضبط الإداري لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، المجلة الجزائرية للعلوم السياسية والقانونية، المجلد 58، العدد: 01، سنة 2021، ص224.

والمشرع الجزائري، ضمن مواد القانون المدني، لم يشر صراحة إلى حماية الخصوصية، بالرغم من النص على دستورية حماية الحق في الحياة الخاصة[1].

بينما توجد نصوص قانونية أخرى أوردت بعض الاستثناءات لاسيما تلك المتعلقة بالإعلام وضمان حق النفاد إلى المعلومة حيث أكد نص المادة 93 من قانون الإعلام الجزائري على منع انتهاك الحياة الخاصة لأشخاص بصفة عامة وللشخصيات العمومية بصفة خاصة[2]، كما أكد نص المادة 2 من نفس القانون على حماية الخصوصية في جانبها المتعلق بسرية التحقيق واحترام كرامة الإنسان[3].

كما أشار القانون المتعلق بالنشاط السمعي البصري إلى جملة من الالتزامات الملقاة على عاتق طالب رخصة البث التلفزيوني أو الإذاعي وفق دفتر الشروط العام والتي من بينها حظر المساس بالحياة الخاصة وشرف وسمعة الأشخاص[4].

والأمر ذاته مكرس في قوانين الإعلام المغربية والتونسية حيث نصت المادة 89 من قانون الصحافة والنشر المغربي على حماية الحق في الصورة وفي الحياة الخاصة عموما حيث اعتبر المشرع المغربي كل تعرض لشخص يمكن التعرف عليه عن طريق اختلاق ادعاءات أو إفشاء وقائع، أو صور فوتوغرافية أو أفلام حميمية لأشخاص دون رضا مسبق منهم يعد تدخلا واضحا في أحد جوانب الخصوصية.

كما تطرق المشرع التونسي ضمن القانون المتعلق بحرية الصحافة والطباعة والنشر إلى عدم تقييد حرية التعبير إلا بنص تشريعي، شريطة أن تكون الغاية مشروعة مع احترام حقوق وكرامة الآخرين[1].

---

[1] انظر نص المادة 47 من الأمر 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

[2] راجع المادة 93 من القانون العضوي 12-05 المؤرخ في 12 يناير 2012، المتعلق بالإعـــــلام، ج.ر.ج.ج عدد 02، المؤرخة في 15 يناير 2012.

[3] راجع المادة 02 من القانون 12-05، المرجع نفسه.

[4] راجع المادة 48 من القانون 14-04 المؤرخ في 2014/02/24، المتعلق بالنشاط السمعي البصري، الجريدة الرسمية عدد 16 بتاريخ 2014/03/23.

ولئن أقر المؤسس الدستوري الجزائري الحق في الحياة الخاصة على إطلاقه بموجب ما تضمنه نصي المادتين 39 و 63 من دستور 1996كانعكاس آلي لتطبيق الالتز امات الدولية تزامنا مع مصادقة الجزائر على مضامين العهد الدولي للحقوق المدنية والسياسية، إلا أنه واعتباراً لبعض الآثار السلبية لتكريس هذا الحق على إطلاقه، تم تقييد ممارسة هذا الحق وفقا لما أقرته العديد من النصوص القانونية والتنظيمية بجواز المساس ببعض الجوانب المرتبطة بالخصوصية، نظرا لاعتبارات قانونية محددة، على غرار تلك المرتبطة بتحقيق الصالح العام ومكافحة الجريمة، لاسيما تلك التي تمس بأنظمة معالجة المعطيات والجريمة العابرة للحدود الوطنية، وكذا الجرائم الماسة بأمن الدولة، وعليه وحسب ما يقتضيه كل ظرف فإنه في حالات محصورة يمكن التقييد من السلطة المطلقة للشخص في إطار احترام الخصوصية، بالموازاة مع المصلحة العامة، بالتقاط صور أو تنصت أو تسجيل أصوات[2].

ومن أمثلة هذا التقييد ما نصت عليه المادتين 03 و 04 من القانون 09-04، والتي حددت الحالات التي يمكن فيها اللجوء إلى المراقبة الإلكترونية في أربع مجالات، واردة على سبيل الحصر، ولغايات أمنية، إستراتيجية، أو لتنفيذ طلبات المساعدة القضائية الدولية المتبادلة، ولا يمكن إجراء هذه المراقبة إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة[3].

رابعا: أنواع الخصوصية: للخصوصية أنواع عدة حسب كل مجال وعليه سنركز على الأنواع التي تخص مجال هذا البحث كما يلي:

1-4 الخصوصية الشخصية: تشكل المجال الأول والأسبق للخصوصية بالنسبة للفرد، مقارنة بالمجالات الأخرى، بحيث تكفل له التعبير عن آرائه وتحديد ممتلكاته

---

[1] رضا هميسي، ضمان حق النفاد إلى المعلومات على ضوء الدساتير المغاربية، مجلة العلوم القانونية والسياسية، ع14، أكتوبر 2016، ص 249.

[2] بن حيدة محمد، مكانة الحق في الحياة الخاصة في ظل التعديل الدستوري 16-01، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد العاشر، المجلد الأول، جوان 2018، ص41.

[3] راجع المادتين 03 و04 من القانون 09-04، المؤرخ في 05 غشت 2009، المحدد للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام والاتصال ومكافحتها.

وطريقة عيشه، وقد أكد الإسلام على هذا النوع من الخصوصية أيما تأكيد بحيث رتبها ضمن أولوياته ورتب لحق الدفاع عنها جزاء إلى الاستشهاد في سبيل الله[1].

كما أكدت العديد من المواثيق الدولية على هذا النوع من الخصوصية على غرار ما أشار إليه الإعلان العالمي لحقوق الإنسان في مادته الثانية عشر(12)، والتي كرست منع التدخل التعسفي في الخصوصية الشخصية للفرد، والتي تشمل حياته الشخصية، مراسلاته، مسكنه وتفاصيل أسرته وصيانة سمعته وشرفه، مع التأكيد على أنه يتم التكفل بهذه التفاصيل بسن قوانين وطنية للحماية من أي انتهاك [2].

4-2 الخصوصية الدينية:

وهي لا تقل أهمية عن مقتضيات الخصوصية الشخصية، بالنظر لمضمونها وشموليتها، وأكد ذلك برهانا الدلائل والاستشهاد ضمن النصوص الشرعية المؤكدة على هذه الخصوصية في مجالها الواسع.

وقد أشار نص المادة 18 من الإعلان العالمي لحقوق الإنسان إلى أهمية هذا المجال من الخصوصية والتي جاء فيها " لكل شخص الحق في حرية التفكير والضمير والدين، ويشمل هذا الحق حرية تغيير ديانته أو عقيدته، وحرية الإعراب عنها بالتعليم والممارسة وا إقامة الشعائر ومراعاتها سواء أكان ذلك سراً أم مع الجماعة"[3].

ومن الجدير بالتوضيح أن أغلب المشرعين لمختلف القوانين الوضعية أكدوا ودافعوا وشجعوا على تكريس حرية المعتقد، بينما الواجب هو ضبط المجال بتوضيح الطريق الصحيح ألا وهو دين الإسلام، وكل ما عداه فهي سبل لا توصل إلى معنى الاعتقاد

[1] كريمة بوحجة، حماية البيانات الطبية الخاصة في العصر الرقمي –دراسة وصفية وتحليلية-، أطروحة دكتوراه، السنة الدراسية 2013-2014، جامعة الجزائر03- كلية علوم الإعلام والإتصال، ص47.

[2] راجع نص المادة 12 من الإعلان العالمي لحقوق الإنسان، المرجع السابق.

[3] كريمة بوحجة، المرجع السابق، ص47.

الصحيح، يقول الله عز وجل " وَمَنْ يَبْتَغِ غَيْرَ الْإِسْلَامِ دِينًا فَلَنْ يُقْبَلَ مِنْهُ وَهُوَ فِي الْآخِرَةِ مِنَ الْخَاسِرِينَ"[1].

3-4 خصوصية الاتصالات:

تشمل سرية مختلف الاتصالات، مهما كانت الوسيلة المستعملة فيها، وهي كذلك من أقدم أنواع الخصوصية، إلا أنه بتأثير الوسائل الحديثة فإن مجالها اتسع كثيرا ولعلها من أهم أهداف موضوع بحثنا الحالي لاسيما إذا ارتبطت بخصوصية الاتصالات الرقمية الحديثة.

وقد اهتمت أغلب التشريعات الدولية وكذا الدساتير على حماية خصوصية الاتصالات وهذا ما نص عليه الدستور الجزائري في مادته 47 والتي نصت في فقرتها الثانية أنه " لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت".

4-4 الخصوصية المعلوماتية:

تشكل الخصوصية المعلوماتية الحلقة الأساس الموصلة لمجال المعطيات والمعلومات الشخصية، بيد أن هذا التراكم من الكم المعلوماتي في حد ذاته يشمل جملة من البيانات المعالجة، حيث عرف كل من الدكتور سيد حسب الله وأحمد محمد الشامي المعلومات بأنها" البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاذ القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها، أو تفسيرها، أو تجميعها في شكل ذي معنى والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية أو في أي شكل"[2].

وعليه فإن خصوصية المعلومات تكتسي بالغ الأهمية في موضوع بحثنا هذا وعليه سنخصص المطلب الموالي للتفصيل حول نشأة وتطور خصوصية المعلومات.

---

[1] (سورة آل عمران، الآية 84)

[2] أحمد محمد الشامي، سيد حسب الله، الموسوعة العربية لمصطلحات علوم المكتبات والمعلومات والحاسبات، المكتبة الأكاديمية، القاهرة، سنة 2001، ص66، نقلا عن كريمة بوحجة، المرجع السابق، ص 49.

الفرع الثاني: التطور التاريخي للخصوصية

إن الخصوصية هي عبارة عن فكرة قديمة متجذرة منذ سالف العصور وحمايتها مكرسة بموجب مختلف التشريعات الدولية، كما أعطت الشرائع السماوية أهمية خاصة وأحاطتها بجانب من الحرمة حيث جاء في سفر التكوين ما يؤكد حرص آدم وحواء على ستر ما ظهر من سوءاتهما بعد وسوسة الشيطان لهما والاقتراب والأكل من الشجرة التي تمت مخالفة لأمر الخالق، الأمر كذالك في الديانة المسيحية، حيث جاء في إنجيل متى، النهي عن المساس بالحق في الحياة وتحريم الاطلاع على العورات والاقتراب من الزنا واعتبار غض البصر من أوكد الضروريات[1].

كما اهتمت الشريعة الإسلامية بالخصوصية أيما اهتمام من خلال حفظ العديد من صورها انطلاقا من مسكن الإنسان ومقر ستر عوراته بحيث نجد تكريس خصوصية وحرمة البيوت بصفة دقيقة ومؤكدة كجانب من جوانب الخصوصية، ولا أدل على ذلك من قول الله عز وجل، في الحث على آداب الاستئذان قبل إيلاج البيوت " يَا أَيُّهَا الَّذِينَ ءامَنُوا لَا تَدْخُلُوا بُيُوتاً غَيرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ"[2] بالإضافة إلى ذلك حفظ الأسرار وعدم إفشائها لاسيما بين الزوجين[3]،وكذا النهي عن التجسس[4] وتتبع آثار وعورات الغير، حفاظا على خصوصياتهم، حيث يقول الله سبحانه "وَلَا تَقْفُ مَا لَيْسَ لَكَ بِهِ عِلْمٌ إِنَّ السَّمْعَ وَالبَصَرَ وَالفُؤَادَ كُلُّ أُولَئِكَ كَانَ عَنْهُ مَسْئُولاً"[5].

---

[1] شريف يوسف خاطر، المرجع السابق، ص11.

[2] سورة النور، الآية 27.

[3] عن عبد الرحمن بن سعد قال سمعت أبا سعيد الخدري يقول قال رسول الله صلى الله عليه وسلم " إن أعظم الأمانة عند الله يوم القيامة الرجل يفضي إلى امرأته وتفضي إليه ثم ينشر سرها " صحيح مسلم ، الصفحة/ الرقم 1437.

[4] جاء في صحيح البخاري (5/1976، رقم 4849) حديث الرسول الله صلى الله عليه وسلم أنه قال " إياكم والظن فإن الظن أكذب الحديث، ولا تحسسوا، ولا تجسسوا، ولا تناجشوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا وكونوا عباد الله إخوانا"

[5] سورة الإسراء، الآية 36.

إلى جانب ذلك أكدت مختلف مضامين الشريعة الإسلامية حماية خصوصيات الفرد ونهت عن تتبع عوراته وحماية سرية مراسلاته وعدم جواز الاطلاع عليها[1]، بحيث اعترفت بحق الخصوصية اعترافا ضمنيا ولم يتم إيرادها مباشرة كمصطلح مثلما يتم التأكيد عليه في القوانين الوضعية المكرسة له.

كما أن نشأة فكرة الخصوصية تميزت بالارتباط الوثيق بالجانب المادي في التشريع الوضعي انطلاقا من الأفكار الأولية ذات النشأة الانجليزية مع ما تضمنته وثيقة الماجناكارتا الصادرة خلال القرن الثالث عشر ميلادي والتي تعد الميثاق العظيم للحريات في بريطانيا[2]، ثم تطورت مرحليا لتعم أيضا الجوانب المعنوية والتي قد ترتبط بها

[1] كما روي عن أبي برزة الأسلمي رضي الله عنه قال قال رسول الله صلى الله عليه وسلم " يا معشر من آمن بلسانه ولم يدخل الإيمان قلبه، لا تغتابوا المسلمين ولا تتبعوا عوراتهم، فإنه من اتبع عوراتهم يتبع الله عورته ومن يتبع الله عورته يفضحه في بيته" صحيح أبي داود، الصفحة/ الرقم 4880.

[2] "**الماجنا كارتا** أو**الميثاق الأعظم** هي وثيقة انجليزية صدرت لأول مرة عام 1215م. ثم صدرت مرة أخرى في عام 1216م. ولكن بنسخة ذات أحكام أقل، حيث ألغيت بعض الأحكام المؤقتة الموجودة في النسخة الأولى، خصوصاً تلك الأحكام التي توجه تهديدات صريحة إلى سلطة الحاكم وقد اعتمدت هذه الوثيقة قانوناً عام 1225م وما تزال النسخة التي صدرت عام 1297م ضمن كتب لوائح الأنظمة الداخلية لإنجلترا وويلز حتى الآن.

و قد وصفت تلك النسخة بأنها " الميثاق العظيم للحريات في إنجلترا والحريات في الغابة."

يحتوي ميثاق عام 1215م على أمور عدة منها مطالبة الملك بأن يمنح حريات معينة وأن يقبل بأن حريته لن تكون مطلقة، وأن يوافق علناً على عدم معاقبة أي " رجل حر"إلا بموجب قانون الدولة وهذا الحق ما زال قائماً حتى اليوم في هذه الدول.

كانت الماجنا كارتا أول وثيقةتُفرض على ملك إنجليزي من مجموعة من رعاياه، في محاولة للحد من نفوذه وحماية امتيازاتهم قانونياً، ولم تكن الماجنا كارتا أول ميثاق للحد من سلطة الملك فقد سبق هذا الميثاق ميثاق آخر للحريات عام 1100 وتأثر به تأثراً مباشراً وكان ذلك في عهد الملك هنري الأول، وبالرغم من أن للميثاق أهميةً لا يختلف عليها اثنان، إلا أن بحلول النصف الثاني من القرن التاسع عشر ألغيت معظم البنود التي كانت في قالبها الأصلي وبقيت ثلاثة بنود كجزء من قانون إنجلترا وويلز، وتعتبر عادةً كجزء من الدستور غير المدون.

و في مرسوم حديث "و مثير للجدل نوعاً ما" لقوانين اللوردات، استشهد بالماجنا كارتا كمثال على لوائح أنظمة داخلية دستورية لم يمكن إلغاؤها إلا بلوائح أنظمة داخلية جديدة تنوي استبدال القديمة بقوانين أكثر وضوحاً فضلاً على أن تلغيها.كان الميثاق جزاء مهماً من عملية تاريخية ممتدة أدت إلى حكم القانون الدستوري في الدول الناطقة بالإنجليزية. بالرغم من أن الماجنا كارتا أبعد من أن تكون فريدة في شكلها أو محتواها إلا أنها لم تنجح في كبح النفوذ الكبيرة للسلطان في تطبيقاتها خلال حقبة العصور الوسطى.

متاحة على الموقع الالكتروني، مدونة الدكتور وسلم نعمت إبراهيم السعدي، على الرابط " https://portal.arid.my/ar-LY/Posts/Details/96fde0a9-2a34-460d-a472-b - تاريخ آخر اطلاع 2022/02/20.

خصوصية البيانات الشخصية ارتباطا وثيقا، بسبب الاستخدام الواسع للوسائل التكنولوجية وتأثير تقات المعلومات وغير ها من وسائل الاتصال الشبكي المسهلة لتدفق المعطيات[1].

ومن جهته، كرس المشرع الفرنسي حماية الخصوصية منذ سنة 1804 من جوانب عدة تضمنها على الخصوص التقنين الجنائي والمدني كما تم التفصيل فيه سابقاً، حيث منعت فرنسا سنة 1858 نشر الحقائق الخاصة، مع إقرار عقوبات على المخالفين[2].

وفي نفس السياق، نصت الاتفاقية الأوربية لحقوق الإنسان لسنة 1950، بموجب مادتها الثامنة (08) على حماية الحياة الخاصة والحياة العائلية وحرمة المسكن وحماية المراسلات لكل فرد يوجد على إقليم أي من الدول الأطراف في هذه الاتفاقية، دون تفرقة بين مواطني هذه الدولة، ومواطني الدول الأطراف، أو غير الأطراف فيها[3].إلا أنه تجدر الإشارة إلى أن هذه الاتفاقية أوردت ضمن نفس المادة استثناءات لهذا الحق العام، وعدم تكريسه بصفة مطلقة، حيث أن الاعتبارات الخاصة بالوضعية الخاصة، العائلية، المسكن والمراسلات ليست على إطلاقها وا ٍنما توجد استثناءات إذا تعلق الأمر بمشروعية تدخل السلطات العامة في مباشرة هذا الحق إذا كان ذلك لازما في المجتمع الديمقراطي، للأمن الوطني، أو للأمن العام أو للرفاهية الاقتصادية للدولة، أو لحماية النظام والتصدي

[1] مروة زين العابدين صالح، المرجع السابق، ص13.

[2] مروة زين العابدين صالح، المرجع السابق، ص 33

[3] https://www.echr.coe.int/documents/convention_ENG.pdf "le14/06/2020 ."

ARTICLE 8, Right to respect for private and family life, 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

لمختلف أنواع الجرائم التي قد تتخذ من هذا الحق ذريعة للتستر، مع شمول الاستثناء مقتضيات الصحة، النظام والآداب العامة وحرمات الغير[1].

كما تم تكريس آليات لتفعيل هذه الاتفاقية والتي من أهمها مجلس التوجيه الأوروبي وكذا المحكمة الأوربية لحقوق الإنسان التي تم تكريسها بموجب البروتوكول الحادي عشر عام 1958، الملحق بالاتفاقية[2]، حيث نذكر من أبرز المستجدات التي تميزت بها هو منح الأفراد حق الإدعاء أمام المحكمة مباشرة لحماية الحريات والحقوق المرتبطة بخصوصيتهم الشخصية ومختلف الجوانب وصولا إلى تكريس حماية البيانات ذات الطابع الشخصي، من خلال فصل المحكمة في العديد من القضايا، التي تشمل هذه الجوانب[3].

وقد تم تناول فكرة الخصوصية المعلوماتية لأول مرة، خلال مؤتمر الأمم المتحدة لحقوق الانسان، المنعقد بطهران سنة 1968، حيث تناولت ورشة منه، موضوع تأثير التكنلوجيات الرقمية على حقوق وحريات الأفراد، والذي كان منطلقا للعديد من الدول لتحيين تشريعاتها وتضمينها بنصوص تخص حماية البيانات الشخصية، وبالخصوص إنشاء هيئات مستقلة تعنى بحماية ومراقبة معالجة بيانات الأفراد[4].

كما أدخل المؤسس الدستوري الأمريكي عدة تعديلات على الدستور الأمريكي سنة 1791 في إطار تكريس الحق في الخصوصية وذلك بإقرار حماية الأفراد جسديا في شخصهم ومساكنهم ووثائقهم وأملاكهم الشخصية، بحيث تم حظر العديد من الممارسات المسببة في انتهاك الخصوصية بأي شكل من الأشكال وكذا حظر كل أنواع التفتيش غير المرخصة رسميا، حيث وبالرغم من كون هذه التعديلات جاءت للتخفيف من شدة وتأثير

---

[1] الاتفاقية الأوروبية لحقوق الإنسان، في كتاب : حقوق الإنسان، مجموعة وثائق أوروبية، ترجمة الدكتور محمد أمين الميداني، والدكتور نزيه كسيبي، الطبعة الثانية، منشورات المعهد العربي لحقوق الإنسان، 2001، من ص 35 إلى ص 102.

[2] انظر المادة 65من الاتفاقية الأوروبية لحقوق الإنسان، المرجع السابق.

[3] رياض العجلاني، تطور إجراءات النظر في الطلبات الفردية أمام المحكمة الأوروبية لحقوق الإنسان،مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28 العدد الثاني، 2012، ص 165.

[4] بن زيطة عبد الهادي، ضرورة إنشاء سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة استخدامات المعلوماتية، مجلة الحقيقية، جامعة أدرار، العدد 39، ديسمبر 2016، ص71.

المخاوف المسجلة من قبل مناوئي الفيدرالية المعترضين على مضامين هذا التعديل الدستوري، إلا أنها كفلت العديد من الحريات الشخصية حيث سميت بوثيقة الحقوق والتي قدمها جيمس ماديسون في شكل مجموعة من النصوص التشريعية وعرضها للمصادقة من قبل الكونغرس الأمريكي بتاريخ 15 ديسمبر 1791 [1].

المطلب الثاني: نشأة وتطور مفهوم الخصوصية المعلوماتية

إن الحديث عن تطور مفهوم الخصوصية المعلوماتية يعكس الأهمية المرتبطة بالتسلسل التاريخي من المفهوم العام التقليدي للخصوصية بمختلف جوانبها لاسيما المادية منها، باعتبارها كحق لحماية الفرد من مظاهر الاعتداء المادي على حياته وما يرتبط بها من أمور شخصية مادية، كالأموال والمسكن وكل الممتلكات العقارية والمنقولة، ثم الوصول إلى الجانب الأكثر أهمية وهو الجانب المعنوي، الفكري، الذي يترجم في شكل الدفاع عن القيم والعناصر المعنوية للشخصية وصولا إلى الحديث عن الخصوصية كحق عام يكفل الحماية للشخص من مختلف الجوانب لاسيما المستجد منها بتأثير التكنولوجيا أو ما يسمى بحماية البيانات الشخصية[2] وهو ما سوف نتطرق له من خلال المجالين الفقهي (الفرع الأول) والقانوني (الفرع الثاني).

الفرع الأول: على الصعيد الفقهي

لقد سبق التطرق في المطلب الأول إلى تعريف الخصوصية بوجه عام وسرد تاريخها، وسنحاول من خلال هذا الفرع التطرق إلى تطور الخصوصية، وعلاقتها بالبيانات والمعلومات من خلال الملاحظات والدراسات التي توصل إليها الفقهاء والمهتمين بهذا المجال لاسيما خلال الفترة الممتدة من خمسينيات القرن الماضي إلى أواخر السبعينات، أين بدأت تظهر نواة تأثير تقنية المعلومات وازدياد مخاطر التقنية على الحياة الخاصة.

وفي هذا الإطار نذكر الفقيه ألان ويستن " Alan Westin" الذي ألف سنة 1967 كتابا حول الخصوصية والحرية انطلاقا مما ساد في المجتمع الأمريكي آنذاك من تدخل

[1] مروة زين العابدين صالح، المرجع السابق، ص33

[2] ريم بلحسن، أحمد بولباري، الحق في خصوصية المعطيات الشخصية في التشريع الجزائري، المرجع السابق، ص242.

في الحريات الشخصية وكان له أثر بارز في زيادة البحث والاهتمام بمجال حماية خصوصية المعطيات المعلوماتية، حيث تطرق في كتابه إلى تعريف الخصوصية المعلوماتية بأنها " الحق المخول للأفراد في اختيار متى وكيفـوا إلى أي مدى تصل معلومات تخصهم للغير "[1] .

كما ذهب الفقيه ميلر سنة 1971، إلى تقديم مفهوم لخصوصية المعلومات بأنها " مقدرة الأشخاص على التحكم في حركة المعلومات المتعلقة بهم"[2].

ومن خلال المقارنة بين هذين التعريفين نلاحظ تأكيد كليهما على وصول المعلومات للغير إلا أن التعريف الثاني للأستاذ ميلر كان أكثر دقة ووضوحا من حيث التأكيد على تحكم الشخص في الكشف عن بياناته أو عدم السماح بمعالجتها أو الولوج إليها، لاسيما وأن هذه البيانات قد تدخل ضمن أنظمة مشتركة على مستوى الأفراد والمؤسسات الحكومية علىوجه الخصوص.

وقد تم التطرق إلى هذه المسألة بالكثير من الاهتمام والبحث الميداني للفقيه **رول** ضمن كتابه بعنوان " قواعد الحياة الخاصة والرقابة العامة" حيث شمل العديد من الأنظمة المستعملة للبيانات الشخصية على غرار نظام الائتمان للمستهلكين بالولايات المتحدة الأمريكية في ظل التحديات التي يقوم بها الفرد، على الخصوص للتحكم في معالجة بياناته المجموعة والمخزنة وضبط الجوانب المتعلقة بالدفاع عنها ضد أي استغلال غير مشروع[3].

وقد علق الأستاذ فهد عبد العزيز سعود على مذكرة المبادئ الأساسية لأمن المعلومات الخاصة بوزارة الداخلية السعودية بأنها تضمنت تعريفا للبيانات الشخصية يرتبط من خلاله مفهوم الخصوصية بحماية البيانات والذي جاء فيه: " البيانات الشخصية تعني كل ما

---

[1] مقتبسة عن مروة زين العابدين صالح، المرجع السابق، ص42.

" The claim of individuals to determine for themselves when, how to what extent information about them is communicated to other"

[2] مقتبسة عن مروة زين العابدين صالح، المرجع نفسه، ص42

" The individual's ability to control the circulation of information relating to him"

[3] مروة زين العابدين صالح، المرجع نفسه، ص42.

يتعلق بالحياة الخاصة للإنسان كهويته وجنسيته واتجاهاته وميوله ومعتقداته وتعاملاته المالية والبنكية، فهي أي معلومات ترتبط بشخص معرف أو قابل للتعريف"[1]

الفرع الثاني: على الصعيد القانوني

تر تبط مفاهيم الخصوصية المعلوماتية للبيانات الشخصية في هذا الشق كذلك بنشأة قوانين حماية خصوصية المعطيات ذات الطابع الشخصي،بالنظر إلى التقارب الموجود والمسجل في جانب من المجالات الأساسية للخصوصية المعلوماتية الشخصية بالنظر إلى تأثير التطور التكنولوجي وزيادة ضخامة حجم المعلومات الشخصية المعالجة والقابلة للنقل إلى مسافات بعيدة في ظرف وجيز مما يتطلب إحاطتها بجانب حماية متخصص سواء من ناحية الإجراءات أو الآليات الفعلية المناسبة، وهو الأمر الذي تفاوتت فيه العديد من التشريعات الدولية مقارنة بالأخرى بتأثير جملة من العو امل أبرزها تطور تقنيات المعلومات والاعتماد على الحواسيب الآلية للمعالجة على مستوى القائمين بالمعالجة، أفرادا أو مؤسسات.

ومن هذا المنطلق بدأ التفكير دوليا من قبل منظمات دولية في إدراج توصيات واتفاقيات ومواثيق دولية، تمخض عنها تحيين لبعض التشريعات الداخلية لبعض الدول لاسيما الأورو بية منها لحماية البيانات ذات الطابع الشخصي، في ظل الانتشار الملحوظ للوسائل التقنية في معالجة هذه البيانات، والتي سهلت طرق الوصول إلى المعلومات المتعلقة بالأشخاص.

حيث نميز العديد من الجهود في هذا الإطار على المستويين الدولي والداخلي أي الفردي لكل دولة، والتي نذكر منها:

<u>أولا: على المستوىالدولي الجماعي و الإقليمي:</u>

لقد برزت العديد من الجهود الجماعية الدولية أسهمت في تكريس إطار عام مفاهيمي مهتم بخصوصية البيانات الشخصية، حيث وبالنظر للتسلسل الزمني المميز لصدور كل

[1] فهد عبد العزيز سعود، مفهوم الخصوصية وتاريخها -رؤية تقنية وا إسلامية، مركز التمييز لأمن المعلومات الرياض- السعودية، 2020، ص2.

من القواعد الإرشادية لمنظمة التعاون الاقتصادي والتنمية سنة 1980، ثم بعدها مضمون قرار الجمعية العامة للأمم المتحدة سنة 1990، المتضمن جملة من المبادئ لحماية خصوصية البيانات، ثم القواعد الأوروبية الإرشادية لحماية البيانات لسنة 1995 وسيتم التطرق لكل منها بشيء من التفصيل كما يلي:

1. **القواعد الإرشادية لمنظمة التعاون الاقتصادي والتنمية:** أصدر مجلس هذه الهيئة الدولية عام 1980 قواعد إرشادية لحماية الحق في الخصوصية المرتبطة بمجال البيانات الشخصية لضمان الاستغلال الشخصي لهذه البيانات بكل سلاسة وحرية.

حيث تضمنت هذه القواعد توصيات إلى البلدان الأعضاء تخص تكريس الحماية النسبية للحق في الخصوصية المعلوماتية للبيانات من جهة وحماية الحق في الانسياب والوصول الحر إلى المعلومات من جهة أخرى، وذلك بقيام الدول الأعضاء بسن قوانين تمنع عرقلة حركة تدفق البيانات عبر الحدود وتضمنت على الخصوص ثمانية مبادئ[1] وهي:

- مبدأ مشاركة صاحب البيانات.
- مبدأ الاستخدام المحدد.
- مبدأ الحد من جمع البيانات.
- مبدأ نوعية البيانات، بحيث تكون مأخوذة لتحقيق الغاية المرجوة حصرا.
- مبدأ الشفافية والانفتاح.
- مبدأ حماية وحفظ البيانات.
- مبدأ المسؤولية
- مبدأ الهدف المحدد.

[1] Annex to the Recommendation of the Council of 23rd September 1980 -OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htuy/'m"

وتجسيدا لهذه المبادئ صدرت الاتفاقية الأوروبية لسنة 1981 والتي ألزمت الدول الأعضاء على إتباع الخطوات اللازمة على المستوى التشريعي لتطبيق المبادئ التي تحددها توفيقا بين حماية الخصوصية المرتبطة بالبيانات وتكريس حرية تبادل المعلومات، حيث أن البارز في هذه الاتفاقية هو التوقيع عليها حتى من دول غير الأعضاء في الاتحاد الأوروبي على غرار المغرب، تونس، الأرجنتين، المكسيك وغيرها[1].

2. قرار الجمعية العامة للأمم المتحدة سنة 1990:

تضمن القرار رقم 45/95 لسنة 1990، الصادر عن الجمعية العامة للأمم المتحدة جملة من المبادئ المتعلقة بتوجيهات ضبط وتنظيم البيانات الشخصية المعالجة والمجموعة باستعمال الحاسب الالكتروني، وقد أكد هذا القرار على ضرورة قيام الدول الأعضاء ببسط رقابة داخلية مع إقرار عقوبات جزائية، ضمن القوانين الداخلية للدول المعنية، للمخالفين لمختلف المبادئ التي يتضمنها والتي تعد واجبة الالتزام من قبل الدول المعنية وتشمل هذه المبادئ ما يلي[2]:

-**مبدأ الأمن:** حيث يتضمن إلزام القائمين بجمع وحفظ البيانات بالالتزام بواجب التحفظ مع بذل العناية للحفاظ على هذه البيانات لعدم تلفها أو تسربها أو الاطلاع عليها دون إذن مسبق.

-**مبدأ صحة البيانات:** والذي يقتضي تحري دقة البيانات وملاءمتها حسب موضوع المعالجة والدافع لقيام المعالج بالاطلاع عليها مع تحمل مسؤولياته.

-**مبدأ عدم التمييز:** يشمل حظر التمييز العنصري بأي شكل من الأشكال خلال عمليات المعالجة المتعلقة بالمعطيات الشخصية سواء بسبب اللون، العرق، المعتقدات، الآراء السياسية وغيرها.

-**مبدأ النزاهة والشرعية:** يقتضي مضمون هذا الإجراء حظر أي شكل من أشكال الجمع أو المعالجة المتعلقة بالمعطيات الشخصية غير المرخصة والمخالفة للضوابط

[1] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية – الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية،المرجع السابق، ص52.

[2] منى الأشقر جبور، محمود جبور، المرجع نفسه، ص53.

المحددة قانونا، أو غير النزيهة بحيث تعكس عدم الانسجام مع مضمون مقاصد ميثاق الأمم المتحدة.

-**مبدأ وصول الأشخاص المعنيين بالبيانات لملفاتهم:** يتضمن حق الاطلاع للأشخاص على بياناتهم ومختلف الجوانب المتعلقة بها لتجنب أي مساس بها، في مختلف المراحل، عند الجمع، المعالجة أو التصحيح أو حتى الإلغاء أو المحو والذي يعد حقا أصيلا مكفولا للشخص المعني بمعالجة معطياته ويمكن الاحتجاج به في أي وقت شاء.

-**مبدأ تحديد وضبط الغاية من الجمع والمعالجة:** حفاظا على بيانات الأشخاص والتي تعد من أدق متطلبات الخصوصية فكان من اللازم توضيح وا ٍعلان أسباب ودوافع المعالجة مسبقا وضبط رقابة لاحقة للتأكد من مطابقة الغاية مع موضوع المعالجة مع اتخاذ الإجراءات والجوانب التقنية من قبل القائم بالمعالجة للتخلص الشرعي المضبوط من البيانات التي لم يعد بحاجة إليها، لاسيما عند الوصول إلى تحقيق أهداف المعالجة، المحددة مسبقا[1].

3. القواعد الأوروبية الإرشادية لحماية البيانات:

صدر سنة 1995 على المستوى الأوروبي من خلال الاتفاقية رقم 108 الخاصة بحماية الأفراد جملة من القواعد الهامة، المكرسة لجانب كبير من الحماية المتعلقة بمعالجة البيانات ذات الطابع الشخصي تزامنا مع مقتضيات الوضع الذي ساد آنذاك بتأثير الإنترنت والمعلومات والبيانات المتداولة دون رقابة أو حماية فعالة حيث شملت القواعد الأوروبية الواردة ضمن نص الاتفاقية الأوروبية رقم 108[2]، المبادئ التالية:

- مبدأ المعالجة المشروعة للمعلومات.
- الهدف المحدد والمحصور.

[1] منى الأشقر جبور، محمود جبور، المرجع السابق، ص54.

[2] راجع الإتفاقية الأوروبية رقم 108، المؤرخة في 28 يناير 1981، المتاحة على موقع مجلس أوروبا على الرابط التالي: "
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentI
."d=09000016802f7e03

- مبدأ نوعية البيانات
- مبدأ المسؤولية والمحاسبة.
- مبدأ المعالجة العادلة والشفافة.

وفي سنة 1997 تم إصدار دليل الاتصالات الذي سن شروطا لحماية خصوصية البيانات المتعلقة بالهاتف والتلفزيون الرقميين والأنشطة المتعلقة بالإنترنت وغيرها من الشبكات، حيث تم حث مختلف البلدان، أعضاء الاتحاد الأوروبي بتكريس التعديلات اللازمة للقوانين الوطنية لتتماشى وتجسيد المبادئ المذكورة ضمن هذا الدليل، حيث أسهمت هذه القواعد في سن حوالي 28 تشريعا وطنيا خاصا بحماية البيانات ذات الطابع الشخصي على مستوى دول الاتحاد الأوروبي نذكر منها صدور سنة 1998، على مستوى المملكة البريطانية تشريعا ينظم حماية البيانات والذي بموجب المبادئ المذكورة سابقا، ألغى التشريع السابق، المختص بنفس المجال لسنة 1984، لتكريس أكثر حماية لهذا الجانب المهم، المرتبط بخصوصيات الأفراد[1].

كما صدر سنة 2000 عن المفوضية الأوروبية نموذجا آخر لدليل ينظم ويضبط آليات معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الالكترونية والذي حل مكان الدليل المذكور أعلاه الصادر سنة 1997، حيث تضمن الدليل الجديد تكريسا أوسع لجوانب حق الأفراد في حماية بياناتهم وتضمين قواعد تخص التقنيات الحديثة ومختلف وسائل الاتصال على غرار البريد الالكتروني[2].

وتنفيذا للنظام 2001/45 الصادر عن البرلمان الأوروبي تم إحداث سلطة موحدة مشتركة لحماية ومراقبة معالجة البيانات على المستوى الأوروبي، تسمى المراقب الأوروبي لحماية البيانات[3].

---

[1] الشيخ الحسين محمد يحي، سيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية –دراسة مقارنة في القانون البريطاني والإماراتي، مجلة القضاء والقانون، مركز البحوث والدراسات القضائية، عدد 04، ابريل 2018، ص11.

[2] شريف يوسف خاطر، المرجع السابق، ص20.

[3] Loura MARCU, PROTECTION DES DONNES A CARACTERE PERSONNEL: QUELLES IMPLIQUATIONS POUR LES ACTIVITES DE MARKETING, Revue Valaque d'Etudes Economiques, Volume6(20) ,N^{0}1, 2015, p65.

كما تضمنت وثيقة الميثاق العربي لحقوق الإنسان المعتمد بتونس سنة 2004، جوانب من مجالات تكريس حماية الخصوصية بالنص صراحة على عدم جواز تعريض أي شخص للتدخل في خصوصياته أو مراسلاته أو شرفه أو سمعته بطرق تعسفية، مع حث الدول الأعضاء على تعديل أو تكريس تشريع جديد وطني يتطرق بالتفصيل لمختلف جوانب الحماية التي تشمل الحق الحياة الخاصة بدرجة أولى، وقد صادقت الجزائر على هذا الميثاق بموجب المرسوم الرئاسي 06-62[1]. وقد جاء التكريس القانوني تباعا بموجب أحكام القانون 18-07، المذكور سابقا.

كما صدر عن البرلمان والمجلس الأوروبيين، سنة 2016، نظاما عاما موحدا لحماية البيانات الشخصية على المستوى الأوروبي، من أخطار المعالجة الرقمية للبيانات الشخصية والتدفق الحر للمعلومات، تحت اسم " النظام الأوروبي الموحد لحماية البيانات الشخصية رقم 2016/607 "، والذي دخل حيز التنفيذ سنة 2018 بعد إلغاء القواعد السابقة و إصدار مدونة القواعد العامة لحماية البيانات والتي أعطت أكثر حقوق وضمانا للأشخاص فعلى سبيل الذكر تم تكريس حق المواطن المقيم في دول الاتحاد الأوروبي في طلب نسخة الكترونية عن بياناته للاطلاع عليها، والفارق بين هذه القواعد الشاملة وسابقتها هو درجة الإلزام وعدم الحاجة إلى تحيين التشريعات الداخلية لكل دولة عضو[2].

وعليه نظرا لأهمية هذه القواعد سيتم التطرق لها بشيء من التفصيل في الفصل المخصص لهذا الجانب لاحقا.

ثانيا: على المستوى الداخلي للدول:

إن الحديث عن تطور خصوصية البيانات على المستوى الداخلي للدول يتطلب العديد من الفصول ولكن سنقتصر في دراستنا هذه على التجارب السباقة في سن تشريعات حماية خصوصية البيانات والتي سيتم التعريج من خلالها على بعض التجارب للدول الأوروبية ثم العربية حسب التسلسل التاريخي.

[1] المرسوم الرئاسي رقم 06-62 المؤرخ في 11 فبراير 2006، المتضمن المصادقة على الميثاق العربي لحقوق الإنسان المعتمد بتونس في مايو سنة 2004، الجريدة الرسمية عدد08، المؤرخة في 15 فبراير 2006.

[2] منى الأشقر جبور، محمود جبور، المرجع السابق، ص56-58.

1. على المستوى الأوروبي:

لقد كان السبق لبعض الدول الأوروبية في سن قوانين لحماية خصوصية البيانات، فعلى مستوى بريطانيا كان تأثير وثيقة الماجناكرتا[1] واضحا منذ القرن الثالث عشر وما تبعه من سن العديد من القوانين المتعلقة بحماية الخصوصية حيث صدر عام 1361 قانون "The justices of the peace Acte" والذي سن حظر اختلاس النظر واستراق السمع وتضمن عقوبات الحبس في حالة الإخلال بذلك[2].

بعد صدور التوجيه الأوروبي لسنة 1995 وما تضمنه من بنود لتوحيد شروط حماية البيانات الشخصية وا ٍلزام مختلف دول الاتحاد الأوروبي بتحيين تشريعاتها الداخلية وفقها أصدرت بريطانيا سنة 1998 قانون حماية البيانات تنفيذا لذلك والذي ألغى تدابير قانون 1984 وأتى بتفاصيل جديدة تشمل في الأساس سن إجراءات وتدابير أكثر دقة ونجاعة لمعالجة البيانات الشخصية، مع تكريس العديد من الحقوق للمعنيين بمعالجة بياناتهم، وكذا التزامات القائمين بالمعالجة بالإضافة إلى إنشاء هيئة مستقلة للإشراف على تطبيق مختلف تدابير حماية البيانات الخاصة بالأفراد[3].

وفي سنة 1776 قام البرلمان السويدي بسن قانون الوصول إلى السجلات العامة، الذي ألزم مختلف الجهات الإدارية التي تحوز معلومات أن تستخدمها لأهداف مشروعة، كما تم سن تشريع محكم خاص بحماية البيانات في السويد سنة 1973[4].

وتعد ألمانيا الدولة الأوروبية الثالثة تاريخيا من حيث إصدار قوانين حماية خصوصية البيانات، حيث تم سنة 1988 إصدار قانون حماية المعطيات ليتم تعديله مرات عديدة أبرزها تعديل سنة 2000 ليتماشى والمبادئ والتوجيهات الأوروبية في هذا المجال[1].

---

[1] هي وثيقة انجليزية صدرت سنة 1215 تتضمن معظم الحقوق البريطانية التي بموجبها تنازل الملك عن سلطاته المطلقة وقد تم التفصيل في ذلك في المطلب الأول.

[2] مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، المرجع السابق، ص 32.

[3] الشيخ الحسين محمد يحي، سيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية –دراسة مقارنة في القانون البريطاني والإماراتي، المرجع السابق، ص47.

[4] مروة زين العابدين صالح، المرجع السابق، ص 47.

وبدوره المشرع الفرنسي وضع تشريعا لحماية البيانات الشخصية رقم 17 الصادر عام1978 ، حيث تضمن جملة من التدابير المكرسة لحقوق الأشخاص المعنيين بمعالجة معطياتهم ذات الطابع الشخصي، كما تم تعديل هذا القانون سنة 2004 بقصد توحيد إجراءات حماية معالجة البيانات سواء علـــــى مستوى الجهات الخاصة أو العامة، على حد سواء[2].

وبتاريخ 23 مايو 2018 تم المصادقة على دخول النظام الأوروبي لحماية البيانات الشخصية رقم 679/2016 حيز التنفيذ والذي كرس جملة من القواعد العامة لحماية البيانات الشخصية والتي بموجبها تم إلزام مختلف الدول الأعضاء لتكريسها على مستوى قوانينها الوطنية، أو الإحالة مباشرة إلى تطبيق مضامين هذا النظام العام، الذي تم بموجبة إلغاء التوجيهات الأوروبية لسنة 1995 [3].

2. على المستوى العربي:

بالرغم من الاهتمام المتأخر من قبل أغلب التشريعات العربية بشأن حماية المعطيات الشخصية مقارنة بالتشريعات الدولية التي كان لها السبق في هذا المجال، والذي ترجع أسبابه لعوامل عدة، إلا أنه ومع نهاية القرن الماضي تم الشروع في تكريس حماية هذا الجانب المهم من الحقوق والحريات، والذي نتطرق له حسب التسلسل التاريخي، تباعا، كما هو موضح أدناه:

في سنة 1999 أقر المشرع اللبناني، القانون رقم 140، المتعلق بصون الحق في سرية المخابرات التي تجري بواسطة أية وسيلة من وسائل الاتصال بموجب مادته الأولى، بالتأكيد على حماية التخابر بأية وسيلة من وسائل الاتصال، مع بسط الآليات المناسبة

---

[1] شريف يوسف خاطر، المرجع السابق، ص22.

[2] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي، مجلة الحقوق، جامعة الكويت، عدد04-السنة 35، ديسمبر 2011، ص408.

[3] اللائحة العامة لحماية البيانات GDPRK، ترجمة د.م حقوقي/مصطفى عبيد، موسوعة العلوم القانونية، مركز البحوث والدراسات متعدد التخصصات، ط1 ، يوليو 2018، متاحة على الرابط "
https://www.mdrscenter.com/%D8%A7%D9%84%D9%84%D8%A7%D8%A6%D8%AD% AA-
/gdpr "

لحماية البريد الالكتروني، في حين تم السماح، في حالات خاصة، بالولوج إلى البيانات إذا ما اقتضت الضرورة الأمنية الوطنية ذلك، لاسيما لمكافحة الجرائم وجمع الأدلة، حيث أقر قانون الدفاع الوطني اللبناني الصادر سنة 1999، جملة من الاستثناءات للاطلاع ومراقبة وتسجيل المعطيات، المكالمات والاتصالات المختلفة بصورة حصرية، في حالة تعرض الوطن أو جزء من أراضيه أو مجموعة من السكان للخطر ويتم ذلك بناء على مراسيم بعد طلب المجلس الأعلى للأمن، كما تم تعديل العديد من الأحكام الخاصة بقوانين حماية خصوصية البيانات من أبرزها قانون تنظيم المعاملات الالكترونية لسنة 2004.[1]

والمشرع التونسي سن عام 2004 تشريعا لحماية المعطيات الشخصية بموجب القانون الأساسي رقم 63، المتعلق بحماية المعطيات الشخصية، حيث تضمن جملة من الإجراءات لمعالجة المعطيات الشخصية كما أقر إنشاء هيئة مستقلة مكلفة بحماية مختلف جوانب معالجة المعطيات الشخصية، تحتوي على تركيبة متجانسة من خمسة عشر عضوا، يعينون بأمر لمدة ثلاث سنوات.[2]

وفي سنة 2009 أصدر المشرع المغربي القانون 08-09 الصادر في 18 فبراير 2009، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي حيث تضمن جملة من الضوابط الخاصة بمعالجة المعطيات، مع تكريس حقوق للأفراد على معطياتهم وفرض التزامات للقائمين بالمعالجة، تسهر على مراقبة احترامها اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي والتي تتشكل من سبع (07) أعضاء لمدة خمسة سنوات قابلة للتجديد مرة واحدة.[3]

---

[1] منى الأشقر جبور، محمود جبور، المرجع السابق، ص 58-59.

[2] راجع الفصل 78 من القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004، المتعلق بحماية المعطيات الشخصية، الموقع الرسمي للهيئة على الإنترنت " http://www.inpdp.nat.tn/Receuil_2019.pdf " تاريخ الاطلاع 2020/01/20.

[3] راجع المادة 32 من القانون 08-09، الصادر في 18 فبراير 2009، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الموقع الرسمي للجنة المغربية على الإنترنت " http://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf " تاريخ الاطلاع: 2020/01/20.

والمشرع الجزائري بدوره أكد على تكريس حماية الأشخاص الطبيعيين عند معالجة بياناتهم ذات الطابع الشخصي لاسيما بموجب التعديل الدستوري لسنة 2016 وكذا أحكام القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي والذي بموجبة تم ضبط وتنظيم عملية معالجة البيانات الشخصية، مع إقرار إنشاء سلطة وطنية لحماية المعطيات سيتم التفصيل في صلاحياتها في الباب الثاني من هذه الأطروحة[1].

كما أقرت دولة الإمارات وبالضبط ب"دبي" سنة 2007 قانونا لحماية البيانات الشخصية وعينت مفوضا للتجسيد الفعلي لأحكام هذا القانون بهدف اعتماد جانب راقي من الحماية للبيانات والتي بموجبها تمنح الأفراد أكثر ضمانات والتي لا بد أن تنعكس إيجابيا على إنعاش الاقتصاد بفضل هامش الأمان المكرس، بالخصوص في مركز دبي المالي العالمي تنفيذا لمختلف اللوائح والتوجيهات الدولية والأوروبية المتعلقة بهذه الجوانب الحيوية[2].

المبحث الثاني: المقصود بالبيانات الشخصية

إن البحث المفصل عن مفهوم البيانات الشخصية يعد بالغ الأهمية من جوانب عدة، لاسيما من حيث ضبط النص التشريعي، حيث يتم التمييز بين العديد من المصطلحات المتشابهة، الأمر الذي دفع بالعديد من التشريعات إلى تخصيص مادة أو مجموعة من المواد الخاصة ضمن نص تشريعي يتعلق بحماية البيانات الشخصية لضبط مجال الحماية وصورها على الخصوص، الأمر الذي سيتم التفصيل فيه في المطلبين التاليين:

المطلب الأول: تعريف البيانات الشخصية

إن الوقوف على مختلف التعريفات المكرسة للبيانات الشخصية حسب ما ذهب إليه مختلف الفقهاء والتشريعات، يضفي على المصطلح أكثر عمقا ودقة وحصرا نظرا للمجال

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

[2] منى الأشقر جبور، محمود جبور، المرجع السابق، ص 61

المشمول بالحماية، وما يمكن أن يترتب عنها من التزامات ضد المعالجين وحقوق لأصحاب هذه البيانات الشخصية.

ومن خلال العناصر الموالية سنحاول الإلمام بالتعاريف الخاصة بالبيانات الشخصية من مختلف الجوانب انطلاقا من النظرة الفقهية (الفرع الأول) ثم القانونية (الفرع الثاني).

الفرع الأول: التعريف الاصطلاحي والفقهي

تشمل المعطيات الشخصية المعنى الواضح لتعريف البيانات، إذ تستعمل كلمة المعطيات على الأشياء المعطاة مسبقا بحيث أطلق عليها باللاتينية "Datum"، وبالانجليزية "Data" ويقابلها باللغة الفرنسية "Données"، وتم تعريفها في معجم الحاسبات بكونها " معلومات معدة في صورة محددة للاستخدام في مجال ما"[1]، وعليه فإنها تشكل معلومات تعطى للحاسب الآلي لتعالج وتخزن، وقد اعتبرها البعض عبارة عن رموز وأرقام تحتاج إلى المعالجة الآلية أو الالكترونية باستعمال الحاسب لتصبح معلومة، أي بمعنى آخر فالمعلومات تتشكل من جملة المعطيات أو البيانات يتم التعبير عنها في شكل خاص نتيجة معالجة آلية [2].

كما تطلق البيانات على جملة القياسات للحقائق أو المشاهدات التي تكون إما على شكل حروف أو أرقام أو رموز خاصة تجسد أو تصف هدف، فكرة موضوع، شرط أو أية عوامل أخرى[3].

وكما أسلفنا فإن البيانات تتداخل مع المعلومات وتتكامل بحيث أن المعلومات عبارة عن بيانات منظمة ومعالجة بطريقة معينة يترتب عنه نتائج وتحاليل تحقق زيادة المعرفة،

[1] معجم الحاسبات، مجمع اللغة العربية، الطبعة الثانية الموسعة، مركز الحاسوب- أكاديمية اللغة العربية، جمهورية مصر العربية، سنة 1995، ص53.

[2] غنية باطلي، الجريمة الالكترونية-دراسة مقارنة، الدار الجزائرية، الجزائر، 2015، ص 70-71.

[3] سامي علي حامد عياد، الجريمة المعلوماتية وا إجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2008، ص24.

كما أن البيانات تتجسد في جملة من الحقائق المفسرة لمواقف حدثت أو ستحدث بحيث تتباين وسيلة التعبير بين رموز أو أشكال أو كلمات[1].

وبدوره أشار الدكتور يوسف بن سعيد الكلباني إلى مصطلح البيانات الإلكترونية بأنها " مجموعة من الرموز أو الأشكال أو الحقائق المادية الملموسة، وأنها بمجرد إتمام المعالجة الآلية إلكترونيا تتحول إلى معلومات تكون في ظاهرة مادية تشكل بيانات متعددة تتبلور عند تجميعها أو نقلها أو تخزينها بواسطة الأفراد أو الأنظمة الالكترونية إلى معلومات فهي تتميز بالمرونة بحيث يمكن تخزينها في وسائل متعددة "[2].

كما تجدر الإشارة إلى أن البيانات الشخصية تعد صنفا من أصناف البيانات الالكترونية في مفهومها الواسع، بحيث تخص التعريف بالشخص أو تخص أحد جوانب الحياة الخاصة المتعلقة بالفرد أو تمس حقا من حقوقه الأساسية[3].

وعليه فإن الإحاطة بتعريف البيانات الشخصية تتطلب اعتماد جملة من العوامل مواكبة للتحولات الرقمية باعتبار أن المعطيات المعالجة والمجسدة في صورة معلومات قابلة للاستغلال تعتمد في جميع مراحلها على الأجهزة التقنية التكنولوجية منذ تجميعها ثم معالجتها وكذا تأمينها سواء باعتماد أساليب تشفير الأجهزة أو البيانات بحيث يصعب فهم معناها والتي تحتاج إلى ترخيص للاطلاع عليها، أو اعتماد برمجيات كتلك المتخصصة في كشف ومقاومة الفيروسات التي تشكل تهديدا كبيرا على أمن المعلومات، والتي تحتاج لبرامج مضادة لهذه الفيروسات تسهم بشكل كبير في الحفاظ على المعطيات من التلف أو الاستغلال غير المشروع[4].

وعليه فإن سلامة البيانات الشخصية من أي تعد من قبل قراصنة الحاسوب تعد بالغة الأهمية لتجنب أي تغيير أو محو لهذه البيانات أو جزء منها ولا يتم ذلك إلا بخلق نظام

[1] يوسف بن سعيد الكلباني الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري، دار النهضة العربية، القاهرة، 2017، ص15.

[2] يوسف بن سعيد الكلباني، المرجع السابق، ص16.

[3] أيمن عبد الله فكري، جرائم نظم المعلومات، دار الجامعة الجديدة، الإسكندرية، 2008، ص29.

[4] أشرف السعيد أحمد، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة للطباعة والنشر والتوزيع، مصر، سنة 2015، ص93-95.

رقابي بين المرسل والمستلم بحيث يتم التأكد من مصدر إرسال هذه البيانات وكذا سلامة محتو اها، وعليه فإن تفعيل آليات سلامة البيانات يعد من الصعوبة بمكان وأكثر تعقيدا من عملية التشفير والحفاظ على سرية البيانات[1].

ومن هذا المنطلق فإن تحديد البيانات الشخصية يتطلب الربط بين الجانبين الإداري القانوني والتقني وتصنيف هذه البيانات إلى فئات بحيث تضم البيانات المسجلة المكتملة المعالجة وتلك التي هي في طور المعالجة، وكذا عملية المعالجة في حد ذاتها والتي تمكن من الوصول إلى مختلف المعلومات، تعديلها أو محوها، مع ضبط وتدقيق مختلف البيانات، قصد الوصول إلى تصنيفها حسب كل فئة وربطها بالأشخاص المعنيين بهذه المعالجة، نظر لوجود ارتباط عضوي بين تحديد البيانات وعمليات المعالجة المتعلقة بها[2].

وقد ورد ضمن مذكرة بالولايات المتحدة الأمريكية صادرة عن مكتب الإدارة والميزانية بالبيت الأبيض، تعريف للمعطيات الشخصية بأنها " المعلومات التي يمكن استخدامها لتمييز أو تعقب هوية الفرد، مثل الاسم ورقم الضمان الاجتماعي والسجلات الحيوية لوحدها أو عند دمجها مع المعلومات الشخصية أو تحديد الأخرى الرابطة مع شخص معين، مثل تاريخ ومكان الميلاد واسم عائلة الأم،..الخ"[3]

وفي السياق ذاته أقرت اللجنة الوطنية للمعلوماتية والحريات (CNIL)، في فرنسا إدراج رقم التعريف الالكتروني للجهاز (L'adresse IP)، ضمن البيانات الشخصية باعتراضها على الاجتهاد الصادر عن محكمة الاستئناف بباريس المتضمن عدم اعتبار العنوان المتعلق برقم التعريف الالكتروني للجهاز من جملة البيانات ذات الطابع الشخصي، نظرا لعدم ارتباطه بتحديد هوية الشخص المستعمل للجهاز، حيث أكدت اللجنة أن مثل هذا

[1] خضر مصباح الطيطي، إدارة تكنلوجيا المعلومات، دار الحامد للنشر والتوزيع، عمان- الأردن، 2012، ص292.

[2] منى الأشقر جبور، محمود جبور، المرجع السابق، ص 74-75.

[3] مروة زين العابدين صالح، المرجع السابق، ص 69.

القرار سيسهم في فتح باب التعدي على الخصوصية، مما يتطلب الحصول على الترخيص المسبق لجمع مثل هذه البيانات[1].

وهذا ما يفسر تبني السلطة الوطنية المستقلة لحماية البيانات ذات الطابع الشخصي بفرنسا، الأخذ بالمفهوم الواسع للبيانات الشخصية من جهة، وكذا المكانة التي تلعبها هذه الهيئة في تكريس حماية البيانات الشخصية، على أوسع نطاق، بما في ذلك طلب مراجعة الاجتهادات القضائية، كما هو الحال في الاعتراض المذكور آنفا[2].

ومن خلال مقارنة بين مختلف التعاريف المذكورة آنفا نلاحظ اعتماد أغلبها على المفهوم الموسع للبيانات الشخصية بحيث تشمل جميع الجوانب المرتبطة بالشخص بما في ذلك رقم تعريف أجهزته الرقمية مثل الحاسوب أو الهاتف المحمول وغيرها ولعل اعتماد مثل هذا التعريف في جانبه الايجابي يساهم في ضمان أكثر حماية للبيانات الشخصية لاسيما وما نشهده بصفة متزايدة حول تأثير استعمال التكنولوجيات الرقمية وتأثير مختلف التطبيقات والمواقع المتاحة على شبكة الإنترنت في كشف العديد من الأسرار المرتبطة بالأشخاص الطبيعيين كالصور والفيديوهات وغيرها.

الفرع الثاني: التعريف القانوني للبيانات الشخصية

يمثل التعريف القانوني للبيانات الشخصية نقطة الانطلاق لتكريس حماية هذه البيانات، نظرا لما للتعريف من أهمية عند فقهاء القانون وكذا يعد المرجع للقاضي في تقرير أو الفصل في أن الإجراء المعني يدخل ضمن مجال البيانات الشخصية أم لا، ومن هذا المنطلق تحرص أغلب التشريعات الدولية على الأخذ بالمفهوم الموسع للبيانات الشخصية لتكريس أكثر حماية ممكنة.

وسيتم التفصيل من خلال هذا الفرع في أهم التعريفات المتعلقة بالبيانات الشخصية التي تضمنتها مختلف مصادر التشريع على المستوى الدولي ثم العربي ووصولا إلى إبراز موقف المشرع الجزائري، كما يلي:

1 منى الأشقر جبور، محمود جبور، المرجع السابق، ص77.

[2] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص386.

أولا: على المستوى الدولي

تضمنت النسخة الأولى من الإرشادات الصادرة عن منظمة التعاون الاقتصادي والتنمية، سنة 1980 تعريفا للبيانات الشخصية بأنها " كل معلومة عائدة لشخص طبيعي محدد، أو قابل للتحديد "[1].

كما أشار نص المادة رقم 02 من اتفاقية مجلس أوروبا لسنة 1981 المتعلقة بحماية الأشخاص في ما يخص التحليل الآلي للبيانات ذات الطابع الشخصي، إلى تعريف هذه الأخيرة ب:" كل معلومة تخص شخصا طبيعيا معروفا أو يمكن التعرف إليه «الشخص المعني"[2].

كما اهتم المشرع البريطاني بتكريس حماية البيانات الشخصية ضمن قانون سنة 1998 والذي جاء بقواعد جديدة وفقا لتوجيهات الاتحاد الأوروبي الملزمة لمختلف الدول الأعضاء الصادرة سنة 1997، حيث عرف في فصله الأول البيانات الشخصية بأنها " البيانات المتعلقة بالشخص الحي الذي يمكن تعريفه بها بضمها لمعلومات أخرى في حوزة المسؤول عن معالجة البيانات أو من المحتمل أن لا تكون في حوزته"[3].

والملاحظ من خلال هذا التعريف أنه خص الحماية بالأشخاص الأحياء تحديدا حصريا، أي بمفهوم المخالفة، فإن هذا القانون لا يحمي البيانات الشخصية المتعلقة بالموتى على عكس ما ذهبت إليه مختلف المواثيق الدولية والقوانين الوطنية لأغلب الدول، لاسيما تلك التي تنتمي إلى الاتحاد الأوروبي، والتي أشارت إلى الشخص المعني بالبيانات، دون حصر كونه حيا أو ميتا.

---

[1] منى الأشقر جبور، محمد جبور، المرجع السابق ص 75-76.

[2]«Données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»)" -Voir Article 02 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Strasbourg, 28.1.1981; disponible sur site – Conseil de l'Europe- " https://rm.coe.int/1680078b39"

[3] الشيخ الحسين محمد يحي، سيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية، المرجع السابق، ص47.

كما تدخل قواعد البيانات في شقها المتعلق بتصنيف معلومات شخصية كتلك التي تدخل ضمن حقوق المؤلف في المجال الواسع للبيانات الشخصية، حيث تطرق نص المادة 03 من القانون الفرنسي الخاص بالملكية الأدبية على تعريف قواعد البيانات ب" يقصد بقواعد البيانات مجموعة مصنفات، معطيات أو عناصر أخرى مستقلة، معدة في هيئة نظامية أو منهجية، يتم الوصول إليها انفرادياً بوسائل الكترونية أو بأية وسيلة أخرى"[1].

كما عرفت الاتفاقية الأوربية الخاصة بتضمين آليات حماية قواعد البيانات، المنعقدة بتاريخ 11 مارس 1996، قواعد البيانات ب" تجميع لمصنفات أو معلومات أو أية مواد منفصلة مرتبة بطريقة نظامية ومنهجية ويمكن الوصول إليها فرديا سواء بوسيلة الكترونية أو أي وسيلة أخرى"[2].

وبدورها أقرت المحكمة الأوروبية لحقوق الإنسان تبني مفهوم شامل موسع للبيانات الشخصية لتشمل حماية الخصوصية، والحياة المهنية في بعض جوانبها كما جاء في قرارها الصادر بتاريخ 2000/02/16، عند الفصل في القضية المحولة إليها سنة 1998 والمتعلقة باعتراض أحد المواطنين السويسريين على استعمال الأحرف الأولى من اسمه، خوفا منه على انعكاسات اكتشاف اسمه، وعليه تم إقرار مذكرة تتضمن" حماية أي معلومة تخص شخصا معرفا أو قابلا للتعريف "[3].

---

[1] Art. L.112-3. Al.2: " On entend par base de données un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen".(https://www.doctrine.fr/l/texts/codes/LEGITEXT00001235)

[2] فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الإنترنت، مكتبة الوفاء القانونية، الإسكندرية، 2017، ص58.

3 منى الأشقر جبور، محمد جبور، المرجع السابق، ص 78.

كما نص القانون المتعلق بحماية البيانات الشخصية والمستندات الالكترونية الكندية على إيجاز وحصر تعريف المعلومات الشخصية ب" المعلومات المتعلقة بشخص معرف"[1]

والمشرع الفرنسي بدوره كان من السباقين في إطلاق تعريف للبيانات الشخصية كما جاء ضمن القانون 78-17 المتعلق بالمعلوماتية والحريات المعدل والمتمم، لاسيما ما تضمنه تعديل سنة 2004، والذي تطرق إلى تعريف البيانات الشخصية، بأنها تتمثل في " أي معلومة تتعلق بشخص طبيعي محددة هويته أومن الممكن تحديد هويته مباشرة بواسطة رقم معين، أو بواسطة عنصر أو أكثر خاص به" [2].

