

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك نموذجًا"

Personal Data Protection Policy For Social Media Users "Facebook as a Model"

♦ قرور شهيناز

جامعة ألكلي محمد أولحاج البويرة/ الجزائر

مخبر الدولة والاعلام المنظم: مقاربات اقتصادية واجتماعية

c.kerour@univ-bouira.dz

تاريخ النشر: 2026/06/30

تاريخ القبول: 2026/06/25

تاريخ الإرسال: 2026/02/24

الملخص:

تعد البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي ملكاً لصاحبها، لا يحق للغير نشرها وتداولها إلا بالحصول على موافقة صريحة منه، غير أن سهولة الوصول إليها عبر هذه المنصات الرقمية جعل من الصعب تحقيق هذا الشرط عملياً، ما استدعى تدخل العديد من التشريعات كالمشرع الجزائري، لوضع إطار قانوني يكفل حماية خصوصية المستخدمين. كما يمكن للأفراد تعزيز الحماية الوقائية لبياناتهم من خلال الالتزام بسياسات الخصوصية المعتمدة في مختلف المواقع. وتبرز أهمية هذه الحماية بصفة خاصة في مواجهة الاستخدامات الإعلانية والتجارية، أين قد يُساء استخدام البيانات أثناء معالجتها، مما يفرض قانوناً للحفاظ على سريتها وسلامتها، وضمان عدم المساس بخصوصية أصحابها.

الكلمات المفتاحية: المستخدم، حماية البيانات الشخصية، مواقع التواصل الاجتماعي، الفيسبوك، الحق في الخصوصية.

Abstract:

Personal data of social media users belongs to its owner; others do not have the right to publish or circulate it except with explicit consent from the owner. However, the ease of access to this data through these digital platforms has made it practically difficult to achieve this condition, which necessitated the intervention of many legislations, such as the Algerian legislator, to establish a legal framework that guarantees the protection of users' privacy.

♦ المؤلف المرسل

Individuals can also enhance the preventive protection of their data by adhering to the privacy policies adopted on these various sites. The importance of this protection is especially evident in the face of advertising and commercial uses, where data may be misused during processing, legally requiring the maintenance of its confidentiality and integrity, and ensuring that the privacy of its owners is not violated.

Keywords: user, personal data protection, social media, Facebook, right to privacy.

مقدمة:

بدأت مواقع التواصل الاجتماعي في الظهور أواخر تسعينات القرن الماضي، وشهدت انتشاراً متسارعاً مع مطلع الألفية الجديدة، نتيجة الزيادة المطردة في أعداد المستخدمين حول العالم¹، حيث تُعرّف هذه المواقع بأنها شبكات الكترونية قائمة عبر الانترنت، تتيح للمستخدمين التواصل فيما بينهم داخل الفضاء الافتراضي، من خلال تبادل اهتماماتهم وأفكارهم المشتركة، سواء كانت ذات طابع شخصي- أو عام، من خلال منشورات، صور، مقاطع فيديو، محادثات، أو علاقات تعارف.

ولكي يتمكن المستخدم من التسجيل على المواقع التواصل الاجتماعي، يطلب منه تقديم عدد من المعلومات الشخصية، التي تدرج ضمن ملفه الشخصي- (profil) الذي يتيح له كذلك التعبير عن ميوله وآرائه ومختلف بياناته الاجتماعية من خلال نشاطه داخل الموقع.

وقد سجلت هذه المواقع ازدياداً ملحوظاً في عدد مستخدميها، حيث تجاوز عدد مستخدمي "فيسبوك" حاجز الملياري شخص، في حين بلغ عدد مستخدمي "إنستغرام" 800 مليون، وأكثر من مليار مستخدم لتطبيق "واتساب". وكنتيجة لهذا الاستخدام المكثف، أصبحت المنصات تولّد كمّاً ضخماً من البيانات، وصل إلى ما يقارب 2.5 إكسابايت (Exabyte) من البيانات في الدقيقة الواحدة².

غير أن هذه الأرقام الهائلة رافقتها تصاعد في حجم الانتهاكات المرتكبة ضد خصوصية المستخدمين، إذ لم تعد هذه المنصات تقتصر على دورها الأساسي في التواصل والتعارف، بل تحولت إلى أدوات لجمع البيانات واستغلالها في أغراض تجارية أو إعلانية، ما أثار العديد من المخاوف بشأن أمن البيانات الشخصية التي يُفصح عنها المستخدم.

¹ أحمد قاسمي، سليم جددي، تأثير مواقع التواصل الاجتماعي على الأمن المجتمعي للدول الخليجية، الطبعة الأولى، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2019، ص 18.

² منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية -أهم الأمان وحقوق الأفراد، الطبعة الأولى، المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان، 2018، ص 12.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك" نموذجاً

وعليه، وأمام هذه المخاطر المتزايدة، ظهرت الحاجة الملحة إلى حماية الحياة الخاصة للمستخدمين، ما دفع العديد من الدول إلى دسترة هذه الحماية¹، ومن بينها الجزائر، حيث نص الدستور الجزائري² في مادتيه 39 و47 على حماية الحياة الخاصة، واعتبار البيانات الشخصية حقاً أساسياً يُعاقب القانون على المساس به.

كما عُرِثَ هذه الحماية بإصدار قوانين خاصة³ مماثلة للتشريع الأوروبي، كقانون رقم 07-18 الذي أصدره المشرع الجزائري المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي⁴، بهدف تنظيم حقوق الأفراد، وضمان سيطرتهم على بياناتهم وحماية خصوصية معلوماتهم، والحد من الجرائم الإلكترونية، كالتهريب، الابتزاز، اختراق الأنظمة، وسرقة الأسرار المهنية والتجارية. كما يُسهم هذا الإطار القانوني في تعزيز ثقة المستخدمين وتمكينهم من استخدام هذه المنصات بأمان واطمئنان.

من هنا تبرز أهمية دراسة موضوع حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي باعتباره من أبرز التحديات المعاصرة التي تمس الحياة اليومية للأفراد. وللتنبية إلى خطورة الإدلاء عن البيانات الشخصية، ومعالجة سبل حمايتها تطرح الإشكالية الآتية: كيف يتم ضمان حماية البيانات الشخصية للمستخدم على مواقع التواصل الاجتماعي، لاسيما الفيسبوك باعتباره الموقع الأكثر استخداماً؟

¹ أقرت بعض الدول العربية في دساتيرها على كفاية حماية الحياة الخاصة، مثل المشرع المصري الذي كرسها في المادة 45 من دستوره وجرم كل اعتداء عليها في المادة 57. كما نص المشرع القطري على هذا الحق في المادة 37 من دستوره، بينما أقر الدستور التونسي في المادة 24 على ضمان الحق في الخصوصية. أنظر: منى الأشقر جبور، محمود جبور، المرجع السابق، ص 26.

² مرسوم رئاسي رقم 20-442 مؤرخ في 30 ديسمبر 2020 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج.ر. العدد 82، الصادر بتاريخ 30 ديسمبر 2020.

³ أقرت فرنسا القانون رقم 77-78 المتعلق بالمعلوماتية والملفات والحريات بتاريخ 6 جانفي 1978، والذي خضع للتعديل سنة 2004. كما أصدرت النمسا بتاريخ 18 أكتوبر 1978 القانون الفيدرالي لحماية المعطيات، الذي تم تعديله سنة 1986 قبل أن يلغى ويُعوض بقانون حماية المعطيات لسنة 2000. وفي السياق ذاته، تبنت فنلندا في 30 أبريل 1987 قانون ملفات المعطيات ذات الطابع الشخصي، الذي غُيِّل سنة 1995 ثم ألغى سنة 1999 ليحل محله قانون حماية المعطيات الشخصية. أما المملكة المتحدة فقد أصدرت بتاريخ 12 جويلية 1988 قانوناً يتعلق بحماية المعطيات، ثم أتبع ذلك بإصدار قانون آخر سنة 1998. وبالنسبة لإسبانيا، فقد اعتمدت في 29 أكتوبر 1992 قانوناً ينظم المعالجة الآلية للمعطيات الشخصية، والذي تم تعويضه سنة 1999 بالقانون الأساسي لحماية المعطيات ذات الطابع الشخصي. ولم يقتصر التنبية التشريعي لحماية المعطيات ذات الطابع الشخصي على دول الاتحاد الأوروبي فحسب، بل امتد ليشمل دولاً أوروبية من خارجه، مثل الزوج التي انتهجت توجه نفسه من خلال إصدار قانون سنة 1978، تم تعديله بتاريخ 14 أبريل 2000، إضافة إلى سويسرا التي أصدرت قانونها الفيدرالي سنة 1992. أما على الصعيد الدولي، فقد اعتمدت كندا قانونها الفيدرالي لحماية المعلومات الشخصية سنة 1982، كما تبنت كل من الولايات المتحدة الأمريكية والأرجنتين تشريعات خاصة بحماية المعطيات، من بينها القانون الأرجنتيني الصادر في 2 نوفمبر 2000. أنظر: توي يحيى، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء قانون رقم 07-18 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، المجلد 04، العدد 02، 2019، ص 1523.

