المواجهة الجنائية للمعالجة والاستغلال غير المشروع للبيانات الشخصية على ضوء القانون رقم ١٥١ لسنة ٢٠٢٠

"دراسة تحليلية-مقارنة"

د. محمد السعيد القزعة

دكتوراه في القانون الجنائي

كلية الحقوق- جامعة طنطا

(ISSN: 2537- 0758)

المواجهة الجنائية للمعالجة والاستغلال غير المشروع للبيانات الشخصية على ضوء القانون رقم ١٥١ لسنة ٢٠٢٠ "دراسة تحليلية-مقارنة"

د. محمد السعيد القزعة

الملخص باللغة العربية

أضحت حماية البيانات الشخصية أحد أهم شواغل الإنسان في العصر الرقمي، حيث برز دورها الجوهري وأهميتها الكبيرة على عديد من الأصعدة، وأصبحت لها قيمة آخذه بالنمو بكل الطرق والوسائل، ونابعت تلك الأهمية للبيانات من خلال وفرتها مع القدرة على التعامل معها وتوظيفها في شتى المجالات بحسب الحاجة إليها، وتتنوع مصادر الحصول على تلك البيانات مع توغل التكنولوجيا الرقمية في حياة الناس، فمثلاً يتصور الناس بأن شركات كجوجل وفيس بوك وتوتير ويوتيوب وغيرهم تقدم خدماتها للجمهور بلا مقابل مالي، بيد أن الواقع بأن المتعاملين مع تلك الشركات وكافة التطبيقات عبر الإنترنت يدفعون لقاء حصولهم على تلك الخدمات ثمناً باهظاً يتمثل في بياناتهم الشخصية، التي يتم الإفصاح عنها مقابل التمتع بتلك الخدمات، وانعكاساً لتلك الأهمية فقد تعرضت في هذا البحث لبيان ماهية البيانات الشخصية والحاجة الماسة لحمايتها، والأسس التي تسند عليها تلك الحماية، وأوضحت أبرز الجرائم المتعلقة بالمعالجة غير المشروعة للبيانات الشخصية، وأبرزت الفوارق بين المعالجة غير المشروعة للبيانات الشخصية العادية، والبيانات الشخصية الحساسة وما استتبعه من تشديد العقاب في الأخيرة، كما بينت الجزاء العقابي المترتب على الإخلال بشروط الجمع والمعالجة والاحتفاظ بالبيانات في غير الأحوال المصرح بها قانوناً، وكذلك نتيجة الاعتداء على حقوق المعني بالبيانات الشخصية والآثار الناجمة عنها.

وتضمن البحث أهمية المواجهة الجنائية لجرائم الاعتداء على البيانات الشخصية الواقعة عبر الحدود لسهولة وقوع هذا النوع من الجرائم عبر الإنترنت، لاسيما وأن البيئة الرقمية تتميز بأنها لا تحدها قيود ولا تعترف بالحدود؛ لذلك اشترطت كافة النظم القانونية المعينة بحماية البيانات الشخصية العديد من الشروط التي يتعين مراعاتها لدى حركة البيانات عبر الحدود، ورتبت عقوبات تختلف حدتها من تشريع لآخر، وفقاً لمدى حرصها على حماية البيانات الشخصية وإعلائها لحق الأفراد في الخصوصية، وألمحت إلى أن تطور أساليب الدعاية والتسويق أدت إلى أن أصبحت البيانات الشخصية هي الأساس الذي يتم بناء أساليب الدعاية عليه؛ غير أنه صاحب استخدامها في التسويق الإلكتروني اعتداء مُتزايد على خصوصية الأشخاص عن طريق الرسائل التسويقية

الموجهة وغير المرغوب فيها؛ لذلك كانت الحاجة ملحة إلى تجريم مخالفة أحكام التسويق الإلكتروني.

وخلصت الدراسة إلى قانون حماية البيانات الشخصية المصري هو خطوة على الطريق الصحيح في حماية البيانات الشخصية، جاء بالعديد من السبل للمواجهة الجنائية للاعتداء على البيانات الشخصية، عبر تجريمه أفعال المعالجة غير المشروعة للبيانات الشخصية، وشملت عدداً من التوصيات وتضمنت مقترحات تهدف لإجراء تعديل تشريعي في القانون يتلافى أوجه النقص التي خرجت بها الصورة الحالية للقانون، وذلك بمد مظلة الحماية الجنائية لكافة البيانات الشخصية سواء المكتوبة أو المحفوظة بشكل غير إلكتروني أو المعالجة إلكترونياً، وشمول الحماية الجنائية البيانات الشخصية للأشخاص المتوفين، وكذلك الأشخاص الاعتبارية، وضرورة التحديد الدقيق للحالات المصرح بها قانوناً التي تشمل معالجة البيانات الشخصية للشخص المعني دون موافقته، وضرورة وضع إطار عام للتعامل مع البيانات الشخصية للأغراض التجارية وعدم قصرها على التسويق الإلكتروني.

كلمات مفتاحية: البيانات الشخصية– العصر الرقمي– المعالجة غير المشروعة للبيانات– نقل البيانات عبر الحدود– التسويق الإلكتروني.

Abstract:

The protection of personal data has become one of the most important human concerns in the digital age, as its essential role and great importance have emerged on many levels, and it has an expanding value in all ways and means, and that importance stems from data through its abundance with the ability to deal with it and employ it in various fields. According to the need for it, and the sources of obtaining this data vary with the penetration of digital technology into people's lives. For example, people think that companies such as Google, Facebook, Twitter, YouTube, and others provide their services to the public without financial compensation. However, the reality is that the audience of those dealing with these companies and all applications via the Internet pay A high price for obtaining these services is represented in their personal data that was disclosed in exchange for enjoying these services, and as a reflection of that importance, I presented an explanation of what personal data is, the urgent need for its protection, and the foundations on which that protection is based, and it explained the most prominent crimes related to the illegal processing of personal data and highlighted the

(ISSN: 2537- 0758)

differences Between the unlawful processing of ordinary personal data and sensitive personal data and the consequent harsher punishment in the latter, it also showed the punitive penalty resulting from breaching the conditions of collection, processing and data retention, as well as the result of the violation of the rights of the person concerned with the personal data and the resulting effects.

And she showed the importance of criminal confrontation for crimes of transgression of personal data that occur across borders because of the ease of occurrence of this type of crime via the Internet, given that the digital environment is characterized by that it is not bounded by restrictions and does not recognize borders. The movement of data across borders, and arranged criminal penalties that vary in severity from one legislation to another according to the extent of its keenness to protect personal data and uphold the right of individuals to privacy, and hinted that the development of advertising and marketing methods led to personal data becoming the basis on which advertising methods are built; However, its use in e-marketing was accompanied by a massive attack on people's privacy through unsolicited marketing messages. Therefore, there was an urgent need to criminalize violating the provisions of electronic marketing.

The study concluded that the Egyptian Personal Data Protection Law is a step on the right path in the protection of personal data, and it came with many ways to criminally confront the assault on personal data, by criminalizing acts of illegal processing of personal data, and showed the need for a legislative amendment in the law to avoid the deficiencies that emerged. The current picture includes the extension of the criminal protection umbrella for all personal data, whether written or saved in a non-electronic form, or processed electronically, and the criminal protection of personal data includes deceased persons, as well as legal persons, and the need for accurate identification and legally authorized cases that include processing the personal data of the person concerned without his consent And by setting a general framework for dealing with personal data for commercial purposes and not limiting it to electronic marketing.

Keywords:

Personal data- The digital age- Unlawful processing of data- Cross-border data transfer- E-Marketing.

مقدمة

تشغل البيانات الشخصية للأفراد وسبل حمايتها أهمية متزايدة في الواقع القانوني في الآونة الأخيرة؛ وذلك لتنامي حملات الاعتداء عليها، وما تمثله من انتهاك صريح لحق الإنسان في الخصوصية، والتي تشمل حماية حق الأفراد من التدخل في حياتهم الخاصة أو نشر معلومات عنهم أو عن ذاويهم، فقد أثر تسارع التقدم التكنولوجي في العقود الأخيرة على حقوق الإنسان وحرياته وبصفة خاصة الحق في الخصوصية، وذلك إبان ظهور الحواسيب والإنترنت، وأصبح هذا التأثير يلمس أشياء أكثر دقة لدى الأفراد وعلى رأسها البيانات الشخصية، فبالرغم من أهمية مشاركة البيانات الشخصية في عديد من الأحيان والتي قد تسفر إلى تحقيق فوائد، وغالبًا لا يخلو الأمر من ضرورة مشاركتها للتفاعل مع الأشخاص الآخرين في المجتمع الحالي، لكن مشاركة تلك البيانات ليست بمنأى عن المخاطر لاسيما وأنها يمكن أن تكشف الكثير عن المعنيين بها وعن أفكار حياتهم، وبات من السهل استغلال هذه البيانات بسهولة لإيذاء أصحابها، وهذا ما يشكل خطراً على الأفراد والمجتمعات.

لذلك بدأ الاهتمام أكثر بحماية البيانات الشخصية وتضافرت الجهود القانونية لسد الفراغ التشريعي المنظم لتكنولوجيا الإعلام والاتصال وتأثيرها السلبي على الإنسان وحقوقه المتعلقة بالخصوصية، وانتهاك حرمته بكشف بياناته الشخصية وجعلها عارية أمام الجميع على الإنترنت؛ لذا لزم تحديث القوانين ذات الصلة لمعالجة واقع اليوم وما أسفر عنه الحاسب الآلي والإنترنت من مثالب على خصوصية الأفراد، فمع تطور استعمال الأفراد بياناتهم الشخصية عبر الإنترنت في مختلف المجتمعات ازدادت الحاجة إلى حماية تلك البيانات التي يتم مشاركتها كل يوم ليس فقط عبر مواقع التواصل الاجتماعي وإنما في البيئة الرقمية بشكل عام ومن خلال الوسائط الإلكترونية، لاسيما وأن القوانين التي تهتم بالخصوصية غير قابلة للتكيف وإسباغ الحماية الكافية عليها بما يتناسب مع تحديات عالم اليوم.

وحيث إن القانون هو مرآة تعكس واقع المجتمع، ويفترض فيه أن يعبر تعبيراً صادقاً عن حاجات أفراده، فقد اقتضت الضرورة وتماشياً مع القفزات المتسارعة فى النظم المعلوماتية وآثارها السلبية على خصوصية أفراد المجتمع، وبشكل خاص على البيانات الشخصية؛ نتيجة لذلك أصدر المشرع المصري قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ والمنشور بالجريدة الرسمية- العدد ٢٨ مكرر (هـ)- في ١٥ يوليه

(ISSN: 2537- 0758)

سنة ٢٠٢٠ في محاولة منه فرض سياج من الأمان على البيانات الشخصية لعموم أفراد المجتمع المصري، وإن كان قد جاء متأخراً للغاية فى إقراره لهذا القانون، إلا أنه محاولة محمودة منه لتدارك تأخيره فى إصدار هذا القانون، لمواكبة التطورات فى مجال التحول الرقمي المقترن بالتطور التكنولوجى، بشكل ينعكس إيجابياً على رفع مستويات أمن الفضاء المعلوماتى، والتكريس لحماية البيانات الشخصية لعموم أفراد المجتمع، والمواجهة الجنائية لآليات المعالجة والاستغلال غير المشروع لها؛ لذلك كانت هناك ضرورة حتمية لإصدار هذا القانون.

أولاً- أهمية الدراسة:

تتجلى أهمية الدراسة في محاولة الإحاطة بهذا الموضوع وتسليط الضوء على التشريعات الجنائية التي وفرت سبل للمواجهة الجنائية لصور الاعتداء على البيانات الشخصية، وبيان مدى كفايتها في تحقيق حماية فاعلة للبيانات الشخصية للأفراد، من خلال العقوبات التي قررتها رداعاً لكل من تسول له نفسه مقارفة أياً من الجرائم المتعلقة بالاعتداء عليها، في ظل الانتشار الكثيف للإتجار بالبيانات الشخصية، لا سيما مع التطور الهائل في مجال الاتصالات وتكنولوجيا المعلومات والتي من خلالها أضحت البيانات الشخصية للأفراد في المتناول، وقد تستغل تلك البيانات بشكل يؤثر سلباً على المعنين بها سواء عبر المعالجة غير المشروعة لها، أو نقلها وتداولها خارج حدود الدولة، أو استغلالها غير المشروع في التسويق الإلكتروني الموجهة، وتكمن أسباب الموضوع في الأهمية الكبيرة التي تمثلها البيانات الشخصية في حياة عموم البشر، والتطور الهائل الذي شهدته الاتصالات وتكنولوجيا المعلومات وما استتبعه من تأثيرات سلبية من تنامي الاعتداءات على خصوصية الأفراد، فلا يكاد يمر يوماً إلا وهناك المئات ويصح القول آلاف حالات انتهاك خصوصية الأفراد عبر الإنترنت، ومن خلال الوسائط الإلكترونية، وقد طفى إلى السطح مؤخراً الاعتداء على البيانات الشخصية كأحد أخطر صور انتهاك حق الأفراد في الخصوصية عبر الإنترنت، ولم يعد الأمر قاصراً على انتهاك الخصوصية بل محاولة الأضرار بالمعنين بتلك البيانات؛ لذلك أثرت التعرض لهذا الموضوع في محاولة للبحث عن سبل المواجهة الجنائية للاعتداء عليها في التشريع المصري والمقارن.

ثانياً- إشكاليات الدراسة:

تتمثل إشكاليات الدراسة في بيان مدى قدرة قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ على تحقيق مواجهة جنائية فاعلة لآليات المعالجة والاستغلال غير المشروع للبيانات الشخصية من عدمه، ومدى تناسب العقوبات الجنائية

المقررة للجرائم التي تضمنها القانون، كما تتمثل في بيان هل تم تحديد مفهوم الخصوصية تحديداً دقيقاً في ظل التشابك الحاصل بين حماية البيانات الشخصية وحق الإنسان في تداول البيانات والمعلومات، وتداخل بعض الصور التجريمية التي جرمها المشرع المصري بين قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠ وقانون مكافحة جرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨، وهل تم وضع إطار قانوني لتذليل قصور القانون في معالجة بعض مواطن الخلل الذي شابه مثل حماية كافة البيانات الشخصية المعالجة إلكترونياً منها وغير المعالجة إلكترونياً، وحماية بيانات الأشخاص الاعتبارية وذلك اقتداءً بالتشريعات المقارنة بهدف الوصول إلى سُبل تعزيز المواجهة الجنائية للاعتداء على البيانات الشخصية في التشريع المصري.

ثالثاً- صعوبات الدراسة:

تكمن صعوبة الدراسة فيما يلي:

حداثة قانون حماية البيانات الشخصية المصري ١٥١ لسنة ٢٠٢٠ وكذلك قوانين حماية البيانات في معظم الأنظمة العربية، نجم عن ذلك من وجود نادرة نسبية في الشروحات التي تناولت هذا الموضوع، وقلة التطبيقات القضائية التي تعرضت له سواء في مصر أو في الأنظمة العربية مقارنة بنظيرتها الغربية صاحبة الريادة في حماية البيانات الشخصية كفرنسا، ومما زاد الأمر صعوبة عدم صدور لائحة تنفيذية لقانون حماية البيانات الشخصية المصري ١٥١ لسنة ٢٠٢٠على الرغم من أن القانون أحال إليها في العديد من المواضع تحديد الإجراءات والضوابط والمعايير المتعلقة بمعالجة وحفظ وتأمين البيانات، وكذلك عدم إنشاء مركز حماية البيانات الشخصية، لاسيما وقد أناط القانون به مهام يصعب القيام بها في ظل عدم وجوده.

رابعاً- منهج الدراسة:

تعتمد الدراسة على المنهج الوصفي التحليلي المقارن في دراسة نصوص القواعد القانونية ذات الصلة بموضوع الدراسة الواردة القانون الفرنسي، مقارنة بالقانون المصري وبعض القوانين العربية مثل كالنظام السعودي لبيان مدى إسهام كل منها في إيجاد الحلول المناسبة لما يثيره موضوع البحث من إشكاليات لدى إعماله عليها.

وقد استخدمت الدراسة المنهج المقارن في بعض مواطن الرسالة وبما يخدم الغاية من الدراسة مستعينًا بالقانون الأمريكي وبعض التشريعات العربية الأخرى كالقانون حماية خصوصية البيانات الشخصية القطري ١٣لعام ٢٠١٦، والقانون المغربي المتعلق

(ISSN: 2537- 0758)

بمعالجة البيانات ذات الطابع الشخصي ٢٠٠٩ الصادر عام ٢٠٠٩، لكونهما أسبق من التشريع المصري في إقرار تشريع معني بحماية البيانات الشخصية.

وكل ذلك من أجل التواصل لآليات المواجهة الجنائية لتلك التشريعات لجرائم المعالجة والاستغلال غير المشروع للبيانات الشخصية، ولبحث مدى تقارب القوانين العربية التي تعنى بحماية البيانات الشخصية، فيما بينها، ومدى انسجامها مع القوانين الدولية ذات الصلة، من خلال تبيان الالتقاء والاختلاف أينما وجدت

خطة الدراسة:

مبحث تمهيدي: ماهية البيانات الشخصية.

الفصل الأول: الجرائم المتعلقة بالمعالجة غير المشروعة للبيانات الشخصية.

المبحث الأول: المعالجة غير المشروعة للبيانات والإخلال بشروط جمعها والاحتفاظ بها.

المبحث الثاني: الاعتداء على حقوق المعني بالبيانات وإخلال الحائز والمتحكم والمعالج بالتزاماتهم.

الفصل الثاني: المواجهة الجنائية للاستغلال غير المشروع للبيانات الشخصية.

المبحث الأول: انتهاك قواعد نقل البيانات الشخصية العابرة للحدود

المبحث الثاني: الاستغلال غير المشروع للبيانات الشخصية في الإعلانات التسويقية الموجهة.

مبحث تمهيدي
ماهية البيانات الشخصية

تمهيد وتقسيم:

يعيش الناس في الآونة الأخيرة ما يسمى بالعصر الرقمي، والذي شهد العديد من الاتجاهات التكنولوجية التي تحدده، لعل من أبرزها ضخامة البيانات[1]، فالناس يتعاملون بشكل يومي ويتبادلون كثيراً من البيانات الشخصية؛ ونتيجةً لتكرار التعامل مع نفس الأشخاص أو الجهات أصبحوا يمتلكون بيانات شخصية لهؤلاء المتعاملين معهم، هذه البيانات يمكن جمعها وتصنيفها ضمن ملفات يدوياً أو باستخدام أجهزة الكمبيوتر وهي ما يطلق عليها عملية معالجة البيانات، وتتم تلك العملية غالباً باستخدام شبكة

(1) ALEXANDRE SOARES DE OLIVEIRA LUCENA E VALE, A Race for Maintaining Personal Data A Work Project, presented as part of the requirements for the Award of a Master Degree in Management from the NOVA– School of Business and Economics, January 3rd 2018, p.4.

الإنترنت وتكنولوجيا الاتصالات الحديثة والتي لا تميز بين البيانات والمعلومات، فالبيانات عبارة عن حقائق أو أشياء معروفة يقيناً، ويمكن من خلالها الوصول إلى نتائج محددة، أما المعلومات فهي تَقْدِيمُ أخبار أو معرفة، وكل شيء يُضيف إلى الشخص معرفة جديدة، وبالرغم من الفرق بينهما، إلَّا أَن نظام المعلومات لا يضع حداً فاصلاً بين ما يُعتبر بيانات (مدخلات) وما يعتبر معلومات (مخرجات)[٢].

وبذلك أصبح الشخص في العصر الرقمي مجموعة بيانات يمكن تجميعها من أجل تكوين معرفة حقيقة عنه؛ وأضحت الحاجة ماسة إلى حماية خصوصيته عبر ما يعرف بحماية بياناته الشخصية، حيث أدى التطور في وسائل الاتصالات وتكنولوجيا المعلومات إلى سهولة الحصول على البيانات الشخصية للأفراد وتداولها؛ الأمر الذي نجم عنه مشكلات عديدة دقت ناقوس الخطر للمشرعين في النظم القانونية حول العالم للفت الانتباه لإرساء نظام فاعل لحماية البيانات الشخصية، وفرض إجراءات قانونية صارمة، ضد الاعتداء عليها، وانتهاك الحق في الخصوصية The right to privacy. وأدى إلى تبني العديد من الدول حول العالم مشروعات لتطوير التشريعات القائمة؛ لتوفير الحماية لخصوصيات الأفراد ضد انتهاكات الأجهزة الإلكترونية الحديثة، منها الإجراءات والترتيبات اللازمة لتنظيم عملية استيراد الأجهزة المستخدمة في التنصت ووجوب تَجْرِيم الوسائل المستحدثة للتطفل على الحياة الخاصة للأفراد، فيما عدا الجرائم ذات الأهمية بالغة الخطورة في تهديد الأمن القومي، وبناءً على إذن من جهة قضائية ذات الصلاحية[٣].

ويمكن القول بأنه وبرغم من الإيجابيات الجمة التي قدمها التحول الرقمي والذكاء الاصطناعي للبشرية إلا أنه أصبح يحيط بنا ويغرو حياتنا، ويتحكم في التفاصيل الصغيرة لمعيشتنا[٤]، لذلك ساهم بشكل ملحوظ في تهديد حق الخصوصية للأفراد عبر تعرض بياناتهم الشخصية للخطر، كأحد مظاهر الضرر الناجم عن التقدم التكنولوجي

---

[٢] د أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، ١٩٨٨، ص٤٨.

[٣] د. محمود أحمد طه، التعدي على حق سرية الاتصالات الشخصية بين التجريم والمشروعية، دار النهضة العربية، القاهرة، ١٩٩٣، ص٦.

[٤] د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٩، ص٧٢.

(ISSN: 2537- 0758)

والتقني، وذلك من خلال جمعها وتخزينها ومعالجتها بطريقة تسمح بالتعرف عليهم بشكل مباشر أو غير مباشر، بما ينتهك حقهم في الخصوصية.وفيما يلي بيان ذلك من خلال:

المطلب الأول: مفهوم البيانات الشخصية وأهمية حمايتها.

المطلب الثاني: مصادر حماية البيانات الشخصية.

المطلب الأول

مفهوم البيانات الشخصية وأهمية حمايتها

تتسم جرائم المعلوماتية[٥] بطابعها الخاص، وتقوم على مصطلحات مستحدثة في مجال القانون الجنائي، لذلك اتجهت العديد من التشريعات المقارنة على تضمين تشريعات مكافحة تلك الجرائم إشارة إلى التعاريف التشريعية للمصطلحات المرتبطة بالجرائم المعلوماتية، وقد أشارت المذكرة الإيضاحية لقانون مكافحة جرائم تقنية المعلومات المصري ١٧٥ لسنة ٢٠١٨ إلى أن المادة الأولى منه تناولت تعريف المصطلحات الواردة بالقانون، والتي جاءت في قائمة مطولة؛ نظراً لكون معظم هذه المصطلحات غير متداولة بصورة واسعة خاصة بمنطوقها في اللغة العربية خارج دائرة المتخصصين، أو تداولها بمفاهيم غير واضحة وغامضة، وبعضها قصد من إيراده في التعاريف توحيد مفهومها في نطاق تطبيق هذا القانون[٦]. وحسناً ما فعله المشرع المصري عبر بيانه تلك المفاهيم المستحدثة في المجال القانوني بشكل عام والجنائي بشكل خاص؛ كون القانون الجنائي يجب أن يواكب هذه التطورات التقنية، التي توفر وسائل معقدة للغاية لإساءة استخدام خدمات الفضاء السيبراني؛ نظرًا لأن شبكات الكمبيوتر لا تعرف حدود[٧].

---

[٥] ويقصد بالمعلوماتية اصطلاحاً: هو علم المعالجة المنطقية للمعلومات باستخدام آلات تعمل ذاتياً، وهي تلك التقنية التي أفرزها التطور التقني كظاهرة حديثة من خلال ما يسمى بالحاسب الآلي. د. أحمد خليفة الملط الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الإسكندرية، ٢٠٠٦، ص ٨١.

[٦] المذكرة الإيضاحية لقانون مكافحة جرائم تقنية المعلومات، مضبطة مجلس النواب، الفصل التشريعي الأول، دور الانعقاد العادي الثالث، مضبطة الجلسة السادسة والخمسون، ص٤٢.

[7] Imane Majdoub, La protection pénale des données à caractère personnel à l'ère numérique, Article ·revue des affaires penales et de la gouvernance sécuritaire, July 2022, p.2.

الفرع الأول
مفهوم البيانات الشخصية

أولاً-التعريف التشريعي:

تُعرف البيانات أو المعطيات الشخصية personal data les données personnelles ويشار لها أيضاً بالمعطيات ذات الطابع الشخصي أو البيانات الاسمية. فالمشرع الفرنسي قد استخدم عبارة البيانات الاسمية بشكل أساسي في القانون رقم ١٩٧٨/١٧، وهو القانون المتعلق بمعالجة البيانات والملفات والحريات الصادر في ٦ يناير ١٩٧٨ في نسخته الأولى، وقد استخدم عبارة البيانات الشخصية في مواضع معينة من هذا القانون، بينما استخدمت الاتفاقية الأوروبية لحماية الأشخاص لسنة ١٩٨١ تسمية المعالجة الآلية، وكذا استخدم التوجيه الأوروبي رقم ١٩٩٥/٤٦ المتعلق بحماية الأفراد فيما يتصل بمعالجة البيانات وحرية انتقالها، عبارة البيانات ذات الطابع الشخصي، الأمر الذي دفع المشرع الفرنسي إلى استبدال عبارة البيانات الاسمية بعبارة البيانات ذات الطابع الشخصي، استجابة للتوجيه الأوروبي لتعميم استخدام هذه التسمية، وتبني تعريفاً أوسع لها بموجب التعديل الذي طال قانون معالجة البيانات والملفات والحريات بالقانون ٢٠٠٤/٨٠١ الصادر في ٦ أغسطس ٢٠٠٤[٨].

ويقصد بمصطلح البيانات الاسمية الذي كان مستعملاً في فرنسا قبل التحول لمصطلح البيانات الشخصية بموجب القانون ٢٠٠٤/٨٠١ بأنها: المعلومات التي تسمح بأي شكل من الأشكال، بطريقة مباشرة أو غير مباشرة، بتحديد هوية الأشخاص الطبيعيين الذين تنطبق عليهم، سواء تم إجراء المعالجة بواسطة شخص طبيعي أو شخص اعتباري. لذلك كان من الضروري الانتظار ستة وعشرون عامًا حتى يتم التحول إلى مفهوم البيانات الشخصية، وبفضل التعديلات التي أدخلت على أحكام المادة ٤ من القانون رقم ٢٠٠٤/٨٠١، تم استبدال تسمية البيانات الاسمية بالبيانات الشخصية، وبذلك زادت الحماية القانونية للشخص وحياته الشخصية المحمية مع توسيع مجال الحماية القانونية؛ فلم تعد البيانات اسمية فحسب، بل يمكن أن تكون شخصية أو اسمية أو شخصية وغير اسمية، وتم التأكيد على هذا التطور من خلال أحكام اللائحة (الاتحاد

---

[٨] د. صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل في الاقتصاد والإدارة والقانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار– عنابة– الجزائر المجلد ٢٤– العدد ٢، أوت ٢٠١٨، ص١٢٧، ١٢٦.

(ISSN: 2537- 0758)

الأوروبي للحماية البيانات الشخصية) رقم ٢٠١٦/٦٧٩المؤرخة ٢٧ أبريل ٢٠١٦ والتي أفسحت المجال بشكل كبير لما يمكن اعتباره بيانات شخصية[٩]. وعرفت تلك اللائحة في المادة الرابعة منها البيانات الشخصية بأنها: أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد (موضوع البيانات) والشخص الطبيعي هو الشخص الذي يمكن تحديده بشكل مباشر أو غير مباشر على وجه خاص بالرجوع إلى معرف للهوية كالاسم أو بيانات الموقع أو المعرف عبر الإنترنت أو لواحد أو أكثر من العوامل الخاصة بالهوية البدنية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي[١٠].

وتضمن قانون معالجة البيانات والملفات والحريات الفرنسي رقم١٧ لسنة ١٩٧٨ المعدل بالقانون رقم ١٠٨ لسنة ٢٠٠٤ تعريفاً للبيانات الشخصية في مادته الثانية جاء فيه بأنه: يعتبر بياناً شخصياً أي معلومة تتعلق بشخص طبيعي مُحدّدة هويته أو يمكن تحديد هويته بشكل مباشر أو غير مباشر من خلالها، سواء تم تحديد هويته عبر رقمه الشخصي أو بالرجوع إلى أي شيء يخصه[١١]. وبناءً على هذا التعريف فإن أي معلومة متعلقة بشخص طبيعي تعتبر بياناً شخصياً مشمولاً بالحماية القانونية طالما أن هذا الشخص محددة هوايته أو يمكن تحديدها سواء كان ذلك بشكل مباشر أو غير مباشر.

وإذا توجهنا لقاء المشرع الأمريكي لبيان مفهوم البيانات الشخصية يتضح أنه يشار إليها باعتبارها المعلومات المتعلقة بالفرد ويطلق عليها مصطلح المعلومات الشخصية (بدلاً من البيانات الشخصية)، على الرغم من أن تشريعات الخصوصية الحديثة في ولايات كفيرجينيا، وكولورادو، ويوتا، تستخدم مصطلح البيانات الشخصية على وجه التحديد، ومن ذلك يتباين أن مفهوم (المعلومات الشخصية– البيانات الشخصية) في الولايات المتحدة ليس موحداً في جميع الولايات أو في جميع اللوائح حيث لا يوجد تشريع رئيسي واحد لحماية البيانات في الولايات المتحدة الأمريكية، وبدلاً من ذلك تعمل مجموع القوانين التي تسنها الدولة على المستويان الفيدرالي أو مستوى الولايات على

---

(9) SIMON CAQUÉ, Le régime juridique des données publiques numériques, Thèse de doctorat de droit, spécialité droit public, Institut du droit public et de la science politique, UNIVERSITÉ DE RENNES 1, 2020, p98.

(١٠) المادة الرابعة من اللائحة الأوروبية لحماية البيانات الشخصية.

(11)Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par loi n°2004-801 du 6 août 2004- art. 1 JORF 7 août 2004. L'article 02.

حماية البيانات الشخصية للمقيمين فيها، وبالرغم من عدم وجود تشريع اتحادي عام لحماية البيانات، إلا أن هناك عدداً من قوانين حماية البيانات الفيدرالية الخاصة بقطاع معين تركز على أنواع معينة من البيانات على سبيل المثال، قانون حماية خصوصية السائق لعام ١٩٩٤ ويحكم الخصوصية والكشف عن المعلومات الشخصية التي تم جمعها من قبل إدارات الدولة للسيارات، وقانون حماية معلومات الأطفال محمية على المستوى الفيدرالي، والذي يحظر جمع أي معلومات من طفل يقل عمره عن ١٣عاما[١٢]، ويلاحظ على المشرع الأمريكي في مجال حماية البيانات الشخصية تجنب وضع تشريع فيدرالي عام متخصص في مجال حمايتها؛ خشية التقييد أو التضييق على النشاط التجاري الهائل والمهم الذي يتم من خلال الشبكة العنكبوتية الدولية (الإنترنت) أحد أهم الروافد الاقتصادية للولايات المتحدة الأمريكية؛ نظراً لأن الإنترنت من أبرز الوسائل من خلالها الاعتداء على البيانات الشخصية عبر المعالجة والاستغلال غير المشروع لها.

وعلى صعيد التشريعات العربية اعتمدت أغلب قوانينها تعاريف موسعة للبيانات الشخصية حيث وضعت جميعها مادة خاصة لتعريف البيانات الشخصية في صدر القانون المعنى بحمايتها، إلا أنها اختلفت من حيث التسمية التي تطلقها كل دولة على اسم ذلك القانون، فتبنت بعضها مصطلح البيانات الشخصية كالمشرع المصري والأردني والمنظم السعودي، ومنها من اعتمدت مصطلح البيانات ذات الطابع الشخصي كالمشرع اللبناني[١٣]، أما المشرع المغربي[١٤] أطلق عليها مصطلح المعطيات ذات الطابع الشخصي، ويمكن القول بأن كل من البيانات الشخصية، أو المعطيات الشخصية، أو البيانات ذات الطابع الشخصي: عبارة عن مترادفات لمعنى واحد، تشمل حق الفرد في التحكم بالبيانات والمعلومات التي تخصه وتتعلق به، ومن جانبي فقد أثرت مصطلح البيانات الشخصية باعتباره المصطلح الأكثر تداولاً في العديد من النظم القانونية المقارنة

(12) F. Paul Pittman ،Kyle Levenberg, Shira Shamir, Data Protection Laws and Regulations USA 2022-2023, iclg, Published: 08/07/2022, منشور على الموقع https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa. تاريخ الزيارة ٢٠٢٣/٢/٣م

(١٣) قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي الصادر في ١٨ تشرين الأول ٢٠١٨

(١٤) الصادر في ١٨ فبراير ٢٠٠٩

(ISSN: 2537- 0758)

التي تعني بحماية البيانات الشخصية للأفراد، عوضاً عن ذلك هو المصطلح الذي أطلقه المشرع المصري على القانون المتعلق بحمايتها.

عرف المنظم السعودي البيانات الشخصية في المادة الأولى من نظام حماية البيانات الشخصية السعودي[١٥] بأنها: "كل بيان– مهما كان مصدره أو شكله– من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي". وتضمنت المادة الثانية من نظام ذات النظام بشأن تطبيق أحكامه على أي عملية معالجة لبيانات شخصية تتعلق بالأفراد بأنها تشمل بيانات المتوفى إذا كانت ستؤدي إلى معرفته أو معرفة أحد أفراد أُسرته على وجه التحديد. ولعل هذا يعكس مدى حرص المنظم السعودي على تكريس حماية البيانات الشخصية. وهي خطوة تحسب للمنظم السعودي شموله بالحماية بيانات المتوفي، وأناشد المشرع المصري شموله بالحماية للبيانات الشخصية بيانات المتوفي شأنه شأن المنظم السعودي؛ وذلك لأنه من خلالها يمكن الوصول إلى معرفة الشخص المعني بالبيانات على وجه التحديد أو معرفة أحد أفراد أسرته.

وأما المشرع المصري فقد عرف البيانات الشخصية في المادة الأولى من قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠[١٦] بأنها: "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى 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".

ويؤخذ على المشرع المصري استخدامه مصطلح (الربط) بين هذه البيانات وأي بيانات أخرى، حيث يتجلى الاختلاف في استخدام القانون المصري مصطلح "الربط" بين هذه البيانات، واستخدام اللائحة الأوروبية لحماية البيانات مصطلح "By Reference"

---

[١٥] الصادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ١٤٤٣/٢/٩هـ، والمنشور صحيفة أم القرى، العدد ٤٩٠١ بتاريخ ١٤٤٣/٢/١٧هـ. والمعدل ب (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ.

[١٦] الجريدة الرسمية– العدد ٢٨ مكرر (هـ)– في ١٥يوليه سنة ٢٠٢٠.

والذي يعني "بالإشارة" وليس "الربط"، وتبدو أهمية الفرق بين المصطلحين في أن مصطلح "الربط" يفهم منه بسهولة أنه لابد من ارتباط بيانين معًا، لكي يصبح البيان شخصي بالمعنى الذي يقصده ويحميه القانون، بينما استخدام لفظ "بالإشارة " الوارد في تعريف اللائحة الأوروبية لحماية البيانات، يوسع من نطاق الشخصية التي قد يشملها القانون بحمايته بجعلها قائمة بذاتها كبيان شخصي من دون الحاجة إلى ربطها ببيان أخر[١٧]؛ لذلك كان حرياً بالمشرع المصري توخي الدقة في الصياغة وأن يعتمد مصطلح "بالإشارة" وليس "الربط" لتوسع نطاق الحماية.

ويتضح من مجمل تلك التعاريف التشريعية سالفة البيان أن التشريعات التي عنيت بحماية البيانات الشخصية ترمي إلى صون جانب من الحياة الخاصة من زحف المعرفة؛ للحد من الانتهاكات التي تأتي على مكامن الذات الإنسانية، فكل معلومة تتعلق أو تخص فرداً مُعرف أو يمكن التعرف عليه بشكل مباشر أو غير مباشر تشكل بياناً شخصياً، فمتى وجد رابط أو صلة بين المعلومة والشخص المتعلقة به، وكان بالإمكان التعرف عليه، شكلت هذه المعلومة إحدى البيانات الشخصية[١٨]؛ وبالتالي وجب حمايتها جنائياً والتصدي لكل محاولة لنيل منها أو التعرض لها.

ولم تقتصر الحماية على البيانات التي تحدد هوية الشخص بشكل مباشر مثل الاسم أو الموطن فحسب، ولكنها أيضًا تشمل البيانات التي يمكنها أن تحدد الشخص بشكل غير مباشر والتي ترتبط في الغالب بالتقنيات الحديثة: كرقم الجوال أو عنوان البريد الإلكتروني أو رقم بطاقة ائتمان، أو بيانات شخصية أخرى مثل صوته أو بصمات الأصابع أو الحمض النووي أو حتى البيانات البيو مترية[١٩][٢٠]، وحيث يتعذر حصر

---

[١٧] دراسة نقدية لقانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، مركز بحوث القانون والتكنولوجيا، ورشة العمل بكلية القانون بالجامعة البريطانية في مصر، المنعقدة يوم الاثنين الموافق ١٢ أكتوبر ٢٠٢٠، ص٩١.

[١٨] أشراف البكوش، حماية الحياة الخاصة في القانون الجنائي، رسالة ماجستير كلية الحقوق والعلوم الاقتصادية والسياسية، سوسة– تونس، العام الجامعي ٢٠٠٦/٢٠٠٧ص ٥٩.

[١٩] يقصد البيانات البيومترية: عرفتها اللائحة الأوروبية لحماية البيانات رقم (٢٠١٦/٦٧٩) والصادرة في ٢٧ابريل ٢٠١٦ في المادة الرابعة بأنها تعني البيانات الشخصية الناتجة عن معالجة تقنية

(ISSN: 2537- 0758)

البيانات التي تعد شخصية وإنما يمكن التدليل عليها بأمثلة كالبيانات الفردية كالاسم والجنسية، والجنس والصورة، وفصيلة الدم، والديانة والسكن والوظيفة والمؤهل الدراسي أو المهني ورقم الهاتف، والعنوان، والبصمة، والبيانات المدنية بالإضافة إلى أهم المعلومات الخاصة التي يسعى الإنسان إلى إبعاد الأنظار عنها، كبيانات واقعة الميلاد، التي تحدد تاريخ الميلاد ومكانه وجنس المولود واسم الأب والأم وبيانات واقعة الوفاة التي تظهر تاريخ الوفاة وعمر المتوفى ومكان الوفاة وسببها، إلى جانب بيانات الزواج والطلاق، والعنوان ورقم بطاقة التعريف، وتاريخ دخول ومغادرة البلاد الأجنبية والتأشيرات المتحصل عليها، والبيانات المالية والتي تتضمن الدخل الفردي الشهري، ومعدل الإنفاق والديون والسمعة المالية لدى البنوك، والمعاملات المالية، وأرقام الحسابات، والبيانات الصحية وهي التي تتعلق بالحالة الصحية، والأدوية الموصوفة، والسوابق المرضية، والأمراض المزمنة أو الوبائية وتاريخ العائلة المرضي وحالة الإدمان أو الأمراض المنتقلة[٢١].

ثانياً- تعريف الفقه القانوني للبيانات الشخصية:

تعد البيانات الشخصية هي قوام الحق في الخصوصية فهي تمثل في مجموعها المعطيات والمعلومات الخاصة بالفرد والتي تكتسب صفة السرية[٢٢]، وجاء في تعريفها بأنها: مجموعة من المعلومات التي تمس الإنسان في شخصه[٢٣]، إلا أن هذان التعريفان يتسمان بالغموض وعدم التحديد الدقيق لكنة تلك البيانات، **ولذلكُ عرفت بأنها:**

محددة تتعلق بالخصائص الجسدية أو الفيزيائية أو السلوكية للشخص الطبيعي والتي تسمح أو تؤكد التحديد الفريد لهذا الشخص الطبيعي مثل صور الوجه أو بصمات الأصبع.

(20) Claudine Guerrier, Protection des données personnelles et applications biométriques en Europe, Communication commerce électronique, 1 juillet 2003, n7, pp.17-22.

[٢١] د. على احمد عبد الزغبي، حق الخصوصية في القانون الجنائي دراسة مقارنة، المؤسسة الحديثة للكتاب، لبنان، ٢٠٠٦، ص٣٣٣-٣٣٧.

[٢٢] د. محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠١٦، ص٩٢.

[٢٣] د. عمرو احمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠، ص١٥٦.

كل معلومة أو صوت أو صورة متعلقة بشخص ما، معرف أو قابل للتعرف عليه سواء بصورة مباشرة أو غير مباشرة، ولاسيما من خلال الرجوع إلى عناصر مميزة لهويته البدنية أو الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية[٢٤].

وقصد بها المعلومات الخاصة بشخص طبيعي قابل للتعرف عليه، وذلك وفقاً لما نص عليه التوجيه الأوروبي الخاص بحماية البيانات الشخصية، ويلاحظ أن هذا التعريف يمثل اتجاه موسعاً من المشرع الأوروبي في تعريف البيانات الشخصية، وترجع الحكمة من ذلك إلى أن التضييق من مفهوم البيانات الشخصية قد يسمح للعديد من الجهات بالتعدي عليها، وبالتالي فرض ذلك من باب أولى على المشرع الأوروبي أن يضع تعريفاً أكثر اتساعاً بدلاً من التعريف الضيق[٢٥].

وجاء في تعريفها بأنها: "أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده (موضوع) البيانات"، بشكل مباشر أو غير مباشر[٢٦]. وفي هذا التعريف يتم الإشارة إلى أن البيان في حد ذاته ليس له جدوى إلا لو التصق بشخص معين، فمثلاً الرقم القومي للشخص في حد ذاته لا يعبر عن شيء بعينه إلا إذا نسب إلى صاحب البطاقة[٢٧].

وتأسيسا على ما سبق يمكن القول أنه يقصد بالبيانات الشخصية: كل نوع من أنواع المعلومات سواء كانت معلومة واحدة أو مجموعة معلومات، يمكن من خلالها أن تحدد شخص ما أو تفرده كفرد، والأمثلة على ذلك عديدة كاسم الشخص وعنوانه، 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

---

[٢٤] د. هشام فريد رستم قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة، أسيوط، ١٩٩٢، ص ١٨٢.

[٢٥] د. ياسر محمد اللمعي، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية– دراسة تحليلية مقارنة، مجلة روح القوانين، كلية الحقوق– جامعة طنطا– العدد السابع والتسعون– يناير ٢٠٢٢ص٢٦.

[26] Narayanan. A.: Shmatikov. V. "De-anonymizing Social Networks". 2009 30th IEEE Symposium on Security and Privacy. 2009. p. 173

[٢٧] د. مروة زين العابدين سعد صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، رسالة دكتوراه، كلية الحقوق– جامعة عين شمس، ٢٠١٤، ص٥٦.

(ISSN: 2537- 0758)

من الشخص سواء تم ذلك بطريقة مباشرة أو غير مباشرة، مثل بصمات اليد أو الحمض النووي أو غيرها من البيانات الأخرى[٢٨]، وقد ذهب القضاء الفرنسي إلى حماية البيانات الشخصية تعنى حق الفرد في اختيار الكشف عن المعلومات التي يختار البوح بها وتحديد الأشخاص الذي يريد التواصل كما أن حماية البيانات المتعلقة بالهوية تتأكد من خلال حق الشخص في الاحتفاظ بسرية المعلومات المتعلقة بهويته[٢٩].