كما تم بموجب النظام العام الأوروبي لحماية البيانات الشخصية رقم 2016/679، المؤرخ في 27 ابريل 2016[3]، الذي دخل حيز التنفيذ بتاريخ 25 مايو 2018، إعطاء تعريف جديد للبيانات الشخصية أكثر وضوحا وشمولا حيث تضمن نص مادته الرابعة ما يلي: " البيانات الشخصيةهي: معلومة تتعلق بشخص طبيعي مـ ُعر ّف أو قابلا للتعرف

[1] Personal Information Protection and Electronic Documents Act ,S.C. 2000, c. 5 , Assented to 2000-04-13 " Personal information means information about an identifiable individual". "https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html"

2 Article 2 La loi N0 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O du 07/08/1978; Modifié par Loi n°2004-801 du 6 août 2004 – art. 1 JORF 7 août 2004 : "Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

[3] Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) , disponible sur Site: https://www.cnil.fr/fr/reglement-europeen-protection-donnees. date de mise en ligne le 11/10/2020.

عليه يشار إليه فيما يلي باسم "الشخص المعني"، ويعتبر شخصًا طبيعيًا قابلاً للتعرف" كل شخص طبيعي يمكن معرفته بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى عنصر معرف مثل الاسم ورقم التعريف وبيانات الموقع ومعرّف الاتصال عبر الإنترنت أو لواحد أو أكثر من العناصر المميزة لهويته الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"[9].

وما تجدر الإشارة إليه هو أن البيانات الشخصية تشمل فقط الشخص الطبيعي دون المعنوي على مستوى ما جاء في هذا النظام وكذا القانون الفرنسي المتعلق بهذا المجال.

كما عرفت المادة الأولى من اتفاقية الاتحاد الإفريقي لسنة 2014، الخاصة بأمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، بأنها" أي معلومات متصلة بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو غير مباشر بالإشارة إلى رقم هويته أو إلى عامل واحد أو أكثر محدد لهويته الطبيعية أو السيكولوجية أو الذهنية أو الاقتصادية أو الثقافية أو الاجتماعية "[1].

ثانيا: على المستوى العربي:

يعد المشرع التونسي من السباقين على المستوى العربي في الاهتمام بمجال حماية البيانات ذات الطابع الشخصي بنصه ضمن الفصل الرابع من القانون الأساسي الخاص بحماية البيانات والذي عرف البيانات الشخصية بأنها" كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصا طبيعيا معرفا أو قابلا للتعريف بطريقة مباشرة وغير مباشرة باستثناء المعلومات المتصلة بالحياة العامة والمعتبرة كذلك قانونا" [2].

---

[1] راجع المادة 01 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، والتي تم اعتمادها في الدورة العادية الثالثة والعشرون لرؤساء دول وحكومات الإتحاد الإفريقي، المنعقدة في ملابو، غينيا الاستوائية بتاريخ 27 يونيو 2014، متاحة على الموقع الالكتروني للاتحاد الإفريقي على الرابط: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_a.pdf.

[2] انظر الفصل 04 من القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004، المتعلق بحماية المعطيات الشخصية، الموقع الرسمي للهيئة على الإنترنت " http://www.inpdp.nat.tn/Receuil_2019.pdf " تاريخ الاطلاع 2020/01/20

والملاحظ من خلال هذا التعريف لجوء المشرع التونسي إلى تضييق مجال المعطيات الشخصية باستثنائه المعلومات المتصلة بالحياة العامة.

كما نصت المادة الأولى من القانون 09-08، الخاص بحماية البيانات الشخصية بالمغرب، على تعريفها بأنها " كل معلومة كيفما كان نوعها بغض النظر عن دعامتها، بما في ذلك الصوت والصورة، المتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه والمسمى بعده بالشخص المعني، ويكون الشخص قابل للتعرف عليه إذا كان بالإمكان التعرف عليه، بصفة مباشرة أو غير مباشرة، ولاسيما من خلال الرجوع إلى رقم تعريف أو عنصر أو عدة عناصر مميزة لهويته البدنية أو الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"[1].

ومن جانبه المشرع المصري فصل تعريف البيانات الشخصية بكونها " أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخر ى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي،أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية"[2].

كما عرف المشرع القطري البيانات الشخصية بموجب أحكام المادة الأولى من القانون 2016/13 المتعلق بحماية خصوصية البيانات الشخصية بأنها" بيانات عن الفرد الذي تكون هويته محددة، أو يمكن تحديدها بصورة معقولة، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى"[3].

---

[1] ظهير شريف رقم 15.09.1 مؤرخ في 18 فبراير 2009 متعلق بتنفيذ القانون 09-08، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 5711 بتاريخ 23 فبراير 2009 الموقع الرسمي للجنة المغربيـــة لحماية المعطيات، "https://www.cndp.ma/images/lois/Loi-09-08-Ar.pdf" تاريخ الاطلاع: 2020/01/20.

[2] انظر المادة 1 من القانون رقم 151 لسنة 2020، المتعلق بحماية البيانات الشخصية المصري، الجريدة الرسمية العد 28 مكرر (هـ) في 15 يوليو سنة 2020.

[3] انظر المادة الأولى من القانون رقم (13) لسنة 2016، بشأن حماية خصوصية البيانات الشخصية، الجريدة الرسمية لدولة قطر، عدد 15 الصادرة بتاريخ 29 ديسمبر 2016.

ومن خلال الرجوع إلى مضمون مختلف التعاريف المتعلقة بالبيانات الشخصية يمكن استخلاص ما يلي:

- الاستيلاء على البيان لا يمثل مساسا أو تعد في حد ذاته إذا لم يكن ملتصقا بشخص محدد.

- عدم اشتراط الدقة أو الصحة في البيانات لاعتبارها شخصية.

- عدم اشتراط إجراء توثيق جميع أصناف البيانات الشخصية للاستفادة من تدابير الحماية بل يكفي أن تكون هذه البيانات ملتصقة بالشخص المعني بعينه.

- عدم سقوط صفة البيانات الشخصية على البيانات التي أصبحت متاحة للعامة إذا كانت مرتبطة أو لصيقة بالشخص وتستفيد من مختلف تدابير الحماية[1].

ثالثا: موقف المشرع الجزائري

إن المشرع الجزائري بدوره تطرق إلى مصطلح البيانات والمعلومات الشخصية في بعض النصوص القانونية على غرار ما ورد في نص المادة 05 من القانون 15-04[2]، كما أطلق على البيانات الشخصية في العديد من النصوص القانونية مصطلح المعطيات ذات الطابع الشخصي، حيث نصت المادة 46 من الدستور المعدل سنة 2016، وكذا القانون 18-07 والذي تناول في مادته الثالثة تعريف المعطيات ذات الطابع الشخصي ب:" كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، " الشخص المعني" – أي كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة- بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"[3].

كما تم تعريف مصطلح "معالجة المعطيات ذات الطابع الشخصي" حسب مضمون الفقرة الثالثة من المادة الثالثة من القانون 18-07 ب" كل عملية أو مجموعة عمليات

[1] مروة زين العابدين بن صالح، المرجع السابق، ص72-73.

[2] انظر المادة رقم 05 من القانون 15-04، المؤرخ في أول فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية عدد 06 المؤرخة في 10 فبراير 2015.

[3] انظر الفقرة الأولى من المادة 03 من القانون 18-07، المرجع السابق.

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 النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف" [1].

وبالرغم من ارتباط مجال إدخال المعطيات بعملية المعالجة الآلية بالاستناد إلى تطبيقات وبرامج متطورة، إلا أن هذه الأخيرة تعتبر وسيلة في حد ذاتها للإدخال أو التخزين أو الاسترجاع لهذه المعطيات، وهي تندرج في إطار الحماية المقررة للمعطيات الشخصية بالرغم من اختلاف وجهات النظر في حسم الخلاف في هذا المجال إلا أن المشرع الجزائري حسم هذا الأمر بإدراج البرامج ضمن قائمة المصنفات المحمية وفقا لقانون حماية المؤلف حسب ما كرسه كل من الأمرين 97-10 و03-05 المعدلين لقانون حقوق المؤلف حيث تم إدماج البرامج وقواعد البيانات ضمن المصنفات الأصلية الواجبة الحماية[2].

ومن وجهة نظرنا فإن التعريف الذي اعتمده المشرع الجزائري للمعطيات الشخصية، جاء بصيغة العموم ولم يتطرق إلى ذكر نماذج واضحة ومباشرة لهذه المعطيات، وعليه كان من المستحسن وضع قائمة، غير محصورة، للمعطيات ذات الطابع الشخصي، لتجنب مختلف التأويلات التي تنعكس سلبا على إهمال جانب من المعطيات الشخصية لاسيما تلك المرتبطة بالجانب الرقمي، على غرار عنوان البريد الإلكتروني ، نظرا لكون صور البيانات الشخصية تختلف حسب عرف وثقافة البلدان والشعوب.

المطلب الثاني: صور البيانات الشخصية

تكملة لما تم تجليته في النقاط السابقة حول تعريف البيانات الشخصية من مختلف الجوانب، إلا أن تعريف البيانات الشخصية لا يكتمل إلا ببسط صور هذه البيانات الشخصية بنوعيها العادية والحساسة كما سيتم دراسته في الفرعين المواليين:

[1] انظر الفقرة الثالثة من المادة 03 من القانون 18-07، المرجع السابق.

[2] غنية باطلي، المرجع السابق، ص 81-82.

الفرع الأول: صور البيانات الشخصية العادية

يعد الجانب الشخصي والاجتماعي الشيء المميز لصور البيانات الشخصية التي تتطلب جانبا مهما من الحماية، المكرسة عبر مختلف التشريعات الدولية، حيث تم ضبط جملة من صور البيانات الشخصية، التي عرفت اتفاقا بين أغلب التشريعات المهتمة بحماية البيانات الشخصية، والتي تم تسجيل اعتماد أغلبها على ذكر مجموعة من الصور لهذه البيانات على سبيل المثال، لا الحصر، وعليه سيتم التطرق إلى تفصيل أغلب هذه الصور، كما يلي:

1-الاسم واللقب: يشكل الاسم مفتاح البيانات الشخصية نظرا لكونه وسيلة التمييز لأي شخص عن الغير وينقسم إلى مجموعة أقسام، فنميز الاسم الشخصي وكذا الاسم العائلي أو ما يسمى باللقب، الذي يشمل كامل أفراد الأسرة التي ينتمي إليها الشخص، طبقا لما يتم تفصيله في القانون المدني لبلد إقامة الشخص المعني، حيث اعتمد المشرع الجزائري في تحديد الهوية على نظام اللقب والاسم كما هو الحال عند المشرع الفرنسي الذي اقر أن اسم الشخص ولقبه يعد بياناً شخصيا مشمولا بالحماية[1].

هذا بالإضافة إلى وجود أصناف أخرى من الأسماء، تشكل جانبا هاما من جوانب حماية المعطيات الشخصية إذا ما قوبلت بالاسم الشخصي، وتتمثل في كل من الاسم المستعار، اسم الشهرة والاسم التجاري.

- ✓ **الاسم المستعار:** يمثل الاسم المؤقت أو الخفي الذي قد يستعمله الشخص في مرحلة من المراحل أو في مهمة من المهام حماية للشخص أو تورية كما يجسد عند ممارسة بعض الأشخاص لنشاطات فنية أو أدبية، وهو كذلك محمي بقوة القانون لاسيما إذا اختار الشخص المعني ذلك واستعمله باستمرار ولمدة طويلة[2].

[1] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية –دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص 390.

[2] سهير منتصر، النظرية العامة للحق، مكتبة الإسكندرية، 2006، من دون ناشر، ص 66.

- ✓ **اسم الشهرة:** هو اسم قد لا يختاره الشخص لنفسه وإنما يختاره الغير له غالبا ولا يرد ذكره في الوثائق الشخصية للمعني.[1]
- ✓ **الاسم التجاري:** وهو الاسم الذي يستعمله التاجر لترويج منتجاته أو خدماته وهو يعتبر من الحقوق المالية التابعة والقابلة للتصرف[2].

2-الصوت والصورة ومقاطع الفيديو:

اعتبرت العديد من التشريعات أن الصوت والصورة مقاطع الفيديو المتعلقة بالشخص تعد من أهم عناصر المعطيات الشخصية، التي تقتضي تكريس حماية مناسبة لها، نظرا لما أحدثه التطور الرقمي من آثار قد تكون سلبية في معالجة الصوت أو الصورة أو مقاطع الفيديو بإضافة أو إنقاص جانب مهم من الجوانب التي قد يعتمد عليها في الإثبات المدني أو الجنائي.

كما قد يؤثر في كشف جوانب شخصية سرية تتعلق بالأشخاص، لاسيما بياناتهم الحساسة، أو تعرضهم لإصابات وأمراض تقتضي المعالجة في سرية تامة، نظر للأثر الاجتماعي والنفسي على المعني بالمعالجة، في حالة معرفة الغير أو اطلاعه على ملفات أو صور تكشف ما كان مستورا، باستعمال تطبيقات متخصصة في هذا المجال، حيث كان التشريع الأوروبي من بين السباقين لضمان حماية هذا الجانب بموجب ما تضمنه التوجيه الأوروبي الخاص بحماية البيانات الشخصية لسنة 1995، من قواعد توجيهية، شكلت محور انطلاق للتشريعات الوطنية الاوروبية في مجال إرساء مجال دقيق لحماية البيانات الشخصية. حيث برز دور المشرع الفرنسي في هذا المجال بفضل الآليات المكرسة على غرار هيئة CNIL، والتي برهنت من خلال مضامين مداولاتها حجم الحماية الفعلية المكرسة، حيث تضمنت المداولة رقم 96-009 المؤرخة في 27 فبراير 1996 المصادقة على التقرير المتضمن اعتبار الصوت والصورة وحماية الحياة الخاصة والحريات الأساسية من ضمن البيانات الشخصية[3].

---

[1] سهير منتصر، المرجع نفسه، ص67.

[2] مروة زين العابدين صالح، المرجع السابق، ص 84.

[3] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية – دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص390.

3-الموطن والعنوان:

ويشمل مكان تواجد الشخص أو مقر ممارسة نشاطه أو عنوانه التجاري والذي يعتبر مرجعا لنشاطه، حيث يمكن أن يكون العنوان الشخصي محلا قانونيا يستعمله الشخص في العقود المبرمة وكذا لاستلام الرسائل بمختلف أنواعها وكذا تضمينه ضمن وثائق الهوية أو مقر العمل ومكان السكن[1].

4-البيانات الصحية :

تعرف البيانات الصحية بمختلف الجوانب التي تقتضيها الرعاية الطبية، المتعلقة بتفصيل الحالة التي تصف المريض والمرض وما يتعلق بها من ظروف وعلاج، والتي تعتمد على مبدأ التحفظ وواجب الكتمان بالنسبة للمعطيات التي يكتشفها الطبيب أو تلك التي يصرح بها المريض من تلقاء نفسه، ضمانا لحمايتها[2].

وقد نميز حالات سلبية استغلالا لهذه الحماية، وهي عدم اتخاذ المريض الإجراءات الاحتياطية لتجنب نقل العدوى، على غرار ما تميز به فيروس كوفيد 19، بحيث انتشر انتشارا كبيرا وكان من أسباب ذلك امتناع بعض المصابين من اتخاذ الإجراءات الوقائية، الأمر الذي اضطر بعض المصالح الطبية بنشر قائمة المشتبه في إصابتهم لأخذ الاحتياط، لاسيما في حالة عدم التزامهم بإجراءات الحجر المنزلي، ومهما يكن فإن هذا الاستثناء لا يشكل مبررا للتخلي عن واجب التحفظ والكتمان، إذ يتوجب مراعاة مبدأ السرية الطبية إلى جانب فرض إجراءات ردعية ضد الأشخاص المخالفين.

وقد حظيت البيانات الصحية بعناية خاصة من قبل مختلف التشريعات الدولية والوطنية، مما دفع ببعض التشريعات إلى تصنيفها ضمن البيانات الحساسة المحظور معالجتها، إلا إذا اقتضت ذلك الضرورة.

[1] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، المرجع السابق، ص 84.

[2] منى الأشقر جبور، محمود جبور، المرجع السابق، ص84.

وتجدر الإشارة إلى اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، أوردت تعريفا للبيانات الصحية بأنها " تعني جميع المعلومات المتصلة بالحالة الجسدية أو العقلية للشخص المعني، بما فيها البيانات الوراثية"[1]

كما أقر المشرع الفرنسي ضمن نص المادة رقم 08 من القانون 87-17، المعدل والمتمم، لاسيما ما أحدثه تعديل سنة 2018، بعد دخول النظام الأوروبي العام الجديد حيز التنفيذ، بتكريس منع وجمع ومعالجة معلومات ذات طابع شخصي تُظهر، بأي صورة كانت، جوانب من المعطيات الشخصية الصحية..

ومن جهتها كذلك اللجنة الوطنية للحريات والمعلوماتية بفرنسا كرست حماية البيانات الشخصية الطبية الجسدية أو النفسية بموجب مداولتها رقم 85-50 المؤرخة في 22 أكتوبر 1985[2].

كما أشار المشرع التونسي ضمن نص القانون الأساسي المتعلق بحماية المعطيات الشخصية[3]، إلى أنه يجوز القيام بمعالجة المعطيات الشخصية المتعلقة بالصحة في حالة ما إذا كانت المعالجة ضرورية لتطوير الصحة العمومية وحمايتها، هذا بالإضافة إلى إقرار الحق لكل شخص في معالجة معطياته.

كما أقر المشرع التونسي من خلال الفصل الرابع من القرار 4 المتعلق بمعالجة المعطيات الشخصية المتعلقة بالصحة، في إطار تعامله مع الأشخاص المشار إليهم

[1] راجع المادة الأولى من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، والتي تم اعتمادها في الدورة العادية الثالثة والعشرون لرؤساء دول وحكومات الإتحاد الإفريقي، المنعقدة في ملابو، غينيا الاستوائية بتاريخ 27 يونيو 2014.

[2] Délibération CNIL n^0 85-50 du 22 Octobre 1985, portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, disponible sur " https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017654812" en date du 25 décembre 2020.

[3] انظر الفصل 62 من القانون الأساسي عدد 63، المرجع السابق.

بالفصل الثاني من هذا القرار بما يكفل احترام حياته الخاصة وحقه في الحفاظ على سرية المعلومات الصحية الخاصة به[1].

وبدوره أكد المشرع المغربي على حماية البيانات الطبية من خلال نص المادة 12 من القانون 08-09 باشتراط الإذن المسبق من اللجنة الوطنية لحماية البيانات عند معالجة بعض البيانات والتي حصر من بينها المعطيات الصحية[2].

والمشرع الجز ائري اهتم بحماية البيانات الصحية من خلال إقرارها في العديد من النصوص القانونية على غرار ما تضمنه قانون الصحة، قانون العقوبات والقانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي. حيث نصت 301 من قانون العقوبات الجزائري على حظر إفشاء السر الطبي وهو ما أكده قانون الصحة رقم 18-11، حيث نصت المادة 440 منه، على إمكانية رفع العقوبة بالحبس إلى غاية سنة كاملة وبغرامة مالية تصل إلى 100.000 دج، مع إمكانية إقرار عقوبات تكميلية جراء إفشاء السر المهني الطبي.

إلا أنه تجدر الإشارة إلى وجود استثناءات عن إفشاء السر الطبي وهذا ما تضمنه نص المادتين38 و 39 من القانون 18-11[3] والتي ألزمت الطبيب في حالات محددة بضرورة إفشاء السر الطبي لجهات محددة للحفاظ على الصحة والمصلحة العامة حيث بالرجوع إلى مضمون نص المادتين 38 و39 من قانون الصحة وكذا التنظيم المحدد لقائمة

---

[1] راجع الفصل الرابع من القرار عدد 4 بتاريخ 05 سبتمبر 2018، المتعلق بمعالجة المعطيات الشخصية المتعلقة بالصحة التونسي.

[2] ظهير شريف رقم 09.01.15 الصادر في 18 فبراير 2009، المتعلق بتنفيذ القانون رقم 08-09 المتعلق بحمية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 5711، المؤرخة في 23 فبراير 2009.

[3] نصت المادة 38 و 39 من القانون 18-11 المتعلق بالصحة على:

1 المادة 38" يخضع الأشخاص المصابون بأمراض متنقلة والأشخاص الذين يكونون على اتصال بهم، الذين قد يشكلون مصدرا للعدوى لتدابير الوقاية والمكافحة المناسبة. تحدد قائمة الأمراض المتنقلة الخاضعة للتصريح الإجباري عن طريق التنظيم".

2 المادة 39 " يجب على كل ممارس طبي التصريح فورا للمصالح الصحية المعنية بكل حالة مشكوك فيها أو مؤكدة من الأمراض الواردة في قائمة الأمراض ذات التصريح الإجباري المذكورة في المادة 38 أعلاه".

الأمراض المتنقلة وكذا بعض الاستثناءات الأخرى التي تقتضيها الضرورات المهنية فإن التحلي بواجب الكتمان، وعدم معالجة المعطيات الطبية بعد تحقيق الهدف المبتغى، يعد التحصين الأساس لحماية المعطيات الطبية.

ووفقا لأحكام المادة 02 من القانون 18-07 والتي عرفت المعطيات في مجال الصحة بأنها" كل معلومة تتعلق بالحالة البدنية و / أو العقلية للشخص المعني، بما في ذلك معطياته الجينية".

والملاحظ من هذا التعريف هو جانب التعميم لمجال الحماية لتشمل مختلف الجوانب الصحية للفرد، بحيث أراد المشرع من خلالها إبراز الأهمية الكبيرة للمعطيات الصحية للفرد مقارنة بتلك المعطيات الحساسة والتي قد تتقارب معها في الكثير من النقاط كما سيتم التفصيل فيه لاحقا في الفرع الثاني من هذا المطلب والخاص بالبيانات الحساسة.

5-البصمة:

تعد البصمة من بين أهم الوسائل البيومترية لتحقيق الهوية، كونها ترتبط بالشخص منذ كونه جنينا في الشهر السادس ولا تتغير إلى ما بعد الوفاة، ولها سمات تميز كل شخص عن الآخر، وتتنوع مواضع الجسم التي يمكن من خلالها الحصول على البصمة الجينية، والتي تشمل: " الدم، أنسجة الجلد، العظام، الأظافر، الشعر، اللعاب، المخاط، المني، الأسنان.."[1]

ولقد ذهبت العديد من التشريعات إلى إدراج البصمة ضمن البيانات الشخصية المشمولة بالحماية، وتشمل جميع أنواع البصمات، العين، الأصبع واليد، وفي هذا الإطار أقرت اللجنة الوطنية للمعلوماتية والحريات بفرنسا ضمن مداولتها رقم 00-15 بتاريخ 21 مارس 2000، بأن بصمة الإنسان بجميع أشكالها تعد بيانا شخصيا[2].

[1] أشرف السعيد أحمد، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة للطباعة والنشر والتوزيع، الطبعة الثانية، مصر، 2015، ص152-153.

[2] Délibération CNIL n^0 00-015 du 21 mars 2000 portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Jean Rostand de Nice, destiné à

6-عنوان جهاز الحاسوب وعنوان بروتوكول الإنترنت (IP):

يتضمن كل جهاز حاسوب عنوانا رقميا يميزه يتشكل من 22 رقما، وعند ربطه بشبكة الإنترنت يمكن تحديد مكان تواجده.

وقد أقرت اللائحة الأوروبية العامة لحماية البيانات الشخصية لسنة 2016 بموجب مادتها الرابعة صراحة بأن معرف الإنترنت (IP) يدخل من ضمن البيانات الشخصية الواجبة الحماية من جهة، كما يمكن من خلالها اكتشاف المتسبب في نشر بيانات شخصية لشخص آخر موضوع المعالجة[1].

كما يعد عنوان بروتوكول الإنترنت من بين أبرز البيانات الشخصية المصنفة حديثا ضمن العديد من التشريعات الدولية، على غرار ما أقره المشرع الفرنسي بعد إجراء تعديلات عدة على أحكام القانون 78-17 ليتماشى مع مقتضيات الأحكام المدرجة ضمن النظام الأوروبي العام لحماية البيانات الشخصية رقم 679/2016، حيث أنه بمقتضى الأمر 2018-1125 المؤرخ في 12 ديسمبر 2018، المتضمن تطبيق مضامين المادة 32 من القانون 2018-493، المتعلق بحماية البيانات الشخصية، والذي بدوره أقر إلغاء التعاريف الخاصة بالبيانات ذات الطابع الشخصي الواردة ضمن القانون 78-17 وأحال إلى نص المادة الرابعة (04) من النظام الأوروبي 679/2016، والتي تضمنت في فقرتها الأولى اعتماد عنوان بروتوكول الإنترنت كبيان شخصي يقتضي تكريس كل آليات الحماية المتعلقة به، لاسيما خلال المعالجة الآلية للمعطيات.، حيث تمت الإشارة ضمن هذه الفقرة إلى ضبط تعريف البيانات الشخصية والذي يعد أساس حمايتها مع تضمينه لبعض صور هذه البيانات على سبيل المثال، كالاسم أو رقم التعريف أو بيانات الموقع أو المعر ّف عبر الإنترنت[2].

---

gérer à la cantine scolaire par la connaissance des empreintes digitales (demande d'avis n° 636.783); disponible sur https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017653883/ , le 25/12/2020.

[1] راجع المادة 04 من اللائحة الأوروبية لحماية البيانات لسنة 2016، المرجع السابق.

[2] «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est

الفرع الثاني: البيانات الشخصية الحساسة (غير العادية).

تكتسي البيانات الحساسة صبغة خاصة تقتضي جانبا دقيقا للحماية وحظر المعالجة إلا في حالات محصورة، يحددها الظرف الطارئ المسجل أو الضرورة الملحة، حيث نصت أغلب التشريعات على منع جمعها ومعالجتها إلا في إطار خاص تبرره مقتضياته المحددة قانونا.

حيث أكد مضمون القواعد الأوروبية الجديدة لحماية البيانات الشخصية على حرية كل دولة منتمية له في تنظيم معالجة البيانات الحساسة مع الالتزام بأحكام التشريع الأوروبي والتي من بينها ما تضمنه نص المادة التاسعة منه والتي أشارت إلى "حظر معالجة البيانات الشخصية التي تكشف الأساس العرقي أو الإثني و الآراء السياسية، والمعتقدات الدينية والفلسفية، والانتماء النقابي، والبيانات الجينية و البيومترية، بهدف تحديد هوية شخص طبيعي بذاته، وكذا حظر معالجة البيانات الصحية أو الجنسية "[1].

كما اهتمت العديد من التشريعات العربية بإدراج تعريف خاص بالبيانات الشخصية الحساسة على غرار ما ذهبت إليه تشريعات دول الجزائر، موريتانيا والمغرب، بينما اكتفت بعض التشريعات بالتعريف الضمني من خلال التشديد على حظر معالجتها مقارنة بالبيانات الشخصية الأخرى وهو ما ذهب إليه مشرعي دول مصر، تونس، وقطر، لكن

---

réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

[1] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية، المرجع السابق، ص 82.

"Art.9: Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdis".

القاسم المشترك هو ضبط مميزاتها والتي تشمل على الخصوص، القناعات الفلسفية، الدينية، الثقافية والاجتماعية وكذا الخصائص الفيزيولوجية، الجينية، البيومترية، العرقية والإثنية، وقد خصص كل من المشرعين المصري والقطري فصلا متعلقا بالبيانات الشخصية ذات الطبيعة الخاصة، حيث بالإضافة إلى إدراج الخصائص المميزة للبيانات الحساسة والمذكورة آنفا، فإنه تم إضافة البيانات المتعلقة بالصحة، العلاقة الزوجية، الأطفال والجرائم الجنائية[1].

ومن هذا المنطلق نرى أن المشرع المصري تبنى تعريفا شاملا للبيانات الشخصية الحساسة بمختلف محاورها، حيث شملت البيانات المتعلقة بالأطفال والصحة النفسية أو العقلية، كما فصله القانون رقم 151 لسنة 2020، والمتعلق بحماية البيانات الشخصية. حيث تمثل من خلاله " البيانات الشخصية الحساسة: البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية البيومترية أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة"[2].

والمشرع الجزائري بدوره عرف المعطيات الحساسة حسب نص المادة 02 من القانون 18-07 بأنها " معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية" وما يستخلص من هذا التعريف هو تفصيل أنواع البيانات الحساسة مع تضمين البيانات الشخصية الصحية ضمنها و التأكيد على المعطيات الجينية المتعلقة بالصفات الوراثية لشخص أو عدة أشخاص ذوي قرابـــــــة[3].

وبالرغم من عدم إشارة المشرع التونسي إلى تعريف المعطيات الحساسة صراحة ضمن القانون الأساسي عدد 63 المتعلق بحماية المعطيات الشخصية، إلا أن مضمون الفصل 14 منه أكد على حظر كل معالجة للبيانات ذات الطابع الشخصي المتعلقة بالأصول

[1] منى الأشقر جبور، محمود جبور، المرجع نفسه، ص83.

[2] راجع المادة الأولى من القانون رقم 151 لسنة 2020، المتعلق بحماية البيانات الشخصية المصري، الجريدة الرسمية العد 28 مكرر (هـ) في 15 يوليو سنة 2020.

[3] راجع المادة 02 من القانون 18-07، المرجع السابق.

العرقية أو الجينية أو بالمعتقدات الدينية أو بالأفكار السياسية أو الفلسفية أو النقابية أو بالصحة، بصفة مباشرة أو غير مباشرة، غير أنه يمكن معالجة المعطيات الشخصية من النوع المذكور بالفقرة السابقة إذا تمت بموافقة صريحة للمعني بالأمر[1].

وتجدر الإشارة إلى وجود جملة من الاستثناءات تحول دون حظر معالجة البيانات الحساسة إعمالا لمبدأ سلطان الإرادة الفردية، وموافقة واضحة دون إذعان، نابعة من الشخص المعني بالبيانات، أو ممثله القانوني، في حالة التعذر، أو بحسب ما تقتضيه الضرورة أو المصلحة العليا للبلاد، بعد الحصول على إذن خاص في شكل مرسوم، أو غيره من القرارات الإدارية في هذا الشأن[2].

وهناك من أدرج حالات أخرى مستثناة من حظر المعالجة، على غرار تلك المعالجة المبنية على اختيار الشخص المعني الانضمام إلى تجمعات حزبية، سياسية أو دينية، أو نقابية تلتزم في مبادئها بمعالجة البيانات الحساسة للمنتسبين إليها، ومرد ذلك هو التداخل الموجود بين تكريس مختلف الحريات وضبط حدودهاكمراعاة احتر ام الحرية الدينية، المخاطرة الطوعية، حرية التجمع، وغيرها من الحريات وعليه فإن سلطات الحماية تقل في هذا المجال[3].

وفي نفس السياق، يمكن أن تنجر عن معالجة البيانات الحساسة جملة من الأخطار إذا لم يتم ضبط استخدامها وكيفيات معالجتها ومن هذا المنطلق نجد أن أغلب التشريعات قد شملتها بحماية خاصة، فلا تعالج إلا بحسب الضرورة المتطلبة للوصول إلى الهدف الموضوعي المحدد مسبقا من هذه المعالجة، مما يقتضي إعمال واجب التحفظ من قبل المسؤول عن المعالجة[4].

---

[1] راجع الفصل 14 من القانون الأساسي عدد 63، المرجع السابق.

[2] سماعيلي مصطفى، البيانات الحساسة وفيروس كورونا - كوفيد19" البيانات الطبية نموذجا"، مجلة القانون والأعمال الدولية، المغرب، 22 ابريل 2020، ص06 متاح على الموقع https://www.droitetentreprise.com/19116/، تاريخ الاطلاع: 2020/12/20.

[3] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية، المرجع السابق، ص82.

[4] سماعيلي مصطفى، البيانات الحساسة وفيروس كورونا - كوفيد19" البيانات الطبية نموذجا"، المرجع السابق، ص10

وتجدر الإشارة أن المشرع الجزائري بدوره منع معالجة المعطيات الحساسة صراحة وأجاز معالجتها استثناء لأسباب مرتبطة بالضرورة المتعلقة بممارسة المهام من قبل المسؤول عن المعالجة، بحسب ما تقتضيه المصلحة العامة، أو عندما تتم المعالجة بناء على الموافقة الصادرة، دون إكراه أو إذعان، من قبل الشخص المعني، إلا في حالة وجود نص قانوني يقضي بذلك[1].

كما حصرت المادة 18 من القانون 18-07 خمسة (05) مجالات يمكن فيها للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي منح ترخيص مسبق لمعالجة المعطيات الحساسة، على النحو التالي:

1- إذا كانت المعالجة ضرورية لتكريس حماية المصالح الضرورية للشخص المعني أو لشخص آخر في حالة وجود الشخص المعني في حالة عجز بدني أو قانوني عن الإدلاء بموافقته.

2- تنفيذ المعالجة، بناء على موافقة الشخص المعني، من طرف مؤسسة أو جمعية أو منظمة غير نفعية ذات طابع سياسي أو فلسفي أو ديني أو نقابي، في إطار نشاطاتها الشرعية، شرط أن تخص المعالجة فقط أعضاء هذه المنظمة أو الأشخاص الذين تربطهم اتصالات منتظمة بها تتعلق بغايتها و ألا ترسل المعطيات إلى الغير دون موافقة الأشخاص المعنيين.

3- إذا كانت المعالجة تخص معطيات صرح بها الشخص المعني علنا عندما يمكن استنتاج موافقته على معالجة المعطيات من تصريحاته.

4- إذا كانت المعالجة ضرورية للاعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء، وأن تكون قد تمت حصرياً لهذه الغاية.

5- معالجة المعطيات الجينية، باستثناء تلك التي يقوم بها أطباء أو بيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي، والقيام بتشخيصات طبية وفحوصات أو علاجات.

وتأكيدا على حماية المعطيات الحساسة رتب المشرع الجزائري أقصى العقوبات مقارنة بغيرها من البيانات حيث جاء ضمن نص المادة 57 من القانون 18-07 " يعاقب

[1] راجع المادة 18 من القانون 18-07، المرجع السابق.

بالحبس من سنتين إلى خمس سنوات وبغرامة مالية من 200.000 دج إلى 500.000دج، كل من قام، دون الموافقة الصريحة للشخص المعني وفي غير الحالات الاستثنائية المذكورة أعلاه، بمعالجة المعطيات الحساسة"[1].

كما أشار القانون 20-05 المؤرخ في 28 ابريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما إلى حماية، بصورة غير مباشرة، للبيانات الشخصية الحساسة، حيث تم تعريف خطاب الكراهية حسب نص المادة الثانية ب" جميع أشكال التعبير التي تنتشر أو تشجع أو تبرر التمييز، وكذا تلك التي تضمن أسلوب الازدراء أو الإهانة أو العداء أو البغض أو العنف الموجهة إلى شخص أو مجموعة أشخاص على أساس الجنس أو العرق أو اللون أو النسب أو الأصل القومي أو الإثني أو اللغة أو الانتماء الجغرافي أو الإعاقة أو الحالة الصحية"، هذا بالإضافة إلى إقرار جملة من الجزاءات بالإضافة إقرار جملة من الآليات تضمنها هذا القانون للقضاء على خطاب الكراهية الذي يمس بالمعطيات الشخصية الحساسة[2].

وما نخلص إليه من خلال هذا الفصل هو أن المشرع الجزائري تبنى تعريفا واسعا للبيانات الشخصية، مميزا لها عن الحقوق الأخرى المرتبطة بحماية الخصوصية، مع إدراج بعض الأمثلة عن عملية معالجة البيانات.

وهذا التوجه يبرهن قصد المشرع الجزائري تكريس أكثر حماية لإدخال مختلف المعطيات ذات الطابع الشخصي ضمن مجال الحماية، إلا أن الممارسة الفعلية، من قبل السلطات الإدارية المستقلة، أو السلطة القضائية في مجال الفصل في المنازعات الخاصة بحماية البيانات الشخصية، هو المعيار الذي من شأنه إعطاء الصورة الحقيقية لمجال الحماية المكرسة تطبيقيا، وهو ما سيتم التفصيل فيه في المحور المخصص لهذا الجانب من الأطروحة.

[1] راجع المادة 57 من القانون 18-07، المرجع السابق.

[2] راجع المواد 2، 9، 30،31 و32 من القانون رقم 20-05 المؤرخ في 28 ابريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية عدد 25 بتاريخ 29 ابريل 2020.

الفصل الثاني: الدوافع الملزمة لحماية البيانات الشخصية

بعد التطرق إلى تعريف البيانات الشخصية لابد من توضيح أهمية هذه الحماية التي دفعت مختلف التشريعات إلى إعطائها أهمية بالغة وتخصيصها بترسانة قانونية تتغير بتغير المستجدات لاسيما وأن هذا المجال مرتبط بالفضاء الرقمي والسيبراني المعروف بسرعة تغيره وتطوره، إذ يعد في نظرنا أهم مؤثر في البيانات الشخصية والذي من خلاله سنتطرق ضمن هذا الفصل إلى تجلية أسباب ودوافع لجوء أغلب التشريعات إلى تقنين حماية البيانات الشخصية على نطاق واسع، والتي من خلال ما وصلنا إليه يمكن حصر هذه الدوافع في مجالين، الأول يخص معالجة البيانات الشخصية في مختلف صورها من تجميع وتصنيف وما يمكن أن يعترضها من سرقة أو تعديل مخالف للحقيقة أو نقل وغيرها من العوامل الموضحة في المبحث الأول من هذا الفصل.

أما الدافع الثاني فيتجسد في تأثير التطور التكنولوجي على البيانات الشخصية، من حيث استعمال التكنولوجيات المتطورة، من هواتف رقمية وحواسب، بطاقات تخزين فائقة في ظل الانتشار الواسع للتطبيقات والمواقع الالكترونية، التي تسهم في التأثير ونشر البيانات الشخصية بسرعة كبيرة، لاسيما بتأثير الإنترنت.

المبحث الأول: مبررات الحماية المتعلقة بتجميع وتصنيف البيانات الشخصية وتهديد خصوصيتها

تعد عمليات الجمع والتصنيف للبيانات الشخصية مراحل جد حساسة تتطلب مراعاة جملة من الضوابط تختلف باختلاف الوسائل المستعملة في المعالجة بالإضافة إلى الشخص القائم بالمعالجة، حيث قد يتسبب أي إهمال لضابط من الضوابط في التأثير على البيانات الشخصية سواء بسرقتها، تعديلها أو نقلها أو نشرها دون موافقة المعني بالمعالجة وعلية سيتم التطرق إلى تقنيات جمع وتصنيف البيانات الشخصية (المطلب الأول)، ثم بسط العوامل التي تهدد خصوصية البيانات الشخصية خلال عملية المعالجة (المطلب الثاني)، كما سيتم تفصيله أدناه.

المطلب الأول: ضوابط تجميع وتصنيف البيانات الشخصية

تشكل عمليات جمع وتصنيف البيانات المتعلقة بالأفراد، المرحلة الحساسة في معالجة البيانات من قبل أي جهة كانت، إذ ليس في كل الأحيان يكون الجمع بغرض الاستغلال السلبي لهذه البيانات و إنما حتى في شقه الايجابي مثل العمل الذي تقوم به الإدارات الرسمية والمؤسسات باختلاف أنواعها، حيث أنه في حالة الوصول إلى هذه البيانات المجمعة المخزنة والتصرف فيها أو تصنيفها ونقلها إلى مجالات أو فضاءات غير ملائمة ودون موافقة المعنيين يمثل الخطر الكبير على هذه البيانات ومن هنا تنطلق وتتأسس حماية البيانات الشخصية[1].

ولتفصيل هذه العوامل أكثر سنتطرق في الفرعين المواليين إلى كل مرحلة على حدا بدءً بجمع المعطيات ثم تصنيفها.

الفرع الأول: تجميع البيانات الشخصية

إن الحديث عن المساس بالبيانات الشخصية والبحث عن أساليب لحمايتها لا يطرح، إذا كانت هذه البيانات مؤمنة ومحفوظة على مستوى الأشخاص المعنيين ولم يتم تجميعها أو تداولها مباشرة أو باستعمال التقنيات الحديثة.

لكن مرحلة المساس بالبيانات الشخصية تبدأ منذ مباشرة تجميعها، لاسيما التجميع الالكتروني باستعمال التقنيات الحديثة كالحاسوب والهواتف الذكية الموصولة بشبكة الإنترنت والتي قد تؤثر في البيانات المجمعة بنقرة واحدة في ثوان أو دقائق معدودة، مما يستدعي مراعاة واجب التحفظ و أخذ كل الاحتياطات اللازمة عند قيام المعالج بجمع المعطيات الشخصية.

كما انتشر في الوقت الراهن، اعتماد أغلب المؤسسات من أجل تحسين الخدمة وسرعة المعالجة، على تجميع البيانات الشخصية ضمن تطبيقات خاصة بكل مجال ونذكر على

[1] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص397.

سبيل المثال موضوع عصرنة المرفق العمومي، بحيث لا ننكر ما تم إحرازه من تقدم في مجال تقريب الإدارة من المواطن والسرعة في التكفل بمعالجة مختلف الملفات والاستفادة من اغلب الخدمات الإدارية عن بعد، إلا أن هذه العملية انطلقت واعتمدت في أساسها على تجميع البيانات الشخصية للمواطنين من السجلات المختلفة ومختلف المؤسسات، وهنا يطرح السؤال كيف يتم الالتزام بحفظ وصيانة كل هذا الحجم من البيانات المجمعة؟

أكيد الجواب سيرتكز على الآليات التقنية المعدة للحماية كالتطبيقات الذكية وعناوين الكومبيوتر وشبكة الإنترنت (IP)، لكن بالمقابل ظهرت العديد من المستجدات على مستوى العديد من الدول وأبانت نسبية برامج وتطبيقات الحماية المقررة، إذا لم يتم تقييد من يقوم بجمع هذه البيانات من جهة وكذا كيفيات تصنيفها ومعالجتها من جهة أخرى، لاسيما ضمان عدم اختراقها أو نقلها إلى الخارج.

أما الجانب الآخر والأكثر حساسية في مجال الحماية هو عملية جمع البيانات الشخصية من قبل مؤسسات وشركات خاصة عبر تطبيقات متاحة أغلبها على شبكة الإنترنت، تجمع كل ما يتعلق بالشخص من تاريخ ميلاده، عناوينه السكنية والالكترونية، رقم هاتفه، وضعه الصحي ونتيجة تحاليله،هواياته وذوقه، بالإضافة إلى غيرها من التفاصيل المصنفة كبيانات شخصية ضمن أغلب التشريعات الدولية بالرجوع إلى تبني المعنى والمفهوم الواسع للبيانات الشخصية، كما تم التطرق إليه في الفصل الأول من هذه الأطروحة.

إن هذا النوع من جمع البيانات له العديد من الدوافع، حيث أرجأ العديد من الباحثين ذلك إلى تبني نظرية التسويق بأساليبه الحديثة لاسيما الاعتماد على ما هو متاح على شبكة الإنترنت من خلال استغلال مضامين مختلف البيانات الشخصية الموجودة على مختلف التطبيقات، الأمر الذي من شأنه تشكيل تحدي في إطار اعتماد الطرق الحديثة

للتجارة الشخصية بالتسويق المباشر من جهة، وكذا تحدي حماية المعطيات الشخصية، من جهة أخرى [1].

وعليه فإن مبدأ نظرية التسويق ينطلق من جمع أكبر حجم من البيانات عن الأفراد المستهدفين مع التدقيق في أذواقهم ورغباتهم لتحقيق أكبر نسبة من الأرباح[2].

كما تعتمد النظرية على الدعاية والإشهار للخدمات واللجوء إلى المعطيات الشخصية لكل زبون وتوجيه المنتج أو الخدمة المطلوبة مع ما يتلاءم ورغباته، وفي هذا الإطار تقوم بإدارة المؤسسة مع الزبائن من خلال التدقيق في معطياتهم المقدمة مسبقا على غرار أرقام الهاتف، البريد الالكتروني، واستغلال هذه الأخيرة لجمع اكبر معلومات حسب كل زبون مع تقديم تحفيزات لترويج المنتج كالاستفادة من بعض الخدمات ما بعد البيع أو منتجات مجانية[3].

وبالرغم من أن هدف نظرية التسويق المباشر هو التعريف بالمنتج أو الخدمة بصفة مباشرة للزبون من خلال بياناته والاستعانة بإنشاء مواقع إلكترونية متخصصة للتعريف لإشهار المنتجات والخدمات من جهة، وكذا جمع أكبر معلومات حول الزبائن من جهة أخرى. إلا أنه يسجل نوع من التضارب بين كل من البائع والمشتري، مما يقتضي إبرام عقود ولو عن بعد تكرس البحث عن أكثر ضمانات من الجانبين للتوافق وتحقيق توازن المفاضلة عن طريق التمييز بين استغلال البيانات وبيع البيانات في حد ذاتها على غرار ما تقوم به الكثير من الشركات العالمية الكبيرة في مجال تكنولوجيا المعلومات[4].

---

1 Tian, Ling; Li, Jiaxin; Li, Wei; Ramesh, Balasubramaniam; Cai, Zhipeng, Optimal Contract-based Mechanisms for Online Data Trading Markets , IEEE Internet of things journal , Vol 14, Nu 08 ,2019, p 1

2 Dawn Iacobucci; Jonathan D. Hibbard, Toward an encompassing theory of business marketing relationships (BMRS) and interpersonal commercial relationships (ICRS): An empirical generalization, Journal of Interactive Marketing, Vol 13, Nu3,1999, P15.

2 سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص400.

4 Tian, Ling; Li, Jiaxin; Li, Wei; Ramesh, Balasubramaniam; Cai, Zhipeng,OP- Cit, P2.

كما ذهب العديد من الباحثين في مجال تجسيد نظرية التسويق إلى الحث على ضرورة تكريس حماية البيانات الشخصية بصفة رضائية فعالة عن طريق مراجعة العلاقات بين المنتجين المسوقين والعملاء، فبدل التحايل في استغلال بياناتهم من أجل تسويق المنتجات، يمكن الاتفاق مسبقا عن تسويق العلاقات في حد ذاتها بصفة رضائية، أي أن العملاء يمكنهم الائتمان على بياناتهَ م لاعتبار التسويق بشكل عام كتبادل للمنافع لضمان أكبر حماية للبيانات وأكبر أرباح للمسوقين[1].

غير أن التطور الذي عرفه مجال البرمجيات لأجهزة الحاسوب يمكن أن يؤمن حماية أوسع لاسيما باعتماد تقنيات حديثة كالتوقيع الالكتروني البحت والذي يشمل رقم سري خاص وآخر عام للتواصل مع مسوقي الخدمات[2].

وبالرجوع إلى نموذج المدينة الذكية أين يتم جمع وتخزين جميع أنواع بيانات المستخدمين في الأجهزة الإلكترونية لجعل كل شيء ذكيا، مع ملاحظة أن الهواتف الذكية في أغلبها تبقى فاقدة لمعايير الحفاظ على الخصوصية وعدم تسريب البيانات المجمعة بسبب الإفراط في جمع البيانات بالنظر لطبيعة التطبيقات الخاصة بكل صنف من أصناف الهواتف الذكية وهو ما يشكل خطرا كبيرا على خصوصية هذه البيانات، وبدوره يبقى التحدي الراهن لمجابهة المخاطر الأمنية المحتملة على مستوى المدينة الذكية[3].

وقد ذهب بعض الباحثين في مجال تكريس الحماية للأنظمة المعلوماتية للمدن الذكية بتقديم بدائل وحلول للتقليل من الإفراط في جمع البيانات عن طريق وضع جميع بيانات

---

[1] Dawn Lacobucci; Jonathan D. Hibbard, Toward an encompassing theory of business marketing relationships (BMRS) and interpersonal commercial relationships (ICRS): An empirical generalization, Op-Cit, P30.

[2] تم استخلاص هذه الفكرة من خلال نقاش مع أحد الخبراء في مجال البرمجيات.

[3] Yibin Li; Wenyun Dai; Zhong Ming; Meikang Qiu , Privacy Protection for Preventing Data Over-Collection in Smart City, IEEE Transactions on Computers, Volume: 65, Issue: 5, May 1 2016, p1347.

المستخدمين في سحابة باستعمال تجارب تقنية أثبتت نجاعتها، يمكن من خلالها تحسين أمان بيانات المستخدمين بشكل ملحوظ وفعال[1].

و أكد المشرع الفرنسي على شرطين أساسيين، لمشروعية مختلف العمليات المتعلقة بجمع البيانات الشخصية وهما[2]:

1.مراعاة المشروعية في جمع البيانات.

ترتكز مشروعية جمع البيانات عن طريق الالتزام بأحكام القانون المتعلق بحماية البيانات ذات الطابع الشخصي، وذلك بتحديد طبيعة، غرض وأنواع البيانات المعنية بالجمع، مع الالتزام بإبلاغ صاحب البيانات قبل الشروع في تجميع بياناته وفي حالة الحصول على الموافقة يتوجب احترام الإجراءات الموضوعية خلال معالجة البيانات وفق ما ينص عليه قانون حماية البيانات حسب كل دولة تكرس ذلك.

وفي حالة مخالفة الإجراءات المحددة فيمكن أن نكون أما جريمة الجمع غير المشروع للمعطيات لاسيما إذا ثبت تسجيل وحفظ هذه البيانات، وقد جاء ذلك واضحا في قرار محكمة النقض الفرنسية بتاريخ 1987/11/03، الصادر عن الغرفة الجزائية، والتي اعتبرت أن لا يكفي لقيام هذه الجريمة جمع البيانات بطريقة تدليسية، غير نزيهة أو غير مشروعة، و إنما يتوجب تسجيل وحفظ هذه البيانات في ملف خاص يدوي أو آلي[3].

كما أقرت اللجنة الوطنية (CNIL)، في قضايا متعددة، غرامات، على مستخدمي الإنترنت الذين يقومون بتجميع عناوين البريد الالكتروني دون علم أصحاب هذه العناوين لاعتباره تصرفا غير مشروع، وهذا ما أكدته محكمة النقض الفرنسية بإقرارها استحقاق معاقبة من يقوم بتجميع عناوين البريد الالكتروني للأشخاص دون علمهم[4].

---

[1] Yibin Li; Wenyun Dai; Zhong Ming; Meikang Qiu, IBID, P1350.

[2] راجع المادة 06 من القانون 87-17، المتعلق بحماية البيانات الشخصية، المرجع السابق.

[3] تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية،- مجلد4، العدد2، 2019،ص 1543.

[4] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص416.

وقد أقر المشرع الجزائري بموجب أحكام المادة 59 من القانون 18-07، عقوبة أقصاها الحبس لمدة ثلاث (03) سنوات لكل من يقوم بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة. والملاحظ هنا هو عدم دقة المصطلحات، لاسيما عند الرجوع إلى نص الفقرة هـ من المادة 09 من القانون 18-07[1]، والتي تشترط في المعطيات الشخصيات المجمعة أن تكون محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها[2].

2. تحديد بوضوح ودقة الهدف من جمع البيانات:

إن ضبط الغاية من جمع البيانات تسهم بصورة كبيرة في ضمان حمايتها، لاسيما إذا كانت الأهداف موضوعية إيجابية، وفي حالة العكس فإنه يتوجب أخذ الاحتياطات اللازمة، وعليه فإن الجمع لابد أن يكون لغاية مشروعة وبكل شفافية[3].

وفي هذا الجانب اعتبر المشرع الفرنسي أن الجمع العشوائي غير المدروس والمضبوط للبيانات الشخصية يعد خرقا لأحكام قانون حماية البيانات الشخصية رقم 87-17، ويقود إلى تنفيذ عقوبات جزائية وأخرى تأديبية تعود السلطة التقديرية فيها للجنة الوطنية للمعلوماتية والحريات (CNIL).

وفي نفس السياق أشار نص المادة السادسة من الإرشاد الأوروبي رقم 46-1995 المتعلق بحماية الأفراد فيما يخص معالجة البيانات الشخصية، على أن الدول الأعضاء التي تقوم بمعالجة البيانات يجب أن تكون هذه البيانات المجموعة محددة الأهداف، مع التزام الدول الأعضاء بتكريس مختلف الضمانات حول طريقة وأغراض جمع هذه البيانات

[1] راجع المادتين 09 و 59 من القانون 18-07، المرجع السابق.

[2] تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07 دراسة تحليلية، المرجع السابق، ص 1543.

[3] انظر الفقرة الثانية من المادة 06 من القانون 87-17، مشار إليه.

بطريقة مشروعة لها صلة بالأهداف التي جمعها من أجلها وأن تكون كافية، ملائمة، مجددة،عادلة وقانونية[1].

وما يمكن استخلاصه في مجال جمع البيانات هو أن رضاء المعني بجمع بياناته وفق الأهداف المسطرة يعد جوهر القيام بهذه العملية، إلا أن الرضاء يبقى مجاله واسعا، ويحتاج إلى التدقيق سواء من ناحية البيانات المسموح بجمعها أو مصير هذه الأخيرة في حالة تغير الأهداف بعد عملية الجمع والشروع في التصنيف وهو ما سيتم التفصيل فيه في الفرع الموالي.

الفرع الثاني: تصنيف البيانات الشخصية

يعد تصنيف البيانات الشخصية المرحلة الموالية لعملية جمع البيانات، حيث يختلف تصنيف البيانات باختلاف مجال المعالجة، فبعد جمع كل البيانات المتعلقة بشخص في ملف واحد، مهما اختلفت أنواعها، أو أوقات جمعها بحيث؛ يتم الاعتماد على تطبيقات حديثة تسهل الوصول إلى أدق البيانات في زمن قصير وهو ما يشكل النقطة السلبية من ناحية خطر الوصول إلى هذه البيانات المجمعة والمصنفة[2].

وانطلاقا من ما تم توضيحه في الفرع السابق الخاص بجمع البيانات، لاسيما تلك المتعلقة بالعملاء في إطار اعتماد نظرية التسويق المباشر، فانه تجدر الإشارة إلى ضرورة إلزام مديري البيانات أو أصحاب المؤسسات،. المستغلة للبيانات الشخصية، تحديد سياسات استخدام هذه البيانات وتصنيفها حسب درجة حساسيتها وسريتها لتخصيص حماية لكل منها على حدا، حسب درجة الأهمية والخطورة التي قد تلحق في حالة الوصول إليها أو سرقتها[3].

---

[1] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، المرجع السابق، ص403-404.

[2] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي (القسم الأول) المرجع السابق، ص397.

[3] مروة زين العابدين صالح، المرجع السابق، ص409

وبالإضافة إلى اعتماد الأطر التقنية لحماية المعطيات الشخصية المصنفة فإنه لابد من إدراج ضمن قوانين حماية هذه المعطيات الشخصية نصوص أخرى تضبط تضييق مجال معالجة البيانات الحساسة أو التي تتطلب حماية أكثر لاسيما تلك التي تتميز بالطابع السري،ويمكن أن يتسبب نشرها أو سرقتها في إلحاق أضرار مادية ومعنوية بالأشخاص المعنيين وكذا على النظام العام، إذا كان المعنيون بهذه البيانات يشغلون وظائف حساسة.

وقد أشار الفقيه بيلتي (Peltier) في مجال تصنيف البيانات إلى ضرورة مراعاة طبيعة كل معلومة عند جمعها بحيث أكد على أنه " يجب أن تصنف جميع المعلومات المنشأة إلى واحدة من التصنيفات الثلاثة: السرية، الاستخدام الداخلي، الاستخدام العام، متاحة من حيث الوصول إليها وممكن أن يكون ممنوع الوصول إليها إلا من قبل أشخاص مخولين بذلك"[1]

والمشرع الجزائري بموجب الأمر 21-09 المؤرخ في 08 يونيو 2021، المتعلق بحماية المعلومات والوثائق الإدارية[2] قد اقر حماية عامة لمختلف الوثائق الإدارية المصنفة سواء ضمت معلومات شخصية أو عامة حيث أشار في الفصل الثاني منه ضمن المادة السادسة (06)إلى تصيف الوثائق حسب درجة حساسيتها،إلى الأصناف التالية:

– "سري جدا"، يشمل كل الوثائق التي قد يلحق إفشاؤها خطرا على الأمن الوطني الداخلي والخارجي.

– "سري"ويتضمن الوثائق التي يلحق إفشاؤها ضررا خطيرا بمصالح الدولة.

– "واجب الكتمان" : يتعلق بالوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الحكومة أو الوزارات أو الإدارات أو إحدى المصالح العمومية

[1] محمد عبد حسين الطائي، ينال محمد الكيلاني، إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان- الأردن، الطبعة الأولى، 2015، ص227.

[2]الجريدة الرسمية، العدد45، المؤرخة في 09 يونيو 2021

– توزيع محدود، ويتضمن الوثائق التي يؤدي انتشارها إلى المساس بمصالح الدولة ولا يجوز الإطلاع عليها إلا من قبل الأشخاص المؤهلين بحكم الوظيفة.

وقد أحال هذا الأمر تقنيات تطبيق وتفعيل هذا التصنيف إلى التنظيم.

وعليه فإن هذا النص القانوني قد أضاف لبنة أساسية في تكريس تصنيف البيانات بمختلف أنواعها وكذا إلزام القائم بجمع وتصنيف مختلف البيانات بتأمين مختلف الوثائق والمعلومات المجموعة لتنظيم تداولها وحفظها.

كما أكد نص المادة السابعة (07) من الأمر 21-09 إلى وجوب إخضاع موظفي السلطات المعنية إلى تكوين خاص في استعمال المعلومات والوثائق المصنفة[1].

كما أقر المشرع الجزائري بموجب هذا النص التشريعي جملة من الضمانات والالتزامات للموظف العمومي لمنع إفشاء المعلومات والمعطيات المصنفة نلخصها كما يلي:

1. يمنع إنشاء أو نشر محاضر وأوراق التحريات والتحقيق القضائي أو تمكين من لا صفة له من حيازتها.
2. يمنع أخذ نسخة أو صور للوثائق المصنفة من قبل أي موظف إلا بعد الحصول على الموافقة الصريحة من قبل السلطة المعنية.
3. يجب على كل شخص يحوز على وثيقة مصنفة دون أن يكون مؤهلا لذلك تسليمها إلى السلطات المعنية ويمنع عليه إفشاء مضمونها.
4. على الموظف العمومي الالتزام بالسر المهني أثناء قيامه بوظيفته وبعد 10 سنوات من توقيفه أو انتهاء علاقته المهنية بآي سبب من الأسباب.
5. يحظر على الموظف العمومي إخراج الوثائق المصنفة أو نسخ منها خارج المؤسسة الرسمية، إلا في حالة ضرورة المصلحة أو الوظيفة.
6. يمنع على الموظف العمومي الإدلاء لوسائل الإعلام أو عبر وسائل التواصل الاجتماعي بأي معلومة أو تعليق أو تصريح أو مداخلة حول المعلومات أو الوثائق

[1] راجع المادة 07 من الأمر 21-09، مشار إليه.

التي اطلع عليها بحكم مهامه أو حول مسائل مازالت قيد الدراسة لدى الجهة التي يعمل فيها، ما لم يكن مرخصا له بذلك.

7.يتعرض الموظف الذي يفشي عمدا وثائق مصنفة إلى التسريح من العمل[1].

هذا بالإضافة إلى إقرار جملة من العقوبات التأديبية والجزائية في حق كل من يقوم بإفشاء أو استغلال معلومات ووثائق مصنفة، هذا كله في انتظار صدور النصوص التنظيمية لتحديد صيغة هذه الوثائق وتكريس حق المواطن المعني في الوصول إلى المعلومة من جهة أخرى[2].

كما يتطلب تصنيف البيانات في رأي العديد من الباحثين في مجال أمن البيانات ضرورة مراعاة إجراءات قبلية صحيحة في التعامل مع الملفات الورقية وكذا مختلف أجهزة المعالجة، يمكن تلخيصها على النحو التالي[3]:

- حظر وصول الأشخاص غير الحائز ين على ترخيص مسبق إلى مختلف الملفات المصنفة السرية وغير السرية.
- ضرورة وضع الملفات، لاسيما السرية منها، في خزانات مقفلة أو مواقع أمينة ذات حماية عالية وتشفير دقيق.
- عدم الاحتفاظ بالعديد من النسخ لنفس البيانات، مع الحذر الشديد على إرجاع النسخ الأصلية بعد إتمام إجراءات النسخ.
- الاستعانة بالماكينات الخاصة بتمزيق الوثائق غير الواضحة أو الزائدة عن الاحتياج وتجنب رميها مباشرة في سلة المهملات.
- توخي الحيطة والحذر عند إرسال معلومات سرية باستعمال أجهزة الفاكس وذلك بتكليف موظفين أمناء على كل جهاز فاكس مع تنصيب هذا الأخير ضمن مكان مقفل

[1] راجع المواد من 08 إلى 19 من الأمر 21-09، مشار إليه.

[2] بالرجوع إلى مضامين الأمر 21-09 نجد العديد من الإحالات للتنظيم، ويرجع ذلك في نظرنا إلى حساسية هذه البيانات المعنية بالحماية من جهة ولضرورة التفصيل حسب كل مجال أو قطاع وزاري لاستخلاص التصنيف الدقيق لهذه البيانات

[3] محمد عبد حسين الطائي، ينال محمد الكيلاني، المرجع السابق، ص 221-224.

ومحمي مسبقا، مع استعمال أجهزة خاصة لمنع حدوث أي مراقبة غير مرخصة لأجهزة الفاكس، لاسيما تلك التابعة للأجهزة الأمنية.

- لابد من تضمين الملفات الالكترونية بكلمات سر دقيقة وغير قابلة للوصول إليها إلا من طرف الشخص المكلف أو المعالج للمعطيات، مع الحرص على تغيير كلمة السر من فترة لأخرى، والحذر من التسجيل الآلي لكلمات السر على أجهزة المعالجة أو على المواقع الالكترونية بتأثير تقنية الكوكيز (cookies)[1]، بجميع أنواعها ومكوناتها[2].

- تخزين المعطيات في أقراص صلبة خارجية والاحتفاظ بها في مكان مقفل وآمن.

- عدم تخزين المعلومات الحساسة على أجهزة الحاسب أو غيرها من الأجهزة الأخرى إلا للضرورة وبنسبة قليلة.

---

[1] هذه الآلية تحتاج إلى الكثير من الدقة حيث أنه بتفعيل آلية الكوكيز فإن تسجيل كلمات السر قد يحدث بمجرد النقر على الإشعار الذي يظهر تلقائيا على جهاز الحاسوب بعد كتابتك لاسم المستخدم وكلمة السر، مما يقتضي مراجعة إجراءات الأمان المتعلقة بالأجهزة المستعملة بالإضافة إلى مختلف محركات البحث تكريسا للحفاظ على سريتها ومنع أي تسجيل غير مشروع لهذه البيانات السرية المعالجة إلكترونيا، بحيث أن تقنية الكوكيز سلاح ذو حدين فكما أنها توفر الوقت والاختصار في البحث، إلا أنها قد تكون سببا لوصول الغير إلى كل محركات ومواضيع البحث الشخصية، ويميز المختصين في هذا المجال نوعين من ملفات الكوكيز، المؤقتة (Session cookies) و الدائمة حسب المعالجة (Persistent cookies).

- "Session cookie: That is erased when the user closes the web brows. The session cookie is stored in temporary memory and is not retained after the browser is closed. Session cookies do not collect information from the user computer. They typically will store information in the form of a session identification that does not personally identify the use".
- Persistent cookie: Also called a permanent cookie or a stored cookie, a cookie that is stored on a user hard drive until it expires) persistent cookies are set with expiration dates) or until the user deletes the cookie. Persistent cookies are used to collect identifying information about the user, such as web surfing behavior or user preference for a specific web site "

Penenberg, Adam; Cookie Monsters, State, November 7,2005,P43

[2] نقلا عن مروة زين العابدين صالح، المرجع السابق، ص334.

