الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري

مفيدة مباركية طالبة دكتوراه علوم

mebmoufida@yahoo.fr

كلية الشريعة والاقتصاد

جامعة الأمير عبد القادر للعلوم ٱسلامية–قسنطينة.

تاريخ الإيداع	تاريخ القبول	تاريخ النشر
20 ديسمبر 2017	30 أفريل 2018	14 جوان 2018

الملخص:

على غرار مختلف التشريعات في العالم وفضلا عن الاعتراف بالحق في الخصوصية وتكريسه كحق أصيل في الدستور، كفل المشرع الجزائري لهذا الحق الحماية الجنائية بشقيها الموضوعي والإجرائي. إلا أنه وفي ظل الانتشار الواسع لاستخدامات المعلوماتية والطبيعة المفتوحة للإنترنت فقد أخذ مفهوم الخصوصية أبعادا جديدة، واستحدث ما يسمى بالخصوصية الرقمية، للتعبير عن الخصوصية عبر الأنظمة المعلوماتية والانترنت كنطاق جديد للخصوصية، الأمر الذي يدفعنا إلى التساؤل عن جدوى سحب النصوص العامة المتعلقة بحماية الحق في الخصوصية وتطبيقها على الخصوصية الرقمية، أم أن هذا المفهوم المستحدث يحتاج إلى خلق نصوص جديدة تتناسب معه.

في هذا السياق، تأتي هذه الورقة لتبحث في الحماية الجنائية التي يقدمها المشرع الجزائري لهذا النوع المستحدث من الخصوصية.

الكلمات المفتاحية: الخصوصية الرقمية، خصوصية المعلومات، حماية البيانات الشخصية، خصوصية الأنظمة المعلوماتية، خصوصية المراسلات والاتصالات، خصوصية وسائل التواصل الاجتماعي، القانون الجنائي الجزائري.

Penal protection of the right to digital privacy in Algerian low

Abstract:

Similar to various laws around the world, the Algerian legislator and, in addition to recognizing the right to privacy, and including it as an inherent right in the Constitution, he has guaranteed protection to this right through both criminal and procedural codes. However, with the widespread use of computers, and the open nature of the Internet, the concept of privacy has taken a new dimension, expressed through confidentiality through information systems and the Internet as a new entourage of private life .So, the jurists wonder about the usefulness of removing the general provisions on the protection of the right to privacy and apply it to the digital privacy, or that we must create new texts who agree this new concept.

Keywords: Digital privacy, Information Privacy, Protection of personal data, Cyber privacy, Communications privacy, Social media privacy, Algerian criminal law.

مقدمة

يعتبر الحق في الخصوصية كما يعبر عنه في النظام الأنجلوكسوني أو ما يعرف بحرمة الحياة الخاصة في النظام اللاتيني، من الحقوق الأصيلة التي كرستها مختلف الشرائع والأنظمة عبر الأزمنة. وبظهور الانترنت والمعلوماتية بشتى استخداماتها، استحدث مفهوم الحق في الخصوصية الرقمية أواخر الستينيات من القرن الماضي للتعبير عن الخصوصية في ظل هذه التقنية الحديثة. وازدادت المخاوف حيال خصوصية المستخدمين عقب كشف إدوارد سنودن العام 2013 عن برنامج تجسس أطلقته وكالة الأمن القومي على شركات الانترنت بتفويض من جورج بوش، بعد هجمات الحادي عشر سبتمبر.

وبالرغم من أن الخصوصية الرقمية هي نوع من الخصوصية المعروفة سابقا، إلا أنها ترتبط بالعديد من المفاهيم المستحدثة الأخرى كالبيانات الشخصية والأنظمة المعلوماتية وخدمات الانترنت، وتثير الكثير

من الإشكالات، خاصة ما تعلق منها بالطبيعة العلنية للإنترنت، وتعارض الحق في الخصوصية مع الحق في التعبير والوصول إلى المعلومة، كذلك ما تعلق بملكية البيانات والمحتويات الشخصية التي ينشرها المستخدمون عبر وسائل التواصل الاجتماعي، وبالتالي المسؤولية القانونية للمستخدم حيال خصوصيته. وغيرها من الأمور التي تدفعنا للتساؤل عن جدوى حماية هذا النوع من الخصوصية بتطبيق النصوص التقليدية ذاتها المتعلقة بحماية الخصوصية، أم أنها تحتاج إلى صياغة نصوص جديدة تتلاءم وهذا النوع من الخصوصية.

لذلك فإن السؤال الذي أطرحه هو: *ما موقف المشرع الجزائري اتجاه الحق في الخصوصية الرقمية؟ وما مدى ملائمة ونجاعة القانون الجنائي الجزائري بشقيه الموضوعي والإجرائي في حمايته؟*

وهو ما أسعى للإجابة عنه في هذه الورقة التي وسمتها ب:"الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري". وذلك من خلال المطالب التالية:

المطلب الأول: مفهوم الحق في الخصوصية الرقمية

المطلب الثاني: الحماية الموضوعية للحق في الخصوصية الرقمية

المطلب الثالث: الحماية الإجرائية للحق في الخصوصية الرقمية

المطلب الأول: مفهوم الحق في الخصوصية الرقمية

الحق في الخصوصية [1] الرقمية مفهوم يقترن بالمعلوماتية ومختلف استخداماتها. وكون هذه الأخيرة اليوم تحتل جانبا هاما من الحياة الخاصة للأفراد فقد طفا هذا المفهوم على السطح منذ الستينيات من القرن الماضي.

([1]) – ورد تعبير "الحق في الخصوصية"،" the right to privacy" لأول مرة في مقال نشر عام 1890 لبرنديسووارن Brandies/Warren في مجلة هارفرد الحقوقية في الولايات المتحدة الأمريكية. وهو مفهوم يرتبط بكيان الانسان أو بحيزه الخاص الذي يسعى من خلاله إلى حماية مشاعره وأفكاره وأسراره الخاصة تجسيدا لكينونته الفردية.

وسيم شفيق الحجار: **النظام القانوني لوسائل التواصل الاجتماعي**، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط1، بيروت، 2017، ص37. كتاب متاح على الرابط:

https://carjj.org/sites/default/files/ebooks/social_media_book-finalforprint.pdf

الفرع الأول: تعريف الحق في الخصوصية الرقمية

من الأوائل الذين كتبوا في موضوع الخصوصية في ظل استخدامات المعلوماتية نجد الفقيه آلانواستن AlenWsten في العام 1967، الذي عبر عنه بـ "خصوصية المعلومات "وعرفه بأنه: "حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنه للآخرين"[1]. فهي شكل مستحدث للخصوصية لها علاقة مباشرة بالمعلومات، لأن جانبا مهما من المعلومات الحساسة والخاصة بالأفراد قد أضحى اليوم متاحا عبر الأنظمة المعلوماتية والانترنت خاصة، بحيث يصعب تعقبه أو استرجاعه أو جعله قابلا للنسيان. لذلك فإن الفقيه ميلرMiller يعرفها بأنها "قدرة الأفراد على التحكم بدورة المعلومات المتعلقة بهم[2]. أي تمكين المستخدمين وحدهم من منع الآخرين أو السماح لهم بالاطلاع على أو التصرف في المعلومات المتعلقة بحياتهم الخاصة.

ويظهر بهذا أن مفهوم الحق في الخصوصية الرقمية هو امتداد لمفهوم الحق في الخصوصية عموما، إلا أنه يختلف عن الأخير بكونه يتصل على وجه التحديد بالمعلومات الخاصة وبمدى قدرة الأفراد على التحكم في تدفقها عبر تكنولوجيات الاعلام والاتصال.

الفرع الثاني: محل الحق في الخصوصية الرقمية

كشفت دراسة صادرة عنلجنة التجارة الفيديرالية (FTC) [3] عام 1999 أن 92.8 % من مواقع الويب كانت جمعت على الأقل نوعا واحدا من بيانات الهوية (identifying information)، على غرار الاسم، العنوان البريدي، عنوان البريد الالكتروني[4]. وغيرها من

([1]) –توبي مندل وآخرون: **دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير**، الأمم المتحدة، منشورات اليونسكو، فرنسا، 2013، ص13.مقال متاح على الرابط:
http://unesdoc.unesco.org/images/0021/002182/218273A.pdf

([2]) – المرجع نفسه، ص13

([3]) – Federal Trade Commission

([4]) – Winnie Chung and John Paynter: **Privacy Issues on the Internet**, Department of Management Science and Information Systems, School of Business, The University of Auckland, Private Bag 92019, Auckland, New Zealand. Proceedings of the 35th Hawaii International Conference on System Sciences – 2002. IEEE.

