مجلة جامعة الملك سعود (الحقوق والعلوم السياسية)، مج (٣٢)، ع (١)، ص ص ١-٦٠، الرياض (٢٠٢٠م/ ١٤٤١هـ)

الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتداولها (دراسة في ضوء اللائحة التنظيمية رقم ٦٧٩/ ٢٠١٦ الصادرة عن البرلمان الأوروبي)

علاء عيد طه

أستاذ القانون المدني المساعد، كليات الشرق العربي للدراسات العليا، الرياض

(قدم للنشر في ٩/ ٥/ ١٤٤٠هـ، وقبل للنشر في ٢٦/ ٦/ ١٤٤٠هـ)

ملخص البحث. فرضت التطورات المتسارعة في مجال تقنية المعلومات قيام المشرع الأوروبي بإصدار تنظيم جديد لحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية وتداولها. فقام بوضع العديد من المبادئ الحاكمة لعملية المعالجة والضوابط على حرية حركة البيانات الشخصية وتداولها.

ويجب النظر إلى الحق في حماية البيانات الشخصية على أنه ليس حقاً مطلقاً، بل ينبغي النظر إليه فيما يخدم المجتمع في كافة المجالات الاجتماعية، والاقتصادية، والأمنية ... إلخ وفق ضوابط محددة. لذا اتجه المشرع الأوروبي نحو إيجاد إطار قوي لحماية البيانات مع السماح بتوظيف معالجة البيانات في دعم الاقتصاد الرقمي والسوق الداخلية.

وقد حافظ المشرع الأوروبي في هذا التنظيم الجديد لحماية البيانات الشخصية على الحقوق الأساسية للأفراد، وتقيد بالمبادئ المعترف بها في الميثاق الأوروبي والمعاهدات الدولية، لاسيما احترام الحياة الخاصة، والأسرية، والاتصالات، وحرية التعبير، والمحاكمة العادلة، وإدارة الأعمال التجارية، والتنوع الثقافي والديني واللغوي.

إضافة لما سبق، فقد حرص المشرع الأوروبي في التنظيم الجديد لحماية البيانات الشخصية على معالجة العديد من الإشكالات القانونية التي تنتج عن عملية معالجة البيانات أبرزها الحق في أمن البيانات وسريتها، ومعالجة البيانات في سياق العمل، والحق في النسيان الرقمي، ومعالجة البيانات الشخصية لأغراض إعلانية، أو لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية ... إلخ.

الكلمات المفتاحية: البيانات الشخصية، اللائحة التنظيمية ٦٧٩/ ٢٠١٦ للاتحاد الأوروبي، معالجة البيانات، النسيان الرقمي، أمن البيانات، سرية البيانات، معالجة بيانات الطفل، معالجة البيانات في سياق العمل، التعويض والمسؤولية.

THE LEGAL PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (STUDY IN REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL)

Alaa Eid Taha
Assistant Professor of Civil Law, Arab East Colleges for Graduate Studies, Riyadh

(Received 09/05/1440 H., Accepted for Publication 26/06/1440 H.)

Abstract. Rapid developments in the field of information technology have forced the European legislator to issue a new regulation to protect people in the processing and handling of their personal data. The European legislator developed several principles governing the processing of data and the controlling of the free movement.

The right to the protection of personal data must be seen as not an absolute right, but should be seen in the service of society in all social, economic, security spheres, etc. according to specific controls. Thus, the European legislator has tended to create a strong data protection framework while allowing the use of data processing to support the digital economy and the domestic market.

The European legislator, in the new data protection regulation, has preserved the fundamental rights of individuals and has applied the principles recognized in the European Charter and international treaties, in particular the respect for private and family life, communications, freedom of expression, fair trial and administration business, cultural, religious and linguistic diversity.

In addition to the above, the European legislator, in the new European Regulation for the protection of personal data, has addressed many of the legal forms that resulted from the process of data processing, most notably the right to data security and confidentiality, data processing in the context of work, and the right to digital forgetting, processing of personal data for advertising purposes, for purposes of scientific or historical research or for statistical purposes, etc.

Keywords: Personal data, Regulation (EU) 2016/679 of the European Union, Data processing, Digital forgetting, Data security, Data confidentiality, Processing of child data, Data processing in the context of work, Compensation and liability.

مقدمة

رافقت التطورات التي عرفتها التقنية المعاصرة وصول المعلومات والبيانات إلى كثير من شركات تكنولوجيا المعلومات في مختلف بقاع العالم، وقد عاشت هذه الشركات نحو عقدين من الزمان خاضعة لتشريعات لم تكن كافية في حينها لحماية البيانات الشخصية بشكل كافٍ من مخاطر انتهاك الخصوصية. إلا أن الأمور تتجه في الوقت الحاضر نحو فرض التزامات صارمة من أجل حماية البيانات الشخصية لمستخدمي منصات التواصل الاجتماعي وغيرها من وسائل التقنية الحديثة.

وقد أرست اللائحة الأوروبية الصادرة لحماية البيانات ذات الطابع الشخصي رقم ٦٧٩/ ٢٠١٦ الصادرة عن البرلمان الأوروبي والمجلس General Data Protection Regulation (GDPR) بتاريخ السابع والعشرين من أبريل/ نيسان ٢٠١٦م، قواعد أكثر صرامة لحماية البيانات الشخصية للأشخاص الطبيعيين فيما يتعلق بمعالجتها واستغلالها في الأغراض المختلفة وتداولها(١). وذلك انطلاقاً من الفلسفة التشريعية للتوجيه السابق المرتكز على مبادئ احترام حقوق الإنسان وضمان حماية خصوصية الحياة الخاصة(٢).

ويشهد العالم اليوم تطوراً هائلاً في مجال تكنولوجيا المعلومات لدرجة مكنت الإنسان من تبادل المعلومات الرقمية والبيانات الشخصية، وعززت من قدراته على التواصل بشكل سريع وفعال.

وتُعد قضية خصوصية البيانات وحمايتها في الآونة الأخيرة من أكثر القضايا التي أرهقت القانونيين والحقوقيين وذلك وسط ما يشهده العالم من مخالفات رقمية تمثلت آخرها في فضيحة تسريب بيانات أكثر من سبعة وثمانين مليون مستخدم لمنصة شبكة التواصل الاجتماعي Facebook(٣).

---

(١) ألغت هذه اللائحة التنظيمية التوجيه الأوروبي رقم ٩٥/ ٤٦/ EC والمعروف باسم (اللائحة العامة لحماية البيانات). وذلك حسب ما نصت عليه المادة (٩٤) من هذه اللائحة والتي جاء نصها على النحو التالي:

Article 94: Abrogation de la directive 95/46/CE: 1. La directive 95/46/CE est abrogée avec effet au 25 mai 2018.
2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE s'entendent comme faites au comité européen de la protection des données institué par le présent règlement.

لمطالعة التوجيه كاملاً يرجى مراجعة الرابط التالي:

Règlement (UE) 679/2016 du Parlement européen et du Conseil du 27 avril 2016 "Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
https://www.cnil.fr/en/official-texts

والتوجيه رقم ٩٥/ ٤٦/ EC هو توجيه من الاتحاد الأوروبي، ويُعد النص المرجعي لحماية البيانات الشخصية للدول الأعضاء في الاتحاد. وقد نشر في الجريدة الرسمية للاتحاد الأوروبي في ٢٣ نوفمبر/ تشرين الثاني ١٩٩٥م، وعنوانه رسمياً التوجيه ٩٥/ ٤٦/ EC الصادر عن البرلمان الأوروبي والمجلس المؤرخ ٢٤ = أكتوبر/ تشرين الأول ١٩٩٥م بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعاملة البيانات الشخصية وحرية حركة مثل هذه البيانات. ولا يشمل البيانات الشخصية التي تعالج في إطار الركيزة الثالثة للاتحاد الأوروبي، وهي التعاون بين الشرطة والقضاء في المسائل الجنائية، التي تشمل جميع ملفات الشرطة والعدالة والاستخبارات. كما أنها لا تعنى إلا بتنظيم الدول الأعضاء؛ وتخضع البيانات الشخصية التي تجمعها المؤسسات المجتمعية للبند ٤٥/ ٢٠٠١ الذي أُنشئ بموجبه الإشراف على حماية البيانات (EDPS). وقد أُلغي هذا التوجيه بموجب اللائحة التنظيمية العامة لحماية البيانات محل الدراسة. وقد كان الغرض من التوجيه هو حماية الحق في الخصوصية، الذي يندرج أيضاً في المادة (٨) من الاتفاقية الأوروبية لحقوق الإنسان، التي صدقت عليها جميع الدول الأعضاء في الاتحاد الأوروبي، وكذلك في ميثاق الحقوق الأساسية للاتحاد الأوروبي الذي أصبح مُلزماً من عام ٢٠٠٧م، ويستثنى من ذلك عدد قليل من البلدان.

(2) Maryline Boizard : Le droit à l'oubli; Faculté de droit et de science politique, Rennes 1 Institut de l'Ouest : Droit et Europe IODE UMR CNRS 6262 Recherche réalisée avec le soutien de la Mission de recherche Droit et Justice Février 2015; p.7

من الفقه المصري انظر: محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. القاهرة: دار النهضة العربية، (٢٠١٦م)، ص ٦٨ وما بعدها. وهامش رقم (٢) من نفس الصفحة. وانظر أيضاً: سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي. القسم الأول، *مجلة الحقوق*، جامعة الكويت، مج (٣٥)، ع (٣)، (سبتمبر ٢٠١١م)، ص ص ٣٧٥-٤٣٤، ص ٣٧٦ وما بعدها.

(٣) نشرت صحيفة نيويورك تايمز وصحيفة الجارديان وصحيفة أوبزيرفر أخباراً في الخامس من أبريل/ نيسان ٢٠١٨م مفادها أن =

وفي سياق حماية ثورة العصر الحديث "البيانات" دخلت هذه اللائحة الأوروبية المعنية بحماية البيانات الشخصية لمستخدمي شبكة الإنترنت ومواقع التواصل الاجتماعي حيز التنفيذ في ٢٥ مايو/ أيار ٢٠١٨م حسب ما نصت عليه الفقرة التاسعة من المادة الثالثة والثمانون منها(٤).

وتجدر الإشارة إلى أن اللائحة الحالية ٢٠١٦/٦٧٩ عالجت حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية من جانب السلطات المختصة لأغراض منع الجرائم الجنائية أو التحقيق فيها أو كشفها أو ملاحقتها قضائياً أو تنفيذ العقوبات الجنائية، بما في ذلك الحماية من التهديدات التي يتعرض لها الأمن العام في الدولة. غير أن البيانات الشخصية التي تجهزها السلطات العامة لأغراض الأمن بموجب هذه اللائحة تخضع عند معالجتها لتوجيه خاص بها وهو التوجيه ٢٠١٦/٦٨٠ (EU) الصادر عن البرلمان الأوروبي والمجلس.

وتوفر اللائحة الأوروبية الجديدة حماية محددة للأطفال فيما يتعلق بمعالجة بياناتهم الشخصية والضمانات الخاصة بتلك المعالجة؛ لأنهم أقل وعياً بالمخاطر والعواقب بحقوقهم. سواءً فيما يتعلق باستخدام بياناتهم الشخصية لأغراض التسويق أو تكوين صورة كاملة عن الطفل لأغراض أخرى. مع الإشارة إلى أن اللائحة لا تشترط موافقة الولي أو المسؤول عن الطفل في سياق الخدمات الوقائية أو الاستشارية أو النافعة المقدمة مباشرة إلى الطفل.

ومن الأمور التي تميزت بها هذه اللائحة مسألة أمن البيانات الشخصية فتشترط ضمان أمن الشبكات والمعلومات بالقدر اللازم والمتناسب مع أهمية هذه البيانات، وبمعنى آخر تشترط قدرة الشبكة أو نظام المعلومات على مقاومة الاختراق المعلوماتي، وأن يكون نظام المعالجة على مستوى عالٍ من الحماية، وقادر على مواجهة المخاطر المختلفة التي قد تتعرض لها البيانات الشخصية المخزنة أو المرسلة وضمان سلامتها وسريتها، وتشمل سبل الأمن على سبيل المثال، منع الوصول غير المصرح به إلى شبكات الاتصالات الإلكترونية والبرمجيات الخبيثة ووقف إلحاق الضرر بنظم الاتصالات الحاسوبية والإلكترونية. ومن أجل الحفاظ على الأمن ومنع التجهيز في انتهاك لهذه اللائحة، ينبغي للمراقب المالي أو المعالج ان يقيم المخاطر الملازمة للمعالجة وأن ينفذ التدابير اللازمة للتخفيف من تلك المخاطر، مثل التشفير.

وقد وضعت اللائحة الجديدة العديد من الضمانات المناسبة لمعالجة الفئات الخاصة من البيانات الشخصية، أهمها أنه لا ينبغي معالجة الفئات الخاصة من البيانات الشخصية التي تستحق حماية قصوى إلا عند الضرورة لتحقيق أغراض لصالح الأشخاص الطبيعيين والمجتمع ككل لاسيما عند

= شركة فيسبوك أفادت بأن شركة كمبردج أناليتيكا للاستشارات السياسية ربما وصلت على نحو غير مشروع إلى معلومات شخصية تخص قرابة سبعة وثمانين مليوناً من مستخدمي شبكة التواصل الاجتماعي، وذلك في زيادة عن تقديرات سابقة لوسائل إعلام إخبارية تجاوزت ٥٠ مليوناً. وقال مايك شروفر كبير مسؤولي التكنولوجيا في الشرطة في تدوينه: "إن معظم السبعة والثمانين مليون شخص الذين وصلت كمبردج أناليتيكا إلى بياناتهم كانوا في الولايات المتحدة". وعملت الشركة مع الحملة الانتخابية للرئيس الأمريكي دونالد ترامب عام ٢٠١٦م. وأوضحت فيسبوك أنها تتخذ إجراءات لتقييد وصول البيانات الشخصية لطرف ثالث. وتتعرض أكبر شركة للتواصل الاجتماعي في العالم لانتقادات شديدة من المستثمرين وتواجه غضب المستخدمين والمعلنين والنواب بعد سلسلة فضائح بشأن موضوعات إخبارية كاذبة والتدخل في الانتخابات والخصوصية. للمزيد راجع الرابط التالي:
https://th2plant.blogspot.com/2018/04/FBUsers-Violate.html

(4) Article 83: **Conditions générales pour imposer des amendes administratives:** 9. Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, le présent article peut être appliqué de telle sorte que l'amende est déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle. En tout état de cause, les amendes imposéeuueyus sont effectives, proportionnées et dissuasives. Les États membres concernés notifient à la Commission les dispositions légales qu'ils adoptent en vertu du présent paragraphe au plus tard le **25 mai 2018** et, sans tarder, toute disposition légale modificative ultérieure ou toute modification ultérieure les concernant.
Le 25 mai 2018, le règlement européen est entré en application. De nombreuses formalités auprès de la CNIL disparaîssent. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité. Voir https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

معالجة البيانات الشخصية في مجال قانون العمل، وقوانين الحماية الاجتماعية بما في ذلك المعاشات التقاعدية والتأمين الصحي، والوقاية من الأمراض المعدية أو مكافحة تهديدات الصحة العامة بما في ذلك الصحة العامة، أو لأغراض الأرشفة للصالح العام، أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية.

ولضمان حفظ حقوق الأشخاص المعنيين الذين عولجت بياناتهم الشخصية، ولضمان الامتثال للأحكام الواردة باللائحة فقد أوجبت على القائم بعملية المعالجة الاحتفاظ بسجلات أنشطة المعالجة التي تندرج تحت مسؤوليته. بل وإلزام كل مراقب ومعالج بالتعاون مع السلطة الإشرافية على عمليات المعالجة وإتاحة تلك السجلات، عند الطلب، لكي يتسنى لها العمل على رصد عمليات التجهيز هذه. خاصة البيانات التي تسهم في تحديد هوية شخص طبيعي، مثل التحليل أو التنبؤ والجوانب المتعلقة بأداء الشخص الطبيعي في العمل، وحالته الاقتصادية، أو الصحة، أو التفضيلات أو المصالح الشخصية، أو السلوك، أو المكان أو الحركات، التي تنتج آثاراً قانونية تتعلق به أو تؤثر عليه بشكل كبير.

ونحن إذ نسلم بأنه يجب النظر إلى الحق في حماية البيانات الشخصية على أنه ليس حقاً مطلقاً، بل ينبغي النظر إليه فيما يخدم المجتمع في شتى المجالات وفق ضوابط محددة. فقد اتجه المشرع الأوروبي نحو إيجاد إطار قوي لحماية البيانات مع السماح بتوظيف معالجة البيانات في دعم الاقتصاد الرقمي والسوق الداخلية، بل قام بالتعزيز من حقوق المستخدمين على بياناتهم الشخصية، وفرض عقوبات كبيرة على معظم المخالفات الرقمية(٥)؛ بحيث سيتمكن المستخدم من السيطرة الكاملة على نشر بياناته الشخصية، ويصبح له الحق في الموافقة أو الرفض بشأن استخدام تلك البيانات ومشاركتها مع المواقع المختلفة، بالإضافة إلى الحق في معرفة الجهات التي تستخدم بياناته والغرض من استخدامها، وطريقة وأسباب هذا الاستخدام. كما تتيح له أيضاً حظر معالجة بياناته لأسباب تجارية، وإمكانية حذفها بموجب الحق في النسيان الذي يتيح للمستخدم حذف بياناته من على شبكة الإنترنت(٦).

---

(٥) وتنص هذه اللائحة على غرامات مالية ضخمة تصل إلى عشرين مليون يورو أو ما يعادل ٤٪ من المبيعات العالمية السنوية للشركات المخالفة إذا حدث انتهاك للبنود المنصوص عليها في المادتان الثالثة والثمانون والرابعة والثمانون.

Règlement (UE) 2016/679, Art. 83 : Conditions générales pour imposer des amendes administratives: 4. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:

a) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43;
b) les obligations incombant à l'organisme de certification en vertu des articles 42 et 43;

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:

a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9;
b) les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22
c) les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale en vertu des articles 44 à 49;
d) toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX;
e) le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58, paragraphe 1.

6. Le non-respect d'une injonction émise par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, fait l'objet, conformément au paragraphe 2 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Article 84 : Sanctions : 1.Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.

2. Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

(٦) للمزيد حول هذا الحق راجع:

Sandrine Carneroli : Le droit à l'oubli, Du devoir de mémoire au droit à l'oubli , 1re édition, Editeur: Larcier, 2016, p.6; David Dechenaud : Le droit à l'oubli numérique, Données nominatives - Approche comparée, Larcier - Création Information Communication,1re édition , Parution , 2015, p.15.

إشكالية الدراسة

إن استخدام التكنولوجيا[٧] الرقمية ذات التقنية العالية في ميدان جمع المعلومات من جهة والتواصل بين الأشخاص من جهة أخرى عمق من هوة التناقضات التي برزت منذ القدم بين حق الأفراد في الحياة الخاصة - كحق مقنن دستورياً - ومستقر عليه دولياً ومقتضيات الاطلاع على بيانات الأشخاص، متجاوزة بذلك أطر الحماية المقررة مما أدى إلى خلق واقع صعب هدد هذا التوازن وجعل هذا الحق عرضة أكثر من أي وقت مضى للانتهاك الذي ترك آثاره السلبية الواضحة على العديد من مناحي الحياة الاقتصادية والاجتماعية والقانونية.

ومن هنا تبرز الإشكالية الرئيسة للدراسة الحالية والتي تكمن في المعالجة القانونية لحماية البيانات الشخصية للأشخاص الطبيعيين في ضوء أحكام اللائحة الأوروبية ٢٠١٦/٦٧٩، وهو ما يقتضي منّا وصف وتحليل ومناقشة الإطار القانوني لهذه الحماية فيما يتعلق بمعالجتها واستغلالها في الأغراض المختلفة وتداولها بين القائمين بالمعالجة.

ولا شك أنه يتفرع عن هذه الإشكالية العديد من المشكلات الأخرى التي تخص عناصر ذلك الإطار القانوني للحماية كمعالجة الحق في النسيان الرقمي كحق ينادي الفقه القانوني بتنظيمه وحق الدولة في تخزين وأرشفة البيانات الشخصية للمصلحة العامة؛ فقد باتت محادثات الأشخاص الطبيعيين وتحركاتهم وبياناتهم الشخصية التي يتم نشرها وتداولها من خلال الوسائط الرقمية على الإنترنت تخضع للمراقبة الإلكترونية من قبل الجهات الحكومية؛ إذ أصبح بإمكان سلطات أي دولة - استناداً لاعتبارات الأمن الوطني وسعياً لمكافحة الجرائم داخلياً أو تلك العابرة للحدود وعن طريق البرامج والتطبيقات الإلكترونية المخصصة لهذا الغرض - اختراق حق الأفراد في الخصوصية المعلوماتية.

وفي نفس الإطار نتساءل أيضاً ماذا عن المستخدمين والأشخاص الذين يتفاعلون كثيراً مع وسائل التواصل الاجتماعي وتطبيقات الهواتف الذكية ويضعون الكثير من البيانات الشخصية والمعلومات الخاصة أحياناً، هل هناك من سبل أو قواعد لحمايتها وضمان تأمينها من أخطار التحليل والمعالجة غير القانونية؟ وهل هناك قواعد لتعويض هذا الشخص عن انتهاك بياناته في حال الاعتداء عليها؟ وهل من حلول أو مبادئ وضعتها اللائحة الأوروبية ٢٠١٦/٦٧٩ لمعالجة هذه الإشكالية القانونية؟

أهمية الدراسة وتقسيمها

إن أهمية هذه الدراسة لا تنبع فقط من كونها تتناول موضوعاً حديثاً يتعلق بحماية البيانات الشخصية لعملية معالجة البيانات تتعدى في كثير من الأحيان الغرض الذي من أجله تمت الموافقة على عملية معالجة البيانات إلى مسألة الأمن الاجتماعي. فالمسألة إذن تتعلق بأمرين الأمن الشخصي للأفراد من جهة، ومسألة السلامة الاجتماعية من جهة أخرى لذا كان من الضروري وصف وتحليل الإطار القانوني.

وعلى جانب آخر، يتم في الوقت الحالي استغلال البيانات الشخصية اقتصادياً لأغراض إعلانية من قبل شركات التواصل الاجتماعي التي تعتبر أن البيانات الشخصية هي رأس مال الشركة، لذلك كان التحدي الأكبر أمام المشرع الأوروبي هو سن مثل هذه اللائحة وإدخالها حيز النفاذ للحد من استخدام البيانات بهذه الطريقة غير المشروعة وهو أمر تقوم به منصات التواصل الاجتماعي، وشركات تكنولوجيا المعلومات[٨].

(٧) نجاة جدي، المعلوماتية وحق المؤلف. بحث منشور بمجلة *دراسات وأبحاث*، جامعة زيان عاشور (الجلفة)، الجزائر، ع (٦)، ص ص ١٨٦-٢٠٠.

(٨) في تقرير نشرته نيويورك تايمز في ٢٧ مارس ٢٠١٨م قالت فيه "أن شركة Palantir Technologies تتعاون مع وكالة الاستخبارات الأمريكية والبنتاجون وضالعة مع فيسبوك وكامبردج أنالتيكا في تحليل البيانات وإرسال رسائل موجهة تدعم المرشح الأمريكي دونالد ترامب، كما عملت «palantir» بشكل وثيق مع علماء البيانات على تكنولوجيا التنميط النفسي، الذي اقترح على العلماء إنشاء التطبيق الخاص بهم - الهاتف المحمول القائم على اختبار الشخصية للوصول إلى مستخدمي فيسبوك "صديق شبكات =

وهنا أرى أن الخصوصية قد أصبحت شيئاً من الماضي[٩] وساعد على ذلك الأمية الرقمية، فإذا سألنا من منا يقرأ نشرة الخصوصية الخاصة بـFacebook أو Twitter أو أي تطبيق يقوم بتحميله على هاتفه الخاص به؟ فستكون الإجابة هي أن غالبيتنا لا يطلعون على سياسات الخصوصية التي توفر في بعض الأحيان حداً أدنى من ضمان عدم الاعتداء على البيانات[١٠].

فرض كل هذا التغير الناتج عن تطور الحياة الرقمية من جهة، وتزايد التهديدات والمخاوف من تلاشي الحق في الخصوصية المعلوماتية من جهة أخرى نفسه على حقل الحماية القانونية المقرر لحماية البيانات الشخصية وتداولها؛ حيث أدى استخدام هذه الأساليب إلى اقتحام حصون هذا الحق، فبات من الواضح أن حماية البيانات الشخصية تقتضي تدخل المشرعين في كافة الدول بالإضافة لتضافر الجهود الدولية لحمياتها بالأسلوب الذي يتلاءم وطبيعة الأخطار المستجدة في الحياة الرقمية من خلال تطوير المعالجة القانونية للموضوعات ذات العلاقة.

كل هذا يدعونا إلى أن نقر بحقيقة معينة هو أن الخصوصية في عصر التواصل الاجتماعي لم تعد موجودة وعلينا بالمقابل أن نخفف الضرر الذي يمكن أن يقع على أي مستخدم لهذه الشبكات والمنصات. فمن يستخدم شبكات التواصل الاجتماعي ويضع معلوماته لابد وأن يدرك تماماً أنه بالرغم مما يسمى بالضوابط الأمنية وسياسات الخصوصية فهي للعلم تحت تأثير الاستخدام بطريقة أو بأخرى. من هنا جاءت أهمية هذه الدراسة التي تحاول أن تناقش وتحلل الإطار القانوني لها. من أجل ذلك كله تم تقسيم هذه الدراسة على النحو التالي:

- الفصل الأول: ماهية البيانات ذات الطابع الشخصي في ضوء أحكام اللائحة الأوروبية رقم ٢٠١٦/٦٧٩.
  - المبحث الأول: مفهوم البيانات ذات الطابع الشخصي في اللائحة الأوروبية الجديدة.
  - المبحث الثاني: المبادئ الحاكمة لمعالجة البيانات ذات الطابع الشخصي وفقاً لأحكام اللائحة الأوروبية.
- الفصل الثاني: الإطار القانوني لحقوق والتزامات القائم بالمعالجة والشخص المعني في ضوء أحكام اللائحة الأوروبية رقم ٢٠١٦/٦٧٩.
  - المبحث الأول: التزامات القائم بعملية المعالجة في ضوء أحكام اللائحة الأوروبية.
  - المبحث الثاني: حقوق الشخص المعني على بياناته موضوع المعالجة في ضوء أحكام اللائحة الأوروبية.
- الفصل الثالث: الإشكالات القانونية التي تثيرها معالجة البيانات الشخصية في اللائحة الأوروبية ٢٠١٦/٦٧٩.

= ومنصات التواصل الاجتماعي" وذلك وفقاً للوثائق التي حصلت عليها صحيفة نيويورك تايمز. واتخذت كامبريدج أنالتيكا في نهاية المطاف نهجاً مماثلاً. بحلول أوائل صيف ٢٠١٤م، حيث وجدت الشركة أن باحثاً جامعياً حصل على البيانات الشخصية لمستخدمي منصة التواصل الاجتماعي فيسبوك. قام الباحث بكشط البيانات الخاصة بأكثر من خمسين مليون مستخدم فيسبوك، كما ذهبت كامبريدج أنالتيكا إلى الأعمال التجارية فقامت ببيع ما يسمى بالملامح السيكولوجية للناخبين الأميركيين، ووضع نفسها على مسار تصادم مع المنظمين والمشرعين في الولايات المتحدة دول وبريطانيا. للمزيد حول هذا الموضوع:
https://www.nytimes.com/2018/03/27/us/cambridge-analytica-palantir.html

(٩) هنا يجدر بنا التنويه – وقبل البدء في الدراسة – الإشارة إلى أمرين:
أولاً: وجوب تكثيف الجهود نحو محو الأمية الرقمية ليكون الجميع على علم بشروط وسياسات الخصوصية التي تعزز من خصوية المستخدم على هذه المنصات.
ثانياً: وجوب دعم المشرعين في شتى أنحاء العالم في سن القوانين تفرض على الشركات والمؤسسات التزامات تحد من الاستخدام السيئ للمعلومات الشخصية. لأنه وبتعبير بسيط "عندما يكون التطبيق مجانياً يكون المستخدم هو السلعة".

(١٠) وفقاً لشركة UPGuard وجدت أن التكنولوجيا في مستودع مفتوح يحتوي على أدوات Smercasbord تستخدم للتأثير على سلوك الأفراد، بما في ذلك "مجموعة من التطبيقات المتطورة، وبرامج إدارة البيانات، وأجهزة تتبع الإعلانات، وقواعد بيانات المعلومات التي يمكن استخدامها بشكل جماعي لاستهداف الأفراد والتأثير عليهم من خلال مجموعة متنوعة من الأساليب، بما في ذلك المكالمات الهاتفية الآلية، ورسائل البريد الإلكتروني، ومواقع الويب السياسية، والتطوع في استطلاع الرأي، وإعلانات Facebook، وغيرها من مواقع التواصل الاجتماعي. للمزيد يرجى مطالعة الرابط التالي:
https://nakedsecurity.sophos.com/ar/2018/03/28/cambridge-analyticas-secret-coding-sauce-allegedly-leaked/

- المبحث الأول: أمن البيانات الشخصية.
- المبحث الثاني: الحق في حذف البيانات (النسيان الرقمي) والعلاقة مع الأرشفة للمصلحة العامة.
- المبحث الثالث: معالجة البيانات الشخصية لأغراض إعلانية أو لأغراض البحث العلمي.
- المبحث الرابع: معالجة البيانات في سياق علاقات العمل.
- المبحث الخامس: المسؤولية والتعويض.

- خاتمة الدراسة.
- قائمة المراجع.

الفصل الأول:
ماهية البيانات ذات الطابع الشخصي
في ضوء أحكام اللائحة الأوروبية ٢٠١٦/٦٧٩

تمهيد وتقسيم

تُحتم شبكات التواصل الاجتماعي على مستخدميها قبل الولوج في عوالمها إدخال بياناتهم الشخصية لأجل إكمال عملية التسجيل في تلك الشبكات والبدء في استخدام خدماتها المتنوعة، لذا كان من المهم معرفة مفهوم البيانات الشخصية حتى يمكن حمايتها من الاستخدام الضار المتمثل في اختراق حق الأفراد في الخصوصية من قبل شبكات ومنصات التواصل الاجتماعي، ومن مزودي خدمات الإنترنت.

كما أصبح هذا الحق منذ لحظة دخول الشخص لعالم الإنترنت، أو بمجرد إجراء مكالمة هاتفية، عرضة لمختلف صور التعدي، سواءً من خلال القرصنة وسرقة الهويات الرقمية أو الحسابات على شبكات التواصل الاجتماعي، أو عن طريق اختراق البريد الإلكتروني، وكسر كلمات المرور واختراق الأجهزة وما قد يترتب عنه من إفشاء للمعلومات والبيانات الشخصية، أو بالاعتداء على سرية المراسلات الاتصالات[١١].

فمن خلال الاطلاع على تلك البيانات وتمريرها لأطراف أخرى للاستفادة منها سياسياً أو اقتصادياً دون علم أصحابها ودون الحصول على الموافقات اللازمة لذلك. أضف لذلك أن هناك العديد من الشركات المتخصصة في مجال جمع البيانات الشخصية وتقسيمها وفق تقسيمات محددة إما جغرافية أو عمرية أو مذهبية أو غيرها، والتي تقوم باستهداف أصحاب تلك البيانات مباشرة من خلال الإعلانات الدعائية للمنتجات أو السلع، أو استخدامها من ناحية سياسية من خلال تمرير بعض الأفكار أو الرسائل السياسية أو تنفيذ أجندة ما لموضوع سياسي معين[١٢].

ويهدد تسريب البيانات الشخصية أمن أصحابها، الأمر الذي يثور معه التساؤل حول قواعد حفظ هذه البيانات. لذا كان لزاماً أن تتخذ منصات التواصل الاجتماعي الإجراءات الوقائية من أجل عدم الإفصاح عن هذه البيانات، أو عدم السماح بالوصول إليها سواءً من مشغلي التطبيقات أو شركات تحليل البيانات لاستخدامها في العديد من الأمور خاصةً إذا كانت تتعلق بأمور جدلية كالانتخابات السياسية.

والسؤال الذي يطرح نفسه هو كيف يمكن أن تؤثر البيانات الشخصية على قرارات أصحابها أو بمعنى أدق ما هي أهمية هذه البيانات؟ فبمعرفة الإجابة نستطيع أن نعرف السبب الذي من أجله تقوم الدول بسن القوانين لحماية البيانات الشخصية في التوقيت الحالي.

تعتبر البيانات – وبحق – عماد اقتصاد العصر الحديث؛ فمن غير البيانات لا يمكن معرفة سلوك صاحبها أو التأثير فيه؛ فشركات تحليل البيانات تقوم بعمل ملفات "سيكو جرافيك" من أجل توجيه رسائل مخصصة لهم، وهو أمر أشبه بالتحليل النفسي من أجل دراسة توجهات الشخص المعني صاحب البيانات وإرسال رسائل موجهة له من أجل التأثير في قناعاته في الأمر الذي تمت المعالجة لأجله، وهذا له تأثير كبير على المجتمع في تعزيز مفاهيم معينة في كثير من الأحيان غير مشروعة.

ولما كانت حماية البيانات الشخصية من الموضوعات التي تحتاج لمزيد من البحوث والدراسات لمعرفة التطورات القانونية

(١١) محمد البكاري، حماية سرية المراسلات الشخصية. مقال محكم ومنشور بمجلة *المنبر القانوني المغرب*، ع (٩)، (٢٠١٥م)، ص ص ٢٠٧-٢١٢، ص ٢٠٩.