- الاستعانة بأنظمة الحماية الناجعة بواسطة الخوارزميات التي تمكن من منع أي دخول لشخص أجنبي وتمكين غلق جهاز الحاسب أو الهاتف المستعمل أمام من يحاول خرق سرية البيانات[1].

المطلب الثاني: عوامل تهديد خصوصية البيانات الشخصية

تجسد خصوصية البيانات الشخصية المدى الذي يمكن أن تبلغه مختلف المعطيات المتداولة المتعلقة بالشخص الطبيعي، بحيث تشكل النواة الأساس في تجسيد حرية الفرد في بياناته من جهة، وكذا حقه في السماح بالتصرف فيها أو اللجوء إلى تفعيل الآليات القانونية التي تكرسها قوانين حماية البيانات، محليا أو دوليا لاقتصاص حقه، من جهة أخرى.

وقد ذهب الفقيه ميلر إلى تعريف خصوصية البيانات ب" قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم" the individual's ability to control the circulation of information relating to him" "[2].

وعليه لا يمكن التحكم في دورة المعلومات إلا بمواجهة العوامل التي تهدد هذه المعلومات في مرحلة من مراحل الدورة التي تسلكها منذ تجميعها إلى غاية محوها أو انتهاء عملية معالجتها.

كما يشكل التصدي لمختلف العوامل والمؤثرات التي تهدد خصوصية هذه البيانات سواء من ناحية التعامل غير الشرعي والاتجار بالبيانات أو فقدان هذه البيانات وسرقتها

---

[1] تزداد الحاجة إلى المحافظة على سرية البيانات، عند معالجة ملفات باستعمال الحاسوب على مستوى المؤسسات العمومية، لاسيما تلك التي تعتمد على ملفات قاعدية تضم بيانات دقيقة عن الأشخاص مقابل منحهم الوثائق والتراخيص اللازمة. وهذا الأمر يستوجب ضمان استخدام آلية التشفير (Encryption)، بحيث لا يمكن قراءة وفهم البيانات إلا بمعرفة مفتاح فك هذا التشفير؛ لأكثر توضيح راجع، خضر مصباح الطيطي،إدارة تكنولوجيا المعلومات، المرجع السابق، ص289.

[2] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مرجع سابق، ص42.

واستغلالها لأغراض تضر بالمعني أو صاحب البيانات، أبرز الدوافع الباعثة بتكريس حماية البيانات الشخصية وهو ما سيتم التفصيل فيه في العنصرين المواليين:

الفرع الأول: التعامل في البيانات الشخصية والاتجار بها

يحتم التعامل في البيانات الشخصية دافعا لبسط الحماية اللازمة لمختلف البيانات المتداولة، لاسيما الاعتماد الكبير على تكنولوجيا المعلومات في مختلف مناحي الحياة، المتعلقة بمعالجة البيانات الشخصية من خلال تبادل هذه البيانات، بواسطة رسائل نصية، صوتية والكترونية، وصولا إلى المعاملات التجارية الالكترونية، والتعليم والتسويق الالكترونيين.

إلا أنه وبالرغم من مزايا استعمال مختلف الوسائط والوسائل الرقمية في تداول البيانات ومعالجتها، إلا أن الأمر يحتاج إلى الحماية اللازمة لمواجهة الاتجار غير الشرعي بهذه البيانات، بمختلف الصور من تجسس وقرصنة وتنصت على الأفراد والمؤسسات، أو تخريب للبرامج والبيانات المتحكمة في خوارزميات حماية هذه البيانات[1].

وعليه وللتفصيل أكثر في إبراز مختلف الجوانب الخاصة بالاتجار والاستعمال غير الشرعي للبيانات الشخصية لابد من التطرق إلى تأثير كل من العقود الالكترونية وقواعد بيانات محر كات البحث على خصوصية هذه البيانات، كما يلي:

أولا:تأثير العقود الإلكترونية على خصوصية البيانات الشخصية

تمثل العقود الالكترونية نوعا خاص من أنواع العقود، وهي تختلف عن العقود التقليدية في نقطة جوهرية من حيث الحضور والتراضي في نفس المكان، إذ تكمن الطرفان من تبادل الإيجاب والقبول باستخدام وسائل تكنولوجية حديثة تنقل البيانات الشخصية لكلا أطراف العقد، مهما كان موقعهم.

[1] خضر مصباح الطيطي، إدارة تكنولوجيا المعلومات، دار الحامد للنشر والتوزيع، عمان، ط1، 2012، ص281.

والقانون لم ينكر صحة وسلامة هذا النوع من التعاقد الالكتروني بين نظام نقني مبرمج وبين شخص طبيعي، إذا أدرك وعلم هذا الأخير أن النظام هو من سيتولى إبرام أو تنفيذ العقد بشكل تلقائي إلكترونيا[1].

ولقد عرف بعض الفقهاء عقد التجارة الإلكترونية، بإعطاء صفة العالمية، على النحو التالي: " العقد الذي تتلاقى فيه عروض السلع والخدمات بقبول من أشخاص في دول أخرى، وذلك من خلال الوسائط الرقمية المتعددة ومنها شبكة الإنترنت بهدف إتمام العقد"[2].

كما تضمن التوجيه الأوروبي المتعلق بحماية المستهلك في العقود المبرمة عن بعد الصادر في 20 ماي 1997، تعريفا لهذا النوع من العقود بأنه " عقد متعلق بالسلع والخدمات يتم بين مورد ومستهلك من خلال الإطار التنظيمي الخاص بالبيع عن بعد أو تقديم الخدمات التي ينظمها المورد والذي يتم باستخدام واحدة أو أكثر من وسائل الاتصال الإلكترونية _ remote communication_ حتى إتمام العقد"[3].

والمشرع الجزائري بموجب قانون التجارة الالكترونية رقم 18-05[4]، ووفق ما نصت عليه المادة 06 منه والتي عرفت العقد الالكتروني بالاستناد إلى المفهوم الذي تضمنه القانون 04-02 المؤرخ في 23 يونيو 2004، المحدد للقواعد المطبقة على الممارسات التجارية، والذي جاء في مادته الثالثة أن العقد يقصد به " كل اتفاق أو اتفاقية تهدف إلى بيع سلعة أو تأدية خدمة، حرر مسبقا من أحد أطراف الاتفاق، مع إذعان الطرف الآخر بحيث لا يمكن هذا الأخير إحداث تغيير حقيقي فيه . يمكن أن ينجز العقد على شكل

---

[1] خالد ممدوح إبراهيم، إبرام العقد الالكتروني –دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2006،ص 26 وكذا مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، المرجع السابق، ص351.

[2] أحمد عبد الكريم سلامة، القانون الدولي الخاص النوعي (الإلكتروني، السياحي والبيئي)، دار النهضة العربية، الطبعة الأولى، 2002، ص53.

[3] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي و القانون الوطني، المرجع السابق، 354.

[4] القانون 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الالكترونية، الجريدة الرسمية عدد 28، المؤرخة في 16 ماي 2018.

طلبية أو فاتورة أو سند ضمان أو جدول أو وصل تسليم أو سند أو أي وثيقة أخرى مهما كان شكلها أو سندها تتضمن الخصوصيات أو المراجع المطابقة لشروط البيع العامة المقررة سلفا"[1].

كما أضاف نص المادة 06 من القانون 18-05 المذكور سالفا بالإضافة إلى هذا التعريف ما يلي "ويتم إبرامه عن بعد، دون الحضور الفعلي والمتزامن لأطرافه باللجوء حصريا لتقنية الاتصال الإلكتروني"[2].

وتضمن نص المادة 11 من القانون 18-05 شروطا واجب توفيرها من قبل المورد الالكتروني ضمن العرض التجاري والتي تشمل على الأقل:"

- رقم التعريف الجبائي، والعناوين المادية والإلكترونية، ورقم هاتف المورد الالكتروني،
- رقم السجل التجاري أو رقم البطاقة المهنية للحرفي،
- طبيعة وخصائص وأسعار السلع أو الخدمات المقترحة باحتساب كل الرسوم،
- حالة توفر السلعة أو الخدمة،
- كيفيات ومصاريف وآجال التسليم،
- الشروط العامة للبيع، لاسيما البنود المتعلقة بحماية المعطيات ذات الطابع الشخصي،
- شروط الضمان التجاري وخدمة ما بعد البيع،
- طريقة حساب السعر، عندما لا يمكن تحديده مسبقا،
- كيفيات وا ٍجراءات الدفع،
- شروط فسخ العقد عند الاقتضاء،
- وصف كامل لمختلف مراحل تنفيذ المعاملة الالكترونية،
- مدة صلاحية العرض عند الاقتضاء،

[1] راجع المادة 03 من القانون 04-02، المؤرخ في 23 يونيو 2004، المتعلق بتحيدي القواعد المطبقة على الممار سات التجارية، الجريدة الرسمية، عدد 41 المؤرخة في 27 يونيو 2004.

[2] راجع الفقرة الثالثة من المادة 6 من القانون 18-05، المتعلق بالتجارة الالكترونية، المرجع السابق.

- طريقة تأكيد الطلبية،
- موعد التسليم وسعر المنتج موضوع الطلبية المسبقة وكيفيات إلغاء الطلبية، عند الاقتضاء.
- طريقة إرجاع المنتج أو استبداله أو تعويضه.
- تكلفة استخدام وسائل الاتصالات الالكترونية عندما تحتسب على أساس آخر غير التعريفات المعمول بها."

ومن خلال هذه الشروط نلمس حرص المشرع الجزائري على وضع الضمانات اللازمة لصالح المستهلك الالكتروني من حيث الاستفادة من العرض التجاري الالكتروني من جهة، وكذا ضمان الحفاظ على معطياته الشخصية من خلال تضمينها صراحة ضمن بنود العقد.

كما نص المشرع الجزائري ضمن نفس القانون، بخصوص الإشهار الالكتروني، على منع الاستبيان المباشر الذي يعتمد فيه على رسائل عن طريق الاتصالات الالكترونية، باستعمال بيانات شخص طبيعي، بأي شكل كان، إلا في حالة قبول الشخص المعني، تلقي استبيانات مباشرة عن طريق الاتصال الإلكتروني[1].

كما كرس المشرع الجزائري في هذا النوع من العقود ضمانات تسبق مرحلة التعاقد الالكتروني، تجنبا لوقوع المستهلك في خداع نتيجة الدعاية أو الممارسات غير المشروعة، على خلاف ما تم تضمينه بخصوص العقد المدني، حيث اهتم بالمراحل التي تلي التعاقد، لاسيما بالنص على تنفيذ كل طرف في العقد لالتزاماته[2].

ومن الناحية الفقهية فإن العقد الالكتروني طرح في عدة دول إشكالات بمناسبة صدور النصوص القانونية الضابطة للتوقيع الالكتروني، من حيث مدى حجيته مقارنة بالتوقيع العادي بحضور طرفي العقد، حيث تم في فرنسا – تزامنا مع صدور القانون 2000-230، المتعلق بالتوقيع الالكتروني في إطار تطوير قانون الإثبات –، تم تسجيل انقسام

[1] راجع المادة 31 من القانون 18-05، المتعلق بالتجارة الالكترونية، المرجع السابق.

[2] بلحاج العربي، مشكلات المرحلة السابقة على التعاقد في ضوء القانون المدني الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2011، ص12.

بين من ذهب إلى عدم حجية الكتابة والتوقيع الالكترونيين وعليه لابد من الرجوع إلى الشكلية التي يتطلبها العقد أو التصرف العادي، بينما أيد القسم الآخر حجية الكتابة أو التوقيع بأي وسيلة كانت، نظرا لعمومية المادة 1/1316 من القانون المدني الفرنسي[1]، والتي أعطت معنى كاملا دون تخصيص[2].

وفي هذا الجانب، كان المشرع الجزائري قد نحا نفس المنحى، حيث أدرج نفس التعديل، الذي تبناه المشرع الفرنسي، بموجب المادة 323 مكرر من القانون المدني المعدل سنة 2005 بموجب القانون 05-10 [3].

كما تم التأكيد على اعتماد الكتابة الآلية الالكترونية كالكتابة على الورق، مع اشتراط تأكيد هوية الشخص المصدر لها وكذا أن تكون معدة ومحفوظة في ظروف تضمن سلامتها، حسب ما تضمنه نص المادة 323 مكرر من القانون المدني الجزائري[4].

وفي نفس السياق، قد يسهم الاستخدام غير المشروع لوسائل الدفع الالكتروني بشكل بارز في التأثير على خصوصية البيانات الشخصية، والمشرع الجزائري عرف وسائل الدفع بمفهومها الواسع الذي يشمل كل وسائل الدفع، الوارد ضمن نص المادة 69 من

---

[1] نصت هذه المادة 1/1316 من القانون المدني الفرنسي على ما يلي: " ينشأ الإثبات الخطي بالكتابة من تتابع أحرف أو أشكال أو أرقام أو أية إشارة لها دلالة قابلة للإدراك، وذلك أيا كانت دعامتها أو الوسائل المستخدمة في نقلها" والمشرع الجزائري أدرج نفس التعديل بموجب المادة 323 مكرر من القانون المدني المعدل سنة 2005 بموجب القانون 05-10 المؤرخ في 20 يونيو 2005(ج.ر 44، ص24) والتي نصت على " ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"

[2] محمد حسن قاسم، التعاقد عن بعد، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص105-106، وكذلك مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، المرجع السابق، 359.

[3] المادة 323 مكرر من الأمر 75-58، المتضمن القانون المدني المعدل والمتمم، لاسيما سنة 2005 بموجب القانون 05-10 المؤرخ في 20 يونيو 2005(ج.ر 44، ص24) والتي نصت على " ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها".

[4] المادة 323 مكرر1 من الأمر 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم، والتي جاء نصها كما يلي " يعتبر الإثبات بالكتابة غي الشكل الالكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

القانون 03-11، المتعلق بالنقد والقرض والتي تضمنت: " تعتبر وسائل دفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل"[1].

بينما خص وسائل الدفع الالكتروني بتعريف خاص تضمنه نص المادة 06 من القانون 18-05، المتعلق بالتجارة الالكترونية، والتي تضمنت فقرتها السادسة ما يلي:

" **وسيلة الدفع الالكتروني:** كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد، عبر منظومة إلكترونية".

وتم بموجب الأمر 10-04 المعدل والمتمم للأمر 03-11، إدراج المادة 56 مكرر والتي نصت على دور بنك الجزائر في التأكد من سلامة وسائل الدفع حيث نصت على " يتأكد بنك الجزائر من وسائل الدفع، غير العملة الائتمانية، وكذا إعداد المعايير المطبقة في هذا المجال وملاءمتها. ويمكنه رفض إدخال أي وسيلة دفع، لاسيما إذا كانت تقدم ضمانات سلامة غير كافية. كما يمكن أن يطلب من مقدم طلب إدخال الوسيلة اتخاذ كل التدابير لتدارك ذلك. يبلغ بنك الجزائر لممارسة مهامه، من قبل أي شخص معني، بالمعلومات المفيدة التي تخص وسائل الدفع والأجهزة التقنية المتعلقة"[2].

كما تم تخويل مجلس النقد والقرض صلاحية إعداد المعايير وسير وسائل الدفع وسلامتها[3].

وقد عرف بعض الفقهاء الاستخدام غير المشروع لبطاقة الدفع الالكتروني ب" عندما يخل الحامل بشروط عقد إصدار البطاقة بما يؤدي إلى فسخ هذا العقد، أو قفل الحساب الذي تقوم البطاقة بتشغيله، حيث يسأل الحامل جنائيا لمجرد امتناعه عن ردها، أواستمراره

[1] راجع المواد 66، 67، 68 و 69 وما يليها من الأمر 03-11 المؤرخ في 26 غشت 2003، المتعلق بالنقد والقرض، المعدل والمتمم، الجريدة الرسمية عدد 52، المؤرخة في 27 غشت 2003.

[2] راجع المادة 56 مكرر من الأمر 03-11، المتعلق بالنقد والقرض، المعدل والمتمم، المرجع السابق.

[3] انظر المادة 62 من الأمر 03-11، المتعلق بالنقد والقرض، المعدل والمتمم، المرجع السابق.

في استخدامها بعد إلغائها من البنك المصدر لها، أو استمراره في استخدامها بعد انتهاء مدة صلاحيتها"[1].

ومن نماذج الاستخدام غير المشروع لبطاقات الدفع الإلكتروني: حالة تزوير هذه البطاقات أو سرقتها واستغلال ما تحتويه من معطيات، للمساس بالحقوق المعنوية أو المادية للشخص المعني قبل قيام هذا الأخير بالتبليغ الرسمي، أو عن طريق الاستعمال غير المشروع من قبل أحد أطراف العقد في حالة الوفاء، خلال الدفع مثلا للتاجر باستعمال البطاقة مباشرة[2]، أو الاستعمال غير المباشر لهذه البطاقات عبر الإنترنت بما توفره من بيانات يمكن من خلالها الاستحواذ على مبالغ مالية ضخمة، وتحويلها من حساب لآخر في أقل من خمس (05) دقائق.

إلا أنه وبالنظر إلى كل ما كرسته مختلف النصوص القانونية الجزائرية في مجال حماية المعطيات الشخصية في مجال إبرام العقود الالكترونية، لاسيما ما تضمنه كل من القانون 18-05، المتعلق بالتجارة الالكترونية، وكذا القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، فإن المستهلك الالكتروني لم تكرس له ضمانات قانونية واضحة أمام القضاء المدني، في مجال المنازعة الإلكترونية، لاسيما من ناحية صعوبة تحديد الاختصاصين النوعي والإقليمي للمنازعات الإلكترونية[3].

فمن ناحية الاختصاص النوعي لم يخص قانون الإجراءات المدنية والإدارية المنازعة الالكترونية بقسم خاص مما يحتم تطبيق القواعد العامة والرأي الفقهي في هذا المجال الذي يعتمد على طبيعة العمل، فإذا كان مدنيا بالنسبة للمدعى عليه، فعلى المدعي أو

---

[1] أبو الوفا محمد أبو الوفا إبراهيم، المسئولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، ورقة عمل مقدمة في مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون من 9 إلي 11 ربيع أول 1424هـ الموافق 10 إلى 12 ماي 2003م، كلية الشريعة والقانون -جامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، دولة الإمارات، المجلد الخامس، ص2070، نقلا عن: حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني في الجزائر دراسة مقارنة، دار الجامعة الجديدة، مصر، 2016، ص403.

[2] حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني في الجزائر دراسة مقارنة، دار الجامعة الجديدة، مصر، 2016، ص402.

[3] هبة أحمد، بن قادة محمود أمين، الآليات القانونية لحماية المستهلك الإلكتروني وفق القانون 18-05، المتعلق بالتجارة الإلكترونية، مجلة القانون الدولي والتنمية، المجلد8 / العدد1 (2020)، ص205.

المستهلك الالكتروني المتضرر رفع دعوى أمام القضاء المدني، أما إذا كان العمل تجاريا بالنسبة للمدعى عليه فالمدعي يلجأ إلى رفع دعوى أما القسم التجاري[1].

أما من حيث صعوبة تحديد الاختصاص الإقليمي، سواء أكان وطنيا أو دوليا، فإن قانون الإجراءات المدنية والإدارية لم يتضمن ضوابط لتحديد الاختصاص الإقليمي لهذا النوع من المنازعات، وا ٍنما يتم العمل بالقواعد العامة المنصوص عليها في المواد من 37 إلى 40 من نفس القانون المذكور[2].

وعليه ولسد الفراغ في هذا المجال ونظرا لأن العقد الالكتروني يعد نوعا من العقود المستجدة بالنظر لتطور المعلوماتية والوسائل الرقمية المستعملة، وعلاقتها الكبيرة بمجال البيانات الشخصية، لكونها النواة الأساس في تبادل الإيجاب والقبول باعتماد مختلف التطبيقات على غرار البريد الإلكتروني أو مواقع التواصل المختلفة، فإننا نقترح إدراج قسم خاص بالمنازعات ذات الطابع الرقمي، تضم مختلف تفاصيل المعاملات الرقمية وتلك الخاصة بمجالات لها علاقة مباشرة بالبيانات الخاصة، مع تكوين قضاة متخصصين في هذا النوع من المنازعات.

ثانيا: تأثير محركات البحث على خصوصية البيانات الشخصية

بالرغم من هامش الأمان الذي تضمنه مختلف التطبيقات المتداولة عبر شبكة الإنترنت، لاسيما تلك التي تعنى بحفظ البيانات الشخصية لفئات محددة مثل زبائن شركات التسويق الإلكتروني لمختلف السلع والخدمات، إلا أن مجال هذه الحماية يبقى محدودا من ناحية التطبيقات الخاصة بضمان الحماية ومن ناحية المكلفين أو القائمين بجمع ومعالجة مختلف المعطيات عبر مختلف محركات البحث.

وعليه فإن المتصفحات المشهورة عبر الإنترنت تبقى كلها قابلة للاختراق في جانب من الجوانب بالنظر للثغرات الموجودة والمعدة مسبقا أو المكتشفة من خلال محترفي اختراق

[1] عمورة عمار، شرح القانون التجاري (الأعمال التجارية، التاجر، الشركات التجارية)، دار المعرفة، الجزائر، 2010،ص84.

[2] هبة أحمد، بن قادة محمود أمين، الآليات القانونية لحماية المستهلك الإلكتروني وفق القانون 18-05، المتعلق بالتجارة الإلكترونية، المرجع السابق، ص206.

مختلف أنظمة المعلومات (Hackers) الذين بإمكانهم رؤية جميع البيانات المخزنة على جهاز الحاسوب، وكذا امكانية معالجتها بمختلف أشكال المعالجة وصولا إلى حذفها وكذا تدمير برامج الحاسوب بإدخال فيروسات[1]، ومن أمثلة ذلك ما قام به أحد المشاهير وهو البلغاري Georgi Guninski والذي قام باستغلال ثغرة لأحد البرمجيات عبر الإنترنت، من خلال وضع مذكرة على موقعه عبر الإنترنت(www.guninski.com) بتاريخ 21 نوفمبر 2000، مع إشارته إلى وجود ثغرة في المتصفح Explorer محذرا من استغلال ملفات المساعدة المدرجة ضمن تطبيقة Windows التي تنتهي بامتداد (*.chm)، والقيام بتحويل الملفات بامتداد تنفيذي Executable (exe)، من أجل جر الهكرة إلى بحث إمكانية التحريك التلقائي لبرمجيات جهاز إعلام آلي ما، واستغلال بياناته، كما ختم بالإشارة إلى أن هذه من الحالات البالغة الخطورة[2].

ولقد واكبت الكثير من المؤسسات العربية المتخصصة في مجال المعلوماتية في فترة وجيزة، التوجه نحو رقمنة بنوك معلوماتها، بعد إتمامها بناء البنية التحتية لتكنولوجيا المعلومات، حيث نورد منها على سبيل المثال: مكتبة الملك فهد الوطنية[3]، المستودع الرقمي لمكتبة الإسكندرية[4]، المنصة الجزائرية للمجلات العلمية[5] وشبكة إسلام أون لاين...إلخ. إلا أن حماية المحتويات الرقمية يبقى هو الأساس، إذ لابد من ضبط إطار عام من خلال تشخيص دقيق للوصول إلى نتائج وحلول ناجعة لتوفير الحماية اللازمة لمختلف الأنظمة المعالجة والحفاظ على المحتويات الرقمية، لكل مؤسسة معلوماتية، وفي هذا الإطار اقترح بعض الباحثين المهتمين، إطارا متكاملا، يتكون من أربعة مراحل:[6] "

---

[1] وليد سليم النمر، حماية الخصوصية في الإنترنت، دار الفكر الجامعي، الاسكندرية ، ط1، سنة 2017، ص95.

[2] عمر محمد أبو بكر بن يونس، الجرائم عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، المرجع السابق، ص671-672.

[3] (www.kfnl.gov.sa) تقوم المكتبة بنشر مطبوعات من خلال الكتاب الالكتروني للمجلة على شبكة الإنترنت.

[4] (http;//dar.bibalex.org) هي مكتبة رقمية عربية تحوي أكثر من 100 ألف كتاب.

[5] (https://www.asjp.cerist.dz/) وهي منصة تضم مختلف الأبحاث العلمية المحكمة المنشورة عبر المجلات العلمية الوطنية.

[6] متولي النقيب، التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية، جمعية المكتبات والمعلومات السعودية، الأمن المعلوماتي، مكتبة الملك فهد الوطنية، الرياض- المملكة العربية السعودية، 2010، ص363.

1. تحديد طبيعة الاختراقات والمخاطر التي تتعرض لها نظم إدارة المحتوى الرقمي بمشار يع الرقمنة بمؤسسات المعلوماتية العربية، المتنوعة بحسب اختلاف طبيعة نشاطها ونوعها.

2. تقييم إجراءات الرقابة والحماية المطبقة من قبل إدارة المشروع، للتصدي لتلك المخاطر التي تتعرض لها نظم إدارة المحتوى الرقمي بمشاريع الرقمنة العربية.

3. تحديد مدى فعالية إجراءات الرقابة والحماية المطبقة، من إدارة المشروع والمؤسسة المعلوماتية، في التصدي للاختراقات التي تتعرض لها نظم إدارة المحتوى الرقمي بمشاريع الرقمنة العربية، بما فيها الاختراقات غير المرتبطة بالجوانب الفنية للنظام. حيث يتم قياس الفجوة بينإجراءات الرقابة المطبقة وإجراءات الرقابة واجبة التطبيق. على ضوء طبيعة المخاطر التي تتعرض لها نظم إدارة المحتوى الرقمي بمشاريع الرقمنة بمؤسسات المعلومات العربية.

4وضع إستراتيجية لسد الفجوة الرقابية، بين إجراءات الرقابة المطبقة وا إجراءات الرقابة واجبة التطبيق، تختلف باختلاف طبيعة نشاط ونوعية المشروع الرقمي"[1].

وقد كشفت دراسة قامت بها مؤسسة "نت نامز"، المتخصصة في مكافحة القرصنة المعلوماتية، بأن نسبة 24 في المائة من البيانات المتداولة على شبكة الإنترنت معرضة للقرصنة ولجوانب محمية بحقوق الطبع والنسخ، وأرجعت نتائج الدراسة زيادة واتساع مجال القرصنة إلى الاستخدام الواسع لشبكة الإنترنت عالميا، كما أشارت الدراسة إلى أنه بالرغم من محاولة العديد من الحكومات تفعيل آليات حماية الملكية الفكرية، إلا أنها نتائج تظل محتشمة، في حين يتوقع القائمين على الدراسة زيادة رقعة القرصنة مستقبلا[2]، وهو ما ينعكس سلبا على حماية البيانات الشخصية المجمعة والمعالجة عبر مختلف محركات البحث، مما يطرح وبشكل كبير هشاشة أمن المعلومات المتداولة عبر شبكة الإنترنت.

[1] متولي النقيب، التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية، المرجع السابق، ص365.

[2] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، المرجع السابق، ص341.

الفرع الثاني: سرقة البيانات الشخصية

تعد سرقة البيانات الشخصية من أعظم الأخطار التي تهدد خصوصية البيانات الشخصية، حيث يتم التفنن فيها باعتماد مختلف الوسائل والآليات، وتختلف أساليب سرقة البيانات الشخصية حسب البيئة والوسائل المستخدمة، لاسيما بتأثير التكنولوجيات الحديثة أو سوء استغلال الوسائل التكنولوجية المستعملة في المعالجة الرقمية للبيانات.

وعليه فإن مفهوم سرقة البيانات يختلف عن المفهوم العام للسرقة المتعلقة بالأموال، لكون المحل المادي الذي يقع عليه الاختلاس هو مال معلوماتي، يتكون من جملة من المعطيات مخزنة بالحاسوب أو أي وسيلة أخرى رقمية (Data) تخص شخص بمفرده أو مجموعة أشخاص، حيث تجدر الإشارة إلى الجدل الواقع حول اعتبار المال المعلوماتي حائزا على الطبيعة المادية في القانون، حيث أن القضاء المقارن كان يرفض اعتبار المال المعلوماتي داخلا في عناصر فكرة الملكية، مما يصعب اعتباره وتصنيف هذا النوع من الاختلاس ضمن جريمة السرقة بالخصوص، والعدوان على الملكية على العموم، إلا أنه وتبعا للتطورات الحاصلة في الواقع بتأثير مختلف الوسائل الرقمية الحديثة أدت إلى تطور المفهوم ليصبح محل الاختلاس المتمثل في المال المعلوماتي ليشمل كذلك مجال العالم الافتراضي أيضا[1].

وجريمة سرقة البيانات الشخصية تختلف كذلك عن غيرها من جرائم السرقة من حيث صعوبة ضبط البيانات المسروقة على أن حيازتها من جانب واحد أو أن السارق قام بأخذ نسخة فقط ولم يقم بحذف البيانات المعالجة الأصلية، وهو ما يشمل الحيازة عن طريق النسخ، وهو الأمر الذي ذهب إليه القضاء الانجليزي، وعملت به العديد من المحاكم، إلا أنه وبعد ممارسة لفترة وجيزة تم إلغاؤه بسبب عدم الشرعية ، من حيث عدم الاستناد على نص واضح يؤكد هذا التوسع في المفهوم[2].

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية- رسالة دكتوراه في القانون الجنائي-، جامعة عين شمس، مصر، سنة 2004، ص 400.

[2] السعيد كامل، جرائم الكومبيوتر والجرائم الأخرى في مجال التكنولوجيا- المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 أكتوبر 1993، دار النهضة العربية، ص 351.

أما بالنسبة للمشرع الجزائري، فإنه أورد تعريفا شاملا للجرائم الالكترونية ولم يستثني جريمة سرقة المعطيات، وفق نص المادة 02 من القانون 04-09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بأنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[1]. كما أنه باستقراء مواد قانون العقوبات الجزائري، لاسيما من المادة 394 مكرر إلى 394 مكرر7 نستنتج أن مختلف الأفعال المجرمة تقتضي بالضرورة الاطلاع على مضمون البيانات المتبادلة للقيام بأفعال غير مشروعة، لاسيما عند استغلال أرقام سرية للغير والتصرف في حسابات أو تغيير وفك شفرة بطاقات ائتمان[2].

إلا أنه بتأثير التكنولوجيات الحديثة وبروز أصناف متعددة لسرقة البيانات بطرق جد معقدة، بالاعتماد على بث فيروسات تقوم بتحويل البيانات إلى صاحب الحاسوب الذي قام بنشر الفيروس، لاسيما بالاعتماد على شبكة اتصالات مشتركة بين الحواسيب. وكذلك مايقوم به الهكر ة من اختراق للحواسيب والاستيلاء أو تشويه المعطيات الموجودة فيها، فقد قام واحد من الهكرة الروس بارتكاب خمسمائة محاولة سرقة من مصرف روسيا المركزي خلال الفترة الممتدة من سنة 1994 إلى سنة 1996، بتحويل مبلغ مائتين وخمسين مليون روبل إلى حساباتهم الشخصية[3].

وفي سياق متصل تم إعداد دراسة سنة 2004 حول أكثر من 500 شركة بخصوص الأخطار والتهديدات الالكترونية التي تعرضت لها، حيث أفضت نتائج هذه الدراسة إلى تعرض كل شركة لحالة هجوم واحدة على الأقل وتعرض البعض منها إلى أكثر من 43

[1] القانون 09-04، المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخة في 16 أوت 2009.

[2] حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني في الجزائر دراسة مقارنة، دار الجامعة الجديدة، مصر، 2016، ص675.

[3] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، المرجع السابق، ص409.

حالة هجوم، في عام واحد فقط، هذا بالرغم من اعتماد هذه الشركات على تقنيات جد متطورة في مجال أنظمة الحماية[1].

كما أودعت شركة مالية بالولايات المتحدة الأمريكية شكوى جراء تعرضها لعملية قرصنة معلوماتية مست قواعد البيانات الخاصة بها أثرت سلبا على وضعية عملائها، حيث تم خلال هذه العملية سرقة ما يربو عن 40 مليون بطاقة بنكية وتأشيرة لعملاء المؤسسة[2].

كما أن سرقة الأجهزة التي تخزن البيانات يعد من أخطر المظاهر التي تهدد البيانات الشخصية، حيث تم سنة 2005 سرقة جهاز حاسوب محمول من إحدى الجامعات الأمريكية **(University of Berkeley)**، كان يحتوي على بيانات شخصية تشمل مائة ألف طالب حائز على شهادة الدكتوراه منذ سنة 1976 [3].

ويوجد صنف من المعطيات الشخصية أكدت الدراسات أنها من أكثر البيانات عرضة للسرقة، لاسيما السرقات العلمية، من مختلف جوانبها سواء من قبل منتسبين للعلم أو من قبل دور النشر، مؤسسات الإعلام وغيرها.. الأمر الذي بالرغم من مساسه بمجهود الآخرين والأمانة العلمية فإنه كذلك يشكل موضوعا جد خطير على الأمن الفكري،

---

[1] خضر مصباح الطيطي، المرجع السابق، 299.

[2] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص405؛

"Joris Evers, plus de 40 millions de numéros de cartes mastercard et visa piratés. Art disponible sur https://www.zdnet.fr/actualites ; la date de mise en ligne le 20 juin 2005.

[3] Yves Grandontagne, USA : l'identité de 100.000 universitaires dans la nature, Article disponible sur https://www.silicon.fr/usa-lidentite-de-100000-universitaires-dans-la-nature, la date de mise en ligne est le 11 Avril 2005.

نقلا عن سامح عبد الواحد التهامي، المرجع السابق، ص406.

الاقتصادي والاجتماعي، لاسيما في ظل الاستعمال الواسع للتكنولوجيات الرقمية في مختلف المجالات العلمية وتشجيع النشر الالكتروني[1].

وقد تم سنة 2007 ضياع قرصي تخزين بيانات رقمية تخص إدارة الضرائب البريطانية، حيث قدم رئيس وزراء بريطانيا آنذاك "جوردن براون" اعتذاراً رسميا أمام البرلمان عن فقد إدارة الضرائب البريطانية لبيانات شخصية لحوالي نصف سكان بريطانيا، مما ولد خوفا من التعرض لخطر القرصنة والاحتيال، حيث قال بهذا الخصوص للبرلمان" أنا آسف بشدة وأعتذر عن أي إزعاج ومخاوف تم التسبب فيها لملايين الأسر"، وقد علق الزعيم المحافظ ديفيد كاميرون على الحادثة بقوله " سيخاف ملايين الناس اليوم بشأن سلامة حساباتهم المصرفية وأمن بيانات أسرهم، وسيغضبون، لأن الحكومة قد أخفقت في واجبها في حماية الجمهور" [2].

كما يشكل أمن البيانات الحلقة الأساس في الرفع من مستوى التعاملات في البيانات الكترونيا، لاسيما في المجال الاقتصادي، وعليه فإن عملية السرقة والتعدي على حقوق الملكية الفكرية، أو كشف بيانات سرية من شأنه عرقلة مختلف الأنشطة، لاسيما التجارية منها[3].

---

[1] سالم بن محمد السالم، السرقات العلمية في البيئة الالكترونية دراسة للتحديات والتشريعات المعنية بحماية حقوق المؤلف، جمعية المكتبات والمعلومات السعودية، الأمن المعلوماتي، مكتبة الملك فهد الوطنية، الرياض- المملكة العربية السعودية، 2010، ص12.

[2] "I profoundly regret and apologies for the inconvenience and worries that have been caused to millions of families…," Brown told parliament when questioned about the data loss.

"When mistakes happen in imposing procedures we have a duty to do everything that we can to protect the public," he said, promising a review of personal data security.

Adrian Croft, Britain's Brown apologies over lost data, at Reuters, on line at https://www.reuters.com/article/britain-data-idUSL2119814420071121, 21 November 2007.

[3] خضر مصباح الطيطي، المرجع السابق، ص285

وتعتمد العديد من التشريعات على متابعة وضبط مختلف السرقات للبيانات الشخصية، لاسيما عند استعمال التجهيزات المتطورة مثل الحواسيب الآلية على رقم التعريف، الخاص بكل جهاز لاسيما عند اتصاله بإحدى شبكات المعلومات.

المبحث الثاني: آثار التطور التكنولوجي على خصوصية البيانات الشخصية

بالرغم من الأثر الايجابي لاستعمال الأجهزة المعلوماتية الحديثة في مجال معالجة مختلف البيانات الشخصية، إلا أن الاستعمال المفرط لهذه الوسائل دون مراعاة ضوابط الحماية وتشفير مختلف الملفات المتضمنة لبيانات شخصية يقتضي تجسيد الآليات اللازمة للحفاظ على مختلف البيانات الشخصية من مختلف مصادر التهديد لاسيما تلك الناجمة عن استعمال الإنترنت وهو ما سيتم التفصيل فيه في المطلبين المواليين.

المطلب الأول:مخاطر الإنترنت والحواسب الآلية على خصوصية البيانات الشخصية

تشكل الإنترنتفضاء ً خصباً لتداول مختلف البيانات الشخصية، لاسيما تلك المتداولة عبر مختلف المواقع الالكترونية ومواقع التوصل الاجتماعي على وجه الخصوص.وعليه فإن مخاطر استعمال التقنيات الحديثة قد يسهم في خلق العديد من المخاوف والتي بدورها تؤثر على استمرار مختلف الأنظمة التكنولوجية الرقمية، التي أسهمت بشكل كبير في اقتصار المسافات والوقت والجهد. حيث نميز في مجال التعاملات المالية - على سبيل الذكر - اعتمادها على التكنولوجيات الرقمية، لاسيما شبكة الإنترنت، مما يستوجب احترام خصوصية الزبائن وتأمين بياناتهم الشخصية من كل التهديدات، للإسهام بصفة كبيرة في التجارة الالكترونية وفي حالة عدم توفير الحماية فسيتم الانتقال لا محالة من عالم الدفع النقدي المستتر إلى عالم الدفع المكشوف من خلال تتبع الأشخاص ومعرفة أذواقهم ومشترياتهم[1]، مما يقتضي سن تشريعات كفيلة بالحماية من مختلف مخاطر الاختراق أو على الأقل التقليل من حدتها.

ومن هذا المنطلق سنتطرق إلى أهم مصادر مخاطر الإنترنت على البيانات الشخصية، وكذا تأثير استعمال الحواسب الآلية لبنوك المعلومات من خلال الفرعين المواليين.

[1] حوالف عبد الصمد، النظام لقانوني لوسائل الدفع الإلكتروني في الجزائر دراسة مقارنة، المرجع السابق، ص434.

الفرع الأول: مظاهر تفاقم مخاطر الإنترنت على البيانات الشخصية

بالرغم من المزايا العديدة لاستخدام شبكةالإنترنت في التواصل باستعمال البيانات الشخصية وغيرها، إلا أن إساءة استخدام هذه التقنية ولد الكثير من المخاطر على البيانات الشخصية على جميع المستويات، حيث أبرزت نتائج إحدى الدراسات التي أجريت بالولايات المتحدة الأمريكية سنة 2016، عن تعرض 47%، من مستخدمي الإنترنت لنوع من التحرش الجنسي، وأن 05%، منهم، تسربت بياناتهم الحساسة وألحقت بهم الأذى. هذا بالإضافة إلى تأكد أن غالبية مستخدمي الإنترنت يجهلون حقوقهم في الدفاع عن المعالجة غير المشروعة لبياناتهم باستخدام الإنترنت[1].

ومن أبرز مخاطر استخدام الإنترنت على البيانات الشخصية:

- عدم إمكانية استرجاع البيانات المستولى عليها، أو سحبها أو إلغائها، بالنظر لمختلف الأبعاد الاجتماعية والسياسية جراء الانتشار الواسع لهذه التقنيات، لاسيما عبر مواقع التواصل الاجتماعي وما لها من انعكاسات على خصوصية مختلف الأفراد المشتركين بالدرجة الأولى، لاسيما من خلال قيام بعض المشرفين على مواقع تخزين البيانات الشخصية على استغلالها لأهداف تسويقية. وعلى سبيل المثال، ما تقوم به شركة فيسبوك، بعد جمع معطيات شخصية لمستخدميها والتي سمحت بالتعرف على أدق التفاصيل المتعلقة بحياتهم وأذواقهم وميولاتهم، فهي تقوم ببيع حق الوصول إليها من قبل شركات الإعلانات لتسويق منتجاتها، باستغلال المعطيات الشخصية لمستخدمي الفايسبوك بطريقة غير مباشرة [2].
- تسهل شبكة الإنترنت من تبادل الأفكار السلبية والخبرات الإجرامية وهو ما تعكسه مظاهر القرصنة للمواقع الالكترونية ومختلف الحسابات المشتملة على أدق تفاصيل البيانات الشخصية للأفراد، حيث تعد الجرائم الماسة بالمعطيات الشخصية عبر

[1] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية – الهم الأمني وحقوق الأفراد، المرجع السابق، ص30.

[2] منى الأشقر جبور، محمود جبور،البيانات الشخصية والقوانين العربية – الهم الأمني وحقوق الأفراد، المرجع السابق، ص33.

الإنترنت أسرع تطورا من التشريعات نظرا لأثر الملتقيات وتبادل الأفكار بين قراصنة الإنترنت[1].

- عزوف الكثير من المتضررين من المعالجة غير المشروعة لبياناتهم عبر الإنترنت، عن التبليغ بذلك خوفا من التشهير، لكون الأمر يخص بيانات تهم خصوصيتهم، وهو ما يؤكد بأن حجم التعدي على البيانات الخاصة أكبر بكثير من الأرقام المصرح بها بعد إحصاء الجرائم المكتشفة، هذا بالإضافة إلى صعوبة الوصول إلى الجاني بسبب استعمال حسابات وهمية وكذا الطابع العالمي للجريمة المعلوماتية عبر الإنترنت[2].
- عدم ترك الجاني أثرا لما اقترفه من مساس بالبيانات الشخصية المتداولة عبر شبكة الإنترنت، نظرا لكون العملية تتم عبر استعمال رموز على وسائل تخزين ممغنطة، لا تفك شفرتها إلا باستعمال حاسوب مبرمج ومن قبل متخصص في المجال، مما يصعب ويؤخر المحقق في الحصول على الدليل مقارنة بمختلف الوسائل التكنولوجية الرقمية التي يلجأ إليها مرتكبو الجرائم الماسة بالبيانات الشخصية، في هذا الجانب، موازاة مع وجود كم هائل من هذه البيانات المخزنة[3].
- انتقال البيانات الشخصية خارج نطاق الدولة مما يعقد عملية متابعة الجرائم الناتجة عن سوء استخدام هذه البيانات من جهة، كما قد يسهم في المساس بالأمن القومي من جهة أخرى، في حالة عدم تكريس الدولة محل المعالجة للبيانات ضمانات قانونية إجرائية مناسبة وفعالة لتسهيل التدخل والكشف عن الأشخاص المتسببين في الاستغلال غير المشروع للبيانات الشخصية، واتخاذ الإجراءات المناسبة ضدهم من جهة وفرض المعالجة الشرعية للبيانات في إطار مراعاة مبدأ الحفاظ على الخصوصية.

---

[1] عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، جامعة محمد خيضر – بسكرة، العدد الثاني، 2014، ص74.

[2] نهلا عبد القادر المومني،الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، سنة 2008، ص51.

[3] عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقارن، المرجع السابق، ص75.

وفي هذا الإطار استثنت العديد من التشريعات، من إجراءات المعالجة الدقيقة فئة البيانات الشخصية المتعلقة بالجنايات، التي تجمعها السلطات الأمنية المختصة في الدولة أو السلطات القضائية في إطار مكافحة الجريمة ورصدها والوقاية منها وكذا في إطار مسائل الدفاع الوطني، لاسيما بعد أحداث الحادي عشر من سبتمبر 2001، والتي أقرت بعدها الولايات المتحدة الأمريكية صلاحيات واسعة للحكومةوالأجهز ة الأمنية حرية أكبر لجمع البيانات الشخصية بإنشاء السجلات الحكومية في إطار تحدي مواجهة الإرهاب[1].

إلا أنه بالرغم من المخاطر التي تتعرض لها البيانات الشخصية على اثر استعمال الإنترنت، إلا أن هناك الكثير من بحث عن حلول للتقليل من هذه المخاطر عن طريق المطالبة بحق الشخص في محو بياناته بعد إتمام المعالجة أو ما يصطلح عليه بالحق في الدخول في طي النسيان الرقمي، والذي يجسد حق الفرد في عدم احتفاظ المسؤول عن المعالجة بمعطياته الشخصية لمدة تتجاوز الغاية التي جمعت من أجلها[2]. كما عرف بعض الفقهاء الحق في النسيان بأنه " حق يمكن من إزالة العناصر المتعلقة بماضي الشخص، سواء كانت دقيقة أو غير دقيقة أو عفا عليها الزمن، من المحتوى عبر الإنترنت أو جعل الوصول إليها صعبً ا " [3].

ويبقى مجال تطبيق الحق في النسيان الرقمي منحصرا في الآثار والذكريات الرقمية، التي تشمل كل البيانات الخاصة بنشاط الشخص جراء استخدامه لوسائل وأنظمة

---

[1] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية –الهم الأمني وحقوق الأفراد، المرجع السابق، ص38.

[2] راجع المادة 06 من القانون الفرنسي 78-17، المرجع السابق.

[3]" Le droit à l'oubli est évoqué principalement, s'agissant d'Internet, comme un droit à ce que les éléments relatifs au passé d'une personne, qu'ils soient exacts, inexacts ou devenus obsolètes puissent être retirés des contenus en ligne, ou rendus difficilement accessible."

Voir ; Jean-Christophe, Duton et Virginie Becht, Le droit à l'oubli numérique : un vide juridique ?, disponible sur https://www.journaldunet.com/ebusiness/le-net/1031442-le-droit-a-l-oubli-numerique-un-vide-juridique/ , le 23/01/2021.

إلكترونية على غرار مواقع التوصل الاجتماعي، مواقع التجارة الالكترونية، محركات البحث وغيرها من التقنيات المتاحة عبر الإنترنت[1].

هذا وبالرغم من الاتفاق الفقهي حول إدراج الحق في النسيان الرقمي ضمن الحقوق الملازمة للشخصية، إلا أنهم انقسموا، في جانب اعتباره من بين عناصر الحق في الحياة الخاصة، إلى قسمين:

الفريق الأول يرى أنه حق مستقل وليس عنصرا من عناصر الحق في الحياة الخاصة لسببين، أولهما أن البيانات التي دخلت طي النسيان لا يعد نشرها دون موافقة الشخص المعني اعتداء على الحياة الخاصة وا ٍنما انتهاك لحقه في النسيان، نظرا للتقادم بمرور مدة زمنية، ولا يتم ذلك إلا بصدور الإذن من الشخص الذي حدثت له الوقائع بصفة مباشرة[2]، والسبب الثاني اتساع نطاق تطبيق الحق في النسيان مقارنة بنطاق تطبيق الحق في الحياة الخاصة[3].

أما الفريق الثاني فيرى النظرة العكسية وهو اعتباره من بين عناصر الحق في حرمة الحياة الخاصة، مبررين ذلك بأن حرمة الحياة الخاصة تشمل ما عاشه الإنسان في حاضره وماضيه، مع حقه في إحاطة كل ذلك بالسرية والكتمان، ويجرم قانونا كل انتهاك أو اعتداء عن هذه الأسرار المتعلقة بحرمة الحياة الخاصة[4].

ولقد أيد القضاء في الدول الأوروبية الاتجاه الثاني الذي يعتبر الدخول في طي النسيان من بين عناصر الحق في الحياة الخاصة، ومثال ذلك ما أقرته محكمة بروكسل الجزائية في 1997/06/30 وحكم محكمة باريس الابتدائية في 2012/02/15 [5].

---

[1] بوخلوط الزين، الحق في النسيان الرقمي، مجلة المفكر، العدد الرابع عشر، 2016، جامعة محمد خيضر - بسكرة، ص552.

[2] محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، الطبعة الأولى، القاهرة، سنة 2005، ص215

[3] بوخلوط الزين، الحق في النسيان الرقمي، المرجع السابق، ص556.

[4] محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، المرجع السابق، ص217.

[5] عبد الهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الإنترنت، دار النهضة، الطبعة الأولى، القاهرة، سنة 2014، ص74-75.

كما اعترفت المحكمة الأوروبية بالحق في النسيان الرقمي من خلال مضمون الحكم المؤرخ في 13 ماي 2014،على اثر الفصل في قضية كوستيغا ماريو ضد محرك البحث غوغل اسبانيا، أين قضت بحق إزالة نتائج البحث المتعلقة بالبيانات الشخصية بعد ثبوت قدمها أو عدم دقتها، ولو كان المحتوى صحيح، بشرط طلب الشخص المعني نسيان بياناته[1].

تجدر الإشارة إلى أن المشرع الجزائري لم يتطرق صراحة إلى الحق في النسيان الرقمي، وا ٍنما بصورة غير مباشرة أكد على حرمة الحياة الخاصة، وحماية المعطيات الشخصية دستوريا وقانونيا من خلال ما تضمنه كل من القانون المدني ضمن نص المادة 47[2]، قانون العقوبات، القانون المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين[3] والقانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة معطياتهم ذات الطابع الشخصي، لاسيما المادتين 42 و 43 منه[4].

وعليه بالنظر لحجم المخاطر التي قد يلحقها الاستعمال غير الشرعي للبيانات الشخصية عبر شبكة الإنترنت فإنه بات من الضروري على المشرع سن نص خاص يضمن الحق في النسيان الرقمي وا ٍنشاء آلية فعلية لتجسيده حفاظا على المعطيات الشخصية المعالجة من أي استغلال يمس بالحياة الخاصة للأفراد.

الفرع الثاني: أثر استخدام الحواسب الآلية لبنوك المعلومات

يعتمد العديد من الأشخاص على حفظ بياناتهم الشخصية عبر تطبيقات وبرامج آلية تتطور بتطور استعمال الحواسب الآلية، في مختلف المجالات الإدارية، التجارية، الصناعية والخدماتية، والتي تجسد فيها البيانات الشخصية الحلقة البارزة في المعالجة.

---

[1] بوزيدي أحمد تجاني، الحق في الدخول في طي النسيان الرقمي كآلية لحماية الحق في الحياة الخاصة، مجلة صوت القانون، المجلد السادس، العدد02/ نوفمبر 2009، ص1254.

[2] راجع المادة 47 من الأمر 75-58، المتضمن القانون المدني، المعدل والمتمم، المرجع السابق.

[3] راجع المادتين 42 و43 من القانون 15-04، المؤرخ في أول فبراير 2005، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية عدد 06، المؤرخة في 10 فبراير 2005.

[4] بوزيدي أحمد تجاني، الحق في الدخول في طي النسيان الرقمي كآلية لحماية الحق في الحياة الخاصة، المرجع السابق، ص1253.

وبالرغم من أن جرائم الحاسوب تعرض لها الفقه الجنائي منذ سنة 1960، إلا أن اختلاف وجهات النظر بين الفقهاء يبقى جلياً من حيث تصنيف هذه الجرائم وما يترتب عنها، حيث أشار الأستاذ Donn Packer إلى التعريف الخاص بالجرائم التي تخص أنظمة الحاسوب بأنها "فعل غير مشروع يتورط نظام الحاسوب فيه، سواء كان الحاسوب كآلة هو موضوع الجريمة أو كان الوسيلة إلى ارتكابها أو مستودع الدليل المرتبط بالجريمة"[1].

وما نلاحظه من خلال هذا التعريف هوالمجال الواسع الذي منحه الفقه لجرائم الحاسوب، لاسيما وأن التمييز والخلاف الفقهي موجود في هذا المجال. حيث أن كل مدرسة تتبنى تصنيفا معينا من حيث توسيع وحصر مجال الجرائم المرتبطة باستعمال الحاسوب، بالخصوص تلك التي تشمل معالجة البيانات الشخصية من جهة وتلك المرتبطة باستعمال الإنترنت من جهة أخرى.

وبدوره مكتب المحاسبة بالولايات المتحدة الأمريكية عرفها بصيغ مختلفة بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه" وكذلك " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[2].

كما عرفتها منظمة التعاون الاقتصادي والتنمية، بمناسبة استبيان الغش المعلوماتي سنة 1982، بأنها" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[3].

---

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية- المرجعالسابق، ص 62.

[2] هدى قشوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، الطبعة الأولى، القاهرة، 1992، ص20. نقلا عن دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع،جمعية المكتبات والمعلومات السعودية، مكتبة الملك فهد الوطنية، الرياض، سنة 1431هـ/2010م، ص536.

[3] خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي للنشر والتوزيع، عمان- الأردن، ط1، سنة 2018، ص25.

وذكر الأستاذ **تاديمان** بأنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"[1].

وقد ظهر لنا من خلال استقراء مضامين التعاريف المذكورة، بأنه يمكن تمييز نوعين أساسيين من هذه الجرائم على ارتباط بمجال المعطيات الشخصية والتي قد تسهم بصورة كبيرة في تهديد خصوصية هذه الأخيرة، كما يلي:

أولا: الجرائم المتعلقة بأنظمة الحاسوب

يشمل هذا النوع من الجرائم كل التأثيرات المحتملة على معطيات الحاسوب وأنظمة التشغيل المعتمدة لضبط، معالجة وتخزين لمختلف البيانات، كنسخ وتقليد البرامج أو تقليد العلامة التجارية وبراءة الاختراع. وهي تشكل صورة من صورة المعطيات الشخصية،لكونها تدخل ضمن حقوق الملكية الفكر ية الخاصة بالشخص مالك أو حائز للبرامج موضوع الجريمة الماسة بمحتوى هذه البرامج، أو الاستغلال غير المشروع لها في حد ذاتها[2].

و عليه فإن هذا النوع من الجرائم يجسد الاعتداء على المكونات المادية للنظام المعلوماتي في الأساس، مما ينعكس على المعطيات الشخصية بصورة غير مباشرة بواسطة إتلاف الأجهزة والمعدات بمختلف الطرق والأشكال الشائعة في هذا المجال والتي من بينها: "الضرب بآلات حادة لإتلاف المكونات" أو "إشعال الحرائق بأماكن وجود المعدات"، أو "استخدام قنبلة غاز" أو" العبث بمفاتيح التشغيل"، أو تغيير وتعديل المحتوى أو إضافة بيانات غير صحيحة مباشرة أو ببرمجة آلية[3].

[1] منير الجنبيهي، جرائم الإنترنت والحاسب الآلي وطرق مكافحتها، الطبعة الأولى، دار الفكر الجامعي، القاهرة، ص56.

[2] خالد داودي، الجريمة المعلوماتية، مرجع سابق، ص44.

[3] دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع،مرجع سابق، ص537.

ومن أمثلة ذلك ما خلفه تنظيم " الألوية الحمراء" في ايطاليا، حيث عمدت مجموعة من أصحاب التخصص هناك في مجال التكنلوجيات الرقمية إلى تدمير مركز المعالجة الآلية لإحدى الشركات بالديناميت مما تسبب في خسائر قدرت قيمتها بأربعة ملايين دولار[1].

كما تم تسجيل ارتفاع مضاعف للخسائر في الأموال نتيجة الجريمة المعلوماتية مقارنة بغيرها من الجرائم، حيث أورد مكتب التحقيقات الفيديرالية في الولايات المتحدة الأمريكية (F.B.I) إلى أن متوسط الخسائر الناجمة عن الجريمة المعلوماتية وصل إلى نحو 500.000دولار، في مقابل مخلفات جرائم السرقة العادية والتي لم تتجاوز مبلغ 3.500 دولار[2].

وقد تأخذ هذه الجرائم شكلا آخر من خلال التلاعب بأنظمة المعلومات داخل الحاسوب التي تتبني عليه مختلف البيانات سواء باستعمال شبكة الإنترنت أو الشبكات الداخلية للمؤسسات باعتماد أنظمة الحاسوب، بحيث يقوم المعالج بتعديل نظام الحاسوب لتحقيق أهداف في الغالب تكون ذات طابع مادي بحت.

ومثال ذلك ما قام به أحد المختصين في مجال البرمجيات، والموظف لدى أحد البنوك الأمريكية، خلال تثبيته لبرنامج إدارة حسابات البنك بإضافة تلقائية لمبلغ 10 سنتات لتكاليف تسيير الحسابات الداخلية إضافة إلى مبلغ عشر دولارات المحددة من قبل مسيري البنك، مع إضافة دولار واحد على كل حساب يزيد عن عشرة دولارات، وبالطبع هذه الزيادة لم يكن الغرض منها تحقيق أرباح لفائدة البنك الذي يشتغل به،وا ٍنما قام بقيد المداخيل الزائدة في حساب خاص وضع له اسما مستعارا "Zzwick"، مكنه من جمع مبالغ كبيرة كل شهر، إلا أنه عن طريق الصدفة أراد البنك في إطار سياسته الدعائية للتسويق بمناسبة تأسيس الشركة أن يقدم مكافئة لأول وآخر عميل له وفقا للترتيب الأبجدي وحينها تم اكتشاف عدم وجود عميل يحمل اسم "Zzwick" [3].

---

[1] أحمد خليفة الملط، الجرائم المعلوماتية، رسالة دكتوراه في الحقوق، جامعة القاهرة، 2005، ص202.

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية- دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية، 2005، ص50.

[3] أحمد خليفة الملط، الجرائم المعلوماتية، المرجع السابق، ص205.

ونذكر من الأضرار المادية لجرائم الحاسوب في الدول الأوروبية، ما تضمنه تقرير المجموعة الاقتصادية الأوروبية من وصول خسائر الجرائم المعلوماتية إلى مبلغ 64,50 مليون أورو، بمعدل 963.000أورو لكل جريمة، هذا بالإضافة إلى تسجيل 15 حالة اختلاس تفوق 150.000 أورو لكل حالة، من بينهما حالتان متميزتان تكبد فيهما مصرفان كبيران خسائر فاقت عشرة (10) ملايين أورو لكل مصرف[1].

ثانيا: الجرائم المترتبة باستعمال الحاسوب

يتميز هذا النوع الجرائم باعتماده على الآثار التي تتسبب فيها وسيلة معالجة المعطيات، كبرمجة تطبيقات تستهدف سرقة الأموال آليا، أو التخزين غير المرخص للبيانات وغيرها من النتائج السلبية على مآل المعطيات، معنويا وماديا.

ومن المفترض أن الغاية من استعمال الحواسيب هو تسهيل معالجة المعطيات ومختلف بنوك المعلومات قصد تسهيل الوصول إليها عند الحاجة، وكذا ضمان تصنيف وترتيب أحسن لها، وهو الأمر الذي تعتمده كذلك العديد من المؤسسات والشركات الكبرى سواء الخاصة أو العمومية. إلا أن عدم تقيد المعالج بالتدابير والشروط المدرجة مسبقا في هذا الجانب من معالجة المعطيات الشخصية لاسيما عندما يكون جهاز الحاسوب مربوطا بشبكة الإنترنت فإن ذلك مما يسهل الوصول إليها دون إذن مسبق أو إساءة استخدامها[2].

ولكن الوصول إلى هذه المعطيات يشكل بحد ذاته خطورة أكبر لاسيما القيام بمحو المعطيات أو إتلافها مما يصعب تتبع مختلف العمليات المتعلقة بها، لاسيما في جانبها المادي بالنسبة للمؤسسات. ومن أمثلة ذلك قيام شخص بعملية اختلاس مبلغ 61000 دولار من أحد المراكز الجامعية وهي تشكل مبالغ مرسلة من شركات التأمين، حيث قام المحللون بمحو كل الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز الجامعي وجعلها غير قابلة للتحصيل[3].وفي هذا النوع يمكن تصنيف نوع آخر من الجرائم

[1] دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع،مرجع سابق، ص542.

[2] حوالف عبد الصمد، النظام القانوني لوسائل الدفع الالكتروني في الجزائر- دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2016، ص436.

[3] دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم الالكترونية وحماية المجتمع، مرجع سابق،ص539

يسمى جرائم التخزين وجرائم المحتوى، حيث عرف الأستاذ **خالد داودي** كل صنف من هذين الجريمتين على النحو التالي[1]:

- **جرائم التخزين**: تعني "تخزين المادة الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها".

- **جرائم المحتوى**: "يعبر عنها بالمحتوى غير المشروع أو غير القانوني، بحيث أصبح يرمز إلى المحتوى غير القانوني بجرائم المقامرة ونشر المواد الإباحية والغسيل الالكتروني للأموال وغيرها.."

ولقد ذهبت العديد من التشريعات إلى اعتبار كذالك ملحقات الحاسوب ومختلف برمجياته من أدوات الجريمة إذا ما اتصلت بعملية تزوير مهما كان نوعها[2].

وعلى مستوى التشريعات العربية فقد تم الاهتمام بإيجاد حلول لهذا النوع من الجرائم الماسة بأمن الأشخاص والممتلكات باستعمال التكنولوجيات الحديثة، ويمكن إيراد أمثلة للجهود المبذولة في هذا المجال من قبل دول الجزائر، مصر والسعودية على النحو التالي:

1. الجرائم المترتبة باستعمال الحاسوب في الجزائر:

أقر المشرع الجزائري من خلال تعديل وتتميم قانون العقوبات لسنة 2004 بموجب القانون 04-15 استحداث مواد خاصة بجرائم المساس بالأنظمة المعلوماتية، حسبما تضمنته المواد 394 مكرر إلى المادة 394 مكرر7 من القسم السابع مكرر، المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات. وهنا تجدر الإشارة إلى مضمون نص المادة 394 مكرر والتي نصت على عقوبة الحبس من شهرين إلى ثلاث سنوات ودفع غرامة مالية تتراوح بين 1.000.000دج و5.000.000دج، على كل من يقوم عمدا وعن طريق الغش بما يلي:

[1] خالد داودي، الجريمة المعلوماتية، المرجع السابق، ص46-47.

[2] عمر محمد بن يونس، المرجع السابق، ص63.

أ- "تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ب- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم "[1].

وتجدر الإشارة أن المواد الموالية أشارت إلى مضاعفة هذه العقوبات في مجالات محددة،و هو ما يعكس حرص المشرع الجزائري على حماية المعطيات من خطر الجرائم المعلوماتية، ولا أدل على ذلك من النص القانوني الخاص الذي فصل مختلف إجراءات المعالجة الآلية للمعطيات ذات الطابع الشخصي وا ٍقرار ضوابط إجرائية، مؤسساتية، إدارية وعقابية في حالة المساس بهذه المعطيات، وهو ما تضمنه نص القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي[2].

2. الجرائم المترتبة باستعمال الحاسوب في مصر:

لم يتضمن قانون العقوبات المصري مواد تخص الجرائم المعلوماتية، باستثناء ما تضمنه قانون الأحوال المدنية رقم 124 لسنة 1994 في جانب النظام المعلوماتي والجرائم المتصلة به، لاسيما نص المواد72،74،75 و76 منه[3].

وقد نصت المادة 72 على عقوبات مشددة تصل إلى السجن لمدة خمسة سنوات في حالة تزوير المحررات الرسمية الآلية[4].

---

[1] راجع المواد 394 مكرر، 394 مكرر1، 394 مكرر2، 394 مكرر3، 394 مكرر4، 394 مكرر5، 394 مكرر 6، 394 مكرر7، من الأمر 66-156 المؤرخ في 18 صفر 1386 الموافق 08 يونيو سنة 1966 المتضمن قانون العقوبات، المعدد والمتمم، لاسيما ما تضمنه القانون رقم 04-15 المؤرخ في 10-11-2004، الجريدة الرسمية عدد 71 المؤرخة في 10 نوفمبر 2004.

[2] انظر القانون 18-07 المؤرخ في 10 يونيو سنة 2018، لاسيما الباب الخامس منه المتعلق بالتزامات المسؤول عن المعالجة، مرجع سابق

[3] دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم الالكترونية وحماية المجتمع، مرجع سابق،ص544.