ومن جانبي أشايع الرأي القائل بأن: البيانات الشخصية لا تعدو أن تكون مجموعة من البيانات أو بالأحرى معلومات تتسم بالشخصية؛ كونها لصيقة بشخص من يُعرف بها، وتمييزه عن غيره، كالاسم، والجنس، والموطن وغيرها، والحق أن سريتها وعدم إفشائها للغير يعتبر من أهم وأعظم صور الحق في حرمة الحياة الخاصة، فالحفاظ على أسرار الإنسان هو جوهر وأساس ضمان حماية الخصوصية ضد انتهاك الغير وتدخله[٣٠]، وقد استقر قضاء المحكمة الدستورية في مصر علي أنه" ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغوارًا لا يجوز النفاذ إليها، وينبغي دوما–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 حدًا مذهلاً، وكان لتنامى قدراتها على الاختراق أثراً بعيداً على الناس جميعهم حتى في أدق شئونهم، وما يتصل بملامح حياتهم، بل وببياناتهم الشخصية التي غدا الاطلاع عليها وتجميعها نهباً لأعينها ولآذانها، وكثيراً ما ألحق النفاذ إليها الحرج أو الضرر بأصحابها، وهذه المناطق من خواص الحياة ودخائلها، يلوذ الفرد بها، مطمئنا لحرمتها ليهجع إليها بعيداً عن أشكال الرقابة وأدواتها– الحق في أن تكون للحياة الخاصة تخومها (أي حدوداً فاصلة) بما يرعى الروابط الحميمة في نطاقها[٣١].

---

[٢٨] د. ياسر محمد اللمعي، المرجع السابق، ص٢٩.

[29] JACQUELINE. POUSSON-PETIT, Le droit à l'anonymat in Mélanges dédies à louis Boyer: Presse Universitaire de Toulouse, 1996, p. 596 s.

[٣٠] د. سوز حميد مجيد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، دراسة تحليلية مقارنة، دراسات قانونية وسياسية، السنة السادسة، العدد (١١) نيسان– ابريل٢٠١٨، ص١٦٦.

[٣١] الدعوى رقم ٢٣ لسنة ١٦ قضائية "دستورية" بجلسة ١٨/ ٣/ ١٩٩٥ جـ ٦ "دستورية" ص ٥٦٧. الموسوعة الذهبية للقضاء الدستوري المصري، ١٩٦٩– ٢٠١٩، المجلد الأول. المحكمة الدستورية العليا، القاهرة، ص١٠١٩، ١٠١٨.

وتنقسم البيانات الشخصية المشمولة بالحماية الجنائية لأي اعتداء يقع عليها إلى بيانات شخصية معالجة إلكترونياً تعبر عن كيان الإنسان الخارجي مثل: الاسم، والعنوان، والسن، وأرقام الهاتف، والحالة الاجتماعية والديانة، وأرقام بطاقات الرقم القومي، وجواز السفر، والبطاقات الائتمانية، ونوع الجنس، والصورة والفيديو والمراسلات، والبصمة الوراثية، وبيانات شخصية معالجة إلكترونياً متعلقة بالهوية الإلكترونية للشخص: كالبريد الإلكتروني، وعنوان الكمبيوتر، وعنوان مواقع التوصل الاجتماعي[٣٢].

الفرع الثاني
أهمية حماية البيانات الشخصية

قررت المادة الأولى من قانون معالجة البيانات والملفات والحريات الفرنسي[٣٣] بأنه يجب أن تكون تكنولوجيا المعلومات في متناول كل مواطن، وألا تنتهك هوية الإنسان أو حقوقه أو خصوصيته أو الحريات الفردية أو العامة[٣٤]، وتنبع أهمية حماية البيانات الشخصية من قيمتها، التي جاءت من وفرتها في العصر الرقمي وما يتيح من قدرة فائقة على التعامل معها عبر معالجتها، وتوظيفها في مجالات متعددة، تختلف باختلاف الجهات المستفيدة منها، سواء كانت حكومات أو شركات تطلبها لإدارة أعمالها، ورفع كفاءتها، وتسويق منتجاتها وزيادة أرباحها، وفي ظل هذا الدور التي تشغله البيانات الشخصية برزت أهميتها والحاجة المتزايدة لحمايتها، فالناس تحتاج للبيانات لمعرفة ما يدور حولهم، ولتسيير حياتهم واتخاذ قراراتهم بشأنها، وحيث قامت هذه البيانات عبر معالجتها واستغلالها المشروع بنقلة نوعية في تغيير مفاهيم العالم الاقتصادية، والاجتماعية وحتى الثقافية، وأضحت أحد أهم الركائز لقيام تكنولوجيا الذكاء الاصطناعي وتطبيقاتها العديدة التي غزت كل نواحي الحياة خلال فترة زمنية وجيزة.

وحظي الحق في حماية البيانات الشخصية باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أو من جانب التشريعات الوطنية، فقد أنتج العالم خلال العام ٢٠١٧ معدلات غير مسبوقة من البيانات، تتجاوز بضخامتها ما أنتج على امتداد كامل تاريخ البشرية، وهوما نبه المعنيين في القطاعين العام والخاص، إلى أهمية إدارتها بشكل فاعل، مع مراعاة الجوانب التقنية، والاقتصادية، والإدارية، والقانونية التي تترتب على

---

[٣٢] د. ياسر محمد اللمعي، المرجع السابق، ص٤٢وما بعدها حتى ٧٥.

[٣٣] الصادر في ٦ يناير ١٩٧٨

[34] Modifié par Ordonnance n°2018-1125 du 12 décembre 2018- art. 1

(ISSN: 2537- 0758)

ذلك، فمع الانتقال إلى الرقمية تحولت البيانات إلى قيمة لا تقدر بثمن، ومورد لاقتصاد المعرفة[٣٥]، فليس خافياً على أحد أن اقتصاديات العالم الرقمي قد وصلت لأرقام تجاوزت بكثير كل التوقعات، وحيث إن من أهم مصادر الثروة في الحياة الرقمية تجارة المعلومات، ويدخل في هذه التجارة على وجه الخصوص، التجارة المتعلقة بالبيانات الشخصية– ليس هذا فحسب– فالبيانات الشخصية تستعمل كذلك سياسياً وعسكرياً وأمنياً[٣٦].

ولم يقتصر الأمر على ذلك بل باتت الشركات العاملة في مجال تقنيات المعلومات تنشر بشكل مستمر عدد المستخدمين الموجودين لديها، كما لا تتأخر شركات الإحصاء، عن إصدار تقاريرها حول هذا الموضوع بهدف تأمين المعلومات اللازمة، للشركات وأصحاب المواقع المختلفة، كي يتمكنوا من وضع خطط انتشارهم، والترويج لمنتجاتهم وتسويق خدماتهم. وإذ يصل حجم الأشخاص وقت كتابة هذا التقرير الذين يستخدمون شبكة الفاسبوك، إلى ما يفوق المليارى شخص، ويصل العدد إلى ٨٠٠ مليون على انستغرام، وإلى أكثر من مليار على واتس آب، يتجاوز حجم البيانات التي تنتج عن هذا الاستخدام، ٢.٥ إكسا بايت Exabyte في الدقيقة الواحدة تقريباً، وتعتبر تطبيقات المحادثات الفورية، مصدراً آخراً لإنتاج البيانات، حيث يتم إرسال أكثر من ٥٢٧ ألف صورة، بواسطة السناب شات، في الدقيقة، وتحصل منصة لينكدن Linked in على أكثر من ١٢٠ حساب جديد، ويرسل مستخدمو توتير ٤٥٦ ألف تغريده، بينما يعالج جوجل أكثر من ٣.٦ مليون عملية بحث، وتجني أمازون أكثر من ثلاثمائة ألف دولار أمريكي من المبيعات، التي تجري في الدقيقة الواحدة على الإنترنت، هذا عدا عن الحجم الهائل للاستثمارات، التي تقوم بها الدول في مجال البيانات الضخمة[٣٧]، حيث أدى تطوير الحواسيب الرقمية وتكنولوجيا الشبكات، وبشكل خاص الإنترنت لإتاحة نقل

---

[٣٥] د منى الأشقر جبور، د محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، الطبعة الأولى، المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان، ٢٠١٨، ص١١.

[٣٦] دراسة نقدية لقانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، مرجع سابق، ص٨.

[37]. Big Data Statistics & Facts for 2017

https://www.w.aterfordtechnologies.com/big-data-interesting-facts/مشار إليه لدى د. منى الأشقر جبور، د محمود جبور، مرجع سابق ص١٢، ١١.

النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي من العالم المادي إلي العالم الافتراضي- البيئة الإلكترونية، ويوماً بعد يوم تتكامل الشبكات العالمية للمعلومات مع مختلف أنشطة الحياة[٣٨].

ولعل هذا يفسر اتجهت الشركات الكبرى نحو الاستثمار في البيانات الشخصية، فهي ثروة تعيش عليها الشركات التقنية منها، والتقليدية، نتيجة استخدامها في مجال تطوير المنتجات والإعلانات عبر تحليلها، وتحليل ميول الأشخاص الطبيعيين، وتحديد حاجتهم، وعاداتهم الاستهلاكية، واهتماماتهم[٣٩]، فقد أدركت الشركات أن ذهب العصر الحالي هي البيانات الشخصية بما تمثله من أهمية كبيرة عبر معالجتها وإسهامها في تحسين الأداء والإنتاج.

ونظراً للخطورة البالغة التي يشكلها الاعتداء على البيانات الشخصية للأفراد، بما يمثله من انتهك صارخ للحق في الخصوصية، والتي تعد من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهي تعد أساس بنيان كل مجتمع سليم، وتعتبر من الحقوق السابقة على وجود الدولة ذاتها؛ لذا حرصت المجتمعات خاصة الديمقراطية منها على كفالة هذا الحق، واعتباره حقاً مستقلاً بذاته ولم تكتفي بسن القوانين لحمايته، بل تسعى إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دوراً كبيراً وفاعلاً في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم[٤٠]؛ لذلك جاء تدخل المشرع المصري لحماية البيانات الشخصية انعكاساً لحمايته الحق في الخصوصية بإصداره تشريعاً لحماية البيانات الشخصية، وقد جاء في مذكرته الإيضاحية بأن "أدت تطورات تكنولوجيا المعلومات والاتصالات المتلاحقة، وخاصة مع تغلغل تكنولوجيات إنترنت الأشياء والحوسبة السحابية والذكاء الاصطناعي وغيرها إلى ظهور تحديات جديدة على مستوى حماية

---

[٣٨] د. يونس عرب، المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، منشور على شبكة المعلومات الدولية- الإنترنت، https://kenanaonline.com/users/ahmedkordy/posts/323471 تاريخ الزيارة ٢٠٢٣/٣/١٥م. ص١٨.

[٣٩] د. منى الأشقر جبور، د حمود جبور، مرجع سابق، ص١٢.

[٤٠] د. عائشة مصطفى بن قارة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون، المغرب، العدد الثاني والأربعون، أبريل ٢٠١٦، ص٧٣.

(ISSN: 2537- 0758)

البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل غير مسبوق مما سمح للشركات والمؤسسات الخاصة والعامة باستخدام البيانات الشخصية للأفراد على نطاق واسع؛ نظراً لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد، وذلك كله يتم دون وجود إطار قانوني حاكم لهذه الأنشطة"[٤١].

وارتكزت فلسفة وأهداف هذا القانون على ما يلي:

ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المعالجة إلكترونياً، وضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين ومكافحة انتهاك خصوصيتهم، تطبيق إطار معياري يتواكب مع التشريعات الدولية لحماية البيانات الشخصية للأفراد وحرياتهم، واحترام خصوصيتهم، وصياغة التزامات على كل من المتحكم في البيانات ومعالج البيانات باعتبارهما من العناصر الفاعلة في مجالات التعامل في البيانات الشخصية، سواء عن طريق الجمع أو النقل أو التبادل أو التخزين أو التحليل أو المعالجة بأي صورة من الصور، وإلزام المؤسسات والجهات والأفراد المتحكمين في البيانات الشخصية والمعالجين لها بتعيين مسئول لحماية البيانات الشخصية داخل مؤسساتهم وجهاتهم، بما يسمح بضمان خصوصية بيانات الأفراد، واقتضاء حقوقهم المنصوص عليها في هذا القانون، وتقنين وتنظيم أنشطة استخدام البيانات الشخصية في عمليات الإعلان والتسويق على الإنترنت وفي البيئة الرقمية بشكل عام، ووضع إطار إجرائي لتنظيم عمليات نقل البيانات عبر الحدود، وضمان حماية بيانات المواطنين وعدم نقلها أو مشاركتها مع دول لا تتمتع فيها البيانات بالحماية، وتنظيم عمليات المعالجة الإلكترونية للبيانات الشخصية، وإصدار تراخيص لمن يقوم بها، وعلى الأخص فيما يتعلق بالبيانات الشخصية الحساسة ذات الطابع الخاص، وإنشاء مركز حماية البيانات الشخصية كهيئة عامة يكون مختصاً بتنظيم والإشراف على تنفيذ أحكام القانون[٤٢].

---

[٤١] المذكرة الإيضاحية، لمشروع قانون حماية البيانات الشخصية، الصادرة من وزارة العدل، بتاريخ ٢٠١٩/٢/١٩م، ص١

[٤٢] المذكرة الإيضاحية، لمشروع قانون حماية البيانات الشخصية، الصادرة من وزارة العدل، بتاريخ ٢٠١٩/٢/١٩م. ص٣، ٢

وقد حرص المشرع المصري في هذا القانون على إبراز دور المواجهة الجنائية للاعتداء على البيانات الشخصية، والتي تمثلت في كافة الوسائل القانونية التي تنفذها الدولة من أجل ضمان أمن وسلامة البيانات التي تشير إلى شخص محدد أو يمكن التعرف عليه بشكل مباشر أو غير مباشر، والتي هي موضوع المعالجة الإلكترونية، وذلك من خلال سن تدابير قمعية لأجل معاقبة أي هجوم وتعدي على البيانات الشخصية للأفراد' بفرض غرامات وعقوبات بالسجن ضد المخالفين، في إطار الإجراءات القسرية التي يمكن للسلطات العامة اللجوء إليها[٤٣].

ويجدر التنويه بأن المعني بحماية بياناته الشخصية حسب نص التشريع المصري: هو أي شخص طبيعي تنسب له البيانات الشخصية المعالجة إلكترونياً وتدل عليه قانوناً أو فعلاً، وتمكن تمييزه عن غيره[٤٤]، ووفقاً لهذا التعريف فإنه يشمل الشخص الطبيعي وليس المعنوي كون الأخير لا تمتد مظلة الحماية إليه[٤٥]، كونه قصد بالبيانات الشخصية محل الحماية هي المتعلقة بالأشخاص الطبيعيين دون الأشخاص الاعتبارية، وذلك في تصوري محل للنقد إذ كان يتعين على المشرع المصري مد مظلة الحماية للأشخاص الطبيعيين والاعتباريين للتأثير الكبير الذي تمثله الأشخاص المعنوية في النواحي الاقتصادية والتنموية بشكل عام؛ وبالتالي كان لابد من إقرار حماية جنائية للبيانات الشخصية لكلاهما على حداً سواء.

ويقابل المعني بالبيانات الشخصية في نظام حماية البيانات الشخصية السعودي مصطلح صاحب البيانات الشخصية: هو الفرد الذي تتعلق به البيانات الشخصية[٤٦].

وعطفاً على ما سبق يمكن القول بأن حماية البيانات الشخصية يجب أن تكون من خلال قانون خاص مصمم لحمايتها، ووضع الضوابط اللازمة للتعامل معها. نتيجة

---

(43) PUTZ J.L., Cybercriminalité; Criminalité informatique en droit luxembourgeoiS, Éditions Larcier, Lefebvre Sarrut Belgium, Luxembourg, 2019, p.27.

(٤٤) المادة الأولى من قانون حماية البيانات الشخصية المصري.

(45) Ida Madicha Azmi, E-Commerce and Privacy Innes An Analysis of the Personal Data Protection Hill, International, Review of Law, Computers & Technology, 2015, p7.

(٤٦) المادة الأولى من نظام حماية البيانات الشخصية السعودي معدلة بالمرسوم الملكي رقم (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ.

(ISSN: 2537- 0758)

التوسع غير المسبوق في البيانات الشخصية في الآونة الأخيرة، 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 كان لابد من حماية هذه الممارسات من خلال قانون يحمي البيانات الشخصية؛ وبناءً على ذلك فقد أصدرت أكثر من ١٠٠ دولة حول العالم قوانين شاملة لحماية خصوصية البيانات الشخصية، وهناك أكثر من ٤٠ دولة أخرى لديها مشاريع قوانين أو مبادرات متعلقة بحماية البيانات الشخصية[٤٧]؛ نظراً لأن انتشار التكنولوجيا التي تستخدم البيانات الشخصية استخداماً كثيفاً على غرار تطبيقات الذكاء الصناعي، ساهم في إقامة بيئة رقمية عززت هي الأخرى من العديد من الممارسات غير المشروعة في سياق الانتهاكات الإلكترونية، وجعلت الحق في الخصوصية على المحك مما تطلب في المقابل وضع نظام لحماية الخصوصية في العصر الرقمي يراعي طبيعة هذه التهديدات[٤٨].

وفي سبيل ذلك الزم القانون الجهات التي تقوم بتخزين البيانات وتجميعها بحمايتها، من دون أن يفصّل في أشكال هذه الحماية، بل يجب أن تكون هناك حماية وقائية سابقة لوقوع الاعتداء، تتمثل بوضع ضوابط على معالجة البيانات الشخصية.

لأجل ذلك كله ظهرت أهمية الحماية الجنائية للبيانات الشخصية 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، **والوجه الثاني:** حماية سرية الحياة الخاصة للشخص: أي حق الشخص في أن تظل أخباره وبياناته سرية، وقد تكون متعلقة بالنواحي النفسية والعقلية مثل الحالة الصحية لجسم الإنسان، وقد تكون متعلقة بالنواحي الخارجية للإنسان مثل مراسلاته وبيانات الشخصية[٤٩].

---

[٤٧] د ياسر محمد اللمعي، مرجع سابق، ص٣٥، ٣٤.

[٤٨] د رشيدة بوكر، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، العدد الثاني، ٢٠٢٢م، المجلد ٧، ص٦٦.

[٤٩] د. ياسر محمد اللمعي، مرجع سابق، ص٤٣.

المطلب الثاني
مصادر حماية البيانات الشخصية

تستند النظم القانونية حول العالم التي تعنى بحماية البيانات الشخصية إلى عديد من المصادر التي تستقي منها الأساس القانوني لبناء تلك التشريعات، وتتنوع هذه المصادر إلى مصادر ذات طابع دولي كالاتفاقيات الدولية أو الإقليمية، وأخرى ذات طابع داخلي كتشريعات حماية البيانات الشخصية الوطنية بكل دولة **وفيما يلي بيان ذلك من خلال:**

الفرع الأول
حماية البيانات الشخصية في الاتفاقيات الدولية والإقليمية

ترتبط الخصوصية بالبيانات الشخصية ارتباطاً وثيقاً، كون الثانية تنبثق من الأولى؛ لذلك حرصت كافة النظم القانونية على حماية الحق في الخصوصية وفي القلب منها البيانات الشخصية، وتنوعت تلك الحماية بين دولية وإقليمية فضلاً عن التشريعات الوطنية.

أولاً-الحماية الدولية:

تضمن الإعلان العالمي لحقوق الإنسان الحق فى الخصوصية فى المادة الثانية عشرة منه، والتى قررت بأنه: "لا يجوز تعريضُ أحد لتدخُّل تعسُّفى فى حياته الخاصة أو فى شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات"(٥٠).

وجاء العهد الدولي للحقوق المدنية والسياسية لينسج على منوال الإعلان العالمي لحقوق الإنسان بإقراره بالمادة السابعة عشر مِنه بأنه: "١-لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، للتدخل في خصوصياته، أو شؤون أسرته، أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.

من حق كل شخص أن يحميه القانون مِن مِثْل هذا التدخل أو المساس"(٥١). وتبنت الجمعية العامة للأمم المتحدة توصيات المؤتمر الدولي الأول لحقوق الإنسان المنعقد في

---

(٥٠) اعتمدت الجمعية العامة الإعلان العالمي لحقوق الإنسان في باريس في ١٠ كانون الأول/ ديسمبر ١٩٤٨ بموجب القرار ٢١٧ ألف بوصفه أنه المعيار المشترك الذي ينبغي أن تستهدفه كافة الشعوب والأمم.

(٥١) العهد الدولي للحقوق المدنية والسياسة الصادر في ١٦ ديسمبر ١٩٦٦والنفاذ مارس ١٩٦٧، والموافق عليه في جمهورية مصر العربية بقرار رئيس الجمهورية رقم ٥٣٦ لسنة ١٩٨١بتاريخ ١٩٨١/١٠/١.

(ISSN: 2537- 0758)

طهران سنة١٩٦٨، والذي خرج بجملة توصيات تبرز خطورة الحاسبات الإلكترونية على الحياة الخاصة، وضرورة إيجاد آليات لحمايتها على المستوى الدولي والإقليمي[٥٢].

وقامت الجمعية العامة للأمم المتحدة، بتاريخ ١٤ كانون الأول/ ديسمبر ١٩٩٠، بالتصويت على قرار حمل الرقم ٩٥/٤٥، تضمن المبادئ التوجيهية، لتنظيم ملفات البيانات الشخصية، المعدة بالحاسبات الإلكترونية. وقد تضمنت هذه المبادئ مجمل مسائل الحماية، عبر نطاق تطبيقها، والذي يشمل جميع الجهات المعنية، بجمع البيانات ومعالجتها، سواء أكانت بيانات عامة أم خاصة، عبر الدعوة إلى توسيع نطاق التطبيق، ليشمل الأشخاص المعنويين، إضافة إلى الأشخاص الطبيعيين، كما تطرقت إلى هذه المسائل على المستوى الوطني، من خلال المبادئ التي يجب إقرارها والاستثناءات الواردة عليها، وضرورة تعيين سلطات الرقابة، والعقوبات الجزائية، وعلى المستوى الدولي، من خلال أصول ومبادئ تدفق البيانات عبر الحدود، وقابلية تطبيق المبادئ على المنظمات الدولية الحكومية، وغير الحكومية.

وأوردت المبادئ التي تلتزم الدول المعنية بإدراجها في قوانينها فهي: مبدا المشروعية والنزاهة، الذي يمنع جمع وتجهيز البيانات الشخصية، بأساليب غير نزيهة أو غير مشروعة، ويدعو إلى الالتزام باستخدامها، بما ينسجم مع مقاصد ميثاق الأمم المتحدة، ومبادئه، كمبدأ صحة البيانات، الذي أعلن مسؤولية معالجي ملفات البيانات، والمحتفظين بها، عن التحقق من دقة البيانات، والتأكد من ملاءمتها، للغاية التي عولجت لأجلها. ومبدأ تحديد الغاية، الذي بموجبه جاء مبدأ الإعلان المسبق عن هدف جمع البيانات ومعالجتها، على أن يكون هذا الهدف مشروعاً ومحدداً، بما يسمح بممارسة الرقابة والتأكد من عدم الانحراف عن الغاية المعلنة، واحترام حق الشخص المعني في الموافقة على استخدام البيانات، وإفشاء الشخصية العائدة له، والالتزام بمحو البيانات بعد إنجاز الهدف المحدد.

ومبدأ وصول الأشخاص المعنيين إلى الملفات، والذي أقر حق المعني بالبيانات في الاطلاع، وتضمن على كيفية التصرف ببياناته، وطرق استخدامها، إضافة إلى حقه في إعلام واضح، دون تكبديه أي كلفة غير مبررة، وحقه في طلب تصحيح البيانات أو محوها، وكذلك مبدأ عدم التمييز، الذي ينطلق من مبدأ عدم جواز التمييز العنصري،

[٥٢] أ/ يونس خالد عرب، جرائم الحاسوب (دراسة مقارنة)، رسالة ماجستير، الجامعة الأردنية، ١٩٩٤، ص١٢٥.

بناء على بيانات شخصية، حول العرق، أو الأثنية، أو اللون، أو الميول الجنسية، أو الآراء السياسية، أو المعتقدات الدينية والفلسفية، أو العضوية النقابية والمهنية، ومبدأ الأمن الذي يلزم المعنيين بعمليات جمع البيانات وحفظها، واتخاذ التدابير الملائمة لمنع فقدان البيانات أو تلفها، أو تسربها، أو الاطلاع عليها، نتيجة العوامل طبيعية، أو لتصرفات بشرية غير مشروعة، كالدخول إلى الأنظمة دون إذن أو استخدامها بشكل غير آمن(٥٣).

وفي تطور لتكريس حماية البيانات الشخصية أعربت الدول الأعضاء في الأمم المتحدة وغيرها من الجهات ذات المصلحة عن قلقها إزاء الأثر السلبي للممارسات الرقابية على حقوق الإنسان واعتمدت الجمعية العامة في كانون الأول/ ديسمبر ٢٠١٣ دون تصويت القرار١٦٧/٦٨ بشأن الحق في الخصوصية في العصر الرقمي، وأكدت الجمعية في هذا القرار الذي اشتركت في تقديمه ٥٧ دولة عضواً أن حقوق الأشخاص خارج الفضاء الإلكتروني يجب أن تحظى أيضاً بالحماية، وأهابت بجميع الدول أن تحترم وتحمي الحق في الخصوصية في الاتصالات الرقمية، وأن تستعرض إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة جميع الاتصالات واعتراضها وجمع البيانات الشخصية، مشددة على حاجة الدول إلى ضمان تنفيذ التزاماتها بموجب القانون الدولي لحقوق الإنسان تنفيذاً كاملاً وفعالاً(٥٤).

وبناءً على القرار الصادر من الجمعية العامة رقم ١٦٧/٦٨ فقد طلب القرار من المفوض السامي لحقوق الإنسان إعداد تقرير حول حماية وتعزيز الحق في الخصوصية في ضوء التطور التكنولوجي على أن يسلم هذا التقرير إلى مجلس حقوق الإنسان والجمعية العامة للأمم المتحدة، في ٣٠ حزيران/ يونيو ٢٠١٤، وقد انجز هذا التقرير والذي أطلق عليه "تقرير" الحق في الخصوصية في العصر الرقمي "والذي يعتبر ذو قيمة قانونية خاصة بالاستناد إلى حقيقة كونه قد اعتمد على ممارسات الدول بهذا الخصوص(٥٥).

---

(٥٣) د. منى الأشقر جبور، محمود جبور، مرجع سابق، ص٥٣، ٥٢.

(٥٤) د. رشيدة بوكر مرجع سابق، ص٨١، ٨٠.

(٥٥) د. خالد د خالد حسن أحمد، الحق في خصوصية البيانات الشخصية بين الحماية القانونية التحديات التقنية– دراسة مقارنة، دار الكتب والدراسات العربية، القاهرة، ٢٠٢٠، ص١٠١.

(ISSN: 2537- 0758)

وقد تضمن التقرير تمتع جميع الأفراد بالحق بالحماية من تلك الهجمات والتدخلات، ومع ذلك فإن عدم إعمال الحق في الخصوصية والحاجة إلى اتخاذ تدابير ملموسة لحماية ذلك الحق، والتصدي على نحو شامل لعمليات الوصول غير المأذون به إلى البيانات الشخصية وللمراقبة المكثفة، دعت إلى اتخاذ تدابير عاجلة لوقف ممارسات المراقبة وحماية الأفراد من انتهاك حقهم في الخصوصية، كما أن القيد على الحق في الخصوصية يجب أن يستند إلى قوانين يسهل الوصول إليها، وتتسم بالشفافية والوضوح والشمول وعدم التمييز، وأن يقتصر هذا القيد على ما هو ضروري لحماية المصلحة العامة في أي مجتمع ديمقراطي، ويجب أن تكون أي مراقبة تقوم بها الدولة متناسبة وعادلة، ومتوافقة مع القواعد والمعايير الدولية، وخاضعة لأحكام القانون، ويجب تحديد ضمانات كافية وفعالة من إساءة الاستعمال[٥٦].

ثانياً- الحماية الإقليمية:

عقب صدور الإعلان العالمي لحقوق الإنسان، حدث تقدم ملحوظ في تبني اتفاقيات تعنى بحقوق الإنسان على الصعيد الإقليمي خاصة إذا كان الإقليم يحمل تراثاً مشتركاً بين أعضائه، ويملك الآليات لتحقيق الإلزام الواجب لسريانها، ولما كان الاتحاد الأوروبي أكثر المنظمات الإقليمية اهتماماً بحماية البيانات الشخصية، فقد أثرت بيان دوره في التكريس الحماية لها، ويعود بداية اهتمام الاتحاد الأوروبي بحماية البيانات إلى العام ١٩٩٥بصدور القواعد الإرشادية، غير أن الاتحاد الأوروبي وفي سبيل تعزيز حمايته للبيانات الشخصية ضد ما قد يعصف بها من أخطار أصدر البرلمان الأوروبي بتاريخ ٢٧ أبريل ٢٠١٦، القواعد الأوروبية لتنتظم حماية الأشخاص الطبيعيين، من المعالجة الرقمية للبيانات الشخصية والتدفق الحر للمعلومات، وقد دخل التشريع الأوروبي الموحد، حول حماية البيانات الشخصية، حيز التنفيذ، في مايو ٢٠١٨، تحت عنوان: "القواعد العامة لحماية البيانات" وهو يهدف إلى تحقيق الانسجام بين القوانين الأوروبية، الخاصة بحماية البيانات عبر توحيد التشريعات، بما يخدم تعزيز الشفافية، لدعم حقوق الأفراد، ونمو الاقتصاد الرقمي. وقد جاء هذا التشريع ملزم لكافة دول الاتحاد[٥٧].

---

[٥٦] د. هشام مسعودي، حماية وتعزيز الحق في الخصوصية في العصر الرقمي قراءة في تقرير مفوضية الأمم المتحدة لحقوق الإنسان في دورته ٢٨، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، العدد ١ أبريل ٢٠٢٢، المجلد ٩، ص١٦٣.

[٥٧] د. منى الأشقر جبور، د محمود جبور، مرجع سابق، ص٥٥.

بالإضافة إلى ذلك فقد نصت المبادئ التوجيهية للاتحاد الأوروبي في المادة (٦) منها على مجموعة من الالتزامات يجب أن تلتزم بها الدول الأعضاء أثناء معالجة الآلية للبيانات الشخصية **وهي على النحو التالي:**

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 ألا تكون متعارضة وأن تقدم الدول الأعضاء الضمانات المناسبة.

ج- أن تكون المعالجة الآلية للبيانات كافية وغير زائدة ومرتبطة بالأغراض التي جمعت أو عولجت من أجلها.

د- أن تكون المعالجة الآلية للبيانات الشخصية دقيقة وعند الضرورة، ويجب اتخاذ كل الخطوات الضرورية لضمان أن البيانات غير الدقيقة أو غير كاملة فيما يخص الأغراض التي جمعت وعولجت من أجلها، تسمح بأن تصحح.

ذ- أن تحفظ البيانات الشخصية التي تم معالجتها آلياً بطريقة تسمح بالتعرف على صاحب البيانات لوقت لا يزيد عن الغرض الذي جمعت البيانات من أجله أو التي تعالج من أجله، ويتعين على الدول الأعضاء وضع الضمانات المناسبة للبيانات الشخصية المخزنة لفترات أطول للاستخدامات التاريخية أو الإحصائية أو العلمية.

ويمكن القول بأن الفضل يرجع في حماية الخصوصية على الصعيد الدولي لجهود المنظمات الدولية والإقليمية، والتي كان لها الأثر البيّن في صياغة النظام القانوني لخصوصية البيانات الشخصية)، غير أن القانون الأوروبي احتل الريادة في هذا الصدد وذلك من خلال اللائحة العامة لحماية البيانات (General Data Protection Regulation (GDPR بالاتحاد الأوروبي، والتي تمثل قانونًا نموذجيًا للعديد من التشريعات الوطنية داخل الاتحاد الأوروبي وخارجه[٥٨].

[٥٨] دراسة نقدية لقانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، مرجع سابق، ص١٢.

(ISSN: 2537- 0758)

الفرع الثاني
حماية البيانات الشخصية في التشريعات الوطنية

تتنوع حماية البيانات الشخصية بالتشريعات الوطنية إلى حماية دستورية واردة في صلب الوثيقة الدستورية للدولة، وأخري في التشريعات الأدنى درجة من الدستور كقانون حماية البيانات، وفيما يلي بيان ذلك من خلال:

أولاً- الحماية الدستورية:

تشكل الأطر القانونية والتنظيمية جزءا أساسياً من منظومة حماية البيانات الشخصية، ولا يمكن الاستغناء عنها بالرغم من كل الإجراءات التقنية، أو الممارسات الشخصية، التي يمكن أن يلجأ إليها مستخدم تقنيات الاتصالات والمعلومات، لاسيما على مستوى تحديد المسؤوليات، ومنهجيات وأساليب الحماية وإقرار الموجبات على معالج البيانات، ومستثمرها، أو ناقلها[٥٩].

فالأصل أن حماية البيانات الشخصية للأفراد في أي مجتمع منوطه بالمشرع الداخلي؛ كونه الأقدر على تقييم سبل الحماية للبيانات الشخصية لأفراد مجتمعة، وطرق المواجهة الجنائية لجرائم الاعتداء عليها، فالاتفاقيات الدولية أو الإقليمية توجه التشريع الداخلي نحو السعي لفرض أكبر قدر من الحماية للبيانات الشخصية، غير أنها ليس لها سلطان ملزم على تلك الدول؛ لذلك فإن التشريعات الداخلية للدول أعضاء الجماعة الدولية هي المعنية بشكل أساسي بحماية البيانات الشخصية، عبر ما تقرره من حماية للخصوصية في الدساتير أو حماية مباشرة للبيانات الشخصية في تشريع خاص.

وقد تناول التعديل الرابع لدستور الولايات المتحدة الأمريكية الصادر عام ١٧٨٩ أنه (لا يجوز المساس بحق الشعب أن يكونوا آمنين في أشخاصهم ومنازلهم ومستنداتهم ومقتنياتهم، من أي تفتيش أو مصادرة غير معقولة، ولا يجوز إصدار مذكرة بهذا الخصوص إلا في حال وجود سبب معقول معزز باليمين أو الإقرار..)[٦٠]، وفي فرنسا أقر المشرع تكريس مفهوم الحق في الحياة الخاصة، وحماية الحياة الخاصة كحق عام على نحو سابق من إقرار النظام القانوني الأمريكي له، غير أن ما يتعين ملاحظته أن اللغة الفرنسية تنطوي على مرادفات لتعبير الحياة الخاصة la Vie privée؛ وتبعا لذلك

---

[٥٩] د. منى الأشقر جبور، د محمود جبور، مرجع سابق، ص٦١.

[٦٠] في الأول من مارس عام ١٧٩٢ أعلن وزير خارجية الولايات المتحدة الأمريكية، توماس جيفرسون بأن هذا التعديل أصبح جزءً من الدستور الأمريكي.

فإن النظام القانوني الفرنسي ينطوي على اصطلاحات عديدة للدلالة على الخصوصية إضافة لاصطلاح الحياة الخاصة كالحق في السرية، والحق في الخلوة، والأهم الحق في الألفة الذي جرى استخدامه تشريعياً في ذات نص المادة (٩) من قانون ١٩٧٠ المعدل للقانون المدني الفرنسي، التي كرست للاعتراف بمبدأ حماية الحياة الخاصة[٦١]، وفي تصوري أن الحق في الحياة الخاصة في فرنسا يجد أساسه الدستوري في المادة (٢) من إعلان حقوق الإنسان والمواطن الصادر عام١٧٨٩ الذي تكفل بحماية الحرية بمختلف صورها، والمادة (٦٦) من دستور ١٩٥٨ التي تكفل الحرية الفردية.

وفيما يتعلق بالمملكة العربية السعودية فقد جاء في المادة السادسة والعشرون من النظام الأساسي للحكم[٦٢] بأنه (تحمى الدولة حقوق الإنسان وفق الشريعة الإسلامية)، ولا شك بأن الحق في الخصوصية أحد أهم حقوق الإنسان، وقد حفلت الشريعة الإسلامية بالعديد من الآيات القرآنية للتكريس لهذا الحق منها قوله تعالى{ يَا أَيُّها الذين آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وتُسَلِّمُوا عَلَى أَهْلِها ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ (٢٧) فَإِنْ لَمْ تَجِدُوا فِيها أحدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤذن لَكُمْ وَإِنْ قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ واللَّهُ بِمَا تَعْمَلُون عليمٌ (٢٨)[٦٣]، وقول رسول الله صلى الله عليه وسلم (إياكم والظن فإن الظن أكذب الحديث، ولا تحسسوا ولاتجسسوا، ولا تناجشوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا وكونوا عباد الله إخوانا)[٦٤]، وتضمنت المادة الأربعون من النظام الأساسي للحكم إمعاناً في حمايتها للحياة الخاصة للأفراد حرمة للمراسلات الخاصة والمحادثات الهاتفية وغيرها من الأمور التي يعد التطفل عليها نوعاً من انتهاك لحرمة الحياة الخاصة للأفراد (كالمراسلات البرقية، والبريدية، والمخابرات الهاتفية، وغيرها من وسائل الاتصال، مصونة، ولا يجوز مصادرتها، أو تأخيرها، أو الاطلاع عليها، أو الاستماع إليها، إلا في الحالات التي يبينها النظام).

---

[٦١] د مروة زين العابدين سعد صالح، مرجع سابق، ص١٤، ١٣.

[٦٢] الصادر بالأمر الملكي رقم (أ/٩٠) وتاريخ ١٤١٢/٨/٢٧هـ. وهو المقابل (للدستور) في النظم القانونية المقارنة.

[٦٣] سورة النور الآيتان ٢٨، ٢٧.

[٦٤] صحيح البخاري، عبد الله محمد بن إسماعيل بن إبراهيم بن المغيرة البخاري، كتاب الأدب، باب يا أيها الذين آمنوا اجتنبوا كثيراً من الظن، الطبعة الأميرية، القاهرة، ١٣١١هـ، ج٨، ص١٩.

(ISSN: 2537- 0758)

وفي مصر نص الدستور المصري[٦٥] في المادة (٥٧) منه بأن "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".

ويثار تساؤل هل تعد النصوص في الدستورية أساساً قانونياً لإضفاء الحماية والخصوصية على البيانات الشخصية أم لا؟

يجاب على هذا التساؤل بأن النص الدستوري يعد بلا شك أساساً قانونياً لضمان خصوصية البيانات الشخصية، مع الوضع في الاعتبار أن النصوص التي حمت الحق في الخصوصية وحرمة الحياة الخاصة دخل الدساتير هي بشكل عام نصوص توجيهية، أي تقوم بتوجيه السلطة التشريعية لسن قانون تفصيلي يحمي تلك البيانات؛ الأمر الذي معه يستلزم تدخل السلطة التشريعية لسن القوانين الداعمة للنص الدستوري. ولما كانت التشريعات المصرية تخلو من أي إطار قانوني ينظم عملية حماية البيانات الشخصية المعالجة إلكترونياً أثناء جمعها أو تخزينها أو معالجتها، لذلك جاء قانون حماية البيانات الشخصية المصري١٥١لسنة ٢٠٢٠ لينظم التعامل مع البيانات الشخصية للأفراد على نطاق واسع، بحيث يكشف عن صور حق الأشخاص في حماية بياناتهم الشخصية، ويجرم جمع البيانات الشخصية بطرق غير مشروعة أو بدون موافقة أصحابها، كما يجرم معالجتها بطرق تدليسيه أو غير مطابقة للأغراض المصرح بها من قبل صاحب البيانات، كما يتناول القانون أيضا تنظيم نقل ومعالجة البيانات عبر الحدود بما يعود بالنفع على المواطنين وعلى الاقتصاد القومي، بما يتوافق مع المعايير الدولية في مجالات حماية البيانات الشخصية، وذلك من خلال قواعد ومعايير واشتراطات يضعها، ويباشر الإشراف عليها المركز المنشأ لهذا الغرض[٦٦].

---

[٦٥] المنشور في الجريدة الرسمية– العدد ٣ مكرر (أ)– السنة السابعة والخمسون، الموافق ١٨ يناير سنة ٢٠١٤م، والمعدل في ٢٣ أبريل ٢٠١٩.

[٦٦] المذكرة الإيضاحية لمشروع قانون حماية البيانات الشخصية، الصادرة من وزارة العدل، بتاريخ ٢٠١٩/٢/١م. ص٢، ١.

وحيث إن النصوص الدستورية الحالية تعتبر حماية البيانات الشخصية للأفراد الطبيعيين في البيئة الرقمية هو حق أساسي من حقوق الإنسان، حيث ترتبط تلك البيانات بحرمة الحياة الخاصة للمواطنين طبقا لنص المادة (٥٧) من الدستور. وتتطلب مزيداً من الاحتياطات والإجراءات الخاصة اللازم اتباعها أثناء تداولها بين أرجاء المجتمع وخارجه؛ وذلك للحفاظ على خصوصيتهم، وحظر استخدام بياناتهم إلا بموافقتهم من خلال إطار تشريعي ينظم عملية حماية وتداول هذه البيانات في إطار الممارسات المقبولة واحترام حقوق الإنسان، كما أن تنظيم تلك الحماية ينعكس بشكل إيجابي على رفع مستويات أمن الفضاء المعلوماتي، باعتباره جزءًا أساسيا من منظومة الاقتصاد والأمن القومي، طبقا لنص المادة (٣١) من الدستور المصري[٦٧].

وجدير بالذكر أن الصور التي عددها النص الدستوري كنماذج للحق في الخصوصية المرادف لحرمة الحياة الخاصة وردت على سبيل المثال وليس الحصر، وليس في عدم ذكر البيانات الشخصية إغفال لها؛ باعتبار أن الحق في الخصوصية يشملها كونها مكملة للشخصية، ويري الباحث من خلال استقراء الدساتير المقارنة كالدستور الفرنسي، والأمريكي، والنظام الأساسي للحكم في المملكة العربية السعودية، أنها لم تتضمن النص صراحة علي حماية حق الخصوصية في سرية البيانات بشكل واضح، وإنما جاءت جميع نصوص الدساتير المقارنة بوضع أساس دستوري لحماية حرمة الحياة الخاصة، والتي تعد مفهومها أوسع من البيانات الشخصية، وهو ما سلكه المشرع الدستوري المصري، إلا أن هذا لا يقدح في كون النصوص الدستورية أساساً قانونياً لتلك الحماية، فليس من وظيفة الدستور تفصيل الحقوق والحريات جميعها وإنما يمنح المشرع سلطة في تقنينها، وبالتالي يلقي علي كاهل المشرع وضع التنظيم القانوني الذي من خلاله يتكفل بحماية البيانات الشخصية.

ثانياً- التشريعات الوطنية:

أولت العديد من التشريعات الوطنية حماية خاصة للبيانات الشخصية، ولعل أول الدول الغربية التي وضعت تشريع لحماية البيانات الشخصية هي السويد عام ١٩٧٣وجرى عليه تعديلات عدة في الأعوام ١٩٧٩ و١٩٨٢ و١٩٨٩ و١٩٩٠ و١٩٩٢، حتى حل محله قانون حماية البيانات الشخصية الحالي لعام ١٩٩٨ وجاءت

[٦٧] المذكرة الإيضاحية لمشروع قانون حماية البيانات الشخصية، الصادرة من وزارة العدل، بتاريخ ٢٠١٩/٢/١٩م. ص١.

(ISSN: 2537- 0758)

هذه المعالجة التشريعية نتيجة للتدخل الدستوري في الفقرة الثانية من المادة الثالثة من الفصل الثاني من الدستور السويدي عام ١٩٨٨[٦٨]، ثم تلا ذلك الولايات المتحدة الأمريكية عام ١٩٧٤، حيث أصدرت عدة تشريعات بشأن حماية الخصوصية منها: قانون الخصوصية لعام ١٩٧٤، وقانون خصوصية الاتصالات الإلكترونية لعام ١٩٨٦، وقانون خصوصية حماية المستهلك لعام ١٩٩٧ وقانون حماية خصوصية الضمان الاجتماعي لعام ١٩٩٧، وقانون خصوصية المعطيات لعام ١٩٩٧، أعقبها ألمانيا حيث أصدرت عام ١٩٧٧ قانوناً بشأن حماية المعطيات وأجريت عليه تعديلات أعوام ١٩٩٠ و ١٩٩٤، ثم صدر قانون حماية البيانات عام ٢٠٠٠، وجاءت فرنسا كرابع دولة علي مستوى العالم في وضع قانون في ٦ يناير ١٩٧٨ بشأن حماية المعالجات الآلية للبيانات والحريات والذي لحقه التعديل عدة مرات[٦٩].

وبموجب هذا القانون يلتزم المشرع الفرنسي بمستوى من الحماية التشريعية الشاملة التي جاء النص عليها في الاتفاقية الأوروبية لحماية الأفراد في مجال المعالجة الآلية للبيانات الشخصية، وما تم إقراره من قواعد وإجراءات لحماية خصوصية المعلومات وفقا لما تقضي به اللائحة الأوروبية لحماية البيانات بشأن حماية الأشخاص أثناء المعالجة الآلية للبيانات وأثناء الحركة لها.

