مجلة جامعة دمشق للعلوم القانونية

اسم المقال: التشريعات الدولية والأوروبية والداخلية لحماية البيانات الشخصية
اسم الكاتب: نلمى الأشقر، د. جمال مذكور
رابط ثابت: https://political-encyclopedia.org/library/1815
تاريخ الاسترداد: 2025/05/05 04:27 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة – Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة دمشق للعلوم القانونية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

التشريعيات الدولية والأوروبية والداخلية لحماية البيانات الشخصية

إعداد طالبة الماجستير: **نلمى الأشقر** *

إشراف الدكتور: **جمال مذكور** **

الملخص

بعد أن استطاعت الثورة التكنولوجية الولوج إلى كافة أوجه حياة الأفراد، أصبحت خصوصية الأفراد معرضة للانتهاك وبات من السهل الاطلاع على البيانات الشخصية وأسرار الأفراد والتلاعب بها. ولذلك تسعى التشريعات إلى تكريس الحق في حماية البيانات الشخصية، والعمل على جعل البيانات الشخصية بمنأى عن أيّ انتهاكات ممكن حصولها في الوقت الحالي أو المستقبل. وبالتالي فإن هذا البحث الحالي يتناول الجهود الدولية والأوروبية والداخلية لحماية حق من الحقوق والحريات الأساسية للأشخاص الطبيعيين وهو حقهم في حماية البيانات الشخصية، لتحقيق الشعور بالأمان والطمأنينة في مجتمع أضحى فيه استعمال الوسائل المعلوماتية أمرًا ضروريًا لا غنى عنه. وقد أظهرت الدراسة أن التشريعات السورية غير قادرة على حماية البيانات الشخصية من تأثير المعلوماتية، ودعت إلى ضرورة سن قواعد قانونية صارمة ومباشرة تحدد هذا الحق وتلزم كافة الأفراد والكيانات باحترامه.

الكلمات المفتاحية: البيانات الشخصية، التشريعات الدولية، التشريعات الأوروبية، التشريعات الداخلية.

* قسم القانون الخاص–كلية الحقوق–جامعة دمشق.
** قسم القانون الخاص–كلية الحقوق–جامعة دمشق.

The International, European and internal legislation to protect personal data

Master student: Nelma Alashqer*

Summary

After the technological revolution penetrated all aspects of individuals' life, the privacy of individuals has become vulnerable to abuse, and it became easy to view and manipulation personal data and individuals' secrets. Therefore, legislations seek to enshrine the right to protect personal data, and to make personal data free of any violations that may occur at present or in the future. Thus, the current research deals with International, European and internal efforts to protect fundamental rights and freedoms of natural persons, which is their right to protect personal data. To achieve a sense of safety and tranquility in a society, where the use of information technology is indispensable. The study showed that the Syrian legislations are unable to protect personal data from the impact of informatics, and called for the need to enact strict and direct legal rules that define this right and oblige all individuals and entities to respect it.

Key Words: Personal data, international legislation, European legislation, internal legislation.

*Department of private law-Faculty of law-Damascus University.

المقدمة:

يشهد العالم اليوم ثورة في المعلومات والاتصالات، بدأت تظهر ملامحها منذ منتصف القرن العشرين، أحدثت تغييرات جذرية في جميع مجالات الحياة وأضحت سلاحًا ذا حدين، فبقدر التطور التكنولوجي الهائل الذي مسَّ حياة الأفراد وأسبغ عليها يسر ومرونة في التعامل والاتصال، إلا أن هذا التطور التكنولوجي، وبفعل الكفاءة العالية للوسائل التقنية وإمكاناتها اللامحدودة في مجال تحليل واسترجاع البيانات، حمل في ثناياه مخاطر عدة، فقد أثار التوسع في استخدام الحواسيب وإنشاء قواعد البيانات مخاوف حول انتهاك بيانات الأفراد الشخصية، ومكمن هذه المخاوف؛ أن هذه البيانات المجمّعة يمكن تخزينها لفترة غير محددة كما يمكن الرجوع إليها بمنتهى السرعة والسهولة؛ كما أنّ الإنترنت أتاحت تبادل البيانات والمعلومات بين المراكز المتباعدة والمختلفة، وأدت إلى تعاظم كمية البيانات الشخصية المُنتَجة والمُجمَّعة والمُعالجة، كما مكّنت من الحصول على البيانات الشخصية عن بعد بصورة غير مشروعة. مما هدّد خصوصية الفرد وسرية بياناته الشخصية.

وعلى وقع اكتساح التكنولوجيا الحديثة لمعظم الوسائل المستخدمة في الحياة اليومية، ما يمثله هذا الواقع من تهديد جدّي للبيانات الشخصية ومن خلالها للخصوصية وللحقوق والحريات المدنية والحقوق الشخصية الأخرى؛ وبالنظر للطابع الحساس الذي تتميز به البيانات الشخصية للأفراد، كونها أحد العناصر المكونة لمحل حقهم في الخصوصية؛ وبفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء عليها؛ وبالنظر إلى عدم كفاية القواعد القانونية التي تحمي الخصوصية وسرية البيانات من تأمين حماية ملائمة للبيانات الشخصية. استدعى ذلك بذل المزيد من الجهود سواء من المشرّع الدولي أو الأوروبي أو الوطني لسنّ تشريعات تهدف إلى حماية بيانات الأفراد الشخصية، وقد حملت هذه التشريعات مسمّى قوانين "حماية البيانات" أو "حماية البيانات الشخصية" أو "حماية الخصوصية"، وارتكزت بشكل أساسي على فلسفة

احترام حقوق الإنسان وحرياته الأساسية، وأقرّت تدابير تهدف إلى صون كرامته الأفراد وضمان خصوصية بياناتهم.

وفي وقت اتجهت الكثير من الدول إلى تبني تشريعات لحماية البيانات الشخصية، ووضع ضوابط حول معالجتها وحركتها وانتقالها إلى الدول الأخرى، وخاصة بعد تبني دول الاتحاد الأوروبي تشريع ملزم، أصبح موجّه لدول العالم، نجد أن البيانات الشخصية لم تحظَ بالعناية الكافية في المنظومة التشريعية السورية، التي خلت من تشريع يحمي البيانات الشخصية، وقد جاءت الحماية مقتصرة على نصوص متناثرة تحمي السرية وبعض البيانات والمعلومات.

مشكلة البحث:

تمحورت مشكلة البحث حول مدى تمكّن المشرّع الدولي والأوروبي من تطوير تشريعات لحماية البيانات الشخصية، وعدم كفاية تدابير المشرّع السوري وملائمتها فيما يخص هذه الحماية.

أهمية البحث:

تأتي أهمية هذا البحث كونه يسلط الضوء على الحماية القانونية لحق من حقوق الإنسان وحرياته الأساسية، هو الحق في البيانات الشخصية، لدورها في حفظ خصوصية الأفراد وصيانة كرامتهم وإنسانيتهم؛ ولأهميتها الاقتصادية في الوقت الحاضر وما تمثله من قيمة لا تقل عن قيمة الأشياء المادية.

هدف البحث:

يهدف البحث إلى إبراز واقع الحماية القانونية للبيانات الشخصية في التشريعات الدولية والأوروبية وقدرتها على مجاراة التطور الحاصل في الواقع التكنولوجي، وبالمقابل إظهار قصور تدابير المشرع السوري بخصوص هذه الحماية من خلال عرض أهم المواد القانونية المتناثرة في التشريعات السورية، ذات الصلة بموضوع البحث، وإظهار ضرورة

وجود تشريع سوري قادر على حماية البيانات الشخصية ومجاراة متغيرات وتحديات التطور التكنولوجي.

منهج البحث:

إن الهدف من هذا البحث هو التعرّض لأهم التشريعيات الدولية والأوروبية والداخلية الخاصة بحماية البيانات الشخصية، فالبحث لن يُقدّم كدراسة تقليدية مقارنة بين الموقف التشريعي الدولي والأوروبي، وبين الموقف التشريعي الداخلي ممثلًا بالسوري نظرًا لغياب الاهتمام التشريعي بهذه الحيثية الجديدة في التشريعات السورية، إنّما سيعرض أهم التطورات التشريعية التي طرأت على موضوع البحث، وأهم العناصر الأساسية لحماية البيانات الشخصية التي تكونت في التشريعات الدولية وتطورت في التشريعات الأوروبية، ولا تزال شبه مغيبة في التشريع السوري. لذلك كان من المناسب، لموضوع البحث، اعتماد المنهج الوصفي لعرض أهم التشريعات الدولية والأوروبية التي عالجت موضوع حماية البيانات الشخصية، وأهم التشريعات الداخلية ذات العلاقة بموضوع البحث، وأيضًا كان من الضروري الأخذ بالمنهج التحليلي بهدف تحليل الموقف التشريعي عمومًا، كما أسهم الاعتداد بالمنهج المقارن في الإسقاط ما أمكن على التطور التشريعي الدولي والأوروبي وعلى موقف المشرّع السوري.

خطة البحث:

وضمن هذا الإطار، تشتمل خطة البحث مقدمة، تضمنت مشكلة البحث وأهميته وهدفه ومنهجه، وفرعين رئيسيين؛ الأول بعنوان التشريعات الدولية والأوروبية لحماية البيانات الشخصية، والثاني بعنوان التشريعات الداخلية لحماية البيانات الشخصية، وخاتمة تتضمن نتائج البحث وتوصياته.

وهنا نرى من الضرورة بمكان، الإشارة إلى العائق الرئيس الذي واجهنا في معرض هذه الدارسة، ألا وهو نقص المراجع القانونية والفقهية العربية المتوافرة حول هذا البحث، لذلك كان لا بد من الاستعانة بالتشريعات الدولية والأوروبية والسورية ذات العلاقة

بموضوع البحث كمصادر أساسية، وهذا الأمر، بقدر ما هو نقطة تسجل على البحث، بقدر ما هو نقطة تسجل لصالح البحث، كونه يبرز أهمية البحث وأصالته.

الفرع الأول: التشريعات الدولية والأوروبية لحماية البيانات الشخصية:

شاع استخدام مفهوم حماية البيانات الشخصية في ظل استخدام أجهزة الحاسب الآلي وإنشاء قواعد البيانات، ومخاطر المعالجة الآلية للبيانات المتعلقة بالحياة الخاصة[1]؛ فاتجاه الكثير من دول العالم، بمختلف هيئاتها ومؤسساتها العامة والخاصة، إلى تنظيم عملها من خلال إنشاء قواعد تحتوي بيانات متنوعة ومفصلة تتعلق بحياة الأفراد الخاصة بصورة مباشرة، كالحالة الصحية أو العائلية أو الاجتماعية أو العملية، وبيانات أخرى تسمح برسم صورة لاتجاهاته وميوله، كاتجاهاته السياسية ومعتقداته الدينية وتعاملاته المالية وهواياته[2]، جعل البيانات الشخصية مجمّعة ومتوافرة ومتكاملة وسهلة المنال بعد أن كانت منعزلة متفرقة والتوصل إليها صعب[3]؛ كما أن إمكانات أجهزة الحاسب الآلي في تخزين كم هائل من البيانات والمعلومات بصفة دائمة، جعل الحياة الخاصة للأفراد شفافة تُظهر أدق الأسرار الشخصية[4]؛ كما أن قدرة أجهزة الحاسب الآلي على استرجاع البيانات المتفرقة ودمجها وتحليلها، حوّل البيانات الشخصية والتي قد تكون غير ضارة وليس لها قيمة أو أهمية، إلى بيانات تفصيلية عن حياة الفرد وأنشطته ومسلكه[5]، بالإضافة لقدرة هذه الأجهزة على نقل البيانات، عبر وسائل متنوعة مثل خطوط الهاتف أو الاتصالات عبر الكابلات أو الأقمار الصناعية أو الشبكات، بسهولة ويسر وفي ثوانٍ معدودة، ومن أدنى بقاع الأرض إلى أقصاها، أدى إلى تسهيل جمع البيانات وهو ما شكّل تهديدًا حقيقيًا على الخصوصية[6].

