مجلة الدراسات القانونية والاقتصادية ISSN 2602-7321/ EISSN 2773- 2649

السنة: 2024 المجلد: 07 العدد: 01 ص- ص: 302-317

حماية الحق في الخصوصية في مواقع التواصل الاجتماعي

Protection of the right to privacy on social media sites

بوخميس أحلام *[1]، مخبر الدستور الجزائري والدراسات القانونية الاستشرافية، جامعة الاخوة منتوري قسنطينة1، الجزائر، ahlam.boukhmis@doc.umc.edu.dz

بوالزيت ندى[2] ، مخبر الدستور الجزائري والدراسات القانونية الاستشرافية، جامعة الاخوة منتوري قسنطينة1، الجزائر، Nada-droit@hotmail.com

تاريخ إرسال المقال: 2024/01/10 تاريخ قبول المقال: 2024/05/20

الملخص:

يعد الحق في الخصوصية من اهم الحقوق الأساسية التي يتمتع بها الفرد على الإطلاق، على الرغم من تأخر المشرع الجزائري من الاعتراف بها على مستوى التشريع والتنظيم المعمول بهما في الدولة، وقد زادت أهميته عند فتح باب الرقمنة على مصراعيه، فأصبحت الحياة الخاصة عرضة للاختراق والانتهاك في أية لحظة وبضغطة زر، وهذا ما زاد من أهمية هذه الدراسة فهي تساهم في تسليط الضوء على دور المشرع الجزائري في تأطير وإحاطة الحياة الخاصة للأفراد في الفضاء الرقمي عامة ومواقع التواصل الاجتماعي خاصة على النحو الذي يكفل لهم حماية قانونية لحياتهم الخاصة.

وقد توصلت الدراسة للعديد من النتائج أهمها أن العديد من البرامج التقنية التي تعمل على حماية البيانات الشخصية في مواقع التواصل الاجتماعي أغلبها تتعرض للاختراق ولابد من احاطتها بحماية قانونية.

الكلمات المفتاحية: الحق في الخصوصية، مواقع التواصل الاجتماعي، الأمن المعلوماتي، الحماية الجزائية.

Abstract: The right to privacy is one of the most basic rights that an individual enjoys at all, despite the delay in the Algerian legislator in recognizing it at the level of legislation and regulation in force in the country, and its importance increased when the door to digitization was opened wide, so that private life became vulnerable to penetration and violation in Any moment and at the click of a button, and this increases the importance of this study, as it contributes to shedding light on the role of the Algerian legislator in framing and surrounding the private lives of individuals in the digital space in general and social networking sites in particular in a manner that guarantees them legal protection for their dealings and their private lives.

* بوخميس أحلام

The study reached many results, the most important of which is that many of the technical programs that work to protect personal data on social networking sites, most of which are exposed to hacking and must be surrounded by legal protection.
Key words : the right to privacy, social networking sites, information security, penal protection.

المقدمة:

بعد الثورة الرقمية التي اجتاحت العالم بأسره وجعلت منه قرية صغيرة تمكن من تقزيم وتقصير المسافات والأزمنة، أصبحت الدولة ملزمة على تخزين ومعالجة المعطيات العامة الخاصة بها، وكذا تلك الخاصة بالأفراد كنوع من أنواع إحكام السيطرة على الحقوق والحريات العامة خاصة تلك العابرة للحدود الجغرافية للدولة، وجعلها تمارس في حدود ضوابط قانونية مسطرة مسبقا، والجزائر كغيرها من الدول خطت خطوة في غاية الأهمية في مجال الرقمنة على رغم من حداثتها في هذا المجال فقد أحاطت جل المجالات والتخصصات بنظام قانوني ورقمي مكنها من مركزة سلطة اتخاذ القرار على مستوى مرافقها العامة، ومن تقييد الحقوق والحريات العامة للأفراد حتى في مواقع التواصل الاجتماعي التابعة للشركات المتعددة الجنسيات وعلى رأسها الفيس بوك، تويتر، أنستغرام، تيك توك وغيرها.

وتكمن أهمية هذه الدراسة لكونها تهتم بالدرجة الأولى بحدود التعامل مع المعطيات الخاصة للأفراد وحمايتها من أي إساءة أو سوء استخدام انتهاك لخصوصيتهم بأي شكل من الأشكال، آخذين بعين الاعتبار طبيعة الفئات الاجتماعية المختلفة من حيث الأعمار والأجناس والجنسيات والاحتياجات والرغبات والاهتمامات والتخصصات داخل مواقع التواصل الاجتماعي.

إن الهدف الأساسي من هذه الدراسة هو الوصول إلى نتائج قانونية تسمح باقتراح حلول جذرية تكفل وقاية المعطيات الخاصة بالأفراد المتاحة عبر منصات التواصل الاجتماعي من أي انتهاك واختراق لخصوصيتهم واستغلالها لإحداث ضرر عمدي بهم، وكذا حلول أخرى تضمن سبل مكافحتها سواء وقعت أضرار فعلية للأفراد أم لا، لأجل ذلك يطرح الإشكال الآتي: هل الحماية التي أحاطها المشرع الجزائري بالمعطيات الشخصية للأشخاص الطبيعيين في مواقع التواصل الاجتماعي كفيلة بضمان أمنها المعلوماتي وضمان الحق في الحياة الخاصة لهم؟

إن الإجابة على الإشكالية أعلاه تتطلب اتباع المنهج التحليلي من خلال استخراج مبادئ الحماية القانونية التي تحقق الضمانات المطلوبة للمعطيات الخاصة في مواقع التواصل الاجتماعي، وكذا استخراج الأحكام القانونية التي تكفل حماية جزائية ومعلوماتية لها من أي اعتداء لهذه الخصوصية متبعين في ذلك الخطة أدناه:

المبحث الأول: مبادئ الحماية القانونية للحق في الخصوصية في مواقع التواصل الاجتماعي.