وتعد الفترة منذ ١٩٦٠ إلى ١٩٧٠ هي التوطئة الحقيقية لنشأة قانون معالجة البيانات والملفات والحريات الفرنسي، وقد شهدت مناقشات وتساؤلات منها ما طرحه النائب العام لمجلس الدولة الفرنسي آنذاك حول تأثير تطور المعلوماتية على الحياة العامة وعلى القرارات الإدارية؛ لذلك تم إنشاء لجنة لهذا الغرض سنة ١٩٧٤من أجل تقديم مقترحات ستكون في الأصل أساس قانون ٦ يناير ١٩٧٨ الذي تم تعديله عدة مرات منذ ذلك التاريخ[٧٠]، لجعله متوافقا مع اللائحة العامة لحماية البيانات ومهام

---

[٦٨] وقد تضمنت تلك المادة بأنه: لا يجوز قيد أي بيان في سجل عام يتعلق بمواطن سويدي دون أن يستند لرضاه فقط.

[٦٩] د شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية (دراسة تحليلية لحق الاطلاع على البيانات في فرنسا)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد ٥٧، إبريل ٢٠١٥، ص٢٣، ٢٢.

[٧٠] د. علي كريمي تأثير التطور التكنولوجي على حقوق الإنسان الحياة الخصوصية وحماية البيانات الشخصية "نموذجا"، مجلة أبحاث احتجاج بالمغرب، مقاربة الإنسان السلوكيات والقيم العدد ٦١ ٦٢ لسنة ٢٠١٥، ص٩٠

وسلطات اللجنة الوطنية وتوسيع نطاق البيانات الحساسة إلى غاية ٢٠١٨ حيث صدر القانون رقم ٤٩٣-٢٠١٨ المؤرخ ٢٠ يونيو ٢٠١٨ بشأن تعديل القانون لينسجم مع ما أقرته اللائحة الأوروبية لحماية البيانات الصادرة في ٢٧ أبريل ٢٠١٦ والنافذه في مايو ٢٠١٨، وأهم ما جاء فيه أنه قرر مزيداً من الاستثناءات ويشمل ذلك معالجة البيانات البيومترية (كبصمات الأصابع) الضرورية لضوابط الوصول إلى مكان العمل، والحواسيب والتطبيقات المستخدمة في مكان العمل وتكييف دور اللجنة الوطنية للمعلوماتية والحريات وسلطاتها في السيطرة و المعاقبة"[٧١].

ومن مظاهر مواجهة المشرع الفرنسي الجنائية التعدي على البيانات الشخصية ما جاء بقانون العقوبات من العقاب على المساس بنظم المعالجة الآلية بمقتضى المادة 1-323 إلى المادة 8-323. فيعاقب على مجرد الدخول للنظام المعلوماتي دون استلزام وجود قصد خاص من ذلك الدخول مشددا في ذلك العقوبة حالة ما اذا ترتب على ذلك محو أو تعديل في المعلومات أو تغبير سير عمل النظام المعلوماتي وكذلك المواد1-226 إلى المادة 7-226 من قانون العقوبات والتي تمت تعديلها عدة مرات الخاصة بالاعتداء على الحياة الخاصة[٧٢].

وفي مصر برز اهتمام المشرع المصري بالبيانات الشخصية لمواطنيه وأن كان لم يفرد له قانوناً مستقلاً حتى عهد قريب، كون الفرد عماد المجتمع وهويته جزء من شخصيته، وهي الأساس في اكتساب الحقوق، والتحمل بالالتزامات لذا حرص المشرع المصري على الاهتمام بالبيانات الشخصية للأفراد، كالأوراق الثبوتية كالبطاقة الشخصية، وجواز السفر، وذلك في إطار تنظيمي وقانوني، كنص المادة ١٣ من قانون الاحوال المدنية رقم ١٤٣ لسنة ١٩٩٤ (تعتبر البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين والتي تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين الملحقة سرية، ولا يجوز الاطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون وفقا لأحكامه).

---

(71) LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

(٧٢) د. رشيدة بوكر، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، العدد الثاني، ٢٠٢٢م، المجلد ٧، ص٨٥، ٨٤

(ISSN: 2537- 0758)

وتكريساً لحرصه على حماية البيانات الشخصية فيما يتعلق ببياناتهم المالية فقد قرر المشرع المصري في قانون البنك المركزي والجهاز المصرفي الصادر بالقانون رقم ١٩٤لسنة ٢٠٢٠ في المادة (١٤٠) منه بأن (تكون جميع بيانات العملاء وحساباتهم وودائعهم وأماناتهم وخزائنهم في البنوك وكذلك المعاملات المتعلقة بها سرية، ولا يجوز الاطلاع عليها أو إعطاء بيانات عنها بطريق مباشر أو غير مباشر إلا بإذن كتابي من صاحب الحساب أو الوديعة أو الأمانة أو الخزينة أو من أحد ورثته أو من أحد الموصى لهم بكل هذه الأموال أو بعضها، أو من نائبه القانوني أو وكيله أو بناء على حكم قضائي أو حكم تحكيم.

ومع عدم الإخلال بالاستعلامات الواردة بهذا القانون، يسرى الحظر المنصوص عليه في الفقرة الأولى من هذه المادة على جميع الأشخاص والجهات بما في ذلك الجهات التي يخولها القانون سلطة الاطلاع أو الحصول على الأوراق أو البيانات المحظور إفشاء سريتها طبقا لأحكام هذا القانون، ويظل هذا الحظر قائماً حتى ولو انتهت العلاقة بين العميل والبنك لأي سبب من الأسباب)[٧٣].

ومن مظاهر الحماية للبيانات الشخصية ما تضمنته المادة (٢٣) من قانون تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على أنه "يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية...".

وتوج المشرع جهوده في حماية البيانات الشخصية بإقراره قانوناً لحمايتها حمل رقم ١٥١لسنة ٢٠٢٠، تناول بشكل مفصل كل ما يتعلق بالبيانات الشخصية وسبل حمايتها، والصور التجريمية للاعتداء عليها، وجاء هذا القانون تلبية للنداءات المتكررة من المعنيين من المتخصصين في مجال حماية البيانات الشخصية والحقوقيين، لإرساء حماية حقيقة لحق المواطنين في حماية بياناتهم الشخصية في العصر الرقمي.

[٧٣] الجريدة الرسمية– العدد ٣٧مكرر (و) في ١٥ سبتمبر ٢٠٢٠.

الفصل الأول
الجرائم المتعلقة بالمعالجة غير المشروعة للبيانات الشخصية

تمهيد وتقسيم:

تشكل معالجة البيانات الشخصية مجموعة من العمليات التي يتم إجراؤها على البيانات الشخصية، وقد تتم بوسائل إلكترونية أو غير ذلك، غير أن المشرع المصري في قانون حماية البيانات الشخصية ١٥١لسنة ٢٠٢٠ قصر حمايته الجنائية على البيانات الشخصية المعالجة إلكترونياً، وتشمل التجميع أو التسجيل، أو التنظيم أو الهيكلة أو التخزين، أو التغيير أو الاسترجاع، أو الاستخدام أو الإفصاح عن طريق الإرسال أو النشر، وكلها صور لمعالجة البيانات الشخصية حسبما أوردت المادة الرابعة من اللائحة الأوروبية لحماية البيانات، ولخطورة تلك العمليات التي ترد على البيانات الشخصية للأفراد ومساسها المباشر بخصوصيتهم، فقد أفرادت التشريعات المعنية بحماية البيانات الشخصية ومن بينها التشريع المصري مجموعة من النصوص التجريمية المؤثمة للجرائم المتعلقة بالمعالجة غير المشروعة للبيانات الشخصية وفيما يلي بينها من خلال:

المبحث الأول: المعالجة غير المشروعة للبيانات والإخلال بشروط جمعها والاحتفاظ بها.

المبحث الثاني: الاعتداء على حقوق المعني بالبيانات وإخلال الحائز والمتحكم والمعالج بالتزاماتهم.

المبحث الأول
المعالجة غير المشروعة للبيانات والإخلال بشروط جمعها والاحتفاظ بها

تمهيد وتقسيم:

تعد الجرائم المتعلقة بالمعالجة غير المشروعة للبيانات الشخصية المعالجة إلكترونياً أحد أهم الموضوعات التي تناولها المشرع المصري في قانون حماية البيانات الشخصية المصري ١٥١لسنة ٢٠٢٠ وكذلك في التشريعات الجنائية المقارنة، كون هذا النوع من الجرائم يشكل خطراً على مختلف التعاملات الإلكترونية التي يقوم بها الفرد، والمجتمع والدولة على حد سواء، ولا تتوقف آثارها على المستوى الداخلي فحسب، بل تمتد لتشمل المستوى الدولي؛ لذلك سعت التشريعات الجنائية ومن بينها التشريع المصري إلى صياغة جملة من القواعد و النصوص العقابية، لردع كل من تسول له نفسه مقارفة تلك الجرائم وفيما يلي بيان ذلك من خلال:

(ISSN: 2537- 0758)

المطلب الأول: المعالجة غير المشروعة للبيانات العادية
المطلب الثاني: المعالجة غير المشروعة للبيانات الحساسة
المطلب الثالث: الإخلال بشروط جمع ومعالجة والاحتفاظ بالبيانات.

المطلب الأول
المعالجة غير المشروعة للبيانات الشخصية العادية

كتب الفقيه الفرنسي ميلر– Mellor عام ١٩٧٢، "إن الكمبيوتر بشراهته لجمع المعلومات على نحو لا يمكن وضع حد لها، وما يتصف به من دقة ومن عدم نسيان ما يخزن فيه، قد يقلب حياتنا رأساً على عقب، يخضع فيها الأفراد لنظام رقابة صارم ويتحول المجتمع إلى عالم شفاف تصبح فيه بيوتنا ومعاملاتنا المالية وحياتنا العقلية والجسمانية عارية لأي مشاهد"[٧٤].

وقد وضع المشرع الفرنسي تعريفاً لمعالجة البيانات الشخصية وذلك في المادة (٣/٢) من القانون رقم معالجة البيانات والملفات والحريات١٩٧٨/١٧ بأنها "أي إجراء يتعلق بالبيانات الشخصية أياً كانت الطريقة المستخدمة في هذا الإجراء، ولا سيما جمع أو تسجيل أو تنظيم أو تخزين أو تكييف أو تعديل أو استخراج أو استشارة أو استخدام أو الاتصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال التزويد أو المصالحة أو الربط البيني، وكذلك الحجب أو المحو أو التدمير"، ووفقاً للتعريف الذي أورده المشرع الفرنسي فقد جاء متوسعاً جداً، للدرجة التي يمكن معها القول بأنه يكاد لا يوجد إجراء يتخذ بشأن البيانات الشخصية ولا يعد معالجة لها.

أما المشرع المصري فقد عرف معالجة البيانات بأنها: 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 تحليلها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئياً أو كلياً[٧٥]، ويظهر جلياً الفرق بين كل من

---

[٧٤] د يونس عرب، المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، منشور على شبكة المعلومات الدولية– الإنترنت، https://kenanaonline.com/users/ahmedkordy/posts/323471 تاريخ الزيارة ٢٠٢٣/٣/١٥م.

[٧٥] المادة الأولى من قانون حماية البيانات الشخصية المصري.

تعريف المشرع الفرنسي والمصري في أن الأخير اشتراط بأن تكون عملية المعالجة إلكترونية أو تقنية، في حين أن نظيره الفرنسي لم يشترط وسيلة بعينها في المعالجة فقد تتم إلكترونياً أو يدوياً، ومن جانبي أرى تأييد المشرع الفرنسي لأن من شأن تعريفه التوسع في تعريف معالجة البيانات الشخصية، وعدم قصر الوسيلة المستخدمة فيها على وسيلة بعينها وفي ذلك بسط مزيد من الحماية لتلك البيانات. ومن خلال التعريفان اللذان ساقهما المشرع الفرنسي والمصري يمكن القول بأن هناك نوعان من معالجة البيانات الشخصية: إحداهما المعالجة المشروعة وهذه لا مشكلة فيها كونها تتم وفقاً للقانون، والأخرى معالجة غير مشروعة ويقصد بها: 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[٧٦]، وقد أثرت تسمية المعالجة غير المشروعة للبيانات الشخصية العادية تمييزاً لها عن البيانات الشخصية الحساسة كون المشرع المصري وقد ميز في المعاملة العقابية لمرتكبي تلك الجرائم، فجاء متشدداً في العقاب في الثانية عن الأولى.

أولاً- نص التجريم:

قررت المادة (٣٦) من قانون حماية البيانات الشخصية بأن "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.

وتكون العقوبة الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكب ذلك مقابل الحصول على منفعة مادية أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر".

[٧٦] د. ياسر محمد اللمعي، مرجع سابق، ص١٨٢، ١٨١.

(ISSN: 2537- 0758)

ثانياً-علة التجريم:

ترجع العلة من تجريم المشرع سلوك بعينه إلى صيانة حق قدر المشرع جدارته بالحماية الجنائية[٧٧]؛ لذلك سعى المشرع إلى تجريم المعالجة غير المشروعة للبيانات الشخصية؛ لتحقيق الردع لكل من الحائز والمتحكم والمعالج من أي اعتداء يمكن أن يقع منهم على البيانات الشخصية للأفراد، حيث تكمن الخطورة في الهدف والقصد من معالجة البيانات الشخصية بطريقة غير مشروعة في الاستغلال السيء لتلك البيانات وإلحاق الضرر بالمعني بها، لذلك عد تجريم المعالجة غير المشروعة للبيانات الشخصية خطوة استبقيه لما قد يصيب المعني بها مستقبلاً من ضرر، عوضاً عن ذلك فيه حماية لخصوصية الأفراد في المجتمع عبر حماية بياناتهم الشخصية، كونها جزءً راسخ من حماية حق الإنسان في الخصوصية.

ثالثاً-محل الجريمة:

تتطلب القانون أن يقع فعل الجمع أو الإفشاء أو الإتاحة أو التداول لبيانات شخصية، واشترطت في تلك البيانات أن تكون معالجة إلكترونياً، فإذا لم تكن تلك البيانات شخصية فلا جريمة، وأن كانت تلك البيانات شخصية غير معالجة إلكترونية ووقع عليها أي من الأفعال الواردة في النص التجريمي فلا ينطبق عليها النص، وإن كان ذلك لا يمنع من تطبيق أي نص جزائي آخر ملاقي لتلك الواقعة.

رابعاً-أركان الجريمة:

يقتضي التعرف على جرائم الحائز، المتحكم، والمعالج بشأن المعالجة غير المشروعة للبيانات الشخصية العادية بيان الركن المادي والمعنوي للجريمة، إلى جانب معرفة الركن المفترض فيها وهو المفترض وجودة في كافة جرائمهم.

١ – الركن المفترض (صفة الجاني):

يفترض في تلك الجريمة أن تقع من قبل الحائز، المتحكم، أو المعالج أن يكون الجاني أما حائزاً أو متحكماً أو معالجاً للبيانات الشخصية وفيما يلي تعريفهم على النحو التالي:

وعرفت المادة الأولى من قانون حماية البيانات الشخصية المصري **الحـائز** بأنه: أي شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعليًا ببيانات شخصية في أي

---

[٧٧] د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، ٢٠٠٦، ص٦٤

صورة من الصور، أو على أي وسيلة تخزين سواءً أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة، ومن خلال النص يفهم بأن مصطلح الحائز اشتق من الحيازة وهي السيطرة الفعلية لشخص على شيء يجوز التعامل فيه، وقد استقر الفقه والقضاء في مصر على أنه يكفي لتحقق الحيازة أن يكون سلطان الجاني مبسوطاً على الشيء ولو أحرزه مادياً شخصاً غيره[٧٨].

والمتحكم: أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها، طبقًا للغرض المحدد أو نشاطه، ويقابله في النظام السعودي ما يعرف بجهة التحكم: وهي أي جهة عامة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك؛ سواء أباشرت معالجة البيانات بوساطتها أم بوساطة جهة المعالجة[٧٩].

أما المعالج: أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته[٨٠].

وفي المملكة العربية السعودية تعرف جهة المعالجة في المادة الأولى من نظام حماية البيانات الشخصية: أي جهة عامة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها.

ووفقا للتعاريف التي أوردها المشرع المصري لكل من الحائز والمتحكم والمعالج فهي غير مقصورة على الشخص الطبيعي، بل يتصور أن ترتكب تلك الجرائم بواسطة الشخص الاعتباري، فإذا كان الجاني شخصاً طبيعياً حركت الدعوى الجنائية في مواجهته مباشرة، أما إن كان شخصاً اعتبارياً فتحرك الدعوى الجنائية في مواجهة ممثلة القانوني.

٢- الركن المادي:

تقوم الجريمة على أركان منها الركن المادي الذيً لا قوام لها بدونه، ويتمثل في فعل أو امتناع يقع بالمخالفة لنص عقابي، مفصحاً بذلك عن أن ما يركن إليه القانون ابتداءً

---

[٧٨] د. فوزية عبد الستار، شرح قانون مكافحة المخدرات، دار النهضة العربية، القاهرة، ١٩٩٠، ص٣٥، ٣٣.

[٧٩] المادة الأولى من نظام حماية البيانات الشخصية السعودية.

[٨٠] المادة الأولى من قانون حماية البيانات الشخصية المصري.

(ISSN: 2537- 0758)

في زواجره ونواهيه، هو مادية الفعل المؤاخذ على ارتكابه، إيجابياً كان هذا الفعل أو سلبياً[٨١]، وتتسم تلك الجريمة بأنها من الجرائم الشكلية لا جرائم الضرر، إذ لا يشترط أن يترتب على سلوكها الإجرامي تحقق نتيجة إجرامية معينة ومن ثم فالركن المادي لها يتكون من النشاط الإجرامي فحسب[٨٢]، وفي فرنسا يقوم الركن المادي للجريمة بتوافر عنصرين أولهما السلوك الإجرامي والذي يتمثل في المعالجة الإلكترونية للبيانات الشخصية، سواء كان ذلك في شكل إدخال بيانات أو تصنيفها أو توزيعها، أو دمجها مع بيانات أخري أو تحليلها لكي تعطي معلومة ذات دلالة خاصة عن المعني بها[٨٣]، وثانيهما إجراء هذه المعالجة دون الحصول على موافقة اللجنة الوطنية للمعلوماتية والحريات، استناداً لما ورد في المادتان ١٦، ١٥من قانون معالجة البيانات والملفات والحريات الصادر سنة ١٩٧٨، وفي مصر يتحقق الركن المادي في لتلك الجريمة بأفعال متعددة قد تكون على سبيل الانفراد أو مجتمعة منها:

(أ) الجمع:

عرف المنظم السعودي جمع البيانات الشخصية بأنها حصول جهة التحكم على البيانات الشخصية وفقاً لأحكام النظام، سواء من صاحبها مُباشرةً أو ممن يُمثله أو ممن له الولاية الشرعية عليه أو من طرف آخر[٨٤]، ويتحقق الركن المادي في هذه الجريمة بكل فعل إيجابي من شأنه جمع للبيانات الشخصية، ويستوي لدى القانون أن يكون يحقق الجاني منفعة لنفسه أم للغير أو عدم تحقق منفعة مطلقاً، وجمع البيانات في غير الأحوال المصرح بها قانوناً أو بدون موافقة صاحبها أحد أبرز صور انتهاك الحق في خصوصية البيانات الشخصية للأفراد، وبمفهوم المخالفة فإذا كان الجمع مصرح به وفقاً للقانون فلا غضاضة في ذلك، وذات الأمر إذا تم الجمع بموافقة صاحب البيانات. غير أن أبرز أوجه النقد التي يمكن توجيهها لقانون حماية البيانات الشخصية المصري ١٥١ لسنة٢٠٢٠ استخدامه لعديد من المرات عبارة "الأحوال المصرح بها قانوناً" وحيث لم

---

[٨١] الدعوى رقم ١٧٣لسنة ٣١ دستورية، جلسة ٢٠١٧/١٢/٢، الموسوعة الذهبية للقضاء الدستوري المصري، ١٩٦٩– ٢٠١٩، المجلد الأول. المحكمة الدستورية العليا، القاهرة، ص٢٣١.

[٨٢] د محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت دراسة مقارنة، الطبعة الأولى، دار الفكر والقانون، المنصورة، ٢٠١٣، ص٦٧.

[83] Patrice GATTEGNO, Droit pénal spécial, Dalloz, 1995, p. 156.

[٨٤] المادة الأولى من نظام حماية البيانات الشخصية السعودي.

يبين تلك الحالات المصرح بها، حتى أن قراءة بعض مواد القانون قد تكون غير مفهومة أو غير قابلة للتطبيق بسبب وجود هذه العبارة التي تفرض قيداً أو تمنح استثناء دون أن توضح ماهية هذا القيد أو الاستثناء، ومما ساعد على هذا الغموض عدم صدور اللائحة التنفيذية للقانون حتى وقت كتابة هذا البحث، ويجدر بالمشرع المصري أن يحدد على وجه الدقة الحالات المصرح بها قانوناً، التي تبيح معالجة البيانات الشخصية للشخص المعني دون موافقته، لكنها رغم ذلك تظل مشروعة كونها مصرح بها قانوناً.

وجمع البيانات هي المرحلة الأولية لمعالجتها، والجمع يشترط لقيام الجريمة أن يتم بطرق غير مشروعة، ومعناها الحصول على بيانات شخصية لفرد أو لعدة أفراد، وتنظيمها وترتبها على نحو يسمح باستعمالها مستقبلاً، وقد يكون جمع تلك البيانات لفرد بعينه أو لمجموعة من الأفراد، وتضمنت المادة الثانية من قانون حماية البيانات الشخصية المصري بأنه لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا.

وقررت المادة (السادسة) من قانون الفرنسي المتعلق بمعالجة البيانات والملفات والحريات هذه الحماية حيث اشترطت أن تجمع وتعالج البيانات الشخصية الخاضعة للمعالجة بطريقة مشروعة وقانونية، ولغاية معينة وصريحة ومشروعة، وألا تتم المعالجة بعد ذلك إلا من أجل هذه الغاية المحددة لها، وفي هذه الحالة يجب أن تكون صحيحة وكاملة، وفقاً لما تقتضي الحالة، وأن تحفظ بشكل يمكن من إظهار شخصية الفرد المعني بالبيانات، ولمدة لا تفوق المدة الضرورية لتحقيق الغاية التي جُمعت وعُولجت من أجلها، واشترطت المادة (السابعة) من ذات القانون أن تسبق أي معالجة للبيانات الشخصية الحصول على موافقة الشخص المعني بهذه البيانات، وأن تتوافر شروط أخرى كاحترام الالتزام القانوني المفروض على المسئول عن المعالجة، و حفظ الحياة الخاصة للفرد المعني بها، و تنفيذ خدمة عامة من طرف المسئول عن المعالجة أو مستقبلها بشرط مراعاة مصلحة الفرد المعني إلى جانب الحقوق والحريات الأساسية[٨٥].

وجاء في المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية التي تنظم حماية الخصوصية وتدفق البيانات عبر الحدود[٨٦]، فيما يتعلق بجمع البيانات بأنه لابد أن

---

[٨٥] د. ياسر محمد اللمعي، مرجع سابق، ص١١٤

[٨٦] اعتمدت في ٢٣ سبتمبر ١٩٨٠.

(ISSN: 2537- 0758)

تكون هناك حدود لجمع البيانات الشخصية، وأن أي بيان من هذا النوع لابد من الحصول عليه بوسائل مشروعة وعادلة وبطريقة مناسبة، وبعلم وموافقة صاحب البيانات، وأن تكون تلك البيانات وثيقة الصلة بالغرض الذي جمعت لأجله، ويجب أن يحدد الأغراض التي تجمع البيانات الشخصية لها في موعد لا يتجاوز وقت جمع البيانات، ويجب أن يقتصر الاستخدام اللاحق لتلك البيانات على تحقيق الأغراض التي جمعت لغرضها تلك البيانات أو التي لا تتعارض معها[٨٧]. وقد أكدت محكمة النقض الفرنسية بأن من صور انتهاك الحق في حماية البيانات الشخصية ما ينتج بشكل خاص عن التقاط أو تخزين هذه البيانات دون موافقة الشخص المعني[٨٨].

(ب) المعالجة:

جاء في تعريف معالجة البيانات (DATA PROCESSING) بأنها: مجموعة العمليات التي تجرى على البيانات لتحويلها إلى شكل مفيد وذا معنى، أي تحويلها إلى معلومات يمكن الاستفادة منها، وذلك من خلال إخضاعها لمجموعة من العمليات الحسابية والمنطقية باستخدام إمكانات النظام الآلي؛ بغرض الحصول على ما يمكن الاستعانة به في اتخاذ القرار، مما يعني أن معالجة البيانات تتضمن مجموعة من العمليات التي يتم من خلالها تحويل المدخلات أي البيانات إلى مخرجات أي إلى معلومات عن طريق عملية معالجة البيانات التي تقوم بها البرامج[٨٩].

أما معالجة البيانات الشخصية إلكترونياً فيقصد بها: استخدام الحاسب الآلي أو أحد تطبيقاته المختلفة؛ بأي إجراء خاص بالبيانات الشخصية، يتم عبر استخدام الكمبيوتر من تنظيم أو تعديل أو تصنيف للمعلومات الشخصية في قواعد البيانات[٩٠]، وجاء في

---

[٨٧] ريموند واكس، مرجع سابق، ص١١٧، ١١٦

[88] **Cour de cassation, criminelle, Chambre criminelle, 8 juillet 2015, 13-86.267, Publié au bulletin**

[٨٩] د. رنا أبو المعاطي محمد الدكروري، الحماية الجنائية للبيانات الشخصية، رسالة دكتوراه– كلية الحقوق جامعة المنصورة، ٢٠٢٢م، ص٦٤.

[90] Julien LE CLAINCHE: La protection des données personnelles nominatives dans le cadre de la recherche dans le domaine de la santé, Comparaison du droit français et du droit américain, Mémoire de D.E.A., Faculté de droit, des Sciences Economiques et de Gestion, Université Montpellier I 2000-2001.p7.

تعريفها بأنها: تلك العمليات التي تهدف إلى جمع البيانات الشخصية أو تسجيلها، أو حفظها أو تنظيمها، أو تغييرها أو استغلالها، أو استعمالها أو إرسالها، أو توزيعها أو نشرها أو إتلافها أو الاطلاع عليها[٩١].

وعلى الصعيد التشريعي عرفها المشرع المصري في المادة الأولى من قانون حماية البيانات الشخصية بأنها: 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 تحليلها، وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيا أو كليًا"

وعرفها النظام السعودي لحماية البيانات الشخصية بأنها: أي عملية تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر، والمشاركة في البيانات أو الربط البيني، والحجب، والمسح، والإتلاف[٩٢].

أما المعالجة غير المشروعة للبيانات الشخصية الإلكترونية فيقصد بها: 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[٩٣]، وتكمن خطورة هذه المعالجة بأنها تشكل اعتداءً خطيراً على من تخصه هذه البيانات، لأنها قد تؤدي لرسم صورة كاملة عنه دون علمه بذلك.

---

[٩١] أ/ أحمد سامر مقرش، د خالد الخطيب، الالتزام بالإخطار في معالجة البيانات الشخصية، مجلة بحوث جامعة حلب– سلسلة العلوم القانونية والشرعية، العدد ١٦ لعام ٢٠١٨، ص٢.

[٩٢] المادة الأولى من نظام حماية البيانات الشخصية السعودي (م/١٩) وتاريخ ١٤٤٣/٢/٩هـ، والمعدل بالمرسوم الملكي (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ.

[٩٣] د ياسر محمد اللمعي، مرجع سابق، ص١٨٢، ١٨١.

(ISSN: 2537- 0758)

(ج) الإفشاء:

ويقصد بالإفشاء، الكشف أو الإفصاح أو الإخبار للغير عن البيانات المحفوظة والمخزنة لدى مقدم الخدمة، ويستوي لدى القانون أن يكون الإفشاء كلياً ويشمل كافة البيانات الشخصية أم جزئياً ليشمل بعض البيانات[٩٤].

واستلزم قانون حماية البيانات الشخصية المصري أن ينصب موضوع الإفشاء على بيانات شخصية لدى الحائز أو المتحكم أو المعالج، هذه البيانات قد تخص فرد بعينة أو مجموعة من الأفراد، ولم يشترط القانون وسيلة معينة لحصول إفشاء البيانات، فقد يكون ذلك بأي ووسيلة من وسائل تقنية المعلومات أو حتى بطرق تقليدية شفاهه أو كتابةً أو بالإشارة، كما لا يعتد بعدد من حصل إليه إفشاء البيانات الشخصية المشمولة بالحماية، فقد يكون شخصاً واحداً؛ كالزوجة أو قريب أو صديق أو عدداً من الأشخاص[٩٥].

كما أن مسألة الإفشاء غير المشروع للبيانات الشخصية كأحد صور انتهاك الحق الخصوصية قد تأخذ مظهرها في بعض المهن التي تعتمد على سرية البيانات، كمهنة المحاماة والطبيب أو أعمال البنوك، بحيث يفترض احتفاظ صاحب المهنة بسرية البيانات الشخصية للزبون أو العميل بحكم التعامل القائم بينهما[٩٦]، حيث إن إفشاء الأسرار المهنية تعني الكشف عن واقعة لها صفة السر، صدرت ممن علم بها بمقتضى مهنته مع توافر القصد الجنائي[٩٧].

ويفترض في هذا السلوك بأن الجاني يحوز تلك البيانات؛ لذلك جرم القانون فعل حيازة البيانات بقصد تصنيفها أو نقلها لمعالجتها تحت أي شكل من الأشكال، كون

---

[٩٤] د. رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) مقارناً بالتشريعات المقارنة والمواثيق الدولية، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، ١٤٤١هـ-٢٠٢٠م، ص ٢٠٣.

[٩٥] د. حسنين عبيد، شرح قانون العقوبات- القسم الخاص، جرائم الاعتداء على الأشخاص والأموال، الطبعة التاسعة، دار النهضة العربية، ص٢٦٦.

[٩٦] أ/ خدوجة الدهبي، حق الخصوصية في مواجهة الاعتداءات الإلكترونية- دراسة مقارنة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف بالمسيلة-الجزائر، العدد الثامن، ديسمبر ٢٠١٧، المجلد الأول، ص١٥٠.

[٩٧] د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، ص١٠ وما بعدها.

الحيازة هي تمهيداً لعملية المعالجة، فجريمة الإفشاء هي من الجرائم ذات النتيجة، التي تقتضي تحقيق نتيجة تتمثل بالمساس بالحياة الخاصة للأفراد، ولا يشترط أن يكون الإفشاء لعديد من الأشخاص بل يكفي أن يكون لشخص واحد.

(د) الإتاحة:

تعد إتاحة بيانات شخصية معالجة إلكترونياً عن طريق الحائز أو المتحكم أو المعالج هي أحد صور السلوك الإجرامي التي تناولها قانون حماية البيانات الشخصية المصري فى المادة السادسة والثلاثون منه، ويقصد بها: كل وسيلة تحقق اتصال علم الغير بالبيانات الشخصية، كالاطلاع أو التداول أو النشر، أو النقل أو الاستخدام أو العرض، أو الإرسال أو الاستقبال أو الإفصاح عنها[٩٨]، ويفهم من ذلك بأنها السماح للغير بالاطلاع على البيانات الشخصية للمجني عليه، يستوى في ذلك أن يكون السماح قد تم بمقابل أو بدون مقابل، فلم يستلزم النص العقابي ضرورة تحصيل الجاني منفعة في مقابل إتاحة البيانات الشخصية للغير، ويقصد بالغير في نطاق تطبيق هذا القانون: أي شخص غير مختص بتلقي تلك البيانات وفقاً للأحكام المنصوص عليها قانوناً.[٩٩]

(ذ) التداول:

يأتي تداول البيانات الشخصية بواسطة الحائز أو المتحكم أو المعالج، كأحد الصور التجريمية التي تناولها المشرع العقابي بالعقاب في القانون، ويراد بتداول البيانات الشخصية التناقل والمبادلة بين الحائز أو المتحكم أو المعالج مع غير صاحبها على نحو غير مشروع.

٣- وسيلة ارتكاب الجريمة:

لم يشترط القانون المصري في الأفعال الإجرامية التي تشكل الركن المادي للجريمة أن تتم بوسيلة بعينها، وإنما أورد في نص الفقرة الأولى من المادة (٣٦) بأنه يتصور وقوع الجريمة "بأي وسيلة كانت"، فقد تكون هذه الوسيلة إلكترونية عن طريق أي وسيلة من وسائل تقنية المعلومات والتى تعرف بأنها "أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا

---

[٩٨] المادة الأولى من قانون حماية البيانات الشخصية المصري ١٥١ لسنة ٢٠٢٠.

[٩٩] د. خالد حسن أحمد، مرجع سابق، ص٧٨.

(ISSN: 2537- 0758)

أو لاسلكيًا"[١٠٠]، أو عبر الشبكة المعلوماتية وهي عبارة عن "مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها"[١٠١]، أو تتحقق الأفعال الواردة في النص التجريمي بشكل يدوي، وآية ذلك أنه من ظاهر النص أن محل الجريمة تتعلق ببيانات معالجة إلكترونياً، دون النظر إلى الوسيلة التي تتحقق بها الجريمة.

ويثار تساؤل حول هل الضرر عنصر من عناصر الركن المادي في تلك الجريمة؟

لم يشر المشرع إلى تحقق عنصر الضرر في الجريمة لقيامها، فيكفي وقوع عناصر السلوك الإجرامي لتحققها، بصرف النظر عن وقوع ضرر على المجني عليه من عدمه، بل أن المشرع جعل من قصد الإضرار بالشخص المعني بالبيانات دون حدوث ضرر ظرفاً مشدداً للعقاب في تلك الجريمة، إذ إن تلك الجريمة في صورتها البسيطة معاقب عليها بعقوبة الغرامة في حين إذا توافر قصد تعريض الشخص المعني بالبيانات للخطر أو الضرر تشدد العقوبة إلى الحبس الذي لا يقل عن ستة أشهر وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين.

ومن ناحية أخرى هل يشترط لكي تقوم الجريمة أن يحقق الجاني منفعة من قيامة بجمع أو معالجة أو إفشاء أو إتاحة أو تداول بيانات شخصية معالجة إلكترونياً؟

تأتي الإجابة على هذا التساؤل من خلال استقراء النص العقابي بالمادة (٣٦) من قانون حماية البيانات الشخصية المصري، والذي ميز بين حالتين **أولاهما:** القيام بالأفعال الإجرامية التي عددها النص العقابي دون الحصول على منفعة، وفي تلك الحالة تقوم الجريمة في صورتها البسيطة ويعاقب عليها بالغرامة.

ثانيهما: أن يكون الجاني قد حصل على منفعة مادية أو أدبية مقابل ارتكب الجريمة، في تلك الحالة شدد المشرع العقاب على ارتكاب تلك الجريمة، باعتبارها صورة مشددة حيث أدرج عقوبة الحبس بما لا يقل عن (ستة أشهر) ضمن عقوبة الجريمة، وضاعف عقوبة الغرامة في حديها الأدنى والأقصى.

---

[١٠٠] المادة الأولى من قانون مكافحة جرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨، والمنشور بالجريدة الرسمية– العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.

[١٠١] ذات المصدر السابق.

وحسناً ما فعله المشرع المصري بتشديد العقاب حال تلقي الجاني (منفعة) لارتكاب الجريمة، ويحمد له مساواته بين أن تكون المنفعة مادية أو أدبية؛ وذلك كون الجاني قد حقق المنفعة بصرف النظر عن طبيعتها، فقد تكون المنفعة أدبية لكنها تفوق فائدتها المنفعة المادية.

٤- النتيجة الإجرامية:

يكفي لاستحقاق الجاني العقاب مقارفته لفعل أو أكثر من الأفعال المكونة لعناصر الركن المادي لتلك الجريمة' بصرف النظر عن حدوث نتيجة لهذا الفعل من عدمه، فالمشرع المصري لم يتطلب للعقاب على تلك الجريمة حدوث نتيجة بعينها، بل يكفي للعقاب عليها إتيان الجاني فعل أو أكثر معاقباً عليه وفقاً للنص التجريمي، ويتحقق السلوك المادي في الجريمة بجمع أو معالجة أو إفشاء أو إتاحة أو تداول بيانات شخصية معالجة إلكترونيًا، بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا، أو بدون موافقة الشخص المعني بالبيانات، وتحقق النتيجة من عدمه برغم عدم أهميته كون الجريمة تقوم بمجرد إتيان أحد الأفعال المكونة للركن المادي للجريمة، هي مسألة موضوعية منوطة بمحكمة الموضوع في ضوء الوقائع والظروف المطروحة أمامها، وهي لا تؤثر على استحقاق الجاني العقاب، وإن كانت من الممكن أن تؤثر على مقدر العقوبة.

٥- علاقة السببية:

يتطلب القانون توافر علاقة سببية بين سلوك الجاني ووقوع النتيجة الإجرامية، فالسببية حلقة الاتصال بين السلوك الإجرامي والنتيجة الإجرامية، ويكمن دورها في بيان ما كان للفعل من نصيب في إحداث النتيجة[١٠٢]، فعلاقة السبية لا وجود لها إلا في الجرائم ذات النتيجة، والواقع أن الضرر في تلك الجريمة مفترض دون الحاجة إلى تحقق نتيجة وبالتالي فليس هناك حاجة لبحث علاقة السببية في تلك الجريمة.

---

[١٠٢] د محمود نجيب حسني، علاقة السببية في قانون العقوبات، طبعة نادي القضاة، ١٩٨٤، بدون رقم طبعة، ص٣.

(ISSN: 2537- 0758)

٦- الركن المعنوي:

يجب أن تتعاصر ماديات الجريمة مع إرادة إجرامية تبعث هذه الماديات إلى الوجود. ويعبر عن هذه الإرادة الإجرامية بالركن المعنوي[١٠٣]، ويقوم الركن المعنوي على القصد الجنائي بعنصريه العلم والإرادة، فيجب أن يكون الجاني عالماً بأن من شأن سلوكه المادي إحداث النتيجة الإجرامية، وهو مستفاد من طبيعة الأفعال التي تقوم بها الجريمة.

(أ) العلم:

ويراد به علم الجاني بالصفة الاسمية أو الشخصية للبيانات، وأن يعلم أن من طبيعة الحاسوب الإلكترونية إجراء المعالجة الإلكترونية لهذه البيانات دون ترخيص من الجهة المختصة بذلك، وينبغي على الجاني في تلك الجريمة وهو لا يخرج عن كونه حائزاً، أو متحكماً، أو معالجاً بأن يعلم أن من شأن فعله المتمثل في (الجمع، أو المعالجة، أو الإفشاء، أو الإتاحة، أو التداول لبيانات شخصية معالجة إلكترونيًا) بأي وسيلة كانت يشكل اعتداءً على البيانات الشخصية للمجني عليه، وأنه غير مصرح له قانوناً إتيان أي من الأفعال التي تشكل السلوك الإجرامي للجريمة، وأنه لا توجد موافقة للمعني بالبيانات الشخصية على تلك المعالجة، ولمحكمة الموضوع تقدير توافر القصد الجنائي في الجريمة من عدمه وفقاً للوقائع المعروضة عليها كونها مسألة موضوعية تختص بها دون معقب عليها من محكمة النقض؛ لأن في مجال تقدير القصد الجنائي فإن محكمة الموضوع لا تعزل نفسها عن الواقعة محل الاتهام التي قام عليها الدليل قاطعاً، لكنها تجيل بصرها فيها، منقبة من خلال عناصرها عما قصد إليه الجاني حقيقة من وراء ارتكابها[١٠٤].

(ب)الإرادة:

يجب أن تتجه إرادة الجاني إلى إجراء المعالجة الإلكترونية لهذه البيانات بأية صورة كانت أي بالمخالفة للمقرر قانوناً بشأن المعالجة الإلكترونية للبيانات[١٠٥]، وينبغي أن

---

[١٠٣] د. أحمد فتحي سرور، الوسيط في قانون العقوبات– القسم العام، الطبعة السادسة، طبعة خاصة لنادي القضاة، ٢٠١٥، ص٦٤١.

[١٠٤] الدعوى رقم ١٧٣لسنة ٣١ دستورية، جلسة ٢٠١٧/١٢/٢، الموسوعة الذهبية للقضاء الدستوري المصري، ١٩٦٩– ٢٠١٩، المجلد الأول، المحكمة الدستورية العليا، القاهرة، ص٢٣١.

[١٠٥] د. محمد عبد اللطيف عبد العال الجرائم المادية وطبيعة المسؤولية الناشئة عنها– دار النهضة العربية– القاهرة– ١٩٩٧ ص ١٢٠

تتجه إرادة الجاني إلى ارتكاب فعل الاعتداء على البيانات الشخصية المعالجة إلكترونياً، بصرف النظر عن وجود قصد خاص فيما يتعلق بالصورة البسيطة لتلك الجريمة، أما فيما يتعلق بالصورة المشددة لتلك الجريمة فينبغي وجود قصداً خاصاً لدى الجاني، يتمثل في تعريض المجني عليه للخطر أو الضرر، حتى وإن لم يتحقق الخطر أو الضرر فيكفي القصد في ذلك لتشديد العقاب.

ويتصور أن يقع الفعل عمداً أو خطأ أو إهمالاً من الجاني وقد قضت محكمة النقض الفرنسية بأن الفعل الذي يتحقق من خلال الإهمال، في إجراء أو المضي قدمًا في معالجة البيانات الشخصية دون الامتثال للإجراءات المنصوص عليها قانوناً معاقب عليه قانونًا(١٠٦).

٧- العقوبة:

قرر المشرع المصري لدى نصه على عقوبة تلك الجريمة، عقوبتان مختلفتان إحداهما الغرامة فقط، والأخرى الحبس أو الغرامة **وذلك على النحو التالي:**

(أ) عقوبة الصورة البسيطة للجريمة:

عاقب المشرع المصري على الجريمة في صورتها البسيطة بالغرامة حدها الأدنى مائة ألف جنيه وحدها الأقصى مليون جنيه، ويقصد بالصورة البسيطة هنا هي ارتكاب الحائز، أو المتحكم، أو المعالج أحد صور السلوك التي يتصور أن تقع بها الجريمة، دون حصوله على أي فائدة مالية أو غير مالية لذلك الفعل، وكذلك انتفاء وجود نية خاصة لدى الجاني وهي قصد تعريض الشخص المعني بالبيانات للخطر أو الضرر.

وجاء في المادة ٢٢٦-٢٢ من قانون العقوبات الفرنسي بأنه يعاقب على المعالجة غير المشروعة للبيانات الشخصية، يعاقب بالسجن لمدة خمس سنوات السجن مدة لا تزيد على خمس سنوات وغرامة قدرها ٣٠٠٠٠٠ ثلاثمائة ألف يورو. ويجوز للقاضي بالإضافة لتلك العقوبة أن يحكم بمحو تلك البيانات محل الجريمة وتراقب الجنة القومية للمعلوماتية والحريات الفرنسية هذا المحو لتلك البيانات(١٠٧).

---

(106) Cour de cassation, criminelle, Chambre criminelle, 23 mai 2018, 16-84.096, In edit.