---

[1]– بولين أنطونيوس أيوب: الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، 2009، ص66.

[2]–المرجع السابق، ص108.

[3]–المرجع السابق، ص115.

[4]–المرجع السابق، ص127–129.

[5]–المرجع السابق، ص132.

[6]–المرجع السابق، ص133–134.

وتعزز استخدام مفهوم حماية البيانات الشخصية في البيئة الرقمية وتحديدًا الإنترنت، نتيجة قدرتها غير المسبوقة على جمع ومعالجة البيانات الشخصية، الأسرية والصحية والمالية والاجتماعية وغيرها لأغراض الرقابة أو التسويق أو الأبحاث أو حتى مجرد الإتجار بالبيانات؛ فقد سهلت الإنترنت جمع البيانات الشخصية فالتصفح عبر الإنترنت يترك لدى الموقع المزار كمية واسعة من البيانات، كما أن الكثير من المواقع التفاعلية ومواقع التجارة الإلكترونية تطلب من المستخدم تقديم بياناته الشخصية للاستفادة من الخدمات أو لإتمام عملية الشراء[7]؛ كما أدت الإنترنت إلى تعاظم كمية البيانات الشخصية المنتجة والمجمّعة والمعالجة بعد التوسع الهائل في استخدام شبكة الإنترنت، ونقل مختلف أنشطة الحياة من العالم المادي إلى العالم الافتراضي[8]. فجمع شتات هذه المعلومات قد يشكل بيانًا بأنشطة الفرد، وقد تكشف هذه البيانات عند تحليلها، تفاصيل كثيرة قد لا يرغب الشخص بكشفها، وفي نفس الوقت تصبح هذه البيانات مادة غنية ومحلًا للبيع[9]. هذه الآفاق والفرص الجديدة التي وفرتها تقنيات المعلومات والاتصالات والأجهزة التي تستخدمها، حملت معها مخاطر عدّة، نتيجة جمع البيانات أو جمعها بطريقة عشوائية وخارج الأطر القانونية الملائمة، أو نتيجة لانكشاف البيانات المُعالجة[10]. وبما أن هذه البيانات تحتوي على معلومات تتعلق بالشخص الطبيعي وتمكّن من تحدد هويته، كالاسم والجنس والسكن والديانة وفصيلة الدم، والوضع الاجتماعي، والشهادات المدرسية، والوظيفة والمهنة والخدمة العسكرية الإلزامية، وتاريخ

[7]– د. بولين أنطونيوس أيوب، مرجع سابق، ص193–195.
[8]– د. أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية،2007، ص651–656
[9]– د. بولين أنطونيوس أيوب، مرجع سابق، ص205.
[10]– د. منى الأشقر جبور؛ د. محمود جبور: البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، أبحاث ودراسات (5)، الطبعة الأولى، بيروت–لبنان، 2018، ص29.

الدخول والخروج من الدولة[11]، فهي توحي بالخصوصية ولا يجوز للغير أن يطّلع على هذه البيانات في أي نظام معلوماتي دون إذن من المعني[12].

وعلى أثر الإحساس بهذه المخاطر تكاتفت الجهود لإقرار تشريعات لحماية البيانات الشخصية وحفظ خصوصية الأفراد من أي انتهاك. وفيما يأتي عرض لهذه التشريعات، ثم عرض إطارها القانوني الذي يبرز أهمية المعالجة التشريعية المتكاملة في كفالة حماية فعّالة للبيانات الشخصية.

أولًا: المواثيق والاتفاقيات والتشريعات الدولية والأوروبية لحماية البيانات الشخصية.

تبلور الاهتمام الدولي بحماية البيانات الشخصية، على شكل توجيهات واتفاقيات تنظّم عملية جمع ومعالجة بيانات الأفراد الشخصية، فنشأت اتفاقيات وقواعد إرشادية تعدّ مرجعية دولية، كالدليل الإرشادي الصادرة عن منظمة التعاون الاقتصادي والتنمية لعام 1980، واتفاقية مجلس أوروبا رقم 108 لعام 1981، وقرار الأمم المتحدة رقم 95/45 لعام 1990. كما سنّ الاتحاد الأوروبي إرشادات وتشريعات لحماية بيانات مواطني الاتحاد فأصدر الإرشاد الأوروبي رقم 95/46/EC لعام 1995، وفي 14 نيسان 2016 أصدر اللائحة العامة لحماية البيانات الشخصية. وفيما يأتي عرض لهذه الجهود بمزيد من التفصيل وباعتماد التسلسل التاريخي من الأقدم إلى الأحدث.

1- دليل منظمة التعاون الاقتصادي والتنمية لعام 1980.

أعدت منظمة التعاون الاقتصادي والتنمية، دليلًا تبناه مجلس المنظمة في توصيته الصادرة بتاريخ 23 أيلول من عام 1980، تحت عنوان حماية الخصوصية وتدفق البيانات الشخصية عبر الحدود. وقد أكدت توصية المجلس بوجوب أن تأخذ الدول

[11]- د. نعيم مغبغب: مخاطر المعلوماتية والإنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، 1998، ص185.

[12]- د. منى تركي الموسوي؛ جان سيريل فضل الله: الخصوصية المعلوماتية وأهميتها ومخاطر التقانات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، جامعة بغداد، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، 2013م، ص6، منشور على شبكة الإنترنت يمكن الوصول إليه عبر الرابط الآتي: https://www.iasj.net/iasj/download/c457ac3d2aaf7fdd
التحميل والدخول إلى الموقع بتاريخ 2020/8/8 الساعة 11:30 صباحًا.

الأعضاء بعين الاعتبار مبادئ حماية الخصوصية وحريات الأفراد التي تضمنها الدليل، وأن تتخذ التدابير التشريعية لتضمينها في تشريعاتها الداخلية. كما طلبت من الدول الأعضاء تجنب خلق عوائق غير مبررة أمام التدفق الحر للبيانات الشخصية بين الدول الأعضاء، من أجل تنمية العلاقات الاقتصادية والاجتماعية فيما بينها، والتعاون من أجل تنفيذ ما تضمنه الدليل[13].

2– اتفاقية مجلس أوروبا رقم 108 لحماية الأفراد من المعالجة الآلية للبيانات الشخصية.

وفي خطوة لاحقة صدرت اتفاقية حماية البيانات رقم 108 في 28 كانون الثاني 1981، كأول نص دولي ملزم، يتعين بموجبه على الدول الأعضاء، اتخاذ الخطوات اللازمة على المستوى التشريعي، لتطبيق المبادئ التي تحددها الاتفاقية[14]، وتهدف هذه الاتفاقية، كما جاء في ديباجتها، إلى التوفيق بين احترام حقوق الإنسان وحرياته الأساسية ولا سيما احترام الحق في الخصوصية للجميع من دون استثناء، وبين حرية تبادل المعلومات عبر الحدود، وتوفير الحماية القانونية للأفراد فيما يتعلق بالمعالجة الآلية

[13]–RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS:
• that Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
• that Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
• that Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
• That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

[14]- Article 4 – Duties of the Parties: "1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter. 2.These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party".

لبياناتهم الشخصية[15]. وقد برزت الحاجة لمثل هذه الحماية في وقت تزايد فيه استخدام أجهزة الحاسب الآلي في أعمال الإدارة المختلفة، كما أدى اندماج الحاسب مع الاتصالات إلى معالجة البيانات على نطاق عالمي وليس وطني فقط[16].

3- قرار الأمم المتحدة رقم 95/45 لعام 1990.

وفي مرحلة لاحقة أصدرت مفوضية الأمم المتحدة لحقوق الإنسان القرار رقم 95/45 بتاريخ 14 كانون الأول 1990 والمعروف بدليل الأمم المتحدة لتنظيم ملفات البيانات الشخصية المؤتمتة لعام 1990[17]. تضمن الدليل المبادئ التوجيهية لحماية البيانات الشخصية والتي يتعين على الدول تضمينها في تشريعاتها الوطنية[18]، كما أشار الدليل إلى ضرورة أن تضع الدول قوانين تلزمها باحترام مبادئ حماية البيانات الشخصية، وحقوق الأشخاص المعنيين بها[19].

4- الإرشاد الأوروبي رقم 95/46/EC الصادر بتاريخ 24 تشرين الثاني عام 1995.

أصدر الاتحاد الأوروبي الإرشاد رقم 95/46/EC، بتاريخ 24 تشرين الأول من عام 1995، بشأن حماية الأشخاص الطبيعيين من معالجة البيانات الشخصية وحرية انتقالها عبر الحدود، وألزم دول الاتحاد تضمين أحكامه في تشريعاتها الوطني. واقتصر تطبيق

---

[15]–Preamble: The member States of the Council of Europe, signatory hereto. Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms; Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing; Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples".

[16]– د. بولين أنطونيوس أيوب، مرجع سابق، ص315-316.

[17]- وقد تبنته وأصدرته الجمعية العامة للأمم المتحدة بالاستناد للمادة العاشرة من ميثاق الأمم المتحدة التي تمنح الجمعية حق إصدار توصيات للدول الأعضاء وتلزم الدول المذكورة بمراعاة هذه التوصيات عند وضع القواعد الوطنية المتعلقة بموضوع التوصية.

[18]– قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، فقرة (أ).

[19]- قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، المادة (8/أ).

قواعد هذا الإرشاد على عمليات معالجة البيانات الشخصية التي تجري ضمن الاتحاد الأوروبي[20]. وقد شكل الإرشاد نواة الحركة التشريعية الأوروبية الهادفة إلى حماية البيانات الشخصية، ومن حيث مبادئ الحماية المقررة فقد جاءت أوسع وأكثر شمولية من المبادئ التي تضمنتها المدونات السابقة[21].

5– اللائحة العامة الأوروبية بشأن حماية البيانات GDPR رقم 679 لعام 2016.

أصدر المشرع الأوروبي في 14 نيسان 2016، نظام قانوني أوروبي جديد باسم النظام العام أو اللائحة العامة لحماية البيانات الشخصية (General Data Protection Regulation)، لتحل محل التوجيه رقم EC/46/95، ومحل جميع القوانين الوطنية للاتحاد الأوروبي، ولتتجاوز نقاط الضعف في الإرشاد الأوروبي السابق؛ من حيث إلزامية القواعد القانونية، فاللائحة تتمتع بقوة القانون، دون الحاجة إلى إصدار قوانين وطنية لإعطائها القوة التنفيذية[22]؛ ومن حيث مجال التطبيق، فاللائحة ملزمة لأي كيان يقوم بمعالجة بيانات شخصية لأفراد من الاتحاد الأوروبي، حتى في حالة وجوده خارج النطاق الإقليمي لدول الاتحاد الأوروبي[23]. فهدف اللائحة تعزيز حماية البيانات

[20]–نص المادة (2/3) باللغة الإنكليزية.
"This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law...".