(١٢) مروة زين العابدين صالح، *الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني*. القاهرة: مركز الدراسات العربية للنشر، (٢٠١٦م)، ص ٨٤.

الجديدة، ولاعتبارها أيضاً حجر الزاوية في الإعلانات والدعاية التجارية عن طريق استغلالها في معرفة توجهات الأشخاص ورغباتهم الاستهلاكية، فقد كانت أول وأكثر العناصر تأثراً بهذه التكنولوجيا، فقد رافقت التطورات التي عرفتها التقنية المعاصرة وصول البيانات الشخصية لكثير من الشركات التجارية التي تعتمد في تعاملاتها على استخدام البيانات الشخصية مثل شركات الطيران والفنادق وشركات السياحة والبنوك وشركات التأمين وشركات تكنولوجيا المعلومات(١٣).

لذا كان لزاماً أن نتعرض لمفهوم البيانات الشخصية من ناحية ثم نناقش المبادئ الحاكمة لمعالجة البيانات ذات الطابع الشخصي التي جاءت بها هذه اللائحة، ومن أجل ذلك فقد قمنا بتقسيم هذا الفصل إلى مبحثين على النحو التالي:

- المبحث الأول: مفهوم البيانات ذات الطابع الشخصي في اللائحة الأوروبية الجديدة.
- المبحث الثاني: المبادئ الحاكمة لمعالجة البيانات ذات الطابع الشخصي وفقاً لأحكام اللائحة الأوروبية.

المبحث الأول: مفهوم البيانات ذات الطابع الشخصي في اللائحة الأوروبية ٢٠١٦/٦٧٩

عرفت الفقرة الأولى من المادة الرابعة من اللائحة(١٤) البيانات الشخصية(١٥) بأنها "أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر، عن طريق الرجوع إلى واحد أو أكثر من العناصر المميزة له(١٦) وعلى وجه الخصوص الاسم أو رقم الهوية أو بيانات الموقع، أو الخصائص البدنية أو الفسيولوجية أو الوراثية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية. وتستلزم جميع مواقع التواصل الاجتماعي ممن يريد إنشاء حساب خاص به على أي موقع منها أن يقوم بوضع بياناته الشخصية التي تميزه عن غيره".

ويلاحظ على التعريف الوارد في نص اللائحة أن المشرع الأوروبي تبنى مفهوماً أكثر مرونة يسمح باستيعاب ودخول كافة أنماط البيانات الشخصية ضمن هذا المفهوم.

أضف لذلك أن التعريف السابق يساهم في جعل البيانات الشخصية أكثر تحديداً من خلال إعطاء أمثلة للعديد من أنماط البيانات الشخصية الخاضعة للحماية القانونية.

ويصف رأي في الفقه المصري(١٧) دور هذه البيانات في عملية التسجيل بمواقع التواصل الاجتماعي بقوله: "الإدلاء بالبيانات الشخصية إجراء أوليٌّ ووجوبيٌّ يتعين على كل من يرغب في الانضمام إلى عضوية مواقع التواصل الاجتماعي أن يقوم به؛ إذ يستهلُّ المستخدم خطوات انضمامه لأي موقع من هذه المواقع بتدوين اسمه، ولقبه، وتاريخ ميلاده، وجنسه، وعنوان بريده الإلكتروني، وغير ذلك من البيانات الوجوبية التي تتفاوت من موقع لآخر".

---

(١٣) أضف لذلك التطورات التكنولوجية الحاصلة في مجالات الحوسبة السحابية والبلوك تشين، وإنترنت الأشياء، أثرت بشكل كبير سلباً على خصوصية الأفراد وحرياتهم أيضاً.

(14) "Règlement (EU) 2016/679, Art. 4. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

(١٥) انظر في التعليق على هذه التسمية الزميل الأستاذ الدكتور أشرف جابر سيد في بحثه القيّم: *الجوانب القانونية لمواقع التواصل الاجتماعي: مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتويتر*. القاهرة: دار النهضة العربية، (٢٠١٣م)، ص ٤٥ وما بعدها. حيث يرى سيادته أن استخدام تعبير البيانات ذات الطابع الشخصي = les données à caractère personnel، أكثر مرونة من تعبير المعلومات الشخصية Information nominative وهو التعبير الذي كان يستخدمه قانون المعلوماتية والحرية ٧٨/١٧ قبل تعديله، وذلك لأن تعبير البيانات ذات الطابع الشخصي وفقاً لرأي سيادته يكفل حماية أوسع تشمل الملفات الصوتية والمرئية للمستخدم.

(16) «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

(١٧) محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. القاهرة: دار النهضة العربية، (٢٠١٦م)، ص ٣٧ وما بعدها.

ومن خلال ما سبق يمكن القول بأن البيانات ذات الطابع الشخصي يتمثل معناها في بيانات ترتبط بشخص محدد أو آخر قابل للتحديد، وهو ما ذهب إليه جانب من الفقه الفرنسي والمصري على حد سواءً[١٨] من خلال تحليل نص المادة الثانية من القانون الفرنسي (٨٠١) لسنة ٢٠٠٤م الخاص بحماية الأفراد إزاء معالجة البيانات ذات الطابع الشخصي، فقام بتصنيفها إلى بيانات للتعريف المباشر les données (d'identification) directe، وبيانات للتعريف غير المباشر.

ولم تقف الأمور في اللائحة الجديدة عند حد بيان مفهوم البيانات ذات الطابع الشخصي بل تناولت العديد من المصطلحات ذات العلاقة، وهي مصطلحات تدخل بشكل أساسي ورئيس في عملية المعالجة ولا يمكن أن تتم بدونها من الأساس، ومن بين هذه المصطلحات التي استخدمها المشرع الأوروبي مصطلح "التنميط" الذي نص عليه في المادة الرابعة وهو يعني "أي شكل من أشكال المعالجة الآلية للبيانات ذات الطابع الشخصي لاستخدام هذه البيانات الشخصية في تقييم بعض الجوانب الشخصية المتعلقة بالشخص الطبيعي، بما في ذلك التحليل أو التنبؤ من خلال العديد من البنود الخاصة بالأداء الوظيفي، والوضع الاقتصادي، والصحة، والتفضيلات الشخصية، والمصالح، والموثوقية، والسلوك، والموقع أو من خلال نشاط الفرد عبر مواقع التواصل الاجتماعي"[١٩].

ومن بين المراحل اللازمة لعملية معالجة البيانات ذات الطابع الشخصي تلك التي عرفها المشرع الأوروبي بعملية "التجهيز" "ويقصد بها عملية أو مجموعة العمليات التي يقوم بها القائم بالمعالجة على مجموعات من البيانات الشخصية، مثل الجمع والتسجيل والتنظيم، والهيكلة والتخزين والتكييف أو التعديل، والاسترجاع، والكشف عن طريق البث أو النشر أو أي شكل آخر من أشكال الإتاحة، أو المحو أو التدمير"[٢٠].

ويشير جانب من الفقه إلى أن "البيانات الشخصية هي تلك التي يستلزم موقع التواصل الاجتماعي من طالب التسجيل وضعها للتسجيل على الموقع"[٢١].

(١٨) على مستوى التشريع المصري، فإن البرلمان المصري يستعد لإصدار قانون ينظم حماية البيانات الشخصية عقب قيام لجنة الاتصالات وتكنولوجيا المعلومات بمجلس النواب بمناقشة مشروع القانون، والذي يهدف إلى ضمان وحماية كل ما يتعلق بمعالجة البيانات الشخصية للأفراد لاسيما خصوصية البيانات الشخصية والأسرية باعتبارها أحد أهم الحريات الشخصية والحقوق الأساسية للأشخاص الطبيعيين.
وتجدر الإشارة إلى أن وزارة الاتصالات كانت قد أرسلت مشروع قانون حماية البيانات الشخصية إلى مجلس الوزراء ووزارة العدل لمراجعته وإقراره قبل إرساله إلى مجلس النواب لمناقشته من أجل ضمان مستوى مناسب من الحماية القانونية والتقنية للبيانات الشخصية المعالجة إلكترونياً. للمزيد راجع الرابط التالي: https://goo.gl/1ZKKAw.
جاء في المذكرة الإيضاحية لمشروع قانون حماية البيانات الشخصية المصري "أن حماية البيانات ذات الطابع الشخصي أحد أهم الحقوق اللصيقة بالشخصية والمرتبطة بالحياة الخاصة للمواطنين، وتتطلب مزيداً من الاحتياطات والإجراءات الخاصة اللازم اتباعها أثناء تداولها بين أرجاء المجتمع، للحفاظ على خصوصية حياة المواطنين وعدم إفشائها وحظر استخدام البيانات الشخصية للمواطنين إلا بموافقة أصحابها ومن خلال إطار تشريعي ينظم عملية تداول البيانات ذات الطابع الشخصي وفي إطار الشفافية والأمانة واحترام كرامة الإنسان والممارسات المقبولة، تطبيقاً لأحد مبادئ حقوق الإنسان العامة والتي نص عليها الدستور المصري في الفقرة الأولى من نص المادة (٥٧)".

(19) «profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

(20) «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

(٢١) أشرف جابر سيد في بحثه القيّم: *الجوانب القانونية لمواقع التواصل الاجتماعي: مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتويتر*. مرجع سابق، ص ٤٧.

فعلى سبيل المثال عندما يقوم الشخص بإنشاء حساب على موقع التواصل الاجتماعي Twitter أو Facebook يطلب منه الموقع إدخال بعض البيانات اللازمة لإتمام عملية التسجيل وإنشاء الحساب الخاص به.

فيتعين عليه أن يضع بياناته الشخصية كالاسم الأول واسم العائلة وعنوان البريد الإلكتروني الخاص به وكلمة المرور وتاريخ الميلاد وجنسه، كما يمكنه أيضاً أن يضع البيانات التي تتعلق بمهنته وخبرته العملية وحالته الصحية، وأرقامه الشخصية، وعنوانه، وحالته الاجتماعية، وجنسيته، وآرائه ومعتقداته الشخصية ... إلخ[٢٢]. فمثل هذه البيانات تعد من قبيل المعلومات الشخصية التي عددتها المادة الرابعة من اللائحة الأوروبية الجديدة، وهو ما حاول المشرع المصري انتهاجه في مشروع قانون حماية البيانات الشخصية[٢٣].

(٢٢) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي. مرجع سابق، ص ٣٧٩ وما بعدها.

(٢٣) عرف مشروع القانون البيانات الشخصية بالبيانات ذات الطابع الشخصي أي معلومات عن الفرد التي تكون هويته محددة أو يمكن تحديدها بصورة معقولة سواء من خلال البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى بما في ذلك الصوت والصورة، كما عرف معالجة البيانات الشخصية بأنها كل عملية أو مجموعة عمليات تجري على البيانات الشخصية.

وترتكز فلسفة مشروع القانون المصري على مبادئ احترام حقوق الإنسان وضمان حماية خصوصية الحياة الخاصة، ويتكون مشروع القانون من ثمانية أبواب تشكل ثلاثة وستين مادة، يتضمن الباب الأول الأحكام العامة والتي تطرقت إلى الغرض من القانون ونطاق التطبيق والتعريفات للمصطلحات الواردة به، والثاني يتضمن حقوق الأفراد، والثالث يتناول البيانات الشخصية ذات الطبيعة الخاصة والتي حددها مشروع القانون وهي البيانات المتعلقة بالأصل العرقي، والإيديولوجيات السياسية، والأطفال، والصحة أو الحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقات الزوجية، والجرائم الجنائية وهي بيانات محمية بشكل خاص، حيث أولى مشروع القانون اهتماماً خاصاً للتعامل مع بيانات الطفل.

والباب الرابع يحدد الالتزامات المفروضة على المراقب والمعالج، ويتناول الباب الخامس طبيعة عمل جهاز حماية البيانات الشخصية المشكل طبقاً لتنفيذ أحكام مواد هذا القانون وصلاحياته وطريقة تشكيله وأسلوب عمله، ووضعيته القانونية، ويتناول الباب السادس تنظيم حركة البيانات الشخصية لخارج البلاد، ويتضمن الباب السابع الجرائم = المنصوص عليها والتي تخرق أحكام هذا القانون والعقوبات المفروضة عليها والتي تراوحت بين الغرامات المالية ما بين عشرين ألف جنيه مصري وبين خمسة ملايين جنيه مصري مع مراعاة خلو باقي التشريعات الأخرى المعمول بها من أي عقوبة أشد، كما يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من خمسين ألف جنيه مصري إلى مليون جنيه مصري أو بإحدى هاتين العقوبتين فقط، كل من نقل بيانات شخصية خارج البلاد على نحو يخالف لأحكام المادتين الرابعة والأربعين والخامسة والأربعين من هذا القانون، وفي حالة العودة وتكرار المخالفة تضاعف العقوبة.

كما يتناول الباب الثامن والأخير الأحكام الختامية والانتقالية وأعطى مشروع القانون المخاطبين بأحكامه سنة واحدة من تاريخ العمل به مهلة لتوفيق أوضاعهم بما يتفق وأحكامه، وفي حالة عدم توفيق الأوضاع في الفترة الزمنية المذكورة، يتعرض المخالف في هذه الحالة إلى العقوبات المنصوص عليها في هذا القانون.

وجاء في الباب الأول من مشروع القانون الأحكام العامة والتعريفات بأن الاتصالات السلكية واللاسلكية هي إرسال أو بث أو استقبال الإشارات أو الرموز أو الصور أو الأشكال أو الأصوات أو البيانات أو النصوص أو المعلومات، أياً كان نوعها أو طبيعتها، عن طريق الوسائل السلكية أو اللاسلكية أو الراديو أو البصرية، أو غيرها من وسائل الاتصالات الكهرومغناطيسية أو بأية وسائل اتصالات أخرى مشابهة.

كما أن الاتصال الإلكتروني يتم بواسطة الشخص الذي يشغل موقعاً على شبكة الإنترنت، أو يعرض منتجات أو خدمات من خلاله، ويقوم بجمع أو معالجة البيانات الشخصية لمستخدمي ذلك الموقع أو زواره.

وجاء في المادة الثالثة أن أحكام هذا القانون تسري على البيانات الشخصية المسجلة على وسائط الإعلام المادية أو التي يتم الحصول عليها أو جمعها أو استخراجها على أي نحو آخر تمهيداً لمعالجتها إلكترونياً، أو التي تتم معالجتها عن طريق الجمع بين المعالجة الإلكترونية والمعالجة التقليدية، مما يجعلها عرضة للمعالجة الإلكترونية وإلى أي شكل من أشكال الاستخدام اللاحق لهذه البيانات.

ويحكم هذا القانون جميع عمليات معالجة البيانات الشخصية داخل حدود مصر عندما يكون المسؤول غير مقيم داخل البلاد ولكن يلجأ لمعالجة بيانات ذات طابع شخصي بوسائل آلية أو غير آلية، باستثناء المعالجات التي لا تستعمل إلا لأغراض العبور فوق التراب الوطني أو في أراضي دولة لها تشريع في مجال حماية البيانات الشخصية.

ولا تسري أحكام هذا القانون على: البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون ويتم معالجتها في نطاق شخصي أو عائلي حصراً والبيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية، أو تطبيقاً لنص تشريعي مستقل والبيانات الشخصية المتعلقة بالتحقيقات القضائية، وقضايا =

أما عملية المعالجة في حد ذاتها فيقصد بها العمليات التي تهدف إلى جمع معلومات شخصية أو تسجيلها أو حفظها أو تنظيمها أو تغييرها أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو إتلافها أو الاطلاع عليها وكذلك العمليات المتعلقة باستغلال قواعد البيانات أو الفهارس أو السجلات أو غير ذلك من خلال الربط أو عقد المقارنات.

فعلى سبيل المثال نجد أن هناك بيانات تحتفظ بها جميع مواقع التواصل الاجتماعي بلا استثناء، فبمجرد قيام الشخص بإنشاء حساب على أحد هذه المواقع فإنه يُلزم بوضع بياناته الشخصية الخاصة به مثل الاسم واللقب وعنوان بريده الإلكتروني وغيرها، كما تحتفظ هذه المواقع بنوع ثانٍ من هذه البيانات وهي البيانات الخاصة بالاتصال بالإنترنت اللازم للاتصال بالموقع وهو ما يعرفه لدى علماء الحاسب الآلي بالهوية الإلكترونية أو (IP)، ثم يأتي دور البيانات الأكثر خطورة من وجهة نظرنا وهي بيانات التصفح الخاصة بالمواقع والصفحات والحسابات التي يتصفحها المستخدم، بالإضافة لكافة التطبيقات التي يشترك فيها صاحب الحساب على موقع التواصل الاجتماعي، والتي تكشف عن شخصيته واهتماماته وميوله وغير ذلك[٢٤].

ووفقاً للتعريف السابق فإن عملية المعالجة تنصب على مجموع العمليات المقصود منها التعرف على الشخص الطبيعي بصورة مباشرة أو غير مباشرة من خلال مجموعة من المعطيات أو الأمور المتعلقة بهويته أو بخصائصه الجسمية أو الفسيولوجية أو الجينية أو النفسية أو الاجتماعية أو الاقتصادية أو الثقافية.

وترتيباً على ما سبق فإن عملية معالجة البيانات الشخصية لابد لها من قائم بالمعالجة وهو ما يعرف بالمسؤول عن المعالجة، وقد عرفته اللائحة الأوروبية في الفقرة الثامنة المادة الرابعة بقولها:

> «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

فالمعالج وفقاً للنص السابق يعني الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي هيئة أخرى تقوم بعملية معالجة البيانات الشخصية، وتبعاً لذلك فالقائم بعملية المعالجة يحدد طريقة المعالجة التي يقوم عن طريقها بالوصول للغرض الذي من أجله تمت عملية المعالجة.

أما الشخص المعني بالأمر الذي تمت معالجة بياناته فهو كل شخص طبيعي تكون بياناته الشخصية موضوعاً للمعالجة من قبل المسؤول عن المعالجة.

وينصب اهتمام رأي في الفقه المصري[٢٥] وآخر في الفقه الفرنسي[٢٦] على عملية جمع البيانات الشخصية ويعتبر هذه العملية من أهم صور المعالجة، ويدلل على قوله بما ورد في نص المادة الثانية من قانون المعلوماتية والحريات الفرنسي والتي نصت على أنه "يحظر جمع أو معالجة البيانات ذات الطابع الشخصي والتي من شأنها أن تكشف بشكل مباشر أو غير مباشر عن الأصول العرقية أو الآراء السياسية أو الفلسفية أو العقيدة الدينية أو الانتماء النقابي لشخص أو تلك التي تتعلق بصحته أو بحياته ...".

= الإرهاب وكافة أشكال الجريمة المنظمة. ومع ذلك، فإنه يتعين على الجهة المسؤولة عن هذه التحقيقات أولاً إخطار: (جهاز حماية البيانات الشخصية) بطبيعة البيانات الموجودة بوحدتها والغرض من معالجتها وأهميتها لدعم هذه التحقيقات.

وجاء في الباب الثاني تحت عنوان (حقوق الأفراد): يحق لجهاز حماية البيانات الشخصية إصدار أي قرارات إدارية إضافية للحفاظ على خصوصية البيانات الشخصية المعالجة، وعلى المراقب أن يحترم أحكام البنود السابقة تحت مراقبة جهاز حماية البيانات الشخصية ويحظر جمع البيانات عن طريق الوسائل الاحتيالية أو غير العادلة أو غير المشروعة.

(٢٤) للمزيد حول هذا الأمر راجع علاء الدين الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية. *مجلة جامعة الشارقة للعلوم الشرعية والقانونية*، مج (٨)، ع (٢)، الإمارات العربية المتحدة، (٢٠١١م)، ص ٥ وما بعدها.

(٢٥) أشرف جابر سيد في بحثه القيّم: *الجوانب القانونية لمواقع التواصل الاجتماعي: مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتويتر*. مرجع سابق، ص ٤٨.

(26) Nathalie WALCZAK: La protection des données personnelles sur l'internet; Thèse de doctorat en Sciences ; Thèse de doctorat en Sciences de l'information et de la communication; univ-lyon2, 2014, p.119 et s.

ويستطرد هذا الرأي في عرض وجهة نظره أن الجمع المحظور والذي قصدته المادة هنا ليس الجمع المجرد للبيانات – لأن الجمع بذاته ليس محظوراً – وإنما المقصود هنا هو الجمع الذي يتم بطريق غير مشروع كالتدليس أو الذي يتم بالرغم من اعتراض صاحب هذه البيانات.

المبحث الثاني: المبادئ الحاكمة لمعالجة البيانات ذات الطابع الشخصي وفقاً لأحكام اللائحة الأوروبية

بادئ ذي بدء يجب أن نشير إلى أن عملية معالجة البيانات الشخصية لا تكون أمراً مشروعاً إلا إذا كان الشخص المعني قد وافق بوضوح وصراحة – بعد إبلاغه بدقة وبلغة بسيطة وواضحة – بأغراض عملية المعالجة.

ويمكن إيعاز قيام المشرع الأوروبي بالتشدد في اشتراط العديد من المبادئ الحاكمة لعملية معالجة البيانات الشخصية إلى تعدد صور الاعتداء على البيانات الشخصية سواءً كانت من قبل الجهات الحكومية أو من قبل الشركات أو الأفراد. وتزداد هذه الاعتداءات يوماً بعد يوم لتشكل خطراً لا يتزايد من الناحية الكمية فحسب وإنما أيضاً من الناحية التقنية؛ إذ في ظل هذا التطور تكمن صعوبة السيطرة على المخاطر المحتمل حدوثها جراء الاعتداء على تلك البيانات خصوصاً لمقدرة العالم الرقمي على تخزين هذا الكم الهائل من البيانات الشخصية لمستخدمي الإنترنت ومنصات التواصل الاجتماعي.

ومما يزيد الأمر تعقيداً هو ضعف معرفة المستخدمين لمجال الأمن المعلوماتي مما يجعلهم صيداً سهلاً للحصول على بياناتهم الشخصية خصوصاً في ظل تسارع غير محسوب العواقب من قبل المستخدمين على مواقع التواصل الاجتماعي[٢٧].

ومن المفيد هنا، أن نشير إلى مفهوم عملية المعالجة قبل أن نشرع في بيان القواعد التي اشترطها المشرع الأوروبي وتحديداً تلك الواردة في المواد الخامسة والسادسة والسابعة من اللائحة الأوروبية ويتم تطبيقها على جميع البيانات محل المعالجة[٢٨]. وهو ما يجعلنا نقسم هذا المبحث إلى مطلبين وفقاً للتالي:

- المطلب الأول: مفهوم عملية معالجة البيانات الشخصية.
- المطلب الثاني: قواعد معالجة البيانات الشخصية في ضوء نصوص اللائحة الأوروبية.

المطلب الأول: مفهوم عملية معالجة البيانات الشخصية

تناول المشرع الأوروبي في اللائحة الأوروبية الجديدة، تعريف عملية معالجة البيانات بأنها "عملية أو مجموعة العمليات التي تجري على البيانات الشخصية أو على مجموعات من البيانات الشخصية، بأية وسيلة تقليدية كانت أو إلكترونية، مثل الجمع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو التكييف أو التعديل أو الاسترجاع، أو التشاور أو الاستخدام أو الإفصاح عن المعلومات عن طريق الإرسال أو النشر أو الإتاحة أو المواءمة أو الجمع أو التقييد أو المحو أو التدمير". وهذا ما نصت عليه الفقرة الثانية من المادة الرابعة من اللائحة المشار إليه[٢٩].

(٢٧) في وقتنا الحاضر أصبحت كل مجالات الحياة اليوم محاصرة بالتطور التقني الهائل وما يقدمه لها من خدمات ومميزات، وعلى الرغم من هذه المزايا المتنوعة والمتعددة والفريدة إلا أنه يوجد لها العديد من السلبيات والتهديدات التي ترقى إلى أن تكون مخاطر منها الاعتداء على الحق في الخصوصية وما يتفرع منه، خصوصاً أن التقنية الحديثة قد تظهر للمستخدم بصورة أو بشكل لا يعكس ما تخفيه من تقنية دقيقة من خلال يمكن التعرض للبيانات الشخصية.

(28) Principes relatifs au traitement des données à caractère personnel.

(٢٩) هذا التعريف يشبه إلى حد كبير التعريف الذي أورده المشرع الفرنسي في نص الفقرة الثانية من المادة الثالثة من قانون المعلوماتية والحريات الفرنسي رقم ٧٨ لسنة ١٩٧٨م والمعدل بأحكام القانون الصادر في ٣٠ يناير ٢٠٠٢م والتي أشارت إلى ذات المعنى تقريباً.

Loi n° 78-17 du 6 janvier 1978, modifiée 22 juin 2018, relative à l'informatique, aux fichiers et aux libertés Pour voir tous les Articles modifiés, voir: https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee.

ولكن تجدر الإشارة في هذا المقام أن فرنسا لم يكن لها السبق في وضع تعريف للبيانات الشخصية أو حتى عملية المعالجة بل سبقتها في ذلك العديد من التشريعات الأوروبية التي نقلت التعريف الوارد بالتوجيه الصادر عن البرلمان الأوروبي عام ١٩٩٥م بشأن حماية الأشخاص الطبيعيين في مجال حماية البيانات ذات الطابع الشخصي وحرية تداولها، ونذكُر من بين هذه التشريعات على سبيل المثال لا الحصر، قانون البيانات الشخصية السويدي رقم (٢٠٤) لسنة ١٩٩٨م الصادر في ٢٤ أكتوبر سنة ١٩٩٨م، وكذلك قانون =

وبناءً على التعريف السابق فإن المعالجة إما أن تكون تقليدية أو إلكترونية فالمعالجة اليدوية تتم عبر طرق تقليدية عن طريق جمع البيانات ذات الطابع الشخصي في ملفات ورقية ويتم الاحتفاظ بها لدى الشخص أو الجهة القائمة بعملية المعالجة ثم القيام بتصنيفها والتوفيق بينها للوصول لنتائج محددة يتم الاستفادة منها في عمليات الدعاية والتسويق المختلفة كأصل عام.

أما المعالجة الإلكترونية فإنها يتم فيها جمع البيانات الشخصية والمعلومات على الحواسيب والأجهزة الإلكترونية وبرامج المعالجة الإلكترونية التي ذاع انتشارها في الآونة الأخيرة، وتتسم عملية المعالجة هذه بالسرعة في التصنيف والتوفيق بين البيانات المختلفة سعياً لاستخلاص النتائج المرجوة[٣٠].

ومن الواجب هنا أن نشير إلى وجود شركات متخصصة في معالجة البيانات تقوم بجمع البيانات الشخصية وتقسيمها وفق تقسيمات محددة إما جغرافية أو عمرية أو مذهبية أو غيرها، وتستخدم هذه المعالجة في استهداف أصحابها مباشرةً من خلال الإعلانات الدعائية للمنتجات أو السلع، أو في النواحي السياسية؛ حيث يتم استخدامها لتمرير بعض الأفكار أو رسائل سياسية معينة أو أجندة ما لموضوع سياسي من خلال رسائل مباشرة أو دعائية عن طريق شبكات أو منصات التواصل الاجتماعي أو تطبيقات الهواتف الذكية[٣١].

وفي سياق مرتبط، تأتي المعلومات والبيانات الشخصية المتاحة على مواقع ومنصات التواصل الاجتماعي كواحدة من البيانات الأساسية التي يسعى علماء الاجتماع والباحثين الاجتماعيين إلى الوصول إليها والوقوف على أسباب ودوافع إتاحتها وعرضها بل ودراسة المشكلات الشخصية التي تتيحها تلك المعلومات في البيئة الرقمية، بل الأكثر من ذلك هو قيام بعض الباحثين بإجراء العديد من الدراسات والبحوث حول كيفية الاستفادة من المعلومات والبيانات الشخصية المتاحة على الويب[٣٢].

= حماية البيانات الشخصية الإسباني الصادر في ١٣ من ديسمبر ١٩٩٩م، فضلاً عن قانون لوكسمبورج الصادر في الثاني من أغسطس سنة ٢٠٠٢م بشأن حماية الأشخاص الطبيعيين عند معالجة البيانات ذات الطابع الشخصي. للمزيد حول هذه التشريعات انظر: محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. القاهرة: دار النهضة العربية، (٢٠١٦م)، ص ٣٨ وما بعدها.

(٣٠) يضرب جانب من الفقه المصري مثالاً على عملية المعالجة عبر مواقع التواصل الاجتماعي بافتراض أن من بين المستخدمين للموقع الإلكتروني رجلاً متوسط العمر تُظهر بياناته الشخصية عضويته بأحد الأندية الرياضية، وممارسته على سبيل الهواية لنشاط رياضي معين، مع حرصه على إبراز لقطات تجمعه مع عدد من مشاهير الرياضة على صفحته الخاصة على الموقع، فمن الممكن بمعالجة هذه البيانات الوصول إلى اهتمام هذا المستخدم بالمنتجات الرياضية، وفي الوقت ذاته تساعد بياناته الشخصية التي سبق أن دونها عند تسجيله للانضمام إلى موقع التواصل على مخاطبته من جانب المعلنين برسائل نصية – سواء عبر بريده الإلكتروني أو رقم هاتفه الجوال – بشأن عروض الشراء على الملابس والأحذية والحقائب الرياضية وبذلك تكون معالجة البيانات الشخصية قد أثمرت في مجال الدعاية والتجارة. للمزيد راجع في هذا الخصوص: محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومظاهر انتهاك الحق في الخصوصية*. مرجع سابق الإشارة إليه، ص ٤٤، وانظر كذلك: سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي. مرجع سابق الإشارة إليه، ص ٤١٠.

(٣١) تتنافس شركات الهواتف الذكية اليوم فيما بينها بإصدار أجهزة تحمل مواصفات تقنية حديثة وعالية مقابل أسعار تنافسية، فأصبحت تقيم كل سنة مؤتمرات لها تعرض فيها أحدث ما توصلت إليه من تقنيات وبرمجيات لتواكب بذلك التقدم السريع في عالم التقنية، فنشاهد مثلاً شركة "آبل" تقيم سنوياً مؤتمر آبل العالمي للمطورين بالإنجليزية: The Apple Worldwide Developers Conference اختصاراً (WWDC)، وهو المؤتمر الذي يقام سنوياً منذ عام ١٩٨٥م في ولاية كاليفورنيا من قبل شركة آبل؛ حيث تستخدمه في المقام الأول لعرض برامجها والتكنولوجيات الجديدة للمطورين، فضلاً عن توفير التدريب العملي على المعامل وجلسات مع مطوري آبل. للمزيد انظر الرابط التالي: https://www.apple.com/sitemap/.

(٣٢) من بين هذه الدراسات التي وجدناها أثناء كتابة هذه الدراسة بحث لريهام عاصم غنيم، المعلومات الشخصية المتاحة على الويب العام: دراسة في إمكانية الوصول وأخلاقيات الاستخدام. بحث منشور ضمن بحوث مؤتمر المحتوى العربي في الإنترنت (التحديات الطموح)، مج (٢)، (٢٠١٠م)، جامعة الإمام محمد بن سعود الإسلامية، الرياض، ص ص ١١٣٩-١١٧٣، ص ١١٤٤ وما بعدها.

في الآونة الأخيرة ظهرت العديد من البرامج والتطبيقات المطورة التي تعمل على جمع وتحليل البيانات الشخصية عقب اتخاذ بعض الأشخاص الحيط والحذر من خلال تفعيل سياسات الخصوصية، وقامت الكثير من شركات جمع المعلومات بتصميم تطبيقات يتم وضعها على الهواتف الذكية تسهل من عملية التواصل لكنها تشترط على المستخدم لكي يستفيد من الخدمة المجانية التي يقدمها التطبيق أن يسمح للتطبيق بالوصول لكافة أنماط الكائنات الرقمية المخزنة على هاتفه أو تلك المخزنة على السحابة الخاصة به، بل إن بعض التطبيقات الذكية تمنح نفسها الحق في تداول البيانات مع آخرين دون الرجوع لصاحبها مؤسسةً ذلك على موافقته على سياسات وشروط استخدام التطبيقات، وهنا لا تكون الخدمة مجانية بل يكون المستخدم وبياناته – بل وكافة المعلومات الموجودة على الجهاز الخاص به – هو الثمن الفعلي للحصول على الخدمة.

المطلب الثاني: قواعد معالجة البيانات الشخصية في ضوء نصوص[٣٣] اللائحة الأوروبية

لا يمكن إجراء أي عملية من عمليات المعالجة أو جمع البيانات أو حتى السماح بتخزينها إلا إذا وافق الشخص المعني على ذلك بعد أن يكون قد تم إبلاغه بلغة بسيطة وواضحة ومفهومة. ما لم تكن المعالجة ضرورية كالمعالجة التي تتم من أجل المصالح الحيوية والضرورية مثل غايات الطب الوقائي أو تنفيذ مسألة متعلقة بالصالح العام، وذلك دون أي إخلال بهذه البيانات أو تحويرها أو الإفصاح عنها بدون إذن أو حتى السماح لأي طرف بالوصول إليها.

والموافقة التي نعنيها في هذا المقام هي التي نصت عليها المادة السابعة من اللائحة الأوروبية ٦٧٩/ ٢٠١٦م[٣٤] وعبرت عنها بـ"أية إشارة حرة ومحددة ومستنيرة لا لبس فيها تفيد رغبة الشخص المعني – مع وجود إجراء إيجابي واضح – في الموافقة على معالجة البيانات الشخصية المتعلقة به ...".

