الجمهورية العربية السورية
جامعة دمشق
كلية الحقوق
قسم القانون الخاص

الحماية القانونية للبيانات الشخصية لمستخدمي شبكة الإنترنت

رسالة مقدمة لنيل درجة الماجستير في القانون الخاص

إعداد
نلمى نسيب الأشقر

إشراف الدكتور
جمال مذكور
المدرس في قسم القانون الخاص

(2022-2021)

فهرس المحتويات

الموضوع **رقم الصفحة**

قائمة المختصرات ..... أ

الملخص ..... ب

المقدمة 1

إشكالية البحث 4

أسئلة البحث 4

أهداف البحث 5

أهمية البحث 5

مسوغات البحث 6

مصطلحات البحث 6

صعوبات البحث 9

حدود البحث 9

الدراسات السابقة 9

منهج البحث 12
خطة البحث 12
الفصل الأول: البيانات الشخصية المفهوم وأهداف الحماية والتحديات التي تواجهها على شبكة الإنترنت ... 13
المبحث الأول: مفهوم البيانات الشخصية وأهداف حمايتها 14
المطلب الأول: مفهوم البيانات الشخصية 14
الفرع الأول: التمييز بين البيانات والمعلومات 15
أولاً: تعريف المعلومات والبيانات 16
ثانيًا: طبيعة العلاقة بين المعلومات والبيانات 21
الفرع الثاني: تعريف البيانات الشخصية ومعالجة البيانات الشخصية 22
أولًا: تعريف البيانات الشخصية 22
ثانيًا: تعريف معالجة البيانات الشخصية 31
المطلب الثاني: أهداف حماية البيانات الشخصية 40
الفرع الأول: ضمان تدفق البيانات الشخصية عبر الحدود 41
أولًا: مبدأ الحماية الكافية الذي يحكم تدفق البيانات الشخصية عبر الحدود 42
ثانيًا: الاستثناءات على مبدأ الحماية الكافية الذي يحكم تدفق البيانات الشخصية عبر الحدود..... 52

الفرع الثاني: حماية الحقوق والحريات وبصورة خاصة الحق في البيانات الشخصية 58

أولًا: التمييز بين الحق في البيانات الشخصية والحق في الخصوصية 59

ثانيًا: أهمية الاعتراف بالحق في البيانات الشخصية على أنّه حق مستقل 73

المبحث الثاني: التحديات التي تواجه البيانات الشخصية على شبكة الإنترنت 87

المطلب الأول: التحديات التي تفرضها طبيعة شبكة الإنترنت 89

الفرع الأول: دور الإنترنت في تسهيل انتاج البيانات الشخصية وجمعها 90

أولًا: تنتج شبكة الإنترنت أنواعًا جديدة من البيانات الشخصية 91

ثانيًا: تقدم الإنترنت وسائل جديدة لجمع البيانات الشخصية 93

الفرع الثاني: دور الإنترنت في تسهيل استخدام البيانات الشخصية في المراقبة والأعمال التجارية.....97

أولًا: استخدام البيانات الشخصية في المراقبة. 98

ثانيًا: استخدام البيانات الشخصية في الأعمال التجارية. 103

المطلب الثاني: التحديات المتعلقة بقصور نماذج الحماية وغياب الأطر التشريعية والتنظيمية الملائمة ...108

الفرع الأول: حماية البيانات الشخصية ضمن نطاق حماية الخصوصية 109

أولًا: الحماية القانونية للخصوصية في القانون السوري 110

ثانيًا: قصور الحماية القانونية للخصوصية عن حماية البيانات الشخصية 115

الفرع الثاني: حماية البيانات الشخصية ضمن نطاق حماية سرية البيانات والمعلومات 119

أولًا: حماية سرية البيانات والمعلومات الشخصية في القانون السوري 120

ثانيًا: قصور الحماية القانونية لسرية البيانات والمعلومات في حماية البيانات الشخصية 128

خلاصة الفصل الأول 130

الفصل الثاني: تطور حماية البيانات الشخصية في التشريعات الدولية والتنظيم القانوني لحمايتها 131

المبحث الأول: تطور الحماية القانونية للبيانات الشخصية في التشريعات الدولية 134

المطلب الأول: جهود المنظمات الدولية في حماية البيانات الشخصية 135

الفرع الأول: جهود منظمة التعاون الاقتصادي والتنمية في حماية البيانات الشخصية 135

الفرع الثاني: جهود مجلس أوروبا في حماية البيانات الشخصية 139

الفرع الثالث: جهود الأمم المتحدة في حماية البيانات الشخصية 145

المطلب الثاني: جهود الاتحاد الأوروبي في حماية البيانات الشخصية 149

الفرع الأول: توجيه الاتحاد الأوروبي رقم (EC/46/95) لعام (1995) 150

الفرع الثاني: لائحة الاتحاد الأوروبي لحماية البيانات (GDPR) رقم (679) لعام (2016) 153

المبحث الثاني: التنظيم القانوني لحماية البيانات الشخصية 157

المطلب الأول: مبادئ حماية البيانات الشخصية 159

الفرع الأول: المبادئ المتعلقة بمعالجة البيانات الشخصية ومشروعيتها 159

أولًا: المبادئ المتعلقة بمعالجة البيانات الشخصية 160

ثانيًا: المبادئ المتعلقة بمشروعية معالجة البيانات الشخصية 165

الفرع الثاني: الاستثناءات على مبادئ حماية البيانات الشخصية 175

أولًا: البيانات الشخصية المستثناة من قواعد الحماية 175

ثانيًا: البيانات الشخصية المستثناة من القاعدة العامة للمعالجة 178

المطلب الثاني: الحقوق والالتزامات في إطار حماية البيانات الشخصية 181

الفرع الأول: حق الشخص المعني في حماية بياناته الشخصية 181

أولًا: التعريف بالشخص المعني بالبيانات 182

ثانيًا: حقوق الشخص المعني بالبيانات بموجب الحق في حماية البيانات الشخصية 189

الفرع الثاني: التزامات القائمين على معالجة البيانات الشخصية 198

أولًا: التعريف بالمتحكّم والمعالج 198

ثانيًا: التزامات المتحكم والمعالج 202

خلاصة الفصل الثاني 213

الخاتمة 214

النتائج 215

المقترحات 218

قائمة المراجع 220

Abstract ..... a

الإهـــداء

إلى من غاب جسدًا ومازال في حنايا القلب حيًا. إلى روح أبي الحبيب أُهدي هذا البحث.

شـــكـر وتـقـدير

يسعدني، وقد وفقني الله في إنجاز هذا البحث، أن أتقدم بالشكر إلى الدكتور **جمال مذكور** لتفضله بالإشراف على هذا البحث، وعلى ما منحه لي من وقتٍ، وما قدّمه لي من توجيهات وإرشادات وملاحظات قيمة، ساهمت في إنجاز هذا البحث.

كما أتوجه بالشكر إلى الدكتور **مؤيد زيدان**، على تفضله ومشاركته في مناقشة هذا البحث وتقويمه، جزاه الله خير جزاء.

كما أتوجه بالشكر للدكتورة **أروى تقوى**، لتفضلها بالمشاركة في مناقشة هذا البحث وتقويمه، جزاها الله خير جزاء.

قائمة المختصرات

CJEU: Court of Justice of the European Union.

CoE: Council of Europe.

EC Treaty: Treaty establishing the European Community.

EU: European Union.

EUPB: European Data Protection Board.

GDPR: General Data Protection Regulation.

No: Number.

OECD: Organization for Economic Co-operation and Development.

P: Page.

TEU: Treaty on European Union.

TFEU: Treaty on the Functioning of the EU

Vol: Volume.

WP: The Article 29 Working Party.

"الملخص"

يناقش البحث الحماية القانونية للبيانات الشخصية لمستخدمي شبكة الإنترنت. إنّ البحث في هذا الموضوع أمر بالغ الأهمية، وبصورة خاصة بعد أن سهّلت شبكة الإنترنت انتاج البيانات الشخصية وجمعها، ووفرت قدرات جديدة لمعالجة البيانات الشخصية واستخدامها، فضاعفت بذلك التحديات التي تتعرض لها البياناتُ الشخصية، الأمر الذي جعل من وجود حماية قانونية للبيانات الشخصية ضرورة ملحة. ولذلك عالج البحث التحديات التي تواجه البيانات الشخصية على شبكة الإنترنت من جانبين؛ الأول يتعلق بالتحديات التي تفرضها طبيعة شبكة الإنترنت؛ والثاني يتعلق بالتحديات المتعلقة بقصور نماذج الحماية وغياب الأطر التشريعية والتنظيمية الملائمة. ومن خلال عرض ما سبق تبيّن أنّ القواعد القانونية الخاصة بحماية الخصوصية وحماية سرية المعلومات والبيانات في سورية، لا توفر حماية قانونية كافية ومناسبة للبيانات الشخصية لمستخدمي شبكة الإنترنت. ولتوضيح مدى أهمية وجود حماية خاصة بالبيانات الشخصية عرض البحث تطور الحماية القانونية للبيانات الشخصية في التشريعات الدولية والتنظيم القانوني لهذه الحماية.

الكلمات الرئيسية: البيانات الشخصية، معالجة البيانات، شبكة الإنترنت، الحق في حماية البيانات الشخصية.

المقدمة

تعدُّ شبكة الإنترنت أعظم تقنية ابتكرها الإنسان، فهي تقدم الكثير من الخدمات على جميع الأصعدة الاجتماعية والسياسية والاقتصادية والحكومية، وتخدم مختلف الأغراض العلمية والتجارية والترفيهية والأمنية، وبالتالي تلبي حاجات أفراد المجتمع والحكومات والشركات التجارية وتطلعاتهم على حد سواء، لذلك أصبحت الإنترنت في عصرنا هذا حاجة أساسية لا تقل أهميتها عن غيرها من الحاجات الأساسية الأخرى. إلا أنّه، وفي مقابل المنافع والآفاق الواسعة والفرص الجديدة التي تؤمنها شبكة الإنترنت لمستخدميها، نشأت عنها تحديات على حقوق الإنسان وحرياته أكثر من تلك الموجودة في العالم المادي، ومنها التحديات التي تتعرض لها البيانات الشخصية لمستخدمي الإنترنت، فالكم الهائل من البيانات المخزنة على المواقع الإلكترونية والبيانات المخزنة في مراكز جمع البيانات وتحليلها، بالإضافة إلى كل ما ينتجه مستخدمو شبكة الإنترنت من بيانات أو ما يضيفونه أو ما يرتبط بهم أو ما يُجمع عنهم، واستخدام هذه البيانات من قبل جهات مختلفة ولأغراض مختلفة، شكّل تهديدًا جديًا على حقوق الأفراد.

إنّ استخدام شبكة الإنترنت، غيّر كثيرًا من التهديدات التي تتعرض لها البيانات الشخصية فالكثير من سمات الإنترنت تظهر مدى صعوبة تحكّم مستخدم شبكة الإنترنت في بياناته الشخصية، فقد أدّت شبكة الإنترنت إلى تعاظم كمية البيانات الشخصية المُنتَجة والمُجمَّعة والمُعالجة، وخاصة بعد التوسع الهائل في استخدامها ودخول غالبية فئات المجتمع إلى قائمة المستخدمين. كما أتاحت طبيعة شبكة الإنترنت المفتوحة والعابرة للحدود بين الدول، الحصول على البيانات الشخصية عن بعد وبدون علم أو معرفة أصحابها، الأمر الذي جعل من الصعب، بل وفي بعض الأحيان من المستحيل، معرفة الدول أو الأشخاص الذين يحصلون على البيانات، وبات من السهل جمعها ومعالجتها من قبل مختلف الجهات العامة والخاصة، ولأهداف مختلفة سواء للتجسس على حياة الأفراد ومراقبتهم، أم لأغراض تجارية. كما أنّ سرعة الاتصالات عبر الإنترنت وانتشارها، بلغت درجة يمكن معها نشر البيانات أبعد بكثير من نطاق سيطرة الفرد، وذلك في أقل من ثانية. فضلاً عن ذلك هناك سوق قويّة على الإنترنت للبيانات الشخصية تتحكم فيها نماذج العمل القائمة على التسويق، ويقوم المستخدمون فيها بالسداد من خلال بياناتهم وليس

من خلال الأموال النقدية. وفي الوقت ذاته تتميز تكلفة تبادل هذه البيانات بأنّها منخفضة للغاية مما يؤدي إلى تبادل سجلات بيانات المستخدم الشخصية بأقل تكلفة تذكر.

ومع التطور التكنولوجي واستخدام الإنترنت في كافة أوجه حياة الأفراد، ازدادت عملية إنتاج المحتوى الرقمي، وارتبطت بها زيادة في إنتاج البيانات الشخصية، كما سمح التطور في المعالجة الحاسوبية، إلى زيادة القدرة على معالجة قدر أكبر من البيانات الشخصية، وباتت عمليات معالجة البيانات لاستخلاص معلومات ذات معنى ودلالة والاستفادة منها، تُستخدم في كافة المجالات. كل ذلك أضعف قدرة الأفراد على التحكم في البيانات والمعلومات المخزنة عنهم، وهدّد حقوق الأفراد وحرياتهم، ولا سيما الحق في حماية الخصوصية والحق في حماية البيانات الشخصية، وأصبح الفرد مقيدًا في تعاملاته بسبب خشيته من معالجة بياناته الشخصية التي تمثل جانبًا مهمًا من شخصيته، الأمر الذي أدى إلى تغيّر المفاهيم القانونية، ولم تعد الأشكال الأولى من الحماية القانونية للخصوصية وسرية المعلومات كافية وشاملة لحماية البيانات الشخصية وصون حقوق الأشخاص وحرياتهم الأساسية. ولذلك فإن مصادر الخطر على البيانات الشخصية لمستخدمي شبكة الإنترنت لا تتعلق بالتحديات التي تواجه البيانات الشخصية على شبكة الإنترنت التي تسهّل جمع أنواع مختلفة من المعلومات الشخصية، وتهيّئ قدرات جديدة للحكومة والقطاع الخاص بتحليل البيانات الشخصية واستخدامها فقط، وإنما ترجع أيضًا إلى قصور نماذج الحماية وغياب الأُطر التشريعية والتنظيمية الملائمة.

بدأ الاهتمام على المستوى الدولي بضرورة حماية البيانات الشخصية من مخاطر التكنولوجيا منذ ستينيّات القرن العشرين، وبدأت دول العالم في سنّ قوانين لحماية البيانات الشخصية في سبعينيّاته، وفي ثمانينيّاته ازداد الاهتمام بحماية البيانات الشخصية، فظهرت اتفاقات وإرشادات وتوجيهات غايتها الأساسية حماية البيانات الشخصية. وفي الوقت الحاضر أصبحت حماية البيانات ضرورة ملحّة بعد اكتساح التكنولوجيا الحديثة لمعظم الوسائل المستخدمة في الحياة اليومية، وما يمثله هذا الواقع من تهديد جدي للبيانات الشخصية، وما يتبعه من تهديد للحقوق والحريات المدنية وحقوق الشخصية.

ومع وعي إمكانات التكنولوجيا وطبيعة الإنترنت؛ وبالنظر للطابع الشخصي الذي تتميز به البيانات الشخصية للأفراد، كونها تعطي تفاصيل عن الشخص الطبيعي وحياته وميوله وتحركاته في الحياة المادية والافتراضية؛ وبفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء عليها؛ وبالنظر لعدم كفاية القواعد القانونية التي تحمي الخصوصية وسرية المعلومات من تأمين حماية كافية للبيانات الشخصية، استدعى ذلك بذل المزيد من الجهود لإيجاد تشريعات تهدف بصورة أساسية إلى حماية بيانات الأفراد الشخصية، فتطوّرت الحماية على المستوى الدولي، وكان لها دور أساسي في قيام الكثير من دول العالم بسن قوانين وطنية لحماية البيانات الشخصية، كما كان لها دور أساسي أيضًا في بلورة الحق في حماية البيانات الشخصية، على أنّه حق متميز ومستقل عن الحق في حماية الخصوصية في مجتمع المعلومات المعاصر.

وعلى الرغم من الاهتمام الكبير الذي تتلقاه حماية البيانات من المشرعين والأكاديميين والمحامين ونشطاء حقوق الإنسان والسياسيين والاقتصاديين، على المستويين الدولي والوطني، لا تزال سورية متأخرة في توفير حماية قانونية للبيانات الشخصية تلائم هذه المرحلة، فلم يتبنَ المشرع السوري حتى الآن تشريعًا خاصًا بحماية البيانات الشخصية، على خلاف الكثير من دول العالم. الأمر الذي أوجب مراجعة القوانين الحالية وتحليل المواد القانونية الرئيسية ذات الصلة بحماية البيانات الشخصية، وهي؛ المواد القانونية المتعلقة بحماية الخصوصية والسرية، التي أظهرت قصورها، فعلى الرغم من أن حماية الخصوصية هي في الواقع جزء كبير منها حماية لبيانات خاصة بالأفراد، إلا أنّ البيانات الشخصية لا تتعلق جميعها بالخصوصية، فالبيانات التي تتعلق بالنشاطات العامة للفرد تشكل بيانات شخصية، لكنها لا تدخل ضمن مفهوم الخصوصية، كما أن حماية البيانات الشخصية لا تحل محل حماية الأسرار، لكنها تكملها وتؤمن تفعيلها في وجه مخاطر الإنترنت؛ والمواد القانونية المتعلقة بحماية سرية البيانات والمعلومات، أظهرت قصورها أيضًا، فقد تبين أن الحماية مقتصرة على بعض أنواع البيانات الشخصية لدى جهات معينة، كما أن الحماية جاءت في مواجهة بعض المخاطر التي تتعرض لها، ولذلك يبيّن البحث أن الإطار القانوني الحالي في سورية غير ملائم لحماية الأفراد من المخاطر الناجمة عن التطور التكنولوجي ولا سيما شبكة الإنترنت تجاه بياناتهم الشخصية.

ومن أجل عرض الحماية القانونية للبيانات الشخصية لمستخدمي شبكة الإنترنت عرض البحث مفهوم البيانات الشخصية، وأهداف الحماية في إيجاد توازن بين حماية حقوق أصحاب البيانات الشخصية من جهة، والحاجة إلى جمع البيانات الشخصية ومعالجتها من جهة أخرى. كما عرض مبادئ حماية البيانات، والتي تتعلق بشروط ومشروعية المعالجة وحقوق الأفراد تمكنهم من السيطرة على بياناتهم الشخصية والتحكم فيها، وحددت التزامات على القائمين على عملية معالجة البيانات.

وأخيرًا لا بد من الإشارة إلى أنّه وعلى خلاف معظم الدراسات التي تناولت موضوع حماية البيانات الشخصية، فإنّ البحث ينظر إلى حماية البيانات الشخصية على أنّه حق مستقل عن الخصوصية، له أهداف وقواعد تميزه، كما أنه يتميّز بأنّ له قيمة نهائية هي حماية الحق في البيانات الشخصية، وله أيضًا قيمة وسيطة أو ثانوية في حماية حقوق الإنسان وحريات الأخرى ولا سيما الخصوصية.

إشكالية البحث

في ظل فراغ تشريعي من قانون خاص بحماية البيانات الشخصية، تتمحور الإشكالية الرئيسية لهذا البحث في **كيفية تحقيق حماية قانونية فعّالة للبيانات الشخصية في سورية، تتلاءم مع المخاطر التي فرضها التطور التكنولوجي ولا سيما شبكة الإنترنت.**

أسئلة البحث

تتفرع عن إشكالية البحث تساؤلات أخرى جديرة بالطرح وهي:

– ما المقصود بالبيانات الشخصية ومعالجة البيانات؟

–ما هي أهم التحديات التي تواجه البيانات الشخصية على شبكة الإنترنت؟

–هل الحماية الحالية المقررة للخصوصية والسرية والبيانات والمعلومات بموجب القوانين السورية كافية لحماية للبيانات الشخصية؟

– كيف تم تطوير حماية البيانات في الصكوك الدولية والإقليمية؟

–ما الهدف من حماية البيانات الشخصية؟

–ما مدى ارتباط حماية البيانات الشخصية بالخصوصية؟

–ما هي مبادئ حماية البيانات الشخصية؟

–ما هي الحقوق الممنوحة لأصحاب البيانات وما هي التزامات القائمين على معالجة البيانات بموجب قوانين حماية البيانات؟

أهداف البحث

عني هذا البحث بدراسة موضوع الحماية القانونية للبيانات الشخصية لمستخدمي شبكة الإنترنت وذلك لتحقيق الأهداف الآتية:

1. التعريف بمفهوم البيانات الشخصية، وعرض مصادر المخاطر التي تتعرض لها البيانات على شبكة الإنترنت لبيان سبل الحماية القانونية لها.

2. إبراز أهمية البيانات الشخصية والمصلحة والقيمة من حمايتها.

3. توضيح مدى قصور القواعد القانونية في سورية عن حماية البيانات الشخصية.

4. أهمية وجود تشريع خاص بحماية البيانات الشخصية.

5. لفت نظر المشرّع السوري والباحث القانوني السوري إلى أهمية هذا الموضوع.

أهمية البحث

تأتي أهمية هذا البحث كونه يسلط الضوء على الحماية القانونية للبيانات الشخصية، التي لها مكانة سامية كونها تعبّر عن شخصية الإنسان وتعطي صورة واضحة عن شخصيته، فالمساس بالبيانات الشخصية هو مساس

بشخصية الإنسان وحقوقه وحرياته، الأمر الذي يشكل مطلبًا قانونيًا ضروريًا لحمايتها، وخصوصًا بعد أن ضاعفت شبكة الإنترنت المخاطر التي تتعرض لها البيانات الشخصية، وأبرزت الاختراقات التي تتعرض لها. كما تبرز أهمية هذا البحث أيضًا بالنظر إلى ندرة الأبحاث العربية التي تعالج هذا الموضوع، ووضع أهم نماذج حماية البيانات الشخصية بين يدي المشرع السوري.

مسوغات البحث

تزخر وسائل الإعلام العالمية بأخبار الاعتداءات على البيانات الشخصية، وغير ذلك من العناوين التي أصبحت تتصدر ليس فقط نشرات الأخبار، بل المؤتمرات والفعاليات القانونية والتكنولوجية والإعلامية المختلفة حول العالم، ومؤخرًا تصاعد الجدل عالميًّا حول حماية البيانات، خصوصًا بعد تكرار حوادث التسريب والاختراقات وسوء الاستخدام، مما جعل عامة الناس، قبل المهتمين والمتخصصين بمجال القانون وحقوق الإنسان والسياسة وعلم الاقتصاد، يتنبهون إلى أثر الإنترنت على بياناتهم الشخصية، وقدرتها على انتهاك حقوقهم وحرياتهم وحياتهم الشخصية وأسرارهم التي كثيرًا ما أرادوا الاحتفاظ بها، فكانت هذه الانتهاكات المتعددة مسوغًا لبحث هذا الموضوع وإلقاء الضوء على أهمية الحماية القانونية في كبح هذه الانتهاكات، ولا سيما أنّ إنجاز البحث جاء في مرحلة ازداد بها الاهتمام بحماية البيانات على المستوى الدولي والوطني.

مصطلحات البحث

بناءً على مشكلة البحث سيوفر هذا القسم تعريفًا بأهم المصطلحات المتعلقة بحماية البيانات الشخصية، ومن هذا المنطلق حددت الباحثة أهم مصطلحات الدراسة الراهنة فيما يأتي:

شبكة الإنترنت (Internet): اختصار للكلمات (Inter Communication Network)، أي شبكة الوصل ما بين الشبكات أو شبكة الشبكات كما يقال أحيانًا[1]. وتعرّف بأنها: شبكة ضخمة من أجهزة الكمبيوتر

[1] ناصيف، الياس. (2009). العقود الدولية، العقد الإلكتروني في القانون المقارن. الطبعة الأولى. بيروت: لبنان. منشورات الحلبي الحقوقية. ص: 22.

تربط بين كثير من المؤسسات التجارية والمعاهد والأفراد حول العالم. حيث تقوم شبكة الإنترنت بربط عشرات الآلاف من شبكات الحاسوب الصغيرة، وتمكّن مستخدميها في جميع أنحاء العالم من إرسال الرسائل واستقبالها، وتبادل المعلومات بأشكالها المختلفة[2]. وقد عرف المشرّع السوري الشبكة بأنها: "ترابط بين وسائل تقانة المعلومات يسمح بتبادل المعلومات أو التشارك فيها وفق إجراءات (بروتوكولات) محددة، وتكون الشبكة داخلية أو دولية"[3].

البيانات الشخصية (Personal data): "أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وبيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية"[4].

معالجة البيانات الشخصية (processing of personal data): "أي عملية أو مجموعة من العمليات تُجرى، على بيانات شخصية أو على مجموعات من البيانات الشخصية، سواء كانت بالوسائل الآلية أم لم تكن؛ مثل جمع البيانات أو تسجيلها أو تنظيمها أو هيكلتها أو تخزينها أو تكييفها أو تعديلها أو استخراجها (استرجاعها) أو مراجعتها أو استخدامها أو الكشف عنها بنقلها أو إذاعتها أو إتاحتها أو تنسيقها أو دمجها أو تقييدها أو محوها أو تدميرها"[5].

حماية البيانات الشخصية: يقصد بحماية البيانات الشخصية مجموعة القواعد المتعلقة بمعالجة البيانات الشخصية، التي يجب أن يأخذها المشرع في اعتباره عند صياغة القوانين، ويجب أن يأخذها في الاعتبار أيضًا المتحكمون بالبيانات الشخصية والقائمون على عملية معالجتها، هذه العملية لا تنتهي بوضع القواعد، وإنّما هي

---

[2] الكسواني. عامر محمود. (2008)، التجارة عبر الحاسوب، دراسة مقارنة. الطبعة الأولى. الأردن: عمان. دار الثقافة للنشر والتوزيع. ص: 90.