⁴ قانون رقم 07-18 مؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر. العدد 34 الصادر في 10 جوان 2018 معدل ومتمم بقانون رقم 25-11 مؤرخ في 24 جويلية 2025، ج.ر. العدد 48 صادر بتاريخ 24 جويلية 2025.

قرار شهيناز

للإجابة على الإشكالية المطروحة يتم الاعتماد على المنهج الوصفي التحليلي من خلال عرض وتحليل كافة جوانب الموضوع والنصوص القانونية ذات الصلة. كما يقسم البحث إلى شقين، بحيث يُعالج الشق الأول خصوصية حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي، بينما يُخصص الشق الثاني لدراسة حماية المستخدم من المخاطر الناجمة عن معالجة هذه البيانات.

1- خصوصية حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي

شهد العالم خلال عام 2017 طفرة هائلة في حجم البيانات المنتجة، تجاوزت في كثافتها مجموع ما تم إنتاجه عبر التاريخ البشري بأكمله، وذلك نتيجة الارتفاع الكبير في استخدام مواقع التواصل الاجتماعي¹. وقد فرض هذا الواقع الجديد ضرورة الوعي بأهمية حماية هذه البيانات، إذ يُعد الحفاظ على خصوصية المعلومات الشخصية حقًا أساسيًا لكل فرد، مع العلم أن حماية البيانات الشخصية لا تقتصر - على الجانب التشريعي - فحسب، بل تمتد لتشمل أيضًا وعي المستخدم ودوره في تأمين بياناته الشخصية.

1.1- حماية البيانات الشخصية من حيث المفهوم وشروط الإقرار

نظرًا لكون حماية البيانات الشخصية من أهم الإشكاليات القانونية المعاصرة، خاصة في ظل ما أفرزه التطور المتسارع لتكنولوجيا المعلومات من تحديات، وما صاحبه من توسع في نطاق المعالجة الآلية للبيانات، بات من الضروري التطرق إلى مفهوم حماية البيانات الشخصية، كما يقتضي - الأمر كذلك بيان الشروط الواجب توافرها لتكريس هذه الحماية قانونًا وتمكين الأفراد من الانتفاع بها فعليًا.

1.1.1- حماية البيانات الشخصية بوصفها مرادفًا لخصوصية معلومات المستخدم

يُطلق على مصطلح "البيان" في اللغة الإنجليزية لفظ (Data) وفي اللغة الفرنسية عبارة (Donné)، ويقصد به من الناحية التقنية الفنية، كل تمثيل يمكن أن تُخزّن فيه المعلومات، سواء أكان نصًا، جدولًا، رسمًا بيانيًا، صورة، رمزًا، إشارة، أو أي شكل آخر قابل للمعالجة².

أما من الناحية القانونية، فقد عرّف المشرع الجزائري البيانات الشخصية تحت مسمى "المعطيات ذات الطابع الشخصي" في المادة 3 من القانون رقم 07-18 المشار إليه سابقًا³، بأنها: كل معلومة، مهما كانت دعما، تتعلق بشخص مُعرّف أو قابل للتعرف عليه، سواء بصفة مباشرة أو غير مباشرة، لاسيما بالاستناد إلى رقم تعريف أو عنصر أو مجموعة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

¹ مني الأشقر جبور، محمود جبور، المرجع السابق، ص 11.

² مباركة مفيدة، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، المجلد 07، العدد 01، 2018، ص 462.

³ قانون رقم 07-18، المصدر السابق.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك" نموذجاً

يتوافق هذا التعريف بشكل كبير مع ما ورد في عدد من المرجعيات الدولية، مثل التعريف الذي أوردته كل من: اللجنة الوطنية للمعلوماتية والحريات الفرنسية (CNIL)¹، واتفاقية مجلس أوروبا رقم 108²، وكذلك التوجيه الأوروبي رقم 95-46³، بالإضافة إلى القانون الفرنسي - رقم 801-2004 المتعلق بحماية البيانات الشخصية⁴.

يلاحظ من خلال استقراء هذه التعاريف، أن حماية البيانات الشخصية تخص فقط الشخص الطبيعي دون المعنوي وهو ما يعكسه بوضوح القانون الجزائري لحماية المعطيات ذات الطابع الشخصي. فرغم أن الأشخاص الاعتباريين (كالشركات والمؤسسات) يجوزون بدورهم بيانات قد تنسم بطابع حساس، إلا أن الحماية القانونية في معظم التشريعات، ومنها التشريع الجزائري، لا تزال مقتصرة على الأشخاص الطبيعيين فحسب. لكن ربما مع التطور المتسارع في مجال حماية المعطيات، قد نشهد مستقبلاً توسيع نطاق هذه الحماية لتشمل الكيانات الاعتبارية، خاصة تلك التي تعتمد على قواعد بيانات ضخمة⁵.

كما يُستخلص من التعاريف السابقة أن البيانات الشخصية تنقسم إلى نوعين: يمثل النوع الأول في البيانات الشخصية المحددة للهوية، والتي تنقسم بدورها إلى صنفين منها ما يتعلق بالحروف والأرقام والرموز والتي تتمثل أهمها في كلمات المرور التي تسمح أو تمنع المستخدم من الولوج إلى الحاسوب الشخصي - أو إلى البريد الإلكتروني أو إلى الحساب الشخصي على الموقع الإلكتروني أو تسجيل الدخول في منتدى...، ومنها ما يتعلق بالقياسات الحيوية، على غرار بصمة الأصبع، البصمة القرحية، البصمة الصوتية، بصمة أبعاد الكف، خط اليد (التوقيع)، وبصمة الوجه...إلخ.

¹ تنص المادة 02 من قانون 06 يناير 1978 المتعلق بالمعلوماتية، الملفات والحريات، الصادر عن اللجنة الوطنية للمعلوماتية والحريات (Commission Nationale de l'informatique et des Libertés - CNIL)، على ما يلي: "كل معلومة تتعلق بشخص طبيعي محدد الهوية أو قابل للتعرف على هويته بشكل مباشر، سواء بالرجوع إلى رقم تعريف أو إلى عنصر واحد أو مجموعة عناصر تخصه".

Loi n° 78_17 du 06 janvier 1978, modifiée le 06 aout 2004. Voir le site: www.legifrance.gouv.fr

² Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens n° 108, Strasbourg, 28.01.1981.

تنص المادة 02 من اتفاقية حول حماية الأشخاص المتعلقة بالمعالجة الآلية للبيانات الشخصية، المجلس الأوروبي رقم 108، ستراسبورغ، 1981، على ما يلي: "كل المعلومات المتعلقة بشخص طبيعي معرف أو قابل للتعرف عليه".

³ تنص المادة 02 من التوجيه الأوروبي رقم 95-46 الصادر بتاريخ 24 أكتوبر 1995 بأن المعطيات ذات الطابع الشخصي هي: "كل معلومة متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه، يعد قابل للتعرف عليه (الشخص المعني)، الذي يمكن معرفته، بصفة مباشرة أو غير مباشرة لاسمًا بالرجوع إلى رقم التعريف أو إلى عنصر أو عدة عناصر خاصة مميزة لهويته الطبيعية الفيزيولوجية النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

⁴ L'Article 02 de La Loi n° 04-108 qui protège les données personnelles stipule: "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".

⁵ لوكال مريم، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 801-2004، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 10، العدد 01، 2019، ص 1309.

قرور شهيناز

أما النوع الثاني فيتعلق بالبيانات الشخصية الخاصة (المحسوبة على البيانات الحساسة) والتي تشمل إما معلومات مرتبطة بالعرق، الدين، الآراء السياسية، أو البيانات التي من شأنها الكشف عن الحالة الصحية، الحياة الجنسية، أو السجل العدلي، وغيرها من البيانات سواء كانت مخزنة لدى الهيئات العامة أو الخاصة في شكل قواعد بيانات، أو محفوظة على خوادم الشبكات المعلوماتية. بما في ذلك المواد الإعلامية المنشورة عبر مواقع التواصل الاجتماعي¹.

انطلاقاً مما سبق ذكره، يتضح إن البيانات الشخصية على مواقع التواصل الاجتماعي تظهر بشكل واضح، بدءاً من المعلومات التي يُطلب من المستخدم إدخالها عند التسجيل مثل: الاسم الكامل، الجنس، تاريخ الميلاد، البريد الإلكتروني، رقم الهاتف، كلمة المرور ووصولاً إلى ما يمكن إضافته لاحقاً من معلومات مهنية، تعليمية، أو تفضيلات شخصية.

وقد تسمح بعض المنصات، مثل "فيسبوك"، بمشاركة معلومات أكثر خصوصية تتعلق مثلاً بالتوجهات الفكرية والدينية، الاهتمامات السياسية، أو تفاصيل الحياة الخاصة، وهذا يزيد من حجم البيانات الحساسة المعرضة للاستخدام أو الاستغلال².

