السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

دراسة تحليلية مقارنة

دكتور

ياسر محمد اللمعي

استاذ القانون الجنائي المساعد

كلية الحقوق جامعة طنطا

ملخص البحث باللغة العربية:

في واقع الأمر أن موضوع السياسية الجنائية المعاصرة في حماية الحق في خصوصية البيانات الشخصية الإلكترونية من الموضوعات التي تثير الكثير من التساؤلات القانونية، خاصة في ظل الانتقال من عصر تكنولوجيا المعلومات (IT) إلى عصر تكنولوجيا البيانات (DT). وتطور أساليب ارتكاب الجرائم من جرائم تقليدية يرتكبها مجرم تقليدي، إلى عصر الجريمة المعلوماتية يرتكبها المجرم المعلوماتي ثم إلى عصر جريمة البيانات والذي يرتكبها مجرم البيانات. حيث أن المعالجة الإلكترونية للبيانات الشخصية أصبحت تشكل مرحلة هامة وخطيرة باعتبارها تأسس لعصر جديد من ثورة المعرفة والتكنولوجيا، عالم السحابة الإلكترونية والتي يتم تخزين البيانات من خلالها. في عالم مختلف مثل ذلك يحتاج إلى سياسة جنائية حديثة من أجل توفير الحماية الجنائية اللازمة للحق في الخصوصية بطريقة تلائم مع هذا التطور من حيث الجمع والنقل والتخزين والنشر والاطلاع والمعالجة لهذه البيانات الشخصية الإلكترونية. فالالتزام بالحفاظ على خصوصية البيانات الشخصية الإلكترونية الخاصة بالأفراد أصبح حق لا مناص منه له على مقدمو الخدمة، والأفراد، وكذلك الالتزام من قبل الشركات والمؤسسات بسياسة الخصوصية أصبح أمراً واجباً تفرضه جميع القوانين.

الكلمات المفتاحية:

البيانات الشخصية الإلكترونية – الحق في الخصوصية – صور الحماية الجنائية لخصوصية البيانات الشخصية الإلكترونية – السياسة الجنائية المعاصرة – خصوصية البيانات الشخصية للأطفال– الإعلانات التسويقية الإلكترونية– جرائم خصوصية البيانات الشخصية الإلكترونية.

الملخص باللغة الإنجليزية:

In fact, the issue of the right to privacy of electronic personal data is one of the topics that raise many legal questions, especially in light of the transition from the era of information technology (IT) to the era of data technology (DT). And the development of methods of committing crimes from traditional crimes committed by a traditional criminal, to the era of information crime committed by the information criminal, and then to the era of data crime committed by the data criminal. As the electronic processing of personal data has become an important and dangerous stage as establishing a new era of knowledge and technology revolution, the world of electronic cloud, through which data is stored. In a different world like that, it needs a modern criminal policy in order to provide criminal protection for the right to privacy in a way that suits this development in terms of collection, transfer, storage, publication, access and processing of this electronic personal data. The obligation to maintain the privacy of personal electronic data of individuals has become an inescapable right of service providers, as well as the commitment of companies and institutions to the privacy policy has become a duty imposed by all laws.

المقدمة:

مما لا شك فيه أنه ومع بدء ظهور طفرة انتشار الإنترنت واستخدام الهواتف الذكية وشبكات التواصل الاجتماعي مثل الفيس بوك والتوتير والإنستجرام وغيرها من وسائل التواصل الاجتماعي الأخرى، وما نجم عنها من ازدياد التعاملات الإلكترونية المتنوعة والمتعددة التي تقوم على تداول البيانات والمعلومات الشخصية، أدى ذلك إلى وجود انتهاكات للحق في خصوصية البيانات الشخصية خاصة التي تم معالجتها إلكترونياً، مما يستدعي وجود تشريع خاص يحمي هذه التعاملات والبيانات للمستخدمين حتى لا تستخدم لأي أغراض غير شرعية. حيث أن النمو الهائل في المجتمع، وكمية البيانات الشخصية التي يتم معالجتها سنويا في جميع قطاعات التجارة والصناعة يتطلب الاستثمار في نظم معالجة متقدمة للبيانات في جميع الدول بما يحمي في نفس الوقت حقوق الانسان وخاصة الحق في خصوصية البيانات الشخصية التي يتم معالجتها بطريقة إلكترونية.

١. أهداف البحث:

ومن الجدير بالذكر أن الهدف العام من وضع تشريع خاص بحماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً هو تحديد الأطر التنظيمية لاستخدام البيانات الشخصية للمستخدمين والمواطنين وحماية هذه البيانات حتى لا تستخدم لغير الأغراض التي يجب أن تستخدم لها. فهناك معلومات عامة لا تتعلق بالأفراد – لا إشكاليه من تداولها في معظم الأوقات بما لا يتعارض مع الحق في الحصول على المعلومات والبيانات، أو معلومات ضرورية لضمان سلامة الدولة أو منظومة الأمن والدفاع الوطني. وعلى صعيد آخر؛ فهناك معلومات وبيانات شخصية يجب أن تخضع لقواعد الحماية، ولإذن صاحبها في حالة جمعها أو معالجتها أو الافصاح عنها، أو أي طريقة من طرق المعالجة الإلكترونية لها. حيث يسرت وسرعت الوسائل الإلكترونية ،

وخصوصاً شبكة الإنترنت ذات السرعة العالية تداول تلك المعلومات والبيانات، كما أصبح هناك نشاطات اقتصادية وطيدة الصلة بالاتصالات وتكنولوجيا المعلومات، تعتمد على معالجة وتداول المعلومات والبيانات ، مثل نشاطات معالجة البيانات واستضافتها والنشاطات الأخرى ذات العلاقة بها وكذلك نشاطات مراكز الاتصال.

٢. أهمية البحث:

فقد انشأت شركات دولية خاصة نظراً لأهمية هذا الموضوع، لكي تتخذ كافة التدابير الأمنية التقنية والتنظيمية اللازمة لحماية خصوصية البيانات الشخصية من مخاطر التخلص بطريق الخطأ أو غير قانوني ، أو فقدانها عن طريق الخطأ ، أو التغيير ، أو الكشف عنها أو الوصول غير المصرح به ، وغيرها من جميع الأشكال الأخرى غير مشروعة في التعامل مع البيانات الشخصية. وهي في ذلك تلتزم بتطبيق المعايير والمتطلبات الدولية القانونية والمعايير الأوروبية رقم EC/٤٦/٩٥، وكذلك النسخة الموحدة الاوربية الخاصة بقانون حماية البيانات والملفات والحريات وفقا لتعديلات اللائحة العامة الاوربية لحماية البيانات الشخصية رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨. وكذلك القانون الفرنسي الخاص بحماية البيانات الشخصية الصادر في ٦ يناير ١٩٧٨، الذي تم ادخال العديد من التعديلات عليه ومنها التعديل بالقانون رقم ٨٠١ لسنة ٢٠٠٤، والتعديل بالقانون رقم ١٣٢١ لسنة ٢٠١٦ الصادر في ٧ أكتوبر ٢٠١٦، والقانون رقم ٥٥ الصادر في ٢٠ يناير ٢٠١٧، والقانون رقم ٤٩٣ الصادر في ٢٠ يونيه ٢٠١٨. بالإضافة إلى قيام بعد الدول العربية بإصدار قانون لحماية خصوصية البيانات الشخصية مثل دولة قطر وتونس والمغرب والجزائر. بالإضافة إلى ذلك فقد أصدر المشرع المصري في ١٤ أغسطس ٢٠١٨

قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨. ثم أصدر المشرع المصري في ١٥ يوليه ٢٠٢٠ قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠([1]).

٣. إشكاليات البحث:

مما لا شك فيه أن هذا الموضوع يثير مجموعة من التساؤلات القانونية حول موضوع الحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها بطريقة إلكترونية وذلك على النحو التالي:

أ. أن قواعد البيانات الشخصية التي تم معالجتها إلكترونياً هي في الوقت الحاضر غير محمية بشكل كاف في جميع الدول مما يشكل خللاً في التشريعات القائمة ويوجب العمل على معالجته. بالإضافة إلى ذلك يجب أن تمتد الحماية إلى المرحلة السابقة وليست فقط المعاصرة للمعالجة الإلكترونية للبيانات الشخصية والتي يتم فيها الحصول عليها أو جمعها أو استخراجها أو تصنيفها أو على أي نحو آخر تمهيداً لمعالجتها إلكترونياً، أو تتم معالجتها عن طريق الجمع بين المعالجة الإلكترونية والمعالجة التقليدية، وكذلك تمتد الحماية القانونية للمرحلة اللاحقة للمعالجة الإلكترونية للبيانات الشخصية.

وبالتالي يثور التساؤل هنا حول مدى كفاية ونفاذ التشريعات الوطنية في مجال حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً أو آلياً، وما هي الضمانات القانونية والإجرائية الوجب اتخاذها في مثل هذه الحالات؟ ثم أفعالا جديدة ترتبط باستعمال الأجهزة الإلكترونية لا تكفي النصوص القائمة لمكافحتها فالاعتداء على حرمة الحياة الخاصة لا يعاقب عليه قانون العقوبات وفقا للمفهوم التقليدي إلا إذا كان مرتبطاً

([1]) – قانون حماية البيانات الشخصية المصرية رقم ١٥١ لسنة ٢٠٢٠، والمنشور في الجريدة الرسمية العدد ٢٨ مكر (هـ) في ١٥ يوليه ٢٠٢٠.

بمكان خاص تم انتهاك خصوصيته. أما مجرد تجميع البيانات عن الاشخاص وتسجلها ونقلها ومعالجتها إلكترونيا فإنها لا تخضع للتجريم وفقا للمفهوم التقليدي لقانون العقوبات، كذلك فأن الدخول غير المشروع والالتقاط وتغيير هذه البيانات الشخصية التي تم معالجتها إلكترونياً يجب النص على تجريمه لمواجهة القصور التشريعي الناجم عن عدم وجود نص قانوني وذلك تطبيقا لمبدأ الشرعية الجنائية.

ب. أغلب التشريعات سواء كانت عربية أو غربية قد أولت الطفل حماية خاصة، وهنا يثور التساؤل حول هل تحمي هذه التشريعات خصوصية البيانات الشخصية للأطفال التي تم معالجتها إلكترونياً؟ خاصة في ظل ما تمثله التكنولوجيا والانترنت من خطورة على حق الأطفال في خصوصية بياناتهم الشخصية وبما لا يخل بحقهم في استخدام وسائل التواصل الاجتماعي.

ج. كذلك فإن اختلاف وتعدد القوانين داخل الدولة في مجال حماية خصوصية البيانات الشخصية لها آثار سلبية مباشرة على سير العمل في الاسواق الداخلية فيما يتعلق بقواعد البيانات وبصفة خاصة على حرية الأشخاص الطبيعية والاعتبارية لتوفير قاعدة بيانات السلع والخدمات عبر الإنترنت تحت نظام قانوني موحد في جميع أنحاء المجتمع. حيث أن قواعد البيانات هي أداة حيوية في تطوير سوق المعلومات والبيانات داخل المجتمع. مما أسهم في انتشار حالات التدخل التعسفي أو غير المشروع لخصوصية البيانات الشخصية دون أن ينال مرتكبي هذه الافعال الإجرامية العقاب وبالتالي تنامي ظاهرة الإفلات من العقاب.

ت. بالإضافة إلى ما سبق يثور التساؤل حول مدى الحاجة إلى اتخاذ تدابير احترازية لحماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياُ؟ وذلك لمنع استخراج أو إعادة الاستفادة من محتويات قاعدة البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً.

ث. وفي النهاية نسعى لتحديد المسئولية الجنائية لكل من مقدمي الخدمة والمراقب والمعالج والمضيف للبيانات الشخصية عن البيانات الشخصية المخزنة والتي تم معالجتها إلكترونياً.

٤. نوع الدراسة:

سوف نتناول دراسة هذا الموضوع وفقا للدراسة التحليلية المقارنة بين النظام اللاتيني والنموذج له القانون الفرنسي، والنظام الأنجلوسكسوني والنموذج له القانون الانجليزي والقانون الأمريكي، والمقارنة مع القوانين العربية مثل القانون المصري والمغربي والتونسي والقطري من أجل التواصل لابد السياسات التشريعية لحماية خصوصية البيانات الشخصية المعالجة إلكترونياً.

٥. خطة البحث:

سوف تنقسم الدراسة للحماية الجنائية لخصوصية البيانات الشخصية المعالجة إلكترونياً إلى فصلين في الفصل الاول نتناول تحديد محل الحماية الجنائية وهي خصوصية البيانات الشخصية المعالجة إلكترونياً، ثم نستعرض بعد ذلك صور الحماية الجنائية لخصوصية البيانات الشخصية المعالجة إلكترونياً، وذلك على النحو التالي:

الفصل الاول: محل الحماية الجنائية لخصوصية البيانات الشخصية الإلكترونية.

الفصل الثاني: صور الحماية الجنائية لخصوصية البيانات الشخصية الإلكترونية.

الفصل الأول. محل الحماية الجنائية لخصوصية البيانات الشخصية الإلكترونية

سوف نتناول في هذا الفصل توضيح ماهية البيانات الشخصية باعتبارها محل للحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً وذلك على النحو التالي: في المبحث الاول نبين ماهية خصوصية البيانات الشخصية التي تم معالجتها إلكترونيا وأنواعها، ثم بعد ذلك نستعرض الجهود الدولية والوطنية في مجال الحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً في المبحث الثاني.

المبحث الأول. ماهية البيانات الشخصية الإلكترونية وأنواعها

بادئ ذي بدء نستعرض الحق في الخصوصية الرقمية من حيث التطور التاريخي لحماية الحق في الخصوصية وتعريف الحق في الخصوصية ثم نوضح بعد ذلك تعريف ماهية البيانات الشخصية التي تم معالجتها إلكترونياً ثم نحدد ما المقصود بخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، وفي النهاية نتناول أنواع البيانات الشخصية محل الحماية الجنائية.

المطلب الاول. الحق في الخصوصية الرقمية

سوف نتناول في الفرع الأول التطور التاريخي لحماية الحق في الخصوصية وخاصة المتعلقة بالخصوصية الرقمية، ثم نستعرض في الفرع الثاني موقف الفقه من تعريف الحق في الخصوصية.

الفرع الاول. التطور التاريخي لحماية الحق في الخصوصية الرقمية

في البداية نوضح مفهوم الخصوصية من وجهة النظر اللغوية حيث يقصد بها أنها تقترب من مفهوم السر، لكنها ليست مرادفة له، ذلك لأن السرية تفترض الكتمان والتخفي ، في حين أن الخصوصية وإن كانت تفترض قدراً من الكتمان والتخفي لكنها قد تتوافر رغم انعدام السرية(١). أما إذا اضيف لفظ حق إلى الخصوصية فيقصد بذلك من الناحية اللغوية بانه حق الشخص في أن ينفرد بأمور لنفسه ، أو خاصته ، على ألا تتخذ هذه الأشياء صفة العموم(٢). أي بأنه كل ما يخص الشخص بشيء دون غيره وبالتالي يقال بأن هذا الشيء خصوصية له دون غيره.وبناء على ما سبق نستطيع القول بأن الخصوصية هي حق الفرد في حماية بعض مظاهر حياته الخاصة والمحافظة على سريتها بما يصون سمعته ومعطيات حياته التي يحرص على عدم التدخل فيها. وتتميز

---

(١) – المصباح المنير لأحمد بن محمد بن علي الفيومي المقري ، مادة خصص ، طبعة دار الحديث ، القاهرة ، ص ١٠٥. مختار الصحاح لمحمد بن أبي بكر بن عبد القادر الرازي ، طبعة دار الحديث ، القاهرة ، ص ١٠٦. المعجم الوجيز ، مجمع اللغة العربية ، طبعة وزارة التربية التعليم جمهورية مصر العربية ، ١٩٩٣، ص ١٩٩.

(٢) – أ. عبد اللطيف هميم محمد ، جرائم الاعتداء على الحياة الخاصة وعقوبتها في الشريعة والقانون ، رسالة ماجستير ، كلية الشريعة والقانون ، جامعة الأزهر ، القاهرة ، ١٩٨١ ، ص ١٠٧.

الخصوصية بأنها فكرة مرنه تختلف من مجتمع إلى آخر تبعاً لاختلف القيم والعادات والمستوى الثقافي لدى المجتمع.

فمن الجدير بالذكر أن التقدم التكنولوجي واستخدام الإنترنت وابتكار أدوات لجمع ونقل ونشر ومعالجة مختلف البيانات الشخصية، نتج عنه امكانية الوصول إلى معلومات وبيانات شخصية كان معها يستحيل أو غير الممكن الوصول إليها في الماضي. بالإضافة إلى ذلك فقد أصبح من الممكن جمع البيانات الشخصية وتحديد أماكن تواجد الأشخاص من خلال IP وهو عنوان بروتوكول الإنترنت لكل جهاز كمبيوتر أو محمول أو أيباد أو أي جهاز آخر متصل بشبكة الإنترنت، وهو ما يعني أنه يمكن تتبع هذه الأجهزة، وبالتالي القدرة على تحديد موقع أي جهاز من الأجهزة الإلكترونية ومعرفة مكان تواجد الشخص مما يمثل معه تحدياً كبيراً وجديداً بشأن خصوصية هذه البيانات والمعلومات الشخصية التي يتم معالجتها إلكترونياً.

كذلك ترتب على توافر الإنترنت بالسرعات الكبيرة والإمكانيات العالية إلى قيام الحكومات والشركات الخاصة بتحليل المعلومات والبيانات الشخصية، وبالإضافة إلى تخزين كميات هائلة من هذه البيانات الشخصية في السحابات الإلكترونية. حيث يسمح التقدم التكنولوجي الربط بين قواعد بيانات المعلومات مع بعضها البعض، الأمر الذي يتيح المزيد والمزيد من كميات البيانات التي تم معالجتها إلكترونيا. مما يهيئ الفرصة للاستغلال التجاري لتلك البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً([1]) ، حيث إن الكثير من الخدمات التي تقدمها هذه الشركات هي خدمات مجانية تعتمد

([1]) – توبي مندل ، وأندرو بوديفات ، وبن واجنر ، وديكسي هوتن ، ونتاليا توريس ، دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير ، منشورات اليونسكو ، منظمة الأمم المتحدة للتربية والعلوم والثقافة ، باريس ، ٢٠١٢ ، ص ٧.

نماذج أعمالها على جمع معلومات وبيانات المستخدم واستخدامها في أغراض التسويق مثل شركة جوجل أو فيسبوك أو توتير .... الخ.

ويرجع الفضل في استخدام مصطلح الخصوصية إلى المشرع الإنجليزي في القرن الخامس عشر ليدل بها على الحالة أو الوضع التي يكون عليها الفرد ، فهي تعتبر حالة انسحاب من المجتمع بحيث يتوارى فيه الشخص عن باقي أفراد المجتمع ويناي بنفسه عن الاهتمام من قبلهم(١). ولكن سبق ذلك محاولات لحماية الحق في الخصوصية ، مثال على ذلك التشريعات الخاصة بحماية الخصوصية في قانون قضاة الصلح لسنة ١٣٦١ ، والذي نص على اعتقال مختلس النظر على عورات الغير وكذلك المتنصت(٢). ثم جاءت بعد ذلك قضية إينتيك ضد كارينجتون عام ١٧٦٥ لتكون السبب الرئيس في التعديل الرابع في الدستور الأمريكي من منطلق الرغبة في حماية الحق في خصوصية الأوراق المملوكة في أي منزل خاص(٣). وفي القرن العشرين، عرفت المعايير الدولية الحق في الخصوصية على أساس أنه حق من حقوق الإنسان، فنص الإعلان العالمي لحقوق الإنسان الصادر ١٩٤٨ في المادة ١٢ منه على "حماية الحق في الخصوصية على أنه لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"(٤).

---

(١) – JOHN H.F. SHATTUCK, Right of privacy, Press view, ١٩٦٦, P. ٢., *see also*, Richard A. POSNER, The right of privacy, ١٢ Georgia law Review, ١٩٧٧, P. ٣٩٣.

(٢) – انظر: د. بيريسفورد إيه وستاجانو إف ، خصوصية الموقع في الحوسبة المنتشرة ، جمعية الاتصالات التابعة لمعهد مهندسي الكهرباء والإلكترونيات IEEE ، ٢٠٠٣.

(٣) – المنظمة الدولية لحماية الخصوصية ، الخصوصية وحقوق الإنسان ، دراسة استقصائية دولية لقوانين وتطويرات الخصوصية ، ٢٠٠٦.

(٤) – الأمم المتحدة ، المادة ١٢ من الإعلان العالمي لحوق الإنسان ، الصادر في ١٩٤٨.

بالإضافة إلى ذلك فقد نصت المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية بكفل حق الانسان في الخصوصية وذلك على النحو التالي([1]):

١- لا يجوز التدخل بشكل تعسفي أو غير قانوني بخصوصيات أحد أو بعائلته أو مراسلاته كما لا يجوز التدخل بشكل غير قانوني لخصوصية شرفة وسمعته.

٢- لكل شخص الحق في حماية القانون ضد مثل هذا التدخل أو التعرض.

وانطلاقا مما سبق نستطيع القول أن المشرع الدولي يحيل في حماية الحق في الخصوصية إلى التشريعات الوطنية، فلا يصح وقوع أي تدخل إلا في الحالات المنصوص عليها في القانون وبشكل معقول وبدون أن يشكل أي صورة من صور التعسف في استخدام الحق في الخصوصية.

بالإضافة إلى ما سبق فقد أرست المبادئ الأساسية لإعلان الأمم المتحدة الخاص باستخدام التقدم العلمي والتكنولوجي لمصلحة السلم وخير البشرية، بضرورة اتخاذ الدول التدابير التشريعية اللازمة لمنع استخدام التطورات العلمية والتكنولوجية من جانب الهيئات التابعة للدول بصورة تتنافي مع ما أكده الإعلان العالمي لحقوق الإنسان والعهود والصكوك الدولية الخاصة بحقوق الإنسان ذات الصلة بحماية الحق في الخصوصية ليصبح بذلك التزاما قانونياً يوضع موضوع التنفيذ بحكم القانون([2]) ، كما أوضح هذا

([1]) – العهد الدولي للحقوق المدنية والسياسية ، أصدرته الجمعية العامة للأمم المتحدة بالقرار رقم ٢٢٠٠ في ١٦ ديسمبر ١٩٦٦. ، د. محمد سعيد الدقاق ، التشريع الدولي في مجال حقوق الانسان ، المجلد الثاني ، دراسات حول الوثائق العالمية والإقليمية ، إعداد د. محمد شريف بسيوني ولآخرون ، دار العلم للملايين ، بيروت ، ١٩٨٩ ، ص ٧٨.

([2]) – اعلان الأمم المتحدة بشأن استخدام التقدم العلمي والتكنولوجي لمصلحة السلو خير البشرية ، الصادر في ١٠ نوفمبر سنة ١٩٧٥ ، وذلك دعماً لحماية التشريعات الوطنية لحقوق الانسان على

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

الإعلان الصورة من مخاوف إساءة استخدام أو استعمال التطورات العلمية والتكنولوجيا وما ينتج عنها من آثار تمس حقوق الانسان ، وتشكل انتهاك له وخاصة الحق في الخصوصية.

وتأسيسا على ذلك فقد اعتمدت الجمعية العامة للأمم المتحدة قرار في ٢٠ ديسمبر ٢٠١٣ خاص بحماية الحق في الخصوصية في العصر الرقمي باعتباره حق من الحقوق الانسان(١)، ومشددة للمرة الأولى، على أن نفس الحقوق التي يتمتع بها الناس يتعين حمايتها أيضا على الإنترنت، وبالتالي يجب على الدول احترام وحماية الحق في خصوصية البيانات الرقمية، وكذلك المحافظة عليها ، وإنشاء نظام فعال ومستقل محلي، قادر على ضمان الشفافية ، حسب الاقتضاء ، ومساءلة عمليات المراقبة واعتراض الاتصالات وجمع البيانات الشخصية. وأن الحق في الخصوصية، والحق في الوصول إلى المعلومات وحرية التعبير يرتبطون ارتباطا وثيقا. والجمهور لديه الحق الديمقراطي في المشاركة في الشئون العامة وهذا الحق لا يمكن أن يمارس على نحو فعال من خلال الاعتماد فقط على المعلومات المصرح بها(٢). وفي نفس الوقت فان المخاوف بشأن الأمن القومي والنشاط الإجرامي قد تبرر استخدام ضيق لبرامج استثنائية ومصممة

مستوى العلاقات الدولية. د. حسن محمد ربيع ، حماية حقوق الأنسان والوسائل المستحدثة للتحقيق الجنائي ، رسالة دكتوراه ، كلية الحقوق جامعة الإسكندرية ، ١٩٨٥ ، ص ٢٨.

(١) – قرار الامم المتحدة ، حول الحق في الخصوصية في العصر الرقمي ، اللجنة الثالثة ، ١٨ ديسمبر ٢٠١٣ ، رقم A/RES/٦٨/١٦٧ ، البند ٦٩(ب).

(٢) – مثال على ذلك حالة المواطن الأمريكي إدوارد سنودن ، توضيح الحاجة الملحة لحماية الأفراد الذين يكشفون عن انتهاكات حقوق الإنسان. حيث أن الحق في الخصوصية، والحق في الوصول إلى المعلومات وحرية التعبير يرتبطون ارتباطا وثيقا. والجمهور لديه الحق الديمقراطي في المشاركة في الشئون العامة وهذا الحق لا يمكن أن يمارس على نحو فعال من خلال الاعتماد فقط على المعلومات المصرح بها. ويشار إلى أن السيد سنودن ، وهو موظف متعاقد في وكالة الأمن القومي في الولايات المتحدة الامريكية ، متهم بتسريب تفاصيل عدة برامج مراقبة الكترونية سرية للصحافة. وكان قد فر من البلاد بعد نشر الأخبار، إلى دولة روسيا.

خصيصا للمراقبة، إلا أن المراقبة دون وجود ضمانات كافية لحماية الحق في الخصوصية تحمل خطر التأثير السلبي على التمتع بحقوق الإنسان والحريات الأساسية.

وبالإضافة إلى ما سبق فقد نص المشرع الاوربي في الاتفاقية الأوربية لحقوق الانسان والحريات الأساسية على أهمية حماية حقوق الأنسان خاصة في ظل بروز دور المعلومات وما تمثله من خطر داهم على خصوصية الانسان، حيث تنص المادة الثامنة على ما يلي:

١- "إن لكل شخص الحق في احترام حياته الخاصة وحياته العائلية ومسكنه ومراسلاته.

٢- لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقاً للقانون وبما تمليه الضرورة في مجتمع ديمقراطي ولصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للبلاد لمنع الاضطراب أو الجريمة أو حماية الصحة أو الآداب أو حماية حقوق الآخرين وحرياتهم".

ويتبين من هذا النص أن المشرع الأوربي قد وضع صراحة حماية قانونية للحق في الخصوصية بشكل عام ، ولكن هذه الحماية المقررة لهذا الحق جاءت مقيدة بمشروعية تدخل السلطات العامة([1])، إذا كان ذلك لازماً في أوقات معينة ، وفقا لما ينص عليه القانون ، وبما تلية حالة الضرورة في المجتمع ولصالح حماية الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للبلاد لمنع الاضطراب أو الجريمة أو حماية الصحة أو الآداب أو حماية حقوق الآخرين وحرياتهم.

([1]) – د. عبد العزيز محمد سرحان ، الاتفاقية الأوربية لحماية الحقوق الأنسان والحريات الأساسية ، دار النهضة العربية ، القاهرة ، ١٩٦٦ ، ص ٣٢٤.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

أما بالنسبة لموقف المشرع الفرنسي فقد نص على حماية خصوصية البيانات الشخصية بالقانون الصادر في ١٩٧٨ رقم ١٧ لسنة ١٩٧٨ الخاصة بالبيانات والحريات المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤ الصادر في ٧ أغسطس ٢٠٠٤ الخاصة بحماية البيانات الشخصية والمعدل بالقانون رقم ٤٩٣ الصادر في ٢٠ يونية ٢٠١٨. وكذلك عزز المشرع الانجليزي ذلك الاتجاه بالتشريعات القانونية التي تحمي البيانات الشخصية ومنها قانون حماية البيانات الشخصية الصادر في عام ١٩٨٤ والذي تم تعديله في عام ١٩٩٨. أما بالنسبة للمشرع الأمريكي فقد نص المشرع على حماية الحق في خصوصية البيانات الشخصية من خلال تشريع خاص، وعلى سبيل المثال لذلك قانون الولوج المصطنع في الحاسب الآلي الصادر في أكتوبر سنة ١٩٨٤ والذي تم أدخال التعديلات عليه في القانون الصادر في عام ١٩٩٦. ويضاف إلى ذلك بعض الدول العربية التي أصدرت قوانين لحماية خصوصية البيانات الشخصية مثل تونس والمغرب والجزائر وقطر ومصر.

الفرع الثاني. موقف الفقه في تعريف الحق في الخصوصية

لقد اختلاف الفقه في تحديد مفهوم موحد يتسم بالدقة والوضوح للحق في الخصوصية أو الحق في الحياة الخاصة، ويرجع ذلك الاختلاف إلى اتساع الحق في الحياة الخاصة بحيث يصعب وضع تعريف جامع مانع له، الامر الذي دفع بعض الفقه إلى القول بأن الحق في الحياة الخاصة هو حق نسبي أكثر منه حق مطلق. وترتب على ذلك أن الفقه قد انقسم إلى العديد من الاتجاهات في تعريف الحق في الخصوصية على النحو التالي:

الاتجاه الأول. هو الاتجاه الواسع في تعريف الحق في الخصوصية(١) حيث ذهب هذا الاتجاه إلى تعريف الحق في الخصوصية بأنه أحد الحقوق اللصيقة بالشخصية والتي تثبت للإنسان بمجرد كونه إنساناً. كما يقر هذا الاتجاه بأنه من الصعوبة بمكان عمل حصر للجوانب المتعددة لهذا الحق أو مفرداته وذلك لصعوبة إقامة حدود فاصلة وبصورة تامة بين الحياة الخاصة والحياة العامة.

ومن أهم التعريفات للحق في الخصوصية وفقاً لمعناها الواسع تعريف معهد القانون الأمريكي ، حيث يعرف الحق في الخصوصية "بأنه كل شخص ينتهك بصورة جدية ، وبدون وجه حق ، حق شخص آخر في ألا تصل أموره وأحواله إلى علم الغير ، وألا

(١) – د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة بأسيوط ، ٢٠٠٦ ، ص ١٧٥.

تكون صورته عرضه لأنظار الجمهور ، يعتبر مسئولاً أمام المعتدي عليه"(١). كما يعرفها الفقيه الأمريكي جون شاتوك بقوله هي أن "يعيش المرء كما يحلو له أن يعيش، مستمتعاً بممارسة أنشطة خاصة معينة حتى ولو كان سلوكه على مرأي من الناس ، فالإنسان حر في ارتداء ما يراه مناسباً ، وحر في أن يظهر بهيئة تتميز بها شخصية"(٢). ويعبر هذا الرأي عن النهج الأمريكي للحرية.

ومن الجدير بالملاحظة أنه الفقيه Martin قد سار على نفس النهج السابق فقد عرف الحق في الخصوصية بأنه الحق في الحياة الأسرية والشخصية والداخلية والروحية للشخص عندما يعيش وراء بابه المغلق. وهو ما دفع الفقيه C . Dennis إلى القول بأن الخصوصية ما هي إلا وصف أو حالة للعزلة أو النأي عن الملاحظة. وبالتالي لا يخرج مفهوم الحق في الخصوصية في أنه مجرد أن يكون للشخص الحق في تركه وحاله أي الاختلاء بنفسه. وكذلك ذهب الفقيه Niza إلى القول بأن "الحق في الخصوصية هو حق الفرد في حياة منعزلة مجهولة ، فالشخص من حقه أن يعيش بعيداً عن أنظار الناس وعن القيود الاجتماعية ، بمعنى أن من حق الشخص ألا يكون اجتماعيا"(٣) أي إلا يكون محل لاطلاع الجميع على حياته.

أما بالنسبة للفقيه Nersom فقد عرف الحق بالخصوصية بأنه "حق الشخص بأن يحتفظ بأسرار من المتعذر على العامة معرفتها إلا بإرادته والتي تتعلق بصفة أساسية

---

(١) – د. مروك نصر الدين ، الحق في الخصوصية ، موسوعة الفكر القانوني ، الجزائر ، بدون تاريخ نشر ، ص ٦١.

(٢) – John H.F. SHATTUCK, Right of privacy, National textbook company, U.S.A, ١٩٧٧, P. ١٩٧.

(٣) – د. أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دارسة مقارنة ، دار النهضة العربية ، القاهرة ، ١٩٨٨ ، ص ١٥.

بحقوقه الشخصية ويقرر أن الحق في الحياة الخاصة يقع في دائرة الحقوق الشخصية وإن كان لا يشملها كلها" (١).

أما الاتجاه الثاني. فهو الاتجاه الضيق في تعريف الحق في الخصوصية حيث ذهب هذا الاتجاه إلى تعريف الحق في الخصوصية وخاصة الفقيه Malherbe بأن "الحياة الخاصة والحقوق الشخصية متطابقتان لأنهما يتضمنا حق الفرد في حماية اسمه وشرفه واعتباره ومراسلاته واتصالاته وحياته المهنية والعائلية وكل ما له تأثير على حياته الشخصية"(٢). فالحياة الخاصة هي قلب للحرية في الدول المتقدمة وضرورة للفرد لحصانة مسكنه ومراسلاته واتصالاته وشرفه. ويذهب هذا الاتجاه إلى وضع إطاراً عاما للحق في الخصوصية وهو يتمثل في العنصرين التاليين:

١- العنصر الأول. الغاية: ويتمثل في النأي بحياة الفرد البعيدة عن النشاط العام عن التقصي والإفشاء الذي يتم بصورة تدخل في الشئون الخاصة للآخرين.

٢- العنصر الثاني. الموضوع: ويتمثل في أوضاع ومراكز متعددة تدخل في إطار هذا الهيكل يجمع بينهما هدف واحد هو صيانة الحياة الخاصة للفرد، وذلك يمنحه الحق في أن يعترض على التدخل في خصوصياته أو التقصي عنها والتوصل لأي أمر يتعلق بهذه الخصوصية، أي توجب في النهاية النأي عن استعمال الغير لبياناته ذات الصلة بخصوصيته.

---

(١) – د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، المرجع السابق ، ص ١٧٦.

(٢) – د. أسامة عبدالله قايد ، المرجع السابق ، ، ص ١٢.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

وبناءً على ما سبق فقد ذهب مؤتمر القانونيين لدول الشمال في ستوكهولم المنعقد في مايو ١٩٦٧ إلى تعريف الحق في الخصوصية([١]) بأنه "حق الفرد في أن يعيش حياته بمنأى عن الأفعال الآتية: التدخل في حياته الأسرية أو المنزلية، والتدخل في كيانه البدني أو العقلي، أو حريته الأخلاقية أو العقلية، والاعتداء على شرفه أو سمعته ، ووضعه تحت الأضواء الكاشفة ، وإذاعة وقائع تتصل بحياته الخاصة، واستعمال اسمه أو صورته ، والتجسس والتلصص والملاحظة ، والتدخل في المراسلات. سوء تم ذلك عن طريق استخدام وسائل الاتصال الخاصة المكتوبة أو الشفوية، وكذلك إفشاء المعلومات المتحصلة بحكم الثقة والمهنة". كذلك فقد عرف الفقيه الفرنسي كاربونيه الحق في الخصوصية بأنها "المجال السري للفرد حيث يكون له القدرة على إبعاد الغير والحق في أن يترك هادئاً"([٢]).

وانطلاقا على ما سبق نستطيع القول بأننا نميل إلى الأخذ بالاتجاه الثاني في تعريف الحق في الخصوصية ولكن مع بعض التعديلات، وذلك لان وضع تعريف للحق في الخصوصية لا يتماشى مع ما تتميز به طبيعتها من أنها فكرة مرنه تتميز بالنسبية بحيث تختلف من مجتمع إلى آخر تبعاً لاختلف القيم والعادات والمستوى الثقافي لدى المجتمع والقيم الدينية والنظام السياسي السائدة لديه. وكذلك تختلف من حيث الزمان فما يعد خاصاً في زمان ما لا يعد كذلك في زمان آخر. وبالإضافة إلى ما سبق نستطيع القول بأنه يصعب وضع تعريف جامع مانع للحق في الخصوصية وانما نستطيع وضع بعض العناصر الأساسية التي يقوم عليها هذا الحق لكي يسترشد بها القضاء بما يضمن

([١]) – د. حسين محمود ابراهيم ، الوسائل العلمية الحديثة في الأثبات الجنائي ، دار النهضة العربية ، القاهرة ، ١٩٨١ ، ص ٤٢٠.

([٢]) – د. آدم عبد البديع آدم حسين ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٠ ، ص ١٨٤.

أن تحترم للإنسان الهدوء والسكينة والأمن عن طريق منع الآخرين من التدخل في خصوصياته. وفي نفس الوقت لا نترك هذا الحق بدون تعريف واضح.

وهكذا يتبين لنا أن ملامح الحق في الخصوصية ينحصر في أن تبقي حياة الشخص بكافة تفصيلاتها الخاصة سراً على غيره من الأشخاص والمؤسسات، لا تنتهك أو يعلم بها الغير، إلا من خلال إذن أو موافقة منه، ومن هنا يمكن استظهار ملامح الحق في الخصوصية على النحو التالي([1]):

١- أن يشكل السر واقعة أو حدث أو بيانات أو معلومات.

٢- أن يكون صاحب الواقعة أو الحدث او البيانات أو المعلومات حريصاً على ألا يعلم بها غيره.

٣- أن تلقي تلك الواقعة أو الحدث أو البيانات أو المعلومات الشخصية حماية قانونية في أي صورة كانت.

وتطبيقا على ذلك فاستخدام الكمبيوتر في تحويل ملفات العاملين في الشركات الكبرى إلى ملفات للبيانات مخزنة بالأجهزة الإلكترونية ، بدلا من أن تحتفظ الشركات بياناتهم في ملفات ورقيه ، يري بأنها تحمل في ثناياها كماً من الأخطار التي تهدد الحياة الخاصة([2]). حيث أن هذه الاجهزة الإلكترونية تعد إضافة أوجه مستجدة وخطرة

([1]) – د. محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ، القاهرة ، ١٩٩٤ ، ص٧٥٣ وما بعدها.

([2]) – د. حسام الدين الأهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي ، بحث مقدم لمؤتمر الكويت الأول للقانون والحاسب الآلي ، كلية الحقوق ، جامعة الكويت ، ١٩٩٤ ، ص ١٠.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

نتيجة الطبيعة التكنولوجيا في مجال تخزين ومعالجة ونقل المعلومات والبيانات الشخصية وامكانية اختراق عن بعد لهذه المواقع مما يشكل تهديد لحق الانسان في خصوصية بياناته الشخصية.

واستخلاصاً لما سبق نستطيع القول بأن مصطلح الخصوصية يقصد به قدرة الأفراد في التحكم في سرية وحفظ معلوماتهم وبياناتهم الشخصية، وكذلك القدرة على التحكم لمن يمكنه الاطلاع أو الوصول على هذه المعلومات والبيانات الشخصية. حيث أدى ظهور التجارة الإلكترونية وشبكات التواصل الاجتماعي والاعتماد بشكل أساسي في المراسلات على شبكة الإنترنت ومواقع التواصل الاجتماعي من خلال الهاتف المحمول. كل ذلك إدي إلى تطور مفهوم حق الأشخاص في الخصوصية بحيث أصبح يشمل حقهم في التراسل دون مراقبة عبر وسائل الاتصال الإلكترونية، وكذلك حق الأفراد في خصوصية معلوماتهم وبياناتهم الموجود على شبكة الإنترنت، ومنع فرض أي نوع من المراقبة عليها بدون سند قانوني أو حكم قضائي لما يشكله هذه التصرفات من انتهاك واضح للحق في خصوصية البيانات الشخصية. ومن هذا المنطلق فإن أغلب شبكات التواصل الاجتماعي تعمل على توفير خيارات متعددة لحماية خصوصية مستخدميها، حيث أن هناك الكثير من البرمجيات وكذلك التقنيات التي تقلل من مخاطر تعرض بيانات المستخدمين أو تصرفاتهم للمراقبة([1]). بالإضافة إلى ذلك فالمعلومات والبيانات التي يفصح عنها الأشخاص يجب أن تكون محدودة خاصة إذا كانت تتعلق بمعلومات وبيانات حساسة مثل الحسابات البنكية أو المعلومات الشخصية الحساسة.

وبذلك يتضح أهمية الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً كمبدأ يجب على الجميع الالتزام به لحماية خصوصية وسرية البيانات والمعلومات الشخصية من الكشف أو التجسس أو أي صورة أخرى من صور الانتهاك لهذا الحق.

([1]) – ا. محمد الطاهر ، الحريات الرقمية ، المفاهيم الأساسية ، مؤسسة حرية الفكر والتعبير ، الحريات الرقمية ، القاهرة ، ٢٠١٣ ، ص ٦ ، ٧.

فالحق في الخصوصية الرقمية هو الحق في حظر إفشاء البيانات الشخصية الخاصة بمستخدم التقنيات الرقمية ([١])، سواء من جانب الحكومة ، أو من جانت الشركات أو من قبل الأشخاص.

وتطبيقا على ذلك فقد ذهبت المحكمة الأوربية لحقوق الإنسان إلى القول بإن المحكمة لا ترى من إمكانية أو صعوبة في محاولة وضع تعريف جامع لمفهوم الحق في الخصوصية ، حيث أن انتفاء الوضوح يبدو أن هناك شيئاً ما خطأ ... فإن هذا غالباً ما يكون الفاصل الأكثر فائدة بين معرفة متي يكون التدخل في الحق في الخصوصية للفرد ، ومتي لا يكون([٢]). وقد حاولت مؤسسة الخصوصية الدولية أن تضفي شيئاً من الوضوح على ذلك من خلال تعريف الخصوصية بأنواعها المختلفة([٣]): خصوصية المعلومات مثل خصوصية البيانات الشخصية، والخصوصية الجسدية مثل الإجراءات العدائية ، وخصوصية الاتصال مثل المراقبة، وخصوصية المكان مثل المسكن. أما فيما يتعلق بمحل الدراسة وهو خصوصية المعلومات فيما يتعلق بخصوصية البيانات الشخصية التي يتم معالجتها إلكترونياً.

([١]) – ا. محمد طاهر ، أ. حسن عبد الحميد ، أحمد عزت ، الحق في الاتصال بين التقنية والقانون ، ورقة تعريفية ، مؤسسة حرية الفكر والتعبير ، القاهرة ، ٢٠١٣ ، ص ٥.

([٢]) – د. حسين جي ، الخصوصية باعتبارها حرية ، في آر جورجيرسين ، حقوق الإنسان في مجتمع المعلومات العالمي ، دار نشر مطبعة MIT ، كامبريدج ، ٢٠٠٦.

([٣]) – المنظمة الدولية لحماية الخصوصية ، ٢٠٠٦.

المطلب الثاني. ماهية البيانات الشخصية الإلكترونية

لابد من الإشارة في البداية إلى أنه يقصد بقاعدة البيانات بصفة عامة بانها مجموعة من المواد الأدبية والفنية والموسيقية وغيرها ، مثل النص والصوت والصور والأرقام والحقائق والبيانات ؛ والتي يجب أن تغطي مجموعة من الأعمال، أو البيانات أو غيرها من المواد المرتبة بطريقة منهجية أو منهجه ويمكن الوصول إليها بشكل فردي، ويترتب على ذلك العمل على تثبيت من مصنف سمعي بصري، سينما، أدبي أو موسيقي ، وعلى هذا النحو تقع البيانات في نطاق هذا التوجيه الاوربي(١) الخاص بحماية البيانات الشخصية.

وفضلاً على ذلك فقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة الثانية منه على أنه يقصد بالبيانات(٢) "بانها كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات ، كالأرقام والحروف والرموز وما إليها" ... ويقصد بتقنية المعلومات "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جمع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة". ويلاحظ مما سبق أن المشرع العربي ذهب إلى وضع تعريف مرن يلائم تطورات العصر وذلك بخلاف المشرع الأوربي، حيث ذكر قاعدة عامة يمكن على أساسها تحديد ماهية البيانات وهو كل ما يمكن تخزينه

---

(١) – التوجيه الاوربي الصادر في ١١ مارس ١٩٩٦ ، البرلمان الاوربي ومجلس الاتحاد الاوربي ، الخاص بشأن الحماية القانونية لقواعد البيانات ، Directive n° ٩٦/٩/CE du Parlement européen et du Conseil, du ١١ mars ١٩٩٦ concernant la protection juridique des bases de données.

(٢) – الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، الموقعة بالقاهرة في ٢١ ديسمبر ٢٠١٠ ، والتي قامت جمهورية مصر العربية بالتصديق عليها في ٢٠١٤ ، ونشرت في الجريدة الرسمية في العدد ٤٦ الصادر بتاريخ ١٣ نوفمبر ٢٠١٤.

ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، وبالتالي يتلائم هذا التعريف مع متغيرات العصر المتطورة خاصة في المجال التكنولوجيا.

الفرع الأول. مفهوم البيانات الشخصية الإلكترونية

يقصد بالبيانات الشخصية بانها هي المعلومات الخاصة بشخص طبيعي قابل للتعرف عليه، وذلك وفقا لما نص عليه التوجيه الأوربي الخاص بحماية البيانات الشخصية. ويلاحظ أن هذا التعريف يمثل اتجاه واسع من المشرع الأوربي في تعريف البيانات الشخصية، وترجع الحكمة من هذا الاتجاه للمشرع الاوربي إلى أن التضييق من مفهوم البيانات الشخصية قد يسمح للعديد من الجهات بالتعدي عليها وبالتالي فرض ذلك من باب أولى على المشرع الاوربي أن يضع تعريف موسع بدلاً من التعريف الضيق.

أما بالنسبة لموقف المشرع الفرنسي فقد نص في المادة الثانية من القانون رقم ١٧ لسنة ١٩٧٨ المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤ الخاص بحماية البيانات الشخصية(١) على تعريف البيانات الشخصية بانه يعتبر بياناً شخصياً هو كل معلومة تتعلق بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر، سواء تم ذلك بالرجوع إلى رقم التعريف أو إلى عنصر واحد أو أكثر من عنصر يخصه. ولتحديد

(١) – Loi n° ٢٠٠٤ – ٨٠١ du août ٢٠٠٤ relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° ٧٨ – ١٧ du ٦ janvier ١٩٧٨ relative à l'informatique, aux fichiers et aux libertés, J.O, ٧ août ٢٠٠٤.

ما إذا كان الشخص قابلاً للتحديد، يجب النظر في جميع الوسائل التي من خلالها يمكن التوصل لتحديد هويته أو التي يمكن للمراقب أو لأي شخص آخر الوصول إليه.

واستخلاصاً مما سبق نستطيع القول بان المشرع الفرنسي قد تبني الاتجاه الذي ينادي بوضع تعريف واسع مرن للبيانات الشخصية بما يسمح بدخول جميع أشكال البيانات الشخصية وبالتالي حماية أوسع لحق الأفراد في الخصوصية(١). فوفقا لتعريف المشرع الفرنسي فإن أي معلومة تتعلق بشخص طبيعي تعتبر بياناً شخصياً يخضع للحماية القانونية وفقا لنص المادة الثانية من قانون حماية البيانات الشخصية، مادام هذا الشخص الطبيعي محدد الهوية، أو أنه من الممكن تحديد هويته بأي طريقة مباشرة أو غير مباشرة.

أما بالنسبة لموقف اللجنة الفرنسية للمعلوماتية والحريات CNIL فقد ذهبت إلى انه لتحديد البيانات الشخصية يجب مراعاة جميع الوسائل المتاحة لوحدة معالجة البيانات لتحديد ما إذا كان الشخص قابلا للتحديد من خلالها أم لا(٢). وتعني بالبيانات الشخصية أي معلومات تتعلق بشخص محدد أو يمكن تحديده؛ فالشخص الذي يمكن التعرف عليه هو الشخص الذي يمكن تحديده، بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى رقم تعريف على سبيل المثال رقم البطاقة الشخصية أو رقم الضمان الاجتماعي أو واحد أو أكثر من العوامل المحددة لهويته البدنية أو الفسيولوجية أو

---

(١) – Baffard WILLIAM, Le système de traitement des infractions constatées et la protection des données personnelles, mémoire de DEA informatique et droit, faculté de droit, université de Montpellier I, ٢٠٠٣, p. ١٥.

(٢) – CNIL, to protect personal data, support innovation, preserve individual liberties, www.cnil.fr/en/personal-data-definition.

العقلية أو الاقتصادية أو الثقافية أو الاجتماعية على سبيل المثال الاسم والاسم الأول، وتاريخ الميلاد، وبيانات القياسات الحيوية، وبصمات اليد، والحمض النووي ... الخ.

أما بالنسبة لموقف المشرع المصري في بادى الأمر لم تحظى خصوصية وحماية البيانات الشخصية باهتمام كما هو موجود بالنسبة للمشرع الأوربي، بحيث لا يوجد تشريع خاص يحمي ويحدد ماهية البيانات الشخصية التي تخضع للحماية القانونية، ولكن هناك محاولات في مجال القضاء منها ما ذهبت اليه المحكمة الدستورية العليا إلي أن ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي دوماً – ولاعتبار مشروع – ألا يقتحمها أحد ضماناً لسريتها، وصوناً لحرمتها، ودفعاً لمحاولة التلصص عليها ، أو اختلاس بعض جوانبها ، وبوجه خاص من خلال الوسائل العلمية الحديثة التي بلغ تطورها حداً مذهلاً ، وكان لتنامي قدراتها علي الاختراق أثراً بعيداً علي الناس جميعهم حتي في أدق شئونهم، بل وبياناتهم الشخصية التي غدا الاطلاع عليها ، وتجميعها نهباً لأعينها ولآذانها، وكثيراً ما الحق النفاذ إليها الحرج أو الضرر بأصحابها، وهذه المناطق من خواص الحياة ودخائلها ، تصون مصلحتين قد تبدوان منفصلتين، إلا أنهما تتكاملان، ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التي ينبغي كتمانها، وكذلك نطاق استقلال كل فرد ببعض قراراته الهامة التي تكون – بالنظر إلي خصائصها وآثارها – أكثر اتصالاً بمصيره وتأثيراً في أوضاع الحياة التي اختار أنماطها، وتبلور هذه المناطق جميعها – التي يلوذ الفرد بها ، مطمئناً لحرمتها ليهجع إليها بعيداً عن أشكال الرقابة وأدواتها – الحق في أن تكون للحياة الخاصة تخومها بما يرعي الروابط الحميمة في نطاقها ، ولئن كانت بعض الوثائق

الدستورية لا تقرر هذا الحق بنص صريح فيها إلا أن البعض يعتبره من أشمل الحقوق وأوسعها ، وهو كذلك أعمقها اتصالاً بالقيم التي تدعو إليها الأمم المتحضرة([1]).

لكن من الجدير بالذكر فإن موقف المشرع المصري قد تغيير في ١٤ أغسطس ٢٠١٨ حيث صدر القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات([2])، والذي نص فيها في المادة الأولى على تعريف البيانات الشخصية "بأنها أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده ، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى". ثم أضافة المادة الأولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ على التعريف السابق للبيانات الشخصية الأمثلة على تلك البيانات الشخصية "وهي كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية"([3]). وبذلك يظهر لنا أن المشرع المصري سار على نفس النهج الفرنسي في وضع أمثلة على البيانات الشخصية محل الحماية في هذا القانون.

وتأسيسا على ما سبق يمكننا القول أن يقصد بالبيانات الشخصية بانها كل نوع من أنواع المعلومات سواء كانت معلومة واحدة أو مجموعة معلومات، التي يمكن من خلالها أن تحدد شخص ما أو تفرده كفرد. والأمثلة على ذلك أسم الشخص وعنوانه

([1]) – المحكمة الدستورية العليا المصرية ، الحكم الصادر في القضية رقم ٢٣ لسنة ١٦ قضائية ، دستورية ، بتاريخ ١٨ مارس ١٩٩٥، القاهرة.

([2]) – المادة الأولى من قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ، الصادر في ١٤ أغسطس ٢٠١٨ ، الجريدة الرسمية لجمهورية مصر العربية ، العدد ٣٢ مكرر (ج) ، ص ٣.

([3]) – المادة الأولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، المنشور في الجريدة الرسمية العدد ٢٨ مكرر (هـ) الصادر في ١٥ يوليه ٢٠٢٠ ، ص ٤.

ورقم البطاقة أو الهوية الشخصية وتاريخ الميلاد أو الصورة أو السجلات الصحية. وبناء على ذلك يعتبر من البيانات الشخصية أي بيان يحدد الهوية ويمكن من خلاله التحقق من الشخص سواء تم ذلك بطريقة مباشرة أو غير مباشرة مثل بصمات اليد أو الحمض النووي أو غيرها من البيانات الأخرى.

وهكذا يمكن أن تكون هذه المعلومات فريدة من نوعها، حيث أن تكنولوجيا المعلومات والاتصالات توليد كمية متزايدة من البيانات على نحو متزايد مثل بطاقة دفع الائتمان، والمكالمات المقدمة من الهاتف الخليوي والتي تسمح بتحديد وبدقة المكان الذي تم من خلالها إجراء المكالمة أو اتصال بالإنترنت. بالإضافة إلى ذلك تمثل البيانات الشخصية قدرا كبيرا من القيمة التجارية. ونتيجة لذلك يتم السعي بشكل متزايد بأن يتم شراء الملفات وبيعها عن بعد، لذلك تهتم المجموعات التجارية بتحديد وتجميع في ملف واحد "العملاء الجيدين" لكل من الشركات التابعة لها، أو "العملاء السيئين." من خلال الآثار التي تركتها استخداماتهم لتكنولوجيا المعلومات بحيث أصبح من السهل من خلالها معرفة اهتماماتهم وبالتالي العمل على استغلالها، فبسبب التطوير الرهيب للبرمجيات مثل تكنولوجيا محرك البحث على الإنترنت، أو بيانات البحث للبرمجيات، يمكن معرفة وتتبع البيانات الشخصية للأفراد، وبناء على ذلك يتم بناء ملف تعريف للسلوك الخاص بالشخص من أجل أرسال الإعلانات التي تناسب كل شخص ويطلق على تلك الملفات اسم ملفات الارتباط. ومن هنا جاءت أهمية التدخل القانوني لحماية البيانات الشخصية التي يتم معالجتها إلكترونياً في هذه الحالات.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

ومن هذا المنطلق تعتبر البيانات من البيانات الشخصية المعالجة إلكترونياً عندما يتم معالجتها على نحو إلكتروني([١])، أو يتم الحصول عليها أو جمعها أو استخراجها على أي نحو آخر تمهيداً لمعالجتها إلكترونياً، أو تتم معالجتها عن طريق الجمع بين المعالجة الإلكترونية والمعالجة التقليدية.

ويقصد بالمعالجة الإلكترونية للبيانات بأنها "مجموعة العمليات التي تتم آلياً وباستخدام الحاسب الآلي، وتتعلق بالتجميع، والتسجيل، والاعداد، والتعديل، والاسترجاع، والاحتفاظ والمحو، للبيانات والمعلومات، وكذلك مجموعة العمليات التي تتم آلياً بهدف الاستفادة من البيانات والمعلومات، وعلى الأخص عمليات الربط والتقريب والانتقال والدمج مع البيانات الأخرى أو تحليلها للحصول على معلومة ذات دلالة خاصة، أو هي إخضاع المعلومات والبيانات لعمليات حسابية ومنطقية من أجل الحصول على نتائج محددة طبقاً لبرنامج مخزون وذلك بواسطة استعمال الحاسبات الآلية"([٢]).

وعلى الرغم مما سبق فان محكمة النقض الفرنسية قد قضت بإن مجرد إدخال البيانات في الكمبيوتر لا يحقق به وصف البيانات التي تم معالجتها إلكترونياً، إذا كان ذلك لا يعدم أن يكون كتابة لتلك البيانات وكان الغرض منها طبعها على ورق وليس الاحتفاظ بها في الجهاز. حيث كانت القضية تتعلق ببيانات نقلت من بعض ملفات

([١]) – الفقرة الأولى من المادة الثانية من القانون القطري رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية الصادر في ٣ نوفمبر ٢٠١٦. وكذلك المادة الأولى من القانون المصري بشأن مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

([٢]) – د. عمرو حسبو ، حماية الحريات في مواجهة نظم المعلومات ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ ، ص ٥٠ ،. د. عبد الفتاح حجازي ، الحماية الجنائية لنظام التجارة الإلكترونية ، الجزء الثاني ، دار الفكر الجامعي ، القاهرة ، ٢٠٠٢ ، ص ٢٨١. وانظر كذلك الفقرة الثانية من المادة الأولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠.

المرضي وأراد الطبيب طباعتها على ورق لتسهيل تجميعها(١). ولكن هذا الحكم محل انتقاد من وجهة نظري حيث أن المشرع الفرنسي كان واضح في وضع تعريف موسع للبيانات الشخصية التي تم معالجتها إلكترونياً بحيث أصبحت مجرد تجميع البيانات الشخصية تمهيداً لمعالجتها إلكترونياً من البيانات التي تدخل في نطاق الحماية القانونية للبيانات الشخصية المعالجة إلكترونياً، وبالتالي لا اجتهاد مع وجود نص يلزم المحكمة في تحديد البيانات الشخصية الإلكترونية. وهذا ما سارت عليها الأحكام الفرنسية بعد ذلك.

وانطلاقا مما سبق فقد نص المشرع الأوربي في المادة ٢٦ من اللائحة العامة لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨ على انه:

فينبغي أن تطبق مبادئ حماية البيانات على أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده. وينبغي اعتبار البيانات الشخصية التي خضعت لاسم مستعار، والتي يمكن أن تعزى إلى شخص طبيعي عن طريق استخدام معلومات إضافية، معلومات عن شخص طبيعي يمكن التعرف عليه ، ولتحديد ما إذا كان الشخص الطبيعي هو الذي يمكن تحديده، فينبغي أن يؤخذ في الحسبان جميع الوسائل التي يحتمل أن تستخدم على نحو معقول ، مثل التفرد، أما من قبل المراقب أو من قبل شخص آخر لتحديد الشخص الطبيعي بشكل مباشر أو غير مباشر. وللتأكد مما إذا كان من المرجح أن تستخدم الوسائل لتحديد الشخص الطبيعي، ينبغي مراعاة جميع العوامل الموضوعية، مثل تكاليف الوقت اللازم لتحديد الهوية ومقدار الوقت

(١) – Cass. Crim, ٦ juill ١٩٩٤, cité par Jacques FRANCILLIN, Infractions relevant du droit de l'information et de la communication, Rev. Sc. Crim, ١٩٩٦, Chronique de jurisprudence, Paris, p.٦٧٦.

اللازم له، مع الأخذ في الاعتبار التكنولوجيا المتاحة في وقت المعالجة والتطورات التكنولوجية. ولذلك ينبغي ألا تنطبق مبادئ حماية البيانات على المعلومات مجهولة الهوية، أي المعلومات التي لا تتعلق بشخص طبيعي محدد أو يمكن تحديده أو بيانات شخصية مجهولة المصدر بحيث لا يكون موضوع البيانات قابلا للتحديد أو لم يعد قابلا للتحديد. ولذلك فإن هذه اللائحة العامة الأوربية لا تتعلق بمعالجة هذه المعلومات المجهولة، بما في ذلك المعالجة لأغراض إحصائية أو بحثية .أي المعلومات التي لا تتعلق بشخص طبيعي محدد أو يمكن تحديده أو بيانات شخصية مجهولة المصدر بحيث لا يكون موضوع البيانات قابلا للتحديد أو لم يعد قابلا للتحديد. ولذلك فإن هذه اللائحة لا تتعلق بمعالجة هذه المعلومات المجهولة ، بما في ذلك البيانات المتعلقة بالأغراض الإحصائية أو البحثية.

أما بالنسبة لموقف المشرع القطري فقد نص في المادة الأولى من القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية على أنه يقصد بالبيانات الشخصية محل الحماية في هذا القانون(١) هي "بيانات عن الفرد الذي تكون هويته محددة، أو يمكن تحديدها بصورة معقولة ، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى". أما معالجة البيانات الشخصية فهي "عبارة عن إجراء عملية أو مجموعة عمليات على البيانات الشخصية، كالجمع والاستلام والتسجيل والتنظيم والتخزين والتهيئة والتعديل والاسترجاع والاستخدام والإفشاء والنشر والنقل والحجب والتخلص والمحو والإلغاء".

(١) – أنظر المادة الاولي من القانون القطري بشأن حماية خصوصية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦.

أما بالنسبة للمشرع المغربي فقد نص في الفقرة الأولى من المادة الأولى من القانون رقم ٠٨ – ٠٩ لسنة ٢٠٠٩ الخاص بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، على تعريف البيانات ذات الطابع الشخصي بانها "كل معلومة كيفما كان نوعها بغض النظر عن دعامتها، بما في ذلك الصوت والصورة، والمتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه والمسمى بعده بالشخص المعني. ويكون الشخص قابلاً للتعرف عليه إذا كان بالإمكان التعرف عليه، بصفة مباشرة أو غير مباشرة، ولاسيما من خلال الرجوع إلى رقم تعريف أو عنصر أو عدة عناصر مميزة لهويته البدنية أو الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"([1]).

أما بالنسبة لموقف المشرع التونسي فقد نص في المادة ٤ من قانون حماية المعطيات الشخصية رقم ٦٣ لسنة ٢٠٠٤([2]) على تعريف البيانات الشخصية "بأنها كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصياً طبيعياً معرّفاً أو قابلاً للتعريف بطريقة مباشرة أو غير مباشرة، باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانوناً". وأضافت المادة ٥ من نفس القانون النص على انه "يعد قابلا للتعريف الشخص الطبيعي الذي يمكن التعرّف عليه بصورة مباشرة أو غير مباشرة من خلال مجموعة من المعطيات أو الرموز المتعلقة خاصة بهويته أو بخصائصه الجسمية أو الفيزيولوجية أو الجينية أو النفسية أو الاجتماعية أو الاقتصادية أو الثقافية. إلا أن المشرع التونسي نص على انه يخرج من نطاق الحماية هذا القانون معالجة المعطيات

([1]) – المادة الأولي الفقرة الثانية من القانون المغربي ، ظهير شريف رقم ١.٠٩.١٥ صادر في ٢٢ من صفر ١٤٣٠ (١٨ فبراير ٢٠٠٩) بتنفيذ القانون رقم ٠٩.٠٨ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي. نشر في الجريدة الرسمية عدد ٥٧١١ بتاريخ ٢٧ صفر ١٤٣٠ (٢٣ فبراير ٢٠٠٩) ، ص ٥٥٢.

([2]) – القانون الاساسي التونسي عدد ٦٣ لسنة ٢٠٠٤ ، الصادر في ٢٧ يوليه ٢٠٠٤ والتعلق بحماية المعطيات الشخصية.

الشخصية لغايات لا تتجاوز الاستعمال الشخصي أو العائلي بشرط عدم إحالتها إلى الغير"([1]).

وانطلاقاً مما سبق نستطيع القول بان حماية البيانات الشخصية التي تم معالجتها إلكترونيا يجب أن يكون من خلال قانون خاص مصمم لحماية هذه البيانات والمعلومات الشخصية التي يتم جمعها ومعالجتها وتخزينها بوسائل آلية أي أن تكون جزء من نظام إيداع للمعلومات والبيانات الشخصية. ففي المجتمعات الحديثة حتى نستطيع حماية المعلومات والبيانات من الانتهاكات لابد من قوانين خاصة تحمي البيانات والمعلومات الشخصية وتقيد وتشكل أنشطة الشركات والحكومات والأفراد. حيث يتم الحصول على هذه البيانات الشخصية بطريق مباشر في كل مرة تستخدم فيها خدمة أو شراء منتج عبر الإنترنت، أو التسجيل بالبريد الإلكتروني، أو الدخول في أي عقد أو طلب خدمة، يتم من خلالها إعطاء معلومات وبيانات شخصية، أو عن طريق غير مباشر من خلال الحصول على هذه المعلومات والبيانات الشخصية دون علم الشخص، وبالتالي لابد من حماية هذه الممارسات من خلال قانون يحمي البيانات الشخصية التي تم معالجتها إلكترونيا. وبناء على ذلك فقد أصدرت أكثر من ١٠٠ دولة في جميع أنحاء العالم قوانين شاملة لحماية خصوصية البيانات الشخصية، وهناك أكثر من ٤٠ دولة أخرى لديها مشاريع قوانين أو مبادرات متعلقة بحماية البيانات الشخصية.

مفهوم البيانات الشخصية ذات الطبيعة الخاصة أي البيانات الحساسة:

تنص المادة ٨ من المبادئ التوجيهية للاتحاد الأوربي على أنه "يحظر على الدول الأعضاء معالجة البيانات الشخصية الحساسة الكاشفة للأصل العرقي، والآراء السياسية، والمعتقدات الدينية أو الفلسفة، والعضوية في النقابات العمالية، ومعالجة البيانات المتعلقة بالصحة أو الحياة الجنسية. إلا واستثناءً من ذلك يجوز النص في

([1]) – المادة ٣ من قانون حماية المعطيات الشخصية التونسي رقم ٦٣ لسنة ٢٠٠٤.

التشريع المحلي للدول الاعضاء في الاتحاد الأوربي على خلاف ذلك ولكن بشرط الحصول على الموافقة المسبقة الصريحة من صاحب البيانات الشخصية الحساسة على معالجة بياناته، ويجوز ذلك عند الضرورة ومن أجل حماية حقوق وواجبات متحكم البيانات في مجال قانون العمل، أو لحماية المصالح الأساسية لصاحب البيانات".

وبناء على ذلك نستطيع القول بأنه يقصد بالبيانات الشخصية الحساسة بأنها هي البيانات المتعلقة بالعرق، والديانة، والمعتقدات، والآراء السياسية، والسجل الإجرامي، أي البيانات التي تتميز بطابع خاص وحساس للشخص بحيث يجعله يعمل على عدم إطلاع الغير عليها لما تشكل من طبيعة خاص له. بحيث تختلف خطورتها وأهميتها عن البيانات الأساسية مثل الاسم، تاريخ الميلاد والعنوان. إذ تتطلب بعض البيانات حماية أكبر من غيرها. فمثلا يتطلب التوجيه الأوروبي من الجهة التي تنوي التعامل مع هذه البيانات الحساسة موافقة صاحب البيانات الصريحة(١). وبناء على ذلك فقد نص المشرع الانجليزي في قانون حماية البيانات الصادر في عام ١٩٩٨ على اعتبار المعلومات بأنها من البيانات الشخصية الحساسة "إذا كانت متعلقة بالأصل العرقي لصاحب البيانات، أو آرائه السياسية، أو دينه أو ما شابه ذلك من معتقدات، أو الانتماء إلى النقابات العمالية، أو صحته الجسدية أو العقلية، أو حياته الجنسية، أو جريمة مرتكبه أو أي جريمة متهم بها، أو أي محاكمات على أي جريمة مرتكبة أو متهم بارتكابها".

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ١٦ من القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية على أنه "تعد من البيانات الشخصية ذات الطبيعة الخاصة، البيانات المتعلقة بالأصل العرقي، والأطفال، والصحة

(١) – انظر: قانون حماية البيانات البريطاني ، القسم الثاني.

أو الحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقة الزوجية، والجرائم الجنائية. وللوزير أن يضيف أصنافاً أخرى من البيانات الشخصية ذات الطبيعة الخاصة، إذا كان من شأن سوء استخدامها أو إفشائها إلحاق ضرر جسيم بالفرد. ولا يجوز معالجة البيانات الشخصية ذات الطبيعة الخاصة، إلا بعد الحصول على تصريح بذلك من الإدارة المختصة، وفقاً للإجراءات والضوابط التي يصدر بتحديدها قرار من الوزير. وللوزير، بقرار منه، فرض احتياطات إضافية لغرض حماية البيانات الشخصية ذات الطبيعة الخاصة".

بالإضافة إلى مما سبق يعتبر المشرع القطري البصمة الوراثية للفرد من البيانات الشخصية الحساسة ، ومع ذلك لا توضع في البطاقة الشخصية كباقي البيانات والسبب أنها معلومات أكثر حساسية للفرد ، حيث أن التعامل مع هذه البيانات يكون بضوابط استثنائية وليس بنفس الضوابط التقليدية ، لذلك أُعطي الحق في إضافة أصناف أخرى من هذه المعلومات ذات الطبيعة الخاصة إذا كان إفشاؤها يسبّب ضرراً للفرد([1]). فهذه البيانات الشخصية الحساسة تتغير وتتنوع حسب كل زمان ومكان.

وقد سار المشرع المصري في تعريف البيانات الشخصية الحساسة في قانون حماية البيانات الشخصية الجديد رقم ١٥١ لسنة ٢٠٢٠ على نفس النهج القطري والفرنسي كذلك فقد عدد المشرع المصري هذه البيانات الشخصية الحساسة على سبيل الحصر وهي البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية ، أو بيانات القياسات الحيوية (البيومترية) أو البيانات المالية أو المعتقدات الدينية أو الآراء

([1]) – انظر في ذلك الفصل الرابع من القانون القطري رقم ١٣ لسنة ٢٠١٦ بشان حماية البيانات الشخصية.

السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة([1]).

أما بالنسبة لموقف المشرع المغربي([2]) فقد نص في الفقرة الثالثة من المادة الأولى من القانون رقم ٠٩-٠٨ لسنة ٢٠٠٩ على تعريف المعطيات الحساسة "بانها معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما في ذلك المعطيات الجينية". ونستخلص مما سبق فان أي تحديد لقائمة البيانات الشخصية الحساسة يحتاج إلى تفسير واضح، وتطبيقا على ذلك فالبيانات عن أن شخص مصاب بالكسر في القدم وأدخل المستشفى بناء عليها، أقل حساسية على نحو واضح من بيانات إصابته بفيروس نقص المناعة المكتسب الإيدز. فالمحافظة على خصوصية السجلات الطبية أمر في غاية الاهمية لما يمثل الإخلال بها من انتهاك للحق في خصوصية البيانات الشخصية التي تم معالجتها الكترونياً.

وتطبيقا على ذلك فقد قضت المحكمة الأوربية لحقوق الإنسان بمعاقبة الحكومة الفنلندية لفشلها في حماية بيانات المريض الطبية التي تحتفظ بها إحدى المستشفيات ضد مخاطر الوصول غير المصرح به، وربط الحكم الصادر بين الحق في الخصوصية بموجب الاتفاقية الأوربية لحقوق الإنسان وحماية البيانات الشخصية، ورأت المحكمة الأوربية لحقوق الإنسان أن المادة ٨ من التوجيهية الأوربية بشأن حماية البيانات الشخصية تفرض واجباً إيجابياً على الدول بضمان أمن البيانات الشخصية ، فنظام حفظ الملفات في المستشفى محل القضية يخالف القانون الفنلندي الذي يتطلب من

([1]) – الفقرة الثالثة من المادة الأولى من قانون حماية البيانات الشخصية المصري، رقم ١٥١ لسنة ٢٠٢٠.

([2]) – القانون المغربي الخاص بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي ، رقم ٠٩-٠٨ الصادر في ١٨ فبراير ٢٠٠٩.

المستشفيات تأمين البيانات الشخصية من الوصول غير المصرح به. حيث ترجع وقائع القضية إلى أن مقدمة البلاغ وهي ممرضة في المستشفى كانت تعالج من فيروس ضعف المناعة المكتسب الإيدز، قد اشتبهت في أن زملاءها في العمل قد اكتشفوا أنها مصابة بفيروس الإيدز من خلال قراءة السجلات الطبية السرية الخاصة بها، وعلى الرغم من أن قواعد المستشفى تحظر الوصول إلى هذه الملفات إلا لأغراض العلاج، فإن سجلات المرضى، في الواقع كانت في متناول جميع العاملين في المستشفى. حيث رأت المحكمة أن حقيقة كون نظام السجلات الطبية في المستشفى غير أمن بالدرجة الكافية ، مما يجعلها مسئولة عن الكشف غير المبرر عن البيانات الشخصية الطبية الخاصة بالممرضة([1]). وبالتالي فقد تم انتهاك للحق في خصوصية البيانات الشخصية. وهكذا يثير هذا الموضوع تساؤل حول هل يعتبر ابلاغ الطبيب إلى السلطات المعنية بالصحة العامة بإن المريض مصاب بفيروس نقص المناعة المكتسب الإيدز انتهاك للحق في خصوصية هذه البيانات الشخصية الحساسة لهؤلاء المرضي؟ للإجابة عن هذا التساؤل انقسم الفقه إلى اتجاهين وهو ما سوف نستعرضه على النحو التالي:

الاتجاه الاول. يري أن سجلات مرضي الإيدز، أو أولئك المصابين بفيروس نقص المناعة المكتسب من سجلات الحساسة، وبالتالي تدخل تحت نطاق الحماية القانونية للبيانات الشخصية الحساسة التي تم معالجتها إلكترونيا، وبناء عليه لا يجوز للطبيب إبلاغ أي جهة أو سلطة بالحالة الصحية للمرضي وإلا عد ذلك انتهاكاً للحق في خصوصية البيانات الشخصية الحساسة.

أما الاتجاه الثاني. فيجيز للطبيب إبلاغ السلطات المعنية بالصحة بحالة المرضي وذلك من أجل احتواء انتشار المرض. حيث تنص بعض الدول على أن مرض الإيدز من

([1]) – أ. ريموند واكس ، الخصوصية: مقدمة قصيرة جداً ، ترجمة ياسر حسن ، الطبعة الأولى ، كلمات عربية للترجمة والنشر ، القاهرة ، ٢٠١٣ ، ص ١٢٤.

الامراض التي يجب التبليغ عنه للسلطات الصحية، ومن ثم هناك واجب قانوني يتعلق بإبلاغ السلطات عند اكتشاف وجوده. ورغم وجاهة هذا الاتجاه إلا انني أري أنه الحجج والمبررات التي ساقها الاتجاه الثاني غير كافية أو مقنعه لانتهاك الحق في خصوصية البيانات الشخصية الحساسة، فبالنظر إلى العواقب الوخيمة التي يمكن أن تنتج عن الكشف هذه البيانات الحساسة. فالواقع أن الفشل في توفير حماية كافيه لهذه البيانات الشخصية الحساسة سوف يتسبب في نتائج عكسية، حيث سوف يترتب على ذلك أن يمتنعوا الأشخاص عن إجراء اختبارات الكشف عن الفيروس، وبالتالي ازدياد نسبة انتشار المرض وقلة مصادر المعلومات عنه. وبناء على ذلك فقد وضعت منظمة التعاون الاقتصادي والتنمية دليلاً ارشادياً لحماية خصوصية البيانات المعالجة إلكترونيا، وهذه القواعد تصف البيانات والمعلومات الشخصية على انها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر.

ومما سبق نستطيع القول أن مفهوم حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً محل الحماية الجنائية في المواثيق والتشريعات المتقدمة يتطلب أن تكون البيانات الشخصية التي تم معالجتها إلكترونياً متوافر فيها الشروط التالية: –

١. أن يتم الحصول عليها بطريق مشروعة وقانونية.

٢. وأن تستخدم للغرض الأصلي المعلن والمحدد ولا تكشف لغير المصرح لهم بالاطلاع عليها، وأن تكون متصلة بالغرض المقصود من الجمع ولا تتجاوزه ومحصورة بذلك.

٣. أن تكون صحيحة وتخضع لعمليات التحديث والتصحيح.

٤. أن يتوفر حق الوصول اليها مع حق الإخطار بأنشطة المعالجة أو النقل وحق التصحيح والتعديل وحتى طلب الإلغاء.

٥. أن تحفظ وفق معيار السرية بحيث تحمى سريتها وفق معايير أمن ملائمة لحماية المعلومات ونظم المعالجة. وأن تتلف عند استنفاذ الغرض من جمعها بطريقه تحمي

هذه البيانات الشخصية من امكانية استرجاعها أو الاطلاع عليها من الغير خلال مدد معقولة.

إلا أن التحديد المسبق لصور البيانات الشخصية محل الحماية القانونية ليس بالأمر الهين، لأنه في المستقبل ومع التطور من المتصور أن تظهر صور من المعلومات التي يمكن اعتبارها بيانات شخصية، مثال على ذلك أدي شيوعا استخدام شبكة الانترنت إلى اعتبار الرقم الخاص بالكمبيوتر الشخصي IP بياناً شخصياً، وهو أمر لم يكن معروف قبل ذلك(١)، وكذلك البيانات الشخصية الموجودة على مواقع التواصل الاجتماعي مثل الفيسبوك أو التوتير أو الماسنجر ... الخ.

(١) – Melle Sophie LALANDE, L'adresse IP de votre ordinateur, une donnée personnelle relevant du régime communautaire de protection, art disponible sur: www.droit-ntic.com, la date de mise en ligne est: ٩ déc. ٢٠٠٣. Sophie LOUVEAUX, Comment concilier le commerce électronique et la protection de la vie privée, en ligne: http://www.crid.be/pdf/crid/٤٧١٠.pdf. Paris, ١٩٩٩. PP. ١٥١ – ١٦٢.

الفرع الثاني. أنواع البيانات الشخصية الإلكترونية

يمكن تقسم البيانات الشخصية المعالجة إلكترونياً والتي انشأها الشخص أو قام غيره بإنشائها لشخصه إلى بيانات الاختيارية وبيانات مرصودة وبيانات استدلالية وذلك على النحو التالي:

١. البيانات الشخصية المعالجة إلكترونياً الاختيارية:

هي البيانات الشخصية التي يقوم الشخص بإدراجها طواعية ويتشاركها مع غيره عبر مواقع التواصل الاجتماعي مثل الفيسبوك والتوتير والإنستجرام وتشمل الاسم والعنوان والتليفون والبريد الالكتروني والصور بالإضافة إلى الأخبار اليومية الحياتية التي يتشاركها مع غيره من المستخدمين.

٢. البيانات الشخصية المعالجة إلكترونياً المرصودة:

هي البيانات الشخصية التي يتم الحصول عليها عن طريق التبع والرصد بواسطة نظام GPS مثل تحديد الأماكن التي يتم من خلالها تم ارسال رسائل الواتساب أو الماسنجر أو البريد الإلكتروني أو التوتير أو الفيسبوك.

٣. البيانات الشخصية المعالجة إلكترونياً الاستدلالية:

هي البيانات الشخصية الناتجة من تحليل البيانات المرصودة والاختيارية والتي يتم تحليلها لارتباطها بالأشخاص الذين تم تتبعهم أو رصد وتحليل بياناتهم لاستخدام هذه البيانات الشخصية في عمل الدعاية والتسوق للتجارة الالكترونية.

ومما سبق يتضح أن الحماية الجنائية للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً يتم من خلال وجهين:

الوجه الأول. حماية حرمة الحياة الخاصة للشخص أي حق الشخص في أن ينتهج الأسلوب الذي يرتضيه ليحي حياته الخاصة بعيداً عن تدخل باقي أفراد المجتمع.

الوجه الثاني. حماية سرية الحياة الخاصة للشخص أي حق الشخص في أن تظل سرية أخباره وبياناته والتي تتولد عن حريته وهذه الاسرار قد تكون متعلقة بالنواحي النفسية والعقلية مثل الحالة الصحية لجسم الانسان، وقد تكون متعلقة بالنواحي الخارجية للإنسان مثل مراسلاته وبيانات الشخصية.

وبناء على ذلك يمكن ذكر بعض الأمثلة للبيانات الشخصية المعالجة إلكترونياً محل الحماية الجنائية وهي كالتالي:

١. البيانات الشخصية المعالجة إلكترونياً التي تعبر عن كيان الانسان الخارجي:

تعتبر البيانات الشخصية التي تعبر عن كيان الانسان الخارجي مثل الاسم والعنوان والسن وأرقام التليفون والحالة الاجتماعية والديانة وأرقام بطاقات الرقم القومي وجواز السفر والبطاقات الائتمانية ونوع الجنس والصورة والفيديو والمراسلات والبصمة الوراثية من البيانات الشخصية التي يحميها القانون لتعلقها بالحق في الخصوصية.

أ. الاسم: يعتبر وسيلة من الوسائل الهامة التي يتميز بها الانسان غيرها من باقي افراد المجتمع([1]) وبالتالي فهي محل لحماية القانون ويعتبر من البيانات الشخصية. وينقسم الأسم إلى ثلاث أنواع هما:

النوع الأول. الاسم الاصلي: وهو الاسم الرسمي الذي يتم ذكره في شهادة الميلاد وبطاقة الهوية([2]) أي الاسم الذي يستخدم في المعاملات الرسمية.

([1]) – د. وفاء حلمي ابو جميل ، محاضرات في نظرية الحق ، ٢٠٠٧ ، بدون دار نشر ، الزقازيق ، مصر ، ص ٦٨.

([2]) – د. سهير منتصر ، النظرية العامة للحق ، بدون دار نشر ، ٢٠٠٦ ، الزقازيق ، مصر ، ص ٦٦ وما بعدها.

النوع الثاني. اسم الشهرة: وهو اسم يختلف عن الاسم الاصلي فلا يرد ذكره في شهادة الميلاد أو بطاقة الهوية فهو الاسم الذي يشتهر به الانسان بين الناس.

النوع الثالث. الاسم المستعار: وهو اسم اضافي يتخذه الانسان لنفسة بالإضافة إلى الاسم الأصلي، وذلك بسبب ممارسة نشاط أو مهني معينة مثل الممثل واللاعب الرياضي، وغالبا ما يكون الهدف من الاسم المستعار هو الشهرة وإخفاء الشخصية الحقيقية للإنسان(١). وذلك على عكس اللقب فهو أسم الأسرة التي ينتمي إليها الشخص وهو اسم أصلي(٢). ومما سبق نستطيع القول بأن اسم الشخص ولقبه يعتبر من البيانات الشخصية التي تخضع للحماية القانونية.

ب. البصمة الوراثية:

تعتبر البصمة الوراثية من البيانات الشخصية التي تعبر عن كيان الانسان الخارجي حيث أن البصمة الوراثية لكل إنسان تحوي كل صفاته الشخصية التي تميزه عن غيره وتوضح نسبه وعائلته، والأمراض الوراثية فيها وأسراره الطبية الدفينة مما يمثل الانتهاك لها انتهاك لحق الانسان في خصوصية البيانات الشخصية. فالبصمة الوراثية أحد أهم الوسائل التي تستخدم للتعرف على الأشخاص، حيث يتم التعرف على الشخص بتحليل بصمته الوراثية عن طريق عدة أشياء منها اللعاب، الشعر، بضع قطرات من العرق، السائل المنوي، حيث أن كل ما يلمسه الفرد مهما كان بسيط، يترك أثرا يمكن من خلاله التعرف على بصمته الوراثية وتحديد هويته. لذلك وجب على المشرع أن يتدخل ويحمي

---

(١) – د. سهير منتصر ، المرجع السابق ، ص ٦٧.