[3] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة الأولى.

[4] قانون حماية البيانات الشخصية المصري رقم 151 لعام 2020. المادة (1).

[5] GDBR. 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

عملية مستمرة فمن الضروري تطوير القواعد القانونية في كل مرة تظهر فيها تحديات جديدة بسبب التطورات التكنولوجية الجديدة[6].

الشخص المعني بالبيانات (data subject): هو الشخص الطبيعي الذي يمكن التعرف عليه بصورة مباشرة 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"[7].

المتحكم (controller): هو الشخص الطبيعي أو الاعتباري أو السلطة العامة أو المرفق أو أي هيئة أخرى تحدد، بمفردها أو بالاشتراك مع آخرين، أغراض معالجة البيانات الشخصية ووسائلها[8].

المعالج (processor): أي شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو هيئة أخرى تعالج البيانات الشخصية نيابة عن المتحكّم"[9].

---

[6] Stefanick. (2011). Controlling knowledge: Freedom of information and privacy in a networked world. AU Press, Athabasca University. Canada. P: 43.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (GDPR). Article (4/1): ('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. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] GDPR. Article (4/7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[9] GDPR. Article (4/8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

صعوبات البحث

إنّ البحث في هذا الموضوع حمل في طياته صعوبات عدة تتمثل في النقاط الآتية؛ النقطة الأولى ندرة المراجع القانونية العربية المتخصصة في موضوع البحث، أما فيما يتعلق بالمراجع السورية فلم تستطيع الباحثة العثور على أي بحث قانوني سوري في هذا المجال، مما كان علينا لزامًا أن نتجه نحو المراجع والتشريعات الأجنبية بالدرجة الأولى؛ والنقطة الثانية عدم وجود تشريع خاص في حماية البيانات الشخصية في سورية أو أحكام قضائية تعالج المشكلات القانونية المرتبطة بموضوع البحث؛ والنقطة الثالثة حداثة مفهوم الحق في حماية البيانات الشخصية بصورة مستقلة عن الحق في الخصوصية، فهو ما يزال في طور التشكل عالميًا، وهناك الكثير من الغموض حول أهميته وأهدافه.

حدود البحث

تقتصر حدود هذا البحث على الحماية القانونية للبيانات الشخصية لمستخدمي شبكة الإنترنت في بعض التشريعات الدولية والوطنية، وذلك من خلال؛ عرض أبرز وأحدث المحاولات في هذا الشأن، على الصعيد الدولي والأوروبي؛ وكذلك تحليل المواد القانونية الرئيسية في التشريعات السورية ذات الصلة بحماية البيانات الشخصية؛ وهي المواد القانونية المتعلقة بحماية الخصوصية والسرية، والمواد القانونية المتعلقة بحماية سرية البيانات والمعلومات، لبيان مدى قصورها عن تأمين الحماية الكافية للبيانات الشخصية لمستخدمي شبكة الإنترنت في سورية. ومن ثم عرض تطور الحماية القانونية للبيانات الشخصية في التشريعات الدولية والتنظيم القانوني لهذه الحماية، وبصورة خاصة في اللائحة الأوروبية مع الأخذ بعين الاعتبار موقف المشرّع المصري.

الدراسات السابقة

نظرًا للأهمية الكبيرة لموضوع حماية البيانات الشخصية، على أنّه حق من حقوق الإنسان المعاصرة، فقد جذبت اهتمام كثير من الباحثين في جميع أنحاء العالم. ومع ذلك فإن الدراسات العربية محدودة ومن أبرز هذه الدراسات:

الدراسة الأولى: بولين أنطونيوس أيوب: "**الحماية القانونية للحياة الشخصية في مجال المعلوماتية**"، **2009**، تناولت الدراسة الحق في الحياة الشخصية أو الخصوصية كأحد حقوق الإنسان الأساسية، وتبنت الدراسة رأي مفاده أن الخصوصية تنطوي على حماية مظاهر مادية ومعنوية ومعلوماتية ولا تقف عند مفهوم حماية البيانات الشخصية الذي شاع استخدامه في ظل انتشار الوسائل التقنية ومخاطر المعالجة الآلية للبيانات المتعلقة بالحياة الخاصة وإنشاء بنوك لمعلومات، وتعزّز في البيئة الرقمية وتحديدًا الإنترنت، كما رأت الدراسة أن مصطلح الخصوصية يتخذ صورًا متعددة تدخل جميعها في نطاق الحق في الحياة الخاصة أو الشخصية، وهذه الصور هي؛ الخصوصية المادية، وخصوصية المكان، وخصوصية الاتصالات، وخصوصية المعلومات التي ترادف مصطلح حماية البيانات بحسب الدراسة. وعرضت الدراسة مخاطر المعالجة الآلية للبيانات الشخصية على الحريات العامة من خلال بحث؛ وظائف بنوك المعلومات، والأساليب التقنية المستخدمة في التعدي على الحياة الشخصية. ثم عرضت الوسائل التقنية والتنظيمية لحماية الحياة الشخصية في مجال المعلوماتية، ومن ثم النظام القانوني لحماية الحياة الشخصية في مجال المعلوماتية، وفيه بحثت الدراسة مبادئ حماية البيانات الشخصية، والحماية الجزائية للبيانات الشخصية من خلال بحث؛ جرائم الاعتداء على البيانات الشخصية في القانون الفرنسي، والقواعد الوقائية لحماية الحياة الخاصة. ومن أهم النتائج التي توصلت الدراسة أنّ اتساع استخدام التكنولوجيا أصبح خطرًا جديدًا على خصوصية الأفراد، وأنّ حماية البيانات الشخصية تشجع التجارة الإلكترونية، وأنّه لا بد من التوجه إلى تشريع شمولي في الدول العربية لتنظيم تقنية المعلومات. وعلى خلاف هذه الدراسة فإنّ البحث ينظر إلى حماية البيانات الشخصية على أنّه حق مستقل عن الخصوصية.

الدراسة الثانية: منى تركي الموسوي وجان سيريل فضل الله: "**الخصوصية وأهميتها ومخاطر التقنيات الحديثة عليها**"، **2013**، تناولت الدراسة موضوع الخصوصية المعلوماتية، وبيّنت أهم تأثيرات التكنولوجيا الحديثة عليه، فضلًا عن استجلاء طبيعة التهديدات التي تفرضها تقنيات الاتصال الحديثة، وتبنت الدراسة الرأي القائل بأن الخصوصية تقسم إلى عدة أنواع، خصوصية الشخص وخصوصية السلوك الشخصي وخصوصية الاتصالات الشخصية، وخصوصية البيانات الشخصية، ورأت الدراسة أن هناك ترادفًا بين خصوصية البيانات الشخصية

وخصوصية المعلومات وبين حماية البيانات، وأن استخدام اصطلاح الخصوصية في بيئة الإنترنت ومسائل عقود التقنية أو خدمات التقنية عمومًا يُشار إليه بحماية الخصوصية المعلوماتية أو حماية البيانات. وهو ما يخالف الاتجاه الحديث واتجاه البحث الذي ينظر إلى الحق في البيانات كحق مستقل.

الدراسة الثالثة: وسيم شفيق الشعار: "**النظام القانوني لوسائل التواصل الاجتماعي**"، **2017**. بحثت الدراسة الإشكالات القانونية التي تثيرها مواقع التواصل الاجتماعي، وما يتعلق منها بخصوصية الفرد ومدى التعرض لها، وما يتأتى عن ذلك من جمع بيانات شخصية وكيفية استعمالها، كما تطرق إلى حرية التعبير عن الرأي والقيود التي تفرض عليها والمسؤولية الناشئة عما ينشر على هذه الوسائل، واستعراض التنظيم القانوني لوسائل التواصل الاجتماعي، وما يستتبع ذلك من مسؤولية عن المحتوى المنشور وتحديد القانون المطبق والمحكمة المختصة. ومن أهم النتائج التي توصلت إليها الدراسة أن البيانات الشخصية تشكل محور الإشكالية القانونية على وسائل التواصل الاجتماعي، فالنموذج التجاري لوسائل التواصل الاجتماعي يقوم على مشاركة البيانات الشخصية بين المستخدمين، الذين يظنون أنّهم يستفيدون من خدمات مجانية، لكنهم في الواقع يدفعون الحق في الوصول إلى بياناتهم الشخصية مقابل الخدمات التي يحصلون عليها. كما توصلت الدراسة إلى أن تصرّف المستخدم على وسائل التواصل الاجتماعي هو الضمانة الأهم لحماية خصوصيته وبياناته الشخصية وممارسة حريته تحت سقف القانون. وعلى خلاف هذه الدراسة فإنّ البحث يركز على القواعد القانونية الخاصة بحماية البيانات الشخصية.

الدراسة الرابعة: سامح عبد الواحد التهامي: "**نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها**" **(دراسة في القانون الإماراتي)، 2018**. تناولت الدراسة المقصود بالبيانات الشخصية ونطاق الحماية التي كفلها المشرع الإماراتي، ومدى إمكانية تطبيق قواعد المسؤولية المدنية لتعويض المضرور من معالجة بيانات الشخصية. وتوصلت الدراسة إلى أن الحماية القانونية للبيانات الشخصية في القانون الإماراتي غير مكتملة، والنصوص الحالية تحكم نطاقًا ضيقًا من البيانات الشخصية، وإلى أن يضع المشرع الإماراتي تنظيم متكامل لحماية البيانات فإن المضرور يستطيع الاستناد لقواعد المسؤولية التقصيرية للحصول على تعويض عما أصابه من ضرر.

وتتفق هذه الدراسة مع ما توصل إليه هذا البحث في أن الحماية القانونية للبيانات الشخصية في القانون السوري غير مكتملة، والنصوص الحالية تحكم نطاقًا ضيقًا من البيانات الشخصية.

منهج البحث

انطلاقًا من طبيعة البحث وموضوعه، وللإجابة على إشكالية الدراسة، كان من المناسب اعتماد المنهج الوصفي والتحليلي، وذلك في عرض أهم التشريعات التي عالجت موضوع حماية البيانات الشخصية، وأهم التشريعات الداخلية ذات العلاقة بموضوع البحث، وتحليل موقف المشرع السوري لمعرفة مدى ملائمته في توفير الحماية للبيانات الشخصية، وكان من الضروري الأخذ بالمنهج المقارن لمعرفة القواعد الخاص بحماية البيانات التي أقرها المشرّعان الأوروبي والمصري، وساعد المنهج التاريخي في تسليط الضوء على تطور التشريعات الخاصة بحماية البيانات الشخصية على الصعيد الدولي والأوروبي.

خطة البحث

تشتمل خطة البحث على ما يأتي:

الفصل الأول: البيانات الشخصية المفهوم وأهداف الحماية والتحديات التي تواجهها على شبكة الإنترنت.

المبحث الأول: مفهوم البيانات الشخصية وأهداف حمايتها.

المبحث الثاني: التحديات التي تواجه البيانات الشخصية على شبكة الإنترنت.

الفصل الثاني: تطور الحماية القانونية للبيانات الشخصية في التشريعات الدولية والتنظيم القانوني لهذه الحماية.

المبحث الأول: تطور الحماية القانونية للبيانات الشخصية في التشريعات الدولية.

المبحث الثاني: التنظيم القانوني لحماية البيانات الشخصية.

الفصل الأول: البيانات الشخصية المفهوم وأهداف الحماية والتحديات التي تواجهها على شبكة الإنترنت

لقد بدأ الوصول إلى الإنترنت في الاتساع بشكل سريع عبر معظم دول العالم[10]، فقد أشارت آخر نتائج الإحصاءات العالمية مطلع عام (2022) أنّ عدد سكان العالم المقدر نحو (7.953) مليار شخص[11]، منهم (5.152) مليار مستخدم للإنترنت[12]، هذه الإحصائيات تشير إلى الدور الحيوي الذي تؤديه شبكة الإنترنت في حياتنا المعاصرة، وعلى أهمية ما تقدمه من خدمات من جهة، وحجم البيانات الشخصية الهائل الذي يتدفق بحرية حول العالم من جهة أخرى. وهنا يكمن التحدي الأكبر لشبكة الإنترنت العابرة للحدود على البيانات الشخصية، في أنّها أنتجت قدرًا هائلًا من البيانات الشخصية الحيوية في قطاع الاقتصاد وأعمال الشركات العاملة على الإنترنت، الأمر الذي أثّر سلبًا على حق الشخص في بياناته الشخصية.

---

[10] تشير الإحصاءات الواردة من الاتحاد الدولي للاتصالات السلكية واللاسلكية (ITU) إلى أنه بين عامي (2005) و (2010)، تضاعف عدد المستخدمين للإنترنت، وأنه في عام (1995) كان (0.4%) من سكان العالم يستخدمون الإنترنت، وبحلول شهر آذار (2011) ارتفعت هذه النسبة حتى وصلت إلى (30.2%) وهو ما يعادل أكثر من ملياري مستخدم للإنترنت منهم (1,2) مليار في الدول المتقدمة. مندل، توبي، بوديفات، أندرو، واجنر، بن، هوتن، ديكسي، وتوريس، نتاليا. (2012). دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير. سلسة اليونسكو بشأن حرية الإنترنت. ص: 12.

ومع نهاية (2016) بلغ عدد المستخدمين لشبكة الإنترنت (3.42) مليار مستخدم مسجل. أليغرين، مات. (2022/2/12). حقائق وإحصائيات حول الإنترنت لعام 2022. 10:30 .25/3/2022. Website Rating مساءً. متاح على الموقع الآتي:
https://www.websitehostingrating.com

كما شهد عام (2018) دخول أكثر من (360) مليون شخص الإنترنت لأول مرة، بمتوسط مليون مستخدم جديد يوميًا. وفي الشرق الأوسط يوجد (182) مليون شخص يتصلون بالإنترنت أي ما يقارب (71%) من سكان المنطقة، وفي عام (2018) وصل ما يقارب 18 مليون مستخدم جديد إلى الإنترنت. الإنترنت في الشرق الأوسط حقائق وأرقام (2019/2/6)، الحرة. 2022/3/24. 11 صباحًا. متاح على الموقع الآتي:
https://www.alhurra.com/

[11] كم عدد سكان العالم 2022؟ الترتيب العالمي للكثافة السكانية. هجرة نيوز. 2022/3/25. متاح على الرابط: https://hijra.news

[12] أليغرين، مات. (2022/2/12). حقائق وإحصائيات حول الإنترنت لعام 2022. مرجع سابق.

ومع وعي أهمية حماية البيانات الشخصية والتحديات التي تواجهها، نصت التشريعات الخاصة بحماية البيانات الشخصية على مفهوم البيانات الشخصية وأهداف حمايتها (المبحث الأول)، في ظل التحديات التي تواجهها على شبكة الإنترنت (المبحث الثاني).

المبحث الأول: مفهوم البيانات الشخصية وأهداف حمايتها

لا تعني البيانات الشخصية ذلك الكم الهائل من البيانات المخزنة على المواقع الإلكترونية أو في مراكز البيانات العملاقة التي تخزنها ملايين الخوادم، أو البيانات المخزنة في مراكز جمع وتحليل البيانات فقط. بل تشير أيضًا إلى كل ما ينتجه مستخدمو شبكة الإنترنت من بيانات أو ما يضيفونه أو ما يرتبط بهم أو ما يُجمع عنهم، والذي ربما لا يشكل قيمة أو أهمية لديهم إلا أن الشركات القائمة على تحليل البيانات تستفيد منه وتحوله إلى كنز لمعرفة توجهات وميول وتفضيلات وأراء المستخدمين[13]. وأصبحت إحدى أهم النقاشات ذات الصلة بموضوع حماية البيانات، تدور حول مفهوم البيانات الشخصية (المطلب الأول) والهدف من حمايتها (المطلب الثاني).

المطلب الأول: مفهوم البيانات الشخصية

لأن وضوح المفاهيم وتأطيرها من حيث مجالات تطبيقها وحدودها، أمر لازم من أجل تطبيق سليم للقواعد القانونية وبالتالي ضمان الأمن القانوني، ولتداخل مفهومي البيانات والمعلومات، وترابط مفهومي البيانات الشخصية

[13] عبد الصادق. (2019/4/14). الثورة الصناعية الرابعة: تحديات وفرص الاستحواذ على القوة الجديدة. المركز العربي لأبحاث الفضاء الإلكتروني. 2020/5/7. الرابط: http://accronline.com/article_detail.aspx?id=29387

ومعالجة البيانات، كان لابدّ من التمييز بين البيانات والمعلومات (الفرع الأول)، ثم تعريف البيانات الشخصية ومعالجة البيانات (الفرع الثاني).

الفرع الأول: التمييز بين البيانات والمعلومات

كثيرًا ما يتداخل استخدام هاتين الكلمتين ويترادف استخدام أحدهما مكان الأخرى، على الرغم من أنهما ليستا شيئًا واحدًا، كما أنّهما تعبران عن أشياء مختلفة وهناك فرق معنوي كبير بينهما[14]. ويرى بعض الباحثين أن محاولة التمييز بين المعلومات والبيانات، تعدُّ من وجهة النظر القانونية مسألة فلسفية أكثر منها ذات أثر قانوني، وذلك لأن مدى الحماية يمتد ليشمل ما يدخل في إطار النص القانوني وتنطبق عليه شروطه دون اعتبار للاسم الذي يطلق عليه، فالعبرة للحقائق والمعاني لا للألفاظ والمباني، والجوهر هو ما يجب الاهتمام به، فسواء كان محل الحماية هو البيانات أو المعلومات يجب أن يشتمل في طياته، وفي عناصر مفهومه، على المصلحة التي يراد من القانون حمايتها، فليس هناك من فرق بين مصطلح وآخر ما دام ليس هناك مردود قانوني، وبالتالي يمكن استخدامهم كمترادفين[15]. في حين ميّز البعض الآخر بين المعلومات والبيانات، فالبيانات أو المعطيات تعدّ مطلبًا أساسيًا للتعامل مع الحاسوب وترتبط بالاستخدام المعلوماتي، فمن أجل الوصول إلى المعلومات باستخدام الحاسوب يجب

[14] خشبة، محمد السعيد. (1991). المعالجة الإلكترونية للمعلومات. سلسلة الحاسبات الإلكترونية وتخطيط البرامج المطورة، الكتاب الثاني، جامعة الأزهر، مصر. المركز الدولي الإسلامي للدراسات والبحوث السكانية. ص: 8.

[15] فكري، أيمن عبد الله (2007). جرائم نظم المعلومات. دراسة مقارنة. دار الجامعة الجديدة للنشر. الإسكندرية. ص: 45-46.

البحث أولًا عن البيانات لتخزينها ومعالجتها ثم تحويلها إلى معلومات[16]. ولتوضيح الفرق بين كل من البيانات والمعلومات، ولوجود تداخل كبير بين هذين المصطلحين، سأبحث في تعريفهما ثم توضيح طبيعة العلاقة بينهما.

أولاً: تعريف المعلومات والبيانات

1. التعريف اللغوي: البيانات لغةً مشتقة من بان يبين، بيانًا وتبيانًا، فهو بائن وبيّن، وبان الشيء ظهر واتضح، وبيان مصدر بان، بمعنى الفصاحة وإبداء المقصود بلفظ حسن ومنطق فصيح معبر، وهي مفرد والجمع بيانات وهي معلومات تفصيلية حول شخص أو شيء ما يمكّن من خلالها الاستدلال عليه، أو رموز عددية وغيرها من المعلومات المتمثلة بشكل ملائم لمعالجتها بالحاسوب. وقاعدة البيانات هي مجموعة بيانات منظمة بحيث توفر سهولة الاستعادة[17].

أما المعلومات لغةً مشتقة من علِمَ يعلَم، فهو عالِم، والمفعول معلوم، وعلم الشخص الخبر حصلت له حقيقة العلم، عرفه وأدركه، درى وشعر به، وعلم الشيء حاصلًا أيقن به وصدقه، والمعلومات جمع مفرده معلومة، وتعني أخبار وتحقيقات أو كل ما يؤدي إلى كشف الحقائق وإيضاح الأمور واتخاذ القرارات، أو مجموعة الأخبار والأفكار المخزنة أو المنسقة بوساطة الكمبيوتر[18].

---

[16] الحسناوي، علي جبار. (2009). جرائم الحاسوب والانترنت. الطبعة العربية. الأردن: عمان. دار اليازوري العلمية للنشر والتوزيع، ص: 26-27.

[17] عمر، أحمد مختار. (2008) معجم اللغة العربية المعاصرة، المجلد الأول. الطبعة الأولى. القاهرة. منشورات عالم الكتب. ص: 275.

[18] عمر، أحمد مختار. (2008). مرجع سابق، ص1541-1544.

2. التعريف التقني: ومن الناحية التقنية تعرّف البيانات بأنها: معلومات مرمزة تتكون من أعداد وحروف ورموز مخزنة في كمبيوتر بحيث تعالج فيما بعد"[19]، أو هي كل ما يُقدّم من أرقام وكلمات ورموز، أو حقائق وإحصاءات خام لا توجد علاقة بينها ولم يقع تفسيرها أو معالجتها يدويًا أو إلكترونيًا[20]. وتشير إلى البيانات الرقمية والنصية والتصويرية الخام التي لا تدل على معنى مفيد، مثل الكلمات أو الجمل التي لا تعبّر عن شيء ولا تدل على معنى لعدم إمكانية فهمها فهي لم تعالج بعد للاستفادة منها واستخلاص النتائج لتصبح معلومات مفيدة، وهي بعكس المعلومات التي تدل على معانٍ مفيدة[21]. والمعلومات من الناحية التقنية تعرف بأنّها: "بيانات تمت معالجتها وتنظيمها لإعطاء حقائق ذات معنى"[22]. أو "معلومات مفيدة تدل على معنى تحققت نتائجها من خلال معالجة البيانات الخام في نظام الحاسوب ولها معنى وإفادة، وهي عكس كلمة بيانات"[23]. فالمعلومة هي القيمة المضافة من معالجة البيانات التي تكون بمثابة المادة الخام بالنسبة للمعلومات[24]. فالكلمات (92،921، علي) تشير إلى بيانات، ولكن عند تنظيمها ومعالجتها وتفسيرها تصبح هذه البيانات معلومات لطالب اسمه علي، ومجموع علاماته 921، ومعدله 92[25].

---

[19] قشوع، رشدي محمد. (1997). قاموس الكمبيوتر–إنكليزي عربي. جامعة ريدينج (بريطانيا). مراجعة د. خيري الجمل. جامعة كامبرج. ص: 63.

[20] خليفة، محمد. (2007). الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن. ص87.

[21] قاري، عبد الغفور عبد الفتاح. (2000). معجم مصطلحات المكتبات والمعلومات. إنكليزي–عربي. السلسلة الثانية. الرياض. مطبوعات مكتبة الملك فهد الوطنية. ص249 و82.

[22] قشوع. (1997). مرجع سابق. ص: 136.

[23] قاري، عبد الغفور عبد الفتاح. (2000). مرجع سابق. ص155.

[24] فكري. (2007). مرجع سابق. ص: 40.

[25] أمن تكنولوجيا المعلومات (د. ت)، الرابط:
http://specto.co/files/Books_Details/Samples/IT_Security_Arabic_SampleLesson.pdf

3. التعريف الفقهي: ميّز الباحثون المتخصصون في المجال القانوني بين المعلومات والبيانات بالقول إن "البيانات مصطلح عام لكل الحقائق والأرقام والرموز والحروف، فهي معطيات أولية يمكن معالجتها وإنتاجها عن طريق نظم المعلومات"، أما "المعلومات فهي البيانات التي عولجت من أجل تحقيق هدف معين أو لاستعمال محدد لغرض اتخاذ القرار ما، فالبيانات هي المواد الخام للمعلومات التي تعدُّ بمثابة المنتج النهائي الذي يأخذ صورًا متعددة وتستعمل في أغراض لا حصر لها"[26]. وميّز البعض بينهما بالقول بأنّه ينظر إلى البيانات على أنّها "سلسلة غير مترابطة من الحقائق الموضوعية التي يمكن الحصول عليها عن طريق الملاحظة أو عن طريق البحث والتسجيل". وترتبط بكونها صماء، أي لا تعبر عن أي اتجاه، بل هي بيانات خام أولية لا قيمة محددة لها إلا إذا ترابطت مع بعضها، سواء كانت مجموعة من الحروف أو الكلمات أو الأرقام أو الرموز أو الصور مثل بيانات الموظفين (الأسماء، الأرقام، الوظيفية، المهنة، الحالة الاجتماعية، السن). أما المعلومات فهي تلك البيانات التي عولجت، بحيث أصبحت ذات معنى، وباتت مرتبطة بسياق معين"[27]. فالمعلومات هي المعنى المستنتج من البيانات وذلك بمعالجتها بغرض تمكين ذوي الشأن من الحكم على الظواهر والمشاهدات[28].

4. التعريف التشريعي: على الصعيد التشريعي ميّزت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية لعام 1992 الخاصة بحماية أنظمة الحواسيب الآلية وشبكات المعلومات بين المعلومات والبيانات، حيث عرّفت البيانات بأنها: "مجموعة من الحقائق أو المفاهيم أو التعليمات التي تتخذ شكلًا محددًا يجعلها قابلة للتبادل والتفسير

---

[26] فكري. (2007). مرجع سابق. ص: 43.

[27] عبد الصادق. (2019/4/14). مرجع سابق.

[28] عفيفي، عفيفي كامل. (2003). جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة، منشورات الحلبي الحقوقية. بيروت: لبنان. ص: 29.

والمعالجة بوساطة الأفراد أو بوسائل إلكترونية"، كما عرفت المعلومات بأنها: "المعنى المستخلص من هذه البيانات"[29].

كما عرّفت اتفاقية بودابست لمكافحة الجريمة المعلوماتية بيانات الكمبيوتر بأنها: "كل تمثيل للوقائع أو للمعلومات أو المفاهيم تحت أي شكل، وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة ويجعل الحاسب يؤدي المهمة"[30].

