

الحماية القانونية للبيانات الشخصية من الجرائم المعلوماتية في ضوء التشريع الجزائري *Cybercrime related to personal data In the light of Algerian legislation*

الدكتورة عبيزة منيرة⁽¹⁾

جامعة محمد لين دباغين - سطيف 2 (الجزائر)

abizamounira@gmail.com

تاريخ النشر
30 نوفمبر 2023

تاريخ القبول:
02 سبتمبر 2023

تاريخ الارسال:
15 أبريل 2023

الملخص:

إن مصطلح الخصوصية من المفاهيم المرنة التي تتغير من وقت لآخر ومن مكان لآخر وتعد خصوصية البيانات الشخصية محل سطو وانتهاك نظرا لانتشارها المذهل على شبكة الانترنت، فسعت التشريعات على المستوى الدولي والوطني- منها المشرع الجزائري- لسن نصوص قانونية تكفل الحماية لخصوصية الفرد، وتكمن إشكالية هذا الموضوع في بيان المقصود بمصطلح البيانات الشخصية، وأهم الآليات القانونية التي كرسها المشرع الجزائري لحمايتها هذا الحق. وللإجابة على هذه الإشكالية يتم في البداية تعريف الجريمة المعلوماتية وكذا تحديد أركانها، وتتناول مفهوم البيانات الشخصية، وفي الأخير نعرض أنواع الجريمة المعلوماتية التي تمس البيانات الشخصية، ودور التشريعات في توفير الحماية القانونية حيث تركز الضوء على التشريع الجزائري، خلصت الورقة البحثية لمجموعة من النتائج أهمها أن المشرع الجزائري كفل حماية للبيانات الشخصية في ظل التطور التكنولوجي الذي شهده العالم، بل كان حريصا على حماية خصوصية الفرد وذلك بفرض عقوبات جزائية رادعة لكل من يحاول التعدي أو يعتدي على خصوصية الفرد.

الكلمات المفتاحية:

الجريمة المعلوماتية، الحياة الخاصة، البيانات الشخصية، البيئة الرقمية، قانون 07-18.

Abstract :

The term privacy is a flescible concept; the development of the personal information protection privacy legislation was coincided with the computer crimes legislations, as the electronic environment is consided the ultimate environment to violate the right of information privacy. The problem of this study in an explanation of what is meant by the term personal information, and the most important legal ,mechanisms devoted by the Algerian legislator to protect this right. In order to answer this problem we first dixussed the concepet of personal information and Cybercrime, finally on the legal protection of personal information.the research paper concludzd zith a set of results is that; the Algerian legislator ensuredthe protection of personal data in light of the technological development ; but rather was keen to protect the privacy of the individual by I,posing deterrent penal for anyone who atempts to infringe the privacy of the individual

Key words :

Cybercrime - private life - personal information - the electronic environment - law 18/07.

مقدمة :

من أسوء إفرزات التقدم التكنولوجي الذي شهده العالم هو التعدي على خصوصية الأفراد، لهذا فقد كان وما زال الاهتمام بحماية الحياة الخاصة هدفا من الأهداف التي توخت القوانين تحقيقها، وهذا ما دفع التشريعات إلى إيجاد نصوص قانونية رادعة لتكريس حماية البيانات الشخصية، كما وضعت وسائل تقنية متطورة لضمان حماية لهذه البيانات الخاصة وبعث الثقة والأمان لدى المتعامل الإلكتروني.

تكمُن أهمية هذا الموضوع في أن البيئة الرقمية أصبحت من سمات العالم المتحضر وتتجلى أساسا في شبكة الإنترنت التي تسمح بالإطلاع على البيانات لمستخدميها مما يجعلها عرضة للسطو والتجسس، وهذا ما استلزم تدخل القوانين لحماية تلك البيانات ومنع الغير من التعامل بها إلا بوجود ترخيص أو إذن من الجهة المختصة بذلك، وأي تعامل غير مشروع وغير مصرح به يعرض صاحبه إلى عقوبات جزائية.

تتمثل مشكلة البحث بوجود العديد من الاعتداءات التي تتعرض لها البيانات الشخصية، وحول ما إذا كان المشرع الجزائري كفل الحماية اللازمة لتلك البيانات وكان ذلك بمثابة الدافع للبحث في هذا الموضوع ومعرفة الآليات القانونية المكرسة لحماية البيانات الشخصية، لذا تتبلور مشكلة الدراسة في تساؤل هو: ما مدى فعالية الحماية القانونية التي أقرها المشرع الجزائري للبيانات الشخصية من الجرائم المعلوماتية؟

وتقتضي طبيعة هذا الموضوع الاعتماد على المنهج التحليلي، وذلك من خلال تحليل النصوص القانونية المنظمة لمسألة حماية البيانات الخصوصية واستخلاص النتائج والغاية المرجوة منها.

كما تمت الاستعانة بالمنهج المقارن من خلال المقارنة بين نصوص القانون الجزائري وغيره من التشريعات للوقوف على سلبيات وإيجابيات نصوص القانون الجزائري ومحاولة سد القصور. وإن طبيعة الإشكالية تتطلب معالجة الموضوع ضمن مبحثين حيث سنتناول في المبحث الأول: الإطار المفاهيمي للربط بين الجريمة المعلوماتية والبيانات الشخصية، حيث خصص المطلب الأول لمفهوم الجريمة المعلوماتية، وتم تخصيص المطلب الثاني لمفهوم البيانات الشخصية. أما المبحث الثاني تطرقنا فيه إلى صور الاعتداء الإلكتروني على البيانات الشخصية والحماية القانونية المقررة لها، تعرضنا في المطلب الأول لصور الاعتداء على البيانات الشخصية، وفي ظل الاعتداءات التي تتعرض لها خصوصية الأشخاص خاصة أمام التطور التكنولوجي اقتضينا تخصيص المطلب الثاني للحماية القانونية للبيانات الشخصية.