[21]–د. بولين أنطونيوس أيوب، مرجع سابق، ص321–322.

[22]–نص المادة (99) من اللائحة الأوروبية:
"1.This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. 2. It shall apply from 25 May 2018"

[23]–نص المادة (3) باللغة الإنكليزية:
"1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2.This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.

الشخصية في أوروبا، وتحقيق الانسجام بين القوانين الأوروبية من جهة، ومواكبة التطورات المتسارعة في مجال تقنيات المعلومات من جهة أخرى[24]، لتعبّر عن سياسات جديدة تمثل نموذجًا لباقي دول العالم، وتعزز الانتقال من حالة الفوضى إلى حالة التنظيم، ومن حالة الانفتاح اللامحسوب إلى حالة الانفتاح المنضبط، كما تعبّر عن حالة دولية جديدة للتعامل مع العولمة في مواجهة المصالح الوطنية، والانتقال إلى مرحلة استعادة دور الدولة في مجال الأمن والحماية وفق بيئة جديدة، لتصبح اللائحة الأوروبية بداية حقيقة لقواعد عالمية ملزمة في مجال حماية البيانات خارج دول الاتحاد الأوروبي[25].

ثانيًا: الإطار القانوني لتشريعات حماية البيانات الشخصية.

يرتكز الإطار القانوني الذي تندرج في نطاقه تشريعات حماية البيانات الشخصية على فلسفة احترام حقوق الإنسان، وضمان حماية الحق في الخصوصية، من خلال إقرار مجموعة من الآليات تضمن تحقيق هذه الفلسفة. وبالرغم من أن حماية البيانات الشخصية ترتبط بالحق في الخصوصية ولا تُعّد حقًا في حد ذاتها[26]، إلا أنّ هناك

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

[24]-د. منى الأشقر جبور، د. محمود جبور، مرجع سابق، ص55.

[25]–مقال بعنوان: كتاب البيانات الشخصية: الصراع على نفط القرن الحادي والعشرين، منشور على شبكة الإنترنت يمكن الوصول إليه عبر الدخول إلى الموقع الآتي: https://www.politics-dz.com/، الدخول إلى الموقع بتاريخ 2020/9/25 الساعة 2 مساءً.

[26]–اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (1): "الغرض من هذه الاتفاقية هو تأمين كل فرد في إقليم كل طرف، مهما كانت جنسيته أو إقامته، واحترام حقوقه وحرياته الأساسية، وبخاصة حقه في الخصوصية، فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية المتعلقة به"؛ دليل منظمة التعاون الاقتصادي والتنمية، المادة (2): "تنطبق هذه الإرشادات على البيانات الشخصية، سواء في القطاعين العام أو الخاص، والتي تشكل خطرًا على الخصوصية وحريات الأفراد بسبب طريقة معالجتها، أو بسبب طبيعتها أو السياق الذي تُستخدم فيه"؛ الإرشاد الأوروبي رقم EC/46/95، المادة (1/1): "وفقًا لهذا الإرشاد، تحمي الدول الأعضاء الحقوق والحريات الأساسية للأشخاص الطبيعيين، ولا سيما حقهم في الخصوصية فيما يتعلق بمعالجة البيانات الشخصية".

اعتراف بالبيانات الشخصية كحق أساسي من حقوق الإنسان[27]. وفيما يأتي عرض لأطر القانونية في القوانين الأوروبية، وتوصيات الجهات الدولية.

أ– إدراج قائمة بالتعريفات الضرورية: حددت قوانين الحماية، عددًا من التعريفات الضرورية لوضوح النص ومجال تطبيقه. وأهم ما تضمنته قوانين حماية البيانات الشخصية من تعريفات؛ تعريف البيانات الشخصية، فعرّف دليل منظمة التعاون الاقتصادي والتنمية واتفاقية مجلس أوروبا، البيانات الشخصية بأنّها: "كل معلومة عائدة لشخص طبيعي محدّد أو قابل للتحديد"[28]. فالبيانات الشخصية، حسب هذا التعريف، هي المعلومات التي يمكن ربطها بشخص معيّن وتتيح إمكانية تحديد هويته والتعرّف عليه. إلا أن هذا التعريف أثار بعض الإشكالات، إذ أنه استثنى بيانات يمكنها أن تساعد على تحديد هوية الشخص أو تعقبه وملاحقته، عبر سماحها بتحديد هويته بطريقة غير مباشر، وإن لم تكن مرتبطة بهويته الشخصية مباشرة، وترد في هذا السياق البيانات التي لا تعود إلى الشخص الطبيعي، وإنّما إلى وسيلة يستعملها: كرقم تسجيل السيارة، ورقم الهاتف الثابت والنقال، أو العنوان الخاص برقم التعريف الإلكتروني للجهاز IP، أو المعلومة المرتبطة بأية وسيلة أخرى يحملها. وتكمن خطورة استثناء هذه الفئة من البيانات، في الإمكانية التي تتيحها، بالتعدي على خصوصية الأشخاص من خلال

[27]–اللائحة العامة الأوروبية بشأن حماية البيانات GDPR رقم 679 المادة (2/1): تحمي هذه اللائحة الحقوق والحريات الأساسية للأشخاص الطبيعيين ولا سيما حقهم في حماية البيانات الشخصية". ميثاق الحقوق الأساسية للاتحاد الأوروبي، والذي اعتمده البرلمان الأوروبيّ ومجلس الوزراء والمفوضية الأوروبيّة بتاريخ 2000/12/7، المادة (7): "لكل شخص الحق في احترام حياته الخاصة وحياته العائلية وبيته واتصالاته". وجاء في المادة (8) من الميثاق: "1–لكل شخص الحق في حماية البيانات الشخصية التي تتعلق به.2–يجب أن تعامل مثل هذه البيانات على نحو ملائم لأغراض محددة، وعلى أساس موافقة الشخص المعني، أو على أساس مشروع يحدده القانون، ويكون لكل شخص الحق في الوصول إلى البيانات التي تم جمعها وتتعلق به، وحق الحصول عليها صحيحة.3–يخضع الإذعان لهذه القواعد لرقابة هيئة مستقلة".

[28]–المادة (1/ب) من دليل منظمة التعاون الاقتصادي والتنمية لحماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود؛ والمادة (2/أ) من اتفاقية مجلس أوروبا لحماية الأفراد في مجال المعالجة الآلية للبيانات الشخصية، باللغة الإنكليزية:

"Personal data" means any information relating to an identified or identifiable individual (data subject).

معالجة هذه البيانات، لعدم إمكانية تطبيق النص الذي يستبعدها بطريقة غير مباشرة، لذلك يجب أن يؤخذ بعين الاعتبار، جميع الوسائل المتاحة والممكنة التي تجعل الشخص قابلًا للتعريف[29]. وبعد ذلك، اعتمدت التشريعات اللاحقة مفهومًا أوسع للبيانات الشخصية، بما يضمن جانبًا موسعًا من الحماية القانونية. فعرّف المشرع الأوروبي، في الإرشاد الأوربي رقم 95/46/EC، البيانات الشخصية بأنها: "أي معلومة متعلقة بشخص طبيعي معرّف أو يمكن التعرّف عليه "الشخص المعني"، والشخص الذي يمكن التعرف عليه هو الذي يمكن معرفته، بصفة مباشرة أو غير مباشر، لاسيما بالرجوع إلى رقم التعريف، أو لواحد أو أكثر من العناصر المميزة لهويته البدنية أو الفسيولوجية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية[30]". ثمّ طوّر المشرع الأوروبي، بموجب اللائحة العامة لحماية البيانات الشخصية(GDPR)، تعريف البيانات الشخصية بإضافة عناصر جديدة فعرّفها بأنها: "أي معلومة متعلقة بشخص طبيعي مُعرّف أو يمكن التعرّف عليه "الشخص المعني"، والشخص الطبيعي الذي يمكن التعرف عليه هو الذي يمكن معرفته بصفة مباشر أو غير مباشرة، لاسيما بالرجوع إلى عنصر مُعَرف، مثل الاسم ورقم التعريف وبيانات الموقع ومعرّف الاتصال عبر الإنترنت، أو لواحد أو أكثر من العناصر المميزة لهويته الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"[31]. ويتناسب هذا التوسع في التعريف مع قانون يهدف إلى توفير حماية

29- د. منى الأشقر جبور؛ د. محمود جبور، مرجع سابق، ص76.

30-نص المادة (2/أ) من الإرشاد الأوربي رقم 95/46/EC، باللغة الإنكليزية:

Article 2. (a) "personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

31-نص (المادة 1/4) من اللائحة العامة لحماية البيانات الشخصية باللغة الإنكليزية:

Article 4. 1. "Personal data" means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

قانونية فاعلة، عن طريق الإحاطة بمختلف هذه البيانات، كما أنه ذو دلالة تمثيلية وليس حصرية؛ كما عرّفت غالبية القوانين الدولية والأوروبية الصادرة في هذا المجال، معالجة البيانات الشخصية، والتي ترتكز في جوهرها، على التعامل مع البيانات الشخصية وتحتل على هذا الأساس، حيزًا واسعًا في قوانين الحماية[32]. فعرّفت اتفاقية مجلس أوروبا المعالجة الآلية بأنها: "العمليات التي تجري كليًا أو جزئيًا بالوسائل الآلية، وتتضمن تخزين البيانات، وتنفيذ العمليات المنطقية أو الحسابية على تلك البيانات أو تعديلها أو محوها أو استرجاعها أو نشرها"[33]. إلا أن ما يؤخذ على هذا التعريف أنه استثنى عمليات المعالجة اليدوية البحتة كما أنه لم يوسع من نطاق عمليات المعالجة التي تتعرض لها البيانات والتي يمكنها أن تساعد في تحديد هوية الشخص أو تعقبه. ثم تطور مفهوم المعالجة في التشريعات اللاحقة فعرّفها المشرع الأوروبي في التوجيه الأوربي رقم 95/46/EC، بأنها: "أي عملية أو مجموعة من العمليات تُجرى على البيانات الشخصية، سواء كانت بوسائل آلية أم لم تكن؛ مثل الجمع والتسجيل والتنظيم، والتخزين، والتكيّف أو التغيير، والاسترجاع، والتشاور، والاستخدام، والكشف عنها بإرسالها أو نشرها أو إتاحتها، والمحاذاة أو الدمج، والحجب أو المحو أو التدمير[34]. وعاد المشرع الأوروبي ليطور من مفهوم المعالجة بموجب اللائحة العامة لحماية البيانات الشخصية(GDPR)، فعرّفها بأنها: "أي عملية أو مجموعة من العمليات تُجرى،

[32]– د. منى الأشقر جبور؛ د. محمود جبور، مرجع سابق، ص90.

[33]–نص المادة (2/ج)، باللغة الإنكليزية:

Article 2. c. "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical

Operations on those data, their alteration, erasure, retrieval or dissemination.

[34]–نص المادة (2/ب)، باللغة الإنكليزية:

Article 2. b. "processing of personal data" ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction .

