مجلة الدراسات القانونية المقارنة
EISSN:2600-6154 المجلد 07/ العـــدد02 (2021)، ص.ص. 413-437 ISSN:2478-0022

ضمانات أمن المعطيات الشّخصية المتداولة عبر الإنترنت

Guarantee safety of personal data transmit on the Internet

الدكتور: دحماني سمير

تـخصص: الـقانون

Specialization: law

جامعة مولود معمري ـ كلية الحقوق والعلوم السياسية ـ تيزي وزو

Faculty of Law and Political Science, University Mouloud Mammeri, Tizi Ouzo, Algeria.

Email: samirvoila@gmail.com

تاريخ إرسال المقال: 2020/11/27 تاريخ القبول:2021/09/15 تاريخ النشر:2021/12/29

ملخص:

تعتبر شبكة الإنترنت البيئة المناسبة لعمليات جمع واستعمال وتسجيل المعطيات الشخصية للأفراد، كالبيانات المتعلقة بهوية المستخدم عبر الإنترنت، وتحديد المواقع الجغرافية(GPS)، والبيانات الفيزيولوجية، الجينية، النفسية، الاقتصادية، الثقافية والاجتماعية، حيث تزايد الاستخدام غير المشروع لهذه المعطيات على الشبكة بشكل هائل، على حساب الحقوق والحريات الأساسية للأفراد، وخِدمة لمصالح الأحزاب السّياسية، الشّركات الرّقمية، القراصنة، الخ...

وعليه فإنّ ازدياد الهجمات عبر الإنترنت وتطوّر تقنيات الاتصالات الإلكترونية، دفع بالدول إلى إعادة النّظر في مفهوم المعطيات الشّخصية والاستعانة بترتيبات تقنية المراقبة الإلكترونيّة على الاتصالات، كآلية إضافية لضمان حرية تنّقل البيانات الشّخصية للأفراد، وترصّد التّهديدات الإلكترونيّة المحتملة التي تمس بسريّة البيانات الشّخصية المتداولة عبر شبكة الإنترنت.

الكلمات المفتاحية:

البيانات الشّخصية؛ مراقبة الاتصالات الإلكترونية؛ معالجة المعطيات؛ أمن المعطيات الشّخصية، المسؤول عن المعالجة؛ الضمانات.

Abstract:

The Internet has become an adequate environment for collection operations, and uses personal data registered at unbeknownst to the individual, such as the connection data, and the cordial(GPS), as well as several elements specific to physical, economic, cultural or social, but the extent of the illegal collection of said data significantly increased on the internet, to the detriment of respect for the fundamental freedoms and rights of the persons concerned, for the benefit of political parties, digital companies, hackers, etc.

Indeed, the risk of internet attack is real and the process resulting from the technical characteristics of electronic communication, imposes on the state of resorting an additional data protection mechanism, that allows them to use the contemporary surveillance practices of communication on the network, so as to ensure the freedom of movement of personal data, anticipate and counter in parallel any attacks, which threaten the integrity of the transmitted data on the Internet.

***Keywords**:*
Personal data ; Control of e-communications ; Data processing; Security of personal data; Treatment responsible; Guaranty.

مقدمة

إنّ شيوع الرقمنة والاستخدام السريع لتكنولوجيات الاتصال والإعلام، ساهم بشكل كبير في تصاعد وتيرة الهجمات الإلكترونية بمختلف أنواعها، التي استطاعت أن تهدّد المؤسسات الحكومية في العديد من الدول ومنشآتها الحيوية، على غرار شبكات الطاقة الكهربائية وأنظمة التحكّم في المفاعلات النووية وحركة الطائرات واختراق أنظمة معلومات المصارف المركزية، وكذا انتهاك الأسرار الخاصة بالمؤسسات العسكرية والسياسية والاقتصادية، وما بالك بالبيانات الشّخصية للأفراد، التي يتم جمعها ومعالجتها بطرق غير مشروعة والمتاجرة بها لأغراض تجارية أو لتحقيق أهداف سياسية بغية جذب آراء الناخبين وتغيير المسار الانتخابي لحزب معيّن، وبالتالي فإنّ أعمال التسريب والاختراقات للمعطيات الشخصية للأفراد تختلف باختلاف نوايا ودوافع المجرمين، فعادة ما يَقِفُ من وَرَائِهَا قراصنة محترفين ذوو خبرة عالية ومعرفة عميقة في مجال الحاسوب وأمن الشّبكات، ويملكون مهارات عاليّة في لُغات البرمجة وأنظمة التّشغيل، الخ....

وعليه، أصبحت قضية أمن البيانات الشّخصية للأفراد المتداولة عبر شبكة الإنترنت، تُشكّل الشّغل الشّاغل لدى أيّة دولة من العالم، التي يستوجب عليها إرساء تدابير قانونية وتقنيّة مُحكمة لمواجهة التحدّيات والمخاطر الواسعة النّطاق للجرائم الإلكترونية، مع تشييد بنية معلوماتية وطنية واسعة، تشمل كافة المجالات لتفادي مختلف التّهديدات الإلكترونيّة وتعقّب حدوثها، حيث قام المشّرع الجزائري بإحداث جهازين ذوي صلاحيات مختلفة، يتعلّق الأوّل بالسّلطة الوطنيّة لحماية المعطيات ذات الطّابع الشّخصي، ويتمثّل الثّاني في الهيئة الوطنيّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تكمن أهمية الموضوع، في تحديد القواعد القانونية التي كرّسها المشّرع الجزائري، لمعالجة المعطيات الشّخصية وضمان أمنها من مخاطر شبكة الإنترنت، التي تُعتبر مُنْذُ نَشأتُها، البيئة الخِصبة لارتكاب الجرائم الإلكترونية والمساس بالحريات العامة وحقوق وكرامة الأشخاص المعنيين بعملية معالجة معطياتهم الشّخصية، وكذا تفسير التّدابير القانونيّة والتّقنية المكرّسة من طرف المشرّع، لضمان عملية معالجة المعطيات الشّخصية مهما كان مصدرها أو شكلها، وحمايتها من أي استعمال غير مشروع من طرف الغير، مع توضيح المهام الموكلة لكل هيئة (المشار إليها أعلاه) تم استحداثها لمنعِ التّعدي على هذه المعطيات، وتفادي مخاطر استعمال شبكة الإنترنت.

وعلى ضوء كلّ هذه المعطيات، نطرح الإشكالية التالية:

ما مدى فعالية التدابير المُكرّسة لحماية المعطيات الشّخصية من مخاطر استعمال شبكة الإنترنت ؟

للإجابة عن هذه الإشكالية يستوجب اتباع منهج تحليلي واستقرائي، من خلاله يتّم توضيح ضوابط المعالجة الآلية للمعطيات الشّخصية (**المبحث الأول**)، مع التّطرق إلى الهيئات التي استحدثها المشرع الجزائري لمنع الاعتداء على المعطيات الشّخصية (**المبحث الثاني**).

المبحث الأول

ضوابط المعالجة الآلية للمعطيات الشّخصية

إن الثّورة الرّقمية أحدثت تغييرات وتحوّلات عميقة في نمط المعاملات الإلكترونية، لاسيما في وسائل وتقنيات الاتصال التي يتّم من خلالها تداول ومعالجة وتخزين مختلف البيانات، خاصة تلك المتعلقة بالمعطيات الشّخصية، حيث قام المشّرع الجزائري، بتدعيم التّرسانة القانونيّة المنظّمة للمسائل المتعلقة بالاتصالات الإلكترونية والمعطيات الشّخصية في إطار القوانين الخاصّة بها (**المطلب الأول**)، كما أنّ عملية المعالجة الآلية للمعطيات الشّخصية المتداولة في نطاق الاتصالات الإلكترونيّة، تخضع لمجموعة من القواعد الأساسية التي كرّسها المشرع، بموجب أحكام القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطّابع الشّخصي (**المطلب الثاني**).

المطلب الأول

الإطار المفاهيمي للاتصالات الإلكترونية والمعطيات الشّخصية

تطرّق المشّرع الجزائري في إطار أحكام القانون رقم 18-04 المؤرخ في 10 ماي 2018، الذي يُحدّد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونيّة، إلى تعريف الاتصالات الإلكترونية من زاوية قانونيّة وتكنولوجيّة بحتة (**الفرع الأول**)، كما أعطى كذلك المشّرع، مفهوما خاصا للمعطيات الشّخصية، في إطار القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطّابع الشّخصي (**الفرع الثاني**).

الفرع الأول

مفهوم الاتصالات الإلكترونية

قدّم المشرع الجزائري وفقا لنص المادة 1/10 من القانون رقم 18-04 المؤرخ في 10 ماي 2018، الذي يُحدّد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونيّة[1]، مفهوما واسعا للاتصالات الإلكترونيّة، التي تشمل:" كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها، عبر الأسلاك أو الألياف البصريّة أو بطريقة كهرومغناطيسيّة."

بينما تطرقت الفقرة الخامسة(05) من نفس المادة(5/10)، إلى تعريف الإنترنت على أنّها: "شبكة معلوماتية عالمية تتشكّل من مجموعة من شبكات وطنيّة وإقليميّة وخاصّة، مَوْصُولَة فيما بينها عن طريق بروتوكول الاتصال(IP)، وتعمل معًا بهدف تقديم واجهة مُوّحدة لمستعمليها."

حيث يُقْصَدُ بالأمن الإلكتروني أو السيبراني، وفقا لنص المادة 3/10 من القانون رقم 18-04، المذكور أعلاه[2]، على أنّه:" مجموعة الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير

المخاطر والأعمال والتكوين والممارسات الجيّدة والضمانات والتكنولوجيات، التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث، من شأنه المساس بتوفير وسلامة وسرّية البيانات المخزنة أو المعالجة أو المرسلة."

بالإضافة إلى ما سبق، تطرّقت أحكام المادة 01/(و) من القانون رقم 09-04، المتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاتصال والإعلام ومكافحتها[3]، إلى تعريف الاتصالات الإلكترونية، التي تتضمّن: " أيّ تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيًا كانت طبيعتها، تتّم عبر أيّ وسيلة إلكترونية بما في ذلك وسائل الهاتف النّقال والثّابت."

أمّا المنظومة المعلوماتية، يُقصد بها وفقا للفقرة(ب) من نفس المادة(01/(ب)): " أي نظام مُنفصل أو مجموعة من الأنظمة المتصلة بعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر على المعالجة الآلية للمعطيات تنفيذا لبرنامج معلوماتي معيّن."، بينما المعطيات المتعلقة بحركة السّير، تعني وفقا للفقرة(ه) من نفس المادة(1/(ه)): " أيّ معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تُنتِجُها هذه الأخيرة باعتبارها جزءً في حلقة الاتصالات، تُوضِّح مصدر الاتصال، ووجهة المرسَل إليها، والطريق الذي يسلكه ووقت وتاريخ وحجم ومُدّة الاتصال ونوع الخدمة."

الفرع الثاني

مفهوم المعطيات الشّخصية

قام المشرع الجزائري، في إطار المادة 03 من القانون رقم 18-07 المؤرخ في 10 جوان 2018، المذكور أعلاه، بوضع تعريف خاص بالمعطيات ذات الطابع الشّخصي، التي تشمل:" كلّ معلومة مهما كانت دعامتها، تتعلّق بشخص مُعرّف الهويّة أو قابل للتّعرف عليها بصفة مباشرة أو غير مباشرة، عن طريق الرّجوع إلى رقم التّعريف أو عنصر أو عدّة عناصر خاصّة بهويته البدنيّة أو الفيزيولوجيّة أو الجينيّة أو البيوميتريّة أو النّفسيّة أو الاقتصاديّة أو الثقافيّة أو الاجتماعيّة."

