

الحق في خصوصية البيانات الشخصية عبر المجال الرقمي وسبل حمايتها

في التشريع الجزائري

The Right to Privacy of Personal Data Through the Digital Field and Ways to Protect It in Algerian Legislation

بهادي عبد القادر^{1*}، الصادق عبد القادر²

1- جامعة أحمد درايعة - أدرار (الجزائر)، مخبر القانون والمجتمع،

bahaddi.abdelkader@univ-adrar.edu.dz

2- جامعة أحمد درايعة - أدرار (الجزائر)، - Saddek7@gmail.com

تاريخ الاستلام: 2024/06/23 تاريخ القبول: 2025 /05/14 تاريخ النشر: 2025/06/05

ملخص:

تعتبر الخصوصية في التشريع الجزائري خط أحمر لا يمكن تجاوزه، وكذا في معظم التشريعات الدولية والتي لها مبدأ الديمقراطية، فلا يمكن لأي شخص المساس بخصوصية شخص آخر ولو كان من السلطات الأمنية إلا بترخيص مسبق، فقد عُنيت الخصوصية بحماية قوية فحماها المشرع بسن ترسانة من القوانين بدأ من الحماية الدستورية إلى الحماية بقوانين خاصة تنظمها، وذلك لردع كل من تسول له نفسه انتهاك خصوصية شخص آخر، خاصة وأنه أصبح من السهل انتهاكها في المجال الرقمي نظرا للتطور الهائل للتبرمجيات والمواقع المتواجدة على شبكة الانترنت.

وبما أن شبكة الانترنت شبكة عالمية لا تعير الحدود الدولية أي اهتمام، فالعالم في منظورها قرية صغيرة، ونظرا كذلك للأهمية البالغة لاستعمالها في شتى المجالات، أصبح جليا لكافة دول العالم إيجاد طرق بديلة ومتطورة تكون مشتركة، كإبرام اتفاقيات ومعاهدات لحماية قوية للبيانات الشخصية في المجال الرقمي.

الكلمات المفتاحية: البيانات الشخصية؛ الخصوصية؛ المخاطر؛ المجال الرقمي؛ عصرنة؛ الذكاء الاصطناعي.

Abstract:

In Algerian legislation, privacy is considered a red line that cannot be crossed, as well as in most international legislations that have the principle of democracy. No person can infringe on the privacy of another person, even if he is from the security authorities, except with prior authorization. Privacy was meant for strong protection, so the legislator protected it by enacting an arsenal of laws that began From constitutional protection to protection through special laws regulating it, in order to deter anyone who tempts himself to violate another person's privacy, especially since it has become easy to violate it in the digital field due to the tremendous development of software and websites on the Internet

Since the Internet is a global network that does not pay any attention to international borders, the world in its perspective is a small village, and also given the extreme importance of its use in various fields, it has become clear for all countries of the world to find alternative and advanced methods that are common, such as concluding agreements and treaties for strong protection of personal data in the digital field.

keywords:

Personal data .privacy; risks; digital field; modernization; artificial intelligence.

مقدمة:

يشهد هذا العصر موجة من التطور الهائل والسريع في مجال التكنولوجيا وكذا المعلوماتية ويظهر هذا التطور جليا في جميع المجالات خاصة على مستوى التواصل بين الافراد وكذا سرعة تدفق المعلومة وانتشارها، إلا أنه من المعلوم أن هذا التطور السالف الذكر في مجال التكنولوجيا والمعلوماتية قد نتج عنه العديد من المخاطر التي تواجه البيانات الشخصية، ويكون ذلك ناتجا عن ادخال المعلومات الشخصية عبر المنصات الإلكترونية.

ومن هنا تظهر أهمية البحث في الموضوع من خلال محاولة إيجاد حلول للمشاكل التي تواجه تخزين وتبادل ونقل وجمع ومعالجة البيانات الشخصية الخاصة بالأفراد في المجال الرقمي، ويكمن هذا الخطر في سهولة الوصول الى تلك البيانات بطرق غير شرعية وجد متطورة واستغلالها في اهداف

غير مشروعة، وهنا نكون أمام انتهاك للحق في الخصوصية والتي تعتبر حق مشروع جدير بالحماية، ولمعالجة هذا الموضوع انطلقنا من الاشكالية التالية : ما هي المخاطر التي تواجه البيانات الشخصية في البيئة الرقمية، وما هي سبل حمايتها في التشريع الجزائري؟

ولمعالجة الاشكالية انتهجنا المنهج الوصفي من أجل شرح المصطلحات المتعلقة بالبحث، وكذا المنهج التحليلي الذي يساعد في تحليل مضمون المواد القانونية التي تم الإستدلال بها في بحثنا، معتمدين على خطة متكونة من مبحثين يضم المبحث الأول: المخاطر المهددة للبيانات الشخصية في البيئة الرقمية، أما المبحث الثاني: الحماية القانونية للبيانات الشخصية عبر المجال الرقمي في التشريع الجزائري.