إن البيانات الشخصية لا تقتصر -على هذه المعلومات فحسب، بل تُنتج تطبيقات التفاعل والمراسلة الفورية، كـ "سناب شات"، "واتساب"، و"لينكدان"، كميات ضخمة من البيانات في كل دقيقة. فمثلاً، تُرسل أكثر من 527 ألف صورة عبر "سناب شات" (Snapchat)، وتُسجل منصة "لينكدان" (Linked in) أكثر من 120 حساباً جديداً، ويُنشر -على "تويتر" (twitter) حوالي 456 ألف تغريدة، ويُسجل "غوغل" (google) أكثر من 3.6 مليون عملية بحث في الدقيقة³.

هذا الواقع يبرز مدى تعقيد البيئة الرقمية التي تُنتج فيها هذه البيانات، لاسيما وأن هذه الأرقام الهائلة لكمية البيانات الشخصية تواجها في الجهة المقابلة خطر الانكشاف أو الاستغلال نتيجة اختراقات إلكترونية، تسريب من داخل الشركات، أو سوء استخدام من قبل منصات التواصل ذاتها، التي تعتمد على نماذج تجارية مبنية على تحليل سلوك المستخدم واستهدافه إعلانياً⁴. لذا، فإن الغرض الأساسي من حماية هذه البيانات هو

¹ مباركية مفيدة، المرجع السابق، ص 463-464.

² أشرف جابر سيد، خالد بن عبد الله الشافي، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع الفيسبوك -دراسة مقارنة في ضوء النظام السعودي-، مجلة الدراسات القانونية والاقتصادية، جامعة حلوان مصر، 2013، ص 05. مقال منشور في موقع: opac.cndl.ma

³ Big Data Statistics & Facts for 2017, <https://www.waterfordtechnologies.com/big-data-interesting-facts/>

نقلا عن: منى الأشقر جبور، محمود جبور، المرجع السابق، ص 12.

⁴ المرجع نفسه، ص 19.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك"

نموذجاً

تمكين المستخدم من التحكم الكامل في خصوصيته، أي أن يقرر بنفسه "متى، وكيف، وإلى أي مدى" يمكن للغير - سواء كانوا أفراداً أو شركات - الوصول إلى معلوماته الشخصية¹.

ومن ثم، فإن حماية البيانات الشخصية في مواقع التواصل الاجتماعي، تستند إلى حرية الفرد في إدارة بياناته، بما يتضمنه من حق في التعبير، الإخفاء، أو التحكم بالوصول، وهو ما يعني حماية خصوصية معلوماته. وعليه، فإن حماية بيانات مستخدمي هذه المواقع تُعد في جوهرها حماية للخصوصية المعلوماتية، مما يبرز وجود ترادف عام بين مفهومي حماية البيانات وخصوصية المعلومات². وبغض النظر عن المصطلح المستخدم، يبقى لكل فرد الحق في عدم التدخل في شؤونه الخاصة، وحقه في اختيار الكيفية التي يعبر بها عن ذاته ورغباته وتصرفاته، في إطار الإمكانيات التقنية التي توفرها هذه المواقع³، غير أن ضمان الحماية القانونية لهذا الحق يظل متوقفاً على توافر شروط محددة يقرها القانون.

2.1.1- شروط خضوع البيانات الشخصية للحماية القانونية

لكي يستفيد الشخص من الحماية القانونية المنصوص عليها في المادة 3 من القانون رقم 18-07 المشار إليه سابقاً، فلا بد بالإضافة إلى شرط أن يكون الشخص طبيعي كما سبق التطرق له، أن يكون هذا الشخص أيضاً محدداً أو قابلاً للتحديد، سواء بشكل مباشر من خلال اسمه، لقبه، عنوانه، موطنه...أو بشكل غير مباشر الذي يرتبط في الغالب بالتقنيات الحديثة مثل رقم الهاتف أو عنوان البريد الإلكتروني أو رقم بطاقة الائتمان أو صوته أو بصمات الإصبع أو الحمض النووي أو حتى البيانات البيومترية...، بالمعنى المخالف إذا كانت هذه البيانات متعلقة بشخص مجهول فلا محل للحديث عن حمايتها؛ لأن المجهول لا تثبت له خصوصية⁴.

يستخلص أنه بتوافر هاذين الشرطين تقرر للمستخدم بطبيعة الحال الحماية المنصوص عليها في القوانين الخاصة بالبيانات الشخصية، لكن رغم أهمية الأطر التشريعية والتنظيمية في حماية هذه البيانات، غير أنها يمكن أن تكون أضيق من استيعاب جميع الحلول الممكنة، لتأمين حماية أفضل، لاسيما أمام التطورات المتسارعة للتكنولوجيا. ما يدعو إلى الاعتماد على الحماية القبلية من طرف المستخدم التي يمكن أن تأخذ مكانها إلى جانب هذه القوانين.

¹ تومي فضيلة، إديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، مجلة الباحث في العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح ورقلة، المجلد 09، العدد 30، 2017، ص 44.

² منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، جامعة بغداد، العراق، عدد خاص بحوث المؤتمر العلمي الدولي الثامن للكلية، 2013، ص 306.

³ رائد محمد فليح نمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على ضوء التشريعات في مملكة البحرين، عدد خاص بالملتقى الدولي المحكم حول: الخصوصية في مجتمع المعلوماتية، مركز جيل البحث العلمي، طرابلس، لبنان، العدد 26، 2019، ص 91.

⁴ أشرف جابر سيد، خالد بن عبد الله الشافي، المرجع السابق، ص 05.

2.1- دور المستخدم في حماية بياناته الشخصية عبر مواقع التواصل الاجتماعي

تُعَدُّ حماية البيانات الشخصية على مواقع التواصل الاجتماعي مسؤولية مشتركة بين القائمين على هذه المنصات والمستخدمين أنفسهم. فعند إنشاء حساب على أي من هذه المواقع، يُطلب من المستخدمين الموافقة على نوعين من السياسات الأساسية: سياسة إعدادات الخصوصية (Privacy Settings Policy)، وسياسة الاستخدام (Usage Policy)، اللتان تشكلان إطارًا تنظيميًا يهدف إلى حماية البيانات الشخصية من التسرب أو الاستغلال غير المشروع.

1.2.1- أهمية سياسة الخصوصية في تمكين المستخدم من تعزيز حماية بياناته الشخصية

تُعنى سياسة إعدادات الخصوصية بتوضيح طبيعة البيانات التي يتم جمعها من المستخدم، وطرق استخدامها وتخزينها، والجهات التي يمكن أن تُشارك معها، فضلاً عن تحديد كيفية التحكم في عرض هذه البيانات للغير. كما تُتيح بعض المنصات للمستخدمين إمكانية تعزيز مستوى الخصوصية أو رفض بعض بنود هذه السياسة¹.

وفي هذا السياق، يتضمن موقع الفيسبوك أقسامًا متعددة في إعدادات الخصوصية من بينها المعلومات الشخصية، وإعدادات الأمان وتسجيل الدخول، وتخصيص الإعلانات، وإعدادات الإشعارات، والوسائط وجهات الاتصال، وغيرها من الخصائص التي تُمكن المستخدم من إدارة خصوصيته على نحو أفضل.

يتبين من خلال استعراض هذه الإعدادات أن تطبيق الفيسبوك يتيح أدوات متعددة لتمكين المستخدم من تخصيص تجربته الرقمية، والحد من انكشاف بياناته، كتفعيل خاصية التنبيهات المتعلقة بتسجيلات الدخول غير المعروفة، وتحديد من يمكنه مشاهدة منشوراته، أو الوصول إلى ملفه الشخصي، أو التفاعل معه، بالإضافة إلى إمكانية تحميل نسخة من البيانات أو حذف الحساب بشكل نهائي.

غير أن فعالية هذه الأدوات تبقى محدودة بسبب ضعف استغلالها من قبل المستخدمين، إذ تشير بعض الدراسات إلى أن 33% فقط من المستخدمين الذين شملهم الاستطلاع يقومون بتعيين إعدادات الخصوصية²، في حين يغفل الغالبية العظمى عنها، إما بسبب الجهل بوجودها أو نتيجة عدم الوعي الكافي بكيفية استخدامها.

يمكن القول إن مواقع التواصل الاجتماعي، وفي مقدمتها الفيسبوك، توفر الإطار التقني، بينما يبقى المستخدم هو الطرف الفاعل الذي يملأ هذا الإطار ببياناته الشخصية، وغالبًا ما يتم ذلك دون وعي كامل للعواقب المترتبة

¹ سارة الشريف، خصوصية البيانات الرقمية، مركز دعم لتقنية المعلومات، القاهرة، د.س.ن، ص 04.

² حفيظة سليمان أحمد البراشدية، الفيسبوك والجرائم الإلكترونية في عان: هل هناك علاقة؟، مجلة دراسات المعلومات والتكنولوجيا، دار جامعة حمد بن خليفة للنشر، عان، 2019، ص 08.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك"

نموذجاً

على إعادة استخدام هذه البيانات¹، فقد يتم فهرستها ونشرها واستغلالها، في كثير من الأحيان، دون تمكن صاحبها من ممارسة حقوقه عليها بشكل كامل.