على بيانات شخصية أو على مجموعات من البيانات الشخصية، سواء كانت بالوسائل الآلية أم لم تكن؛ مثل الجمع والتسجيل والتنظيم والهيكلة، والتخزين، والتعديل أو التغيير، والاسترجاع، والمداولة، والاستخدام، والكشف عنها بإرسالها أو نشرها أو اتاحتها، والمحاذة أو الدمج، والتقييد، والمحو أو التدمير"[35]. فالمشرع في الإرشاد الأوروبي ومن ثم في اللائحة الأوروبية وسّع مفهوم المعالجة ليشمل إضافة للمعالجة التي تجرى كليًا أو جزئيًا بالوسائل الآلية، المعالجة اليدوية البحتة، وليغطي مجموعة أكبر من العمليات المادية والإلكترونية، التي تطال البيانات الشخصية، وقد أكّد أنّها ذُكرت على سبيل المثال لا الحصر. ويهدف هذا التوسع إلى توفير حماية قانونية فاعلة، عن طريق الإحاطة بمختلف عمليات معالجة البيانات.

ب–إدراج قائمة مبادئ لحماية البيانات الشخصية: تمثل المبادئ القانونية التي أقرّتها تشريعات حماية البيانات الشخصية، الحد الأدنى من المعايير والأساس الواجب توافرها في أي إطار قانوني يسعى إلى حماية الخصوصية والحريات الفردية[36]. وإذا كان المصدر الأساسي لهذه المبادئ هو المعايير الدولية، ولا سيما إرشاد منظمة التعاون الاقتصادي والتنمية واتفاقية مجلس أوروبا[37]، إلا أن الأحكام الخاصة بهذه المبادئ تداخلت واختلف تنظيمها بين تشريع وآخر، ويمكن تفسير هذا الأمر، بناءً على فلسفة القانون وأهدافه[38]، كما اختلفت القوانين لناحية إقرار مبدأ عام أو إعطاء تفصيل لمبدأ

[35]– نص المادة (2/4)، باللغة الإنكليزية:
Article 4. 2. "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction .

[36]– دليل منظمة التعاون الاقتصادي والتنمية، المادة (6).

[37]– تقرير بعنوان: دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الأوروبي، إكسس ناو، 2018، ص5، منشور على الموقع الآتي:
https://www.accessnow.org/cms/assets/uploads/2019/01/Updated-version-BOOKlet.pdf،
الدخول إلى الموقع بتاريخ 2020/9/23، الساعة 8 مساء.

[38]– د. منى الأشقر جبور؛ د. محمود جبور، مرجع سابق، ص121.

دون آخر، وربما يعود ذلك إلى تطور مفهوم الحماية ومسايرة القوانين لمستجدات التطور التكنولوجي. ومن أهم المبادئ التي وردت في القوانين الأوروبية، وتوصيات الجهات الدولية؛ مبدأ مشروعية ونزاهة وشفافية المعالجة: أي أن يكون الحصول على البيانات بوسائل مشروعة، وفق أساس قانوني واضح ومن أجل غاية مشروعة، حتى يتمكن المستخدمون من التعرف بشكل كافٍ عن كيفية جمع واستخدام وتخزين البيانات الخاصة بهم، وعن الجهة التي تقوم بذلك[39]؛ ومبدأ تحديد الغاية: أي أن تكون الغاية من جمع البيانات محددة ومشروعة ومعلنة، وأن تكون البيانات الشخصية التي جُمعت ذات صلة بالغاية المستهدفة، وأن البيانات التي جُمعت أو عولجت لغاية معينة لا تستخدم لغاية أخرى لا تتفق مع الغايات المحددة[40]؛ ومبدأ تحديد الجمع (مبدأ تقليص البيانات): أي يجب أن تقتصر البيانات الشخصية التي تُجمع أو تُستخدم على ما هو ضروري للغاية المحددة والمعينة، كما يجب أن تكون البيانات الشخصية كافية وذات صلة ومناسبة لهذه الغاية[41]؛ ومبدأ صحة البيانات: أي أن يلتزم المسؤولون عن حفظ البيانات بالتحقق من دقتها، والعمل على استكمالها وتصحيحها وتحديثها[42]؛ ومبدأ قيود التخزين: أي الاحتفاظ بالبيانات بصورة تسمح بتحديد أصحابها وألا تتجاوز مدة الاحتفاظ بالبيانات الشخصية المدة المحددة التي تتيح بلوغ الغاية المحددة من المعالجة[43]؛ ومبدأ الأمن والسرية: أي

[39]– اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (5/أ)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، المادة (أ/1)؛ الإرشاد الأوروبي رقم EC46/5/، المادة (1/6/أ)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (1/5/أ).

[40]– دليل منظمة التعاون الاقتصادي والتنمية، المادة (9و 10)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (5/ب)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، (أ/3)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (1/6/ب)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (1/5/ب).

[41]–دليل منظمة التعاون الاقتصادي والتنمية، المادة (7)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (5/ج)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (1/6/ج)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (1/5/ج).

[42]– دليل منظمة التعاون الاقتصادي والتنمية، المادة (8)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (5/د)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، (أ/2)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (1/6/د)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (1/5/د).

[43]– اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (5/هـ)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (1/6/هـ)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (1/5/هـ).

ينبغي اتخاذ التدابير التقنية أو التنظيمية الملائمة في معالجة البيانات الشخصية لحمايتها ضد المخاطر الطبيعية، مثل فقدها أو تلفها أو تضررها عرضيًا، أو ضد المخاطر البشرية مثل المعالجة غير المصرح بها أو غير المشروعة، والاطلاع عليها بغير إذن[44]؛ ومبدأ مشاركة الأفراد: أي تمكين أي شخص أن يعرف ما إذا كانت تجري معالجة آلية لبيانات تتعلق به، وأن يلبي طلبه بإجراء عمليات التصويب أو المحو في حالة البيانات التي تفتقر إلى المشروعية أو اللزوم أو الدقة[45]؛ ومبدأ حرية نقل وتدفق البيانات عبر الحدود: أي إنشاء آليات مناسبة لنقل البيانات تمكّن من التدفق الحر للبيانات بين الدول، بنفس الحرية التي تنتقل بها داخل حدود الدولة، وتجنّب وضع سياسات وممارسات باسم حماية الخصوصية والحريات الفردية، تتجاوز متطلبات هذه الحماية، وتخلق عقبات أمام تدفق البيانات الشخصية عبر الحدود[46]؛ ومبدأ التلاؤم: أي وجود ضمانات فعّالة تحافظ على حماية البيانات الشخصية فلا يجوز نقلها إلى دولة لا تضمن حماية مكافئة لها[47]؛ ومبدأ المساءلة: أي مسؤولية الأشخاص والجهات المرخص لهم الوصول والاطلاع على البيانات، عن تطبيق هذه المبادئ وضمان تنفيذها، ومعاقبتها في حال تجاوز أي من الإجراءات التي تكفل حماية البيانات الشخصية[48].

---

[44]–دليل منظمة التعاون الاقتصادي والتنمية، المادة (11)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (7)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، المادة (أ/7)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (11)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (5/1/و).

[45]–دليل منظمة التعاون الاقتصادي والتنمية، المادة (13)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (8)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990 المادة (أ/4)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (12)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (15و 22).

[46]–دليل منظمة التعاون الاقتصادي والتنمية، انظر المادتين (16و 18)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (2/12)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، المادة (أ/9)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (2/1)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR رقم 679، المادة (3/1).

[47]–دليل منظمة التعاون الاقتصادي والتنمية، المادة (17)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (3/12)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (25)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR رقم 679، المادة (44 وما بعدها).

[48]–دليل منظمة التعاون الاقتصادي والتنمية، المادة (14)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، (أ/8)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (2/6)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (2/5).

ج– إدراج قائمة بحقوق أصحاب البيانات: نصت قوانين الحماية على مجموعة من الأحكام تكرّس حقوق أصحاب البيانات، وتمكّنهم من حماية بياناتهم والتحكّم بها وإدارتها، وقد عززت اللائحة الأوروبية الحقوق التي أُقرتها التشريعات السابقة لها، كما أقرت عددًا من الحقوق الجديدة للأفراد. وأهم الحقوق الواردة في قوانين الحماية؛ الحق في النفاذ إلى البيانات: يضمن هذا الحق لأصحاب البيانات الحصول على تأكيد حول جمع بياناتهم الشخصية وهل هي في طور المعالجة، وإذا كان هذا هو الحال يجب تمكينهم من النفاذ إلى البيانات المعالجة، والتعرف على الغرض من المعالجة ومدة التخزين والكيانات التي تعالج بياناتهم الشخصية وتفاصيل الاتصال بهم في حال وجود أي إشكال[49]؛ والحق في التصحيح: يسمح هذا الحق لكل فرد أن يطلب تصحيح بياناته الشخصية، أو استكمالها، أو حجبها، أو تحديثها، متى كانت هذه البيانات غير صحيحة أو غير كاملة أو غير مناسبة[50]؛ والحق في المحو والحق في النسيان: يتيح هذا الحق السماح لكل فرد في ظروف معينة بطلب محو بيانات متعلقة بهم، ويطبق الحق في المحو من خلال طلب الأشخاص مسح بياناتهم من المواقع الواردة فيها، أو عند مغادرة الخدمة أو التطبيق، (الحق في محو البيانات)[51]، أما الحق في النسيان فيطبق من خلال الطلب من محركات البحث بإلغاء عناوين المواقع الإلكترونية عند البحث باستخدام أسمائهم (الحق في النسيان أو الحق في الحذف من قوائم البحث)[52]؛ والحق في تقييد المعالجة: يسمح هذا الحق للفرد طلب تقييد معالجة بياناته الشخصية، إذا اعترض على دقة البيانات أو على المعالجة غير القانونية أو تلك التي لم تعد ضرورية[53]؛ والحق في نقل البيانات: يتيح هذا الحق للشخص المعني الوصول إلى بياناته الشخصية التي قدمها إلى المعالج، ونقل هذه البيانات إلى وحدة معالجة أخرى دون عائق من المعالج الذي قدّم إليه بياناته الشخصية[54]؛ والحق في الاعتراض على معالجة البيانات: يمكّن هذا الحق

[49]–دليل منظمة التعاون الاقتصادي والتنمية، المادة (13)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (8)؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990 المادة (أ/4)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (12/أ)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (15).

[50]–الإرشاد الأوروبي رقم EC46/95/، المادة (12/ب)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (16).

[51]–الإرشاد الأوروبي رقم EC46/95/، المادة (12/ب)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (1/17).

[52]–اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (2/17).

[53]–اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (18).

[54]–اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (20).

صاحب البيانات، الاعتراض على معالجة بياناته الشخصية، ما لم يثبت المسؤول أسباب مشروعة للمعالجة تتجاوز مصالح وحقوق وحريات صاحب البيانات[55].

د- تحديد الأساس القانوني الذي يسمح بمعالجة البيانات: لتكون معالجة البيانات الشخصية مشروعة حددت قوانين حماية البيانات الأُسس القانونية التي يجب أن يستند عليها أي كيان عام أو خاص يعالج بيانات شخصية وهي؛ إما موافقة الشخص صاحب البيانات على معالجة بياناته لغاية محددة وبصورة مسبقة؛ أو عندما تكون المعالجة ضرورية لأداء عقد يكون صاحب البيانات طرفًا فيه؛ أو عندما تكون المعالجة ضرورية للامتثال لالتزام قانوني؛ أو لأنّها ضرورية لحماية مصالح حيوية لصاحب البيانات أو لشخص طبيعي آخر؛ أو لأنّها ضرورية لأداء مهمة يتم تنفيذها للمصلحة العامة؛ أو لأنّها ضرورية لمصلحة مشروعة للمراقب أو للطرف الثالث[56].