أمّا عملية معالجة المعطيات الشّخصية، تتضمّن:" كل عملية أو مجموعة العمليات المنجزة بطرق أو بوسائل آلية أو حتّى من دونها على معطيات شخصيات، كالجمع أو التّسجيل أو التّنظيم أو الحفظ أو الملائمة أو التّغيير أو الاستخراج أو الاطلاع أو الاستعمال، أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التّقريب أو الرّبط البيني وكذا الإغلاق أو التّشفير أو المسح أو الإتلاف." [4].

المطلب الثاني

متطلبات المعالجة الآلية للمعطيات الشّخصية

تُشكل شبكة الإنترنت باعتبارها شبكة الشبكات، البيئة الإلكترونية الملائمة لأهل الاختصاص (القراصنة) في ارتكاب مختلف الجرائم الإلكترونية التي تمس بالخصوص أنظمة المعالجة الآلية للبيانات الشّخصية، أو انتهاك خصوصية المعطيات الشّخصية للأفراد، أو المساس بحياتهم الخاصة، أو حتّى المتاجرة بمعطياتهم الشّخصية لأغراض معيّنة، الخ... (**الفرع الأول**)، حيث أخضع المشّرع الجزائري، بموجب أحكام القانون رقم 18-07 المتعلق بحماية المعطيات

الشّخصية، عملية جمع ومعالجة المعطيات الشّخصية للشّخص المعني، لمجموعة من التّدابير القانونية، لضمان تأمين هذه المعطيات وتفادي استعمالها لغايات غير مشروعة (**الفرع الثاني**).

الفرع الأول

صُور الاعتداء على المعطيات الشّخصية

يمكن تقسيم جرائم الاعتداء على المعطيات الشّخصية، على النّحو التّالي:

أولا– التّجسس على البيانات الشخصيّة: تتّم هذه الجرائم باستخدام البرمجيات الخبيثة التي يُعَوَّلُ عليها كثيرا في عمليات اختراق أنظمة معلومات شبكات الحواسيب أو مُراقبة الاتصالات الإلكترونية للأفراد، بُغية تعقّب وترصّد تحرّكاتهم عبر الانترنت أو شبكات التّواصل الاجتماعي من دون علمهم بذلك، كتسجيل بياناتهم الإلكترونيّة وسرقة أرقام هواتفهم الشّخصية وتسجيل ونقل المحادثات والمكالمات الهاتفية، واستخدام الصُّور الشّخصية، الخ...، من دون أيّ ترخيص من أصحابها، وهذا ما يُشكّل خرقا أو مساسا بسريّة المراسلات الإلكترونيّة المحميّة بموجب القانون [5]، فعادة ما تعتمد الدّول على برامج التصنّت(Pegasus, Prism, etc.) في إطار عمليات التجسس أو التّحقيقات والتّحريات القضائيّة، أو لغرض التّصدي ومكافحة الجرائم (الإرهاب، الجرائم المنظّمة العابرة للحدود، التّجسس الاقتصادي...) التي تمس بالنظام العام وأمن المرافق الحيويّة الوطنيّة [6].

ثانيا– المُتاجرة بالبيانات الشّخصية: تشمل هذه الجرائم على المعطيات الشّخصية أو البيانات المتّصلة بالأشخاص المحمية بموجب القوانين الأساسيّة(الدّساتير)[7] أو الخاصّة بها، حيث تتعدّد هذه الجرائم بحسب دوافع ونوايا المجرمين والأغراض التي تستعمل من أجلها البيانات المتحصّل عليها، كاستخدام البيانات الشخصية للأفراد لأغراض البيع والتسويق في مجال التجارة الإلكترونية، أو المتاجرة بها لأغراض سياسية بتواطؤٍ من المسؤول عن المعالجة، من خلال الولوج غير المصرّح إليها ومن دون الحصول على موافقتهم الصّريحة بمعالجتها(معطياتهم الشخصية)، الخ...[8].

وعليه، تعرضت البيانات الشّخصية للأفراد لأعمال الاختراق والتّسريب لأغراض تخدم مصالح الشّركات التجارية والأحزاب السّياسية، وخصوصا إثر حادثة كامبريدج أناليتيكا((Cambridge Analytica(CA) التي من خلالها قامت تلك الشركة منذ 2014، بتسريب ما يُقارب 87 مليون من البيانات الشّخصية لمستخدمي شبكة (Facebook) لأهداف الحملة الانتخابية للرئيس الأمريكي(Donald Trump)، حيث أثّرت كذلك تسريبات تلك الشّركة(CA) على أراء المواطنين البريطانيين خلال الحملة الانتخابية لخروج بريطانيا من الاتحاد الأوروبي(Le Brexit)، حسب تصريحات السّيد (Christopher Wylie) الذي سبق له أن اِشْتَغَلَ في تلك الشّركة(CA) [9].

ثالثا– انتهاك الحياة الخاصة للأفراد: تستهدف هذه الجرائم حرمة وكرامة الأشخاص في حياتهم الخاصّة، كجرائم القذف والسّب والشّتم عبر مواقع الاتّصال الاجتماعي(Facebook, Twiter, etc.)، والتّحريض على الأنشطة المنافيّة للعادات والآداب العامّة، ونشر الأخبار المزيّفة، أو الحصول غير المشروع على البيانات الشّخصية للأفراد عن طريق التّقنيات التّكنولوجية المتاحة(Drones, Caméras de surveillances-cachées, etc.)، التي تسمح بالتقاط أو تسجيل

أو نقل المكالمات أو الصُّور أو الأحاديث الخاصّة أو السّريّة، من دون الحصول على الموافقة الصّريحة لأصحابها، الخ... [10].

رابعا– الاحتيال وسرقة البيانات الشّخصية: تتم هذه الجرائم باستخدام أساليب الهندسة الاجتماعية (Social engeneering) المعروفة، كالهاتف ورسائل البريد الإلكتروني الخادعة، الخ...، لهدف الاحتيال على الأفراد وسرقة بياناتهم الشّخصية واستعمالها لأغراض غير مشروعة، حيث تتعلق هذه الجرائم بالخصوص بقيام المحتال بإلقاء مكالمة هاتفية إلى أحد المستخدمين في الشركة، مُنتحلا صورة المدير بغية الحصول على الرقم السّري الذي يسمح بالدخول إلى النظام المعلوماتي للشركة، والاستحواذ على البيانات السريّة الحسّاسة، أو يقوم(المحتال) بإرسال رسالة اصطياد خادعة (Phishing Scam) التي عادةً ما تحتوي على فيروسات أو برمجيات خبيثة(Malwares)، لأحد المستخدمين في الشركة، لغرض الحصول على البيانات الحسّاسة بمجرّد الضّغط على رابط الرسالة(Lien hypertexte) والاطّلاع على محتواها (Spam, Hoax, SMS, etc.).

كما يمكن كذلك للقراصنة، القيام باختراق أنظمة حماية المعلومات التّابعة لمواقع التّجارة الإلكترونيّة أو مواقِع المصارف والمؤسّسات الماليّة ومُؤسّسات الضّمان الاجتماعي، لغرض الحصول على البيانات السريّة لأصحاب البطاقات الإلكترونيّة الذكيّة(المصرفية، الصّحة، الضّمان الاجتماعي،...)، على غرار كلمات السّر، وأرقام حساباتهم، الخ...[11]، واستخدامها لتحويل أموالهم إلى حسابات مجهولة تابعة للقراصنة من دون عِلمِ أصحاب البطاقات بذلك[12]، أو يقوم هؤلاء(القراصنة) باستغلال هذه البيانات، للحصول على الأموال عن طريق إحدى برامج الفدية الخبيثة(Ransomware)، التي من خلالها يتّم تقييد الوصول إلى البيانات الإلكترونية المخزّنة في نظام الحاسوب المصاب، أين يُطالب المجرِم صاحبه(الحاسوب المصاب) بدفع فِدية من أجل السّماح بالوصول إلى الملّفات المحتجزة[13].

خامسا– المساس بأنظمة المعالجة الآلية للبيانات الشّخصية: تنصب هذه الجرائم حول اختراق أنظمة حماية شبكات الحاسوب بطريقة غير مشروعة من خلال استغلال الثّغرات والهفوات المتواجدة فيها للمستخدم، التي تسمح لمنفذي الهجمات الإلكترونيّة بالدخول إلى كل أو جزء من منظومة المعالجة الآلية للمعطيات، لغرض حيازة أو نسخ أو تجميع أو تعديل أو إفشاء أو تدمير البيانات الالكترونيّة المخزنة في أجهزة الحواسيب، أو حتى الحصول على البيانات الحسّاسة للمستخدم (كلمات السّر، أرقام بطاقاته المصرفية، الضمان الاجتماعي...) [14].

الفرع الثاني

تدابير جمع ومعالجة المعطيات الشّخصية

تعتبر المعطيات الشّخصية للأشخاص الطبيعيين من بين الحقوق الأساسيّة التي كفلتها مختلف التّشريعات، حيث يجب أن تتّم عملية معالجتها في إطار احترام الكرامة الإنسانية والحياة الخاصة ومُراعاة الحرّيات العامة، مع عدم المساس بحقوق الأشخاص وشرفهم وسمعتهم، وقد أخضع المشرّع الجزائري، عملية معالجة المعطيات الشّخصية بموجب المادة 09 من القانون رقم 18-07 المذكور أعلاه[15]، لمجموعة من الإجراءات التي من خلالها يجب أن تتّم عملية جمع ومعالجة المعطيات الشّخصية لغايات محدّدة وواضحة ومشروعة، وأن تكون (المعطيات) صحيحة وكاملة ومُعالجة بطريقة

مشروعة ونزيهة، ولا تُعَالَجُ لاحقًا بطريقة تتنافى مع هذه الغايات، مع حفظها أو تخزينها بطريقة مؤمّنة خلال المدّة اللاّزمة لإنجاز تلك الغايات، حيث يمكن للمسؤول عن المعالجة، في حالة وجود مصلحة مشروعة وبعد حصوله على إذنٍ من "السّلطة الوطنيّة"، القيام بحفظ المعطيات الشّخصيّة للأفراد لغايات تاريخيّة أو إحصائيّة أو علميّة، بعد انتهاء المدّة اللاّزمة لإنجاز الأغراض التي من أجلها تمّ جمعها ومعالجتها.

حيث تُستثنى من مجال تطبيق القانون رقم 18-07، المذكور أعلاه، المعطيات الشّخصية التي يتّم معالجتها لغايات لا تتجاوز الاستعمال الشّخصي أو العائلي، بشرط عدم إحالتها للغير أو نشرها، وكذا المعطيات المحصّلِ عليها ومعالجتها لأغراض الدّفاع والأمن الوطنيين، أو لأغراض الوقاية من الجرائم ومتابعة مرتكبيها وقمعها، أو معطيات قواعد البيانات القضائيّة المتعلّقة بالجرائم والعقوبات وتدابير الأمن، التي يتم مُعالجتها من طرف السّلطة القضائيّة والسّلطات العموميّة والأشخاص المعنويين الذين يسيّرون مصلحة عموميّة، ومُساعدي العدالة في إطار اختصاصاتهم القانونيّة[16].

