مجلة العلوم

الشرعية والقانونية

مجلة علمية محكمة تصدرها

كلية القانون بالخمس

جامعة المرقب

العدد الأول لسنة 2018

مجلة العلوم الشرعية والقانونية مجلة محكمة تصدر عن كلية القانون بجامعة المرقب

رقم الإيداع المحلي 2015/379م.

دار الكتب الوطنية ببنغازي . ليبيا

هاتف:

9097074 . 9096379 . 9090509

بريد مصور:

9097073

البريد الإلكتروني:

Nat-Liba@hotmail.com

ملاحظة /

الآراء الواردة في هذه البحوث لا تعبر إلا عن وجهة نظر أصحابها، وهم وحدهم المسؤولون عن صحة المعلومات وأصالتها، وإدارة المجلة لا تتحمل أية مسؤولية في ذلك.

للاتصال برئيس التحرير: 091-1431325 / 092-7233083

شروط النشر بالمجلة:

الأخوة الأفاضل حرصاً على حسن إخراج المجلة نرجو التكرم بالالتزام بالآتي:

1. أن لا يكون قد تمَّ نشر البحث من قبل في أي مجلة أو كتاب أو رسالة علمية أو وسيلة نشر أخرى.
2. أن لا تزيد صفحات البحث عن (35) صفحة تقريبا بما فيها قائمة المراجع.
3. هوامش الصفحة من اليمين ، على ورق A4 . وحجم الخط (14) ونوعه (Traditional Arabic). وللهوامش (12) وبين السطور (1).
4. العناوين الوسطية تكتب مسودة وبحجم خط (16) Bold.

العناوين الجانبية: تكتب من أول السطر مسودة وبحجم (14) Bold ، وتوضع بعدها نقطتان رأسيتان.

5. تبدأ الفقرات بعد خمس فراغات.
6. يجب الاهتمام بوضع علامات الترقيم في أماكنها المعروفة الصحيحة، وبرموز أسمائها بالخط العربي .
7. ضرورة استخدام رمز القوسان المزهران للآيات القرآنية (﴿ ﴾) ، والرمز (« ») للنصوص النبوية، والرمز: (" ") علامة التنصيص.

8. تكتب في الهوامش أسماء الشهرة للمؤلفين كالبخاري، الترمذي، أبو داود، ابن أبي شيبة، ولا يكتب الاسم الكامل للمؤلفين في الهوامش.
9. الإحالات للمصادر والمراجع تكون في هوامش صفحات البحث وليس في آخره.
10. لا تكتب بيانات النشر للمصادر والمراجع في الهامش، وإنما يكتب ذلك في قائمة المصادر والمراجع في آخر البحث.

مثل : ابن حجر، فتح الباري شرح صحيح البخاري، ج 2، ص 332

11. عند الإحالة إلى كتب الحديث المرتبة على الأبواب الفقهية والموضوعات العلمية تكتب أسماء الكتب والأبواب، مع كتابة الجزء، والصفحة، ورقم الحديث إن

وجد. هكذا: أخرجه البخاري في صحيحه، كتاب. الإيمان، باب الإيمان وقول النبي « بني الإسلام على خمس» : ج 1، ص 12 ، رقم 1.

12. تخرَّج الآيات القرآنية في المتن بعد الآية مباشرة بحجم 12.

مثل: قال الله تعالى: (سَيَقُولُ السُّفَهَاءُ مِنَ النَّاسِ مَا وَلَّاهُمْ عَنْ قِبْلَتِهِمُ الَّتِي كَانُوا عَلَيْهَا قُلْ لِلَّهِ الْمَشْرِقُ وَالْمَغْرِبُ يَهْدِي مَنْ يَشَاءُ إِلَى صِرَاطٍ مُسْتَقِيمٍ)..[البقرة: 142]

13. في الهوامش، يترك بعد أرقام الهوامش فراغ واحد ثم تبدأ كتابة المعلومات التِي يراد كتابتها، وهوامش كل صفحة تبدأ بالرقم واحد.

14. قائمة المصادر ترتب على أسماء الشهرة للمؤلفين، كالآتي:

ابن حجر، أحمد بن علي بن محمد العسقلاني، فتح الباري شرح صحيح البخاري، تحقيق: علي محمد البجاوي، بيروت: دار الجيل، ط 1، سنة 1112 هـ/ 1992م.

15. يرفق الباحث ملخصًا لسيرته الذاتية في حدود صفحة واحدة، ويرفق صورة شخصية له.

16. ترسل البحوث، والسير الذاتية المختصرة مطبوعة على ورق وقرص مدمج لرئيس التحرير مباشرة أو عبر البريد الإلكتروني الآتي.

iaelfared@elmergib.edu.ly

17. للمجلة الحق في رفض نشر أي بحث بدون إبداء الأسباب والبحوث التي لا تقبل للنشر لا ترد إلى أصحابها.

18. لصاحب البحث المنشور الحق في الحصول على عدد (5) نسخ من عدد المجلة المعني مجاناً.

19. ترتيب ورود الأبحاث في المجلة لا يدل على أهمية البحث أو الباحث، إنما للكل التقدير والاحترام .

20. لإدارة المجلة حرية تغيير الخطوط والتنسيق بما يناسب إخراج المجلة بالصورة التي تراها.

نأمل من السادة البحاث والقراء المعذرة عن إي خطأ قد يحدث مقدماً ، فلله الكمال وحده سبحانه وتعالى.

ملاحظة /

الآراء الواردة في هذه البحوث لا تعبر إلا عن وجهة نظر أصحابها، وهم وحدهم المسؤولون عن صحة المعلومات وأصالتها، وإدارة المجلة لا تتحمل أية مسؤولية في ذلك.

للاتصال برئيس التحرير: 091-1431325 / 092-7233083

مجلة العلوم الشرعية والقانونية
مجلة علمية محكمة تصدرها
كلية القانون بالخمس – جامعة المرقب

فهرس الموضوعات

كلمة رئيس التحرير

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

والحمد لله رب العالمين، والصلاة والسلام على المبعوث رحمة للعالمين، وعلى آله وصحبه الكرام الطيبين، ومن تبعهم بإحسان إلى يوم الدين.

أما بعد: فإنه يسر هيئة التحرير أن تهديكم العدد الأول من المجلة للعام 2018م. ونظراً للعمل الذؤوب، والجهد المتواصل للرقي بالمجلة، فقد منَّ الله تعالى علينا بأن داع صيت مجلتكم في الآفاق، بحيث صارت معتمدة في ترقيات اعضاء هيئة التدريس الجامعي في كل الجامعات الليبية وكذلك بعض الجامعات العربية، الحمد لله وله المنة والفضل، وهذا الأمر مما يثقل كاهلنا من ناحية، ويشجعنا على مزيد من بدل الجهد والعطاء، وكل ذلك كان بفضل جنود مجهولين يقدمون العمل للمجلة بدون ادنى مقابل ـ جزاهم الله أحسن الجزاء، وشكر جهدهم، وزادهم علما وتقى ـ كما لا يفوتني أن أنبه أن بحوث طلاب الدراسات العليا التي تنشر في المجلة تتم بإشراف من أساتذتهم بجامعاتهم المختلفة، ثم تأخذ دورتها في المجلة مثل البحوث المقدمة من السادة أعضاء هيئة التدريس الجامعي.

وفي الختام نشكر كل من ساهم معنا في أن تخرج المجلة بهذه الصورة، ونشكر كذلك كل من اتخذها منبرا لنشر نتاجه العلمي، ونسأل الله ـ تعالى ـ أن يوفق الجميع لما يحب ويرضى، وله الحمد في الأولى والأخرى.

د. إبراهيم عبدالسلام الفرد
رئيس التحرير

الحماية الجنائية للبيانات الشخصية الإلكترونية في القانون الليبي و المقارن

د.ماشاءالله عثمان الزوي

عضو هيئة تدريس بكلية القانون / جامعة بنغازي

مُـقَدّمَـــــةُ

للتقنيةِ ووسائِلِ الاتِّصَالِ الحديثةِ دورٌ مهمٌّ في تطوُّرِ المجتمعاتِ وتغييرِهَا منْ مجتمعِ الصناعةِ إلى مجتمعِ المعلوماتِ والمعرفةِ، وتحديثِ الخدماتِ بها، وأضْحَى استخدامُ تلكَ التقنيةِ ووسائلِ الاتصالِ منْ سماتِ العالَمِ الذِي نعيشُهُ اليومَ، وباتَ واضحًا أنَّ الاعتمادَ عليها أمرٌ لا غنىً عنهُ لكلِّ مرافقِ الدولةِ، خصوصًا القطاعاتِ الخدميَّةَ الخاصَّة والعامَّة منها، التي تسعَى إلى تقديمِ خدماتٍ أفضلَ للفردِ؛ بتوفيرِ الجهدِ والوقتِ، بل وحتَّى المسافاتِ.

ووصولاً إلى هذِهِ الغايةِ تقومُ تلكَ القطاعاتُ بإنشاءِ بنوكٍ مختلفةٍ للمعلوماتِ Banque de données، وقدْ تَستخدِمُ البياناتِ أو المعلوماتِ المختزنةِ في بنوكِ المعلوماتِ لأغراضٍ غيرِ مشروعةٍ، أو أنْ تقومَ بعضُ الشركاتِ ببيعهَا بعدَ تبويبِهَا لمن يرغبُ في ذلك.

كمَا أنَّ الخدماتِ والمعاملاتِ الإلكترونيةَ التي أضحَى يتَّجهُ إليهَا الاقتصادُ الوطنيُّ لدَى كثيرٍ مِنَ الدولِ تجدُ في المعلوماتِ مُحَرِكَهَا الأساسيَّ، الأمرَ الذي يعزّزُ منْ أهميَّةِ المعلوماتِ، والعملِ على حمايتِهَا.

غيرَ أنَّ التعاملَ بالخدماتِ والمعاملاتِ الإلكترونيَّةِ المختلفةِ لدَى كثيرٍ منَ الدُّوَلِ كشَفَ عنْ ضَعْفِ مستَوَى الحمايةِ المقرّرةِ للبياناتِ والمعلوماتِ الشخصيَّةِ في البيئةِ الرَّقَمِيَّةِ.

إنَّ استخدامَ العديدِ منَ المواقعِ على الإنترنت بقصْدِ الترفيهِ أو مواقعِ التواصلِ الاجتماعيّ وغيرِهَا منَ المواقعِ و الخدماتِ على الشبكةِ بلا شكَّ يشَكِّلُ خطورةً على خصوصيةِ المستخدمِ في كثيرٍ منَ الأحيان، لاَ سِيَمَا

معَ ضعفِ مستوى الأمنِ والحمايةِ في تلكَ المواقعِ، الأمرَ الذي قدْ يجعلُهَا تتعرَّضُ لهجماتٍ إلكترونيةٍ، الهدفُ منهَا الحصولُ على المعلوماتِ والبياناتِ الشخصيَّةِ للمستخدمِ.

بالإضافةِ إلى الجهودِ الوطنيَّةِ والدوليَّةِ لمكافحةِ الإرهابِ أوِ الجريمةِ المنظمَةِ Crime organisé قدْ تقتضِي الاطلاعَ على البياناتِ والمعلوماتِ الشخصيةِ، والكشفَ عليها، فضلاً عنْ إمكانيَّةِ نقلِ وتبادلِ تلك البياناتِ والمعلوماتِ منْ دولةٍ لأخرى، ومَا يتبعُ ذلك مِنْ تعرضِهَا لأعمالِ القرصنةِ، والاطلاعِ أو الوصولِ غيرِ المشروعِ.

إنَّ زيادةَ حجمِ البياناتِ والمعلوماتِ الإلكترونيَّةِ والمخاطر التي تتعرَّضُ لها في الوقتِ الحالي مقارنَةً بأيّ وقتٍ مضَى، وما قدْ يترتَّبُ عليه منْ خسائرَ جسيمةٍ على الصعيدِ الأمنيّ والاقتصاديّ للدولةِ، يجعلُ الأمنَ المعلوماتيَّ cybersécurité جزءًا لا يتجزَّأُ منْ منظومَةِ الأمنِ القومي للدولةِ، والدفاعِ عنْ مواطنيهَا وأجهزتِهَا المختلفةِ.

وتبدُو الإشكاليَّةُ في أنَّه على الرغمِ منَ التأثيرِ الإيجابي للتقنيةِ ووسائلِ الاتصالِ الحديثةِ في المجتمعِ والاستفادة منها بأنْ يسّرَتْ وطوَّرَتِ الخدماتِ الإلكترونيةِ المختلفةِ إلاَّ أنَّها قد توظفُ بشكلٍ سيّءٍ، الأمرَ الذِي يُشَكِّلُ تهديدًا كبيرًا لسِريَّةِ البياناتِ والمعلوماتِ الشخصيَّةِ للمستخدمِ، وهذا التهديدُ في تطورٍ مستمرٍّ مع زيادةِ استخدامِ تلك التقنيةِ ووسائلِ الاتصالِ الحديثةِ، والاعتمادِ عليها في المجتمعِ.

ولا شكَّ فِي أنَّ للتقنياتِ الحديثةِ في مجالِ الاتصالِ والمعلوماتيَّةِ تأثيرًا كبيرًا ومتزايدًا على حقوقِ الأفرادِ وحرياتهم، فعلى سبيلِ المثالِ فقد تَلَقَّتِ اللجنةُ الوطنيةُ للمعلوماتيةِ والحرياتِ[1] بفرنسا في سنة 2011 وحدَهَا ما يَصِلُ إلى 700 شَكْوَى منَ الأشخاصِ تتضمَّنُ اعتراضَهم على نشرِ صورِهم، وما يتعلَّقُ ببياناتهم الشخصيةِ على الإنترنت، وهو ما يزيدُ عمَّا كانَ عليهِ الوضعُ عام 2010 بنسبة 42% منْ قضايَا حمايةِ الخصوصيَّةِ

(1)Commission nationale de l'informatique et des libertés (CNIL)

على الإنترنت أو خصوصية المعلومات[2]، وقد سُجِّلَتِ الأعوامُ الأخيرةُ –كذلك– تزايدَ عددِ الهجماتِ الإلكترونيةِ على النُّظُمِ المعلوماتيَّةِ بالدول العربية، لاَ سِيَّمَا القطاعاتِ الحكومية وقطاعاتِ الطاقةِ والخدماتِ الماليةِ، وقد شكّلت هذه القطاعاتُ نسبةَ 65% من مجموعاتِ الهجماتِ، ولأسبابٍ مختلفةٍ [3].

لا شكَّ فِي أنَّ الأمرَ يحتاجُ إلى إحداثِ توازنٍ بشكلٍ يضمنُ الاستفادةَ منَ التقنيةِ ووسائلِ الاتصالِ الحديثةِ، مع ضمانِ حمايةِ حقِّ الفردِ في سِرِيَّةِ البياناتِ والمعلوماتِ الشخصيةِ، وعدم التعرُّضِ لهذا الحق.

ومن أجلِ ذلك فقد عَنَتِ الكثيرُ منَ الدولِ بوضعِ تشريعاتٍ تكفلُ تنظيمَ استخدامِ تقنيةِ المعلوماتِ، بحيثُ تكونُ في خدمةِ الفردِ لا وبالاً عليه، فتنتهكُ من خلالها الحقوقَ والحرياتِ الفرديةَ أو العامةَ.

وفي المنطقةِ العربيةِ كليبيا والسعوديةِ وسلطنةِ عمانَ يمكنُ ملاحظةُ زيادةِ اعتمادِ مؤسَّسَاتِ ومرافقِ الدولةِ على البياناتِ الشخصيةِ، واستخدامها لأغراضٍ مختلفةٍ، الأمرَ الذي يجعلُنا نتساءلُ عن مدَى الحمايةِ الجنائيةِ التي تتمتَّعُ بها البياناتُ الشخصيةُ الإلكترونيةُ في تلك الدول ؟ لا سِيَّمَا في ظلِّ تَنَامِي استخدامِ تقنيةِ المعلوماتِ في مختلفِ المجالات، وسنحاوِلُ معرفةَ ذلك عبرَ صفحاتِ البحثِ كما سيأتي:

المطلبُ الأوَّلُ: مفهومُ البياناتِ الشخصيةِ الإلكترونيةِ ووضعُها في قانونِ العقوباتِ الفرنسي.

المطلبُ الثاني: مَدَى الحمايةِ التي تكفلُهَا بعضُ التشريعاتِ العربيةِ للبياناتِ الشخصيةِ الإلكترونيةِ.

(2)Carole Girard–Oppici : Les donnéespersonnelles et la protection de la vie privée à l'heure des nouvelles technologies, sur : http://www.net–iris.fr/veille–juridique/dossier/20679/les–donnees–personnelles–et–la–protection–de–la–vie–privee–a–heure–des–nouvelles–technologies.4–9–2015 .

(3)www.alweeam.com.sa/407005/%D9%81%D8%A7%D9%8A%D8%B1–

المطلبُ الأوَّلُ

مفهومُ البياناتِ الشخصيةِ الإلكترونيةِ ووضعُها في قانونِ العقوباتِ الفرنسي

كَفَلَتِ المادةُ الثامنةُ من الاتفاقيةِ الأوروبيةِ لحقوقِ الإنسانِ في فقرتها الأولى حرمةَ الحياةِ الخاصةِ[4]، وتتضمَّنُ البياناتُ الشَّخصيَّةُ أسرارَ الفردِ، ولكلِّ فردٍ الحقُّ في احترامِ حياتِهِ الخاصَّةِ ومُراسَلاتِهِ.

وقدْ أصدرَ المُشَرِّعُ القانونَ رقم 17 لسنة 1978[5] بشأنِ المعلوماتيَّةِ والملفاتِ لحمايَةِ الحرياتِ؛ لكي تكونَ تقنيةُ المعلوماتِ أقربَ ما تكونُ في خدمةِ الفردِ. و جاءتِ المادةُ الأولى والمعدَّلةُ مؤخَّرًا بالقانونِ رقم 1321 – 2016 الصادرِ في 7 أكتوبر 2016م بشأنِ الحكومةِ الرقمية Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. لتؤكِّدَ على أنَّ تقنيةَ المعلوماتِ يجبُ أنْ تكونَ في خدمةِ المواطنِ، وأنَّ التنميةَ يجبُ أنْ تكونَ في إطارِ التعاونِ الدولي، كما يجبُ أن لا يترتبَ عليها المساسُ بهويةِ الإنسانِ أو حقوقِهِ أو حياتِهِ الخاصةِ أو الحرياتِ الفرديةِ والعامة libertés individuelles ou publiques، وأنَّ لكلِّ شخصٍ الحقَّ أنْ يقرِّرَ التحكمِ في استخدامِ البياناتِ الشخصيةِ وفقاً للشروطِ المنصوصِ عليها في القانون.

(4)Marine Farshian: Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne, Droit a la vie privée et protection des données personnelles (Assemblée Parlementaire du Conseil de l'Europe), La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 28 mai 2015,p 3.

(5)Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

وتجدرُ الإشارةُ إلى أنَّ هذا القانونَ عُدِّلَ عِدَّةَ مرَّاتٍ كالتعديلِ بمُقتَضَى القانونِ رقم 239 لسنةِ 2003[6]، والقانونِ801 لسنةِ 2004، والقانونِ 64 لسنةِ 2006 بشأنِ مكافحةِ الإرهابِ[7]، والقانونِ 334 لسنةِ 2011 [8] والمرسومِ رقم 1012 لسنةِ2011 بشأنِ المراسلاتِ الإلكترونيةِ[9]، والقانونِ 954 لسنةِ 2012 بشأنِ التحرُّشِ الجنسيّ[10]، والقانونِ رقم344 لسنةِ 2014 بشأنِ الاستهلاك[11]، والمرسوم 1341لسنة2015[12]والقانون رقم 1321 لسنة 2016 بشأن الحكومة الرقمية[13]،والقانون رقم 41 لسنة 2016

(6)Loi n° 2003-239 du 18 mars 2003 pour la sécuritéintérieure

(7)Loi n° 2006-64 du 23 janvier 2006 relative à la luttecontre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôlesfrontaliers.

(8)Loi n° 2011-334 du 29 mars 2011 relative au Défenseur des droits

(9)Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques

(10)Loi n° 2012-954 du 6 août 2012 relative au harcèlementsexuel

(11)Loi n° 2014-344 du 17 mars 2014 relative à la consommation

(12)Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration

(13)Loi n° 2016-1321 du 7 octobre 2016 pour uneRépubliquenumérique

بشأنِ تحديثِ نظامِ الرعايةِ الصحيةِ[14].والقانونِ رقم 1547 لسنة 2016. [15]والقانونِ رقم 31 لسنة 2016 والصادرِ في 3 يونيه 2016م بشأنِ تعزيزِ مكافحةِ الجريمةِ المنظمةِ والإرهابِ وتمويلها. [16]

وسنتناولُ الحمايةَ التي يقررها التشريعُ الفرنسي للبياناتِ الشخصيةِ، على أن نسبقَ ذلك ببيانِ مفهومِ البياناتِ الشخصيةِ الإلكترونيةِ، أو الخصوصيةِ المعلوماتيةِ، وتأثير التقنياتِ الحديثةِ عليها كما يأتي:

الفرعُ الأوَّلُ

مفهومُ البياناتِ الشخصيةِ الإلكترونيةِ وتأثيرُ التقنياتِ الحديثةِ عليها

يعتبر أمنُ وسلامةُ البياناتِ والمعلوماتِ الشخصيةِ sécurité des données منَ القضايا الهامَّةِ لدى الفرد، وعدمُ وجودِ حمايةٍ فعالةٍ للبياناتِ الشخصيةِ يُعَدُّ حجرَ عثرةٍ أمامَ نجاحِ الخدماتِ الإلكترونيةِ رغم توفيرها الجهدَ والوقتَ للفرد. خاصَّةً معَ تنامي مخاطِرِ البياناتِ والمعلوماتِ الشخصيَّةِ بالتطوُّرِ السريعِ في الإنترنت والحاسباتِ الآلية، وعليه سنحاولُ من خلالِ هذه الجزئيةِ من الدراسةِ بيانَ تأثيرِ تقنيةِ المعلوماتِ على البياناتِ الشخصيةِ، على أنْ نسبقَ ذلك ببيانِ المقصودِ مِنَ البياناتِ الشخصيةِ الإلكترونيةِ أو الخصوصيةِ المعلوماتيةِ كما يأتي:

أولاً: مفهومُ البياناتِ الشخصيةِ الإلكترونيةِ:

للفردِ الحقُّ في الخصوصيةِ المعلوماتيةِ، ويُقْصَدُ بالخصوصيةِ المعلوماتيةِ سِرِيَّةُ البياناتِ والمعلوماتِ الشخصيةِ الإلكترونيةِ، وتختلفُ البياناتُ عنِ المعلوماتِ في أنَّها تُشَكِّلُ الحقائقَ أو الرسائلَ أو الإشاراتِ أو المفاهيمَ التي تُعْرَضُ بطريقةٍ صالحةٍ للإبلاغِ أو التوصيلِ أو التفسيرِ أو المعالجةِ، أمَّا المعلوماتُ فهي المعنى الذي يُسْتَخْلَصُ

(14)Loi n° 2016-41 du 26 janvier 2016 de modernisation de notresystème de santé

(15)Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du xxle siècle.

(16)Loi n° 2016-731 du 3 juin 2016 renforçant la luttecontre le crime organisé, le terrorisme et leurfinancement, et améliorantl'efficacité et les garanties de la procédurepénale

من البيانات، فالمعلومةُ عبارةٌ عن رمزٍ أو مجموعةٍ منَ الرموزِ تُفْضِي إلى معنىً معيَّنٍ[17]، على أنَّ البياناتِ والمعلوماتِ المكفولةَ بالحماية هي المتعلقةُ بالشخصِ الطبيعِي وليس المعنوي، وذلك طبقًا للقانونِ رقم 17 لسنةِ 1978 بشأنِ المعلوماتيةِ والملفاتِ والحرياتِ في فرنسا[18] (المادة الثانية)،على اعتبارِ أنَّ القانونَ يهدِفُ إلى حمايةِ الحقوقِ والحرياتِ الفرديةِ، وهذه المفاهيمُ لا تتفِقُ وطبيعةَ الشخصِ المعنوي.

كمَا يكفلُ القانونُ الحمايةَ لاسمِ الشخصِ المعنوي إذا كانَ اسمُهُ متكونًا منِ اسمِ شخصٍ طبيعيٍّ أو لقبِهِ ،كاسمِ أحدِ الشركاءِ أو المساهمينَ بالشركة[19].

وبيَّنَ القانونُ –سالف الذكر– المقصودَ بالبياناتِ الشَّخصيَّةِ بأنَّهَا البياناتُ التي مِنْ شأنهَا الكشفُ عن هويَّةِ الشَّخصِ الطبيعي، سواءٌ أكانَ بشكلٍ مباشرٍ أم غيرِ مباشرٍ، كبياناتِ حالةِ الشَّخصِ الصحيَّة، والبياناتِ المتعلِّقةِ بالجرائمِ، وتدابيرِ الأمنِ والسلامة[20]،وكذلك الاسمِ، واللقبِ، والصورِ الشخصيَّةِ، وتاريخِ الميلادِ، والحالةِ الاجتماعيةِ، وعنوانِ البريدِ الإلكترونيّ[21]، وعنوانِ بروتوكولِ الإنترنت IP،و رقمِ الضمانِ الاجتماعيّ، ورقمِ الهاتفِ، رقمِ البطاقةِ المصرفيةِ، والبصمةِ الجينيةِ وأرقامِ بطاقاتِ الائتمانِ، و رقمِ رخصةِ القيادةِ، وملفاتِ تعريفِ الارتباطِ cookies، وغيرِها منَ البرامجِ التي تسمحُ بالتعرُّفِ على هويَّةِ الفردِ أو حاسبِهِ الآلي.

---

(17) راجع : هشام محمد فريد رستم ،قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط،1994م،ص26.

(18)Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(19)Marie-Laure Laffaire: Protection des données à caractère personnel,Éditionsd'Organisation, 2005,p45.

(20)Panorama des infractions Informatique et libertés en France, https://www.alain-bensoussan.com/avocats/infractions-informatique-et-libertes/2017/02/21/

(21)https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

أمَّا عنْ تشريعِ الاتحادِ الأوروبيّ الجديدِ لحمايةِ البياناتِ رقم 679- 2016 والصادرِ في 27 أبريل 2016مفقد حدَّدَ مفهومَ البياناتِ الشخصيةِ بأنها: " أيُّ بياناتٍ تتعلَّقُ بشخصٍ طبيعيٍّ محددٍ أو قابلٍ للتحديدِ، والشخصُ الطبيعيُّ المعنيُّ هو الشخصُ الذي يمكنُ تحديدُهُ بشكلٍ مباشرٍ أو غيرِ مباشرٍ، وذلكَ بالرجوعِ إلى الاسمِ، أو رقمِ التعريفِ، أو بياناتِ الموقعِ، أو عبرَ الإنترنت، أو إلى أَحَدِ العواملِ المحددةِ للفيزيائيةِ، الفسيولوجية؛ الهويةِ الجينيةِ أو العقليةِ أو الاقتصاديةِ أو الثقافيةِ أو الاجتماعيةِ لهذا الشخصِ الطبيعيّ[22]، ولا تفقدُ البياناتُ تلكَ الصفةَ حتَّى عندَ مَا تكونُ مشفرةً أو لا تسمحُ بالتعريفِ، طالما يمكنُ استخدامُها لإعادَةِ تحديدِ هويةِ الشخصِ، وتتمتَّعُ بحمايةِ القانونِ، ولا البيانات شخصية متى كانت لا تسمحُ بتحديدِ هويةِ الشخصِ بأيّ حالٍ منَ الأحوال[23].

في حين حدَّدَ مشروعُ قانونِ حمايةِ البياناتِ الشخصيةِ المصريُّ لعام 2017 المقصودَ منَ البياناتِ الشخصيةِ بأنَّها " أيُّ معلوماتٍ عنِ الفردِ الذي تكونُ هويتُهُ محددةً، أو يمكنُ تحديدُها بصورةٍ معقولةٍ، سواءٌ أكانَ منْ خلالِ هذِهِ البياناتِ أم عنْ طريقِ الجمعِ بينهَا وبينَ أيّ بياناتٍ أخرَى، بما في ذلك الصوتُ والصورةُ، والمتعلقةُ بشخصٍ ذاتيٍّ مُعرَّفٍ أو قابلٍ للتعرفِ عليه.

كمَا عرَّفَ نظامُ مكافحةِ جرائمِ تقنيةِ المعلوماتِ السعوديُّ البياناتِ بأنَّهَا المعلوماتُ أو الأوامرُ أو الرسائلُ أو الأصواتُ، وكذلكَ الصوَرُ التي تُعَدُّ أو التي سَبَقَ إعدادُها لاستخدامِهَا في الحاسبِ الآليّ،كالأرقامِ والرموزِ والحروفِ وغيرهَا. و عرَّفَ قانونُ مكافحةِ جرائمِ تقنيةِ المعلوماتِ العُمانيُّ البياناتِ والمعلوماتِ بأنَّهَا كلُّ ما يمكنُ تخزينُهُ ومعاجلتُهُ وتوليدُهُ ونقلُهُ بوسائل تقنيةِ المعلومات، أيًّا كانَ شكلُهُ كالكتابةِ والصوَرِ والأصواتِ، والرموزِ والإشارات، في حين بيَّنَ المقصودَ منْ معالجةِ البياناتِ الشخصيةِ بأنَّهَا أيُّ عمليةٍ أو مجموعةِ عملياتٍ

(22)Article 4 of The EU general data protection regulation 2016/679 (GDPR).

(23)https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

تُجْرَى علَى البياناتِ، عن طريقِ وسائلَ تلقائيةٍ أو غيرِهَا، أو جمعِها، أو تسجيلِها، أو تنظيمِها، أو تخزينِها، أو تعديلِها، أو تحويرِها، أو استرجاعِها، أو مراجعتِها، أو الإفصاحِ عنها، عن طريقِ إرسالِهَا أو توزيعِها، أو إتاحتِها بوسائلَ أخرَى، أو تنسيقِها، أو ضمِّ بعضِها إلَى بعضٍ، أو محوِها أو إلغائِهَا.

أمَّا قانونُ تنظيمِ الاتصالاتِ رقم 22 لسنة 2010 في ليبيا فقدْ عَرَّفَ الاتصالاتِ بأنَّهَا كلُّ عمليةِ نقلٍ أو بثٍّ أو استقبالٍ أو إرسالِ الرموزِ، أو الإشاراتِ، أو الأصواتِ، أو الصوَرِ، أو البياناتِ، مهمَا كانتْ طبيعتُها بواسطةِ الوسائلِ السلكيَّةِ أو اللاسلكيَّةِ، أو أيّ وسيلةٍ أخرى من وسائلِ تقنيةِ الاتصالاتِ.