وقد ثبت أن الفيسبوك يجمع كلاً هائلاً من البيانات الذي يمكنه من معرفة تفاصيل دقيقة عن حياة المستخدمين وميولهم، وهو ما يتجلى في طبيعة الأسئلة التي يطرحها على مستخدميه، مثل: ماذا في ذهنك الآن؟ ما الجديد اليوم؟ بما تفكر؟ وغيرها من الأسئلة التي تتجاوز مجرد التواصل الاجتماعي إلى السعي لفهم ميول المستخدم ورصد تفاصيل حياته اليومية، بما يسمح ببناء ملف شخصي - دقيق عنه، يمكن استغلاله في استهدافه بالإعلانات أو الأخبار أو انضمامه إلى مجموعات معينة².

ورغم تأكيد الفيسبوك على عدم بيع البيانات الشخصية بشكل مباشر، إلا أن تقارير متعددة تشير إلى أنه يبيع الملف التعريفي (profil) للمستخدمين لشركات التسويق الإلكتروني مقابل مبالغ مالية لا تتجاوز في بعض الحالات خمسة دولارات³، أو بمنح شركات الإعلانات "حق الوصول" إلى هذه البيانات⁴، وهو ما يسمح باستثمار هذه البيانات لأغراض تجارية، ولو بصفة غير مباشرة.

وعليه، فإن حماية البيانات الشخصية على مواقع التواصل الاجتماعي، ولا سيما الفيسبوك، تتطلب من المستخدم توخي الحذر في نوعية المعلومات التي يشاركها، نظراً للمخاطر الناجمة عن إنشاء ملف تعريف يعتمد على بيانات يتم جمعها بوسائل متعددة، مثل ملفات تعريف الارتباط (Cookies)، والتصيد الاحتيالي الإلكتروني، وسرقة الهوية، والبرمجيات الخبيثة⁵، بل وحتى من خلال التفاعلات البسيطة كاستخدام زر الإعجاب (j'aime). وبصرف النظر عن ذلك، فإنه يمكن للمستخدم الحد من تسرب بياناته أيضاً عبر الالتزام بسياسة الاستخدام.

¹ تسعى مواقع التواصل الاجتماعي إلى تحقيق غرض تجاري رئيسي يتمثل في تسويق البيانات ذات الطابع الشخصي التي يقوم المستخدمون بإدخالها على المنصة. ويبرز موقع فيسبوك كمثال على ذلك، إذ يعتمد على تنوع مصادر دخله، بما في ذلك الإعلانات المستهدفة من نوع الدفع بالنقرة (PPC) والإعلانات المدعومة (sponsor) بالإضافة إلى متجر الهدايا والنقود الافتراضية المعروفة باسم "نقود فيسبوك". مع العلم أن الفيسبوك يوفر نوعين رئيسيين من الإعلانات، وهما الإعلانات الاجتماعية والإعلانات الدليلية أو الإرشادية، اللتان تعززان من فعالية التسويق واستغلال البيانات الشخصية لأغراض تجارية. أنظر: أشرف جابر، استهداف مستخدمي الانترنت بالإعلانات التجارية وحماية الحق في الخصوصية، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، عدد خاص، 2015، ص 16.

² أشرف جابر، المرجع السابق، ص 16.

³ عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، المجلد 11، العدد 76، 2021، ص 18.

⁴ منى الأشقر جبور، محمود جبور، المرجع السابق، ص 34.

⁵ للمزيد من التفاصيل أنظر: محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي -دراسة مقارنة-، مجلة كلية الشريعة والقانون بطنطا، جامعة الأزهر، المجلد 04، العدد 33، ص 1964-1967.

2.2.1- أهمية الالتزام بسياسة الاستخدام في صون البيانات الشخصية للمستخدم

توضح أهمية سياسة الاستخدام التي لا تقل شأنًا في حماية البيانات عن سياسة الخصوصية، القواعد المنظمة لاستخدام الموقع، وما هو مسموح به أو محظور، والعقوبات المترتبة على المخالفات، كإيقاف الحساب أو حذفه¹. ويُعد قبول المستخدم بهذه السياسة بمثابة إقرار قانوني بالالتزام بمضمونها، الأمر الذي يجعله طرفًا فاعلاً في حماية بياناته الشخصية، ويُحمّله مسؤولية أي تصرف قد يؤدي إلى تعريضها للخطر.

وبالرجوع إلى سياسة الاستخدام في فيسبوك، نجد أنها مدرجة ضمن قسم السياسات والشؤون القانونية، تشمل طبيعة الخدمات المقدمة، ومصادر تمويلها، والالتزامات المستخدم، إضافة إلى شروط إضافية. غير أن هذه السياسة، عادة ما تُكتب بخط صغير وغير جذاب، ما يجعل كثيرًا من المستخدمين يتجاوزونها دون الاطلاع عليها أو فهم مضمونها، الأمر الذي يُضعف من فعاليتها في تحقيق الحماية المرجوة للبيانات الشخصية.

ومن الملاحظ كذلك أن سياسة الاستخدام تشترط ألا يقل عمر المستخدم عن ثلاثة عشر (13) سنة²، غير أن الواقع يبيّن انتشار حسابات لأطفال دون هذا السن، نتيجة إدخال تواريخ ميلاد غير صحيحة. ويكشف هذا الوضع عن خطورة مضاعفة في مجال حماية البيانات لاسيما عندما يشارك المستخدم القاصر إلى جانب بياناته الشخصية، معلومات تخص أفراد أسرته، مثل عنوان السكن أو البريد الإلكتروني أو رقم الهاتف³.

وفي هذا السياق، لا يمكن إلقاء عبء الحماية على المستخدم وحده، بل تتحمل المنصات الرقمية مسؤولية تبسيط سياسة الاستخدام وجعلها أكثر وضوحًا وجاذبية، مع اعتداد لغة مفهومة تراعي مختلف الفئات العمرية، وخاصة فئة القُصّر. كما تبرز أهمية الرقابة الأبوية بوصفها آلية مكملّة لسياسة الاستخدام، تسهم في توجيه سلوك الطفل الرقمي والحد من المخاطر التي قد يتعرض لها نتيجة سوء استعمال المنصات الاجتماعية.

وعليه، يمكن القول إن إحاطة حساب المستخدم بالحماية الكافية تستوجب الاطلاع على كل من سياستي الخصوصية والاستخدام، لفهم الحقوق والالتزامات، وتفادي استغلال بيانات الآخرين أو التعدي على حساباتهم، بما قد يؤدي إلى إيقاف الحساب أو إلغائه. كما ينبغي للمستخدم اعتماد كلمات مرور قوية ومختلفة، وعدم مشاركتها مع الآخرين، وتجنب الاتصال بالشبكات الاجتماعية عبر الأماكن العامة، وعدم الاستجابة للرسائل التي تطلب بيانات شخصية⁴.

وبذلك، يستطيع المستخدم توفير قدر من الحماية الوقائية لبياناته الشخصية من خلال الحيلة والحذر واتباع التدابير الوقائية المشار إليها. ومع ذلك، يمكن أن تبقى هذه البيانات عرضة لبعض المخاطر أثناء مرحلة معالجتها.

¹ سارة الشريف، المرجع السابق، ص 04.

² هذا الشرط موجود في خانة شروط الخدمة في تطبيق الفيسبوك

³ أشرف جابر سيد، خالد بن عبد الله الشافي، المرجع السابق، ص 05.

⁴ محمد أحمد المعداوي، المرجع السابق، ص 1977.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك"

نموذجاً

2- حماية المستخدم من مخاطر معالجة البيانات الشخصية

تعتبر معالجة البيانات الشخصية من أخطر المراحل التي تهدد خصوصية معلومات المستخدم، لما قد ينجم عنها من تسرب للمعلومات أو استغلالها بأساليب احتيالية ولأغراض غير مشروعة. الأمر الذي دفع معظم التشريعات، ومن بينها المشرع الجزائري إلى إيلاء اهتمام خاص بتنظيم هذه العملية، من خلال وضع إطار قانوني يحدد مفهوم معالجة البيانات الشخصية وشروط ممارستها، إضافة إلى تحديد الجهة المسؤولة عن هذه المعالجة والالتزامات القانونية الملقاة على عاتقها.

1.2- مفهوم معالجة البيانات الشخصية

خَصَّ القانون رقم 07-18 المشار إليه سابقاً، أحكاماً واضحة لتنظيم عملية معالجة البيانات الشخصية، لاسيما من خلال تعريفها، ووضع جملة من الشروط والضوابط التي يتعين احترامها عند القيام بهذه المعالجة، وفقاً لما يضمن تحقيق التوازن بين التطور التكنولوجي وحماية الحياة الخاصة.