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية والبيانات الشخصية

لقد أفرز التقدم العلمي وسائل جديد للتواصل من شأنها تسهيل كثير من الخدمات والأعمال وذلك بتوفير الوقت والجهد، من خلال استخدام الحاسب الآلي لتخزين ومعالجة واسترجاع المعلومات، علاوة عن استخدامه في التعليم والتصنيع والإدارة والخدمات الترفيهية من خلال شبكات الإنترنت، فقد دخل الحاسب الآلي وغيره من التقنيات الحديثة شتى نواحي الحياة الإنسانية فتوصلت البشرية إلى السيطرة على المعلومات.

غير أن بعض مستخدمي التقنية الحديثة استغل التقدم العلمي في ارتكاب العديد من الجرائم التي لم تكن معروفة من قبل كالدخول إلى المواقع وتدميرها واختراق المواقع الرسمية والشخصية، واختراق بطاقات الائتمان، ونشر الإباحة وبث الأفكار المتطرفة ناهيك عن التعدي على خصوصية وحرية الأفراد¹ خاصة بعد ظهور وسائل حديثة للتواصل الاجتماعي التي سمحت بانتشار مذهل للمعلومات الشخصية على شبكة الانترنت مما يهدد حرمة الحياة الخاصة.

وعلى ذلك سنتناول في هذا المحور مفهوم الجريمة المعلوماتية في المطلب الأول، لنتطرق بعدها لمفهوم البيانات الشخصية وهذا في المطلب الثاني.

المطلب الأول: مفهوم الجريمة المعلوماتية

إن التعرف على مفهوم الجريمة المعلوماتية شرط أساسي للتوصل إلى أشكال الاعتداءات التي تتعرض لها البيانات الشخصية، ولذلك فخصص الفرع الأول من هذا المطلب لمعنى الجريمة المعلوماتية، ثم ناقش في الفرع الثاني أركان الجريمة المعلوماتية، ونتطرق في الفرع الثالث لصور الجريمة المعلوماتية.

الفرع الأول: تعريف الجريمة المعلوماتية

الجريمة المعلوماتية تختلف عن الجريمة التقليدية في كون الأولى جريمة ترتكب عبر الفضاء الإلكتروني فهي جريمة افتراضية تكون في عالم غير مادي، وتتعدد المصطلحات التي تطلق على هذا النوع من الجرائم فيسميها البعض بالجرائم الإلكترونية أو جرائم الكمبيوتر والإنترنت أو جرائم السير أو الغش المعلوماتي أو الجرائم الافتراضية وغيرها من المصطلحات، ويبقى مصطلح الجريمة المعلوماتية أشمل وأوسع، فمصطلحي الجرائم المعلوماتية وجرائم السير يشملان إلا الجرائم المعلوماتية الواقعة عبر شبكة الإنترنت، في حين أن مصطلح جرائم الغش المعلوماتي يشمل جرائم الإتلاف المعلوماتي والتجسس المعلوماتي، أمّا مصطلح جرائم الكمبيوتر والانترنت قاصر عن شمول الجرائم المعلوماتية التي تقع بواسطة الهاتف النقال²، ولقد اختلف

الفقه في وضع تعريف جامع مانع للجريمة المعلوماتية باختلاف المعيار المعتمد عليه، وسوف نحاول توضيح هذه الاتجاهات كالآتي:

أولاً - الاتجاه الأول لتعريف الجريمة المعلوماتية:

يعرف الجريمة المعلوماتية بالاستناد إلى وسيلة ارتكاب الجريمة. ويرى أصحاب هذا الاتجاه على ضرورة الاعتماد على معيار وسيلة ارتكاب الجريمة في تعريف هذه الجريمة، ومن أنصار هذا الاتجاه الفقيه الألماني تاديان حيث عرف الجريمة المعلوماتية أنها: «العمل غير المشروع الذي يكون الحاسب داخلاً في ارتكابه»³.

غير أن الاعتماد على وسيلة ارتكاب الجريمة منتقد لأن الجريمة المعلوماتية تقوم في الأساس على العمل الرئيسي المكون لها فقط الوسيلة المعتمدة هذا من جهة، ومن جهة أخرى فإنّ المشرع عندما يجرم سلوكاً ما يهتم بمدى خطورة السلوك وليس بالوسيلة المستخدمة.

ثانياً - الاتجاه الثاني لتعريف الجريمة المعلوماتية:

يعرف أنصار هذا الاتجاه الجريمة المعلوماتية بالاستناد إلى موضوعها. ويرى أصحاب هذا الاتجاه أن الجريمة تكون معلوماتية إذا كان محلها الكمبيوتر أو نظامه المعلوماتي أي تشمل الجرائم الواقعة على الكمبيوتر ومعطياته وعرفها أنصار هذا الاتجاه أنها: «نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه»⁴.

إنّ هذا الاتجاه، يجعل التعريف قاصراً وشاملاً فقط للجرائم الواقعة على الكمبيوتر أو معطياته دون الجرائم التي تقع بواسطة الكمبيوتر فأهم دور الكمبيوتر في وقوع هذه الجرائم⁵.

ثالثاً - الاتجاه الثالث لتعريف الجريمة المعلوماتية:

يعرف أنصار هذا الاتجاه الجريمة المعلوماتية بالاستناد إلى معيار المعرفة الفنية. واستناداً إلى هذا الاتجاه تكون الجريمة معلوماتية إذا ما توافرت لدى مرتكبها المعرفة والدراية الفنية بتكنولوجيات المعلومات، حيث عرف أنصار هذا الاتجاه الجريمة المعلوماتية أنها: «جريمة تتطلب لاقترافها معرفة بتقنية النظام المعلوماتي لدى فاعلها».

ويؤخذ على هذا الاتجاه أنّه حصر نطاق ارتكاب الجريمة المعلوماتية بالقدرة التقنية في حين أنّه هناك حالات أخرى ترتكب فيها الجريمة المعلوماتية دون أن يتطلب ذلك قدر من المعرفة والخبرة الفنية هذا من جهة⁶، ومن جهة أخرى فإنّ الأخذ بهذا المعيار يستلزم البحث في الظروف الخاصة للجاني وهو ما يتناقض مع أحكام القانون الجنائي باعتباره قانون موضوعي لا يُعتمد بالظروف الشخصية إلا على سبيل الاستثناء⁷.