المعلومات ذات الطبيعة الخاصة والشخصية المتداولة عبر الانترنت، والممثلة تمثيلا رقميا، تسمى بالبيانات الشخصية. لذلك فإن هذه الأخيرة تعتبر المحل الذي ينصب عليه موضوع الحق في الخصوصية الرقمية.

أولاً: تعريف البيانات الشخصية

البيان يجد مرادفه في اللغة الانجليزية Data وفي اللغة الفرنسية Donnée، ويقصد به من الناحية الفنية، كل تمثيل يمكن أن تخزن فيه المعلومة، يمكن أن يكون نصا أو جدولا أو رسما بيانيا، كما يمكن أن يكون منديلا أو لونا أو إشارة أو أية رموز أخرى، تكون ذات دلالة ومعنى لدى معالج المعلومة[1].

وتقوم مختلف الأنظمة المعلوماتية اليوم في أدائها على تمثيل البيانات تمثيلا رقميا، باستعمال الرقمين 0 و1 فقط.

ومن الناحية القانونية –وغير بعيد عن هذا المعنى–فقد أورد المشرع الجزائري تعريفا للبيانات الرقمية، حيث عبر عنها بـ "*المعطيات المعلوماتية*" وعرفها بأنها:" أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها" [2].

أما البيانات الشخصية فلم يورد لها تعريفا خاصا بها. وهي بحسب اللجنة الوطنية للمعلوماتية والحريات (CNIL) [3]:" كل معلومة تتعلق بشخص طبيعي معروف الهوية أو ممكن التعرف على هويته بصفة مباشرة أو غير مباشرة بالرجوع إلى رقم تعريفي أو إلى واحد أو مجموعة من العناصر التي تخصه..." [4].

([1]) –كيث دفلين، **الإنسان والمعرفة في عصر المعلومات**، ترجمة: شادن اليافي، مكتبة العبيكان، السعودية، ط: 1، 2001م، بتصرف

([2]) – القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 5 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية/ العدد 47.

([3]) Commission Nationale de l'Informatique et Libérés –

([4]) –المادة الثانية من قانون 6 جانفي 1978 المتعلق بالمعلوماتية، الملفات والحريات.

Loi nº 78-17 du 6 janvier 1978, modifiée le 6 août 2004

أو كما تعرفها اتفاقية 108 [1] "كل معلومة تتعلق بتحديد هوية الفرد، أو بفرد محدد".

ثانياً: أنواع البيانات الشخصية

من خلال التعريفات السابقة يتضح أن البيانات الشخصية تنقسم إلى نوعين أساسيين هما: البيانات المحددة للهوية والبيانات الخاصة.

1. البيانات الشخصية المحددة للهوية

بالنظر إلى الوسائل والتقنيات المعلوماتية المتعلقة بتحديد هوية الأشخاص، نجد أن البيانات المحددة للهوية تنقسم إلى نوعين من البيانات. يتمثل النوع الأول في الحروف والأرقام والرموز. والتي تتمثل أهمها فيكلمات المرور التي تسمح أو تمنع المستخدم من الولوج إلى الحاسوب الشخصي أو قاعدة البيانات أين يعمل أو الولوج إلى البريد الالكتروني أو البيانات التي يقتضيها اتمام معاملة من معاملات التجارة الالكترونية. أو تسجيل الدخول إلى منتدى أو حساب شخصي على موقع الكتروني.فيما يتمثل النوع الثاني في القياسات الحيوية، على غرار بصمة الإصبع، بصمة القزحية، البصمة الصوتية، بصمة أبعاد الكف، خط اليد (التوقيع)، بصمة الوجه... إلخ [2].

2. البيانات الشخصية الخاصة

يتعلق هذا النوع من البيانات بالحياة الخاصة للأفراد وتشمل كل البيانات التي من شأنها الكشف عن الأصل العرقي أو الآراء السياسية أو المعتقدات الدينية أو غيرها، وكذلك البيانات الشخصية المتعلقة

---

https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive-annotee.pdf

خالد ممدوح إبراهيم: **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص50.

([1]) –المادة الثانية من **الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية (108)**، المجلس الأوربي ستراسبورغ 1981.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

([2]) – منصور بن محمد الغامدي: **البيانات الحيوية، البصمة الصوتية**، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، ط1، 2005، ص 06.

بالصحة أو الحياة الجنسية، أو السوابق العدلية [1] المخزنة لدى المؤسسات العامة والخاصة في شكل قواعد بيانات، أو في خوادم الشبكات المعلوماتية [2]. وتعتبر قواعد البيانات لمختلف المنظمات مصدرا هاما لهذا النوع من البيانات، كذلك المواد الإعلامية المنشورة على صفحات شبكات التواصل الاجتماعي، والبيانات التي تقوم وكالات التحقيق والاستخبارات بتقصيها وجمعها.

الفرع الثالث: نطاق الحق في الخصوصية الرقمية

إذا كانت البيانات الشخصية هي المحل الذي ينشأ حوله الحق في الخصوصية الرقمية باعتبارها مصدرا للمعلومات الخاصة، فإن نطاق هذا الحق واسع ومتعدد باعتبار البيانات الشخصية تتواجد في أكثر من نطاق عبر مختلف الأنظمة المعلوماتية. وبالنظر إلى استخدامات الأنظمة المعلوماتية المتاحة اليوم، يمكن القول إن الحق في الخصوصية الرقمية يتعلق على وجه الخصوص بالبيانات الشخصية المخزنة في قواعد البيانات والأنظمة المعلوماتية للمؤسسات والإدارات كالملفات الطبية والقضايا المسجلة في المحاكم، وقوائم العمال والموظفين. كما يتعلق الحق في الخصوصية الرقمية بالاتصالات والمراسلات عبر الشبكات والانترنت.

كما تظهر الكثير من سمات الانترنت أنه من الصعب أن يتحكم المستخدم في بياناته الشخصية، لذلك فقد أدى التوتر بين الحقوق والقدرة الفعلية لمستخدمي الانترنت على التحكم في بياناتهم الشخصية إلى الكثير من الجدل حول الخصوصية على الانترنت. ويركز هذا الجدل في العادة على عدم قدرة المستخدم على التحكم وتمكينه من أن يقرر كيفية استخدام بياناته، مع التركيز على دور المؤسسات في مراقبة وإدارة البيانات الشخصية. فضلا عن ذلك دائما تكون سيطرة الجهات الخاصة في مقارنة سيطرة الجهات العامة والتي تعتبر غير قادرة أو غير راغبة في تنفيذ الحماية الفعلية لبيانات المستخدمين الشخصية [3].

([1]) –المادة السادسة من **الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية (108)**، المرجع السابق.

([2]) –إيان ليه: **الإشراف على استخدام البيانات الشخصية**، مقال متاح على الرابط:
www.dcaf.ch/content/download/…/1/…/Tool_6_intel_over_AR.pdf

([3]) –توبي مندل وآخرون: المرجع السابق، ص19.

أولاً: الأنظمة المعلوماتية

يعرف النظام من الناحية التقنية بأنه مجموعة من الأجزاء المترابطة فيما بينها بحيث ينتظر منها أداء سلوك يمكن مشاهدته على الواجهة مع بيئته[1].

ومن الناحية البنيوية، فإن النظام يتكون من مجموعة من المكونات المترابطة بحيث يمكنها التفاعل فيما بينها. كل مكون هو نظام آخر قائم بذاته [2].

وانطلاقا من التعريف التقني أمكن لرجال القانون اعتماد التعريف القانوني للنظام المعلوماتي، حيث جاء في المادة الأولى من اتفاقية بودابست حول الجريمة السيبيرانية: "النظام المعلوماتي يعني أي جهاز أو مجموعة من الأجهزة المتصلة أو المترابطة بحيث واحد من بينها أو أكثر يقوم بالمعالجة الآلية للبيانات وفقا لبرنامج"[3].

أما المشرع الجزائري فقد عبر عنه ب: "المنظومة المعلوماتية" وعرفه بأنه أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[4].

ويعد جهاز الحاسوب بمختلف أشكاله أهم الأنظمة المعلوماتية، بالإضافة إلى الألواح والهواتف الذكية، والصراف الآلي، والأنظمة المدمجة، وغيرها. هذه الأجهزة يمكن أن تكون مفصولة عن غيرها من الأجهزة والأنظمة، كما يمكن أن تكون موصولة بأنظمة معلوماتية أخرى لتشكل نظاما معلوماتيا أوسع يعرف بالشبكة المعلوماتية. هذه الأخيرة بدورها يمكن أن تكون منفصلة أو موصولة بغيرها من

([1]) –Jerome H. Saltzer& M. FransKaashoek: **Principles of Computer System Design**. Morgan Kaufmann Publishers - Elsevier-.USA.2009. p6

([2])– FernardLone Sang. **Protection des systemes informatiques contre les attaques par entrees– sorties**. Doctorat de l'Uinivercite de Toulouse. Directeurs de these : Yves Deswarte et Vincent Nicomette. 2012.p06

([3]) – **Convention On Cybercrime**. Budapest, 23.XI.2001. Article 1

([4]) –المادة الأولى من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 حول المساس بأنظمة المعالجة الآلية. الجريدة الرسمية للجمهورية الجزائرية، العدد 71. السنة الواحدة والأربعون.