المبحث الأول: المخاطر المهددة للبيانات الشخصية في البيئة الرقمية

إن التطور التكنولوجي في مجال المعلوماتية أدى الى صنع أرض خصبة لتزايد الاخطار التي تهدد البيانات الشخصية في البيئة الرقمية وتعدد صور انتهاكها أما بالتزوير او الحذف أو القرصنة واستعمالها في أمور غير مشروعة لذلك سنعالج في هذا المبحث المخاطر التي تهدد البيانات الشخصية من خلال مطلبين في المطلب الأول نعالج المخاطر التي تهدد البيانات الشخصية عند المعالجة الرقمية وفي المطلب الثاني نعالج المخاطر المهددة للبيانات الشخصية في الظروف الاستثنائية.

المطلب الأول: المخاطر التي تهدد البيانات الشخصية عند المعالجة الرقمية.

تبقى البيانات الشخصية بعيدة عن المخاطر قبل ادخالها الى البيئة الرقمية، لكن وبعد ادخالها لهذه الأخيرة ندق ناقوس الخطر وتبدأ رحلة المغامرة بالبيانات الشخصية، وأول خطر يهدد البيانات الشخصية في هذه المرحلة وهو عند إدخالها للبيئة الرقمية وتعديلها سنتطرق له في الفرع الأول، ثم يأتي بعدها خطر الانترنت والذكاء الاصطناعي على البيانات الشخصية في الفرع الثاني.

الفرع الأول: المخاطر المهددة للبيانات الشخصية عند إدخالها وتعديلها.

تعتبر مرحلة إدخال وتعديل البيانات الشخصية في البيئة الرقمية من أول الخطوات خطورة على انتهاك البيانات الشخصية، إذ يعد الفرد مجبرا لا مخريرا للإدلاء بمعلوماته أو بياناته الخصوصية حين يطلب منه ذلك من طرف مؤسسات عامة تابعة للدولة مثل الإدارات، أو المؤسسات الخاصة ذات الطابع الاقتصادي أو التجاري مثل البنوك، الفنادق... وغيرها.

"فعند تلقي البيانات الشخصية من قبل الجهات التي تتولى جمع هذه البيانات فإنها تقوم بتصنيفها، أي يتم إنشاء ملف خاص بكل شخص إذ يعتبر زبون أو عميل، ويحتوي هذا الملف على كل البيانات الخاصة به " (حسام محمد نبيل الشنراقي، 2019، صفحة 27).

ومن المعلوم أن هذه العملية تتم بواسطة استخدام الكمبيوتر، الذي يعمل بتقنية البرمجيات والتي تعتبر جد متطورة عكس العمل بالملفات الورقية التي أصبحت طي النسيان، فبهذه التقنية الحديثة يسهل إدخال بيانات الشخص وتنظيمها فتبقى محفوظة فيه إلا ان هذه التقنيات الحديثة لها سلبيات ومخاطر وخيمة على البيانات الشخصية من حيث التلاعب بيها كمسحها أو تغييرها أو تداولها.

"بل أنه في الكثير من الأحيان لا تعتمد المنشأة على البيانات التي قامت بجمعها فحسب، بل أنها تكمل هذه البيانات ببيانات أخرى تم جمعها من قبل منشآت أخرى، وهذا ما يؤدي إلى التعامل بالبيانات و الاتجار بها ، وهو ما من شأنه أن يشكل خطرا كبيرا على البيانات الشخصية للأفراد " (حسام محمد نبيل الشنراقي، 2019، الصفحات 27-28)

الفرع الثاني: تهديد شبكة الانترنت وبرامجها على البيانات الشخصية

تعتبر الانترنت أكبر خطرا محققا بالبيانات الشخصية، حيث بعد ظهور ما يسمى بالإنترنت الذي أحدث ثورة في العالم في مجال الاتصالات والمعلومات أين تخطت جميع حدود العالم الجغرافية وجعلته كقرية صغيرة، فبظهورها اختصر الزمان والمكان، والأدهى والأمر من ذلك أصبح الجميع لا يستغنون عن الانترنت حيث أصبحت شريان الحياة بالنسبة للفرد أو المؤسسة أو الشركة.

ونتيجة لذلك باتت خصوصية البيانات الشخصية عرضة للإطلاع من طرف الغير سواء بالموافقة أو خلافا لرغبة أصحابها، كما أن الخطير في الأمر أن مجرد التصفح عبر صفحات الانترنت يترك آثار وكمية واسعة من البيانات التي تدل على أصحابها "مثال ذلك ما يحصل في مجال التجارة الإلكترونية عبر الانترنت حيث تطلب الشركات من المستخدمين تعبئة نماذج تحتوي على معلومات شخصية، كالاسم والعنوان والعمل ورقم الهاتف والبريد الإلكتروني والدخل وغيرها، بالإضافة إلى دفع الثمن إلكترونيا ما يتطلب إدخال رقم بطاقة الإئتمان ونوعها وتاريخ إنتهاء صلاحيتها مثلا" (علي وهي ديب، 2023، صفحة 320)