وبعدما تعرضنا لأهم الاتجاهات الفقهية المعتمدة في تعريف الجريمة المعلوماتية، يتضح أنه من الصعوبة الاعتماد على معيار واحد فقط لتعريف الجرائم المعلوماتية، وبما أن هذه الجريمة لا تختلف عن الجريمة المعلوماتية إلا من حيث محلها فهو دائما يكون في فضاء إلكتروني افتراضي غير ملموس لأنه قد تكون في الأساس جريمة تقليدية غير أنها تتم عن طريق التقنية المعلوماتية بعد أن كانت ترتكب سلوك مادي ملموس واستنادا إلى ذلك يمكننا أن نعرف الجريمة المعلوماتية أنها: «سلوك غير مشروع معاقب عليه قانونا صادرا عن إرادة محله بيئة إلكترونية».

الفرع الثاني: أركان الجريمة المعلوماتية

جاء قانون العقوبات الجزائري على غرار غيره من الدول بعقوبات تفرض على الجاني لينال جزاؤه تختلف باختلاف درجة خطورة الجريمة، ولكن عند توافر أركان الجريمة المحددة بثلاثة أركان، ولما كانت الجرائم المعلوماتية لا تختلف عن الجرائم التقليدية إلا من حيث أن محلها المعلومات الرقمية في بيئة إلكترونية وبالتالي تتكون هي الأخرى من ثلاثة أركان كالآتي:

أولا - الركن المادي:

إن الركن المادي للجريمة يشمل جميع صور السلوك الإيجابية والسلبية في بيئة رقمية، كأن يقوم مرتكب الجريمة بتجهيز الحاسب تمهيدا لحدوث الجريمة، أو يتولى تحميل الكمبيوتر ببرامج اختراق، أيضا كأن يقوم بتهيئة صفحات تحمل في طياتها أفعال إباحية وغيرها من السلوكات غير مشروعة.

وما يستحق التنويه إليه أنه يُصعب الفصل بين الأعمال التحضيرية في مجال تكنولوجيات المعلومات تمثل جريمة في حد ذاتها كشراء برامج اختراق وكلمات المرور.⁸

وبطبيعة الحال تثير الجريمة المعلوماتية إشكالات قانونية تتعلق بالنتيجة الإجرامية فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فهذه الجريمة لا تعترف بالحدود الإقليمية للدول فقد يكون الجاني في دولة والمجني عليه في دولة أخرى، فعلى سبيل المثال جريمة نشر المواد المخلة بالأداب العامة يكون هناك عدد متضررين في دول مختلفة، كما تثير الجريمة الإلكترونية إشكالات أخرى تتعلق بالقانون الواجب التطبيق والمحكمة المختصة.⁹

ثانيا - الركن المعنوي:

الركن المعنوي للجريمة هو السلوك الصادر عن شخص مسؤول يتوفر لديه القصد الجنائي بشقيه (العلم والإرادة) بغض النظر إذا كان على دراية بالمعرفة الضنية أولا¹⁰، وقد فرق المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فمثلا يعتمد في قانون العلامات التجارية في القانون الفيدرالي الأمريكي على مبدأ الإرادة، ويأخذ

أحيانا أخرى بمبدأ العلم كما هو الحال في قانون مكافحة الاستنساخ الأمريكي، وقد تبنى القضاء الأمريكي في قضية موريس المتعلقة بالدخول غير مصرح به على جهاز حاسب فيدرالي معيارين هما الإرادة بالدخول غير المصرح به، وكذا معيار العلم على الحضر باستخدام نظم معلومات فيدرالية دون تصريح.

وقد اعتمد القضاء الفرنسي على مبدأ سوء النية في شأن الجريمة المعلوماتية وهو نفس المبدأ الذي تبناه المشرع الجزائري بموجب قانون العقوبات 04-15¹¹ حيث استوجب في جل النصوص القانونية التي تضمنها القسم السابع المكرر المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أن ترتكب عن طريق الغش أي تتوفر فيه سوء النية.

ثالثا- الركن الشرعي:

يقصد بالركن الشرعي السلوكات التي يجرمها المشرع ويفرض لها عقوبات فلكي يعتبر السلوك جريمة لا بد أن يجرمه القانون وهو ما أقره المشرع الجزائري في المادة الأولى من قانون العقوبات بنصها: «لا جريمة ولا عقوبة أو تدبير أمن بغير قانون»، وقد اعتبر المشرع الجزائري الاعتداء على المعلومات أو البيانات الإلكترونية في بيئة إلكترونية جريمة يعاقب عليها القانون بإضافة القسم السابع مكرر إلى قانون العقوبات تحت عنوان 'المساس بأنظمة المعالجة الآلية للمعطيات'.

المطلب الثاني: مفهوم البيانات الشخصية

أمام التطور المذهل الذي شاهده العالم اليوم في مجال الاتصالات وغزو الحاسوب لحياتنا الخاصة وبالأخص الإنترنت التي أصبحت أكثر وسيلة لتواصل في مختلف الميادين، أصبحت البيانات الشخصية للأفراد عرضة للتداول والانتشار وهذا ما دفع التشريعات إيجاد نصوص قانونية لتكريس الحماية للبيانات الشخصية للفرد وأهمها قانون 07/18¹²، وعليه سنتناول في الفرع الأول تعريف البيانات الشخصية، ومن ثم تحديد أنواع البيانات الشخصية من خلال الفرع الثاني.

الفرع الأول: تعريف البيانات الشخصية

سنركز في تعريفنا للبيانات الشخصية أو ما يسمى بالمعطيات الشخصية على تعريف المشرع الجزائري، حيث عرفها في المادة الثالثة من القانون 18-07 السالف الذكر أنها: «كل معلومة بغض النظر عن دعائمتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه الشخص المعني بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهوية البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية».