ثانياً: تأثيرُ التقنياتِ الحديثةِ علَى البياناتِ الشخصيةِ الإلكترونيةِ وأهميةُ حمايتِهَا:

أدَّى التطورُ المذهلُ إلى زيادةِ الاعتمادِ على استخدامِ الحاسبِ الآليّ والإنترنت، حتَّى غَدَتْ وسائلُ الاتصالِ الحديثةِ –وفي مقدِّمتِها الإنترنتُ– منَ الوسائلِ التِي لا يمكنُ الاستغناءُ عنهَا في الاتصالِ ونقلِ المعلومات[24]، علَى اعتبارِ أنَّ تكنولوجيا المعلوماتِ والاتصالاتِ منَ الأدواتِ التي تضمَّنُ جودةَ الخدماتِ العامَّةِ وتطويرِهَا [25]، غيرَ أنَّ التطوُّرَ الذي تشهدُهُ تقنيةُ المعلوماتِ له –بلَا شكٍّ– تأثيرٌ قويٌّ على حقوقِ الأفرادِ وحرياتِهم، لاَ سِيَّمَا الحقّ في سريَّةِ البياناتِ الشخصيَّةِ [26] ففِي إطارِ تطويرِ الخدماتِ المختلفةِ بالدولةِ،وزيادةِ فعاليتِهَا وتسهيلِهَا، يقومُ الفردُ بتقديمِ بياناتِهِ ومعلوماتِهِ الشخصيَّةِ للقطاعاتِ المختلفةِ بالدولَةِ،لاَ سِيَّمَا تلكَ التي تعتمدُ علَى الإنترنت في التواصُلِ معَ عملائِهَا، أو معَ غيرِهَا منَ القطاعاتِ، إلَّا أنَّ ذلكَ يؤدِّي إلى اتِّسَاعِ نطاقِ الرقابةِ الاجتماعيَّةِle contrôle social،فاستخدامُ الحاسبِ لِمَا يتَّسِمُ بِهِ منْ قُدُراتٍ عاليةٍ في تخزينِ البياناتِ وتجميعِهَا

(24) خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009م، ص31.

(25) Alexis Ngounou: Logicielslibres et administration électronique,Thèse de doctorat,UniversitéLille 2,2010,Résumé

(26) Monika Zwolinska: Sécurité et libertésfondamentales des communications électroniques en droit français, européen et international,tése de doctrat,Université de Nice,2015,résumé.

ومعالجتِهَا،وهيَ التي تُجْمَعُ عنِ الأفرادِ، وتُخَزَّنُ في بنوكِ المعلوماتِ، واحتمالُ تعرضِهَا للاستخدامِ والإفشاءِ غيرُ مشروعٍ، وتلكَ الخطورةُ في تزايدٍ إذا رُبِطَتْ أجهزةُ الحاسبِ الآليّ بعضِهَا معَ بعضٍ، أو بشبكاتٍ عامةٍ للاتصالِ، حيثُتَتَبَادَلُ المعلوماتُ بينَ مراكزِ المعلوماتِ المختلفةِ، منْ حيثُ الغايةُ منْ تجميعِ البياناتِ وتخزينِهَا،ومنْ ثَمَّ ربطُ هذهِ المعلومات ببعضِهَا معَ بعضٍ[27]، حيثُ تسمحُ في نهايةِ الأمرِ بالتَّعرُّفِ عنْ هويةِ الفردِl'identitéd'unepersonne ومعرفةِ اهتماماتِهِ[28].

ويُلَاحَظُ أَنَّ العديدَ منْ شركاتِ الاتصالاتِ والتأمينِ وغيرها – في الدولِ العربيةِ خاصَّةً– تطلُبُ منْ عملائِهَا صُوَرًا شخصيَّةً إلكترونيَّةً،وبصماتٍ إلكترونيَّةً، وصُوَرًا لجوازاتِ سفرِهِمْ، ومستنداتٍ إلكترونيَّةً أخرى لا تقلُّ عنهَا أهميَّةً،وتقومُ بحفظِهَا في أجهزتهَا،الأمرَ الذي قدْ يُعَرِضُهَا لمخاطرِ الدخولِ غيرِ المشروعِ إلَى النظامِ المعلوماتيّ، والاطلاعِ علَى مَا يحتويهِ منْ بياناتٍ ومعلوماتٍ.

وقدْ تقومُ هذِهِ القطاعاتُ؛ لتسهيلِ الخدمةِ على العملاءِ وتطويرِ خدماتِهَا، بتبادُلِ تلكَ الصورِ الشخصية، أو صورِ جوازاتِ السفرِ الإلكترونيَّةِ،مَعَ فروعِهَا في مختلفِ المناطقِ بإرسالها عبرَ الإنترنت،ممَّا يعني احتمالَ تعرضِهَا للسرقةِ باختراقِ الحساباتِ الإلكترونيَّةِ لتلك القطاعاتِ منْ قِبَلِ الهاكرز أو محترفي جرائمِ التقنيةِ الحديثةِ والحاسبِ الآلي،ومن ثَمَّ الاطلاعُ عليهَا أو استخدامُهَا بشكلٍ غيرِ مشروعٍ في جهاتٍ أخرى، أو بيعُهَا لأشخاصٍ أو جهاتٍ مقابل المالِ.

---

(27) راجع : هشام محمد فريد رستم، قانون العقوبات، مرجع سابق، ص 178 وما بعدها.

(28) محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، المكتبة العصرية للنشر والتوزيع الطبعة الأولى، 2010م، ص 359.

إنَّ الإنترنت يحتوي على كميَّاتٍ هائلةٍ منَ المعلوماتِ المتبادَلةِ بسهولةٍ ويسرٍ ،والمشكلةُ تكمنُ في أنَّ تطويرَ الخدماتِ على الإنترنت يصاحبُهُ–عادةً– زيادةَ المعلوماتِ التي تُجْمَعُ عنِ المستخدمينَ، وتعرَّضُ هذه المعلوماتُ بعد ذلك لمخاطرِ الإفشاءِ للغيرِ[29].

فالإنترنت بخدماتهِ أرضٌ خصبةٌ لانتهاكِ الخصوصيةِ،وشبكةٌ بلا حدودٍ Sans Frontière، ففي خلالِ شهرٍ واحدٍ تحصَّلَتْ وكالةُ NASA على مليارااتِ المعلوماتِ منَ الرسائلِ المتبادلَةِ بينَ الأفرادِ،وهذه الأرقامُ تجعلُ الفردَ يشعرُ عندَ دخولِهِ إلَى الإنترنت بأنَّه مُراقَبٌ ومنتهَكُ الخصوصيَّةِ[30].

ويحدثُ ذلك عبرَ المواقعِ المختلفةِ،؛كمحركاتِ البحثMoteur de recherché التي تعتبرُ منْ أهمِّ وسائلِ الحصولِ علَى المعلوماتِ عبرَ الإنترنت[31]، ففي محركاتِ البحثِ يتركُ الشخصُ بعضَ البياناتِ التي تدلُّ علَى هويتِهِ ومُيُولِهِ،منْ خلالِ عملياتِ البحثِ التي يقومُ بها، ويُعَرِّضُهَا لمخاطرِ الاستخدامِ أو الإفشاءِ غيرِ المشروعِ، ولهذا تظهرُ أهميَّةُ تطبيقِ الحقِّ في النسيانِDroit à l'oubli لمستخدمِ محركاتِ البحثِ؛ في سبيلِ حمايةِ البياناتِ الشخصيَّةِ[32]. وهو ما ينطبِقُ كذلك علَى ملفاتِ تعريفِ الارتباطِ، ومواقعِ التواصُلِ الاجتماعيِّ ، التي قدْ تحصُلُ منهَا الشركاتُ والجهاتُ الأمنيَّةُ علَى البياناتِ والمعلوماتِ الشخصيةِ للمستخدمِ، كتلك التي تقومُ

---

(29)AndréJacquesAugand :Respect de la vie privée en matière de nouvelles technologies à travers des études de cas, UniversitéPanthéon-Assas (Paris2) , thèse de doctorat,2015,rèsumè.

(30) Marine Farshian: op,cit,p 1- 2 .

(31) يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، الجزء الثاني، الخصوصية وحماية البيانات في العصر الرقمي،اتحاد المصارف العربية، بيروت، 2002م، ص 185.

(32)Jean-Philippe Foegle: La CJUE, magicienneeuropéenne du « droit à l'oubli » numérique, Protection des donnéespersonnelles (Union européenne), La Revue des droits de l'homme, [En ligne], ActualitésDroits-Libertés, mis en ligne le 16 juin 2014,p 9.

بتجميعِهَا وتخزينِهَا هذه المواقعُ عنه، وتتعلَّقُ بوضعِهِ المادِيّ أو الاجتماعيّ أو الصحي... إلخ[33]. وليسَ بعيدًا عنْ ذلك أعمالُ الرقابةِ التي قدْ تحدُثُ عبرَ المواقعِ المختلفةِ باختراقِ حسابِ المستخدمِ بطرقٍ وبرامجَ مختلفةٍ في تطوُّرٍ مستمرّ، وتعجزُ هذه المواقعُ عن توفيرِ حمايةٍ فعَّالةٍ للبياناتِ الشخصيَّةِ، أو أنَّ المستخدمَ لم يكنْ علَى درايةٍ كاملةٍ وفَهْمٍ لسياسةِ الخصوصيةِ Politique de confidentialité المتعلقةِ بتلك المواقعِ.ومنْ أجلِ ذلك ظهرَتْ جمعياتٌ تهدِفُ إلى توعيَةِ الأفرادِ بحقوقِهِمْ في العالمِ الافتراضي، وكيفيةِ الدفاعِ عنها، وعنْ حرياتهم على الإنترنت، والعملِ على ضمانِ احترامِ المبادِئِ الأساسيَّةِ في العالم الافتراضي[34].

إنَّ كثيرًا منَ المواقعِ- شبكاتِ التواصُلِ الاجتماعيّ خاصَّةً - تحتفظُ بالبياناتِ الشخصيةِ للمستخدمِ ومعلوماتِهِ، حتى في حالِ إلغاءِ تفعيلِ حسابِهِ، ممَّا يعني أنَّ بياناتِهِ ومعلوماتِهِ الشخصيَّةَ لا تزالُ لدَى الموقعِ،وسيجدُهَا في حالِ إعادةِ تفعيلِ الحسابِ، ممَّا يعرِّضُهَا لمخاطرِ الاطِّلاعِ أو الاستخدامِ غيرِ المشروعِ[35]،

(33) سليم عبد الله الجبوري، الحماية القانونية للمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، بيروت، 2009م، ص 372.

(34)L'action de groupe de La Quadrature du Net contre les GAFAM, https://www.alain-bensoussan.com/avocats/action-de-groupe-quadrature-du-net-gafam/2018/05/30/.

(35) صدر عن الاتحاد الأوروبي في 26 أبريل 2016 تشريع لحماية الخصوصية والبيانات والذي سيدخلُ حيزَ التطبيقِ في 25 مايو 2018 م الذي يقضي في المادة 83 منه بفرضِ غرامةٍ تقدَّرُ بما يصل إلى 20 مليون يورو أو بنسبة 4% من العائدات السنوية للشركات العاملة في مجال الانترنت؛ كشبكاتِ التواصلِ الاجتماعي وغيرها في حال قيامها بالتصرف في البيانات والمعلومات الشخصية للمستخدمين بدون موافقتهم المحدد والواضحة على ذلك .

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Data Protection Regulation).

حيثُ تعتبرُ مواقعُ التواصلِ بيئةً خِصْبَةً للاعتداءِ علَى الخصوصيةِ المعلوماتيةِ، أو حياةِ الفردِ الخاصَّةِ في العالمِ الافتراضي، أو تعريضِ أمنِ الدولةِ القوميّ للخطرِ، أو ارتكابِ جرائمِ الإرهابِ والجرائمِ المنظمَّةِ، وتكونُ وملاذًا أمِنًا للمجرمينَ في ظلِّ غيابِ النصِّ التشريعي، والقدراتِ الفنيَّةِ والتقنيَّةِ على المواجهةِ.

الأمرَ الذي دفعَ الدولَ إلى سنِّ تشريعاتٍ لتنظيمِ استخدامِ شبكاتِ التواصُلِ الاجتماعي؛ للحَدِّ منْ مخاطرِهَا،ومنْ ذلك مشروعُ قانونِ تنظيمِ شبكاتِ التواصُلِ الاجتماعي داخلَ جمهوريةِ مِصْرَ العربيَّةِ[36].

أَضِفْ إلى ذلكَ مخاطرَ استخدامِ تقنياتِ البصماتِ في الشركاتِ والمؤسساتِ التعليميَّةِ؛ للتعرُّفِ على هويةِ الفردِ، وما قدْ يتبعُهُ منْ إنشاءِ قواعدَ بياناتٍ لتلكَ البصماتِ، ولذلك لا تَسْمَحُ اللجنةُ الوطنيةُ للمعلوماتيةِ والحرياتِ

(36) تلزم المادة الأولى من المشروع مقدمي خدمات الإنترنت التابعين لها بإنشاء شبكاتٍ للتواصل الاجتماعي في مصر، على أنْ يحدثَ ذلك بالتنسيق مع الجهاز القومي للاتصالات ، ووفقاً للمادةِ الثانية من المشروعِ تُشَكَّلُ لجنةٌ أو فريقٍ بالجهاز القومي للاتصالات يتكفَّلُ بأعمال الإشراف والمراجعة والرقابة على مقدمي خدمات الانترنت في مصر، أما المادة الثالثة من المشروع فقد حظرت فتح حساب على مواقع التواصل الاجتماعي ألا عن طريق بطاقة الرقم القومي ، و أن لا يقلَّ عمرُ المستخدم عن 18 سنة ، ولا شكَّ في أنَّ هدا النصَّ يهدِفُ إلى التحقُّقِ من هوية صاحب الحساب؛ لملاحقته إذا ما تطلَّبَ الأمرُ ذلك، ، كما أجازت المادة الرابعة لجهات التحقيق المختصة متى قامت أدلةٌ على وجود حساباتٍ على شبكة التواصل الاجتماعي أو مواقعَ تضرُّ بالأمن القومي أو تنتهكُ حرمةَ الحياة للأفراد، أن تأمر بحجبها من خلال العرض على المحكمة؛ وذلك لإزالة مصدر الضررِ أو الانتهاك، ومحو آثاره في العالم الافتراضي، في حين تعاقب المادة الخامسة بالحبس مدةً لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنيهٍ، ولا تجاوز مائةَ ألفِ جنيهٍ، أو بإحدى هاتين العقوبتين كلَّ من قام بفتحِ حسابٍ وهميٍّ (غير حقيقي) على شبكة المعلوماتِ، أو دخلَ عمداً على موقع أو حساب ينتهك حرمةَ الحياةِ الخاصَّةِ للغير .

http://www.albawabhnews.com/3134232.

في فرنسا CNIL[37] باستخدامِهَا إلَّا إذَا كانتِ المتطلباتُ الحتميةُ للأمنِ والنظامِ العام تبرّرُ ذلكَ[38] ، أو استخدامِ شركاتِ النقلِ نظامَ تحديدِ الموقعِ الجغرافيّ في سيارتها؛ منْ أجلِ توجيهِ أقربِ سيارةٍ لموقعِ العميلِ، وكذلك مراقبةِ السائقينَ عندَ القيامِ بعملهم، لما لهذه الأجهزةِ منْ خطورةٍ علَى الحرياتِ الفرديةِ، فإنَّ اللجنةَ الوطنيةَ للمعلوماتيةِ والحرياتِ في فرنسا تطلبُ أنْ يسمحَ النظامُ للسائِقِ بإيقافهِ عن العملِ عندَ سفرهِ الشخصي بالسيارةِ؛ فليسَ ذلكَ كالذهابِ إلَى المنزلِ عندَ الانتهاءِ من العملِ أو زيارةِ صديقٍ... إلخ[39].

ومنْ تلكَ الخدماتِ –أيضًا– سحابُ الحوسبةِ Cloud Computingالتِي تُعَدُّ إحدَى أساليبِ الحوسبةِ، تُقَدَّمُ فيها الموارِدُ الحاسوبيةُ كخدماتٍ، ويُتَاحُ للمستخدمينَ الوصولُ إليها عبرَ الإنترنت، ويشملُ خدمةَ الويب 2.0، وغيرها منَ التطبيقاتِ التي تشتركُ في فكرةِ الاعتمادِ علَى الإنترنت؛ لتلبيةِ متطلباتِ المستخدمِ، بأنْ يطلبَ العميلُ الخدمةَ منْ مزوّدِ الخدمةِ، ويختارَ نظامَ التشغيلِ... إلخ[40]. ومع أنَّ البياناتِ تُخـزَّنُ في السحابةِ، ويقتصرُ

(37) تتولى هذه اللجنةُ مراقبةَ تطبيقِ قانون المعلوماتية والحريات والملفات في فرنسا، والتأكدَ من تقيد الجهات المختلفة بأحكامه، وقد أُنْشِئَ – بمقتضى المادة 68 من التشريع الأوروبي الجديد المتعلق بالخصوصية وحماية البيانات لسنة 2016 مجلسُ حمايةِ البيانات الأوروبي Le comitéeuropéen de la protection des données كهيأةٍ تابعةٍ للاتحاد، ولها شخصيةٌ قانونيةٌ مستقلةٌ، وتتكون من مفوضي حماية البيانات الشخصية في الدول الأعضاء بالاتحاد، ومن مهامه مراقبةُ التطبيقِ السليمِ لهذا التشريعِ الجديدِ وضمَانُهُ، وتقديمُ المشورة لمجالس حماية البيانات الشخصية في الدول الأعضاء بالاتحاد، وتقديمُ أيَّ مقترحاتٍ لتعديل هذا التشريع الجديدِ، و وغيرها من المهام المنصوصِ عليها في المادة 70.

(38)Alexis Baumann:Nouvelles décisions de la CNIL en matière de biométrie,Publié le: http://www.declaration-cnil.com/Articles/A20060130-nouvelles-decisions-cnil-biometrie.php.

(39)Hélène Lebon: Les prochaines recommandations de la CNIL en matière de géolocalisation, Publié le: http://www.declaration-cnil.com/Articles/A20051020-geolocalisation-recommandations-cnil.php.

(40)www.m-aljelban.com/vb/archive/index.php/t-166html,

الدخولُ إليها على الأشخاصِ المسموحِ لهم، إلَّا أنَّ النظامَ يُشَكِّلُ خَطَرًا على البياناتِ والمعلوماتِ الشخصيةِ الإلكترونيةِ؛ وتتجلَّى هذِهِ الخطورةُ في إمكانيةِ الوصولِ إلَى البياناتِ المخزَّنةِ، والاطِّلاعِ عليهَا مِنْ دُونِ موافقةِ المعنيِّ أو علمِهِ، كاطلاعِ المهندسِ المسْؤُولِ عن السيرفر في السحابة،كمَا أنَّ كثرةَ وجودِ السيرفر يجعلُ منَ الصعبِ تحديدَ السيرفر المختزنةِ فيه البيانات، أو تحديدَ الدولةِ الموجودِ بها[41]، واحتمال عدمِ حذفِ الملفاتِ المحتويةِ على البياناتِ عندما يطلبُ المعني بالبياناتِ منَ الشركةِ مسحَ البياناتِ، وهذا يجعلُ الفردَ أمامَ خطرٍ مستمرٍّ بتهديدِه بالإفشاء،ناهيك عنْ خطرِ تعرُّضِ البياناتِ المختزنةِ في السحابةِ للضياع[42].

إنَّ الكمَّ الهائلَ منَ البياناتِ والمعلوماتِ الموجودَ بنظامِ سحابِ الحوسبةِ جعلَ السلطاتِ في مختلفِ الدولِ تطلبُ الدخولَ السهلَ إلَى النظامِ، والحصولَ على البياناتِ والمعلوماتِ،الأمرَ الذي جعلَ التشريعاتِ الأوروبيةِ تفرضُ علَى الشركاتِ التزامَ بحمايةِ تلك النُّظُمِ المعلوماتيةِ[43].

ومنْ تلك المخاطرِ –أيضًا– انتشارُ الفيروساتِ في الإنترنت، وهي برامجُ يمكنُهَا التأثير على كافةِ برامجِ الحاسبِ الأخرى، بأنْ تجعلَهَا نسخةً منهَا، أو أنْ تعملَ على مسحِ كافَّةِ البرامجِ الأخرَى، ومنْ ثَمَّ تعطيلُها عنِ العملِ[44]، إذْ تظهرُ على خلافِ الحقيقةِ بأنَّهَا برامجُ مفيدةٌ أو مساعدةٌ للبحثِ،فَيَسْتَقْبِلَهَا المستخدمُ، فيحدثُ عنْ طريقِهَا التجسسُ على معلوماتهِ، وتعرضه فيما بعدُ لمخاطرِ الابتزازِ وإفشاءِ المعلوماتِ أو إتلافِهَا أو سرقَتِهَا، كمَا أنَّ

(41) Emmanuel sordet: le cloud computing, unevraiefausserevoltion?, article, sure:www.ce4arab.com/vb7/archive/index.php/t-273313.html

(42) www.almashned.com/archive/index.php/t-75131.html

(43)Etienne Papin: Le cloud computing et la sécurité des données,sur: www.claranet.fr/blog/2014-02-24-le-cloud-computing.

(44) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص 68.

الإنترنت ساعدَ علَى انتشارِ جرائمِ قرصنةِ البرامجِ؛ لِمَا يُتِيحُهُ الإنترنت منْ إمكانيةِ نسخِ البرامجِ الباهظَةِ الثمنِ في زمنٍ قصيرٍ، وكذلك تسويقِ تلكَ البرامجِ عبرَ المواقعِ المختلفةِ(45).

بالإضافةِ إلى مخاطرِ تقنياتِ النانوNanotechnologiesوتعني تكنولُوجيَا تعديلِ الذرَّةِ أو الجزيئاتِ؛ لصناعةِ منتجاتٍ جديدةٍ(46)، فالنانو متر هوَ جزءٌ منْ ألفِ مليونٍ منَ المتر، وجزيئاتُه تُعطي المادةَ الداخلةَ في تركيبِهَا خصائصَ جديدةً، والجسيماتُ تعطي مفاهيمَ جديدةً، مِمَّا يقودُ إلَى سُلوكٍ جديدٍ، يعتمدُ علَى حجمِ تلكَ الجسيماتِ، ويعتبرُ النانو منَ الاكتشافاتِ المُهِمَّةِ في عدَّةِ مجالاتٍ، وأتاحَ المجالَ لثوراتٍ مستقبليةٍ سيترتبُ عليهَا ظهورُ التقنيةِ بمظهرٍ جديدٍ في العديدِ منَ التطبيقات(47).

ففي مجالِ الإلكتروناتِ نلاحظُ أنَّ البطاقاتِ المستخدمةَ في الحاسبِ في عالمنا اليومَ التي يُقَدَّرُ سمكها ببضعَةِ ملليمتراتٍ هيَ فِي حقيقَتِهَا تتكوَّنُ من خمسِ طبقاتٍ، ومع انتقاصِ حجمِهِ ازدادتِ القدرةُ والفعاليةُ للحاسبِ فأكسَبَهُ سرعةً وقدرةً كبيرةً للقيامِ بعملياتهِ المختلفةِ(48).

(45) نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، 2004، ص 24.

(46) صفات سلامة، النانو تكنولوجي عالم صغير ومستقبل كبير، الدار العربية للعلوم ناشرون، بيروت، 2009 م، ص20.

(47)https://nano.ksu.edu.sa/ar/nanotech-introduction

(48)http://kenanaonline.com/users/ahmedkordy/posts/315451.

غيرَ أنَّ هذه التقنيةُ من شأنِهَا توسيعُ دائرةِ الرقابةِ على الفردِ، فقدْ أدَّتْ إلى تصغيرِ الأجهزةِ وتقويةِ فعاليتها، وتطويرِ قدراتِهَا التخزينيةِ، فالحاسباتُ وأجهزةُ التجسُّسِ قدْ تكونُ في ظلِّ هذِه التقنيةِ صغيرةَ الحجمِ أكثرَ منْ أيِّ وقتٍ مضَى، فيَصْعُبُ اكتشافُهَا واحتمالُ وجودِهَا في أماكنَ لم تكنْ متوقعةً في السابقِ.

مِمَّا جعلَ هذِه التقنيةَ تُشَكِّلُ خطرًا حقيقيّاً على حقوقِ الإنسانِ وحرياتِهِ، كحقِّه في احترامِ الحياةِ الخاصَّةِ عندَ استخدامِ أجهزةِ الشرطةِ أو العدالةِ الجنائيةِ لتقنيةِ النانو(49).

وهكذَا فإذا كانتْ حوسبةُ البياناتِ قدْ سهَّلَتْ حياةَ المواطنينَ، بالإضافةِ إلى مقدمي الخدماتِ المختلفةِ في الدولةِ، فينبغي ألَّا تُسْتَخْدَمَ تلك البياناتِ بشكلٍ سيّءٍ، لذلك تفرِضُ العديدُ منَ الدولِ القيودَ على جمعِ تلكَ البياناتِ واستخدامِهَا ومعالجتها(50).

وفي ظلِّ المعطياتِ السابقةِ للتقنيةِ الحديثةِ تظهرُ أهميَّةُ توفيرِ حمايةٍ فعالةٍ للخصوصيةِ المعلوماتيةِ؛ تأكيدًا على حقٍّ دستوريٍّ للشخصِ؛وهو حقُّه في السريَّةِ أو الخصوصيةِ، فضلاً على أنَّ حمايةَ تلك البياناتِ يُعَدُّ عاملاً مُهِمًّا فِي نجاحِ الخدماتِ الإلكترونيةِ المختلفةِ بالدولةِ.

(49)Quellessont les questions éthiquesposées par les nanotechnologies ?:www.cnrs.fr/cw/dossiers/dosnano/decouv/04/04_4/04_4.htm.

(50)Stéphane Tijardovic: La protection juridique des données personnelle ,Vers une nécessaire adaptation de la norme juridique aux évolutions du monde numérique, Publié le :https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-185.htm.

الفرعُ الثاني

وضعُ البياناتِ الشخصيَّةِ الإلكترونيَّةِ في قانونِ العقوباتِ الفرنسي

يكفلُ المشرّعُ الفرنسيُّ الحمايةَ لحقوقِ الإنسانِ وحرياتِهِ في مجالِ المعلوماتيةِ، عنْ طريقِ تجريمِ الاعتداءِ على نُظُمِ معالجةِ البياناتِ، بالإضافةِ إلى تجريمِ الاعتداءِ على البياناتِ والمعلوماتِ الشخصيةِ ذاتِهَا، وفي ذلكَ حمايةٌ مباشرةٌ وغيرُ مباشرةٍ للبياناتِ الشخصيَّةِ الإلكترونيَّةِ أو حقِّ الفردِ في الخصوصيةِ في العالمِ الافتراضي.

أولاً: الاعتداءُ علَى نُظُمِ المعالجةِ الآليَّةِ للبياناتِ الشخصيَّةِ:

يعاقبُ المشرّعُ الفرنسيُّ على الدخولِ في نُظُمِ المعالجةِ الآليةِ للبياناتِ الشخصيَّةِ، أو البقاءِ فيهَا، أو الاعتداءِ علَى سيرِهَا، والتلاعبِ بالبياناتِ والمعلوماتِ الشخصيةِ، وهو ما سنحاولُ بيانهُ فيمَا يأتي:

1. الدخولُ أو البقاءُ عنْ طريقِ الاحتيالِ في نُظُمِ معالجةِ البياناتِ:

تحتوي أنظمةُ معالجةِ البياناتِ على العديدِ منَ البياناتِ والمعلوماتِ الشخصيةِ بمختلفِ أنواعِهَا، مِمَّا جعلَ الدخولَ أو البقاءَ غيرَ المشروعِ لتلكَ الأنظمةَ يهدِّدُ سِرِيَّةَ البياناتِ والمعلوماتِ الشخصيةِ أو الخصوصيةِ المعلوماتيةِ وسَلامَتَهَا، وإلحاقَ الضرَرِ بالمعني.وعليه تعاقبُ المادةُ 323-1 عقوبات **والمعدلة بالقانون رقم 912 لسنة 2015 م**[51]علَى فعلِ الدخولِ أو البقاءِ غيرِ المشروعِ في نظامِ معالجةِ البيانات بالحبسِ سنتينِ، وغرامةِ 60 ألفَ يورو كلَّ منْ يقومُ عنْ طريقِ الاحتيالِ بالدخولِ أو البقاءِ في كاملِ نظامِ معالجةِ البياناتِ أو في جزءٍ منه، وتشدِّدُ العقوبةَ لتكونَ الحبسُ ثلاثَ سنواتٍ و غرامةَ 100 ألفِ يورو إذا ترتَّبَ علَى الفعلِ محوُ البياناتِ الموجودةِ في النظامِ، أو حذفُهَا أو تعديلُهَا، أو تعطيلُ عملِ النظامِ أو إضعافُه، في حين قدْ تصلُ العقوبةُ السالبةُ للحريةِ إلى خمسِ سنواتٍ، وغرامةِ 150 ألفَ يورو إذَا وقعَ الفعلُ على أنظمةِ معالجةِ البياناتِ

(51)Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

الشخصيةِ التابعةِ للدولةِ، وتغليظُ العقوبةِ في هذه الحالاتِ قدْ يُعْزَى لأهميةِ البياناتِ وحساسيةِ المعلوماتِ التي يحتويها النظامُ، وخطورةِ الجاني الذي تمكَّنَ منِ اختراقِ منظومةِ الحمايةِ الخاصَّةِ بتلكَ النُّظُمِ، التي تمتازُ عادةً بتشديدِ الحمايةِ ضِدَّ الاختراقِ عمَّا هوَ واردٌ في أنظمةِ معالجةِ البياناتِ التابعةِ للقطاعِ الخاص، فهي من الجرائمِ الشكلية التي لا يلزَمُ لقيامِها تحققُ نتيجةٍ معينةٍ، بل تقعُ تامَّةً بمجردِ ارتكاب السلوكِ الإجرامي بفعلِ الدخول أو البقاء في النظامِ عن طريقِ الاحتيالِ frauduleusement، وإنْ لم يقعْ ضَرَرٌ للبياناتِ أو المعلوماتِ، غيرَ أنَّ المشرّعَ يشدّدُ منَ العقوبةِ في حال تحقُّقِ حذفِ أو تعديلِ البيانات المختزنة بالنظامِ، أو تعطيلِ عملِ النظامِ، ويتحقَّقُ الدخولُ باتصالِ الجاني بالنظامِ بأيّ طريقةٍ منَ الطرق التي يمكنُ من خلالها أنْ يتحقَّقَ الاتصالُ بالنظام[52]، سواءٌ أكانَ باستخدامِ قرصٍ مُدْمَجٍ أم جهازِ حاسبٍ آليٍّ آخرَ لدَى الجاني[53].