كما يمنعُ معالجة المعطيات الشّخصية الحسّاسة، التي تُبيّنُ الأصل العرقي أو الإثني، أو الآراء السّياسية أو القناعات الدّينية أو الفلسفيّة، أو الانتماء النّقابي، أو المعطيات المتعلقة بصّحة الشّخص المعني بما فيها الجينيّة، حيث يُمكن بالمقابل، أن تتّم عملية معالجة هذه المعطيات بناءً على الموافقة الصّريحة للشّخص المعني، أو في حالة وجود نص قانوني أو بترخيص من "السّلطة الوطنيّة"، لأسباب تتعلّق بالمصلحة العامة، وتكون ضرورية لضمان ممارسة المهام القانونيّة أو النّظامية للمسؤول عن المعالجة، أو توافر إحدى الحالات المذكورة بموجب المادة 3/18 من القانون رقم 07/18، المذكور أعلاه[17].

وعليه، يجب أن لا تتم عملية معالجة المعطيات الشخصية، إلاّ بعد الحصول على الموافقة المسبقة والصريحة للشّخص المعني، الذي يملك الحرية في العدول عن موافقته في أي وقت، ولا يُسمح للغير بالاطلاع على المعطيات الشّخصية الخاضعة للمعالجة الآلية، إلاّ لغرض انجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة والمرسل إليه، مع الحصول المسبق على موافقة الشّخص المعني، وفي حالة ما إذا كانت عملية المعالجة، تتعلق بمعطيات شخصية لطفل معين، يجب الحصول على موافقة ممثّله الشّرعي، أو تتّم تلك المعالجة عند الإقتضاء، بترخيص مُسبق من طرف القاضي المختص، الذي يمكن له أن يأمر بالمعالجة إذا استدعت مصلحة الطفل لذلك، حتى ولو لم يتّم الحصول على الموافقة المسبقة لممثّله الشّرعي، حيث يملك القاضي، السّلطة التّقديرية في العدول عن التّرخيص بالمعالجة في أي وقت[18].

وبالتالي فإنّ مُوافَقة الشّخص المعني، لا تكون واجبة في حالة ما إذا كانت عملية معالجة معطياته الشّخصية ضروريّة لاحترام التزام قانوني يخضع له الشّخص المعني أو المسؤول عن المعالجة، أو لحماية حياة الشّخص المعني، أو للحفاظ على مصالحه الحيوية إذا كان من الناحية البدنيّة أو القانونيّة غير قادر عن التّعبير على رضاه، أو لتنفيذ عقد يكون الشّخص المعني طرفا فيه أو لتنفيذ مُهمّة تدخل ضمن مهام الصّالح العام أو ضمن ممارسة مهام السّلطة العموميّة التي يتولاها المسؤول عن المعالجة أو الغير الذي يتّم اطلاعه على المعطيات، أو لتحقيق مصلحة مشروعة من قِبَلِ المسؤول عن المعالجة أو المرسل إليه، مع مراعاة مصلحة الشّخص المعني وحقوقه وحرياته الأساسيّة [19].

وفي جميع الظروف، أخضع المشرع الجزائري بموجب المادة 12 من القانون رقم 07/18، المذكور أعلاه، كل عملية معالجة المعطيات الشّخصية لتصريح مُسبق لدى "السّلطة الوطنيّة"، أو لترخيص منها في حال ما إذا تبيّن لها عند دراسة التّصريح المقدّم لها، أنّ عمليةَ معالجة المعطيات الشّخصية، تتضمّن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسيّة للأشخاص[20].

المبحث الثاني

الهيئات المستحدثة لمنع الاعتداء على المعطيات الشّخصية

تعتبر الجرائم الالكترونية من بين إفرازات الثّورة الرّقمية التي انتشرت كثيرا في الآونة الأخيرة، وذلك تزامنا مع التّطور السّريع واللامتناهي لتكنولوجيا المعلومات والاتصالات، التي سمحت بظهور صور وأشكال متعدّدة من الاعتداءات التي تمس بالبيانات الالكترونية المتداولة عبر الانترنت، ولمنع الاعتداء على المعطيات الشّخصية، قام المشّرع الجزائري بإحداث الهيئة الوطنيّة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المكلفة بمهام مُراقبة الاتصالات الالكترونيّة في إطار الحدود التي رسمها القانون، لضمان أمن المعطيات المتداولة عبر شبكة الإنترنت(**المطلب الأول**)، وكذا الهيئة الوطنيّة لحماية المعطيات ذات الطّابع الشّخصي (**المطلب الثاني**).

المطلب الأول

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

بالرغم من الآفاق الضّخمة والمستوى الأفضل الذي فتحته الثّورة الرّقمية في حياة البشرية، إلاّ أنّها حملت في طياتها مخاطر ضخمة متعدّدة باتت تهدّد قيم وأمن الأفراد في جميع النّواحي، حيث بدت الحاجة ماسّة لمواجهة هذه المخاطر ومراقبة الاتصالات الإلكترونيّة في إطار "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" (**الفرع الأول**)، التي تباشر مهامها المتعلقة بمراقبة الاتصالات الإلكترونية، في حدود الضّوابط القانونيّة والتّقنية المحدّدة مُسبقاً (**الفرع الثاني**)، حيث يُعتبر أمن المعطيات الشّخصية المتداولة عبر الإنترنت من بين الركائز الأساسيّة للأمن الوطني الشّامل، الذي يستدعي ضرورة ترقّب وترصّد الجرائم الإلكترونيّة، حتّى خارج حالات الرّقابة القضائيّة أو القانونيّة لمقتضيات النظام العام والأمن والاقتصاد الوطنيين (**الفرع الثالث**).

الفرع الأول

مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

قام المشّرع الجزائري وفقا للمادة 13 من القانون رقم 09-04، المذكور أعلاه[21]، بإحداث لدى **رئيس الجمهورية** (**وزير الدفاع الوطني**) "هيئة وطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال ومكافحتها"، كمؤسسة عمومية ذات طابع إداري تتمتّع بالشّخصيّة المعنويّة والاستقلاليّة الماليّة، مُكلّفة بمهام تنسيق عمليات الوقاية من الجرائم الإلكترونيّة ومكافحتها، كجرائم الإرهاب أو الماسّة بأمن الدّولة، أو احتمال تواجد اعتداء على منظومة معلوماتيّة، من شأنه أن يُهَدِّدَ مؤسّسات الدولة أو النّظام العام أو الدّفاع والاقتصاد الوطنيين، وكذا مُساعدة السّلطات القضائيّة وأعوان الشّرطة القضائيّة في التّحريات بشأن الجرائم الإلكترونيّة، بما فيها جمع المعلومات وإنجاز الخبرات القضائيّة

أو جمع المعطيات المفيدة للتّعرف على المجرمين، وتحديد مكان تَواجُدِهم من خلال تبادل المعلومات مع نظيراتها الأجنبيّة في إطار طلبات المساعدة القضائيّة الدّولية المتبادلة.

تجدر الإشارة في هذا السّياق، إلى أنّ "الهيئة" كانت تحت تصرّف **"وزير العدل"**، في ظل المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، غير أنّه، بعد صدور المرسوم الرئاسي رقم 19-172 المؤرخ في 06 جوان 2019، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها ، أصبحت تلك "الهيئة" تحت تصرف **"رئيس الجمهورية"** باعتباره **وزيرا للدفاع الوطني**، حيث أُلغيت بالتّالي جميع أحكام المرسوم الرئاسي رقم 15-261 [22].

الفرع الثاني

الحالات التي تسمح باللّجوء إلى المراقبة الإلكترونيّة

إنّ اللجوء إلى إجراء المراقبة الإلكترونية على الاتصالات، يجب أن يتم وفقا للحالات التي حدّدها المشرع الجزائري في المادة 04 من القانون رقم 09-04، المذكور أعلاه، والمتعلقة بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسّة بأمن الدولة، وكذا توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يُهدّد مؤسّسات الدّولة أو النظام العام أو الدفاع والاقتصاد الوطنيين، أو يكون ذلك لمقتضيات التّحريات والتّحقيقات القضائيّة التي تستدعي ذلك الإجراء، أو في إطار تنفيذ طلبات المساعدة القضائيّة الدّولية المتبادلة.

حيث لا يجوز إجراء عمليات المراقبة الإلكترونيّة على الاتصالات في جميع هذه الحالات، إلاّ بعد الحصول على **"إذنٍ مكتوب من السّلطة القضائية المختصّة"**، فعندما يتعلّق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التّخريب أو الجرائم الماسّة بأمن الدّولة، يجب على قُضاة وضُبّاط الشّرطة القضائيّة المنتمين للهيئة الالتزام تحت طائلة العقوبات المتعلقة بالمساس بالحياة الخاصّة بِالغَيْرِ[23]، بعدم مُباشرة إجراءات المراقبة الإلكترونيّة على الاتصالات إلاّ بعد الحصول على "إذن من طرف النائب العام لمجلس قضاء الجزائر" لمدّة ستة(06) أشهر قابلة للتّجديد، يُبيّن فيه طبيعة التّرتيبات التّقنية المستعملة والأغراض الموجّهة لمراقبة الاتصالات الإلكترونية، المتعلقة فقط بجمع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابيّة والاعتداءات على أمن الدّولة ومكافحتها [24].

وعليه، فإنّ "الهيئة" تتمتّع بصلاحيات واسعة في إطار التّرتيبات التّقنية للرّقابة والوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التّخريب أو الجرائم الماسّة بأمن الدّولة، حيث يمكنها القيام بتجميع وتسجيل محتوى الاتصالات الإلكترونية ومباشرة إجراءات التّفتيش والحجز داخل منظومة معلوماتيّة تحت "**سُلطة قاض مختص**"[25]، وتستعين بأيّ خبير أو شخص يُعِينُهَا في أعمالها، وكذا تَطْلُبُ من أيِّ جهاز أو مؤسّسة أو مصلحة كلّ وثيقة أو معلومة ضروريّة لإنجاز المهام المسندة إليها، حيث يجب على "مُقدّمِي خدمات الإنترنت"، الالتزام تحت طائلة العقوبات بتقديم المساعدة للسّلطات القضائيّة في حالة إجراء التّحريات القضائيّة حول محتوى الاتّصالات ووضعها تحت تصرّفها في سريّة تامّة، مع حفظ

المعطيات المتعلّقة بحركة السّير لمدّة سنة(01) واحدة ابتداءً من تاريخ تسجيلها، كالمعطيات التي تسمح بالتّعرف على مُستعملي الخدمة، أين يلتزم متعامل الهاتف، بحفظ المعطيات التي تسمح بالتّعرف على مَصدر الاتصال وتحديد مكانه، وكذا المعطيات المتعلقة بالتّجهيزات الطرفيّة المستعملة في الاتصال، أو الخصائص التّقنية وتاريخ ووقت ومدّة كلّ اتصال، أو المعطيات المتعلّقة بالخدمات التّكميلية المطلوبة أو المستعملة ومُقدّميها أو التي تسمح بالتّعرف على المرسَل إليهِ أو المرسَل إليهم في الاتصال، وكذلك عناوين المواقِع الإلكترونية المطّلعِ بها [26].

كما يجب على "مزوّدي خدمات الإنترنت"، الالتزام بإخطار السّلطات القضائيّة المختصة(النيابة العامّة) عن كل فعل ذي طابع جزائي يتّم كشفه أثناء مزاولة نشاطاتهم، حيث ألزم المشرع بموجب المادة 24 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطّابع الشّخصي، "السّلطة الوطنيّة" في إطار ممارسة مهامها، بضرورة إعلام "النّائب العام المختص" فورا في حالة معاينة وقائع تحتمل "الوصف الجزائي"، وكذا تلتزم "السّلطة الاقتصاديّة للتّصديق الإلكتروني" وفقا للمادة 30 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلّقة بالتّوقيع والتّصديق الإلكترونيين، بضرورة تبليغ النيابة العامّة بكل فعل ذي "طابع جزائي" يُكْتَشَفُ بمناسبة تأدية مَهَامُهَا.