1.1.2- تعريف معالجة البيانات الشخصية

عزت المادة الثالثة الفقرة الثالثة (03/03) من القانون رقم 07-18 المشار إليه سابقاً، معالجة البيانات ذات الطابع الشخصي- بأنها: كل عملية أو مجموعة من العمليات التي تُنجز، سواء بوسائل آلية أو غير آلية، وتنصب على معطيات شخصية، كالجمع¹ أو التسجيل² أو التنظيم أو الحفظ³ أو الملاءمة أو التعديل أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو الإتاحة بأي شكل آخر، أو التقريب أو الربط البيئي⁴، فضلاً عن الإغلاق أو التشفير أو المسح أو الإتلاف.

ويُستشف من هذا التعريف الواسع أن المشرع الجزائري لم يقيّد مفهوم المعالجة بوسيلة معينة، بل جعله شاملاً لكل الأساليب، سواء كانت تقنية حديثة أو يدوية تقليدية، وهو ما يعكس إرادته الصريحة في إخضاع جميع صور التعامل مع البيانات الشخصية لنظام الحماية القانونية، دون الأخذ بعين الاعتبار الأداة المستعملة. كما أن

¹ يقصد بجمع البيانات العملية التي يتم من خلالها استرجاع البيانات الشخصية، ويتم هذه العملية بطرق متعددة، مثل استخدام المواقع الإلكترونية، أو الاعتماد على الكوكيز، أو عبر التطبيقات المختلفة. ويشترط في هذه العملية أن تكون مرتبطة بشخص محدد فقط، مع ضرورة الحصول على موافقة صريحة منه قبل جمع بياناته.

² يعد التسجيل المرحلة التالية بعد جمع البيانات، ويتم عن طريق إدخال هذه البيانات في قاعدة بيانات، سواء كانت إلكترونية أو تقليدية، لتخزينها وتنظيمها بشكل يسهل الوصول إليها ومعالجتها لاحقاً.

³ تتم عملية الحفظ بعد جمع البيانات الشخصية، حيث يصبح من الضروري تحديد مدة زمنية واضحة لتخزينها، والالتزام بهذه المدة وفق ما نص عليه

اللائحة العامة لحماية البيانات (RGPD – Règlement Général sur la Protection des Données).

⁴ نصّت المادة 17/03 من القانون رقم 07-18 المشار إليه سابقاً على أن "الربط البيئي للمعطيات" هو كل شكل من أشكال المعالجة التي تقوم على إحداث علاقة أو ترابط بين معطيات خاضعة للمعالجة من أجل غاية محددة، سواء مع معطيات أخرى يحتفظ بها مسؤول أو عدة مسؤولين آخرين عن المعالجة، أو مع معطيات يحتفظ بها نفس المسؤول، سواء لنفس الغرض أو لأغراض مختلفة.

قرور شهيناز

اعتماد أسلوب التعداد غير الحصري يدل على رغبة المشرّع في استيعاب أي أساليب مستحدثة قد تفرزها التطورات التكنولوجية المستقبلية، بما يمنع التحايل على القانون أو التهرب من أحكامه.

وبناءً عليه، فإن أي تصرف يطلال البيانات الشخصية، أيًا كانت طبيعته أو غايته، يُعدّ معالجاً بالمعنى القانوني، وهو ما يكرّس توجهاً وقائياً يهدف إلى تعزيز حماية الحياة الخاصة للأفراد والحد من الاستعمال غير المشروع لمعطياتهم الشخصية.

ويتكامل هذا المفهوم مع ما جاءت به المادة الثانية (02) من القانون رقم 07-18، التي أوجبت أن تتم معالجة المعطيات ذات الطابع الشخصي، مهما كان مصدرها أو شكلها، في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، وألاّ تمس بحقوق الأشخاص أو شرفهم أو سمعتهم. ويقابل هذا التوجه ما نصت عليه المادة الثامنة (08) من قانون المعلوماتية الفرنسي، التي ذهبت إلى حظر جمع أو معالجة البيانات الشخصية التي من شأنها الكشف، بصورة مباشرة أو غير مباشرة، عن الأصول العرقية، أو الآراء السياسية أو الفلسفية، أو المعتقدات الدينية، أو الاتناء النقابي، أو تلك المتعلقة بالصحة أو بالحياة الجنسية للشخص.

ومن خلال المقارنة بين النصين، يتبيّن أن المشرّع الجزائري اعتمد مقارنة مرنة تقوم على إرساء مبادئ عامة تحكم عملية معالجة البيانات الشخصية، في حين انتهج المشرّع الفرنسي أسلوباً أكثر صرامة، من خلال الحظر الصريح لمعالجة أنواع معينة من البيانات الحساسة. ويعكس هذا التباين اختلافاً في التقنية التشريعية ومستوى التفصيل، مع وحدة الغاية المتمثلة في حماية الإنسان وحقوقه الأساسية في العصر الرقمي، لاسيما من خلال اشتراط مشروعية جمع البيانات الشخصية، باعتبار أن كل جمع يتم بطرق غير مشروعة يُعدّ محظوراً ولا يُعتدّ به قانوناً.

وفي إطار هذه الدراسة، تتجلى معالجة البيانات في مواقع التواصل الاجتماعي من خلال جمع¹ وحفظ ثلاثة أنواع رئيسية من البيانات، تتمثل في البيانات الشخصية للمستخدمين، وبيانات الاتصال بالإنترنت مثل عناوين بروتوكول الإنترنت (IP)، إضافة إلى بيانات التصفح المرتبطة بالمواقع والصفحات التي يترادها المستخدم.

وبالاستناد إلى ذلك، يُعد موقع فيسبوك (Facebook) مثالاً بارزاً لمعالجة البيانات الشخصية، إذ يُعتبر مالك المنصة شخصاً مرخصاً له بالوصول إلى بيانات المستخدمين. وبالتالي، فإن كل ما يقوم به من عمليات جمع أو تسجيل أو تخزين أو تصنيف أو غيرها من الأفعال التي ترد على البيانات التي يقدمها المستخدمون يندرج، من حيث المبدأ، ضمن مفهوم معالجة البيانات الشخصية. غير أن الترخيص الممنوح لا يعني بالضرورة مشروعية جميع صور المعالجة، إذ أثبتت الوقائع المرتبطة بمسألة مالك فيسبوك على خلفية قضايا استغلال البيانات

¹ تعتمد مواقع التواصل الاجتماعي على عدة مصادر رئيسية في جمع البيانات، من أبرزها أساليب استخدام تقنيات الإنترنت المختلفة، وتقنيات ملفات تعريف الارتباط (Cookies) والبريد الإلكتروني غير المرغوب فيه، إضافة إلى حالات تسرب أو فقدان البيانات الشخصية. للمزيد من التفصيل أنظر: عثمان بكر عثمان، المرجع السابق، ص ص 13-15.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك" نموذجاً

الشخصية أن المعالجة قد تتم بطرق غير قانونية، حتى من قبل الجهة المرخص لها¹، وهو ما يؤكد أن الترخيص لا ينفى إمكانية قيام المسؤولية القانونية متى تم تجاوز الضوابط والشروط التي قررها القانون.

2.1.2- شروط معالجة البيانات الشخصية

حتى تنقسم عملية معالجة البيانات الشخصية بالمشروعية وتتم في إطار قانوني سليم، أقر القانون رقم 07-18 على توافر مجموعة من الشروط الأساسية، يمكن إجمالها فيما يلي:

__ **الحصول على الموافقة الصريحة للشخص المعني بالبيانات**² باعتبارها الركيزة الأساسية لمشروعية المعالجة. أما إذا كان الشخص عديم الأهلية أو ناقصها، فيخضع التعبير عن الموافقة للقواعد العامة المنظمة للأهلية. ويترتب على هذا الشرط تمكن الشخص المعني من جملة من الحقوق، من بينها حقه في سحب موافقته في أي وقت، فضلاً عن ضمان سرية معطياته الشخصية ومنع اطلاع الغير عليها دون مسوغ قانوني³.

__ **أن تتم معالجة البيانات الشخصية بطريقة مشروعة ونزيهة**، بما يستبعد أي أساليب احتيالية أو مضللة في جمع البيانات أو استعمالها.

__ **أن يتم جمع البيانات الشخصية لتحقيق غايات محددة ومشروعة**، على أن تُعالج لاحقاً بما يتوافق مع هذه الغايات، دون الانحراف عنها أو استعمالها لأغراض تتنافى مع الهدف الذي جُمعت من أجله.

__ **أن تكون البيانات الشخصية ملائمة ومتناسبة وغير مفرطة** بالنظر إلى الغايات المرجوة من جمعها أو معالجتها، بحيث لا يجوز لأي جهة مطالبة الأفراد ببيانات غير ضرورية أو لا تتناسب مع الغرض المحدد للمعالجة.

__ **وجوب اتسام البيانات الشخصية بالدقة**، أي أن تكون صحيحة وكاملة ومحيطة كلما اقتضت الضرورة ذلك، بما يمنع اعتماد بيانات مغلوطة قد تضر بالشخص المعني.

__ **تحديد مدة الاحتفاظ بالبيانات الشخصية**، بحيث لا يجوز الاحتفاظ بها لمدة تتجاوز الفترة اللازمة لتحقيق الأغراض التي جُمعت أو عولجت من أجلها⁴.