وقد عرّفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[31]، البيانات بأنها: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوساطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها"[32]. أما المشرع السوري لم يعرّف البيانات واكتفى بتعريف المعلومات في المادة (1) من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17) بأنّها: "العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة الرقمية التي تتم معالجتها لتصبح ذات معنى أو مغزى معين وترتبط بسياق محدد". ويوضح التعريف أن المعلومات هي ناتج عملية معالجة البيانات، وبحسب هذا التعريف نستطيع أن نعرّف البيانات بأنها العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة الرقمية التي لا تعطي معنى أو مغزى معين ولا ترتبط بسياق محدد.

---

[29] فكري، أيمن عبد الله (2007). مرجع سابق. ص: 45.

[30] اتفاقية مجلس أوروبا لمكافحة الجريمة المعلوماتية. بودابست. 23 تشرين الثاني لعام 2001. المادة الأولى، فقرة (ب). الرابط: https://rm.coe.int/budapest-convention-in-arabic/1680739173

[31] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21. ووقعت عليها الجمهورية العربية السورية بتاريخ (21/ 12/ 2010).

[32] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المادة الأولى.

يتضح لنا بعد عرض التعريفات المختلفة للبيانات والمعلومات، أنّ مفهوم البيانات مفهوم مختلف عن مفهوم المعلومات، فالبيانات هي كل ما يمكن معالجته من حروف أو أصوات أو صور أو رموز أو كلمات أو أرقام أو حقائق عشوائية وغير منتظمة، سواء كانت بيانات لا يمكن قراءتها وفهم دلالتها بدون الدخول في عمليات معالجتها، بتحليلها أو بالربط فيما بين أكثر من بيان، أو بإجراء أي عملية من عمليات المعالجة الأخرى التي تؤدي إلى استخلاص نتائج مترتبة عليها، أو كانت معلومات ذات معنى تُعالج لغاية استخلاص معلومات أُخرى تلبي غاية محددة مختلفة عن المعنى السابق لها. وبالنتيجة فإنّ البيانات هي معلومات لا تتحقق الفائدة منها على صورتها الحالية، لذلك فالأمر يستدعي تحليلها وإجراء العمليات الحسابية والمنطقية عليها، أو بمعنى آخر معالجتها للاستدلال منها على معلومات مطلوبة، فالبيانات هي مدخلات عملية المعالجة. أما المعلومات فهي ناتج عملية معالجة البيانات بعد أن أصبح لها معنى وفائدة وتكون منظمة ومحددة بما فيه الكفاية لتوليد معنى قابل للإدراك وأكثر فائدة من صورتها السابقة، وبالتالي قد تختلف المعلومات الناتجة عن المعالجة باختلاف الهدف من المعالجة، وبهذا تكون الحصيلة النهائية المترتبة على عملية معالجة أي بيانات أو معلومات واستنتاج ما يمكن استنتاجه منها هي المعلومات، فالمعلومات تأتي في مرحلة تالية ومتأخرة عن البيانات، وهي مخرجات عملية المعالجة التي تصل للإنسان. فمفهوم البيانات أوسع من مفهوم المعلومات، وتشمل أي نوع من البيانات أو المعلومات تتعرض لأي إجراء من إجراءات المعالجة.

ثانيًا: طبيعة العلاقة بين المعلومات والبيانات

توضح التعريفات السابقة أن المعلومات تعتمد على البيانات، فهي ناتج معالجة البيانات، بهدف استخلاص ما تتضمنه البيانات أو تشير إليه، وتتميز العلاقة بين البيانات بالمعلومات بأنها ذات طبيعة دورية ومتجددة، حيث تُجمع البيانات وتُعالج للحصول على المعلومات ثم تستخدم هذه المعلومات في اتخاذ قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات، ثم تُعالج مرة أُخرى للحصول على معلومات أخرى مختلفة أو لاتخاذ قرار آخر يؤدي بدوره إلى تنفيذ مجموعة جديدة من الإجراءات، وهو ما يسمى بالدورة الاسترجاعية للمعلومات[33]. وهنا تجدر الإشارة إلى أنه عند معالجة البيانات بشكل مختلف، فإنه قد ينتج من البيانات نفسها معلومات مختلفة.

نستنتج مما سبق أنّ هناك اختلافًا بين ما يدل عليه مصطلح البيانات التي تمثل سلسلة غير مترابطة من المعلومات يمكن الحصول عليها عن طريق الملاحظة أو التتبع، وتتصف بأنها لا تعبّر بالضرورة عن أي معنى وليس لها قيمة محددة لها إلا إذا ترابطت مع بعضها أو تمت معالجتها بأي صورة أُخرى، سواء كانت هذه البيانات مجموعة من الحروف أو الكلمات أو الأرقام أو الرموز أو الصور أو الأصوات. أما المعلومات فتعني تلك البيانات التي خضعت لعملية من عمليات المعالجة بحيث أصبحت ذات معنى وباتت مرتبطة بسياق معين، كما أنه من الممكن معالجة المعلومات مرة أخرى للحصول على معلومات مختلفة، وبالتالي فإن البيانات قد يكون لا معنى لها ولا ترتبط بسياق محدد، وتُعالج للحصول على معلومات ذات معنى، وقد تكون معلومات ذات معنى لكن الغاية منها لم تتحقق في صورتها الحالية ولاستخلاص المعلومات المنشودة لا بد من معالجتها، لذلك فهي معلومات لكنها

[33] خشبة. (1991). مرجع سابق، ص: 9.

غير مفيدة في صورتها الحالية. فتكون البيانات هي أي بيانات أو معلومات وتُعالج، وبذلك يكون مفهوم البيانات أوسع من مفهوم المعلومات، كما أنه مفهوم مرتبط بعملية المعالجة.

الفرع الثاني: تعريف البيانات الشخصية ومعالجة البيانات الشخصية

يعدّ مصطلحا البيانات الشخصية ومعالجة البيانات الشخصية من المصطلحات الحديثة نسبيًا، وقد عرفتهما التشريعات التي عنيت بتوفير الحماية للبيانات الشخصية. في حين خلت التشريعات السورية من تعريف لهما، وانطلاقًا من هذا المبدأ سأستعرض التعريفات البارزة في قوانين حماية البيانات الشخصية على المستوى الدولي والأوروبي والعربي، وتبيان مدى تقاربها وتباعدها ومواكبتها للتطورات التقنية.

أولًا: تعريف البيانات الشخصية

تعرّف البيانات الشخصية بأنها: "أي معلومات عائدة لشخص طبيعي محدد أو قابل للتحديد (الشخص المعني)"[34]. وهو التعريف الذي جاءت به المادة (b/1) منظمة التعاون الاقتصادي والتنمية[35] في دليل حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود، والمادة (a/2) من اتفاقية مجلس أوروبا[36] لحماية الأفراد

---

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

[35] منظمة دولية هدفها الرئيسي تعزيز السياسات التي من شأنها تعزيز الرفاهية الاقتصادية والاجتماعية للناس في جميع أنحاء العالم، والعمل على وضع معايير دولية قائمة على الأدلة وإيجاد حلول لمجموعة من التحديات الاجتماعية والاقتصادية والبيئية إلى جانب الحكومات وصانعي السياسات والمواطنين، تأسست عام 1961 وتضم 34 عضوًا ينتشرون حول العالم من أمريكا الشمالية والجنوبية إلى أوروبا ومنطقة آسيا والمحيط الهادئ: about the OECD. Last updated: (1/6/2021). Available at: https://www.oecd.org/about/

[36] مجلس أوروبا: المنظمة الرئيسة المعنية بالدفاع عن حقوق الإنسان في القارة الأوروبية يضم (47) عضوًا، 27 منهم أعضاء في الاتحاد الأوروبي Council of Europe portal, The Council in brief, Last updated: 3/6/2021. Available At: https://www.coe.int/en/web/about-us/who-we-are.

في مجال المعالجة الآلية للبيانات الشخصية رقم 108، فالبيانات الشخصية حسب هذا التعريف هي أي معلومة مهما كانت، ترتبط بشخص طبيعي وتتيح إمكانية تحديد هويته والتعرّف عليه، إلا أنّ هذا التعريف أثار بعض الإشكالات، إذ أنّه استثنى بيانات لا ترتبط بالشخص الطبيعي، ولكن يمكنها أن تساعد على تحديد هوية الشخص، عبر سماحها بتحديد هويته بشكل غير مباشر، مثل البيانات التي لا ترتبط بالشخص الطبيعي ذاته، وإنما ترتبط بوسيلة يستعملها كرقم تسجيل السيارة، ورقم الهاتف الثابت والنقال، أو المعلومة المرتبطة بوسيلة إلكترونية أو رقم التعريف الإلكتروني للجهاز (IP). فمعرفة متى أو كيف يكون الشخص قابلًا للتحديد، يجب أن يأخذ بعين الاعتبار، جميع الوسائل المتاحة والممكنة لتحديد الهوية، التي يمكن أن يحصل عليها المسؤول عن المعالجة، أو أي شخص آخر[37]. وتكمن خطورة استثناء هذه الفئة من البيانات وبقائها خارج الحماية القانونية، في الإمكانية التي تتيحها بالتعدي على حقوق الأشخاص وحرياتهم الأساسية، من خلال معالجة هذه البيانات، بعيدًا عن قواعد قانونية تنظم عملية المعالجة، لعدم إمكانية تطبيق النص الذي يستبعدها من الحماية بطريقة غير مباشرة.

وفيما بعد اتخذت تشريعات الاتحاد الأوروبي والتشريعات الداخلية اللاحقة تعريفًا واسعًا للبيانات الشخصية، هذا التوسع بسبب التطور التكنولوجي وبصورة خاصة الاستعمال المكثّف لشبكة الإنترنت، الأمر الذي فرض متغيرات في الحياة الاقتصادية والاجتماعية، مما فتح المجال أمام ظهور مشكلات جديدة تهدد البيانات الشخصية. فالتوجيه الأوربي لحماية الأشخاص الطبيعيين من معالجة البيانات الشخصية وحرية تداولها رقم (95/46/EC)،

[37] الأشقر جبور، منى؛ وجبور، محمود. (2018). البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد. أبحاث ودراسات (5). الطبعة الأولى. بيروت: لبنان. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب ص: 76.

لعام (1995)[38]، اعتمد تعريفًا واسعًا للبيانات الشخصية، وعرّف البيانات الشخصية بأنها: "أي معلومة متعلقة بشخص طبيعي محدد أو قابل للتحديد (الشخص المعني)". وتابع التعريف بتوضيح أن البيانات الشخصية "تمكّن من معرفة الشخص، بصفة مباشرة أو غير مباشر، ولاسيما بالرجوع إلى رقم التعريف، أو من خلال عنصر أو عدة عناصر خاصة بهويته الجسدية أو الفسيولوجية أو الفكرية أو الاقتصادية أو الثقافية أو الاجتماعية[39]".

وقد تطرقت محكمة العدل الأوروبية[40] في الكثير من أحكامها لمفهوم البيانات الشخصية، وأكدت أن قائمة أسماء المشاركين في الاجتماع هي بيانات شخصية، حيث يمكن التعرف على الأشخاص[41]. وأن البيانات المتعلقة

---

[38] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

[39] Directive 95/46/EC. 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;

[40] محكمة العدل الأوروبية: هي أعلى هيئة أوروبية قضائية للاتحاد الأوروبي. تتخلص مهمة المحكمة باختصار في ضمان الالتزام بالقوانين والحقوق الأوروبية عند التوقيع على الاتفاقات والمعاهدات التي يبرمها الاتحاد مع الجهات الأخرى. تتخذ محكمة العدل الأوروبية من لوكسمبورغ مقرا لها. أنظر موقع (DW). (13.10.2022) الرابط:
https://p.dw.com/p/1FvZ2

[41] Court of Justice. Judgment of the Court (Grand Chamber) of 29 June 2010. Case C-28/08 P. (European Commission v The Bavarian Lager Co. Ltd). operative part: "1. Sets aside the judgment of the Court of First Instance of the European Communities of 8 November 2007 in Case T-194/04 Bavarian Lager v Commission, in so far as it annuls the Commission's decision of 18 March 2004, rejecting an application for access to the full minutes of the meeting of 11 October 1996, including all the names, and in so far as it orders the European Commission to pay the costs of The Bavarian Lager Co. Ltd؛ 2. Dismisses the action of The Bavarian Lager Co. Ltd against the Commission's decision of 18 March 2004, rejecting an application for access to the full minutes of the meeting of 11 October 1996, including all the names...". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0028

بالدخل المكتسب وغير المكتسب[42]، بالإضافة إلى ممتلكات الأشخاص الطبيعيين يُشكل بيانات شخصية[43]. كما رأت أن المعلومات المتعلقة بفترات العمل اليومية وفترات الراحة بكل عامل الواردة في سجل العمل تشكل بيانات شخصية لأنها تمثل معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه[44]. وفي اجتهاد آخر أقرّت المحكمة أن اسم الشخص المقترن برقم هاتفه أو المقترن بمعلومات تتعلق بظروف عمله أو هواياته هي بيانات شخصية، والإشارة إلى حقيقة أن شخصًا قد أصيب في قدمه وكان يعمل نصف الوقت لأسباب طبية يشكل بيانات شخصية تتعلق بالصحة[45]، أيضًا تشكل صورة الشخص التي سجلت بوساطة الكاميرا بيانات شخصية لأنها تتيح

---

[42] الدخل المكتسب: الدخل الذي يحصل عليه المستقل أو أفراد الأسرة نتيجة جهد يُبذل، مثل العمل أو النشاط التجاري المسجل. والدخل غير المكتسب: الدخل المستمد من مصادر -غير العمل أو النشاط التجاري المسجل- مثل الممتلكات وعوائدها والإعانات الاجتماعية أو الحكومية التي يحصل عليها المستقل أو أفراد الأسرة. اللائحة التنفيذية لنظام الضمان الاجتماعي السعودي. متاحة على الموقع أرقام. على الرابط الآتي:
https://www.argaam.com/ar/article/articledetail/id/1477312

[43] Court of Justice. Judgment of the Court (Grand Chamber) of 16 December 2008. Case C-73/07. (Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy). Operative part: "1.Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is to be interpreted as meaning that an activity in which data on the earned and unearned income and the assets of natural persons ". Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0073&qid=1652172677513

[44] Judgment of the Court (Third Chamber). of 30 May 2013. Case C-342/12. (Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)). operative part : "1. Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is to be interpreted as meaning that a record of working time, such as that at issue in the main proceedings, which indicates, in relation to each worker, the times when working hours begin and end, as well as the corresponding breaks and intervals, is included within the concept of 'personal data', within the meaning of that provision. 2. Article 6(1)(b) and (c) and Article 7(c) and (e) of Directive 95/46 do not preclude national legislation, such as that at issue in the main proceedings, which requires an employer to make the record of working time available to the national authority responsible for monitoring working conditions so as to allow its immediate consultation, provided that this obligation is necessary for the purposes of the performance by that authority of its task of monitoring the application of the legislation relating to working conditions, in particular as regards working time." Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CA0342&qid=1652178526664

[45] Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist. Case C-101/01 paragraph (24): "The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition

التعرف على الشخص المعني[46]. وتشكل بصمات الأصابع بيانات شخصية، لأنها تحتوي بشكل موضوعي على معلومات فريدة عن الأفراد تتيح التعرف عليهم بدقة[47]. وفي اجتهاد آخر أكّدت على أنّ البيانات التي عثر عليها بوساطة محركات البحث وخزنت وجعلت متاحة لمستخدميها، وكانت تتضمن معلومات تتعلق بأشخاص طبيعيين محددين أو يمكن تحديدهم هي بيانات شخصية[48]، وقد أقرت أن مفهوم البيانات الشخصية شاملة للعنوان الخاص برقم التعريف الإلكتروني للجهاز IP، ولكن عند وجود بيانات أخرى تمكنها من تحديد هوية صاحب البيانات[49].

---

in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies". Operative part (3): " Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46." Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

[46] Judgment of the Court (Fourth Chamber). Of 11 December 2014. (František Ryneš v Úřad pro ochranu osobních údajů). Case C-212/13. Paragraph (22): "Accordingly, the image of a person recorded by a camera constitutes personal data within the meaning of Article 2(a) of Directive 95/46 inasmuch as it makes it possible to identify the person concerned". Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212

[47] Judgment of the Court (Fourth Chamber) of 17 October 2013. (Michael Schwarz v Stadt Bochum). Case C-291/12. Paragraph (27): "Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows those individuals to be identified with precision". Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0291&qid=1652189786723

[48] Judgment of the Court (Grand Chamber). Of 13 May 2014. (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González). Case C-131/12. Paragraph (27): " So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of that directive". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

[49] Court of Justice. Judgment of the Court (Second Chamber). of 19 October 2016. Case C-582/14. 19. 10. 2016. (Patrick Breyer v Bundesrepublik Deutschland). operative part: "1. Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation

كما اتخذت اللائحة الأوروبية لحماية البيانات الشخصية، التي دخلت حيز التنفيذ في (25 أيار 2018) وألغت التوجيه الأوروبي رقم (95/46/EC)، لعام (1995)، موقفًا أكثر تطورًا ودقة وملاءمة لمخاطر التكنولوجيا على البيانات الشخصية، فعرّفت البيانات الشخصية بأنّها: "أي معلومة متعلقة بشخص طبيعي محدد أو قابل للتحديد "الشخص المعني""، وتابعت بالتوضيح والتفصيل بأن البيانات الشخصية "المتعلقة بالشخص الطبيعي القابل للتحديد تمكّن من معرفته بصورة مباشرة أو غير مباشر، ولاسيما بالرجوع إلى عنصر مُعَرف، مثل الاسم ورقم التعريف وبيانات الموقع ومعرّف الاتصال عبر الإنترنت أو لواحد أو أكثر من العناصر المميزة لهويته الجسدية أو الفيزيولوجية أو الجينية أو الفكرية أو الاقتصادية أو الثقافية أو الاجتماعية"[50].

كما عرّف المشرع المصري البيانات الشخصية بأنها: "أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وبيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية"[51].

---

to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582&qid=1652172799454

[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (GDPR). 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."

[51] قانون حماية البيانات الشخصية المصري رقم 151 لعام 2020. المادة (1).

تؤمن التعريفات المعتمدة في اللائحة الأوروبية والقانون المصري حماية فاعلة للبيانات والمعلومات الشخصية، باستخدامها تعابير ومصطلحات واسعة الدلالة تخدم هذه الغاية، وتغطي فئات واسعة من البيانات، باستخدام عبارات مثل أي بيانات أو معلومات بغض النظر عن مصدرها أو شكلها، بمجرد أنّها تساعد على تحديد هوية الشخص الطبيعي أو تجعل قابلًا للتحديد، سواء بصورة مباشرة أو غير مباشرة، مما يؤكد على ضرورة تحقيق مستوى أعلى من الحماية للبيانات الشخصية داخل المجتمع، وبالتالي للأشخاص المعنيين بالبيانات، فالحماية لا تنطبق على المعلومات التي تحدد هوية الشخص بشكل مباشر مثل الاسم أو الموطن أو بيانات الحياة الصحية أو السجلات الخاصة بالمهنيين، أو السجلات الخاصة بالحالة الاقتصادية للأشخاص فحسب، ولكن أيضًا على بعض البيانات التي تحدد هوية الشخص بصورة غير مباشرة؛ مثل البيانات البيومترية، التي تتضمن الصورة والصوت أو بصمات الأصابع؛ والبيانات الشخصية التي ترتبط غالبًا بالتقنيات الحديثة، مثل رقم الجوال، أو عنوان البريد الإلكتروني، أو رقم بطاقة ائتمان، أو رقم التعريف الإلكتروني للجهاز (IP)، أو أي بيانات تعريفية أخرى قد يفرضها التطور التكنولوجي.

وتعدّ هذه التعريفات مواكبة للتطور التكنولوجي الحديث الذي يجمع الكثير من البيانات الشخصية، ويربط فيما بينها ويقارنها بينها وبين أي بيانات أخرى، بالإضافة إلى الدلالة التمثيلية، غير الحصرية، التي تشير إليها هذه التعاريف، وبالتالي أي بيانات أو معلومات تتعلق بالشخص الطبيعي ومن الممكن أن تحدده بصورة مباشرة أو غير مباشرة تدخل في نطاق البيانات الشخصية. ولا شك أنّ هذا التوسع في التعريف يتناسب مع هدف توفير

حماية قانونية فاعلة للبيانات الشخصية وبالتالي تأمين الطمأنينة والثقة لدى الأشخاص من جهة، ومواكبة التطورات التكنولوجية المتسارعة من جهة أخرى. كما نستنتج أنّ البيانات الشخصية تتميز بمجموعة من الخصائص أهمها:

1. تتضمن البيانات الشخصية أي نوع من المعلومات أو البيانات المتعلقة بالشخص الطبيعي. وتكون البيانات متعلقة بالشخص إذا تعلق محتوى المعلومات أو البيانات به، بغض النظر عن أي هدف من جانب المتحكم في البيانات، أو أي تأثير لتلك المعلومات على صاحب البيانات[52]. وذلك يغطي معلومات موضوعية، مثل وجود مادة معينة في دم الشخص؛ وأيضًا معلومات أو آراء أو تقويمات ذاتية، ويشكل هذا النوع الأخير من البيانات حصة كبيرة من معالجة البيانات الشخصية في الكثير من المجالات مثل الخدمات المصرفية والتأمين والعمل[53].

كما تكون هذه البيانات متعلقة بالشخص إذا كان الغرض من استخدامها تقييمه أو التأثير على حالته أو سلوكه؛ فعلى سبيل المثال يوفر سجل المكالمات الخاص بهاتف داخل مكتب الشركة معلومات حول المكالمات التي أُجريت من هذا الهاتف المخصص للشركة، والشركة ملزمة تعاقديًا بدفع أجرة تلك المكالمات، ولكن من ناحية أخرى يوفر سجل المكالمات أيضًا معلومات حول الاتصالات الخاصة التي يقوم بها الموظف في أثناء أوقات العمل، كما يوفر أيضًا معلومات حول الشخص الذي استقبل الاتصال، فهنا يمتد مفهوم البيانات الشخصية ليشمل

[52] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data, 01248/07/EN. WP 136. Adopted on 20th June. Example No. 1. P. 11. Last updated: 18/4/2021. Available at: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

[53] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference. Example No. 1. P. 7.

كل من المكالمات الصادرة والواردة بقدر ما تحتوي من معلومات تتعلق بحياة الأفراد وعلاقاتهم الاجتماعية واتصالاتهم[54].

2. البيانات الشخصية تشير إلى هوية الشخص الطبيعي أو حالته أو سلوكه وبالتالي من الممكن أن تكون هذه المعلومات، بيانات شخصية إذا أشارت إلى هوية الشخص الطبيعي أو حالته أو سلوكه، سواء كانت صحيحة أم خاطئة، وسواء كانت على درجة من السرية والخصوصية أم معلومات عادية[55]. كما تتضمن البيانات الشخصية معلومات عن الأفراد، بغض النظر عن صفة هؤلاء الأشخاص (مستهلك، أو مريض، أو موظف، أو عميل، إلخ)، فعلى سبيل المثال تعدّ معلومات وصفة الدواء، بيانات شخصية عن الطبيب الذي يصف هذا الدواء، حتى لو كان المريض مجهول الهوية، وبالتالي فإن توفير معلومات حول الوصفات الطبية المكتوبة من قبل أطباء محددين أو قابلين للتحديد، لمنتجي العقاقير الطبية يشكل بيانات شخصية[56].

3. البيانات الشخصية تتضمن أي بيانات شخصية بصرف النظر عن التنسيق أو الوسيط الذي تحتوي عليه هذه المعلومات أو البيانات، سواء أكان ذلك أبجديًا أو رقميًا أو فوتوغرافيًا أو صوتيًا، كما تشمل البيانات المحفوظة على الورق، وكذلك البيانات المخزنة في ذاكرة الكمبيوتر عن طريق رمز ثنائي، أو على شريط فيديو، فتعدّ بيانات

---

[54]Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference. Example No. 1. P: 11.

[55] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference. Example No. 1. P. 7.

[56] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference. Example No. 1. P. 7.

الصوت والصورة بيانات شخصية بقدر ما تعطي معلومات عن فرد، كما يمكن أن تكون البيانات الواردة في نص مستند إلكتروني بيانات شخصية، بشرط استيفاء المعايير الأخرى في تعريف البيانات الشخصية[57].

ثانيًا: تعريف معالجة البيانات الشخصية

اتضح مما سبق أن البيانات هي المادة الخام التي يتم معالجتها للحصول على شكل أكثر فائدة واستخدامًا وتسمى في هذه الحالة المعلومات، وتُعرف عملية تحويل البيانات إلى معلومات باسم معالجة البيانات (Data Processing)[58].

تُعرّف المعالجة من الناحية التقنية بأنها: "تنظيم واستنباط المعلومات من البيانات" أو هي: التعامل مع البيانات لإعطاء معلومات مفيدة أو لتصنيف ملفات البيانات وتنظيمها[59]. كما تُعرّف أيضًا بأنها: "تنفيذ مجموعة منظمة من العمليات المتتالية على البيانات المدخلة في الحاسوب، وتضم عمليات مختلفة ومتباينة من حيث الشكل والإدخال والإخراج والتنفيذ لمعالجتها. أو هي "الطريقة التي يتبعها نظام الحاسوب في معالجة البيانات[60]". ومما سبق نستطيع تعريف المعالجة بأنها: إجراء أو أكثر يُنفذ على أي نوع من البيانات أو المعلومات للحصول على معلومات ذات معنى أو أكثر فائدة.

---

[57] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference. Example No. 1. P: 7-8.

[58] خشبة. (1991). مرجع سابق. ص: 8.