الشبكات. لتشكل نظاما أكثر اتساعا، وهكذا إلى أن تكون منفصلة عن أو متصلة بشبكة الشبكات المعروفة بشبكة الانترنت والتي تعتبر أوسع الأنظمة المعلوماتية.

وتدخل الأنظمة المعلوماتية في نطاق الحق في الخصوصية الرقمية باعتبارها البيئة التي تولد فيها البيانات الشخصية وتعالج وتخزن ويتم تبادلها. يمكن لها اليوم أن تحتوي صور الأشخاص ومذكراتهم. كما تعتبر أهم وسيلة لإجراء الاتصالات الشخصية، والمحادثات السرية، والتقاط الصور الخاصة... وبظهور الحكومة الالكترونية، أصبح تسيير مختلف المؤسسات يتم عبر الأنظمة المعلوماتية، ما يتطلب تبني قواعد البيانات التي تحتوي على بيانات شخصية تعود لعمال أو موظفين أو تلاميذ، أو مرضى في المستشفيات، أو متابعين قضائيا في المحاكم. وهي كلها بيانات تستحق الحماية.

ثانياً: وسائل الاتصال الرقمية (البريد الالكتروني والسكايب)

يتم اليوم إجراء جانب كبير من الاتصالات والمراسلات عبر الخدمات التي تتيحهما تكنولوجيات الاعلام والاتصال. أهمها: البريد الالكتروني والسكايب.

أما البريد الالكتروني فهو عبارة عن رسالة يتم إرسالها من نظام معلوماتي (حاسوب شخصي، هاتف ذكي...) نحو آخر عبر شبكة الانترنت. ولتتم العملية لا بد من تحقق أمرين: الأول أن يكون كلا من جهاز المرسل والمرسل إليه موصولا بالإنترنت، والأمر الآخر هو وجود العنوانين الالكترونيين للطرفين، تمنحهما إحدى الشركات التي تملك خوادم بريد. وهي عبارة عن أجهزة كمبيوتر خاصة تستطيع إيصال البريد الالكتروني إلى العنوان الصحيح [1].

وفيما تسمح خدمة البريد الالكتروني بتبادل الرسائل الالكترونية (النصية غالبا) عبر شبكة الانترنت، فإن خدمة السكايب وفضلا عن ذلك تتيح للمستخدمين إمكانية إجراء المحادثات المسموعة والمرئية بحيث يتم تبادل الصوت والصورة بين الطرفين عبر الانترنت. وهو ما قد يهدد الخصوصية باعتبار أن جوهرها يتمثل في "قدرة الأشخاص على التحكم في دورة المعلومات التي تتعلق بهم". الأمر الذي يصعب تحققه عبر وسائل الاتصالات وشبكة الانترنت، باعتبار وجود طرف ثالث يمكن من خلاله

(1) - http://www.halifaxpubliclibraries.ca/assets/files/handouts/Email.pdf

التعقب والاطلاع على المعلومات التي يرغب أصحابها في حجبها عن الغير. ذلك أن البيانات المتبادلة تمر عبر خوادم الانترنت قبل الوصول إلى المرسل أو المرسل إليه.

ثالثاً: وسائل التواصل الاجتماعي

وسائل التواصل الاجتماعي هي إحدى تطبيقات الويب، التي تسمح لكل شخص ليس فقط بالوصول إلى المحتوى على الانترنت، بل بتحرير المحتوى وبتحميله والتعليق عليه وتعديله [1].

ويرتكز تعريف وسائل التواصل الاجتماعي على ثلاثة عناصر: إنشاء سيرة ذاتية من قبل المستخدم، وجود أدوات تسمح بإنشاء لائحة المعارف والتفاعل معهم، تمكين المستخدم من وضع المحتوى الخاص به على الشبكة، وبتحديثه (نصوص، رسوم، صور، صوت، أغاني، أفلام...). وما ينشر قد يكون مفتوحا للعموم، أو خاصا أو مختلطا، وقد يكون مفتوحا لفئات مختلفة. وقد أثبتت الدراسات حول حسابات طلاب على موقع فيسبوك أن 88% يفشون كامل تاريخ ولادتهم وجنسيتهم لوسيلة التواصل الاجتماعي، وينشر أيضا 45.8% منهم عنوان سكنهم. وهذه المعلومات هي كافية لتحديد هوية الشخص. كما تمكن طلاب من جامعة أم أي تي MIT من الوصول إلى 70 ألف سيرة على موقع الفيسبوك من خلال برنامج ابتكروه. وبالتالي، فمن المنطقي القول إنه من غير الصعب على فنيين محترفين تجاوز إعدادات الخصوصية لموقع فيسبوك [2].

رابعاً: محركات البحث

تقوم محركات البحث على غرار Google في العادة بجمع قدر هائل من البيانات الشخصية بما في ذلك عناوين بروتوكولات الانترنت IP وطلبات البحث والوقت والتاريخ والمكان الذي قدم فيه جهاز الكمبيوتر الطلب. يمكن أن تكون المعلومات قابلة لتحديد الهوية الشخصية ويمكن أن تكشف عن أجزاء حساسة من المعلومات مثل المعتقدات السياسية للشخص أو ميوله الجنسي أو معتقداته الدينية أو المسائل الطبية[3].وفي هذا الخصوص قضت محكمة الدرجة الأولى في باريس بتاريخ

([1]) – وسيم شفيق الحجار: المرجع السابق، ص15.

([2]) –المرجع نفسه، ص49.

([3]) – توبي مندل وآخرون: المرجع السابق، ص32

2013/11/6 بإلزام غوغل، بالاستناد إلى الحق في حرمة الحياة الخاصة، بوقف عرض صور تكشف الحياة الجنسية لأحد الأشخاص [1].

وبالانتشار المتزايد للمعاملات التجارية الالكترونية، تقوم معظم الشركات بجمع البيانات الشخصية عبر مواقعها على شبكة الانترنت. وكما هو موضح في الجدول (1)، فإنها لا تصرح دائما عن الأغراض من تجميع البيانات الشخصية، كما أنها لا تلتزم بإشعار المستخدمين بالتجميع عن طريق بيان سياسة الخصوصية التي يفترض أن يتبناها الموقع.

القطاع	عدد المواقع الالكترونية	البيانات الشخصية المجمعة	الاشعاربغرض التجميع	الاشعارعن طريق بيان الخصوصية
البنوك	9	%100	%44	%33
السفر	7	%57	%25	%25
السيارات	14	%50	%14	%14
بيع التجزئة	13	%100	%69	%62
الرياضة	15	%33	%40	%20
الموضة	5	%80	%0	%0
الزراعة	11	%55	%67	%83
مجالات أخرى	48	%63	%50	%47

الجدول(1): تجميع البيانات الشخصية عبر مختلف المواقع الالكترونية[2]

بالإضافة إلى ذلك، تقوم الحكومات بالتجسس الرقمي اتجاه الأفراد برصد أداء الأشخاص وتفاعلاتهم اليومية عبر الانترنت، وقد يتوسع هذا التجسس ليطال مواطني دول أخرى. ومن الأمثلة الفعلية على ذلك التفويض الذي أعطاه الرئيس الأمريكي الأسبق جورج بوش إلى وكالة الأمن القومي بعد هجمات الحادي عشر من سبتمبر لتطوير آليات للتجسس، وإطلاق برنامج الرقابة

(1) –وسيم شفيق الحجار: المرجع السابق، ص 32، 43.

(2) – المرجع السابق :Winnie Chung and John Paynter

PRISM[1] الذي يستهدف جميع بيانات مستخدمي خدمات الانترنت لشركات PalTalk,AOL,Yahoo, Microsoft, Appele, Google في جميع أنحاء العالم[2].

خامساً: الحوسبة السحابية

الحوسبة السحابية عبارة عن هيكل شبكات ناشئ يتم من خلاله تخزين البيانات أو طاقة المعالجة أو البرامج في أجهزة خادم عن بعد، على خلاف الأجهزة الشخصية. وتكون متاحة من خلال الانترنت. تتوفر أشكال مختلفة من الحوسبة السحابية وتوفر مجموعة كبيرة من الخدمات ويمكن للأفراد أو المنظمات تأجير القدرة الحاسوبية بشكل فعال من مزودي الخدمة عن بعد. فمثلا تسمح خدمة تطبيقات جوجل (Google's Apps) للأفراد بإنشاء وحفظ مستندات معالجة spreadsheet وword على الانترنت وتشتمل بعض الخدمات الأخرى على منصات تعاونية تسمح للمستخدمين بحرية الوصول إلى المستندات بشكل فوري مثل منصات wiki ومستندات Google docs.