(١٠٧) وقد تم إنشاء هذه اللجنة بمقتضى القانون رقم ١٧ لسنة ١٩٧٨ لتلعب الدور المحوري في حماية حقوق وحريات الأفراد. ولها بالتالي دور رئيسي في حماية البيانات الشخصية، حيث أعطاها المشرع الفرنسي سلطات كبيرة في هذا الشأن، فلها إصدار تعليمات ومعايير متعلقة بمعالجة البيانات الشخصية، وعلى من يقوم بمعالجة البيانات احترام هذه التعليمات والمعايير وإلا ترتب على

(ISSN: 2537- 0758)

(ب)عقوبة الصورة المشددة للجريمة:

شدد المشرع المصري العقاب على تلك الجريمة إذا ارتكبت مقابل الحصول على منفعة مادية أو أدبية، وقد تتمثل الفائدة المادية في مقابل مالي، وحتى إن كانت الفائدة أدبية فتشدد العقوبة بناءً على حصول الجاني على تلك المنفعة، وفي تلك الحالة تقوم فرضية مفادها إذا كان مرتكب الجريمة موظفاً عاماً أو من في حكمه، نكون إزاء سلوك مادي تتعدد أوصافه القانونية، فيعد في ذات الوقت منطوياً على جريمة (الرشوة) وفي تلك الحالة يتعين تطبيق عقوبة جريمة الرشوة باعتبارها العقوبة الأشد[١٠٨]، والحالة الثانية التي شدد فيها العقاب في تلك الجريمة تتعلق بالقصد الجنائي للجريمة، وهي أن ترتكب بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر، إذ لابد من وجود نية خاصة لدى الجاني، تتمثل في قصد تعريض المعني بالبيانات الشخصية للخطر أو الضرر، وفي تلك الحالة تكون العقوبة الحبس الذي لا يقل حده الأدنى عن ستة أشهر وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه أو احدى هاتين العقوبتين، وحيث لم يبين النص الحد الأقصى للحبس فيتعين الرجوع للقواعد العامة التي تقضي بأن حده الأقصى ثلاث سنوات[١٠٩]، وبالتالي تكون عقوبة الجريمة فيما يتعلق بالحبس من ستة أشهر ويصل حدها الأقصى لثلاث سنوات.

ذلك عقابه. د سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، العدد ٩مارس ٢٠١٥، مجلد ٣، ص٤١٤.

[١٠٨] حيث نصت المادة (١٠٤) من قانون العقوبات المصري بأن كل موظف عام طلب لنفسه أو لغيره أو قبل أو أخذ وعداً أو عطية للامتناع عن عمل من أعمال وظيفته أو للإخلال بواجباتها أو لمكافأته على ما وقع منه من ذلك يعاقب بالسجن المؤبد....) وإعمالاً لنص الفقرة الأولى من المادة (٣٢) من قانون العقوبات المصري والتي جاء فيها (إذا كون الفعل الواحد جرائم متعددة وجب اعتبار الجريمة التي عقوبتها أشد والحكم بعقوبتها دون غيرها).

[١٠٩] جاء في المادة (١٧) من قانون العقوبات المصري والتي جاء فيها بأن (عقوبة الحبس هي وضع المحكوم عليه في أحد السجون المركزية أو العمومية المدة المحكوم بها عليه لا يجوز أن تنقص هذه المدة عن أربع وعشرين ساعة ولا أن تزيد على ثلاث سنوات إلا في الخصوصية المنصوص عليها قانونا.....).

المطلب الثاني
المعالجة غير المشروعة للبيانات الشخصية الحساسة

حظيت البيانات الشخصية الحساسة للأفراد بحماية متميزة عن سواها من البيانات الشخصية الأخرى، وتنبع تلك الحماية من أهميتها في حياة عموم البشر، وقد حظر المشرع الفرنسي في المادة السادسة من قانون معالجة البيانات والملفات والحريات جمع أو معالجة البيانات الشخصية التي تكشف بشكل مباشر أو غير مباشر، عن الأصول العرقية أو الإثنية، أو الآراء السياسية أو الفلسفية، أو الدينية أو العضوية النقابية للأشخاص، أو التي تتعلق بصحتهم أو حياتهم الجنسية[١١٠].

وعُرفت البيانات الحساسة أيضاً بالبيانات ذات الطبيعة الخاصة، فجاء في المادة(١٦) من القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية القطري[١١١] بأنه "تعد من البيانات الشخصية ذات الطبيعة الخاصة: البيانات المتعلقة بالأصل العرقي، والأطفال، والصحة 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".

وقصد بها المنظم السعودي كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو أصله القبلي، أو معتقده الديني أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية. وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الائتمانية، أو البيانات الصحية، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما[١١٢] .

---

[110] Modifié par Ordonnance n°2018-1125 du 12 décembre 2018- art. 1.

[١١١] المنشور بالجريدة الرسمية العدد ١٥بتاريخ ٢٠١٦/١٢/٢٩.

[١١٢] المادة الأولى من نظم حماية البيانات الشخصية السعودي.

(ISSN: 2537- 0758)

وعرفها المشرع المصري بأنها البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيو مترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة[١١٣]، وعلى الرغم من أن تعريف المشرع المصري للبيانات الحساسة فإنه قد أعطى عديد من الأمثلة لتلك البيانات إلا أنه يؤخذ عليه بأنه لم يبين تعريف لبعض تلك البيانات التي أوردها المشرع المصري كأمثلة (كالبيانات البيومترية، البيانات المالية وغيرها من البيانات عددها المشرع المصري في مصف البيانات الحساسة) ولذلك يتعين على المشرع المصري إدراج تعريف تلك البيانات الحساسة داخل القانون.

وتتميز البيانات الحساسة للأفراد بطبيعتها الخاصة التي تجعل الشخص يحرص على عدم كشفها لأحد لما لها من طبيعة خاصة، وِاَنعَكَس هذا التمييز بدوره على المشرع بتشديده العقاب حال الاعتداء على تلك البيانات، حيث إدراج عقوبة الحبس الذي لا تقل مدته عن ثلاثة أشهر بالإضافة للغرامة، وللقاضي أن يقضي بهما معاً أو بأحدهما، في حين أن نص على عقوبة الغرامة دون الحبس، فيما يتعلق بالمعالجة غير المشروعة للبيانات الشخصية العادية، طالما لم يكن ذلك بمقابل الحصول على منفعة أو صاحبته نية خاصة للأضرار بالمعني بالبيانات أو تعريضه للخطر.

أولاً- نص التجريم:

نصت المادة (٤١) من قانون حماية البيانات الشخصية المصري" يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل حائز أو متحكم أو معالج جمع أو أتاح أو تداول أو عالج أو أفشي أو خزن أو نقل أو حفظ بيانات شخصية حساسة بدون موافقة الشخص المعني بالبيانات أو في غير الأحوال المصرح بها قانونًا".

أما بالنسبة لموقف المشرع الفرنسي فالقاعدة العامة هي حظر معالجة البيانات الشخصية التي تتعلق بالبيانات الحساسة، وعددت المادة (٤٤) من قانون معالجة البيانات والملفات والحريات الفرنسي مجموعة من الحالات تعد استثناء من حظر معالجة البيانات الحساسة الواردة في المادة السادسة من هذا القانون، وتشمل استيفاء أحد الشروط المنصوص عليها في المادة ٢/٩ من اللائحة (الاتحاد الأوروبي) ٢٠١٦/٦٧٩

[١١٣] المادة الأولى من قانون حماية البيانات الشخصية المصري.

الصادرة في ٢٧ أبريل ٢٠١٦[١١٤]، وتشمل العلاجات اللازمة لأغراض الطب الوقائي أو التشخيص الطبي، أو إدارة الرعاية أو العلاج أو إدارة الخدمات الصحية، والتي يقوم

[١١٤] وتتلخص هذه الشروط في إعطاء صاحب البيانات موافقة صريحة على معالجة هذه البيانات الشخصية لغرض محدد واحد أو أكثر، وتكون المعالجة ضرورية لأغراض تنفيذ الالتزامات وممارسة الحقوق الخاصة للمراقب أو للمادة الخاضعة في قانون العمل، والضمان الاجتماعي، والحماية الاجتماعية، بقدر ما يسمح به الاتحاد أو قانون الدولة العضو أو اتفاق جماعي وفقًا لقانون الدول الأعضاء، ينص على ضمانات مناسبة للحقوق الأساسية ومصالح صاحب البيانات، وتكون المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر حيث يكون صاحب البيانات غير قادر جسدياً أو قانونياً على منح الموافقة، وتتم المعالجة في سياق أنشطتها المشروعة بضمانات مناسبة، من قبل مؤسسة أو جمعية أو أي هيئة أخرى غير هادفة للربح، ذات هدف سياسي أو فلسفي أو ديني أو نقابي بشرط أن تكون المعالجة فقط للأعضاء أو لأعضاء سابقين في الهيئة أو للأشخاص الذين لديهم اتصال منتظم به فيما يتعلق بأغراضها، وأن البيانات الشخصية لا يتم الكشف عنها خارج تلك الهيئة دون موافقة أصحاب البيانات، وتتعلق المعالجة بالبيانات الشخصية التي يتم نشرها بشكل علني من قبل صاحب البيانات، لضرورة إقامة الدعاوى القانونية أو ممارستها أو الدفاع عنها أو عندما تكون المحاكم تعمل بصفتها القضائية، وأن المعالجة ضرورية لأسباب تتعلق بمصلحة عامة كبيرة، على أساس قانون الاتحاد أو الدول الأعضاء الذي يتناسب مع الهدف المنشود وتحترم جوهر الحق في حماية البيانات وتوفر تدابير مناسبة ومحددة لحماية الحقوق الأساسية ومصالح صاحب البيانات، أن تكون المعالجة ضرورية لأغراض الطب الوقائي أو المهني، لتقييم القدرة على العمل للموظف والتشخيص الطبي، وتوفير الرعاية الصحية أو الرعاية الاجتماعية أو العلاج أو إدارة نظم وخدمات الرعاية الصحية أو الاجتماعية على أساس قانون الاتحاد أو الدول الأعضاء أو بموجب عقد مع أخصائي صحي وخاضعة للشروط والضمانات المشار إليها في الفقرة ٣، أن تكون المعالجة ضرورية لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة، مثل الحماية من التهديدات الخطيرة عبر الحدود للصحة أو ضمان مستويات عالية من جودة وسلامة الرعاية الصحية والمنتجات الطبية أو الأجهزة الطبية، على أسس الاتحاد أو قانون الدول الأعضاء الذي ينص على تدابير مناسبة ومحددة لحماية حقوق وحريات صاحب البيانات، ولا سيما السرية المهنية، أن تكون المعالجة ضرورية لأغراض الأرشفة في المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية وفقا للمادة ٨٩ (١) استناداً إلى قانون الاتحاد أو الدول الأعضاء الذي يتناسب مع

(ISSN: 2537- 0758)

بها عضو في مهنة صحية أو شخص آخر يفرض عليه الالتزام بسبب واجباته، والمعالجة الإحصائية التي يقوم بها المعهد الوطني للإحصاء والدراسات الاقتصادية أو إحدى الخدمات الإحصائية الوزارية، وعمليات المعالجة التي تنطوي على بيانات تتعلق بالصحة تبررها المصلحة العامة، ووفقا لأحكام المعالجة وفقا للوائح النموذجية المذكورة في (ج) من ٢ ° ا من المادة (٨) التي ينفذها أصحاب العمل أو الإدارات والتي تتعلق بالبيانات البيومترية الضرورية للغاية للتحكم في الوصول إلى أماكن العمل، وكذلك الأجهزة والتطبيقات المستخدمة في سياق المهام الموكلة إلى الموظفين، الوكلاء أو المتدربين أو المقاولين، بالإضافة إلى المعالجة المتعلقة بإعادة استخدام المعلومات العامة الواردة في القرارات المذكورة في المادة L. 10 من قانون القضاء الإداري والمادة L. 111-13 من قانون التنظيم القضائي، شريطة ألا يكون لهذه المعالجة غرض أو تأثير السماح بإعادة تحديد هوية الأشخاص المعنيين، وأخيراً المعالجة اللازمة للبحث العام بالمعنى المقصود في المادة L. 112-1 من قانون البحث، شريطة أن تكون أسباب المصلحة العامة هامة ضرورية بموجب الشروط المنصوص عليها في G من ٢ من المادة (٩) من اللائحة (الاتحاد الأوروبي) ٢٠١٦/٦٧٩ الصادرة في ٢٧ أبريل ٢٠١٦، بعد رأي مسبب ومنشور من اللجنة الوطنية للمعلوماتية والحريات المقدمة وفقا للإجراءات المنصوص عليها في المادة (٣٤) من هذا القانون[١١٥]. وقد استثنت كذلك عمليات المعالجة للبيانات الحساسة لفائدة الأمن القومي، والمتعلق ببيانات شخصية يكون الحصول عليها ومعالجتها يرتبطان بالمصالح العليا للبلاد، وكذلك تلك البيانات التي تم الحصول عليها أو تمت معالجتها لأغراض الوقاية من الجريمة أو بمناسبة متابعة مرتكبي الجريمة والتحقيق فيها، والبيانات القضائية المتعلقة بالجرائم والعقوبات وتدابير الأمن الواردة في قواعد البيانات القضائية.

ثانيًا- علة التجريم:

تكمن العلة التجريمية في الأهمية الكبيرة التي تشكلها تلك البيانات لصاحبها بحكم طبيعتها، حيث تعتبر هذه البيانات وثيقة الصلة بأشخاصهم، ويمكن أن تكشف عن

الهدف المنشود ويحترم جوهر الحق في حماية البيانات وتوفير تدابير مناسبة ومحددة لحماية الحقوق الأساسية ومصالح صاحب البيانات.

(115) Article44 Modifié par Ordonnance n°2018-1125 du 12 décembre 2018-art.1.

هويتهم وطبيعة ونمط حياتهم بسهولة ويسر كبيرين، مما قد يفضي إلى تهديد سلامتهم في حالة تم الاعتداء على تلك البيانات.

ثالثاً- محل الجريمة:

محل تلك الجريمة هي بيانات شخصية (حساسة) معالجة إلكترونياً، وباستقراء تعريف المشرع المصري وعدد من التشريعات المقارنة للبيانات الشخصية الحساسة يتضح أنها تدور حول بيانات تتعلق بالناحية الصحية والمالية، وبيانات متعلقة بالمعتقدات الدينية والسياسية والحالة الأمنية، وفي كل الأحوال تكون بيانات الأطفال من البيانات الحساسة، ووفقاً للمادة الثانية من قانون الطفل المصري[١١٦] فإنه يعد طفلاً كل من لم يتجاوز الثمانية عشرة سنة ميلادية. **وفيما يلي بيان ذلك من خلال:**

١- البيانات الصحية:

تتعلق البيانات الصحية بجميع البيانات الطبية الخاصة بوصف حالة المريض وظروفه وعلاجاته ومسار الشفاء وغير ذلك مما يتعلق بمسيرة المرض والمريض، وعرف المنظم السعودي البيانات الصحية بأنها: كل بيان شخصي يتعلق بحالة الفرد الصحية، سواء الجسدية أو العقلية أو النفسية أو المتعلقة بالخدمات الصحية الخاصة به[١١٧]، وقد ميز المنظم السعودي بين البيانات الصحية والخدمات الصحية التي تعني الخدمات المتعلقة بصحة الفرد، ومن ذلك الخدمات الوقائية والعلاجية والتأهيلية والتنويم وتوفير الدواء.

وقد استثني القانون الفرنسي في قانون معالجة البيانات ١٩٧٨/١٧ بعض أشكال معالجة البيانات المتعلقة بالصحة من مجال التطبيق، ويتعلق الأمر بالبيانات الشخصية التي يكون الغرض منها: المتابعة العلاجية أو الطبية الفردية للمرضى، السماح بإجراء دراسات انطلاقاً من البيانات التي تم جمعها بغرض المتابعة العلاجية أو الطبية الفردية للمرضى، التعويض أو الرقابة من قبل الهيئات المكلفة بالتأمين على المرضى، وكذلك

---

[١١٦] قانون الطفل المصري رقم ١٢لسنة١٩٩٦، والمعدل بالقانون رقم ١٢٦ لسنة ٢٠٠٨ والمنشور بالجريدة– العدد ٢٤(مكرر) في ١٥ يونيه سنة ٢٠٠٨.

[١١٧] المادة الأولى من نظام حماية البيانات الشخصية السعودي.

(ISSN: 2537- 0758)

استثناء المعالجات التي تتم داخل مؤسسات الصحة من قبل الأطباء المسؤولين عن المعلومة الطبية[١١٨].

ومما لا شك فيه أن هذه البيانات التي تتعلق بالشخص المريض والمعلومات التي تجمع عنه بمناسبة مرضه، ستجعله في حالة مكشوفة أمام الآخرين خصوصاً أمام شركات التامين، وهو ما سيجعل الأطباء يترددون في تقديم رعاية طبية أفضل لحساسية المعلومات التي يريدون اطلاع الغير عليها، كما أبدى التحفظ ذاته بالخشية من تأثير نشر أسماء الأشخاص الذين كانت لهم سوابق صحية ذات سمعة غير طيبة كالإدمان على المواد المخدرة مثلاً، وهو ما يشكل الإساءة إليهم دون أن يكون مثل هذا الأمر مستقراً ومستمراً في مسلكهم الحياتي، إذ إن مثل هذه المعلومات الضارة لم تعد واقعية أو صادقة[١١٩]، وتطبيقاً لذلك عاقبت المحكمة الأوروبية لحقوق الإنسان حكومة فنلندا لفشلها في حماية بيانات المريض الطبية، التي تحتفظ بها أحد المستشفيات ضد مخاطر الوصول غير المشروع للبيانات، وربط الحكم الصادر بين الحق في الخصوصية بموجب قانون حقوق الإنسان وحماية المعلومات الشخصية، ورأت المحكمة أن المادة تشمل واجبًا إيجابياً بضمان أمن البيانات الشخصية، فنظام حفظ الملفات في المستشفى يخالف القانون الفنلندي الذي يتطلب من المستشفيات تأمين البيانات الشخصية من الوصول لغير المصرح لهم، فقد اشتبهت مقدمة البلاغ، وتعمل ممرضة في مستشفى، وكانت تعالج ضد فيروس (ضعف المناعة المكتسب– الإيدز) في أن زملاءها في العمل قد اكتشفوا أنها مصابة بالفيروس، 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، فقد رأت المحكمة أن حقيقة كون نظام السجلات الطبية في المستشفى غير

---

[١١٨] أ/ ليديا رشام، الحماية الجنائية للمعطيات الشخصية دراسة مقارنة، رسالة لنيل شهادة الماجستير، جامعة البويرة، الجزائر، ٢٠١٩، ص٣١.

[١١٩] محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة استخدام الحاسب الآلي دراسة تحليلية مقارنة للحق في الخصوصية وتطبيقاته في القانون الكويتي، مطبوعات جامعة الكويت، بدون رقم طبعة وتاريخ نشر، ص٨٨.

أمن كانت كافية لجعلها مسئولة عن الكشف غير المبرر عن البيانات الطبية الخاصة بالممرضة[١٢٠].

ويجدر التنويه بأن من شأن إفشاء البيانات الصحية لأحد المرضي فيه تعدد للجرائم إذا كان الجاني من العاملين بالقطاع الطبي كالطبيب أو ممرض فإنه يكون بذلك مسؤولاً عن إفشاؤه لأسرار مهنية.

٢- البيانات المالية:

يقصد بالبيانات المالية: مجموع ما للشخص وما عليه من حقوق والتزامات مالية[١٢١]، وتحتوي هذه البيانات على دخل الفرد الشهري، والاتفاقات التي أجراها، والديون التي في ذمته، ووضعه وسمعته المالية لدى البنوك وشركات التأمين، أو وضعه وسمعته لدى السوق التجاري والمحلي، ولدى غرفة التجارة والصناعة، وسمعته التجارية في الخارج، وكل ذلك يدخل في مجال الذمة المالية العائدة إلى الشخص وهي بدورها ترتكز على الرصيد الشخصي المالي والتزاماتها[١٢٢].

وتعد أكثر البيانات عرضة للإفشاء غير المشروع هي الخاصة بتعاملات البنوك الإلكترونية، وهذا ما ثبت من خلال قضية بنك جزل تشافت السويسري التي حاول خلالها عملاء فرنسيين تابعين لإدارة خدمات الرقابة على التعاملات التجارية والمالية، فك شفرة بيانات شخصية لمواطنين فرنسيين تحمل حسابات لدى البنك، وذلك للاستعانة بها في أعمال البحث والتقصي التي تجري بشأن التهرب الضريبي[١٢٣].

وقد ولضمان حماية البيانات المالية في المملكة العربية السعودية فقد تضمن البند سادساً من نظام حماية البيانات الشخصية السعودي بأن يُنسق بين الجهة المختصة (وهي الجهة التي يصدر بتحديدها قرار من مجلس الوزراء) والبنك المركزي السعودي،

---

[١٢٠] ريموند واكس، الخصوصية مقدمة قصيرة جدا، ترجمة ياسر حسن، الناشر مؤسسة هنداوي، ٢٠١٣، ص١٢٤.

[١٢١] د. حسن كيرة، المدخل إلى القانون، القسم الثاني- النظرية العامة للحق، مكتبة مكاوي، ١٩٧٧، ص٦٢٨.

[١٢٢] محمد عبد المحسن المقاطع، مرجع سابق، ص٧٩.

[١٢٣] د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢، ص١٩٥.

(ISSN: 2537- 0758)

لإعداد **مذكرة** تفاهم لتنظيم بعض الجوانب المرتبطة بتطبيق أحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية في الجهات الخاضعة لإشراف البنك المركزي السعودي تنظيميًّا، وتحديد دور كل منهما في هذا الشأن، وذلك مراعاةً لعدم تداخل الاختصاصات بينهما في شأن تطبيق أحكام النظام ولوائحه التنفيذية على الجهات الخاضعة لإشراف البنك المركزي السعودي تنظيميًّا، وللحيلولة دون التأثير في استقلالية البنك المركزي السعودي، وللطبيعة الخاصة للتعاملات المالية والمصرفية، ولأجل تعزيز استقرار ونمو القطاعات التي يشرف عليها البنك المركزي السعودي، على أن يستكمل إعداد المذكرة وتوقيعها بالتزامن مع نفاذ النظام.

وعلى الصعيد القضائي فقد حرص القضاء في مصر على كفالة سرية البيانات المالية للأشخاص ومن بينهم عملاء البنوك، فقد قضت محكمة النقض المصرية بأن 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 يخل 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 الذي يوجب نقضه والإعادة في خصوص الدعوى المدنية"[١٢٤].

[١٢٤] نقض جنائي مصري، مجموعة أحكام محكمة النقض، الطعن رقم ٥٥١٥ لسنة ٦٦، جلسة ١٤ أبريل ٢٠٠٣، س ٥٤، ق ٦٥، ص ٥٤٠.

٣- البيانات الدينية والآراء السياسة والنقابية:

يعود السبب من منع معالجة البيانات المتعلقة بالأصل الديني إلى الماضي الأليم الذي عرفته الإنسانية في القرون الأخيرة، من تعصب وتمييز على أساس الدين، والتي مازالت آثاره قائمة إلى وقتنا هذا؛ وبالتالي لمكافحة هذا التمييز أو أي تحامل أخر يمكن أن يستند إلى اعتبارات دينية، أجمعت التشريعات المقارنة على حظر معالجة البيانات الشخصية المبنية الأصل الديني[١٢٥]، وفي تصوري أن المشرع المصري فيما يتعلق بحظر معالجة البيانات الشخصية المتعلقة بالدين، جاء مردداً للعديد من النظم الغربية المقارنة وعلى وجه التحديد الفرنسي، حيث إن الهوية الدينية للأفراد في المجتمع المصري مثبته بموجب البطاقة الشخصية، وبالتالي فلا جدوي من إدراجها ضمن البيانات الشخصية الحساسة كونها معروفة ومعلومة للجميع ومثبته ضمن الوثائق الرسمية للأفراد.

وفيما يتعلق بالآراء السياسة والنقابية فقد اعتبرت اللجنة الوطنية للمعلوماتية والحريات الفرنسية بأن البيانات المتعلقة بالآراء السياسية والفلسفية أو النقابية، كذلك المعتقدات الدينية هى من قبيل البيانات الشخصية، وبالتالي يتعين الحصول علي موافقة خطية من الأشخاص المعنيين للقيام بمعالجتها[١٢٦].

٤- البيانات الشخصية المتعلقة بالأصل الاثني والعرقي:

يقصد بالأصل العرقي للشخص الانتساب إلى جماعة من الجماعات الإنسانية، وفق تصنيف يعتمد على القوميات، أو السلالات المختلفة للبشر[١٢٧]، ويرجع سبب حظر معالجة البيانات الشخصية للأفراد المتعلقة بالأصل الاثني والعرقي شأنها في ذلك شأن الحظر بمعالجة الأصل الديني؛ لما شهدته البشرية من صراعات داميه بين الناس بسبب اختلاف الأصل الاثني أو العرقي؛ لذلك نأى المشرع المصري والعديد من النظم القانونية

---

(125) Ibrahim COULIBALY, La protection des données à caractère personnel dans le domaine de la recherche scientifique thèse pour obtenir le grade de docteur, spécialité: droit prive. Université de Grenoble, 25 novembre 2011, p 371.

(126) V. CNIL, Délibération n° 85-050 du 22 oct. 1985 portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, JO 17 nov 1985. sans page.

(١٢٧) د. ايمن مصطفى احمد، الحماية القانونية للبيانات الشخصية في إطار أنشطة البحث العلمي، مجلة الدراسات القانونية تصدرها كلية حقوق أسيوط، العدد ٣٧ الجزء الأول، ٢٠١٥، ص٦١٧.

(ISSN: 2537- 0758)

المقارنة بأنفسهم عن فتح المجال لمعالجة تلك البيانات تلافياً لأي مشكلة قد تحدث مستقبلاً استناداً لتلك المعالجة.

رابعاً- أركان الجريمة:

عددت المادة (٤١) من قانون حماية البيانات الشخصية المصري مجموعة من الأفعال التي يقع بها الاعتداء على البيانات الشخصية الحساسة، وهي تتمثل في تلك الأفعال التي يقع بها الاعتداء على البيانات الشخصية العادية (كجمع، الإتاحة، التداول، أو المعالجة، أو الإفشاء) وقد تعرضت لبيانها مسبقاً في المطلب السابق، غير أن المشرع المصري شمل بعض الأفعال بالتجريم حال حدوثها آزاء بيانات شخصية حساسة وهي كالتخزين، النقل، والحفظ، وفي كل الأحوال لابد أن تتم تلك الأفعال دون موافقة صاحب البيانات، وفي غير الأحوال المصرح بها قانوناً.

ولا تثير عدم موافقة الشخص المعني على معالجة بياناته الشخصية أي إشكالية؛ إذ أن المشرع اشتراط فيما يتعلق بمعالجة البيانات الحساسة ضرورة أن تكون الموافقة صريحة، غير أن اللبس قد يثار فيما يتعلق بالمعالجة لتلك البيانات فى الأحوال المصرح بها قانوناً؛ حيث إن القراءة الأولية لقانون حماية البيانات الشخصية المصري تُشير إلى أن عبارة "الأحوال المصرح بها قانوناً وقد وردت في المواد أرقام ٢، ١/٤، ٥/٤، ٥/٥، ١٢، ٣٦، ٤١من القانون، وجميعها تفيد بمشروعية معالجة البيانات دون الحصول على موافقة الشخص المعني بالبيانات طالما كانت المعالجة في نطاق الأحوال المصرح بها قانوناً، وهناك رأي وأؤيده يتجه إلى اعتبار أن الأحوال المصرح بها قانونا هي: المذكورة في المادة السادسة من القانون حيث إن المشرع قدم هذه المادة بعبارة تعد المعالجة الإلكترونية مشروعة وقانونية في حال توافر أي من الحالات الآتية بما يفيد أنها حالات تدخل في نطاق تطبيق هذا القانون، وتعتبر فيها المعالجة مشروعة. على الرغم من وجود لبس وغموض حول طبيعة البنود المذكورة في المادة السادسة لتكون المعالجة مشروعة وقانونية، وما إذا كانت هذه البنود شروط يجب توافرها جميعاً أم حالات يكفي توافر واحدة منها على الأقل، وأميل إلى اعتبار أن هذه البنود" حالات مشروعة للمعالجة "كما هو الحال في لائحة الاتحاد الأوروبي، وتفصيل ذلك أن نص المادة السادسة من القانون يعتبر كما لو كان مترجماً من نص الفقرة الأولى من المادة السادسة من لائحة الاتحاد الأوروبي، والتي أشارت صراحة لحالات المعالجة المشروعة في هذه المادة

وتجعل الإحالة إليها في كل موضع يستلزم الإشارة إلى الحالات المشروعة للمعالجة[١٢٨].

أما فيما يخص الركن المعنوي فيتخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة أي يجب أن يعلم الجاني بأن الأفعال التي يقوم بها تشكل معالجة لبيانات ذات طابع شخصي، وأن البيانات التي يعمل على معالجتها تشكل بيانات حساسة، وأنه يجري المعالجة المذكورة دون الحصول على موافقة صريحة من الشخص المعني ودون أن يكون مصرح بها قانوناً، فضلا عن ذلك يستوجب القصد أن تكون للجاني إرادة للقيام بهذه الأفعال من أجل تحقيق نتيجتها[١٢٩].

خامساً-العقوبة:

قرر المشرع الفرنسي العقاب على تلك الجريمة بموجب المادة ٢٢٩-١٩من قانون العقوبات الفرنسي بالسجن مدة خمس سنوات بالإضافة للغرامة ٣٠٠٠٠٠ يورو وقد جرى نصها (باستثناء الحالات التي ينص عليها القانون، وضع أو تخزين البيانات الشخصية في التخزين المحوسب، دون موافقة صريحة من الطرف المعني، والتي تكشف، بشكل مباشر أو غير مباشر، عن الأصول العرقية أو الإثنية، أو الآراء السياسية أو الفلسفية أو الدينية، أو العضوية النقابية للأشخاص، أو التي تتعلق بصحتهم أو ميولهم الجنسية أو هويتهم الجنسية، يعاقب عليه بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠,٠٠٠ يورو)[١٣٠].

وعاقبت المادة (٤١) من قانون حماية البيانات الشخصية المصري على جريمة المعالجة غير المشروعة للبيانات الشخصية الحساسة بدون موافقة الشخص المعنى بالبيانات أو في غير الأحوال المصرح بها قانونًا، بالحبس مدة لا تقل عن ثلاثة شهور

---

[١٢٨] د. دعاء حامد محمد عبد الرحمن، الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي، قراءة في قانون حماية البيانات الشخصية رقم ١٥١لسنة٢٠٢٠، مقدم إلى المؤتمر العلمي الأول لكلية الحقوق جامعة مدينة السادات، المقام في الفترة من ٣٠-٣١ يوليو ٢٠٢٢، والمنشور بعدد خاص بالمؤتمر.

[١٢٩] د. سليم محمد سليم حسين، الحماية الجنائية للبيانات المعالجة آلياً دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق– جامعة عين شمس، العدد الأول يناير ٢٠٢٠، المجلد ٦٢، ص١٦٢.

[130] Modifié par Ordonnance n°2018-1125 du 12 décembre 2018- art. 13

(ISSN: 2537- 0758)

وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين.

ونصت المادة (٣٥) من نظام حماية البيانات الشخصية السعودي بأن (١- مع عدم الإخلال بأي عقوبة أشد منصوص عليها في نظام آخر، تكون عقوبة ارتكاب المخالفات الآتية وفقاً لما دون أمامها:

أ. كل من أفصح عن بيانات حساسة أو نشرها مخالفًا أحكام النظام يعاقب بالسجن مدة لا تزيد على (سنتين) وبغرامة لا تزيد على (ثلاثة ملايين ريال)، أو بإحدى هاتين العقوبتين؛ إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية.....) ويؤخذ على المنظم السعودي اشتراطه تطبيق العقوبة المقررة في المادة الخامسة والثلاثون في فقرتها الأولى، أن يكون الإفصاح عن البيانات الحساسة بقصد الإضرار بصاحب البيانات أو قصد تحقيق منفعة شخصية، وفي تقديري أنه لم تكن هناك حاجة لإضافة قصد الإضرار بصاحب البيانات، أو تحقيق منفعة، إذ يكفي أن يكون الفعل مجرداً لاستحقاق الجاني العقاب.

وجاء في المادة (٢٤) من قانون حماية خصوصية البيانات الشخصية القطري بأنه يعاقب على مخالفة الحظر المنصوص عليه في المادة (١٦/ فقرة ثالثة) بشأن معالجة البيانات الشخصية ذات الطبيعة الخاصة دون التصريح بذلك من الإدارة المختصة بغرامة تصل إلى (خمسة ملايين ريال)، وقد جاء النص مبيناً للحد الأقصى لعقوبة الغرامة دون بيان الحد الأدنى لها.

وفي تقديري بأن المشرع الفرنسي كان أكثر توفيقاً من المشرع المصري، والمنظم السعودي، والمشرع القطري، فيما يتعلق بتغليظ العقوبة على جريمة المعالجة غير المشروعة للبيانات الحساسة حيث قرر عقوبة السجن مضافاً إليها غرامة مالية كبيرة؛ ولعل هذا يعكس مدى حرص المشرع الفرنسي على حمايته للبيانات الشخصية للأفراد، وتكمن شدة هذه العقوبة في مقدارها وفي كونها ذات حد واحد، لا يُعمل فيها بالتفريد القانوني للعقوبة الذي يجعلها تتراوح بين حدين أدنى وأقصى.

وان كان يحسب للمشرع المصري تمييزه على نظيريه السعودي والقطري بإقراره عقوبة الحبس لمرتكبي تلك الجريمة ولم يقصرها على الغرامة المالية، وحتى إن كانت عقوبة الحبس تخييرية في القانون المصري فإن ذلك يسمح بتطبيقها، ويشكل رداعاً أكبر لكل من تسول له نفسه مقارفة هذا السلوك الإجرامي، وتوضح مدى حرص المشرع المصري على تحقيق أكبر قدر من الحماية الجنائية لتلك البيانات والمعنيين بها.

المطلب الثالث
الإخلال بشروط جمع البيانات ومعالجتها والاحتفاظ بها

قررت المادة الرابعة من قانون معالجة البيانات والملفات والحريات الفرنسي مجموعة من الضوابط اللازم مراعاتها لدى معالجة البيانات الشخصية وهي: أن تتم المعالجة بشكل قانوني وعادل، وأن تتسم بالشفافية فيما يتعلق بالشخص المعني، وجمعها لأغراض محددة وصريحة ومشروعة، وألا يتجاوز الجمع تلك الأغراض، وأن تكون كافية وذات صلة فيما يتعلق بالأغراض التي تتم المعالجة من أجلها، وأن تقتصر على ما هو ضروري، وينبغي لعمليات المعالجة أن تكون دقيقة وعند الضرورة وتبقى محدثة، ويجب اتخاذ جميع الخطوات المعقولة لضمان محو البيانات الشخصية غير الدقيقة، مع مراعاة الأغراض التي تتم المعالجة من أجلها أو تصحيحها دون تأخير، وأن يتم تخزينها في شكل يسمح بتحديد موضوعات البيانات لمدة لا تزيد عن اللازم، فيما يتعلق بالأغراض التي تتم معالجتها من أجلها، ومعالجتها بطريقة تضمن الأمان المناسب للبيانات الشخصية، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية والخسارة التدمير، أو التلف العرضي، أو الوصول من قبل أشخاص غير مصرح لهم، باتخاذ التدابير الفنية أو التنظيمية المناسبة[١٣١].

وجاء في المادة الثالثة من قانون حماية البيانات الشخصية المصري عدد من الشروط اللازمة لجمع ومعالجة والاحتفاظ بالبيانات الشخصية وهي كالتالي:

"يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية:

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...." ورتب عقاباً على مخالفة تلك الشروط سواء مجتمعة أو بشكل فردي، وذلك في المادة (٣٧) من ذات القانون.

ونصت المادة (٣٧) بأنه ".....ويعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في

(131) Modifié par Ordonnance n°2018-1125 du 12 décembre 2018- art. 1

(ISSN: 2537- 0758)

المادة (٣) من هذا القانون" وعلى ذلك فإن جريمة الإخلال بشروط جمع البيانات، ومعالجتها، والاحتفاظ بها، تشمل عدد من الصور الإجرامية بعضها متعلق بالإخلال شروط جمع البيانات، والأخرى تتعلق بالإخلال شروط الاحتفاظ بالبيانات، وأخيراً الإخلال الشروط المتعلقة بإجراءات المعالجة **وفيما يلي بيانها على النحو التالي:**

الفرع الأول

الإخلال بشروط جمع البيانات الشخصية

تضمنت المادة الحادية عشرة من نظام حماية البيانات الشخصية السعودي عدداً من الشروط اللازمة لجمع البيانات الشخصية وجرى نصها على النحو التالي "١- يجب أن يكون الغرض من جمع البيانات الشخصية ذا علاقة مباشرة بأغراض جهة التحكم، وألا يتعارض مع أي حكم مقرر نظاماً.

٢- يجب ألا تتعارض طرق جمع البيانات الشخصية ووسائلها مع أي حكم مقرر نظاماً، وأن تكون ملائمة لظروف صاحبها، ومباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل أو الابتزاز.

٣- يجب أن يكون محتوى البيانات الشخصية ملائماً ومقصوراً على الحد الأدنى اللازم لتحقيق الغرض من جمعها، مع تجنب شموله على ما يؤدي إلى معرفة صاحبها بصورة محددة متى تحقق جمعها. وتحدد اللوائح الضوابط اللازمة لذلك.

٤-إذا اتضح أن البيانات الشخصية التي تجمع لم تعد ضرورية لتحقيق الغرض من جمعها، فعلى جهة التحكم التوقف عن جمعها، وإتلاف ما سبق أن جمعته منها دون تأخير "[١٣٢].

وأَوْرَد المشرع المصري مجموعة من الشروط اللازم توافرها لدى جمع البيانات الشخصية، لا تخرج في مجملها عما جاء في قانون معالجة البيانات والملفات والحريات الفرنسي أو نظام حماية البيانات الشخصية السعودي **وفيما يلي بيان تلك الشروط:**

١- أن يتم جمع البيانات بطريقة مشروعة

يقصد بذلك أن تكون طريقة الحصول على البيانات الشخصية تتفق مع صحيح القانون، وألا يوجد فيها ثمة مخالفة له، وألا أضحت طريقة جمع المعلومة غير

---

[١٣٢] الفقرة الرابعة من المادة الحادية عشرة عدلت بموجب مرسوم ملكي رقم (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ، صحيفة أم القرى إصدار ١٤٤٤/٩/١٦هـ.

مشروعة، وبذلك يكون جمعها مخالفاً للشروط التي أوجبها القانون لجمع البيانات الشخصية.

وحتى تكون طريقة الجمع مشروعة، يجب أن يكون الجمع مُرخصا إما صراحة وإما ضمنيًا بجمعها، وألا يكون في ذلك الجمع تدخل صارخ في الحياة الخاصة، حسب ما تقتضيه الاتفاقيات الدولية لحقوق الإنسان، وتضمنت المادة (٢٥)[١٣٣] من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥لسنة ٢٠١٨ تجريم جمع البيانات الشخصية دون موافقة المعني بها، ولا يكفي لهذه المشروعية أن يُنفّذ المسؤول عن المعالجة التزاماته تجاه السلطة الوطنية بإجراءات التصريح والترخيص المسبقين، ولكن يجب عليه مراعاة التزاماته تجاه الشخص المعني، وذلك بتمكينه من حقه في إعلامه المسبق وموافقته المسبقة[١٣٤]. وقضت الغرفة الجنائية بمحكمة النقض الفرنسية أن جمع عناوين البريد الإلكتروني على الإنترنت يعتبر غير عادل وغير مشروع بسبب الطبيعة الغامضة تجاه أصحاب العناوين[١٣٥].

٢- أن يتم جمع البيانات لغاية محددة ومعلنة للمعني بها:

لعل من أبرز الأمور التي اشتراطها قانون حماية البيانات الشخصية المصري لدي جمع البيانات الشخصية هي تحديد الغاية والهدف من جمع تلك البيانات، فلابد من هدف واضح من جمع البيانات، فجمع البيانات الشخصية ليست هدفاً بذاته، وإنما لابد له من غاية يستهدفها، وفي حالة عدم وجود الغاية من جمع البيانات الشخصية يضحى السلوك مجرماً، ويستحق فاعله العقاب المنصوص عليه بالفقرة الثانية من المادة (٣٧)

---

[١٣٣] يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة أو ارسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة.

[134] Ives BISMUTH, Droit de l'informatique, éléments de droit à l'usage des informaticiens, édition L'harmattan, Paris, 2011, p201.

[135] Déloyauté du recueil d'adresses électroniques sur Internet par l'utilisation d'un logiciel– Cour de cassation, crimenelle. 14 mars 2006– AJ pénal 2006. p260

(ISSN: 2537- 0758)

من قانون حماية البيانات الشخصية المصري، وتحديد الغاية من جمع البيانات هو بمثابة تطبيق عملي لفكرة الشفافية عبر إبلاغ الشخص المعني بكل ما يحدث لبياناته.

وتضمنت المادة الثالثة من ذات القانون شرطاً غاية في الأهمية لدى جمع البيانات، وهو إبلاغ الشخص المعني بالبيانات محل الجمع، وهو من الأمور المهمة في مشروعية جمع البيانات وإعلام الشخص المعني بإجراء جمع لبياناته الشخصية، وطريقة جمعها والغرض منها وبيان أنواع البيانات التي تم جمعها(١٣٦).

وقد أكدت محكمة النقض الفرنسية على هذا المعنى في قضائها بأن القانون رقم ٧٨/١٧ المتعلق بمعالجة البيانات والملفات والحريات لا يسمح بجمع البيانات الشخصية إلا "لأغراض محددة وصريحة ومشروعة"؛ ولذلك في حالة عدم وجود قانون يجيز الاطلاع على الملفات واستخدامها من قبل ضابط شرطة قضائية لأغراض التحقيق الذي له هدف أو غرض مغير لأغراض التحقيق، عد ذلك انتهاكاً للمادة٨١ من قانون الإجراءات الجنائية والمادتين ٦ و٨ من الاتفاقية الأوروبية لحقوق الإنسان(١٣٧).

٣- أن تكون البيانات صحيحة وسلمية:

تضمنت المادة الثالثة من قانون حماية البيانات الشخصية المصري ضرورة أن تكون البيانات الشخصية التي تجمع صحيحة وسليمة، وهذا الالتزام يقع على عاتق جامع البيانات، إذ ينبغي عليه التأكد بكافة السبل الممكنة من صحة البيانات وإلا عد مخالفاً للقانون، وتعد اشتراط صحة البيانات ضرورة منطقية حتى أن المشرع داعماً للحفظ على هذا الشرط مكن المعني بالبيانات من ممارسة حقوقه عليها، ومنها حق التصحيح والتعديل، وتقوم جريمة الجمع غير المشروع إذا نُفّذت عملية الجمع بوسيلة أو بطريقة غير نزيهة مثل: أن تتم بدون علم المعني، وباستعمال تدابير ذات طابع تطفلي استقصائي دون الالتزام بواجب إعلام المعني(١٣٨)، وفي حالة الإخلال بكل تلك الشروط الواجب توافرها لجمع البيانات أو إحداها، تقوم في حق الجاني الجريمة المؤثمة بموجب

(136) Sophie PENA PORTA, les données à caractère personnel; les données nominatives, Art disponible sur www.pedagogie.ac-aix-marseille.fr, la date de mise en ligne est: 2/3/2005.

(137) **Cour de cassation, criminelle, Chambre criminelle, 13 décembre 2022, 22-81.851, Publié au bulletin**

(138) Jean PRADEL, Michel DANTI-JUAN, Manuel de droit pénal spécial, 3e éd CUJAS, Paris, 2004, p234.

الفقرة الثانية من المادة (٣٧) من قانون حماية البيانات الشخصية المصري ويستحق فاعلها العقاب.

الفرع الثاني
الإخلال بشروط الاحتفاظ بالبيانات الشخصية

يقصد بالاحتفاظ غير المشروع للبيانات الشخصية المعالجة إلكترونياً، 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، ويتبين من ذلك أن المشرع الفرنسي يجرم الاحتفاظ بالبيانات الشخصية المعالجة إلكترونياً في حالتين **الحالة الأولى:** إذا تم الاحتفاظ بالبيانات الشخصية المعالجة 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[١٣٩].

ولذلك وضع القانون المصري مجموعة من الضوابط لجمع وتخزين المعلومات، ومن ذلك أن يكون هناك تناسب بين المعلومات الشخصية المطلوب تسجيلها والهدف من التسجيل، فلا تخزن المعلومات الخاصة أو الشخصية إلا بالقدر الذي تكون فيه مرتبطة بالهدف، وكذلك وضع حدود زمنية للاحتفاظ بالمعلومات ترتبط بمدة تحقيق الغرض من التسجيل، وخصوصاً البيانات المتعلقة بالحالة الصحية، وأيضاً البيانات المتعلقة بالحالة الاجتماعية المقيدة بخصوص الزواج والطلاق والإعالة والأسرة والنسب والمصاهرة، والحالة العلمية والثقافية والفكرية المقيدة بخصوص الانتماء لمؤسسات أو جهات معينة، والحالة المالية المقيدة بخصوص الائتمان ودرجة اليسر والملاءة المالية والعلاقات المالية[١٤٠].