وجميعُ المعداتِ أوِ الأجهزةِ أو البرامجِ لحفظِ البياناتِ أو تخزينِهَا أو معالجتِهَا أو التحكُّمِ فيها أو عرضِهَا أو إرسالِهَا أو استقبالِهَا بشكلٍ تلقائي[54]، أو غيرها من البرامجِ الخبيثةِ التي تسهّلُ أو تسمحُ بارتكابِ الجرائمِ المنصوصِ عليها في المواد 323إلى 323-3 من قانونِ العقوبات، ولا يشترطُ -كما هو الحالُ في الاتفاقيةِ

(52) غنام محمد غنام ،دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة، 2010م، ص128.

(53) عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، 1995م، ص127.

(54)Murielle Cahen:Loi : Intrusion dans un systèmeinformatique (hacking), publié le 01/05/2009 ,sur : https://www.legavox.fr/blog/murielle-cahen/intrusion-dans-systeme-informatique-hacking-314.htm.

الأوروبيةِ[55] – أنْ تكونَ هذه البرامجُ مصمَّمةً في الأساسِ لارتكابِ تلك الجرائمِ[56]، أوِ استخدامِ برامجَ مخفيةٍ يمكنُ إرسالها عبرَ البريدِ الإلكترونيّ، وعن طريقِهَا يُتَحَكَّمُ في الحاسبِ الآلي وإدارته عنْ بُعْدٍ، أو استهداف كلمات مرورِ النظامِ المعلوماتي، واستخدام برامج فكِّ التشفيرِ للمعلوماتِ المشفرةِ[57]، وإن كانَ المشرّعُ الفرنسيُّ يوفرُ الحمايةَ للنظامِ من الدخولِ أو البقاء غيرِ المشروعِ، وإن لم يكنِ الدخولُ إليه يتطلَّبُ كلمةَ مرورٍ pass word [58]. فالاختراقُ يتحقَّقُ وفقاً للنصّ السابقِ بالدخولِ غيرِ المشروعِ أو المصرَّحِ به للنظام[59]، عن طريقِ برامجَ حديثةٍ وتقنيةٍ متطورةٍ لا يستخدمُهَا عادةً إلَّا من يملكُ الخبرةَ والدرايةَ في هذا المجالِ[60]، ومن أشهرِ تلك

(55)la Convention sur la cybercriminalité du Conseil de l'Europe.

(56)Etienne Wery :Le nouvel article 323-3-1 du Code pénal : luttercontre les virus, d'accord, mais attention aux effetspervers,Publié le 02/09/2004 ,sur : https://www.droit-technologie.org/actualites/le-nouvel-article-323-3-1-du-code-penal-lutter-contre-les-virus-daccord-mais-attention-aux-effets-pervers/.

(57)http://www.murielle-cahen.com/publications/p_intrusion.asp.

(58)Alain Bensoussan: Internet, aspects juridiques,éd Hermes, 1998, p. 198,Murielle Cahen:Loi : Intrusion dans un systèmeinformatique (hacking), **publié le 01/05/2009 ,sur** : https://www.legavox.fr/blog/murielle-cahen/intrusion-dans-systeme-informatique-hacking-314.htm

(59)Murielle Cahen:Loi : Intrusion dans un systèmeinformatique (hacking), publié le 01/05/2009 ,sur : https://www.legavox.fr/blog/murielle-cahen/intrusion-dans-systeme-informatique-hacking-314.htm.

(60) خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي ،الإسكندرية، الطبعة الأولى، 2009م، ص 242.

البرامجِ ما يُعرَفُ بحصانِ طروادة[61]. كذلك كأنْ يستخدمَ شخص برامجَ منْ شأنِهَا اختراقُ كلمةِ المرورِ الخاصَّةِ بالحاسبِ الآليّ؛ المحمولِ الخاصّ بشخص أخر، ونقلُ البياناتِ من حاسبٍ لآخرَ؛ للاطلاعِ علَى ما يحتويه من بياناتٍ؛وما في ذلك من مساسٍ بسريةِ تلك المعلوماتِ، فالجريمةُ تتحقَّقُ بالدخولِ إلى نظام التجهيزِ أو المعالجةِ الآليةِ للبياناتِ الشخصيةِ، المتكوّنِ من وحدةٍ أو أكثرَ من وحداتٍ معالجةِ البياناتِ وأجهزةِ التدقيقِ والاتصالِ، التي تساهمُ في تحقيقِ نتيجةٍ معينةٍ، مع عدم وجودِ ترخيصٍ أو إذْنٍ بالدخولِ.

أمَّا البقاءُ في النظامِ فقد يسبقُهُ دخولٌ مشروعٌ أو قانونيٌّ للنظامِ[62] أو غيرُ مشروعٍ، ففي الحالةِ الأولى يُسْأَلُ الجاني عن جريمةِ البقاءِ بطريقِ الاحتيالِ في النظامِ بعد الدخولِ المشروعِ إليه ،كأنْ يكونَ المستخدمُ قد استنفذَ الوقتَ المحدَّدَ أو المسموحَ به للدخولِ،إلَّا أنَّه استمرَ في البقاءِ بالنظامِ، مهمَا كانَ غرضُهُ من ذلك البقاءِ، من ذلك أنْ يتوصلَ شخصٌ عن طريقِ المصادفةِ إلى الاطلاعِ على رمزِ الحمايةِ الخاصّ بالنظام، ويبقى بداخلهِ[63] على اعتبارِ أنَّ ذلك يُعَدُّ طريقةً من طرقِ الدخولِ غيرِ المشروعِ إلَى النظامِ[64]،مِمَّا يهدِّدُ سريةَ البياناتِ والمعلوماتِ الشخصيةِ المختزنةِ بالنظامِ.

فيعاقبُ المشرِّعُ على فعلِ الدخولِ عن طريقِ الاحتيالِ للنظامِ إذْ يتطلبُ المشرِّعُ لقيامِ الجريمةِ توفرَ القصدِ الجنائيّ العامِ بعنصرِ العلمِ والإرادةِ؛ بأنْ تتجهَ إرادةُ الجاني إلى الدخولِ أو البقاءِ مع علمِهِ بعدم مشروعيةِ ذلكَ، ولا قيامَ لهذه الجريمةِ إذا تخلَّفَ أيُّ عنصرٍ من عناصرِ القصدِ الجنائيّ،وذلك كأنْ يعتقِدَ المستخدمُ مشروعيَّةَ

(61)منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص 46-47.

(62)https://ssi.ac-strasbourg.fr/referentiels/le-juridique/les-themes/la-cybercriminalite.

(63) هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،1992، ص 39.

(64) مدحت رمضان ،الحماية الجنائية للتجارة الإلكترونية،دار النهضة العربية،القاهرة،2000،ص41.

الفعلِ، كمَا لا يشترطُ لقيامِ الجريمةِ وجودُ قصدٍ خاصّ لدى الجاني، ولا عبرةَ بالباعثِ على ارتكابهِ للجريمةِ[65]، فالباعثُ ليسَ ركناً من أركانِ الجريمةِ ولا عنصراً من عناصرها[66].

وجديرٌ بالذكرِ أنَّ الجريمةَ تقعُ منْ أيّ شخصٍ بغضِ النظرِ عن صفتِه، فلا يشترطُ أنْ يكونَ من العاملين في مجالِ نُظُمِ معالجةِ البياناتِ،كمَا يستوي أنْ تكونَ لديه درايةٌ وفهمٌ بأسلوبِ التشغيل أم لا، ويكفي لقيامِ الجريمةِ أن يكونَ الجاني ليس له الحقُّ في القيامِ بما صدرَ عنه، ولا تقومُ الجريمةُ إذَا دُخِلَ إلى عنصرٍ لا علاقةَ له بنظامِ معالجةِ البياناتِ، أو مجرد الإطلاعِ على الحاسب[67]، إذْ يهدِفُ النصُّ إلى حمايةِ نظمِ المعالجة الآلية للبيانات.

2. الاعتداءُ علَى سَيْرِ نُظُمِ المعالجةِ الآليَّةِ للبياناتِ والتلاعبُ بالبياناتِ:

تعاقِبُ المادةُ 323-2 عقوبات،**المعدلةُ بالقانونِ رقم 912لسنة 2015**[68] علَى فعلِ إعاقةِ سيرِ نظمِ معالجة البياناتِ أوِ الإخلالِ بها أو تشويهِها – بالحبسِ خمسِ سنواتٍ، وغرامةٍ لا تزيدُ علَى 150 ألفَ يورو، وتتحقَّقُ الإعاقةُ أو العرقلةُ Entraverبمنعِ النظامِ منَ العملِ بشكلٍ جزئيّ أو كاملٍ،فتشملُ جميعَ الممارساتِ التي تؤدّي

(65) راجع :صالح شنين، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان،2013-2012، ص 78-79.

(66) نقض جنائي مصري 2 أبريل 2014م، الطعن رقم 12754 لسنة 82 ق .

(67) على عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، كتاب بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتجية ومركز تقنية المعلومات بالجامعة،1-3 مايو 2000م، الطبعة الثالثة 2004م، ص 600-601.

(68)Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

إلـى عرقلـةِ النظـامِ، سـواءٌ أكـانَ ذلـكَ بـالإتلافِ أمِ التخريـب[69]، فـي حـين يتحقَّـقُ الإخـلالُ أو التشـويهُ Fausserبإدخالِ كلِّ ما منْ شأنهِ أنْ يُسَبِّبَ خللًا في عملِ النظامِ؛ أي أنَّ النظـامَ يعملُ فـي هذه الفرضيةِ ولكنْ بشكلٍ غيرِ طبيعي أو بخلافِ ما هو معتادٌ[70]، فلا يؤدِّي العملَ المطلوبَ منه كالمعتادِ.

وتتحقَّقُ هذه الأفعالُ بطريقةٍ ماديةٍ عن طريقِ التحطيمِ أو العنفِ ضدَّ الأنظمةِ،أو بطريقةٍ معنويـةٍ عن طريقِ إدخـال الفيروسـاتِ التـي يمكـنُ أن تحقِّقَ هذا الغرضَ [71]، كالـدخولِ علـى البيانـاتِ وعرقلـةِ عملِ نظـمِ معالجـةِ البيانـاتِ لشركةٍ من الشركات [72]، وهي منَ الجرائمِ العمديَّةِ[73]، فيلزمُ أنْ يتعمَّدَ الجاني إعاقةَ عملِ النظـامِ أو الإخلالِ بـهِ لقيام الجريمـة.ولا يُشترَطُ أنْ تقعَ تلك الأفعالُ علـى جميـعِ عناصرِ النظـامِ، بل يكفـى أنْ تؤثرَ علـى بعضِ تلك العناصرِ، سواءٌ أكانتْ عناصرَ ماديَّةً كالحاسب الآلي نفسِـهِ أمْ عناصر معنوية كالبيانات[74].

وقد عملَ المشرِّعُ الفرنسيُّ على حمايةِ البياناتِ منَ العبَثِ بها بمقتضَى نصِّ المادةِ 323-3؛ وذلك لعدمِ كفايةِ القواعد العامةِ في تزويرِ المحرراتِ في توفيرِ حمايةٍ ملائمةٍ للبياناتِ منَ العبثِ أو التلاعبِ بها؛ وذلك لعدمِ

---

(69) هدى حامد قشقوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الإلكتروني، كتاب بحوث مؤتمر القانون والكمبيوتر والإنترنت 1-3 مايو 2000م، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتجية ومركز تقنية المعلومات بالجامعة، الطبعة الثالثة 2004، ص 893.

(70) غنام محمد غنام، مرجع سابق، ص 147،148.

(71) علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، مرجع سابق، ص 605.

(72) لا يجوزُ لربِّ العملِ الاطلاعُ على البياناتِ الشخصيةِ الموجودةِ بالحاسبِ الآلي للعاملِ، لاَ سِيَّمَا تلك الموجودةُ بالقرص الصلبِ، ما لم يكن ذلك بسببِ وجودِ خطرٍ أو حالةٍ خاصةٍ risqueoud'événementparticulier تبرّرُ ذلك، وفي هذه الحالة يُطَّلَعُ حتى منْ دونِ إخطارِ العامل بذلك.

Alexis Baumann: op,cit.

(73)https://ssi.ac-strasbourg.fr/referentiels/le-juridique/les-themes/la-cybercriminalite.

(74) علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، مرجع سابق، ص 604.

توافرِ شرطِ المحررِ في البيانات المعالجةِ آلياً [75]، فتعاقبُ المادةُ 323-3 عقوبات **المعدلة بالقانون رقم 912 لسنة 2015** بالحبسِ خمسَ سنواتٍ وغرامةِ 150 ألفَ يورو على فعلِ إدخالِ بياناتٍ عن طريقِ الاحتيالِ للنظامِ أو التعديلِ أو المسحِ أو الاستخراجِextraireأو الاحتفاظِ dtenir أو النسخِ reproduire أو النقلِtransmettreللبياناتِ عن طريقِ الاحتيال. ويتحقَّقُ فعلُ الإدخالِ بإضافةِ بياناتٍ جديدةٍ على الدعامةِ الخاصَّةِ بالبياناتِ عنْ طريقِ الاستخدامِ السيِّءِ لبطاقاتِ الائتمانِ أو السحبِ، سواءٌ أكانَ من صاحبِهَا الشرعي أمْ من غيرِهِ،كما يتحقَّقُ فعلُ الإدخالِ بإضافةِ بياناتٍ جديدةٍ غيرِ موجودةٍ بالدعامةِ عن طريقِ الفيروساتِ،في حينِ أنَّ المسحَ يتحقَّقُ بإزالةِ كلِّ البياناتِ الموجودةِ بالدعامةِ أو بعضِهَا، أو نقلِ جزءٍ منها إلى المنطقةِ الخاصَّةِ بالذاكرةِ وتخزينِهَا، أمَّا التعديلُ فيتحقَّقُ بتغييرِ البياناتِ الموجودةِ واستبدالها ببياناتٍ أخرى، عنْ طريقِ البرامج المختلفةِ المستخدمةِ في هذا المجالِ[76]، كأنْيحدثُ التلاعبُ بالبياناتِ المعالجةِ آلياً عن طريقِ إدخالِ بياناتٍ أخرى للبياناتِ الموجودةِ بالنظامِ؛ للمَسَاسِ بصحتِهَا، أو محوِ البياناتِ بتدميرِهَا إلكترونيّاً كلياً أو جزئياً [77].

جديرٌ بالذكرِ أنَّ المادةَ 323-3 كانتْ تعاقبُ على ثلاثةِ أفعالٍ فقط، وهي أفعالُ الإدخالِ والمسحِ والتعديلِ،وأضيفت الأفعالُ الأخرَى بعد تعديلِهَا بمقتضَى المادةِ **16** منَ القانونِ رقم **1353**لسنة **2014 م**[78]، ولا شكَّ في أنَّ هذا التعديلَ قدْ وسَّعَ من الحمايةِ المقررةِ لسلامةِ البياناتِ المعالجةِ آلياً منَ التلاعبِ أو العبثِ، لاَ سِيَّمَا وأنَّ القواعدَ التقليديَّةَ لا تكفي لحمايتِهَا،وقد كانتِ البياناتُ المختزنةُ بنُظُمِ معالجةِ البياناتِ في حاجةٍ إلَى الحمايةِ منَ الأفعالِ التي جاءَ بها التعديلُ الأخيرُ،وذلك بالعقابِ على فعلِ استخراجِ البياناتِ منَ المكانِ المختزنةِ

(75) غنام محمد غنام، مرجع سابق،ص 152.

(76) علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، مرجع سابق، ص 608.

(77) هدى حامد قشقوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الإلكتروني، مرجع سابق، ص 893.

(78)Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la luttecontre le terrorisme.

به في نُظُمِ المعالجةِ؛ كذاكرةِ التخزينِ والاحتفاظِ، أو نسخِ البياناتِ، أو نقلهَا منْ دونِ أنْ يكونَ للشخصِ الحقَّ في ذلك،عن طريقِ التحايُلِ، ويتحقَّقُ ذلك باستخدامِ البرامجِ المختلفةِ؛ كالفيروساتِ وغيرهَا.

كمَا يتطلب المشرّعُ لقيامِ الجريمةِ أنْ تحدثَ الأفعالُ السابقةُ عن طريقِ الاحتيالِ أو الغشّ وهذا يعني أنها من الجرائمِ العمديةِ التي يلزَمُ لقيامِهَا توافرُ القصدِ الجنائي،مع ملاحظةِ أنَّ المشرّعَ يعاقبُ على تعديلِ البياناتِ أو مسحها، وإن حدثَ ذلك عن طريقِ الخطأ وفقًا للمادة 323-1 عقوبات[79].

تجدرُ الإشارةُ إلَى أنَّ المشرّعَ الفرنسيَّ يعاقبُ بمقتضَى المادة 323-3-1 عقوبات والمعدَّلةِ بالقانونِ رقم 1168 لسنة 2013 م[80] كلَّ منْ يقومُ في غيرِ الأحوالِ المشروعةِ باستيرادِ أو حيازةِ أو توفيرِ الأدواتِ والمعدَّاتِ الحاسوبيةِ المستخدمةِ في الجريمةِ المنصوصِ عليهَا في الموادِ 323-1 إلى 323-3 عقوبات، بالعقوبةِ المقررةِ للجريمةِ نفسِهَ وبعقوبةٍ أشدُّ في حالِ استخدمتْ تلك المعداتِ في ارتكابِ جرائمَ أشدُّ خطورةً. ولا شَكَّ فِي أنَّ في ذلك توسيعًا لنطاقِ الحمايةِ المقررةِ لنظمِ المعالجةِ الآلية للبياناتِ، وما تحتويهِ من معلوماتٍ.أمَّا القانونُ رقم 912لسنةِ 2015 مفقد شدَّدَ من عقوبةِ الغرامةِ المقررةِ للجرائم المنصوصِ عليها في الموادِ

323-1 إلى 323-3 عقوبات، ويُلاحَظُ أنَّ المشرّعَ الفرنسيَّ يعاقبُ علَى حيازَةِ تلكَ البرامجِ الخبيثةِ، ما لم تكنْ حيازتُها لسببٍ قانوني أ و عادلٍ «saufjuste motif»

ويَرى البعضُ – وبحقٍّ – أنَّ هذِه العبارةَ يحيطُ بها الغموضُ وتثيرُ مخاوفَ المتخصصينَ في تقنيةِ المعلوماتِ، الذينَ قد يقومونَ بحيازةِ تلكَ البرامج؛ لغرضِ معرفةِ الثغراتِ الأمنيةِ أو عيوبِ أنظمةِ الكمبيوتر، الأمرَ الذي كانَ

(79) غنام محمد غنام، مرجع سابق، ص 153.

(80)Loi n° 2013-1168 du 18 décembre 2013 relative à la programmationmilitaire pour les années 2014 à 2019 et portantdiverses dispositions concernant la défense et la sécuriténationale .

يقتضي صياغةَ المادةِ بشكلٍ أكثرَ وضوحاً[81]. كمَا أنَّ المادةَ 323-4-1 عقوبات المضافةَ مؤخراً بمقتضى المادة **17** منَ القانونِ رقم **1353**لسنة **2014م** والمعدَّلةَ بالقانونِ رقم **912**لسنةِ**2015م** تُغَلِّظُ العقوبةَ المقررةَ للجريمةِ المنصوصِ عليهَا في المواد 323-1 إلى 323-3-1 عقوبات متى ارتكبتْ عن طريقِ العصاباتِ المنظمةِBandeorganisée ضدَّ أنظمةِ معالجةِ البياناتِ التابعةِ للدولة؛ لتكونَ السجنَ 10 سنواتٍ وغرامةَ 300 ألفِ يورو[82]. فارتكابُ تلك الجريمةِ عن طريقِ العصاباتِ المنظمةِ يكشفُ عن خطورةِ القائمِ بارتكابِهَا،مِمَّا يقتضي تشديدَ العقابِ عليهِ، لاَ سِيَّمَا إذا كانَ للشخصِ المعنوي دورٌ في ذلك.

مع ملاحظةِ أنَّ المادةَ 323-7 تعاقبُ على الشروعِ في الجريمةِ بالعقوبةِ ذَاتِهَا المقررةِ للجريمةِ الكاملةِ في الجرائم السابقةِ،في حين تعاقبُ المادةُ 323-4 عقوبات المعدلةُ بالقانونِ رقم **575** لسنةِ **2004م** على الاشتراكِ في مجموعةٍ للإعدادِ والتنسيقِ؛ لارتكابِ الجرائمِ المنصوصِ عليه في المواد 323-1 إلى 323-3-1 بالعقوبةِ المقررةِ للجريمة، كما تقرّرُ المادةُ 323-5 عقوبات إضافية PeinesComplémentaires للشخصِ الطبيعي متى ارتكبَ جريمةً من الجرائمِ السابقةِ؛ كالحرمان خمسَ سنواتٍ منَ الحقوقِ المدنيةِ، أو شغلِ الوظائفِ العامةِ، أو النشاطِ المهني الذي ارتكب الجريمة بسببهِ أو بمناسبتهِ،مصادرة الأدواتِ المستخدمةِ في الجريمةِ أو الموادِ المتحصلِ عليها منَ الجريمةِ، ما لم تكنْ منَ الأدواتِ التي ينبغي أنْ تُرَدَّ لأصحابِهَا.

وقدْ أضيفتْ مؤخراً المادةُ **323-8** عقوبات بمقتضَى القانونِ رقم **912** لسنةِ **2015 م** وتقضي بعدمِ تطبيقِ الأحكامِ المتعلقةِ بالجرائمِ السابقةِ على الإجراءاتِ والتدابيرِ التي نُفِّذَتْ منْ قِبَلِ المسْؤُولينَ المعنيينَ بخدماتِ

---

(81)Etienne Wery :Le nouvel article 323-3-1 du Code pénal : luttercontre les virus, d'accord, mais attention aux effetspervers,Publié le 02/09/2004 ,sur : https://www.droit-technologie.org/actualites/le-nouvel-article-323-3-1-du-code-penal-lutter-contre-les-virus-daccord-mais-attention-aux-effets-pervers/.

(82) كانت عقوبةُ الغرامةِ قبلَ التعديلِ بالقانونِ رقم 912 لسنة 2015 م تبلغُ 150 ألفَ يورو .

الدولةِ بإذْنٍ من رئيسِ الوزراءِ؛ كأجهزةِ الاستخباراتِ المتخصصةِ المشارِ إليها في المادة L. 811-2 منْ قانونِ الأمنِ الداخلي، لضمانِ حمايةِ المصالحِ الأساسيَّةِ للدولةِ خارجَ ترابِ الوطنِ، المشار إليها في المادة L. 811-3 منَ القانونِ نفسِه، وعليه فلا عقابَ على الفعلِ في مثلِ هذهِ الحالاتِ.

ثانياً: مدَى التزامِ موردِ خدماتِ الاتصالاتِ الإلكترونيةِ وكيفيةُ استخدامِ الكوكيز cookies:

أصدرَ المشرّعُ الفرنسيُّ مؤخراً القانونَ رقم **731**لسنةِ **2016**[83]وذلك من أجلِ مواكبةِ قانونِ الإجراءاتِ الجنائيةِ مع التغيراتِ في المجتمعِ، وتطوُّرِ الجريمةِ بفرنسا، ومنْ أجلِ فعاليةِ مكافحةِ الجريمةِ المنظمةِ والإرهابِ،ومصادرِ التمويلِ، وحمايةِ الشهودِ، وتوسيعِ سلطاتِ التحقيقِ في مجالِ مراقبةِ البياناتِ الشخصيةِ، من أجلِ مكافحةِ تلك الجريمةِ، وجرائم الإرهاب [84]. ويعتبرُ هذا القانونُ من أهمِّ القوانينِ التي صدرتْ عن المشرّعِ الفرنسيّ لمكافحةِ الجريمةِ المنظمةِ والإرهابِ.

وبموجبِ هذا القانونِ عُدِّلَتِ المادةُ 226-17-1 عقوبات - المضافةُ مؤخراً بالمرسومِ رقم **1012**لسنةِ**2011 م** بشأنِ المراسلاتِ الإلكترونية[85]- إذْ تعاقبُ مزودَ خدماتِ الاتصالاتِ الإلكترونيةِ إذَا لمْ يقُمْ بالإخطارِ عنْ أيِّ انتهاكاتٍ للبياناتِ الشخصيةِ للجنةِ الوطنيةِ للمعلوماتيةِ والحرياتِ، أو المعني بالبياناتِ، وتعاقبُ المسْؤُولَ عنِ المعالجةِ في حالِ عدمِ إخطارِ اللجنةِ بالإفشاءِ أو الوصولِ غيرِ المرخَّصِ إلَى البياناتِ المعالجةِ في المادة

(83)Loi n° 2016-731 du 3 juin 2016 renforçant la luttecontre le crime organisé, le terrorisme et leurfinancement, et améliorantl'efficacité et les garanties de la procédurepénale.

(84) Laetitia Valy,Au coeur des préoccupations, la luttecontre le terrorismeconnait un nouveau tournant avec cetteloi du 3 juin 2016 visant à mettre en oeuvre de nouvelles dispositions pour renforcer la prévention et la repression, http://www.net-iris.fr/veille-juridique/actualite/35232/lutte-contre-le-terrorisme-les-3-nouveautes-a-ne-pas-manquer.php.

(85)Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques .

L1-9-4123 منْ قانونِ الدفاعِ. حيثُ يُلْزِمُ المشرّعُ مزوّدَ خدماتِ الاتصالاتِ الإلكترونيةِ un fournisseur de services de communications électroniques بإخطارِ اللجنةِ عن أيّ انتهاكاتٍ للبياناتِ، كأنْ تتعرَّضَ للضياعِ أو الإتلافِ أو الإفشاءِ أو الوصولِ غيرِ المرخَّصِ، وإذَا كانتْ هذه الانتهاكاتُ ذاتَ تأثيرٍ سلبيّ على البياناتِ الشخصيةِ أو حرمةِ الحياةِ الخاصَّةِ، فينبغي ومنْ دُونِ تأخيرٍ إبلاغُ المعني.

كمَا يجبُ على المورِدِ إعدادُ قائمةٍ بالانتهاكاتِ ومصدرِها، والكيفية التي حدثتْ بها،ولا يلزمُ الإخطارُ عن انتهاكِ البياناتِ إذا وجدتِ اللجنةُ أنَّ المورِدَ قد قامَ بالتدابيرِ المناسبةِ لجعلِ البياناتِ الشخصيَّةِ أكثرَ أماناً، منَ الأشخاصِ غيرِ المرخَّصِ لهم بالدخولِ[86] كاستخدامِ نظامِ تشفيرِ البياناتِ[87].

وجديرٌ بالذكرِ أنَّ المادةَ **33** منَ التشريعِ الأوروبي الجديدِ الصادرِ في **27** أبريل **2016** الذي سيدخلُ حيزَ التطبيقِ في **25** مايو **2018م**قدْ ألزمتِ المورِدَ بالإخطارِ عنْ أيّ انتهاكٍ للبياناتِ خلالِ مدّةٍ لا تتجاوزُ 72 ساعةً منْ تاريخِ وقوعِ الانتهاكاتِ بعدَ علمِهِ بهَا إلى الجهةِ المختصَّةِ بحمايةِ البياناتِ (وهي في فرنسا اللجنةُ الوطنيةُ للمعلوماتيةِ والحرياتِ) وفي حالِ التأخيرِ يجبُ عليه أنْ يبينَ أسبابَ التأخيرِ.

في حين أوجبتِ المادةُ 34 منْ التشريعِ ذاتهِ إخطارَ المعني بالبياناتِ -ومنْ دُونِ تأخيرٍ مبرّرٍ- عن تلكَ الانتهاكاتِ متى كانَ منَ المرجَّحِ أنْ تؤدّيَ إلى مخاطرَ عاليةً على حقوقِ الأشخاصِ الطبيعيينّ وحريَّاتِهم، ولا يجِبُ إخطارُ المعني بالبياناتِ في عدةِ حالاتٍ؛ منها: إذا كانَ المسْؤُولُ عن المعالجةِ قد نفَّذَ تدابيرَ الحمايةِ الفنيةِ والتنظيميةِ المناسبةِ على البياناتِ الشخصيةِ التي تعرضَتْ للانتهاكِ،لاَ سِيَّمَا تلك التدابيرُ التي تجعلُ البياناتِ الشخصيةَ غيرَ مفهومةٍ لأيّ شخصٍ غيرِ مرخَّصٍ له بالوصولِ إليهَا؛ كاستخدامِ تقنياتِ التشفيرِ للبياناتِ الشخصيةِ.

(86) http://www.lexagone.fr/Obligation-de-notification-en-cas-de-violation

(87) http://www.murielle-cahen.com/publications/p-informatique-liberte.asp.

كمَا أنَّ المادةَ 35 منَ التشريعِ ذَاتِهِ أوجبتْ إجراءَ تقييمٍ لتأثيرِ عملياتِ المعالجةِ المرادِ القيامُ بها على حمايةِ البياناتِ الشخصيةِ، وعلى المسْؤُولِ عنِ المعالجةِ أنْ يسعى إلَى الحصولِ على مشورةِ الجهةِ المختصَّةِ بحمايةِ البياناتِ (وهي فرنسا اللجنةُ الوطنيةُ للمعلوماتيةِ والحرياتِ) عندَ إجراءِ تقييمٍ لتأثيرِ عملياتِ المعالجةِ على مستوى حمايةِ البياناتِ. ولخطورةِ ملفاتِ الكوكيز على الخصوصيةِ المعلوماتيةِ أو البياناتِ الشخصيةِ الإلكترونيةِ للمستخدمِ فإنَّ المشرّعَ الفرنسيَّ يحظرُ استخدامَ ملفاتِ تعريفِ الارتباطِ أو الكوكيز cookies ألَّا بعدَ موافقةِ المستفيدِ منَ الخدمةِ، وبالضوابطِ المتفقِ عليها مسبقاً[88].

فالتعديلُ سالفُ الذكرِ أخضعَ استخدامَ المواقعِ الإلكترونيةِ –لاَ سِيَّمَا مواقع محركاتِ البحثِ لملفاتِ تعريفِ الارتباطِ– لنظامِ اشتراكِ opt in –opt outومنْ ثم عدمُ جوازِ استخدامِها في حالِ عدمِ موافقةِ المستفيدِ منْ خدمةِ الاتصالاتِ[89]، وأصبحتِ المواقعُ الإلكترونيةُ تنبّهُ المستخدمَ الزائرَ لها أنها تستخدمُ ملفاتِ تعريفِ الارتباطِ، وتطلبُ منه صراحةً اختيارَ القبولِ أو الرفضِ. على اعتبارِ أنَّ ملفاتِ تعريفِ الارتباطِ[90]–وإنْ كانتْ تفيدُ المستخدمَ في تسهيلِ البحثِ عن المعلوماتِ والوصولِ إلَى المواقعِ التي يريدها– ألاَّ أنها تساهمُ في الكشفِ عن شخصيته منْ خلالِ عملياتِ البحثِ التي قامِ بها،ومن ثم فإنَّ استخدامَهَا ينبغي أنْ يكونَ بموافقته،وعدم منعِ استخدامِهَا.