(٢) – Joëlle BEDEREDE, Données personnelles dans L'entreprise : quelles précautions faut – il prendre aujourd'hui, art disponible sur www.entreprise-et-droit.com.

حق الانسان في خصوصية هذه البيانات الشخصية سواء كانت في الصورة التقليدية أو في صورة بيانات تم معالجتها الكترونيا.

وهكذا فقد اعتبرت اللجنة القومية للمعلوماتية والحريات في فرنسا CNIL(١) بصمة الانسان من البيانات الشخصية أيا كانت صورة هذه البصمة سواء كانت بصمات الاصبع أو بصمة محيط اليد أو بصمة العين، أو غيرها من الصور الأخرى. وهي صورة من البصمات أصبح من الممكن تجميعها ومعالجتها إلكترونيا، وبالتالي تكون محل للحماية القانونية للبيانات الشخصية التي يتم معالجتها إلكترونياً.

وتأسيسا على ذلك فقد نص المشرع الفرنسي على حماية الخصائص الوراثية للشخص باعتبارها من البيانات الشخصية الهامة في المادة ٢٢٦ – ٢٥ من قانون العقوبات(٢) على أنه لا يجوز دراسة الخصائص الوراثية للشخص لأغراض غير البحث الطبي أو العلمي دون الحصول أولاً على موافقته وثانيا الالتزام بالشروط المنصوص عليها في المادة ١٦-١٠ من القانون المدني، ويعاقب الشخص في حالة عدم الالتزام بذلك بالحبس لمدة لا تزيد عن سنة واحدة وبالغرامة المالية التي تبلغ مقدارها ١٥.٠٠٠ ألف يورو.

---

(١) – CNIL, Délibération n°٠٠ – ٠١٥ du ٢١ mars ٢٠٠٠ portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège jean Rostand de Nice, destiné à gérer l'accès à la cantine scolaire par la reconnaissance des empreintes digitales.

(٢) – Code de droit pénal, article ٢٢٦ –٢٥, Modifié par Loi n°٢٠٠٤ – ٨٠٠ du ٦ aout ٢٠٠٤.

وتأكيداً على ذلك التوجه فقد أصدرت المحكمة الدستورية الكويتية في ٥ أكتوبر ٢٠١٧، حكمًا بعدم دستورية قانون البصمة الوراثية الكويتي(١)، وهو قانون صدر في شهر أغسطس عام ٢٠١٥ وأثار جدلًا واسعًا حول دستوريته بعد أن أقره مجلس الأمة الكويتي. والقانون المذكور يلزم وزارة الداخلية بإنشاء قاعدة بيانات تخصص لحفظ البصمات الوراثية الناتجة عن العينات الحيوية التي تؤخذ من الأشخاص الخاضعين للقانون. ويخضع لهذا القانون كما بينت المادة ١١ منه جميع المواطنين والمقيمين والزائرين وكل من دخل الأراضي الكويتية. ويلزم القانون الأشخاص الخاضعين له بإعطاء العينة اللازمة للفحص متى طلب منهم ذلك، ولا يجوز لهم الامتناع أو الرفض وإلا تعرضوا للحبس مدة لا تزيد على سنة وبغرامة لا تزيد على عشرة آلاف دينار أو إحدى هاتين العقوبتين.

واستخلاصا لما سبق فان المحكمة الدستورية الكويتية بنت حكمها على أساس انتهاك مواد هذا القانون للحرية الشخصية للإنسان أي الحق في الخصوصية باعتبار أن البصمة الوراثية لكل إنسان تحوي كل صفاته الشخصية التي تميزه عن غيره وتوضح نسبه وعائلته، والأمراض الوراثية فيها وأسراره الطبية الدفينة. وقد وصفت المحكمة ذلك بأنه يمثل انتهاكًا صارخًا للحرية الشخصية التي حرص الدستور على صونها. كما قالت المحكمة – أن أطلق التحليل دون أن يقصره على إعطاء الحد الأدنى الضروري من المعلومات والذي يكفي لتحقيق الغاية التي صدر من أجلها القانون. ودون أن يسبغ الحماية الواجبة على العينات ذاتها ودون أن يبين مآلها بعد الوفاة، كما جاءت النصوص عامة تطبق أحكامها على جميع المواطنين والمقيمين والزائرين وكل من دخل الأراضي الكويتية.

(١) – حكم المحكمة الدستورية العليا الكويتية ، الصادر في ٥ أكتوبر ٢٠١٧، سجل المحكمة الدستورية برقم ٦ و٩ لسنة ٢٠١٦ ، طعن مباشر دستوري ، دولة الكويت ، ٢٠١٧.

وهكذا فلم ترى المحكمة الدستورية العليا الكويتية حجة لمن يذهب إلى أن القانون عند تطبيقه يسهم في الحفاظ على الأمن والمساعدة في كشف الجرائم وتحديد ذاتية مرتكبيها، والتعرف على هوية الجثث المجهولة، مبينة بأن ممارسة الدولة لحقها في حماية الأمن العام يحده حق الفرد الدستوري في كفالة حريته الشخصية. وتتمثل الفائدة هنا في تأكيد المحكمة على أن عدم دستورية المواد الجوهرية في قانون معين يؤدي إلى سقوط القانون بأكمله إن كانت المواد الأخرى غير الجوهرية مرتبطة بها ارتباطَ لزومٍ لا يقبل التجزئة.

أما بالنسبة لموقف المشرع الانجليزي فقد نص في قانون العدالة الجنائية الانجليزي الصادر في ٢٠٠٣ على وجوب أخذ عينة الحمض النووي من الذين يتم القبض عليهم بأي تهم مختلفة وكانت نتيجة ذلك في احصائية عام ٢٠٠٧ أن ثلاثة أربع من أخضعوا لهذا كانوا من السود، مما طرح الكثير من الاشكاليات الاجتماعية داخل المجتمع البريطاني، ثم كانت احصائية أخرى صدرت في عام ٢٠١١ مفاداها أن قرابة مليون شخص كانوا قد تم أخذ عينات منهم وثبت براءتهم، نتيجة لذلك وحماية للحق في خصوصية البيانات الشخصية تم التخلص من ٦ مليون عينة من بنك DNA البريطاني، وذلك في ضوء قانون حرية المعلومات البريطاني الصادر عام ٢٠٠٠ الذي أوجب التوازن بين الحق في حرية المعلومات حماية الحق في خصوصية البيانات الشخصية.

أما بالنسبة لموقف المشرع الأوربي فيعرف البيانات الشخصية الجينية في اللائحة العامة الجديدة لحماية البيانات الشخصية(١) على أنها بيانات شخصية تتعلق

(١) – المادة ٣٤ من اللائحة العامة الأوربية لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ ، والتي سوف تدخل إلى حيز التنفيذ في ٢٥ مايو ٢٠١٨.

بالخصائص الوراثية الموروثة أو المكتسبة لشخص طبيعي تنتج عن تحليل عينة بيولوجية من الشخص الطبيعي المعني، ولاسيما الكروموسومات والحمض النووي ، أو من تحليل عنصر آخر مما يتيح الحصول على معلومات مكافئة.

ت. الصورة:

تعتبر صورة الانسان هي محاكاة للجسم أو جزء منه، فلا يجوز نشر صورة أي شخص دون إذن منه وإلا اعتبر ذلك إخلال بحق الانسان في الخصوصية(١). لذلك نص المشرع المصري في المادة ٣٠٩ مكرراً من قانون العقوبات على "تجريم تصوير شخص في مكان خاص سواء أكان ذلك بالالتقاط أم بالنقل بجهاز من الأجهزة أياً كان نوعه". ويلاحظ أن المشرع المصري يجرم تصوير المواطنين في حياتهم الخاصة بدون علمهم أو إذن منهم، إذ أن صورة الشخص امتداد لجسمه، فهي وإن كانت لا تعبر عن حديث أو فكرة أو رأي لكنها تشير إلى شخصية صاحبها في الوضع الذي يمارس فيه حياته الخاصة ومن ثم تأخذ حكم الإنسان نفسه من حيث المساس بحياته الخاصة .

ومن هذا المنطلق فقد نص المشرع المصري في قانون العقوبات المادة رقم ٣٠٩ مكرر على أن "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني على ... (ب) التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص". وعليه لا يقتصر التجريم على الشخص القائم بالتقاط الصورة فقط وفقا للنص السابق، ولكن التجريم يمتد ليشمل كلا من سهل أو أذاع

(١) – انظر.، د. محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٩٤ ، ص ١٠٥٥.، د. حسام الدين كامل الأهواني ، الحق في احترام الحياة الخاصة ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، بدون تاريخ نشر ، ص ٧٦ وما بعدها.

أو شارك في نشر الصورة .فقد نصت المادة رقم ٣٠٩ مكرر (أ) على أن يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلا أو مستندا متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن.

ويتضح مما سبق أن المشرع المصري لم ينص على أجهزة محددة بنوعها تستخدم في التقاط أو نقل صور الأشخاص الخاصة، وبالتالي يمتد التجريم إذا ما ارتكبت الجريمة عن طريق استخدام جهاز من الأجهزة أياً كان نوعه مثل التقاط الصور من خلال برنامج معين يتم اختراق الاجهزة الالكترونية من خلاله أو اختراق الملفات الشخصية للبريد الالكتروني أو نشر صورة لأحد الأشخاص او التهديد بنشرها على شبكة الانترنت.

إلا أنه ومع صدور قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ فقد تم النص في المادة ٢٥ منه على "أن يعاقب بالحبس لمدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائة ألف جنية، أو بإحدى هاتين العقوبتين كل من ... نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة". وبالتالي أصبح هناك نص واضح وصريح يحمي الحق في خصوصية البيانات الشخصية المتعلقة بالصورة المعالجة إلكترونياً.

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ٣٣٣ من قانون العقوبات المعدلة بالقانون رقم ٤ لسنة ٢٠١٧ على "أن يعاقب بالحبس مدة لا تجاوز سنتين(١)، وبالغرامة التي لا تزيد على (١٠٠٠٠٠) عشرة آلاف ريال، أو بإحدى هاتين العقوبتين ، كل من اعتدى على حرمة الحياة الخاصة للأفراد، بغير رضائهم في غير الأحوال المصرح بها قانوناً، وذلك بارتكاب أحد الأفعال الآتية : ... ٤- التقط أو نقل صوراً أو مقاطع فيديو لفرد أو أفراد في مكان خاص ، عن طريق جهاز أياً كان نوعه. ويعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من:

١- التقط أو نقل صوراً أو مقاطع فيديو لفرد أو أفراد في مكان عام، عن طريق جهاز أياً كان نوعه، بقصد استخدامها في الإساءة أو التشهير.

٢- التقط أو نقل صوراً أو مقاطع فيديو للمصابين أو المتوفين في الحوادث، عن طريق جهاز أياً كان نوعه، في غير الأحوال المصرح بها قانوناً".

أما بالنسبة لموقف المشرع الفرنسي فنجد أنه قد عالج مسألة الحماية الجنائية للحق في الصورة في المادة ٣٦٨ من قانون العقوبات الفرنسي القديم وأبقي عليها دون تعديل في المادة ٢٢٦ – ١ من قانون العقوبات الفرنسي ويشترط لتطبيق هذه المادة أن تكون الصورة قد التقطت في مكان خاص(٢) وأن يتم ذلك بدون رضائه، حيث ينص على تجريم التقاط أو تسجيل أو نقل صورة شخص في مكان خاص دون رضاء منه، وعلى أن يعاقب بالحبس لمدة لا تزيد عن سنة واحدة وبالغرامة المالية التي تبلغ مقدارها ٤٥.٠٠٠ الف يورو. وتنص المادة ٢٢٦- ٢ من قانون العقوبات الفرنسي كل من قام

---

(١) – المادة ٣٣٣ من قانون العقوبات القطري رقم ١١ لسنة ٢٠٠٤ ، المعدلة بالقانون رقم ٤ لسنة ٢٠١٧ ، الصادر في ٩ مارس ٢٠١٧.

(٢) – Michèle – Laure RASST, Droit pénal spécial, éd., Dalloz, Paris, ١٩٩٧, p. ٣٦٩.

بأي وسيلة بارتكاب فعل من الأفعال المتعلقة بجريمة حفظ أو إعلان أو استعمال تسجيل أو مستند تم الحصول عليه بأحد الأفعال المشار إليها في المادة السابقة، يعاقب بنفس العقوبة المنصوص عليها بالمادة السابقة. وكذلك جرم المشرع الفرنسي كل فعل من شأنه نشر مونتاج أو تركيب لصوت أو صورة لشخص بدون رضاء منه وفقا لنص المادة ٢٢٦ – ٨ من قانون العقوبات الفرنسي.

وتطبيقا على ذلك فقد قضت محكمة السين الفرنسية(١) بأن الحق في الصورة هو الحق لكل شخص على صورته وملامحه ورسمه يخوله أن يحظر على الغير نشر صورته وإلا كان ذلك خطأ يستوجب التعويض(٢)، وفي حكم أخر جرت عبارات أسبابه بأن للشخص الذي التقطت صورته، له على هذه الصورة حق ملكية لا يسمح لغيره أن يستخدمها دون موافقته. ومن هنا أمكن تشبيه الحق في الصورة بحق الملكية خاصة من الواجهة المادية. وعلاوة على ذلك فإن اللجنة القومية للمعلوماتية والحريات في فرنسا CNIL قد اعتبرت صورة الشخص الطبيعي سواء كانت صورة ثابتة أو صورة متحركة من البيانات الشخصية الخاصة التي تخضع لحماية القانون، وبالتالي تكون محل للحماية الجنائية لخصوصية البيانات الشخصية التي يتم معالجتها إلكترونياً.

أما في الولايات المتحدة الأمريكية فقد فتح مكتب التحقيقات الفيدرالي تحقيق حول إدخالات غير مشروعة من خلال استخدام الصور من رخص القيادة وجوازات السفر

---

(١) – محكمة السين الابتدائية الفرنسية ، حكم بتاريخ ١٠ فبراير ١٩٠٥ ، باريس.، د. نعيم عطية ، حرمة الحياة الخاصة في القانونين المصري والفرنسي ، مجلة العلوم الإدارية ، السنة ٢٣ ، العدد الأول ، القاهرة ، ١٩٨٠ ، ص ٧٧.، د. سعيد جبر ، الحق في الصورة ، دار النهضة العربية ، القاهرة ، ١٩٨٦ ، ص ١٠٧.

(٢) – Cass. Civ, ٥ Novembre ١٩٩٦, N°٩٤ – ١٤٧٩٨, Publié au Bulletin, Paris, p. ٢٦٥.

في تكنولوجيا التعرف على الوجه، كذلك التوسع في تقنية التعرف على الوجوه من خلال كاميرات المراقبة عن طريق مسح وجوه الناس الذين يسيرون في الطرقات. وقد اكتشف أن مكتب التحقيقات الفيدرالي الأمريكي قد أطلق لأول مرة قاعدة بيانات البيومترية المتقدمة في عام ٢٠١٠، والتي تمكن من التعرف على الأشخاص من خلال التعرف على الوجه، دون أن يقوم المكتب بإبلاغ الجمهور بهذه القدرات الجديدة ، كذلك لم ينشر تقييماً لأثر هذه الإجراءات على الحق في الخصوصية([1])، مما شكل انتهاك واضح للحق في خصوصية الصورة وعدم استخدامها أو معالجتها آليا بدون تصريح.

وعليه فعند إطلاق أبل لهاتف إيفون x الجديد في نهاية عام ٢٠١٧ كان هناك العديد من التخوفات من استخدام ميزة التعرف على ملامح الوجه بشكل سيء من بعض الجهات، وبالتالي التعرض للحق في خصوصية المستخدمين، حيث يمكن لمطوري هواتف إيفون من الوصول والاحتفاظ بهذه البيانات الشخصية الخاصة بالتعرف على ملامح الوجه وتخزينها على خوادمهم الخاصة مما يمكنهم من الوصول إلى بيانات إطار وجه المستخدم، وقراءة ٥٢ حركة فريدة من نوعها من الحركات الدقيقة للجفن والفم والوجه وغيرها من الميزات الأخرى، وهذه المعلومات يمكن استخدامها في العديد من الأمور التي تمثل انتهاك للحق في خصوصية البيانات الشخصية لمستخدمي هواتف إيفون، خاصة إذا ما وقعت في أيدى المسوقين، أو المتسللين أو الهاكرز([2]).

([1]) – أوليفيا سولون ، مقال تحت عنوان قاعدن بيانات التعرف على الوجه المستخدمة من قبل مكتب التحقيقات الفيدرالية خارج نطاق السيطرة ، جريدة The Guardian ، سان فرانسيسكو ، في ٢٧ مارس ٢٠١٧.

([2]) – لذلك قام أحد المطورين بوضع برنامج يسمى ماسوريكيت ، والذي يتيح لمستخدمي هواتف أيفون من روية البيانات الشخصية التي تجعلها شركة آبل متاحة للمطورين للتطبيقات والبرامج الإلكترونية.

فمما لا شك فيه أن تقنية التعرف على الوجه FRT قد أدت إلى التعرف على الهوية والتحقق من صحتها، حيث انها تجمع بين النظم الأخرى للتحقق من الهوية من خلال السمات البيولوجية، والتي تحاول ربط الهوية بسمات مميزة من الجسد لدى كل فرد ، وتستخدم هذه التقنية في أنظمة المراقبة المرئية(١). وبالتالي أصبح تقنية تحتاج إلى العمل على إيجاد آلية قانونية تضمن عدم اساءة استخدامها في الانتهاك للحق الفرد في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً المتعلقة في الحق في الصورة ولكن في ضوء المتغيرات التكنولوجية الحديثة.

ج. الصوت:

تعتبر اللجنة القومية للمعلوماتية والحريات في فرنسا CNIL صوت الشخص من البيانات الشخصية الخاصة التي تخضع لحماية القانون. وذلك استناداً إلى أن التكنولوجيا الرقمية الحديثة قد سمحت بمعالجة الصوت والصورة ووضعهم على دعامة واحدة بجانب النص ، مما يؤدي إلى اعتبارهما من البيانات الشخصية التي يمكن معالجتها إلكترونياً بطريقة منفصلة(٢). لذلك يعتبر الاخلال بهما إخلالاً بحق الانسان في خصوصية بياناته الشخصية.

---

(١) – انظر : إنتروما إل دي ، ونيسينبام إتش إف ، تقنية التعرف على الوجه ، دراسة استقصائية حول مائل السياسة والتنفيذ ، SSRN eLibray ، ٢٠٠٩. انظر كذلك ، توبي مندل ، واندرو بوديفات ، وبن واجنر ، وديسكي هوتن ، ونتاليا توريس ، دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير ، سلسلة اليونسكو بشأن حرية الإنترنت ، منظمة الأمم المتحدة للتربية والعلم والثقافة ، منشورات اليونسكو ، باريس ، ٢٠١٢ ، ص ٣٧ وما بعدها.

(٢) – CNIL, Délibération ٩٦ – ٠٠٩ du ٢٧ février ١٩٩٦, Délibération portent adoption du rapport intitulé, Les informations personnelles issues de la voix et de l'image et la protection de la vie privée et des libertés fondamentales, disponible sur., www.legifrqnce:gouv.fr.

وتأسيسا على ذلك فقد صدر التوجيه الاوربي في ٢٤ أكتوبر ١٩٩٥ على اعتبار صوت الانسان وصورته من البيانات الشخصية التي يمكن معالجتها(١) ، وبالتالي تخضع للحماية القانون لحق الانسان في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً ، وكذلك نصت اللائحة الأوربية الجديدة التي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨. وبناء على ذلك فقد نص المشرع الفرنسي على تجريم نشر تركيب أو أي مونتاج لصوت أو صورة شخص دون رضاءه في المادة ٣٧٠ من قانون العقوبات الفرنسي القديم، وكذلك جرم أخذ الصور بغير إذن بالقانون الصادر في ١٧ يوليو ١٩٧٠، بحيث جرم أخذ صور فوتوغرافية أو أفلام أو تسجيل خلسة دون معرفة الشخص الذي تم أخذ صورته أو سجل صوته أو أخذ فيلم له، ونص على ذلك في المادة ٣٦٨. وقد أبقي قانون العقوبات الفرنسي الجديد عليها دون تعديل في المادة ٢٢٦ – ٨ ، ويقصد بالمونتاج المعاقب عليه وفقا لنص المادة بانها كل تدخل في الصوت أو الصورة ، وكل حيلة تهدف إعطاء الجمهور فكرة كاذبة أو محرفة لما تم أو قيل أو شوهد أو سجل أو تم سماعه في الواقع(٢) أي على خلاف الحقيقة.

بالإضافة إلى فقد نصت المادة ٢٢٦ – ١ من قانون العقوبات الفرنسي على تجريم التقاط أو تسجيل أو نقل الكلام الصادر بصورة خاصة أو سرية دون موافقة المجني عليه، وايضاً المادة ٢٢٦ – ٢ تجريم الأفعال المتعلقة بجريمة حفظ أو إعلان أو استعمال تسجيل أو مستند تم الحصول عليه بأحد الأفعال المشار عليها في المادة ٢٢٦

---

(١) – Directive Européenne n° ٩٥ – ٤٦ du ٢٤ octobre ١٩٩٥ du parlement européen et du conseil n° ٩٥٤٦ relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données, JOUE du ٢٣ novembre ١٩٩٥, p. ٣١.

(٢) – Roger MERLE et André VITU, Trait de droit criminel, droit pénal spécial, éd., Cujas, Paris, tome ١١ , n°٢٠٣١.

– ١ من قانون العقوبات. وتكون العقوبة في هذه الحالات هي الحبس لمدة لا تزيد عن سنة واحدة وبالغرامة المالية التي تبلغ مقدراها ٤٥.٠٠٠ ألف يورو. ويفهم من ذلك أن المشرع الفرنسي يرى أن الحق في الصورة أو الصوت يعد أحد مظاهر الحق في الخصوصية ، كما أن الاعتداء على صورة أو صوت الفرد يعد اعتداء على الحق في الخصوصية ، فصورة وصوت الأنسان مظهراً من مظاهر خصوصيته شأنها شأن حياته العاطفية وحياته العائلية بل تعد أكثر المظاهر قدسية في الخصوصية(١). وبالتالي يعتبر الصوت والصورة من البيانات الشخصية محل للحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

أما بالنسبة لموقف المشرع المصري فقد نص في قانون العقوبات المادة ٣٠٩ مكرراً على الحماية القانونية للصوت من خلال حماية سجل الاتصالات الخاصة فنص على معاقبة من استرق السمع أو سجل أو نقل محادثات عن طريق جهاز من الأجهزة أياً كان نوعه، لمحادثات جرت في مكان خاص أو عن طريق التليفون. ويلاحظ من ذلك أن المشرع المصري قد ساوي في حماية سرية المحادثات سواء كانت في مكان خاص أو باستخدام التليفون وذلك لحماية الحق في الخصوصية(٢).

وتطبيقاً على ذلك فقد ذهبت محكمة النقض المصرية إلى القول بأنه(٣) "لما كان تحقيق الحرية لإنسانية المصري هدفاً أساسياً تضمنته وثيقة إعلان دستور جمهورية مصر العربية، وكانت مراقبة وتسجيل المحادثات السلكية واللاسلكية والأحاديث الشخصية إجراء مرذولا يعتبر انتهاكا لحرمة الحياة الخاصة انتقاصا من الأصل في

(١) – د. حسام الدين الأهواني ، المرجع السابق ، ص ٧٨.
(٢) – د. طارق سرور ، في جرائم النشر والأعلام ، المرجع السابق ، ص ٥٨٨ ، ٦٠٣.
(٣) – نقض جنائي مصري ، الطعن رقم ٦٨٥٢ لسنة ٥٩ ، جلسة ١٤ يناير ١٩٩٦ ، س ٤٧ ، ع ١ ، ق ٩ ، ص ٧٢.

الحرية الشخصية التي سجلها الدستور باعتبارها حقا طبيعيا للإنسان لا يجوز الإخلال به أو تقييده بالمخالفة لأحكامه، وكان الدستور إذ كفل في صلبه حرمة الحياة الخاصة بما تشتمله من حرمة الحديث ضد تسجيله قد قرنها بضمانات إجرائية توازن بين حق الفرد في الحرية من ناحية وحق الجماعة في الدفاع عن مصالحها الأساسية من ناحية أخرى، وليوفر لها الحماية من جوانبها العملية وليس من معطياتها النظرية، بما نص عليه في المادة ٤٥ منه أن (لحياة المواطنين الخاصة حرمة يحميها القانون وللمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة ووفقا لأحكام القانون) وإنفاذا للضمانات الدستورية فإن قانون الإجراءات الجنائية في الفقرتين الثانية والثالثة من المادة ٢٠٦ منه المستبدلة بالقانون رقم ٣٧ لسنة ١٩٧٢ بتعديل بعض النصوص المتعلقة بضمان حريات المواطنين في القوانين القائمة لم يجز هذا الإجراء إلا إذا كانت هناك فائدة في ظهور الحقيقة في جناية أو جنحة معاقبا عليها بالحبس لمدة تزيد على ثلاثة أشهر وأن يكون بناء على أمر مسبب من القاضي الجزائي ولمدة محددة، ومفاد ذلك ألا يسمح بهذا الإجراء لمجرد البلاغ أو الظنون والشكوك أو البحث عن الأدلة وإنما عند توافر أدلة جادة تقتضى تدعيمها بنتائج هذا الإجراء، وليحول المشرع بهذه الضمانات المتكاملة دون اتخاذ هذا الإجراء لدوافع وهمية أو إساءة استعماله فلا يكون إلا لضرورة تفرضها فاعلية العدالة الجنائية وما تقتضيه من تأكيد الأدلة المتوافرة بضبط ما يفيد في كشف الحقيقة في الجرائم، وعلى تقدير أن القضاء إذ يقدر توافر هذه الأدلة وتلك الضرورة هو الحارس الطبيعي للحريات والحرمات في مواجهة كل صور التحكم والتسلط والتحامل والعاصم لها دون أي تعد عليها أو عبث بها أو جموح ينال منها".

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

ونستخلص ما سبق أن موقف المشرع المصري محل انتقاد فيما يتعلق بعدم مسايرة التطور التكنولوجي، حيث يجب النص على توافر الحماية القانونية للمحادثات الخاصة أيا كانت نوع الدعامة التي تستخدم، خاصة في ظل التطور المتسارع في مجال تكنولوجية المعلومات مثال وسائل التواصل الاجتماعي الإلكترونية الحديثة من فيسبوك أو توتير أو ماسنجر أو واتساب أو فيبر أو ... الخ. وعليه فقد تغيير هذا الموقف للمشرع المصري مع اصدار المشرع قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ والذي نص في المادة ٢٥ منه على حماية حرمة الحياة الخاصة للبيانات المعالجة إلكترونياً، إلا أننا نري أن ذلك غير كافة لإسباغ الحماية الشاملة لخصوصية البيانات الشخصية المعالجة إلكترونيا، وانما يجب إصدار تشريع خاص لحماية خصوصية البيانات الشخصية. وبناء على ذلك فقد أصدر المشرع المصري قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، ونص فيه على حماية البيانات الشخصية من الصوت أو الصورة من قبل كل حائز أو متحكم أو معالج جمع أو عالج أو أفشى أو أتاح أو تداول هذه البيانات الشخصية المعالجة إلكترونيا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونا أو بدون موافقة الشخص المعني بالبيانات بالغرامة التي لا تقل عن مائة ألف جنية ولا تجاوز مليون جنية. وتشدد العقوبة إذا ارتكبت ذلك مقابل الحصول على منفعة مادية، أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر، لتصبح الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائتي ألف جنية ولا تجاز مليوني جنية، أو بإحدى هاتين العقوبتين([1]).

([1]) – المادة ٣٦ من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية ١٥ يوليه ٢٠٢٠، ص ٢٧.

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ٣٣٣ من قانون العقوبات المعدل بالقانون ٤ لسنة ٢٠١٧ على أن "يعاقب بالحبس مدة لا تجاوز سنتين(١)، وبالغرامة المالية التي لا تزيد على (١٠.٠٠٠) عشرة آلاف ريال، أو بإحدى هاتين العقوبتين، كل من اعتدى على حرمة الحياة الخاصة للأفراد، بغير رضائهم في غير الأحوال المصرح بها قانوناً ، وذلك بارتكاب أحد الأفعال الآتية : ... ٣. سجل أو نقل محادثات جرت في مكان خاص، عن طريق جهاز أياً كان نوعه".

د. الارقام الشخصية:

مما لا شك فيه أن الارقام الشخصية تعتبر من البيانات الشخصية التي تخضع للحماية القانونية، والمقصود بها هي كل رقم يتم منحه للشخص الطبيعي بحيث يكون خاصا به هو فقط ومميزاً له ومحدداً لهويته. مثال على ذلك رقم تحقيق الهوية الشخصية (الرقم القومي)، وهو رقم خاص بكل شخص على مستوى الدولة، وكذلك رقم جواز السفر، والرقم التأمين وهو رقم التأمين الاجتماعي الخاص بالشخص الطبيعي، كذلك رقم التأمين الصحي، وأي رقم آخر ينفرد به الشخص الطبيعي كرقم الاشتراك في مكتبة أو مجلة الكترونية أو وسيلة مواصلات أو رقم البطاقة الائتمانية أو رقم الحساب البنكي وهو عندما يقوم الشخص بفتح حساب في أحد البنوك ، فإن هذا الحساب يكون له رقم خاص، فرقم الحساب البنكي أحد البيانات الشخصية(٢). ويشترط في جميع هذه الارقام

---

(١) – المادة ٣٣٣ من قانون العقوبات القطري رقم ١١ لسنة ٢٠٠٤ ، المعدلة بالقانون رقم ٤ لسنة ٢٠١٧ ، الصادر في ٩ مارس ٢٠١٧.

(٢) – Sophie PENA PORTA, Les données personnelles et leur traitement, art disponible sur., http://www.crid.be/pdf/crid/٤٧١٠.pdf. Paris, ٢٠٠٥.

أن يكون الرقم خاصاً بالشخص فقط وغير متكرر(١) ، حتي يكمن اعتبار الرقم محل للحماية القانونية باعتباره بيان من البيانات الشخصية والتي يجوز معالجتها الكترونياً.

وبناء على ذلك فقد قامت السلطات الفيدرالية الأمريكية في مدينة ديترويت بالقبض على ١١ شخص بتهمة سرقة واستخدام بيانات شخصية للمشتركين في شركة بلو كروس بلو شيلد للتأمين الصحي حيث تبين من بيان الاتهام بأن أنجيلا باتون وهي موظفة سابقة في الشركة وزعتها على عدد من المشبوهين الذي قاموا بدورهم بالاستفادة من تلك المعلومات للحصول على البطاقة ائتمان وشراء بضائع بأسماء آخرين.

وتطبيقا على ذلك فقد قضت محكمة النقض الفرنسية بأن التحقيقات والتحريات المتعلقة بالحالة المالية للشخص تمثل انتهاكاً للحق في الخصوصية ، خاصة إذا ركز البحث في البيانات والمعلومات المالية على معرفة البيانات الشخصية مثل أسلوب حياة الشخص أو عنوانه أو ظروفه العائلية الخاصة بالنواحي العاطفية(٢). وبذلك يتضح أن محكمة النقض الفرنسية تشترط لاعتبار البيانات والمعلومات المتعلقة بالحالة المالية من البيانات والمعلومات الشخصية أن تكون هدف هذه المعلومات المتعلقة بالحالة المالية البحث عن معلومات وبيانات شخصية.

---

(١) – Nathalie MALLET – POUJOL, Protection de la vie privée et des données à caractère personnel, étude disponible sur sité. www.educent.education.fr. Paris, ٢٠٠٧, p. ٣٢

(٢) – Cass. Civ. ٣٠ mai ٢٠٠٠, n°٩٨ – ١٤.٦١٠, Juris, ٢٠٠٠, Bull. Civ, ٢٠٠٠, RTD. Civ, ٢٠٠٠, P. ٨٠١.

٢. البيانات الشخصية المعالجة إلكترونياً المتعلقة بالمراقبة البصرية:

مما لا شك فيه أن تعتبر من البيانات الشخصية التي تخضع للحماية القانونية البيانات الشخصية المتعلقة بالمراقبة البصرية، لذلك فقد نص المشرع التونسي في المواد من ٦٩ إلى ٧٤ من قانون حماية البيانات الشخصية على أنه "يشترط لمعالجة البيانات الشخصية لأغراض المراقبة البصرية ما يلي:

A. أن يخضع استعمال وسائل المراقبة البصرية إلى ترخيص مسبّق من الهيئة الوطنية لحماية المعطيات الشخصية. وعلى الهيئة أن تبت في طلب الترخيص في أجل أقصاه شهر من تاريخ تقديمه.

B. لا يمكن استعمال وسائل المراقبة المذكورة بالفصل المتقدم إلا بالأماكن التالية

i. الفضاءات المفتوحة للعموم ومداخلها.

ii. الماوي ووسائل النقل المستعملة من العموم ومحطاتها وموانيها البحرية والجوية.

iii. أماكن العمل الجماعية.

A. لا يمكن استعمال وسائل المراقبة البصرية في الأماكن المنصوص عليها بالفصل المتقدم إلا إذا كانت ضرورية لضمان سلامة الأشخاص والوقاية من الحوادث وحماية الممتلكات أو لتنظيم حركة الدخول إلى الفضاءات والخروج منها. وفي كل الحالات، لا يجوز أن تكون التسجيلات البصرية مرفوق بتسجيلات صوتية.

B. يجب إعلام العموم بطريقة واضحة ومستمرة بوجود وسائل مراقبة بصرية.

C. لا تجوز إحالة التسجيلات البصرية الواقع جمعها لأغراض المراقبة إلا في الحالات التالية :

i. إذا وافق المعني بالأمر أو ورثته أو وليه. وإذا كان المعني بالأمر طفلا تطبق أحكام الفصل ٢٨ من هذا القانون.

ii. إذا كانت ضرورية لتنفيذ المهام الموكلة إلى السلطة العمومية.

iii. إذا كانت ضرورية لغاية معاينة جريمة أو الكشف عنها أو تتبع مرتكبها.

D. يجب إعدام التسجيلات البصرية إذا أصبحت غير ضرورية لتحقيق الغاية التي وضعت من أجلها أو إذا كانت مصلحة المعني بالأمر تقتضي عدم إبقائها إلا إذا كانت ضرورية لإجراء الأبحاث والتحريات في التبعات الجزائية".

٣. البيانات الشخصية المعالجة إلكترونياً المتعلقة بالحالة الصحية:

تعتبر البيانات الشخصية المعالجة إلكترونياً المتعلقة بالحالة الصحة من البيانات التي تتعلق بالحق في الخصوصية والتي يحميها القانون، فتعد التقارير الطبية والعينات التحليلية التي تشمل معلومات حول حالة الشخص الصحية والعقلية والتشخيص المرضي وجرعات الأدوية والتقارير الدورية للأمراض المزمنة من البيانات الشخصية التي تتمتع بالحماية وفقا لحق في الخصوصية([1]).

ولذلك ينص المشرع الأوربي في اللائحة العامة لحماية البيانات رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨ على أنه تعتبر من البيانات الشخصية المتعلقة بالصحة كل موضوع بيان يكشف عن معلومات تتعلق بالحالة الصحية البدنية أو العقلية السابقة أو الحالية أو المستقبلية([2]). ويشمل كذلك المعلومات عن الشخص الطبيعي الذي تم جمعها أثناء التسجيل أو تقديم خدمات الرعاية الصحية على النحو المشار إلية في التوجيه الأوربي رقم ٢٤ لسنة ٢٠١١، بالإضافة إلى ذلك كل رقم أو رمز أو شيء معين يمكن من خلاله لشخص طبيعي تعريف الشخص بشكل فريد لأغراض صحية، وكذلك المعلومات المستمدة من اختبار أو فحص جزء من الجسم

([1]) – Latanya SWEENEY, Comments from Latanya Sweeney and the Data Privacy Lab, Ph.D., on Standards of privacy of individually identifiable health information, Carnegie Mellon University, ٢٠١١.

([2]) – انظر: المادة ٣٥ من اللائحة العامة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ بشأن حماية البيانات الشخصية والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨.

أو مادة جسدية، بما في ذلك البيانات الجينية والعينات البيولوجية، وأية معلومات، على سبيل المثال مرض أو عجز أو خطر مرض أو تاريخ طبي أو علاج سريري، أو حالة فسيولوجية أو طبية حيوية من موضوع البيانات مستقله عن مصدرة، على سبيل المثال من طبيب أو أخصائي صحي آخر، ومستشفى، جهاز طبي أو اختبار في المختبر التشخيصي.

وتطبيقا على ذلك حالة الإخلال بالحق في خصوصية البيانات الشخصية المتعلق بالحالة الصحية ما قام به الطبيب الخاص بالرئيس الفرنسي ميتران من تأليف كتاب عن مرض الرئيس الفرنسي الاسبق ميتران. وعلى الرغم من مصادرة الكتاب من الاسواق بناء على حكم قضائي إلا أن أحد مديري مقاهي الإنترنت قام برفع ونشر الكتاب على أحد المواقع الالكترونية(١)، مما شكل جريمة انتهاك لحق الرئيس الفرنسي الاسبق ميتران في خصوصية البيانات الشخصية الإلكترونية التي تتعلق بالحالة الصحية.

وعليه فقد تم ذلك التجريم وفقا لنص المادة ٨ من قانون حماية البيانات الشخصية الفرنسي رقم ٧ لسنة ١٩٧٨ المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤، التي تعتبر المعلومات المتعلقة بالحالة الصحية للإنسان من البيانات الشخصية التي تخضع بالحماية القانونية(٢). وعلى الرغم من أنه لم يكن هناك نص صريح في القانون الفرنسي

---

(١) – J. PARDEL et M. DANTI – JUAN, Le droit pénal, le droit pénal special, éd., Cujas, Paris, ٢٠١٤, N ٢٠٥ ets. راجع كذلك القضية رقم ٨٩/٧٣ لسنة ١٩٨٩ محكمة القاهرة ، القسم المدني ، قسم عابدين ، الحكم الصادر بتاريخ ٧ يونيه ١٩٨٩ في حق الممثلة شرين ضد جريدة الأهرام بسبب ما نشرته الجريدة بتاريخ ٣١ يناير ١٩٨٩ عن مرضها ونقلها للعلاج في باريس والتقاط صور لها رغم رفضها لذلك ، فاعتبر ذلك مساس بالحق في الخصوصية البيانات الشخصية المتعلقة بالحالة الصحية وكذلك الحق في الصورة.

(٢) – Art ٨ – ١, II est interdit de collecter ou de traiter des données à caractère personnel qui font apparaitre, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

لحماية البيانات الشخصية قبل تعديله يعتبر أي معلومات متعلقة بالحالة الصحية بيانات الشخصية، إلا أن اللجنة القومية للمعلوماتية والحريات في فرنسا CNIL قد اعتبرت البيانات المتعلقة بالحالة الصحية بيانات شخصية تخضع لحماية فالقانون في حق الانسان في الخصوصية([١]). وهذا دليل على أهمية اللجنة في المساعدة على حماية البيانات الشخصية والعمل على تعديل قانون حماية البيانات الشخصية الفرنسي بما يتلائم مع تطورات ومتغيرات العصر.

وبناء على ذلك فقد اعتبرت اللجنة القومية الفرنسية للمعلوماتية والحريات CNIL أن نتائج الاختبارات النفسية لأي شخص هي بيانات شخصية تخضع لحماية القانونية في ضوء حماية الحق في الخصوصية([٢])، فنتائج الاختبارات النفسية هي معلومات متعلقة بالحالة الصحية للإنسان، والجائب النفسي للإنسان هو جزء من صحته وبالتالي تدخل في نطاق الحماية القانونية.

ولكن وبناءً على التعديل الصادر في ٧ أغسطس ٢٠٠٤ بالقانون رقم ٨٠١ لسنة ٢٠٠٤ لقانون حماية البيانات الشخصية الفرنسي نصت المادة ٤٣ على تنطبق القواعد القانونية لحماية البيانات الشخصية على البيانات الصحية الشخصية، وبالتالي لا يجوز معالجة هذه البيانات إلا بعد الحصول على موافقة صريحة من الشخص المعني وبعد

---

religieuses ou l'appartenance syndicale des personnes; ou qui sont relatives à la santé ou à la vie sexuelle de celles – ci.

([١]) – CNIL, Délibération n°٩١ – ٣٣ du ٧ mai ١٩٩١ portant avis relative à la création d'un traitement automatisé d'informations nominatives concernant une application de gestion des dossiers des ressortissants étrangers en France, disponible sur sité, www.legifrance.gouv.fr.

([٢]) – CNIL, Délibération n°٨٥ – ٥٠ du ٢٢ oct. ١٩٨٥, disponible sur site, www.legifrance.gouv.fr.

اخطاره مباشرة أو عن طريق طبيب يعينه هو لهذا الغرض ، وكل ذلك وفقا لنص المادة ٧-١١-١١ من قانون الصحة العامة([1]).

إلا أن المشرع الفرنسي يستثني من الحماية القانونية للبيانات الشخصية المتعلقة بالحالة الصحية طائفة من البيانات يجوز جمعها والاحتفاظ بها في حالتين التاليين وهما:

الحالة الأولى. حالة متابعة المرضي طبيا، أي تلك الحالة التي يقوم فيها الأطباء بتدوين بيانات عن مرضاهم، سواء كان هذا التجميع يدوياً أو في نظام إلكترونياً.

الحالة الثانية. حالة البحث العلمي، حيث يجوز وفقا للضرورات العلمية أن تقوم مراكز البحث العلمي بتجميع والاحتفاظ ببيانات تتعلق بصحة الاشخاص في صورة أرقام وبيانات للاستخدام في مجال البحث العلمي.

([1]) – تنص المادة ٧-١١-١١ من قانون الصحة العامة الفرنسي والمعدلة بالقانون رقم ٤١ لسنة ٢٠١٦ الصادر في ٢٦ يناير ٢٠١٦ على أنه "لكل شخص الحق في الحصول على جميع المعلومات المتعلقة بصحته التي يحتفظ بها ، من قبل المهنيين والمؤسسات الصحية ، التي تكون رسمية أو كانت موضوع تبادل مكتوب بين المهنيين الصحيين ، ولاسيما نتائج الفحص ، تقارير التشاور ، التدخل ، الاستكشاف أو الاستشفاء ، البروتوكولات والوصفات العلاجية المنفذة ، أوراق المراقبة ، المراسلات بين المهنيين الصحيين ، باستثناء المعلومات التي تفيد بأن تم جمعها من أطراف ثالثة غير متدخلة في العلاج. فيما يتعلق بهذا الطرف الثالث يجوز له الوصول إلى هذه المعلومات مباشرة أو عن طريق طبيب يعينه ويحصل على الاتصالات بموجب شروط تحددها اللائحة في موعد أقصاه ثمانية أيام بعد طلبه وفي أقرب وقت ويعطي ثماني واربعون ساعة وتمتد الفترة إلى شهرين عندما تكون المعلومات الطبية قد مرة عليها أكثر من خمس سنوات أو عندما تكون متعلقة باختصاص لجنة رعاية الامراض النفسية. وفي حالة القاصر، يمارس حق الوصول الشخص أو الأشخاص الذين يتمتعون بسلطة أبوية".

أما بالنسبة لموقف المشرع التونسي فقد نص في المواد من ٦٢ إلى ٦٥ من قانون حماية المعطيات الشخصية على ضرورة توافر شروط حتي يجوز معالجة البيانات الشخصية المتعلقة بالصحة وهي كالتالي([1]):

A. إذا وافق المعني بالأمر أو ورثته أو وليه على ذلك. وإذا كان المعني بالأمر طفلا يتم مراعاة المادة ٢٨ من هذا القانون([2]).

B. إذا كانت المعالجة لازمة لتحقيق أغراض يقتضها القانون أو التراتيب.

C. كانت المعالجة ضرورية لتطوير الصحّة العمومية وحمايتها بما في ذلك البحث عن الأمراض.

D. إذا اتضح من الظروف أن المعالجة ستعود على المعني بالأمر بالفائدة على المستوى الصحّي أو اقتضتها متابعة حالته الصحية لأغراض وقائية أو علاجية.

F. إذا كانت المعالجة في نطاق البحث العلمي في مجال الصحة.

G. لا تتم معالجة المعطيات الشخصية المتعلقة بالصحة إلا من قبل أطباء أو أشخاص خاضعين بحكم مهامهم إلى واجب المحافظة على السر المهني. ويجوز للأطباء إحالة المعطيات الشخصية التي بحوزتهم إلى أشخاص أو مؤسسات تقوم بالبحث العلمي في مجال الصحّة بناء على طلب صادر عنها وبمقتضى ترخيص من الهيئة الوطنية لحماية المعطيات الشخصية. وعلى الهيئة أن تبت في طلب الترخيص في أجل أقصاه شهر من تاريخ تقديمه.

H. لا يمكن أن تتجاوز المعالجة المدة الضرورية لتحقيق الغرض الذي أجريت من أجله.

([1]) – انظر قانون حماية المعطيات الشخصية التونسي الصادر في ٢٧ يوليو ٢٠٠٤ ، عدد ٦٣ لسنة ٢٠٠٤ ، المواد من ٦٢ إلى ٦٥.

([2]) – تنص المادة ٢٨ على أنه: "لا يمكن معالجة معطيات شخصية متعلقة بطفل إلا بعد الحصول على موافقة وليه وإذن قاضي الأسرة. ويمكن لقاضي الأسرة أن يأذن بالمعالجة ولو دون موافقة الولي إذا اقتضت مصلحة الطفل الفضلى ذلك. ولقاضي الأسرة الرجوع في الإذن في كل وقت".

ا. يمكن للهيئة أن تحدد عند إسناد الترخيص المشار إليه في الفقرة الثانية من المادة ٦٣ من هذا القانون الاحتياطات والإجراءات الواجب اتخاذها لضمان حماية المعطيات الشخصية المتعلقة بالصحة. ويمكن للهيئة أن تحجر نشر المعطيات الشخصية المتعلقة بالصحة.

٤. البيانات الشخصية المعالجة إلكترونياً المتعلقة بالحالة الاجتماعية:

يقصد بالبيانات الشخصية المعالجة إلكترونياً التي تتعلق بالحالة العائلية للشخص، أي ما إذا كان متزوجاً ويعول أو متزوجاً ولا يعول أو أعزب أو مطلقاً(١)، كل هذه البيانات الشخصية تخضع للحماية القانونية وبالتالي تكون محل لجرائم الاعتداء على خصوصية البيانات الشخصية التي يتم معالجتها الكترونياً.

٥. البيانات الشخصية المعالجة إلكترونياً المتعلقة بالمعتقدات الدينية والآراء السياسية والأصول العرقية:

فقد نص المشرع الفرنسي في المادة ٨ من قانون حماية البيانات الشخصية، على أن كل المعلومات المتعلقة بالآراء السياسية والفلسفية تعتبر من البيانات الشخصية، وكذلك الأمر فإن المعلومات المتعلقة بالمعتقدات الدينية والأصول العرقية للإنسان تعتبر من البيانات الشخصية التي تكون محل حماية القانون للبيانات الشخصية التي يتم معالجتها الكترونياً.

---

(١) – Sophie PENA PORTA, Les données personnelles et leur traitement, art disponible sur,
http://www.fidal-avocats-leblog.com/theme/propriete-intellectuelle-et-technologies-de-linformation.

وتطبيقاً على ذلك فقد قضت محكمة الاستئناف بمدينة تولوز الفرنسية بالإدانة على عمدة مدينة تولوز وإلزامه تعويض المضرورين، حيث إنه قام بجمع البيانات الشخصية لأولياء أمور الطلاب في مدينته وخاصة ما يتعلق بانتماءاتهم السياسية، وذلك ليرسل إليهم برنامجه الانتخابي الخاصة به(١)، مما شكل انتهاك للحق في خصوصية البيانات الشخصية التي تم معالجتها الكترونياً والتي تنص عليها المادة ٨-١ من قانون حماية البيانات الشخصية الفرنسي.

٦. البيانات الشخصية المعالجة إلكترونياً المتعلقة بصحيفة الحالة الجنائية:

يقصد بالبيانات الشخصية المعالجة إلكترونياً المتعلقة بصحيفة الحالة الجنائية هي البيانات المتعلقة بالجرائم أو أحكام الإدانة أو الإجراءات أو التدابير الامنية والاحترازية التي خضع لها الشخص. وقد نص المشرع الفرنسي في المادة التاسعة من قانون حماية البيانات الشخصية رقم ٧ لسنة ١٩٧٨ المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤ على أنه لا يجوز معالجة البيانات الشخصية المتعلقة بالجرائم أو أحكام الإدانة أو الإجراءات الأمنية إلا عن طريق الجهات المحددة التالية:

أ- السلطات القضائية.

ب-معاوني القضاء، ولكن بشرط أن تكون متعلقة ممارسة مهامهم التي خولها القانون لهم.

ج- مؤسسات حماية حقوق الملكية الأدبية والفكرية، ولكن بشرط أن يتم ذلك لحماية حقوق ضحايا عمليات الاعتداء على حقوق الملكية الأدبية والفكرية.

(١) - T.G.I de Toulouse, Jugement correctionnel du ١٣ septembre ٢٠٠١, et disponible sur site, www.alain-bensoussan.com. France.

وبناء على ذلك فقد أستقر القضاء الفرنسي على أعطا الحق في معالجة وجمع البيانات الشخصية لمرتكبي جرائم قرصنة البرامج والمصنفات الفنية على الإنترنت وتعقبهم عبر الإنترنت، لجهات حماية الملكية الأدبية والفكرية(١). ولكن بشرط أن يتم ذلك بقصد حماية ضحايا الاعتداء على حقوق الملكية الأدبية والفكرية.

٧. الصور الحديثة لبيانات الشخصية المعالجة إلكترونياً المتعلقة باستخدام التكنولوجيا:

من أهم صور الحديثة للبيانات الشخصية المعالجة إلكترونياً المتعلقة باستخدام التكنولوجيا عنوان البريد الإلكتروني وعنوان الكمبيوتر IP والبيانات الشخصية على مواقع التواصل الاجتماعي الإلكترونية، وسوف نتناول ذلك بالشرح على النحو التالي:

د- عنوان البريد الالكتروني الايميل E- mail:

مما لاشك فيه أن عنوان البريد الإلكتروني من الصور الحديثة للبيانات الشخصية ، حيث يحق لأي مستخدم لشبكة الأنترنت أن يستخدم خدمة البريد الإلكتروني أي أن يكون له عنوان إلكتروني يتلقى ويرسل من خلاله الرسائل الإلكترونية(٢). ويعتبر البريد الإلكتروني من البيانات الشخصية التي تخضع للحماية القانونية وذلك لأنه يتعلق بشخص معين محدد الهوية أو قابل للتحديد.

ويقصد بالبريد الإلكتروني وفقاً لتعريف المشرع الأمريكي في قانون خصوصية الاتصالات الإلكترونية الصادرة في عام ١٩٨٦ بأنه وسيلة اتصالات يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تليفونية عامة أو خاصة، وفي الغالب يتم عن

---

(١) – C.A. Paris, ١٣ ème ch., section A, ١٥ mai ٢٠٠٧, disponible sur site, www.foruminternet.org. C.A. Paris, ١٣ ème ch., section B, ٢٧ avril ٢٠٠٧. Ibid.

(٢) – Nathalie MALLET – POUJOL, Protection de la vie privée et des données à caractère personnel, *Op. Cit.*, p.٣٢.

طريق كتابة الرسالة على جهاز الحاسب الآلي ثم يتم إرسالها إلكترونياً على حاسب إلى مورد الخدمة الذي يتولى تخزينها حتي يستعيدها المرسل إليه.

أما بالنسبة للمشرع الفرنسي فقد عرف البريد الإلكتروني في المادة ٤ الفقرة الأولى من القانون رقم ٥٧٥ لسنة ٢٠٠٤ بشأن الثقة في الاقتصاد الرقمي بأنه "كل رسالة، أيا كان شكلها نصية أو صوتية أو مصحوبة بصورة وأصوات، يتم إرسالها عبر شبكة عامة للاتصالات، ويتم تخزينها على أحد خوادم هذه الشبكة أو في المعدات الخاصة بالمرسل إليه، حتى يتمكن هذا الأخير من استعادتها".

أما بالنسبة لموقف المشرع المصري فقد نص في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على يقصد بالبريد الإلكتروني "بأنه وسيلة لتبادل رسائل إلكترونية على عنوان محدد ، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها"(١).

وبناء على ما سبق يمكن تعريف البريد الإلكتروني بانه وسيلة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة الأنترنت(٢)، ومستودع لحفظ الأوراق والمستندات

(١) – انظر المادة الأولى من القانون المصري بشأن مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

(٢) – Verbiest THIBAULT et Wéry ETIENNE, Le droit de l'internet et de la société de l'information : droits européen, Belge et Français, éd., Larcier, Paris, ٢٠٠١, p. ٦١١.

الإلكترونية(١) ، يتم الدخول إلية عن طريق كلمة سر أو أي نظام آخر من نظم التشفير والحماية. وعليه فقد أقر المشرع الفرنسي حماية خاصة للبريد الإلكتروني نظراً لما يحتويه من بيانات ومعلومات خاصة تدخل في نطاق الحماية الجنائية للحق في خصوصية البيانات الشخصية الإلكترونية ، ونص في المادة ٢٢٦ – ١٥ من قانون العقوبات المعدلة بالقانون رقم ١١٦٨ لسنة ٢٠١٣ على أن(٢) يعاقب بالحبس لمدة عام وبالغرامة المالية التي تبلغ مقدارها ٤٥.٠٠٠ ألف يورو كل من يقوم بقطع أو بالاطلاع أو الفتح أو الحذف أو التحويل أو نشر الاتصالات الخاصة، المتراسلة بوسيلة الاتصالات أو بواسطة إعداد أجهزة مهمتها ارتكاب هذه الأفعال، أو أي مراسلات إلكترونية أرسلت إلى طرف آخر ، وتم ذلك بطريق الاحتيال، وبسوء نية.

وتطبيقا على ذلك فقد قضت محكمة جنح باريس(٣) ووفقا لقانون الاتصالات على إحدى الوقائع التي تمكن فيه ثلاث أشخاص يعملون في إدارة مدرسة الفيزياء الصناعية والكيميائية في باريس باختراق بريد إلكتروني يخص طالب كويتي وقد كان الانتهاك بقصد مراقبة بريد الطالب، وقدم هؤلاء الأشخاص إلى المحاكمة وتم إدانتهم بجنحة انتهاك وسيلة اتصال من قبل أشخاص مكلفين بخدمة عامة، مما يشكل اعتداء على الحق في خصوصية البيانات والمعلومات الشخصية الموجودة على البريد الإلكتروني.

---

(١) – Frédéric COLANTONIO. La protection du secret des courriers électroniques en Belgique : Aspects techniques, D.E.S en criminologie, Université liège, Faculté de droit, ٢٠٠١ –٢٠٠٢, p. ٩.

(٢) – L'Article ٢٢٦ –١٥ de code de droit pénal, modifié par loi n°٢٠١٣ – ١١٦٨ du ١٨ décembre ٢٠١٣ – art. ٢٣.

(٣) – T.G. I. Paris, ٢ Nov. ٢٠٠٠, sur le site, www. Legalis.net. انظر كذلك د. أحمد محمد صالح ، هوس الإنترنت ، كتاب الهلال ، القاهرة ، العدد ٦١٥ مارس ٢٠٠٢.

وكذلك فقد قضت كذلك محكمة النقض الفرنسية في قضية Nikon في أكتوبر ٢٠٠١ بأن البريد الإلكتروني من المراسلات الخاصة التي تتمتع بالخصوصية(١)، وبالتالي يخضع للأحكام الخاصة بسرية المراسلات التي تحظر على غير المرسل إليه الاطلاع عليها أو التعرف على محتواها(٢). وبناء على ذلك فإن أي إفشاء لمضمون هذه الرسائل أو نشرها يعتبر تعدي على حق الفرد في خصوصية البيانات الشخصية الإلكترونية.

بالإضافة إلى ذلك فقد نص المشرع السويسري على الحق في خصوصية المراسلة الإلكترونية وفقا للمادة ٣٢١ – ٣ من قانون العقوبات فسرية الاتصالات والمراسلات الإلكترونية مشمولة بالحماية الجنائية. بالإضافة إلى ذلك فقد نصت المادة ٤٣ من القانون الفيدرالي السويسري للاتصالات الصادر في ٣٠ أبريل ١٩٩٧ على أن يتضمن الالتزام بالسرية على عاتق المهني في إطار خدمة الاتصالات بحيث يلتزم بالامتناع عن نشر المعلومات عن اتصالات ومراسلات المستخدمين، ويلتزم كذلك بعدم تقديم تسهيلات الاتصال بهذه المعلومات(٣). وبناء على ذلك يتضح أن المشرع يعتبر المراسلات الإلكترونية وخاصة البريد الإلكتروني من البيانات والمعلومات التي تدخل في نطاق الحماية الجنائية للحق في خصوصية للبيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً.

---

(١) – Cons. Prud'hon, Paris, ١ février ٢٠٠٠, disponible sur : www.prudhommes.comprendrechoisir.com

(٢) – M. CAHEN, Que deviennent les emails, les comptes Webmail et les sites web après un décès? A qui appartiennent – ils ? Rentrent ils dans la succession ?; Paris, ٢٠١٣, p. ٢. www.murielle-cahen.com

(٣) – د. عمر محمد أبو بكر يونس ، الجرائم الناشئة عن استخدام الإنترنت ، الأحكام الموضوعية والإجرائية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ ، ص ٦٢٤.

أ- عنوان الكمبيوتر IP:

يتم منح كل كمبيوتر متصل بشبكة الإنترنت عنوانا يتكون من ٣٢ رقماً ، هذا العنوان يمكن من خلاله تحديد مكان هذا الكمبيوتر(١). لذلك فإنه يعتبر من المعلومات التي تتعلق بالبيانات الشخصية التي يمكن من خلالها وبطريقة غير مباشرة تحديد هوية الشخص. حيث أن الشخص لدى تصفحه للمواقع الإلكترونية على شبكة الانترنت يترك آثاراً ومعلومات خاصة به دون أن يعلم من خلال IP، مما قد يساهم في تحديد تواريخ وساعات الاتصال والمواضيع التي قام بتصفحها. فالشخص يعطي وبدون اختياره وبدون علمه بيانات شخصية عنه يمكن استغلالها سواء على المستوي الاقتصادي أو السياسي أو الاجتماعي.

وقد ثار تساؤل في الفقه الفرنسي حول هل يمكن اعتبار عنوان IP للكمبيوتر من البيانات ذات الطابع الشخصي وبالتالي تخضع للحماية القانونية أم لا؟ وللإجابة على هذا التساؤل فقد انقسم الفقه الفرنسي إلى اتجاهين، وهو ما سوف نستعرضه على النحو التالي:

الاتجاه الأول. الاتجاه الرافض لاعتبار عنوان IP للكمبيوتر من بين البيانات ذات الطابع الشخصي: وذلك لأنه لا يحدد هوية شخص طبيعي، وانما يتعلق بجهاز الحاسب الآلي وليس بالشخص. وتطبيقا لذلك قضي بأن بيانات المستخدمين التي يجب على متعهدي الإيواء جمعها والاحتفاظ بها هي اسم المستخدم ولقبه ومحل إقامته ورقم

(١) – Melle Sophie LALANDE, L'adresse IP de votre ordinateur; une donnée personnelle relevant du régime communautaire de protection? *Op.cit.*

الهاتف، وذلك تأسيسا على أن عنوان IP للكمبيوتر لا يحدد ، ولو بصورة غير مباشرة هوية شخص طبيعي(١) ، وبالتالي لا يجوز اعتباره من البيانات ذات الطابع الشخصي. الاتجاه الثاني. الاتجاه المؤيد لاعتبار عنوان IP للكمبيوتر من قبيل البيانات ذات الطابع الشخصي: لأنه يحدد هوية الشخص وخاصة الهوية الرقمية للفرد. وتطبيقا لذلك قضي في شأن قيام بعض مستخدمي موقع اليوتيوب بنشر مصنفات مقلدة(٢)، بإلزام الموقع بالكشف للمدعي عن البيانات التي تحدد هوية المستخدمين ، ومنها عنوان IP للكمبيوتر وعنوان البريد الإلكتروني، استناداً إلى ان عنوان IP للكمبيوتر هو بيان من البيانات ذات الطابع الشخصي، لأنه وسيلة لتحديد الهوية الرقمية للشخص مستخدم الكمبيوتر عن طريق غير مباشر.

ونستخلص مما سبق فإن الرأي الراجح الذي نؤيده هو الاتجاه الثاني والذي يذهب إلى أن عنوان IP للكمبيوتر بيان من البيانات ذات الطابع الشخصي وهو ما أخذت به اللجنة القومية الفرنسية للمعلومات والحريات CNIL، إذا الزمت على مقدمي خدمات الإنترنت ضرورة الحصول على ترخيص قبل معالجة أو جمع أي عنوان IP للكمبيوتر(٣)، وذلك باعتباره من البيانات ذات الطابع الشخصي لأنه يعبر بطريقة غير

---

(١) – Cour d'appel de Paris, ١٣ ème chambre, A, ١٥ mai ٢٠٠٧, ٠٦/٠١٩٥٤, Sté civile des producteurs phonographiques et a, c/ Sebaux Henir., CA Paris, ٢٧ avril ٢٠٠٧.

(٢) – Crim. ١٣ janv.٢٠٠٩, n° ٠٨-٨٤.٠٨٨ ; *D.* ٢٠٠٩. ٤٩٧, obs. J. Daleau ; ibid. ٢٨٢٥, obs. G. Roujou de Boubée, T. Garé et S. Mirabail ; *RTD com.* ٢٠١٠. ٣١٠, obs. F. Pollaud-Dulian

(٣) – Const. Const. ١٠ juin ٢٠٠٩, Loi favorisant la diffusion et la protection de la création sur internet, n° ٢٠٠٩-٥٨٠ DC ; AJDA ٢٠٠٩. ١١٣٢ ; *D.* ٢٠٠٩. ١٧٧٠, point de vue J.-M. Bruguière ; ibid. ٢٠٤٥, point de vue L. Marino ; ibid. ٢٠١٠. ١٥٠٨, obs. V. Bernaud et L. Gay ; ibid. ١٩٦٦, obs. J. Larrieu, C. Le Stanc et P. Tréfigny-Goy ; Dr. soc. ٢٠١٠. ٢٦٧, chron. J.-E. Ray

مباشرة عن الهوية الرقمية للشخص، وبالتالي يخضع للحماية القانونية لخصوصية البيانات الشخصية التي يتم معالجتها إلكترونياً.

ب-البيانات الشخصية على مواقع التواصل الاجتماعي:

تعتبر مواقع التواصل الاجتماعي على شبكة الانترنت وسيلة للتعبير عن الآراء والتواصل من خلال تحميل الصور والفيديوهات ومشاركة الروابط الخاصة عبرها، والتعبير شخصياً عن الذات والآراء، وأحياناً الحالة الشخصية من خلال مواقع التواصل مثل الفيس بوك والتوتير والإنستجرام وغيرها من مواقع التواصل الاجتماعي. فالبيانات المجمعة من هذه الحسابات الشخصية Profiles على مواقع التوصل الاجتماعي تمثل في الأصل وثيقة هوية([1])، تتعلق المعلومات المتوفرة من خلالها بالخصوصية الشخصية وبالتالي تخضع للحماية القانونية.

; *RFDA* ٢٠٠٩. ١٢٦٩, chron. T. Rambaud et A. Roblot-Troizier ; *Constitutions* ٢٠١٠. ٩٧, obs. H. Périnet-Marquet ; ibid. ٢٩٣, obs. D. de Bellescize ; *RSC* ٢٠٠٩. ٦٠٩, obs. J. Francillon ; ibid. ٢٠١٠. ٢٠٩, obs. B. de Lamy ; ibid. ٤١٥, étude A. Cappello ; *RTD civ.* ٢٠٠٩. ٧٥٤, obs. T. Revet; ibid. ٧٥٦, obs. T. Revet; *RTD com.* ٢٠٠٩. ٧٣٠, étude F. Pollaud-Dulian. CJUE ٢٤ nov. ٢٠١١, aff. C-٧٠/١٠, *D.* ٢٠١١. ٢٩٢٥, obs. C. Manara ; ibid. ٢٠١٢. ٢٣٤٣, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; ibid. ٢٨٣٦, obs. P. Sirinelli ; *RSC* ٢٠١٢. ١٦٣, obs. J. Francillon ; *RTD eur.* ٢٠١٢. ٤٠٤, obs. F. Benoît-Rohmer ; ibid. ٩٥٧, obs. E. Treppoz. Civ. ١re, ٣ nov. ٢٠١٦, n° ١٥-٢٢.٥٩٥.

([1]) – ا. نور سلمان ، نهاية الخصوصية: الحريات الشخصية وأمن الدول في عصر البيانات الضخمة ، مجلة اتجاهات الأحداث ، المجلد الأول ، العدد ٥ ، الامارات العربية المتحدة ، ديسمبر ٢٠١٤ ، ص ٢.

وعليه فقد نصت المادة ٣٠ من اللائحة العامة الأوربية لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨ على انه قد يرتبط الأشخاص الطبيعيون بمعرفات عبر الإنترنت التي توفرها أجهزتهم وتطبيقاتهم وأدواتهم وبروتوكولاتهم مثل عناوين بروتوكول الإنترنت أو معرفات ملفات تعريف الارتباط أو معرفات أخرى مثل علامات تحديد تردد الراديو. وقد يترك ذلك آثارا يمكن أن تستخدم، خاصة عند الجمع بينها وبين المعرفات الفريدة وغيرها من المعلومات التي تتلقاها الخوادم، لإنشاء ملفات تعريف للأشخاص الطبيعيين والتعرف عليها. وبالتالي فهي من البيانات الشخصية التي تخضع للحماية القانونية .

الفرع الثالث : معالجة البيانات ذات الطابع الشخصي

يقصد بالمعالجة للبيانات ذات الطابع الشخصي وفقا للمشرع المغربي([1]) بانها "كل عملية أو مجموعة من العلميات تنجز بمساعدة طرق آلية أو بدونها وتطبق على معطيات ذات طابع شخصي ، مثل التجميع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الايصال عن طريق الإرسال أو الإذاعة أو أي شكل أخر من أشكال إتاحة المعلومات، أو التقريب أو الربط البيني وكذا الإغلاق أو المسح أو الإتلاف".

مما لا شك في أن استخدام وسائل التكنولوجية الحديثة في مجال جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأشخاص ترك آثار إيجابية عريضة، لا

([1]) – الفقرة الثانية من المادة الاولى من القانون رقم ٠٨– ٠٩ لسنة ٢٠٠٩ ، الخاص بحماية الأشخاص الذاتيين تجله معالجة المعطيات ذات الطابع الشخصي. نشر في الجريدة الرسمية عدد رقم ٥٧١١ الصادرة يوم ٢٣ فبراير ٢٠٠٩.

يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة للشئون الاقتصادية والاجتماعية والثقافية ، وغيرها ، وهذا أوجد ما يعرف ببنوك المعلومات Les Banques des Donnes وهذه البنوك قد تكون قاصرة على بيانات ومعلومات خاص بقطاع معين، كقطاع الصحة أو التعليم أو البنوك، أو قد تكون شاملة مختلف القطاعات، وقد تكون مستخدمه على مستوى وطني عام كمركز المعلومات الوطنية مثال مركز دعم واتخاذ القرار بمجلس الوزراء بجمهورية مصر العربية أو مستخدمه على نحو خاص كمراكز وبنوك المعلومات للشركات المالية كالبنوك الخاصة، وكذلك قد تكون مستخدمه على مجال الإقليمي أو العالمي. ويقصد ببنوك المعلومات "هو تكوين قاعدة بيانات خاصة بموضوع معين(١) ، لخدمة غرض معين، بحيث يتم معالجتها آليا من خلال الأجهزة الإلكترونية، لإخراجها في صورة معلومات وبيانات تفيد المستخدمين والجهات المختلفة".

أما بالنسبة لموقف المشرع المصري فقد نص في المادة الأولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، على أنه يقصد بالمعالجة "أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها أو دمجها، أو عرضها أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئياً أو كلياً"(٢).

---

(١) – د. أسامة قايد ، المرجع السابق ، ص ٤٨.

(٢) – وقد نصت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على "أنه يقصد بالمعالجة الإلكترونية بأنها أي عملية إلكترونية أو تقنية تتم كلياً أو جزئياً لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استنباط البيانات والمعلومات الإلكترونية ، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخرى".

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ٣٧٠ من قانون العقوبات(١) على انه يقصد بنظام معالجة الآلية للبيانات بانه "كل مجموعة من واحدة أو أكثر من وحدات المعالجة ، سواء تمثلت في ذاكرة الحاسب الآلي، أو برامجه، أو وحدات الإدخال أو الإخراج أو الاتصال التي تساهم في تحقيق نتيجة معينة". كذلك فقد نص المشرع القطري في المادة الأولى من القانون رقم ١٣ لسنة ٢٠١٦ الخاص بحماية خصوصية البيانات الشخصية على انه يقصد بمعالجة البيانات الشخصية هو "إجراء عملية أو مجموعة عمليات على البيانات الشخصية ، كالجمع والاستلام والتسجيل والتنظيم والتخزين والتهيئة والتعديل والاسترجاع والاستخدام والإفشاء والنشر والنقل والحجب والتخلص والمحو والإلغاء".

أما بالنسبة لموقف المشرع الفرنسي فقد نص في المادة ٨ – ١ من قانون حماية البيانات الشخصية لعام ٢٠٠٤ على أنه يمتنع إطلاقاً معالجة البيانات التي تظهر بطريق مباشر أو غير مباشر أياً من الأمور الآتية: الأصول العرقية أو الآراء السياسية أو المعتقدات الدينية أو الانتماء النقابي أو الحالة الصحية أو الحياة الجنسية. وبالتالي فالقاعدة العامة لدى المشرع الفرنسي هي حظر معالجة البيانات الشخصية التي تتعلق بالأصول العرقية أو الآراء السياسية أو المعتقدات الدينية أو الانتماء النقابي أو الحالة الصحية أو الاجتماعية أو الحياة الجنسية. أما الاستثناءات على ذلك فقد نص عليها المشرع الفرنسي في المادة ٨ – ١ من قانون حماية البيانات الشخصية، بحيث يمكن معالجة البيانات الشخصية الخاصة في إحدى الحالات الآتية:

١- إذا عبر الشخص الذي سوف يتم معالجة بياناته عن رضائه الصريح بمعالجة أي من هذه البيانات سالفة الذكر في المادة ٨ – ١ من قانون البيانات الشخصية.

---

(١) – المادة ٣٧٠ من قانون العقوبات القطري ، رقم ١١ لسنة ٢٠٠٤.

٢- إذا كان الغرض من معالجة أي من هذه البيانات هو حماية حياة الشخص الذي سيتم معالجة بياناته، وكان هذا الشخص غير قادر على التعبير عن رضائه بهذه المعالجة. مثال على ذلك حالة أن يصاب الشخص في حادث ويكون فاقد الوعي، هنا يحق لإدارة المستشفى أن تقوم بالكشف عن بياناته الصحية لمعرفة تاريخه الصحي حتى تستطيع إجراء عملية جراحية له لإنقاذ حياته.

٣- ويحق للجمعيات أو أي شخص اعتباري غير هادف للربح أن تقوم بمعالجة البيانات السياسية أو الدينية أو النقابية فقط، وذلك وفقاً للشروط التالية:

i. أن تكون هذه المعالجة تناسب مع غرض الجمعية أو الشخص الاعتباري.
ii. أن تقتصر المعالجة على البيانات الخاصة بأعضاء هذه الأشخاص الاعتبارية.
iii. إلا يتم إفشاء هذه البيانات خارج الجمعية أو الشخص الاعتباري.

٤- إذا أصبحت هذه البيانات عامة بمعرفة صاحب هذه البيانات الشخصية نفسه. مثال على ذلك كأن يكون شخصاً سياسياً معروفاً ويقوم بالتعبير عن آراءه وأفكاره السياسية في وسائل الإعلام، فبذلك يصبح كل الناس يعرفون انتمائه السياسي الشخصي، وبالتالي لم يعد حاجة لحظر معالجة البيانات الخاصة بالانتماء السياسي له.

٥- إذا كانت معالجة هذه البيانات الشخصية الخاصة أمرا لازما لإثبات حق أمام القضاء أو ممارسة الدفاع عن حق أمام القضاء، فيجوز هنا معالجة هذه البيانات.

٦- إذا كانت المعالجة تتم بهدف الوقاية الصحية من الأمراض أو التشخيص الطبي أو إدارة الرعاية الطبية أو إدارة الخدمات الطبية، ويشترط في هذه الحالة أن تتم المعالجة بمعرفة شخص ممارس لمهنة الطب أو أي شخص يكون ملتزماً بعدم إفشاء سر المهنة بمقتضى القانون. ومما لاشك فيه أن المعالجة في هذه الحالة

ستقتصر على البيانات الصحية فقط(١) ولا تمتد إلى غيرها من البيانات الشخصية الأخرى.

٧- حالة المعالجات الإحصائية للبيانات التي تقوم بها المؤسسة العامة للإحصاء والدراسات الاقتصادية.

٨- حالة المعالجات الضرورية للبيانات في مجال البحث العلمي الطبي.

٩- إذا كان الهدف من المعالجة للبيانات هو التعبير الأدبي والفني.

١٠- حالة المعالجات الضرورية للبيانات لممارسة مهنة الصحافة ولكن بشرط احترام القواعد المهنية لممارسة الصحافة.

المسئول عن المعالجة للبيانات الشخصية:

يقصد به الشخص الذاتي أو المعنوي أو السلطة العامة أو المصلحة أو أي هيئة تقوم، سواء بمفردها أو باشتراك مع آخرين، بتحديد الغايات من معالجة البيانات ذات الطابع الشخصي ووسائلها. إذا كانت الغايات من المعالجة ووسائلها محددة بموجب نصوص تشريعية أو تنظيمية، تجب الإشارة إلى المسئول عن المعالجة في قانون التنظيم والتسيير أو النظام الأساسي للهيئة المختصة بموجب القانون أو النظام الأساسي في معالجة البيانات ذات الطابع الشخصي المعينة.

(١) - Philippe VANLANGENDONCK, Le dossier médical électronique: problème de vie privée et de responsabilité, l'ASBL; Droit nouvelles technologies, art disponible sur site; www.droit-technologie.org. Paris, ١١ mai ٢٠٠٠. P.٢, ٣.

واستخلاصا مما سبق نستطيع القول بأن حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً من حيث مفهومها جرى التعامل معها كحق لمنع إساءة استخدام الحكومات أو الاشخاص للبيانات التي يتم معالجتها إلكترونيا([1]) وكذلك تقييد استخدامها لغير الغرض المخصص لها أو على خلاف القانون. وعليه فتقرير حماية خصوصية المعلومات والبيانات الشخصية التي تعالج إلكترونيا يعني في المقام الأول أن ما يخزن عن الأفراد من معلومات وبيانات يجب أن يبقى في مأمن من أيدي العابثين والمتطفلين، وأن يعطى لصاحبها الحق في المحافظة عليها وعدم الاعتداء عليها إلا في حالات استثنائية وبضوابط محددة وبغرض الحفاظ على أمن الدولة ومصالحها العليا.

فحماية البيانات الشخصية من أي اختراق خلال عمليات جمعها أو معالجتها أو مشاركتها هو واجب على الجهة جامعة البيانات، وبالتالي يجب عليها التأكد من وجود هذه الاحتياطات ومدى فعالياتها في نفس الوقت. مثال على ذلك نص المشرع الكوري الجنوبي في قانون حماية البيانات الصادر في عام ٢٠١١ على أتباع وسائل محددة ومعينة من قبل التعليمات الصادرة من وزارة الاتصالات في حماية البيانات، وشدد على الوسائل المتبعة في حالات معينة مثل نقل البيانات عبر الحدود، وتخضع هذه الوسائل لتفتيش من قبل خبراء([2]). بالإضافة إلى ذلك أناط القانون بهيئة حماية البيانات دوراً توعوياً بنشر المعلومات عن كيفية حماية البيانات بين أفراد المجتمع.

([1]) – د. يونس عرب ، دور حماية الخصوصية في تشجيع الاندماج الرقمي ، ورقة عمل ، مقدمة في ندوة أخلاق المعلومات ، نادي المعلومات العربي ، ١٦ – ١٧ اكتوبر ٢٠٠٢ ، عمان.

([2]) – ا. شهد حموري ، ا. ريم المصري ، قانون حماية البيانات الشخصية ، ما يمكن تعلمة من تجارب الدول الأخرى ، اكتوبر ٢٠١٤ ، بدون دار نشر ، ص ٤.

كذلك فقد نص المشرع المغربي في المادة ٢٣ من القانون الخاصة بالتزام بسرية وسلامة المعالجات والسر المهني على مجموعة الالتزامات تقع على عاتق المسئول عن معالجة وهي على النحو التالي([1]):

١- يجب على المسئول عن المعالجة القيم بالإجراءات التقنية والتنظيمية الملائمة لحماية البيانات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو الإذاعة أو الولوج غير المرخص، خصوصا عندما تستوجب المعالجة إرسال بيانات عبر شبكات معينة، وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة. ويجب أن تضمن هذه الإجراءات مستوى ملائما من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة وطبيعة البيانات الواجب حمايتها، وذلك مع الاخذ بعين الاعتبار التقنيات المستعملة في هذا المجال والتكاليف المترتبة عن القيام بها،

٢- عندما تجري المعالجة لحساب المسئول عن المعالجة يجب على هذا الأخير اختيار معالج من الباطن يقدم الضمانات الكافية بالنظر إلى إجراءات السلامة التقنية والتنظيمية المتعلقة بالمعالجة الواجب القيام بها، ويسهر كذلك على احترام هذه الإجراءات،

٣- تنظيم عملية المعالجة من الباطن بموجب عقد أو محرر قانوني يربط المعالج من الباطن بالمسئول عن المعالجة وينص خصوصاً على ألا يتصرف المعالج

([1]) – انظر المادة ٢٣ من القانون المغربي الخاص بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي ، ظهير شريف رقم ١٥ -٠٩ – ١ صادر في ١٨ فبراير ٢٠٠٩ ، بتنفيذ القانون رقم ٠٩ – ٠٨.

من الباطن إلا بتعليمات من المسئول عن المعالجة وعلى تقيده كذلك بالالتزامات المنصوص عليها في الفقرة رقم ١،

٤- تضمن عناصر العقد أو المحرر القانوني المتعلق بحماية البيانات، وكذا المتطلبات المتعلقة بالإجراءات المشار إليها في الفقرة رقم ١، كتابة أو عن طريق شكل آخر معادل ، وذلك لأغراض حفظ الأدلة.

المراقب أو المتحكم للبيانات الشخصية:

يقصد بالمراقب للبيانات الشخصية بأنها كل شخص طبيعي أو معنوي يقوم منفرداً أو بالاشتراك مع آخرين بتحديد كيفية معالجة البيانات الشخصية والغرض منها. وقد عرف المشرع المصري المتحكم في البيانات الشخصية بأنه أي "شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصول على البيانات الشخصية تحديد طريقة وأسلوب ومعايير الاحتفاظ بها أو معالجتها والتحكم فيها طبقاً للغرض المحدد أو نشاطه". وهو يختلف عن الشخص المعالج "الذي يكون مختص بطبيعة عمله بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه وفقا لتعليماته"([1]). وبعد تحديد تعريف واضح للحماية الجنائية لخصوصية البيانات الشخصية المعالجة إلكترونياً نستعرض السياسة الجنائية في مجال حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

([1]) – المادة الأولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠.

لمبحث الثاني. اتجاهات السياسة الجنائية المعاصرة لحماية خصوصية البيانات الشخصية الإلكترونية

في واقع الأمر أن فكرة الحماية الجنائية لخصوصية البيانات الشخصية المعالجة إلكترونياً قد شهدت تطوراً من خلال حزمة شاملة من مبادئ السلوك والممارسات التي نصت عليها التشريعات الأوربية، أهمها، تأكيد الاستخدام العادل والمنصف للبيانات الشخصية، والتدخل بالحدود الدنيا، وتقييد وحصر أغراض استخدام البيانات الشخصية المعالجة إلكترونيا. وقد ظهرت أول معالجة تشريعية في مجال حماية البيانات كان في عام ١٩٧٠ في ولاية هيس بألمانيا، ولكن هذه المعالجة لم تكون معالجة متكاملة في صور قانون للدولة الالمانية ولكن كان خاص بولاية هيس فقط. ثم تبع ذلك صدور أول قانون متكامل في السويد لحماية البيانات الشخصية وتنظيم السجلات الإلكترونية وهو القانون الصادر في عام ١٩٧٣ بشأن حماية البيانات الشخصية، ثم الولايات المتحدة الأمريكية عام ١٩٧٤، ثم في المانيا صدر القانون على مستوي الفيدرالي عام ١٩٧٧، وفي فرنسا صدر قانون حماية البيانات الشخصية في عام ١٩٧٨ ثم اجري عليه الكثير من التعديلات أخرها تعديل بالقانون رقم ٤٩٣ الصادر في ٢٠ يونية ٢٠١٨.

وسوف نتناول موضوع اتجاهات السياسة الجنائية في مجال حماية خصوصية البيانات الشخصية المعالجة إلكترونيا من خلال مطلبين، في المطلب الاول نوضح الجهود الدولية في مجال حماية خصوصية البيانات الشخصية المعالجة إلكترونياً، ثم نستعرض في المطلب الثاني الجهود الوطنية في مجال حماية خصوصية البيانات الشخصية المعالجة إلكترونيا.

المطلب الاول. الجهود الدولية لحماية خصوصية البيانات الشخصية الإلكترونية

في البداية سوف نتناول في هذا المطلب استعراض جهود الأمم المتحدة في مجال حماية خصوصية البيانات الشخصية المعالجة إلكترونياً في الفرع الأول، ثم بعد ذلك نوضح الجهود الأوربية في مجال حماية خصوصية البيانات الشخصية المعالجة إلكترونياً، وفي النهاية نتناول الجهود العربية في مجال حماية خصوصية البيانات الشخصية المعالجة إلكترونياً.

الفرع الأول. جهود الأمم المتحدة لحماية خصوصية البيانات الشخصية الإلكترونية

في البداية وضعت منظمة التعاون الاقتصادي والتنمية OECD دليلاً ارشادياً لحماية الخصوصية ونقل البيانات الشخصية في عام ١٩٧٨ ودخلت حيز النفاذ في عام ١٩٨٠ بحيث انها وضعت مجموعة من القواعد التي تحكم عمليات المعالجة الإلكترونية للبيانات الشخصية، وهذه القواعد تصف البيانات والمعلومات الشخصية على أنها معطيات تتوافر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر والنقل.