إضافة إلى ما سبق، يلتزم "مزودي خدمات الإنترنت" وفقا للمادة 12 من القانون رقم 09-04، المذكور أعلاه، والمادتين 23 و24 من القانون رقم 20-05 المؤرخ في 28 أفريل 2020 ،الذي يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، بضرورة التّدخل الفوري لسحب المحتويات التي يتيحون الاطّلاع عليها، بمجرد العِلم بطريقة مُباشِرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير مُمكِن، وكذا وضع ترتيبات تقنيّة تسمح بحصر إمكانية الدّخول إلى الموّزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامّة وإخبار المشتركين لديهم بتواجدها [27].

الفرع الثالث

حدود ممارسة إجراء المراقبة الوقائية على الاتصالات الإلكترونية

إنّ "الهيئة" تُمارس مهامها "**أصلاً**" تحت رقابة السّلطة القضائيّة طبقا لأحكام التّشريع السّاري المفعول، لاسيما منها قانون الإجراءات الجزائيّة والقانون رقم 09-04، المذكور أعلاه، مع مراعاة بالخصوص الأحكام القانونيّة التي تضمن "سريّة" المراسلات والاتصالات[28]، لكن بالرّجوع إلى نص المادتين 11 و2/12 من المرسوم الرّئاسي رقم 19-172، المذكور أعلاه، نجد أنّ "المديرية التقنية" التّابعة "للهيئة"[29]، تُشرف على مُهِمَّة "المراقبة الوقائية للاتصالات الإلكترونية" في إطار الوقاية من الجرائم الإلكترونية الماسة بأمن الدولة، وتقوم بجمع وتسجيل وحفظ المعطيات الرّقمية وتحديد مَصْدَرُهَا مع تَتَبُّعِهَا لغرض استعمالها في الإجراءات القضائيّة، وكذا تُزَوِّد السّلطات القضائيّة ومصالح الشّرطة القضائيّة بناءً على "**طلبها**"، بالمعلومات والمعطيات المتعلّقة بالجرائم الإلكترونيّة، حيث تَضَعُ "المديرية التّقنية" التّجهيزات والوسائل والأجهزة التّقنية الضّرورية لتنفيذ مهامها، على مستوى المنشآت القاعدية للمتعاملين ومقدمي الخدمات في مفهوم التشريع المعمول به.

وعليه، تتمتّع "الهيئة" بصلاحيات واسعة في مراقبة جميع الاتّصالات الإلكترونيّة، حيث يُمكِنها مباشرة مهامها الرّقابيّة حتى خارج إطار الرّقابة القضائيّة أو القانونيّة [30]، لغرض تحقيق هدف "**إيجابي**" معمول به لدى جميع دول العالم، ألا وهو التّنبؤ بمختلف التّهديدات الإلكترونيّة(الإرهاب الإلكتروني،...) التي تشّكل خطرا على مؤسّسات الدولة والنّظام العام أو الأمن والاقتصاد الوطنيين، أو حتّى القيام بعمليات التّجسّس على الاتّصالات الدّاخلية أو الجوسسة المضّادة على الاتّصالات الأجنبيّة لمقتضيات الأمن والاقتصاد الوطنيين الخ...، غير أنّه بالمقابل، نجد أن مُمارسة تلك المهام خارج الرّقابة القضائيّة أو القانونيّة يُشّكل تعدّيا أو مساسًا بسريّة المراسلات والاتّصالات والمعطيات الشّخصيّة المحميّة بموجب القوانين الخاصّة، ونحن نَعْلَمُ أنّ المادة 09 من القانون رقم 09-04 المذكور أعلاه، منعت تحت "طائلة العقوبات" المنصوص عليها في التّشريع المعمول به، استعمال المعلومات المتحصّل عليها عن طريق عمليات المراقبة على الاتّصالات الإلكترونيّة خارج الحدود الضّروريّة للتّحريات أو التّحقيقات القضائيّة [31].

المطلب الثاني

السّلطة الوطنيّة لحماية المعطيات ذات الطّابع الشّخصي

إنّ التطبيق الفعلي للقواعد القانونيّة التي كرّسها المشّرع الجزائري، لمعالجة المعطيات ذات الطّابع الشّخصي وضمان احترام الحياة الخاصة والحريات العامة للشّخص المعني، وعدم المساس بحقوقه وشرفه وسُمعته، لا يتّم إلاّ في إطار السّلطة الوطنيّة لحماية المعطيات ذات الطّابع الشّخصي (**الفرع الأول**)، التي تُشرف بالخصوص في إطار مهامها الرّقابية، على ضمان احترام حقوق أطراف عملية المعالجة الآلية للمعطيات الشّخصية (المسؤول عن المعالجة والشخص المعني)، ومدى استيفائهم للالتزامات المفروضة عليهم بموجب أحكام القانون رقم 07/18، المذكور أعلاه (**الفرع الثاني**).

الفرع الأول

تشكيلة ومهام السّلطة الوطنيّة لحماية المعطيات ذات الطّابع الشّخصي

إنّ إحداث أيّ هيئة رسمية وطنية في أي بلد من العالم، لا يتّم إلاّ في إطار نص قانوني يحدّد من خلال أحكامه تشكيلة ومهام تلك الهيئة، وهذا ما قام به المشرع الجزائري الذي أنشأ السلطة الوطنية لحماية المعطيات ذات الطّابع الشخصي بموجب أحكام القانون رقم 18-07 المتعلق بحماية المعطيات الشخصية، الذي حدّد كيفية اختيار أعضائها(**أولا**)، وكذا المهام المكلفة بها(السّلطة الوطنيّة) للسّهر على مطابقة عمليات معالجة المعطيات الشخصية لأحكام هذا القانون(**ثانيا**).

أولا- تشكيلة السّلطة الوطنيّة لحماية المعطيات ذات الطّابع الشّخصي.

قام المشّرع الجزائري بموجب المادة 22 من القانون رقم 18-07 المتعلق بحماية المعطيات الشخصية، بإنشاء لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات الشّخصية تُدعى "**السّلطة الوطنيّة**"، تتمتّع بالشّخصية المعنويّة والاستقلال الإداري والمالي، تتضمّن مجموعة من الأعضاء معيّنين بموجب مرسوم رئاسي لمدة خمس(05) سنوات قابلة للتّجديد، وهم:

– ثلاث(03) شخصيات من بينهم الرئيس، يختارهم رئيس الجمهورية من ذوي الإختصاص في مجال عمل السّلطة الوطنيّة؛

–ثلاثة(03) قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة؛

– عضو عن كل غرفة من البرلمان يتّم اختياره من قِبَلِ رئيس كلّ غُرفة بعد التّشاور مع رؤساء الكتل البرلمانيّة؛

– ممثّل واحد(01) عن المجلس الوطني لحقوق الإنسان؛

ممثّل واحد(01) عن مختلف الوزارات (الدّفاع الوطني، الشّؤون الخارجيّة، الدّاخلية، العدل، البريد والمواصلات السّلكية واللاّسلكية والتّكنولوجيات والرّقمنة، الصّحة، والعمل والتّشغيل والضّمان الاجتماعي.).

والجدير بالذكر، أنّ عملية اختيار أعضاء "السلطة الوطنية"، تتّم وفقا لاختصاصهم القانوني أو التّقني في مجال معالجة المعطيات الشّخصية، مع إمكانية استعانتها(السّلطة الوطنيّة) أثناء أدائها لمهامها بأيّ شخص مُؤهّل، حيث يجب على هؤلاء الأعضاء تأدية اليمين أمام مجلس قضاء الجزائر العاصمة، وفقا للصيغة المشار إليها في نص المادة 24 من القانون رقم 18–07، المذكور أعلاه، وذلك قَبْلَ التّنصيب في وظائفهم[32].

ثانيا– مهام السّلطة الوطنيّة لحماية المعطيات ذات الطّابع الشّخصي.

تُشرف "السّلطة الوطنيّة" على مجموعة من المهام الموكلة لها في إطار نص المادة 25 من القانون رقم 18–07 المتعلق بحماية المعطيات الشخصية، التي من خلالها تَسْهَرُ(السّلطة الوطنيّة) على مدى احترام أحكام هذا القانون لدى المعالجة الآلية للمعطيات الشّخصية، وضمان عدم المساس بحقوق الأشخاص والحرّيات العامة والحياة الخاصّة عند استعمال تكنولوجيا الإعلام والاتصال[33]، وكذا تقوم بمنح التّراخيص وتلقي التّصريحات المتعلّقة بالمعالجة الآلية للمعطيات الشّخصية، مع إعلام كل من الأشخاص المعنيين والمسؤولين بحقوقهم وواجباتهم، وتقديم الاستشارات وتلقي الاحتجاجات والطّعون والشّكاوى المتعلقة بتنفيذ المعالجة، والتّرخيص بعمليات نقل المعطيات الشّخصية إلى الخارج، والأمر سواء بإجراء التّغييرات اللازمة بشأن المعطيات الشّخصية المعالجة أو بإغلاقها أو سحبها أو إتلافها، وتقوم في كل سنة بإعداد تقرير ترفعه إلى رئيس الجمهورية.

فإلى جانب ذلك، تقوم"السّلطة الوطنيّة" بتطوير علاقات التّعاون مع السّلطات الأجنبيّة المماثلة وفقا لمبدأ المعاملة بالمثل، مع تقديم الاقتراحات بشأن أيّ إطار تشريعي أو تنظيمي متعلّق بمعالجة المعطيات الشّخصية ونشر التّراخيص والآراء المدلى بها في السّجل الوطني، مع وضع معايير وقواعد السّلوك والأخلاقيات التي تخضع لها عمليّة المعالجة، حيث يمكن "للسّلطة الوطنيّة" في إطار مهامها أن تقوم بالتّحريات المطلوبة ومعاينة المحلات(باستثناء محلات السكن) والأماكن التي تتم فيها معالجة المعطيات، والولوج إلى المعطيات المعالجة مع جمع المعلومات والوثائق أيّاً كانت دعامتها، وأن تُصْدِرَ عقوبات إدارية في حق المسؤول عن المعالجة، مع إعلام النّائب العام المختص فورا في حالة معاينة وقائع جريمة معيّنة[34]، وفي حالة اطلاع أعضاء السّلطة الوطنيّة على المعلومات والمعطيات الشّخصية أثناء أو بعد الانتهاء من مهامهم، يجب عليهم الالتزام بالسّر المهني ما لم يوجد نص قانوني يقضي بخلاف ذلك.

وعليه، لا يجوز لرئيس "السّلطة الوطنيّة" وأعضائها أن يمتلكوا بصفة مباشرة أو غير مباشرة مصالح في أي مؤسسة تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي، حيث يستفيدون بالمقابل، من حماية الدولة ضد التهديدات أو الإهانات أو الاعتداءات من أي طبيعة كانت التي قد يتعرّضون لها بسبب تأديتهم مهامهم أو بمناسبتهم[35].

الفرع الثاني

التزامات وحقوق أطراف عملية المعالجة الآلية للمعطيات الشّخصية

فرض المشرع الجزائري في الباب الخامس من القانون رقم 18-07 المتعلق بحماية المعطيات الشّخصية للأشخاص الطبيعيين، مجموعة من الالتزامات على عاتق المسؤول عن المعالجة الآلية للمعطيات الشّخصية سواء قبل مباشرة مهامه أو أثناءها (**أولا**)، وبالمقابل يتمتّع الشّخص الطبيعي المعني بمعالجة معطياته الشّخصية بمجموعة من الحقوق المنصوص عليها في الباب الرابع من نفس القانون (رقم 18-07) (**ثانيا**).