وقد حظيت عملية المعالجة باهتمام كبير من المشرع الأوروبي في هذه اللائحة. فقد أورد في المادة الخامسة من هذه اللائحة العديد من القواعد الخاصة بعملية المعالجة نقوم بتفصيلها في فروع خمسة على النحو التالي:

- الفرع الأول: معالجة قانونية وعادلة وشفافة (العدالة والشفافية).
- الفرع الثاني: أن يكون جمع المعلومات لأغراض محددة وواضحة ومشروعة (المشروعية).
- الفرع الثالث: أن تكون عملية المعالجة ملائمة ومناسبة ومقصورة على ما هو ضروري فيما يخص الأغراض التي جُمعت من أجلها (تقليل البيانات).
- الفرع الرابع: أن تقتصر مدة تخزين وأرشفة البيانات على الوقت اللازم لأغراض المعالجة (الحد من التخزين والأرشفة).
- الفرع الخامس: أن تتم المعالجة بشكل يضمن أمن وسلامة البيانات (السرية والنزاهة).

الفرع الأول: معالجة قانونية وعادلة وشفافة (العدالة والشفافية)[٣٥]

حرص المشرع الأوروبي على تحقيق المشروعية والإنصاف والشفافية في معالجة البيانات سواءً تمت هذه

(33) Règlement (UE) 2016/679, Art. 5 ; Art 6 ; Art 7.

(34) Règlement (UE) 2016/679, Art. 7 "Conditions applicables au consentement":

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et = simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.
4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

(35) Règlement (UE) 2016/679, Art.5, "traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

المعالجة بوسيلة تقليدية أو إلكترونية - باعتبار أنه لا تتم عملية جمع البيانات من خلال شخص طبيعي أو اعتباري إلا بعد موافقة الشخص المعني وتعبيره الصريح عن رضاه عن تلك المعالجة - كأصل عام - وباستثناء تلك الحالات التي أشرنا إليها سابقاً.

تبعاً لما تقدم، وإعمالاً لهذا الشرط المنصوص عليه في عجز المادة الخامسة من اللائحة الأوروبية، لا يجوز استعمال طرق احتيالية في جمع المعلومات عن طريق القيام بتضليل الشخص المعني فيقوم بإعطاء معلوماته بناءً على استعمال هذه الوسائل الاحتيالية من قبل الغير.

وبمفهوم المخالفة، فإن أي تجميع واستخدام للبيانات بدون علم صاحبها أمر غير مشروع يوجب مساءلة الجهة القائمة بالعملية وتتحقق به مسؤوليتها. ولهذا اعتبرت اللجنة الوطنية للمعلوماتية والحرية (CNIL) أن القيام بعملية جمع بيانات مستخدمي الإنترنت لغايات إعلانية دون علمهم وموافقتهم على ذلك هو من باب الفعل غير المشروع الذي يوجب مساءلة فاعله[٣٦].

كما يجب أن تكون هناك شفافية كاملة بشأن البيانات الشخصية المراد الحصول عليها من الشخص المعني، بحيث يتم إطلاعه على نوعية البيانات والغرض المراد من عملية المعالجة، والمدة، وما هو مصير هذه البيانات بعد ذلك، ومن هم الفئات الذين يحق لهم الاطلاع عليها.

الفرع الثاني: أن يكون جمع المعلومات لأغراض محددة وواضحة ومشروعة (المشروعية)

هذا الشرط في غاية الأهمية؛ لأنه ينصب على مضمون عملية المعالجة في حد ذاتها فإذا كان الشرط الأول قد تطرق لشرعية الإجراء فإن هذا الشرط يعالج المضمون.

ووفقاً لذلك، يجب أن تتم عملية المعالجة لغايات محددة وواضحة ومشروعة بحيث يتم التأكد من أنه لم تتم معالجتها بطريقة لا تتماشى مع الأغراض المحددة.

وبطبيعة الحال، لا يمكن اعتبار عمليات المعالجة الإضافية التي تتم لأهداف عامة أو لأغراض البحث العلمي أو لتوثيق أحداث تاريخية أو لأغراض إحصائية متعارضةً مع الأغراض الأولية؛ فالعبرة هنا في هذا المقام بتحديد الهدف أو الغرض الذي من أجله تتم عملية المعالجة؛ لأن هذا يعني تحقيق الشفافية في شتى مراحل عملية المعالجة، فإذا كان الغرض غير محدد، فلا يمكن تصور إتمام عملية المعالجة أو حتى البدء في جمع البيانات فالغموض الذي يشوب عملية جمع البيانات قد يحمل من الخطورة ما يؤثر على خصوصية الفرد، ويهدر حقاً أصيلاً له كفله الدستور والقوانين.

وقد خصص المشرع الأوروبي مادة كاملة لهذا المبدأ المهم، وهي المادة السادسة والتي تنص على أنه "لا تكون المعالجة مشروعة إلا إذا انطبقت الإجراءات التالية:

(أ) أن يكون الشخص المعني قد أعطى الموافقة على معالجة بياناته الشخصية لغرض واحد أو أكثر من الأغراض المحددة.

(ب) أن تكون المعالجة ضرورية لتنفيذ العقد الذي يكون الشخص المعني طرفاً فيه أو من أجل اتخاذ إجراء بناء على موافقة الشخص المعني قبل إبرام العقد.

(ج) أن تكون المعالجة ضرورية من أجل حماية مصالح ضرورية لصاحب البيانات أو لشخص طبيعي آخر.

(د) أن تكون المعالجة ضرورية لأداء مهمة يضطلع بها للصالح العام.

(هـ) أن تكون المعالجة ضرورية من أجل تحقيق أغراض أو مصالح مشروعة."

---

(٣٦) تلعب CNIL دوراً مهماً في حماية حقوق المواطنين على المستوى الأوروبي، فيمكن لأي فرد الاتصال بهم عندما يواجه صعوبات في ممارسة حقوق حماية البيانات الشخصية الخاصة به. وتكفل CNIL تمكين الجميع من الوصول بفعالية إلى بياناتهم محل المعالجة. وفي العام ٢٠١٣م، تلقت CNIL ٥٦٤٠ شكوى تشمل ما يلي: السمعة الإلكترونية (طلب محو البيانات على الإنترنت)، والتجارة (طلبات لوقف الدعاية عن طريق البريد)، والمصارف والقروض (الاعتراض على تسجيلها في ملفات بنك فرنسا) بالإضافة إلى إمكانية تقديم الشكاوى عبر الإنترنت لمعالجة بعض المسائل مثل: (محو البيانات الشخصية على الإنترنت، والاعتراض على تلقي الدعاية عن طريق البريد، وتحديث دقة هذه البيانات). للمزيد حول دور الهيئة فضلاً راجع الرابط التالي: https://www.cnil.fr/en/cnils-missions.

بالإضافة لما سبق، فقد أوردت المادة سالفة الذكر وكذلك المادة الخامسة من اللائحة العديد من الشروط العامة التي تحكم مشروعية المعالجة والتي نخص بالذكر منها نوع البيانات التي تخضع للمعالجة ومضمونها، والجهات التي يمكن الإفصاح لها عن البيانات الشخصية، إضافة إلى تحديد الغرض من معالجة هذه البيانات، وتحديد فترات الاحتفاظ بالبيانات، وإجراءات المعالجة والتدابير اللازمة لضمان المعالجة القانونية والعادلة مثل تلك التي تتعلق بالحالات المنصوص عليه في المادة التاسعة والثمانون من اللائحة الجديدة[٣٧].

وكذلك الحال بالنسبة لما نصت عليه المادة التاسعة من معالجة الفئات الخاصة من البيانات الشخصية، والتي تثير في الغالب العديد من الإشكالات القانونية التي سنتعرض لها لاحقاً[٣٨].

(37) Règlement (UE) 2016/679, Art. 89. Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

1. Le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au présent règlement, à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière.
2. Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, le droit de l'Union ou le droit d'un État membre peut prévoir des dérogations aux droits visés aux articles 15, 16, 18 et 21, sous réserve des conditions et des garanties visées au paragraphe 1 du présent article, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités.
3. Lorsque des données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, le droit de l'Union ou le droit d'un État membre peut prévoir des dérogations aux droits visés aux articles 15, 16, 18, 19, 20 et 21, sous réserve des conditions et des garanties visées au paragraphe 1 du présent article, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités.
4. Lorsqu'un traitement visé aux paragraphes 2 et 3 sert dans le même temps une autre finalité, les dérogations sont applicables au seul traitement effectué aux fins visées auxdits paragraphes.

(٣٨) راجع المبحث الثاني من الفصل الثاني من هذه الدراسة والذي سوف نعرض فيه للعديد من الإشكالات القانونية المتعلقة بمعالجة بعض الفئات الخاصة من البيانات الشخصية والتي أثارتها المادة التاسعة من هذه اللائحة والتي جاء نصها على النحو التالي:

Règlement (UE) 2016/679, Art.9: Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.
2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie:

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;
b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée;
c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;
d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées;
e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée;
f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle;

وفي الحالات التي لا تستند فيها عملية المعالجة إلى موافقة الشخص المعني على معالجة البيانات أو إلى قانون الاتحاد أو الدولة العضو باعتبار أن ذلك يشكل تدبيراً ضرورياً ومتناسباً لحماية الأهداف المشار إليها في المادة الثالثة والعشرين من اللائحة، فإنه يتعين على القائم بالمعالجة أن يأخذ في الاعتبار جملة أمور أهمها ما يلي:

١- العلاقة بين جمع البيانات الشخصية وأغراض المعالجة المزمع القيام بها.
٢- السياق الذي جُمعت فيه البيانات الشخصية.
٣- طبيعة البيانات الشخصية، لاسيما إذا كانت الفئات الخاصة من البيانات الشخصية عملاً بالمادة التاسعة من اللائحة.
٤- النتائج المحتملة للمعالجة الإضافية للبيانات.
٥- وجود الضمانات المناسبة التي تشمل سرية وأمن البيانات[٣٩].

الفرع الثالث: أن تكون عملية المعالجة ملائمة ومناسبة ومقصورة على ما هو ضروري فيما يخص الأغراض التي جُمعت من أجلها (تقليل البيانات)

يعرف هذا الشرط بشرط "تقليل البيانات"، ويتسق هذا الشرط ويتكامل مع الشرط السابق، ويتضح هذا الاتساق من خلال مؤدى هذا الشرط وهو أن يكون هناك تناسب بين كمية البيانات التي تم جمعها لإجراء عملية المعالجة عليها والغرض أو الهدف المحدد سلفاً منعاً من تخزين البيانات بلا هدف وحتى لا يساء استخدامها في ظل تزايد انتهاك خصوصية الأفراد عند معالجة ونقل البيانات الشخصية. لذلك يجب ألا يتعدى الجمع والتخزين الغرض المخصص له، كما يجب على القائم بعملية المعالجة تقليل البيانات قدر الاستطاعة، بالشكل الذي يفي بالغرض. مع الوضع في الاعتبار أن هذه المسألة موضوعية يختص بها قاضي الموضوع؛ فهو وحده الذي يقرر ما إذا كانت البيانات التي تم تجميعها وتخزينها كافية للوفاء بالغرض أم أن هناك بيانات قام المعالج بجمعها ولا حاجة لعملية المعالجة لمثل هذه البيانات.

وعطفاً على المنحى السابق، وسعياً من دول لاتحاد الأوروبي إلى مراقبة هذا الأمر بشكل مسبق فقد اشتمل كل تشريع من التشريعات التي صدرت في هذا الخصوص على

(39) Règlement (UE) 2016/679, Art.5, f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;
h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;
i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel;
j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé.

إنشاء هيئة رقابية الهدف منها حماية حقوق وحريات الأفراد عند معالجة بياناتهم الشخصية بحيث يناط بها تلقي طلبات معالجة البيانات ومنح التراخيص في هذا المجال، وهي في سبيل ذلك تتثبت من الشروط المطلوبة قانوناً عند معالجة البيانات الشخصية.

وحتى يتحقق هذا الشرط أيضاً يجب أن تكون البيانات دقيقة، وإذا لزم الأمر يجب اتخاذ خطوات معقولة لضمان أن البيانات الشخصية غير الدقيقة قد تم محوها أو أنه قد تم تصحيحها دون إبطاء وهو ما عبر عنه المشرع الأوروبي بشرط (الدقة)[٤٠].

الفرع الرابع: أن تقتصر مدة تخزين البيانات على الوقت اللازم لأغراض المعالجة (الحد من التخزين)

يجب أن يتم الاحتفاظ بالبيانات التي يتم الاحتياج إليها فقط في شكل يسمح بتحديد الضروري منها للقيام بعملية المعالجة، واستثناءً من ذلك يمكن تخزين البيانات الشخصية لفترات أطول بالقدر اللازم للقيام بمعالجتها من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية وفقاً للمادة ٨٩/ ١ من اللائحة، وذلك شريطة أن يتم اتخاذ التدابير التقنية والتنظيمية المناسبة التي تقتضيها هذه اللائحة من أجل ضمان حقوق وحريات الشخص المعني؛ حيث يلتزم المعالج بضمان عدم تعرض البيانات لأي اعتداء خارجي وتوفير كافة السبل اللازمة لضمان حقوق أصحابها حال وقوعه. كما يجب أن يتم حفظ البيانات للمدة اللازمة للغرض الذي جُمعت من أجله، وذلك لعدم جعل عملية تخزين البيانات أبدية، وهو ما يستوجب من القائم بعملية المعالجة أن يقوم بتحديد وقت كل عملية؛ لكي يتم محو البيانات عقب انتهاء الغاية من استخدامها، وهو ما عبر عنه المشرع الأوروبي بشرط (قصرة مدة التخزين على الوقت اللازم لأغراض المعالجة).

الفرع الخامس: أن تتم المعالجة بشكل يضمن أمن وسلامة البيانات (السرية والأمن)

يجب أن تتم عملية معالجة البيانات ذات الطابع الشخصي بطريقة تكفل السرية والأمن المناسب لهذه البيانات، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير المشروعة ومن الخسارة أو التدمير أو الضرر العارض عن طريق استخدام التدابير التقنية أو التنظيمية المناسبة وهو ما عبر عنه المشرع الأوروبي بشرط (السرية والأمن)[٤١].

وتطبيقاً لهذا الشرط لا يجوز الاطلاع على البيانات الشخصية دون علم صاحبها، وإبداء موافقته على ذلك، ومن باب أولى يجب ألا يتم نقل هذه البيانات للغير إلا بموافقة صاحبها أيضاً. فالخطر هنا – حسب ما أوردته المادة – يتمثل في أمور عدة من بينها اطلاع الغير على البيانات بدون إذن صاحبها الأمر الذي يشكل تعدياً وانتهاكاً لحقوقه نتيجة إفشاء هذه المعلومات وتداولها بدون موافقة صاحبها أو حتى علمه بذلك. كما يمكن أن يتمثل هذا الخطر في فقد هذه البيانات أو تدميرها أو سرقتها نتيجة تفشي ظاهرة القرصنة المعلوماتية[٤٢]، أو تداولها بشكل غير قانوني مقابل قيمة مالية يجنيها من ورائها القائم بالمعالجة.

ويتبادر إلى الذهن في هذا المقام سؤال حول الآلية التي تتم بها عملية المعالجة وما هي المخاطر التي يمكن أن تحدث للشخص المعني؟

للإجابة على ذلك يمكن القول بأن عملية المعالجة تمر بمرحلتين رئيسيتين وفي كل مرحلة نواجه مخاطر متنوعة قد تمس الحياة الخاصة للأفراد بصورتها المستحدثة والمتمثلة في بنوك المعلومات والتي غدت مهددة بالعديد من الانتهاكات والاعتداءات لاسيما مع ظهور برامج وتطبيقات[٤٣] تقوم بتجميع البيانات بصورة سريعة وهو ما يعرف لدى الفقه بنظم

(40) Règlement (UE) 2016/679, Art.5; d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

(41) Règlement (UE) 2016/679, Art. 5; a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence;

(٤٢) محمد زايد، الجريمة والقرصنة في مجال المعلوماتية والشبكات. بحث منشور في *المجلة العربية العلمية*، تونس، مج (١٠)، ع (١٩)، (٢٠٠٦م)، ص ص ٧٣-٨٤، ص ٧٤ وما بعدها.

(٤٣) برامج وتطبيقات المكالمات الهاتفية عبر الإنترنت مثل imo، و JusTalk، و Real Caller وغيرها من التطبيقات المتعارف عليها.

المعالجة الآلية للمعطيات والبيانات الشخصية الأمر الذي ازدادت معه الرغبة الملحة في معالجة القصور والفراغ التشريعي لحماية ما يتم تداوله من معلومات وبيانات عبر هذه النظم، وهاتان المرحلتان هما:

الأولى: مرحلة جمع وتخزين البيانات ذات الطابع الشخصي، حيث يتم عمل تجميع للبيانات الشخصية لفئة معينة من الأشخاص المستهدف تجميع بياناتهم عن طريق القائم بالمعالجة أو أي شخص آخر وتعرف هذه البيانات كما يسميها جانب من الفقه[٤٤] بالبيانات الاسمية والتي تشمل بيانات الحالة الصحية والمالية والمهنية والعائلية وغيرها، وبمجرد القيام بتجميع وتخزين هذه البيانات وإجراء المعالجة لها فإنه يمكن التعرف على الشخص والوصول إليه.

وقد يتم جمع المعلومات عن الأشخاص المعنيين بمعالجة بياناتهم عن طريق إجبارهم على الإدلاء بها وحفظها في مكان واحد مما يكون له أثر كبير على إلحاق الضرر بهؤلاء الأفراد؛ حيث إن جمع البيانات الشخصية عنهم وتفصيلات أوضاعهم المادية والعائلية أو غيرها وحفظها على شبكة الإنترنت يسهل الوصول إليها بشكل مشروع أو غير مشروع مما قد يُعرضهم لأضرار بالغة[٤٥].

وعدم المشروعية لعملية الجمع أو التخزين هنا لبيانات شخصية صحيحة قد يكون مصدره أساليب الحصول على البيانات أو مضمون هذه البيانات؛ ذلك أن انتهاك الخصوصية للحصول على بيانات ذات طبيعة شخصية يمكن أن يتحقق بأساليب مختلفة، كالتوصل بطريق غير مشروع إلى ملفات بيانات تخص الآخرين، أو عن طريق مراقبة واعتراض تفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني، أو عن طريق القرصنة الرقمية أو المعلوماتية للحاسوب الذي يحوي هذه البيانات على قرص الذاكرة الخاص به.

ثم تعقب عملية الجمع قيام المُعالج بإجراء عملية تصنيف وتخزين للبيانات من خلال استخدام برامج آلية أو بشكل يدوي حتى يسهل عليه استخدام هذه البيانات أو تجهيزها لاستغلالها من قبل آخرين من خلال انتقالها دون علم صاحبها وهو ما قد يشكل جملة من المخاطر التي تتعلق بالمرحلة التالية وهي مرحلة التعامل على البيانات واستخدامها.

الثانية: مرحلة التعامل على البيانات وهذه المرحلة تتم من خلال عدة صور - كما ذكرنا في المرحلة الأولى من آلية المعالجة - استخدام بيانات شخصية صحيحة لكن من خلال الحصول عليها عن طريق القرصنة المعلوماتية بكافة صورها المعروفة حالياً وأيضاً استخدام بيانات شخصية غير صحيحة إما عن طريق التلاعب في البيانات الشخصية أو محوها من قبل أشخاص غير مرخص لهم قانوناً بذلك، أو عن طريق معالجة أو نشر بيانات غير صحيحة من قبل الأشخاص المرخص لهم بذلك قانوناً الأمر الذي يترك غالباً آثاراً سلبية وسيئة على حياة الفرد وسيرته بسبب انتهاك حقه في الخصوصية[٤٦].

ويُعد من قبيل التعامل على البيانات الشخصية الإفشاء غير المشروع لهذه البيانات وإساءة استخدامها، وهذا الإفشاء الذي يمكن أن يلحق الضرر بالفرد، ذلك أن المعلومات التي تجمع عن فرد من الأفراد لغرض معين ومحدد ابتداءً يمكن أن يساء استعمالها لصالح جهات أخرى وهو ما حظره التشريع الأوروبي كأصل عام.

ومن جانبنا نؤكد على أمر في غاية الأهمية وهو أن مشروعات قوانين حماية البيانات الشخصية التي طالعناها

---

(٤٤) شريف يوسف حلمي خاطر، حماية الحق في الخصوصية المعلوماتية: دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا. *مجلة البحوث القانونية والاقتصادية*، كلية الحقوق، جامعة المنصورة، مصر، ع (٥٧)، (أبريل ٢٠١٥م)، ص ص ١-١٧٠، ص ٣٩ وما بعدها.

(٤٥) نفس الإشارة السابقة.

(٤٦) هشام محمد فريد رستم، *الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة*. أسيوط: مكتبة الآلات الحديثة، (١٩٩٢م)، ص ١٩٠ وما بعدها. وانظر كذلك: شمس الدين إبراهيم أحمد، *وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانونين السوداني والمصري: دراسة مقارنة*. القاهرة: دار النهضة العربية، ط١، (٢٠٠٥م)، ص ١١٦ وما بعدها. وانظر: محمد المقاطع، *حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي*. مطبوعات جامعة الكويت، (١٩٩٢م). انظر أيضاً: محمود أحمد عبابنة، *جرائم الحاسوب وأبعادها الدولية*. عمان: دار الثقافة للنشر والتوزيع، ط١، (٢٠٠٥م)، ص ٧٢ وما بعدها.

اهتمت بالمعايير الأوروبية ولم يكتف أغلبها في حمايته التشريعية للخصوصية بتجريم المساس الموضوعي بها، وإنما وضع كذلك قواعد تنظم ممارسة عمليات الجمع والتخزين ونشر البيانات ومعالجتها وتبادلها ومحوها وكافة أشكال وصور التعامل مع البيانات ذات الطبيعة الشخصية، بحيث أصبحت مخالفة معظم هذه القواعد تصبح مكوناً لجريمة معاقب عليها قانوناً[٤٧].

إذن من الواضح أن عملية معالجة البيانات الشخصية عن طريق نظم المعالجة الآلية أو بالطرق التقليدية تحمل مخاطر كبيرة، وهذا ما استدعى المشرع الأوروبي لوضع قواعد حماية خاصة في ظل عكس القواعد الحالية عن توفير حماية فعالة للبيانات ذات الطبيعة الشخصية خاصة في عصر قرصنة المعلومات والتطور الهائل الذي شهدته السنوات الأخيرة في نظم الجمع والمعالجة والاختراق المعلوماتي.

الفصل الثاني:
الإطار القانوني لحقوق والتزامات القائم بالمعالجة والشخص المعني في ضوء أحكام اللائحة الأوروبية ٦٧٩/ ٢٠١٦م

تمهيد وتقسيم

في الثاني من فبراير ٢٠٠٥م أكدت محكمة Pontoise الابتدائية على أن "حرية الاتصال وتبادل المعلومات عبر الإنترنت لا ينبغي أن يجعل منها بيئة متحررة من القواعد القانونية"[٤٨] فالإنترنت ليس فضاء بلا قانون[٤٩].

إن كافة أشكال التعامل غير المشروع مع البيانات الشخصية متنوعة وكثيرة وفي ازدياد دائم بفعل هذا التطور المتسارع[٥٠]، لذا كان لزاماً أن يكون هناك تطوراً تشريعياً موازياً لمواجهة كافة الانتهاكات كسرقة البيانات أو تحويلها إلكترونياً من خلال معالج من الباطن بشكل غير مشروع أو الاعتداء عليها تحت ما يوصف بالقرصنة المعلوماتية وهي قرصنة تتم في البيئة الإلكترونية، وهو أمر يمثل انتهاكاً صارخاً للأخلاق الحميدة ولحياة الأفراد الخاصة.

وانطلاقاً من ذلك وترتيباً عليه، يجب أن نتطرق لتحديد الإطار القانوني لحقوق والتزامات القائم بالمعالجة والشخص المعني الذي تمت معالجة بياناته في ضوء المخاطر التي تحيط بنا نتيجة استغلال البيانات الشخصية من خلال عمليات المعالجة غير المشروعة، الأمر الذي حدا بالمشرع الأوروبي إلى إصدار توجيهين في نفس الإطار.

من هنا كان يجب أن نسلط الضوء على الإطار القانوني لهذه المعالجة وكيف تعامل معها المشرع الأوروبي في ظل التطورات المتسارعة لبرامج وتطبيقات معالجة البيانات، وسعي العديد من الجهات والأفراد إلى الحصول على هذه البيانات واستغلالها على نحو قد يضر بالأشخاص المعنيين ضرراً بالغاً يتعذر تدارك آثاره السلبية في كثير من الأحيان في الوقت الذي بدأ يتركز اهتمامهم على مستوى الالتزام بخصوصيتهم، ومتابعة كيف تم استغلال البيانات والمعلومات التي جُمعت منهم، وهل يجري تمرير هذه البيانات والمعلومات إلى منظمات أخرى بمعرفة المرخص له بعملية المعالجة، وما هو مصير هذه البيانات، وهل يجري الالتزام بسياسة الخصوصية التي أدلى الشخص المعني بالبيانات والمعلومات في ضوء بنودها؟

وللإجابة على ما سبق فإننا سوف نقوم بتقسيم هذا الفصل إلى مبحثين على النحو التالي:

- المبحث الأول: التزامات القائم بعملية المعالجة في ضوء اللائحة الأوروبية ٦٧٩/ ٢٠١٦.
- المبحث الثاني: حقوق الشخص المعني على بياناته موضوع المعالجة في ضوء اللائحة الأوروبية ٦٧٩/ ٢٠١٦.

---

(٤٧) من بين هذه المشروعات مشروع القانون المصري لحماية البيانات الشخصية والذي أشرنا إليه سلفاً ومشروع القانون التونسي رقم ٢٠١٨/٢٥ المتعلق بحماية المعطيات الشخصية والمتوفر على الرابط التالي: http://cutt.us/L1BA4.

(٤٨) للمزيد حول هذا الحكم راجع الدراسة التي أجراها الزميل الأستاذ الدكتور أشرف جابر سيد، مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع: دراسة خاصة لمسؤولية متعهدي الإيواء. *مجلة حقوق حلوان للدراسات القانونية والاقتصادية*، مصر، ع (٢٢)، يناير/ يوليو ٢٠١٠م، ص ص ١٠-٢١٢، ص ١١ هامش رقم ١. للمزيد أيضاً حول قضاء محكمة Pontoise الابتدائية راجع الرابط التالي:

https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-pontoise-6eme-chambre-2-collegiale tribunal de grande instance de Pontoise 6ème chambre2, 2 février 2005.

(٤٩) سيد، أشرف جابر، المرجع السابق، نفس الإشارة السابقة، ص ١١.

(٥٠) نفس الإشارة السابقة.

المبحث الأول: التزامات القائم بعملية المعالجة في ضوء اللائحة الأوروبية ٢٠١٦/٦٧٩

تقسيم

فرضت اللائحة الأوروبية ٢٠١٦/٦٧٩ على القائم بعملية معالجة البيانات العديد من الالتزامات التي ينبغي عليه أن يراعيها عند قيامه بمسألة المعالجة، ومن خلال استقراء نصوص اللائحة محل الدراسة نجد أنه شدد على التزام القائم بعملية المعالجة على اتباع عدد من الأمور التي نتناولها تباعاً في وفق ما يلي.

المطلب الأول: تطبيق مبدأ حماية البيانات على أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته

ينبغي أن ينطبق مبدأ حماية البيانات على أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته. وينبغي توفير الحماية اللازمة للبيانات الشخصية التي تعرضت لإساءة الاستعمال، والتي يمكن أن تنسب إلى شخص طبيعي باستخدام معلومات إضافية أو معلومات تساهم في تحديد هويته. ولتحديد ما إذا كان الشخص الطبيعي قابلاً للتحديد فإنه ينبغي أن تؤخذ في الاعتبار جميع الوسائل التي يحتمل استخدامها بشكل معقول من خلال مراعاة جميع العوامل الموضوعية، مثل تكاليف ومقدار الوقت اللازم لتحديد الهوية، مع الأخذ في الاعتبار التكنولوجيا المتاحة والتطورات التكنولوجية وقت المعالجة. ولذلك ينبغي ألا تنطبق مبادئ حماية البيانات على المعلومات المجهولة المصدر، أي المعلومات التي لا تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه.

فالإخلال بالبيانات الشخصية يعني حدوث إخلال يؤدي إلى التدمير العرضي أو غير المشروع للبيانات الشخصية المرسلة أو المخزنة أو المعالجة بطرق أخرى، أو ضياعها أو تحويرها أو الإفصاح عنها، أو الوصول إليها بدون إذن(٥١).

وتحقيقاً لهذه الحماية استحدث المشرع الأوروبي فكرة تطبيق الأسماء المستعارة على البيانات الشخصية، والتي من شأنها العمل على تقليل المخاطر التي يتعرض لها الشخص المعني، ويساعد المتحكمين والقائمين بالمعالجة على الوفاء بالتزاماتهم المتعلقة بحماية البيانات.

ولا يقصد المشرع الأوروبي بطبيعة الحال من ذكره صراحةً لفكرة "أمن البيانات" في هذا القانون أن يستبعد أي تدابير أخرى لحماية البيانات. ومن ذلك ربط الأشخاص الطبيعيين بالمعرفات المتوفرة عبر الإنترنت التي توفرها أجهزتهم وتطبيقاتهم وأداتهم وبروتوكولاتهم، مثل عناوين بروتوكول الإنترنت أو معرفات ملفات تعريف الارتباط أو المعرفات الأخرى مثل علامات تعريف الترددات الراديوية. وقد يترك ذلك آثاراً يمكن استخدامها، ولاسيما عندما تقترن بالمعرفات الفريدة وغيرها من المعلومات التي تتلقاها الخوادم، لوضع لمحات عن الأشخاص الطبيعيين وتحديد هويتهم.

ومن أجل تحقيق الحماية لا ينبغي أن تتم معالجة الفئات الخاصة من البيانات الشخصية التي تستحق حماية أعلى لأغراض تتعلق بالصحة إلا عند الضرورة لتحقيق تلك الأغراض لصالح الأشخاص الطبيعيين والمجتمع. كما ينبغي أن تخضع عملية التجهيز هذه لتدابير مناسبة ومحدده لحماية حقوق الأشخاص الطبيعيين وحرياتهم(٥٢).

---

(51) Règlement (UE) 2016/679, Art. 7 :**Conditions applicables au consentement**

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne = également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

(٥٢) يكون تجهيز الفئات الخاصة من البيانات الشخصية ضرورياً لأسباب تتعلق بالمصلحة العامة في هذا السياق، ينبغي تفسير "الصحة العامة" على النحو المحدد في اللائحة (EC) No. 1338/2008 الصادرة عن البرلمان الأوروبي والمجلس، أي جميع العناصر المتصلة بالصحة، وهي الحالة الصحية، بما في ذلك الاعتلال الذي يؤثر على هذه الحالة الصحية، واحتياجات الرعاية الصحية، والموارد المخصصة للرعاية =

وفي هذا السياق، ينبغي تفسير "الصحة العامة" على النحو المحدد في اللائحة (EC) No. 1338/2008 الصادرة عن البرلمان الأوروبي والمجلس بأنها جميع العناصر المتصلة بالصحة، وهي الحالة الصحية – بما في ذلك الاعتلال الذي يؤثر على الحالة الصحية – واحتياجات الرعاية الصحية، والموارد المخصصة لها والحصول عليها على الصعيد العالمي، فضلاً عن نفقات الرعاية الصحية وتمويلها، وأسباب الوفاة. وينبغي ألا يؤدي هذا التجهيز للبيانات المتعلقة بالصحة لأسباب تتعلق بالمصلحة العامة إلى معالجة البيانات الشخصية لأغراض أخرى من جانب أطراف ثالثة مثل أرباب العمل أو شركات التامين والمصارف(٥٣).

المطلب الثاني: الحصول على موافقة الشخص المعني بمعالجة بياناته بصورة حرة ومحددة ومستنيرة

ينبغي أن تكون موافقة الشخص على معالجة البيانات الشخصية المتعلقة به بصورة حرة، ومحددة، ومستنيرة، لا لبس فيها ولا غموض، بواسطة مستند مكتوب، أو عن طريق الوسائل الإلكترونية وعلى سبيل المثال وضع علامة على مربع مخصص لهذا الغرض عند زيارة موقع على شبكة الإنترنت، مع الأخذ في الاعتبار أنه إذا كانت موافقة الشخص المعني على معالجة بياناته الشخصية ستقدم بموجب وسيلة إلكترونية، فيجب أن يكون الطلب واضحاً وموجزاً ولا يعطل بدون داعٍ استخدام الخدمة التي قدم من أجلها.

ولذلك لا ينبغي أن يشكل السكوت موافقة على إجراء المعالجة. وينبغي أن تشمل الموافقة جميع أنشطة المعالجة التي سيقوم المعالج بها، وعندما يكون للمعالجة أغراض متعددة، ينبغي الموافقة عليها جميعاً وأن يوضح ذلك في بيان الموافقة المقدم من الشخص المعني.

ويستثنى مما تقدم معالجة البيانات لأغراض البحث العلمي شريطة أن تتفق مع المعايير الأخلاقية المتعاف عليها؛ لأنه غالباً ما يتعذر التحديد الكامل للغرض من معالجة البيانات الشخصية لأغراض البحث العلمي وقت جمع البيانات. ولذلك ينبغي السماح للشخص المعني بإعطاء موافقته على مجالات معينة من البحث العلمي عندما تكون متمشية مع المعايير الأخلاقية المعترف بها للبحث العلمي.