وعليه فقد قامت منظمة التعاون الاقتصادي والتنمية OECD بأنشطة مختلفة بشأن حماية الخصوصية ونقل البيانات فوضعت قواعد ذات طابع توجيهي للخطوات التي ينبغي اتخاذها في إطار التشريع الوطني في كل دولة فيما يتعلق بالأحكام الموضوعية

والإجرائية. كما وضعت ضمن أجندتها السنوية موضوع تتبع وفحص مختلف الحلول التي تسهل تطبيق مبادئ حماية الخصوصية في بيئة شبكات المعلوماتية العالمية في إطار السعي لبناء الثقة بالتجارة العالمية. وهذه القواعد بوصفها إرشادية، فهي مجرد توصية فحسب بتنفيذ المبادئ العامة التي تتضمنها، ونطاق تطبيقها يقتصر على الأشخاص الطبيعيين. وأحكامها تسري على القطاعين العام والخاص وعلى المعالجة الآلية وغير الآلية للبيانات وأبرز مبادئها الموصي بتطبيقها على المستوى الوطني يتمثل في المبادئ التالية:

١- فرض قيد على تجميع البيانات ذات الطبيعة الشخصية، بشكل يوفر الضمان على أن الحصول على هذه البيانات يتم بطرق وأساليب مشروعة نزيهة، مع توفر علم ورضا أولي الشأن.

٢- الاقتصار على طبيعة البيانات الشخصية وتحديد الغرض الذي سوف يستخدم من أجله وأن تكون في نطاق الحدود الضرورية لتحقيقه، فضلا عن ضرورة كونها دقيقة وكاملة ومحدثة.

٣- تحديد الغرض منها، يقصد بها أن تكون الأغراض التي سوف تستخدم لأجل تحقيقها محددة سلفا.

٤- حصر الاستخدام بالغرض المحدد، مقتضى هذا المبدأ الالتزام بعدم إفشاء أو كشف البيانات لغير المصرح لهم بذلك أو استخدامها في غير الأغراض المخصصة لها إلا بموافقة الشخص المعني أو وفقا لأحكام قانونية.

٥- الحق في المشاركة، ومقتضى هذه المشاركة أن يكون للأشخاص المعنيين الحق في الحصول والتعرف على البيانات التي تخصهم فضلا عن رقابة مدى صحتها.

٦- المحاسبة أو المساءلة، ويعني هذا المبدأ مساءلة الجهات المنوط بها التعامل مع البيانات ذات الصبغة الشخصية عن مدى الاستجابة للإجراءات التي تكفل الفاعلية للمبادئ السابقة.

٧- سياسة معلنه، ضرورة أن تكون السياسة العامة للتطوير والتخطيط والتطبيقات معلنة فيما يتعلق بالبيانات ذات الطبيعة الشخصية، بحيث يكون متاحا للكافة معرفتها.

٨- الوقاية الأمنية، ويعني هذا المبدأ ضرورة إحاطة البيانات في مراحل الجمع والتخزين والنقل والمعالجة بسياج من التدابير والإجراءات الأمنية الملائمة.

وفي نفس السياق، نصت المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية على أنه:

١. لا يجب أن يخضع أي شخص لتدخل تعسفي أو غير قانوني في خصوصيته أو عائلته أو منزله أو مراسلاته أو لتعدي غير قانوني على شرفه وسمعته.

٢. لكل شخص الحق بحماية القانون من هذه التدخلات والهجمات.

وكذلك تنص المادة ١٢ من الإعلان الدولي لحقوق الانسان بأنه "لا يجب على أي شخص أن يخضع لتدخل تعسفي أو اعتداء على شرفه وسمعته. وللجميع الحق بحماية القانون ضد هذا التدخل والاعتداء".

وعليه فقد قامت مجموعة الدول الثمانية (G٨) وهي مجموعة الدول الصناعية السبعة التي لحقت بها روسيا وأصبحت معروفة بـ G٨، بإقرار في مؤتمرها الذي انعقد في بروكسل عام ١٩٩٥ بضرورة حماية الحياة الخاصة للأفراد في المجال المعلوماتية، وذلك بحضور حوالي أربعين مدعوا خاصا من أوساط الشركات. كما أكدت نفس الموقف في ميثاق أوكيناوا حول مجتمع المعلومات العالمي، المنبثق عن مؤتمرها المنعقد بمدينة أوكيناوا اليابانية عام ١٩٩٩، حيث ورد من بين توصيات هذا الميثاق ما يلي:

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

١- ضرورة تطوير حماية خصوصية المستهلكين بطريقة فعالة وهادفة، وكذلك حماية خصوصية معالجة البيانات الشخصية للأفراد، وفي الوقت نفسه الحفاظ على الانسياب الحر للمعلومات.

٢- وجوب مرافقة الجهود الدولية لتطوير مجتمع المعلومات العالمي بالتنسيق الفعلي لرعاية فضاء سيبراني آمن وخالٍ من الجريمة.

٣- وجوب وضع مقاييس فعالة من أجل أمن نظم المعلومات، كتلك التي أقرتها منظمة التعاون الاقتصادي والتنمية (OECD) ، والتي وضعت قيد التطبيق لمحاربة الجريمة السيبرانية.

بالإضافة إلى ذلك فإن مسألة حماية خصوصية البيانات الشخصية لم تكن غائبة عن اهتمامات الأمم المتحدة، ولا أدل على ذلك تبني الهيئة العامة التابعة للأمم المتحدة دليلا لتنظيم استخدام المعالجة الآلية للبيانات الشخصية، وذلك في ١٤ ديسمبر عام ١٩٩٠. وتضمن هذا الدليل نفس المبادئ المقررة لدى منظمة التعاون الاقتصادي والتنمية، وهي عبارة عن توصيات للدول الأعضاء لتضمينها التدابير التشريعية في مجال حماية خصوصية البيانات الشخصية.

وانطلاقا مما سبق وتنسيق مع الاهتمامات الدولية بمسألة حماية الخصوصية – تم انعقاد عدة مؤتمرات خاصة بها نذكر منها : مؤتمر دول الشمال لعام ١٩٦٧ والذي دعي إلى ضرورة اتخاذ الوسائل المدنية والجنائية لحماية الأفراد من التعدي على حق في الخصوصية عن طريق التشريع أو سائل قانونية أخرى(١). وكذلك مؤتمر طهران لعام ١٩٦٨ وهو المؤتمر الدولي الأول الخاص بأثر التقدم التكنولوجي على حقوق

(١) – مؤتمر دول الشمال لسنة ١٩٦٧ ، عقد في استكهولهم بالسويد في الفترة ما بين ٢٢ – ٢٣ مايو ١٩٦٧ ، تحت رعاية اللجنة الدولية للقانونية.

الإنسان([1]). وقد تبنت الجمعية العامة للأمم المتحدة توصياته واعترفت بالحق في الحياة الخاصة، وبأن من حق الإنسان أن يعيش لوحده بعيدا عن كشف أسراره ، وقد أهتم المؤتمر بالاكتشافات الحديثة وأحوال التطور التي فتحت آفاقا شاسعة للتقدم الاقتصادي والاجتماعي ، كذلك للخطر الداهم الذي يعترض حقوق الأفراد وحرياتهم مما يتحتم أن يكون محل انتباه متواصل([2]). وفي نهاية المؤتمر قدم السكرتير العام للأمم المتحدة تقريراً أوصى من خلاله ما يأتي:

١- أن تقوم الدول بتبني المشروعات أو تطوير التشريعات القائمة لتوفير حماية خصوصيات الأفراد ضد انتهاكات الأجهزة التكنولوجية الحديثة.

٢- أن تتخذ الإجراءات الإدارية والترتيبات اللازمة لتنظيم عملية استيراد الأجهزة المستخدمة في التنصت وتضيعها وتداولها وحيازتها.

٣- وجوب تجريم الوسائل المستخدمة للتطفل على حياة الخاصة للأفراد إلا في الجرائم ذات الأهمية البالغة الخطورة في تهديد الأمن القومي للدولة، وبناءً على إذن أو أمر من الجهة القضائية ذات الصلاحية.

وعليه فقد ذهب كذلك مؤتمر فيينا لسنة ١٩٩٩ لمكافحة استغلال الأطفال في المواد الإباحية عبر شبكة الدولية للاتصالات Internet، وكذلك اتفاقية بودابست Budapest الصادرة في ٢٣ نوفمبر ٢٠٠١ لمواجهة الأفعال الإجرامية التي ترتكب

([1]) – مؤتمر طهران الدولي لحقوق الأنسان ١٩٦٨ ، عقد في الفترة ما بين ٢٢ أبريل إلى ١٣ مايو ١٩٦٨ ، بالعاصمة الايرانية طهران ، تحت رعاية المنظمة الدولية للأمم المتحدة ، منشورات إدارة الإعلام بالأمانة العامة للأمم المتحدة ، نيويورك ، ١٩٧٤ ، ص ١ وما بعدها.

([2]) – البند ١٨ من الإعلان الصادر عن المؤتمر ، مجموعة الصكوك الدولية ، منشورات الأمم المتحدة ، نيويورك ، ١٩٨٣ ، ص ٢٩ وما بعدها.

ضد نظم الحواسيب الآلية إلى إصدار وثيقة لحماية الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً والتي وقعت عليها ٣٠ دولة أوربية إضافة إلى كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية.

وبالإضافة إلى ذلك قد نص قرار الجمعية العامة للأمم المتحدة(١) رقم ١٦٧/٦٨ الصادر في ديسمبر ٢٠١٣ على أن القانون الدولي لحقوق الإنسان يوفر الإطار العالمي الذي يجب أن يقيم على أساسه أي تدخل في حقوق الخصوصية الفردية. وذلك وفقا لنصوص العهد الدولي الخاص بالحقوق المدنية والسياسية التي تنص على أنه لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شئون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. وينص العهد، بالإضافة إلى ذلك، على أن من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس. وتتضمن صكوك دولية أخرى لحقوق الإنسان أحكاما مماثلة. وفي حين أن الحق في الخصوصية بموجب القانون الدولي ليس حقاً مطلقاً، فإن أي حالة تدخل يجب أن تخضع لتقييم دقيق ونقدي لمدى ضرورتها ومشروعيتها وتناسبها.

وتأسيسا على ذلك وعلى نهج الأمم المتحدة فقد سارت منظمة العمل الدولية، التي بذلت جهداً متميزاً في مجال حماية البيانات الشخصية المتعلقة بالعمال في تقنينها لمجموعة من التوصيات العملية التي تبناها مكتب العمل الدولي عام ١٩٩٦ وذلك من خلال مؤتمر الخبراء المتعلق بحماية الحياة الخاصة للعمال والذي اقيم في جنيف من ١-٧ أكتوبر ١٩٩٦، وعلى الرغم من أن جميع هذه التوصيات لم تكن تتكلم بعبارة صريحة عن جرائم ترتكب بوسائل الاتصال الحديثة، إلا انها كانت نواة البناء والاهتمام

(١) – قرار الجمعية العامة للأمم المتحدة رقم ١٦٧/ ٦٨ ، الذي اعتمد في ديسمبر ٢٠١٣ في الدورة الثامنة والستون البند ٦٩ (ب) من جدول الاعمال ولك بناء على تقرير اللجنة الثالثة...

بالقوانين الداخلية في الدول الاعضاء على حماية البيانات الشخصية التي تسجل على أجهزة الحاسوب الآلي عن طريق برامج خاصة ، أي التي يتم معالجتها الكترونياً.

الفرع الثاني. الجهود الأوربية لحماية خصوصية البيانات الشخصية الإلكترونية

في واقع الامر يظهر اهتمام المشرع الأوربي بحماية خصوصية البيانات الشخصية المعالجة إلكترونياً ابتداءً من عام ١٩٧٦، حيث صدرت تعليمات المجلس الأوربي رقم ٨-٤-٧٦ المتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات، وكذلك التعليمات رقم ٨-٥-٧٩ المتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة البيانات.

وعليه في ٢٨ يناير عام ١٩٨١ بمدينة ستراسبورغ وضع المجلس الأوربي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية. وذلك لضمان حق كل شخص طبيعي في أية دولة مهما كانت جنسيته أو مكان إقامته واحترام حقوقه وحرياته الأساسية وخصوصيته في مواجهة الاستخدام الآلي للمعلومات ذات الطابع الشخصي الذي تتعلق به. وقد وضعت الدول الموقعة للاتفاقية مجموعة من التوصيات الخاصة بحماية البيانات الشخصية المعالجة إلكترونياً، لكي تلتزم بها الدول الأعضاء عند وضع تشريعاتها الخاصة بهذا المجال، وهي على النحو التالي:

١- أن تكون البيانات التي تجرى جمعها كاملة ودقيقة، وأن يتم الحصول عليها بطريقة مشروعة، فضلاً عن أن تكون حفضها لأغراض المعالجة محددة بمدة معينة.

٢- عدم إفشاء أو استعمال البيانات في غير الأغراض المخصصة لها، وذلك بتوفير الحماية الأمنية الكافية لها من الناحيتين التقنية والإدارية الملائمة لضمان

تصحيحيها وتعديلها ومحوها من قبل صاحبها إذا كان الحصول عليها بطريقة مشروعة، كما ويتم تحديد الأشخاص والجهات المرخص لهم الوصول والاطلاع على تلك البيانات وإخضاعهم لقيد الالتزام بالسر المهني.

٣- أن تكون السياسة العامة للتطوير والتطبيق والحفظ المتعلقة بالبيانات الشخصية معلنة ومتاحة معرفتها للجميع.

٤- مساءلة الأشخاص والجهات المرخصة للوصول والاطلاع على حقول البيانات في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات الشخصية.

وكذلك كان الفضل لهذه الاتفاقية في كفالة الحماية للبيانات الشخصية التي تم معالجتها آلياً(١) ، كما كان لهذه التوصيات الكثير من الأثر على التشريعات الوطنية للدول الأعضاء للاتحاد الأوربي مثل التشريع الألماني ، والفرنسي ، والإنجليزي. وفي مرحلة لاحقه لإعادة تنظيم الحماية للحق في خصوصية البيانات الشخصية المعالجة إلكترونياً أصدر الاتحاد الاوربي في عام ١٩٩٥ الامر التشريعي الخاص بحماية البيانات الشخصية ونقلها عبر الحدود، مما جعل العديد من دول أوربا تعمل على تطوير التشريعات القائمة الخاص بحماية خصوصية البيانات الشخصية المعالجة إلكترونياً. وتطبيقا لذلك فقد أصدرت المحكمة الدستورية العليا في المانيا حكماً مهماً في شأن حماية خصوصية البيانات الشخصية للأفراد المعالجة إلكترونيا في مجال الاحصاء

(١) - Pierre KAYSER, La protection de la vie privée par le droit, ٣ éd, Economica, ١٩٩٥, Paris, pp. ٣٥٦ – ٣٥٩.

القومي([1])، حيث قضت المحكمة بأن عدم التقييد والضبط في الوصول إلى البيانات الشخصية للأفراد يعرض للخطر وبشكل فعلي ، جميع الحقوق المحمية في الدستور. وكذلك فقد قام المشرع الفرنسي بتعديل قانون حماية البيانات الشخصية بالقانون رقم ٨٠١ لسنة ٢٠٠٤ وكذلك كانت هناك تعديلات متعددة آخر هذه التعديلات صدرت بالقانون رقم ٤٩٣ في ٢٠ يونية ٢٠١٨. وقد ساهمت اللجنة القومية للإعلام والحريات الفرنسية CNIL في تطور الحماية القانونية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

بالإضافة إلى ذلك فقد نصت المادة الثامنة من الاتفاقية الأوربية لحقوق الانسان على أنه:

١. للجميع الحق باحترام حياتهم الخاصة والعائلية ومنزلهم ومراسلتهم([2]).

٢. لن يكون هناك أي تدخل من سلطة عامة في ممارسة هذا الحق إلا بما يتوافق مع القانون وعند الضرورة في مجتمع ديمقراطي ولصالح الأمن القومي أو السلامة العامة أو الرفاهية الاقتصادية للبلد لتجنب الفوضى أو الجريمة ولحماية الصحة والأخلاقيات ولحماية حقوق وحريات الآخرين.

ونستخلص مما سبق أن المشرع الأوربي قد نص على أحكام هامة وصريحة في الاتفاقية الأوربية لحقوق الانسان بالنسبة لحماية البيانات الشخصية وخاصة التي نتناولها في البحث والتي يتم معالجتها إلكترونياً وذلك على النحو التالي:

([1]) – د. محمد عبد المحسن المقاطع ، نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر ، مؤتمر الكويت الأول للقانون والحاسب الألي ، كلية الحقوق ، جامعة الكويت ، الطبعة الأولى ، ١٩٩٤ ، ص ١٧٥.

([2]) – وقد فسرت المحكمة الأوربية لحقوق الانسان الفقرة الأولى من المادة الثامنة للاتفاقية الأوربية لحقوق الانسان بحيث تشمل الاتصالات الهاتفية وأي وسيلة تواصل إلكترونية.

١. أن للجميع الحق بحماية خصوصية بياناتهم الشخصية التي يتم معالجتها إلكترونياً. وأن أي حد من ممارسة الحقوق والحريات الواردة في هذه الاتفاقية يجب أن يكون بموجب القانون ودون أي إخلال بجوهر هذه الحق. وفي ضوء مبدأ التناسب بين المصلحة العامة في فرض قيود على الحقوق والحريات وحماية خصوصية البيانات الشخصية المعالجة إلكترونياً.

وتطبيقا لذلك فقد قضت المحكمة الاوربية لحقوق الانسان أن الملفات الأمنية الحكومية التي تحتوي على البيانات الشخصية تقع ضمن النطاق المحمي للحياة الشخصية المنصوص عليها في المادة الثامنة من الاتفاقية الأوربية لحقوق الانسان. بالإضافة إلى ذلك فقد لوحظ أن هناك حالات عديدة يتم فيها تجميع وتخزين ونشر البيانات الشخصية من قبل جهاز الاستخبارات بطريق غير قانوني مما يشكل اعتداء على الحق في خصوصية البيانات الشخصية وخاصة التي يتم معالجة إلكترونيا([1]).

٢. يجب معالجة هذه البيانات الشخصية بشكل عادل ولأهداف محددة وعلى أساس موافقة الشخص المعني أو على أساس مشروع آخر تنص عليه القوانين الوطنية لدول الاتحاد الاوربي، ينظم للجميع الحق في حماية خصوصية بياناتهم الشخصية التي تم معالجتها إلكترونياً والطرق المشروعة لاستخدامها أو الاحتفاظ بها.

٣. وبناء على ذلك كان لابد من انشاء هيئة مستقلة للرقابة على الالتزام بهذه القواعد. وبناء على لك فقد انشاء المشرع الفرنسي اللجنة القومية للمعلومات والحريات الخاصة بحماية البيانات الشخصية CNIL.

([1]) – انظر المحكمة الاوربية لحقوق الانسان ECHR: قضية روتارو ورومانيا ، Rotaru v. Romania، ٢٨٣٤١/ ٩٥ ، ٢٠٠٠.

وعليه في ٢٧ أبريل ٢٠١٦ أصدر الاتحاد الاوربي اللائحة العامة لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨. وتشمل اللائحة الجديدة العديد من التعديلات الجوهرية على الامر التشريعي الاوربية لمعالجة البيانات الشخصية، وسوف تطبق هذه اللائحة الاوربية الجديدة على وحدات التحكم أو المعالجة للبيانات الشخصية التي تتم كذلك من خلال شركات من الباطن والتي تتم من خارج الاتحاد الاوربي، ولكن تعالج البيانات لمواطنين في الاتحاد الاوربي. كما الزمت اللائحة الاوربية الجديدة الشركات التي تعمل على معالجة البيانات الشخصية بمجموعة من القواعد وهي كالتالي([1]) :

١- ضرورة الالتزام بمبدأ المساءلة والامتثال لأحكام القانون في عمليات معالجة وأداره البيانات الشخصية. مثال التزام موظف معالجة أو حماية البيانات الشخصية بعدم المعالجة واسعة النطاق للإدانات الجنائية وغيرها وكذلك المراجعة المستمرة لبيانات الشخصية في السجلات المحفوظة، واعداد قائمة بالإجراءات الضرورية الواجب اتباعها وتحديد ألوياتها في ضوء المخاطر من الناحية العلمية.

٢- تعزيز النهج القائم على التقييم المستمر لمخاطر الاعمال عالية الخطورة على خصوصية البيانات الشخصية، وبالتالي يجب استخدام تقنيات مثل الاسم المستعار والتشفير في جميع عمليات المعالجة والنقل والحفظ وغيرها من العمليات الأخرى التي تتم على البيانات الشخصية.

([1]) – GPDR, General data protection regulation, EU ٢٠١٦ – ٦٧٩, ٢٧ April ٢٠١٦, part ١, which comes into force in ٢٥ may ٢٠١٨. www.fidal-avocats-leblog.com.

٣- تخضع عمليات نقل البيانات الشخصية خارج الاتحاد الاوربي لقانون حماية البيانات الشخصية، مع إلزام الشركات باستخدام بنود تعاقدية قياسية وقواعد ملزم من خلال تطبيق نظام حماية الخصوصية الخاص بالاتحاد الاوربي.

٤- تخضع لتطبيق القانون جميع عقود البيانات بين مراقبي البيانات والمتعاقدين معهم من الباطن وذلك وفقا للائحة الاوربية الجديدة، وسيكون على الشركات من الباطن التزام مباشر في حفظ السجلات والأمن، بشكل منفصل عن الالتزامات المتعلقة بمراقبي البيانات.

٥- أنشئ سلطة عليا أو لجنة واحدة أوربية لحماية البيانات الشخصية، تسند إليها العمل مع السلطات الوطنية الأخرى سواء في الاتحاد الاوربي أو مع الولايات المتحدة الأمريكية لحماية البيانات الشخصية.

٦- في حالة انتهاك قانون حماية البيانات الشخصية ، تلزم الشركات بإبلاغ لجنة حماية البيانات الشخصية خلال فترة زمنية قصيرة وكذلك في حالة وجود مخاطر عالية باحتمالية حدوث انتهاك للبيانات الشخصية وفي حالة مخالفة ذلك يتم فرض غرامات مالية على الشركات قد تصل إلى مبلغ ٢٠ مليون يورو(١).

وانطلاقا على ما سبق نستطيع القول بأن اللائحة العامة لحماية البيانات الشخصية الأوربية GPDR قد وضعت معايير جديدة لحماية خصوصية البيانات الشخصية، مما يوجب على الدول الأوروبية تعديل تشريعاتها لحماية البيانات الشخصية. ففي المجال

(١) – اللائحة الأوربية بشأن حماية الأشخاص الطبيعيين فيما يتعلق بتجهيز البيانات الشخصية وحرية تنقل هذه البيانات رقم ٦٧٩ لسنة ٢٠١٦ ، نشرت في الجريدة الرسمية للاتحاد الأوربي في ٤ مايو ٢٠١٦ ، وتدخل حيز التنفيذ في ٢٥ مايو ٢٠١٨، والتي يترتب عليها إلغاء التوجيه رقم ٤٦ لسنة ١٩٩٥ لحماية البيانات الشخصية.

الإلكتروني والاتصالات يحظر فك التشفير واستعمال الهندسة العكسية أو رصد هذه الاتصالات عند استعمال تشفير بيانات الاتصالات الإلكترونية. ولا يقتصر تأثير اللائحة الجديدة على الشركات العاملة ضمن دول الاتحاد الأوربي فحسب بل يمتد ليشمل جميع المؤسسات والشركات التي لديها أعمال وأنشطة تجارية واستثمارية مع دول الاتحاد الأوربي، ومنها بطبيعة الحال قطاع الأعمال. وعلى سبيل المثال لذلك لو قام مواطن أوربي باستخدام خدمة أو تطبيق للجوال من بلد خارج الاتحاد الأوربي، وتعرضت بيانات ذلك المواطن للتسريب أو تعرضت معلومات خصوصيته للكشف فإن صاحب التطبيق أينما يكن، سيخضع للمساءلة فضلا عن تعرضه لغرامات تصل إلى ٤ % من أرباح شركته.

كذلك كما يحق للأفراد أن يطلبوا من أي شركة الكشف عن البيانات الشخصية التي تحتفظ بها في غضون ٣٠ يوما، وتغيير أو حذف تلك البيانات إذا رغب المستخدم بذلك، ويمكن إنشاء ما يصل إلى ٢٨٠٠٠ وظيفة في مجال حماية البيانات لتلبية احتياجات اللائحة العامة لحماية البيانات، وتعتبر العقوبات المفروضة على عدم الامتثال لقواعد اللائحة العامة لحماية البيانات ، هي عقوبات صارمة – حيث يمكن فرض غرامات على الشركات تصل إلى ٤٪ من مبيعاتها السنوية العالمية ، أو دفع مبلغ ٢٠ مليون يورو ، أيهما أكبر إذا كانوا يعانون من خرق البيانات التي تؤدي إلى تعرض البيانات الشخصية للخطر. وسيتم التخفيف من الغرامات تبعاً لأهمية البيانات الشخصية، والخطوات المتخذة لحماية البيانات ودعم معايير الخصوصية. فالغرامات هي أيضا ليست العقوبة الوحيدة، مع الشركات التي تخالف البيانات الشخصية فتكون مسئولة عن التعويض للمستخدمين. وسوف يترتب على ذلك ارتفاع عدد الأفراد الذين يطلبون بالتعويضات، كما ينمو الوعي بين الجمهور.

بالإضافة إلى ما سبق نصت اللائحة الأوربية لحماية البيانات الشخصية على تدبير احترازي للوقاية من احتمال انتهاك لخصوصية البيانات الشخصية وهي التزام الشركات

بحدود زمنية – لا تقل عن ٧٢ ساعة – لتقييم أي خروقات أمنية قد تكون لها والتنبيه على السلطات المختصة بأي نشاط يمكن أن ينتهك خصوصية البيانات الشخصية، وهو تدبير أشد صرامة من القواعد القائمة. وعلى العموم، فأن اللائحة الاوربية العامة لحماية البيانات ستجبر الشركات على تغيير كامل في كيفية التعامل مع البيانات الشخصية. كما سيتغير الطريقة التي تمارس بها الشركات الأعمال. وهو ينطبق على وكالات القطاع العام في ٢٨ دولة عضوا في الاتحاد الأوربي. وينطبق كذلك على الشركات التي تعمل في الدول الأعضاء في الاتحاد الأوروبي، حتى لو كانت شركات مقرها في مكان آخر مثل شركات الطيران والسياحة والرعاية الصحية، أي أن اللائحة سوف تطبق على جميع من يتعامل مع البيانات الشخصية.

الفرع الثالث. الجهود العربية لحماية خصوصية البيانات الشخصية الإلكترونية

في البداية نص الميثاق العربي لحقوق الأنسان في المادة السادسة منه([1]) على "أن للحياة الخاصة حرمة مقدسة ، والمساس بها جريمة وتشمل هذه الحياة الخاصة خصوصيات الأسرة وحرمة المسكن ، وسرية المراسلات ، وغيرها من سبل المخابرة العامة. وبالرغم من ذلك يجوز وضع قيود على هذه الحقوق ولكن بنص القانون، ووفقاً لما تمليه ضرورة الأمن والاقتصاد الوطنيين أو النظام العام أو الصحة العامة أو

([1]) – الميثاق العربي لحقوق الأنسان ، اعتمد في سبتمبر سنة ١٩٩٤ من دول أعضاء منظمة جامعة الدول العربية. د. عبد العظيم وزير ، حول مشروع ميثاق الإنسان والشعب في الوطن العربي ، المجلد الأول ، ط١ ، دار العلم للملايين ، بيروت ، ١٩٨٨. د. أمير موسى ، حقوق الإنسان مدخل إلى وعي حقوقي ، ط١ ، مركز دراسات الوحدة العربية ، بيروت ، ١٩٩٤ ، ص ١٠١.

الأخلاق أو حقوق الآخرين وحرياتهم. الامر الذي يتيح لدول العربية الأعضاء في منظمة جامعة الدول العربية قدراً من الموائمة وحرية التطبيق على النحو الذي يتفق مع مقتضيات ظروف كل منها".

كذلك في ديسمبر عام ٢٠١١ تم توقيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات([1]) ، والتي جاء في ديباجتها التأكيد على "رغبة الدول العربية في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات ومنها الاعتداء على خصوصية البيانات الشخصية المعالجة إلكترونية والتي تهدد أمن ومصلحة وسلامة الاشخاص ومن ثم المجتمع ، بالتالي لابد من تبني سياسة جنائية مشتركة تهدف إلى حماية خصوصية المجتمع العربي ضد الانتهاك لها".

بالإضافة إلى ذلك فقد نصت المادة ١٤ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على "تجريم الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات. ويتضح من مما سبق أن المشرع مطالب ببذل المزيد من الجهود من أجل أصدر اتفاقية جديدة خاصة بحماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونيا، وذلك على غرار المشرع الأوربي ، ومن أجل أن مساير متغيرات العصر الرقمي التي تنتهك الحق في خصوصية البيانات الشخصية".

([1]) – الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، والتي وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الامانة العامة لجامعة الدول العربية بالقاهرة ، في ٢١ ديسمبر ٢٠١٠.

المطلب الثاني. موقف التشريعات الوطنية من حماية خصوصية البيانات الشخصية الإلكترونية

نجد أن التشريعات الوطنية قد انقسمت في كيفية مواجهة الانتهاكات لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً إلى ثلاثة اتجاهات وهما كالتالي : الاتجاه الأول من التشريعات ذهب إلى عدم وضع تشريع خاص لحماية البيانات الشخصية المعالجة إلكترونياً والاكتفاء بالنص في القوانين العامة على حماية البيانات الشخصية المعالجة إلكترونياً ومثال على ذلك التشريع المصري (وذلك ما قبل التعديلات الأخيرة وإصدار المشرع المصري القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية)، أما الاتجاه الثاني من التشريعات فقد ذهب إلى ضرورة وضع تشريع شامل وخاص لحماية عمليات الجمع والادخال والنقل والمعالجة للبيانات الشخصية الإلكترونية ومنها في الفقه اللاتيني على سبيل المثال التشريع الفرنسي وفي الفقه الأنجلوسكسوني التشريع الانجليزي. وفي التشريعات العربية التشريع التونسي والمغربي والقطري. وهناك اتجاه ثالث وهو اتجاه وسط بين الاتجاه الاول والاتجاه الثاني من التشريعات المقارنة فهو تجنب اصدار تشريع شامل لحماية البيانات الشخصية المعالجة إلكترونياً ولكن اصدار قوانين متخصصة تحكم قطاعات بعينة في مجال حماية البيانات الشخصية المعالجة إلكترونياً، وعلي سبيل المثال على ذلك التشريع الأمريكي، فقد أصدر قوانين خاصة بحماية البيانات الشخصية المتعلقة بالجينات وكذلك بالبيانات الشخصية المتعلقة بالاقتراض لعملاء بالبنوك وخصوصية البيانات الشخصية المهنية مثال مجال المحاماة والطب ، والبيانات الشخصية المتعلقة بسجلات تأجير الفيديو والخصوصية المالية وغيرها من المجالات المختلفة المرتبطة بخصوصية البيانات الشخصية التي يتم معالجتها إلكترونياً.

الاتجاه الاول من التشريعات. يذهب إلى عدم وجود تشريع شامل لحماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، والاكتفاء بالنص في القوانين العامة على حمايتها، على سبيل المثال في ذلك التشريع المصري (وذلك قبل القانون الجديد الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠):

أولا. موقف المشرع المصري ما قبل القانون الجديد الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠:

فقد نص الدستور المصري الجديد الصادر في عام ٢٠١٤ على حرمة الحياة الخاصة في المادة ٥٧ والتي نصت على أن للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك.

وتطبيقا على ذلك فقد تناولت المحكمة الدستورية العليا المصرية حدوداً لعدم جواز استخدام القوانين في فرض قيود على حقوق الإنسان، فذهبت إلى القول بأن "لما كان منطقياً وضرورياً أن تعمل الدول المتمدينة على أن تقيم تشريعاتها الجزائية وفق أسس ثابتة تكفل بذاتها انتهاج الوسائل القانونية السليمة في جوانبها الموضوعية والإجرائية، لضمان ألا تكون العقوبة أداة قامعة للحرية عاصفة بها بالمخالفة للقيم التي تؤمن بها الجماعة في تفاعلها مع الأمم المتحضرة واتصالها بها، وكان لازماً – في مجال دعم هذا الاتجاه وتثبيته – أن تقرر الدساتير المعاصرة القيود التي ارتأتها على سلطان المشرع في مجال التجريم تعبيراً عن إيمانها بأن حقوق الإنسان وحرياته لا يجوز التضحية بها في غير ضرورة تمليها مصلحة اجتماعية لها اعتبارها، واعترافا منها بأن

الحرية في أبعادها الكاملة لا تنفصل عن حرمة الحياة([١]). وعلى نفس المنهاج فقد أكدت محكمة القضاء الإداري على أهمية الحق في الخصوصية فذهبت إلى القول بان الحق في الخصوصية هو حق أصيل سواء نصّ عليه الدستور أو أغفله"([٢]).

ويلاحظ من نص المادة ٥٧ في الدستور المصري الجديد أن المشرع الدستوري تلافي الانتقادات التي كانت موجودة في نص الدستور عام ١٩٧١ حيث كان المشرع الدستوري ينص على لحياة المواطنين حرمة خاصة .... وبالتالي استعمل كلمة مواطنين تعني أن الحماية الدستورية تقتصر على المواطنين فقد دون الأجانب، وذلك يتناقض مع التزام الدولة بحماية كل من يقيم على أراضيها دون تمييز بين المواطنين والأجانب([٣]). ولكن يأخذ على المشرع الدستوري في الدستور الجديد أنه نص في الفقرة الثالثة من المادة ٥٧ من الدستور على أن تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها... وهذا يعود بالمشرع الدستوري لمخالفة الدولة للالتزامات الدولية الخاصة بتوفر هذا الحق لجميع المقيمين سواء كانوا مواطنين أو أجانب.

بالإضافة إلى ذلك يتبين لنا من الوهلة الاولى أن المشرع الدستوري المصري قد ساوى ما بين الحماية للحق في الخصوصية سواء كانت في مجال الفضاء الإلكتروني أو خارج الفضاء الإلكتروني. إلا انه يظهر بوضوح لا يحتمل اللبس فيما يتعلق بحماية الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً فأن الواقع مغاير لذلك ، فلا توجد في القوانين المصرية النصوص التي من شأنها أن تحمي الحق في الخصوصية

([١]) – المحكمة الدستورية العليا المصرية ، الطعن رقم ٣ لسنة ١٠ قضائية ، تاريخ الجلسة ٢ يناير ١٩٩٣ ، مكتب فني ٥ ، رقم الجزء ٢ ، ص ١٠٣.

([٢]) – حكم محكمة القضاء الإداري المصرية ، الدعوى رقم ١٤٣٠ لسنة ٦٥ قضائية.

([٣]) – د. أحمد فتحي سرور ، الحماية الجنائية للحقوق والحريات ، ط ٢ ، دار الشروق ، القاهرة ، ٢٠٠٠ ، ص ٧٢١.

البيانات الشخصية التي تم معالجتها إلكترونياً، رغم النص الدستور في المادة ٥٧ على حماية الحق في الحياة الخاصة بالنسبة للجانب الإلكتروني، إلا في مجالات محددة للبيانات والمعلومات كالبنوك والتاريخ الطبي وفيما يتعلق بحرمة الحياة الخاصة بمعناها الواسع فهناك مادة واحدة بقانون العقوبات تتحدث عن ذلك([1]) ، فقط فيما يتعلق بتجريم التنصت أو انتهاك حريمة الحياة الخاصة، وهي المادة ٣٠٩ مكرر، والمادة ٣٠٩ مكرر (أ) وذلك وفقا لما يلي :

فالمادة ٣٠٩ مكرر من قانون العقوبات المصري تنص على أنه "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن ، وذلك بان ارتكب أحد الافعال الاتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجنى عليه([2]) :

(أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الاجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

(ب) التقط أو نقل بجهاز من الاجهزة أياً كان نوعه صورة شخص في مكان خاص".

([1]) – وتطبيقاً لذلك قضت محكمة النقض المصرية بأن "وقائع السب والقذف التي يتضمنها النشر تعد من الحقوق الخاصة ولا تندرج ضمن ما نصت عليه المادة ٥٧ من الدستور" ، نقض ٢٨ يوليو ١٩٩٢ ، الطعن رقم ٢٨٨ لسنة ٥٨ قضائية ، مجلة القضاة الفصلية ، السنة ٢٥ ، العدد الثاني ، يوليو – ديسمبر ١٩٩٢ ، ص ٥٤٩.، وينظر : د. أشرف توفيق شمس الدين ، الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ١٩٩٦ ، ص ٢.

([2]) – انظر محكمة النقض المصرية ، نقض جنائي ، الطعن رقم ١٤٣٤٨ لسنة ٦٥ ، جلسة ١٨ يناير ٢٠٠٤ ، س ٥٥ ، ع ١ ، ق ٨ ، ص ١٢٤. فالقصد العام الذي يتحقق بمجرد ارتكاب الفعل المادي وتستوى البواعث التي دفعت المتهم إلى فعله وأن مجرد الاعتداء على حرمة الحياة الخاصة باسترق السمع يفترض فيه القصد إذا ما توافر عنصراه: العلم والإرادة.

وعليه إذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع ومرأي من الحاضرين في ذلك الاجتماع فإن رضا هؤلاء يكون مفترضاً ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الاجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عليه، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو اعدامها.

أما المادة ٣٠٩ مكرر (أ) من قانون العقوبات المصري فتنص على أنه "يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن. ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصيل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه. ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويحكم بمصادرة الاجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عليها. كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها".

أما فيما يتعلق بالمادة ٧٣ من قانون العقوبات المصري فقد نصت على انه "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال الآتية :

١- إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها دون أن يكون له سند قانوني في ذلك.

٢- إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات أو لجزء منها تكون قد وصلت إليه.

٣- الامتناع عمداً عن إرسال رسالة اتصالات بعد تكليفه بإرسالها.

٤- إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق".

وفي ذات الاتجاه نصت المادة ٩ من قانون رقم ٢٦٠ لسنة ١٩٦٠ في شأن الأحوال المدنية المعدل بالقانون رقم ١١ لسنة ١٩٦٥ والقانون رقم ١٥٨ لسنة ١٩٨٠ على "أن البيانات التي تحويها سجلات الأحوال المدنية تعتبر سرية، ولما كانت هذه البيانات سراً فإن إفشاءها من قبل الموظف يوقعه تحت طائلة القانون"، والمساءلة بموجب أحكام قانون العقوبات .كما قرر المشرع معاقبة كل من أخل بسرية البيانات الإحصائية، أو أفشى بياناً من البيانات الفردية، أو سراً من أسرار الصناعة، أو التجارة، أو غير ذلك من أساليب العمل التي يكون قد اطلع عليها بمناسبة عمله بالحبس. كما حرص المشرع علي سرية بيانات العملاء البنكية، فحظر الاطلاع والإفشاء بغير المقرر للأشخاص والجهات المسموح لها وفقاً لأحكام القانون، ويمتد الحظر حتى بعد زوال العلاقة بين العميل والبنك، ويسري الحظر على جميع الأشخاص والجهات بما في ذلك الجهات التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها . طبقاً لأحكام قانون سرية الحسابات بالبنوك.

وعليه فقد تم تعديل قانون الأحوال المدنية بالقانون رقم ١٣٤ لسنة ١٩٩٤ لحماية البيانات الشخصية المسجلة بالحاسبات الآلية بمراكز الأحوال المدنية، حيث تنص المادة ٧٢ منه على "أن في تطبيق أحكام قانون الأحوال المدنية وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات

الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية، فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة السجن المشدد أو السجن لمدة لا تقل عن خمس سنوات".

بالإضافة إلى ذلك فقد نصت المواد ٧٤ و٧٥ و٧٦ من قانون الأحوال مدنية على بعض الجرائم الأخرى التي تتعلق بحماية البيانات الشخصية التي يتم تسجيلها بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية(١). ويتضح من ذلك أن المشرع المصري حاول التصدي لبعض جرائم التي تمس بخصوصية البيانات الشخصية التي يتم معالجتها في مراكز الأحوال المدنية وفي سجلات وأجهزة الحاسب الآلي الخاص بالأحوال المدنية.

كما حرص المشرع المصري علي حماية بيانات الطفل، فقد قرر تغريم من ينشر بيانات تخص هوية طفل معرض للخطر حيث جرم نشر أو إذاعة أي معلومات، أو بيانات، أو أي رسوم، أو صور تتعلق بهوية الطفل حال عرض أمره على الجهات المعنية بالأطفال المعرضين للخطر أو المخالفين للقانون، كما حظر القانون على من اتصل علمه بحكم عمله إفشاء بيانات ومعلومات متعلقة بالتوقيع الإلكتروني، ففرض المشرع على تلك البيانات السرية وقرر توقيع الغرامة لمن يخالف ذلك.

كذلك فقد نصت المواد ٢١ و٥١ و٧٦ من قانون التنظيم للصحافة والإعلام رقم ٩٢ لسنة ٢٠١٦ على حماية الحياة الخاصة من الاعتداء عليها عن طريق النشر حيث نصت على أنه يلتزم العاملون بالمجلس الاعلى (المجلس الأعلى لتنظيم الإعلام)،

(١) – د. عادل يحي ، السياسة الجنائية في مواجهة الجريمة المعلوماتية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠١٤ ، ص ٧٥.

وكذلك العاملون بالهيئة الوطنية للصحافة والعاملون بالهيئة الوطنية للإعلام بالحفاظ على سرية المعلومات والوثائق التي يتم الحصول أو الاطلاع عليها بمناسبة القيام بمهامهم، وذلك بعدم إفشائها أو استخدامها في غير الأغراض المخصصة لها. ونص كذلك في المادة ٧٩ منه على أنه "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في أي قانون أخر، يعاقب بالغرامة التي لا تقل عن مائة ألف جنية ولا تزيد على خمسمائة ألف جنية، كل من خالف أحكام المواد ٢١ و٥١ و٧٦ من هذا القانون".

أما بالنسبة لقانون الإجراءات الجنائية المصري فقد أعطي الحق في المادة رقم ٩٥ "لقاضي التحقيق أن يضبط المراسلات التي تتم عبر البريد أو المحادثات السلكية واللاسلكية أو إجراء تسجيلات في مكان خاص متي رأي أن في ذلك فائدة لظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ٣ أشهر، يجب أن يتم ذلك بناء علي أمر قضائي مسبب ولمدة لا تزيد عن ٣٠ يوماً قابلة للتجديد لمدد أخري". أما في المادة رقم ٩٥ مكرر فقد نص المشرع المصري على منح رئيس المحكمة المختصة الحق في وضع جهاز تليفون شخص محدد تحت المراقبة إذا وقعت دلائل على استخدامه لهذا التليفون في ارتكاب جرائم معينة، فيما منحت المادة ٢٠٦ من قانون الإجراءات الجنائية الصلاحيات السابقة للنيابة العامة ولكن بعد الحصول مقدماً علي أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق.

كذلك فقد نصت المادة ٥٢ من قانون الإجراءات الجنائية المصري "على وضع قاعدة عامة لضمان الأسرار التي تحتويها سائر وسائط وأوعية حفظ وتخزين ونقل المعلومات سواء ما كان منها تقليديا كالأوراق أو مستحدثا كالأقراص المرنة والأشرطة الممغنطة والذاكرات الداخلية للحاسبات وشبكات المعلومات المحلية والإقليمية والعالمية".

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

وعليه فقد امتدت هذه السياسة التشريعية للمشرع المصري على قانون الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣ فيما يتعلق بعدم حماية الحق في خصوصية البيانات الشخصية الإلكترونية بنصوص واضحة وصريحة فلم يجرم المشرع المصري بنصوص واضحة مراقبتها، كل ما هناك فقط أن تم منح الجهاز القومي لتنظيم الاتصالات سلطة وضع بعض القواعد التي تتعلق بالحق في الخصوصية باعتباره من التصرفات والأعمال اللازمة لتحقيق أهدافه وذلك بنص البند ٦ من المادة الخامسة والتي نصت على أن للجهاز في سبيل تحقيق أهدافه أن يباشر التصرفات والأعمال اللازمة لذلك. وله على الأخص ما يأتي ٦ – وضع القواعد التي تضمن حماية المستخدمين بما يكفل سرية الاتصالات وتوفير أحدث خدماتها بأنسب الأسعار مع ضمان جودة أداء هذه الخدمات، وكذلك وضع نظام لتلقى شكاوى المستخدمين والتحقيق فيها والعمل على متابعتها مع شركات مقدمي الخدمة.

ويتضح من ذلك النص انه نص عام وعابر يمثل سلطة للجهاز أكثر من كونه حق للمستخدمين، فلا يتضمن حماية واضحة للحق في خصوصية البيانات الشخصية للمستخدم لشبكة الاتصالات أو الوسائل الإلكترونية الحديثة من شبكات الانترنت والترددات السلكية واللاسلكية.

بينما نصت المادة ٢٥ في البند رقم ١٩ منها على "أن يحدد الترخيص الصادر التزامات المرخص له والتي تشمل على الأخص ما يأتي: – ضمان سرية الاتصالات والمكالمات الخاصة بعملاء المرخص له ووضع القواعد اللازمة للتأكد من ذلك. وهو كذلك نص مرن وعابر لم يحدد إجراءات خاصة يجب على الشركات التي تحصل على تراخيص والتي تقديم خدمات الاتصالات الالتزام بها لضمان حماية خصوصية العملاء في بياناتهم الشخصية".

وفي النهاية نستطيع الجزم بأن قانون تنظيم الاتصالات قد اتى في مجمله متجاهلا النص على حماية الحق في خصوصية البيانات الشخصية للمستخدمين لشبكة الاتصالات. ويرجع ذلك إلى أن الفلسفة التي يقوم عليها قانون تنظيم الاتصالات المصري لا تكترث بأي حال من الأحوال بحماية الحق في خصوصية البيانات الشخصية بقدر اهتمامها أكثر بضمان إمكانية السلطات العامة في الوصول للمعلومات والبيانات التي تريدها وهو ما يظهر جلياً في نص المادة ٦٤ من قانون تنظيم الاتصالات التي الزمت مقدمي خدمات الاتصالات والمستخدمون بعدم استخدام أنظمة التشفير في اتصالاتهم، فضلاً عن إنها أجبرت مقدمي الخدمات علي توفير الإمكانيات اللازمة للحصول علي البيانات لأجهزة الأمن القومي، والقوات المسلحة، كما خول القانون لمقدمي خدمات الاتصالات الحصول علي بيانات شخصية دقيقة خاصة بالمستخدمين ، وهو ما يحدث فعلياً بناءً علي تعليمات من الجهاز القومي لتنظيم الاتصالات.

وتأكيداً على ذلك فقد نصت المادة ٦٤ من قانون تنظيم الاتصالات على انه "يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز والقوات المسلحة وأجهزة الأمن القومي، ولا يسرى ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني. ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة، كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق

تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة".

وتأسيسا على ما سلف فقد أبرمت حكومتي جمهورية مصر العربية ورومانيا اتفاق التعاون في مجال مكافحة الجريمة في ٢٠٠٣/١٢/٣، وبمطالعة نصوص الاتفاق يتبين تبادل دولي للمعلومات وبيانات عن الأشخاص المتورطين في أنشطة وجرائم الجماعات والمنظمات الإرهابية وإنتاج وتهريب المخدرات. وقد اشترط بند (و/١٠) "علي مراعاة مجموعة قواعد لحماية البيانات الشخصية يتعهد الطرفان المتعاقدان الالتزام بها وعدم الاخلال بها وهي كالتالي: في سائر حالات نقل البيانات الشخصية يتولى الطرف المتعاقد المصدر إخطار الطرف المتعاقد المتلقي بالمدة الزمنية المحددة لاستخدام البيانات التي ينبغي عقب انقضائها محو تلك البيانات وفقا لتشريعاته الوطنية بصرف النظر عن المدة الزمنية المحددة ، ويجب محو أية بيانات شخصية متعلقة بأي شخص في حالة انعدام سبب حفظها، ويجب إخطار الطرف المتعاقد المصدر بأية عملية محو لمثل هذه البيانات وأسباب هذا المحو ، وحال إنهاء العمل بهذا الاتفاق يجب تدمير كافة البيانات المتلقاه وفقاً لأحكامه".

ومن جمع ما سبق يستنتج أن هناك قصور تشريعي في مجال الحماية القانونية للحق في خصوصية البيانات الشخصية وخاصة التي تم معالجتها إلكترونياً، وفي نفس الحال ينطبق على غالبية التشريعات العربية التي تعتمد علي النص علي حرمة الحياة الخاصة في الدستور وفي مواد بقانون العقوبات، بحيث تبقى تلك النصوص القانونية نصوص متفرقة تعالج بعض أوجه الخصوصية في مجالات محددة، دون أن تفرد قانوناً خاصاً يحمي خصوصية البيانات الشخصية التي يتم معالجتها إلكترونياً باستثناء بعض الدول مثل تونس والمغرب وقطر فقد أفردوا قانون خاص لحماية خصوصية البيانات الشخصية. وبناء على ما سبق نجد أن المشرع المصري في حاجة إلى استحداث قانون خاص لحماية البيانات الشخصية التي يتم معالجتها إلكترونياً وذلك لمواكبة العصر

الحديث الذي أصبح فيه التعامل الإلكتروني هو السائد فيتم استخدام وتخزين ونقل ومعالجة البيانات والمعلومات الشخصية من خلال الشبكات الإلكترونية ومواقع التواصل الاجتماعي.

لكن مع إصدار المشرع المصري في ١٤ أغسطس ٢٠١٨، قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، فقد تغيير وضع المشرع المصري وأصبح يمثل الاتجاه الثالث من التشريعات التي تنص في قوانين خاصة متعلقة بالجرائم الإلكترونية على حماية خصوصية البيانات الشخصية المعالجة إلكترونياً(١)، فقد نص في المادة ١٣ من هذا القانون على تجريم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، كما نص في المادة ١٤ على جريمة الدخول غير المشروع سواء كان الدخول عن طريق العمد أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. كذلك جرم المشرع المصري في المادة ١٥ من نفس القانون تجاوز حدود الحق في الدخول من حيث الزمان أو مستوى الدخول. هذا وقد فرق المشرع المصري في التجريم ما بين الدخول غير المشروع والاعتراض غير المشروع، فنص في المادة ١٦ من قانون مكافحة جرائم تقنية المعلومات على تعريف الاعتراض غير المشروع بأنه كل اعتراض بدون وجه حق لأي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها.

بالإضافة إلى ذلك جرم المشرع المصري في المادة ٢٥ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ "كل من اعتدى على أي من المبادئ أو القيم

---

(١) – قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ ، صدر في ١٤ أغسطس ٢٠١٨ ، الجريدة الرسمية لجمهورية مصر العربية ، العدد ٣٢ مكرر (ج) ، ص ٣.

الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة". كذلك نصت المادة ٢٦ من نفس القانون على "تجريم كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".

إلا أنه على الرغم من هذا المجهود التشريعي الواضح من المشرع المصري في سد ثغرة خطيرة تهدد خصوصية البيانات الشخصية خاصة التي تم معالجتها إلكترونياً، إلا أننا نري أن المشرع المصري يجب أن يحذوا اتجاه التشريعات الحديثة في وضع تشريع خاص لحماية خصوصية البيانات الشخصية المعالجة إلكترونيا، وإلا يكتفي بمجرد وضع بعض النصوص لحماية هذه البيانات الشخصية في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

ثانيا. موقف المشرع المصري بعد قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠:

نتيجة للانتقادات التي وجهت للمشرع المصري لعدم وجود تشريع خاص لحماية البيانات الشخصية، مما يشكل معه عائق أمام ملاءمة تطورات العصر الحديث، فقد أصدر المشرع المصري في ١٥ يوليه ٢٠٢٠ قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ والذي نص فيه على مجموع من الالتزامات فيما يتعلق بالمعالجة للبيانات الشخصية على المتحكم والحائز والمعالجة ونص على حماية هذه البيانات الشخصية

في جميع مرحلها منذ لحظة الجمع أو التسجيل والحفظ والتخزين والدمج والتعديل، والاسترجاع والتحليل لهذه البيانات الشخصية إلى مرحلة الاستخدام سواء جزئياً أو كلياً. كذلك نص المشرع المصري على أنشاء مركز لحماية البيانات الشخصية كهيئة اقتصادية تتبع الوزير المختص، تهدف لحماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، وإصدار التراخيص والتصاريح والموافقات والتدابير المختلفة المتعلقة بحماية البيانات الشخصية.

الاتجاه الثاني من التشريعات. ويذهب هذا الاتجاه إلى وضع تشريع خاص لحماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً مثال على ذلك التشريع الفرنسي بالنسبة للتشريعات اللاتينية والتشريع الانجليزي بالنسبة للتشريعات الانجلوسكسونية. أما بالنسبة للتشريعات العربية التي نحت إلى الأخذ بهذا الاتجاه هي تونس والمغرب وقطر.

بالنسبة لموقف المشرع الفرنسي فأول الأحكام اعترافا بحق الخصوصية في فرنسا هو القرار الصادر من محكمة السين في ١٦ يونيه ١٨٥٨ بخصوص قضية راشيل(١). وقد تعاقبت الدساتير الفرنسية في النص على احترام مظاهر الحق في الخصوصية وحمايتها من دستور ١٩٢٣ حتي دستور ١٩٥٨ وتعديلاته ، جميعها نادت بعدم المساس بالحقوق الفردية وهذا يعني احترام المجلس الدستوري الفرنسي لحياة الأفراد الخاصة بشكل عام ، وخصوصاً بعد أن طعن أمامه أكثر من مرة بأن القانون لم يحترم الحق في الخصوصية ، فعلى سبيل المثال صدر قرار في ١٢ يناير ١٩٧٧ ، بعدم

---

(١) – محكمة السين الابتدائية ، بتاريخ ١٦ يوليو ١٨٥٨ ، قضية راشيل ، "وتتلخص وقائع القضية في أن أسرة الممثلة الفرنسية الشهيرة راشيل قد أقامت في النصف الثاني من القرن التاسع عشر الميلادي دعوى ضد إحدى الصحف التي التقطت لها صوراً فوتوغرافية بعد موتها مسجاه على فراشها قبل دفنها ، فقرت المحكمة بأنه لا يجوز لأحد دون موافقة المتوفاة وورثتها التقاط صوراً فوتوغرافية لها مهما كانت شهرتها الفنية ، حتي ولو كان الغرض من التصوير إعداد برنامج كامل عن تاريخ حياتها".

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

دستورية نص يخول مأمور الضبط القضائي ومساعديه اقتحام الحياة الخاصة ، بوصفه مخالفاً للحق في الحرية الشخصية إلا أنه قرر في ١٩٩٦ دستورية النص الذي يجيز التفتيش في مجال البحث عن مرتكبي جرائم الإرهاب طالما كان هذا البحث لازماً لحماية المبادئ والحقوق ذات القيمة الدستورية(١)، وعليه يجيز المشرع الدستوري الفرنسي استثناءً من الأصل في حماية الحق في خصوصية البيانات الشخصية سواء كانت في صورتها التقليدية أم كانت إلكترونية ولكن بشرط أن يكون ذلك لازما لحماية المبادئ والحقوق ذات القيمة الدستورية وعلى السبيل المثال على ذلك حالات مكافحة الإرهاب لحفظ أمن الدولة.

وعليه فقد اهتمام المشرع الفرنسي بالحق في الخصوصية فذهب إلى أن الامور التي تدخل في نطاق الحياة الخاصة هي الأمور التي تتعلق بالحياة العائلية، كالبنوة والزواج والطلاق والحياة العاطفية والصورة والذمة المالية وما يدفعه الشخص من ضرائب وكذلك الحق في الاسم والصوت والشرف والاعتبار وسيرة حياته وجوانب حياته المهنية غير المعلنة وحياته الشخصية، أي الحياة التي يعيشها الشخص عندما يغلق على نفسه باب منزله. وتطبيقا على ذلك فقد استقر القضاء الفرنسي على مجموعة من المبادئ القانونية فيما يتعلق بالحق في الخصوصية وهي كالتالي(٢) :

١- يعتبر من قبيل المساس بالحق في الخصوصية نشر كل ما من شأنه الكشف عن الذمة المالية للشخص.

---

(١) - J. RIVERO, Le conseil constitutionnel et les libertés, Paris, ١٩٨٤, pp. ٧١ - ٨٥.

(٢) - انظر: د. محمد ثامر مخاط ، الحماية القانونية القضائية لحق الانسان في الخصوصية ، جامعة ذي قار ، الجزائر، موقع الحوار المتمدن ، ٢٠١٥.

٢- لا يجوز نشر ما يتصل بصحة الشخص وما بها من أمراض إلا بعد الحصول على إذنه.

٣- عدم جواز نشر العلاقات العاطفية لفتاة صغيرة السن أو ما يتعلق بعلاقة الرجل بزوجته.

٤- كذلك تعتبر من المسائل التي تدخل في نطاق الحياة الخاصة للشخص ومن ثم لا يجوز الكشف عنها إلا بعد الحصول على إذنه الآراء السياسية للمواطن والتي يحميها القانون عن طريق سرية التصويت.

٥- لا يجوز إلزام الشخص بأن يظهر ديانته في سجل الفندق باعتبار أن من حق الشخص أن يحتفظ بعقيدته لنفسه.

وفي مجال حماية البيانات الشخصية المعالجة إلكترونياً فقد نص المشرع الفرنسي في المادة الأولى من القانون رقم ١٧ الصادر في ٦ يناير ١٩٧٨ المتعلق بحماية البيانات الشخصية على أن المعلومات في خدمة الفرد، ويجب أن لا تمس بحقوق الإنسان، وبالحياة الخاصة، وبالحريات الفردية والعامة.

وفضلا عن ذلك فقد نصت المادة ٦ من قانون الفرنسي المتعلق بحماية البيانات الشخصية على هذه الحماية، حيث اشترطت أن تجمع وتعالج البيانات الشخصية الخاضعة للمعالجة بطريقة مشروعة وقانونية ولغاية معينة وصريحة ومشروعة كذلك، وألا تتم المعالجة بعد ذلك إلا من أجل هذه الغاية المحددة لها، وفي هذه الحالة يجب أن تكون صحيحة وكاملة، وفقا لما تقتضي الحالة، وأن تحفظ بشكل يمكن من إظهار شخصية الفرد المعني بالأمر، ولمدة لا تفوق المدة الضرورية لتحقيق الغاية التي جمعت وعولجت من أجلها. أما المادة ٧ فاشترطت أن تسبق أية معالجة للبيانات الشخصية

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

الحصول على موافقة الشخص المعني بهذه البيانات، وأن تتوافر شروط أخرى كاحترام الالتزام القانوني المفروض على المسئول عن المعالجة أو حفظ الحياة الخاصة للفرد المعني أو تنفيذ خدمة عامة من طرف المسئول عن المعالجة أو مستقبلها بشرط مراعاة مصلحة الفرد المعني إلى جانب الحقوق والحريات الأساسية.

بالإضافة إلى ذلك فقد فرضت المادة ٣٥ على المسئول عن المعالجة اتخاذ كل الاحتياطات الضرورية للحفاظ على البيانات الشخصية، وعدم إفشائها للغير والحيلولة دون تغيير شكلها أو الإخلال بها أثناء المعالجة، أما المادة ٣٦ فنصت على منع حفظ البيانات الشخصية بعد المدة المحددة إلا من أجل غايات إحصائية أو علمية أو في حالة ترخيص الفرد أو رخصة اللجنة الوطنية للمعلوماتية والحريات CNIL.

وعليه فقد أعطت المادة ٣٩ للفرد حق مساءلة القائمين على معالجة بياناته الشخصية عن نوعية هذه البيانات والغاية من معالجتها وعن الأشخاص المستقلين لهده البيانات، كما يمكن له الحصول على نسخة من هذه البيانات. ونصت مواد الباب الثالث من هذا القانون على تشكيل لجنة إدارية مستقلة تسمى CNIL "اللجنة الوطنية للمعلومات والحريات Commission nationale de l'informatique et des libertés وهي مكلفة على السهر على مراقبة تنفيذ أحكام القانون حماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨ وقد حددت المادتان ٦ و٧ طريقة مراقبتها والعقوبات التي يمكن أن تقررها.

وبالإضافة إلى ما سبق فقد نص المشرع الفرنسي بالقانون رقم ١٩٨٨ الصادر في ٥ يناير ١٩٨٨ على أضافة باب جديد في قانون العقوبات الفرنسي يتعلق بالجرائم المعلوماتية. ويلاحظ أن هذه الجرائم الجديدة تتجه في حقيقتها إلى فكرة الحماية الجنائية

المتكاملة لمعالجة البيانات الشخصية الإلكترونية(١). كذلك يجرم المشرع الفرنسي مجرد الدخول أو التسلل غير المشروع إلى نظام المعالجة الإلكتروني ، كما يجرم البقاء غير المشروع في نظام المعالجة الإلكترونية(٢).

وكذلك فقد نص المشرع الفرنسي في قانون العقوبات على تطبق أحكاما جنائية صارمة لحماية الحق في الخصوصية في المواد ٢٢٦ – ١ إلى ٧ من قانون العقوبات. حيث تنص المادة ٢٢٦ – ١ على أنه تعتبر جريمة يعاقب عليها القانون بالسجن لمدة تصل إلى عام والغرامة المالية التي تبلغ مقدارها ٤٥٠٠٠ يورو كل انتهاك عمدي للحياة الخاصة للغير بدون موافقته عن طريق ما يلي:

١. اعتراض أو تسجيل أو نقل كلمات قالها بثقة أو في ظروف خاصة؛

٢. أخذ أو تسجيل أو نقل صورة الشخص في مكان خاص ولكن تفترض الموافقة عند تنفيذ هذه الإجراءات على مسمع أو مرأي من الشخص دون اعتراضه مع تمكنه من الاعتراض. كل هذه الأحكام مقصورة على أنها تستهدف في الأساس المصورين للشخصيات البارزة.

---

(١) – J. DEVEWE; Infraction en matière informatique, N° ٣١-٣٣, ١٩٨٨-٩-٤٦٢, jurissclasseur pénale, art. ٣٦٢-٢ Chamoux: la loi sur la fraude informatique, de nouvelles incrimination, J.C.P, ١٩٨٨, I. DOCT, P. ٣٣٢١; R. GASSIN, La protection pénale d'une universalité de fait en droit français, Act. Legis. Dalloz, N°٤٥, ١٩٨٨, P. ١٢. د. على عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونياً ، بحوث مؤتمر القانون والكمبيوتر والانترنت ، بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة المجلد الثاني من ١ إلى ٣ مايو ٢٠٠٠ ، جامعة الإمارات العربية المتحدة ، كلية الشريعة والقانون ، الطبعة الثالثة ، ٢٠٠٤ ، ص ٦١٤ ، ٦١٥.

(٢) – H. CROZE, L'apport du droit pénal à la théorie général propos de la loi N° ٨٨-١٩ DU DROIT DE L'informatique ٥ jan ١٩٨٨ relative à la fraude informatique, éd, J.C.P, ١٩٨٨, I. doct, p. ٣٣٣٣.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

ولذلك فقد أصدر المشرع الفرنسي العديد من التشريعات التي يمكن من خلالها توفير حماية للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، منها كذلك القانون رقم ٥٧٥ الصادر في ٢١ يونية ٢٠٠٤ بشأن الثقة في الاقتصاد الرقمي(١)، والذي يجرم من خلالها مخاطر البريد الإلكتروني المزعج والذي ينتهك الحق في الخصوصية. وعليه وفي ٦ اغسطس عام ٢٠٠٤ أصدر المشرع الفرنسي تعديلاً على القانون رقم ١٧ لسنة ١٩٧٨ الخاص بحماية البيانات الشخصية وذلك بموجب القانون رقم ٨٠١ لسنة ٢٠٠٤. وقد جاء التعديل الجديد بتعريف موسع ومرن للبيانات الشخصي محل الحماية القانونية على عكس القانون القديم الذي كان يعرفها في المادة الرابعة منه بأنها أي معلومات تسمح بطريقة مباشرة أو غير مباشرة بتحديد هوية الأشخاص الطبيعيين.

ومما سبق يتضح لنا أن المشرع الفرنسي قد انشأ اللجنة القومية للمعلوماتية والحريات CNIL بمقتضي القانون رقم ١٧ لسنة ١٩٧٨ لتلعب دور محوري في حماية حقوق الأفراد وحرياتهم ، من خلال حماية البيانات الشخصية ، وبتعديل القانون الفرنسي الصادر في ٦ أغسطس ٢٠٠٤ بالقانون رقم ٨٠١ لسنة ٢٠٠٤ فقد توسع المشرع في سلطات اللجنة القومية للمعلوماتية والحريات فخولها سلطة إصدار تعليمات ومعايير متعلقة بمعالجة البيانات الشخصية، وعلى من يقوم بمعالجة البيانات باحترام هذه التعليمات والمعايير وإلا ترتب على ذلك عقابه بالسجن لمدة خمس سنوات وبالغرامة المالية التي تبلغ مقدارها ٣٠٠.٠٠٠ ألف يورو ، سواء كانت مخالفة هذه التعليمات بقصد أم بدون قصد، وذلك وفقا لنص المادة ٢٢٦-١٦-١-أ من قانون العقوبات الفرنسي. بالإضافة إلى ذلك فإن المادتين ٤٥ و٤٧ من قانون حماية البيانات الشخصية

---

(١)- Solanki Jigar et Akpakpo Brune, Authentification d'utilisateur, Gestion des Identites, Universite Sciences et Technologies, Bordeaux I, ٣٥١ Cours de la lib eration, ٣٣٤٠٠ talence. Decembre ٢٠٠٧, p.٦.

أعطت للجنة سلطة إنذار القائم بمعالجة البيانات الشخصية، وذلك في حالة مخالفته لأي التزام وارد في القانون – بالتوقف عن المعالجة، فإذا لم يتوقف كان للجنة الوطنية للمعلوماتية والحريات CNIL الحق في توقيع عقوبة الغرامة المالية عليه والتي تبلغ مقدارها ١٥٠.٠٠٠ ألف يورو، ويشدد العقاب لتصبح الغرامة المالية التي تبلغ مقدارها ٣٠٠.٠٠٠ ألف يورو في حالة تكرار المخالفة.

بالإضافة إلى ذلك فقد نص المشرع الفرنسي في قانون العقوبات على توقيع عقوبة السجن لمدة خمس سنوات والغرامة المالية التي تبلغ مقدارها ٣٠٠.٠٠٠ ألف يورو على معالج البيانات الشخصية في حالة عدم توقفه عن المعالجة بعد إنذار اللجنة له بذلك، سواء أكان عدم التوقف بقصد أم بدون قصد. كذلك تنص المادة ٣٢٣ –٢ من قانون العقوبات الفرنسي المعدلة بالقانون رقم ٥١٢ لسنة ٢٠١٥ الصادر في ٢٤ يوليه ٢٠١٥ على انه يعاقب المشرع على كل فعل يعرقل أو يعطل نظم المعالجة الآلية للبيانات بالسجن خمسة سنوات وبالغرامة المالية التي تبلغ مقدارها ١٥.٠٠٠ ألف يورو، ويشدد المشرع الفرنسي العقوبة لتصل إلى السجن سبع سنوات والغرامة المالية والتي تبلغ مقدارها ٣٠.٠٠٠ ألف يورو إذا وقع الاعتداء على نظم المعالجة الآلية للبيانات الشخصية التي تدار بواسطة الدولة. كأن يتم عرقلة أو تعطيل نظم المعالجة الآلية للبيانات عن طريق إدخال الجاني لبرامج ضارة أو فيروسات داخل تلك النظم مما يترتب عليه إعاقة عملها.

هذا وقد تم ادخال العديد من التعديلات على القانون الفرنسي الخاص بحماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨ ومنها التعديل بالقانون رقم ٨٠١ لسنة ٢٠٠٤، والتعديل بالقانون رقم ١٣٢١ لسنة ٢٠١٦ الصادر في ٧ أكتوبر ٢٠١٦، والقانون رقم ٥٥ الصادر في ٢٠ يناير ٢٠١٧، والتعديل بقانون رقم ٤٩٣ الصادر في ٢٠ يونية

٢٠١٨ وهو التعديل الجديدة لملاءمة اللائحة العامة الاوربية لحماية البيانات الشخصية رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨.

كذلك من التشريعات التي حرصت على حماية البيانات الشخصية المعالجة إلكترونيا كذلك التشريع الاسباني حيث نص في الفقرة الرابعة من المادة ١٨ من الدستور الصادر في ٩ ديسمبر١٩٧٨، على أن القانون هو الذي يحدد البيانات التي تخضع للمعالجة الإلكترونية لضمان الكرامة والحصانة الشخصية والأسرية للمواطنين في ممارستهم لحقوقهم.

أما بالنسبة لموقف المشرع البرتغالي فقد نص في الفقرة الأولى من المادة ٣٥ من الدستور البرتغالي الصادر في ٢ ابريل ١٩٧٦، على أن يكون لكل المواطنين الحق في معرفة المعلومات التي تتعلق بهم وما تتضمنه بنوك المعلومات من بيانات خاصة بهم والاستخدامات المعدة لها، ويكون لهم طلب تصحيحها أو تصويبها أو الإضافة إليها كل فقرة عندما يطرأ عليها تغيير. أما الفقرة الثانية من الدستور البرتغالي فنصت على انه لا يجوز استخدام الحواسيب الإلكترونية في معالجة البيانات التي تتعلق بالاتجاهات السياسية أو المعتقدات الدينية أو الحياة، عدا البيانات التي تتعلق بالتعداد السكاني أي بقصد إجراء إحصاء للسكان، والبيانات غير الشخصية.

أما بالنسبة لموقف المشرع الإنجليزي بالنسبة لحماية خصوصية البيانات الشخصية وخاصة البيانات التي تم معالجتها الكترونياً، فقد أصدر المشرع الانجليزي في عام ١٩٨٤ قانون حماية البيانات الشخصية والذي يشتمل على المبادئ التالية:

١. مبدأ ضرورة الحصول على البيانات الشخصية المخزنة لأغراض المعالجة بأسلوب صحيح ولتحقيق أغراض مشروعة.

٢. مبدأ الحفاظ على تلك البيانات الشخصية في نطاق أهداف محدودة.

٣. مبدأ عدم جواز استخدام البيانات الشخصية إلا للغرض المحدد لها ولا يجوز الكشف عنها إلا بما يتفق مع ذلك الغرض المحدد لها.

٤. مبدأ عدم تعدى الاستخدام للبيانات الشخصية للغرض المحدد لها.

٥. مبدأ توفير حق الاطلاع للفرد على بياناته الشخصية مع السماح له بحق التصحيح له بإجراء أي تعديلات لازمة لها.

٦. مبدأ حفظ البيانات الشخصية بصورة آمنة تحميها من عمليات الدخول غير المشروع كما تحميها من الفقد.

وهكذا يتبين مما سبق أن المشرع الإنجليزي في قانون حماية البيانات الشخصية قد استثنى من تطبيق هذا القانون البيانات الشخصية المختزنة المتعلقة بالرواتب، والمعاشات، وبيانات الحسابات، علاوة على الأسماء والعناوين المخصصة لأغراض توزيع المعلومات مثل اتحاد البريد. وكذلك في حالة جمع البيانات الشخصية لأغراض التحقيق أو الأغراض الإحصائية فقط، أو حفظها كنسخة اضافية مجردة

وقد نص المشرع الإنجليزي في قانون حماية البيانات الشخصية الصادر في عام ١٩٨٤ على أساليب لحماية البيانات الشخصية وهي على النحو التالي:

١. الحماية للبيانات الشخصية عن طريق باسورد أو كلمة السر: حيث يتم تخزين أسماء المستخدمين وكلمات المرور في جداول، وتحفظ هذه الجداول بشكل دائم على ملف موجود على أسطوانة. ويجب إلا تكون جداول كلمات المرور مشفرة على نحو لا يمكن تعديلها وذلك لتجنب أي اختراق لخصوصية هذه البيانات الشخصية.

٢. الحماية للبيانات الشخصية عن طريق التشفير: حيث يتم حماية خصوصية البيانات الشخصية عن طريق التشفير من خلال تحويل الرسالة من نص واضح مقروء إلى نص

مشفر غير مقروء، ويتم إرسال الرسالة المشفرة عبر قناة اتصال، حيث يقوم الجهاز الإلكتروني المتلقي بفك شفرة هذه الرسالة بعد ذلك لتصبح رسالة مقروءة.

٣. طرق حماية البيانات الشخصية الأخرى: حيث يمكن حماية خصوصية البيانات الشخصية عن طريق وسائل أخرى متعددة يتم من خلالها وضع نظام للتعرف على المستخدم المصرح له بالدخول لقاعدة البيانات وذلك عن طريق([1]):

A. التعرف على بصمة العين.

B. التعرف على بصمات الأصابع.

C. التعرف على الصوت.

D. التعرف على الوجه.

وعليه فقد قام المشرع الانجليزي في عام ١٩٩٨ بتعديل القانون الصادر في عام ١٩٨٤ وتم تسمية جهة الرقابة على حماية البيانات الشخصية بمفوض حماية البيانات في أعقاب قانون حماية البيانات الشخصية الانجليزي الصادر في عام ١٩٩٨ بدلاً من مفوض تسجيل البيانات الذي أنشئ بموجب قانون حماية البيانات الصادر عام ١٩٨٤. كذلك وبموجب قانون حرية المعلومات الانجليزي الصادر في عام ٢٠٠٠ جري تعديل قانون ١٩٩٨ فتم إعادة تسمية مفوض حماية البيانات ومحكمة البيانات المنشأتين بموجب قانون ١٩٩٨ ليصبحا مفوض المعلومات ومحكمة المعلومات وتم اسناد اختصاصات تتعلق بالحقين معا حق حماية خصوصية البيانات الشخصية وحق حرية

([1]) – د. عبد الله حسين على محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الثانية ، الامارات العربية المتحدة ، دبي ، دار النهضة العربية ، القاهرة ، ٢٠٠٢ ، ص ٣٢١ ، ٣٢٢.

المعلومات أي حق الوصول للمعلومات والسجلات وهو توجه أريد منه إيجاد جهة واحدة للحفاظ على معيار التوازن بين الحقين(١).

أما بالنسبة لموقف المشرع التونسي فقد افرد المشرع حماية خاصة للمعطيات الشخصية في مواجهة التطور التقني في المواد من ١٨ إلى ٤٢ من قانون التجارة الإلكترونية الصادر في عام ٢٠٠٠، وفرض عقوبات أصلية وتكميلية على الأفعال التي تقع بالمخالفة لتلك المواد. ثم أصدرت تونس قانون رقم ٦٣ لسنة ٢٠٠٤ الخاص بحماية المعطيات الشخصية، وبموجب هذا القانون أصبح يحظر جمع البيانات الشخصية إلا في أغراض مشروعة ومحددة وواضحة، واشترط القانون وجوب أخذ موافقة الشخص المعني بالأمر، وأناط القانون إلى الهيئة الوطنية لحماية المعطيات الشخصية منح تصاريح الحصول على البيانات. واشترط القانون أن تكون البيانات المجمعة بغرض تحقيق مصلحة حيوية للشخص المعني بالأمر أو لأغراض علمية ثابتة، كما اشترط القانون لإجراء عملية معالجة البيانات الشخصية ضرورة استخراج تصريح مسبق يودع بمقر الهيئة الوطنية لحماية المعطيات الشخصية.

وعليه تتمتع الهيئة الوطنية لحماية المعطيات الشخصية بالشخصية المعنوية والاستقلال المادي، وتتكون من قضاة وممثلين لوزراء الداخلية، والدفاع، والتعليم العالي، والصحة، وخبراء في مجال الاتصال، هذا بجانب أعضاء يتم اختيارهم من مجلس النواب والشخصيات المتصلة بالمجال، وتقدم الهيئة تقرير سنوي لرئيس الجمهورية. كما نص القانون على حزمة من المحظورات وهي:

(١) – J. MAC DONALD, The law of freedom of information, BBC Press, ٢٠٠٣, p. ٤٠.

١- يحظر معالجة البيانات الشخصية المتعلقة بطفل إلا بعد أخذ موافقة وليه وإذن قاضي الأسرة، ويجوز لقاضي الأسرة أن يصرح بمعالجة البيانات بدون موافقة الولي إذا اقتضت مصلحة الطفل الفضلى ذلك، وللقاضي الرجوع في الإذن.

٢- ويحظر استعمال البيانات الشخصية لأغراض دعائية إلا بموافقة صريحة وخاصة من الشخص المعني بالأمر.

أما بالنسبة لموقف المشرع المغربي: فقد أصدر المشرع المغربي قانون حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي في عام ٢٠٠٩، حيث وضع القانون إجراءات للحفاظ علي سرية المعطيات للأشخاص، وأوجب القيام بإجراءات تقنية وتنظيمية ملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف أو الإذاعة. بالإضافة إلى حمايتها من أي شكل من أشكال المعالجة غير المشروعة. يشترط القانون الحصول على إذن مسبق من اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي لمعالجة المعطيات، ويمنح هذا الإذن بناء على موافقة الشخص المعني.

وكذلك يعطي القانون المغربي لحماية الأشخاص الذاتيين للشخص المعني الحق في الحصول على تأكيد بأن المعطيات ذات الطابع الشخصي المتعلقة به تعالج أو لا تعالج، كما يحق للشخص المعني أن يتقدم بطلب للمسئول عن المعالجة لتصحيح المعطيات أو محوها. وتتألف اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي من ٧ أعضاء وهم على النحو التالي:

١- رئيس اللجنة يعينه الملك.

٢- أعضاء يتم تعينهم من الملك باقتراح من الوزير الأول، رئيس مجلس النواب، رئيس مجلس المستشارين. وتمتد عضوية اللجنة خمس سنوات قابلة للتجديد مرة واحدة.

بالإضافة إلى ذلك فقد نص القانون المغربي كذلك على التزم أعضاء اللجنة الوطنية بكتمان السر المهني، ويحظى الأعضاء والموظفين أو الأعوان العاملين باللجنة بالحماية من خلال توفير الحصانة لهم، فلا يجوز المساس بشخصهم أو أهانتهم ومن يقوم بذلك يضع نفسه تحت طائلة أحكام القانون الجنائي. كما يحظر على المسئول عن المعالجة نقل البيانات الشخصية إلي دولة أجنبية إلا إذا كانت هذه الدولة تضمن مستوي حماية كاف للحياة الشخصية وللحريات والحقوق الأساسية للأشخاص، وتعد اللجنة الوطنية قائمة الدول المتوفر فيها تلك المعايير وذلك بعد إجراء تقييم كافي لبيان مستوي الحماية الذي تضمنه دولة معينة، وإجراءا ت الأمن التي تطبق فيها، واستثني القانون نقل المعطيات ذات الطابع الشخصي إلى دولة لا تتوفر فيها الشروط السابقة في حال الموافقة الصريحة للشخص الذي تخصه المعطيات، أو في الحالات التالية :

أ) إذا كان النقل ضرورياً من أجل المحافظة علي حياة الشخص المعني، أو المحافظة على المصلحة العامة، أو تنفيذاً لإجراء متعلق بتعاون قضائي دولي، أو الوقاية من إصابات مرضية.

ب) إذا كان النقل يتم تنفيذ لاتفاق ثنائي أو متعدد الأطراف يكون المغرب عضواً فيه.

ج) بناء على إذن صريح ومعلل للجنة الوطنية.

وعليه فقد خصص القانون المغربي الباب السابع للعقوبات في حال مخالفة أحكامه، فقرر المعاقبة بالحبس من ثلاثة أشهر إلى سنة وبغرامة من ٢٠.٠٠٠ إلي ٢٠٠.٠٠٠ درهم أو بإحدى هاتين العقوبتين لكل من يقوم بجمع معطيات ذات طابع شخصي بطريقة تدليسيه، أو أنجز معالجة المعطيات بطريقة غير نزيهة أو مشروعة، أو بطريقة متعارضة مع الأغراض المحددة والمعلنة والمصرح بها. كما قرر القانون المعاقبة بالحبس من ستة أشهر إلي سنة وبغرامة من ٥٠.٠٠٠ إلي ٣٠٠.٠٠٠ درهم أو بإحدى هاتين العقوبتين لكل من قام دون الموافقة الصريحة للأشخاص المعنيين؛ بمعالجة معطيات ذات طابع شخصي تبين بشكل مباشر أو غير مباشر الأصول العرقية، أو الآراء السياسية أو الفلسفية أو الدينية أو الانتماءات النقابية للأشخاص المعنيين أو المتعلقة بصحة هؤلاء.

أما بالنسبة لموقف المشرع القطري، فقد أصدر المشرع القطري القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية، وقد نص القانون القطري في المادة الثانية منه "على أنه تسري أحكام هذا القانون على البيانات الشخصية عندما تتم معالجتها على نحو إلكتروني، أو يتم الحصول عليها أو جمعها أو استخراجها على أي نحو آخر تمهيداً لمعالجتها إلكترونياً، أو تتم معالجتها عن طريق الجمع بين المعالجة الإلكترونية والمعالجة التقليدية". ولا تسري أحكام هذا القانون على البيانات الشخصية التي يقوم الأفراد بمعالجتها في نطاق شخصي أو عائلي، أو البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية وفقاً لأحكام القانون رقم ٢ لسنة ٢٠١١ المشار إليه. كما نص في المادة الثالثة على "أنه لكل فرد الحق في حماية خصوصية بياناته الشخصية، ولا يجوز معالجة تلك البيانات إلا في إطار

الشفافية والأمانة واحترام كرامة الإنسان والممارسات المقبولة، وفقاً لأحكام هذا القانون.

كما نص على أنه يجوز للفرد ، في أي وقت، ما يلي([1]) :

١. سحب موافقته السابقة على معالجة بياناته الشخصية.

٢. الاعتراض على معالجة بياناته الشخصية إذا كانت غير ضرورية لتحقيق الأغراض التي جمعت من أجلها، أو كانت زائدة على متطلباتها، أو تمييزية أو مجحفة أو مخالفة للقانون.

٣. طلب حذف بياناته الشخصية أو محوها في الحالات المشار إليها في البندين السابقين، أو عند انتهاء الغرض الذي تمت من أجله معالجة تلك البيانات، أو إذا لم يكن هناك مبرر للاحتفاظ بها لدى المراقب.

٤. طلب تصحيح بياناته الشخصية، مرفقاً به ما يثبت صحة طلبه".

كذلك فقد نص المشرع القطري على أنه مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر، يعاقب بالغرامة المالية التي لا تزيد على (١,٠٠٠,٠٠٠) مليون ريال للمراقب معالجة البيانات الشخصية في حالة المعالجة غير المشروعة.

الاتجاه الثالث من التشريعات. وهو الاتجاه الوسط بين الاتجاه الاول والاتجاه الثاني من التشريعات، حيث لا يضع تشريع شامل جامع لحماية خصوصية البيانات الشخصية الإلكترونية ولكن في نفس الوقت يضع بعض القوانين الخاصة التي تحمي مجال من مجالات البيانات الشخصية، مثال على ذلك التشريع الأمريكي.