أوّلا- التزامات المسؤول عن المعالجة الآلية للمعطيات الشّخصية.

بمجرد إبرام عقد تقديم خدمة المعالجة الآلية للمعطيات الشّخصية يتحمّل المسؤول عن المعالجة مجموعة من الالتزامات، والمتمثّلة فيما يلي:

1- الالتزام بالإجراءات المُسبقة عن المعالجة: إنّ كل عملية معالجة للمعطيات الشّخصية تخضع "لتصريح مُسبق" لدى السّلطة الوطنيّة أو "لترخيص مُسبق" منها، وذلك ما لم يوجد نص قانوني يقضي بخلاف ذلك[36]، فالتّصريح يتم إيداعه مباشرة لدى السّلطة الوطنيّة أو إرساله بالطريقة الإلكترونيّة حيث يُسلّم وصل الإيداع بنفس الطريقة فورا في أجل 48 ساعة، فبمجرد استلام المسؤول عن المعالجة للوصل، يمكنه مباشرة عملية المعالجة تحت مسؤوليته، وبالتالي يمكن أن تكون المعالجات التّابعة لنفس المسؤول عن المعالجة محل تصريح واحد بشرط أن تتّم المعالجات لنفس الغرض أو لأغراض مرتبطة، في حين تُحدّد السّلطة الوطنيّة قائمة خاصة تتضمّن على أصناف المعالجات(الآلية أو غير الآلية) التي لا تمس بحرّيات وحقوق الأشخاص المعنيين وحياتهم الخاصة، وبالمقابل لا تُطبّق إلزامية التّصريح على المعالجات التي يكون الغرض منها فقط مسك سجل مفتوح ليطّلع الجمهور عليه، أو كل شخص يثبت مصلحته المشروعة في ذلك[37].

وعليه، يمكن للسّلطة الوطنيّة أثناء دراستها للتّصريح المقدّم أن تُقرّرَ إخضاع المعالجة المعنيّة لنظام "التّرخيص المسبق"، عندما يتبيّن لها بأنّ المعالجة المعتزم القيام بها تمس بالحريات العامة والحقوق الأساسية للأشخاص وحياتهم الخاصّة، حيث يجب أن يكون قرار السّلطة الوطنيّة مُسبب مع تبليغه للمسؤول عن المعالجة في أجل العشرة(10) أيام التي تلي تاريخ إيداع التّصريح، وفي حالة طلب التّرخيص بمعالجة المعطيات الحسّاسة لأسباب تتعلق بالمصلحة العامّة وتكون ضروريّة لممارسة المهام القانونيّة أو النّظامية للمسؤول عن المعالجة، أو عندما تتم المعالجة بناءً على الموافقة الصريحة للشّخص المعني، أو وجود نص قانوني يقضي بذلك أو وفقا للحالات المبيّنة في المادة 18 من نفس القانون، فتتخذ السّلطة الوطنيّة قرارها في أجل شهرين(02) من تاريخ إخطارها مع إمكانية تمديد نفس المدّة بقرار مُسبّب من رئيس

السّلطة الوطنيّة، ويُعد رفضًا للطلب في حالة عدم رد السّلطة الوطنيّة في الأجل المذكور، وفي جميع الظروف، يجب أن يتضمّن كل من التّصريح وطلب الترخيص المعلومات الواردة في المادة 14 من نفس القانون[38].

2- الالتزام بسلامة وسريّة المعالجة: يجب على المسؤول عن المعالجة أن يقوم بوضع تدابير تقنيّة وتنظيميّة تضمن مستوى ملائما من السّلامة بالنظر إلى المخاطر التي تواجهها المعالجة وطبيعة المعطيات الواجب حمايتها، وذلك خصوصا عندما تستوجب المعالجة إرسال معطيات عبر شبكة معيّنة وحمايتها من أشكال المعالجة غير المشروعة(الضياع العرضي، الإتلاف العرضي أو غير المشروع، التّلف، النّشر أو الولوج غير المرخصين) ، حيث يمكن للسّلطة الوطنيّة أن تُقرّر تأمين الإرسال عبر الإنترنت عن طريق التّشفير، نظرا لما تحتويه هذه الشبكة من مخاطر على حقوق الأشخاص المعنيين وحرياتهم والضمانات الممنوحة لهم[39].

كما يجب على المسؤول عن المعالجة، والأشخاص الذين اطلعوا أثناء ممارسة مهامهم أو بعدها على معطيات شخصيّة، التقيّد بالسّر المهني، وذلك تحت طائلة عقوبات التّشريع الساري المفعول[40].

3- الالتزام بِحُسنِ اختيار المُعالج من الباطن(Sous-traitant): عندما تتم عملية المعالجة لحساب المسؤول عن المعالجة، يجب على هذا الأخير الالتزام في إطار عقد أو سند قانوني، باختيار معالج من الباطن، يقدّم الضّمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها، ويسهر على احترامها، مع التزامه بالتّصرف وفقا لتعليمات من المسؤول عن المعالجة، كما لا يجوز لأي شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن، القيام بمعالجة المعطيات الشّخصية من دون تعليمات المسؤول عن المعالجة باستثناء حالة تنفيذ التزام قانوني[41].

فعندما يكون المسؤول عن المعالجة مُقيماً خارج التراب الوطني، ويقوم بمعالجة المعطيات الشّخصية للمواطنين الجزائريين عن طريق وسائل آلية أو غير آلية مُتواجدة فوق التراب الوطني، وذلك باستثناء المعالجات التي تُستعمل لأغراض العبور فوق التراب الوطني، يجب على ذلك المسؤول أن يُبلّغَ السّلطة الوطنيّة بهويّة مُمثله المقيم بالجزائرِ، الذي يَحُلُّ محلّه في جميع حقوقه والتزاماته المترتّبة عن أحكام القانون رقم 18-07 المذكور أعلاه، ونصوصه التّنفيذية[42].

4- احترام حريّة وكرامة الشّخص المعني: ألزم المشرع الجزائري بموجب المادة 02 من القانون رقم 18-07 المتعلق بحماية المعطيات الشّخصية، المسؤول عن المعالجة، بضرورة احترام الكرامة الإنسانية والحياة الخاصّة والحرّيات العامة وعدم المساس بحقوق الأشخاص وشرفهم وسُمعتهم، أثناء معالجته لمعطياتهم الشّخصية مهما كان مصدرها أو شكلها.

5- الالتزام بمشروعية ونزاهة عملية المعالجة: يجب على المسؤول عن المعالجة احترام أحكام القانون رقم 18-07، المتعلق بحماية المعطيات الشّخصية، المذكور أعلاه، وذلك قَبْلَ وأثناء مباشرته لعملية معالجة المعطيات الشّخصية للأفراد، حيث يتحمّل المسؤولية الجزائية عن كل عملية معالجة لهذه المعطيات تتّم خارج أحكام هذا القانون، وذلك دون الإخلال بالعقوبات المنصوص عليها في قانون العقوبات[43]، وكذا الجزاءات الإدارية التي يمكن أن تفرضها "السّلطة الوطنيّة" بموجب أحكام الفصل الأول من الباب الثاني من نفس القانون[44].

6- الحصول على الموافقة الصريحة للشّخص المعني: يجب على المسؤول على المعالجة الالتزام بعدم معالجة معطيات الشّخص المعني إلا بعد الحصول على موافقته الصريحة، الذي يملك الحرية الكاملة في التّراجع عن موافقته في أيّة لحظة، فإذا كان ذلك الشّخص عديم أو ناقص الأهلية، فإنّ الموافقة تخضع للإجراءات المنصوص عليها في التّقنين المدني، غير أنّ موافقة الشّخص المعني لا تكون واجبة، إذا كانت المعالجة ضروريّة وفقا للحالات الواردة بموجب أحكام نص الفقرة الأخيرة من المادة 07 من نفس القانون(رقم 18-07)[45].

7- الالتزام بالغرض الذي جُمعت من أجله المعطيات: يجب على المسؤول عن المعالجة، الالتزام باحترام الغاية التي جُمعت من أجلها المعطيات الشّخصية للشّخص المعني[46]، مع عدم معالجته للمعطيات الشّخصية المتعلقة بالجرائم والعقوبات وتدابير الأمن التي تدخل في اختصاص السّلطات القضائيّة والعموميّة والأشخاص المعنويين، الذين يسّيرون مصلحة عموميّة ومساعدي العدالة في إطار اختصاصاتهم القانونيّة[47]، حيث نصت المادة 43 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، المحدّد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على ضرورة التزام مقدّم خدمات التّصديق الإلكتروني بجمع البيانات الشّخصية الضّرورية لمنح وحفظ شهادة التّصديق الالكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى[48].

8- عدم استعمال البيانات الشّخصية في الاستكشاف المباشر: يُقصد بالاستكشاف المباشر أي إرسال لرسالة مهما كانت دعامتها وطبيعتها، مُوجّهة للتّرويج المباشر أو غير المباشر لسلع وخدمات أو لسمعة شخص يبيع سلعا أو يقدم خدمات، وبالتالي لا يمكن للمسؤول عن المعالجة، استخدام البيانات الشّخصية للمعني في أيّ شكل من الأشكال لغرض الاستكشاف المباشر من دون موافقته المسبقة، سواء تم ذلك بواسطة آلية اتصال أو جهاز الاستنساخ البعدي أو بريد الكتروني أو أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة، غير أنّه، يمكن لذلك المسؤول استعمال البيانات الشّخصية للمعني لغرض الاستكشاف المباشر، بمناسبة بيع منتجات أو تقديم خدمات مشابهة يقدمها نفس الشّخص الطبيعي أو المعنوي، من دون المساس بحق المرسل إليه في الاعتراض دون مصاريف إضافية، باستثناء التّكلفة المرتبطة بإرسال الرفض على استعمال بياناته الشّخصية وقت جمعها، وكلّما وجّه إليه بريد الكتروني لأجل الاستكشاف [49].

وعليه، يُمْنَعُ إخفاء هويّة الشّخص الذي أوصلت لفائدته الرّسائل وذكر موضوع لا صلة له بالخدمات المقترحة، وكذا إرسال رسائل في أيّ شكل من الأشكال لغرض الاستكشاف المباشر دون الإشارة إلى بيانات صحيحة لتمكين المرسل إليه من إرسال طلب توقيف هذه الإيصالات، من دون مصاريف غير تلك المرتبطة بإرسالها. **9- عدم نقل المعطيات الشّخصية إلى الخارج:** لا يمكن للمسؤول عن المعالجة إرسال أو تحويل المعطيات الشّخصية للجزائريين إلى دولة أجنبية من دون أي ترخيص للسّلطة الوطنيّة، وأنّ تلك الدولة لا تضمن مستوى حماية كافٍ للحياة الخاصّة والحرّيات والحقوق الأساسيّة للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات، أو التي قد تخضع لها، وفي جميع الظروف، يمنع إرسال وتحويل المعطيات الشّخصية إلى أي دولة أجنبيّة، عندما يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيويّة للدولة، غير أنّه، يمكن لذلك المسؤول نقل المعطيات الشّخصية نحو دولة أجنبية لا تتوفّر فيها تلك الشّروط، وذلك في حالة الموافقة الصّريحة للشّخص المعني، أو إذا كان النّقل ضروريًا في الحالات المذكورة في المادة 2/45

من نفس القانون، أو إذا تم النّقل وفقًا لاتفاق ثنائي أو مُتعدّد الأطراف أبرمته الجزائر، أو بناء على ترخيص من "السّلطة الوطنية" في حالة تتطابق المعالجة مع نص المادة 02 من نفس القانون [50].