هـ- تحديد نطاق موضوعي واضح للتطبيق: القاعدة أن الحقوق والمبادئ المنصوص في قوانين حماية البيانات تطبق على معالجة البيانات الشخصية لدى جميع الكيانات العامة أو الخاصة، سواء اقتصرت على المعالجة التي تجري كليًا أو جزئيًا بطريقة آلية، كما جاء في اتفاقية مجلس أوروبا[57]، أو شملت إضافة لذلك المعالجة التي تنفذ بطريقة يدوية إذا كانت البيانات الشخصية تشكل جزءًا من نظام حفظ الملفات أو تهدف إلى تشكيل جزء من نظام حفظ الملفات[58]. وفي المقابل، تُجمع هذه القوانين على عدد من الاستثناءات لا بد منها، لتحقيق التوازن المطلوب بين حق الفرد في حماية حقوقه وحرياته الأساسية من جهة أولى، وبين حق المجتمع في التمتع بالرفاه والأمن

[55]-اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (21و 22).

[56]-الإرشاد الأوروبي رقم EC46/95/، المادة (7)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (6).

[57]-اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (1/3): "تلتزم الأطراف بتطبيق هذه الاتفاقية على الملفات والمعالجة الآلية للبيانات الشخصية في القطاعين العام والخاص".

[58]-دليل منظمة التعاون الاقتصادي والتنمية، المادة (2): "تنطبق هذه الإرشادات على البيانات الشخصية ، سواء في القطاعين العام أو الخاص، والتي تشكل خطرًا على الخصوصية وحريات الأفراد بسبب طريقة معالجتها، أو بسبب طبيعتها أو السياق الذي تُستخدم فيه" والمادة (3/ج): "لا يجب تفسير هذه الإرشادات على أنها تمنع: ج-تطبيق المبادئ التوجيهية فقط للمعالجة الآلية للبيانات الشخصية"؛ قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990، المادة (أ/10) ينبغي أن تطبق هذه المبادئ في المقام الأول علي جميع الملفات العامة والخاصة المعالجة آليا، بما في ذلك، شريطة إجراء التكييف الملائم، الملفات التي تعالج يدويًا..."؛ الإرشاد الأوروبي رقم EC46/95/، المادة (3): "ينطبق هذا الإرشاد على معالجة البيانات الشخصية كليًا أو جزئيًا بوسائل آلية، وعلى المعالجة بخلاف الوسائل الآلية للبيانات الشخصية التي تشكل جزءًا من نظام حفظ الملفات أو تهدف إلى تشكيل جزء من نظام حفظ الملفات"؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR رقم 679، المادة (1/2): "تنطبق هذه اللائحة على معالجة البيانات الشخصية كليًا أو جزئيًا بوسائل آلية وعلى المعالجة بخلاف الوسائل الآلية للبيانات الشخصية التي تشكل جزءًا من نظام حفظ الملفات أو تهدف إلى تشكيل جزء من نظام حفظ الملفات".

والاستقرار، وممارسة الدولة لواجباتها في هذه المجالات من جهة ثانية. وتتعلق هذه الاستثناءات بالبيانات والمعلومات الشخصية التي تجمعها وتعالجها الدولة في إطار نشاطها المعتاد، كسلطة عامة مسؤولة عن ضمان الأمن والسلم الوطنيين، لأغراض التحقيق في الجرائم أو اكتشافها أو مقاضاة مرتكبيها أو تنفيذ العقوبات الجنائية، وفي إطار الحفاظ على أمن الدولة بما فيها الأمن الاقتصادي، وضرورات الدفاع الوطني[59].

و– إنشاء آليات ملزمة وشفافة لنقل البيانات بشكل آمن إلى بلدان ثالثة: يُشكّل انتقال البيانات خارج الحدود الوطنية، البعد العالمي لعملية معالجة البيانات. ويعدّ هذا الانتقال إخراجًا لها من نطاق تطبيق القوانين المحلية وصلاحية السلطات الوطنية. لذلك كان من البديهي، أن يعطى هذا البعد اهتمامًا أساسيًا في قوانين حماية البيانات[60].

ي– إنشاء سلطة مستقلة وآليات قوية للإنفاذ: من المؤشرات على وجود إطار قانوني مناسب لحماية البيانات الشخصية، وجود سلطة إشرافية مستقلة لإنفاذ القانون وإجراء التحقيقات ومعاقبة الكيانات في حالة حدوث انتهاكات، بالإضافة لدورها في مساعدة الأشخاص المعنيين وتوجيههم، في كيفية ممارسة حقوقهم ومساعدة الشركات والسلطات العامة والمنظمات غير الحكومية في فهم واجباتها والتزاماتها في تنفيذ القانون[61].

الفرع الثاني: التشريعات الداخلية لحماية البيانات الشخصية

حرصت الدول، مع اختلاف أنظمتها القانونية والاجتماعية والاقتصادية، على الاعتراف بالحق في الخصوصية لكل مواطنيها وذلك بالنص في الدساتير على كفالة

[59]–دليل منظمة التعاون الاقتصادي والتنمية، المادة (4)؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، المادة (2/9/أ)؛ قرار الجمعية العامة للأمم المتحدة، المادة (6/أ)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (2) و (13)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR، المادة (2/3/د) والمادة (23).

[60]–دليل منظمة التعاون الاقتصادي والتنمية، الجزء الثالث، المبادئ الأساسية للتطبيق الدولي، التدفق الحر والقيود الشرعية، المواد من 15 إلى 18؛ اتفاقية مجلس أوروبا لحماية الأفراد من المعالجة الآلية للبيانات الشخصية رقم 108، الفصل الثالث، تدفقات البيانات عبر الحدود، المادة (12)؛ قرار الجمعية العامة للأمم المتحدة، المادة (أ/9)؛ الإرشاد الأوروبي رقم EC46/95/، المادة (25)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR رقم 679، المادة (44).

[61]-الإرشاد الأوروبي رقم EC46/95/، المادة (28)؛ اللائحة العامة الأوروبية بشأن حماية البيانات GDPR رقم 679، المواد (51 إلى 58).

هذه الحماية[62]. وتبع ذلك تدخل المشرع لحماية تطبيقات معينة تتصل بتكريس هذا الحق وصونه وردع الاعتداءات التي تطاله، ومن الطبيعي أن تكون الحماية متلائمة مع الاعتراف بهذا الحق ومشتملاته من جهة، ومع المستجدات والمخاطر التي تهدده من جهة أخرى. فالحق في الخصوصية يحمي الشخص من كافة أوجه الاعتداءات والتدخل في حياته أيًا كانت طبيعتها ويشمل؛ الحق في الخصوصية المادية الذي يعطي الشخص الحق في حماية جسده ومسكنه ومراسلاته ووثائقه وكل ما يتعلق به من الناحية المادية من أي إجراءات ماسة بجسده؛ والحق في الخصوصية المعنوية الذي يعطي الشخص الحق في حماية أسراره من أنشطه الرقابة والتجسس والتنصت؛ أما المفهوم الجديد فهو الحق في خصوصية المعلومات الذي يعطي الشخص الحق في حماية بياناته الشخصية والسيطرة عليها، وقد ارتبط هذا المفهوم الجديد بأثر التقنية وتحديات العصر الرقمي على الخصوصية[63]. فالحق في الخصوصية، بوصفه الحق الذي يحمى حياة الفرد الخاصة من كل اعتداء أو تطاول أو انتهاك أو تدخل، ينطوي على حماية جميع هذه المظاهر دون أن ينتقص ذلك من كونه حقًا موحدًا مستقلًا[64].

وفي سورية حظيت الخصوصية بحماية دستورية وقانونية؛ فقد اعترف المشرع السوري بحق الأفراد في حماية حياتهم الخاصة، من خلال منح الصفة الدستورية للحق في الخصوصية كحق عام[65]، وتجريم كل فعل من شأنه المساس بسلامته، وأضحى انتهاك الحياة الخاصة من قبل الأفراد أو الدولة جريمة مخالفة لأحكام الدستور[66]، كما أفرد الدستور عدداً من المواد لحماية بعض مظاهر الحياة الخاصة، فنص على حرمة

[62]–عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت–لبنان،2003، ص283.

[63]–د. بولين أنطونيوس أيوب، مرجع سابق، ص43.

[64]–د. منى تركي الموسوي؛ جان سيريل فضل الله، مرجع سابق، 2013م، ص20.

[65]–نص المادة (1/36) من الدستور السوري الصادر بتاريخ 27شباط لعام 2012، على أنه: "للحياة الخاصة حرمة يحميها القانون".

[66]–نص المادة 54 من الدستور السوري على أن: "كل اعتداء على الحرية الشخصية أو على حرمة الحياة الخاصة أو على غيرها من الحقوق والحريات العامة التي يكفلها الدستور يعد جريمة يعاقب عليها القانون".

المساكن[67]، وعلى سرية المراسلات والاتصالات[68]، وعلى حرية الاعتقاد[69]، وأكد على حماية الحرية الشخصية وكرامة وأمن المواطنين[70]. ولكن يؤخذ على الدستور السوري الذي صدر في العقد الثاني من القرن الحادي والعشرين، أنه لم يتضمن صراحة نص صريح يعترف بحق الأفراد في حماية بياناتهم الشخصية من مخاطر تقنية المعلومات وأنشطة معالجة البيانات. كدساتير الدول الأوروبية التي نصت منذ تسعينيات القرن العشرين بصراحة على هذه الحماية[71]، والدساتير الحديثة التي تورد نص صريح بهذا الشأن[72]؛ كما اعترف المشرع السوري بحق الأفراد في حماية حياتهم الخاصة، بموجب القوانين، فنصّ في القانون المدني[73]، على طائفة من الحقوق الملازمة لشخصية الإنسان، ووضع ضمانات عدة لحمايتها، فأقرّ إمكانية طلب وقف الاعتداء دون حاجة لإثبات الضرر[74]، والحق في الخصوصية يدخل في نطاق هذه الحقوق التي ترتبط بكيان الشخص وآدميته[75]. كما نصّ في قانون العقوبات[76]، على حق الأفراد في حماية بعض مظاهر الخصوصية فجرّم خرق حرمة المنزل[77]، والاطلاع أو إتلاف أو اختلاس الرسائل أو البرقيات البريدية، أو إفشاء مضمونها إلى غير المرسل إليه أو أفشاء مخابرة

---

[67]–نص المادة (2/36): "المساكن مصونه لا يجوز دخولها أو تفتيشها إلا بأمر من الجهة القضائية المختصة وفي الأحوال المبينة في القانون".

[68]–تنص المادة (37):"سرية المراسلات البريدية والاتصالات السلكية واللاسلكية وغيرها مكفولة وفق القانون".

[69]–نص المادة (1/42): "حرية الاعتقاد مصونة وفقًا للقانون".

[70]–نص المادة (1/33): "الحرية حق مقدس وتكفل الدولة للمواطنين حريتهم الشخصية وتحافظ على كرامتهم وأمنهم".

[71]–د. بولين أنطونيوس أيوب، مرجع سابق، ص395.

[72]–دستور الجمهورية التونسية الصادر بتاريخ 27 كانون الثاني لعام 2014، الفصل (24): " تحمي الدولة الحياة الخاصة، وحرمة المسكن، وسرية المراسلات والاتصالات والمعطيات الشخصية".