[4] نصت المادة 72 من القانون 124 لسنة 1994، على " إنه في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز الأحوال المدنية ومحطات الإصدار الخاصة بها والمستخدمة في

كما تضمنت المادة 74 عقوبات تصل إلى الحبس لمدة ستة أشهر، كما جاء في نص المادة " إنه مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو غيره من القوانين يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من اطلع على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة أو قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو المساس بها بأي صورة من الصور أو إذاعتها أو إفشائها في غير الأحوال التي نص عليها القانون وفقا للإجراءات المنصوص عليها فيه، فإذا وقعت الجريمة على البيانات أو الإحصاءات المجمعة تكون العقوبة السجن"[1].

كما تم تجريم إتلاف الشبكة الناقلة لمعلومات الأحوال المدنية نتيجة الإهمال أو الرعونة أو عدم الاحتراز حسب ما تم تضمنه نص المادة 75 من نفس القانون، بالإضافة إلى نص المادة 76 الذي يحظر اختراق سرية البيانات أو المعلومات أو الإحصائيات المجمعة بأي صورة من الصور[2].

3. الجرائم المترتبة باستعمال الحاسوب في السعودية:

تم إقرار نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية من قبل مجلس الوزراء للملكة بتاريخ 1426/03/07هـ الموافق 2007/03/26، والذي حددت أهدافه بموجب نص المادة الثانية منه على النحو التالي: " يهدف هذا النظام إلى ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها وتوفير إطار نظامي لها بما يؤدي إلى تحقيق ما يلي:

إصدار الوثائق وبطاقات تحقيق الشخصية وبيانات واردة في محررات رسمية فإذا وقع التزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة السجن المشدد أو السجن لمدة لا تقل عن خمس سنوات".

[1] راجع المادة 74 من قانون العقوبات ، المرجع السابق.

[2] نصت المادة 75 على " أنه يعاقب بالحبس مدة لا تتجاوز ستة أشهر وغرامة لا تقل على مائتي جنيه ولا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية أو جزءا منها وكان ذلك ناشئا عن إهماله أو رعونته أو عدم احترازه أو عدم مراعاته للقوانين واللوائح والأنظمة. فإذا وقع الفعل عمدا تكون العقوبة السجن المشدد مع عدم الإخلال بحق التعويض في الحالتين. ونصت المادة 76 على " أنه يعاقب بالسجن المشدد كل من اخترق أو حاول في سرية اختراق البيانات أو المعلومات أو الإحصاءات المجمعة بأي صورة من الصور، تكون العقوبة السجن المشدد إذا وقعت الجريمة في زمن الحرب".

- إرساء قواعد نظامية لاستخدام التعاملات والتوقيعات الالكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بوساطة سجلات الكترونية يعول عليها.
- إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الالكترونية وسلامتها.
- تيسير استخدام التعاملات والتوقيعات الالكترونية على الصعيدين المحلي والدولي للاستفادة منها في جميع المجالات، كالإجراءات الحكومية والتجارة والطب والتعليم والدفع المالي الالكتروني.
- إزالة العوائق أمام استخدام التعاملات والتوقيعات الالكترونية"[1].

هذا وقد وضحت المواد من 03 إلى 10 من نفس النظام أنواع الجرائم المعلوماتية والعقوبة المقررة لكل منها، حيث شملت في الأساس عقوبة السجن لمدة تصل إلى ثلاث سنوات لكل من يصل دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال أو ما تتيحه من خدمات. كما يمكن تخفيف العقوبة لأقل من سنة في حالة المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها، أو جراء التصنت على ما هو مرسل عبر الشبكة المعلوماتية أو الدخول غير المشروع إلى موقع إلكتروني [2].

المطلب الثاني: تحديات حماية خصوصية البيانات الشخصية عبر الإنترنت

لقد أسهمت الوسائل التكنولوجية الحديثة للاتصال وحجز البيانات إلى تذليل مختلف صعوبات التواصل ونشر ونقل المعطيات الشخصية من حيث الزمان والمكان، بل أسهمت في تحفيز وتفضيل الاتصال باختيار المواقع الالكترونية الحديثة المنتشرة عبر الإنترنت، إلا أن تطور هذه الوسائل أثر بصورة أخرى على تأمين المعلومات المتداولة عبر شبكة الإنترنت، لاسيما تلك التي تخص البيانات الشخصية.

يرى الكثير من الباحثين في هذا المجال، التغير الجذري الذي طرأ في جوانب الاتصال وانعكاسه على حماية البيانات الشخصية، حيث يوجد العديد من التطبيقات تضم

1 دويب حسين صابر، المرجع السابق، ص545.

[2] دويب حسين صابر، المرجع السابق،ص545-546.

ملايين المشتركين، وتسهل تبادل البيانات الشخصية فيما بينهم، بمجرد نقرة واحدة بالرجوع إلى الاختصارات والتصاميم التي تسهل بسط كل تفاصيل الحياة الخاصة. كما تم تسجيل تنافس بين مختلف التطبيقات والشبكات الاجتماعية المختلفة، باعتماد أساليب استقطاب متباينة كمجانية العضوية، وا ٍعلانات العملاء، واستغلال بيانات مختلف المشتركين لتوجيه إعلانات ورسائل مشفرة يمكن من خلالها تحقيق أغراض تجارية باستغلال البيانات الشخصية للغير، حيث تعتمد مثلا شركة فيسبوك على جمع أدق التفاصيل عن مستخدميها، لاسيما ميولاتهم وفي المقابل تقوم ببيع حق الوصول إلى هذه البيانات من قبل شركات التسويق والإعلانات عبر الإنترنت[1].

وعليه سيتم التطرق من خلال هذا المطلب إلى دراسة تأثير الإنترنت على البيانات الشخصية خلال المعالجة (الفرع الأول) وكذا إبراز المخاطر التي تتسبب فيها الإنترنت على البيانات الشخصية وتأثير الجرائم السيبرانية على خصوصية البيانات الشخصية (الفرع الثاني).

الفرع الأول: تأثير الإنترنت على البيانات الشخصية أثناء المعالجة

وضح المشرع الجزائري من خلال نص المادة 03 من القانون 18-07، تعريف عملية معالجة المعطيات ذات الطابع الشخصي بأنها" كل عملية أو مجموعة عمليات منجزة بطرق أو سائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو النشر أو أي شكل من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف" كما أوضح في الفقرة السادسة من نفس المادة تعريف المعالجة الآلية بأنها " العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها"

وما نلاحظه من خلال هذين التعريفين اعتماد المفهوم الواسع الذي تبناه المشرع الجزائري لعملية معالجة المعطيات، وهو ما يؤكد أهمية هذه العملية وحساسيتها وكذا

[1] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية –الهم الأمني وحقوق الأفراد، المرجع السابق، ص34.

الحيز الواسع لضمان حماية شاملة وفعالة لأي عملية معالجة غير مشروعة للمعطيات ذات لطابع الشخصي.

كما نلاحظ كذلك التشابه أو التطابق مع التعريف الذي وضعه المشرع الفرنسي لعملية معالجة البيانات الشخصية، حسب مضمون الفقرة الثالثة من المادة الثانية من القانون 78-17، المعدل والمتمم، والتي عرفت عملية معالجة البيانات الشخصية بأنها " أي إجراء يتعلق بالبيانات الشخصية أيا كانت الطريقة المستخدمة فيه، لاسيما التجميع، التسجيل، الضبط، الحفظ، التعديل، الاستخلاص، الاطلاع، الاستخدام، الإبلاغ عن طريق النقل، النشر، الربط، المنع، المحو والإتلاف"[1].

ومن خلال مضمون التعريفين السابقين نستخلص اعتماد كل من المشرعين الجزائري والفرنسي على إعطاء أمثلة لبعض إجراءات المعالجة ولم يتم حصرها، مما يترك المجال واسعا لأي إجراء متعلق بالبيانات الشخصية[2].

تعتبر عملية معالجة البيانات الشخصية سلاح ذو حدين، لما تتطلبه العملية من إجراءات دقيقة تكرس باحترامها حماية المعطيات المعالجة، وعند الإخلال بأي ضابط من ضوابط المعالجة فإننا نكون بصدد خرق لمبادئ الحماية ومواجهة مختلف الأخطار المحتملة على هذه البيانات، كالاستغلال للمعطيات بجمعها وتخزينها بطرق غير مشروعة، التسجيل، الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

---

[1] Le texte selon l'article 02 , alinéa 03 de la loi 78-17 , modifiée et complétée: " constituer un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procède utilisé, et notamment la collecte, d'enregistrement, d'organisation, la conservation l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, de rapprochement ou l'interconnexion ainsi que le verrouillage , l'effacement ou la destruction ."

[2] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص410.

وعليه يمكن التفصيل في مختلف المخاطر المرتبطة بمعالجة البيانات الشخصية على النحو التالي:

أولا: معالجة المعطيات بصورة غير مشروعة

يمكن أن نكون في معالجة غير مشروعة بمجرد مخالفة إجراء من إجراءات المعالجة المحددة قانونا، على غرار عدم الحصول على التراخيص اللازمة أو القيام بالتصريح خلافا لما أقره المشرع الجزائري طبقا لأحكام المادة 12 من القانون 18-07[1]، أو القيام بالمعالجة بعد انتهاء المدة المرخص بها، حيث تم إقرار عقوبات بموجب أحكام المادة 56 من القانون 18-07، تصل إلى السجن لمدة أقصاها خمسة (05) سنوات[2] .

كما أن عدم الالتزام بالإجراءات التي تحددها السلطة الوطنية لحماية المعطيات الشخصية أثناء القيام بالمعالجة والذي من شأنه عرقلة عمل هذه الأخيرة فإنه يشكل عائقا أمام ضمان مشروعية هذه المعالجة، وهو يعد جريمة يعاقب عليها القانون طبقا لأحكام المادة 61 من القانون 18-07 والتي نصت على عقوبة الحبس من ستة أشهر إلى سنتين وكذا غرامة مالية من 60.000دج إلى 200.000دج ضد كل من يقوم بالاعتراض على إجراء عملية التحقق في عين المكان من قبل السلطة الوطنية أو يرفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة[3].

وتجدر الإشارة إلى أن معالجة بعض المعطيات الشخصية يتطلب من المسؤول عن المعالجة القيام بنقل هذه المعطيات إلى دولة أجنبية، وفي هذه الحالة ألزم المشرع الجزائري، المسؤول عن المعالجة بطلب ترخيص من السلطة الوطنية، وكذا ضمان هذه

---

[1] راجع أحكام المادة 12 من القانون 18-07، المرجع السابق.

[2] نصت المادة 56 من القانون 18-07 على " يعاقب بالحبس من سنتين (02) إلى خمس (05) سنوات، وبغرامة من 200.000دج إلى 500.000دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون. ويعاقب بنفس العقوبات كل من قام بتصريحات كاذبة أو واصل معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له".

[3] انظر المادة 61 من القانون 18-07، المرجع السابق.

الدولة مستوى كاف لحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات[1].

ثانيا: الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

تشكل عملية الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات خطرا كبيرا على البيانات الشخصية خلال المعالجة لاسيما إذا تعلق الأمر بتطبيقات مربوطة مباشرة بشبكة الإنترنت، سواء أتمت العملية عن بعد دون معرفة الشخص المعني، عن طريق اختراق حسابه أو معرفة كلمات المرور الخاصة به على التطبيق موضوع محل الجريمة المعلوماتية في مفهوم القانون 09-04، لاسيما نص المادة 02 منه[2].

ولقد تنوعت التعريفات الفقهية للدخول والبقاء غير المشروع من حيث ربطها بجهاز الحاسوب أو الإبقاء على مصطلح النظام المعلوماتي بصفة عامة، حيث عرفت العملية ب" الولوج غير المصرح به أو بشكل غير مشروع إلى نظام معالجة للمعطيات باستخدام الحاسوب"[3]. وما نلاحظه من خلال هذا التعريف هو اشتراط التصريح أو موافقة صاحب الجهاز أو الحساب على النظام المعلوماتي، سواء قصد الاطلاع على المعطيات أو التعامل في هذه المعطيات ومعالجتها بصورة غير مشروعة.

والمشرع الجزائري من خلال نص المادة 12 من القانون 18-07 أكد على ضرورة الحصول على ترخيص أو تصريح مسبق لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، عند كل عملية معالجة لمعطيات ذات طابع شخصي.

---

[1] انظر المادة 45 من القانون 18-07، المرجع السابق

[2] عرف المشرع الجزائري من خلال المادة 02 من القانون 09-04، المؤرخ في 05 غشت 2009، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ب "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

[3] فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية: الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر و الإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، مصر، 2007، ص128.

كما أقر قانون العقوبات الجزائري ضمن نص المادة 394 مكرر عقوبات تصل إلى السجن لمدة سنة، ضد كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو عند محاولة القيام بذلك[1].

وما تؤكده هذه المادة هو تجريم الدخول دون تصريح مسبق أو ترخيص كما أسلفنا أو البقاء غير المشروع، والملاحظ من خلال نص المادة أعلاه أن المشرع الجزائري لم يربط الدخول بالبقاء غير المشروع وا ٍنما توحيد الجزاء لكل من يدخل بطريقة غير شرعية فقط أو يدخل بدون ترخيص ويبقى عن طريق الغش بالرغم من معرفته بالمخالفة.

ولقد تباينت الآراء الفقهية حول جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، حيث ذهب فريق إلى اعتبارها جريمة عمدية وبالتالي يستبعد الدخول المفاجئ أو غير العمدي، في حين ذهب الفريق الآخر إلى اعتبارها جريمة سواء أكان الدخول عمداً أو عرضياً عن طريق الخطأ. والمشرع الجزائري توافق مع الاتجاه الأول باشتراط الركن المعنوي بوجود القصد العام المجسد في العلم والإرادة والقصد الخاص الذي يترجمه مضمون المادة 394 مكرر من قانون العقوبات السالفة الذكر بإيراد عبارة الدخول أو البقاء "**عن طريق الغش**"، أي أن اتجاه إرادة الجاني هو الدخول أو البقاء داخل نظام المعالجة بدون علم أو موافقة الشخص المعني أو الحصول على ترخيص من السلطة المؤهلة[2].

ثالثا: عدم الحفاظ على سرية وسلامة المعالجة

تعد المحافظة على سرية وسلامة المعالجة من أهم الالتزامات المترتبة على المسؤول عن المعالجة، وهذا تجنبا لأي كشف أو تسريب لمعطيات شخصية بصورة مقصودة أو غير مقصودة، ولقد ضبط المشرع الجزائري جملة من الضمانات للمحافظة على سلامة وسرية المعطيات الشخصية من خلال تخصيص فصل من القانون 18-07 لهذه

[1] راجع المادة 394 مكرر و394 مكرر1 من القانون 04-15 المعدل للأمر 66-156، المتضمن قانون العقوبات، المرجع السابق.

[2] هشام بخوش، الجرائم الماسة بسلامة المعطيات ذات الطابع الشخصي وفقا للقانون 18-07- معالجة معطيات فيروس كورونا –نموذجا، مجلة أبحاث قانونية وسياسية، المجلد6، العدد01، جوان(2021)، ص228.

الضوابط كما نص على عقوبات مالية تتراوح بين 200.000دج و500.000دج في حالة التسبب بإفشاء بيانات شخصية أو المساس بسلامتها خلافا للضمانات التي نصت عليه المادتين 38 و39 من القانون 18-07، كما يعاقب بنفس العقوبة كل من قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها قانونا أو تلك الواردة في الترخيص أو التصريح[1]. ويمكن تلخيص مختلف الضوابط المتعلقة بسلامة وسرية المعطيات المحددة ضمن المواد 39،38،40 و41 من القانون 18-07 على النحو التالي:

- يتعين على المسؤول على المعالجة وضع التدابير التقنية والتنظيمية الملائمة لسلامة وحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين، خصوصا عندما تستوجب المعالجة إرسال المعطيات عبر شبكة معينة وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة[2].
- يجب على المسؤول عن المعالجة اختيار معالج من الباطن، يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها، في حالة إجراء المعالجة لحسابه[3].
- يلتزم المسؤول عن المعالجة والأشخاص الذين اطلعوا أثناء ممارسة مهامهم على معطيات شخصية بالسر المهني، حتى بعد انتهاء مهامهم[4].
- يمنع على أي شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن الذي يلج إلى معطيات شخصية، أن يعالج هذه المعطيات دون تعليمات المسؤول عن المعالجة، باستثناء حالة تنفيذ التزام قانوني[5].

[1] انظر المادة 65 من القانون 18-07، المرجع السابق.
[2] راجع الفقرة الأولى من المادة 38 من القانون 18-07، المرجع السابق.
[3] راجع الفقرة الأولى من المادة 39 من القانون 18-07، المرجع السابق.
[4] راجع المادة 40 من القانون 18-07، المرجع السابق.
[5] راجع المادة 41 من القانون 18-07، المرجع السابق.

ومن الجدير بالذكر أن التدابير التي اشترطها المشرع الجزائري في المسؤول عن معالجة المعطيات، غير دقيقة وتحتاج إلى التفصيل، لاسيما في حالة ما إذا قام المسؤول عن المعالجة باتخاذ التدابير اللازمة إلا أنه تم ضياع أو تلف هذه المعطيات، مما يستوجب قيام أسباب الجريمة بالرغم من عدم تقصير المسؤول عن المعالجة[1].

كما نصت المادة 43 من القانون 18-07 على وجوب إعلام السلطة الوطنية لحماية المعطيات والشخص المعني، من قبل مقدم الخدمات، في حالة ما أدت معالجة المعطيات الشخصية في شبكات الاتصالات الالكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، إلى المساس بحياته الخاصة. مع ضرورة إمساك جرد محين من قبل كل مقدم خدمات حول الانتهاكات المتعلقة بالمعطيات الشخصية وما تم اتخاذه من إجراءات في شأنها. وفي حالة عدم الالتزام من قبل مقدم الخدمات فإنه تطبق عليه العقوبات الواردة في نص المادة 66 من القانون 18-07، والمتمثلة في الحبس من سنة إلى ثلاث سنوات ودفع غرامة من 100.000دج إلى 300.000دج[2].

وعليه تعد المعالجة غير المشروعة للمعطيات الشخصية باستعمال تقنية الإنترنت من أكبر الأخطار التي تحيط بعملية الحفاظ على سرية المعطيات الشخصية، مما يقتضي على المشرع التدقيق في ضبط كيفية المعالجة أولا ثم إقرار العقوبات اللازمة للتصدي لمختلف الجرائم ذات الصلة.

الفرع الثاني: تفاقم مخاطر الإنترنت والجرائم السيبرانية على البيانات الشخصية

تتنوع المخاطر التي تعترض البيانات الشخصية باختلاف نوع البيانات من جهة وكذا البيئة والتطور التكنولوجي من جهة أخرى، هذا الأخير الذي أسهم فيه تأثير الإنترنت بصورة بارزة، حيث أعزى الكثير من الباحثين سبب كل المخاطر والجرائم الناجمة عن استخدام الإنترنت إلى القصور المسجل في هذا الجانب من حيث مستعملي الإنترنت،

[1] هشام بخوش، الجرائم الماسة بسلامة المعطيات ذات الطابع الشخصي وفقا للقانون 18-07- معالجة معطيات فيروس كورونا –نموذجا، المرجع السابق، ص232.

[2] راجع المادة 66 من القانون 18-07، المرجع السابق.

وكذا استحالة توقع النتائج السلبية للاعتداءات في ظل استعمال التكنولوجيات الرقمية المربوطة بشبكة الإنترنت لعدة مؤشرات.

حيث تمثل الجرائم السيبرانية الوجه السلبي لاستعمال التكنولوجيات الرقمية، بالاعتماد على شبكة الإنترنت. ونظرا لتشعبها فإن الفقهاء والباحثين لم يجمعوا على تعريف موحد لها، والبعض الآخر ارتكز في تعريفه على موضوع الجريمة باعتبارها كل سلوك ايجابي أو سلبي يقع باستخدام تقنية المعلومات على مصلحة مشروعة بالاعتداء[1]. في حين ذهب جانب من الفقه إلى الإعتداد بالوسيلة المستعملة في الجريمة حيث تم تعريفها على نحو " كل نشاط إجرامي تستخدم فيه التقنية الالكترونية المتمثلة في الحاسوب الآلي الرقمي وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف"[2] وعرفها جانب آخر من الفقه بأنها" ما يقع على الشبكات وأنظمة تنقية المعلومات والأنظمة التشغيلية ومكوناتها (الأجهزة، والبرمجيات، والخدمات) من اختراق أو تعديل أو تعطيل أو دخول أو استخدام أو استغلال غير مشروع"[3].

كما أن المشرع الجزائري من خلال أحكام القانون 09-04، المؤرخ في 2009/08/05، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أورد تعريفا لهذا النوع من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كما يلي: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[4].

[1] رامي متولي القاضي، مكافحة الجرائم المعلوماتية، دار النهضة العربية، مصر، سنة 2011،ص17

[2] بهلول سمية، الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها،مجلة العلوم القانونية والاجتماعية، المجلد السادس، العدد الثالث، ديسمبر 2021،ص291.

[3] عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية : دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد09، العدد03، سنة 2020، ص149.

[4] راجع المادة 02 من القانون 09-04، المؤرخ في 05 غشت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخة في 16 غشت 2009.

والملاحظ من خلال هذا التعريف بالرغم اتساعه وشموليته، إلا أنه لم يتم فيه الفصل بين الجرائم السيبرانية عن الجرائم المعلوماتية. حيث تعد الجرائم السيبرانية أوسع من الجرائم المعلوماتية، نظرا لكونها تشمل الجرائم الواقعة على المعلومات والشبكات وتقنية المعلومات[1].

كما أن جانب من الفقه يرى أن الفاصل بين الجريمة السيبرانية والمعلوماتية هو أن الجريمة السيبرانية تستلزم باتصال جهازين الكترونيين أو أكثر مربوطين بشبكة انترنت محلية أو دولية باعتماد إحدى التقنيات الالكترونية المتطورة[2].

وعليه فان الإنترنت يمكن أن تكون وسيلة لإرتكاب الجريمة السيبرانية كما قد تشكل محلا لها.[3]

ومن أشد أنواع الجرائم خطورة ومساسا بالمعطيات الشخصية تلك الجرائم التي تستهدف الأطفال جسديا، عقليا ونفسيا، من خلال استغلالهم ونشر صور ومقاطع فيديو حول أعمال إباحية سواء كمحتوى متاح عبر شبكة الإنترنت دون قيود ومراعاة لهذه الشريحة من المجتمع، أو باستغلالهم كأطفال وبث صور ومقاطع عن الممارسات غير الشرعية ونشر ذلك عبر مواقع التواصل أو إتاحتها ضمن مختلف تطبيقات الشبكة العنكبوتية[4].

ولقد أكدت أدركت العديد من التشريعات الدولية خطر مثل هذا النوع من الجرائم، مما جعلها تسن قوانين صارمة وآليات لمجابهة انتشارها، ومن بين التشريعات الدولية التي حظرت مثل هذه الممارسات اللاشرعية، ما تضمنته اتفاقية بودابست المتعلقة بمكافحة الجريمة الإلكترونية لسنة 2001، في فصلها الثالث الخاص بالجرائم ذات الصلة

---

[1] عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية : دراسة تأصيلية مقارنة، المرجع نفسه، 149.

[2] حسينة شرون، فعالية التشريعات العقابية في مكافحة الجرائم الالكترونية، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد الأول، العدد1،2009، ص428.

[3] الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات- دراسة مقارنة-، أطروحة دكتوراه، جامعة أحمد دراية –أدرار، الجزائر، 2020-2021، ص37.

[4] سمية بهلول،الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها، المرجع السابق،ص 299.

بالمحتوى، والتي نصت مادتها التاسعة على الجرائم ذات الصلة بمواد إباحية عن الأطفال، والتي أقرت بشأنها ضمانات على النحو التالي[1]:

" 1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية أو غيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني إذا ارتكبت عمدا وبغير حق:

أ. إنتاج مواد إباحية عن الأطفال بغرض توزيعها عبر نظام الكومبيوتر.

ب. عرض مواد إباحية عن الأطفال أو إتاحتها عبر نظام الكومبيوتر.

ت. توزيع مواد إباحية عن الأطفال أو نقلها عبر نظام الكومبيوتر.

ث. الحصول على مواد إباحية عن الأطفال عبر نظام الكومبيوتر لصالح الشخص ذاته أو لفائدة الغير.

ج. حيازة مواد إباحية عن الأطفال داخل نظام الكومبيوتر أو على دعامة لتخزين بيانات الكومبيوتر.

2. لغرض الفقرة أعلاه تشمل عبارة " مواد إباحية" المواد الإباحية التي تعرض بشكل مرئي:

أ- قاصر وهو يمارس سلوكا جنسيا واضحا.

ب- شخص يبدو قاصرا وهو يمارس سلوكا جنسيا واضحا.

ج- صور واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا واضحا".

هذا ويزداد خطر الجريمة السيبرانية على مختلف الفئات عن طريق سرقة بياناتهم واستغلالها لأغراض متعددة، في إطار ما يسمى بالإرهاب الالكتروني. هذا الأثر السلبي للجريمة السيبرانية الذي بدأ بالانتشار منذ أواخر القرن الماضي واستفحل في العصر الحالي، حيث عرفه **دوروثي دينينغ**، أحد الباحثين في مجال الأمن السيبراني، بأنه " هجوم إلكتروني أو تهديد بهجوم مدمر وتخريبي من قبل جهات بارزة غير حكومية ضد

[1] راجع المادة 09 من اتفاقية بودابست، المتعلقة بالجرائم الالكترونية، الموقعة في 23 نوفمبر 2001 والتي دخلت حيز التنفيذ بتاريخ 2004/07/01، والمحملة من الموقع الالكتروني للمجلس الأوروبي بتاريخ 2021/01/28. " https://rm.coe.int/budapest-convention-in-arabic/1680739173 "

الحكومات والشركات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو اجتماعية"[1]. وفي هذا الإطار برز في الوقت الحالي جليا الخطر الذي تلحقه هذه الجرائم الصعب التحكم فيها، لاسيما وأنه يتم اللجوء إلى استغلال الأطفال على نحو واسع بالإغراء والإغواء وا ٍقناعهم بالتجنيد في جماعات متطرفة بأفكار أولية عن طريق استغلال الشبكات والمواقع الإلكترونية، وحصرهم في المواقع الخاصة بما يسمى الأشبال بمناطق النفوذ وغيرها من الطرق لينتقل التجنيد من العالم الافتراضي إلى الواقع [2].

وتوجد طوائف عدة لمجرمي المعلوماتية أخطرها طائفة " The Criminally Negligent" والتي تهتم بإساءة استخدام الحواسب الآلية المبرمجة، وقد تصل في أعمالها الإجرامية إلى إزهاق الأرواح، كما حدث في نيوزلندا، أين قام اثنان من مبرمجي الحواسب الآلية بتغيير نظام أحد البرامج المحددة لخط سير إحدى الطائرات، دون إبلاغ قائد الطائرة في الحين، مما تسبب في تحطم الطائرة بعد اصطدامها بجبل وخلفت الحادثة مقتل 60 مسافرا على متنها، حيث تم محاكمة ومحاسبة المتهمين بتهمة القتل الخطأ[3].

والمشرع الجزائري بدوره أيقن بخطر هذا النوع من الجرائم وانعكاساتها على التركيبات الاجتماعية بمختلف أصنافها، لاسيما في ظل الاستعمال الواسع والمفرط للانترنت، بحيث تم تضمين تعديلات لقانون العقوبات بإدراج ثمان (08) مواد خاصة بمكافحة الجريمة

[1] Dorothy Denning considère que le cyberterrorisme est « une attaque informatique ou menace d'attaque informatique entrainant d'importants dégâts conduite par des acteurs non étatiques contre des systèmes d'information pour intimider ou contraindre des gouvernements ou sociétés dans le cadre d'objectifs d'ordre politique ou sociaux »

Pour plus de détaille voir ; Desforges Alix, « Cyber-Terrorism : quel Périmètre », fiche N11 de l'institut de recherche stratégique de l'école militaire (IRSEM), Décembre 2011, Article on ligne disponible sur le site : www.defense.gov.fr " file:///C:/Users/USER/Downloads/Fiche_n11_perimetre_cyberterrorisme.pdf" date de consultation de site le : 29 /01/ 2021.

[2] بليدي دلال، وبوقرين عبد الحليم، الآليات القانونية لمكافحة الجرائم الإلكترونية ضد الأطفال،مجلة التمكين الاجتماعي،العدد01، مارس2019،ص80.

[3] خالد داودي، الجريمة المعلوماتية، المرجع السابق، ص36.

المعلوماتية بمفهومها الواسع مع تعديل قانون العقوبات لسنة 2004، بإدراج المواد 394 مكرر إلى المادة 394 مكرر7 من القسم السابع مكرر، المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات[1].

كما صدر سنة 2009 القانون 09-04[2]، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي ضبط إطارا هاما لمكافحة الجريمة الالكترونية وأحدث آلية مؤسساتية مكلفة بالوقاية من الجرائم الالكترونية، تسمى "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي لم يصدر التنظيم المتعلق إلى غاية سنة 2015، بموجب أحكام المرسوم الرئاسي 15-261، المتضمن تنظيم الهيئة، ليتم إعادة تنظيمها بموجب المرسوم الرئاسي 20-183، المؤرخ في 13 يوليو 2020، ثم ليعاد تنظيمها كذلك بموجب المرسوم الرئاسي 21-439، المؤرخ في 07 نوفمبر 2021، وهو ما يعكس التردد والتأخر الملحوظ من قبل المشرع في ضبط تنظيم هذه الهيئة الحساسة والتي بإمكانها أن تلعب دور اكبير ا في مكافحة الجرائم السيبرانية، لاسيما تلك التي تمس خصوصية المعطيات الشخصية المعالجة آليا، إلى جانب المؤسسات الأخرى المشتركة في نفس الغاية، لاسيما سلطة ضبط البريد والاتصالات الالكترونية المنشأة بموجب القانون 18-04، المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية[3]. ليليها إقرار إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، بموجب القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[4].

[1] راجع المواد المذكورة ضمن قانون من الأمر 66-156 المؤرخ في 18 صفر 1386 الموافق 08 يونيو سنة 1966 المتضمن قانون العقوبات، المعدد والمتمم، لاسيما ما تضمنه القانون رقم 04-15، المرجع السابق.

[2] راجع المادتين 13 و14 من القانون 09-04، المرجع السابق.

[3] لأكثر تفصيل راجع المواد من 11 إلى 28 من القانون 18-04، المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية عدد 27، المؤرخة في 13 ماي 2018.

[4] لأكثر تفصيل راجع المواد من 23 إلى 31 من القانون 18-07، المرجع السابق.

وسيتم التفصيل أكثر حول مجال الحماية المكفول من قبل مختلف النصوص القانونية و التنظيمية الوطنية والآليات المؤسساتية المنشأة لذات الغرض، في الفصل الثاني من الباب الموالي من هذه الأطروحة.

الباب الثاني:
الحماية القانونية الدولية والوطنية للبيانات الشخصية

الباب الثاني: الحماية القانونية الدولية والوطنية للبيانات الشخصية

بعد تفصيل مفهوم البيانات الشخصية، من مختلف الجوانب، وتوضيح أبرز الدوافع الملز مة للبحث عن مجال مناسب لتكريس حمايتها، سيتم التطرق ضمن هذا الباب إلى التكريس القانوني الفعلي لهذه الحماية من خلال التفصيل في مختلف الآليات المكرسة دوليا ووطنيا لحماية البيانات الشخصية.

ومن هذا المنطلق تم تخصيص الفصل الأول، بالدراسة والتحليل لمختلف جوانب حماية البيانات الشخصية، على الصعيد الدولي من خلال الرجوع إلى مضامين مختلف الاتفاقيات الدولية، مع التفصيل في دور أجهزة مختلف المنظمات الدولية الجماعية والإقليمية المهتمة بمجال حماية البيانات الشخصية بصورة مباشرة أوغير مباشرة، مع الإشارة إلى موقف المشرع الجزائري بخصوص المصادقةو الانضمام لمختلف المعاهدات الدولية المكرسة لحماية البيانات الشخصية، أو التحفظ على ذلك، بالنظر إلى اعتبارات محددة سيتم التفصيل فيها عند دراسة كل آلية.

كما تم تخصيص الفصل الثاني لعرض وتدقيق مختلف جوانب حماية البيانات الشخصية، المكرسة من قبل المشرع الجزائري ضمن مختلف النصوص القانونية الوطنية، سواء بصورة مباشرة أوغير مباشرة باستقراء مضامين مختلف النصوص القانونية ذات الصلة، نظرا لكون مجال البيانات الشخصية ميدان متشعب، يرتبط بميادين عدة على غرار قوانين العقوبات، الإجراءات الجزائية، البريد والاتصالات الإلكترونية، المعلومات والوثائق الإدارية، التوقيع والتصديق الإلكترونيين، حماية معطيات الأشخاص الطبيعيين...الخ.

و عليه سيتم التفصيل في مختلف الآليات المكرسة على مختلف المستويات، مع الاستعانة ببعض المقاربات مع بعض التشريعات الدولية السباقة في تكريس هذه الحماية، للوقوف على مواطن الخلل، وتقييم فعالية مختلف الآليات.

الفصل الأول: الحماية القانونية الدولية الجماعية والإقليمية للبيانات الشخصية

لقد برز اهتمام القانون الدولي بحماية البيانات الشخصية بصورة أدق وأنجع مع نهاية القرن العشرين، لاسيما مع تأثير التطور التكنولوجي وتسارعه بوتيرة عالية، وبروز العديد من المعدات الرقمية المعالجة للمعطيات، لاسيما جهاز الحاسوب والهواتف الذكية وبالخصوص تلك المربوطة بشبكة الإنترنت أو غيرها من شبكات الاتصال.

وفي هذا الإطار هرعت العديد من المنظمات الدولية والإقليمية إلى بحث حلول مستعجلة لمواكبة موجة هذا التطور من جهة والحفاظ على الخصوصية والبيانات الشخصية من جهة أخرى، وفي هذا الإطار تم إقرار جملة من المبادئ والمعاهدات الرامية إلى ضبط معايير حماية هذه البيانات على المستوى الدولي أو على المستوى الإقليمي، حسب ما سيتم التطرق له في المبحثين المواليين.

المبحث الأول: الحماية الدولية الجماعية للبيانات الشخصية

اهتم التشريع الدولي بموضوع حماية البيانات الشخصية منذ القرن الماضي لاسيما بإقرار جملة من المعاهدات والاتفاقيات الدولية التي تهدف إلى تكريس حماية الخصوصية بصفة عامة والبيانات الشخصية بصفة خاصة، بالإضافة إلى بروز دور بعض المنظمات الدولية في حماية البيانات الشخصية على غرار قرارات الجمعية العامة للأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية، وهو ما سيتم التطرق له بالتفصيل في المطلبين المواليين.

المطلب الأول: المعاهدات والاتفاقيات الدولية الجماعية لحماية البيانات الشخصية

وضحت اتفاقية فينا لقانون المعاهدات المبرمة في 23 مايو 1969 والتي انضمت لها الجزائر بتحفظ سنة 1987 بأن مصطلح الاتفاقية يشمل " يراد بتعبير المعاهدة " اتفاق دولي معقود بين دول بصورة خطية وخاضع للقانون الدولي، سواء أثبت في وثيقة واحدة

أو اثنتين أو أكثر من الوثائق المترابطة، وأيا كانت تسميته الخاصة"[1]. كما أن المعاهدات الدولية تصنف إلى عقدية وشارعة، فالمعاهدات العقدية هي التي تعقد بين شخصين أو أكثر من أشخاص القانون الدولي العام، وتهدف إلى تنظيم العلاقات بين الدول بحسب الطرق المناسبة لها، بينما المعاهدات الشارعة فهي تلك المشرعة والملزمة لأكثر من شخص من أشخاص القانون الدولي، ويصطلح عليها كذلك المعاهدات الجامعة وتقسم إلى تصنيفات عدة من أهمها صنفين[2]:

- المعاهدات الجماعية: وهي المعاهدات العامة التي تضم كل أو أغلب الدول مثل ميثاق الأمم المتحدة.

- المعاهدات الدولية الإقليمية: وهي التي تضم مجموعة من الدول التي تقع في قارة أو أكثر، وتشمل كل الاتفاقيات الموافق عليها من قبل أحد أجهزتها، ومن تلك المعاهدات، نميز الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010[3].

وفي هذا الإطار تم إقرار بعض الاتفاقيات والمعاهدات الدولية المكرسة لحماية البيانات الشخصية بصور مباشرة أو غير مباشرة من خلال مضامينها على غرار معاهدة بودابست لمكافحة جرائم الإنترنت ومعاهدة برن لحماية المصنفات الأدبية والفنية، حيث سيتم التطرق لكل معاهدة بالتفصيل على النحو التالي:

الفرع الأول: الاتفاقية المتعلقة بالجريمة الالكترونية "بودابست"

في عام 1976 تم اعتماد الإطار الدولي لجرائم الحاسوب من قبل المجلس الأوروبي وتم تكريس جملة من الآليات على المستوى الوطني للدول الأعضاء وكذا على المستوى

[1] راجع المادة الثانية من اتفاقية فينا لقانون المعاهدات المبرمة في 23 مايو سنة 1969، التي انضمت إليها الجزائر، بتحفظ، بموجب المرسوم 87-222، المؤرخ في 13 أكتوبر 1987، الجريدة الرسمية عدد 42، المؤرخة في 14 أكتوبر 1987.

[2] لأكثر تفصيل راجع : جمال عبد الناصر مانع، القانون الدولي العام –المدخل والمصادر، دار العلوم للنشر والتوزيع، مصر، 2005، ص63.

[3] جمال عبد الناصر مانع، القانون الدولي العام –المدخل والمصادر، المرجع السابق، ص64.

الإقليمي، حيث تم سنة 1996 إنشاء لجنة خبراء للتعامل مع مشكلة الجرائم السيبرانية وذلك تحت إشراف اللجنة الأوروبية لمعالجة مشاكل الجريمة.

وقد تم تشكيل لجنة خبراء من عدة دول، والتي كلفت في الأساس بإعداد مشروع نص إقليمي يكفل حماية البيانات الشخصية والذي تبلور من خلال البحث ومناقشة العديد من المسودات إلى إعداد مشروع اتفاقية مكافحة الجريمة الالكترونية[1] والتي اعتمدها البرلمان الأوروبي في جلسته العامة في شهر ابريل 2001، وتم التصديق على هذه الاتفاقية من قبل 30 دولة أوروبية[2]، كما تم التعاون في وضعها بين العديد من الدول من مجلس أوروبا وكذا كل من دولة كندا، اليابان، جنوب إفريقيا والولايات المتحدة الأمريكية، وقد دخلت الاتفاقية حيز التطبيق سنة 2004، كما أتيح المجال لأي دولة تريد الانضمام حتى من غير الدول الأوروبية، حيث وقعت على هذه الاتفاقية العديد من الدول غير الأوروبية، على غرار الولايات المتحدة الأمريكية وجنوب إفريقيا، الأمر الذي يؤكد الطابع الدولي لهذه الاتفاقية[3]، وهي تعد الإطار المرجعي لمكافحة جرائم المعلوماتية[4].

ومن خلال استقرائنا لمختلف بنود اتفاقية بودابست لاحظنا الكثير من التشابه والتقارب في العديد من المحاور التي تخص مجالات الحماية المكرسة بموجب الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، وهو ما سيتم التفصيل فيه في المبحث الثاني من هذا الفصل.

---

[1] الاتفاقية المتعلقة بالجريمة الالكترونية "بودابست"، متاحة على الموقع الرسمي لمجلس أوروبا، على الرابط التالي " "https://rm.coe.int/16802fa3ff

[2] جورج لبكي، المعاهدات الدولية للانترنت،: حقائق وتحديات، مجلة الدفاع الوطني اللبناني، العدد 83، كانون الثاني/ يناير 2013، ص91.

[3] خالد ممدوح إبراهيم محمد، الحماية الجنائية للتوقيع الإلكتروني في القانون الاتحادي رقم2 لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات (المعدل بالقانون رقم 5 لسنة 2012)، مجلة الفكر الشرطي، المجلد الثالث والعشرون، العدد88، يناير 2014، ص184.

[4] أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 17، العدد01، 2018، ص740.

وقبل الرجوع إلى مضمون الاتفاقية سيتم الإشارة إلى الأهداف المسطرة من خلال لجنة الخبراء المختصة في هذا المجال و التي رسمت جملة من الأهداف نلخصها كما يلي:

- ضبط الإجراءات والسبل الكفيلة لتكريس التعاون الدولي في مجالات التحري ضد الجرائم الالكترونية، لاسيما بشأن تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وضبط الإجراءات القضائية المناسبة للفصل في هذه الجرائم.

- تكييف المنظومات التشريعية الداخلية لكل دولة مع الأحكام المتعلقة بالجرائم الإلكترونية.

- بسط الإطار العام للتحري ومتابعة الجرائم الالكترونية باستعمال الحاسوب

- تعيين نظام سريع وفعال للتعاون الدولي.

- الحفاظ بشكل سريع على البيانات موضوع المعالجة، المخزنة على أجهزة الكمبيوتر وحفظها وفق آليات دقيقة ومراقبة تدفقها الجزئي لاسيما خارج إقليم الدولة المعنية.

- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها[1].

وعليه سيتم التطرق إلى أهم محاور الاتفاقية والتي تخص حماية معالجة البيانات الشخصية من كل مخاطر الجريمة الإلكترونية، بدءا بعرض توضيح مختلف المصطلحات الواردة ضمن نص الاتفاقية.

أولا: عرض وتوضيح مصطلحات الاتفاقية الخاصة بمجال معالجة البيانات الشخصية

لقد احتوت الاتفاقية على العديد من المصطلحات التي تخص مجال معالجة البيانات الشخصية بصفة مباشرة أو غير مباشرة، والتي فصلتها المادة الأولى من الاتفاقية على النحو التالي:

1- منظومة الكومبيوتر: "أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقا لبرنامج، بالمعالجة الآلية للبيانات ".

[1] جور ج لبكي، المرجع السابق ص92.

2- بيانات الكومبيوتر: " أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معينة".

3- مقدم الخدمة: " يقصد به:

- أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوتر،
- أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة".

ثانيا: الجرائم المرتبطة بمجال حماية البيانات الشخصية المنصوص عليها في الاتفاقية:

نصت الاتفاقية على جملة من الجرائم التي تخص البيانات الشخصية مباشرة بحيث تؤثر على خصوصية وسلامة البيانات، ونظم الكومبيوتر، وكذا جرائم ذات الصلة بالمحتوى، وجرائم انتهاك حقوق النشر والتأليف والحقوق ذات الصلة، وسيتم التفصيل في كل نوع من أنواع الجرائم المذكورة على النحو التالي:

1. الجرائم الماسة بخصوصية وسلامة وتوافر بيانات ونظم الكومبيوتر:

تم حصر هذه الجرائم حسب مضمون الاتفاقية في أربعة أنواع، تشمل النفاذ غير المشروع، الاعتراض غير المشروع، التدخل في البيانات والتدخل في النظام.

1.1 **جريمة النفاذ غير المشروع:** أشار نص المادة 02 من الاتفاقية إلى ضرورة اتخاذ كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير في قانونها الوطني لتجريم النفاذ الكامل أو الجزئي إلى نظام حاسوب في حالة ما ارتكب عمدا وبغير حق. كما يجوز لطرف أن يستلزم ارتكاب الجريمة عن طريق مخالفة التدابير الأمنية، بنية

الحصول على بيانات الكومبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط واتصال بين حاسوبين بنظام معلوماتي معين[1].

وقد وضح التقرير التفسيري لاتفاقية بودابست أن الولوج غير القانوني يعتبر جريمة رئيسية تشكل تهديدا لأمن وسلامة وسرية النظم والإتاحة غير القانونية للبيانات والمعلومات التي تتضمنها، كما من شأن الدخول غير المشروع أن يساعد الهكرة والقراصنة على ارتكاب جرائم أخرى كالتزوير والغش المعلوماتي[2].

1.2 جريمة الاعتراض غير المشروع: أشارت المادة 03 من الاتفاقية على أن جريمة الاعتراض غير المشروع تثبت في حالة الاعتراض العمدي وبغير حق، باستخدام وسائل فنية للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من داخل نظام كومبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كومبيوتر يحمل هذه البيانات. وتم من خلال نص المادة المذكورة التأكيد على قيام الدول الأطراف بتحيين تشريعاتها الوطنية لتتماشى مع تجريم الاعتراض غير المشروع.

1.3 جريمة التدخل في البيانات: وضحت المادة 4 من الاتفاقية أن جريمة التدخل في البيانات تتمثل في القيام عمدا بإتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها. كما أبقت المجال مفتوحا لكل دولة في أن تحتفظ بحقها في أن تشترط حصول ضرر جسيم لتجريم الأفعال الأفعال المذكورة.

1.4 جريمة التدخل في النظام: نصت الاتفاقية على اعتماد كل دولة ما يلزم من تدابير تشريعية لتجريم ارتكاب، بغير وجه حق وبصورة عمدية، الإعاقة الخطيرة لاشتغال نظام الكومبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها[3].

---

[1] انظر المادة 02 من الاتفاقية المتعلقة بالجريمة الإلكترونية "بودابست"، المرجع السابق.

[2] خالد ممدوح إبراهيم محمد، الحماية الجنائية للتوقيع الإلكتروني في القانون الاتحادي رقم2 لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات (المعدل بالقانون رقم 5 لسنة 2012)، المرجع السابق، ص185

[3] راجع المادة 5 من الاتفاقية المتعلقة بالجريمة الإلكترونية " بودابست"، المرجع السابق.

2. الجرائم ذات الصلة بالكومبيوتر:

تشمل جريمتين التزوير والاحتيال:

2.1 **جريمة التزوير المرتبط بالكومبيوتر:** عرفت المادة 08 من الاتفاقية هذه الجريمة بالقيام عمدا وبغير حق بإدخال، حذف أو إتلاف بيانات كومبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. كما أتيح المجال لأي دولة طرف أن تشترط وجود القصد الجنائي، أي نية الاحتيال، أو نية غير صادقة مشابهة، سابقة لإلحاق المسؤولية الجنائية.

2.2 **جريمة الاحتيال المرتبط بالكومبيوتر:** وهنا أشارت الاتفاقية إلى أن جريمة الاحتيال يقصد بها التسبب العمدي في إلحاق خسائر بملكية شخص آخر عن طريق القيام بإدخال تغيير، حذف أو إتلاف بيانات الكومبيوتر، أو التدخل في وظيفة نظام الكومبيوتر، بنية الاحتيال أو نية سيئة، للحصول بدون وجه حق على منفعة اقتصادية ذاتية أو لفائدة شخص آخر.

3. الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة:

أحالت الاتفاقية تعريف انتهاك حقوق النشر والتأليف إلى التشريعات الداخلية لكل دولة، وكذا التزامات كل دولة بموجب وثيقة باريس لسنة 1979، المعدلة لاتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية[1]. وسيتم التفصيل في هذا النوع من الجرائم وكذا الآليات والاتفاقيات المذكورة لحماية المصنفات الأدبية والفنية الرقمية، على وجه الخصوص في الفرع الموالي.

[1] انظر المادة 10 من اتفاقية بودابست، المرجع السابق.

الفرع الثاني: معاهدات حماية المصنفات الأدبية والفنية الرقمية

تم إبرام العديد من المعاهدات والاتفاقيات في مجال حماية البيانات الشخصية المدرجة ضمن المصنفات الأدبية والفنية الرقمية التي يمكن أن تتداول عبر شبكة الإنترنت، ومن أهمها اتفاقية برن لحماية المصنفات الأدبية والفنية لسنة 1886، واتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية ومعاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف، وهو ما سيتم التفصيل فيه على النحو التالي:

أولا: اتفاقية برن لحماية المصنفات الأدبية والفنية:

تعد اتفاقية برن لحماية المصنفات الأدبية والفنية من أقدم المواثيق الدولية المهتمة بحماية حقوق المؤلف حيث أُبرمت منذ سنة 1886 وعرفت العديد من التعديلات والتنقيحات سنوات 1896، 1908، 1914، 1928، كان آخرها تعديل باريس سنة 1971 [1]، المتمم سنة 1979[2].

وقد انضمت الجزائر بتحفظ إلى هذه الاتفاقية سنة 1997، بموجب أحكام المرسوم الرئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997[3]. وقد أدخل المشرع الجزائري عدة

---

[1] تضمنت المادة الأولى من اتفاقية حقوق المؤلف المعدلة بباريس سنة 1971 ما يلي: " تتعهد كل دولة من الدول المتعاقدة بأن تتخذ كل التدابير اللازمة لضمان حماية كاملة وفعالة لحقوق المؤلفين وغيرهم من أصحاب تلك الحقوق في الأعمال الأدبية والعلمية والفنية بما في ذلك المواد المكتوبة والأعمال الموسيقية والمسرحية والسينمائية وأعمال التصوير والنقش والنحت"

لأكثر تفصيل راجع: سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، لبنان،الطبعة الأولى 2011، ص 284

[2] فتيحة حواس، حماية المصنفات الفنية وأسماء النطاقات على شبكة الإنترنت، مكتبة الوفاء القانونية، الإسكندرية، ط1، سنة 2017، ص183.

[3] المرسوم الرئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997، المتضمن انضمام الجمهورية الجزائرية الديمقراطية الشعبية، مع التحفظ، إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، المؤرخة في 09 سبتمبر 1886، والمتممة بباريس في 04 مايو سنة 1896 والمعدلة ببرلين في 13 نوفمبر سنة1908، والمتممة ببرن في 20 مارس 1914 والمعدلة بروما في 02 يونيو سنة 1928 وبروكسل في 26 يونيو سنة 1948 و استوكهولم في 14 يوليو سنة 1967 وباريس في 24 يوليو سنة1971 والمعدلة في 28 سبتمبر سنة 1979. الجريدة الرسمية عدد 61، المؤرخة في 14 سبتمبر 1997.

تعديلات مست قانون حقوق المؤلف والحقوق المجاورة بموجب الأمر 03-05، المؤرخ في 09 يوليو 2003، تضمنت تجريم الاعتداء على الملكية الفكرية لاسيما مضمون المادتين 152 و153 منه[1] هذا بالإضافة إلى نص المادة 162 منه على تكريس حماية جميع المصنفات والأداءات المحمية بموجب الاتفاقيات الدولية التي تكون الجزائر طرفا فيها[2]. وهذا الانضمام والتكريس كان متزامنا مع الشروط المطروحة آنذاك للانضمام إلى المنظمة العالمية للتجارة[3].

وتجدر الإشارة أن الإتفاقية تضمنت جملة من المبادئ التي تشكل الحد الأدنى الواجب توفره لحماية مختلف المصنفات الأدبية والفنية حيث أشار نص المادة الثانية منها إلى تعريف هذه المصنفات ب: "كل إنتاج في المجال الأدبي والعلمي والفني، أيا كانت طريقة أو شكل التعبير عنه". حيث يمكن تلخيص المبادئ التي نصت عليها المعاهدة في ثلاث نقاط أساسية[4]:

1. يجب أن تكون الحماية شاملة ومستقلة ولا تتوقف فقط على الحماية الممنوحة في بلد منشأ المصنف، ومع ذلك، إذا حدد تشريع أية دولة عضو مدة أطول للحماية من الحد الأدنى المنصوص عليه في الاتفاقية وتوقفت حماية المصنف في بلد المنشأ، جاز رفض الحماية عند انتهاء مدتها في بلد المنشأ.

2. يجب أن تحظى المصنفات الناشئة في إحدى الدول المنضمة للمعاهدة أو تلك التي نشرت لأول مرة في تلك الدولة أن تحظى بالحماية اللازمة في كل دولة من الدول المتعاقدة، بحيث تتيح نفس الحماية التي تتمتع بها المصنفات الداخلية لمواطني ذات الدولة، في إطار مبدأ عدم التمييز، وقد اشترطت بعض التشريعات إقرار هذا المبدأ بشرط

---

[1] الأمر 03-05 المؤرخ في 19 يوليو سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 44 المؤرخة في 23 يوليو سنة 2003.

[2] راجع المادة 162 من الأمر 03-05، المرجع نفسه.

[3] خالد داودي، الجريمة المعلوماتية، المرجع السابق، ص91.

[4] ملخص اتفاقية برن لحماية المصنفات الأدبية والفنية لسنة 1886، موقع المنظمة العالمية للملكية الفكرية (WIPO)، الاطلاع بتاريخ 06 نوفمبر 2021على العنوان التالي: "
https://www.wipo.int/treaties/ar/ip/berne/summary_berne.html "

المعاملة بالمثل، على غرار ما أقره المشرع الفرنسي في القانون المتعلق بحماية حقوق المؤلف لسنة 1985، حيث أشار إلى أن الأجانب تكفل لهم الحماية قانونا متى كانت الدولة التي يحملون جنسيتها أو يقيمون بها أو يمارسون عملهم فيها تمنح حمايتها للمعلومات التي يدخلها حاملوا الجنسية الفرنسية أو القاطنون بفرنسا أو العاملون فيها[1].

3. يجب تكريس الحماية التلقائية دون اشتراط أي إجراء شكلي للحماية مهما كان موضوع المصنف المشمول بهذه الحماية.

كما أوردت المواد 09، 10 و11 من معاهدة برن بعض التقييد مس الحقوق المالية، والتي تجسد مختلف الوضعيات التي يجوز فيها الانتفاع بالمصنفات المشمولة بالحماية بدون تصريح مالك حق المؤلف، وبدون دفع أي مقابل مكافئ بل يمكن الانتفاع المجاني من خلال الاقتباس والانتفاع بالمصنفات بغرض التعليم والمساهمة في تشجيع مختلف البحوث العلمية أو القيام بالإبلاغ عن الأحداث الجارية، أو التسجيلات المؤقتة بهدف البث فيها[2].

ويسمح ملحق وثيقة باريس الخاصة بالاتفاقية أيضا للدول النامية بإنفاذ تراخيص غير طوعية لترجمة المصنفات واستنساخها في بعض الحالات، التي تخص المجالات التعليمية. وفي هذه الحالات، يسمح بالانتفاع المشار إليه بدون ترخيص مالك الحق، بشرط دفع المكافأة التي ينص عليها القانون[3].

وتجدر الإشارة إلى أن هذه المعاهدة نصت على جملة من الحقوق المعنوية، على غرار الحق في المطالبة بنسب المصنف إلى مؤلفه والحق في الاعتراض على أي تشويه أو تحريف أو تعديل أو تقييد للمصنف من شأنه الإضرار بمكانة المؤلف أو بشهرته أو نزاهته. إلا أن ما يستخلص من هذه المعاهدة هو عدم التطرق لبرامج الإعلام الآلي ضمن جملة المصنفات الأدبية والفنية موضوع الحماية المكرسة، كما أنها لم تعالج النشر

[1] سليم عبد الله الجبوري، المرجع السابق، ص285.

[2] راجع المواد 9، 10 و11 من معاهدة برن لسنة 1886، المعدلة والمتممة.

[3] ملخص معاهدة برن لحماية المصنفات الأدبية والفنية لسنة 1886، المرجع السابق.

الالكتروني أو استغلال وتأثير برمجيات وتطبيقات الإعلام الآلي والوسائل الرقمية في نقل أو تعديل المعطيات ضمن مختلف المؤلفات الرقمية[1].

ولعل هذا الأمر من بين الدوافع المساهمة في إبرام اتفاقيات أخرى تعنى بهذا الجانب على غرار اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية.

ثانيا: اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية "تريبس"

تم التوقيع على هذه الاتفاقية سنة 1994، ودخلت حيز التنفيذ بتاريخ 01 يناير 2000، بلغ عدد الدول المنضمين إلى الاتفاقية 117 دولة من بينها مصر الدولة العربية الوحيدة ، حيث تضمنت العديد من القواعد المكرسة لحماية المصنفات الرقمية، والاعتماد على استخدام الحاسوب في معالجة المصنفات الرقمية، وكذا آليات حماية برامج الحاسوب وقواعد البيانات، مع تكريس حماية مدنية وجزائية للبيانات الشخصية التي تشتمل عليها مختلف المصنفات الرقمية[2].

وقد أشار نص المادة 10 من الاتفاقية على حماية برامج الحاسب، مع إدراجها ضمن المصنفات الفنية والأدبية، بحيث يتمتع مؤلفها بكافة الحقوق المعنوية والمالية، هذا إلى جانب المواد المجمعة أو البيانات الأخرى سواء أكانت في شكل مقروء آليا أو في أي شكل آخر[3].

---

[1] فتيحة حواس، المرجع السابق، ص184.

[2] هاجر كرماش، سلامي ميلود، حماية المصنفات الرقمية في ظل اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية "تربس"، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد13، العدد 02، أكتوبر 2021، ص1343.

[3] راجع المادة 10 من اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، الموجودة على الربط الخاص بمكتبة الكويت الوطنية "https://nlk.gov.kw/Upload/Bibligra/Trips(1)831201621700PM.pdf"، تاريخ آخر اطلاع 2022/02/12، على الساعة 12:20.

وفي ذات السياق أقر الفقه المقارن حماية برمجيات الحاسوب لكونها تدخل ضمن أنواع المصنفات الأدبية، التي تقتضي حماية من مختلف الجوانب على غرار النسخ، التعديل، الدخول والاستعمال غير المشروع.. وغيرها[1].

وبخصوص مدة الحماية فقد نصت الاتفاقية على أن حماية المؤلفات تمتد إلى خمسين سنة (50)، كحد أدنى، من نهاية السنة التقويمية التي أجيز فيها نشر الأعمال، وفي حالت عدم وجود ترخيص بالنشر فإن الحماية تمتد إلى 50سنة ابتداء من نهاية سنة إنتاج العمل المعني. وفي هذا الجانب أقر المشرع الجزائري بموجب الأمر 03-05، المتعلق بحقوق المؤلف والحقوق المجاورة حماية العمل، إلى مدة 50 سنة من تاريخ نشره أو إنتاجه حسب ما تضمنته الاتفاقية، ولم يشر إلى هذه المدة كحد أدنى[2].

ولقد تضمنت الاتفاقية حماية مدنية للبيانات الشخصية المتعلقة بالملكية الفكرية جراء أعمال المنافسة غير المشروعة، التي تستلزم لقيام الدعوى توفر ثلاث أركان أساسية، بإثبات وجود الخطأ وكذا إلحاق الضرر المادي أو المعنوي، بالإضافة إلى علاقة السببية بين فعل المنافسة غير المشروعة والضرر المعاين[3]. كما أكدت المادة 45 من الاتفاقية على تعويض الضرر المادي جزاء للمسؤولية العقدية أو التقصيرية، وقد نصت على أنه " تمنح للسلطات القضائية صلاحية أن تأمر بدفع تعويضات مناسبة لصاحب الحق مقابل الضرر الذي حدث بسبب التعدي. وللسلطات القضائية صلاحية أن تأمر المدعى عليه بأن يدفع لصاحب الحق المصاريف التي تكبدها والتي يجوز أن تشمل أتعاب المحامي المناسبة، وفي الحالات المناسبة، يجوز للدول الأعضاء تخويل السلطات القضائية

---

[1] وفي هذا الجانب نذكر حكم محكمة ليون الفرنسية الصادر بتاريخ 30 نوفمبر 2000، بخصوص انتهاك موزع Prodiag حقوق المؤلف عند قيامه بنسخ برمجية حاسوب تابعة لشركة مايكروسوفت، على حامل بيانات (Disque Dur) بإدانته ب03 سنوات سجن مع دفع تعويض للشركة بمبلغ 150.000 فرنك فرنسي، أي ما يعادل 20400 دولار آنذاك. لأكثر تفصيل راجع: عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص554.

[2] راجع المادة 58 من الأمر 03-05، المتعلق بحقوق المؤلف والحقوق المجاورة، المرجع السابق.

[3] أحمد بوراوي، الحماية القانونية لحق المؤلف والحقوق المجاورة في التشريع الجزائري والاتفاقيات الدولية، أطروحة دكتوراه في القانون، كلية الحقوق، جامعة باتنة، 2005، ص137.

صلاحية أن تأمر باسترداد الأرباح و/أو دفع تعويضات مقررة سلفا حتى حين لا يكون التعدي على علم أو كانت هناك أسباب معقولة تجعله يعلم أنه قام بذلك التعدي".

وفي الإطار ذاته تم إقرار تعويض للمدعى عليه بسبب الضرر الذي لحق به، مع دفع أتعاب المحامي المحتملة كذلك، كما يمكن للسلطات القضائية أن تأمر المدعي بدفع تعويض المصروفات التي تكبدها المدعى عليه[1].

كما كرست الاتفاقية حماية جزائية بتجريم كل تقليد للمصنفات الرقمية أو انتحال حقوق المؤلف على نطاق تجاري، حيث أكدت المادة 61 من الاتفاقية على ضرورة فرض جزاءات تشمل الحبس وفرض غرامات مالية بما يكفي لتوفير رادع يتناسب مع مستوى العقوبات المطبقة فيما يتعلق بالجرائم ذات الخطورة المماثلة.

وتشمل جريمة التقليد الكشف غير المشروع عن المصنف وكل تحويل، تعديل أو حذف أو إدراج بيانات ضمن مصنف بدون الحصول على موافقة صاحبه[2]. هذا بالإضافة إلى كل أنواع المساس بسلامة المصنف سواء بإتلاف تعليمات البرامج، أو إتلاف البيانات والمعلومات والتي لها أضرارا تفوق تلك الناتجة عن إتلاف المعدات المادية المتعلق بنظم المعلومات[3]. وكذا استنساخ المصنف في شكل نسخ مقلدة، وهذا السلوك الأخير يعد من أخطر عمليات التقليد واسعة الانتشار لسهولته وقلة تكاليفه، لاسيما إذا تعلق ببرامج الحاسوب[4].

ومن جانب آخر فإن الاتفاقية تضمنت إجراءات فعالة لحماية المصنفات، لاسيما الرقمية منها، وذلك بفرض تدابير تقوم بها الدول الأعضاء لمكافحة الجريمة عن طريق القيام بمداهمات وحملات مفاجئة لضبط دلائل إثبات ارتكاب الجريمة، وفي حالة عزوف

---

[1] راجع المادة 48 من اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، المرجع السابق.

[2] فاطمة مصفح، دور محاربة التقليد في حماية برامج الحاسوب في التشريع الجزائري، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة، المجلد الأول، العدد12، سنة 2017، ص544.

[3] سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، المرجع السابق، ص352.

[4] هاجر كرماش، سلامي ميلود، حماية المصنفات الرقمية في ظل اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية "تربس"، المرجع السابق، ص1339.

الدولة العضو عن القيام باتخاذ مختلف التدابير التي تتضمنها الاتفاقية، فإن المنظمة العالمية للملكية الفكرية تعلن قصور هذه الدولة في مجال تطبيق الشروط المنصوص عليها في الاتفاقية، مما يجعلها عرضة لاتخاذ إجراءات عقابية من باقي الدول الأعضاء[1].

وبالرغم من الإضافات التي تضمنتها اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، لاسيما بإدراج المصنفات والبرامج الرقمية ضمن أنماط الملكية الفكرية المعنية بالحماية إلى جانب المصنفات الأدبية والفنية، إلا أنه بتأثير التطور التكنولوجي وما يشكله من تأثير على حقوق المؤلف، فإن المنظمة العالمية للملكية الفكرية تبنت معاهدة سنة 1996 تخص حقوق المؤلف، وهو ما سيتم التفصيل فيه في الفرع الموالي.

ثالثا: معاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف لسنة 1996.

تعد هذه المعاهدة تكريسا لمضامين معاهدة برن، لاسيما نص المادة 20 منها والتي أعطت الحق للدول الأعضاء في إمكانية التوقيع على اتفاقيات خاصة، لضمان أكبر حماية للمؤلف، بحيث شمل مجال هذه المعاهدة مختلف المصنفات المادية والرقمية المتداولة عبر شبكة الإنترنت، بالإضافة إلى ضبط كيفيات معالجة وتخزين مختلف المعلومات التي تتضمنها مختلف المصنفات الرقمية[2].

