حماية المعطيات الشخصية في قلب تحديات الأمن السبراني

آمنة ثامر أحمد الجراية*

DOI:10.15849/ZJJLS.240330.26

* **قسم القانون الخاص، كلية الحقوق، جامعة صفاقس، تونس.**

* للمراسلة: emna25jarraya@gmail.com

الملخص

تتناول هذه المقالة موضوع حماية المعطيات الشخصية من حيث صلتها بالأمن السيبراني. والواقع أن كمية وسرعة إنشاء البيانات الرقمية وتخزينها مستمرة في التزايد بشكل كبير. في حين أن معظم البيانات غير مهمة، إلا أن كمية كبيرة منها تحتوي على معلومات حساسة ويجب حمايتها. وبالتالي، يجب اعتماد تدابير هامة للأمن السبراني لضمان حماية المعطيات الشخصية .ومن منطق الشروط إلى منطق الآثار، نظرا لهذه التغيرات التكنولوجية يجب على المشرع أن يأخذها بعين الاعتبار لمنع الاستهانة بتجارة هذه المعلومات. الهدف هو بناء نهج نقدي وتواصلي للتشريعات السيبرانية الخاصة بحماية المعطيات الشخصية في العصر الرقمي و ضمان أمان الإنترنت.

الكلمات الدالة: التشريعات السيبرانية؛ حماية المعطيات الشخصية؛ الأمن السبراني

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

Protection of Personal Data at the Heart of Cybersecurity Challenges

Emna Thameur Jarraya*

***Department of private Law, Faculty of Law, university of sfax, Tunisia**

*** Crossponding author: emna25jarraya@gmail.com**

Abstract

This article investigates personal data protection as it relates to cybersecurity. Indeed, the amount and speed of digital data creation and storage continues to increase dramatically. While most of the data is insignificant, a considerable amount of it contains sensitive information and must be protected. Therefore, important cybersecurity measures must be adopted to ensure the protection of personal data. From the logic of conditions to the logic of effects, in view of these technological changes, the legislator must take them into account to prevent underestimation of the trade in this information. The aim is to build a critical and communicative approach to cyberlaw to protect personal data in the digital age and ensure Internet security.

Keywords: cyberlaw; Protection of personal data; Cyber security

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

المقدمة:

"ليس الفلاسفة بنظرياتهم، ولا الفقهاء بصيغهم، بل المهندسون باختراعاتهم هم الذين يصنعون القانون، وخاصة تقدم القانون."[1]

إن عالمية التكنولوجيات الجديدة و أهميتها تجعل من الممكن جمع المعلومات وتخزينها ومشاركتها[1]، مما يزيد من تدفق[2] البيانات وحركتها[3]. في هذا السياق، مراقبة الامتثال لواجب حماية المعطيات الشخصية يبدو أنه غير فعال. نظرًا لأن الحياة الاجتماعية بأكملها تتطلب تبادل هذه المعطيات. فإن القدرة على جمع هذه البيانات وبناء قواعد البيانات ليست مهمة صعبة.

لقد حدد المشرع التونسي مفهوم المعطيات الشخصية في المادة 4 من القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية[4])حيث :" تعتبر معطيات شخصية على معنى هذا القانون كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصا طبيعيا معرّفا أو قابلا للتعريف بطريقة مباشرة أو غير مباشرة باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانونا."

وصف ألبرت دي جوفري دي لا براديل العلاقة بين القانون والتقدم العلمي بأنه أي تقدم تكنولوجي يتبعه القانون الذي يأتي لتنظيمه ومحاولة الحد من عيوبه أو التجاوزات التي يمكن أن يسببها.

هذه التقنيات الجديدة تتطلب المزيد من الحماية لأنه بالإضافة إلى البيانات التي يتم جمعها بعلم الشخص المعني، يتم جمع بيانات أخرى دون علمه. ولذلك فمن الضروري استخدام الأدوات الأخلاقية المناسبة في جميع مراحل تطوير وتنفيذ واستخدام هذه التكنولوجيات.

مشكلة البحث

في هذا السياق، كثيرا ما يُطرح السؤال حول كيفية متابعة ودعم النظام القانوني التونسي لهذا التغيير السريع للتكنولوجيات الحديثة و المزعزع للاستقرار في بعض الأحيان، وما إذا كان على مستوى التحديات، والسعي إلى حلول وسط محفوفة بالمخاطر بين المتطلبات القانونية والتقنيات الجديدة.

أهمية البحث:

من الضروري وجود إطار قانوني مناسب لزيادة الثقة في الاقتصاد الرقمي وضمان أمن التبادلات الإلكترونية بين الشركات والمستهلكين والسلطات. ولذلك من المهم أن تضع الدولة إطارًا قانونيًا يسمح للسلطات العامة؛ المهنيين

---

(1) J.-L. SOULIER et S. SLEE, « La protection des données à caractère personnel et de la vie privée dans le secteur des communications électroniques Perspective française », R.I.D.C., 2002, n° 2, p. 663. ; A. LUCAS, J. FRAYSSINET, Droit de l'informatique et de l'Internet, Paris, PUF, 2001, p. 8.

(2) W. JARRAYA, « La protection des données personnelles dans le commerce électronique » Rapport de recherche, Faculté de droit de Sfax, 2013, p. 1.

