بحث بعنوان

الحماية الدولية للبيانات الشخصية الرقمية
دراسة في ضوء أحكام الاتفاقيات والمحاكم الدولية

مقدم إلى

كلية الحقوق - جامعة المنيا

قسم القانون الدولي العام

أ.د/ حسن سعد محمد عيسي سند

أستاذ القانون الدولي العام

عميد كلية الحقوق - جامعة المنيا

الباحث/ مصطفى كمال احمد

ماجستير في القانون الدولي العام

المستخلص:

نصت غالبية التشريعات الوطنية على كفالة حماية الحق في الخصوصية (اتفاقاً مع المواثيق والاتفاقيات الدولية، والهيئات الدولية ذات الصلة)، وذلك بما يشمله من الحق في حماية البيانات الشخصية، ولاسيما الرقمية، التي ظهرت مع التقدم التقني والتكنولوجي، وأكدت أحكام المحاكم الدولية(محكمة العدل الأوربية – المحكمة الأوربية لحقوق الإنسان) وأحكام محاكم الدول المختلفة، على تلك الحماية، وذلك من خلال أحكامها في القضايا ذات الصلة.

وتبين مما سبق، الحقوق المقررة دولياً لصاحب البيانات الرقمية، من حيث الرضا أو الاعتراض استخدام بياناته الرقمية، والحق في الاتصال أو النفاذ إليها، إضافة إلى حق النسيان الرقمي، وحق تقديم الشكوى حال الاعتداء على بياناته الشخصية الرقمية.

كذلك تم تنظيم أحكام معالجة البيانات الشخصية الرقمية، من حيث وضع ضوابط والتزامات تقع على عاتق الشخص القائم بتلك العملية، وذلك في ضوء مبادئ دولية وضعتها الاتفاقية الأوربية، للإحاطة بعملية المعالجة، ومن ثم يخضع المخالف لتلك الالتزامات والمبادئ إلى المساءلة القانونية، إضافة إلى ما وضعته المواقع والتطبيقات الإلكترونية(انستجرام – تويبيك– فيسبوك– تويتر– ياهوو – واتس آب) لحماية البيانات الشخصية الرقمية، من سياسات لحماية الخصوصية، وذلك عند استخدام تلك التطبيقات، خاصة من قبل الأطفال.

ولكن رغم أهمية حماية الحق في البيانات الشخصية الرقمية، اتضح أن هناك حقوق وحريات أخرى، قد تتعارض مع حق خصوصية البيانات الشخصية الرقمية، وذلك كالحق في الحصول على المعلومة وتداولها ونشرها، وكذلك الحق في الإطلاع في حالات الطوارئ لحماية الأمن القومي، أو إذا كانت معالجة تلك البيانات تتم لغرض إعلامي، أو بغرض الحصول على بيانات إحصائية رسمية، ولعل ذلك التعارض قد استدعى العمل بمبدأ التناسب هذه الحقوق لعدم طغيان إحداها على الأخرى، حرصاً على حماية حقوق وحريات الإنسان بصفة عامة، في ضوء الصالح العام.

الكلمات المفتاحية:

البيانات الشخصية الرقمية – الحق في الخصوصية – التجارة الإلكترونية – حقوق الإنسان – الحماية الدولية – الاعتداء على البيانات – التقنيات المعلوماتية – المعالجة الإلكترونية للبيانات الشخصية – الحق في النسيان الرقمي – البيانات التوصيفية – اللائحة الأوربية لحماية البيانات.

International Protection of Digital Personal Data

A study in the light of the provisions of international conventions and courts

Research Summary

The majority of national legislation stipulates ensuring the protection of the right to privacy (in agreement with international charters and agreements, and relevant international bodies), including the right to protect personal data, especially digital data, which has emerged with technical and technological progress The rulings of international courts (the European Court of Justice - the European Court of Human Rights), and the rulings of the courts of various countries, have confirmed this protection, through their rulings in relevant cases It is clear from the above, the internationally established rights of the digital data owner, in terms of consent or objection to the use of his digital data, the right to communicate or access it, in addition to the right to digital oblivion, and the right to file a complaint in the event of an attack on his digital personal data

The provisions for processing digital personal data have also been regulated, in terms of setting controls and obligations that fall on the person carrying out that process, considering international principles established by the European Convention, to surround the processing process, and then the violator of those obligations and principles is subject to legal accountability. In addition to the policies that websites and electronic applications (Instagram, Tweep, Facebook, Twitter, Yahoo, and WhatsApp) have established to protect digital personal data, including policies to protect privacy when using these applications, especially by children. But despite the importance of protecting the right to digital personal data, it has become clear that there are other rights and freedoms that may conflict with the right to privacy of digital personal data, such as the right to obtain, circulate, and disseminate information, as well as the right to access in emergency situations to protect national security, or if it is being processed. This data is made for informational purposes, or for the purpose of obtaining official statistical data. Perhaps this conflict has necessitated applying the principle of proportionality to these rights so that one does not overpower the other, to protect human rights and freedoms in general.

Key words:

Digital Personal Data - Right to Privacy - E-Commerce - Human Rights - International Protection - Data Abuse - Information Technologies - Electronic Processing of Personal Data - The Right to Digital Forgetfulness - Metadata -

European Data Protection Regulation.

مقدمة:

نص "الإعلان العالمي لحقوق الإنسان" عام ١٩٤٨م، على كفالة حق المكان والاتصالات، من حيث السرية، فلا يتعرض أحد لتدخل تعسفي في حياته الخاصة، أو أسرته أو مسكنه أو مراسلاته (المادة رقم ١٢)، وأكد على ذلك "العهد الدولي للحقوق المدنية والسياسية"، الصادر عن الأمم المتحدة عام ١٩٦٦م (المادة رقم ١٧) وكفل حماية حق الإنسان في الأمان على شخصه (المادة رقم٩) وذلك توافقاً مع ما نصت عليه "الاتفاقية الأوربية لحقوق الإنسان والحريات الأساسية" لعام ١٩٥٠م، والتي أوجبت ضرورة حماية الحق في الحياة الخاصة، ضد أي تدخل من جانب السلطة العامة، إلا في حدود ما يفرضه القانون، وذلك في المادة رقم ٨[١]، والتي نصت على أن: { لكل شخص الحق في احترام حياته الخاصة، وحياته العائلية، وكذا مسكنه ومراسلاته، وليس للسلطة العامة أن تتدخل في ممارسة هذا الحق، إلا في الحدود التي يفرضها القانون، وبالقدر الضروري لحماية الأمن الوطني، والأمن العام، والمصلحة الاقتصادية للدولة، وكذا الدفاع عن النظام، والوقاية من الجرائم، أو لحماية الصحة العامة، أو الأخلاق، أو لحماية حقوق وحريات الآخرين}[٢].

وعليه؛ فإنه يتوجب احترام هذه الخصوصية، وهو ما يعبر عنه بالحياة الخاصة للإنسان، وما يتعلق بشخصيته، والتي تتسع لتشمل الحق في سرية المراسلات والمحادثات، لما قد تتضمنه من بيانات شخصية ومعلومات (محل الدراسة)، بالإضافة إلى حرية الاعتقاد والفكر، والمسائل العاطفية، والعائلية والروحية والمالية.. إلخ وبالتالي فهي من المظاهر الاجتماعية, الضرورية لكل إنسان، وجزءاً لا يتجزأ من الوجود الإنساني، يجب حمايته ضد التعسف والاعتداء، مع عدم الاعتراض مع الحريات[٣] والحقوق[٤]، إذ أن أمن البيانات الشخصية في البيئة الرقمية, يمثل حماية المعلومات من حيث توافرها، وإضفاء الثقة فيها وسلامتها، وتعتبر السرية خاصية ترتبط بعدم تغيير البيانات والمعلومات، أو فقدها، وإتاحتها فقط لأشخاص وكيانات معتمدة، مصرح لها فقط باستخدام البيانات، وتتضمن العمليات التي تستخدم أساليب التشفير، والترميز والحجب لمحتويات البيانات والمعلومات الشخصية، والسماح بها في أوقات وبطرق معتمدة[٥].

---

1 Gloria Gonzalez Fuster, Security and the future of personal data protection in the Europen Union, Security and Human Rights, January 2013, published on: http://www.researchgate.net .Visited on 11/7/2023.

٢ تم التوقيع على هذه الاتفاقية في مدينة روما, بتاريخ ١٩٥٠/١٠/٤م، ودخلت حيز التنفيذ في ١٩٥٣/٩/٣م.

٣ انظر؛ د. محمد أمين الميداني، النظام الأوروبي لحماية حقوق الإنسان، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٩، ص١٨٠ وما بعدها.

4 P.Bouzat et J.Pinatel, Traité de droit pénal de criminology, T. III, Dalloz, 1975, p 171.

٥ د.محمد محمد الهادي, توجهات أمن وشفافية المعلومات في ظل الحكومة الالكترونية, بدون دار نشر, ٢٠١٩, ص ١٩.

أهداف الدراسة:

تهدف الدراسة إلى بيان مضمون البيانات الشخصية الرقمية، وذلك في ظل تطور التقنية المعلوماتية، بالإضافة إلى كيفية حمايتها تشريعياً ضد الاعتداء عليها، من خلال ما قضت به أحكام المحاكم الدولية في القضايا ذات الصلة، مع توضيح كيفية التوازن بين حماية البيانات الشخصية والحقوق الأخرى عند التعارض.

إشكالية الدراسة:

تعد حماية خصوصية البيانات الشخصية، من أهم التحديات التي تواجه الدول، خاصةً في ظل نظم التحول الرقمي، وإشكالية محاولة التوازن والتنسيق فيما بين "حماية البيانات الشخصية الرقمية"، و"المحافظة على الأمن القومي للدولة"، خاصة في ظل التهديدات الأمنية التي يتعرض لها العالم، من قبل الإرهاب بصفة عامة، والإرهاب السيبراني بصفة خاصة، ومن ثم كيفية التناسب بين "حماية البيانات الشخصية الرقمية" و"تحقيق الصالح العام"، بعدم المساس بالحقوق والحريات العامة.

خطة البحث:

- المبحث الأول: وسائل وصور التعدي على البيانات الشخصية الرقمية.
- المبحث الثاني: نطاق الحماية الدولية للبيانات الشخصية الرقمية.
- المبحث الثالث: ضوابط الحماية الدولية للبيانات الشخصية الرقمية.

المبحث الأول

وسائل وصور التعدي على البيانات الشخصية الرقمية

تمهيد وتقسيم:

تطورت البيانات الشخصية، واتسعت صورها، لتشمل البيانات الشخصية التقليدية للإنسان، مثل:(الاسم واللقب– الرقم الهاتفي– الرقم البريدي– السن وتاريخ الميلاد– الجنس والجنسية)، إضافة إلى كافة البيانات التي يمكن من خلالها تحديد صاحبها، كالصورة مثلاً، أو يكون من شأنها أن تجعله قابلاً للتحديد، وكذلك بياناته التجارية)، والتي إذا ما تم استخدامها عبر تقنيات الوسائل التكنولوجية، فإنها تعتبر رقمية، إضافة إلى صور البيانات الشخصية الحديثة، التي أفرزتها تلك التقنيات المعلوماتية، وهي:(رسائل البريد الالكتروني– رقم بطاقة الخصم – الحسابات البنكية والالكترونية – كلمة السر أو الرقم السري – اسم المستخدم أو رمز التوجيه– البيانات التوصيفية[1]– ملفات الكوكيز[2] – البيانات الحساسة[3]).

ومن ثم تعرف "البيانات الشخصية الرقمية"، بأنها بيانات تعد من قبيل الخصوصية المعلوماتية،

---

١ البيانات التي تعبر عن رغبات الشخص, من حيث الاستهلاك, كتفضيله لشراء منتج معين, والمواصفات والكميات التي يرغبها. كما أنها البيانات التي تعبر عن سلوك الشخص, وطباعه, ومعاملاته الاجتماعية, وهواياته, بحيث يصعب مع التطور والتنوع, القيام بوصف قوائم المنتجات يدوياً, فتقوم برامج الذكاء الاصطناعي بتقديم آلية للمسوقين, بإنشاء محتوى من خلال الكتابة التلقائية للأوصاف التفصيلية, مع أخذ المعلومات من مواقع الشركة المصنعة, ودمجها مع التفاصيل الأكثر صلةً بالمنتج الموجود على الإنترنت. د. محمود محمد محمد مهنى, استخدام التسويق الالكتروني لتطبيقات تكنولوجيا الذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي, مجلة مستقبل العلوم الاجتماعية, العدد ٨, يناير ٢٠٢٢, ص٢١٣.

٢ وهي عبارة عن ملفات نصية, يقوم جهاز الحاسب الآلي بجمعها, وذلك عند تصفح مواقع الإنترنت, من خلال برنامج يتم تثبيته على حاسب المستخدم, وتكون مهمته القيام بجمع معلومات خاصة عن المستخدم, تفيد المواقع على التعرف عليك, وذلك عندما يقوم بالدخول مرة أخرى للتصفح. د.عثمان بكر عثمان, المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي, مجلة كلية الشريعة والقانون, كلية الحقوق, جامعة طنطا, ٢٠١٨, ص١٤.

٣ وهي بيانات ترتبط بشكل مباشر أو غير مباشر بالأصول العرقية أو الجينية, أو الآراء السياسية أو الفلسفية أو الدينية أو النقابية, أو الصحة أو الحياة الجنسية للأفراد, بحيث تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية, أو بيانات القياسات الحيوية (البيومترية), أو البيانات المالية, أو المعتقدات الدينية والآراء السياسية, والحالة الأمنية, وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة. د.عبد الهادي فوزي العوضي, الحق في الدخول في طي النسيان على شبكة الإنترنت, دراسة قانونية تطبيقية مقارنة, دار النهضة العربية, ٢٠١٤, ص ١٠٨ .

ويتم معالجتها بطريقة آلية, ويود صاحبها في إخفائها عن الغير، وحمايتها ضد الاعتداء عليها وإفشائها[١]، ووفقاً لاتفاقية الاتحاد الأفريقي بشأن الفضاء الإلكتروني وحماية البيانات الشخصية لعام ٢٠١٤، فإن تلك البيانات تعرف بأنها:{ المعلومات المتصلة بشخص طبيعي محدد أو غير قابل للتحديد، بشكل مباشر أو غير مباشر}[٢]، لذا فهي بيانات شخصية لصيقة بالشخصية(وفقاً لتعريف الاتفاقية الدولية لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية رقم ١٠٨ لسنة ١٩٨١)، ومن ثم وجب حمايتها ضد كافة وسائل الاعتداء على تلك الخصوصية, التي تطورت من حيث طرق نقل البيانات وتصويرها، بحيث يتم تسريبها من خلال الوسائل التكنولوجية، بما تتضمنه من أجهزة ذكية، مثل الهاتف المحمول، وأيضاً بما تتضمنه من أقراص معدنية (اسطوانات)، وفلاشات ضوئية[٣]، حيث تتعدد وسائل التعدي على البيانات الشخصية الرقمية، وهي تتمثل في حيازة وإنتاج تلك البيانات بطرق غير مشروعة، والإطلاع غير المشروع عليها، وتصويرها أو تسجيلها خلسةً، ومن ثم إفشائها، وكذلك تزوير تلك البيانات بالمحو أو الإضافة، للاستخدام غير المشروع لها، والإضرار بصاحبها، كذلك تكثر صور التعدي على البيانات الشخصية الرقمية، في المعاملات التجارية ذات الطبيعة الإلكترونية، بما يفقدها الثقة التجارية، وفيما يلي نوضح ذلك من خلال المطالب الآتية:-

- **المطلب الأول: حيازة وإنتاج البيانات الشخصية الرقمية.**
- **المطلب الثاني: الإطلاع غير المشروع على البيانات الشخصية الرقمية.**
- **المطلب الثالث: تصوير وتسجيل البيانات الشخصية وإفشائها.**
- **المطلب الرابع: الاعتداء على البيانات الشخصية في المعاملات التجارية الإلكترونية.**

---

١ د.سامح عبد الواحد التهامي, ضوابط معالجة البيانات الشخصية, دراسة مقارنة بين القانون الفرنسي والقانون الكويتي, مجلة كلية القانون الكويتية العالمية, العدد٩, السنة ٣, مارس ٢٠١٥, ص ٤٠٤.

٢ المادة رقم ١, الفقرة رقم ٣٥ من اتفاقية الاتحاد الأفريقي بشأن الفضاء الإلكتروني وحماية البيانات الشخصية لعام ٢٠١٤.

3 Jean-Michel Bruguiere, Droits patrimoniaux de la personnalité — RTD civ. 2016. 1: 21 mars 2016. et, T. Hassler, La crise d'identité des droits de la personnalité, LPA 2004, p. 3.

المطلب الأول

حيازة وإنتاج البيانات الشخصية الرقمية

أوضحت المادة رقم ٩ من "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، وسائل التعدي على البيانات الشخصية الرقمية، وذلك بالنص على تجريم (إنتاج[١] أو بيع أو شراء أو استيراد، أية أدوات أو برامج مصممة للاعتداء على البيانات الشخصية والمعلومات، وكذلك حيازة أية أدوات أو برامج, بقصد استخدامها في الاعتداء على سلامة البيانات)[٢]، **وتطبيقاً على ذلك**, نجد أنه تم إدانة طبيب الرئيس الفرنسي "ميتران"، حيث قام بتأليف كتاب عن مرض الرئيس، وتم مصادرة الكتاب من الأسواق، لأنه ارتكب جريمة انتهاك خصوصية البيانات الشخصية، المتمثلة في البيانات الصحية(مادة رقم ٣٥ من اللائحة العامة لحماية البيانات الشخصية GDBR رقم ٦٧٩ لسنة ٢٠١٦)[٣].

هذا ويقع الفعل المادي لحيازة تلك البيانات، من قبل الشخص المسئول عن مباشرة تسجيلها، أو فهرستها، أو نقلها, والقيام بأي من الأعمال التي يترتب عليها معالجة البيانات، **وتطبيقاً على ذلك**، نجد أنه عام ٢٠٠٠، قام بعض القراصنة بالدخول على موقع شركة تسجيل النطاقات (Network Solutions) وحازت البيانات الشخصية للعملاء، وغيرت بيانات النطاق, لضعف إجراءات أمن المعلومات بالشركة، وتم إعادة توجيه العملاء من مستخدمي الإنترنت إلى موقع شركة انترنت أخرى في اسكتلاندا[٤].

وتجدر الإشارة، أنه لم يحدد المشرع المصري آلية الإنتاج، أو طريقته، أو مقداره، وإنما جعل كل إعداد ينتج عنه المساس بالمصالح المذكورة سابقاً، جريمة يعاقب عليها القانون، ويتحقق الإرسال بكافة الوسائل، سواء كانت عن طريق الرسائل العادية أم الإلكترونية، وهو ما يوسع من نطاق انتهاكها بتوسيع

---

١ يقصد بإنتاج البيانات الشخصية الرقمية: القيام بتجسيد المعلومات الشخصية في شكل مادة منتجة، سواء كانت مادية أم معنوية، تؤدي إلى المساس بخصوصية الشخص صاحب البيانات، وإضراره. أ. منصور بن صالح السلمي، المسئولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، دراسة تأصيلية مقارنة، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم العربية، ٢٠١٠، ص٨٨.

٢ أنظر: نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشئون القانونية، الشبكة القانونية العربية. http://www.arablegalnet.org.visited on 13/5/2023

٣ د. رزق سعد، الحماية الجنائية للبيانات الشخصية المعالجة الكترونياً في ضوء القانون رقم ١٥١ لسنة ٢٠٢٠،مؤتمر الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي "رؤية مصر ٢٠٣٠ في المجال الصحي"، المؤتمر الدولي الأول بكلية الحقوق، جامعة السادات، ٢٠٢٢، ص ٢٣ .

٤ د. محمد حجازي، جرائم الحاسبات والانترنت، الجرائم المعلوماتية، المركز المصري للملكية الفكرية، مارس ٢٠٠٥، ص ١٤.

نشرها، أما التخزين فيقصد به حفظ هذه المعلومات, وذلك بالأجهزة الإلكترونية المختلفة[١].

ولعل هذا الأمر قد يتجسد في قيام الجاني, بخلق حسابات وهمية، والحصول على بيانات المجني عليهم بالبنوك، وإرسال بعضها إليهم، ليطمئنوا أنه تابع للبنك، فيعطوه باقي البيانات المطلوبة، مثل (رقم الفيزا – الرقم السري)، ويستولي على أرصدتهم البنكية.

وكان أشهر هذه الجرائم، ما قام به مهندس حاسبات آسيوي، استولى على حسابات عملاء، وذلك في ١٣ بنك محلي وعالمي بالإمارات، وبلغ مجموع ما استحوذه من مال، جراء تلك العمليات الإجرامية، حوالي ٣٠٠ ألف درهماً من البنوك المحلية بالإمارات فقط[٢].

وقد يعتمد الإنتاج والتخزين والحيازة غير المشروعة للبيانات الشخصية، على التجميع غير المشروع لها، أي دون رضاء صاحب البيانات، ويتم ذلك التجميع منذ اللحظة التي يقوم المستخدم بتصفح أحد المواقع الالكترونية، من خلال بعض العناصر التي تتضمنها صفحة الإنترنت، مثل عنوان بروتوكول الإنترنت، أو ما يعرف ب " **IP adrdress**"، وهو بروتوكول يوضح كيفية تبادل المعلومات بين طرفين على شبكة الإنترنت، بحيث لا يتشابه أي عنوان لبروتوكول مع غيره، فيما يشبه بصمة اليد، ولكن ذلك يكون بشكل رقمي. ويتم الوصول إلى البيانات الشخصية، عن طريق تتبع عنوان البروتوكول، والتجسس على موقع الجهاز، الذي يقوم بعملية التصفح على الإنترنت[٣]، فمثلاً إذا كان عنوان "**IP**"، للمستخدم (**01- 04 -03 -02**)، فإن رقم **01** يشير إلى بلد جهاز المستخدم، ورقم **02** يشير إلى الجهة المنظمة للإنترنت داخل البلد، أما رقم **03** فإنه يشير إلى شركة الإنترنت المشترك معها المستخدم, ورقم **04** يشير إلى رقم المشترك لدى شركة الإنترنت.

ومن ثم فإنه عند إرسال مجموعة من البيانات، أو استقبالها على شبكة الإنترنت، يتم تقسيم تلك الرسالة إلى مجموعة من القطع الصغيرة، والتي تعرف باسم "حزم"، يحتوي كل منها على عنوان المرسل والمستقبِل.

إضافة إلى ملفات تعريف الارتباط "كوكيز"، التي يمكن من خلالها التوصل إلى البيانات الشخصية للمستخدم، وكذلك هناك "الويب باجز"**Web Bugs**، وهي عناصر غير مرئية، تتضمنها صفحات البريد الإلكتروني، والمواقع الإلكترونية، وتعمل على إرسال المعلومات والبيانات، الخاصة بحركة المستخدم على الموقع الإلكتروني، كنسخ أو تحميل الصفحات، كما أنه يتم من خلالها التمكن من معرفة إطلاع المستخدم

---

١ د. محمد رايس، الحماية الجنائية للسند الإلكتروني في القانون الجزائري، مجلة الدراسات القانونية، كلية الحقوق، جامعة بيروت العربية، لبنان، العدد الأول، ٢٠٠٦/٢٠٠٧، ص ٩٦.

٢ د. محمد حجازي, المرجع السابق, ص ١٩.

3 INTERNET PROTOCOL http://toolsietforg/html/rfc760. visited on 8/5/2023.

على بريده الإلكتروني، وهل قام بإرسال رسائل بريدية إلى شخص آخر أم لا؟ ويمكن توفير بعض من الحماية للبيانات، من تطفل عناصر **Web Bugs**، من خلال إغلاق ملفات الكوكيز من متصفح الإنترنت[١].

وتطبيقاً على ذلك، فقد فرضت "اللجنة القومية للمعلوماتية والحريات"، غرامة على شركة جوجل، لجمعها بيانات المحتوى من كلمات المرور، ورسائل البريد الالكتروني، وغيرها من الوسائل، التي يتم تجميع البيانات الشخصية من خلالها، وذلك عبر شبكة الواي فاي، لأجل خدمتها الجديدة، والتي تعرف ب "جوجل سترتيت فيو"، وقد تعهدت جوجل بالتخلص من تلك البيانات المخزنة، جراء ذلك[٢].

كما قد يتم تجميع البيانات وإرسالها إلى الشركات الدعائية، من خلال الوكيل الالكتروني لأغراض تجارية، وهو ما اعتبرته "محكمة النقض الفرنسية"، عملاً غير مشروعاً[٣].

إضافة إلى ما سبق، فقد أوجب "مشروع معاهدة المنظمة العالمية للملكية الفكرية" الخاص بقواعد البيانات لعام ١٩٩٦، توفير نوع آخر من الحماية القانونية لقواعد البيانات، وذلك بناء على توافر شرط يسمى "الاستثمار الجوهري"، وقد قررت المادة الأولى من هذا المشروع، أن الشرط المطلوب توافره لمنح الحماية لقواعد البيانات، هو أن تنطوي قاعدة البيانات على استثمار جوهري، وأوردت المادة رقم (٤/٢)، المقصود بعبارة "الاستثمار الجوهري"، وذلك بأنه: {كل استثمار مهم نوعاً أو كماً لموارد بشرية، أو مالية، أو تقنية، أو غيرها، من أجل جمع قاعدة البيانات أو تجميعها، أو تمحيصها، أو ترتيبها، أو عرض محتوياتها}[٤].

كما أوضحت المادة (٣/٢) من المشروع، المقصود بعبارة "واضع قاعدة البيانات"، وذلك بأنه: {كل شخص طبيعي أو معنوي، واحد أو أكثر، له سلطة الإشراف والمسئولية، للاضطلاع باستثمار جوهري، من أجل وضع قاعدة البيانات}.

وترجع أهمية الاستثمار الجوهري, التي تنصب على القيمة التجارية لقواعد البيانات إلى عنصرين أساسيين، يتمثل الأول في التكلفة المالية لإعدادها، والثاني في القيمة المتوقعة لها في السوق، أي قيمتها

---

١ د.سارة الشريف, خصوصية البيانات الرقمية, سلسلة أوراق الحق في المعرفة, مركز دعم لتقنية المعلومات, القاهرة, ٢٠١٤, ص ٣.