[59] قشوع. (1997). مرجع سابق. ص: 136.

[60] قاري. (2000). مرجع سابق. ص83.

وترتكز عملية المعالجة في جوهرها على التعامل مع البيانات الشخصية، وتحتل على هذا الأساس، حيزًا واسعًا في قوانين حماية البيانات الشخصية. وفي حين أنّ المشرع السوري سنَّ عدة قوانين في محاولة منه لمواجهة التحديات الناجمة عن التطور التكنولوجي على حقوق الأفراد[61]، ولكنه لم يرد في أيّ من هذه القوانين تعريف للمعالجة، لذلك سنتتبع تعريف المعالجة كما جاءت في بعض تشريعات حماية للبيانات الشخصية لنتبين المقصود من معالجة البيانات.

لم تعرّف اتفاقية مجلس أوروبا معالجة البيانات الشخصية، واكتفت بتعريف المعالجة الآلية بأنها تشمل العمليات التي تجري كليًا أو جزئيًا بالوسائل الآلية، وتتضمن تخزين البيانات، وتنفيذ العمليات المنطقية أو الحسابية على تلك البيانات أو تعديلها أو محوها أو استخراجها (استرجاعها) أو نشرها[62]. إلا أن ما يؤخذ على هذا التعريف أنّه استثنى عمليات المعالجة اليدوية البحتة، ومع أنّ نطاق عمليات المعالجة المذكورة ضيقه، إلا أنّها وردت على سبيل المثال لا الحصر، وربما كانت أبرز عمليات المعالجة التي تجري في وقت صدور الاتفاقية، لذلك لم يتوسع التعريف في عرض عمليات المعالجة التي تتعرض لها البيانات.

---

[61] على سبيل المثال: قانون التوقيع الإلكتروني وخدمات الشبكة الصادر بالقانون رقم (4) بتاريخ (2009/2/25)، قانون الاتصالات السوري الصادر بالقانون رقم (18) بتاريخ (6/1/ 2010)، قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، الصادر بالمرسوم التشريعي رقم (17) تاريخ (2012/2/8)، قانون المعاملات الإلكترونية السوري رقم (3) الصادر بتاريخ (2014/3/4)، قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17).

[62] اتفاقية مجلس أوروبا لحماية الأشخاص اتجاه المعالجة الآلية للبيانات الشخصية. ستراسبورغ (1981/1/28). المادة (2/ج): "معالجة آلية" تتضمن العمليات التالية التي يتم القيام بها، كليًا أو جزئيًا، استنادًا إلى طرق آلية: تسجيل البيانات، تطبيق عمليات منطقية أو حسابية أو الاثنين معا على تلك البيانات أو تعديلها أو محوها أو استخراجها (استرجاعها) أو نشرها".

وقد تفادت التشريعات اللاحقة هذا القصور فاعتمدت مفهومًا أوسع في تعريف معالجة البيانات الشخصية فأكّد المشرع الأوروبي، في التوجيه الأوربي رقم 95/46/EC، أن المقصود بمعالجة البيانات الشخصية: "أي عملية أو مجموعة من العمليات تُجرى على البيانات الشخصية، سواء كانت بوسائل آلية أم لم تكن؛ مثل جمع البيانات الشخصية أو تسجيلها أو تنظيمها أو تخزينها أو تكييفها أو تعديلها أو استخراجها (استرجاعها) أو مراجعتها أو استخدامها، أو الكشف عنها بنقلها أو إذاعتها أو إتاحتها، أو تنسيقها أو دمجها أو حجبها أو محوها أو تدميرها"[63].

ليعود المشرّع الأوروبي ويطور من مفهوم معالجة البيانات الشخصية بموجب اللائحة العامة لحماية البيانات الشخصية (GDPR)، ويضيف عمليتي الهيكلة والتقييد من ضمن الأمثلة على عملية معالجة البيانات ويزيل حجب البيانات، فعّرف معالجة البيانات بأنها: "أي عملية أو مجموعة من العمليات تُجرى، على بيانات شخصية أو على مجموعات من البيانات الشخصية، سواء كانت بالوسائل الآلية أم لم تكن؛ مثل جمع البيانات أو تسجيلها أو تنظيمها أو هيكلتها أو تخزينها أو تكييفها أو تعديلها أو استخراجها (استرجاعها) أو مراجعتها أو استخدامها أو الكشف عنها بنقلها أو إذاعتها أو إتاحتها أو تنسيقها أو دمجها أو تقييدها أو محوها أو تدميرها"[64].

---

[63] Directive 95/46/EC. 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".

[64] GDBR. 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

ويعدُّ هذا التعريف لفكرة المعالجة تعريفًا واسعًا، فرضه التطور التكنولوجي، ويؤدي بنا إلى القول بأنه لا يمكن تخيل أي إجراء يتعلق بالبيانات الشخصية لا يعدُّ معالجة لهذه البيانات. وبالتالي فمعالجة البيانات الشخصية تتضمن أي إجراء يتعلق بهذه البيانات أيًا كانت الطريقة التي اُستخدمت، فأيُّ إجراء يُتخذ ويكون متعلقًا بالبيانات الشخصية يعدُّ في نظر القانون معالجة لهذه البيانات. كما يجب ملاحظة أن ما ذكر في التعريفات السابقة من إجراءات المعالجة التي تقع على البيانات الشخصية هي أمثلة لأكثر الإجراءات تطبيقًا وليس حصرًا لها، فالتعريفات السابقة نصت صراحة أن هذه العمليات مجرد أمثلة على المعالجة، وبالتالي من الممكن أن يكون أي إجراء آخر خلاف لهذه الإجراءات معالجة للبيانات الشخصية[65].

في حين عرّف المشرع المصري معالجة البيانات الشخصية بأنها: "أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها، أو تحليلها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيا أو كليا". وبمقارنة التعريف في القانون المصري مع التعريفات الواردة في اللائحة الأوروبية يظهر جلياً أن المشرّع المصري لم يذكر صراحة أن إجراءات المعالجة الواردة قد ذُكرت على سبيل المثال، وهذا ما يدعو للقول بأن هذه الإجراءات قد وردت على سبيل الحصر. وإن كان تعداد الأفعال التي تدخل في نطاق المعالجة وفقا لتعريف المشرّع المصري يكاد يبدو كافياً من الوهلة

[65] التهامي، سامح عبد الواحد. (3/2015). ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي. مجلة كلية القانون الكويتية العالمية. السنة الثالثة. العدد التاسع. ص: 40.

الأولى، وقد لا يُتخيل وجود أفعال أو عمليات يمكن أن تقع على البيانات غير تلك الواردة في التعريف إلا أنّه كان من الأفضل لو اقتدى المشرع المصري بنظيره الأوروبي في هذا الشأن حتى يترك الباب مفتوحاً أمام استيعاب أي أفعال أخرى قد تنشأ عن التطور التكنولوجي المستمر في معالجة البيانات الشخصية. كما قصر المشرّع المصري المعالجة على العمليات الإلكترونية أو التقنية التي تقع على البيانات، بينما توسّع المشرع الأوروبي في وسيلة المعالجة أياً كان نوعها سواء كانت إلكترونية أم لم تكن كذلك، وكان من الأفضل أن يحذو المشرّع المصري حذو المشرّع الأوروبي في هذا الشأن أيضًا[66].

ومما عُرض سابقًا نستطيع القول إنّ المقصود بمعالجة البيانات الشخصية؛ هو إجراء أو مجموعة من الإجراءات تُنفذ على أي بيانات أو معلومات متعلقة بشخص طبيعي محدد أو يمكن تحديده؛ وتتضمن هذه الإجراءات التي أوردتها قوانين حماية البيانات الشخصية كأمثلة لمعالجة البيانات، كما تتضمن أيضًا العمليات التي قد تظهر مستقبلًا نتيجة التطور التكنولوجي، بصرف النظر عن الوسيلة المستخدمة آلية أم غير آلية، ويشمل هذا المفهوم المعالجة اليدوية البحتة، إذا كانت جزءًا من نظام لحفظ البيانات.

ويدخل في هذا مفهوم المعالجة، العمليات التي تطال إدارة شؤون الموظفين، وإدارة المرتبات، والوصول إلى قاعدة بيانات الاتصالات التي تحتوي بيانات شخصية، وإرسال رسائل البريد الإلكتروني الترويجية، وإتلاف الوثائق التي تحوي بيانات شخصية، ونشر صور أو بيانات الأشخاص على الإنترنت، وتخزين عناوين الأجهزة

---

[66] مركز بحوث القانون والتكنولوجيا. (2020). دراسة نقدية لقانون حماية البيانات الشخصية رقم (151) لسنة 2020، الجامعة البريطانية في مصر، كلية الحقوق، إشراف حسن عبد الحميد. ص: 35.

الإلكترونية (IP) أو تسجيل الفيديو والأفلام التصويرية[67]. ومما سبق نستطيع تلخيص إجراءات المعالجة الأكثر أهمية بالآتي:

1. جمع البيانات: وهي أكثر عمليات المعالجة استخدامًا، فالكثير من المؤسسات والشركات الكبرى الخاصة والهيئات الحكومية تجمع بيانات مفصّلة عن الأفراد، تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل، كما أن جمع البيانات هو إجراء ضروري في إجراءات المعالجة الأخرى للبيانات الشخصية مثل تخزينها وتحليلها والربط بينها ونقلها. وقد ذكرت محكمة العدل الأوروبية أن البيانات الشخصية المتعلقة بالدخل المكتسب وغير المكتسب وأصول الأشخاص الطبيعيين التي جمعت من المستندات المملوكة من قبل السلطات الضريبية ومعالجتها للنشر، ومن ثم نشرها في شكل قوائم مطبوعة، أو نقلها على قرص مضغوط لاستخدامها في الأغراض التجارية، أو معالجتها من أجل خدمة الرسائل النصية، حيث يمكن لمستخدمي الهاتف المحمول، عن طريق إرسال رسالة نصية تحتوي على تفاصيل عن اسم الفرد ومحل الإقامة إلى رقم معين، تلقي معلومات متعلقة بالدخل والأصول المكتسبة وغير المكتسبة لهذا الشخص تعد كلها أشكالاً لمعالجة البيانات الشخصية[68].

---

[67] الأشقر جبور؛ وجبور. (2018). مرجع سابق. ص: 89.

[68] Judgment of the Court (Grand Chamber) of 16 December 2008. (Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy). Case C-73/07. Operative part (1): " 1. Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data is to be interpreted as meaning that an activity in which data on the earned and unearned income and the assets of natural persons are: collected from documents in the public domain held by the tax authorities and processed for publication; published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists; transferred onward on CD-ROM to be used for commercial purposes, and; processed for the purposes of a text-messaging

2. تخزين البيانات: وهي الخطوة الثانية بعد عملية جمع البيانات، ويكون ذلك من خلال حفظ هذه البيانات في قاعدة بيانات إلكترونية أو غير إلكترونية؛ فمعالجة البيانات لا تقتصر فقط على الطرق الإلكترونية بل يمكن أن تقع أيضًا من خلال الطرق العادية إذا كان الأمر يتعلق بحفظ بطاقات البيانات الشخصية لأحد العملاء داخل الخزانة وكذلك ترتيبها حسب الترتيب الأبجدي؛ فكل هذه العمليات تعتبر معالجة بيانات[69]، وفي اجتهاد آخر قضت محكمة العدل أن قيام السلطات الوطنية بأخذ بصمات أصابع الشخص وتخزينها في جواز سفر ذلك الشخص يقع في إطار معالجة البيانات الشخصية[70].

3. الإفصاح عن البيانات: إنَّ الإفصاح عن البيانات الشخصية بإرسالها أو نشرها أو إتاحتها بأي طريقة أخرى يدخل في مفهوم معالجة البيانات، ويترتب على ذلك أن عملية تحميل البيانات الشخصية على صفحة الإنترنت يجب أن تعدّ معالجة للبيانات[71]. ويقصد بإتاحة البيانات الشخصية إعطاء البيانات أو تسليمها أو إبلاغها بأي

---

service whereby mobile telephone users can, by sending a text message containing details of an individual's name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person, must be considered as the 'processing of personal data' within the meaning of that provision'. Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0073&qid=1652172677513

[69] المعداوي، أحمد محمد. (2018). حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي. دراسة مقارنة. كلية الحقوق، جامعة بنها، مجلة جامعة الأزهر، مجلد 33، العدد 4، الصفحة (1926-2057)، هامش (1)، ص:1951.

[70] Judgment of the Court (Fourth Chamber) of 17 October 2013. (Michael Schwarz v Stadt Bochum). Case C-291/12. Paragraph (29): " Applying Article 1(2) of Regulation No 2252/2004 means that national authorities are to take a person's fingerprints and that those fingerprints are to be kept in the storage medium in that person's passport. Such measures must therefore be viewed as a processing of personal data". Available at:
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0291

[71] Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist. Case C-101/01 paragraph (25) "According to the definition in Article 2(b) of Directive 95/46, the term processing of such data used in Article 3(1) covers any operation or set of operations which is performed upon personal data, whether or not by automatic means. That provision gives several examples of such operations, including disclosure by

شكل من الأشكال وبأي وسيلة من الوسائل إلى شخص أو عدة أشخاص[72]، وفي هذا الإطار أقرّت محكمة العدل الأوروبية أن عملية إتاحة البيانات الشخصية على صفحة الإنترنت، إلى أشخاص مختلفين وتحديد هويتهم بالاسم أو بوسائل أخرى، عن طريق إعطاء رقم هاتفهم على سبيل المثال أو معلومات تتعلق بظروف عملهم وهواياتهم، يشكل معالجة للبيانات الشخصية[73]. فنشر البيانات الشخصية على موقع إلكتروني من صور المعالجة. وأشارت المحكمة أنّ نشاط محرك البحث الذي يتمثل في العثور على المعلومات المنشورة أو الموضوعة على الإنترنت الذي قد يقوم به شخص ما، وقدرته على إتاحة معلومات عن تفاصيل البحث تحتوي على بيانات شخصية، تعدُّ من قبيل المعالجة كما هو الحال بالنسبة لكل العمليات السابقة على الإتاحة مثل قيام محرك البحث بجمع تلك

transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

[72] المعداوي، (2018)، مرجع سابق، هامش (3)، ص:1951.

[73] Judgment of the Court of 6 November 2003. (Criminal proceedings against Bodil Lindqvist). Case C-101/01 operative part (1): " 1. The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

البيانات وتسجيلها وتنظيمها وتخزينها بصورة تلقائية ومستمرة وممنهجة[74]، وحقيقة أن هذه البيانات قد نشرت بالفعل على الإنترنت ولم يغيرها محرك البحث لا يؤثر على تصنيف هذه العملية على أنها معالجة للبيانات[75].

5. الربط أو الربط البيني: يقصد بالربط أو الربط البيني إقامة ترابط مع بيانات مدرجة في سجل أو سجلات يمسكها مسؤول أو مسؤولون عن معالجة البيانات الشخصية، أي ربط بين البيانات الشخصية المتفرقة العائدة للشخص بهدف تكوين ملف كامل عنه[76].

6. محو البيانات أو تدميرها: ويعد محو البيانات التي جُمعت سابقًا أو تدمير قواعد البيانات التي تتضمن البيانات الشخصية من أشكال المعالجة[77].

---

[74] Judgment of the Court (Grand Chamber). Of 13 May 2014. (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González). Case C-131/12. Operative part (1): " Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d)". Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

[75] Judgment of the Court (Grand Chamber). Of 13 May 2014. (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González). Case C-131/12. Previous reference paragraph (29): " Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine."

[76] التهامي، سامح عبد الواحد. (2018). نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها، دراسة في القانون الإماراتي. مجلة البحوث القانونية والاقتصادية. العدد: 6. ص: 648. المعداوي، (2018)، مرجع سابق، هامش (4)، ص:1951.

[77] التهامي، (2018). مرجع سابق. ص:648.

المطلب الثاني: أهداف حماية البيانات الشخصية

أصبحت إحدى النقاشات ذات الصلة بموضوع حماية البيانات، تدور حول الهدف من حماية البيانات، وينشأ هذا الجدل بسبب الأهداف الواسعة والغامضة للوثائق القانونية المتعلقة بحماية البيانات الشخصية، فقد جاء في اتفاقية مجلس أوروبا أنّ الهدف الأساسي من حماية البيانات الشخصية هو؛ حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين، وعلى وجه الخصوص حقهم في الخصوصية فيما يتعلق بمعالجة البيانات الشخصية[78]. وحدد التوجيه الأوروبي أهداف حماية البيانات في المادة الأولى منه بأنّها؛ حماية الحقوق والحريات الأساسية للأفراد، ولا سيما حقهم في الخصوصية؛ بالإضافة إلى منع تقييد التدفق الحر للبيانات الشخصية أو حظره بين الدول الأعضاء[79]. وذكرت اللائحة الأوروبية في المادة الأولى بأنّ حماية البيانات تهدف إلى حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين ولا سيما حقهم في حماية البيانات الشخصية؛ وعدم تقييد حرية حركة البيانات الشخصية داخل الاتحاد أو حظرها لأسباب مرتبط بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية[80].

---

[78]. اتفاقية مجلس أوروبا لحماية الأشخاص اتجاه المعالجة الآلية للبيانات الشخصية. ستراسبورغ (1981/1/28). المادة (1): الموضوع والهدف: "تهدف هذه الاتفاقية، إلى ضمان احترام الحقوق والحريات الأساسية لكل فرد كيفما كانت جنسيته أو مكان إقامته، وخاصة حقه في حياة خاصة اتجاه المعالجة الآلية للبيانات الشخصية المتعلقة به...".

[79] Directive 95/46/EC. Article (1): "1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."

[80] GDPR. Article (1): "1.This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2.This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of

ومن هذه النصوص يتضح أنّ الهدف من حماية البيانات هو ضمان مستوى مكافئ من الحماية لحقوق الأشخاص وحرياتهم من جهة، وضمان التدفق الحر للبيانات الشخصية من جهة أخرى[81]، وبالتالي تحقيق التوازن بين حماية مصلحة أصحاب البيانات من جهة، وحماية المصالح التجارية من جهة أخرى.

ومن هنا سنبحث أهداف حماية البيانات الشخصية من خلال بحث؛ ضمان تدفق البيانات الشخصية عبر الحدود (الفرع الأول)؛ وحماية الحقوق والحريات وبصورة خاصة الحق في البيانات الشخصية. (الفرع الثاني).

الفرع الأول: ضمان تدفق البيانات الشخصية عبر الحدود

يقصد بتدفق البيانات الشخصية عبر الحدود نقل البيانات الشخصية عبر الحدود الوطنية[82]. ويشكل انتقال البيانات أو تبادلها، الحركة الأهم التي تتسم بها البيانات على الإنترنت، عندما تنتقل البيانات الشخصية بين الشبكات والتطبيقات وقواعد المعلومات، وغير ذلك، من الأجهزة والبرامج، التي تعالجها لتتم عملية نقلها أو حفظها أو توزيعها، أو أية عملية أخرى من عمليات المعالجة[83].

---

personal data. 3.The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

[81] GDPR. Recital (170): "Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union…"

[82] OECD Guidelines. Article (1/C): "transborder flows of personal data" means movements of personal data across national borders."

[83] الأشقر جبور، وجبور، (2018). ص: 43.

وتعدُّ عملية تدفق البيانات الشخصية ضرورية لتوسيع التجارة الدولية والتعاون الدولي[84]، ولها دور مهم في تحقيق التنمية الاقتصادية والاجتماعية وتنمية العلاقات الاقتصادية والاجتماعية بين الدول، لذلك أكّدت تشريعات حماية البيانات على تجنب خلق عوائق غير مسوغة أمام تدفق البيانات الشخصية عبر الحدود، باسم حماية الحقوق والحريات، ولا سيما الخصوصية، قد تعرقل مثل هذه التدفقات عبر الحدود[85].

ولكن ارتباط الدول فيما بينها بمصالح والتزامات، توجب عليها انفاذ استراتيجيات وسياسات الدول، وتحقيق التوافق بين تشريعاتها الوطنية وتشريعات الدول الأخرى التي توفر حماية قانونية شاملة للبيانات الشخصية[86]. ولذلك أقرّت تشريعات حماية البيانات أنّه لا يجوز إجراء عمليات النقل إلى جهات أخرى، سواء دول أو منظمات إلا في حالة توفر شروط معينة. ومن هنا سيبحث هذا الفرع مبدأ الحماية الكافية الذي يحكم تدفق البيانات الشخصية عبر الحدود، ومن ثم سيبحث استثناءات هذا المبدأ.

أولًا: مبدأ الحماية الكافية الذي يحكم تدفق البيانات الشخصية عبر الحدود

الحق في البيانات الشخصية هو حق أساسي من حقوق الإنسان في الاتحاد الأوروبي، ومع ذلك يواجه هذا الحق تحديات جديدة كل يوم، ومن هذه التحديات تدفق البيانات الشخصية عبر الحدود. والمبدأ الرئيسي المطبق

---

[84] GDPR. Recital (101): "Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation…"

[85] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980). Last updated: 1\6\2021. Available at: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[86] فكري. (2007). مرجع سابق، ص726.

على تدفق البيانات الشخصية عبر الحدود هو مبدأ الحماية الكافية. يشير هذا المبدأ إلى أنّ نقل البيانات الشخصية إلى دولة أخرى أو منظمة دولية مسموح به فقط إذا ضُمن مستوى كافٍ من الحماية للبيانات الشخصية المنقولة، يؤمن استمرار الحماية لحقوق الأشخاص[87].

1. أهمية ضمان تدفق البيانات الشخصية عبر الحدود

قد يعود السبب لاتخاذ إجراءات دولية تتعلق بحماية البيانات الشخصية؛ إلى خشية بعض المنظمات من أن تفرض القوانين الوطنية ضوابط قوية أمام تدفق البيانات الشخصية عبر الحدود، ومن جهة أخرى إلى خشية الدول التي تبنت تشريعات لحماية البيانات، من تحايل المنظمات أو الدول التي تستقبل البيانات لمعالجتها–والتي تفرض القليل من الضوابط على أنشطة المعالجة–على القوانين والسياسات الوطنية[88]. وهذا يعني من أجل حماية البيانات لا بد من تظافر الجهود الوطنية والدولية من أجل الوصول إلى معيار موحد، يحمي حقوق الأفراد وحرياتهم من جهة أولى، ويسمح بالتدفق الحر للبيانات من أجل تعزيز التجارة الدولية من جهة ثانية.

---

[87] GDPR. Article (44): "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

[88] Lloyd, Ian. j. (2011). Information technology law. Sixth Edition. Oxford university press. United States: New York. P: 23.

فالتركيز على ضمان تدفق البيانات الشخصية عبر الحدود له ما يسوغه، في ضوء حقيقة أنّه من بين أسباب أخرى لظهور قوانين حماية البيانات في أوروبا كانت الأسباب ذات الطابع الاقتصادي في المقام الأول[89]، فالخوف من تعطّل تدفقات البيانات كان له أثر كبير في تحفيز المنظمات الدولية لاعتماد قوانين لحماية البيانات، ولا سيما إرشادات منظمة التعاون الاقتصادي والتنمية وتوجيه الاتحاد الأوروبي، فشعرت بعض الدول بالقلق، ولا سيما تلك التي التزمت بموجب معاهدة لتخفيض الحواجز الجمركية، من أنّ الدول الأخرى قد تستخدم قوانين حماية البيانات الوطنية على أنّها حواجز تجارية غير جمركية[90].

2. دور التشريعات الدولية في ضمان تدفق البيانات الشخصية عبر الحدود

أ. دور إرشادات منظمة التعاون والتنمية في ضمان تدفق البيانات الشخصية عبر الحدود: كان لإرشادات منظمة التعاون والتنمية دور مهم في ضمان تدفق البيانات الشخصية عبر الحدود، فالاتفاقية المنشئة لمنظمة التعاون الاقتصادي والتنمية كما جاء في مقدمتها، تؤمن بأنّ زيادة التوسع في التجارة العالمية هي من أهم عوامل التنمية الاقتصادية، وتحسين العلاقات الاقتصادية بين الدول[91]، فقد أُنشئت منظمة التعاون الاقتصادي والتنمية أساسًا من

[89] Bygrave, Lee. A. (2014). Data privacy law: An international perspective. Oxford university press. First Edition. United States of America: New York. P: 9-15.

[90] Bygrave. (2014). Previous reference. P: 45.

[91] Convention on the Organization for Economic Co-operation and Development, PARIS 14th December 1960, "RECOGNISING that the further expansion of world trade is one of the most important factors favouring the economic development of countries and the improvement of international economic relations". Last updated: 9/9/2021. Available at: https://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm

أجل التعاون بين الدول الأعضاء، لتعزيز السياسات الهادفة إلى تحقيق أعلى نمو اقتصادي وعمالة مستدامين، ورفع مستوى المعيشة في الدول الأعضاء، والتوسع الاقتصادي في دول العالم، وتوسيع التجارة العالمية[92].

كما لاحظت منظمة التعاون الاقتصادي والتنمية، أن المخاوف الجديدة المتعلقة بتطوير المعالجة الآلية البيانات، مع القدرة على نقل كمية كبيرة من البيانات في غضون ثوانٍ، قد دفعت الدول الأعضاء إلى إصدار قوانين لمنع ما يعّد انتهاكًا لحقوق الإنسان الأساسية، مثل التخزين غير القانوني للبيانات الشخصية، وتخزين البيانات الشخصية غير الدقيقة، أو حتى إساءة استخدام هذه البيانات أو الكشف عنها بشكل غير مصرح به[93]، وتباين الحماية في التشريعات الوطنية يمكن أن تعيق التدفق الحر للبيانات الشخصية عبر الحدود، الذي ينمو بسرعة مع الإدخال الواسع لتكنولوجيا الكمبيوتر والاتصالات الجديدة، لذلك رأت منظمة التعاون الاقتصادي والتنمية أنّه يجب القضاء على عوائق التدفقات والقيود التي يسببها التباين في القوانين الوطنية، الذي قد يؤدي إلى اضطراب خطير في الاقتصاد، لذلك يجب على الدول الأعضاء في المنظمة إزالة العقبات غير المسوغة لتدفقات البيانات الشخصية

---

[92] Convention on the Organization for Economic Co-operation and Development, PARIS 14th December 1960. Article 1: "The aims of the Organisation for Economic Co-operation and Development (hereinafter called the "Organisation") shall be to promote policies designed: (a) to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy; (b) to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and (c) to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations."