¹ The key moments from Mark Zuckerberg's testimony to Congress
<https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments>
- This is how Facebook uses your data for ad targeting
<https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg>.

نقلا عن: منى الأشقر جبور، محمود جبور، المرجع السابق، ص 30.

² عرفت المادة 04/03 من القانون رقم 07-18 المشار إليه سابقاً "الموافقة الصريحة للشخص المعني بالبيانات" بأنها: كل تعبير عن الإرادة المبررة يدي بموجبه الشخص المعني أو ممثله الشرعي قبوله بمعالجة المعطيات الشخصية المتعلقة به بطريقة يدوية أو إلكترونية.

³ غزال نسرين، حماية الأشخاص الطبيعيين في مجال المعطيات ذات طابع الشخصي، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة الجزائر، المجلد 56، العدد 01، 2019، ص 120.

⁴ راجع المواد 07، 08، 09 من قانون 07-18، المصدر السابق.

قرور شهيناز

وبإسقاط هذه الشروط على أحد أبرز مواقع التواصل الاجتماعي، وهو موقع فيسبوك، يتبين أن المستخدم عند رغبته في إنشاء حساب يعبر، من حيث المبدأ، عن رضاه الحر من خلال الإجابة على مجموعة من الأسئلة الأساسية، مثل الاسم، اللقب، تاريخ الميلاد، الجنس، رقم الهاتف أو البريد الإلكتروني، وكلمة السر. كما يُمنح المستخدم حرية حذف بعض هذه البيانات أو إخفاءها أو الامتناع عن تقديمها، مما يدل على أن تقديم المعطيات يتم ظاهرياً، بناءً على إرادة واعية وبعد الاطلاع على شروط الاستخدام وسياسة الخصوصية المعتمدة من قبل الموقع¹.

قد يبدو للوهلة الأولى أن البيانات التي يطلبها فيسبوك عند إنشاء الحساب، تندسم بالملائمة وعدم المبالغة فيها بالنظر إلى الغاية من معالجتها. غير أنه في الحقيقة بعد إنشاء الحساب، قد يلجأ الموقع إلى استدراج المستخدمين عبر أسئلة، أو ألعاب، أو تطبيقات ترفيهية تبدو غير مهمة، إلا أنها في الواقع تُشكل وسيلة غير مباشرة لجمع كم كبير من البيانات، يستغلها الموقع لاحقاً لأغراض إعلانية وتسويقية، مقابل إتاحة خدماته مجاناً للمستخدمين الذين لا يتفطنون لها؛ لأنهم يخضونها من باب التسلية فقط².

وفي هذا الإطار، يتعين على موقع فيسبوك، بصفة خاصة، وعلى مواقع التواصل الاجتماعي بصفة عامة، الالتزام بمبادئ الأمانة والمشروعية في جمع البيانات الشخصية ومعالجتها، والتقيّد الصارم بالغاية التي جُمعت من أجلها هذه البيانات، وعدم التوسع في جمعها أو استعمالها بما يتجاوز هذا الغرض. كما يجب عليهم ضمان سرية البيانات وحمايتها من أي استعمال غير مشروع، وتمكين المستخدم من حق الاطلاع على بياناته الشخصية وتصحيحها في أي وقت³، فضلاً عن ممارسة حقه في الاعتراض⁴ على تداول بياناته الشخصية عبر شبكة الإنترنت⁵.

2.2- المسؤول عن معالجة البيانات الشخصية في مواقع التواصل الاجتماعي والتزاماته القانونية

لا يقتصر الأمر على استيفاء الشروط السابقة فحسب، لكي تتم معالجة البيانات الشخصية على مواقع التواصل الاجتماعي بطريقة مشروعة وسليمة، بل يتعين أيضاً تحديد المسؤول عن هذه المعالجة، مع بيان الالتزامات الملزمة على عاتقه وفقاً لأحكام القانون رقم 07-18 المشار إليه سابقاً.

¹ أشرف جابر سيد، خالد بن عبد الله الشافي، المرجع السابق، ص 07.

² محمد أحمد المعداوي، المرجع السابق، ص 1972.

³ حق المستخدم في التصحيح منصوص عليه في المادة 35 من قانون رقم 07-18، المصدر السابق.

⁴ حق المستخدم في الاعتراض منصوص عليه في المادة 36 من قانون رقم 07-18، المصدر السابق. للمزيد من التفصيل حول الحقوق الممنوحة للمستخدم أنظر: تومي يحيي، المرجع السابق، ص 1532-1533.

⁵ راند محمد فليح نمر، المرجع السابق، ص 95.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك" نموذجاً

1.2.2- تعيين المسؤول عن معالجة البيانات الشخصية في مواقع التواصل الاجتماعي

يستوجب تحديد المسؤول عن معالجة البيانات الشخصية في مواقع التواصل الاجتماعي الإجابة عن التساؤل الآتي: هل تتحمل مواقع التواصل الاجتماعي وحدها مسؤولية معالجة البيانات الشخصية، أم أن المستخدم يشاركها هذه المسؤولية؟

للإجابة عن هذا التساؤل، لابد من الرجوع إلى تعريف "مسؤول المعالجة" الوارد في المادة 12/03 من القانون رقم 07-18، التي عرفته بأنه: "كل شخص طبيعي أو معنوي، عمومي أو خاص، أو أي كيان آخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد غايات معالجة المعطيات ووسائلها".

ويتضح من هذا التعريف أنه يتقارب إلى حد كبير مع التعريف الوارد في التوجيه الأوروبي رقم 95-46، ولا سيما في المادة الثانية منه¹، حيث أخذ هذا الأخير بفكرة المسؤولية المشتركة (co-responsabilité) بين إدارة الموقع والمستخدم، على أساس أن إدارة الموقع لا تُعد وحدها مسؤولة عن معالجة البيانات، لأن دورها يقتصر - على توفير وسائل المعالجة دون تحديد أغراضها، في حين أن المستخدم هو من يقرر إدراج بياناته الشخصية أو تعديلها وتحديد الغاية من معالجتها، الأمر الذي يقتضي - اعتباره بدوره مسؤولاً عن المعالجة. وقد أكدت هذا الاتجاه اللجنة الوطنية للمعلوماتية والحريات (CNIL) في نشرتها الصادرة سنة 2005، حين اعتبرت أن المدون يُعد مسؤولاً عن معالجة البيانات².

غير أن هذا الطرح، وإن كان يجد سنده في التعريف القانوني لمسؤول المعالجة، يبقى محل نقاش؛ لأن مجرد قيام المستخدم بإدراج بياناته الشخصية أو الإفصاح عنها لا يكفي لاعتباره مسؤولاً عن معالجتها، مادام لا يملك سلطة فعلية على وسائل المعالجة التقنية ولا على كيفية تخزين البيانات أو مشاركتها أو إعادة استخدامها. فالعبرة، في هذا المجال، لا تتعلق بالفعل المادي للإفصاح عن البيانات، وإنما بمدى التحكم الحقيقي في مسار المعالجة والمخاطر الناجمة عنها.

زيادة على ذلك، لاعتبار المستخدم مسؤولاً عن المعالجة، ينبغي التمييز بين استعمال المستخدم لحساباته على مواقع التواصل الاجتماعي لأغراض شخصية محضة، وبين استعمالها في إطار نشاط منظم ذي طابع مهني أو تجاري أو إعلامي كما هو الحال بالنسبة لأصحاب الصفحات والمجموعات. فإذا كانت الحالة الأولى، يصعب القول معها بقيام مسؤولية قانونية عن المعالجة، نظرًا لغياب الطابع الاحترافي والتنظيمي، فإنه في الحالة الثانية يمكن،

¹ نصت المادة 02 من التوجيه الأوروبي رقم 95-46 على ما يلي: "الشخص الطبيعي أو المعنوي، أو سلطة عامة أو مرفق عام، أو أي هيئة أخرى يتولى وحده أو بالاشتراك مع الغير، تحديد أغراض ووسائل معالجة البيانات ذات الطابع الشخصي".

² أشرف جابر سيد، خالد بن عبد الله الشافي، المرجع السابق، ص 10.

قرور شهيناز

على سبيل الاستثناء، اعتبار المستخدم مسؤولاً عن المعالجة متى ثبت أنه يحدد بصورة مستقلة أغراض ووسائل معالجة بيانات الغير، لا مجرد بياناته الشخصية.

وفي هذا الصدد، نرى أنه رغم الدور الذي يلعبه المستخدم في معالجة بياناته الشخصية باعتباره من يقوم بالإفصاح عنها، فإن الدور الرئيسي- والأساسي يظل منوطاً بإدارة مواقع التواصل الاجتماعي، ذلك أن معالجة البيانات الشخصية تنطوي على مخاطر جسيمة، وهو ما دفع التشريعات الحديثة إلى تخصيص قواعد خاصة لحمايتها، قصد صون حقوق وحرّيات الأفراد.