[73]–الصادر بالمرسوم التشريعي رقم /84/ بتاريخ 18 أيار 1949.

[74]-المادة (52): "لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر".

[75]–د. محمد واصل: الحقوق الملازمة للشخصية، دراس مقارنة، دمشق، الطبعة الأولى، 1995، ص251.

[76]–قانون العقوبات الصادر بالمرسوم التشريعي رقم 148لعام 1949.

[77]–المادة (557): "1–من دخل منزل أو مسكن آخر أو ملحقات مسكنه أو منزل خلافًا لإرادته، وكذلك من مكث في الأماكن المذكورة خلافًا لإرادته خلافًا لإرادة من له الحق في إقصائه عنها، عوقب بالحبس مدة لا تتجاوز الستة أشهر". والمادة (558) على: "يعاقب بالحبس التكديري أو بغرامة لا تتجاوز ألفي ليرة من تسلل بواسطة الكسر أو العنف على الأشخاص إلى أماكن تخص الغير وليست مباحة للجمهور أو مكث فيها على الرغم من إرادة من له الحق في إقصائه عنها".

هاتفية[78]، وإفشاء الأسرار المؤتمنة لدى بعض الأشخاص[79]. وقد اكتفى المشرع بهذه النصوص، التي كانت كافية لحماية الخصوصية قبل التطور التكنولوجي الذي صاحب نهايات القرن العشرين. كما شهدت السنوات الأخيرة استجابة تشريعية على مستويات مختلفة لدواعي هذه الحماية، من خلال النص على حماية الخصوصية في عدد من القوانين التي استحدثها المشرّع السوري تماشيًا مع التطور التكنولوجي، تأكيدًا على الأهمية القصوى لخصوصية الأفراد على كيان الفرد والمجتمع معًا، واستجابة لدستورية هذا الحق ومشروعيته، فأكّد قانون الاتصالات[80] على خصوصية الاتصالات بين المستخدمين[81]، وأكّد قانون الإعلام[82] على أن احترام خصوصية الأفراد وكرامتهم وحقوقهم والامتناع عن انتهاكها بأي شكل من الأشكال من مبادئ العمل الإعلامي[83]، وحظر على الإعلامي التعرض للحياة الخاصة بأي شكل[84]. كما حظر المشرع في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية[85]، نشر معلومات على الشبكة تنتهك الخصوصية[86].

[78]–المادة (566): "1–يعاقب بالحبس من شهرين إلى سنتين كل شخص ملحق بمصلحة البريد والبرق يسيء استعمال صفته هذه بأن يطلع على رسالة مختومة، أو يتلف أو يختلس احدى الرسائل، أو يفضي بمضمونها إلى غير المرسل إليه. 2–وتنزل العقوبة نفسها بمن كان ملحقاً بمصلحة الهاتف وأفشى مخابرة هاتفية اطلع عليها بحكم وظيفته أو عمله". ونصت المادة (567) أن: "1–كل شخص آخر يتلف أو يفض قصداً رسالة أو برقية غير مرسلة إليه، أو يطّلع بالخدعة على مخابرة هاتفية، يعاقب بغرامة لا تتجاوز ألفي ليرة سورية. 2–ويقضي بالعقوبة نفسها على من اطّلع على رسالة أو على مخابرة برقية أو هاتفية في إذاعتها إلحاق ضرر بآخر، فأعلم بها غير من أرسلت إليه".

[79]–المادة (565): "من كان بحكم وضعه أو مهنته أو فنه على علم بسر وأفشاه دون سبب مشروع أو استعمله لمنفعته الخاصة أو لمنفعة آخر عوقب بالحبس سنة على الأكثر وبغرامة لا تتجاوز ألفي ليرة إذا كان الفعل من شأنه أن يسبب ضررًا ولو معنويًا".

[80]–الصادر بالقانون رقم /18/ بتاريخ 2010/6/1.

[81]–المادة (50/أ): أ–... للاتصالات بين المستخدمين صفة الخصوصية".

[82]–الصادر بالمرسوم التشريعي رقم /108/ لعام 2011.

[83]–نص المادة (4/4): "يقوم العمل الإعلامي على استخدام الوسائل الإعلامية لوضع المحتويات الإعلامية التي ليست لها صفة المراسلات الشخصية في متناول عامة الجمهور او فئة منه مع مراعاة المبادئ الاساسية الآتية:
4–احترام خصوصية الأفراد وكرامتهم وحقوقهم والامتناع عن انتهاكها بأي شكل من الأشكال".

[84]–نص المادة (13): "يحظر على الإعلامي أن يتعرض للحياة الخاصة للأفراد ولا يعد مساساً بالخصوصية الشخصية توجيه نقد أو نشر معلومات عن المكلفين بعمل أو خدمة عامة على أن يكون المحتوى الإعلامي وثيق الصلة بأعمالهم ومستهدفا المصلحة العامة".

[85]–قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، الصادر بالمرسوم التشريعي رقم /17/ تاريخ 2012/2/8.

[86]–نص المادة (23): يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة، كل من نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه، حتى ولو كانت تلك المعلومات صحيحة".

فالمشرع السوري كفل حماية دستورية وقانونية للخصوصية كحق عام، ونص على حماية بعض مظاهرها، لكنه لم يسنّ قانون خاص لحماية البيانات الشخصية، في حين بدأ توفير الأداة القانونية لحماية البيانات الشخصية في دول العالم على المستوى الداخلي، مطلع سبعينيات القرن الماضي، على أثر المؤتمر الأول للأمم المتحدة الخاص بحقوق الإنسان المنعقد في طهران عام 1968، الذي جاء تلبية للمتغيرات الغير مسبوقة التي أتاحها التقدم التكنولوجي، فنبه المؤتمر في الإعلان الذي أصدره[87]، من مخاطر التقدم التكنولوجي على الحقوق والحريات الأساسية، وكان محركًا أساسيًا حول تأثير التطور التكنولوجي على حقوق الإنسان وحرياته[88]. فظهر أول قانون وطني متكامل في السويد عام 1973، ثم في فرنسا عام 1978[89]، بينما تأخرت المنطقة العربية كثيراً في وضع قوانين لحماية البيانات الشخصية، فأوّل قانون عربي صدر في تونس عام 2004، ولاحقاً أصدرت دول عربية قوانين مماثلة، كالإمارات عام 2007، والمغرب عام 2009، وقطر عام 2016، ومصر عام 2020[90]. وأظهرت الدراسات الحديثة أن نحو 50 دولة من دول العالم أقرت تشريعات شاملة لحماية البيانات الشخصية في القطاعين العام والخاص، وأن عشرات الدول تبذل جهودًا تشريعية في هذه الفترة، لوضع قوانين في ذات الحقل، أو تعديل قواعدها القانونية القائمة لتحقق حماية البيانات[91].

ومن العوامل الرئيسة في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، أنه وقبل اختراع الكمبيوتر، كانت حماية بيانات الأشخاص بواسطة النصوص التقليدية التي تحمي الأسرار التقليدية والسرية المهنية، ولكن هذه النصوص أصبحت بعيدة

[87]–إعلان طهران، أصدره المؤتمر الدولي لحقوق الإنسان في طهران، رسميًا، في 13 أيار/مايو 1968.

[88]–إعلان طهران، الفقرة (18) من الإعلان: "أن الحديث عن المكتشفات العلمية وخطوات التقدم التكنولوجي، على رغم كونه قد فتح آفاقا واسعة للتقدم الاقتصادي والاجتماعي والثقافي، يمكن أن يعرض للخطر حقوق الأفراد وحرياتهم، وبالتالي سيكون من الضروري أن يجعل محل انتباه متواصل".

[89]–د. بولين أنطونيوس أيوب، مرجع سابق، ص309–310.

[90]–مقال بعنوان: الأمية الرقمية تجعل خصوصية العرب على الإنترنت وهمًا كبيرًا، منشور على الموقع الآتي: https://www.dw.com/ar/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9/s-9106%، الدخول إلى الموقع بتاريخ 2020/9/20 الساعة 10 مساءً.

[91]–د. بولين أنطونيوس أيوب، مرجع سابق، ص332.

عن توفير الحماية لبيانات الأشخاص من مخاطر جمع وتخزين البيانات والوصول إليها ونقلها في بيئة الوسائل التقنية، مما دفع الدول لوضع تشريعات ابتداءً منذ السبعينات، تتضمن قواعد مدنية وجنائية وإدارية[92]. وبمراجعة القوانين السورية نجد أن المشرّع السوري نصّ على حماية محدودة للمعلومات والبيانات سنتعرض لها فيما يأتي.

أولًا: تدابير المشرع السوري في حماية سرية البيانات الشخصية.

حمى المشرع السوري سرية البيانات الشخصية وذلك في قانون العقوبات، وقانون الأحوال المدنية[93]، وقانون السرية المصرفية[94]، ففي قانون العقوبات عاقب المشرّع على إفشاء الأسرار المؤتمنة التي تُعدّ جانبًا من جوانب الحياة الخاصة للأفراد، والتي نظمت أحكامها المادة (565)[95]، وفي مدى مطابقة السر للبيانات الشخصية ، فالسر قد يكون معلومة عن الحياة الخاصة، وقد يكون بيان شخصي يتصف بدرجة كبيرة من السرية[96]، ولكن المشرع يشترط أن يتصل هذا السر بوضع أو مهنة أو فن ما، أي يجب أن يكون نطاق العلم بالسر محصورًا بأشخاص يُفترض توافر عنصر الثقة بهم، بسبب مركزهم الاجتماعي أو العملي أو المهني بالنسبة لصاحب السر، أما إذا كان السر لا يتعلق بوضع أو مهنه أو فن الشخص المؤتمن عليه، أو إذا لم تكن المعلومات والبيانات سرية فتنتفي عنها الحماية.

وفي قانون الأحوال المدنية حمى المشرّع بيانات ومعلومات السجل المدني فأكّد على سريتها ومنع نقل السجلات المدنية الورقية والإلكترونية من أماكنها أو تقديمها للمحاكم أو اطلاع الأفراد عليها لأي سبب، باستثناء العاملين المختصين وفي حدود

---

[92]–د. منى تركي الموسوي؛ جان سيريل فضل الله، مرجع سابق، ص12.

[93]–الصادر بالمرسوم التشريعي رقم /26/ تاريخ 2007/4/12.

[94]–الصادر بالمرسوم التشريعي رقم /30/ تاريخ 2010/4/15.

[95]–المادة (565) من قانون العقوبات السوري: "من كان بحكم وضعه أو مهنته أو فنه على علم بسر وأفشاه دون سبب مشروع أو استعمله لمنفعته الخاصة أو لمنفعة آخر عوقب بالحبس سنة على الأكثر وبغرامة لا تتجاوز ألفي ليرة إذا كان الفعل من شأنه أن يسبب ضررًا ولو معنويًا".

[96]–د. أيمن عبد الله فكري، مرجع سابق، ص740.

صلاحياتهم[97]، وجاءت الحماية في مواجهة بعض أنواع المخاطر التي تتعرض لها وهي الدخول إلى معلومات السجل المدني المؤتمت بقصد تعديل بياناته[98].

وفي قانون السرية المصرفية الخاص بالمؤسسات المالية في سورية، حمى المشرع معلومات العملاء مثل هويتهم وحساباتهم وموجوداتهم ومعاملاتهم مع المؤسسات المالية فأقرّ بسريتها وحظر إفشاءها من قبل جميع الأشخاص[99]، وجاءت الحماية في مواجهة بعض المخاطر التي تتعرض لها وهي الإفشاء أو على الشروع به[100].