وتثير الحوسبة السحابية كذلك العديد من المخاوف من منظور الخصوصية. حيث يتم تخزين البيانات في جهاز طرف ثالث يتحمل المسؤولية عن حمايتها ويفقد المستخدم قدرته على التحكم فيها. يضاف إلى ذلك أن القوانين التي تغطي الحوسبة السحابية غير محددة بما يكفي فليس هناك ما يضمن خصوصية بيانات المستخدمين[3].

المطلب الثاني: الحماية الموضوعية للحق في الخصوصية الرقمية في القانون الجزائري

بعد بيان مفهوم الحق في الخصوصية الرقمية، نركز في هذا الجزء من البحث على استقصاء الحماية الجنائية للحق في الخصوصية الرقمية في قانون العقوبات الجزائري. وتحديدا الخصوصية عبر الأنظمة المعلوماتية، والخصوصية عبر وسائل الاتصال والمراسلات، ومواقع التواصل الاجتماعي.

---

(1) –كشف عنه إدوارد سنودن، فني سابق بوكالة الاستخبارات الأمريكية لصحيفة الجارديان في يونيو 2013.

كريم عاطف: **الخصوصية الرقمية بين الانتهاك والغياب التشريعي**، مركز دعم لتقنيات المعلومات، القاهرة. مقال متاح على الرابط:info@sitcegypt.org

(2) –المرجع نفسه.

(3) –كريم عاطف المرجع السابق.

الفرع الأول: الحماية الموضوعية لخصوصية الأنظمة المعلوماتية

عبر المشرع الجزائري عن الأنظمة المعلوماتية ب"منظومة للمعالجة الآلية للمعطيات". وعبر عن البيانات الرقمية ب" المعطيات"، كما التفت إلى الحماية الجنائية للبيانات بصفة عامة، دون تحديد للبيانات الشخصية، أو إفرادها بنصوص خاصة. حيث جرم جملة من الأفعال الموصوفة في المواد من 394مكرر إلى 394 مكرر7 من قانون العقوبات[1]، منها ما تعلق بسلامة الأنظمة والبيانات، ومنها ما تعلق بإتاحة الأنظمة والبيانات، فيما يتعلق جانب منها بخصوصية الأنظمة وسرية البيانات وهو ما يعنينا في هذا المقام.

أولاً: تجريم الولوج إلى أو البقاء غير المصرح بهما في نظام معلوماتي

يعتبر الولوج غير المصرح به إلى النظام المعلوماتي أحد أهم الجرائم الماسة بالحق في الخصوصية. إذ أضحت الحواسيب الشخصية للأفراد تحتل جانبا كبيرا من حياتهم الخاصة. لذلك فإن الولوج غير المصرح به إلى الأنظمة المعلوماتية يشكل جريمة في معظم التشريعات الحديثة، بما فيها التشريع الجزائري الذي ينص في المادة 394مكررمن قانون العقوبات [2] على أنه: "يعاقب بالحبس من ثلاثة أشهر إلى سنة، وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

من خلال النص يتضح أن الركن المادي للجريمة يكون إما بالولوج إلى النظام المعلوماتي وإما بالبقاء فيه.

1. الولوج غير المصرح به إلى نظام معلوماتي

يمكن تعريف الولوج غير المصرح به إلى نظام معلوماتي بأنه أي نشاط يقوم به الشخص عمدا، وبدون رضى صاحب النظام، يجعله في حالة تسمح له بالاتصال الحسي مع النظام أو بالتحكم في نظام التشغيل ولو جزئيا. يمكن أن يكون فعل الولوج غير المصرح به بسيطا وبالاتصال الحسي المباشر مع النظام. إلا أنه في الكثير من الحالات يتم عن بعد وباستخدام أساليب وتقنيات القرصنة المعقدة.

([1]) – القانون رقم 04-15، المرجع السابق.

([2]) – المرجع نفسه.

ولاكتمال الركن المادي اشترط المشرع أن يتم الفعل بطريق الغش وهو ما يمكن أن يعبر عن أحد أمرين: الأمر الأول هو عدم رضا صاحب النظام بفعل الولوج. والأمر الآخر هو اللجوء إلى استخدام تقنيات وأساليب فنية لاقتحام النظام. وهو ما يتصور في حال كون النظام مؤمنا بالأدوات اللازمة على غرار كلمة السر والجدران النارية وغيرها من أنظمة الحماية ضد البرمجيات الخبيثة التي تستعمل في التجسس والتحكم في عمل النظام، فضلا عن اقتحامه.

وفي اشتراط كون النظام المعلوماتي مؤمنا حتى يتمتع بالحماية ينقسم الفقه إلى رأيين[1]: الرأي الأوليرى عدم اشتراط انتهاك نظام الحماية الفنية لتجريم فعل الولوج غير المشروع، بحجة أن التمسك بهذا الشرط يؤدي إلى قصر نطاق الحماية الجنائية على الأنظمة المعلوماتية المحمية فقط. ما يعني زيادة حالات الإفلات من العقاب. فيما يرى جانب آخر من الفقه ضرورة وجود نظام أمان، استنادا إلى أن المنطق والعدالة يستلزمان ذلك. فالقانون الجنائي –بحسب هؤلاء–لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم والمتطلب من انسان متوسط الذكاء.

أما المشرع الجزائري فواضح من خلال نص المادة أعلاه أنه لا يشترط وجود هذه الحماية الفنية حتى يتمتع النظام المعلوماتي بالحماية الجنائية. وهو ما يمكن الاستدلال عليه بكون المشرع جرم فعل البقاء داخل النظام، وهو ما يتصور حدوثه في حالة الولوج بطريق الخطأ، أي دون أدنى صعوبة، ثم التمادي بالبقاء بعد التفطن لذلك. فكون النظام غير مؤمن بكلمة المرور مثلا يجعل من الولوج إليه أمرا غاية في البساطة، لكن في حال حدوث ذلك خطأ، فإن الفاعل مسؤول جنائيا عن البقاء غير المصرح به.

([1]) – دلخار صالح بوتاني: **الحماية الجنائية الموضوعية للمعلوماتية**، دار الفكر الجامعي، الإسكندرية، ص1، 2015، ص200.

عبد العال الديربي، محمد صادق إسماعيل: **الجرائم الالكترونية**، المركز القومي للإصدارات القانونية، القاهرة، ص1، 2012، ص189.

2. البقاء غير المصرح به في نظام معلوماتي

يلحق المشرع الجزائري بفعل الولوج غير المصرح به، فعل البقاء غير المصرح به. ويقصد به التواجد داخل النظام المعلوماتي ضد إرادة من له الحق في السيطرة على هذا النظام[1]. ويتصور وقوع هذا الفعل في إحدى حالتين[2]:

الحالة الأولى: تتحقق إذا تم الدخول إلى النظام عن غير قصد كالخطأ أو السهو، أي بدون قصد جنائي، ولكنه وبعد تفطنه للأمر يختار البقاء في النظام، أي بعد تكون العلم والإرادة اللازمين لتشكل القصد الجنائي.

الحالة الثانية: تتحقق إذا تم الدخول بتصريح من صاحب الحق على النظام، ولكن بتصريح مشروط بمدة محددة أو بجزء محدد من النظام، فيتجاوز الحدود المسموح بها من خلال التصريح. وهذه الحالة توافق ما ينص عليها المشرع الأمريكي صراحة في القانون الفيديرالي[3]CFAA.

أما بالنسبة للركن المعنوي: فالجريمة تعتبر تامة ومرتبة للجزاء متى توفر القصد العام أي اتجاه إرادة الفاعل نحو إتيان السلوك مع العلم بنتيجة هذا السلوك، وهو التواجد داخل نظام معلوماتي دون إذن صاحبه. وبغض النظر عن البواعث والنوايا. فإن الجريمة تعتبر تامة وإن كان الغرض منها هو التعلم والفضول العلمي البحت.

وبهذا فإن جريمة الولوج غير المشروع في القانون الجزائري هي من الجرائم الشكلية، حيث يشكل فعل الولوج المجرد دون تصريح من صاحب النظام جريمة ولو لم ينتج عنه أي ضرر مادي أو معنوي

([1]) – محمود أحمد طه: **المواجهة التشريعية لجرائم الكمبيوتر والانترنت**، دار الفكر والقانون، المنصورة، ط1، 2017، ص30.