من ناحية أخرى، تتسم العلاقة بين المستخدم وإدارة مواقع التواصل الاجتماعي بعدم التكافؤ، سواء من حيث المعرفة التقنية أو القدرة على التحكم في البيانات، وهو ما يجعل تحميل المستخدم عبء المسؤولية القانونية أمراً يتنافى مع فلسفة قوانين حماية البيانات، التي تقوم أساساً على حماية الطرف الأضعف في علاقة المعالجة. فمن غير المتصور، في الغالب، أن يُقدّم المستخدم العادي على استغلال بياناته الشخصية أو بيانات غيره لأغراض غير مشروعة، في حين تملك إدارة مواقع التواصل الاجتماعي الإمكانيات التقنية والقدرة الفعلية على جمع البيانات وتحليلها واستثمارها لأغراض متعددة، تجارية أو إعلانية أو غيرها. ويعزز هذا الرأي ما تفرضه القوانين من التزامات مشددة على عاتق مسؤول المعالجة.

2.2.2- الالتزامات المفروضة على إدارة مواقع التواصل الاجتماعي

نظراً لما تنطوي عليه معالجة البيانات الشخصية من مخاطر متعددة، ألقى المشرّع الجزائري على عاتق مسؤول معالجة البيانات الشخصية جملة من الالتزامات، وذلك بموجب أحكام القانون رقم 07-18 المشار إليه سابقاً، ويمكن إجمال هذه الالتزامات فيما يأتي:

__الالتزام بتأمين سلامة المعالجة: يقصد بهذا الالتزام وجوب قيام مسؤول المعالجة باتخاذ التدابير التقنية والتنظيمية المناسبة الكفيلة بحماية البيانات الشخصية من مختلف المخاطر التي قد تهددها، ولاسيما مخاطر الإلتفاف العرضي أو غير المشروع، أو الضياع، أو التلف، أو النشر، أو الولوج غير المرخص به، خاصة في الحالات التي تستوجب فيها المعالجة نقل البيانات عبر الشبكات الإلكترونية، فضلاً عن حمايتها من أي شكل من أشكال المعالجة غير المشروعة. ويتعين أن تضمن هذه التدابير مستوى ملائماً من السلامة، يتناسب مع طبيعة البيانات المراد حمايتها والمخاطر التي تنطوي عليها عملية المعالجة¹.

وفي هذا الإطار، يلاحظ أن بعض مواقع التواصل الاجتماعي، وعلى رأسها موقع فيسبوك، قد تبنت سياسات تتعلق بأمن وسلامة المستخدمين، حيث تتضمن إعدادات الخصوصية قسماً خاصاً بالسلامة يتيح للمستخدمين الاطلاع على سبل حماية أنفسهم وعائلاتهم أثناء استخدام المنصة، من خلال زيارة مركز السلامة، والاطلاع على الموارد الموجهة للآباء، والآليات المخصصة للحد من المضايقات.

¹ المادة 38 من قانون رقم 07-18، المصدر السابق.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "فيسبوك" نموذجاً

وبصرف النظر عن ذلك، يتعين على مسؤول المعالجة، في حال استعان بمعالج من الباطن¹ لتنفيذ المعالجة لحسابه، أن يختار هذا الأخير بعناية، وأن يحرص على أن يتصرف وفقاً لتعليماته، مع تقديم ضمانات كافية فيما يتعلق باتخاذ إجراءات السلامة التقنية والتنظيمية اللازمة، والسهر على احترامها².

وبناءً عليه، فإن التزام مسؤول معالجة البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي بتأمين سلامة المعالجة يُعد شرطاً أساسياً لتوفير الحماية القانونية لهذه البيانات، لاسيما في ظل تزايد المخاطر المرتبطة بالاعتداء عليها من قبل أشخاص غير مرخص لهم بالاطلاع عليها، وما قد ينجم عن ذلك من تعديل البيانات أو إفشائها. وقد أكدت محكمة العدل الأوروبية هذا التوجه في القضية المتعلقة بشركة ألمانية قامت بالترويج لخدمات التدريب والتعليم عبر صفحة أنشأتها على موقع فيسبوك، مستفيدة من الأدوات المجانية التي يتيحها الموقع لمديري الصفحات، والتي تسمح بجمع بيانات إحصائية عن زوار الصفحة، مثل السن والجنس. ويتم جمع هذه البيانات بواسطة ملفات تعريف الارتباط (Cookies) يحمل كل منها رمز مستخدم فريداً، ويظل نشطاً لمدة عامين، ويتم تخزينه على القرص الصلب لأجهزة الزوار أو على أي وسيلة تخزين أخرى.

وقد اعتبرت محكمة العدل الأوروبية أن شركة فيسبوك تُعد مسؤولة عن معالجة البيانات الشخصية التي تم جمعها، كما انتهت إلى اعتبار مدير الصفحة مسؤولاً بدوره، على أساس أنه يستفيد من المنصة والخدمات التي تقدمها، ومن ثم لا يمكن إعفاؤه من الالتزامات القانونية المتعلقة بحماية البيانات الشخصية. وهو ما كرسته المحكمة في حكمها الصادر بتاريخ 5 جوان 2018، حيث قضت بقيام مسؤولية تضامنية بين فيسبوك ومدير أو مشرف الصفحة عن معالجة بيانات المستخدمين الخاصة بهذه الصفحة³.

وبناءً على ذلك، يحق للشخص المتضرر من معالجة بياناته الشخصية أن يرفع دعوى قضائية ضد مدير صفحة فيسبوك، كما يمكنه كذلك مقاضاة الشركة التابعة لفيسبوك في الدولة المعنية.

¹ عرفته المادة 03 من قانون رقم 07-18، المصدر السابق، بأنه كل: "شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة".

² المادة 39 من القانون نفسه.

³ Voir : _ CJUE , le 5 juin 2018 , L'administrateur d'une page fan sur Facebook est conjointement responsable avec Facebook du traitement des données des visiteurs de sa page, l'affaire C-210/16, Luxembourg, COMMUNIQUE DE PRESSE n° 81-18.

_ La société allemande Wirtschaftsakademie Schleswig-Holstein est spécialisée dans le domaine de l'éducation. Elle offre des services de formation au moyen notamment d'une page fan hébergée sur Facebook.

_ Les administrateurs de pages fan, tels que la Wirtschaftsakademie, peuvent obtenir des données statistiques anonymes sur les visiteurs de ces pages à l'aide d'une fonction intitulée Facebook Insight, mise gratuitement à leur disposition par Facebook selon des conditions d'utilisation non modifiables. Ces données sont collectées grâce à des fichiers témoins («cookies») comportant chacun un code utilisateur unique, actifs pendant deux ans et sauvegardés par Facebook sur le disque dur de l'ordinateur ou sur tout autre support des visiteurs de la page fan. Le code utilisateur, qui peut être mis en relation avec les données de connexion des utilisateurs enregistrés sur Facebook, est collecté et traité au moment de l'ouverture des pages fan.

نقلا عن: محمد أحمد المعداوي، المرجع السابق، ص 1994-1995.

قرور شهيناز

__ **الالتزام باحترام سرية المعالجة:** يتمثل هذا الالتزام في ضرورة التزام مسؤول المعالجة، والمعالج من الباطن، وكافة الأشخاص الذين يطلعون بحكم مهامهم على البيانات الشخصية، باحترام السر- المهني، وعدم إفشاء هذه البيانات، حتى بعد انتهاء مهامهم، وذلك تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول¹.

وعليه، يتعين على مسؤول معالجة البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي الالتزام باحترام سرية المعالجة، ولاسيما من خلال صون خصوصية رسائل واتصالات المستخدمين، وضمان عدم الاطلاع عليها أو استغلالها دون سند قانوني.

خاتمة:

أصبحت شبكات التواصل الاجتماعي تلعب دورًا محوريًا في ربط المستخدمين بعضهم ببعض داخل الفضاء الرقمي، من خلال إتاحة إمكانية إنشاء حسابات شخصية يُعبر الأفراد عبرها عن آرائهم وأفكارهم بواسطة التعليقات والمنشورات والرسائل والاتصالات الإلكترونية. غير أن الدور الذي تؤديه هذه الشبكات في تشكيل العلاقات الاجتماعية الرقمية يظل مرتبطًا بأهدافها وغاياتها، إذ تقوم هي نفسها بفرض شروط وقواعد الاستخدام، وتوجه المستخدم نحو أنماط محددة من العلاقات الاجتماعية في سياق رقمي يختلف عن الواقع الفعلي، من خلال اقتراح الأصدقاء وتوسيع دوائر المعارف، بل ودفع المستخدم إلى التعرف على أصدقاء أصدقائه، الأمر الذي يجعل هذا الأخير في وضعية خضوع نسبي لسياسات هذه المنصات بما يخدم مصالحها الخاصة.

وإلى جانب ذلك، تقوم مواقع التواصل الاجتماعي، ولاسيما موقع فيسبوك، باستغلال البيانات والمعلومات الشخصية لمستخدميها لأغراض تجارية، عبر مشاركتها أو إتاحتها للغير، مما يؤدي إلى تضخم حجم المعلومات المتداولة والمتاحة للشركات والأفراد على حد سواء، وهو ما قد يفضي- إلى المساس بخصوصية الأشخاص وانتهاك بياناتهم الشخصية.