[93] Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980). Last updated: 1\6\2021. Available at: https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation

عبر الحدود باسم حماية الخصوصية أو تجنبها، ويجب وضع مبادئ توجيهية من شأنها أن تساعد على مواءمة التشريعات الوطنية، وفي الوقت الذي تدعم فيه حقوق الإنسان، لا تمنع من انقطاع التدفقات الدولية للبيانات[94].

توضح المناقشة أعلاه أنّ الهدف الرئيسي لمنظمة التعاون الاقتصادي والتنمية من تنظيم حماية البيانات الشخصية، هدف اقتصادي بالدرجة الأولى، من خلال تعزيز التدفق الحر للبيانات الشخصية عبر الحدود، وهذا ليس مفاجئًا فمنظمة التعاون الاقتصادي والتنمية أُنشئت أساسًا بهدف تسهيل التعاون بين الدول الأعضاء من أجل تعزيز التنمية الاقتصادية.

ب. دور توجيه الاتحاد الأوروبي في ضمان تدفق البيانات الشخصية عبر الحدود: كان لتوجيه الاتحاد الأوروبي أيضًا دور مهم في ضمان تدفق البيانات الشخصية عبر الحدود، وذلك لأنّ الاتحاد الأوروبي أنشئ في الأصل على أنه مؤسسة للتكامل الاقتصادي بين أسواق دول الاتحاد، وبالتالي فإن اختصاصها في التشريع في مجال حقوق الإنسان ملتبس، لذلك يرى البعض أنّ هدف التوجيه من تنظيم حماية البيانات الشخصية اقتصادي بالدرجة الأولى أكثر منها لحماية حقوق الإنسان[95]، كما أنّ التوجيه يركز كثيرًا على التسويق بدلاً من حماية حقوق الإنسان، وهو ما نلمحه في الحيثية (3) من التوجيه، التي أفادت أن إنشاء سوق داخلي وتشغيله لا يتطلب فقط ضمان حرية حركة السلع والأشخاص والخدمات ورؤوس الأموال، وحرية تدفق البيانات الشخصية إنما لا بد أيضًا من حماية

[94] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980). Previous reference.

[95] Fuster, Gloria. G. (2014). The emergence of personal data protection as a fundamental right of the EU. Law, Governance and Technology Series. Springer International Publishing Switzerland. Volume 16. P. 164.

الحقوق الأساسية للأفراد[96]. وتشير الحيثية (2) من التوجيه إلى دور معالجة البيانات الشخصية في خدمة الإنسان وإحراز التقدم الاقتصادي والاجتماعي والتوسع التجاري ورفاهية الأفراد[97]، وأيضًا تشير الحيثية (56) إلى أن تدفق البيانات الشخصية عبر الحدود ضرورية في توسيع التجارة الدولية، وأن احترام حقوق الأشخاص وحرياتهم لا تقف في طريق نقل البيانات الشخصية إلى دول ثالثة تضمن مستوى مناسبًا من الحماية[98]، مما قد يخلق انطباعًا بأن جدول الأعمال التجاري للتوجيه هو الأبرز. لذلك يمكن القول بأن توجيه الاتحاد الأوروبي من حيث المبدأ قائم على الحقوق، على الأقل لأنّ أصوله تشمل المادة (8) من الاتفاقية الأوروبية لحقوق الإنسان، والحق في احترام الخصوصية، ولكن من الناحية العملية، فإن حماية البيانات في التوجيه تتعلق بتنظيم تدفق البيانات أكثر من حماية حقوق الأفراد[99].

---

[96] Directive 95/46/EC. Recital (3): "Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."

[97] Directive 95/46/EC. Recital (2): "Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals."

[98] Directive 95/46/EC. Recital (56): "Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations."

[99] Bernal, Paul. (2014). Internet privacy right, right to protect autonomy. First Edition. Cambridge University Press. New York. P: 223.

ج. دور لائحة الاتحاد الأوروبي في ضمان تدفق البيانات الشخصية عبر الحدود: على الرغم من أن لائحة الاتحاد الأوروبي لحماية البيانات الشخصية تركز بشكل أكبر على حقوق الأفراد، وتحترم حقوقهم وحرياتهم الأساسية، ولا سيما حقهم في حماية البيانات الشخصية فيما يتعلق بمعالجة بياناتهم الشخصية، إلا أنّها لا تزال تركز على الدور الاقتصادي للبيانات أكثر من تركيزها على حقوق الأفراد، وهو ما نلمحه في الحيثية (2) التي أكدت على أنّ الغرض من اللائحة هو تحقيق مجال للحرية والأمن والعدالة والاتحاد الاقتصادي، والتقدم الاقتصادي والاجتماعي، وتعزيز وتلاقي الاقتصادات داخل السوق الداخلية، وتحقيق الرفاه للأشخاص الطبيعيين[100].

كما أشارت الحيثية (7) إلى أن التحديات الجديدة التي جلبتها التطورات التكنولوجية السريعة تطلبت وجود إطار قانوني قوي وأكثر تماسكًا لحماية البيانات الشخصية، نظرًا لأن الثقة في الاقتصاد الرقمي ستسمح له بالتطور، لذلك يجب تمكين الأشخاص الطبيعيين من التحكم في بياناتهم الشخصية[101]، ومن أجل ضمان مستوى عالٍ من الحماية للأشخاص الطبيعيين، ولإزالة العقبات التي تعترض تدفق البيانات الشخصية داخل الاتحاد، يجب أن يكون

---

[100] GDPR. Recital (2): "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."

[101] GDPR. Recital (7): "Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced."

مستوى حماية حقوق وحريات الأشخاص الطبيعيين فيما يتعلق بمعالجة هذه البيانات متماثلًا في جميع الدول الأعضاء كما أشارت الحيثية (10)[102].

ونصت الحيثية (9) بأنه الاختلاف في مستوى حماية حقوق الأشخاص الطبيعيين وحرياتهم، ولا سيما الحق في حماية البيانات الشخصية، فيما يتعلق بمعالجة البيانات الشخصية في الدول الأعضاء، يعود إلى وجود الاختلاف في تنفيذ وتطبيق التوجيه 46/95 / EC، وهذ الاختلاف سيؤدي إلى منع التدفق الحر للبيانات الشخصية في جميع أنحاء الاتحاد، وقد يشكل ذلك عقبة أمام متابعة الأنشطة الاقتصادية على مستوى الاتحاد ويشوه المنافسة[103]. وكذلك أكدت الحيثية (6) على أنّ التحول الذي أحدثته التكنولوجيا في الاقتصاد والحياة الاجتماعية، يجب أن يسهّل التدفق الحر للبيانات الشخصية داخل الاتحاد ونقلها إلى دول ثالثة ومنظمات دولية، لكن يجب ضمان مستوى عال من حماية البيانات الشخصية[104].

---

[102] GDPR. Recital (10): "In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. …".

[103] GDPR. Recital (9): "The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC."

[104] GDPR. Recital (6): "Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data."

وبحسب اللائحة الأوروبية يجوز للمفوضية الأوروبية أن تتخذ قرارًا، بأثر سارٍ بالنسبة للاتحاد بأكمله، أنّ دولة ثالثة أو إقليمًا أو قطاعًا محددًا أو منظمة دولية، توفر مستوىً كافيًا من الحماية للبيانات، مما يوفر اليقين القانوني والتوحيد في جميع دول الاتحاد، بأن الدولة الثالثة أو المنظمة الدولية توفر المستوى المطلوب من الحماية، وفي هذه الحالة لا تحتاج عملية نقل البيانات إلى إذن آخر، كما يجوز لها إلغاء هذا القرار بعد تقديم إشعار وبيان كامل يوضح الأسباب[105]. في حين اشترط المشرع المصري بالإضافة إلى توافر الحماية الكافية في الدولة المعنية بتلقي البيانات، أخذ ترخيص أو تصريح بنقل البيانات من السلطة الوطنية المختصة بحماية البيانات[106].

وبحسب اللائحة فإنّ تقويم كفاية مستوى الحماية في الدولة المعنية بتلقي البيانات، يتم بناءً على مؤشرات تتعلق بالنظام القانوني المعتمد، ومدى احترامه لحقوق الإنسان، سواء أكان ذلك في القوانين العامة أم القوانين الخاصة بقطاعات معينة، بما فيها أنظمة الدفاع، والأمن العام، والقوانين الجزائية، وحق السلطات العامة في الوصول إلى البيانات الشخصية، وشروط إعادة نقل البيانات إلى بلد ثالث آخر، أو منظمة دولية، والحقوق التي

---

[105] GDPR. Recital (103): "The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision."

[106] قانون حماية البيانات المصري. المادة (14): "يحظر إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية أو تخزينها أو مشاركتها إلا بتوفر مستوى من الحماية لا يقل عن تلك المنصوص عليها في هذا القانون، وبترخيص أو تصريح من المركز".

يمكن الاعتداد بها، من قبل الأشخاص المعنيين بالبيانات المنقولة، وسبل المراجعة القضائية والإدارية، التي يمكن أن يلجأ إليها المعنيون بالبيانات[107].

وأيضًا من المؤشرات على وجود أطر قانونية مناسبة للحماية، وجود سلطة مستقلة معنية بحماية البيانات الشخصية، لها القدرة على ممارسة صلاحيات فاعلة تضمن تطبيق قوانين الحماية، ومساعدة الأشخاص المعنيين وتوجيههم في كيفية ممارسة حقوقهم[108]. ويجب أن تراقب المفوضية عمل القرارات المتعلقة بمستوى الحماية، وينبغي أن تنص في قراراتها المتعلقة بالكفاية على آلية مراجعة دورية لأداء هذه الهيئات، بالتشاور مع البلد الثالث أو المنظمة الدولية المعنية[109].

---

[107] GDPR. Article (45/2/a): "2.When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements: (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred."

[108] GDPR. Article (45/2/b & c): (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

[109] GDPR. Recital (106): "The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organization…In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation…"

ثانيًا: الاستثناءات على مبدأ الحماية الكافية الذي يحكم تدفق البيانات الشخصية عبر الحدود.

مع أنّ تدفق البيانات الشخصية مطلب ضروري لتوسيع التجارة الدولية والتعاون الدولي، ولكن الزيادة في تدفق البيانات عبر الحدود أدّت إلى ظهور تحديات ومخاوف جديدة، تتعلق بحماية الحق في البيانات الشخصية، لذلك؛ عند نقل البيانات الشخصية لا ينبغي تقويض مستوى حماية الأشخاص الطبيعيين، ولا يجوز إجراء عمليات النقل من دول الاتحاد الأوروبي إلى دول أخرى أو منظمات دولية إلا في حالة الامتثال للقواعد المتعلقة بحماية البيانات[110]. وفي حالة عدم توافر مستوى من الحماية لحقوق وحريات الأفراد في الدولة المعنية بتلقي البيانات، لا يقل عن تلك المنصوص عليها في قانون الاتحاد الأوروبي، لا يجوز نقل البيانات الشخصية إلا بتوافر استثناءات خاصة في حالات معينة.

1. المبدأ العام حظر إجراء عمليات نقل للبيانات الشخصية إلى الدول التي لم تستوفِ متطلبات مبدأ الحماية الكافية.

[110] GDPR. Recital (101): "Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor"

في حالة عدم توافر مستوى من الحماية لحقوق الأفراد وحرياتهم في الدولة المعنية بتلقي البيانات، لا يقل عن تلك المنصوص عليها في قانون دول الاتحاد الأوروبي، وبالتالي لم تستوفِ متطلبات نقل البيانات الضمانات الكافية، لا يجوز نقل البيانات الشخصية إلا بتوافر استثناءات خاصة بحالات محددة على سبيل الحصر. وفي هذه الحالة، ينبغي النص على إجراء مشاورات بين المفوضية وتلك الدول الثالثة أو المنظمات الدولية. ويجب على المفوضية إبلاغ الدولة الثالثة أو المنظمة الدولية بالأسباب والدخول في مشاورات معها من أجل تصحيح الوضع في الوقت المناسب[111].

ويجب على المتحكم أو المعالج اتخاذ تدابير للتعويض عن نقص حماية البيانات في الدولة المعنية بتلقي البيانات عن طريق الضمانات المناسبة لصاحب البيانات، ويجب أن تتضمن هذه الضمانات الامتثال لمتطلبات حماية البيانات وحقوق الأشخاص المعنيين بالبيانات، بما في ذلك توافر حقوق أصحاب البيانات القابلة للتنفيذ وسبل الانتصاف القانونية الفعّالة، بما في ذلك الحصول على تعويض إداري أو قضائي فعّال والمطالبة بالتعويض، كما يجب أن تتعلق الضمانات بشكل خاص بالامتثال للمبادئ العامة المتعلقة بمعالجة البيانات الشخصية، كما يمكن أيضًا إجراء عمليات النقل من قبل السلطات أو الهيئات العامة مع السلطات أو الهيئات العامة في بلدان

[111] GDPR. Recital (107): "The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation."

أخرى أو مع المنظمات الدولية ذات الواجبات أو الوظائف المقابلة، بما في ذلك على أساس الأحكام التي ستدرج في الترتيبات الإدارية، مثل مذكرة التفاهم، التي تنص على الحصول على حقوق واجبة التنفيذ وفعالة لأصحاب البيانات[112].

2. حالات نقل البيانات الشخصية إلى الدول التي لم تستوفِ متطلبات مبدأ الحماية الكافية.

سمحت قوانين حماية البيانات في حالات محدده على سبيل الحصر نقل البيانات الشخصية عبر الحدود، في حال عدم توافر مستوى من الحماية القانونية والضمانات المناسبة. وهذه الحالات حسب اللائحة هي؛ حالة الموافقة الصريحة للشخص المعني بالبيانات بعد إبلاغه بالمخاطر المحتملة لعمليات النقل بسبب عدم وجود حماية وضمانات مناسبة[113]، أو إذا كان النقل ضروريًا لحماية المصالح الحيوية لصاحب البيانات أو الأشخاص الآخرين،

[112] GDPR. Recital (108): "In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding."

[113] GDPR. Article (49/1/a): "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards".

حيث يكون صاحب البيانات غير قادر جسديًا أو قانونيًا على منح الموافقة[114]، أو المحافظة على حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له[115]. أو إذا كان نقل البيانات ضروريًا لإبرام عقد بين صاحب البيانات والمتحكم أو تنفيذ التدابير التعاقدية المسبقة المتخذة بناءً على طلب صاحب البيانات، أو لإبرام عقد، أو تنفيذ عقد مبرم بالفعل لمصلحة صاحب البيانات بين المتحكم وشخص طبيعي أو اعتباري آخر[116]. أو كان النقل ضروريًا لأسباب تتعلق بحماية المصلحة العامة[117]. أو كان النقل ضروريًا لإقامة الدعاوى القانونية أو ممارستها أو الدفاع عنها[118].

ونص المشرع المصري على أنّه في حال عدم توافر مستوى من الحماية القانونية والضمانات المناسبة، يجوز استثناءً نقل البيانات الشخصية عبر الحدود وذلك في حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه في نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة لا يتوفر فيها مستوى الحماية إذا ترافقت مع إحدى الحالات الآتية وهي؛ المحافظة على حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له[119]؛ أو تنفيذ التزامات بما يضمن اثبات حق أو ممارسته أمام العدالة أو

---

[114] GDPR. Article (49/1/f): "the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent"

[115] قانون حماية البيانات المصري. المادة (1/15).

[116] GDPR. Article (49/1/b & c): "(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person".

[117] GDPR. Article (49/1/d): "the transfer is necessary for important reasons of public interest".

[118] GDPR. Article (49/1/e): "the transfer is necessary for the establishment, exercise or defence of legal claims"

[119] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020. المادة (1/15).

الدفاع عنه[120]؛ أو إبرام عقد، أو تنفيذ عقد مبرم بالفعل أو سيتم إبرامه بين المسؤول عن المعالجة والغير، وذلك لمصلحة الشخص المعني بالبيانات[121]؛ أو تنفيذ إجراء خاص بتعاون قضائي دولي[122]؛ أو وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة[123]؛ أو عند إجراء تحويلات نقدية إلى دولة أخرى وفقا لتشريعاتها المحددة والسارية[124]؛ أو إذا كان النقل أو التداول يتم تنفيذا لاتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفًا فيه[125].

3. النتائج المترتبة على عدم استيفاء متطلبات مبدأ الحماية الكافية، أو استثناءات تسمح بنقل البيانات.

أدى الاختلاف في تنظيم حماية البيانات، إلى تهديد الاتحاد الأوروبي، بحظر انتقال البيانات الشخصية، إلى البلاد التي لا تؤمن معايير حماية كافية كتلك القائمة في الاتحاد الأوروبي، الأمر الذي نتج عنه مشاورات بين وزارة التجارة الأمريكية واللجنة الأوروبية، لإيجاد آلية تسهل عملية الانتقال هذه، فكانت اتفاقية الملاذ الآمن، بموجب قرار المفوضية الأوروبية رقم (EC/520/2000)[126]. وبعد أن تبيّن قصور هذه الاتفاقية عن تأمين الحماية اللازمة للبيانات العابرة للحدود، وحماية الحقوق الأساسية للأفراد في الاتحاد الأوروبي، أصدرت محكمة العدل في الاتحاد

[120] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020. المادة (2/15).
[121] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020. المادة (3/15).
[122] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020. المادة (4/15).
[123] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020. المادة (5/15).
[124] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020. المادة (6/15).
[125] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020. المادة (7/15).
[126] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. (2000/520/EC). Available At: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520

الأوروبي (CJEU) حكمها بأنّ قرار المفوضية الأوروبية رقم (EC/520/2000) المُنشئ لاتفاقية الملاذ الآمن بين الاتحاد الأوروبي والولايات المتحدة باطل وذلك بالحكم الصادر بتاريخ (2015/10/6)[127].

وفي إطار السعي لدعم التجارة عبر الحدود، وحماية الحقوق الأساسية للأفراد، وقّع الاتحاد الأوروبي والولايات المتحدة على اتفاقية جديدة لنقل البيانات عبر الحدود، بموجب قرار المفوضية الأوروبية رقم (1250/2016)[128]، وهي اتفاقية درع الخصوصية، التي تقضي بتزويد الشركات بآلية تساعد على الامتثال لمتطلبات حماية البيانات المنصوص عليها في اللائحة الأوروبية، عند نقل البيانات من جهة ومعالجتها، كما يضمن استمرار توافر المستوى المطلوب من الحماية[129]. ولكن بتاريخ (2020/7/16)، أبطل حكم محكمة العدل الأوروبية اتفاقية درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة الأمريكية، وأوضحت المحكمة في حكمها أنّ قرار المفوضية الأوروبية رقم (1250/2016) المنشئ لدرع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة باطل[130].

---

[127] Judgment of the court (Grand Chamber). Of 6 October 2015. (Maximillian Schrems v Data Protection Commissioner). ('Schrems I'). Case C-362/14. Operative part (2): "Decision 2000/520 is invalid". Available At:
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362

[128] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Available At:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

[129] الأشقر جبور، وجبور. (2018). مرجع سابق، ص: 103.

[130] Judgment of the court (Grand Chamber). Of 16 July 2020. (Data Protection Commissioner V Facebook Ireland Limited and Maximillian Schrems). ('Schrems II'). Case C-311/18. Operative part (5): " Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid". Available At:

الفرع الثاني: حماية الحقوق والحريات وبصورة خاصة الحق في البيانات الشخصية

مما لا شك فيه أنّ إحدى المحركات الأولية لتنظيم معالجة البيانات الشخصية كانت تجارية أو ذات صلة بالأعمال التجارية، ومع تزايد حجم البيانات الشخصية، استمرت في جذب المزيد من الاهتمام وتزايدت الحاجة إليها في مجال الأعمال التجارية الداخلية والدولية، ولكن هناك الكثير من الحجج المؤيدة لحقيقة؛ أنّ حماية البيانات ونظام الاتحاد الأوروبي يستندان على الحقوق على الأقل في الآونة الأخيرة[131]؛ وأنّ حماية البيانات تعتمد اعتماداً كبيراً على وثائق حقوق الإنسان، فحماية البيانات إحدى المجالات الرئيسية للمنظمات الدولية، التي تقوم وظيفتها الأساسية على حماية حقوق الإنسان، فقد صاغت الأمم المتحدة ومجلس أوروبا صكوكًا بشأن حماية البيانات بناءً على اختصاصهما بتعزيزها حقوق الإنسان[132].

ومما يزيد من تعزيز الحجة القائلة بأن حماية البيانات تهدف لحماية الحقوق، وجود دعوات إلى وضع إطار قانوني دولي لحق الإنسان في الخصوصية وحماية البيانات تحت مظلة الأمم المتحدة، الأمر الذي كان جزءًا من مناشدة إعلان مونترو، الذي وجه نداء إلى الأمم المتحدة لإعداد صك قانوني ملزم، يحدد بوضوح وبالتفصيل الحق في حماية البيانات والحق في الخصوصية بوصفهما من الحقوق الإنسانية واجبة الإنفاذ[133]. ويمكننا القول

https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2789(RSP)

[131] Lynskey, Orla. (2013). From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis. Editors: Serge Gutwirth, Ronald Lee Nes, Paul de Hert, Yves Poulet. European Data Protection: Coming of Age. P: 73.

[132] Kuner, Christopher. (2009). An international legal framework for data protection: Issues and prospects. Computer Law & Security Review. P: 309.

[133] Montreux Declaration. (14- 16 September 2005). The protection of personal data and privacy in a globalized world: a universal right respecting diversities. "a. to the United Nations to prepare a legal binding instrument

إن حماية البيانات تحمي الحقوق، لأنّها تطورت من الصكوك التي تُعنى بحماية حقوق الإنسان، فهدف حماية البيانات بتعزيز التدفق الحر للبيانات عبر الحدود لا يمكنه إنكار هدفها بحماية الحقوق.

ولكن هدف من حماية البيانات الشخصية في حماية حقوق الأفراد وحرياتهم، يثير التساؤل عن ماهية الحق الذي تحميه القواعد القانونية المنظمة لموضوع الحماية، وعن علاقته بحماية الحقوق والحريات الأخرى، فهل حماية البيانات الشخصية تقع ضمن إطار حماية الخصوصية، وبالتالي تكون فئة فرعية من الخصوصية، أم أنّها حق مستقل عن الحق في الخصوصية وإن كانت كذلك فما أهمية الاعتراف بحماية البيانات الشخصية على أنه حق مستقل. وهذا ما سوف يُعرض فيما يأتي.

أولًا: التمييز بين الحق في البيانات الشخصية والحق في الخصوصية

من المسلم به أنّ حقوق الإنسان وحرياته مترابطة فيما بينها، وبالتالي فإنّ أي انتهاك لحق من الحقوق يشكل انتهاكًا للحقوق والحريات الأُخرى. وبناءً على ذلك فإن الهدف من القوانين التي تحمي حقوق الإنسان، مثل قوانين حماية البيانات، هو أولًا وقبل كل شيء حماية حقوق الأفراد وحرياتهم، ولذلك فمن المنطقي لضمان ذلك أن تُحترم حقوق جميع الأشخاص بغض النظر عن ماهية الجهات التي تعالج بياناتهم[134]. فالحقوق والحريات يمكن

which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'. Last updated: 9/9/2021. Available at: https://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf

[134] أكسس ناو. (2018). دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الأوروبي. مرجع سابق. ص: 5.

أن تتأثر نتيجة جمع البيانات، أو جمعها بطريقة عشوائية وغير منظمة وخارج الأطر القانونية الملائمة، أو نتيجة لانكشاف البيانات التي عولجت، أو وقوعها بين أيدي أشخاص غير مناسبين[135].

وبالتالي تحاول قوانين حماية البيانات التوفيق بين القيم الأساسية ولكن المتضاربة مثل الخصوصية، والتدفق الحر للمعلومات، والحاجة إلى المراقبة الحكومية، وتحديد الضرائب، وما إلى ذلك، وموازنة مصالح أصحاب المصلحة من أفراد وشركات وحكومات مع بعضها. فحماية البيانات مهمة ليس فقط لإبقاء الأفراد أو الشركات التجارية التي تقوم بمعالجة البيانات خاضعة للمساءلة، وإنما أيضًا لإبقاء الحكومات منفتحة وخاضعة للمساءلة، من خلال السماح للمواطنين بقدر من السيطرة على معلوماتهم الشخصية التي تحتفظ بها حكوماتهم، ومعرفة أغراض استخدامها[136].

1. العلاقة بين الحق في البيانات الشخصية والحق في الخصوصية

لقد حظي الحق في الخصوصية بالحماية في الإعلان العالمي لحقوق الإنسان لعام (1948)[137]، بنص المادة (12)[138]، ولم يذكر الإعلان وسيلة التعرض للحياة الخاصة والبيانات المتعلقة بالحياة الخاصة، وبذلك يستوي أن تكون وسيلة تقليدية أو إلكترونية. كما أكدت المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية

---

[135] الأشقر جبور، جبور. (2018). مرجع سابق. ص: 29-30.

[136] Stefanick. (2011). Previous reference. P: 43.

[137] الإعلان العالمي لحقوق الإنسان، الذي اعتمد وصدر رسمياً بقرار الجمعية العامة ٢١٧ ألف (د-٣) بتاريخ (1948/12/10). متاح على الموقع الآتي: http://hrlibrary.umn.edu/arab/b001.html

[138] المادة (12) من الإعلان العالمي لحقوق الإنسان:" لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات".