وكما هو معلوم "إن الوسائل التي يتم بواسطتها تحديد هوية مستخدمي الانترنت كثيرة ومتنوعة لا يمكن حصرها ويكون ذلك بدأ من تسجيل المستخدم من خلال مزودي الخدمات إلى ترقيم وتحديد الأجهزة التي غالبا ما تكون مرتبطة بحسابات على الإنترنت وصولا إلى معرفة الهوية الفردية التي توفرها متصفحات الانترنت أو تحفظ في ملفات تعريف الارتباط، فضلا عن عنوان بروتوكولات الانترنت IP addresses التي يتم تخصيصها للمستخدمين، إن جميع هذه الإجراءات قد تؤدي إلى إظهار هوية المستخدم" (توبي مندل وأندور بوديفات وبن واجنر وديكسي هوتن ونتاليا توريس، 2013، صفحة 39).

ومن هنا نجد أن شبكة الانترنت لها خطرا جسيما على البيانات الشخصية فبواسطتها يتم كشف البيانات الشخصية للمستخدم وتكون عرضة للانتهاك.

كما أن البرامج المرتبطة بالإنترنت لها نفس خطورة الانترنت بحد ذاتها ومثال ذلك "موقع الفابيسبوك، يواجه مستخدمي موقع الفاييسبوك Facebook يوميا مخاطر ناجمة عن تقديمهم طلبات تسجيل على الموقع، ومن هذه المخاطر اختراق الحسابات وتوزيع الصور الخاصة وصعوبة إزالة أو إلغاء الحساب وما إلى ذلك" (محمد أحمد المعداوي، 2018، صفحة 1967).

كما أنه وبواسطة استخدام تقنيات وملفات الكوكيز Cookise المتواجدة بمتصفحات الانترنت، والتي تعتبر جزءا مهما فيها وهي المسؤولة بشكل كبير في اسطياد البيانات الشخصية لمستخدم الانترنت.

"ويعتبر الكوكيز من حيث المبدأ وسيلة فعالة لتوفير الوقت والطاقة وتجنب التكرار وتحسين الخدمة التي يحصل عليها المستخدم والحد من إعادة إدخال المعلومات أكثر من مرة" (مروة زين العبدین صالح، 2017، صفحة 333).

فإذا كانت هذه ميزة إيجابية في الكوكيز فإن من سلبياته هو أنه قد يكون وسيلة لتتبع المستخدم وكشف بياناته الشخصية.

كما تعد محركات البحث في الانترنت أكثر خطورة من ملفات الكوكيز وعنوان بروتوكول الانترنت على البيانات الشخصية من حيث انتهاكها، إذ تعتبر الوسيلة التي تسهل على المستخدم الوصول إلى المعلومة المطلوبة.

"وتقوم محركات البحث بعمليات جمع وتبويب وتحليل بيانات الاستخدام على نحو واسع مستخدمة إما وسيلة الكوكيز أو غيرها من حزم النبضات أو البتات اللاصقة **Stcky bits**، التي تخزن في كميوترات الزائرين من أجل مساعدة الموقع على التعرف على اتجاه الخصوصية للزائر وتحديد اتجاهات الإعلان وتقديم المحتويات، والمشكلة المثارة أن غالبية هذه المواقع لا تطلع المستخدم على ذلك، وإن كان ثمة توجه في إطار التنظيم الذاتي لقطاعات التجارة الإلكترونية والإعلان على الانترنت أن يتم إعلام المستخدم قبل القيام بذلك إتاحة الخيار له بالقبول أو الرفض" (محمود عبد الرحمان، 2020، صفحة 110).

ومن هنا نجد أن محركات البحث لها دور كبير كذلك في خرق والتعدي على البيانات الشخصية للمستخدم دون علمه، وهذا ما يهدف إلى المساس بحقه والذي هو ضمان الحق في الخصوصية.

ويعد كذلك الذكاء الاصطناعي من أخطر الآليات على البيانات الشخصية من حيث انتهاكها.

حيث يعتبر مصطلح الذكاء الاصطناعي مصطلح حديث النشأة.

"فمن الصعوبة بمكان تعريف الذكاء الاصطناعي، وذلك لكون طبيعة هذا المفهوم نفسه صعب التحديد إلى حد بعيد، ولتبسيط الأمر يمكن القول أن الذكاء الاصطناعي كما وصفه Joh McCarthy، هو أحد العلوم التي تهدف لهندسة وصنع أجهزة وآلات ذكية لا سيما عبر

استخدام برامج الكمبيوتر، وهو يقوم أي الذكاء الاصطناعي على استخدام الحواسيب وبرمجياتها المختلفة لفهم الذكاء والسلوك البشري، والقيام بعمليات تحاكي ما يقوم به الإنسان ولكن من دون الاعتماد على العامل البيولوجي" (علي وهي ديب، 2023، صفحة 339).