([1]) – المادة الخامسة من القانون القطري رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

بالنسبة لموقف المشرع الأمريكي فقد صدرت عدة تشريعات لحماية البيانات الشخصية من أخطار قواعد البيانات ، ومن هذا القوانين الأمر بالقانون رقم٩١-٥٠٨ الصادر في ١٩٧٠ والذي أقر حق الفرد في الوصول إلى البيانات ، والقانون رقم ٩٣-٥٧٩ لسنة ١٩٧٤ والمتعلق بحماية الخصوصية ، ويعد من التشريعات المتقدمة في مجال حماية الحياة الخاصة للأفراد من الإفشاء غير المشروع للمعلومات الخاصة بهم، وقد كان الهدف من هذا القانون تقرير حماية لكل فرد ضد الاعتداءات التي تطال حياته الخاصة، ووضع قواعد لحمايته من الاطلاع غير المشروع على المعلومات الخاصة به والمحفوظة في الكمبيوتر. وكذلك القانون رقم ٥٣ – ٣٨٠ الصادر في ٢١ اغسطس ١٩٧٤ والخاص بإقرار حقوق التربية للأسرة. وبالإضافة إلى ذلك فرض المشرع الأمريكي حماية لخصوصية الأفراد أثناء عمليات الاتصال وتبادل المعلومات من خلال إصداره لقانون خصوصية الاتصالات الإلكترونية الصادر في عام ١٩٨٦.

وبالرغم مما سبق إلا انه يلاحظ بأن قانون الأمن الوطني الأمريكي الصادر في عام ٢٠٠١ أو ما يصطلح عليه بقانون باتريوت، قد ساهم في إضعاف حماية الخصوصية للبيانات والمعلومات الشخصية، لأنه قام بتوسيع مجال تدخل السلطات الأمنية بدافع حماية الأمن القومي الأمريكي. وذلك لأنه جاء في أعقاب هجمات ١١ سبتمبر في الولايات المتحدة الأمريكية. أما قانون جرام- ليش- بلا يلى (Gramm-leach-Billey Act) الصادر في عام ١٩٩٩، فهو قانون يضمن حماية الخصوصية، أثناء تبادل المعلومات بين المؤسسات المالية.

بالإضافة إلى ذلك فهناك قانون الصادر في عام ١٩٩٤ الذي يضمن حماية الخصوصية بالنسبة لسائقي السيارات كما يجرم قانون سجلات التليفون، والحصول على السجلات الخاصة بالهواتف الشخصية وبيعها وشرائها. وبالرغم من ذلك ، فأن هناك

مجهود تشريعي فيدرالي واضح لحماية البيانات الشخصية التي تم معالجتها الكترونياً، فهناك مجموعة من القوانين التي تعمل بها الولايات الأمريكية والتي تهتم بقضايا الخصوصية والانترنت(١).

وكذلك نص المشرع الأمريكي على حماية خصوصية البيانات والمعلومات الشخصية المسجلة في جهات حكومية الصادر تحت عنوان قانون الحكومة الإلكترونية في عام ٢٠٠٢(٢)، بحيث يجب على الحكومة الإلكترونية الأمريكية عند معالجة أو

---

(١) – اعتمدت الولايات المتحدة الامريكي في عام ١٩٩٤ قانون حماية خصوصية السائق استجابة لبيع سجلات السيارات ، بما فيها الكثير من البيانات الشخصية الحساسة – مثل أرقام الهواتف والعناوين والتفاصيل الشخصية والمعلومات الطبية التي ادت على عدد من الجرائم الخطيرة كان من بينها قبل أدى الممثلات الشهيرات. ويجرم قانون سجلات التليفون وحماية الخصوصية لسنة ٢٠٠٦ استخدام ذريعة كاذبة للحصول على أو شراء أو بيع السجلات الهاتفية الشخصية ، في حين أنشأ قانون المعاملات الائتمانية العادلة والدقيقة لسنة ٢٠٠٣ بعض الخصوصية ، مثل الحق في الحصول على تقرير ائتماني مجاني من مكتب الائتمان مرة في السنة. وكان جزءا من استراتيجية شاملة لمواجهة انتحال الهوية. ويشرط قانون حماية خصوصية الأطفال على الانترنت لسنة ٢٠٠٠ (coppa) موافقة أولياء الأمور قبل جمع المعلومات عن الأطفال دون سياسات خصوصية. ومن ثم العمل على أساس نهج يقوم على التنظيم الذاتي. وجاء قانون ضبط هجوم الصور الإباحية وإعلانات التسويق المتطفلة لسنة ٢٠٠٤ (CAN–SPAM ACT) كمحاولة لوضع معايير للرسائل غير المرغوبة، على الرغم من أنه يعتبر ذو تأثير قليل جدا. فهو لا يتطلب موافقة المتلقي للرسالة غير المرغوبة، ولكنه يتطلب قيام المرسل بالإشارة إلى أن هذه الرسالة هي إعلان وتزويد عنوان بريدي صالح للمرسل. وللمستلمين الحق في عدم تلقي الرسالة من خلال إرسال إشعار بذلك. وحتى الآن رفضت الولايات المتحدة الأمريكية، اعتماد قواعد الاحتفاظ بالبيانات على غرار تلك المنصوص عليها في توجيه الاحتفاظ بالبيانات للاتحاد الأوروبي. وقد اقترحت مشاريع قوانين في هذا العدد مثل مشروع قانون منع الانترنيت من تسهيل استغلال البالغين لشباب اليوم لسنة ٢٠٠٩ (SAFETY BILL)، الذي اقترح في عام ٢٠٠٩ ولم يعتمد بها. حيث كان سيتطلب من مقدمي خدمات الاتصال الاحتفاظ لمدة لا تقل عن سنتين "بكافة السجلات أو المعلومات المتعلقة بهوية أي مستخدم لعنوان شبكة تخصصه الخدمة له بصورة مؤقتة.

(٢) – Federal management and promotion of electronic government services accessibility usability and preservation of government information, Title II, The E – Government, U.S.A, ٢٠٠٢, www.justice.gov.

جمع أو استخدام البيانات والمعلومات الشخصية حماية الحق في الخصوصية للمواطن وتأكيد حقه في الاطلاع على المعلومات. الامر الذي يفرض على الحكومة الإلكترونية انشاء نظام قانوني وإداري وتقني لحماية الحق في الخصوصية أثناء فترة معالجة البيانات والمعلومات الشخصية.

وبالإضافة إلى ذلك فقد نص المشرع الأمريكي على حماية خصوصية البيانات الشخصية للأطفال على الانترنت بموجب قانون COPPA الصادر في ٢١ أكتوبر ١٩٩٨ ، ودخل حيز النفاذ في ٢١ أبريل ٢٠٠٠ بحيث يحمي خصوصية البيانات الشخصية لكل طفل لم يبلغ من العمر ١٣عاما، وقد صدرت تعديلات على هذا القانون في ديسمبر ٢٠١٢ ودخلت حيز النفاذ في الأول من يوليو ٢٠١٣، بحيث أضافت شرط اشعار الوالدين للموافقة على أي معالجة للبيانات الشخصية للطفل، وكذلك فرضت التزام على كل موقع إلكتروني أو مقدم خدمة عبر الإنترنت موجهة إلى الاطفال أقل من ١٣ عاما ، بنشر سياسة خصوصية واضحة وشاملة على الإنترنت فيما يتعلق بمعالجة البيانات الشخصية للأطفال أقل من ١٣ عاما.

المطلب الثالث. موقف الشريعة الإسلامية من حماية خصوصية البيانات الشخصية الإلكترونية

مما لا شك فيه أن الشريعة الإسلامية صانت الحياة الخاصة للفرد، فقد نهى الله سبحانه وتعالى عن اقتحام خصوصيات الأشخاص سوء تعلق ذلك ببيانات شخصية عادية أو بيانات شخصية تم معالجتها إلكترونياً ، وذلك مصداقاً لقوله تعالى : [يأيها الذين امنوا اجتنبوا كثيراً من الظن إن بعض الظن إثم ولا تجسسوا ولا يغتب بعضكم

بعضاً أيحب أحدكم أن يأكل لحم أخيه ميتا فكرهتموه واتقوا الله إن الله تواب رحيم (١)]. فإذا كانت الشريعة الإسلامية قد حرمت إفشاء السر الذي يحصل عليه المسلم دون تجسس ، كأن يعرفه من صاحب السر نفسه، فإنها قد حرمت من باب أولى التجسس بطرق خفيه لكشف أسرار الآخرين، ومعرفة خصوصياتهم(٢). سواء كانت هذه المعلومات والبيانات عن الحياة الخاصة موجودة في الصورة التقليدية أو كانت بيانات شخصية تم معالجتها إلكترونياً.

وعليه فالشريعة الإسلامية جعلت حماية الحق في الخصوصية ضرورة إنسانية كباقي الضرورات التي تعد من مقومات التي يقوم عليها المجتمع الإسلامي، لذلك وضعت قواعد كلية لحمايتها تتسم بالشمول لا تتبدل مع تغير الزمان والمكان، قادرة على صون خصوصية الإنسان، وعلى سبيل المثال لذلك قاعدة لا ضرر ولا ضرار. فهذه الحماية تستمد جذورها من القرآن الكريم والسنة النبوية الشريفة(٣)، في تنظيم متكامل لحماية حقوق الانسان.

بالإضافة إلى ذلك فقد نهى الرسول صلى الله عليه وسلم عن انتهاك خصوصيات الناس، وذلك لما ينطوي عليه ذلك من كشف ما أراد الله تعالى ستره على المسلم، ولما فيه من انتهاك لحرمات العباد، وتدخل من الغير فيما لا يعنيه، ومن هنا جاء النهى عن انتهاك خصوصيات الناس حتي يستطيعوا أن يعيشوا آمنين على أنفسهم وعلى

---

(١) – القرآن الكريم ، سورة الحجرات ، الآية ١٢.

(٢) – الأمام الطبري ، محمد بن جرير ، جامع البيان في تأويل القرآن ، تهذيب صلاح الخالدي ، الطبعة الأولى ، دار القلم والدار الشامية ، بيروت ، ١٩٩٧ ، ص ٤٠ ، ٤١.

(٣) – د. عادل بسيوني ، تاريخ القانون المصري ، مصر الإسلامية ، مكتبة نهضة الشرق ، القاهرة ، ١٩٨٥ ، ص ١٠٣ – ١٠٥. ، د. محمد السقا ، فلسفة وتاريخ القانون المصري ومراحل تطوره ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ ، ص ٣٩٨.، د. صوفي أبو طالب ، تاريخ النظم القانونية والاجتماعية ، جامعة القاهرة ، ١٩٧٨ ، ص ٣٨٩.

بيوتهم وعلى حرماتهم وأسرارهم([١]). فإذا كان ذلك فيما يتعلق بحماية الشريعة للحق في الخصوصية في الحياة العادية فإنه من باب أولى يمتد نطاق الحماية للحق في خصوصية البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً، حيث وفر التقدم العملي والتكنولوجي إمكانية الاطلاع على أسرار الحياة الخاصة بالآخرين، بالدخول إلى أخص خصوصيات الإنسان دون أن يشعر وبطريقة خفية. مما يشكل إخلال بحق الإنسان في الحق في خصوصية البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً.

كذلك فقد قررت الأحاديث الكثيرة الواردة عن النبي صل الله عليه وسلم تحريم الاعتداء على الحق في الخصوصية معاقبة من يقوم بذلك ، منها قوله من اطلع في بيت قوم بغير إذنهم ففقؤوا عينه ، فلا ديه ولا قصاص([٢]). كذلك فقد روي عن النبي صل الله عليه وسلم أنه قال من حدث في مجلس بحديث فالتفت فيهي أمانة([٣])، وروى عنه صل الله عليه وسلام قوله المجالس بالأمانة إلا ثلاثة مجالس ما سفك فيه دم حرام، أو فرج حرام، أو اقتطع فيه مال بغير حق([٤]). وعن أبي هريرة رضي الله عنه قال رسول الله صلى الله عليه وسلم إياكم والظن، فإن الظن أكذب الحديث ، ولا تجسسوا ولا تحسسوا

([١]) – انظر : د. حسني الجندي ، ضمانات حرمة الحياة الخاصة في الإسلام ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ١٩٩٣ ، ص ١٦٦.

([٢]) – حديث نبوي رواه أحمد والنسائي ، نيل الأوطار كتاب الدماء باب من اطلع من بيت قوم مغلق عليهم بغير إذنهم.

([٣]) – حدثنا أحمد بن محمد أخبرنا عبدالله بن المبارك عن ابن أبي ذئب قال أخبرني عبد الرحمن بن عطاء عن عبد الملك بن جابر بن عتيك عن جابر بن عبدالله عن النبي صل الله عليه وسلام قال إذا حدث الرجل الحديث ثم التفت فهي امانة قال أبو عسي هذا حديث حسن وانما نعرفه من حديث ابن ابي ذئب.

([٤]) – حديث نبوي ، سنن أبي داود كتاب الأدب في نقل الحديث.

ولا تنافسوا ولا تحاسدوا ولا تباغضوا ولا تدابروا، وكونوا عباد الله إخوانا([1]). وكذلك قوله صلى الله عليه وسلم يا معشر من امن بلسانه ولم يدخل الايمان قلبه، لا تغتابوا المسلمين، ولا تتبعوا عوراتهم ، فإن من اتبع عوراتهم ، يتبع الله عورته ، ومن يتبع الله عورته يفضحه ولو في بيته([2]).

وانطلاقا مما سبق نستنتج أن الشريعة الإسلامية قد أحاطت الخصوصية في المعلومات والبيانات الشخصية سواء كانت في صورتها التقليدية أو كانت في صورة إلكترونية بحماية شاملة وبضمانات حتي لا تكون محلاً للاعتداء عليها من الغير ، وذلك لاتحاد العلة وذلك مصداقا لقولة تعالى : يا أيها الذين آمنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأنسوا وتسلموا على أهلها ذلكم خير لكم لعلكم تذكرون ، فإن لم تجدوا فيها أحدا فلا تدخلوها حتى يؤذن لكم وإن قيل لكم ارجعوا فأرجعوا هو أزكى لكم والله بما تعملون عليم([3]).

وعليه فالشريعة الإسلامية حرمت الدخول إلى المسكن دون إذن أصحابها، ولكن في الوقت نفسه بينت مشروعية الاقتراب منها ودخولها عن طريق الاستئناس، كما حرمت إفشاء الحديث والإسرار الخاصة ودعت إلى حفضها، فضلا عن تحريم الوصول إلى الإسرار والمعلومات والبيانات الشخصية عن طريق التطفل والتجسس لأي سبب كان([4]). وبالتالي تمتد الحماية في الشريعة الإسلامية للحق في الخصوصية البيانات

([1]) – الحافظ أحمد بن حجر العسقلاني ، فتح الباري بشرح صحيح البخاري ، دار الفكر للطباعة والنشر والتوزيع ، ج ١٢ ، بيروت ، ١٩٩٣ ، ص ١٠٦.

([2]) – أبي داود سليمان بن الاشعث السجستاني ، سنن ابى داود ، ج٢ ، طباعة مصطفي البابي الحلبي ، القاهرة ، ١٩٥٢ ، ص ٥٦٨.

([3]) – القران الكريم ، سورة النور ، الآيتين ٢٧ ، ٢٨.

([4]) – د. محمد راكان الدغمي ، حماية الحياة الخاصة في الشريعة الإسلامية ، دار السلام للنشر والتوزيع ، ط١ ، القاهرة ، ١٩٨٥ ، ص ١٣٥.

الشخصية التي يتم معالجتها إلكترونياً، لما يمثل الحق في الخصوصية من أهمية تجعله يرتفع إلى مصاف الواجبات المفروضة على الشخص، كما يجعل منها واجبات والتزامات يقع على المجتمع والدولة واجب الوفاء بها.

المطلب الرابع. مبدأ التناسب بين حماية الحق في خصوصية والحق في الوصول للمعلومات

مما لا شك فيه ضرورة أن تتم الحماية الجنائية للبيانات الشخصية التي تم معالجتها إلكترونياً في ضوء مبدأ التوازن بين الحق في الخصوصية والحق في الوصول للمعلومات وذلك على النحو التالي: فمبدأ التوزان بين الحق في حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً وبين الحق في الوصول للمعلومات(١)، يتطلب إقرار معيار توازن مقبول حتي لا يتحول مبدأ التوازن بين الحق في الخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً والحق في الوصول للمعلومات إلى قيد على حق الاشخاص في حماية خصوصية بياناتهم الشخصية مع الاخذ في الاعتبار أن الحق في الخصوصية في حقيقتها قيد على حق الوصول للمعلومات.

وعليه فقد نصت اتفاقية بودابست للجرائم الإلكترونية(٢) في المقدمة على ضرورة تحقيق التوازن بين حماية حقوق الانسان الاساسية المعترف بها بموجب اتفاقية الاتحاد الاوربي لحماية حقوق الانسان، والعهد الدولي للحقوق المدنية والسياسية ١٩٦٦

(١) – W.A, BRAIN, Legal analysis of a single market for the information society, citation European, ٢٠١١, p. ٤.; see also: Guide lines on the protection of privacy and trans border flows of personal data, ٢ Dec ٢٠١٣.

(٢) – في ٢٠ أبريل ٢٠٠٠ تقدمت اللجنة الاوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية CYBERCRIME بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من اصدار مشروعها الاول وحتى اعداد مسودتها النهائية التي اقرت لاحقا في بودابست ٢٠٠١ وتعرف باتفاقية بودابست لعام ٢٠٠١ للجرائم الالكترونية.

والاتفاقية الأخرى المتعلقة بحقوق الانسان، وبين الحق في الخصوصية وفي تداول المعلومات والبيانات. ويرجع ذلك لنظرة الفلسفية لظاهر جرائم الاعتداء على خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً ووجوب الحماية منها دون الوصول إلى مدى تتأثر فيه حقوق الأفراد بالوصول إلى المعلومات أو تتأثر بأنشطة الاحتكار والاستغلال غير المشروع للحق في المعرفة.

وتطبيقا على ذلك قضية شركة أبل ومكتب التحقيقات الفيدرالي الأمريكي في عام ٢٠١٦ حيث تمت عملية قتل في مدينة سان برناردينو بالولايات المتحدة الأمريكية ولإجراء التحقيقات والكشف عما إذا كان هناك متواطئين مع هؤلاء القتلة أم لا سعى مكتب التحقيقات الفيدرالي الأمريكي FBI بالضغط على شركة أبل لفك تشفير وانشاء برامج تقوض ميزات الأمان لهواتفها خاصة فيما تعلق ببرنامج تخزين السحابات للبيانات الشخصية للمستخدمين I CLOUD. بالتالي اصبحنا أمام نسبة وتناسب فمن أجل احتمالية غير مؤكدة حول الوصول للمعلومات عن طريق اكتساب معلومات إضافية حول الجريمة المروعة التي ارتكبها الجناة في سان برناردينو في الولايات المتحدة الأمريكية سوف يتم انتهاك حق من الحقوق الانسان وهو الحق في خصوصية(١). ونظرا لأهمية التشفير القوي في الحفاظ على الأمن وحقوق الإنسان. لذلك في قضية منفصلة في نيويورك، قضي برفض طلب الحكومة بإجبار شركة أبل على المساعدة على استخراج المعلومات من إيفون يملكه أحد المشتبه بهم في قضية مخدرات. وبناء على ذلك فقد تم رفض طلب الشرطة الفيدرالية الأمريكية من القضاء الأمريكي.

(١) – تقرير لجنة حقوق الانسان بالأمم المتحدة ، المفوض السامي للأمم المتحدة لحقوق الانسان ، مكتب اللجنة العليا في جنيف الصادر في ٣ مارس ٢٠١٦ ، ص ٢.

وبالتالي نستطيع القول بأن مجرد وجود برنامج للمراقبة الجماعية للاتصالات التي تجري عبر البريد الإلكتروني ولأشكال التعبير الرقمي الأخرى يشكل تدخلاً في الحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، مما يرتب على الدولة مسئولية إثبات أن هذا التدخل ليس مخالفاً للقانون وليس تعسفياً(١). غير أن تلك المراقبة يشترط لكي تكون مشروعة توافر الشروط التالية:

١. أن تكون هذه المراقبة ضرورية. حيث أن التناقض بين الحق في الخصوصية وحق الدولة في المراقبة، يعمقه تزايد تدخل الدولة في شئون الاشخاص، ولا يقصد بهذا التدخل الاطلاع على معلومات معينة عن الاشخاص لتنظيم الحياة الاجتماعية على نحو أفضل، كالاحتفاظ بسجلات المواليد والوفيات والزواج والطلاق والإحصاءات أو غيرها من البيانات الهامة للأمن القومي، أما استخدام الدولة للبيانات الشخصية الخاصة لأغراض تتناقض مع صونها واحترام الحق في خصوصيتها، فذلك فعل مجرم يعاقب عليه القانون.

٢- ضرورة الالتزام بمبدأ الشرعية، أي أن المراقبة تتم من خلال نص قانوني يسمح بإجرائها. حيث أن الجهود التنظيمية، والإدارية، والتشريعية، تسعى إلى إقامة التوازن بين هذه الحقوق المتعارضة، خاصة وأن استخدام التقنية الإلكترونية في مجال جمع ومعالجة البيانات الشخصية، قد خلق واقعاً صعبا ومتناقض لحماية الحق في خصوصية البيانات الشخصية يجب لتجنبه الالتزامات بنصوص قانونية واضحة

(١) – التقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان وتقارير المفوضية السامية والأمين العام حول ، تعزيز وحماية جميع حقوق الانسان المدنية والسياسية والاقتصادية والاجتماعية والثقافية ، بما في ذلك الحق في التنمية ، مجلس حقوق الانسان الدورة الثامنة والعشرون البندان ٢ و٣ من جدول الاعمال ، A/HRC/٢٨/٣٩ ، ١٩ ديسمبر ٢٠١٤ ، ص ٤.

تعالج هذا الامر من خلال تشريع جامع شامل لأحكام البيانات الشخصية التي يتم معالجتها إلكترونياً.

٣- أن تتناسب مع الخطر المحدد الذي تجري مواجهته. مثال استثناءً من الالتزام بالحق في خصوصية البيانات الشخصية التي يتم معالجتها إلكترونيا، يجوز السماح بالحق في جمع المعلومات والبيانات الشخصية لغاية البحث العلمي، أو للحفاظ على الأمن القومي من المخاطر التي تهدد أمن وسلامة أو صحة المجتمع. حيث يذهب الاستاذ Frosini في مؤتمر روما عام ١٩٨٧ إلى القول بأن لا وجود اليوم لحرية رفض اعطاء المعلومات ذات المصلحة العامة والمتصلة بالبيانات الشخصية ، ولكن بدلاً من ذلك، فإن الحرية استقرت في المقدمة على السيطرة على المعلومات الشخصية التي أدخلت في برنامج الحاسب الآلي ... وترتيباً على ذلك هناك الحق في الوصول إلى بنوك المعلومات، والحق في التأكد من سلامة المعلومات، والحق في تحديثها وتصحيحها، والحق في سرية المعلومات الحساسة، والحق في السماح بنشرها(١)، وجميع هذه الحقوق اليوم تشكل ما يطلق عليه بالحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

٤- أن يتم ذلك في ضوء مبدأ عدم التمييز، أي تكفل الدولة التوافق أي تتدخل في الحق في الخصوصية مع مبادئ الشرعية والتناسب والضرورة، بغض النظر عن الأصل

(١) - B. N WALDEN and R.N SAVAGE, Data protection and privacy and law should organizations be protected, in international and comparative law and comparative law Quarterly, Vol ٣٧ part ٢, ١٩٨٨, p. ٣٣٧.

العرقي للأشخاص الذين تراقب الدولة اتصالاتهم، أو جنسيتهم، أو مكانهم، أو أي وضع آخر يخصهم.

وتأسيسا على ما سبق فمن الواجب على الدولة أن تكفل الحماية القانونية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً من أي تدخل غير قانوني أو تعسفي، كما يجب أن تتم تنفذ جميع أشكال مراقبة الاتصالات استناداً إلى قانون يسهل وصول الجمهور إليه، بشرط أن يتوافق هذا القانون مع النظام الدستوري للدول ومع القانون الدولي لحقوق الانسان. فمبدأ وضوح القوانين وإمكانية الوصول إليها في كثير من الاحيان لا يتوافق مع القوانين أو القواعد التي تمنح السلطات التنفيذية، كدوائر الامن والاستخبارات سلطات استثنائية وتقديرية واسعة.

بالإضافة إلى ذلك يجب أن تمارس الدولة ولايتها التنظيمية والرقابية على الطرف الثالث الذي يتحكم مادياً في البيانات الشخصية التي تم معالجتها إلكترونياً، حيث تقوم شركات الهاتف ومقدمي خدمات الإنترنت بتخزين بيانات وصفية عن الاتصالات التي يجريها عملاؤها لكي تمكن هيئات إنفاذ القانون والأجهزة الامنية والاستخباراتية من الوصول إلى هذه البيانات في وقت لاحق.

حيث أن الدول في الوقت الحالي تعتمد بشكل متزايد على الشركات في القيام بالمراقبة الرقمية وتيسيرها. وقد توجد في بعض الحالات أسباب شرعية تتيح لأية شركة تقديم هذه البيانات. ولكن عندما يكون طلب الحصول على البيانات الشخصية مخالفاً لقانون حقوق الإنسان، أو عندما تستخدم المعلومات على نحو ينتهك قانون حقوق الإنسان، فقد تتعرض تلك الشركة في هذه الحالة لخطر التواطؤ في ارتكاب انتهاكات حقوق الإنسان.

وبالإضافة إلى ذلك فقد نصت المادة ٥٢ الفقرة الأولى من الاتفاقية الاوربية لحقوق الأنسان على أن أي حد من ممارسة الحقوق والحريات الواردة في هذه المعاهدة يجب أن يكون بموجب القانون ويحترم جوهر هذه الحقوق والحريات. وبحسب مبدأ التناسب، قد تفرض هذه الحدود فقط إذا كانت ضرورية وتحقق فعلا أهداف المصلحة العامة المتفق عليها من قبل الاتحاد أو الحاجة لحماية حقوق وحريات الآخرين.

وتطبيقا على ذلك فقد قضت المحكمة الأوربية لحقوق الانسان بإن الملفات الأمنية الحكومية التي تحتوي على البيانات الشخصية تقع ضمن النطاق المحمي للحق في الخصوصية أي للحياة الشخصية المذكورة في المادة الثامنة من الاتفاقية الأوربية المتعلقة بحقوق الانسان. ووجدت المحكمة أيضا في حالات عدة أن جمع وتخزين ونشر البيانات الشخصية من قبل أجهزة الأمن يشكل تداخلاً على حق الانسان في خصوصية البيانات الشخصية، ولا يسمح به إلا وفق معايير صارمة تحددها الماد ٨ من الاتفاقية الاوربية لحقوق الانسان. ولا تنطبق ذلك على ما اكتشفته المحكمة من الإفصاح عن المعلومات لمؤسسات وجهات حكومية أخرى فحسب ، بل أيضا على استخدامها للتدقيق الأمني الداخلي والتصريح الأمني([1]). ولدى معاينة قضية روتارو ورومانيا لعام ٢٠٠٠ حول الملفات أمنية تحتفظ بها أجهزة الاستخبارات الرومانية([2]) ، وجدت المحكمة أن تخزين هيئة أو مؤسسة عامة لمعلومات مرتبطة بالحياة الخاصة لفرد ما واستخدامها وإعطاء الفرصة بنقضها يعتبران تداخلاً من الحق في خصوصية البيانات الشخصية التي نصت المادة الثامنة من الاتفاقية لحقوق الانسان على حمايتها.

([1]) – المحكمة الأوربية لحقوق الانسان ، قضية لياندر ، رقم ٨١ / ٩٢٤٨ ، لسويد ، ١٩٨٧.
([2]) – المحكمة الأوربية لحقوق الانسان ، قضية روتارو ، رقم ٨١ / ٩٢٤٨ / ٥٤٩٣٤ ، رومانيا ، ٢٠٠٦.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

وبناء على ذلك فقد ذهب المشرع الألماني إلى الاعتراف بمبدأ التناسب بين الحق في خصوصية البيانات الشخصية وبين الحق في الوصول إلى المعلومات، وبالتالي يربط بين الحاجة لجمع البيانات وجدية التهديد ذات الصلة. ويتطلب المكتب الفيدرالي لحماية الدستور الألماني وبشكل خاص من جهاز الاستخبارات المحلية الألماني دراسة إذا ما كان من الممكن الحصول على المعلومات المرغوبة من مصادر مفتوحة باستخدام وسائل أقل انتهاكا للحق في خصوصية البيانات الشخصية(١). هذا وقد يحدد مثل هذا القانون من احتمال انتهاك المؤسسات الحكومية للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

وعليه تطرح المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان، التي اعتمدها مجلس حقوق الإنسان في قراره ٤/١٧ المؤرخ في ١٦ يونية ٢٠١١، معياراً عالمياً لمنع ومواجهة الآثار السلبية للنشاط التجاري على حقوق الإنسان. وتبين هذه المبادئ بوضوح أن على الشركات أن تتحمل المسئولية عن حماية حقوق الإنسان في جميع عملياتها العالمية، أياً كان مكان وجود المستفيدين من هذه الشركة، وبغض النظر عن وفاء الدولة بالتزاماتها الذاتية المتعلقة بحقوق الإنسان أم لا.

وكذلك تنص المادة ٨٥ من اللائحة العامة لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨ على أن تقوم الدول الاعضاء بالتوفيق بين الحق في حماية البيانات الشخصية والحق في حرية التعبير والإعلام، بما في ذلك التجهيز لأغراض صحفية أو أغراض التعبير الأكاديمي أو الفني

---

(١) – القانون الفيدرالي الألماني حول حماية الدستور الصادر في ٢٠ ديسمبر ١٩٩٠ ، الجريدة الرسمية عدد ١ ، ص ٢٩٥٤ ، وتم تعديله بالمادة رقم ١ (أ) من قانون الفيدرالي الصادر في ٣١ لسنة ٢٠٠٩ ، الجريدة الرسمية ١ ، ص ٢٤٩٩ ، القسم ٩.

أو الأدبي، بالتالي يجوز النص على استثناءات في قوانين الدول من القواعد السابقة في اللائحة الأوربية وذلك إذا كانت ضرورية للتوفيق بين الحق في حماية البيانات الشخصية والحق في حرية التعبير والمعلومات.

الفصل الثاني. صور الحماية الجنائية لخصوصية البيانات الشخصية الإلكترونية

مما شك فيه أن استخدام الحاسب الآلي كوسيلة لتخزين البيانات والمعلومات الشخصية أصبح الان من الأشياء المسلم بها في هذا العصر، ونتيجة لأهمية عملية استخدام وتخزين ونقل البيانات الشخصية التي تم معالجتها إلكترونياً، وجب على المشرع التدخل بالنص على حماية الانسان من استعمال أو استغلال او تخزين هذه البيانات الشخصية بطريقة غير مشروعة([١]). وكذلك نقلها أو تمكن الغير للاطلاع عليها بطريق تخالف الضوابط القانونية التي ينص عليها القانون.

فلكل فرد الحق في حماية خصوصية بياناته الشخصية([٢]) ، وبالتالي لا يجوز معالجة تلك البيانات إلا في اطار من الشفافية والأمانة واحترام كرامة الإنسان والممارسات المقبولة المشروعة وفقا لما ينص عليه القانون. وبناء على ذلك يجب أن يتدخل المشرع في درء جميع الأفعال غير المشروعة عن الحقوق والمصالح المحمية، وكل ما يؤدي إلى المساس بها وفقا ما يقرره القانون من جزاء مناسب لهذه الجرائم. فنتيجة للتداول السريع للبيانات والمعلومات عبر شبكات الانترنت عالية السرعة([٣]) ، وسرعة انتشار شبكة المعلومات والبيانات كل ذلك أدي إلى سهولة تداول المعلومات

([١]) – انظر : د. علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الألي ، دار الجامعة الجديدة ، الاسكندرية ، ١٩٩٧ .، د. هدى حامد قشوش ، جرائم الحاسب الإلكترونية في التشريع المقارن ، دار النهضة العربية ، القاهرة ، ١٩٩٢.

([٢]) – المادة الثالثة من القانون القطري رقم ١٣ لسنة ٢٠١٦ الخاص بشأن حماية البيانات الشخصية.

([٣]) – د. محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، ١٩٩٣ ، ص ٦.

والبيانات ومن ثم سهولة ارتكاب الجرائم الإلكترونية وخاصة جرائم الاعتداء على الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً.

فما لا شك فيه أن مخازن وبنوك المعلومات وخاصة المتعلقة بالبيانات الشخصية تشكل خطرا كبيرا على الحياة الخاصة للأفراد خصوصاً في حالة إساءة استخدام البيانات الشخصية المتعلقة بخصوصياتهم، أو في حالة استخدامها لغايات غير تلك التي من أجلها جمعت. فمن القضايا الشهيرة في حقل الاعتداء على البيانات الخاصة ما حصلت في جنوب إفريقيا، حيث تمكن معتدون من الوصول إلى الشرائط التي خزنت عليها المعلومات الخاصة بمصابي أمراض الإيدز Sida، وفحوصاتهم وقاموا بتسريبها إلى جهات عديدة، ومنها أيضا الحادثة التي وقعت عام ١٩٨٩ حيث قام أحد كبار موظفي أحد البنوك السويسرية بتسريب أشرطة تحتوي على أرصدة عدد من الزبائن إلى سلطات الضرائب الفرنسية. وفي عام ١٩٨٦ اتهمت شركة IBM بأن النظام الأمني التي تنتجه المعرف بـ "RACF" يستخدم للرقابة على الموظفين داخل المنشآت والمؤسسات، كل هذه الصور تشكل تهديد للحق في خصوصية البيانات الشخصية.

وبناء على ما سبق يمكننا تحديد صور الحماية الجنائية لخصوصية البيانات الشخصية المعالجة إلكترونياً وذلك على التالي:

١. الولوج أو الدخول بوسائل غير مشروعة إلى سجل البيانات أليا.
٢. حماية البيانات الشخصية المعالجة الكترونياً من مخاطر التخلص بطريق الخطأ أو الغير قانوني،
٣. فقدانها عن طريق الخطأ،
٤. التغيير،
٥. الكشف عنها أو الوصول غير المصرح به،

٦. جميع الأشكال الأخرى الغير مشروعة في التعامل مع البيانات الشخصية. الحصول عليها بطريق غير مشروع، تستخدم لغير الغرض الأصلي والمحدد لها.

وسوف نتناول بالدراسة لصور الحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً من خلال توضيح جريمة الدخول غير المشروع لنظم المعلومات والبيانات الشخصية المعالجة إلكترونياً في المبحث الأول، ثم نستعرض في المبحث الثاني جرائم المعالجة غير المشروعة للبيانات الشخصية الإلكترونية، ثم في المبحث الثالث نبين جريمة إتلاف وتعطيل أنظمة المعالجة الآلية والتخزين للبيانات الشخصية الإلكترونية ، وفي المبحث الرابع جريمة الإعلانات التسويقية الإلكترونية غير المرغوب فيها من خلال استخدام البيانات الشخصية ، وفي النهاية نتناول الجرائم المتعلق بانتهاك الحماية القانونية لخصوصية البيانات الشخصية للأطفال التي تم معالجتها إلكترونياً.

المبحث الأول. جريمة الدخول غير المشروع لنظم المعلومات والبيانات الشخصية الإلكترونية

مما لا شك فيه أن الحماية الجنائية للبيانات الشخصية التي تم معالجتها إلكترونياً تبدأ من خلال التجريم للدخول أو الالتقاط أو الولوج غير المشروع لنظم المعلومات والبيانات الشخصية الإلكترونية، لذلك حظر المشرع الجنائي اطلاع الغير عليها بدون أذن. ونص في قانون الإجراءات الجنائية الألماني في المادة ١١٠ على أنه تقتصر سلطة الاطلاع على مخرجات الحاسب الآلي وغيرها من دعائم البيانات على المدعي العام وحده، ولا يكون لضباط الشرطة حق الاطلاع على البيانات عن طريق تشغيل البرامج أو الاطلاع على ملفات البيانات المخزنة داخل الحاسب الآلي بغير إذن ممن له حق التصرف فيها، ومالهم قانونا هو فحص دعائم البيانات عن طريق النظر فحسب دون استخدام مساعدات فنية. وهو ما يؤكد خصوصية البيانات الشخصية الإلكترونية وعدم السماح لاحد الاعتداء على هذه الحق إلا بناء على تصريح من النيابة العامة باعتبارها سلطة التحقيق الابتدائي والقادرة على تقييم الدلائل والتحريات التي تتطلب الاطلاع على هذه البيانات الشخصية التي تم معالجتها إلكترونياً.

وسوف نستعرض في البداية ماهية الدخول أو الالتقاط غير المشروع للبيانات الشخصية التي تم معالجتها إلكترونية في المطلب الأول، ثم نوضح في المطلب الثاني الاشكالية القانونية التي تثيرها جريمة الدخول أو الالتقاط غير المشروع للبيانات الشخصية المعالجة إلكترونية.

المطلب الأول. ماهية الدخول أو الالتقاط غير المشروع للبيانات الشخصية الإلكترونية

في واقع الامر لقد أدركت الدول بمدى خطورة الجريمة المعلوماتية بوصفها جريمة عابرة للحدود لذلك فقد تم التوقيع على اتفاقية بودابست لمقاومة جرائم المعلوماتية والاتصالات في عام ٢٠٠١ من طرف ثلاثون دولة في العاصمة المجرية بودابست، وقد تضمنت المذكرة التفسيرية لاتفاقية بودابست المتعلقة بالجرائم الإلكترونية في تعليقها على المادة الثانية الخاصة بالدخول غير القانوني على أنه كمبدأ عام يعتبر الدخول غير المصرح به بمعني القرصنة أو السطو أو الدخول غير المشروع في النظام المعلوماتي، مجرم أو غير قانوني، وذلك لما ينجم عن هذه الأفعال من عقبات تحول بين المستخدمين الشرعيين والانتفاع من النظم المعلوماتية والبيانات. ولما قد يترتب عليها من إتلاف أو تدمير يتطلب مبالغ طائلة لإعادة بنائه. وأن هذا الدخول يؤدي إلى الوصول إلى بيانات سرية خاصة بالشخص(١)، مما يشكل انتهاك لحق الشخص في خصوصية البيانات الشخصية.

ومن الجدير بالذكر أن مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في الفترة من ٤-٩ اكتوبر ١٩٩٤ -البرازيل - ريو دي جانيرو بشان جرائم الكمبيوتر، قد نصت على أنه تتضمن قائمة الحد الادنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر، جريمة الدخول غير المصرح به، وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات

(١) - د. هلالي عبد الله أحمد ، الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء اتفاقية بودابست في ٢٣ نوفمبر ٢٠٠١ ، دار النهضة العربية ، القاهرة ، الطبعة الأولى ، ٢٠٠٣ ، ص ٦٩ - ٧٠.

الامن. كذلك جريمة الاعتراض غير المصرح به ، وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم او شبكة اتصالات. بالإضافة إلى ذلك فقد نصت المادة الثانية من اتفاقية بودابست للجرائم الإلكترونية على تجريم كل دخول غير المشروع إلى شبكات الانترنت وانتهاك إجراءات الحماية بقصد الحصول على البيانات أو لأي غرض إجرامي آخر(١). ويلاحظ أن المشرع الاوربي في اتفاقية بودابست يتطلب للعقاب عن جريمة الدخول غير المشروع أن يتم النشاط الإجرامي وهو الدخول غير المشروع بقصد الحصول على البيانات أو لأغراض إجرامي آخر أي أن يكون الشخص على علم بأن يقوم بالدخول غير المشروع، وأنه يقوم بانتهاك إجراءات الحماية للبيانات الشخصية الإلكترونية. وأن إرادته الحرة الواعية قد اتجهت إلى الدخول غير للمشروع وانتهاك إجراءات الحماية للبيانات الشخصية الإلكترونية بهدف الحصول على هذه البيانات أو لتحقيق أي غرض إجرامي آخر.

وعليه يتكون الركن المادي للجريمة من سلوك إجرامي يتمثل في قيام الجاني بصورة من صور النشاط الإجرامي في الدخول أو الولوج أو الاتصال بالبيانات أو المعلومات أي التواجد في نظام المعالجة الآلية للبيانات الشخصية، ويتحقق السلوك الإجرامي كذلك في حالة الدخول الخطأ ثم المكوث بعد ذلك رغم علم الجاني بعدم مشروعية الدخول. وانطلاقا مما سبق فقد حصل خلاف واسع بين كلاً من الادعاء العام والقضاء الأمريكي بشأن النشاط الاجرامي لمدلول الدخول غير المشروع إلى النظام الآلي لمعالجة البيانات الشخصية في القضية التي أقيمت ضد المتهم Allen ، فقد كانت هذه القضية مناسبة مهمة للقضاء الأمريكي ممثلا في المحكمة العليا لولاية كانساس لأبداء الرأي بشأن

(١) – في ٢٠ أبريل ٢٠٠٠ تقدمت اللجنة الاوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية CYBERCRIME بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من اصدار مشروعها الاول وحتى اعداد مسودتها النهائية التي اقرت لاحقا في بودابست ٢٠٠١ وتعرف باتفاقية بودابست لعام ٢٠٠١ للجرائم الالكترونية.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

معني الدخول الذي يرى بأنه يتحقق من خلال المعني الواسع التي استخدمها المشرع Access التي تعني الاقتراب أو إصدار أمر الاتصال ب ... أو تخزين بيانات في ... أو استرداد بيانات من ... أو استخدام أشياء أخرى تؤدي إلى استخدام مصادر للحاسب الألي([١]). فإذا قام المتهم بأحد من الافعال السابقة يعتبر قد ارتكب النشاط الإجرامي المكون للركن المادي في جريمة الدخول غير المشروع على البيانات الشخصية التي تم معالجتها إلكترونياً.

كذلك ينص قانون ولاية فلوريدا الأمريكية على معاقبة كل ولوج بسوء نية في نظام أو شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير، أو كل من أدخل معلومات مصطنعة بغرض تحسين أو إساءة سمعة الغير([٢]). ويتضح من ذلك أن المشرع الأمريكي اشترط للمعاقبة على الدخول غير المشروع لنظم وشبكات المعلوماتية ضرورة أن يتم ذلك بسوء نية وبغرض الحصول على معلومات غير مسموح الحصول عليها.

وعليه فقد فرض المشرع الأمريكي حماية لخصوصية البيانات الشخصية للأشخاص أثناء عمليات الاتصالات وتبادل المعلومات والبيانات، وذلك بموجب قانون حماية خصوصية الاتصالات الإلكترونية الصادر في عام ١٩٨٦ ECPA. بحيث يجرم هذا القانون الدخول غير المشروع إلى الاتصالات الإلكترونية المخزنة والتي يتم بثها، وهي تتضمن البريد الصوتي والبريد الإلكتروني، فالدخول إلى بريد إلكتروني لشخص ما بدون

([١]) – KAN, State V.Allen, USA, ١٩٩٦, ٩١٧, P.٢ D ٨٤٨.

([٢]) – د. أسامة أحمد المناعسة ، جرائم الحاسب الآلي والإنترنت ، دراسة تحليله مقارنة ، الطبعة الأولي ، دار وائل للنشر ، الأردن ، عمان ، ٢٠٠١ ، ص ٢٢٤.

إذنه يشكل انتهاك لقانون خصوصية الاتصالات الإلكترونية(١). وذلك بالنص في المادة ٢٧٠١ من قانون حماية خصوصية الاتصالات الإلكترونية ECPA على أنه يجرم الدخول غير المشروع لمخزون الاتصالات، وكذلك الدخول غير المشروع إلى خدمات الاتصالات الإلكترونية، بالإضافة إلى مجاوزة الدخول المحظور والاستيلاء على الاتصالات الإلكترونية أو التلاعب بها أو تجنب الدخول إلى خطوط الاتصالات أو الاتصالات الإلكترونية في التخزين الإلكتروني(٢)، وتتراوح العقوبة في هذه الحالات ما بين الحبس الذي لا تزيد عن خمس سنوات والغرامة المالية التي لا تزيد عن ١٠٠٠٠٠ ألاف دولار. وتدخل في نطاق التجريم الدخول إلى موقع شبكات الانترنت بدون وجه حق بنيه سيئة بغرض الحصول على معلومات وبيانات شخصية خاصة.

أما بالنسبة لموقف المشرع الفرنسي فقد نص على جريمة الولوج غير المشروع لنظم المعلومات لأول مرة في القانون الصارد في ٥ يناير ١٩٨٨ في المادة ٤٦٢ الفقرة الثانية بقانون العقوبات، والتي تم تعديلها بموجب القانون الصادر في ٢٩ مارس ١٩٩٣ المادة ٣٣١ الفقرة الاولى من قانون العقوبات حيث يعاقب بالحبس لمدة سنة واحدة وبالغرامة المالية التي تبلغ مقدارها ١٠٠,٠٠٠ فرنك كل من تواجد أو بقي على نحو غير مشروع في نظام معالجة آلية للبيانات سواء على نحو كلى أو جزئي. وتشدد العقوبة بالحبس لمدة سنتين وبغرامة المالية التي تبلغ مقدراها ٢٠٠,٠٠٠ فرنك إذا ما ترتب على ذلك ألغاء أو تعديل للبيانات التي يحتويها هذا النظام أو بإتلاف وظيفة النظام. وقد خضع هذا القانون لتعديلات في عام ١٩٩٣ وسعت من نطاق السلوكيات محل التجريم إضافة إلى تعديل بعض العقوبات لتحقيق مزيد من الأبعاد الردعية .

---

(١) – Thomas J. SMEDINGHOFF, On line law, The spa`s legal guide to donning business on the internet, The Software publishers Association, ١٩٩٦, p. ٤٨١.

(٢) – Jonathan ROSENOER, Cyber law, The law of internet, Springer – Verlag, New York, ١٩٩٧, p. ١٧٠.

ويستخلص من ذلك أن المشرع الفرنسي جرم مجرد الولوج أو الدخول سواء كان كليا أو جزئيا دون حاجة إلى اشترط تحقق النتيجة الإجرامية فهي من الجرائم الشكلية التي تقع بمجرد ارتكاب السلوك الإجرامي، وجعل من تحقق النتيجة الإجرامية ظرف مشدد للعقاب في هذه الحالة، وذلك على عكس المشرع الأمريكي.

أما بالنسبة لموقف المشرع المصري فقد سار على نهج المشرع الفرنسي بتجريم مجرد الدخول غير المشروع سواء عن طريق الدخول العمدي أو الدخول بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول علية(١)، بحيث يعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائة ألف جنية، أو بإحدى هاتين العقوبتين.

كذلك يشدد المشرع المصري العقوبة فتصبح الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنية ولا تجاوز مائتي ألف جنية، أو بإحدى هاتين العقوبتين. إذا نتج عن الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على الموقع أو الحساب الخاص أو النظام المعلوماتي.

بالإضافة إلى ذلك فقد جرم المشرع المصري مجرد تجاوز حدود الحق في الدخول في نهج محمود للمشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، حيث نص في المادة ١٥ منه على أن "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنية ولا تجاوز خمسين ألف جنية، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول".

(١) – انظر المادة ١٤ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.

وأن كنا نري أنه يجب على المشرع المصري عدم تقيد طرق التجاوز لحدود الحق في الدخول في حالتين فقط وهما التجاوز من حيث الزمان أي مدة الدخول المسموح فيها ممارس هذا الحق، ومستوى الدخول، وكذلك نري أن ترك المشرع المصري طريقة تجاوز حدود الحق في الدخول غير محددة، وذلك لتطور التكنولوجي في مجال الاختراق والدخول على البيانات والمعلومات بطريقة سريعة ومتغيرة بحيث يصعب حصره في طرق محددة مسبقاً.

المطلب الثاني. الإشكاليات القانونية التي تثيرها جريمة الدخول غير المشروع للبيانات الشخصية الإلكترونية

في واقع الأمر أن جريمة الدخول غير المشروع للبيانات الشخصية التي تم معالجتها إلكترونياً تثير العديد من التساؤلات القانونية، وسوف نتناول هذه الإشكاليات بالشرح واستعراض موقف الفقه منها على النحو التالي.

أولا. يثور التساؤل هل يشترط لقيام الجريمة أن يكون النظام محمياً بواسطة جهاز أمن حتى يمكن العقاب عن جريمة الولوج الغير المشروع لنظم معلوماتي؟ للإجابة عن هذا التساؤل انقسم الفقه إلى اتجاهين وهما على النحو التالي:

الاتجاه الاول(١) ذهب إلى انه يشترط أن يكون النظام محمياً بواسطة جهاز أمن وذلك لدفع أصحاب هذه الأنظمة المتعلقة بالأمن المعلومات إلى أن يدعموا أنظمتهم بالتطبيقات والبرامج التي تمنع الدخول غير المشروع إليها وبالتالي تعريض خصوصية البيانات الآلية للانتهاك والخطر.

أما الاتجاه الثاني(٢) فيذهب إلى أن من غير المناسب التمسك بهذا الشرط، وهذا ما نؤيده لأنه سوف يترتب عليه قصر الحماية الجنائية على البيانات والمعلومات الموجودة في الأنظمة المحمية بواسطة أجهزة الأمن ومن ثم يستبعد من مجال التجريم الولوج التي ترتكب ضد الانظمة المفتوحة للجميع مثل الدليل الإلكتروني وهذا ليس

---

(١) – J. PRADEL, Droit pénal, éd., ٢٠١٠, Dalloz, Paris, p. ٨٢٧ ; A. LUCAS, Le droit de l'informatique, éd., PUF, ١٩٨٧, Paris, p. ٢١.

(٢) – La rapport de R. ANDRE, Assemble nationale, N°١٠٧٨, Paris, ١٩٨٧ – ١٩٨٨, p. ٥.

صحيح فمجال الحماية الجنائية يشمل الأنظمة المحمية بواسطة أجهزة الأمن أو الأنظمة الغير محمية بواسطة أجهزة الأمن.

وتماشياً مع تم ذكره نجد أن المشرع الفرنسي قد تناول جريمة الدخول غير المشروع أو البقاء بدون صلاحية داخل نظام معلوماتي من خلال المواد ٣٢٣ – ١ إلى ٣٢٣-٣ من قانون العقوبات مجرما فعل الدخول أو البقاء بطريق الغش في نظام المعالجة الآلية للبيانات أو جزء منه، وفرق بين مجرد الدخول أو البقاء، وبين ما يترتب عن هذا الدخول أو البقاء من محو أو تعديل في البيانات المخزنة أو اتلاف تشغيل هذا النظام.

كذلك فقد نص المشرع الفرنسي في المادة ١٢١ – ٨ من قانون العمل الفرنسي الملغي رقم ١٤٤٥ الصادر في ١٩٩٣ بالقانون الصادر في ٢٠٠٧ على أنه(١) لا يجوز التقاط أية معلومات شخصية تخص أجير أو مستخدم من قبل صاحب العمل ما لم يكن قد تم إبلاغ الأجير أو المستخدم سلفاً بذلك. وذلك لأنه أصبح هناك قانون خاص موحد لحماية البيانات الشخصية. وعليه فقد حرص المشرع الفرنسي على النص على تدابير احترازية وعقوبات تكميلية بالإضافة إلى العقوبات الاصلية المنصوص عليها، وذلك لمواجهة الخطورة الإجرامية الكامنة في شخص مرتكب هذا النوع من الجرائم. وذلك وفقا لنص المادة ٣٢٣ – ٥ من قانون العقوبات على أنه يعاقب الأشخاص مرتكبي الجرائم المنصوص عليها في الباب الحالي بالعقوبات التكميلية التالية:

١. الحرمان من الحقوق المدنية والعائلية وذلك على النحو المنصوص عليه في المادة ١٣١ الفقرة ٢٦ لمدة خمس سنوات كحد أقصى.

---

(١) – L'article L ١٢١ – ٨, Loi n°٩٢ – ١٤٤٦ du ٣١ décembre ١٩٩٢ – art ٢٦ JOFR ١er janvier ١٩٩٣., Abrogé par Ordonnance n°٢٠٠٧ – ٣٢٩ du ١٢ mars ٢٠٠٧ – art ١٢ VD, JORF ١٣ mars ٢٠٠٧ en vigueur au plus tard le ١ er mars ٢٠٠٨.

٢. الحرمان من ممارسة الوظيفة العامة أو ممارسة أي نشاط مهني أو اجتماعي والذي بمناسبته ارتكبت الجريمة لمدة خمس سنوات كحد أقصى.

٣. مصادرة الأشياء التي استخدمت في ارتكاب الجريمة أو الأشياء المتحصلة منها باستثناء الاشياء ملك الغير حسن النية.

٤. غلق المؤسسات التي استخدمت في ارتكاب الأفعال الإجرامية لمدة تصل إلى خمس سنوات.

٥. الاستبعاد من الأسواق العامة لمدة تصل إلى خمس سنوات.

٦. حظر اصدار الشيكات بخلاف التدابير التي تسمح بسحب الأموال بواسطة الساحب لدى المسحوب عليه لمدة تصل إلى خمس سنوات.

٧. نشر الحكم الصادر في الأماكن المنصوص عليها في المادة ١٣١ – ٣٥.

وعلاوة على ذلك فقد ادخل المشرع الفرنسي العديد من التعديلات على القانون الخاص بحماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨ ومنها التعديل بالقانون رقم ٨٠١ لسنة ٢٠٠٤، والتعديل بالقانون رقم ١٣٢١ لسنة ٢٠١٦ الصادر في ٧ أكتوبر ٢٠١٦، والقانون رقم ٥٥ الصادر في ٢٠ يناير ٢٠١٧، والقانون رقم ٤٩٣ الصادر في ٢٠ يونية ٢٠١٨ وفقا لتعديلات اللائحة العامة الاوربية لحماية البيانات الشخصية رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨.

أما بالنسبة لموقف المشرع الدانماركي فقد نص في المادة ٢٦٣ من القانون الصادر في الأول من يوليه ١٩٨٥ على أنه يعد من قبيل الجرائم جريمة الولوج في المعلومات أو البرامج المختزنة في أجهزة المعالجة الإلكترونية للمعلومات والبيانات(١). أما المشرع

(١) – د. هدى حامد قشقوش ، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ ، ص ٤٨.

السويدي فينص في المادة ٢١ من القانون رقم ٢٨٩ الصادر في ٢ إبريل ١٩٧٣ على أنه يعاقب كل من ولج بوسائل غير مشروعة إلى سجل مخصص لمعالجة البيانات آليا. أي أن المشرع السويد يسير على نهج المشرع الفرنسي في تجريم مجرد الولوج غير المشروع لنظم المعلومات والبيانات دون اشتراط تحقق نتيجة إجرامية وذلك لخطورة الفعل الإجرامي الذي يهدد أمن البيانات والمعلومات سواء كانت شخصية أو كانت متعلقة بأمن الدولة المعلومات.

أما بالنسبة للمشرع الانجليزي فقد نص على تجريم الولوج غير المشروع من أي فرد على البيانات المختزنة بالحاسب الألي أو البرامج في القانون الصادر عام ١٩٩٠ الذي يعالج اساءة استخدام نظم المعلومات(١) ، وكذلك في قانون حماية البيانات الصادر في عام ١٩٨٤ الذي ينص على تجريم الدخول المتعمد غير المشروع أو الدخول غير المشروع والذي يتم بنية ارتكاب الجريمة. فيجب حفظ البيانات الشخصية بصورة آمنة تحميها من عمليات الدخول غير المشروع كما تحميها من الفقد، وذلك من أجل حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

وكذلك نجد أن المشرع الانجليزي قد كفل حماية البيانات المخزنة في الحواسب الآلية من الاعتداء عليها، أو إساءة استخدامها بإصداره لقانون إساءة استخدام الكمبيوتر عام ١٩٩٠ COMPUTER MISUSEACT فجرم من خلال المادة الأولى منه فعل الدخول غير المشروع إلي أي برنامج أو بيانات موضوعة في أي كمبيوتر ، مع جعله يؤدي أية وظيفة لتحقيق الدخول، كما عاقب على أي دخول يقصد به تدبير غير مشروع ، إذا توافر للجاني العلم بعدم مشروعية الدخول، وقت تغييره لوظيفة الكمبيوتر ، أو إذا

(١) – M. GODFRAIN, Relative à la fraude informatique, ١٩٨٦, ٨٧, N° ٧٤٤, p. ١٣.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

اتجهت نيته للاعتداء على تفاصيل أي برامج أو بيانات في أي كمبيوتر محدد أو غير محدد ، وتعلقت المادة الثانية من ذات القانون بتجريم فعل الدخول غير المشروع لارتكاب أية جريمة يعاقب عليها النص، أو لتسهيل ارتكاب الجريمة، سواء للجاني نفسه أو لشخص آخر ، وقد جرم في المادة الثالثة فعل الدخول إذا كانت الغاية منه تعمد تعديل modification محتوى أي كمبيوتر، فيعاقب على إتلاف عمل الكمبيوتر أو إعاقة الدخول لأي برنامج أو بيانات موضوعة في أي كمبيوتر أو إتلاف عمل أي برنامج أو صحة أي بيانات ، ويعاقب الجاني متى اتجهت نيته بصورة مباشرة إلى أي كمبيوتر للشخص أو برنامج خاص أو بيانات من نوع خاص أو تعديل من نوع خاص، من توافرت لديه المعرفة السابقة، والمتمثلة بأي تعديل يقصده الجاني كي يتسبب بفعله غير مشروع. ويتضح مما سبق أن المشرع الانجليزي يعاقب عن هذه الجريمة بمجرد الشروع أو التحريض أو التآمر، كما لم يشترط من جهة الادعاء أن تقدم دليل يستفاد منه أن الأفعال المقترفة قد استهدفت بيانات أو برامج معينة. بالإضافة إلى ذلك لم يشترط تواجد المتهم وقت ارتكاب ولا بيانات الحاسب الآلي المستهدفة في انجلترا وذلك وفقا لمبدأ الاختصاص العالمي للقانون الجنائي.

أما بالنسبة للمشرع الكندي فقد نص في قانون العقوبات الكندي في المادة ٣٠١ الفقرة الثانية على تجريم كل من ولج بنية الغش، بواسطة جهاز إلكتروني أو صوتي أو آلي مباشرة أو بطريق غير مباشر في حاسب آلي. ونص على أنه يعاقب بالحبس لمدة لا تزيد عن عشرة سنوات. ويلاحظ هنا أن المشرع الكندي وعلى عكس المشرعين الفرنسي والانجليزي يشترط للعقاب عن جريمة الولوج غير المشروع توافر قصد جنائي خاص وهو أن ترتكب هذه الجريمة بنية الغش.

أما بالنسبة لموقف المشرع الأمريكي من جريمة الولوج غير المشروع لنظم المعلومات والبيانات الإلكترونية فقد نص على تجريم كل ولوج عمدى في حاسب آلي بدون إذن أو كان مسموحاً له بالولوج واستغل الفرصة التي سنحت له عن طريق هذا الولوج لأغراض لم يشملها الإذن(١)، وذلك في القانون الولوج المصطنع في الحاسب الآلي الصادر في أكتوبر سنة ١٩٨٤ وقد تم أدخال تعديلات على هذا القانون في عام ١٩٩٦.

ولابد من الإشارة أنه يختص بسلطة التحقيق في عمليات الولوج غير المشروع لنظم المعلومات والبيانات الإلكترونية في الولايات المتحدة الأمريكية قطاع الخدمة السرية وذلك بناء على تفويض من الكونجرس الأمريكي وذلك بموجب البند رقم ١٨ من قانون الولايات المتحدة الأمريكية القسم رقم ١٠٢٩. وقد وضع المشرع الأمريكي بموجب هذا القانون تعريف لوسائل الدخول للمعلومات وهو أية بطاقة أو لوحة أو رقم كودي أو رقم حساب أو أية وسيلة أخرى من وسائل الدخول على الحسابات بغرض التحصل على أموال أو بضائع أو خدمات أو أي شيء آخر ذو قيمة يمكن استخدامه كوسيلة من وسائل بدء نقل الأموال. وقد تضمن قانون الاحتيال وإساءة استخدام الكمبيوتر CFAA الصادر في عام ١٩٩٦ عن المشرع الأمريكي، تجريم الدخول غير المشروع الى أنظمة المعلوماتية ، معدداً صور هذه الجريمة من خلال المادة ١٠٣٠ من هذا القانون وهي على النحو التالي(٢) :

---

(١) – د. طارق سرور ، ذاتية جرائم الإعلام الإلكتروني ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠١ ، ص ٥٣.

(٢) – الأستاذ Orin Kerr ، المرشد الامريكي الصادر عام ١٩٩٤م ، المعد من قبل قسم جرائم الحاسب الآلي والملكية الفكرية بإشراف الأستاذ Orin Kerr،المعدل سنة ٢٠٠٢ الذي تضمن تطبيقا للقانون الوطني الأمريكي الصادر في ٢٠٠١/١٠/٢٦.

١- الدخول العمدي إلى جهاز الحاسب الآلي بدون تصريح أو تجاوزاً للتصريح الممنوح له، ويحصل هذا الدخول بأية وسيلة على معلومات تقررت من قبل حكومة الولايات المتحدة بناء على أمر تنفيذي وتصريح برلماني يتطلب الحماية، ضد الافشاء غير المخول به لأسباب تتعلق بالدفاع الوطني أو العلاقات الأجنبية.

٢- الوصول عمداً إلى الحاسب الآلي بدون ترخيص، أو تجاوز الترخيص الممنوح بقصد الحصول على معلومات واردة في سجل مالي بمؤسسة مالية، أو أن تشمل هذه المعلومات المتضمنة في ملف وكالة أو معلومات من أي حاسب محمي إذا تعلق بمحتوى اتصالات خارجية أو بين الولايات المتحدة الأمريكية.

٣- الوصول العمدي بدون ترخيص لأي حاسب آلي غير عام يخص إحدى إدارات أو وكالات الولايات المتحدة مخصص لاستعمال حكومة الولايات المتحدة، أو لم يكن مخصص لها ولكن استعمل من قبل أو لأجل حكومة الولايات المتحدة الأمريكية وكان ذلك التصرف مؤثرا على ذلك الاستعمال من قبل أو لأجل حكومة الولايات المتحدة الأمريكية.

٤- الوصول لمعرفة وبقصد الغش للحاسب الآلي محمي، بدون ترخيص أو بتجاوز الترخيص الممنوح له، وبأيه وسيلة تسهل نية الغش ويتحصل على أي شيء ذي قيمة، مالم يكن موضوع الغش والشيء المتحصل عليه يتوقف فقط على

استخدام الحاسب وأن قيمة هذا الاستخدام لا تزيد عن ٥٠٠٠ دولار خلال فترة سنة(١).

٥- كل من:

أ- سبب عن معرفة بث برنامج ومعلومات أو شفرة أو أمر وسبب ضرر عن قصد كنتيجة لهذا التصرف، وبدون ترخيص لكمبيوتر محمى.

ب- يتصل متعمدا لكمبيوتر محمي بدون ترخيص وكنتيجة لهذا السلوك سبب ضررا نتيجة إهمال.

ج- يصل متعمدا لكمبيوتر – محمي – بدون تفويض وكنتيجة لهذا السلوك يسبب ضررا.

٦- كل من توصل باحتيال عن قصد ومعرفة، تجاره أو مقايضة على أي كلمة سر أو معلومات مشابهة يمكن من خلالها الوصول للكمبيوتر بدون تفويض.

وبالرغم مما سبق إلا انه يؤخذ على المشرع الأمريكي في هذا القانون ينطوي على الكثير من الغموض والقصور، بحيث يمكن للمجرمين الهروب من عدم تطبيق القانون عليهم في حالات معينة، وذلك باستخدام حاسبات آليه وشبكات من خارج الولايات المتحدة والدخول إلى أنظمة الحاسبات الآلية داخل الولايات المتحدة الأمريكية والاعتداء عليها أو استخدام هذه الأنظمة ذاتها عن بعد للاعتداء على حاسبات الآلية تقع في دول أخرى.

---

(١) – J. CHAMPLAIN, (٢٠٠٣) . Auditing Information Systems. Hoboken, New jersey , John wiley of sons, Icove, D, Segar.K& Vonstorch ,W et al,١٩٩٩&Wright, ٢٠٠٠d.

أما فيما يتعلق بموقف المشرع الجزائري نجد انه، قد عاقب على جرائم أدرجها في القسم السابع مكرر من قانون العقوبات المعدل بالقانون ٢٣/٠٦ المؤرخ في ٢٠٠٦/١٢/٢٠ المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بالمواد ٣٩٤ مكرر الى ٣٩٤ مكرر ٧ وذلك بتجريم الافعال التالية:

١- فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعلومات أو محاولة ذلك، أو متى ترتب عنه تغيير معطيات المنظومة أو حذف نظام التشغيل أو تخريبه.

٢- الإدخال أو الإزالة بطريقة الغش لمعطيات في نظام المعالجة الآلية للمعلومات.

٣- القيام عمداً وعن طريق الغش بتصميم أو بحث أو بتوفير، نشر، أو الاتجار بمعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

٤- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم الخاصة بأنظمة المعالجة الآلية للمعطيات.

٥- لمشاركة في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم المنصوص عليها الخاصة بأنظمة المعالجة الآلية للمعطيات".

ويتضح لنا مما سبق أن المشرع الجزائري يشترط في جريمة الدخول الغير للمشروع للبيانات لتحققها توافر السلوك الإجرامي المكون الركن المادي الذي يتمثل في أحد أشكال الاعتداء على نظام المعالجة الآلية للبيانات والذي يكمن في أحد الصور التالية:

١- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات.

٢- الاعتداءات العمدية على نظام المعالجة الآلية للبيانات والتي تشترط وجود نظام معالجة للبيانات كشرط مسبق.

٣- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام: تخريب، اتلاف، الاتجار...

بينما يتكون الركن المعنوي لهذه الجريمة باعتبارها من الجرائم العمدية من القصد الجنائي العام بعنصرية العلم والارادة، بالإضافة إلى القصد الجنائي الخاص الذي يتمثل في نية الغش. فيجب أن تتجه ارادة الجاني إلى ارتكاب أحد صور السلوك الإجرامي المتمثل في الدخول أو البقاء غير المشروع وهو يعلم أن ما يقوم به ليس له الحق في ذلك حتى لو كان بهدف الفضول واثبات القدرة على المهارة. أما فيما يتعلق بالقصد الجنائي الخاص وهو نية الغش فيستدل عليها من خلال الاسلوب الذي تم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، أو بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام انها تمت بقصد الغش.

وتأسيسا على ذلك فقد ذهب الفقه الأمريكي فيما يتعلق بدعوى موريس الذي كان متهماً في قضية دخول غير مصرح به على جهاز حاسب فيدرالي في الولايات المتحدة الأمريكية، فقد دفع محامي موريس بانتفاء الركن المعنوي للجريمة، وذلك وفقا للمعيار التقليدي للقصد الجنائي في الجرائم التقليدية خارج الشبكة، الأمر الذي جعل المحكمة تذهب إلى القول بأن هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المتهم في الولوج إلى حاسب الآلي فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد على استخدام نظم المعلومات والبيانات في

الحاسب الآلي وتحقيق خسائر نتيجة هذا الانتهاك([1]). وبالتالي فللوصول إلى ذلك يستتبع تحديد أركان جريمة الدخول دون تصريح على نظام معالجة للبيانات إلكتروني. وبناء على ذلك تبنت المحكمة معيارين لتحديد الركن المعنوي هما الإرادة أي أن الجاني قد دخل بدون تصريح إلى جهاز غير مصرح بالدخول إليه، وبالإضافة إلى معيار العلم أي أن الجاني كان يعلم بوجود حظر على استخدام هذه النظم للبيانات الإلكترونية.

أما بالنسبة لموقف المشرع المغربي فقد نص في المادة ٧ من قانون حماية المعطيات على الحق في الولوج المشروع للمعطيات الشخصية على "انه يحق للشخص المعني بعد الإدلاء بما يثبت هويته أن يحصل من المسئول عن المعالجة في فترات معقولة وعلى الفور ودون عوض على ما يلي([2]):

أ- تأكيد على أن المعطيات ذات الطابع الشخصي المتعلقة به تعالج أو لا تعالج وكذا على معلومات مرتبطة على الأقل بغايات المعالجة وفئات المعطيات التي تنصب عليها والمرسل إليهم أو فئات المرسل إليهم أو فئات المرسل إليهم الذين أوصلت إليهم المعطيات ذات الطابع الشخصي؛

ب-إحاطة، وفق شكل مفهوم، بالمعطيات التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات، يحق للمسئول عن المعالجة أن يطلب من اللجنة الوطنية تحديد آجال الإجابة على طلبات الولوج المشروعة كما يمكنه التعرض

([1]) - د. وليد طه ، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست ، قطاع التشريع بوزارة العدل جمهورية مصر العربية ، القاهرة ، بدون دار نشر أو تاريخ نشر ، ص ١٧.

([2]) - انظر المادة السابع من القانون المغربي الخاص بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي ، ظهير شريف رقم ١.٠٩.١٥ صادر في ٢٢ من صفر ١٤٣٠ (١٨ فبراير ٢٠٠٩) بتنفيذ القانون رقم ٠٩.٠٨ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

على الطلبات التي يكون شططها بينا، ولاسيما من حيث عددها وطابعها التكراري. في حالة التعرض، يلزم المسئول عن المعالجة الذي قدمت إليه الطلبات بالإدلاء بالحجة على شططها الظاهر.

ج– معرفة المنطق الذي يحكم كل معالجة آلية للمعطيات ذات الطابع الشخصي المتعلقة به".

كذلك فقد نص أن المشرع المغربي على جريمة الدخول الاحتيالي أو المكوث بعد تحقق الاتصال غير المقصود في نظام للمعالجة الآلية للبيانات الشخصية، وهي الأفعال التي نصت عليها المادة ٣-٦٠٧ الفقرتين الأولى والثانية من القانون رقم ٠٣. ٠٧ المتمم لمجموعة القانون الجنائي المغربي وعاقبت عليها بعقوبة الحبس الذي تتراوح مدته ما بين شهر وثلاثة أشهر والغرامة من ٢٠٠٠ إلى ١٠٠٠٠ درهم أو إحدى هاتين العقوبتين فقط مع تشديد العقوبة بمضاعفتها في حالة إذا نتج عن الدخول غير المشروع حذف أو تغيير في البيانات المدرجة في نظام المعالجة أو اضطراب في سيره.

ونستخلص مما سبق أن المشرع المغربي يعاقب في حقيقة الامر بموجب النص السابق عن جريمتين، الجريمة الأولى هي جريمة الدخول غير المشروع بطريقة الغش إلى نظام المعالجة الآلية للبيانات الشخصية محل الحماية القانونية، أما الجريمة الثانية فهي جريمة عدم الخروج من نظام المعالجة الآلية للبيانات الشخصية في حالة تحقق الاتصال الذي قد جرى بطريق الخطأ أو للتجريب([1])، أي الاحتفاظ بحالة الاتصال

([1]) – د. سومية عكور ،الجرائم المعلوماتية وطرق مواجهتها : قراءة في المشهد القانوني والأمني ، ورقة علمية مقدمة إلى المتلقي العلمي في الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من ٢ – ٤ سبتمبر ٢٠١٤ ، كلية العلوم الاستراتيجية ، عمان ، المملكة الأردنية الهاشمية ، ٢٠١٤ ، ص ٥.

وعدم الخروج منه على الرغم من علم الجاني بعدم مشروعية الاتصال الذي حصل أي توافر الارادة الجنائية التي تعتبر في هذه الحالة لاحقة على قيام الشخص بالنشاط الإجرامي المتمثل في الدخول غير المشروع وذلك بانه رغم علمه بذلك ظل في حالة اتصال بنظام المعالجة الآلية للبيانات الشخصية الإلكترونية.

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ٣٧١ من قانون العقوبات على "انه يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة المالية التي لا تزيد على عشرة آلاف ريال، أو بإحدى هاتين العقوبتين ، كل من توصل بطريقة التحايل إلى نظام المعالجة الآلية للبيانات المحفوظة في جهاز حاسب آلي ، أو ضبط داخله ، أو في جزء منه ، بدون وجه حق".

ويستخلص من ذلك أن المشرع القطري يجرم الوصول بأي طريقة كانت بالتحايل إلى نظام المعالجة الآلية للبيانات المحفوظة بالحاسب الآلي. فالمشرع القطري في المادة ٣٧١ عقوبات يجرم الدخول غير المشروع إلى نظام المعالجة الآلية للبيانات المحفوظة في الحاسب الآلي سواء كان ذلك عن طريق التحايل أو كان بدون وجه حق. وكذلك ساوي في العقاب ما بين أن تتم الجريمة عن طريق الدخول غير المشروع بدون وجه حق أو الدخول غير المشروع عن طريق التحايل، وجعل العقاب هو الحبس مدة لا تزيد عن ثلاث سنوات والغرامة التي لا تزيد عن عشرة آلاف ريال أو بإحدى هاتين العقوبتين.

بالإضافة إلى ذلك فقد نص المشرع القطري على تشديد العقاب لتصبح العقوبة حبس مدة لا تقل عن سنة ولا تجاوز ثلاث سنوات، والغرامة المالية التي لا تقل عن عشرة آلاف ريال ولا تزيد على خمسين ألف ريال، أذا ترتب على الدخول غير المشروع

محو أو تعديل في المعلومات الموجودة داخل النظام، أو إتلافه، أو تعطيل تشغيله وذلك وفقا لما تنص عليه المادة ٣٧٢ من قانون العقوبات القطري([1]).

وتطبيقا على ذلك فقد قضت محكمة التمييز القطرية([2]) "بانه صراحة النصوص ووضوح عباراتها تدل بجلاء على أن المشرع قد أثم التوصل بالتحايل إلى نظام المعالجة الآلية للبيانات المحفوظة بالحاسب الآلي ولم يحدد طريقة الدخول على الحاسب الآلي سواء كانت من جهاز المجني عليه نفسه أو من أي جهاز آخر ، فإن ما تقول به الطاعنة من أنه يلزم للتجريم أن يكون الدخول إلى نظام المعالجة الآلية للبيانات المحفوظة في الحاسب أن يكون من خلال جهاز الحاسب الخاص بالمجني عليه فقط إنما هو تخصيص للنص بغير مخصص ، هذا فضلاً عن أنه يترتب عليه عدم تأثيم الدخول إلى نظام المعالجة الآلية للبيانات المحفوظة إذا كان عن طريق جهاز آخر خلاف جهاز المجني عليه وهو ما لم يقره الشارع بتلك المادة، وإذ كانت المادة ٣٧٠ من قانون العقوبات سالفة البيان قد بينت أن وحدات الإدخال لجهاز الحاسب الآلي من نظام المعالجة الآلية للبيانات المحفوظة في الجهاز، فإن كلمة السر للمرور إلى البريد الإلكتروني بجهاز الحاسب الآلي الخاص بالمجني عليه هي ولاشك وحدة من نظام المعالجة الآلية للبيانات إذ إنها إحدى البيانات الموجودة على الجهاز وبها يمكن إعطاء نتيجة وهي الدخول إلى البريد الإلكتروني للمجني عليه ، ومن ثم فإن تعديلها يكون تعديلاً في المعلومات الموجودة داخل النظام مؤثم بالمادة ٣٧٢ من قانون العقوبات".

([1]) – تنص المادة ٣٧٢ من قانون العقوبات القطري على انه "يُعاقب بالحبس مدة لا تقل عن سنة ولا تجاوز ثلاث سنوات، وبالغرامة التي لا تقل عن عشرة آلاف ريال ولا تزيد على خمسين ألف ريال، كل من ارتكب فعلاً من الأفعال المنصوص عليها في المادة السابقة، إذا نتج عن ذلك محو أو تعديل في المعلومات الموجودة داخل النظام، أو إتلافه، أو تعطيل تشغيله".

([2]) – تمييز جنائي قطري ، جلسة ١٦ نوفمبر ٢٠٠٩ ، الطعن رقم ٢٢٩ لسنة ٢٠٠٩ تمييز جنائي.

كذلك فقد قضت محكمة التمييز القطرية بإن تجريم الشارع للتوصل بالتحايل إلى نظام المعالجة الآلية للبيانات المحفوظة في جهاز حاسب آلي خاص بالغير والتعديل في المعلومات الموجودة داخل هذا النظام يحول دون اعتبار هذا الفعل مرتبطاً بحق وإنما يجعل منه إذا وقع جريمة يستحق جانيها العقاب الذي فرضه الشارع لفعلته.

أما بالنسبة لموقف المشرع الإماراتي فقد نص في المادة الثانية من قانون مكافحة جرائم تقنية المعلومات رقم ٢ لسنة ٢٠٠٦ على "أنه ١- كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين. ٢- فإذا ترتب على الفعل الغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين. ٣- فإذا كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة المالية التي لا تقل عن عشرة آلاف درهم أو بإحدى هاتين العقوبتين".

وتطبيقا على ذلك فقد قضت محكمة التمييز الإماراتية بتايد حكم محكمة الاستئناف بمصادرة المضبوطات وبتغريم المتهم مبلغ عشرة الاف درهم(١) "في التهمة الخاصة بقيام أحد الاشخاص باستخدام كمبيوتر خاص بكسر الكلمات السرية الخاصة ببعض موظفي مؤسسة الأمارات للاتصالات والدخول إلى الأماكن غير المصرح بها لمشتركي الشبكة ونسخ بعض الملفات الخاصة بالكلمات السرية ورسائل البريد الإلكتروني لموظفي مؤسسة الأمارات للاتصالات مع علمه بذلك، مما يشكل انتهاك للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً. حيث ارتكب المتهم جريمتين هما إساءة

(١) – تمييز جنائي دبي ، محكمة التمييز بدبي جلسة ٨ ديسمبر ٢٠٠١ ، في القضية رقم ٢٣٠ /٢٠٠١ جزاء.

استخدام واستغلال شبكة الانترنت في أعمال غير مشروعة تمثلت في تزويد الكمبيوتر الخاص الذي يستخدمه والمتصل بهذه الخدمة ببرنامج قرصنة تمكن بواسطته من كسر الكلمات السرية الخاصة ببعض موظفي مؤسسة الأمارات للاتصالات والدخول إلى الأماكن غير المصرح بها لمشتركي الشبكة دخولها ونسخ بعض الملفات الخاصة بالكلمات السرية ورسائل البريد الإلكتروني لموظفي مؤسسة الأمارات للاتصالات مع علمه بذلك. بالإضافة إلى ذلك فض عدد من الرسائل الواردة إلى بعض موظفي مؤسسة الأمارات للاتصالات والمسجلة على البريد الإلكتروني للمؤسسة والاحتفاظ بها في جهاز الكمبيوتر الخاص به. وذلك بالمخالفة للمادة ٤٦ الفقرة السابعة من القانون رقم ١ لسنة ١٩٩١ في شأن مؤسسة الاتصالات والمادة ٣٨٠ من قانون العقوبات الإماراتي".

وفي تطبيق أخر لجريمة الدخول غير المشروع قضت محكمة العين الابتدائية الإماراتية بمعاقبة المتهم بالحبس لمدة ستة أشهر مع إيقاف التنفيذ والابعاد عن الدولة ومصادرة جهاز الحاسب الآلي المضبوط(١) "عن تهمة توصل المتهم وبغير حق إلى الدخول على جهاز الحاسب الآلي للمجني عليها ونسخ البيانات والمعلومات الشخصية الخاصة بها. ثم هدد المتهم المجني عليها بواسطة الشبكة المعلوماتية بإسناد أمور خادشه بالشرف والاعتبار وهو بأنه سوف يقوم بنشر صورها الخاصة عبر فضاء الانترنت إذا لم تضيفه إلى قائمة أصدقائها في برنامج المحادثة المرئية والمسموعة ماسنجر. وذلك لمخالفة المواد رقم ١، ٩ الفقرة الثانية، و٢٥ من قانون مكافحة جرائم تقنية المعلومات الاتحادي الإماراتي".

---

(١) – القضية رقم ٥٠٤٤ لسنة ٢٠٠٩ ، محكمة العين الابتدائية ، دولة الامارات العربية المتحدة.، انظر ذلك : المستشار: محمد محمود الكمالي ، ورقة بحثية حول بعض قضايا جرائم تقنية المعلومات من محاكم دولة الامارات العربية المتحدة ، المؤتمر الاقليمي الاول لحماية برنامج الحاسوب وجرائم الانترنت ، ٢٤ ألي ٢٥ اكتوبر ٢٠١٠ ، عمان ، الاردن.

ثانيا. يثور التساؤل حول ما إذا تم الدخول غير المشروع على نظام المعالجة الآلية للبيانات الشخصية من خلال تقنية التقاط البيانات الإلكترونية هل يشكل ذلك سلوك إجرامي مكون للركن المادي لجريمة الدخول غير المشروع؟

ويقصد بذلك أن الجاني لم يحصل على البيانات الشخصية الإلكترونية من خلال التواجد داخل نظام المعالجة الآلية للبيانات وانما تم ذلك من خلال التقاط الجاني للبيانات الشخصية الإلكترونية المرسلة من نظام المعالجة الآلية للبيانات عن طريق الذبابات المغناطسية أو أي وسيلة إلكترونية أخرى تسمح لذلك، دون أن يضطر معها الجاني الدخول على نظام المعالجة الآلية للبيانات الشخصية.

في بادئ الأمر لم يكن المشرع الفرنسي يجرم التقاط البيانات الشخصية الإلكترونية، لذلك حول بعض الفقه الفرنسي الاعتماد على التفسير الواسع لنص المادة ٢٢٦-١ من القانون العقوبات الفرنسي الذي يجرم استعمال الوسائل التقنية للمساس بالحياة الخاصة للأفراد، عبر الالتقاط وتسجيل أقوالهم أو الحصول على صورهم في الأماكن الخاصة دون رضاهم. إلا أن هذا الاتجاه من الفقه الفرنسي كان محل للانتقاد لمخالفته أحد أهم القواعد الجنائية وهي التفسير الضيق للنصوص الجنائية(١). حيث أن النص المذكور في المادة السابقة يجرم التقاط الأقوال والصور الخاصة وليس التقاط البيانات الإلكترونية الذي ينصب على البيانات لا الأقوال أو الصور، وبالتالي لا يجوز للفقه الفرنسي التوسع في تفسير المادة ٢٢٦-١ من قانون العقوبات الفرنسي بأن يتم إلباس عملية التقاط الأقوال والصور الخاصة غيرها من حالات التقاط البيانات الشخصية الإلكترونية.

(١) – د. رشيد وظيفي ، الاطار القانوني للجريمة الإلكترونية في التشريع المغربي ، ندوة حول الجرائم الإلكترونية المالية ، نظمت من خلال محكمة الاستئناف بالرباط بمناسبة الذكرى المئوية لتأسيسها ندوة علمية ثالثة ، المملكة المغربية ،٥ ديسمبر ٢٠١٣ ، ص ٢٨ ، ٢٩.