ومما تجدر الإشارة إليه في هذا الصدد على وجه الخصوص أنه إذا استندت المعالجة إلى موافقة الشخص المعني، فإنه يجب على القائم بها أن يثبت أن الشخص المعني قد وافق على معالجة بياناته الشخصية والأغراض التي تمت من أجلها هذه المعالجة على النحو السالف ذكره.

وقد اشترط المشرع الأوروبي عدة شروط فيما يتعلق بهذه الموافقة لعل أهمها أنه إذا قدمت الموافقة على البيانات في سياق إعلان مكتوب يتعلق أيضاً بمسائل إضافية، فلابد أن يقدم طلب الموافقة بطريقة يمكن تمييزها بوضوح عن المسائل الإضافية، باستخدام لغة واضحة وسهلة. ورتب المشرع الأوروبي جزاءً على مخالفة أحكام هذه المادة بقوله "أي جزء من هذا الإعلان يشكل انتهاكاً لهذه المادة لا يكون ملزماً"(٥٤).

كما أنه أعطى الشخص المعني الحق في سحب موافقته على إجراء عملية المعالجة في أي وقت.

ويُفهم من ذلك أن قيام الشخص المعني بسحب موافقته على عملية معالجة بياناته لا يؤثر على مشروعية عمليات المعالجة التي تمت قبل قيامه بسحب الموافقة. واشترطت اللائحة الأوروبية القيام بإبلاغ الشخص المعني بذلك قبل إعطاء الموافقة.

وفي سبيل حصول القائم بعملية المعالجة على موافقة حرة، وصريحة، ومحددة، ومستنيرة – على حد تعبير المادة ١١/ ٤ – يجب أن تتم عملية جمع ومعالجة البيانات في ظل احترام مبدأ الشفافية، واحترام حق الشخص المعني في الإعلام(٥٥)؛ لذلك

= الصحية، وتوفير الرعاية الصحية والحصول عليها على الصعيد العالمي، فضلاً عن نفقات الرعاية الصحية وتمويلها، وأسباب الوفاة. وينبغي ألا يؤدي هذا التجهيز للبيانات المتعلقة بالصحة لأسباب تتعلق بالمصلحة العامة إلى تجهيز البيانات الشخصية لأغراض أخرى من جانب أطراف ثالثة مثل أرباب العمل أو شركات التأمين والمصارف. للمزيد انظر: https://www.cnil.fr/en/official-texts.

(٥٣) نفس الإشارة السابقة.

(54) Voir texte de Règlement (UE) 2016/679, Art. 7.

(55) Règlement (UE) 2016/679, (39) Tout traitement de données à caractère personnel devrait être licite et loyal. Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être =

يجب على القائم بالمعالجة أن يقوم بإعلام الشخص المعني الذي يتم جمع معلوماته وبياناته الشخصية بأن عملية الجمع تتيح له حق الدخول لبياناته كما أن له الحق في إجراء ما يراه لازماً من تعديلات عليها.

وهذا هو المعنى المشار إليه في البند (٣٩) الوارد في مقدمة اللائحة الأوروبية والذي ينص على أن معالجة البيانات الشخصية يجب أن تتم بصورة قانونية. كما ينبغي أن تكون كافة العمليات التي يتم إجراؤها على البيانات الشخصية المتعلقة بالأشخاص المعنيين سواءً ما يتعلق بجمعها أو استخدامها أو تداولها أو معالجتها بأي طريقة أخرى خاضعة لمبدأ الشفافية، أي أن تكون جميع المعلومات والاتصالات المتعلقة بمعالجة هذه البيانات الشخصية سهلة المنال ويسهل فهمها وتصاغ بعبارات واضحة وبسيطة.

أضف لما تقدم، فإنه يجب إعلام الشخص المعني بكل المعلومات الأخرى الرامية لضمان معالجة عادلة وشفافة وضمان حقه في الوصول للبيانات الشخصية المتعلقة به في أي وقت شاء، كما ينبغي إبلاغ الأشخاص المعنيين بالقواعد والضمانات والحقوق المتعلقة بمعالجة البيانات الشخصية والإجراءات المتعلقة بممارسة حقوقهم فيما يتعلق بهذه المعالجة(٥٦).

وتجدر الإشارة إلى قيام المشرع الأوروبي في هذه اللائحة بإيراد شروطٍ خاصة فيما يتعلق بمسألة الموافقة على معالجة البيانات في حالات ثلاث شديدة الخصوصية نذكرها على النحو التالي:

الحالة الأولى: الشروط المتطلبة لمعالجة بيانات الطفل فيما يتعلق بدخوله لمجتمع المعلومات

فيما يتعلق بعرض خدمات مجتمع المعلومات مباشرةً على الطفل تكون معالجة البيانات الشخصية للطفل قانونياً إذا كان الطفل عمره ست عشرة سنة على الأقل. وإذا كان الطفل دون سن السادسة عشرة، لا تكون هذه المعالجة قانونية إلا إذا أعطى الولي أو الوصي على الطفل الإذن بذلك القبول.

وأعطت اللائحة الأوروبية الحق للدول الأعضاء في الاتحاد الأوروبي أن تنص بموجب القانون على سن أقل من المنصوص عليه في المادة الثامنة شريطة ألا يقل العمر عن ثلاث عشرة سنة(٥٧).

وجدير أن نشير هنا أن من بين القوانين التي قامت بحظر جمع أو معالجة البيانات الشخصية للطفل في وقت مبكر "قانون حماية خصوصية الأطفال على الخط" وهو قانون أنشئ لحماية خصوصية الأطفال دون سن الثالثة عشر عاماً. وقد برزت سياسة المشرع الفيدرالي الأمريكي في تحقيق العديد من الأهداف أهمها، وجوب الحصول على موافقة الولي أو الوصي على جمع أو استخدام أي معلومات شخصية للأطفال

= transparents à l'égard des personnes physiques concernées. Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement. Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement. En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel. Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique. Il y a lieu de prendre toutes les mesures raisonnables afin de garantir que les données à caractère personnel qui sont inexactes sont rectifiées ou supprimées. Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement.

(56) Règlement (UE) 2016/679, Art 8.

(٥٧) للمزيد حول هذا الموضوع راع تفصيلاً محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. مرجع سابق الإشارة إليه، ص ٦٨ وما بعدها.

مستخدمي مواقع الويب، وما يجب تضمينه في سياسة الخصوصية، بما في ذلك كيفية الحصول على موافقة أحد الوالدين أو الوصي على الطفل[٥٨]، بما في ذلك القيود المفروضة على أنواع وأساليب التسويق التي تستهدف أولئك الذين تقل أعمارهم عن ثلاثة عشر عاماً. وقد سجلت لجنة التجارة الاتحادية عدد من الخروقات والانتهاكات لهذا القانون[٥٩].

الحالة الثانية: القواعد الحاكمة لمعالجة الفئات الخاصة للبيانات الشخصية

حظر المشرع الأوروبي إفشاء البيانات الشخصية التي تكشف عن الأصل العرقي، أو الآراء السياسية، أو المعتقدات الدينية أو الفلسفية، أو عضوية الجمعيات أو النقابات، وكذلك معالجة البيانات الوراثية، وبيانات الاستدلال البيولوجي والبيانات المتعلقة بالصحة أو البيانات المتعلقة بالحياة الجنسية للشخص أو ميوله الجنسية، التي يمكن أن تؤدي إلى تحديد هويته. واستثنى المشرع من ذلك المعالجة البيانات التي تتم في الحالات التالية:

١- أن يكون الشخص المعني قد أعطى موافقة صريحة على معالجة تلك البيانات الشخصية لغرض أو أكثر من الأغراض المحددة، إلا إذا نص قانون الاتحاد أو الدولة العضو غير ذلك.

٢- المعالجة الضرورية لأغراض الوفاء بالتزامات وممارسة حقوق محددة للشخص المعني في ميدان العمل والضمان الاجتماعي وقوانين الحماية الاجتماعية.

٣- المعالجة الضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص طبيعي آخر عندما يكون الشخص المعني غير قادر مادياً أو قانونياً على إعطاء الموافقة.

٤- المعالجة الضرورية لأسباب تتعلق بالمصلحة العامة، على أن يتم احترام جوهر الحق في حماية البيانات، وأن ينص قانون الدولة العضو على تدابير مناسبة ومحددة لحماية الحقوق والمصالح الأساسية للشخص المعني.

٥- المعالجة الضرورية لأغراض الطب الوقائي أو المهني، ولتقييم قدرة الموظف على العمل، والتشخيص الطبي، وتوفير الرعاية الصحية أو الاجتماعية أو العلاج أو إدارة نظم الرعاية الصحية أو الاجتماعية.

٦- المعالجة الضرورية لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة، مثل الحماية من الأخطار الكبيرة التي تهدد الصحة عبر الحدود أو ضمان مستويات عالية من الجودة والسلامة في الرعاية الصحية والمنتجات الطبية أو الأجهزة[٦٠].

---

(58) The Children's Online Privacy Protection Act (COPPA) is a law created to protect the privacy of children under 13. The Act was passed by the U.S. Congress in 1998 and took effect in April 2000. COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. See: https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5. See also: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

تجدر الإشارة إلى أن هذا القانون حظر على مشغلي المواقع الإلكترونية Operators، تجميع أي معلومات تفيد في تحديد الهوية الشخصية من قبل الأطفال تحت ١٣ سنة، دون موافقة الوالدين، والمعلومات التي يسمح بتجميعها هي تلك المعلومات التي تكون ضرورية بشكل معقول Reasonably necessary للنشاط عبر الخط، والمعلومات الشخصية التي لا يسمح بتجميعها من الأطفال هي: الاسم بالكامل، والعنوان، ورقم بطاقة الضمان الاجتماعي، ورقم الهاتف، وغيرها. وبذلك يعطي هذا القانون للأبوين سلطة الرقابة على تجميع بيانات أطفالهم، وكيفية مشاركة هذه المعلومات عبر الإنترنت، وتراقب غرفة التجارة الفيدرالية FTC مدى استجابة المواقع الإلكترونية لمتطلبات هذا القانون. وبناءً على ذلك قامت الغرفة بتغريم موقع Xanga غرامة قدرها مليون دولار لقيامه بتسجيل طفل تحت ١٣ سنة لاستخدام خدماته، دون أخذ موافقة أبويه، ولنفس السبب أيضاً فرضت غرامة قدرها ٤٠٠٠٠٠ دولار أمريكي على شركة UMG Recording, Inc. للمزيد راجع:

Lee, C.F., and Lee, A. (Hrsg.). *Encyclopedia of Finance*. New York: Springer U.S., (2006). ISBN: 978-387-26284-0. 307 p.

وانظر أيضاً: عصام محمد رشيد منصور، قوانين حماية خصوصية الأطفال على الإنترنت: قراءة في القانون الأمريكي COPPA مع استعراض للموقف العربي من مثل هذه القوانين. *مجلة دراسات المعلومات*، مجلة علمية محكمة، ع (٦)، (سبتمبر ٢٠٠٩م)، ص ص ١٣١-١٦٣، ص ١٣٥ وما بعدها.

(٥٩) من بين أبرز المواقع التي تم توقيع عقوبات عليها:

Girl's Life, Inc., American Pop Company, The Xanga, Lisa Frank, Mrs. Field's Cookies, Hershey Foods, Bonzi Software, and UMG Recording, Inc.

(٦٠) على أساس قانون الاتحاد أو الدولة العضو الذي ينص على تدابير مناسبة ومحددة لضمان حقوق وحريات الشخص المعني، ولاسيما السرية المهنية.

٧- المعالجة الضرورية لأغراض الحفظ من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية.

٨- وأجاز اللائحة للدول الأعضاء أن تحتفظ بشروط إضافية، بما في ذلك القيود الخاصة بمعالجة البيانات الجينية أو بيانات الاستدلال البيولوجي أو البيانات المتعلقة بالصحة.

الحالة الثالثة: تجهيز البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية

فيما يخص معالجة البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية، فإنه لا يتم تجهيز البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية أو التدابير الأمنية المتصلة بها إلا تحت رقابة السلطة الرسمية أو عندما يؤذن بالمعالجة قانون الاتحاد أو الدولة العضو، على أن ينص على توفير الضمانات المناسبة لحقوق وحريات الشخص المعني. على ألا يتم الاحتفاظ بأي سجل شامل للإدانة الجنائية إلا تحت رقابة السلطة الرسمية[٦١].

المطلب الثالث: الالتزام باحترام مبدأ الشفافية واحترام حق الشخص المعني في الإعلام

يقتضي مبدأ الشفافية أن تكون المعلومات الموجهة إلى الجمهور أو إلى الشخص المعني موجزة، ويسهل الوصول إليها ويسهل فهمها، وأن تستخدم لغة واضحة وسهلة. ويمكن تقديم هذه المعلومات إلى الجمهور في شكل إلكتروني، من خلال موقع على شبكة الإنترنت على سبيل المثال.

ويتسم هذا المبدأ بأهمية بالغة خاصةً في الحالات التي تتزايد فيها الجهات الفاعلة في مسألة المعالجة، أضف لذلك التعقيد التكنولوجي للممارسات والذي قد يزيد من صعوبة فهم ما إذا كانت البيانات الشخصية المتعلقة به أو الغرض منها هي التي يجري جمعها، مثل في حالة الإعلان على الإنترنت.

ويُعد التزام القائم بعملية المعالجة بالإعلام شرطاً ضرورياً لنزاهة وشفافية عملية جمع البيانات الشخصية، على أن تكون موافقة الشخص المعني التي يبديها في ضوء كافة المعلومات المفصح عنها، ومن ذلك الإشارة بشكل صريح لهوية المسؤول عن عملية جمع البيانات أو ممثله، وذكر الغرض من المعالجة، وطريقة الإيداع، وطريقة الدخول للبيانات، وكيفية محوها، ومصير البيانات فيما بعد ... إلخ.

أيضاً تقتضي مبادئ المعالجة العادلة والشفافة أن يُزود الشخص المعني بأي معلومات إضافية ضرورية لضمان التجهيز العادل والشفاف مع مراعاة الظروف الخاصة والسياق الذي تُجهز فيه البيانات الشخصية. وعلاوة على ذلك ينبغي إبلاغ الشخص بالحالات التي تجمع فيها البيانات الشخصية.

غير أنه ليس من الضروري فرض التزام بتقديم المعلومات عندما يكون الشخص المعني حائزاً بالفعل على المعلومات؛ حيث ينص القانون صراحةً على تسجيل البيانات الشخصية أو الإفصاح عنها. ويمكن أن تكون الحالة الأخيرة على وجه الخصوص تلك التي يجري فيها التجهيز لأغراض الحفظ من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية. وفي هذا الصدد، ينبغي أن يؤخذ في الاعتبار الأغراض المتعلقة بمعالجة البيانات، ومدة الاحتفاظ بالبيانات، وأي ضمانات مناسبة أخرى[٦٢].

المطلب الرابع: الالتزام بالإخطار فيما يتعلق بتصحيح أو محو البيانات الشخصية أو تقييد عملية المعالجة

يجب على القائم بمعالجة البيانات القيام بإبلاغ الشخص المعني بأي تصحيح أو محو للبيانات الشخصية أو بأي تقييد لعملية المعالجة.

وقد نص المشرع الأوروبي على هذا الالتزام في المادة (١٩) بقوله "أنه يجب على القائم بالمعالجة أن يقوم بإبلاغ الشخص المعني بأي تصحيح أو محو للبيانات الشخصية الذي يجري وفقاً للمادة (١٦)، والمادة (١٧/ ١)، والمادة (١٨)، ما لم يثبت

(61) Règlement (UE) 2016/679, Art 10.

(62) Règlement (UE) 2016/679, Art 6, 7, 8.

أن ذلك يصعب القيام به لأسباب خارجة عن إرادته أو أن القيام به يتطلب جهوداً غير عادية".

ويُفهم من النص السابق أن المشرع الأوروبي ألزم القائم بعملية المعالجة بإبلاغ الشخص المعني بأي تصحيح يتم على البيانات الشخصية، واستثنى من ذلك تلك الحالة التي يثبت فيها القائم بالمعالجة أن يتعذر عليه إبلاغ الشخص المعني بذلك لأسباب قاهرة خارجة عن إرادته، أو أن إبلاغ الشخص المعني يتطلب بذل جهود غير عادية، وفي هاتين الحالتين فقط يُعفى القائم بالمعالجة من إخطار الشخص المعني بالتصحيح أو المحو، لكن بطبيعة الحال يقع عليه عبء إثبات توافر حالة القوة القاهرة أو أن إبلاغ الشخص المعني يتطلب بذل جهد غير عادي حتى يُعفى من أداء هذا الالتزام.

المطلب الخامس: الالتزام بحظر معالجة البيانات الشخصية الأطفال

إن السماح للأطفال بالاستخدام المطلق لخدمات الإنترنت يؤدي إلى مشكلات كثيرة، وقد ينجم عنه انحراف في سلوكياتهم، ولذلك فإن جميع المهتمين بالطفولة تنبهوا لهذا الأمر فصدرت تشريعات تحدد آلية وشروط التعامل مع القاصرين عبر الإنترنت في كثير من دول العالم(٦٣).

ومؤدى ذلك يتلخص في أن عدم وضع قيود على استخدام الأطفال للإنترنت يجعلهم قادرين على الوصول إلى العديد من المواقع التي قد تنمي لديهم نزعات الكراهية والعدوانية وغيرها.

وسعياً في إيجاد حل لهذه الإشكالية التي تؤرق الكثيرين منا فإن هناك أموراً ثلاثة لا يجب أن يغفل عنها أي مشرع عند وضعه لتشريع لحماية بيانات الطفل، ونجمل هذه الأمور في محاور ثلاثة هي:

- المحور الأول: يتعلق بالدولة فهي مسؤولة عن حماية الأطفال بحظر المواد غير المناسبة التي يتم عرضها عبر الإنترنت.
- المحور الثاني: يتعلق بالوالدين فهما مسؤولان عن متابعة أطفالهما ومراقبتهم وتوجيههم.
- المحور الثالث: يتعلق بمسؤولية مزودي خدمات الإنترنت ISP(٦٤) وهم المسؤولون عن توفير الخدمات التي تناسب العائلات ولا تسيء إلى سلوكيات وأخلاق الأطفال(٦٥).

وفي هذا المقام سيتم التركيز على الحماية التي أولاها المشرع الأوروبي في اللائحة للأطفال الذين يقل عمرهم عن ثلاثة عشر عاماً.

فالأطفال في هذه المرحلة العمرية على وجه التحديد، يستحقون حماية محددة فيما يتعلق ببياناتهم الشخصية؛ لأنهم يكونون أقل وعياً بالمخاطر والعواقب والضمانات المعنية بحقوقهم فيما يتعلق بتجهيز ومعالجة بياناتهم الشخصية. وينبغي أن تنطبق هذه الحماية المحددة – على وجه الخصوص – استخدام البيانات الشخصية للأطفال لأغراض التسويق.

ويجب النظر هنا إلى أن الأطفال يستحقون حماية خاصة؛ لأنه عندما تكون المعالجة موجهة إلى البيانات والمعلومات الخاصة بالطفل، ينبغي أن تكون بلغة واضحة وسهلة يمكن للطفل أن يفهمها بسهولة ومتناسبة مع الفئة العمرية له.

المبحث الثاني: حقوق الشخص المعني على بياناته موضوع المعالجة في ضوء اللائحة الأوروبية ٦٧٩/ ٢٠١٦

تمهيد

لقد حرص المشرع الأوروبي في اللائحة محل الدراسة على حماية خصوصية البيانات الشخصية للأشخاص الطبيعيين؛ فنجد أن الطابع الحمائي يسيطر على السياسة التشريعية للمشرع الأوروبي(٦٦) عن طريق إلزام كل من يقوم باستخدام هذه البيانات بتوفير العديد من الحقوق للشخص التي تكون بياناته

(٦٣) للمزيد حول هذا الموضوع راجع الرابط التالي:
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

(64) Internet Service Provider.

(٦٥) نفس الإشارة السابقة، وانظر كذلك يوسف أحمد أبو فارة، تحليل العلاقة بين حماية الخصوصية وبين التسجيل والإفصاح عن البيانات الشخصية في المتاجر الإلكترونية. *مجلة العلوم الإدارية*، الأردن، مج (٣٣)، ع (٢)، (٢٠٠٦م)، ص ص ١٨٩-٢٠٨، ص ١٩٣ وما بعدها.

(٦٦) محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. مرجع سابق الإشارة إليه، ص ٦٦.

محلاً للمعالجة، من خلال السماح لصاحب هذه البيانات بالتحقق من نظام التخزين أو كيفية إيداع هذه البيانات، وكيفية معالجتها، والتعرف على هوية السلطات العامة أو الجهات المختصة التي تهتم بها فضلاً عن إقرار العديد من الحقوق الأخرى كالحق في المحو أو النسيان الرقمي، والحق في تصحيح البيانات إن كانت خاطئة، والحق في الاعتراض على هذه المعالجة، وغيرها، وذلك كله على النحو التالي.

المطلب الأول: الحق في الوصول للبيانات محل المُعالجة

تناولت الفقرة السادسة من المادة الرابعة من اللائحة الأوروبية ما يعرف بـ"نظام الإيداع" بقولها "أي مجموعة منظمة من البيانات الشخصية التي يمكن الوصول إليها وفقاً لمعايير محددة سواءً كانت مركزية أو لامركزية أو مصنفة على أساس وظيفي أو جغرافي"[٦٧].

وينبغي أن يكون للشخص المعني الحق في الوصول إلى البيانات الشخصية التي جمعت بشأنه من خلال الوصول إلى هذه المجموعات المنظمة والتي أدرجها المشرع الأوروبي تحت ما يسمى بـ"نظام الإيداع"، ويجب أن يمارس هذا الحق بسهولة ويسر، وعلى فترات معقولة لكي يكون على علم بمشروعية عملية المعالجة، والتحقق منها.

ويشمل ذلك حق الأشخاص الخاضعة بياناتهم للمعالجة في الحصول على البيانات المتعلقة بصحتهم، مثل البيانات التي تتضمنها سجلاتهم الطبية والتي تحتوي على معلومات مثل التشخيص ونتائج الفحص والتقييمات عن طريق علاج الأطباء وأي علاج مقدم لهم.

كما ينبغي أن يكون للشخص المعني الحق في معرفة المعلومات والحصول عليها، ولاسيما فيما يتعلق بالأغراض التي تُعالج من أجلها البيانات الشخصية، والفترة التي يمكن فيها معالجة البيانات الشخصية، والجهات المتلقية لهذه البيانات، والمنطق الذي ينطوي على أي معالجة تلقائية لهذه البيانات.

(67) Règlement (UE) 2016/679, Art 4/6: «fichier», tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

وينبغي أن يكون القائم بالمعالجة قادراً - متى أمكن ذلك - على توفير إمكانية الوصول عن بعد وفق نظام آمن يوفر للشخص المعني إمكانية الوصول المباشر إلى بياناته الشخصية، وألا يؤثر هذا الحق تأثيراً سلبياً على حقوق الآخرين أو حرياتهم، بما في ذلك الأسرار التجارية أو الملكية الفكرية، وبوجه خاص حق مؤلفي البرمجيات. مع الوضع في الاعتبار ألا تكون هذه الاعتبارات مبرراً لرفض لتقديم وصول الشخص المعني إلى المعلومات الخاصة به.

وفي الحالات التي يقوم فيها القائم بالمعالجة، بمعالجة كمية كبيرة من المعلومات المتعلقة بالشخص المعني فإنه لابد من تحديد الغرض من المعالجة قبل البدء فيها حتى لا تتعرض تلك المعلومات لإساءة استخدامها[٦٨].

المطلب الثاني: الحق في تصحيح البيانات الشخصية غير الدقيقة

ينبغي أن يكون للشخص المعني الحق في تصحيح بياناته الشخصية، كما لابد من الاعتراف بحقه في "النسيان الرقمي" إذا كان الاحتفاظ بهذه البيانات يشكل إخلالاً أو انتهاكاً لخصوصيته على النحو الذي سنعرض له لاحقاً.

ويحرص معالجو البيانات ذات الطابع الشخصي ومن بينهم مقدمي خدمات التواصل الاجتماعي عبر شبكة الإنترنت على الإعلان عن سياسة استخدامهم للبيانات الشخصية للمستخدمين (politique d'utilisation des données) بحيث يتعين على كل مستخدم أن يقبل بهذه السياسة قبل

(68) Règlement (UE) 2016/679, (58).Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. Ces informations pourraient être fournies sous forme électronique, par exemple via un site internet lorsqu'elles s'adressent au public. Ceci vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne. Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre.

انضمامه لعضوية مواقع التواصل والاستفادة من خدماته[٦٩] ومن بين هذه السياسات حق المستخدم أو الشخص المعني في تصحيح بياناته الشخصية، وهو ذات المعنى الذي اتجهت إليه المادة الثانية عشر من اللائحة العامة لحماية البيانات الصادرة عام ١٩٩٥م الملغاة بموجب اللائحة الحالية[٧٠].

وتتأتى أهمية هذا الحق فيما ذكرناه آنفاً من أنه يمكن أن تنتهك خصوصية الفرد وتلحق به أضراراً قد يتعذر تداركها، عن طريق التلاعب في البيانات الشخصية من قبل أشخاص غير مرخص لهم، أو عن طريق جمع ومعالجة بيانات شخصية غير صحيحة من قبل المرخص لهم بذلك قانوناً.

ونظراً لأن هذا الحق من الحقوق الأصيلة للشخص المعني، فإنه يجب على القائم بعملية المعالجة أن يقوم بتبصيره بالمعطيات التقنية اللازمة لإجراء التصحيح الذي يراه لازماً لبياناته الشخصية.

المطلب الثالث: الحق في الاعتراض على معالجة البيانات

يعرف هذا الحق بـ"حق تقييد عمليات المعالجة"، وهو حق للشخص المعني يتمكن بموجبه من الاعتراض على عمليات المعالجة التي تتم على بياناته الشخصية.

أما عن آلية الاعتراض فإن الشخص المعني يقوم به خلال مرحلة الجمع وتخزين البيانات أو بعد ذلك، بأن يمتنع عن إعطاء المعلومات أو الإدلاء بأية بيانات تُطلب منه بمعرفة القائم بالمعالجة بواسطة أي طريقة من طرق جمع البيانات وتحليلها، وعلى سبيل المثال فإن الخروج من الموقع الإلكتروني، أو القيام بتعبئة البيانات المطلوبة للحصول على خدمة معينة، أو القيام بتفعيل الحق الممنوح من مالك الموقع والمعروفة بتقنية (opt-in) يعتبر رفضاً لعملية معالجة البيانات وهو حق أصيل للشخص المعني في مرحلة ما قبل الإدلاء بالبيانات[٧١].

وفيما يخص الاعتراض لوقف عملية معالجة البيانات الشخصية فإن الشخص المعني يستطيع القيام بها عبر أكثر من وسيلة، من بينها تقنية (opt-out) وذلك بطلب من الشخص المعني بموجب رسالة إلكترونية يوجهها للقائم بالمعالجة ويبدي فيها رغبته بوقف معالجة بياناته الشخصية.

وقد أحصى المشرع الأوروبي في المادة الثامنة عشر من اللائحة عدداً من الحالات التي يحق فيها للشخص المعني الاعتراض على عملية معالجة بياناته، وذلك على النحو التالي:

(أ) الحق في إبداء الاعتراض على دقة البيانات الشخصية محل المعالجة. ويستثنى من ذلك أنه إذا كانت المعالجة مقيدة وتم

(٦٩) انظر السياسات الخصوصية التي يتبعها موقع فيسبوك الشهير في استخدام البيانات الشخصية عبر الرابط التالي:
https://ar-ar.facebook.com/privacy/explanation/
وانظر كذلك محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. مرجع سابق الإشارة إليه، ص ٦٦.

(70) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)

(71) Règlement (UE) 2016/679, Art. 21. Droit d'opposition:
1. La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.
2. Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.
3. Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins.
4. Au plus tard au moment de la première communication avec la personne concernée, le droit visé aux paragraphes 1 et 2 est explicitement porté à l'attention de la personne concernée et est présenté clairement et séparément de toute autre information.
5. Dans le cadre de l'utilisation de services de la société de l'information, et nonobstant la directive 2002/58/CE, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.
6. Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques en application de l'article 89, paragraphe 1, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public.

إيقافها لهذا السبب فإنه لا يتم إجراء أي عمل من عمليات المعالجة باستثناء عملية التخزين إلا بموافقة الشخص المعني، أو باستخدام وسائل قانونية لإضفاء الشرعية على عملية المعالجة، أو لحماية حقوق شخص طبيعي أو اعتباري آخر أو لأسباب تتعلق بالمصلحة العامة.

(ب) للشخص المعني الحق في إبداء الاعتراض على عمليات المعالجة غير القانونية للبيانات، كما أنه له الحق في طلب محوها، على النحو الذي سنعرض له.

(ج) للشخص المعني الحق في الاعتراض على عملية المعالجة عملاً بنص المادة (٢١/ ١) إلى حين التحقق مما إذا كانت الأسباب المشروعة للقائم بالمعالجة تتجاوز تلك الواردة في طلب المعالجة من عدمه.

وجدير بالإشارة أنه في حال حصول الشخص المعني على تقييد عملية المعالجة طبقاً لتوفر حالة من الحالات المذكورة آنفاً، فإنه يجب على القائم بالمعالجة إخطار الشخص المعني قبل رفع القيود المفروضة على عملية المعالجة. وللشخص المعني الحق في أن يعترض في أي وقت - لأسباب تتعلق بحالته الخاصة - على معالجة البيانات الشخصية المتعلقة به ما لم يثبت القائم بالمعالجة أن هناك أسباباً مشروعة قاهرة للمعالجة، وبالتالي لا يمكن للشخص المعني أن يتذرع بأن هناك مساساً بمصالحه أو حقوقه[٧٢]. ويكون الاعتراض لحظة البدء في جمع المعلومات أو بعد ذلك، بأن يقوم الشخص المعني في الحالة الأولى بالامتناع عن نقل وإعطاء المعلومات بمجرد أن يطلب منه تقديمها؛ فهو يمارس هذا الحق عن طريق خروجه من الموقع الإلكتروني، ومن بين الحالات التي يحق للشخص المعني الاعتراض عليها:

(أ) عدم الحصول على موافقته الصريحة على ذلك، أو أن يتضح أن الغرض من المعالجة كان غرضاً آخر غير التسويق المباشر على سبيل المثال.

(ب) عندما يتم جمع وتحليل البيانات الشخصية لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية يحق للشخص المعني - لأسباب تتعلق بحالته الخاصة - الاعتراض على معالجة البيانات الشخصية المتعلقة به، ما لم يكن ذلك ضرورياً لأداء مهمة يضطلع بها لأسباب تتعلق بالمصلحة العامة.

ونظراً لأننا في سياق مجتمع المعلومات، فإنه يجوز للشخص المعني أن يمارس حقه في الاعتراض باستخدام الوسائل التقنية.

المطلب الرابع: الحق في النسيان الرقمي

نحيل هذا الموضوع لما سوف نذكره عن هذا الحق وما يثيره من إشكالات قانونية ولكننا سوف نتعرض هنا له بالقدر اللازم باعتباره أحد أهم حقوق الشخص المعني على بياناته الشخصية.

يُعد الحق في النسيان الرقمي[٧٣] للبيانات والمعلومات الشخصية التي تبقى عالقة في خوادم الشركات أو تلك التي

(٧٢) هذا ما نصت عليه المادة (٤) من التوجيه الأوروبي لسنة ١٩٩٥م الملغي، ويتضمن هذا الحق إمكانية الاعتراض على التدخل أو التقصي عن خصوصياته من جهة، وسلطة الاعتراض على وصول معلومات تتعلق بخصوصياته إلى الغير من جهة أخرى.

(٧٣) أطلق عملاق المعلوماتية الأمريكي "جوجل" خدمة جديدة على الإنترنت مخصصة للأوروبيين فقط تمكنهم من حذف معلومات وروابط لا يرغبون في أن ترتبط بأسمائهم على الإنترنت انطلاقاً من "حق النسيان" الرقمي الذي فرضته عليه محكمة العدل الأوروبية.
وأضاف الخبر الذي نشره موقع France 24 تحت عنوان "جوجل يمنح "حق النسيان" على الإنترنت ... ولكن للأوروبيين فقط" روابط ومعلومات لا تريدون أن ترتبط بكم عندما يكتب اسمكم على محرك البحث الأمريكي جوجل، الحل موجود، يقترحه العملاق الأمريكي اعتباراً من الخميس ٢٩ مايو/ أيار يدخل ضمن إطار ما صار يطلق عليه مؤخراً بـ"حق النسيان" الرقمي. وتقترح هذه الخدمة الجديدة المخصصة للأوروبيين فقط، مسح نتائج البحث على الإنترنت المرتبطة باسم المستخدم كروابط ومعلومات ومشاركات في مواقع تواصل اجتماعي، يعتبر صاحبها بأنها "في غير محلها، غير ملائمة، أو لم تعد ذات صلة".
وتتم العملية عبر استمارة على الإنترنت يملأ عبرها المستخدم خانة متعلقة بالبيانات الشخصية (الاسم واللقب والبريد الإلكتروني...) وبعدها يضع الروابط التي يريد حذفها. ولم توضح شركة جوجل المدة الزمنية التي تستغرقها عملية البحث ولا المعايير التي تأخذ بعين الاعتبار في تبريرات من يتقدم بالطلب.

قامت بجمعها بأية طريقة من طرق الجمع المعروفة التي تعرضنا لها آنفاً، أحد أهم الحقوق الذي ازدادت أهميتها بشكل كبير في الآونة الأخيرة في ظل تزايد انتهاكات الخصوصية في محيط البيئة الرقمية.