1966[139]، على ما جاء في المادة (12) من الإعلان العالمي لحقوق الإنسان[140]. وجاء في الفقرة (1) من التعليق[141] العام رقم (16) الصادر عن اللجنة المعنية بحقوق الإنسان المدنية والسياسية[142] في الأمم المتحدة، أنّه وفقًا للمادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية، فإنَّ هناك حقًا لكل شخص في عدم التعرض على نحو تعسفي أو غير قانوني لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، أو لأي حملات غير قانونية تمس بشرفه أو سمعته. كما جاء في الفقرة (8) من التعليق أنّه يتوجب ضمان سلامة المراسلات وسريتها، وينبغي حظر الرقابة بالوسائل الإلكترونية أو بغيرها على السواء، وحظر اعتراض طريق الاتصالات الهاتفية والبرقية وغيرها من أشكال الاتصالات، والتنصت على المحادثات وتسجيلها.

والنقطة المهمة التي ذكرتها اللجنة، وردت في الفقرة (10) من تعليقها، ضمّنت البيانات الشخصية في نطاق الخصوصية، وذكر فيها بأنّه يجب أن ينظم القانون عمليات جمع المعلومات الشخصية وحفظها باستخدام الحاسوب وبنوك البيانات وغيرها من الوسائل، سواء أكانت تجريها السلطات العامة أم الأفراد العاديون أو الهيئات الخاصة. ويتعين أن تتخذ الدول تدابير فعّالة لكفالة عدم وقوع المعلومات المتعلقة بالحياة الخاصة للشخص في

---

[139] العهد الدولي الخاص بالحقوق المدنية والسياسية الذي اعتمد وفتح باب التوقيع والتصديق عليه والانضمام إليه بقرار الجمعية العامة 2200 ألف (د-21) بتاريخ (1966/12/16). متاح على الموقع الآتي: http://hrlibrary.umn.edu/arab/b003.html

[140] المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية: "1-لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني لتدخل في خصوصياته أو شؤون أسرته أو بيئته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. 2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس".

[141] تعليق اللجنة المعنية بالحقوق المدنية والسياسية رقم (16)، على المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية الدورة الثانية والثلاثون (1988)، التعليق العام رقم 16، متاح على الموقع الآتي: http://hrlibrary.umn.edu/arabic/hrc-gc16.html

[142] وهي لجنة فنية تعمل ضمن منظومة الأمم المتحدة منذ 1946، كانت عبارة عن هيئة فرعية للمجلس الاقتصادي والاجتماعي للأمم المتحدة، وكانت المفوضية السامية للأمم المتحدة لحقوق الإنسان (وهي الهيئة الرئيسة التابعة إلى الأمم المتّحدة المعنيّة بحقوق الإنسان) تساعدها في عملها، وفي 15 آذار عام 2006، صوتت الجمعية العامة للأمم المتحدة بأغلبية ساحقة على قرار الجمعية العامة للأمم المتحدة، ليحل مجلس حقوق الإنسان محل لجنة حقوق الإنسان المنتهية ولايتها وتأسيس مجلس حقوق الإنسان الذي يعد سلطة أعلى في نظام الأمم المتحدة نظراً لتبعيته المباشرة للجمعية العامة. لمزيد من التفاصيل زيارة الموقع الآتي:
https://www.ohchr.org/AR/HRBodies/Pages/HumanRightsBodies.aspx

أيدي الأشخاص الذين لا يجيز لهم القانون الحصول عليها أو معالجتها أو استخدامها. ولكي يتسنى حماية الحياة الخاصة للفرد على أكفأ وجه، ينبغي أن يكون من حق كل فرد التحقق مما إذا كانت هناك بيانات شخصية مخزنة في ملفات البيانات الآلية، وماهية هذه البيانات، والغرض من الاحتفاظ بها. كما ينبغي أن يكون بمقدور كل فرد التحقق من هوية السلطات العامة أو الأفراد العاديين أو الهيئات الخاصة التي تتحكم أو قد تتحكم في هذه الملفات. وإذا كانت الملفات تتضمن بيانات شخصية غير صحيحة أو بيانات جمعت أو عولجت بطريقة تتعارض مع أحكام القانون، ينبغي أن يكون من حق كل فرد أن يطلب تصحيحها أو حذفها.

هذا التوسع في التعليق على المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية، يفتح المجال أمام كل الظواهر الجديدة التي لم تكن ملحّة في وقت صدور الإعلان والعهد الدولي، ومنها الاعتداءات الواقعة عبر شبكة الإنترنت على الحق في الخصوصية، ويساير الاتجاه القائل بأنّ حماية البيانات تتعلق بصورة رئيسية بحماية الحياة الخاصة، لكنه من جهة أُخرى يُظهر أنّ الحق في الخصوصية في القانون الدولي لحقوق الإنسان يتضمن المبادئ الأساسية لحماية البيانات[143].

ومراعاة من أعضاء مجلس أوروبا للإعلان العالمي لحقوق الإنسان وحرياته الأساسية، ولتحقيق اتحاد فعلي بين أعضاء مجلس أوروبا بالتأكيد على مفهوم واحد مشترك لحقوق الإنسان التي تنادي بها، وقّعت الدول الأعضاء في مجلس أوروبا على الاتفاقية الأوروبية لحقوق الإنسان وحرياته الأساسية لعام 1950[144]، وقد أدّت

---

[143] Bygrave, Lee. A. (1998). Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. International Journal of Law and Information Technology. Volume 6. P: 249-250.

[144] الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، روما، الصادرة بتاريخ (1950/11/4). متاحة على الموقع الآتي:
https://www.echr.coe.int/Documents/Convention_ARA.pdf

دوراً مهمًا في تطوير الوعي وحماية حقوق الإنسان في جميع أنحاء أوروبا، وأكد المجلس في المادة (8) من الاتفاقية على وجوب احترام خصوصية الأفراد وحماية هذا الحق من التدخل والاعتداء[145].

وقد فسّرت المحكمة الأوروبية لحقوق الإنسان هذه المادة على نطاق واسع، بحيث شملت في نطاقها البيانات الشخصية، وذلك بسبب التجربة الأوروبية مع الحكومات الفاشية والنازية خلال حقبة الحرب العالمية الثانية، والأعمال الوحشية نتيجة الاستخدام غير الخاضع للرقابة للبيانات الشخصية التي كشفت عن العرق والتوجهات الجنسية والسياسية، الأمر الذي أدى إلى توعية الأوروبيين بأهمية حماية البيانات الشخصية، وتطوير إرشادات صارمة لمعالجة البيانات[146].

وفي ذات سياق النصوص القانونية المذكور آنفًا، وبالنظر إلى نطاق الحق في الخصوصية الذي يزداد اتساعًا، فقد فُسِّر أنّ الحق في الخصوصية يغطي التحديات الناشئة المتعلقة بمعالجة البيانات الشخصية[147]، لذلك فإن العديد من الباحثين ينظرون إلى حماية البيانات الشخصية على أنّها فئة فرعية من الخصوصية ضمن ما يطلق علية خصوصية المعلومات، ويرى هذا الاتجاه أنّ مفهوم الخصوصية تطور تبعًا للتطور التكنولوجي وهو يشمل حماية الشخص من كافة أوجه الاعتداءات والتدخل في حياته أيًا كانت طبيعتها؛ ولا يقتصر على الخصوصية المادية التي تعطي الشخص الحق في حماية جسده ومسكنه ومراسلاته ووثائقه وكل ما يتعلق به من الناحية المادية

---

[145] نصت المادة (8)، الحق في احترام الحياة الخاصة والعائلية: "1-لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته.2-لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقاً للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم".

[146] Stefanick. (2011). Previous reference. p. 45.

[147] Fuster. (2014). Previous reference. P: 94-97.

من أنشطة التفتيش أو أية إجراءات ماسة بجسده كفحوص الجينات وفحص المخدرات؛ والخصوصية المعنوية تعطي الشخص الحق في حماية أسراره من أنشطه الرقابة والتجسس والتنصت؛ وخصوصية الاتصالات التي تشمل في مفهومها التقليدي كافة أنواع المراسلات والاتصالات العادية كالهاتف والبريد وغيرها، وتغطي في تطورها الراهن سرية وخصوصية المراسلات الإلكترونية والبريد الإلكتروني وغيرها من وسائل الاتصال في البيئة الرقمية؛ وإنما تتضمن أيضًا خصوصية المعلومات، التي تعطي الشخص الحق في حماية معلوماته الشخصية والسيطرة عليها، وتتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة به وهي المعبّر عنها باصطلاح حماية البيانات، هذا المفهوم الجديد للخصوصية ارتبط بأثر التقنية وتحديات العصر الرقمي على الحياة الخاصة[148].

ويرى هذا الاتجاه، أنّ هناك ترادفًا بين خصوصية البيانات الشخصية أو خصوصية المعلومات وبين حماية البيانات، وأنّ استخدام اصطلاح الخصوصية في بيئة الإنترنت ومسائل عقود التقنية أو خدمات التقنية عمومًا يُشار إليه بحماية الخصوصية المعلوماتية أو حماية البيانات[149]، وبالتالي فإنّ حماية البيانات والمعلومات الشخصية تمثّل عنصرًا أساسيًا من عناصر الحياة الخاصة، ونطاق الحق في الخصوصية يشمل حماية البيانات والمعلومات الشخصية، بالرغم من تأييده عدم دخول جميع البيانات الشخصية في نطاق الحق في الحياة الخاصة[150].

---

[148] أيوب، بولين أنطونيوس. (2009). الحماية القانونية للحياة الشخصية في مجال المعلوماتية. دراسة مقارنة. الطبعة الأولى. بيروت: لبنان. منشورات الحلبي الحقوقية. ص: 66-67.

[149] الموسوي، منى تركي، وفضل الله، جان سيريل. (2013). الخصوصية المعلوماتية وأهميتها ومخاطر التقانات الحديثة عليها. مجلة كلية بغداد للعلوم الاقتصادية. العدد الخاص بمؤتمر الكلية. مركز بحوث السوق وحماية المستهلك. جامعة بغداد. ص: 306-307.

[150] داود، إبراهيم. (2017). الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية، دراسة تحليلية مقارنة. مجلة الحقوق للبحوث القانونية والاقتصادية بكلية الحقوق-جامعة الإسكندرية، العدد الأول، المجلد الثاني. ص: 318-319.

وقد يكون السبب المحتمل لهذا الرأي، كما أشار البحث في موضع سابق، ما جاء في اتفاقية مجلس أوروبا وتوجيه الاتحاد الأوروبي رقم (EC/46/95)، بأن الهدف الأساسي من حماية البيانات الشخصية هو حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين، وعلى وجه الخصوص حقهم في الخصوصية فيما يتعلق بمعالجة البيانات الشخصية[151].

2. فصل الحق في حماية البيانات الشخصية عن الحق في الخصوصية.

نشأ الفصل ما بين الحق في البيانات الشخصية والحق في الخصوصية في أوروبا، فميثاق الاتحاد الأوروبي لعام (2000)[152]، اعترف بالحق في البيانات الشخصية على أنّه حق مستقل عن الحق في الخصوصية، مخالف بذلك ما جاء في إرشادات منظمة التعاون الاقتصادي والتنمية، واتفاقية مجلس أوروبا، وتوجيه الاتحاد الأوروبي رقم (EC/46/95)، الذين قدّموا حماية البيانات الشخصية على أنّها تخدم الحقوق والحريات، وعلى وجه الخصوص الحق في الخصوصية.

فنصت المادة (7) على احترام الحياة الخاصة والعائلية والمنزل وجاء فيها أن: "لكل شخص الحق في احترام حياته الخاصة وحياته العائلية وبيته واتصالاته". ثم أفرد مادة مستقلة اعترف فيها بحماية البيانات الشخصية

---

[151] Directive 95/46/EC. Article (1/1): "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data". Similarly, Convention No 108 of the Council of Europe defines data protection as, Article 1: "The purpose of this Convention is to secure in the territory of each Party for every individual، whatever his nationality or residence, respect of the rights and freedoms, and in particular his right to privacy, with regard to automated processing of personal data relating to him".

[152] Charter of fundamental rights of the European Union. (2000/C 364/01). Last updated 15/12/2021. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

على أنه حق مستقل عن الحق في الخصوصية وذلك في المادة (8) من الميثاق التي جاءت على النحو الآتي: "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 جمعت عنه وتتعلق به، وحق الحصول عليها صحيحة.3-يخضع الإذعان لهذه القواعد لرقابة هيئة مستقلة"[153].

فميثاق الاتحاد الأوروبي خطا خطوة إلى الأمام بالاعتراف بالحق في حماية البيانات الشخصية على أنّه حق مستقل[154]، من خلال النص على الحق في احترام الحياة الخاصة وحماية البيانات الشخصية، وهو ما يعني أنّهما حقان مختلفان، لكنه لم يوضح طبيعة الاختلاف بينهما، أو طبيعة العلاقة بين هذين الحقين.

ويقول البعض بأنّ الحق في المادة (8) من الميثاق المتعلقة بالحق في حماية البيانات الشخصية يجب اعتبارها مكملاً للمادة (7) المتعلقة بالحق في احترام الحياة الخاصة، أو تطويرًا لها في مجال معالجة البيانات

---

[153] Charter of fundamental rights of the European Union. (2000/C 364/01), Article (7): Respect for private and family life "Everyone has the right to respect for his or her private and family life, home and communications." Article (8): Protection of personal data "1. Everyone has the right to the protection of personal data concerning him or her. 2.Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

[154] De Hert, Paul, Gutwirth, Serge. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Editors: Serge Gutwirth. Yves Poullet. Paul De Hert. C´ecile de Terwangne· Sjaak Nouwt. Reinventing Data Protection?. P: 6.

الشخصية، بينما يؤكد آخرون أن مجرد وجود الحق في حماية البيانات الشخصية بصورة منفصلة، يعني أنّها تتعارض بطريقة ما مع مفاهيم معينة للحق في احترام الحياة الخاصة[155].

لقد كان من الشائع نسبيًا قبل عام (2000)، التأكيد على أنّ الحق في احترام الحياة الخاصة يشمل حماية البيانات الشخصية، فالأولى كانت فكرة أوسع من الثانية، وغالبًا ما كان يُنظر إلى حماية البيانات الشخصية على أنّها بُعد معلوماتي للحق في الخصوصية، وبالتالي فهي مجرد جانب من مفهوم أوسع يشمل العديد من المفاهيم الأخرى، وبعد إعلان ميثاق الاتحاد الأوروبي وعلى أساس المادة (8) منه، أصبح هذا النهج أقل شيوعًا، وأعطى مكانًا لفكرة وجود مفهومين منفصلين ومتميزين؛ الخصوصية أو احترام الحياة الخاصة من ناحية؛ وحماية البيانات الشخصية من ناحية أخرى، وبدأ يزداد الاعتراف بحماية البيانات الشخصية على أنّه حق مستقل، مع التأكيد على أنّ الخصوصية وحماية البيانات الشخصية مرتبطتان ارتباطًا وثيقًا، وفي بعض الحالات وصفت هذه العلاقة الوثيقة بين الخصوصية وحماية البيانات الشخصية بالتداخل الجزئي[156].

3. التأصيل القانوني للفصل ما بين الحق في حماية البيانات الشخصية والحق في الخصوصية.

يكمن التساؤل المهم عن الأساس القانوني للفصل بين هذين الحقين في ميثاق الاتحاد الأوروبي، وقد يساعد ذلك في تقديم دليل لنوع العلاقة أو الاختلافات بين هذين الحقين.

---

[155] Fuster. (2014). Previous reference. P: 199-200.

[156] Fuster. (2014). Previous reference. P: 214.

لا يقدّم توجيه الاتحاد الأوروبي رقم (EC/46/95) الصادر بتاريخ (1995/10/24) أي فائدة في هذا الخصوص، لأنه لا يشير إلى الحق في حماية البيانات، وعدم الإشارة إلى الحق في حماية البيانات في التوجيه ليس مفاجئًا، لأنه صدر قبل صدور ميثاق الحقوق الأساسية للاتحاد الأوروبي، الذي لم يُعلن إلا في عام (2000). كما أنّ مشروع ميثاق الحقوق الأساسية للاتحاد الأوروبي لا يقدم أي تسويغ للأحكام المنفصلة لكلا الحقين، فهو لا ينص إلا على أنّ المادة (8) التي تنص على الحق في حماية البيانات الشخصية، تستند إلى المادة (286) من المعاهدة المنشئة للمجموعة الأوروبية (EC Treaty)[157]، والتوجيه (EC/46/95) الصادر عن البرلمان الأوروبي والمجلس الأوروبي بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وعلى حرية حركة هؤلاء البيانات، والمادة (8) من الاتفاقية الأوروبية لحقوق الإنسان واتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية الصادرة بتاريخ (1981/1/28)، التي صدقت عليها جميع الدول الأعضاء[158]. كما أكّدت

---

[157] Treaty establishing the European Community. (Amsterdam consolidated version). (10/11/1997). Article (286): "1. From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty." Last updated 15/12/2021Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:11997E/TXT&rid=1

[158] Draft Charter of Fundamental Rights of the European Union. Last updated 15/12/2021. Explanation. Article (8). Protection of personal data. "This Article is based on Article 286 of the Treaty establishing the European Community and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281، 23.11.1995), as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States. The right to protection of personal data is to be exercised under the conditions laid down in the above Directive, and may be limited under the conditions set out by Article 52 of the Charter". Available at:
https://www.europarl.europa.eu/charter/pdf/04473_en.pdf

المذكرة التفسيرية لميثاق الحقوق الأساسية للاتحاد الأوروبي على ما جاء في مشروع الميثاق، وأشارت إلى استبدال المادة (286) من المعاهدة المنشئة للمجموعة الأوروبية (EC Treaty)[159] بالمادة (16) من معاهدة عمل الاتحاد الأوروبي (TFEU)[160]، والمادة (39)[161] من معاهدة الاتحاد الأوروبي (TEU)[162].

---

[159] Originally signed in 1957 as the European Economic Community Treaty (or Treaty of Rome), it was renamed in 1993 with the entry into force of the Treaty on European Union (Maastricht Treaty), and became known as the Treaty establishing the European Community (EC Treaty). In December 2009, it was amended again under the EU Reform Treaty (Lisbon Treaty) and renamed the Treaty on the Functioning of the European Union (TFEU). Last updated 15/12/2021. Available at:
https://uk.practicallaw.thomsonreuters.com/2-375-8102?transitionType=Default&contextData=(sc.Default)&firstPage=true

[160] The Treaty on the Functioning of the European Union. Consolidated versions. (26/10/2012). Article (16): "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union". Last updated 15/12/2021. Available at:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

[161] The Treaty on European Union (TEU). Consolidated versions. (26/10/2012). Article (39): "In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities". Last updated (13/1/2022). Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT

[162] Explanations relating to the Charter of Fundamental Rights. (2007/C 303/02). Explanation on Article (8). Protection of personal data. This Article has been based on Article 286 of the Treaty establishing the European Community and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31) as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States. Article 286 of the EC Treaty is now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union. Reference is also made to Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free

وبما أنّ التشريعات الأوروبية لم تعطِ رأيًا نستطيع الاستناد إليه لتسويغ الأساس القانوني للفصل بين كلا الحقين، نستطيع اللجوء إلى الرأي القائل إنّ الفصل بين الحقين وإدراج الحق في حماية البيانات الشخصية في الميثاق يتعلق بأهداف حماية البيانات الشخصية في الاتحاد الأوروبي[163]، وذلك لأنّ توجيه الاتحاد الأوروبي رقم (EC/46/95) له هدفان مزدوجان هما تهيئة الأسواق الداخلية وترسيخها بين دول الاتحاد الأوروبي من جهة، وحماية الحقوق الأساسية من جهة أخرى، ولكن طغى هدف دمج الأسواق على هدف الحقوق الأساسية[164]، ونظرًا لأنّ توجيه الاتحاد الأوروبي تضمن أحكاماً ملائمة للأعمال التجارية، برزت الحاجة إلى أساس قانوني لتعزيز شرعية توجيه الاتحاد الأوروبي في حماية البيانات الشخصية، وإثبات هدف التوجيه في حماية حقوق الإنسان، من خلال التأكيد على بُعد التوجيه في حماية الحقوق الأساسية من خلال حماية البيانات الشخصية التي لم تكن واضحة فيه[165].

ومع أنّ الأهداف المعلنة للتوجيه في ضمان التدفق الحر للبيانات الشخصية في السوق الداخلية للاتحاد الأوروبي وحماية الحقوق الأساسية، إلا أنّ البعض يرى أنّ التسويغ القانوني للتوجيه هي اعتبارات السوق الداخلية

movement of such data (OJ L 8, 12.1.2001, p. 1). The above-mentioned Directive and Regulation contain conditions and limitations for the exercise of the right to the protection of personal data. Last updated: 24/7/2021. Available at:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF

[163] De Hert, Gutwirth. (2009). Previous reference. P: 8.

[164] European Commission. (4.11.2010). Brussels COM (2010) 609 final. 'A comprehensive approach on personal data protection in the European Union' Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Available At: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

[165] De Hert, Gutwirth. (2009). Previous reference. P: 8.

وحدها، لأنّ الاتحاد الأوروبي يفتقر إلى الكفاءة لسن تشريعات لحماية الحقوق الأساسية؛ ولذلك فإنّ هذا التسويغ المحتمل معقول لكن من جهة أخرى لا يجوز الاعتراف بحق جديد لإضفاء شرعية لاحقة بأثر رجعي على تشريع قائم، بالإضافة إلى ذلك، إذا كانت حماية البيانات مجموعة فرعية من الحق في الخصوصية، فلماذا لا يكون الحق في الخصوصية المعترف فيه منذ فترة طويلة في تشريعات الاتحاد الأوروبي، والمنصوص عليه في ميثاق الاتحاد الأوروبي كافيًا لإضفاء الشرعية على حماية البيانات الشخصية[166].

وبعد سلسلة التحديات التي أبرزتها التطورات التكنولوجية لحماية البيانات الشخصية، وازدياد انتاج البيانات وحجمها، وعمليات تبادلها وجمعها سواء من قبل الشركات الخاصة أو السلطات العامة من أجل متابعة أنشطتها، وإتاحة الأفراد لمعلوماتهم الشخصية بشكل عام وعالمي، نشأت ضرورة لإجراء مراجعة عامة للتوجيه الأوروبي بعد أن غيّرت التكنولوجيا كلًا من الاقتصاد والحياة الاجتماعية[167]، وخاصة عام (2009) بعد أن دخلت معاهدة لشبونة حيز النفاذ[168]، وأدخلت المادة (1/16) من معاهدة عمل الاتحاد الأوروبي، وأقرّت بالقواعد المتعلقة بحماية البيانات

---

[166] Lynskey, Orla. (2014). International and Comparative Law Quarterly. Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. International and Comparative Law Quarterly. Vol. (63). Issue (3). P: 570-571.

[167] European Commission. (25.1.2012). Brussels. COM (2012) 11 final. 2012/0011 (COD). C7-0025/12. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). P: 1. last updated 5/6/2021. Available at: https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

[168] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, Article (6): "2. This Treaty shall enter into force on 1 January 2009, provided that all the instruments of ratification have been deposited, or, failing that, on the first day of the month following the deposit of the instrument of ratification by the last signatory State to take this step." Last updated 15/12/2021. Available at:

الشخصية في المادة (8) من ميثاق الحقوق الأساسية للاتحاد الأوروبي، على أنّه حق مستقل عن الحق في الخصوصية، فقدمت بذلك أساسًا قانونيًا لاعتماد قواعد جديدة لحماية البيانات الشخصية[169].

مهما كان الأمر، فإنّ كلا الحقين موجودان الآن في النظام القانوني للاتحاد الأوروبي، فسياسة الاتحاد الأوروبي الحالية بدون أدنى شك تتجاوز هذا النقاش، فاللائحة العامة لحماية البيانات (GDPR) رقم (679) التي أصدرها الاتحاد الأوروبي عام (2016) ودخلت حيز النفاذ عام (2018)، والتي حلت محل التوجيه رقم (EC/46/95)، نصت صراحة أنّ حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية هي حق أساسي وذلك بموجب نص المادة (8) من ميثاق الحقوق الأساسية للاتحاد الأوروبي والمادة (16) من معاهدة عمل الاتحاد الأوروبي، اللتين نصتا على أنّ لكل فرد الحق في حماية البيانات الشخصية المتعلقة به[170]، وأكّدت المادة (2/1) أن حماية البيانات الشخصية تحمي الحقوق والحريات الأساسية للأشخاص الطبيعيين ولا سيما حقهم في حماية البيانات الشخصية فيما يتعلق بمعالجة البيانات والقواعد المتعلقة بحرية حركة البيانات الشخصية[171].

---

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

[169] European Commission. (25.1.2012). Brussels. COM (2012) 11 final. 2012/0011 (COD). C7-0025/12. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Previous reference. P.2.

[170] GDPR. Recital (1): "The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her".

[171] GDPR. Article (1/2): "2.This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".

ثانيًا: أهمية الاعتراف بالحق في البيانات الشخصية على أنّه حق مستقل

قد تكون محاولات الفصل التام بين البيانات الشخصية والخصوصية مهمة صعبة بالنظر إلى؛ اعتماد قوانين حماية البيانات في نشأتها اعتمادًا كبيرًا على حماية الحق في الخصوصية؛ بالإضافة إلى عدم الاعتراف بالحق في حماية البيانات الشخصية في كثير من الدول بما فيها سورية. ولكن من جهة أخرى يتميز مفهوم البيانات الشخصية بأنّه مفهوم قانوني محدد بدقة ولا يثير أي مشكلات في تحديده فهو لا يعتمد على الظروف أو السياق، ولا يختلف باختلاف الأشخاص أو الدول، على عكس مفهوم الخصوصية. فتقييم ما إذا كان للفرد مصلحة في خصوصية اسمه يعتمد على السياق، وبالتالي الكشف عن اسم شخص ما في سياق الأنشطة المهنية لا يرتبط عادة بالحياة الخاصة، في حين تشكل الإشارة إلى اسم أحد المشاركين في محضر الاجتماع بيانات شخصية[172].