في مقابل ذلك يأخذ المشرع الأمريكي من البداية بالتعريف الواسع لجريمة الدخول غير المشروع لنظم معالجة البيانات الشخصية الإلكترونية حيث يعتبر أن الالتقاط للإشارات الناجمة عن عملية التبادل للبيانات الشخصية من خلال الشبكات يعد دخولاً غير مشروع به إلى نظام معالجة البيانات الشخصية الإلكترونية، ونص على ذلك في المادة ١٠٣٠ الفقرة (a) من قانون الأمريكي الخاص بإساءة استخدام الحاسبات الآلية(١). فيجرم المشرع الأمريكي الدخول المجرد إلى الحاسبات الخاصة بالحكومة الأمريكية، أو إلى الحاسبات التي تؤدي الدخول غير القانوني إليها المساس بأعمال الحكومة الأمريكية، والحاسبات الآلية تشتمل وفقا لهذا القانون على كل جهاز إلكتروني أو كيمائي أو كهربائي أو جهاز سريع لمعالجة البيانات والمعلومات وكذلك وسائل الاتصالات التي تعمل بالاتصال مع أي من هذه الاجهزة(٢).

وتطبيقاً على ذلك القضية التي يطلق عليها الجحيم العالمي Global Hell والتي تتلخص وقائعها في قيام مجموعة من الأشخاص باختراق مواقع البيت الابيض الإلكتروني وكذلك المباحث الفيدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وقد تم إدانة اثنين من الأفراد هذه المجموعة، وظهر من التحقيقات أن الدافع وراء ارتكاب هذه المجموعات لجريمتهم هو مجرد الاختراق أكثر من التدمير أو التقاط المعلومات والبيانات ، وقد تطلب الوصول إلى هذه المجموعات مئات الساعات بين

---

(١) – USA Computer crimes acts ١٨ U.S.C. ١٠٣٠, Fraud and related activity in connection with computers,
www.law.cornell.edu/uscode/١٨/١٠٣٠/html.

(٢) – د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادية ، دراسة نظرية وتطبيقية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ ، ص ٣٣٤ ، ٣٣٥.

ملاحقتها وتتبع آثار أنشطتها ، وكلف التحقيق في هذه القضية مبالغ طائلة نظراً لما تطلبه من وسائل معقدة في المتابعة([1]).

أما بالنسبة لموقف المشرع المغربي فقد نص في المادة ١١٥ من قانون الجنائي على "أنه دون الإخلال بالمقتضيات الجنائية الأشد، يعاقب بالحبس من شهر إلى سنة وبالغرامة المالية من ١٠٠.٠٠٠ إلى ١٠٠.٠٠٠ درهم أو بإحدى هاتين العقوبتين فقط كل من قام بوضع وسائل مهيأة لإنجاز التقاطات أو التقط أو بدد أو استعمل أو نشر مراسلات مرسلة بواسطة وسائل الاتصال عن بعد خلافاً للمقتضيات المشار إليها في المواد السابقة".

ويتضح مما سبق أن المشرع المغربي قد جرم عملية الالتقاط للبيانات صراحة باعتبارها جريمة مستقلة عن جريمة الدخول غير المشروع على نظام المعالجة للبيانات، إلا أن المشرع المغربي قد ربط عملية الالتقاط بالمراسلات أو الاتصالات المنجزة أو المرسلة بواسطة وسائل الاتصال عن بعد ، أي أنه يشترط للتجريم عن هذه الجريمة أن يتم انجاز الالتقاط للبيانات والمعلومات حتي يتم العقاب وفقا لنص المادة ١١٥ من قانون الجنائي المغربي([2]). ولكن في هذه الحالة يؤخذ على المشرع المغربي عدم النص الصريح على تجريم حالة التقاط بيانات الحاسب الآلي عن طريق ذبذبات الحقل المغناطيسي حتى ولو كان الحاسب الآلي غير مرتبط بشبكة الإنترنت، وحتي ولو كانت

([1]) – د. عبد الفتاح مراد ، شرح جرائم الكمبيوتر والانترنت ، البهاء للبرمجيات والكمبيوتر للنشر الالكتروني ، الاسكندرية ، بدون سنة نشر ، ص ٣٨٤.

([2]) – د. عبد الرحمان اللمتوني ، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة ، الندوة العلمية الثالثة التي نظمتها محكمة الاستئناف بالرباط بمناسبة الذكري المئوية لتأسيسها تحت عنوان تأثير الجريمة الإلكترونية على الائتمان المالي ، ٥ ديسمبر ٢٠١٣ ، المملكة المغربية ، ص ٥٢ ، ٥٣.

البيانات الملتقطة مخزنة في ذاكرة الحاسب الآلي (الهارد دسك) أو غير مرسلة أو معدة للأرسال.

أما بالنسبة لموقف المشرع المصري فقد كان واضح في تجريم الاعتراض غير المشروع للبيانات والمعلومات الشخصية، حيث نص في المادة ١٦ من قانون مكافحة جرائم تقنية المعلومات على "أن يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائتين وخمسين ألف جنية ، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها".

وعليه فقد نصت المادة ٣ من اتفاقية بودابست لعام ٢٠٠١ للجرائم الإلكترونية على تجريم الالتقاط المتعمد وغير المشروع للبيانات والمعلومات باستخدام الوسائل الفنية المختلفة، وذلك أثناء إرسال هذه البيانات إلى المرسل إليه أو لدى المصدر أو داخل شبكة المعلومات. ويدخل في ذلك أيضاً الرسائل المرسلة بواسطة الأجهزة الكهرومغناطيسية الصادرة عن شبكة معلومات والتي تحوي مثل هذه البيانات، سواء بغرض إجرامي أو لمجرد الاتصال بين شبكة معلومات وشبكة أخرى.

ولقد أوضحت المذكرة التفسيرية لاتفاقية بودابست للجرائم الإلكترونية بأن الهدف من هذه المادة هو حماية الحق في حرية الاتصالات واحترام الحق في خصوصية البيانات خاصة البيانات الشخصية الإلكترونية، بحيث لا يجوز للغير أن يخل بقواعد حماية خصوصية البيانات ويقوم بالاطلاع عليها عن طريق التقاط هذه البيانات بطريقة

غير مشروعة مما يشكل في نفس الوقت انتهاك للحق في احترام المراسلات التي تنص عليها المادة الثامنة من الاتفاقية الأوربية لحقوق الانسان([1]).

ثالثا. يثور كذلك إشكالية خاصة بصورة من الصور الحديثة للولوج غير المشروع للبيانات الشخصية المعالجة إلكترونياً، ويتمثل عندما يتيح موقع التوصل الاجتماعي مثل الفيسبوك أو التوتير أو غيرها للمستخدمين إضافة أدوات إلى حساباتهم الشخصية وممارسة الألعاب مع تطبيقات طرف ثالث دون مغادرة موقع فيسبوك، الأمر الذي يترتب عليه انتهاك لخصوصية البيانات الشخصية، فعندما يقوم المستخدم بتثبيت تطبيق خاص بفيسبوك ، فإن التطبيق يمكن أن يطلع على أي شيء يطلع عليه المستخدم ، وربما يطلب ذلك التطبيق بيانات ومعلومات عن المستخدم، وعن أصدقائه، وأعضاء شبكته، وليس هناك شيء يمكنه إيقاف مشغل التطبيق من جمع هذه البيانات الشخصية والاطلاع عليها وإسادة استخدامها .

ونظرا لخطورة هذا الأمر فقد قامت شركة فيسبوك وبوضع شروط اتفاقية لاستخدام الفيسبوك تحث فيها مطوري التطبيقات على الامتناع عن القيام بذلك الأمر، ولكن في حقيقة الأمر لا يملك موقع فيسبوك أي وسيلة لكشفهم أو لمنعهم عن القيام بهذا الأمر. وبناء على ذلك فقد قام المفوض الكندي بحماية خصوصية البيانات الشخصية بالضغط على فيسبوك لتعديل سياسة الحفاظ على خصوصية البيانات الخاصة بالموقع والقيام بتعديلها بحيث لا يمكن للتطبيقات الوصول إلى البيانات الشخصية لحسابات أصدقاء المستخدم دون الحصول على إذن صريح من كل صديق.

([1]) – تنص المادة الثامنة من الاتفاقية الأوربية لحقوق الانسان المبرمة في ٤ نوفمبر ١٩٥٠ على أنه": ١. لكل إنسان حق احترام حياته الخاصة ، والعائلية ومسكنه ومراسلاته. ٢. لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقا للقانون وبما يمليه الضرورة في مجتمع ديمقراطي لصالح الامن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع ، أو حفظ النظام ومنع الجريمة ، أو حماية الصحة العامة والآداب ، او حماية حقوق الاخرين وحرياتهم". د. محمود شريف بسيوني ، خالد محي الدين ، الوثائق الدولية والإقليمية المعنية بحقوق الانسان ، المجلد الثالث ، دار النهضة العربية ، القاهرة ،٢٠٠٣ ، ص ١٣٨.

وانطلاقا مما سبق نري أن واقع هذا الأمر يتمثل في درجة عالية من الخطورة، حيث أن المستخدمون لمواقع التواصل الاجتماعي يعتبروا أن ملفاتهم الشخصية على مواقع التواصل الاجتماعي بمنزلة شكل من أشكال التعبير عن الذات، ولكنها في حقيقة الأمر ذات قيمة تجارية كبيرة لشركات التسويق الإلكتروني، وكذلك لمواقع الشبكات المنافسة ولصوص البيانات الشخصية المعالجة إلكترونياً. وبالتالي فإن عملية الولوج غير المشروع للبيانات الشخصية المعالجة إلكترونياً والقيام بالتنقيب في هذه البيانات لها آثار خطيرة على الحق في الخصوصية. حيث أن عملية التحليل للبيانات الشخصية وتلخيصها في معلومات يمكن استخدامها لزيادة الدخل أو خفض التكاليف أو كليهما ، فتسمح برمجيات التنقيب في المعلومات للمستخدمين بتحليل البيانات من وجهات نظر متعدة (١)، وتصنيفها، وتقييم العلاقات المحددة، أي تبحث عن الأنماط أو الارتباط بين العديد من المجالات في قواعد البيانات. وبالتالي التوصل بالتنقيب في الكشف في البيانات عن نمط من السلوك للشخص يمثل انتهاك واضح لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، مما يوجب العمل على مواجهته من الناحية القانونية.

رابعا. مدى الالتزام الشركات الخاصة العاملة في مجال البيانات الشخصية الإلكترونية في مواجهة الدخول غير المشروع للبيانات الشخصية الإلكترونية:

فقد نص البند الثالث من قرار مجلس الوزراء السعودي رقم ١٦٣ لسنة ١٤١٧هـ على أن تلتزم الشركات المقدمة لخدمة الانترنت والأطراف المستخدمة للشبكة بما يلي:

(١) – ريموند واكس ، الخصوصية ، المرجع السابق ، ص ١٣٤.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

١- الامتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الإنترنت، أو إلى معلومات خاصة أو مصادرة معلومات دون الحصول على موافقة.

٢- الامتناع عن الاستخدام الشبكة لأغراض غير مشروعة.

٣- ما صدر عن لجنة الإنترنت الأمنية الدائمة من ضوابط لاستخدام وأمن الإنترنت في المملكة العربية السعودية بخصوص احترام خصوصية البيانات والمعلومات المنقولة عبر الإنترنت من خلال الوحدة([١]) ، والتي تتم كنتيجة للتعامل بين الأطراف المختلفة داخل وخارج المملكة العربية السعودية.

أما بالنسبة للولايات المتحدة الأمريكية فقد قاومت في البداية اعتماد تشريعات لحماية البيانات وفقا للمبادئ التوجيهية الأوربية بالنسبة للقطاع الخاص، حيث أن نهج التنظيم الذاتي الخاص يتناقض مع النهج الاوربي ، ولكن ونتيجة لأزمة الائتمان العقاري في الولايات المتحدة الأمريكية في عام ٢٠٠٨ ، تم تعيين مفوض فيدرالي مستقل خاص بشأن خصوصية البيانات. بالإضافة إلى ذلك فقد تم تصميم برنامج اطلق عليها اسم الملاذ الآمن([٢])، وقد صمم هذا البرنامج لإقناع الاتحاد الأوربي بأن الشركات الأمريكية المصادقة على الخطة سوف تقدم الحماية الكافية للخصوصية البيانات الشخصية على النحو المحدد في الإرشادات التوجيهية لحماية البيانات التابعة للاتحاد الأوربي. وتنص مبادئ الملاذ الآمن على ما يلي:

([١]) – المقصودة بالوحدة هي وحدة خدمات الانترنت بمدينة الملك عبد العزيز للعلوم والتقنية الجهة الوحدة المخولة بتوفير خدمة الانترنت بالمملكة العربية السعودية، وذلك حسب ما نص عليه قرار مجلس الوزراء السعودي رقم ١٦٣ بتاريخ ١٤١٧/١٠/٢٤ هـ.

([٢]) – جي بي رول ، الخصوصية في خطر ، اكسفورد يونيفرستس برس ، ٢٠٠٧ ، ص ١٣٨.

المبدأ الأول. الالتزام بالإشعار: فيجب على المؤسسة إعلام الأفراد بالأغراض التي تجمع المعلومات من أجلها، وكيفية الاتصال بالمؤسسة في حال وجود أي استفسارات أو شكاوى، وأنواع الأطراف الثالثة التي قد تفصح عن المعلومات لها ، والخيارات والوسائل التي تقدمها المؤسسة للأفراد من أجل الحد من استخدام المعلومات والإفصاح عنها.

المبدأ الثاني. الاختيار: فيجب على المؤسسة أن توفر للأفراد الفرصة لاختيار عدم قبول هل ستستخدم المعلومات الشخصية التي يقدمونها أو يكشف عنها لأطراف ثالثة وكيفية ذلك حينما يتنافى هذا الاستخدام مع الغرض الذي من أجلة جمعت أصلاً أو مع أي غرض آخر يعلم الشخص به بإشعار.

المبدأ الثالث. نقل المعلومات: يحق للمؤسسة كشف المعلومات الشخصية لطرف ثالث بما يتفق مع مبادئ الإشعار والاختيار.

المبدأ الرابع. الأمن: يجب على المؤسسات التي تنشئ المعلومات الشخصية أو تصونها أو تستخدمها أو تنشرها أن تتخذ إجراءات معقولة لضمان موثوقيتها في الاستخدام المقصود والاحتياطات المعقولة لحمايتها من الضياع وسوء الاستخدام والوصول غير المصرح به والكشف والتعديل والتدمير.

المبدأ الخامس. سلامة البيانات: تماشياً مع هذه المبادئ يحق فقط للمؤسسة معالجة المعلومات الشخصية المرتبطة بالأغراض التي جمعت لها، بالقدر اللازم من أجل هذه الأغراض، ويجب على المؤسسة أن تتخذ خطوات معقولة لضمان أن البيانات دقيقة وكاملة وحديثة.

المبدأ السادس. الوصول للمعلومات: يجب أن يكون للأفراد قدرة معقولة على الوصول إلى المعلومات الشخصية التي تمتلكها المؤسسة عنهم، وأن يكونوا قادرين على تصحيح أو تعديل تلك المعلومات إذا كانت غير دقيقة.

المبدأ السابع. التطبيق: يجب أن تتضمن الحماية الفعالة للخصوصية آليات لضمان الامتثال لمبادئ الملاذ الآمن، وحق الأفراد أصحاب البيانات الذين تأثروا بسبب عدم الامتثال للمبادئ في الشكوى، والعواقب للمؤسسة عندما لا يتم اتباع هذه المبادئ.

وبالرغم مما سبق إلا أن وثيقة مبادئ الملاذ الآمن محل انتقاد على أساس أنها وثيقة تفتقر للنصوص الجزائية الصارمة لمواجهة المؤسسات التي تتعامل في البيانات الشخصية في الولايات الأمريكية وبالتالي نجد أن الواقع العملي هو عدم امتثال المؤسسات بهذه المبادئ بل وصل الأمر بتجاهلها لهذه الوثيقة. بالإضافة إلى ذلك فهناك قصور واضح في سياسة تنفيذ وثيقة الملاذ الآمن يتمثل في عدم وجود آليه لتنفيذ الشكاوى من تلك الشركات التي اعتمدت هذا النظام.

وتطبيقا على ذلك وفي عام ٢٠١٥ قضت محكمة العدل الأوربية ببطلان اتفاق الاتحاد الأوربي مع الولايات المتحدة الأمريكية المتعلق باتفاقية الملاذ الأمن للبيانات، وبناء على ذلك فقد تم تعديل اتفاق الملاذ الأمن وأصبح هناك اتفاق جديد بين الاتحاد الأوربي والولايات المتحدة الأمريكية لحماية البيانات يطلق عليه درع الخصوصية الأوربية الأمريكية في يوليو ٢٠١٦، وتهدف الاتفاقية الجديدة إلى تسهيل عمل المنظمات في نقل البيانات عبر المحيط الأطلسي. وتتمثل النقاط الرئيسية للاتفاقية على النحو التالي:

١) تشكل الولايات المتحدة هيئة للتعامل مع شكاوى مواطني الاتحاد الأوروبي بشأن الأميركيين الذين يتجسسون على البيانات الخاصة بهم.

٢) يقدم المكتب لمدير الاستخبارات الوطنية الأمريكية التزامات كتابية بأن البيانات الشخصية للأوروبيين لن تخضع للمراقبة الجماعية.

٣) يجري الاتحاد الأوروبي والولايات المتحدة مراجعة سنوية للتأكد من أن النظام الجديد يعمل بشكل صحيح.

وانطلاقا مما سبق فقد أقرت الهيئة الأوروبية للإشراف على حماية البيانات إن اتفاقية درع الخصوصية يجب أن يتوافر فيه الحماية الكافية ضد المراقبة العشوائية والتزامات بشأن الرقابة والإنصاف وحقوق حماية البيانات. ومن خلال هذه التعديلات الاتفاقية الآن نستخلص انها قد اضافت العديد التغييرات وهي كالتالي:

١- ثمة تعهد من الولايات المتحدة الأمريكية يؤكد على أن جمع مجموعة كبيرة من البيانات المرسلة من الاتحاد الأوروبي إلى الولايات المتحدة لا يمكن أن يحدث إلا في ظل شروط محددة مسبقاً، ويجب أن يكون محددا ومركزا قدر المستطاع.

٢- يتعين على الشركات حاليا حذف البيانات التي لم تعد تخدم الغرض الذي جمعت من أجله.

٣- التأكيد على أن هيئة الشكاوى ستكون مستقلة عن الأجهزة الأمنية الوطنية.

المطلب الثالث. اتجاهات السياسة الجنائية التشريعية لتجريم الدخول أو الالتقاط غير المشروع للبيانات الشخصية

في واقع الأمر أن اتجاهات السياسة الجنائية التشريعية بالنسبة لتجريم الدخول أو الالتقاط غير المشروع للبيانات الشخصية المعالجة إلكترونياً، قد انقسمت إلى اتجاهين فيما يتعلق بالنص على تجريم الدخول والالتقاط غير المشروع للبيانات الشخصية التي

تم معالجتها إلكترونياً في قانون خاص بذلك أو بالرجوع إلى القواعد العامة التقليدية في قانون العقوبات وهو ما سوف نتناوله على النحو التالي:

الاتجاه الاول من التشريعات المقارنة هي التشريعات السالف ذكرها وهي الأمريكي، الانجليزي، الفرنسي، الجزائري، الإماراتي، القطري، فقد جرمت الدخول إلى النظام الإلكتروني للبيانات الشخصية بالنص على ذلك في قواعد خاص بهذه الجريمة، والذي وصفته مرة بالدخول عن طريق الغش، ومرة بالدخول عن طريق التحايل، وأخرى بالدخول غير المشروع([1]). كما أنها قد فرقت بين فعل الدخول والبقاء، فقد يكون فعل البقاء المجرم نتيجة دخول مشروع، بينما الدخول المجرم هنا هو فعل غير مشروع، ويعد من الجرائم المؤقتة والشكلية، التي تكتمل بمجرد تحقيق السلوك الإجرامي دون تطلب ركن مادي للجريمة، في حين يعتبر البقاء من الجرائم المستمرة فمجرد التواجد المعنوي للجاني داخل نظام للمعالجة الآلية للمعلومات واستغراقه لحيز وقتي بداخله تحقق الجريمة. وتتحقق الجريمة متى كان الدخول أو البقاء مسموح ومشروع ولكن تجاوز الفاعل الوقت المحدد والمسموح به أو الغرض المصرح له بالدخول خلافاً لإرادة صاحب الشأن المسيطر على النظام، وينتفي القصد الجنائي إذا دخل المستخدم إلى النظام بطريق الخطأ، لان ذلك يعد جهلاً بالوقائع ولكن يسال جنائيا إذا دخل بطريق الخطأ إلى نظام معلوماتي، وظل متجولا فيه مع علمه بذلك.

وبالرغم مما سبق إلا أنه يؤخذ على هذه التشريعات السابقة انها لم تورد تعريف لنظام المعالجة الآلية للبيانات مكتفية بوضعه محلاً للحماية أي محل لجريمة الدخول

([1]) – د. محمد حماد مرهج الهيتي ، الجريمة المعلوماتية نماذج من تطبيقاتها ، دراسة مقارنة في التشريع الاماراتي والسعودي والبحريني والقطري والعماني ، دار الكتب القانونية ، القاهرة ، ٢٠١٤ ، ص ٢٢٩.

غير المشروع. لذلك فقد عرف الفقه الفرنسي نظام المعالجة الآلية للبيانات بانه: "كل مركب يتكون من وحدة أو ومجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والبيانات وأجهزة الادخال والاخراج وأجهزة الربط والتي يربط بينها مجموعة العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة البيانات على أن يكون هذا المركب خاضع لنظام الحماية الفنية"([1])، وبناء على ذلك نستطيع القول بأن نظام معالجة البيانات يتكون من عنصرين هما كالتالي:

١- مركب: يتكون من عناصر مادية ومعنوية مختلفة تربط بينها نتيجة علاقات توحدها نحو تحقيق هدف محدد.

٢- ضرورة خضوع النظام لحماية فنية: حفاظا على خصوصية البيانات المتناقلة عبر الشبكات، ويوجد ثلاث أنواع من الانظمة: أ. أنظمة مفتوحة للجمهور، ب. أنظمة قاصرة على أصحاب الحق وبدون حماية فنية، ج. أنظمة قاصرة على أصحاب الحق وتتمتع بالحماية الفنية، والنوع الثالث فقط هو المتمتع بالحماية الجنائية، ولكن التشريعات لم تشرط وجوده، تماشيا مع الراي الراجح من الفقه ذلك أن الحماية الجنائية تمتد لتغطي أنظمة المعالجة الآلية للبيانات سواء كانت محمية وغير محمية.

أما بالنسبة للاتجاه الثاني من التشريعات التي لم تجرم جريمة الدخول أو الالتقاط غير المشروع في قانون خاص بحماية البيانات الشخصية، ويتضح من ذلك أن هذه التشريعات أخذت بالنهج التقليدي وفقا للقواعد العامة من قانون العقوبات، مثال أن يتم قياس جريمة الدخول غير المشروع لنظام معالجة الآلية للبيانات الشخصية الإلكترونية وجريمة الاستيلاء على البيانات من النظام على القواعد التقليدية الموجودة في قانون

([1]) – انظر المادة الخامسة من القانون الفرنسي لحماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨.

العقوبات أو أي قانون آخر. فهل يجوز أن يقاس السلوك الأول على جريمة دخول منزل الغير بدون إذن وهي اختراق حرمة المنازل، والقياس هنا لتوافر وحدة العلة وهو الدخول بدون إذن فأي نص من نصوص السرقة العادية سيطبق على الاستيلاء على البيانات الشخصية الإلكترونية، وهل نحن أمام اختلاس تقليدي أم اختلاس مشدد، وإذا كان ذلك كذلك فما هو ظرف التشديد، سيكون الليل أو التسور أو دخول بيوت مسكونة أو استخدام السلاح؟ والواضح أن هذه الظروف المشددة غير متصور وجودها في جريمة الدخول أو الالتقاط غير المشروع للبيانات الشخصية المعالجة إلكترونياً، وبالتالي لا يقبل أن نأخذ بالاتجاه التقليدي وتوقيع عقوبات الجرائم التقليدية لجرائم مختلفة وتمثل خطورة على حق الأشخاص في الخصوصية الذي يحميه الاتفاقيات الدولية والدساتير والقوانين.

أما بالنسبة لموقف المشرع المصري فنجد أنه قد أخذ في البداية بالنهج التقليدي في تجريم الدخول غير المشروع للبيانات الشخصية المعالجة إلكترونياً، فقد نص في المادة ٧٦ من قانون الأحوال المدنية رقم ١٣٤ لسنة ١٩٩٤ على "انه يعاقب بالسجن المشدد كل من اخترق أو حاول احتراق سرية البيانات أو المعلومات أو الاحصاءات المجمعة بأية صورة من الصور، وتشدد العقوبة فتصبح السجن المؤبد إذا وقعت الجريمة في زمن الحرب". وكذلك نصت المادة ٧٤ من نفس القانون على تجريم "كل من أطلع أو شرع في الاطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها أو قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو بالمساس بها بأي صورة من الصور أو أذاعها أو أفشاها في غير الأحوال التي نص عليها القانون ووفقا للإجراءات المنصوص عليها، ويعاقب الشخص بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تزيد عن خمسمائة جنية أو بإحدى هاتين العقوبتين". ويشدد العقوبة وتصبح السجن إذا وقعت الجريمة على البيانات أو المعلومات أو الاحصاءات المجمعة.

بالإضافة إلى ذلك فقد نص المشرع المصري في المادة الثالثة من قرار رئيس الجمهورية بالقانون رقم ٣٥ لسنة ١٩٦٠ بشأن الإحصاء والتعداد، المعدل بالقانون رقم ٢٨ لسنة ١٩٨٢ على أن "البيانات الفردية التي تتعلق بأي إحصاء أو تعداد سرية ولا يجوز إطلاع أي فرد أو هيئة عامة أو خاصة عليها أو إبلاغه شيئًا منها كما لا يجوز استخدامها لغير الأغراض الإحصائية أو نشر ما يتعلق منها بالأفراد إلا بمقتضى إذن مكتوب من ذوي الشأن. ولا يجوز استغلال أي بيان إحصائي كأساس لربط ضريبة أو لترتيب أي عبء مالي آخر ولا اتخاذه دليلًا في جريمة أو أساسًا لأي عمل قانوني" .

كذلك تنص المادة الرابعة من نفس القانون على أن "يعاقب بالحبس مدة لا تتجاوز ستة أشهر وبالغرامة المالية التي لا تزيد على مائة جنيه أو بإحدى هاتين العقوبتين:

١- كل من أخل بسرية البيانات الإحصائية أو أفشى بيانًا من البيانات الفردية أو سرًا من أسرار الصناعة أو التجارة أو غير ذلك من أساليب العمل التي يكون قد أطلع عليها بمناسبة عمله في الإحصاء أو التعداد.

٢- كل من حصل بطريق الغش أو التهديد أو الإيهام بأية وسيلة أخرى على بيانات أو معلومات سرية بشأن الإحصاءات أو التعدادات أو شرع في ذلك".

ونستخلص مما سبق أن المشرع المصري يحمي خصوصية البيانات الشخصية التي تم معالجتها على الحاسبات الآلية الخاصة بمصلحة الأحوال المدنية فقط، ولا يمتد إلى حماية البيانات الشخصية الموجودة على الحاسبات الآلية الخاصة أو غيرها من المؤسسات. بالإضافة إلى ذلك يحمي البيانات والمعلومات الشخصية التي تتعلق بأي تعدد أو إحصاء أيا كانت الوسيلة التي يحتفظ بها بما في ذلك حفظها وتخزينها في نظم المعلومات والبيانات الإلكترونية، كما يشمل بالحماية الدخول غير المشروع أو الاطلاع عليها أو التمكن من الحصول عليها، وجعل المشرع المصري المحافظة على سريتها يقع على عاتق من له صله بتلك المعلومات والبيانات بحكم طبيعة عمله وفقا لما ينص

عليه القانون واللوائح. وبناء على ذلك يتضح أن موقف المشرع المصري محل انتقاد وذلك لأنه لم ينص على الحماية الكاملة والشاملة للبيانات الشخصية التي تم معالجتها إلكترونياً ، فالمواد السابقة لا يمتد فيها الحماية الجنائية للجرائم التي ترتكب عبر شبكة الإنترنت على البيانات والمعلومات الشخصية(١) التي تم معالجتها إلكترونياً. وبالتالي يجب على المشرع المصري التدخل بإصدار تشريع خاص للمواجهة الشاملة وحماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونيا على غرار ما فعل المشرع الفرنسي والتشريعات العربية مثل المشرع التونسي والقطري والمغربي.

إلا أن موقف المشرع المصري قد تغيير بعد صدور قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ في ١٤ أغسطس ٢٠١٨، والذي نص في المواد ١٤، ١٥، ١٦ على تجريم الدخول غير المشروع على البيانات والمعلومات، وجريمة تجاوز حدود الحق في الدخول، وجريمة الاعتراض غير المشروع. مما يوفر حماية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونيا ، إلا أننا نري أن هذه الحماية غير كافية للحماية هذا الحق من حقوق الإنسان الجوهرية في عصر تداول البيانات والمعلومات واننا في حاجة إلى تشريع خاص لحماية خصوصية البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً من أي انتهاك أو اعتداء عليها بحيث تكون الحماية شاملة للمراحل المختلفة التي تمر بها صياغة وأنشاء واعداد هذه البيانات الشخصية ثم مدة الاحتفاظ بها، ثم بعد ذلك كيفية التخلص الأمن لهذه البيانات الشخصية التي تم معالجتها إلكترونياً.

(١) – د. جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠١ ، ص ٦٤.

المبحث الثاني. جرائم المعالجة غير المشروعة للبيانات الشخصية الإلكترونية

في واقع الامر لقد أحدثت التطورات التكنولوجية الحديثة والعولمة تحديات جديدة لحماية البيانات الشخصية التي تم معالجتها إلكترونياً، وازداد حجم جمع البيانات الشخصية ومعالجتها زيادة كبيرة، حيث تسمح التكنولوجيا للشركات الخاصة والسلطات العامة باستخدام البيانات الشخصية على نطاق واسع. بل أكثر من ذلك فقد غيرت التكنولوجيا كل من الاقتصاد والحياة الاجتماعية وكذلك القانون، فينبغي معها أن تزيد من التدفق الحر للبيانات الشخصية بين الدول والمؤسسات، مع ضمان مستوى عال من الحماية للبيانات الشخصية، خاصة في مراحل المعالجة للبيانات الشخصية.

لذلك فقد نص المشرع المصري على تعريف المعالجة الإلكترونية للبيانات والمعلومات في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات على أنها "أي عملية إلكترونية أو تقنية تتم كلياً أو جزئياً لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استنباط البيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخرى"(١).

(١) – أنظر المادة الأولى من القانون المصري بشأن مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

أما بالنسبة المعالجة للبيانات الشخصية فيقصد بها "كل عملية أو مجموعة عمليات تجرى على البيانات الشخصية، سواء كانت بوسائل آلية أو غير آليه، مثل التجميع أو التسجيل أو التنظيم أو التخزين أو التكيف أو التغيير، أو استرجعها، أو استخدامها، أو الكشف عنها عن طريف الإرسال أو النشر أو غير ذلك من وسائل الإتاحة أو الموائمة أو الجمع أو الحجب أو المحو أو الأنهاء".

ولذلك فقد نصت مبادئ منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة على مبدأ الحدود لجمع البيانات(١)، "بحيث توجب على الدول أن يكون هناك حدود لجمع البيانات الشخصية، فأي بيانات من هذا القبيل يجب أن يحصل عليها بوسائل مشروعة وعادلة، وحيثما يكون مناسباً، بعلم أو موافقة صاحب البيانات. بالإضافة إلى ذلك أن يلتزم بمبدأ جودة البيانات الشخصية أثناء المعالجة الآلية، أي يجب أن تكون البيانات الشخصية على علاقة وثيقة بالأغراض التي جمعت لتستخدم فيها، ووفق ضرورة هذه الأهداف بحيث يتم الالتزام بشروط مشروعة المعالجة الآلية للبيانات الشخصية وأن تكون هذه البيانات الشخصية دقيقة وكاملة ومحدثة. وكذلك الالتزام بمبدأ تحديد الغرض، فيجب أن تحدد الأغراض التي تجمع البيانات الشخصية لها في موعد لا يتجاوز وقت جمع البيانات(٢)، ويجب أن يقتصر الاستخدام اللاحق على تحقيق هذه الأغراض أو غيرها من الأغراض التي لا تتعارض معها وتحدد أيضا في كل مناسبة يتغير فيها الغرض ما هو الغرض الجديد الذي يجب أن يلتزم به أثناء المعالجة الآلية للبيانات الشخصية".

---

(١) – المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية التي تنظم حماية الخصوصية وتدفق البيانات الشخصية عبر الحدود ، الجزء الثاني ، الأمم المتحدة ، والتي اعتمدت في ٢٣ سبتمبر ١٩٨٠ ، وقد تم تعديلها وتنقيح هذه المبادئ في عام ٢٠١٣.

(٢) – ريموند واكس ، الخصوصية ، مقدمة قصيرة جداً ، ترجمة ياسر حسن ، ومراجعة هاني فتحي سليمان ، الطبعة الأولى ، كلمات عربية للترجمة والنشر ، القاهرة ، ٢٠١٣ ، ص ١١٦ ، ١١٧.

وتأسيسا على ما سبق نري أنه يقصد بالمعالجة غير المشروعة للبيانات الشخصية الإلكترونية هو كل فعل من شأنه أن يخالف الشروط الواجب توافرها لمشروعية المعالجة للبيانات الشخصية. مثل مخالفة الشروط الخاصة بجمع أو حفظ البيانات الشخصية أو معالجة البيانات بطريقة لا تتلاءم مع الهدف من جمعها، أو مخالفة ضوابط معالجة البيانات الشخصية الخاصة مثل البيانات الشخصية المتعلقة بالأصول العرقية والآراء السياسية والحالة الصحية والحياة الجنسية أو البيانات الشخصية المتعلقة بأحكام الإدانة أو الجرائم أو السجل الإجرامي.

كذلك فقد نصت المادة الأولى من الاتفاقية الأوربية لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية إلى أن الغرض منها هو أن يكون في كل دولة أو إقليم طرف في الاتفاقية ولجميع الأفراد، مهما كانت جنسيتهم أو محل إقامتهم، ضمان احترام حقوقهم وحرياتهم الأساسية، خصوصاً حقهم في الخصوصية، فيما يتعلق بالمعالجة الآلية للبيانات الشخصية المتعلقة بهم. ويلاحظ أن المشرع الاوربي يوفر إطارا قانونياً لحماية عملية المعالجة الآلية للبيانات الشخصية فيشترط أن يتم الحصول والجمع للبيانات بطريقة عادلة، وبالتالي الحد من الأنشطة التطفلية، مثل الاعتراض لرسائل البريد الإلكتروني للحصول على المعلومات والبيانات الشخصية بطريقة غير عادلة.

وتطبيقاً على ذلك فقد قضت محكمة جنح باريس في حكمها الصادر في ٢ نوفمبر ٢٠٠٠ في قضية تتخلص وقائعها في "أن طالباً بالمدرسة العليا للفيزياء والكمياء الصناعية بباريس وضع تحت المراقبة الدقيقة من جانب إدارة المدرسة لشكوكها في أنه يقوم بأعمال قرصنة إلكترونية(١)، من خلال استخدام بريده الإلكتروني على نحو يخالف

(١) – F. PARRAIN, Secret des correspondances et courrier électronique, disponible sur site, www.adno-avocats.com, Paris, ٢٠١٢.

الاستخدام المشروع له ، وبعد عملية اعتراض ومتابعة للبريد الإلكتروني للطالب ، لاحظت اللجنة أن ٩٠% من الرسائل كانت خاصة والبعض منها كان ينطوي على تشهير بالمدرسة، نتيجة لذلك رفضت المدرسة إعادة تسجيله في العام التالي. مما دفع بالطالب إلى رفع دعوى مدعياً انتهاك خصوصية وسرية بريده الإلكتروني. إلا أن إدارة المدرسة تمسكت أمام المحكمة بأن سرية المراسلات لا ينطبق على الرسائل الإلكترونية بحجة أن المراسلات غير المشفرة يعهد بها لخوادم وسيطة، وأضافوا دفاعاً عما قاموا به، أنه في ظل انتشار الفيروسات المعلوماتية فإنه يجب أن نمارس رقابة شديدة على البريد الإلكتروني خاصة أنها تسبب أضرار جسيمة. إلا أن المحكمة قضت بالرد على ذلك بالقول بإن إرسال رسالة إلكترونية من شخص لآخر بشكل مراسلة خاصة تخضع لأحكام القانون رقم ٩١ – ٦٤٦ المتعلق بحماية سرية المراسلات التي تتم بواسطة الاتصال عن بعد، وبالتالي تجريم ما قامت به إدارة المدرسة".

وسوف نتناول بالدراسة لجرائم المعالجة غير المشروعة للبيانات الشخصية التي تم معالجتها إلكترونيا، في المطلب الاول بعرض موقف الاتحاد الأوربي من هذا النوع من الجرائم، خاصة بعد صدور اللائحة الأوربية العامة الخاصة بحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦، والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨. ثم بعد ذلك نستعرض صور جرائم المعالجة غير المشروعة للبيانات الشخصية التي تم معالجتها إلكترونية وموقف التشريعات المقارنة منها في المطلب الثاني.

المطلب الأول: موقف الاتحاد الأوربي من المعالجة غير المشروعة للبيانات الشخصية الإلكترونية

مما لا شك فيه أن موقف الاتحاد الأوربي من المعالجة الغير المشروعة للبيانات الشخصية الإلكترونية قد تغيير مع اصداره للائحة العامة الأوربية بشأن حماية البيانات الشخصيةGPDR رقم ٦٧٩ لسنة ٢٠١٦، والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨. لذلك حريا بنا التطرق لعرض هذه اللائحة الهامة في مجال حماية خصوصية البيانات الشخصية الإلكترونية، خاصة المادة الثالثة منها والتي نصت على مبادئ الاتحاد الأوربي التوجيهية بشأن معالجة البيانات الشخصية وذلك وفقا لما يلي:

١- يجب تطبيق هذه المبادئ التوجيهية على معالجة البيانات الشخصية كلياً أو جزئياً بالوسائل الآلية، وعلى المعالجة التي تحدث بدون الوسائل الألية للبيانات الشخصية التي تعد جزءاً من نظام حفظ الملفات أو التي يرجى منها أن تمثل جزءاً من نظام حفظ الملفات.

٢- لا يجب تطبيق هذه المبادئ التوجيهية على معالجة البيانات الشخصية في سياق نشاط يقع خارج نطاق قانون الاتحاد الاوربي ... وعلى أي حالة لعمليات المعالجة المتعلقة بالأمن العام والدفاع وأمن الدولة بما في ذلك المصلحة الاقتصادية للدولة عندما تتعلق عملية المعالجة بأمور أمن الدولة، والأنشطة التي تضطلع بها الدولة في مجالات القانون الجنائي، من قبل الشخص العادي في سياق نشاط شخصي أو منزلي بحت. إلا انه وفقا للتعديل الاخير باللائحة العامة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو

٢٠١٨ أصبحت مجال تطبيقها يمتد لخارج دول الاتحاد الاوربي لنشاط يتم في داخل الاتحاد الأوربي.

بالإضافة إلى ذلك فقد نصت المبادئ التوجيهية للاتحاد الاوربي في المادة ٦ منها على مجموعة من الالتزامات يجب أن تلتزم بها الدول الأعضاء أثناء معالجة الآلية للبيانات الشخصية وهي على النحو التالي([1]) :

أ- تعالج البيانات الشخصية بصورة عادلة وقانونية.

ب- تجمع البيانات الشخصية وفقا لأغراض محددة وواضحة وشرعية ولا تعالج بعد ذلك بطريقة لا تتفق مع تلك الأغراض، ويجوز المعالجة الآلية للبيانات الشخصية لأغراض تاريخية أو إحصائية أو عملية، بشرط إلا تكون متعارضة وأن تقدم الدول الأعضاء الضمانات المناسبة.

ت- أن تكون المعالجة الآلية للبيانات الشخصية كافية وغير زائدة ومرتبطة بالأغراض التي جمعت أو عولجت من أجلها.

ث- أن تكون المعالجة الآلية للبيانات الشخصية دقيقة، وعند الضرورة، وتحدث، ويجب اتخاذ كل الخطوات المنطقية لضمان أن البيانات غير الدقيقة أو غير كاملة، فيما يخص الأغراض التي جمعت وعولجت من أجلها، تسمح بأن تصحح.

ج- أن تحفظ البيانات الشخصية التي تم معالجتها آلياً بطريقة تسمح بالتعرف على صاحب البيانات لوقت لا يزيد عن ضرورة الأغراض التي جمعت البيانات من أجلها أو التي تعالج من أجلها، ويتعين على الدول الأعضاء وضع الضمانات المناسبة

([1]) – المبادئ التوجيهية للبرلمان والمجلس الأوربي ، الاتحاد الأوربي ، الصادرة في ٢٤ أكتوبر ١٩٩٥. والمعدلة بموجب اللائحة العامة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ بشأن حماية الأشخاص الطبيعيين فيما يتعلق بتجهيز البيانات الشخصية وحرية تنقل هذه البيانات والتي تلغي التوجيه الأوربي رقم ٤٦ لسنة ١٩٩٥، والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨.

للبيانات الشخصية المخزنة لفترات أطول للاستخدامات التاريخية أو الإحصائية أو العلمية.

ونستخلص مما سبق أن المشرع الأوربي قد وضع مجموعة من المبادئ لحماية مشروعية عملية الجمع والمعالجة للبيانات الشخصية سوء تمت عملية المعالجة آلياً أو إلكترونيا، والتي يجب أن تلتزم بها الهيئات والمؤسسات العامة والخاصة، وهذه المبادئ ما يلي:

المبدأ الأول. يحظر فيه وفقاً للقانون جمع البيانات الشخصية مالم تجمع لغرض مشروع يرتبط مباشرة بوظيفة أو نشاط مستخدم البيانات التي سوف يستخدم البيانات، على أن يتم ذلك الجمع للبيانات على القدر الكافي والضروري وبلا إفراط وفي ضوء الغرض المحدد. كذلك يجب أن تتم عملية الجمع للبيانات الشخصية من خلال الوسائل المشروعة والعادلة فقط، وهذا يلزم معالج البيانات إبلاغ صاحب البيانات بالغرض الذي سوف تستخدم البيانات من أجلة، وفئات الأشخاص الذين يجوز نقل البيانات لهم، سواء كان تقديم البيانات يتم بطريق إجبارية أو اختيارية لصاحب البيانات، ولصاحب البيانات الشخصية الحق في طلب الوصول إلى بياناته وتصحيحها. أي أنه يجب أن تكون هناك حدود لما يتم جمعة من بيانات شخصية، وأن تكون هناك قيود عليه فيما يتعلق بموافقة الشخص. ولذلك فقد نصت المادة الأولى والثانية من اللائحة العامة الأوربية لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨ على أن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية حق أساسي، منصوص عليه في المادة ٨ الفقرة الأولى من ميثاق الأساسية لحقوق الانسان الأوربي، والمادة ١٦ الفقرة الأولى من معاهدة تيسير الاتحاد الأوربي على أن لكل شخص الحق في حماية البيانات الشخصية المتعلقة به. وينبغي أن تحترم مبادئ

الحقوق والحريات الأساسية للأشخاص الطبيعيين خاصة فيما يتعلق بمعالجة بياناتهم الشخصية، بغض النظر عن جنسيتهم أو إقامتهم.

وتطبيقا على ذلك فقد قضت محكمة العدل الأوربية في القضية الخاصة ببولندا بأن نظم معالجة البيانات الشخصية هي نظم لخدمة الإنسان(١)، يجب عليهم فيها بغض النظر عن جنسية أو إقامة الأشخاص الطبيعيين ، أن يحترموا حقوقهم وحرياتهم الأساسية، ولاسيما الحق في خصوصية البيانات الشخصية التي يتم معالجتها. فالهدف من القوانين الوطنية المتعلقة بمعالجة البيانات الشخصية هو حماية الحقوق والحريات الأساسية، ولاسيما الحق في الخصوصية، المنصوص عليه في المادة ٨ من الاتفاقية الأوربية لحماية البيانات، وكذلك في المبادئ العامة للاتحاد الأوربي، ولهذا السبب لا ينبغي أن يؤدي التعديل لهذه القوانين إلى تقليل الحماية التي يجب أن تتوافر لها، بل العكس يجب ضمان مستوى عالي من الحماية للبيانات الشخصية التي يتم معالجتها. بالإضافة إلى ذلك ينبغي أن تكون الأغراض التي تعالج من أجلها البيانات الشخصية محددة وصريحة ومشروعة، وأن تحدد في وقت جمع البيانات الشخصية. كذلك أن تكون البيانات الشخصية كافية وذات صلة وتقتصر على ما هو ضروري للأغراض التي تم معالجتها. وبالتالي لا ينبغي معالجة البيانات الشخصية إلا إذا تعذر تحقيق الغرض المعقول من المعالجة بوسائل أخرى(٢). فلكي تكون المعالجة مشروعة للبيانات الشخصية ينبغي أن تكون على أساس موافقة على موضوع البيانات المعنية وعلى أساس نص قانوني أو لائحة.

---

(١) – محكمة العدل الأوربية ، قضية ماكسيمليان شكرمز الخاصة بالحقوق الرقمية ايرلندا ، رقم ١٤-٣٦٢ لسنة ٢٠١٤ ، الحكم الصادر في ٦ اكتوبر ٢٠١٥.

(٢) – أنظر المادة ٣٩ من اللائحة العامة الأوربية بشأن حماية البيانات الشخصية رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨.

كما يجب أن تتم المعالجة للبيانات الشخصية وفقا للحد الضروري للغاية والمتناسب مع أغراض ضمان أمن الشبكات والمعلومات، أي مدى قدرة شبكة أو نظام معلوماتي للمقاومة على مستوي معين من الثقة، للأحداث العرضية أو الإجراءات غير المشروعة أو الضارة التي ممكن أن تضر بتوافر البيانات الشخصية المخزنة أو المنقولة وأمنها وسريتها، وأمن الخدمات ذات الصلة التي تقدمها أو يمكن الوصول إليها عن طريق تلك الشبكات والأنظمة. حيث ينبغي إلا يسمح بمعالجة البيانات الشخصية لأغراض أخرى غير تلك التي تم جمع البيانات الشخصية في البداية من أجلها، فيجب أن تكون المعالجة متوافقة مع الأغراض التي جمعت من أجلها البيانات الشخصية في البداية. وفي هذه الحالة، لا يلزم وجود أساس قانوني منفصل عن ذلك الذي يسمح بجمع البيانات الشخصية. أما إذا كانت المعالجة ضرورية لأداء مهمة تنفيذاً للمصلحة العامة أو لممارسة السلطة الرسمية المخولة للمراقب ، يجوز للدول أن تحدد المهام والغايات التي ينبغي النظر فيها لأي معالجات أخرى للبيانات الشخصية وإذا ما كانت متوافقة مع القانون([1]). وبالتالي يستثنى من ذلك المعالجة للبيانات الشخصية لأغراض البحث العلمي أو التاريخ أو الأغراض الإحصائية.

وتطبيقا لذلك فقد قررت شركة جوجل في ديسمبر ٢٠١٧ لتوفير الحماية لمستخدمي برامج الآندرويد، منع التطبيقات من جمع البيانات الشخصية غير الضرورية التي ليست أساسية لعمل التطبيق، كما طالبت أن توضح التطبيقات التي تقوم بحفظ ونشر مثل هذه البيانات الشخصية التي لا تحتاج إلى جمعها للمستخدم كيفية استخدام البيانات. بالإضافة إلى ذلك يجب على المستخدم إعطاء الإذن للمطور أو المعالج لجمع هذه

([1]) – انظر المادة ٥٠ من اللائحة العامة الأوربية لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨.

المعلومات والبيانات الشخصية. كذلك لابد أن يظهر تحذير على سطح الجهاز لتذكر المستخدمين أن التطبيق يحاول جمع البيانات الشخصية دون إذن منه.

أما المبدأ الثاني. من المبادي التوجيهية للاتحاد الأوربي لحماية مشروعية المعالجة الآلية للبيانات الشخصية فإنه يتطلب من معالج أو مستخدم البيانات الشخصية التي تم معالجتها آلياً من أن يلتزم بحفظ هذه البيانات بطريقة دقيقة ومحدثة([1])، وإذا كان في شك في حدوث إخلال بهذا المبدأ يجب عليه أن يتوقف فوراً عن استخدام هذه البيانات الشخصية التي تم معالجتها، بالإضافة إلى ذلك يجب عليه عدم الإبقاء على البيانات الشخصية التي تم معالجتها آلياً لفترة أطول مما هو ضروري للغرض الذي جمعت من أجلة. كما ينبغي أن تكون المعلومات التي يتم معالجتها أو جمعها عن الشخص معلومات صحيحة ودقيقة وحدثة وكاملة.

وتطبيقا على ذلك فقد قضت محكمة العدل الأوربية في قضية وتيلي الخاصة بالحقوق الرقمية في إيرلندا في عام ٢٠١٤([2])، وقضية واتسون ديسيسون في عام

([1]) – مثال على ذلك ، حيث تم تكليف مكتب تقييم التقنية في الولايات المتحدة (OTA) في عام ١٩٨١ الدكتور لوردن ، وهو عالم في مجال الجريمة ، بإجراء دراسة حول قيمة بيانات التاريخ الإجرامي التي تحويها ملفات (FBI– وكالة الشرطة الفيدرالية) وملفات وكالة شرطة ولاية نيويورك ، وقد وجد أن النسبة عالية من البيانات كانت غير كاملة وغير دقيقة ومبهمة ، ويتضمن العديد منها اعتقالات وتقصيات لم تؤد الى إدانة ، أو أنها متعلقة بجنح بسيطة تمت في الماضي القديم ، وأظهرت دراسات آخري أن أصحاب العمل لم يوظفوا في الغالب مثل هؤلاء الأشخاص لسجلاتهم الإجرامية غير الدقيقة ، واعترفت أربع من خمس ولايات أمريكية تم الاتصال معها بواسطة مكتب تقييم التقنية (OTA) أنها لم تتأكد أبدا من دقة البيانات في ملفاتها أو أنها لم تقم باستماع نوعي منتظم .

([2]) – Digital Rights Ireland Ltd *v.* Minister of Communications, Marine and Natural Resources et al. (C–٢٩٣/١٢); Kärntner Landesregierung and others (C–٥٩٤/١٢), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (٨ April ٢٠١٤).

٢٠١٦([1]) ، حيث أوجبت محكمة العدل الأوربية أن تمتثل جميع نظم معالجة والاحتفاظ بالبيانات الشخصية لمبادئ الشرعية والضرورة وفقا لمعيار التناسب، فغالبا ما تكون النظم الوطنية للبيانات الشخصية غير محدثة وتفتقر إلى الوضوح الامر الذي يجعلها مخالفة للمبادئ التوجيهية للاتحاد الاوربي لحماية مشروعية معالجة البيانات الشخصية.

وبالتالي لابد أن تقتصر الفترة التي تخزن فيها البيانات الشخصية على الحد الأدنى من الوقت اللازم. ومن أجل ضمان عدم الاحتفاظ بالبيانات الشخصية لفترة أطول من اللازم ، لابد وأن يضع المراقب للبيانات الشخصية حدوداً زمنية للمحو أو لإجراء استعراض دوري([2]). بالإضافة إلى ذلك اتخاذ الضمانات لتصحيح أو حذف البيانات الشخصية غير الدقيقة إن وجدت، بما في ذلك منع الوصول غير المصرح به إلى البيانات الشخصية أو استخدامها بطريقة غير مشروعة.

المبدأ الثالث. يشترط كي تتم المعالجة الآلية للبيانات الشخصية الحصول على موافقة صاحب البيانات، فبدون موافقة صاحب البيانات، لا يجوز استخدام البيانات الشخصية لأي غرض آخر غير الغرض الذي جمعت لاستخدامها فيه وقت جمعها. لذلك ينبغي الحصول على الموافقة بطريقة ايجابية واضحة وبإشارة حرة ومحددة ومستنيرة لا لبس فيها لاتفاق موضوع البيانات على معالجة البيانات الشخصية المتعلقة به، ومن خلال ايصال مكتوب، ويجوز عن طريق الوسائل الإلكترونية، أو عن الطريق الشفوي. كما

([1]) – Tele٢ Sverige AB *v.* Post– Och telestyrelsen (C–٢٠٣/١٥); Secretary of State for the Home Department *v.* Tom Watson et. al. (C–٦٩٨/١٦), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (٢١ December ٢٠١٦). Privacy International was an intervener in that case.

([2]) – انظر المادة ٣٩ من اللائحة العامة الأوربية بشأن حماية البيانات الشخصية رقم ٦٧٩ لسنة ٢٠١٦والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨.

يمكن أن يتم ذلك عن طريق وضع علامة على مربع عند زيارة موقع على الإنترنت، أو اختيار إعدادات تقنية لخدمات مجتمع المعلومات أو بيان آخر أو سلوك آخر يشير بوضوح في هذا السياق إلى قبول موضوع البيانات للتجهيز المقترح والمعالجة لبياناته الشخصية. ولذلك فإن الصمت أو عدم الرد أو الطريق السلبي لا ينبغي أن تشكل موافقة. وينبغي أن تشمل الموافقة جميع أنشطة التجهيز والمعالجة المنفذة لنفس الغرض أو الأغراض. وعندما يكون للمعالجة أغراض متعددة ، ينبغي منح الموافقة عليها جميعا([1]).

المبدأ الرابع. يلزم كل مستخدم للبيانات الشخصية التي تم معالجتها آلياً باتخاذ إجراءات أمنية مناسبة لحماية البيانات الشخصية، فيجب عليه ضمان أن تتمتع بحماية وافية ضد الوصول أو المعالجة أو المحو أو الاستخدام غير المصرح به أو العرضي من آخرين يفتقرون صلاحية القيام بذلك. ويجوز حماية للمجتمع وللأهداف الهامة ذات المصلحة العامة بوجه عام السماح للمراقب بإجراء مزيد من العمليات على البيانات الشخصي بصرف النظر عن التوافق مع الأغراض المحددة للمعالجة، مع اتخاذ التدابير الضرورية والمتناسبة لحماية هذه البيانات. وينبغي اعتبار أن الأعمال الإجرامية المحتملة أو التهديدات التي قد يتعرض لها الأمن العام من قبل المراقب والمعالج للبيانات الشخصية بالإضافة إلى الأفعال الإجرامية من الآخرين في نفس مستوى التهديدات التي يتعرض لها الأمن العام للسلطة المختصة، فعلى سبيل المثال ينبغي الحظر على المراقب ارسال أي إجراء يتم لمعالجة غير مشروعة للبيانات الشخصية غير متوافقة مع الالتزام القانوني أو المهني أو غير ذلك من الالتزامات المتعلقة بسرية المهنة.

([1]) – المادة ٣٢ من اللائحة العامة الأوربية لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ ، والتي دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨.

وتطبيقا على ذلك فقد قضت المحكمة الأوربية لحقوق الانسان إلى اعتبار كل حالة لا تتوافر فيها إجراءات وقائية تتيح للإنسان حماية حقه في خصوصية البيانات الشخصية انتهاكاً للمادة ٨ من الاتفاقية الأوربية لحقوق الانسان. ففي قضية تورك وسلوفاكيا في عام ٢٠٠٦، اشتكى المدعي من كونه مسجلاً كمتعاون مع الوكالة الامنية الشيوعية التشيكوسلوفاكية السابقة، ومن إصدار تصريح أمني لهذا الغرض ووقف عمله الذي يشكل تحدياً لهذا التسجيل، وقضيت المحكمة أن غياب أي إجراء يمكن للمدعي من خلاله الحصول على حماية حقه في خصوصية البيانات الشخصية ينتهك بذلك المادة ٨ من الاتفاقية الأوربية لحقوق الانسان.

فحتى ولو تضمن القانون هذه الإجراءات لحماية الحق في الخصوصية، إلا أن يعتبر التأخر الشديد في الاستجابة لطلبات الأفراد بالوصول إلى معلوماتهم بياناتهم انتهاكا لان الإجراءات الوقائية أصبحت عائق على تمتع الأفراد بحقهم في خصوصية معلوماتهم وبياناتهم. وتطبيقا لذلك فقد قضت المحكمة الأوربية لحقوق الانسان في قضية هرالامبيي ورومانيا عام ٢٠٠٩ ، أن تأخر الحكومة الرومانية لمدة ست سنوات في السماح لوصول المدعي إلى ملفه الأمني الشخصي الذي تم معالجته في ظل النظام الشيوعي السابق ينتهك حقه بموجب المادة ٨ من الاتفاقية الأوربية لحقوق الانسان(١) ، لما يمثله ذلك من اعتداء على حق الشخص في الوصول إلى معلوماته أو بياناته الشخصية.

المبدأ الخامس. الالتزام بإعلان واضح لسياسة الخصوصية التي يلتزم بها المعالج أو المستخدم للبيانات الشخصية التي يتم معالجتها، وذلك يتعلق بالإعلان المطلوب تقديمه من مستخدم البيانات حيال نوع البيانات الشخصية التي تم معالجتها آلياً والتي يملكها،

(١) – المحكمة الأوربية لحقوق الانسان ، قضية هرالامبيي ، رقم ٠٣ / ٢١٧٣٧ ، رومانيا ، ٢٠٠٩.

وسياساته وممارسته فيما يتعلق بالتعامل مع البيانات الشخصية. من حيث التفاصيل الدقيقة عن البيانات الشخصية التي تم معالجتها آلياً، وفترة الاحتفاظ بها، وكيفية تأمينها، وطرق استخدامها، بالإضافة إلى توضيح الإجراءات التي يجب اتخاذه للوصول إلى هذه البيانات وكيفية طلب تصحيحها.

ومثال على ذلك موضوع التنميط للبيانات الشخصية:

حيث ينبغي أن يكون لصاحب البيانات الشخصية الحق في عدم الخضوع لقرار قد يتضمن تدبيراً أو تقييم الجوانب الشخصية المتعلقة به أو التي تعتمد فقط على المعالجة الآلية وتنتج آثارا قانونية تتعلق به أو تؤثر عليه بصورة مماثلة أو رفضها تلقائياً، مثل تطبيق الائتمان الإلكتروني أو ممارسات التوظيف الإلكتروني دون أي تدخل بشرى. وتشمل هذه المعالجة التنميط الذي يعتبر شكل من أشكال المعالجة الآلية للبيانات الشخصية يتم من خلاله تقييم الجوانب الشخصية المتعلقة بشخص طبيعي، ولاسيما لتحليل أو التنبؤ بالجوانب المتعلقة بأداء موضوع من موضوعات البيانات في العمل، والوضع الاقتصادي والصحة والاهتمامات الشخصية أو المصالح، أو السلوك المتوقع، حيث تنتج آثاراً قانونية تتعلق به أو لها تأثير مماثل على نحو ما. وبالتالي لا يجب السماح بأجراء هذه المعالجات وخاصة التنميط إلا من أذن خاص صراحة بذلك وفقا للنظم والقوانين المعمول بها وتحت اشراف المراقب. ففي جميع الأحوال لا يجوز أن تخضع هذه البيانات الشخصية لهذه المعالجات إلا بعد توفير الضمانات المناسبة والتي تتضمن معالجة لمعلومات محددة، مع السماح لصاحب البيانات بحق التدخل والتعبير عن وجهة نظره، والحصول على تفسير للقرار الذي تم التوصل إليه وكذلك الحق في الطعن فيه مع عدم السماح بإجراء هذا النوع من المعالجات على الأطفال(١).

(١) – انظر المادة ٧١ من اللائحة العامة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ بشأن حماية البيانات الشخصية ، وكذلك المادة ٧٢ منه والتي تنص على اخضاع التنميط للبيانات الشخصية لقواعد اللائحة

وفي جميع الأحوال لا يسمح باتخاذ القرارات الآلية والتنميط استناداً إلى فئات خاصة من البيانات الشخصية إلا في أضيق الظروف المحددة.

وبناءً على ذلك ففي عام ٢٠١٠ قدمت لجنة التجارة الفيدرالية الأمريكية FTC تقريراً يكشف عن أحقية المستهلكين في منع المواقع الإلكترونية من متابعة سلوكهم في استخدام الإنترنت. وبالتالي يجب أن تقيد برامج تصفح الإنترنت بإدراج وظيفة لعدم التتبع بالنص على ذلك في قانون حماية البيانات الشخصية، كما يجب أن يكون التزام على الكيانات التجارية بأن تكشف عن الوضع الحالي للبيانات الشخصية التي قامت بجمعها ومع من قامت بمشاركتها وذلك لحماية حق الشخص في خصوصية بياناته الشخصية وعدم استغلالها على المستوي التجاري بدون أذن منه. لذلك اقترحت المفوضية الأوربية في يناير ٢٠١٢ تعديل لقانون لحماية البيانات الشخصية بحيث يجعل من حق الشخص أن يطلب من مقدمي خدمات الإنترنت بمسح بياناته الشخصية التي يمكن أن تظهر في محركات البحث ويطلق على التشريع Right to Be Forgotten، يخول القانون المقترح السماح للمستخدمين أن يطالبوا شركات مثل توتير وفيسبوك بحذف بياناتهم وكذلك جوجل بأن تمنع من ظهور هذه البيانات في محركات البحث لديهما وهو ما قامت به هذه الشركات بعد ذلك من تعديل سياسة خصوصية البيانات الشخصية وأصبح من حق الشخص المطالبة بمسح جميع بياناته الشخصية الإلكترونية.

المبدأ السادس. لتوجيهات الاتحاد الأوربي بخصوص مشروعية المعالجة الآلية للبيانات الشخصية يتعلق بالالتزام بمبدأ الشفافية أي ما يتعلق بحق صاحب البيانات في الوصول

العامة مع تخويل المجلس الأوربي لحماية البيانات الشخصية الحق في إصدار الإرشادات في هذا السياق.

والاطلاع على البيانات الشخصية الخاصة به. وكذلك الحق في طلب أخذ نسخة من البيانات الشخصية التي يحتفظ بها المعالج أو المستخدم للبيانات، وإذا تبين له أن هذه البيانات غير دقيقة، فيحق له طلب تصحيحها. وفي النهاية يحق للضحايا الانتهاك أو الكشف غير المصرح به لخصوصية البيانات الشخصية التي تم معالجتها آليا الحق في تقديم شكوى عن خرق هذه المبادئ السالف ذكرها إلى المفوض الأوربي لخصوصية للبيانات الشخصية. وفي هذه الحالة يجوز للمفوض الأوربي إصدار إخطار تنفيذي لإجبار مستخدم تلك البيانات على الامتثال للقانون، وحالة عدم الامتثال لهذا الإخطار يعد جريمة معاقب عليها عند الإدانة بالسجن لمدة لا تزيد عن سنتين وبالغرامة المالية، كذلك الالتزام بالحق بالتعويض عن الأضرار المترتبة عن عدم الامتثال ومنها الأضرار العاطفية. كذلك يخول المفوض الأوربي لخصوصية البيانات الحق في الموافقة على قواعد الممارسة من أجل تقديم إرشادات عملية لمستخدمي وأصحاب البيانات الشخصية على حد سواء، وتعتبر هذه الإرشادات وثيقة أساسية في أن مستخدم البيانات الشخصية قد أخفق في اتباع القوانين ودليلاً مقبولاً تتحرك بسببها الدعويين الجنائية والمدنية.

ونستخلص مما سبق أنه لا يجوز إجراء المعالجة للبيانات الشخصية إلا بعد استيفاء جميع متطلبات شرعية المعالجة الأصلية، التي يمكن ذكر أهم أمورها وهي الربط بين تلك الأغراض وأغراض المعالجة الإضافية المزمع القيام بها ، مراعاة السياق الذي جمعت فيه البيانات الشخصية، ولاسيما التوقعات المعقولة لمواضيع البيانات الشخصية استنادا إلى علاقتها مع المراقب للبيانات فيما يتعلق باستخدامها خارج الإطار المسموح به، وطبيعة البيانات الشخصية وعواقب المعالجة المزمع إدخالها على مواضيع البيانات، وجود ضمانات مناسبة في كل عمليات المعالجة الأصلية والمستهدفة.

وتطبيقاً لذلك في قضيتي بيك والأميرة كارولين(١) ، فقد رأت المحكمة الأوربية لحقوق الانسان انهما يخضعان لمظلة المادة ٨ بالميثاق الأوربي المتعلقة بالخصوصية، "حيث تتلخص المشكلة الأساسية للقضية في مدي مشروعية التصوير خلسة في مكان عام، حيث إن ترى المحكمة أن قوانين حماية البيانات ليست موضوعة لتوفير حماية شاملة لخصوصية الفرد، ولكنها تشترط، وعلى نحو روتيني، أنه يجب جمع البيانات الشخصية بوسائل مشروعة وعادلة، ومن ثم يتيح هذا التشريع الأوربي حماية عرضية للخصوصية. حيث جاء في قرار المحكمة الأوربية لحقوق الانسان أن التقاط الصور ونشرها هو قضية تتخذ فيها حماية حقوق الفرد وسمعته أهمية خاصة، حيث إنها لا تتعلق بنشر أفكار، وإنما بنشر صور تحتوي على بيانات شخصية، بل شديدة الخصوصية عن ذلك الشخص، وعلاوة على ذلك، فإن الصور التي نشرت في صحفة الفضائح التقطت في جو من المضايقة وللد في الأشخاص الذين يطاردهم (الباباراتزي) شعوراً بالانتهاك، بل الاضطهاد".

وبناء على ذلك فقد قررت المحكمة أن المعيار الجوهري للموازنة بين حماية الحياة الخاصة وحماية حرية التعبير والاطلاع(٢)، يتمثل في المصلحة العامة من النشر

(١) – حيث تقدمت الأميرة كارولين ، أميرة موناكو ، بشكوي تفيد بأن مصوري المشاهير الذين يعملون لدي عدد من المجلات الألمانية قد التقطوا صوراً لها أثناء انشغالها بمجموعة مختلفة من الأنشطة ، بما في ذلك تناول الطعام في أحد المطاعم ، وركوب الخيل ، والتجديف ، واللعب مع أطفالها ، والتسوق ، والتزلج ، وتقبيل رفيقها ، ولعب التنس ، الجلوس على الشاطئ ، وما إلى ذلك ، وقد حكمت إحدى المحاكم الألمانية لمصلحتها فيما يتعلق بالصور الفوتوغرافية التي على الرغم من أنها أخذت في أماكن عامة ، القطت لها بينما كانت تنشد العزلة. ولكن بالرغم من موافقة المحكمة على أن بعض الصور كانت خاصة بما يكفي لتستحق الحماية ، إلا أنه رفضت المحكمة شكواها فيما يتعلق ببقية الصور ، فحولت الأميرة دعوتها إلى المحكمة الأوربية لحقوق الانسان ، والتي أقرت أن المادة ٨ تنطبق على هذه الحالة ، ولكنها سعت إلى الموازنة بين حماية الحياة الشخصية للأميرة وحماية حرية التعبير التي كفلتها المادة ١٠ من الميثاق الأوربي لحقوق الانسان.

(٢) – ريموند واكس ، الخصوصية ، المرجع السابق ، ص ٩٠ ، ٩١.

للصور. وبالتالي قضت المحكمة بأن صور الاميرة كانت ذات طبيعة خاصة تماما، بالإضافة إلى أنها لم تلتقط بمعرفتها أو رضاها ، بل خلسة في بعض الأحيان، وهكذا لم تقدم هذه الصور أي إسهام لموضوع ذي مصلحة عامة من نشرها، فليس للعامة شأن مشروع في معرفة أماكن وجود الاميرة كارولين ولا الكيفية التي تتصرف بها في حياتها الشخصية، حتي في الأماكن التي لا يمكن وصفها دائما بالمنعزلة، بالإضافة إلى أن المجلات قد حققت مصالح تجارية من وراء نشر تلك الصور والمقالات ، فإن تلك المصالح ، في نظر المحكمة ، يجب أن تخضع لحق المدعية في الحماية الفعالة لحياتها الشخصية ، لما تمثله من انتهاك لخصوصية البيانات الشخصية.

وانطلاقا ما سبق نستطيع القول بإن أي معالجة للبيانات الشخصية يجب أن تلتزم بمبدأ الشفافية بمعني أن يتم جمع البيانات الشخصية أو استخدامها أو معالجتها بأي طريقة أخرى كانت بحيث تكون بعد ذلك سهلة المنال والفهم وأن تستخدم لغة واضحة وصريحة. مع ضمان حق الاشخاص في الحصول على تأكيدات وتواصل شخصي للبيانات المتعلقة به والتي يجري تجهيزها(١). كما ينبغي أن يتم إطلاع الاشخاص على المخاطر والقواعد والضمانات والحقوق فيما يتعلق بمعالجة البيانات الشخصية وكيفية ممارسة حقوقهم فيما يتعلق بهذه المعالجة.

بالإضافة إلى ذلك، ينبغي اعتبار معالجة البيانات الشخصية قانونية عندما يكون من الضروري حماية مصلحة ضرورية لموضوع البيانات أو للشخص الطبيعي(٢)، على سبيل المثال عندما تكون المعالجة ضرورية لأغراض إنسانية، بما في ذلك رصد الأوبئة

(١) – انظر المادة ٣٩ من اللائحة العامة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ بشأن حماية البيانات الشخصية ، والتي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨.
(٢) – انظر المادة ٤٦ من اللائحة العامة الأوربية بشأن حماية البيانات الشخصية رقم ٦٧٩ لسنة ٢٠١٦.

وانتشارها أو في حالات الطوارئ الإنسانية، ولاسيما في حالات الكوارث الطبيعية أو الكوارث التي من صنع الانسان مثل الانفجارات النووية أو البيولوجيا.

المطلب الثاني. موقف التشريعات المقارنة من جرائم المعالجة غير المشروعة للبيانات الشخصية الإلكترونية

في بداية الأمر نص المشرع الفرنسي في قانون حماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨ المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤، على عقوبة السجن مدة لا تزيد على خمس سنوات بالإضافة إلى الغرامة المالية التي لا تزيد مقدارها عن ثلاثمائة ألف يورو لمخالفة الشروط العامة لمشروعة معالجة البيانات الشخصية وكذلك في حالة مخالفة الشروط الخاصة لمشروعية معالجة بعض أنواع البيانات الشخصية. بالإضافة إلى عقوبات تكميلية جوازيه للقاضي مثل أن يأمر بإزالة البيانات الشخصية التي تكون محلاً للجريمة، وللجنة القومية للمعلوماتية والحريات الفرنسية CNIL الحق في مراقبة مدى تحقق هذه الإزالة. أي يعتبر الشخص مرتكب لجريمة المعالجة غير المشروعة للبيانات الشخصية في حالة توافر إحدى هذه الحالات التالية:

١- حالة المعالجة المخالفة للشروط الخاصة بجمع البيانات الشخصية.

٢- حالة المعالجة المخالفة للشروط الخاصة بحفظ البيانات الشخصية.

٣- حالة معالجة البيانات الشخصية بطريقة لا تتلاءم مع الهدف من جمعها.

٤- حالة المخالفة لضوابط معالجة البيانات الشخصية الخاصة المتعلقة بالأصول العرقية والآراء السياسية والحالة الصحية والحياة الجنسية(١).

٥- حالة مخالفة ضوابط معالجة البيانات الشخصية المتعلقة بالجرائم أو الأحكام الإدانة أو الإجراءات الامنية أو التدابير الاحترازية.

---

(١) – Code pénal français, L' arts ٢٢٦ – ٢٢ -٢, ٢٢٦ – ١٨, ٢٢٦ – ١٩, ٢٢٦ – ٢٠, ٢٢٦ – ٢١.

ومن الجدير بالملاحظة أن المشرع الفرنسي لم يكون في بادئ الأمر يعاقب على القيام بمعالجة البيانات الشخصية بطريقة غير مشروعة بعقوبة جنائية أو على القيام بمعالجة البيانات الشخصية دون الحصول على رضاء من تم معالجة بياناته، أو مخالفة شرط أن تكون البيانات ملائمة ودقيقة وكاملة، حيث كان المشرع ينص في المادتين ٤٥ و٤٧ من قانون حماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨ على أنه يكتفي في هذه الأحوال بالجزاء المدني. وقد احالت المواد من ٤١ إلى ٤٤ والمادة ٤٦ من قانون حماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨ إلى قانون العقوبات الفرنسي المواد من ٢٢٦ – ١٦ إلى ٢٢٦ – ١٩ ، حيث قرر المشرع الفرنسي خمس أنواع من الجرائم التي تتعلق بالمعالجة الإلكترونية للبيانات الشخصية، والتي تتمثل في جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص المنصوص عليها في المادة ٢٢٦ – ١٦ من قانون العقوبات والمعدلة بالقانون رقم ٤٩٣ الصادر في ٢٠ يونيه ٢٠١٨، وجريمة التسجيل غير المشروع للبيانات الشخصية المنصوص عليها في المادتين ٢٢٦ – ١٧ و٢٢٦ – ١٩ من قانون العقوبات، وجريمة الاحتفاظ غير المشروع للبيانات الشخصية المنصوص عليها في المادة ٢٢٦ –٢٠ من قانون العقوبات، وجريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية المنصوص عليها في المادة ٢٢٦ – ٢١ من قانون العقوبات، وجريمة الإفشاء غير المشروع للبيانات الشخصية المنصوص عليها في المادة ٢٢٦ –٢٢ من قانون العقوبات الفرنسي.

علاوة على ذلك فان المشرع الفرنسي يخول اللجنة القومية للمعلوماتية والحريات CNIL في اتخاذ التدابير الملائمة لمواجهة مخالفات معالجة البيانات الشخصية. كذلك من حق اللجنة أن تنذر من يقوم بمعالجة البيانات الشخصية بأن يتوقف عن المعالجة غير المشروعة في حالة مخالفته لأي شرط من الشروط العامة لمشروعية معالجة

البيانات أو الشروط الخاصة لمشروعية معالجة بعض أنواع البيانات الشخصية([1]). ويظهر ذلك أهمية دور اللجنة القومية للمعلوماتية والحريات في فرنسا في التطور التشريعي لمواجهة الانتهاكات لخصوصية البيانات الشخصية التي تم معالجتها الكترونياً. أما الان وبعد التعديل للقانون رقم ١٧ لسنة ١٩٧٨ الخاص بحماية البيانات الشخصية بالقانون رقم ٨٠١ لسنة ٢٠٠٤ أصبح يعاقب على هذه الجرائم بعقوبة السجن مدة لا تزيد على خمس سنوات بالإضافة إلى الغرامة المالية التي تبلغ مقدارها ثلاثمائة ألف يورو. كذلك يجوز للقاضي أن يأمر بإزالة البيانات الشخصية التي تكون محلاً للجريمة، وللجنة القومية للمعلوماتية والحريات الفرنسية مراقبة مدى تحقق هذه الإزالة. وسوف نتناول بالشرح لصور المعالجة غير المشروعة للبيانات الشخصية الإلكترونية في التشريعات المقارنة وذلك على النحو التالي.

([1]) – د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، دراسة القانون الفرنسي – القسم الأول ، مجلة الحقوق الكويت ، مجلد ٣٥ ، العدد ٣ ، الكويت ، سبتمبر ٢٠١١ ، ص ٤٣٢ ، ٤٣٣.

الفرع الأول. المعالجة الإلكترونية للبيانات الشخصية بدون ترخيص

يقصد بالمعالجة الإلكترونية للبيانات الشخصية بدون ترخيص بانها كل فعل يتخذ شكل المعالجة الإلكترونية للبيانات من تحليل أو تسجيل أو تعديل أو حفظ أو محو للبيانات أو المعلومات الشخصية، دون مراعاة الإجراءات الأولية للقيام بذلك، ووفقا للشروط المحددة بالقانون، حتى ولو تم ذلك عن طريق الإهمال.

وقد نص المشرع الفرنسي على تجريم المعالجة الإلكترونية للبيانات الشخصية دون الحصول على ترخيص في المادة ٢٢٦ – ١٦ من قانون العقوبات الفرنسي والمعدلة بالقانون رقم ٧٣١ لسنة ٢٠١٦ في المادة ١١٧ منه ، والتي تم تعديلها كذلك بموجب القانون رقم ٤٩٣ الصادر في ٢٠ يونيه ٢٠١٨ على(١) أنه يعاقب كل من يقوم ولو بإهمال بمعالجة إلكترونية للبيانات الشخصية دون مراعاة الإجراءات الأولية للقيام بها ، والشروط المحددة في القانون بالحبس لمدة لا تزيد عن خمس سنوات وبالغرامة المالية والتي تبلغ مقدارها ٣٠٠.٠٠٠ ألف يورو. وفي نفس الوقت، عدم الأخلال بحق اللجنة القومية للمعلوماتية والحريات الفرنسية CNIL في توقيع التدابير الاحترازية المنصوص عليها في المادة ٤٥ من قانون حماية البيانات الشخصية الفرنسي. مثل الالتزام بتصحيح هذا الأخلال خلال مدة ٢٤ ساعة فإذا تم هذا التصحيح، تم أغلق الموضوع. أما في حالة عدم الالتزام بذلك يتم البدء بتدبير التحذير، ثم الإلزام بدفع مصاريف معالجة الدولة لهذا الاهمال في حالات الضرورة وحماية للأمن تتدخل الدول بتصحيح هذه المعالجة. أما التدبير الاخير وهو سحب الترخيص بمعالجة البيانات الشخصية لمدة لا تزيد عن

(١) – Code de droit pénal, modifié par Loi n°٢٠١٦ – ٧٣١ du ٣ Jiu ٢٠١٦ – art. ١١٧., Loi n° ٤٩٣ du ٢٠ Jiu ٢٠١٨ – Art ٧ , ٨ , Légifrance. Gouv.fr.

ثلاثة أشهر أو وقف التصريح بعد رفع الأمر إلى المحكمة المختصة وفقا للإجراءات المستعجلة في هذه الحالة.

ونستخلص مما سبق أن المشرع الفرنسي يتطلب لقيام هذه الجريمة أن يكون السلوك الإجرامي المكون لها يتخذ صورة المعالجة الإلكترونية للبيانات الشخصية دون اتخاذ الإجراءات الأولية وفقا للشروط التي يتطلبها القانون رقم ١٧ لسنة ١٩٧٨ الخاص بحماية البيانات الشخصية المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤. وكذلك عدم الحصول على ترخيص بالمعالجة من اللجنة القومية للمعلوماتية والحريات الفرنسية أو الاهمال في تلك المعالجة الإلكترونية. ويقصد بالمعالجة الإلكترونية هنا هو كل فعل يتخذ شكل المعالجة الإلكترونية للبيانات الشخصية أو تعديل البيانات، أو تسجيلها، أو تحليلها والاستخلاص أو الاستخدام، أو تعديلها، أو تصنيفها ثم حفظها، أو نشرها، الابلاغ، أو محوها وتدميرها، أو كل مجموعة من العلميات من ذات الطبيعة تحمل معالجة لهذه البيانات بقصد الربط بينها للحصول على معلومات شخصية. وعلى سبيل المثال لذلك تعتبر معالجة إلكترونية للبيانات الشخصية دون ترخيص إنشاء موقع على شبكة الإنترنت يقوم بتجميع بعض البيانات الشخصية لمستخدمة وانشاء قواعد بيانات لهم بدون الحصول على موافقتهم على ذلك(١).

أما بالنسبة للركن المعنوي فهذه الجريمة يمكن أن تقع عن طريق الخطأ في صورة الاهمال في المعالجة الإلكترونية للبيانات الشخصية أو في صورة العمد والتي يتطلب القصد الجنائي ، بأن يعلم الجاني بأنه يقوم بالمعالجة الإلكترونية للبيانات الشخصية بدون ترخيص من اللجنة القومية للمعلوماتية والحريات أو بدون مراعاة الإجراءات الأولية

(١) – CA. Paris, ٣٠ octobre ٢٠٠٢, disponible sur site, www.legifrance.gouv.fr.

والشروط المنصوص عليها في القانون(١)، وأن تتجه إرادة الحرة الواعية إلى ارتكاب هذه الأفعال الإجرامية.

ويعتبر الحكم الصادر من محكمة نانتير الفرنسية في ١٦ ديسمبر ١٩٨٥، أول حكم يصدر عن القضاء الفرنسي يعاقب عن جريمة المعالجة الآلية للبيانات الشخصية بدون ترخيص(٢). حيث قضت المحكمة بمعاقبة شخص بالحبس لمدة شهرين مع إيقاف التنفيذ، وغرامة ٢٠.٠٠٠ ألف فرنك، وذلك لقيامه بتسجيل بيانات خاصة دون إجراء إخطار مسبق إلى اللجنة المختصة، بالإضافة إلى قيامه بالاحتفاظ بهذه البيانات بدون الحصول على ترخيص بذلك. كذلك فقد قضت محكمة النقض الفرنسية بأن "جمع البيانات الشخصية، بما يمكن من خلاله التعرف على عناوين البريد الإلكتروني للأشخاص ، يعتبر تجميعا غير مشروع للمعطيات، ولو كانت البرامج المعلوماتية لا تسجل وتخزن تلك العناوين التي تستغل لأرسال البريد المزعج الذي يطلق عليه "Spam"(٣).

أما في الولايات المتحدة الأمريكية فقد كشف إدوارد سنودن في يونيو ٢٠١٣ أن وكالة الامن القومي الأمريكية تقوم بجمع ومعالجة البيانات الشخصية للمواطنين الأمريكيين من خلال سجلات الاتصالات الهاتفية الخاصة بدون الحصول على ترخيص

---

(١) – ا. محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، الجريمة المعلوماتية ، الطبعة الرابعة ، دار الثقافة للنشر والتوزيع ، المملكة الأردنية الهاشمية ، عمان ، ٢٠١١ ، ص ٨٧ – ٨٩.

(٢) – Pierre SARGOS et Michel MASSE, Le droit pénal spécial ne de l'informatique, Travaux de sciences criminelles de Poitiers. Éditions Cujas, Paris, ١٩٨٥, P. ٣٦.

(٣) – أ. عبد المجيد غميجة ، الحماية القضائية للمعطيات الشخصية ، المعهد العالي للقضاء ، المغرب ، بدون تاريخ أو دار نشر ، ص ٧.

بذلك ، بالإضافة إلى قيام الهيئات الفيدرالية الأمريكية بموجب برنامج PRISM بإمكانية الوصول إلى الحواسب الخادمة لكبريات شركات التكنولوجيا بما فيها مايكروسوفت وآبل وجوجل وفيسبوك وياهو وسكايب(١). وبالتالي يشكل ذلك انتهاكا واضح لخصوصية البيانات الشخصية المعالجة إلكترونياً، فلا ينبغي تقوض حرية وحق الأفراد في خصوصية بياناتهم الشخصية من خلال القول بأن يتم ذلك لمواجهة الإرهاب.