ومن هذا المفهوم يتضح لنا أن الذكاء الاصطناعي يشير إلى ذكاء الآلات التي تعمل وفق نظام وبرمجة متطورة لتدرك البيئة المحيطة وتتخذ إجراءات وفق خوارزميات وتقنيات معينة. ومن هنا نقول إنها تعمل عمل الانسان لكن بطريقة أسرع.

لذا أصبح الذكاء الاصطناعي حالياً أكبر الإهتمامات في جل القطاعات إن لم نقل كلها، وذلك نظراً لما له من إمكانيات لتحسين الخدمات بشكل سريع ودقيق.

وبالرغم من إيجابيات الذكاء الاصطناعي إلا أن له سلبيات منها انتهاك الخصوصية وذلك بقدرة الذكاء الاصطناعي للوصول إلى كم هائل من البيانات الشخصية للمستخدم وفي وقت وجيز لتحليلها واستخدامها.

"فتحليل البيانات الشخصية باستخدام تقنيات الذكاء الاصطناعي قد أثر بلا شك على موضوع حماية البيانات الشخصية، ليس فقط بالنظر إلى حجم البيانات فحسب بل أيضاً الطرق التي يتم جمعها بها وطريقة استخدامها وتعقيد المعالجة وعواقبها التي قد تطل الأفراد" (علي وهي ديب، 2023، صفحة 347).

المطلب الثاني: المخاطر المهددة للبيانات الشخصية في الظروف الاستثنائية.

ناهيك إلى ما تم الإشارة إليه فيما سبق من المخاطر المحدقة بالبيانات الشخصية نتيجة المراقبة باستخدام التقنيات الرقمية وكذا الذكاء الاصطناعي، نرجع إلى أخطار أخرى محدقة بالبيانات الشخصية وتتمثل في استهدافها بواسطة إجراءات تباشرها الجهات الأمنية بغرض الحماية والأمن والحفاظ على النظام العام والآداب العامة وكذا في إطار مكافحة الإرهاب وهذا ما سيتم التطرق له في الفرع الأول، أما الفرع الثاني سنتطرق إلى المخاطر المهددة لها نتيجة تدفقها عبر حدود الدولية.

الفرع الأول: المخاطر المهددة للبيانات الشخصية في إطار التحقيق الأمني

إن إلزام الدول المعتمدة النظام الديمقراطي لمبدئ حقوق الإنسان والذي يحميه الدستور، كما يكرس ويضمن حماية الحريات الفردية، والتي تضم بدورها حماية البيانات الشخصية، بحيث لا يتم التعرض لها حتى من قبل السلطات العامة في الدولة أو غيرها.

إلا أنه في حالة الضرورة تستثنى هذه الحماية خاصة إذا تعلق الأمر بالأمن العام للدولة، لأن المصلحة العامة تسبق مصلحة الفرد، لكن كل هذا يلتزم ويراعى مبدأ التناسب، أي يفترض أن تكون الإجراءات التي تتجاوز تلك الحدود ضرورية وتحقق أهداف المصلحة العامة أو حماية حقوق وحريات أشخاص آخرين.

ومن المعلوم أن القانون الدولي لحقوق الإنسان قد أعطى أهمية بالغة لحماية البيانات الشخصية، وكذا الاتفاقية الأوروبية لحقوق الإنسان حثت على ذلك،

أما على المستوى الوطني قد ضمن الدستور حق حماية الخصوصيات ومنها البيانات الشخصية، كما هو الشأن في باقي دول العالم، كما أوجد المشرع الجزائري قوانين تنظم وتحمي هذه الحقوق، حتى في الظروف الإستثنائية وذلك بالتقيد بضوابط تشريعية للحد من احتمال انتهاك أجهزة الأمن لحقوق الإنسان. خاصة في إطار التحقيقات الجنائية.

فحتى في التحقيقات الجنائية لا يسمح بمعالجة البيانات الشخصية بمختلف أنواعها ولو تعلقة بجرائم وإجراءات جنائية، إلا إذا توافرت الضمانات الإجرائية المناسبة ضد المخاطر التي قد تشكلها معالجة تلك البيانات على مصالح حقوق وحريات الأفراد الأساسية.

وكما هو معلوم أن الجزائر شهدت موجة وسنوات سوداء في مجال مكافحة الإرهاب الذي يعتبر مهددا لأمن الدولة واستقرارها، كما يعتبر ظرفا استثنائيا على غرار التحقيق الأمني.

"فتعتمد أحيانا أجهزة الأمن لجمع وحفظ ومعالجة والكشف عن البيانات الشخصية للأفراد بسبب الإشتباه بضلوعهم بجرائم خطيرة كالتجسس أو الإرهاب" (نصيرة تواتي، 2017، صفحة 93)

فمن هنا نجد أنه وبمجرد الاشتباه لزم على أجهزة الأمن أخذ الإحتياط اللازم وذلك بمعالجة وكشف البيانات الشخصية للمشتبه فيه وذلك لأن مصلحة الدولة تفوق مصلحة الفرد بالإضافة أن الأمر يتعلق بحماية وصون الدولة من عمليات إرهابية.