ومن الجدير بالذكر أن نص المادة الرابعة من المعاهدة أكد على أن برامج الحاسوب تدخل من ضمن المصنفات الأدبية والفنية في مفهوم المادة الثانية من معاهدة برن، مع التأكيد على أن تطبق الحماية على برامج الحاسب مهما كانت طريقة التعبير أو شكلها[3].

ولقد أكد نص المادة الثامنة من هذه المعاهدة على حق المؤلف في النشر الرقمي لمصنفه، حيث تضمنت " يتمتع مؤلفو المصنفات الأدبية والفنية بالحق الاستئثاري في

[1] فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاقات، المرجع السابق، ص186.

[2] فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الإنترنت، المرجع السابق، ص188.

[3] راجع المادة 04 من معاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف، موقع المنظمة العالمية للملكية الفكرية، تاريخ الاطلاع 2021/02/12، "https://wipolex.wipo.int/ar/text/295156 "

التصريح بنقل مصنفاتهم إلى الجمهور بأي طريقة سلكية أو لاسلكية بما في ذلك إتاحة مصنفاتهم للجمهور بحيث يكون في استطاعة أي شخص من الجمهور الاطلاع على تلك المصنفات في أي مكان وفي أي وقت يختارهما أي فرد من الجمهور نفسه، وذلك دون إخلال بأحكام معاهدة برن"[1].

وفي إطار مراعاة حماية البيانات الشخصية المعالجة آليا فإن المعاهدة كرست الحماية لمختلف البيانات المجمعة مهما كان شكلها[2]، مع اعتبارها من ضمن الابتكارات الواجبة الحماية، نظرا للمجهود المبذول في تصنيفها وترتيبها بغض النظر عن المعلومات التي تحتويها، سواء تم تكريس حماية مناسبة لها أم لا[3]. وما نستخلصه من مضمون هذا الإجراء هو تكريس حماية معالجة البيانات الشخصية بمناسبة ترتيب وتجميع مختلف المصنفات، باستعمال تقنيات الحاسوب، وما لهذه الأخير ة من آثار سلبية في تعديل ومحو ومختلف أنواع المعالجة إذا استغلت بصورة سلبية دون مراعاة الضوابط القانونية اللازمة، لاسيما إذا كانت هذه الحواسيب مربوطة بشبكات المعلوماتية، على غرار شبكة الإنترنت.

كما كرست المادة 12 من الاتفاقية التزام مبدأ الشرعية في معالجة البيانات ضمن أي مصنف إلكتروني، وذلك بالنص على التزام الدول الأعضاء أن تنص في قوانينها على جزاءات مناسبة وفعالة توقع ضد أي شخص يباشر، عن علم أو لديه أسباب كافية ليعلم بأن تلك الأعمال تحمل على ارتكاب تعد على أي حق من الحقوق التي تشملها هذه المعاهدة أوتسهل من ذلك أو تبين ذلك أو تخفيه، أيا من الأعمال التالية:"

1- أن يحذف أو يغير، دون إذن، أي معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق.

[1] هاجر كرماش، سلامي ميلود، حماية المصنفات الرقمية في ظل اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية "تربس"، المرجع السابق، ص1332.

[2] راجع المادة 05 من معاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف، المرجع نفسه.

[3] فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الإنترنت، المرجع السابق، ص190.

2- أن يوزع أو يستورد لأغراض التوزيع أو يذيع أو ينقل إلى الجمهور، دون إذن، مصنفات أو نسخا عن مصنفات مع علمه بأنه قد حذفت منها أو غير ت فيها، دون إذن، معلومات واردة في شكل إلكتروني تكون ضرورية لإدارة الحقوق"[1].

هذا، كما أحالت المعاهدة في كثير من الأحكام، لاسيما تلك المتعلقة بمجالات الحماية والتطبيق الزمني، على معاهدة برن، كونها أساس ومنطلق هذه المعاهدة. مع النص على تشكيل جمعية تحت إشراف الويبو[2]، من شأنها متابعة مدى تنفيذ هذه المعاهدة. هذا في ظل لجوء العديد من أصحاب الحقوق إلى ابتداع طرق تقنية خاصة لحماية مصنفاتهم الرقمية من الاعتداءات المتزايدة بتأثير تقنية المعلومات لسد النقص الذي عجزت عن سده القوانين الوطنية في هذا الجانب[3].

ومن وجهة نظرنا فإن تكريس حماية حق المؤلف يشكل نواة وحلقة رئيسة في حماية مختلف البيانات الشخصية نظرا لحساسية هذا الحق بالنظر لما يشتمل عليه بيانات ذات طابع شخصي تشمل مجالات متعددة.

المطلب الثاني: دور المنظمات العالمية في حماية البيانات الشخصية

لقد ساهمت العديد من المنظمات العالمية في إرساء العديد من المبادئ المكرسة لحماية الخصوصية بصفة عامة والبيانات الشخصية بصفة خاصة، والتي بفضل جهودها تم إبرام العديد من الاتفاقيات أسهمت في إبراز دور القانون الدولي الاتفاقي في حماية البيانات الشخصية، وسيتم التطرق لدور كل من منظمة الأمم المتحدة (الفرع الأول)، ومنظمة التعاون الاقتصادي والتنمية (الفرع الثاني).

الفرع الأول: دور منظمة الأمم المتحدة في حماية البيانات الشخصية

لقد برز دور منظمة الأمم المتحدة في الاهتمام بحماية الخصوصية بصفة عامة منذ أوائل نشأتها ولا أدل على ذلك من مضمون الإعلان العالمي لحقوق الإنسان الذي تم

[1] راجع المادة 12 من معاهدة المنظمة العالمية للملكية الفكرية بشأن حقوق المؤلف، المرجع السابق.

[2] "WIPO": المنظمة العالمية للملكية الفكرية (World Intellectual Property Organization).

[3] فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الإنترنت، المرجع السابق، ص 191.

إقراره من قبل الجمعية العامة للأمم المتحدة سنة 1948 حيث اهتم بحماية الخصوصية المعلوماتية لجملة من البيانات لاسيما ما تضمنته المادة 12 منه[1]. وكذا ما تضمنه العهد الدولي للحقوق المدنية والسياسية لسنة 1966، لاسيما مضمون مادته السابعة عشر والتي كرست حماية الخصوصية وسرية المراسلات [2].

كما تبنت توصيات المؤتمر الدولي الأول لحقوق الإنسان والتقدم العلمي والتكنولوجي بطهران سنة 1986، والتي خلصت إلى بيان خطر استعمال الحواسب الآلية على الحريات الفردية والحياة الخاصة، حيث اعتبرت من أدوات التطفل، لاسيما إذا استعملت لمعالجة وتحليل البيانات الشخصية المخزنة ضمن قواعد بياناتها[3].

أما الاهتمام المباشر بحماية البيانات الشخصية فلم يبرز إلا خلال سنة 1990 بموجب قرار الجمعية العامة للأمم المتحدة رقم 45/95 لسنة 1990 والذي من خلاله تبنت جملة من المبادئ التوجيهية لتنظيم البيانات الشخصية المعالجة والمجموعة باستعمال الحاسب الالكتروني، وقد أكد هذا القرار على ضرورة قيام الدول الأعضاء ببسط رقابة داخلية مع إقرار عقوبات جزائية، ضمن القوانين الداخلية للدول المعنية، للمخالفين لمختلف المبادئ التي يتضمنها والتي تعد واجبة الالتزام من قبل الدول المعنية وتشمل هذه المبادئ ما يلي[4]:

---

[1] حسب القرار رقم 217 المؤرخ في 10 ديسمبر 1948، المتضمن الإعلان العالمي لحقوق الإنسان والذي جاء نص مادته 12 كما يلي: " لا يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"

[2] تضمن نص المادة 17 من العهد الدولي للحقوق المدنية والسياسية لسنة 1966 المصادق عليه بموجب قرار الجمعية العامة للأمم المتحدة رقم 2200 بتاريخ16 ديسمبر 1966 والذي دخل حيز التنفيذ في 23 مارس 1976، ما يلي: "1. لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني، للتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. 2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس".

[3] كمال بوبعاية ومبروك لمشونشي، الحماية القانونية الدولية للمعطيات الشخصية في البيئة الرقمية، مجلة الدراسات القانونية والسياسية،، المجلد07، العدد01، يناير 2021، ص75.

[4] منى الأشقر جبور، محمود جبور، المرجع نفسه، ص53.

- **مبدأ الأمن**: حيث يتضمن إلزام القائمين بجمع وحفظ البيانات بالالتزام بواجب التحفظ مع بذل العناية للحفاظ على هذه البيانات لعدم تلفها أو تسربها أو الاطلاع عليها دون إذن مسبق.
- **مبدأ صحة البيانات**: والذي يقتضي تحري دقة البيانات وملاءمتها حسب موضوع المعالجة والدافع لقيام المعالج بالاطلاع عليها مع تحمل مسؤولياته.
- **مبدأ عدم التمييز**: يشمل حظر التمييز العنصري بأي شكل من الأشكال عند معالجة البيانات الشخصية سواء بسبب اللون، العرق، المعتقدات، الآراء السياسية وغيرها.
- **مبدأ المشروعية والنزاهة**: نص هذا المبدأ على منع جمع ومعالجة البيانات الشخصية بطرق غير شرعية وغير نزيهة تعكس عدم الانسجام مع مضمون مقاصد ميثاق الأمم المتحدة.
- **مبدأ وصول الأشخاص المعنيين بالبيانات لملفاتهم:** يتضمن حق الاطلاع للأشخاص على بياناتهم وما يتعلق بها من مساس سواء عند المعالجة أو التصحيح أو حتى الإلغاء أو المحو والذي يعد حقا أصيلا يمكن طلبه من قبل الشخص المعني بالمعالجة.
- **مبدأ تحديد وضبط الغاية من الجمع والمعالجة:** يعد الحفاظ على بيانات الأشخاص من أدق متطلبات الخصوصية، وبالتاليمن اللازم توضيح وا ٍعلان أسباب ودوافع المعالجة مسبقا وضبط رقابتها لاحقا للتأكد من تطابق الغاية مع موضوع المعالجة، وضبط مختلف الآليات الاحتياطية للتأكد من محو أو تدمير مختلف البيانات مباشرة بعد تحقيق الغاية المحددة.

للإشارة فإن الأمم المتحدة تبنت دليلا خاصا باستخدام الكومبيوتر في سير عملية تدفق البيانات الشخصية سنة1989، وبتاريخ 14 ديسمبر 1990 تبنت الهيئة العامة قراراً يشمل تنظيم المعالجة الآلية للمعطيات الشخصية[1].

[1] مروة زين العابدين صالح، المرجع السابق، ص303.

كما خلص المؤتمر العاشر المنعقد ببودابست سنة 2000، إلى وجوب العمل من قبل كل الأطراف لمكافحة جرائم تقنية المعلومات المتزايدة، مع العمل على فرض إجراءات وتدابير وقائية وردعية للحد من عملية القرصنة لمختلف البيانات[1].

وخلال المؤتمر الثاني عشر للأمم المتحدة المنعقد بالبرازيل سنة 2010، الخاص بموضوع منع الجريمة وتحقيق العدالة الجنائية، ناقش ممثلو الدول الأعضاء أثر التطور التكنولوجي على ارتفاع الجرائم الالكترونية، لاسيما تلك التي تخص المعلوماتية وما لها من آثار سلبية على مختلف البيانات المعالجة، والتي استغرقت جانبا كبيرا من النقاش[2].

الفرع الثاني: دور منظمة التعاون الاقتصادي والتنمية

يبرز دور منظمة التعاون الاقتصادي والتنمية من خلال ما تضمنته القواعد الإرشادية المكرسة لحماية الخصوصية وضمان نقل البيانات ذات الطابع الشخصي عبر الحدود والتي انطلقت المنظمة في إعدادها منذ سنة 1978[3]، حيث قام فريق من الخبراء من مختلف الدول الأعضاء بإعداد العديد من المسودات موضوع القواعد الإرشادية وتم مناقشة العديد من التقارير التي تحتوي جملة من التحليلات المقارنة للتشريعات المتعلقة بحماية الخصوصية، لاسيما في المجالات التالية[4]:

- موضوع البيانات الحساسة وما يجب أن تتضمنه المبادئ التوجيهية بأن تكون ذات طبيعة عامة ينبغي تنظيمها للتعامل مع أنواع مختلفة من البيانات أو الأنشطة في الواقع.

---

[1] كمال بوبعاية ومبروك لمشونشي، الحماية القانونية الدولية للمعطيات الشخصية في البيئة الرقمية، المرجع السابق، ص75.

[2] أنيس العذار، مكافحة الجريمة الإلكترونية، ص 739.

[3] مروة زين العابدين صالح، المرجع السابق، ص 297.

[4] OECD Guideline sonthe protection of privacy and transborder flows of personal data (1980) updated in 2013, See the link below,

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Viewed date: October 14, 2021 at 10:00.)

- قضية الأشخاص الاعتباريين مقارنة بالأشخاص الطبيعيين، حيث أّن هناك اختلاف بحسب كل تشريع داخلي تجاه حماية بعض القوانين الوطنية للشخص الاعتباري في مجال معالجة المعطيات، بالموازاة فإن العديد من التشريعات تقتصر على حماية بيانات الأشخاص الطبيعية فقط.
- آليات الرقابة وتوقيع الجزاءات: بحيث تختلف مناهج آليات الرقابة اختلافاكبير ا فالبعض يلجأ إلى سلطات الضبط الإداري وتوقيع جزاءات تأديبية بينما يتم اللجوء إلى المحاكم المتخصصة في العديد من التشريعات، مما يتطلب تدقيق المبادئ التوجيهية حسب الآلية الأنجع أو المزج بين الآليتين.
- موضوع تأمين وحفظ البيانات بعد المعالجة بتحديد المدة الزمنية للاحتفاظ بالبيانات، أو متطلبات محوها، وينطبق الشيء نفسه على متطلبات أن تكون البيانات ذات صلة بأغراض محددة. وعلى وجه الخصوص، من الصعب رسم خط فاصل واضح بين مستوى المبادئ أو الأهداف الأساسية ومسائل "الآلية" ذات المستوى الأدنى والتي ينبغي تركها للتنفيذ المحلي.
- كما تم مناقشة أهم نقطة وهي كيفية تكريس فعالية هذه القواعد بالرغم من أنها توجيهية فقط وغير ملزمة، إلا إذا ما قوبلت بموافقة التشريعات الداخلية للدول وسن قوانين تستلهم من هذه القواعد ما يضمن حماية المعطيات الداخلية وكذا تدفقها خارج إقليم الدول مع الاحتكام إلى القانون الدولي المناسب في هذا الجانب.

وبعد ضبط مسودة هذه التوجيهات نهاية سنة 1979، ضبط مجلس المنظمة سنة 1980 نطاق هذه الإرشادات وتم تبنيها بمصادقة العديد من الدول الكبرى على غرار الولايات المتحدة الأمريكية، ألمانيا، بلجيكا، بريطانيا، اليابان، سويسرا، كند والنمسا.

وقد تم تحديد نطاق هذه المبادئ الإرشادية وتأثيراتها على حماية البيانات الشخصية في القطاعين العام أو الخاص بحيث أنها لا تخص البيانات التي لا تشكل معالجتها خطر ا على الخصوصية والحريات الفردية، وكذا عدم تفسير أهداف هذه المبادئ على أنها تجر إلى منع:

أ- تطبيق تدابير وقائية مختلفة على فئات مختلفة من البيانات الشخصية حسب طبيعتها والسياق الذي يتم فيه جمعها أو تخزينها أو معالجتها أو نشرها.

ب- استبعاد البيانات الشخصية من تطبيق المبادئ التوجيهية التي من الواضح أنها لا تحتوي على أي خطر على الخصوصية الفردية.

ت- تطبيق الإرشادات فقط على المعالجة التلقائية للبيانات الشخصية.

ث- الحاجة إلى تدفقات مستمرة ومتواصلة بشكل عام للمعلومات بين البلدان، وكذا المصالح المشروعة للدول في منع نقل البيانات التي تشكل خطورة على أمنها أو تتعارض مع قوانينها المتعلقة بالنظام العام والآداب العامة أو التي تنتهك حقوق مواطنيها.

ج- القيمة الاقتصادية للمعلومات وأهمية حماية "تجارة البيانات" بقواعد مقبولة للمنافسة العادلة، مع الحاجة إلى ضمانات أمنية لتقليل انتهاكات بيانات الملكية وإساءة استخدام المعلومات الشخصية[1].

وعليه تم ضبط نطاق هذه الإرشادات على أنها معايير دنيا يمكن استكمالها بتدابير إضافية لحماية الخصوصية والحريات الفردية حسب نطاق كل دولة.

وتضمنت هذه المبادئ جملة من القواعد الإرشادية منها ما يخص القوانين الداخلية للدول ومنها الالتزامات الدولية للدول الأعضاء والتي تم تلخيصها بحسب القواعد الإرشادية كما يلي[2]:

1- مبدأ تقييد جمع ومعالجة البيانات: وذلك بتضمين جملة من الضوابط على جمع، معالجة، تخزين أو محو البيانات الشخصية، كما يتطلب الرجوع إلى رأي

[1] OECD Guideline sonthe protection of privacy and transborder flows of personal data (1980) updated in 2013, See the link below,

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Viewed date: October 14, 2021 at 10:00.)

[2] OECD Guideline sonthe protection of privacy and transborder flows of personal data (1980) updated in 2013, Op.cit.

صاحب البيانات قبل معالجتها أو حتى الحصول على أي منها إلا باحترام الإجراءات القانونية المحددة مسبقا، وعند الاقتضاء، بمعرفة أو موافقة صاحب البيانات.

2- **مبدأ تطابق هدف المعالجة مع طبيعة البيانات**: حيث يستلزم أن تكون البيانات الشخصية ذات صلة بالأغراض التي سيتم استخدامها من أجلها، ويجب أن تكون دقيقة وكاملة ومحدثة بالقدر اللازم لتلك الأغراض.

3- **مبدأ المشاركة الفردية**: بحيث يتاح للمعني بالبيانات كل الحق في الحصول على المعلومات المطلوبة لتأكيد مدى ارتباط البيانات المعالجة بشخصه، مع إمكانية الاعتراض عن معالجتها في حالة عدم موافقته أو طلبه التحفظ عليها أو محوها أو تعديلها، كما يمكنه مساءلة الهيئة أو الشخص المناط بمراقبة هذه البيانات.

4- **مبدأ تقييد التصرف في البيانات الشخصية**: يستوجب عدم الكشف عن البيانات الشخصية أو إتاحتها أو استخدامها بطريقة أخرى لأغراض أخرى غير تلك التي من أجلها يتم جمع البيانات الشخصية في موعد لا يتجاوز وقت جمع البيانات، والاستخدام اللاحق يقتصر على تحقيق تلك الأغراض أو غيرها من الأغراض، شريطة موافقة صاحب البيانات أو الهيئة المخولة قانونا لذات الغرض.

5- **مبدأ تأمين البيانات وفق ضمانات محددة**: يجب حماية البيانات الشخصية بضمانات أمنية معقولة ضد مختلف مخاطر مثل فقدان البيانات أو الوصول غير المصرح به أو إتلافها أو استخدامها أو تعديلها أو الكشف عنها.

أما بخصوص القواعد الدولية الإرشادية في نطاق التشريعات الداخلية للدول فهي تشتمل على:

- التزام الدول الأعضاء بالآثار المترتبة عن المعالجة الملغية وا عادة تبادل البيانات الشخصية فيما بينها.
- التزام الدول الأعضاء باتخاذ جميع الخطوات المعقولة والمناسبة لضمان أن تكون تدفقات البيانات الشخصية عبر الحدود غير متقطعة وآمنة.
- يجب على الدولة العضو الامتناع عن تقييد تدفقات البيانات الشخصية عبر الحدود بينها وبين دولة أخرى عضو في المنظمة، إلا إذا كانت هذه الأخيرة لا تلتزم بشكل

كبير بهذه المبادئ التوجيهية أو إذا كانت إعادة تصدير هذه البيانات من شأنها أن تتحايل على تشريعات الخصوصية المحلية الخاصة بها.

- إمكانية سن قيود وشروط من قبل أي دولة عضو أن تفرض دولة لها عضوية قيوداً فيما يتعلق بفئات معينة من البيانات الشخصية، التي تتضمن تشريعات الخصوصية المحلية الخاصة بها تنظيما خاصا نظراً لطبيعة تلك البيانات والتي لا توفر الدولة العضو الأخرى حماية مكافئة لها.
- يجب على الدول الأعضاء تجنب تضمين القوانين والسياسات والممارسات لمنع تدفقات البيانات، باسم حماية الخصوصية والحريات الفردية، والتي من شأنها أن تخلق عقبات أمام تدفقات البيانات الشخصية عبر الحدود التي تتجاوز متطلبات هذه الحماية[1].

ومن خلال استقراء مضامين هذه القواعد الإرشادية نستخلص مدى دقتها وتكريسها لحماية البيانات الشخصية، نظرا لاشتمالها على مضامين ارتكزت عليها مختلف التشريعات الدولية والوطنية المكرسة لحماية البيانات الشخصية، كما سيتم الوقوف عليه، ضمن المحاور الموالية.

المبحث الثاني: الحماية الدولية الإقليمية للبيانات الشخصية

على غرار الحماية المكرسة على المستوى الدولي من خلال اهتمام العديد من المنظمات الدولية بمجال حماية البيانات الشخصية، فإن دور المنظمات الإقليمية ظهر بارزا، لاسيما على المستوى الأوروبي، نظرا للسبق على مستوى المنظمات الأوروبية وكذا العديد من دول الاتحاد الأوروبي في إعطاء العناية والأهمية اللازمة لحماية الخصوصية والبيانات الشخصية وتكريس الآليات الإقليمية الكفيلة بتجسيد ومراقبة مدى الالتزام بالمبادئ الاتفاقية المكرسة لحماية هذه البيانات.

[1] OECD Guideline sonthe protection of privacy and transborder flows of personal data (1980) updated in 2013, Op.cit.

وتجدر الإشارة إلى الدور البارز على مستوى سن الاتفاقيات والمعاهدات الإقليمية المكرسة لحماية البيانات الشخصية بصفة مباشرة أو غير مباشرة وهو ما تم تجسيده من بدءا بالاتفاقية الأوروبية لحقوق الإنسان لسنة 1950، إلى غاية اعتماد النظام العام الأوروبي لحماية البيانات الشخصية لسنة 2016، وعلى المستوى العربي بتكريس الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ثم على المستوى الإفريقي بإصدار اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، هذا من جهة، ومن جهة ثانية كان الدور البارز لبعض المنظمات الإقليمية في تكريس حماية المعطيات الشخصية والتي سيتم التطرق إليها في المطلب الثاني من هذا المبحث بإبراز دور كل من مجلس أوروبا وكذا الاتحاد الإفريقي وكذا جامعة الدول العربية في هذا المجال.

المطلب الأول: الاتفاقيات والمعاهدات الإقليمية المكرسة لحماية البيانات الشخصية

لقد اهتمت العديد من المنظمات الإقليمية بمجال حماية البيانات الشخصية، مما دفعها إلى إبرام العديد من الاتفاقيات الإقليمية، المكرسة لحماية الخصوصية والبيانات الشخصية، ولقد كانت اتفاقيات الاتحاد الأوروبي من أبرز الصكوك الدولية المكرسة لحماية البيانات الشخصية منذ منتصف القرن العشرين، حيث تم إبرام الاتفاقية الأوروبية لحقوق الإنسان سنة 1950 والنظام الأوروبي لحماية البيانات لسنة 2016 (الفرع الأول)، كما كان للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، واتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي دور بارز في حماية البيانات الشخصية (الفرع الثاني).

الفرع الأول: الاتفاقيات والمعاهدات الأوروبية المكرسة لحماية البيانات الشخصية

من خلال ما تضمنته مختلف المراجع التي تم الاستناد عليها في هذا الموضوع تم تمييز جملة من الاتفاقيات الأوروبية التي كان لها دور في تكريس حماية البيانات الشخصية بدءً بالجانب العام لتكريس الحق في الحياة الخاصة بموجب ما تضمنته الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950، وكذا اتفاقية مجلس أوروبا رقم1981/108 لحماية الأشخاص إزاء المعالجة الآلية للبيانات الشخصية ثم النظام

الأوروبي لحماية البيانات الشخصية رقم 2016/679، والتي سيتم التفصيل في كل منها على النحو التالي:

أولا: الاتفاقية الأوروبية لحقوق الإنسان لسنة 1950

بدأ تحضير الاتفاقية الأوروبية لحقوق الإنسان من قبل مجموعة من الدول الأعضاء في مجلس أوروبا سنة 1949، وتم إبرام الاتفاقية في 04 نوفمبر 1950، ودخلت حيز التنفيذ بتاريخ 03 سبتمبر 1953 وذلك بعد تصديق 10 دول عليها[1]. كما تم التوقيع عليها من جميع الدول الأعضاء في الإتحاد الأوروبي[2].

كرست الاتفاقية الأوروبية لحقوق الإنسان ثلاثة أجهزة لمتابعة وضمان تنفيذ بنودها في مجال حماية الحقوق والحريات[3]، وتتمثل في كل من اللجنة الأوروبية لحقوق الإنسان، المحكمة الأوروبية لحقوق الإنسان ولجنة الوزراء بمجلس أوروبا.

ولقد نصت الاتفاقية في مادتها الأولى على التزام الدول الأعضاء باحترام الحقوق والحريات الخاصة بكل شخص، لاسيما السياسية منها، كالحق في حماية الخصوصية اتجاه معالجة البيانات الشخصية.

كما أكد نص المادة الثامنة من هذه الاتفاقية على حماية الحياة الخاصة، وبالتحديد النص على حماية الحياة الشخصية للفرد ومنزله ومراسلاته من أي تدخل أو اعتداء، مع ضبط مجموعة من القيود تكرس هذه الحماية. كما كرست المادة العاشرة من ذات

---

[1] ويس نوال، آليات حماية حقوق الإنسان في إطار مجلس أوروبا، مجلة الدراسات الحقوقية، جامعة سعيدة، العدد الثامن، ص 224.

[2] مروة زين العابدين صالح، المرجع السابق، ص140.

[3] الاتفاقية الأوروبية لحقوق الإنسان، في كتاب : حقوق الإنسان، مجموعة وثائق أوروبية، ترجمة الدكتور محمد أمين الميداني، والدكتور نزيه كسيبي، الطبعة الثانية، منشورات المعهد العربي لحقوق الإنسان، 2001، من ص 35 إلى ص 102.

الاتفاقية تكريس حماية حق الوصول إلى المعلومات من خلال فرض بعض الشروط والقيود على حرية التعبير المطلقة[1].

وعليه فإن هذه الضمانات تعد من بين أوجه الحماية غير المباشرة لخصوصية البيانات الشخصية، والتي تطورت شيئا فشيئا بتأثير استعمال الإنترنت بعد سنة 1969، حيث اتجهت العديد من التشريعات إلى ضبط نصوص مباشرة تكرس حماية البيانات الشخصية خلال المعالجة الآلية لهذه البيانات، وهو ما دفع لجنة وزراء مجلس أوروبا إلى اعتماد اتفاقية تخص حماية الأفراد في مجال المعالجة الآلية للبيانات الشخصية، والتي سيتم التفصيل فيها في العنصر الموالي.

ثانيا: الاتفاقية الأوروبية لحماية الأشخاص اثر المعالجة الآلية للبيانات ذات الطابع الشخصي.

تعد الاتفاقية الأوروبية رقم 108 لسنة 1981، المتعلقة بحماية الأشخاص تجاه معالجة البيانات ذات الطابع الشخصي من جملة المواثيق الدولية الاتفاقية المكرسة لحماية البيانات الشخصية على المستوى الأوروبي، والتي دخلت حيز التنفيذ بتاريخ 01 أكتوبر 1985 بعد التوقيع عليها من حوالي 31 دولة،إلا أنه لم يصادق منها سوى 21 دولة إلى غاية تاريخ 31 يناير 2000[2].

وتجدر الإشارة إلى أن الاتفاقية تضمنت أحكاما وتفاصيل تخص معالجة البيانات الشخصية باستخدام تقنية الحاسوب، وما لهذه الأخيرة من انعكاسات حول وضعية البيانات المخزنة، مع التأثير في طبيعتها من حيث التعديل، الإزالة وسرعة النشر وكذا إمكانية تعريضها للمعالجة غير المشروعة.

[1] انظر المادتين 08 و10 من الاتفاقية الأوروبية لحقوق الإنسان، مشتملة على أحدث التعديلات والبروتوكالات الملحقة، متاحة على الربط أدناه، بتاريخ 2021/02/22:
https://www.echr.coe.int/documents/convention_ara.pdf

[2] مروة زين العابدين صالح، المرجع السابق، ص301.

كما تضمنت الاتفاقية تعريفا واسعا للبيانات الشخصية، يشمل أي معلومة تخص شخصا معرفا أو قابلا للتعريف[1].

ثالثا: التوجيه الأوروبي 46/95 المتعلق بحماية الأشخاص فيما يتعلق بمعالجة البيانات وحرية انتقالها.

تضمن التوجيه الأوروبي لسنة 1995 جملة من المبادئ الأساسية والقواعد الإرشادية واجبة الالتزام من قبل الدول الأعضاء وكذا القائم بمعالجة البيانات الشخصية، وقد تضمنت هذه المبادئ جملة من الشروط الواجب توفرها في البيانات، وتشمل:

- أن يتم معالجتها بشكل شرعي وعادل.
- أن تكون المعالجة مناسبة وغير مبالغ فيها.
- أن يتم تحديد الأغراض الواضحة من عملية المعالجة
- أن تكون المعالجة كاملة ودقيقة.
- أن يتم نقل البيانات المعالجة إلى الدول التي تكرس الحماية المناسبة للبيانات الشخصية.
- أن يتم معالجتها بناء على حقوق صاحب البيانات.
- أن تكون محفوظة ومؤمنة[2].

وقد تم إلزام الدول الأعضاء بتحيين قوانينها الوطنية المتعلقة بحماية البيانات الشخصية وتضمينها هذه القواعد الإرشادية.

ثالثا:النظام الأوروبي العام لحماية البيانات 2016/679.

دخل النظام الأوروبي العام لحماية البيانات، رقم 2016/679 المؤرخ في 27 ابريل 2016، حيز التنفيذ في 25 مايو 2018 وهو يعد المرجع في مجال حماية البيانات الشخصية، نظرا لكونه أدرج قواعد جديدة وخلق تغييرات كبيرة في المنظومة القانونية

[1] راجع المادة 02 من الاتفاقية الأوروبية 108 لسنة 1981، المتعلقة بحماية الأشخاص تجاه معالجة البيانات ذات الطابع الشخصي، متاحة على الربط "https://rm.coe.int/1680078b37 ".

[2] مروة زين العابدين صالح، المرجع السابق، ص141.

الخاصة بحماية البيانات الشخصية، بإرساء نظام صارم يراعي حماية الحياة الخاصة في ظل تحديات تقنيات المعلومات في العالم الرقمي[1].

تم إعداد النظام والمصادقة عليه من قبل البرلمان الأوروبي وجاءت الأهداف محددة ضمن نص المادة الأولى[2] وهي :

1- وضع القواعد المتعلقة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية والقواعد المتعلقة بحرية البيانات الشخصية.

2- حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين وخاصة حقهم في حماية البيانات الشخصية.

3- حظر تقييد حرية نقل البيانات الشخصية داخل الاتحاد الأوربي أو حظرها لأسباب تتعلق بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية.

وقد تضمنت هذه اللائحة شروطا واجبة الاحترام من قبل المكلف بمعالجة البيانات الشخصية على مستوى الاتحاد الأوربي وداخل كل دولة عضو، حددها نص المادة 28 على النحو التالي:

1. يجب استخدام المعالجات التي توفر الحماية والضمانات الكافية لتنفيذ مختلف الإجراءات التنظيمية بطريقة تجعل هذه المعالجة تكفل حقوق صاحب البيانات طبقا لما تضمنه اللائحة من شروط وا ٍجراءات.

2. ضرورة حصول المعالج على إذن كتابي مسبق أو عام لإشراك معالج آخر، ويجب على المعالج إبلاغ المراقب بأي تغيرات تتعلق بإضافة أو استبدال المعالجات، ويمكن للمراقب الاعتراض على كل أو بعض التغييرات في البيانات.

3. في حالة إشراك المعالج لشخص آخر للقيام بأنشطة معالجة محددة نيابة عن المراقب، يتم فرض نفس التزامات حماية البيانات المنصوص عليها في العقد، أو أي

[1] منى الأشقر جبور، محمود جبور، المرجع السابق، ص55.

[2] راجع المادة 06 من اللائحة الأوروبية لحماية البيانات، المرجع السابق.

تصرف قانوني آخر بين المراقب والمعالج لاسيما من خلال توفير ضمانات كافية لتنفيذ التدابير التقنية والتنظيمية بطريقة تجعل المعالجة تلبي متطلبات اللائحة، وفي حالة فشل المعالج الآخر في الوفاء بالتزاماته الخاصة بحماية البيانات يجب أن يكون المعالج الرئيسي مسؤولا بشكل كامل عن أداء التزامات ذلك المعالج الآخر.

4. لا يجوز للمعالج أو أي شخص آخر يعمل تحت سلطة المراقب أو المعالج، الذي لديه إمكانية الوصول إلى البيانات الشخصية معالجة هذه البيانات إلا بناءا على تعليمات من المراقب إلا إذا كان ذلك مطلوبا من قبل الاتحاد الأوربي أو قانون الدول الأعضاء[1].

5. إلزامية إخضاع المعالجة بواسطة المعالج إلى عقد أو أي إجراء قانوني آخر، حسب ما حدد في قانون الاتحاد الأوربي أو أي قانون داخلي للدولة العضو، بحيث يحدد ضمنه موضوع ومدة المعالجة، والطبيعة والغرض من المعالجة، نوع البيانات الشخصية والتزامات وحقوق المراقب بحيث يجب على أن يتضمن الإجراء أو العقد البيانات التالية:

5.1 التأكد من أن الأشخاص المرخص لهم بمعالجة البيانات الشخصية قد ألزموا أنفسهم بالسرية في جميع مراحل المعالجة.

5.2 معالجة البيانات وفقا للتعليمات المبلغة من مراقب البيانات بأدلة موثقة، بما فيها نقل البيانات إلى بلد آخر مع ضرورة الالتزام بالنصوص القانونية للدول الأعضاء في الاتحاد.

5.3 مراعاة طبيعة المعالجة، كما يساعد المراقب على اتخاذ التدابير التقنية والتنظيمية المناسبة، بقدر ما يكون ذلك ممكنا، من أجل الوفاء بالتزام المراقب بالرد على طلبات ممارسة حقوق صاحب البيانات.

5.4 اتخاذ التدابير اللازمة لضمان مستوى من الأمن لاسيما:

1- الاسم المستعار وتشفير البيانات الشخصية.

2- القدرة على ضمان السرية المستمرة والنزاهة ومرونة نظم وخدمات المعالجة.

[1] راجع المواد من 26-31 من اللائحة الأوروبية لحماية البيانات الشخصية رقم 2016/679، المرجع السابق.

3- سرعة الوصول إلى البيانات الشخصية في حالة حدوث حادث مادي أو تقني.

4- يساعد المراقب في ضمان الامتثال للالتزامات المحددة مع الأخذ بعين الاعتبار طبيعة المعالجة والمعلومات المتوفرة للمعالجة.

5- إجراء عملية الاختبار والتقييم لفعالية الإجراءات التقنية والتنظيمية لضمان مستوى من الأمن لعملية المعالجة.

6- يخول للمراقب القيام بمهام الرقابة والتفتيش في إطار التأكد من التزام المعالج بالإجراءات القانونية المتعلقة بعملية المعالجة من البداية إلى النهاية.

7- يجب على المعالج إبلاغ وحدة التحكم في حالة تسجيل وجود تعليمات تتعارض وأحكام اللائحة أو أحكام حماية البيانات الأخرى للاتحاد والدول الأعضاء.

وبالنظر لمختلف المضامين المكرسة بموجب النظام العام فإنه يعد أكثر ضمانا لحماية البيانات الشخصية، مقارنة بالقواعد الإرشادية لسنة 1995، السالفة الذكر وذلك لافتقار هذه الأخيرة للإلزام، بينما النظام العام لسنة 2016، يتمتع بقوة القانون، بدون الرجوع إلى إصدار قوانين داخلية لكل دولة لإعطائها القوة التنفيذية، حيث أشار نص المادة 99 منه بأن النظام يسري مفعوله في جميع الدول الأعضاء بعد مدة عشرين (20) يوما من نشره في الجريدة الرسمية للاتحاد الأوروبي[1].

الفرع الثاني: الاتفاقيات والمعاهدات العربية والإفريقية لحماية البيانات الشخصية

سيتم من خلال هذا الفرع التطرق إلى الجوانب الخاصة بتكريس حماية البيانات الشخصية ضمن كل من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، وكذا اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014.

[1] منى الأشقر جبور، محمد جبور، المرجع السابق، ص65-57.

أولا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

تعد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تبنتها جامعة الدول العربية بتاريخ 2010/01/21 أول اتفاقية عربية تعنى بحماية الحق في الخصوصية والبيانات الشخصية، والتي جاءت بنفس منهج اتفاقية **بودابست** العالمية[1]. وهي تمثل " الاتفاق الدولي الإقليمي المبرم بين الدول العربية في نطاق جامعة الدول العربية بصورة خطية في أكثر من وثيقة والذي وافق عليه مجلس وزراء الداخلية والعدل العرب في اجتماعهما المنعقد في مقر الأمانة العامة لجامعة الدول العربية بتاريخ 2010/12/21 م، بالقاهرة"[2].

كما تجدر الإشارة أن التصديق على الاتفاقية على المستوى الوطني لم يتم إلا سنة 2014 بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 08 سبتمبر 2014[3].

وعليه سيتم الوقوف على الأحكام العامة التي تضمنتها الاتفاقية بتوضيح أهدافها ، مختلف المصطلحات المرتبطة بالبيانات الشخصية إلى جانب مجالات تطبيقها، ثم التعريج على الجرائم الماسة بالبيانات الشخصية والتي تضمنتها الاتفاقية.

أ. الأحكام العامة المرتبطة بمجال حماية البيانات الشخصية:

تم الإشارة في ديباجة الاتفاقية وكذا مادتها الأولى إلى أهداف سن هذه الاتفاقية وهى كالتالي:

- تعزيز التعاون فيما بين الدول العربية لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها.
- الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات.

---

[1] الذهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية -دراسة مقارنة-، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد08، المجلد01،سنة 2017، الجزائر، ص151.

[2] أحمد حمي و زهيرة كيسي، صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، المجلد 10، العدد01، ابريل 2019، ص778-779.

[3] راجع المرسوم الرئاسي رقم 14-252، المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010.

ولتحقيق الأهداف المسطرة تم حصر مجالات تطبيق الاتفاقية وتوضيح مصطلحاتها التي تعنى بحماية البيانات الشخصية على النحو التالي:

1. مجالات تطبيق الاتفاقية

حددت المادة الثالثة من الاتفاقية مجالات التطبيق لمختلف جرائم تقنية المعلومات قصد منعها والتحقيق فيها وملاحقة مرتكبيها، في الحالات الأربع الاتية:

1- إذا ارتكبت في أكثر من دولة.

2- إذا ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.

3- إذا ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية تمارس أنشطة في أكثر من دولة.

4- إذا ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى[1].

2. توضيح مصطلحات الاتفاقية المتعلقة بالبيانات الشخصية:

عرفت المادة الثانية من الاتفاقية جملة من المصطلحات، وسيتم عرض المتعلق منها بمجال البيانات الشخصية على النحو التالي:

- **"مزود الخدمة**: أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها". وقد اعتمد العديد من التشريعات العربية الداخلية على وضع شروط وا إجراءات يقوم بها المسؤول عن المعالجة قبل وبعد عملية المعالجة، على غرار ما تضمنه القانون 18-07 من شروط في هذا الجانب[2].

[1] راجع المادة 03 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الملحقة بالمرسوم الرئاسي 14-252، المرجع السابق.

[2] راجع المواد من 38 إلى 41 من القانون 18-07، المرجع السابق. ص20.

- "**البيانات:** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها..." وهناك من التشريعات العربية من اعتمدت المصطلح ذاته والبعض الآخر أوردها بمصطلح المعطيات، وهو ما ذهب إليه المشرع الجزائري ضمن نص المادة 47 من الدستور الجزائري لسنة 2020 "... حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق"[1].
- " **الشبكة المعلوماتية:** ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها".

وعليه فإننا لاحظنا جل المصطلحات المنصوص عليها في مضمون الاتفاقية يمكن أن تعالج أو ترتبط بمجال البيانات الشخصية، مما يؤكد دور هذه الآلية الاتفاقية العربية في حماية البيانات الشخصية إقليميا، في حالة تجسيد مضامينها ضمن القوانين الداخلية لجميع الدول الأعضاء، مما يسهل مكافحة الجرائم المعلوماية العابرة للحدود.

ب. الجرائم المرتبطة بمجال حماية البيانات الشخصية المنصوص عليها في الاتفاقية:

نصت الاتفاقية على جملة من الجرائم المرتبطة بمجال حماية البيانات الشخصية، والمتمثلة في كل من جريمة الدخول غير المشروع، جريمة الاعتراض غير المشروع، جريمة الاعتداء على سلامة البيانات، جريمة الاعتداء على حرمة الحياة الخاصة وجريمة انتهاك حق المؤلف والحقوق المجاورة وسيتم التفصيل في كل منها على النحو التالي:

1. **النص على جريمة الدخول أو البقاء غير المشروع:**

نصت المادة السادسة من الاتفاقية على تجريم الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرارية به، كما تشدد العقوبة في

[1] راجع المرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر 2020، الجريدة الرسمية عدد82، المؤرخة في 30 ديسمبر 2020.

حالة ما أدى هذا الدخول أو البقاء غير المشروع إلى محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة، للأجهزة والأنظمة الالكترونية وشبكات الاتصال وا لحاق الضرر بالمستخدمين والمستفيدين[1].

وفي هذا الإطار يعرف الدخول أو الاتصال غير المشروع ب" الولوج والاتصال بكل أو جزء من نظام أو شبكة تقنية المعلومات دون رضا المسؤول عن النظام"[2]، أو يمثل الدخول إلى البيانات المخزنة داخل تقنية المعلومات بغرض الاطلاع أو التسلية وا شباع الشعور الشخصي بالنجاح في اختراق الحاسب الآلي[3]. وهناك من عرف الدخول بالاستناد إلى البعدين المكاني والزماني، فيقصد به فعل التسلل إلى النظام حسب البعد المكاني، وتجاوز حدود وقت الترخيص بالدخول حسب البعد الزماني[4].

كما يلاحظ أن الاتفاقية في هذا الجانب لم تحدد وسيلة الدخول الموجبة للتجريم وا نما أبقت المجال مفتوحا سواء بالدخول عبر جهاز الحاسوب للمعني أو جهاز آخر بعد الاطلاع أو اختراق كلمة السر أو عن طريق إطلاق فيروسات وغيرها.و هو الأمر الذي ذهب إليه القضاء في فرنسا، حيث تضمن قرار محكمة الاستئناف بباريس الصادر في 05 ابريل 1994، بأن الدخول يشمل جميع أنواع الاختراق غير المشروعة لنظام المعالجة الآلية للبيانات التي يقوم بها مرتكب هذه الجناية على جهاز الحاسوب ولو تم بالاتصال مع نظام آخر عن بعد[5].

[1] راجع المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق، ص05.

[2] محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، جامعة زياني عاشور الجلفة، المجلد الأول، العدد الأول، 2017، ص378.

[3] محمد خليفة، المرجع نفسه، ص379.

[4] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي – الحماية الجنائية للحاسب الآلي-، دراسة مقارنة، رسالة دكتوراه،قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، سنة 2000، ص304.

[5] بطيحي نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، المجلد01، العدد01، جوان 2019، ص78.

وتجدر الإشارة أن قانون العقوبات الجزائري نص على هذه الجريمة منذ التعديل الحاصل سنة 2004، بموجب أحكام المادة 394 مكرر المدرجة بموجب القانون 04-15، المؤرخ في 10 نوفمبر 2004[1].

2. النص على جريمة الاعتراض غير المشروع: أوضحت المادة السابعة من الاتفاقية على أن جريمة الاعتراض غير المشروع تتجسد في "الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي وسيلة من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات".

والمشرع الجزائري بدوره أشار ضمنيا إلى جزاءات نتيجة إعاقة أو اعتراض طريق نظام المعلومات بغرض قرصنة المعطيات أو الاتجار فيها، وهذا باستقراء مضمون نص المادة 394 مكرر2 من قانون العقوبات[2].

3. النص على جريمة الاعتداء على سلامة البيانات: حصرت الاتفاقية أساليب الاعتداء على سلامة البيانات في تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق. كما تم اشتراط وقوع ضرر جسيم من أجل تجريم الأفعال المذكورة أعلاه[3].

4. النص على جريمة إساءة استخدام وسائل تقنيات المعلومات: حصرت الاتفاقية جملة من الأفعال بموجبها تستلزم وقوع جريمة إساءة استخدام وسائل تقنيات المعلومات، وتتمثل هذه الأفعال فيما يلي:

1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ- أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة أعلاه، أي جرائم الدخول والبقاء والاعتراض غير المشروع والاعتداء على سلامة البيانات.

---

[1] المشرع الجزائري بدوره بموجب المادة 394 مكرر من قانون العقوبات أكد على أن الدخول يتضمن " كل أو جزء من منظومة للمعالجة الآلية للمعطيات ".

[2] زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2011، ص66.

[3] انظر المادة 08 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

ب-كلمة سر نظام معلومات أو شفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة من نص الإتفاقية.

2- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم الثلاث المذكورة أعلاه.

5. النص على جريمة التزوير: عرفت الاتفاقية جريمة التزوير في مجال تقنية المعلومات ب"استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغيير ا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة"[1].

والركن المادي لجريمة التزوير، حسب مضمون هذه المادة، يشترط تغير الحقيقة، بالتلاعب بالبيانات المخزنة في تقنية المعلومات، وا ٍدخال بيانات غير صحيحة، وأن يقع التزوير في مستند معلوماتي، مع ثبوت تغير الحقيقة بإحدى طرق التزوير وا ٍثبات إلحاق الضرر النسبي[2].

6. النص على جريمة الاحتيال: تعرف جريمة الاحتيال بأنها " استعمال الجاني وسيلة من وسائل التدليس المحدد على سبيل الحصر وحمل المجني عليه بذلك على تسليم الجاني مالا مملوكا للغير"[3]، كما عرفته منظمة التعاون الاقتصادي والتنمية بأنه كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يرتبط بالمعالجة الآلية للمعطيات[4].

---

[1] المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] أحمد حمي و زهيرة كيسي، صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014، المرجع السابق، ص783-784.

[3] أحمد حمي و زهيرة كيسي، صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014، المرجع السابق، ص784.

[4] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الاسكندرية، 2009، ص160.

كما نصت المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن جريمة الاحتيال تتجسد في " التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:

1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

2- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أومحاولة تعطيلها أو تغييرها.

3- تعطيل الأجهزة والبرامج والمواقع الالكترونية".

7. النص على جريمة الاعتداء على حرمة الحياة الخاصة:

نصت الاتفاقية العربية المذكورة أعلاه، في مادتها الرابعة عشر على جريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنيات المعلومات، وهو الأمر الذي ترجمته لاحقا أغلب الدساتير والقوانين العربية في مفهوم جريمة الاعتداء على المعطيات الشخصيةبالإضافة إلى تحيين قوانين العقوبات وا إدراج العقوبات الناجمة عن الاستعمال غير المشروع للتقنية، حيث في هذا الجانب نلاحظ أن المشرع الجزائري ومنذ تعديل قانون العقوبات لسنة 2006، أدرج الجزاءات اللازمة للاعتداء على الحياة الخاصة باستعمال تقنيات المعلومات، كالتقاط الصور أو تسجيل الفيديوهات، أو الاحتفاظ بها أو وضعها في متناول الجمهور بطريقة غير شرعية ودون أخذ الإذن من الشخص المعني، بإقرار عقوبات تتراوح بين ستة أشهر و ثلاث سنوات سجن وبغرامة من 50.000 إلى 300.000دج[1].

كما أقر المشرع الجزائر ي عقوبات بموجب القانون 18-07 ضد انتهاك حرمة الحياة الخاصة بمختلف أنواع الانتهاك سواء بالجمع والتخزين للبيانات الشخصية بدون ترخيص

[1] راجع المواد 303 مكرر، 303 مكرر1 و303 مكرر 02 من قانون العقوبات الجزائري، المرجع السابق، ص128.

أو إفشاء أو استخدام غير مشروع لهذه البيانات وهو ما سيتم توضيحه في الفصل الثاني من هذا المحور.

8. النص علىجريمة انتهاك حق المؤلف و الحقوق المجاورة: نصت المادة 17 من الاتفاقية على تجريم "انتهاك حق المؤلف، كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وتجريم انتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي".

والمشرع الجزائري بموجب نص الأمر 03-05، المتعلق بحماية حقوق المؤلف والحقوق المجاورة[1]، كرس حماية لحق المؤلف، حيث نصت المواد 151 و152 و153 على جنحة التقليد المستلزمة للحبس من 06 أشهر إلى ثلاث سنوات ودفع غرامة تتراوح بين 500.000 و1000.000دج ضد كل من يقوم ب:"

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف .
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة.
- بيع نسخ مقلدة لمصنف أو أداء.
- تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء"[2].
- "كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني أو البث الإذاعي السمعي أو السمعي البصري أو التوزيع بواسطة الكابل أو بأية وسيلة نقل أخرى لإشارات تحمل أصواتاً أو صورا بأي منظومة معالجة معلوماتية"[3].

9. النص على جريمة الاستخدام غير المشروع لأدوات الدفع الالكتروني: نظرا للاعتماد على وسائل الدفع الالكتروني في الكثير من المعاملات التجارية والمالية، على المستوى العالمي بصفة عامة، والعربي بصفة خاصة، فإنه نتج عنها العديد من المخاطر

[1] الأمر 03-05 المؤرخ في 19 جويلية 2003، المتعلق بحق المؤلف والحقوق المجاورة

[2] راجع المادة 151 من الأمر 03-05، المرجع نفسه.

[3] راجع المادة 152 من الأمر 03-05، المرجع نفسه.

المتعلقة ببيانات الأفراد وأموالهم، وهو ما أكدت عليه الاتفاقية العربية بتجريم الاستخدام غير المشروع لوسائل الدفع الالكتروني، حيث تم بموجب المادة 18 من الاتفاقية حصر صور هذه الجريمة في أربع صور من السلوك الإجرامي كما يلي:

1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.

2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهل للغير الحصول عليها.

3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك[1].

ولقد نص قانون العقوبات الجزائري على جريمة التزوير في المحررات العرفية أو التجارية أو المصرفية بموجب أحكام المواد 219، 220 و221، وبالرغم من الجدل القائم حول اعتبار التزوير في المعطيات على مستوى جهاز رقمي أو اعتبار الدفع الالكتروني والنقود الالكترونية محررات، وبعد مصادقة الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية بموجب المرسوم الرئاسي 14-252، السالف الذكر، فإن هناك وجهة نظر تؤيد تكريس اعتبار بطاقة الدفع محرر عرفي إذا كانت الجهة المصدرة لها مصرفا أو بنكا خاصا، ووصف المحرر الرسمي إذا كانت صادرة عن مؤسسة مالية عمومية تابعة للدولة[2].

وعليه من خلال دراسة مختلف مضامين الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، نستنتج الأثر البارز لهذه الاتفاقية في تجريم الكثير من السلوكيات التي من شأنها المساس بالمعطيات الشخصية، كما لاحظنا في كثير من مضامين الاتفاقية قد تناولها المشرع الجزائري بموجب التعديلات التي شملت قانون العقوبات سنتي 2005

[1] انظر المادة 18 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق، ص06.

[2] حوالف عبد الصمد، النظام القانوني لنظام الدفع الالكتروني في الجزائر –دراسة مقارنة-، المرجع السابق، ص690-691.

و2006، إلا أن تحيين بعض النصوص القانونية مع ما يتماشى ومضامين الاتفاقية يبقى ضرورة حتمية من حيث اعتماد نص الاتفاقية منذ سنة 2014، من جهة وكذا ما تفرضه التطورات الحاصلة في مختلف المجالات والاعتماد الكبير على الفضاء الرقمي، مما يتطلب مرونة تشريعية للتكيف مع مختلف هذه التطورات ومقابلة انعكاساتها على المعطيات الشخصية.

ثانيا: اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي

لقد أدى تطور المناخ العام المتعلق بالتكنولوجيات الرقمية وما لها من آثار سلبية أفضت إلى سرعة انتشار الجرائم الإلكترونية، لاسيما مع أواخر تسعينيات القرن الماضي، لدفع بأغلب التشريعات الإقليمية إلى توقيع اتفاقيات للحد من الآثار السلبية للتكنولوجيات الرقمية، والاتحاد الإفريقي كمنظمة إقليمية كان من بين الأهداف الرئيسة لإنشائه، التي تضمنها قانونه التأسيسي، هو اعتماد الرؤية الإفريقية الموحدة، لمختلف القضايا، والتي من بينها تأثير التكنولوجيات الرقمية على الخصوصية المعلوماتية، حيث وضعت بذرة تكريس هذه الاتفاقية خلال مؤتمر الاتحاد الإفريقي للوزراء المسؤولين عن تكنولوجيا الاتصال لسنة 2008 ليليه عدة قرارات واقتراحات، كللت بمشروع أولي للاتفاقية الإفريقية حول الثقة والأمن في الفضاء الرقمي، والتي كانت خلاصة مجهود مشترك بين مفوضية الاتحاد الإفريقي ولجنة الأمم المتحدة الاقتصادية لإفريقيا، والذي طرح للنقاش سنة 2013، ليتم اعتماده من قبل رؤساء الدول والحكومات خلال الدورة العادية الثالثة والعشرين لمؤتمر الاتحاد الإفريقي يومي 26 و27 جوان2014، مع إتاحة المجال للمصادقة على مشروع الاتفاقية[1]. كما تجدر الإشارة إلى أنه وتزامنا مع المصادقة على مشروع الاتفاقية، تم تعديل اسمها على النحو التالي، الوارد في نسخة الاتفاقية المترجمة إلى اللغة العربية، "اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات

[1] مريم لوكال، قراءة في اتفاقية الاتحاد الإفريقي حول المن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، المجلد 04، العدد03، 2021، ص660.

ذات الطابع الشخصي." Convention on cyber security and personal data protection "[1].

وعليه سنتطرق إلى مضامين الاتفاقية مع التركيز على الجانب المتعلق بحماية البيانات الشخصية كما يلي:

أ. المضامين العامة للاتفاقية:

تضمنت الاتفاقية ديباجة حوت مختلف الأسباب التي دفعت إلى اعتماد الاتفاقية، والأهداف المرجوة، كما تضمنت المادة الأولى من الاتفاقية تعريفات لمختلف مصطلحات الاتفاقيةو تم تقسيم محاور الاتفاقية إلى ثلاثة (03) فصول، حيث خصص الفصل الأول لضبط المعاملات الالكترونية، بحيث كرست حرية التجارة الالكترونية مع حث الدول على توفير آليات الحماية ومختلف الضمانات لتجسيد ذلك[2].

أما الفصل الثاني والذي يعني موضوع هذه الدراسة بصفة مباشرة، فقد خصص لبسط آلية حماية البيانات ذات الطابع الشخصي، حيث وضح أهداف الاتفاقية بشأن البيانات

ذات الطابع الشخصي، وضبط مجال الاتفاقية في هذا الجانب، بتحديد الإجراءات الأولية لمعالجة هذه البيانات، والإطار المؤسساتي لحمايتها، بالإضافة إلى التدقيق في حقوق صاحب البيانات والالتزامات المتعلقة بالشروط التي تحكم معالجة البيانات ذات الطابع الشخصي، لاسيما تلك المتعلقة بالبيانات الحساسة[3].

---

[1] اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخص (Convention on cyber security and personal data protection)، متاحة على رابط الموقع الإلكتروني للاتحاد الإفريقي، بتاريخ 2022/02/21، رابط التحميل:

https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_a.pdf.

[2] راجع الفصل الأول من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص11-17.

[3] انظر المادة 14 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص28-30.

كما تناول الفصل الثالث والأخير من الاتفاقية تدابير تعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية، من حيث حث الدول الأعضاء على تأمين الفضاء الإلكتروني الوطني، وتكريس التعاون بين الدول الأعضاء في مجال تبادل المعلومات، ثم اختتام هذا الفصل بتوضيح الآليات الجزائية لمكافحة الجرائم الالكترونية.

ونظرا لاتساع مجال الاتفاقية فإننا سنتطرق للجوانب الخاصة بحماية البيانات ذات الطابع الشخصي من حيث مصطلحات الاتفاقية والتدقيق في آليات الحماية المكرسة.

ب. التعاريف الخاصة بالمصطلحات التي تشمل مجال البيانات ذات الطابع الشخصي: تطرقت المادة الأولى من الاتفاقية إلى وضع تعريفات لمختلف المصطلحات الخاصة بمجال البيانات ذات الطابع الشخصي، على النحو التالي:

- **البيانات المحوسبة:** تعني أي عرض لحقائق أو معلومات أو مفاهيم على شكل ملائم للمعالجة بالحاسوب.
- **موافقة الشخص المعني:** وتعني إظهار رغبة شخصية صريحة وواضحة ومحددة ومدروسة يقبل بموجبها الشخص المعني أو ممثله القانوني أو القضائي بمعالجة بياناته الشخصية يدويا أو إلكترونيا.
- **المسؤول عن معالجة البيانات:** وهو أي شخص طبيعي أو معنوي عام أو خاص أو أي هيئة أو جمعية أخرى تقرر بمفردها أو مع آخرين جمع ومعالجة بيانات ذات طابع شخصي وتحدد أهداف هذه المعالجة.
- **الشخص المعني بالبيانات:** يعني أي شخص طبيعي يكون محل معالجة البيانات ذات الطابع الشخصي.
- **تجاوز النفاذ المسموح به:** يعني النفاذ إلى نظام معلومات واستعمال هذا النفاذ للحصول على معلومات أو تغييرها في جزء من الحاسوب غير مسموح للفرد بالنفاذ إليه.
- **البيانات الصحية:** وتشمل مختلف المعلومات المتصلة بالحالة الجسدية أو العقلية للشخص، بما في ذلك البيانات الوراثية.

- **الربط بين البيانات ذات الطابع الشخصي:** يعني أي آلية ربط متمثلة في الربط بين بيانات تمت معالجتها لبلوغ هدف محدد وبيانات أخرى معالجة لأهداف مشابهة أو غير مشابهة أو مترابطة بواسطة مسؤول أو أكثر عن المعالجة.
- **البيانات ذات الطابع الشخصي:** وتعني أي معلومات متصلة بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو غير مباشر بالإشارة إلى رقم هويته أو إلى عامل واحد أو أكثر محدد لهويته الطبيعية أو السيكولوجية أو الذهنية أو الاقتصادية أو الثقافية أو الاجتماعية[1].
- **ملفات البيانات ذات الطابع الشخصي:** وهي كل مجموعة مهيكلة من البيانات التي يمكن الوصول إليها وفق معايير محددة بغض النظر عما إذا كانت هذه البيانات مركزية أو غير مركزية أو موزعة وظيفيا أو جغرافيا.

- **معالجة البيانات ذات الطابع الشخصي:** وتشمل أي عملية تجرى على بيانات شخصية بمساعدة أو بدون مساعدة طرق آلية مثل جمع وتسجيل وتنظيم وحفظ وتكييف وتعديل واستخلاص وحماية ونسخ واستشارة واستعمال والكشف من خلال الإرسال ونشر أي شكل آخر من أشكال الإتاحة عن طريق المحاذاة أو الربط والقفل، بالإضافة إلى تشفير وحذف وا ٍتلاف بيانات شخصية.

- **المستفيد من معالجة البيانات:** ويعني أي شخص مؤهل لتلقي هذه البيانات غير الشخص المعني، المسؤول عن معالجة البيانات، والمقاول الفرعي والأشخاص المكلفين بسبب وظائفهم بمعالجة البيانات.

- **البيانات الحساسة:** وتعني جميع البيانات ذات الطابع الشخصي المتصلة بالآراء والأنشطة الدينية والفلسفية والسياسية والنقابية، بالإضافة إلى الحياة الجنسية والعرقية والصحية والتدابير الاجتماعية والقضايا والدعاوى القانونية والعقوبات الجزائية أو الإدارية.

[1] هذا التعريف يتطابق مع التعريف الذي وضعه المشرع الجزائري للمعطيات ذات الطابع الشخصي الوارد ضمن القانون 18-07، السالف الذكر.

- **المقاول الفرعي:** يعني أي شخص طبيعي أو معنوي عام أو خاص أو أي منظمة أو جمعية تقوم بمعالجة البيانات بالنيابة عن مسؤول معالجة البيانات[1].

ج. آليات حماية البيانات الشخصية المكرسة بموجب الاتفاقية:

كرست الاتفاقية آليات إجرائية أولية لحماية معالجة البيانات الشخصية، وآليات مؤسساتية لمتابعة عملية معالجة البيانات ثم كرست التزامات القائم بالمعالجة وحقوق الشخص المعني، كما سيتم التفصيل فيها في النقاط الثلاث الموالية:

1- الآليات الإجرائية الأولية لمعالجة البيانات الشخصية: كرست الاتفاقية جملة من الآليات الإجرائية الأولية قبل وأثناء القيام بأي معالجة لبيانات ذات طابع شخصي، بالحصول على إذن مسبق من السلطة الوطنية للحماية بالنسبة للبيانات الوراثية والبحوث في المجال الصحي، وكذا المعلومات حول الجرائم أو الإدانات الجنائية، وتلك المطلوبة لأغراض أمنية أو مرتبطة برقم هوية وطنية أو بالمصلحة العامة، لاسيما إذا كانت لأغراض إحصائية أو علمية.

كما أشارت الاتفاقية إلى ضرورة استشارة سلطة الحماية، عندما تتم المعالجة البيانات، بالنيابة عن الحكومة والمؤسسات العامة والمجتمع المحلي وهيئة اعتبارية من القطاع الخاص مفوضة للقيام بخدمات عامة، وفقا لقانون أو تنظيم، ترتبط معالجة هذه البيانات بأمن الدولة، الوقاية، التحقيق والمتابعات القضائية وكذا البيانات الحساسة. مع تحديد طرق التعامل مع السلطة الوطنية للحصول على التراخيص اللازمة أو الرأي عند تقديم الاستشارة، حسب كل مجال[2].

[1] المشرع الجزائري اعتمد مصطلح " المعالج من الباطن"، وعرفه ضمن نص المادة 03 من القانون 18-07 بأنه " كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة"، وهو ما يبين التطابق بين كلا التعريفين.

[2] انظر المادة 10 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 20.

2- الآليات المؤسساتية لحماية البيانات ذات الطابع الشخصي:

ألزمت الاتفاقية الدول الأعضاء بإنشاء سلطة وطنية، إدارية مستقلة، مسؤولة عن حماية البيانات ذات الطابع الشخصي، تتكفل بإبلاغ الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم. مع تزويدها بالإطار البشري والمادي للقيام بمهامها المرتكزة على ضمان أن تتم معالجة البيانات الشخصية وفقا لأحكام الاتفاقية. كما تم تخويل السلطة لتوقيع عقوبات إدارية و إجرائية، من توجيه إنذارات، خطابات التحذير، سحب مؤقت أو دائم للرخصة وغرامات مالية، وفي حالة الضرورة، إيقاف معالجة بيانات، حجب بعض البيانات أو حظر مؤقت أو دائم لأي معالجة مخافة لأحكام الاتفاقية[1].