([2]) – المرجع نفسه ص31.

مدحت محمد عبد العزيز إبراهيم: **الجرائم المعلوماتية الواقعة ضد النظام المعلوماتي**، دار النهضة العربية، القاهرة، ط1، 2015، ص84

([3]) – Computed Fraud and Abuse Act. صدر عن الكونغرس لأول مرة عام 1986 وتم تنقيحه عدة مرات على مدى العقود الثلاثة التالية. كان الهدف الأساسي من هذا القانون هو حماية الأنظمة المعلوماتية التي تعود إلى إحدى الفئات التالية: الكيانات الاتحادية، المؤسسات المالية، ومؤسسات التجارة الداخلية والخارجية. تعدل القانون أربع مرات في: 1986، 1994، 1996، و2001.

ملموس[1]. لكن الجزاء يضاعف في حال احداث ضرر بالحذف أو التغيير[2]. أما الضرر الناتج عن الحيازة أو الافشاء فقد اعتبرها جريمة مستقلة.

ثانياً: تجريم ادخال معطيات إلى النظام المعلوماتي أو إزالتها أو تعديلها

تنص المادة 394 مكرر1: " يعاقب بالحبس من ستة (6) أشهر وثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

ما يعنينا في هذا المقام هو المساس بحرمة الحياة الخاصة. والمشرع أطلق لفظ المعطيات ولم يقيده بصنف معين. والمعطيات من الناحية الفنية وحتى القانونية لفظ يتسع ليشمل جملة من الأصناف. فهي يمكن أن تكون برامج خبيثة (فيروسات) يقوم الفاعل بإدخالها إلى النظام بهدف التجسس وجمع البيانات الخاصة. كما يمكن أن تكون غير ذلك. يمكن مثلا أن تكون مواد إباحية يتعارض وجودها داخل النظام مع إرادة مالكه أو المسؤول عنه، يكون القصد من إدخالها هو الازعاج أو احداث أي ضرر معنوي آخر. ولا شك في أن هذا يتعارض وحرمة الحياة الخاصة.

كذلك هو الشأن مع أفعال تعديل البيانات الشخصية المخزنة داخل النظام أو إزالتها دون علم صاحبه. والواقع يثبت –من الناحية النظرية على الأقل–أن فعل التعديل يمكن أن يمس بالحق في الخصوصية. يتصور هذا مثلا في حال تعديل أو حذف يتم في قاعدة بيانات تخص موظفين أو مرضى أو أي فئة أخرى من الأشخاص.

فكل من أفعال الإدخال والتعديل والإزالة هي جريمة شكلية، وتعتبر تامة بغض النظر عن حدوث ضرر من عدمه، وبغض النظر عن البواعث وحجم الضرر الناتج، ويعاقب عليها المشرع بالعقوبة نفسها، مهما كانت طبيعة البيانات والحقوق أو المصالح المستهدفة. والمشرع وإن لم يعبر صراحة عن

([1]) – مجرد الولوج غير المصرح به لا يشكل جريمة في القانون الأمريكي، إلا إذا حصل الفاعل بعد فعل الولوج على بيانات تتمتع بالحماية القانونية موجودة في النظام. المادة 1030 في الباب 18 من القانون الأمريكي المتعلق بالاحتيال وإساءة استخدام الحاسوبCFAA.

([2]) – الفقرة الثانية من المادة 394 مكرر نفسها.

المعطيات الشخصية فإن النص يستغرقها كونه عاما في حماية المعطيات، وكون المعطيات (البيانات) الشخصية صنفا من المعطيات.

ثالثاً: تجريم حيازة أو افشاء أو نشر أو استعمال البيانات الشخصية

تنص المادة 394 مكرر 2 في فقرتها الثانية على المعاقبة بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا وبطريق الغش ب: حيازة أو افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم.

وعلى غرار المادة السابقة فإن المشرع أطلق لفظ "المعطيات"، دون أن يخص المعطيات الشخصية بعبارة خاصة. لكن هذا لا يمنع من إمكانية سحب النص وتطبيقه لحماية البيانات الشخصية باعتبارها صنفا من البيانات. هذا إذا ما أخذنا بعين الاعتبار أن الولوج أو البقاء غير المصرح بهما في النظام المعلوماتي هو جريمة من الجرائم المنصوص عليها في هذا القسم، أي القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات. والتي يمكن أن ترتكب بهدف حيازة بيانات شخصية أو افشائها أو نشرها أو التصرف فيها بأي شكل آخر. كما أن هذه الجرائم شكلية وتعتبر تامة متى حصل الفعل ولا يشترط توافر قصد خاص مهما كان الباعث والغرض من حيازتها أو افشائها أو نشرها أو استعمالها بأي شكل آخر.

الفرع الثاني: الحماية الموضوعية لخصوصية الاتصالات والمراسلات والصور الشخصية

في الواقع يمكن لجملة من الأفعال المهددة للخصوصية أن ترتكب عبر خدمات التراسل والاتصالات التي تقدمها الانترنت. تتمثل هذه الأفعال أساسا في الاطلاع على محتوى الرسائل، والالتقاط (الاعتراض)، والتسجيل، والتجميع وغيرها من الأفعال التي يجرمها المشرع الجزائري في سياق حماية الحق في الخصوصية، بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006[1] المعدل والمتمم لقانون العقوبات.

([1]) – قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006. المعدل والمتمم لقانون العقوبات. الجريدة الرسمية للجمهورية الجزائرية/ العدد 84.

أولاً: تجريم فض واتلاف الرسائل والمراسلات

تنص المادة 303 من قانون العقوبات على أن:"كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر (1) إلى سنة (1) وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط." [1]

واضح من خلال النص أن التجريم عام ليستغرق كافة الرسائل والمراسلات، دون تقييد لشكل الرسائل والمراسلات. فهو لا يتعلق فقط بالورقية منها بل يشمل أيضا –بمفهوم العموم–رسائل البريد الالكتروني والرسائل الالكترونية المرسلة عبر السكايب أو أي تقنية اتصال أخرى. إلا أن السؤال المطروح الذي يمكن طرحه هنا يتعلق بأفعال القرصنة والاقتحام المرتكبة ضد البريد الالكتروني وحساب السكايب الشخصي، ومدى إمكانية اعتبارها من قبيل الفض المنصوص عليه في المادة 303.

ثانياً: تجريم التقاط وتسجيل ونقل بيانات شخصية

بالنظر إلى الإمكانات التقنية التي تسمح بتسجيل الصورة والحدث عبر كاميرات الهواتف الذكية والقدرة على نقلها مباشرة إلى جمهور غير محدود عبر الانترنت فإن موضوع الخصوصية يصبح مطروحا بإلحاح. وفي إطار حماية خصوصية الاتصالات والحق في خصوصية الصورة الملتقطة من مكان خاص، لأسباب غير مشروعة، تنص المادة 303مكرر[2] من قانون العقوبات على أنه:" يعاقب بالحبس من ستة أشهر (6) إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1. بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو سرية، بغير إذن صاحبها أو رضاه.
2. بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

([1]) – المرجع نفسه.

([2]) –القانون رقم 06-23، المرجع السابق.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة. ويضع صفح الضحية حدا للمتابعة الجزائية."

الشاهد هنا أن التجريم يقع مهما كانت الوسيلة أو التقنية المستخدمة في ارتكاب الفعل. وبالرغم من أن التقنيات المتاحة اليوم يمكن أن تسهل من ارتكاب هذه الأفعال. فجميع الحواسيب الشخصية والهواتف مجهزة بكاميرا ولواقط الصوت، إلا أن المشرع لم يشدد أو يخص الأفعال المرتكبة عبر هذه التقنيات الحديثة بنصوص خاصة.

ثالثاً: تجريم الاحتفاظ وإفشاء واستخدام بيانات شخصية

تنص المادة 303 مكرر1[1] من قانون العقوبات: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون. "

تستهدف الأفعال المجرمة في هذه المادة، التسجيلات (السمعية والسمعية البصرية)، والصور والوثائق، وغيرها من البيانات الشخصية المتحصل عليها جراء احدى الجرائم المنصوص عليها في المادة 303 مكرر (الالتقاط أو التسجيل أو النقل).

ويكتمل الركن المادي بإتيان أحد أفعال: الاحتفاظ، أو الوضع في متناول الجمهور، أو الغير، أو الامتناع عن منع وضعها في متناول الجمهور أو الغير، أو الاستخدام بأية وسيلة كانت.

وعلى غرار المادة303 مكرر السابقة، فالمشرع أطلق التجريم ولم يلتفت إلى الوسيلة المستخدمة في ارتكاب الجريمة. وبذلك فإن نشر البيانات الشخصية الذي يتم عبر المواقع الالكترونية والأنظمة المعلوماتية عموما أو استخدامها بأي وسيلة كانت يمثل جريمة تستغرقها المادة القانونية.