فمن المحتمل أن ينجم عن عمليات المعالجة للبيانات الشخصية أضراراً نفسية أو مادية، فمن هنا يجب الاعتراف

وكانت محكمة العدل الأوروبية فرضت في مايو/ أيار ٢٠١٣م على جوجل ضمان "حق النسيان الرقمي" لمستخدميه، باعتبار أن مشغل محرك البحث على الإنترنت مسؤول عن معالجة المعطيات الشخصية التي تظهر على صفحاته. ولذلك يجب عليه تمكين الأفراد من التوصل في بعض الظروف إلى إلغاء روابط معينة على صفحات إلكترونية تتضمن معطيات شخصية، من خلال التوجه مباشرة إلى المشغل.

ويبقى عملاق المعلوماتية جوجل، محرك البحث الأكثر استخداماً على الإنترنت حيث تمر عبره ٩٠٪ من عمليات البحث، ويضم ٢,٥ مليار مستخدم عبر العالم من خلال تطبيقاته المختلفة. تم نشر هذا الخبر عبر الرابط: http://www.france24.com/ar.

وكان الحكم قد صدر إثر قيام مواطن إسباني يدعى ماريو كوستيخا غونزالس بنشر اسمه في صحيفة عام ١٩٩٨م بصفته مالك عقار سيتم عرضه في مزاد لتسديد ديونه، وعلى الرغم من تجاوز الرجل أزمته إلا أن الروابط المتعلقة بهذه المعلومات استمرت بالظهور في محركات البحث عند جوجل بعد مرور ما يزيد على ١٦ عاماً، وحاول الرجل من جانبه في محاولة لإنهاء تأثير ذلك عليه نفسياً وتجارياً إلى السعي إلى مسح هذه المعلومات، وفي عام ٢٠١٠م وقفت هيئة حماية البيانات في إسبانيا إلى جانبه، حيث أمرت جوجل بمسح الروابط. واستأنفت من جانبها جوجل القرار، الأمر الذي دفع المحكمة الإسبانية إلى تحويل القضية لمحكمة العدل الأوروبية لاستشارتها.

والجدير بالذكر أن المفوضية الأوروبية قد اقترحت عام ٢٠١٢م قانوناً يمنح مستخدمي الإنترنت "الحق في محو البيانات". وسيتعين على محرك البحث إدخال تعديلات على بعض نتائج البحث حتى تكون متطابقة مع التوجيهات الأوروبية بخصوص حماية البيانات الشخصية.

واستندت محكمة العدل الأوروبية على قانون الاتحاد الأوروبي، والذي يعتبر أن محرك البحث "مسؤول عن العمليات التي تجرى على البيانات الشخصية التي تظهر على صفحاته وتشمل المحتوى الذي نشر بالفعل في وسائل الإعلام". وإن هذه المعلومات تحتوي على جوانب عدة للحياة الشخصية للفرد. ويؤكد الحكم على أن حق الأشخاص أقوى عندما يتعلق بالتصرف في بياناتهم الخاصة، على الرغم من حق الناس - بصفة عامة - في الحصول على المعلومات المتعلقة بالشخصيات العامة.

ومن ثم فقد خلصت المحكمة إلى أن ذلك يتعارض مع الحقوق الأساسية للفرد، بـ"حق محو البيانات". بل وقررت أنه يجب أن تتوافر الآلية أمام المواطنين لطلب مسح روابط تحتوي على بيانات "غير كافية أو ليست ذات صلة أو أنها أصبحت مسيئة"، واعتبرت جوجل من جانبها أن هذا الحكم مخيب للآمال بالنسبة لمحركات =

= البحث والجهات الأخرى الناشرة على شبكة الإنترنت بشكل عام، وأن هذا القرار جاء رغم توصية أحد كبار المحامين بالمحكمة العام الماضي بأنه لا يجب أن تتحمل محركات البحث مسؤولية المعلومات التي تظهر في صفحات البحث.

وقد امتثلت جوجل للحكم وبدأت في وضع نموذج الطلب على الموقع في ٣٠ مايو الماضي، والإعلان عن إجراءات بشأن طلبات الإزالة، وتلقت جوجل أكثر من ٧٠ ألف طلب لمحو روابط تحتوي على بيانات شخصية، في ظل القانون الأوروبي لحماية البيانات الشخصية. وأعلنت شركة جوجل أنه سيتم النظر والدراسة في كل طلب على حدة، لتحديد ما إذا كان يتطابق مع معايير المحكمة أم لا.

وقد أثر ذلك على احتجاج الصحف ووكالات الأخبار والتي ربما يتم إزالة أخبار خاصة بها بسبب احتوائها على بيانات لأشخاص لا يرغبون في وجودها على محرك البحث العملاق. وهو ما تعده تلك المؤسسات الصحفية بمثابة ملكية فكرية، وهو ما يتم الرد عليه أن المادة ما تزال محفوظة على موقع الجريدة إلا أنها لن تظهر فقط في محركات البحث، وقامت بعض الصحف مثل الجارديان والبي بي سي بنشر قائمة بالروابط التي تم حذفها من أخبار وقصص حظر تداولها على النسخ الأوروبية لموقع جوجل.

ويحمل الحكم أيضاً تبعات على كل من ينشر معلومات عن أشخاص على الإنترنت. وأن أي شخص لا يعجبه منشور قديم ذو صلة به، من حقه أن يطلب إلغاءه وبخاصة بعد مرور فترة كبيرة على نشره وأن من شأن تلك المعلومات أو الروابط أن تؤثر على الحرية الشخصية وعلى سمعة الشخص وهو ما يكون له تأثيرات خاصة في مجال المال والأعمال، وذلك كحالة نشر روابط عن قضية فساد إحدى الشركات والتي تظل تؤثر في سمعة الشركة بغض النظر عن نتائج التحقيق أو تغير إدارة الشركة أو تغير طبيعة القوانين المتبعة. راجع في ذلك الرابط التالي: http://www.accronline.com/article_detail.aspx?id=19502.

وللمزيد حول هذا الموضوع بصفة عامة يرجى مراجعة دراسة الزميل عبدالهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الإنترنت: دراسة قانونية تطبيقية مقارنة. *مجلة القانون والاقتصاد*، كلية الحقوق، جامعة القاهرة، مصر، علمية، محكمة، مج (٨٥)، (٢٠١٥م)، ص ص ٣١٣-٤٦٣.

بالحق في النسان الرقمي للبيانات الشخصية والمعلومات متى انتهى الغرض من معالجتها أو انتهت المدة التي وافق الشخص على استخدام بياناته الشخصية خلالها.

ومن خلال البحث وجدت أن هناك خلطاً شائعاً بين مصطلحين هما، الحق في النسيان الرقمي والحق في التصحيح الذي قد يصل للحذف، وهو ما أوضحه المشرع الأوروبي بالنص على الحق في التصحيح في المادة السادسة عشر منه بقوله "للشخص المعني الحق في الحصول من القائم بالمعالجة على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به دون أي تأخير في ذلك". ومع مراعاة أغراض المعالجة، يكون للشخص المعني الحق في استكمال البيانات الشخصية الناقصة بأي طريقة، بما في ذلك عن طريق تقديم بيان تكميلي.

أما ما نقصده هنا هو الحق في النسيان الرقمي وهو ما أورده المشرع الأوروبي في نص المادة السابعة عشر من اللائحة الأوروبية، والتي تناولت هذا الحق تحت عنوان (droit à l'oubli).

المطلب الخامس: الحق في محو البيانات الشخصية

يعرف هذا الحق بحق الشخص المعني الذي تمت معالجة بياناته الشخصية في اتخاذ القرار الخاص بالمعلومات المتعلقة به. وهذا يعني منح الشخص سلطة اتخاذ القرار في مصير المعلومات الخاصة به.

وإذا طبقنا هذا الحق في المجال الرقمي يصبح بإمكان الشخص التمتع بسلطة مراقبة كل المعلومات المتعلقة به وحذفها سواءً تلك المرتبطة بشخصه والمنشورة في مواقع التواصل الاجتماعي أو معلوماته التي تحصل عليه المواقع والتطبيقات الرقمية. ويلتزم القائم بعملية المعالجة بتمكين الشخص المعني من ممارسة حقه في تقرير مصير البيانات المتعلقة به بمحوها أو حذفها أو حتى تدقيقها دون أي تأخير لا مبرر له.

والعلة من جوب ذلك الحق تكمن في أن الشخص المعني قد يرى أنه من الأصلح محو أو حذف بياناته في الحالات التي لم تعد فيها هذه البيانات ضرورية فيما يتعلق بالأغراض التي جمعت من أجلها أو معالجتها. ويتحقق هذا الفرض في حالات عدة من بينها أن يكون الشخص المعني قام بسحب موافقته أو أبدى اعتراضه على معالجة البيانات الشخصية المتعلقة به، أو في تلك الحالة التي لا يمتثل فيها القائم بمعالجة بياناته الشخصية لأحكام القانون.

ومن جانبنا نرى أن هذا الحق تتعاظم أهميته عندما يكون الشخص المعني طفلاً قد أعطى موافقته وهو لا يدرك تماماً المخاطر التي تنطوي عليها عمليات الجمع والمعالجة، ويريد لاحقاً إزالة هذه البيانات الشخصية. وينبغي إذن في هذه الحالة أن يسمح له بممارسة هذا الحق وأن يكون قادراً على الحذف بصرف النظر عن كونه لم يعد طفلاً.

ومما تجدر الإشارة إليه في هذا الصدد أن توسيع نطاق الحق في محو البيانات يعزز كثيراً الحق في النسيان في بيئة الإنترنت على النحو الذي سنعرض له عند التطرق للحديث عن النسيان الرقمي من خلال السماح بحذف أية ارتباطات قد تؤدي إلى نسخ أو تكرار هذه البيانات الشخصية مع مراعاة التكنولوجيا المتاحة والوسائل المتاحة للقائم بعملية المعالجة.

ونص المشرع الأوروبي على هذا الالتزام إذا توافرت حالة من الحالات التي نصت عليها المادة السابعة عشر من اللائحة الأوروبية، وأهمها:

١- إذ لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي جمعت من أجلها أو تمت معالجتها بطريقة أخرى غير تلك المتفق عليها.
٢- في حالة عدم وجود سبب قانوني للمعالجة فإنه يحق للشخص المعني سحب الموافقة التي تستند إليها عمليات المعالجة وفقاً للفقرة (أ) من المادة السادسة، أو الفقرة (أ) من المادة التاسعة.
٣- في حالة معالجة البيانات الشخصية بصورة غير قانونية سواءً فيما يخص شرعية الإجراء أو مشروعية المضمون.
٤- في حال قيام المُعالج بجعل البيانات الشخصية علنية، فإنه يكون ملزماً بموجب الفقرة الأولى بمحو البيانات الشخصية وعليه أن يتخذ اللازم بشكل عاجل، آخذاً في الاعتبار التكنولوجيا المتاحة وتكلفة اتخاذ التدابير التقنية اللازمة، والخطوات المطلوبة لإبلاغ المراقبين

الذين يعالجون البيانات الشخصية أن الشخص المعني صاحب البيانات طلب محو أي صلات أو روابط تخص بياناته الشخصية.

ويتعين على القائم بعملية المعالجة محو البيانات الشخصية والامتثال لرغبة الشخص المعني حفاظاً على خصوصيته، مع أننا نرى أنه يتوجب أن يكون هناك نص قانوني يلزم الشخص المعني بذلك، وفي حال مخالفته تترتب مسؤوليته قانوناً.

ويرد على ما سبق استثناءات تتعلق بعدم الاستجابة في حالة ما إذا كان الاحتفاظ بالبيانات ضرورياً، كأن يكون امتثالاً لالتزام قانوني بموجب قانون الدولة التي ينتمي إليها الشخص المعني أو لأداء مهمة يضطلع بها للصالح العام أو لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة وفقاً للفقرات (ح) و (ط) من المادة (٩/ ٢) وكذلك المادة (٩/ ٣)، أو لأغراض الحفظ من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية وفقاً للمادة (٨٩/ ١).

ويمكن تعليل تقييد حق الشخص المعني وتعطيله بموجب الاستثناءات السابقة، بأن إعطاء الشخص المعني الحق في المحو في الحالات آنفة الذكر يستحيل معه تحقيق أهداف تلك المعالجة أو على الأقل من شأنه أن يعرقل ذلك بشكل يؤثر على الهدف الأولى والأسمى والذي قد يرتبط غالباً بتحقيق مصلحة عامة.

الفصل الثالث:
الإشكالات القانونية التي يثيرها معالجة البيانات الشخصية في ضوء أحكام اللائحة الأوروبية الجديدة ٦٧٩/ ٢٠١٦

تمهيد وتقسيم

تتعدد الإشكالات القانونية التي تثيرها عملية معالجة البيانات الشخصية بتعدد المراحل التي تمر بها هذه البيانات. فهناك إشكالية أمن البيانات الشخصية والتي تعتبر من الإشكاليات التي ما زالت تحتاج إلى معالجة فنية وقانونية. وكما رأينا، فإن البيانات الشخصية قد يتم تخزينها لدى القائم بعملية المعالجة لأغراض إعلانية وهو أمر من قد يشكل انتهاكاً لخصوصية صاحبها. أما نقل هذه البيانات لطرف ثالث سواءً كان شخصاً طبيعياً أو اعتبارياً أو أرشفة هذه البيانات لأغراض تخص المصلحة العامة، أو لغرض البحث العلمي أو التاريخي أو لأغراض إحصائية، فإنه يثير مشكلة حق الشخص في النسيان الرقمي ومدى حقه في المطالبة بحذف هذه البيانات نهائياً. وترتيباً على ما سبق فإننا سوف نقسم هذا الفصل على النحو التالي:

- المبحث الأول: أمن البيانات الشخصية.
- المبحث الثاني: الحق في حذف البيانات (النسيان الرقمي) والعلاقة مع الأرشفة للمصلحة العامة.
- المبحث الثالث: معالجة البيانات الشخصية لأغراض إعلانية أو لأغراض البحث العلمي.
- المبحث الرابع: معالجة البيانات في سياق علاقات العمل.
- المبحث الخامس: المسؤولية والتعويض.

المبحث الأول: أمن وسرية البيانات الشخصية

يُعد أمن البيانات الشخصية من أبرز الأمور التي تثير إشكاليات قانونية في هذا الخصوص؛ لذا يجب أن تستوفي جميع العمليات والنظم الجديدة (بما في ذلك البرمجيات والمعدات التي يتم إدخالها في عمليات المعالجة) السرية والحماية الكاملة. لكن الأمر يزداد تعقيداً يوماً بعد يوم في ظل تنامي وتزايد ظاهرة قرصنة المعلومات أو البيانات؛ الأمر الذي يزيد من صعوبة تصدي المشرع لمعالجة مثل هذه المسألة في ضوء التطورات المستحدثة بشكل كبير في هذا المجال.

ويعرف الفقه[٧٤] أمن المعلومات بصفة عامة من زاوية أكاديمية، بأنه العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات والبيانات من أنشطة الاعتداء عليها والمخاطر التي تهددها. ومن زاوية تقنية بأنه الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار

(٧٤) عبدالفتاح بيومي حجازي، *حماية المستهلك عبر شبكة الإنترنت*. مصر: دار الكتب القانونية، (٢٠٠٨م)، ص ٧٧. وانظر كذلك ماء العينين سعداني، الأمن القانوني والمعلوماتي. *مجلة الفقه والقانون*، المغرب، ع (١٩)، (مايو ٢٠١٤م)، ص ٢٦٠ وما بعدها. وراجع أيضاً عبدالصبور عبدالقوي علي، *التنظيم القانوني للتجارة الإلكترونية*. الرياض: مكتبة القانون، (٢٠١٣م)، ص ٢٩٤ وما بعدها.

الداخلية والخارجية. ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية، وسلامة محتوى، وتوفير المعلومات، ومكافحة أنشطة الاعتداء عليها، أو استغلالها.

وعلى الرغم من أن اصطلاح أمن المعلومات وإن كان استخداماً قديماً سابقاً لظهور وسائل تكنولوجيا المعلومات، إلا أنه وجد استخدامه الشائع بل والفعلي في نطاق أنشطة معالجة ونقل البيانات بواسطة مقدمي خدمات التواصل الاجتماعي والحوسبة السحابية والاتصال، بل ربما أمسى أحد الهواجس التي تؤرق الجميع دولاً وأفراداً[٧٥]. ومن المُلاحظ أن التعريف الأخير هو الذي يعنينا في هذا المقام، وفي ضوء ما جاءت به اللائحة الأوروبية والذي قام بتنظيم هذه الإشكالية في المواد الثانية والثلاثون[٧٦]، والثالثة والثلاثون[٧٧]، والرابعة والثلاثون[٧٨]؛ وذلك في محاولة منها لمجاراة هذا التطور المتسارع والمتلاحق في تكنولوجيا المعلومات.

(٧٥) ممدوح شحات الصقر، أمن المعلومات. *أعمال ندوة مكافحة الجريمة عبر الإنترنت، وورشة عمل أمن المعلومات والتوقيع الإلكتروني، المنظمة العربية للتنمية الإدارية*، القاهرة، (٢٠١٠م)، محكمة، ص ص ١٤٣-١٨٠، ص ١٥٥.

(76) **Article 32 : Sécurité du traitement:** 1.Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique = agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

(77) **Article 33 : Notification à l'autorité de contrôle d'une violation de données à caractère personnel:**

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins:

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

(78) **Article 34 : Communication à la personne concernée d'une violation de données à caractère personnel:**

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

والناظر في السياسة التشريعية التي تبناها المشرع الأوروبي في اللائحة الجديدة يجد أنه كان شديد الحرص في التعامل مع هذه المسألة في ضوء التطورات الحاصلة في ها المجال، ويظهر ذلك من خلال تقنين ما يعرف بإعدادات الأمن والخصوصية للمستخدم، والتي تم وضعها في ضوء أنها لا تحمي المستخدم إلا من بقية الأعضاء في الشبكة الاجتماعية أو الموقع، ولكنها لا تمنع بياناته عن مالك الخدمة؛ فالمستخدم يسلم بياناته للموقع أو الشبكة الاجتماعية ويأتمنهم عليها، ومن هنا نجد أن المشرع الأوروبي قد راعى هذه المسألة فقام بتخصيص نص المادة الثانية والثلاثون لـ "أمن المعلومات" بقوله: "مع مراعاة الحالة المعرفية وتكاليف التنفيذ وطبيعة المعاملة والمخاطر ونطاقها وسياقها وأغراضها، وتفاوت درجه احتمالها وشدتها، وبالنسبة لحقوق الأشخاص الطبيعيين وحرياتهم يقوم المتحكم والمتعاقد من الباطن بتنفيذ التدابير التقنية والتنظيمية المناسبة من أجل ضمان مستوى معين من السلامة يتناسب مع المخاطر – بما في ذلك جملة أمور – أهمها:

(أ) الأسماء المستعارة وتشفير البيانات الشخصية.

(ب) وسائل ضمان السرية المستمرة لنظم المعالجة وضمان سلامتها.

(ج) وسائل استعادة البيانات الشخصية والوصول إليها في حدود الوقت المناسب في حالة وقوع حادث مادي أو تقني.

(د) إجراء اختبار للتأكد من فعالية التدابير التقنية والتنظيمية وتحليلها وتقييمها بانتظام لضمان سلامة البيانات".

ويتضح من استعراض النص السابق أن المشرع الأوروبي قد راعى التطور الهائل في تقنية المعلومات؛ مما يظهر أنها أصبحت المحرك الرئيس لكثير من التحولات الاقتصادية والاجتماعية في المجتمعات بشكل عام.

كما يتضح أيضاً سعي المشرع الأوروبي لإيجاد نوع من التكامل بين بنية المعلومات والأجهزة والحماية لتلك البيانات وذلك بوضعه نظاماً متكاملاً لأمن وحماية المعلومات من خلال توفير أدوات حماية تقنية، والإجراءات الواجب اتباعها من قبل الدول المعنية من خلال توفير البناء القانوني الملائم لتنظيم حماية البيانات الشخصية، وفي سبيل تحقيق ذلك جاء نص الفقرة الأولى من المادة السابقة بالنص على عدة وسائل لتعزيز الأمن والسلامة ولعل أبرزها ما يلي.

١ – تشفير البيانات والأسماء المستعارة

يُعد التشفير أهم وسائل حماية سلامة البيانات خاصةً في المراحل التي يقوم فيها القائم بالمعالجة بنقل البيانات أو تبادلها مع آخرين. ويعرف التشفير بأنه "منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونياً بحيث تمنع من الحصول هذه البيانات والمعلومات إلا عن طريق مفتاح فك التشفير"(٧٩).

أما عن الأسماء المستعارة فهي من الظواهر التي تستلفت الأنظار لدى الدارسين والباحثين، وتكاد تكون سمة من سمات عالم التكنولوجيا المعاصرة وموقفاً جديراً بالدراسة والتأمل خاصةً في ظل نص اللائحة الأوروبية عليها.

وسعياً من المشرع الأوروبي في إماطة اللثام عن غوامض التطور في مجال قرصنة المعلومات، وإسباغ المشروعية القانونية عليها فقد نص على استخدامها كوسيلة لحماية البيانات الشخصية. ويقصد بها في هذا المضمار قيام الشخص المعني أو المستخدم بتسجيل بياناته لدى المواقع أو وسائل التواصل

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

(٧٩) محسن عبدالحميد البيه، *الإثبات في المواد المدنية والتجارية، وفقاً لقانون الإثبات وقانون التوقيع الإلكتروني*. كتاب مقرر على طلاب كلية الحقوق، جامعة المنصورة، (٢٠٠٧م)، ص ٢١٥ وما بعدها.

الاجتماعي على سبيل المثال ببيانات لا علاقة لها بشخصيته الحقيقية، ولا تحمل أسماء أصحابها صريحة، مستعيضين عن ذلك بأسماء مستعارة (pseudonyms) ارتضوها لأنفسهم ووضعوها كاسم على حساباتهم الشخصية.

وتهدف هاتان الوسيلتان إلى حماية البيانات الشخصية من مخاطر الاختراق المعلوماتي[٨٠] بتوفير الحماية اللازمة ومنع الوصول غير المشروع إليها، ويمكن تحقيق ذلك عن طريق وسيلتين:

- الأولى: تتمثل في تنظيم استدامة تكنولوجيا تشفير المعلومات التي تنقل عبر الإنترنت بحيث لا يستطيع فهمها أو قراءتها سوى من القائم بعملية المعالجة أيا كانت صفته.
- الثانية: وضع نظام موثوق لنقل البيانات لطرف ثالث بشكل يمنع من التعديل عليها أو إعادة نقلها مرة أخرى.

ويستفاد مما سبق أن تشفير البيانات الشخصية يقوم على عدة مبادئ يجب التنويه إليها على النحو التالي.

الأول: إباحة المشرع الأوروبي تأمين البيانات والمعلومات الشخصية وتشفيرها[٨١]

أباح المشرع الأوروبي تشفير البيانات والمعلومات الشخصية التي يتم تخزينها أو معالجتها؛ وذلك كأسلوب يحقق تأمين هذه البيانات وتلك المعلومات وبالتالي حماية المستخدم أو الشخص المعني من انتهاك خصوصيته.

وبطبيعة الحال فإن المشرع الأوروبي ترك تحديد القواعد الخاصة بتأمين البيانات والمعلومات التي يتم تخزينها أو معالجتها وكذلك تشفير التوقيع الإلكتروني لقوانين دول الاتحاد وحسب ما توصلت إليه علوم التقنية في هذا المجال.

الثاني: الرقابة الصارمة على عمليات تأمين البيانات وتشفيرها

يخضع تأمين البيانات لرقابة صارمة ومشددة في كافة الدول وليس على مستوى دول الاتحاد الأوروبي فقط هذا بشكل عام. وقد ترك المشرع الأوروبي تنظيم عملية التشفير والقواعد المتعلقة باستخدامه والبرامج التي تستخدم لإتمامه للقائم بعملية المعالجة في ضوء الحدود المسموح بها قانوناً، وعند مستوى معين؛ حتى لا يحول استخدام التشفير دون قيام الأجهزة الأمنية بدورها في حماية المصالح العليا للدولة، ولعمل نوع من المواءمة بين حماية الخصوصية الشخصية من ناحية وبين متطلبات تحقيق السلامة العامة والأمن القومي من ناحية أخرى[٨٢].

الثالث: الحرص على سلامة وسرية البيانات والمعلومات الشخصية

يقصد بهذا المبدأ احترام سرية البيانات المشفرة والالتزام بحق أصحاب هذه البيانات والمعلومات الشخصية في الخصوصية. وقد راعى المشرع الأوروبي من خلال نص الفقرة الثالثة خضوع عمليات التشفير واستخدام الأسماء المستعارة لمدونة السلوك المعتمدة بقوله: "يجوز أن يكون تطبيق مدونة قواعد السلوك المعتمدة، على النحو المنصوص عليه في المادة الأربعين أو آليات التصديق المعتمدة على النحو المنصوص عليه في المادة الثانية والأربعون، بمثابة عنصر إثبات الامتثال لمقتضيات الفقرة الأولى من هذه المادة".

وقد اهتم المشرع الأوروبي بسلامة وسرية البيانات الشخصية المشفرة، ومنع الاعتداء عليها أو إفشاءها أو معالجتها بطرق أخرى أو نقلها إلا بموافقة صاحبها أو بأمر من القضاء. وفي ذلك تنص الفقرة الثانية من ذات المادة على أن "عند تقييم المستوى المناسب من السلامة يراعى بصفة خاصة المخاطر التي تنطوي عليها المعاملة، والتي تؤدي في المجمل إلى تدمير البيانات الشخصية وفقدانها وتعديلها وإفشاءها بدون إذن لنقل هذه البيانات أو حفظها أو معالجتها بطريقة أخرى، أو الوصول إليها بدون إذن، إما بطريق الخطأ أو بصورة غير مشروعة".

ويتضح مما سبق أن القائم بعملية معالجة البيانات الشخصية يلتزم بأن يكفل سلامة البيانات الشخصية، بما في ذلك التزامه بعدم قيام أي شخص طبيعي يعمل لديه بالاطلاع على البيانات الشخصية ويشمل ذلك أيضاً المتعاقد من الباطن الذي تم نقل نسخة البيانات إليه دون موافقة الشخص المعني.

(٨٠) نفس الإشارة السابقة.

(81) LES GUIDES DE LA CNIL - ÉDITION 2018: LA SÉCURITÉ DES DONNÉES PERSONNELLES; Disponible sur le lien: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

(82) Ibid.

الرابع: قانونية عملية تأمين البيانات والمعلومات

وتتضح أهمية عملية التشفير إذا ما علمنا أن أي نظام لمعالجة البيانات الشخصية قد يتفاعل مع الأفراد؛ لذا يجب أن تكون هناك سياسة لضبط وتحديد طريقة التعامل مع هذا النظام، ويتم ذلك عن طريق وسائل وطرق تضمن تحقيق الدرجة المطلوبة من تأمين بيانات النظام وتشمل تلك الوسائل تحديد حق كل مستخدم للنظام من الوصول إلى البيانات وتحديد الجزء الذي يمكنه التعامل معه والقيام بالمعالجة المطلوبة.

ويجب الإشارة هنا إلى أن بناء نظم كاملة لتأمين البيانات والمعلومات قد يبلغ من الصعوبة بمكان تحقيقه في ظل تطور وسائل الاختراق بشكل عام، أو لأن الواقع قد حتم علينا الاكتفاء بدرجة عالية من التأمين لمختلف مراحل النظام، وحيث إن معظم أنظمة المعالجة اليوم يديرها برامج ونظم حاسبات إلكترونية؛ لذا نجد أن تلك البرامج هي الوسيط الأمثل لتطبيق السلامة والأمن لحماية البيانات.

ومما تجدر الإشارة إليه أيضاً في هذا المقام أن ضوابط الأمن القانونية للبيانات والمعلومات الشخصية ترتكز على عدد من العوامل التي يجب تحديدها والتي تتمثل غالباً في الإجراءات القانونية الواجب اتخاذها ضد من يحاول اختراق نظام المعلومات بهدف الحصول على بيانات المستخدمين دون وجه حق هذا من ناحية، ومن ناحية ثانية: الإجراءات القانونية الواجب اتخاذها ضد من يسيء استخدام بيانات حصل عليها بحكم عمله. ومن ناحية ثالثة: الضوابط القانونية الواجب تنفيذها بهدف حماية الأفراد الموجودة بياناتهم الشخصية في نظم المعلومات المعالجة آلياً. ومن ناحية رابعة: الضوابط القانونية التي تنظم إمكانية تبادل البيانات الشخصية الخاصة بالمستخدمين بين الجهات المختلفة. ومن ناحية خامسة: حقوق المستخدم في الاطلاع وتصحيح المعلومات الخاصة به والمسجلة في ملفات قواعد البيانات، ومن ناحية سادسة: الوسائل المعترف بها قانونياً التي تثبت حالة محاولة اختراق النظام[٨٣].

(83) Ibid.

وأخيراً، فبالإضافة لذلك كله يستدعي حماية البيانات والمعلومات الشخصية المنقولة عبر شبكات الاتصال قدراً أكبر من الاهتمام لتأمينها حيث إنها تتعرض لعدد كبير جداً من المستخدمين، وتمر عبر أماكن ونقاط كثيرة يمكن عند أي نقطة منها التلاعب بها أو العدوان عليها بأي صورة من الصور[٨٤].

المبحث الثاني: حق الإنسان في أن تُمحى بياناته (الحق في النسيان الرقمي) والعلاقة مع الأرشفة للمصلحة العامة

Droit à l'effacement («droit à l'oubli»)[٨٥]

قد يرى الشخص المعني الذي وافق مسبقاً على معالجة بياناته مع مرور الوقت، أن استمرار وجود هذه البيانات أصبح ضاراً بمصالحه، أو أنه لم يعد هناك ضرورة لبقاء هذه البيانات، فمن حقه إذن المطالبة بالحق في النسيان. أضف لذلك هناك حالات تقتضي الإبقاء على هذه البيانات من أهمها أرشفة البيانات للمصلحة العامة، وهو ما يقتضي التعرض لحق الإنسان في أن تُمحى بياناته (أولاً)، والعلاقة مع الأرشفة للمصلحة العامة (ثانياً)[٨٦].

(84) Ibid.

(٨٥) يشير جانب من الفقه الفرنسي إلى نشأة هذا الحق بقوله:

"La notion de « droit à l'oubli » a émergé en doctrine, pour la première fois, dans une note relative à l'affaire Landru de 1965 où le professeur Gérard Lyon-Caen l'invoque comme fondement juridique possible d'une action intentée par une des maîtresses de Landru, qui demandait alors réparation du dommage que lui aurait causé un film de Claude Chabrol relatant cette ancienne liaison. Le juge a alors évoqué une "prescription du silence", pour finalement rejeter la demande au motif que la requérante avait elle même publié ses mémoires. Cette notion de « prescription du silence », laissant planer la dérive d'une appréciation au cas par cas justifiée par des intérêts en cause, a légitimement été écartée, au profit de l'entrée définitive de la notion de droit à l'oubli en droit positif. Ainsi, lors de la décision dite Madame M. c. Filipacchi et Cogedipresse de 1983, le TGI de Paris s'est appliqué à consacrer une nouvelle liberté publique." Charlotte HEYLLIARD: Le droit à l'oubli sur Internet. Mémoire de Master 2 recherche, Mention DNP. le 4 juin 2012; p.9; Voir aussi: 5 TGI Seine, 14 octobre 1965, Mme S. c. Soc. Rome Paris Film, JCP 1966 I 14482, n. Lyon-Caen, confirmé en appel, CA Paris 15 mars 1967 6 TGI Paris, 20 avril 1983, JCP., 1983.II.20434, obs. R. Lindon.

(٨٦) نفس الإشارة السابقة.

أولاً: الحق في النسيان الرقمي

في الواقع، أنه إذا كانت التكنولوجيات الجديدة تتيح فرصاً جديدة لمكافحة انعدام الأمن[٨٧] فإنه يجب إعطاء الشخص المعني الحق في أن تُمحى البيانات المتعلقة به في أقرب وقت ممكن، وعلى القائم بعملية المعالجة الالتزام بمحو البيانات الشخصية في أقرب وقت ممكن من تحقق سبب المحو أو بناءً على طلب الشخص المعني ذلك.

ويتم هذا الأمر في حالات عديدة على سبيل المثال نذكر منها تلك الحالة التي لم يعد فيها للبيانات الشخصية ضرورة بالنظر إلى الأغراض التي جمعت من أجلها أو تلك التي تمت معالجتها بطريقة أخرى لم يتم الاتفاق عليها، أو أن يقوم الشخص المعني بسحب موافقته على عملية المعالجة، بالإضافة لعدم وجود أساس قانوني آخر تتم المعالجة وفقاً له.

وقد عبر Christian Charriere-Bournazel عن هذا الحق بقوله أن "الذاكرة الزائلة للورقة استبدلت بذاكرة غير قابلة للتغيير، وأن العالمية لم تترك أي فرصة للنسيان"[٨٨].

والحق في النسيان الرقمي أو ما يعرف بحق الشخص في أن تُمحى بياناته هو المشكلة الأساسية للخصوصية، فمع ظهور التكنولوجيات الجديدة وانتشار الشبكات الاجتماعية في حياتنا، يبدو أن الحق في النسيان أصبح بطبيعة الحال مبدأً أساسياً في تقرير ترك المعلومات والبيانات على شبكة الإنترنت من عدمه[٨٩].