يتضح من نص المادة أعلاه أن المشرع الجزائري أجمل جميع البيانات الشخصية وعددها على سبيل التخيير، بمعنى أي من البيانات الواردة في التعريف يمكن أن يعد بيانا شخصيا متعلق بالشخص لا بد من حمايتها سواء تمت معالجتها بطريقة يدوية أو إلكترونية تخص الشخص المعني، وعرفه المشرع في نفس المادة في الفقره الموالية أنه: «كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع المعالجة» ويتبين لنا أن المشرع اعتبر البيانات الشخصية تلك البيانات المتعلقة بالشخص الطبيعي فحسب من دون الشخص المعنوي، فالأشخاص المعنوية مستبعدة من نطاق هذه الحماية وهو ما يتناقض مع بعض النصوص القانونية الواردة في القانون 18-07 السالف الذكر حيث استوجب مثلا الحصول على ترخيص من السلطة الوطنية إذا تعلق الأمر بالربط البيني للقات تابعة لشخص أو عدة أشخاص معنويين يسيرون مرفقا عموميا لأغراض مختلفة مرتبطة بالمنفعة العامة¹³.

الفرع الثاني: أنواع البيانات الشخصية

سنتناول صور البيانات الشخصية إلا أنه ليس من السهولة تحديد صور البيانات الشخصية أمام التطور التكنولوجي المستمر الذي يسمح بسعة مدلول هذه البيانات وسرعة تطورها، وعليه يمكن تصنيف البيانات الشخصية على سبيل المثال لا الحصر إلى بيانات اسمية وبيانات غير اسمية على النحو الآتي:

أولا - البيانات الاسمية:

يضم البيانات التي تتعلق باسم الشخص ولقبه ويتنوع الاسم إلى اسم أصلي واسم الشهرة والاسم المستعار، وعادة ما يتم استخدام البيانات الاسمية على مواقع التواصل الاجتماعي كالفيس بوك وتويتر والانستغرام، وكذلك يستعمل في حساب البريد الإلكتروني، وعند التسوق عبر الانترنت لطلب السلعة أو الخدمة¹⁴.

ثانيا - البيانات غير الاسمية:

تتضمن هذه البيانات المعلومات الاسمية غير المباشرة التي لا يمكن من خلالها تحديد هوية الشخص إلا باقترانها بمعلومات أخرى، ومن أهم هذه البيانات الأرقام الشخصية مثل رقم الهاتف والسيارة كذا البيانات المالية مثل الدخل الشهري للفرد والديون التي له أو عليه، والبيانات الصحية¹⁵.

المبحث الثاني: صور الاعتداء الإلكتروني

على البيانات الشخصية والحماية القانونية المقررة لها

يعد مبدأ الحق في الخصوصية من الحقوق المكرسة دستوريا والملازمة لشخصية الإنسان، وأمام التطور المذهل الذي شاهده العالم اليوم في مجال الاتصالات وغزو الحاسوب لحياتنا

الخاصة وبالأخص الانترنت التي غزت جميع ميادين الحياة أعطي لمبدأ الخصوصية اهتمام خاص فقد لا تكون البيانات الشخصية المتنقلة عبر شبكة الانترنت آمنة من التغير والسطو والتجسس، علاوة عن ذلك قد يتم نشر بيانات خاصة بالغير دون الحصول على إذن مسبق بذلك من صاحبها.

وتعتبر مسألة حماية الحق في الخصوصية بعد انتشار المعلومات الالكترونية من أكثر الأمور تعقيدا نظرا لطبيعة المفتوحة لشبكة الانترنت، لهذا سعت التشريع-----ات إلى إيجاد آليات قانونية لحماية هذه البيانات كالالتزام بالتصريح المسبق عند إجراء أي معالجة للبيانات الشخصية، وكذلك الترخيص إذا تبين للسلطة الوطنية أن المعالجة المعترزم القيام بها تتضمن أخطاراً ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأفراد، لكن تبقى الحماية القانونية لوحدها غير كافية لضمان سرية البيانات الخصوصية فظهرت وسائل تقنية كفيلة لضمان سرية هذه البيانات ومن أهم هذه التقنيات تقنية التشفير وكذا التصديق.

انطلاقاً مما سبق نتناول صور الاعتداء على البيانات الشخصية في المطلب الأول والحماية القانونية للبيانات الشخصية في المطلب الثاني

المطلب الأول: صور الاعتداء على البيانات الشخصية

إن البيانات الشخصية للأفراد تتعرض لعدو اعتداءات إلا أننا سنركز في دراستنا على أهم الاعتداءات التي تمس البيانات الشخصية

من خلال هذا المطلب نتناول جريمة سرقة البيانات الشخصية في الفرع الأول، وجريمة التشهير بالبيانات الشخصية في الفرع الثاني، وأخيراً جريمة المعالجة الالكترونية غير المشروعة للبيانات الشخصية في الفرع الثالث

الفرع الأول: سرقة البيانات الشخصية

عرفت سرقة البيانات أنها: «اختلاس للبيانات الشخصية وسحب نسخة منها باستخدام الانترنت» أي أنه إذا كان النظام المعلوماتي يتضمن كلمة سر فلا يجوز اختراقها، كسرقة الرقم السري الخاص ببطاقة الائتمان أو المتعلقة بباب البيت فإذا ما تم اختراق كلمة السر فيكون الشخص قد ارتكب جريمة يعاقب عليها القانون¹⁶ وكذلك الدخول إلى حساب بعض العملاء في المصارف وتحويلها إلى الحساب الشخصي باستخدام برمجيات معينة، أو نقل المعلومات باستخدام الفيروسات¹⁷.

القرصنة ليست هي الطريقة الوحيدة لسرقة البيانات الشخصية، بل من الممكن سرقة الحاسوب الذي يحتوي على قواعد تلك البيانات مثلما حدث في عام 2015 تمت سرقة صندوق

بيانات البنك (لويديز) البريطاني من خلاله تمت سرقة بياناتهم الشخصية للآلاف من عملاء البنك.

كما أنه بالإمكان السطو والاحتيال عبر مواقع التواصل الاجتماعي، وذلك بإنشاء مواقع لشركات تجارية وهمية بهدف جذب الأشخاص مقابل مبالغ مالية زهيدة تدفع عن طريق الفيزا كارد لسرقة الأرقام السرية للبطاقات وغيرها من طرق النصب والاحتيال التي انتشرت مؤخراً¹⁸.