أما الركن المعنوي فيتمثل في توافر القصد الجنائي العام (العلم والإرادة)، ولم يشترط المشرع القصد الجنائي الخاص.

([1]) – المرجع نفسه.

الفرع الثالث: الحماية الموضوعية للحق في الخصوصية عبر مواقع التواصل الاجتماعي

إذا كان سحب قواعد الخصوصية على الأنظمة المعلوماتية ووسائل المراسلات والاتصالات ممكننا ومقبولا فإن سحبها على وسائل التواصل الاجتماعي يمكن أن يكون مع الكثير من التحفظ، نظرا لطبيعة هذه التكنولوجيا والاشكالات التي تثيرها. لذلك فإنني وقبل الخوض في موقف المشرع الجزائري اتجاه خصوصية مستخدمي وسائل التواصل الاجتماعي، أجد من المهم بيان الإشكالات المتعلقة بهذه الوسائل.

أولاً: اشكاليات الحماية الموضوعية للحق في الخصوصية عبر وسائل التواصل الاجتماعي

تختلف وسائل التواصل الاجتماعي عن وسائل الاتصال الأخرى (الهاتف والسكايب والبريد الالكتروني...). ويمكن القول إن موضوع الحماية القانونية للخصوصية عبر وسائل التواصل الاجتماعي لا يزال يثير الجدل، ولم يستقر الاجتهاد بعد حول العديد من المسائل في هذا الجانب. خاصة ما تعلق منها بملكية البيانات الشخصية المتداولة عبر هذه الوسائل، ومدى قدرة الأشخاص على التحكم في دورة ما ينشرونه من محتويات عبرها، كذلك مسألة تعارض الخصوصية عبر هذه الوسائل مع حرية التعبير والحق في التجمع والوصول إلى المعلومة. هذا بالإضافة إلى العنصر الدولي الذي تتسم به مواقع التواصل الاجتماعي وخدمات الانترنت عموما والعديد من المسائل الأخرى التي تدفعنا للتساؤل أولا عن مدى إمكانية تطبيق القواعد القانونية العامة المتعلقة بحماية الحق في الخصوصية، أم أن موضوع الخصوصية عبر وسائل التواصل الاجتماعي يحتاج إلى إيجاد القواعد الخاصة. ثم التساؤل عن جدوى وفاعلية هذه النصوص الخاصة، إذا ما نظرنا إلى الإشكالات التي تحول دون تطبيقها.

1. الملكية والقيمة التجارية للبيانات الشخصية المتداولة عبر مواقع التواصل الاجتماعي

خلافا للشعور العام لدى المستخدمين بمجانية وسائل التواصل الاجتماعي، فهي ليست منشأة على وجه مجاني، ولها هدف مادي هو الربح، وتدخل ضمن إطار اقتصاد الويب الاجتماعي الذي يستند على تمويل الخدمات المقدمة من خلال الإعلانات الموجهة، وبالتالي من خلال استثمار البيانات الشخصية للمستخدمين. عمالقة الانترنت المجانية كفيسبوك وغوغل، تحول البيانات الشخصية لمستخدميها إلى أموال، لاسيما ما تعلق بعاداتهم الاستهلاكية ومحور اهتماماتهم وبنمط حياتهم.

وتشكل القيمة الاجمالية للبيانات الشخصية للمواطنين الأوروبيين 330 مليار يورو في السنة من خلال الزيادة في الإنتاج والوصول إلى أسواق جديدة، وذلك وفق ما ورد في دراسة بوستن كونسلتينغ غروب Bosten consulting Group لعام 2012[1].

فوسائل التواصل الاجتماعي تعرض خدمات مبتكرة، مجانية بالعموم، لكن غالبا متاحة مقابل الاستخدام التجاري للبيانات الشخصية للمستخدمين. وقد اعتبرت محكمة التمييز الفرنسية أن تجميع البيانات الشخصية على الانترنت هو عمل غير مشروع. ويرى بالتالي البعض أنه قد يظن المستخدمون أنهم يملكون البيانات الشخصية العائدة لهم. وفي الحقيقة لا أحد يملك الحقائق. فحقائق المعلومات هي مستبعدة من نطاق الحماية بموجب قوانين الملكية الفكرية التي تحمي فقط الابتكار. أما القوانين المتعلقة بأسرار التجارة فهي تحمي المعلومات التي تبقيها الشركات سرية إذا كانت ذات قيمة اقتصادية. ولا تشكل البيانات الشخصية على مواقع التواصل الاجتماعي من هذا القبيل من المعلومات. وعندما تجمع شركات التواصل الاجتماعي معلومات حول ميول المستخدمين واستخدامهم للخدمات، لها وحدها حق المطالبة بملكية هذه الأسرار التجارية وليس المستخدمين. كذلك يمكن حماية قواعد البيانات ومحتواها من البيانات الشخصية بموجب القوانين الأوروبية المتعلقة بقواعد البيانات كونها عائدة لشركات التواصل الاجتماعي ولكن ليس كونها عائدة للمستخدمين. [2]

ومع أن مواقع التواصل الاجتماعي قد أقرت بحاجة المستخدمين لديها إلى الخصوصية ووضعت آليات لها، إلا أنها ومنذ البداية قد وضعت السياسات المطبقة لحماية صناعة وسائل التواصل الاجتماعي ولتأمين ازدهارها ومصالحها وليس لخصوصية الأفراد عليها، فإفشاء معلومات أكثر يؤمن مدخولا أكبر[3].

2. التعارض مع حرية التعبير والحق في الوصول إلى المعلومة

إن الحق في الخصوصية يتقاطع مع غيره من الحقوق والحريات التي تمارس على شبكة الانترنت، لذلك فقد أشار قرار الجمعية العامة للأمم المتحدة رقم 167/68 إلى هذا التقاطع وشدد على علاقة الحق

(1) – وسيم شفيق الحجار: المرجع السابق، ص68.

(2) – المرجع نفسه، ص66.

(3) – المرجع نفسه، ص53.

في الخصوصية مع ثلاثة حقوق على وجه الخصوص، وهي الحق في حرية التعبير، والحق في التجمع والحق في الوصول إلى المعلومات والعمل ضد الدعاية المروجة للجريمة والإرهاب[1].

وفي هذا الخصوص، اعتبرت محكمة الدرجة الأولى في باريس في قرارها تاريخ 2013/11/13 أن حق الشخص باحترام حياته الخاصة قد ينحصر امام متطلبات حرية التعبير عن الرأي، ويتم تقدير ذلك في ضوء مجموعة من الظروف تتعلق بالضحية وبصفتها وبتصرفها السابق وبموضوع النشر وبمحتواه وبشكله وكذلك في ضوء سوء النية ومدى التعرض لكرامة الشخص والمشاركة في نقاش ذات اهتمام عام. وتعمد المحاكم إلى موازنة الحقوق المتعلقة بالخصوصية بالحقوق المدنية، ولا سيما تلك المتعلقة بالحق في التعبير الحر وفي المعلومات. ويتفوق الحق في حرية التعبير وفي المعلومات، المعترف بهما في الدساتير واتفاقيات حقوق الانسان على الحق في الخصوصية [2].

3. مسؤولية المستخدم اتجاه حقه في الخصوصية

يعتبر الكثيرون أن مفهوم المساحة الخاصة على وسائل التواصل الاجتماعي كفيسبوك، لم يعد لها معنى بالنظر لطبيعة هذه الوسائل. فهي أدوات للاتصال، يمكن لكل مستخدم إعادة إرسال المحتوى أو المعلومات التي يتلقاها. فما نقوله لأصدقائنا عليها يمكن نقله إلى أصدقاء الأصدقاء وهكذا دواليك دون وجود طريقة فعالة للتحكم في حركة المعلومات[3].

كما أن المستخدم نفسه مسؤول عن انتهاك حيزه الخاص، سواء اتجاه شركات الإنترنت أو اتجاه المستخدمين. فالكثير من المستخدمين يتقبل رقابة تجارية مستمرة من طرف شركات الانترنت. والعديد منهم يهملون وضع إعدادات الخصوصية بالنظر لتعقيداتها وصعوبة إجرائها. ونرى أن الكثير منهم، وإن كانوا يعلنون عن حرصهم على خصوصيتهم، لا يقومون بما هو مطلوب منهم لجهة إعدادات الخصوصية على مواقع التواصل الاجتماعي لضمان هذه الخصوصية. بالإضافة إلى ذلك، قد يهمل مستخدمون كثر إجراء هذه الإعدادات أو لا يهتمون أصلا بها لاعتقادهم أن ما ينشرونه ليس بدي أهمية ولا يشكل خطرا عليهم أو لرغبتهم في نشر صورهم وتعليقاتهم للجمهور ولأكبر عدد

([1]) – وسيم شفيق الحجار: المرجع السابق، ص41.