المبحث الثاني: أصناف الحماية القانونية للحق في الخصوصية في مواقع التواصل الاجتماعي.

المبحث الأول: مبادئ الحماية القانونية للحق في الخصوصية في مواقع التوصل الاجتماعي.

تدخل المشرع الجزائري لحماية الحق في الخصوصية من خلال إحاطته بمنظومة تشريعية، تكفل له حماية تشريعية وأساس قانوني يشكل ضمانة للأشخاص الطبيعيين للمطالبة بحماية حقوقهم من أي انتهاك لخصوصيتهم في مواقع التواصل الاجتماعي بسبب أخطاء ارتكبها المستخدمين لهذه المواقع كعدم حفظ البيانات الخاصة أو افشاء سريتها بعد أن تم حفظها وتخزينها أو بسبب اختراق الغير لهذه المواقع، وقد استند المشرع الجزائري في هذه الإحاطة التشريعية إلى العديد من المبادئ سنجملها بمزيد من التفصيل ضمن المطالب أدناه:

المطلب الأول: مبادئ خاصة بضمان الأمن المعلوماتي للحق في الخصوصية.

تعددت المبادئ المتعلق بضمان الأمن المعلوماتي للحق في الخصوصية منها مبدأ الشرعية ومبدأ سلامة المعطيات الشخصية وحساسيتها، ومبدأ الملاءمة بين طبيعة المعطيات والهدف من تخزينها ومعالجتها.

الفرع الأول: مبدأ الشرعية.

جاء في نص المادة 47 من التعديل الدستوري لسنة 2020 [1]أنه:" **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**". فمن نص المادة أعلاه يتضح أنه اعتراف الدستور بأن الحق في الخصوصية حق من الحقوق الأساسية ولا يهم الشكل الذي يكون فيه، ولا يمكن الاطلاع عليه إلا بعلم وإذن صاحبه، أو خرقه إلا في ظروف خاصة وبموجب أمر معلل من السلطة القضائية، ومثالها أن تقوم هذه الأخيرة بمناسبة التحقيق في جرائم التمييز وخطاب الكراهية بإصدار[2]:

[1] – التعديل الدستوري لسنة 2020 الصادر بموجب المرسوم الرئاسي رقم 20–442 المؤرخ في 30 ديسمبر 2020، جريدة رسمية رقم 82 مؤرخة في 30 ديسمبر 2020.

[2] – المواد 22،23، 24 من القانون رقم 20–05 المؤرخ في 28 أبريل 2020 والمتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، جريدة رسمية رقم 25 مؤرخة في 29 أبريل 2020.

- أمر تسليم أية معلومة أو بيان يكون مخزنا باستخدام وسائل تكنولوجيات الإعلام والاتصال.
- أمر بالتحفظ الفوري عليها إذا كان المحتوي يشكل جريمة من جرائم التمييز.
- أمر بالتدخل الفوري لسحب أو تخزين معلومات والمحتويات لمقدم الخدمات ليتم الاطلاع عليها أو لجعل الدخول إليها غير ممكن.

ومن هذا المنطلق فإن الحق في الخصوصية لا يؤخذ على إطلاقه بل ضمن الحدود التي تجعل ممارسته في إطار الشرعية القانونية، لذا حتى يكون الحق في الخصوصية مشروعا لابد أن يشمل معطيات لا تحمل مضمون مخالف للتنظيم والتشريع المعمول به أو مضمون ذو طابع تخريبي أو من شأنه المساس بالنظام العام أو الآداب العامة (كالمضامين المخلة بالآداب العام) لذا يجب أن تشمل المعطيات الخاصة مضمون شرعي كما هو مبين أدناه:

- المعلومات والمعطيات الخاصة للأفراد الغير قابلة للنقل والتداول عبر الوسائط الالكترونية إلا بعلم ورغبة حائزها.
- المعلومات والمعطيات الخاصة بالأفراد السرية وتكون متداولة بين عدد محدد من الأشخاص[3] ويستوي في ذلك أن ترد على حدث أو حقيقة أو أن ترد على فكرة أو عمل ذهني[4].
- المعلومات والمعطيات الشخصية والمرتبطة بشخص المخاطب بها كحالته الصحية وذمته المالية وحالته الاجتماعية واسمه، وهي معلومات يملك صاحبها سلطة قانونية فلا يجوز الاطلاع عليها أو تداولها إلا بإذنه أو بموجب أمر من السلطة القضائية المختصة.

الفرع الثاني: مبدأ سلامة المعطيات الشخصية وحساسيتها.

حتى تحظى المعطيات الشخصية المخزنة والمعالجة في مواقع التواصل الاجتماعي بالحماية القانونية لابد أن تكون صحيحة كاملة ومحينة ، خالية من أي غموض أو تدليس، وهذا الأمر يسري على جميع المعطيات الخاصة بالفرد سواء كانت اجتماعية أو دينية أو مالية[5]، وفي هذا الخصوص عرف المشرع الجزائري المعطيات ذات الطابع الشخصي بموجب نص المادة الثالثة من القانون رقم 18-07 المؤرخ في

[3] – عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا (دراسة مقارنة)، دار النهضة العربية، 2010، مصر، ص189.