تجدر الإشارة في هذا السّياق، أنّ "محكمة العدل الأوروبية(CJUE)" أصدرت قراراً في 16 جويلية 2020 يقضي بإلغاء قرار المفوضيّة الأوروبيّة رقم 1250/2016 الصادر بتاريخ 12 جويلية 2016، المتعلق بتحويل البيانات الشّخصية لمواطني الاتحاد الأوروبي إلى الولايات المتّحدة الأمريكيّة [51]، تكريساً للاتفاق الثّنائي المبرم بين الاتحاد الأوروبي مع الولايات المتحدة الأمريكية (Le bouclier de protection des données UE-États-Unis ou (Privacy Shield))، الذي يسمح للشّركات الرقميّة الأمريكيّة (Facebook, Google, Amazon, etc.) بنقل المعطيات الشّخصية لمواطني الاتحاد إلى الولايات المتّحدة(USA)، على نحو يسمح للسّلطات الإدارية والأمنيّة الفيدرالية(NSA, FBI, CIA) بالاطلاع عليها في إطار برنامج المراقبة على الاتصالات الدوليّة، لغرض جمع المعلومات الضّرورية والتصنّت على مختلف الاتصالات الإلكترونيّة لمقتضيات الأمن والاقتصاد الوطنيين، وهذا ما يشكّل في رأي المحكمة الأوروبية(CJUE) خطرا على سلامة وأمن البيانات الشّخصية لمواطني الاتحاد الأوروبي، المحمية بموجب التّنظيم الأوروبي رقم 679/2016 المؤرخ في 27 أفريل 2016، الذي يتعلق بحماية الأشخاص الطبيعيّة لدى معالجة معطياتهم الشّخصية مع حرية تنقلها(RGPD) [52].

10- الالتزام بحفظ أو تخزين المعطيات الشّخصية: يجب على المسؤول عن المعالجة أن يقوم بحفظ جميع المعطيات الشّخصية التي قام بجمعها ومعالجتها بطريقة قانونية، وذلك خلال مُدّة لا تتجاوز المدّة اللاّزمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها، حيث يمكن لذلك المسؤول في حالة تواجد مصلحة مشروعة، أن يَطْلُبَ لدى "السّلطة الوطنيّة" الإذن بِتَمْدِيدِ مُدَّةِ حفظ أو تخزين المعطيات الشّخصية لغايات علمية أو تاريخية أو إحصائية[53].

ثانيا- حقوق الشّخص المعني بمعالجة معطياته الشّخصية.

بمقابل الالتزامات التي تقع على المسؤول عن المعالجة، يتمتّع الشّخص المعني بمعالجة معطياته الشّخصية بمجموعة من الحقوق التي كرّسها له القانون، والمتمثّلة فيما يلي:

1- الحق في الإعلام: يجب على الشّخص المعني بجمع معطياته الشّخصية أن يكون على عِلم مُسبق بجميع المعلومات المتعلقة بهوية المسؤول عن المعالجة أو مُمثّله عند الاقتضاء، وبأغراض معالجة معطياته الشّخصية وبأيّ معلومة إضافية مُفيدَة تخص المرسَل إليهِ ومدى إلزامية الرّد والآثار المترتّبة عن ذلك، وكذا حقوقه ونقل المعلومات إلى بلد أجنبي، وفي حالة جمع المعطيات الشّخصية عبر الشبكات المفتوحة، يجب على المسؤول عن المعالجة أو ممثله أن يقوم بإعلام الشّخص المعني بأنّ معطياته الشّخصية سوف يتم تداولها في الشّبكات من دون ضمانات السّلامة، وقد تتعرّض للقراءة والاستعمال غير المرخص من طرف الغير.

وعليه، فإنّ إلزامية الإعلام بكامل العناصر المذكورة أعلاه، ترد عليه بعض الاستثناءات المتعلقة في حالة ما إذا تمّت معالجة المعطيات الشّخصية للمعني حصريا لأغراض صحفيّة أو فنيّة أو أدبيّة أو تطبيقا لنص قانوني، أو استحالة

إعلام الشّخص المعني في حالة معالجة معطياته الشّخصية لأغراض علميّة أو إحصائيّة أو تاريخيّة، أين يجب على المسؤول عن المعالجة تقديم إخطار للسّلطة الوطنيّة يُوضّح فيه سبب الاستحالة [54].

2- الحق في الولوج: يحق للشّخص المعني بمعالجة معطياته الشّخصية أن يطلب من المسؤول عن المعالجة إبلاغه ما إذا كانت معطياته محل مُعالجة أم لا، أو إفادته بشكل مفهوم وواضح بالمعطيات التي تخضع للمعالجة وبكل معلومة متاحة تتعلق بمصدر المعطيات، وبالمقابل يحق للمسؤول عن المعالجة أن يطلب لدى السّلطة الوطنيّة تحديد آجال الإجابة على طلبات الولوج المشروعة، غير أنّه، يمكن لذلك المسؤول الاعتراض على الطلبات التّعسفية في حالة ما إذا كَثُرَ عددها وطابعها المتكرّر، حيث يقع على عاتقه التزام إثبات الطابع التّعسفي لطلب الولوج غير المشروع[55].

3- الحق في التّصحيح: يجب على المسؤول عن المعالجة أن يَسْتَجِيبَ لطلبات الشّخص المعني بمعالجة معطياته الشّخصية أو ورثته، المتعلقة بتصحيح أو تحيين أو مسح أو إغلاق المعطيات الشّخصية، لسبب الطّابع غير المكتمل أو غير الصحيح لها، أو أنّ معالجتها ممنوعة قانونا، حيث يلتزم المسؤول القيام بالتّصحيحات اللاّزمة مجانًا في أجل العشرة(10) أيام من إخطاره من الشّخص المعني، وفي حالة رفضه أو عدم رَدِّهِ خلال هذه الفترة، يحق للشّخص المعني إيداع طلب التّصحيح لدى السّلطة الوطنيّة التي تقوم بتكليف أحد أعضائها بالقيام بكل التّحقيقات الضّرورية وإجراء التّصحيحات اللاّزمة في أقرب الآجال مع إخبار الشّخص المعني بمآل طلبه.

كما يحق للشّخص المعني بمعالجة معطياته الشّخصية أن يطلب من المسؤول عن المعالجة بتبليغ الغير الذي أوصلت إليه المعطيات الشّخصية، بكل تحيين أو تصحيح أو مسح أو إغلاق للمعطيات وذلك ما لم يكن مُستحيلا[56].

4- الحق في الاعتراض: يحق للشّخص المعني تقديم اعتراض لدى المسؤول عن المعالجة(الحالي أو اللاّحق) على استعمال معطياته الشّخصية لأغراض دعائية لاسيما التّجارية منها، أو لأسباب أخرى مشروعة ذات صلة بمعالجة معطياته، حيث لا يمكنه مباشرة حق الاعتراض في حالة ما إذا كانت المعالجة تستجيب لالتزام قانوني أو أنّ الاعتراض قد استبعد بموجب إجراء صريح في المحرّر الذي يرخص معالجة معطياته الشّخصية[57].

خاتمة

من خلال ما سبق، نصل إلى أنّ مسألة أمن المعطيات الشّخصية للأفراد تعتبر أحد ركائز الأمن الوطني لكلّ دولة، التي يستوجب عليها أن تتعامل مع القضية باعتبارها قضية أمن بحتة، لكون أنّ هذه المعطيات أصبحت تَسْتَعْمِلُهَا الكيانات التّابعة للدّول(NSO Group, etc.) والشّركات الرّقميّة العملاقة (Google, Facebook, Twitter, Amazon, etc.) بالخصوص، لتحقيق أغراض تجارية تتعلق بتقديم خدمات وسلع تتناسب مع احتياجات الزبائن، أو التّجسّس لأغراض سياسيّة من أجل تغيير مسار حملة انتخابية لحزب مُعيّن، أو أي غرض أخر، حيث تتّم عملية جمع ومعالجة معطيات الأفراد مُباشرة عبر المواقع الإلكترونية أو البرمجيات الخبيثة(Pegasus, etc.) أو باستعمال خاصيّة "المشاركة"

لمنصات التّواصل الاجتماعي، وذلك من دون الحصول على موافقتهم الصّريحة، أو حتّى عِلمهم بالأغراض التي أُستعملت من أجلها معطياتهم.

ولضمان أمن المعطيات الشّخصية المتداولة عبر الإنترنت، يجب على أصحاب المواقع الإلكترونيّة والتّطبيقات البرمجيّة، القيام بإعداد وتطوير سياسة موثوقة لحماية هذه المعطيات، مع تكييفها مع أحكام التّشريع السّاري المفعول، التي من خلالها يتّم تحديد مبادئ وإجراءات معالجتها والتّدابير الأمنيّة المتّخذة لضمان حُسن تداولها، وتفادي أي تدخّل أو ضرر أو تغيير أو إفشاء غير مُصرّح به من قِبَلِ الغَيْرِ للمعطيات الشّخصية المعالَجة أو المخزّنة.

كما أنّ أمن الشّبكات والبيانات الإلكترونية المتداولة عبرها، يستوجب على الدّولة الجزائرية تشييد بنية معلوماتية وطنية واسعة النّطاق تمس جميع المجالات، للتّخفيف من حِدّة مخاطر الإنترنت والتّنبؤ بمختلف التّهديدات الإلكترونية، من خلال تطوير سياسة وطنيّة شاملة لحماية هذه البنية وصيانة أمنها، وأمن ما يتداول عبرها من بيانات إلكترونية حسّاسة، وترقّب ورصد وضبط وملاحقة منفّذي الهجمات الإلكترونية في الوقت المناسب، وبشكل شامل، في إطار الترتيبات القانونيّة والتقنيّة لمراقبة الاتصالات الإلكترونيّة، حيث يجب على الهيئات المكلّفة بمهمّة المراقبة احترام الأحكام القانونيّة التي تضمن سريّة المراسلات والاتصالات، وعدم المساس بكرامة وحُرمة الحياة الخاصّة بالمواطنين، وبحقوقهم وحرياتهم المضمونة.

قائمة المراجع المستعملة:

I- اللّغة العربية:

أولا- النّصوص القانونيّة للجمهوريّة الجزائريّة الديمقراطيّة الشعبيّة:

أ)- النّصوص التّشريعيّة:

1- أمر رقم 66-156 مؤرخ في 08 جويلية 1966، يتضمن قانون العقوبات، معدل ومتمم.

2- قانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر.ج.ج.د.ش، عدد 47، الصادر في 16 أوت 2009.

3- قانون رقم 15-04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج.د.ش، عدد 06، الصادر في 10 فيفري 2015.

4- قانون رقم 16-01 مؤرخ في 06 مارس 2016، يتضمن التعديل الدستوري، ج.ر.ج.ج.د.ش، عدد 14، الصادر في 07 مارس 2016.

5- قانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج.ر.ج.ج.د.ش، عدد 27، الصادر في 13 ماي 2018.

6- قانون رقم 18-07 مؤرخ في 10 جويلية 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج.د.ش، عدد 34، الصادر في 10 جوان 2018.

7– قانون رقم 20-05 مؤرخ في 28 أفريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ج.ر.ج.ج.د.ش، عدد 25، الصادر في 29 أفريل 2020.