"فعن طريق جمع المعلومات الشخصية عن الأفراد، تكتسب أجهزة الأمن السيطرة على أصحاب تلك البيانات الشخصية." (حسام محمد نبيل الشراقي، 2019، صفحة 70)

فمن هذا المنطلق نلاحظ أن تشديد الرقابة على المشتبه فيهم في مجال الإرهاب ذلك لأخذ الإحتياط من طرف الأمن لأي طارئ ولسهولة تتبع الأحداث عن قرب والتصدي للأعمال الإرهابية المتوقعة والمبرمجة من طرف هؤلاء الارهاب وكذلك للتضييق عليهم.

إلا أنه كما تم التطرق له سابقا أن صلاحيات أجهزة الدولة في هذا المجال تكون مراعية مبدأ التناسب، أي يفترض أن تكون الإجراءات التي تتجاوز تلك الحدود ضرورية وتحقق أهداف المصلحة العامة أو حماية حقوق وحريات أشخاص آخرين.

الفرع الثاني: المخاطر المهددة للبيانات الشخصية بعد تدفقها عبر الحدود الدولية

من المعلوم أن الانترنت تنسم بالطبيعة العالمية، أي أنها كما قلنا سابقا لا تعير الحدود الجغرافية للدولة أي اهتمام، وهنا يثار الإشكال بعد التدفق الواسع للبيانات الشخصية إلى خارج الحدود الإقليمية للدول وخاصة أنها تتفاوت في أطر الحماية التي توفرها قوانين وتشريعات كل دولة، أي القوانين الواجبة التطبيق والضمانات الإجرائية التي تمكن أصحاب هذه البيانات الشخصية من ضمان حقهم في الحماية، "عمد الإتحاد الأوروبي إلى إقرار التوجيه الإرشادي لحماية البيانات في عام 1995، والذي نص في فحواه على عدم جواز نقل البيانات الشخصية خارج الحدود إلا إذا توافرت الضمانات الأساسية لحماية البيانات في الدولة التي تنتقل تلك البيانات إليها" (علي وهي ديب، 2023، صفحة 326).

ومن المعلوم أن النشاط التجاري القائم بين الإتحاد الأوروبي والولايات المتحدة الأمريكية هو من أهم الأسباب التي تبعث بحركية البيانات الشخصية للمتعاملين التجاريين عبر الحدود

الدولية، لذا كان لزاما على المسؤولين الأوروبيين والأمريكيين للوصول لحل يسمح بتبادل البيانات وحمايتها رغم إختلاف التوجه بينهما.

"وفي عام 2000 أصدرت وزارة التجارة الأمريكية لائحة بنود سميت ب مبادئ "الملاذ الآمن" والتي شكلت الأساس بين التجارة الإمبريكية والمفوضية الأوروبية وذلك بغية تسهيل آلية نقل البيانات " (علي وهي ديب، 2023، صفحة 363).

وهذا الإتفاق الذي سمي بإتفاق الملاذ الآمن يعد أول اتفاق يسهل آلية نقل البيانات بين الحدود الدولية ويحافظ على الحق في حمايتها من الانتها، ووضع آلية قانونية ردعية ضد متتهكها، فبدون هذا الإتفاق كان من الصعب بمكان استمرار العلاقات التجارية والإستثمارية بين الجانبين.

لكن مرور الوقت أصبح إتفاق الملاذ الآمن غير قادر عن تأمين الحماية اللازمة للبيانات العابرة للحدود، حيث كلن من الضروري البحث عن بديل لحماية البيانات عبر الحدود وذلك لدعم التجارة الدولية دون المساس بحق الخصوصية للمتعاملين.

فظهر بما يسمى ذرع الخصوصية، "حيث وقع الإتحاد الأوروبي مع وزارة التجارة الأمريكية في العام 2016 على إطار عمل خاص بحماية الخصوصية أطلق عليه إسم "ذرع الخصوصية" وقد سعى من خلاله الطرفين إلى تعزيز التعاون الدولي في مجال تبادل ونقل البيانات الشخصية عبر الحدود" (علي وهي ديب، 2023، صفحة 367).

فبإعمال هذا الإتفاق يضمن تعزيز التعاون بين الولايات المتحدة الأمريكية والإتحاد الأوروبي، وكذا استعادة الثقة في مدي فعالية الحماية القانونية للبيانات الشخصية، وعدم خوف المتعاملين من انتهاك خصوصياتهم، وضمان الحماية لها والإستفادة من مبدأ المعاملة بالمثل، حيث يحصل مواطني الإتحاد الأوروبي على حقوقهم القانونية أمام المحاكم الأمريكية تماما كما يحصل عليها الأمريكيون عند حدوث إنتهاك لبياناتهم الشخصية في الولايات المتحدة الأمريكية.