أما بالنسبة لموقف المشروع الألماني فقد نص في القسم الرابع من القانون الفيدرالي لحماية البيانات الصادر في ١ سبتمبر ٢٠٠٩ BDSG على اشتراط مشروعية جمع البيانات معالجتها واستخدامها، فقرر في المادة الأولى منه بأن "جمع ومعالجة واستخدام البيانات الشخصية يجب أن يكون مشروعاً وقانوناً، إذا كان مسموح به بموجب هذا القانون أو أي قانون آخر أو إذا قدم صاحب البيانات الموافقة وفقا للقواعد القانونية". وعليه فقد اشترط القسم ٤ (أ) من نفس القانون على "ألا تكون الموافقة على معالجة البيانات الشخصية مؤثرة على موضوع البيانات الشخصية، وأن يخطر صاحب البيانات بالغرض من جمع البيانات معالجتها واستخدامها. أما في حالة إذا كان هناك عواقب لحجب موافقته ، فيجب أن تكون موافقة صاحب البيانات مكتوبة، إلا إذا كانت هناك ظروف تبرر بأن تكون الموافقة في شكل آخر ولكن في جميع الأحوال يجب أن تكون الموافقة صريحه وواضحة"(٢).

---

(١) – David LOWE, Surveillance and international terrorism intelligence exchange : balancing the interests of national security and individual liberty, Terrorism and political violence, August, ٢٠١٤, p. ٤. انظر كذلك أ. نور سليمان ، نهاية الخصوصية : الحريات الشخصية وأمن الدول في عصر البيانات الضخمة ، تحليل المستقبل ، مجلة اتجاهات الأحداث ، المجلد الأول ، العدد ٥ ، سبتمبر ٢٠١٤ ، مركز المستقبل للأبحاث والدراسات المتقدمة ، الامارات العربية المتحدة ، أبوظبي ص ٣.

(٢) – Bundesdatenschutzgesetz BDSG, Zuletzt geandet durch, art. ٣ G.V., ١٤ aout ٢٠٠٩, I, ٢٨١٤, Zweck dieses Gesetzes ist es, den Einzelnen davorzu schutzen, dass er durch den Umgang mit seinen personenbezgenen Daten

أما بالنسبة لموقف المشرع المغربي فقد نص في قانون حماية الاشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر في عام ٢٠٠٩ في المادة ٥٢ على تجريم كل إنجاز ملف معطيات ذات طابع شخصي دون التصريح بذلك أو الحصول على الإذن، المنصوص عليه في المادة ١٢ من نفس القانون، أو مواصلة نشاط معالجة المعطيات ذات الطابع الشخصي رغم سحب وصل التصريح أو الإذن. وقد نص المشرع المغربي على أن يعاقب الشخص في هذه الحالة بالغرامة المالية من ١٠.٠٠٠ درهم إلى ١٠٠.٠٠٠ درهم، بالإضافة إلى الحق في التعويض لكل من تعرضوا للضرر نتيجة هذه الجريمة.

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ٣ من قانون حماية خصوصية البيانات الشخصية على أن "لكل فرد الحق في حماية خصوصية بياناته الشخصية، ولا يجوز معالجة تلك البيانات إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان والممارسات المقبولة، وفقاً لأحكام هذا القانون". بالإضافة إلى ذلك فقد نص في المادة ٤ من نفس القانون على أنه "لا يجوز للمراقب معالجة البيانات الشخصية، إلا بعد الحصول على موافقة الفرد، ما لم تكن المعالجة ضرورية لتحقيق غرض مشروع للمراقب أو الغير الذي ترسل إليه البيانات. ويعاقب كل من يخالف ذلك بالغرامة المالية التي لا تزيد على ١.٠٠٠.٠٠٠مليون ريال".

---

in seinem Personlichkeitsrecht beeintrachtigt. د. وليد سليم النمر ، حماية الخصوصية في الإنترنت ، دار الفكر الجامعي ، الاسكندرية ، ٢٠١٧ ، ص ٤٩١ ، ٤٩٢.

كذلك فقد نص المشرع القطري في المادة ١٦ من نفس القانون على أنه "لا يجوز معالجة البيانات الشخصية ذات الطبيعة الخاصة، إلا بعد الحصول على تصريح بذلك من الإدارة المختصة، وفقاً للإجراءات والضوابط التي يصدر بتحديدها قرار من الوزير. وللوزير، بقرار منه، فرض احتياطات إضافية لغرض حماية البيانات الشخصية ذات الطبيعة الخاصة، ويعاقب كل من يخالف ذلك بالغرامة المالية التي لا تزيد عن ٥.٠٠٠.٠٠٠ مليون ريال".

أما بالنسبة لموقف المشرع المصري فقد نص في الفقرة الأولى من المادة الثانية من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على "أن يلتزم مقدمو الخدمة بما يأتي([1]):

١- حفظ وتخزين النظام المعلوماتي أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوما متصلة، وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي:

أ- البيانات التي تمكن من التعرف على مستخدم الخدمة.

ب- البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة.

ت- البيانات المتعلقة بحركة الاتصال.

ث- البيانات المتعلقة بالأجهزة الطرفية للاتصال.

ج- أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز".

([1]) - يقصد بمقدم الخدمة أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصال ، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات.

ويعاقب كل مقدم خدمة خالف ذلك بالغرامة المالية التي لا تقل عن خمسة ملايين جنية ولا تجاوز عشرة ملايين جنية، وتضاعف عقوبة الغرامة في حالة العود([1])، بالإضافة إلى ذلك للمحكمة أن تقضى بإلغاء الترخيص كعقوبة تكميلية جوازيه لمحكمة الموضوع.

وبالإضافة إلى ذلك فقد نص المشرع المصري في الفقرة الرابعة من نفس القانون على أن "يلتزم مقدمو خدمات تقنية المعلومات ووكلاؤهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غيرهم القيام بذلك. ويعاقب كل مقدم خدمة خالف ذلك بغرامة مالية لا تقل عن عشرين ألف جنية ولا تجاوز مائتي ألف جنية". ونستخلص مما سبق أن موقف المشرع المصري محل انتقاد، حيث أنه لم ينص على تجريم المعالجة غير المشروعية للبيانات والمعلومات الشخصية، ولكن وضع فقد التزامات على مقدمو الخدمة بحفظ وتخزين النظام المعلوماتي أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوما متصلة، وبعدم الحصول على هذه البيانات لغير الغرض المخصص له ولا يسمح للغير بالحصول على هذه البيانات والمعلومات الشخصية.

وبناء على ذلك فقد تغيير موقف المشرع المصري بصدور قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ لتلافي هذه الانتقاد، فقد نص في المادة ٣٦ منه على أن "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات". وقد نص المشرع على تشديد العقوبة لتصبح الحبس مدة لا تقل عن

([1]) – أنظر المادة ٣٣ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ ، الصادر في ١٤ أغسطس ٢٠١٨ ، في الجريدة الرسمية عدد ٣٢ مكرر (ج) ، ص ٢١.

ستة شهور وبغرامة لا تقل عن مائتي ألف جنية ولا تجاوز مليوني جنية، أو بإحدى هاتين العقوبتين، في حالة ما إذا توافرت ما يلي([1]) :

أ- إذا ارتكب ذلك مقابل الحصول على منفعة مادية أو أدبية،

ب-أو إذا تم ارتكاب الجريمة بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر.

الفرع الثاني. الإفشاء غير المشروع للبيانات الشخصية الإلكترونية

يقصد بالإفشاء للبيانات الشخصية بانه كل فعل يقوم به الشخص الذي تلقي بيانات أو معلومات أو قام بأي إجراء من إجراءات المعالجة الآلية لها، من شأنه الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة عن طريق قيامه باطلاع أو بنقل هذه البيانات أو المعلومات الشخصية إلى من لا يحق له العلم بها. سواء وقع هذا الإفشاء للبيانات الشخصية التي تم معالجتها إلكترونياً عن طريق العمد أو عن طريق الإهمال.

وقد جرم المشرع الفرنسي الإفشاء غير المشروع للبيانات الشخصية التي تم معالجتها إلكترونياً في المادة ٢٢٦ – ٢٢ من قانون العقوبات المعدلة بالقانون رقم ٨٠١ لسنة ٢٠٠٤ الخاص بحماية البيانات الشخصية حيث تنص على أنه يعاقب بالحبس لمدة لا تزيد عن خمس سنوات وبالغرامة المالية التي تبلغ مقدارها ٣٠٠.٠٠٠ آلف يورو كل شخص قد استقبل أو تلقى بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الإلكترونية للبيانات الشخصية من شأن إفشائها الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة، وقام بنقلها إلى من لا حق

([1]) – انظر المادة ٣٦ من القانون المصري بشأن حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

له في العلم بها. أما إذا وقع هذا الإفشاء للبيانات الشخصية التي تم معالجتها إلكترونياً بطريق الإهمال تكون العقوبة هي الحبس الذي لا يزيد مدته عن ثلاث سنوات وبالغرامة المالية التي تبلغ مقدارها ١٠٠.٠٠٠ ألف يورو. ويتضح من ذلك أن في كلتا الحالتين قد وضع المشرع الفرنسي قيد على تحريك الدعوى الجنائية، فلا يمكن تحريك الدعوى الجنائية وفقاً للفقرتين السابقتين، إلا بعد تقديم المجني عليه أو ممن يمثله قانونيا، أو من له صفه في ذلك بشكوى.

ونستخلص مما سبق أن المشرع الفرنسي بالتعديل الاخير قد شدد العقوبة من عقوبة الحبس لمدة سنة إلى الحبس لمدة خمس سنوات وبالغرامة المالية التي وصلت إلى ٣٠٠.٠٠ آلف يورو، مما يعكس توجه المشرع الفرنسي في حماية خصوصية البيانات الشخصية المعالجة إلكترونياً من الانتهاك سواء تمت من المعالج لهذه البيانات أو من الغير([1])، وكذلك الحفاظ على الغاية من المعالجة الإلكترونية لهذه البيانات الشخصية، مهما كان شكل أو مجال الذي تنصب عليه هذه المعالجة. ويتضح كذلك أن المشرع الفرنسي قد وضع مجموعة من الشروط الواجب توافرها من أجل تجريم فعل الإفشاء غير المشروع للبيانات الشخصية المعالجة إلكترونياً وهي كالتالي:

١- أن يكون من شأن الإفشاء للبيانات الشخصية المعالجة إلكترونياً الإضرار بالمجني عليه أو بحرمة حياته الخاصة.

٢- أن يتم هذا الإفشاء للبيانات الشخصية المعالجة إلكترونياً بدون رضاء المجني عليه أو من يمثله قانوناً أو من له صفة في ذلك.

٣- أن يكون الإفشاء إلى شخص ليس له حق الاطلاع على هذه البيانات الشخصية المعالجة إلكترونياً، ويجوز استثناءً من ذلك إفشاء البيانات الشخصية للمصلحة

([1]) – د. صفية بشاتن ، الحماية القانونية للحياة الخاصة ، دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، الجزائر ، ٢٠١٢ ، ص ٣٨٤.

العامة، حيث تنص المادة ٢٢٦ – ١٤ من قانون العقوبات الفرنسي على أنه يجوز إفشاء للبيانات الصحية للمصلحة العامة دون رضاء المريض. وذلك دون الإخلال بنص المادة ٢٢٦– ١٣ من قانون العقوبات الفرنسي والتي تنص جريمة إفشاء اسرار المهنة.

وقد أتبع المشرع الأمريكي نفس نهج المشرع الفرنسي وذلك لخطورة الاعتداء على الحق في خصوصية البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً، وخاصة فعل الإفشاء غير المشروع للبيانات الشخصية المعالجة إلكترونياً. وانطلاقا من ذلك فقد استحدث الدستور الأمريكي قانوناً خاصاً عاقب فيه كل من يفشي بأية بيانات أو معلومات شخصية وبأية وسيلة كانت ما لم يكن لديه تصريح بذلك من الشخص صاحب البيانات أو المعلومات الشخصية أو ممن ينوب عنه أو يخوله القانون هذا الحق(١). ويتضح من ذلك أن كلا الاتجاهين القانونين اللاتيني ممثلاً في التشريع الفرنسي الأنجلوسكسوني ممثلاً في التشريع الأمريكي يجرما الإفشاء غير المشروع للبيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً، وذلك لما يمثله هذا السلوك الإجرامي من خطورة إجرامية وانتهاك واضح للحق في خصوصية البيانات والمعلومات الشخصية المعالجة إلكترونياً.

وعلى خلاف الأصل نصت بعض التشريعات على أنه يحق للأجهزة الامنية النفاذ للبيانات الشخصية على سبيل الاستثناء وفي حدود ضيقة ولغرض المصلحة العامة. وعلى سبيل المثال على ذلك ينص القانون الهولندي الخاص بحماية البيانات الشخصية على حق الأجهزة الامنية في الوصول للبيانات الشخصية، ولكن في مقابل ذلك وحفاظاً

(١) – د. طارق أحمد السرور ، الحماية الجنائية لأسرار الأفراد في مواجهة النشر ، دار النهضة العربية ، القاهرة ، ١٩٩١ ، ص ٢٠٥.

على حماية الحق في خصوصية البيانات الشخصية يعطي الشخص صاحب البيانات والمعلومات الشخصية الحق في الوصول لبياناته الشخصية التي تحتفظ بها الأجهزة الامنية، فينص في المادة ٤٧ منه على أن يبلغ الوزير المعني أي شخص بطلبه في أسرع وقت ممكن وفي مدة لا تتجاوز ثلاثة أشهر، سواء أكانت البيانات الشخصية المرتبطة بهذا الشخص معالجة عنه أو بالنيابة عن الجهاز. وتنص المادة ٤٨ على أن يحق للشخص الذي عاين بموجب المادة ٤٧ المعلومات المعالجة التي تعنيه من قبل أو بالنيابة عن جهاز، تقديم بيان خطي بهذا الشأن. يضاف هذا البيان إلى المعلومات ذات الصلة. على أن يتم الرد على هذا الطلب على النحو التالي([1]):

أ. في إطار أي تحقيق تمت معالجة معلومات أو بيانات حول الشخص الذي قام بالطلب إلا إذا:

i. تمت معالجة المعلومات ذات الصلة منذ أكثر من ٥ سنوات.

ii. كذلك، وفيما يتعلق بالشخص الذي يقوم بالطلب، لم تتم معالجة معلومات جديدة فيما يتعلق بالتحقيق الذي عولجت المعلومات ضمنه وكانت هذه المعلومات غير مرتبطة بالتحقيق الحالي.

ب. لم تتعلق معالجة أي معلومات خاصة بالشخص الذي يقوم بالطلب.

ويتضح من ذلك أن المشرع الهولندي يمنح للشخص صاحب البيانات والمعلومات الحق في أولوية الوصول لهذه البيانات والمعلومات بمجرد طلب ذلك من هيئة إشراف تنفيذية، ولكنه يخضع لبعض القيود التي تتعلق بحماية التحقيقات الجارية وحماية مصادر وأساليب الحصول على هذه البيانات والمعلومات ذات الطابع الشخصي بشكل يتناسب مع التهديدات وتخضع دائما للمراجعة المستمرة، مما يشكل تدبير وقائي لاحتمال التعسف أو الفساد من جهة الإدارة.

([1]) – القانون الهولندي المتعلق بالأجهزة الامنية والاستخبارات العامة ، الصادر في عام ٢٠٠٢.

وعليه فقد أقرت الأمم المتحدة بالحق في الوصول للبيانات الشخصية التي تحتفظ بها الأجهزة الامنية([١])، بل اعتبرت ذلك من الممارسات الجيدة التي تحافظ على الحق في الخصوصية، فذهبت إلى أنه يمكن للأفراد الوصول إلى بياناتهم الخاصة التي تحتفظ بها الأجهزة الأمنية. وتتم ممارسة هذا الحق من خلال طلب للهيئة المعنية او من خلال مؤسسة حماية بيانات أو إشراف مستقلة. كما يحق للأفراد تصحيح أي أخطاء في بياناتهم الشخصية. وترد أي استثناءات لهذه القواعد العامة في القانون وتنحصر بشكل صارم بأداء مهام الأجهزة الأمنية وتكون متناسبة معه وضرورية. ويقع على عاتق جهاز الأمن تبرير أي قرار بعدم الكشف عن البيانات والمعلومات ذات الطابع الشخصي لمؤسسة إشراف مستقلة.

أما بالنسبة لموقف المشرع المصري فقد نص في قانون العقوبات المادة ٣٠٩ مكررا (أ) على تجريم القيام بإذاعة أو تسهيل إذاعة أو استعمال ولو في غير علانية تسجيلاً أو مستنداً تم التحصل عليه بإحدى الطرق الموضحة في المادة ٣٠٩ مكررا([٢]) أو كان ذلك بغير رضاء صاحب الشأن ، وقد جعل المشرع المصري هذه جريمة جنحة معاقب عليها بعقوبة الحبس. ويشدد المشرع المصري العقوبة فتصبح السجن مدة لا

([١]) – مجلس حقوق الإنسان التابع للأمم المتحدة ، تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب ، كتيباً خاصة بالممارسات الجيدة للأطر القانونية والمؤسسات والإجراءات التي تضمن احترام حقوق الانسان من قبل وكلات أمن والاستخبارات في الإرهاب بما في ذلك الإشراف ، وثيقة الأمم المتحدة ، رقم A/HRC/١٤/٤٦ ، الصادرة في ١٧ مايو ٢٠١٠ ، الممارسة رقم ٢٦ ، ص ٢٣

([٢]) – تنص المادة ٣٠٩ مكررا من قانون العقوبات المصري على أن يعاقب بالحبس مدة لا تزيد عن سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن ، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه ، التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص. ولا يقتصر التجريم على الشخص القائم بالتقاط الصورة فقط وفقا للنص السابق ولكن التجريم يمتد ليشمل كل من سهل أو أذاع أو شارك في نشر الصورة.

تزيد على خمس سنوات وذلك لكل من هدد بإفشاء أمر من الامور التي تم التحصل عليها بإحدى الطرق المشار اليها لحمل شخص على القيام بعمل أو الامتناع عنه. ويعاقب بالسجن الموظف العام الذي يرتكب أحد الافعال المبينة بهذه المادة اعتمادا على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو اعدامها.

ونستخلص من ذلك أن المشرع المصري قد قصر الحماية الجنائية لصورة وصوت الشخص في المكان الخاص، رغم أن حماية الحق في الخصوصية يمتد في حد ذاتها إلى حماية المعلومات والبيانات الشخصية المعالجة إلكترونياً، الأمر الذي يجعل هذا النص معيب ومنتقد لأنها لا يشمل بالحماية للبيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً. وبالتالي يجب على المشرع المصري التدخل بالتعديل لنص المادة السابقة أضافة فقرة جديدة تنص على تجريم كل من حصل أو نقل أو أطلع أو بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الإلكترونية للبيانات الشخصية من شأن إفشائها الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة، وقام بنقلها إلى من لا حق له في العلم بها. ويعاقب كذلك في حالة ما إذا تم هذا الإفشاء للبيانات الشخصية التي تم معالجتها إلكترونياً بطريق الإهمال. تطبيقا لما ذهب إليه المشرع الفرنسي في تجريم هذا النشاط الإجرامي.

كذلك نص المشرع المصري في المادة ٣١٠ من قانون العقوبات على أن "كل من الأطباء أو الصيادلة أو غيرهم ، مودعا إليه بمقتضي صناعته أو وظيفته سر خصوصي

ائتمن عليه ، فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تتجاوز خمسمائة جنية مصري"([1]).

وتأسيسا على ما سبق نستطيع القول بان المشرع المصري يحمي الحق في الخصوصية لكل سر يتعلق بالشخص من أمور يخشى معرفة الناس بها، أي كل ما يضر إفشاؤه بسمعة أو كرامة الشخص. ولسر يشمل المعلومات والبيانات الشخصية التي تم معالجتها إلكترونيا. وبالتالي يثور التساؤل حول هل تمتد نص المادة السابق ليشمل بالحماية الجنائية للحق في خصوصية البيانات الشخصية المعالجة إلكترونياً من الإفشاء. نجد أن الحماية الجنائية مقصوره وفقا لهذه المادة على ما يتعلق بالسر المهني في مجال المعلومات والبيانات التي يتحصل عليها الشخص بموجب وظيفته، فعلى سبيل المثال قيام العاملين على نظام معلوماتي في هيئة معينة مثل المعالج أو المراقب بجمع معلومات وبيانات شخصية عن الاشخاص فإنهم يعتبرون من أهل الثقة المهنية الاضطرارية بحسب نص القانون أما غيرهم وهم الكثير ممن يمكن أن يصل إليه تلك المعلومات أو البيانات الشخصية ويقوم بإفشائها فلن يسأل جنائياً. وهذا يعني أن نص هذه المادة هو الآخر قاصر عن حماية البيانات الشخصية المعالجة إلكترونياً من الإفشاء([2])، مما يوجب على المشرع المصري التدخل لسد هذه الثغرة على غرار ما فعل المشرع الفرنسي بالنص على تجريم جميع صور الانتهاكات للبيانات الشخصية التي تم معالجتها إلكترونيا.

([1]) – "لا تسرى احكام هذه المادة إلا في الاحوال التي لم يرخص فيها القانون بإفشاء أمور معينه كالمقررة في المواد ٢٠٢ و ٢٠٣ و ٢٠٤ و ٢٠٥ من قانون المرافعات في المواد المدنية والتجارية ".اما فيما يتعلق بأسرار الدفاع عن البلاد فلم يستثني المشرع المصري أي حالة منها وشدد العقاب في حالة إفشاء هذه الاسرار فتصل العقوبة إلى الإعدام كما جاء في نص المادة ٨٠ من قانون العقوبات.

([2]) – د. عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٩٥ ، ص ٦٦ ، ٦٧.

وتأكيدا على ما سبق نجد أن المشرع المصري قد نص في المادة ٧٥ من قانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات على "أن يعاقب بالحبس وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائه ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام بإفشاء أو نشر أو إذاعة أية معلومات حصل عليها بحكم وظيفته أو بسببها عن منشأة عاملة في مجال الاتصالات متى كان من شأن ذلك أن يؤدى إلى قيام منافسة غير مشروعة بين المنشآت العاملة في هذا المجال".

ويتضح من ذلك صحة وجهة الرأي التي سبق وأن أوضحناها في أن المشرع المصري يحمي الحق في خصوصية البيانات والمعلومات الشخصية من الإفشاء أو النشر أو الإذاعة، ولكن قصر هذه الحماية على المعلومات والبيانات التي تم الحصول عليها من الموظف بالجهة القائمة على الاتصالات بحكم وظيفته أو بسببها عن منشأة عاملة في مجال الاتصالات. ويشترط للعقاب عن هذه الفعل أن يؤدي الإفشاء أو النشر أو الإذاعة إلى قيام منافسة غير مشروعة بين المنشآت العاملة في هذا المجال، أما غير ذلك من صور الإفشاء سواء عن طريق الاطلاع أو النقل للبيانات والمعلومات الشخصية التي تتم من غير الشخص المؤتمن عليها لم يجرمها المشرع المصري.

ولكن موقف المشرع المصري قد تغيير بعد صدور قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ حيث نص في الفقرة أولا البند (٢) من المادة الثانية على "أن يلتزم مقدمو الخدمة بالمحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها. ويعاقب كل من يخالف ذلك من مقدمو الخدمة بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسة آلاف جنية ولا تجاوز عن عشرين ألف

جنية، أو بإحدى هاتين العقوبتين، وتتعدد عقوبة الغرامة بتعدد المجني عليهم من مستخدمي الخدمة. كذلك يلزم مقدمو الخدمة وفقا للفقرة الأولى البند (٣) المادة الأولى من نفس القانون بتأمين المعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها".

بالإضافة إلى ذلك فقد نصت المادة ٥ من القانون رقم ١٨ لسنة ٢٠٢٠ الخاص بتنظيم نشاط التمويل الاستهلاكي والذي ينظم عمل شركات البيع بالتقسيط على "أن تلتزم شركات التمويل الاستهلاكي ومديروها ومستشاروها والعاملون بها، بالمحافظة على السرية التامة لعملائها، وعدم إفشاء أي معلومات عنهم أو عن معاملاتهم إلى الغير بدون موافقتهم الكتابية المسبقة وفي حدود هذه الموافقة، وذلك باستثناء الحالات التي يلزم فيها تقديم معلومات محددة وفقاً لما تفرضه القوانين المعمول بها. ويترتب على ارتكاب تلك السلوك الإجرامي أن يعاقب الشخص بعقوبة الحبس والغرامة التي لا تقل عن ٢٠٠ ألف جنية ولا تزيد عن مليون جنيه أو بإحدى هاتين العقوبتين ، وتتعدد الغرامات بتعدد المجني عليهم"([1]).

كذلك فقد نصت المادة ٣٦ من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ على "تجريم أفشاء أو أتاحه او تداول بيانات شخصية معالجة إلكترونيا بأي وسيلة من الوسائل وفي غير الأحوال المصرح بها قانوناً، أو بدون موافقة الشخص المعني بالبيانات بالغرامة المالية التي لا تقل عن مائة ألف جنية ولا تجاوز مليون جنية. وتشدد العقوبة في حالتين لتصبح الحبس مدة لا تقل عن ستة شهور بغرامة لا تقل عن مائتي ألف جنية ولا تجاوز مليوني جنية وذلك على النحو التالي:

أ- إذا ما تم ارتكاب جريمة الإفشاء مقابل الحصول على منفعة مادية أو أدبية.

([1]) – أنظر المادة ٥ و٢٥ من قانون رقم ١٨ لسنة ٢٠٢٠ الخاص بشأن تنظيم نشاط التمويل الاستهلاكي المصري ، الصادر في الجريدة الرسمية العدد ١١ مكرر (ك) في ١٧ مارس ٢٠٢٠، ص٢.

ب–حالة ما إذا تم ارتكاب جريمة الإفشاء بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر".

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ٦ من قانون حماية خصوصية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦ على أن "للفرد، في أي وقت، الوصول إلى بياناته الشخصية وطلب مراجعتها، في مواجهة أي مراقب، وله بوجه خاص الحق فيما يلي .... ٢. إخطاره بأي إفشاء لبياناته الشخصية غير دقيقة عنه. كذلك نص في المادة ١٣ من نفس القانون على أنه يجب على كل من المراقب والمعالج اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية من ... الإفشاء، أو الوصول إليها، أو استخدامها بشكل عارض أو غير مشروع ويجب أن تكون تلك الاحتياطات متناسبة مع طبيعة وأهمية البيانات الشخصية المراد حمايتها. هذا وفي جميع الأحوال يجب على المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات المشار إليها، أو عند حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، وفور علمه بذلك. ويعاقب المعالج في مخالفة ذلك بالغرامة المالية التي لا تزيد عن ٥.٠٠٠.٠٠٠ مليون ريال ما لم ينص القانون على عقوبة أشد"([1]).

كما يجب على المراقب إعلام الفرد والإدارة المختصة([2]) ، بحدوث أي إخلال بالاحتياطات المشار إليها ، إذا كان من شأن ذلك إحداث ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد ، ويعاقب المراقب في حالة مخالفة ذلك بالغرامة المالية التي لا تزيد عن ١.٠٠٠.٠٠٠ مليون ريال ما لم ينص على عقوبة أشد في قانون أخر([3]).

([1]) – انظر المادة ٢٤ من قانون حماية خصوصية البيانات الشخصية القطري رقم ١٣ لسنة ٢٠١٦.
([2]) – أنظر المادة ١٤ من قانون حماية خصوصية البيانات الشخصية القطري.
([3]) – انظر المادة ٢٣ من قانون حماية خصوصية البيانات الشخصية القطري.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

الفرع الثالث. الاحتفاظ غير المشروع للبيانات الشخصية الإلكترونية

في بداية الأمر لابد من توضيح مفهوم الاحتفاظ غير المشروع للبيانات الشخصية المعالجة إلكترونياً حيث يقصد به كل نشاط يؤدي إلى الاحتفاظ بالبيانات أو المعلومات الشخصية التي تم معالجتها آلياً بدون ترخيص من الجهات المختصة، أو الاحتفاظ بها بعد الحصول على ترخيص ولكن بمدة تزيد عن المدة التي سبق طلبها أو التي تضمنها الترخيص، ويستثني من ذلك الاحتفاظ بهذه البيانات الشخصية لأغراض تاريخية أو إحصائية أو علمية وفقا للشروط التي ينص عليها القانون.

وبناء على خطورة هذا الفعل الإجرامي فقد نص المشرع الفرنسي على تجريم الاحتفاظ غير المشروع للبيانات الشخصية الإلكترونية في المادة ٢٢٦ – ٢٠ من قانون العقوبات([1]) والتي تنص على أن "يعاقب بالحبس لمدة لا تزيد عن خمس سنوات وبالغرامة المالية التي لا تزيد مقدارها عن ٣٠٠.٠٠٠ آلف يورو كل من احتفظ بغير موافقة اللجنة القومية للمعلوماتية والحريات CNIL بمعلومات أو بيانات شخصية، لمدة أكثر من المدة التي سبق طلبها أو التي تضمنها الإخطار المسبق. مالم يتم الاحتفاظ بهذه البيانات الشخصية لأغراض تاريخية أو إحصائية أو علمية وفقا للشروط التي ينص عليها القانون".

ويتبين من ذلك أن المشرع الفرنسي يجرم الاحتفاظ بالبيانات الشخصية المعالجة إلكترونياً في حالتين، الحالة الأولى إذا تم الاحتفاظ بالبيانات الشخصية المعالجة

([1]) – المادة ٢٢٦ –٢٠ من قانون العقوبات الفرنسي قد تم تعديلها بموجب القانون رقم ٣٢١ لسنة ٢٠٠٠ بنص المادة ٦ منه ، وكذلك بالقانون رقم ٨٠١ لسنة ٢٠٠٤ المادة ١٤ ، الصادر في ٧ أغسطس ٢٠٠٤ الخاص بتعديل قانون حماية البيانات الشخصية رقم ١٧ لسنة ١٩٧٨.

إلكترونياً بدون ترخيص أي بدون موافقة اللجنة القومية للمعلوماتية والحريات CNIL. والحالة الثانية إذا ما تم الاحتفاظ بالبيانات الشخصية المعالجة إلكترونياً من الشخص المرخص له الاحتفاظ بها ولكن بمدة تزيد عن المدة التي سبق طلبها أو التي تضمنها الإخطار المسبق للجنة القومية للمعلوماتية والحريات. ويستثني من ذلك الحالات التالية:

١- الاحتفاظ بالبيانات الشخصية المعالجة إلكترونياً لأغراض تاريخية.

٢- الاحتفاظ بالبيانات الشخصية المعالجة إلكترونياً لأغراض علمية.

٣- الاحتفاظ بالبيانات الشخصية المعالجة إلكترونياً لأغراض إحصائية.

وبناء على ذلك فقد قصر المشرع الفرنسي الاحتفاظ بالبيانات الشخصية الخاصة بالجرائم أو الأحكام القضائية على الجهات القضائية والعامة، بالإضافة إلى ذلك فقد تم تأسيس بنك للمعلومات والبيانات المتعلقة بالجرائم المرتكبة من قبل الأفراد والعقوبات المطبقة عليهم، وبناء على هذه البيانات والمعلومات يعطى أصحابها إفادات عن واقع حالهم ، وبعد مرور مدة معينة يحددها القانون يتم محو أثرها من الملفات، ويعطي أصحابها شهادات خالية من ذكر هذه العقوبات أو الجرائم، وهو ما يطلق عليه بحق النسيان([1]). حيث بموجب هذا الحق يمكن للشخص أن يحصل على شهادات لا يظهر فيها أثر الأحكام التي مرت عليها المدد التي ينص عليها القانون.

([1]) – د. نعيم مغبغب ، مخاطر المعلوماتية والإنترنت ، المخاطر على الحياة الخاصة وحمايتها ، دراسة مقارنة ، بدون دار نشر ، بيروت ، ١٩٩٨ ، ص ١٩٣.، وكذلك د. علاء الدين منصور المغايرة ، الأوجه الحديثة للجرائم المعلوماتية ، دراسة مقارنة ، رسالة ماجستير ، كلية الحقوق ، جامعة الحكمة ، بيروت ، ٢٠٠٠ ، ص ٦٢.

وعليه فقد نص التقرير الصادر عن مجلس حقوق الانسان التابع للأمم المتحدة الصادر في عام ٢٠١٠ على أن تحدد القوانين أنواع البيانات الشخصية التي قد تطبق على استخدام والاحتفاظ وحذف والكشف عن هذه البيانات أو المعلومات الشخصية. واستثناء من ذلك يسمح للأجهزة الحكومية المختصة بالاحتفاظ بالبيانات الشخصية الضرورية لغايات الاضطلاع وحفظ الأمن (١). ونستخلص من ذلك أن لمستخدم للإنترنت الحق في طلب عدم الاحتفاظ بالبيانات الشخصية المعالجة إلكترونياً أو ما يطلق عليه الحق في المسح الرقمي بحيث يكون للمستخدم للإنترنت الحق في أن يكون الحفظ الإلكتروني لبياناته الشخصية حفظاً مؤقتاً(٢)، أي أن المهلة الزمنية المؤقتة قيد على حفظ البيانات ذات الطابع الشخصي على مواقع البحث الإلكترونية. وهذا الحق يتضمن ما يلي:

أولاً. حق طلب تعديل بياناته الشخصية أو إزالتها حال ما شابها نقص أو غموض أو قدم، والتحقق من شمول هذه العملية لجميع البيانات المخزنة في محركات البحث على الانترنت على سبيل مثال لذلك محرك البحث الخاص بجوجل. وفي نفس الوقت له هذا الحق عندما يقوم بوقف حسابه الإلكتروني.

ثانيا. حق المستخدم للإنترنت في الاعتراض على معالجة بياناته الشخصية، متي كان ذلك مبرراً، كما يكون له الحق حتى ولو بدون مبرر، وذلك وفقا لحقه في خصوصية بياناته الشخصية التي تم معالجتها إلكترونياً.

---

(١) – تقرير المقرر الخاص بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب على هذه الحاجة ، في تقريره لمجلس حقوق الإنسان التابع للأمم المتحدة ، وثيقة الأمم المتحدة ، وثيقة الأمم المتحدة HRC /١٤/ ٤٦/ A ، الصادر في ١٧ مايو ٢٠١٠ ، ص ٢١.

(٢) – M-P. FENOLL – TROUSSEAU et G. HAAS, Jurisclasseur communication fascicule ٤٧٣٥ protection des données à caractère personnel – vie privée et communication électronique, Paris, ٢٠٠٥, P.٣٧.

وتأسيسا على ما سبق فقد التزمت فرنسا بالتوجيه الأوربي بشأن الاحتفاظ بالبيانات الشخصية، وطلبت من مقدمي خدمات الاتصالات الاحتفاظ ببيانات حركة المرور بين مواقع الإلكترونية لمدة عام واحد. ثم قام المشرع الفرنسي بتنفيذ التوجيه الأوربي رقم ١٣٦ لسنة ٢٠٠٩ بشأن ملفات تعريف الارتباط، والذي تم اعتماده في ٢٤ اغسطس ٢٠١١ مما استوجب إخبار المستخدمين للإنترنت عن تثبت واستخدام ملفات تعريف الارتباط، ويتم ذلك بموجب القواعد قبل تثبت ملفات تعريف الارتباط لأول مرة. وبالرغم من هذا النص، تنص القواعد الفرنسية على أنه إذا تم ضبط المتصفحات بما يجعلها تقوم بتثبيت ملفات تعريف الارتباط، فإن الوضع الافتراضي في معظم أجهزة الحاسب الآلي هو أنه ليس على المستخدمين تقديم موافقة صريحة. ويتضح من ذلك أن هذا النص منتقد لأنه بمثابة حل ينحرف عن حماية المصالح الخاصة الشخصية للفرد من الانتهاك([1])، فبدلا من أن ينص على حماية خصوصية هذه البيانات الشخصية المعالجة إلكترونياً نص على خلاف ذلك.

كذلك فقد نص المشرع الفرنسي في المادة ٦ من قانون حماية البيانات الشخصية المعدل بالقانون رقم ٤١ لسنة ٢٠١٦ الصادر في ٢٦ يناير ٢٠١٦، في المادة ١٩٣ الفقرة الخامسة منه على أن تحفظ البيانات الشخصية في شكل يسمح بتحديد الأشخاص المعنيين، لفترة لا تتجاوز الفترة اللازمة للأغراض التي يتم جمعها ومعالجتها. ومعني ذلك أنه لا يجوز جمع أو تخزين البيانات والمعلومات الشخصية إلا لمدة مؤقته ومحددة تتناسب مع الغرض المشروع من جمع وتخزين ومعالجة هذه البيانات الشخصية. ويتم تحديد ماذا كانت المدة المحددة متناسبة مع الغرض المشروع للجمع أو التخزين وفقا

([1]) – انظر قضية Ponzetti de Balbin ، محكمة العدل العليا CS الفرنسية ، ١١ ديسمبر ١٩٨٤ ، الفقرة ٨.

لمعيار موضوعي(١) وهو المدة المعقولة التي تتناسب مع الغرض من معالجة هذه البيانات الشخصية. وانطلاقا مما سبق فقد أوصت الهيئة الأوربية الاستشارية G٢٩ بأن على محركات البحث الإلكترونية أن تزيل البيانات ذات الطابع الشخصي التي سجلت عليها في أقرب وقت ممكن، أو على الأكثر في مدة لا تتجاوز ستة أشهر من تاريخ هذا التسجيل للبيانات الشخصية.

وتطبيقا على ذلك يجب على موقع التواصل الاجتماعي مثل فيسبوك أو توتير أو انستجرام أن تلتزم بإزالة البيانات الشخصية للمستخدم خلال ٦ شهور على الأكثر من تاريخ انتهاء علاقة المستخدم بالموقع ، وذلك في ضوء توصية الهيئة الاستشارية الأوربية G٢٩، والتي تلزم المواقع الإلكترونية بأن تقوم بإزالة بيانات المستخدم خلال فترة لا تتجاوز ستة شهور من تاريخ وقف تفعيل الموقع أو الحساب الإلكتروني للشخص المستخدم(٢). وذلك على عكس المشرع الأمريكي الذي لم ينص على مدة معينة يجب على الموقع الإلكترونية إزالة البيانات ذات الطابع الشخصي التي كانت محتفظة بها، وبالتالي أصبح الأمر متروك لكل شركة على حدة في اتخاذ ما تراه مناسب.

وتطبيقا على ذلك فقد قضت المحكمة الأوربية لحقوق الانسان في ١٣ مايو ٢٠١٤ بحق الانسان في أن ينسى، وذلك لصالح مواطن إسباني في مواجهة شركة جوجل، وألزمت الشركة بإزالة رابط قديم يظهر في نتائج البحث على محرك البحث لشركة جوجل

---

(١) – C. THIERACHE et Matthieu BERGUIG, L'oubli numérique est – il de droit face à une mémoire numérique illimitée ? Rapport, ٢٥ mai ٢٠١٠, Revue Lamy droit de l'immatériel, juillet ٢٠١٠, N° ٦٢, PP. ٣٤, ٣٥.

(٢) – Marine DE MONTECLER, Le droit @ l'heure des réseaux sociaux, Mémoire, HEC, Université Paris I– Panthéon–Sorbonne Paris, ٢٠١١, P. ٣٨.

ويتعلق بخبر إشهار إفلاس المدعي(١). ويتضح من ذلك أن المحكمة الأوربية تحمي الحق في الخصوصية البيانات الشخصية المعالجة إلكترونياً من خلال التأكيد على حق الشخص في محو بياناته الشخصية التي تم معالجتها إلكترونياً.

أما بالنسبة لموقف المشرع الانجليزي فإنه في الطريق لإقرار مشروع قانون مقدم في عام ٢٠١٨ يمكن المواطنين من طلب بياناتهم الشخصية أو معلوماتهم التي نشروها في السابق، ليتم حذفها. وتشكل هذه المقترحات جزءاً من مراجعة لقوانين حماية البيانات في المملكة المتحدة التي تمت صياغتها من قبل. ويشمل المقترحات المدرجة في مشروع القانون مجموعة تسهيلات، من بينها أنها تسهل على الأشخاص سحب الموافقة على استخدام بياناتهم الشخصية أو حذفها، وتتطلب من الشركات الحصول على موافقة صريحة عند معالجة بيانات أو معلومات شخصية حساسة.

وفي ألمانيا قام ما يزيد عن ٣٤.٠٠٠ مواطن برفع دعوى عدم دستورية جماعية ضد قانون الاحتفاظ بالبيانات للشخصية الصادر في عام ٢٠٠٧ أمام المحكمة الدستورية الألمانية(٢)، وقد أصدر المحكمة الدستورية أمراً مبدئياً ضد قانون الاحتفاظ بالبيانات الشخصية في عام ٢٠٠٨ ، ثم صدر القرار النهائي بعدم دستورية قانون الاحتفاظ بالبيانات الشخصية في عام ٢٠١٠، وذلك حماية للحق في خصوصية البيانات الشخصية المتعلق بالهوية، بالإضافة إلى أن قانون الاحتفاظ بالبيانات الشخصية

(١) – Case C – ١٣١/ ١٢, Google Spain SL v. Agencia Espanola de proteccion de Datos, ١٣ May, ٢٠١٤., www.curia.europa.eu.

(٢) – Initiative Vorratsdatenspeicherung, Stoppt die Vorratsdatenspeicherung, ١٣ Nov ٢٠١١.
www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html.

الألماني كان على خلاف ما تنص عليه نصوص التوجيه الأوربي الخاص بالاحتفاظ بالبيانات الشخصية.

أما بالنسبة لموقف المشرع المصري من جريمة الاحتفاظ غير المشروع للبيانات الشخصية المعالجة إلكترونياً، في البداية جرم المشرع الاعتداء على سرية المعلومات والبيانات في المجال الصناعي والتجاري بالنص في المادة ٦١ من القانون رقم ٨٢ لسنة ٢٠٠٢ بشأن حماية الملكية الفكرية على أنه "... يعاقب كل من يقوم بوسيلة غير مشروعة بالكشف عن المعلومات المحمية طبقاً لأحكام هذا القانون أو حيازتها أو باستخدامها مع علمه بسريتها وبأنها متحصلة عن تلك الوسيلة ...". ونستخلص من ذلك أن المشرع المصري يحمي المعلومات والبيانات الشخصية الغير مفصح عنها عن طريق الاحتفاظ بها أو استخدامها بطريقة غير مشروعة ولكن بشروط وهي كالتالي([1]):

١- أن تتصف هذه البيانات والمعلومات بالسرية سواء كانت في مجموعها أو في تكوينها الذي يضم مفرداتها الغير معروفة أو غير متداولة بشكل عام لدى المشتغلين بالفن الصناعي الذي تقع المعلومات والبيانات في نطاقه.

٢- أن تستمد هذه البيانات والمعلومات محل الحماية قيمتها التجارية من كونها سرية وأن يتم الحصول عليها بطريقة غير مشروعة.

٣- أن ما يتم اتخاذه من إجراءات يأتي للحفاظ على سرية المعلومات والبيانات محل الحماية من الاحتفاظ بها أو استخدامها بطريقة غير مشروعة.

([1]) – د. محمد حسين منصور ، المسئولية الإلكترونية ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠٠٣، ص ٣٧٤.

كذلك يتبين مما سبق أن المشرع المصري قد حاول أن يحمي الحق في خصوصية البيانات والمعلومات التي تم معالجتها إلكترونياً التي تتسم بالسرية والخصوصية ولكن في مجال محدد يتعلق بالمعلومات والبيانات التي تم معالجتها إلكترونيا في نطاق المحافظة على خصوصية وسرية التجارة الإلكترونية([1]). وليس على نحو شامل وافي لحماية الحق في خصوصية البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً في حد ذاته وأي كان نوعها تجارية أو اجتماعية أو مدنية أو مالية.

إلا أن موقف المشرع المصري قد تغيير بعض صدور قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ حيث نص في المادة الثانية الفقرة أولا البند (١) على أن "يلتزم مقدمو الخدمة بحفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوماً متصلة". أما في الفقرة ثالثا فنص على أن "مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي ووفقاً لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون". أما في الفقرة رابعاً من نفس المادة نص المشرع المصري على أن "يلتزم مقدمو خدمات تقنية المعلومات ووكلاؤهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غيرهم القيام بذلك". ونستخلص مما سبق أن المشرع المصري قد ألزم مقدمو الخدمة أن يحتفظوا بالبيانات والمعلومات الشخصية لمدة لا تقل عن مائة وثمانين يوماً متصلة، كما ألزمهم بأن يوفروا هذه المعلومات والبيانات حال طلب جهات الأمن القومي، كما أباح المشرع المصري لمقدمو الخدمة الحق في الحصول على بيانات ومعلومات المستخدمين دون غيرها. ونري مما سبق أن المشرع المصري قد غلب

([1]) – د. هدى قشقوش ، الحماية الجنائية للتجارة عبر الإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ ، ص ٣٦ وما بعدها.

المصلحة العامة على المصلحة الخاصة في حماية البيانات والمعلومات الشخصية وهذا وأن كان يفهم لتحقق الأمن العام والاستقرار بالنسبة للدولة، أما بخصوص مقدمي الخدمة فيجب على المشرع وضع ضوابط أكثر وضوحاً لحماية خصوصية البيانات والمعلومات الشخصية من أن يتم الاحتفاظ بها لمدة تزيد عن الغرض الأساسي من جمعها أو معالجتها.

وانطلاقا مما سبق فقد نص المشرع المصري في قانون حماية البيانات الشخصية الجديد رقم ١٥١ لسنة ٢٠٢٠ في المادة ٤١ منه على أن "كل حائز أو متحكم أو معالجة خزن أو نقل أو حفظ بيانات شخصية حساسة بدون موافقة الشخص المعني بالبيانات أو في غير الأحوال المصرح بها قانوناً، بعقوبة الحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنية ولا تجاوز خمسة ملايين جنية ، أو بإحدى هاتين العقوبتين"([1]).

أما بالنسبة لموقف المشرع القطري فقد نص في المادة ١٠ من قانون حماية خصوصية البيانات الشخصية رقم١٣ لسنة ٢٠١٦ على أن "يلتزم المراقب بالا يحتفظ بالبيانات الشخصية التي يجمعها لمدة تزيد عن المدة الضرورية لتحقيق تلك الأغراض. يعاقب في حالة مخالفة ذلك بالغرامة المالية التي لا تزيد عن ١.٠٠٠.٠٠٠ مليون ريال، ما لم ينص على عقوبة أشد في قانون آخر".

أما بالنسبة لموقف المشرع المغربي فقد نص في المادة ٥٥ من قانون حماية معطيات الاشخاص الذاتيين الصادر في عام ٢٠٠٩ على أن "يعاقب بالحبس من ٣ أشهر إلى سنة وبغرامة مالية من ٢٠.٠٠٠ درهم إلى ٢٠٠.٠٠٠ درهم أو بإحدى هاتين العقوبتين فقط في الحالات التالية:

([1]) – أنظر المادة ٤١ من القانون المصري بشأن حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

١-كل من أحتفظ بمعطيات ذات طابع شخصي لمدة تزيد عن المدة المنصوص عليها في النصوص التشريعية الجاري بها العمل ، أو المنصوص عليها في التصريح أو الإذن.

٢-كل من احتفظ بالمعطيات المذكورة خرقا لأحكام الفقرة (هـ) من المادة ٣ من هذا القانون.

٣-كل من قام لأغراض أخرى غير تاريخية أو إحصائية أو علمية، بمعالجة معطيات ذات طابع شخصي تم الاحتفاظ بها بعد المدة المنصوص عليها في الفقرة الأولى أعلاه".

ويثور هنا تساؤل حول هل تمتد الحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً بعد الوفاة بالنسبة للبيانات الشخصية على البريد الإلكتروني ومواقع التواصل الاجتماعي مثل الفيسبوك والتوتير؟ فقد اختلف الفقه في الاجابة على هذا التساؤل وهذا ما سوف نستعرضه على النحو التالي:

الاتجاه الأول. يذهب هذا الاتجاه إلى رفض امتداد الحماية الجنائية لخصوصية البيانات الشخصية على مواقع التواصل الاجتماعي والبريد الإلكتروني بعد الوفاة، ويؤيد هذا الاتجاه أغلب الفقه الفرنسي استنادا إلى قاعدة أن الحق في حرمة الحياة الخاصة لا يثبت إلا للأحياء(١)، وباعتبار أن الحق في الخصوصية من الحقوق اللصيقة بالإنسان والتي لا تمتد إلى ما بعد الوفاة عكس الحقوق المالية فهي تمتد إلى ما بعد الوفاة. حيث تنقضي هذه الحقوق بوفاة الشخص، نظراً لأنها لصيقة بشخص صاحبها، ومن ثم يكون

(١) – Angela Vivanco MARTINEZ, Les libertés de opinion y de information, éd., Andres Bello, Paris, ١٩٩٢, p. ٢١٩.

من المستحيل انتقالها إلى الورثة. ويستند هذا الاتجاه إلى قاعدة أن الحق في حماية الحياة الخاصة شأنه في ذلك سائر الحقوق غير المالية، لا ينتقل إلى الورثة بسبب الوفاة على أساس أن الوظيفة الأساسية لهذا الحق تكمن في حماية الشخصية وهو ما لا يكون له محل إلا في حال حياة صاحبها(١). وهذا التوجه يرجع إلى حكم محكمة النقض الفرنسية الصادر في ٤ ديسمبر ١٩٩٩ في قضية الرئيس ميتران والتي أطلق عليها السر الكبير، حيث قام الطبيب المعالج بنشر كتاب يتضمن البيانات الشخصية الصحية للرئيس الفرنسي الاسبق ميتران، وقد قضت المحكمة بأن حرمة الحياة الخاصة من الحقوق الملازمة للشخصية والتي تنتهي بالوفاة.

وبناء على ذلك الاتجاه فإن شركات البريد الإلكتروني تذهب إلى التحفظ على أسرار الرسائل الإلكترونية في حالة وفاة المستخدم ، وتستند في ذلك إلى أن البريد الإلكتروني وسيلة من وسائل التواصل وتبادل الآراء والأسرار بين طرفين ينبغي عدم الخلط بين أسرارهما ، وطالما أن أحد الطرفين لا يزال حيا ، فإن الإفصاح عن محتويات البريد الإلكتروني لأحدهما يعد اعتداء على الحق في الخصوصية للطرف الآخر(٢)، وهذا يعد مخالفة لبنود سياسة الخصوصية للشركة المزودة لخدمة البريد الإلكتروني. ويتضح من ذلك أن شركات البريد الإلكتروني لم تذهب إلى امتداد الحماية الجنائية للبيانات الشخصية على البريد الإلكتروني بعد الوفاة لحماية الحق في الخصوصية ولكن لحماية الطرف الآخر الذي مازال حياً، وبالتالي يتمتع بالحماية الجنائية للحق في خصوصية البيانات الشخصية المعالجة إلكترونياً.

---

(١) – M. CAHEN, Déxès : les E-mails sont des données personnelles, Paris, ٢٠١٣, p. ٢., www.clic-droit.com.

(٢) – د. محمد عيسى ، الميراث الإلكتروني ، مقال منشور على جريدة الأهرام المصرية ، بتاريخ ١٥ مارس ٢٠١٣.

الاتجاه الثاني. وهو الاتجاه الموافق على امتداد الحماية الجنائية لخصوصية البيانات الشخصية على مواقع التواصل الاجتماعي والبريد الإلكتروني بعد الوفاة، ويتزعم هذا الاتجاه القضاء الأمريكي وبعض موردي منافذ الدخول لخدمة البريد الإلكتروني في الولايات المتحدة الأمريكية، حيث يذهب هذا الاتجاه إلى القول بأن البريد الإلكتروني يكون ملكاً للمستخدم سواء أكان شخصاً طبيعياً أو معنوياً، وبالتالي ففي حالة وفاة مالك البريد الإلكتروني أو موقع التواصل الاجتماعي تمتد الحماية الجنائية لخصوصية البيانات الشخصية الإلكترونية ويصبح صاحب الحق في ذلك الورثة.

وتطبيقا على ذلك قضية الجندي الأمريكي جستين السوورث الذي توفي في العراق في ١٣ نوفمبر ٢٠٠٤، حيث أمضي في العراق مدة شهرين فقط، وكانت الوسيلة الوحيدة للتواصل بينه وبين عائلته وأصدقائه في الولايات المتحدة الأمريكية هي بريده الإلكتروني، حيث كان يقوم بإرسال كافة صورة ومذكراته وأخباره عن الايام التي امضاها في العراق باستخدام البريد الإلكتروني. وبعد هذا الحادث طلب والد جستين من شركة ياهو أن يسلموه محتوى صندوق البريد الإلكتروني الخاص بابنه، استنادا على اتفق مع ابنه قبل موته على انشاء سجل تذكاري يدون فيه مذكرات ابنه، وأن إرادة ابنه كانت متجهة إلى نشر ما يتضمنه بريده الإلكتروني من رسائل، وإلى السماح لوالده وعائلته بالولوج إلى بريده الإلكتروني والاطلاع عليه. غير أن شركة ياهو قد رفضت طلبه بحجة أن ذلك يمثل اعتداء على حرمة الحياة الخاصة للمتوفي وللأشخاص الذين كان يراسلهم. وأمام ذلك الرفض لجأ الاب إلى القضاء ، الذي قضى بإن العقد المبرم بين جستين وشركة ياهو يلزم هذه الاخيرة بالمحافظة على خصوصية البيانات الشخصية المعالجة

إلكترونياً حتي لو بعد وفاة المستخدم(١)، وبالتالي امتداد الحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً إلى ما بعد الوفاة.

ونحن نؤيد الاتجاه الثاني الذي يري أن الحماية الجنائية للحق في خصوصية البيانات الشخصية على مواقع التواصل الاجتماعي والبريد الإلكتروني تمتد حتى بعد وفاة الشخص المستخدم للبريد الإلكتروني أو لمواقع التواصل الاجتماعي، وذلك لأن المشرع يحمي الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً وهو حي فمن باب أولى أن تظل هذه الحماية الجنائية سارية حتى ولو بعد الوفاة. وأن كنا نرى أنه يجب النص في قانون خاص على قواعد تنظيم ذلك من خلال توضيح كيفية التعامل مع حساب البريد الإلكتروني أو مواقع التواصل الاجتماعي في حالة وفاة المستخدم أو إصابته بمرض أو عارض يفقده أهليته للإدراك والتمييز في ضوء احترام الحق في خصوصية بياناته الشخصية.

---

(١) – *V.* Ph. CROUZILLACQ, Les E– mails peuvent reposer en pais, Paris, ٢٠١٣., www.٠١net.com. انظر كذلك: د. عبد الناصر زياد هياجنه ، الميراث الرقمي : المفهوم والتحديات القانونية ، المجلة الدولية للقانون ، كلية القانون ، جامعة قطر ، ٢٠١٦ ، ص ٦.

الفرع الرابع. جريمة التسجيل غير المشروع للبيانات الشخصية الإلكترونية

في البداية نستعرض موقف المشرع الفرنسي الذي نص على تجريم التسجيل غير المشروع للبيانات الشخصية المعالجة إلكترونياً، في المواد ٢٢٦ – ١٦، ٢٢٦ – ١٨، ٢٢٦ – ١٩، من قانون العقوبات الفرنسي على أن يعاقب بالحبس مدة لا تزيد عن خمس سنوات وبالغرامة المالية التي لا تزيد مقدارها عن ٣٠٠.٠٠٠ آلف يورو كل من يقوم بأحدي الأفعال التالية:

١- إجراء المعالجة للبيانات الشخصية الإلكترونية دون اتخاذ الاحتياطات اللازمة لضمان أمن هذه البيانات الشخصية.

٢- جمع البيانات الشخصية بدون سبب مشروع أو بأي وسيلة غير مشروعة، بالإضافة إلى ذلك يمنع جمع البيانات والمعلومات عن طريق الغش والتدليس.

٣- جمع البيانات التي تقتضي طبيعتها عدم جمعها ، مثل البيانات الخاصة بالمعتقدات الدينية والاتجاهات السياسية أو الفلسفية أو الانتماءات النقابية أو الاخلاق الشخصية وذلك حماية لحرية الفكر والاعتقاد(١) ، باستثناء الجهات التي يسمح لها بالقانون جمع هذه البيانات الشخصية. مثل البيانات التي تتعلق بإجراءات الأمن القومي أو الأحكام القضائية أو لتحقيق مصلحة عامة في التخطيط والتنمية وفقا لما تنص عليه مواد قانون حماية البيانات الشخصية. ونستخلص من ذلك أن المشرع الفرنسي يشترط لقيام الركن المعنوي لجريمة التسجيل غير المشروع للبيانات الشخصية المعالجة إلكترونياً قيام الجاني

(١) – د. نعيم مغبغب ، المرجع السابق ، ص ٢٥٣.

بارتكاب بأحد الافعال السابقة عن عمد أي توافر القصد الجنائي بعنصريه العلم والإرادة، أي أن يعلم الجاني بأنه يقوم إجراء المعالجة للبيانات الشخصية المعالجة إلكترونياً دون اتخاذ الاحتياطات اللازمة لضمان أمن هذه البيانات الشخصية، أو جمع البيانات الشخصية بدون سبب مشروع أو بأي وسيلة غير مشروعة، أو جمع البيانات التي تقتضي طبيعتها عدم جمعها. وبالتالي لا يتصور ارتكاب هذه الجريمة عن طريق الاهمال أو السهو.

وقد نص المشرع الفرنسي على تعديل للمادة ٦ من قانون حماية البيانات الشخصية الصادر في ١٩٧٨ بالقانون رقم ٤١ لسنة ٢٠١٦ الصادر في ٢٦ يناير ٢٠١٦، في المادة ١٩٣ منه على أنه تتعلق المعالجة فقط للبيانات الشخصية التي تستوفي الشروط التالية:

١ ° أن يتم جمع البيانات ومعالجتها بطريقة عادلة ومشروعة؛

٢ ° أن يتم جمعها لأغراض محددة وصريحة ومشروعة ولا تتم معالجتها بطريقة تتنافي مع هذه الأغراض. ومع ذلك، فإن معالجة البيانات لأغراض إحصائية أو لأغراض البحث العلمي أو التاريخي تعتبر متوافقة مع الأغراض الأصلية لجمع البيانات، إذا تم تنفيذها وفقا للمبادئ والإجراءات المنصوص عليها في هذا القانون، الفصل الرابع والفصل الخامس، والفصل التاسع، ولا تستخدم في اتخاذ القرارات فيما يتعلق بمواضيع البيانات؛

٣ ° أنها كافية وملائمة وغير مفرطة فيما يتعلق بالأغراض التي تجمع من أجلها وتجهيزها اللاحق؛

٤ ° أنها دقيقة وكاملة، وإذا لزم الأمر، تحديث؛ يجب اتخاذ التدابير المناسبة لضمان حذف أو تصحيح البيانات غير الدقيقة أو غير المكتملة فيما يتعلق بالأغراض التي تجمعها أو تعالجها؛

٥ ° تحفظ في شكل يسمح بتحديد الأشخاص المعنيين لفترة لا تتجاوز الفترة اللازمة للأغراض التي يتم جمعها ومعالجتها.

وبالإضافة إلى ذلك فقد نص المشرع الفرنسي على انه "يجب أن تكون معالجة البيانات الشخصية بموافقة الشخص موضوع البيانات أو تتوافر أحد الشروط التالية([1]) :

١ ° الامتثال للالتزام القانوني الذي يقع على المراقب؛

٢ ° الحفاظ على حياة الشخص المعني؛

٣ ° تنفيذ لأمر المصلحة العامة التي تتم وفقا لمسئولية المراقب أو المرسل إليه للمعالجة؛

٤ ° تنفيذ أي عقد يكون الطرف المعني طرفا فيه أو تدابير سابقة تعاقدية تتخذ بناء على طلب الأخير؛

٥° لأغراض المصالح المشروعة من قبل وحدة تحكم أو من قبل المرسل، ولكن مع مراعاة عدم تجاهل المصالح أو الحقوق والحريات الأساسية للشخص موضوع البيانات".

وقد سار المشرع المصري على نفس نهج المشرع الفرنسي فنص على في المادة ٣ من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ على أنه "يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها توافر الشروط التالية([2]):

([1]) – انظر نص المادة ٧ من القانون الفرنسي الخاص بحماية البيانات الشخصية رقم ٨٠١ لسنة ٢٠٠٤ الصادر في ٦ أغسطس ٢٠٠٤ ، وذلك تعديلاً لقانون الصادر في ٢٣ يوليو ١٩٧٨.

([2]) – أنظر المادة ٣ من القانون المصري بشأن حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

١- أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني.

٢- أن تكون صحيحة وسليمة ومؤمنة.

٣- أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها.

٤- ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها".

بالإضافة إلى ذلك نص المشرع المصري في المادة ٤ من قانون حماية البيانات الشخصية على أن "يلتزم المتحكم بما يأتي([1]):

١- الحصول على البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا.

٢- التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها.

٣- وضع طريقة وأسلوب ومعايير المعالجة طبقا للغرض المحدد، ما لم يقرر تفويض المعالج في ذلك بموجب تعاقد مكتوب.

٤- التأكد من انطباق الغرض المحدد من جمع البيانات الشخصية لأغراض معالجتها.

([1]) – أنظر المادة ٤ من القانون المصري بشأن حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

٥- القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية إلا في الأحوال المصرح بها قانونًا.

٦- اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظًا على سريتها، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قِبَل أي إجراء غير مشروع.

٧- محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض، فيجب ألا تبقي في صورة تسمح بتحديد الشخص المعني بالبيانات.

٨- تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به.

٩- إمساك سجل خاص للبيانات، علي أن يتضمن وصف فئات البيانات الشخصية لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتحها لهم وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها وأي بيانات أخري متعلقة بنقل تلك البيانات الشخصية عبر الحدود ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات.

١٠- الحصول على ترخيص أو تصريح من المركز للتعامل مع البيانات الشخصية.

١١- يلتزم المتحكم خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية.

١٢- توفير الإمكانيات اللازمة لإثبات التزامه بتطبيق أحكام هذا القانون وتمكين المركز من التفتيش والرقابة للتأكد من ذلك".

كذلك فقد نص المشرع الفرنسي في المادة ٢٢-١ من قانون حماية البيانات الشخصية على أن يجب إخطار اللجنة القومية للمعلوماتية والحريات CNIL قبل إنشاء نظام لمعالجة البيانات الشخصية، وهذا الإخطار يلتزم به كل من سيقوم بإنشاء نظام للمعالجة سواء أكان جهة عامة أو جهة خاصة. ويتم هذا الإخطار بمجرد أن يرسل المسئول عن المعالجة خطاباً للجنة القومية للمعلوماتية والحريات، وإنه وفقا لنص المادة ٢٣-١ من قانون حماية البيانات الشخصية الفرنسي، يجوز مجرد إرسال رسالة إلكترونية للجنة القومية للمعلوماتية والحريات تتضمن الإخطار بإنشاء نظام لمعالجة البيانات الشخصية، يتحقق معه شرط الإخطار التي يتطلبها القانون. وبناءً على ذلك فقد اعتبرت اللجنة القومية الفرنسية للمعلوماتية والحريات CNIL أن إنشاء موقع على الإنترنت يتضمن تجمعياً للبيانات الشخصية للمستخدمين له بهدف إرسال نشرات دورية لهم ، إنشاء لنظام معالجة البيانات الشخصية(١)، الأمر الذي يتطلب معه إخطار اللجنة القومية للمعلوماتية والحريات قبل أن يتم أنشاء الموقع وإلا عد الشخص مخالف لقانون حماية البيانات الشخصية.

ويتضح ما سبق أن الهدف من الإخطار هو تمكين اللجنة القومية الفرنسية للمعلوماتية والحريات من ممارسة سلطاتها في العلم بأي عملية معالجة للبيانات الشخصية، ومن ثم رقابتها للتأكد من الالتزام بالقواعد المنصوص عليها في قانون حماية

(١) – CNIL, Délibération ٩٩ – ٠٢٦ du avril ١٩٩٩, délibération portant modification de la norme simplifiée n°٢٣ concernant des membres des associations a dut non lucratif régies par la loi du ١er juillet ١٩٠١, et disponible sur site, www.legifrance.gouv.fr.

البيانات الشخصية(١). بالإضافة إلى ذلك يحقق الإخطار مبدأ الشفافية لمن يتم معالجة بياناتهم والتأكد من أن نظام معالجة البيانات التي يتعامل معهم نظام مطابق للقانون.

وتطبيقاً على ذلك فقد قضت محكمة النقض الفرنسية بالعقاب على أحد رجال الأعمال(٢)، لأنه قام بإنشاء نظام للحضور والانصراف يتضمن معالجة البيانات الشخصية دون إخطار اللجنة القومية للمعلوماتية والحريات بهذا النظام المعالج للبيانات الشخصية. بالإضافة إلى ذلك فقد أقر الحكم بحق العامل في عدم الخضوع لهذا النظام، لأنه يعتبر نظاما غير مشروع للمعالجة ما دام أنه لم يتم إخطار اللجنة القومية للمعلوماتية والحريات به(٣).

أما بالنسبة للمشرع الألماني فقد نص في قانون تقييد خصوصية المراسلات والبريد والاتصالات على واجب إبلاغ المعنيين بالبيانات والمعلومات الشخصية التي تم معالجتها(٤)، أي ما يطلق عليه بمبدأ التبليغ. فيجب تبليغ الشخص موضوع البيانات بالإجراءات المقيدة بحسب القسم ٣ من القانون بعد وقفها. ويجب الحفاظ على هذا

---

(١) – Grévin ANTHONY, Les rapports entre le secret professionnel et le droit de la protection des données personnelles, mémoire de DEA informatique et droit, Fac droit; Univ Montpelliers I, ٢٠٠١, p. ٦٢.

(٢) – Cass. Crim, ٦ avril ٢٠٠٤, disponible sur sité, www.legifrance.gouv.fr.

(٣) – Nicolas IVALDI et Pascaline VINCENT, Cyber surveillqnce des salariés chartes informatiques, disponible sur sité, www.caproli-avocats.com, septembre ٢٠٠٥.

(٤) – القانون الألماني الخاص بتقييد خصوصية المراسلات والبريد والاتصالات ، الصادر في ٢٦ يونيو ٢٠٠١ ، الجريدة الرسمية الفيدرالية رقم ١ ، ص ١٢٥٤ وتنقيحه في ص ٢٢٩٨ ، وتم أخر تعديل له وفقا للقانون الصادر في ٣١ يوليو ٢٠٠٩ المادة رقم ١ ، الجريدة الرسمية الفيدرالية ، عدد رقم ١ ، القسم ١٢ ، ١، ص ٢٤٩٩.

التبليغ طالما لا يمكن استبعاد أن تبليغ الشخص موضوع البيانات قد يهدد غاية القيود أو طالما أن أي عقبات عامة لمصالح الاتحاد أو الدولة الاتحادية متوقعة. ويستمر التبليغ بحسب القسم ٢ من القانون بعد ١٢ شهراً من إنهاء الإجراء، ويجوز أن يطلب استمرار هذا الحق ولكن بشرط موافقة لجنة G١٠ على هذا الطلب. ويتعلق ذلك الحق لجميع البيانات والمعلومات ، وكذلك لحماية خصوصية الرسائل والبريد الإلكتروني والبيانات والمعلومات الشخصية على مواقع التواصل الاجتماعي بحيث يجب الالتزام بما يلي([1]) :

أ- أن يتم تبليغ الشخص موضوع البيانات والمعلومات الشخصية بالإجراء بعد الانتهاء منه معالجتها وبشرط إلا يكون غاية الإجراء مهددة.

ب-يجب تبليغ لجنة الرقابة البرلمانية.

وعليه يقوم المكتب الفيدرالي الألماني لحماية الدستور بتصحيح البيانات الشخصية وفقا لمبادئ المراجعة والتصحيح والحذف للبيانات الشخصية التي تم معالجتها، والمنصوص عليها في القانون وهي كالتالي([2]) :

ج- يجب أن تحذف البيانات الشخصية المحفوظة في ملفات من قبل المكتب الفيدرالي لحماية الدستور إذا كان تخزينها غير مقبول أو لم تعد معرفتها ضرورية لإتمام مهامها. ولا تحذف البيانات إذا لم يكن من سبب الظن بأن محوها قد يعيق المصالح المشروعة للشخص موضوع البيانات. في هذه الحالة تجمد البيانات ولا تنقل إلا بموافقة الشخص موضوعها.

([1]) – القانون الألماني الفيدرالي الخاص بحماية الدستور ، القسم ٩ ، ٣. والقانون الخاص G١٠ ، القسمان ١ ، ٤ ، ٥.

([2]) – القانون الالماني الفيدرالي السابق الاشارة اليه ، القسم ١٢.

د- في حالة التعامل مع الحالات الخاصة، على مكتب الفيدرالي لحماية الدستور التأكد من الفترات الزمانية المحددة، وبحد أقصى بعد خمس سنوات، إذا ما كان يجب تصحيح أو حذف البيانات الشخصية المحفوظة.

بالإضافة إلى ذلك فقد نص المشرع الفرنسي في المادة ٣٠ – ١ من قانون حماية البيانات الشخصية على مجموعة من البيانات يجب أن يتضمنها الإخطار وهي كالنحو التالي:

١- ذكر بيانات الهوية والعنوان للمسئول عن المعالجة للبيانات الشخصية في حالة ما إذا كان الشخص موجود على الإقليم الفرنسي، أما في حالة عدم وجود هذا الشخص على إقليم فرنسا أو إقليم دولة تابعة للاتحاد الأوربي يجب تحديد ممثل قانوني له في فرنسا.

٢- عرض الأغراض المبتغاة من عملية المعالجة للبيانات الشخصية.

٣- توضيح أي صلة قد تكون موجودة بين نظام المعالجة للبيانات الجديد وأنظمة المعالجة الأخرى الموجودة بالفعل.

٤- ذكر أنواع البيانات الشخصية التي سوف يتم معالجتها، وفئة الأشخاص المستهدفين من هذه المعالجة.

٥- كذلك يجب كتابة المدة التي سيتم حفظ البيانات الشخصية خلالها.

٦- بالإضافة إلى ذلك يذكر في بيانات الإخطار الأشخاص المخول لهم بمقتضي وظائفهم الاطلاع على هذه البيانات الشخصية.

٧- يوضح في الإخطار أي شخص يمكن إرسال هذه البيانات الشخصية إليه.

٨- كذلك ذكر كيفية ممارسة من سيتم معالجة بياناته لحقه في الدخول على بياناته الشخصية.

٩- يوضح في الإخطار التدابير التي سيتم اتخاذها لضمان أمن وسرية البيانات الشخصية التي سوف يتم معالجتها.

١٠- في النهاية يتم ذكر إذا كان سيتم نقل هذه البيانات الشخصية إلى دولة غير تابعة للاتحاد الأوربي والشكل الذي سيتم فيه هذا النقل للبيانات الشخصية.

ويتبين مما سبق أنه في جميع الأحوال لا يجوز البدء في إجراء المعالجة إلا بعد الحصول من اللجنة القومية الفرنسية للمعلوماتية والحريات CNIL على إيصال يفيد تسلمها للإخطار(١) ، هذا الإيصال يمكن أن يتم إرساله إلكترونياً ، وقد أوجب القانون على اللجنة أن تقوم فور استلمها الإخطار أن تقوم بإرسال ايصال الاستلام.

واستثناءً من الأصل إخطار اللجنة القومية الفرنسية للمعلوماتية والحريات CNIL قبل معالجة البيانات الشخصية، استثنى المشرع الفرنسي بعض الحالات من ذلك، وهي صور للمعالجة بدون الالتزام بشرط الإخطار وهي على النحو التالي:

١- المعالجات التي تهدف فقط لإنشاء سجل أو دفتر بموجب قواعد قانونية، ويكون الهدف من هذا السجل هو إعلام الكافة حيث يكون لأي شخص الحق في الحصول على معلومة منه مادامت له مصلحة مشروعة في ذلك(٢). مثال على ذلك السجل

(١) – انظر المادة ٢٣ – ١ من قانون حماية البيانات الشخصية الفرنسي.
(٢) – أنظر المادة ٢٢ – II من قانون حماية البيانات الشخصية الفرنسي.

الذي يتم إنشاؤه للمزارعين بمقتضى القانون الزراعي(١)، أو السجل التجاري الذي يتم إنشاؤه للتجار حيث يتضمن بيانات عن كل تاجر بموجب قانون التجارة. فهذه السجلات رغم أنه تعتبر معالجة للبيانات الشخصية لأصحاب هذه المهن إلا أنه لا يتطلب الأمر فيها أخطار اللجنة القومية للمعلوماتية والحريات وذلك لأنها تتم وفقاً للقواعد القانونية المنظمة لهذه المهن.

٢- المعالجات التي تتم للبيانات الشخصية من قبل جمعية أو أي شخص اعتباري لا يهدف لتحقيق الربح ويكون له صفة دينية أو سياسية أو نقابية(٢). مثال على ذلك إنشاء ملف خاص بأعضاء حزب سياسي داخل هذا الحزب، فيجوز تناول الآراء السياسية لهؤلاء الأعضاء ومعالجة البيانات الشخصية دون حاجة لإخطار اللجنة القومية للمعلوماتية والحريات(٣). ولكن بشرط أن تكون المعالجة في حدود الغاية من الشخص الاعتباري ولا يجوز نقل هذه البيانات خارج إطار الشخص الاعتباري.

٣- المعالجات التي تتم بهدف ممارسة مهنة الصحافة ، بشرط أن تتم في إطار احترام القواعد المهنية لهذه الممارسة(٤).

---

(١) - Benoit TABAKA et Yann TESAR, Loi informatique et libérés, un nouveau cadre juridique pour le traitement des données à caractère personnel, Disponible sur sité, www.foruminternet.org, octobre ٢٠٠٤, p. ٤٥. Art ٢٢

(٢) - أنظر : المادة ٢٢ – II من قانون حماية البيانات الشخصية الفرنسي.

(٣) - Benoit TABAKA et Yann TESAR, *Op.Cit.*, p. ٤٦.

(٤) - أنظر : المادة ٦٧ al ١– ٠ ، ٢ من قانون حماية البيانات الشخصية الفرنسي. وانظر كذلك : د. سامح عبدالواحد التهامي ، الحماية القانونية للبيانات الشخصية ، دراسة في القانون الفرنسي ، القسم الثاني ، مجلة الحقوق الكويتية ، العدد ٤ ، ديسمبر ٢٠١١ ، ص ٢٢٣ – ٢٢٥.

بالإضافة إلى ما سبق فقد نص المشرع الفرنسي على أن يقوم المراقب أو الشخص الذي يحق له تمثيله بتقديم البيانات وطلبات إبداء الرأي وطلبات الإذن، وذلك في حالة ما إذا كان المراقب شخصاً طبيعياً، أما في حالة ما كان المراقب شخص اعتباري أو سلطة عامة ينتمي إليها، فتقدم البيانات والطلبات إلى اللجنة كالتالي([1]) :

١- برسالة موجهة مزيلة بتوقيع.

٢- أو عن طريق تسليمها باليد إلى أمانة اللجنة.

٣- أو عن طريق إلكتروني، مع ضرورة الحصول على إقرار أو ايصال بالاستلام. يحدد تاريخ الاستلام، حيث يجب على اللجنة الرد خلال مدة لا تتجاور شهرين من تاريخ الاستلام.

ويقصد بالمراقب "كل شخص طبيعي أو معنوي يقوم منفرداً أو بالاشتراك مع آخرين بتحديد كيفية معالجة البيانات الشخصية والغرض منها وفقا لما تنص عليه القوانين واللوائح". أما المعالج "فهو الشخص الطبيعي أو المعنوي الذي يقوم بمعالجة البيانات الشخصية لصالح المراقب"([2]).

وأما بالنسبة للموقف المشرع القطري فقد نص في القانون رقم ١٣ لسنة ٢٠١٦ الخاص بحماية خصوصية البيانات الشخصية على مجموعة من الالتزامات التي تقع

([1]) – المادة ٨ من المرسوم رقم ١٣٠٩ لسنة ٢٠٠٥ ، الصادر في ٢٠ أكتوبر ٢٠٠٥ المتعلق بتطبيق القانون رقم ١٧-٧٨ لسنة ١٩٧٨ المتعلق بمعالجة البيانات والملفات والحريات ، والمعدل بالمرسوم رقم ٤٥١ لسنة ٢٠٠٧ الصادر في ٢٥ مارس ٢٠٠٧.

([2]) – انظر المادة الأولى من القانون القطري رقم ١٣ لسنة ٢٠١٦ لحماية خصوصية البيانات الشخصية.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

على المراقب للبيانات الشخصية الإلكترونية سواء في مرحلة ما قبل المعالجة، أو أثناء المعالجة، وبعد الانتهاء من المعالجة، هو ما سوف نتناوله بالشرح على النحو التالي:

أولا. الالتزامات التي تقع على المراقب في مرحلة ما قبل المعالجة: أي قبل البدء في معالجة أية بيانات شخصية، ويشترط أن يعلم الفرد بها قبل إجراء المعالجة لبياناته الشخصية وهي على النحو التالي([1]):

١- بيانات المراقب، أو أي طرف آخر يتولى معالجة البيانات لصالح المراقب أو لاستغلالها من قبله.

٢- الأغراض المشروعة التي يرغب المراقب أو أي طرف آخر في معالجة البيانات الشخصية من أجلها.

٣- الوصف الشامل والدقيق لأنشطة المعالجة ودرجات الإفصاح عن البيانات الشخصية للأغراض المشروعة، وإذا لم يتمكن المراقب من ذلك، فيتعين عليه تمكين الفرد من وصف عام لها.

٤- أية معلومات أخرى تكون ضرورية ولازمة لاستيفاء شروط معالجة البيانات الشخصية.

وكذلك هناك التزامات إجرائية تقع على عاتق المراقب لحماية خصوصية البيانات الشخصية قبل المعالجة وهي على النحو التالي

١- مراجعة الإجراءات لحماية الخصوصية قبل إدراج عمليات معالجة جديدة.

([1]) - أنظر المادة ٩ من القانون القطري لحماية خصوصية البيانات الشخصية.

٢- تحديد المعالجين المسئولين عن حماية البيانات الشخصية.

٣- تدريب وتوعية المعالجين على حماية البيانات الشخصية.

٤- وضع نظم داخلية لتلقي ودراسة الشكاوى، وطلبات الوصول للبيانات، وطلبات تصحيحها أو حذفها، وإتاحة ذلك للأفراد.

٥- وضع نظم داخلية للإدارة الفعالة للبيانات الشخصية، والإبلاغ عن أي تجاوز للإجراءات التي تهدف إلى حمايتها.

٦- استخدام الوسائل التكنولوجية المناسبة لتمكين الأفراد من ممارسة حقهم في الوصول إلى البيانات الشخصية ومراجعتها وتصحيحها بشكل مباشر.

٧- إجراء عمليات تدقيق ومراجعة شاملة عن مدى الالتزام بحماية البيانات الشخصية.

٨- التحقق من التزام المعالج بالتعليمات التي يوجهها إليه، واتخاذ الاحتياطات المناسبة لحماية البيانات الشخصية، ورصد ومتابعة ذلك بصفة مستمرة.

بالإضافة إلى ذلك تقع على عاتق المراقب الالتزام بالتحقق من أن البيانات الشخصية التي يجمعها، أو التي يتم جمعها لصالحه يتوافر فيها الشروط التالية:

١- ذات صلة بالأغراض المشروعة وكافية لتحقيقها.

٢- عليه التحقق من أن تلك البيانات دقيقة ومكتملة.

٣- وأن تكون هذه البيانات محدثة بما يفي بالأغراض المشروعة.

٤- إلا يتم الاحتفاظ بهذه البيانات الشخصية لمدة تزيد على المدة الضرورية لتحقيق تلك الأغراض.

ثانيا. الالتزامات التي تقع على المراقب في مرحلة المعالجة: أي ما يتعلق بمرحلة المعالجة للبيانات الشخصية فيتعين على المراقب الالتزام بالشروط التالية:

١- معالجة البيانات الشخصية بأمانة ومشروعية.

٢- مراعاة الضوابط الخاصة بتصميم أو تغيير أو تطوير المنتجات والنظم والخدمات المتعلقة بمعالجة البيانات الشخصية.

٣- اتخاذ الاحتياطات الإدارية والفنية والمادية المناسبة لحماية البيانات الشخصية، وفقاً لما تحدده الإدارة المختصة.

٤- سياسات حماية الخصوصية، التي تضعها الإدارة المختصة ، ويصدر بها قرار من الوزير .

٥- يجب على المراقب لدى إفصاحه عن البيانات الشخصية أو نقلها إلى المعالج، مراعاة أن تكون مطابقة للأغراض المشروعة، وأن تكون تلك البيانات معالجة وفقاً لأحكام هذا القانون.

ثالثا. الالتزامات التي تقع على المراقب في مرحلة ما بعد المعالجة: أي ما يجب على المراقب اتخاذ من إجراءات لحماية البيانات الشخصية التي تم معالجتها وهى على النحو التالي:

١- يجب اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية من الضياع أو التلف أو التعديل أو الإفشاء، أو الوصول إليها أو استخدامها بشكل عارض أو غير مشروع.

٢- ويجب أن تكون تلك الاحتياطات متناسبة مع طبيعة وأهمية البيانات الشخصية المراد حمايتها. وعلى المعالج أن يخطر المراقب بوجود أي إخلال بالاحتياطات المشار إليها، أو عند حدوث أي خطر يهدد البيانات الشخصية للأفراد بأي وجه، فور علمه بذلك.

٣- يجب على المراقب إعلام الفرد والإدارة المختصة، بحدوث أي إخلال بالاحتياطات المنصوص عليها في الفقرة السابقة، إذا كان من شأن ذلك إحداث ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد.

٤- يُحظر على المراقب اتخاذ أي قرار أو إجراء من شأنه الحد من تدفق البيانات الشخصية عبر الحدود، إلا إذا كانت معالجة تلك البيانات مخالفة لأحكام هذا القانون، أو كان من شأنها إلحاق ضرر جسيم بالبيانات الشخصية أو بخصوصية الفرد.

أما بالنسبة لموقف المشرع المصري فقد ألزم قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤ الجهات التي تعطي شهادة التصديق على التوقيع الإلكتروني بكفالة الحق في خصوصية البيانات والمعلومات الشخصية التي تم معالجتها في مجال التوقيع الإلكتروني من أي انتهاك، فنصت المادة ١٢ من اللائحة التنفيذية لهذا القانون على أن يجب أن تتوافر لدى طالب الحصول على الترخيص بإصدار شهادات التصديق الإلكتروني المتطلبات التالية: أ. نظام تأمين للمعلومات وحماية البيانات وخصوصيتها بمستوى حماية لا يقل عن المستوى المذكور في المعايير والقواعد المشار إليها في الفقرة (د) من الملحق الفني والتقني للائحة. ونستخلص مما سبق أن المشرع المصري ينص على حماية الحق في خصوصية البيانات والمعلومات الشخصية المتعلقة بالتوقيع

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

الإلكتروني من خلال إلزام القانون الجهة التي تم الترخيص لها بإصدار التوقيع الإلكتروني أن تعمل على المحافظة على تلك البيانات والمعلومات الشخصية ضد أي اعتداء عليها فنص على معاقبة الشخص الاعتباري ممثلاً في شخص المسئول عن الإدارة الفعلية بالمادة ٢٤ من نفس القانون بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحاكم هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة بهذا القانون، مما يكون قد أسهم في وقوع الجريمة مع علمه بذلك ، وفي هذه الحالة يعاقب بالحبس وبالغرامة المالية التي لا تقل عن عشرة آلاف جنية ولا تتجاوز مائة ألف جنية أو بإحدى هاتين العقوبتين.