كما تكمن المشكلة في الرأي القائل بأنّ حماية البيانات الشخصية فئة فرعية من الخصوصية في احتمال تفسير انتهاكات البيانات الشخصية في ضوء معايير الخصوصية، وبالتالي فإنّ انتهاك هذه البيانات لا يمكن أن تؤيده المحكمة إلا إذا كان ذلك بمثابة انتهاك للخصوصية[173]. وتأتي أهمية الاعتراف بالحق في حماية البيانات الشخصية على أنّه حق مستقل لأنّه يحمي مجموعة أوسع من البيانات والإجراءات المتعلقة بها، ولأنه يحمي حقوق تتجاوز الحق في الخصوصية. وفيما يأتي محاولة لإبراز أهمية الاعتراف بحماية البيانات الشخصية على أنّه حق مستقل، من خلال عرض النطاق الواسع للبيانات المحمية والإجراءات المتعلقة بها، والنطاق الواسع للحقوق المحمية.

---

[172] Lynskey. (2014). Previous reference. P: 18.

[173] Lynskey. (2013). Previous reference. 76-80.

1. النطاق الواسع للبيانات المحمية والإجراءات المتعلقة بها.

إنّ نطاق تطبيق قواعد حماية البيانات أوسع من النطاق المحمي بموجب حماية الخصوصية، ونلحظ ذلك من خلال نطاق البيانات الشخصية المحمية وعمليات معالجة البيانات الشخصية.

أ. النطاق الواسع للبيانات المحمية.

إنّ نطاق حماية البيانات الشخصية بموجب الحق في حماية البيانات الشخصية واسع جدًا، لأنّه يشمل جميع البيانات الشخصية[174]، أما مفهوم حماية الخصوصية أو السرية لا ينطبق على هذا النطاق الواسع من البيانات المحمية. فالحق في البيانات الشخصية يحمي أيّ بيانات تتعلق بالشخص الطبيعي المحدد أو القابل للتحديد[175]. وهذا يعني أنّه ينطبق على جميع البيانات الشخصية المتعلقة بشخص طبيعي سواء أكانت سرية أم غير سرية، وسواء تعلقت بحياته الخاصة أم بحياته العامة، وبذلك يغطي طائفة كبيرة من المعلومات التي تمس الحياة الخاصة والعائلية للفرد، وأيضًا المعلومات المتعلقة بأي نوع من الأنشطة التي يقوم بها الفرد، مثل المعلومات المتعلقة بعلاقات العمل أو السلوك الاقتصادي أو الاجتماعي للفرد[176]، والمعلومات التي تحدد هويته.

هذا المفهوم لا يتوافق مع ما يتضمنه مفهوم الخصوصية، فالأفكار الثلاث التي تجد أساسًا لها في مفهوم الخصوصية تتمثل في حماية السرية والسكينة والألفة[177]، وبالتالي فإنّ التعدي على الخصوصية غالبًا ما يكون في

---

[174] De Hert, Gutwirth. (2009). Previous reference. P: 9-10.

[175] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. P: 25.

[176] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. P: 7.

[177] الشماط، كندا. (2004-2005). الحق في الحياة الخاصة. رسالة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة دمشق: سورية. ص: 121-126.

صورة كشف الحياة الخاصة الحميمية أو العائلية أو الأسرار التي لا يود الشخص إطلاع الغير عليها أو التطفل على أخباره التي يود الاحتفاظ بها لنفسه، في حين أنّ الكثير من المعلومات الشخصية التي تُجمع حول الأفراد على شبكة الإنترنت، أو تُخزن في قواعد البيانات، غالبًا ما تكون غير سرية، مثل الاسم والعنوان ورقم الهاتف وتاريخ الميلاد وما إلى ذلك، فحماية البيانات لا تسعى إلى جعل المعلومات الشخصية سرية، ومحاولة تكييف حماية البيانات الشخصية مع مفهوم الخصوصية على أنّها حماية البيانات السرية أو الخاصة، تتجاهل أو تهمش فئات كثيرة من البيانات الشخصية؛ كما يخفق مفهوم الخصوصية، إذا عرفناه على أنّه حماية الحميمية في استيعاب المشكلة، لأنّ قواعد البيانات في الغالب لا تغزو حياتنا الحميمية أو تعطلها، فأسماؤنا وعناويننا وأنواع السيارات التي نمتلكها وما إلى ذلك ليست حقائق حميمة، وبالتأكيد لا تعادل أسرارنا الخاصة التي نسعى إلى حمايتها، ففي الفضاء الإلكتروني، معظم علاقاتنا تشبه المعاملات التجارية أكثر منها علاقات شخصية أو حميمية[178].

وقد تتقاطع الخصوصية على الإنترنت مع حماية البيانات، فحماية الخصوصية هي في الواقع جزء كبير منها حماية للبيانات، ولكن البيانات الشخصية لا تتعلق جميعها بالخصوصية، فالبيانات التي تتعلق بالنشاطات العامة للفرد تشكّل بيانات شخصية، لكنها لا تدخل ضمن مفهوم الخصوصية، كما أنّ حماية البيانات الشخصية لا تحل محل حماية الأسرار وطمأنينة الفرد واستقلاليته، لكنها تكملها وتؤمن تفعيلها في وجه مخاطر الإنترنت[179].

---

[178] Solove, Daniel. J. (2002). Conceptualizing privacy. California law review. California Law Review. Vol 90. P: 1153.

[179] الحجار، وسيم شفيق. (2017). النظام القانوني لوسائل التواصل الاجتماعي (واتساب، فيسبوك، تويتر). دراسة قانونية مقارنة حول الخصوصية والحرية الشخصية والمسؤولية والاختصاص. أبحاث ودراسات (4). الطبعة الأولى. بيروت: لبنان. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب. ص: 59.

كما أنّ الحق في حماية البيانات الشخصية أوسع نطاقًا وأكثر دقة مقارنة بمفهوم خصوصية المعلومات وهي إحدى أكثر نظريات الخصوصية انتشارًا وتتعلق بالتحكم في المعلومات الشخصية والسيطرة عليها[180]. فإذا كانت الخصوصية تعبّر عن حالة يتعذر فيها على الآخرين الوصول إلى الشخص داخل المجال الخاص به، تصف خصوصية المعلومات عدم إمكانية الوصول إلى المعلومات الخاصة بالشخص، لذلك يمكن النظر إلى أنّ الخصوصية وخصوصية المعلومات يشيران إلى السرية وعدم إمكانية الوصول إلى المعلومات الخاصة أو تعتيمها[181]، وبغض النظر إنّ تركيز النظرية على المعلومات يجعل من مفهوم الخصوصية مفهومًا ضيقًا، ويستبعد جوانب الخصوصية غير المعلوماتية، فإنّ النظرية غامضة لأنّ مؤيديها غالبًا ما يخفقون في تحديد أنواع المعلومات التي يجب أن يتحكم بها الأفراد، وما المقصود بالتحكّم الذي غالبًا ما يفسّر على نطاق واسع جدًا أو ضيق جدًا[182]. أما مفهوم حماية البيانات فهو أكثر انفتاحًا، حيث ترتبط الحماية بقيم مختلفة عن الخصوصية ومتعلقة بالبيانات الشخصية، وبالتالي يُنظر إلى حماية البيانات على أنّها تشمل خصوصية المعلومات ولكنّها تغطي أكثر من ذلك على سبيل المثال مسائل تتعلق بدقة البيانات وإمكانية الوصول إليها[183].

كما أنّ تعريف الخصوصية على أنّها السيطرة على المعلومات يلتقط المشكلة جزئيًا فقط، في حين أن حماية البيانات الشخصية تعطي حلًا من خلال عملية جمع المعلومات ومعالجتها واستخدامها، وهي عملية خارجة

---

[180] Solove, Daniel. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. Stanford Law Review. Vol. 53. P: 1109-1110.

[181] Schartum Dag. W. (2008). Designing and formulating data protection laws. International Journal of Law and Information Technology. Vol. 18 No. 1. P: 2-3.

[182] Solove, Daniel.J. (2002). Conceptualizing privacy. California law review. California Law Review. Vol 90. 1111-1112.

[183] Schartum. (2008). Previous reference. P: 2.

عن تحكّم الأفراد وسيطرتهم. وبعبارة أخرى، إنّ ما يجعل حماية البيانات الشخصية مهمة، هو أنّ المعلومات المجمّعة، التي يمكن استخدامها لاتخاذ قرارات مهمة بشأن حياة الناس، غالبًا ما تخضع لعملية تفتقر إلى الكثير من الانضباط والسيطرة، كما أنّ الفرد لديه معرفة ضئيلة بكيفية معالجة معلوماته الشخصية واستخدامها[184]. فحماية البيانات الشخصية أوسع نطاقًا من خصوصية المعلومات، ولكنه في نفس الوقت أكثر تحديدًا من الخصوصية لأنه يتعامل بشكل أساسي مع المعلومات الشخصية[185].

كما تنطبق قواعد حماية البيانات الشخصية على معالجة البيانات الشخصية المتعلقة بشخص طبيعي محددًا أو من الممكن تحديده، فتشمل الحماية البيانات المتعلقة بأفراد مجهولين ولكن من الممكن تحديدهم، فتنطبق قواعد معالجة البيانات متى كان تحديد الهوية ممكنًا، بغض النظر عما إذا كان تحديد الشخص صاحب البيانات سيحدث أم لا، أما الحق في الخصوصية لا ينطبق في هذه الحالة فهو يحمي المعلومات الخاصة التي تتعلق بشخص محدد.

ب. النطاق الواسع للإجراءات المحمية.

يساعد مفهوم المعالجة أيضًا في تحديد نطاق تطبيق الحق في حماية البيانات الشخصية، فهو أكثر شمولاً من التدخل في الخصوصية، فحماية البيانات الشخصية تغطي جميع عمليات المعالجة التي تُجرى على البيانات الشخصية، فمجرد قيام صاحب العمل بتسجيل بيانات متعلقة بأسماء الموظفين والأجور المدفوعة لهم لا يمكن أن

---

[184] Solove. (2002). Previous reference. P: 1153-1154.

[185] Schartum. (2008). Previous reference. P: 2.

يشكل تدخلاً في الحياة الخاصة، ولكن هذا التسجيل يشكل معالجة لبيانات شخصية وبالتالي يقع ضمن نطاق الحق في حماية البيانات فلا يمكن القول إنّ هذه العملية تتعلق بالخصوصية[186]. وبالتالي من الصعب تصور أي عملية تجري على البيانات الشخصية لا يغطيها مفهوم حماية البيانات. ومن الممكن التفكير في العديد من الأمثلة اليومية الأخرى لمعالجة البيانات التي تقع ضمن نطاق الحق في حماية البيانات الشخصية، ولكن لا يمكن القول إنّها تتعلق بالخصوصية، فعلى سبيل المثال، إذا تنافست طالبة مع فريقها الرياضي بالجامعة، فقد يُنشر الاسم والفئة العمرية للطالب على موقع الجامعة، ويشكل هذا النشر معالجة، ولكنه لا يشكل تدخلًا في الخصوصية، لأن المعلومات المعنية هي بيانات متاحة للجمهور، ولم تجمع وتخزن وتنشر بصورة ممنهجة، بالإضافة إلى ذلك كان على الطالبة أن تتوقع معالجة بياناتها الشخصية بهذه الطريقة[187]، فحماية الخصوصية غالبًا ما يُنظر إليها من منظور أكثر كلاسيكية وتحديدًا بالحق في التعتيم أو العزلة، والتي تتعامل في الغالب مع إخفاء جوانب معينة عن معرفة الآخرين، وحماية المعلومات الخاصة من الكشف عنها في المجال العام، فالحق في الخصوصية ينتهك فقط إذا كُشف عن حقائق خاصة حقيقية تتعلق بشخص ما للجمهور[188]. ويمكننا القول بقدر ما تحمي القواعد القانونية معالجة البيانات الشخصية التي تتعلق بالأشخاص، التي ليس من الضروري أن تكون خاصة أو تنتهك الخصوصية، فهو نظام خاص بحماية البيانات بغض النظر عن التسمية المستخدمة[189].

---

[186] Lynskey. (2014). Previous reference. P: 285.

[187] Lynskey. (2014). Previous reference. P: 285.

[188] De Andrade, Norberto Nuno Gomes. (2012). Oblivion: The Right to Be Different from Oneself – Reproposing the Right to Be Forgotten. Monograph "VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet". Universitat Oberta de Catalunya. IDP. Revista de Internet, Derecho y Política. No. 13. P: 126. P: 122-137.

[189] De Hert, Gutwirth. (2009). Previous reference. P: 24-25.

2. النطاق الواسع للحقوق المحمية.

يسعى الحق في حماية البيانات الشخصية إلى حماية مصالح تتجاوز الحق في الخصوصية، ومع أنّه ليس من السهل تحديد المصلحة الأساسية لحماية البيانات، فهناك العديد من المصالح الكامنة وراء حماية البيانات الشخصية. فوفقًا لمعظم الوثائق الخاصة بحماية البيانات الشخصية، الهدف الرئيسي من الحماية هو حماية حقوق الأفراد وحرياتهم الأساسية، من الضرر الناتج عن معالجة بياناتهم الشخصية، لضمان المصالح المتصلة بالبيانات الشخصية. فالحق في حماية البيانات الشخصية يحمي حقوق الإنسان وحرياته الأساسية الأخرى بدءًا من حماية الحرية والأمن والعدالة[190] والمساواة والإجراءات القانونية الواجبة[191]، كما يعزز تقرير المصير المعلوماتي[192] والتوازن بين القوى والنزاهة ويحمي كرامة الأشخاص ويعزز الديمقراطية[193] وهو ما تعكسه مبادئ حماية البيانات.

كما تضمن الحقوق المنصوص عليها لأصحاب البيانات، إمكانية وصول الأفراد إلى معلوماتهم الشخصية في أيدي أشخاص آخرين لضمان أنها ملائمة وصحيحة وكافية، وإمكانية طلب تصحيحها أو محوها إذا لزم الأمر، وهنا يتقاطع الحق في حماية البيانات مع الحق في حرية المعلومات[194].

---

[190] GDPR. Recital (2): "...This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."

[191] Schartum. (2008). Previous reference. P: 2.

[192] GDPR. Recital (7): "... Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced."

[193] De Hert, Gutwirth. (2009). Previous reference. P: 4-5.

[194] Jeske, Margo, Intahchomphoo, Channarong, Landriault, Emily, Bioni, Bruno. (March 2016) The Intersection of Freedom of Information, Privacy Legislation and Library Services in Canadian Jurisdictions. P: 4. Last updated: 21/1/2022. Available at:

إنّ نطاق الحقوق المحمية بموجب قواعد حماية البيانات الشخصية يتعدى حماية الحق في الخصوصية، وفيما يأتي تفصيل لأهم الحقوق المحمية بموجب الحق في حماية البيانات الشخصية.

أ. الحق في تقرير المصير المعلوماتي: يقصد بالحق في تقرير المصير المعلوماتي أن يكون الأفراد قادرين على ممارسة السيطرة على ما يحدث لبياناتهم الشخصية، ففي نهاية المطاف هو شيء يعود لهم[195]، ويترك لهم تحديد ما إذا كان ينبغي الكشف عنها وكيف ينبغي استخدامها، فإذا لم يستطع شخص ما توقع ماهية المعلومات المخزنة عنه، والأطراف الذين يستطيع التواصل معهم لمعرفة هذه المعلومات، فإنه يُمنع من حريته في التخطيط أو اتخاذ القرار بحرية دون التعرض لأيّة ضغوط، وإذا كان الشخص يعتقد أنّ المشاركة في جمعية أو مبادرة ستسجل رسميًا وأنّ هناك مخاطر قد تنجم عن ذلك، فقد يتخلى عن ممارسة حقوقه، وذلك لن يؤثر ذلك على فرصته في التطور فحسب، بل سيؤثر أيضًا على الصالح العام، لأنّ تقرير المصير المعلوماتي شرط أساسي لمجتمع ديمقراطي حر قائم على تمكين مواطنيه على العمل والتعاون[196].

فالحق في حماية البيانات يعزز الحق في تقرير المصير المعلوماتي من خلال تعزيز التحكم في البيانات الشخصية التي يمنحها هذا الحق للأفراد والذي يخدم غرضين رئيسيين؛ فهو يعزز حقوق الشخصية التي تهددها معالجة

https://www.researchgate.net/publication/298733944_The_Intersection_of_Freedom_of_Information_Privacy_Legislation_and_Library_Services_in_Canadian_Jurisdictions

[195] Koops, Bert-Jaap. (2014). The trouble with European data protection law. International Data Privacy Law. Vol. 4. No. 4. P: 251.

[196] Rouvroy, Antoinette, Poullet, Yves. (2009). The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. Serge Gutwirth. Yves Poullet. Paul De Hert, C´ecile de Terwangne, Sjaak Nouwt, Reinventing Data Protection? P: 53.

البيانات الشخصية، كما أنّه يقلل من عدم تناسق المعلومات والقوة بين الأفراد من جهة والمتحكمين بالبيانات الشخصية من جهة أخرى[197]. ولا يُسمح بالتدخل في الحق في تقرير المصير المعلوماتي إلا عندما تفوق المصالح العامة أو الخاصة السائدة المصلحة الفردية التي تؤسس للحق في التنمية الذاتية[198].

ب. الحق في التنمية الذاتية: حماية البيانات الشخصية تسمح للفرد أن يعيش حياته بالطريقة التي يريدها دون خوف من المراقبة أو المتابعة، فشعور الشخص بأنّه مراقب يجعله يتصرف بطريقة واعية، وبالتالي، تتأثر أفعاله بشعوره بالمراقبة، مما يؤثر على حق الفرد في التنمية الذاتية[199]. فالمراقبة عن طريق معالجة البيانات، لها تأثير مخيف على السلوك الفردي، فمجرد تصور المراقبة قد يكون كافياً لكبح السلوك الفردي، سواء كان هناك مراقبة على الشخص أم لا، مثل هذه المراقبة، يمكن أن تعيق التطور الفردي أو التنمية الذاتية[200].

إنّ الحق في حماية البيانات الشخصية يجعل الفرد قادرًا على تقديم جانب من شخصيته للمجتمع، فعلى سبيل المثال قد يشعر الفرد بالراحة عند مناقشة أفكاره مع أصدقائه، ولكنه قد يشعر براحة أقل عند مناقشة الموضوع نفسه مع عائلته، وفي هذا الصدد، تسّهل حماية البيانات التقديم الانتقائي للشخصية خلافًا للحق في الخصوصية، وبالتالي يعمل على أنّه أداة لتنمية شخصية الفرد وتطويرها، فيتمكن من التحكم في الجزء الذي يريد إظهاره لشريحة معينة من المجتمع[201]، وإمكانية تقييد محتوى معين على جهات محددة فقط على مواقع التواصل الاجتماعية هو

---

[197] Lynskey. (2014). Previous reference. P: 589-592.

[198] Rouvroy, Poullet. (2009). Previous reference. P: 56.

[199] Rouvroy, Poullet. (2009). Previous reference. P: 53.

[200] Lynskey. (2014). Previous reference. P: 588.

[201] Lynskey. (2014). Previous reference. P: 589.

انعكاس لهذه الحقيقة، كما أنّ حرمان الأفراد من حقوق معينة على أساس البيانات الشخصية التي أتاحوها على مواقع الشبكات الاجتماعية، أو من خلال الربط غير المصرح به للبيانات الشخصية يمكن أنّ يكون له أيضًا تأثير على السلوك الفردي مماثل لتلك الناتجة عن المراقبة[202].

ج. الحق في عدم التمييز: ينبع الحق في عدم التمييز من الفرضية العامة للمساواة في الكرامة بين البشر[203]، وهو يشكل أحد المبادئ الأساسية، غير القابلة للانتقاص من حقوق الإنسان ويتألف من مبدأ عام للمساواة، أي أنّه يجب التعامل مع المواقف المماثلة بالطريقة نفسها، ويجب التعامل مع المواقف المختلفة بشكل مختلف، ويتعلق بأحكام محددة متعلقة ببعض الأسس المحمية، مثل العرق والجنس والدين وما إلى ذلك، ومجال تطبيق محدد، مثل سوق العمل والتدريب المهني والتعليم والضمان الاجتماعي والرعاية الصحية والحصول على السلع والخدمات والقانون الجنائي[204]. وقواعد حماية البيانات التي تعبر عن الحق في حماية البيانات، أكثر فعالية من الحق في الخصوصية في تقليل مخاطر تعرّض الأفراد لأضرار ملموسة معينة ناجمة عن معالجة البيانات، فمن المرجح أن تؤدي فئات معينة من البيانات الشخصية إلى تمييز غير قانوني أو تعسفي، بما في ذلك معلومات عن الأصل العرقي أو الإثني، والدين والآراء السياسية والمعتقدات الفلسفية وغيرها، فضلاً عن العضوية في جمعية أو نقابة[205]. فالحق

---

[202] Blackman, Josh. (2009). Omniveillance, Google, Privacy in Public, and the right to your digital identity: a tort for recording and disseminating an individual's image over the internet. Santa Clara Law Review. Vol 49. P: 341-343.

[203] Ozden, Melik. (June 2011). The right to non-discrimination. Part of a series of the Human Rights Programme of the Europe - Third World Centre (CETIM). Geneva Switzerland. P: 7.

[204] Ferraris, Valeria, Bosco, Francesca, D'Angelo, Elena. (2013). The impact of profiling on fundamental rights. P: 22-23. Last updated: 21/4/2022. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753

[205] Ferraris, Bosco, D'Angelo. (2013). Previous reference. P: 34.

في حماية البيانات الشخصية، يحظر التمييز من خلال قواعد خاصة تتعلق بمعالجة بعض الفئات الخاصة من البيانات[206] فلا يُسمح بمعالجتها إلا وفقًا لشروط صارمة.

كما تقلل حماية البيانات من مخاطر التمييز من خلال تقليل احتمالية اتخاذ قرارات تؤثر سلبًا على الأفراد، وذلك لأنّ حماية البيانات تمنع صانعي القرار من اتخاذ قرارات من المحتمل أن تؤثر على الفرد، بناءً على المعالجة الآلية للبيانات[207]، بما في ذلك التنميط، وهو أي شكل من أشكال المعالجة الآلية للبيانات الشخصية لاستخدامها في تقويم جوانب معينة تتعلق بشخصية الفرد، لتحليل أو توقع الجوانب المتعلقة بأدائه في العمل أو وضعه الاقتصادي أو الصحي أو اهتماماته أو موثوقيته أو سلوكه أو موقعه أو تحركاته[208]، وبالتالي فإنّ حماية البيانات تجعل التمييز المباشر وغير المباشر أكثر صعوبة، فعلى سبيل المثال، لا يمكن لصاحب العمل أن يرفض النظر تلقائيًا من عملية اختيار الوظيفة، المتقدمين الذين تزيد أعمارهم عن (30) عامًا (تمييز مباشر)، ولا يمكن لصاحب

---

[206] GDPR. Article (9/1): Article (9), Processing of special categories of personal data, "1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[207] GDPR. Article (22/1): "1.The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

[208] GDPR. Article (4/4): 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

العمل استبعاد جميع المرشحين الذين حصلوا على مؤهلاتهم الجامعية منذ أكثر من عشر سنوات (التمييز غير المباشر)[209]. وبالتالي تقلل حماية البيانات من التمييز الذي يؤدي إلى معاملة غير عادلة للفرد.

إنّ توضيح هذه القيمة الوسيطة لحماية البيانات الشخصية، من خلال حماية الحق في تقرير المصير المعلوماتي أو التنمية الذاتية أو الحق في عدم التمييز، مهم لأنّه يزيل الخلط الشائع مع مفهوم الخصوصية، لذلك يجب أن يتدخل القانون لحماية هذا الحق، وبصورة خاصة في ظل الظروف الحالية والمستقبلية لمعالجة البيانات، فالوسائل التقنية لجمع البيانات الشخصية وتخزينها غير محدودة عمليًا، كما يمكن استرجاعها في غضون ثوانٍ بغض النظر عن المسافة، كما يمكن ربطها مع بيانات أخرى لتكوين ملف شخصي جزئي أو شبه كامل عن مستخدم الإنترنت، حيث لا يمتلك الأشخاص وسائل كافية للتحكم مما قد يؤثر على سلوك الأفراد.

هذه القيمة الوسيطة لحماية البيانات الشخصية دفعت البعض للقول إنّ حماية الحق في الخصوصية حق موضوعي لضمان حماية وتعزيز المصالح المتعلقة بالحياة الخاصة للأفراد، فالحق في الخصوصية جزء من مجموعة أكبر من الحقوق التي تسمى حقوق الشخصية، بينما الحق في حماية البيانات الشخصية حق إجرائي يحدد القواعد والأساليب والشروط التي من خلالها تنفذ الحقوق الموضوعية وتحمى بفعالية، وتعمل على أنّها شروط لا غنى عنها للتنسيق بين المصالح والحقوق المختلفة، فحماية البيانات، على هذا النحو، لا تمثل قيمة أو مصلحة في حد ذاتها، إنّما تحدد الإجراءات والأساليب لاحترام القيم والمصالح المنصوص عليها في الحقوق الموضوعية

[209] Lynskey. (2014). Previous reference. P: 588.

الأخرى مثل الحق في الخصوصية والهوية وحرية المعلومات والأمن وحرية الدين وما إلى ذلك، وبالتالي من الخطأ تقليل حماية البيانات إلى الخصوصية، لأن الأولى تحمي مجموعة أوسع بكثير من المصالح والحقوق[210].