(3) A. LUCAS, J. DEVEZE et J. FRAYSSINET, op.cit, p. 13.

(4) يضيف الفصل 5 من نفس القانون أنه : "يعد قابلا للتعريف الشخص الطبيعي الذي يمكن التعرّف عليه بصورة مباشرة أو غير مباشرة من خلال مجموعة من المعطيات أو الرموز المتعلقة خاصة بهويته أو بخصائصه الجسمية أو الفيزيولوجية أو الجينية أو النفسية أو الاجتماعية أو الاقتصادية أو الثقافية".

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

والمستهلكين للاستفادة الكاملة من الإمكانيات التي توفرها الأجهزة والتقنيات المختلفة. لقد تسبب الكشف السهل والواسع عن المعلومات في حدوث بعض المشكلات القانونية المتعلقة بحماية البيانات الشخصية.

المنهجية:

يُظهر فحص القواعد التي تحكم البيانات الشخصية أن الحماية يتم ضمانها من خلال الالتزامات الواقعة على عاتق مراقب المعطيات الشخصية (المبحث الأول) والحقوق التي تتطلب اجتهاد مستخدم التقنيات الجديدة (المبحث الثاني).

المبحث الأول: التزامات المسؤول عن معالجة المعطيات الشخصية.

معالجة المعطيات الشخصية عرفها المشرع التونسي في الفصل 6 من القانون الأساسي الصادر في 27 يوليو 2004 بأنها: "(...) العمليات المنجزة سواء بطريقة آلية أو يدوية من شخص طبيعي أو معنوي والتي تهدف خاصة إلى جمع معطيات 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 جميع العمليات المتعلقة باستغلال قواعد البيانات أو الفهارس أو السجلات أو البطاقات أو بالربط البيني".

وبموجب نفس القانون، يمكن أن تتم المعالجة إما بواسطة شخص طبيعي أو بواسطة شخص معنوي[1]. وإذا كانت الحماية تتعلق بالأشخاص الطبيعيين فقط، فإنها تنطبق على أي شخص مسؤول، حتى لو كان شخصاً اعتبارياً.

ينص القانون على عدد معين من الالتزامات التي تقع على عاتق مراقب البيانات قبل معالجة المعطيات الشخصية وبالتزامن معها.

المطلب الأول: الالتزامات السابقة لمعالجة المعطيات الشخصية:

قبل أي تنفيذ للمعالجة، يجب على المسؤول عن المعالجة تنفيذ بعض الإجراءات الشكلية.

في معظم الحالات، لا يتطلب القانون سوى إعلام[2] الهيئة الوطنية لحماية المعطيات الشخصية وفي حالات أخرى، يجب إرسال طلب الترخيص[3] إلى الهيئة وفقا للمادة 2 من المرسوم رقم 2007-3004 المؤرخ في 27 نوفمبر 2007، المتعلق بتحديد شروط وإجراءات التصريح والترخيص لمعالجة البيانات الشخصية "تخضع أي عملية معالجة للبيانات الشخصية لتصريح أو ترخيص مسبق في الحالات المنصوص عليها في القانون الأساسي المتعلق بحماية البيانات الشخصية المذكورة أعلاه ."

---

(1) أولا، قائمة العمليات المذكورة ليست شاملة، مما يترك الباب مفتوحا لتشمل عمليات أخرى، مثل التكيف، والاستخراج، والاتصال بالإرسال، وتحديث التصرف، والتوفيق، والقفل والمحو. وقد اعتمد توسيع التعريف حتى في الفقه.

ثانياً، قد تتعلق المعالجة بـ"(...) العمليات التي تتم بطريقة آلية أو يدوية". حتى لو كان من الممكن تصور المعالجة اليدوية، فإن الممارسة تظهر أن العمليات على الإنترنت تتم بطريقة آلية، وهو ما يمكن تفسيره من خلال العدد المتزايد من المعطيات الشخصية التي يتم جمعها.

(2) الفصل 8 من المرسوم عدد 3004-2007 المؤرخ في 27 نوفمبر 2007

(3) الفصل 10 من المرسوم عدد 2007-3004 المؤرخ في 27 نوفمبر 2007

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

للإعلان وظيفتان: من ناحية، فهو يسمح للهيئة بالعلم بوجود المعالجة. ومن ناحية أخرى، فهو يشمل أيضًا "الالتزام بأن المعالجة مستوفية لمتطلبات القانون": من المفترض أن يكون الشخص الذي يرسل الإقرار على علم بجميع التزاماته وأن يكون قد اتخذ جميع الإجراءات اللازمة للامتثال لها .

إذا أخل مراقب البيانات أو المقاول من الباطن بالالتزامات القانونية التي يخضع لها، تقرر الهيئة بعد سماعها سحب الترخيص أو منع المعالجة.

المطلب الثاني: الالتزامات المتزامنة مع معالجة المعطيات الشخصية.

إن مسألة معالجة البيانات السلوكية أو المعلوماتية للجمهور من قبل المنظمات الخاصة أو العامة لأغراض مختلفة – تجارية وتسويقية وسياسية – تطرح مشكلة. يأتي التعقيد من تنوع ،لا بل اختلاف، الالتزامات المتنافسة في علاج المعطيات الشخصية.