ويشير جانب من الفقه المصري[٩٠] إلى "أنه على الرغم من الارتباط الوثيق بين الحق في النسيان الرقمي والخصوصية، إلا أن هذا لا يعني حتمية التلازم بينهما، ومن ثم تظهر أهمية الاعتراف بالحق في النسيان كحق مستقل عن الحق في الخصوصية من جهتين: الأولى أن الوقائع والبيانات والتي سبق نشرها قد انتفت عنها صفة الخصوصية، وبالتالي فإن إعادة نشرها بغير رضاء صاحبها لا يعد انتهاكاً لخصوصيته، بل هو انتهاك لحقه في النسيان؛ إذ يتعلق الأمر حينئذ بوقائع – وإن وقعت علانية – إلا أنها تقادمت، ومن ثم فلا يجوز إثارتها مجدداً إلا بإذن من تتعلق به هذه الوقائع. والثانية أن اعتبارات المصلحة العامة قد تقتضي الكشف عن بيانات تتعلق بخصوصية بعض الأشخاص، كما هو الحال بالنسبة للشخصيات العامة متى ارتبطت هذه البيانات بوقائع عامة، ففي مثل هذه الحالة لا يمكن حماية هذه البيانات على أساس حماية الخصوصية بل على أساس حماية الحق في النسيان. وبمفهوم المخالفة فلو تعلقت هذه البيانات بالحياة الخاصة للشخص فإن حمايتها تكون على أساس حماية الخصوصية باعتبار أن الحق في النسيان في هذا الفرض هو عنصر من عناصر الحق في الخصوصية".

وقبل أن نحدد العلاقة بين حق الشخص في أن تُمحى بياناته تلقائياً (الحق في النسيان) ومسألة الخصوصية يجدر بنا أن نوضح بشكل أكثر دقة مفهوم الحق في النسيان الرقمي.

في الواقع، إذا كان الحق في النسيان بمعناه الأول هو بالأحرى فرصة "الخلاص" المتعلقة بالمساس ببعض عناصر الحياة الخاصة للفرد؛ فإن هذا الحق يؤدي بحثه إلى دراسة تسارع التقدم التكنولوجي.

وما من شك في أن العالم يشهد تسارعاً في التقدم التكنولوجي غير مسبوق وسريع للغاية. فالإنترنت فضاء تتسارع وسائله وأشكال المشاركة فيه باستمرار، كما أن الابتكارات الحديثة مثل "الحوسبة السحابية" أدت إلى تزايد كم المعلومات في هذا الفضاء الواسع؛ خاصة في ظل الوصول

(87) Commission des lois du Senat ; « Vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », Rapport d'information de M. Yves DÉTRAIGNE et Mme AnneMarie ESCOFFIER, fait au nom de la commission des lois, n° 441 (2008-2009), 27 mai 2009, adoptée le 23 mars 2010. Disponible sur le site Web suivant https://www.senat.fr/notice-rapport/2008/r08-441-notice.html

(88) A la mémoire éphémère du papier s'est substituée une mémoire inaltérable et universelle qui ne laisse aucune chance à l'oubli », Christian Charriere-Bournazel, « Propos autour d'Internet : l'histoire et l'oubli », Gazette du Palais, 21 avril 2011 n°111, p.6 Gazette du Palais, 21 avril 2011. Voir aussi Agathe Lepage, «Droit à l'oubli : une Jurisprudence tâtonnante », Recueil Dalloz 2001, p. 2079.

(89) Théo Hassler, « Droits de la personnalité : rediffusion et droit à l'oubli », Recueil Dalloz 2007 p.2829

(٩٠) أشرف جابر سيد، *الجوانب القانونية لمواقع التواصل الاجتماعي: مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتويتر*. مرجع سابق الإشارة إليه، ص ص ٦٦-٦٧

الفوري والمتزايد إلى العالم الافتراضي، وتسهيل الوصول إليها من قبل نظم الاتصالات المتعددة أبرزها الهواتف الذكية. وعلى الرغم من أن جميع هذه الوسائل تهدف إلى تحقيق سهولة في الاستخدام إلا أنها تنطوي على مخاطر أبرزها يتعلق بانتهاكات صارخة للحق في الخصوصية[٩١].

ومن جانبنا، نتفق مع الرأي السابق في أنه يجب احترام الحق في نسيان ما يرغب المرء في نسيانه. ولكن إذا اعتبرنا أن القوانين الحالية لا توفر ضمانات كافية للحفاظ على الحقوق والحريات الأساسية للفرد في هذا الفضاء الافتراضي، فهنا يثور تساؤل مفاده هل نحن بحاجة إلى رؤية لينة، أو فكرة موحدة من شأنها أن تكون معياراً لتقييم احترام حقوق الإنسان الأساسية؟ وهل من المناسب المضي إلى أبعد من ذلك بتقنين الحق في النسيان بالاتفاق حول تلبية رغبة الكثير من الفقه الفرنسي[٩٢] والفقه العربي[٩٣] الذي يرغب في رؤية حق مستقل جديد يظهر على الساحة القانونية؟

ومن أجل الإجابة على هذه الأسئلة من المهم توضيح ثلاثة مفاهيم هي: النسيان، والنسيان الرقمي، والحق في النسيان.

أما مفهوم النسيان[٩٤] فمن ناحية أولى، هو متلازمة تتسم بحدوث تدهور في الذاكرة والتفكير والسلوك والقدرة على الاضطلاع بالأنشطة اليومية. وعلى الرغم من أنّ النسيان يصيب المسنين بالدرجة الأولى فإنّه لا يُعتبر جزءاً طبيعياً من الشيخوخة[٩٥]. كما أن النسيان من أهمّ الأسباب التي تؤدي إلى إصابة المسنين بالعجز وفقدانهم استقلاليتهم في كل أنحاء العالم. فهو يخلّف النسيان آثاراً جسدية ونفسية واجتماعية واقتصادية على من يقومون برعاية المرضى وعلى أسرهم بشكل خاص والمجتمع بشكل عام؛ فهو فشل الذاكرة، وهو بهذا المعنى، يعد نقطة ضعف؛ لأنه يمنع الفرد من التذكر، وبالتالي يعد عقبة لحفظ المعرفة، والأكثر من ذلك، يعتبر النسيان عقبة أمام ممارسة واجب الذاكرة اللازم لعدم تكرار أخطاء الماضي.

والنسيان هو شكل من أشكال الانحطاط العصبي، ينتج عن الأمراض العصبية التي تؤدي إلى فقدان وظائف الذاكرة تدريجياً (وهذا هو الحال مع مرض الزهايمر، على سبيل المثال).

ومن ناحية أخرى، فإن النسيان له منظور إيجابي هو إرادة وقدرة الفرد على إبعاد بعض الأحداث من ذاكرته، فالنسيان هنا له وظيفة بناءة وصالحة يحتاجها الفرد. على سبيل المثال، الوقت يخفف من الألم؛ لأن مرور الوقت يسمح للنسيان بلعب دور مهم في تخفيف ما قد يؤثر سلباً على الصحة العامة للفرد. وهذا المفهوم مدعوم من قبل الفيلسوف نيتشه، الذي يرى أن النسيان هو "الكلية النشطة المسؤولة عن الحفاظ على النظام الروحاني للإنسان"[٩٦].

(91) Théo Hassler, «Droits de la personnalité : rediffusion et droit à l'oubli », Recueil Dalloz 200, op.cit. 2829 voir aussi " Commission des lois du Senat ; « Vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », Rapport d'information de M. Yves DÉTRAIGNE et Mme Anne Marie ESCOFFIER, fait au nom de la commission des lois, n° 441 (2008-2009), 27 mai 2009, adoptée le 23 mars 2010.

(92) Ibid.

(93) Ibid.

(٩٤) تجدر الإشارة إلى أن أجزاء الدماغ المؤثرة على ظاهرة الذاكرة والنسيان، تتمثل بالممرات السائدة على طول المنطقة نظيرة الحصينية الوسطى وقن أمون والفصوص الصدغية الوسطى السفلى والسطح الحجاجي للفص الأمامي والدماغ المتوسط أو سرير المخ. وتلعب التلافيف الحصينية، وتحت المهاد، ونواة قاعدة الدماغ الأمامي ومنتف المهاد الظهري الوسطاني، دوراً مهماً في الذاكرة. كما تؤثر النواة اللوزية على مدى اتساع نطاق الذاكرة. ولما بين الصفائح المهادية دور مهم في توسيع نطاق وتنشيط الذاكرة. وتعمل نواة ما بين الصفائح المهادية والتكوين الشبكي في جذع الدماغ، على تحفيز الانطباع السلوكي للذكريات. للمزيد راجع الرابط التالي:
http://apdfanswer.blogspot.com/2015/02/Amnesia.html

(٩٥) يشير موقع منظمة الصحة العالمية إلى الحقائق التالية حول مرض الخرف الذي يعد النسيان أحد أهم أعراضه، عبر مقال مؤرخ أبريل/ نسيان ٢٠١٦م على الرابط التالي:
http://www.who.int/mediacentre/factsheets/fs362/ar

(٩٦) ينظر الفيلسوف فريدريك نيتشه للنسيان على أنه ظاهرة حيوية: "لا السعادة، لا الصفاء، لا أمل، لا فخر، لا يمكن التمتع بهذه اللحظة الموجودة دون نسيان". للمزيد حول هذا الأمر راجع فريدريك نيتشه، *في جنيالوجيا الأخلاق، المقالة الثانية، الذنب "الضمير المذنب"*. ترجمة: فتحي المسكيني، مراجعة الترجمة: محمد المحجوب، تونس: المركز الوطني للترجمة، (٢٠١٠م)، سلسلة الفلسفة، منشورات دار سيناترا، ص ص ٨٢-٨٣. وانظر أيضاً:
Jacques Le Rider: Oubli, mémoire, histoire dans la « Deuxième Considération inactuelle » p. 207et.s Disponible via le lien suivant: http://journals.openedition.org/rgi/725; Le lien a été visité le 23/02/2018.

أما النسيان الرقمي فقد ظهر وبرز مع ظهور التكنولوجيات الرقمية والحاسوبية، ومر هذا المصطلح بمراحل أربعة على النحو التالي:

- أولاً: كشف التطور عن الجيل الجديد من أساليب معالجة المعلومات، وكافة أنماط الكائنات الرقمية.
- ثانياً: تخزين المعلومات يشكل الآن الصورة الرقمية الأوسع انتشاراً في الوقت الحالي، والوصول إليها يعد أمراً في غاية السهولة بسبب انخفاض كبير في التكلفة، والنتيجة هي زيادة في مساحة التخزين، وبالمقابل زيادة في تكلفة النسيان الرقمي، إلى الحد الذي يختفي معه الغرض من فرز المعلومات[٩٧].
- ثالثاً: تقنيات استرجاع المعلومات، لا غنى عنها في مواجهة وفرة من المعلومات المخزنة، هي الآن في متناول الجميع، وهذا ما نلمسه عند تصفح محركات البحث أو حتى البرمجيات الحاسوبية، وبطبيعة الحال، قد يكون الوصول لبعض المعلومات محدود. ويشمل ذلك بيانات السجلات الجنائية – ومع ذلك – فإنها تظل متاحة لفئات معينة من الناس الذين يضمنون ذاكرتهم[٩٨].
- وأخيراً، رابعاً: العولمة التي فرضتها الشبكات الرقمية الآن، على كافة أنماط الكائنات الرقمية والمعلومات الممسوحة ضوئياً والتي أصبح الوصول إليها يسيراً بواسطة اتصال بسيط عبر الشبكة. كل ذلك يؤكد أنه تحول نموذجي من خلال السماح لظهور ثورة الذاكرة الرقمية ما بين الذاكرة/ النسيان[٩٩].

والسؤال الذي يطرح نفسه بقوة الآن هو هل ينبغي تقنين هذا التغيير؟

بداهة، يمكن القول إن التقنيات التكنولوجية الحديثة، والوصول إلى البيانات الشخصية، في حد ذاتها يشكل تهديداً للإنسان. فمن المناسب إذن أن يكون هناك قدر من الحذر والوعي بعواقب التخزين الرقمي؛ الأمر الذي ينبغي معه اتخاذ وقت معين تراعى فيه قدرات الإنسان في السيطرة الصارمة على الأنشطة الرقمية بعدها يتم السماح للنسيان بطي كل هذه البيانات وحذفها من الشبكة الرقمية.

ومما تجدر الإشارة إليه أنه يتم تخزين الكثير والكثير من المعلومات الموجودة بشكل يومي عن الأفراد عبر شبكة الإنترنت، بل تتفاقم هذه الظاهرة بنمو الإنترنت وتطوره يوماً بعد يوم. وتتفاوت المعلومات المخزنة بطبيعة الحال في أهميتها. فمن الأشخاص من يسمح بإعطاء الإذن في الإفصاح عن هويته عبر تحديد بياناته الشخصية. ولا يزال البعض الآخر متحفظاً ولا يسمح عل الإطلاق بتحديد هويته[١٠٠].

وفي هذا السياق، يخشى الأفراد من انتهاك حرياتهم عند تصفح الإنترنت وترك الآثار الرقمية الناشئة عن هذا التصفح؛ لأن كل المعلومات التي يتم تخزينها بسبب عملية تصفح الشخص لأي موقع لها قيمتها السوقية. وعلى الرغم من أن الكثير من الخدمات المتاحة على شبكة الإنترنت أولاً وقبل كل شيء مجاناً، ولكن تدفع بطريقة أو بأخرى مقدمي خدمات الإنترنت (المواقع، ومحركات البحث، والشبكات الاجتماعية ... إلخ) عبر تمويل هذه الخدمات من خلال إيرادات الإعلانات.

ومن أجل تقديم الإعلانات الأكثر ملاءمة لاهتمامات المستخدم، يتم الحصول على معلومات عن عادات ورغبات مستخدم الإنترنت، هذه المعلومات تصبح "المادة الخام التي يتم معالجتها بشكل يخدم العالم الاقتصادي"[١٠١] عن طريق قيام الشركات الخاصة باستغلال هذه المعلومات لأغراض توجيه الإعلانات المناسبة التي تهم المستخدم. فعلى سبيل المثال يقوم المستخدم أثناء إجرائه عملية شراء عبر موقع التسوق الشهير (Amazon) بتمرير المعلومات على موقع أمازون، وهذا يستدعي وجوب قيام العملاء بإنشاء حساب ويضع كافة البيانات الخاصة به بما في ذلك بيانات الاتصال الشخصي. وبالتالي يحصل المورد على معلومات قيمة تجعله قادراً فيما بعد

(97) Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, (2009), 237 p.

(98) Etienne Quillet : Le droit à l'oubli numérique sur les réseaux sociaux, mémoire, dir. E. Decaux, 2011, p.8.

(99) V.Mayer Schönberger, préc., p.52.

(100) Antoinette Rouvroy : « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? » in La sécurité de l'individu numérisé, Réflexions prospectives et internationales, S. Lacour (dir.), L'Harmattan 2010, p.249s.

(101) Ibid.

على تخصيص عروضه لهم. أو قد يتم الحصول على هذه الاهتمامات من خلال معالجة معلومات تواصل الشخص على مواقع التواصل الاجتماعي مثل فيسبوك أو تويتر، وبالتالي يتحقق حصول المعلن على اهتمامات الشخص ويستطيع عرض السلع أو الخدمات التي يعلم مسبقاً بحاجته لها بطريقة تجعله يُقدم على التعاقد عليها دون تأخير في معظم الأحيان. لكن تدق المشكلة عندما يتعلق الأمر بمعلومات يمكن أن تستخدم ضد الشخص المعني مثل البيانات الخاصة بالرأي السياسي أو الميل الجنسي على سبيل المثال. وهذا هو الحال أيضاً بالنسبة للبيانات التي يمكن أن تكون مصدراً للمعلومات للبنوك، وشركات التامين أو حتى أصحاب العمل ... إلخ(١٠٢).

وبطبيعة الحال، فإن شبكة الإنترنت تعتبر أداة للاتصال وتبادل المعلومات، وبالتالي فهي تتيح للمشغلين الاقتصاديين الذين يستغلونها أن يبنوا تراثاً معلوماتياً ذا قيمة مضافة عالية لا يمكن معه الاعتراف بحق الشخص المعني في النسيان.

وفي هذا السياق من المصالح المتضاربة ينبغي بذل محاولة لتعريف الحق في النسيان. والصعوبة الرئيسية التي تواجه تعريف الحق في النسيان هي تعقيد مفهوم النسيان. فالنسيان هو في الواقع، قبل أي شيء آخر – ظاهرة نفسية طبيعية – ولذلك، فالرغبة في تحديد الحق في النسيان تتبدى في محاولة إعطاء معنى قانوني لفكرة نفسية.

وعلاوة على ذلك، عندما يتوخى القانوني تطبيق الحق في نسيان التكنولوجيات الجديدة – وهو الحق في النسيان الرقمي – فإنه يواجه تناقضاً: فهو يستخدم صكاً قانونياً لتحقيق نتيجة نفسية، ونتيجة لذلك التكنولوجيا مصممة خصيصاً للقتال.

ويمكن تحديد مفهوم الحق في النسيان حالياً بتحديد الغرض الأساسي منه: "استبعاد أي خطر بأن يكون للشخص الذي أودع البيانات الحق في أن تُنسى وتُحذف بياناته بشكل تلقائي بغض النظر عن موافقة هذا المستخدم مسبقاً على معالجتها"، وفي ذات لا يمكن أن ننكر حق القائم المعالجة في استخدام حقه في استغلال البيانات الشخصية في الأغراض التي تمت معالجتها من أجلها بناءً على موافقة صريحة ومستنيرة من المستخدم، ومن أجل التوفيق بين هذين الحقين، ينبغي التأكيد أيضاً على الحق في احترام الخصوصية. لأن للشخص الاحتجاج بالحق في نسيان بياناته على سند أن له امتيازاً يبرر الاحتجاج بهذا الحق.

بيد أن الأمر لا يتعلق بالطرح الكامل للبيانات؛ لأنه حتى لو كان للفرد امتياز على بياناته الشخصية، إلا أنه يظل مديناً بالتزامات تجاه المجتمع الذي ينتمي إليه، وقد يتعارض بالضرورة مع حقوق الأفراد الآخرين. ولذلك، إذا كان الحق في النسيان مكرساً لصالح المستخدم، فإنه لا يمكن أن يكون بشكل أو بطريقة مطلقة أو غير مقننة أو منظمة.

ويبدو هذا النهج القانوني في الواقع مفرطاً في التبسيط ولا يكشف عن البيئة القانونية الكاملة للحق في النسيان، وبالتالي فإن هناك غموضاً واختلافاً حول طبيعة هذا الحق وما ينشأ عنه من إشكالات قانونية.

بصورة أعم، يمكن التأكيد على أن هناك العديد من الآليات القانونية التي لا يشار إليها صراحة بوصفها أدوات للحق في النسيان ولكنها مستوحاة بصورة غير مباشرة تحقيقاً للعدالة؛ لأنها تحمي الأفراد من الإفراط في التدفقات والتجاوزات في استخدام المعلومات وحفظها والتعامل عليها بشكل مطلق ولا نهائي. وبالتالي فإن الحق في النسيان ليس مفهوماً جديداً تماماً من العدم(١٠٣).

وعلاوة على ذلك، فمن الناحية العملية، فقد كان القاضي يجتهد في محاولة إيجاد الأساس القانوني السليم في ضوء قواعد العدالة الذي يستطيع الارتكاز عليه عندما يُطلب منه الاعتراف بالحق في النسيان الرقمي الذي لم يكن مقنناً كما هو الحال في اللائحة الأوروبية الصادرة عام ٢١٠٦م؛ لأنه لا يمكنه رفض البت في النزاع بحجة أنه ليس له أساس قانوني كاف، وإلا اعتبر مرتكباً لجريمة إنكار العدالة.

(102) Ibid.

(١٠٣) "سيكون المرء تحت أنوف بعض الاقتصاديين، مثل الوشاح الأحمر أمام أعين الثور" تعبير استخدمته Maryline Boizard في بحثها "LE DROIT A L'OUBLI":

Maryline Boizard: LE DROIT A L'OUBLI E DROIT A L'OUBLI ; Faculté de droit et de science politique, Rennes 1 Institut de l'Ouest : Droit et Europe IODE UMR CNRS 6262 Recherche réalisée avec le soutien de la Mission de recherche Droit et Justice Février 2015 ; p.17

ومع ذلك، فإن الحق في النسيان الرقمي والتصور الذي لدينا اليوم يجب أن يتم تفسيره على نطاق واسع؛ لأنه من الواضح تماماً أن تطوير تقنيات الاتصال ونشر المعلومات عبر الإنترنت – لاسيما نمو الشبكات الاجتماعية – يعطي إشكالية الحق في النسيان بعداً واسعاً.

ومع ذلك، فإن تعريفها خضع من الجانب الفقه الفرنسي لتفسيرات عديدة مختلفة، فهناك تفسير يرى أنه يجب أن تمحى من تلقاء نفسها دون طلب من الشخص المعني[١٠٤]، واتجاه آخر يرى أنها تأتي في سياق "الحق في الخصوصية"، ومن ثم فإن الحق في النسيان سيكون نتيجة للحق في الخصوصية[١٠٥]. وتفسير ثالث يقرر أن الحق في النسيان أقرب إلى "الحق في تقرير المصير المعلوماتي"[١٠٦]. وهنا سيكون الأمر متعلقاً بتخويل الشخص سلطة البت في مدى إمكانية معالجة المعلومات المتعلقة به والإبلاغ عنها والاحتفاظ بها، عقب انتهاء الغرض من المعالجة الأولى التي وافق عليها، أو انتهاء المدة التي سمح بها في موافقته الأولى. وبالتالي ووفقاً لهذا الاتجاه فإن الحق في النسيان سيكون بالتالي هو الحق في أن يقرر بنفسه ما هي المعلومات المتعلقة به التي يجب أن تقع في طي "النسيان".

ومن وجهة نظرنا، يبدو أن الحق في النسيان الرقمي يختلف عن "الحق في تقرير المصير المعلوماتي"، الذي ينطوي في الواقع على إتقان عام للمعرفة به. والواقع أن الحق في النسيان بالمعنى الدقيق، لا يشير سوى إلى اختفاء الذكرى ومن ثم السيطرة على "النسيان".

ويبدو أن تنوع هذا النهج واختلاف الرؤى حول هذا الحق يُعزى إلى غموض مصطلح "الحق في النسيان" في حد ذاته. والسبب في ذلك أن النسيان يشمل أمرين منفصلين تماماً. الأول يخص النسيان كحقيقة نفسية (اختفاء الذكرى)، وعلى الجانب الآخر يخص الحقيقة الملموسة التي يجب أن نستوعبها وهي (اختفاء المعلومات من على الشبكة الرقمية).

وعلى ذلك يمكن تحديد طبيعة الحق في النسيان بأنه حذف المعلومات مباشرة من "الذاكرة الرقمية"، أي المعلومات المتعلقة بشخص محدد يمكن التعرف عليه، والتي يتم الاحتفاظ بها في الذاكرة الرقمية.

أما الغرض من الحق في النسيان الرقمي يتمثل في حماية الشخص المعني من عدم المساس به بسبب معلومات تخص ماضيه، على أساس أن الفرد يتمتع بسلطة تتمثل في أن يكون للفرد الحق في وجود أو اختفاء المعلومات المتعلقة به. وبالتالي فإن من حق مستخدمي الإنترنت اختفاء "ذكرياته الرقمية وبيانات التصفح وسائر أنماط الكائنات الرقمية من على شبكات ومواقع الإنترنت".

وفي هذا المقام يمكن أن نطرح سؤالاً حول الأهمية التي يكتسبها هذا الحق من خلال الخدمات التي تُقدم عبر شبكات التواصل الاجتماعي (services de réseautage social) وتتمثل الإجابة في أن تلك الأهمية تظهر من خلال تطبيق القواعد الحاكمة والمنظمة لـ "الحق في النسيان الرقمي" والتي تبرز في جميع الأماكن التي يتوفر لها الاتصال بشبكة الإنترنت.

والشبكات الاجتماعية اليوم هي واحدة من أهم هذه الأماكن، والابتكارات الأكثر تميزاً على شبكة الإنترنت، وقد تطورت بسرعة فائقة في السنوات الأخيرة، سواءً بظهور شبكات جديدة أو بالزيادة الكبيرة في عدد أعضائها. وعرفها الفقه بأنها "منصات اتصال إلكترونية تمكن الناس من إنشاء شبكات من المستخدمين الذين يتقاسمون المصالح المشتركة".

وتكمن خصوصية الحق في النسيان الإلكتروني من خلال بيان الخصائص المشتركة التي تتمتع بها هذه الشبكات وهي أن تتم دعوة المستخدمين إلى تقديم بيانات شخصية لتشكيل "ملف تعريف خاص بكل مشترك"، هذا من ناحية، ومن

(104) A. BELLEIL : E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'Internet, Dunod, 2001, p.11.

(105) Roseline LETTERON « Le droit à l'oubli », Revue du droit public, 1996, T. CV, n°2, p. 32

(106) Ce droit a fait l'objet de nombreux développements, notamment de la part d'Yves POULLET et d'Antoinette ROUVROY, à la suite d'un arrêt venu consacrer ce droit, rendu par la Cour Constitutionnelle fédérale allemande du 15 décembre 1983 (BVGE 65, 1.). Voir également Y. POULLET, J.-M. DINANT, avec la collaboration. de C. de TERWANGNE ET M.-V. PEREZ-ASINARI : «L'autodétermination informationnelle à l'ère de l'Internet », Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004. Disponible via le lien: https://rm.coe.int/16806ae51f

ناحية ثانية فإنها تتيح لأعضائها أدوات تمكنهم من وضع المحتوى الخاص بهم عبر الإنترنت (مثل الصور، والتعليقات، والموسيقى، وأشرطة الفيديو أو وصلات إلى مواقع أخرى ... إلخ). ومن ناحية ثالثة: يوجد تحت تصرف كل عضو أيضاً قائمة بالاتصالات التي تمكنه من أن يتفاعل مع باقي الأعضاء المشتركين بنفس الشبكة. وأخيراً، يتم تمويل الخدمات التي تقدمها الشبكات الاجتماعية من إيرادات الإعلانات على صفحات الويب التي يقوم المستخدمون بالوصول إليها.

فالمعلومات المقدمة من المستخدمين والتي يضعونها بملفات التعريف على حسابهم الشخصي على الشبكة الاجتماعية يتم استهدافها من قبل مختلف المعلنين، وبالتالي يتعمد نجاح الشبكة بشكل كبير على كم المعلومات المقدم من أعضائها. فعن طريق البيانات الشخصية والآراء وبيانات التصفح والبحث تقوم الشبكات الاجتماعية بتقديم ميزات مختلفة، ومتابعة الأهداف، التي يمكن أن يكون لها غرض اجتماعي بحت (Facebook, YouTube, Twitter, Google+, Myspace)[١٠٧].

وفي الواقع نجد أن الشبكات الاجتماعية تعتمد على الحجة القائلة بأن أي عضو يمتلك حساباً على الشبكة، على علم تام بشروط وأحكام النشر واستخدام بياناته الشخصية من خلال "الأحكام والشروط العامة" التي علم بها وقبلها عند قيامه بإتمام عملية التسجيل. بالإضافة إلى أن المستخدم يمكنه، من خلال "إعدادات الخصوصية"، تقييد الوصول إلى المعلومات التي ينشرها على الحساب الخاص به؛ لأنها من الناحية النظرية ممنوعة التسجيل إلا بعد بلوغ الشخص سناً معينة (١٣ عاماً، الحد الأدنى على موقع الفيسبوك على سبيل المثال).

بيد أنه من الناحية العملية، نجد في بعض الأحيان أن البعض لا يقرأ "الشروط العامة للاستخدام" وأنه غالباً ما يتم فتح مشاركة جميع البيانات بشكل افتراضي لكافة المستخدمين والموجودين على الصفحة أو الحساب وهو ما أشارت الدراسات إلى أن سببه يعزى إلى تزايد أعداد المراهقين الصغار جداً الذين لا يبلغون العمر المتطلب قانوناً للتسجيل وإنشاء الحساب في الشبكات الاجتماعية، ويجهلون خطورة مشاركة هذه البيانات[١٠٨].

وهنا يبرز التساؤل حول تحديد من له الحق في النسيان الرقمي عبر الشبكات الاجتماعية؟ وما الحالات التي يحق فيها للشخص المعني ممارسة هذا الحق على بياناته؟ ونجيب على ذلك على النحو التالي.

أولاً: تحديد من له الحق في ممارسة النسيان الرقمي

بعد تحديد الخطوط العريضة لمفهوم الحق في النسيان يمكن أن نحدد من له الحق في ممارسة النسيان الرقمي من خلال التقيد بتفسير نص المادة السابعة عشر من اللائحة الأوروبية الجديدة ٢٠١٨/٦٧٩ والتي نصت على الحق في محو البيانات الشخصية أو ما يعرف بالحق في النسيان بقولها "للشخص المعني الحق في الحصول على محو البيانات الشخصية في أقرب وقت ممكن، وعلى القائم بالمعالجة الالتزام بمحو هذه البيانات الشخصية في أقرب وقت ممكن....".

(١٠٧) أشرف جابر سيد، *الجوانب القانونية لمواقع التواصل الاجتماعي: مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتويتر*. مرجع سابق الإشارة إليه، ص ٢٣ وما بعدها.

(108) Article 8 -Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information.
Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.
Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.
Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.
Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant. Voir https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article8 Visiter le site au 11/03/2018
Selon une étude réalisée en 2011 par TNS SOFFRES pour le compte de la CNIL, près de 20% des moins de 13 ans ont un compte 48% des enfants de 8-17 ans sont connectés à un réseau social (Facebook). http://www.cnil.fr/la-cnil/actu-cnil/article/article/reseaux-sociaux-quelles-sont-les-pratiques-de-nosenfants-quel-est-le-role-des-parents/?tx_ttnews[backPid]=2&cHash=66639ddc7d Visiter le site au 03/11/2018. Voir Aussi :
Emmanuel DECAUX : « La protection de la vie privée au regard des données informatiques », Revue électronique Droits fondamentaux, n° 7, janvier 2008 – décembre 2009, p.3.

ومن خلال النص السابق يتضح أن الشخص المعني هو فقط الشخص صاحب البيانات الشخصية الذي أعطى الموافقة على معالجتها[١٠٩].

إذن للشخص المعني الحق في السيطرة على كافة بياناته الشخصية، ويتجسد ذلك خلال فترة محددة من الاحتفاظ بالبيانات، بالحق في الحصول على معلومات عن موضوعها، والحق في الوصول إليها متى شاء، والحق في التصحيح والحذف منها، والحق في المعارضة على عملية المعالجة التي تتم عليها. أي أن الشخص المعني له الحق في السيطرة على بياناته والتأكد بالفعل من اختفائها الكامل والفعلي. مع الأخذ في الاعتبار القيود التقنية الخاصة بالإنترنت؛ لأن عملية اختفاء البيانات من على جميع المواقع ومحركات البحث تُعد أمراً صعباً لنشرها في أماكن عديدة بالإضافة لوجودها لدى الكثير من الأشخاص.

ثانياً: الحالات التي يحق فيها للشخص المعني ممارسة هذا الحق على والحالات المستثناة من ذلك

١- باستقراء نص المادة السابعة عشر من اللائحة الأوروبية السابق الإشارة إليها[١١٠] نلاحظ أنها أوجبت في الفقرة الأولى منها محو البيانات الشخصية دون تأخير لا مبرر له إذا انطبق أحد الأسباب التالية:

(أ) إذ لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي جمعت من أجلها أو تمت معالجتها بطريقة أخرى غير المتفق عليها.

(ب) إذا سحب الشخص المعني الموافقة التي تستند إليها المعالجة، بالإضافة لعدم وجود سبب قانوني آخر للمعالجة، وفي حالة معالجة البيانات الشخصية بصورة غير قانونية.

(ج) محو البيانات الشخصية إذا نص القانون على ذلك.

(د) أجازت اللائحة الأوروبية محو البيانات الشخصية التي يتم جمعها كمتطلب للحصول على خدمات مجتمع المعلومات، إذا تم هذا المتطلب بشكل غير قانوني وأشار إلى المعلومات التي يتم الحصول عليها من الأطفال بقوله في نص الفقرة الأولى من المادة الثامنة من اللائحة "تكون معالجة البيانات

(109) Règlement (UE) 2016/679, Art. 17 - Droit à l'effacement («droit à l'oubli»)
La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:
a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;
b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement;
c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;
d) les données à caractère personnel ont fait l'objet d'un traitement illicite;
e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;
f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.
Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.
Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire:
a) à l'exercice du droit à la liberté d'expression et d'information;
b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3;
d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou
e) à la constatation, à l'exercice ou à la défense de droits en justice.

(110) Ibid.

الشخصية للطفل قانونية إذا كان عمر الطفل ١٦ سنة على الأقل. وإذا كان الطفل دون سن السادسة عشرة، لا تكون هذه المعالجة قانونية إلا إذا كان الشخص الذي يتحمل المسؤولية الأبوية على الطفل أعطى الإذن بذلك القبول".

كما أعطى النص الحق للدول الأعضاء في تضمين قوانينهم الداخلية بموجب القانون على سن أدنى لهذه الأغراض، شريطة ألا يقل هذا العمر عن ١٣ سنة(١١١).

٢- وقد أضاف المشرع الأوروبي إلى ما سبق حالة أخرى هي تلك الحالة التي يكون فيها المتحكم في البيانات الشخصية قد جعلها علنية فهو ملزم بموجب الفقرة الأولى من ذات المادة بمحو هذه البيانات الشخصية. على أن يأخذ في الاعتبار التكنولوجيا المتاحة وتكلفة التنفيذ، بما في ذلك التدابير التقنية، لإبلاغ الذين يعالجون البيانات الشخصية أن البيانات محل المعالجة تقدم بشأنها طلب لمحوها، ومنع نسخ أو تكرار، تلك البيانات الشخصية.