[4] – عمر أبو الفتوح عبد العظيم الحمامي، المرجع نفسه، ص 191.

[5] – جمال صالح عبد الحليم، الحماية الجنائية للحق في الخصوصية في مواجهة نظم المعلومات، دار النهضة العربية، 2018، مصر، ص110.

10 يونيو 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[6]، على أساس طبيعة البيانات الشخصية والتي يفترض بها أن تبقى سليمة تحت طائلة عقوبات جزائية وهي: رقم التعريف أو عناصر خاصة بالهوية البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

وجدير بالذكر أن مدى حساسية المعطيات الخاصة حددها المشرع الجزائري وربطها بالأصل العرقي للشخص أو أصله الاثني أو آرائه السياسية وقناعاته الدينية أو الفلسفية أو الانتماءات النقابية، أو حتى المعطيات الجينية[7]، وفي هذا الخصوص أجاز المشرع الجزائري للجهات القضائية استعمال تقنية المحادثة المرئية عن بعد في الإجراءات القضائية، مراعيا بذلك مقتضيات المحاكمة العادلة وضمانا لسرعة الإجراءات وحماية للنظام العام في الظروف العادية والظروف الاستثنائية، بشرط أن تضمن الوسائل المستعملة سرية الإرسال وأمانته نظريا لحساسية الحياة الخاصة للمتهم[8].

الفرع الثالث: مبدأ الملاءمة بين طبيعة المعطيات والهدف من تخزينها ومعالجتها.

اعتمد المشرع الجزائري في تأطيره القانوني للمعطيات الخاصة على مبدأ الملائمة بين البيانات الشخصية والهدف من تخزينها ومعالجتها، فمثلا تسجيل المعطيات الخاصة بالطلبة على مستوى المنصة الرقمية البروقرس بهدف الانتفاع بخدمات مؤسسات التعليم العالي، وتسجيل بيانات الأشخاص العاطلين عن العمل وغير المؤمنين في منصة منحة البطالة للحصول على منحة البطالة، وتسجيل التاريخ الصحيح للفرد للحصول على الضمان الاجتماعي، وتسجيل الناخبين في البطاقية الوطنية للناخبين لتنظيم عملية الانتخابات.

وهناك أيضا فكرة تسجيل المعطيات الخاصة في مواقع التواصل الاجتماعي للحصول على خدمة أو منتج عن بعد، فيضطر الفرد بإرسال معطياته الخاصة كرقم هاتف وعنوانه الشخصي واسمه إلى المورد الالكتروني ليتمكن من الحصول على الخدمة أو المنتج المروج له في الوسائط الالكترونية.

وبالرجوع للقانون 18-07 السالف الذكر نجده كرس هذا المبدأ بموجب نص المادة التاسعة منه والتي تنص:" **يجب أن تكون المعطيات الشخصية:**

---

[6] – القانون رقم 18-07 المؤرخ في 10 يونيو 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي جريدة رسمية رقم 34 مؤرخة في 10 يونيو 2018.

[7] – المادة 43 من القانون 18-07.

[8] – المادة 441 مكرر من الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المعدل والمتمم بموجب الأمر رقم 20-04 المؤرخ في 30 أوت 2020، جريدة رسمية رقم 51 مؤرخة في 31 أوت 2020.

- **معالجة بطريقة مشروعة ونزيهة؛**
- **مجمعة لغايات محددة وواضحة ومشروعة وألا تعالج لاحقا بطريقة تتنافى مع هذه الغايات؛**
- **ملاءمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها؛**
- **صحيحة وكاملة ومحينة إذا اقتضى الأمر؛**
- **محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها أو معالجتها".**

المطلب الثاني: مبادئ خاصة بضمان حقوق الأشخاص الطبيعيين المسجلة بياناتهم.

ويشمل مبدأ تمكين الأشخاص المعنويين أو الطبيعيين من ممارسة حقوقهم الأساسية في الوسائط الرقمية عامة ومواقع التواصل الاجتماعي خاصة وأبرزها على الإطلاق الحقوق المبينة أدناه:

الفرع الأول: الحق في الحصول على المعلومة

فمن حق الشخص المعني بمحتوى المعلومة سواء مباشرة أو عن طريق ممثله القانوني، الاطلاع على مضمون المعلومات والبيانات التي تخصه والتي تم تخزينها ومعالجتها بأي شكل كان، فالصور والطرق مختلفة خاصة وأن المعطيات تخصه ولا تخص الغير ولا تمس بأي شكل كان النظام العام أو الآداب العامة، وفي هذا الخصوص نصت المادة 55 من التعديل الدستوري لسنة 2020 التي تنص على: " **يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات والحصول عليها وتداولها. لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم وبالمصالح المشروعة للمؤسسات وبمقتضيات الأمن الوطني**".

الفرع الثاني: حق تصحيح المعلومات الخاصة.