1.واجب الشفافية والإعلام

إذا كان من الممكن تعريف مفهوم الشفافية على أنها الجودة التي تسمح "(...) بالسماح بظهور الحقيقة"، فإن أي عملية معالجة للمعطيات الشخصية يجب أن تكون متوافقة مع الحقيقة[1] التي أعلنها الشخص المسؤول.

الشفافية عامل أساسي لتعزيز المعاملات الإلكترونية، تتطلب أن تتم أي معالجة للمعطيات الشخصية بشكل مخلص. تنص المادة 11 من القانون الأساسي صراحة على ما يلي: "يجب معالجة المعطيات الشخصية بشكل عادل[2]."

على الرغم من غموضه، إلا أنه من المقبول عمومًا أن مبدأ الولاء يتطلب أن تتم أي عملية معالجة بموافقة صاحب البيانات.

حتى يتمكن الشخص من إعطاء الموافقة، يجب أن يعرف منطقيًا أنه يتم جمع البيانات المتعلقة به. ولذلك فإن مراقب البيانات ملزم بالتزام الشفافية. ويعاقب القانون نفسه بشدة جمع البيانات الشخصية عن طريق وسائل احتيالية أو غير عادلة أو غير مشروعة[3].

ولذلك، يجب على الشخص المسؤول أن يحترم التزامه بالمعلومات وأن يشير في وقت جمع المعلومات إلى ما يلي:

هويته

الغرض ومدة معالجة البيانات

---

[1] الفصل الأول من القانون الأساسي الصادر في 27 جويلية 2004 يتطلب صراحة الشفافية من خلال توفير أن: "لكل شخص الحق في حماية البيانات الشخصية المتعلقة بحياته الخاصة باعتباره أحد الحقوق الأساسية التي يكفلها الدستور ولا يمكن تناولها إلا في في إطار الشفافية والوفاء واحترام كرامة الإنسان ووفقاً لأحكام هذا القانون".

[2] بعض النصوص القانونية تتطلب الولاء والشرعية في نفس الوقت. انظر الفن. 6 من التوجيه الصادر في 24 أكتوبر 1995، والمادة 2 من القانون الفرنسي الصادر في 6 يناير 1978 والمادة 4-1 من قانون لوكسمبورغ الصادر في 2 أغسطس 2002

[3] المادة 86 و ما بعدها من القانون الأساسي عدد 63 لسنة 2004..

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

طبيعة الإجابات الإجبارية أو الاختيارية

العواقب المحتملة لعدم الاستجابة

متلقي البيانات

الحقوق المتاحة للشخص الذي يتم جمع البيانات منه

إمكانية نقل البيانات إلى بلد أجنبي

هذه المعلومات مهمة: من ناحية، فهي تسمح للشخص المعني بمعالجة البيانات بمعرفة الغرض من جمع البيانات بدقة: وعلى أساس هذه المعلومات سيعطي موافقته على استخدام البيانات بشأن ذلك. ومن ناحية أخرى، فإنها تلزم مراقب البيانات الذي إذا قام بمعالجة البيانات بشكل لا يتوافق مع ما أعلنه، فإنه يتعرض لعقوبات جنائية.

ويظل الالتزام بتقديم المعلومات حتى بعد جمعها. طوال فترة معالجة المعطيات الشخصية، يتعين على مراقب البيانات تقديم هذه المعلومات للأشخاص الذين يطلبونها.

2.الالتزام بتأمين المعطيات الشخصية

يجب أن يتم جمع المعطيات الشخصية بشكل آمن. ينص الفصل 18 من القانون الأساسي على ما يلي: "يتعين على كل شخص يقوم، شخصيا أو عن طريق شخص ثالث، معالجة البيانات الشخصية فيما يتعلق بالأشخاص المعنيين، اتخاذ جميع الاحتياطات اللازمة لضمان أمن هذه البيانات ومنع أي طرف ثالث من القيام بذلك". ولا يجوز للأطراف تعديلها أو تغييرها أو الاطلاع عليها دون إذن من الشخص المعني."[1]

ووفقا لهذه المادة، حتى المعالجة التي تتم من خلال الاستعانة بطرف ثالث لا تعفي الشخص المسؤول من المسؤولية.

كما تسير المادة 20 الفقرة 3 من القانون الأساسي في نفس الاتجاه من خلال النص على ما يلي: " ويكون المسئول عن المعالجة والمناول مسؤولين مدنيا عن كل إخلال بمقتضيات هذا القانون ."

ويتعين على مراقب البيانات اتخاذ "الاحتياطات اللازمة" لضمان أمن المعطيات الشخصية. وقد تم تفصيل هذا التعبير الذي يدل على أن مبدأ الأمن ذو طبيعة وقائية[2] في المادة 19 من نفس القانون. ويهدف إلى منع تطفل الأشخاص غير المصرح لهم، إما عن طريق الوصول إلى المعدات والمنشآت، أو عن طريق قراءة حاملات البيانات أو تعديلها أو نقلها، أو حتى إدخال البيانات أو محوها. يجب تأمين المعطيات الشخصية ضد تدخل الغير. يمكن أن يكون مفهوم الغير يطرح إشكاليات معينة، ولهذا عرفها المشرع في المادة 6 من نفس القانون، فأشارت إلى "

---

[1] Droit de l'Internet, [En ligne]. Disponible : https://www.cours-de-droit.net/droit-de-l-internet-a121603676.
كما نصت القوانين على مبدأ الأمن. ف17 من توجيه عام 1995، و22 من قانون لوكسمبورغ الصادر في 2 أغسطس 2002، و34 من القانون الفرنسي لعام 1978.