(88) http://www.village-justice.com/articles/Transposition-droit-francais-Paquet,11388.html.

(89) http://www.murielle-cahen.com/publications/p-informatique-liberte.asp.

(90) ملفاتُ تعريفِ الارتباط Cookies ملفاتٌ نصيةٌ صغيرةٌ تُثَبَّتُ بطريقةٍ آليةٍ على القرصِ الصلب لجهازِ الحاسبِ الآلي للمستخدمِ عند زيارته للموقعِ الذي يستخدمها، ومن ثم تُرْسَلُ ملفاتُ تعريفِ الارتباط إلى موقع الويب الأصلي في كلِّ زيارةٍ جديدةٍ، أو إلى موقع ويبٍ آخرَ يتعرف على ملف تعريف الارتباط التي ثُبِّتَتْ بجهازِ الحاسبِ الآلي للمستخدمِ.

للمزيد من التفاصيل:

https://www.definitions-marketing.com/definition/cookie

ثالثاً: الإجراءاتُ الشكليةُ لمعالجةِ البياناتِ الشخصيةِ:

لا تكتفي أغلبُ التشريعاتِ عندَ حمايتِهَا للخصوصيةِ بالتجريمِ والعقابِ على انتهاكِهَا من الناحيةِ الموضوعيةِ،بل تجـرِّمُ–أيضًـا– عـدمَ احتـرامِ القواعـدِ التنظيميـةِ التـي وُضِـعَتْ لممارسـةِ عمليـاتِ جمـعِ البيانـاتِ وتخزينِهَـا ومعالجتِهَا[91]، فالمادةُ 226– 16 عقوبات، المعدلةُ مؤخراً بالقانونِ رقم **1321** لسنة **2016** بشأنِ الحكومةِ الرقميـةِ تعاقـبُ علـى إجـراءِ المعالجـةِ الآليـةِ للبيانـاتِ الشخصـيةِ، مـنْ دُونِ إعـلانِ اللجنـةِ الوطنيـةِ للمعلوماتيـةِ والحرياتِ بالمعالجةِ قبلَ القيامِ بهاوطلبِ الرأي أو الحصولِ على تصريحٍ من اللجنةِ، ولا يُشْتَرَطُ هنا موافقتُها على المعالجـةِ، بلِ المطلوبُ فقط إخطارُهَا بالمعالجـةِ، وتقومُ بعدَ ذلكَ بالتحقُّقِ منْ مدَى احترامِ المسْؤُول عنِ المعالجةِ لأحكامِ القانونِ [92].

و فـي فرنسـا فـإنَ صـاحبَ العملِ مسْؤُولٌ مدنياً[93] عن أعمـالِ تابعيـه التـي تقـعُ منهمْ بالمخالفةِ للقانونِ، وذلك باستخدامِ الإنترنت والحاسبَ الآلـي ووسائلِ الاتصـالِ المتاحـة لهم، وإنْ كانَ ذلكَ خارجَ أوقاتِ العملِ، طالما سمحَ لهم صـاحبُ العملِ باستخدامِهَا بحريـةٍ[94]، وتُطَبَّقُ المـادةُ ذاتُـهَا علـى منْ يقومُ بمعالجـةِ آليـةِ البيانـاتِ – كانتْ محـلاً للإجراءاتِ المنصـوصِ عليهـا فـي المـادة 45 مـن القانون 17– 78 – أو مـن يعملُ علـى السماحِ بالـدخولِ للبيانـاتِ الـواردةِ فـي المعالجـةِ المـذكورةِ بالمـادةِ1–9–L4123 مـن قـانونِ الـدفاعِ مـنْ دُونِ اتِّبـاعِ الإجراءاتِ، أو الحصولِ على الرأيِّ من اللجنةِ.

---

(91) هشام فريد رستم، قانون العقوبات، مرجع سابق، ص 200.

(92) غنام محمد غنام، مرجع سابق، ص109.

(93) دفاع الطاعن الموضوعي بعدم وجودِ سوابقَ له وبحسنِ سيره وسلوكِه بياناً لموجبات الرأفةِ لا يعفيه من المسْؤُوليَّةِ الجنائيةِ، ولا أثر له على قيام الجريمةِ، ولا يجوز إثارته لأول مرةٍ أمام محكمةِ النقض . نقض جنائي مصري 5 يناير 2017م، الطعن رقم 2005 لسنة 78 " غير منشور "

(94)ALEXIS Baumann: op,cit.

كمَا تعاقبُ المواد 226- 16- 1 ، 226- 16- 1- (أ) على المعالجةِ الآليةِ لرقمِ تسجيلِ الأفرادِ في السجلِ القوميّمنْ دُونِ مراعاةِ الشروطِ المنصوصِ عليها في القانون، أو مُعالجةِ البياناتِ، أو الترتيبِ لها،منْ دُونِ احترامِ القواعدِ التي وضعتهَا اللجنةُ.

وفيما يتعلَّقُ بالتدابيرِ اللازمةِ لحمايةِ البياناتِ يُلْزِمُ المشرّعُ المسْؤُولَ عنِ المعالجةِ باتخاذِ ما يلزمُ؛ للحفاظِ على سريةِ البياناتِ والمعلوماتِ وأمْنِهَا؛ كمنعِ الوصولِ غيرِ المُرَخَّصِ له، كإيجادِ رموزٍ للدخولِ وغيرها منَ الأمورِ الفنيَّةِ[95]كاستخدامِ موظفينَ مؤهلينَ للأمنِ، وأرشفةِ البياناتِ واستخدامها وفقاً للقانونِ، وتنفيذِ الحلولِ الفنيةِ وإجراءاتِ التنظيمِ والمراقبةِ لضمانِ أمنِ البياناتِ وحمايتِهَا وحفظِهَا[96]ضدّ أعمالِ التشويهِ أو الاطلاعِ غيرِ المرخَّصِ على البياناتِ،أو محوِ البياناتِ أو إتلافِهَا، وهذه الأفعالُ قد تتحقَّقُ بطريقةٍ ماديةٍ أو إلكترونيةٍ،بإدخالِ الفيروساتِ لنظمِ معالجةِ البياناتِ[97]وطبقًا للمادةِ 37 منَ القانونِ رقم 17-78المعدلةِ بالمرسومِ رقم 1341لسنةِ

(95)Jean Pradel et Michel danti -Juan:Manuel de droitPénalspécial,éditions Cujas,Paris,2007,P.247.

(96)Alexis Baumann: Commentaire du décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé, Publié le : http://www.declaration-cnil.com/Articles/A20060110-decret-sur-l-hebergement-de-donnees-de-sante.php.

(97) عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة المعلوماتية والمجرم المعلوماتي، دراسة متعمقة في التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي، انحراف الأحداث بسبب الإنترنت، مكافحة إدمان الإنترنت لدى بعض الفئات، منْ دُونِ ناشر ومكان نشر، الطبعة الأولى، 2009م،، ص147-148.

2015 [98] لا تقعُ الجريمةُ من صاحبِ الحقِّ في الحصولِ على الوثائقِ الإداريةِ أو السجلاتِ العامةِ، على اعتبارِ أنَّه من المرخصِ لهم بالوصولِ إلَى تلكَ البياناتِ والمعلوماتِ.

كما يتطلبُ المشرِّعُ عندَ جمعِ البياناتِ الشخصيةِ عن الأفراد أوْ مُعالجتِهَا، المتعلقةِ بالأصلِ العرقي أو معتقداتِه أو ميولِه الدينيِّ أو السياسيِّ أو الفلسفيِّ أو النقابيِّ، أو هويتِه الجنسيةِ – الحصولَ على موافقتِهِمْ،وبخلافِ ذلك يكتفي المشرعُ بإخطارِ اللجنةِ بالمعالجةِ، ولا شَكَّ فِي أنَّ ذلك يرجعُ لطبيعةِ هذه البياناتِ وخطورتها في الكشفِ عن هويةِ الشخصِ.وقد يكونُ للمعني الحقُّ في الاعتراضِ على معالجةِ البياناتِ، وفي حالِ اعتراضِهِ يجبُ عدمُ معالجةِ البياناتِ[99]، فتعاقبُ المادةُ226-18-1 عقوبات على المعالجةِ علَى الرغمِ منِ اعتراضِ المعني، وكان هذا الاعتراضُ مشروعاً،على اعتبار أنَّه من الضروري في نطاقِ تسجيلِ البياناتِ في نظامِ المعالجةِ أنْ يكونَ هناك تناسبٌ بينَ المعلوماتِ والهدفِ من تسجيلِهَا،فلا يجوزُ حفظُهَا إلَّا بالقَدَرِ اللازمِ؛ لتحقيقِ الغرضِ من حفظها[100]، ولا يكونُ للشخصِ الحقُّ في الاعتراضِ في الحالاتِ التي يجيزُ فيها القانونُ المعالجةَ.

كمَا يَحِقُّ للمعني بالبياناتِ طلبُ تصحيحِ البياناتِ غيرِ الصحيحةِ أو مسحِهَا،فوفقاً للمادة R625-12 من قانونِ العقوباتِ الفرنسي المضافةِ بالأمر رقم 1306 لسنة 2005 يُعَاقَبُ الشخصُ المسْؤُولُ أو القائمُ على المعالجةِ إذَا رفضَ – منْ دُونِ نفقاتٍ إضافيةٍ– طلبَ المعني تصحيحَ البياناتِ الشخصيةِ المتعلقةِ به أو استكمالَهَا أو تحديثَهَا أو قفلَهَا أو محوَهَا، أو الشخص المتوفَى متى طالبَ ورثتُه بذلك، عندما تكونُ تلك البياناتِ غيرَ دقيقةٍ، أو ناقصةٍ، أو مبهمةٍ ملتبسةٍ، أو قديمةٍ غيرِ محدثةٍ.

---

(98)Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration.

(99) غنام محمد غنام، مرجع سابق، ص117.

(100) راجع : عبد الفتاح بيومي حجازي، مرجع سابق، ص 159.

مع ملاحظةِ أنَّ المادةَ R625-13 من قانونِ العقوباتِ المعدلةِ بالمرسومِ رقم 671 لسنة 2010 تشدِّدُ العقوبةَ علَى الشخصِ القائمِ بالمعالجةِ في حالِ قيامِه بتكرارِ تلك الأفعالِ [101]، ولعلَّ في ذلك توسيعًا لحمايةِ البياناتِ الشخصيةِ، ومنعَ الاعتداءاتِ التي قد تقعُ على حقوقِ الشخصِ؛ بسببِ المعالجةِ الآليةِ للبياناتِ الشخصيةِ، فقد يترتَّبُ على عدمِ تصحيحِ البياناتِ، أو تحديثِ القديمةِ، أو توضيحِ المبهمةِ-فقدانَ الفردِ لحقٍّ من حقوقِهِ أو الانتقاصِ منها؛ كحقِّهِ في الحصولِ علَى وظيفةٍ معينةٍ تتطلَّبُ شروطًا معينةً غيرَ موجودةٍ في البياناتِ القديمةِ أو المبهمةِ أو غيرِ الصحيحةِ، المختزنةِ في النظامِ المعلوماتي، أو يؤدِّي إلى الإخلالِ بمبدأ تكافُؤِ الفرصِ مع غيره منَ الأفرادِ، إلى غيرِ ذلك من الأمور.

ولكن ما هي التدابيرُ الأمنيةُ لمعالجةِ البياناتِ في ظلِّ التشريعِ الأوروبيِّ الجديدِ الصادرِ في 27 أبريل 2016 الذِي سيدخلُ حيزَ التطبيقِ في 25 مايو 2018 م ؟

نصَّ هذا التشريعُ على مجموعةٍ من التدابيرِ الأمنيةِ، ينبغي مراعاتُهَا من القائمِ بالمعالجةِ، ومن تلك التدابيرُ: مراعاةُ أحدثِ ما توصلتْ إليه التكنولوجيا في هذا المجال، والأخذُ في الاعتبارِ مختلفَ المخاطرِ التي قد تتعرضُ لها حقوقُ الشخصِ الطبيعي وحريّاتُه في هذا المجالِ، وطبيعةَ المعالجةِ والغرضَ منها، والعملَ على تشفيرِ البياناتِ الشخصيةِ، والقدرة على ضمانِ السريةِ المستمرةِ والنزاهةِ ومرونةِ نظامِ المعالجةِ وخدماتِهَا، والقدرة على استعادةِ الوصولِ إلَى البياناتِ في الوقتِ المناسبِ في حالِ وقوعِ حادثٍ ماديٍّ أو تقنيٍّ، وأنْ يقومَ المسْؤُولُ عنِ المعالجةِ باختبارِ فعاليةِ الإجراءاتِ التقنيةِ والتنظيميةِ وتقييمِهَا؛ لضمانِ أمنِ المعالجةِ على أنْ يُؤْخَذَ في الاعتبارِ مخاطرُ التدميرِ العرضي أو غيرِ القانوني للبياناتِ، وأنْ يقومَ المسْؤُولُ عنِ المعالجةِ باتخاذِ الإجراءاتِ التي تضمنُ عدمَ دخولِ أيّشخصٍ

(101)Décret n° 2010-671 du 18 juin 2010 relatif à la signature électronique et numérique en matière pénale et modifiant certaines dispositions de droit pénal et de procédure pénale.

طبيعي غيرِ مرخَّصٍ له على نُظُمِ معالجةِ البياناتِ، أو الوصولِ إلَى تلكَ البياناتِ والاطلاع عليها، وأنْ تعملَ الشركاتُ على تأهيلِ موظفيهَا وتدْريبِهم، الذينَ لهمْ دخولٌ مُنْتَظِمٌ إلى البياناتِ الشخصيةِ على حمايةِ تلك البياناتِ.ولا شَكَّ فِي أنَّ الجانبَ الفني والتقني يساهمُ بقَدْرٍ كبيرٍ في توفيرِ حمايةٍ فعالةٍ للبياناتِ والمعلوماتِ الشخصية، لاَ سِيَّمَا لدَى الدولِ التي تعاني من عدمِ تحديثِ تشريعاتها، وقصورِ أو عجز تلك التشريعاتِ؛ لمواجهة الجرائمِ المستحدثةِ.

رابعا: الجمعُ والحفظُ غيرُ المشروعِ وسوءُ الاستخدامِ للبياناتِ الشخصيةِ:

1. **تجميعُ البياناتِ وحفظُهَا:**تعاقبُ المادةُ 226 – 18 عقوبات على جمعِ البياناتِ بطريقةٍ غيرِ مشروعةٍ أو بالاحتيالِ، سواءٌ أكانَ ذلكَ بشكلٍ مباشرٍ أمْ غيرِ مباشرٍ، عن طريقِ استخدامِ ملفاتِ cookies[102]،ويقرّرُ المشرّعُ–كذلك– الحمايةَ لبعضِ البياناتِ ذاتِ الطبيعة الحسَّاسةِ كتلك التي تكشفُ عن الأصلِ العرقيّ أو الميولِ السياسيّ أو الدينيّ أو الهويةِ الجنسيةِL'identité sexuelle، وكذلك البيانات التي تتعلَّقُ بالإدانةِ والسوابقِ الجنائيةِ، فضلاً عن البياناتِ الطبيةِ، لذلكَ جاءتِ المادةُ 226–19 عقوبات،المعدلةُ مؤخراً بمقتضى القانونِ رقم 86–2017 الصادرِ في 27 يناير 2017 بشأنِ المساواةِ في المواطنةِ Loi n° 2017–86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté، لتعاقبَ على الاحتفاظِ غيرِ المشروعِ للبياناتِ الحسَّاسةِ في غيرِ الحالاتِ التي يجيزُهَا القانونُ، ومنْ دُونِ "رضىً صريحٍ " منَ المعني بها، حيثُ يجبُ الحصولُ على موافقتهِ الصريحة،فيجبُ ألَّا تتضمنَ تلك البياناتُ الطبيةُ في مجالِ البحثِ بياناتٍ شخصيةً مباشرةً للمرضى، كما يجبُ تحديدُ الأشخاصِ الذين بإمكانهم الوصولُ إلَى تلك البياناتِ التي عُولِجَتْ، والتقيُّدُ بالمدَّةِ المحدَّدَةِ للاحتفاظِ بتلك البياناتِ، معَ مراعاةِ الحدِّ الأدنى منَ التدابيرِ الأمنيةِ، ومن بينِ تلكَ التدابيرِ التي يطلب

(102)Carole Girard–Oppici : op,cit.

من مديري مراكزِ البحوثِ القيامُ بها إنشاءُ سياسةٍ خصوصيَّةٍ وأمْنٍ للبياناتِ ونظامٍ للتوثيقِ،كما يجبُ تشفيرُ تلكَ البياناتِ في حالِ نقلِهَا إلى خارجِ الاتحادِ الأوروبي(103).

ثم أضيفتْ عبارةُ "أو أي نوعٍ منْ أنواعِ أو أشكالِ الهوية للفردِ" **l'identité de genre de celles-ci**، بمقتضَى التعديلِ التشريعي الأخيرِ عام 2017م ، ولا شَكَّ فِي أنَّ المشرّعَ أرادَ التوسُّعَ في مفهومِ البياناتِ الحسَّاسةِ المكفولةِ بالحمايةِ، وهو –في نظرنا– توسُّعٌ جيّدٌ من جانبِ المشرّعِ، فهذه البياناتُ تتَّسِمُ بالخطورةِ بكشفها عنْ هويةِ الفردِ أكثرَ من غيرها.وتعاقِبُ المادةُ ذاتُهَا على الحفظِ الآلي للبياناتِ المتعلقةِ بالجرائمِ أو الإدانةِ أو تدابيرِ الأمنِ في ذاكرةِ تخزينٍ آليةٍ بخِلافِ الحالاتِ التي يجيزُها القانون(104)،إذ يجوزُ تخزينُ أو حفظُ البياناتِ المتعلّقةِ بالجرائمِ والعقوباتِ وإجراءاتِ الأمنِ في بعضِ الحالاتِ كالأعمالِ التي تقومُ بها بعضُ الجهاتِ، مثل القضاءِ والسُّلطاتِ العَامَّة.

كمَا أنَّ للبياناتِ والمعلوماتِ الطبيَّةِ وضعًا خاصًّا؛ لما لها من خصوصيَّةٍ تتعلَّقُ بحالةِ المريضِ الصحيَّةِ، وعدم رغبتهِ في إطلاع غيرِه عليهَا قدرَ الإمكانِ، خاصَّةً وإنَّ هذه البياناتِ قدْ يكونُ المريضُ مضطراً لتقديمها، حتَّى يتمكَّنَ الطبيبُ منَ التشخيصِ السليمِ للمرضِ والعلاجِ، فتعاقبُ المادةُ 226 –19 –1 عقوبات على معالجةِ البياناتِ بهدفِ البحثِ في المجالِ الطبي، مِنْ دُونِ إخطارِ المعنِي بحقِّه في الوصولِDroit d'accès إلَى البياناتِ والمعلوماتِ، وحقِّه في الاعتراضِ على المعالجةِ وعنْ طبيعةِ البياناتِ المرسلةِ، أو معالجةِ البياناتِ على الرَّغمِ منْ اعتراضه، أو في غيرِ الأحوالِ التي يجيزُها

(103)Hélène Lebon: Méthodologie de référence de la CNIL pour les recherchesbiomédicales,Publié le: http://www.declaration-cnil.com/Articles/A20060405-recherches-biomedicales.php.

(104)Panorama des infractions Informatique et libertés en France, https://www.alain-bensoussan.com/avocats/infractions-informatique-et-libertes/2017/02/21/

القانونُ.وتُعَدُّ حالةُ متابعةِ المرضى بغرضِ الرعايةِ الطبيَّةِ والبحثِ العلمِي مِنَ الحالاتِ التي يجوزُ فيها جمعُ البياناتِ الطبيةِ، فقد تقتضِي الضرورةُ أنْ تقومَ مراكزُ البحثِ العلمي بتجميعِ بياناتٍ طبيَّةٍ للفردِ ومعالجتِهَا وتخزينِهَا(105).

وفي مجالِ الأبحاثِ الطبيةِ أجازَ المرسومُ رقم 1306 لسنةِ 2016 الصادرُ في 11 أغسطس 2016 لمعهدِ الحمايةِ منَ الإشعاعِ والسلامةِ النوويةِ–القيامَ بمعالجةِ البياناتِ الشخصيةِ، خاصَّةً عنْ طريقِ استخدامِ رقم التسجيلِ في السِّجِلِ الوطني أو القومِي للأشخاصِ الطبيعيينَ؛ لجمعِ البياناتِ من نظامِ التأمينِ الصحي الوطني بينَ الأنظمةِ لدراسةِ مخاطرِ مرضِ السرطانِ، الناجمِ عنِ الإشعاعِ ، وبيان مجموعةِ الأطفالِ الذين استفادُوا من إجراءِ طبِّ القلبِ التدخلي، وكذلك الجرعات التي أُخِذَتْ في المراكزِ المشاركةِ في الدراسةِ(106). كمَا أجازتِ المادةُR1461 من قانونِ الصحَّةِ العامَّةِ الفرنسي المعدَّلةُ بالمرسومِ رقم 1871 لسنةِ 2017 الصادِرُ فِي 26 ديسمبر 2016 بشأنِ معالجةِ البياناتِ الشخصيةِ "النظام الوطني للبياناتِ الصحيةِ" –القيامَ بمعالجةِ البياناتِ الشخصيةِ الواردةِ في النظامِ الوطنِي للبياناتِ الصحيَّةِ système national des données de santé وفقًا لشروطٍ معينةٍ، ولأغراضٍ عديدةٍ؛

(105) غنام محمد غنام، مرجع سابق، ص108.

(106)Décret n° 2016-1103 du 11 août 2016 portant création d'un traitement automatisé de données à caractère personnel relatif à une étude, dénommée « Coccinelle », du risque de cancer radio-induit après exposition aux procédures de cardiologie interventionnelle dans l'enfance, (JORF n°0188 du 13 août 2016,texte n° 11.)

منهَا: تقييمُ سياساتِ الصحَّةِ والحمايةِ الاجتماعيةِ،وتوفيرُ معلوماتٍ عنِ الرعايةِ الطبيَّةِ للمرضَى، وكذلك البحوثُ والدراساتُ والتقييمُ والابتكارُ في مجالاتِ الصحةِ والرعايةِ الطبيةِ الاجتماعيةِ[107].

وفي السياقِ ذَاتِهِ أجازَ المرسومُ رقم 37 لسنةِ 1998 وفقاً لشروطٍ معينةٍ–استخدامَ البياناتِ الواردةِ في الدليلِ الوطني لتحديدِ الهويةِ، أو التعرفِ على الأشخاصِ الطبيعيينَ،والأشخاصِ المتوفَيينَ لإجراءِ المعالجةِ الآليَّةِ للبياناتِ الاسميةِ؛ لغرضِ البحثِ في مجالِ الصحةِ[108].

ولكن ماذا عن موافقةُ المعنِي بالبياناتِ وحقوقُه في التشريعِ الأوروبي الجديدِ لحمايةِ الخصوصيةِ والبياناتِ لعام 2016 الذِي سيدخلُ حيزَ التطبيقِ في 25 مايو 2018 م ؟

يُلاحَظُ أنَّ التشريعَ الأوروبي الجديدَ الصادرَ عنِ الاتحادِ الأوروبي لعام 2016 الذي سيدخلُ حيِّزَ التطبيقِ في 25 مايو 2018م[109] يتطلبُ أنْ تكونَ الموافقةُ واضحةً لا لَبْسَ فيها، وبلغةٍ واضحةٍ، ويمكنُ الوصولُ إليها بسهولةٍ ويسرٍ، ويحقُّ للشخصِ سحبُ الموافقةِ في أيِّ وقتٍ، ويجبُ أنْ يكونَ سحبُ الموافقةِ سهلًا ومُيَسَّرًا، مثلمَا كانَ عليه الأمرُ عندَ تقديمِ الموافقةِ، على أنَّ سحبَ الموافقةِ لا يؤثِّرُ بطبيعةِ الحالِ علَى مشروعيَّةِ المعالجةِ التي حدثتْ قبلَ سحبِهَا، وهذا يعني أنَّ الموافقةَ الضمنيةَ للمعنِي

(107)Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

(108)Décret n°98-37 du 16 janvier 1998 autorisant l'accès aux données relatives au décès des personnes inscrites au Répertoire national d'identification des personnes physiques dans le cadre des recherches dans le domaine de la santé.

(109)The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

لَيْسَ لَـهَا أيُّ أثرٍ فـي هذا الشأنِ، وذلك مردُّهُ إلَـى خطـورةِ تلكَ البيانـاتِ وأهميتهَـا، كالبيانـاتِ التـي تـدلُّ بشكلٍ مباشرٍ أو غيرِ مباشرٍ علـى الأصـولِ العرقيَّةِ أو الأثنيـة أو الآراءِ السياسيَّةِ أو الفلسفيَّةِ أو الدينيَّةِ أو الخلفياتِ النقابيَّةِ للفردِ، أو تلك التي تتعلَّقُ بالتوجُّهِ الجنسي للفردِ (الهوية الجنسية) أو بالصحَّةِ.

وقدْ أجازَ التشريعُ الأوروبي الجديدُ أنْ تحدُثَ المعالجةُ مِنْ دُونِ موافقةِ المعني الصريحةِ والواضحةِ في حالاتٍ عديدةٍ منها[110]: أنْ تكونَ المعالجةُ ضروريةً لحمايةِ المعني بالبياناتِ أو شخصٍ طبيعيٍّ آخر، متى كانَ المعني بالبياناتِ عاجزًا جسدياً أو قانونياً عنْ تقديمِ الموافقةِ، أو متى كانتِ المعالجةُ قد حدثتْ لأنشطةٍ مشروعةٍ لجهاتٍ أو مؤسساتٍ لا تهدفُ إلى تحقيقِ الربحِ، وذاتِ هدفٍ فلسفيٍّ أو دينيٍّ أو اجتماعيٍّ أو نقابيٍّ، بشرطِ تقديمِ ضماناتٍ مناسبةٍ من تلكَ الجهاتِ، وأنْ تكونَ المعالجةُ فقط للأعضاءِ الحاليينَ أو لأعضاءٍ سابقينَ في الهيأةِ أو للأشخاصِ الذينَ لديهمُ اتصالٌ منتظمٌ بها فيما يتعلَّقُ بأغراضِهَا أو أنشطتِهَا، وألَّا يُكْشَفَ عنِ البياناتِ الشخصيَّةِ خارجَ تلكَ الهيأةِ مِنْ دُونِ موافقةِ المعنِي بالبياناتِ، أوْ أنْ تكونَ المعالجةُ ضروريةً لأغراضِ الطبِّ الوقائيِّ أوِ المهني؛ لتقييمِ قدرةِ الموظَّفِ علَى العملِ، والتشخيصِ الطبي، وتوفيرِ الرعايةِ الصحيَّةِ أو الرعايَّةِ الاجتماعيَّةِ أو العلاجِ، أو إدارةِ نُظُمِ الرعايةِ الصحيَّةِ أو الاجتماعيَّةِ وخدماتِهَا، على أساسِ قانونِ الاتحادِ أو الدولِ الأعضاءِ، أو بموجبِ عقدٍ مع شخص مختص خاضعٍ للشروطِ والضماناتِ المشارِ إليهَا في هذا القانونِ. أو أنْ تكوَن المعالجةُ ضروريةً لأسبابٍ تتعلَّقُ بالمصلحةِ العامَّةِ في مجالِ الصحَّةِ العامَّةِ، مثل الحمايةِ منَ التهديداتِ الخطيرةِ عبرَ الحدودِ للصحة، أو ضمان مستوياتٍ عاليةٍ من جودةِ الرعايةِ الصحيةِ وسلامتِهَا، والمنتجاتِ الطبيةِ

(110)Article 9 of The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

أو الأجهزةِ الطبيةِ، مع مراعاةِ السريةِ المهنيةِ، أو أنْ تكونَ المعالجةُ ضروريةً لأغراضِ الأرشفةِ في المصلحةِ العامةِ، أو لأغراضِ البحثِ العلمي أو التاريخي أو الأغراضِ الإحصائيةِ.

كمَا أنَّ المادةَ 16 منَ التشريعِ الأوروبي الجديدِ تقرّرُ حقَّ المعنِي بالبياناتِ في التصحيحِ droit de corrigerوذلك بأنْ يكونَ له الحقُّ في الوصول –مِنْ دُونِ تأخيرٍ مبرَّرٍ–إلَى البياناتِ الشخصيةِ غيرِ الدقيقةِ أو غيرِ الصحيحةِ المتعلقةِ به، واستكمال البياناتِ الشخصيةِ غيرِ الكاملةِ، عن طريقِ تقديمِ بيانٍ تكميليّ مع الأخذِ في الاعتبارِ بغرضِ المعالجةِ، في حين أنَّ المادةَ 17 منَ التشريع ذَاتِهِ تقرّرُ للمعنِي بالبياناتِ الحقَّ في مسحِ البياناتِ الشخصيةِ أو محوِهَا Droit d'effacer مِنْ دُونِ تأخيرٍ مبررٍ،وذلك في أحوالٍ مختلفةٍ؛ كأنْ يكونَ حفظُ البياناتِ الشخصيةِ لم يَعُدْ ضرورياً فيما يتعلَّقُ بالغرضِ الذي جُمِعَتْ من أجله،وقررتِ المادةُ 18 للمعني بالبياناتِ الحقَّ في الاعتراضِ على تجميعِ البياناتِ أو معالجتها أو استخدامِهَا في عدَّةِ حالاتٍ، منهَا: أنْ تكونَ البياناتُ غيرَ دقيقةٍ، أو أنَّ المعالجةَ كانتْ غيرَ قانونيةٍ، ويعارضُ المعني في مسحِ البياناتِ، ويطلبُ فقط تقييدَ استخدامِهَا،في حين أوجبتِ المادةُ 19 على المراقبِ أو الشخصِ الذي يتحكَّمُ بالبياناتِ إخطارُ المعني بالبياناتِ فيما يتعلَّقُ بتصحيحِ البياناتِ الشخصيةِ أو مسحِهَا، أو تقييدِ المعالجةِ مالم يثبتْ أنَّ ذلك كانَ متعذراً أو مستحيلاً، كما تناولتِ المادةُ 20 الحقَّ في قابليةِ نقلِ البياناتِ بمعنى حقِّ المعني بالبياناتِ في نقلِ البياناتِ من جهةٍ لأخرَى،مِنْ دُونِ تعطيلٍ من جانبِ الجهةِ التي تحوزُ البياناتِ، ولا مجالَ لإعمالِ هذا الحقِّ على المعالجاتِ اللازمةِ لأداءِ مهمةٍ في مصلحةٍ منَ المصالحِ العامَّةِ، أو تقومُ بها السلطاتُ و الجهاتُ الرسميَّةُ في الدولةِ.