في كثير من الأحيان يلجأ الأفراد إلى تصحيح بعض المعطيات والمعلومات في صفحاتهم الخاصة في مواقع التوصل الاجتماعي، والتي يفترض بها أنها محجوبة عن بقية المستخدمين باستثناء المسؤولين عن الموقع، الذين ينبغي عليهم تمكينهم من ذلك، كما يتعين عليهم معالجة معطيات الأفراد مهما كان مصدرها أو شكلها، على النحو الذي يضمن لهم عدم المساس بحقوقهم وشرفهم وسمعتهم وكذا احترام الكرامة الإنسانية والحياة الخاصة[9].

[9] – المادة 02 من القانون رقم 18-07.

ويقصد بالمعالجة هنا كل العمليات المنجزة بطريقة آلية تشمل جمع البيانات وتسجيلها وحفظها و/أو تغييرها واستخراجها أو القيام بأي شكل من أشكال الإتاحة أو القريب أو الربط البيني أو غيرها من العمليات التي تتضمن الاغلاق، التشفير، المسح أو الاتلاف[10].

الفرع الثالث: الحق في محو البيانات الشخصية

تعتمد الكثير من مواقع التوصل الاجتماعي على خاصية الحذف أو المسح أو الاتلاف، وهذا لتمكين أصحاب الصفحة ومالك المعلومة أو البيان من التخلص من المعلومات التي يرغب في حذفها مهما كان السبب، وهذا يعتبر ضمانة أساسية لحماية خصوصية الأفراد في منصات التواصل الاجتماعي، لأنه سيحجب المعلومة التي تخصه ليس فقط عن الغير بل أيضا عن مقدمي الخدمات الذين يقومون بمعالجة أو تخزين المعلومات لفائدة خدمة الاتصال.

المبحث الثاني: أصناف الحماية القانونية للحق في الخصوصية في مواقع التواصل الاجتماعي.

تتنوع أصناف الحماية القانونية للحق في الخصوصية بين الحماية المعلوماتية كتدبير وقائي، والجزائية كتدبير ردعي عقابي، لذا سنتولى ضمن هذا المبحث دراسة الحماية المعلوماتية للحق في الخصوصية في مواقع التواصل الاجتماعي كإجراء وقائي (المطلب الأول)، والحماية الجزائية للحق في الخصوصية كإجراء ردعي (المطلب الثاني).

المطلب الأول: الحماية المعلوماتية للحق في الخصوصية مواقع التواصل الاجتماعي كإجراء وقائي.

توجد الى جانب الحماية الجنائية حماية معلوماتية للحق في الخصوصية في مواقع التواصل الاجتماعي وذلك بهدف منع المتطفلين والقراصنة من الدخول الى شبكاتهم، لذا يجب اتخاذ كافة تدابير الحيطة والحذر عند استخدام الأجهزة الالكترونية عموما ومواقع التواصل الاجتماعي خصوصا.

فإن المقصود بالحماية المعلوماتية هي انشاء برامج تقنية حمائية تعمل على حماية البيانات الرقمية من شتى أشكال الهجومات الالكترونية، ومن خلال هذا المبحث سيتم التعرف على أهم التطبيقات التي تحمي المعلومات الشخصية في البيئة الافتراضية ودورها الفعال في تحقيق الحماية ضمن الفروع التالية:

[10] – الفقرة الثالثة من المادة 03 من القانون رقم 18-07.

الفرع الأول: أنواع التطبيقات الالكترونية لحماية الخصوصية المعلوماتية.

هناك العديد من التطبيقات التي يمكن الاعتماد عليها لحماية المعطيات الخاصة، تختلف باختلاف درجة الحماية التي توفرها وعلى حسب نوعية الاختراقات وطبيعة الفيروسات المستعملة في الاختراق ومن أبرز هذه التطبيقات لدينا:

تطبيق ماي داتا مانجر my data manager:[11] يعد هذا التطبيق من بين أهم التطبيقات التي تساعد على حماية خصوصية المستخدم اثناء استخدام الأنترنيت، والتحكم باستهلاك البيانات، حيث يقوم هذا الأخير على تأمين استخدام الأنترنيت من خلال إيجاد ما يعرف بالشبكة الخاصة الافتراضية VPN لتشفير البيانات الغير محمية الى جانب مراقبته لكمية البيانات التي يستهلكها كل تطبيق. وجدير بالذكر بأن تشغيل هذا التطبيق مجاني بالنسبة لنظامي الآندرويد وIOS.[12]

تطبيق المراسلة سيغنال signal:[13] سيغنال من أكثر التطبيقات التي تعمل على دعم الحفاظ وحماية الخصوصية المعلوماتية والأمان الرقمي، فهو يوفر ميزة التشفير من طرف الى طرف end to end enycryption لجميع المحادثات النصية والصوتية وكذلك محادثات الفيديو...الخ، وقد حصل على العديد من الموافقات من قبل الهيئات التي تهتم بحماية حق الخصوصية لمستخدميها مثل مؤسسة موزيلا، والتي تطور متصفح فاير فوكس ولجنة حماية الصحافيين مع العلم أن هذا التطبيق مجاني لكل مستخدمي أجهزة الأندرويد وIOS في متجري قوقل وآب ستور.[14]

تطبيق بروتن مايل protonmail:[15] من أفضل التطبيقات التي تسعى الى تجسيد تأمين البريد الكتروني، حيث يسمح بتشفير الرسائل قبل ارسالها، ومن ثم تدميرها بمجرد تلقيها من الطرف الثاني، فمن جهة وظيفة التطبيق يعمل مثل بقية التطبيقات البريد الالكتروني الأخرى، لكن هو الآخر يسعى الى توفير مستويات