ب)– نصوص تنظيميّة:

1– مرسوم رئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج.د.ش، عدد 53، الصادر في 08 أكتوبر 2015.

2– مرسوم رئاسي رقم 19-172 مؤرخ في 06 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها ، ج.ر.ج.ج.د.ش، عدد 37، الصادر في 09 جوان 2019.

ثانيا– الكتب:

1- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.

2- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2010.

3- دلال صادق الجواد، حميد ناصر الفتال، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2008.

4- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

5- عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية(الحاسب الآلي وشبكة المعلومات(الإنترنت))، دار الوراق للطباعة والنشر والتوزيع، بيروت، لبنان، 2004.

6- علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن، 2017.

7- عمرو عيسى الفقي، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الاسكندرية، مصر، 2006.

8- محمد عبد حسين الطائي، ينال محمود الكيلاني، إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015.

9- مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، 2017.

10-هدى هامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

ثالثا– مواقع الإنترنت:

1- أحمد السيد كردي، "أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها"، مقال منشور عبر الموقع الالكتروني التالي: https://www.kenanonline.com/user/ahmedkordy/posts/323552(تم الاطلاع عليه بتاريخ 2019/11/12.)

2- جمال محمد غيطاس، "الأمن المعلوماتي والجرائم الإلكترونية...أدوات جديدة للصراع"، مقال منشور في يوم الخميس، 01 مارس 2012، على الساعة 12:38 من توقيت مكة المكرمة، عبر الموقع الإلكتروني التالي: https://www.AlJazeeraCenter.forStudies.htm (تم الاطلاع عليه بتاريخ 2020/01/20.)

II - *En Français*:

A - *Ouvrage* :

- **Zouheir TRABELSI, Henri LY**, « La sécurité sur Internet, Lavoisier », Paris, 2005.

B - Articles :

1- **Arnaud BELLEIL**, « La régulation économique des données personnelles », LEGICOM 2009/1 (N° 42), p.p.143-151.

2- **Myriam QUÉMÉNER**, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », Revue Sécurité et Stratégie 2011/1 (5), p.p.56-67.

3- **Zygmunt BAUMAN, Didier BIGO et al.** « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », Revue Cultures & Conflits, 215/02 n° 98, p.p.133-166.

C - Droit de l'Union Européenne:

- Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du parlement européen et du Conseil, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-états Unis, [notifiée sous le numéro C(2016) 4176] (Texte présentant de l'intérêt pour l'EEE) (2016/1250/UE), JOUE, L 207/1 du 01/08/2016. https://www.eur-lex.europa.eu/legal-content/FR/, consulté le 12/05/2020.

D- Jurisprudence :

- Arrêt de la Cour de Justice de l'Union Européenne (G. Ch.) du 16 juillet 2020, affaire C-311/18, Data Protection Commissioner contre/ Facebook Ireland Ltd et Maximillian Schrems. https://www.curia.europa.eu/jcmc/jcmc/Jo2_7052/fr/, consulté le 14/08/2020.

E- Articles de presse :

1-**Matthew ROSENBERG, Nicholas CONFESSORE et Carole CADWALLADR**, « How Trump Consultants Exploited the Facebook Data of Millions », The New York Times, March 17, 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html, consulté le 28 avril 2018.

2-**Olivia SOLON**, « Facebook says Cambridge Analytica may have gained 37m more users' data», The Guardian, April 04, 2018. https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought, consulté le 20 avril 2018.

3-Stephen LAM, « Cambridge Analytica : 87 millions de comptes Facebook concernés », article publié le 04/04/2018 à 21h52- Mis à jour le 05/05/2018 à 10h46, sur le site : http://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernes_5280752_ 4408996.html, consulté le 23 avril 2018.

4-Thomas CHENEL, « Google et Facebook ne pourront plus transférer comme avant les données des utilisateurs européens », article publié le 16/07/2020 à 13h02 à partir de l'adresse suivante : https://www.businessinder.fr/, consultée le 27/07/2020.

F- Rapport :

-Christiaan BEEK, « Déclin des logiciels de demande de rançon au 2e semestre 2017 », p.p.32-34. Rapport McAfee Labs- Prévisions 2017 en matière de menaces, novembre 2016. https://www.mcafee.comfrresourcesreportsrp-threats-predictions-2017.pdf. , consulté le 12/03/2019.

الهوامـش:

[1] راجع نص المادة 1/10-5 من القانون رقم 18-04 المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 27، الصادر في 13 ماي 2018، ص.ص.6-7. (تم الاطلاع عليه في 2019/08/12.)

[2] راجع نص المادة 3/10 من القانون رقم 18-04 المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، سالف الذكر، ص.7. (تم الاطلاع عليه في 2019/08/12.)

[3] راجع نص المادة 2(ب)،(ه)،(و) من القانون رقم 09-04 المؤرخ في 05 أوت 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 47، الصادر في 16 أوت 2009، ص.5.(تم الإطلاع عليه في 2018/06/02.)

[4] قانون رقم 18-07 مؤرخ في 10 جوان 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 34، الصادر في 10 جوان 2018، ص.12.(تم الاطلاع عليه في 2019/05/14.)

تنص المادة 03 منه، على ما يلي: "[...]. **"الشخص المعني"**: كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة؛

"معالجة المعطيات ذات الطابع الشخصي" المشار إليها أدناه "معالجة": كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل أخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف؛

"المعالجة الآلية": العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها؛ [...]."

[5] **أحمد السيد كردي**، "أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها"، مقال منشور عبر الموقع الالكتروني التالي:
https://www.kenanonline.com/user/ahmedkordy/posts/323552(تم الاطلاع عليه بتاريخ 2019/11/12.)

جمال محمد غيطاس، "الأمن المعلوماتي والجرائم الإلكترونية...أدوات جديدة للصراع"، مقال منشور في يوم الخميس، 01 مارس 2012، على الساعة 12:38 من توقيت مكة المكرمة، عبر الموقع الإلكتروني التالي: https://www. AlJazeeraCenter.forStudies.html(تم الاطلاع عليه بتاريخ 2020/01/20.)

راجع كذلك نص المادتين 303 مكرر و303 مكرر 1، من الأمر رقم 66-156 المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات(الجزائر)، المعدل والمتمم، ص.83.(تم الاطلاع في 2020/06/02.)

راجع كذلك نص المادة 164 من القانون رقم 18-04، سالف الذكر. ص.30. (تم الاطلاع في 2020/06/02.)

[6] **Zygmunt BAUMAN, Didier BIGO et al.,** « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », Cultures & Conflits, 98 | été 2015, p.p.134-136 et 139-141. https://conflits.revues.org/19033

[7] قانون رقم 16-01 مؤرخ في 06 مارس 2016 يتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 14، الصادر في 07 مارس 2016، ص.10.(تم الاطلاع عليه في 2017/06/02.)

تنص المادة 38 منه، على ما يلي: "الحريات الأساسية وحقوق الإنسان والمواطن مضمونة. [...]."

[8] **مروة زين العابدين صالح**، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، مصر، 2017، ص-ص.336- 338.

تنص المادة 02 من القانون رقم 09-04، سالف الذكر، ص.05.، على ما يلي:" يُقصد في مفهوم هذا القانون بما يلي:

أ- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية. [...]."

راجع كذلك نص المادة 394 مكرر 2، من الأمر رقم 66-156(الجزائر)، سالف الذكر، ص.113. (تم الاطلاع عليه في 2018/06/02.)

[9] **Olivia SOLON**, « Facebook says Cambridge Analytica may have gained 37m more users' data», The Guardian, April 04, 2018. https://www.the guardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought, consulté le 20/04/2018.

- **Matthew ROSENBERG, Nicholas CONFESSORE et Carole CADWALLADR**, « How Trump Consultants Exploited the Facebook Data of Millions », The New York Times. March 17, 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html, consulté le 28 avril 2018.

- **Stephen LAM**, « Cambridge Analytica : 87 millions de comptes Facebook concernés », article publié le 04/04/2018 à 21h52- Mis à jour le 05/05/2018 à 10h46, sur le site : http://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernes_5280752_ 4408996.html, consulté le 23 avril 2018.

[10] **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتي، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص.145.

هدى هامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص.20.

Voir aussi : **Arnaud BELLEIL**, « La régulation économique des données personnelles ? », LEGICOM 2009/1 (N° 42), p.p.150-151.

أنظر كذلك أحكام المواد 38 و40 و41 من دستور الجزائر لسنة 2016، سالف الذكر، ص.10. (تم الاطلاع عليه في 2017/06/02.)

أنظر كذلك أحكام المواد من 296 إلى 299، والمادتين 303 مكرر و303 مكرر1 من الأمر رقم 66-156(الجزائر)، سالف الذكر، ص.ص.79-80-81-83. (تم الاطلاع عليه في 2020/07/02.)

[11] **حسن طاهر داود**، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص.73.

خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2010، ص.76.

عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية(الحاسب الآلي وشبكة المعلومات(الإنترنت))، دار الوراق للطباعة والنشر والتوزيع، بيروت، لبنان، 2004، ص.ص.368-369.

[12] **عمرو عيسى الفقي**، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الاسكندرية، مصر، 2006، ص.ص.107-109.

محمد عبد حسين الطائي، ينال محمود الكيلاني، إدارة أمن المعلومات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2015، ص.ص.142-147.

Voir aussi : **Zouheir TRABELSI, Henri LY**, « La sécurité sur Internet, Lavoisier », Paris, 2005, p.p. 69-70-88.

[13] **Christiaan BEEK**, « Déclin des logiciels de demande de rançon au 2e semestre 2017 », p.p. 32-34. Rapport McAfee Labs- Prévisions 2017 en matière de menaces, novembre 2016. https://www.mcafee.comfrresourcesreportsrp-threats-predictions-2017.pdf., consulté le 12/03/2019.

[14] **دلال صادق الجواد، حميد ناصر الفتال**، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2008، ص.ص.15-16-17.

علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن، 2017، ص.ص.374- 376.

أنظر كذلك أحكام المواد من 394 مكرر إلى 394 مكرر7 من الأمر رقم 66-156(الجزائر)، سالف الذكر، ص.113. (تم الاطلاع عليه في 2019/06/02.)

[15] راجع نص المادة 09 من القانون رقم 18-07، سالف الذكر، ص.14. (تم الاطلاع عليه في 2019/06/20.)

[16] راجع أحكام المادة 06 من القانون رقم 18-07، سالف الذكر، ص.13. (تم الاطلاع عليه في 2019/06/20.)

[17] راجع نص المادة 18 من القانون رقم 18-07، سالف الذكر، ص.ص.15-16. (تم الاطلاع عليه في 2019/06/21.)

[18] راجع نص المادتين 07 و08 من القانون رقم 18-07، سالف الذكر، ص.ص.13-14. (تم الاطلاع عليه في 2019/06/21.)

[19] راجع أحكام المادة 5/07 من القانون رقم 18-07، سالف الذكر، ص.14. (تم الاطلاع عليه في 2019/06/20.)

[20] راجع أحكام المواد 12 و 13 و14 و17 من القانون رقم 18-07، سالف الذكر، ص.ص.14-15. (تم الاطلاع عليه في 2019/06/24.)

[21] تنص **المادة 13** من القانون رقم 04/09، سالف الذكر، ص.08.، على ما يلي:" تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم." (تم الاطلاع عليه في 2019/05/20.)