الفرع الثاني: التشهير بالبيانات الشخصية

إن التعامل الإلكتروني يقدم بيانات شخصية للشركات التجارية وجهات أخرى يتعامل معها عبر شبكة الانترنت، إضافة إلى ذلك قد تتحصل السلطات على البيانات الشخصية للأفراد أثناء ممارستها لوظيفتها كالتحري والتحقيق مثلاً ففي هذه الأحوال لا بد من استعمال تلك البيانات الشخصية للأغراض المخصصة، وهو ما أقرته معظم التشريعات منها المشرع الجزائري الذي كرس ذلك في عدة قوانين حيث حصر بموجب القانون 09-04¹⁹ تسجيل مكالمات الأشخاص الخاصة والسرية، إلا إذا كان ذلك بدافع حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، أو للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وفي هذا الإطار لا يجوز استعمال المعلومات المتحصل عليها إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية تحت طائلة العقوبات الجزائية كما أكد المشرع على حماية البيانات الشخصية ومنع التشهير بها بموجب قانون 15-04²⁰، حيث استلزم على مؤدي خدمات التصديق الإلكتروني الحصول على الموافقة الصريحة للمعني لجمع البيانات الشخصية الخاصة به، وأن لا يحصل إلا على البيانات الشخصية الضرورية لمنع وحفظ شهادة التصديق الإلكتروني، وحضر استعمالها لأغراض أخرى كالتشهير مثلاً وذلك تحت طائلة العقوبات المنصوص عليها في المادة 71 من نفس القانون، أيضاً حرص المشرع من خلال قانون 18-05²¹ على حماية المعطيات الشخصية للمتعامل الإلكتروني لأن المورد الإلكتروني يقوم بتصنيف البيانات الشخصية وعمل ملف خاص لكل عميل من عملائها فقد يؤدي ذلك إلى التشهير بالمستخدم والضغط عليه وابتزازه من خلال استخدام هذه البيانات وهو ما تفتن إليه المشرع في قانون التجارة الإلكترونية فنص على ضرورة حصول المورد الإلكتروني أولاً على البيانات الضرورية وأن يضمن أمنها وسريتها، لكن لم تضاف الحماية على البيانات الشخصية في حقيقة الأمر إلا بإصدار قانون 18-07 السالف الذكر.

يتضح ممّا سلف أن المشرع الجزائري حرص على حماية خصوصية الأفراد والبيانات الشخصية التي قد يقدمونها لدى جهة ما، لأن مسألة التشهير بالبيانات الشخصية تعتبر من

أبرز الأمور الواقعة في الانترنت، وهناك قسم من المواقع خصص لهذا الغرض، وعادة الغاية من ذلك التشهير هو الإساءة لسمعة الأشخاص أو شرفهم حتى وإن كانت تلك البيانات صحيحة، وأبرز مثال عن ذلك هو ما نشر عن الرئيس الفرنسي (ميتران) عقب وفاته، حيث نشر طبيبه الخاص مذكرات سرية عن الحياة الخاصة لرئيس الفرنسي تناولت علاقاته الجنسية، والأمراض التي كان يعاني منها، ولم يعد بالإمكان السيطرة عليها بسبب تداولها وانتشارها على الانترنت، فرغم صحة هذه البيانات إلا أنها اعتداء على خصوصية الرئيس بحيث أساءت إلى سمعته وحطت من قيمته²².

الفرع الثالث: جريمة المعالجة الالكترونية

لقد اعترفت بعض الدول بمبدأ حرية الاتصال ونقل المعلومات إلا أنها تأخذ بنظام الترخيص المسبق في معالجة أو استعمال المنشآت والأجهزة التي تستخدم في بث أو نقل المعلومات أو معالجتها وتسمى بعقود نقل التكنولوجيا، فمن حق صاحب البرنامج التصرف في البرنامج واستغلاله واستعماله وأن يتنازل صاحب البرنامج عن حقوقه المتفرعة عن الملكية كلها أو بعضها للغير ببيعها أو بمنح ترخيص باستغلالها.

وعليه نشير أن المشرع الجزائري سن في هذا الصدد قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، واستوجب عند معالجة المعطيات الشخصية الحصول على موافقة سابقة من المعني، غير أنه استثنى الحصول على موافقة مسبقة من المعني في حالات معينة إذا كانت مصلحة المعني أو المجتمع تقتضي ذلك، وقد حدد هذه الحالات بموجب المادة السابعة من القانون 07-18 السالف الذكر

يتضح لنا بعد تمعن في هذه الحالات ان المشرع لم يستوجب ضرورة الحصول على الموافقة الصريحة للمعني لمعالجة البيانات الشخصية أنه كان حريصا على حماية الحقوق والحريات الأساسية للأفراد.

ونظرا لحساسية موضوع معالجة البيانات الشخصية استلزم المشرع أيضا الحصول على تصريح مسبق من السلطة الوطنية أو ترخيص منها وذلك في حالة إذا ما تبين للسلطة عند دراسة التصريح المقدم لها أن المعالجة المعتمز القيام بها تشكل خطرا ظاهرا على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأفراد، وهو ما أقره المشرع في المادة 17 من القانون 07-18 السالف الذكر التي نصت أنه: «تقرر السلطة الوطنية إخضاع المعالجة المعينة لنظام الترخيص المسبق عندما يتبين لها، عند دراسة التصريح المقدم لها، أن المعالجة المعتمز القيام بها تتضمن أخطار ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص».

في هذا المقام حرص المشرع الجزائري على حماية المعطيات الشخصية من أي اعتداء يهددها، وذلك بفرض عقوبات جزائية على كل شخص يرتكب فعل من شأنه المساس بالمعطيات ذات الطابع الشخصي كجريمة المعالجة غير المشروعة للمعطيات الشخصية المعاقب عليها بموجب المادة 59 من القانون 07-18 بنصها: «يعاقب بالحبس من سنة (1) إلى ثلاثة (3) سنوات وبغرامة من 10.000 دج 300.000 دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة».