([2]) – المرجع نفسه، ص40..42. بتصرف.

([3]) – المرجع نفسه، ص51.

من الناس رغبة في التباهي بما يملكونه أو بمواهبهم أو بشكلهم. ويبدو أن أغلبية مستخدمي وسائل التواصل الاجتماعي لا يحسنون ضبط إعدادات الخصوصية [1].

وبموجب القوانين المتعلقة بحماية البيانات، على شركات وسائل التواصل الاجتماعي أخذ موافقة المستخدمين بخصوص معالجة بياناتهم ومشاركتها مع الغير أو استعمالها في الإعلانات. فالمادة السابعة من التوجه الأوروبي لعام 1995 تسمح بمعالجة البيانات الشخصية في حال موافقة الشخص المعني بها. وعندما يسجل الفرد، يمكن لمشغل الموقع إبلاغه بالتعليمات المتعلقة بالخصوصية والحصول على موافقته. إلا أن معظم المستخدمين يكبسون على الفأرة لإعطاء الموافقة على شروط الخصوصية دون فهمها أو قراءتها حتى. وتتعلق هذه الشروط في الأساس بمعالجة البيانات التي تجمعها وسائل التواصل الاجتماعي من المستخدمين من خلال التسجيل عليها أو الكعكات.

كما أن العلنية هي عدو الخصوصية بمعنى أن ما يكون علنيا على وسائل التواصل الاجتماعي لا يحترم بطبيعة الحال خصوصية الفرد. والمستخدم بإطلاق التصريحات بشكل علني على موقع التواصل الاجتماعي، يكون قد تخلى عن أي حق باعتبار هذه التصريحات كخاصة [2].

لذلك فالمعلومات الشخصية التي يشاركها مع أشخاص آخرين على مواقع التواصل الاجتماعي هي معفية من القيود بموجب القوانين الأوربية المتعلقة بالبيانات الشخصية. فهذه القوانين هي معدة لتحمي الأفراد اتجاه الحكومات والشركات التجارية وليس لتقليص الاتصالات بين الأفراد وتجميع المعلومات من قبلهم. وهذه القوانين لا تحمي الفرد من نفسه ولا من أصدقائه. لأن المستخدم ذاته هو من يضع معلومات متعلقة بحياته الخاصة بتصرف الجمهور. والاجتهاد مستقر على حرمان البيانات الشخصية من الحماية عندما يفشي الشخص المعني ذاته بياناته الشخصية. وفي هذا الاتجاه، قضت المحكمة الأوروبية لحقوق الانسان في قرارها تاريخ 2009/7/23 بأن المعلومات، في حال إيصالها لمعارف الجمهور من قبل الشخص المعني ذاته، فإنها تتوقف عن كونها سرية وتصبح متاحة بحرية [3].

([1]) – المرجع نفسه، ص، 55، 47. بتصرف.

([2]) – وسيم شفيق الحجار: المرجع السابق، ص50، 65. بتصرف.

([3]) – المرجع نفسه، ص70، 72. بتصرف

ثانياً: الحق في الخصوصية عبر وسائل التواصل الاجتماعي في قانون العقوبات الجزائري

إن الأفعال التي تتعرض للخصوصية على وسائل التواصل الاجتماعي هي مشابهة لتلك المرتكبة في العالم الحقيقي، ولا تختلف عنها إلا بطريقة حصولها عبر وسائل التواصل الاجتماعي والاتصالات وعن بعد مقارنة بالوسائل الشفهية أو المادية المباشرة والحاصلة في مجلس واحد. وبالتالي يمكن –بحسب البعض–تطبيق القواعد القانونية ذاتها على هذه الأفعال لا سيما إذا لم يحدد المشرع وسيلة ارتكابها [1].

إلا أنه وبالنظر إلى الاعتبارات المذكورة أعلاه والتي تحول دون حماية فعلية للحق في الخصوصية عبر وسائل التواصل الاجتماعي فإنني أرى أنه من المستبعد ومن غير المنطقي أن تعيد المحاكم تفسير القوانين الخاصة بالخصوصية لتطبقها على ما يحدث عبر وسائل التواصل الاجتماعي. لذلك فإنه يتوجب على المشرع الجزائري (التشريعات الوطنية) أن يبتكر قوانين جديدة للخصوصية على وسائل التواصل الاجتماعي المستجدة [2].

أما فيما يتعلق بحماية هذا الحق اتجاه شركات الانترنت والحكومات الأجنبية، فإن المسألة تحتاج إلى أكثر من ذلك. وفي هذا الصدد يمكن أن نذكر الاتفاق الذي توصلت إليه المفوضية الأوروبية عام 2016 مع الإدارة الأمريكية المسمى " Privacy Shield" والذي يسمح باحترام الحريات الأساسية للمواطنين الأوروبيين عند معالجة بياناتهم الشخصية في الولايات المتحدة الأمريكية. وهذا الاتفاق يعطي المواطنين الأوروبيين الحقوق المنصوص عليها في التوجيه الرئاسي حول الحياة الخاصة الصادر عام 2014، وكذلك في القانون الأمريكي لعام 1974 حول الخصوصية المسمى "Privacy Act"، والذي ينص على حق الأمريكيين بالاطلاع وبالطعن –ما خلا حالة الأمن الوطني–في حال استعمال بياناتهم بصورة غير مشروعة. مع العلم أن البيانات الشخصية المجمعة في أوروبا، وفي الجزائر وفي أية دولة عبر العالم من قبل وسائل التواصل الاجتماعي الأمريكية، كفيسبوك يتم تخزينها في الواقع في الولايات المتحدة الأمريكية [3].

([1]) – المرجع نفسه، ص53.

([2]) –المرجع نفسه، ص45. بتصرف.

([3]) – المرجع نفسه، ص71. بتصرف.

المطلب الثالث: الحماية الإجرائية للحق في الخصوصية الرقمية

بالإضافة إلى موازنة الحق في الخصوصية مع الحق في التعبير والوصول إلى المعلومات، توازن التشريعات والمحاكم بين حق الشخص في الخصوصية ومبررات حماية الأمن الوطني في الدولة لجهة استخدام المراقبة الرقمية على الأفراد لرصد الجرائم وتعقب مرتكبيها.

بالرجوع إلى قانون الإجراءات الجزائية الجزائري، وتحديدا إلى القانون رقم 09-04 المؤرخ في 5 أوت 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نجد أنه يعطي صلاحيات للسلطات القضائية المختصة وضباط الشرطة القضائية بمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية، وهو الأمر الذي قد يتعارض مع الحق في الخصوصية. كون هذه القواعد تنص على السماح بمراقبة الاتصالات الالكترونية وجمع البيانات وحجزها، سواء من طرف السلطات الداخلية أو الأجنبية في إطار التعاون الدولي والمساعدة القضائية. كما تنص أيضا على إلزام مقدمي خدمات الانترنت بحفظ بيانات المستخدمين التي تمكن من التعرف عليهم مثل مكان المرسل والمرسل إليه وعناوين المواقع الالكترونية المطلع عليها [1].

إلا أن اهتمام المشرع بحماية الحق في الخصوصية ليس مغيبا تماما في هذا القانون، حيث يمكن أن نلمس إرادته بالتوفيق بين تبني القواعد الإجرائية الناجعة لمكافحة جرائم المعلوماتية والوقاية منها وبين تكريس هذا الحق.

من مظاهر تكريس الحق في الخصوصية يمكن أن نسجل ما يلي:

- التأكيد على سرية المراسلات والاتصالات من خلال المادة الثالثة حيث تنص على أنه:" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام والآداب العامة أو لمستلزمات التحريات أو التحقيقات القضائية الجارية... وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"

(1) – المادة 11 من القانون رقم 09-04،المرجع السابق.

- تحديد الحالات التي يلجأ فيها إلى هذه الإجراءات، حتى تنص عليها المادة الرابعة وهي على سبيل الحصر:
  - الوقاية من الأفعال الموصوفة بجرائم الإرهاب
  - في حالة وجود معلومات تفيد احتمال وقوع اعتداء على منظومة معلوماتية اعتداء يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
  - إذا تعذر الوصول إلى نتيجة بعد استيفاء كافة آليات التحريات والتحقيقات القضائية المتاحة.
  - إذا كانت في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة
- اشتراط إذن مكتوب من السلطة القضائية المختصة بإجراء عمليات مراقبة الاتصالات الالكترونية
- تقييد مجال استعمال المعلومات المتحصل عليها حيث تنص المادة التاسعة على أنه: "تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية"
- إلزام مقدمي خدمات الانترنت وتحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها[1].
- تحديد مدة الاحتفاظ بالبيانات المحجوزة بمدة سنة واحدة من تاريخ التسجيل [2].