وعلى الرغم مما أنجزه المشرع السوري، من نصوص تهدف إلى حماية الأسرار وسرية البيانات الشخصية لدى بعض الأشخاص والكيانات، نجد أن هذه الحماية قاصرة عن حماية البيانات الشخصية فهي حماية جزئية ومحدودة؛ فحماية الأسرار في قانون العقوبات حماية جزئية لأنّها تحمي بيانات ومعلومات الأفراد السرية الموجودة لدى بعض الأشخاص، في حين أن حماية البيانات الشخصية تشمل في طياتها جميع البيانات المعلومات المتعلقة بالأفراد، سواء كانت سرية أم غير سرية، وبمواجهة كل من يقوم بمعالجة البيانات، كما أنها حماية محدودة فهي مقتصرة على الإفشاء وبالتالي قاصرة عن حماية البيانات الشخصية من مخاطر التقنية، التي حولت بيانات الأفراد والتي قد تكون بذاتها غير ضارة، إلى بيانات قد تشكل تهديدًا حقيقيًا لخصوصية الأفراد، بفعل

---

[97]–المادة (5/ج): " الحفاظ على سرية السجل المدني وما يتضمنه من بيانات ومعلومات وعدم جواز الاطلاع عليها إلا من قبل العاملين المختصين ضمن حدود صلاحياتهم". المادة (5/هـ): " لا يجوز نقل السجلات المدنية الورقية والإلكترونية من أماكنها أو تقديمها للمحاكم أو اطلاع الأفراد عليها لأي سبب. وإذا اقتضى الحال في دعاوى التزوير فحص هذه السجلات ومستنداتها فيجب أن يتم هذا الفحص في مكان السجلات بواسطة المحكمة أو القاضي المنتدب لهذا الغرض."

[98]–المادة (73/د): "يعاقب بالأشغال الشاقة من ثلاث إلى خمس سنوات كل من دخل وهو غير مخول بالدخول إلى معلومات السجل المدني المؤتمت بقصد تعديل بياناته (حذف، إضافة، تعديل) أو برامجه وتضاعف العقوبة إذا كان من قام بالفعل عاملاً بالوزارة سواء أكان مخولاً أم غير مخول بالدخول بقصد التزوير ويقدر ذلك من اللجان المختصة في الوزارة".

[99]–المادة (2): "أ–تعتبر معلومات سرية في معرض تطبيق هذا المرسوم التشريعي المعلومات التي تتعلق بهوية العملاء وحساباتهم وموجوداتهم ومعاملاتهم مع المؤسسات المالية... ب–لا يجوز لكل من اطلع على المعلومات المذكورة في الفقرة السابقة بحكم وظيفته أو صفته أو بما تسمح به القوانين والأنظمة النافذة إفشاؤها بما يخالف أحكام هذا المرسوم التشريعي".

[100]–المادة (9): "مع عدم الإخلال بأي عقوبة أشد، يعاقب بناء على شكوى المتضرر بالحبس من ثلاثة أشهر إلى سنة كل من أقدم على إفشاء المعلومات السرية المشار إليها في المادة الثانية بما يخالف أحكام هذا المرسوم التشريعي" ب–يعاقب على الشروع بذات العقوبة المنصوص عليها في الفقرة السابقة".

عمليات جمع البيانات المتفرقة ومعالجتها وتحويلها إلى بيان تفصيلي عن حياة الأفراد؛ كما أن حماية سرية البيانات الشخصية في قانوني الأحوال المدنية والسرية المصرفية؛ حماية جزئية مقتصرة على بيانات الأفراد المخزنة لدى هذه الكيانات، ولا تشمل البيانات الشخصية التي تجمعها وتخزنها الكيانات الأخرى العامة والخاصة، كما أنها حماية محدودة في مواجهة أنواع المخاطر التي تتعرض لها هذه البيانات والتي اقتصرت في قانون الأحوال المدنية على النقل والاطلاع غير المأذون به وتعديل البيانات بالحذف أو الإضافة أو التعديل، واقتصرت في قانون السرية المصرفية على الإفشاء أو الشروع به.

ثانيًا: تدابير المشرع السوري في حماية بيانات التجارة الإلكترونية.

حمى المشرع السوري البيانات والمعلومات في نطاق التعاملات الإلكترونية، بما فيها البيانات والمعلومات الخاصة بالأفراد، وذلك من خلال قانون التوقيع الإلكتروني وخدمات الشبكة[101]، وقانون الاتصالات، وقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، وقانون المعاملات الإلكترونية[102]. وفي هذا النطاق حمى المشرع في قانون التوقيع الإلكتروني وخدمات الشبكة، سرية بيانات التوقيع الإلكتروني وجميع المعلومات التي تقدم إلى مزود خدمات التصديق الإلكتروني[103]، بما في ذلك البيانات والمعلومات الخاصة بالأفراد التي يتعلق بها التوقيع الإلكتروني، وجاءت الحماية في مواجهة تزوير أو تحريف بيانات إنشاء التوقيع الإلكتروني[104]، أو الحصول بغير حق وبأي وسيلة كانت على بيانات إنشاء توقيع إلكتروني أو اختراقها أو اعتراضها أو تعطيلها عن أداء

[101]–الصادر بالقانون رقم /4/ تاريخ 2009/2/25.

[102]–الصادر بالقانون رقم /3/ بتاريخ 2014/3/4.

[103]-المادة (4/ب): تعد بيانات إنشاء التوقيع الإلكتروني والمعلومات التي تقدم إلى مزود خدمات التصديق الإلكتروني المرخص له بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله".

[104]–المادة (31/أ/2): "أ–يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة إلى مليوني ليرة سورية ككل من قام قصدًا بارتكاب أحد الأفعال التالية:2–تزوير أو تحريف توقيع الكتروني أو بيانات أو منظومة إنشاء توقيع الكتروني بأي طريق كان."

وظيفتها[105]، أو إفشاء العاملين لدى مزود خدمات التصديق الإلكتروني بيانات تتعلق بالتوقيع الإلكتروني أو التحقق من عائديته، أو استخدامها في غير الغرض الذي قدمت لأجله[106].

وفي قانون الاتصالات حمى المشرع سرية البيانات في قطاع الاتصالات، وجاءت الحماية في مواجهة مخاطر محددة وهي؛ إفشاء المعلومات أو استخدامها في غرض مختلف عن الغرض الذي قدمت من أجله أو العبث بها[107]؛ كما نصّ المشرّع بعبارات عامة ومبهمة على واجب المرخّص له باتخاذ الإجراءات الكفيلة بضمان سرية وخصوصية بيانات المشتركين[108]، ثم أحال تحديد شروط حماية خصوصية بيانات الحركة وبيانات الموقع إلى اللائحة التنفيذية لقانون الاتصالات، فشروط الحماية مقتصرة على فئات من البيانات الشخصية، وبالتالي لا يجوز مد الحماية المقررة لهذه الفئات إلى فئات أخرى[109].

كما حمى المشرع في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، سرية المعلومات لدى مقدمي الخدمات على الشبكة، فأضفى طابع السرية

105–المادة (31/أ/4): "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر نافذ: أ–يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة إلى مليوني ليرة سورية ككل من قام قصدًا بارتكاب أحد الأفعال التالية: 4–التوصل بأي وسيلة كانت إلى الحصول بغير حق على بيانات إنشاء توقيع الكتروني أو منظومة إنشاء توقيع الكتروني أو وثيقة الكترونية، أو اختراق أي منها، أو اعتراضها أو تعطيلها عن أداء وظيفتها."

106–المادة (31/أ/6): "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر نافذ: أ–يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة إلى مليوني ليرة سورية ككل من قام قصدًا بارتكاب أحد الأفعال التالية: 6–إفشاء أية بيانات تتعلق باستخدام التوقيع الإلكتروني أو التحقق من عائديته، أو استخدامها في غير الغرض الذي قدمت من أجله من قبل أحد العاملين لدى مزود خدمات التصديق الإلكتروني. ويكون المزود في هذه الحالة مسؤولًا بالتضامن عن الوفاء بما يحكم به العامل من غرامات إذا ثبت أن إخلال المسؤول عن الإرادة الفعلية للمزود بواجباته قد أسهم في وقوع الجريمة".

107–المادة (13): "يحظر على أي من أعضاء مجلس المفوضين أو المدير العام أو أي من موظفي الهيئة الإفصاح للغير عن المعلومات السرية التي تلقاها بصورة مباشر أو غير مباشرة عند القيام بمهام وظيفته أو بسببها. ويسري هذا الحظر بعد ترك المنصب أو الوظيفة"؛ والمادة (27/أ): "أ–يحظر على المرخص له، أو العاملين لديه، استخدام أي معلومات تخص مرخص له آخر لأي غرض غير الغرض الذي حصل عليها من أجله، أو إفشاؤها بأي طريقة كانت، دون الحصول على موافقة المرخص له صاحب تلك المعلومات"؛ والمادة (27/ب): "ب–يحظر على المرخص له، أو على العاملين لديه، العبث ببيانات أي مشترك، أو استخدامها لأي غرض آخر غير الغرض الذي حصل عليها من أجله، أو إفشاؤها بأي طريقة كانت، دون الحصول على موافقة المشترك".

108–المادة (50/ب): ب–يتخذ كل مرخص له جميع الإجراءات الكفيلة بضمان سرية وخصوصية بيانات المشتركين لديه".

109–المادة (50/ج): "تحدد اللائحة التنفيذية لهذا القانون شروط حماية خصوصية بيانات الحركة وخصوصية بيانات موقع المشترك".

علـى بيانـات الحركـة المحفوظـة[110] والمحتـوى[111]المخـزن لـديهم[112]، والمعلومـات[113] المتبادلة عن طريق مقدم خدمات النفاذ إلى الشبكة[114]، وجاءت هذه الحماية في مواجهة بعض أنواع التهديدات التي تختلف باختلاف الأشخاص والتي نستطيع تصنيفها إلى؛ تهديدات من جانب مقدّم الخدمات على الشبكة، وهي تغيير المحتوى المخزّن أو البيانات أو المعلومات المخزنة لديه بصورة غير مشروعة[115]، أو إفشاء المحتوى أو البيانات أو المعلومات المخزنة[116]؛ وتهديدات من الغير وهي نسخ البيانات أو المعلومات أو إلغائها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها[117]، واعتراض أو التقاط المعلومات المتداولة على منظومة معلوماتية أو الشبكة، أو التنصت عليها، والحصول على معلومات شخصية أو سرية باستخدام الخداع[118].

[110]–عرفت المادة (1) بيانات الحركة بأنها: "أي معلومات يجري تداولها في إطار التواصل على الشبكة تحدّد، بوجه خاص، مصدر الاتصال ووجهته ومساره والمواقع الإلكترونية التي يجري الدخول إليها ووقت الاتصال ومدته".

[111]–عرفت المادة (1) المحتوى بأنه: "المعلومات أو الخدمات التي يمكن الوصول اليها وتداولها في إطار التواصل على الشبكة".

[112]–المادة (2): "على مقدم الخدمات على الشبكة حفظ نسخة من المحتوى المخزن لديهم، في حال وجوده، وحفظ بيانات الحركة التي تسمح بالتحقق من هويه الأشخاص الذين يسهمون في وضع المحتوى على الشبكة، وذلك لمدة تحددها الهيئة. وتخضع هذه البيانات والمحتوى لسر المهنة...".