كمَا نصَّتِ المادةُ 21 على حقِّ المعني بالبياناتِ فِي الاعتراضِ علَى معالجةِ البياناتِ في أيِّ وقتٍ، في عدَّةِ حالاتٍ منها: أنْ تكونَ معالجةُ البياناتِ الشخصيةِ لأغراضِ التسويقِ المباشرِ، أو أغراضٍ

بحثيةٍ علميةٍ أو تاريخيةٍ، أو أغراضٍ إحصائيةٍ، مالم تكنِ المعالجةُ ضروريةً لإداءِ مهمَّةٍ نُفِّذَتِ لدواعي المصلحةِ العامةِ.

غيرَ أنَّ المادةَ 23 من التشريعِ الجديدِ أجازتْ لقانونِ الاتحادِ الأوروبي أو الدولِ الأعضاءِ–فرضَ قيودٍ علَى الحقوقِ السالفةِ الذكرِ في حالاتٍ معينةٍ، منهَا: الأمنُ القوميُّ والدفاعُ ومنعُ الجرائمِ الجنائيةِ أو التحقيقُ فيهَا، أو الكشفُ عنهَا أو عن مرتكبيها، أو مقاضاةُ مرتكبيها، أو تنفيذُ العقوباتِ الجنائيةِ، بما في ذلكَ حمايةُ الأمنِ العام ومنعُ تهديدِهِ،أو لأهدافٍ مهمَّةٍ أخرَى للمصلحةِ العامَّةِ للاتحادِ أو الدولِ الأعضاءِ، وخاصةً المصالحُ الاقتصاديةُ أو الماليةُ المهمةُ للاتحادِ أو لدولةٍ عضوٍ في الاتحادِ، بما في ذلك المسائلُ المتعلقةُ بالنقديةِ والماليةِ والميزانيةِ، وفرضُ الضرائبِ، والصحةُ العامةُ، والضمانُ الاجتماعيُّ، أو لغرضِ حمايةِ استقلالِ القضاءِ والإجراءاتِ القضائيةِ، ولا شَكَّ فِي أنَّ النصَّ على تلك الحقوقِ يوسِّعُ من نطاقِ حمايةِ البياناتِ الشخصيةِ الإلكترونيةِ، ويضمنُ للمعني عدمُ استخدامِ أو معالجةِ بياناتِه بشكلٍ غيرِ مشروعٍ.

2.سوءُ استخدامِ البياناتِ: يُعَدُّ الإفشاءُ منْ صورِ سوءِ استخدامِ البياناتِ، وبلَا شَكٍّ يشكِّلُ الإفشاءُانتهَاكاً للحياةِ الخاصَّةِ للفردِ وحقِّهِ في السِّريَّةِ، والإفشاءُ نقيضُ السرِّ، ويعني نقلَ المعلوماتِ من حالِ الكتمانِ إلى العلانيةِ،فالإفشاءُ يتحقَّقُ بالنسبةِ للمعلوماتِ السريَّةِ أو التي يشملُهَا الالتزامُ بالكتمانِ، ويتحقَّقُ الإفشاءُ بأنْ يقومَ الشخصُ الذي يحوزُ البياناتِ لسببٍ مشروعٍ كأغراضِ المعالجةِ أو الحفظِ، بنقلِ تلكَ البياناتِ لشخصٍ غيرِ مختصٍّ بتلقي البياناتِ أو الاطلاعِ عليهَا[111]. وتعاقبُ المادةُ 226 – 22 عقوبات على الإفشاءِ الذي يقعُ منَ الحائزِ للبياناتِ عندَ التسجيلِ أو أيّ شكلٍ آخرَ منْ أشكالِ المعالجةِ لبياناتٍ تتعلَّقُ بحرمةِ الحياةِ الخاصَّةِ للشخصِ، أو شرفِهِ أو اعتبارِهِ،علَى أنْ يترتَّبَ علَى الإفشاءِ الاعتداءُ على تلك القيمِ أو الحقوقِ، وتعتبرُ هذه

(111) يونس عرب، مرجع سابق، ص 510.

الجريمةُ من الجرائمِ العمديةِ التي يلزمُ لقيامِهَا تحقُّقُ القصدِ الجنائي العام Dol général بعنصرَيْهِ العلمِ والإرادةِ، وبغضّ النظرِ عنِ الباعثِ من ارتكابِ الفعلِ الإجرامي.

كمَا قدْ تقومُ مختلفُ الجهاتِ بالدولة بحفظِ البياناتِ الشخصيةِ المقدَّمةِ إليها من الزبائنِ في بنوكٍ للمعلوماتِ،غيرَ أنَّه ينبغي ألَّا تزيدَ مدَّةُ حفظِ البيانات عن الوقتِ اللازمِ للاحتفاظ بها،كذلك لا تجوزُ الإساءةُ في استخدام تلك البياناتِ، فتعاقبُ المادةُ 226- 20 عقوبات على الاحتفاظِ بالبيانات لمدةٍ تطولُ عن المدةِ التي يسمحُ بها القانون؛ ما لم يكنِ الاحتفاظُ قدْ كَانَ لأغراضٍ تاريخيَّةٍ أو إحصائيَّةٍ أو علميَّةٍ، وطبقًا للشروطِ التي يحددُهَا القانونُ. ففي إطارِ حمايةِ حقوقِ الإنسان ومنعِ الاعتداءاتِ الناتجةِ عنِ المعالجةِ الآليَّةِ للبياناتِ، تُجِيزُ المادةُ11-R625 من قانونِ العقوباتِ الفرنسي، المضافةُ بالأمرِ رقم 1309 لسنة 2005 الصادر في 20 أكتوبر 2005 بشأنِ تطبيقِ القانونِ رقم 78-17 بتاريخ 6 يناير 1978 المتعلقِ بمعالجة البياناتِ والملفات والحرياتِ[112]-للشخصِ القائمِ على المعالجةِ الاحتفاظَ بالبياناتِ الشخصيةِ عن تلك المدَّةِ إذَا كان لغرضٍ وحيدٍ، وهو تجميعُ الإحصاءاتِ أو البحوثِ العلميةِ أو التاريخيةِ. على أنْ يكونَ ذلك بموافقةِ المعني أو بمقتضى المبادئِ التوجيهيةِ الواردةِ في المادةِ 40 أو بإذنٍ منَ اللجنةِ، وذلك طبقًا للمادةِ 36 من القانونِ رقم17-78 المعدلةِ بالقانونِ رقم **2016-1321** الصادرِ **في 7** أكتوبر **2016م**، وتفترضُ هذه الجريمةُ أنَّ المعالجةَ قد تكونُ بشكلٍ مشروعٍ، غيرَ أنَّ الاحتفاظَ بالبياناتِ قد تجاوز المدة التي حددَهَا القانونُ إذَا كانَ النظامُ يتبعُ جهةً حكوميةً، أو المدة المحددة في إخطارِ اللجنةِ إذَا كانَ النظامُ يتبعُ للقطاعِ الخاص[113].

---

(112) Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(113) عبد الفتاح بيومي حجازي، مرجع سابق، ص 150.

كمَا تعاقبُ المادةُ 226 –21 عقوبات على المعالجةِ لغرضٍ آخرَ غيرِ الغرضِ المحدَّدِ أو المسموحِ به قانونًا[114]، كأنْ تستخدمَ شركةُ الهاتفِ تلك البياناتِ في أغراضِ التسويقِ التجاري لبعضِ المنتجاتِ، أو بيع أو تقديم تلك البيانات لأيّ جهةٍ أخرى بهدفِ تحقيقِ الربحِ... إلخ، وتعتبرُ هذه الجرائمُ من الجرائمِ العمديةِ، ويلزمُ لقيامها القصدُ الجنائي العام، بأنْ تتجهَ إرادةُ الجاني إلى ارتكابِ الجريمةِ معَ العلمِ بعناصرِهَا، بغضِ النظرِ عنِ الباعثِ من ارتكابها[115]. وإذا كانَ الأصلُ هو حرية الحصولِ على المعلوماتِ وتدفقِهَا وانسيابهَا، مما يستوجبُ تقريرَ حريةِ جمعِ المعلوماتِ وترتيبها ومعالجتها، ومن ثم التعاملُ بها[116]، على اعتبارِ أنَّ الإنترنت شبكةٌ من غيرِ حدودٍ ومنْ دُونِ قيودٍ، فإنَّ المشرّعَ الفرنسيَّ يوفرُ حمايةً للبياناتِ، حتَّى في حالِ نقلهَا إلَى خارجِ الدولةِ، فيتطلبُ عند نقلِ البياناتِ إلى خارجِ الاتحادِ الأوروبي توافر شروطٍ معينةٍ لضمانِ سلامةِ تداولِ البياناتِ المعالجة آلياً أو تبادلِهَا Échange de données informatisé، إذْ تعاقبُ المادةُ 226 – 22 – 1 عقوبات على نقلِ بياناتٍ شخصيةٍ كانت أومن الممكنِ أنْ تكونَ محلاً للمُعالجةِ الآليةِ بالمخالفة للتدابيرِ التي وضعتها اللجنةُ الأوروبيةُ أو اللَّجنةُ الفرنسيةُ إلى دولةٍ غيرِ عضوٍ في الاتحادِ الأوروبي، ولا تقومُ الجريمةُ إذا نُقِلَتِ البياناتُ إلَى دولةٍ عضوٍ في الاتحادِ الأوروبي، أو إلَى دولةٍ غيرِ عضوٍ في الاتحادِ الأوروبي، ولكن مع احترامِ التدابيرِ التي وضعتهَا اللجنةُ الأوروبيةُ أو اللجنةُ الفرنسيةُ، ومن الحالاتِ التي ينسحبُ عليها النصُّ شركاتُ نقلِ المسافرينَ أو البنوكُ التي توجدُ في فرنسا وتتعاملُ بالبياناتِ الشخصيةِ، ولها فروعٌ أو تعاملُ مع شركاتٍ أخرى خارجَ نطاقِ الاتحادِ الأوروبي، فعليها عند نقلِ البياناتِ خارج فرنسا أنْ تتقيَّدَ بتلك الضوابطِ.

---

(114)voir : Cass,Crim9février 2016,Bulletin criminel 2016, n° 29.

(115) عبد الفتاح بيومي حجازي، مرجع سابق، ص 159–162.

(116) خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، دراسة تحليلية مقارنة، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، 2009، ص72.

وطبقًا للمادةِ bis49 من القانونِ رقم **17-78** المضافةِ بالقانونِ رقم **1321-2016** الصادرِ في **7** أكتوبر **2016م** بشأنِ الحكومةِ الرقميةِ تقومُ اللجنةُ الوطنيةُ في فرنسا بالتنسيقِ مع الجهةِ التي تمارسُ سلطاتٍ مماثلةً لسلطاتِهَا في تلك الدولةِ التي تُنْقَلُ البياناتُ الشخصيةُ إليها،ويجبُ أنْ تتوافرَ في معالجة تلك البياناتِ الشروطُ التي نصَّتْ عليها المادةُ 44 من القانونِ رقم 17-78.

وتجدرُ الإشارةُ إلى أنَّ المشرّعَ الفرنسيَّ يعاقبُ على الجرائمِ السابقةِ كافَّةً بعقوباتٍ سالبةٍ للحريةِ، تصلُ إلى خمسِ سنواتٍ، وغرامةِ ثلاثمائةِ ألفِ يورو، بالإضافةِ إلى ذلك تُمْسَحُ البياناتُ-موضوع المعالجةِ- في الموادِ 226-16 إلى 226- 22 -1 على أنْ يكونَ ذلك في حضورِ الأعضاءِ ووكلاءَ عنِ اللَّجنةِ الوطنيةِ للمعلوماتيةِ والحرياتِ؛ إعمالًا للمادةِ 226 -22 -2 عقوبات.

ولكن ما هي ضمانات نقلُ البياناتِ الشخصيةِ وفقاً للتشريعِ الأوربي الجديدِ المتعلّقِ بالخصوصيةِ وحمايةِ البياناتِ الصادرِ عنِ الاتحادِ الأوروبي في 27 أبريل 2016 الذي سيدخلُ حيزَ التطبيقِ في 25 مايو 2018 ؟

لا يجوزُ للدولِ الأعضاءِ وفقاً للمادةِ 44 نقلُ البياناتِ الشخصيةِ من دولِ الاتحادِ الأوروبي إلى دولٍ خارجَ الاتحادِ، أو إلى منظماتٍ دوليةٍ، أو من تلك الدولِ والمنظماتِ إلى دولِ الاتحاد الأوروبي ألَّا وفقَ أحكامِ هذَا التشريعِ، ووفقَ المادةِ 45 يجوزُ نقلُ البياناتِ متى كانتْ تلك الدولُ أو المنظماتُ يوجدُ بها مستوىً كافٍ منَ الحمايةِ للبياناتِ الشخصيةِ، ولا يكونُ لدى الدولةِ خارج الاتحادِ الأوروبي هذا المستوَى من الحمايةِ إلَّا بعدَ مراعاةِ مجموعةٍ منَ العناصرِ في تلكَ الدولةِ، حددتها المادةُ السالفةُ الذكرِ، منها احترامُ سيادةِ القانونِ،وحقوقُ الإنسانِ وحرياتهُ الأساسية، وكذلك وجودُ سلطةٍ مستقلةٍ أو أكثر ولها أداءٌ فعالٌ في مجالِ حمايةِ البياناتِ الشخصيةِ،مع مسؤوليةِ ضمانِ وفرضِ الامتثالِ لقواعدِ حمايةِ البياناتِ، والالتزاماتِ الدوليةِ الملتزمةِ بها تلك الدولةُ أو المنظمةُ، و أيُّ التزاماتٍ أخرى ناشئةٍ عن اتفاقياتٍ أو

صكوكٍ ملزمة قانوناً، وكذلك عن مشاركتها في أنظمةٍ متعددةِ الأطرافِ أو إقليميةٍ، ولا سِيَّمَا فيما يتعلَّقُ بحمايةِ البياناتِ الشخصيةِ، كما أوجبتِ المادةُ السالفةُ الذكرِ؛ أنْ يُرَاجَعَ مستوَى حمايةِ البياناتِ الشخصيةِ في تلك الدولِ أو المنظماتِ بشكلٍ دوريٍّ على الأقل كلَّ أربعِ سنواتٍ،على أنْ تنشرَ مفوضيةُ الاتحادِ الأوروبي في الجريدةِ الرسميةِ للاتحادِ، وعلى موقعِهَا على الإنترنت قائمةً بالدولِ والجهاتِ أو المنظماتِ الدوليةِ التي تتمتَّعُ بمستوىً كافٍ منْ حمايةِ البياناتِ الشخصيةِ.

ونرَى أنَّ مثلَ هذه الإجراءاتِ توسّعُ من نطاقِ حمايةِ الخصوصيةِ المعلوماتيةِ أو البياناتِ الشخصية الإلكترونية؛ وذلك لحمايتِهَا في حالِ نقلِهَا إلَى خارجِ حدودِ الدولةِ، بأنْ تجعلَهَا تتمتَّعُ بالمستوَى ذَاتِهِ منَ الحمايةِ عندَ نقلها منْ بلادٍ إلَى آخرَ، وعدم السماحِ بنقلِ البياناتِ إلَى جهةٍ ليس لديها مستوىً كافٍ من الحمايةِ؛ لحماية البياناتِ والمعلومات الشخصيةِ وتأمينها ضدَّ مخاطرِ الاطلاعِ أو الإفشاءِ أو الاستخدامِ غيرِ المشروعِ خاصَّةً.

وجديرٌ بالذكرِ أنَّ المادةَ 49 منَ التشريعِ ذَاتِهِ أجازتْ نقلَ البياناتِ الشخصيةِ إلى خارجِ الاتحادِ الأوروبي، حتى في حالِ عدمِ وجودِ مستوىً كافٍ منَ الحمايةِ في الدولِ أو المنظماتِ الدوليةِ المنقولِ إليهَا البيانات في عدَّةِ حالاتٍ، منها الموافقةُ الصريحةُ للمعنِي بالبياناتِ على نقلِها بعدَ إبلاغِه بالمخاطرِ المحتملةِ التي قدْ تتعرَّضُ لها البياناتُ، أو إذَا كانَ النقلُ ضروريّاً لأسبابٍ تتعلَقُ بالمصلحةِ العامةِ، أو أنْ يكونَ النقلُ أو التحويلُ ضروريّاً لإنشاءِ الدعاوى القانونيةِ أو ممارستِهَا أو الدفاعِ عنها، أو أنْ يكونَ النقلُ ضروريّاً لحمايةِ المصالحِ الحيويةِ للمعنِي بالبياناتِ أو الأشخاصِ الآخرينَ متى كانَ المعنِي بالبياناتِ غيرَ قادرٍ جسديًا أو قانونيًا علَى تقديمِ الموافقةِ... إلخ.

المطلبُ الثاني

مدى الحماية التي تكفلُهَا بعض التشريعات العربية للبيانات الشخصيَّةِالإلكترونيَّةِ

على الرغمِ منْ تزايدِ الاعتمادِ على الحاسبِ الآلي والإنترنت في مختلفِ القطاعاتِ بالدول العربيةِ منذُ وقتٍ ليسَ بالقريبِ،وقيامِ أجهزةِ الدولة المختلفةِ؛ كشرطةِ المرورِ والجوازاتِ وسائرِ الأجهزة الإداريةِ الأخرى بتقديمِ خدماتها بشكلٍ إلكترونيٍّ، بما يُعْرَفُ بالحكومةِ الإلكترونيةِ(117)، حيثُ أصبحتْأغلبُ المعاملاتِ والخدماتِ تحدثُ بطريقةٍ إلكترونيةٍ(118)، وضعفُ حمايةِ البياناتِ والمعلوماتِ الشخصيةِ الإلكترونيةِ يثيرُ مخاوفَ المستخدمينِ وقلقَهم؛ بسببِ عملياتِ القرصنةِ والاحتيالِ(119).مِمَّا نتجَ عنهُ الاحجامُ عنِ التعاملِ مع تلك الخدماتِ، إلَّا أنَّ المشرِّعَ في بعضِ الدولِ العربيةِ–فيما يبدُو– قد غابَ عنه مواجهةُ الآثارِ السيئةِ لاستخدامِ الحاسبِ الآلي والإنترنت، وتأثيرها على الحرياتِ الفرديةِ أو العامةِ والاقتصاد القومي.

وفي المقابلِ تفطَّنَ المشرِّعُ–في بعضِ الدولِ الأخرى– لمواجهةِ تلك الآثارِ السيئةِ، سواءٌ أكانَ بتحديثِ التشريعاتِ القائمةِ أمْ إصدارِ تشريعاتٍ حديثةٍ على اختلافٍ فيما بينهَا في التنظيمِ ونطاقِ الحمايةِ.إذْ ينبغي أن يكونَ التطورُ في تقنيةِ المعلومات في خدمة الفردِ، لا معوّقاً لحياته، ومنتهكاً لحقوقه، ولن يتحقَّقَ ذلك إلا من خلالِ التنظيمِ التشريعي لاستخدام تقنيةِ المعلومات، بشكلٍ يضمنُ الاستفادةَ من تلك التقنيةِ، ويَضَعُ الجزاءاتِ

(117) خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص49.

(118) محمد أمين الخرشة، نايف عبد الجليل الحمايدة، الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني، دراسة مقارنة ،مجلة جامعة الأزهر، سلسلة العلوم الإنسانية 2014م، المجلد 16، العدد 1، ص320 .

(119) عطا عبد العاطي السنباطي، الإثبات في العقود الإلكترونية، دراسة فقهية مقارنة، دار النهضة العربية القاهرة، 2008م، ص 67،68.

الرادعةَ للمجرمينَ والعابثينَ بخصوصياتِ غيرهم، وغيابُ التنظيمِ التشريعي من شأنه أنْ يجعلَ تقنيةَ المعلوماتِ آفةً على الفردِ والمجتمعِ، وسنحاول من خلالِ هذه الجزئيةِ من الدراسةِ معرفةَ مدى فاعليةِ تلك التشريعاتِ في توفيرِ حمايةٍ للخصوصية المعلوماتية، كما يأتي:

أولاً:حمايةُ البياناتِ الشخصيةِ الإلكترونيةِ في التشريعِ السعودي:

أدَّى التطوُّرُ السريعُ في مجال تقنيةِ المعلوماتِ إلى ظهورِ أنماطٍ جديدةٍ من المعاملاتِ وجرائمَ مستحدثةٍ لم تكنْ موجودةً من قبل، ولما كانَ القانونُ هو مرآة المجتمع فقد صدرَتْ في المملكةِ العربيةِ السعوديةِ مجموعةٌ من التشريعاتِ الخاصةِ، تهدفُ إلَى مواكبةِ المجتمعِ والقانونِ مع تلك المتغيراتِ، ومن تلك التشريعات:

1. **نظامُ الاتصالاتِ لسنةِ 2001م:** أكَّدتِ المادةُ الثالثةُ على سريةِ الاتصالاتِ وأمنِ المعلوماتِ، ومنعتِ المادةُ 37 مزودَ خدمةِ الإنترنت وشركاتِ الاتصالاتِ منِ التقاطِ أيّ مكالماتٍ هاتفيةٍ أو معلوماتٍ منقولةٍ عبرَ شبكاتِ الاتصالِ العامةِ، ونعنِي بذلكَ البياناتِ أو المعلوماتِ التي حازها مشغلُ الخدمةِ وتتصلُ بالمشترك؛ كالاسمِ، وتاريخِ الميلادِ ومكانِهِ، والمهنةِ، والبياناتِ الخاصةِ بوسيلةِ إثباتِ الشخصيةِ، ومحلِ الإقامةِ... إلخ[120].

وتعاقبُ على الكشفِ المتعمدِ عنِ معلوماتِ أو محتوياتِ أيّ رسالةٍ اعتُرِضَتْ خلال إرسالها، متى كان الكشفُ عنها خارج نطاق الواجبِ، وهذه الجريمةُ يلزمُ لقيامِهَا توافرُ القصدِ العام، فالقصدُ العام يتحقَّقُ بإرادةِ الفعلِ الإجرامي، مع العلمِ بالعناصرِ التي يتكوَّنُ منها الركنُ الماديُّ للجريمة[121]، ولا عقابَ إذا

(120) راجع : إبراهيم حامد طنطاوي، أحكام التجريم والعقاب في قانون تنظيم الاتصالات، دراسة تأصيلية وتحليلية لنصوص القانون رقم 10 لسنة 2003م، دار النهضة العربية، القاهرة، 2003م، ص 149.

(121) محمد زكي أبو عامر،سليمان عبد المنعم، قانون العقوبات الخاص، منشورات الحلبي الحقوقية، بيروت، 2004م، ص 79.

تخلَّفَ القصدُ أو كانَ الكشفُ متعمداً، ولكن في الحالاتِ التي يجيزُهَا القانونُ.غيرَ أنَّ هذا القانونَ وإن كانَ يكفلُ الحمايةَ للرسالةِ ومحتوياتها؛ إلَّا أنَّه كما يتضحُ في الموادِ 13و 37 يوفرُ الحمايةَ للاتصالاتِ التي تُجْرَى عبرَ شبكاتِ الاتصالِ العامَّةِ منْ دُونِ غيرها؛ كشبكاتِ الاتصالِ الخاصَّةِ والعاملينَ بها، فلا يمكنُ الاعتمادُ عليه في توفيرِ حمايةٍ فعالةٍ للبياناتِ الشخصية الإلكترونيةِ بشكلٍ عامٍّ ضدَّ مخاطرِ المعالجةِ الآليةِ للبياناتِ خَاصَّةً.

2. **نظامُ مكافحةِ جرائمِ المعلوماتيةِ لسنةِ 2007م:**لَا شَكَّ فِي أنَّ الجرائمَ المعلوماتيةَ تشكِّلُ مخاطرَ جسيمةً على الحرياتِ الفردية؛ وذلك لاعتمادِهَا على تقنيةِ المعلوماتِ والإنترنت، وهي دائمًا في تطورٍ مستمرٍّ، ولذلك أصدَرَ المشرِّعُ هذا النظامَ لحمايةِ الحقوقِ والحرياتِ، والحدِّ منَ الجرائمِ المعلوماتيةِ، والمساعدة على تحقيقِ الأمنِ وحفظِ الحقوقِ المترتبةِ على الاستخدامِ المشروعِ للحاسباتِ الآليةِ والإنترنت بالإضافةِ إلى حمايةِ الاقتصادِ القومي والآدابِ العامةِ[122].

وُيْقَصَدُ بالجرائم المعلوماتيةِ سلوكٌ غير مشروعٍ يرتبطُ بالمعالجة الآليةِ للبيانات أو نقلها[123] أو غشٍّ معلوماتي ينصرفُ إلى سلوكٍ غير قانوني، يتعلَّقُ بالمعلوماتِ التي عُولِجَتْ[124]، في حين توسَّعَ النظامُ في تعريفها بأنَّها أيُّ فعلٍ يرتكب متضمنًا استخدامَ الحاسبِ الآلي أو الشبكةِ المعلوماتية بالمخالفةِ لأحكامِ النظام[125]، وتعاقبُ المادةُ الثالثةُ على التنصُّتِ عمَّا هو مرسَلٌ عبر شبكة المعلومات أو عن

(122) المادة الثانية من نظام مكافحة جرائم تقنية المعلومات السعودي.

(123) عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، رسالة دكتوراه، جامعة عين شمس،2001م، ص42.

(124) راجع : علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، 1997م، ص2.

(125) المادة الأولى من نظام مكافحة جرائم تقنية المعلومات السعودي.

طريقِ الحاسب الآلي منْ دونِ حقٍّ، و على الالتقاطِ أو الاعتراض، وأيِّ فعلٍ يشكِّلُ مساسًا بحرمة الحياة الخاصةِ باستخدام الهواتفِ المحمولة المزودةِ بكاميرا أو ما في حكمها، وإذا كان يُقْصَدُ بالالتقاطِ مشاهدةُ البيانات أو الحصول عليها منْ دونِ مسوّغٍ قانوني صحيحٍ[126] فإنَّ التنصُّتَL'écoute يعني التجسُّس على ما هو مرسلٌعبر شبكة المعلوماتِ أو عن طريقِ الحاسب عن طريقِ الأذنِ باستراقِ السمع.

ويهدفُ المشرع بهذا النصّ إلى حماية نقل البياناتِ، والحق في احترام المراسلاتِ وحرمةِ الاتصالاتِ، وكافة أشكالِ النقل الإلكتروني للبياناتِ والمعلومات، والنشاطُ الإجرامي للجريمة يتحقَّقُ بالاعتداء على الرسائلِ المتبادلة عبر البريدِ الإلكتروني، أو مصيدةِ البيانات التي تلتقط البيانات[127].

ولا شَكَّ فِي أنَّ عبارة "ما هو مرسَلٌ عبرَ الشبكة وكل فعل" قد وسَّعتْ من حماية الخصوصيةِ في مواجهة وسائلِ التقنية الحديثةِ،بحيث تشملُ الأحاديثَ والصورَ الشخصية والرموزَ وعناوينَ البريد الإلكتروني... إلخ، وأي فعلٍ ينطوي على المساسِ بالخصوصيةِ عبر تلك الأجهزةِ،وإن كان الأمرُ يقتضي–في نظرنا– بيانُ الأفعال المعاقَبِ عليها على وجهِ التحديدِ تماشياً مع مبدأ شرعيةِ الجرائم والعقوباتِ، والفصل بين سلطة التشريعِ والقضاء.

جديرٌ بالذكر أنَّ المشرّعَ الفرنسي يعاقبُ بمقتضى المادة 226–1عقوبات على انتهاكِ حرمة الأصواتِ الخاصة، وصورة الشخصِ في مكانٍ خاص بالحبسِ سنةً وغرامة 45 ألف يورو، وأضيفتْ مادةٌ جديدةٌ هي المادة **226–2-1** لقانونِ العقوباتِ بمقتضى القانون رقم **1321**لسنة **2016** وبمقتضى هذه المادةِ يشدِّدُ المشرعُ من العقوبة، ويجعلها الحبسَ سنتين وغرامة 60 ألفَ يورو إذا وقع الاعتداءُ بالطريقة المنصوصِ عليها في المواد

(126) المادة الأولى من نظام مكافحة جرائم تقنية المعلومات السعودي.

(127) حسني الجندي، التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، الكتاب الثالث، قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، مِنْ دُونِناشر ومكان نشر، الطبعة الأولى، 2009م، ص 25 .

226-226،1-2 على الأصواتِ الخاصةِ والصور الشخصيةِ ذات الطابع الجنسي ، كما تطبّقُ العقوباتُ ذَاتُهَا على منْ يقوم بنشرِ أو عرض الصوت الخاص أو الصورةِ ذات الطابع الجنسي للجمهورِ، أو لطرفٍ ثالثٍ ، بالطرق المحددة في المادة 226-1[128].

كما اهتمَّ المشرعُ السعودي بحماية السر المصرفيsecret bancaire باعتباره من أهمِّ المبادئ التي يقومُ عليها العملُ المصرفي، إذْ يشعر المتعاملين مع المصرفِ بالطمأنينة على سريَّةِ أعمالهم المصرفية[129]، وبطاقات الائتمان التي تُعَدُّ وسيلةً هامَّةً من وسائل الدفعِ الإلكتروني للمال، حيث تعتبرُ بمثابة صكٍّ أو بطاقةٍ تصدر عن مؤسسةٍ ماليةٍ باسم شخصٍ معيَّنٍ، وتقومُ بوظيفتي الوفاء والائتمان[130]، وتُمَكِّنُ صاحبَهَا من شراءِ السلع و الخدمات من مُعتَمِدِ البطاقةِ منْ دونِ دفع الثمن في الحال؛ لتضمنها التزامَ المصدر بالدفع، أو تمكّنُ صاحبها من سحب الأموالِ من المصارف[131]، إذْ تسهّلُ عليهم الوفاءَ بالتزاماتهم المالية في مواجهة الغير[132]، لذلك نجدُ المادة الرابعة تعاقبُ على الوصول منْ دونِ حقٍّ إلى البيانات البنكيةِ أو الائتمانية، أو المتعلقةِ بملكية أوراقٍ ماليةٍ؛ للحصولِ على بياناتٍ أو معلوماتٍ أو أموالٍ، وكل ما تتيحه من خدماتٍ، فلا تقومُ الجريمةُ متى حدثَ

---

(128) المادة 226-2-1 من قانون العقوبات الفرنسي والمضافة مؤخراً بالقانون رقم 3121 لسنة 2016م بشأن الحكومة الرقمية.