المبحث الثاني: الحماية القانونية للبيانات الشخصية عبر المجال الرقمي في التشريع الجزائري

إن التطور الهائل الذي مس المجال الرقمي كان لازما على الدول سن آلية قانونية لحماية ما تحويه هذه البيئة الرقمية من خصوصيات لمستخدميها، ومن بين أهم الخصوصيات، البيانات الشخصية لمستخدمي البيئة الرقمية التي مست جميع القطاعات بدءا من التجارة إلى السياسة، فأصبحت البيانات الشخصية عرضة للانتهاكات بدأ من تداولها إلى سرقتها والتلاعب بها وقرصنتها من طرف مختصين في المجال، "خاصة وأنه أصبح الفضاء الرقمي بديلا للفضاء الحقيقي في أغلب التعاملات والاتصالات، وهذا ما يترتب عنه سهولة التعرض لحياقتهم الخاصة وسرعة انتقال المعلومات المتعلقة بهم" (كريكت عائشة، 2019، صفحة 246)، فقد حمى الدستور الجزائري حرمة الإنسان، وجعل انتهاكها جريمة يعاقب عليها القانون وهذا ما جاء في المادة 39 منه " (الدستور رقم 20/442، 2020).

فمن خلال هذا المبحث نتطرق إلى الحماية القانونية للبيانات الشخصية عبر المجال الرقمي في إطار القانون 07-18 في المطلب الأول، وحمايتها في إطار القانون 09-04، في المطلب الثاني وذلك على التفصيل التالي:

المطلب الأول: الحماية القانونية للبيانات الشخصية عبر المجال الرقمي في إطار القانون 18-07

نحاول تركيز الدراسة في هذا المطلب على حماية البيانات الشخصية في إطار القانون 07-18، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،

ففي الفرع الأول من هذا المطلب، سنتطرق إلى الأحكام والمبادئ العامة للقانون 07-18. أما في الفرع الثاني نقوم بدراسة الإجراءات الإدارية والجزائية من نفس القانون.

الفرع الأول: الأحكام والمبادئ العامة لحماية المعطيات ذات الطابع الشخصي.

حصرت الأحكام والمبادئ العامة لهذا القانون في الابواب الاربعة الأولى منه حيث جاء في مضمون الباب الأول، الأحكام العامة، وتتمثل في أهداف سن القانون وإيضاح مفهوم المعطيات

ذات الطابع الشخصي، وكل المصطلحات الأخرى التي لها علاقة بالموضوع، ففي المادة الأولى منه جاء في فحواها "يهدف هذا القانون إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي" (المادة 1، القانون 18/07، 2018).

وهنا نستنتج أنه لا يمكن معالجة معطيات أخرى عدى المتعلقة بالطابع الشخصي، وتستثنى باقي المعطيات الأخرى من المعالجة.

أما الباب الثاني منه فقد خصص للمبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي، أين تم التطرق إلى الموافقة الصريحة والمسبقة من طرف الشخص المعني، كما له حق العدول عن ذلك في أي وقت شاء وتستثنى الموافقة عند الضرورة، وهذا ما نصت عليه المادة 7 من هذا القانون "لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني....." (المادة 7، القانون رقم 18/07، 2018)، فمن هنا تتجلى وتظهر جليا حرية الفرد داخل الدولة، والحماية القوية التي حظيت بها البيانات الشخصية.

كما أن المشرع لم يغفل عن نوع المعطيات ذات الطابع الشخصي فقد استثنى تلك المتعلقة بالجرائم والعقوبات وتدابير الأمن فقد شخص لها مؤهلين لذلك وهذا ما جاء في فحوى المادة 10 من نفس القانون، ونظر المشرع أيضا من حيث تأسيس الأحكام القضائية فنفي تأسيسها تقييما لسلوك الشخص على المعالجة الآلية للمعطيات ذات الطابع الشخصي.

أما من حيث الهيئة المخصصة لحماية المعطيات ذات الطابع الشخصي، فقد خصص المشرع سلطة وطنية لذلك، ووضع تشكيلاتها وضوابط عملها وكذا الرقابة عليها، في الباب الثالث من نفس القانون، وذلك لتقييد وحصر من لهم الحق في حماية المعطيات ذات الطابع الشخصي وذلك لحساسية الأمر، وتعلقها بحقوق وحرريات الأفراد التي كرس لها الدستور حماية شاملة وخاصة.

أما ما جاء في الباب الرابع من نفس القانون وهو حقوق الشخص المعني بمعالجة معطياته، حيث شملت، الحق في الإعلام، الحق في الولوج إلى والتأكد من صحة معطياته، وكذا الحق في التصحيح عند وجود خطأ فيها، كما يحق له الاعتراض على معالجة معطياته وذلك عند وجود سبب

مشروع، وتستثنى من ذلك إذا كانت المعالجة تستجيب للإلتزام القانوني. ومن الملاحظ أن كل أحكام هذا الباب تنصب على الحفاظ على حقوق وخصوصية الشخص المعني بالأمر.