وعليه وفي جميع الأحوال يكون الشخص الاعتباري مسئولاً بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد ارتكبت من أحد العاملين به باسم ولصالح الشخص الاعتباري. كذلك يكون لهيئة تنمية صناعة تكنولوجيا المعلومات أن تلغي الترخيص، كما يكون لها أن توقف سريانه حتى يتم إزالة أسباب المخالفة.

بالإضافة إلى ذلك فقد نص المشرع المصري في المادة ٥٨ من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ على إلزام الجهات التي تقوم بالاتصالات وتحصل على ترخيص باحترام الخصوصية بمجموعة من الالتزامات وهي كالتالي:

١- يتولى الجهاز القومي لتنظيم الاتصالات تجميع وإدارة وتحديث قاعدة بيانات مستخدمي الطيف الترددي، ويلتزم الجهاز بالحفاظ على سرية هذه البيانات حماية لحق المستخدمين في خصوصية بياناته.

٢-يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزه لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز والقوات المسلحة وأجهزة الأمن القومي، ولا يسري ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني.

ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة ، كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة(١). وقد نص المشرع المصري على معاقبة كل من يخالف ذلك بالحبس وبالغرامة المالية التي لا تقل عن عشرة آلاف جنية ولا تجاوز مائة ألف جنية. فضلاً عن ذلك تحكم المحكمة بوقف الترخيص مؤقتاً لحين قيام المخالف بتوفير المعدات والنظم وبرامج الاتصالات المشار إليها في نفس القانون.

ولكن مع إصدار المشرع المصري قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ ونص في المادتين الرابعة والخامسة منه على مجموعة من الالتزام على المتحكم والمعالج، ونص في المادة ٣٨ من نفس القانون على معاقبة كل متحكم أو معالج لم

(١) – المادة ٦٤ من قانون تنظيم الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣ ، الصادر في ٤ فبراير ٢٠٠٣.

يلتزم بواجباته المنصوص عليها بالغرامة التي لا تقل عن ثلاثمائة ألف جنية ولا تجاوز ثلاثة ملايين جنية.

الفرع الخامس. جريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية

في البداية نستعرض موقف المشرع الفرنسي من تجرم الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية، حيث نص في المادة ٢٢٦ -٢١ من قانون العقوبات المعدلة بالقانون رقم ٨٠١ لسنة ٢٠٠٤ الخاص بحماية البيانات الشخصية والتي تنص على أن يعاقب بالحبس مدة لا تزيد عن خمس سنوات والغرامة المالية التي لا تزيد مقدارها عن ٣٠٠.٠٠٠ آلف يورو كل من حاز بيانات شخصية بمناسبة تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة، إذا غير من الغرض أو الغاية أو الوجهة النهائية المقررة لهذه البيانات المحددة في القانون أو القواعد التنظيمية أو قرار اللجنة الوطنية للمعلوماتية والحريات المتعلقة بالإخطار المسبق على القيام بالمعالجة. ونستخلص من ذلك أن السلوك الإجرامي المكون للركن المادي لهذه الجريمة يتمثل في مجرد الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية(١). حيث تفترض هذه الجريمة أن المعالجة الإلكترونية للبيانات الشخصية كانت مشروعة وفقا للقواعد القانونية، وبعد الحصول على ترخيص من اللجنة القومية للمعلومات والحريات، ولكن قام الجاني بالانحراف عن الغرض أو الغاية المقصود من المعالجة الإلكترونية للبيانات الشخصية والتي بموجبها حصل على الترخيص بالمعالجة.

وتطبيقا على ذلك في عام ١٩٨٩ عندما تمكن أحد كبار موظفي أحد البنوك السويسرية بمساعدة سلطات الضرائب الفرنسية بأن سرب إليها شريطاً يحتوي على

(١) – آدم عبد البديع حسين ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٠ ، ص ٥٧٩.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

أرصدة عدد من العملاء، وقد تكرر مثل هذه الحادث في ألمانيا أيضا ، وقد أظهرت القضايا التي حصلت ما بين عامي ١٩٩٦ و ١٩٩٧ في المجال الصرفي أو الوصول إلى البيانات الشخصية المعالجة إلكترونياً ارتبط في الغالب بالابتزاز التي يتعلق بالتحايل على الضريبة من قبل عملاء البنوك(١). نستخلص من ذلك أن النشاط الإجرامي المكون لجريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية يتحقق بالكشف عن مصادر الثروة أو معرفة المركز المالي للعميل من أجل الاستدلال عليه لخدمة مصلحة الضرائب(٢)، بطريق غير مشروعة يعاقب عليها قانون العقوبات الفرنسي. ويتبين من ذلك أن من أبلغ الأخطار التي تصيب الفرد في خصوصية بياناته هو أن يتم جمع البيانات والمعلومات الشخصية لغرض معين ومحدد ابتداءً ولكن يتم الانحراف عن الغرض أو الغاية التي جمعت من أجلها في الاساس(٣). مما يمثل معه انتهاك للحق في خصوصية البيانات الشخصية.

أما بالنسبة لموقف المشرع المصري فقد نص في المادة ٩٧ من قانون البنك المركزي والجهاز المصرفي والنقد رقم ٨٨ لسنة ٢٠٠٣ على أن "تكون جميع حسابات العملاء وودائعهم وأماناتهم وخزانتهم في البنوك وكذلك المعاملات المتعلقة بها سرية، ولا يجوز الاطلاع عليها أو إعطاء بيانات عنها بطريق مباشر أو غير مباشر إلا بإذن

---

(١) – انظر: د. محمد سامي الشوا ، جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال ، المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ، البرازيل ، ريو دي جانيرو ، في الفترة من ٤ إلى ٩ سبتمبر ١٩٩٤. Siber ULRICH, Computer crimes and other crimes against information technology, R.I.D.P, ١٩٩٤, Vol. ٦٢, p. ١٠٣٦.

(٢) – أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، الطبعة الثالثة ، دار النهضة العربية ، القاهرة ، ١٩٩٤ ، ص ٩٩.

(٣) – د. محمد عبد المحسن المقاطع ، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي ، ذات السلاسل للطباعة والنشر ، الكويت ، ١٩٩٢ ، ص ٩٦.

كتابي من صاحب الحساب أو الوديعة أو الأمانة أو الخزينة أو من أحد ورثته أو من أحد الموصي لهم بكل أو بعض هذه الأموال، أو من النائب القانوني أو الوكيل المفوض في ذلك أو بناء على حكم قضائي أو حكم محكمين. ويسرى الحظر المنصوص عليه في الفقرة السابقة على جميع الأشخاص والجهات بما في ذلك الجهات التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقاً لأحكام هذا القانون، ويظل هذا الحظر قائماً حتى ولو انتهت العلاقة بين العميل والبنك لأي سبب من الأسباب".

وكذلك تنص المادة ٩٨ من نفس القانون على "أن للنائب العام أو لمن يفوضه من المحامين العامين الأول على الأقل من تلقاء نفسه أو بناء على طلب جهة رسمية أو أحد من ذوي الشأن، أن يطلب من محكمة استئناف القاهرة الأمر بالاطلاع أو الحصول على أية بيانات أو معلومات تتعلق بالحسابات أو الودائع أو الأمانات أو الخزائن المنصوص عليها في المادة السابقة أو المعاملات المتعلقة بها إذا اقتضى ذلك كشف الحقيقة في جناية أو جنحة قامت الدلائل الجدية على وقوعها. ولأي من ذوي الشأن في حالة التقرير بما في الذمة بمناسبة حجز موقع لدى أحد البنوك الخاضعة لأحكام هذا القانون أن يتقدم بالطلب المشار إليه في الفقرة السابقة إلى محكمة الاستئناف المختصة. وتفصل المحكمة منعقدة في غرفة المشورة في الطلب خلال الأيام الثلاثة التالية لتقديمه بعد سماع أقوال النيابة العامة أو ذي الشأن. وعلى النائب العام أو من يفوضه في ذلك من المحامين العامين الأول على الأقل وعلى ذي الشأن بحسب الأحوال إخطار البنك وذوي الشأن بالأمر الذي تصدره المحكمة خلال الأيام الثلاثة التالية لصدوره. ويبدأ سريان الميعاد المحدد للتقرير بما في الذمة من تاريخ إخطار البنك بالأمر المذكور. ويكون للنائب العام أو من يفوضه من المحامين العامين الأول على الأقل أن يأمر مباشرة بالاطلاع أو الحصول على أية بيانات أو معلومات تتعلق بالحسابات أو الودائع أو الأمانات أو الخزائن المنصوص عليها في المادة ٩٧ من هذا

القانون أو المعاملات المتعلقة بها إذا اقتضى ذلك كشف الحقيقة في جريمة من الجرائم المنصوص عليها في القسم الأول من الباب الثاني من الكتاب الثاني من قانون العقوبات، وفي الجرائم المنصوص عليها في قانون مكافحة غسل الأموال الصادر بالقانون رقم ٨٠ لسنة ٢٠٠٢".

بالإضافة إلى ذلك فقد نصت المادة ٩٩ من نفس القانون على "أن يضع مجلس إدارة البنك المركزي القواعد المنظمة لتبادل البنوك معه وفيما بينها المعلومات والبيانات المتعلقة بمديونية عملائها والتسهيلات الائتمانية المقررة لهم ، بما يكفل سريتها ويضمن توافر البيانات اللازمة لسلامة تقديم الائتمان المصرفي ، كما يضع القواعد التي يلزم اتباعها لإعداد تقارير الفحص الشامل عن البنوك تمهيداً لبيع أسهمها كلها أو بعضها أو لاندماجها". أما المادة ١٠٠ فتنص على "أن يحظر على رؤساء وأعضاء مجالس إدارة البنوك ومديريها أو العاملين بها إعطاء أو كشف أية معلومات أو بيانات عن عملاء البنوك أو حساباتهم أو ودائعهم أو الأمانات أو الخزائن الخاصة بهم أو معاملاتهم في شأنها أو تمكين الغير من الاطلاع عليها في غير الحالات المرخص بها بمقتضى أحكام هذا القانون. ويسرى هذا الحظر على كل من يطلع بحكم مهنته أو وظيفته أو عمله بطريق مباشر أو غير مباشر على البيانات والمعلومات المشار إليها". وفي النهاية يعاقب كل من يخل بأي من القواعد المنصوص عليها في المواد السابقة بالحبس مدة لا تقل عن سنة وبغرامة مالية لا تقل عن عشرين آلف جنية ولا تزيد على خمسين ألف جنية.

وتطبيقاً على ذلك فقد قضت محكمة النقض المصرية إلى أن(١) "مؤدى تلك النصوص أن القانون كفل سرية المراكز المالية لعملاء البنوك من حسابات وودائع وخزانات لديها ومعاملاتهم عليها، ولم يصرح بالكشف عنها أو الاطلاع عليها إلا في الأحوال التي حددها وفقاً للإجراءات التي رسمها ووضع الالتزام بالمحافظة على هذه السرية على جميع القائمين على أمر تلك البنوك وعمالها وعلى العاملين بالجهات الأخرى التي خولها القانون الاطلاع على شيء من ذلك، ولم يحل أي من هؤلاء من التزامه هذا إلا في الأحوال المشار إليها. لما كان ذلك، وكان الحكم المطعون فيه استند في قضائه ببراءة المطعون ضده ورفض الدعوى المدنية إلى مجرد القول بذيوع بيانات الحساب عن مديونية الطاعن للبنك بتوقيع الحجز عليه وبإبلاغ النيابة العامة ضده، في حين أن كلا الإجرائيين توقيع الحجز وإبلاغ النيابة العامة من الإجراءات التي ألزم القانون القائمين عليها من البنك وغيره بالمحافظة على سرية ما يتصلون به من بيانات بمناسبتها بطريقة مباشرة أو غير مباشرة، فإنه يكون قد أخطأ في تأويل القانون وفي تطبيقه خطأ حجب المحكمة عن بحث صلة المطعون ضده ببيانات حساب الطاعنين ومدى مسئوليته عن كشف مديونيتهما للبنك الذى يعمل به وعما يكون قد لحق بالطاعنين من أضرار من جراء ذلك وهو ما يعيبه فضلاً عن الخطأ في القانون بالقصور الذى يوجب نقضه والإعادة في خصوص الدعوى المدنية". وبناءً على ما سبق، يتضح لنا أن المشرع المصري يحمي الحق في خصوصية البيانات والمعلومات الشخصية المعالجة إلكترونياً المتعلقة بنوع معين من البيانات والمعلومات(٢) وهي الخاصة بالحسابات والمعاملات المالية التي تتم فيما بين البنك وعملائه أيا كانت وسيلة حفظها وتخزينها بما في ذلك نظم المعلومات والبيانات الإلكترونية. ولكن ينتقد المشرع المصري على أنه

---

(١) – نقض جنائي مصري ، مجموعة أحكام محكمة النقض ، الطعن رقم ٥٥١٥ لسنة ٦٦ ، جلسة ١٤ أبريل ٢٠٠٣ ، س ٥٤ ، ق ٦٥ ، ص ٥٤٠.

(٢) – د. هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، الطبعة الأولى ، مكتبة الآلات الحديثة ، أسيوط ، ١٩٩٢ ، ص ٣٧٣ ، ٣٧٤.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

يقصر العقاب على هذه الجرائم على المختصين بالتعامل مع تلك البيانات والمعلومات بالحسابات والبنوك فقط، وبالتالي كان من باب أولى أن يمتد العقاب ليشمل المختصين وغير المختصين وذلك لحماية البيانات والمعلومات في حد ذاته سواء وقع الجرم من قبل مختصين أو غير مختصين.

بالإضافة إلى ذلك فقد نص المشرع المصري في المادة ٢١ من قانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الإلكتروني على "أن بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجلة. وبناء على ذلك فقد قرر المشرع المصري الحماية الجنائية لسرية البيانات الخاص بالتوقيع الإلكتروني والوسائط الإلكترونية والمعلومات المتعلقة بذلك والتي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني. وتعني السرية في هذا القانون عدم معرفة الغير من غير المتعاقدين بيانات العملية التجارية ، أما الخصوصية تعني ارتباط هذه البيانات بالمتعاقدين أطراف العملية التجارية مما يحتم عدم إطلاع الغير عليها"(١)، وذلك حفاظاً على خصوصية وسرية المعلومات والبيانات الشخصية المتعلقة بالتوقيع الإلكتروني والبيانات والمعلومات المقدمة لذلك حتي ولو لم يترتب على ذلك نتيجة إجرامية. ويستخلص مما سبق أن موقف المشرع المصري محل انتقاد وذلك لأنه قصر الحماية الجنائية على خصوصية وسرية البيانات والمعلومات الشخصية المتعلقة بالتوقيع الإلكتروني وكذلك البيانات والمعلومات المقدمة لذلك الموضوع فقط، أي أن محل هذه الجريمة هي البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً والمتعلقة بالتجارة

(١) – د. هدى قشقوش ، المرجع السابق ، ص ٤١.

الإلكترونية أما أي بيانات أو معلومات شخصية إلكترونية فلا تخضع لحماية جنائية للحق في الخصوصية في مجملها.

ولكن موقف المشرع المصري تغيير مع صدور قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، حيث نص في المادة الخامسة منه على "يلتزم معالج البيانات الشخصية بما يأتي([1]):

١ – إجراء المعالجة وتنفيذها طبقًا للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقًا للحالات المشروعة والقانونية وبناءً علي التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أي ذي صفة بحسب الأحوال، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها ونوع البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد له.

٢ – أن تكون أغراض المعالجة وممارستها مشروعة، ولا تخالف النظام العام أو الآداب العامة.

٣ – عدم تجاوز الغرض المحدد للمعالجة ومدتها، ويجب إخطار المتحكم أو الشخص المعني بالبيانات أو كل ذي صفة، بحسب الأحوال، بالمدة اللازمة للمعالجة.

٤ – محو البيانات الشخصية بانقضاء مدة المعالجة أو تسليمها للمتحكم.

٥ – القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانونًا.

٦ – عدم إجراء أي معالجة للبيانات الشخصية تتعارض مع غرض المتحكم فيها أو نشاطه إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة.

([1]) – انظر المادة ٥ من القانون المصري بشأن حماية خصوصية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

٧ – حماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك وما عليها من بيانات شخصية.

٨ – عدم إلحاق أي ضرر بالشخص المعني بالبيانات بشكل مباشر أو غير مباشر.

٩ – إعداد سجل خاص بعمليات المعالجة لديه، علي أن يتضمن فئات المعالجة التي يجريها نيابة عن أي متحكم وبيانات الاتصال به ومسئول حماية البيانات لديه، والمدد الزمنية للمعالجة وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها، ووصفًا للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة .

١٠–توفير الإمكانيات لإثبات التزامه بتطبيق أحكام هذا القانون عند طلب المتحكم وتمكين المركز من التفتيش والرقابة للتأكد من التزامه بذلك.

١١–الحصول على ترخيص أو تصريح من المركز للتعامل على البيانات الشخصية.

١٢–يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية".

كذلك فقد نص المشرع المصري في المادة ٣٨ من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ على أن "يعاقب كل متحكم أو معالج لم يلتزم بواجباته والمنصوص عليها كما سبق وتناولنا سابقاً في المادة الخامسة أو الرابعة أو السابعة من نفس القانون، أي بأي انحراف أو إخلال بالواجبات المنصوص عليها في القانون بعقوبة الغرامة التي لا تقل عن ثلاثمائة ألف جنية ولا تجاوز ثلاثة ملايين جنية".

المبحث الثالث. جريمة إتلاف وتعطيل أنظمة المعالجة الآلية والتخزين للبيانات الشخصية الإلكترونية

في مستهل هذه المبحث لابد من تحديد مفهوم جريمة الإتلاف والتعطيل لأنظمة المعالجة الآلية والتخزين للبيانات الشخصية الإلكترونية فيقصد بها "كل محو للبيانات أو للمعلومات الشخصية أو تدميرها إلكترونياً أو أن يتم تشويه البيانات والمعلومات الشخصية على نحو يجعلها غير صالحه للاستخدام أو يعطلها"(١). فالإتلاف هنا هو إتلاف للبيانات والمعلومات الشخصية التي تم معالجتها إلكترونيا بحيث يؤثر على أنظمة المعالجة الآلية والتخزين للبيانات والمعلومات الشخصية الإلكترونية. وبالتالي يجعلها لا تستطيع أن تقوم بإداء مهامها المختلفة التي تعمل من أجلها.

وفي واقع الامر يظهر لنا أهمية هذه الموضوع في الوقت الحالي خاصة مع ظهور الحوسبة السحابة في تخزين المعلومات والبيانات الشخصية، ويقصد بالحوسبة السحابية بانها هي مجموعة من مصادر تقنية المعلومات ويشمل ذلك أجهزة الحواسب ومصادر البرامج الحاسوبية التي يتمكن المستخدم من الوصول إليها عبر الشبكة الحاسوبية. يقوم مزود الخدمة للحوسبة السحابية بإنشاء البنية التحتية للحوسبة السحابية وتشغيلها وإدارتها. والحوسبة السحابية هي القالب الذي يمكن المستخدم من سهولة إيجار أصول تقنية المعلومات وهي بذلك خدمة يقدمها مزود الخدمة للحوسبة السحابية .وخدمة الحوسبة السحابية هي تجميع لمصادر تقنية المعلومات، مثل شبكة يمكن الوصول إليها لتخزين ومعالجة البيانات، وبها تطبيقات ذات ميزات متكاملة ومعدات لتطوير ونشر

(١) – Bey. E.–M, Le financement des logiciels – peuton louer ou donner financièrement à bail Un Logiciel? Gazette du Palais, Paris, ١٩٨٥, P. ٣٩٦.

البرنامج وبذلك يقدمها مزود الخدمة للحوسبة السحابية للمستهلك. ويحافظ المزود على أدوات مشتركة لمصادر تقنية المعلومات وتكون هذه المصادر متاحة للجمهور كخدمة عبر أي شبكة كالشبكة العالمية الإنترنت أو الشبكة الداخلية الإنترانت([1]). وعلى سبيل مثال لذلك برنامج ICloud لتخزن البيانات والمعلومات التابع لشركة آبل الأمريكي من أشهر البرامج التي تستخدم الحوسبة السحابية في تخزين البيانات والمعلومات، وبالتالي الإتلاف أو التعطيل لهذه الانظمة المخزن عليها البيانات الشخصية التي تم معالجتها إلكترونيا يشكل خطورة كبيرة مما يوجب على المشرع التدخل بالنص على تجريم لهذا النشاط الإجرامي.

وتأسيسا على ما سبق قد نصت المادتين ٤ و٥ من اتفاقية بودابست لعام ٢٠٠١ للجرائم الإلكترونية على تجريم الأفعال التي من شأنها الإضرار بالبيانات الشخصية المعالجة إلكترونياً، باعتبارها من الجرائم العمدية التي تتم بدون وجه حق عن طريق الإضرار، أو المسح، أو إتلاف، أو إفساد أو حذف البيانات والمعلومات الشخصية. بالإضافة إلى ذلك تجريم الأفعال التي من شانها الإعاقة المتعمدة، وبدون وجه حق، لمنع تشغيل شبكة البيانات والمعلومات وذلك عن طريق الدخول للشبكة، أو تحويل، أو إرسال، أو الإضرار، أو مسح، أو إتلاف، أو إفساد، أو حذف البيانات الشخصية المعالجة إلكترونياً.

وانطلاقا مما سبق فقد ذهبت لجنة الخبراء الخاصة بوضع اتفاقية بودابست لمكافحة الجرائم الإلكترونية إلى أن تعديل البيانات يشمل خلطها بالغش أما عن طريق تعطيلها

([1]) – د. جمال درويش ، شبكات الحواسب السحابية ودورها في التنمية ، المنتدى السنوي الثاني لتكنولوجيا المعلومات والاتصالات ، بعنوان دور تكنولوجيا المعلومات والاتصالات في الإسراع بالتنمية في الوطن العربي ، القاهرة ، من ١٣ – ١٥ ديسمبر ٢٠١٥ ، ص ١.

أو إخماد أو كبت البيانات الشخصية المعالجة إلكترونياً، وعلى سبيل المثال لذلك أن يقوم الشخص بإجراءات من شانه منع وصول البيانات إلى العنوان المرسلة إليه كحذف جزء منها على نحو لا يتيح وصولها إلى الموقع الإلكتروني المطلوب أو تصبح غير قادرة على ذلك أو منع الغير من الوصول إليها. وقد ذهب جانب من الفقه(١) إلى القول بانه يشترط حصول الضرر جراء التدخل غير المشروع في البيانات الشخصية المعالجة إلكترونياً كنتيجة إجرامية للنشاط الاجرامي المتمثل في إتلاف البيانات الشخصية المعالجة إلكترونياً أو نظم المعالجة الآلية للبيانات الشخصية الإلكترونية.

وعليه فقد جاء بالمذكرة التفسيرية تعليقا على المادة الرابعة من الاتفاقية الاوربية بودابست لعام ٢٠٠١ ما يشير إلى أن الهدف من تقرير هذا النص هو أن تكون بيانات وبرامج ونظم المعالجة الآلية مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً، والمصالح القانونية التي تتمتع بها الأشياء المادية هي سلامة وحسن تشغيل أو حسن استخدام البيانات أو برامج ونظم المعالجة الآلية وكذلك حماية خصوصية هذه البيانات من الإتلاف أو التعطيل لنظم المعالجة وكل فعل من شأنه الأضرار بالحق في خصوصية البيانات أو المعلومات الشخصية المعالجة إلكترونياً من إتلاف أو محو أو تدمير أو تعطيل نظم المعالجة الآلية لها أي كل فعل من الأفعال السابقة متي ترتب عليها ضرر. ويتبين لنا مما سبق أن الفقرة الأولى من المادة الرابعة من اتفاقية بودابست لعام ٢٠٠١ استخدمت مصطلح الإضرار ومصطلح التعطيل لتعبير عن جريمة الإتلاف للبيانات والمعلومات الشخصية المعالجة إلكترونياً عن طريق كل فعل يؤثر على سلامة أو محتوي هذه البيانات والمعلومات الشخصية أو أنظمة وبرامج

(١) – د. يونس عرب ، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان ، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية ٢ – ٤ أبريل ٢٠٠٦ ، هيئة تنظيم الاتصالات ، مسقط – سلطنة عمان. ص ٣٦.

المعالجة الآلية لها، كما استخدمت نفس الفقرة أيضا مصطلح محو البيانات ، وهذا مصطلح يعادل مصطلح تدمير الأشياء في مجال تدمير الأشياء المادية ، فهو يهدمها ويجعلها في حالة لا يمكن التعرف عليها ، واستخدم النص مصطلح طمس البيانات والمعلومات، وهذا المصطلح يمتد ليشمل كل تصرف من شأنه أن يجعل هذه البيانات والمعلومات غير موجودة أو غير متاحة للشخص الذي له حق الولوج إلى داخل الحاسب الآلي أو الاعتماد على تلك البيانات التي كانت مخزنه، واستخدم النص كذلك مصطلح الإتلاف ويقصد به تغيير البيانات الموجودة، وكذلك إدخال شفرات عدوانية مثل الفيروسات أو البرامج الضارة(١) ، والتي من شأنها أن تغيير أو تدمر أو تتلف هذه البيانات أو تعطل أنظمة المعالجة الآلية الخاص بها.

ولذلك فقد نصت الاتفاقية الاوربية فيما يتعلق بالمعالجة الآلية للبيانات الشخصية(٢) في المادة ٧ على أنه يجب اتخاذ إجراءات أمنية مناسبة لحماية البيانات الشخصية المحفوظة في ملفات البيانات الآلية ضد الإتلاف العرضي وغير المجاز والفقدان العرضي والوصول والتعديل والنشر غير المصرح به.

وتأكيداً على خطورة السلوك الإجرامي المكون لجريمة إتلاف أو تدمير أو تعطيل البيانات الشخصية المعالجة إلكترونياً أو نظم المعالجة الآلية للبيانات الإلكترونية، فقد نصت المادة ٨ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في عام

---

(١) – د. أيمن عبدالله فكري ، الجرائم المعلوماتية ، دراسة مقارنة ، في التشريعات العربية والأجنبية ، الطبعة الأولى ، مكتبة القانون والاقتصاد ، الرياض ، ص ٣٤٥ ، ٣٤٦.

(٢) – الاتفاقية الأوربية المتعلقة بحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية ، الصادرة في ١٢ يناير ١٩٨١ ستراسبورغ ، والتعديلات عليه حتي التعديل الاخير باللائحة الاوربية العامة لحماية البيانات الشخصية GPDR رقم ٦٧٩ لسنة ٢٠١٦ ، والتي سوف تدخل حيز النفاذ في ٢٥ مايو ٢٠١٨.

٢٠١٠ على إلزام الدول الموقعة على هذه الاتفاقية بحماية سلامة البيانات من الاعتداء على النحو التالي:

١- من تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصداً ودون وجه حق.

٢- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (١) من هذه المادة أن تتسبب بضرر جسيم.

وبناء على ذلك نستطيع القول بأن جريمة الاتلاف في مجال البيانات والمعلومات الشخصية المعالجة إلكترونياً تقع بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج والبيانات والمعلومات الشخصية المخزنة والمتبادلة بين الحواسب وشبكاته، وتدخل ضمن الجرائم الماسة بسلامة البيانات الشخصية المخزنة ضمن نظام الآلي لمعالجة البيانات الشخصية الإلكترونية، ويكون الاتلاف العمدي للبرامج والبيانات الشخصية المعالجة إلكترونياً كمحوها أو تدميرها الكترونيا، أو تشويهها على نحو يجعلها غير صالحة للاستعمال ويتم ذلك نتيجة لدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للبيانات الشخصية كما سبق ذكره، ويتحقق الاتلاف للبيانات الشخصية المعالجة إلكترونياً من خلال الحالتين التاليتين هو ما سوف نتناوله في المطلب الاول، وفي المطلب الثاني نستعرض صور الإتلاف أو التخريب للبيانات الشخصية المعالجة إلكترونيا.

المطلب الاول. طرق الإتلاف للبيانات الشخصية الإلكترونية

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

في واقع الامر يتحقق الإتلاف للبيانات الشخصية التي تم معالجتها إلكترونياً من خلال طريقتين محددتين وذلك على النوع التالي:

الطريقة الأولى. اعاقة سير العمل في نظام المعالجة الآلية للبيانات الشخصية:

ويتمثل ذلك بكل فعل من شأنه أن يسبب تباطؤ عمل نظام المعالجة الالية للبيانات والمعلومات الشخصية أو ارباكه مما يؤدي إلى تغير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت وذلك من خلال تعديل البرامج في نظام المعالجة أو عمل برنامج احتيالي، أو من خلال التحويلات الإلكترونية كإغراق موقع على الشبكة الانترنت بالرسائل الالكترونية مما يؤدي إلى شله، بحيث يصبح غير قادر على أدي المهام والوظائف الذي أنشئ من أجله وإيقافه عن العمل أو تعطله.

وتطبيقا على ذلك ما ذكره مكتب التحقيقات الفيدرالي الأمريكي FBI في ٢٦ من سبتمبر ٢٠٠٢ من القبض على أحد عملائه ويدعى ماريو كاستللو ٣٦ عاما ومحاكمته بتهمة تخطي الحاجز الأمني المسموح له به والدخول على أحد أجهزة المكتب ستة مرات بغرض الحصول على بعض الأموال. حيث أن تعطيل العمل والذي يطلق عليه Denial of service attack واختصاراً DOS والذي يعتمد على إغراق أجهزة الخوادم بالآلاف أو ملايين الطلبات الحصول على معلومات الأمر الذي لا تحتمله قدرة المكونات المادية Hardware أو نظم قواعد البيانات والتطبيقات والبرامج الموجودة على تلك الخوادم التي تصاب بالشلل التام لعدم قدرتها على تلبية هذا الكم الهائل من الطلبات والتعامل معها(١) ، مما يؤدي إلى إعاقة سير العمل في نظام معالجة البيانات الشخصية الإلكترونية.

---

(١) – www.tashreaat.com/view studies٢.

وتأكيداً على ذلك فقد نصت المادة الخامسة من الاتفاقية بودابست لعام ٢٠٠١ على أن يجب على كل عضو في الاتفاقية أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم، تبعاً لتشريعيه الداخلي، الإعاقة الخطيرة، إذا حدث ذلك عمداً، ودون حق، لوظيفة نظام الحاسب، عن طريق إدخال، أو نقل، أو إضرار، أو محو، أو تعطيل، أو إتلاف، أو طمس البيانات المعلوماتية. وفقا لما جاء بالمذكرة التفسيرية للمادة الخامسة للاتفاقية يوضح أن التوصية رقم ٨٩/٩ أشارت إلى هذا العنوان تحت مسمى تخريب نظام الحاسب الآلي، وبهدف النص إلى تجريم الإعاقة العمدية للاستخدام أو التأثير على بيانات الحاسب الآلي، والمصالح القانونية المحمية هي مصلحة مشغلي، ومستخدمي نظام الحاسب الآلي، أو نظام الاتصالات في القيام بأعماله بدقه وحماية جميع أنواع الوظائف.

ونستخلص مما سبق أن المشرع الأوربي يجرم كل فعل يمثل اعتداء على حسن تشغيل النظام ويترتب عليه اعاقة سير العمل في نظام المعالجة الآلية للبيانات والمعلومات الشخصية، والمقصود بالإعاقة هي كل فعل ينحم عنه الإضرار أو المحو، أو الإتلاف، أو طمس البيانات والمعلومات الشخصية أي عدم سير العمل في نظام المعالجة الآلية للبيانات والمعلومات الشخصية بطريقة التي تؤدي إلى قيامه بمهامه التي أنشئ من أجلها، سواء تم ذلك لمشغلي النظام أو لمستخدميه.

وبناء على ذلك فقد نص المشرع الفرنسي على تجريم الاتلاف والتخريب والتهديد في المواد من ٣٢٢ – ١ إلى ٣٢٢ – ٤ من قانون عقوبات ، فقد نص في المادة ٣٢٢ –١ من قانون العقوبات الفرنسي على أن يعاقب كل من يقوم بالإتلاف أو التخريب أو التدمير بالسجن لمدة لا تزيد عن سنتين وبالغرامة المالية والتي لا تزيد مقدارها عن

٣٠٠٠٠٠ آلف يورو ولكن بشرط أن يترتب على هذا السلوك الإجرامي تحقق ضرر(١). ويتبين لنا مما سبق أن هذه الجريمة تختلف عن جريمة الدخول أو البقاء في النظام، كون أن مجرد الدخول الاحتيالي يعد جريمة قائمة بذاتها سواء كان الدخول إلى كل أو جزء من النظام المعلوماتي والبيانات الشخصية. كما أن الاعتداء على النظام المعلوماتي والبيانات الشخصية قد يقع دون المرور إلى النظام نفسه، مثال على ذلك حالة بث برامج من شأنها أن تؤثر على سير النظام أو على الشبكات المربوط بها.

أما بالنسبة لموقف المشرع الأمريكي فقد جرم نفس الأفعال ضمن قانون حماية الحاسب الآلي الصادر في عام ١٩٨٤ فنص على أن يعاقب كل شخص يقوم عمداً وبدون تصريح بإتلاف أو تدمير أو بمحاولة إتلاف أو تدمير حاسب أو أي من برامجه أو البيانات المخزنة داخلة بالسجن أو بالغرامة او بإحدى هاتين العقوبتين(٢). ويتضح من ذلك أن المشرع الأمريكي قد ساوي في التجريم بين أن يكون الاعتداء على المكونات المادية أو المكونات غير المادية للحاسب الآلي.

ومن الجدير بالذكر أنه قد تم تعديل هذا القانون من المشرع الأمريكي بقانون CCA بنص المادة ١٠٣٠ /٣/A بحيث أصبحت تنص على "أن يعاقب كل من توصل عن علم وبدون إذن إلى نظام الحاسب أو استغل فرصة وصولة إليه على نحو غير مصرح به لتحقيق أغراض لا يمتد إليها التصريح الممنوح له إذا تمكن بهذا السلوك من استخدام أو تعديل أو تدمير أو كشف المعلومات المخزنة داخله عن علم بذلك، أو منع الاستخدام

(١) – L'article ٣٢٢-١ du Code pénal, Modifié par Loi n° ٢٠٠٢ – ١١٣٨ du ٩ septembre ٢٠٠٢ – art. ٢٤ JORF ١٠ septembre ٢٠٠٢.

(٢) – M.W. MENDES, La législation pénale en matière de ordinateurs et les mesures de sécurité aux Etats – Uni, Droit de le informatique numéro spécial, ١٩٨٥, p. ٤٠.

المصرح به لنظام الحاسب ، ذلك إذا ما كان هذا الحاسب لأجل أو بالنيابة عن الحكومة الولايات المتحدة الأمريكية وكان من شأن سلوك الفاعل التأثير في تشغيل الحاسب". وقد قام المشرع الأمريكي بالعديد من التعديلات على هذه المواد في أعوام ١٩٨٦، ١٩٩٤، ١٩٩٦. وبذلك يتضح أن المشرع الأمريكي يعاقب على كل من يقوم بمنع أو يحرم أو يتسبب في منع أو حرمان الغير من استعمال كمبيوتر أو خدمات كمبيوتر أو نظام أو شبكة أو معلومات أو بيانات أو برامج(١).

بالإضافة إلى ذلك فإن المشرع الأمريكي قد نص في المادة ١٠٣٠ من نفس القانون على أن يعاقب كل من يقوم بقصد بالتسبب في تحويل لبرامج أو معلومات مشفرة، أو أمر، لنظام آلي مما يتسبب وكنتيجة لهذا السلوك بتعمد إحداث أضرار بدون تصريح، لحاسب مشمول بالحماية. مما يظهر أن المشرع الأمريكي يحمي الحق في خصوصية البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً من الإتلاف أو تعطيل لنظم معالجة هذه البيانات أو المعلومات الشخصية الإلكترونية.

أما بالنسبة لموقف المشرع الألماني فقد أصدر في ١٥ مايو ١٩٨٦ القانون الثاني لمكافحة الجريمة الاقتصادية والذي جرم فيه إتلاف أو محو أو تغيير أو تزوير البيانات المعالجة آلياً، وشدد العقوبة بالنسبة للبيانات ذات الأهمية الاساسية لقطاع الأعمال أو السلطة الإدارية لتصل إلى حد السجن لمدة خمس سنوات والغرامة. كذلك سن المشرع الدنماركي في ٦ يونيو ١٩٨٥ فصل خاص بجرائم الحاسب الآلي في قانون العقوبات من المواد ١٩٣ إلى ٢٦٣، وعاقب في المادة ١٩٣ من قانون العقوبات على جريمة إتلاف وتعطيل أنظمة المعالجة الآلية وتخزين البيانات.

---

(١) – د. مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الإلكترونية ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠١ ، ص ٤١ – ٤٢.

الطريقة الثانية. الاعتداء على البيانات والمعلومات الشخصية داخل نظام المعالجة الآلية لها، ويتم ذلك بإحدى الطرق التالية:

أ- محو البيانات والمعلومات الشخصية المعالجة إلكترونياً كلية وتدميرها: وقد استخدمت غالبية التشريعات التي تجرم الاعتداء على البيانات والمعلومات الشخصية داخل نظام المعالجة الآلية تعبير محو وتدمير البيانات والمعلومات الشخصية باعتبارها صورة متميزة من صور الإتلاف، على خلاف المشرع الانجليزي الذي يستخدم فعل التعديل غير المشروع للبيانات والمعلومات الشخصية باعتباره الصورة الوحيدة للركن المادي لهذه الجريمة.

ب- نقل البيانات والمعلومات الشخصية المعالجة إلكترونياً دون إذن : ويقصد بذلك هو كل نقل للبيانات والمعلومات الشخصية المعالجة إلكترونياً يترتب عليه الاعتداء على نظم المعالجة الآلية لها بدون إذن مما يمثله انتهاك للحق في الخصوصية، فهذا الفعل الإجرامي لا يشترط له تحقق نتيجة إجرامية لقيام الركن المادي المكون للجريمة ، بل يكفي السلوك الإجرامي المتمثل في نقل للبيانات والمعلومات الشخصية بدون تصريح فهي من الجرائم الشكلية ، أما بالنسبة للركن المعنوي فيشترط تحقق القصد الجنائي باعتبارها من الجرائم العمدية ، التي تشترط لقيامها توافر العلم بأنه يقوم بنقل بيانات ومعلومات بدون إذن وتصريح، بالإضافة إلى ذلك أن تكون الإرادة الحرة الواعية قد اتجهت إلى تحقق السلوك الإجرامي المكون للركن المادي لهذه الجريمة.

ت- أن يتم تشويه المعلومة أو البرامج بتعديل البيانات الشخصية أو تعديل طرق معالجتها أو وسائل انتقالها بحيث يجعلها غير صالحها للاستخدام الذي أنشئت من أجله. ويقصد بالتعديل غير المشروع للبيانات والمعلومات المبرمجة آلياً بأنه كل تغيير غير مشروع للمعلومات والبيانات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب

الآلي([1]). وبناء على ذلك فقد نص المشرع الانجليزي في المادة ١٧ من قانون إساءة استخدام الحاسب الآلي على أن يعاقب على كل فعل من شانه أن يؤدي إلى تعديل المعلومات والبيانات الشخصية غير المصرح به سواء أكان التعديل بشكل دائم أو مؤقت.

ويترتب على ذلك أن الإتلاف بالمعنى القانوني يكون متوافر متى كانت المعلومات والبرامج محل الاتلاف هي هدف الجاني، بقصد الاضرار بالغير أي دون اتجاه إرادة الجاني إلى ارتكاب جريمة أخرى. ومن التطبيقات القضائية على ذلك ما ذهبت اليه محكمة الاستئناف الفرنسية بإدانة متهم بالجنحة الواردة ضمن المادة ٣٢٣ – ٣ من قانون العقوبات الفرنسي، لقيامه بتعديل البيانات التي سبق وأن سجلها بطريقة نهائية على نظام آلي للمحاسبة. وقد أيدت محكمة النقض الفرنسية في قرارها في ٨ ديسمبر ١٩٩٩، واقعة التعديل أو الالغاء العمدي لبيانات شخصية يحتوي عليها نظام معالجة آلية بالمخالفة للوائح المطبقة والتي استخلصتها محكمة الاستئناف، وقد يستهدف من هذا الاتلاف ارتكاب أفعال أخرى أضافة لجريمة الاتلاف ، كتكييف واقعة قيام محاسب بمحو بيانات ومعلومات معالجة آليا تخص احدى الشركات على انها تشكل نصب معلوماتي، اذ اعتبر المحو وقع بهدف النصب، رغم انه ركن مادي للإتلاف، كما قد يأخذ الإتلاف صورة التزوير، واختلاس أموال مثل الطلبات المزورة المقدمة عن طريق الانترنت إلى شركات لطلب البضائع بالتلاعب بتعديل المعلومات والبيانات. وكذلك من ضمن صور تلك الاعتداءات الإلكترونية ما يسمى بتدمير المواقع ويقصد به الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام الآلي أو مجموعة نظم مترابطة شبكياً بالإنترنت بهدف تخريب نقطة الاتصال

([1]) – د. نائلة عادل فريد قورة ، جرائم الحاسب الاقتصادية ، دراسة نظرية تطبيقية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ ، ص ٢٢٠.

أو النظام. ومن الاعتداءات أيضا إغراق البريد الإلكتروني، وفيروسات الحاسب الآلي وغير ذلك من صور الاعتداءات التي يترتب عليها إتلاف البيانات الشخصية المعالجة إلكترونياً (١)، مما يشكل انتهاكاً للخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

وبناء على ما سبق فقد قام المشرع الفرنسي في ٢٤ يوليه ٢٠١٥ بإصدار القانون رقم ٥١٢ لسنة ٢٠١٥ لتعديل نص المادة ٣٢٣ -٢ من قانون العقوبات الفرنسي بحيث أصبحت تنص على انه يعاقب المشرع على كل فعل يعرقل أو يعطل نظم المعالجة الآلية للبيانات بالسجن لمدة لا تزيد عن خمس سنوات وبالغرامة المالية التي لا تزيد مقدارها عن ١٥.٠٠٠ ألف يورو. ويشدد المشرع الفرنسي العقوبة لتصل إلى السجن مدة لا تزيد عن سبع سنوات والغرامة المالية التي لا تزيد مقدارها عن ٣٠.٠٠٠ ألف يورو إذا وقع الاعتداء على نظم المعالجة الآلية للبيانات الشخصية التي تدار بواسطة الدولة. كأن يتم عرقلة أو تعطيل نظم المعالجة الآلية للبيانات عن طريق إدخال الجاني لبرامج ضارة أو فيروسات داخل تلك النظم مما يترتب عليه إعاقة عملها.

أما بالنسبة لموقف المشرع الأمريكي فقد عقد مؤتمر في جامعة ستانفورد في ولاية كاليفورينا بالولايات المتحدة الأمريكية عام ١٩٩٩ للموافقة على اتفاقية تعزيز الحماية من الارهاب وجرائم الحاسب الآلي. وتضمنت الاتفاقية في المادة ٣ منها الجرائم المعلوماتية ومن بينها جريمة التعديل والحذف للبيانات بهدف الاضرار بالمؤسسات التي تملك هذه الخدمات أو حذف البيانات بتغييرها لإعطاء معلومات كاذبة بهدف ايقاع

(١) – حسن طاهر داود ، جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم الأمنية ، مركز الدراسات والبحوث ، الرياض ، ٢٠٠٠ ، ص ٢٣.

اضرار مادية([1]). وبالتالي الإتلاف لنظام معالجة البيانات والمعلومات الشخصية الإلكترونية.

المطلب الثاني. صور الإتلاف للبيانات الشخصية الإلكترونية

وفي واقع الأمر تتنوع صور إتلاف للبيانات والمعلومات الشخصية المعالجة إلكترونياً بحسب ما إذا اتخذت صورة التدخل في البيانات، أو اتخذت صورة التدخل في الكيان المنطقي:

أ. التدخل في البيانات والمعلومات الشخصية المعالجة إلكترونياً:

فالبيانات الشخصية تمثل المعلومات المدخلة في النظام الآلي للحاسب بغرض معالجتها، ويتم التدخل فيها أما بإدخال معلومات وبيانات وهمية في النظام المعلوماتي أو بتزوير البيانات والمعلومات الموجودة فيه. والتغيير والتبديل الذي يقع على البيانات والاوامر المخزنة والمنقولة عبر شبكة الانترنت لا ينطبق عليه نصوص التزوير التقليدية إلا إذا اخرجت في صورة محرر مكتوب، ومن أجل ذلك ظهر تيار قوي ينادي بالمساواة بين مستند ورقي ومستخرجات الحاسب الآلي من اجل المعاقبة على هذه الصورة.

ب. التدخل في الكيان المنطقي للبيانات والمعلومات الشخصية المعالجة إلكترونياً:

ويقصد بالتدخل في الكيان المنطقي للبيانات والمعلومات المعالجة إلكترونياً بانه مجموعة البرامج المخصصة للقيام بالمعالجة للبيانات والمعلومات الشخصية عن طريق الحاسب الآلي، ويتم ذلك أما بتعديل البرنامج أو خلق برنامج جديد مما يدمر أو يعطل نظم معالجة البيانات أو المعلومات الشخصية. ولذلك فقد ظهرت الحاجة في القانون الإنجليزي لوضع تجريم خاص بالإتلاف المعلومات بعد قضية Cox. V. Riley وما

([1]) – الاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والانترنت ديسمبر ١٩٩٩ ، ولاية كاليفورنيا ، الولايات المتحدة الامريكية. انظر: د. محروس نصار غايب ، الجريمة المعلوماتية ، in formational crime ، المعد التقني ، الانبار ، العراق ، ٢٠١١ ، ص ٢٣.

أثارته من شك حول مدى صلاحية الاتجاه الذي اتخذته المحكمة في تطبيق النصوص التقليدية على الإتلاف للمعلومات أو البيانات بقانون الإتلاف الصادر في عام ١٩٧١. ولتفادي هذه الاختلافات تبنى المشرع الانجليزي في المادة الثالثة من قانون إساءة استخدام الحاسبات الآلية الصادر في عام ١٩٩٠ نص واضح لتجريم هذا السلوك الإجرامي ، فتنص الفقرة الأولى منه على أن يعد مرتكباً لجريمة الإتلاف المعلوماتي كل من يقوم بعمل من شأنه إحداث تغييرات غير مصرح بها في محتوى أي حاسب آلي متى توافر القصد الجنائي بعنصريه العلم والإرادة وقت قيامه بهذا الفعل([1]). وبالتالي يتضح أن المشرع الانجليزي يجرم كل سلوك إجرامي يعتبر تدخل في الكيان المنطقي لنظم معالجة البيانات أو المعلومات الشخصية مما يضر بحق الاشخاص في خصوصية بياناتهم أو معلوماتهم الشخصية التي تم معالجتها إلكترونياً.

ج. تعديل البرنامج المتعلقة بالبيانات والمعلومات الشخصية المعالجة إلكترونياً:

يعد البرنامج كيانا ماديا، له أصل ومولد صادر عنه، يمكن رؤيته على شاشة الحاسب الآلي كترجمة إلى أفكار كما يمكن الاستحواذ عليه عن طريق تشغيله في الحاسب الآلي ويتجسد في احدى الصور التالية:

الصورة الأولى. التلاعب في البرنامج المتعلقة بالبيانات والمعلومات الشخصية المعالجة إلكترونياً:

ويقصد بالتلاعب في البرنامج الخاص بالبيانات أو المعلومات الشخصية المعالجة إلكترونياً كل فعل من شأنه أن يؤدي إلى اختفاء البيانات أو المعلومات الشخصية كليا أو جزئيا كما هو الحال. وتطبيقاً على ذلك أحكام القضاء الانجليزي وفقا لنص المادة

([1]) – د. كامل السعيد ، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا ، المؤتمر السادس للجمعية المصرية للقانون الجنائي ، ٢٥ – ٢٨ أكتوبر ١٩٩٣ ، دار النهضة العربية ، القاهرة ، ١٩٩٣ ، ص ٣٤٢ وما بعدها.

الثالثة من قانون إساءة استخدام الحاسب الآلي في قضية Pile التي عرضت على محكمة اكستر في ١٥ نوفمبر ١٩٩٥ حيث اشتهر الجاني بأنه هو البارون الأسود لنشاطاته المتعلقة بالأتلاف المعلوماتي والبيانات(١)، فقد أدين بخمسة تهم من بينها إحداثه تعديلات في نظم وبرنامج المعلومات والبيانات بقيامه ببث ونشر فيروس أطلق عليه أسم Pathogen وآخر أطلق عليه Queeg، وهو الأمر الذي أدي إلى إلحاق أضرار كبيرة بالشركات المتصلة بشبكة المعلومات ، وذكر القاضي الذي نظر الدعوى بأنه يجب أخذ هؤلاء الأشخاص الذين يسعون في انتهاك وإضعاف نظم المعلومات بالشدة والحزم نظراً لما تمثله أفعالهم من خطورة على تكنولوجيا المعلومات والبيانات وخصوصياته.

الصورة الثانية. اختلاس نتائج الحاسب الآلي المتعلقة بالبيانات والمعلومات الشخصية المعالجة إلكترونياً:

ويتم ذلك بإعادة نسخ البيانات والمعلومات الشخصية المعالجة إلكترونياً عن بعد أو عن طريق النقل الإلكتروني للبيانات، وذلك باتباع أسلوب التجسس المعلوماتي عن طريق بث برامج خاصة بالتقاط البيانات المتبادلة عبر الشبكة. وقد نصت المادة ٢٥ من المبادئ الأوربية الخاصة بحماية البيانات الشخصية على أن أي نقل للبيانات الشخصية التي تعالج أو التي ستعالج بعد نقلها يجب أن تحصل على مستوي كاف من الحماية من جانب النطاق القضائي الذي ترسل إليه. وإن مدى كفاية الحماية يقيم بالرجوع إلى طبيعة البيانات، والغرض ومدة المعالجة المقترحة، وبلد المنشأ والمقصد النهائي، والنظام العام أو نظام القطاع في الولاية القضائية المعنية، وطبيعة ونطاق الإجراءات الأمنية.

---

(١) – R.V. SIMBA, Crime, ١٩٩٥, LR ٦٨.

الصورة الثالثة. تغيير نظام التشغيل لبرامج البيانات والمعلومات الشخصية المعالجة إلكترونياً:

ويقصد بذلك كل فعل من شأنه أن يؤدي إلى تزوير في برنامج نظام التشغيل للبيانات والمعلومات الشخصية المعالجة إلكترونياً بمجموعة تعليمات اضافية يسهل الوصول اليها بواسطة كلمة السر أو مفتاح الشفرة واداة الربط، بحيث تتيح الوصول إلى جميع البيانات الموجودة بالجهاز الآلي، مما يشكل انتهاكا للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

د. كيفية إتلاف البرنامج المتعلقة بالبيانات والمعلومات الشخصية المعالجة إلكترونياً:

تتم عملية الإتلاف للبرامج المتعلقة بالبيانات والمعلومات الشخصية بطريقة فنية وتقنية متنوعة منها الفيروسات مرورا بالبرامج الدودة وأخيرا القنبلة المنطقية أو الزمنية، ويتفق الفقهاء في انجلترا والولايات المتحدة على أن المشكلات القانونية التي تنشأ عن جميع الفيروسات تكون غالبا واحدة، فلا وجه للتفرقة بين الفيروس والدودة وحصان طروادة لأنها ترتب نفس الاثار. طالما قام الشخص بارتكاب السلوك الإجرامي المكون لهذه الجريمة بالإضافة إلى توافر القصد الجنائي الخاص بالإتلاف أو التعطيل نظم معالجة البيانات والمعلومات الشخصية الإلكترونية على اعتبار أن هذه الجريمة من الجرائم العمدية التي تتطلب توافر القصد الجنائي العام. بالإضافة إلى ذلك تنص بعض التشريعات إلى ضرورة توافر قصد جنائي خاص وهو أن يتجه نية الجاني إلى الإضرار بالغير أو إلى تحقيق ربح غير مشروع له أو للغير، كما نص على ذلك المشرع الفرنسي في قانون العقوبات بالمواد ٣٢٣- ٢، ٣.

وعليه يمكن تحدد الصور التي يتم من خلالها الإتلاف للبرامج ونظم البيانات والمعلومات الشخصية التي تم معالجتها إلكترونياً وذلك على النحو التالي:

أ. من خلال اتلاف سجلات الخوادم والكوكيز، حيث أن سجلات الخوادم التي تحتفظ بأرقام IP الخاصة بالحاسب الآلي للمستخدمين الذين اتصلوا بهذه الخوادم والكوكيز التي تحتفظ بها مواقع الويب أي الانترنت في العادة لتسهيل التصفح وحفظ تفضيلات ومعلومات المستخدم مما يشكل انتهاك للخصوصية.

ب. فيروسات الحاسب الآلي : يقصد بفيروسات الحاسب الآلي بانها برامج يتم تسجيلها أو زرعها في داخل أجهزة الحاسب الآلي، فيظل خامل لفترة ما ثم بعد ذلك ينشط ليدمر المعلومات والبيانات المخزنة أو يتلفها أو يعرقل نظم المعالج لها عن أداء وظيفتها([1]) أي أنها في الحقيقة عبارة عن برامج خبيثة تتسلل إلى البرمجيات فتدخل اليها وتنسخ نفسها على برامج أخرى، عبر كامل الحاسب الآلي، وقد تستعمل لحماية البيانات والبرامج، من خطر النسخ غير المشروع، ولها هدف تخريبي عندما تستعمل للدعاية أو الابتزاز، وتنشط هذه الفيروسات عند نسخ البرنامج من حاسب لآخر أو نقل المعلومات عبر شبكة الانترنت وتكون مخبأة داخل الرسائل الالكترونية والوثائق والمعلومات التجارية والمالية. وكان أول ظهور للبرامج الخبيثة كان فيرس Brain عام ١٩٨٦، ولكن مع التطور ظهر الالاف من هذه البرامج الخبيثة، من أمثلتها الفيروسات وأحصنة طروادة، وتمكن خطورة هذه البرامج على خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً في أنها تصيب أنظمة التشغيل بالعطب أو تقوم بحذف ملفات وبيانات أو يكون هدفها اختراق بيانات ومعلومات الضحية المخزنة على الإنترنت أو الحاسب الآلي واستغلالها بطريقة غير مشروعة([2])، مما تشكل معه خطورة كبيرة على خصوصية هذه البيانات الشخصية التي تم معالجتها إلكترونياً.

([1]) – د. هدي حامد قشقوش ، الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني ، مؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون ، جامعة الأمارات العربية المتحدة ، ٢٠٠٠ ، ص ١٣.

([2]) – مثال على ذلك ما يسمى بالدودة الحمراء ، حيث استطاعت خلال أقل من تسع ساعات من اقتحام ما يقرب من ربع مليون جهاز في ١٩ يوليو ٢٠٠١ ، وتدمير واتلاف البيانات الشخصية الإلكترونية الموجودة عليه.

ج. البرامج الخبيثة: هي برامج ضارة يمكنها أن تلحق ضررا بنظام التشغيل أو الاضطلاع على البيانات الشخصية المعالجة إلكترونياً الموجودة بالجهاز المصاب ومن أمثلتها الفيروسات، وأحصنة طروادة التي تمكن الجاني من الاطلاع واتلاف المعلومات والبيانات الشخصية التي تم معالجتها إلكترونياً.

د. الفيروسات المعلوماتية: وهي أحدى أنواع البرامج المخصصة للتعامل مع أجهزة الحاسب الآلي، والتي تتكون من مجموعة من الأوامر، إلا أن تلك الأوامر المكتوبة في هذه البرامج تقتصر على أوامر الغرض منها تخريبي والإضرار بالجهاز ومحتوياته من البيانات والمعلومات الشخصية المعالجة إلكترونياً، فيمكن عند كتابة كلمة أو أمر ما أو حتي مجرد فتح البرنامج الحامل للفيروس أو الرسالة البريدية المرسل معها الفيروس إصابة الجهاز به، ومن ثم يقوم الفيروس بمحو أو إتلاف أو تعطيل محتويات الجهاز من البيانات والمعلومات وخاصة البيانات والمعلومات الشخصية([1]) التي تم معالجتها إلكترونياً.

هـ. رسائل التصيد pushing: ويقصد بها كل رسائل تحتوي على روابط مزيفة، تحاول الحصول بمجرد الدخول على هذه الروابط الحصول على المعلومات والبيانات الشخصية، وبالتالي الاعتداء عليها مما يشكل انتهاك لخصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

([1]) – د. أيمن عبدالله فكري ، الجرائم المعلوماتية ، دراسة مقارنة في التشريعات العربية والأجنبية ، الطبعة الأولى ، مكتبة القانون والاقتصاد ، الرياض ، ٢٠١٥ ، ص ١٧٠ ، ١٧١.

و. برامج الدودة: ويقصد ببرامج الدودة تلك البرامج التي تشغل الفراغ الموجود في نظم التشغيل بحيث تنتقل من حاسب لأخر وشبكة لأخرى عبر الوصلات التي تربط بينها، ثم بعد ذلك تتكاثر أثناء عمليات الانتقال، بحيث تعمل على خفض كفاءة الشبكة، والتخريب الفعلي للملفات والبرامج من خلال ملئها لأي حيز من الشبكة. ومثال على ذلك إطلاق دودة الانترنت من قبل طالب امريكي " روبرت موريس " بجامعة علوم الكمبيوتر – كورنيل– لأثبات عدم ملائمة اساليب الأمان المستعملة، فتسبب في تدمير الاف من شبكات الاعلام الآلي المنتشرة في الولايات المتحدة الأمريكية وخسائر مالية معتبرة لمواجهة دودة الانترنت، وقد أدين من أجل ذلك بانتهاك قانون الاحتيال واساءة استخدام الكمبيوتر وعوقب بثلاث سنوات حبس والعمل لأربعمائة ساعة في الخدمة الاجتماعية وبالغرامة المالية التي تبلغ مقدارها ١٠.٥٠٠ دولار أمريكي.

أما بالنسبة لموقف المشرع المصري فنجد أن المادة ٧٥ من القانون رقم ١٣٤ لسنة ١٩٩٤ بشأن الأحوال المدنية تنص "على جريمة التعطيل أو الإتلاف غير العمدي للشبكة الناقلة لمعلومات الأحوال المدنية أو جزء منها بحيث يعاقب بالحبس مدة لا تجاوز ستة أشهر وغرامة لا تقل عن مائتي جنيه ولا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية أو جزء منها وكان ذلك ناشئ عن إهماله أو رعونته أو عدم احترازه أو عدم مراعاته للقوانين واللوائح والأنظمة. ويشدد العقاب في حالة إذا ما وقع الفعل عمدا بحيث تكون العقوبة السجن مع عدم الإخلال بحق التعويض في الحالتين".

ونستخلص من ذلك أن المشرع المصري قد نص على تجريم هذه الأفعال سواء كانت في صورة الخطأ بحيث يقع الإتلاف أو التعطيل نتيجة الإهمال أو الرعونة أو عدم الاحتراز أو عدم مراعاة القوانين واللوائح والأنظمة ، أو كانت في صورة العمد

بتوافر القصد الجنائي أي أن يكون الشخص يعلم بانه يقوم بسلوك إجرامي يترتب عليه إتلاف أو تعطيل الشبكة الناقلة للبيانات والمعلومات الشخصية الخاصة بالأحوال المدنية، مع اتجاه إرادته الحرة الواعية إلى القيام بذلك السلوك الإجرامي، وقد اعتبر المشرع المصري توافر القصد الجنائي واعتبار الجريمة من الجرائم العمدية ظرف مشدد للعقاب يجعل الجريمة معاقبة عليها بعقوبة السجن بدلاً من العقوبة البسيطة في حالة الخطأ وهي الحبس لمدة لا تزيد عن ستة أشهر وغرامة لا تقل عن مائتي جنية ولا تزيد عن خمسمائة جنية أو بإحدى هاتين العقوبتين، وفي جميع الأحوال يلزم الشخص بدفع التعويض اللازم لإصلاح الضرر المترتب على الجريمة في الحالتين.

ويتبين لنا مما سبق أن المشرع المصري يجرم الإتلاف أو التعطيل للشبكات الناقلة للبيانات والمعلومات الشخصية الموجودة على أجهزة الحاسب الآلي الخاصة بمصلحة الأحوال المدنية فقط ولا يمتد التجريم إلى غيرها من البيانات والمعلومات الشخصية الموجودة على أجهزة الحاسب الآلي الشخصي أو الخاص بالمؤسسات والهيئات والشركات العامة أو الخاصة. وكذلك لا تمتد الحماية الجنائية للبيانات الشخصية التي تم معالجتها إلكترونياً سواء كانت على شبكة الإنترنت أو على وسيلة أو دعامة إلكترونية وهذه ثغرة خطيرة يجب على المشرع المصري تداركه لخطورة هذه الأفعال الإجرامية على الأمن القومي والاجتماعي والاقتصادي.

وبالإضافة إلى ما سبق فقد نص المشرع المصري في المادة ٢٣ من القانون رقم ١٥ لسنة ٢٠٠٤ الخاص بالتوقيع الإلكتروني على تجريم إتلاف التوقيع الإلكتروني حماية للبيانات الشخصية المتعلقة بالتوقيع الإلكتروني للشخص(١)، حيث نصت المادة على

(١) – وقد نصت المادة الأولى من قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤ على مصطلح التوقيع الإلكتروني ويقصد به كل ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون لها طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره.

"أن مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر ، يعاقب بالحبس وبالغرامة المالية التي لا تقل عن عشرة آلاف جنية ولا تجاوز مائة ألف جنية أو بإحدى هاتين العقوبتين كل من: ... ب. أتلف أو عيب توقيعاً أو وسيطاً أو محرر إلكترونياً، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر. وفي حالة العود تزداد العقوبة بمقدر المثل في حديها الأدنى والأقصى، وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وكذلك ينشر على شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه".

وكذلك فقد نص المشرع المصري على معاقبة المسئول عن الإدارة الفعلية في حالة إتلاف التوقيع الإلكتروني، فنصت المادة ٢٤ الفقرة الأولي من قانون التوقيع الإلكتروني على أنه "يعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك". كما قرر المشرع المصري في المادة ٢٤ الفقرة الثانية من قانون التوقيع الإلكتروني مسئولية الشخص الاعتباري بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد ارتكبت من أحد العاملين به باسم ولصالح الشخص الاعتبار. ولكن يظل موقف المشرع المصري محل انتقاد في عدم النص على الحماية الجنائية لخصوصية البيانات الشخصية التي تم معالجتها إلكترونيا أي كان نوعها.

بالإضافة إلى ذلك فقد نص المشرع المصري في المادة ١٧ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على أن يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز خمسمائة ألف جنية، أو بإحدى

هاتين العقوبتين، "كل من أتلف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أياً كانت الوسيلة التي استخدمت في الجريمة". وبناء على ذلك يتضح أن المشرع المصري نص على حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونيا من التعرض العمدي بدون وجه حق لها بالإتلاف أو التعطيل أو التعديل أو إلغاء لمسارها سواء تم ذلك بصورة كليه أو جزئية، وأياً كانت الوسيلة المستخدمة في ارتكاب الجريمة.

أما بالنسبة لحماية البيانات والمعلومات الشخصية في المرحلة السابقة على المعالجة الإلكترونية لهذه للبيانات والمعلومات الشخصية، فقد نص المشرع المصري في المادة ٢٢ من نفس القانون على "أن يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة جنية ولا تجاوز خمسمائة ألف جنية ، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة ، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أي جريمة من الجرائم المنصوص عليها في هذ القانون ، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام او التسهيل أو الإخفاء. ويتضح من ذلك أن المشرع المصري قد نص على حماية المرحلة السابقة على المعالجة للبيانات الشخصية من خلال تجريم حيازة أو أحراز أو جلب أو باع أو اتاح أو صنع أو أنتج أو استورد او صدر أو تداول أي أجهزة أو معدات أو أدوات أو برامج من شأنه أن تستخدم في الاعتداء على خصوصية البيانات والمعلومات الشخصية التي تم معالجتها أو سوف يتم معالجتها إلكترونياً".

المبحث الرابع. جريمة الإعلانات التسويقية الإلكترونية غير المرغوب فيها من خلال استخدام البيانات الشخصية

مما لا شك فيه أنه لا يسمح في الأصل باستخدام أنظمة الاتصال الآلي دون تدخل بشري أي آلات الاتصال الدولي أو آلات الفاكس أو البريد الإلكتروني لأغراض التسوق المباشر إلا فيما يتعلق بالمشتركين الذين قدموا موافقتهم المسبقة. أما في حالة حصول شخص طبيعي أو اعتباري من عملائه على معلومات شخصية من خلال الاتصال الإلكتروني مثل استخدام البريد الإلكتروني، في سياق بيع منتج أو خدمة، أو الشخص الاعتباري استخدام تفاصيل الاتصالات الإلكترونية هذه للتسويق المباشر لمنتجاتها أو خدماتها المماثلة، شريطة أن تتاح للعملاء بوضوح وبشكل مميز فرصة الاعتراض مجانا وبطريق سهلة على استخدام البيانات الشخصية في الاتصالات الإلكترونية عندما يتم جمعها وبمناسبة كل رسالة في حالة العميل الذي لم يرفض في البداية مثل هذا الاستخدام.

وعليه يشكل الإنترنت تحدياً جديد فيما يتعلق بحماية الحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً خاصة في مجال التسوق الإلكتروني، حيث يهيئ فرص للاستخدام التجاري للبيانات الشخصية المعالجة إلكترونياً، حيث إن الكثير من الخدمات التي تقدمها هذه الشركات هي خدمات مجانية، ولكن في نفس الوقت تعتمد نماذج أعمالها على جمع معلومات المستخدم للإنترنت، واستخدامها في أغراض التسويق التجاري من خلال الإعلان والاتصالات غير المرغوبة التسويقية. وبناء على ذلك فقد نص المشرع الاوربي على التزام الدول الاعضاء باتخاذ التدابير المناسبة التي تكفل

بعدم السماح بالاتصالات غير المرغوبة لأغراض التسويق المباشر دون موافقة المشتركين المعنيين([١]). كذلك مواجهة حالات ارسال البريد الإلكتروني لأغراض التسويق المباشر عن طريق التمويه أي إخفاء هوية المرسل الذي يجري الاتصال، أو أن يكون الاتصال بدون عنوان صحيح يمكن للمستلم أن يرسل إليه طلباً بوقف هذه الرسائل.

وسوف نتناول في هذا المطلب توضيح ماهية الإعلانات التسويقية الإلكترونية الموجهة في المطلب الاول، وفي المطلب الثاني نستعرض أنواع الإعلانات التسويقية الإلكترونية الموجهة، وفي المطلب الثالث نتناول بالعرض لموقف التشريعات المقارنة من جريمة الإعلانات التسويقية الإلكترونية غير المرغوب فيها.

المطلب الأول. ماهية الاعلانات التسويقية الإلكترونية الموجهة

في واقع الأمر أن الإعلانات التسويقية الإلكترونية الموجهة تعتمد بالأساس على تقنية تقوم على بمسح تاريخ المواقع والروابط الإلكترونية التي يقوم المستخدم بزيارتها وتحليلها للوصول لصورة قريبة من الميول الاستهلاكية للمستخدم، وبالتالي استخدامها في ارسال الإعلانات التسويقية من خلال رسائل إلكترونية غير مرغوب فيها، مما يشكل انتهاك للحق في خصوصية البيانات الشخصية التي يتم استخدامها تجارياً بدون وجه حق.

ولذلك فقد نص المشرع المصري في المادة الأولى من قانون حماية البيانات الشخصية على تعريف التسويق الإلكتروني([٢]) "بأنه إرسال أي رسالة أو بيان أو محتوى إعلاني

([١]) – المادة ١٣ من الأمر التوجيهي المتعلق بالخصوصية والاتصالات الإلكترونية رقم ٥٨ لسنة ٢٠٠٢ ، الصادر عن الاتحاد الأوربي بتاريخ ١٢ يوليو ٢٠٠٢ بشأن تجهيز البيانات الشخصية وحماية خصوصية في قطاع الاتصالات الإلكترونية.

([٢]) – المادة الأولى من القانون المصري بشأن حماية خصوصية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

أو تسويقي بأي وسيلة تقنية أيًا كانت طبيعتها أو صورتها تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو التماسات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلى أشخاص بعينهم". ويقصد بالرسائل غير المرغوب فيها([1]) بأنها الرسائل التي تتم بوسيلة إلكترونية وتوجه إلى شخص أو إلى مجموعة من الأشخاص بدون تمييز وبغير طلب من جانبهم، بل وبدون موافقتهم([2]).مما تشكل معه إخلالا بالحق في خصوصية المعلومات والبيانات الشخصية المعالجة إلكترونياً. أما بالنسبة للجنة القومية للمعلومات والحريات الفرنسية CNIL فقد عرفت الرسائل الدعائية بأنها هي عملية إرسال مكثف أو مكرر لنفس الرسائل غير المرغوب فيها، لأشخاص لم يتعامل معهم المرسل من قبل ولم يطلبوا منه هذه الرسائل التي تم إرسالها.

وفي واقع الأمر فان الطابع الغالب من الرسائل الإلكترونية غير المرغوبة هي الإعلانات التجارية كالإعلان والدعاية لمنتج أو لخدمة جديدة، أو تروج لأفكار دينيه متطرفة أو تدعو للإباحة والجنس. وتتم هذه العملية من خلال استخدام برامج تقوم بالتقاط العناوين التي تمر عبر شبكة الإنترنت، ثم يتم بعد ذلك عملية الارسال للإعلانات التسويقية. وانطلاقا مما سبق نستطيع القول بأن الإعلانات التسويقية الإلكترونية الموجهة بانها نمط من الإعلانات التي تعتمد على تتبع نشاط المستخدم للإنترنت عن طريق مسح وتحليل البيانات والمعلومات الإلكترونية الخاصة به، وذلك لوضع وإرسال الإعلانات التسويقية على المواقع أو البريد الإلكتروني للشخص للمستهدف أو من خلال الاتصال الهاتفي، وذلك لتحقيق أغراض تجارية محددة من خلال تسويق البيانات

([1]) – E. MAILJINK BULK, Spamming, pollupostage, porriel, www.traidnt.net, ٢٠١٣.

([2]) – د. زينب غريب ، النظام القانوني للبريد الإلكتروني ، رسالة دكتوراه ، الطبعة الأولى ، طوب بريس ، الرباط ، ٢٠١٦ ، ص ٦٤.

الشخصية الإلكترونية للمستخدم، باعتبارها مورد هام للإعلانات(١). مما يشكل انتهاك للحق ي خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، وذلك لان الإعلانات التسويقية الموجه تتم عن طريق أنشاء ملفات شخصية منتظمة لمستخدمي الإنترنت عن غير إرادة منهم، وبعد ذلك يتم التعامل على الملفات الشخصية للمستخدمين باعتبارها سلعة تجارية بين موردي البيانات والمعلومات الشخص مثل مواقع التواصل الاجتماعي الفيسبوك والتوتير والإنستجرام وغيرها وبين المعلنين. مما يشكل انتهاك واضح للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونيا.

وعليه فقد عبر عن هذه المخاطر كلا من Jerry BERMAN و Deirdre MULLIGAN بالقول بأن تصور أنك تسير في أحد مخازن الأسواق بين مخازن عديدة لا تعرف أيا منها ، فتوضع على ظهرك إشارة تبين كل محل زرته وما الذي قمت به وما اشتريته، إن هذا شيء شبيه لما يمكن أن يحصل في بيئة الإنترنت(٢). فعندما يستخدم الأشخاص الانترنت ووسائل التواصل الاجتماعي الإلكترونية يتوقعون قدار من الخصوصية في نشاطهم، فحتي ولو لم يكشفوا عن بياناتهم الخاصة ولكن الإنترنت وعبر خوادم ونظم إدارة الشبكات لملفات الارتباط تحصل على معلومات وبيانات عن كل وقفة وكل شير أو أعجاب في فضاء شبكات الانترنت، وهذه البيانات يتم تجميعها وتحليلها لتقدم سلوكيات وصورة عن الشخص لم يرد كشف أي من تفاصيلها مما يشكل انتهاك وضح للحق في خصوصية البيانات الشخصية المعالجة إلكترونياً.

---

(١) – د. أشرف جابر ، استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصية ، مجلة العلوم الإنسانية ، جامعة الإخوة منتوري ، قسنطينة ، الجزائر ، عدد خاص ٢٠١٥، ص ٩.

(٢) – Jerry BERMAN & Deirdre MULLIGAN, Privacy in the digital age : work in progress, Nova law review, Vol ٢٣, N°٢, winter ١٩٩٩, The internet and law, p. ٤.

وتأسيسا على ذلك يجب اتخاذ تدابير وقائية لمنع وصول هذه الاعلانات التي تنتهك الحق في خصوصية البيانات والمعلومات الشخصية، ومنها أن يتم استحداث خاصية جديدة تسمح باستخدام بوابات البريد الإلكتروني لمسح جميع رسائل البريد الإلكتروني الواردة. بالإضافة إلى ذلك أن يتم تأمين قوائم توزيع البريد الإلكتروني الداخلية لمنع وصول الأطراف الخارجية إلى المعلومات والبيانات الشخصية من أجل الحد من مخاطر رسائل البريد الإلكترونية غير المرغوب فيها.

المطلب الثاني. أنواع الإعلانات التسويقية الإلكترونية الموجهة

تتعدد أنواع الإعلانات التسويقية الإلكترونية الموجهة ، ففي التقرير الصادر في ٢٦ مارس ٢٠٠٩ عن اللجنة القومية للمعلوماتية والحريات الفرنسية CNIL بشأن الاعلانات التسويقية عبر الانترنت تم تقسيمها إلى ثلاث أنواع وذلك على النحو التالي([1]):

النوع الأول. الإعلانات التسويقية الإلكترونية الشخصية.

النوع الثاني. الإعلانات التسويقية الإلكترونية الموضوعية.

النوع الثالث. الإعلانات التسويقية الإلكترونية السلوكية.

الفرع الاول. الإعلانات التسويقية الإلكترونية الشخصية

تعتبر الإعلانات التسويقية الإلكترونية الشخصية النوع التقليدي للإعلانات الموجهة التسويقية، والأكثر انتشاراً على مواقع التواصل الاجتماعي، ويقصد بها الإعلان الذي يكون موجه إلى المستخدم الإنترنت من خلال المعلومات والبيانات الشخصية المتوافرة عنه على مواقع التواصل الاجتماعي وصفحات الانترنت، والتي يقدمها المستخدم نفسه عند التسجيل في أي خدمة من الخدمات الموجودة على الانترنت مثل الاسم والسن والجنس والعنوان والبريد الإلكتروني ورقم التليفون بل تشمل كذلك معلومات وبيانات

([1]) – اللجنة القومية الفرنسية للمعلوماتية والحريات ، التقرير الخاص بالإعلانات التسويقية عبر الإنترنت ، الصادر في ٢٦ مارس ٢٠٠٩. www.cnil.fr.

CNL, Rapport du ٩ février ٢٠٠٩, La publicité ciblée en ligne, de la CNIL, P.٢٦.

شخصية عن الطابع الشخصي مثل المعتقدات والاهتمامات والهويات وغيرها التي يعتقد الانسان عدم أهميتها إلا انها تمثل تعبير عن ما يحبه الانسان ويثر انتباه.

وبناء على ذلك فهناك تطبيقات إلكترونية تراقب ميكروفون الهواتف الذكية عن طريق الميكروفونات الموجودة بهذه الأجهزة، بحيث تحتوي تلك التطبيقات على تقنية تتعرف على الصوت حتى عند وضع الهاتف بالجيب، أو في أثناء عملها بالخلفية، ويستطيع المسوقون حينها استخدام تلك المعلومات للتعرف على مستهلكيهم بصورة أفضل وتوجيه إعلاناتهم بفاعلية أكبر. ومن أشهر هذه البرامج برنامج طورته شركة تدعى ألفونسو، حيث تقوم سراً بجمع بيانات عن عادات مشاهدي التلفاز وتبيعها للمسوقين. ويستخدم برنامج شركة ألفونسو الميكروفون الخاص بالهاتف للاستماع إلى البيئة المحيطة بالمستخدم، من أجل التعرف على ما يفضل مشاهدته في التلفاز من خلال عينات قصيرة المدة من ميكروفون جهازك. لكي يتم مقارن التوقيعات الصوتية بالمحتوي التجاري الجاري تشغيله على جهاز التلفاز الخاص، ويشمل ذلك أيضا المحتوي الذي يجمع من أجهزة الريسيفر، وأجهزة تشغيل الوسائط، وأجهزة تشغيل ألعاب الفيديو، وأجهزة البث الأخرى، وأي مصدر آخر للفيديو مثل برامج التلفاز وبرامج البث والإعلانات وغيرها، وفي حالة تطابق، يمكن لشركة ألفونسو استخدام تلك المعلومات في تقديم إعلانات أكثر ملائمة لجهاز الهاتف الخاص. ويتم ذلك من خلال برنامج ACR بمطابقة العينات مع المحتوي الصوتي التجاري المعروف.

وانطلاقا مما سلف فقد ظهرت مخاوف من أن أجهزة التلفزيونات الذكية يمكن أن تراقب مالكيها بادئ الأمر في ٢٠١٥، لذلك حذرت إحدى سياسات الخصوصية لشركة سامسونغ من أن كل بيانات التعرف الصوتي قد تمرر إلى طرف ثالث. وفي عام ٢٠١٧ صدر حكم في انجلترا بتغريم شركة Vizio ٢.٢ مليون دولار، لتتبعها عادات

المشاهدة الخاصة بالمستخدمين دون علمهم ومشاركة تلك المعلومات في المجال التسويقي، مما يشكل انتهاك للحق في خصوصية البيانات الشخصية التي تم معالجتها آلياً.

وبناء على ذلك فقد نص المشرع الفرنسي على تجريم التعدي على اللوائح التجارية من خلال استخدام آلات أو معدات للاعتداء على الخصوصية الشخصية فينص في المادة ٤ – R٦٢٣ من قانون العقوبات الفرنسي(١) على أن يعاقب كل شخص حصل على ترخيص بشأن الآلات أو المعدات التجارية التي تمس بالخصوصية ولم يقوم بالاحتفاظ بالسجل وفقا للقواعد المنصوص عليها في القانون بشكل يشكل اعتدي على الخصوصية بالغرامة المقررة للمخالفات من الدرجة الثالثة. أي استخدام أجهزة يمكن من خلالها التجسس على البيانات والمعلومات واستخدامها في مجال الاعلانات التسويقية مما يشكل اعتداء على خصوصية البيانات الشخصية.

الفرع الثاني. الإعلانات التسويقية الإلكترونية الموضوعية

يقصد بالإعلانات التسويقية الإلكترونية الموضوعية بانها إعلانات مرتبطة بالمحتوي أي يقصد بها كل الإعلانات التسويقية التي توجه إلى مستخدم الإنترنت بالنظر إلى المحتوي الإلكتروني الذي يقوم بالبحث عنه على مواقع الانترنت(٢)، وبالتالي ترسل إليه الإعلانات المتعلقة بالاهتمامات البحثية له على مواقع الإنترنت وذلك بتتبع

(١) – Code de droit pénal, l'article R٦٢٣ – ٤, Modifié par décret n°٢٠١٠ – ٦٧١ du ١٨ juin ٢٠١٠ – art. ٤.

(٢) – Car LEVIN & John MCCAIN, Majority and Minority, Online advertising and hidden hazards to consumer security and data privacy, Staff report, ١٥ May, ٢٠١٤, p. ١٧.

الاثر المتعلق ب IP المتعلق بالحاسب الآلي المستخدم في عمليات البحث على الإنترنت ، باستخدام ملفات تعريف الارتباط او ما يعرف بالكوكيز.

الفرع الثالث. الإعلانات التسويقية الإلكترونية السلوكية

يقصد بالإعلانات التسويقية الإلكترونية السلوكية بانها نوع من الإعلانات التي تجمع بين الإعلانات التسويقية الموضوعية خلال فترة زمنية سابقة، وذلك من خلال الجمع بين الإعلانات التي ترتبط بالسلوك السابق لمستخدم الإنترنت خلال فتره زمنية سابقة وبين ما تم جمعه من كلمات مفتاحية، وذلك دون النظر إلى أية بيانات أو معلومات شخصية متوافره عنه، كسنه أو جنسه أو اسمه أو عنوانه. ويقصد بالإعلانات التسويقية السلوكية بانها كل إعلان يوجه إلى مستخدم الإنترنت من خلال تتبع سلوكه عبر الإنترنت خلال فترة زمنية معينة، يتم فيها تحليل هذا السلوك وميوله واهتماماته من خلال زياراته المتتابعة على مواقع الإنترنت، وبناء على ذلك يتم تحديد الإعلانات المناسبة لاهتمامات مستخدم الإنترنت الشخصية.

المطلب الثالث. موقف التشريعات المقارنة من جريمة الإعلانات التسويقية الإلكترونية غير المرغوب فيها

في البداية نستعرض موقف المشرع الفرنسي الذي نص في المادة ٨ من قانون حماية البيانات الشخصية على انه يحظر جمع أو معالجة البيانات ذات الطابع الشخصي، والتي من شأنها ان تكشف، بشكل مباشر أو غير مباشر، عن الاصول

العرقية أو الآراء السياسية أو الفلسفة أو العقيدة الدينية أو الانتماء النقابي للشخص، أو تلك التي تتعلق بصحته أو بحياته الجنسية.

ونستخلص مما سبق أن المشرع الفرنسي قد وضع نص عام يحظر جمع البيانات الشخصية ولكن ليس هناك نص خاص يحظر جمع البيانات الشخصية الخاصة بمستخدم على الإنترنت، بل المحظور هو الجمع الذي يتم بطريقة غير مشروعة مثل التدليس أو ذلك الذي يتم بالرغم من اعتراض صاحب هذه البيانات الشخصية، ويعاقب على ذلك بالسجن لمدة لا تزيد عن خمس سنوات وبالغرامة المالية والتي لا تزيد مقدارها عن ٣٠٠.٠٠٠ ألف يورو، وذلك وفقا لنص المادة ٢٢٦ – ١٨ من قانون العقوبات الفرنسي.