---

[١٣٩] د. ياسر محمد اللمعي، مرجع سابق، ص٢١٩، ٢١٨.

[١٤٠] المستشار الدكتور محمد جبريل إبراهيم، التحول الرقمي في منظور القانون الجنائي– دراسة تحليلية تأصيلية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٢٣، ص٥١.

(ISSN: 2537- 0758)

وباستقراء ما جاء في قانون حماية البيانات الشخصية المصري وبعض النظم المقارنة بشأن الشروط اللازمة للاحتفاظ بالبيانات الشخصية وجد أنها تدور حول مجموعة من الشروط وفيما يلي بيانها:

١- تأقيت المدة الزمنية اللازمة للاحتفاظ بالبيانات الشخصية:

يشترط فيما يتعلق بالاحتفاظ بالبيانات الشخصية شرطاً جوهرياً مفاده: ألا يتم الاحتفاظ بها لمدة زمنية أطول من المدة اللازمة للوفاء بالغرض، وهذا الشرط يعد نتيجة منطقية رتبها الشارع على الشرط المتعلق بأن يكون جمع البيانات لغاية محددة، حتى اذا انقضى الغرض من الجمع لم يعد هناك حاجة للاحتفاظ بالبيانات الشخصية، ولذلك كان لابد من تحديد المدة الزمنية اللازمة للوفاء بالغرض من الجمع، إذ لا يصح أن تكون تلك المدة الزمنية للاحتفاظ بالبيانات الشخصية على إطلاقها دون تحديد، وفي فرنسا جاء في الفقرة الخامسة من المادة الرابعة من قانون معالجة البيانات والملفات والحريات ١٩٧٨/١٧بأنه يجب أن يتم الاحتفاظ بها في شكل يسمح بتحديد هوية الأشخاص المعنيين لفترة لا تتجاوز تلك اللازمة فيما يتعلق بالأغراض التي تتم معالجتها من أجلها[١٤١]، وتضمنت الفقرة الرابعة من المادة الحادية عشرة من نظام حماية البيانات الشخصية السعودي بأنه يجب "٤- ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض".

وإذا توجهنا لقاء المشرع المصري يتضح بأن الفقرة الرابعة من المادة الثالثة من قانون حماية البيانات الشخصية قد أوردت صراحةً بأنه يتعين "ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها". ولكن يؤخذ المشرع المصري عدم تحديده على وجه الدقة تلك المدة الزمنية، وإن كان قد يفهم بأنه أَحالَ إلى اللائحة التنفيذية تحديد (المدة الزمنية) الكافية للوفاء بالغرض من جمع البيانات، ويفهم ذلك مما جاء بعجز المادة الثالثة من القانون بأن "وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والحفظ والتأمين لهذه البيانات".

وتحديد ماذا كانت المدة المحددة متناسبة مع الغرض المشروع للجمع أو التخزين أم لا تخضع لمعيار موضوعي، يتمثل بالفترة الزمنية التي تتناسب مع الغرض من معالجة هذه البيانات الشخصية؛ لذلك أوصت الهيئة الأوربية الاستشارية G29 بأن على محركات البحث الإلكترونية أن تزيل البيانات ذات الطابع الشخصي التي سجلت عليها

(141) Modifié par Ordonnance n°2018-1125 du 12 décembre 2018- art. 1

في أقرب وقت ممكن، أو على الأكثر في مدة لا تتجاوز ستة أشهر من تاريخ هذا التسجيل للبيانات الشخصية[١٤٢]. ولعل تأقيت الاحتفاظ بالبيانات الشخصية المعالجة آلياً تجد أصلها فيما يعرف بالنسيان الرقمي، ومفاده حق الفرد في عدم احتفاظ المسؤول عن معالجة بياناته الشخصية لفترة تتجاوز الغرض أو الغاية التي جمعت لأجلها[١٤٣]؛ لذلك كان لزماً على المسؤول عن معالجة البيانات الشخصية للأفراد، إنفاذ هذا الشرط بعدم الاحتفاظ بالبيانات الشخصية مدة تتجاوز الغرض الذي جمعت لأجله[١٤٤].

٢- أن يتم الاحتفاظ بالبيانات الشخصية بطريقة تحدد هوية صاحبها:

يلزم للاحتفاظ بالبيانات الشخصية وجود شروط تحكم عملية الاحتفاظ بتلك البيانات، من بين أهم تلك الشروط أن يكون الاحتفاظ بتلك البيانات وفقاً لطريقة يمكن من خلالها التعرف على هوية صاحبها، وبمفهوم المخالفة فإنه لا يجوز أن يتم الحفظ بشكل عشوائي للبيانات الشخصية، وإنما يجب أن يحدد صاحب هذه البيانات، وذلك حتى يمكن السماح لهذا الشخص بممارسة حقوقه على بياناته، كالحق في الدخول لهذه البيانات أو تعديلها[١٤٥].

٣- تأمين البيانات المحتفظ بها:

أدى استخدام قواعد البيانات في حفظ البيانات الشخصية إلى تعظم خطر الدخول غير المشروع إليها، خصوصاً في ظل ارتباط قواعد البيانات بالإنترنت؛ لذلك حرصت كافة النظم القانونية التي تعنى بحماية البيانات الشخصية على تضمين قوانيها أحكام توجب الالتزام بتأمين البيانات الشخصية باعتبارها أحد المحاور الرئيسية لحمايتها.

وجاء في الرابعة من قانون معالجة البيانات والملفات والحريات الفرنسي، والمادة الثالثة من قانون حماية البيانات الشخصية المصري تأمين البيانات كأحد الشروط اللازمة للاحتفاظ بها، ويراد بتأمين البيانات هي حفظها بشكل يمنع وصول الغير إليها، وعدم الإضرار بالمعني بالبيانات بطريقة مباشرة أو غير مباشرة.

---

[١٤٢] د. ياسر محمد اللمعي، مرجع سابق، ص٢٢٢.

[143] Etienne Quillet: Le droit à l'oubli numérique sur les réseaux sociaux. Master de droits de l'homme et droit humanitaire. Université panteon- Asas. 2011 p 21.

[١٤٤] د. محمود زكي زكي زيدان، الحماية الجنائية الموضوعية للحق في النسيان الرقمي "دراسة مقارنة"، مجلة روح القوانين– العدد المائة وواحد– إصدار يناير ٢٠٢٣–الجزء الأول، ص٣٨٦.

[١٤٥] د. سامح عبد الواحد التهامي، مرجع سابق، ص٤٠٨

(ISSN: 2537- 0758)

لذلك حرص المشرع المصري على أن يتخذ المتحكم بالبيانات جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية، وتأمينها والحفاظ على سريتها، وعدم اختراقها أو إتلافها أو تغييرها أو العبث، عبر أي إجراء غير مشروع، وهو في سبيل ذلك ألقى التزاماً على المعالج بحماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك، وما عليها من بيانات شخصية.

الفرع الثالث
الإخلال بالشروط الخاصة بإجراءات المعالجة

ينبغي لصحة معالجة البيانات الشخصية وجود شروطاً تتعلق بإجراءات المعالجة حتى تتفق مع صحيح القانون وبيانها كالتالي:

١- أن تتم معالجة البيانات بطريقة مشروعة:

أحد أهم الإجراءات التي أوجبها المشرع فيما يتعلق بمعالجة البيانات هي طريقة المعالجة، والتي استلزم بأن تكون مشروعة، ويتحقق ذلك من خلال إبلاغ المعني بالبيانات بما سوف يتم لبياناته من إجراءات معالجة، وأخذ موافقته على ذلك، ويتعين أن يكون هذا الإبلاغ قبل الشروع بأي إجراء من إجراءات المعالجة، وإلا عد الفعل غير مشروع، كونه يشكل عدواناً على الخصوصية، والتي تشكل الجريمة المنصوص عليها في قانون معالجة البيانات والملفات والحريات الفرنسي الصادر في ٦ يناير١٩٧٨، والمؤثمة بالمادة 19-226 من قانون العقوبات الفرنسي، والتي تتكون من التخزين المحوسب، دون موافقة صريحة من الشخص المعني، لإظهار البيانات الشخصية، وعلى وجه الخصوص، آرائه السياسية أو الفلسفية أو الدينية[١٤٦]؛ لذلك حتى تَوَصف المعالجة بالمشروعة، لابد من الموافقة الصريحة للمعني بالبيانات إلا في الحالات المستثناة من موافقته بموجب القانون.

٢- ألا تتم معالجة البيانات بطريقة لا تتلاءم مع الغاية من تجميعها:

يهدف هذا الشرط إلى تقييد معالجة البيانات الشخصية بالهدف الذي تم جمع هذه البيانات من أجله، بحيث ينسجم أسلوب معالجة هذه البيانات مع الغاية من جمعها، فيظل الهدف من جمع هذه البيانات حاكماً ومقيداً لكل إجراء من إجراءات معالجة

(146) **Cour de Cassation, Chambre criminelle, du 4 mars 1997, 96-84.773, Publié au bulletin.**

البيانات الشخصية بعد ذلك[١٤٧]، وتكمن أهمية هذا الشرط في أنه يؤدي إلى عدم استخدام البيانات الشخصية بعد جمعها استخداماً غير مُبرّر، والاستخدام غير المبرر هو الاستخدام غير المتوافق مع الغاية من جمع البيانات[١٤٨]، وتعرف هذه الجريمة في فرنسا اصطلاحاً بأنها الانحراف عن الغرض من المعالجة، وقد عاقب قانون العقوبات الفرنسي عليها بموجب المادة 21-226 بالسجن مدة خمس سنوات وغرامة تصل إلى ٣٠٠ألف يورو.

وعلى ذلك فإن أي شخص سلم بياناته الشخصية لأي جهة يتعامل معها بناءً على طلبه لتقديم خدمة إليه، فإنه لا يجوز لتلك الجهة إجراء معالجة لتلك البيانات الشخصية إلا في إطار الغاية التي من أجلها جمعت تلك البيانات، وفي حالة انحرفت تلك الجهة عن هذا الهدف أضحت المعالجة غير مشروعة.

العقوبة:

تضمنت المادة 18-226 من قانون العقوبات الفرنسي العقاب على معالجة البيانات الشخصية المتعلقة بشخص طبيعي على الرغم من معارضته، عندما تكون هذه المعالجة لأغراض التنقيب، ولا سيما الأغراض التجارية، أو عندما تستند هذه المعارضة إلى أسباب مشروعة، يعاقب بالسجن خمس سنوات وغرامة ٣٠٠٠٠٠يورو[١٤٩].

وعاقب على الاحتفاظ غير المشروع بالبيانات بموجب المادة 20-226 من قانون العقوبات الفرنسي والتي جاء فيها يعاقب على الاحتفاظ بالبيانات الشخصية بعد الفترة المنصوص عليها في القانون أو اللوائح، أو طلب الإذن أو الرأي، أو الإعلان المسبق الموجه إلى اللجنة الوطنية للمعلوماتية والحريات، بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠ يورو، ما لم يتم هذا الحفظ لأغراض تاريخية، إحصائية أو علمية وفقاً للشروط المنصوص عليها في القانون.

---

[١٤٧] د سامح عبد الواحد التهامي، مرجع سابق، ص٤١١.

[148] Benoit TABAKA et Yann TESAR, Loi «informatique et liberés»: un nouveau cadre juridique pour le traitement des données à caractère personnel, Dossier disponiblesur:www.foruminternet.org. la date de mise en ligneest:Octobre 2004,p33..

[149] Modifié par Loi n°2004-801 du 6 août 2004- art. 14 () JORF 7 août 2004.

(ISSN: 2537- 0758)

وقد عاقب قانون العقوبات الفرنسي في مادته 21-226 على الإخلال بالشروط الخاصة بإجراءات المعالجة- الانحراف عن الغرض من المعالجة بالسجن مدة خمس سنوات وغرامة تصل إلى ٣٠٠ألف يورو، وجاء نصها كالتالي: أي شخص يحتفظ ببيانات شخصية في وقت تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة، لتحويل هذه المعلومات عن غرضها على النحو المحدد في الحكم التشريعي أو القانون التنظيمي أو قرار اللجنة الوطنية للمعلوماتية والحريات الذي يأذن بالمعالجة الآلية، أو بموجب الإعلانات قبل تنفيذ هذه المعاملة، يعاقب عليها بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠ ألف يورو.

ونصت المادة السادسة والثلاثون من نظام حماية البيانات الشخصية السعودي على أنه (١- فيما لم يرد في شأنه نص خاص في المادة (الخامسة والثلاثين) من النظام، ودون إخلال بأي عقوبة أشد منصوص عليها في نظام آخر؛ تُعاقب بالإنذار أو بغرامة لا تزيد على (خمسة ملايين ريال، كل شخصية ذات صفة طبيعية أو اعتبارية خاصة- مشمولة بأحكام النظام خالفت أيا من أحكام النظام أو اللوائح. وتجوز مضاعفة عقوبة الغرامة في حالة تكرار المخالفة حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد.....)

وقررت الفقرة الثانية من المادة (٣٧) من قانون حماية البيانات الشخصية المصري عقوبة الغرامة على مخالفة الشروط الواردة بالمادة (٣) من ذات القانون بشأن جمع أو معالجة أو الاحتفاظ بالبيانات الشخصية وجرى نصها على ".....ويعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في المادة (٣) من هذا القانون".

ويؤخذ على المشرع المصري والمنظم السعودي ضآلة حجم العقوبة المفروضة على تلك الجريمة وكان ينبغي عليه فرض عقوبة مقيدة للحرية بالإضافة لعقوبة الغرامة، كنوع زجر الجناة في تلك الجرائم الخطيرة، والتي تشكل تهديداً حقيقياً للبيانات الشخصية لعموم أفراد المجتمع، وانتهاكاً للحق في الخصوصية، وذلك على غرار المشرع الفرنسي.

ويلاحظ على مسلك المشرع الفرنسي في العقاب على تلك الجريمة تشدده البالغ في العقوبة المفروضة، فقرر عقوبة السجن والغرامة، ولعل هذا يبرز مدى إعلاء المشرع الفرنسي للحق في الخصوصية، وإظهار مواجهة جنائية فاعلة لكل من تسول له نفسه الاجتراء على ارتكاب تلك الجريمة.

المبحث الثاني
الاعتداء على حقوق المعني بالبيانات وإخلال الحائز والمتحكم والمعالج بالتزاماتهما

تمهيد وتقسيم:

قرر قانون حماية البيانات الشخصية المصري عدد من الحقوق للمعني بالبيانات الشخصية، والتي تعد لازمة لممارسة سلطته على بياناته الشخصية، وفي المقابل فرض على الحائز أو المتحكم أو المعالج للبيانات الشخصية عدد من الالتزامات التي يتعين عليهم اتباعها ليتصف عملهم بالمشروعية، وإلا رتب القانون عقاباً جزاء على الإخلال بأي من تلك الالتزامات المفروضة قانوناً وفيما يلي بيان ذلك من خلال:

المطلب الأول: جريمة الاعتداء على حقوق المعني بالبيانات.

المطلب الثاني: جريمة إخلال الحائز والمتحكم والمعالج بالتزاماتهما.

المطلب الأول
جريمة الاعتداء على حقوق المعني بالبيانات.

تعد جريمة منع المعني البيانات الشخصية المعالجة إلكترونياً من ممارسة حقوقه عليها المنصوص عليها في المادة الثانية من هذا القانون، أحد صور الجرائم التي يمكن أن ترتكب بواسطة الحائز أو المتحكم أو المعالج، والشخص المعنى بالبيانات عرفته المادة الأولى من قانون حماية البيانات الشخصية المصري بأنه: أي شخص طبيعي تنسب إليه بيانات شخصية معالجة إلكترونيًا تدل عليه قانوناً أو فعلاً، وتمكن من تمييزه عن غيره، ويُعرف المعني بالبيانات الشخصية في نظام حماية البيانات الشخصية السعودي بصاحب البيانات ويقصد به الفرد الذي تتعلق به البيانات الشخصية[١٥٠].

أولاً- نص التجريم:

نصت المادة (٣٧) من قانون حماية البيانات الشخصية بأنه" يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، كل حائز أو متحكم أو معالج امتنع دون مقتض من القانون عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في المادة (٢) من هذا القانون.....).

---

[١٥٠] المادة الأولى من نظام حماية البيانات الشخصية السعودي، والمعدلة بالمرسوم الملكي (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ.

(ISSN: 2537- 0758)

وجاء في المادة الثانية من ذات القانون بأن (.... ويكون للشخص المعني بالبيانات الحقوق الآتية:

1 - العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.

2 - العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

3 - التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية.

4 - تخصيص المعالجة في نطاق محدد.

5 - العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

6 - الاعتراض على معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.....).

ونصت المادة الرابعة من نظام حماية البيانات الشخصية السعودي[١٥١] على مجموعة من الحقوق لصاحب البيانات لا تخرج في مجموعها عما جاء في قانون حماية البيانات الشخصية المصري.

---

[١٥١] "يكون لصاحب البيانات الشخصية-وفقاً للأحكام الواردة في النظام- الحقوق الآتية:

١. الحق في العلم، ويشمل ذلك إحاطته علماً بالمسوغ النظامي أو العملي المعتبر لجمع بياناته الشخصية، والغرض من ذلك، وألاَّ تعالج بياناته لاحقاً بصورة تتنافى مع الغرض من جمعها أو في غير الأحوال المنصوص عليها في المادة (العاشرة) من النظام.

٢. الحق في وصوله إلى بياناته الشخصية المتوافرة لدى جهة التحكم، ويشمل ذلك الاطلاع عليها، والحصول على نسخة منها بصيغة واضحة ومطابقة لمضمون السجلات وبلا مقابل مادي-وفقاً لما تحدده اللوائح- وذلك دون إخلال بما يقضي به نظام المعلومات الائتمانية فيما يخص المقابل المالي، ودون إخلال بما تقضي به المادة (التاسعة) من النظام .

٣. الحق في طلب تصحيح بياناته الشخصية المتوافرة لدى جهة التحكم، أو إتمامها، أو تحديثها.

٤. الحق في طلب إتلاف بياناته الشخصية المتوافرة لدى جهة التحكم مما انتهت الحاجة إليه منها، وذلك دون إخلال بما تقضي به المادة (الثامنة عشرة) من النظام.

٥. الحقوق الأخرى المنصوص عليها في النظام، التي تُبينها اللوائح". وحسناً ما فعلة المنظم السعودي فيما أورده من النص على حق العلم لصاحب البيانات بالمسوغ النظامي أو العملي المبرر لجمع البيانات الشخصية والغرض منها.

وتناول المشرع الفرنسي حقوق المعني بالبيانات الشخصية بقانون معالجة البيانات والملفات والحريات ١٩٧٨/١٧وذلك الفصل الثاني من الباب الثاني المعنون بعمليات المعالجة بموجب نظام حماية البيانات الشخصية المنصوص عليه في اللائحة (لائحة الاتحاد الأوروبي)٢٠١٦/٦٧٩ المؤرخة ٢٧ أبريل ٢٠١٦ من القانون في المواد من (٤٨-٥٦) وتضمنت تلك المواد مجموعة من الحقوق لحماية الأفراد من المخاطر الناتجة عن كافة صور معالجة البيانات الشخصية، ولم يخرج المشرع المصري أو المنظم السعودي عما جاءت به وشملت: الحق في الإعلام، حق الوصول الحق في التصحيح، الحق في المحو الحق في حظر المعالجة، الحق في أن تكون البيانات قابلة للنقل، حق الاعتراض[١٥٢].

ثانيًا- علة التجريم:

تكمن علة التجريم بأن لصاحب البيانات الشخصية حقوقاً عليها باعتباره المعني بها، وله الحق في ممارستها دونما ثمة عائق في ذلك، ومن شأن منع الحائز أو المتحكم أو المعالج للمعني بالبيانات الشخصية دون سند من القانون، أن يقوض حقه في الانتفاع بها على نحو يتنافى مع الواقع والقانون، ويمنح حائز البيانات أو المتحكم فيها أو معالجها سلطة على البيانات الشخصية المعالجة أكبر من سلطة الشخص المعني بها، دون متقض، ويشكل تقاعساً من جانبهم عن أداء دوارهم في تسهيل ممارسة المعني بالبيانات الشخصية لحقوقه على بياناته لذلك وجب التجريم حماية لحقوق المعني بالبيانات من الافتئات عليها.

ثالثًا- صفة الجاني:

وفقاً لما جاء بنص التجريم فقد تتطلب المشرع العقابي أن تقع الجريمة، من حائز البيانات الشخصية أو المتحكم فيها أو معالجها، وبالتالي لا يتصور أن تقع تلك الجريمة من غيرهم، فقد حصر النص التجريمي ارتكاب تلك الجريمة فيهم، وقد يحدث أن تقع تلك الجريمة منهم مجتمعين أو من أحداهم على سبيل الانفراد، فإن ارتكبوها مجتمعين عدوا فاعلين جميعاً في الجريمة وتنعقد مسؤوليتهم الجنائية، وان وقعت الجريمة من أحداهما دون الآخر فتتحقق مسؤولية الفاعل الجنائية وحده عن الجريمة.

---

[١٥٢] د. هيثم السيد أحمد عيسى، التشخيص الرقمي لحالة الإنسان في عصر التنقيب في البيانات عبر تقنيات الذكاء الاصطناعي وفقاً للائحة الأوروبية العامة لحماية البيانات لعام ٢٠١٦م، دار النهضة العربية، القاهرة، ٢٠١٩، ص٦٦.

(ISSN: 2537- 0758)

رابعاً-الركن المادي:

تقع معظم الجرائم بسلوك إيجابي، ولذا يطلق عليها الجرائم الإيجابية؛ لأن الأصل أن ينص الشارع علي عقاب الأفعال في مقام النهي عن ارتكابها، فيكون ارتكابها بما يخالف هذا النهي جريمة تستوجب العقوبة المقررة لها، ومع ذلك فقد يعمد المشرع في بعض الأحوال إلى فرض القيام بأعمال معينة عن طريق النص علي عقاب مجرد الامتناع عن القيام بها، وعندئذ يكون الامتناع عن القيام بهذه الأعمال جريمة سلبية، أي جريمة امتناع عن عمل أو جريمة ترك تستوجب العقوبة المقررة لها[١٥٣]، ويفهم من ذلك بأن تلك الجريمة هي إحجام الشخص إرادياً عن اتخاذ سلوك إيجابي معين، كان يتعين عليه اتخاذه، أي أنه إمساك إرادي عن الحركة العضوية في الوقت الذى كان يجب إتيانها فيه[١٥٤]، وفي تلك الجريمة يتحقق السلوك الإجرامي بامتناع الحائز، أو المتحكم، أو المعالج، من تمكين صاحب البيانات الشخصية المعالجة إلكترونياً من ممارسة حقوقه عليها، والتي كفالتها المادة الثانية من القانون دون وجود مقتض من القانون لذلك، فإذا وجود مقتض من القانون يمنع الحائز، أو المتحكم، أو المعالج من تمكين صاحب البيانات الشخصية المعالجة إلكترونياً من ممارسة حقوقه عليها، فلا ينطبق النص التجريمي إذ إن التجريم يستلزم بأن يكون الامتناع دون مسوغ من القانون.

وتشمل تلك الحقوق:

الإعلام بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز، أو متحكم، أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها، وهي أبسط الحقوق التي يمكن أن يمنحها القانون لصاحب البيانات الشخصية، فإذا كان هو صاحبها والمعني بها فبالتالي يحق له العلم بماهية البيانات الشخصية الخاصة به لدى الحائز أو المتحكم أو المعالج، ويعد هذا الحق من تطبيقات مبدأ الشفافية الذي نص عليها المشرع الأوروبي في المادة ١/٥من اللائحة الأوروبية لحماية البيانات، ومفاده: حق الفرد في أن يزوده المتحكم بمعلومات ذات أهمية بشأن معالجة بياناته سواء تم الحصول على البيانات منه شخصياً (م١٣) أو من مصدر آخر (م١٤)، على أن يكون تزويده بالمعلومات الواردة

---

[١٥٣] د. هلالي عبد اللاه أحمد، الوجيز في شرح قانون العقوبات–القسم العام، ٢٠١٩، بدون دار نشر، ص٤٩.

[١٥٤] د. فتوح عبد الله الشاذلي، شرح قانون العقوبات– القسم العام، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٨، ص٣٧.

في المادتين المشار إليهما من اللائحة في الوقت الذي تم الحصول على البيانات الشخصية فيه إن كان تم الحصول عليها من الشخص موضوع البيانات نفسه، أو في وقت معقول من تاريخ الحصول عليها بما لا يزيد عن شهر، إذا كان من مصدر آخر غير الشخص موضوع البيانات[١٥٥].

كما له الاطلاع على تلك البيانات والوصول إليها والحصول عليها إذ أنه في ذلك يمارس حقاً طبيعياً على بياناته الشخصية المعالجة إلكترونياً، وقد نصت المادة (١٥) من اللائحة الأوروبية لحماية البيانات بحق المعني بالبيانات في معرفة إن كانت بياناته محل للمعالجة أم لا، وينجم عن ذلك حقوقه السابقة بالعلم والاطلاع والوصول، والحصول عليها حقه في العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها، كما له حق التصحيح أو التعديل أو المحو، أو الإضافة أو التحديث للبيانات الشخصية، وتخصيص المعالجة في نطاق محدد، العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

وله كذلك حق الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع حقوقه وحرياته الأساسية، ولم يشترط القانون وجود شكل معين يظهر به الاعتراض على معالجة البيانات، غاية ما في الأمر وجود تصرف من المعني بالبيانات يفيد اعتراضه، لكن يشترط أن يكون هذا التصرف إيجابي فلا مجال لاعتبار السكوت قرينة على الاعتراض، وفي تصوري أن ما عدده المشرع من حقوق للمعني بالبيانات الشخصية هو بمثابة كاشف لها وليس منشئ، حيث إن المعني بالبيانات الشخصية له في ممارسته لحقوقه على بياناته الشخصية حقوق الملكية.

خامساً- الركن المعنوي:

تعد تلك الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة بأن يعلم الحائز أو المتحكم أو المعالج للبيانات الشخصية المعالجة إلكترونياً بحقوق المعني بها التي كفلها له القانون، والعلم في هذه الحالة مفترض وجوده لدى الحائز أو المتحكم أو المعالج، وعدم وجود مسوغ من القانون يمنحه الامتناع عن تمكين صاحب البيانات من ممارسة حقوقه عليها، وأن يعلم بأن شأن امتناعه عدم تمكين المعني بالبيانات الشخصية من ممارسة حقوقه المنصوص عليها في المادة الثانية من هذا القانون، وأن تتجه إرادته إلى السلوك السلبي المتمثل في

[١٥٥] د. هيثم السيد احمد عيسى، مرجع سابق، ص٦٦-٧٠.

(ISSN: 2537- 0758)

امتنع دون مقتض من القانون عن تمكين الشخص المعنيِ بالبيانات من ممارسة حقوقه المنصوص عليها في المادة الثانية من هذا القانون، ولا عبرة بالباعث على ارتكاب الجريمة.

سادساً-العقوبة:

عاقب المشرع الفرنسي كل من قام بالاعتداء على حق المعني بالبيانات الشخصية في رفض معالجة البيانات رغم اعتراضه على ذلك، وهي أحد صور انتهاك حقوق المعني بالبيانات بعقوبة السجن مدة تصل خمس سنوات والغرامة التي تصل ٣٠٠ألف يورو، وفقاً لما قررته أحكام المادة 1-18-226 من قانون العقوبات.

وعاقب قانون حماية البيانات الشخصية المصري على امتنع الحائز، أو المتحكم، أو المعالج دون مقتض من القانون عن تمكين الشخص المعنى بالبيانات من ممارسة حقوقه المنصوص عليها فيه، وفقاً لما جاء بالمادة الثانية من ذات القانون بعقوبة الغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه.

ونصت المادة السادسة والثلاثون من نظام حماية البيانات الشخصية السعودي (١- فيما لم يرد في شأنه نص خاص في المادة (الخامسة والثلاثين) من النظام، ودون إخلال بأي عليها في نظام آخر؛ تُعاقب بالإنذار أو بغرامة لا تزيد على (خمسة ملايين ريال، كلُّ شخصية ذات صفة طبيعية أو اعتبارية خاصة مشمولة بأحكام النظام خالفت أيا من أحكام النظام أو اللوائح. وتجوز مضاعفة عقوبة الغرامة في حالة تكرار المخالفة حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد)، وحيث إن الاعتداء على حقوق صاحب البيانات الشخصية الواردة بالمادة الرابعة من النظام ليست ضمن الجرائم التي لها نص عقابي خاص مدرج بالمادة (٣٥) من النظام؛ وبالتالي تكون العقوبة في تلك الحالة هي أم الإنذار أو الغرامة التي تصل لخمسة ملايين ريال.

وفي تصوري بأن العقوبة المنصوص عليها في القانون المصري أو النظام السعودي تتسم بالضآلة ولا تحقق الردع العام، فهي غير متناسبة مع فادحة الجريمة التي من شأنها منع المعني بالبيانات من ممارسة حقوقه المنصوص عليها قانوناً دون متقض أو سند من القانون، وكان من المناسب أن ينص المشرع على عقوبة الحبس في تلك الجريمة بالإضافة إلى الغرامة، حتى وأن كانت العقوبة تخييرية، إلا أنها كانت ستظهر مدى حرص المشرع على الحفاظ على حقوق المعني بالبيانات، وعلى الرغم من ذلك أرى بأن المشرع المصري كان أكثر توفيقاً من نظيره السعودي فيما يتعلق بالعقوبة،

فبالرغم أن كلاهما أقر عقوبة الغرامة، إلا أن المنظم السعودي جعل عقوبة الغرامة تخييرية مع عقوبة الإنذار، فقد تقتصر عقوبة عدم تمكين الشخص المعني من ممارسة حقوقه على البيانات في النظام السعودي على الإنذار، وهي عقوبة ضئيلة لا تتناسب مطلقاً مع حجم الجرم المرتكب. واتفق مع ما قرره المشرع العقابي الفرنسي من عقاب للمعتدي على حقوق المعني للبيانات الشخصية عبر معالجتها رغم اعتراضه على ذلك، وأرى أن جسامة العقوبة تأتي من فادحة الجرم المرتكب وتعكس مدى حرص المشرع الفرنسي على حماية حقوق المعني بالبيانات الشخصية، وإنزال عقوبة جسيمة لكل من يحاول النيل منها.

المطلب الثاني
جريمة إخلال الحائز والمتحكم والمعالج بالتزاماتهم

أولاً- نص التجريم:

نصت المادة (٣٨) من قانون حماية البيانات الشخصية بأنه "يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، كل حائز أو متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في المواد (٧، ٥، ٤) من هذا القانون). وقد تلخص ما جاء بتلك المواد بجملة من الالتزامات التي ألقها المشرع على عاتق كل من الحائز أو المتحكم والمعالج والتي ينبغي عليهما القيام بها، وفي حال الإخلال بتلك الالتزامات بشكل جزئي أو كلي يستحق فاعلها العقوبة المقررة بموجب المادة (٣٨) من قانون حماية البيانات الشخصية المصري.

ثانياً-علة التجريم:

يمثل التعامل مع البيانات الشخصية للأفراد أمراً بالغ الدقة والخطورة خصوصاً إذا خضعت تلك البيانات للمعالجة الإلكترونية، وحيث إن الحائز هو من يحوز البيانات الشخصية، والمتحكم بحكم عمله وطبيعته يحق له الحصول على بيانات شخصية للأفراد والتحكم فيها، وكذلك للمعالج بحكم الاختصاص بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم، فإن القانون ألقى على كاهلهم عديد من الالتزامات التي من شأنها كفالة أكبر قدر من حماية البيانات الشخصية وصيانتها، ورتب جزاءً جنائياً حال مخالفة أحد تلك الالتزامات من أي منهم؛ وذلك لصيانة البيانات الشخصية والمعنيين بها، ضد أي تصرف من حائز البيانات، أو المتحكم فيها، أو المعالج لها قد يعرضها للخطر، أو يصيب المعنيين بهل بضرر مباشر أو غير مباشر.

(ISSN: 2537- 0758)

ثالثاً- صفة الجاني:

وفقاً لما جاء بنص التجريم فقد تتطلب المشرع العقابي أن تقع الجريمة من حائز أو متحكم أو معالجها حصراً دون غيرهما، وبالتالي فلا يتصور أن تقع تلك الجريمة من غيرهم، لأن النص التجريمي حددهما وحدهما، وقد يحدث أن تقع تلك الجريمة منهم مجتمعين أو من إحداهما على سبيل الانفراد، فإن ارتكبوها مجتمعين عدوا فاعلين جميعاً في الجريمة وتنعقد مسؤوليتهم الجنائية، وإن وقعت الجريمة من إحداهما دون الآخر انعقدت المسؤولية الجنائية ضد مرتكبه واحده.

رابعاً- التزامات المتحكم:

قررت المادة الرابعة من قانون حماية البيانات الشخصية المصري عدد من الالتزامات على عاتق المتحكم والتي يرتب على مخالفتها مجتمعة أو مخالفة أياً منها استحقاق العقاب المنصوص عليه في المادة (٣٨) من القانون، وتتمحور تلك الالتزامات حول الحصول على البيانات الشخصية بطريقة مشروعة وبعد موافقة الشخص المعني بالبيانات، والتأكد من صحة تلك البيانات وكفايتها للغرض المحدد لجمعها، وانطباق الغرض المحدد من جمع البيانات مع الغرض من المعالجة، وعدم إتاحة تلك البيانات إلا في الأحوال المصرح بها قانوناً، كما ألقى القانون التزاماً جوهرياً على المتحكم بحماية البيانات عن طريق اتخاذ كافة الإجراءات اللازمة لسلامة البيانات والحفاظ على سريتها، وتأمينها ضد الاختراق أو إتلاف أو العبث بها بأي إجراء غير مشروع، والزام القانون المتحكم بالقيام بعملية محو البيانات فور انقضاء الغرض من المعالجة، وفي حالة الاحتفاظ بها عقب انتهاء الغرض منها لأي سبب مشروع، فلابد من أن تبقى تلك البيانات المتحفظ بها بشكل لا يسمح بتحديد الشخص المعني بها.

وأوجب القانون على المتحكم القيام بتصحيح أي خطأ يحدث بالبيانات فور علمه أو إبلاغه به، كما يتعين على المتحكم إمساك سجل خاص بالبيانات، يتضمن وصف فئات البيانات الشخصية الموجودة لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم، والسند في ذلك والمدة الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها، وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود، كما يلزم

المتحكم قبل ممارسة مهام عمله بالحصول على ترخيص أو تصريح من مركز حماية البيانات الشخصية[١٥٦].

أما في فرنسا فقد جاء في قانون معالجة البيانات والملفات والحريات ١٩٧٨/١٧ بأنه يجب على المتحكم تنفيذ التدابير الفنية والتنظيمية المناسبة لضمان والقدرة على إثبات أن المعالجة تتم وفقا للائحة الأوروبية وهذا القانون، وعليه وعند الاقتضاء الاحتفاظ بسجل لأنشطة المعالجة[١٥٧].

خامساً- التزامات المعالج:

تضمنت في المادة الخامسة من قانون حماية البيانات الشخصية المصري بيان بالالتزامات التي ينبغي على المعالج اتباعها لدى معالجة البيانات الشخصية، وهي أن يكون غرض معالجة أي بيانات شخصية وممارسة نشاطها مشروع، وألا يخالف النظام العام أو الآداب، وألا تجاوز الغرض المحدد للمعالجة ومدتها، ولابد من إخطار المتحكم أو الشخص المعني بالبيانات أو كل من له صفة (حسب الأحوال) بالمدة الزمنية اللازمة للمعالجة، وعقب انتهاء تلك المدة يلزم المعالج بمحو تلك البيانات، وكذلك عقب تسليمها للمتحكم، ولا يجوز له إتاحة البيانات أو نتائج المعالجة للغير، إلا في الأحوال المصرح بها قانوناً، ويقصد بالغير في إطار حماية البيانات الشخصية هو كل شخص لا يملك إذناً خاصاً ولا حقاً مشروعاً بالاطلاع على تلك البيانات.

ويلزم كذلك ليس بحماية البيانات الشخصية فحسب، بل تأمين الوسائط والأجهزة المستخدمة فيها، وعدم الإضرار بشكل مباشر أو غير مباشر بالمعني بالبيانات، وقد يتمثل هذا الإضرار في إفشاء البيانات الشخصية للمعنى بها للغير، دون الحصول على إذنه أو موافقته، متى كان في إفشاء تلك البيانات تهديد لشخصه أو اعتباره، وعليه إعداد سجل خاص بعمليات المعالجة لديه، على 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، ووصفاً للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة، كما يلزم

---

[١٥٦] حتى تاريخ كتابة هذا البحث لم ينشئ في مصر مركز حماية البيانات الشخصية، ولم تصدر اللائحة التنفيذية لقانون حماية البيانات الشخصية.

[157] Article 57 Modifié par Ordonnance n°2018-1125 du 12 décembre 2018-art. 1

(ISSN: 2537- 0758)

المتحكم قبل ممارسة مهام عمله بالحصول على ترخيص أو تصريح من مركز حماية البيانات الشخصية.

سادساً- الالتزامات بالإبلاغ والإخطار:

ألزمت المادة (٥٨) من قانون معالجة البيانات والملفات والحريات الفرنسي المتحكم بالبيانات بإخطار اللجنة الوطنية للحوسبة والحريات بأي خرق للبيانات الشخصية وفقًا للمادتين ٣٣ و٣٤ من لائحة الاتحاد الأوروبي لحماية البيانات ٢٠١٦/٦٧٩ المؤرخة ٢٧ أبريل ٢٠١٦[١٥٨]، ولعل هذا الأمر نابع من التزامه بتأمين البيانات الشخصية الذي هو أحد محاور الحماية القانونية لها، وبالتالي تعين عليه حال حدوث خرق للبيانات المسارعة إلى إخطار اللجنة الوطنية للحوسبة والحريات لاتخاذ ما يلزم في حماية البيانات.

وقررت المادة السابعة من قانون حماية البيانات الشخصية المصري التزاماً مشتركاً على كل من المتحكم أو المعالج حسب الأحوال، بإبلاغ والإخطار حال وجود انتهاك أو اختراق للبيانات الشخصية، وذلك خلال مدة (٧٢) ساعة من تاريخ العلم، غير أنه ينبغي الإبلاغ الفوري حالة كان الانتهاك أو الاختراق متعلق باعتبارات الأمن القومي[١٥٩]، كما يجب إبلاغ مركز حماية البيانات الشخصية خلال اثنان وسبعين ساعة من تاريخ العلم بانتهاك أو الخرق بالتالي:

١- وصف طبيعة الخرق أو الانتهاك، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها.
٢- بيانات مسئول حماية البيانات الشخصية لديه.
٣- الآثار المحتملة لحادث الخرق أو الانتهاك.
٤- وصف الإجراءات المتخذة والمقترح تنفيذها لمواجهة هذا الخرق أو الانتهاك والتقليل من آثاره السلبية.

---

(158) Article 58 Modifié par Ordonnance n°2018-1125 du 12 décembre 2018- art. 1

(١٥٩) اعتبارات الأمن القومي: هي أي أمر له صله بجهات الأمن القومي التي عددها قانون حماية البيانات الشخصية المصري في مادته الأولي وهي (رئاسة الجمهورية، وزارة الدفاع، وزارة الداخلية، جهاز المخابرات العامة، هيئة الرقابة الإدارية).

٥- توثيق أي خرق أو انتهاك للبيانات الشخصية، والإجراءات التصحيحية المتخذة لمواجهته.

٦- أي وثائق أو معلومات أو بيانات يطلبها المركز.

وفي جميع الأحوال يجب على المتحكم والمعالج، بحسب الأحوال، إخطار الشخص المعنى بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ وما تم اتخاذه من إجراءات، وتحدد اللائحة التنفيذية لهذا القانون الإجراءات الخاصة بالإبلاغ والإخطار.

سابعًا-العقوبة:

عاقب المشرع الفرنسي على إخلال المتحكم أو المعالج بالالتزامات المفروضة عليهم بعدم اتخاذ الإجراءات المناسبة لتأمين البيانات الشخصية، بالسجن لمدة تصل لخمس سنوات والغرامة التي تصل إلى ٣٠٠ ألف يورو وفقاً للمادة 17-226 من قانون العقوبات الفرنسي.

ونصت المادة 22-226 من ذات القانون على عقوبة السجن لمدة خمس سنوات والغرامة تصل ٣٠٠ ألف يورو حالة الإخلال بالالتزام بعدم إفشاء البيانات الشخصية، وذلك إذا ما تم بصورة عمدية، أما إن حصل الإفشاء بصوره غير عمدية نتيجة إهمال أو عدم اكتراث فتخفض العقوبة لتكون السجن مدة لا تزيد عن ثلاثة أشهر، وبغرامة لا تزيد عن ١٠٠ألف يورو.

وقرر المشرع المصري في المادة (٣٨) من قانون حماية البيانات الشخصية معاقبة كل من الحائز أو المتحكم أو المعالج حال إخلال أيهما بالالتزامات المفروضة عليهما قانوناً بمقتضى المواد ٧، ٥، ٤ بعقوبة الغرامة التي حدها الأدنى ثلاثمائة ألف جنيه وحدها الأقصى ثلاثة ملايين جنيه، وفي تصوري أن ضآلة العقوبة التي قررها المشرع المصري على كل من الحائز أو المتحكم أو المعالج لا تتناسب مطلقاً مع جسامة الجرم المرتكب منهما، حال إخلالهما بالالتزامات المفروضة عليهم قانوناً، وكان يتعين على المشرع المصري، إقرار عقوبة الحبس مع الغرامة أو احدهما لتتناسب مع جسامة تلك الجريمة.

(ISSN: 2537- 0758)

الفصل الثاني
المواجهة الجنائية للاستغلال غير المشروع للبيانات الشخصية

تمهيد وتقسيم:

أصبحت البيانات الشخصية بمثابة الوقود لكثير من الأنشطة التجارية، لا سيما في ظل وجود كثير من الحالات التي يتم الاحتفاظ فيها بالبيانات الشخصية للعملاء أثناء مباشرة النشاط التجاري، وتقوم الآن الكثير من النماذج التجارية على الاتجار في البيانات الشخصية للأفراد، فالعديد من الخدمات الإلكترونية ومواقع التواصل الاجتماعي والتطبيقات والألعاب وخلافهم، يقدمون خدماتهم مجاناً– ويعتمدون في جزء كبير من أنشطتهم على جمع البيانات الشخصية لعملائهم، كل بحسب نشاطه ونوعية البيانات التي يجمعها لبيعها لشركات أخرى، تستخدمها لدراسة الأسواق وتسويق منتجاتها بشكل أفضل، والأمر كذلك في كافة المجالات التي تتطلب التعامل مع جمهور تقريباً، حتى أن السياسيين يستعينون بخدمات محللي البيانات لفهم القواعد الانتخابية والوصول إلى أفضل طريقة دعاية انتخابية، مما يعزز فرصهم في الفوز؛ لذلك فالبيانات الشخصية أضحت عماداً اقتصاديًا رئيسياً.

ولا يتصور مع اتساع قاعدة تجارة البيانات على هذا النحو أن تغلق كل دولة على بيانات مواطنيها داخل حدودها، فالبيانات بحكم تطور وسائل الاتصال أصبحت بطبيعتها عابرة للحدود؛ لذلك فقد تنبهت الكثير من الدول لأهمية وضع تنظيم قانوني محكم لنقل البيانات إلى الخارج وكذلك للتسويق الإلكتروني المباشر(١٦٠)، وفي خضم تلك التعاملات تقع على البيانات الشخصية للأفراد العديد من الجرائم التي تشكل في مجملها خطراً داهماً على حقهم في الخصوصية، ومن أبرز تلك الجرائم نقل البيانات الشخصية عبر الحدود والتسويق الإلكتروني غير المرغوب فيه، وقد تنامت تلك الجرائم بشكل مفزع مع انتشار الإنترنت وما صاحبه من سهولة نقل وتداول البيانات عبر حدود الدول، واستغلال البيانات الشخصية في عمليات التسويق الإلكتروني غير المرغوب فيه،

(١٦٠) أ/ عبد الرحمن جمال يعقوب، قراءة في حكم محكمة العدل الأوروبية في قضية شريمز ٢بشأن نقل البيانات الشخصية من الاتحاد الأوروبي إلى الولايات المتحدة الأمريكية، مجلة القانون والتكنولوجيا، كلية القانون الجامعة البريطانية، القاهرة، المجلد الثالث، العدد الأول، إبريل ٢٠٢٣، ص٢٨٩.