Loi n° 2016-1321 du 7 octobre 2016 pour uneRépubliquenumérique

(129) عبد القادر عطير، سر المهنة المصرفية في التشريع الأردني، دراسة مقارنة، الطبعةالأولى، دار الثقافة للنشر والتوزيع، عمان، 1996، ص2.

(130) فايز رضوان، بطاقات الوفاء، المطبعة العربية، القاهرة، الطبعة الأولى، 1990، ص71.

(131)راجع: عمرسالم، الحماية الجنائية لبطاقات الوفاء، دار النهضة العربية، القاهرة، الطبعة الأولى، 1995، ص 14.

(132) فياض ملفي القضاة، مسؤولية البنوك الناتجة عن استخدام الكمبيوتر كوسيلة وفاء ، كتاب بحوث مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون،1-3 مايو 2000م، جامعة الإمارات العربية المتحدة ، كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتجية ومركز تقنية المعلومات بالجامعة، الطبعة الثالثة،2004م،ص 930 .

الوصولُ إلَى تلك البياناتِ في الأحوال التي يجيزُها القانون،فقد يتطلبُ الأمرُ الكشفَ عن البيانات والمعلوماتِ في إطار مكافحةِ الإرهاب والجريمة المنظمة وغسلِ الأموال، إذ ينبغي أن تكتسيَ البياناتُ الشخصية للفرد بطابعِ السرية،غير أنَّ مكافحةَ الإرهاب قد تقتضي إحداث توازنٍ دقيقٍ بين الحقِّ في خصوصية المعلومات والحقِّ في الأمن(133)، فكلاهما من حقوق الإنسان الواجبِ احترامُها.

وفيما يتعلَّقُ بالدخولِ إلَى النظام أو المواقع نجد أنَّ المادة الثالثة في فقرتها الثانيةِ تعاقبُ على الدخول غير المشروع؛ لتهديد شخصٍ أو ابتزازه لحمله على القيامِ بعملٍ معينٍ أو الامتناع عنه، أما الفقرة الثالثة من المادة الثالثة تعاقبُ على الدخول غير المشروع إلى المواقعِ الإلكترونية(134)، أو الدخول إليها لتغيير تصميماتِ الموقعِ أو إتلافه أو تعديلهِ أو شغل عنوانه، في حين تعاقبُ المادةُ الخامسةُ على فعلِ الدخول غير المشروع؛ لإلغاء البياناتِ أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو القيام بإعادة نشرها.

أمَّا عن المادة السابعة فتعاقبُ على الدخول غير المشروع إلى موقعٍ إلكترونيٍّ أو نظامٍ معلوماتي مباشرةً أو عن طريق الإنترنت أو بواسطة أجهزةِ الحاسب؛ للحصول على بيانات تمسُّ الأمنَ الداخلي أو الخارجي للدولة أو الاقتصاد الوطني.ويتحقق الدخول غير المشروع طبقا لهذا النظام بدخول شخص بشكل متعمد إلى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مرخص للشخص بالدخول إليها. (135)

و الملاحظُ أنَّ النصوصَ السابقة تعاقبُ على الدخولِ إلَى النظام أو المواقع، وأغفلت النصَّ على تجريم صورة البقاءLe maintien غير المشروع في النظامِ،وهذه الصورة لا تقلُّ خطورةً عن صورة الدخول غير المشروع،

---

(133) Marine Farshian: op,cit,p.6.

(134) عرف نظام مكافحة الجرائم المعلوماتية السعودي في مادته الأولى الموقع الإلكتروني بأنَّه مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

(135) المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي .

وكان ينبغي النصُّ على تجريم فعلِ البقاء غير المشروعِ؛ لتوفير حمايةٍ أوسعَ للنظام والبيانات التي يحتويها،إذ يترتبُ عليه المساسُ بسرية البيانات وسلامتها.

إنَّ النصَّ على تجريم فعلِ الدخول منْ دونِ فعل البقاء غير المشروع،كانت هي ذاتُها سياسةَ المشرعِ الفرنسي فيما يتعلَّقُ بجريمة انتهاكِ حرمة المسكن، فقد كان التجريمُ القديمُ في المادة 184 عقوبات يقتصرُ على الدخول منْ دونِ البقاء غير المشروع في المنزل، وجرَّمَ المشرِّعُ بعد ذلك فعلَ البقاء غير المشروعِ بمقتضى المادةِ 226-4 عقوبات الحالي،والمعدلةِ مؤخراً بالقانونِ رقم 714-2015 الصادرِ في 24 يونيه 2015[136].

(136) راجع: المادة 184 من قانون العقوبات الفرنسي القديم والمادة 226-4 من قانون العقوبات الفرنسي الحالي ، وهذه الأخيرة تم تعديلها مؤخراً بالقانون رقم 174-2015 الصادر في 24 يونيه 2015 م

Loi n° 2015-714 du 24 juin 2015 tendant à préciserl'infraction de violation de domicile.

وكانت صياغة المادة 226-4 من قانون العقوبات الحالي قبل هذا التعديل قد نصت على الدخول أو البقاء في منزل الآخرين بالاحتيال أو التهديد أو الإكراه ، غير أن عبارة " الدخول أو البقاء " ألغيت بموجب التعديل سالف الذكر واستبدلت بعبارة " والبقاء في المنزل بعد الدخول طبقا للفقرة الأولى ..." وقد أصبحت بعد التعديل :

L'introductiondans le domicile d'autrui à l'aide de manoeuvres, menaces, voies de fait oucontrainte, hors les casoù la loi le permet, estpuni d'un an d'emprisonnement et de 15 000 euros d'amende.Le maintiendans le domicile d'autrui à la suite de l'introductionmentionnée au premier alinéa, hors les casoù la loi le permet, estpuni des mêmespeines.

وبمقتضى هذا التعديل تقع جريمة انتهاك حرمة المسكن بمجرد وجود الفاعل داخل المنزل، وتحقق فعل البقاء دونما الحاجة إلى إثبات أنَّ فعل البقاء قد حدثَ عن طريق المناورات أو التهديد أو الإكراه، بل يكفي فقط أن يكون فعل الدخول وحده قد حدثَ عن طريق المناورات أو التهديد أو الإكراه .

كما أنَّ المشرعَ لا يكتفي بالقصد العامDol général بل يتطلبُ قصدًا خاصّاً للعقابِ على فعلِ الدخولِ إلَى النظام،فالقصدُ الخاصُّ يتطلبُ أن يرتكبَ الفعل عن علمٍ وإرادةٍ، واتجاه إرادة الجاني إلى تحقيقِ نتيجةٍ معينةٍ تخرج عن عناصر الفعل[137]، وذلك بأن يكونَ القصدُ منَ الدخول التهديد أو الابتزاز أو تغييرِ تصميم الموقعِ أو إتلافهِ أو تعديلهِ أو شغل عنوانه... إلخ،وعليه فإنَّ النصوصَ السابقة لا تستوعبُ حالة الاطلاع أو التجسُّسِ على البيانات والمعلوماتِ التي يحتويها النظامُ أو الموقع، وهو ما يتناوله نصُّ المادة الثالثة في فقرتها الأولى،إذا لم يشترط تحقّقُ قصدِ خاص من الدخولِ إلَى النظام.

و لا يشترطُ لقيام الجرائم السابقة أنْ يحقِّقَ الجاني مبتغاه من الدخول،فالجريمةُ هي جريمة سلوكٌ مجردٌ، وتقع تامةً بمجرد ارتكابِ السلوك المتمثل في الدخولِ إلَى النظام أو الموقع منْ دونِ حقٍّ، وهذه الجرائمُ لا يتصور فيها الشروعle tentativeوتخرج عن نطاقه[138]، وفي إطار الوقاية من الاعتداء على الخصوصية أو البياناتِ والمعلومات الشخصية فإنَّ المادةَ السادسةَ تعاقبُ كلَّ شخصٍ يقوم بإنتاجِ ما من شأنه المساسُ بالخصوصية، وإرساله أو تخزينه عن طريق الإنترنت أو الحاسب الآلي، وحسناً فعل المشرع ذلك.

3. نظامُ التعاملاتِ الإلكترونيةِ لسنةِ 2007م: أكَّدتِ المادةُ 18 على التزامِ مقدم خدمات التصديقِ ومنْ يتبعه من العاملينَ بالمحافظة على سريةِ المعلوماتِ التي تحصَّل عليها بسبب نشاطه، باستثناءِ المعلومات التي سمحَ صاحبُ الشهادة بنشرها،أو في الحالات التي يجيزُها القانونُ، وتتطلب السريةَ أنْ يحافظَ مقدمُ الخدمات على البيانات التي يقدمُها العميلُ لحفظها أو تبادلها أو استخدامها في إصدارِ شهادة التوثيق، أو إعداد مفاتح التوثيق الإلكتروني، فالتصديقُ الإلكترونيُّ يعمل على خلق بيئةٍ إلكترونية آمنةٍ لمن يريدُ التعاملُ عبر الإنترنت، ولذلك

(137) عمر السعيد رمضان، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، منْ دونِ تاريخ نشر، ص 258.

(138) علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2008، ص 386-387.

يكتسي أهميةً كبيرةً في مجال المعاملاتِ الإلكترونيةِ وتكنولوجيا المعلومات[139]، كما أكَّدَ النظامُ على احترام مبدأ الغايةِ من جمع البياناتِ، فحظرت المادةُ 23 في فقرتها الثانية على مقدم خدماتِ التصديق استغلالَ المعلوماتِ التي جمعها عن طالبِ الشهادةِ لأغراض أخرى خارج إطار أنشطة التصديق، منْ دونِ موافقة المعني، أمَّا الفقرةُ الثالثة منَ المادةِ ذَاتِهَا فقد أكدت على سريةِ البيانات وحمايتها منْ مخاطرِ الكشفِ عن سريتها للغير، فحظرت على مقدمِ خدمات التصديق إفشاءَ المعلومات التي اطَّلَعَ عليها بحكم عمله، ما لم يأذنْ له صاحبُ الشهادة بإفشائها، أو في الحالات التي يجيزُها القانون.

فيلزم لقيام الجريمة أن يكونَ الإفشاءُ قد حدثَ للبيانات أو المعلومات التي وصلت لمقدم الخدماتِ الإلكترونية بحكم عمله، وليس كافة البيانات والمعلومات،فهي بياناتٌ لها علاقةٌ بعمله،فلا تقوم الجريمةُ عندما تُكْشَفُ المعلوماتُ بموافقة المعني أو في الحالات التي يجيزُها القانون، وهذه الجريمة من الجرائم التي يلزم لقيامها تحقُّقُ القصد الجنائي بعنصرَيْهِ العلمِ والإرادةِ، بأن يكون مقدمُ خدمات التصديق عالماً بأنَّه يقومُ بإفشاء المعلومات التي قدِّمتْ له، وأنْ تتجه إرادته إلى ارتكاب الإفشاء[140]. كما نجد المادةُ ذَاتُهَا قد وفرت حمايةً للبيانات ضدَّ مخاطر التجسُّسِ أو السرقة أو الاحتيال، من خلال تجريم الدخولِ على منظومة توقيعٍ إلكتروني متعلقةٍ بشخصٍ آخرَمنْ دونِ تفويضٍ صحيحٍ منه، أو إذا قام بنسخها أو إعادة تكوينها أو قام بالاستيلاء عليها، ويتحقَّقُ الركنُ المادي بقيام الجاني بالدخول بطريقةٍ غيرِ مشروعةٍ منْ دونِ تفويضٍ بقصد النسخِ أو إعادة التكوين أو الاستيلاء على منظومةِ التوقيعِ الإلكتروني[141]، كما يلاحظ أنَّ النظام لم يتناول تنظيم مسؤولية وسطاء الإنترنت على خلاف

(139) زهيرة كيسي، النظام القانوني لجهات التوثيق(التصديق) الإلكتروني، مجلة دفاتر السياسة والقانون، جامعة ورقلة –الجزائر، العدد السابع ،2012م، ص 213.

(140) أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، كلية الحقوق، جامعة عين شمس، 2009، ص216.

(141) خالد بن عبدالله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، دراسة تحليلية مقارنة، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، 2009، ص138.

قانون المعاملات الإلكترونية بدولة البحرين وتونس[142]، على الرغم من أهميَّةِ الدورِ الذي يقومون به؛ مثل متعهدِ الوصول، ومتعهد الإيواء وغيرهم،وهذا نقصٌ في النظام كان ينبغي معالجته.

4.مشروعُ نظامِ حمايةِ البياناتِ الشخصيَّةِ الإلكترونيَّةِ:يعتبرُ هذا المشروعُ من الخطوات المُهِمَّة في سبيلِ الوصول إلى قانونٍ خاصّ بحماية البيانات الشخصية، ويدلُّ على الوعي القانوني ومدى الاهتمام بها، والرغبة في توفير حماية لها؛ حرصاً على احترام الحرياتِ الفردية.ويعاقبُ المشروعُ كلَّ شخصٍ ينشر بيانات الغير بعقوبة الغرامة 50 ألفَ ريالٍ، وتضاعف العقوبة في حالِ العود،سواءٌ أكانَ فيما يتعلقُ بتخزينها أمْ طباعتها ؛كالرسائل والصور الخاصة أو الصوت.

فالمجرمونَ قد يستخدمونَ الإنترنت أو تقنيةَ المعلومات للعبثِ بخصوصيات الغير، وذلك بنشر عناوين البريدِ الإلكتروني أو الصورِ وأرقام الهواتفِ، مِمَّا يشكِّلُ انتهاكاً للخصوصيةِ،وهذا من أكثر الأنشطةِ الإجراميةِ التي تُجْرَى عبر تقنية المعلوماتِ والإنترنت لدَى المراهقينَ خاصَّةً، كأنْ تُجمَعَ عناوينُ البريد الإلكتروني للشخص من فضاءِ الإنترنت، واستخدامها بإرسالها في رسائلَ إلكترونيةٍمنْ دونِ علمه، ولذلك نجد أنَّ المشروعَ يحظرُ عمليةَ نشر البريد الالكتروني، أو أرقامِ الهواتف، أو الفاكس، أو الهوية، أو السماتِ الحيوية؛ كالصورة الرقميةِ، وبيانات تمييز الوجهِ، أو نشر البيانات الطبية والجسدية والعقلية والجنسية الخاصة بالأفراد داخل المملكة أحياءً أو أمواتًا، وإذا كان يحسب للمشروع أنَّه كفل الحمايةَ للبيانات الشخصية للأفراد بشكلٍ عام ،على خلافِ الأنظمة السابقة التي تكفلُ الحماية للبياناتِ في مجالٍ معينٍ فقط، غير أنَّ هذا المشروعَ لا يكفلُ حمايةً فعالةً للخصوصية المعلوماتية.

ومن ذلك عدمُ توفير حماية للبياناتِ الشخصيةِ في حالِ نقلها إلى خارج الدولة، أو الاستخدام غير المشروع للبياناتِ،وغير ذلك من مخاطر المعالجةِ الآلية للبياناتِ الشخصيةِ، بالإضافة إلى ضعفِ العقوبات المقررة

(142) راجع: قانون المعاملات الإلكتروني بدولة البحرين وتونس.

للأفعالِ الإجرامية على خلافِ ما ورد في التشريع المقارنِ، فهذه الجرائمُ تقتضي تشديدَ العقاب على مرتكبها؛ لما يترتَّبُ عليها من ضررٍ جسيمٍ يصيبُ الفردَ،كتشويه سمعة الإناث في فضاء الإنترنت خاصَّةً، وما قد يحقِّقُه الجاني من أموالٍ ضخمةٍ من وراء تلك الجرائم .

ثانياً: حمايةُ البياناتِ الشخصيةِ الإلكترونيةِ في التشريعِ العُماني:

تعتبرُ سلطنة عمان من ضمنْ أوائل الدول العربيةِ التي أدركت مخاطرَ تقنية المعلومات على الحرياتِ، فقدأصدرتْ تشريعاتٍ حديثةً، الغايةُ منها مواجهةُ الجرائم المستحدثة أو تنظيم المعاملات الإلكترونية، ومن أهم تلك التشريعاتِ[143]:

1.قانونُ المعاملاتِ الإلكترونيةِ رقم 69 لسنة 2008م: حرصَ القانونُ على توفير الثقة والرقابة اللازمةِ لصحة المعاملات الإلكترونية وسلامتِها، و ماية البيانات والمعلومات الشخصية، بوضعه العديدَ من القواعد التي يمكن من خلالها حمايةُ تلك البيانات أو المعلوماتِ من الاعتداء عليها[144]، فالفصلُ السابعُ يؤكِّدُ على حماية بياناتِ المستخدمِ، فتعاقبُ المادةُ 43 على تجميع البيانات أو معالجتها أو استخدامها منْ دونِ موافقةِ المعني، وتعاقبُ المادةُ 44 على الإفشاء أو التحويل أو الإعلان أو نشر بيانات شخص منْ دونِ موافقته،فيما عدا الحالات التي يجيزها القانونُ،كأنْ تكونَ تلك البياناتُ ضروريةً للكشف عن جريمة أو منعها، بناءً على طلبٍ

(143) كان المشرع العُماني قد أدخل تعديلاً على قانون الجزاء سنة2001م لمكافحة جرائم الحاسب الآلي، فكانت المادة 276 مكرر تعاقب على تعمد استخدام الحاسب الآلي في الالتقاط غير المشروع للمعلومات، أو البيانات أو التنصتِ عليها، ..الخ وهذه المادة وغيرها ألغِيَتْ لاحقاً بقانون مكافحة جرائم تقنية المعلومات رقم 22 لسنة 2011م.

(144) حسين بن سعيد الغافري، شرح قانون المعاملات الإلكترونية العماني 2008/69 ، دار النهضة العربية، القاهرة،2011م، ص 2،3.

رسميٍّ من جهاتِ التحقيقِ أو إذا كانت المعالجةُ ضروريةً لحماية مصلحةٍ حيويةٍ لصاحب الشأن... إلخ، وفيما يتعلق بالعاملين يكون الالتزام بعدم الإفشاء قائمًا حتى بعد تركِ الوظيفةِ؛ احتراماً للسر المهني(145).

ثم أكدت المادةُ 45 على الحق في الإعلام أو المعلوماتِ، فأوجبت على من يحوزُ بياناتٍ بحكم عمله في المعاملاتِ الإلكترونيةِ أن يقومَ قبل المعالجة بإعلام المعني عن طريق إشعارٍ خاص بالإجراءات المتبعة لحماية البيانات الشخصية، شرطَ أنْ تتضمنَ هذه الإجراءاتُ تحديدَ هوية الشخص المسْؤُول عن المعالجة، وكذلك تحديد طبيعة البيانات، والغرض من المعالجة، وطرق ومواقع المعالجة، وكل ما من شأنه تحقيق الأمن للمعالجة.

أمَّا عن الحقِّ في الوصولِ إلَى البياناتِ Droitd'accès aux données الذي يعتبرُ من حقوق المعني بالبياناتِ، ومن المبادئ المهمَّةِ التي تقومُ عليها المعالجةُ الآمنة للبيانات الشخصيةِ، فقد أكدت عليه المادةُ 46 عندما أوجبت على الشخصِ الذي يحوزُ البيانات تمكينَ المعني من الدخولِ إلَى مواقعِ البياناتِ الشخصيةِ جميعِهَا إذا طلب ذلك(146)،وكان من المفترض أن يستتبعَ ذلك حق المعني في تعديلِ تلك البياناتِ، كأنْ يوجدَ بها خطأ ولم ينص عليه المشرع،كما تمنعُ المادةُ 47 مستخدمَ البيانات الشخصية التي جُمِعَتْ وفقًا للمادة 43 من إرسال وثائق إلكترونيةٍ للشخص الذي جمعت عنه البياناتُ، متى كان يرفض قبولها صراحةً؛ وذلك لمنع الاطلاع غير المشروع على البيانات والمعلومات، والمادةُ 48 تحظر معالجة البيانات الشخصيةِ متى كانت تلك المعالجةُ تسبّبُ ضرراً لمن جمعت عنهم البياناتُ أو تنال من حقوقهم أو حرياتهم.

2.قانونُ مكافحةِ جرائمِ تقنيةِ المعلوماتِ رقم 22 لسنة 2011م: صدر هذا القانونُ في سنة 2011م وأُلْغِيَ بمقتضاه الفصل الثاني مكرر من قانون الجزاء، ويهدفُ إلى مكافحة الجرائم المعلوماتيةِ،والاستخدام السيئ لتقنية المعلوماتِ،وعلى خلاف الوضع في التشريع السعودي يعاقبُ المشرعُ العماني بالمادةِ الثالثةِ على فعلِ الدخول

(145) قارن مع المواد 28 ،39 من مشروع قانون حماية البيانات الشخصية المصري لعام 2017.

(146) قارن مع المادة السابعة لمشروع قانون حماية البيانات الشخصية المصري لعام 2017.

المتعمد وغير المشروع للمواقعِ أو النظمِ المعلوماتية أو وسائلِ تقنية المعلوماتِ أو تجاوز الدخول المصرح به إليها أو الاستمرار فيه بعد العلم بذلك[147]، ويعالج المشرعُ من خلال الفقرةِ الأخيرةِ حالَ البقاء غير المشروعِ في النظم أو المواقع الإلكترونية أو وسائلِ تقنية المعلومات،وهذا الفعل لا يقلُّ خطورةً عن فعل الدخول غير المشروع، ويحقِّقُ الغايةَ ذَاتَهَا التي قصد المشرعُ تحقيقها من تجريم فعل الدخول غير المشروع، وهي الاطلاعُ والتجسُّسُ على البيانات... إلخ، ولا تقومُ الجريمة بطبيعة الحالِ متى حدثَ الفعلُ في الحالات التي يجيزُها القانون.

وتغلَّظُ العقوبةُ إذا ترتَّبَ على الأفعالِ السابقة تعرضُ البيانات والمعلومات الإلكترونية المختزنة في النظام أو وسائل تقنية المعلومات للإلغاءِ، أو التعديلِ، أو التغيير، أو التشويهِ، أو الإتلافِ، أو النسخِ، أو التدمير، أو النشرِ، أو إعادة النشرِ، أو تدمير النظمِ المعلوماتية أو سائل تقنية المعلومات أو شبكة المعلومات، أو إلحاقِ الضررِ بالمستفيدين أو المستخدمين، أو إذا وقعت الأفعال السابقة من شخصٍ أثناء تأديةِ عمله، وذلك وفقًا للمادة الرابعة، والإتلافُ أو التدميرُ قد يتحقَّقُ بالطرق التقليديةِ؛ كتحطيمِ النظامِ أو إشعالِ النيرانِ، ويكفي لقيام الجريمة توافرُ القصد الجنائي العام، الذي يكفي لقيامه علم الجاني بأنَّ من شأن فعله إتلافَ مالِ الغير منْ دونِ اعتدادٍ بالباعث على ارتكاب الجريمة[148].

(147) تتفق سياسة المشرع البحريني مع المشرع السعودي في هذا الشأن فلا يوجد تجريم لفعل البقاء بالنظم المعلوماتية، راجع المادة الثانية من القانون رقم 60 لسنة 2014 م بشأن جرائم تقنية المعلومات بالبحرين.

(148) طعن جنائي ليبي 24 فبراير 1987م ،الطعن رقم 33/511ق، مجلة المحكمة العليا، السنة 1 ، 2 ،العدد 25، ص 233.

غيرَ أنَّ الصورة الغالبة للإتلاف أو التدمير هي التدميرُ أو الإتلافُ المعنوي، وتتحقَّقُ هذه الصورةُ بمحوِ المعلوماتِ كليّاً أو تدميرها إلكترونيّاً أو تشويه المعلومات أو البرامج على نحوٍ يجعلها غيرَ صالحةٍ للاستعمالِ[149].

كما اهتمَّ المشرعُ بحماية البياناتِ في المجال الطبي ، فيعاقبُ على استخدام تقنيةِ المعلومات في التغييرِ أو التعديل أو الإتلاف المتعمد منْ دونِ حقٍّ لبياناتٍ أو معلوماتٍ إلكترونيةٍ في هيْأَةِ تقريرِ فحصٍ أو تشخيصٍ أو علاجٍ أو رعايةٍ طبيةٍ، مختزنة في النظام أو وسائلِ تقنية المعلوماتِ، ولا عقابَ إذا حدثتِ الأفعالُ السابقةُ في الحالاتِ التي يجيزُها القانون أو بموافقة المعني[150].

ويكفل القانونُ كذلك الحمايةَ للبيانات والمعلومات الحكومية، التي تقتضي طبيعتها أن تكونَ سريةً، وكذلك البيانات والمعلومات السرية الخاصة بالمصارفِ والمؤسساتِ الماليةِ، في إطار حمايةِ السرية المصرفية، وذلك بالعقابِ على الدخولِ المتعمدِمنْ دونِ حقٍّ إلى النظمِ أو المواقع الإلكترونية؛ بقصد الحصولِ على تلك البيانات والمعلوماتِ، وتغلظُ العقوبةُ إذا ترتَّبَ على ذلك تعرضُ البيانات والمعلوماتِ المختزنة إلى الإلغاء أو التغيير أو التعديل أو التشويه أو الإتلاف أو النسخ أو التدمير أو النشر، فلا محلَّ لقيام الجريمة إذا كانَ الدخول غير متعمَّدٍ، أو كان لغرضٍ آخرَ غير قصد الحصول على البيانات والمعلومات المختزنة[151].

(149) هدى حامد قشقوش،مرجع سابق،ص43.

(150) المادة الخامسة من قانون مكافحة جرائم تقنية المعلومات بسلطنة عمان.

(151) المادة السادسة من قانون مكافحة جرائم تقنية المعلومات بسلطنة عمان.

كما حرصَ المشرعُ على حماية المواقعِ من مخاطرِ الاختراق أو السرقة والعبث ببيانات الموقعِ،فيعاقبُ القانونُ على الدخول المتعمد منْ دونِ حقٍّ باستخدام وسائل تقنية المعلومات لموقع إلكتروني، بقصد تغيير تصميمه أو تعديله أو إتلافه أو إلغائه أو شغل عنوانه[152]، فهذه الأفعالُ تؤدّي إلى عرقلة دخول المستخدم الشرعي إلَى النظامِ، فضلاً عمَّا يترتَّبُ على هذا الدخول غير المشروع من مساسٍ بسرية البيانات والمعلوماتِ، وإتاحةِ الفرصة أمام القراصنة لارتكاب جرائم أخرى كالتزوير أو الاحتيال[153].

ويعاقبُ المشرعُ كذلك على الاعتراضِ المتعمَّدِمنْ دونِ حقٍّ باستخدام وسائل تقنية المعلومات لخطِّ سير البيانات أو المعلومات المرسلة عبر الإنترنت أو وسائل تقنية المعلومات، أو قطع بثها أو استقبالها أو التنصُّتِ عليها[154]؛ وذلك لضمانِ سلامة نقلِ البيانات والمعلوماتِ، وكذلك عدم اطلاع الغير عليها منْ دونِ حقٍّ.

وقد وسَّعتِ المادةُ التاسعة من تلك الحماية، حيث تعاقبُ كلَّ من أدخل عمداً ومنْ دونِ حقٍّ في نظامٍ أو شبكة معلوماتية أو وسائل تقنية المعلومات، ما من شأنه إيقاف أيٍّ منها أو تعطيله عن العمل، أو أن يلغيَ أو يعدلَ أو يغيّرَ أو يشوه أو يتلف أو يدمر البرامجَ أو البيانات أو المعلومات الإلكترونية المستخدمة أو المخزنة في أيٍّ منها، مع علمه بأنَّ ذلك من شأنه إيقافُها أو تعطيلُها عن العمل، وذلك باستخدام وسائل تقنية المعلومات، وهي من الجرائمِ العمدية التي يلزم لقيامها توافرُ القصد بعنصريه العلمِ والإرادةِ،فلا تقوم إذا تخلَّفَ القصدُ،بأن حدثتِ الأفعالُ عن طريق الإهمالِ أو غيرها من صور الخطأ غيرِ العمدي[155].

(152) المادة السابعة من قانون مكافحة جرائم تقنية المعلومات بسلطنة عمان.

(153) د.خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2009، ص 278.

(154) المادة الثامنة من قانون مكافحة جرائم تقنية المعلومات بسلطنة عمان.

(155)راجع المادة التاسعة من قانون مكافحة جرائم تقنية المعلومات بسلطنة عمان.

كما قد يحدثُ إعاقة المراسلات، وهو فعلٌ يؤدّي إلى تباطؤ أو إرباك عملِ نظام المعالجة الآلية للبيانات، فيترتَّبُ عليه تغييرٌ في حالِ عمل النظام، ويتحقَّقُ ذلك بوضع أيّ عقباتٍ ماديةٍ أو فنيةٍ تحول دونَ وصولِ المراسلة، كأنْ يستخدمَ أحدُ موظفي شبكة اتصالات لاسلكية جهازًا يسمى jammer ؛ لإعاقة الاتصال بين مستخدمٍ وآخرَ للشبكة(156)، لذلك تعاقبُ المادة العاشرة مَنْ يقومُ بإعاقة أو تعطيل عمدي منْ دونِ حقّ الوصول إلى خدمات مزود الخدمة أو الدخول إلى نظام معلوماتي أو وسائل تقنية المعلومات، وذلك باستخدام وسائل تقنية المعلومات المختلفة.

وإن كان القانونُ قد وسَّعَ من الحمايةِ المقررةِ للبيانات والمعلوماتِ ووسائلِ تقنية المعلومات بتجريمِ العديد من الأفعالِ التي لم يكنِ الفصلُ الثاني مكرر من قانونِ الجزاء يعاقبُ عليها، إلَّا أنَّه لم يصلْ إلَى تحقيقِ حمايةٍ فعالةٍ للبيانات الشخصيةِ،لاَ سِيَّمَا ضدَّ مخاطر المعالجةِ الآلية للبيانات الشخصيةِ.

3.قانونُ تنظيمِ الاتصالاتِ رقم 30 لسنة 2003م:كفلَ القانونُ الحمايةَ لسريةِ الاتصالات والبياناتِ والمعلومات الشخصيةِ، فيعاقبُ على استخدامِ أجهزةٍ أو وسائل الاتصالات في غير الأحوال المرخص بها،منْ هيْأَةِ الاتصالاتِ أو حالات تأدية مهام وظيفية لدى المرخَّصِ له بقصدِ الحصول على معلوماتٍ عن مضمون الرسالةِ أو مرسلها، أو المرسل إليه إذا كان المستخدمُ لهذه الوسائل أو الأجهزة غيرَ مصرَّحٍ له منَ الهيْأَةِ لأسبابٍ تشغيليةٍ بالحصول عليها، أو كان استخدامها بقصدِ إفشاء سرية البياناتِ،وذلك فيما عدا الحالات التي يجيزُها القانون(157).