تبين من نص المادة أعلاه أنه مجرد حصول الجاني على المعطيات الشخصية الخاصة بالغير بطريقة غير مشروعة يتحقق الركن المادي للجريمة يعاقب بصرف النظر إذا ما تم استعمالها أو لا، فهي تعتبر من أبسط أشكال الاعتداء على المعطيات الشخصية فهي لا تزال في المراحل الأولى من المعالجة.

أما الركن المعنوي يتطلب لقيامه توافر القصد الجنائي من علم الجاني بأن ما يقوم به هو طريق غير مشروع ومع ذلك تتجه إرادته إلى ذلك أي بالمخالفة لاتخاذ الإجراءات الأولية لإجراء المعالجة الالكترونية للبيانات²³، أي أن القصد المتطلب لقيام هذه الجريمة هو القصد العام بصرف النظر عن البواعث التي دفعت الجاني إلى ارتكاب فعله فسواء كان الباعث هو الإضرار المادي بالشخص أم استغلال هذه البيانات للإساءة إلى سمعة الشخص أو كان مجرد فضول²⁴.

إضافة إلى ذلك فإذا ما تم خرق المبادئ الأساسية التي يجب مراعاتها عند جمع المعطيات الشخصية المحددة بموجب المادة التاسعة من القانون 07-18 السالف الذكر يعتبر صاحبها مرتكب لجريمة الاستعمال غير المشروع للمعطيات الشخصية، وهي الجرائم التي نصت عليها المادة 60 من القانون 07-18 والمتعلقة بالسماح للأشخاص غير مؤهلين بالتولج لمعطيات الشخصية، والمادة 62 من ذات القانون المتعلقة بإفشاء معلومات محمية، كذلك ما جاء في المادة 67 من نفس القانون المتعلقة بنقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية دون احترام شروط عملية النقل المنصوص عليها في المادة 44 من ذات القانون وهي الحصول على ترخيص من السلطة الوطنية لنقل المعطيات ذات الطابع الشخصية وضروره توفر الدولة الأجنبية المزمع نقل المعلومات إليها على الحماية الكافية للحياة الخاصة والحريات والحقوق الأساسية إزاء المعالجة التي تخضع لها هذه المعطيات.

المطلب الثاني: الحماية القانونية للبيانات الشخصية

إن التقدم العلمي الذي أفرز وسائل حديثة للتواصل الفوري وبالأخص شبكة الانترنت سمح بالتعدي على خصوصية وسرية البيانات الشخصية للأفراد، وهو ما تداركه المشرع

الجزائري عند تعديله لقانون العقوبات في 2004، حيث أضاف القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات يتضح من خلال هذه الموارد بتشديد المشرع العقاب على مثل هذه الجرائم المعلوماتية، بحيث جعل من عقوبة الحبس أصلية إلى جانب عقوبة الغرامة وهو ما يمنح فعالية لنص القانوني لأن المشرع لم يفتح المجال للسلطة التقديرية للقاضي بهدف ردع المجرم إضافة إلى ذلك يتجلى اهتمام المشرع بحماية حرمة وخصوصية الفرد عندما أصدر القانون 04-09 السالف الذكر، حيث حضر تسجيل مكالمات الأشخاص الخاصة والسرية، إلا إذا كان ذلك بدافع حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، أو للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وأهم ما استحدثه هذا القانون هو إنشاء هيئة وطنية خصيصا للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، كما تتولى مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجري بشأن الجرائم الالكترونية، وهو أحسن ما فعله المشرع باعتبار أن هذا النوع من الجرائم تتطلب الاستعانة بمختصين في مجال المعلوماتية.

علاوة على ذلك حرص المشرع الجزائري على غرار غيره من التشريعات على صيانة الحياة الخاصة لكل مواطن من مواطنيه، وذلك بالنص في صلب دستوره على كفالة هذه الحماية، وهو ما كرسه في المادة 48 من القانون 16-01²⁵ وأكدته عند التعديل الدستوري بموجب المرسوم الرئاسي رقم 20-442 وذلك في المادة 47.²⁶

لكن لم يضيف القانون الجزائري الحماية على البيانات الشخصية إلا بصدر قانون حماية البيانات الشخصية 18-07 الذي استحدث آليات قانونية لحماية هذه البيانات كالالتزام بالتصريح المسبق عند إجراء أي معالجة للبيانات الشخصية وكذا إجراءات الترخيص.

الفرع الأول: التصريح المسبق بمعالجة البيانات الشخصية

لم يترك التشريع الجزائري حماية البيانات الشخصية من دون قيود وإنما وضع لها قيود وأسس قانونية عدو لحماية تلك البيانات ولم يتركها لإرادة الأشخاص منها إجراء التصريح المسبق.

وعليه سنتناول الجهة المسؤولة عن التصريح المسبق، ومضمون ذلك التصريح.

أولا - الجهة المسؤولة عن التصريح المسبق:

نصت المادة 13 من قانون حماية البيانات الشخصية 18-07 السالف الذكر، على وجوب إيداع التصريح المسبق الذي يتضمن بإجراء المعالجة لدى السلطة الوطنية ويقدم بالطريقة اليدوية أو الطريقة الالكترونية، أي هو عبارة عن إخطار من المسؤول عن المعالجة يتضمن

الالتزام بإجراء المعالجة يقدم لدى السلطة الوطنية، وتعتبر هذه السلطة من الضمانات المهمة لكفالة احترام تطبيق أحكام قانون حماية البيانات الشخصية، وتختص هذه السلطة بتسليم وصل الإيداع أو يرسل بالطريق الإلكتروني في أجل لا يتعدى 48 ساعة للمسؤول عن المعالجة الذي يباشر عملية المعالجة مجرد استلام الوصل ويلتزم بالقيام بمعالجة المعطيات الشخصية.