18–الموقع الرسمي للبرنامج ماي داتا ماناجر تم الاطلاع على الموقع بتاريخ 2023/05/28 على الساعة 22:30 موجود على الرابط التالي: https://play.google.com/store/apps/details?id=com.mobidia.android.mdm&hl=ar&gl=US

[12] – خلدون غسان سعيد، تطبيقات مفيدة لحماية الخصوصية الرقمية –تؤمن تصفح الأنترنيت والتراسل ورسائل البريد الالكتروني–، مقال منشور بتاريخ 12 جانفي2021، تم الاطلاع عليه بتاريخ 2023/06/01 على الساعة 10:00 موجودة في الرابط التالي: https://my-data-manager.ar.uptodown.com/android

[20]– الموقع الرسمي للبرنامج سيغنال تم الاطلاع على الموقع بتاريخ 2023/06/02 على الساعة 13:20 موجود على الرابط التالي: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=ar&gl=US

[14] – خلدون غسان سعيد، المرجع السابق.

[15] – الموقع الرسمي للبرنامج بروتن مايل تم الاطلاع عليه بتاريخ 2023/06/10 على الساعة 00:00 موجودة على الرابط التالي: https://play.google.com/store/apps/details?id=ch.protonmail.android&hl=ar&gl=US

إضافية من الأمان في الرسائل التي تشمل حماية الرسائل المرسلة بكلمة السر، وفي حالة وقوع اختراق الكتروني فلن يتمكنوا من قراءة الرسائل حتى يدخلوا كلمة السر التي تم إدخالها سابقا[16].

تطبيق fingersecurity:[17] يشكل هذا التطبيق نوع من الحماية الخاصة بغلق وقفل التطبيقات المتواجدة على مستوى الأجهزة التي تعمل بنظام التشغيل الأندر ويد عن طريق بصمة الأصبع، كما يحتوي ذات التطبيق على ثيمات متعددة للبصمة يمكنك تثبيتها والاختيار من بينها الشكل الذي يساعد صاحب الجهاز، ومن أهم الصفات التي يتصف بها هذا التطبيق انه يمنح مدة زمنية معنية لمنع قفل التطبيقات المعنية به، وبعد مرور تلك الفترة يطلب منك التطبيق إعادة ادخال البصمة من جديد للتأكد من صاحب الهاتف، كما يمنع من الاشعارات من الظهور ودعم حمايتها، فضلا عن إمكانية التطبيق بأخذ صور تلقائية لكل غريب حاول فتح الهاتف.[18]

التشفير Encryption: يعتبر التشفير أحد برامج الوقاية والحماية من الهجمات السيبرانية، حيث تظهر مهمته في تشفير البيانات المتبادلة وضمان عدم المساس بمحتوى البيانات لأي تعديل أو تغيير، ولعل الخاصية الأساسية من التشفير تبرز في إمكانية تغيير البيانات المتبادلة عند حل التشفير عن طريق مفتاح التشفير من طرف المرسل أو من الطرف المستقبل، وجدير بالذكر أن نظام التشفير يحتوي على اسلوبين من الحماية منها ما هو متعلق بحماية الشبكة الخاصة الافتراضية من خلال تشفير كل الرسائل والبيانات المتجمعة في البيئة الافتراضية قبل تبادلها، في حين الأسلوب الثاني يبدوا في شكل نظام يسمى SSL حيث يوفر هذا النظام أمن معلوماتي لمعلومات وبيانات خاصة وفقا لاستراتيجية معمقة ومدروسة من خلال الحصول على شهادات رقمية موثوقة مدعمة ببروتوكول SSL.[19]

يبدوا بصورة جلية أن الأعوان المتخصصين في مجال الرقمنة والأنظمة المعلوماتية في تطوير مستمر للبرامج والتطبيقات التكنولوجية للمواجهة الدائمة للهجمات السيبرانية، والتقليل من الآثار الكارثية الناتجة عن هاته الجريمة التي طغت على حياة الفرد في كل جوانبه.

الفرع الثاني: دور التطبيقات الالكترونية في حماية الخصوصية المعلوماتية.

[16] – خلدون غسان سعيد، المرجع السابق.

[17] – الموقع الرسمي للبرنامج فينغر سيكيريتي تم الاطلاع عليه بتاريخ 2023/06/13 على الساعة 02:05 موجود على الرابط التالي: https://fingersecurity.ar.uptodown.com/android/download

[18] – خلدون غسان سعيد، المرجع السابق.

[19]– حكيمة جاب الله، انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، حوليات جامعة الجزائر 1، الجزائر، المجلد 35، العدد 03، 2021، ص 663.