٢ د. عثمان بكر عثمان, المرجع السابق, ص ١٦.

3 Cass.crim, 14 mars, 2006. Available on: http:// www.Legi France. gouv-Fr.7/5/2023.

٤ المستشار. مصطفى الصديق إبراهيم خورشيد, الحماية القانونية لحقوق المؤلف علي مصنفاته الرقمية في بيئة الانترنت,"دراسة مقارنة في التشريع المصري والاتفاقيات الدولية", بحث مقدم للمؤتمر العلمي الخامس للمعهد القومي للملكية الفكرية, ٢٦ ابريل ٢٠٢٢, ص١٧ .

الفعلية، إلا أن الأخذ بشرط الاستثمار الجوهري, يدخل تحت نطاق السلطة التقديرية للمحكمة[١] .

١ د. حسام محمد موسي توني, حماية قواعد البيانات في ضوء الاتفاقيات الدولية وقانون حماية الملكية الفكرية المصري, دراسة مقارنة, الطبعة الأولى, دار النهضة العربية،٢٠٢١، ص٥ – ٤٩.

المطلب الثاني

الإطلاع غير المشروع على البيانات الشخصية

كفلت الاتفاقيات الدولية ضمان الحق في الاطلاع على المعلومات للكافة، وذلك بأن يكون مجاناً وبحرية، عدا ما يتعلق بالمعلومات المرتبطة بخصوصية الإنسان، حيث تم استثنائها من الاطلاع، سواء كانت بيانات تقليدية أم رقمية، تواكباً مع التطور التكنولوجي، حيث يستطيع كثير من مستخدمي البرامج الالكترونية، اختيار كلمات مرور سهلة, يسهل تذكرها فيما بعد، وبعد الدخول إلى النظام، وإتمام العمليات المراد القيام بها من قبل المستخدم، فإنه يخرج من النظام، إلا أنه قد يترك كلمة المرور الخاصة (سهواً أو لعدم دراية منه بالخطورة) معروضة وغير مستخدمة على النهايات الطرفية النشطة، المرتبطة بنظم الشبكة، تاركين منافذ الرقابة والوصول متاحة، ومفتوحة في مواقع الأمن، مما يعرضها للاختراق، ومن ثم الإطلاع على البيانات الواردة بها[1].

مثال على ذلك، استغلال الفيسبوك في التعرف على البيانات الأشخاص، من خلال بياناتهم, وجهات الاتصال الخاصة بهم، وعناوين البريد الالكتروني، وكلمة السر، والدخول إلى صفحتهم الشخصية.

وقد عرف المشرع الكويتي في القانون رقم ٦٣ لسنة ٢٠١٥، "الدخول غير المشروع"، وذلك بأنه:{ النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي، أو لنظام معلوماتي أو شبكة معلوماتية أو موقع الكتروني، من خلال اختراق وسائل وإجراءات الحماية لها، وذلك بشكل جزئي أو كلي، لأي غرض كان, بدون تفويض، أو تجاوز للتفويض الممنوح}.

كما يتحقق الاطلاع غير المشروع، إذا تم من شخص غير مرخص له قانوناً، بالدخول إلى تلك البيانات والمعلومات الشخصية، ولذلك لا يتصور ارتكاب الفعل من الشخص، المخول له تخزين وحفظ البيانات والمعلومات الخاصة، أو تصنيفها أو إجراء أية معالجة آلية لها[2].

وبالتالي فإن الإطلاع قد يكمن في الدخول غير المشروع لأنظمة المعلومات، وقواعد البيانات، وذلك بصورة غير مشروعة، والخروج دون إحداث أثر سلبي عليها, أو أي ضرر، من خلال الاختراق لأمن البيانات والمعلومات، استغلالاً لبعض الثغرات في نظم الحاسب، أو شبكات المعلومات، أو مواقع الانترنت.

ولعل ذلك يحتاج إلى استخدام الجدار الناري Fire Wall ، وتشفير البيانات بكلمات سر لحماية المعلومات، بما يعطي إشارة إلى المسئولين عن البيانات، بوجود خطر ما، ومن ثم القيام بإعادة بناء النظام

---

١ د.محمد محمد الهادي، مرجع سابق، ص ١٦.

٢ د. أشرف محمد نجيب، جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، مجلة روح القوانين، كلية الحقوق،جامعة طنطا، العدد الخامس والتسعون، يوليو ٢٠٢١، ص ٢٧١.

الأمني للبيانات مرة أخرى[١]، حيث يمثل ذلك الجدار حاجزاً بين "الموقع الالكتروني التجاري" و"قراصنة الإنترنت"، لأنه عبارة عن سياسات آمنة بين "الإنترنت" و"شبكة المتجر الالكتروني"، تقوم بإجبار عمليات العبور إلى الشبكة والخروج منها؛ أن تمر من خلال هذا الجدار، الذي يصد أي متطفل غريب يقوم بالاختراق[٢]، الذي يتمثل في إطلاع غير مسموح به على المعلومات، المخزنة في النظم المعلوماتية، بما يشكل التحدي الأكبر الذي يواجه الأفراد والشركات، حيث يؤدي إلى رصد التحركات الشخصية لهم[٣].

ومن خلال ذلك؛ يتضح أن الوسيلة السابقة الذكر، تتمثل في تشفير البيانات والرسائل المرسلة بين كل من "البائع" و"المشتري" عبر الإنترنت، لعدم قرصنتها، وأن التشفير يعد أكثر من عملية إغلاق المحرر الالكتروني، فهو أفضل الوسائل التكنولوجية، وأحد وسائل الأمان المتبعة، في الحفاظ على سلامة تبادل البيانات عبر الموقع التجاري، بحيث تكون تلك الرسائل غير مقروءة، إلا لمن يملك الشفرة، المتمثلة في رقم أو كلمة سرية معينة[٤].

وقد عرفته "اللائحة التنفيذية لقانون التوقيع الالكتروني المصري" بأنها :{ منظومة تقنية حسابية، تمنع من استخلاص هذه البيانات والمعلومات، إلا عن طريق استخدام مفاتيح فك الشفرة}[٥].

والجدير بالذكر؛ أن المعلومات والبيانات المجهولة، لا تنتهك الحياة الخاصة لأي شخص، لأن المجهول لا خصوصية له، ولكن المسئولية القانونية تثور عند المساس بالمعلومات والبيانات، التي تسمح بالتعرف على الشخص محل هذه المعلومات، بشكل مباشر أو غير مباشر، ولا يرغب الشخص الذي تتعلق به هذه المعلومات أو البيانات، كشفها للغير، وفي هذه الحالة يتحقق الاعتداء على الحق في الحياة الخاصة.

ويعد الجمع أو التخزين للمعلومات والبيانات الشخصية، أحد الأساليب غير المشروعة، التي تشكل اعتداء على الحق في الحياة الخاصة، من خلال مراقبة وعرض وتفريغ وقراءة الرسائل المتبادلة، عن طريق البريد الإلكتروني، والتوصل غير المشروع إلى ملفات تعود للآخرين، خاصةً إذا تم هذا الجمع أو التخزين

---

١ د. محمد حجازي, المرجع السابق, ص ١١.

٢ د . محمد سعيد أحمد إسماعيل, أساليب الحماية القانونية لمعاملات التجارة الالكترونية, دراسة مقارنة, رسالة دكتوراه, جامعة عين شمس, ٢٠٠٥, ص ٣٥.

٣ د. بن سماعيل سلسبيل, الحماية الجنائية للخصوصية المعلوماتية في التشريعين الجزائري والفرنسي, مجلة الاجتهاد القضائي, جامعة محمد خضر بسكرة, الجزائر, المجلد ١٢, ابريل ٢٠٢٢, ص ٧٤٣ .

4 Philippe Dimitriou; L' application du droit de la cryptologie en Matiére de sécurite desréseaux informatiques, Faculté des sciences juridiques, Politiques et socials de Lille 2, Droit et Santé école Dctorale , No 74, 2002, P 17 , 19 .

٥ د.حسين عبده الماحي، نظرات قانونية في التجارة الالكترونية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، ٢٠٠٢، ص ٣٢.

بصورة غير قانونية من أشخاص، أو جهات ليس لهم الحق في القيام بهذا العمل[١].

وقد تتمثل تلك الصورة غير المشروعة، في انتحال شخصية أو هوية مستخدم آخر، بقصد سرقة البيانات الشخصية، وتنتشر تلك الصورة في التجارة الالكترونية[٢].

ونتيجة لما سبق؛ فإنه يكون هناك حاجة إلى تفعيل القوانين الخاصة بحالات الاعتداء على نظم التجارة، عبر استخدام الحاسب الآلي، وذلك وفقاً لما أشار إليه قانون تقنية المعلومات (رقم ١٧٥ لسنة ٢٠١٨)؛ إلى الالتقاط غير المشروع للمعلومات أو البيانات، وتم الإشارة كذلك إلى نشر واستخدام برامج الحاسب الآلي، بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية، بالإضافة إلى إتلاف البيانات وتغييرها، وكذلك تقليد أو تزوير بطاقات الوفاء أو السحب، واستعمال تلك البطاقات مع العلم بحقيقتها، وقبول الدفع بالبطاقات المزورة أو المقلدة، مع العلم بذلك، واستعمال البطاقات بعد انتهاء صلاحيتها مع العلم بذلك، واستخدام بطاقة الغير بدون علم صاحبها[٣].

وتلك الجرائم قد قررتها القوانين الدولية, حرصاً منها على زيادة الأثر في الحماية القانونية للبيانات الشخصية، المتداولة أثناء عمليات التجارة الحديثة، التي لا يمكن الاستغناء فيها عن الحاسب الآلي، وذلك ضد الاستخدام السيئ لنظام الحاسب الآلي في التجارة الالكترونية الدولية[٤].

بالإضافة إلى ما أشار إليه القانون الفرنسي الخاص بجرائم الكمبيوتر لعام ١٩٧٨م، وما لحق به من تعديلات عام ١٩٨٥م و ١٩٨٨م، وما نظّمه الكتاب الثالث من قانون العقوبات لعام ١٩٨٦م، في نصوص المواد أرقام "٣٢٣-١" إلى "٣٢٣-٧"[٥], والتي جرمت بصورة مباشرة الدخول بطريق الغش أو التدليس على نظام الحاسوب الآلي، وإنتاج أو بيع أو حيازة أو استيراد أو توزيع أو توفير أي وسيلة، بما فيها برامج الكمبيوتر، المستخدمة لارتكاب الجرائم المشار إليها، وكلمات أو أرقام السر، وكذلك تزوير برامج الحاسب الآلي، من خلال التعديل أو الحذف أو المسح، دون الحاجة إلى التعرف على تلك البيانات بواسطة

---

١ د. أسامة بن غانم العبيدي، حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، مركز الدراسات والبحوث والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، المجلد ٢٢، العدد ٤٦، ص٥٦ – ٦٦.

٢ د.تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي ، دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد ٤، العدد ٢، ٢٠٢٠، ص ١٥٢١ وما بعدها .

٣ د . يونس عرب، قانون تقنية المعلومات والتجارة الالكترونية، ط١، مجلة نقابة المحاميين الأردنيين، عمان، ٢٠٠٣/ ٢٠٠٤، ص ٢٦ وما بعدها.

4 Emmanuel, Cornu – Alexandre Cruquenaire, La protection des marquees sur internet, Cahiers du centre recherché information et droit, 2007, p 17.

5 Van Dael ,La fascalite indirecte des transactions electroniques, sur la livre commerce electronique, Le temps des cetitudes, Editions Delta, 2001, p 150.

القراءة، ولو كانت غير واضحة, وليست أصلية، ولو لم توثق بمخطوطات[١].

ولعل عدم حماية الموقع الالكتروني، وتأمينه التأمين الكافي من الاعتداء على بيانات العملاء وبطاقاتهم الائتمانية، من قبل قراصنة الإنترنت، التي تنتهك خصوصية المواقع الالكترونية التجارية؛ يفقد تلك التجارة أهم عناصرها، وهو "عنصر الأمان"، حيث يتسبب ذلك في سحب أرصدتهم البنكية، وبالتالي يقل عدد المستخدمين من العملاء.

وقد يتم نسخ الموقع التجاري، ونسخ علامته التجارية، ويتعامل العملاء مع الموقع التجاري، ولا يعلمون أنهم يتعاملون مع آخرين[٢]، وهذا الاختراق يفقد الثقة في البطاقات الائتمانية، كأحد الوسائل التي تستخدم في المعاملات الاقتصادية، كما يفقد التجارة إحدى سبلها التي تساعد في ترويجها، وهي الاتجار عبر الالكترونيات[٣]، مما يؤثر بالسلب على التنمية الاقتصادية، التي تعتمد على الأمان التجاري في المعاملات التجارية، نظراً لصعوبة الإثبات في جرائم الخداع التجاري عبر الإنترنت[٤].

ونتيجة لما سبق، فقد أشارت إليه "محكمة العدل الأوربية"، إلى مدى حاجة البيانات الرقمية الوصفية، إلى حماية تتواكب مع تكنولوجيا عصر التحول الرقمي[٥].

وذلك فقد قامت الولايات المتحدة بتشريع قانون "باتريوت" عام ٢٠٠١، عقب أحداث ١١ سبتمبر ٢٠٠١، والذي يتضمن تدخل الدولة بالإطلاع على البيانات الشخصية للمواطنين، بدعوى مكافحة الإرهاب، حيث إن بموجبه يستطيع مكتب التحقيقات الفيدرالي(FBI)، ووكالة الاستخبارات المركزية (CII)، مراقبة وتفتيش المشتبه فيهم، والإطلاع على الممتلكات الشخصية للأفراد، والتنصت على المكالمات الهاتفية،

---

1 Nathalie Moreau, La formation du contrat electronique, DEA, droit des contrats, Université de Lille 2, 2003 . 2004, p 54.

٢ د. يونس أبو عرب، مرجع سابق، ص ٤.

٣ أ. حرية شعبان محمد الشريف، نظم المعلومات المحاسبية الإلكترونية، دراسة تطبيقية على المصارف العاملة في قطاع غزة، رسالة ماجستير، الجامعة الإسلامية، فلسطين، ٢٠٠٦، ص ٦٩.

4 Constancias Claire – Mavault Laureen, La publicites sur internet, Sans maiso d' éditions, 2010 , p 4 -6.

٥ محكمة العدل الأوربية، الحكم الصادر في القضية رقم C-293/12 ، والقضية رقم C-594/12، الخاصة بالحقوق الرقمية في ايرلندا, بتاريخ ٨ ابريل ٢٠١٤. منشور على الرابط الالكتروني الآتي:
http://curia.europa.eu/juris/document.jsf.visited on 2/5/2023.

والتجسس على الرسائل الهاتفية والالكترونية، والمعاملات البنكية[١]، والملفات الطبية, والمعلومات الصحية[٢]، من خلال برنامج الجمع المكثف للبيانات الوصفية الهاتفية(الفصل رقم ٢١٥ من قانون الوطنية المتحدة الأمريكي)، وكذلك عمليات الرصد، التي ينص عليها الفصل رقم ٧٠٢، من قانون تعديل جمع محتوى الاتصالات بالمخابرات(PRISM)، والتي يتم تنفيذها من خلال برنامج(UPSTREM)، من قبل شركات الإنترنت. إضافة إلى برنامج جمع البيانات الوصفية للاتصالات وفحواها، عن طريق استغلال كابلات الألياف البصرية، المستخدمة في الربط مع الإنترنت.

ولعل ذلك كان مثاراً للنقد، من قبل "اللجنة المعنية بحقوق الإنسان"، والذي اتضح من تقريرها الصادر بتاريخ ٢٠١٤/٤/٢٣[٣].

هذا وقد حصل "مكتب التحقيقات الفيدرالي الأمريكي" عام ٢٠١٦، على أمر من المحكمة، يلزم شركة آبل، بوضع برامج جديدة تعطل التشفير، الذي يحمي الجهاز، بما يؤدي إلى السماح بالدخول إلى هاتف آيفون، كان قد استخدمه أحد الإرهابيين، المتهمين بمذبحة "سان برناردينو"، بولاية كاليفورنيا، إلا أن شركة آبل رفضت طلب الحكومة، وتمسكت بحماية خصوصية مستخدمي الهواتف.

وبصدد ذلك؛ نجد أنه قد أعرب "المفوض السامي للأمم المتحدة لحقوق الإنسان"، أن هناك العديد من الطرق، التي يمكن لمكتب التحقيقات، أن يستخدمها في كشف الجرائم الإرهابية، بدلاً من إجبار شركة "آبل"، على إنشاء برامج تقوض مميزات الأمن لهواتفها[٤].

---

١ هذا وقد أقر مجلس الشيوخ الأمريكي، في أكتوبر ٢٠٠٩ , قانوناً يبيح المراقبة المتحركة لاتصالات المشتبه فيهم، وكذلك الذئب المنفرد، والذي يتيح التحقيق مع شخص يعمل لحسابه الخاص، والوصول إلى أي معطى ملموس، كبريد الكتروني، أو حساب الكتروني، لمشتبه فيهم، وذلك دون إذن قضائي، بما يمثل انتهاكاً لحرمة الهواتف، واعتداء على سرية المعاملات المالية.

– د.طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، دراسة مقارنة، مجلة الاقتصاد والقانون، كلية الحقوق، جامعة القاهرة، ملحق خاص بالعدد رقم ٩٢، ٢٠١٦، ص١٩٨ .

2 World Health Organization: The protection of personal data in health information systems principles and processes for public health. 2021 , p. 2.

٣ التقرير الدوري للجنة المعنية بحقوق الإنسان، بشأن الملاحظات الختامية قبل التقرير الدوري الرابع للولايات المتحدة،الصادر بتاريخ ٢٠١٤/٤/٢٣، فقرة رقم ٢٢.

4 http://www.hespress.com/international/297330.html.visited on 4/5/2023.

المطلب الثالث

تصوير وتسجيل البيانات الشخصية وإفشائها

يعتبر التنصت والتسجيل الإلكتروني، من أهم وسائل التعدي السمعي، الذي يقع على الحق في الخصوصية، ويقصد بفعل "التصوير والتسجيل خلسة" {الاعتداء البصري على الشخص، من خلال تصويره المفاجئ والتسجيل له، وذلك دون رغبته} ويعتبر الرضا بالتصوير ليس إذناً بنشر الصورة[١]، والذي يتم بالأدوات الفنية البصرية, مثل:{المنظار المقرب (التلسكوب)– كاميرات التصوير – المنظار المزود بالأشعة تحت الحمراء}.

وهذا النوع من المراقبة، إما أن يقع في الأماكن العامة، وإما في الأماكن الخاصة، وكلاهما يقوم به الاعتداء على الحق في الخصوصية، فالصورة تعتبر من أدق عناصر الخصوصية، بصرف النظر عن المكان الذي تم التقاطها فيه، خاصةً في ظل استخدام أجهزة المحمول والإنترنت[٢].

وعليه فإن إطلاق شركة آبل لهاتف أيفون X عام ٢٠١٧, والذي يحمل على ميزة التعرف على ملامح الوجه، وقراءة ٥٢ حركة فريدة من نوعها، من الحركات الدقيقة للجفن والفم والوجه، وبالتالي التعرض لخصوصية الصورة، بما قد يتم إساءة استخدامه من قبل المسوقين، أو الهاكرز[٣].

ولذلك فقد نصت من قبل؛ المادة رقم ٦٥٢(ج)، من المدونة الثانية للأفعال الضارة، الصادرة عام ١٩٧٧، على تجريم نشر الصورة، دون إذن من صاحبها.

وبناء عليه, قضت المحكمة لصالح الملاكم العالمي (محمد علي كلاي) ضد مجلة (بلاي جيرل)، التي نشرت له صورة عادية، دون الحصول على موافقته، بوصف أن ذلك يعد اعتداء على حياته الخاصة،ممثلةً في حقه في حماية خصوصية بياناته الشخصية، وهي الصورة[٤]، كما قضي بموجب المادة

---

١ حكم محكمة النقض المصرية، الطعن رقم ٩٥٤٢ لسنة ٩١ ق، جلسة بتاريخ ٢٠٢٢/٣/١٦. المستحدث من المبادئ التي قررتها الهيئة العامة للمواد المدنية والجنائية ودوائر المجموعات المدنية والتجارية وطلبات رجال القضاء, في الفترة من أكتوبر ٢٠٢١: ديسمبر ٢٠٢٢، المكتب الفني، ص ١٥٥.

٢ د. محمد أحمد المعدواي، حماية خصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، مجلة كلية الحقوق، جامعة بنها، العدد ٣٣،الجزء الرابع، ٢٠٢١، ص٢٠٠٥ وما بعدها.

٣ د.ياسر محمد اللمعي، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية، دراسة تحليلية مقارنة، مجلة روح القوانين، كلية الحقوق، جامعة طنطا،العدد ٩٧، يناير ٢٠٢٢، ص ٥٢ .

٤ د.الشافعي محمد بشير، قانون حقوق الإنسان، مصادره وتطبيقاته الوطنية والدولية، مكتبة الجلاء الجديدة، ٢٠٠٩، ص ١٦٠.

رقم ٦٥٢(هـ)، من المدونة الثانية للأفعال الضارة، الصادرة عام ١٩٧٧[١]، أن الشخص المحبوس، والذي قد تم الحصول على صورته وبصماته، ثم تم الإفراج عنه، بعد اكتشاف خطأ ما، يؤكد برأته مما نسب إليه، فإنه إذا تم الاحتفاظ بسجل صورته وبصماته في سجل المجرمين، يعتبر ذلك اعتداء على خصوصية بياناته الشخصية[٢].

لذا تعتبر "اللجنة القومية للمعلوماتية والحريات" بفرنسا CNIL، صوت الشخص من البيانات الشخصية التي تخضع إلى الحماية القانونية، نظراً لما قد تقوم به التكنولوجية الرقمية الحديثة، من معالجة للصوت، ووضعها على دعامة واحدة بجانب النص، بما قد يساء استغلاله[٣].

هذا وقد تتضمن المحادثات الحديث عن بيانات شخصية، إضافة إلى كونها من عناصر الحق في الخصوصية، بما يستلزم حماية خصوصيتها، حيث يتبسط المتحدث مع الطرف الآخر، ويبوح له بأسراره، لأنه مطمئن لعدم وجود شريك ثالث، دون أن يقصدا معرفة الآخرين، لما دار بهذا الحديث، حيث تعتبر الأحاديث الشخصية (ومنها المكالمات التليفونية) أسلوباً من أساليب حرمة الحياة الخاصة للناس، وهذه الأحاديث والمكالمات التليفونية مجالاً لتبادل الأسرار، وتناقل الأفكار الشخصية(التي تعتبر من البيانات الشخصية كما أسلفنا)، لذلك فلا يجوز مطلقاً تسجيل الأحاديث الشخصية، والمكالمات التليفونية، أو مراقبتها والتنصت عليها بأية وسيلة[٤].

وبذلك يقصد بالاعتداء على المحادثات، تتبع المحادثة وملاحظتها ومعاينتها، من خلال التنصت عليها، والاستماع لها خلسةً، سواء بالأُذن أم باستخدام جهاز مخصص لذلك، أياً كان نوعه, وقد يتعدى نطاق الاعتداء إلى تسجيل المحادثة، وعدم الاكتفاء بسماعها فقط[٥] .

أما عن وسيلة إفشاء البيانات الشخصية الرقمية، فهي تتمثل في انتشار وشيوع السر(البيان الشخصي) إلى الغير[٦].

---

١ راجع كذلك، القواعد النموذجية الدنيا لمعاملة السجناء الصادرة عن مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين، وذلك في دور انعقاده بجنيف عام ١٩٥٥، وقد أقرها المجلس الاقتصادي والاجتماعي بتاريخ ١٩٥٧/٧/٣١.

٢ د.الشافعي محمد بشير،مرجع سابق، ص ١٦٠.

3 CNIL, Délibération 96 – 009 du 27 février 1996, Délibération portent adoption du rapport intitulé, Les informations personnelles issues de la voix et de l'image et la protection de la vie privée et des libertés fondamentales, www.legifrqnce:gouv.fr .22/5/2023.

٤ المستشار. عادل الشهاوي، د. محمد الشهاوي، الاعتداء على الحياة الخاصة بواسطة القنوات الفضائية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٥ ، ص ١٧٦.

٥ د. أحمد محمد حسان، نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة والأفراد.. دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠١، ص٢٧٢.

6 Jean Malherb, La vie privee et droit moderne, Paris, 1967, p 22.

لذلك فقد فرض المشرع الفرنسي على موظفي مصلحة البريد، احترام سرية المراسلات، وفقاً للمادة رقم ١٨٧ من قانون العقوبات الفرنسي, رقم ١٧ لسنة ١٩٩٠، ولم يذكر الشروط الواجب توافرها لإفشاء الرسائل أو إذاعتها، وهو ما جعل القضاء يضع "مبدأ عدم انتهاك حرمة المراسلات"، ضمن المبادئ الفقهية في أحكامه[١]، ويحظر على الوكيل التجاري، إفشاء الأسرار التجارية للموكل بطريق النشر، وذلك وفقاً لقانون العمل الفرنسي[٢].

كذلك قد يتم الإفشاء بطريق النشر الالكتروني، من خلال قيام أشخاص ناشرين، بصياغة البيانات والمعلومات، أو تحويرها، ونشرها بوضعها على مواقع التواصل الاجتماعي، وذلك بأن يتم إنشاء صفحة، أو موقع على شبكة الإنترنت، أو إرسال رسائل للمستخدمين، من خلال البريد الإلكتروني[٣].

ويصعب تحديد القائم بالنشر الالكتروني, فمن يقوم بتلك الأساليب يستخدم أسماء وهمية. لذا يلزم الرصد الدائم من قبل منشئي المنتديات والمواقع، لما يتم نشره عندهم، حيث تتوافر المسئولية القانونية لديهم، لافتراض العلم منهم بما يتم نشره، إلى جانب مسئولية المدون، باعتبار أن لهم السيطرة على المحتوى، ومن ثم يستطيع أن يتحكم في المعلومات الواردة فيه، سواء عند إنشائه أم كتابته أم صياغته.