ويُعَدُّ ذلك تأكيدًا من المشرعِ على حرمة المراسلاتِ التي تحتوي على أسرارِ الفردِ وتعكس شخصيته،غيرَ أنَّ هذا القانونُ لا يوفر حمايةً فعالةً للخصوصية المعلوماتية،إذْ يكفل الحماية للبيانات والمعلومات في نطاق

(156) راجع: إبراهيم حامد طنطاوي، مرجع سابق، ص 141.

(157) المادة 61 من قانون تنظيم الاتصالات بسلطنة عمان.

الاتصالات،والتي يتحصلُ عليها العاملونَ لأسبابٍ تشغيليةٍ، لا حماية غيرها من البيانات والمعلومات الشخصيةِ التي يُحْصَلُ عليها في غيرِ تلك الأحوال، وبشكلٍ خاصّ ضدَّ مخاطرِ المعالجة الآلية للبيانات.

وتجدرُ الإشارةُ إلى أنَّ المشرعَ العمانيَّ –خلافًا للمشرع في المملكة العربية السعوديةِ والبحرين[158]– وتماشياً مع سياسةِ المشرعِ الفرنسي ومشروع قانونِ حماية البيانات الشخصية المصري لعام 2017، يقرّرُ حماية للبياناتِ حتى في حالِ نقلهِ إلَى خارجَ الدولة، فالمادةُ 49 تتطلب أن يؤخذ في الاعتبار المستوى الكافِي منَ الحمايةِ للبيانات؛كطبيعة البياناتِ ومصدر المعلومات التي تتضمنها البياناتُ خاصَّةً، والغرضُ من المعالجة ومدته،وكذلك القانونُ المطبَّقُ في الدولة المنقول إليها البيانات، ومدى التزاماتها الدولية، وكذلك القواعدُ ذاتُ الصلةِ المطبقة في تلك الدولة لحماية البيانات، ولا شَكَّ فِي أنَّ ذلك يوسّعُ من نطاق حماية البياناتِ،غير أنَّ ذلك يقتضي أنْ تتولَّى الجهةُ المختصةُ بضمان احترامِ هذه القواعد في الدولةِ التنسيقَ مع نظيرتها التي تمتَّعُ بالسلطاتِ نفسِهَا في الدولةِ المنقولِ إليهَا البيانات؛ لضمان تطبيقِ تلك الأحكام على نحوً أفضل[159].

ويلاحظُ أنَّ المادةَ الثامنةَ من مشروعِ قانون حماية البيانات الشخصية المصري لعام 2017 قد نصَّتْ على حقِّ المعني بالبيانات في تصحيحِ أو مسح أو عدم السماحِ بالدخولِ إلى البيانات الشخصية التي تتعارض معالجتها مع أحكام القانونِ،في حين نصَّتِ المادةُ التاسعة من المشروعِ ذَاتِهِ على حقِّ المعني في الاعتراض على معالجة البياناتِ التي تخصُّه، على أن يكونَ ذلك لأسبابٍ مشروعةٍ، أو استعمالها لأغراضِ الاستقراء التجاريةِ (التسويق المباشر)،وهو ما لم ينص عليه المشرّعُ العماني أو السعودي،كما أنَّ المشروع السالف الذكر في المادة 12 يضفي على البياناتِ المتعلقةِ بالعلاقاتِ الزوجيةِ والحالةِ الجنسيةِ، والتوجهاتِ السياسيةِ، والأصلِ العرقي والمعتقدات الدينية، والصحة والحالة النفسية للشخص، وبيانات الأطفال –حمايةً خاصَّةً، فلا يجوز معالجتُها إلَّا

(158) راجع قانون مكافحة الجرائم المعلوماتية بدولة البحرين.

(159)انظر كذلك: المادة 44 من مشروع قانون حماية البيانات الشخصية المصري لعام 2017م .

بتصريحٍ من الجهة المختصة، وفي جميع الأحوالِ لا يجوزُ معالجة أو جمع البيانات المتعلقة بالأصل العرقي أو المعتقدات الدينية أو العلاقات الزوجية ألَّا بغرض تحقيقِ مصلحةٍ عامةٍ، وبعد أخذِ تصريحٍ خاصّ بذلك من جهاز حماية البيانات الشخصية، ولا شَكَّ فِي أنَّ المشروعَ قد وسَّعَ من حماية تلك البيانات لأهميتها وخطورتها في تحديدِ هوية الفرد وميولهِ، وهو ما أغفلهُ المشرعُ العماني والمشرعُ السعودي والمشرعُ الليبي.

و ما هي الضمانات المقررة لحماية البيانات الشخصية للأطفال ؟

على خلافِ الوضع في التشريعات محل الدراسةِ فإنَّ المادةَ 13 من مشروع قانون حماية البياناتِ الشخصيةِ المصري لعام 2017 قد قررتْ حمايةٌ خاصَّةٌ للبيانات الشخصية للأطفالِ، عندما أوجب على مالكِ أيّ موقعٍ إلكتروني موجهٍ للأطفال أو مشغِلِهِ بوضع إخطارٍ على الموقع يوضحُ ماهية بيانات الأطفالِ، وكيفية استخدامِها، والسياسة المتبعة في الإفصاحِ عنها، كما أوجبَ على المالكِ أو المشغلِ للموقع الإلكتروني الحصولَ على موافقةٍ صريحةٍ من ولي أمر الطفل الذي تُجرَى معالجةُ بياناتٍ شخصيةٍ عنه، وتزويد ولي الأمر بناءً على طلبه –وبعد التأكُّدِ من هويته– بتوضيحٍ لنوعِ البياناتِ الشخصية التي جرَتْ معالجتُها، والغرض من المعالجة، ونسخة من البيانات التي جرتْ معالجتها أو جمعها عن الطفل، وأنْ يقومَ بحذفِ أو مسح البياناتِ أو قفِ معالجة أيّ بياناتٍ شخصيةٍ جرَى تجميعها عن الطفل إذَا طلب ولي الأمر ذلك ، وعدم طلب أيّ بياناتٍ شخصيةٍ عن الطفل كشرطٍ للمشاركة في أيّ نشاط يقدّمه الموقع.كما أنَّ تشريعَ حماية الخصوصيةِ والبيانات الجديدِ الصادر عن الاتحاد الأوروبي في **27** أبريل **2016** الذي سيدخل حيزَ التطبيق في **25** مايو **2018م** يتطلبُ–حتى تكونَ معالجةُ بياناتِ الطفل مشروعةً– موافقةَ الطفلِ الواضحةَ والصريحة، إذَا كان عمره ستَّ عشرةَ سنةً على الأقل، ولا تكون المعالجةُ مشروعةً قبل هذه السن إلَّا بعد الحصول على موافقة ولي أمر الطفل،وقد أجاز التشريعُ الأوروبي للدول الأعضاء تحديدَ سنٍّ أقل للطفل؛ لغرضِ الموافقة على معالجةِ بياناته الشخصية، على ألَّا تقلَّ في جميع الأحوال عن ثلاثَ عشرة سنةً.

وحسناً فعلَ المشرعُ بذلك؛ تقديراً لسن الطفل وظروفه بعدم إدراكه لخطورة الإجراءِ، وما قد يترتَّبُ عليه من آثار، ومنعاً لاستغلال الأطفالِ واستخدامِ بياناتهم الشخصية بشكلٍ غير مشروعٍ عبر الإنترنت والعالم الافتراضي في الإعلانات والدعاية على المنتجات والخدمات، أو بيع صورهم وبياناتهم للشركاتِ التجارية، أو المواقع الإلكترونية الجنسية الإباحية،ومن ثم لا تكونُ معالجة البيانات الشخصية للطفل مشروعةً إذا كان عمرُه أقلَّ من ستَّ عشرةَ سنةً، أو كان يبلغها وكانت موافقته غير صريحة وواضحة، فالموافقة الضمنية أو غير الواضحة لا تعفي القائمَ على المعالجة من المسؤولية، إلَّا إذا كان قد تحصَّلَ على الموافقةِ الصريحة على المعالجة من ولي أمر الطفل، لاَ سِيَّمَا مع سياسةِ الخصوصيةِ التي تضعها بعض المواقع، وتكون غير واضحة للمستخدمِ في كثيرٍ من الأحيان، وإن كان الأمرُ يقتضي –حسب وجهة نظرنا– إلزامَ مالكِ الموقع الإلكتروني أو المشغِّلِ بضرورةِ توضيحٍ وتبسيطٍ أكثرَ لسياسة الخصوصية الخاصة بالموقع، بعيداً عن التعقيدات، بشكلٍ يضمن فهمَ المستخدم، لاَ سِيَّمَا الأطفالُ والقاصرون لسياسة الخصوصية بشكلٍ أفضل.

ثالثاً: حمايةُ البياناتِ الشخصيةِ الإلكترونيةِ في التشريعِ الليبي:

لئن كانتْ تقنيةُ المعلومات وتطبيقاتها كالحاسب الآلي والإنترنت قد أضحتْ من الأهمية بحيثُ تستخدمُها أغلبُ الأجهزة في الدولة والقطاع الخاص، فإنَّ المشرعَ الليبي لم يقدمْ على مواجهةِ سلبيات تلك التقنية وتأثيرها على الحريات[160]–وذلك على خلافِ الوضع في بعضِ التشريعاتِ العربية ومنها قانونُ الجزاء العماني، حيثُ أدخل المشرعُ تعديلاتٍ على قانون العقوبات، الهدفُ منها مكافحةُ الجرائم المستحدثة أو جرائم الحاسب الآلي– فقد ظلَّ

(160) أضيفت إلى قانون العقوبات الفرنسي مادة جديدة برقم 226–4–2 بالقانون رقم 366لسنة 2014

Loi n° 2014–366 du 24 mars 2014 pour l'accès au logement et un urbanismerénové

وتعاقبُ هذه المادةُ كلَّ من يرغم شخصًا على مغادرة المكان الذي يقيم فيه، عن طريق المناورات أو التهديد أو الإكراه –في غير الأحوال التي تجيزها الدولة وبمساعدتها وفقاً لأحكام المادة 153–1 ـمن قانون المرافعات المدنية والتنفيذ – بالحبس ثلاثَ سنواتٍ وغرامة 30 ألفَ يورو.

قانون العقوبات الليبي بعيداً عن أيّ تعديلاتٍ يمكنها مواجهةُ الإجرام الحديث أو الجرائم المعلوماتية،وفي ظلِّ هذا الوضع بات قانونُ العقوبات عاجزاً عن مواجهةِ تلك الجرائم، إذْ لا يزالُ رهن الأفكار التقليدية، ولم تلحقْ نصوصه التطوُّر الذي لحق بالجريمة.

إنَّ القواعد التقليدية في قانون العقوباتِ لا تكفي لتوفير حمايةٍ فعالةٍ للخصوصية المعلوماتية أو البيانات والمعلومات الشخصيةِ الإلكترونية، لاَ سِيَّمَا ضد مخاطر المعالجة الآلية، فقد صدرتْ تلك النصوصُ لمواجهةِ أفعالٍ معينةٍ في بيئةٍ تختلف تمامًا عن بيئةِ التقدُّمِ السريعِ في مجالِ تقنيةِ المعلومات،إذ لا حمايةَ فعالةً للبياناتِ والمعلومات الشخصيةِ في إطار القواعدِ التقليدية في التشريع الليبي، الأمر الذي جعلَ التشريعاتِ المقارنة لا تكتفي بتلك القواعد التقليدية، وجاءت بأحكامٍ خاصَّةٍ ومستحدثةٍ لمواجهة ذلك النمطِ المستحدثِ منَ الجرائم، وسنتناول بعض هذه القوانين لأهميتها كما يأتي:

1. مشروعُ الدستورِ الليبي لسنةِ 2017:

صدرَ عن الهيأة التأسيسيةِ لصياغة مشروع الدستور، مشروع الدستور الليبي في 19 يوليو 2017 في مدينة البيضاءِ، وإدراكًا بأهمية حمايةِ البيانات الشخصيةِ والوعي المجتمعي بالتحديات التي تتعرَّضُ لها، خاصةً مع زيادة التقدمِ العلمي والتكنولوجي في مجالِ تقنية المعلوماتِ والحاسب الآلي، وما قد يترتَّبُ على ذلك من مخاطر وأضرار جسيمةٍ تمس الحياة الشخصية للفردِ، فقد أكدت المادةُ 35 من المشروع صراحةً على حماية البياناتِ الشخصية للمواطن بقولها: "للحياة الخاصة حرمةٌ، ولا يجوزُ دخول الأماكنِ الخاصة إلَّا لضرورة، ولا تفتيشها إلَّا في حالة التلبس أو بأمرٍ قضائي،كما لا يجوزُ المساسُ بالبيانات الشخصيةِ أو إخضاعِ الاتصالات والمراسلاتِ

للمراقبة إلَّا بإذنٍ من القاضي المختص" [161]، كما أكدتِ المادةُ 46 على أنْ تضعَ الدولةُ التدابيرَ اللازمة للشفافية، وتضمن حرية تلقي المعلوماتِ ونقلِهَا وتبادلِهَا، والاطلاع عليها،وتعدد مصادرها بما لا يمسُّ الأسرار العسكرية و أسرار الأمن العام،ولوازم إدارة العدالة، وحرمة الحياة الخاصة،وما اتفقَ مع دولةٍ أخرى على اعتباره سرياً، مع حقِّ الحفاظ على سرية المصدر.

فالنصُّ السابق يؤكدُ على حقِّ الفرد في الوصولِ إلى المعلوماتِ ونقلها وتبادلها، وفقاً للضوابط الواردةِ في النصّ، وإن كان من الأفضل النصُّ صراحةً على عدم جوازِ نقل البيانات أو تبادلها مع دولةٍ لا توفر تشريعاتها الحماية الكافية للبيانات الشخصية، إلَّا في حالاتٍ معينةٍ، ووفقاً لضوابطَ يحددُها القانون، والحق في محو البياناتِ وتصحيحِهَا، والاعتراض على معالجتها وفقاً للضوابط التي يضعها القانون.

وتجدرُ الإشارةُ إلى أنَّ هناك دساتيرَ اعتبرت أنَّ أمنَ الفضاء المعلوماتي جزءٌ من منظومة الأمن القومي والاقتصادي للدولةِ، ولا شَكَّ في أنَّ ذلك يعكسُ مدى الاهتمام بالبيانات والمعلومات، لما للاعتداء عليها خاصة عبر الهجمات الإلكترونية من أضرارٍ جسيمةٍ تلحق بمختلفِ القطاعات في الدولةِ،شرطَ ألَّا يؤدّي ذلك إلى المساسِ بالحقِّ في حرية التعبير باعتباره من الحقوق المكفولة في الدستور.

ومن تلك الدساتيرِ الدستور المصري لسنة 2014،فقد نصَّتِ المادةُ 31 (من الباب الثاني:المقومات الأساسية للمجتمع) على أنَّ "أمن الفضاء المعلوماتي جزءٌ أساسيٌّ من منظومةِ الاقتصادِ والأمن القومي، وتلتزم الدولةُ باتخاذِ التدابيرِ اللازمةِ للحفاظِ عليه،على النحوِ الذي ينظمه القانونُ.

(161) كفلت بعض الدساتير العربية صراحةً سرية وحماية البيانات الشخصية للفرد، ومن تلك الدساتير : الدستور التونسي لسنة 2014 وفقاً للفصل 24 ، الدستور الجزائري لسنة 2016 وفقاً للمادة 46 (معدل بالقانون رقم 01-16 الصادر في 6 مارس 2016، ومنشور في الجريدة الرسمية للجمهورية الجزائرية، العدد 14، بتاريخ 7 مارس 2016) .

إنَّ النصَّ على حماية البياناتِ الشخصية في الدستورِ من شأنه توفيرُ حمايةٍ فعالةٍ لها، ويلزمُ المشرعُ بإصدار قانونٍ لحماية البيانات والمعلومات الشخصيةِ، ويمنع مختلفَ السلطات والجهات والأشخاصِ في الدولة من الاعتداء على البياناتِ والمعلوماتِ الشخصيةِ، فالدستور هو الضامنُ الأول للحقوقِ والحريات؛ لسموِّه على غيره من القواعدِ والنصوصِ.

2. **القانونُ رقم (8) لسنةِ 2014م بشأنِ الرقمِ الوطني:** تكفلتِ المادةُ الأولى من القانونِ بتعريفِ الرقم الوطني بقولها: "بيانٌ رقميٌّ ذو دلالةٍ، ومدخلٌ إلى البياناتِ المعرِّفة بالفردِ بقاعدة البيانات الوطنية،ويعتبرُ مصدراً للتعرُّفِ والتأكد من الهوية الشخصية أمامَ جميع مؤسساتِ الدولةِ..."، وتقرِّرُ المادةُ الثالثة تكوينَ قاعدةِ بياناتٍ وطنيةٍ، و تشمل البيانات الأساسية للمواطن، متضمنةً الرقم الوطني، والاسم الرباعي، وكذلك اسم الأم، وتاريخ الميلادِ ومكانه، كما تشمل بياناتٍ حيويةً كالبصمة العشرية[162]، وبصمة العين، والصورة الفوتوغرافية، والتوقيع، ويسمح القانون لجميع التطبيقات والخدمات الخاصة بالمواطن الوصولَ إلى بياناتِ المواطن عن طريق قاعدةِ البياناتِ الوطنية، وعلى الرغم من أهمية وخطورة تلك البيانات على اعتبار أنَّها تدل على هوية الشخص وميوله، إلَّا أنَّ القانون السابق لم يتضمن أيَّ حمايةٍ تذكر لها،وهذا كان ينبغي على المشرع تداركه –لاَ سِيَّمَا في ظلِّ عدم وجود قانونٍ خاصٍّ بحماية البياناتِ الشخصية في القانون الليبي– فهذا النوعُ من البياناتِ كان يقتضي تقريرَ حمايةٍ فعالةٍ لها،كما هو الحالُ في التشريعات المقارنة.

(162)البصمة العشرية أو البصمة الآلية هي عبارة عن تصوير رقمي للبصمات كبصمة اليد والعين عبر ماسح ضوئي معدٍّ لهذا الغرض، وتعدُّ من الوسائل التقنية المتطورة للتأكد من هوية الفرد، وتستخدم في مجالات مختلفة، لعل أهمها المجال الأمني كالمنافذ البرية والبحرية أو الجوية، وتدخل ضمن بيانات البطاقة القومية أو الشخصية لدى العديد من الدول .

3.القانونُ رقم (17) لسنةِ 1986م بشأنِ المسؤولية الطبيَّةِ[163]: لا شَكَّ في القولِ بأهميةِ حقِّ الفرد في سلامة جسده، فللفرد الحقُّ في سلامةِ جسمه والمحافظةِ على صحته العقلية والنفسية[164]، والحقُّ في سرية المعلومات،فمحافظةُ الطبيبِ على أسرارِ المريض تجعلُ المريضَ يطمئن ويقدم أسراره للطبيب،وتلك الأسرارُ قد تكونُ ضروريةً لكي يتمكَّنَ الطبيبُ من التشخيصِ ووصف العلاجِ المناسب[165]،ومن أجل ذلك صدرَ قانونُ المسؤولية الطبية رقم 17 لسنة 1986م وأكَّدَ على حماية سريةِ البيانات والمعلوماتِ، وقضت المادةُ 13 بعدم جوازِ إفشاءِ أسرار المريض، التي يجري الاطلاعُ عليها بسببِ ممارسةِ المهنةِ، ما لم يكن ذلك للجهاتِ القضائية ووفقاً للقانون[166].

---

(163)المحكمة غير ملزمة بعرض قضايا المسؤولية الطبية على المجلس الطبي، والالتزام بما يرد في تقريره بشأن مدى قيام المسؤولية الطبية، ومن حق المحكمة اختيار طريق الإثبات الذي تراه مؤدياً إلى ذلك، يذكر أن قضاء المحكمة العليا كان يقرر خلاف ذلك، وضرورة عرض تلك القضايا على المجلس الطبي، إلا أن المحكمة العليا عدلت عن ذلك.انظر :حكم المحكمة العليا الليبية بتاريخ 23 ديسمبر 2013م، رقم 811 لسنة 53 ق، غير منشور .

(164) نبيلة غضبان، المسؤولية الجنائية للطبيب، رسالة ماجستير، كلية الحقوق، جامعة مولود معمري–تيزي وزو، 2009، ص10.

(165) وجود عقد تأمين في نطاق المسؤولية عن تعويض الضرر الناجم عن أخطاء ممارسة المهن الطبية، والمهن المرتبطة بها لا يمنع من مخاصمة المسؤول عن الضرر. حكم المحكمة العليا الليبية بتاريخ 5 فبراير 2017م، طعن مدني رقم 567 لسنة 60 ق . " غير منشور "

(166) بعد حلول شركة ليبيا للتأمين محل هيئة التأمين الطبي فإنَّها تكون ملزمة بتغطية المسؤولية المدنية الناشئة عن أخطاء المهن الطبية، والمهن الطبية المرتبطة معها، وذلك بالنسبة للمشمولين بالتغطية التأمينية الالزامية، طالما يمارسون تلك المهنة، ويُقَدَّرُ التعويض وفقاً للقواعد العامة في القانون المدني . طعن مدني ليبي 26 مارس 2017م، رقم الطعن 60/368 ق، المحكمة العليا، غير منشور .

والإفشاءُ يتحقَّقُ بالإفضاء بالسر أو المعلوماتِ إلى الغير[167] بأيّ وسيلةٍ كانت، ولو كـان بجزء من السر، وليس بكامل الوقائع السريةِ [168].

ويتعلَّقُ السرُّ بالمعلومات التي اطلع عليها الطبيبُ بناءً على صفته، ولا يشمل ما علم به منْ دونِ الاستنادِ إلى تلك الصفةِ، كأنْ يعلمَ بها من الأصدقاء أومن وسائل الإعلامِ [169]، ونطاق السرية يتعيَّنُ أنْ يشملَ المعلومات التي تصلُ إلى علمه وتتعلَّقُ بالحالة الصحيةِ للمريض، سواءٌ أكان المريضُ قد أدلَى له بها أمْ تمكن من استنباطها أو استنتاجها من حالةِ المريضِ،منْ دونِ أنْ يكونَ قد أدلى بها، وفي ذلك توسيعٌ لنطاق الحماية، غير أنَّ هذا القانون لا يوفر حمايةً للبيانات والمعلومات الشخصيةِ إلَّا من مخاطر الإفشاءِ، الذي يقعُ من الأشخاصِ الخاضعين لهذا القانون منْ دونِ غيرهم، وهم كلُّ من يمارس المهن الطبية والمهن المرتبطة بها،المشار إليها في المادتين 109 و 123 من القانون الصحي(القانون رقم 106 لسنة 1973م)،على أن يكونَ ذلك الإفشاء للمعلومات أو الأسرار التي قد جرى الاطلاعُ عليها بسبب مزاولة المهنةِ، ولا يوفر حمايةً للبيانات في المجال الطبي ضدَّ مخاطر أخرى، قد تتمثل في إتلافِ أو تعديلِ أو تغيير البياناتِ الطبية الخاصة بالمريض،كما لا يوفر حمايةً للبيانات الشخصية، ألَّا في مجالٍ معينٍ، وتبقى بعيدةً عن حمايتها ضدَّ مخاطر المعالجة الآلية للبيانات الشخصيةِ.

(167) فوزية عبد الستار، شرح قانون العقبات، القسم الخاص، الطبعة الثانية، دار النهضة العربية، القاهرة، 2000،ص 628.

(168) فوزية عبد الستار،مرجع سابق، ص 628.

(169) محمد عبد الظاهر حسن، المسؤولية المدنية في مجال الطب وجراحة الأسنان، دار النهضة العربية، القاهرة،2004، ص120.

4.القانونُ رقم (22) لسنة 2010م بشأنِ تنظيمِ الاتصالاتِ:صدر قانونُ تنظيمِ الاتصالات رقم 22 لسنة 2010، وبمقتضى المادةِ 40 منه أُلْغِيَ القانونُ رقم 8 لسنة 1990 بشأنِ الاتصالات السلكية واللاسلكية، ولم يغفل القانونُ عن التأكيد على سريةِ البيانات الشخصية وسلامتِهَا،حيثُ ألزمت المادة 15 الجهة التي تقدم الخدماتِ باتخاذ كافةِ الخطوات والإجراءات اللازمة لضمانِ سريةِ اتصالات المستفيدِ من خدمة الاتصالات، كما منعتْ تلك الجهة من اعتراضِ اتصالات المستفيدِ أو مراقبتِهَا أو تعديلِهَا أو تغييرها،غير أنَّهيجوز المساسُ بسريةِ تلك البيانات متى اقتضى الأمرُ ذلك؛ كدواعي متابعةِ وتحديدِ الأماكنِ، أو الردِّ على المضايقات أو المكالمات العدوانية أو غير القانونية أو حسب القانون،بأن تقومَ الجهةُ المقدمة للخدمات بمراقبةِ الاتصالات بناءً على طلب المستفيدِ أو طلبِ الجهات القضائيةِ المختصةِ قانوناً لدواعي المصلحة العامة في مكافحة الجريمة،كما يجوزُ للجهة أنْ تقومَ بالإجراءاتِ اللازمة لحمايةِ الأشخاصِ من الاتصالاتِ التي تتضمنُ مضايقاتٍ أو مكالماتٍ عدوانية أو غير قانونية.

كما أكدتِ المادةُ 16 على حمايةَ اتصالات المستفيد،فألزمت الجهات المقدمة للخدمة بحمايةِ اتصالات المستفيدِ بوسائلِ الحماية الأمنيةِ، ومنعها من أعمالِ الحفظ أو التجميعِ أو الاستعمالِ أو الإفشاء لاتصالاته أو معلوماته الشخصيةِ، التي يكونُ قد قدمَها لتلك الجهةِ في بداية التعاقد؛ من أجل تقديمِ الخدمة أو البيانات التي قد تطلبُها الجهاتُ المقدمة للخدمة من أجل استمرارِ الخدمةِ كصورةِ جوازِ السفر أو شهادةِ الميلادِ أو الرقم الوطني... إلخ، إلَّا في الحدودِ التي يسمحُ بها القانونُ أو بموافقةِ المستخدم الشخصيةِ، على أنْ يكونَ ذلك للأغراضِ التي قامت من أجلها دونَ سواها، وفي ذلك تأكيدٌ على عدمِ الانحراف عن الغرضِ الذي من أجله جُمِعَتْ تلك البياناتُ والمعلوماتُ الشخصية.

أمَّا عن حماية بيانات المستفيدِ من مخاطرِ الإفشاء فقد أكدتْ عليه المادةُ 26 فحظرت إذاعةَ مضمونِ رسالة الاتصالاتِ أو إفشاءَها أو إشاعتَهامنْ دونِ أنْ يكونَ هناك مبررٌ قانوني،غير أنَّ الحماية تقتصرُ على البياناتِ والمعلوماتِ التي اطلع عليهَا الجاني بحكمِ عمله، أو قامَ الجاني بإساءةِ استخدامِ المعلومات المتعلقةِ بالمستفيد، ومن ثم فإنَّه كغيره من القوانينِ التي سبقته، لا يكفل حمايةً واضحةً وفعالةً للبيانات والمعلومات الشخصية، فهو ليس بقانونٍ خاصٍّ بحماية البياناتِ الشخصية الإلكترونية، إذ تقتصرُ الحماية في ظلِّ هذا القانون على البياناتِ والمعلومات الشخصيةِ،من بعض صورِ الاعتداء على البياناتِ والمعلومات دونَ غيرها،ومن ذلك أنَّه لا يوفرُ الحمايةَ من مخاطر المعالجةِ الآلية للبياناتِ كما ورد في التشريع المقارن،كما أنَّه لا يكفلُ الحمايةَ إلَّا للبيانات والمعلوماتِ في قطاع الاتصالاتِ، وفي جانبٍ منها من أعمالِ الاعتداءِ التي تقع من العاملين في الجهة التي تقدم خدمة الاتصالات دونَ غيرها.

5.القانونُ رقم (2) لسنةِ 2005م بشأنِ مكافحةِ غسلِ الأموالِ:

صدرَ هذا القانونُ رغبةً من المشرع في مكافحةِ جرائم غسلِ الأموال ، وتعتبرُ هذه الجريمةُمن الجرائم المستحدثة[170] التي جاءتْ كنتيجةٍ للتطوُّرِ وتوظيف التقنيات الحديثةِ في مجال الجريمة، ويمكنُ تعريفُها بأنَّها تغييرُ وصفِ المالِ بالتمويهِ والإخفاءِ للمصدرِ غير المشروعِ للأموال؛ حتى تظهرَ في صورةٍ مشروعةٍ؛ للابتعاد عن الملاحقة القانونية[171].

(170)لا يشترط لإثبات جريمة غسل الأموال طريقة خاصة، بل يكفي أنْ تقتنع المحكمة بوقوع الفعل المكون لها من أيِّ دليلٍ أو قرينة تقدم لها . نقض جنائي مصري 17 فبراير 2011م، الطعن رقم 11248 لسنة 80 ق، غير منشور .

(171)MmeDjazira MEHDI, Les instruments de lutte contre le blanchIment d’argent en al gerie,thése de doctorat, universite nice sophia antipolis,2015,p6.

ومن المستقرِّ عليه قضاءً أنَّ جريمة غسل الأموال تتطلبُ–بالإضافة إلى القصد الجنائي العام– قصداً خاصّاً، يتمثَّلُ في نية إخفاء المال، أو تمويه طبيعته أو مصدره أو مكانه، أو صاحبِ الحقِّ فيه، أو تغيير حقيقته [172].

وقد سجَّلت هذه الجريمةُ تناميًا كبيرًا؛ بسبب التقدُّمِ التكنولوجي المستمر، الأمر الذي دفعَ بالمجتمع الدولي لإبرامِ العديدِ من المعاهدات لمكافحةِ غسل الأموالِ، وتمويل الإرهاب، ناهيك عن الآثارِ السلبيةِ لهذه الجريمةِ على الاقتصادِ الدولي،باعتبارها غشًّا يستهدفُ إضفاء الصفة المشروعةِ على أموالٍ ذات مصدرٍ غير مشروع [173].

وقد أوجبت المادةُ الرابعةَ عشرَ من هذا القانونِ على الجهات التي تحصل على البياناتِ والمعلوماتِ، طبقًا لأحكام هذا القانونِ المحافظةَ على سرِّيتها، وعدمَ الإفصاح عنها إلَّا بالقدر اللازمِ والضروري في التحقيقات والدعاوى والقضايا المُتعلِّقة بغسل الأموال وغيرها من الجرائم التي يعاقبُ عليها هذا القانون.