أما الحالات المستثناة مما سبق فهي على النحو التالي:

(أ) ممارسة الحق في حرية التعبير والإعلام.

(ب) الامتثال لالتزام قانوني يتطلب المعالجة بموجب قانون الاتحاد أو الدولة العضو التي يخضع لها المتحكم أو لأداء مهمة يضطلع بها للصالح العام.

(ج) لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة كالمعالجة التي تجرى لأغراض الوفاء بالتزامات وممارسة حقوق محددة في ميدان العمل والضمان الاجتماعي، أو المعالجة التي تتم للوقاية من الأوبئة والأمراض الخطيرة التي تهدد الصحة عبر الحدود أو لضمان مستويات عالية من الجودة والسلامة في الرعاية الصحية والمنتجات الطبية، أو تلك التي تتم لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية مع الحرص على احترام جوهر الحق في حماية البيانات والنص على تدابير مناسبة ومحددة لحماية الحقوق الأساسية ومصالح الشخص المعني. وكذلك المعالجة التي تتم لأغراض الطب الوقائي أو المهني، لتقييم قدرة الموظف على العمل، والتشخيص الطبي، وتوفير الرعاية الصحية أو الاجتماعية أو العلاج أو إدارة نظم الرعاية الصحية أو الاجتماعية(١١٢).

(111) Article 8: **Conditions applicable to child's consent in relation to information society services**

1. Where Point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

(112) 2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in Paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious =

(د) لأغراض الحفظ من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية وفقاً للمادة التاسعة والثمانين من اللائحة الأوروبية محل الدراسة.

(هـ) لإنشاء المطالبات القانونية أو ممارستها أو الدفاع عنها.

المبحث الثالث: معالجة البيانات الشخصية لأغراض إعلانية أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية

عالجت المادة التاسعة والثمانين من اللائحة الأوروبية، الضمانات والاستثناءات المتعلقة بالمعالجة والتجهيز لأغراض الحفظ للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية[١١٣].

ومن بين الإشكاليات ذات الأهمية القصوى التي يثيرها معالجة البيانات الشخصية مسألة خضوع المعالجة لأغراض الحفظ للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية، من أجل الحصول على الضمانات المناسبة التي تكفل حماية الحقوق والحريات المتعلقة بالشخص المعني.

وتكفل هذه الضمانات اتخاذ التدابير التقنية والتنظيمية على وجه الخصوص من أجل ضمان احترام مبدأ تقليل البيانات إلى الحد الأدنى اللازم لعملية لمعالجة وتجهيز البيانات الشخصية لأغراض التسويق المباشر، وقد تشمل هذه التدابير وأمن البيانات شريطة أن يتسنى الوفاء بتلك الأغراض بهذه الطريقة. ويكون للشخص المعني في جميع الأحوال - بصفة عامة - الحق في أن يعترض في أي وقت على تجهيز البيانات الشخصية المتعلقة به بالنسبة لهذا التسويق، والتي تشمل المعالجة الآلية بقدر ارتباطها بالتسويق المباشر[١١٤].

وقد أجاز المشرع الأوروبي في نص الفقرة الثانية من هذه المادة أن ينص في قانون الاتحاد أو الدولة العضو على أنه "عندما تجهز البيانات الشخصية لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية، يجوز أن ينص على عدم التقيد بالحقوق المشار إليها في المواد الخامسة عشر والسادسة عشر والثامنة عشر والحادية والعشرين إذا كانت هذه الحقوق مستحيلة أو تعيق بشكل كبير تحقيق هذه الأغراض...." كل ذلك شريطة أن يتم الوفاء بالشروط والضمانات المشار إليها في هذه المادة[١١٥].

أما في حالة معالجة وتجهيز البيانات الشخصية لأغراض الحفظ من أجل المصلحة العامة، فقد أجاز المشرع الأوروبي أيضاً على أنه "يجوز أن ينص قانون الاتحاد أو الدولة العضو على عدم التقيد بالحقوق المشار إليها في المواد الخامسة عشر والسادسة عشر والثامنة عشر والتاسعة عشر والعشرين والحادية والعشرين من حيث إن هذه الحقوق من المرجح أن تجعل من المستحيل أو تعيق بشكل خطير تحقيق الأغراض

= cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in Paragraph 1 may be processed for the purposes referred to in Point (h) of Paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

(113) Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(١١٤) وفي الحالات التي يمكن فيها الوفاء بهذه الأغراض عن طريق التجهيز الإضافي الذي لا يسمح بتحديد المواد الخاصة بالبيانات أو التي لم تعد تسمح بذلك، يتم الوفاء بهذه الأغراض بهذه الطريقة. انظر نص المادة ٨٩ آنف الذكر.

(115) 89/2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in Paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

المحددة، وهذه الاستثناءات ضرورية لتحقيق تلك الأغراض(١١٦).

وقد شدد المشرع الأوروبي على عدم التوسع في هذه الاستثناءات فنجده قد قام بالنص على أنه في الحالات التي يخدم فيها تجهيز ومعالجة البيانات المشار إليه في الفقرتين الثانية والثالثة من المادة التاسعة والثمانين في الوقت ذاته غرضاً آخر، فلا تنطبق الاستثناءات المنصوص عليها في هذه الحالة، وبالتالي لا يجوز التوسع فيها أو القياس عليها(١١٧).

ويُفهم مما سبق أن عملية تجهيز البيانات الشخصية أو معالجتها لغرض من أغراض الإعلان أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية التي نص عليها المشرع الأوروبي على سبيل الحصر، وبالتالي فلا يجوز أن ينسحب هذا التجهيز لخدمة أغراض أخرى غير تلك التي نص عليه القانون الأوروبي.

فإذا حدث وأن استفاد من تجهيز البيانات غرض آخر فللشخص المعني الحق في الاعتراض على هذا التجهيز وتلك المعالجة وما يترتب عليها من آثار مع الاحتفاظ بحقه في الرجوع بالتعويض على المتسبب في ذلك واقتضاء التعويض اللازم وفق ما تقتضيه المادة الثانية والثمانين من هذه اللائحة.

المبحث الرابع: معالجة البيانات في سياق علاقات العمل(١١٨)

إن المعالجة الخاطئة لبيانات المُستخدمين وتحليلها على نحو غير مطابق للواقع أو غير دقيق يشكل صورة أخرى من صور التعدي على حياتهم الخاصة، لاسيما وأن هذه البيانات قد تترك آثاراً سيئة على سيرة العامل أو صورته لدى المتعاملين معه والمحيطين به وتلحق به أضراراً خاصة بالنسبة لوضعه الاجتماعي أو مركزه المالي أو مستقبله الوظيفي في محيط عمله(١١٩).

ومن أجل منع الأضرار السابقة وغيرها، أجازت اللائحة الأوروبية الحديثة للدول الأعضاء أن تضمن قوانينها الداخلية بموجب القانون أو بواسطة اتفاقات جماعية، وقواعد دقيقة لضمان حماية الحقوق والحريات فيما يتعلق بتجهيز ومعالجة البيانات الشخصية للعمال في إطار علاقات العمل، لأغراض عديدة من بينها التوظيف، وتنفيذ عقد العمل، بما في ذلك الامتثال للالتزامات المنصوص عليها في القانون أو الاتفاقات الجماعية، والإدارة، والتخطيط، وتنظيم العمل، والمساواة والتنوع في مكان العمل، والصحة والسلامة في الأعمال، وحماية الممتلكات التي يملكها رب العمل أو الزبون، وبغرض ممارسة الحقوق والاستحقاقات المتصلة بالعمل والتمتع بها، على أساس فردي أو جماعي، وكذلك لغرض إنهاء علاقة العمل.

ويجب أن تشمل هذه القواعد التدابير المناسبة والمحددة لحماية الكرامة الإنسانية والمصالح المشروعة والحقوق الأساسية للأشخاص المعنيين، مع إيلاء اهتمام خاص للشفافية في المعاملة ونقل البيانات الشخصية بإنشاء نظام أو سجل داخلي للبيانات في مكان العمل أو لدى مجموعة من الشركات العاملة في النشاط الاقتصادي المشترك(١٢٠). ويمكن تقسيم الحديث في هذا الصدد على مرحلتين.

الأولى: معالجة وتجهيز البيانات في سياق التقدم لشغل الوظيفة من أجل أغراض التوظيف

إن معالجة وتجهيز البيانات في سياق التوظيف، لا يعطي الحق لجهة العمل في استخدام البيانات المجمعة إلا لتقييم

(116) 89/3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in Paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

(117) 89/4. Where processing referred to in Paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those Paragraphs.

(١١٨) تجدر الإشارة إلى أن ١٠٪ من الشكاوى التي تلقتها اللجنة الوطنية للحرية والمعلوماتية في عام ٢٠١٢م كانت لها صلة مباشرة بعالم الأعمال. راجع في ذلك الرابط التالي:
https://www.captaincontrat.com/articles-gestion-entreprise/limites-protection-donnees-personnelles-salarie

(١١٩) محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. مرجع سابق الإشارة إليه، ص ٦٦.

(١٢٠) نصت الفقرة الثالثة من هذه المادة على وجه التحديد على أن "تخطر كل دولة عضو اللجنة بالأحكام القانونية التي تعتمدها بموجب الفقرة ١ بحلول ٢٥ مايو/ أيار ٢٠١٨م على أقصى تقدير، ودون تأخير، بأي تعديلات لاحقة تتعلق بها".

قدرة المرشح على شغل الوظيفة المقترحة فقط. ويحظر على جهة العمل أن تقوم بجمع معلومات عن والديه أو الأشقاء أو الآراء السياسية أو عضوية النقابات. كما يحظر جمع وحفظ البيانات الشخصية التي تكشف، بصورة مباشرة أو غير مباشرة، عن الأصل العرقي أو الاثني أو الآراء السياسية أو الفلسفية أو الدينية أو الانتماءات النقابية، وكذلك كافة المعلومات المتعلقة بصحة الأشخاص أو حياتهم الجنسية أو غير ذلك.

كما أنه وفقاً للقواعد العامة في عملية المعالجة، لا يمكن جمع هذه البيانات إلا إذا كانت هذه المعلومات غير متصلة اتصالاً مباشراً وضرورياً بالوظيفة المقترحة. ولذلك، لا يمكن جمع هذه المعلومات إلا في بعض الحالات التي تبررها - على النحو الواجب - خصوصية الوظيفة التي يتعين ملؤها. وبمجرد الانتهاء من تقييم المرشحين، يمكن تخزين المعلومات التي يتم جمعها في قاعده بيانات تُنشأ خصيصاً لهذا الغرض.

وإجمالاً، يجب اتباع القواعد التي تكفل احترام حقوق وحريات العمال والمتقدمين لشغل الوظائف عن طريق التطبيق السليم للقوانين والأنظمة. وعلى سبيل المثال إعطاء المرشح الحق في أن يعترض على جمع بياناته الشخصية. أو إعطائه الحق في تصحيح هذه البيانات. مع الوضع في الاعتبار أنه اعتباراً من ٢٥ مايو/أيار ٢٠١٨م يجب الاحتفاظ بسجل داخلي لتجهيز البيانات الشخصية في إطار عمليات التوظيف داخل دول الاتحاد الأوروبي.

الثانية: معالجة البيانات عقب إبرام عقد العمل

سيكون من المناسب سرد كافة البيانات الشخصية التي تم جمعها مع المعالجة والنقل والمدة وطريقة التخزين المقترنة بها وتحديد جهاز حماية البيانات.

ويجوز لصاحب العمل، بعد تعيين الموظف، أن يجمع معلومات إضافية بما في ذلك المعلومات المتصلة التي تعينه على القيام بإدارة العاملين، وتنظيم العمل، والإجراءات التي يتخذها صاحب العمل[١٢١]. ويتعين على صاحب العمل أن يوفر الأمن المادي والرقمي وأجهزة الوصول إلى البيانات الشخصية.

وعلى هذا النحو، سيكون لديه سجل وإجراءات لتوثيق أمن البيانات. كما أن الأشخاص التابعين لرب العمل يمكنهم الحصول على معلومات المرشحين هم أولئك الذين يتدخلون في عملية التوظيف، وكذلك الإدارات التي تبلغ بالتوظيف مثل (التأمين ضد البطالة، والمرض، والتقاعد ... إلخ).

وعطفاً على المنحى السابق يجب تحديد مدة أرشفة وتخزين كل نوع من البيانات، كما يجب تحديد الإجراءات الخاصة بحذفها. وبمفهوم آخر يمكن القول بأنه بمجرد الوصول إلى الهدف من جمع البيانات، فلا توجد حاجة إلى الاحتفاظ بها ويجب حذفها، أما إذا كان هناك غرض من الاحتفاظ بها، ففي هذه الحالة يجب تحديد مدة الاحتفاظ بالبيانات، مع الإشارة إلى أن أوقات التخزين وحفظ البيانات تختلف حسب الأهداف والغرض المنشود. أما إذا تم توفير إجراء الحذف التلقائي، فيجب على إدارة الملفات التأكد من حذف البيانات بشكل فعال.

ويجب على رب العمل أن يبلغ موظفيه بوجود معالجة لبياناتهم الشخصية. كما يخضع الغرض من تجهيز البيانات الشخصية لرقابة صارمة من جانب اللجنة الوطنية للحريات والمعلوماتية، ولذلك يسمح بوجود جهاز لتحديد مكان المركبة عندما يراد به ضمان سلامة الأشخاص والبضائع.

ويعنى بالعامل في هذا الصدد أي شخص في علاقة عمل مع صاحب العمل سواءً كان هناك عقد عمل أم لا. ويتسع النطاق ليتعلق بكل من العمال والمتدربين والخبراء الاستشاريين.

---

(١٢١) اعتباراً من ٢٥ مايو/أيار ٢٠١٨م يستعاض عن هذا الإعلان بالتزام الشركة بالاحتفاظ بسجل داخلي لتجهيز البيانات الشخصية التي تنفذها وفي المؤسسات التي لا تقل عن ٢٥٠ موظفاً. وهناك التزام بالاحتفاظ بسجل يفصل المرتبات التي تقع في نطاق مسؤوليتهم. ويخضع المتعاقدون من الباطن أيضاً لهذا الالتزام. ويجب أن يوضع هذا السجل تحت تصرف اللجنة الوطنية لتكنولوجيا المعلومات والحريات.

وتتركز معالجة بيانات الفرد العامل على ثلاثة مبادئ: مبدأ الشرعية، ومبدأ الشفافية، ومبدأ احترام حقوق الأشخاص في تجهيز بياناتهم الشخصية.

الأول: مبدأ الشرعية، نادراً ما يكون الموظف في وضع يسمح له برفض جمع بياناته الشخصية من قبل صاحب عمله، – لاسيما بسبب العلاقة التبعية الموجودة – وفي هذا السياق، لا ينبغي لصاحب العمل أن يعامل البيانات الشخصية للموظف على أساس الموافقة فقط.

كما أن تجهيز البيانات يمكن أن يكون مشروعاً إذا استند إلى قواعد أخرى. كالحالة التي تكون فيها المعالجة ضرورية للامتثال لالتزام قانوني يخضع له صاحب العمل أو إذا كان ضرورياً لتحقيق مصلحة مشروعة يتبعها صاحب العمل.

الثاني: مبدأ الشفافية، ويتطلب هذا الأخير من الشخص المعني الاطلاع على المعلومات المتعلقة بتجهيز بياناته الشخصية. ويجب أن تكون المعلومات واضحة ومفهومة ويسهل الوصول إليها. وهي تشمل أغراض المعاملة، والجهات المتلقية للبيانات، وهوية المتحكم، أو صاحب العمل.

الثالث: مبدأ احترام حق العامل، مثله مثل أي شخص في ممارسة حقوقه على بياناته (حق الوصول، والحق في التصحيح ... إلخ) التي أقرتها اللائحة الأوروبية الجديدة.

وبالإضافة إلى المبادئ المبينة أعلاه، يجب على رب العمل أن يحترم المبادئ الأخرى المنصوص عليها في ذات اللائحة، وهي مبدأ التناسب، ومبدأ الحد من الاحتفاظ بالبيانات أو مبدأ دقة البيانات. كما يجب أن تكون كل معالجة للبيانات الشخصية مطابقة لأحكام اللائحة الجديدة وعلى وجه التحديد ما نصت عليه المادة الثامنة والثمانون منها فيما يتعلق بمعالجة البيانات الشخصية في سياق علاقات العمل لأغراض التوظيف، ولأغراض تنفيذ عقد العمل. وينبغي أن تراعي إلى جانب هذه القواعد المبادئ الأوروبية العامة لحماية البيانات.

المبحث الخامس: الحق في التعويض وأحكام المسؤولية

تفرض اللائحة الأوروبية الجديدة لحماية البيانات الشخصية الحق في التعويض لكل شخص تعرض لضرر مادي أو معنوي.

فالشخص المعني يمتلك الحق في المطالبة بالتعويض عن الأضرار أو الآلام الناتجة عن مخالفة القواعد الخاصة بحماية البيانات التي نصت عليها اللائحة. وقد عالجت هذه المسألة المادة الثانية والثمانون من اللائحة[١٢٢] والتي نصت على:

١- لكل شخص لحق به ضرر مادي أو معنوي نتيجة لانتهاك مواد هذه اللائحة الحق في الحصول على تعويض من المتحكم أو القائم بالمعالجة عن الضرر الذي لحق به.

٢- يُعد أي متحكم معني بالمعالجة مسؤولاً عن الضرر الناجم عن الإخلال بهذه اللائحة. ولا يكون المعالج مسؤولاً عن الضرر الناجم عن المعالجة إلا في الحالة التي لا يمتثل فيها للالتزامات التي تنص عليها اللائحة والموجهة تحديداً إلى المعالجين أو في تلك الحالة التي تصرف فيها خارج التعليمات القانونية للمتحكم أو بالمخالفة لها.

(122) Article 82: **Droit à réparation et responsabilité :** 1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

2. Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

4. Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

5. Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2.

6. Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant les juridictions compétentes en vertu du droit de l'État membre visé à l'article 79, paragraphe 2.

٣- يعفى المتحكم أو المعالج من المسؤولية بموجب الفقرة الثانية من هذه المادة إذا أثبت أنه ليس مسؤولاً بأي شكل من الأشكال عن الحادث الذي تسبب في وقوع الضرر.

٤- في الحالات التي تشترك فيها أكثر من وحدة تحكم واحدة أو أكثر من معالج، أو كل من المتحكم والمعالج، في نفس المعالجة، تكون مسؤولة بموجب الفقرتين الثانية والثالثة عن أي ضرر ناجم عن المعالجة، ويتحمل كل متحكم أو قائم بالمعالجة المسؤولية عن الضرر بأكمله من أجل ضمان التعويض الفعال للشخص المعني صاحب البيانات.

٥- إذا قام المتحكم أو المعالج، وفقاً للفقرة الرابعة، بدفع تعويض كامل عن الضرر المُتكبد، يحق لهذا المتحكم أو القائم بالمعالجة أن يعود على المتحكمين الآخرين أو القائمين بالمعالجة الضالعين في نفس العملية بالمبلغ الخاص بهم من المسؤولية عن الضرر، وفقاً للشروط المبينة في الفقرة الثانية.

٦- ترفع الإجراءات القضائية المتعلقة بممارسة الحق في الحصول على التعويض أمام المحاكم المختصة بموجب قانون الدولة العضو المشار إليها في الفقرة الثانية من المادة التاسعة والسبعين.

ويتضح من النص السابق أن اللائحة الجديدة لحماية الأشخاص الطبيعيين فيما يتعلق بتجهيز ومعالجة البيانات الشخصية تبنى نهجاً واسعاً لتعويض الأضرار من حيث أساس المسؤولية وطرق التعويض. فمن الممكن المطالبة بالتعويض عن كافة الخسائر الناجمة عن الخروج على أحكام اللائحة التي دخلت حيز التنفيذ وأصبحت ملزمةً في الخامس والعشرين من مايو/ أيار ٢٠١٨م[١٢٣].

وبطبيعة الحال يُشترط للحكم بالتعويض أن يكون هناك اعتداء على البيانات الشخصية الذي يسبب دائماً وأبداً ضرراً حقيقياً يتمثل في انتهاك الخصوصيات؛ فالمعلومات والبيانات التي يتم تجميعها ومعالجتها لابد وأن يكون لا هدفٌ واضح ومحددٌ سلفاً، ولابد من التزام شبكات التواصل الاجتماعي بالهدف الذي من أجله قامت بتجميع ومعالجة تلك البيانات؛ وبالتالي إذا تجاوزت هذا الهدف فلا مناص من الرجوع عليها بدعوى المسؤولية[١٢٤].

كما تخضع الكثير من المعلومات والبيانات الشخصية المتاحة للمعالجة للسرية. ويفرض هذا التزاماً قانونياً أو تعاقدياً يتمثل في أن أي إفشاء للمعلومات والبيانات سيترتب عليه مسؤولية قانونية، مع ما قد ينص عليه العقد من آثار قد تتمثل في توقيع الجزاءات المنصوص عليها في العقد أو حتى إنهائه من جانب المتعاقد المضرور حماية للخصوصية التي هي على المحك في حالة انتهاك المعلومات الشخصية المتعلقة بالعملاء أو حتى العمال[١٢٥].

وبموازاة الأساس الذي تقوم عليه حماية الخصوصية، تجب الإشارة إلى أنه تم سن تشريعات محددة في وقت مبكر جداً في فرنسا لحماية البيانات الشخصية كجزء من تجهيزها بالحاسوب: فهو قانون المعلوماتية والحريات المؤرخ في ٦ يناير/ كانون الثاني ١٩٧٨م[١٢٦]، ويبدو أن هذا القانون قد

(123) Le 25 mai 2018, le règlement européen est entré en application. De nombreuses formalités auprès de la CNIL disparaîssent. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité. Voir https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

(١٢٤) محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. مرجع سابق الإشارة إليه، ص ٦٤ وما بعدها.

(١٢٥) تنص المادة (٨) من الاتفاقية الأوروبية لحقوق الإنسان على أن لكل فرد الحق في احترام حياته الخاصة. ولذلك فإن لكل شخص الحق في الانتصاف عندما تنتهك خصوصيته، وهذا هو الحال عندما يفصح عن المعلومات الشخصية المتعلقة به دون أن يرغب في ذلك.

(١٢٦) المادة الأولى من قانون ١٩٧٨م، تعطي اللهجة التالية: "يجب ألا يؤثر على هوية الإنسان، ولا على حقوق الإنسان، ولا على الحياة الخاصة، ولا على الحريات الفردية أو العامة". ومن أجل حماية المواطنين، ينص هذا القانون على عدة التزامات للأشخاص أو المنظمات التي تجمع و/ أو تقوم بتجهيز البيانات الشخصية. وعلى هذا النحو، فإن معظم الشركات تشعر بالقلق لأن لديها بالضرورة معلومات شخصية عن عملائها أو موظفيها، بنسب أكثر أو أقل أهمية. للمزيد راجع شريف يوسف حلمي خاطر، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا. مرجع سابق الإشارة إليه، ص ٧٢ وما بعدها.

فرض العديد من الالتزامات على الشركات التي تتعامل مع البيانات الشخصية، ولاسيما فيما يتعلق بالأمن، وهو أمر له أهمية خاصة بالنسبة لنا.

وعلى الرغم من سهولة إثارة مسؤولية القائم بعملية معالجة البيانات وفقاً للنص السابق؛ لقيامه بإلحاق الضرر المادي أو المعنوي بالشخص الذي تمت معالجة بياناته، إلا أنها تبدو أمراً في غاية الصعوبة من الناحية العملية؛ ذلك أن ملاحقة المسؤول عن الضرر يستلزم تحديد هويته، ثم تحديد الأضرار التي تسبب بفعله في إحداثها.

لذلك، ومن وجهة نظرنا فإن هذه المادة تعد – وبحق – انعكاساً صادقاً لعمق مشكلة الممارسات غير المشروعة التي تتم على البيانات الشخصية؛ لما تمثله من تهديد حقيقي لحقوق جديرة بالحماية، إذ ليس بخافٍ أن العديد من القائمين بالمعالجة قد قاموا باستغلال البيانات الشخصية في الدعاية التجارية[١٢٧] أو المساس بحرمة حياته الخاصة[١٢٨].

ويمكن استخراج المبادئ التالية من النص السابق والتي تحكم المسؤولية والتعويض في هذا الإطار.

أولاً: تبني مبدأ المسؤولية المشروطة

يتضح من خلال الفقرة الثانية من المادة المشار إليها أعلاه أن المشرع الأوروبي تبنى نهجاً تشريعياً كان قد انتهجه في قوانين سابقة ألا وهو مبدأ التوازن بين مصلحة القائم بعملية المعالجة أو المتحكم في البيانات من جهة وعدم تحميله بالتزامات أو أعباء مرهقة، وحماية أصحاب البيانات الشخصية من جهة أخرى.

لذلك وضعت اللائحة مبدأً عاماً هو عدم مسؤولية المعالج إلا في أحوال معينة وبشروط خاصة لذلك يوصف نظام المسؤولية الذي تبنته اللائحة بأنه نظام المسؤولية أو المسؤولية المشروطة وهذا ما ظهر في الفقرة الثانية من المادة سالفة الذكر.

فالأصل – وفقاً لهذه المادة، وتحديداً الفقرة الثانية منها – هو عدم مسؤولية المتحكم أو معالج البيانات عن أي ضرر يلحق بصاحب البيانات الشخصية عن الأضرار التي لحقت به نتيجة معالجة هذه البيانات الحساسة الخاصة به طالما أنه التزم بكافة الالتزامات التي نصت عليها اللائحة؛ لأن الأصل العام هو حظر جمع أو معالجة هذه البيانات، إلا أن الشخص المعني يستطيع عن طريق الرضاء الصحيح – طبقاً للقانون الجديد – أن يرخص بذلك وهنا تصبح المعالجة التي تقع على هذه البيانات أمراً مشروعاً، ولا يتعارض مع أحكام الخصوصية[١٢٩].

وينسجم مبدأ المسؤولية المشروطة الذي جاءت به الفقرة الثانية من المادة مع ما نصت عليه المادة من مسؤولية القائم بالمعالجة عن تعويض الأضرار التي تلحق بالشخص المعني في الحالة التي لا يمتثل فيها للالتزامات المنصوص عليها في اللائحة الخاصة بعملية المعالجة.

ثانياً: أثر الأخذ بفكرة الخطأ – فرض التزامات محددة على القائم بمعالجة البيانات الشخصية

يقتضي تأسيس مسؤولية القائم بعملية المعالجة على فكرة الخطأ أن تكون هناك التزامات محددة على عاتقهم؛ لأن توفر الخطأ يفترض الإخلال بالتزام محدد، وقد حصرت اللائحة هذه الالتزامات في عدد من المواد التي تناولناها تحت ما يسمى بالمبادئ الحاكمة لعملية معالجة البيانات الشخصية.

---

(١٢٧) عبدالهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الإنترنت: دراسة قانونية تطبيقية مقارنة. مرجع سابق، ص ٣٣٢ وما بعدها.

(١٢٨) حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني. *مجلة العلوم القانونية والاقتصادية*، كلية الحقوق، جامعة عين شمس، مج (٣٢)، ع (١، ٢)، (يوليو ١٩٩٠م)، ص ص ١-٩٠، ص ٢٣ وما بعدها.

(١٢٩) تجدر الإشارة إلى أن الجمعية العامة للأمم المتحدة اعتمدت القرار رقم ١٦٧/٦٨ وهو من أول القرارات الصادرة عن الجمعية العامة للأمم المتحدة والتي تعنى بموضوع الحق في الخصوصية منذ العام ١٩٨٨م، لاسيما وأنه حث جميع الدول والحكومات على إنهاء الانتهاكات التي تمس الحق في الخصوصية. للمزيد راجع: سارة علي رمال، *الحق في الخصوصية في العصر الرقمي: قراءة تحليلية في ضوء قرار الجمعية العامة للأمم المتحدة رقم ١٦٧/٦٨* . لبنان: منشورات الحلبي الحقوقية، (٢٠١٦م)، ص ٧١ وما بعدها.

ومن بين أهم الالتزامات التي أشارت إليها اللائحة الأوروبية ما ينص عليه في المادة الثالثة والثلاثون المتعلقة بالتعاون مع السلطات المختصة بإخطارها بحدوث انتهاك للبيانات الشخصية.

ووفقاً لهذه المادة يجب على مراقب البيانات أو المتحكم أن يقوم – دون تأخير مبرر – في موعد لا يتجاوز ٧٢ ساعة من علمه بحدوث انتهاك للبيانات الشخصية أن يقوم بإخطار السلطة المشرفة المختصة بهذا الانتهاك وفق ما نصت عليه المادة الخامسة والخمسون.

وقد حددت الفقرة الثالثة من المادة سالفة الذكر مواصفات الإخطار المشار إليه بقولها: "يجب أن يشتمل الإخطار على ما يلي:

(أ) وصف طبيعة انتهاك البيانات الشخصية بما في ذلك – قدر الإمكان – الفئات والعدد التقريبي للأشخاص المعنيين والعدد التقريبي لسجلات البيانات.

(ب) الإبلاغ عن اسم وتفاصيل الاتصال الخاصة بمسؤول حماية البيانات أو نقاط الاتصال الأخرى التي يمكن الحصول فيها على مزيد من المعلومات.

(ج) وصف العواقب المحتملة لانتهاك البيانات الشخصية.

(د) وصف التدابير المتخذة أو المقترح اتخاذها من جانب المراقب الخاص أو المتحكم لمعالجة انتهاك البيانات الشخصية بما في ذلك – عند الاقتضاء – تدابير للتخفيف من آثاره الضارة المحتملة."

ولكن إذا كان المتحكم أو القائم بعملية المعالجة ملتزماً بتزويد السلطات العامة بأية خروقات للبيانات الشخصية شاملة على الوقائع المتعلقة بانتهاك البيانات الشخصية وآثارها والإجراءات التصحيحية المتخذة، فإن التساؤل يثور عما إذا كان من الجائز لغير السلطات وتحديداً المضرور أن يلزمه بالكشف عن الهوية أم لا؟[١٣٠]

للإجابة على هذا السؤال، أرى أنه لا يجوز إلزام المتحكم أو القائم بعملية معالجة البيانات إلا وفقاً لضوابط وإجراءات محددة تضمن سرية المعلومات. ولا ينال من سلامة هذا النظر أن الفقرة الأولى من المادة الثالثة والثلاثين من اللائحة الأوروبية لم تتعرض سوى لإخطار السلطات المختصة؛ لأننا لو كنا نسلم بحق المضرور بإلزام القائم بعملية المعالجة بإزالة الضرر وتعويض الشخص المعني في حال عدم التزامه بالاشتراطات التي نص عليها اللائحة، فلماذا لا نجيز له أن يطلب الكشف عن هوية مرتكب الفعل الضار أو سبب الانتهاك عندما تكون عدم المشروعية ظاهرة.

ثالثاً: القاعدة العامة مبدأ التعويض الكامل والعادل للمضرور

من المبادئ التي اعتمدها المشرع الأوروبي أيضاً في المادة (٨٢/ ١) مبدأ التعويض الكامل للأضرار المادية والمعنوية التي تنشأ نتيجة انتهاك القائم بالمعالجة لأحكام اللائحة الأوروبية الجديدة[١٣١].

ويعتبر انتهاك الخصوصية مناطاً للتعويض بصرف النظر عن توافر الخطأ من عدمه، فإذا تحقق الضرر وجب التعويض عن كافة عناصره بحيث يعوض عن الضرر ولا شيء غير الضرر وفقاً لمبدأ التعويض الكامل الذي يمنع أن يثرى المضرور من التعويض، ويشمل التعويض ما لحقه من خسارة وما فاته من كسب.

ومن الواجب الإشارة إلى أن الاعتداء على الحياة الخاصة بسبب فعل القائم بالمعالجة يمكن أن ينشأ عنه ضرر مادي يتمثل في الخسارة التي تلحق بمن انتهكت خصوصياته أو الكسب الذي يفوت جراء الاعتداء، غير أن هذه الأضرار تبقى قليلة مقارنةً بالأضرار الأدبية التي تحدث في هذا الإطار[١٣٢].

---

(١٣٠) أشرف جابر سيد، *الجوانب القانونية لمواقع التواصل الاجتماعي: مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتويتر*. مرجع سابق الإشارة إليه، ص ١١٨.

(١٣١) محمد سامي عبدالصادق، *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. مرجع سابق الإشارة إليه، ص ٦٤ وما بعدها.

(١٣٢) نفس الإشارة السابقة.

كما يجب أن يكون التعويض عادلاً، ولن يكون كذلك إلا إذا كان تقدير الأضرار عادلاً[١٣٣]. ومن العناصر التي يجب أن تؤخذ في الاعتبار استخدام البيانات الشخصية في الإعلانات والدعاية التجارية.

ويستحق الشخص المعني مقابلاً عادلاً عن الاعتداء على بيناته الشخصية، حتى ولو كان قد أعطى الإذن بمعالجة بياناته؛ لأنه مما لا شك فيه أن إساءة استخدام البيانات يساهم بشكل كبير في انتهاك الخصوصية كما أن المعلومات والبيانات التي يتم تجميعها ومعالجتها لابد وأن يكون لها هدف واضح ومحددٌ سلفاً ولابد من التزام القائم بعملية المعالجة بالهدف الذي من أجله قام بتجميع البيانات ومعالجتها.