ولذلك يلتزم مدير تحرير الموقع، الذي أنشاء صفحة على موقع شبكات التواصل الاجتماعي، بعدة التزامات اعتمدها "المجلس الدستوري الفرنسي، ومجلس الشيوخ, والجمعية الوطنية"، تتمثل في إدراج اسم موقعه، وتحديد هويته على شبكة الإنترنت، لإمكانية التعرف عليه بسهولة، ويكون لمدير التحرير والناشر، الحق في تعديل كل ما يتضمنه المحتوى من بيانات مخالفة، أو ما يشكل لشروط الاستخدام، سواء كان تعديلاً كلياً أم جزئياً.

وعليه أيضاً أن يحدد شروط استخدام هذا الموقع، وأن يقيد استخدامه في أغراض التبادل الثقافي، والعلمي والاجتماعي، دون استغلاله في ارتكاب جرائم، إضافة إلى التزامه بعدم قبول دخول المستخدمين إلى هذه المواقع، إلا بالهوية الحقيقية، دون استخدام هوية مزورة، مع تحذير المستخدم بأن الدخول بهوية غير حقيقية، أو هوية وهمية، يعتبر جريمة يعاقب عليها القانون.

علاوة على أنه يتعين الإبلاغ عن إساءة استخدام مواقع التواصل الاجتماعي ضد الأطفال، لعدم درايتهم بحقوقهم في حماية بياناتهم، كذلك يلتزم مدير تحرير الموقع في حالات النشر عن طريق

---

١ د. باسم فاضل، الحماية القانونية للحق في الخصوصية، الطبعة الأولى, المصرية للنشر والتوزيع، ٢٠١٧، ص ١٣٢.

2 Piere Albert, La Presse Francaise , Notes et études documentaires kai 1978, P 233.

3 Rapport d'information de l'Assemblée Nationale sur la mise en application de la loi no.2004-575 du 21 juin2004 pour la confiance dans l'économie numérique, présenté par M. Jean Dionis du Séjour et Corinne Erhel. Ce.rapport est disponible sur: http://www.assemblee-nationale.fr/13/rap-info/i0627.asp .12/5/2023.

الوسائل الإلكترونية، الالتزام بتوفير المعلومات العامة، وتحديد هوية مؤلفي المحتوى ودور النشر[1].

1 Frédéric Pollaud-Dulian: Programmes d'ordinateur. Épuisement du droit de distribution. Revente d'occasion de copies. Supports physiques qui ne sont pas d'origine. Exceptions au droit de reproduction du logiciel, RTD Com, N° 04 du 19/01/2017, p.741 ets.

المطلب الرابع

الاعتداء على البيانات الشخصية في المعاملات التجارية الإلكترونية

هناك عدة بيانات تجارية تكون خاصة بشخص التاجر أو الصانع، ومن ثم فإننا نعتبرها في دراساتنا "بيانات شخصية"، وهي تتعدد صورها فيما بين (العلامة التجارية[١] – الاسم التجاري[٢]– أسرار الصناعة[٣])، لما تتسم به من ملكية فكرية، ترتبط بشخص صاحبها (وفقاً لوجهة نظر دراساتنا)، حيث تعتبر العلامة التجارية، إحدى العناصر التجارية، التي تتضمنها حقوق الملكية الفكرية التجارية، بالإضافة إلى الاسم التجاري، وأسرار الصناعة، وما إلى ذلك من عناصر تشكل مميزات، يتميز بها منتج عن الآخر في السوق التجاري، وتعتبر حقوقاً معنوية، يفرض عليها القانون حمايته، فتلك العناصر تكون ثمرة لنشاط تجاري، يقوم به التاجر لجلب العملاء[٤].

وعليه فقد يقوم أحد التجار بتزوير العلامات التجارية، لمنح المنتَج ثقة استهلاكية في السوق التجاري، وهو ما يؤدي إلى تضليل جمهور المستهلكين بالأسواق.

وقد عرفت اتفاقية TRIPS الخاصة بحماية الجوانب التجارية لحقوق الملكية الفكرية (عام)١٩٩٤ في المادة رقم ١٥ منها "العلامة التجارية" بأنها:{ تعتبر أي علامة أو مجموعة من العلامات تسمح بتمييز السلع والخدمات التي تنتجها منشأة ما عن تلك التي تنتجها المنشآت الأخرى }[٥].

---

١ وتعرف العلامة التجارية BRAND بأنها:{ رمز حسي مختصر يرتبط بذهن الجمهور بالعديد من الصفات النوعية التي ترتضيه وتشبع رغبته، لتميز السلعة عن الأخرى من المنتجات}.

Wong. J., Using a brand identity index for relevancy in teaching collegiate marketing, Journal of applied business and economic, 2007, p 23.

٢ وهو ما يشتهر به التاجر محلياً أو عالمياً، بسبب جودة السلعة وإتقانها، وكذلك تميزها عن أمثالها بين المستهلكين، وبسبب حسن معاملته للجمهور والخدمة التي يقدمها، والاسم التجاري هو كذلك اللقب المخصص لمحل تجاري اكتسب شهرة بهذا اللقب.

– د.عاطف محمود الفقيه، الحماية القانونية للاسم التجاري، دار النهضة العربية، ٢٠٠٧، ص ١٢ .

ومثال على الأسماء التجارية: (أحذية باتا البريطانية العالمية – محلات الغندور العالمية – أسماء العطور الفرنسية – مطاعم البغل).

٣ هي المعرفة الفنية، أي تلك التكنولوجيا التي يحتفظ بها المنتجون في سرية، دون حمايتها من خلال براءات الاختراع.

٤ د. نادية أبو العزم السيد حسن، الحقوق المعنوية في ميزان الشريعة الإسلامية، دراسة فقهية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد ٤٦، أكتوبر ٢٠٠٩، ص ٣٠٨ – ٣٠٩.

5 Maitre Jean, Pierre Gasnier, Les identifiants de l’ internet , Noms de domaine – Conflites avec les autres droit, Le droit de l ‘ enterprise et internet, Actes de colloque de Marseille, Institut de droit des affaires, 2001, p 11 etc.

وفي الوقت الحالي؛ نجد أنه قد ظهرت المعاملات الالكترونية في التجارة الالكترونية، والتعاقدات الالكترونية، وهو ما يعرف ب "السوق الالكتروني"، والذي يتم عبر التجهيزات الالكترونية، مثل الهاتف والفاكس والحاسوب والإنترنت[١].

فلقد استلزمت الضرورات العلمية إخضاع فئة معينة من المعاملات التجارية إلى تنظيم خاص، يتواءم مع مطالب التعامل التجاري، ولأن أساس التجارة هو الائتمان أو الثقة، التي يوليها التجار لبعضهم البعض في معاملاتهم التجارية، فهي في مجال التجارة الدولية، تيسر على المصدرين والمستوردين عمليات التبادل التجاري بينهما[٢].

لذا فقد تم اللجوء إلى سوق آخر أكثر سهولةً، وأسرع اتصالاً، وهو "السوق الالكترونية"، ونتيجة لذلك فقد تعقّدت الحياة التجارية بشكل واضح، قد جعل الكثير من المتعاملين، ليس لديهم ما يكفي من الخبرة الكافية، للإحاطة الكاملة بالعقود والمعقود عليه، ومواصفاته وعيوبه، ومدى فعاليته وخطورته، لذلك وضعت التشريعات الحديثة، وسائل متعددة لحماية المستهلك، ومن تلك الوسائل "الالتزام بالإعلام في العقود"، وخاصةً العقود الالكترونية، لما لها من طابع خاص، حيث تتم عن بعد, ومن خلال وسائل الكترونية حديثة عبر شبكة الإنترنت، والموقع الالكتروني Web Site[٣].

ويعرف الموقع الالكتروني وفقاً للفقه الفرنسي بأنه:{ عمل جماعي لتقديم المعروض من الخدمات عبر شبكة الإنترنت، ويحمل في طياته العديد من مختلف الأعمال، التي من الممكن حمايتها بعدة طرق، كقانون حماية الملكية الفكرية، وحماية العنوان الإلكتروني أو العلامة التجارية}[٤]، حيث يشمل قاعدة بيانات المنتجات، وهو المكان الذي يتم فيه تخزين كافة المعلومات عن السلع المتواجدة بالمتجر الالكتروني، وجزء من هذه المعلومات يكون متاحاً للعملاء المستهلكين، وذلك من أجل إدارة كتالوجات المنتجات, والبحث عن فئة معينة, وتقوم ما تسمى ب.."عربة التسوق الإفتراضية" Virtual trolley بالسماح للعميل، باختيار

---

١ د. محمد حجازي، جرائم الحاسابات والانترنت (الجرائم المعلوماتية)، المركز المصري للملكية الفكرية، ٢٠٠٥، ص ١.

٢ د.عماد الشربيني، القانون التجاري الجديد لسنة ١٩٩٩، الكتاب الأول، الالتزامات والعقود التجارية، بدون دار نشر، ٢٠٠٠، ص ١٩٢.

٣ د.عقيل فاضل حمد الدهان ، د.غني ريسان جادر الساعدي، الالتزام بالإعلام في العقد الالكتروني، مجلة أهل البيت، العدد الخامس، كلية القانون، جامعة البصرة، ٢٠١٧، ص ١.

4 Michelle & Philippe Jean – Baptiste, Le marketing en ligne, Guide pratique, Eyrolles, Editions d' organization, p 52.

المزيد من المنتجات والخدمات[١]، الكائنة بالموقع الالكتروني "المتجر الالكتروني"[٢]، مع بيان السعر والكمية والوصف، وهو ما أوضحه قانون المعاملات الالكترونية المصري رقم ١٥ لسنة ٢٠٠٤، وقانون المعاملات والتجارة الالكترونية الإماراتي رقم ٢ لسنة ٢٠٠٢.

ولقد عرف مشروع قانون التجارة الالكترونية بولاية "لوكسمبورج"، في المادة الأولى المخصصة للتعريفات بالتجارة الالكترونية، بأنها:{ كل استعمال لوسيلة من وسائل الاتصال الالكترونية لتجارة السلع والخدمات، باستثناء العقود المبرمة بطريق اتصال تليفوني شفهي أو باستخدام التصوير)[٣]. كما عرف مشروع قانون التجارة الالكترونية المصري, في المادة الأولى، "التجارة الالكترونية" بأنها: {كل معاملة تجارية تتم عن بعد باستخدام وسيلة الكترونية}، إلا أنه لم يحصر المشرع المصري التجارة الالكترونية بوسيلة معينة مثل الانترنت, وذلك لسرعة تطور الوسائل الالكترونية[٤].

وبناء عليه فإن التجارة الالكترونية، تتمثل في عرض للسلع والخدمات على موقع الانترنت، ليحصل على طلبات العملاء، بحيث تشمل جميع المعاملات التي تتم عبر الانترنت، حتى ولو لم تتمتع بالصفة التجارية، وإن كان من الغالب؛ أن تتمتع بهذه الصفة من طبيعة السلعة أو الخدمة على الأقل، والذي غالباً ما يكون صاحبها تاجراً[٥].

ولا تختلف "التجارة الالكترونية" عن "التجارة العادية"، سوى فقط في الوسائل التي يتم فيها إجراء التبادل التجاري للسلع والخدمات، وذلك من حيث تسهيل التعامل، وإجراء تلك المبادلات عن بعد، دون

---

١ د.إلهام محمد حامد إبراهيم, المتجر الالكتروني، رسالة دكتوراه، كلية الحقوق, جامعة المنصورة، ٢٠١٦، ص ١٧٥.

٢ والمتجر الالكتروني هو صورة حديثة للمتجر بصورته التقليدية، ويعرف "المتجر" بصورة عامة وفقاً للمادة رقم ٣٤ من القانون التجاري المصري بأنه: { مجموعة من الأموال المنقولة تخصص لمزاولة تجارة معينة، ويجب أن يتضمن عنصر الاتصال بالعملاء والسمعة التجارية}، ويتضح من النص أن المتجر يتركب من منقولات، فلا يدخل العقار في تركيبه، ولو كان صاحب المنشأة يملك العقار الذي يمارس فيه التجارة, وقد يتركب المتجر من منقولات معنوية ومادية، أو من منقولات معنوية فقط، ولكن لا يجوز أن يتركب من منقولات كلها مادية، ومن المنقولات المعنوية (السمعة التجارية – الاسم التجاري – العلامات التجارية – براءات الاختراع والرسوم والنماذج الصناعية – حقوق الملكية الأدبية والفكرية)، أما المنقولات المادية فهي كالسلع والأثاث والآلات والأجهزة والمعدات.

– د.عماد الشربيني، مرجع سابق، ص ٢٦.

3 Tomas Jon, Electronic telephonic trade , Paris, Dalloz ,1990 . p 25

٤ د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة ، مجموعة أعمال المؤتمر المنعقد في الفترة من ١–٣ مايو ٢٠٠٠.

الحاجة إلى التواجد المادي، فهي مبادلات تجارية تتم عن طريق وسائل الكترونية[١].

ونتيجة لما سبق، نجد أنه تتطلب تلك المعاملات التجارية الالكترونية، تبادل بيانات المتعاملين، واستخدام الوثائق الالكترونية، عن طريق مورد الخدمات الالكترونية.

وبالتالي يتعلق الأمر ببيانات تخص العملاء المستهلكين، مما يحتاج إلى الحماية، في مواجهة الإطلاع على تلك البيانات الاسمية والشخصية، ضد الاستغلال غير المشروع لها، إذ أن تلك البيانات، قد يكون من شأنها، أن ترسم أو تعطي تصوراً لمسلك صاحبها، أو ميوله، أو اهتماماته، ونمط تفكيره، بما قد يتم استغلاله للإضرار به، سواء بصورة مباشرة أم غير مباشرة, خاصةً إذا كان الشخص المعني بالبيانات "شخص اعتباري"، فيمكن استغلال بياناته في المنافسة التجارية، بما يحقق جريمة "المنافسة غير المشروعة والاحتكار"، خاصةً عند استغلال الاسم التجاري أو العلامة التجارية، باعتبار أنهما يعتمدان على البيانات الشخصية والاسمية (كما أوضحنا من قبل).

لذا يحظر تسويق البيانات الشخصية للأغراض التجارية، دون الحصول على موافقة الشخص صاحب البيانات، وأن يتضمن اتصال التسويق الالكتروني هوية صاحب الاتصال، وعنوانه، والإشارة إلى أن الاتصال الالكترونية مرسلاً لأغراض التسويق المباشر, مع وضع آليات تمكن الشخص المعني بالبيانات من رفض الاتصال الالكتروني[٢].

صور التجارة الالكترونية. لقد أخذت الأنشطة التجارية, التي تتم عبر الإنترنت ازدياداً يوماً تلو الآخر، إلى أن ظهرت التجارة الالكترونية، كأحد روافد ثورة تكنولوجيا المعلومات، مما أدى إلى تضاعف أعداد مستخدمي شبكة الإنترنت، ما بين مستخدم وصاحب موقع وبائع ومشتري، وذلك لكونها شبكة لا حدود لها زمنية لها ولا مكانية، مما دفع بالعديد من التجار (الذين أرادوا أن يثبتوا وجودهم في سوق المنافسة العالمية) أن يتوجهوا بنشاطهم التجاري إلى شبكة الإنترنت[٣]، وأصبح بإمكان كل مشروع، أن يمتلك موقعاً خاص به، كي يعرض من خلاله كل ما لديه من سلع وخدمات، والتفاعل والتواصل مع المستهلك، ومن ثم القدرة على التعاقد على تلك المنتجات مع جمهور المستهلكين[٤].

---

١ د. طاهر شوقي مؤمن، خدمة الاتصال بالإنترنت، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، أكتوبر ٢٠١٢، الجزء الثاني، العدد ٥٢، ص ٣٥١.

٢ المستشار. مصطفى الصديق إبراهيم خورشيد، الحماية القانونية لحقوق المؤلف علي مصنفاته الرقمية في بيئة الانترنت,"دراسة مقارنة في التشريع المصري والاتفاقيات الدولية "، بحث مقدم للمؤتمر العلمي الخامس للمعهد القومي للملكية الفكرية، ٢٦ ابريل ٢٠٢٢، ص ٢٥ : ٢٧.

٣ د. إلهام محمد حامد إبراهيم، مرجع سابق، ص ٣.

4 Ropert Neumann, The electronic business foundation, Master Thesis, OTTO – VON, Guericke Magdeburg, Germany, p 16.

ولذلك فقد بدأت الحماية التشريعية للمعلومات والبيانات المخزنة، ضمن برامج الحاسب الآلي بصورة عامة، في الاتفاقيات الدولية, سواء كانت تلك البيانات والمعلومات شخصية أم تجارية، ولكن لأغراض حماية البيانات والمعلومات التجارية؛ فقد تم تجريم صور عديدة للعدوان على تلك المعلومات، مثل تجريم الدخول غير المشروع إلى حاسوب الغير وبرامجه، عبر الانترنت، أو تجريم حذف بعض البيانات أو المعلومات التجارية، أو تعديلها أو تبديلها أو إتلافها[١]، كذلك حماية تلك المعلومات من التزوير أو التقليد.

ولعل جريمة التزوير تتخذ طابع خاص في جرائم الحاسب الآلي، وذلك لعدم تطلب ركن المحرر بصورة مادية، وإنما بصورة حكمية، وذلك هو الجديد في نصوص التجريم الذي خرج به المشرع عن نصوص التجريم التقليدية، وفقاً لما صدر بالقانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بمكافحة جرائم تقنية المعلومات، حيث تعد أفعال التزوير أو التقليد، وصور الاعتداء على البيانات والمعلومات التجارية، محققة لجريمة التزوير في الغالب، وانتهاك الأسرار التجارية، كنتائج الأبحاث والاختبارات، الجارية على بعض السلع، قبل وضعها في الأسواق[٢].

وهنا تتساءل الدراسة عن؛ كيفية التعاقد عبر الإنترنت؟. يتم عرض السلع والمنتجات على شبكة الإنترنت من خلال ما يلي :-

١. تتم التجارة للبضائع عبر شبكة الإنترنت، من خلال بيع وشراء البضائع التجارية بالأجهزة الالكترونية، كالحاسب الآلي وأنواعه المختلفة، والهواتف المحمولة، وذلك عن طريق عرض صورها من قبل التاجر، سواء بطريق عمل "جروب على برنامج واتس آب"، أم بعرض المنتجات على "الفيس بوك"، أم بعمل موقع خاص بالتاجر, يتضمن صفحة خاصة به، ويشترك عليها العملاء من جميع الدول، بحيث يرى العميل صورة المنتج، ويبدي إرادته ورغبته في قبوله بالشراء، وذلك عن طريق الضغط بالقبول والتأكيد عليه[٣].

٢. الفاترينة الخاصة بموقع المتجر الالكتروني: تلك التي تشغل حيزاً على موقع المتجر بالذاكرة المعلوماتية، الخاصة بمستضيف الموقع (Hosting)، بشكل يسمح بالإطلاع عليها في كل وقت.

٣. اللافتة الإعلانية: يقوم مالك الموقع التجاري، بتأجير حيز دعائي بالفاترينة، وذلك في شكل شريطي

---

١ د. عبد الله الخشروم، عقود التجارة الالكترونية عبر شبكة الإنترنت، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، الكتاب الثالث، أكاديمية شرطة دبي بالإمارات، خلال الفترة من ٢٦ إلى ٢٨ ابريل، عام ٢٠٠٣.

3 For more on the content of this ; Ahmed Sarhan – Ehab Abiu Aish, The impact of attitude towards electronic word of mouth on Egyptian consumers, The Egyptian Journal for Commercial Studies, Mansoura University, Faculty of Commerce, Vol 36, No 4, Part 2, 2012.

٣ د. كيسي زهيرة، الإطار القانوني للتعبير عن الإرادة في العقود المبرمة عبر الإنترنت، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لتامنغست، الجزائر، بدون سنة نشر، ص ١٠.

أفقي أو رسوم متحركة على الصفحات الخاصة، وبالتالي حال زيارة أي مستخدم للإنترنت إلى تلك الفترينات، يرى الدعاية عن السلع والخدمات المعروضة.

٤. الروابط التجارية: وهي ما تظهر في محركات البحث، عندما يتزامن محتواها مع الكلمات التي يختارها المعلن مسبقاً، وبذلك فهي وصف موجز في هامش الصفحات العامة، التي تهم في نتائج محركات البحث، ويطلق عليها أيضاً "محتوى الصفحة"، أو "سياق الصفحة الخاصة بمالك المتجر".

٥. دليل الإنترنت: وهي وسيلة تعمل كفاترينة لدى مالك المتجر عن جمهور المستخدمين، فهو من أهم الوسائل الدعائية، والذي يتم التسجيل عليه، بناء على المعلومات التي يقدمها مالك المتجر، وعليه يجب أن تتميز هذه المعلومات بالمصداقية، والأمانة التجارية، حيث لا يعمل الدليل الإلكتروني على التحقق من تلك المصداقية، ومن أمثلتها(ALLTAVISTA – EXCIT) YAHOO. وكتطبيق عملي على ذلك؛ نجد أن شركة (Medical Marketing Service) قد قامت بعملية بيع قوائم تتعلق بالأفراد الذين يعانون أمراضاً معينة، وتتضمن هذه القائم قائمة ببياناتهم الشخصية، لتحقيق عوائد مادية[١].

٦. قائمة العناوين الالكترونية للعملاء: وهي التي تعمل على إرسال مالك المتجر لعروض أو دعايات عن السلع والخدمات الخاصة به، إلى صناديق البريد الالكتروني للعملاء المحتملين، وذلك من خلال تعرفه على قائمة عناوينهم الالكترونية، التي تظهر على موقعه، ويتم إرسال تلك العروض دون موافقتهم المبدئية[٢].

ومن المفترض تحلي مسئول معالجة البيانات في المعاملات الالكترونية، بالأمانة والمشروعية، وعدم إطلاع الغير عليها، ومسحها بعد انقضاء الغرض منها.

إذ أن الوقت مقدر بكل جزيئاته، خاصة في مثل هذه المعاملات التجارية الالكترونية، فهناك توقيت لعملية التخزين، وتوقيت لعملية المعالجة، وهو ما نصت عليه المادة رقم ٢٨ من قانون المعلوماتية والحريات الفرنسي، بحيث لا يجوز الاحتفاظ بالبيانات الشخصية، إلا للمدة المحددة في طلب إقامة نظم المعلومات، أو لمدة تزيد على المدة اللازمة لتحقيق الغرض من تجميع البيانات, واحتياجات البرنامج، إلا إذا سمحت "اللجنة القومية للمعلوماتية والحريات"، بالاحتفاظ بهذه المعلومات أكثر من المدة المحددة، وبالتالي فإنه يتحقق الركن المادي لتلك الجريمة، إذ ما احتفظ المسئول عن جمع ومعالجة البيانات، بما تمت معالجته

---

١ د.سارة الشريف، خصوصية البيانات الرقمية، سلسلة أوراق الحق في المعرفة، الإصدار الثالث، مركز دعم تقنية المعلومات، ٢٠١٤، ص ٤.

2 Constancias Claire, Mavault Laureen, La publicites sur internet, Sans maiso d' éditions, 2010 , p 4 -6.

آلياً، أكثر من المدة المطلوبة للحفظ، والمحددة في القانون، بحيث تجاوز تلك المدد، بما يضر بسمعة أصحاب البيانات، ولو كانت بيانات غير مهمة.

وتطبيقاً على كيفية الاعتداء على البيانات الشخصية الرقمية في التجارة الإلكترونية، نجد أنه قد أفرزت التجارة الالكترونية الحديثة، ما يعرف ب"الوكالة الالكترونية"، والتي يقوم بها "الوكيل الالكتروني"، وهو عبارة عن برنامج خاص، من برامج الحاسب الآلي، يقوم بعمل ما نيابةً عن الشخص الذي يستخدم الحاسب الآلي، ويكون له في قيامه بهذا العمل قدراً من الاستقلالية، فلا يتطلب قيامه بهذا العمل تدخلاً مباشراً من الشخص الذي يمثله، وينظم ذلك نصوص القانون المصري الخاص بتقنية المعلومات، رقم ١٧٥ لسنة ٢٠١٨.

وقد عرف قانون التجارة الالكترونية الإماراتي رقم ١ لسنة ٢٠٠٦، "الوكيل الالكتروني" بأنه: {برنامج أو نظام الكتروني لوسيلة تقنية المعلومات، تعمل تلقائياً، بشكل مستقل جزئياً أو كلياً، دون إشراف من أي شخص طبيعي}[١].

وقد تتمثل مهامه في البحث عن معلومات حول سوق معينة، أو مراقبة المستجدات التي تحدث عبر شبكة الإنترنت، في نوع معين من المعلومات، عن شركات منافسة مثلاً، وقد يقوم هذا الوكيل الالكتروني بالمساعدة في إنجاز أعمال فنية، عن طريق جهاز الحاسب، كالقيام بفلترة بريد المستخدم، من حيث الترتيب بالتاريخ أو الأهمية مثلاً، وقد يقوم هذا الوكيل بتصرفات قانونية، كالتفاوض في العقود وإبرامها وتنفيذها، ولا يكون الوكيل الالكتروني وكيلاً عن البائع فقط، بل من الممكن أن يكون وكيلاً عن المشتري، في تحديد الأفضل له من بين المنتجات المنافسة، من حيث السعر والجودة، وذلك من خلال عقد مقارنة بين السلع المتنافسة، ويقوم بتمثيل البائع من خلال عرض بضائعه، وتلقي الطلبات عنها، والتعاقد على بيعها واستلام الثمن وتسليم المبيع, ويحدد فئة المشترين المستهدفة، بحيث يعرض منتجاته عليهم، وذلك من خلال تسجيل السيرة الذاتية، ومفضلات كل مشتري، عن طريق البيانات التي يزود بها المشتري الموقع, خلال عملية الشراء، وتسجيل الطلبات المتتابعة التي يقدمها المشتري، وتكمن فائدة ذلك في التعرف على التطورات، التي يدخلها المشتري في طلباته كل مرة, من حيث نوعية البضائع والجودة, وشروط التسليم وطريقة السداد[٢].

وبالتالي نجد أنه يتم الاتجار بالبيانات الشخصية، من خلال بيع السيرة المهنية "البروفايل"، للمشترك،

---

١ د. آلاء يعقوب النعيمي، الوكيل الالكتروني، مفهومه وطبيعته القانونية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد ٧، العدد ٢, ٢٠١٢، ص ١٥٥.

٢ د. شريف محمد غنام، دور الوكيل الالكتروني في التجارة الالكترونية، دار الجامعة الجديدة، ٢٠١٢، ص ٢٠ .