[2] A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 163.

كل شخص طبيعي أو معنوي أو السلطة العمومية والتابعين لهم باستثناء الشخص المعني بالأمر والمستفيد، والمسؤول عن المعالجة والمناول والتابعين لهم"[1].

ومن مشاكل تطبيق المادتين 18 و19 صعوبة مراقبة الالتزام بمبدأ الأمان، خاصة في حالة المعالجة التي تتم عبر الإنترنت. وبما أن سيطرة الشخص المعني أمر لا يمكن تصوره، فإن الاحتمال الوحيد يظل هو تدخل الهيئة الوطنية لحماية المعطيات الشخصية حتى لو كان الفصل 77 من القانون الأساسي يمنح الهيئة حق التحقيق[2]، فإن ثقل مهامها والجانب الفني للتدابير الأمنية يثيران الشكوك حول فعالية الضوابط التي يتعين القيام بها. وما يزال الشك قائمًا، خاصة مع تزايد عدد معالجي المعطيات من يوم لآخر.

يجب إنشاء الأمان خاصة في حالات تدفقات المعطيات الشخصية ويميز القانون الأساسي بين التدفق الداخلي الذي يسمى الاتصال، وبين التدفق الخارجي أي نحو بلد أجنبي الذي يسمى نقل المعطيات الشخصية . وفيما يتعلق بإبلاغ البيانات، ينص الفصل 47 من القانون الأساسي على مبدأ واستثناءات. ويتكون المبدأ من حظر نقل المعطيات الشخصية "(...) دون موافقة صريحة بأية وسيلة تترك أثراً كتابياً."

وتكريسًا لشكليات الحماية، تنص المادة 47 على نظامين للاستثناءات من مبدأ الحظر. الأول، المنصوص عليه في الفقرة 1، لا يتطلب الحصول على ترخيص من الهيئة الوطنية لحماية المعطيات الشخصية، حيث يتم إرسال البيانات إلى السلطات العمومية. في الواقع، هذا الاستثناء واسع جدًا. إن استخدام عبارات "الأمن العام" و"الدفاع الوطني" و"المهام التي يعهد بها" يدل على أن هذا المبدأ قد تم التحايل عليه من خلال هذه الاستثناءات.

ويتطلب النظام الاستثنائي الثاني المنصوص عليه في الفقرة الثانية من نفس المادة الحصول على ترخيص من الهيئة الوطنية لحماية المعطيات الشخصية[3] ووفقا للفقرة 2 من المادة 47، يجوز للهيئة الوطنية أن تأذن بالاتصال، عندما يثبت أن هذا الاتصال ضروري لتحقيق المصالح الحيوية لصاحب الشأن أو ورثته أو وليه[4].

فيما يتعلق بنقل البيانات الشخصية، تنص المادة 51 من القانون الأساسي على ما يلي: "لا يمكن أن يتم نقل البيانات الشخصية التي تتم معالجتها أو التي يعتزم معالجتها إلى بلد آخر إلا إذا ضمنت هذه الدولة مستوى مناسبًا من الحماية يتم تقييمه من خلال فيما يتعلق بجميع العناصر المتعلقة بطبيعة البيانات المراد نقلها، وأغراض معالجتها، ومدة المعالجة المتوقعة، والبلد الذي سيتم نقل البيانات إليه بالإضافة إلى الاحتياطات اللازمة المتخذة لضمان أمن البيانات. وفي جميع الأحوال يجب أن يتم نقل المعطيات الشخصية وفقاً للشروط المنصوص عليها في هذا القانون.

---

[1] الفصل 2 (س) من قانون لوكسمبورغ المؤرخ 2 أغسطس 2002 يعطي أمثلة للغير في القطاع العام مثل الوزارة والإدارة والمؤسسة العامة والبلدية أو الخدمة العامة.

[2]^ الفصل 76من القانون الأساسي والمرسوم رقم 2007–3003 المؤرخ في 27 نوفمبر 2007 المتعلق بتحديد إجراءات عمل الهيئة الوطنية لحماية المعطيات الشخصية.

[3] يمكن تبرير شرط الترخيص بحقيقة أنه في هذا النظام الثاني، لا يتم إرسال البيانات لصالح سلطة عامة.

[4] هناك حالة أخرى تسمح للهيئة بإعطاء تصريحها تستحق التوضيح وهي الحالة التي يكون فيها البلاغ ضروريا "لتنفيذ عقد يكون صاحب الشأن طرفا فيه". والمثال النموذجي هو حجز فندق تجريه وكالة سفر في بلد ثالث لصالح العميل، V. S. LOUVEAUX,المقال سابق الذكر, ص 202

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

المبحث الثاني: حقوق الأشخاص المعنيين بمعالجة المعطيات الشخصية

يعترف القانون بحقوق المعنيين بمعالجة البيانات الشخصية: الحق في الموافقة والحصول على المعلومات، والحق في الوصول، والحق في المعارضة.