ولما كان إثبات قيمة الضرر الفعلي أمراً صعباً فإن القضاء "يلجأ إلى التقدير الجزافي للضرر، لانسجامه مع اعتبارات العدالة خاصة في ظل عدم وجود تقدير محدد". ويراعى في هذا التقدير أن يكون كافياً بالقدر الذي لا يحقق معه القائم بالمعالجة أية ميزة مالية من الاعتداء غير المشروع على البيانات ذات الطابع الشخصي. كما يجب أن تراعى الاعتبارات الخاصة بالمضرور المعتدى على بياناته الشخصية، وأهمها مركزه الاجتماعي والثقافي والعلمي والفني، ومدى تأثير الاعتداء على سمعته.

وإذا كان تقدير التعويض عن الضرر المادي يبدو سهلاً، فإن الأمر لا يبدو كذلك بالنسبة للضرر المعنوي الناتج عن الاعتداء على البيانات الشخصية، وذلك لما تتسم به هذه البيانات من طابع غير ملموس يتعلق بسمعة المؤلف واعتباره، فضلاً عما يسببه اجتماع الضررين المادي والأدبي من صعوبة في تقدير التعويض المالي، ولذلك يتم عادة دمجهما وتقدير التعويض عنهما دون تخصيص[١٣٤].

وفي تقديرنا يجب ألا يقتصر القاضي عنده تقديره لمقدار التعويض على ما لحق المضرور من خسارة وما فاته من كسب، ولكن يجب ضرورة الأخذ في الاعتبار الأرباح التي جناها القائم بالمعالجة أو المسؤول من فعل الاعتداء.

أيضاً يجب أن يلزم المشرع القاضي بقواعد خاصة لتقدير التعويض من خلال الاعتداد بجميع عناصر الضرر على نحو مفصل، وهو ما يحقق العدالة ويفضي إلى ارتفاع مبلغ التعويض المحكوم به، ويؤدي بطبيعة الحال إلى ردع القائم بالمعالجة أو الشخص المسؤول عن الضرر عن معاودة الإخلال بأحكام القانون أثناء معالجة البيانات الشخصية، مع الوضع في الاعتبار أننا لا نقصد من ذلك تقنين فكرة التعويض العقابي في هذا الصدد؛ لأن الأساس الذي تقوم عليه قواعد المسؤولية بالدرجة الأولى هو تعويض المضرور لا معاقبة المسؤول. فالتعويض إذن يقاس بمقدار الضرر الذي أصاب المضرور بالذات حسب الأصل وخاصة الآثار المالية المترتبة على وقوع الضرر حيث تختلف من شخص لآخر، فالتعويض يقدر بحسب الظروف الشخصية للمضرور وليس تقديراً مجرداً[١٣٥].

ونعتقد مع آخرين[١٣٦] أن هذه الطريقة في حساب التعويض تعد الأفضل في تحقيق العدالة على وجه الخصوص في مجال شبكة الإنترنت؛ حيث تساهم هذه الأخيرة في انتشار الضرر الذي يصيب المضرور على نطاق واسع، بسبب زيادة حجم المستخدمين لها. وبالتالي فإذا كان المسؤول قد استفاد من تحقيق

(١٣٣) للمزيد حول مسألة تقدير الأضرار راجع: أشرف جابر سيد، المرجع السابق، ص ١٨٤.

(١٣٤) أشرف جابر سيد، *مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع (دراسة خاصة لمسؤولية متعهدي الإيواء)*. القاهرة: دار النهضة العربية، (٢٠١٠م)، ص ١٨٦.

(١٣٥) محمود جمال الدين ذكي، *الوجيز في نظرية الالتزام في القانون المدني المصري، الجزء الأول في مصادر الالتزام*. ط٢، مطبعة جامعة القاهرة والكتاب الجامعي، (١٩٧٦خ)، ص ٥١٨ وما بعدها. وانظر أيضاً: إبراهيم الدسوقي أبو الليل، التقدير القضائي للتعويض. *مجلة المحامي الكويتية*، السنة الثامنة، أعداد (أبريل، مايو، يونيو)، (١٩٨٥م)، ص ١٣١ وما بعدها. وانظر: جميل الشرقاوي، *النظرية العامة للالتزام، الكتاب الأول، مصادر الالتزام*. القاهرة: دار النهضة العربية، (١٩٩٥م)، ص ٤٧٨ وما بعدها.

(١٣٦) عبدالهادي فوزي العوضي، *المسؤولية التقصيرية لناشري برامج التبادل غير المشروع للمصنفات الفكرية (peer-to-peer): دراسة مقارنة في القانون الفرنسي والمصري والعماني*. القاهرة: دار النهضة العربية، (٢٠١٦م)، ص ١٦٤ وما بعدها.

المزيد من الأرباح، فيجب أن يأتي التعويض ليحرمه من كل الأرباح التي جناها[١٣٧].

رابعاً: مبدأ التعويض الفعال للمضرور عن طريق فكرة الحلول

يبدو أن المعالجة التشريعية التي انتهجتها اللائحة الأوروبية الجديدة تؤدي إلى تبني نظام التعويض الفعال للمضرور، ويتضح ذلك من خلال الحصول على التعويض الكامل سواءً من القائم بالمعالجة أو المتحكم في البيانات حال اشتراك أكثر من وحدة تحكم أو أكثر من معالج في إحداث الضرر للشخص المعني أثناء معالجة بياناته.

وما خلصنا إليه هنا ليس فرضاً نظرياً بحتاً، بل يفرضه واقع ما نصت عليه الفقرة الرابعة من المادة السابقة بقولها "في الحالات التي تشترك فيها أكثر من وحدة تحكم واحدة أو أكثر من معالج، أو كل من المتحكم والمعالج، في نفس المعالجة، وحيثما تكون، بموجب الفقرتين الثانية والثالثة مسؤولة عن أي ضرر ناجم عن المعالجة، ويتحمل كل متحكم أو معالج المسؤولية عن الضرر بأكمله من أجل ضمان التعويض الفعال للشخص المعني صاحب البيانات".

ويبدو أن النهج الذي تبناه المشرع الأوروبي في تعويض الأضرار يقضي بأن يتم صرف التعويض مباشرة من خلال قيام المتحكم أو المعالج، وفقاً للفقرة الرابعة بدفع تعويض كامل عن الضرر المُتكبد، على أن يقوم هذا المتحكم أو القائم بالمعالجة لاحقاً بالرجوع على أي مسؤول آخر سواءً كان متحكماً في البيانات أو قائماً بالمعالجة بمبلغ التعويض الخاص بهم كجزء من مسؤوليتهم عن الضرر، وفقاً للشروط المبينة في الفقرة الثانية من المادة سالفة الذكر.

وتبرز فكرة فاعلية التعويض عن انتهاك البيانات الشخصية أو الإخلال بالالتزامات التي أقرتها اللائحة الأوروبية أثناء عملية معالجة البيانات، في أن عملية تعويض المضرور عن الأضرار التي تصيبه تمثل الهدف الأسمى للتوجيه الجديد. فأياً كانت أهمية الالتزامات التي يخالفها فاعل الضرر، فإن المحصلة النهائية لهذه لمخالفة هي الحكم بالتعويض على هذا المسؤول[١٣٨].

وعلى الرغم من أن اللائحة الأوروبية نصت على مسألة فاعلية التعويض إلا أنها لم تنص على آلية واضحة ومحددة أو طريقة تضمن سرعة تحقيق الوظيفة التعويضية لحصول المضرور على التعويض الكافي لإشباع حاجته إلى الشعور بالأمان والعدالة في المجتمع الذي يعيش فيه باستثناء فكرة الحلول التي نص عليها في محاولة منه لإيجاد وسيلة فاعلة وسريعة لحصول المضرور على التعويض.

خامساً: الرجوع على المسؤول عن تعويض الضرر في حال القيام بالوفاء بقيمة التعويض للمضرور

نصت الفقرة الخامسة من المادة سالفة الذكر على أنه ".... يحق للمتحكم في البيانات أو القائم بالمعالجة أن يرجع على المتحكمين الآخرين أو الضالعين في عملية إحداث الضرر للشخص المعني بالمبلغ الخاص بهم من المسؤولية عن الضرر وفقاً للشروط المبينة بالفقرة الثانية".

وبناءً عليه يمكن القول بأن اللائحة الأوروبية تبنت مبدأ حلول الموفي محل المضرور في الرجوع على فاعل الضرر، واشترط لذلك أن يتم الامتثال لما نصت عليه الفقرة الثانية من نفس المادة السابقة.

---

(١٣٧) إذا كان التقدير الموضوعي للتعويض لا يعتد فيه بظروف المسؤول، ولا يختلف من شخص لآخر، ويفترض وحدة وموضوعية آثار الفعل الضار، فعلى العكس من ذلك تماماً يكون تقدير الضرر اللاحق بالمضرور، حيث يقدر تقديراً واقعياً ذاتياً، ومقتضاه الاعتداد بالظروف الخاصة للمضرور، كسنه ومركزه الاجتماعي، والمهني والمالي، وحالته الصحية والجسمانية. للمزيد، انظر: عربي السيد عبدالسلام محمد، *أحكام تقدير التعويض وأثر تغير القوة الشرائية للنقود على تقديره: دراسة مقارنة*. رسالة دكتوراه، كلية الحقوق، جامعة أسيوط، (٢٠٠٨م)، ص ١١٦ وما بعدها.

(١٣٨) حول هذا الموضوع يرجى مراجعة الدراسة القيمة للزميل الدكتور عابد فايد عبدالفتاح، *التعويض التلقائي للأضرار بواسطة التأمين وصناديق الضمان: دراسة مقارنة في القانون المصري والقانون الفرنسي*. الإسكندرية: دار الجامعة الجديدة، (٢٠١٤م)، ص ١٣ وما بعدها. وللمزيد حول تأثير التعويض التلقائي على وظائف المسؤولية المدنية انظر نفس المرجع ص ٩٨ وما بعدها.

وهذا التوجه يتوافق مع ما يراه جانب من الفقه الفرنسي[١٣٩] من أن المسؤولية المدنية تبدو كنظام موجه نحو تعويض الأضرار، هذا التعويض يتحقق عن طريق دفع مبلغ للمضرور يتطابق من حيث المبدأ مع الخسارة التي لحقت به والكسب الذي فاته. وهذه الصيغة تتجه من باب أولى نحو مفهوم اقتصادي بحت للتعويض.

ويؤكد جانب آخر من الفقه الفرنسي أيضاً[١٤٠] على ذات المعنى المتقدم من أن المستقر عليه في مجال المسؤولية المدنية، أن الجبر الكامل للأضرار التي تلحق بالمضرور يحول دون أي إفقار أو إثراء لهذا الأخير. وبالتالي فإن الأموال التي يدفعها المسؤول تهدف إلى إعادة الشخص إلى الوضع الذي كان عليه قبل وقوع الضرر.

ومن المثير للاهتمام في هذا الصدد أن اعتماد اللائحة الأوروبية لفكرة حلول الموفي محل المضرور تحقق أكثر من فائدة، الأولى: أن يقع العبء النهائي للتعويض على عاتق الشخص المسؤول عن الضرر، والثانية: منع إثراء المضرور من التعويض بعدم حصوله على تعويض يزيد عن الضرر الذي أصابه، والثالثة: تخفيف التكلفة الاجتماعية للحصول على التعويض[١٤١].

وبالتالي يمكن القول بأن دعوى الرجوع التي يمارسها الموفي ليست وسيلة لتحديد شخصية المسؤول، بل هي وسيلة وعلى حد تعبير Geneviève Viney تهدف إلى الرجوع على المسؤول بقيمة التعويض الذي أخذه على عاتقه الذي قام بالوفاء بقيمته للمضرور[١٤٢].

الخاتمة

شكلت اللائحة الأوروبية الصادرة في السابع والعشرين من أبريل/ نيسان ٢٠١٦م منعطفاً مهماً في حماية خصوصية البيانات الشخصية للأفراد وتحديداً في الشق المتعلق بتجهيز هذه البيانات ومعالجتها، بحكم أنها جاءت بقواعد جديدة كاشفة بذلك عن تحولات عميقة طالت قوانين حماية البيانات الشخصية على مستوى دول الاتحاد الأوروبي. وقد تم ذلك من خلال إقرار هذه اللائحة لمبادئ وأساليب جديدة، يتم توظيفها لغايات المعالجة المشروعة، ومن هذه المبادئ ما تم اقتباسه من اللائحة العامة لحماية البيانات والتي ألغيت بصدور هذه اللائحة (95/46/CE) ومنها ما أفرزته الثورة الحاصلة في تقنية المعلومات، وبالتالي وجبت مواجهتها تشريعياً لعدم الإضرار بالأفراد وانتهاك خصوصياتهم.

ومن بين الأمور التي عملت اللائحة الأوروبية الجديدة على مواجهتها ذلك الاجتياح لخصوصية بيانات الأفراد والمعالجة غير المشروعة لها؛ فعن طريق معالجة البيانات الشخصية أصبح من الممكن الحصول على معلومات يعتد بها وموثوق في مصداقيتها، واكتشاف أدق تفصيلات حياة الفرد الشخصية اجتماعية كانت أم مالية أو أحواله الصحية أو ميوله السياسية أو اهتماماته الترويحية أو تعاملاته الرسمية.

لذا لجأ المشرع الأوروبي إلى تنظيم معالجة البيانات الشخصية للأفراد بموجب هذه اللائحة التي حاول من خلالها إيجاد نوع من التوازن الملائم بين الخصوصية بأن يكون للمرء الحق في أن يترك وشأنه من جهة، والحق في معالجة البيانات الشخصية لأغراض مشروعة من جهة أخرى، وقد يبدو للقارئ أنهما متضادين، إلا أنه بإمعان النظر فيهما سيجد أنهما يرتبطان ببعضهما البعض ارتباطاً وثيقاً لا تضاد فيه بل هو تكامل يجب أن يتم وفق أطر وأسس قانونية محددة.

وهذا التكامل يتأتى من خلال التحليل الدقيق للعلاقة بينهما؛ فالمعلومات بصفة عامة والبيانات الشخصية بصفة خاصة تشكل جوهر الحق في الخصوصية في العصر الرقمي، هذا من ناحية، ومن ناحية ثانية فإن معالجة المعلومات والبيانات الشخصية تُعد أساس اقتصاد العصر الحديث وعماد تنميته في ظل تنامي القدرات التكنولوجية للحاسب في تخزينها

(139) Suzanne Carval, Patrice Jourdain, Geneviève Viney: Les effets de la responsabilité 4e édition, Editeur : L.G.D.J , 2017, n o2 , p.5

(140) Linda Maizener, membre du conseil d'administration de l'Association des jeunes magistrats Tout le dommage, rien que le dommage ? Gaz. Pal. 24 juill. 2018, n° GPL329s3, p.3, Pour en savoir plus sur ce principe, voir: https://www.gazette-du-palais.fr/article/GPL329s3/

(141) Patrice Jourdain, Geneviève Viney : Traité de droit civil, Les conditions de la responsabilité Dommage, fait générateur, régimes spéciaux, causalité , 4e édition , Editeur: L.G.D.J, 2013, p.88 et s.

(142) Geneviève Viney : Introduction à la responsabilité, 3e édition, Editeur: L.G.D.J, 2008, no 32 p.51.

وتجهيزها ومعالجتها، وسرعته الفائقة على استرجاعها وتداولها تحت مظلة التطورات التقنية التي يمكن إخضاعها لضوابط قانونية وتشريعية على نحو يضمن توجيه مسارها واستثمار مزاياها والحد من خطرها وأضرارها بالقدر اللازم للاستفادة منها وفق مبادئ محددة ولفئة عمرية محددة.

وعلى هذا النحو، أضحى تجهيز البيانات والمعلومات الشخصية ومعالجتها سلاحاً ذو حدين يوفر أحدهما حياة سلسة للشخص عن طريق تحليل بياناته لأغراض تخدم مصالحه، بالإضافة إلى أنها توفر له بيئة آمنة من خلال تطويع هذه المنظومة بما يتلاءم ويتوافق مع خصوصياته. والثاني يمكنه أن يحيل حياة الأفراد والمجتمعات إلى جحيم من الناحيتين المادية والمعنوية لتهديده خصوصية الفرد من ناحية والسلامة المجتمعية من ناحية أخرى.

فالعبرة إذن بالسياق الذي يتم فيه معالجة البيانات الشخصية، فقد يكون السياق مشروعاً بل واجباً اجتماعياً – من وجهة نظرنا – كأن تتم المعالجة من أجل تطوير التعليم أو البحث العلمي أو الصحة العامة، أو خدمة المجتمع، أو مواجهة التحديات، وتوفير الرعاية الصحية، ومكافحة الجريمة، والتصدي للإرهاب ودعم قيم المواطنة والمشاركة الإيجابية في تحقيق التقدم للأفراد والمجتمعات على حد سواء ... إلخ.

وقد يكون السياق غير مشروع، ويتطلب لمجابهته إعمال أحكام القانون كأن يتم استخدام المعالجة للنيل من سمعة إنسان أو التشهير به أو استخدام التاريخ الرقمي الخاص به في ذلك، أو لاستخدام المعالجة في أي وجه من الأوجه غير المشروعة التي تمثل خروجاً على قواعد القانون والقيم والأخلاق والعدالة السائدة في المجتمع.

وقد واجه التشريع الأوروبي الأخير قضية معالجة البيانات الشخصية معالجة تبدو شاملة، احتلت فيها خصوصية البيانات الجزء الأكبر منه خاصةً ما نتج عن تقنية المعلومات من إشكالات في الآونة الأخيرة تتعلق بالحق في أمن البيانات الشخصية، والحق في حذف البيانات (النسيان الرقمي) والعلاقة مع الأرشفة وتخزين البيانات للمصلحة العامة، ومعالجة البيانات الشخصية لأغراض إعلانية أو لأغراض البحث العلمي، ومعالجة البيانات في سياق علاقات العمل، وأحكام المسؤولية والتعويض عن الأضرار التي تلحق بالشخص المعني نتيجة المعالجة غير المشروعة التي تتم على بياناته الشخصية.

ولكن ثمة مشكلة واجهت المشرع الأوروبي تكمن في صعوبة التوفيق بين مقتضيات الإفصاح والشفافية من ناحية متطلبات الخصوصية والأمن الوطني لدول الاتحاد الأوروبي من ناحية أخرى فقام بالعمل على حلها وأجاز بشروط معالجة البيانات الشخصية في هذا الإطار.

وأرى أن يبادر المشرع المصري ونظرائه من المشرعين العرب الذين لم يقوموا بسن تشريع لحماية البيانات الشخصية بالمسارعة في إصدار قانون يحمي البيانات الشخصية للأفراد من الانتهاكات الصارخة التي تمارس عليها ليلاً ونهاراً، وأن يركز على الوضع الراهن لتشريعات تقنية المعلومات وحماية البيانات الشخصية في بريطانيا ودول الاتحاد الأوروبي والولايات المتحدة الأمريكية لأغراض المقارنة والاستفادة من تجارب الآخرين نظراً لتفاوت التشريعات من دولة إلى أخرى، وربما يكون هناك ما يمكن الاستفادة منه في تطوير المنظمة التشريعية في هذا المجال ومن المعايير الأوروبية لحماية البيانات التي جاءت بها اللائحة الأوروبية الجديدة. كما أدعو إلى ما يلي:

- أولاً: تنظيم حق الإنسان في أن تُمحى بياناته الشخصية (حق النسيان الرقمي) (droit à l'oubli) وتنظيم العلاقة الجدلية بين هذا الحق والحق في أرشفة البيانات للمصلحة العامة، وذلك انطلاقاً من أن استمرار وجود هذه البيانات قد يصبح ضاراً بمصالح الشخص الذي عولجت بياناته، وأنه لم يعد هناك ضرورة لبقاء هذه البيانات، فمن حقه إذن المطالبة بالحق في النسيان الرقمي بالتزامن مع وجود حالات تقتضي الإبقاء على هذه البيانات وأرشفتها للمصلحة العامة.
- ثانياً: ضرورة تقنين ووضع الضمانات المناسبة التي تكفل حماية الحقوق والحريات المتعلقة بالشخص المعني أثناء معالجة بياناته الشخصية لأغراض إعلانية أو لأغراض

البحث العلمي أو التاريخي أو للأغراض الإحصائية. على أن تكفل هذه الضمانات العديد من التدابير القانونية وأهمها النص على مبدأ تقليل البيانات إلى الحد الأدنى اللازم لعملية معالجة وتجهيز البيانات الشخصية.

- رابعاً: وضع قواعد دقيقة لضمان حماية الحقوق والحريات فيما يتعلق بتجهيز ومعالجة البيانات الشخصية للعامل في إطار علاقات العمل، سواء كانت المعالجة لأغراض التوظيف أو تنفيذ عقد العمل.
- خامساً: وضع قواعد خاصة للتعويض عن الأضرار المادية والمعنوية الناجمة عن عملية المعالجة لضمان التعويض الفعال للمضرور سواءً من القائم بالمعالجة أو المتحكم في البيانات.

المراجع

أولاً: المراجع باللغة العربية

(أ) المراجع العامة

البيه، محسن عبدالحميد (٢٠٠٧م). *الإثبات في المواد المدنية والتجارية. وفقاً لقانون الإثبات وقانون التوقيع الإلكتروني*. كتاب مقرر على طلاب كلية الحقوق، جامعة المنصورة.

ذكي، محمود جمال الدين (١٩٧٦م). *الوجيز في نظرية الالتزام في القانون المدني المصري. الجزء الأول في مصادر الالتزام*. ط٢، مطبعة جامعة القاهرة والكتاب الجامعي.

الشرقاوي، جميل (١٩٩٥م). *النظرية العامة للالتزام. الكتاب الأول. مصادر الالتزام*. القاهرة: دار النهضة العربية، ص ٤٨ وما بعدها.

علي، عبدالصبور عبدالقوي (٢٠١٣م). *التنظيم القانوني للتجارة الإلكترونية*. الرياض: مكتبة القانون.

(ب) المراجع الخاصة

أبو الليل، إبراهيم الدسوقي (١٩٨٥م). التقدير القضائي للتعويض. *مجلة المحامي الكويتية*، السنة الثامنة، أعداد (أبريل، مايو، يونيو).

أحمد، شمس الدين إبراهيم (٢٠٠٥م). *وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانونين السوداني والمصري: دراسة مقارنة*. ط١، القاهرة: دار النهضة العربية.

حجازي، عبدالفتاح بيومي (٢٠٠٨م). *حماية المستهلك عبر شبكة الإنترنت*. مصر: دار الكتب القانونية.

الخصاونة، علاء الدين (٢٠١١م). الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية. *مجلة جامعة الشارقة للعلوم الشرعية والقانونية*، مج (٨)، ع (٢)، الإمارات العربية المتحدة.

رستم، هشام محمد فريد (١٩٩٢م). *الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة*. أسيوط: مكتبة الآلات الحديثة.

رمال، سارة علي (٢٠١٦م). *الحق في الخصوصية في العصر الرقمي: قراءة تحليلية في ضوء قرار الجمعية العامة للأمم المتحدة رقم ٦٨/١٦٧*. لبنان: منشورات الحلبي الحقوقية.

سيد، أشرف جابر (٢٠١٣م). *الجوانب القانونية لمواقع التواصل الاجتماعي: مشكلات الخصوصية وحرية التعبير والملكية الفكرية والإثبات مع التركيز على موقعي فيسبوك وتويتر*. القاهرة: دار النهضة العربية.

عبابنة، محمود أحمد (٢٠٠٥م). *جرائم الحاسوب وأبعادها الدولية*. ط١، عمان: دار الثقافة للنشر والتوزيع.

عبدالصادق، محمد سامي (٢٠١٦م). *شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية*. القاهرة: دار النهضة العربية.

عبدالفتاح، عابد فايد (٢٠١٤م). *التعويض التلقائي للأضرار بواسطة التأمين وصناديق الضمان: دراسة مقارنة في القانون المصري والقانون الفرنسي*. الإسكندرية: دار الجامعة الجديدة.

العوضي، عبدالهادي فوزي (٢٠١٦م). *المسؤولية التقصيرية لناشري برامج التبادل غير المشروع للمصنفات الفكرية (peer-to-peer): دراسة مقارنة في القانون الفرنسي والمصري والعُماني*. القاهرة: دار النهضة العربية.

المقاطع، محمد (١٩٩٢م). *حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي*. مطبوعات جامعة الكويت.

(ج) أبحاث ومقالات

أبو فارة، يوسف أحمد (٢٠٠٦م). تحليل العلاقة بين حماية الخصوصية وبين التسجيل والإفصاح عن البيانات الشخصية في المتاجر الإلكترونية. *مجلة العلوم الإدارية*، الأردن، مج (٣٣)، ع (٢)، ص ص ١٨٩-٢٠٨.

الأهواني، حسام الدين كامل (يوليو ١٩٩٠م). الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني. *مجلة العلوم القانونية والاقتصادية*، كلية الحقوق، جامعة عين شمس، مج (٣٢)، ع (١، ٢)، ص ص ١-٩٠.

البكاري، محمد (٢٠١٥م). حماية سرية المراسلات الشخصية. *مقال محكم ومنشور بمجلة المنبر القانوني*، المغرب، ع (٩)، ص ص ٢٠٧-٢١٢.

التهامي، سامح عبدالواحد (سبتمبر ٢٠١١م). الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي - القسم الأول. *مجلة الحقوق*، جامعة الكويت، مج (٣٥)، ع (٣)، ص ص ٣٧٥-٤٣٤.

جدي، نجاة (د.ت.). المعلوماتية وحق المؤلف. *بحث منشور بمجلة دراسات وأبحاث*، جامعة زيان عاشور (الجلفة)، الجزائر، ع (٦)، ص ص ١٨٦-٢٠٠.

خاطر، شريف يوسف حلمي (أبريل ٢٠١٥م). حماية الحق في الخصوصية المعلوماتية: دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا. *مجلة البحوث القانونية والاقتصادية*، كلية الحقوق جامعة المنصورة، مصر، ع (٥٧)، ص ص ١-١٧٠.

زايد، محمد (٢٠٠٦م). الجريمة والقرصنة في مجال المعلوماتية والشبكات. *بحث منشور في المجلة العربية العلمية*، تونس، مج (١٠)، ع (١٩)، ص ص ٧٣-٨٤.

سعداني، ماء العينين (مايو ٢٠١٤م). الأمن القانوني والمعلوماتي. *مجلة الفقه والقانون*، المغرب، ع (١٩).

سيد، أشرف جابر (يناير/ يوليو ٢٠١٠م). مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع: دراسة خاصة لمسؤولية متعهدي الإيواء. *مجلة حقوق حلوان للدراسات القانونية والاقتصادية*، مصر، ع (٢٢)، ص ص ١٠-٢١٢.

الصقر، ممدوح شحات (٢٠١٠م). أمن المعلومات. *أعمال ندوة مكافحة الجريمة عبر الإنترنت، وورشة عمل أمن المعلومات والتوقيع الإلكتروني*، المنظمة العربية للتنمية الإدارية، القاهرة، محكمة، ص ص ١٤٣-١٨٠.

العوضي، عبدالهادي فوزي (٢٠١٥م). الحق في الدخول في طي النسيان على شبكة الإنترنت: دراسة قانونية تطبيقية مقارنة. *مجلة القانون والاقتصاد*، كلية الحقوق، جامعة القاهرة، مصر، علمية محكمة، مج (٨٥)، ص ص ٣١٣-٤٦٣.

غنيم، ريهام عاصم (٢٠١٠م). المعلومات الشخصية المتاحة على الويب العام: دراسة في إمكانية الوصول وأخلاقيات الاستخدام. *بحث منشور ضمن بحوث مؤتمر المحتوى العربي في الإنترنت (التحديات الطموح)*، مج (٢)، جامعة الإمام محمد بن سعود الإسلامية، الرياض، ص ص ١١٣٩-١١٧٣.

منصور، عصام محمد رشيد (سبتمبر ٢٠٠٩م). قوانين حماية خصوصية الأطفال على الإنترنت: قراءة في القانون الأمريكي COPPA مع استعراض للموقف العربي من مثل هذه القوانين. *مجلة دراسات المعلومات*، علمية محكمة، ع (٦)، ص ص ١٣١-١٦٣.

(د) رسائل علمية

صالح، مروة زين العابدين (٢٠١٦م). *الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني*. رسالة دكتوراه منشورة، مركز الدراسات العربية للنشر، القاهرة.

محمد، عربي السيد عبدالسلام (٢٠٠٨م). *أحكام تقدير التعويض وأثر تغير القوة الشرائية للنقود على تقديرها: دراسة مقارنة*. رسالة دكتوراه، كلية الحقوق، جامعة أسيوط.

ثانياً: المراجع باللغة الفرنسية

(a) Ouvrages Généraux

Geneviève Viney: Introduction à la responsabilité, 3e édition, Editeur: L.G.D.J, 2008.

Patrice Jourdain, Geneviève Viney: Traité de droit civil, Les conditions de la responsabilité Dommage, fait générateur, régimes spéciaux, causalité, 4e édition, Editeur: L.G.D.J, 2013.

Suzanne Carval, Patrice Jourdain, Geneviève Viney: Les effets de la responsabilité, 4e édition, Editeur : L.G.D.J, 2017.

(b) Ouvrages spéciaux

A.BELLEIL:E-privacy: le marché des données personnelles: protection de la vie privée à l'âge d'Internet, Dunod, 2001.

David Dechenaud : Le droit à l'oubli numérique, Données nominatives –Approche comparée, Larcier - Création Information Communication,1re édition, Parution, 2015.

Sandrine Carneroli : Le droit à l'oubli, Du devoir de mémoire au droit à l'oubli, 1re édition, Editeur: Larcier, 2016.

(c) Articles

Antoinette Rouvroy : « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? » in La sécurité de l'individu numérisé, Réflexions prospectives et internationales, S. Lacour (dir.), L'Harmattan 2010.

Christian Charriere-Bournazel, « Propos autour d'Internet : l'histoire et l'oubli », Gazette du Palais, 21 avril 2011 n°111, p.6 Gazette du Palais, 21 avril 2011. Voir aussi Agathe Lepage, «Droit à l'oubli : une Jurisprudence tâtonnante », Recueil Dalloz 2001.

Emmanuel DECAUX : « La protection de la vie privée au regard des données informatiques », Revue électronique Droits fondamentaux, n° 7, janvier 2008 – décembre 2009.

Etienne Quillet : Le droit à l'oubli numérique sur les réseaux sociaux, mémoire, dir. E. Decaux, 2011

Linda Maizener, membre du conseil d'administration de l'Association des jeunes magistrats Tout le dommage, rien que le dommage ? Gaz. Pal. 24 juill. 2018 .

Maryline Boizard : Le droit à l'oubli; Faculté de droit et de science politique, Rennes 1 Institut de l'Ouest : Droit et Europe IODE UMR CNRS 6262 Recherche réalisée avec le soutien de la Mission de recherche Droit et Justice Février 2015.

Roseline LETTERON « Le droit à l'oubli », Revue du droit public, 1996.

(d) Thèses

Charlotte HEYLLIARD: Le droit à l'oubli sur Internet. Mémoire de Master 2 recherche, Mention DNP. le 4 juin 2012.

Nathalie WALCZAK : La protection des données personnelles sur l'internet ; Thèse de doctorat en Sciences ; Thèse de doctorat en Sciences de l'information et de la communication ; univ-lyon2, 2014.

(e) Rapports

Commission des lois du Senat ; « Vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information » Rapport d'information de M. Yves DÉTRAIGNE et Mme AnneMarie ESCOFFIER, fait au nom de la commission des lois, n° 441 (2008-2009), 27 mai 2009, adoptée le 23 mars 2010.

Jacques Le Rider : Oubli, mémoire, histoire dans la « Deuxième Considération inactuelle »

Y. POULLET, J.-M. DINANT, avec la collaboration. de C. de TERWANGNE ET M.-V. PEREZ-ASINARI : «L'autodétermination informationnelle à l'ère de l'Internet », Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

ثالثاً: المراجع باللغة الإنجليزية

Mayer-Schönberger, Viktor (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 237 p.

رابعاً: المواقع الإلكترونية

- http://apdfanswer.blogspot.com/2015/02/Amnesia.htm l
- http://journals.openedition.org/rgi/725
- http://www.accronline.com/article_detail.aspx?id=195 02
- http://www.cnil.fr/la-cnil/actu-cnil/article/article/reseaux-sociaux-quelles-sont-les-pratiques-de-nosenfants-quel-est-le-role-des-parents/?tx_ttnews[backPid]=2&cHash=66639ddc7d
- http://www.france24.com/ar
- http://www.who.int/mediacentre/factsheets/fs362/ar
- https://ar-ar.facebook.com/privacy/explanation/
- https://nakedsecurity.sophos.com/ar/2018/03/28/cambr idge-analyticas-secret-coding-sauce-allegedly-leaked/

- https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5
- https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
- https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
- https://www.gazette-du-palais.fr/article/GPL329s3/
- https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-pontoise-6eme-chambre-2-collegiale tribunal de grande instance de Pontoise 6ème chambre2, 2 février 2005.
- https://www.nytimes.com/2018/03/27/us/cambridge-analytica-palantir.html
- https://www.senat.fr/notice-rapport/2008/r08-441-notice.html
- https://rm.coe.int/16806ae51f
- https://th2plant.blogspot.com/2018/04/FBUsers-Violate.html
- https://www.apple.com/sitemap/
- https://www.captaincontrat.com/articles-gestion-entreprise/limites-protection-donnees-personnelles-salarie
- https://www.cnil.fr/en/cnils-missions
- https://www.cnil.fr/en/official-texts
- https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee
- https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
- https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
- https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article8