بمقابل نقدي، وذلك إلى شركات التسويق الالكتروني عبر الإنترنت[١].

كذلك يقوم الوكيل الالكتروني بالمقارنة بين "المنتجات محل الوكالة" و"المنتجات المتنافسة معها"، ويقدم توصيات للبائع الذي يعمل وكيلاً له، تتعلق بأذواق المستهلكين، وتطور العروض المقدمة منهم، وإحصائية بأكثر السلع المبيعة، وكذلك سبب الزيادة في المبيعات أو نقصها، واقتراح علاج المشكلات، ويحصل البرنامج على نسبة من المبيع[٢].

ولعل طبيعة الوكيل الالكتروني (كبرنامج الكتروني) تجعله قد يصاب بفيروس، أو عملية قرصنة، تهدد تجارة البائع، حيث يكون هو المسئول أمام الغير، وهو ما لا يحدث بالنسبة للوكالة التجارية العادية[٣].

وبالتالي فإن البيانات الشخصية المدونة على الحاسب، تستطيع الشركات التجارية من خلالها، معرفة التفاصيل الشخصية لهذا الشخص، مثال على ذلك أيضاً، تلك البيانات الوصفية على الهاتف الذكي، والتي تسجل معلومات حول زمن المكالمات والرسائل، ومدتها، ونطاقها الجغرافي[٤]. وغيرها من البيانات، التي يمكن أن تسمح في النهاية، بالتوصل إلى استنتاجات دقيقة، بشأن الحياة الخاصة للشخص، ومن ثم؛ فإن بيانات الاتصالات، تعتبر بيانات شخصية، مما لا يجوز الاطلاع عليها، دون إذن أو سماح، من قبِل صاحبها، وإلا اُعتبر اعتداء على خصوصية الشخص، من حيث بياناته الشخصية الرقمية[٥].

---

١ د.جبالي أبو هشيمة كامل، حماية البيانات الشخصية في البيئة الرقمية، مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق، جامعة أسيوط، الفترة من ١٢:١٣ ابريل ٢٠١٦، ص ٣٠.

2 Emily M . Weitzenbock, Electronic Agents and the Formation of Contracts, The International Journal of Law and Information Technology ,Vol.9 No.3, pp. 204-234, Journal website at :http// www3.oup.co.uk.inttec. Oxford University Press, 2001,P 1 ,3.

-Oren Etzioni ,Daniel S. Weld ,Intelligent Agents On The Internet , Department of Computer Science and Engineering , University of Washington, May 30, 2005 , P 3 .

3 Giovanni (S), Agent in cyber law, in "Workshop on the law on electronic agent", LEA, 2002, p 54.

٤ دراسة قامت بها جامعة اكسفورد، بعنوان {انتهاء عنصر الخصوصية – ٨ تغريدات على تويتر كافية لتحديد المتلصصين على موقعك}، جريدة الشرق الأوسط، العدد رقم ١٣٦٩٩، بتاريخ ٢٠١٦/٥/٣١. منشور على الرابط الالكتروني الآتي: http://aawsat.com/home/article. visited on 3/5/2023.

٥ وفي ضوء ذلك، حكمت محكمة العدل الأوربية، لصالح طالب نمساوي, يدعى "ماكس شريمز"، كان قد رفع دعواه ضد شركة فيسبوك، مدعياً أنها تنقل البيانات الشخصية إلى خوادمها في الولايات المتحدة، مشيراً إلى وجود وثائق، قد استند إليها، سربها موظف سابق بوكالة الأمن القومي في أمريكا، بما يمثل تجسساً من قبِل أجهزة الاستخبارات الأمريكية. وأكدت المحكمة بصدد ذلك، أم الدول الأعضاء في الاتحاد الأوربي، يجب عليها التحقيق في تلك الشكاوى بشكل

المبحث الثاني

نطاق الحماية الدولية للبيانات الشخصية الرقمية

تمهيد وتقسيم:

انعقدت العديد من المؤتمرات الدولية، لبحث موضوع الحق في الحياة الخاصة، وما يتعرض له من أخطار بسبب التطورات العلمية والتكنولوجية الحديثة، وأصدرت عدة توصيات تتعلق بحماية هذا الحق، ومنها "**المؤتمر الدولي لحقوق الإنسان المنعقد في طهران**" (والذي انعقد في الفترة من ٢٢ ابريل إلى ١٣ مايو ١٩٦٨، بمقتضى القرار رقم "٢٨١" الصادر من الجمعية العامة للأمم المتحدة، في ٢٠ ديسمبر ١٩٦٥)، وذلك كجزء من "البرنامج العام الدولي لحقوق الإنسان" لعام ١٩٦٨[١].

وتناول المؤتمر المشكلات المرتبطة بأنشطة الأمم المتحدة، التي تهدف تأكيد احترام حقوق الإنسان وحرياته الأساسية[٢]، وتجدر الإشارة؛ أنه يعتبر القرار رقم ١١ الذي تبناه المؤتمر بالإجماع في ١٩٦٨/٥/١٢، من أهم قرارات حماية حق الإنسان في حياته الخاصة، حيث أكد ضرورة احترام السرية بالنسبة إلى أساليب التسجيل، وحماية الشخصية وتكاملها المادي والعقلي[٣].

ونتحدث في نطاق الحماية الدولية للبيانات الشخصية الرقمية، عن حقوق صاحب تلك البيانات، والضوابط التي تقيد عملية المعالجة الإلكترونية للبيانات الرقمية، إضافة إلى ضوابط نقل البيانات الشخصية الرقمية خارج نطاق الدولة. وذلك من خلال المطالب الآتية:-

المطلب الأول: حقوق صاحب البيانات الرقمية.

مستقل، ولها حق حظر الشركات الناقلة للبيانات. وهو ما يعتبر ضربةً قوية لعمليات المراقبة العالمية للولايات المتحدة،التي تعتمد فيها على شركات القطاع الخاص.

١ ونشير هنا إلى قرار الجمعية رقم ٦٨/١٦٧ الصادر بتاريخ ١٨ ديسمبر ٢٠١٣ بعنوان الحق في الخصوصية في العصر الرقمي، وذلك عقب فضيحة ادوارد سنودين المتعاقد مع وكالة الأمن الوطني NSA الأمريكية، لما قام بتسريبه من وثائق إلى الصحافة من خلال برنامج بريسم التجسسي.

د.بولين انطونيوس ايوب، الحماية القانونية للحياة الشخصية في نجال المعلوماتية، منشورات الحلبي القانونية، بيروت،٢٠٠٩، ص٣٢٠.

٢ د.عبد الرحمن جمال الدين حمزة، الحق في الخصوصية في مواجهة حرية الإعلان، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنوفية، ٢٠٠٢، ص١٠٢.

٣ د.آدم عبد البديع آدم، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكلفها له القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٠٠، ص١١١.

المطلب الثاني: أحكام معالجة البيانات الشخصية الرقمية.

المطلب الثالث: أحكام نقل البيانات الشخصية خارج إقليم الدولة.

المطلب الرابع: سياسة المواقع والتطبيقات الإلكترونية لحماية البيانات الشخصية الرقمية.

المطلب الأول

حقوق صاحب البيانات الرقمية

لصاحب البيانات الرقمية عدة حقوق أقرتها الأحكام القضائية الدولية والاتفاقيات الدولية، وذلك كالآتي:

أولاً: رضاء الشخص المراد معالجة بياناته:

حيث نصت "اللائحة العامة الأوربية لحماية البيانات الشخصية"، في المادة رقم ٩ منها, على أن:{ معالجة البيانات الشخصية، التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية، أو العضوية في النقابات، ومعالجة البيانات الجينية أو البيانات المتعلقة بالصحة، والبيانات المتعلقة بالحياة الجنسية، أو الميل الجنسي للشخص، ينبغي أن تكون محظورة، إلا إذا وافق صاحب البيانات موافقة صريحة بمعالجتها}[١]، وهو ما توافق معه قانون حماية البيانات الشخصية المصري، رقم ١٥١ لسنة ٢٠٢٠[٢]، حيث نجد أنه نصت المادة رقم ٢ منه، على أنه لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو الإفشاء، بأي وسيلة من الوسائل، إلا بموافقة صريحة من الشخص صاحب البيانات.

كذلك أكد المشرع الفرنسي (المادة رقم ٧٨-١٨ لسنة ١٩٧٨) بوجوب حصول المسئول عن معالجة البيانات الشخصية، على موافقة الشخص المراد معالجة بياناته الشخصية، وأن يلتزم الشخص المسئول عن معالجة البيانات "المعالج"، بتوفير الحماية القانونية للحياة الخاصة لهذا الشخص صاحب البيانات[٣]، على أن تكون الموافقة صريحةً وكتابية، فالشخص المعني بجمع بياناته الشخصية، هو وحده من يملك حق التحكم في عملية جمع المعلومات، ومعالجتها آلياً، وحفظها وتوزيعها.

ويمتد ذلك الحق أيضاً إلى الورثة، بحيث يكون لهم الحق في الدخول إلى البيانات الخاصة بمورثهم، وذلك وفقاً لما قرره "مجلس الدولة الفرنسي"، في حكمه الصادر بتاريخ ٢٠١١/٦/٢٩، وذلك

---

1 Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. Online behavioral advertising: A literature review and research agenda. Journal of advertising, 46(3), 363-376. 2017, p. 364.

٢ الجريدة الرسمية، العدد ٢٨ مكرر (هـ)، السنة ٦٣، بتاريخ ٢٠٢٠/٧/١٥.

٣ د. مصطفى إبراهيم العربي خالد، مظاهر الحماية الجنائية للحق في النسيان الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، الجمعية العربية لعلوم الأدلة الجنائية والطبي الشرعي، جامعة نايف العربية للعلوم الأمنية، المجلد الثاني، السنة ٢، ٢٠٢٠، ص٢١٣.

بمناسبة قيام ورثة بتقديم طلب إلى جهة الإدارة، للإطلاع على الملف الخاص بعمتهم، والمتعلق بحساباتها البنكية، لتصفية التركة، وسداد ما عليها من ديون، إلا أنه قد رفضت جهة الإدارة هذا الطلب، فلجأ الورثة إلى محكمة القضاء الإداري الفرنسي، وحكمت بإلغاء قرار الإدارة، وطعنت الإدارة، وحكم مجلس الدولة برفض الطعن، لمخالفته للمادة رقم ٢ و٣٩ من القانون رقم ١٩٧٨/١/٦[١].

ثانياً: الحق في الاتصال أو النفاذ إلى البيانات الشخصية.

يقصد بهذا الحق أن يكون للشخص المراد معالجة بياناته, حق الإطلاع على جميع المعلومات الشخصية الخاصة به، وطلب تصحيحها وتعديلها، أو تغييرها، أو إيضاحها إذا كانت غامضة، أو شطبها إذا كانت خاطئة (المادة رقم ٢ من قانون حماية البيانات الشخصية المصري، فقرة ٢و٣). وكذلك حق الحصول على نسخة من المعلومات، وذلك بلُغة واضحة، ومطابقة لمضمون التسجيلات، وبطريقة مبسطة إذا تمت معالجتها آلياً[٢].

وذلك للتأكد عما إذا كانت بياناته الشخصية، تخضع إلى المعالجة الآلية أم اليدوية، من عدمه، وأيضاً التأكد من أهداف المعالجة الآلية، وعدم نقل البيانات إلى دولة غير عضو في الاتحاد الأوربي[٣].

إضافة إلى الحق في إخطاره بمعالجة بياناته الشخصية، وبأهداف تلك المعالجة، وإخطاره بأي إفشاء لبيانات شخصية غير دقيقة، والحصول على نسخة من بياناته الشخصية، بعد سداد الرسوم المقررة لذلك مقابل الخدمة، ولكن استثنى المشرع الفرنسي عدة صور للمعالجات من الالتزام بالإخطار، وهي كالآتي:-

- المعالجات التي تهدف إلى إنشاء سجل أو دفتر، بموجب قواعد قانونية، ويكون الهدف من هذا السجل إعلام الكافة، أو أي شخص له الحق في الحصول على معلومة منه، طالما أن له مصلحة مشروعة(المادة رقم ٢٢ من القانون الفرنسي رقم ١٣٢١، الصادر بتاريخ ٢٠١٦/١٠/٧)، ومثال على ذلك (سجل قيد الزراعيين – السجل التجاري الخاص بالتجار)[٤].

- المعالجات التي تتم بواسطة الجمعيات أو الهيئات غير الربحية، وتتعلق بالمعتقدات الدينية

---

1 Ch. Caron, Appréciation de l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile, Comm., JCP E, n° 9, 28 Février 2008,P 1270.

2 Ch. Caron, Appréciation de l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile, Comm., JCP E, n° 9, 28 Février 2008,P 1270.

٣ الهيئة الوطنية للأمن السيبراني، مذكرة إرشادية حول النظام الأوربي لحماية البيانات الشخصية، ٢٠١٩، ص ١٠. متاح على الموقع الإلكتروني : http://www.gdbr@nca.gov.sa.visited on 19/10/2023

4 Benoit Tabaka et Yann Tesar, Loi informatique: un nouveau cadre juridique pour le traitement des données à caractère personnel, Dossier, 2004, p. 45.

والآراء، والانتماء النقابي لأعضائها، بحيث تقتصر المعالجة على الأعضاء فقط (المادة رقم ٨).

– المعالجات التي تتم في إطار التعبير الأدبي أو الفني، أو في إطار ممارسة مهنة الصحافة، بشرط احترام القواعد المهنية (المادة رقم ٦٧).

وتجدر الإشارة إلى أنه يمتد نطاق هذا الحق إلى كافة البيانات والمعلومات الشخصية المعالجة والمخزنة، والتي تخص صاحب شهادة التصديق الالكتروني، ويتضمن هذا الحق أيضاً، حق الاعتراض على معالجة البيانات التي قد تؤدي إلى ضرر ما (كأن تنال من حرية أو حقوق صاحب البيانات)، على أن يكون حق الاعتراض مقيداً بأسباب مشروعة وجدية، ويشمل هذا الحق الدخول إلى جميع مواقع البيانات الشخصية المتعلقة بالشخص، الذي جمعت عنه، وعليه وضع وسائل التقنية المناسبة، لتمكينه من ذلك بطريقة الكترونية، بحيث يلتزم المسئول عن جمع ومعالجة البيانات، بأن يوفر جميع الوسائل الفنية المناسبة، ليتمكن صحاب البيانات من النفاذ إليها.

ثالثاً: الحق في النسيان الرقمي للبيانات الشخصية:

يعرف هذا الحق بالحق في المحو للبيانات من محرك البحث[١]، فقد يتم تسجيل البيانات الشخصية، على محركات البحث المختلفة، مثل (جوجل وياهوو)، وما إلى ذلك من محركات، وتكون هذه البيانات عرضة للتداول والنقل بين العديد من المستخدمين، الذين تسمح لهم المحركات بالدخول إلى هذه البيانات، مما يسبب قلقاً لأصحاب هذه البيانات، لتدولها ونقلها، دون رضاء صادر منهم.

ولذلك يعرف الحق في النسيان، بأنه الحق في أن يتحكم الشخص صاحب البيانات في بياناته الشخصية، وأن يقرر في أي وقت حذفها، أو محوها كلية من مواقع الإنترنت[٢].

وقد نصت المادة رقم ٨ من التوجيه الأوربي، على إقرار الحق في النسيان، كأحد الحقوق المقررة لصاحب البيانات الشخصية[٣].

كما ترسخ الاعتراف بذلك الحق تشريعياً أيضاً، بموجب اللائحة العامة الأوربية لحماية البيانات General Data Protection Regulation (GDPR)، رقم ٦٧٩، الصادرة عن المجلس الأوربي،

---

١ د. مصطفى إبراهيم العربي خالد، مظاهر الحماية الجنائية للحق في النسيان الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، الجمعية العربية لعلوم الأدلة الجنائية والطبي الشرعي، جامعة نايف العربية للعلوم الأمنية، المجلد الثاني، السنة ٢٠٢٠، ص٢٠٦.

٢ د.عبد الهادي فوزي العوضي، الحق في الدخول في طي النسيان الرقمي على شبكة الإنترنت، دار النهضة العربية، ٢٠١٣، ص ٢٥.

٤ أ. أثير فاضل عباس رضا، التنظيم الدولي لحماية البيانات ذات الطابع الشخصي، رسالة ماجستير، كلية القانون، جامعة بابل، العراق, ٢٠٢٠، ص١٥.

والبرلمان الأوربي، عام ٢٠١٦ [١]، وأيضاً توصية الهيئة الاستشارية الأوربية G29، الخاصة بسمح البيانات الشخصية، خلال فترة لا تتجاوز ٦ شهور من تاريخ وقف تفعيل الموقع أو الحساب الالكتروني للمستخدم[٢].

كذلك أكدت على هذا الحق "محكمة باريس الابتدائية"، في حكمها الصادر بتاريخ ٢٠١٢/٢/١٥، بخصوص قضية السكرتيرة التي كانت تقوم بتصوير أفلام إباحية، وعندما أرادت العمل كمستشارة قانونية بإحدى المؤسسات، أرادت أن تمحو تلك الفيديوهات، وطلبت ذلك من مخرج هذه الأفلام، والذي رفض، فرفعت دعواها أمام هذه المحكمة، مطالبة شركة جوجل، بمحو وإزالة جميع الروابط الإلكترونية المتعلقة باسمها ولقبها، واستجابت المحكمة لطلبها، وألزمت شركة جوجل بدفع غرامة ألف يورو، وذلك عن كل يوم تتأخر فيه عن إزالة تلك الروابط[٣].

إضافة إلى قرار محكمة العدل الأوربية، رقم ١٢/١٣١، الصادر عام ٢٠١٤، في قضية المواطن الإسباني "ماريو كوستيجا غونزاليس"Mario Costeja Gonzalez ، الذي تقدم بشكوى إلى وكالة حماية البيانات الأساسية Agencia Española de Protección de Datos (AEPD)، ضد Google Inc و Google Spain، وصحيفة لافانجارديا La Vanguardia، وذلك لأنه عندما يدخل أي شخص إلى محرك البحث جوجل، سوف يجد إعلان قديم له متعلق ببيع بيته بالمزاد العلني، وما حدث بشأن إجراءات الحجز لاسترداد ديون الضمان الاجتماعي المدين بها، وأنه قد سدد تلك الديون، ولا داعي لوجود هذا الإعلان حتى وقت تقديم الشكوى، بحيث يتم إخفاء ومحو ذلك الإعلان، حتى لا يتم تضمينه في نتائج البحث، ولا تظهر للمستخدمين، وقامت شركة جوجل باستئناف هذا القرار أمام المحكمة الوطنية الإسبانية، والتي أوقفت الدعوى وأحالتها إلى "محكمة العدل"، التابعة للاتحاد الأوربي، طالبة تحديد ما إذا كانت نصوص التوجيه الأوربي ٩٥/٤٦، الصادر عن البرلمان الأوربي بتاريخ ١٩٩٥/١٠/٢٤، بشأن حماية الأفراد، فيما يتعلق بمعالجة البيانات الشخصية، هل يمكن تطبيقها باعتبار أن مقر شركة جوجل، يقع خارج الدائرة الجغرافية لدول الاتحاد الأوربي؟ وقد انتهت المحكمة بأنه يمكن تطبيق هذه النصوص على الشركة لأن لها فروع تدخل في النطاق الجغرافي للاتحاد الأوربي[٤].

---

1 General Data Protection Regulation. "Commission Nationale de l'Informatique et des Libertés"(CNIL) ،https://www.cnil.fr/en/official-texts. Visited on 13/5/2023.

2 Marine DE Montecier, Le droit @ l'heure des réseaux sociaux ,Mémoire, HEC, Université Paris I– Panthéon-Sorbonne Paris, 2011, P. 38.

3 Tribunal de grande instance de Paris Ordonnance de référé 15 février. (2012). https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-deparis ordonnance - de-refere-15-fevrier-2012. 13/5/2023.

4 Judgment of the court (Grand Chamber). (2014 ,May 13).http://curia.europa.eu/ juris/ document/document_print.jsf?13/5/2023.

ويرى الباحث؛ أن القانون المصري الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، لم ينص صراحةً على هذا الحق، إلا أنه ينبثق من مضمون نص المادة رقم ٢و٣ ، ما يفيد بالحق في النسيان، ويؤكد عليه.

وتتضح أهمية هذا الحق، من خلال الآتي:-

- الحكم الصادر بتاريخ ٢٠١٤/٥/١٣، من محكمة العدل الأوربية، والذي بموجبه ألزمت شركة جوجل، بمسح جميع البيانات الشخصية القديمة لمستخدميها، من جميع روابط محرك البحث جوجل، وهذا الحكم صدر نتيجة قيام رجل أسباني برفع دعوى قضائية، ضد شركة جوجل، لاكتشافه وجود بياناته الشخصية، على موقع محرك البحث جوجل، وذلك بعد مرور ١٠ سنوات، من نشره لإعلان يبيع فيه منزله، وقد لاحظت المحكمة، أن هذه الظاهرة منتشرة، وأن البيانات الشخصية للعديد من مستخدمي روابط البحث، تظل كما هي موجودة، حتى بعد انتهاء الغرض من نشره، بما يثير مسئولية الشركة حول حماية خصوصية مستخدميها، ومسئوليتها عن إزالة البيانات الشخصية لهم، بعد استيفاء الغرض من نشر تلك البيانات، وأنه يحق لأي شخص طلب مسح بياناته في أي وقت[١].

وقد أكد المشرع التونسي على ذلك الأمر، حيث استخدم لفظ وجوب إعدام تلك البيانات، بما يوحي بالتشديد بضرورة المحو الكامل لها(الفصل رقم ٤٥)، وقد نصت المادة رقم ٣٢ من قانون حماية البيانات الشخصية المصري، على أنه يجوز للشخص صاحب البيانات، ولكل ذي صفة، أن يتقدم إلى أي حائز أو متحكم أو معالج، بطلب يتعلق بممارسة حقوقه، المنصوص عليها في هذا القانون، ويلتزم المقدم إليه هذا الطلب بالرد عليه، وذلك خلال ٦ أيام عمل من تاريخ تقديمه إليه[٢].

- وتكمن أهمية هذا الحق أيضاً من خلال عرض إحصائية لمحرك البحث جوجل، خلال الفترة من ٢٠١٤: ٢٠٢٢، والتي يتضح منها أنه تلقى هذا المحرك عدد ٤٦٤.٢٧٥.١ طلباً بشأن إزالة روابط بعدد ٩٤١.٩٧٣.٤ غير مرغوب فيها، وتمت الموافقة على إزالة ٤٩٪ من تلك الطلبات، ولم يتم البت في ٥١٪ منها، مما يدل على مدى أهمية هذا الحق لصاحب البيانات الشخصية[٣].

---

1 Costeja González , JCP E 2014, act.P 374.

- Case C – 131/ 12, Google Spain SL v. Agencia Espanola de protection de Dates, 13 May, 2014., www.curia.europa.eu.22/5/2023.

٢ د.طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، دراسة مقارنة، مجلة الاقتصاد والقانون، كلية الحقوق، جامعة القاهرة، ملحق خاص بالعدد رقم ٩٢، ٢٠١٦، ص٢٥١.

٣ د.محمود زكي زكي زيدان، الحماية الجنائية الموضوعية للحق في النسيان الرقمي، دراسة مقارنة، مجلة روح القوانين، كلية الحقوق،جامعة طنطا، العدد ١٠١، الجزء الأول, يناير ٢٠٢٣، ص٣٥٣.

رابعاً: الحق في تقديم الشكوى:

لصاحب البيانات حق تقديم الشكوى، وذلك إلى السلطة الإشرافية، كمفوض للبيانات في دولته، ضد أي انتهاك لبياناته الشخصية، كذلك يحق للمعتدى على بياناته الشخصية، أن يقيم دعوى مباشرة ضد المسئول عن تجميع أو معالجة البيانات الشخصية، وذلك أمام المحكمة المختصة بدولته، كما يحق لموضوع البيانات تكليف هيئة أو منظمة أو جمعية (لا تهدف الربح)، تكون معنية بحماية حق الخصوصية في البيانات الشخصية، وتقوم بتقديم الشكوى نيابةً عن الشخص صاحب البيان المعتدى عليه[١].

وقد أكدت اللائحة العامة لحماية البيانات (GDPR)[٢] على هذا الأمر، حيث حدد سلطة مختصة بشئون البيانات الشخصية، من حيث حمايتها، وتقديم العون للمعتدي عليه، وهي جهة (DPA)، اختصاراً ل (Data Protection Authority)، وهي سلطة مختصة بحماية البيانات الشخصية، وتوجد بكل دولة من دول الأعضاء بالاتحاد الأوربي، كما أن لها سلطة الامتثال لتنفيذ اللائحة العامة لحماية البيانات، وإصدار العقوبات للمؤسسات، التي لا تلتزم بما نصت عليه اللائحة والتشريعات ذات الصلة[٣]، وقد نصت المادة رقم ٢٢ من اللائحة العامة لحماية البيانات (GDPR) على حق الاعتراض من قبل صاحب البيانات المراد معالجتها، وفي فرنسا فإنه تختص اللجنة الوطنية للمعلومات والحريات(CNIL)، بقبول شكاوى المعتدى على بياناتهم الشخصية[٤].

ويرى الباحث، أنه ينبثق "حق الشكوى" من "حق الاعتراض"، والذي يعني حق صاحب البيانات في الاعتراض على معالجة بياناته (المادة رقم ٢١ من اللائحة الأوربية لعام ٢٠١٨)، والاعتراض على عمل المسئول عن تجميع والمعالجة للبيانات الشخصية، والذي يتم وفق ضوابط معينة، يحددها كل تشريع لأسباب جدية ومشروعة، بما يترتب عليه أنه إذا لم يتم الاستجابة لهذا الاعتراض؛ فإنه يتقدم صاحب البيانات بالشكوى.

---

١ أ. أثير فاضل عباس رضا، التنظيم الدولي لحماية البيانات ذات الطابع الشخصي، رسالة ماجستير، كلية القانون، جامعة بابل، العراق، ٢٠٢٠، ص٩٦ .

٢ دخلت "اللائحة العامة لحماية البيانات (GDPR) حيز النفاذ عام ٢٠١٨، وتعد أهم لائحة لحماية البيانات الشخصية، بعد الأمر التوجيهي رقم (95/47/EC).