([1]) – المادة 3/10 من القانون رقم 09-04،المرجع السابق.

([2]) – المادة 11 من المرجع نفسه.

خاتمة

يمكن إجمال أهم النتائج المتوصل إليها من خلال هذا البحث، في النقاط التالية:

- الحق في الخصوصية الرقمية مفهوم مستحدث يعبر عن قدرة الأشخاص على التحكم في تدفق بياناتهم الشخصية عبر الأنظمة المعلوماتية ومختلف تكنولوجيات الإعلام والاتصال الحديثة. وبالرغم من كونه امتدادا لمفهوم الخصوصية التي نعرفها منذ القدم فإن لهذا المفهوم المستحدث محلا ونطاقا مختلفين.
- تمثل البيانات الشخصية بنوعها المحددة للهوية والبيانات الشخصية الخاصة محلا للحق في الخصوصية الرقمية، باعتبارها الدعامة الالكترونية للمعلومات الشخصية التي يحق للأشخاص التكتم عنها وعدم إعلانها للغير. لذلك فقد حظيت بالكثير من الجهود التشريعية على المستويين الدولي والوطني في سبيل تنظيمها وحمايتها.
- تمثل الأنظمة المعلوماتية البيئة الالكترونية حيث تخلق البيانات وتعالج وتخزن وتتدفق، لذلك فهي تمثل نطاق الحق في الخصوصية بمختلف أنواعها، بدء بالحواسيب الشخصية والهواتف الذكية والشبكات المعلوماتية ووصولا إلى مواقع الانترنت، وخدمات البريد الالكتروني والسكايب ووسائل التواصل الاجتماعي. فجميعها تمثل بدورها نطاقا للحق في الخصوصية الرقمية.
- على غرار معظم الدول المتقدمة، فقد كفل المشرع الجزائري حق الأفراد في الخصوصية من خلال الدستور. وسعى إلى تكريس هذا الحق من خلال صياغة قواعد جنائية على المستويين الموضوعي والإجرائي من شأنها ضمان الحماية الجنائية لهذا الحق. إلا أنه وبخلاف الكثير من التشريعات الداخلية–على غرار فرنسا وتونس مثلا–لا يخص البيانات الشخصية بتشريع خاص يكفل لها الحماية الجنائية رغم كونها تمثل محل وجوهر الحق في الخصوصية الرقمية.
- يقدم القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 حول المساس بأنظمة المعالجة الآلية، حماية موضوعية للحق في الخصوصية عبر الأنظمة المعلوماتية، بتجريم جملة من الأفعال الماسة بالبيانات عموما دون أن يخص البيانات الشخصية بحماية خاصة، بل هي تدخل في عموم النصوص المتعلقة بحماية الأنظمة المعلوماتية والبيانات بصفة عامة. تتمثل جملة الأفعال الماسة بالحق في الخصوصية الرقمية أساسا في:

- الولوج إلى أو البقاء غير المصرح بهما في نظام معلوماتي
- ادخال معطيات إلى النظام المعلوماتي أو إزالتها أو تعديلها.
- حيازة أو افشاء أو نشر أو استعمال البيانات الشخصية.

- يقدم القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، حماية موضوعية لخصوصية الاتصالات والمراسلات والصور الشخصية، بتجريم جملة من الأفعال أهمها:
  - فض واتلاف الرسائل والمراسلات.
  - تجريم التقاط وتسجيل ونقل بيانات شخصية.
  - تجريم الاحتفاظ وإفشاء واستخدام بيانات شخصية.
- فيما تثير وسائل التواصل الاجتماعي العديد من المسائل التي قد تحول دون خلق القواعد الجنائية اللازمة لحماية الحق في الخصوصية عبرها. تتمثل أهم هذه الاشكالات في:
  - تعارض الحق في الخصوصية عبر وسائل التواصل الاجتماعي مع حرية التعبير والحق في الوصول إلى المعلومة.
  - الملكية والقيمة التجارية للبيانات الشخصية المتداولة عبر مواقع التواصل الاجتماعي.
  - الطبيعة العلنية للإنترنت وبالتالي، مسؤولية المستخدم اتجاه حقه في الخصوصية عبر هذه الوسائل.

بالإضافة إلى تدفق البيانات والمحتويات الشخصية عبر وسائل التواصل الاجتماعي لتستقر خارج الحدود السياسية للدول، لذلك فإنه من الصعب خلق قواعد جنائية على المستوى الداخلي فقط. ولا بد من التعاون وابرام اتفاقات دولية لتنظيم وخلق الإطار القانوني لحركة البيانات الشخصية المتدفقة عبر الانترنت.

- إلى جانب الحماية الموضوعية، يقدم القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 الحماية الإجرائية للحق في الخصوصية الرقمية. تظهر من خلال عمل المشرع الجزائري على إيجاد التوازن

بين تبني القواعد الإجرائية الناجعة لمكافحة جرائم المعلوماتية والوقاية منها وبين تكريس هذا الحق.

قائمة المراجع

أ. المراجع باللغة العربية

الكتب

1. دلخار صالح بوتاني: **الحماية الجنائية الموضوعية للمعلوماتية**، دار الفكر الجامعي، الإسكندرية، ص1، 2015.
2. خالد ممدوح إبراهيم: **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1، 2009.
3. عبد العال الديربي، محمد صادق إسماعيل: **الجرائم الالكترونية**، المركز القومي للإصدارات القانونية، القاهرة، ص1، 2012.
4. كيث دفلين، **الإنسان والمعرفة في عصر المعلومات**، ترجمة: شادن اليافي، مكتبة العبيكان، السعودية، ط1، 2001م.
5. مدحت محمد عبد العزيز إبراهيم: **الجرائم المعلوماتية الواقعة ضد النظام المعلوماتي**، دار النهضة العربية، القاهرة، ط، 2015.
6. محمود أحمد طه: **المواجهة التشريعية لجرائم الكمبيوتر والانترنت**، دار الفكر والقانون، المنصورة، ط1، 2017.
7. منصور بن محمد الغامدي: **البيانات الحيوية، البصمة الصوتية**، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005.
8. وسيم شفيق الحجار: **النظام القانوني لوسائل التواصل الاجتماعي**، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط1، بيروت، 2017. متاح على الرابط:

https://carjj.org/sites/default/files/ebooks/social_media_book-finalforprint.pdf

المقالات

9. إيان ليه: **الإشراف على استخدام البيانات الشخصية**، مقال متاح على الرابط:
www.dcaf.ch/content/download/…/1/…/Tool_6_intel_over_AR.pdf

10. توبي مندل وآخرون: **دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير**، الأمم المتحدة،منشوراتاليونسكو،فرنسا، 2013، ص13.متاح على الرابط:
http://unesdoc.unesco.org/images/0021/002182/218273A.pdf

11. كريم عاطف: **الخصوصية الرقمية بين الانتهاك والغياب التشريعي**، مركز دعم لتقنيات المعلومات، القاهرة. متاح على الرابط: info@sitcegypt.org

النصوص القانونية

12. **الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية**، المجلس الأوربيستراسبورغ 1981.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

13. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 حول المساس بأنظمة المعالجة الآلية. الجريدة الرسمية للجمهورية الجزائرية، العدد 71. السنة الواحدة والأربعون.

14. قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006. المعدل والمتمم لقانون العقوبات. الجريدة الرسمية للجمهورية الجزائرية/ العدد 84.

15. القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 5 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية/ العدد 47.

ب. المراجع باللغة الأجنبية

الكتب

1. Jerome H. Saltzer& M. FransKaashoek: **Principles of Computer System Design**. Morgan Kaufmann Publishers - Elsevier- .USA.2009. p6
2. FernardLone Sang. **Protection des systemes informatiques contre les attaques par entrees– sorties**. Doctorat de l'Uinivercite de Toulouse. Directeurs de these : Yves Deswarte et Vincent Nicomette. 2012.p06

المقالات:

3. Winnie Chung and John Paynter:**Privacy Issues on the Internet**, Department of Management Science and Information Systems, School of Business, The University of Auckland, Private Bag 92019, Auckland, New Zealand. Proceedings of the 35th Hawaii International Conference on System Sciences – 2002. IEEE

النصوص القانونية

4. The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, Human Rights Council Twenty-seventh session, 30 June 2014, A/HRC/27/37. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session 27/Documents/A.HRC.27.37_en.pdf
5. Convention On Cybercrime. Budapest, 23.XI.2001.

6. Loi nº 78-17 du 6 janvier 1978, modifiée le 6 août 2004. https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive-annotee.pdf