تتطلب الطبيعة الدولية وغير الملموسة للإنترنت الحرص من الشخص المعني حتى يتمكن من ممارسة حقوقه سواء عند جمع البيانات الشخصية أو تخزينها.

المطلب الأول: الحقوق الممارسة أثناء جمع المعطيات الشخصية

أثناء عملية جمع المعلومات، يجب على صاحب البيانات التأكد من ممارسة حقوقه من أجل حماية بياناته.

1.الحق في الحصول على المعلومات

تتم معالجة المعطيات الشخصية إذا كانت قانونية وعادلة وشفافة، فيجب وضع شرط آخر، وهو ضمان حق الأشخاص المعنيين في الحصول على المعلومات.[1]

وتنص الفقرة الأولى من الفصل 31 من القانون الأساسي لسنة 2004 على وجوب تقديم الإخطار "(...) بأي وسيلة تترك أثرا كتابيا". يهدف شرط النموذج الكتابي إلى حماية الشخص المعني من أي شكل من أشكال سوء المعاملة.

ويجب إجراء المعلومات المنصوص عليها في المادة 31 "(...) خلال شهر واحد على الأقل قبل التاريخ المحدد لمعالجة البيانات الشخصية". وقد يتم إعفاء مراقب البيانات من شرط الموعد النهائي إذا كانت المعلومات متاحة بشكل دائم على موقعه".

والغرض من تحديد وقت المعلومات هو تمكين الطرف المعني من ممارسة حقوقه[2].

ويجب الإعلان عن أي انتهاك لهذا الحق، وخاصة أمام الهيئة الوطنية لحماية المعطيات الشخصية و قد يطالب صاحب البيانات أيضًا بوجود ملصق يضمن امتثال مراقب البيانات لواجب الإعلام[3].

2.الحق في الموافقة

على الرغم من غموضه، إلا أنه من المقبول عمومًا أن مبدأ الولاء يتطلب أن تتم أي عملية معالجة بموافقة صاحب بيانات الشخص المعني؛ وإذا كان الأخير شخصًا غير قادر أو محظوراً أو غير قادر على التوقيع، فإن الموافقة تخضع لقواعد القانون العامة.

---

(1) J. LE CLAINCHE, « Spam : la technologie a-t-elle dépassé le droit ? », noté sous T.G.I. Paris, Le XVIIe siècle, 7 décembre 2004, Rév. Lamy Droit Immatériel, mai 2005, p. 30.

(2) J. LE CLAINCHE المرجع سابق الذكر

(3) Abdel Raouf ElLoumi, « Protection des données personnelles sur Internet », R.J.L., 2010, n°2, p.9.

ومع اشتراط موافقة الشخص المعني على أي عملية معالجة للبيانات الشخصية، إلا أن المشرع لم يجد ضرورة لتعريف مفهوم الموافقة. تحدد المادة 2-ح من التوجيه الصادر في 24 أكتوبر 1995 أنها: "(...) أي مظهر من مظاهر الإرادة، حرة ومحددة ومستنيرة يقبل بموجبها الشخص المعني أن تكون البيانات الشخصية المتعلقة به موضوعًا للعلاج"[1]

يمكن لمراقب البيانات إعداد مستند الكتروني يعبر عن الموافقة على الإدلاء بمعطيات لتتم معالجتها وتعرض على الأشخاص الذين يصلون إلى موقعها والقيام بمنح موافقتهم من خلال وضع تواقيعهم.

وقد شدد المشرع على شرط الحصول على موافقة صاحب الشأن في عدة مواد. ويعاقب على عدم الامتثال لشرط الموافقة بموجب المادتين 87 و88 من نفس القانون. تمنح المادة 29 من القانون الأساسي استثناءات لشرط موافقة صاحب البيانات "(...) عندما يثبت بوضوح أن هذه المعالجة تتم لمصلحته ويكون اتصاله مستحيلا، أو عندما ينطوي الحصول على الموافقة على جهد غير متناسب أو إذا كانت تتم معالجة البيانات الشخصية بموجب القانون أو الاتفاقية التي يكون صاحب البيانات طرفًا فيها".

3.الحق في الاعتراض

لا يمكن أن يكون حق المعارضة حقيقيًا إلا إذا تم إبلاغ صاحب البيانات بالمعالجة. يعتبر "(...) الوسيلة الوحيدة لصاحب البيانات لحماية نفسه من احتمالات تنزيل قواعد البيانات وتحويل غرضها (...)"، ويتطلب حق المعارضة أيضًا اجتهاد الشخص المعني لضمان فاعليته[2].

ينص الفصل 42 من القانون الأساسي على ما يلي: "يحق للشخص المعني، أو ورثته أو وليه، الاعتراض في أي وقت على معالجة البيانات الشخصية المتعلقة به لأسباب وجيهة ومشروعة وخطيرة، إلا في الحالات التي تكون فيها المعالجة منصوصاً عليها في القانون أو تقتضيه طبيعة الالتزام.