بالإضافة إلى ذلك فقد نص المشرع الفرنسي في المادة ٣٢٣ – ٢ من قانون العقوبات على أن يعاقب بالسجن مدة لا تزيد عن خمس سنوات وبالغرامة المالية التي لا تزيد مقدرها عن ٧٥.٠٠٠ ألف يورو، كل فعل يترتب عليه إعاقة أو إفساد عمل نظام المعالجة الآلية للبيانات الشخصية. وتشدد العقوبة لتصبح السجن سبع سنوات وبالغرامة المالية التي لا تزيد مقدراها عن ١٠٠.٠٠٠ ألف يورو إذا كان هذا الاعتداء يمس نظام المعالجة الآلية للبيانات التي تملكها الدولة. ويتبين مما سبق أن المشرع الفرنسي يطبق هذه النصوص في حالة قيام مواقع التواصل الاجتماعي مثل الفيسبوك أو التوتير أو الانستجرام وغيرها بجمع وحفظ البيانات الشخصية للمستخدم(١)، أو أن

(١) – Sophie LOUVEAUX, Comment concilier le commerce électronique et la protection de la vie privée ? Droit des technologies de l'information. Regards prospectifs, sous la direction d'Etienne Montero, Cahier du centre de recherché informatique et droit, Bruylant, Bruxelles, ١٩٩٩, PP. ١٥١ – ١٥٢.

يتم إعاقة أو إفساد عمل لنظام للمعالجة الآلية للبيانات الشخصية، من أجل استخدامها في أغراض الإعلانات التسويقية الموجهة عبر الإنترنت.

وعليه يتحدد المسئولية الجنائية في حالة الإعلانات التسويقية الموجهة التي تمثل انتهاكا للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونية لكلاً من إدارة الموقع ولوكالات الإعلان أي الناشر والمورد للمحتوى الإعلاني، فأي موقع أو تطبيق إلكتروني يقوم بإتاحة المساحات الإعلانية لنشر المحتوي الإعلاني، سواء عن طريق حفظ أو نقل أو معالجة البيانات والمعلومات الشخصية للمستخدم، إلى مورد المحتوي الإعلاني، حتي يتمكن الاخير من توجيه الإعلان إلى المستخدم للإنترنت المستهدف(١). وعلى سبيل المثال لذلك يعتبر موقعي جوجل وياهو من المواقع الناشرة للإعلانات عن طريق معالجة البيانات الشخصية الإلكترونية واتاحة تلك البيانات إلى مورد المحتوى الإعلامي وبالتالي تكون مسئولة مع المورد عن انتهاك الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً عن طريقة الإعلانات التسويقية غير المرغوبة.

وتطبيقا على ذلك فقد قضت محكمة باريس في ١٥ يناير ٢٠٠٢ بأن إرسال الإعلانات التسويقية غير المرغوب فيها من خلال البريد الإلكتروني يمثل ممارسة غير مشروعة ويخل بدرجة كبيرة بالحق في الخصوصية(٢) ، كما يخالف العقد المبرم بين المستخدم الذي يمارس هذا النشاط ومورد منافذ الدخول إلى الإنترنت.

---

(١) – Jean – Philippe MOINY, Facebook au regard de la protection des données, Revue Européenne de droit de la consommation, ٢٠١٠, p. ٢.

(٢) – TGI Paris, ١٥ janvier ٢٠٠٢, n° ٢٥٩., www.legalis.net.

ولذلك فقد أنشأت اللجنة الفرنسية القومية للمعلومات والحريات CNIL في عام ٢٠٠٢ موقعاً خاصاً لمكافحة الرسائل التسويقية غير المرغوب فيها ، يجيز للأشخاص مراسلة الموقع بكل رسائل غير مرغوب فيها تصل إلى صناديق بريدهم الإلكترونية ، وذلك لتحديد وملاحقة هؤلاء الاشخاص جنائياً. وبناء على ذلك فالإعلان التسويقية الموجهة قد تتسلل من خلال برامج ضارة إلى جهاز مستخدم الإنترنت، وتتمثل خطورتها في أنها تعمل بصورة تلقائية بمجرد ظهور الإعلان على الحاسب الآلي. وهذا ما حدث في فبراير ٢٠١٤ لأحدى مستخدمات موقوع يوتيوب، حيث اكتشفت أن برنامجا ضاراً قد تسلل إلى جهازها عن طريق رابط الموقع ويقوم بالتجسس على معلوماتها وبياناتها الشخصية بمجرد مشاهدتها للفيديو حتي دون أن تنقر على الإعلان(١)، فيقوم هذه البرامج بإطلاق فيروس خاص باختراق الحسابات المصرفية على الإنترنت وإجراء عمليات تحويل غير مشروعة لأموال المستخدم للإنترنت.

وقد حاول المشرع الفرنسي تدارك الانتقادات السابقة فنص في قانون رقم ٥٧٥ لسنة ٢٠٠٤ المتعلق بالثقة في الاقتصاد الرقمي بأحكام لمكافحة الإعلانات التسويقية غير المرغوب فيها. وبموجب هذا القانون كرس المشرع الفرنسي نظام الرضاء المسبق الصريح لقبول هذا النوع من الإعلانات التسويقية الإلكترونية، وذلك من خلال نص المادة ٥-٢٠ -L١٢١ من قانون حماية المستهلك، وكذلك المادة ١-٥-L٣٤ من قانون البريد والاتصالات عن بعد، بحيث يشترط الرضاء المسبق الصريح قبل إرسال الإعلانات التسويقية الإلكترونية وذلك لحماية الخصوصية في البيانات الشخصية التي تم معالجتها إلكترونيا. وقد وضع المشرع الفرنسي شروط يجب توافرها في الرضاء المسبق حتي لا تقع الجريمة وهي على النحو التالي:

(١) - *V.,* McEnroe NAVARAJ, The wild wild web : YouTube ads serving malware, Bromium labs call of the wild blog, ٢١ feb, ٢٠١٤.

أ- أن يكون هذا الرضاء المسبق حراً وليس تحت أي نوع من الإكراه أو التهديد أو أي شكل من أشكال الاعتداء على حرية الإرادة.

ب-أن يكون الرضا محدداً على نوع من الإعلانات وليس عاما.

ت-يشترط أن يتم الرضاء المسبق بناء على معلومات واضحة تقدم للشخص المستقبل للإعلانات أي أن يكون متبصراً.

أما بالنسبة لموقف المشرع الأمريكي فقد نص قانون مكافحة البريد التجاري الإعلاني غير المرغوب فيه الصادر في ١٦ ديسمبر ٢٠٠٣ على حماية الحق في الخصوصية في مواجهة الإعلانات التجارية غير المرغوب فيها، ونص المشرع على الحق في الاعتراض على هذه الإعلانات التجارية التي تنتهك الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً وتمثل مصدر للإزعاج. وكذلك ألزم المشرع الأمريكي من يرسل الرسائل الإلكترونية أن يوفر آلية تمكن مستقبل الرسالة من إبلاغ المرسل عن رغبته في عدم استقبال مثل هذه الرسائل(١)، بالإضافة إلى ذلك ألزم المشرع المرسل بأن يتضمن الرسالة الإعلانية بيانات واضحة منها انها رسالة إعلانية وعنوان بريد حقيقي حتي يتمكن المستقبل ممارسة حقه في الاعتراض وفقا لقواعد المقررة في القانون.

وتطبيقاً على ذلك في الولايات المتحدة الأمريكية في عام ٢٠١٢ تعرض نحو ثلاثمائة ألف من مستخدمي موقع دوري بيسبول الشهير في الولايات المتحدة الأمريكية ، لبرامج ضارة تنفذ إلى جهاز المستخدم للإنترنت بمجرد النقر على إعلان خبيث بشأن

(١) – د. عبد الهادي فوزي العوضي ، الجوانب القانونية للبريد الإلكتروني ، دار النهضة العربية ، القاهرة ، ٢٠٠٥ ، ص ٩٢.

ساعات يد ثمينة بأسعار مخفضة، بحيث تعمل هذه البرامج بمجرد أن يقوم المستخدم بالنقر على الإعلان فيظهر له برنامج حماية وهمية ضد الفيروسات، يتظاهر بفحص ملفات جهاز المستخدم للإنترنت ويوهمه بالعثور على فيروسات تحتاج إزالتها إلى شراء هذا البرنامج الوهمي بسعر منخفض(١)، ويتم بذلك اختراق خصوصية البيانات والمعلومات الشخصية للمستخدم عن طريق هذه الإعلانات التسويقية عبر الانترنت.

ولذلك فقد قامت اللجنة الفيدرالية للتجارة الأمريكية FTC بالإدانة لشركة الإعلانية الأمريكية المتخصصة في إعلانات الفيديو على الإنترنت في القضية المتعلقة بالانتهاكات القانونية لشبكة Scan Scout، حيث ترجع وقائع القضية إلى الفترة من أبريل ٢٠٠٧ إلى سبتمبر ٢٠٠٩ حيث قامت باستعمال ملفات الارتباط في جمع وتخزين البيانات والمعلومات الشخصية للمستخدمين، وذلك بهدف دراسة سلوكياتهم على الإنترنت، ومن ثم استهدافهم بإعلانات الفيديو المناسبة لسلوكياتهم. بالإضافة إلى أن الشركة استعملت هذه الملفات على نحو يتعذر معه على المستخدم حذفها أو منع عملها من خلال متصفحة ، فتبقي فاعليتها قائمة مهما حاول التخلص منها(٢). الامر الذي يترتب عليه الإخلال بالحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونيا عن طريق هذه النوع من الإعلانات التسويقية. وفي ٢١ ديسمبر ٢٠١١ تم التوصل إلى تسوية بموجبها تلتزم الشركة بوضع إشعار تقر فيه بانها تجمع بيانات المستخدم من بعض المواقع لاستخدامها في الإعلانات وذلك لمدة خمس سنوات.

(١) – *V.,* Evan KEISER, MLB. Com distributing Fake AV Malware via compromised AD network, Silversky altitude blog, ١٨ jun ٢٠١٢.

(٢) – *V.,* Sara FORDEN and Karen GULLO, Google judge accepts ٢٢.٥ s Milion FTC privacy settlement, Bloomberg, ١٧ nov ٢٠١٢.

وفي تطبيقا أخري في الولايات المتحدة الأمريكية أثارت قصية الجدل بشأن الحق في الخصوصية على الإنترنت ووسائل التواصل الاجتماعي، ففي عام ٢٠٠٧ قام شخص يدعي لين بشراء هدية عيد ميلاد لزوجته لمفاجأتها، وفوجئ بظهور إعلان على موقع الفيسبوك بواسطة برنامج إعلاني يسمى بيكون يقوم بنشر أخبار مشتريات أعضاء الفيسبوك على الموقع، فاعتبر المدعي أن ذلك يمثل خرقاً لخصوصياته وفقا للقانون الأمريكي ECPA الخاص بحماية خصوصية الاتصالات الإلكترونية، وبناء على ذلك فقد قضت محكمة ولاية كاليفورنيا الشمالية بأن معلومات التصفح على الإنترنت قد انتهكت من خلال موقع الفيسبوك الخاصة بحساب المدعي وأن تلك المعلومات قد تم اعتراضها لغرض غير قانوني وهو تعزيز الربحية من خلال الإعلانات التسويقية الموجهة([1]) ، وبناء على ذلك قررت المحكمة بموجب تسوية بين الشركة والمدعي إغلاق برنامج بيكون على الفيسبوك لمدة ٦٠ يوماً من تاريخ التسوية ، وألزمت موقع الفيسبوك بدفع مبلغ ٩.٥ مليون دولار لإنشاء صندوق لدعم الخصوصية على الموقع ، وتعويض المدعي عما أصابه من ضرر المساس بخصوصية بياناته ومعلوماته الشخصية.

وبناء على ما سبق فقد نصت اتفاقية بودابست الاوربية الصادرة في عام ٢٠٠١ على مكافحة الإعلانات التسويقية غير المرغوب بها، واعتبرت هذا الفعل سلوك إجرامي يندرج ضمن الأفعال الإجرامية التي تمس الحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

([1]) – د. عمر أبو بكر يونس ، الجرائم الناشئة عن استخدام الإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ ، ص ٦٠٦.
www.dockets.justia.com/docket/california/candce/٥:٢٠٠٨cv٠٣٨٤٥/٢٠٦٠٨٥.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

أما بالنسبة لموقف المشرع المغربي فقد نص على مكافحة الإعلانات التسويقية غير المرغوب فيها ولكن بطريقة غير مباشرة في المادة ٦٠٧ -٥ من قانون رقم ٠٣-٠٧ بشأن الجرائم التي تمس بنظم المعالجة الآلية للمعطيات، بحيث يعاقب بالحبس من سنه إلى ثلاث سنوات وبالغرامة المالية من ١٠.٠٠٠ إلى ٢٠٠.٠٠٠ درهم أو بإحدى هاتين العقوبتين كل من عرقل عمداً سير نظام للمعالجة الآلية للمعطيات أو أحدث فيها خللاً. وكذلك نص في قانون حماية المستهلك على شرط الرضاء المسبق الصريح. ويتضح من ذلك النص أن المشرع المغربي قد سار على نهج المشرع الفرنسي في عدم النص على التجريم المباشر للإعلانات التسويقية الإلكترونية غير الرغوب فيها. وبالتالي يتعرض لنفس الانتقادات التي وجهت للمشرع الفرنسي.

ولكن بالرغم من ذلك فغن المشرع المغربي قد أخذ اتجاه مغاير لاتجاه المشرع الفرنسي، وذلك بالنص في المادة ١٠ من قانون حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي([1]) على منع الاستقراء المباشر بواسطة آليه اتصال أو جهاز الاستنساخ البعدي أو بريد إلكتروني أو وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة باستعمال بيانات شخص ذاتي ، في أي شكل من الأشكال، لم يعبر عن رضاه المسبق عن استقبال الاستقراءات المباشرة بهذه الوسيلة. ويقصد بالرضاء هو كل تعبير عن الإرادة الحرة والمميزة وعن علم يقبل بموجبه شخص معين باستعمال المعطيات ذات الطابع الشخصي التي تخصه لأغراض الاستقراء المباشر. وقد عرف المشرع المغربي الاستقراء المباشر بأنه إرسال أية رسالة موجهة للترويج المباشر أو غير المباشر لسلع أو خدمات أو بسمعة شخص يبيع سلعاً أو يقدم خدمات.

([1]) – قانون حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي ، ظهير شريف رقم ١٥ – ٠٩- ١ صادر في ١٨ فبراير ٢٠٠٩ ، بتنفيذ القانون رقم ٠٩ – ٠٨ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية رقم ٥٧١١ الصادرة في ٢٣ فبراير ٢٠٠٩.

واستثناءً من ذلك فقد نص المشرع المغربي على أنه يرخص بالاستقراء المباشر عن طريق البريد الإلكتروني إذا ما طلبت البيانات مباشرة من المرسل إليه، مع التقيد بأحكام القانون، بمناسبة بيع أو تقديم خدمات، إذا كان الاستقراء المباشر يهم منتجات أو خدمات مشابهة يقدمها نفس الشخص الذاتي أو المعنوي، وتبين للمرسل إليه بشكل صريح ولا يشوبه لبس وبسيط توفره على إمكانية التعرض دون صوائر، باستثناء التكلفة المرتبطة بإرسال الرفض، على استعمال بياناته وقت جمع هذه الأخيرة وكلما وجه إليه بريد إلكتروني لأجل الاستقراء. وقد وضع المشرع شروط حتى يمكن إرسال هذا الاستقراء المباشر أي أرسل رسائل تسويقية إلكترونية أو آليه وهي على النحو التالي:

١- يمنع إرسال رسائل بواسطة آليات الاتصال الهاتفي وجهاز الاستنساخ البعدي والبريد الإلكتروني لأجل الاستقراء المباشر دون الإشارة إلى بيانات صحيحة يمكن أن تعين المرسل إليه على إرسال طلب توقيف هذه الاتصالات دون صوائر غير تلك المرتبطة بإرسالها.

٢- كذلك يمنع إخفاء هوية الشخص الذي أوصلت لفائدته الرسائل وذكر موضوع لا صلة له بالخدمات المقترحة.

وكذلك نص المشرع القطري على تجريم الاتصالات الإلكترونية لغرض التسويق المباشر في المادة ٢٢ من قانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية، حيث تنص على أن "يحظر إرسال أي اتصال إلكتروني بغرض التسويق المباشر إلى الفرد، إلا بعد الحصول على موافقته المسبقة. ويجب أن يتضمن الاتصال الإلكتروني هوية منشئه، وما يفيد بأنه مرسل لأغراض التسويق المباشر، كما يجب أن يتضمن عنواناً صحيحاً يسهل الوصول إليه، ويستطيع الفرد من خلاله أن يرسل طلباً

إلى المنشئ بإيقاف تلك الاتصالات أو الرجوع في موافقته على إرسالها. ويعاقب المشرع القطري على مخالفة ذلك بالغرامة المالية التي لا تزيد عن ١.٠٠٠.٠٠٠ مليون ريال ، مالم ينص على عقوبة أشد في قانون آخر"([1]).

أما بالنسبة لموقف المشرع المصري فنجد أنه نص على حماية البريد الإلكتروني والمواقع والحسابات الخاصة من الاعتداء عليها بأي صوره، ويدرج تحت صور الاعتداء حالة الإعلانات التسويقية غير المرغوب فيها، فنص في المادة ١٨ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على أن "يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائة ألف جنية، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريداً إلكترونيا أو موقعاً أو حساباً خاصاً بآحاد الناس. فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز مائتي ألف جنية، أو بإحدى هاتين العقوبتين".

بالإضافة إلى ذلك ففي عام ٢٠٢٠ أصدر المشرع المصري قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، وقد نص في المادة ١٧ منه على القواعد العامة الحاكمة لعملية التسويق الإلكتروني بحيث أنه "يحظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات، إلا بتوافر الشروط الآتية:

١ – الحصول على موافقة من الشخص المعني بالبيانات.

٢ – أن يتضمن الاتصال هوية منشئه ومرسله.

٣ – أن يكون للمرسل عنوان صحيح وكاف للوصول إليه.

([1]) – المادة ٢٣ من قانون حماية خصوصية البيانات الشخصية القطري.

٤ – الإشارة إلى أن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر.

٥ – وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها".

كذلك فقد نص المشرع المصري في المادة ١٨ من نفس القانون على التزامات على الشخص المرسل بحيث أنه "يلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر بالالتزامات الآتية:

١. الغرض التسويقي المحدد.

٢. عدم الإفصاح عن بيانات الاتصال للشخص المعني بالبيانات.

٣. الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعني بالبيانات وتعديلاتها، أو عدم اعتراضه علي استمراره، بشأن تلقي الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال".

وفي حالة مخالفة أحكام التسويق الإلكتروني المنصوص عليها في المادتين السابقتين ١٧، و١٨ في قانون حماية البيانات الشخصية، بعقوبة الغرامة التي لا تقل عن مائتي ألف جنية ولا تجاوز مليوني جنيه([1]).

([1]) – أنظر المادة ٤٣ من القانون المصري بشأن حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

المبحث الخامس. حماية خصوصية البيانات الشخصية الإلكترونية للأطفال

مما لا شك فيه أن الأطفال يستحقون حماية خاصة فيما يتعلق بياناتهم الشخصية، لأنهم أقل وعياً بالمخاطر والعواقب والضمانات المعنية وبحقوقهم فيما يتعلق بمعالجة البيانات الشخصية. وعلى وجه الخصوص ينبغي أن تشمل هذه الحماية الخاصة استخدام البيانات الشخصية للأطفال لأغراض التسويق أو إنشاء ملفات شخصية أو لمستخدمي البيانات وجمع البيانات الشخصية فيما يتعلق بالأطفال عند استخدام الخدمات المقدمة مباشرة إلى الطفل(١). وبالإضافة إلى ذلك وفي سياق الإجراءات والتدابير الوقائية ينبغي الحصول على موافقة المسئول عن الطفل قبل إجراء المعالجة للبيانات الشخصية الخاصة بالطفل أو إجراء الخدمات التي تعتمد أو تستخدم البيانات الشخصية الخاصة بهم.

وفي هذا المطلب سوف نتناول بالعرض لموقف التشريعات المقارنة من حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونيا للأطفال في المطلب الاول، وفي المطلب الثاني نوضح الحماية الجنائية لخصوصية البيانات الشخصية للأطفال على مواقع التواصل الاجتماعي، أما في المطلب الثالث نستعرض موقف القانون الدولي من حماية خصوصية البيانات الشخصية المعالجة إلكترونياً للأطفال.

(١) – انظر المادة ٣٨ من اللائحة العامة الأوربية رقم ٦٧٩ لسنة ٢٠١٦ بشأن حماية البيانات الشخصية والتي سوف تدخل حيز النفاذ في ٢٥ مايو ٢٠١٨.

المطلب الأول. موقف التشريعات المقارنة من حماية خصوصية البيانات الشخصية الإلكترونية للأطفال

بادئ ذي بدء نستعرض موقف المشرع الأمريكي حيث اهتم المشرع في الولايات المتحدة الأمريكية بحماية خصوصية البيانات الشخصية للطفل فوضع تشريع يعتبر من أوائل التشريعات التي وضعت قواعد لحماية خصوصية البيانات الشخصية للأطفال، فقد أصدر المشرع الأمريكي في عام ١٩٧٤ قانون خاص بحماية حقوق العائلة في التعليم والخصوصية والذي ينص على إلزام المدارس ابقاء سجلات تلاميذها سرية، بحيث لا يستطيع الآباء الاطلاع عليها، إلا إذا وافقت الادارة، كما لا يجوز تسليم أي سجل لأية دائرة حكومية إلا بأمر من المحكمة، ويستطيع الطالب أو الوالدين رفع دعوى ضد المدرسة يطالبون فيها بتعديل السجل أن كان خاطئاً ومتحيزاً في اعتقادهم.

ومن هذا المنطلق فقد حرص المشرع المصري على حماية خصوصية البيانات والمعلومات الشخصية بالطفل فنص في المادة ٨٠ من الدستور الجديد على أن تلتزم الدولة برعاية الطفل وحمايته من جميع أشكال العنف والإساءة وسوء المعاملة والاستغلال الجنسي والتجاري. وكذلك نص المشرع المصري في قانون الطفل رقم ١٢ لسنة ١٩٩٦ والمعدل بالقانون رقم ١٢٦ لسنة ٢٠٠٨(١) ؛ على تغريم كل من ينشر أو أذاع بأحد أجهزة الإعلام أي معلومات أو بيانات تخص هوية طفل معرض للخطر حيث جرم نشر أو إذاعة أي معلومات، أو بيانات، أو أي رسوم، أو صور تتعلق بهوية الطفل حال عرض أمره على الجهات المعنية بالأطفال المعرضين للخطر أو المخالفين للقانون.

(١) – المادة ١١٦ مكررا (ب) مضافة بالقانون رقم ١٢٦ لسنة ٢٠٠٨ ، المنشور بالجريدة الرسمية العدد ٢٤ مكرر ، الصادر في ١٥ يونيو ٢٠٠٨.

وقد عاقب المشرع المصري من قام بهذه الجريمة بعقوبة الغرامة المالية التي لا تقل عن عشرة آلاف جنية ولا تجاوز خمسين ألف جنية.

بالإضافة إلى ذلك فقد نص المشرع المصري في المادة ١١٦ مكرا (أ) من قانون الطفل على "أن يعاقب بالحبس مدة لا تقل عن سنتين وبالغرامة المالية التي لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه كل من استورد أو صدر أو أنتج أو أعد أو عرض أو طبع أو روج أو حاز أو بث أي أعمال إباحية يشارك فيها أطفال أو تتعلق بالاستغلال الجنسي للطفل، ويحكم بمصادرة الأدوات والآلات المستخدمة في ارتكاب الجريمة والأموال المتحصلة منها ، وغلق الأماكن محل ارتكابها مدة لا تقل عن ستة أشهر، وذلك كله مع عدم الإخلال بحقوق الغير حسن النية. ومع عدم الإخلال بأي عقوبة أشد ينص عليها في قانون آخر، يعاقب بذات العقوبة كل من :

أ- استخدام الحاسب الآلي أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لإعداد أو لحفظ أو لمعالجة أو لعرض أو لطباعة أو لنشر أو لترويج انشطة أو أعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة والأعمال الإباحية أو التشهير بهم أو بيعهم.

ب-استخدام الحاسب الآلي أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لتحريض الأطفال على الانحراف أو لتسخيرهم في ارتكاب جريمة أو على القيام بأنشطة أو أعمال غير مشروعة أو منافية للآداب، ولو لم تقع الجريمة فعلا".

ونستخلص مما سبق أن المشرع المصري يجرم الاعتداء على خصوصية البيانات والمعلومات الشخصية المتعلقة بالأطفال المعرضين للخطر أو المخالفين للقانون سواء تم ذلك عن طريق النشر أو إذاعة فقط دون أن يشمل بالحماية لخصوصية البيانات

الشخصية للأطفال عموما وليس فقط المخالفين للقانون أو المعرضين للانحراف. كذلك كان المشرع المصري قاصر في تجريمه فقط كل من استورد أو صدر أو أنتج أو أعد أو عرض أو طبع أو روج أو حاز أو بث أي أعمال إباحية يشارك فيها أطفال أو تتعلق بالاستغلال الجنسي للطفل، أي يحمي حق الطفل في خصوصية البيانات والمعلومات المتعلقة بالحق في الصورة من الاستغلال الجنسي دون أن تمتد الحماية الجنائية لباقي صور الحماية للبيانات والمعلومات الشخصية المتعلقة بالطفل، فالحماية الجنائية قاصره وليست شاملة تحمي جزء وليس كل الحق في الخصوصية للبيانات والمعلومات الشخصية التي يتم معالجتها إلكترونياً.

أما بالنسبة لموقف المشرع التونسي فقد نص في المادة ٢٨ من قانون حماية المعطيات الشخصية الصادر في ٢٧ يوليو ٢٠٠٤، على أنه "لا يمكن معالجة معطيات شخصية متعلقة بطفل إلا بعد الحصول على موافقة وليه وإذن قاضي الأسرة. ويمكن لقاضي الأسرة أن يأذن بالمعالجة ولو دون موافقة الولي إذا اقتضت مصلحة الطفل الفضلى ذلك. ولقاضي الأسرة الرجوع في الإذن في كل وقت". وتبين لنا من ذلك أن المشرع التونسي لم يشترط موافقة ولى الطفل فقط كما تنص أغلب التشريعات المقارنة، ولكنه يشترط بالإضافة إلى ذلك موافقة قاضي الأسرة حتى يمكن معالجة البيانات الشخصية للطفل، مما يشكل بذلك ضمانه إجرائية لعدم استغلال البيانات الشخصية الخاصة بالطفل وحماية لخصوصية بياناته الشخصية.

أما بالنسبة لموقف المشرع القطري فقد وضع شروط يجب على مالك أو مشغل أي موقع إلكتروني موجه للأطفال، "أن يقوم بها لحماية البيانات الشخصية الخاصة بالأطفال والتي تم معالجتها إلكترونياً وهي على النحو التالي([1]) :

([1]) – المادة ١٧ من قانون حماية خصوصية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦ ، الصادر في الجريدة الرسمية العدد ١٥ بتاريخ ٣ نوفمبر ٢٠١٦.

١- وضع إخطار على الموقع حول ماهية بيانات الأطفال، وكيفية استخدامها، والسياسات التي يتبعها في الإفصاح عنها.

٢- الحصول على موافقة صريحة من ولي أمر الطفل الذي تتم معالجة بيانات شخصية عنه، وذلك عن طريق اتصال إلكتروني أو أي وسيلة أخرى مناسبة.

٣- تزويد ولي أمر الطفل، بناءً على طلبه، وبعد التحقق من هويته، بوصف لنوع البيانات الشخصية التي تتم معالجتها، مع بيان الغرض من المعالجة، ونسخة من البيانات التي تمت معالجتها أو جمعها عن الطفل.

٤- حذف أو محو أو وقف معالجة أية بيانات شخصية تم جمعها من الطفل أو عنه، إذا طلب ولي الأمر ذلك.

٥- ألا تكون مشاركة الطفل في لعبة، أو عرض جائزة، أو أي نشاط آخر، مشروطة بتقديم الطفل بيانات شخصية تزيد على ما هو ضروري للمشاركة في ذلك النشاط".

ونستخلص مما سبق أن المشرع القطري قد نص على وضع حماية خاصة لخصوصية البيانات الشخصية للطفل، والمقصود بالطفل هو كل من لم يبلغ سنة الثامنة عشر من عمره. وجعل لولي أمر الطفل الحق في الموافقة أو الرفض في حذف أو محو أو وقف معالجة أية بيانات شخصية ثم جمعها من الطفل أو عنه.

المطلب الثاني. الحماية الجنائية لخصوصية البيانات الشخصية للأطفال على مواقع التواصل الاجتماعي

لقد حرصت العديد من الدول بسن قوانين تمنع استخدام مواقع التواصل الاجتماعي لمن هم دون سن الثالثة عشر عاما مثال على ذلك التشريع الأمريكي، بينما تقوم بعض الدول الأخرى بوضع قواعد تسمح باستخدام الأطفال لمواقع التواصل الاجتماعي ولكن تحت أشراف ومراقبة الوالدين. والهدف من ذلك هو حماية خصوصية البيانات الشخصية للأطفال وحمايتهم كذلك من التحرش والتنمر الإلكتروني والايذاء النفسي ، بالإضافة إلى ذلك يجب اتخاذ تدابير لمواجهة هذه الظاهرة الخطيرة من خلال تعليم الأطفال بضرورة الحفاظ على البيانات والمعلومات الشخصية مثل الاسم والعنوان ورقم الهاتف والسن والجنس ويجب الانتباه بشكل خاص للصورة التي قد يشاركها الطفل عبر الإنترنت ، لأنها تحتوي في ذاتها معلومات أخرى كمكان وقت التقاط الصورة والأشخاص الموجودين بها، الأمر الذي لا ينبغي مشاركته مع الغرباء، وبالتالي امكانية استغلالها في التعرض لخصوصية الأطفال.

وتطبيقا لذلك فقد نص المشرع الأمريكي على حماية خصوصية البيانات الشخصية الإلكترونية للأطفال، فقد أصدر عام ١٩٩٨ قانون COPPA لحماية خصوصية البيانات الشخصية للأطفال عبر الإنترنت والذي دخل حيز النفاذ في ٢١ أبريل ٢٠٠٠، بحيث يحظر هذا القانون على معدي المواقع عبر الإنترنت نشر معلومات شخصية مصدرها الأطفال الذين لا تتجاوز أعمارهم ثلاثة عشر عاما، حيث يلتزم معدو المواقع وفقا لهذا القانون بالحصول على إذن مسبق من أولياء الأمور لأجل نشر معلومات

وبيانات عبر الإنترنت يكون مصدرها أطفال أقل من ثلاثة عشر عاما. بالإضافة إلى ذلك يلتزم أصحاب المواقع الإلكترونية باتخاذ كافة الإجراءات التقنية والقانونية للمحافظة على المعلومات المتحصلة من هؤلاء الأطفال بمناسبة تعاملهم مع هذه المواقع الإلكترونية وعدم الكشف عنها لطرف آخر(١)، وذلك لحماية الحق في خصوصية هؤلاء الأطفال في بياناتهم ومعلوماتهم الشخصية التي تم معالجتها إلكترونياً.

وتطبيقا على ذلك فقد قضت المحكمة العليا بنيويورك في عام ١٩٨٢ قرار حظرت فيه تصوير أو رسم القاصرين الممارسين للسلوك الجنسي(٢)، حيث جاء في قرارها بأن الذي يستخدم الأطفال كمحل للخلاعة والفحش يؤذيهم في أجسامهم وفي نفسيتهم ، فمن المصلحة بالتالي أن يكون أولى بالحظر والتجريم. وبناء على ذلك صدر قانون آداب الاتصالات عام ١٩٩٦، والذي يجرم الاعتداء المتمثل بالتصوير الجنسي أو إظهار النشاطات الجنسية للأطفال علي الإنترنت(٣)، وكذلك يحظر الأحاديث الجنسية للأطفال على الإنترنت. وقد تم إلغاء هذا القانون وصدر قانون حماية الأطفال على الإنترنت في عام ١٩٩٨ COPPA بتوسع تجريم الأعمال والمواد التي تجرى على الإنترنت والتي تشكل اعتداء على الأطفال من التعرض للمواد غير الملائمة.

وعليه فقد أصدر المشرع الأمريكي تعديلات على القانون COPPA في ديسمبر ٢٠١٢ ودخلت حيز النفاذ في الأول من يوليو ٢٠١٣، بحيث أضافت شرط اشعار

---

(١) - The children`s online privacy protection act, COPPA, ١٩٩٨, U.S.A, available at : www.ftc.gov.

(٢) - Martin FORST, E- Law, Appellate court cases about information technology, by Montclair, enterprises san Francissco, ١٩٩٩, p. ١٦.

(٣) - Lilan EDWARDS & Charlotte WAELDE, Law and the internet, Regulating cyber space, Hart Publishing, Exford, ١٩٩٧, P. ٢٣١.

الوالدين للموافقة على أي معالجة للبيانات الشخصية للطفل، وكذلك فرضت التزام على كل موقع إلكتروني أو مقدم خدمة عبر الإنترنت موجهة إلى الاطفال أقل من ١٣ عاما، بنشر سياسة خصوصية واضحة وشاملة على الإنترنت فيما يتعلق بمعالجة البيانات الشخصية للأطفال أقل من ١٣ عاما. بالإضافة إلى ذلك نص تعديل القانون على شرط الاحتفاظ والحذف للبيانات الشخصية للأطفال، بحيث يكون الاحتفاظ بالبيانات الشخصية التي تم الحصول عليها من الأطفال بطريقة مشروعه للوقت اللازم لتحقيق الغرض الذي جمعه من أجلة. وأن يضمن المشغلون أن أي طرف ثالث يحصل على البيانات الشخصية للأطفال أن يلتزم باتخاذ الإجراءات المعقولة لحماية خصوصية هذه البيانات والمعلومات الشخصية للأطفال، ويعاقب كل مخالف لهذه القواعد بالغرامة المالية والتي لا تزيد مقدارها عن ٤٠.٠٠٠ ألف دولار.

ونستخلص مما سبق أن هناك مجموعة من الالتزامات المفروضة لحماية خصوصية البيانات الشخصية للأطفال على المواقع الإلكترونية وفقا للتعديلات الاخيرة لقانون COPPA، وهي على النحو التالي:

١- الالتزام بعدم مطالبة الطفل بالكشف عن مزيد من البيانات والمعلومات الشخصية أكثر مما هو ضروري بشكل معقول للمشاركة في هذا النشاط على شبكة الإنترنت.

٢- الالتزام بتوفير الامكانية للآباء لمراجعة بيانات ومعلومات أطفالهم الشخصية والتوجيه بحذفها وعدم السماح بجمع المزيد من المعلومات عن أطفاهم أو استخدامها.

٣- الالتزام بالحصول على موافقة الوالدين على جمع واستخدام معلومات طفلهم، ولكن ذلك لا يعني السماح بكشف المعلومات لطرف ثالث إلا إذا كان ذلك الطرف جزء من هذه الخدمة.

٤- يملك الوالدين الحق في مراجعة أو حذف أو إدارة أو رفض أو تحديد الجهات التي يمكن مشاركة بيانات ومعلومات طفلهم معها، ويتم ذلك من خلال إعدادات الحساب على مواقع على شبكة الإنترنت، أومن خلال مراسلة موظفي الدعم لدي هذه الشركات من خلال البريد الإلكتروني، أو من خلال الاتصال مباشرة على أرقام الدعم الفني الخاصة بها.

٥- الالتزام بإخطار الآباء بشكل مباشر قبل جمع البيانات والمعلومات الشخصية من أطفالهم. وهذا يشمل ما هي المعلومات المحددة المراد جمعها والكيفية التي يمكن أن يتم الكشف عنها، وأن يتم تزويدهم أيضا برابط لسياسة الخصوصية الخاصة بهذه الشركات على الانترنت، وكيف يمكن للوالدين إعطاء موافقتهم. أيضا، أما إذا لم يكن الوالدين موافقين في غضون فترة زمنية معقولة، يجب حذف بيانات ومعلومات الاتصال الخاصة بالوالدين والطفل من السجلات هذه الشركات أو المواقع الإلكترونية.

وبالرغم من ذلك فإن يؤخذ على القانون الأمريكي المتعلق بحماية البيانات الشخصية للأطفال على الإنترنت COPPA انه لم يواجه صور الانتهاكات الحديثة لخصوصية البيانات الشخصية للأطفال والتي تم معالجتها إلكترونياً مثل على ذلك الإعلانات الموجهة التسويقية والتي تتم من خلال برامج الارتباط عن طريق التجسس على البيانات الشخصية للأطفال. كذلك لا يمنع هذا القانون الأطفال من الوصول إلى المواقع الاباحية عن طريق الكذب عن اعمارهم، وفي النهاية نستطيع القول بأن هذا القانون لا يوفر بيئة أمنه للأطفال على الإنترنت وخاصة فيما يتعلق بحقهم في خصوصية بياناتهم ومعلوماتهم الشخصية التي تم معالجتها إلكترونياً. كذلك يؤخذ

على المشرع الأمريكي انه لم يوسع الحماية الجنائية لخصوصية البيانات الشخصية للطفل، حيث فان المشرع القطري قد وسع الحماية لخصوصية البيانات الشخصية للطفل حتي سنة الثامنة عشر من عمره على عكس المشرع الأمريكي الذي يجعل الحماية لخصوصية البيانات الشخصية للطفل حتي سن الثالثة عشر من عمره، وهذا موقف محمود للمشرع القطري ويتماشى مع ما تنص عليه الاتفاقيات الدولية التي حددت سن الطفل بأنه كل من لم يبلغ سن الثامنة عشر من عمره.

وتطبيقا على ذلك فقد نصت سياسة الخصوصية لموقع الفيسبوك بشأن كيفية التعامل ما الأطفال([1])، على منع الاطفال من هم دون سن ١٣ عاما من الاشتراك أو وضع بياناتهم على الموقع – وقد نصت بنود سياسة الخصوصية على أن المسئولين عن الموقع أن يسارعون بمحو بيانات من يسجلون من الأطفال أقل من سن ١٣ عاما، أما من تتراوح أعمارهم بين ١٣ و١٨ عاما فيتح الموقع لهم استمارة لتعبئة الموافقة من ولي الأمر على نشر بيانات أولادهم على موقع الفيسبوك.

أما بالنسبة لموقف المشرع الانجليزي فقد نص في المادة الأولى من قانون حماية الطفل الصادر في عام ١٩٧٨ على معاقبة كل شخص التقط أو سمح بالتقاط أو أنتاج أية صور ضوئية فاحشة حقيقية أو زائفة لطفل أو قام بتوزيع أو عرض أي من هذه الصور الضوئية الفاحشة الحقيقية أو الزائفة. وقد تم تعديل هذه القانون بقانون العدالة الجنائية والنظام العام الصادر في عام ١٩٩٤ والذي نص في المادة ٨٤ منه الفقرة الرابعة بأن تحديد معني الصورة الفوتوغرافية (الضوئية) بحيث تتضمن الصور

([1]) – د. اماني جمال مجاهد ، الخصوصية وتطبيقات الويب ٠٠٢,٠ ، وكيفية تحقيق المعادلة الصعبة ، كتاب دوري محكم ، الاتجاهات الحديثة في المكتبات والمعلومات ، العدد ٣٥ ، مجلد ١٦ ، يناير ٢٠١١ ، ص ٨٨ ، ٨٩.

١- السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية

الفوتوغرافية قواعد البيانات الإلكترونية، أي أن الحماية الجنائية تشمل كل التقاط أو السماح بالتقاط أو إنتاج أية صورة على الوسائط الإلكترونية، وبالتالي امتداد الحماية الجنائية لخصوصية البيانات الشخصية للأطفال التي يتم معالجتها إلكترونيا.

أما بالنسبة لموقف المشرع الفرنسي فقد نصت المادة ٥٨ من قانون حماية البيانات والحريات الصادر في ١٩٧٨ والمعدل بالقانون رقم ١٣٢١ لسنة ٢٠١٦ على ألا يجوز معالجة البيانات الشخصية الخاصة بالطفل أقل من ١٥ عاما إلا بعد الحصول على موافقة من ولي أمره، كذلك نصت هذه المادة على السماح للطفل أكثر من ١٥ سنة الحق في الاعتراض على السلطة الابوية الخاصة بالموافقة على معالجة البيانات الشخصية كذلك الحق في الوصول والتصحيح لهذه البيانات الشخصية. ويتضح من ذلك أن المشرع الفرنسي يقصر الحماية الجنائية لخصوصية البيانات الشخصية للأطفال ما دون سن ١٥ عاما فقط، هو بذلك يعمل على مد فترة الحماية للطفل مدة اطول وهو اتجاه محمود وان كان يفضل أن تصل الحماية إلى سن ١٨ عام كما ذهب المشرع القطري في ذلك الاتجاه. وليس كما ذهب المشرع الأمريكي الذي يقصر الحماية للأطفال ما دون سن ١٣ عاما.

المطلب الثالث. موقف القانون الدولي من حماية خصوصية البيانات الشخصية الإلكترونية للأطفال

نستعرض في البداية أبرز مظاهر الجهود الدولي لمكافحة وحماية خصوصية البيانات والمعلومات الشخصية للأطفال على شبكة الإنترنت، ومنها منتدى الشرق الأوسط وشمال أفريقيا حول أمن الأطفال عند استخدام الإنترنت الذي انعقد في عام ٢٠٠٥ والذي خرج بالتوصيات التالية([1]):

١- ضرورة خلق ائتلاف إقليمي على مستوى عالمي لتطوير مهارات مواجهة تلك الاعتداءات وصولاً إلى تحقيق سلامة استغلال الأطفال للإنترنت.

٢- دعوة الحكومات لمراجعة قوانينها وتشديد العقاب الخاص بجرائم الإنترنت ضد الأطفال، منها جرائم انتهاك حق الأطفال في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

٣- تطوير التربية وبرامج التوعية العامة للطفل وولى أمره وخاصة في كيفية اتخاذ التدابير والاحتياطات لحماية البيانات والمعلومات الشخصية لهم.

وكذلك فقد نصت الاتفاقية الدولية المتعلقة بحقوق الطفل الصادرة في ٢٠ نوفمبر ١٩٨٩ في المادة ١٦ على أن "من حق الطفل ألا يتم التدخل غير القانوني في حياته الخاصة ، فالطفل له الحق في الحماية القانونية في مواجهة هذا التدخل أو هذا الاعتداء،

([1]) – منتدى الشرق الأوسط شمال أفريقيا حول أمن الأطفال عند استخدام الإنترنت ، المنعقدة في جمهورية مصر العربية ، في الفترة من ٢٥ – ٣٠ يونيو ٢٠٠٥.

فهو يتمتع بحماية حقه في الصورة وحياته الخاصة حتى ولو كان مشهوراً"(١). ومن الجدير بالملاحظة أنه في أغلب الحالات تتداخل حماية الحق في خصوصية البيانات والمعلومات المتعلقة بالطفل مع حق الاسرة في خصوصية البيانات والمعلومات، فعلى سبيل المثال القيام بعمل تحقيق صحفي يحتوي على اعتداء على الحق في خصوصية البيانات والمعلومات الشخصية لسيدة انفصلت عن زوجها يمثل في نفس الوقت اعتداء على خصوصية البيانات والمعلومات الشخصية المتعلقة بالطفل(٢) وذلك لتدخل التحقيق الصحفي في البيانات والمعلومات الشخصية المتعلقة بنمط حياة الطفل.

وأما بالنسبة لحماية خصوصية البيانات الشخصية للأطفال على المستوي العربي فقد نصت الاتفاقية العربية لمكافحة جرائم تقنية نظم المعلومات الصادرة في عام ٢٠١١ في المادة ١٢ منها على أن "تشديد العقاب في حالة ما إذا ارتكبت الجرائم المتعلقة بالإباحية على الأطفال والقصر سواء كانت من خلال انتاج أو عرض أو توفير أو نشر أو بيع أو استراد أو حيازة مواد اباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات".

ولكن بالرغم من ذلك فان الاتفاقية العربية لمكافحة جرائم تقنية المعلومات محل الانتقاد، وذلك لأنها لم تنص بشكل واضح على مواد يكون من شأنها حماية الحق في خصوصية البيانات والمعلومات الشخصية وخاصة المتعلقة بالأطفال والتي تم معالجتها إلكترونياً. بالإضافة إلى ذلك كان يجب أن تكون النصوص القانونية محددة وصريحة بحيث لا ترك مساحة للتفسيرات والتأويل القانوني بالشكل الذي يوفر ضمانه حقيقية للحقوق والحريات، مما يجعلها تخالف المعايير الدولية لحماية حقوق الانسان.

---

(١) – TGI. Pairs, ٢١ juin ٢٠٠١, Légipresse, ٢٠٠١, paris, n° ١٨٤, I, P. ١٠٩.
اتفاقية حماية حقوق الطفل الصادرة بموجب قرار الجمعية العامة للأمم المتحدة رقم ٢٥/٤٤ في ٢٠ نوفمبر ١٩٨٩ ، ودخلت حيز النفاذ في ٢ سبتمبر ١٩٩٠.

(٢) – TGI. Nanterre, ١ere ch, ٤mars ٢٠٠٢, Légipresse, ٢٠٠٢, n°١٩٤, I, p. ١٠٩.

الخاتمة

في واقع الأمر أن موضوع الحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً من الموضوعات التي تثير الكثير من التساؤلات القانونية، خاصة في ظل الانتقال من عصر تكنولوجيا المعلومات (IT) إلى عصر تكنولوجيا البيانات (DT)إلى عصر الذكاء الاصطناعي (AI). وتطور أساليب ارتكاب الجرائم من جرائم تقليدية يرتكبها مجرم تقليدي، إلى عصر الجريمة المعلوماتية يرتكبها المجرم المعلوماتي ثم إلى عصر جريمة البيانات والذي يرتكبها مجرم البيانات إلى عصر مجرم الذكاء الاصطناعي. حيث أن المعالجة الإلكترونية للبيانات الشخصية أصبحت تشكل مرحلة هامة وخطيرة باعتبارها تأسس لعصر جديد من ثورة المعرفة والتكنولوجيا، عالم السحابة الإلكترونية والتي يتم تخزين البيانات من خلالها. في عالم مختلف مثل ذلك يحتاج إلى حماية جنائية للحق في الخصوصية بطريقة تلائم هذا التطور من حيث الجمع والنقل والتخزين والنشر والاطلاع والمعالجة لهذه البيانات الشخصية الإلكترونية. فالالتزام بالحفاظ على خصوصية البيانات الشخصية الإلكترونية الخاصة بالأفراد أصبح حق لا مناص منه على مقدمو الخدمة، وكذلك فالالتزام من قبل الشركات والمؤسسات بسياسة الخصوصية أصبح أمراً واجباً تفرضه جميع القوانين.

ومن خلال الدراسة التحليلية المقارنة لخصوصية البيانات الشخصية التي معالجتها إلكترونياً يتضح أن التشريعات الغربية سواء كانت تشريعات لاتينية مثال التشريع الفرنسي أو التشريعات الانجلوسكسونية مثل التشريع الانجليزي والتشريع الأمريكي قد قطعت شوطاً كبيراً في ملاحقة تطورات العصر فيما يتعلق بحماية خصوصية البيانات والمعلومات الشخصية التي يتم معالجتها إلكترونياً، فقامت بحماية كافة المراحل التي تمر بها معالجة البيانات والمعلومات الشخصية، بدءاً من المرحلة السابقة على المعالجة،

ثم المرحلة المعاصرة للمعالجة، ثم المرحلة اللاحقة للمعالجة للبيانات والمعلومات الشخصية. بالإضافة إلى ذلك نصت على حماية خصوصية البيانات الشخصية للفئات الضعيفة من أن تتعرض للانتهاك أو الاعتداء عليها مثل حماية خصوصية البيانات الشخصية للأطفال. كذلك واجهت الاتصالات غير مرغوبه التسويقية التي تعتدي على خصوصية البيانات الشخصية فتقوم باستغلالها تجاريا. وعلى نفس النهج سارة بعض الدول العربية مثل المشرع التونسي والمغربي والقطري والجزائري. أما بالنسبة للمشرع المصري فهو مازال متأخر في معالجة هذا الامر، بحيث أصبح واجب عليه سرعة اصدار تشريع خاص يواجه به توغل واعتداء التكنولوجيا الحديثة على خصوصية الأشخاص في البيانات والمعلومات الشخصية التي تم معالجتها إلكترونيا. بالرغم أنه في ١٤ أغسطس ٢٠١٨ أصدر المشرع المصري قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، مازال الحاجة إلى تشريع خاص لحماية خصوصية البيانات الشخصية المعالجة إلكترونياً. وهو ما تم في بإصدار المشرع المصري قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ في ١٥ يوليه ٢٠٢٠.

وفي نهاية البحث ننتهي إلى مجموعة من التوصيات وهي على النحو التالي:

١- الحاجة إلى وجود تشريع خاص لحماية خصوصية البيانات الشخصية المعالجة إلكترونياً، يحمي خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً ويضمن في نفس الوقت الحق في الوصول للمعلومات في ضوء مبدأ التناسب والتوازن بين حماية الحق في الخصوصية والحق في الوصول إلى المعلومات وكذلك حماية الأمن القومي للدولة. وقد أصدر المشرع المصري قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، ولكن مازال هذا التشريع بعيداً عن الحماية الكاملة والشاملة لخصوصية البيانات الشخصية المعالجة إلكترونيا، وخاصة فيما يتعلق بحماية خصوصية الأطفال.

٢- ضرورة توافر الضمانات الإجرائية والمراقبة الفعالة من أجل حماية الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً في إطار القانون والممارسة العملية، فقد ترتب على غياب هذه الإجراءات في الإفلات من العقاب على التدخل التعسفي أو غير القانوني. بالإضافة إلى ذلك فإن الضمانات الداخلية التي تفتقر إلى المراقبة المستقلة ثبت عدم فعاليتها في مواجهة أساليب المراقبة غير القانونية أو التعسفية. فيجب أن تنطوي الضمانات المناسبة على المراقبة المدنية المستقلة ومشاركة جميع أجهزة الدولة، من أجل ضمان الحماية الفعالة بموجب القانون.

٣- ضرورة التزام الدول بتطبيق مبدأ الشفافية بشأن ما تم اتخاذه من تدابير لها تأثير على الحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، مما يساعد على التصدي للثغرات والمشاكل القانونية الناتجة عن الممارسة العلمية لحماية حق الخصوصية في البيانات الإلكترونية.

٤- انشاء الهيئة الوطنية لحماية البيانات الشخصية، تتسم بالاستقلالية والمهنية، تراقب وترصد الإجراءات المتعلقة بالبيانات الشخصية. كما تعمل على حل أي نزاع يتعلق بالبيانات الشخصية. وتكون لها دور هام في تطور الحماية القانونية للحق في خصوصية البيانات الشخصية الإلكترونية، وذلك على غرار اللجنة القومية الفرنسية للمعلومات والحريات. وهذا ما نص عليه المشرع المصري في المادة ١٩ من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ بنشأ مركز لحماية البيانات الشخصية كهيئة عامة اقتصادية تتمتع بالشخصية الاعتبارية.

٥- نظرا لتعدد وتنوع البيانات المدرجة في نظم معالجة البيانات الشخصية الإلكترونية، فان تنفيذ المكنات القسرية (المنوطة برجال السلطة العامة) يجب أن يكون متناسبا مع الطابع الخطير للانتهاك، ولا يسبب سوى الحد الادنى من اعاقة الانشطة القانونية للفرد.

كما يجب عند بدء التحريات أن يوضع في الاعتبار – بالإضافة الى القيم المالية التقليدية – كل القيم المرتبطة ببيئة تكنولوجيا المعلومات، مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسارة الاقتصادية، كلفة اعادة بناء تكامل البيانات الشخصية الإلكترونية كما كانت من قبل .

٦- ضرورة تعزيز التعاون الدولي في مجال مكافحة جرائم الاعتداء على خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، وتوفير آلية يمكن من خلالها التنسيق بين القوانين الوطنية والدولية المتشعبة للجرائم الإلكترونية وتشجيع التعاون في مجال تطبيق القانون في مجال حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

٧- ضرورة العمل على تعديل قوانين الإجراءات الجنائية في الدول العربية، لتكون متوافقة ومتلائمة مع التطورات التكنولوجية في عالم الجريمة وخاصة الجرائم المتعلقة بالانتهاك للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

٨- العمل على تأهيل كوادر البشرية لمكافحة هذه النوعية من الجرائم الإلكترونية، بما ذلك تدريب وتأهيل القضاة، وكلاء النيابة العامة، والمحامين، ضباط الشرطة، وأخصائي الأدلة الجنائية والمحققين وأخرين لمكافحة جرائم الانتهاك للحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً.

٩- ضرورة النص في قانون حماية البيانات الشخصية على التزام مقدمي خدمات الإنترنت بحماية البيانات والمعلومات الشخصية للمستخدم للإنترنت فيما يتعلق بالإعلانات التسويقية الموجهة، مع إلزامهم بعدم جمع أو تخزين او استعمال أو أي صوره من صور المعالجة لهذه البيانات أو المعلومات الشخصية للمستخدم إلا بعد الحصول على تصريح منه بذلك، وإلا تلتزم بالإضافة للجزاء الجنائي الالتزام بدفع التعويضات المناسبة لأصلح الضرر المترتب على انتهاك الحق في خصوصية البيانات الشخصية للمستخدم على الإنترنت.

١٠-حق الشخص المستخدم للإنترنت في عدم الحفظ الإلكتروني لبياناته الشخصية إلا حفظاً مؤقتاً، أي أن حفظ البيانات ذات الطابع الشخصي والتي يتم تخزينها على مواقع البحث الإلكترونية يكون حفظها لمدة زمنية محددة معقولة. وذلك بمقتضي الحق في طلب حذف بياناته الشخصية وليس مجرد وقف الحساب الإلكتروني، كذلك حذف كافة الروابط التي تؤدي إلى هذه البيانات الشخصية وحذف كافة النسخ التي أخذت عنها في حالة قيام المسئول عن معالجتها بإتاحتها للجمهور.

١١-يجب وضع ضوابط واضحة وفعالة على الأجهزة الأمنية فيما يتعلق بكيفية استخدام البيانات الشخصية ومدة الاحتفاظ بها، وذلك في ضوء مبدأ حماية خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، وكذلك حق الشخص في الوصول والتبليغ عن بياناته ومعلوماته التي تم معالجتها لدي هذه الأجهزة بما لا يخل بالحفاظ على الأمن القومي للدولة. كذلك يجب أن يتم مراجعة البيانات الشخصية التي قامت بتخزينها الأجهزة الأمنية بواسطة لجنة إشراف مستقلة مع السماح للأشخاص الحق في تصحيح أو حذف بياناتهم الشخصية.

قائمة المراجع

أولا. قائمة المراجع باللغة العربية :

أبي داود سليمان بن الاشعث السجستاني ، سنن ابى داود ، ج٢ ، طباعة مصطفي البابي الحلبي ، القاهرة ، ١٩٥٢.

أحمد بن محمد بن علي الفيومي المقري ، المصباح المنير ، مادة خصص ، طبعة دار الحديث ، القاهرة ، بدون تاريخ نشر.

أحمد فتحي سرور ، الحماية الجنائية للحقوق والحريات ، ط ٢ ، دار الشروق ، القاهرة ، ٢٠٠٠.

أحمد محمد صالح ، هوس الإنترنت ، كتاب الهلال ، القاهرة ، العدد ٦١٥ مارس ٢٠٠٢.

آدم عبد البديع آدم حسين ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٠.

أسامة أحمد المناعسة ، جرائم الحاسب الآلي والإنترنت ، دراسة تحليله مقارنة ، الطبعة الأولي ، دار وائل للنشر ، الأردن ، عمان ، ٢٠٠١.

أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، الطبعة الثالثة ، دار النهضة العربية ، القاهرة ، ١٩٩٤.

أشرف توفيق شمس الدين ، الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ١٩٩٦.

أشرف جابر ، استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصية ، مجلة العلوم الإنسانية ، جامعة الإخوة منتوري ، قسنطينة ، الجزائر ، عدد خاص ، ٢٠١٥.

أماني جمال مجاهد ، الخصوصية وتطبيقات الويب ٠٠٢,٠ ، وكيفية تحقيق المعادلة الصعبة ، كتاب دوري محكم ، الاتجاهات الحديثة في المكتبات والمعلومات ، العدد ٣٥ ، مجلد ١٦ ، يناير ٢٠١١.

أمير موسى ، حقوق الإنسان مدخل إلى وعي حقوقي ، ط١ ، مركز دراسات الوحدة العربية ، بيروت ، ١٩٩٤.

إنتروما إل دي ، ونيسينبام إتش إف ، تقنية التعرف على الوجه ، دراسة استقصائية حول مائل السياسة والتنفيذ ، SSRN eLibray، ٢٠٠٩.

أوليفيا سولون ، مقال تحت عنوان قاعدن بيانات التعرف على الوجه المستخدمة من قبل مكتب التحقيقات الفيدرالية خارج نطاق السيطرة ، جريدة The Guardian ، سان فرانسيسكو ، في ٢٧ مارس ٢٠١٧.

أيمن عبدالله فكري ، الجرائم المعلوماتية ، دراسة مقارنة في التشريعات العربية والأجنبية ، الطبعة الأولى ، مكتبة القانون والاقتصاد ، الرياض ، ٢٠١٥.

بيريسفورد إيه وستاجانو إف ، خصوصية الموقع في الحوسبة المنتشرة ، جمعية الاتصالات التابعة لمعهد مهندسي الكهرباء والإلكترونيات IEEE، ٢٠٠٣.

توبي مندل ، وأندرو بوديفات ، وبن واجنر ، وديكسي هوتن ، ونتاليا توريس ، دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير ، منشورات اليونسكو ، منظمة الأمم المتحدة للتربية والعلوم والثقافة ، باريس ، ٢٠٠١٢.

جمال درويش ، شبكات الحواسب السحابية ودورها في التنمية ، المنتدى السنوي الثاني لتكنولوجيا المعلومات والاتصالات ، دور تكنولوجيا المعلومات والاتصالات في الإسراع بالتنمية في الوطن العربي ، القاهرة ، من ١٣ – ١٥ ديسمبر ٢٠١٥ ، ص ١.

جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠١ ، ص ٦٤.

جي بي رول ، الخصوصية في خطر ، اكسفورد يونيفرستس برس ، ٢٠٠٧.

الحافظ أحمد بن حجر العسقلاني ، فتح الباري بشرح صحيح البخاري ، دار الفكر للطباعة والنشر والتوزيع ، ج ١٢ ، بيروت ، ١٩٩٣.

حسام الدين الأهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي ، بحث مقدم لمؤتمر الكويت الأول للقانون والحاسب الآلي ، كلية الحقوق ، جامعة الكويت ، ١٩٩٤ ، ص ١٠.

– الحق في احترام الحياة الخاصة ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، بدون تاريخ نشر ، ص ٧٦ وما بعدها.

حسن طاهر داود ، جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم الأمنية ، مركز الدراسات والبحوث ، الرياض ، ٢٠٠٠.

حسن محمد ربيع ، حماية حقوق الأنسان والوسائل المستحدثة للتحقيق الجنائي ، رسالة دكتوراه مقدمة إلى كلية الحقوق جامعة الإسكندرية ، ١٩٨٥.

حسني الجندي ، ضمانات حرمة الحياة الخاصة في الإسلام ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ١٩٩٣.

حسين جي ، الخصوصية باعتبارها حرية ، في آر جورجيرسين ، حقوق الإنسان في مجتمع المعلومات العالمي ، دار نشر مطبعة MIT ، كامبريدج ، ٢٠٠٦.

حسين محمود ابراهيم ، الوسائل العلمية الحديثة في الأثبات الجنائي ، دار النهضة العربية ، القاهرة ، ١٩٨١.

رشيد وظيفي ، الاطار القانوني للجريمة الإلكترونية في التشريع المغربي ، ندوة حول الجرائم الإلكترونية المالية ، نظمت من خلال محكمة الاستئناف بالرباط بمناسبة الذكرى المئوية لتأسيسها ندوة علمية ثالثة ، المملكة المغربية ،٥ ديسمبر ٢٠١٣.

ريموند واكس ، الخصوصية ، مقدمة قصيرة جداً ، ترجمة ياسر حسن ، ومراجعة هاني فتحي سليمان ، الطبعة الأولى ، كلمات عربية للترجمة والنشر ، القاهرة ، ٢٠١٣.

زينب غريب ، النظام القانوني للبريد الإلكتروني ، رسالة دكتوراه ، الطبعة الأولى ، طوب بريس ، الرباط ، ٢٠١٦.

سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، دراسة القانون الفرنسي – القسم الأول ، مجلة الحقوق الكويت ، مجلد ٣٥ ، العدد ٣ ، الكويت ، سبتمبر ٢٠١١.

سعيد جبر ، الحق في الصورة ، دار النهضة العربية ، القاهرة ، ١٩٨٦.

سهير منتصر ، النظرية العامة للحق ، بدون دار نشر ، الزقازيق ، مصر، ٢٠٠٦.

سومية عكور ، الجرائم المعلوماتية وطرق مواجهتها : قراءة في المشهد القانوني والأمني ، ورقة علمية مقدمة إلى المتلقي العلمي في الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من ٢ – ٤ سبتمبر ٢٠١٤ ، كلية العلوم الاستراتيجية ، عمان ، المملكة الأردنية الهاشمية ، ٢٠١٤.

شهد حموري ، ريم المصري ، قانون حماية البيانات الشخصية ، ما يمكن تعلمة من تجارب الدول الأخرى ، تشرين الثاني ٢٠١٤ ، بدون دار نشر.

صفية بشاتن ، الحماية القانونية للحياة الخاصة ، دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، الجزائر ، ٢٠١٢.

صوفي أبو طالب ، تاريخ النظم القانونية والاجتماعية ، جامعة القاهرة ، ١٩٧٨.

طارق السرور ، الحماية الجنائية لأسرار الأفراد في مواجهة النشر ، دار النهضة العربية ، القاهرة ، ١٩٩١.

– ذاتية جرائم الإعلام الإلكتروني ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠١.

عادل بسيوني ، تاريخ القانون المصري ، مصر الإسلامية ، مكتبة نهضة الشرق ، القاهرة ، ١٩٨٥.

عادل يحيى ، السياسة الجنائية في مواجهة الجريمة المعلوماتية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠١٤.

عبد الرحمان اللمتوني ، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة ، الندوة العلمية الثالثة التي نظمتها محكمة الاستئناف بالرباط بمناسبة الذكري المئوية لتأسيسها تحت عنوان تأثير الجريمة الإلكترونية على الائتمان المالي ، المملكة المغربية ، ٥ ديسمبر ٢٠١٣.

عبد العزيز محمد سرحان ، الاتفاقية الأوربية لحماية الحقوق الأنسان والحريات الأساسية ، دار النهضة العربية ، القاهرة ، ١٩٦٦.

عبد العظيم وزير ، حول مشروع ميثاق الإنسان والشعب في الوطن العربي ، المجلد الأول ، ط١ ، دار العلم للملايين ، بيروت ، ١٩٨٨.

عبد الفتاح حجازي ، الحماية الجنائية لنظام التجارة الإلكترونية ، الجزء الثاني ، دار الفكر الجامعي ، القاهرة ، ٢٠٠٢.

عبد الفتاح مراد ، شرح جرائم الكمبيوتر والانترنت ، البهاء للبرمجيات والكمبيوتر للنشر الالكتروني ، الاسكندرية ، بدون سنة نشر.

عبد اللطيف هميم محمد ، جرائم الاعتداء على الحياة الخاصة وعقوبتها في الشريعة والقانون ، رسالة ماجستير ، كلية الشريعة والقانون ، جامعة الأزهر ، القاهرة ، ١٩٨١.

عبد الله حسين على محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الثانية ، الأمارات العربية المتحدة ، دبي ، دار النهضة العربية ، القاهرة ، ٢٠٠٢.

عبد الناصر زياد هياجنه ، الميراث الرقمي : المفهوم والتحديات القانونية ، المجلة الدولية للقانون ، كلية القانون ، جامعة قطر ، ٢٠١٦.

عبد الهادي فوزي العوضي ، الجوانب القانونية للبريد الإلكتروني ، دار النهضة العربية ، القاهرة ، ٢٠٠٥.

علاء الدين منصور المغايرة ، الأوجه الحديثة للجرائم المعلوماتية ، دراسة مقارنة ، رسالة ماجستير ، كلية الحقوق ، جامعة الحكمة ، بيروت ، ٢٠٠٠.

على عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونياً ، بحوث مؤتمر القانون والكمبيوتر والانترنت ، بالتعاون مع مركز الأمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة المجلد الثاني من ١ إلى ٣ مايو ٢٠٠٠ ، جامعة الأمارات العربية المتحدة ، كلية الشريعة والقانون ، الطبعة الثالثة ، ٢٠٠٤.

– الحماية الجنائية لبرامج الحاسب الألي، دار الجامعة الجديدة ، الاسكندرية ، ١٩٩٧ .

عمر أبو بكر يونس ، الجرائم الناشئة عن استخدام الإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٤.

عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٩٥.

عمر محمد أبو بكر يونس ، الجرائم الناشئة عن استخدام الإنترنت ، الأحكام الموضوعية والإجرائية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤.

عمرو حسبو ، حماية الحريات في مواجهة نظم المعلومات ، دار النهضة العربية ، القاهرة ، ٢٠٠٠.

كامل السعيد ، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا ، المؤتمر السادس للجمعية المصرية للقانون الجنائي ، ٢٥ – ٢٨ أكتوبر ١٩٩٣ ، دار النهضة العربية ، القاهرة ، ١٩٩٣.

محروس نصار غايب ، الجريمة المعلوماتية ، in formational crime ، المعد التقني ، الانبار ، العراق ، ٢٠١١.

محمد السقا ، فلسفة وتاريخ القانون المصري ومراحل تطوره ، دار النهضة العربية ، القاهرة ، ٢٠٠٠.

محمد الطاهر ، الحريات الرقمية ، المفاهيم الأساسية ، مؤسسة حرية الفكر والتعبير ، الحريات الرقمية ، القاهرة ، ٢٠١٣.

محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ، الجريمة المعلوماتية ، الطبعة الرابعة ، دار الثقافة للنشر والتوزيع ، المملكة الأردنية الهاشمية ، عمان ، ٢٠١١.

محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح ، طبعة دار الحديث ، القاهرة ، ص ١٠٦. المعجم الوجيز ، مجمع اللغة العربية ، طبعة وزارة التربية التعليم جمهورية مصر العربية ، ١٩٩٣.

محمد بن جرير ، الأمام الطبري ، جامع البيان في تأويل القرآن ، تهذيب صلاح الخالدي ، الطبعة الأولى ، دار القلم والدار الشاميه ، بيروت ، ١٩٩٧.

محمد ثامر مخاط ، الحماية القانونية القضائية لحق الانسان في الخصوصية ، جامعة ذي قار ، الجزائر، موقع الحوار المتمدن ، ٢٠١٥.

محمد حسين منصور ، المسئولية الإلكترونية ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠٠٣.

محمد حماد مرهج الهيتي ، الجريمة المعلوماتية نماذج من تطبيقاتها ، دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني ، دار الكتب القانونية ، القاهرة ، ٢٠١٤.

محمد راكان الدغمي ، حماية الحياة الخاصة في الشريعة الإسلامية ، دار السلام للنشر والتوزيع ، ط١ ، القاهرة ، ١٩٨٥.

محمد سامي الشوا ، جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال ، بحث مقدم للمؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ، البرازيل ، ريو دي جانيرو ، في الفترة من ٤ إلى ٩ سبتمبر ١٩٩٤.

محمد سعيد الدقاق ، التشريع الدولي في مجال حقوق الانسان ، المجلد الثاني ، دراسات حول الوثائق العالمية والإقليمية ، إعداد د. محمد شريف بسيوني وآخرون ، دار العلم للملايين ، بيروت ، ١٩٨٩.

محمد طاهر ، أ. حسن عبد الحميد ، أحمد عزت ، الحق في الاتصال بين التقنية والقانون ، ورقة تعريفية ، مؤسسة حرية الفكر والتعبير ، القاهرة ، ٢٠١٣.

محمد عبد المحسن المقاطع ، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي ، ذات السلاسل للطباعة والنشر ، الكويت ، ١٩٩٢.

– نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر ، مؤتمر الكويت الأول للقانون والحاسب الألي ، كلية الحقوق ، جامعة الكويت ، الطبعة الأولى ، ١٩٩٤.

محمد عيسى ، الميراث الإلكتروني ، مقال منشور على جريدة الأهرام المصرية ، بتاريخ ١٥ مارس ٢٠١٣.

محمد محمود الكمالي ، ورقة بحثية حول بعض قضايا جرائم تقنية المعلومات من محاكم دولة الأمارات العربية المتحدة ، المؤتمر الاقليمي الاول لحماية برنامج الحاسوب وجرائم الانترنت ، ٢٤ ألي ٢٥ اكتوبر ٢٠١٠ ، عمان ، الاردن.

محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، ١٩٩٣.

محمود شريف بسيوني ، خالد محي الدين ، الوثائق الدولية والإقليمية المعنية بحقوق الانسان ، المجلد الثالث ، دار النهضة العربية ، القاهرة ، ٢٠٠٣.

محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ، الطابعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٩٤.

مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الإلكترونية ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠٠١.

مروك نصر الدين ، الحق في الخصوصية ، موسوعة الفكر القانوني ، الجزائر ، بدون تاريخ نشر.

المنظمة الدولية لحماية الخصوصية ، الخصوصية وحقوق الإنسان ، دراسة استقصائية دولية لقوانين وتطويرات الخصوصية ، ٢٠٠٦.

نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادية ، دراسة نظرية وتطبيقية ، دار النهضة العربية ، القاهرة ، ٢٠٠٤.

نعيم عطية ، حرمة الحياة الخاصة في القانونين المصري والفرنسي ، مجلة العلوم الإدارية ، السنة ٢٣ ، العدد الأول ، القاهرة ، ١٩٨٠.

نعيم مغبغب ، مخاطر المعلوماتية والإنترنت ، المخاطر على الحياة الخاصة وحمايتها ، دراسة مقارنة ، بدون دار نشر ، بيروت ، ١٩٩٨.

نور سليمان ، نهاية الخصوصية : الحريات الشخصية وأمن الدول في عصر البيانات الضخمة ، تحليل المستقبل ، مجلة اتجاهات الأحداث ، المجلد الأول ، العدد ٥ ، مركز المستقبل للأبحاث والدراسات المتقدمة ، الأمارات العربية المتحدة ، أبوظبي ، ديسمبر ٢٠١٤.

هدى حامد قشقوش ، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٠.

– جرائم الحاسب الإلكترونية في التشريع المقارن ، دار النهضة العربية ، القاهرة ، ١٩٩٢.

– الحماية الجنائية للتجارة عبر الإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٠.

– الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني ، مؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون ، جامعة الأمارات العربية المتحدة ، ٢٠٠٠.

هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة بأسيوط ، ٢٠٠٦.

هلالي عبد الله أحمد ، الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء اتفاقية بودابست في ٢٣ نوفمبر ٢٠٠١ ، دار النهضة العربية ، القاهرة ، الطبعة الأولى ، ٢٠٠٣.

وفاء حلمي ابو جميل ، محاضرات في نظرية الحق ، ٢٠٠٧ ، بدون دار نشر ، الزقازيق ، مصر.

وليد سليم النمر ، حماية الخصوصية في الإنترنت ، دار الفكر الجامعي ، الاسكندرية ، ٢٠١٧.

وليد طه ، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست ، قطاع التشريع بوزارة العدل جمهورية مصر العربية ، القاهرة ، بدون دار نشر أو تاريخ نشر.

يونس عرب ، دور حماية الخصوصية في تشجيع الاندماج الرقمي ، ورقة عمل ، ندوة أخلاق المعلومات ، نادي المعلومات العربي ، ١٦ – ١٧ اكتوبر ٢٠٠٢ ، عمان.

– قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان ، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية ٢ – ٤ أبريل ٢٠٠٦ ، هيئة تنظيم الاتصالات ، مسقط – سلطنة عمان.

Orin Kerr ، المرشد الأمريكي الصادر عام ١٩٩٤م ، المعد من قبل قسم جرائم الحاسب الآلي والملكية الفكرية بإشراف الأستاذOrin Kerr ،المعدل سنة ٢٠٠٢ الذي تضمن تطبيقا للقانون الوطني الأمريكي الصادر في ٢٠٠١/١٠/٢٦.

ثانيا. قائمة المراجع باللغة الاجنبية :

A. LUCAS, Le droit de l'informatique, éd., PUF, ١٩٨٧, Paris, p. ٢١ .

A. V. MARTINEZ, Les libertés de opinion y de information, éd., Andres Bello, Paris, ١٩٩٢, p. ٢١٩.

B. BDSG, Zuletzt geandet durch, art. ٣ G.V., ١٤ aout ٢٠٠٩, I, ٢٨١٤, Zweck dieses Gesetzes ist es, den Einzelnen davorzu schutzen, dass er durch den Umgang mit seinen personenbezgenen Daten in seinem Personlichkeitsrecht beeintrachtigt .

B. N WALDEN & R.N SAVAGE, Data protection and privacy and law should organazations be protected, in international and comparative law and comparative law Quartely, Vol ٣٧ part ٢, ١٩٨٨, p. ٣٣٧ .

B. TABAKA & Y. TESAR, Loi informatique et libérés, un nouveau cadre juridique pour le traitement des données à caractère personnel, Disponible sur sité, www.foruminternet.org, octobre ٢٠٠٤.

B. WILLIAM, Le système de traitement des infractions constatées et la protection des données personnelles, mémoire de DEA informatique et droit, faculté de droit, université de Montpellier I, ٢٠٠٣, p. ١٥ .

C. LEVIN & J. MCCAIN, Majority and Minority, Online advertising and hidden hazards to consumer security and data privacy, Staff report, ١٥ May, ٢٠١٤, p. ١٧ .

C. THIERACHE & M. BERGUIG, L'oubli numérique est – il de droit face à une mémoire numérique illimitée ? Rapport, ٢٥ mai ٢٠١٠, revue Lamy droit de l'immatériel, juillet ٢٠١٠, N° ٦٢, PP. ٣٤, ٣٥ .

D. LOWE, Surveillance and international terrorism intelligence exchange: balancing the interests of national security and individual liberty, Terrorism and political violence, August, ٢٠١٤, p. ٤.

E. KEISER, MLB. Com distributing Fake AV Malware via compromised AD network, Silversky altitude blog, ١٨ jun ٢٠١٢.

E. MAILJINK BULK, Spamming, pollupostage, porriel, www.traidnt.net, ٢٠١٣.

E.–M, Le financement des logiciels – peuton louer ou donner financièrement à bail Un Logiciel? Gazette du Palais, Paris, ١٩٨٥, P. ٣٩٦.

F. COLANTONIO. La protection du secret des courriers électroniques en Belgique : Aspects techniques, D.E.S en criminologie, Université liege, Faculté de droit, ٢٠٠١ –٢٠٠٢, p. ٩ .

F. PARRAIN, Secret des correspondances et courrier électronique, disponible sur sité, www.adno-avocats.com, Paris, ٢٠١٢.

G. ANTHONY, Les rapports entre le secret professionnel et le droit de la protection des données personnelles, mémoire de DEA informatique et droit, Fac droit; Univ Montpellies I, ٢٠٠١, p. ٦٢ .

H. CROZE, L'apport du droit pénal à la théorie général propos de la loi N° ٨٨-١٩ DU DROIT DE L'informatique ٥ jan ١٩٨٨ relative à la fraude informatique, éd, J.C.P, ١٩٨٨, I. doct, p. ٣٣٣٣ .

H.F. SHATTUCK, Right of privacy, National text Book Company, U.S.A, ١٩٧٧, P. ١٩٧.

J – P. MOINY, Facebook au regard de la protection des données, Revue Européenne de droit de la consommation, ٢٠١٠, p. ٢ .

J. BEDEREDE, Données personnelles dans L'entreprise : quelles précautions faut – il prendre aujourd'hui, art disponible sur www.entreprise-et-droit.com .

J. BERMAN & D. MULLIGAN, Privacy in the digital age : work in progress, Nova law review, Vol ٢٣, N°٢, winter ١٩٩٩, The internet and law, p. ٤ .

J. CHAMPLAIN, Auditing Information Systems. Hoboken, New jersey , John wiley of sons, Icove, D, Segar.K& Vonstorch ,W et al,١٩٩٩&Wright, ٢٠٠٠d.

J. DEVEWE; Infraction en matière informatique, N° ٣١-٣٣, ١٩٨٨-٩-٤٦٢, jurissclasseur pénale, art. ٣٦٢-٢ Chamoux: la loi sur la fraude informatique, de nouvelles incriminations, J.C.P, ١٩٨٨, I. DOCT, P. ٣٣٢١.

J. MAC DONALD, The law of freedom of information BBC press, ٢٠٠٣, p. ٤٠.

J. PARDEL & M. DANTI – JUAN, Le droit pénal, le droit pénal special, éd., Cujas, ٢٠١٤, Paris, N ٢٠٥ ets .

J. PRADEL, Droit pénal, éd., ٢٠١٥, Dalloz, Paris, p. ٨٢٧.

J. RIVERO, Le conseil constitutionnel et les libertés, Paris, ١٩٨٤, pp. ٧١ – ٨٥.

J. ROSENOER, Cyber law, the law of internet, Springer – Verlag, New york, ١٩٩٧, p. ١٧٠ .

J. SMEDINGHOFF, On line law, The spa`s legal guide to donning business on the internet, The Software publishers Association, ١٩٩٦, p. ٤٨١.

L. EDWARDS & C. WAELDE, Law and the internet, Regulating cyber space, Hart Publishing, Exford, ١٩٩٧, P. ٢٣١.

L. SWEENEY, Comments from Latanya Sweeney and the Data Privacy Lab, Ph.D., on Standards of privacy of individually identifiable health information, Carnegie Mellon University, ٢٠١١ .

M. – L. RASST, Droit pénal spécial, éd., Dalloz, Paris, ١٩٩٧, p. ٣٦٩.

M. CAHEN, Déxès : les e-mails sont des données personnelles, Paris, ٢٠١٣, p. ٢., www.clic-droit.com.

- Que deviennent les emails, les comptes Webmail et les sites web après un décès? A qui appartiennent – ils ? Rentrent-ils dans la succession ? Paris, ٢٠١٣, p. ٢. www.murielle-cahen.com.

M. DE MONTECLER, Le droit @ l'heure des réseaux sociaux, Mémoire, HEC, Université Paris I– Panthéon-Sorbonne Paris, ٢٠١١, P. ٣٨ .

M. FORST, E- Law, Appellate court cases about information technology, by Montclair, enterprises san Francissco, ١٩٩٩, p. ١٦ .

M. GODFRAIN, Relative à la fraude informatique, ١٩٨٦, ٨٧, N° ٧٤٤, p. ١٣ .

M. NAVARAJ, The wild wild web : YouTube ads serving malware, Bromium labs call of the wild blog, ٢١ feb, ٢٠١٤.

M.S LALANDE, L'adresse IP de votre ordinateur, une donnée personnelle relevant du régime communautaire de protection, art disponible sur: www.droit-ntic.com, la date de mise en ligne est: ٩ dec ٢٠٠٣.

M.W MENDES, La législation pénale en matière d'ordinateurs et les mesures de sécurité aux Etats – Uni, Droit de le informatique numéro spécial, ١٩٨٥, p. ٤٠ .

M-P FENOLL – TROUSSEAU & G. HAAS, Jurisclasseur communication fascicule ٤٧٣٥ protection des données à caractère personnel – vie privée et communication électronique, Paris, ٢٠٠٥, P.٣٧ .

N. IVALDI & P. VINCENT, Cyber surveillance des salariés chartes informatiques, disponible sur sité, www.caproli-avocats.com, septembre ٢٠٠٥ .

N. MALLET – POUJOL, Protection de la vie privée et des données à caractère personnel, étude disponible sur sité. www.educent.education.fr. ٢٠٠٧, p. ٣٢

P. KAYSER, La protection de la vie privée par le droit, ٣ ed, Economica, ١٩٩٥, Paris, pp. ٣٥٦ – ٣٥٩.

P. SARGOS & M. MASSE, Le droit pénal spécial ne de l'informatique, Travaux de sciences criminelles de Poitiers. Éditions Cujes, Paris, ١٩٨٥, P. ٣٦ .

P. VANLANGENDONCK, Le dossier médical électronique: problème de vie privée et de responsabilité, l'ASBL; Droit nouvelles technologies, art disponible sur sité; www.droit-technologie.org. Paris, ١١ mai ٢٠٠٠. P.٢, ٣.

Ph. CROUZILLACQ, Les E- mails peuvent reposer en pais, Paris, ٢٠١٣., www.٠١net.com .

R. ANDRE, La rapport Assemble nationale, N°١٠٧٨, Paris, ١٩٨٧ – ١٩٨٨, p. ٥ .

R. GASSIN, La protection pénale d'une universalité de fait en droit français, Act. Legis. Dalloz, N°٤٥, ١٩٨٨, P. ١٢.

R. MERLE & A. VITU, Trait de droit criminel, droit pénal spécial, éd., Cujas, Paris, tome ١١ , n°٢٠٣١ .

S. FORDEN & K. GULLO, Google judge accepts ٢٢.٥ s Milion FTC privacy settlement, Bloomberg, ١٧ Nov ٢٠١٢ .

S. JIGAR & A. BRUNE, Authentification d'utilisateur, Gestion des Identites, Université Sciences et Technologies, Bordeaux I, ٣٥١ Cours de la lib eration, ٣٣٤٠٠ talence. Décembre ٢٠٠٧, p.٦.

S. LOUVEAUX, Comment concilier le commerce électronique et la protection de la vie privée, en ligne :

S. PENA PORTA, Les données personnelles et leur traitement, art disponible sur.,

http://www.crid.be/pdf/crid/٤٧١٠.pdf. Paris, ٢٠٠٥.

S. ULRICH, Computer crimes and other crimes against information technology, R.I.D.P, ١٩٩٤, Vol. ٦٢, p. ١٠٣٦.

S: LOUVEAUX, Comment concilier le commerce électronique et la protection de la vie privée ? Droit des technologies de l'information. Regards prospectifs, sous la direction d'Etienne Montero, Cahier du centre de recherché informatique et droit, Bruylant, Bruxelles, ١٩٩٩, PP. ١٥١ – ١٥٢ .

V. THIBAULT & W. ETIENNE, Le droit de l'internet et de la société de l'information : droits européen, Belge et Français, éd., Larcier, Paris, ٢٠٠١, p. ٦١١ .

W.A BRAIN, Legal analysis of a single market for the information society, citation European, ٢٠١١, p. ٤; see also: Guidelines on the protection of privacy and trans border flows of personal data, ٢ Dec ٢٠١٣ .