تلعب التطبيقات الالكترونية دورا بارزا في تكريس وظيفة الأمن المعلوماتي من خلال التصدي للهجمات الالكترونية وحماية الخصوصية المعلوماتية، ويكمن هذا الدور الرئيسي في:

- اتخاذ التدابير اللازمة والضرورية لحماية المعلومات الحساسة من أي اختراق.
- ضمان سلامة المعلومات واستمرارها ضد أي تعديل أو تغيير أو محو غير مشروع أو تدمير.[20]
- مهمة الكشف عن الفيروسات ومكافحتها أو محاولة تدميرها قبل البدء في الاطلاع على البيانات الشخصية الالكترونية أو تشويه البيانات المتوفرة في مختلف منصات التواصل الاجتماعي.[21]
- تشفير البيانات والمعلومات التي يتم تسجيلها في مواقع التواصل الاجتماعي.[22]
- تعمل التطبيقات الالكترونية الهادفة لحماية البيانات الشخصية على منع تحميل البرامج الخبيثة، التي يمكن أن تتواجد بذاكرة الحاسوب أو الهواتف الذكية.
- تعد البرامج الذكية بمثابة آليات احترازية أمنية تعمل على إيقاف الهجومات السيبرانية بواسطة برامج الجوسسة ولعل أهمها acunetix nettouls، coffre fort، antisnifer.[23]

المطلب الثاني: الحماية الجزائية للحق في الخصوصية في مواقع التواصل الاجتماعي كإجراء ردعي.

لقد تظافرت جهود الدولة الجزائرية من أجل وضع تصور قانوني فعال في تعزيز الحق في الخصوصية ورفع مكانته، وتحقيق الحماية القانونية من جهة وصيانة البيانات والمعطيات من جهة أخرى، وفي ظل الرقمنة تمكنت تقنية المعلوماتية الجديدة من الحصول على معلومات وتخزين وتحليل كم هائل من البيانات الشخصية من قبل العديد من المؤسسات والوكالات الحكومية والغير الحكومية، مما رتب آثار جد سلبية على خصوصية الحياة الفردية للأشخاص، ودرءً للخطر حمل المشرع القائم بهذه العملية المعلوماتية الدقيقة مسؤولية كبيرة نظرا لما يتمتع به مركزه من حساسية، وعليه فإن الحماية الجزائية للحق في

[20] الجواد دلال صادق، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، 2008، عمان، ص41.

[21] حزام فتيحة، حماية الأنظمة الرقمية بين الأليات التقنية وأجهزة الحماية–قراءة في احكام المرسوم الرئاسي 20–05، مجلة الحقوق والعلوم الإنسانية، الجزائر، المجلد 13، العدد 03، 2020، ص175، نقلا عن عبد الله بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية، دار الفكر الجامعي، 2004، مصر، ص400.

[22] حزام فتيحة، المرجع نفسه، ص176، نقلا عن عبد الفتاح بيوم الحجازي، النظام لحماية التجارة الالكترونية، الكتاب الأول، دون طبعة، دار الفكر الجامعي، 2002، مصر، ص196

[23] – حكيمة جاب الله، المرجع السابق، ص 663.

الخصوصية في الوسائط الالكترونية ولاسيما مواقع التواصل الاجتماعي تتجلى أساسا في تجريم الأفعال والسلوكيات التي تشكل اعتداءً على حرمة الحياة الخاصة وهو ما سيم التطرق له في الفروع أدناه:

الفرع الأول: جريمة الدخول والبقاء الغير مشروع.

نص المشرع الجزائري على جريمة الدخول والبقاء الغير مشروع في المادة 394 مكرر من قانون العقوبات، حيث يرتكز الركن المادي لهذه الجريمة في فعل الدخول أو البقاء الغير مشروع وهو دخول بطريقة الغش والاحتيال إلى ما يقوم به نظام المعالجة الآلية للمعطيات وهو عملية غير مصرح بها تكون هذه الأخيرة لإساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له للوصول إلى المعطيات والمعلومات المخزنة بداخله، وفعل البقاء هو التواجد داخل نظام المعالجة الالية للمعطيات ضد إرادة من له حق في السيطرة على هذا النظام[24].

ويعتبر الفعلين سلوكين مجردين بمعنى تقع وتكتمل بمجرد انتهاء السلوك المكون لها، وهو الدخول أو البقاء ولا يشترط أي إضافة له أو تحقيق لأي نتيجة إجرامية.

كما لا يمكن إلا أن نتطرق إلى الصورة المشددة من هذا الفعل والتي جاء بها المشرع في المادة 394 مكرر في فقرتها 2 و3 من قانون العقوبات الجزائري وهي تكون إما محوا أو تغيرا في المعطيات الموجودة في النظام أو تخريب لنظام أشغال المنظومة ويكون هذا الطرف بمجرد وجود علاقة سببية ما بين الدخول أو البقاء الغير مشروع وبين النتيجة المحققة، وهي كما سبق الذكر المحو، أو تعديل البيانات أو عدم قدرة النظام على أداء وظيفته وبذلك جعل المشرع العقوبة مضاعفة في هذه الحالة[25].

وبما أن هذا النوع من الجرائم يندرج ضمن الأفعال الإجرامية العمدية فإنه يتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، حيث أنه يثبت للجاني تلقائيا توفر عنصر الاحتيال باعتباره أنه تعمد أثناء قيامه بهذا الفعل دون الحصول على رخصة، كما أنه إذا أثبت انتفاء العلاقة السببية بين السلوك

[24]– محمد خليفة، التواجد الغير مشروع في أنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة باجي مختار، عنابة، الجزائر، 2011، ص 142.

[25]– مختارية بوزيدي، ماهية الجريمة الالكترونية، كتاب أعمال الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، يوم 29 مارس 2017، مركز جيل للبحث العلمي، الجزائر، ص 15.

المجرم وهو الدخول أو البقاء الغير المشروع والنتيجة الإجرامية، كأن يثبت أن هذه النتيجة ترجع إلى قوة قاهرة أو حادث مفاجئ سقط السلوك الإجرامي والقصد لدى الجاني[26].