الأمر الذي شكل تهديداً كبيراً للمعنيين بتلك البيانات الشخصية، مما استلزم تدخل المشرعين في العديد من النظم القانونية حول العالم إلى إيجاد سبل للمواجهة الجنائية لتلك الجرائم من خلال قوانين حماية البيانات الشخصية **وفيما يلي بيان ذلك من خلال:**

المبحث الأول: انتهاك قواعد نقل البيانات الشخصية العابرة للحدود.

المبحث الثاني: الاستغلال غير المشروع للبيانات الشخصية في الإعلانات التسويقية الموجهة.

المبحث الأول
انتهاك قواعد نقل البيانات الشخصية العابرة للحدود

تمهيد وتقسيم:

يعد الاعتداء على البيانات الشخصية عبر الحدود أحد أبرز الجرائم التي تقع على البيانات الشخصية، وقد تلحق أضرار جسيمة بالمعني بها، لذلك أخضعت قوانين حماية البيانات الشخصية حول العالم نقل البيانات عبر الحدود لعديد من الضوابط التي يتعين مراعاتها لدى نقل البيانات عبر الحدود، ورتبت عقوبات تختلف حدتها من مشرع لآخر في حالة الإخلال بتلك الضوابط، **وفيما يلي بيان ذلك من خلال:**

المطلب الأول
ماهية نقل البيانات الشخصية عبر الحدود وضوابطها

أولاً- ماهية نقل البيانات

تتدفق المعلومات والبيانات عبر الحدود دون أي اعتبار للجغرافيا والسيادة في بيئة الإنترنت، ويتيح الأفراد معلوماتهم لجهات داخلية وخارجية، وربما لجهات ليس لها مكان معروف، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها مستويات الحماية القانونية للبيانات الشخصية، وقد لا تخدم القوانين الوطنية كثيراً في تلك الحالة، حيث إن تضمينها نصوصاً بشان السيطرة على نقل البيانات قد لا يكون فاعلاً في ظل غياب التنسيق، وضمان أن يكون نقل البيانات محكوماً باتفاقات تكفل حمايتها، أو تضمن توفر حماية مماثلة في الدولة المنقول لها البيانات، وتغدو المخاطر أوسع مع نشوء ملاجئ آمنة لا تقيد عمليات المعالجة بأي قيد، ولا تتوفر عندها قيود على جمع ومعالجة البيانات، وتلك الملاجئ تهرب إليها مؤسسات الأعمال في بيئة الإنترنت للإفلات من القيود القانونية، كما في حالات البحث عن ملاجئ لا تفرض فيها

(ISSN: 2537- 0758)

الضرائب، أو تتيح تبادل الأموال دون رقابة، وهذه تمثل تحدياً عالمياً وليس مجرد تحد وطني.

ولذلك برزت الحاجة نحو إبرام الاتفاقيات الثنائية والعالمية في حقل حماية البيانات الشخصية عبر الحدود، والتي توجب إيجاد الأدوات العقدية التي تفرض على الجهة متلقية البيانات أو الوسيطة في تلقيها لإرسالها لطرف ثالث، التزامات قانونية معينة تدور في مجموعها حول هدف حماية الخصوصية، ومنع إساءة استخدام بيانات الأفراد الخاصة، إلى جانب عرضها في منع الأنشطة الاحتيالية والمساس بالمستهلك في بيئة الإنترنت[١٦١].

وتعرف عملية نقل البيانات عبر الحدود أو حركة البيانات الشخصية عبر الحدود بأنها: "نقل البيانات أو إتاحتها أو تسجيلها أو تخزينها أو تداولها أو نشرها أو استخدامها أو عرضها أو إرسالها أو استقبالها أو استرجاعها أو معالجتها من داخل النطاق الجغرافي لجمهورية مصر العربية إلى خارجة أو العكس"[١٦٢]، وقد قرر لذلك القانون عدم جواز نقل البيانات الشخصية إلى دولة أجنبية إلا بترخيص من السلطة الوطنية وفقاً لأحكام القانون، وبشرط أن تكون هذه الدولة تضمن مستوى كافٍ لحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص، إزاءَ تلك المعالجة التي تخضع لها هذه البيانات، أو التي قد تخضع لها، ويناط بالسلطة الوطنية تقدير مستوى الحماية.

ويشكل انتقال البيانات، أو تبادلها الحركة الأهم التي تتسم بها البيانات الشخصية في الفضاء السيبراني، وعلى الإنترنت، حين تنتقل بين الشبكات والتطبيقات وقواعد المعلومات، وغير ذلك من الأجهزة والبرامج، التي تعالجها لتتم عملية نقلها، أو حفظها، أو توزيعها، أو أية عملية أخرى من أنواع المعالجة، والتي تساعد في الاطلاع عليها. ويشكل نقل البيانات خارج الحدود الوطنية للدولة البعد العالمي لعملية معالجة البيانات الشخصية، ويعتبر هذا الانتقال من الناحية القانونية، نسبة إلى مبدأ السيادة الإقليمية،

---

[١٦١] د. منى تركي الموسوي، أ/ جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، عدد خاص بمؤتمر الكلية ٢٠١٣، ص ٣١٠.

Anne Bliss, Ph.D., TECHNOLOGY AND PRIVACY IN THE NEW MILLENNIUM, Ethica Publishing, 2004 P163-199

[١٦٢] المادة الأولى من قانون حماية البيانات الشخصية المصري.

وإخراجاً لها من نطاق تطبيق القوانين المحلية، وصلاحية السلطات الوطنية؛ لذلك، كان من طبيعياً أن يعطى هذا البعد، اهتماما أساسيا، في قوانين حماية البيانات[١٦٣].

ثانياً- ضوابط نقل البيانات

تتسم عملية نقل البيانات الشخصية عبر الحدود بدرجة عالية من الأهمية والخطورة في آن واحد، لذلك حرصت كافة الأنظمة التي تعني بحماية البيانات الشخصية، بإفراد عدد من الضوابط اللازم مراعاتها لدى نقل البيانات عبر الحدود وفيما يلي بيان ذلك من خلال:

١- ضوابط نقل البيانات عبر الحدود في الاتحاد الأوروبي:

كان للتوجيه الصادر عن الاتحاد الأوروبي بشأن حماية البيانات عام ١٩٩٥، بمثابة نقله نوعية شكلت تكريساً لمفهوم خصوصية المعلومات، وإقامة التوازن بينها وبين الحق في تدفق المعلومات عبر الحدود، ومواجهة تحديات توظيف التكنولوجيا في الأنشطة الإدارية والإنتاجية والخدمية في الدولة، وقد أصدر الاتحاد الأوروبي عام ١٩٩٥ دليلاً شاملاً- ملزماً لدول الاتحاد الأوروبي، ولهذا يطلق عليه الأمر التشريعي أو تعليمات- تتعلق بحماية خصوصية المعلومات وتنظيم نقل المعلومات خارج الحدود[١٦٤]، ويمكن القول بأن هذا التوجيه شكل الركيزة الأساسية التي تضمن ضوابط نقل البيانات الشخصية عبر الحدود، وتوفير مستوى حماية ملائم لتلك البيانات، إذ يمثل مرحلة جديدة في إعادة تنظيم خصوصية المعلومات، فيلزم كافة الدول الأعضاء في الاتحاد الأوروبي بوجوب تضمين أحكامه في التشريعات الوطنية، مما أدى بالعديد من دول أوروبا إلى إعادة وضع تشريعات جديدة أو تطوير تشريعاتها القائمة في هذا الحقل، خاصة فيما يتعلق بمعايير نقل البيانات خارج الحدود، لتسعي العديد من دول العالم خارج نطاق أوروبا إلى التواؤم مع ما قرره هذا القانون[١٦٥].

فقد نصت المادة الفقرة الثانية من المادة (٢٥) من التوجيه الأوروبي على إمكانية نقل البيانات الشخصية إلى بلد من بلدان العالم الثالث، متى كانت هذه الدولة تضمن وتكفل توفير مستوى كاف من الحماية القانونية لهذه البيانات، ويتم تقييم مدى كفاية هذه الحماية في ضوء جميع الظروف المحيطة بنقل البيانات، وتتمثل هذه الظروف في

---

[١٦٣] د. منى الأشقر جبور، مرجع سابق، ص١٠١، ١٠٠.

[١٦٤] د. مروة زين العابدين سعد صالح، مرجع سابق، ص٩٢

[١٦٥] د. صبرينة جدي، مرجع سابق، ص١٣٣.

(ISSN: 2537- 0758)

طبيعة البيانات، والغرض من معالجتها، والمدة المفترضة لهذه المعالجة، وبلد المنشأ، وبلد المستورد النهائي للبيانات، والقواعد القانونية المعمول في الدولة والقواعد المهنية والتدابير الأمنية المطبقة داخل الدولة.

وتناولت اللائحة الأوروبية لحماية البيانات الصادرة في ٢٧ أبريل٢٠١٦ والتي دخلت حيز التنفيذ في مايو ٢٠١٨ تنظيم عملية نقل البيانات عبر الحدود في الفصل الخامس منها فقررت في المادة (٤٤) بأن "أي نقل للبيانات الشخصية قيد المعالجة أو مخصصة للمعالجة بعد النقل إلى بلد أخر أو لمنظمة دولية، لا يتم إلا مع مراعاة الأحكام الأخرى لهذه اللائحة، والتي تتمثل في أن يتم النقل على أساس الملاءمة، كما أوضحت المادة (٤٥) من ذات اللائحة بأنه قد يتم نقل البيانات الشخصية إلى بلد أو منظمة دولية، وذلك حال قررت المفوضية الأوروبية أن الدولة أو الإقليم أو قطاعًا محددًا أو أكثر داخل ذلك البلد المنقول إليه البيانات، أو المنظمة الدولية المعنية تضمن مستوى مناسبًا من الحماية، فيجب أن تقوم الجهة التي ترغب بنقل البيانات خارج الحدود الوطنية بإجراء تقييم الآثار والمخاطر المحتملة– لكل حاله على حده– لتحديد ما إذا كانت جهة التحكم/ جهة المعالجة الخارجية ستوفر مستوى كاف من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على المسؤول الأول للجهة) لتحديد مستوى قبول المخاطر وإقرارها. وللقيام بذلك يجب أن تقوم الجهة بالالتزام بمعايير التقييم سواء المعايير العامة أو القانونية– وذلك لضمان أن يكون مستوى الحماية ملائماً في جميع الظروف[١٦٦].

مع مراعاة عند تقييم مدى كفاية مستوى الحماية، بأنه يجب على المفوضية، على وجه الخصوص، أن تأخذ في الاعتبار العناصر التالية: سيادة القانون، واحترام حقوق الإنسان والحريات الأساسية، والتشريعات ذات الصلة العامة والخاصة، بما في ذلك الأمن العام والدفاع والأمن القومي والقانون الجنائي، ووصول السلطات العامة إلى البيانات الشخصية، وكذلك تنفيذ مثل هذه التشريعات وقواعد حماية البيانات والقواعد المهنية والتدابير الأمنية، بما في ذلك قواعد النقل المستمر للبيانات الشخصية إلى

---

[١٦٦] القواعد العامة لنقل البيانات الشخصية خارج الجغرافية للمملكة، النسخة الأولى الصادرة في ٢٠٢٠/١١/٢٥، المملكة العربية السعودية منشورة على موقع ص٨ https://sdaia.gov.sa/ndmo/Files/Policies003.pdf تاريخ الزيارة ٢٠٢٣/٥/١٤م.

شخص آخر في بلد أخر أو منظمة دولية ويتم الامتثال لها في ذلك البلد أو المنظمة الدولية، بالإضافة إلى السوابق القضائية، وكذلك حقوق موضوع البيانات الفعالة والقابلة للتنفيذ، والتعويض الإداري والقضائي الفعال لأصحاب البيانات الذين يتم نقل بياناتهم الشخصية، ومدى وجود تشغيل فعال لواحدة أو أكثر من السلطات الإشرافية المستقلة في الدولة المنقول إليها البيانات أو التي تخضع لها المنظمة الدولية، مع مسؤولية ضمان وفرض الامتثال لقواعد حماية البيانات، بما في ذلك سلطات الإنفاذ الكافية للقانون، والمساعدة وتقديم المشورة لأصحاب البيانات في ممارسة حقوقهم، والتعاون مع السلطات الإشرافية في الدول الأعضاء للالتزامات الدولية التي دخلها البلد محل النقل أو المنظمة الدولية المعنية، أو الالتزامات الأخرى الناشئة عن الاتفاقيات أو الصكوك الملزمة قانونًا، وكذلك عن مشاركتها في الأنظمة متعددة الأطراف أو الإقليمية، ولا سيما فيما يتعلق بحماية البيانات الشخصية.

ويتعين على المتحكم عندما ينوي أن ينقل البيانات الشخصية، أو كما في حالة الملفات الشخصية وناتج تطبيقها إلى بلد آخر أو إلى منظمة دولية، إعلام الفرد المعني بالبيانات بتفاصيل ذلك والضمانات والتدابير التي اتخذها المتحكم بالبيانات للقيام بهذا الأمر، وقد جاء ذلك في الفقرة الفرعية (F) من المادتين ١٣/١، ١٤/١[١٦٧] من اللائحة.

وقد تضمن حكم لمحكمة العدل الأوروبية تأكيدًا من المحكمة على فكرة تساوي مستوى حماية البيانات الذي يكفله قانون الاتحاد الأوروبي، ومستوى الحماية الذي تأتي به هذه الضمانات، ويمكن استخلاص تأكيد المحكمة في هذا الصدد من خلال معيار مستوى الحماية المساوي هو حجر الزاوية في أية عملية نقل بيانات للخارج، أيا كانت الوسيلة التي تعتمد عليها، سواء كانت قرار ملاءمة أو غير ذلك. وهذا ليس التناول القضائي الأول لهذه الفكرة، إذ أكد عليها أيضًا حكم المحكمة ذاتها في قضية شريمز ١. ذلك أن الحكم أرسى لمعيار في غاية الأهمية، بأن أوضح أن مستوى الحماية المساوي لا يعني التطابق بين الحماية القانونية للبيانات في الدولة المستقبلة والاتحاد الأوروبي،

[١٦٧] د. هيثم السيد أحمد عيسى، مرجع سابق، ص٧٢.

(ISSN: 2537- 0758)

وإنما يقصد به التساوي في جوهر الحماية. وهو ما يترتب عليه أنه لا يفترض بالضرورة أن يتم اتباع الآليات ذاتها، وأن يحتوي التنظيم القانون على النصوص ذاتها، وإنما يكفي أن تتوافر بدائل في جوهرها متكافئة للحماية[١٦٨].

٢- ضوابط نقل البيانات عبر الحدود في فرنسا:

تطبيقاً لما جاءت به اللائحة الأوروبية وما تضمنته من توجيهات بشأن نقل البيانات الشخصية عبر الحدود، فقد قرر المشرع الفرنسي في قانون معالجة البيانات والملفات والحريات بالمادة (١١٢) بأنه يجوز للمتحكم بالبيانات الشخصية نقل البيانات فقط أو السماح بنقل البيانات المرسلة بالفعل إلى دولة لا تنتمي إلى الاتحاد الأوروبي عند استيفاء شروط، كأن يعد نقل هذه البيانات ضروريًا لأحد الأغراض المنصوص عليها في الفقرة الأولى من المادة ٨٧[١٦٩] من هذا القانون[١٧٠]، ويمكن القول بأن جملة ما أورده المشرع الفرنسي بشأن تنظيم نقل البيانات الشخصية عبر الحدود لا يخرج في مجمله عما قررته اللائحة الأوروبية لحماية البيانات، باعتبارها ملزمة لكافة دول الاتحاد الأوروبي وفي القلب منها الجمهورية الفرنسية؛ لذلك قام المشرع الفرنسي بتعديل نصوص قانون معالجة البيانات والملفات والحريات رقم ١٩٧٨/١٧ بموجب القانون رقم ٢٠١٨/١١٢٥ بتاريخ ١٢ ديسمبر ٢٠١٨ ليتوافق مع ما جاءت به اللائحة الأوروبية في يتعلق بحماية البيانات الشخصية ومنها حركة البيانات عبر الحدود.

---

[١٦٨] أ/ عبد الرحمن جمال يعقوب، قراءة في حكم محكمة العدل الأوروبية في قضية شريمز ٢بشأن نقل البيانات الشخصية من الاتحاد الأوروبي إلى الولايات المتحدة الأمريكية، مجلة القانون والتكنولوجيا، كلية القانون الجامعة البريطانية، القاهرة، المجلد الثالث، العدد الأول، إبريل٢٠٢٣، ص٣٠٠.

[١٦٩] وتتعلق بمعالجة البيانات الشخصية المنفذة لأغراض منع وكشف الجرائم الجنائية والتحقيقات والملاحقات القضائية في هذا المجال أو تنفيذ العقوبات الجنائية، بما في ذلك الحماية من التهديدات للأمن العام ومنع مثل هذه التهديدات، من قبل أي سلطة عامة مختصة أو أي هيئة أو كيان آخر مفوض، لنفس الأغراض، بممارسة السلطة وصلاحيات السلطة العامة، المشار إليها فيما بعد باسم السلطة المختصة.

[170] Article 112 Création Ordonnance n°2018-1125 du 12 décembre 2018- art. 1

٣- ضوابط نقل البيانات عبر الحدود في المملكة العربية السعودية:

أصدر مكتب إدارة البيانات الوطنية في المملكة العربية السعودية دليلاً[١٧١] طوي على مجموعة من القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة، وتتضمن قائمة الاعتماد وهي: قائمة معتمدة من مكتب إدارة البيانات الوطنية تتضمن أسماء الدول التي تتمتع بمستوى كاف من الحماية لحقوق

أصحاب البيانات فيما يتعلق بمعالجة بياناتهم الشخصية، وألقت التزاماً على الجهات بعدم نقل البيانات أو معالجتها خارج الحدود إلا بعد التحقق من:

١. إذا كانت جهة المعالجة الخارجية المسند إليها أنشطة معالجة البيانات الشخصية في دولة ضمن قائمة الاعتماد، فتقوم جهة التحكم/ جهة المعالجة الداخلية بأخذ موافقة كتابية من الجهة التنظيمية على نقل البيانات، وعلى الجهة التنظيمية التنسيق مع المكتب.
٢. إذا كانت جهة المعالجة الخارجية في دولة ليست ضمن قائمة الاعتماد، فإن نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة يتطلب مستوى كاف من الحماية- لا يقل عن مستوى الحماية الذي كفلته سياسة حماية البيانات الشخصية الصادرة من المكتب- بعد إجراء تقييم مستوى الحماية التي توفرها جهة المعالجة الخارجية.
٣. إذا لم يكن هناك مستوى كافي من الحماية، فتقوم الجهة بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، ومنها على سبيل المثال، استخدم البنود القياسية، أو القواعد الملزمة.
٤. إذا لم تتمكن الجهة من توفير الضمانات الكافية، فيمكن الاعتماد على أحد الاستثناءات النظامية التي تتطلب نقل البيانات، وفي جميع الحالات الواردة في الفقرات (٢) و(٣) و(٤) أعلاه، يجب على جهة التحكم أو المعالجة الداخلية الحصول على موافقة كتابية من الجهة التنظيمية على نقل البيانات، وعلى الجهة التنظيمية التنسيق مع المكتب[١٧٢].

---

[١٧١] النسخة الأولى صادرة في ٢٠٢٠/١١/٢٥م.

[١٧٢] القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة، مكتب إدارة البيانات الوطنية، النسخة الأولى ٢٠٢٠/١١/٢٥، ص٨.

(ISSN: 2537- 0758)

٤- ضوابط نقل البيانات عبر الحدود في مصر:

جاءت المادة (١٤) من قانون حماية البيانات الشخصية المصري، بمجموعة من الضوابط المنظمة لعملية نقل البيانات عبر الحدود، فحظرت إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية، أو تخزينها أو مشاركتها إلا بتوافر مستوى من الحماية لا يقل عن المستوى المنصوص عليه في هذا القانون لدى الدولة المنقول لها البيانات، وضرورة الحصول على ترخيص أو تصريح من مركز حماية البيانات الشخصية قبل الشروع في عملية النقل، على أن تشمل المعايير التي بموجبها يتم تقييم مستوى الحماية الكافي، وتتعلق بشروط الجمع والمعالجة والاحتفاظ بالبيانات ومدتها والغاية منها وكل ما يضمن حماية تلك البيانات.

وأجازت المادة (١٥) من ذات القانون على سبيل الاستثناء من حكم المادة (١٤) نقل البيانات أو مشاركة أو معالجة البيانات الشخصية إلى دولة لا يتوافر فيها مستوى الحماية الذي تطلبه القانون، وذلك شريطة موافقة الشخص المعني بالبيانات أو ينوب عنه في عدد من الحالات هي:

١- المحافظة على حياة الشخص المعنى بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له.

٢- تنفيذ التزامات بما يضمن إثبات حق أو ممارسته أمام جهات العدالة أو الدفاع عنه.

٣- إبرام عقد، أو تنفيذ عقد مبرم بالفعل، أو سيتم إبرامه بين المسئول عن المعالجة والغير، وذلك لمصلحة الشخص المعنى بالبيانات.

٤- تنفيذ إجراء خاص بتعاون قضائي دولي.

٥- وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة.

٦- إجراء تحويلات نقدية إلى دولة أخرى وفقا لتشريعاتها المحددة والسارية.

٧- إذا كان النقل أو التداول يتم تنفيذاً لاتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفا فيه.

وفي تصوري أن تلك الاستثناءات الواردة في القانون قد جاءت على سبيل المثال وليس الحصر؛ نظراً لأنه رهن النقل بالموافقة الصريحة للشخص المعني؛ وبالتالي فهو الذي يقرر إمكانية النقل من عدمه، بل وسمح وفقاً لما جاء بالمادة (١٦) من ذات القانون للمتحكم أو المعالج إتاحة البيانات عقب الحصول على تصريح من المركز في حالة توافر مجموعة من الشروط هي:

1 - اتفاق طبيعة عمل كل من المتحكمين أو المعالجين، أو وحدة الغرض الذي يحصلان بموجبه على البيانات الشخصية.
2 - توافر المصلحة المشروعة لدى كل من المتحكمين أو المعالجين للبيانات الشخصية، أو لدى الشخص المعنى بالبيانات.
3 - ألا يقل مستوى الحماية القانونية والتقنية للبيانات الشخصية لدى المتحكم أو المعالج الموجودة بالخارج عن المستوى المتوافر في جمهورية مصر العربية، وتحدد اللائحة التنفيذية لهذا القانون الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لذلك.

وفي تقديري بأن المشرع المصري بهذا النص قد جاء متعارضاً مع حقوق المعني بالبيانات الشخصية؛ لأنه أتاح للمتحكم أو المعالج نقل البيانات خارج مصر بعد موافقة المركز، دون اشتراط موافقة المعني بالبيانات الشخصية ذاته، وفي ذلك افتئات واضح على حقوقه، كما أن ضوابط نقل البيانات عبر الحدود الواردة في القانون المصري وأن تشابهت في عدد منها بما جاء في اللائحة الأوروبية لحماية البيانات الشخصية والتشريع الفرنسي والسعودي، إلا أنها ومن الناحية الواقعية تفتقد للفاعلية، وأعزو ذلك إلى أن قانون حماية البيانات الشخصية المصري أحال إلى اللائحة التنفيذية له، وضع الاشتراطات المتعلقة بنقل البيانات والمعايير اللازمة لذلك، وحتى الآن لم تصدر تلك اللائحة على الرغم من مرور فترة زمنية تزيد على ثلاث سنوات منذ صدور القانون، وبالتالي فإن تلك المعايير غير معلومة، ولا يكمن تحديد ملامحها، كما يزداد موقف المشرع المصري تعقيداً وضبابية جراء عدم إنشاء المركز الوطني لحماية البيانات الشخصية، المنوط به منح التصريح أو الترخيص لنقل البيانات عبر الحدود؛ وبالتالي فلا يمكن القول أن هناك ضمانات حقيقية لعملية نقل البيانات الشخصية عبر الحدود في جمهورية مصر العربية، طالما لم تصدر اللائحة التنفيذية للقانون، ولم ينشئ ويمارس مهام عمله مركز حماية البيانات الشخصية، حتى يمكن الوقف بشكل دقيق على إعمال الضوابط الواردة في القانون لعملية نقل البيانات الشخصية عبر الحدود.

المطلب الثاني

جريمة انتهاك قواعد نقل البيانات الشخصية عبر الحدود

تناول الفصل السابع من قانون حماية البيانات الشخصية المصري ١٥١لسنة٢٠٢٠ الأحكام المنظمة للبيانات الشخصية العابرة للحدود، تحت عنوان

(ISSN: 2537- 0758)

"البيانات الشخصية عبر الحدود" وجزاء انتهاك القواعد المنظمة لعملية نقل البيانات عبر الحدود.

أولاً-نص التجريم:

نصت المادة (٤٢) من قانون حماية البيانات الشخصية المصري بأن "يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل من خالف أحكام حركة البيانات الشخصية عبر الحدود المنصوص عليها في المواد (١٤، ١٦١٥) من هذا القانون".

ونصت المادة (٤٣) القانون المغربي المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي على أن "لا يجوز لمسؤول عن معالجة أن ينقل معطيات ذات طابع شخصي إلى دولة أجنبية إلا إذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الشخصية وللحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات أو قد تخضع لها. يتم تقديم كفاية مستوى الحماية الذي تضمنه دولة معينة لا سيما وفقا لمقتضيات المعمول بها في هذه الدولة ولإجراءات الأمن التي تطبق فيها، وللخصائص المتعلقة بالمعالجة مثل الغايات والمدة وكذا طبيعة وأصل ووجهة المعطيات المعالجة تعد اللجنة الوطنية قائمة الدول المتوفرة فيها المعايير المحددة في الفقرة ١ والفقرة ٢ أعلاه"[١٧٣].

ثانياً-علة التجريم:

تنتقل البيانات عبر الإنترنت من دولة لدولة، ومن منظمة لمنظمة، ومن جهة عمل إلى أخرى، ومن فرد إلى مؤسسة، دون قيود وبكل اللغات، وتسافر المعلومة عبر الشبكات المحلية إلى دول شتى، وتوجه من نقطة لأخرى في الفضاء، وفي تلك الأثناء تمر بالعديد من مناطق الاختصاص القضائي ومناطق السيادة، ومناطق قد لا تكون بينها تعاون أو حتى روابط، ففي مثل هذه البيئة ثمة حاجة لجهد استثنائي على النطاق الدولي، أهم ما يتعين أن يتصف به الخروج من الأطر والمفاهيم التقليدية للسيطرة، فلم تعد إرادة القوي هي حجر الزاوية، فربما يكون لفرد ما القدرة في مثل هذه بيئة أن يتحدى أعظم القوى، لهذا فإن ما نسميه ديمقراطية الإنترنت، وعدالة التعامل مع المعرفة، وعدم

---

[١٧٣] الصادر بالظهير شريف رقم ١.٠٩.١٥صادر في ٢٢ صفر (١٨فبراير ٢٠٠٩) والمنشور بالجريدة الرسمية عدد ٥٧١١ بتاريخ ٢٧ صفر ١٤٣٠ (٢٣ فبراير ٢٠٠٩).

التمييز وانتهاء عهد الاحتكار والسيطرة، تلك هي الأسس التي يتعين أن يتم التفكير فيها، في كل نشاط يهدف إلى تنظيم ضروري لمسائل الإنترنت، والأهم أن يكون تنظيماً يراعي هذه السمات التقنية، وفضلاً عن الخصائص والميزات التفاعلية اللامتناهية[١٧٤]؛ ولأن البيانات الشخصية في تلك الرحلة لابد أن تحط بقدر كبير من الأمان؛ حتى لا تعرض خصوصية أصحابها للخطر، فقد قرر المشرع المصري مجموعة من الضوابط اللازمة لنقل البيانات الشخصية عبر الحدود، وفرض عقوبة جنائية لانتهاك تلك الضوابط.

ثالثاً-صور السلوك الإجرامي للجريمة:

يتصور وقوع السلوك الإجرامي لتلك الجريمة بأكثر من صورة، كنقل بيانات إلى دولة لا يتوافر فيها مستوى من الحماية الموجود في القانون المصري، أو القيام بنقل البيانات دون الحصول على التصريح اللازم لذلك من مركز حماية البيانات الشخصية، **وفيما يلي بيان ذلك:**

١- نقل البيانات لدولة لا يتوافر فيها مستوى من حماية البيانات الشخصية الموجودة في القانون المصري

حظرت المادة (١٤) من قانون حماية البيانات الشخصية المصري، إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية، أو تخزينها أو مشاركتها إلا بتوافر مستوى من الحماية لا يقل عن المستوى المنصوص عليه في هذا القانون، وبترخيص أو تصريح من مركز حماية البيانات. ومعايير تقييم مستوى الحماية الكافي تتعلق بشروط الجمع والمعالجة والاحتفاظ بالبيانات ومدتها والغاية منها، وكل ما يضمن حماية تلك البيانات، وأحال النص إلى اللائحة التنفيذية لهذا القانون وضع السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها، إلا أنه وحتى كتابة هذا البحث وبعد مرور ثلاث سنوات كاملة على صدور القانون فإنه لم تصدر حتى الآن لائحة تنفيذية له، بما يضع المشرع بمأزق كبير حيال التعامل مع نقل البيانات الشخصية عبر الحدود، بشأن معرفة السياسات أو المعايير والضوابط لنقل أو مشاركة

---

[١٧٤] أ/ عبد الله على الشنبري، التحولات المعرفية الكبرى من العصر الحجري وحتى جوجل، مدارك للنشر ٢٠١١، ص٣٢٠.

(ISSN: 2537- 0758)

البيانات عبر الحدود، في ظل عدم وجود اللائحة التنفيذية للقانون والتي أنيط بها هذا الأمر.

وأوردت المادة (١٥) من هذا القانون جواز نقل البيانات بالرغم من عدم توافر مستوى كاف من الحماية هو أمر حتمي فرضته طبيعة البيانات وكيفية التعامل معها، فمثلاً الحماية الممنوحة للبيانات الشخصية في الدولة (أ) في عالم رقمي، تصبح بلا قيمة عندما تنسخ على جهاز كمبيوتر في الدولة (ب) التي لا يوجد فيها قيود على استخدامها، ومن ثم فإن الدول التي لديها قوانين حماية بيانات كثيراً ما تُحرم نقل البيانات إلى البلدان التي ليست لديها هذه القوانين، ولذلك سعى الاتحاد الأوروبي في واحد من مبادئه التوجيهية العديدة سعيًا واضحاً للقضاء على" ملاذات البيانات"، وحيث إن الدول من دون تشريع حماية البيانات تخاطر باستبعادها من تجارة المعلومات التي تتوسع سريعا[١٧٥]، وفي فرنسا أجازت المادة(١١٣) من قانون معالجة البيانات والملفات والحريات على سبيل الاستثناء من المادة (١١٢)، لا يجوز للمتحكم بالبيانات الشخصية، في حالة عدم وجود قرار كفاية أو ضمانات مناسبة، نقل هذه البيانات أو السماح بنقل البيانات المرسلة بالفعل إلى دولة لا تنتمي إلى الاتحاد الأوروبي، فقط عندما يكون النقل ضروريًا:

لحماية المصالح الحيوية لصاحب البيانات أو لشخص آخر؛ لحماية المصالح المشروعة للشخص المعني، عندما ينص القانون الفرنسي على ذلك؛ أو لمنع تهديد خطير وفوري للأمن العام لدولة أخرى، وفي حالات لأحد الأغراض المنصوص عليها في الفقرة الأولى من المادة ٨٧؛ وفي حالة الاعتراف بالحقوق القانونية أو ممارستها أو الدفاع عنها فيما يتعلق بنفس الأغراض[١٧٦].

ونصت المادة (التاسعة والعشرين) من نظام حماية البيانات الشخصية السعودي بعد تعديلها بأن:

"١-مع مراعاة ما ورد في الفقرة (٢) من هذه المادة، يجوز لجهة التحكم نقل البيانات الشخصية إلى خارج المملكة أو الإفصاح عنها لجهة خارج المملكة، وذلك لتحقيق أي من الأغراض الآتية:

ا- إذا كان ذلك تنفيذاً لالتزام بموجب اتفاقية تكون المملكة طرفاً فيه.

---

[١٧٥] ريموند واكس، الخصوصية، مرجع سابق، ص١١٩.

[176] Article 113 Création Ordonnance n°2018-1125 du 12 décembre 2018- art.1

ب- إذا كان ذلك لخدمة مصالح المملكة
ج- إذا كان ذلك تنفيذاً لالتزام يكون صاحب البيانات الشخصية طرفاً فيه.
د- إذا كان ذلك تنفيذاً لأغراض أخرى وفق ما تحدده اللوائح.
٢- تكون الشروط الواجب توافرها عند نقل البيانات الشخصية أو الإفصاح عنها وفق ما ورد في الفقرة (١) من **هذه المادة على النحو الآتي:**
أ- ألا يترتب على النقل أو الإفصاح مساس بالأمن الوطني أو بمصالح المملكة الحيوية.
ب- أن يتوافر مستوى مناسب لحماية البيانات الشخصية في خارج المملكة بما لا يقل عن مستوى الحماية المقرر في النظام واللوائح، وفقاً لنتائج تقويم تجريه الجهة المختصة في هذا الشأن بالتنسيق مع من تراه من الجهات المعنية.
ج- أن يقتصر النقل أو الإفصاح على الحد الأدنى من البيانات الشخصية الذي تدعو الحاجة إليه....."[١٧٧].

وقد جاء في المادة (٤٤) من المغربي المتعلق بحماية الأشخاص الذاتيين تجاه معالجة البيانات ذات الطابع الشخصي مجموعة من الاستثناءات من حكم المادة ٤٣ أعلاه، يمكن للمسؤول عن المعالجة نقل معطيات ذات طابع شخصي نحو دولة لا تتوفر فيها الشروط التي تنص عليها المادة السابقة في حال الموافقة الصريحة للشخص الذي تخصه المعطيات، أو في حالة:
١. إذا كان النقل ضروريا.
أ) للمحافظة على حياة هذا الشخص.
ب للمحافظة على المصلحة العامة.
ج) احتراما لالتزامات تسمح بضمان إثبات حق أمام العدالة أو ممارسته أو الدفاع عنه.
د) تنفيذاً لمقتضيات عقد بين المسؤول عن المعالجة والمعنى أو لإجراءات سابقة على التعاقد متخذة بطلب من هذا الأخير.
هـ) لإبرام أو تنفيذ عقد مبرم أو سيبرم بين المسؤول عن المعالجة وأحد الأغيار، وذلك لمصلحة الشخص المعني.
و) تنفيذاً لإجراء متعلق بتعاون قضائي دولي.

---

[١٧٧] مرسوم ملكي (م/١٤٨) تاريخ الاعتماد ١٤٤٤/٩/٥هـ، صحيفة أم القرى، العدد ٤٩٧٧، تاريخ الإصدار ١٤٤٤/٩/١٦هـ.

(ISSN: 2537- 0758)

ز) الوقاية من إصابات مرضية أو فحصها أو معالجتها.

٢. إذا كان النقل يتم تنفيذا لاتفاق ثنائي أو متعدد الأطراف يكون المغرب عضوا فيه.

٣. بناء على إذن صريح ومعمل للجنة الوطنية وذلك إذا كانت المعالجة تضمن مستوى كاف من الحماية الحياة الشخصية وكذا للحريات والحقوق الأساسية للأشخاص، لا سيما بالنظر إلى بنود عقد أو نظام داخلي تخضع له.

وقد أوردت المادة (١٥) من قانون حماية البيانات الشخصية المصري استثناءً من حكم المادة (١٤) من ذات القانون والمتعلقة بحظر نقل البيانات الشخصية عبر الحدود إلا في ظل ضوابط صارمة يتعين الالتزام بها، وهي الموافقة الصريحة للشخص المعني أو من ينوب عنه، وذلك في أن يكون النقل ضرورياً للمحافظة على حياة الشخص المعني، احترام التزامات قانونية تتعلق بتحقيق العدالة، وحقوق الدفاع أمام المحاكم، والتعاون القضائي الدولي، وجود ضرورة لحماية المصلحة العامة، وجود عقد أو تنفيذ عقد مبرم بالفعل لمصلحة المعني بالبيانات، إجراء تحويلات نقدية لدولة أخرى وفقا لتشريعاتها، إذا كان النقل تنفيذاً لاتفاق دولي مصر طرفاً فيه.

ويحمد للمنظم السعودي أدرجه شرط ألا يترتب على نقل البيانات الشخصية أو الإفصاح عنها المساس بالأمن الوطني للبلاد أو بمصالحها الحيوية، لما في ذلك من تغليب للمصالح العليا للبلاد على المصالح الخاصة للأفراد، ويجدر بالمشرع المصري أن يحذو حذو نظيره السعودي في إعلاء المصلحة العامة للدولة فيما يتعلق بنقل البيانات عبر الحدود.

٢- نقل البيانات لدولة أخرى مخالفة الشروط دون تصريح من المركز:

أتاحت المادة السادسة عشر من القانون للمتحكم أو المعالج جواز نقل البيانات الشخصية لدولة أخرى بعد الحصول على الترخيص اللازم لذلك من مركز حماية البيانات الشخصية، حال توافر مجموعة من الشروط التي يمكن إجمالها في:

1- اتفاق طبيعة عمل كل من المتحكمين أو المعالجين، أو وحدة الغرض الذي يحصلان بموجبه على البيانات الشخصية.

2- توافر المصلحة المشروعة لدى كل من المتحكمين أو المعالجين للبيانات الشخصية أو لدى الشخص المعنى بالبيانات.

3- ألا يقل مستوى الحماية القانونية والتقنية للبيانات الشخصية لدى المتحكم أو المعالج الموجودة بالخارج عن المستوى المتوافر في جمهورية مصر العربية، وتتولى

اللائحة التنفيذية لهذا القانون بيان الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لنقل البيانات الشخصية لدولة أخرى.

وفي حالة مخالفة المتحكم أو المعالج حسب الأحوال للشروط المنصوص عليها في تلك المادة، وقيامة بنقل البيانات الشخصية دون مراعاتها يكون مستحقاً للعقوبة المقررة بالمادة (٤٢) من هذا القانون، وكذلك تتوافر الجريمة في حق كل من المتحكم والمعالج بحسب الأحوال، حال قيامة بنقل البيانات الشخصية لدولة أجنبية برغم توافر الشروط التي تتطلبها القانون، إلا أنه لم يحصل على الترخيص الذي يمكنه من نقل تلك البيانات من مركز حماية البيانات الشخصية، فالمشرع المصري الزم المتحكم أو المعالج عند نقل البيانات عبر الحدود ضرورة الحصول على الترخيص اللازم للسماح بنقل البيانات خارج الدولة من مركز حماية البيانات الشخصية، ومراعاة الاشتراطات الواردة في هذا القانون فيما يتعلق بنقل البيانات عبر الحدود.

والواقع أن مسألة نقل البيانات الشخصية عبر الحدود وفقاً لهذا لقانون حماية البيانات الشخصية المصري، تكتنفها العديد من الصعوبات التي تجعل من هذا النص معطلاً عن التطبيق، لعل من أبرزها عدم إنشاء مركز لحماية البيانات الشخصية في مصر حتى تاريخ كتابة هذا البحث، وكذلك عدم صدور لائحة تنفيذية لهذا القانون، والتساؤل الذي أسعى لتلمس إجابة مرضية حوله كيف يتم تفعيل حماية نقل البيانات الشخصية عبر الحدود في ظل عدم إنشاء المركز المنوط به منح الترخيص بنقلها؟

وكيف يمكن قياس التزام المتحكم أو المعالج حسب الأحوال، بالمعايير والقواعد والاشتراطات اللازمة لنقل البيانات عبر الحدود، في ظل عدم صدور اللائحة التنفيذية للقانون، والتي أحال إليها تنظيم تلك الأمور؟ وعليه فإننا نهيب بالمشرع المصري إتمام العمل بإنجاز إنشاء مركز حماية البيانات الشخصية، وإصدار اللائحة التنفيذية للقانون؛ حتى يتسنى وجود رقابة فاعلة على المتحكمين أو المعالجين بشأن نقل البيانات الشخصية عبر الحدود.

رابعاً-العقوبة:

قرر قانون العقوبات الفرنسي العقاب على نقل البيانات الشخصية التي هي موضوع المعالجة أو المقصود منها أن تكون موضوع معالجة إلى دولة لا تنتمي إلى الاتحاد الأوروبي، أو إلى منظمة دولية، بأن في انتهاك للفصل الخامس من اللائحة الأوروبية لحماية البيانات(الاتحاد الأوروبي ٢٠١٦/٦٧٩ للبرلمان الأوروبي والمجلس بتاريخ ٢٧ أبريل ٢٠١٦ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية والحركة الحرة

(ISSN: 2537- 0758)

لهذه البيانات) وعاقب على تلك الجريمة بالسجن خمس سنوات وغرامة قدرها ٣٠٠,٠٠٠ يورو[١٧٨].

وجاء في القانون المغربي المتعلق بحماية الأشخاص الذاتيين تجاه معالجة البيانات ذات الطابع الشخصي بمعاقبة كل من نقل معطيات ذات طابع شخصي نحو دولة أجنبية، خرقاً لأحكام المادتين (٤٤، ٤٣) من هذا القانون بالحبس من ٣أشهر إلى سنة وبغرامة من ٢٠ألف درهم إلى ٢٠٠ ألف درهم أو بإحداهما.

ونصت المادة الخامسة والثلاثون من نظام حماية البيانات السعودي بأن (١- مع عدم الإخلال بأي عقوبة أشد منصوص عليها في نظام آخر، تكون عقوبة ارتكاب المخالفات الآتية وفقاً لما دون أمامها:

ب- كل من خالف أحكام المادة التاسعة والعشرين من النظام يعاقب بالسجن مدة لا تزيد على (سنة) وبغرامة لا تزيد على (مليون) ريال، أو بإحدى هاتين العقوبتين.

٢- تختص النيابة العامة بمهمة التحقيق والادعاء أمام المحكمة المختصة عن المخالفات المنصوص عليها في هذه المادة.

٣- تتولى المحكمة المختصة النظر في الدعاوى الناشئة من تطبيق هذه المادة وإيقاع العقوبات المقررة.

٤- يجوز للمحكمة المختصة مضاعفة عقوبة الغرامة في حالة العود حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد.

أما المشرع المصري عاقب على مخالفة أحكام نقل البيانات الشخصية عبر الحدود بعقوبة الحبس الذي لا تقل مدته عن ثلاثة أشهر وحده الأقصى ثلاث سنوات، والغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، وذلك وفقاً لنص المادة (٤٢) من القانون فالعقوبة تخييرية للقاضي أما أن يحكم بالحبس أو الغرامة أو بكليهما.

ويلاحظ على العقوبات الواردة على نقل البيانات عبر الحدود في التشريعات العربية تشابها إلى حد كبير حيث إن جميع العقوبات الواردة فيها جاءت تخييرية بين الحبس والغرامة، وتطابقت مدة الحد الأقصى لعقوبة الحبس بين كل من المنظم السعودي والمشرع المغربي فبلغت العقوبة (سنة في حدها الأقصى)، في حين كان المشرع

(178) Article 226-22-1 Modifié par Ordonnance n°2018-1125 du 12 décembre 2018- art. 13

المصري أكثر تشدداً من نظيريه السعودي والمغربي، حيث إن الحد الأقصى لعقوبة الحبس لدية يصل إلى ثلاث سنوات وفقاً لنص المادة (١٨) من قانون العقوبات المصري، والتي قررت بأن (عقوبة الحبس هي وضع المحكوم عليه في أحد السجون المركزية أو العمومية المدة المحكوم بها عليه ولا يجوز أن تنقص هذه المدة عن أربع وعشرين ساعة ولا أن تزيد على ثلاث سنين إلا في الأحوال الخصوصية المنصوص عليها قانونا.....)