3- الإلتزامات الخاصة بالمعالجة وحقوق الشخص المعني بالبيانات :

نصت المادة 13 من الاتفاقية على جملة من الالتزامات والضوابط والمبادئ الخاصة بمعالجة البيانات لشخصية، وكذا تكريس مجموعة من الحقوق للشخص موضوع البيانات ذات الطابع الشخصي، والتي يمكن ذكرها إجمالا على النحو التالي:

3.1- الالتزامات الخاصة بمعالجة البيانات ذات الطابع الشخصي:

وتشمل الالتزامات الخاصة بحماية عملية المعالجة والالتزامات الخاصة بالمسؤول عن عملية معالجة البيانات ذات الطابع الشخصي:

3.1.1- الالتزامات الخاصة بحماية عملية المعالجة: تضمنت جملة من المبادئ الواجبة الاحترام خلال كل عملية معالجة وهي:

- مراعاة المبادئ الأساسية في معالجة البيانات ذات الطابع الشخصي: والتي تشمل مبدأ الموافقة والشرعية في المعالجة، مبدأ القانونية والنزاهة، مبدأ القصد، الصلة والتخزين

[1] راجع المادتين 11 و 12 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 22-26.

للبيانات، مبدأ الدقة، مبدأ الشفافية، ومبدأ السرية والتأمين في معالجة البيانات ذات الطابع الشخصي.

- مراعاة المبادئ المحددة المتعلقة بمعالجة البيانات الحساسة: وذلك بإلزام الدول الأعضاء بحظر جمع ومعالجة البيانات الحساسة، إلا في حالة اقتضت الضرورة أو المصلحة العامة ذلك، بموافقة الشخص المعني، ومختلف الاستثناءات التي تم تفصيلها ضمن نص المادة 14 من هذه الاتفاقية[1].

3.1.2- التزامات المسؤول عن معالجة البيانات ذات الطابع الشخصي:وتشمل جملة من الالتزامات المحددة ضمن القسم الخامس من الاتفاقية كما يلي:

- **التزامات السرية:** تقتضي السرية في المعالجة وحصر القيام بهذه الأخيرة من قبل أشخاص يعملون تحت سلطة المسؤول عن المعالجة وبموجب تعليمات صادرة عنه[2].
- **التزامات التأمين:** يتعين على مسؤول المعالجة اتخاذ التدابير والاحتياطات المناسبة لمنع تغيير البيانات أو إتلافها أو الاطلاع عليها من قبل الغير غير المرخص له.
- **التزامات التخزين:** يجب حفظ البيانات ذات الطابع الشخصي لمدة لا تتجاوز المدة الضرورية لتحقيق الهدف من جمع ومعالجة البيانات.
- **التزامات الاستدامة:** يتعين على المسؤول على المعالجة اتخاذ مجمل الاحتياطات اللازمة لضمان أن البيانات المعالجة يمكن استخدامها، بغض النظر عن الجهاز التقني المستخدم في العملية، وكذا ضمان، بصفة خاصة، أن لا تشكل التطورات التقنية عائقا أمام هذا الاستعمال[3].

---

[1] راجع المادة 14 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 28-30.

[2] انظر المادة 20 من اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 32.

[3] انظر المادة 23 اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المرجع السابق، ص 33.

3.2 الحقوق الخاصة بالشخص موضوع البيانات ذات الطابع الشخصي:

كرست الاتفاقية العديد من الحقوق للشخص على بياناته ذات الطابع الشخصي، شملت: الحق في الإعلام، الحق في الوصول إلى المعلومات، الحق في الاعتراض على معالجة البيانات الشخصية المتعلقة به، بالإضافة إلى الحق في التصحيح أو الحذف.

كما تجدر الإشارة أن الاتفاقية تضمنت جملة من التدابير الجزائية الخاصة بمكافحة الجرائم الالكترونية، لاسيما تلك التي تتعلق بالبيانات ذات الطابع الشخصي، إلا أن ما يلاحظ في هذا الشأن هو بالرغم من أهمية هذه الاتفاقية إلا أنها لم تدخل حيز التطبيق نظرا لعدم اكتمال العدد المشترط من الدول الإفريقية للمصادقة على هذه الاتفاقية، حيث حدد نص المادة 36 من هذه الاتفاقية مصادقة 15 دولة افريقية من مجموع 45 دولة عضو في الاتحاد الإفريقي، وتعد الجزائر من بين الدول المتأخرة في المصادقة على هذه الاتفاقية[1]، بالرغم من الآليات القانونية المكرسة لحماية المعطيات ذات الطابع الشخصي منذ أكثر من ثلاث (03) سنوات، على غرار الآليات التي كرسها القانون 18-07، والتي تشتمل على العديد من البنود والمحاور المتطابقة مع التوصيات المحددة بموجب اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

المطلب الثاني: دور أجهزة المنظمات الإقليمية في حماية البيانات الشخصية

لقد برز دور أجهزة المنظمات الإقليمية، لاسيما الأوروبية منها، في إرساء وتكريس آليات لحماية الخصوصية والبيانات الشخصية، والتي تم تمييز الفاعلة منها، حسب مجال الدراسة والمراجع المتاحة في هذا المجال، مع مراعاة الطرح المعتمد عليه في مختلف

[1] مريم لوكال، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي (في ضوء قانون حماية المعطيات رقم: 18-07)، مجلة العلوم القانونية والسياسية، جامعة حمة لخضر- الوادي، العدد 01، سنة 2019، الجزائر، ص1307.

جوانب هذه الأطروحة، وعليه سيتم التطرق إلى دور كل من أجهزة المنظمات الأوروبية، الإفريقية وكذا العربية في حماية البيانات الشخصية بصفة مباشرة أو غير مباشرة.

الفرع الأول: دور أجهزة المنظمات الأوروبية في حماية البيانات الشخصية

إن من أبرز المنظمات الإقليمية العالمية المهتمة بمجال حماية البيانات الشخصية هي منظمة الاتحاد الأوروبي، والتي كرست بموجب الاتفاقية الأوروبية لحقوق الإنسان ثلاثة أجهزة لمتابعة وضمان تنفيذ بنودها في مجال حماية الحقوق والحريات[1]، وتتمثل في كل من اللجنة الأوروبية لحقوق الإنسان، المحكمة الأوروبية لحقوق الإنسانولجنة الوزراء بمجلس أوروبا.

وعليه سيتم التطرق فيما يلي إلى الأجهزة والآليات التي كرستها هذه الاتفاقية لحماية الحياة الخاصة ومن خلالها البيانات الشخصية:

أولا: اللجنة الأوروبية لحقوق الإنسان

تعد اللجنة الأوروبية لحقوق الإنسان الآلية الأوروبية الأولى لحماية الحقوق والحريات المكرسة بموجب الاتفاقية الأوروبية لحقوق الإنسان وسيتم التطرق إليها من حيث الجانب التاريخي لتسهيل المقارنة بينها وبين باقي الآليات على المستوى الإفريقي وكذا العربي نظرا لوجود بعض القواسم المشتركة في الكثير من الآليات.

1- تشكيلة اللجنة الأوروبية لحقوق الإنسان: تتشكل اللجنة من عدد أعضاء يساوي عدد الدول المتعاقدة، يختار هؤلاء الأعضاء عن طريق الانتخاب لمدة ست (06) سنوات قابلة للتجديد، تتخذ قراراتها بأغلبية الأعضاء الحاضرين[2].

2- **آليات عمل اللجنة الأوروبية لحقوق الإنسان:** في البداية تم اعتماد آليتين:

[1] الاتفاقية الأوروبية لحقوق الإنسان، في كتاب : حقوق الإنسان، مجموعة وثائق أوروبية، ترجمة الدكتور محمد أمين الميداني، والدكتور نزيه كسيبي، الطبعة الثانية، منشورات المعهد العربي لحقوق الإنسان، 2001، من ص 35 إلى ص 102.

[2] انظر المادة 34 من الاتفاقية الأوروبية لحقوق الإنسان، المرجع السابق.

أ-تلقي الشكاوى: وتشمل كل من شكاوى الأفراد، الدول والمنظمات غير الحكومية وتنظر في الشكاوى الخاصة بالدول الأطراف في الاتفاقية كما تشترط في شكاوى الأفراد اعتراف الدولة باختصاص اللجنة بتلقي هذا النوع من الشكاوى، بالإضافة إلى ضرورة استفاد طرق التظلم الداخلية [1].

ب- التقارير: تعتمد على التسوية الودية وتعد تقريرا مفصلا يرسل إلى الحكومة المعنية ولجنة الوزر اء وفي حالة عدم نجاح التسوية الودية تقدم تقريرا مدعوما برأيها إلى مجلس الوزراء.

وبصدور البروتوكول الحادي عشر (11) تم إلغاء اللجنة الأوروبية لحقوق الإنسان وأصبحت المحكمة الأوروبية الآلية العامة الأساس لحماية الحقوق والحريات على المستوى الأوربي.

ثانيا: المحكمة الأوروبية لحقوق الإنسان

تأسست المحكمة الأوروبية لحقوق الإنسان عام 1958 بعد موافقة ثمانية (08) دول أعضاء من مجلس أوروبا[2] ،كما تم منح الأفراد حق الإدعاء أمام المحكمة وتم تقليص صلاحيات مجلس الوزراء فيما يتعلق بالإجراءات القضائية[3].

1- الهيكل التنظيمي للمحكمة الأوروبية ومجال اختصاصها

بعد صدور البروتوكول الحادي عشر أصبح الاختصاص النوعي للمحكمة الأوروبية يمتد إلى النظر في شكاوى الأفراد، إضافة إلى شكاوى الدول وعليه ونظرا لتوسع اختصاصها أضحت المحكمة الأوروبية تتألف من :

[1] راجع المادة 33من الاتفاقية الأوروبية لحقوق الإنسان، المر جع السابق.

[2] بوحملة كوثر، دور المحكمة الأوروبية لحقوق الإنسان في تطوير القانون الدولي الأوروبي لحقوق الإنسان،رسالة ماجستير،جامعة يوسف بن خدة الجزائر،كلية الحقوق بن عكنون،السنة الجامعية 2009-2010،ص 01.

[3] رياض العجلاني، تطور إجراءات النظر في الطلبات الفردية أمام المحكمة الأوروبية لحقوق الإنسان،مجلة جامعة دمشق للعلوم الاقتصادية والقانونية المجلد 28 العدد الثاني 2012،ص 165.

أ – **قسم التسجيل :** نظم قرار المحكمة الأوروبية مهام قسم التسجيل وبنيته حيث يختص بتهيئة الطلبات والوثائق واستكمال النواحي الإجرائية والمساعدة القانونية والمعلوماتية والعلاقات العامة والتوثيق،وينتخب رئيس قسم التسجيل ونائبيه من الهيئة العامة للمحكمة ويعمل تحت سلطة رئيس المحكمة.

ب – أقسام المحكمة : تتألف المحكمة الأوروبية من خمسة أقسام ودوائر، إضافة إلى الدائرة الكبرى، ويجب أن يراعى في تشكيلها التوزيع الجغرافي وتمثيل الجنسين وكذا النظم القانونية لمختلف الدول الأطراف في الاتفاقية الأوروبية وكل قسم من أقسام المحكمة رئيس ونائب رئيس وكاتب ونائب كاتب،كما تشكل الأقسام لجان القضاة الثلاثية،وتشكل أيضا دوائر تتألف من سبعة (07) قضاة من بين أعضائها،ويرأس الدوائر قضاة ينتخبون من الهيئة العامة للمحكمة لمدة محدودة أما الدائرة الكبرى فتتشكل من سبعة عشر (17) قاضيا هم رئيس المحكمة ونائبه ورؤساء الدوائر وقضاة ينتخبون وفقا لقواعد المحكمة.

ج – الهيئة العامة للمحكمة : تتشكل من قضاة المحكمة،ولها مهام إدارية تتمثل فيما يلي :

- انتخاب رئيس المحكمة ونائبه أو نوابه
- تشكيل دوائر المحكمة
- انتخاب رؤساء دوائر المحكمة
- انتخاب كاتب المحكمة ونائبه أو نوابه
- إقرار اللائحة الداخلية للمحكمة وتعديلها

وتتألف المحكمة من عدد قضاة يعادل عدد الدول الأطراف في الاتفاقية الأوروبية لحقوق الإنسان وينتخبون من الجمعية البرلمانية لمجلس أوروبا بأغلبية الأصوات،ويشترط في القاضي المؤهل العلمي العالي الذي يمكنه من التعيين في أعلى هيئة قضائية ببلده،وينتخب القضاة لفترة ست سنوات قابلة للتجديد وينتهي تعيينهم ببلوغ سن سبعين (70) سنة ولا يمكن عزل أي قاض إلا بقرار من قضاة المحكمة بأغلبية ثلثي القضاة،كما

تنتخب الهيئة العامة رئيس المحكمة ونائبه لفترة ثلاث سنوات قابلة للتجديد وتنتخب دوائر المحكمة رؤسائها وكاتب المحكمة ونائبه [1].

2- إجراءات التقاضي أمام المحكمة الأوروبية لحقوق الإنسان وفاعليتها

يمكن للأفراد إيداع شكواهم أمام المحكمة التي تقوم بدراستها على مرحلتين تقوم في المرحلة الأولى بالبث في قبولها،ثم تقوم في المرحلة الثانية بالنظر فيها وا إصدار حكم فيها ولقبول طلبات الأفراد لابد من توفر جملة من الشروط هي :

- استنفاد المتضرر جميع طرق الطعن المتاحة في القوانين الداخلية لبلده.
- تقديم الطلب خلال ستة (06) أشهر من صدور القرار أو الحكم في الطعن الداخلي.
- يجب أن يكون الطاعن معلوما.
- أن لا يكون الطلب سبق وأن نظرته المحكمة وأن لا يكون محل تحقيق دولي أو تسوية.

بعد تقديم الطلب تتم إحالته إلى لجنة القضاة الثلاثية لدراسته وتقرر قبوله من عدمه والقرار يكون بالإجماع وهو نهائي وا إذا لم تتوصل لجنة القضاة الثلاثية إلى قرار بشأن الطلب المقدم يحال إلى غرفة المداولة المشكلة من سبعة قضاة (07) للفصل فيه بأغلبية الأصوات وبعد دخول البروتوكول الرابع عشر (14) المعدل للاتفاقية الأوروبية لحقوق الإنسان حيز التنفيذ في 01 جوان 2010 من أجل تحسين فعالية آلية حماية حقوق الإنسان أضاف معيار جديد لقبول الطلبات الفردية حيث عدلت المادة 35 من الاتفاقية الأوروبية لحقوق الإنسان[2]، والتي حددت معايير قبول الطلبات الفردية إذ أعطى البروتوكول الرابع عشر للمحكمة الأوروبية لحقوق الإنسان الحق في عدم قبول الطلبات الفردية إذا لم يعلن مقدم الطلب عن أي ضرر جدي عن انتهاك الحقوق المنصوص عليها في الميثاق وبروتوكو لاته، والغاية من إضافة هذا المعيار هو تمكين المحكمة من

[1] انظر المادة 65 من الاتفاقية الأوروبية لحقوق الإنسان، المرجع السابق.

[2] البروتوكول الرابع الملحق بالاتفاقية الأوروبية، متاح على الموقع الخاص بمجلس أوروبا، على الرابط " https://www.echr.coe.int/documents/convention_ara.pdf " تاريخ آخر زيارة للموقع: 2022/02/17.

آلية أخرى لتصفية الطلبات المقدمة لها وقد أثار هذا المعيار جدلا كبيرا، فالجمعية البرلمانية لمجلس أوروبا عارضته بشدة واعتبرته عائقا لحق الأفراد في نظر المحكمة الأوروبية في طلباتهم ومن جهة أشارت أن استعمال عبارة " أضرار غير جدية أو غير ذات أهمية " قابلة للاستغلال ولتفسيرات مختلفة فضلا عن مدى صلاحية تفسير القضاة للأضرار غير الجدية ؟ وهل يتبنون التفسير الواسع أم الضيق ؟ ولتوفيق وجهات النظر المتباينة تم اعتماد تعديلين جديدين في هذا الشأن يقضي الأول بعدم رفض المحكمة للطلب لعدم وجود ضرر جدي إذا كان احترام حقوق الإنسان يتطلب دراسة الطلب ويقضي التعديل الثاني عدم رفض المحكمة للطلبات لعدم جدية الضرر إذا كان الفصل في القضية أمام القضاء الوطني قد تم بشكل مخالف للإجراءات وللقوانين الوطنية[1].

كما أن المادة 20 من البروتوكول قضت بعدم تطبيق المعيار الجديد على الطلبات السابقة، وبعد قبول الطلب يحال إلى الدوائر المشكلة من سبع قضاة للفصل فيه، أو للدائرة الكبرى حيث ترفع الدوائر المكونة من سبع قضاة يدها من النزاع إذا كان يتعلق بمناقشة مسألة مهمة تتعلق بتفسير أحد أحكام الاتفاقية الأوروبية لحقوق الإنسان أو أحد ملحقاتها أو إذا كان الحكم الذي ستقرره المحكمة يتعارض مع حكم سابق لها فلأحد أطراف النزاع الاعتراض على قرار الدائرة لرفع يدها عن الدعوى خلال شهر من تاريخ تبليغه القرار وفي كلتا الحالتين يحال النزاع للدائرة الكبرى للفصل فيه[2].

وقد لعبت المحكمة الأوروبية دورا كبيرا في الفصل في العديد من القضايا تخص معالجة البيانات الشخصية، مكرسة حق أصحاب هذه البيانات وا إنصافهم، والتي من بينها القرار رقم 1496 الصادر بتاريخ 06 أوت 2016، المتضمن إدانة مؤجر استعمل رسائل إلكترونية شخصية كانت مسجلة على جهاز كومبيوتر تابع للأجير في مقر العمل، مؤكدة

[1] رياض العجلاني،المرجع السابق،ص 187

[2] رياض العجلاني،المرجع نفسه،ص180.

في ذلك بأن هذه الرسائل الالكترونية تخص الشخص المعني بانتهاك حرمة بياناته الشخصية[1].

ثالثا: لجنة الوزراء لمجلس أوروبا : أدت لجنة الوزراء لمجلس أوروبا دورا مزدوجا من حيث إصدار القرارات و التنفيذ وهي جهاز سياسي أكثر منه قضائي.

تضم اللجنة من حيث التشكيلة عضواً عن كل دولة لها عضوية في مجلس أوروبا حيث يقوم وزراء الخارجية أومن ينوب عنهم بتمثيل دولهم في لجنة الوزراء طبقا لمضمون النظام الأساسي لمجلس أوروبا[2].

وفي سنة 1981 أشرفت لجنة الوزراء على تبني اتفاقية حماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية[3]، حيث وقعت على هذه الاتفاقية حوالي واحد وثلاثين (31) دولة، وأصبحت نافذة وملزمة للدول الأعضاء ابتداء من بتاريخ 1985/10/10[4].

وا ٍجمالا فإن أجهزة المنظمات الأوروبية بسطت جانبا مهما من حماية البيانات الشخصية وفق ما أقرته من آليات لتجسيد هذه الحماية، هذا بالإضافة إلى إحاطة هذه الحماية بضمان محاكمة عادلة بتكريس دور المحكمة الأوروبية لحقوق الإنسان وما لعبته من دور بارز في مجال حماية البيانات الشخصية.

---

[1] ألفة المنصوري، حماية المعطيات الشخصية في مواقع التواصل الاجتماعي- دراسة مقارنة، المجلة الدولية للقانون، كلية القانون بجامعة قطر، المجلد التاسع، العدد الثالث، 2020، ص100. (89-121).

[2]. تم تحميل نسخة من الميثاق العربي لحقوق الإنسان من الموقع الالكتروني لجامع الدول العربية بتاريخ 2018/02/12.

"www.lasportal.org/ar/sectors/dep/HumanRightsDep/Documents/عربي.pdf"

[3] Convention for the project of the individuals with regard to automatic processing of personel data

[4] مروة زين العابدين صالح، المرجع السابق، ص301.

الفرع الثاني: دور أجهزة المنظمات العربية والإفريقية في حماية البيانات الشخصية

سيتم التطرق إلى دور كل من المحكمة العربية لحقوق الإنسان المنبثقة عن جامعة الدول العربية، وكذا دور كل من اللجنة الإفريقية والمحكمة الإفريقية لحقوق الإنسان في مجال حماية البيانات الشخصية بصفة ضمنية.

أولا: دور المحكمة العربية في حماية البيانات الشخصية:

تعد المحكمة العربية لحقوق الإنسان الآلية الوحيدة المنبثقة عن مجلس وزراء جامعة الدول العربية في مجال حماية حقوق الإنسان، حيث انطلق مشروع إنشاء المحكمة العربية لحقوق الإنسان سنة 2012، بعد تقديم دولة البحرين مقترح إلى مجلس الوزراء لجامعة الدول العربية المشكل من 137 دولة، وفي 10 مارس 2013، وبموجب قرار المجلس الذكور تم التأكيد على أهمية المقترح، حيث تم تشكيل لجنة من الخبراء القانونيين للتنسيق مع الأمين العام لجامعة الدول العربية لإعداد دراسة بالمقارنة مع التجارب الإقليمية المشابهة، وبعد تقديم تقرير لجنة الخبراء للدراسة من قبل مؤتمر القمة العربية المنعقد بالدوحة سنة 2013 تمت الموافقة على إنشائها في 03/26/ 2013 [1].

وتم تكليف لجنة قانونية بمهمة إعداد نظام لها حيث قدم المقترح وأدخلت عليه بعض التعديلات ليتم اعتماده بموجب القرار "779"المؤرخ في 2014/09/07 المتخذ اثر اجتماع وزراء الخارجية في جامعة الدول العربية في جلستها 142 المنعقدة بالقاهرة يومي 06 و07 سبتمبر 2014، على أن يدخل هذا النظام حيز النفاذ متى صادقت عليه سبعة (07) أعضاء في الجامعة[2].

[1] راجع تقرير حول الموضوع بعنوان" المحكمة العربية المقترحة لحقوق الإنسان- يجب التراجع عن تبني مشروع ميثاق المحكمة وبدء عملية إنشائها بشكل سليم، ص6 موجود على الموقع الالكتروني للجنة الدولية للحقوقيين بتاريخ 2018/02/15 على الرابط التالي:

https://www.fidh.org/IMG/pdf/final_pp_arab_court_-_ar-2.pdf

[2] تقرير حول الموضوع بعنوان" المحكمة العربية المقترحة لحقوق الإنسان ، المرجع نفسه، ص7.

1- تشكيلة المحكمة العربية لحقوق الإنسان:

تتألف من سبعة (07) قضاة ويمكن رفع عددهم إلى إحدى عشر (11) قاضيا، يجري انتخاب القضاة من قائمة الأشخاص الذين ترشح كل دولة شخصين منهم، ينتخبون عن طريق الاقتراع السري لمدة 04 سنوات قابلة للتجديد مرة واحدة فقط[1].

كما تم التأكيد على استقلالية القضاة ومنحهم الحصانة والامتيازات الممنوحة لممثلي الدول الأعضاء لدى جامعة الدول العربية [2]

وتجدر الإشارة أنه لم ينص الميثاق على تأسيس هذه المحكمة على عكس مع ما تم ملاحظته في نظيرتها على المستوى الأوروبي حيث تم الإشارة إلى المحكمة في نص الاتفاقية الأوروبية بل أكثر من ذلك تم إلغاء الآلية السابقة ألا وهي اللجنة الأوروبية نظرا للدور الناجع للمحكمة بالنظر إلى حجم ونوعية القضايا المفصول فيها سنويا.

والملاحظ في هذا الجانب، أنه كان من الأجدر اعتماد نظام المحكمة كآلية فعالة بموجب بروتوكول ملحق بالميثاق العربي لحقوق الإنسان لإعطائها مصداقية أكثر بجانب الآليات المذكورة سابقا[3].

2- اختصاص المحكمة العربية لحقوق الإنسان:

تختص المحكمة بكافة الدعاوى و النزاعات الناشئة عن تطبيق و تفسير الميثاق العربي لحقوق الإنسان أو أية اتفاقية عربية أخرى في هذا المجال وتفصل في أي نزاع يثار حول اختصاصها بنظر الدعاوى أو الطلبات أو الحالات التي تنظرها.

---

[1] راجع المواد5،6،7 و8 من النظام الأساسي للمحكمة العربية لحقوق الإنسان، نسخة الكترونية محملة من موقع جامعة الدول العربية بتاريخ 2018/02/12"
http://www.lasportal.org/ar/humanrights/Committee/Documents/

[2] انظر المادتين 14 و15 من النظام الأساسي للمحكمة العربية، نفس المرجع.

[3] حيث نصت المادة 52 من الميثاق العربي لحقوق الإنسان على أنه " يمكن لأية دولة طرف أن تقترح ملاحق إضافية اختيارية لهذا الميثاق ويتخذ في إقرارها الإجراءات التي تتبع في إقرار تعديلات الميثاق".

ويتطلب قبول الدعاوى مجموعة من الشروط [1]، تتمثل فيما يلي:

1. استنفاد طرق التقاضي في الدولة.
2. عدم رفع الدعوى أمام محكمة إقليمية أخرى.
3. أن تكون الدعوى رفعت بعد ستة أشهر.

لا يمكن للأفراد رفع شكاواهم أمام المحكمة إذ يحق فقط للدولة الطرف التي يدعي أحد رعاياها أنه ضحية انتهاك حق من حقوق الإنسان اللجوء للمحكمة بشرط أن تكون الدولة الشاكية والدولة المشكو في حقها طرفاً في النظام الأساسي، أو أن تكون قد قبلت اختصاص المحكمة[2].

وهذا على عكس ما لاحظناه بالنسبة للمحكمة الأوروبية فإنها تتيح للأفراد إمكانية اللجوء إليها عند المساس بحقوقهم المكرسة ضمن الاتفاقية.

ثانيا: دور أجهزة المنظمات الإفريقية في حماية البيانات الشخصية

لقد أقر الميثاق الإفريقي لحقوق الإنسان والشعوب والبروتوكول الملحق به، المعد من طرف أعضاء منظمة الوحدة الإفريقية (الاتحاد الإفريقي حاليا) في 1981/06/27، والذي دخل حيز التنفيذ بتاريخ 1986[3]/10/21، إنشاء أجهزة تضمن حماية حقوق الإنسان بصفة مباشرة والتي من بينها الحق في الخصوصية، المكرس بموجب المادة 04 منه، وبصورة غير مباشرة حماية البيانات الشخصية، لاسيما بالرجوع إلى دور كل من اللجنة الإفريقية والمحكمة الإفريقية لحقوق الإنسان والشعوب.

أ- اللجنة الإفريقية لحقوق الإنسان و الشعوب

نصت عليها المادة 30 من الميثاق الإفريقي، بدأت عملها في نوفمبر 1987.

---

[1] تفصيل الشروط وارد في المادة 18 من النظام الأساسي للمحكمة العربية لحقوق الإنسان، المرجع السابق

[2] انظر المادة 19 من النظام الأساسي للمحكمة العربية لحقوق الإنسان، المرجع السابق.

[3] راجع الميثاق الإفريقي لحقوق الإنسان والشعوب، على الموقع "http://hrlibrary.umn.edu/arab/a005.html" تاريخ الاطلاع: 15 فبراير 2018.

1- تشكيلة اللجنة الإفريقية لحقوق الإنسان والشعوب: تتشكل من إحدى عشر عضوا يتم اختيارهم من بين الشخصيات الإفريقية التي تتحلى بأعلى قدر من الاحتر ام ومشهود لها بسمو الأخلاق والنزاهة والحيدة وتتمتع بالكفاءة في مجال حقوق الإنسان مع ضرورة إشراك الأشخاص ذوي الخبرة في القانون، ينتخب مؤتمر رؤساء الدول أعضاء اللجنة عن طريق الاقتراع السري من بين قائمة مرشحين يمثلون كل الدول الأطراف في الميثاق[1]، مهمتها الأساس تعزيز حماية حقوق الإنسان في القارة.

2- نظام عمل اللجنة الإفريقية لحقوق الإنسان. تتلقى الشكاوى من الأفراد، المنظمات غير الحكومية والدول الأعضاء بشأن قضايا انتهاك حقوق الإنسان المنصوص عليها في الميثاق.

كما لها سلطة تقديم توصيات إلى الدول الأطراف المعنية و إلى مؤتمر دول الإتحاد الإفريقي بشأن الإجراءات التي يمكن اتخاذها لمعالجة الانتهاكات كما تقوم ببرمجة زيارات إلى الدول الأعضاء لمراقبة مطابقة القوانين الداخلية والإجراءات المتخذة مقارنة بمضمون الميثاق.

كل دولة طرف تقدم تقريرا للجنة كل عامين بشأن التدابير التشريعية و غيرها لتفعيل حقوق الإنسان الواردة في الميثاق.

تستعرض اللجنة هذه التقارير وتقدم توصيات إلى الدولة المعنية.

ب- المحكمة الإفريقية لحقوق الإنسان والشعوب

أنشئت بموجب البروتوكول الملحق بالميثاق الإفريقي لحماية حقوق الإنسان و الشعوب المعتمد من قبل منظمة الوحدة الأفريقية في جوان 1998 ودخل حيز التنفيذ في 2004، يقع مقرها في أورشا تنزانيا[2].

[1] راجع المواد 31، 32 و33 من الميثاق الإفريقي لحقوق الإنسان والشعوب، نفس المرجع.

[2] انظر البروتوكول الملحق الميثاق الإفريقي لحقوق الإنسان والشعوب تم تحميله باللغة العربية من موقع جامعة منيسوتا بتاريخ 2018/02/15 على الرابط التالي:http://hrlibrary.umn.edu/arab/am2.html

والملاحظ هنا أنه بالرغم من عدم نص الميثاق الإفريقي لحقوق الإنسان والشعوب على إنشاء هذه الآلية إلا أنه تم تداركها فيما بعد بموجب بروتوكول على عكس ما تم ملاحظته بالنسبة للمحكمة العربية لحقوق الإنسان التي لم تعتمد سوى بقرار مجلس وزراء الخارجية لجامعة الدول العربية.

1- تشكيلة المحكمة الإفريقية: تتألف من إحدى عشر (11) قاض ينتخبون لمدة ست (06) سنوات، قابلة للتجديد مرة واحدة فقط.

2- اختصاص المحكمة الإفريقية: يمتد اختصاصها إلى كافة القضايا و النزاعات التي تقدم إليها و التي تتعلق بتفسير وتطبيق الميثاق والبروتوكول المنشئ لها أو أي اتفاقية أخرى تتعلق بحقوق الإنسان كما يمكن أن تقدم آراء استشارية بشأن مسائل قانونية إذا طلب منها ذلك [1].

كما يمكن للمنظمات، الأفراد والدول الأعضاء التي أصدرت إعلانا بقبولها اختصاص المحكمة أن ترفع شكاوى. حيث تم تسجيل سنة 2017 من بين 30 دولة طرف لم تعلن بقبول اختصاص المحكمة سوى ثمانية (08) دول.

من أشكال تدخلها: الأمر بالإجراءات المناسبة لمعالجة الانتهاكات كالتعويض العادل، وقد تتخذ عند الضرورة و في حالة الخطورة و لتجنب ضرر لا يمكن إصلاحه إجراءات مؤقتة .

حيث أن أول حكم صدر عن المحكمة كان ضد ليبيا بتاريخ 25 مارس2011، و المنشور بتاريخ 30 مارس2011، حيث حكمت المحكمة بالإجماع بأن تقوم ليبيا بوضع حد للإجراءات التي تتسبب في الخسائر في الأرواح أو انتهاك السلامة البدنية لأي فرد،

[1] راجع المادة 03 من البروتوكول الملحق بالميثاق الإفريقي لحقوق الإنسان والشعوب، المرجع السابق

الحكم ملزم لليبيا وعليها أن تجيب المحكمة خلال 15 يوما بالخطوات التي اتخذتها لتنفيذه [1].

هذا كما برز دور منظمات إقليمية أخرى في مجال حماية المعطيات الشخصية، على غرار جهود اللجنة الاقتصادية والاجتماعية لغربي آسيا (الاسكوا)، سنة 2007 بإعداد دراسة حول نماذج تشريعات الفضاء السيبراني في الدول الأعضاء في هذه اللجنة، وقد اعتمدت عليها الكثير من الدول كمرجع أساس في سن قوانينها الداخلية المتعلقة بحماية المعطيات الشخصية والأمن السيبراني[2].

[1] انظر المقال بعنوان " African Rights Court Issues First Ruling Against a State: Libya " على موقـــع Human Rights Wach على الرابط التالي:
https://www.hrw.org/ar/news/2011/03/30/242460
تاريخ الاطلاع: 2021/09/30.

[2] مريم لوكال، المرجع السابق، ص1308.

الفصل الثاني: الحماية القانونية الوطنية للبيانات الشخصية

سيتم من خلال هذا الفصل التعرض بالدراسة والتحليل لمختلف الآليات القانونية الوطنية التي كرسها المشرع الجزائري لحماية البيانات الشخصية، والتي تم تقسيمها إلى صنفين، حماية إجرائية وتقنية وهو موضوع المبحث الأول والذي سيخصص للتفصيل في مختلف التدابير والإجراءات التي كرسها المشرع الجزائري لمعالجة البيانات الشخصية في مختلف مراحلها. كما سيتم بسط مختلف الحقوق المكرسة للشخص على بياناته وكذا التزامات القائمين بالمعالجة لهذه البيانات.

وقد تم تخصيص المبحث الثاني للتفصيل في مختلف آليات الحماية المؤسساتية والجزائية المكرسة عبر مختلف مراحل معالجة المعطيات الشخصية.

المبحث الأول: التدابير الوقائية لحماية البيانات الشخصية في الجزائر

لقد عمدت مختلف القوانين الدولية المقارنة المهتمة بمجال حماية البيانات الشخصية إلى تكريس آليات وتدابير إجرائية تعد اللبنة الأساس لحماية البيانات الشخصية، وفي حالة عدم احترامها ومراعاتها فإنه يتم الانتقال إلى آليات أخرى ردعية جزائية.

والمشرع الجزائري بدوره كرس جملة من التدابير الوقائية لحماية البيانات الشخصية تضمنتها نصوص قانونية متعددة على غرار ما تضمنه الأمر 03-05، المتعلق بحقوق المؤلف والحقوق المجاورة، وكذا بعض أحكام القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى بعض مضامين القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، بحيث تعد حماية البيانات الشخصية في هذا الجانب من أهم العو امل لتدعيم الثقة وتشجيع التجارة ومختلف الخدمات الإلكترونية[1].

[1] تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية،المجلد04، العدد 02، سنة 2019، ص1524.

كما أضاف القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية[1]، إجراءات تساهم في حماية المعطيات الشخصية. ليتم بعده إصدار نص قانوني يخص مباشرة الأشخاص الطبيعيين في مجال معالجة معطياتهم ذات الطابع الشخصي بموجب أحكام القانون 18-07 ، والذي كرس آليات تخص مختلف تفاصيل معالجة المعطيات ذات الطابع الشخصي.

المطلب الأول: القواعد الإجرائية الوقائية الأساسية لحماية البيانات الشخصية

يتضح لنا من خلال عنوان هذا المطلب بأن هناك معالجة مشروعة وأخرى غير مشروعة، فأما المعالجة المشروعة فإنها هي تلك التي تتم وفق تدابير وا ٍجراءات سليمة مطابقة لتلك المنصوص عليها قانونا، وعليه بصورة غير مباشرة تضمن حماية للبيانات الشخصية المعالجة بمعرفة الشخص المعالج، أهدافه وتحمل مسؤولياته في حالة أفضت المعالجة إلى نتائج سلبية، كما أن الشخص المعني بمعالجة بياناته يتحمل مسؤولياته في حالة موافقته الصريحة على معالجتها، هذه الموافقة التي تشمل تعبير عن إرادته المميزة والتي تقبل بموجبها الشخص المعني أو ممثله الشرعي معالجة معطياته الشخصية بأي طريقة إلكترونية أو يدوية[2]، وهو ما تؤكد عليه مختلف التدابير الخاصة بمعالجة المعطيات، لاسيما تلك التي أقرها القانون 18-07.

وعليه سيتم التفصيل في كل القواعد الإجرائية الوقائية التي أقرها المشرع الجزائري قبل القيام بأي معالجة للبيانات الشخصية كما هو مفصل في الفرعين المواليين.

الفرع الأول: شروط مشروعية معالجة البيانات الشخصية

إن المشرع الجزائري من خلال نص القانون 18-07 لم يمنع معالجة البيانات الشخصية وا ٍنما حدد جملة من الشروط والضوابط يجب مراعاتها قبل، أثناء وبعد القيام

[1] القانون 18-04 المؤرخ في 10 مايو 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية عدد 27 المؤرخة في 13 مايو 2018.

[2] انظر المادة 02 من القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المرجع السابق.

بمعالجة المعطيات ذات الطابع الشخصي، وفي حالة عدم مراعاتها تعتبر المعالجة غير شرعية يترتب عنها جزاءات إدارية وجنائية.

وعليه لتوضيح مشروعية معالجة المعطيات ذات الطابع الشخصي، سيتم تقديم الشروط العامة والخاصة لمشروعية المعالجة مع إدراج الاستثناءات المتعلقة بها.

أولا: الشرط المتعلق بموافقة الشخص المعني بالمعالجة

لقد أكد المشرع الجزائري من خلال نص المادة 07 لقانون 18- 07 على أن معالجة المعطيات ذات الطابع الشخصي لا تتم إلا بعد الحصول على الموافقة الصريحة للشخص المعني[1]، وهو يعد إجراء أساسيا يقوم به المعني لصالح القائم بالمعالجة، بحيث يمكن كذلك للمعني أن يتراجع عن موافقته متى رأى ذلك مناسبا.

إلا أن موافقة الشخص المعني، عند المعالجة الآلية، تطرح كثيرا من الإشكالات حول تطبيق النظرية العامة للعقد، ففي حالة معالجة المعطيات عبر مواقع التوصل الاجتماعي فإن صاحب المعطيات يكون بصدد عقد إذعان، لاعتماد هذه المواقع أحادية مراجعة الشروط التعاقدية، ومثال ذلك ما يؤكده موقع تويتر بأن "كل ما يعبر عنه المستخدمون في هذا الموقع يظهر في نفس اللحظة في كافة أنحاء العالم"[2].

وفي حالة معالجة المعطيات الخاصة بشخص ناقص أو عديم الأهلية، فإنها تخضع للقواعد المنصوص عليها في القانون العام، والتي تقتضي الحصول على رأي وليه أو ممثله القانوني، أو بترخيص من القاضي بحسب كل حالة. حيث أنه تم توضيح الحالة المتعلقة بمعالجة معطيات تتعلق بطفل حيث اشترط المشرع ضرورة الحصول على الموافقة من ممثله الشرعي أو بترخيص من القاضي المختص عند الاقتضاء، إلا أن

[1] انظر المادة 07 من القانون 18-07، المرجع السابق.

[2] ألفة المنصوري، حماية المعطيات الشخصية في مواقع التواصل الاجتماعي- دراسة مقارنة، المرجع السابق، ص101.

القاضي استثناءا يمكنه الأمر بالمعالجة دون أخذ موافقة الممثل الشرعي للطفل إذا استدعت المصلحة الفضلى للطفل ذلك[1].

كما تجدر الإشارة أن المشرع أورد جملة من الاستثناءات، في حالات الضرورة، والتي بموجبها لا تكون موافقة الشخص المعني واجبة حيث تم حصر هذه الحالات ضمن نص المادة 07 على النحو التالي:

- احترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة.
- لحماية حياة الشخص المعني.
- لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه.
- للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه.
- لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم إطلاعه على المعطيات.
- لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/أو حقوقه وحرياته الأساسية.

ومن خلال تحديد مجال مختلف الاستثناءات الواردة أعلاه، فإن جانبا من الفقه، يرى أن الضابط المخول بممارسة السلطة التقديرية في هذا الجانب هو السلطة الوطنية لحماية المعطيات، نظرا للصلاحيات المخولة لها قانونا، كذلك القاضي المختص الذي له سلطة عليا في الرقابة الوجوبية لضمان التوازن بين المصلحة المشروعة للقائم بالمعالجة وكذا مصلحة الشخص المعني بمعالجة معطياته، هذا من أجل منح أكثر ضمانة لتجنب سوء

[1] انظر المادة 08 من القانون 18-07، المرجع السابق.

استخدام الاستثناء المتعلق بشرط الرضائية كذريعة وقاعدة للمساس بالمعطيات الشخصية[1].

ثانيا: الشروط المتعلقة بالمعطيات ذاتها

كما تم تحديد جملة من الشروط الواجب توفرها في المعطيات الشخصية تم حصرها ضمن نص المادة 09 من القانون 18-07، والمتمثلة في[2]:

1. **تكون المعالجة بطريقة مشروعة ونزيهة:** وحتى تكون المعالجة مشروعة فلابد أن تحصل على موافقة الشخص المعني كما أوردنا سالفا، هذا بالإضافة إلى مراعاة جملة من الضوابط في حالة الاستثناءات الخاصة بالمعالجة لوجود ضرورة.

2. **أن تجمع هذه المعطيات لغايات محددة وواضحة ومشروعة وألا تعالج بطريقة تتنافى مع هذه الغايات:** وعليه يشترط لمشروعية تجميع المعطيات إبلاغ صاحب المعطيات قبل الشروع في عملية الجمع، ومن أبرز المخالفات التطبيقية في هذا المجال، القيام بجمع عناوين بريد إلكتروني لمستخدمي الإنترنت دون علم أصحابها، يعتبر إجراء غير مشروع كما أقرت بذلك اللجنة الوطنية للمعلوماتية والحريات بفرنسا، كما اعتبرت محكمة النقض الفرنسية أن تجميع عناوين بريد إلكتروني دون علم أصحابها يعد مخالفة تستحق العقاب[3].

3. **أن تكون صحيحة، كاملة ومحينة:** إن التأكد من دقة وصحة المعطيات يستلزم أخذ رأي الشخص المعني في غالب الحالات، نظرا لارتباط المعطيات بالشخص، إلا في حالات انعدام أو نقص الأهلية أو أسباب تحول دون إمكانية التأكد من صاحب المعطيات مباشرة. حيث يوجد الكثير من بنوك المعلومات تشتمل على معلومات غير

---

[1] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية – دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص427.

[2] انظر المادة 9 من القانون 18-07، المرجع السابق.

[3] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية – دراسة في القانون الفرنسي (القسم الأول)، المرجع السابق، ص416.

صحيحة، أو ناقصة المحتوى، تجر إلى الفهم الخاطئ أو تلفيق تهم، تمس بخصوصية صاحب هذه البيانات، وهو ما يشكل اعتداء واضحا على الخصوصية المعلوماتية[1].

4. **أن تكون ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها**يمنع التجميع من أجل التجميع، وا ٍنما يتطلب وجود رابط بين مبدئي السببية والغائية من تجميع المعطيات، مع توضيح ذلك للشخص المعني مسبقا. والهدف من وراء هذا الشرط كذلك هو تقييد معالجة المعطيات الشخصية بالأهداف التي من أجلها تم جمعها، كما يشترط انسجام أسلوب المعالجة مع الغاية من عملية الجمع لهذه المعطيات[2].

5. **أن تكون محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي تم جمعها ومعالجتها من أجلها:** وهذا لمنح أكثر حماية للمعطيات وحتى لا يمكن استغلالها لغير الأغراض المجمعة من أجلها، وهنا تطرح مسؤولية المكلف بالمعالجة والذي يشترط أن يقوم بالتخلص من المعطيات التي قضي الغرض الذي جمعت من أجله، ومن أمثلة ذلك الملفات الطبية، حيث لا توجد ضرورة للاحتفاظ بها بعد شفاء المريض..

الفرع الثاني: الشروط المتعلقة بإجرائي التصريح المسبق والترخيص

بالرجوع إلى نص المادة 12 من القانون 18-07 فإنه تم تحديد واشتراط إما إيداع تصريح مسبق لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو لترخيص من هذه الأخيرة لأي عملية معالجة لمعطيات شخصية، وعليه سيتم التفصيل في إجراءات على الحصول على التصريح المسبق أو الترخيص على النحو التالي:

[1] جيهان فقيه، حماية البيانات الشخصية في الإعلام الرقمي، مجلة العلوم الإنسانية، العدد السابع /الجزء(1)، جوان 2017، ص123

[2] سامح عبد الواحد التهامي، المرجع نفسه، ص421.

أولا: إجراء التصريح المسبق:

أشار نص المادة 13 من القانون 18-07 إلى كيفيات إيداع التصريح المسبق الذي يعد التزاما من قبل المعالج بإجراء عملية المعالجة، يودع لدى السلطة الوطنية، أو يرسل بواسطة البريد الالكتروني، وبنفس الطريقة يكون رد السلطة الوطنية سواء بتسليم المعني وصل إيداع فور استلام التصريح أو يتم إرساله بواسطة البريد الالكتروني[1].

كما حددت المادة 14 من نفس القانون جملة من الشروط التي يجب أن يتضمنها التصريح، تتمثل فيما يلي:

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

2- طبيعة المعالجة وخصائصها والغرض أو الأغراض المقصود منها.

3- وصف فئة أو فئات الأشخاص المعنيين والمعطيات أو فئات المعطيات ذات الطابع الشخص المتعلقة بهم.

4- المرسل إليهم أو فئات المرسل إليهم الذين قد توصل إليهم المعطيات.

5- طبيعة المعطيات المعتزم إرسالها إلى دول أجنبية.

6- مدة حفظ المعطيات.

7- المصلحة التي يمكن للشخص المعني عند الاقتضاء، أن يمارس لديها الحقوق المخولة له بمقتضى أحكام القانون 18-07 وكذا الإجراءات المتخذة لتسهيل ممارسة هذه الحقوق.

8- وصف عام يمكن من تقييم أولي لمدى ملائمة التدابير المتخذة من أجل ضمان سرية وأمن المعالجة.

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

[1] راجع المادة 13 من القانون 18-07، المرجع السابق.

هذا كما تجدر الإشارة إلى أن أي تغيير يحدث يتعلق بهذه المعلومات حسب البنود التسع فإنه يستوجب الإبلاغ الفوري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي[1].

ثانيا: الترخيص المسبق:

يعد الترخيص المسبق إجراء مباشرا بعد دراسة التصريح من قبل السلطة الوطنية والتأكد من أن المعالجة موضوع التصريح تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص، حيث يبلغ هذا الترخيص في شكل قرار إلى المسؤول عن المعالجة في العشرة (10) أيام من موعد إيداع التصريح المسبق[2].

هذا كما أكد المشرع الجزائري ضمن نص المادة 18 من نفس القانون على حظر معالجة المعطيات الحساسة[3]، إلا أنه، وللضرورة المرتبطة بالمصلحة العامة ومن أجل قيام المسؤول عن المعالجة بمهامه القانونية والنظامية، أو عندما تتم المعالجة بناء على الموافقة الصريحة للشخص المعني، أو النص على ذلك قانونا، وبترخيص من السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي إذا سجلت حالة من الحالات المحددة حصرا، كما يلي:

1- إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر وفي حالة وجود الشخص المعني في حالة عجز بدني أو قانوني عن الإدلاء بمواقفه.

[1] راجع المادة 14 من القانون 18-07، المرجع السابق.

[2] انظر المادة رقم 17 من القانون 18-07، المرجع السابق

[3] يقصد بالمعطيات الحساسة حسب ما تضمنته المادة رقم 02 من القانون 18-07، " معطيات ذات طابع شخصي تبين الأصل لعرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية".

2- تنفيذ المعالجة بناء على موافقة الشخص المعني، من طرف مؤسسة أو جمعية أو منظمة غير نفعية ذات طابع سياسي أو فلسفي أو ديني أو نقابي، في إطار نشاطاتها الشرعية.

3- إذا كانت المعالجة تخص معطيات صرح بها الشخص المعني علنا عندما يمكن استنتاج موافقته على معالجة المعطيات من تصريحاته.

4- أن المعالجة ضرورية للاعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء وأن تكون قد تمت حصرياً لهذه الغاية.

5- معالجة المعطيات الجينية، باستثناء تلك التي يقوم بها أطباء أو بيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي والقيام بتشخيصات طبية وفحوصات أو علاجات.

كما تم اشتراط الحصول على الترخيص في حالة نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية، حيث تم منح سلطة التقدير للسلطة الوطنية مع مراعاة مدى توفر مستوى كافي من الأمن والحماية للحريات في تلك الدولة، كما يمكن للسلطة الوطنية أن تمنح الترخيص بنقل المعطيات إلى دولة أجنبية استثناء[1]، إذا كانت المعالجة تتطابق مع أحكام المادة 02 من هذا القانون[2].

المطلب الثاني: حقوق الشخص والتزامات المسؤولين عن معالجة بياناته

أقر المشرع الجزائري حماية المعطيات الشخصية للأفراد خلال المعالجة وذلك من خلال منحهم الحق في الاطلاع على بياناتهم، الاعتراض عليها، تعديلها أو إلغائها، وفي نفس السياق تم ضبط جملة من الإجراءات تحدد مسؤولية والتزامات القائم بالمعالجة من خلال عدم التعدي على البيانات باعتماد الأنظمة التقنية وضبط عملية المعالجة من

[1] راجع المادة 45 من القانون 18-07، المرجع السابق.

[2] نصت المادة 02 من القانون 18-07 إلى أنه " يجب أن تتم معالجة المعطيات ذات الطابع الشخصي، مهما كان مصدرها أو شكلها، في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة و ألا تمس بحقوق الأشخاص وشرفهم وسمعتهم".

الباطن إلى جانب الالتزام بالسر المهني وعدم تدخل الغير في المعالجة وهو ما سنتطرق له بالتفصيل في النقاط التالية:

الفرع الأول: حقوق الشخص المعني بمعالجة البيانات

لقد عمدت مختلف التشريعات الدولية المهتمة بمجال حماية البيانات الشخصية إلى جرد مختلف الحقوق المخولة للأشخاص إثر معالجة بياناتهم الشخصية، تحضيرا لمواجهة أي مخاطر تنجم عن المعالجة الآلية لهذه البيانات، باعتماد تقنيات المعلومات الحديثة، والتي تشكل مخاطر عدة على البيانات الشخصية، حيث توافقت مختلف التشريعات الدولية على تكريس الحق في الولوج الشخصي إلى البيانات وتصحيحها أو الاعتراض عليها وا ٍعلام الشخص المعني مباشرة بأي معالجة مهما كانت طبيعتها، باستثناء تلك المعالجات لأغراض موضوعية بحثية، فنية أو المعالجة لأغراض أمنية، محددة قانونا[1].

والمشرع الجزائري بدوره كرس جملة من الحقوق للشخص المعني بمعالجة بياناته، وردت ضمن نص القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[2]، شملت الحق في الإعلام، الحق في الولوج، الحق في التصحيح، الحق في الاعتراض والحق في منع الاستكشاف المباشر، وسيتم التفصيل في كل منها على النحو الموالي:

أولا: الحق في الإعلام

يمثل الحق في الإعلام الحق الأساسي قبل مباشرة أي عملية معالجة لمعطيات ذات طابع شخصي، بحيث ألزم المشرع المسؤول عن المعالجة أو ممثله، الإعلام المسبق وبصفة صريحة لا يكتنفها أي لبس عن كل شخص يتم الاتصال به قصد تجميع معطياته ذات الطابع الشخصي، بالعناصر التالية: هوية المسؤول عن المعالجة وعند الاقتضاء،

[1] حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد08، العدد04، سنة 2019، ص286.

[2] راجع المواد 32، 33، 34، 35، 36 و37 من القانون 18-07، المرجع السابق، ص18-20.

هوية ممثله، أغراض المعالجة وكل معلومة إضافية مفيدة، لاسيما المرسل إليه ومدى إلزامية الرد والآثار المترتبة عن ذلك وحقوقه ونقل المعطيات إلى بلد أجنبي.

كما أنه إذا لم يتم جمع المعطيات ذات الطابع الشخصي لدى الشخص المعني، يجب على المسؤول عن المعالجة أو من يمثله، قبل تسجيل المعطيات أو إرسالها للغير، أن يزوده بالمعلومات المشار إليها أعلاه، ما لم يكن قد علم بها مسبقا.

وفي حالة جمع المعلومات في شبكات مفتوحة، يجب إعلام الشخص المعني، ما لم يكن على علم مسبق، بأن المعطيات ذات الطابع الشخصي المتعلقة به يمكن أن تتداول في الشبكات دون ضمانات السلامة وأنها قد تتعرض للقراءة والاستعمال غير المرخص من طرف الغير[1].

كما أن المشرع أورد استثناءات لتطبيق الحق في الإعلام المحدد وفق المادة 32 من القانون 18-07، في حالات ثلاث محددة كما يلي:

1. إذا تعذر إعلام الشخص المعني، ولاسيما في حالة معالجة المعطيات ذات الطابع الشخصي لأغراض إحصائية أو تاريخية أو علمية، يلزم المسؤول عن المعالجة في هذه الحالة بإشعار السلطة الوطنية لحماية المعطيات باستحالة إعلام الشخص المعني وتقديم لها سبب الاستحالة.
2. إذا تمت المعالجة تطبيقا لنص قانوني.
3. إذا تمت المعالجة حصريا لأغراض صحفية أو أدبية أو فنية[2].

ثانيا: الحق في الولوج

نصت المادة 34 من القانون 18-07 على حق الشخص المعني في الحصول من المسؤول عن المعالجة، على:

[1] راجع المادة 32 من القانون 18-07، المرجع السابق، ص18.

[2] راجع المادة 33 من القانون 18-07، المرجع السابق، ص19.

- التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، وأغراض المعالجة وفئات المعطيات التي تنصب عليها والمرسل إليهم.

- إفادته، وفق شكل مفهوم، بالمعطيات الخاصة به التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات.

كما يحق للمسؤول عن المعالجة أن يطلب من السلطة الوطنية تحديد آجال الإجابة على طلبات الولوج المشروعة، ويمكنه الاعتراض على الطلبات التعسفية، لاسيما من حيث عددها وطابعها المتكرر، ويقع على عاتقه إثبات الطابع التعسفي لهذا الطلب[1].

ثالثا: الحق في التصحيح

وضح المشرع الجزائري من خلال مضمون نص المادة 35 من القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، أن الحق في التصحيح يقصد به تمكين الشخص المعني بالمعالجة من حقه في الحصول مجانا، من المسؤول عن المعالجة على:

أ- تحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة للقانون 18-07، بسبب الطابع غير المكتمل أو غير الصحيح لتلك المعطيات على الخصوص، أو لكون معالجتها ممنوعة قانونا، ويلزم المسؤول عن المعالجة بالقيام بالتصحيحات اللازمة مجانا، لفائدة الطالب في أجل عشرة (10) أيام من تاريخ إخطاره.

وفي حالة الرفض أو عدم الرد على الطلب خلال الأجل المذكور أعلاه، يحق للشخص المعني إيداع طلب التصحيح لدى السلطة الوطنية، التي تكلف أحد أعضائها للقيام بكل التحقيقات الضرورية والعمل على إجراء التصحيحات اللازمة في أقرب الآجال، وا ٍخبار الشخص المعني بمآل طلبه.

[1] انظر المادة 34 من القانون 18-07، المرجع السابق، ص19.

ب- تبليغ الغير الذي أوصلت إليه المعطيات الشخصية بكل تحيين أو تصحيح أو مسح أو إغلاق للمعطيات ذات الطابع الشخصي، يتم تطبيقا للمطة (أ) أعلاه، ما لم يكن ذلك مستحيلا. ويمكن استعمال الحق المنصوص عليه في هذه المادة من قبل ورثة الشخص المعني.

وتجدر الإشارة أن من بين تطبيقات الحق في التصحيح إصدار اللجنة الوطنية للمعلوماتية والحريات بفرنسا (CNIL) بموجب مداولتها رقم SAN-2021-014189 بتاريخ 15 سبتمبر 2021، حكم ضد الشركة الجديدة للحوليات الفرنسية بفرض غرامة مالية إدارية قدرها ثلاثة آلاف (3000) يورو، نظرا لانتهاكها حقوق تخص حماية البيانات الشخصية تتضمن الحق في التصحيح والحق في التعديل ومحو البيانات المنصوص عليها في المواد 16 و 17 وكذا العلاقات مع اللجنة (CNIL) المحددة بموجب المواد 30 و 31 من النظام العام الأوروبي رقم 2016/679 [1].

رابعا: الحق في الاعتراض ومنع الاستكشاف المباشر

يعد الحق في الاعتراض ومنع الاستكشاف المباشر[2] من الحقوق غير المباشرة للشخص المعني بمعالجة بياناته بالنظر لطبيعتها[3]، وبالرجوع إلى نص المادة 36 من القانون 18-07، فإن الحق في الاعتراض يخول للشخص المعني أن يعترض، لأسباب مشروعة على معالجة معطياته ذات الطابع الشخصي. كما له الحق في الاعتراض على استعمال المعطيات المتعلقة به لأغراض دعائية، ولاسيما التجارية منها، من طرف المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة. كما أن لهذا الإجراء

---

[1] Voir Délibération SAN-2021-014 du 15 septembre 2021 disponible sur site Cnil " https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044043045". Consulté le 13/01/2022 à 20h30.

[2] عرف الاستكشاف المباشر حسب نص المادة 02 من القانون 18-07 بأنه " إرسال أي رسالة، مهما كانت دعامتها وطبيعتها، موجهة للترويج المباشر أو غير المباشر لسلع أو خدمات أو لسمعة شخص يبيع سلعا أو يقدم خدمات".

[3] حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 18-07، المرجع السابق، ص287.

استثناءات إذا كانت المعالجة تستجيب لالتزام قانوني، أو إذا كان تطبيق هذه الأحكام قد استبعد بموجب إجراء صريح في المحرر الذي يرخص المعالجة[1].

كما نصت المادة 37 من نفس القانون على منع الاستكشاف المباشر، بواسطة آلية اتصال أو جهاز الاستنساخ البعدي أو بريد إلكتروني أو أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة، باستعمال بيانات شخص طبيعي، في أي شكل من الأشكال، لم يعبر عن موافقته المسبقة على ذلك.

غير أنه يرخص بالاستكشاف المباشر عن طريق البريد الالكتروني، إذا ما طلبت البيانات مباشرة من المرسل إليه، وفقا لأحكام هذا القانون، بمناسبة بيع أو تقديم خدمات، إذا كان الاستكشاف المباشر يخص منتجات أو خدمات مشابهة يقدمها نفس الشخص الطبيعي أو المعنوي، وتبين المرسل إليه، بشكل صريح لا يشوبه لبس إمكانية الاعتراض دون مصاريف، باستثناء التكلفة المرتبطة بإرسال الرفض، على استعمال بياناته وقت جمع هذه الأخيرة وكلما وجه إليه بريد إلكتروني لأجل الاستكشاف.

وفي جميع الحالات يمنع إرسال رسائل بواسطة آليات الاتصال الهاتفي وجهاز الاستنساخ البعدي والبريد الالكتروني لأجل الاستكشاف المباشر دون الإشارة إلى بيانات صحيحة لتمكين المرسل إليه من إرسال طلب توقيف هذه الإيصالات دون مصاريف غير تلك المرتبطة بإرسالها.

كما يمنع إخفاء هوية الشخص الذي أو صلت لفائدته الرسائل وكذا ذكر موضوع لا صلة له بالخدمات المقترحة[2].

الفرع الثاني: مسؤوليات والتزامات القائمين بمعالجة البيانات الشخصية

حرص المشرع الجزائري على حماية المعطيات ذات الطابع الشخصي بتكريس جملة من الحقوق لصالح الشخص المعني بمعالجة بياناته، بالإضافة إلى إلزام القائم بالمعالجة ومن يحل محله، من شخص طبيعي أو معنوي أو مصلحة معينة أو أي هيئة مخولة

[1] راجع المادة 36 من القانون 18-07، المرجع السابق، ص19.

[2] راجع المادة 37 من القانون 18-07، المرجع السابق، ص19-20.

بمفردها أو مع أطراف آخرين بتحديد الأهداف من معالجة المعطيات ذات الطابع الشخصي ووسائلها[1]، بجملة من الضوابط تخص مختلف جوانب المعالجة، بمراعاة سرية وسلامة المعالجة، ضبط عملية المعالجة من الباطن، والمعالجة المرتبطة بخدمات التصديق والتوقيع الالكترونيين وكذا الاتصالات الالكترونية، هذا إلى جانب ضبط عملية نقل المعطيات نحو دولة أجنبية، وعليه سيتم التفصيل في كل التزام على النحو التالي:

أولا: الالتزام بسرية وسلامة المعالجة

تتمحور التزامات المسؤول عن المعالجة لضمان سرية وسلامة المعالجة ضمن جملة من التدابير القانونية، التقنية والتنظيمية التي تتماشى وحماية المعطيات ذات الطابع الشخصي، وقد ألزم القانون 18-07 المسؤول عن المعالجة بوضع هذه التدابير لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو التلف أو النشر أو الولوج غير المرخصين، لاسيما إذا استوجبت المعالجة إرسال معطيات عبر شبكة معينة وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة.

ويجب أن تضمن هذه التدابير مستوى ملائما من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها.

وما نستخلصه من خلال هذا الالتزام أن المشرع الجزائري أبقى المجال مفتوحا أمام المسؤول عن المعالجة لفرض ووضع أي تدبير إذا كان الهدف منه هو حماية المعطيات ذات الطابع الشخصي، بحسب أهمية هذه المعطيات والشروط التي تتطلبها لضمان عدم الضياع والتلف أو الولوج غير المشروع.

كما أكد على جانب الحيادية في حالة معالجة معطيات لحساب المسؤول عن المعالجة ونظم المعالجة من الباطن، حيث تم التأكيد على تدابير تخص الالتزام بالسر المهني، وعدم تدخل الغير في المعالجة وهو ما سيتم التفصيل فيه كما يلي:

[1] حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 18-07، المرجع السابق، ص289.

أ. ضوابط حياد المسؤول عن المعالجة وتنظيم عملية المعالجة من الباطن:

أوجب المشرع الجزائري بموجب أحكام المادة 39 من القانون 18-07 المعالجة من الباطن عندما تجرى المعالجة لحساب المسؤول عن المعالجة، وذلك باختيار معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها مع السهر على احترامها.

كما تطرق نص المادة 02 من القانون 18-07 إلى تعريف المعالج من الباطن، بأنه " كل شخص طبيعي أو معنوي، عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة".

وقد تم التأكيد كذلك على تنظيم عملية المعالجة من الباطن بموجب عقد أو سند قانوني يربط المعالج من الباطن بالمسؤول عن المعالجة، يتضمن خصوصا النص على أن لا يتصرف المعالج من الباطن إلا بناء على تعليمات المسؤول عن المعالجة وعلى تقيده بالالتزامات المنصوص عليها في المادة 38 من القانون 18-07، والخاصة بالمسؤول عن المعالجة. وتقيد عناصر العقد أو السند القانوني المتعلق بحماية المعطيات وكذا المتطلبات المتعلقة بالتدابير المنصوص عليها في الفقرة الأولى من المادة 38 من القانون المذكور أعلاه، كتابة أو في شكل آخر معادل، وذلك لأغراض حفظ الأدلة[1].

وتجدر الإشارة إلى أنه يحظر معالجة المعطيات ذات الطابع الشخصي التي يلج إليها المعالج من الباطن دون أخذ تعليمات من المسؤول عن المعالجة، ما عدا حالة تنفيذ التزام قانوني[2].

ب. مراعاة ضوابط السر المهني:

إن مبدأ الحياد والالتزام بكتمان السر المهني يعد واجبا أخلاقيا وقانونيا أكدت عليه مختلف القوانين، لاسيما تلك المتعلقة بدراسة الملفات الخاصة بالأفراد على غرار ضوابط

[1] راجع المادتين 38 و 39 من القانون 18-07، المرجع السابق، ص20.

[2] انظر المادة 41 من القانون 18-07، المرجع السابق.