الفرع الثاني: جريمة الاعتداء العمدي على المعطيات الموجودة داخل النظام المعلوماتي.

نص المشرع الجزائري على هذا النوع من الجرائم في المادة 394 مكرر1 من قانون العقوبات، هذه الجريمة تتمثل في صورتين الأولى الاعتداء العمدي على المعطيات الموجودة داخل النظام، أما الثانية فهي المساس العمدي خارج النظام.

يتمثل الركن المادي للصورة الأولى من هذا النوع من الجرائم والذي يتجسد أساس في ثلاث أفعال وهي الإدخال، المحو، التعديل والملاحظ أن المشرع لم يشترط اجتماع هذه الأفعال معا لتكون صورة واحدة بهذه الجريمة، بل بكفي أن يكون فعلا واحدا صادرا عن الجاني كي يقوم الركن المادي، كما أن هذا التلاعب في المعطيات يقتصر على المعلومات التي يحتويها النظام سواء بإضافة ما هو جديد صحيحا كان أو غير ذلك، أو تعديل ما هو موجود بأي شكل من الأشكال، وقد ذكر المشرع العقوبة الواجب تطبيقها في المادة 394 مكرر1[27].

أما الصورة الثانية وهي المساس العمدي للمعطيات خارج النظام، فقد جاء بها المشرع الجزائري في نص المادة 394 مكرر2، وبذلك يكون قد كرس حماية جزائية للمعطيات في حد ذاتها لكونها أنه لم يشترط أن تكون المعلومة داخل نظام المعالجة الآلية أو قد تم معالجتها آليا.

فالقفرة 01 من نفس المادة تنص على أن محل الجريمة يتمثل أساسا في المعطيات بغض النظر عن كيفية وطريقة تخزينها سواء كانت مرسلة عن طريق منظومة معلوماتية أم معالجة آليا أو كانت ضمن أقراص لكونها استعملت لارتكاب جرائم منصوص عليها، أما بخصوص فقرتها الثانية فقد خصها بالأفعال المجرمة في حد ذاتها بغض النظر عن الغرض من هذه الجرائم، وهذا ما ميز المشرع الجزائري عن غيره[28]، أما بخصوص العقوبة فهي واضحة في المادة 394 مكرر2.

[26]– مختارية بوزيدي، المرجع نفسه، ص 16.
[27]– مختارية بوزيدي، المرجع نفسه، ص 16.
[28]– مختارية بوزيدي، المرجع السابق، ص 18.

الخاتمة:

إن الحماية القانونية التي أحاطها المشرع الجزائري بالمعطيات الشخصية للأشخاص الطبيعيين في مواقع التواصل الاجتماعي غير كافية بضمان أمنها المعلوماتي، بدليل التزايد المستمر للجرائم الماسة بالحق في الخصوصية الناتجة عن الاستخدام اللامشروع لمنصات التواصل الاجتماعي، وما تبعها عن ذلك من جرائم ذات الصلة بها.

وصحيح ان مواقع التواصل الاجتماعي تلعب دورا بارزا في تعزيز العلاقات الاجتماعية بين مختلف الشعوب والاجناس والاعمار من جهة، وتشجيع الاعلام الالكتروني، وتوريد الخدمات والسلع من جهة ثانية، إلا أنها تشكل في نفس الوقت أرضية خصبة ومغرية لكل من تسول له نفسه انتهاك قواعد الخصوصية التي تتسم بها هذه المواقع، فقد باتت عيوبها تطغى على مزاياها على جميع الأصعدة، وبالخصوص انتشار جرائم انتهاك حق الخصوصية الرقمية، لأجل ذلك توصلت الدراسة للعديد من النتائج والاقتراحات نوردها على النحو الآتي:

أولا: النتائج:

- إن الحق في الخصوصية في العالم الواقعي أو الافتراضي مكفول بحماية قانونية ودستورية، بحيث يمنع منعا باتا من الغير الاطلاع على البيانات والمعطيات الشخصية الخاصة دون إذن من المعني، كإستثناء من القاعدة يمكن الاطلاع على هذه الاخيرة دون علم صاحبها متى اقتضت الضرورة ذلك.
- استنادا للأحكام التي جاء بها المشرع الجزائري في القانون 18-07 أنه يشترط أن تكون المعطيات المسجلة في المواقع الالكترونية عموما ومنصات التواصل الاجتماعي خصوصا بيانات صحيحة ومتطابقة مع بيانات هوية المعني حتى تكون محل حماية واعتدائها يشكل جريمة عدا ذلك فلا نكون أمام جريمة الاعتداء على حرمة الحياة الخاصة.
- إن تكريس مبدأ الملائمة بين طبيعة البيانات المسجلة الكترونيا والهدف من تسجيلها ومعالجتها يضفي نوع من الثقة والأمان لدى المستخدمين الكترونيا.
- كلما تحدثنا عن الحماية الجزائية في أي موضوع كان تقابلها المسؤولية الجزائية المترتبة عن انتهاك هذه الحماية، وأن الحق في الخصوصية في مواقع التواصل الاجتماعي هو معني أيضا بهذه الحماية والمسؤولية وما يتولد بينهما من سلوكات إجرامية متنوعة ومختلفة بحسب طريقة وأسلوب اقترافها.
- توجد العديد من البرامج التقنية التي تعمل على حماية البيانات الشخصية سواء بالنسبة لنظام التشغيل اندرويد أو أي او آس لكن في أغلبها تتعرض للاختراق.