علاوة على ذلك، يحق لصاحب البيانات أو ورثته أو ولي أمره الاعتراض على إرسال البيانات الشخصية المتعلقة به إلى أطراف ثالثة بهدف استخدامها لأغراض إعلانية. المعارضة تعلق المعالجة على الفور."

تعمل هذه الفصول على توسيع قائمة الأشخاص الذين يمكنهم ممارسة حق المعارضة، الذي من المرجح أن يوفر المزيد من الحماية للبيانات الشخصية. وتنص المادة نفسها على أن حق المعارضة يمكن ممارسته في أي وقت.

وبالرجوع إلى تعريف مفهوم المعالجة، فمن الممكن ممارسة هذا الحق حتى عند جمع المعطيات الشخصية[3].

---

[1] فصل 2-ج من قانون لوكسمبورغ الصادر في 2 أغسطس 2002 يتطلب أيضًا أن تكون هذه الموافقة صريحة وليست ملتبسة

[2] A. LUCAS, J. FRAYSSINET, Droit de l'informatique et de l'Internet, Paris, PUF, 2001, p.9

[3] يضيف أحد الباحثين: "من الغريب أن نعتبر الجمع علاجاً، لأن العلاج يتطلب جمعاً مسبقاً. لكن كيف يمكننا معالجة البيانات التي لم نجمعها بعد (...)" W. JARRAYA ، المرجع المذكور، ص. 23.

ووفقاً للمادة 42، يجوز ممارسة حق المعارضة في حالة "(...) أسباب مشروعة وجادة (...)". ولذلك فإن المشرع يشترط ضمناً تبريراً أو دافعاً لهذا الحق.

ولم يبين القانون الأساسي ما إذا كان حق المعارضة حرا أم لا.

تؤكد بعض النصوص القانونية على حق المعارضة الحر، خاصة في حالة المعالجة التي تتم لأغراض التنقيب. من الناحية العملية، يمكن لصاحب البيانات ممارسة حقه من خلال ملء نموذج متاح على الإنترنت أو ببساطة عن طريق النقر على أيقونة موجودة على الموقع الإلكتروني لوحدة تحكم المعطيات[1].

يتمثل هذا الحق في الاعتراض الذي ينهي المعالجة. وتنص المادة 42 صراحة على أن: "المعارضة تعلق المعالجة فورا". إن ممارسة حق المعارضة، الذي "(...) يشهد اهتمامًا متجددًا في سياق الإنترنت"، يتطلب اجتهاد الشخص المعني لمعرفة ما إذا كان مراقب البيانات يحترم التزاماته أم لا. من المشكوك فيه أن يقوم مستخدم الإنترنت بعد إعطاء معطياته الشخصية ويتابع أسلوب علاجهم، خاصة أن عدم المادية يحد بشكل خطير من هذا المسعى. وتصبح المشكلة أكثر تعقيدًا في حالة الجمع غير المباشر، على سبيل المثال من خلال ملفات تعريف الارتباط. وفي هذه الحالة، فإن الشخص المعني لا يعرف حتى أن بياناته الشخصية. تم جمعها ومعالجتها[2].

المطلب الثاني: الحقوق التي تتم ممارستها أثناء حفظ المعطيات الشخصية

أثناء عملية الاحتفاظ بالبيانات، تنص اللوائح على الحق في تصحيح المعطيات الشخصية المتعلقة بها وحق الوصول إلى هذه المعطيات.

1.الحق في الوصول الى المعطيات الشخصية

لحق الوصول أهمية حاسمة عند تخزين المعطيات الشخصية لأنه يسمح لأصحاب البيانات بمعرفة ما إذا كانت معطياتهم الشخصية أم لا. هل تتم معالجتها أم لا. وجميع المعلومات المتعلقة بعملية المعالجة، مثل طبيعة البيانات الشخصية والغرض منها وإبلاغها ونقلها[3].

ونظرا لهذه الأهمية، فقد خصص المشرع قسما في القانون الأساسي الصادر في 27 جويلية 2004 لتنظيم حق الولوج والحقوق المترتبة عليه. ويحدد الفصل 32 من هذا القانون الأساسي حق الولوج بأنه: "(...) حق الشخص المعني أو ورثته أو وليه في الاطلاع على جميع المعطيات الشخصية المتعلقة به، وكذلك الحق في تصحيحها وإكمالها وتصحيحها، تحديثها أو تعديلها أو توضيحها أو حذفها عندما يثبت أنها غير دقيقة أو غامضة أو معالجتها محظورة."

(1) A. LUCAS, J. FRAYSSINET ، المرجع السابق، ص 10

(2) Abdel Raouf ElLoumi, نفس المرجع

(3) W.Jarraya ، المرجع.

ويشمل حق الوصول[1] أيضًا الحق في الحصول على نسخة من البيانات بلغة واضحة متطابقة مع محتوى السجلات، وبشكل واضح عند معالجتها باستخدام العمليات الآلية.

إن توسيع قائمة الأشخاص الذين لهم حق الوصول إلى البيانات الشخصية يظهر رغبة المشرع في توفير الحماية الفعالة. ويمكن تأكيد هذه الرغبة من خلال الجانب المباشر لهذا الوصول.

وقد نص المشرع في القانون الأساسي على شرطين لممارسة حق الوصول. وقد تم تفصيل الشرط الأول في المادة 34 التي نصت على أن: "يمارس حق الوصول صاحب الشأن أو ورثته أو وليه على فترات معقولة وعلى نحو غير مفرط."