وهذا القانونُ هو الآخر لا يوفر حمايةً إلَّا للبيانات التي يُتحصَلُ عليهَا وفقاً لأحكامه دونَ غيرها، كما أنَّه يوفرُ الحمايةَ للمعلومات الشخصية فقط من مخاطر الإفشاءِ أو الكشفِ غير المشروعِ،ولا يشمل المخاطر الأخرى التي قد تتعرَّضُ لها أمنُ البياناتِ وسلامتهَا،والمعلومات الشخصية،خاصة مخاطر المعالجة الآلية.

(172)نقض جنائي مصري 12 مايو 2013م، الطعن رقم 12808 لسنة 82 ق، غير منشور، نقض جنائي مصري 13 نوفمبر 2011م، الطعن رقم 8948 لسنة 79 ق، غير منشور.

(173)CélestinFoumdjem,Blanchiment de capitaux et la fraudefiscale,

Thèse de doctorat,Université de Cergy-Pontoise, 2010,Résumé.

6.القانونُ رقم (9) لسنةِ 1968م بشأنِ حمايةِ حقِّ المؤلِّفِ:

تُعَدُّ حقوقُ الملكيةِ الفكريةِ أو الذهنية Propriété intellectuelleمن وسائلِ حماية جهودِ المبدعينَ في مختلفِ المجالاتِ، لاَ سِيَّمَا مجالُ الاختراعِ أو التأليف[174]، وفي إطار الاهتمام بحمايةِ الملكية الفكريةِ على اعتبار أنَّها ثمرةُ الابتكارِ ونتاجُ الإبداعِ في شتَّى مناحِي النشاط الإنساني [175].

فقد صدرَ عن المشرِّعِ الليبي القانون رقم 9 لسنة 1968م لحمايةِ حقِّ المؤلف، ووفقاً للمادة الأولى من هذا القانونِ يتمتَّع بالحمايةِ مؤلفُو المصنفاتِ المبتكرةِ في الآداب والفنون والعلومِ أيًّا كان نوعُ هذه المصنفاتُ أو طريقة التعبيرِ عنها أو أهميتها أو الغرض من تصنيفها، وتشملُ الحماية وفقاً للمادة الثانية:المصنفاتِ المكتوبة، والمصنفاتِ الداخلة في فنون الرسمِ والتصويرِ بالخطوط أو الألوان أو الحفر أو النحت أو العمارة، والمصنفات التي تُلْقَى شفوياً ؛كالمحاضراتِ والخطب والمواعظِ وما يماثلها، والمصنفاتِ المسرحية والمسرحياتِ الموسيقيَّة، والمصنفاتِ الموسيقية، سواءٌ أَقترنت بالألفاظ أمْ لم تقترن بها، والمصنفات الفوتوغرافية والسينمائية،الخرائط الجغرافية والمخطوطات، والمصنفات المجسمة المتعلقة بالجغرافيا أو الطبوغرافيا أو العلوم،المصنفات التي تؤدَّى بحركاتٍ أو خطواتٍ، وتكون معدَّةً ماديّاً للإخراج، والمصنفات المتعلقة بالفنون التطبيقية، والمصنفات التي تعدُّ خصيصاً أو تذاع بواسطةِ الإذاعةِ اللاسلكيةِ أو التلفزيون، وتشملُ الحماية بوجهٍ عامٍ مؤلفي المصنفات التي يكون مظهرُ التعبير عنها الكتابةَ أو الصوتَ أو الرسمَ أو التصويرَ أو الحركةَ، وتعاقبُ المادةُ 48 من القانونِ بغرامةٍ

(174) د.مؤيد أحمد عبيدات، د.مهند عزمي أبو مغلي، سلطات طالب تسجيل براءة الاختراع أثناء مدة الحماية المؤقتة وأثرها على حقوق الغير، مجلة الحقوق، الكويت، العدد الأول، السنة 34، مارس 2010م، ص 378.

والحقوق الذهنية DroitsIntellectuelsهي الحقوق التي ترد على أشياء معنوية غير محسوسة، تتمثل في إنتاج فكري للشخص، ويمكن إدراكها عن طريق الفكر المجرد، د.عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً، دراسة مقارنة، دارالنهضة العربية، القاهرة، 2010م، ص 381.

(175)نقض مصري 27 ديسمبر 2016م، الطعن رقم 3354 لسنة 85 ق، غير منشور.

لا تقلُّ عن عشرينَ جنيهاً، ولا تزيد على خمسمائة جنيهٍ كلَّ منِ اعتدى على حقوقِ المؤلف، أو قامَ ببيعها أو عرضها للبيع، أو أذاعَ على الجمهور بأيّ طريقةٍ كانت، أو أدخل إلى أراضي الدولة أو أخرج منها مصنفاً مقلّداً، مع علمه بالتقليد، أو قلَّد في البلاد مصنفاتٍ منشورةً في الخارج، وتشملها الحماية التي يقررها هذا القانونُ، ويعاقبُ بالعقوبةِ ذَاتِهَا منْ باعها أو صدَّرها أو تولَّى شحنها للخارج.كمَا أجازت المادةُالسالفة الذكر للمحكمة أنْ تقضيَ بمصادرةِ جميعِ الأدواتِ المخصَّصَةِ للنشر غير المشروعِ، التي لا تصلحُ إلَّا لهذا النشر، وكذلك مصادرة جميع النسخ محل الجريمة.

وبالنظر إلى وقتِ صدورِ هذا القانونِ فإنَّه لم يتضمنْ حمايةَ برامج الحاسبِ الآلي[176]،فضلاً على أنَّه لا يوفرُ حمايةَ للبياناتِ إلَّا في نطاقِ حقوقِ المؤلف، بعيداً عن الاعتداءاتِ الأخرى التي قد تتعرَّضُ لها البياناتُ الشخصيةُ،لاَ سِيَّمَا في ظلِّ التقنيات الحديثة.

ولكن ما هي جهود أو خطوات حمايةِ البياناتِ الشخصيةِ الإلكترونيةِ ومكافحةِ الجرائمِ المعلوماتيةِ في ليبيا؟

إنَّ عدمَ وجودِ تشريعاتٍ مستحدثةٍ في ليبيا تختصُّ بمكافحة الجرائمِ المعلوماتية أو تنظم المعاملاتِ الإلكترونية،لم يمنع مجلسَ الوزراء من إصدارِ القرارِ رقم 28 لسنة 2013م بإنشاءِ الهيْأَة الوطنية لسلامةِ وأمنِ المعلوماتِ،

ومن مهامِّ هذه الهيأة[177] –حسب قرار إنشائها– توفيرُ المُنَاخِ والمعايير الاستراتجية اللازمةِ لضمانِ تحقيقِ أمن البياناتِ الإلكترونيةِ وسلامتِهَا، ووسائل الاتصال المختلفة، بالإضافةِ إلى توفيرِ خدماتِ التشفير، وإعداد التقارير السنويةِ حول أمنِ المعلومات، وكذلك العملُ مع الجهاتِ ذاتِ العلاقة لوضعِ الإطارِ القانوني لأمنِ المعلوماتِ

(176) على خلاف الوضع في بعض التشريعات المقارنة كقانون الملكية الفكرية المصري رقم 82 لسنة 2002 م (المادة 140).

(177) انظر موقع الهيأة الوطنية لسلامة المعلومات وأمنها على الإنترنت : http://nissa.gov.ly/

وسلامتها، وتوفيرِ الأمن الفني لها، ويعدُّ التشفيرُ من ضمنِ الحلولِ المقترحةِ لحمايةِ البياناتِ الشخصيةِ المعالجةِ آليا[178].

ويتحقَّقُ باستخدام رموزٍ أو إشاراتٍ تصبح بمقتضاه المعلوماتُ المرادُ إرسالها أو تمريرها غيرَ قابلةٍ للفهم من قِبَلِ الغير، أو استخدام رموزٍ أو إشاراتٍ لا يمكن الوصولُ إلى المعلومة منْ دونها[179]، وذلك بهدفِ إضفاء طابعِ السريةِ على المعاملاتِ بإخفاء محتوياتها، ومنعِ استخدامها بشكلٍ غير قانوني، مما يؤدّي إلى ثقة الأفراد في المعاملات الإلكترونية[180].

وقد يعملُ الشخص على إخفاء جريمته باستخدامِ تقنياتِ التشفير؛ وذلك للإفلاتِ من قبضة العدالةِ الجنائيةِ، وعلى هذا الأساسِ نجدُ أنَّ المشرّعَ البحريني بمقتضى القانونِ رقم 60 لسنة 2014م بشأنِ جرائم تقنية المعلوماتِ يعاقبُ على استخدامِ التشفير في ارتكابِ أو إخفاءِ أيّ من الجرائمِ المنصوصِ عليها في هذا القانون، أو أيّ قانونٍ آخر، وذلك وفقًا للمادة التاسعةِ،وحسنًا فعلَ المشرّعُ بذلك، وللغايةِ ذَاتِهَا نجدُ أنَّ المشرّعَ الإماراتي يعاقبُ على فعلِ التحايل على عنوانِ بروتوكول الإنترنت IP باستخدامِ عنوانٍ وهميّ أو عنوانٍ عائدٍ للغير أو بأيّ وسيلةٍ أخرى بقصدِ ارتكاب جريمةٍ أو الحيلولةِ دونَ اكتشافها[181].

---

(178)Jean-Philippe Foegle: op,cit,p.4.

(179) المادة الأولى من القانون رقم 22 لسنة 2010 بشأن الاتصالات في ليبيا.

(180) د.مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2000م، ص21.

(181) المادة التاسعة من القانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة.

وبالإضافةِ إلى الهيأةِ الوطنيةِ لسلامةِ المعلوماتِ وأمنِهَا فقد صدرَ قرارُ وزيرِ العدلِ رقم 20 لسنة 2016م بإنشاء إدارةِ أبحاث ودراسات مكافحة الجريمة الإلكترونية، وقد جاءَ هذا القرارُ بناءً على طلبِ المركز؛ لعدم وجود تشريعاتٍ في ليبيا خاصَّة بمكافحة الجرائم المعلوماتية.

هذه الخطواتُ وإنْ كانت مهمَّةً وتعبرُ عن رغبةٍ صادقةٍ في توفيرِ بيئة آمنةٍ للمعلومات والبياناتِ الشخصيةِ sécurité des données –لاَ سِيَّمَا مع الاستخدامِ المتنامي للبياناتِ للشخصية والحاسبِ الآلي والإنترنت في ليبيا– ألَّا أنَّه ينبغي أنْ تكتملَ بإعدادِ قانونٍ لحماية البياناتِ والمعلومات الشخصية الإلكترونيةِ.

نخلُصُ من كلِّ ذلك بأنَّ البياناتِ الشخصيةَ الإلكترونيةَ لا تتمتَّعُ بحمايةٍ فعالةٍ في التشريعات العربيةِ محلَّ الدراسةِ، وإذا كانت هناك تشريعاتٌ توفر حمايةَ للبيانات الشخصيةِ الإلكترونية ضدَّ بعض صور الاعتداء، أو توفر الحمايةَ لبيانات ومعلوماتٍ ذاتِ طبيعةٍ خاصةٍ أو في مجالٍ معينٍ، فهي تظلُّ حمايةً غير فعالةٍ،وإذا كان هذا هو حالُ الدولِ العربية التي سنَّتْ تشريعاتٍ لمكافحة الجريمة المعلوماتيةِ؛ كالسعودية وسلطنة عمان، فوضع تلك البياناتِ سيكونُ أكثرَ خطورةٍ في التشريعِ الليبي، الذي لا توجد فيه تشريعاتٌ خاصةٌ بمكافحة الجرائم المعلوماتية، فهذا التطوُّرُ في وسائل الاتصالاتِ وتقنية المعلوماتِ ينبغي أنْ يقابله تطوُّرٌ في التشريعاتِ المنظمةِ لاستخدامِ تلك التقنيةِ، على اعتبار أنَّ القانونَ مرآةُ المجتمعِ التي تحاكي الواقعَ، لكي تكونَ التقنياتُ الحديثةُ في خدمة الفردِ ولا تنقلبُ وبالاً عليه،الأمر الذي يهدِّدُ الحرياتِ، ويعكِّرُ صفوَ حياتهِ وخصوصياتهِ.

الخَـــاتِمَـــةُ

حاولنَا منْ خلالِ هذه الدراسةُ الوقوفَ على الحمايةِ الجنائيةِ للبياناتِ الشخصيَّةِ الإلكترونيَّةِ في ليبيا، مقارنةً بالقانونِ الفرنسي وبعضِ القوانين العربيةِ،وتوصلنَا من خلالِ هذه الدراسةِ إلى مجموعةٍ منَ النتائجِ، نوجزهَا فيما يأتي:

1- على الرغمِ من الاستخدامِ الواسع وغير المحدودِ للإنترنت وتقنيةِ المعلومات والحاسبِ الآلي في قطاعاتِ الدولة المختلفةِ العامة والخاصةِ فلا يوجدُ قانونٌ خاصٌّ بحماية الخصوصيةِ المعلوماتيةِ أو البيانات الشخصيةِ الإلكترونيةِ في التشريعاتِ العربيةِ محلَّ الدراسةِ.

2- اهتمَّتِ التشريعاتُ العربيةُ محلَّ الدراسةِ – عدَا التشريعِ الليبي- بإصدارِ تشريعاتٍ لحماية حقوقِ الإنسانِ وحرياتهِ ومعاملاتهِ في الفضاءِ الإلكتروني، ونعني بذلك مكافحةَ جرائمِ تقنية المعلوماتِ، وتنظيم المعاملاتِ الإلكترونيةِ، وإنْ كان ذلك يُعَدُّ في نظرنا خطوةً مهمةً في سبيلِ حماية حقوقِ الإنسان وحرياته ضدَّ مخاطرِ التقدم العلمي في مجال تقنيةِ المعلوماتِ، التي تمتازُ بقدراتٍ عاليةٍ جدّاً في مجالِ جمعِ البياناتِ والمعلومات وتخزينِهَا واسترجاعها، ممَّا يهدّدُ خصوصيةً الفرد أكثرَ من أيّ وقتٍ مضى، غير أنَّ المشرع العربي لم يصلْ من خلال ما أصدره من تشريعاتٍ إلى توفيرِ حمايةٍ فعالةٍ إلى البياناتِ الشخصيةِ الإلكترونية،وهذه الخطواتِ وإن لم تكنْ كافيةً لتوفيرِ الحمايةِ المنشودةِ إلَّا أنَّها تظلُّ خطواتٍ مهمَّةً في سبيلِ بلوغ تلك الحمايةِ، وهذه الخطوات لم يبلغها المشرّعُ الليبي،فالتشريعاتُ الحاليةُ في ليبيا لا تزال عاجزةً عن حمايةٍ فعالةٍ لحقوق الإنسان وحرياته من مخاطرِ تقنيةِ المعلوماتِ.

ولذلك نقترحُ :

- العمل على توعيةِ الأفرادِ من مخاطرِ استخدام مواقعِ وخدمات الإنترنت، وتقنية المعلومات على البيانات الشخصيةِ، والحقّ في الخصوصية في العالمِ الافتراضي،والاطلاع المُتعمق على سياسةِ الخصوصية Politique de confidentialité الخاصة بكلِّ موقعٍ على الإنترنت قبلَ الاشتراك، خاصة فيما يتعلَّقُ بمواقع التواصلِ الاجتماعي،ومحركاتِ البحثِ، والمواقع التي تستخدم ملفاتِ تعريفِ الارتباطِ، وتتبع معلومات الكوكيز cookies.
- إلزام مواقعِ الإنترنت بضرورةِ بيان تأثير الخدماتِ التي يقدِّمُهَا الموقعُ على خصوصية المعلوماتِ، وأخذ موافقةِ المستخدمِ الصريحةِ على ذلك، وأنْ تكون وثيقةُ الخصوصيةِ مكتوبةً بأكثر من لغةٍ، وبأسلوبٍ مبسطٍ، يفهمه الشخص العادي غير المتعمق في خفايا تقنيةِ المعلومات أو الإنترنت أو الأطفال والقاصرين.
- منع مالكِ الموقع الإلكتروني أو المشغلِ من جمعِ أو معالجةِ أو حفظِ أو استخدامِ البيانات الشخصيةِ للأطفال والقاصرين منْ دُونِ الحصولِ على الموافقةِ الصريحةِ لولي الأمر.
- زيادة توعيةِ العاملين بقطاعاتِ الدولة المختلفةِ بأهميَّةِ خصوصيَّةِ البيانات والمعلوماتِ للأفراد، وكيفية المحافظة على سلامتِهَا وسريتها، وما قد يترتَّبُ على الاعتداءِ عليها من ضررٍ بالنسبة للفردِ، وكذلك الضرر الذي قد يلحقُ بقطاعي التجارة والحكومة الإلكترونية، فالمحافظةُ على سريتها مقدمةٌ مهمةٌ لنجاحِ قطاعي التجارةِ والحكومةِ الإلكترونية.
- إصدار قانونٍ خاص بحماية البياناتِ الشخصية الإلكترونيةِ، أو الحق في الخصوصية في العالم الافتراضي، ونظم معالجة البياناتِ،والتأكيد على تأسيسِ جهةٍ رقابيةٍ تكون مهمتُها الرقابةَ على عملياتِ جمع البياناتِ الشخصيةِ ومعالجتِهَا في قطاعات الدولةِ المختلفةِ، ومدى تقيد تلك القطاعاتِ بأحكام القانونِ وحماية الحقوقِ والحرياتِ من مخاطر المعلوماتيةِ، وأجهزة أمنٍ تختصُّ بقضايا الإنترنت

والخصوصية المعلوماتيةِ، وكذلك ضرورة تنظيمِ مسؤوليةِ وسطاءِ الإنترنت كمزود خدماتِ الإنترنت، وإلزامه بالالتزامات التي تكفل توفيرَ حمايةٍ فعالةٍ للخصوصية المعلوماتيةِ، أو في الفضاء الإلكتروني،وتنظيم عملِ شبكاتِ التواصلِ الاجتماعي، والمواقع الخدميةِ عبرَ الإنترنت في ليبيا؛ للوقايةِ من مخاطرِ الاستخدام السيّئِ لها، وتوظيفها في ارتكاب الجرائمِ المختلفةِ، على نحوٍ يكفلُ تحقيقَ المصلحةِ العامةِ واحترام الحقّ في حرية التعبيرِ،وتوفيرِ بيئةٍ آمنةٍ للبياناتِ والمعلومات الشخصيةِ.

- عقد المؤتمراتِ والندواتِ المحليَّةِ والدوليَّةِ على نحوٍ متكررٍ؛ لمناقشةِ مخاطرِ المعلوماتيَّةِ أو تقنيةِ المعلوماتِ على حقوقِ الإنسانِ وحرياتهِ، خاصةً الحق في السريةِ،على اعتبارِ أنَّ هذه التقنيةُ في تطوُّرٍ مستمرٍّ وبوتيرةٍ سريعةٍ، مع التأكيدِ على ضرورةِ دعوةِ الخبراءِ الفنيينَ في مجالِ أمنِ المعلوماتِ؛ للاستفادة منْ خبراتهم، ومعرفةِ الطرقِ الحديثةِ والمتطورةِ لانتهاكِ سريةِ البياناتِ والمعلوماتِ الشخصيةِ؛ لإيجادِ أفضلِ السبُلِ لتحقيقِ الأمنِ المعلوماتي.

ثَبْتُ المَرَاجِعِ

أولاً: المراجعُ باللغةِ العربيةِ:

1.إبراهيم حامد طنطاوي،أحكام التجريم والعقاب في قانون تنظيم الاتصالات،دراسة تأصيلية وتحليلية لنصوص القانون رقم 10 لسنة 2003م،دار النهضة العربية،القاهرة،2003م.

2.أمين أعزان،الحماية الجنائية للتجارة الإلكترونية،دراسة مقارنة،كليةالحقوق،جامعة عين شمس،2009م.

3. حسني الجندي،التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة،الكتاب الثالث،قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، مِنْ دُونِ ناشر ومكان نشر، الطبعة الأولى،2009م.

4.حسين بن سعيد الغافري، شرح قانون المعاملات الإلكترونية العماني 2008/69،دار النهضة العربية، القاهرة،2011م.

5.خالد بن عبدالله بن معيض العبيدي،الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، دراسة تحليلية مقارنة، رسالة ماجستير،أكاديمية نايف العربية للعلوم الأمنية،2009م.

6.خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى،2009م.

7.خالد ممدوح إبراهيم، إبرام العقد الإلكتروني،دار الفكر الجامعي،الإسكندرية،2006م.

8. زهيرة كيسي،النظام القانوني لجهات التوثيق(التصديق) الإلكتروني،مجلة دفاتر السياسة والقانون،جامعة ورقلة –الجزائر، العدد السابع،2012م.

9.سليم عبدالله الجبوري،الحماية القانونية لمعلومات شبكة الإنترنت،منشورات الحلبي الحقوقية،بيروت،2009م.

10.صالح شنين،الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة تلمسان،2013-2012.

11.صفات سلامة،النانو تكنولوجي عالم صغير ومستقبل كبير،الدار العربية للعلوم ناشرون،بيروت،2009م.

12.عبد الفتاح بيومي حجازي،نحو صياغة نظرية عامة في علم الجريمة المعلوماتية والمجرم المعلوماتي،دراسة متعمقةفي التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي،انحراف الأحداث بسبب الإنترنت، مكافحة إدمان الإنترنت لدى بعض الفئات، منْ دُونِ ناشر ومكان نشر، الطبعة الأولى،2009م.

13. عبد القادر عطير،سر المهنة المصرفية في التشريع الأردني،دراسة مقارنة ،دار الثقافة للنشر والتوزيع،عمان،الطبعة الأولى،1996م.

14.عبدالله حسين علي محمود،سرقة المعلومات المخزنة في الحاسب الآلي،رسالةدكتوراه،جامعة عين شمس،2001م.

15.عطا عبد العاطي السنباطي،الإثبات في العقود الإلكترونية، دراسة فقهية مقارنة،دار النهضة العربية القاهرة،2008م.

16.علي عبد القادر القهوجي،الحماية الجنائية للبيانات المعالجة إلكترونياً،كتاب بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث ومركز تقنية المعلومات بالجامعة، 1-3 مايو 2000م، الطبعة الثالثة، 2004م

17.علي عبد القادرالقهوجي،الحماية الجنائية لبرامج الحاسب،دار الجامعة الجديدة للنشر، الإسكندرية، 1997م.

18.علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام،دراسة مقارنة،منشورات الحلبي الحقوقية،بيروت،2008م.

19.عمر السعيد رمضان،شرح قانون العقوبات،القسم العام، دارا لنهضة العربية،القاهرة، منْ دُونِ تاريخ نشر.

20.عمر الفاروق الحسيني،المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية،1995م.

21.عمر سالم،الحماية الجنائية لبطاقات الوفاء،دار النهضة العربية، القاهرة،الطبعة الأولى،1995م.

22.غنام محمد غنام،دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت،دار الفكر والقانون، المنصورة،2010م.

23.فايز رضوان،بطاقات الوفاء،المطبعة العربية،القاهرة،الطبعة الأولى،1990م.

24. فياض ملفي القضاة،مسؤولية البنوك الناتجة عن استخدام الكمبيوتر كوسيلة وفاء،كتاب بحوث مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، 1-3 مايو 2000م، جامعة الإمارات العربية المتحدة،كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتجية ومركز تقنية المعلومات بالجامعة، الطبعة الثالثة،2004م

25.فوزية عبد الستار،شرح قانون العقبات،القسم الخاص،الطبعة الثانية،دار النهضة العربية،القاهرة،2000م.

26. محمد أمين الخرشة، نايف عبد الجليل الحمايدة،الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني،دراسة مقارنة، مجلة جامعة الأزهر،سلسلة العلوم الإنسانية 2014م،المجلد 16، العدد1.

27.محمد زكي أبو عامر، د.سليمان عبد المنعم،قانون العقوبات الخاص،منشورات الحلبي الحقوقية،بيروت،2004م.

28.محمد عبد الظاهر حسن،المسؤولية المدنية في مجال الطب وجراحة الأسنان،دار النهضة العربية،القاهرة،2004م.

29.محمد محمود المكاوي،الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، جرائم الكمبيوتر والإنترنت،المكتبة العصرية للنشر والتوزيع، الطبعة الأولى،2010م.

30.مدحت رمضان،الحماية الجنائية للتجارة الإلكترونية،دار النهضة العربية،القاهرة،2000م.

31.منير محمد الجنبيهي، ممدوح محمد الجنبيهي،جرائم الإنترنت والحاسب الآلي وسبل مكافحتها، دار الفكر الجامعي، الإسكندرية،2006م.

32. نائلة عادل محمد فريد قورة،جرائم الحاسب الاقتصادية،دار النهضة العربية،القاهرة،2004م.

33.نبيلة غضبان،المسؤولية الجنائية للطبيب،رسالة ماجستير،كليةالحقوق،جامعة مولود معمري-تيزي وزو،2009م.

34. هدى حامد قشقوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الإلكتروني، كتاب بحوث مؤتمر القانون والكمبيوتر والإنترنت 1-3 مايو 2000م، جامعة الإمارات العربية المتحدة،كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتجية ومركز تقنية المعلومات بالجامعة،الطبعة الثالثة، 2004م.

35.هدى حامد قشقوش،جرائم الحاسب الإلكتروني في التشريع المقارن،دار النهضة العربية،القاهرة،1992م.

36. هشام محمد فريد رستم،قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة بأسيوط،1994م.

37. يونس عرب، موسوعة القانون وتقنية المعلومات،دليل أمن المعلومات والخصوصية، الجزء الثاني،الخصوصية وحماية البيانات في العصر الرقمي،اتحاد المصارف العربية،بيروت،2002م.

ثانياً: المراجعُ باللغةِ الفرنسيةِ:

1.Alain Bensoussan: Internet, aspects juridiques, éd Hermes, 1998.

2. Alexis Baumann: Nouvelles décisions de la CNIL en matière de biométrie, Publié le: http://www.declaration-cnil.com/Articles/A20060130-nouvelles-decisions-cnil-biometrie.php.

3. ALEXIS Baumann: Responsabilité de l'employeur du fait de l'utilisationd'Internet par le salarié, Publié le: http://www.declaration-cnil.com/Articles/A20060407-responsabilite-de-l-employeur-et-informatique.php.

4. Alexis Baumann: Commentaire du décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé, Publié le : http://www.declaration-cnil.com/Articles/A20060110-decret-sur-l-hebergement-de-donnees-de-sante.php.

5. Alexis Baumann: La protection des fichiersinformatiques "personnels" du salarié, Publié le: http://www.declaration-cnil.com/Articles/A20051107-fichiers-informatiques-personnels-du-salarie.php.

6. Alexis Ngounou: Logicielslibres et administration électronique,Thèse de doctorat,UniversitéLille 2,2010.

7.AndréJacquesAugand :Respect de la vie privée en matière de nouvelles technologies à travers des études de cas, UniversitéPanthéon-Assas (Paris2) , thèse de doctorat,2015.

8.Etienne Wery :Le nouvel article 323-3-1 du Code pénal : luttercontre les virus, d'accord, mais attention aux effetspervers, Publié le 02/09/2004 ,sur : https://www.droit-technologie.org/actualites/le-nouvel-article-323-3-1-du-code-penal-lutter-contre-les-virus-daccord-mais-attention-aux-effets-perver0073.

9.Carole Girard-Oppici : Les donnéespersonnelles et la protection de la vie privée à l'heure des nouvelles technologies, sur : http://www.net-iris.fr/veille-juridique/dossier/20679/les-donnees-personnelles-et-la-protection-de-la-vie-privee-a-heure-des-nouvelles-technologies2015.

10.CélestinFoumdjem,Blanchiment de capitaux et la fraudefiscale, Thèse de doctorat,Université de Cergy-Pontoise, 2010.

11. Hélène Lebon: Les prochainesrecommandations de la CNIL en matière de géolocalisation, Publié le: http://www.declaration-cnil.com/Articles/A20051020-geolocalisation-recommandations-cnil.php.

12.Hélène Lebon: Méthodologie de référence de la CNIL pour les recherchesbiomédicales, Publié le: http://www.declaration-cnil.com/Articles/A20060405-recherches-biomedicales.php.

13.Jean Pradel et Michel danti -Juan : Manuel de droitPénalspécial, éditionsCujas, Paris,2007.

14.Jean-Philippe Foegle: La CJUE, magicienneeuropéenne du « droit à l'oubli » numérique, Protection des donnéespersonnelles (Union européenne), La Revue des droits de l'homme, [En ligne], ActualitésDroits-Libertés, mis en ligne le 16 juin 2014.

15.Jean-Philippe Foegle: Le Conseild'Etat, héraut de la révolutionnumérique ?, Protection des donnéespersonnelles (Conseild'Etat), La Revue des droits de l'homme [En ligne], ActualitésDroits-Libertés, mis en ligne le 30 décembre 2014.

16.Laetitia Valy,Au coeur des préoccupations, la luttecontre le terrorismeconnait un nouveau tournant avec cetteloi du 3 juin 2016 visant à mettre en oeuvre de nouvelles dispositions pour renforcer la prévention et la repression, www.net-iris.fr/veille-juridique/actualite/35232/lutte-contre-le-terrorisme-les-3-nouveautes-a-ne-pas-manquer.

17.Marie-Laure Laffaire: Protection des données à caractère personnel, Éditionsd'Organisation, 2005.

18. Marine Farshian: Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne, Droit a la vie privée et protection des donnéespersonnelles (Assemblée Parlementaire du Conseil de l'Europe), La Revue des droits de l'homme [En ligne], ActualitésDroits-Libertés, mis en ligne le 28 mai 2015.

19.MmeDjazira MEHDI, LES INSTRUMENTS DE LUTTE CONTRE LE BLANCHIMENT D'ARGENT EN ALGERIE,Thèse de doctorat, UNIVERSITE NICE SOPHIA ANTIPOLIS,2015.

20.Murielle Cahen:Loi : Intrusion dans un systèmeinformatique (hacking), publié le 01/05/2009 ,sur : https://www.legavox.fr/blog/murielle-cahen/intrusion-dans-systeme-informatique-hacking-314.htm

21.Monika Zwolinska: Sécurité et libertésfondamentales des communications électroniques en droit français, européen et international,Thése de doctrat,Université de Nice,2015.

22.Stéphane Tijardovic: La protection juridique des données personnelle ,Vers une nécessaire adaptation de la norme juridique aux évolutions du monde numérique, Publié le :https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-185.htm.