ثانيا: الاقتراحات:

- يتعين على المشرع الجزائري سن نصوص قانونية فعالة تتماشى وتطور السلوكيات الاجرامية الالكترونية، فضلا عن تشديد العقوبات الرادعة في تحقيق العدالة الجنائية.
- محاولة خلق علاقة متكاملة بين رجال القانون والمتخصصين في مجال الاعلام أو الاتصال والرقمنة وإخضاع كل منهما لتكوين مكثف من أجل السعي وراء محاربة هذا النوع الحديث من الاجرام أو كما يسميه البعض بالإجرام المعاصر.
- نشر حلقات توعوية للجمهور بخصوص حسن استخدام بيانتهم الشخصية في مواقع التواصل الاجتماعي حتى لا يقعوا موقع الضحية.
- إعطاء أهمية قانونية وقضائية لمسألة الحق في الخصوصية في مواقع التواصل الاجتماعي لما يترتب عنها من صور أخرى للجرائم ذات الطبيعة الالكترونية.

قائمة المصادر والمراجع:

أولا: النصوص القانونية

1. التعديل الدستوري لسنة 2020 الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، جريدة رسمية رقم 82 مؤرخة في 30 ديسمبر 2020.
2. الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المعدل والمتمم بموجب الأمر رقم 20-04 المؤرخ في 30 أوت 2020، جريدة رسمية رقم 51 مؤرخة في 31 أوت 2020.
3. القانون رقم 18-07 المؤرخ في 10 يونيو 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي جريدة رسمية رقم 34 مؤرخة في 10 يونيو 2018.
4. القانون رقم 20-05 المؤرخ في 28 أبريل 2020 والمتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، جريدة رسمية رقم 25 مؤرخة في 29 أبريل 2020.

ثانيا: الكتب

1. أسنر خالد سلمان الناصري، المسؤولية المدنية عن انتهاك الخصوصية عبر وسائل التواصل الاجتماعي، دار النهضة العربية، مصر، 2019.
2. جمال صالح عبد الحليم، الحماية الجنائية للحق في الخصوصية في مواجهة نظم المعلومات، دار النهضة العربية، 2018.

3. جمال صالح عبد الحليم، علانية جرائم الانترنت الأخلاقية، دار النهضة العربية، مصر، 2019.
4. الجواد دلال صادق، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2008.
5. الزبير حايف سالم، الاعتداء على الحياة الخاصة عن طريق الانترنت في التشريع العراقي واللبناني دراسة مقارنة، دار النهضة العربية، مصر، 2018.
6. عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا (دراسة مقارنة)، دار النهضة العربية، مصر، 2010.
7. محمد رشاد القطعاني، الحماية الجنائية للحق في حرمة الاتصالات الشخصية: دراسة مقارنة بين القانونين المصري والإماراتي وبعض القوانين الأجنبية، دار الكتب المصرية، دار الفتح للطباعة والنشر، مصر، 2015.

ثالثا: الرسائل والمذكرات

1. محمد خليفة، التواجد الغير مشروع في أنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة باجي مختار، عنابة، الجزائر، 2011.

رابعا: المقالات

1. حزام فتيحة، حماية الأنظمة الرقمية بين الأليات التقنية وأجهزة الحماية–قراءة في احكام المرسوم الرئاسي 20–05، مجلة الحقوق والعلوم الإنسانية، الجزائر، المجلد 13، العدد 03، 2020.
2. حكيمة جاب الله، انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها، حوليات جامعة الجزائر 01، الجزائر، المجلد 35، العدد 03، 2021.

خامسا: أشغال الملتقيات

1. مختارية بوزيدي، ماهية الجريمة الالكترونية، كتاب أعمال الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، يوم 29 مارس 2017، مركز جيل للبحث العلمي، الجزائر.

سادسا: المواقع الإلكترونية

1. الموقع الرسمي للبرنامج ماي داتا ماناجر تم الاطلاع على بتاريخ 2023/05/28 على الساعة 22:30 على الرابط:
https://play.google.com/store/apps/details?id=com.mobidia.android.mdm&hl=ar&gl=US

2. خلدون غسان سعيد، تطبيقات مفيدة لحماية الخصوصية الرقمية –تؤمن تصفح الأنترنيت والتراسل ورسائل البريد الالكتروني– مقال منشور بتاريخ 12 جانفي2021، تم الاطلاع بتاريخ 2023/06/01 على الساعة 10:00 في الرابط التالي: https://my-data-manager.ar.uptodown.com/android

3. الموقع الرسمي للبرنامج سيغنال تم الاطلاع على الموقع بتاريخ 2023/06/02 على الساعة 13:20 على الرابط التالي:
https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=ar&gl=US

4. الموقع الرسمي للبرنامج بروتن مايل تم الاطلاع عليه بتاريخ 2023/06/10 على الساعة 00:00 على الرابط التالي:
https://play.google.com/store/apps/details?id=ch.protonmail.android&hl=ar&gl=US

5. الموقع الرسمي للبرنامج فينغر سيكيريتي تم الاطلاع عليه بتاريخ 2023/06/13 على الساعة 02:05 على الرابط التالي:
https://fingersecurity.ar.uptodown.com/android/download