الفرع الثاني: الإجراءات الإدارية والجزائية ضد المسؤولين والمعالجين للمعطيات

وضع المشرع ضمن هذا القانون إجراءات إدارية وجزائية ضد مسؤولي ومعالجي المعطيات ذات الطابع الشخصي، أين تم التطرق في الباب الخامس من هذا القانون لإلتزامات المسؤول عن المعالجة حيث تعتبر هذه الإلتزامات تقييدا للمسؤول عن المعالجة بغية عدم الإسراف والتعسف عند المعالجة وذلك حفاظا على مبدئ الخصوصية، وتشمل هذه الإلتزامات "تدابير تقنية وتنظيمية ملائمة لحماية المعطيات ذات الطابع الشخصي" (المادة 38، القانون رقم 18/07، 2018). وهذا ما جاء في مضمون المادة 38 من نفس القانون.

كما تم تقسيم المعطيات ذات الطابع الشخصي حسب ارتباطها، ففي الفصل الثاني من هذا الباب تم التطرق إلى كيفية معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التصديق والتوقيع الإلكترونيين، حيث تم ايضاحها في المادة 42 من نفس القانون (المادة 42، القانون رقم 18/07، 2018).

أما المعالجة لهذه الأخيرة في مجال الإتصالات الإلكترونية تم التطرق إلى إجراءاتها في الفصل الثالث من نفس الباب وبالضبط في المادة 43 من نفس القانون "حيث ركزت على التزام مقدم الخدمة بالحرص الشديد للمحافظة على المعطيات ذات الطابع الشخصي من انتهاكها" (المادة 43، القانون رقم 18/07، 2018).

أما في الفصل الرابع من هذا الباب تم التطرق لإجراءات نقل المعطيات نحو دولة أجنبية، من طرف المسؤول عن المعالجة، "أين تم وضع إجراءات وقائية لضمان حماية قانونية حين نقل المعطيات لدولة أخرى" (المادة 44، القانون رقم 18/07، 2018)، وهذا ما تناولته المادة 44 من نفس القانون. كما تم التطرق إلى "الاستثناءات أي حتى ولو لم تكن الدولة المستقبلة للمعطيات تستوفي الضمانات المذكورة في المادة 44 السالفة الذكر" (المادة 45، القانون رقم 18/07، 2018)، وهذا ما جاء في نص المادة 45 من نفس القانون.

كما تناول الباب السادس من نفس القانون أحكام إدارية وجزائية ضد المسؤول عن المعالجة في حال خرقه أحكام هذا القانون، وذلك لتسليط الرقابة على المسؤول عن المعالجة لتفادي انتهاك المعطيات الشخصية المعالجة والتلاعب بيها، حيث بين المشرع العقوبات التي تطبق على المسؤول في حالة خرقه للقانون.

ويأتي في الأخير الباب السابع من نفس القانون والذي ينص صراحة في المادة ما قبل الأخيرة منه 75 "على الإمتثال لأحكام هذا القانون من طرف مسؤولي وممارسي نشاط معالجة المعطيات" (المادة 75، القانون رقم 18/07، 2018).

المطلب الثاني: الحماية القانونية للبيانات الشخصية عبر المجال الرقمي في إطار القانون 09-04

إن القانون 09-04 المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أنه سيتم التطرق إلى لهذا لقانون خلال الفرع الأول، أما في الفرع الثاني ستم دراسة القواعد الإجرائية والإلتزامات للوقاية من هاته الجرائم.

الفرع الأول: الأحكام والمبادئ العامة للقانون 09-04.

حصر المشرع الأحكام والمبادئ العامة في هذا القانون في الفصلين الأول والثاني حيث تم التطرق في الفصل الأول منه إلى أهداف هذا القانون وهو "وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" (المادة 1، القانون 09/04، 2009)، وهذا ما نصت عليه المادة الأولى منه صراحة، كما تم التطرق إلى مجال إعمال وتطبيق هذا القانون في المادة رقم ثلاثة منه. حيث جاء في مضمونها "يتم مراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل صورة معلوماتية ويكون ذلك بطبيعة الحال وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون" (المادة 3، القانون 09/04، 2009).

أما في الفصل الثاني من هذا القانون تم التطرق إلى الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، فمن خلال المادة رقم أربعة من هذا القانون أشار المشرع إلى الحالات التي يخول لها

ويسمح بمراقبتها إلكترونياً، حيث أوضحها وعدها على سبيل الحصر وتشمل كل الإعتداءات مهما كان نوعها من أعمال إرهابية وتخريبية، تؤثر سلباً على النظام العام والسكينة العامة.

الفرع الثاني: القواعد الإجرائية والإلتزامات للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

حصر المشرع القواعد الإجرائية والإلتزامات للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في الفصول الأربعة الأخيرة من هذا القانون حيث "وضح المعنيون بهذا العمل كما تم ضبط مهامهم وطريقة التفتيش للمنظومات المعلوماتية" (المادة 5، القانون 09/04، 2009)، وذلك تفادياً للمساس بحق الخصوصية للأفراد، وجاء ذلك في نص المادة رقم خمسة من هذا القانون.