أما الشرط الثاني لممارسة حق الوصول فقد نصت عليه المادة 56 من نفس القانون التي تنص على أنه فيما يتعلق بالبيانات التي تتم معالجتها بشكل رئيسي من قبل المؤسسات الصحية العمومية، يجوز للشخص المعني أو ورثته أو ولي أمره "(...) الأسباب، أو طلب تصحيح أو استكمال أو تصحيح أو تحديث أو تعديل أو مسح البيانات عندما يثبت عدم دقتها وأخذ العلم عنها". ومما قد يبدو متناقضا أن المشرع يشترط تبرير حق الوصول إلى البيانات الحساسة، في حين أنه يعفي صاحب البيانات من تبرير حقه في حالة البيانات العادية.

وينص الفصل 35 من القانون الأساسي على ما يلي: "لا يجوز تقييد حق وصول الشخص المعني أو ورثته أو وليه إلى البيانات الشخصية المتعلقة به إلا في الحالات التالية:

كما يضيف الفصل 38 من القانون الأساسي على أن: "يقدم طلب الولوج من قبل صاحب الشأن أو ورثته أو ولي أمره كتابة أو بأية وسيلة تترك أثرا كتابيا". قد يؤدي تقديم طلب الوصول إلى حدوث مشكلات معينة على الإنترنت. ولهذا السبب نصت المادة 37 من نفس القانون على ما يلي: "يجب على الشخص المسؤول عن المعالجة الآلية للبيانات الشخصية والمقاول من الباطن توفير الوسائل التقنية اللازمة لتمكين الشخص المعني أو ورثتهم أو ولي أمره من إرسال طلبه إلكترونيا" تصحيح أو تعديل أو تصحيح أو مسح البيانات الشخصية.

إن طلب الوصول، الذي يتطلب اجتهاد الشخص المعني، يمكن أن يحد بشكل خطير من ممارسة حق الوصول، خاصة أن المشرع لم يفرض مهلة محددة بوضوح على المراقب للرد على هذا الطلب، وهذا مخالف للشريعة. طلب الحصول على نسخ من البيانات. وينص الفصل 38 من القانون الأساسي في الواقع على ما يلي: "يجوز للشخص المعني أو ورثته أو وليه أن يطلب بنفس الطريقة الحصول على نسخ من المعطيات في أجل لا يتجاوز شهرا واحدا من تاريخ الطلب المذكور". في حالة وجود نزاع بشأن ممارسة حق الوصول أو الحصول على نسخ من البيانات، فإن الهيئة الوطنية لحماية المعطيات الشخصية يمكن إدخالها.[2]

غير أنه دون ممارسة حق الوصول، لا يمكن لصاحب البيانات تصحيح بياناته الشخصية.

---

[1] ينص الفصل 36 من القانون الأساسي على أنه :" إذا تعدد المسؤولون عن معالجة المعطيات الشخصية أو إذا تمت المعالجة بواسطة مناول يمارس حق النفاذ لدى كل واحد منهم"

[2] الفصل 38 من القانون الأساسي

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

2.الحق في التصحيح

وينص الفصل 40 من القانون الأساسي على ما يلي: "يجوز للشخص المعني أو ورثته أو وليه أن يطلب تصحيح البيانات الشخصية المتعلقة به وإتمامها وتعديلها وتوضيحها وتحديثها وحذفها عند ثبوت عدم صحتها". أو غير مكتملة أو غامضة أو طلب إتلافها عندما يكون جمعها أو استخدامها قد تم بالمخالفة لهذا القانون".

يطرح حق التصحيح ثلاثة إشكالات في الممارسة:

الأول يتعلق بإثبات دقة المعطيات الشخصية وتحل المادة 39 من القانون الأساسي هذه الإشكالية بالنص على ما يلي: "في حالة وجود نزاع حول دقة المعطيات الشخصية، يجب على القائم بمعالجة المعطيات والمناول الإشارة إلى وجود هذا النزاع حتى يتم الفصل فيه.

الإشكال الثاني الذي يطرحه حق التصحيح يتعلق بالحالة التي يكون فيها المعطيات الشخصية التي يتم إرسالها أو نقلها إلى طرف ثالث. في مثل هذه الحالة، لا يمكن لصاحب البيانات إلا تصحيح البيانات التي تتم معالجتها بواسطة وحدة التحكم أو المعالج. ومع ذلك، فإن المدير والمناول ملزمان بموجب المادة 21 من القانون الأساسي بـ "(...) تصحيح أو استكمال أو تعديل أو تحديث الملفات الموجودة لديهما، ومسح البيانات الشخصية من هذه الملفات إذا كانا على علم بعدم الدقة أو عدم كفاية هذه البيانات". كما يجب عليهم "(...) إبلاغ الشخص المعني والمستفيد الشرعي[1] من المعطيات بأي تعديل[2] يتم إجراؤه على المعطيات الشخصية (...)".

وتتمثل المشكلة الثالثة في الحقيقة أنه على الرغم من اعتماد حق التصحيح على حق الوصول، إلا أنه مهمل للغاية في الممارسة العملية.