ثانيا- مضمون التصريح المسبق:

طبقا لأحكام القانون 18-07 السالف الذكر يتبين أنّ المشرع ميز في تحديد البيانات التي يتضمنها التصريح المسبق بين نوعين من التصريحات كما يلي:

1 - التصريح العادي: حددت المادة 14 من القانون 18-07 البيانات التي يتضمنها التصريح المسبق، وهذه البيانات هي بيانات الجهة المسؤولة عن المعالجة وكذا بيانات الشخصية للشخص المعني، والأشخاص المخولون بالاطلاع عليها، والذين سترسل إليهم، وإجراءات المعالجة المتمثلة في طبيعتها وخصائصها والغرض أو الأغراض المقصود منها، والمدد التي ستبقى فيها هذه البيانات تحت الحفظ، إضافة إلى تحديد نوع المعطيات المعترمة إرسالها إلى دول أجنبية، كذلك المصلحة التي يمكن الشخص المعني عند الاقتضاء، أن يمارس لديها الحقوق المخولة له بمقتضى أحكام هذا القانون وكذا الإجراءات المتخذة لتسهيل ممارسة هذه الحقوق أيضا وصف عام يمكن تقييم أولي لدى ملائمة التدابير المتخذة من أجل ضمان سرية وأمن المعالجة، وأخيرا لا بد من تحديد جميع أشكال التقريب الأخرى بين المعطيات، وكذا التنازل عنها للغير أو معالجتها من الباطن، تحت أي شكل من الأشكال سواء مجانا أو بمقابل.

2-التصريح المبسط: نص المشرع على هذا النوع بموجب المادة 15 من القانون 18-07 السالف الذكر ويكون في حالة إذا ما تعلق الأمر بأصناف معالجات المعطيات ذات الطابع الشخصي التي ليس من شأنها الإضرار بحقوق وحرريات الأشخاص المعنيين وحياتهم الخاصة، ففي هذه الحالة يكون التصريح مبسطا يكفي ببيانات محددة حيث يشار فيها فقط إلى العناصر المذكورة في البنود 1 من المادة 14 من ذات القانون.

وقد استثنى المشرع الجزائري بعض صور معالجة البيانات الشخصية من شرط التصريح المسبق وذلك عند إنشاء سجل مفتوح ليطلع عليه الجمهور أو كل شخص ثبت له أن له مصلحة مشروعة في ذلك لأنّ المعالجة التي تهدف إلى إنشاء هذا السجل أو الدفتر هو إعلام الكل، فبإمكان أي شخص أن يحصل على معلومة منه.

الفرع الثاني: الترخيص المسبق بمعالجة البيانات الشخصية

يجب الحصول على ترخيص مسبق عند القيام بأنواع معينة من المعالجات للبيانات الشخصية، وهذا ما اشترطه المشرع الجزائري، لأنّ هذا النوع من المعالجة فيه نوع من الخطورة،

إذ اعتبر المشرع أنَّ مجرد التصريح المسبق لا يكفي فأوجب الحصول على الترخيص قبل القيام بالمعالجة، ويمكن تعريف الترخيص استنادا لنص المادة 17 من القانون 07-18 أنه: «وثيقة رسمية تصدر عن السلطة الوطنية يتضمن قرار الموافقة على القيام بالمعالجة البيانات الشخصية»

وهذا الترخيص يكون في حالات معينة يمكن تحديدها وفق أحكام قانون حماية البيانات الخصوصية كالآتي:

❖ الحالة الأولى: يجب على المسؤول عن المعالجة الحصول على ترخيص مسبق من السلطة الوطنية لمزاولة نشاط معالجة البيانات الخصوصية، إذا تبين للسلطة عند دراسة التصريح المسبق، أنَّ المعالجة المعترزم القيام بها تتضمن أخطار ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص وهذا طبقا لنص المادة 17 من القانون 07-18 السالف الذكر.

❖ الحالة الثانية: إذا تعلق الأمر بمعالجة المعطيات الحساسة فهي من الحالات التي استثنائها المشرع أصلا من نطاق المعالجة بموجب المادة 18 من القانون 07-18 السالف الذكر، لكن يمكن للسلطة الترخيص بذلك إذا توافرت الحالات المنصوص عليها في المادة 18.

❖ الحالة الثالثة: إذا تعلق الأمر بالربط البيني للملفات تابعة لشخص أو عدد أشخاص معنويين يسيرون مرفقا عموميا لأغراض مختلفة مرتبطة بالمنفعة العامة وكذلك الربط البيني للملفات التابعة للأشخاص الطبيعية الذي يتم لأغراض مختلفة وهذا طبقا لأحكام المادة 19 من القانون 07-18.

❖ الحالة الرابعة: وتتعلق بمعالجة المعطيات الشخصية التي تهدف إلى تحقيق مصلحة عامة للبحث أو الدراسة أو التقييم في مجال الصحة، حسب ما جاء في المادة 21 من القانون 07-18. يتضح أنَّ المشرع الجزائري كرس الحماية القانونية للأفراد في مجال معالجة المعطيات ذات الطابع الشخصي من خلال أحكام نصوص القانون 07-18 السالف الذكر، وذلك باستحداث جهة إدارية مستقلة المتمثلة في السلطة الوطنية تتولى مراقبة معالجة المعطيات ذات الطابع الشخصي بشكل يسمح بالتطبيق الصارم لقانون حماية المعطيات ذات الطابع الشخصي، وقد حدد المشرع الجهة القائمة بمعالجة المعطيات الشخصية وهو ما يعرف "بالمسؤول عن المعالجة"، حيث عرفه في المادة الثالثة من القانون أنه: «كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها»، كما أوجد المشرع إلى جانبه "المعالج من الباطن الذي يعمل لحساب المسؤول عن المعالجة وهو ما أوضحه المشرع عند تعريفه في المادة الثالثة من نفس القانون أنه: «كل شخص طبيعي أو معنوي،

عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة».

وحرصا من المشرع على حماية المعطيات الشخصية للأفراد حدد بموجب المادة التاسعة من ذات القانون المبادئ الأساسية التي يجب التقيد بها سواء من قبل المسؤول عن المعالجة أو المعالج من الباطن عن معالجة المعطيات الشخصية فاستوجب أن تكون المعالجة بطريقة مشروعة ونزيهة، وأن تكون مجمعة لغايات محددة، وواضحة ومشروعة وألا تعالج لاحقا بطريقة تتناف مع هذه الغايات، وأن تكون ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها أي يتم جمع ومعالجة المعطيات الشخصية الضرورية فقط، وأن تكون صحيحة وكاملة ومحينة إذا اقتضى الأمر، ومحافظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة معينة وفق ما يتناسب لانجاز الأغراض التي من أجلها تم جمعها ومعالجتها أي أنه إذا تحققت الغاية من جمع ومعالجة المعطيات الشخصية لا بد من محوها إلا إذا أذنت السلطة الوطنية لحفظها لغايات تاريخية أو عملية أو إحصائية بناء على طلب من المسؤول عن المعالجة.