3 Andrew Moore, The GDPR & Managing Data Risk, John Wiley & Sons, Ltd, Great British, 2018, P.7.

٤ أ. أثير فاضل عباس رضا، مرجع سابق, ص١٠٢.

المطلب الثاني

أحكام معالجة البيانات الشخصية الرقمية

عرف المشرع الفرنسي "المعالجة الآلية للبيانات الشخصية الرقمية"، بأنها :{ واحدة أو أكثر من عمليات المعالجة للبيانات، دون النظر إلى الوسيلة المستخدمة، ويكون محلها البيانات الشخصية، بما في ذلك جمع وتسجيل وتنظيم وتخزين وتحوير، أو تعديل واسترجاع أو مراجعة هذه البيانات، أو الإفصاح عنها، من خلال إرسالها أو نشرها، بأي وسيلة أخرى، وتنسيقها للتقريب بينها} (المادة رقم ٢)، ومن ثم يتضح أن المعالجة الآلية للبيانات الشخصية الرقمية، لا تكون إلا للملفات أو البطاقات FICHIERS، والتي عرفتها المادة رقم ٢ من قانون المعلوماتية الفرنسي، بأنها:{جميع البيانات الشخصية المنظمة والثابتة للشخص، ويمكن الدخول إليها وفقاً لمعايير محددة، بما من شأنه التعرف على شخص معين}،وذلك بغض النظر عن نوع الدعامة أو الوسيلة الفنية، المثبت عليها تلك البيانات، في حين أن اللجنة الوطنية CNIL، قد اعتبرت أن مفهوم المعالجة الآلية للبيانات الشخصية الرقمية، يتطابق مع جميع المعلومات والبرامج، التي يمكن أن تساهم في تنفيذ الوظيفة الأساسية للبيانات[1].

وبالتالي يتضح أن ما يتم نشره عبر شبكة الإنترنت، من معلومات تتعلق بالأشخاص الطبيعيين، يعتبر من قبيل المعالجة الآلية للبيانات الشخصية الرقمية، في حين أن "محكمة النقض الفرنسية"،قد حكمت بأن تخزين بيانات العامل على الحاسب الآلي لرب العمل، لا يعتبر من قبيل البيانات الشخصية الرقمية المعالجة الكترونياً، حيث لا يعد ذلك معالجة آلية[2].

ومن ثم يتضح أن دخول رب العمل على هذه البيانات، لا يكون ممثلاً لجريمة انتهاك خصوصية معلوماتية للعامل.

وجدير بالذكر، أنه قد شدّد المشرع الفرنسي، على وجوب أن تكون المعالجة الالكترونية للبيانات الشخصية الرقمية، بمثابة خدمة مقدمة إلى كل مواطن، دون أن تنطوي على مساس بكرامة وحقوق الإنسان، وحرياته وحياته الخاصة، وذلك من خلال ما نصت عليه المادة رقم (١) من قانون الجرائم المعلوماتية وحرية تداول الملفات، الصادر بتاريخ ١٩٧٨/١/٦، ولعل ذلك يدل على أن نشر البيانات الشخصية عبر الإنترنت، لا يكون متاحاً بحرية كاملة لجميع مستخدمي شبكة الإنترنت، حيث أن للشخص صاحب البيانات، حق الاعتراض على تجميع بياناته الشخصية، في شكل معين، يكون من شأنه أن يجعلها متاحة لأي

1 Rapport d'activité pour l'année 1979. P 25 . disponible sur http://www.clauses-abusives.fr/activ/ra1979.htm.5/5/2023.

2 Cass. Ch, sociale Arrêt du 4 juillet 2012, disponible sure le site: http://www.legalis.net/spip.php?page=jurisprudencedecision&id_article=3490. 5/5/2023.

شخص معني بمعرفتها[1].

كذلك نجد أن القضاء الفرنسي، قد حكم أيضاً بأنه في مجال حماية البيانات المتعلقة بالحياة الخاصة للأفراد، يمكن أن تكون هذه البيانات المنشورة على شبكة الإنترنت، متاحةً بحرية لمستخدمي الشبكة، إذا كان الهدف من نشرها، تقديم المعرفة للجمهور[2].

وفيما يلي نوضح تلك الضوابط من خلال ما يلي:-

أولاً: التزامات ومبادئ عملية معالجة البيانات الشخصية الرقمية:

اهتمت "الاتفاقية الأوربية" بحماية الأفراد من المعالجة الإلكترونية للمعلومات الشخصية، لأن شبكات المعلومات (وفي مقدمتها الانترنت)، أتاحت التبادل الواسع لمختلف أنماط المعلومات والبيانات، وتتيح التراسل الفوري، وحيث إن التقارير الصادرة عن هيئات ومنظمات حماية البيانات، قد أظهرت أن بيانات الأفراد والمؤسسات، ليست آمنة من الإطلاع عليها وإفشائها، وليست الخطورة فقط فيما يمكن الوصول إليه من بيانات في وقت معين، إذ الخطورة الأكبر فيما يمكن جمعه من بيانات، وتحليلها كحزمة واحدة، للوصول إلى حقائق عن الفرد، تساهم في تنفيذ أنشطة المساس به، أو الاعتداء على حقوقه الأخرى.

وعليه فقد تم إبرام هذه الاتفاقية، بغرض ضمان حق كل شخص طبيعي في أي دولة، مهما كانت جنسية أو مكان إقامته، باحترام حقوقه وحرياته الأساسية وخصوصيته، وذلك في مواجهة الاستخدام الآلي للبيانات ذات الطابع الشخصي، التي تتعلق به، وقد نظّمت الدول الموقعة على الاتفاقية، عدة توصيات خاصة بحماية تلك البيانات، لكي تلتزم الدول الأعضاء في ضوئها، بوضع تشريعاتها الخاصة بهذا المجال، وهي كما يلي:-

١. أن تكون البيانات المدرجة في بنوك المعلومات صحيحة ودقيقة، وأن يتم الحصول عليها بطريقة مشروعة، ويعين أن يكون حفظها موقوتاً بمدة معينة.
٢. عدم جواز إطلاع الغير على مثل هذه البيانات، أو استعمالها لغير الغرض المخصص لها، ويكون ذلك عن طريق تحديد الأشخاص، الذين يحق لهم الاطلاع على تلك البيانات، وإخضاعهم لقيد الالتزام بالسر المهني.
٣. منح الشخص حق الاطلاع على البيانات الخاصة به، وتصحيحها أو تعديلها أو محوها، متى كانت غير صحيحة، أو تم الحصول عليها بطريقة غير مشروعة.

---

1 G. LOISEAU, L'exploitation de données personnelles collectées sur le web, Com. Comm. Electr, N° 9, Septembre 2012, P. 94.

2 Cass. 1 re civ., 22 mai 2008, n° 07-13.165 ,inédit. - Rapp. CEDH, 23 juill. 2009, n° 12268/03, Hachette Filipacchi c /France, 52: Juris Data n° 2009-022257.

٤. مساءلة الأشخاص والجهات، المرخص لها الوصول والإطلاع على حقوق البيانات، حال تجاوز أي من الإجراءات، التي تكفل حماية البيانات ذات الصفة الشخصية.

كذلك وضع التوجيه الأوربي الصادر بتاريخ ١٩٩٥/١٠/٢٤، التزامات وضوابط معالجة البيانات الشخصية آلياً، بهدف حمايتها، دون تمييز بين المعالجة اليدوية والآلية للملفات (المبدأ رقم ٢٧)[١].

وهناك أيضاً عدة ضوابط قد أقرتها التشريعات، لتحيط بعملية المعالجة للبيانات الشخصية، كي تتسم بالمشروعية والقانونية، وهي تتمثل في الآتي:-

١. موافقة الشخص صاحب البيانات على إجراء المعالجة، لأجل تحقيق هدف محدد.
٢. أن تكون المعالجة للبيانات ضرورية ومهمة، تنفيذاً لالتزام تعاقدي أو تصرف قانوني،أو لأجل إبرام عقد لصالح الشخص صاحب البيانات، أو لمباشرة إجراء من إجراءات المطالبة بالحقوق القانونية، أو الدفاع عنها.
٣. تتطلب عملية المعالجة للبيانات الشخصية، تمكين المتحكم من القيام بالتزاماته، أو أي ذي صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.
٤. يجب أن تكون المعالجة للبيانات الشخصية، تنفيذاً لالتزام ينظمه القانون، أو أمر من أوامر جهات التحقيق المختصة، أو بناء على حكم قضائي[٢].

وجدير بالذكر، أن هناك بيانات شخصية ذات حساسية، يحظر على الشخص المعالج (سواء كان شخصاً طبيعياً أم معنوياً) جمعها أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها، إلا بترخيص من المركز، وفي حالة إجراء عملية تتعلق ببيانات أطفال، يلزم موافقة ولي الأمر، مع مراعاة ألا تكون مشاركة الطفل في لعبة أو مسابقة أو أي نشاط آخر، مشروطة بتقديم بيانات شخصية للطفل، تزيد على ما هو ضروري للمشاركة في ذلك(المادة رقم ١٢).

هذا وقد أصدر الاتحاد الأوربي عام ٢٠١٦، "اللائحة العامة لحماية البيانات (GDPR)، وتُعد تلك اللائحة امتداداً للحماية المقررة من قبل التوجيه الأوربي, وتتضمن عدة مبادئ لا بد أن تلتزم بها

---

١ وقد أكدت على ذلك، أحكام التوجيه الأوربي الصادرة بتاريخ ١٩٩٧/١٢/١٥، وكذلك الصادرة بتاريخ ٢٠٠٢/٧/١٢، وتم تعديلها بموجب أحكام التوجيه الأوربي الصادرة بتاريخ ٢٠٠٦/٣/١٥، وكذلك بتاريخ ٢٠٠٩/١١/٢٥.

Sédaillan, La directive européenne, Vie privée et communications électroniques, Légipresse janv 2003, N 198, p12.

٢ الهيئة الوطنية للأمن السيبراني، مذكرة إرشادية حول النظام الأوربي لحماية البيانات الشخصية، ٢٠١٩، ص ١١ وما بعدها. متاح على الموقع الإلكتروني : http://www.gdbr@nca.gov.sa.visited on 19/10/2023.

عملية معالجة البيانات الشخصية، وهي كالآتي:-

١. **مبدأ الشرعية والإنصاف:** يجب أن تتم معالجة البيانات الشخصية بطريقة قانونية، بما يستلزم موافقة صاحب البيانات، وأن تكون ضرورية لأداء عقد موضوع البيانات، كذلك يلزم أن تكون المعالجة ضرورية للامتثال لالتزام قانوني، يخضع له الجهة المتحكمة بالبيانات، إضافة إلى لزوم أن تكون المعالجة ضرورية لحماية المصالح الحيوية لموضوع البيانات[١].

كما يلزم أن تكون المعالجة للبيانات أيضاً، ضرورية لأداء مهمة تم تنفيذها من أجل المصلحة العامة، أو في ممارسة السلطة الرسمية المخولة، وأن يكون التدبير ضرورياً ومتناسباً مع مجتمع ديمقراطي (المادة رقم ٦ من اللائحة)[٢].

٢. **مبدأ الشفافية:** يقصد بمبدأ الشفافية هنا؛ ضمان أن تكون أي معلومات أو اتصال موجه للشخص صاحب البيانات، موجزة، ويمكن الوصول إليها بسهولة، وأن تكون بلُغة مفهومة وواضحة، خاصة عندما يتم توجيهها إلى طفل، كذلك يلزم أن يكون الأشخاص على دراية وعلم بالقواعد والضمانات والمخاطر، وأيضاً الحقوق المتعلقة بمعالجة البيانات، وكيفية ممارسة حقوقهم(المادة رقم ٧٧، ٧٩ من اللائحة).

٣. **مبدأ تحديد الهدف المنشود:** بمعنى أن يتم تجميع البيانات الشخصية لأهداف محددة وواضحة، وألا تتعارض أهداف تلك المعالجة مع القوانين(المادة رقم ٥ من اللائحة)[٣]، وقد أكدت على ذلك الأمر أيضاً، المادة رقم ٣ من قانون حماية البيانات المصري رقم ١٥١ لسنة ٢٠٢٠.

٤. **مبدأ الحد الأدنى من البيانات:** يلزم أن تكون البيانات الشخصية كافية، وأيضاً تكون ذات صلة ومحددة بما هو ضروري، وذلك فيما يتعلق بالأهداف التي تتم معالجتها لأجلها.

٥. **مبدأ دقة البيانات:** يلزم أن تكون البيانات المخزنة دقيقة، ويتم تحديثها بصفة دائمة، من خلال تصحيحها، ومحو الخطأ منها.

٦. **مبدأ التخزين المقيد:** يقتضي هذا المبدأ عدم الاحتفاظ بالبيانات الشخصية، وذلك لمدة أطول من

---

1 Sulliman Omrajee, Le data mining , Aspects juridiques de l'intelligence artificielle auregard de la protection des données personnelles. Mémoire, Faculté de Droit Université Montpellier I, Année Universitaire 2001-2002, p. 26 .

2 V. Julien Le Clainche, La protection des données personnelles nominatives dans le cadre de la recherché dans le domaine de la santé. Comparaison du droit français et Américain, Mémoire de D.E.A. Faculté de droit des sciences économiques et de gestion ,Université Montpellier I, 2001, p. 46

3 Prashant Mali, GDPR Articles With Commentary & EU Case Laws, Cyber Iformedia Publishing, 2019, P.16

المدة اللازمة لتحقيق الغرض من المعالجة (المادة رقم ٥ من اللائحة)[١].

٧. **مبدأ السرية:** من الضروري أن تتم المعالجة بطريقة تضمن توفير الأمان المناسب للبيانات الشخصية، واتخاذ التدابير التقنية والتنظيمية، التي تحقق ذلك الأمر.

٨. **مبدأ الحفاظ على البيانات:** يقتضي ذلك المبدأ؛ اتخاذ التدابير التقنية والتنظيمية المناسبة، للحفاظ على البيانات ضد التلف أو الضياع أو السرقة والاعتداء.

٩. **مبدأ حماية البيانات بالتصميم:** ويعني هذا المبدأ تطبيق المبادئ والحقوق، التي تنص عليها نظم حماية البيانات الشخصية، في تصميم النظم التي تعالج البيانات من الناحية التكنولوجية والإدارية، وأيضاً في تأمين حقوق موضوع البيانات، وذلك كتأمين اتصال آمن بموضوع البيانات الشخصية، للإطلاع على البيانات أو نقلها.

١٠. **مبدأ المساءلة:** وفقاً لهذا المبدأ؛ فإنه يتحمل الشخص القائم بمعالجة البيانات الشخصية، مسئولية تنفيذ وضمان الالتزام بالمبادئ السابقة الذكر[٢].

ثانياً: التزامات المسئول عن معالجة البيانات الشخصية الرقمية:

هناك عدة التزامات وواجبات، تقع على عاتق الشخص المسئول عن معالجة البيانات الشخصية، سواء كان شخص طبيعي أم معنوي (المادة رقم ٨٠١ من القانون الفرنسي الصادر بتاريخ ٢٠٠٤/٨/٦)، ويتسع نطاق تلك الالتزامات، ليشمل مرحلة ما قبل المعالجة للبيانات، ومرحلة أثناء تنفيذ عملية المعالجة، وذلك كالآتي:-

١. **التزامات ما قبل معالجة البيانات الشخصية:** يقع على عاتق المتحكم في البيانات الشخصية، الحصول على البيانات الشخصية، أو تلقيها من الحائز أو من الجهات المختصة، بتزويده بها، بعد موافقة الشخص المعني بالبيانات، والتأكد من صحة البيانات، ومدى اتفاقها وكفايتها مع الغرض المحدد لجمعها، ووضع طريقة أو أسلوب محدد للمعالجة (المادة رقم ٤ من قانون حماية البيانات الشخصية المصري، الفقرة ١: ٤)، كذلك يقع على عاتق المسئول عن معالجة البيانات الشخصية، واجب إعلام الشخص المراد معالجة بياناته الشخصية، بأهداف المعالجة، وأسماء المستفيدين من بياناته(المادة رقم ٣٢ من القانون الفرنسي، الصادر بتاريخ ١٩٧٨/١/٦)، كذلك إعلام كل مشترك

---

1 Paul Voigt And Axel von dem Bussche, The EU General Data Protection Regulation (GDPR), A Practical Guide, Springer International Publishing, 2017 ,P.6.

٢ أ. أثير فاضل عباس رضا، التنظيم الدولي لحماية البيانات ذات الطابع الشخصي، رسالة ماجستير، كلية القانون، جامعة بابل، العراق، ٢٠٢٠، ص٩٣ .

أو مستخدم لخدمة الاتصالات الالكترونية، بطريقة واضحة ومحددة، بالهدف من التسجيل أو الدخول إلى المعلومات المخزنة بالفعل على أجهزته النهائية، للاتصال الالكتروني، والوسائل المتاحة للاعتراض على هذا الدخول أو التسجيل لهذه البيانات على أجهزته[١].

٢. التزامات أثناء معالجة البيانات الشخصية:

- يلتزم المسئول عن معالجة البيانات الشخصية، بالتحلي بالأمانة الوظيفية، وألا يستخدم البيانات في أغراض غير مشروعة(المادة رقم ٣ من قانون حماية البيانات الشخصية المصري، فقرة ١،٢،٣) بما يشكل جريمة معالجة غير مشروعة للبيانات، يأخذ ركنها المادي صورة الغش والتحايل.
- يلتزم المسئول عن جمع ومعالجة البيانات الشخصية، بأن يتم التجميع بدقة، ومسح البيانات غير الصحيحة، بحيث يلتزم بالتحقيق من سلامة البيانات.
- الالتزام بمراعاة مدة حفظ البيانات(المادة رقم ٣ من قانون حماية البيانات الشخصية المصري، فقرة (٤) بحيث لا يتجاوز الاحتفاظ بها، بما يسمح بتحديد الأشخاص، التي تتعلق البيانات بشخصيتهم، المدة اللازمة لأغراض الجمع والمعالجة، فلا تزيد على المدة الضرورية لتحقيق تلك الأغراض(م ٦)[٢].

إذ أن عامل الوقت في المعاملة الالكترونية، يعد عاملاً محورياً، بحيث يمكن حفظ بيانات متعلقة بشخص في ظرف وقت قياسي.

وتطبيقاً لذلك؛ فإنه قد قضى مجلس الدولة الفرنسي، بأن عملية جمع ومعالجة البيانات الشخصية، الخاصة بالقروض المستحقة على العملاء، بهدف تبادلها بين مؤسسات الائتمان، لا تتعارض مع واجب الأمانة والمشروعية، وذلك لكي تتخذ قراراتها بقبول أو رفض طلب الائتمان أو القرض، ولكن لا يتم ذلك إلا بعد موافقة العميل على نقل بياناته، قبل رد المؤسسة البنكية عليه، بقبول أو رفض طلبه[٣].

- الالتزام باتخاذ وسائل الحيطة والحذر، في مواجهة تسريب البيانات الشخصية، من خلال عدم وضع المعدات والأجهزة، المستخدمة في معالجة البيانات، في ظروف أو أماكن، تمكن من الوصول إليها من قبل الآخرين، وأيضاً اتخاذ جميع الإجراءات التقنية والتنظيمية، وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية، وتأمينها, حفاظاً على سريتها، وعدم اختراقها، أو العبث بها(المادة رقم ٤ من قانون حماية البيانات الشخصية المصري، الفقرة ٦)، كذلك عدم تمكين شخص

---

١ د.السيد محمد السيد عمران، الالتزام بالإعلام الالكتروني قبل التعاقد عبر شبكة الإنترنت، دار الجامعة الجديدة، ٢٠٠٦،ص ١٠٥ وما بعدها.

٢ القانون الفرنسي الصادر بتاريخ ١٩٧٨/١/٦، المعدل بالقانون الصادر بتاريخ ٢٠٠٤/٨/٦.

3 CE 30 déc. 2009, Sté Experian, req. No 306173, Lebon 535. http://www.dalloz.fr/documentation/Document?id 5/5/2023.

غير مأذون له، بالإطلاع على تلك البيانات، مع إمكانية تفعيل نظام، يتم من خلاله، معرفة ما إذا تمكّن شخص غير مأذون له، بالإطلاع على تلك البيانات، أم لا وتاريخ الإطلاع، أو تفعيل نظام الكتروني لا يسمح بدخول الغير للإطلاع، أو نقل البيانات أو نسخها أو تعديلها.

- الإمساك بسجل خاص للبيانات، يتضمن وصف فئات البيانات الشخصية لديه، وتحديد من لهم حق الإطلاع على هذه البيانات، والمدة الزمنية للبيانات،ونطاقها، وآليات محوها (المادة رقم ٤ من قانون حماية البيانات الشخصية المصري، الفقرة ٩) ومتابعة القيد والتحديث لسجل البيانات الشخصية لدى المتحكم، وذلك لضمان دقة البيانات المقيدة به، وإزالة أي مخالفات متعلقة بالبيانات الشخصية(المادة رقم ٩ – الفقرة ٦, ٧).
- الحصول على ترخيص من المركز المختص للتعامل مع البيانات الشخصية بكل دولة، وكذلك الالتزام حال العلم بوجود اختراق للبيانات الشخصية، بإبلاغ هذا المركز خلال ٧٢ ساعة، بطبيعة الانتهاك، وصورته وأسبابه، والعدد التقريبي للبيانات الشخصية وسجلاتها، والإخطار ببيانات مسئول الحماية، وآثار الانتهاك المحتملة،الواقعة نتيجة هذا الانتهاك، وذكر الإجراءات المتخذة والمقترحة لمواجهة الانتهاك، مع توثيق وسيلة الانتهاك وإجراءات مواجهته، وموافاة المركز بأي وثائق أو معلومات يطلبها، ويكون الإبلاغ فورياً، إذا كانت بيانات تتعلق بالأمن القومي، وعلى المركز إخطار جهات الأمن القومي، إضافة إلى إخطار الشخص صاحب البيانات، خلال ٣ أيام عمل من تاريخ الإبلاغ، وما تم اتخاذه من إجراءات (المادة رقم ٧)، على أن يلتزم مسئول البيانات بالعمل كنقطة اتصال مباشرة مع المركز، وتنفيذ قراراته (المادة رقم ٩– فقرة ٢).

هذا وقد نصت المادة رقم ١-١٧-٢٢٦ عقوبات فرنسي، المضافة بالمرسوم رقم ٢٠١٢ لسنة ٢٠١١، بشأن المراسلات الإلكترونية[1]، على إلزام مزود خدمة الاتصالات، بإخطار "اللجنة الوطنية للمعلومات والحريات"، بحالات الاعتداء على البيانات الشخصية، وكذلك تفرض عليه التزام الإخطار بحالات الإفشاء، أو الوصول غير المرخص إلى البيانات المعالجة الكترونياً، أو تلف البيانات أو ضياعها، وذلك دون تأخير (المادة رقم ١-٩-٤١٢٣ من قانون الدفاع الفرنسي)، كما يلتزم الشخص "مورد البيانات" بإعداد قائمة بالانتهاكات ومصدرها، والكيفية التي حدثت بها، وعليه أن يتخذ التدابير الملائمة لجعل البيانات الشخصية أكثر أماناً في مواجهة الاعتداء عليها، كاستخدام نظام تشفير البيانات الشخصية، وهو ما أكدت عليه أيضاً, المادة رقم ٣٣ من التشريع الأوربي رقم ٢٠١٦/٦٧٩ (الصادر عن الاتحاد الأوربي بتاريخ ٢٠١٦/٤/٢٧، ودخل حيز التنفيذ في ٢٠١٨/٥/٢٥)، ونظراً لخطورة ملفات تعريف الارتباط "الكوكيز" Cookies، على البيانات الشخصية، فإنه يحظر على المعالجين استخدامها، دون موافقة المستفيد من

1 Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques.

الخدمة، وبالضوابط القانونية[١]، وذلك لأنها بيانات يمكن الاستدلال بها على الشخص للتعرف عليه،وفقاً لما أوضحته الاتفاقية رقم ١٠٨ لسنة ٢٠١٨ الخاصة بحماية البيانات الشخصية[٢].

وتجدر الإشارة بهذا الخصوص، أنه تتطلب بعض المعالجات ترخيصاً من "اللجنة الوطنية للمعلوماتية الحريات"(المادة رقم ٢٥ من قانون المعلوماتية والحريات الفرنسي, رقم ١٣٢١ الصادر بتاريخ ٢٠١٦/١٠/٧)، وذلك إذا كانت تتعلق بالآتي: (المعالجات الخاصة بالأصول العرقية والآراء السياسية والدينية – معالجة البيانات الجينية – معالجة البيانات التي تتعلق بالجرائم أو أحكام الإدانة، باستثناء ما يتم بمعرفة معاوني القضاء– المعالجات التي تجري على بيانات الرقم القومي – المعالجة المتعلقة بإجراء أبحاث علمية طبية)، وذلك بناء على طلب يتم تقديمه إلى اللجنة, ولها مهلة الرد عليه خلال شهرين، من تاريخ تقديم الطلب[٣]، كما أنه يتعين الحصول على ترخيص يصدر بمرسوم وزاري (المادة رقم ٢٦) إذا كانت المعالجة تتعلق بأمن الدولة، أو لمنع حدوث جرائم جنائية، أو للاستدلال عنها، أو لإثباتها، أو لملاحقة مرتكبي الجريمة وتنفيذ العقوبة عليهم[٤].

ولعل تلك الالتزامات السابقة الذكر، تحتاج إلى تدريب للأشخاص المعالجين (المادة رقم ٩ – فقرة ٨ من التشريع الأوربي الصادر بتاريخ ٢٠١٦/٤/٢٧)، وتوعيتهم بخصوصية وخطورة ما يقومون به من أعمال معالجة، فهم مسئولون عن التلف لتلك البيانات، أو ضياعها، أو إفشائها[٥].

علاوة على ما سبق من التزامات، نشير إلى أنه يقع على عاتق ناشرو المواقع الالكترونية، الالتزام بالإعلان المسبق لدى "اللجنة الوطنية لتنفيذ المعالجات الآلية للبيانات الشخصية"، بحيث تخضع جميع المعالجات الآلية للبيانات الشخصية، إلى الالتزام بوجوب الإعلان المسبق لدى تلك اللجنة، ولكن هذا الالتزام يختلف نطاقه وفق نوع الموقع الالكتروني، فمواقع التجارة الالكترونية، تخضع إلى نظام الإعلان المسبق لدى اللجنة الوطنية، أما المواقع غير التجارية، التي تنشر أو تجمع البيانات الشخصية (التي يقوم مستخدمو المواقع بجمعها أو نشرها، في إطار نشاطهم الشخصي)، يتم إعفاؤها من هذا الإعلان[٦].