الخاتمة:

النتائج:

في هذه المقالة، سعينا إلى إظهار الاهتمام بالنهج النقدي والتواصلي لتحليل طرق حماية البيانات الشخصية في الفضاء الرقمي.

وعلى الرغم من وضعها كحق أساسي من حقوق الإنسان، فقد استوعبت العولمة والتصنيع وتسليع المعلومات، وذلك باستخدام التكنولوجيات الجديدة كوسيلة للجمع والمعالجة.

ومنذ تزايد المعلومات الرقمية على نطاق عالمي، أدت هذه الممارسات، بالتزامن مع التطورات التقنية، إلى ظهور مخاوف أخلاقية وقانونية تتعلق بحماية الخصوصية من خلال أساليب حماية البيانات الشخصية. وعلى وجه الخصوص، فإن اللجوء إلى مفهوم البيانات الشخصية يفتح المجال أمام إمكانية إنشاء قائمة وتقديم وصف

[1] S. Khaled, « Le droit à la protection des données personnelles », R.J.L., 2004

[2] ينص الفصل 21 الفقرة. 3 من القانون الأساسي على ما يلي: " ويتم الإعلام في أجل شهرين من تاريخ التغيير برسالة مضمونة الوصول مع الإعلام بالبلوغ أو بأي وسيلة تترك أثرا كتابيا".

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

للخصائص المرتبطة بالفرد. وكان من الضروري في الواقع أن يركز الذكاء الاصطناعي والتقنيات الجديدة على البيانات التي تعتبر مواد أو مواد إعلامية أو تجارية يمكن استغلالها في الاقتصاد الرقمي.

تطور هذا المجال، يؤدي إلى صراعات ذات طبيعة سياسية وإيديولوجية واقتصادية. تشكل النصوص والتقنيات التنظيمية الآن زوجين متحدين بفضل الوساطة الاجتماعية والتقنية الهامة عبر الأدوات المحوسبة وشبكات الاتصالات. هناك مجال واسع من البحث مفتوح سواء في تحليل مفاهيم الخصوصية أو في التطورات المشتركة للسياسات التنظيمية والتطورات التكنولوجية جنبا إلى جنب مع الأمن السيبراني.

التوصيات:

في نهاية المطاف، يجب على المنظمات العامة أو الخاصة التأكد من أن سياساتها وممارساتها تتوافق مع النصوص القانونية والتقنية الحالية، والعمل على تعزيز وتطوير الترسانة القانونية والإشراف على التطور السريع للتكنولوجيات الجديدة. أما الجمهور، فيواجه مشاكل تتعلق بالأمن الفني والحماية القانونية لبياناته الشخصية، التي تحكمها نصوص غالبًا ما تكون غير مألوفة له ولم يتم استشارته بشأنها. إن ثقة مستخدمي الخدمات الرقمية والتحف فيما يتعلق بالاستخدام التجاري أو الحكومي لبياناتهم الشخصية هي قضية اجتماعية وسياسية. إنه جزء من "ملف المخاطر الجديد الذي أحدثته الحداثة". ومن ثم، يجب على مستخدم الإنترنت أن يتبنى إجراءات كمستخدم تتجاوز هذا النهج على المستوى العام للأمن الذي تقترحه الدولة، من خلال تطبيق وسائل أخرى أكثر سهولة لتأمين البيانات الشخصية على أساس يومي.

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

المصادر والمراجع:

- الكتب

1. C-A. COLLIARD, « La machine et le droit privé français contemporain », Mélange offert à Georges RIPERT, Paris, L.G.D.J., 1950, p. 115.
2. J.-L. SOULIER et S. SLEE, « La protection des données à caractère personnel et de la vie privée dans le secteur des communications électroniques Perspective française », R.I.D.C., 2002, n° 2, p. 663; .
3. J. LE CLAINCHE, « Spam : la technologie a-t-elle dépassé le droit ? », noté sous T.G.I. Paris, Le XVIIe siècle, 7 décembre 2004, Rév. Lamy Droit Immatériel, mai 2005, p. 30.
4. LUCAS, J. FRAYSSINET, Droit de l'informatique et de l'Internet, Paris, PUF, 2001, p. 8.

- **الرسائل العلمية: (أطروحات ورسائل الماجستير).**

1. W. JARRAYA, « La protection des données personnelles dans le commerce électronique » Rapport de recherche, Faculté de droit de Sfax, 2013, p. 1

- **الأبحاث**

1. Abdel Raouf ElLoumi, « La protection des données personnelles sur Internet », R.J.L., 2010, n°2, p.9
2. S. Khaled, « Le droit à la protection des données personnelles », R.J.L., 2004.

- **القوانين والتشريعات**

1. القانون الأساسي عدد 63 لسنة 2004 مؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية
2. المرسوم رقم 2007-3003 المؤرخ في 27 نوفمبر 2007 المتعلق بتحديد إجراءات عمل الهيئة الوطنية لحماية المعطيات الشخصية.

- **المواقع الإلكترونية**

1. Droit de l'Internet, [En ligne]. Disponible : https://www.cours-de-droit.net/droit-de-l-internet-a121603676

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024

© جميع الحقوق محفوظة،عمادة البحث العلمي والابتكار/ جامعة الزيتونة الأردنية 2024