كما أشار المشرع في المادة رقم عشرة من نفس القانون إلى "إلتزامات مقدمي الخدمات لمساعدة السلطات إذا اقتضى الأمر وذلك لتسهيل العملية واختصار الجهد إلا أن ذلك يكون بسرية تامة كما يعرض المفشي للسر لعقوبات صارمة" (المادة 10، القانون 09/04، 2009).

فبالنظر إلى أهمية المعطيات الشخصية أولى لها المشرع اهتماماً كبير وذلك حفاظاً على مبدأ الخصوصية واحترامها، وتكريساً لمبدأ حماية الحقوق والحريات المكفول دستورياً.

الخاتمة:

إن مبدأ الحق في الخصوصية مبدأ شرعي تكفله السلطات العليا في البلاد، لكن يرد الإستثناء في حالات خاصة تم التطرق لها خلال البحث، أي أن مصلحة المجتمع تسبق مصلحة الفرد، كما أنه من المعلوم لدى العامة أن التطور التكنولوجي الهائل الذي أدى إلى جعل العالم كله قرية صغيرة حيث تلاشت الحدود الجغرافية، لأن المجال الرقمي لا تحكمه الحدود الدولية، لذا كان لزاماً على كل دول العالم التكتل لمحاربة والتصدي لإنتهاك الخصوصية في المجال الرقمي خاصة البيانات الشخصية التي باتت من ضمن التجارة المربحة لمروجيها، لذا وجب إبرام اتفاقيات دولية ومعهادات لوضع قوانين تحمي هذا الحق، لأنه ضمن الحقوق التي تسعى جميع الدول لحمايتها، علماً أن جل التعاملات أصبحت اليوم ترمز إفتراضياً لا واقعياً أي عن بعد مما استوجب تدفق البيانات الشخصية لخارج حدود الدولة، ناهيك عن الإتصالات بمختلف أنواع مواقع التواصل

الحق في خصوصية البيانات الشخصية عبر المجال الرقمي وسبل حمايتها في التشريع الجزائري

الإجتماعي التي تحوي البيانات الشخصية لجميع متعاملها والتي أصبحت لا غنى عنها في التواصل بين الأفراد سواء كانوا من نفس الدولة أو خارجها، أما ما زاد الطين بلاء هو ما يعرف بالذكاء الاصطناعي الذي أجهز العالم والذي له تأثير كبيراً على انتهاك الخصوصية المعلوماتية.

فمن هنا يتبين لنا عدم إمكانية حماية البيانات الشخصية على المستوى الوطني فقط لأنه لا يضمن حماية كافية بل وجب حمايته في باقي الدول الأخرى، وذلك بإبرام اتفاقيات ومعاهدات.

قائمة المصادر والمراجع:

قائمة المصادر:

1 الدستور رقم 20/442، (2020/12/30)، الجريدة الرسمية رقم 82 بتاريخ 2020/12/30.

2 القانون رقم 09/04، (5/ 08/2009) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدة الرسمية رقم 47 بتاريخ 2009/08/16.

3 القانون رقم 18/07، (10/06/2018)، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34 بتاريخ 2018/06/10.

قائمة المراجع:

1 توبى مندل، (2013)، دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير، منظمة الأمم المتحدة للتربية والعلوم والثقافة، منشورات اليونسكو.

2 حسام محمد نبيل، الشراقي، (2019)، حماية البيانات الشخصية عبر الانترنت-التحديات والحلول، الطبعة الأولى، القاهرة-مصر، المنظمة العربية للتنمية الإدارية جامعة الدول العربية.

3 علي، وهي ديب، (2023)، الحق في حماية البيانات الشخصية، الطبعة الأولى، بيروت-لبنان، منشورات الحلبي الحقوقية.

4 مروة، زين العبدین صالح، (2017)، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الإنفاقي والقانون الوطني، الطبعة الأولى، القاهرة- مصر، مركز الدراسات العربية.

5 يوسف، كمال الحاج، (1999)، حقوق الانسان- تعلق ولا يعلى عليها، الطبعة الأولى، بيروت- لبنان، مؤسسة فريدريش ناومان ومؤسسة رينة معوض وبنيان.

قائمة المجلات:

1 كريكت، عائشة. (2019)، "حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات"، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، جامعة أدرار، مجلد 18، عدد 2، الصفحات 253-279.

2 محمد أحمد، المعداوي، (2018)، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مجلة كلية الشريعة والقانون، طنطا، مجلد 33، العدد 4، الصفحات 1926-2057.

3 محمود، عبد الرحمن، (2020)، التطورات الحديثة لمفهوم الحق في الخصوصية - الحق في الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، المجلد 8، العدد 1، الصفحات 449-488.

4 نصيرة، تواتي، (2017)، حماية البيانات الشخصية في إطار مكافحة الإرهاب الدولي المجلة الجزائرية للعلوم القانونية والإقتصادية والسياسية، جامعة الجزائر، المجلد 54، العدد 5، الصفحات 93-123.