مهنة المحاماة والتي تلزم المحامي بمراعاة السر المهني[1]، وكذا قانون الوظيفة العمومية الذي يلزم الموظف العمومي بالسر المهني تحقيقا للمصلحة العامة[2].

وكذلك نص القانون رقم 18-07 الذي ألزم صراحة المسؤول عن المعالجة وكل الأشخاص الذين اطلعوا، أثناء ممارسة مهامهم على معطيات ذات طابع شخصي، بالسر المهني، حتى بعد انتهاء مهامهم، تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول[3]، وهو الأمر الذي يعاقب عليه على الخصوص بموجب أحكام المواد 137، 301-303 من قانون العقوبات الجزائري[4].

ثانيا: التزامات معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التوقيع والتصديق الإلكترونيين

أكد المشرع الجزائري بموجب القانون رقم 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[5]، على التزام مؤدي خدمات التصديق الالكتروني بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق[6]، أين اشترط الموافقة الصريحة للشخص المعني قبل قيام مؤدي خدمات التصديق الالكتروني بجمع بياناته الشخصية، وهو ملزم أيضا بجمع البيانات الشخصية الضرورية فقط لمنح وحفظ شهادة التصديق الالكتروني، مع منع استعمال هذه البيانات لمآرب أخرى[7].

---

[1] انظر المادة 13 من القانون رقم 13-07، المؤرخ في 29 أكتوبر 2013، المتضمن تنظيم مهنة المحاماة، الجريدة الرسمية عدد 55 المؤرخة في 30 أكتوبر سنة 2013.

[2] انظر المادة 48 من الأمر 06-03 المؤرخ في 15 يوليو 2006، المتضمن القانون الأساسي العام للوظيفة العمومية، الجريدة الرسمية عدد 46 المؤرخة في 16 يوليو 2006.

[3] انظر المادة 40 من القانون 18-07، المرجع السابق.

[4] راجع المواد 137، 301-303 من الأمر 66-156، المتضمن قانون العقوبات المعدل والمتمم، المرجع السابق.

[5] القانون رقم 15-04 المؤرخ في أول فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية عدد 06 المؤرخة في 10 فبراير 2015.

[6] انظر المادة 42 من القانون 15-04، المرجع نفسه.

[7] انظر المادة 43 من القانون 15-04، المرجع السابق.

وفي نفس السياق أشار نص المادة 42 من القانون 18-07 على أنه يتعين الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني، من الأشخاص المعنيين بها مباشرة، كما يحظر معالجتها لأغراض غير تلك التي جمعت من أجلها، ما عدا في حالة الموافقة الصريحة لأصحاب المعطيات ذات الطابع الشخصي.

ثالثا: التزامات معالجة المعطيات ذات الطابع الشخصي المرتبطة بالاتصالات الإلكترونية.

لقد تم تعريف "الاتصالات الالكترونية" حسب نص المادة 10 من القانون 18-04، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية ب" كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية"[1].

وتجدر الإشارة إلى أن المشرع الجزائري ألزم متعاملي الاتصالات الإلكترونية باتخاذ كل التدابير اللازمة لضمان سرية المكالمات والمعلومات التي يحوزونها عن مشتركيهم، وألا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية من دون الحصول على إذن مسبق من السلطة القضائية المختصة.[2].

حيث كرس نص المادة 160 من نفس القانون حماية المعطيات الشخصية للمشتركين من خلال إلزام المتعاملين وكذا مستخدميهم باحترام سرية المراسلات الصادرة عن طريق الاتصالات الالكترونية وشروط حماية الحياة الخاصة والمعلومات الاسمية للمشتركين.

و بالرجوع إلى أحكام القانون 18-07 لاسيما نص مادته 43 التي أكدت على وجوب الإعلام الفوري للسلطة الوطنية والشخص المعني من قبل مقدم الخدمات، في حالة ما

[1] جاء هذا التعريف مطابقا للتعريف الوارد ضمن نص المادة 02 من القانون 18-07.

[2] انظر المادة 119 من القانون 18-04، المرجع السابق.

أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الاتصالات الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها.

كما تم إلزام مقدم الخدمات بمسك جرد محين حول مختلف الانتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي والإجراءات التي اتخذها بشأنها.

رابعا: الالتزامات المقررة إثر نقل المعطيات نحو دولة أجنبية

إن القاعدة العامة في مجال نقل المعطيات الشخصية نحو بلد أجنبي هي المنع، حيث أشار نص المادة 44 من القانون 18-07 صراحة إلى منع إرسال وتحويل معطيات ذات طابع شخصي إلى دولة أجنبية عندما قد يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة.

وتجدر الإشارة أنه يمكن أن تتم عملية نقل المعطيات في حالة الحصول على ترخيص من قبل السلطة الوطنية المختصة، مع التأكد من أن الدولة التي سيتم نقل المعطيات إليها تكرس مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات الشخصية[1]، أين تم إيراد بعض الاستثناءات، يمكن من خلالها أن يقوم المسؤول عن المعالجة بنقل معطيات ذات طابع شخصي لا تتوفر فيها هذه الشروط، في الحالات الآتية:

1- الموافقة الصريحة للشخص المعني.
2- إذا كان النقل ضروريا:
أ- للمحافظة على حياة هذا الشخص.
ب- للمحافظة على المصلحة العامة.
ت-احتراما لالتزامات تسمح بضمان إثبات أو ممارسة حق أو الدفاع عنه أمام القضاء.

[1] السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي هي المخولة قانونا لتقدير المستوى الكافي من الحماية وكذا الخصائص المتعلقة بالمعالجة وا إجراءات الأمن المطبقة، حسب ما نصت عليه الفقرة الثانية من المادة 44 من القانون 18-07.

ث-تنفيذا لعقد بين المسؤول عن المعالجة والشخص المعني أو تنفيذا لإجراءات سابقة للعقد والمتخذة بناء على طلب هذا الأخير.

ج- لإبرام أو تنفيذ عقد مبرم أو سيبرم بين المسؤول عن المعالجة والغير، لمصلحة الشخص المعني.

ح- تنفيذا لإجراء يتعلق بتعاون قضائي دولي.

خ- للوقاية من إصابات مرضية أو تشخيصها أو معالجتها.

3- إذا تم التنقل تطبيقا لاتفاق ثنائي أو متعدد الأطراف تكون الجزائر طرفا فيه.

4- بناء على ترخيص من السلطة الوطنية، إذا كانت المعالجة تتطابق مع أحكام المادة 2 من القانون 18-07 [1].

والملاحظ من خلال هذا الإجراء هو توسيع المشرع الجزائري لمجالات الترخيص بنقل المعطيات الشخصية إلى الخارج، وهو ما من شأن أن يشكل خطرا على معطيات الأفراد من جهة وكذلك على أمن المؤسسات بالنظر لطبيعة هذه المعطيات من جهة أخرى.

المبحث الثاني: الحماية المؤسساتية والجزائية للبيانات الشخصية في الجزائر

بعد التفصيل في الشروط الوقائية الإجرائية المكرسة لحماية البيانات الشخصية في التشريع الجزائري، سيتم التطرق إلى تفصيل الحماية التي يمكن أن تشملها المؤسسات المنشأة لهذا الغرض، والتي تدخل ضمن السلطات الإدارية المستقلة، والمتمثلة في كل من السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، والتي أقر لها المشرع صلاحيات مباشرة في مجال حماية وضمان المعالجة الشرعية للمعطيات ذات الطابع الشخصي، ثم التطرق إلى دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا ما سيتم التفصيل فيه في المطلب الأول.

[1] انظر المادة 45 من القانون 18-07، المرجع السابق.

أما المطلب الثانيفقد خُصص لتفصيل الآليات الجزائية المكرسة من قبل المشرع الجزائري ضمن مختلف القوانين، لاسيما قانون العقوبات وقانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المطلب الأول: دور السلطات الإدارية المستقلة لحماية البيانات الشخصية

لقد كرس المشرع الجزائري على غرار مختلف التشريعات الدولية الأخرى سلطات إدارية مستقلة تتكفل بحماية البيانات الشخصية بصورة مباشرة أو غير مباشرة، حيث نميز السلطة الأساس المكرسة في إطار حماية الأشخاص الطبيعيين في مجال معالجة معطياتهم ذات الطابع الشخصي، والتي تسمى بموجب أحكام القانون 18-07 ب"السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي"، هذا بالإضافة إلى السلطات المخولة بصفة غير مباشرة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لاسيما عندما يتعلق الأمر بجرائم تخص البيانات الشخصية وتتطلب في متابعتها الحصول على معلومات من خارج التراب الوطني، مما يتيح المجال لطلب المساعدة وتبادل المعلومات قصد جمع الأدلة للتعرف على مرتكبي الجرائم المتصلة بتقنية المعلومات.

الفرع الأول: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

جاء إقرار إنشاء هذه الهيئة تجسيدا لأحكام الدستور الجزائري المعدل سنة 2016، لاسيما أحكام المادة 46 منه، وما تم إقراره بموجب أحكام القانون 18-07، وكذا تأكيد التعديل الدستوري الأخير لسنة 2020، مبدأ تكريس حماية المعطيات الشخصية بموجب أحكام الفقرتين الرابعة والخامسة من المادة 47 منه[1].

[1] نصت المادة 47 من الدستور الجزائري المصادق عليه بموجب استفتاء أول نوفمبر 2020 على ما يلي:
" لكل شخص الحق في حماية حياته الخاصة وشرفه.
لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.
لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.
حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.
يعاقب القانون على كل انتهاك لهذه الحقوق. "

وهي تعد سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، تقيد ميزانيتها في ميزانية الدولة، تعد نظامها الداخلي وتصادق عليه، وعليه سنتطرق بشيء من التفصيل والتقييم لكل من تشكيلة هذه السلطة والصلاحيات المخولة لها لحماية المعطيات ذات الطابع الشخصي كما يلي:

أولا: تشكيلة السلطة الوطنية:

تتشكل السلطة الوطنية من مجموعة من الشخصيات الوطنية، الذين يتم اقتراحهم من مجموعة متجانسة من الهيئات الوطنية لاسيما الدستورية منها، وقد حدد نص المادة الثالثة والعشرين من القانون 18-07، بدقة تشكيلة هذه الهيئة، التي تضم ستة عشر (16)عضوا أساسيا، مع إمكانية الاستعانة بأي شخص مؤهل يمكنه أن يساعدها في مهامها، وحددت كيفية تعيين رئيس وأعضاء السلطة الوطنية، والتي تتم بموجب مرسوم رئاسي لمدة خمس سنوات (05)، قابلة للتجديد، وهم على النحو التالي:

- ثلاث (03) شخصيات، من بينهم الرئيس يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية.
- ثلاث (03) قضاة، يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.
- عضو من كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية.
- ممثل عن المجلس الوطني لحقوق الإنسان.
- ممثل عن وزير الدفاع الوطني.
- ممثل عن وزير الشؤون الخارجية.
- ممثل عن الوزير المكلف بالداخلية.
- ممثل عن وزير العدل، حافظ الأختام.
- ممثل عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة.
- ممثل عن الوزير المكلف بالصحة.

- ممثل عن وزير العمل والتشغيل والضمان الاجتماعي[1].

هذا إلى جانب الأمانة التنفيذية والمستخدمون الذين يتم توظيفهم لمساعدة الأمين التنفيذي للقيام بمهامه.

ومن خلال قراءة في التركيبة الخاصة بممثلي المؤسسات المشكلة لهذه السلطة المستقلة نلاحظ إهمال المشرع لجانب مهم يمكن أن يكون عنصر دعم لهذه التشكيلة ألا وهم الأساتذة الجامعيون والباحثون في مجال الحقوق والحريات وكذا الإعلام الآلي، من أجل الاستفادة من خبرتهم في هذا المجال لاسيما بالرجوع إلى التشريع المقارن والدراسات المنجزة في هذا الإطار، حيث اكتفى المشرع على ذكر تعيين ثلاث شخصيات من بينهم الرئيس، مختصين في مجال عمل السلطة وأبقى المجال مفتوحاً، لاسيما وأن اختصاص السلطة يشمل مجالات عدة تقنية، قانونية، إدارية وشبه قضائية، حيث منحت بعض التشريعات الهيئة المكلفة بحماية البيانات الشخصية صلاحيات تنظيمية وتنفيذية واسعة واعتبرت عدم تنفيذ الأوامر الصادرة عن رئيس الهيئة جريمة، وهو ما ذهب إليه المشرع البريطاني ضمن القانون 98 المتعلق بحماية البيانات الشخصية في البيئة الإلكترونية والذي أنشأ هيئة حماية البيانات الشخصية وسماها " مكتب مفوض حماية البيانات"[2].

ومقارنة بالتشريع التونسي فإن الهيئة الوطنية لحماية المعطيات الشخصية بتونس، تتشكل من خمسة عشر عضوا يعينون بأمر لمدة ثلاث سنوات من بينهم الرئيس يكون من بين الشخصيات المختصة في المجال، وكذا عضو يتم اختياره من بين الخبراء المختصين في مجال تكنولوجيات الإعلام والاتصال[3].

والمشرع المغربي أقر إنشاء اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي سنة 2009 بمقتضى القانون 08-09 الصادر في 18 فبراير 2009،

---

[1] انظر المادة 23 من القانون 18-07، المرجع السابق.

[2] الشيخ الحسين محمد يحي، سيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية، المرجع السابق، ص 52.

[3] راجع الفصل 78 من القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004، المتعلق بحماية المعطيات الشخصية. الموقع الرسمي للهيئة على الإنترنت " http://www.inpdp.nat.tn/Receuil_2019.pdf " تاريخ الاطلاع 2020/01/20.

المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي والتي تتشكل من سبع (07) أعضاء لمدة خمسة سنوات قابلة للتجديد مرة واحدة، أربعة (04) منهم تابعين للسلطة القضائية وممثلين عن السلطة التنفيذية، وتعد الكفاءة والتخصص والنزاهة شروطا أساسية في جميع أعضاء هذه اللجنة[1].

ثانيا: صلاحيات السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تكلف السلطة الوطنية أساساً بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون 18-07 وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار ونتائج سلبية على الحياة الخاصة والحريات العامة وجميع حقوق الأشخاص[2].

وطبقا لنص المادة 25 من القانون 18-07 فإن صلاحيات السلطة الوطنية تتمثل في:

1- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.

2- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.

3- تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.

4- تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وا ٍعلام أصحابها بمآلها.

---

[1] راجع المادتين 02 و03 من المرسوم رقم 09-165 المؤرخ في 21 ماي 2009، المتعلق بتطبيق أحكام القانون 08-09، الصادر في 18 فبراير 2009، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الموقع الرسمي للجنة المغربية على الإنترنت " http://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf " تاريخ الاطلاع: 2020/01/20.

[2] عائشة بن قارة مصطفى، آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم (18-07)، مجلة العلوم القانونية والسياسية، المجلد 10، العدد1، ابريل 2019، ص750.

5- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط القانونية المحددة في هذا الإطار[1].

6- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.

7- الأمر بإغلاق معطيات أو سحبها أو إتلافها.

8- تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

9- نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني لحماية المعطيات ذات الطابع الشخصي.

10- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.

11- إصدار عقوبات إدارية، تتراوح بين الإنذار، السحب المؤقت أو النهائي لوصل التصريح أو الترخيص والغرامة في حالة إخلال المسؤول عن المعالجة بالإجراءات المحددة قانونا[2].

12- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.

13- وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

وتجدر الإشارة إلى أن للسلطة الوطنية صلاحيات موسعة أخرى على غرار القيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها معالجة المعطيات[3]، وفي إطار ممارسة مهامها تعلم النائب العام المختص فور معاينة وقائع تحتمل الوصف الجزائي.

---

[1] وبالرجوع إلى نص المادة 44 من القانون 17-07 فإنه من صلاحية السلطة الوطنية الترخيص للمسؤول عن المعالجة بنقل البيانات الشخصية إلى دولة أجنبية بعد تأكد السلطة من توفر مستوى كاف من الحماية للحياة الخاصة والحقوق والحريات الأساسية للأشخاص والإجراءات الأمنية المناسبة والخصائص المتعلقة بالمعالجة مثل غايتها ومدتها وكذا طبيعة وأصل ووجهة هذه المعطيات المعالجة على مستوى هذه الدولة، كما أنه يمنع إرسال وتحويل معطيات ذات طابع شخصي إلى دولة أجنبية في حالة إمكانية مساسها بالأمن العمومي أو المصالح الحيوية للدولة.

[2] راجع المادة 46 من القانون 18-07، المرجع السابق.

[3] راجع المادة 49 من القانون 18-07، المر جع السابق.

كما أن المسؤول عن معالجة المعطيات مطالب بالالتزام بالتعاون مع السلطة الوطنية وفي حالة العكس وعرقلة عمل السلطة من حيث الاعتراض على إجراء عملية التحقيق في عين المكان، أو رفض تزويد أعضائها أو الأعوان الذين هم تحت تصرفها بالوثائق المطلوبة للقيام بالمهام المسندة لهم من طرف السلطة الوطنية، أو إرسال معلومات غير مطابقة لمحتوى السجلات وقت تقديم الطلب أو عدم تقديمها بشكل واضح ومباشر، ويعد من بين أشكال عرقلة عمل السلطة إرسال وثائق ناقصة أو تحتوي جملة من الأخطاء المقصودة لعدم معرفة الحقيقة وبهذا يعد المسؤول عن المعالجة مرتكباً لجريمة تتضمن عقوبات منصوص عليها ضمن نص المادة 61 من القانون 18-07 [1].

ومن أجل ضمان النزاهة لأعضاء السلطة عند قيامهم بمختلف المهام فتم تحديد جملة من الضوابط يمكن تلخيصها على النحو التالي:

- يتعين على رئيس وأعضاء السلطة الوطنية بالمحافظة على الطابع السري للمعطيات ذات الطابع الشخصي للمعلومات التي اطلعوا عليها ولو بعد انتهاء مهامهم.

- لا يجوز لرئيس و أعضاء السلطة الوطنية امتلاك مصالح في أي مؤسسة تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي.

- إنشاء سجل وطني لحماية المعطيات ذات الطابع الشخصي، يمسك من طرف السلطة وتقيد فيه مختلف الملفات موضوع المعالجة من قبل السلطات العمومية أو من قبل الخواص، وكذا مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية، كما تقيد فيه جميع التصريحات المقدمة للسلطة الوطنية والتراخيص المسلمة وغيرها من المعطيات الضرورية المخول للأشخاص الاطلاع عليها وفق الإجراءات المحددة قانونا أو تنظيما.

كما أن السلطة الوطنية لحماية المعطيات تعد جهازا فعالا لضبط مختلف آليات المعالجة، بحيث منحها المشرع جملة من الصلاحيات الإجرائية إلى الرقابية والردعية من

[1] يحي تومي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد رقم04، العدد رقم 02، سنة 2019، ص1546.

أجل تكريس حماية فعالة للمعطيات ذات الطابع الشخصي، بحيث يمكنها أن تتخذ كل الإجراءات والتدابير المناسبة والعقوبات الإدارية التي تشمل الإنذار، الإعذار، السحب المؤقت أو النهائي لوصل التصريح أو الترخيص وكذا إصدار غرامة قدرها 500.000دج ضد كل من يقوم بالرفض دون سبب شرعي حقوق الإعلام والولوج أو التصحيح أو الاعتراض، المكرسة لصاحب المعطيات[1]. أو الذي لا يقوم بالتبليغ المنصوص عليه في القانون 18-07[2].

هذا إلى جانب قيام السلطة الوطنية بجميع التحريات والمعاينات الميدانية للأماكن والمحلات التي تتم فيها المعالجة، مع التقيد بمراعاة حرمة المسكن، كما يمكنها الولوج إلى مختلف الوثائق والمعلومات مهما بلغت درجة سريتها أو الدعامة التي تتضمنها[3].

إلا أنه وبالرغم من مرور أزيد من ثلاث (03) سنوات على إقرار إنشاء هذه السلطة قانوناً إلا أنه لم يتم تنصيبها فعليا سواء من حيث بسط هيكلها التنظيمي أو تعيين أعضائها مما يبقي هذه الآلية مجرد حبر على ورق، بالرغم من إقرار المشرع ضمن القانون 18-07، في بابه السابع الخاص بالأحكام النهائية والانتقالية إلى أن الأشخاص الذين يمارسون نشاط معالجة المعطيات ذات الطابع الشخصي ملزمون بالامتثال لأحكام هذا القانون- أي القانون 18-07 – في أجل أقصاه سنة (01) من تاريخ تنصيب السلطة الوطنية وفقا لنص المادة 75 من القانون 18-07.

حيث تجدر الإشارة وبالرجوع إلى العديد من التشريعات الدولية فإن السلطة الإدارية المستقلة لحماية المعطيات الشخصية تلعب دورا محوريا في حماية المعطيات بإصدارها لجملة من القرارات الآنية والملزمة فور تلقي عرائض أو شكاوى من طرف الأشخاص المعنيين في حالة وقوع مخالفات اثر معالجة معطياتهم الشخصية.وعليه فإن دور السلطة

[1] كحلاوي عبد الهادي، بن زيطة عبد الهادي، آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، المجلد 07، العدد02، 2021، ص 123.

[2] راجع أحكام المادة 47 من القانون 18-07، المرجع السابق.

[3] راجع أحكام المادة 49 من القانون 18-07، المرجع السابق.

الوطنية بالإضافة إلى تنظيم معالجة المعطيات وا ٍنزال عقوبات إدارية وشبه قضائية ضد المخالفين فإنها توجه وترافق القائمين بالمعالجة للمعطيات ذات الطابع الشخصي وكذا مساعدة وتوجيه أصحاب المعطيات موضوع المعالجة[1].

يمكن للسلطة الوطنية، كذلك، تحريك الدعوى في أي جريمة تقع مخالفة لقانون حماية المعطيات وهو ما ذهب إليه المشرع البريطاني حيث أقر لفوض البيانات إمكانية تحريك الدعوى إلى جانب النيابة العامة حسب ما تضمنه الفصل 60 من قانون حماية البيانات البريطاني لسنة 1998[2].

الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

كرس المشرع الجزائري إنشاء هذه الهيئة الوطنية المستقلة، بموجب أحكام المادة 13 من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما تم الإحالة إلى التنظيم لضبط تشكيلتها، تنظيمها وكيفيات سيرها، هذا التنظيم الذي لم يصدر إلا بعد حوالي ست سنوات من صدور القانون، أي بصدور المرسوم الرئاسي رقم 15-261، المؤرخ في 08 أكتوبر 2015[3]، إلا أن هذا المرسوم تم إلغاؤه سنة 2019 بموجب المرسوم الرئاسي رقم 19-172، ليعاد تنظيم هذه الهيئة بموجب هذه الأخير، ليتم إلغاؤه كذلك سنة 2020 بموجب المرسوم الرئاسي 20-183[4] ويعاد تنظيم هذه الهيئة بموجب أحكام المرسوم الرئاسي 21-439

[1] خالدي فتيحة، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كآلية لحماية الحق في الخصوصية، مجلة الحقوق والعلوم الإنسانية، المجلد 13، العدد 04(2020)، ص55.

[2] الشيخ الحسين محمد يحي، سيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية، المرجع السابق، ص 53.

[3] المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 53 المؤرخة في 08 أكتوبر 2015.

[4] المرسوم الرئاسي 20-183 المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 40 المؤرخة في 18 يوليو 2020.

المؤرخ في 07 نوفمبر 2021، الساري المفعول[1]. وما يلاحظ من خلال هذه التغييرات في فترات متقاربة بخصوص هذه الهيئة هو التردد في ضبط الإطار التنظيمي لهذه الهيئة نظرا لدورها الحساس والبالغ الأهمية[2]، لاسيما بالنسبة لحماية المعطيات الشخصية، التي تكون موضوع جرائم متصلة بتكنولوجيات الإعلام والاتصال، حيث في هذا الصدد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، السالفة الذكر، على حوالي عشر (10) جرائم تخص المعطيات الشخصية، وهو ما يجسد أهمية دور هذه الهيئة إلى جانب السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وعلية سيتم التطرق إلى تشكيلة وسير هذه الهيئة وكذا الصلاحيات المخولة لها قانونا في هذا المجال، وفق ما تضمنه المرسوم الرئاسي رقم 21-439، والذي أشار إلى أن هذه الهيئة تعد سلطة إدارية مستقلة، تتمتع بالشخصية المعنوية والاستقلال المالي[3].

أولا: تشكيلة وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

سيتم التطرق إلى تشكيلة وسير هذه الهيئة بالرجوع إلى أحكام المرسوم الرئاسي المنظم لها، على النحو الموالي:

1. تشكيلة الهيئة:

أشار نص المادة 05 من المرسوم الرئاسي 21-439 إلى أن الهيئة تتشكل من مجلس توجيه ومديرية عامة توضعان تحت سلطة رئيس الجمهورية.

---

[1] المرسوم الرئاسي 21-439 المؤرخ في 07 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 86 المؤرخة في 11 نوفمبر 2021.

[2] بعد إجرائنا لمقارنة شكلية بين مختلف المراسيم الرئاسية السابقة المنظمة للهيئة مع أحكام المرسوم الرئاسي رقم 21-439، تبين أن التعديلات شملت كل من المادة 02 فيما يخص وضع الهيئة لدى رئيس الجمهورية وفي سنة 2015 كرس النص وضعها لدى الزير المكلف بالعدل، هذا بالإضافة إلى تعديل وتوسيع صلاحيات الهيئة، المحددة بنص المادة 04 حيث تم إدراج صلاحية ضمان المراقبة الالكترونية عندما يتعلق الأمر بأمن الجيش.، هذا بالإضافة رئاسة مجلس التوجيه التي كانت موضوعة تحت رئاسة رئيس الجمهورية وبحضور بعض الوزراء المعنيين، تم إسنادها للأمين العام لرئاسة الجمهورية وبعضوية الأمناء العامون لبعض الوزارات إلى جانب الأجهزة الأمنية المعنية.

[3] انظر المادة 02 من المرسوم الرئاسي رقم 21-439، المرجع السابق.

1.1 مجلس التوجيه:

تم تحديد تشكيلة مجلس التوجيه بموجب نص المادة 06 من المرسوم الرئاسي المذكور أعلاه، والتي أشارت إلى أن رئاسة المجلس تعهد للأمين العام لرئاسة الجمهورية، وتضم التشكيلة الأعضاء التاليين:

- الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج.
- الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية.
- الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية.
- قائد الدرك الوطني.
- المدير العام للأمن الداخلي.
- المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي
- المدير العام للأمن الوطني.
- رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي.
- ممثل عن رئاسة الجمهورية، يعينه رئيس الجمهورية.

والملاحظ من خلال هذه التشكيلة هو حصر عضويتها نظرا لحساسية الموضوع، إلا أنه كان من الأحسن فتح المجال لبعض الخبراء الأمنيين في مجال الجرائم الالكترونية، أو غير هم من الخبراء الباحثين في هذا المجال للاستفادة من خبراتهم، بشرط ضمان الكفاءة والنزاهة.

1.2 المديرية العامة:

يشرف على المديرية العامة مدير عام، يعين بموجب مرسوم رئاسي، تسند له جميع مهام التسيير الإداري والمالي والتمثيل القضائي في أعمال الحياة المدنية للهيئة[1].

[1] راجع المواد 9 و10 من المرسوم الرئاسي 21-439، المرجع السابق.

كما تضم المديرية العامة كل من مديرية المراقبة الوقائية واليقظة الالكترونية، مديرية الإدارة والوسائل، مصلحة للدراسات والتلخيص، مصلحة للتعاون واليقظة التكنولوجية وملحقات جهوية، يتم تعيين كل مسؤول لهذه الفروع بموجب مرسوم رئاسي، بناء على اقتراح من المدير العام للهيئة، كما تنهى مهامه بنفس الطريقة[1].

2. سيـــــر الهيئة:

وضح نص المادة 20 من التنظيم المتعلق بالهيئة بأنه لضمان سير هذه الهيئة فإنه يلحق بها قضاة وضباط وأعوان للشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والأمن الوطني[2]، بالإضافة إلى مستخدمي الدعم التقني والإداري للمصالح العسكرية والأمن الوطني، كما يمكن للهيئة توظيف فئات أخرى، حسب الحاجة[3].

حيث تم التأكيد على إلزام المستخدمين بالسر المهني وواجب التحفظ، مع تأكيد تأديتهم لليمين، المحدد نصها بموجب أحكام المادة 22 من المرسوم الرئاسي المذكور.

وقد تم منح صلاحيات لمستخدمي الهيئة المؤهلين لطلب أي وثائق أو تسجيل ومراقبة اتصالات إلكترونية، مع التأكيد على أن تحفظ المعلومات المستقاة أثناء عملية المراقبة، خلال حيازتها من طرف الهيئة، وفقا للقواعد المطبقة على حماية المعلومات المصنفة. وفي هذا الإطار تجدر الإشارة أن المشرع الجزائري بموجب الأمر 21-09، المتعلق بحماية المعلومات والوثائق الإدارية[4]، كرس حماية المعلومات والوثائق المصنفة المتعلقة بالدولة ومؤسساتها وهيئاتها التشريعية والقضائية والتنفيذية والإدارات العمومية والجماعات المحلية وكل مؤسسة تملك الدولة كل أو بعض رأسمالها وكل مؤسسة تقدم خدمة

[1] انظر المادتين 11 و12 من المرسوم الرئاسي 21-439، المرجع السابق.

[2] تم الإشارة ضمن نص المادة 20 بأن العدد المطلوب من ضباط وأعوان الشرطة القضائية المؤهلين، يتم تحديده بموجب قرارات مشتركة بين وزير الدفاع الوطني والوزير المكلف بالداخلية والأمين العام لرئاسة الجمهورية.

[3] انظر المادتين 20 و21 من المرسوم الرئاسي 21-439، المرجع السابق.

[4] الأمر 21-09 المؤرخ في 08 يونيو 2021، المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية عدد 45 المؤرخة في 09 يونيو 2021.

عمومية[1]. كما تم تعريف المعلومات والوثائق المصنفة موضوع الحماية بموجب أحكام المادة 03 من الأمر 21-09 كما يلي:

- **"المعلومات:** أي حدث أو خبر مهما كان مصدره، وثيقة أو صورة أو شريط صوتي مرئي أو سمعي بصري أو محادثة أو مكالمة هاتفية، يؤدي الكشف عنها إلى المساس بالسلطات المعنية".

- **"الوثائق المصنفة:** أي مكتوب ورقي أو إلكتروني أو رسم أو مخطط أو خريطة أو صورة أو شريط صوتي أو سمعي بصري أو أي سند مادي إلكتروني آخر كانت محل تدابير ترمي إلى منع نشرها أو تقييد الاطلاع عليها".

كما تم تحديد تصنيف الوثائق، حسب درجة حساسيتها بموجب أحكام المادة 06 من الأمر 21-09 إلى أربعة (04) أصناف: "

- **"سري جدا":** يتضمن الوثائق التي يلحق إفشاؤها خطرا بالأمن الوطني الداخلي والخارجي.

- **"سري":** يتضمن الوثائق التي يلحق إفشاؤها ضررا خطيرا بمصالح الدولة.

- **" واجب الكتمان":** يتضمن الوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الحكومة أو الوزارات أو الإدارات أو إحدى الهيئات العمومية.

- **"توزيع محدود":** يتضمن الوثائق التي يؤدي إفشاؤها إلى المساس بمصالح الدولة ولا يجوز الاطلاع عليها إلا من قبل الأشخاص المؤهلين بحكم الوظيفة أو المهمة.

كما تجدر الإشارة إلى أن المشرع أحال إلى التنظيم لضبط شروط وكيفيات التطبيق وكذا كل ما يتعلق بتحسيس وتكوين موظفي السلطات العمومية في استعمال المعلومات والوثائق المصنفة[2].

[1] انظر المادة 02 من الأمر 21-09، المرجع نفسه.

[2] انظر المادتين 06 و07 من الأمر 21-09، المرجع السابق.

ثانيا: مهام وصلاحيات الهيئة الوطنية

حدد نص المادة 14 من القانون 09-04 مهام الهيئة بصفة إجمالية كما يلي:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وا إنجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم[1].

كما أورد تفصيلا نص المادة 4 من المرسوم الرئاسي 21-439، مهام هذه الهيئة كما يلي:

- تحديد الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ.

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- ضمان المراقبة الوقائية للاتصالات الالكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التي تمس بأمن الدولة.

كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني، المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش.

[1] راجع المادة 14 من القانون 09-04، المرجع السابق.

- تجميع وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

- المساهمة في تحيين المعايير القانونية في مجال اختصاصها.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، عن طريق جمع المعلومات والتزويد بها وا ٍنجاز الخبرات القضائية.

- تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- السهر على تنفيذ طلبات المساعدة القضائية الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها[1].

وفي إطار تبادل المعلومات والتعاون الدولي، يتعين إبرام اتفاقيات ثنائية تخص مجال مكافحة الجرائم الماسة بأنظمة معالجة البيانات الشخصية، في إطار تكريس مبدأ السيادة وضمان حقوق الأفراد[2].

وتجدر الإشارة إلى أن التكريس الفعلي لتنصيب هذه الهيئة من شأنه تكريس حماية من مختلف الجرائم المتعلقة بتقنية المعلومات، بصفة عامة وتكريس حماية خاصة بالنسبة للبيانات الشخصية المعالجة آليا، إلا أن التأخر في تنصيب مثل هذه الهيئات على غرار السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من شأنه أن يفرغ هذا الإجراء من محتواه، موازاة مع تزايد الجريمة الالكترونية التي تستهدف المعطيات الشخصية للأشخاص الطبيعيين والاعتباريين على حد السواء.

[1] راجع المادة 4 من المرسوم الرئاسي 21-439، المرجع السابق.

[2] الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات- دراسة مقارنة-، المرجع السابق، ص331.

المطلب الثاني: الحماية الجزائية للبيانات الشخصية في القانون الجزائري

بالرغم من الضمانات التي كرسها الإطار الإجرائي والمؤسساتي لحماية البيانات الشخصية إلا فعالية هذه الآليات تبقى نسبية مقارنة بالآليات الجزائية التي تمثل أنجع آلية لحماية البيانات الشخصية سواء من ناحية الجهاز الذي يقوم على ضمانتها أو من ناحية الجزاءات التي تتضمنها، وعليه نتطرق بالتفصيل لمختلف الآليات الجزائية التي تضمنها كل من قانون العقوبات وقانون الإجراءات الجزائية (الفرع الأول) وكذا الجزاءات التي تضمنتها مختلف القوانين الأخرى على غرار قانون حماية المعطيات ذات الطابع الشخصي (الفرع الثاني).

الفرع الأول: الجزاءات المقررة بموجب قانوني الإجراءات الجزائية والعقوبات

لقد حدد المشرع بموجب الأمر 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم جملة من الإجراءات لحماية الحياة الخاصة بصفة عامة، وكذا مكافحة الجريمة المعلوماتية بصفة خاصة، لاسيما ما أقره القانون 06-22 [1]، المعدل والمتمم للأمر 66-155، من تأكيد على حرمة الحياة الخاصة وسرية التحقيقات، لاسيما في الاستثناءات التي تقتضيها الضرورة كتلك المتعلقة بالتحري عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. وكذلك الأمر 66-156، المتضمن قانون العقوبات، المعدل والمتمم، تضمن الفصل الثالث ضمن قسمه السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات جملة من العقوبات المتعلقة بجرائم التصميم، البحث، التجميع، التوفير، النشر أو الاتجار في المعطيات.

وعليه سيتم التفصيل في كل الجزاءات المقررة بموجب قانوني الإجراءات الجزائية والعقوبات في النقطتين المواليتين:

[1] القانون 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 84 المؤرخة في 24 ديسمبر 2006.

أولا: الجزاءات المقررة بموجب قانون الإجراءات الجزائية:

لقد كرس قانون الإجراءات الجزائية مجموعة من الضمانات تمنع إساءة استعمال السلطة لانتهاك حرمة الحياة الخاصة حيث تم اشتراط الإذن بالتفتيش الصادر عن وكيل الجمهورية أو قاضي التحقيق ويكون مكتوبا يوضح بدقة أماكن التفتيش مع اشتراط حضور صاحب المسكن المعني أثناء التفتيش أو ممثلا عنه وعند التعذر يتم بحضور شاهدين[1].

كما كرس المشرع الجزائري إجراءات استثنائية للتحري عن الجرائم الالكترونية، لاسيما تلك المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث تم تخصيص الفصل الرابع من قانون الإجراءات الجزائية لبسط إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتي يمكن اللجوء إليها لضرورات التحري في الجريمة، حيث تم الترخيص باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، تحت الرقابة المباشرة لوكيل الجمهورية المختص[2].

كما جاء في نص المادة 46 من نفس القانون بأنه "يعاقب بالحبس من شهرين إلى سنتين وبغرامة تتراوح بين 2000 إلى 20.000 دج كل من أفشى مستندا ناتجا من التفتيش أو أطلع عليه شخصا لا صفة له قانونا في الاطلاع عليه وذلك بغير إذن من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى ذلك".

وما يتضح من خلال نص هذه المادة عناية المشرع الجزائري بحماية الخصوصية لاسيما في جانبها المتعلق بحماية المراسلات والمستندات الشخصية حتى وا ٍن كان المعني بالإجراء مشتبها فيه.

وبالإضافة إلى منع إفشاء المعلومات المتحصل عليها خلال عملية التفتيش فإن المشرع ضبط وقيد الحيز الزمني لهذه العملية عندما يتعلق الأمر بالمسكن الخاص

[1] انظر المادة 44من قانون الإجراءات الجزائية، المرجع السابق.

[2] راجع المادة 65 مكرر من الأمر 66-155، المرجع السابق.

بالمشتبه فيه حيث حدد توقيت التفتيش بين الخامسة (05:00) صباحا والثامنة (20:00) مساء إلا إذا أذن صاحب المسكن خارج ذلك أو وجهت نداءات من الداخل في أمور مضبوطة قانونا، إلا أنه ما يعيب هذا التقييد هو في حالة تم الانطلاق في التفتيش خلال الوقت المسموح به ولم تكتمل عملية التفتيش فكيف يكون الإجراء[1]؟

وبالموازاة فقد تم إطلاق توقيت التفتيش عندما يتعلق الأمر بجرائم تم حصرها ضمن نص الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية[2] و التي من ضمنها الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات بصفة عامة والمعطيات الشخصية بصفة خاصة، وهذا ما يبرز جليا اهتمام المشرع ومنذ سنة 2006 بمجال حماية المعطيات الشخصية أو ذات الطابع الشخصي إلا أن النص الخاص لم يصدر إلا بعد اثنا عشر (12) سنة من هذا التاريخ ضمن القانون 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ثانيا: الجزاءات المقررة بموجب قانون العقوبات:

لقد كفل المشرع الجزائري جانبا من المعطيات الشخصية، لاسيما من خلال تعديل قانون العقوبات لسنة 2004 بموجب القانون 04-15[3] ضمن قسمه السابع المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات بعد استحداث مواد جديدة من المادة رقم 394 مكرر إلى المادة 394 مكرر7. كما تضمن التعديل الصادر سنة 2006، بموجب القانون 06-23 المؤرخ في 20 ديسمبر 2006، أحكاما تخص الاعتداء على الخصوصية باستعمال تقنيات رقمية، من خلال نص المواد من 303 إلى 303

[1] راجع المادة 47 من قانون الإجراءات الجزائية، المرجع السابق

[2] جاء نص الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية كما يلي: "وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

[3] الشيخ الحسين محمد يحي، سيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية، المرجع السابق، ص 53.

مكرر02، والتي نصت، كما سيتم التفصيل فيه أدناه، على الجرائم المتصلة بنظام الإخلال بالمعالجة الآلية للمعطيات في مختلف جوانبها.

وفي هذا الإطار تضمنت المادة 394 مكرر عقوبة السجن من ثلاثة (03) أشهر إلى سنة وغرامة مالية من 50.000دج إلى 100.000 دج نتيجة الدخول أو البقاء عن طريق الغش ضمن منظومة للمعالجة الآلية للمعلومات وفي حالة حذف أو تغيير لمعطيات هذه الأخيرة فإن العقوبة تضاعف[1].

أما في حالة إدخال أو إزالة أو تعديل عن طريق الغش لمعطيات في نظام المعالجة الآلية فإن العقوبة تشدد حيث تتراوح مدة الحبس بين ستة (06) أشهر وثلاث سنوات وبغرامة بين 500.000 دج و200.000 دج [2].

كما نصت المادة 303 مكرر على ترتيب جزاءات ضد الجرائم الماسة بحرمة الحياة الخاصة للأشخاص، بأي تقنية مستعملة، للقيام بالتقاط أو تسجيل أو نقل مكالمات وأحاديث خاصة أو سرية، بدون إذن أو رضا صاحبها، بحيث تتراوح العقوبة بين 06 أشهر إلى 03 سنوات سجن وبغرامة من 50.000 إلى 300.000دج، كما أشار نص المادة 303 مكرر1 إلى ترتيب نفس العقوبة ضد كل من احتفظ أو وضع في متناول الجمهور أو الغير، أو استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المذكورة أعلا. هذا بالإضافة إلى تطبيق نفس العقوبات في حالة الشروع فقط في ارتكاب الجنحة بالعقوبات المقررة للجريمة التامة[3].

ورتب كذلك المشرع الجزائري بموجب نص المادة 394 مكرر2 عقوبة الحبس من شهرين (02) إلى ثلاث سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج كل من يقوم عمدا أو عن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن

[1] راجع المادة 394 مكرر من قانون العقوبات، المرجع السابق

[2] انظر المادة 394 مكرر 1 من قانون العقوبات، المرجع السابق.

[3] انظر المادة 303 مكرر1 من الأمر 66-156، المرجع السابق.

ترتكب بها الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، والجزاء نفسه لمن يقوم بحيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها ضمن نفس القسم.

وحسب مضمون نص المادة 394 مكرر3، فإن العقوبات السالفة الذكر تضاعف في حالة استهداف الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

وقد اعتبر المشرع مجرد الشروع في ارتكاب المخالفات المنصوص عليها ضمن هذا القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات جزاؤه نفس جزاء القيام بالمخالفة كاملة، بالإضافة إلى التأكيد على مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في هذا الفرع وكذا إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها[1].

الفرع الثاني: الجزاءات المقررة بموجب القانون 18-07 المتعلق بحماية المعطيات الشخصية

حدد المشرع بموجب أحكام القانون 18-07، جملة من الشروط للقيام بمعالجة المعطيات ذات الطابع الشخصي رتب على عدم مراعاتها أو الإخلال بها جملة من الجزاءات ويكون ذلك إما نتيجة المعالجة قبل الحصول على موافقة المعني أو بعد اعتراضه (الفرع الأول) أو بالإخلال بالإجراءات المسبقة المتعلقة بمنح التصريح أو الترخيص من قبل السلطة الوطنية لحماية المعطيات الشخصية (الفرع الثاني).

أولا: تجريم مساس عملية المعالجة بحرمة الحياة الخاصة والحريات العامة:

أكد نص المادة 02 من القانون 18-07 على وجوب احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، خلال كل عملية معالجة للمعطيات ذات الطابع الشخصي، كما يجب ألا تمس، هذه الأخيرة بحقوق الأشخاص وشرفهم وسمعتهم.

[1] انظر المادتين 394 مكرر6 و394 مكرر 7 من قانون العقوبات، المرجع السابق.

ورتب المشرع ضمن نص المادة 54 على أنه يعاقب على خرق أحكام المادة 2، المشار إلي مضمونها أعلاه، ب"الحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة من 200.000دج إلى 500.000دج."[1].

وتجدر الإشارة أن المادة 02 اشتملت على تدابير تخص مجالا عاما باشتراط مراعاة الحريات العامة ومختلف جوانب الحياة الخاصة، حتى أنه ذهب البعض إلى أن هناك صعوبة في تحديد الحالات التي يمكن أن تدخل في مجال هذه المخالفة بالنظر للمصطلحات المستعملة في نص هذه المادة، إلا أنه وباعتبار سكوت المشرع عن توضيح تفاصيل المخالفة يؤكد أنه يخص التصرف العمدي، مما يقتضي توسيع مجال التجريم ليشمل مختلف الجوانب المتعلقة بحماية الخصوصية في إطار المعالجة للمعطيات الشخصية، من أجل حث القائمين على المعالجة بأخذ احتياطاتهم والتحلي بالدقة والحس المهني العالي تجنبا لأي عواقب سلبية على الشخص المعني بالبيانات[2].

ثانيا: تجريم المعالجة بدون تصريح أو ترخيص من السلطة الوطنية:

لقد رتب المشرع الجزائري جملة من الإجر اءات والشروط الواجب مراعاتها قبل الشروع في أي عملية معالجة للمعطيات ذات الطابع الشخصي، وفي حالة مخالفة ذلك فإن المعالج يكون قد اقترف جريمة ركنها المادي يتجسد في السلوك الإجرامي والمتمثل في الجمع أو الشروع في المعالجة غير المشروعة أو غير المرخصة من قبل الهيئة المخولة قانونا، أما ركنها المعنوي فيتمثل في التهاون في هذه الشكليات التي تخص المعالجة المتعلقة ببيانات شخصية، وقد أقرت محكمة النقض الفرنسية ثبوت الجريمة بمجرد عدم مراعاة الجانب الشكلي، في المعالجة، وذلك بافتراض الركن المعنوي، وليس للمتهم أي مجال للتبرير والبراءة من التهمة إلا في حالة ثبوت القوة القاهرة[3]. كما رتب المشرع الجزائري على مخالفة الإجراءات المنصوص عليها في المادة 12 من القانون 18-07،

[1] انظر المادة 54 من القانون 18-07، المر جع السابق.

[2] نبيلة رزاقي، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي -دراسة مقارنة-، مجلة الدراسات القانونية المقارنة، المجل07، العدد 01، 2020، ص-2006-2007.

[3] نبيلة رزاقي، المرجع نفسه، ص2001-2002.

عقوبة بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500.000دج لكل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي. كما تم التأكيد على أنه يعاقب بالمثل كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له [1].

وما يستخلص من خلال هذه الجريمة أنها تستوجب إذا تم انجاز المعالجة أو الأمر بذلك، أما عملية الحذف والتي تناقض الانجاز منطقيا، فإنها لا تدخل في إطار هذه الجريمة المعاقب عليها بموجب نص المادة 56 من القانون 18-07.[2]

كما رتب المشرع الجزائري بموجب نص المادة 58 من نفس القانون، عقوبة لتجاوز حدود الترخيص أو التصريح بالحبس لمدة تتراوح من ستة أشهر إلى سنة وبغرامة من 60.000دج إلى 500.000دج أو بإحدى هاتين العقوبتين فقط، كل من قام بانجاز أو استعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها من قبل السلطة الوطنية [3].

وفي السياق ذاته تم تحديد ضوابط تخص نقل البيانات نحو دولة أجنبية نظرا لحساسية هذا الإجراء حيث تم إلزام المعالج الراغب في نقل المعلومات نحو دولة أجنبية بالحصول على ترخيص من السلطة الوطنية، بينما تم تقييد نقل بعض الأنواع من البيانات أو حظر نقلها كلية، حيث يتطلب نقل المعطيات الصحية المستعجلة الحصول على موافقة صريحة للشخص المعني، ويوجد حالات يمنع فيها نقل المعطيات عندما قد يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة[4].وقد تم إقرار عقوبة الحبس من سنة (01) إلى خمس (05) سنوات وبغرامة من 500.000دج إلى 1000.000دج ضد كل

---

[1] راجع المادة 56 من القانون 18-07، المرجع السابق.

[2] طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري – دراسة في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للباحث، العدد 02-2018، ص 40.

[3] انظر المادة 58 من القانون 18-07، المرجع السابق.

[4] راجع المادتين 44 و45 من القانون، 18-07، المرجع السابق.

من يقوم بنقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادة 44 من القانون 18-07 [1] .

والملاحظ في هذا الجانب ترتيب المشرع الجزائري ضمن نص القانون 18-07 أقصى عقوبة من بين العقوبات الواردة ضمن نص هذا القانون، نتيجة خرق أحكام المادة 44، وهو ما يكرس أكثر حماية لهذا النوع الحساس من المعطيات ذات الطابع الشخصي، بالنسبة للشخص المعني و المصلحة العامة للوطن بعلاقة متعدية.

ثالثا: تجريم المساس بالقواعد الشكلية للحماية والتعاون مع السلطة الوطنية لحماية المعطيات

تعد السلطة الوطنية لحماية المعطيات الشخصية وسيلة فعالة في بسط الرقابة على معالجة المعطيات ذات الطابع الشخصي، وفي إطار القيام بدورها الهام فإن لها أن تستعين بأعوان رقابة آخرين متخصصين بالإضافة إلى ضباط وأعوان الشرطة القضائية وقد رتب المشرع وفقا لأحكام المادة 61 من القانون 18-07 عقوبات بين الحبس من ستة (06) أشهر إلى سنتين (02) وبغرامة من 60.000دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط حسب حجم العرقلة وتقدير القاضي المختص ضد كل من يقوم بتعطيل عمل السلطة الوطنية سواء بالاعتراض عن إجراء عملية التحقق في عين المكان أو عند رفض تزويد أعضاء السلطة أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم أو القيام بإخفاء أو إزالة الوثائق أو معلومات تفيد في التحقيق أو بإرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح[2].

ومن خلال استقراء مضمون هذه المادة نلاحظ اعتماد المشرع على صيغة التعميم وعدم ضبط أو تخصيص المخالفات بالمسؤول عن المعالجة أو تحديد صفة المعالج وا ٍنما أبقى على الصيغة بصفة عامة لتشمل أي فعل يعطل عمل السلطة بغض النظر عن

[1] انظر المادة 67 من القانون 18-07، المرجع السابق.

[2] انظر المادة 61 من القانون 18-07، المرجع السابق.

مرتكب هذه المخالفة، حتى وا ٍن كان مجر د الامتناع عن القيام بإجراء محدد أو حتى القيام بفعل إيجابي[1].

كما نصت المادة 66 على تجريم امتناع مقدمي الخدمات[2]، عن إعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية، خلافا لأحكام المادة 43 والتي تلزم مقدم الخدمات بإعلام السلطة الوطنية في حالة ما أدت معالجة المعطيات في شبكات الاتصالات الالكترونية[3]، إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المر خص إليها[4].

رابعا: تجريم المعالجة والاستعمال غير المشروع للمعطيات ذات الطابع الشخصي

تتجسد المعالجة غير المشروعة للمعطيات ذات الطابع الشخصي في مخالفة أحكام المادة 07 من القانون 18-07، والمتعلقة بضرورة الحصول على موافقة الشخص المعني، حيث أكد نص هذه المادة على شرط الحصول على موافقة الشخص المعني قبل الشروع في أي عملية معالجة للمعطيات ذات الطابع الشخصي، إلا في حالات حددها المشرع على سبيل الحصر ضمن نفس المادة[5].

وقد تم تجريم كل من يخالف الإجراء المنصوص عليه في المادة أعلاه، نظرا لكون موافقة الشخص المعني تعد أهم شرط في معالجة المعطيات الشخصية، لذلك رتب المشرع على ارتكاب هذه الجريمة عقابا بالحبس من سنتين (02) إلى خمس (05)

---

[1] تومي يحي، المرجع السابق، ص1547.

[2] عرف "مقدم الخدمات" بموجب نص المادة 3 من القانون 18-07 وهو " 1- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات. 2/ أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو للمستعملين".

[3] عرفت "الاتصالات الالكترونية " حسب نص المادة 03 من القانون 18-07 " كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية".

[4] راجع المادتين 43 و66 من القانون 18-07، المرجع السابق.

[5] كما تجدر الإشارة إلى ورود استثناء آخر يخص المعطيات الحساسة المنصوص عليه ضمن المادة 18 من القانون 18-07.

سنوات، وبغرامة من 100.000دج إلى 500.000دج [1]. وفي حالة القيام بالمعالجة بالرغم من حالة الاعتراض الصريح من قبل المعني بالمعالجة[2]، فإنه يترتب على جريمة المعالجة بعد الاعتراض حسب نص المادة 55 من القانون 18-07 عقوبة الحبس من سنة (01) إلى ثلاث (03) سنوات وبغرامة من 100.000دج إلى 300.000دج.

ويدخل كذلك ضمن جريمة المعالجة غير المشروعة عملية جمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة، بحيث يعاقب بالحبس من سنة (01) إلى ثلاث (03) سنوات، وبغرامة من 100.000 إلى 300.000دج[3].

أما جريمة الاستعمال غير المشروع للمعطيات ذات الطابع الشخصي فنصت عليها المادتين 68 و69 من القانون 18-07.

حيث تضمن نص المادة 68 تجريم كل من قام، في غير الحالات المنصوص عليها قانونا، بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن، وذلك يستلزم عقوبة الحبس من ستة أشهر إلى ثلاث سنوات وكذا دفع غرامة تتراوح بين 60.000دج و300.000دج.

أما نص المادة 69 من القانون 18-07 فأشار صراحة إلى الجريمة، التي يتمثل ركنها المادي في الاستعمال غير المشروع للمعطيات، حيث يتم ارتكاب هذه الجريمة من قبل أشخاص محددين، بهدف الاستعمال التعسفي، أو تدليس وتشويه المعطيات، أو نقلها إلى أشخاص غير مؤهلين من طرف المسؤول عن المعالجة[4].

[1] انظر المادتين 55 و 57 من القانون 18-07، المرجع السابق.

[2] انظر المادة 36 من القانون 18-07 من القانون 18-07.

[3] راجع المادة 59 من القانون 18-07، المرجع السابق.

[4] تومي يحي، المرجع السابق، ص 1544.

وقد نصت المادة 69 على أن مجرد الإهمال من قبل أحد المعالجين يرتب قيام هذه الجريمة، والتي تستوجب عقوبة الحبس من سنة (01) إلى خمس (05) سنوات، وكذا تسديد غرامة مالية من 100.000دج إلى 500.000دج[1].

خامسا: تجريم عدم الالتزام بسرية وسلامة المعالجة

تعد سلامة وسرية المعالجة من بين الواجبات المستلزمة على المسؤول عن المعالجة، والتي تحتم عليه اتخاذ الإجراءات التقنية المناسبة لحماية المعطيات المعالجة من الإتلاف أو الضياع أو النشر أو الولوج غير المرخصين، مع ضرورة تقديم الضمانات الكافية المتعلقة بإجراءات السلامة للمعالجات الواجب القيام بها والسهر على احترامها بحيث يجب أن تتضمن التدابير مستوى من السلامة بالنظر إلى حجم المخاطر التي يمكن أن تشكلها المعالجة. كما يتعين مراعاة ضوابط اختيار المعالج من الباطن ومسؤولياته، مع التقيد بواجب كتمان السر المهني لأي معالجة يقوم بها[2].

وبالرجوع إلى نص المادة 65 من القانون 18-07، الذي رتب عقوبات الإخلال بالالتزام بالسر المهني و شروط وإجراءات السلامة، بوجوب تسديد غرامة من 200.000دج إلى 500.000دج ضد المسؤول عن المعالجة الذي يقوم بخرق الالتزامات المنصوص عليها في المادتين 38 و39 من القانون 18-07، هذا بالإضافة إلى العقوبات الأخرى الأشد المنصوص عليها قانونا، نظر لأن مبدأ التحفظ ومراعاة حفظ السر المهني مكرسة في قوانين متفرقة، حسب طبيعة كل معالجة. وهي تعد جريمة بتوفر ركنيها المادي والمعنوي، فالركن المادي يتجلى في هذا النوع من الجرائم بحيازة المعالج للمعطيات وثبوت فعل إفشاء هذه المعطيات الشخصية، أما الركن المعنوي فيشمل قيام القصد الجنائي للإخلال بمبادئ السر المهني وسلامة البيانات، وفي حالة الخطأ فالجزاء يكون نتيجة الاستخفاف والإهمال بإجراءات المعالجة وهو ما أقره المشرع الفرنسي في الجانب حماية للبيانات ذات الطابع الشخصي[3].

---

[1] انظر المادة 69 من القانون 18-07، المرجع السابق.

[2] انظر المواد 38،39 و40 من القانون 18-07، المرجع السابق.

[3] مروة زين العابدين صالح، المرجع السابق، ص 472

وقد رتب المشرع من خلال نص المادة 62 عقوبات نتيجة عملية إفشاء المعلومات المحمية بموجب القانون 18-07، من قبل أي عضو من أعضاء السلطة الوطنية لحماية المعطيات أو أي مستخدم بالأمانة التنفيذية للسلطة[1]. وتم الإحالة في تحديد طبيعة العقوبات إلى نص المادة 301 من قانون العقوبات، والتي نصت صراحة في فقرتها الأولى على جزاء إفشاء الأسرار المرتبطة بالمهنة أو الوظيفة، بأنه: " يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 500دج إلى 5000دج الأطباء والجراحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى بها إليهم وأفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشاءها أو يصرح لهم بذلك"[2].

سادسا: تجريم السماح للأشخاص غير مؤهلين بولوج معطيات ذات طابع شخصي

لقد جاء نص المادة 60 من القانون 18-07 بحكم عام، يقتضي تجريم كل شخص، مهما كان، مسؤول عن المعالجة، أو معالج من الباطن أو غير ذلك، يقتضي قصده الجنائي السماح لأّشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي، مهما كانت طبيعتها، وذلك بعقوبة الحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة مالية من 200.000دج إلى 500.000دج[3].

هذا كما تجدر الإشارة أن القانون 18-07، قد أشار في جانب الجزاءات المترتبة عن ارتكاب الجرائم المنصوص عليها ضمن هذا القانون، من قبل الشخص المعنوي، بالإحالة إلى قانون العقوبات[4].

كما أتاح المجال للسلطة الوطنية أو للقاضي المختص للأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة والتي نتج عنها ارتكاب الجريمة، وفي هذا الإطار يكلف أعضاء ومستخدمو السلطة الوطنية لمعاينة مسح هذه المعطيات.

[1] انظر المادتين 23 و27 من القانون 18-07، المرجع السابق.

[2] راجع المادة 301 من الأمر 66-156، المتضمن قانون العقوبات، المرجع السابق.

[3] انظر المادة 60 من القانون 18-07، المرجع السابق.

[4] المادة 71 من القانون 18-07، المرجع السابق.

هذا إلى جانب تضمين أحكام تقتضي مصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره، كما يتحمل المحكوم عليه مصاريف إعادة تخصيص المحل أو تدميره[1].

هذا كما أكد نص المادتين 73 و74 من القانون 18-07 على أن محاولة ارتكاب احدى الجنح المنصوص عليها ضمن نص هذا القانون تقتضي تطبيق العقوبة المقررة للجريمة التامة، وفي حالة العود يتم مضاعفة العقوبات.

الفرع الثالث: الجزاءات المقررة بموجب النصوص القانونية الأخرى

نظرا لتشعب وتداخل مجال البيانات الشخصية بالعديد من المجالات الأخرى، نظر لارتباطها الوثيق بخصوصية الأشخاص، فإن قانون العقوبات أو قانون حماية المعطيات الشخصية، لم يتضمنا كل الجزاءات المترتبة عن المساس بالمعطيات الشخصية، مما دفع بالمشرع الجزائري إلى إير اد عقوبات ضمن نصوص قانون أخرى، كتلك المتعلقة بحق المؤلف والحقوق المجاورة، التجارة الإلكترونية، الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، التوقيع والتصديق الإلكترونين والقواعد المتعلقة بالبريد والاتصالات الالكترونية، وهو ما سيتم التفصيل فيه تباعا، على النحو الموالي:

أولا: الجزاءات المنصوص عليها ضمن قانون حماية حق المؤلف

بعد إلغاء مواد الفصل السابع من قانون العقوبات، المتعلقة بالتعدي على الملكية الأدبية والفنية، بموجب الأمر 97-10، المؤرخ في 06 مارس 1997، ثم تأكيد ذلك بموجب المادة 163 من الأمر 03-05، المتعلق بحقوق المؤلف والحقوق المجاورة. هذا ليتم تجريم المساس بحقوق المؤلف بموجب مواد الفصل السادس من الأمر 03-05، لاسيما مضمون المواد من 151 إلى 160.

حيث نصت المادتين 151 و152 منه على تعريف جنحة التقليد والتي تشمل :"

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف.
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة.
- بيع نسخ مقلدة لمصنف أو أداء.

[1] المادة 72 من القانون 18-07، المرجع السابق.

- تأجير أو وضع رهن التداول لنسخ مقلدة من مصنف أو أداء."[1]
- انتهاك الحقوق المحمية بموجب الأمر 03-05، بتبليغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني، أو البث الإذاعي السمعي أو السمعي البصري، أو التوزيع بواسطة الكبل أو بأية وسيلة نقل أخرى لإشارات تحمل أصواتا أو صورا أو بأي منظومة معالجة معلوماتية."[2]

كما رتب نص المادة 153 عقوبة جنحة التقليد بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000دج إلى 1.000.000دج.

وفي نفس السياق يجدر التوضيح أن المشرع الجزائري بموجب المادة 160 من الأمر 03-05، خول لمالك الحقوق المحمية ومن يمثله تقديم شكوى للجهة القضائية المختصة محليا، إذا كان ضحية جريمة تقليد، كما يخول صاحب المصنف المعتدى عليه، إجراء حجز التقليد، بدون ترخيص قضائي مسبق، وقد تم تحديد الجهات المخولة للقيام بهذا الإجراء وهم: ضباط الشرطة القضائية والأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف، وللقاضي سلطات واسعة في إقرار رفع اليد، أو رفض الحجز، أو توقيع الجزاءات المقررة بموجب أحكام المو اد 153-154- 155-156-157-158 و159 من الأمر 03-05، مع إقرار مضاعفة العقوبة في حالة العود [3]. كما يمكن توقيع عقوبات تكميلية تشمل مصادرة العتاد المستعمل في الجريمة وكذا حجز المبالغ المالية الناتجة عن الاستغلال غير المشروع للمصنف أو العمل الذهني، وكذا نشر الحكم القضائي في الصحف والأماكن العمومية طبقا لما تم تفصيله بموجب المواد157، 158 و159، المذكورة أعلاه[4].

[1] المادة 151 من الأمر 03-05، المرجع السابق.

[2] المادة 152 من الأمر 03-05، المرجع السابق.

[3] خالد داودي، الجريمة المعلوماتية، المرجع السابق، ص100-102.

[4] جدي نجاة،عدلي محمد عبد الكريم، مبررات تدخل الأداة الجنائية في مجال حقوق التأليف، المجلد السابع، العدد02، نوفمبر 2020، ص 575.

ثانيا: الجزاءات المقررة بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

نظرا لتمييز العديد من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، هي في حد ذاتها جرائم ماسة بالمعطيات الشخصية، مما يجعل مضامين القانون 09-04، كآلية فعالة في مجال حماية المعطيات الشخصية، حيث نصت المادة 11 منه والمتعلقة بحفظ المعطيات المتعلقة بحركة السير[1]، على إلزام مقدمي الخدمات، الحائزين على معطيات معلوماتية، على القيام بحفظ هذه المعطيات لمدة سنة ابتداء من تاريخ تسجيلها، وتشمل:"

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الظرفية، المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها".

كما تم إقرار تجريم عدم احترام هذه الالتزامات، وكذا تحمل المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، بحيث يعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50.000دج إلى 500.000دج، أما الشخص المعنوي فيعاقب وفقا لما تم النص عليه في مواد قانون العقوبات[2].

كما أشار نص المادة 29 من المرسوم الرئاسي 21-439، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

[1] تم تعريف مصطلح "المعطيات المتعلقة بحركة السير" في مفهوم القانون 09-04، بموجب نص المادة 02 منه ب " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة".

[2] انظر المادة 11 من القانون 09-04، المرجع السابق.

إلى إلزام أعضاء هذه الهيئة ومستخدميها، تحت طائلة العقوبات الجزائية، بالاستعمال المشروع للمعطيات المتحصل عليها، مهما كانت طبيعتها، من اتصالات إلكترونية أو غيرها من المعلومات التي تستلمها أو تجمعها الهيئة، بغرض الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1].