1http://www.village-justice.com/articles/Transposition-droit-francaisPaquet, 11388.html. Visited on 18/5/2023.

2 Council of Europe, Explanatory Report To The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data,Strasbourg ,2018,P 4.

٣ د.سليم محمد سليم حسن، الحماية الجنائية للبيانات الشخصية المعالجة آلياً، دراسة مقارنة، الأكاديمية الحديثة لعلوم الكمبيوتر وتكنولوجيا الإدارة، بدون تاريخ نشر، ص ٦٥ وما بعدها .

4 Ibrahim Coulibaly, La protection des données à caractère personnel dans le domaine de la recherche scientifique. Thèse, Université de Grenoble, 2011, p 184.

٥ د.طارق جمعة السيد راشد، مرجع سابق، ص ٢٦١ : ٢٦٤.

٦ د.رزق سعد، مرجع سابق، ص ٣٢ وما بعدها.

ويقوم المسئول عن عملية المعالجة الآلية للبيانات الشخصية، بملء النموذج الخاص بهذا الإعلان، وكتابة البيانات، وفق ما نصت عليه المادة رقم ٣٠ من قانون المعلوماتية،الصادر بتاريخ ١٩٧٨/١/٦ (المعدل بالقانون الصادر بتاريخ ٢٠٠٤/٨/٦)، بحيث يتم تحديد هوية وعنوان المسئول عن عملية المعالجة الآلية للبيانات الشخصية، أو ممثله القانوني، وكذلك تحديد الهدف من المعالجة الآلية للبيانات الشخصية، وتحديد البيانات الشخصية من حيث أصول وأصناف الأشخاص محل المعالجة الآلية، ومدة حفظ المعلومات محل التعامل الآلي، وتحديد مستقبل الاتصال بهذه البيانات والترتيبات، التي ستكفل تحقيق الأمان لهذه المعالجات والبيانات والأسرار، التي يحميها القانون.

وكتطبيق قضائي للإخلال بالالتزام بالإعلان المسبق لدى اللجنة الوطنية؛ نجد أنه قامت اللجنة الوطنية للمعلوماتية CNIL، بإحالة جمعية التحالف الأوربي للدفاع عن ضحايا الموثقين، إلى محكمة جنح بورجيه، لإخلالها بالحق في الاعتراض، وذلك بتهمة أنها نشرت على موقعها الالكتروني لمدة ١٨ شهر، قائمة تضم ٢٥٠٠ موثقاً، لم يستطيعوا بالوفاء بالتزاماتهم المهنية، بما يدل على فشلهم المهني، وذلك دون الإعلان المسبق لدى اللجنة الوطنية للمعلوماتية، وانتهاكها للحق في الاعتراض المشروع، للأشخاص الذين تضمهم القائمة، كما قامت الجمعية بتسجيل وتخزين البيانات المتعلقة بالجرائم، بما يمس سمعة وكرامة الأشخاص، المعلن أسمائهم عبر شبكة الإنترنت[١].

كذلك أدانت "اللجنة الوطنية" إحدى الشركات، لأنها أرسلت إلى الأفراد عبر الفاكس، بعض الإعلانات المتعلقة ببيع بعض الملابس، وذلك بسعر المصنع, ولم يستطع الأفراد ممارسة حقهم في الاعتراض, على استقبالهم لهذه الإعلانات التجارية، من قبِل الشركة المدانة، لذا قامت اللجنة بإنذار هذه الشركة، لإخلالها بالالتزام بالحق في الاعتراض[٢].

1 NIL, délib. n° 04-033, 27 avr. 2004 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978. http://www.cnil.fr. Visited on 5/5/2023.

2 CNIL, délib. No 2010-232, 17 juin 2010 .http://www.cnil.fr.visited on 6/5/2023.

المطلب الثالث

أحكام نقل البيانات الشخصية خارج إقليم الدولة

قامت "منظمة التعاون الاقتصادي والتنمية" بوضع دليل إرشادي لحماية الخصوصية، ونقل البيانات الشخصية خارج الدولة، كذلك وضع الاتحاد الأوربي "اتفاقية حماية الأشخاص ضد مخاطر المعالجة الآلية للبيانات الشخصية"، عام ١٩٨١م، إضافة لما أصدره الاتحاد من العديد من التوجيهات الأوربية للدول الأعضاء، وذلك للاسترشاد بها عند سن القوانين ذات الصلة[١].

وذلك استثناء على مبدأ حرية الحصول على المعلومات وتدفقها, نصت المادة رقم ١٤ من قانون حماية البيانات الشخصية المصري، على حظر إجراء عمليات نقل البيانات الشخصية إلى دولة أجنبية، إلا بتوافر مستوى معين من الحماية، لا يقل عن المستوى المنصوص عليه في هذه القوانين، وبترخيص أو تصريح من المركز سابق الإشارة، وطبقاً للمادة رقم ٤٩ من القانون رقم ١٧ – ٧٨ المضافة بالقانون رقم ١٣٢١ لسنة ٢٠١٦، الصادر بتاريخ ٢٠١٦/١٠/٧، بشأن الحكومة الرقمية الفرنسية، فإنه تقوم "اللجنة الوطنية الفرنسية"، بالتنسيق مع الجهة التي تمارس سلطات مماثلة لسلطاتها في تلك الدولة، التي تنقل البيانات الشخصية إليها، لضمان توافر الشروط السابقة الذكر[٢].

ولكن في حال الموافقة الصريحة للشخص صاحب البيانات، فإنه يجوز نقل بياناته إلى دولة لا يتوافر فيها مستوى مناسب من الحماية القانونية، وذلك في حالات معينة ذكرتها المادة رقم ١٥ من القانون المصري الخاص بحماية البيانات الشخصية: (المحافظة على حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج، أو إدارة الخدمات الصحية له – تنفيذ التزامات بما يضمن إثبات حق أو ممارسته أمام جهات العدالة، أو الدفاع عنه – إبرام عقد أو تنفيذ عقد مبرم بالفعل، لمصلحة صاحب البيانات – تنفيذ إجراء خاص بتعاون قضائي دولي – وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة – إجراء تحويلات نقدية إلى دولة أخرى – إذا كان النقل يتم تنفيذاً لاتفاق دولي بين الدولتين)، وهو ما يتوافق مع المادة رقم ٤٩ من القانون الفرنسي سابق الإشارة.

كذلك يجوز للقائم على أعمال المعالجة، أن يتيح البيانات الشخصية، لمسئول عن المعالجة أيضاً في دولة أخرى، وذلك حال توافر الشروط المنصوص عليها في المادة رقم ١٦، وهي : (اتفاق طبيعة عمل كل من المعالجة – وحدة الغرض من المعالجة – توافر المصلحة المشروعة من المعالجة لديهما –

---

١ للمزيد راجع بخصوص ذلك؛ د.الشافعي محمد بشير، مرجع سابق، ص ١٣ وما بعدها.

٢ د. ماشاء الله عثمان الزوي، الحماية الجنائية للبيانات الشخصية الإلكترونية في القانون الليبي والمقارن، مجلة العلوم الشرعية والقانونية، كلية القانون، جامعة المرقب، ليبيا، العدد الأول، ٢٠١٨، ص ١٨٧.

ألا يقل مستوى الحماية بتلك الدولة عن مستوى الحماية المقرر بمصر)، وهو ما أكد عليه أيضاً المبدأ رقم ٩ من مبادئ "منظمة التعاون الاقتصادي والتنمية", فيما عرف ب "مبدأ تدفق البيانات عر الحدود"[١].

وتجدر الإشارة، أن للتوجيه الأوربي دوراً مهماً، في الحد من نطاق تدفق البيانات، لدول العالم الثالث، ويكمن سبب ذلك الحد، في افتقار تلك الدول إلى قوانين تحمي الخصوصية المعلوماتية للأشخاص، ومعايير الحماية التي وضعها هذا التوجيه، لذا فهي دول قد تعتبر خارج نطاق التوجيه الأوربي، وقد نصت المادة رقم ٢٥ من هذا التوجيه،على إمكانية نقل البيانات الشخصية إلى دولة من دول العالم الثالث، في حال إذا ما كانت تضمن وتكفل توفير حماية قانونية مناسبة لتلك البيانات، وتتوقف طبيعة تلك الحماية ومدى ملاءمتها، على طبيعة البيانات، والهدف من معالجتها، والمدة المفترضة لهذه المعالجة، وبلد المنشأ، وبلد المستورد النهائي للبيانات، والقواعد القانونية المعمول بها في الدولة، والقواعد المهنية والتدابير الأمنية المطبقة داخل الدولة[٢].

واستثناء من نطاق ومضمون تلك الحماية المقررة للبيانات الشخصية الرقمية، نجد أن "محكمة النقض الفرنسية"، قد حكمت بأنه {لا يعد عنوان الحاسب الآلي IP، من قبيل البيانات الشخصية بصفة عامة، وذلك لأنه لا يعرف إلا جهاز الحاسب الآلي، الذي يستخدمه الشخص، ولا يمكن عن طريقه تحديد هوية الشخص المشترك، عبر موقع الإنترنت، إلا بعد الرجوع إلى السلطة المختصة}[٣]، ولكن رغم ذلك، فإنه قد يكون عنوان IP مرتبطاً ببعض البيانات الأخرى، التي يمكن الوصول من خلالها إلى تحديد هوية الشخص المشترك، وذلك بطريقة غير مباشرة[٤].

لذا فهو يعتبر بيان شخصي، والدليل على ذلك, أن "اللجنة الوطنية للمعلوماتية والحريات" CNIL، قد ألزمت مقدمي خدمات الإنترنت بالحصول على تصريح منها، وذلك قبل القيام بمعالجة أو جمع أي عنوان IP[٥].

---

1 im Mather, Subra Kumaraswamy and Shahad Latif, Cloud Security And Privacy, Published By O Reilly Media Inc, United State Of America, 2009, P.164.

2 Paul Voigt And Axel von dem Bussche, The EU General Data Protection Regulation (GDPR), A Practical Guide, Springer International Publishing, 2017 ,P.7.

3 Cass. crim., 13 jan. 2009, n° 08-84.088, p. 497.

4 R. Perray, Adresse IP et données personnelles, un besoin de convergence d'interprétation entre juges, Gaz. Pal. 2009, doctr. p. 1244.

٥ د. أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات ،مع التركيز على موقعي فيس بوك وتويتر، دار النهضة العربية، ٢٠١٣، ص ١٠٢.

المطلب الرابع

سياسة المواقع والتطبيقات الإلكترونية لحماية البيانات الشخصية الرقمية

تنص سياسة الخصوصية، في العديد من المواقع والتطبيقات الإلكترونية، على بعض الشروط التي تمثل انتهاكاً لخصوصية المستخدم، والتي قد لا يلتفت إليها، عند إنشائه لحاسبه الإلكتروني على الموقع، أو تحميله لتطبيق ما _ وقد استجابت بعض الشركات المنتجة لتلك التطبيقات، إلى مطالب المستخدمين، التي أُثيرت حول مستويات الخصوصية التي توفرها، وتحسين شروط خصوصيتها_ مثال على تلك التطبيقات والبرامج, تطبيق انستجرام Anistgram، فقد كانت سياسة الخصوصية، تنص على حق الموقع، في استعمال أو حذف أو تعديل، أو عرض صور المستخدمين بشكل علني، ولكن بعد اعتراض المستخدمين، اعتذرت عن هذا الشرط.

كذلك تطبيق تويتبيك Twitpic، وهو موقع لمشاركة الصور عبر موقع التدوينات القصيرة "تويتر"، وتنص سياسة خصوصيتها، على حق استخدام الصور، وبيعها إلى طرف ثالث.

وفي عام ٢٠١١، قام بتوقيع عقد شراكة مع إحدى شبكات الأخبار، المتخصصة في تغطية أخبار المشاهير، لتتمكن من استخدام الصور، الموجودة على الموقع، بينما ينص موقع تويتر في سياسة خصوصيته، على حق الاحتفاظ بصور المستخدم المحذوفة، لمدة ٥ أسابيع على الأكثر[١].

أيضاً برنامج المحاثة Skype، وموقع التدوين Word Press ، قد نصا في صفحة السؤال والجواب، بأحقية المستخدم في إلغاء حسابه من على الموقع أو التطبيق، ولكن ذلك لا يمنع الشركة من الاحتفاظ بنسخة من بياناته الشخصية المحذوفة، أما تطبيق فيس بوك Face Book، نصت سياسته الخصوصية، على استغلال البيانات الشخصية، وذلك بيعها إلى شركات تجارية إعلانية، تستهدفهم طبقاً لبياناتهم الشخصية، كذلك تم تسريب بيانات شخصية لنحو ٨٧ مليون من مستخدمي فيسبوك، لصالح شركة "كامبردج انالیتیکا"، خلال حملة انتخابات الرئاسة لعام ٢٠١٦.

كما تم توجيه رسائل عبر البريد الإلكتروني، للتأثير على الناخبين في استفتاء انسحاب بريطانيا من الاتحاد الأوربي، ويتم محوها ذاتياً خلال ساعتين[٢].

بالإضافة إلى أنه، قد قامت شركة فيس بوك، بشراء تطبيق واتس آب Whats App، لأجل

---

1 Terms & Conditions: Twitpic holds your photos hostage http:// www.digitaltrends.com/social-media/ termsconditions-avoid-twitpic/Visited on 8/5/2023.

٢ د.خالد سويلم محمد سويلم، الحماية القانونية للبيانات الشخصية الإلكترونية،دراسة مقارنة، مجلة الدراسات والبحوث القانونية، كلية الحقوق،جامعة الزقازيق، ٢٠٢١، ص ١٨٩٨ .

الأغراض التجارية، ولعل تطبيق واتس آب، يقوم بالنفاذ إلى كل الأرقام المسجلة على هاتف المستخدم، دون سؤاله[١].

أما تطبيق ياهوو Yahoo فهو ينص في سياسته الخصوصية، على إمكانية تغيير سياستها، وذلك دون إعلام مسبق للمشتركين، بما يمثل اعتداء على خصوصية بيانات المشتركين الشخصية[٢]، ففي الوقت الذي حدد فيه فيسبوك أن يجب أن يملك الأشخاص معلوماتهم الخاصة، وأنهم يتمتعون بحرية مشاركتها مع من يريدون، وإزالتها كما يشاءون، ووضع عناصر التحكم بالخصوصية، وحظر من لا يرغب في رؤية المنشور، وبالتالي عدم إمكانية إبداء رأيه، إلا أن ذلك لا يمنع من استغلال البيانات الشخصية والمعلومات، حيث يتطلب أي تطبيق من المستخدم السماح له بالوصول إلى المعلومات، وكذلك التي شاركها معه الآخرون، بما يمنح فيسبوك ترخيص دولي بالنقل للمعلومات، وحذف كل ما يؤيد الفكر العنصري الديني أو الجنسي، والفكر الإرهابي، وكل خطاب يتسم بالعنف، ويحض على الكراهية والعدوانية، والإبلاغ عن الصور غير المرخص بها، التي تنتهك الخصوصية[٣].

ولذلك فقد قامت "المنظمة الدولية للتوحيد القياسي" ISO 177799 عام ١٩٩٩ بإقرار معيار خاص بإدارة أمن المعلومات، مبني على معيار معهد المعايرة البريطاني BS 7799 الصادر عام ١٩٩٥ ويتضمن Shrink- Wrapped يحوي رقم تمهيدي للمستخدم ID وكلمة مرور لمدير أو إداري الأمن، الذي قد يكونا معروفا للمخترقين Hackers، لذلك يجب تغيير هذه القيم بمعايير محددة موافق عليها، قبل استخدام هذه المنتجات، كما يعتمد هذا المعيار على التمييز بين النظم المختلفة، وعدم وجود نظام واحد يطبق في كل المنظمات، لذلك يصبح من الضروري أن تعرف كل منظمة على متطلبات الأمن الخاصة بنظم معلوماتها.

وبموجب هذه السياسة الأمنية، فإنه يتم إنشاء منتدى لأمن المعلومات، وذلك على مستوى الإدارة العليا في المنظمة، وتقديم حملات وبرامج توعية وتدريب على أمن المعلومات، وإدارة المخاطر، كمدخل من مداخل العملية الإدارية في المنظمة، وذلك مع مراعاة القوانين والتشريعات الملائمة، وتوفير إجراءات رقابة الوصول لنظم المعلومات وبياناتها، لتجنب البرمجيات المصابة، وتحديد الإجراءات المطلوب

---

1 Dutch and Canadian DPAs challenge WhatsApp's compliance with their privacy laws . http:// wwwprivacylawscom/Publications/enews/International-Enews/Dates/2013/1/ Dutch-and-Canadian-DPAschallenge-WhatsApp/22/5/2023.

٢ د.سارة الشريف، خصوصية البيانات الرقمية، سلسلة أوراق الحق في المعرفة، الإصدار الثالث، مركز دعم لتقنية المعلومات، القاهرة، ٢٠١٤، ص ٥-٦.

٣ د. عبد الأمير مويت الفيصل, د.إسراء هاشم سيد, انتهاك الخصوصية في مواقع التواصل الاجتماعي, مجلة الباحث الإعلامي، العراق، العدد ٣٦، ٢٠٢٢، ص ٢٣٢ وما بعدها.

اتخاذها، عند حدوث عدم التوافق مع السياسة، كوجود نشاط مصاب أو استخدام غير مناسب، إضافة إلى صيانة أمن المعلومات، فيما يتعلق بمسئولية معالجة المعلومات، وخدمات إتاحتها أو إمدادها المتعاقد عليها خارجياً، من خلال التعهد Qutsourcing، وتخصيص مسئولية أمن المعلومات للموظفين القائمين على أمن البيانات الشخصية.

وبالتالي يكون مديرو أمن المعلومات المهنيين، مسئولين مباشرة عن تطوير وإدخال وإدارة العمليات، التي تساند إدارة ومراجعة عقود التوريد مع سياسات الأمن المطبقة، لكي يستجاب لشروطها وقواعدها المتفق عليها، وتشتمل هذه العمليات على مهمة مراجعة الحالات، والأحداث والاتجاهات، إضافة إلى الإشعارات والإنذارات الصناعية[١].

هذا وقد قامت شركة جوجل، في ديسمبر عام ٢٠١٧، بتوفير الحماية لمستخدمي برامج الآندرويد، من خلال منع التطبيقات من جمع البيانات الشخصية غير الضرورية، والتي تكون غير أساسية لعمل التطبيق، كما طلبت توضيح من التطبيقات، التي تقوم بحفظ ونشر البيانات الشخصية، بتزويد المستخدم بكيفية استخدام البيانات، مع وجوب إعطاء المستخدم إذناً موجهاً إلى معالج البيانات الشخصية، كذلك لا بد من إظهار تحذير على سطح الجهاز، لتذكر المستخدمين أن التطبيق يحاول جمع البيانات الشخصية، دون إذنه[٢].

سياسات حماية البيانات الشخصية الرقمية للأطفال:

أكد تشريع حماية خصوصية البيانات(الصادر عن الاتحاد الأوربي, بتاريخ ٢٠١٦/٤/٢٧) على وجوب توضيح الموقع الالكتروني الموجه للأطفال، لماهية بيانات الطفل، وكيفية استخدامه للموقع، والسياسة المتبعة في الإفصاح عنها.

كما يجب على مشغل الموقع الالكتروني الحصول على موافقة واضحة وصريحة من ولي أمر الطفل، وهو ما يستلزم توضيح نوع البيانات الشخصية التي جرت معالجتها، والهدف من المعالجة، وتزويده أيضاً بنسخة من البيانات الشخصية التي تم تجميعها عن الطفل، إضافة إلى مسح ومحو البيانات الشخصية التي يطلب ولي الأمر بشأنها ذلك، مع عدم تطلب أي بيانات شخصية من الطفل، كشرط للمشاركة في أي نشاط يقدمه الموقع.

---

١ د.محمد محمد الهادي، توجهات أمن وشفافية المعلومات في ظل الحكومة الالكترونية، بدون دار نشر، ٢٠١٩، ص ٢٧: ٢٩.

2 Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2017).

ويترتب على ما سبق من أحكام، حماية الطفل عند استخدامه للمواقع الالكترونية، من خلال حماية بياناته الشخصية، التي يمكن استغلالها في تهديد الطفل، واستغلاله في أعمال منافية للآداب، حيث نجد أن الانفتاح الكبير للنشء الصغير على شبكة المعلومات الدولية، والاستخدام المستمر للإنترنت، دون الوعي الكافي بإرشادات وطرق الأمان, الواجب ابتاعها، يشكل خطورة لهم، وتتمثل تلك الضمانات في عدم قيامهم بتسجيل بياناتهم الخاصة، وتحميل صورهم, وأيضاً عدم تحميل أفلام شخصية في المواقع الاجتماعية، إذ أن شبكة الإنترنت حالياً عالم واسع مفتوح، دون حدود، مما يسمح بكل سهولة بنقل المعلومات وملفات الصور والأفلام، وبالتالي فتح المجال لتسهيل أعمال الاتجار بالبشر، واصطياد الضحايا والترويج لهذه التجارة المشينة، ومن ثم استغلال الأطفال اقتصادياً أو جنسياً[1].

وإذا كان يصعب وضع قيود على شركات الإنترنت، وغلق استخدام الإنترنت، وانغلاق العالم من حولنا أمام أطفالنا، فإن حائط الحماية يتمثل في نشر ثقافة الاستخدام الأمني للانترنت، وأهمية حماية بياناتهم الشخصية، وتوعيتهم بطرق حماية أنفسهم من أي دخيل، كما يتحمل الوالدين مسئولية الإشراف المباشر منهما على استخدام أطفالهما لشبكة الإنترنت[2].

---

١ د. صلاح رزق عبد الغفار يونس، جرائم الاستغلال الاقتصادي للأطفال، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠١٤ ، ص ٤٠٧.

2 http:// www.child-trafficking.info - Anti human trafficking unit (Women and children) - The daily news – Interior ministry officers receive training by international human trafficking experts – 24 Jan 2011.

وذلك كان اقتراح السيدة / نجوى شعيب .. مدير عام حركة سوزان مبارك الدولية للمرأة من أجل السلام ، أثناء المائدة المستديرة التي نظمتها تلك الحركة، في ٢٠١٠/٤/٢٠.

http://www.women for peace. org. international .visited on 18/5/2023.

المبحث الثالث

ضوابط الحماية الدولية للبيانات الشخصية الرقمية

تمهيد وتقسيم:

تكمن إشكالية الدراسة في كيفية التوازن بين "حماية الحق في خصوصية البيانات الشخصية الرقمية" و "حماية الحقوق الأخرى"، وذلك دون تعارض، ودون طغيان إحداها على الأخرى.

لذا فإنه بعرض عرض مظاهر الحماية الدولية للبيانات الشخصية الرقمية (سابقاً)، فإننا نعرض الآن لكيفية الموازنة والتناسب لعدم تجاوز تلك الحماية للحقوق للمساس بالحقوق العامة الأخرى.

وتتمثل تلك الضوابط في بعض القيود، التي تحد من الحماية الدولية للبيانات الشخصية الرقمية، وذلك لتقرير "مبدأ التناسب" فيما بين حماية الحقوق المختلفة، ويقصد بهذا المبدأ: {آلية التوازن فيما بين المبادئ القانونية ذات القيمة المتساوية، والقابلة للتطبيق في وقت واحد، ولكنها متعارضة}. فالتناسب يكون ضامناً للحريات الفردية، وللأهداف المشروعة الأخرى، كالمصالح العامة، ومن ثم فإن هذا المبدأ يعمل على إعمال التوازن، وذلك بين "وزن الحق" و"ثقل الأسباب التي دعت المشرع إلى اتخاذ قرار بتقييد هذا الحق"، لأجل تحقيق أهداف مشروعة، فهو يهدف إلى السعي لتحقيق التوافق فيما بين الحقوق، وإعطاء الأولوية لحقٍ على آخر, وفق الأهداف المشروعة التي يسعى إليها الحق الأول[١].

ومن ثم يستلزم مبدأ التناسب، وجود ضرورة اجتماعية ملحة، تستوجب تقييد حماية حق البيانات الشخصية[٢]. ونوضح ذلك من خلال المطلبين الآتيين :-

المطلب الأول: مبدأ التناسب بين حماية البيانات الشخصية الرقمية والحق في المعلومة.

المطلب الثاني: مبدأ التناسب بين حماية البيانات الشخصية الرقمية والحق في الإطلاع.

---

1 Al-Mahrouky Mayada., Hate Crimes and Freedom of Speech .International Review of law and Economics. Article submission No .109069, Chicago (USA) , 2023, P 9.

٢ أ.ريهام زين، وآخرين، حرية تداول المعلومات، دراسة قانونية مقارنة، برنامج الحق في المعرفة،الطبعة الأولى، مؤسسة حرية للفكر والتعبير،٢٠١١، ص ١٥.

المطلب الأول

مبدأ التناسب بين حماية البيانات الشخصية الرقمية والحق في المعلومة

نص "الإعلان العالمي لحقوق الإنسان" على حرية تداول المعلومات، وذلك في المادة رقم ١٩ منه، دون قيود ترد عليه، على عكس الحريات والحقوق الأخرى التي تتقيد بالقانون[١]، وكذلك نص إعلان "اليونسكو" العالمي حول وسائل الإعلام، الصادر في نوفمبر عام ١٩٧٨، في المادة رقم ٢ بالفقرة ٣ منه، على حق الصحفيين في الحصول على المعلومات، وإرسال التقارير، مؤكداً أن تنوع مصادر الإعلام، يمكّن الفرد من التحقق من صحة المعلومات، مما ييسر دقة وموضوعية تقييم الأحداث[٢]، كما أكد "ميثاق الحقوق الأساسية للاتحاد الأوربي"، على أنه عندما يكون للتدابير التي تنطوي على التدخل في الحقوق الأساسية، التي أرساها الميثاق، ومصدرها في قانون تشريعي للاتحاد الأوربي، فإن الأمر في تلك الحالة يكون متروكاً ل "الهيئة التشريعية للاتحاد الأوربي"، لتحديد العناصر الأساسية التي تحدد نطاق تلك التدخلات[٣].