أما بالنسبة للمشرع الفرنسي فقد كان الأكثر تشدداً بين التشريعات المصري والمغربي والسعودي، وذلك بإقراره عقوبة السجن مدة خمس سنوات بالإضافة إلى الغرامة ٣٠٠ألف يورو، وذلك تقديراً منه للقيمة التي تمثلها البيانات الشخصية، والخطورة التي تشكلها عملية نقلها عبر الحدود بالمخالفة للضوابط التي حددتها اللائحة الأوربية لحماية البيانات الشخصية.

وفي رأيي كان يتعين على المشرع المصري أن يسلك مسلكاً أكثر تشدداً فيما يتعلق بالعقوبة المقررة منه على تلك الجريمة وذلك لضآلة العقوبة بالمقارنة بنظيرة الفرنسي، لاسيما في ظل الخطورة الكبيرة التي تمثلها وما قد ينجم عنها من أضرار جمة للمعني بالبيانات الشخصية.

المبحث الثاني

الاستغلال غير المشروع للبيانات الشخصية في الإعلانات التسويقية الموجهة

تمهيد وتقسيم:

يوحي التسويق بالتقدم المجتمعي، ويعترف برغبات المستهلك، مع التركيز على البضائع أو الخدمة لتحقيق تلك الاحتياجات، في محاولة لدفع المستهلكين نحو البضائع أو الخدمات المقترحة، وفي الواقع إن التسويق ضروري لتطوير أي عمل تجاري[١٧٩]، غير أن التسويق الإلكتروني الموجه وغير المرغوب فيه من خلال استغلال البيانات الشخصية للأفراد، بات أحد الهموم الكبرى التي ألقت بظلالها وآثارها الوخيمة على الحياة الخاصة للأفراد، وبالتالي كان لابد من تدخل المشرع لإقرار عقوبات جنائية رادعة لمكافحة هذا السلوك المضر لعموم المتعاملين في البيئة الرقمية، وخصوصاً مع استغلال

(179) Hamed Taherdoost, Neda Jalaliyoon, Marketing vs E-Marketing, International Journal of Academic Research in Management (IJARM), Vol. 3, No. 4, 2014, © Helvetic Editions LTD, Switzerland, p336.

(ISSN: 2537- 0758)

البيانات الشخصية في عملية التسويق الإلكتروني على غير إرادة أو رغبة منهم في ذلك، **وفيما يلي بيان ذلك من خلال:**

المطلب الأول
ماهية التسويق الإلكتروني

يشكل التسويق الإلكتروني وسيلة ونشاط لترويج السلع والخدمات عبر شبكة الإنترنت، حيث يمثل الاستخدام الأمثل للتقنيات الرقمية، بما في ذلك تقنيات المعلومات والاتصالات لتفعيل الإنتاجية التسويقية، وتتمثل أهم عملياته في الوظائف التنظيمية، والعمليات والنشطات الموجهة لأجل تحديد حاجات الزبون، وتقديم السلع والخدمات له، فالتسويق كنشاط اتصالي يقدم بالضرورة خدمات للمجتمع وفق ما يحتاجه أفراده، والقيم السائدة فيه، ومن هذا المنطلق يشكل قوة تدفع إلى تميز مؤسسات الخدمات من خلال جذب الجماهير المستهدفة، نتيجة تقديمهم خدمات متميزة، وقربهم للزبائن أو المستهلكين، فهو يعمل على توحيد المواقف من خلال غرس وهم حول منتج أو سلعة معينة، فإذا كان التسويق الإلكتروني المرأة العاكسة للمؤسسات ولأهم الخدمات المقدمة من جانبها، فإن مؤسسات الخدمات تستخدمه من أجل بناء صورة عاكسة لأهم مميزاتها الخدماتية المقدمة للزبائن[١٨٠].

ومع تطور أساليب الدعاية والتسويق أدى ذلك إلى أن أصبحت البيانات الشخصية هي الأساس الذي عليه يتم بناء أساليب الدعاية، فقد ظهرت نظرية التسويق المباشر التي تقوم على أساس إنشاء دعاية خاصة لكل عميل وفقاً لما يتم تجميعه من معلومات عنه، تمثل هذه المعلومات البيانات الشخصية لهذا العميل، أفضى ذلك إلى أن تصبح لهذه البيانات الشخصية قيمة مادية، وظهور تجارة البيانات الشخصية، حيث أصبحت سبباً لربح كثير من الشركات والأفراد[١٨١]، ويتحقق ذلك من خلال عمليه جمع المعلومات الشخصية وتحديد مواقعها، حيث يختص كل جهاز كمبيوتر أو هاتف محمول أو أي جهاز آخر يتصل بالإنترنت بعنوان بروتوكول إنترنت (IP) مميز يحدد

---

[١٨٠] أ/ أسمهان جبير، دور التسويق الإلكتروني في تحسين الصورة الذهنية للمؤسسة الخدماتية دراسة ميدانية على عينة من زبائن وكالة موبيليس لأم البواقي، رسالة ماجستير، كلية العلوم الإنسانية والاجتماعية، جامعة العربي بن مهيدي أم البواقي، الجزائر، ٢٠١٨/٢٠١٩، ص٦، ٥.

[١٨١] د. سامح عبد الواحد التهامي، مرجع سابق، ص٣٩٨، ٣٩٧.

هويته، يمكنه من تتبع هذه الأجهزة، والقدرة على تحديد موقع أي جهاز من الأجهزة، الأمر الذي أسفر عن تحديات كبيرة وجديدة بشأن الخصوصية، وهيأ قدرات للحكومة أو القطاع الخاص لتحليل المعلومات الشخصية، الأمر الذي يمكن من خلاله وبدون تكلفة وبشكل فَعَال تخزين كميات هائلة من المعلومات، ودمجها وتحليلها بمجرد جمعها، ويسمح التقدم التكنولوجي بالربط بين قواعد بيانات المعلومات مع بعضها البعض، الأمر الذي يتيح المزيد والمزيد من كميات البيانات التي يمكن معالجتها، ويهيئ فرصاً جديدة للاستخدام التجاري للبيانات الشخصية، حيث إن الكثير من الخدمات التي تقدمها هذه الشركات هي خدمات مجانية وتعتمد نماذج أعمالها على جمع معلومات عن المستخدم واستخدامها في أعراض التسويق[١٨٢]، ويكون ذلك عبر مراقبة بيانات data veillance المستخدمين للتنبؤ بسلوكهم المستقبلي ومن ثم صياغة إعلانات موجهة Targeted advertisements تناسبهم، ويكون ذلك من خلال التنقيب في البيانات الضخمة المتوفرة عنهم، لمعرفة أذواقهم أو ميولهم وتوجيه الدعاية لهم على أساس ذلك[١٨٣].

لذلك أعلن موقع "فيسبوك" منذ فترة قريبة نسبياً أنه يستخدم أرقام هواتف المستخدمين، من بين غيرها من البيانات الشخصية، لحُسن توجيه الإعلانات التجارية إلى الفئة المناسبة، مؤكداً بذلك معلومات نشرتها دراسة جامعية، حيث إن إضافة البيانات الشخصية الأخرى التى يضعها المستخدم على "فيسبوك"، صارت تُستخدم فى توجيه الإعلانات التجارية إلى جمهور مناسب، بحسب مكان الإقامة والعمر والاهتمامات وغير ذلك، وصار رقم الهاتف والبريد الإلكتروني اللذان يوضعان لتأمين حماية الحساب من القرصنة من العناصر التي سيستفيد منها الموقع لهذه الغاية التجارية[١٨٤]؛ الأمر الذي دق ناقوس الخطر لدى المشرعين في عديد من النظم القانونية

---

(182) Eneken Tikk IP addresses subject to Personal data regulation, Our Law, 2013 P34.

(183) Guido Noto La Diega, "Data as digital assets: The case of targeted advertising, in Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?, eds, Gintarė Surblytė-Namavičienė, et al. (Berlin, Germany: Springer, 2018), 471;

(١٨٤) فيسبوك يستخدم أرقام هواتف المستخدمين لتوجيه الإعلانات التجارية، مونت كارلو الدولية بتاريخ ٢٠١٨/٩/٢٨م، منشور على موقع https://www.mc-doualiya.com/articles/20180928- تاريخ الزيارة ٢٠٢٣/٥/١٥م.

(ISSN: 2537- 0758)

لوضع ضوابط للتسويق الإلكتروني، وترتيب جزاء جنائي على مخالفتها تكريساً لحق مواطنيها في حماية بيانتهم الشخصية وحفظاً على خصوصيتهم.

والتساؤل الذي يثار هنا إذا كانت عمليه جمع المعلومات الشخصية وتحديد مواقعها تتم عبر العنوان بروتوكول إنترنت (IP) لجهاز الكمبيوتر أو هاتف محمول أو أي جهاز آخر يتصل بالإنترنت يحدد هويته، يمكنه من تتبع هذه الأجهزة، **فهل يعد هذا البيان من البيانات الشخصية أم لا؟ وبالتالي يعد مشمولاً بالحماية الجنائية للبيانات الشخصية.**

للإجابة على هذا التساؤل **اتجه** القضاء في فرنسا إلى اتجاهان: **الأول** يرى بأن (IP) ليس من البيانات الشخصية كونه لا يحدد ولو بصورة غير مباشرة هوية الشخص الطبيعي كونه يتعلق بجهاز وليس بشخص(١٨٥)، وفي حكم صادر في ٢٨ أبريل ٢٠١٥عن الغرفة التجارية لمحكمة "استئناف رين" تضمن أن مجرد بيان عنوان IP بغرض تحديد موقع مزود الوصول، لا تشكل معالجة آلية للبيانات الشخصية بالمعنى المقصود في المواد٢ و٩ و٢٥ من قانون حماية البيانات الصادر في ٦ يناير ١٩٧٨، حيث إن عنوان IP ليس بياناً اسمياً بشكل غير مباشر ويتعلق فقط بجهاز الكمبيوتر وليس بالمستخدم(١٨٦).

أما الاتجاه الثاني فيرى اعتباره من قبل البيانات الشخصية، وبالتالي يمثل أحد عناصر الهوية الرقمية، استناداً إلى أن عنوانIP هو بيان ذو طابع شخصي؛ نظراً لأنه وسيلة للتعرف على شخص مستخدم جهاز الحاسب الآلي، وإن كان ذلك بطريق غير مباشر؛ لأنه يحدد شخص المشترك "labonné لا "المستخدمlinternaute"، وهذا الاتجاه الأخير هو ما أخذت به الجمعية الوطنية للمعلوماتية والحريات (CNIL) إذ أوجبت على مقدمي خدمات الإنترنت الحصول على إذن منها، قبل معالجة أو جمع أي

(185) CA Paris 27 avril 2007:
CA http://www.legalis.net/jurisprudencedecision.php3?id_article=1954 Paris 15 mai 2007: http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-d-appel-de-paris-13e-chambresection-a-15-mai-2007.html

(186) Torkia HOUNKI, LA PROTECTION CIVILE ET PENALE DU CONSOMMATEUR DANS LE COMMERCE ELECTRONIQUE: Étude comparée entre le droit français, le droit égyptien et le droit libyen, UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE, Le 29 mars 2021, p 290

عنوان هوية (IP) باعتباره بيانا ذا طابع شخصي(١٨٧). ووضعت المحكمة العليا في فرنسا حدًا للشكوك القانونية المتعلقة بطبيعة عنوان IP في الحكم الصادر في ٣ نوفمبر ٢٠١٦، الصادر عن الغرفة المدنية الأولى لمحكمة النقض بمناسبة رقابتها على حكم محكمة الاستئناف، معتبرة أن "عناوينIP، والتي تجعل من الممكن التعرف بشكل غير مباشر على شخص طبيعي، هي من البيانات الشخصية(١٨٨).

وفي الولايات المتحدة الأمريكية حكمت محكمة ولاية كاليفورنيا العليا في العاشر من فبراير ٢٠١١، بإدانة موظف البنك الذي تحرى عن الرقم البريدي بخصوص تعاملات تجري على البطاقة الائتمانية، واعتبرت الرقم البريدي من بيانات التعريف الشخصي والمشمولة بمظلة حماية البيانات الشخصية(١٨٩).

أولاً- تعريف التسويق الإلكتروني:

يعرف مصطلح التسويق المباشر بأنه أي شكل من أشكال عرض السلع أو الخدمات في شكل مكتوب أو شفوي، يتم إرساله أو تقديمه عن طريق خدمة متاحة للجمهور مباشرة إلى مستخدم واحد أو أكثر، ويغطي هذا التعريف مجموعة واسعة من الأنشطة، تهدف إلى تعزيز رواد الأعمال بالوسائل الإلكترونية، كإرسال الرسائل الإخبارية، والعروض التجارية المزعومة عبر البريد الإلكتروني، والاتصال بالمستخدمين عبر الهاتف.. الخ(١٩٠)، أو هو ذلك الإعلان الذي يعتمد على تحليل ودراسة كل ما يتوافر من معلومات وبيانات ذات طابع شخصي، أو سلوكي للمستخدم على الإنترنت، بالإضافة إلى أي محتوى إلكتروني يتعامل معه، مما يضحي معه المستخدم ليس مستفيداً من خدمة فحسب، بل هدف أيضا، وبياناته مجرد سلعة تستعملها مواقع

(187) Cass. Crim. 4 avril 2007 disponible sur http://www.legalis.net/jurisprudence- decision php3? id article 1959.

(188) Cass. civ. 1ere, 3 nov. 2016, n15-22.695, publié au Bulletin; AJDA 2017. 23; D. 2016. 2285; Dalloz IP/IT 2017.
120, obs. G. Péronne et E. Daoud.

(189) By Daniel T. Rockey Requesting at Point of Sale Subject to Statutory Penalties, Counsel, Bullivant Houser Bailey PC 2011. P 23 .

(190) Bird & Bird LLP- Katarína Ondrovičová, Robert Čuperka and Filip Vlnečka, Direct Marketing and unsolicited communications, European Union, Slovakia April 19 2022 https://www-lexology-com.translate.goog/library/detail.aspx?g=571f28ec-9df0-40f0-8f7b-80defb1614e9&_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=sc تاريخ الزيارة ٢٠٢٣/٧/١٧

(ISSN: 2537- 0758)

الإنترنت في إدارة الحملات الإعلانية، يتلقاها المعلنون لتوجيه الإعلانات التي تتوافق مع هذه البيانات، مما يعنى أن الإعلان لا يستهدف إلا المستخدم المهتم فعلاً بمحتواه، وذلك بإفصاحه عن هذا الاهتمام من خلال نقرات الإعجاب ومشاركات الصور وتحديثات الحالة وغير ذلك[١٩١].

وعرف قانون حماية خصوصية البيانات الشخصية القطري رقم (١٣) لسنة ٢٠١٦ التسويق المباشر بأنه: "إرسال أي مادة إعلانية أو تسويقية بأي وسيلة إلى أشخاص بعينهم". أما المشرع المصري عرف التسويق الإلكتروني في المادة الأولى من قانون حماية البيانات الشخصية "بأنه إرسال أي رسالة أو بيان أو محتوى إعلامي أو تسويقي بأي وسيلة تقنية أيا 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"، ونظم الفصل الثامن من قانون حماية البيانات الشخصية الأحكام المتعلقة بالتسويق الإلكتروني المباشر، وحددت المادة (١٧) من قانون حماية البيانات الشخصية المصري حظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات إلا بتوافر مجموعة من الشروط **تتمثل في:**

١- الحصول على موافقة الشخص المعني بالبيانات.
٢- أن يتضمن الاتصال هوية منشئه ومرسله.
٣- أن يكون للمرسل عنوان صحيح وكاف للوصول إليه.
٤- الإشارة إلى أن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر.
٥- وضع آليات واضحة وميسرة لتمكين الشخص المعنى بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها.

وأتصور أن استغلال البيانات الشخصية في عملية التسويق الإلكتروني الموجه أو غير المرغوب فيه ليست هي الصورة الوحيدة للتعامل مع البيانات الشخصية لغرض تجاري- وإن كانت هي الصورة الأبرز- غير أن المشرع المصري كان من الأجدى نفعاً له، وضع إطار عام للتعامل مع البيانات الشخصية لأغراض تجارية وليس قصرها على نوع بعينه وهو التسويق الإلكتروني المباشر.

---

[١٩١] د. أشرف جابر، استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصية، مجلة العلوم الإنسانية، جامعة الأخوة منتوري- قسنطينة، الجزائر، عدد خاص ٢٠١٥، ص١٠.

ثانياً-طرق التسويق الإلكترونى المباشر:

تنامت بشكل ملحوظ عملية التسويق الإلكتروني، والتي غزت ساحة التكنولوجيا وازدادت بصفة خاصة مع انتشار الهواتف الذكية و تطبيقاتها المتطورة باستمرار، وكذلك مع انتشار وسائل التواصل الاجتماعى، وما تتطلبه من إفصاح عن البيانات الشخصية للمتعاملين، والتي من خلالها تسطيع أن تحدد اهتمامات كل فرد وشواغله، وتستغل تلك المعلومات عن اهتمامات رواد شبكات التواصل الاجتماعي في انتقاء عينة من جمهور المتعاملين، ومعرفة كيفية توجيه المادة الإعلانية إليهم، فمثلاً عند البحث عن موضوع ما على أحد هذه الوسائل الاجتماعية على شبكة الإنترنت، أو المشاركة لمنشور أعجبت به، ستواجه الكثير من المنشورات الدعائية المشابهة له، لذا لا تستغرب بأنك إن قررت حجز تذكرة طائرة إلى نيويورك على الإنترنت، وبعد يومين أثناء قراءة الجريدة اليومية على الإنترنت، يقدم لك إعلاناً عرضاً لاستئجار سيارة في نيويورك، هذه ليست مجرد مصادفة إنها آلية إعلانية مستهدفة، حيث يتم تطويرها أكثر فأكثر على الإنترنت[١٩٢].

وتتنوع الطرق التي تستخدم في التسويق الإلكتروني الموجهة، فهناك **الإعلان عن طريق محركات البحث** والذي يمكن المعلن من تحديد الكلمات الرئيسة Ad Words الأكثر بحثاً من جانب مستخدمي هذه المحركات، كاختيار كلمة تأمين مثلاً، فيظهر الإعلان الخاص بالمعلن بمجرد البحث عن هذه الكلمة، إما أعلى أو بجوار مستطيل البحث مباشرة، ومن أبرز الأمثلة على ذلك الإعلان عن طريق محرك البحث Google Ad Words.

وتتميز هذه الطريقة بأنها تمكن المعلن من الوصول إلى العملاء المستهدفين، وذلك بواسطة تحديد أو اختيار الكلمات الرئيسة لظهور الإعلان، ومن ثم يستطيع عرض الإعلان أمام أكبر عدد ممكن من المستخدمين المتوقع اهتمامهم بالمحتوى الإعلاني المعروض، كما تتميز هذه الطريقة أيضاً بأنها تمكن المعلن من تحقيق الاستهداف المحلي والإقليمي، حيث يستطيع تحديد نطاق جغرافي لظهور الإعلان أمام متصفحي هذا النطاق فقط، كأن يظهر الإعلان لمستخدمي مدينة معينة فقط أو أكثر، تقع داخل مسافة معينة من موقع المعلن، وأخيراً فإن هذه الطريقة تتميز بالمرونة، بحيث يستطيع

---

[١٩٢] التقرير الصادر عن اللجنة القومية للمعلوماتية والحريات الفرنسية CNIL بشأن التسويق الإلكتروني بجلسة ٥ فبراير ٢٠٠٩، ص٤ منشور على http://www.audentia-gestion.fr/CNIL/Publicite_Ciblee_rapport_VD.pdf تاريخ الزيارة ٢٠٢٣/٥/٢٢م.

(ISSN: 2537- 0758)

المعلن تعديل محتوى الإعلان في أي وقت، وعلى أي نحو، في ضوء ما قد يطرأ من مستجدات، وكذلك الإعلان عن طريق المواقع والمنتديات، ومؤدى ذلك أن يتفق المعلن مع الموقع أو المنتدى، بحيث يدفع المعلن قيمة عرض الإعلان على أي منهما، سواء تم عرض الإعلان في شكل شريط إعلاني Banner Ads أو إعلان منبثق Pop-up Ad أو إعلان نصى Text Ads أو إعلان فيديو Video Ads أو رعاية من الموقع(١٩٣).

ومن ضمن طرق **الإعلانات الموجهة رسائل البريد الإلكتروني العشوائية:** وهي رسائل بريد إلكتروني يتم إرسالها للأفراد دون علم أو موافقة منهم، وغالبًا ما تحتوي على مواد تسويقية، ويمكن أن يتسبب محتواه في الإزعاج والإحراج وحتى الضيق، لذلك في أحد التطبيقات القضائية: اعتبرت المحكمة الابتدائية الكبرى بباريس أن إرسال رسائل إلكترونية دعائية لشخص على الرغم من اعتراضه على ذلك يعتبر انتهاكاً لحقه في الاعتراض على معالجة بياناته الشخصية(١٩٤)، ومع ذلك يجدر التنويه أن مرسل البريد الإلكتروني عمومًا لا يستهدف المستلمين بشكل شخصي، ويمكن إرسال نفس البريد الإلكتروني العشوائي إلى ملايين الأشخاص في نفس الوقت، ويمكن غالبًا تخمين العناوين كما أنه ليست كل رسائل البريد الإلكتروني التسويقية المرسلة دون موافقة رسائل بريد إلكتروني غير مرغوب فيها.

فيمكن إرسال رسائل البريد الإلكتروني التسويقية دون موافقة مسبقة من قبل أحد المحلات التي حصلت على عنوان بريدك الإلكتروني عندما اشتريت شيئًا منها، وتعلن عن منتجات أو خدمات مماثلة، ومع ذلك يجب أن تلتزم رسائل البريد الإلكتروني التسويقية هذه بقواعد صارمة فيما يتعلق بمحتواها، وتوفر للمستلم فرصة الانسحاب، ويمكن القول بأن التسويق المباشر عن طريق البريد الإلكتروني واحدًا من أهم طرق التسويق المباشر السريعة والمميزة، كما تتميز تلك الطريقة بتكلفتها المحدودة، كذلك بإمكانها متابعة العملاء بأخر تطورات الأعمال، ومتابعتهم في الكافة الأحداث التي تجري في السوق من حولك.

وهناك التسويق المباشر عبر الهاتف: يتم من خلال تلك الطريقة تحديد الجمهور المستهدف وجمع بياناتهم الخاصة ومتابعتهم في إرسال الخدمات والمنتجات لهم،

(١٩٣) د. أشرف جابر، مرجع سابق، ص١٤.

(194) TGI paris, 17 èmech, 7 décembre 2004, et disponible sur www.droit-tic.com

وترقبهم في كل ما هو جديد من خلال محادثات هاتفية، كما يمكن من خلال تلك الطريقة استخدام وسيلة البيع الفوري مع العميل ومعرفة آرائهم ومتطلباتهم من أجل تطوير الخدمات أو المنتجات المقدمة لهم.

وكذلك التسويق المباشر من خلال الرسائل النصية (SMS) تعتبر الرسائل الإعلانية والدعاية التسويقية الإلكترونية للسلع أو الخدمات عبر الرسائل النصية القصيرة للهواتف النقالة لجمهور المستهلكين وسيلة فعالة وسريعة، تمكن من خلالها المعلنين أو الموردين من الوصول السريع الجمهور المستهلكين، وبطريقة بسيطة حيث أصبح استخدام الهواتف النقالة ضرورة من ضرورات الحياة في العصر الحالي، والتي لا يمكن للإنسان الاستغناء عنها في حياته اليومية، وتظل ملاصقة معه أثناء عمله أو تواجده في الشارع أو المنزل، وبالتالي يضمن المعلن أو المزود وصول الرسالة الإعلانية والدعاية التسويقية للسلعة أو الخدمة[١٩٥] وهي من أفضل وأسرع طرق التسويق المباشر وأكثرها انتشارًا من بين الطرق الأخرى.

فضلاً حصول التسويق المباشر عن طريق وسائل التواصل الاجتماعي والتي تعتبر من أكثر قنوات التسويق انتشارًا من بين العديد من قنوات التسويق الإلكتروني، كما تعد الأكثر استخدامًا في آلية التواصل مع الآخرين، ويمكن من خلالها التواصل مع العملاء وتقديم العروض المختلفة عن طريق إرسال رسائل نصية عبر منصات التواصل المختلفة، خاصة استخدام الفيس بوك فهو الأكثر انتشاراً واستخداماً من بين العديد من المنصات، ولمواقع التواصل الاجتماعي، بوجه عام، غرض تجارى محدد هو تسويق البيانات ذات الطابع الشخصي التي توضع عليها، ويعد هذا التسويق مورداً هاماً من مواردها المالية، ويتميز موقع (كفيس بوك) بتنوع مصادر دخله من الإعلانات المستهدفة، وهي إعلانات الدفع بالنقرةPPC ، وإعلانات الرعايةsponsor ، ومتجر الهدايا، والنقود الافتراضية ولإدارة هذه الإعلانات يعتمد الموقع في المقام الأول ونظير إتاحة التسجيل المجاني عليه، على تحليل المعلومات التي تم جمعها وذلك بغرض استخدامها لأغراض تسويقية، وتمثل هذه المعلومات قاعدة بيانات غير محدودة تكشف

[١٩٥] د. ياسر محمد اللمعي، المواجهة الجنائية للممارسات الإعلانية والدعاية التسويقية الإلكترونية غير المشروعة للسلع والخدمات، دراسة تحليلية مقارنة، مجلة روح القوانين، كلية الحقوق جامعة طنطا، العدد ١٠١، يناير ٢٠٢٣، الجزء الأول، ص٧٧.

(ISSN: 2537- 0758)

عن ميول واهتمامات المستخدمين، وهو ما يمثل مادة تسويقية تجذب المعلنين لدفع ثمنها إلى الموقع للحصول عليها[١٩٦].

ثالثاً-أنواع التسويق الإلكتروني:

يرى Kotler إمكانية تصنيف التسويق الذي تمارسه المؤسسات في ثلاث أنواع رئيسية على النحو التالي:

١- التسويق الخارجي Marketing external ويرتبط هذا النوع بالوظائف التقليدية التي يمر بها التسويق مثل تصميم وتنفيذ عناصر المزيج التسويقي: المنتج، والسعر، وتوزيع، والترويج.

٢- التسويق الداخلي Internal Marketing وهو يرتبط بعالمين داخل المنظمة، وهو يسير إلى ضرورة إتباع المنظمة لسياسات فعالة لتدريب العاملين وتحفيزهم للاتصال الجيد بالعملاء، ودعم العاملين للعمل كفريق واحد، ويسعى إلى تلبية حاجات ورغبات العملاء وكسب رضاهم، وعليه يجب أن يكون كل فرد في المؤسسة موجد في عمله بالعملاء، ولا يكفي وجود قسم خاص يمارس الأعمال التقليدية للتسويق ويعمل بقية الأفراد والأقسام في اتجاه مختلف.

٣- التسويق التفاعلي Interactive Marketing ويرتبط هذا النوع بفكرة وجود خدمات والسلع المقدمة للعملاء، وهي التي يجب أن تعتمد بشكل أساسي ومكثف على الجودة والعلاقة بين البائع والمشتري[١٩٧].

وقد تضمن التقرير الصادر عن اللجنة القومية للمعلوماتية والحريات الفرنسية CNIL بشأن التسويق الإلكتروني أنواع الإعلانات عبر الإنترنت كشكل من أشكال التسويق الإلكتروني وقسمها إلى ثلاث أنواع:

١- **إعلانات مخصصة كلاسيكية، والإعلان المخصص هو:** إعلان يتم اختياره وفقاً للسمات المعروفة لمستخدم الإنترنت العمر، والجنس، والموقع، وما إلى ذلك والتي قدمها بنفسه، على سبيل المثال عن طريق التسجيل في إحدى الخدمات.

وهذا النوع من الإعلانات هو الأكثر كلاسيكية، ولكن تمت إعادة النظر فيه الآن بواسطة الشبكات الاجتماعية، وفي الواقع لا يوفر مستخدمو الشبكات الاجتماعية عناصر من هويتهم فحسب، بل يوفرون أيضًا عناصر مفصلة لاهتماماتهم وشغفهم،

---

[١٩٦] د. أشرف جابر، مرجع سابق، ص١٦.

[١٩٧] أ/ أسمهان جبير، مرجع سابق، ص٣٣.

تسمح هذه المجموعة المفصلة من البيانات الشخصية للشبكات الاجتماعية بتقديم منصة توزيع إعلانات مخصصة الغاية.

٢- **الإعلان السياقي هو:** إعلان يتم اختياره بناءً على المحتوى الفوري المقدم لمستخدم الإنترنت، وبالتالي يتم اختيار المنتج أو الخدمة المعلن عنها في الإعلان السياقي وفقاً للمحتوى النصي للصفحة التي يتم إدخال الإعلان فيها، أو إذا كان محرك بحث، وفقًا للكلمة الأساسية التي أدخلها مستخدم الإنترنت لبحثه، وتستكمل هذه البيانات أحيانًا بمعلومات تحديد الموقع الجغرافي المستخلصة من عنوان IP الخاص بمستخدم الإنترنت، أو عن طريق الطلب السابق في الحالة المحددة لمحرك البحث، ويتم استهداف الإعلان وفقًا لاهتمامات المستخدم المفترضة بقدر ما ينتقل الأخير إلى صفحة يمكن افتراض أنها مرتبطة بمجالات اهتمامه، فعادة ما يعرض الموقع الذي يقدم نتائج رياضية إعلانات عن السلع الرياضية.

٣- **الإعلان السلوكي:** هو إعلان يتم اختياره من خلال مراقبة سلوك مستخدم الإنترنت بمرور الوقت، وبالتالي يهدف إلى دراسة خصائص مستخدم الإنترنت من خلال أفعاله والزيارات المتتالية للمواقع، والتفاعلات، والكلمات الرئيسية، وإنتاج المحتوى غير الإنترنت، وما إلى ذلك لاستنتاج ملفه الشخصي وتقديم الإعلانات المناسبة له[١٩٨].

رابعاً-خصائص التسويق الإلكتروني:

يتسم التسويق الإلكتروني بالعديد من الخصائص منها:

١. الخدمة الواسعة يتميز التسويق الإلكتروني باتساع نطاق خدماته، وبالتالي يمكن العملاء المتعاملون مع الموقع التسويقي من الدخول إلى الموقع في أي وقت، دون معرفة الشركة صاحبة الموقع إلا إذا اتصل بها.

٢. عالمية التسويق الإلكتروني: إن التقنيات المستخدمة في التسويق الإلكتروني لا تعترف بوجود الحدود الجغرافية أو الزمنية بين الأسواق، وهنا يمكن للتسويق من الوصول إلى مكان أي عميل وفي أي وقت مهما اختلف الزمان ليلاً ونهاراً.

---

[١٩٨] التقرير الصادر عن اللجنة القومية للمعلوماتية والحريات الفرنسية CNIL بشأن التسويق الإلكتروني بجلسة ٥ فبراير ٢٠٠٩، ص٥، منشور على http://www.audentia-gestion.fr/CNIL/Publicite_Ciblee_rapport_VD.pdf تاريخ الزيارة ٢٠٢٣/٥/٢٢م.

(ISSN: 2537- 0758)

٣. سرعة تغير المفاهيم: يتميز التسويق الإلكتروني بسرعة تغير المفاهيم المرتبطة بالأنشطة والقواعد التي تحكمه، ذلك أن التجارة الإلكترونية باعتبارها الإطار الأوسع للتسويق الإلكتروني والمعلومات والتي تتغير وتتطور بشكل متسارع جدا، وضرورة انعكاس ذلك على مواكبة التشريعات والوسائل القانونية لهذا التغير.
٤. أهمية الإعلان عبر الشبكة الدولية وهنا يجب استخدام عنصر الإثارة ولفت انتباه المستخدم إلى الرسائل الإلكترونية، على غرار ما هو حاصل في الإعلانات التلفزيونية.
٥. تضيق المسافة بين الشركات: يساهم التسويق الإلكتروني بتضييق المسافة بين الشركات الكبيرة والصغيرة في كثير من القضايا مثل: الإنتاج والتوزيع والكفاءات البشرية، حيث تتمكن الشركات الصغيرة من الوصول إلى السوق الدولية، دون أن تكون لها البنية التحتية المتاحة للشركات الضخمة في السوق التنافسي(١٩٩).

وعلى الرغم مما تحققه الإعلانات المستهدفة من مزايا أهمها ما تقدمه من إعلانات تتوافق مع ميول واهتمامات "المستهلك المستهدف"، إلا أنها تنطوي على مخاطر تتعلق بالحرية الشخصية، واحترام حرمة الحياة الخاصة، ولعل أهمها هو أن هذه الإعلانات تساعد على "إنشاء ملفات شخصية منتظمة لمستخدمي الإنترنت profilnge systematique des internautes " عن غير إرادة منهم، كما أنها قد تؤدى إلى جعل الملفات الشخصية للمستخدمين بمثابة سلعة تجارية un risque de marchandisation des profils individuels بين موردي المضمون كمواقع التواصل الاجتماعي والمعلنين، ولا شك في أن هذا الوضع يثير مشكلة على قدر كبير من الأهمية، وهي حماية خصوصية هؤلاء المستخدمين، وضرورة وضع ضوابط لاستعمال هذه البيانات(٢٠٠).

خامساً- مخاطر التسويق الإلكتروني:

يدخل المتسللون من خلال اختراق المواقع الرئيسية على الإنترنت لتضمين برامج ضارة، تبرز عدد من المخاطر الخفية لـ المستهلكين في صناعة الإعلان عبر الإنترنت من بين هذه المخاطر (البرامج الضارة) التي يتم تقديمها من خلال الإعلان عبر الإنترنت، دون أي نقرات أو تفاعل من قبل المستخدم، علاوة على ذلك فإن جمع

(١٩٩) أسمهان جبير، مرجع سابق، ص٣٤.
(٢٠٠) د. أشرف جابر، مرجع سابق، ص٩.

البيانات الذي يجعل الإعلان عبر الإنترنت ممكناً، ويسمح أيضًا لمجرمي الإنترنت باستهداف أنشطتهم ضد المستخدمين الضعفاء؛ نظراً لأن صناعة الإعلان عبر الإنترنت تصبح أكثر تعقيداً ومجزأة، فقد تكون هناك مساءلة أقل للمشاركين الأفراد على الرغم من أن الشركات نفسها تعاني أيضًا من الأضرار التي تلحق بالسمعة أو غيرها من هذه الهجمات، إلا أنه غالبًا ما يُترك المستهلكون مع القليل من التعويض-إن وجد- عن الأضرار التي لحقت بهم[٢٠١].

كما أنه من ضمن مخاطر التسويق عبر الإلكتروني قد يشكل وسيلة للابتزاز المالي ففي سبتمبر ٢٠٠٩، تقدمت شبكة إعلانية وهمية إلى صحيفة New York Times بطلب شراء مساحات إعلانية على موقع الصحيفة الإلكتروني NYTimes.com زاعمه أنها تمثل إحدى شركات الاتصالات وتدعى Vonage، والتي كان قد سبق لها بث إعلانات على موقع الصحيفة، الأمر الذي لم تتردد معه هذه الصحيفة في قبول بيع المساحات الإعلانية لذلك الطرف الوهمي، الذي بث في بادئ الأمر ولعدة أسابيع إعلانات مشروعة لصالح شركة Vonage، ثم ما لبث أن استبدلها بأخرى تتضمن رسالة للمستخدم تفيده بأن جهاز الحاسب الخاص به غير أمن، وأنه في حاجة إلى شراء برنامج حماية- وهو في حقيقته وهمى- وبمجرد تحميل البرنامج على الجهاز يقوم بسرقة البيانات الشخصية للمستخدم وابتزازه مالياً في مقابل إزالة البرنامج الضار من على جهازه[٢٠٢]، ويمكن القول بأن نمو الإعلانات الموجهة عبر الإنترنت أدت إلى زيادة عدد مجرمي الإنترنت الذين يحاولون البحث عن نقاط الضعف في النظام البيني،

---

(201) ONLINE ADVERTISING AND HIDDEN HAZARDS TO CONSUMER SECURITY, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS UNITED STATES SENATE, RELEASED IN CONJUNCTION WITH THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS' MAY 15, 2014 HEARING, p26. منشور على موقع تاريخ الزيارة ٢٠٢٣/٧/٢٤م
https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/REPORT%20-%20Online%20Advertising%20&%20Hidden%20Hazards%20to%20Consumer%20Security%20&%20Date%20Privacy%20(May%2015%202014)2.pdf

(202) **Elinor Mills, Ads--the new malware delivery format, Sept. 15, 2009, منشور على موقع تاريخ الزيارة ٢٠٢٣/٧/٢٤م https://www-cnet-com.translate.goog/news/privacy/ads-the-new-malware-delivery-format/?_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=sc**

(ISSN: 2537- 0758)

واستغلالها وتحديد مواقع الضحايا المحتملين الجدد، حيث لا يدرك العديد من المستهلكين أن مواقع الويب الرئيسية أصبحت طرقًا متكررة لمجرمي الإنترنت الذين يسعون للإضرار بالمستهلكين ببرامج ضارة قائمة على "الإعلانات الضارة.

المطلب الثاني

جريمة انتهاك قواعد التسويق الإلكتروني

يعد التسويق الإلكتروني الموجهة في الأصل سلوك مشروع متى حصل مستوفياً للشروط والضوابط التي حددها القانون، إلا أنه في حالة إخلال المرسل لغرض تسويقي بأحد الضوابط والأحكام المتعلقة به، نكون آزاء جريمة فرض لها المشرع عقاباً لقاء مقارفتها. فقد اتجهت السياسة التشريعية الجنائية المعاصرة إلى تجريم الممارسات الإعلانية والدعاية التسويقية غير المشروعة للسلع أو الخدمات، والتي يكون من شأنها أن تؤدي إلى خداع أو تضليل أو غش أو إزعاج أو انتهاك الخصوصية المستهلك عبر الإنترنت والهواتف النقالة الذكية، وكذلك تجريم كافة أنواع الممارسات الإعلانية غير المشروعة والتي تخالف من خلالها القواعد المنصوص عليها قانوناً[٢٠٣].

أولاً-نص التجريم:

نصت المادة (٤٣) من قانون حماية البيانات الشخصية المصري بأن "يعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، كل من خالف أحكام التسويق الإلكتروني المنصوص عليها في المادتين (١٨، ١٧) من هذا القانون".

وقررت المادة (٢٢) من قانون حماية خصوصية البيانات الشخصية القطري رقم (١٣) لسنة ٢٠١٦ بأنه "يُحظر إرسال أي اتصال إلكتروني بغرض التسويق المباشر إلى الفرد، إلا بعد الحصول على موافقته المسبقة .ويجب أن يتضمن الاتصال الإلكتروني هوية مُنشئه، 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.

ثانياً-علة التجريم:

تضمنت المذكرة الإيضاحية لقانون حماية البيانات الشخصية المصري والصادرة عن وزير العدل مبررات تجريم انتهاك قواعد التسويق الإلكتروني، بأنه مع تطور تكنولوجيا

---

[٢٠٣] د. ياسر محمد اللمعي، المواجهة الجنائية للممارسات الإعلانية والدعاية التسويقية الإلكترونية غير المشروعة للسلع والخدمات، مرجع سابق، ص٨٣.

المعلومات والاتصالات المتلاحقة، وخاصة مع تغلغل تكنولوجيات إنترنت الأشياء، والحوسبة السحابية والذكاء الاصطناعي وغيرها أدت إلى ظهور تحديات جديدة على مستوى حماية البيانات الشخصية، حيث زاد نطاق وحجم جمع وتبادل ومعالجة هذه البيانات إلكترونياً بشكل غير مسبوق، مما سمح للشركات والمؤسسات الخاصة والعامة باستخدام البيانات الشخصية للأفراد على نطاق واسع؛ نظرًا لأن الأنشطة الإلكترونية القائمة على جمع وتحليل واستنباط وتخزين تلك البيانات تساعد الشركات والمؤسسات على الاستفادة الاقتصادية والتجارية من تلك البيانات الرقمية بشكل متزايد، وذلك كله يتم دون وجود إطار قانوني حاكم لهذه الأنشطة، وارتكزت فلسفة وأهداف هذا القانون على العديد من الأسباب منها وضع آليات كفيلة بالتصدي للأخطار الناجمة عن استخدام البيانات الشخصية للمواطنين ومكافحة انتهاك خصوصيتهم.

وتقنين وتنظيم أنشطة استخدام البيانات الشخصية في عمليات الإعلان والتسويق على الإنترنت وفي البيئة الرقمية بشكل عام، كون التسويق الإلكتروني غير المرغوب فيه يعد عدواناً سافراً على حق الأفراد في الخصوصية وحماية بياناتهم الشخصية، لذلك وجب التجريم، حيث إن أعداد هائلة من المستخدمين للإنترنت وشبكات التواصل الاجتماعي دفعت الشركات الكبرى في العالم نحو استثمار بياناتهم باعتبارها ثروة تعيش عليها هذه الشركات وخاصة التقنية منها لاستخدامها تلك البيانات في مجال الإعلانات عن طريق تحليلها وتحليل ميول ورغبات الأشخاص الطبيعيين، وتحديد اهتماماتهم وحاجاتهم وعاداتهم الاستهلاكية، وبذلك بدأت تلك الشركات بالتحرك بشكل واسع عندما أدركت حقيقة هذه البيانات بانها ذهب العصر الرقمي الحديث للقيام في جمع تلك البيانات، ومعالجتها، وإدارتها واستثمارها بالشكل الذي يحقق لها أرباحاً ويساعدها بالوصول إلى أسواق جديدة لخدماتها وسلعها الإنتاجية[٢٠٤]، مما شكل خطراً داهماً على الحق في خصوصية البيانات الشخصية التي تم معالجتها إلكترونياً، عبر الاستغلال غير المشروع لها في التسويق الإلكتروني الموجهة لذلك لزم تدخل المشرع بتجريم هذا

[٢٠٤] د. ميري كاظم عبيد، فلاح ساهي خلف، ماهية الاعتداء على البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي وتطبيقاتها العملية، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثالث/ السنة الثالثة عشر ٢٠٢١، ص٤٢٤.

(ISSN: 2537- 0758)

السلوك المشين حماية للأفراد لحقهم في خصوصية بياناتهم الشخصية، ودراءً لأي استغلال غير مشروع لها.

ثالثًا-محل الجريمة:

يتعلق النص التجريمي في تلك الجريمة بنوع محدد من التسويق وهو التسويق الإلكتروني، أي أن هذه المادة لا تمتد لتشمل أنواع أخرى من التسويق، فهي حصراً تتعلق بالتسويق الإلكتروني، ويشمل إرسال أي رسالة أو بيان أو محتوى إعلاني أو تسويقي بأي وسيلة تقنية أيا كانت طبيعتها، تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلى أشخاص بعينهم.

فمحل الجريمة هو عبارة عن رسائل التي تتم بوسيلة إلكترونية وتوجه إلى شخص أو إلى مجموعة من الأشخاص بدون تمييز وبغير طلب من جانبهم، بل وبدون موافقتهم[٢٠٥]، الأمر الذي يشكل انتهاكاً للحق في الخصوصية وعدواناً على البيانات الشخصية.

ويشترط في الإعلان التسويقي الإلكتروني بأن تكون الوسيلة المستخدمة في إرسال الرسائل التسويقية (تقنية) أما إن كانت الوسيلة غير ذلك فلا يعد تسويقاً إلكترونياً، فقد ترسل الرسالة التسويقية على الإيميل أو عبر وسائل الحسابات الخاصة على وسائل التواصل الاجتماعي، وقد حرصت العديد من الأنظمة القانونية المعنية بحماية البيانات ومن بينها المشرع المصري، على المواجهة الجنائية لتلك الجريمة عبر حماية الوسائل التي يمكن استخدامها في استقبال تلك الإعلانات التسويقية، كالبريد الإلكتروني، والمواقع والحسابات الخاصة بواسطة قانون حماية البيانات الشخصية، ومن قبله قانون مكافحة جرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨، فنص في المادة (١٨) من هذا القانون" 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

---

[٢٠٥] د. زينب غريب، النظام القانوني للبريد الإلكتروني، الطبعة الأولى، طوب بريس، الرباط، ٢٠١٦، ص٦٤، مشار إليها لدى د ياسر محمد اللمعي السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية، مرجع سابق، ص٢٨٠.

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".