وتجدر الإشارة أن هذا النص القانوني بالرغم من تركيز مضامينه على الجانب الإجرائي المتعلق بمكافحة الجريمة الإلكترونية، إلا أنه تضمن كذلك موقفا تشريعيا هاما في مجال حماية البيانات الشخصية، المتداولة عبر الإنترنت، في حالة مخالفة مقدم خدمة الإنترنت الالتزام بسحب المحتوى غير الشرعي، حيث يترتب عن هذه المخالفة قيام المسؤولية القانونية، حسب الآثار الناجمة عن عدم سحب هذا المحتوى غير الشرعي[2].

ثالثا: الجزاءات المقررة بموجب القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين

نظرا للارتباط الوثيق بين التوقيع الإلكتروني والبيانات الشخصية، لاسيما تلك المعالجة آليا، فإن المشرع الجزائري أقر جملة من العقوبات تضمنها القانون 15-04، والتي سيتم التفصيل في طبيعة كل منها، على النحو التوالي:

أ- جريمة حيازة، إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني خاص بالغير:

لقد أكد نص المادة 68 من القانون 15-04 على تجريم القيام باستعمال، حيازة، أو إفشاء بيانات متعلقة بإنشاء توقيع إلكتروني بأوصافه، خاص بالغير وذلك بتسليط عقوبة الحبس من ثلاثة (03) أشهر إلى ثلاث (03) سنوات وبغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين دينار (5.000.000دج)، وللقاضي تقرير تنفيذ إحدى العقوبتين فقط. وعليه فإن هذه الجريمة تثبت مباشرة بمجرد حيازة بيانات إنشاء توقيع إلكتروني خاص بالغير، مما يؤكد حرص المشرع على حماية التوقيع الالكتروني

[1] انظر المادة 29 من المرسوم الرئاسي 21-439، المرجع السابق.

[2] بن زيطة عبد الهادي، ضرورة إنشاء سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة استخدامات المعلوماتية، المرجع السابق، ص59.

حفاظا على حرمة البيانات الشخصية من جهة وكذا الآثار المترتبة عن ذلك وانعكاساتها على التجارة أو التعاملات الالكترونية ككل.

ب- جريمة إخلال مقدمي الخدمات بالحفاظ على سرية البيانات والمعلومات:

ألزم المشرع مؤدي خدمات التصديق الإلكتروني[1]، بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة، وفي حالة الإخلال بهذا الالتزام فإنه يستوجب العقوبة بالحبس من ثلاثة (03) أشهر إلى سنتين (02) وبغرامة تتراوح بين 200.000دج و 1.000.000دج، أو تطبيق إحدى هاتين العقوبتين فقط[2].

كما نصت المادة 73 من القانون 15-04 على منع المكلف بالتدقيق من كشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق، وفي حالة المخالفة يعاقب بالسجن من ثلاثة أشهر إلى سنتين وبغرامة من 20.000دج إلى 200.000دج أو بتطبيق و احدة من هاتين العقوبتين.

ج. جريمة جمع البيانات الشخصية للمعني بدون موافقته الصريحة:

أكد القانون 15-04، بموجب مادته 43 على منع مؤدي خدمات التصديق الإلكتروني من جمع البيانات الشخصية للمعني إلا بعد الحصول على موافقته الشخصية الصريحة، وكذا عدم جمع البيانات الأخرى غير تلك الضرورية لمنح وحفظ شهادة التصديق الإلكتروني. وفي حالة الإخلال بأحكام هذه المادة فإن مؤدي الخدمات يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من مائتي ألف دينار إلى مليون دينار جزائري، أو بواحدة من هاتين العقوبتين[3].

[1] تم تعريف " مؤدي خدمات التصديق الإلكتروني" بموجب نص المادة 2 من القانون 15-04، كما يلي: " شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني".

[2] المادة 70 من القانون 15-04، المرجع السابق.

[3] المادة 71 من القانون 15-04، المرجع السابق.

كما أكد نص المادة 75 من نفس القانون على مضاعفة الغرامة بخمس (05) مرات في حالة ارتكاب إحدى الجرائم المنصوص عليها، من قبل شخص معنوي، مقارنة بتلك المنصوص عليها بالنسبة للشخص الطبيعي.

رابعا: الجزاءات المقررة بموجب القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

تضمن القانون 18-04 ضمن بابه الرابع المتعلق بالأحكام الجزائية، جملة من الأحكام العقابية تخص تكريس الحماية الجزائية للبيانات الشخصية، المتعلقة بالمراسلات والاتصالات الإلكترونية، والتي سيتم التفصيل فيها كما يلي:

أ. تجريم انتهاك سرية المراسلات أو الاتصالات الإلكترونية:

تعد سرية المراسلات من بين الجوانب الأساسية للحق في الخصوصية، وعند التدقيق في مضامين هذه المراسلات والاتصالات الإلكترونية فإنه يتأكد ارتباطها بالجانب الشخصي للفرد، مما يدخلها ضمن البيانات الشخصية، التي تتطلب جانبا واسعا من الحماية، وعليه فقد نصت المادة 164 من القانون 18-04، على تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو إفشاء مضمونها أو نشره أو استعماله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها. وعقوبة هذه الجريمة هي الحبس من سنة إلى خمس سنوات وبغرامة من 500.000 دج إلى 1.000.000دج.

ب. تجريم فتح أو تحويل أو تخريب البريدو الاتصالات الإلكترونية:

أشار نص المادة 165 إلى تجريم كل من يقوم بفتح أو تحويل أو تخريب بريد أو المساعدة في ذلك، وكذا على كل متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية أو أمر أو ساعد في ارتكاب هذه الأفعال، وذلك بإقرار عقوبة الحبس من سنة إلى ثلاث سنوات وبغرامة من 1.000.000دج إلى 5.000.000 دج.

كما يعاقب العون المستخدم من طرف متعامل للبريد، الذي يقوم بفتح، تحويل أو تخريب البريد أو المساعدة في ذلك في إطار قيامه بمهامه، وكذلك الأمر بالنسبة لكل شخص مستخدم لدى متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية بعقوبة الحبس من ستة (06) أشهر إلى سنتين (02)، وبغرامة من 500.000دج إلى 1.000.000دج[1].

وفي حالة ارتكاب هذه الجريمة من قبل أشخاص آخرين غير المذكورين في نص المادتين 165 و166، فإنه يعاقب بالحبس من شهرين إلى سنة واحدة وبغرامة من 200.000دج إلى 500.000دج[2].

ج. تجريم الاستغلال غير المشروع لشبكة اتصالات الكترونية:

نصت المادة 171 من القانون 18-07 على عقوبة الحبس من سنة إلى ثلاث سنوات وغرامة من 1.000.000دج إلى 5.000.000دج، أو بإحدى هاتين العقوبتين، كل من يقوم بإنشاء أو استغلال شبكة اتصالات إلكترونية مفتوحة للجمهور دون الرخصة، المنصوص عليها ضمن المادة 123 من نفس القانون أو عند ممارسة النشاط خرقا لقرار التعليق أو السحب لهذه الرخصة.

وتم النص على معاقبة كل من يوفر خدمات الاتصالات الإلكترونية المفتوحة للجمهور دون الترخيص العام المنصوص عليه في المادة 131 من هذا القانون، وكذا كل من ينشئ أو يستغل أو يعمل على إنشاء شبكة خاصة دون الترخيص المنصوص عليه ضمن نص المادة 138 من نفس القانون[3].

[1] المادة 166 من القانون 18-04، المرجع السابق.

[2] انظر المادة 167 من القانون 18-04، المرجع السابق.

[3] راجع المواد 131، 138 و172 من القانون 18-04، المرجع السابق.

خامسا: الجزاءات المنصوص عليها ضمن الأمر 21-09، المتعلق بحماية المعلومات والوثائق الإدارية

لقد تطرق الأمر 21-09 إلى جانب هام يخص حماية المعلومات والوثائق المصنفة، بغض النظر عن محتواها، والذي ترك فيه المجال للتنظيم لضبطه، للتمييز وتحديد درجة الأهمية والسرية الواجبة التحفظ والكتمان.

والمشرع من خلال نص هذا الأمر طرق بصفة غير مباشرة باب حماية المعطيات الشخصية للشخص المعنوي، فكما للأشخاص الطبيعيين خصوصيات فالشخص المعنوي يمكن أن يتميز بجانب من الخصوصية تقتضي حظر معالجة معطياته إلا بترخيص، فكذلك المشرع من خلال نص هذا الأمر ضبط قواعد حماية المعلومات والوثائق بدءا بتصنيفها إلى أربعة (04) أصناف، "سري جدا"، "سري"، "واجب الكتمان" و"توزيع محدود" وباستقراء مواد الفصل السادس من هذا الأمر فإننا نستخلص جملة من الجوانب المكرسة للحماية الجزائية للبيانات الشخصية، حسب كل وثيقة مصنفة نفصلها على النحو الموالي:

أ. تجريم كشف أو تسريب المعلومات والوثائق المصنفة "توزيع محدود":

أكد نص المادة 28 من الأمر 21-09 على تجريم نشر أو إفشاء أو إطلاع الغير أو السماح له بأخذ صورة من المعلومات أو الوثائق المصنفة " توزيع محدود"، ورتب عقوبة الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 60.000دج إلى 300.000دج، أو تطبيق واحدة من العقوبتين. مع التأكيد على رفع حجم العقوبة إذا أدى ذلك إلى المساس بالاعتبار الواجب للسلطات المعنية، لتصل إلى عقوبة الحبس من سنة إلى خمس سنوات وغرامة من 100.000دج إلى 500.000دج.

كما أن العقوبة تخفف إذا ارتكبت الجريمة نتيجة عدم مراعاة الموظف العمومي الأحكام التشريعية و/أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه

بحيث تصبح عقوبة الحبس من ثلاثة أشهر إلى سنة والغرامة من 30.000دج إلى 100.000دج أو إحدى هاتين العقوبتين فقط[1].

ب. تجريم كشف أو تسريب المعلومات والوثائق المصنفة "واجب الكتمان"، "سري"، و"سري جدا":

لقد تدرج المشرع في ضبط شدة العقوبة حسب درجة أهمية كل وثيقة باعتبارها والآثار التي قد تترتب عن الاطلاع عليها من قبل الموظف أو قيامه بنشرها أو اطلاع الغير عليها بمختلف الوسائل.

وتجدر الإشارة أن جزاء الموظف العمومي الذي يقوم بإفشاء أو نشر معلومة أو وثيقة مصنفة " واجب الكتمان" إلى علم الجمهور أو علم شخص لا صفة له في الاطلاع عليها أو يسمح له بأخذ صور منها أو يترك الغير يقوم بذلك، هو العقوبة بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500.000دج[2].

ونصت كذلك الفقرة الثانية من المادة 29 على تشديد العقوبة في حالة تعلق الأمر بوثائق مصنفة " سري جدا" أو "سري"، بحيث تتراوح عقوبة الحبس بين خمس (05) وعشر (10) سنوات، والغرامة بين 500.000دج و1.000.000دج.

هذا مع إقرار تخفيض العقوبات المنصوص عليها في المادة 29 والتي تخص الوثائق المصنفة " واجب الكتمان"، "سري" و "سري جدا"، في حالة ارتكبت الجريمة نتيجة لعدم مراعاة الموظف العمومي للأحكام التشريعية/ أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه، إلى الحبس من ستة أشهر إلى سنتين و/ أو الغرامة من 60.000دج إلى 200.000دج[3].

[1] راجع الفقرة الأولى من المادة 30 من الأمر 21-09، المرجع السابق.

[2] المادة 29 من الأمر 21-09، المرجع السابق.

[3] راجع الفقرة الثانية من المادة 30 من الأمر 21-09، المرجع السابق.

وقد أقر المشرع بموجب نص المادة 35 من هذا الأمر، عقوبة الحبس من ستة أشهر إلى سنتين وبغرامة من 60.000دج إلى 200.000دج، أو بإحدى هاتين العقوبتين، ضد كل من يحوز وثيقة مصنفة، دون أن يكون مؤهلا لذلك، ولم يقم بتسليمها إلى السلطات المعنية[1].

ج. تجريم نشر أو إفشاء محتوى وثائق قضائية:

تعتبر جريمة نشر محاضر و/أو أوراق التحريات والتحقيق القضائي أو إفشاء محتواها أو تمكين من لا صفة له حيازتها، أداة فعالة في حماية البيانات الشخصية التي تحتويها من جهة، وكذا تفادي الآثار السلبية التي يمكن أن تنتج عن معرفة الغير بها، لاسيما تلك التي تخص الأمن والنظام العام، وما تقتضيه ضرورة التحريات للوصول إلى المجرمين، بالإضافة إلى إقرار عقوبة الحبس من ثلاث إلى خمس (3-5) سنوات، وبتسديد غرامة تتراوح بين 300.000دج و500.000دج[2].

د. تجريم إطلاع الغير بمقابل على معلومة أو وثيقة مصنفة:

جرم نص المادة 33 كل من أطلع الغير، أو يسر له ذلك، بمقابل، مهما كانت طبيعته، على معلومة أو وثيقة مصنفة، ورتب جزاء لذلك الحبس من خمس إلى خمسة عشر (5-15) سنة وبغرامة من 500.000دج إلى 1.500.000دج، وفي حالة القيام بهذه الجريمة بغرض تنفيذ خطة مدبرة داخل الوطن أو خارجة فإن العقوبة تشدد، لتصل مدة الحبس بين سبع (7) و خمسة عشر سنة (15)، والغرامة بين 700.000دج و1.500.000دج[3].

[1] المادة 35 من الأمر 21-09، المرجع السابق.

[2] انظر المادة 32 من الأمر 21-09، المرجع السابق.

[3] انظر المادة 34 من الأمر 21-09، المرجع السابق.

هـ. تجريم الدخول إلى منظومة معلوماتية للحصول غير المشروع على معلومات أو وثائق مصنفة:

لقد جرم المشرع الجزائري كل عملية دخول دون ترخيص إلى منظومة معلوماتية أو موقع إلكتروني أو شبكة إلكترونية أو أي وسيلة أخرى من وسائل تكنولوجيات الإعلام والاتصال للسلطات المعنية، بقصد الحصول بغير وجه حق على معلومات أو وثائق مصنفة، مع النص على عقوبة الحبس من خمس إلى عشر سنوات، وبغرامة من 500.000دج إلى 1.000.000دج، كما تضاعف هذه العقوبات في حالة نشر هذه المعلومات أو الوثائق المصنفة قصد الإضرار بالسلطات المعنية أو الحصول على منافع مباشرة أو غير مباشرة[1].

و. تجريم إنشاء أو إدارة مواقع إلكترونية بغرض نشر المعلومات والوثائق المصنفة:

تطرق نص المادة 38 إلى جريمة إنشاء أو إدارة أو الإشراف على مواقع حسابات أو برامج إلكترونية معلوماتية، تستعمل لنشر المعلومات والوثائق المصنفة أو محتواها كليا أو جزئيا، أو يقوم بنشر ذلك على شبكة إلكترونية أو بإحدى وسائل تكنولوجيات الإعلام، بإقرار عقوبة الحبس من خمس إلى عشر سنوات وبغرامة مالية من 500.000دج إلى 1.000.000دج[2].

كما تشدد العقوبة في حالة نشر أو بث أي معلومة أو وثيقة مصنفة،عن طريق الاتصالات الإلكترونية أو منظومة معلوماتية، بغرض المساس بالنظام العام والسكينة العمومية[3].

ز. جريمة نشر أو تداول أو توزيع الوثائق الإدارية غير المصنفة:

بالإضافة إلى تفصيل الجرائم المتعلقة بنشر المعلومات والوثائق المصنفة، فقد أقر المشرع من خلال هذا الأمر، عقوبات، كذلك، لكل من يقوم بنشر أو تداول أو توزيع

[1] انظر المادة 37 من الأمر 21-09، المرجع السابق.

[2] المادة 38 من الأمر 21-09، المرجع السابق.

[3] راجع المادة 39 من الأمر 21-09، المرجع السابق.

المراسلات الإدارية التي لا تندرج ضمن الوثائق المصنفة الصادرة من وإلى السلطات المعنية دون موافقتها أو في غير الحالات التي سمح فيها القانون بذلك، وذلك بإقرار عقوبة الحبس من ثلاثة أشهر إلى سنة و/أو بغرامة من 30.000دج إلى 100.000دج، كما تضاعف هذه العقوبات في حالة العود[1].

كما أشار نص المادة 42 إلى أن الشخص المعنوي المرتكب لإحدى الجرائم المنصوص عليها ضمن الأمر 21-09، تطبق عليه نصوص قانون العقوبات.

وتجدر الإشارة إلى أن هذا النص القانوني، أقر الحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة أو أكثر من الجرائم المنصوص عليها، وكذا الأموال المتحصل عليها منها، مع إغلاق الموقع أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن وإغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه[2].

وتكريسا لحماية مختلف الوثائق المصنفة فقد أقر المشرع بموجب نص المادة 48 من هذا الأمر مضاعفة العقوبات في حالة العود.

وما نلاحظه من خلال مضامين هذا النص القانوني هو تكريس حماية جزائية فعالة للمعطيات الشخصية للأشخاص الطبيعيين التي تختويها الوثائق والمراسلات الإدارية المختلفة، حسب درجة تصنيفها، بالإضافة إلى تكريس جانب من حماية معطيات الشخص المعنوي، لا سيما تلك المعالجة آليا. مما من شأنه أن يكبح أو يقلل من الاختراقات المسجلة في هذا الجانب لمعلومات المؤسسات العمومية المتداولة عبر مختلف المواقع الإلكترونية المتعلقة بها.

[1] راجع المادة 41 من الأمر 21-09، المرجع السابق.

[2] المادة 44 من الأمر 21-09، المرجع السابق.

خاتمة

خاتمة

إن تكريس الحماية القانونية للبيانات الشخصية في التشريع الجزائري أملته ضرورة التماشي والتكيف مع التطور التكنولوجي في مختلف المجالات لاسيما تلك التي تخص الجوانب المعلوماتية، التي تقتضي خلق بيئة تشريعية متطورة تضبط مختلف إجراءات معالجة المعطيات الشخصية داخليا وخارجيا نظرا لما تتسم به من حساسية، الأمر الذي يقتضي توفير مختلف الضمانات لخلق بيئة آمنة تضمن فيها حقوق الأشخاص وتهدف إلى خلق توان بين مشروعية معالجة المعطيات وفق ما تقتضيه الحاجة، أو لاعتبارات شخصية تخص صاحب البيانات، وبين إقرار جزاءات مناسبة في حالة تجاوز الإطار المحدد للمعالجة، ضمانا لحقوق الشخص المعني على بياناته وخصوصيته.

وعليه فإن المشرع الجزائري كرس حماية للبيانات الشخصية، ذات فعالية نسبية، على مستويات متنوعة، من حماية شكلية إجرائية، إلى حماية إدارية مؤسساتية، ثم حماية جزائية بعد استنفاد مختلف الإجراءات الوقائية لضمان عدم المساس بخصوصية هذه البيانات.

فالحماية الشكلية الإجرائية تشمل مختلف التدابير الوقائية لضمان مشروعية معالجة البيانات الشخصية، والتي تتطلب في الدرجة الأولى موافقة ورضا الشخص المعني، وعدم المساس بكل حقوقه المتعلقة بمعالجة بياناته، إلا في حالة التعذر أو الضرورة، يتم اتباع إجرائي التصريح المسبق أو الترخيص من قبل السلطة الوطنية المختصة.

وتشمل الحماية الإدارية المؤسساتية، الدور المنوط بالسلطات الإدارية المستقلة لحماية البيانات الشخصية، التي كرسها المشرع الجزائري، بصفة مباشرة، وتشمل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وبصفة غير مباشرة، الهيئة الوطنية لمكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، نظرا لما اختصت به من آليات قانونية لمكافحة مختلف الجرائم، والتي من بينها تلك المرتبطة بالمساس بالمعالجة الآلية للمعطيات الشخصية.

وأما الحماية الجزائية، والتي تصنف كآخر وأنجع آلية، لمكافحة الجرائم الماسة بخصوصية البيانات الشخصية، نظرا لما أقره المشرع الجزائري ضمن مختلف النصوص القانونية المكرسة لحماية البيانات الشخصية، على غرار قانون العقوبات، والقانون 18-

07، المتعلق بحماية الأشخاص الطبيعيين في مجال حماية المعطيات ذات الطابع الشخصي، والتي تضمنت جزاءات تتناسب حسب كل جريمة، تمس بخصوصية البيانات.

ومن خلال دراستنا هذه، تم التوصل إلى النتائج التالية:

- تبني المشرع الجزائري للمفهوم الواسع للمعطيات الشخصية، الأمر الذي من شأنه تكريس مجال أكبر لهذه الحماية لتشمل مختلف أصناف البيانات الشخصية الممكن اكتشافها مستقبلا بتأثير مختلف المعالجات الرقمية في إطار مستجدات التطور التكنولوجي في مجال المعلوماتية.

- تكريس المشرع الجزائري لحماية عملية معالجة المعطيات ذات الطابع الشخصي بأي طريقة كانت هذه المعالجة، سواء آلية أو يدوية، كلية أو جزئية، مما يضمن شرعيتها، والحفاظ على خصوصية صاحب البيانات، قبل، أثناء وبعد المعالجة.

- أسهمت المعالجة الآلية للمعطيات الشخصية في تراكم حجم هائل من المعطيات المخزنة داخل مختلف أنظمة المعالجة، بحيث تتنوع هذه المعطيات لتشمل مختلف الجوانب، المتعلقة بشرائح واسعة من المجتمع باختلاف توجهاتها ومكانتها، بالإضافة إلى إمكانية نقل هذه المعطيات إلى ما وراء الحدود بكبسة زر، وهو ما يبرهن على خطورة هذه المعالجة بالرغم من الانعكاسات الإيجابية في تقريب المسافات وتوفير الوقت والجهد، إلا أن الانتشار الواسع للجرائم المعلوماتية، جعل تكريس أمن المعلومات وأمن أنظمة المعالجة بالدرجة الأولى ضمن الأولويات .

- كرس القانون الدولي حماية متنوعة للبيانات الشخصية، أسهمت في ضبطها مختلف المنظمات الدولية الجماعية على غرار منظمة الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية، والمنظمات الدولية الإقليمية كالاتحاد الأوربي بمساهمة مجلس أوروبا لاسيما باعتماده النظام الأوروبي العام لحماية البيانات لسنة 2016، والاتحاد الإفريقي الذي بادر، على وجه الخصوص، باتفاقية لمكافحة جرائم الفضاء المعلوماتي وحماية البيانات ذات الطابع الشخصي، وكذا دور الجامعة العربية في تكريس مكافحة جرائم تقنية المعلومات ضمن الاتفاقية الخاصة بهذا المجال الصادرة سنة 2010، والتي انضمت إليها الجزائر سنة 2014.

- تعدد وتداخل النصوص القانونية المكرسة لحماية المعطيات الشخصية، كالتداخل المسجل في صلاحيات السلطات الإدارية المستقلة لحماية البيانات، وكذا في مجال ضبط الجزاءات المترتبة لمختلف الجرائم، المنصوص عليها ضمن مختلف النصوص القانونية، بصفة مباشرة أو غير مباشرة.

- توسيع المشرع الجزائري لمجال الحماية المتعلقة بالدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، وكذا البقاء غير المصرح، حتى في حالة عدم مساسه بمكونات نظام المعالجة الآلية، بحسب ما نص عليه قانون العقوبات، بالرجوع إلى مضمون مادته 394 مكرر.

- بالرغم من النص على بعض مجالات الحماية للبيانات الشخصية التي تضمنتها نصوص متباينة بصفة عامة كتجريم المعالجة غير المشروعة والمساس بأنظمة المعالجة الآلية للمعطيات، المنصوص عليها ضمن القسم السابع مكرر من قانون العقوبات، إلا أنها لم تشمل الحماية الدقيقة لمعطيات الأشخاص الطبيعيين الجزائريين، المحجوزة ، بالخصوص، ضمن مختلف أنظمة المعالجة الآلية للشركات الدولية لاسيما تلك المتعلقة بمواقع التواصل الاجتماعي التي تخزن بيانات تخص شريحة كبيرة من المشتركين، وكذا مختلف الشركات الأجنبية للاتصالات وهو الأمر الذي لم يتم تداركه إلا بعد صدور القانون 18-07 .

- تعرض المشرع الجزائري في بعض الجوانب إلى حماية معطيات الشخص الاعتباري، لاسيما من خلال النصوص المتعلقة بمكافحة الجريمة الإلكترونية وحماية الوثائق المصنفة، إلا أنها تبقى غير كافية نظرا لحساسية الملفات التي تحوزها الأشخاص الاعتبارية، لاسيما المؤسسات العمومية منها، والتي تضم أدق تفاصيل المعطيات الشخصية الخاصة بالأشخاص الطبيعيين.

- بعد استقراء مختلف الآليات والضمانات التي أتى بها المشرع الجزائري من خلال مضامين النصوص القانونية المكرسة لحماية البيانات الشخصية، لاسيما القانون 18-07، تم الوقوف على الكثير من الملاحظات المسجلة للنقص الموجود في هذا الجانب، لاسيما من حيث وجوب التفعيل وا زالة اللبس من جهة على بعض الإجراءات المتداخلة ومرهون، من جهة أخرى، بمستوى التطور التكنولوجي والمعلوماتي.

وعليه يمكن تقديم بعض الاقتراحات والتوصيات لضمان تفعيل مختلف إجراءات الحماية المتعلقة بالمعطيات الشخصية، كما هو موضح أدناه:

1- الاستفادة من التجارب الدولية السابقة في مجال طرق ضبط معالجة البيانات الشخصية ومكافحة الجرائم الماسة بخصوصيتها، وذلك من خلال التكوين المستمر لمختلف الموظفين في هذا المجال،خاصة المكلفين بالإشراف على أنظمة المعالجة الآلية للمعطيات، على مستوى مختلف الهيئات والمؤسسات، لاسيما تلك المتخصصة في مجال الاتصالات الرقمية.

2-تنظيم ندوات وملتقيات علمية وطنية ودولية حول المواضيع المستجدة لاسيما في جانب الممارسات المتعلقة بتكريس آليات حماية البيانات الشخصية ، مع الوقوف على تفعيل دور السلطات الإدارية المستقلة لحماية البيانات وكذا مختلف الأحكام والقرارات القضائية الخاصة بهذا المجال.

3- الإسراع في استكمال استصدار مختلف النصوص التنظيمية لاسيما ما تعلق منها بتنصيب وتفعيل السلطات الإدارية المستقلة لحماية البيانات الشخصية، حيث أن القانون 18-07، نص في مادته 75 على أنه يتعين على الأشخاص الذين يمارسون نشاط معالجة المعطيات ذات الطابع الشخصي، الامتثال لأحكام هذا القانون في أجل أقصاه سنة من تنصيب السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، إلا أنه مضى أكثر من ثلاث سنوات من إصدار هذا القانون ولم يتم تنصيب هذه السلطة التي من شأنها أن تلعب دورا محوريا في تكريس المعالجة المشروعة للبيانات الشخصية، نظرا لما اختصها المشرع من سلطات واسعة في هذا المجال، وبالنظر للتشريعات المقارنة، لاسيما على مستوى دول مجلس أوروبا، فإن أساس حماية بياناتها الشخصية هو السلطة الإدارية المستقلة المكلفة بحماية البيانات، بفضل ما تفرضه من غرامات وا ٍجراءات تصل إلى المتابعة القضائية لمكافحة الجرائم الماسة بالبيانات الشخصية.

4-نهيب بالمشرع الجزائري إلى الإسراع في إصدار نص يتضمن حماية البيانات الشخصية المتعلقة بالأشخاص الإعتبارية نظرا للأهمية البالغة التي تمثلها البيانات التي تحوزها أغلب المؤسسات العمومية أو الخاصة، لاسيما تلك المعتمدة على جمع بيانات

بيومترية، والتي من شأنها أن تنعكس بصورة مباشرة على حماية بيانات الأشخاص الطبيعيين .

5- التصديق والإنضمام إلى اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، بحكم ما تتضمنه من بنود من شأنها تعزيز حماية البيانات الشخصية، التي تعد الركيزة الأساس في تفعيل مجالات متعددة لاسيما الجانب الاقتصادي، بحكم أن الاسترتيجية الوطنية في الوقت الراهن تعول على السوق الإفريقية، والتي لايمكن ولوجها بأمان إلا بتأمين البيانات الشخصية.

6- الإسراع في إنشاء سجل وطني إلكتروني يتضمن مختلف الطرق والآليات لاستقبال الشكاوى وكيفيات الحماية للمعطيات الشخصية عن بعد، في أقصر مدة، للتدخل الفاعل مباشرة فور تسجيل أي مساس بالمعطيات الشخصية، لاسيما تلك المعالجة آليا من أجل ضمان الفعالية والنجاعة.

7- تفعيل مجالات أمن المعلومات بإنشاء تشكيل أمني متخصص في متابعة ومكافحة الجرائم المرتبطة بالمعلوماتية بصفة عامة ومختلف الأجهزة التكنلوجية الحديثة.

المصادر والمراجع

1- المصادر

- **القرآن الكريم برواية ورش عن نافع.**
- **السنة النبوية/ صحيح البخاري، صحيح أبي داود.**

2- المراجع العامة

- **باللغة العربية**

1- أحمد عبد الكريم سلامة، القانون الدولي الخاص النوعي (الإلكتروني، السياحي والبيئي)، دار النهضة العربية، ط1، 2002.

2- الشافعي محمد بشير، قانون حقوق الإنسان- مصادره وتطبيقاته الوطنية والدولية، مصر – منشأة المعارف، الطبعة 05، 2005.

3- السعيد كامل، جرائم الكومبيوتر والجرائم الأخرى في مجال التكنولوجيا- المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 أكتوبر 1993، دار النهضة العربية.

4- القاموس المحيط، محمد الدين محمد بن يعقوب الفيروز آبادي، دار الحديث، القاهرة.

5- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2009.

6- بلحاج العربي، مشكلات المرحلة السابقة على التعاقد في ضوء القانون المدني الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2011.

7- جمال عبد الناصر مانع، القانون الدولي العام –المدخل والمصادر، دار العلوم للنشر والتوزيع، مصر، 2005.

8- حسين إبراهيم خليل، تطبيقات قضائية على جريمة الإزعاج المعتمد عن طرق وسائل الاتصال الحديثة، مصر- دار الفكر والقانون للنشر والتوزيع، ط1، سنة 2015.

9- حقوق الإنسان، مجموعة وثائق أوروبية، ترجمة الدكتور محمد أمين الميداني، والدكتور نزيه كسيبي، منشورات المعهد العربي لحقوق الإنسان، ط2، 2001.

10- خالد ممدوح إبراهيم، إبرام العقد الالكتروني –دراسة مقارنة، دار الفكر الجامعي، الإسكندرية- مصر، سنة 2006.

11- رامي متولي القاضي، مكافحة الجرائم المعلوماتية، دار النهضة العربية، مصر، سنة 2011.

12- عبد العزيز محمد سرحان،الاتفاقية الأوروبية لحقوق الإنسان، دار النهضة العربية، القاهرة، 1966.

13- فهد عبد العزيز سعود، مفهوم الخصوصية وتاريخها-رؤية تقنية وا إسلامية، مركز التمييز لأمن المعلومات،2020.

14- فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية: الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر و الإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، مصر، 2007.

15- سهير منتصر، النظرية العامة للحق، مكتبة الإسكندرية، 2006، د.د.ن.

16- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، لبنان، ط1، 2011.

17- شريف يوسف خاطر، حرية تداول المعلومات بين المنع والإباحة – دراسة مقارنة، دار الفكر والقانون، المنصورة- مصر، ط1، سنة 2015.

18- عمورة عمار، شرح القانون التجاري (الأعمال التجارية، التاجر، الشركات التجارية)، دار المعرفة، الجزائر، 2010،

19- محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، ، القاهرة، ط1، سنة 2005.

20- محمد عبد حسين الطائي، ينال محمود الكيلاني، إدارة أمن المعلومات، دار الثقافة، عمان- الأردن، ط1، سنة 2015.

21- معجم الحاسبات، مجمع اللغة العربية، الطبعة الثانية الموسعة، مركز الحاسوب- أكاديمية اللغة العربية، جمهورية مصر العربية، سنة 1995.

22- معجم محيط المحيط، تأليف المعلم بطرس البستان، مكتبة لبنان ناشرون، سنة 1998.

23- منير الجنبيهي، جرائم الإنترنت والحاسب الآلي وطرق مكافحتها، دار الفكر الجامعي، القاهرة، ط1، سنة 2014.

24- مصطفى عبيد، موسوعة العلوم القانونية، مركز البحوث والدراسات متعددة التخصصات، ط1،سنة 2018.

25- نهلا عبد القادر المومني،الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان- الأردن، ط1، سنة 2008.

26- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية- دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية، 2005.

27- هدى قشوش، جرائم الحاسب الإلكتروني في التشر يع المقارن، دار النهضة العربية، القاهرة، ط1، سنة 1992.

- باللغة الأجنبية

1- Ruth Gavison, Privacy and the limits of the law, in Michel J.Gorr and Sterling Harwood, eds, Crime and Punishment: Philosophic Explorations **(** Bwl;ontm CA: wadsworth, Publishing Co. 2000. Formerly Jones and Bartlett Publishers, 1996**)**, pp 46-68

2- Westin, A F, Privacy and Freedom, New York, Atheneum, 1967.

3- المراجع المتخصصة

1- أشرف السعيد أحمد، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة للطباعة و النشر والتوزيع، مصر، ط2، سنة 2015.

2- حوالف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني في الجزائر - دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية-مصر، سنة 2016.

3- خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي للنشر والتوزيع، عمان- الأردن، ط1، سنة 2018.

4- خضر مصباح الطيطي، إدارة تكنولوجيا المعلومات، دار الحامد للنشر والتوزيع، عمان، ط1، 2012.

5- ريموند واكس، الخصوصية مقدمة قصيرة جدا، ترجمة ياسر حسن، مراجعة هاني فتحي سليمان، مؤسسة هنداوي للتعليم والثقافة، القاهرة، مصر، ط01، سنة 2013.

6- زيدان زيبحة، الجريمة لمعلوماتية في التشريع الجزائري، دار الهدى، الجزائر، 2011.

7- سامي علي حامد عياد، الجريمة المعلوماتية وا إجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2008.

8- شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية – دراسة مقارنة، دار الفكر والقانون، المنصورة – مصر، ط1، سنة 2015.

9- عبد الهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الإنترنت، دار النهضة، القاهرة، ط1، سنة 2014.

10- غنية باطلي، الجريمة الالكترونية- دراسة مقارنة، الدار الجزائرية، الجزائر، 2015.

11- فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاقات على شبكة الإنترنت، مكتبة الوفاء القانونية، الإسكندرية، ط1، 2017.

12- محمد عبد حسين الطائي، ينال محمد الكيلاني، إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان- الأردن، ط1، 2015**.**

13- مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، ط1،2016.
14- منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية – الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت لبنان، سنة 2018.
15- وليد سليم النمر، حماية الخصوصية في الإنترنت ، دار الفكر الجامعي، الاسكندرية، ط1، 2017.
16- وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، بيروت، ط1 ، 2017 .
17- يوسف بن سعيد الكلباني الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري، دار النهضة العربية، القاهرة، ط1، 2017.

4- الرسائل العلمية

أ- أطروحات الدكتوراه:

1- الطيبي البركة، الحماية الجنائية لنظام المعالجة الآلية للمعطيات- دراسة مقارنة-، أطروحة دكتوراه، جامعة أحمد دراية –أدرار، الجزائر، 2020-2021.
2- أحمد بوراوي، الحماية القانونية لحق المؤلف والحقوق المجاورة في التشريع الجزائري والاتفاقيات الدولية، أطروحة دكتوراه في القانون، كلية الحقوق، جامعة باتنة، 2005.
3- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي – الحماية الجنائية للحاسب الآلي-، دراسة مقارنة، أطروحة دكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، سنة 2000.
4- أحمد خليفة الملط، الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق، جامعة القاهرة، 2005، ص202.
5- آدم عبد البديع آدم حسن، الحق في الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، سنة 2000.
6- كريمة بوحجة، حماية البيانات الطبية الخاصة في العصر الرقمي –دراسة وصفية وتحليلية-، أطروحة دكتوراه، سنة 2014.
7- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية- رسالة دكتوراه في القانون الجنائي، جامعة عين شمس، مصر، الطبعة الأولى، سنة 2004.

ب- رسائل الماجستير

1- بوحملة كوثر، دور المحكمة الأوروبية لحقوق الإنسان في تطوير القانون الدولي الأوروبي لحقوق الإنسان،رسالة ماجستير،جامعة يوسف بن خدة الجزائر،كلية الحقوق بن عكنون،السنة الجامعية 2009-2010.

2- سليم جلاد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، رسالة ماجيستير في الشريعة والقانون، جامعة وهران، جوان 2013.

5- المقالات

باللغة العربية

1- أحمد حمي و زهيرة كيسي، صور جرائم تقنية المعلومات وفقا للاتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، المجلد 10، العدد01، ابريل 2019.

2- احمد فتحي سرور، الحق في حرمة الحياة الخاصة، مجلة القانون والاقتصاد، العدد54، سنة1984.

3- الذهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية –دراسة مقارنة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد08، المجلد01،سنة 2017.

4- ألفة المنصوري، حماية المعطيات الشخصية في مواقع التواصل الاجتماعي- دراسة مقارنة، المجلة الدولية للقانون، كلية القانون بجامعة قطر، المجلد التاسع، العدد الثالث، 2020، ص100. (89-121).

5- الشيخ الحسين محمد يحي، سيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية –دراسة مقارنة في القانون البريطاني والإماراتي، مجلة القضاء والقانون، مركز البحوث والدراسات القضائية، عدد 04، ابريل 2018.

6- أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 17، العدد01، 2018.

7- بخوش، الجرائم الماسة بسلامة المعطيات ذات الطابع الشخصي وفقا للقانون 18-07- معالجة معطيات فيروس كورونا –نموذجا، مجلة أبحاث قانونية وسياسية، المجلد6، العدد01، جوان(2021).

8- بطيحي نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، المجل01، العدد01، جوان 2019.

9- بليدي دلال، وبوقرين عبد الحليم، الآليات القانونية لمكافحة الجرائم الإلكترونية ضد الأطفال،مجلة التمكين الاجتماعي،العدد01، مارس2019.

10- بن حيدة محمد، مكانة الحق في الحياة الخاصة في ظل التعديل الدستوري 16-01، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد العاشر، المجلد الأول، جوان 2018.
11- بن زيطة عبد الهادي، ضرورة إنشاء سلطة إدارية مستقلة كآلية للحماية القانونية للبيانات الشخصية في مواجهة استخدامات المعلوماتية، مجلة الحقيقة، جامعة أدرار، العدد 39، ديسمبر 2016.
12- بهلول سمية، الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال ومكافحتها،مجلة العلوم القانونية والاجتماعية، المجلد السادس، العدد الثالث، ديسمبر 2021.
13- بوخلوط الزين، الحق في النسيان الرقمي، مجلة المفكر، العدد الرابع عشر، 2016، جامعة محمد خيضر - بسكرة، الجزائر.
14- بوزيدي أحمد تجاني، الحق في الدخول في طي النسيان الرقمي كآلية لحماية الحق في الحياة الخاصة، مجلة صوت القانون، المجلد السادس، العدد02/ نوفمبر 2009.
15- تبينة حكيم، آليات الضبط الإداري لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، المجلة الجزائرية للعلوم السياسية والقانونية، المجلد 58، العدد: 01، سنة 2021.
16- تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18-07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية،المجلد04، العدد 02، سنة 2019.
17- جدي نجاة، عدلي محمد عبد الكريم، مبررات تدخل الأداة الجنائية في مجال حقوق التأليف، المجلد السابع، العدد02، نوفمبر 2020.
18- جليلة بنت صالح نعمان، حق الخصوصية دراسة مقارنة بين القانون الإسلامي والقانون الوضعي- القانون الجزائري أنموذجا، مجلة الشريعة والاقتصاد، جامعة الإخوة منتوري – قسنطينة، عدد10، المجلد05، سنة 2016.
19- جورج لبكي، المعاهدات الدولية للانترنت،: حقائق وتحديات، مجلة الدفاع الوطني اللبناني، العدد 83، كانون الثاني/ يناير 2013.
20- جيهان فقيه، حماية البيانات الشخصية في الإعلام الرقمي، مجلة العلوم الإنسانية، العدد السابع /الجزء(1)، جوان 2017.
21- حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد08، العدد04، سنة 2019.
22- حسينة شرون، فعالية التشريعات العقابية في مكافحة الجرائم الالكترونية، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، المجلد الأول، العدد01، سنة 2009.

23- خالد ممدوح إبراهيم محمد، الحماية الجنائية للتوقيع الإلكتروني في القانون الاتحادي رقم2 لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات (المعدل بالقانون رقم 5 لسنة 2012)، مجلة الفكر الشرطي، المجلد الثالث والعشرون، العدد88، يناير 2014.

24- خالدي فتيحة، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كآلية لحماية الحق في الخصوصية، مجلة الحقوق والعلوم الإنسانية، المجلد 13، العدد 04(2020).

25- دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع،جمعية المكتبات والمعلومات السعودية، مكتبة الملك فهد الوطنية، الرياض، سنة 1431هـ/2010م.

26- رضا هميسي، ضمان حق النفاد إلى المعلومات على ضوء الدساتير المغاربية، مجلة العلوم القانونية والسياسية، عدد 14، أكتوبر 2016، ص 249.

27- رياض العجلاني، تطور إجراءات النظر في الطلبات الفردية أمام المحكمة الأوروبية لحقوق الإنسان،مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28 العدد الثاني، 2012.

28- ريم بلحسن، أحمد بولباري، الحق في خصوصية المعطيات الشخصية في التشريع الجزائري – دراسة في ظل القانون رقم 18-07، مجلة العلوم القانونية والاجتماعية، المجلد الخامس، العدد الثالث، سبتمبر 2020.

29- سالم بن محمد السالم، السرقات العلمية في البيئة الالكترونية دراسة للتحديات والتشريعات المعنية بحماية حقوق المؤلف، جمعية المكتبات والمعلومات السعودية، الأمن المعلوماتي، مكتبة الملك فهد الوطنية، الرياض- المملكة العربية السعودية، 2010.

30- سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية – دراسة في القانون الفرنسي (الجزء الأول)، مجلة الحقوق، جامعة الكويت، عدد03-السنة 35، سبتمبر 2011.

31- سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية- دراسة في القانون الفرنسي(الجزء الأول)، مجلة الحقوق، جامعة الكويت، عدد04-السنة 35، ديسمبر 2011.

32- سعد منور سعد البشتاوي، الحماية الدستورية للخصوصية المعلوماتية، المجلة الأردنية للمكتبات والمعلومات، مج(52)، ع2، الجامعة الأردنية مايو 2017.

33- سماعيلي مصطفى، البيانات الحساسة وفيروس كورونا- كوفيد19" البيانات الطبية نموذجا"، مجلة القانون والأعمال الدولية، المغرب، 22 ابريل 2020، ص06 متاح على الموقع **./**https://www.droitetentreprise.com/19116

34- طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري – دراسة في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للباحث، العدد 02-2018.

35- عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية : دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد09، العدد03، سنة 2020.

36- عائشة بن قارة مصطفى، آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم (18-07)، مجلة العلوم القانونية والسياسية، المجلد 10، العدد1، ابريل 2019.

37- عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقار ن، مجلة الحقوق والحريات، جامعة محمد خيضر – بسكرة، العدد الثاني، 2014.

38- فاطمة مصفح، دور محاربة التقليد في حماية برامج الحاسوب في التشريع الجزائري، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة، المجلد الأول، العدد12، سنة 2017.

39- كحلاوي عبد الهادي، بن زيطة عبد الهادي، آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، المجلد 07، العدد02، 2021.

40- كمال بوبعاية ومبروك لمشونشي، الحماية القانونية الدولية للمعطيات الشخصية في البيئة الرقمية، مجلة الدراسات القانونية والسياسية، المجلد07، العدد01، يناير 2021.

41- كوثر منسل وحميد شاوش، حماية المعطيات الشخصية في التشريعات العربية –دراسة مقارنة، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد02، 2021.

42- ماروك نصر الدين، الحق في الخصوصية، مجلة كلية العلوم الإسلامية- الصراط-، السنة الرابعة، العدد السابع، ربيع الثاني 1424هـ، جوان 2003م، رابط المقال" **https://www.asjp.cerist.dz/en/downArticle/412/5/1/84523**"

43- متولي النقيب، التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية، ورقة بحث مقدمة في إطار المؤتمر السادس لجمعيات المكتبات والمعلومات السعودية، جمعية المكتبات والمعلومات السعودية، الأمن المعلوماتي، مكتبة الملك فهد الوطنية، الرياض- المملكة العربية السعودية، 2010.

44- محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، جامعة زياني عاشور الجلفة، المجلد الأول، العدد الأول، 2017.

45- مروة زين العابدين صالح، الحماية القانونية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقين والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع،مصر، سنة 2016.

46- مريم لوكال، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي (في ضوء قانون حماية المعطيات رقم: 18-07)، مجلة العلوم القانونية والسياسية، جامعة حمة لخضر- الوادي، العدد 01، سنة 2019، الجزائر.

47- مريم لوكال، قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، المجلد 04، العدد03، 2021.

48- نبيلة رزاقي، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي –دراسة مقارنة-، مجلة الدراسات القانونية المقارنة، المجلد07، العدد 01، 2020.

49- هاجر كرماش، سلامي ميلود، حماية المصنفات الرقمية في ظل اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية "تربس"، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد13، العدد 02، أكتوبر 2021.

50- هبة أحمد، بن قادة محمود أمين، الآليات القانونية لحماية المستهلك الإلكتروني وفق القانون 18-05، المتعلق بالتجارة الإلكترونية، مجلة القانون الدولي والتنمية، المجلد8 / العدد1 (2020).

51- ويس نوال، آليات حماية حقوق الإنسان في إطار مجلس أوروبا، مجلة الدراسات الحقوقية، جامعة سعيدة، العدد الثامن،2013.

52- يحي تومي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد رقم04، العدد رقم 02، سنة 2019.

-باللغة الأجنبية:

1- Bracy Jididiah, Westin's privacy scholarship, research influenced a generation GR,TRND2013, p04.

2- Dawn Iacobucci; Jonathan D. Hibbard, Toward an encompassing theory of business marketing relationships (BMRS) and interpersonal commercial relationships (ICRS): An empirical generalization, Journal of Interactive Marketing, Vol 13, Nu3,1999**.**

3- Desforges Alix, « Cyber-Terrorism : quel Périmètre », fiche N11 de l'institut de recherche stratégique de l'école militaire (IRSEM), Décembre 2011, Article on ligne disponible sur le site : www.defense.gov.fr " file:///C:/Users/USER/Downloads/Fiche_n11_perimetre_cyberterrorisme.pdf "date de consultation de site le : 29 /01/ 2021.

4- Jean-Christophe, Duton et Virginie Becht, Le droit à l'oubli numérique : un vide juridique ?, disponible sur https://www.journaldunet.com/ebusiness/le-net/1031442-le-droit-a-l-oubli-numerique-un-vide-juridique/ , le 23/01/2021.

5- Loura MARCU, PROTECTION DES DONNES A CARACTERE PERSONNEL: QUELLES IMPLIQUATIONS POUR LES ACTIVITES DE MARKETING, Revue Valaque d'Etudes Economiques, Volume6(20) ,$N^0$1, 2015.

6- Miller,A, The assault of privacy, An Arbor, university of Michigan press, 1971.

7- RENALD OTTENHOF, Infraction contre les biens, Rev.sc.crim, 1996, chronique de jurisprudence.

8- Samuel D. Warren; Louis D. Brandeis, The Right To Privacy, Harvard law review, Vol 6, No-5-m December 15,1890, p193-194.

9- Tian, Ling; Li, Jiaxin; Li, Wei; Ramesh, Balasubramaniam; Cai, Zhipeng, Optimal Contract-based Mechanisms for Online Data Trading Markets , IEEE Internet of things journal , Vol 14, Nu 08,2019.

10- Yibin Li; Wenyun Dai; Zhong Ming; Meikang Qiu , Privacy Protection for Preventing Data Over-Collection in Smart City, IEEE

11- Transactions on Computers, Volume: 65, Issue: 5, May 1 2016.

6- النصوص القانونية

أ- التشريع الجزائري

أ-1- الدستور

دستور الجمهورية الجزائرية الديمقراطية الشعبية، ج.ر.ج.ج عدد 76 المؤرخة في 08 ديسمبر 1996، المعدل ب:

- القانون رقم 02-03 المؤرخ في 10 ابريل 2002- ج.ر.ج.ج عدد25 المؤرخة في 2002/04/14.

- القانون رقم 08-19 المؤرخ في 15 نوفمبر 2008 – ج.ر.ج.ج عدد63 المؤرخة في 2008/11/16.
- القانون رقم 16-01 المؤرخ في 6 مارس 2016 – ج.ر.ج.ج عدد14 المؤرخة في 2016/03/7
- المرسوم الرئاسي رقم 20-442الممؤر خ في في 30 ديسمبر 2020، ج.ر.ج.ج عدد 82، المؤرخة في 30 ديسمبر 2020.

أ-2- القوانين العضوية

1- القانون العضوي 12-05 المؤرخ في 12 يناير 2012، المتعلق بالإعـــــلام، ج.ر.ج.ج عدد02 المؤرخة في 15 يناير 2012.

أ-3- القوانين

1- الأمر 66-156 المؤرخ في 18 صفر 1386 الموافق 08 يونيو سنة 1966 المتضمن قانون العقوبات، المعدد والمتمم، لاسيما ما تضمنه القانون رقم 04-15 المؤرخ في 10-11-2004، ج.ر.ج.ج عدد71 المؤرخة في 10 نوفمبر 2004.

2- الأمر 75-58، المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم، ج.ر.ج.ج عدد25 المؤرخة في 26 سبتمبر 1975.

3- الأمر 03-05 المؤرخ في 19 يوليو سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر.ج.ج عدد44 المؤرخة في 23 يوليو سنة 2003.

4- الأمر 03-11 المؤرخ في 26 غشت 2003، المتعلق بالنقد والقرض، المعدل والمتمم، ج.ر.ج.ج عدد52، المؤرخة في 27 غشت 2003.

5- القانون 15-04، المؤرخ في أول فبراير 2005، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر.ج.ج عدد06، المؤرخة في 10 فبراير 2005.

6- الأمر 75-58، المتضمن القانون المدني المعدل والمتمم، لاسيما سنة 2005 بموجب القانون 05-10 المؤرخ في 20 يونيو 2005(ج.ر 44، ص24)

7- الأمر 06-03 المؤرخ في 15 يوليو 2006، المتضمن القانون الأساسي العام للوظيفة العمومية، ج.ر.ج.ج عدد46 المؤرخة في 16 يوليو 2006.

8- القانون 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد84 المؤرخة في 24 ديسمبر 2006.

9- القانون 09-04، المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد47، المؤرخة في 16 أوت 2009.

10- القانون رقم 13-07، المؤرخ في 29 أكتوبر 2013، المتضمن تنظيم مهنة المحاماة، ج.ر.ج.ج عدد55 المؤرخة في 30 أكتوبر سنة 2013.

11- القانون 14-04 المؤرخ في 2014/02/24، المتعلق بالنشاط السمعي البصري، ج.ر.ج.ج عدد16 بتاريخ 2014/03/23.

12- القانون 15-04، المؤرخ في أول فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج عدد 06 المؤرخة في 10 فبراير 2015.

13- القانون 18-04، المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج.ر.ج.ج عدد 27، المؤرخة في 13 ماي 2018.

14- القانون 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الالكترونية، ج.ر.ج.ج عدد 28، المؤرخة في 16 ماي 2018.

15- القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج عدد34، المؤرخة في 10 يونيو 2018.

16- القانون رقم 20-05 المؤرخ في 28 ابريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ج.ر.ج.ج عدد 25 بتاريخ 29 ابريل 2020.

أ-4- المراسيم:

1. المرسوم الرئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997، المتضمن انضمام الجمهورية الجزائرية الديمقراطية الشعبية، مع التحفظ، إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، المؤرخة في 09 سبتمبر 1886، والمتممة بباريس في 04 مايو سنة 1986 والمعدلة ببرلين في 13 نوفمبر سنة1908، والمتممة ببرن في 20 مارس 1914 والمعدلة بروما في 02 يونيو سنة 1928 وبروكسل في 26 يونيو سنة 1948 و استوكهولم في 14 يوليو سنة 1967 وباريس في 24 يوليو سنة1971 والمعدلة في 28 سبتمبر سنة 1979. ج.ر.ج.ج عدد61، المؤرخة في 14 سبتمبر 1997.

2. المرسوم الرئاسي رقم 06-62 المؤرخ في 11 فبراير 2006، المتضمن المصادقة على الميثاق العربي لحقوق الإنسان المعتمد بتونس في مايو سنة 2004، ج.ر.ج.جعدد08، المؤرخة في 15 فبراير 2006.
3. المرسوم الرئاسي رقم 14-252، المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010.
4. المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد53 المؤرخة في 08 أكتوبر 2015.
5. المرسوم الرئاسي 20-183 المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد40 المؤرخة في 18 يوليو 2020.
6. المرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر 2020، ج.ر.ج.ج عدد82، المؤرخة في 30 ديسمبر 2020.
7. المرسوم الرئاسي 21-439 المؤرخ في 07 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد86 المؤرخة في 11 نوفمبر 2021.

ب- التشريع المصري

1- القانون 05-10 المؤرخ في 20 يونيو 2005(ج.ر 44، ص24) محمد حسن قاسم، التعاقد عن بعد، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص105-106.
2- القانون رقم 151 لسنة 2020، المتعلق بحماية البيانات الشخصية المصري، ج.ر العد 28 مكرر (هـ) في 15 يوليو سنة 2020.

ت- التشريع التونسي

1- القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004، المتعلق بحماية المعطيات الشخصية، الموقع الرسمي للهيئة على الإنترنت " http://www.inpdp.nat.tn/Receuil_2019.pdf الدستور التونسي لسنة 2014 محمل من الموقع الالكتروني " http://www.inpdp.nat.tn/Receuil_2019.pdf " .

ث- التشريع المغربي

1- القانون 08-09، الصادر في 18 فبراير 2009، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الموقع الرسمي للجنة المغربية على الإنترنت " http://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf

2- ظهير شريف رقم 15.09.1 مؤرخ في 18 فبراير 2009 متعلق بتنفيذ القانون 09-08، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 5711 بتاريخ 23 فبراير 2009 الموقع الرسمي للجنة المغربيـــة لحماية المعطيات، "https://www.cndp.ma/images/lois/Loi-09-08-Ar.pdf"

3- المرسوم رقم 09-165 المؤرخ في 21 ماي 2009، المتعلق بتطبيق أحكام القانون 08-09، الصادر في 18 فبراير 2009، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الموقع الرسمي للجنة المغربية على الإنترنت " http://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf "

ج- التشريع الفرنسي

- La Loi N^0 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O du 07/08/1978; Modifié par Loi n°2004-801 du 6 août 2004 , disponible sur site : https://www.legifrance.gouv.fr/loda/id/LEGIARTI000006529397/2004-08-07/.

ح- الاتفاقيات:

- باللغة العربية

1. اتفاقية فينا لقانون المعاهدات المبرمة في 23 مايو سنة 1969، التي انضمت إليها الجزائر، بتحفظ، بموجب المرسوم 87-222المؤر خ في 13 أكتوبر 1987، ج.ر.ج.ج عدد42، المؤرخة في 14 أكتوبر 1987.

2. الاتفاقية الأوروبية 108 لسنة 1981، المتعلقة بحماية الأشخاص تجاه معالجة البيانات ذات الطابع الشخصي، متاحة على الربط "https://rm.coe.int/1680078b37 ".

3. اتفاقية برن لحماية المصنفات الأدبية والفنية لسنة 1886، موقع المنظمة العالمية للملكية الفكرية (WIPO)، الاطلاع بتاريخ 06 نوفمبر 2021على العنوان التالي: " https://www.wipo.int/treaties/ar/ip/berne/summary_berne.html "

4. اتفاقية بودابست، المتعلقة بالجرائم الالكترونية، الموقعة في 23 نوفمبر 2001 والتي دخلت حيز التنفيذ بتاريخ 2004/07/01، والمحملة من الموقع الالكتروني للمجلس الأوروبي بتاريخ 2021/01/28. https://rm.coe.int/budapest-convention-in-arabic/1680739173 "

5. اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، والتي تم اعتمادها في الدورة العادية الثالثة والعشرون لرؤساء دول وحكومات الإتحاد الإفريقي، المنعقدة في ملابو، غينيا الاستوائية بتاريخ 27 يونيو 2014، متاحة على الموقع الالكتروني للاتحاد الإفريقي على الرابط: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_a.pdf.

6. الميثاق العربي لحقوق الإنسان ،تم تحميل نسخة من الميثاق العربي لحقوق الإنسان من الموقع الالكتروني لجامع الدول العربية، المتاح على الرابط التالي:_

www.lasportal.org/ar/sectors/dep/HumanRightsDep/Documents/عربي.pdf

"

7. الميثاق الإفريقي لحقوق الإنسان والشعوب، على الرابط " http://hrlibrary.umn.edu/arab/a005.html" .

8. معاهدة المنظمة العالمية للملكية الفكرية بشأن حق المؤلف، موقع المنظمة العالمية للملكية الفكرية، متاحة على الرابط "https://wipolex.wipo.int/ar/text/295156 "

9. الاتفاقية المتعلقة بالجريمة الالكترونية "بودابست"، متاحة على الموقع الرسمي لمجلس أوروبا، متاحة على الرابط التالي "https://rm.coe.int/16802fa3ff "

10. اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخص (Convention on cyber security and personal data protection)، متاحة على رابط الموقع الإلكتروني للاتحاد الإفريقي، رابط التحميل: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_a.pdf.

11. البروتوكول الرابع الملحق بالاتفاقية الأوروبية، متاح على الموقع الخاص بمجلس أوروبا، على الرابط "https://www.echr.coe.int/documents/convention_ara.pdf " تاريخ آخر زيارة للموقع: 2022/02/17.

12. الاتفاقية الأوروبية لحقوق الإنسان، مشتملة على أحدث التعديلات والبروتوكالات الملحقة، متاحة على الربط أدناه، بتاريخ 2021/02/22:

https://www.echr.coe.int/documents/convention_ara.pdf

- **باللغة الأجنبية**

1. la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Strasbourg, 28.1.1981; disponible sur site – Conseil de l'Europe- " https://rm.coe.int/1680078b39"

2. Convention for the project of the individuals with regard to automatic processing of personel data Wiliam J. Clinton & Albert Gore, Jr, "A Framework for global electronic commerce" , July 1 , 1997, P146

3. OECD Guideline sonthe protection of privacy and transborder flows of personal data (1980) updated in 2013, See the link below, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Viewed date: October 14, 2021 at 10:00.)

4. OECD Guideline sonthe protection of privacy and transborder flows of personal data (1980) updated in 2013, OP-CIT. https://www.echr.coe.int/documents/convention_ara.pdf

7- الإعلانات:

1. الإعلان العالمي لحقوق الإنسان لسنة 1948، موقع منظمة الأمم المتحدة، منشور على الموقـــــع الالكتروني " **www.un.org/ar/universal-declaration-human-refights/index.htmail**

2. النظام الأساسي للمحكمة العربية لحقوق الإنسان، نسخة الكترونية محملة من موقع جامعة الدول العربية بتاريخ 2018/02/12"

http://www.lasportal.org/ar/humanrights/Committee/Documents/

8- التقارير والتوصيات:

1- Délibération CNIL n^0 85-50 du 22 Octobre 1985, portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, disponible sur " https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017654812" en date du 25 décembre 2020.

2- Délibération CNIL n^0 00-015 du 21 mars 2000 portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Jean Rostand de Nice, destiné à gérer à la cantine scolaire par la connaissance des empreintes digitales (demande d'avis n° 636.783); disponible sur https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017653883/ , le 25/12/2020.

3- Délibération SAN-2021-014 du 15 septembre 2021 disponible sur site Cnil " https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044043045". Consulté le 13/01/2022

4- Desforges Alix, « Cyber-Terrorism : quel Périmètre », fiche N11 de l'institut de recherche stratégique de l'école militaire (IRSEM), Décembre 2011, Article on ligne disponible sur le site : www.defense.gov.fr " file:///C:/Users/USER/Downloads/Fiche_n11_perimetre_cyberterrorisme.pdf "date de consultation de site le : 29 /01/ 2021.

5- المواقع الإلكترونية

1- أحمد محمد الشامي والدكتور سيد حسب الله، الموسوعة العربية لمصطلحات علوم المكتبات والمعلومات والحاسبات،"https://portal.arid.my/ar-LY/Posts/Details/96fde0a9-2a34-460d-a472-b

2- Adrian Croft, Britain's Brown apologies over lost data, at Reuters, on line at https://www.reuters.com/article/britain-data-idUSL2119814420071121, 21 November 2007.

3- John Shattuck, Rights of privacy, national textbook Co, 1977. Available at the site:" http://publications.ceu.edu/publications/shattuck/1977/13078".

4- Libya : African Rights Court Issues First Ruling Against a State Human Rights Wach: https://www.hrw.org/ar/news/2011/03/30/242460, la date de mise en ligne le 30/09/2021.

5- Wiliam J. Clinton & Albert Gore, Jr, "A Framework for global electronic commerce" , July 1 1997. https://www.fidh.org/IMG/pdf/final_pp_arab_court_-_ar-2.pdf

الفهرس

ملخص

ملخص:

كرست العديد من التشريعات الدولية تدابير متنوعة لحماية البيانات الشخصية من تأثير التقنيات الرقمية المتسارعة، من خلال ضبط كيفيات المعالجة و إقرار جزاءات عند المساس غير المشروع بأي جانب من جوانب هذه البيانات. والمشرع الجزائري بدوره تدارك هذا الجانب الحساس وأكد على حماية المعطيات الشخصية بصورة مباشرة أو غير مباشرة، بموجب نصوص قانونية متفرقة، كرست تدابير تتراوح بين الحماية الإجرائية، المؤسساتية والجزائية، شكلت في مجملها حماية قانونية نسبية، تخص في الأساس المعالجة الآلية لمعطيات الأشخاص الطبيعيين.

الكلمات المفتاحية: الخصوصية، البيانات؛ المعطيات ذات الطابع الشخصي؛ المعالجة الآلية؛ المعطيات الحساسة.

Summary:

Much international legislation have dedicated various measures to protect personal data from the impact of accelerating digital technologies, by controlling the processing methods and imposing penalties when any aspect of this data is unlawfully violated. The Algerian legislator, in turn, redressed this sensitive aspect and emphasized the protection of personal data, directly or indirectly, according to separate legal texts, which enshrined measures ranging from procedural, institutional and penal protection, as a whole, which constituted relative legal protection mainly, related to the automated processing of data of natural persons.

Key words: privacy; data; personal data; automated processing; sensitive data.

Résumé:

De nombreuses législations internationales ont consacré diverses mesures pour protéger les données personnelles de l'impact de l'accélération des technologies numériques, en contrôlant les méthodes de traitement et en imposant des sanctions en cas de violation illicite de tout aspect de ces données. Le législateur algérien a, à son tour, redressé cet aspect sensible et mis l'accent sur la protection des données personnelles, directement ou indirectement, selon des textes juridiques distincts, qui consacrent des mesures allant de la protection procédurale, institutionnelle et pénale, dans leur ensemble, qui constituent une protection juridique relative, principalement liés au traitement automatisé de données de personnes physiques.

Mots-clés : vie privée; données; données personnelles; Traitement automatisé; données sensibles.