[22] **مرسوم رئاسي رقم 15-261** مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 53، الصادر في 08 أكتوبر 2015، ص.16. (تم الاطلاع عليه في 2016/03/09.)

تنص **المادة 02** منه، على ما يلي:" الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل."

مرسوم رئاسي رقم 19-172 مؤرخ في 06 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها ، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 37، الصادر في 09 جوان 2019، ص.ص.05-07. (تم الاطلاع عليه في 2019/07/04.)

تنص **المادة 02** منه، على ما يلي:" الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني."

وتنص **المادة 24** من نفس المرسوم الرئاسي(رقم 19-172)، على ما يلي:" تلغى جميع الأحكام المخالفة لهذا المرسوم، لاسيما أحكام المرسوم رقم 15-261 المؤرخ في 24 ذي الحجة عام 1436 الموافق 08 أكتوبر سنة 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها."

[23] راجع أحكام المواد من 303 مكرر إلى 303 مكرر3، من الأمر رقم 66-156(الجزائر)، سالف الذكر، ص.113. (تم الاطلاع عليه في 2018/07/04.)

[24] راجع نص المادة 04 من القانون رقم 09-04، سالف الذكر، ص.06. وكذا أحكام المواد 16 و17 و18 من نفس القانون، ص.08. (تم الاطلاع عليه في 2017/07/04.)

[25] راجع كذلك نص المادتين 65 مكرر5 و65 مكرر10، من الأمر رقم 66-155(الجزائر)، سالف الذكر، ص.30. (تم الاطلاع عليه في 2017/07/04.)

[26] راجع أحكام المواد 08 و10 و11 من نفس القانون رقم 09-04، سالف الذكر، ص.ص.07-08. وكذا نص المادة 14 من المرسوم الرئاسي رقم 19-172، سالف الذكر، ص.06. (تم الاطلاع عليه في 2018/07/04.)

[27] تنص المادة 24 من القانون رقم 18-07، سالف الذكر، ص.17.، على ما يلي:"[...]. في إطار ممارسة مهامها تُعلم السلطة الوطنية النائب العام المختص فورا، في حالة معاينة وقائع تحتمل الوصف الجزائي.[...]." (تم الاطلاع عليه في 2017/07/09.)

وتنص المادة 30 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 06، الصادر في 10 فيفري 2015، ص.11، على ما يلي:"[...]. تقوم السلطة الاقتصادية للتصديق الإلكتروني بتبليغ النيابة العامة بكل فعل ذي طابع جزائي يكتشف بمناسبة تأدية مهامها." (تم الاطلاع عليه في 2017/08/04.)

راجع كذلك نص المادتين 23 و24 من القانون رقم 20-05 المؤرخ في 28 أفريل 2020 ،الذي يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 25، الصادر في 29 أفريل 2020، ص.08. (تم الاطلاع عليه في 2020/05/14.)

راجع كذلك نص المادة 12 من القانون رقم 04/09، سالف الذكر، ص.08. وكذا المادة 2/14 من المرسوم الرئاسي رقم 19-172، سالف الذكر، ص.06. (تم الاطلاع عليه في 2017/05/10.)

[28] راجع نص المادة 03 من القانون رقم 09-04، سالف الذكر، ص.06. (تم الاطلاع عليه في 2017/05/10.)

راجع كذلك أحكام المواد 160، 164، 165، 187، 188، من القانون رقم 18-04، سالف الذكر، ص.ص.30-32. (تم الاطلاع عليه في 2019/05/12.)

[29] كان تنظيم وتشكيل "الهيئة" وفقا لنص المادة 06 من المرسوم الرئاسي الرقم 15-261(الملغى)، ص.17.، يشمل على: – لجنة مديرة؛ – مديرية عامة؛ – مديرية للمراقبة الوقائية واليقظة الإلكترونية؛ – مديرية للتنسيق التقني؛ – مركز للعمليات التقنية؛ – ملحقات جهوية.

لكن تشكيلة "الهيئة" وتنظيمها تغيّر وأصبح وفقا لنص المادة 04 من المرسوم الرئاسي رقم 19-172، سالف الذكر، ص.05.، الساري المفعول، يضم على **"مجلس توجيه"، "ومديرية عامة"** فقط.

راجع كذلك نص المادة 10 من نفس المرسوم الرئاسي(رقم 19-172)، ص.06. (تم الاطلاع عليه في 2020/05/10)

[30] تنص **المادة 20** من المرسوم الرئاسي رقم 19-172، سالف الذكر، ص.07.، على ما يلي:" يعاد إدماج القضاة والمستخدمين التابعين للدوائر الوزارية الأخرى العاملين على مستوى الهيئة، في هياكلهم الأصلية." (تم الاطلاع عليه في 2020/02/10)

[31] تنص **المادة 09** من القانون رقم 09-04، سالف الذكر، ص.07.، على ما يلي: " تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية." (تم الاطلاع عليه في 2017/05/10)

وتنص **المادة 18** من المرسوم الرئاسي رقم 19-172، سالف الذكر، ص.07.، على ما يلي:" تخضع الهيئة لمختلف أنواع المراقبة المنصوص عليها في التشريع والتنظيم المعمول بهما." (تم الاطلاع عليه في 2020/02/11)

[32] راجع نأحكام المواد 22 و23 و24 من القانون رقم 18-07، سالف الذكر، ص.ص.16-17. (تم الاطلاع عليه في 2019/02/10)

[33] راجع أحكام المادة 25 من القانون رقم 18-07، سالف الذكر، ص.17. (تم الاطلاع عليه في 2019/02/10)

[34] راجع أحكام المواد الواردة في الباب السادس(أحكام إدارية وجزائية) من القانون رقم 18-07، سالف الذكر، ص.ص.21-23. (تم الاطلاع عليه في 2019/02/10)

[35] راجع أحكام المادتين 24 و 26 من القانون رقم 18-07، سالف الذكر، ص.ص.17-18. (تم الاطلاع عليه في 2019/02/10)

[36] تنص المادة 12 من القانون رقم 18-07، سالف الذكر، ص.14.، على ما يلي:" ما لم يوجد نص قانوني يقضي بخلاف ذلك، تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية أو لترخيص منها طبقا للأحكام المنصوص عليها في هذا القانون." (تم الاطلاع عليه في 2019/02/13)

[37] راجع أحكام المواد من 13 إلى 16 من القانون رقم 18-07، سالف الذكر، ص.15. (تم الاطلاع عليه في 2019/02/14)

[38] راجع أحكام المواد من 17 إلى 21 القانون رقم 18-07، سالف الذكر، ص.ص.15-16. (تم الاطلاع عليه في 2019/02/15)

[39] راجع نص المادتين 30 و38 من القانون رقم 18-07، سالف الذكر، ص.ص.18-20. (تم الاطلاع عليه في 2019/02/15)

[40] راجع نص المادتين 26 و40 من القانون رقم 18-07، سالف الذكر، ص.ص.17-18-20. (تم الاطلاع عليه في 2019/02/15)

[41] راجع نص المادتين 39 و41 القانون رقم 18-07، سالف الذكر، ص.20. (تم الاطلاع عليه في 2019/02/17)

[42] راجع نص المادة 2/04 من القانون رقم 18-07، سالف الذكر، ص.13. (تم الاطلاع عليه في 2019/02/17)

[43] لمزيد من المعلومات حول الموضوع، راجع نص المادة 09 من القانون رقم 18-07، سالف الذكر، ص.14.

راجع كذلك أحكام المواد من 54 إلى 74، من القانون رقم 18-07، سالف الذكر، ص.ص. 22-23. (تم الاطلاع عليه في 2019/02/18)

راجع كذلك نص المادتين 18 مكرر، و51 مكرر، من الأمر رقم 66-156(الجزائر)، سالف الذكر، ص.ص.15-22.

راجع كذلك أحكام المواد من 65 مكرر إلى 65 مكرر 4، من الأمر رقم 66-155 المؤرخ في 08 جوان 1966(الجزائر)، الذي يتضمن قانون الإجراءات الجزائية، المعدل والمتمم، ص.29. (تم الاطلاع عليه في 2019/02/19)

[44] راجع أحكام المواد من 46 إلى 48، من القانون رقم 18-07، سالف الذكر، ص.21. (تم الاطلاع عليه في 2019/02/19)

[45] راجع نص المادتين 07 و08 من القانون رقم 18-07، سالف الذكر، ص.ص.13-14. (تم الاطلاع عليه في 2019/02/19)

[46] تنص المادة 42 من القانون رقم 18-07، سالف الذكر، ص.20.، على ما يلي:" ما عدا في حالة موافقتهم الصريحة، يجب الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني، من الأشخاص المعنيين بها مباشرة، ولا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها."

راجع كذلك أحكام المادتين 09/(ب) و2/14 من القانون رقم 18-07، سالف الذكر، ص.ص.14-15. (تم الاطلاع عليه في 2019/02/19)

[47] راجع نص المادة 10 من القانون رقم 18-07، سالف الذكر، ص.14. (تم الاطلاع عليه في 2019/02/19)

[48] تنص المادة 43 من القانون رقم 15-04، سالف الذكر، ص.12، على ما يلي:" لا يمكن على مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلاّ بعد موافقته الصريحة.

ولا يمكن مقدم خدمات التصديق الإلكتروني أن يجمع إلاّ البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى." (تم الاطلاع عليه في 2018/07/02.)

[49] راجع نص المادة 37 من القانون رقم 18-07، سالف الذكر، ص.ص.19-20. (تم الاطلاع عليه في 2019/02/20)

[50] راجع نص المادتين 44 و45 من القانون رقم 18-07، سالف الذكر، ص.21. (تم الاطلاع عليه في 2019/02/20)

[51] **Arrêt** de la Cour de Justice de l'Union Européenne (Grande. Ch.) du 16 juillet 2020, affaire C-311/18, Data Protection Commissioner contre/ Facebook Ireland Ltd et Maximillian Schrems, p.p.01-26. Disponible sur : https://www.curia.europa.eu/jcmc/jcmc/Jo2_7052/fr/, consultés le 05/08/2020.

Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du parlement européen et du Conseil, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-états Unis [notifiée sous le numéro C(2016) 4176] (Texte présentant de l'intérêt pour l'EEE) (2016/1250/UE), Journal Officiel de l'Union Européenne, L 207/1, du 01/08/2016, p.p.01-112. https://www.eur-lex.europa.eu/legal-content/FR/, consulté le 10/04/2020.

Voir aussi : **Thomas CHENEL**, « Google et Facebook ne pourront plus transférer comme avant les données des utilisateurs européens », article publié le 16/07/2020 à 13h02 à partir de l'adresse suivante : https://www.businessinder.fr/, consultée le 27/07/2020.

[52] **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**), Journal Officiel de l'Union Européenne, L 119/1, du 04/05/2016, p.p.01-88.

[53] راجع نص المادة 09/(هـ) من القانون رقم 18-07، سالف الذكر، ص.14. (تم الاطلاع عليه في 2019/02/20)

[54] راجع نص المادتين 32 و33 من القانون رقم 18-07، سالف الذكر، ص.ص.18-19. (تم الاطلاع عليه في 2019/02/21)

[55] راجع نص المادة 34 من القانون رقم 18-07، سالف الذكر، ص.19. (تم الاطلاع عليه في 2019/02/21)

[56] راجع نص المادة 35 من القانون رقم 18-07، سالف الذكر، ص.19. (تم الاطلاع عليه في 2019/02/22)

[57] راجع نص المادة 36 من القانون رقم 18-07، سالف الذكر، ص.19. (تم الاطلاع عليه في 2019/02/22)