خاتمة:

إن أهم ما يميز المعاملات الإلكترونية وقوعها في عالم افتراضي يعتمد أساسا على شبكة الانترنت وهي شبكة مفتوحة تسمح بتداول المعلومات والإطلاع عليها من قبل الغير، مما يهدد حقوق المتعامل الإلكتروني فظهرت الحاجة للبحث عن حماية تحمي البيانات الخاصة به وبالأخص الشخصية منها، لذا أصدر المشرع الجزائري مجموعة من القوانين أهمها قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي لإضفاء نوع من الحماية على البيانات الشخصية للفرد.

- النتائج:

بعد أن تم الاطلاع بمختلف جوانب الموضوع، نطرح ما توصلنا إليه من نتائج على النحو التالي:

- 1- إن البيانات الشخصية هي تلك المعلومات المعالجة بشكل الكتروني وتقليدي تتعلق بشخص طبيعي، وقد تكون هذه البيانات اسمية تتعلق باسم الشخص ولقبه أو بيانات غير اسمية التي لا يمكن من خلالها تحديد هوية الشخص.
- 2- كفل المشرع الجزائري حماية للبيانات الشخصية في قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ليشمل بذلك حماية البيانات الشخصية بمفهومها

المعاصر، كما كان حريصا على حماية خصوصية الفرد وذلك بفرض عقوبات جزائية لكل من يهدد أو يعتدي على خصوصية الفرد.

- المقترحات:

على ضوء ما تقدم من نتائج، نقترح بما يلي:

- 1- ضرورة إقرار المشرع الجزائري في إصدار قانون خاص بمكافحة الجريمة المعلوماتية يحدد فيها بالأخص إجراءات التحري والتحقيق في ميدان البيئة الرقمية.
 - 2- العمل على القيام بدورات تدريبية وتفعيلها لرجال القانون في تخصصات علوم الحاسب الآلي والاتصال المعلوماتي، وتوعية المجتمع على ضرورة قراءة بنود وشروط التعاقد والتسجيل في المواقع والتأكد من سياسة الخصوصية حتى لا يقع ضحية الاعتداء على بياناته الخاصة.
 - 3- نهيب بالمشرع الجزائري تنظيم تقنية التشفير بشكل من التفصيل خاصة وأن هذه التقنية أصبحت ضرورية بانتشار المعاملات الإلكترونية فمن شأنها حماية البيانات والمراسلات وبالأخص الشخصية والسرية منها، وهو ما يضيف حماية قانونية على التعامل الإلكتروني.
- الهوامش:**

- 1 - محمد خليفة الغفلي، حجية الدليل الرقمي في الإثبات الجنائي، رسالة دكتوراه، جامعة عين شمس، كلية الحقوق، سنة 2021، ص 71-72.
- 2 - رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، سنة 2018، ص 20.
- 3 - رشاد خالد عمر، المرجع السابق، ص 22.
- 4 - محمد خليفة الغفلي، المرجع السابق، ص 75.
- 5 - رشاد خالد عمر، المرجع السابق، ص 22.
- 6 - محمد خليفة الغفلي، المرجع السابق، ص 77.
- 7 - رشاد خالد عمر، المرجع السابق، ص 29.
- 8 - مروء زين العابدين سعد صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، سنة 2014، ص 411.
- 9 - محمد خليفة الغفلي، المرجع السابق، ص 86.
- 10 - رشاد خالد عمر، المرجع السابق، ص 27.
- 11 - قانون رقم 04-15 الصادر في 10.11.2004، المعدل والمتمم لقانون العقوبات، جريدة رسمية لعدد 71 لسنة 2004.
- 12 - قانون رقم 18-07 الصادر بتاريخ 10.07.2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34 لسنة 2018.
- 13 - راجع المادة 19 من القانون 18-07 السالف الذكر.

- 14 - فلاح ساهي خلف حسين، الحماية المدنية للبيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي (دراسة مقارنة)، دار وليد، القاهرة، سنة 2022، ص 65.
- 15 - فلاح ساهي خلف حسين، المرجع السابق، ص 70.
- 16 - سوزان عدنان، انتهاك حرمة الحياة الخاصة عبر الانترنت (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد 3، سنة 2013، ص 35.
- 17 - فلاح ساهي حسين، المرجع السابق، ص 93.
- 18 - المرجع نفسه، ص ص 92-93.
- 19 - قانون رقم 09-04 الصادر بتاريخ 05.08.2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصالات ومكافحتها، جريدة رسمية العدد 47 لسنة 2009.
- 20 - قانون رقم 15-04، الصادر بتاريخ 10 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، جريدة رسمية عدد 06 لسنة 2015.
- 21 - قانون رقم 18-05، الصادر بتاريخ 16.05.2018، المتعلق بالتجارة الالكترونية، جريدة رسمية عدد 28 لسنة 2018.
- 22 - فلاح ساهي حسين، المرجع السابق، ص ص 95-96.
- 23 - مشتة نسرين، بن عبید إخلاص، الحماية القانونية للمعطيات الشخصية في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، كلية الحقوق، جامعة أحمد بن يحيى الونشريسي تيسمسيلت المجلد 06، العدد 01، سنة 2021، ص 682.
- 24 - مروءة زين العابدين سعد صالح، المرجع السابق، ص 418.
- 25 - قانون رقم 16-01 الصادر بتاريخ 06.03.2016، المتضمن التعديل الدستوري جريدة رسمية عدد 14 لسنة 2016.
- 26 - المرسوم الرئاسي رقم 20-442 المؤرخ في 30.12.2020 المتضمن التعديل الدستوري جريدة رسمية عدد 82 لسنة 2020.