إضافة إلى الأحكام التي تتطلب السماح بنقل البيانات الشخصية للأشخاص الطبيعيين، وذلك إلى طرف ثالث، مثل السلطة العامة، فيجب أن تصنف في غياب موافقة هؤلاء الأشخاص الطبيعيين (وأياً كان الاستخدام اللاحق لتلك البيانات) على أنها تدخل في حياتهم الخاصة، ولا يمكن تبرير هذا التدخل إلا إذا نص عليه القانون، وكان ضرورياً امتثالاً لمبدأ التناسب، ويحقق أهداف المصلحة العامة، التي يبتغيها الاتحاد الأوربي، أو الحاجة إلى حماية حقوق الآخرين وحرياتهم[٤].

وتطبيقاً على ما سبق من نصوص، نجد أنه في الواقع العملي، قد أكد قرار "مفوضي المعلومات والخصوصية على المستوى الاتحادي والإقليمي" الصادر عام ٢٠٢١ بشأن جائحة كوفيد ١٩ على أن تشريعات الخصوصية تنص على استثناءات للسماح بجمع هذه المعلومات, واستخدامها والكشف عنها، لأسباب تتعلق بالصحة العامة أثناء الجائحة، وغيرها من الحالات الطارئة، ويجب ألا ينظر إلى هذه القوانين من قبِل الخاضعين لها، على أنها عقبة أمام جمع المعلومات واستخدامها، والكشف عنها بصورة مشروعة،

---

١ للمزيد راجع؛ د. الشافعي محمد بشير، مرجع سابق، ص١٧ وما بعدها .

٢ د. فتحي فكري، دراسة تحليلية لبعض جوانب قانون سلطة الصحافة، دار النهضة العربية،١٩٨٧، ص ١٤٨.

٣ د. ميادة مصطفى المحروقي ، الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً، دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوربي GDPR، المجلة القانونية، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، السعودية، ٢٠٢٣، ص ١٥٠٣ .

4 CASE OF STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA, 7/3/2022. Application no. 39378/15. European Court of Human Rights ,Fourth Section . https://hudoc.echr.coe.int/fre. Visited on 13/7/2023.

بل على العكس من ذلك، ينبغي النظر إلى قوانين الخصوصية وأفضل ممارستها، باعتبارها وسيلة لضمان الاستخدام المسئول للبيانات، والكشف عنها، بما يدعم أهداف الصحة العامة، ويعزز الثقة في نظام الرعاية الصحية[١].

كما أكدت "المحكمة الأوربية لحقوق الإنسان" (في العديد من أحكامها) على مبدأ التناسب بين الحقوق، مثال على ذلك, قضية LIEBSCHER v. AUSTRIA لعام ٢٠٢١م بشأن الحكم بانتهاك الحق في الخصوصية، بسبب الالتزام بتقديم اتفاق الطلاق بأكمله إلى السجل العقاري، حيث يكون متاحاً للجمهور، وأوضح أن الطلب الذي قدمته محكمة السجل العقاري، لتقديم تسوية الطلاق الكاملة، لا يتوافق مع قوانين حماية البيانات، حيث سيعني ذلك أن بياناته الشخصية (مثل أسماء وأماكن إقامة أطفاله القصر، وبيانات زوجته السابقة، ومقدار مدفوعات النفقة, واتفاقيات الحضانة) ستكون متاحة للجمهور، وذلك في أرشيف المستندات، وانتهت المحكمة إلى وجود انتهاك المادة رقم ٨ من الاتفاقية الخاصة باحترام الحياة الخاصة والأسرية[٢] .

وبالتالي نجد أن الحقوق الأساسية في احترام الحياة الخاصة، وحماية البيانات الشخصية، ليست امتيازات مطلقة، بل يجب أن يؤخذ في الاعتبار ما يتعلق بوظيفتها في المجتمع، وأن تتوازن مع الحقوق الأساسية الأخرى، ومن ثم يجوز فرض قيود على ممارسة تلك الحقوق، بشرط أن تكون تلك القيود منصوصاً عليها في القانون، وأن تحترم جوهر الحقوق الأساسية، ومبدأ التناسب، وبالتالي تكون قيوداً ضرورية، تستهدف الصالح العام، أو حماية حقوق وحريات أخرى[٣].

ويجب توافر عدة شروط لتحقق إباحة نشر المعلومات، وهي كما يلي :-

- أن يكون الخبر صحيحاً، وهذا ما تقتضيه المصلحة العامة للمجتمع، لأن نشر الأخبار غير الصحيحة (سواء بقصد أم بدون قصد) يؤدي إلى أضرار بالمجتمع، وتضليل الرأي العام، مع الالتزام عند النشر بالموضوعية والحياد.
- أن يكون الخبر ذا طابع اجتماعي؛ بمعنى أنه يهم الجمهور، وليس متعلقاً فقط بالحياة الخاصة للأفراد، كنشر أخبار عن ثرواتهم أو صحتهم أو صفاتهم، لأن في ذلك إضراراً بسمعة الغير.

---

1 https://www.cnil.fr/en. visited on 13/7/2023. موقع اللجنة الوطنية لحماية البيانات CNI

2 Case of Lilbscher v. Austria (06/07/2021). European Court of Human Rights, (Application, no. 5434/17). https://hudoc.echr.coe.intvisited on 14/7/2023.

3 Court of Justice of the European Union (CJEU). REQUEST for a preliminary ruling under Article 267 TFEU from the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia),Case C-439/ 19, 22 June 2022 .http://www.curia .europa.eu/juris/document/document.jsf? visited on 13/7/2023.

- حسن النية، بحيث يكون الهدف من نشر الخبر هو تحقيق الصالح العام للمجتمع، وليس مجرد التشهير والانتقام.
- أن يرد الخبر على معلومات لا يحظرها القانون، لأن الرأي العام ليس له حق في معرفة تلك المعلومات السرية، كإذاعة سر من أسرار البلاد، أو نشر خبر يدخل في نطاق الحياة الخاصة للمواطنين وبياناتهم الخاصة، بدون رضا، أو نشر محاكمات سرية، تتعلق بالنظام العام أو الآداب العامة[1].

١ د. عمار وصفي، الحماية الجنائية للصحفي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠٢٢،ص ١٤٨.

المطلب الثاني

مبدأ التناسب بين حماية البيانات الشخصية الرقمية والحق في الإطلاع

يسمح في بعض الأحيان بالإطلاع على البيانات الشخصية، متى توافرت ضرورة تستدعي هذا الأمر، كما إذا كانت تتعلق بالصالح العام، والأمن القومي، وذلك كما نصت عليه المادة رقم ٨ : ١٠ من "الاتفاقية الأوربية لحقوق الإنسان"، والتي تضمنت الحد من ممارسة الحقوق التي تحميها، عندما يشكل هذا القيد تدبيراً ضرورياً في المجتمع، لتحقيق الصالح العام،كتحقيق الديمقراطية مثلاً، أو الأمن القومي، أو حفظ النظام، وحماية حقوق الآخرين وحرياتهم.

وهو ما يتوافق مع ما انتهت إليه "محكمة العدل" التابعة للاتحاد الأوربي، وذلك في قضية Human Rights League V Council of Ministers لعام ٢٠٢٢ باعتبار أن نقل بيانات سجلات أسماء المسافرين ومعالجتها آلياً بشكل عام، يتفقان مع الحقوق الأساسية في احترام الحياة الخاصة، وحماية البيانات الشخصية في "بلجيكا"، ولم يخالف القانون[1].

وتجدر الإشارة، أن البيانات الشخصية المتعلقة بمحاضر الضبط الجنائي والتحقيقات، لا يجوز معالجتها إلا من جانب السلطات العامة فقط، أو يكون مصرحاً بها وفقاً للقانون واللوائح، ويجوز معالجتها من خلال معالجي البيانات الآخرين، متى كان ذلك ضرورياً لإنشاء مطالبات قانونية، أو الدفاع عنها، ولا يجوز الاحتفاظ بملف كامل عن الإدانات الجنائية، إلا تحت رقابة السلطة العامة (المادة رقم ١٠ من اللائحة الأوربية – المادة رقم ٣ من قانون حماية البيانات المصري) وبالتالي لا يطبق عليها قوانين حماية البيانات الشخصية، حيث يجوز لاعتبارات يقدرها "مركز حماية البيانات الشخصية"، بناء على طلب جهات الأمن القومي، وتتمثل في: (رئاسة الجمهورية – وزارة الدفاع – وزارة الداخلية –جهاز المخابرات العامة – هيئة الرقابة الإدارية)، إخطار جهة المعالجة بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، خلال مدة زمنية معينة، وعلى جهة المعالجة الالتزام بما ورد في الإخطار، خلال المدة المحددة.

وقد أيدت "المحكمة الأوربية لحقوق الإنسان" ذلك في قضية Uzun v Germany بقرار بعدم انتهاك نص المادة رقم ٨ من الاتفاقية الأوربية لحقوق الإنسان، وذلك فيما يتعلق بطلب الطاعن (المشتبه في ارتكابه جريمة إرهاب) بانتهاك حرمة حياته الخاصة، عندما قامت السلطات العامة بمراقبته عن طريق جهاز GPS،واستخدام البيانات التي يتم الحصول عليها عبر هذا الجهاز، في الإجراءات الجنائية

1 Human Rights League V Council of Ministers, Case C-817/19. Court of Justice of the European Union (CJE), 27 January 2022.

المقامة ضده، لاعتبار ذلك انتهاكاً لخصوصية بياناته، وقضت المحكمة بأن معالجة واستخدام البيانات التي تتم معالجتها في هذه الحالة، إنما يهدف إلى حماية الأمن القومي، والصالح العام للمجتمع الديمقراطي[1].

وعلى النقيض انتهت المحكمة الأوربية في قضية Marper the United Kingdom S. v إلى حدوث انتهاك للمادة رقم ٨ من الاتفاقية، فيما يتعلق بالاحتفاظ في قاعدة بيانات ببصمات الأصابع، وملفات الحمض النووي لأشخاص مشتبه فيهم، ولكنهم غير مدينين، واعتبرت المحكمة أن ذلك يمثل تدخلاً في احترام الحياة الخاصة، ولا يمكن اعتباره ضرورياً في مجتمع ديمقراطي، وأكدت المحكمة أنه وإن كان من الضروري استخدام تقنيات العلم الحديث في نظام العدالة الجنائية، إلا أن ذلك يتطلب الموازنة الدقيقة بين "المزايا المحتملة لاستخدام مثل هذه التقنيات" و"الحق في الخصوصية"، حيث لم تحقق السلطات في هذه القضية توازناً عادلاً بين "المصالح العامة" و"المصالح الخاصة"[2].

كذلك هناك تقييد لحماية البيانات الشخصية إذا كان هناك معالجة لها تتعلق بغرض إعلامي، حيث اشترطت اللائحة الأوربية لضمان حماية تلك البيانات، ضرورة التوفيق بين "الحق في حماية البيانات الشخصية" و"الحق في حرية التعبير والمعلومات", بما في ذلك المعالجة التي تتم لأغراض صحفية، أو أغراض التعبير الفني أو الأدبي، وقضت المحكمة الدستورية النمساوية، بعدم دستورية المادة ٥٨ /أ من اللائحة الأوربية، التي تسمح للدول الأعضاء، بتطبيق استثناءات على قواعد اللائحة العامة لحماية البيانات، والتي من بينها عدم خضوع معالجة البيانات الشخصية بواسطة وسائل الإعلام، وموظفي الشركات الإعلامية، بما يعرف ب "الإعفاء الصحفي"، بشرط موافقة صاحب البيانات.

كما صدر عن المحكمة الأوربية لحقوق الإنسان في مارس ٢٠٢٢، حكم في قضية STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA يقضي بانتهاك المادة رقم ١٠ من الاتفاقية الأوربية لحقوق الإنسان، والمتعلقة بالحق في حرية التعبير، وقد تعلّقت القضية بقرارات قضائية، تأمر وسائل الإعلام، بالكشف عن بيانات تسجيل المستخدمين،الذين نشروا تعليقات على إحدى المواقع الإلكترونية، ترتبط ببعض الشخصيات السياسية المتعلقة بالفساد، وكانت الشركة مقدمة طلب قد سحبت تلك التعليقات، بينما رفضت الكشف عن معلومات تتعلق بمؤلفيها، وعلى الرغم من اعتبار

---

1 European Court of Human Rights: Uzun v. Germany, 02.09.2010 .(application no. 35623/05). https://hudoc.echr.coe.int. visited on 12/8/2023.

-Kennedy v. the United Kingdom, 18.05.2010. (application no. 26839/05)

-Privacy International and Others v. the United Kingdom, 4 September 2020, Application no. 46259/16 .

2 European Court of Human Rights , S. And Marper v. the United Kingdom, 4 December 2008 (Grand Chamber). https://hudoc.echr.coe.int/eng. visited on 3/7/2023.

المحكمة أن بيانات المستخدمين لا تغطيها حماية المصادر الصحفية، ولا يوجد حق مطلق في عدم الكشف عن هويتهم على الإنترنت، غير أنها وجدت أن المحاكم الوطنية المذكورة لم توازن بين مصالح المدعين ومصالح الشركة الطالبة في الحفاظ على عدم الكشف عن هوية مستخدميه، بهدف تعزيز التبادل الحر للأفكار والمعلومات المحمية، بموجب المادة رقم ١٠ وبناء عليه؛ قررت المحكمة أن هذه القرارات القضائية ليست ضرورية في مجتمع ديمقراطي[١].

ومن ثم يستفاد أن معالجة البيانات الشخصية، التي تتم لأغراض إعلامية، يجب أن تتم بشكل حصري، دون أن تنسحب لخدمة أغراض أخرى، غير تلك المحددة في القانون، وأن يتم ذلك وفق الشروط والضمانات المعنية المحددة لأصحاب البيانات، لتمكينهم من ممارسة حقوقهم.

إضافة للبيانات السابقة الذكر، التي لا تخضع معالجتها إلى الحماية القانونية، فهناك البيانات الشخصية المعالجة بغرض الحصول على البيانات الإحصائية الرسمية, مما يعني شرعية الحق في الإطلاع عليها، إلا أنه يجب أن تخضع تلك المعالجة لأغراض الأرشفة للصالح العام، أو لأغراض البحث العلمي أو التاريخي، أو للأغراض الإحصائية، للضمانات التي تتناسب مع حقوق وحريات صاحب البيانات، على أن تشتمل تلك الضمانات على تنفيذ التدابير الفنية والتنظيمية، لضمان الامتثال لمبدأ "تقليل الإطلاع على البيانات"، ويمكن أن تشتمل هذه التدابير على استخدام أسماء مستعارة، بالقدر الذي يحمي حقوق صاحب البيانات[٢].

وتطبيقاً لذلك؛ فإنه قد قضت "المحكمة الأوربية لحقوق الإنسان" في قضية Glavna direktsia za borba s ، في يناير ٢٠٢٣م، بأن معالجة البيومترية والجينية من قبل السلطات الشرطية، بهدف تحقيق أغراض الأرشفة للمصلحة العامة، فيما يتعلق بمكافحة الجريمة، والحفاظ على النظام العام، وبشأن حرية نقل هذه البيانات، مصرحاً به بموجب نص المادة رقم ١٠/أ من "اللائحة الأوربية لحماية البيانات الشخصية".

وكذلك المادتين ٤٧ و ٤٨ من "ميثاق الحقوق الأساسية للاتحاد الأوربي"، ويستبعد أي تشريع يسمح بجمع البيانات البيومترية، وذلك لأي شخص كان قد تم اتهامه بارتكاب جريمة، دون وجود رقابة من السلطات المختصة، لأجل التحقق مما إذا كان جمع هذه البيانات كان ضرورياً، وهل بالفعل يتعلق الصالح العام أم لا؟ مع ضرورة التحقق من أن إجراءات هذا الهدف، تشكل تدابير أقل خطورة،في حال المساس

---

1 CASE OF STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA, 7/3/2022. Application no. 39378/15. European Court of Human Rights ,Fourth Section . https://hudoc.echr.coe.int/fre. Visited on 13/7/2023.

٢ للمزيد راجع حول مضمون ذلك؛ أ. ريهام زين، وآخرين، حرية تداول المعلومات، دراسة قانونية مقارنة،برنامج الحق في المعرفة، الطبعة الأولى، مؤسسة حرية للفكر والتعبير،٢٠١١، ص٥٣ وما بعدها.

بحقوق وحريات الآخرين[١].

ولعل ذلك التعارض قد استدعى العمل بمبدأ التناسب هذه الحقوق، لعدم طغيان إحداها على الأخرى، حرصاً على حماية حقوق وحريات الإنسان بصفة عامة، في ضوء الصالح العام[٢].

وتطبيقاً لذلك نجد أن "اجتماع خبراء اليونسكو لدراسة مسألة الخصوصية" (الذي عقد في باريس عام ١٩٧٠ لبحث المسائل المتعلقة بالخصوصية وصور الاعتداء عليها)، قد تناول ضرورة إزالة التعارض بين "الحياة الخاصة للأفراد" و"المصلحة العامة"، أي إقامة توازن بين "حقوق الأفراد" و"حقوق المجتمع" وأصدر عدة ملاحظات على المادة رقم ١٢ من الإعلان العالمي لحقوق الإنسان[٣]، وأهمها: (ضرورة فرض بعض القيود على الحق في الحياة الخاصة، وذلك عند تعارضها مع المصالح العليا للمجتمع – ضرورة توفير الحماية الكافية والضمانات الفعالة، لصيانة الحق في الحياة الخاصة، لاسيما بعد اتساع نطاق تدخل الدولة، وما طرأ من تطور علمي وتكنولوجي – التقرير بجواز اتخاذ إجراءات مشروعة للحد من حقوق معينة، كتلك التي تتصل بالحياة الخاصة، على أن يكون ذلك محدوداً وموقوتاً، وأن يكون ذلك في إطار الحفاظ على الكرامة الإنسانية، وآدمية الأشخاص– العمل على استخدام وسائل التعليم المختلفة، بقصد توعية المواطنين، وإعلامهم على النحو الذي يمكنهم من التعرف على حقهم في الحياة الخاصة – ضرورة وجود وسائل للرقابة على تخزين البيانات الشخصية، وإقرار حق الأفراد في الوصول إلى هذه البيانات، وتصحيحها أو إلغائها، وذلك لمواجهة أخطار الحاسب الآلي، وآثار الاستخدام السيئ له على الحياة الخاصة).

---

1 European Court of Human Rights: Judgment of the court (Fifth Chamber). Ministerstvo na vatreshnite raboti ،Glavna direktsia za borba s Organiziranata prestapnost. 26 January 2023 (C-205/21) https://curia.europa.eu/juris/ document/ document.jsf. visited on 14/7/2023.

٢ د.رزق سلمودي، د.ليندا ربايعة، الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي، مجلة الجامعة الامريكية، فلسطين، المجلد ٣، العدد٢، ٢٠١٧،ص٥– ١٥ وما بعدهما.

٣ د. محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة، دراسة مقارنة ، دار النهضة العربية، بدون سنة نشر، ص٩٠.

الخاتمة

نصت غالبية التشريعات الوطنية على كفالة حماية الحق في الخصوصية (اتفاقاً مع المواثيق والاتفاقيات الدولية، والهيئات الدولية ذات الصلة) وذلك بما يشمله من الحق في حماية البيانات الشخصية، ولاسيما الرقمية، التي ظهرت مع التقدم التقني والتكنولوجي، وأكدت أحكام المحاكم الدولية(محكمة العدل الأوربية – المحكمة الأوربية لحقوق الإنسان) وأحكام محاكم الدول المختلفة على تلك الحماية, وذلك من خلال أحكامها في القضايا ذات الصلة.

وتبين مما سبق، الحقوق المقررة دولياً لصاحب البيانات الرقمية، من حيث الرضا أو الاعتراض استخدام بياناته الرقمية، والحق في الاتصال أو النفاذ إليها، إضافة إلى حق النسيان الرقمي، وحق تقديم الشكوى حال الاعتداء على بياناته الشخصية الرقمية.

كذلك تم تنظيم أحكام معالجة البيانات الشخصية الرقمية، من حيث وضع ضوابط والتزامات تقع على عاتق الشخص القائم بتلك العملية, وذلك في ضوء مبادئ دولية وضعتها الاتفاقية الأوربية، للإحاطة بعملية المعالجة، ومن ثم يخضع المخالف لتلك الالتزامات والمبادئ إلى المساءلة القانونية. إضافة إلى ما وضعته المواقع والتطبيقات الإلكترونية(انستجرام – تويبيك– فيسبوك– تويتر– ياهوو – واتس آب) لحماية البيانات الشخصية الرقمية، من سياسات لحماية الخصوصية، وذلك عند استخدام تلك التطبيقات، خاصة من قبل الأطفال.

ولكن رغم أهمية حماية الحق في البيانات الشخصية الرقمية، اتضح أن هناك حقوق وحريات أخرى، قد تتعارض مع حق خصوصية البيانات الشخصية الرقمية، وذلك كالحق في الحصول على المعلومة وتداولها ونشرها، وكذلك الحق في الإطلاع في حالات الطوارئ لحماية الأمن القومي، أو إذا كانت معالجة تلك البيانات تتم لغرض إعلامي، أو بغرض الحصول على بيانات إحصائية رسمية.

ومن خلال العرض السابق للبحث؛ فإننا قد توصلنا إلى عدة نتائج وتوصيات، وهي كما يلي :-

أولاً: النتائج:

نستنتج من خلال دراستنا العناصر الآتية :

١-يعتبر الحق في حماية البيانات الشخصية الرقمية من أهم عناصر الحق في الخصوصية والحياة الخاصة.

٢- تتسع البيانات الشخصية الرقمية لتشمل جميع البيانات الشخصية التقليدية، المقيدة إلكترونياً بالتقنيات التكنولوجية الحديثة، وملفات الكوكيز، والبيانات الوصفية، والحسابات البنكية، والبيانات التجارية.

٣-تتمثل وسائل التعدي على البيانات الشخصية الرقمية في: (الإفشاء – الإطلاع غير المشروع –

التصوير والتسجيل خلسةً – التزوير).

٤-لصاحب البيانات الرقمية حق الموافقة أو الاعتراض عند معالجتها على التعدي عليها, وكذلك حق نسيانها إلكترونياً, وحق الإبلاغ وتقديم الشكوى في حال مخالفة ذلك.

٥-هناك عدة مبادئ تحكم عملية معالجة البيانات الشخصية, وهي:(مبدأ الشرعية والإنصاف – مبدأ الشفافية – مبدأ الحد الأدنى من البيانات – مبدأ دقة البيانات – مبدأ التخزين المقيد – مبدأ السرية – مبدأ حماية البيانات بالتصميم – مبدأ المساءلة).

٦-يقع على عاتق المسئول عن معالجة البيانات الشخصية (الأمانة الوظيفية – الدقة في العمل – مراعاة مدة حفظ البيانات – الحصول على ترخيص بعملية المعالجة)

٧- يستثنى على مبدأ حرية الحصول على المعلومات وتدفقها, القيام بنقل البيانات الشخصية خارج إلى الدولة, إلا بتوافر مستوى معين من الحماية.

٨- الحق في حماية البيانات الشخصية ليس مطلقاً.

٩- قد يكون هناك تعارض بين "الحق في حماية البيانات الرقمية", و"الحق في الحصول على المعلومات ونشرها", و"حق الاطلاع عند الضرورة لحماية الأمن القومي".

ثانياً: التوصيات:

نقترح عدة توصيات، وهي كالآتي:-

- ضرورة إعمال مبدأ التناسب بين "الحق في حماية البيانات الشخصية الرقمية" و "الحقوق والحريات الأخرى", وذلك في ضوء تحقيق أهداف الصالح العام.
- ضرورة وضع معايير قانونية محددة للقاضي, يستدل منها على احترام التوازن بين "المصلحة المشروعة لجهة المعالجة" و"مصلحة الشخص المعالج بياناته", بما يضمن كفالة حقوقه وحرياته الخاصة, حيث إن فكرة المصلحة المشروعة تعتبر واسعة للغاية, ويمكن التذرع بها لأجل معالجة بيانات الشخص دون موافقة مسبقة منه.
- ضرورة تدريب القائمين بضبط جرائم الاعتداء على البيانات الشخصية الرقمية, وكذلك القائمين بالتحقيق مع الهاكرز ومحاكمتهم, على التعامل مع وسائل التقنية الحديثة. مع تطوير القوانين الوطنية والدولية, كي تتواكب مع تلك التقنيات, خاصةً في عصر التحول الرقمي.

قائمة المراجع

أولاً: المراجع العامة.

- د. الشافعي محمد بشير, قانون حقوق الإنسان, مصادره وتطبيقاته الوطنية والدولية, قانون حقوق الإنسان, مصادره وتطبيقاته الوطنية والدولية, مكتبة الجلاء الجديدة, ٢٠٠٩.
- د.عماد الشربيني, القانون التجاري الجديد لسنة ١٩٩٩, الكتاب الأول, الالتزامات والعقود التجارية, بدون دار نشر, ٢٠٠٠.

ثانياً: المراجع الخاصة.

- د. أحمد محمد حسان، نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة والأفراد, دراسة مقارنة، دار النهضة العربية، القاهرة, ٢٠٠١.
- د. أشرف جابر سيد, الجوانب القانونية لمواقع التواصل الاجتماعي, مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات, مع التركيز على موقعي فيس بوك وتويتر, دار النهضة العربية, ٢٠١٣.
- د. السيد محمد السيد عمران, الالتزام بالإعلام الالكتروني قبل التعاقد عبر شبكة الإنترنت, دار الجامعة الجديدة, ٢٠٠٦.
- د. باسم فاضل، الحماية القانونية للحق في الخصوصية، الطبعة الأولى, المصرية للنشر والتوزيع، ٢٠١٧.
- د.بولين انطونيوس ايوب, الحماية القانونية للحياة الشخصية في نجال المعلوماتية, منشورات الحلبي القانونية, بيروت, ٢٠٠٩.
- د. حسام محمد موسي توني, حماية قواعد البيانات في ضوء الاتفاقيات الدولية وقانون حماية الملكية الفكرية المصري, دراسة مقارنة, الطبعة الأولى, دار النهضة العربية،٢٠٢١.
- د.ريهام زين, وآخرين, حرية تداول المعلومات, دراسة قانونية مقارنة, برنامج الحق في المعرفة, الطبعة الأولى, مؤسسة حرية للفكر والتعبير, ٢٠١١.
- د.سارة الشريف, خصوصية البيانات الرقمية, سلسلة أوراق الحق في المعرفة, الإصدار الثالث, مركز دعم تقنية المعلومات, القاهرة, ٢٠١٤.
- د.سليم محمد سليم حسن, الحماية الجنائية للبيانات الشخصية المعالجة آلياً, دراسة مقارنة, الأكاديمية الحديثة لعلوم الكمبيوتر وتكنولوجيا الإدارة, بدون تاريخ نشر.