ومن هذا المنطلق، ولغرض توفير حماية فعالة للبيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي، لاسيما فيسبوك، يتعين أن يكون الشخص المعني محددًا أو قابلاً للتحديد، سواء بشكل مباشر أو غير مباشر، وألا يقل عمره عن ثلاث عشرة (13) سنة، فضلًا عن ضرورة تمتعه بالوعي الكافي بطبيعة المعلومات التي يقوم بالإفصاح عنها، مع توخي الحيلة والحذر إزاء المخاطر المترتبة على ذلك.

كما ينبغي عليه عدم ترك البيانات أو التعليقات منشورة بشكل عام، بل تقييد الاطلاع عليها من خلال تفعيل إعدادات الخصوصية المناسبة، إلى جانب تفعيل خاصية التنبيه بشأن محاولات تسجيل الدخول غير المعروفة، واعتماد كلمات مرور قوية ومتنوعة وعدم مشاركتها مع الغير، وتجنب الولوج إلى الحسابات عبر الشبكات

¹ المادة 40 من قانون رقم 07-18، المصدر السابق.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك"

نموذجاً

العامّة، وعدم الاستجابة للرسائل الإلكترونية التي تطلب بيانات شخصية، فضلاً عن ضرورة الاطلاع المسبق على سياسات الاستخدام والالتزامات المترتبة عنها.

غير أن هذه التدابير الفردية، رغم أهميتها، لا تكف وحدها لتحقيق حاية فعالة، ما لم تتم معالجة البيانات الشخصية وفقاً للشروط والمبادئ التي كرسها القانون رقم 07-18، مع التزام إدارة مواقع التواصل الاجتماعي، بصفتها مسؤولة عن المعالجة، باحترام مبدأي سلامة المعالجة وسريتها.

ومن خلال دراسة هذا الموضوع، تم التوصل إلى جملة من النتائج، من أبرزها:

— يمكن للبيانات الشخصية المتداولة عبر مواقع التواصل الاجتماعي أن تشكل وسيلة من وسائل الإثبات، سواء من خلال تقديم الرسائل الإلكترونية أو الصور أو مقاطع الفيديو المستخرجة من المحادثات، أو عبر تقنية لقطة الشاشة (capture d'écran)، غير أن ذلك يستوجب على الجهات المختصة اعتماد آليات تقنية وقانونية كفيلة بالتحقق من مصداقية وأصالة هذه الأدلة، ضماناً لفعاليتها في مجال الإثبات القضائي.

— إن فتح حساب على مواقع التواصل الاجتماعي يقتضي موافقة المستخدم على شروط خدمة معدة مسبقاً من قبل هذه المواقع، دون إمكانية مناقشتها أو تعديلها، الأمر الذي يجعل العلاقة التعاقدية بين الطرفين تأخذ طابع عقد الإذعان.

— إن قبول المستخدم لشروط الخدمة، سواء عن وعي أو بدونه، ولا سيما في ظل لجوء أغلب المستخدمين إلى الموافقة السريعة دون الاطلاع على مضمونها طولها وتعقيدها، يترتب عليه في كثير من الأحيان السماح باستغلال بياناته الشخصية، خاصة البيانات الديمغرافية، من قبل المعلنين، مما يعرض خصوصيته للانتهاك، رغم ما تروّج له هذه المنصات من خلال ما يُعرف بسياسات إعدادات الخصوصية، التي قد توهم المستخدم بوجود حاية كافية لبياناته.

ورغم أن المشرّع الجزائري قد نظم عملية معالجة البيانات الشخصية بموجب القانون رقم 07-18، من خلال إقرار شروط والتزامات واضحة على عاتق مسؤول المعالجة، إلا أن البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي تظل عرضة للاستغلال والانتهاك، لا سيما من قبل الجهات التجارية التي توظفها في مجالات الإعلان والتسويق.

وانطلاقاً مما سبق، ومن أجل تعزيز حاية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي وصون خصوصية معلوماتهم، يمكن اقتراح ما يلي:

— توسيع نطاق الحماية القانونية للبيانات الشخصية في قانون رقم 07-18 بشكل لا يقتصر على الشخص الطبيعي بل يمتد ليشمل أيضاً الأشخاص المعنويين.

قرور شهيناز

__ العمل على تكوين مواطنين ملمين بالتقنيات الرقمية الحديثة، وقادرين على التحكم في بياناتهم الشخصية وخصوصيتهم، من خلال تنظيم حملات تحسيسية ودورات تكوينية تشرح آليات عمل هذه المواقع ومخاطرها وطرق الاستخدام الآمن لها.

__ إلزام مواقع التواصل الاجتماعي وعلى رأسها فيسبوك بتقديم سياسي استخدام وخصوصية بشكل مختصر وواضح، مع شرح مبسط لطبيعة البيانات التي تجمع وكيفية استخدامها، وعدم تفعيل جمع البيانات إلا بعد موافقة صريحة من المستخدم.

__ حصر - جمع البيانات في المعلومات الضرورية فقط لتقديم الخدمة، ومنع جمع البيانات الحساسة أو تتبع السلوك دون سبب مشروع وواضح.

__ تفعيل آليات تطبيق قوانين حماية البيانات الشخصية، من خلال التحقيق في الانتهاكات المحتملة للخصوصية وفرض الجزاءات القانونية كلما اقتضى الأمر ذلك.

__ ضرورة إخضاع مواقع التواصل الاجتماعي، عند معالجتها للبيانات الشخصية، لقواعد تقنية وقانونية موحدة وفعالة، بما يضمن حماية حقيقية ومستدامة لخصوصية المستخدمين.

قائمة المراجع:

1/القوانين

__ مرسوم رئاسي رقم 20-442 مؤرخ في 30 ديسمبر 2020 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج.ر العدد 82، الصادر بتاريخ 30 ديسمبر 2020.

__ قانون رقم 07-18 المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر العدد 34 صادر في 10 جوان 2018، معدل ومتمم بقانون رقم 25-11 المؤرخ في 24 جويلية 2025، ج.ر العدد 48 صادر بتاريخ 24 جويلية 2025.

2/الكتب

__ أحمد قاسمي، سليم جدي، تأثير مواقع التواصل الاجتماعي على الأمن المجتمعي للدول الخليجية، الطبعة الأولى، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2019.

__ منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية -أهم الأمن وحقوق الأفراد، الطبعة الأولى، المركز العربي للبحوث القانونية والقضائية، بيروت، لبنان، 2018.

3/المقالات

__ أشرف جابر سيد، خالد بن عبد الله الشافي، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع الفيسبوك _دراسة مقارنة في ضوء النظام السعودي_، مجلة الدراسات القانونية والاقتصادية، جامعة حلوان مصر، 2013. مقال منشور في موقع: opac.cndl.ma

__ تومي فضيلة، إيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، مجلة الباحث في العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح ورقلة، المجلد 09، العدد 30، 2017.

سياسة حماية البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي "الفيسبوك"

نموذجاً

- تومي يحيى، الحماية القانونية للمعطيات ذات الطابع الشخصي- على ضوء قانون رقم 18_07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، المجلد 04، العدد 02، 2019.
- حفيظة سليمان أحمد البراشدية، الفيسبوك والجرائم الالكترونية في عمان: هل هناك علاقة؟، مجلة دراسات المعلومات والتكنولوجيا، دار جامعة محمد بن خليفة للنشر، عمان، 2019.
- عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي مواقع التواصل الاجتماعي، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، المجلد 11، العدد 76، 2021.
- غزال نسرين، حياة الأشخاص الطبيعيين في مجال المعطيات ذات طابع الشخصي، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة الجزائر، المجلد 56، العدد 01، 2019.
- لوكال مريم، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي- في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية والسياسية، جامعة الشهيد الحامة لخضر- الوادي، المجلد 10، العدد 01، 2019.

- مباركة مفيدة، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، المجلد 07، العدد 13، 2018.
- محمد أحمد العدداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي _دراسة مقارنة_، مجلة كلية الشريعة والقانون بطنطا، جامعة الأزهر، المجلد 4، العدد 33، 2018.
- منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، جامعة بغداد، العراق، عدد خاص ببحوث المؤتمر العلمي الدولي الثامن للكلية، 2013.

4/المداخلات

- رائد محمد فليح نمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على ضوء التشريعات في مملكة البحرين، عدد خاص بالملتقى الدولي المحكم حول: الخصوصية في مجتمع المعلوماتية، مركز جيل البحث العلمي، طرابلس، لبنان، العدد 26، 2019.
- سارة الشريف، خصوصية البيانات الرقمية، مركز دعم تقنية المعلومات، القاهرة، دس.ن.

5/ المصادر باللغة الفرنسية

Loi:

— Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des traités européens n° 108, Starsbourg, 28.01.1981.

— Loi n° 78_17 du 06 janvier 1978, modifiée le 06 aout 2004. Voir le site: www.legifrance.gouv.fr