[113]–عرفت المادة (1)، المعلومات بأنها: "العلامات أو الاشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة التي تحمل معنى قابلا للإدراك مرتبطًا بسياق محدد".

[114]–المادة (3/آ): "يجوز لمقدم خدمات النفاذ إلى الشبكة تخزين المعلومات المتبادلة عن طريقة تخزينًا مؤقتًا، مباشرة أو عن طريق العهدة بذلك إلى الغير، شريطة أن يكون ذلك بغرض تحسين الخدمة، وألا يؤدي إلى انتهاك خصوصية المستخدمين أو بياناتهم الشخصية؛ وعليه ألا يقوم بأي تغيير على المحتوى المخزن لديه، وأن يتخذ جميع الإجراءات اللازمة لضمان عدم الوصول غير المشروع إلى هذا المحتوى المخزن، والعمل على إتلافه فور انتفاء الحاجة إليه...".

[115]–المادة (10): "يُعاقب مقدّم الخدمات على الشبكة، الذي يقوم بصورة غير مشروعة بتغيير المحتوى أو البيانات أو المعلومات المخزّنة لديه، بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سورية، مع حفظ حق المتضرّر بالمطالبة بالتعويض

[116]–المادة (9): "يعاقب مقدم الخدمات على شبكة الإنترنت، الذي يقوم بإفشاء المحتوى أو البيانات أو المعلومات المخزنة لديه، مخالفًا بذلك التزامات المحافظة على سر المهنة، وبالغرامة من مئتي ألف إلى مليون ليرة سورية، مع حفظ حق المتضرر بالمطالبة بالتعويض".

[117]–المادة (15): "آ–يعاقب بالغرامة من عشرين ألف إلى مئة ألف ليرة سورية، كل من دخل قصدًا، بطريقة غير مشروعة، إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الإنترنت، دون أن يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك. ب–وتكون العقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها، أو إلغائها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها".

[118]–المادة (18): "آ–يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من اعترض أو التقط قصدًا، بوجه غير مشروع، المعلومات المتداولة على منظومة معلوماتية أو الشبكة، أو تنصت عليها. ب–يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من استخدم الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة، بمكن استغلالها لأغراض إجرامية".

كما ألزم المشرّع في قانون المعاملات الإلكتروني، أطراف النشاط الاقتصادي بالوسائل الإلكترونية، بحماية جميع المعلومات العائدة لباقي الأطراف[119]. فحماية البيانات في هذا القانون تقتصر على البيانات المتبادلة بوسائل إلكترونية، وفي أثناء القيام بنشاط اقتصادي فقط. كما أن الحماية المقررة جاءت في مواجهة بعض أنواع المخاطر التي تتعرض لها هذه البيانات وهي تصرف أطراف النشاط الاقتصادي بالمعلومات أو التعامل بها في حال إلحاق الضرر المادي أو المعنوي بأصحاب هذه المعلومات.

فتدابير المشرع السوري في حماية بيانات التجارة الإلكترونية، بما فيها البيانات والمعلومات الخاصة بالأفراد، حماية جزئية مقتصرة على البيانات والمعلومات الخاصة بالأفراد المخزنة لدى أفراد وكيانات محددة وعلى فئات من البيانات الشخصية، كما أنّها حماية محدودة لا تغطي مخاطر المعالجة التي تتعرض لها البيانات الشخصية.

وعلى الرغم مما أنجزه المشرع السوري، من نصوص تهدف إلى حماية البيانات الشخصية نجد أن مفهوم البيانات الشخصية في التشريعات السورية غير واضح وغير محدد، كما أن تدابير المشرّع في حماية السرية والبيانات الشخصية وبيانات التجارة الإلكترونية تقدم حماية جزئية ومحدودة للبيانات الشخصية، فمحل الحماية في النصوص السابقة هو البيانات والمعلومات الموجودة لدى أفراد أو كيانات محددة، أما محل حماية البيانات الشخصية في قوانين حماية البيانات هو أي معلومة متعلقة بشخص طبيعي، تخضع لأي عملية من عمليات المعالجة، بغض النظر عن ماهية أو مكان الكيان مستلم البيانات، كما أن الحماية في النصوص السابقة تهدف بالدرجة الأولى إلى الالتزام بواجب الحفاظ على السرية المفروض على بعض الأشخاص، أما حماية البيانات الشخصية فتهدف أولًا إلى احترام حق الأفراد في حماية خصوصيتهم وبياناتهم الشخصية، التي

[119]–المادة (23): "يلتزم أطراف النشاط الاقتصادي الذين يمارسون نشاطهم بالوسائل الإلكترونية، بحماية جميع المعلومات العائدة لباقي الأطراف، ولا يجوز لهم التصرف أو التعامل بما من شأنه أن يحمل ضررًا ماديًا أو معنويًا لأصحاب هذه المعلومات، إلا بموافقة صريح من أصحابها".

أصبحت محلًا لعمليات الجمع والمعالجة والتخزين في قواعد البيانات لدى مختلف الكيانات العامة والخاصة، وكذلك في قواعد البيانات المنتشرة عبر الإنترنت سواء في حالة جمعها أو معالجتها أو إساءة استغلالها، وما يرافق ذلك من مخاطر المراقبة والتجسس على الحياة الخاصة للأفراد، والاتجار غير المشروع بهذه البيانات كاستعمالها في الإعلانات التجارية وتطوير أعمال الشركات، كل ذلك بدون رضا ومعرفة أصحاب البيانات، وهو ما يشكل اعتداء صارخ على حقوق الأفراد وحرياتهم الأساسية. فهذه التدابير لا تتناسب مع التطور الذي شهده المجتمع السوري بدخوله عصر تكنولوجيا الاتصالات والمعلومات، والمخاطر التي أوجدها على أمن وسلامة البيانات الشخصية. لذلك يجب على المشرع السوري تحديث حماية الخصوصية وتعزيزها وتوسيعها لمواجهة المستجد، والاعتراف بحق الأفراد في حماية بياناتهم الشخصية بالنص عليه في الدستور، وضع تنظيم قانوني لحماية البيانات الشخصية مع الوضع في الاعتبار التنظيم الذي اتبعته اللائحة الأوروبية العامة كونها قننت تنظيمًا متكاملًا لحماية البيانات الشخصية.

الخاتمة:

تناول هذا البحث موضوع التشريعيات الدولية والأوروبية والداخلية لحماية البيانات الشخصية، فعرض في الفرع الأول التشريعات الدولية والأوروبية لحماية البيانات الشخصية، وفي الفرع الثاني التشريعات الداخلية لحماية البيانات الشخصية، وقد توصل البحث إلى النتيجتين الآتيتين:

1- إن التغيير الحاصل في الواقع التكنولوجي انعكس على واقع الحماية القانونية للخصوصية، فبدأ الاهتمام العالمي بحماية البيانات؛ مع تنامي القلق من مخاطر التقنية على الحقوق والحريات العامة وخصوصية الأفراد، بسبب الاستخدام غير المشروع للبيانات الشخصية؛ وتزايد القلق في ظل الثورة التكنولوجية الحديثة، ما دفع إلى صدور تشريعات دولية وإقليمية ووطنية لحماية

البيانات الشخصية، تؤمن حماية تتناسب وحجم التهديدات التي تتعرض لها البيانات الشخصية.

2- لم يُشر المشرع السوري إلى الحق في حماية البيانات الشخصية في الدستور، ولم يضع، حتى حينه، قانونًا خاصًا لحماية البيانات الشخصية، ولم يحدد ماهية البيانات الشخصية، واكتفى بالإشارة إلى حماية البيانات الشخصية بتعابير عامة في بعض النصوص. وقد جاءت الحماية جزئية من حيث نطاق البيانات المحمية، ومحدودة من حيث المخاطر التي تتعرض لها البيانات.

كما اقترح التوصيتين الآتيتين:

1- المبادرة إلى الاهتمام بحماية البيانات الشخصية في سورية وذلك؛ بالنص على هذا الحق في صلب الدستور؛ وصياغة تنظيم تشريعي يحدد ماهية تلك البيانات وكيفية التعامل معها؛ وإنشاء هيئة مختصة تعمل على مراقبة معالجة البيانات الآلية، وصياغة التعديلات التشريعية اللازمة، والتطوير المستمر لتشريعات حماية البيانات الشخصية بما يحقق مرونتها ومواكبتها للتطورات التكنولوجية المتسارعة، ونشر التوعية اللازمة لمستخدمي النظام المعلوماتي بمخاطر التعامل عبر شبكة الإنترنت.

2- تعزيز الوعي في المجتمع بأهمية البيانات الشخصية، وذلك من خلال؛ عقد الندوات والمؤتمرات بصفة دورية حول هذا الموضوع لمناقشة أبعاده وتأثيره على المجتمع؛ واستحداث مواقع متخصصة تقدم المعلومات التقنية والقانونية حول وسائل حماية الخصوصية والبيانات الشخصية لمستخدمي شبكة الإنترنت؛ واهتمام وسائل الإعلام المرئية والمسموعة والمقروءة بتنمية الوعي والإدراك بأهمية حماية البيانات الشخصية، وتمكين أفراد المجتمع من فهم حقيقة ما يجري، من ممارسات تطال بياناتهم الشخصية وتمس حقوقهم كونهم خط الدفاع الأول.

المراجع:

أولًا: الكتب.

1- د. أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية،2007.

2- د. بولين أنطونيوس أيوب: الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، 2009.

3- عفيفي كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت–لبنان، 2003.

4- د. محمد واصل: الحقوق الملازمة للشخصية، دراس مقارنة، دمشق، الطبعة الأولى، 1995.

5- د. منى الأشقر جبور؛ د. محمود جبور: البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربي، أبحاث ودراسات (5)، الطبعة الأولى، بيروت–لبنان، 2018.

6- د. نعيم مغبغب: مخاطر المعلوماتية والإنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، 1998.

ثانيًا: الأبحاث القانونية.

1- منى تركي الموسوي؛ جان سيريل فضل الله: الخصوصية المعلوماتية وأهميتها ومخاطر التقانات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، جامعة بغداد، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، 2013م، منشور على الموقع الآتي:
https://www.iasj.net/iasj/download/c457ac3d2aaf7fdd
التحميل والدخول إلى الموقع بتاريخ 2020/8/8 الساعة 11:30 صباحًا.

ثالثًا: المواقع الإلكترونية.

1– إسماعيل عزام، مقال بعنوان: الأمية الرقمية تجعل خصوصية العرب على الإنترنت وهماً كبيراً، منشور على الموقع الآتي:
https://www.dw.com/ar/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9/s-9106
الدخول إلى الموقع بتاريخ 2020/9/20 الساعة 10 مساءً.

2– دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الأوروبي، إكسس ناو، 2018، منشور على الموقع الآتي:
https://www.accessnow.org/cms/assets/uploads/2019/01/Updated-version-BOOKlet.pdf
الدخول إلى الموقع بتاريخ 2020،/9/23 الساعة 8 مساء.

3– مقال بعنوان كتاب البيانات الشخصية: الصراع على نفط القرن الحادي والعشرين، منشور على الموقع الآتي: https://www.politics-dz.com/
الدخول إلى الموقع بتاريخ 2020/9/25 الساعة 2 مساءً.