- د . شريف محمد غنام, دور الوكيل الالكتروني في التجارة الالكترونية, دار الجامعة الجديدة, ٢٠١٢.
- د.عبد الهادي فوزي العوضي, الحق في الدخول في طي النسيان الرقمي على شبكة الإنترنت, دار النهضة العربية, ٢٠١٣.
- المستشار. عادل الشهاوي، د. محمد الشهاوي، الاعتداء على الحياة الخاصة بواسطة القنوات الفضائية، الطبعة الأولى, دار النهضة العربية، القاهرة, ٢٠١٥.
- د. عاطف محمود الفقيه, الحماية القانونية للاسم التجاري, دار النهضة العربية, ٢٠٠٧.
- د.عبد الهادي فوزي العوضي, الحق في الدخول في طي النسيان على شبكة الإنترنت, دراسة قانونية تطبيقية مقارنة, دار النهضة العربية, ٢٠١٤.
- د.عثمان بكر عثمان, المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي, كلية الحقوق, جامعة طنطا, ٢٠١٨.
- د. فتحي فكري, دراسة تحليلية لبعض جوانب قانون سلطة الصحافة, دار النهضة العربية, ١٩٨٧.
- د. محمد أمين الميداني، النظام الأوروبي لحماية حقوق الإنسان، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٩.
- د. محمد حجازي, جرائم الحاسبات والانترنت, الجرائم المعلوماتية, المركز المصري للملكية الفكرية, مارس ٢٠٠٥.
- د.محمد محمد الهادي, توجهات أمن وشفافية المعلومات في ظل الحكومة الالكترونية, بدون دار نشر, ٢٠١٩.
- د. محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة، دراسة مقارنة، دار النهضة العربية, بدون سنة نشر.

ثالثاً: المجلات العلمية .

- د. أسامة بن غانم العبيدي، حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، مركز الدراسات والبحوث والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، المجلد ٢٢، العدد ٤٦.
- د. أشرف محمد نجيب, جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات, مجلة روح القوانين, كلية الحقوق, جامعة طنطا, العدد الخامس والتسعون, يوليو ٢٠٢١.
- د. آلاء يعقوب النعيمي, الوكيل الالكتروني, مفهومه وطبيعته القانونية, مجلة جامعة الشارقة للعلوم

الشرعية والقانونية, المجلد ٧, العدد ٢, ٢٠١٢.

- د. بن سماعيل سلسبيل, الحماية الجنائية للخصوصية المعلوماتية في التشريعين الجزائري والفرنسي, مجلة الاجتهاد القضائي, جامعة محمد خضر بسكرة, الجزائر, المجلد ١٢, ابريل ٢٠٢٢.
- د.تومي يحي, الحماية القانونية للمعطيات ذات الطابع الشخصي, دراسة تحليلية, مجلة الأستاذ الباحث للدراسات القانونية والسياسية, المجلد ٤, العدد ٢, ٢٠٢٠.
- د. حسين عبده الماحي, نظرات قانونية في التجارة الالكترونية, مجلة البحوث القانونية والاقتصادية, كلية الحقوق, جامعة المنصورة, ٢٠٠٢.
- د. خالد سويلم محمد سويلم, الحماية القانونية للبيانات الشخصية الإلكترونية, دراسة مقارنة, مجلة الدراسات والبحوث القانونية, كلية الحقوق, جامعة الزقازيق, ٢٠٢١.
- د.رزق سلمودي, د٠ليندا ربايعة, الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي, مجلة الجامعة الامريكية, فلسطين, المجلد ٣, العدد٢, ٢٠١٧.
- د. سامح عبد الواحد التهامي, ضوابط معالجة البيانات الشخصية, دراسة مقارنة بين القانون الفرنسي والقانون الكويتي, مجلة كلية القانون الكويتية العالمية, العدد٩, السنة ٣, مارس ٢٠١٥.
- د.طارق جمعة السيد راشد, الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي, دراسة مقارنة, مجلة الاقتصاد والقانون, كلية الحقوق, جامعة القاهرة, ملحق خاص بالعدد رقم ٩٢, ٢٠١٦.
- د. عبد الأمير مويت الفيصل, د.إسراء هاشم سيد, انتهاك الخصوصية في مواقع التواصل الاجتماعي, مجلة الباحث الإعلامي, العراق, العدد ٣٦, ٢٠٢٢.
- د . عقيل فاضل حمد الدهان – د . غني ريسان جادر الساعدي, الالتزام بالإعلام في العقد الالكتروني, مجلة أهل البيت, العدد الخامس, كلية القانون, جامعة البصرة, ٢٠١٧.
- د . كيسي زهيرة, الإطار القانوني للتعبير عن الإرادة في العقود المبرمة عبر الإنترنت, مجلة الاجتهاد للدراسات القانونية والاقتصادية, المركز الجامعي لتامنغست, الجزائر, بدون سنة نشر.
- د.ماشاء الله عثمان الزوي, الحماية الجنائية للبيانات الشخصية الإلكترونية في القانون الليبي والمقارن, مجلة العلوم الشرعية والقانونية, كلية القانون, جامعة المرقب, ليبيا, العدد الأول, ٢٠١٨.
- د. محمد أحمد المعدواي, حماية خصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي, دراسة مقارنة, مجلة كلية الحقوق, جامعة بنها, العدد ٣٣, الجزء الرابع, ٢٠٢١.
- د. محمد رايس، الحماية الجنائية للسند الإلكتروني في القانون الجزائري، مجلة الدراسات القانونية، كلية الحقوق، جامعة بيروت العربية، لبنان، العدد الأول، ٢٠٠٦/٢٠٠٧.

- د. محمود زكي زكي زيدان, الحماية الجنائية الموضوعية للحق في النسيان الرقمي, دراسة مقارنة, مجلة روح القوانين, كلية الحقوق, جامعة طنطا, العدد ١٠١, الجزء الأول, يناير ٢٠٢٣.
- د. محمود محمد محمد مهنى, استخدام التسويق الالكتروني لتطبيقات تكنولوجيا الذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي, مجلة مستقبل العلوم الاجتماعية, العدد ٨, يناير ٢٠٢٢.
- د. مصطفى إبراهيم العربي خالد, مظاهر الحماية الجنائية للحق في النسيان الرقمي, المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي, الجمعية العربية لعلوم الأدلة الجنائية والطبي الشرعي, جامعة نايف العربية للعلوم الأمنية, المجلد الثاني, السنة ٢, ٢٠٢٠.
- د. ميادة مصطفى المحروقي, الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً, دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوربي GDPR, المجلة القانونية, كلية العدالة الجنائية, جامعة نايف العربية للعلوم الأمنية, السعودية, ٢٠٢٣.
- د. نادية أبو العزم السيد حسن, الحقوق المعنوية في ميزان الشريعة الإسلامية..دراسة فقهية, مجلة البحوث القانونية والاقتصادية, كلية الحقوق, جامعة المنصورة, العدد ٤٦, أكتوبر ٢٠٠٩.
- د.ياسر محمد اللمعي, السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية, دراسة تحليلية مقارنة, مجلة روح القوانين, كلية الحقوق, جامعة طنطا, العدد ٩٧, يناير ٢٠٢٢.
- د . يونس عرب, قانون تقنية المعلومات والتجارة الالكترونية, ط١, مجلة نقابة المحاميين الأردنيين, عمان, ٢٠٠٣/ ٢٠٠٤.

رابعاً: الرسائل العلمية.

- أ.أثير فاضل عباس رضا, التنظيم الدولي لحماية البيانات ذات الطابع الشخصي, رسالة ماجستير, كلية القانون, جامعة بابل, العراق, ٢٠٢٠.
- د. آدم عبد البديع آدم، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكلفها له القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٠٠.
- د.إلهام محمد حامد إبراهيم, المتجر الالكتروني, رسالة دكتوراه, كلية الحقوق, جامعة المنصورة, ٢٠١٦.
- أ. حرية شعبان محمد الشريف, نظم المعلومات المحاسبية الإلكترونية, دراسة تطبيقية على المصارف العاملة في قطاع غزة, رسالة ماجستير, الجامعة الإسلامية, فلسطين, ٢٠٠٦.

- د.صلاح رزق عبد الغفار يونس, جرائم الاستغلال الاقتصادي للأطفال, دراسة مقارنة, رسالة دكتوراه, كلية الحقوق, جامعة المنصورة, ٢٠١٤.
- د. عبد الرحمن جمال الدين حمزة، الحق في الخصوصية في مواجهة حرية الإعلان, دراسة مقارنة، رسالة دكتوراه، كلية الحقوق, جامعة المنوفية، ٢٠٠٢.
- د. عمار وصفي, الحماية الجنائية للصحفي, رسالة دكتوراه, كلية الحقوق, جامعة المنصورة, ٢٠٢٢.
- د . محمد سعيد أحمد إسماعيل, أساليب الحماية القانونية لمعاملات التجارة الالكترونية, دراسة مقارنة, رسالة دكتوراه, جامعة عين شمس, ٢٠٠٥.
- أ.منصور بن صالح السلمي, المسئولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي, دراسة تأصيلية مقارنة, رسالة ماجستير, كلية الدراسات العليا, جامعة نايف العربية للعلوم العربية, ٢٠١٠.

خامساً: المؤتمرات العلمية.

- د. أسامة أبو الحسن مجاهد, خصوصية التعاقد عبر الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة ، مجموعة أعمال المؤتمر المنعقد في الفترة من ١-٣ مايو ٢٠٠٠.
- د.رزق سعد, الحماية الجنائية للبيانات الشخصية المعالجة الكترونياً في ضوء القانون رقم ١٥١ لسنة ٢٠٢٠, مؤتمر الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي "رؤية مصر ٢٠٣٠ في المجال الصحي", المؤتمر الدولي الأول بكلية الحقوق, جامعة السادات, ٢٠٢٢.
- د.جبالي أبو هشيمة كامل, حماية البيانات الشخصية في البيئة الرقمية, مؤتمر العصر الرقمي وإشكالياته القانونية, كلية الحقوق, جامعة أسيوط, الفترة من ١٢:١٣ ابريل ٢٠١٦.
- د . طاهر شوقي مؤمن, خدمة الاتصال بالإنترنت, مجلة البحوث القانونية والاقتصادية, كلية الحقوق, جامعة المنصورة, أكتوبر ٢٠١٢, الجزء الثاني, العدد ٥٢.
- د. عبد الله الخشروم, عقود التجارة الالكترونية عبر شبكة الإنترنت, مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية, الكتاب الثالث, أكاديمية شرطة دبي بالإمارات, خلال الفترة من ٢٦ إلى ٢٨ ابريل, عام ٢٠٠٣.
- المستشار. مصطفى الصديق إبراهيم خورشيد, الحماية القانونية لحقوق المؤلف علي مصنفاته الرقمية في بيئة الانترنت,"دراسة مقارنة في التشريع المصري والاتفاقيات الدولية", بحث مقدم للمؤتمر العلمي الخامس للمعهد القومي للملكية الفكرية, ٢٦ ابريل ٢٠٢٢.

سادساً: التقارير والأحكام والاتفاقيات الدولية .

- التقرير الدوري للجنة المعنية بحقوق الإنسان, بشأن الملاحظات الختامية قبِل التقرير الدوري الرابع للولايات المتحدة, الصادر بتاريخ ٢٠١٤/٤/٢٣, فقرة رقم ٢٢.
- القواعد النموذجية الدنيا لمعاملة السجناء الصادرة عن مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين, وذلك في دور انعقاده بجنيف عام ١٩٥٥, وقد أقرها المجلس الاقتصادي والاجتماعي بتاريخ ١٩٥٧/٧/٣١.
- أحكام التوجيه الأوربي الصادرة بتاريخ ١٩٩٧/١٢/١٥, وكذلك الصادرة بتاريخ ٢٠٠٢/٧/١٢, المعدلة بموجب أحكام التوجيه الأوربي الصادرة بتاريخ ٢٠٠٦/٣/١٥, وكذلك بتاريخ ٢٠٠٩/١١/٢٥.
- أحكام محكمة النقض المصرية, المستحدث من المبادئ التي قررتها الهيئة العامة للمواد المدنية والجنائية ودوائر المجموعات المدنية والتجارية وطلبات رجال القضاء, في الفترة من أكتوبر ٢٠٢١: ديسمبر ٢٠٢٢, المكتب الفني.
- اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات الشخصية, لعام ٢٠١٤.

سابعاً: المراجع الإلكترونية.

- محكمة العدل الأوربية, الحكم الصادر في القضية رقم C-293/12 , والقضية رقم C-594/12, الخاصة بالحقوق الرقمية في ايرلندا, بتاريخ ٨ ابريل ٢٠١٤. منشور على الرابط الالكتروني الآتي:- http://curia.europa.eu/juris/document.jsf.visited on 2/5/2023.
- نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات, الأمانة العامة لجامعة الدول العربية, إدارة الشئون القانونية, الشبكة القانونية العربية. http://www.arablegalnet.org.visited on 13/5/2023.
- الهيئة الوطنية للأمن السيبراني, مذكرة إرشادية حول النظام الأوربي لحماية البيانات الشخصية, ٢٠١٩. متاح على الموقع الإلكتروني : http://www.gdbr@nca.gov.sa.visited on 19/10/2023.
- INTERNET PROTOCOL http://toolsietforg/html/rfc760. visited on 8/5/2023.
- Cass.crim, 14 mars, 2006. Available on: http:// www.Legi France. gouv-Fr.7/5/2023.
- http://www.hespress.com/international/297330.html.visitedon 4/5/2023.
- http://aawsat.com/home/article. visited on 3/5/2023.
- General Data Protection Regulation. ”Commission Nationale de

l'Informatique et des Libertés"(CNIL) .https://www.cnil.fr/en/official-texts. Visited on 13/5/2023.

- Tribunal de grande instance de Paris Ordonnance de référé 15 février. (2012). https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-deparis ordonnance - de-refere-15-fevrier-2012. 13/5/2023.
- Judgment of the court (Grand Chamber). (2014 ,May 13) .http:// curia. europa.eu/ juris/ document /document_print.jsf?13/5/2023.
- Case C – 131/ 12, Google Spain SL v. Agencia Espanola de protection de Dates, 13 May, 2014. www.curia.europa.eu.22/5/2023.
- Rapport d'activité pour l'année 1979. disponible sur http://www.clauses-abusives.fr/activ/ra1979.htm.5/5/2023.
- Cass. Ch, sociale Arrêt du 4 juillet 2012, disponible sure le site: http://www.legalis.net/spip.php?page=jurisprudencedecision&id_article= 3490. 5/5/2023.
- Gloria Gonzalez Fuster , Security and the future of personal data protection in the Europen Union, Security and Human Rights, January 2013, published on: http://www.researchgate.net .Visited on 11/7/2023.
- CNIL, Délibération 96 – 009 du 27 février 1996, Délibération portent adoption du rapport intitulé, Les informations personnelles issues de la voix et de l'image et la protection de la vie privée et des libertés fondamentales. www.legifrqnce:gouv.fr .22/5/2023.
- Rapport d'information de l'Assemblée Nationale sur la mise en application de la loi no.2004-575 du 21 juin2004 pour la confiance dans l'économie numérique, présenté par M. Jean Dionis du Séjour et Corinne Erhel. Ce.rapport est disponible sur: http://www.assemblee-nationale.fr/13/rap-info/i0627.asp .12/5/2023.
- CE 30 déc. 2009, Sté Experian, req. No 306173, Lebon 535. http://www.dalloz.fr/documentation/Document?id 5/5/2023.
- http://www.village-justice.com/articles/Transposition-droit-francaisPaquet, 11388.html. Visited on 18/5/2023.
- CNIL, délib. No 2010-232, 17 juin 2010 .http://www.cnil.fr.visited on 6/5/2023.
- NIL, délib. n° 04-033, 27 avr. 2004 portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978. http://www.cnil.fr. Visited on 5/5/2023.
- Terms & Conditions: Twitpic holds your photos hostage http://

www.digitaltrends.com/social-media/ termsconditions-avoid-twitpic/Visited on 8/5/2023.

- Dutch and Canadian DPAs challenge WhatsApp's compliance with their privacy laws. http://wwwprivacylawscom/Publications/enews/International-Enews/Dates/2013/1/Dutch-and-Canadian-DPAschallenge-WhatsApp /22/5/ 2023.
- http:// www.child-trafficking.info - Anti human trafficking unit (Women and children) -The daily news – Interior ministry officers receive training by international human trafficking experts – 24 Jan 2011.
- http://www.women for peace. org. international .visited on 18/5/2023.
- https://www.cnil.fr/en. visited on 13/7/2023. موقع اللجنة الوطنية لحماية البيانات
- Case of Lilbscher v. Austria (06/07/2021). European Court of Human Rights, (Application, no. 5434/17). https://hudoc.echr.coe.intvisited on 14/7/2023.
- Court of Justice of the European Union (CJEU). REQUEST for a preliminary ruling under Article 267 TFEU from the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia),Case C-439/ 19, 22 June 2022 .http://www.curia .europa.eu/juris/document/document.jsf? visited on 13/7/2023.
- European Court of Human Rights: Uzun v. Germany, 02.09.2010 . (application no. 35623/05). https://hudoc.echr.coe.int. visited on 12/8/2023.
- European Court of Human Rights , S. And Marper v. the United Kingdom, 4 December 2008 (Grand Chamber). https://hudoc.echr.coe.int/eng. visited on 3/7/2023.
- CASE OF STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA, 7/3/2022. Application no. 39378/15. European Court of Human Rights ,Fourth Section .https://hudoc.echr.coe.int/fre. Visited on 13/7/2023.
- European Court of Human Rights: Judgment of the court (Fifth Chamber). Ministerstvo na vatreshnite raboti ،Glavna direktsia za borba s Organiziranata prestapnost. 26 January 2023 (C-205/21) https://curia.europa.eu/juris/ document/ document.jsf. visited on 14/7/2023.

ثامناً: المراجع الأجنبية.

أ. المراجع الإنجليزية.

- Ahmed Sarhan , Ehab Abiu Aish, The impact of attitude towards electronic word of mouth on Egyptian consumers, The Egyptian Journal for Commercial Studies, Mansoura University, Faculty of Commerce, Vol 36, No 4, Part 2, 2012.
- Al-Mahrouky Mayada., Hate Crimes and Freedom of Speech . International Review of law and Economics. Article submission No . 109069, Chicago (USA) , 2023.
- Andrew Moore, The GDPR & Managing Data Risk, John Wiley & Sons, Ltd, Great British, 2018.
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. Online behavioral advertising: A literature review and research agenda. Journal of advertising, 46(3), 363-376. 2017.
- Council of Europe, Explanatory Report To The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, Strasbourg ,2018.
- Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2017).
- Emily M . Weitzenbock, Electronic Agents and the Formation of Contracts, The International Journal of Law and Information Technology ,Vol.9 No.3, pp. 204-234, Journal website at :http// www3.oup.co.uk.inttec. Oxford University Press, 2001.
- Giovanni (S), Agent in cyber law, in "Workshop on the law on electronic agent", LEA, 2002.
- Human Rights League V Council of Ministers, Case C-817/19. Court of Justice of the European Union (CJE), 27 January 2022.
- im Mather, Subra Kumaraswamy and Shahad Latif, Cloud Security And Privacy, Published By O Reilly Media Inc, United State Of America, 2009.
- Kennedy v. the United Kingdom, 18.05.2010. (application no. 26839/05).
- Oren Etzioni ,Daniel S. Weld ,Intelligent Agents On The Internet , Department of Computer Science and Engineering , University of

Washington, May 30, 2005 .
- Paul Voigt And Axel von dem Bussche, The EU General Data Protection Regulation (GDPR), A Practical Guide, Springer International Publishing, 2017.
- Prashant Mali, GDPR Articles With Commentary & EU Case Laws, Cyber Iformedia Publishing, 2019.
- Privacy International and Others v. the United Kingdom, 4 September 2020, Application no. 46259/16 .
- Ropert Neumann, The electronic business foundation, Master Thesis, OTTO – VON, Guericke Magdeburg, Germany.
- Tomas Jon, Electronic telephonic trade , Paris, Dalloz ,1990.
- World Health Organization: The protection of personal data in health information systems principles and processes for public health. 2021.

ب. المراجع الفرنسية.

- Benoit Tabaka et Yann Tesar, Loi informatique: un nouveau cadre juridique pour le traitement des données à caractère personnel, Dossier, 2004..
- Ch. Caron, Appréciation de l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile, Comm., JCP E, n° 9, 28 Février 2008.
- Constancias Claire – Mavault Laureen, La publicites sur internet, Sans maiso d' éditions, 2010 .
- Emmanuel, Cornu – Alexandre Cruquenaire; La protection des marquees sur internet, Cahiers du centre recherché information et droit, 2007
- Frédéric Pollaud-Dulian: Programmes d'ordinateur. Épuisement du droit de distribution. Revente d'occasion de copies. Supports physiques qui ne sont pas d'origine. Exceptions au droit de reproduction du logiciel, RTD Com, N° 04 du 19/01/2017.
- G. LOISEAU, L'exploitation de données personnelles collectées sur le web, Com. Comm. Electr, N° 9, Septembre 2012.
- Ibrahim Coulibaly, La protection des données à caractère personnel dans le domaine de la recherche scientifique. Thèse, Université de Grenoble, 2011.
- Jean Malherb, La vie privee et droit moderne, Paris, 1967
- Jean-Michel Bruguiere, Droits patrimoniaux de la personnalité— RTD civ. 2016. 1: 21 mars 2016.
- Maitre Jean, Pierre Gasnier, Les identifiants de l' internet , Noms de domaine , Conflites avec les autres droit, Le droit de l ' enterprise et

internet, Actes de colloque de Marseille, Institut de droit des affaires, 2001.
- Marine DE Montecier, Le droit @ l'heure des réseaux sociaux , Mémoire, HEC, Université Paris I– Panthéon-Sorbonne Paris, 2011.
- Michelle & Philippe Jean – Baptiste, Le marketing en ligne, Guide pratique, Eyrolles, Editions d' organization.
- Nathalie Moreau, La formation du contrat electronique, DEA, droit des contrats, Université de Lille 2, 2003 / 2004.
- P.Bouzat et J.Pinatel, Traité de droit penal de criminology, T. III, Dalloz, 1975.
- Philippe Dimitriou, L' application du droit de la cryptologie en Matiére de sécurite desréseaux informatiques, Faculté des sciences juridiques, Politiques et socials de Lille 2, Droit et Santé école Dctorale , No 74, 2002.
- Piere Albert, La Presse Francaise , Notes et études documentaires kai 197.
- R. Perray, Adresse IP et données personnelles, un besoin de convergence d'interprétation entre juges, Gaz. Pal. 2009.
- Sédaillan, La directive européenne, Vie privée et communications électroniques, Légipresse janv 2003, N 198.
- Sulliman Omrajee, Le data mining , Aspects juridiques de l'intelligence artificielle auregard de la protection des données personnelles. Mémoire, Faculté de Droit Université Montpellier I, Année Universitaire 2001-2002.
- T. Hassler, La crise d'identité des droits de la personnalité, LPA 2004.
- V. Julien Le Clainche, La protection des données personnelles nominatives dans le cadre de la recherché dans le domaine de la santé. Comparaison du droit français et Américain, Mémoire de D.E.A. Faculté de droit des sciences économiques et de gestion, Université Montpellier I, 2001.
- Van Dael ,La fascalite indirecte des transactions electroniques, sur la livre commerce electronique, Le temps des cetitudes, Editions Delta, 2001.
- Wong. J., Using a brand identity index for relevancy in teaching collegiate marketing, Journal of applied business and economic, 2007.

الفهرس

المستخلص: ..... - ٧٣ -
الكلمات المفتاحية: ..... - ٧٣ -
Research Summary ..... - ٧٤ -
Key words: ..... - ٧٤ -
مقدمة: ..... - ٧٦ -
المبحث الأول: وسائل وصور التعدي على البيانات الشخصية الرقمية ..... - ٧٨ -
المطلب الأول: حيازة وإنتاج البيانات الشخصية الرقمية ..... - ٨٠ -
المطلب الثاني: الإطلاع غير المشروع على البيانات الشخصية ..... - ٨٤ -
المطلب الثالث: تصوير وتسجيل البيانات الشخصية وإفشائها ..... - ٨٩ -
المطلب الرابع: الاعتداء على البيانات الشخصية في المعاملات التجارية الإلكترونية ..... - ٩٣ -
المبحث الثاني: نطاق الحماية الدولية للبيانات الشخصية الرقمية ..... - ١٠١ -
المطلب الأول: حقوق صاحب البيانات الرقمية ..... - ١٠٣ -
المطلب الثاني: أحكام معالجة البيانات الشخصية الرقمية ..... - ١٠٩ -
المطلب الثالث: أحكام نقل البيانات الشخصية خارج إقليم الدولة ..... - ١١٨ -
المطلب الرابع: سياسة المواقع والتطبيقات الإلكترونية لحماية البيانات الشخصية الرقمية ..... - ١٢٠ -
المبحث الثالث: ضوابط الحماية الدولية للبيانات الشخصية الرقمية ..... - ١٢٤ -
المطلب الأول: مبدأ التناسب بين حماية البيانات الشخصية الرقمية والحق في المعلومة ..... - ١٢٥ -
المطلب الثاني: مبدأ التناسب بين حماية البيانات الشخصية الرقمية والحق في الإطلاع ..... - ١٢٨ -
الخاتمة ..... - ١٣٢ -
أولاً: النتائج: ..... - ١٣٢ -
ثانياً: التوصيات: ..... - ١٣٣ -
قائمة المراجع ..... - ١٣٤ -
الفهرس ..... - ١٤٥ -