وفي تلك الحالة نكون أمام سلوك مادي تتعدد أوصافه القانونية، فيعد في ذات الوقت منطوياً على جريمة (اختراق البريد الإلكتروني أو حساباً خاصاً) وفي تلك الحالة يتعين تطبيق العقوبة المنصوص عليها في المادة (١٨) من قانون مكافحة جرائم تقنية المعلومات، وليس العقوبة المنصوص عليها في المادة (٤٣) من قانون حماية البيانات الشخصية، إعمالاً لنص الفقرة الأولى من المادة (٣٢) من قانون العقوبات والتي جاء فيها(إذا كون الفعل الواحد جرائم متعددة وجب اعتبار الجريمة التي عقوبتها أشد والحكم بعقوبتها دون غيرها). ولما كانت عقوبة اختراق البريد الإلكتروني أو الحساب الخاص هي الأشد كونها معاقب عليها بالحبس أو الغرامة، في حين أن المشرع عاقب على مخالفة التسويق الإلكتروني في قانون حماية البيانات الشخصية بعقوبة الغرامة فقط.

رابعاً-صور السلوك الإجرامي للجريمة:

وحددت المادة (٤٣) من قانون حماية البيانات الشخصية المصري بأن يخضع للعقاب بموجبها من خالف أحكام المادتان (١٨، ١٧) من ذات القانون، وهاتان المادتان تتعلقان بمخالفة شروط التسويق الإلكتروني المباشر، ومخالفة المرسل لالتزامات التسويق الإلكتروني **وفيما يلي بيان ذلك:**

(أ) مخالفة شروط التسويق الإلكتروني:

حظرت المادة (١٧) من قانون حماية البيانات الشخصية المصري إجراء أي اتصال بهدف التسويق الإلكتروني المباشر للشخص المعني بالبيانات إلا بوجود مجموعة من الشروط وهي:

١- الحصول على موافقة الشخص المعني بالبيانات:

حظيت موافقة الشخص المعني بالبيانات الشخصية بدور بالغ الأهمية في قانون حماية البيانات الشخصية المصري، وجعل المشرع المصري من تلك الموافقة شرطاً أساسياً لتقنين التعامل فيها، فنصت المادة الثانية من القانون على أنه لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعنى بالبيانات..." فالمشرع في تلك المادة جعل موافقة الشخص المعني الأساس القانوني الوحيد لمشروعية معالجة البيانات الشخصية، وذلك

(ISSN: 2537- 0758)

فيما عدا الأحوال الأخرى المصرح بها قانوناً، ونصت المادة السادسة من ذات القانون بأن تكون المعالجة الإلكترونية مشروعة وقانونية في حال توفر موافقة الشخص المعنى بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر.

وفي فرنسا اشتراط المشرع الفرنسي نظام الرضاء المسبق الصريح لقبول هذا النوع من الإعلانات التسويقية الإلكترونية، وذلك من خلال نص المادة L121-20-5 من قانون حماية المستهلك، وكذلك المادة L34-5-1 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 عرفت ١١/٤من اللائحة الأوروبية لحماية البيانات الرضا بأنه "أي إشارة حرة محددة، مستنيرة لا لبس فيها، لرغبات الشخص المعني بالبيانات بواسطة تصريح أو فعل إيجابي، يعبر بها عن الموافقة على معالجة البيانات الشخصية المرتبطة به"

وقد وضع المشرع الفرنسي شروط يجب توافرها في الرضا المسبق حتى لا تقع الجريمة وهي على النحو التالي:

(أ) أن يكون هذا الرضا 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 عاماً.

(ج) يشترط أن يتم الرضا المسبق بناء على معلومات واضحة تقدم للشخص المستقبل للإعلانات أي أن يكون متبصراً[٢٠٦].

واشتراط القانون أن يُعطى ببيان لا لبس فيه بالموافقة، أو من خلال أداء عمل لا لبس فيه يؤكد إعطاء الموافقة، ويُستبعد الحصول على الموافقة بالصمت أو السلبية، أو بفعل ضمني لا يعبر بشكل لا لبس فيه عن الموافقة، حيث لابد من فعل نشط يمكن تفسيره على أنه موافقة دون أي شك، ويعد ذلك الأساس القانوني الصالح لمعالجة المعلومات الشخصية لأي فرد لأغراض التسويق، وستكون أنسب أساس قانوني هو الموافقة- ويمكنك الاعتماد على موافقة الفرد للتسويق لهم ويجب أن يكون هذا إجراءً إيجابيًا واضحًا لمعالجة البيانات بهذه الطريقة، ويجب أن تشرح للفرد البيانات الشخصية التي ستستخدمها، وكيف سيتم استخدامها، وأنه يمكنهم سحب الموافقة في أي وقت.

---

[٢٠٦] د ياسر محمد اللمعي، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية، مرجع سابق، ص٢٩٠، ٢٨٩.

ونصت المادة (٢٥) من نظام حماية البيانات الشخصية السعودي بأن "فيما عدا المواد التوعوية التي ترسلها الجهات العامة لا يجوز لجهة التحكم استخدام وسائل الاتصال الشخصية بما فيها العناوين البريدية والإلكترونية الخاصة بصاحب البيانات الشخصية لأجل إرسال مواد دعائية أو توعوية إلا وفقاً لما يأتي: ١- أن تؤخذ موافقة المتلقي المستهدف على إرسال هذه المواد إليه.

٢- أن يوفر مرسل المواد آلية واضحة- بحسب ما تحدده اللوائح- تمكن المتلقي المستهدف من إبداء رغبته في التوقف عن إرسالها إليه عند رغبته في ذلك، وتحدد اللوائح الأحكام المتعلقة بالمواد الدعائية والتوعوية المشار إليها في هذه المادة وشروط وأحوال موافقة المتلقي المستهدف على إرسال هذه المواد إليه".

وأجازت المادة (٢٦) من ذات النظام "فيما عدا البيانات الحساسة، تجوز معالجة البيانات الشخصية لأغراض تسويقية، إذا جرى جمعها من صاحبها مباشرة ووافق على ذلك وفق أحكام النظام. وتحدد اللوائح الضوابط اللازمة لذلك".

٢- أن يتضمن الاتصال هوية منشئه ومرسله:

تطلبت المادة (١٧) من قانون حماية البيانات الشخصية المصري ضرورة أن يتضمن الاتصال الذي يجرى لغرض التسويق الإلكتروني المباشر هوية الشخص المتصل والتعريف به، فلا يجوز أن يكون من يجرى الاتصال شخصاً مجاهلاً.

٣- أن يكون للمرسل عنوان صحيح وكاف للوصول إليه:

يتعين أن يكون للشخص المرسل عنوان ولا يكفي وجود عنوان، بل يشترط بأن يكون صحيح، ويمكن من خلاله الوصول إلى المرسل، ويعد هذا الأمر ضرورة منطقية تقضيها طبيعة عمل المرسل في التسويق الإلكتروني المباشر، ولزوم الوصول إليه إذا استدعت الحاجة ولن يتسنى حصول هذا الأمر دون الرجوع إلى عنوان صحيح يكفي للوصول إليه.

٤- الإشارة إلى أن الاتصال الإلكتروني بغرض التسويق المباشر:

ألزم القانون ضرورة أن يتضمن الاتصال الإلكتروني الإشارة إلى أنه بغرض التسويق المباشر، والا اتسمت عملية التسويق بعدم المشروعية، لفقدانها أحد الشروط التي استلزامها القانون لصحة التسويق الإلكتروني المباشر.

(ISSN: 2537- 0758)

٥- وضع آليات واضحة وميسرة لتمكين الشخص المعنى بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها:

جاء ضمن الشروط التي أوردها المشرع المصري لمشروعية التسويق الإلكتروني المباشر، ضرورة وجود آليات واضحة تمكن الشخص المعني بالبيانات الشخصية من رفض الاتصال الإلكتروني، بمعنى آخر ألا يكون المعنى بالبيانات مجبراً على الموافقة على تلقي الاتصال الإلكتروني وليس له خير الرفض، كما أن له العدول عن موافقته المسبقة، ويعد هذا الشرط نتيجة طبيعية لممارسة المعني بالبيانات حقوقه على بياناته في كافة الأنشطة ومنها التسويق الإلكتروني المباشر، ويعد ذلك تطبيقاً لما جاءت به حيثيات اللائحة الأوروبية في المادة (٧٠) عندما تتم معالجة البيانات الشخصية الأغراض التسويق المباشر، يجب أن يكون لصاحب البيانات الحق في الاعتراض على هذه المعالجة، بما في ذلك التنميط إلى الحد الذي يرتبط بمثل هذا التسويق المباشر. سواء فيما يتعلق بالمعالجة الأولية أو المعالجة الإضافية في أي وقت وبدون مقابل. وينبغي لفت انتباه موضوع البيانات صراحة إلى هذا الحق وتقديمه بوضوح وبشكل منفصل عن أي معلومات أخرى.

وقد تناولت اللائحة الأوروبية لحماية البيانات في الفقرة (٣، ٢) من المادة (٢١) من اللائحة بعض الضوابط المتعلقة باستخدام البيانات الشخصية في عملية التسويق الإلكتروني (عند معالجة البيانات الشخصية لأغراض تسويقية مباشرة، يحق لصاحب البيانات الاعتراض في أي وقت على معالجة البيانات الشخصية المتعلقة به أو بها من أجل هذا التسويق، بما في ذلك التنميط[٢٠٧] إلى الحد الذي يكون مرتبطا به بشكل مباشر تسويق، عندما تخضع البيانات للمعالجة الأغراض التسويق المباشر لن تتم معالجة البيانات الشخصية بعد الآن لهذه الأغراض.

[٢٠٧] عرفته المادة الرابعة من اللائحة الأوروبية لحماية البيانات بأنه "يعني أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتكون من استخدام البيانات الشخصية لتقييم بعض الجوانب الشخصية. المتعلقة بشخص طبيعي، ولا سيما لتحليل أو توقع الجوانب المتعلقة بأداء ذلك الشخص الطبيعي في العمل والوضع الاقتصادي أو الصحة أو التفضيلات الشخصية أو الاهتمامات أو الموثوقية أو السلوك أو الموقع أو الحركات".

(ب) مخالفة المرسل لالتزامات التسويق الإلكتروني:

نصت المادة (١٨) من القانون على مجموعة من الالتزامات التي ألقتها على عاتق المرسل لأي اتصال إلكتروني بغرض التسويق المباشر.

١- الالتزام بالغرض التسويقي المحدد:

ينبغي على المرسل أن يلتزم بالغرض التسويقي المحدد، الحاصل على الموافقة بشأن القيام به، ويكون في مجاوزة المرسل للغرض بالتطرق لأي موضوعات أخرى من شأنها الانحراف عن الغرض التسويقي المحدد مخالفة لنص المادة (١٨) من القانون وتستحق العقاب.

٢- عدم الإفصاح عن بيانات الاتصال للشخص المعنى بالبيانات:

ألزمت المادة (١٨) المرسل بعدم الإفصاح عن بيانات الاتصال للشخص المعني بالبيانات، وبالتالي فإن في الإفصاح عن تلك البيانات انتهاك للالتزام المفروض على المرسل بموجب تلك المادة.

٣- الاحتفاظ بسجلات إلكترونية بها موافقة الشخص المعنى بالبيانات وتعديلاتها، أو عدم اعتراضه على استمراره بشأن تلقي الاتصال الإلكتروني التسويقي المدة القانونية:

أوردت المادة (١٨) من القانون التزاماً على المرسل غاية في الأهمية لتقنين عملة التسويق الإلكتروني المباشر، يتلخص حول التزامه بإعداد سجلات إلكترونية يدرج بها موافقة الشخص المعني بالبيانات على عملية التسويق، وأي تعديلات تطرأ على تلك الموافقة الصادرة منه، أو عدم اعتراضه على تلقي الاتصال الإلكتروني التسويقي، وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال، ويعد هذا الالتزام على عاتق المرسل امتداداً طبيعياً للشروط التي أوجبها المشرع لمشروعية التسويق الإلكتروني المباشر التي تتمحور في ضرورة موافقة الشخص المعني بالبيانات ووضع آليات واضحة وميسرة لتمكين الشخص المعنى بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها وهذا الأمر لن يتسنى تحقيقه إلا بالاحتفاظ بسجلات إلكترونية معدة خصيصاً لذلك. وأحال القانون إلى اللائحة التنفيذية له تحديد القواعد والشروط والضوابط المتعلقة بالتسويق الإلكتروني المباشر.

(ISSN: 2537- 0758)

خامساً-العقوبة:

نص المشرع الفرنسي في المادة ٤ من قانون معالجة البيانات والملفات والحريات على أنه يحظر جمع أو معالجة البيانات ذات الطابع الشخصي، والتي من شأنها أن تكشف، بشكل مباشر أو غير مباشر، عن الأصول العرقية أو الآراء السياسية أو الفلسفة أو العقيدة الدينية أو الانتماء النقابي للشخص، أو تلك التي تتعلق بصحته أو بحياته الجنسية.

ويستخلص من ذلك 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 ١٠٠ألف 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 الفيس بوك أو التوتير أو الانستجرام وغيرها بجمع وحفظ البيانات الشخصية للمستخدم، أو أن يتم إعاقة أو إفساد عمل لنظام للمعالجة الآلية للبيانات الشخصية، من أجل استخدامه في أغراض الإعلانات التسويقية الموجهة عبر الإنترنت[٢٠٨].

[٢٠٨] د. ياسر محمد اللمعي، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية، ص٢٨٨، ٢٨٧.

وقررت المادة السادسة والثلاثون من نظام حماية البيانات الشخصية السعودي بأنه" فيما لم يرد في شأنه نص خاص في المادة (الخامسة والثلاثين) من النظام، ودون إخلال بأي عقوبة أشد منصوص عليها في نظام آخر؛ تعاقب بالإنذار أو بغرامة لا تزيد على (خمسة ملايين ريال، كل شخصية ذات صفة طبيعية أو اعتبارية خاصة مشمولة بأحكام النظام خالفت أياً من أحكام النظام أو اللوائح. وتجوز مضاعفة عقوبة الغرامة في حالة تكرار المخالفة حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد" وبما أن جريمة التسويق الإلكتروني الموجهة ليست من ضمن الجرائم التي تضمنت المادة (٣٥) العقاب عليها فإنها تخضع للعقاب المنصوص عليه بالمادة (٣٦).

ونصت المادة (٢٣) من قانون حماية خصوصية البيانات الشخصية القطري بأن (مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر، يعاقب بالغرامة التي لا تزيد على (١,٠٠٠,٠٠٠) مليون ريال، كل من خالف أياً من أحكام المواد (٤)، (٨)، (٩)، (١٠)، (١١)، (١٢)، (١٤)، (١٥)، (٢٢) من هذا القانون) وحيث إن المادة (٢٢) قد تضمنت الضوابط المنظمة لعملية التسويق الإلكتروني وبالتالي فإن مخالفة أياً من أحكامها فيعاقب الجاني بالغرامة التي تصل في حدها الأقصى مليون ريال قطري.

وعاقب المشرع المصري بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، كل من خالف أحكام التسويق الإلكتروني المنصوص عليها في المادتين (١٧) (١٨) من هذا القانون.

والملاحظ أن التشريعات العربية السعودي، والقطري، والمصري اتفقت على معاقبة مخالفة أحكام التسويق الإلكتروني بعقوبة الغرامة، غير أن ما يميز المشرع المصري في تلك العقوبة هو أن جعل لها حد أدني لا يجاوز أن تقل عنه وهو يتسم بالجسامة النسبية، بالمقارنة بنظيريه السعودي والقطري اللذان جعل العقوبة بدون حد أدنى، تاركاً مساحة كبيرة للقاضي في إنزال العقوبة بما قد يؤدى إلى أحكام ضئيلة بشكل قد يجعل العقوبة غير رادعة بما يفضي لتكرار الجريمة.

(ISSN: 2537- 0758)

الخاتمة

تمثل البيانات الشخصية أحد أهم مرتكزات الخصوصية بالنسبة لعموم البشر، ودائما ما يحرص الأشخاص على إحاطتها بسياج من الأمان من تطفل الغير عليها، لذا كان تدخل التشريعات لتحقيق مواجهة جنائية فاعلة للاعتداء على البيانات الشخصية ضرورة حتمية، واستناداً لما سبق توصلت لمجموعة من النتائج والتوصيات أوجزها فيما يلي:

أولاً- النتائج: توصلت الدراسة إلى جملة من النتائج على النحو التالي:

١- عدم اتفاق التشريعات المقارنة محل الدراسة على تسمية مواحدة للقوانين المتعلقة بالبيانات الشخصية، فمنها ما أطلق عليها مسمي (البيانات الشخصية كالمشرع المصري والمنظم السعودي، ومنها ما قامت بتسميتها بحماية البيانات ذات الطابع الشخصي كالمشرع اللبناني، ومنها ما عرفها بالمعطيات ذات الطابع الشخصي كالمشرع المغربي) وجميع هذه التسميات مترادفات لمعنى واحد، يشمل حق الفرد بالتحكم في بياناته والمعلومات التي تخصه وتتعلق به.

٢- اتسم تعريف المشرع المصري للبيانات الشخصية بعدم الدقة في الصياغة من حيث استخدام مصطلح (الربط) بين هذه البيانات أو أي بيانات أخرى كالاسم، في حين أن اللائحة الأوروبية لحماية البيانات استخدمت مصطلح (بالإشارة)؛ لأن مصطلح الربط يفهم منه أنه لابد من ارتباط بيانين معًا، لكي يصبح البيان شخصي بالمعنى الذي يقصده ويحميه القانون، بينما استخدام لفظ "بالإشارة" يوسع من نطاق الشخصية التي قد يشملها القانون بحمايته، بجعلها قائمة بذاتها كبيان شخصي دون الحاجة إلى ربطها ببيان آخر.

٣- قصور المشرع المصري في شموله الحماية القانونية للبيانات الشخصية على المعالجة إلكترونياً دون غيرها من البيانات المعالجة يدوياً، أو محفوظة بشكل غير إلكتروني، كونها تنطوي على تميز غير مبرر بين أنواع البيانات لا يستند إلى واقع أو مسوغ قانوني.

٤- اقتصار القانون المصري في حماية للبيانات الشخصية على الأشخاص الطبيعيين دون الأشخاص الاعتبارية، على الرغم من الأهمية التي تشكلها الأخيرة في الحياة العامة عموماً والاقتصادية خصوصاً.

٥- تضمن القانون المصري حماية البيانات الشخصية للمعنيين بها على قيد الحياة، ولم يشمل بيانات المتوفين ضمن البيانات المشمولة بالحماية على عكس المنظم السعودي بالرغم من أنها قد تؤدي إلى معرفته أو أحد أفراد أسرته على وجه التحديد.

٦- أغفل المشرع المصري وضع تعريفاً لبعض البيانات الشخصية الحساسة كالبيانات البيومترية والبيانات المالية والبيانات الجينية، وكان يتعين إيضاحها بشكل جلي، لإزالة أي غموض يكتنف مفهومها.

٧- أورد القانون المصري حالات تتسم فيها معالجة البيانات بالمشروعية أولاهما موافقة الشخص المعني بالبيانات، وثانيهما أن يصرح القانون بذلك، غير أنه لم يبين كنة هذه الحالات أو تفصيلاتها على نحو دقيق بما قد يسمح بالاستطالة على البيانات الشخصية تحت ذريعة أن القانون صرح بذلك.

٨- تباينت المعاملة العقابية للمشرع المصري لجرائم معالجة البيانات والاستغلال غير المشروع لها، من جريمة لأخرى بحسب جسامتها، ونتيجتها والأضرار الناجمة عنها للمعني بالبيانات، إلا أنه بمقارنة العقوبات المقررة على تلك الجرائم، مع نظيره الفرنسي يظهر هزالة العقوبات المقررة في القانون المصري والنظام السعودي، بما يستدعي إعادة النظر فيها بالتشديد لجسامة تلك الجرائم.

٩- تضمن القانون المصري مجموعة من الحقوق للمعنى بالبيانات، تشهد بسلطته على بيانته الشخصية، إلا أن ذات القانون تضمن في بعض موضعه نصوصاً تجعل من تلك الحقوق عديمة القيمة، كالسماح للمتحكم أو المعالج بنقل البيانات الشخصية عبر الحدود خارج الدولة، دون موافقة المعني بها ودون علمه، عند التصريح من مركز حماية البيانات الشخصية.

١٠- قصور القانون في عدم وضع إطار عام للتعامل مع البيانات الشخصية للأغراض التجارية وقصرها على التسويق الإلكتروني المباشر.

١١- عدم صدور لائحة تنفيذية لقانون حماية البيانات الشخصية المصري حتى تاريخ الانتهاء من الدراسة، مما يعد أكبر عقبات تفعيل حمايتها، لاسيما وأن القانون في عديد من مواضعه أحال إلى اللائحة التنفيذية وضع الضوابط والشروط التي تتعلق بحماية البيانات.

(ISSN: 2537- 0758)

١٢- عدم إنشاء مركز حماية البيانات الشخصية المصري، تعد من أبرز معوقات وجود حماية فاعلة للبيانات الشخصية في القانون المصري، فقد خول له القانون عديد من الصلاحيات التي بموجبها يساهم بشكل إيجابي وفاعل في حماية البيانات، وفي ظل عدم وجوده وإنشائه تغدو تلك الصلاحيات والاختصاصات مفرغة من معانيها.

ثانياً-التوصيات:

من خلال استعراض هذه الدراسة ونتائجها على النحو السابق إيضاحه خلصت إلى عدة توصيات بهدف تدعيم المواجهة الجنائية للمعالجة والاستغلال غير المشروع للبيانات الشخصية، لذلك يقترح الباحث ما يلي:

١- إجراء تعديل تشريعي على قانون حماية البيانات الشخصية، يسمح بمد مظلة الحماية الجنائية لكافة البيانات الشخصية، سواء المكتوبة أو المحفوظة بشكل غير إلكتروني أو المعالجة إلكترونياً.

٢- أقترح على المشرع المصري شمول بيانات المتوفي الشخصية بالحماية شأنه في ذلك شأن المنظم السعودي؛ لأنه من خلالها يمكن الوصول إلى معرفة الشخص المعني بالبيانات على وجه التحديد أو معرفة أحد أفراد أسرته.

٣- كما أقترح على المشرع تضمن قانون حماية البيانات الشخصية المصري، حماية بيانات الأشخاص الاعتبارية العامة أو الخاصة؛ لخطورة المساس بالبيانات الخاصة بهم وإمكانية استغلالها للإضرار بهم.

٤- إجراء تعديل تشريعي يتضمن تعديل صياغة تعريف البيانات الشخصية باستبدال (عن طريق الربط بين هذه البيانات) إلى (بالإشارة لهذه البيانات) لتوسيع من نطاق الشخصية التي قد يشملها القانون بالحماية.

٥- إضافة تعاريف للبيانات التي أغفل القانون تعريفها وأوردها كأمثلة للبيانات الحساسة كالبيانات البيومترية، والبيانات المالية والبيانات الجينية وغيرها من البيانات، مما جرى ذكرها كبيانات حساسة أو الإحالة إلى اللائحة التنفيذية للقانون لتتكفل بذلك.

٦- يجدر بالمشرع المصري أن يحدد على وجه الدقة الحالات المصرح بها قانوناً، التي تشمل معالجة البيانات الشخصية للشخص المعني دون موافقته، لكنها تظل مشروعة

رغم ذلك كونها مصرح بها قانوناً، حتى لا يتم التوسع في إعمال النص دون ضوابط تضمن عدم الإخلال به.

٧- يتعين على المشرع المصري إدراج شرط ألا يترتب على نقل البيانات الشخصية عبر الحدود أو الإفصاح عنها المساس بالأمن الوطني للبلاد، أو بمصالحها الحيوية، لما في ذلك من تغليب للمصالح العليا للبلاد على المصالح الخاصة على غرار المنظم السعودي لما في ذلك من إعلاء للمصلحة العامة للدولة.

٨- أناشد المشرع المصري بضرورة تعديل تشريعي لنص المادة السادسة عشر من قانون حماية البيانات الشخصية المصري، بإضافة ضرورة حصول المتحكم أو المعالج على (الموافقة الصريحة للمعني بالبيانات)، بالإضافة إلى تصريح مركز حماية البيانات الشخصية لنقل البيانات الشخصية لمتحكم آخر خارج مصر.

٩- إجراء تعديل تشريعي يسمح بوضع إطار عام للتعامل مع البيانات الشخصية للأغراض التجارية وعدم قصرها على التسويق الإلكتروني المباشر؛ لضمان عدم التعارض بين النصوص القانونية المنظمة لاستغلال البيانات الشخصية لأغراض تجارية.

١٠- ضرورة تشديد المشرع المصري العقاب على جرائم الاعتداء على البيانات الشخصية، بما يتناسب مع جسامتها، بأن تكون العقوبة الحبس الوجوبي في بعض الجرائم كالمعالجة غير المشروعة للبيانات الحساسة ومخالفة شروط وضوابط نقل البيانات الشخصية عبر الحدود للخطورة البالغة التي تشكلها تلك الجرائم.

١١- ضرورة الإسراع في إصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري، وإنشاء مركز حمايتها المنصوص عليه قانوناً لتفعيل حماية حقيقة للبيانات الشخصية.

(ISSN: 2537- 0758)

المصادر والمراجع

أولاً- كتب في الحديث وعامة:

١- صحيح البخاري، عبد الله محمد بن إسماعيل بن إبراهيم بن المغيرة البخاري، كتاب الأدب، باب يا أيها الذين آمنوا اجتنبوا كثيراً من الظن، الطبعة الأميرية، القاهرة، ١٣١١هـ، ج٨.

٢- أ/ عبد الله على الشنبري، التحولات المعرفية الكبرى من العصر الحجري وحتى جوجل، مدارك للنشر ٢٠١١.

٣- ريموند واكس، الخصوصية مقدمة قصيرة جدا، ترجمة ياسر حسن، الناشر مؤسسة هنداوي، ٢٠١٣.

ثانياً- المؤلفات القانونية العامة:

١- د. أحمد فتحي سرور، الوسيط في قانون العقوبات- القسم العام، الطبعة السادسة، طبعة خاصة لنادي القضاة، ٢٠١٥.

٢- د. حسن كيرة، المدخل إلى القانون، القسم الثاني- النظرية العامة للحق، مكتبة مكاوي، ١٩٧٧.

٣- حسنين عبيد، شرح قانون العقوبات- القسم الخاص، جرائم الاعتداء على الأشخاص والأموال، الطبعة التاسعة، دار النهضة العربية.

٤- د. فتوح عبد الله الشاذلي، شرح قانون العقوبات- القسم العام، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٨.

٥- د. فوزية عبد الستار، شرح قانون مكافحة المخدرات، دار النهضة العربية، القاهرة، ١٩٩٠.

٦- د. محمد عبد اللطيف عبد العال الجرائم المادية وطبيعة المسؤولية الناشئة عنها- دار النهضة العربية- القاهرة- ١٩٩٧.

٧- د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، ٢٠٠٦.

٨- د. محمود نجيب حسني، علاقة السببية في قانون العقوبات، طبعة نادي القضاة، ١٩٨٤، بدون رقم طبعة.

٩- د. هلالي عبد اللاه أحمد، الوجيز في شرح قانون العقوبات-القسم العام، ٢٠١٩، بدون دار نشر.

ثالثاً- المؤلفات القانونية الخاصة:

١- د. أحمد خليفة الملط الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الإسكندرية، ٢٠٠٦.

٢- د. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، ١٩٨٨.
٣- د. خالد حسن أحمد، الحق في خصوصية البيانات الشخصية بين الحماية القانونية التحديات التقنية-دراسة مقارنة، دار الكتب والدراسات العربية، القاهرة، ٢٠٢٠.
٤- د. رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) مقارناً بالتشريعات المقارنة والمواثيق الدولية، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، ١٤٤١هـ-٢٠٢٠م.
٥- د. على احمد عبد الزغبي، حق الخصوصية في القانون الجنائي دراسة مقارنة، المؤسسة الحديثة للكتاب، لبنان، ٢٠٠٦، ص٣٣٣-٣٣٧.
٦- د. عمرو احمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠.
٧- د. محمد جبريل إبراهيم، التحول الرقمي في منظور القانون الجنائي- دراسة تحليلية تأصيلية، الطبعة الأولى، دار النهضة العربية، القاهرة، رقم الإيداع ٢٠٢٣/١٤٦٨٢، تاريخ النشر ٢٠٢٣.
٨- د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٩.
٩- د. محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة استخدام الحاسب الآلي دراسة تحليلية مقارنة للحق في الخصوصية وتطبيقاته في القانون الكويتي، مطبوعات جامعة الكويت، بدون رقم طبعة وتاريخ نشر.
١٠- د. محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠١٦.
١١- د. محمود أحمد طه، التعدي على حق سرية الاتصالات الشخصية بين التجريم والمشروعية، دار النهضة العربية، القاهرة، ١٩٩٣.
١٢- د. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت دراسة مقارنة، الطبعة الأولى، دار الفكر والقانون، المنصورة، ٢٠١٣.
١٣- د. منى الأشقر جبور، د. محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، الطبعة الأولى، المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان، ٢٠١٨.
١٤- د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢.

(ISSN: 2537- 0758)

١٥- د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢.

رابعاً- دوريات علمية ومؤتمرات:

١- أ. أحمد سامر مقرش، د. خالد الخطيب، الالتزام بالإخطار في معالجة البيانات الشخصية، مجلة بحوث جامعة حلب- سلسلة العلوم القانونية والشرعية، العدد ١٦ لعام ٢٠١٨.

٢- د. أشرف جابر، استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصية، مجلة العلوم الإنسانية، جامعة الأخوة منتوري- قسنطينة، الجزائر، عدد خاص ٢٠١٥.

٣- د. ايمن مصطفى احمد، الحماية القانونية للبيانات الشخصية في إطار أنشطة البحث العلمي، مجلة الدراسات القانونية تصدرها كلية حقوق أسيوط، العدد ٣٧ الجزء الأول، ٢٠١٥.

٤- د. خدوجة الدهبي، حق الخصوصية في مواجهة الاعتداءات الإلكترونية- دراسة مقارنة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف بالمسيلة- الجزائر، العدد الثامن، ديسمبر ٢٠١٧، المجلد الأول.

٥- دراسة نقدية لقانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، مركز بحوث القانون والتكنولوجيا، ورشة العمل بكلية القانون بالجامعة البريطانية في مصر، المنعقدة يوم الاثنين الموافق ١٢ أكتوبر ٢٠٢٠.

٦- د. دعاء حامد محمد عبد الرحمن، الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي، قراءة في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، مقدم إلى المؤتمر العلمي الأول لكلية الحقوق جامعة مدينة السادات، المقام في الفترة من ٣٠-٣١ يوليو ٢٠٢٢، والمنشور بعدد خاص بالمؤتمر.

٧- د. رشيدة بوكر، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، العدد الثاني، ٢٠٢٢م، المجلد٧.

٨- د. سليم محمد سليم حسين، الحماية الجنائية للبيانات المعالجة آلياً دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق- جامعة عين شمس، العدد الأول يناير ٢٠٢٠، المجلد ٦٢.

٩- د. سوز حميد مجيد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، دراسة تحليلية مقارنة، دراسات قانونية وسياسية، السنة السادسة، العدد (١١) نيسان- ابريل٢٠١٨.

١٠- د. شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية (دراسة تحليلية لحق الاطلاع على البيانات في فرنسا)، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد ٥٧، إبريل ٢٠١٥.
١١- د. صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل في الاقتصاد والإدارة والقانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار- عنابة- الجزائر المجلد ٢٤- العدد٢، أوت ٢٠١٨.
١٢- د. عائشة مصطفى بن قارة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون، المغرب، العدد الثاني والأربعون، أبريل ٢٠١٦.
١٣- أ. عبد الرحمن جمال يعقوب، قراءة في حكم محكمة العدل الأوروبية في قضية شريمز ٢بشأن نقل البيانات الشخصية من الاتحاد الأوروبي إلى الولايات المتحدة الأمريكية، مجلة القانون والتكنولوجيا، كلية القانون الجامعة البريطانية، القاهرة، المجلد الثالث، العدد الأول، إبريل٢٠٢٣.
١٤- د. على احمد عبد الزغبي، حق الخصوصية في القانون الجنائي دراسة مقارنة، المؤسسة الحديثة للكتاب، لبنان، ٢٠٠٦، ص٣٣٣-٣٣٧.
١٥- د. علي كريمي تأثير التطور التكنولوجي على حقوق الإنسان الحياة الخصوصية وحماية البيانات الشخصية "نموذجا"، مجلة أبحاث احتجاج بالمغرب، مقاربة الإنسان السلوكيات والقيم العدد ٦١ ٦٢ لسنة ٢٠١٥.
١٦- د. محمود زكي زكي زيدان، الحماية الجنائية الموضوعية للحق في النسيان الرقمي "دراسة مقارنة"، مجلة روح القوانين- العدد المائة وواحد- إصدار يناير ٢٠٢٣-الجزء الأول.
١٧- د. منى تركي الموسوي، أ/ جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، عدد خاص بمؤتمر الكلية ٢٠١٣.
١٨- كاظم عبيد، فلاح ساهي خلف، ماهية الاعتداء على البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي وتطبيقاتها العملية، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثالث/ السنة الثالثة عشر ٢٠٢١،.
١٩- د. هشام مسعودي، حماية وتعزيز الحق في الخصوصية في العصر الرقمي قراءة في تقرير مفوضية الأمم المتحدة لحقوق الإنسان في دورته ٢٨، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، العدد ١ أبريل ٢٠٢٢، المجلد ٩.

(ISSN: 2537- 0758)

٢٠- د. هيثم السيد أحمد عيسى، التشخيص الرقمي لحالة الإنسان في عصر التنقيب في البيانات عبر تقنيات الذكاء الاصطناعي وفقاً للائحة الأوروبية العامة لحماية البيانات لعام ٢٠١٦م، دار النهضة العربية، القاهرة، ٢٠١٩.
٢١- د. ياسر محمد اللمعي، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية- دراسة تحليلية مقارنة، مجلة روح القوانين، كلية الحقوق- جامعة طنطا- العدد السابع والتسعون- يناير ٢٠٢٢.
٢٢- د. ياسر محمد اللمعي، المواجهة الجنائية للممارسات الإعلانية والدعاية التسويقية الإلكترونية غير المشروعة للسلع والخدمات، دراسة تحليلية مقارنة، مجلة روح القوانين، كلية الحقوق جامعة طنطا، العدد ١٠١، يناير ٢٠٢٣، الجزء الأول.

خامساً- الرسائل العلمية:

(أ) رسائل الماجستير

١- أ. أسمهان جبير، دور التسويق الإلكتروني في تحسين الصورة الذهنية للمؤسسة الخدماتية دراسة ميدانية على عينة من زبائن وكالة موبيليس لأم البواقي، رسالة ماجستير، كلية العلوم الإنسانية والاجتماعية، جامعة العربي بن مهيدي أم البواقي، الجزائر، ٢٠١٨/.٢٠١٩
٢- أ. أشراف البكوش، حماية الحياة الخاصة في القانون الجنائي، رسالة ماجستير كلية الحقوق والعلوم الاقتصادية والسياسية، سوسة- تونس، العام الجامعي ٢٠٠٦/.٢٠٠٧
٣- أ. ليديا رشام، الحماية الجنائية للمعطيات الشخصية دراسة مقارنة، رسالة لنيل شهادة الماجستير، جامعة البويرة، الجزائر، .٢٠١٩
٤- أ. يونس خالد عرب، جرائم الحاسوب (دراسة مقارنة)، رسالة ماجستير، الجامعة الأردنية، ١٩٩٤.

(ب) رسائل الدكتوراه

١- د. رنا أبو المعاطي محمد الدكروري، الحماية الجنائية للبيانات الشخصية، رسالة دكتوراه- كلية الحقوق جامعة المنصورة، ٢٠٢٢م.
٢- د. مروة زين العابدين سعد صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، رسالة دكتوراه، كلية الحقوق- جامعة عين شمس، ٢٠١٤.

سادساً- الموسوعات والأحكام القضائية:

١- الموسوعة الذهبية للقضاء الدستوري المصري، ١٩٦٩- ٢٠١٩، المجلد الأول. المحكمة الدستورية العليا، القاهرة.

٢- نقض جنائي مصري، مجموعة أحكام محكمة النقض، الطعن رقم ٥٥١٥ لسنة ٦٦، جلسة ١٤ أبريل ٢٠٠٣، س ٥٤، ق ٦٥.
٣- الدعوى رقم ٢٣ لسنة ١٦ قضائية "دستورية" بجلسة ١٩٩٥/٣/١٨ جـ ٦ "دستورية".

سابعاً- مصادر من الإنترنت:

١- التقرير الصادر عن اللجنة القومية للمعلوماتية والحريات الفرنسية CNIL بشأن التسويق الإلكتروني بجلسة ٥ فبراير ٢٠٠٩ منشور علي http://www.audentia-gestion.fr/CNIL/Publicite_Ciblee_rapport_VD.pdf
٢- القواعد العامة لنقل البيانات الشخصية خارج الجغرافية للمملكة، النسخة الأولى الصادرة في ٢٠٢٠/١١/٢٥، المملكة العربية السعودية منشورة على موقع https://sdaia.gov.sa/ndmo/Files/Policies003.pdf
٣- فيسبوك يستخدم أرقام هواتف المستخدمين لتوجيه الإعلانات التجارية، مونت كارلو الدولية بتاريخ ٢٠١٨/٩/٢٨م، منشور على موقع https://www.mc-doualiya.com/articles/20180928-
٤- يونس عرب، المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، منشور على شبكة المعلومات الدولية– الإنترنت، https://kenanaonline.com/users/ahmedkordy/posts/323471

المصادر باللغة الأجنبية:References in English

1. ALEXANDRE SOARES DE OLIVEIRA LUCENA E VALE, A Race for Maintaining Personal Data A Work Project, presented as part of the requirements for the Award of a Master Degree in Management from the NOVA– School of Business and Economics, January 3rd 2018.
2. Anne Bliss, Ph.D., TECHNOLOGY AND PRIVACY IN THE NEW MILLENNIUM, Ethica Publishing,2004.
3. Bird & Bird LLP- Katarína Ondrovičová, Robert Čuperka and Filip Vlnečka, Direct Marketing and unsolicited communications, European Union, Slovakia April 19 2022 https://www-lexology-com.translate.goog/library/detail.aspx?g=571f28ec-9df0-40f0-8f7b-80defb1614e9&_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=sc.
4. Daniel T. Rockey Requesting at Point of Sale Subject to Statutory Penalties, Counsel, Bullivant Houser Bailey PC 2011.

(ISSN: 2537- 0758)

5. Elinor Mills, Ads--the new malware delivery format, Sept. 15, 2009, https://www-cnet-com.translate.goog/news/privacy/ads-the-new-malware-delivery-format/?_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=sc
6. F. Paul Pittman ،Kyle Levenberg, Shira Shamir, Data Protection Laws and Regulations USA 2022-2023, iclg, Published: 08/07/2022.
7. Guido Noto La Diega, "Data as digital assets: The case of targeted advertising, in Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?, eds, Gintarė Surblytė-Namavičienė, et al. (Berlin, Germany: Springer, 2018).
8. Hamed Taherdoost, Neda Jalaliyoon, Marketing vs E-Marketing, International Journal of Academic Research in Management (IJARM), Vol. 3, No. 4, 2014, © Helvetic Editions LTD, Switzerland.
9. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.https://www.w.aterfordtechnologies.com/big-data-interesting-facts/
10. Ida Madicha Azmi, E-Commerce and Privacy Innes An Analysis of the Personal Data Protection Hill, International, Review of Law, Computers & Technology, 2015.
11. Narayanan. A.: Shmatikov. V. (2009). "De-anonymizing Social Networks". 2009 30th IEEE Symposium on Security and Privacy.
12. ONLINE ADVERTISING AND HIDDEN HAZARDS TO CONSUMER SECURITY, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS UNITED STATES SENATE, RELEASED IN CONJUNCTION WITH THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS' MAY 15, 2014 HEARING,p26. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/REPORT%20-%20Online%20Advertising%20&%20Hidden%20Hazards%20to%20Consumer%20Security%20&%20Date%20Privacy%20(May%2015%202014)2.pdf
13. Références en français
14. Benoit TABAKA et Yann TESAR, Loi «informatique et liberés»: un nouveau cadre juridique pour le traitement des données à caractère personnel, Dossier disponiblesur:www.foruminternet.org. la date de mise en ligneest: Octobre 2004.

15. Déloyauté du recueil d'adresses électroniques sur Internet par l'utilisation d'un logiciel– Cour de cassation, crimenelle. 14 mars 2006– AJ pénal 2006.
16. Etienne Quillet: Le droit à l'oubli numérique sur les réseaux sociaux. Master de droits de l'homme et droit humanitaire. Université panteon- Asas. 2011.
17. Ibrahim COULIBALY, La protection des données à caractère personnel dans le domaine de la recherche scientifique thèse pour obtenir le grade de docteur, spécialité: droit prive. Université de Grenoble, 25 novembre 2011.
18. Imane Majdoub, La protection pénale des données à caractère personnel à l'ère numérique, Article ·revue des affaires penales et de la gouvernance sécuritaire, July 2022.
19. Ives BISMUTH, Droit de l'informatique, éléments de droit à l'usage des informaticiens, édition L'harmattan, Paris, 2011.
20. JACQUELINE. POUSSON-PETIT, Le droit à l'anonymat in Mélanges dédies à louis Boyer: Presse Universitaire de Toulouse, 1996
21. Jean PRADEL, Michel DANTI-JUAN, Manuel de droit pénal spécial, 3e éd CUJAS, Paris, 2004, p234.
22. Julien LE CLAINCHE: La protection des données personnelles nominatives dans le cadre de la recherche dans le domaine de la santé, Comparaison du droit français et du droit américain, Mémoire de D.E.A., Faculté de droit, des Sciences Economiques et de Gestion, Université Montpellier I 2000-2001.
23. Patrice GATTEGNO, Droit pénal spécial, Dalloz, 1995.
24. PUTZ J.L., *Cybercriminalité ; Criminalité informatique en droit luxembourgeoiS,* Éditions Larcier, Lefebvre Sarrut Belgium, Luxembourg, *2019.*
25. SIMON CAQUÉ, Le régime juridique des données publiques numériques, Thèse de doctorat de droit, spécialité droit public, Institut du droit public et de la science politique, UNIVERSITÉ DE RENNES 1, 2020.
26. Sophie PENA PORTA, les données à caractère personnel; les données nominatives, Art disponible sur www.pedagogie.ac-aix-marseille.fr, la date de mise en ligne est: 2/3/2005.
27. Torkia HOUNKI, LA PROTECTION CIVILE ET PENALE DU CONSOMMATEUR DANS LE COMMERCE ELECTRONIQUE: Étude comparée entre le droit français, le droit égyptien et le droit

(ISSN: 2537- 0758)

libyen, UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE, Le 29 mars 2021.

28. V. CNIL, Délibération n° 85-050 du 22 oct. 1985 portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, JO 17 nov 1985. sans page.

Des décisions judiciaires françaises:

1- Claudine Guerrier, Protection des données personnelles et applications biométriques en Europe, Communication commerce électronique, 1 juillet 2003, n7.
2- Cour de Cassation, Chambre criminelle, du 4 mars 1997, 96-84.773, Publié au bulletin.
3- CA Paris 27 avril 2007: Paris 15 mai 2007: http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-d-appel-de-paris-13e-chambresection-a-15- mai-2007.html
4- Cour de cassation, criminelle, Chambre criminelle, 8 juillet 2015, 13-86.267, Publié au bulletin
5- Cass. civ. 1ere, 3 nov. 2016, n15-22.695, publié au Bulletin; AJDA 2017. 23; D. 2016. 2285; Dalloz IP/IT 2017. 120, obs. G. Péronne et E. Daoud
6- Cour de cassation, criminelle, Chambre criminelle, 23 mai 2018, 16-84.096, In edit.
7- Cour de cassation, criminelle, Chambre criminelle, 13 décembre 2022, 22-81.851, Publié au bulletin.
8- Cour de cassation, crimenelle. 14 mars 2006– AJ pénal 2006.
9- Cass. Crim. 4 avril 2007 disponible sur http://www.legalis.net/jurisprudence- decision php3? id article 1959.
10- Cass. civ. 1ere, 3 nov. 2016, n15-22.695, publié au Bulletin; AJDA 2017. 23; D. 2016. 2285; Dalloz IP/IT 2017.120, obs. G. Péronne et E. Daoud.
11- TGI paris, 17 èmech, 7 décembre 2004, et disponible sur www.droit-tic.com.