ومع احترامنا لهذا الرأي إلا أنّ تحديد الإجراءات المتعلقة بمعالجة البيانات الشخصية وتنظم استخدامها، وغيرها من الإجراءات الأخرى التي تعزز احترام الحقوق والحريات الأخرى، لا يعني أنّ الحق في حماية البيانات حق إجرائي، فالهدف من حماية البيانات الشخصية بالدرجة الأولى، هو احترام الحق في حماية البيانات الشخصية، وهذا الحق يسعى إلى حماية واحترام مصلحة وقيمة مهمة في حد ذاتها، لا تتعلق أهميتها بقيمة المعلومات ومدى سريتها أو خصوصيتها، لكن من تعلقها بشخصية الإنسان. والاتجاه الحالي، كما كرّسه ميثاق الحقوق الأساسية للاتحاد الأوروبي واللائحة الأوروبية، يعترف بحماية البيانات على أنّه حق أساسي وقيمة نهائية، بالإضافة إلى قيمته الوسيطة في حماية الحقوق والحريات الأخرى.

وبناءً على ذلك، كلا المفهومين مرتبطان بطريقة معينة، وإن كانت حماية البيانات هي نتاج للخصوصية وكلا الحقين مرتبطان ارتباطًا وثيقًا[211]، ولكن حماية البيانات ليست مجرد فئة فرعية من فئات الحق في الخصوصية بل هي جارة قريبة جدًا منها[212]. فكلا الحقين متداخلان جزئيًا[213]، ولكنهما متمايزان في جوانب أخرى[214]. وكلا

---

[210] De Andrade, Norberto Nuno Gomes. (2012). Previous reference. P: 125-126.

[211] Tzanou, Maria. (2013). Data Protection as a fundamental right next to privacy? "Reconstructing" a not so new right. International Data Privacy Law. Vol. 3. No. 2. P: 88.

[212] Birnhack, Michael. D. (2008). The EU Data Protection Directive: An engine of a global regime. Computer Law & Security Review. Volume 24. P: 509.

[213] Fuster. (2014). Previous reference. P: 214.

[214] Lynskey. (2014) Previous reference. P: 587.

الحقين يكمل أحدهما الآخر في حماية الفرد من التدخل غير المشروع في حياته الشخصية. وللأسف فإن هذا التمييز بين كلا الحقين، لا يعترف به سوى الاتحاد الأوروبي وعدم إدراك هذه الاختلافات في أجزاء أخرى من العالم يشكل عائقاً رئيسياً أمام إنشاء نظام دولي لحماية البيانات[215].

وبالإضافة إلى ذلك، فإن الادعاء بأنّ حماية البيانات تندرج ضمن نطاق الحق في الخصوصية له جانب سلبي آخر، وينطبق هذا بصفة خاصة على البلدان النامية، مثل سورية، التي لديها مستوى منخفض من الوعي بأهمية حماية البيانات الشخصية. وقد يفترض، أن أحكام القانون بشأن الحق في الخصوصية كافية لحماية الأفراد من الضرر الناجم عن معالجة بياناتهم، ولذلك يمكن التقليل من قيمة نظام قانوني مخصص لحماية البيانات الشخصية.

ومما سبق عرضه نستنتج أنّ القول بإنّ الحق في الخصوصية يتضمن الحق في حماية البيانات لا ينصف الطبيعة الفريدة لكلا الحقين، ومن المؤكد أنّ الحق في حماية البيانات الشخصية يؤدي إلى حماية أكبر للبيانات الشخصية من الحق في الخصوصية، فمفهوم الخصوصية لا يستطيع أن يستغرق مفهوم حماية البيانات؛ فالحق في حماية البيانات يشمل نطاقًا أوسع من البيانات الشخصية المحمية، وينظم الإجراءات المتعلقة بمعالجة البيانات، كما أنّه يحمي حقوقًا وحريات تتجاوز الحق في الخصوصية. لذلك يجب النظر إلى حماية البيانات على أنّها تتداخل جزئيًا مع الخصوصية، ولكنّها توفر مزايا إضافية ومميزة للأفراد، وبالتالي يمكن فهم أهمية حماية البيانات، والتعامل

[215] De Hert, Paul, Papakonstantinou, Vagelis. (2013). Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency? I/S: A Journal of Law and Policy for the Information Society. Vol. 9:2. P: 316.

معها بشكل أفضل، ابتداءً من خلال تنظيم الحماية من احتمالية التعدي على البيانات الشخصية، ومحاولة احتوائها بصورة أكثر فعالية.

المبحث الثاني: التحديات التي تواجه البيانات الشخصية على شبكة الإنترنت

تعدُّ شبكة الإنترنت أعظم تقنية ابتكرها الإنسان[216]. حيث تقوم بربط آلاف الشبكات الخاصة والعامة ببعضها البعض[217]، وتمكّن مستخدميها في جميع أنحاء العالم من إرسال الرسائل واستقبالها، وتبادل المعلومات بأشكالها المختلفة[218]. وتقدّم خدمات حيوية عدة لمستخدميها تشمل كلًا من؛ الشبكة العنكبوتية العالمية المعروفة (WWW أو الوب)، التي تمكّن من إنشاء المواقع وعرض المعلومات المتنوعة من نصوص وصور ضوئية أو متحركة[219]، ونقل الملفات، وأدوات لتحديد مكان وجود المعلومات على شبكة الإنترنت أو محركات لبحث، المدونات،

---

[216] بدأت شبكة الإنترنت تتشكل في أمريكا أواخر ستينات القرن العشرين وتحديدًا عام 1968. ففي ذلك الوقت كانت وزارة الدفاع الأمريكية قلقة بشأن إمكانية نشوب حرب نووية مدمرة، فبدأت البحث عن وسائل لربط المنشآت الحاسوبية معًا، بطريقة تجعل قدرتها على الاتصال فيما بينها تصمد في مواجهة الحرب. وقامت وزارة الدفاع بتمويل مشروع، بالتعاون مع وكالة مشروعات البحث المتقدم التابع لها، بهدف إنشاء شبكة تستطيع نقل المعلومات العسكرية، والاتصال بالجنود على نطاق الولايات الأمريكية المختلفة، وتضمن استمرارية الاتصال بين السلطات الأمريكية في حال نشوب حرب نووية مباغتة، وأطلقت على هذه الشبكة اسم أربانت (Arpanet). وبالفعل حصل ربط بين حاسوبين في تشرين الثاني (1969)، الأول يقع في مدينة لوس أنجلوس، والثاني في معهد ستانفور للأبحاث داخل مدينة منلو بارك، وكلتا المدينتين تقعان في ولاية كاليفورنيا. وفي كانون الأول (1969)، اتسعت الشبكة لتربط بين أربعة حواسيب، تشمل بالإضافة إلى الحاسوبين السابقين، حاسوبًا ثالثًا في مدينة سانتا بربرا، ورابعًا في جامعة يوتاه، وظلت أربانت تنمو طوال عقد السبعينات على نحو بطيء، وفي عام (1972)، تطورت لتغطي معظم الجامعات الأمريكية مما دعا الحكومة الأمريكية إلى إنشاء هذه الشبكة بصفة رسمية، وبدأ ظهور ما يعرف بشبكة المنطقة المحلية، وبحلول عام (1981)، كان عدد الحواسيب المتصلة بشبكة أربانت يزيد قليلًا على (200) حاسوبًا، ثم قامت وزارة الدفاع بتقسيم الشبكة إلى شبكة أربانت وشبكة أخرى عسكري بحتة، وخلال الثمانينات جرى احتواء أربانت من قبل نسفنت، وهي شبكة أكثر تقدمًا طورتها مؤسسة العلوم القومية، وبعد مرور فترة وجيزة، أصبح هناك ملايين من أجهزة الحاسوب، وآلاف من الشبكات التي تستخدم مراسيم وبروتوكولات خاصة، وقد نشأت الإنترنت الحديثة من ترابط هذه الشبكات، لتربط فيما بعد بين الدول بحيث أصبحت شبكة الشبكات. الكسواني. عامر محمود. (2008)، التجارة عبر الحاسوب، دراسة مقارنة. الطبعة الأولى. الأردن: عمان. دار الثقافة للنشر والتوزيع. ص: 89. ناصيف. (2009) المرجع السابق، ص: 23-24.

[217] ناصيف. (2009). مرجع سابق. ص: 22.

[218] الكسواني. (2008). مرجع سابق. ص: 90.

[219] الكسواني، (2008). مرجع سابق. ص: 90. ناصيف. (2009). مرجع سابق. ص: 27.

الإعلانات الإلكترونية، المنتديات[220]، والتواصل والاتصال والتخاطب والتفاعل المباشر، بالصوت والصورة من خلال مواقع خاصة على الشبكة، كما تقدّم الإنترنت خدمات هائلة للباحثين فالإنترنت تشبه مكتبة ضخمة، تحتوي على قدر كبير من المعرفة يضاهي ما تحتويه ملايين الكتب، كما يستخدم الناشرون الإنترنت للنشر الإلكتروني بوصفها وسيلة لعرض الصحف والمجلات والكتب، وتستخدم الإنترنت الكثير من الشركات للقيام بأعمالها التجارية، وتبيع مؤسسات البيع كل أنواع المنتجات، تقريبًا، على الإنترنت[221].

وفي مقابل المنافع والآفاق الواسعة والفرص الجديدة التي تؤمنها شبكة الإنترنت للأشخاص، تنشأ عنها تهديدات يتعرض لها المستخدمون على الشبكة أكثر من تلك الموجودة في العالم المادي، وذلك بسبب طبيعة شبكة الإنترنت المفتوحة وطابعها الدولي العابر للحدود بين الدول وإمكانية التعامل عن بعد مع أشخاص مجهولين وصعوبة تتبعهم أو مقاضاتهم في بعض الأحيان[222]. وتتصاعد نسبة القلق مع تزايد أعداد مستخدمي الإنترنت وما قد ينتج عن ذلك من انكشاف البيانات الشخصية، ولاسيما تلك التي تستهدف الأشخاص في سمعتهم، أو عبر تهديدهم وابتزازهم والتحرش بهم، والانتقام الجنسي منهم أو التنمر عليهم، نتيجة جمع بياناتهم الشخصية أو تسربها، وخاصة مع جهل غالبية مستخدمي الإنترنت، لحقوقهم ولحقيقة معالجة بياناتهم الشخصية واستخدامها[223]، ولم يرافق ذلك مواكبة فاعلة من قبل الحكومات والمشرعين كما هو الحال في سورية.

---

[220] تقوى، أروى. (2013)، المسؤولية المدنية في مجال الاتصال الإلكتروني. أطروحة دكتوراه. كلية الحقوق. جامعة دمشق. ص: 32-41.

[221] الكسواني. (2008). مرجع سابق. ص: 90-94.

[222] الحجار. (2017). مرجع سابق. ص: 28-29.

[223] الأشقر جبور، جبور، (2018). مرجع سابق. ص 29-30.

ومما سبق عرضه يظهر بوضوح، أنّ التحديات التي تواجه حماية البيانات الشخصية لمستخدمي شبكة الإنترنت ترجع من جهة أولى؛ إلى تحديات تفرضها طبيعة شبكة الإنترنت التي تسهل جمع أنواع مختلفة من المعلومات الشخصية، وتهيئ قدرات جديدة للحكومة والقطاع الخاص لتحليل البيانات الشخصية واستخدامها (المطلب الأول). ومن جهة ثانية؛ إلى تحديات متعلقة بقصور نماذج الحماية وغياب الأطر التشريعية والتنظيمية الملائمة (المطلب الثاني)، وسنناقش فيما يأتي ما تتضمنه كل مسألة من هذه المسائل بالتفصيل.

المطلب الأول: التحديات التي تفرضها طبيعة شبكة الإنترنت

أثّرت شبكة الإنترنت بدرجة كبيرة على مختلف جوانب حياة الأفراد، وأصبح التعامل معها جزءًا من الحياة اليومية، فإذا تعطّل الاتصال بالإنترنت تعطل جانب من حياة مستخدمي الشبكة. كما أدت شبكة الإنترنت إلى ظهور أنماط جديدة من العلاقات القائمة أساسًا على هذه الشبكة، بل وأدّت إلى ظهور علاقات وطيدة بين أفراد التقوا في عالم الإنترنت الافتراضي ولم يلتقوا في الواقع المادي إطلاقًا. وتعمل شبكة الإنترنت على خلق فرص العمل والدراسة وغيرها من الفرص الأُخرى لقدراتها على تحقيق التواصل السريع بين أرجاء العالم، فهي تنطوي على فرص كثيرة لكل من يستطيع استخدامها بكفاءة وذلك بسبب طابعها العالمي، فالدول والحكومات والشركات والأفراد في جميع أنحاء العالم أصبحوا متصلين معًا من خلال هذه الوسيلة التكنولوجية الحديثة، كما أنّ للإنترنت دورًا مهمًا في نقل المعرفة ومختلف العلوم والأخبار في لحظة حدوثها.

وبالرغم من المنافع الكبيرة لشبكة الإنترنت، إلا أنّها أوجدت تهديدًا حقيقيًا، يتمثّل بإمكانية جمع أنواع كثيرة من البيانات الشخصية بسهولة، وتخزينها والوصول إليها وجعلها متاحه وقابلة للاستخدام، من قبل مختلف الجهات

والأشخاص بدون علم أو معرفة أصحابها، أو حتى بدون اهتمامهم بجمعها ومعالجتها، وما قد ينتج عن ذلك من إمكانية الوصول إلى هذه البيانات على وجه غير مأذون به أو عن طريق التحايل، وفتح المجال لإساءة استخدامها أو توجيهها توجيهًا منحرفًا أو خاطئًا أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكمًا خفيًا من واقع سجلات البيانات الشخصية المخزنة[224].

فالتحديات التي تواجه البيانات الشخصية قد تغيرت بشكل كبير مع ظهور واستخدام شبكة الإنترنت، فشبكة الإنترنت تُسهّل إنتاج البيانات الشخصية وجمعها (الفرع الأول)، وتسهّل استخدام البيانات الشخصية في المراقبة والأعمال (الفرع الثاني).

الفرع الأول: دور الإنترنت في تسهيل انتاج البيانات الشخصية وجمعها

رافق تطور البيئة التكنولوجية واستخدام شبكة الإنترنت، زيادة هائلة في إنتاج المحتوى الرقمي بما في ذلك البيانات الشخصية، فالبيانات الشخصية تنشأ في كل ثانية من أي شخص لديه اتصال بالإنترنت، من دون وجود رقابة مباشرة من قبل السلطات المحلية حول تدفق البيانات من الداخل إلى الخارج والعكس؛ كما أنّ شبكة الإنترنت جعلت الوصول إلى المعلومات وتبادلها أسهل وأسرع من أي وقت مضى، وباتت البيانات الشخصية تُستخدم في كافة نواحي الحياة سواء في تقديم الخدمات أو في إنشاء البنية التحتية[225]. فشبكة الإنترنت تنتج أنواعًا جديدة من البيانات الشخصية (أولًا)، كما تقدم وسائل جديدة لجمع البيانات الشخصية (ثانيًا).

---

[224] أيوب. (2009). مرجع سابق. ص: 112-113.

[225] عبد الصادق. (2019/4/14). مرجع سابق.

أولًا: تنتج شبكة الإنترنت أنواعًا جديدة من البيانات الشخصية

طوّرت الإنترنت أنواع البيانات الشخصية، وبذلك لاحقت البيانات الشخصية التطور التكنولوجي، فلم تعد تقتصر على البيانات التقليدية كالاسم واللقب والرقم الوطني ورقم الضمان الاجتماعي والعنوان، بل اتسعت لتشمل صورة الشخص وصوته وسلوكياته وعادته وميوله وأذواقه علاوة على بيانات أخرى لا ترتبط بصورة مباشرة بالشخص الطبيعي، كالمعرفات الفنية مثل بيانات الموقع أو عنوان بروتكول الإنترنت[226]. وعند اتصال المستخدمين بشبكة الإنترنت واستخدام الخدمات التي تقدمها ينتج عن ذلك الكثير من البيانات الشخصية، ونستطيع توضيح ذلك من خلال ما يأتي:

1. إنّ الاتصال بشبكة الإنترنت من خلال الأجهزة المتعددة المتصلة بها التي يستخدمها الأفراد، واستعمال الخدمات المتاحة عبرها كتصفح المواقع الإلكترونية، أو إجراء معاملة إلكترونية، أو شراء سلعة أو خدمة، يترك لدى الموقع المزار مجموعة كبيرة ومتنوعة من المعلومات الشخصية، وجزء من هذه البيانات لازم لإتاحة خدمات الاتصال بالإنترنت والتصفح، وبمجرد الدخول إلى صفحة الموقع فإن هناك معلومات معينة تتوفر عن المستخدم، وهي ما يعرف بمعلومات رأس الصفحة، وهي معلومات يزودها الكمبيوتر المستخدم للكمبيوتر الخادم الذي يستضيف مواقع الإنترنت، وهذه المعلومات تتضمن؛ عنوان بروتوكول الإنترنت العائد للمستخدم ومن خلالها يمكن تحديد اسم النطاق وتبعًا له تحديد اسم الجهة التي قامت بتسجيل النطاق؛ المعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام الأساسية المستخدمة من قبل المستخدم؛ وقت وتاريخ زيارة الموقع؛ مواقع الإنترنت وعنوان الصفحات السابقة

[226]–أيوب. (2009). مرجع سابق. ص: 193–194.

التي زارها المستخدم قبل دخوله الموقع؛ معلومات محرك البحث الذي استخدمه المستخدم للوصول إلى الموقع، وتبعًا لنوع المتصفح قد يظهر عنوان البريد الإلكتروني للمستخدم؛ الوقت الذي قضاه المستخدم في الموقع وبيان المعلومات التي أُرسلت أو اُستقبلت[227].

2. أتاح انتشار استخدام شبكة الإنترنت، نقل النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي، من العالم المادي إلى العالم الافتراضي على شبكة الإنترنت، ونتج عن ذلك قدر هائل من البيانات الشخصية، هذا التداخل بين مشاركة مستخدمي الإنترنت أنشطة الحياة المختلفة على الشبكة، يُخلف بيانات رقمية كثيرة تتصل بالمستخدم على شكل سجلات رقمية تتضمن تفاصيل دقيقة عن المواقع التي قام بزيارتها، والوقت التي قضاه على الشبكة، والأمور التي قام بالبحث عنها والمواد التي قام بتنزيلها، والرسائل التي أرسلها، والخدمات والبضائع التي قام بطلبها وشرائها، فهي سجلات تتضمن تفاصيل دقيقة عن شخصية المستخدم وحياته وهواياته[228].

3. تتميز شبكة الإنترنت بصفة أساسية تميزها عن التقنيات القديمة مثل التلفاز والراديو والهاتف وهي إمكانية التفاعل، فيطلب من المستخدمين دائماً تقديم معلومات عن أنفسهم في كل خطوة مثلاً؛ ما هو البحث المراد؛ وما هي الروابط التي ينقرون عليها؛ وما هي الصفحات التي اطلع عليها ومدة فتحه لهذه الصفحات[229]. ويقدم الأفراد

---

[227] أيوب. (2009). مرجع سابق. ص: 193-194.

[228] فكري. (2007). مرجع سابق. ص: 656.

[229] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 15.

بياناتهم الشخصية عبر الإنترنت، عن قصد وأحيانًا عن غير قصد لأغراض عديدة ومختلفة، مثل شراء السلع والخدمات أو اللعب أو التعلم الإلكتروني أو دفع الضرائب[230].

4. مع تزايد استخدام الإنترنت في التعاملات اليومية، مثل القيام بالأعمال المصرفية والتسوق وزيارة المواقع الإلكترونية، والنشر والتدوين على الشبكة، والتفاعل مع الآخرين على مواقع التواصل الاجتماعي، يزداد كذلك الإفصاح عن البيانات الشخصية دون قصد، بما فيها معلومات حساسة متعلقة بالأوضاع المالية والصحية والمعتقدات الدينية والآراء السياسية والحياة الجنسية، مما يسمح بزيادة حجم المعلومات المجمّعة عن حياة المرء التي تصبح يومًا بعد يوم، سجلاً يتزايد حجمًا مع الاستمرار باستخدام الإنترنت.

ثانيًا: تقدم الإنترنت وسائل جديدة لجمع البيانات الشخصية

أدى استخدام شبكة الإنترنت إلى استحداث وسائل جديدة تمكّن من جمع المزيد من البيانات الشخصية، ومن ثم معالجتها وتحويلها إلى معلومات حول كل من يتصل بشبكة الإنترنت[231]. ويمكن القول إن شبكة الإنترنت أكبر تقنية لجمع البيانات الشخصية وانطلاقًا من هنا سنتعرض لأهم وسائل جمع البيانات الشخصية لمستخدمي شبكة الإنترنت.

---

[230] Council of Europe, Protection of personal data and privacy. Last updated 15/12/2021. Available at: https://www.coe.int/en/web/portal/personal-data-protection-and-privacy

[231] الأشقر جبور، وجبور. (2018). مرجع سابق. ص: 29.

1. ملفات تعريف الارتباط (Cookies): وهي من أشهر الوسائل التي أُبتكرت لتتبع مستخدمي شبكة الإنترنت وجمع بياناتهم، وهي أجزاء نصية صغيرة يخزنها متصفح الإنترنت على جهاز حاسوب المستخدم، وتقوم هذه الملفات بالتسجيل مع متصفح الإنترنت في كل مرة يقوم فيها المستخدم بالدخول على هذا المتصفح ويمكن استخدامها في تتبع الجلسات وتخزين المواقع المفضلة وتصاريح الدخول وغير ذلك[232]. ومع أنّ ملفات تعريف الارتباط وسيلة اتبعت أساسًا لغرض تحسين الخدمات، أو في إطار الأنشطة الدعائية للمواقع الإلكترونية، إلا أنّ ذلك لا يمنع من أنّها تمثل وسيلة لجمع البيانات التي قد لا يرغب الشخص بالكشف عنها، وهي في تطوراتها اللاحقة تمثل وسيلة لتتبع الأشخاص وكشف حياتهم، وإهدار توقعهم في التخفي، وتستخدم الشركات ما تحصل عليه من ملفات تعريف الارتباط لتحديد أهداف وخطط الإعلان، وتقارنه مع ما تجمعه من معلومات لتصبح بيانات متكاملة عن تصرفات المستخدمين على شبكة الإنترنت[233].

2. برامج المراقبة: وهي ملفات لا يراها المستخدم عادةً، وتكون مخفية ضمن صفحات الإنترنت والرسائل الإلكترونية، وعند الاطلاع على الصفحة أو الرسالة الإلكترونية التي تحتوي على ملف المراقبة، يقوم هذا الملف بإرسال معلومات إلى الخادم تشتمل على عنوان بروتوكول الإنترنت الخاص بالمستخدم، وموعد وتاريخ الدخول على الصفحة أو فتح الرسالة الإلكترونية ونوع المتصفح المستخدم[234]. كما أنّها وسيلة تجمع بوساطتها جهات الرقابة الحكومية في دول كثيرة، حتى تلك المتطورة منها، أكبر قدر من المعلومات السرية والخاصة، وغالبًا لأهداف سياسية أو اقتصادية،

---

[232] مندل، بوديفات، واجنر، هوتن، وتوريس.(2012). مرجع سابق. ص: 14.

[233] أيوب. (2009). مرجع سابق. ص: 198-199.

[234] مندل، بوديفات، واجنر، هوتن، وتوريس. -(2012). مرجع سابق. ص: 14.

ما يشكّل اعتداءات على البيانات المستهدفة، ولذلك تزدهر صناعة برامج التجسس وتطويرها، لرصد البيانات عبر شبكة الإنترنت[235].

3. مواقع التواصل الاجتماعي[236]: تتضمن مواقع التواصل الاجتماعي تطبيقات مختلفة على الإنترنت تسمح للمستخدم بإنتاج المحتوى وتحميله وتبادل المعلومات في عدة اتجاهات[237]. ويظهر تأثير وسائل التواصل الاجتماعي ليس فقط من خلال عدد المستخدمين الكبير والمتزايد بل أيضًا من خلال الدور الذي تؤديه في حياتهم، فوسائل التواصل الاجتماعي أتاحت للأشخاص مجالًا أوسع للتعبير عن الرأي والوصول إلى شريحة واسعة من الأشخاص ودون أي كلفة، ولكن من جهة أخرى أصبحت تعرضهم لمخاطر انتهاك خصوصيتهم[238] وبياناتهم الشخصية وغير ذلك من حقوقهم وحرياتهم. وتعدّ مواقع التواصل الاجتماعي أكثر المواقع انتاجًا للبيانات[239]. ولا يزال موقع فيسبوك هو الأهم في ميدان المراسلات والتفاعل بين الأصدقاء ونشر الصور والفيديوهات والمنشورات المختلفة بحجم مستخدمين يتجاوز (2.234) مليار مستخدم نشط شهريا، وبانتشار شاسع في أكثر من (120) دولة حول العالم، ويستخدم واتساب أكثر من (1.500) مليار مستخدم نشط شهريا حول العالم، ويستخدم فيسبوك ماسنجر أكثر من (1.300) مليار مستخدم نشط شهريًا بعد أن كان في بداياته عام (2016) لا يستخدمه أكثر من (200) مليون

---

[235] أيوب. (2009). مرجع سابق. ص: 200-201.

[236] مواقع التواصل الاجتماعي هي مواقع إلكترونية تركز على بناء أو إظهار العلاقات الاجتماعية بين الأفراد، وتعمل على تسهيل الصداقات الافتراضية مع الأفراد المعروفين للمستخدم في الواقع، مما يسمح لهم بمشاركة الصور وتبادل الحديث على الإنترنت، ويسمح النموذج الموحد للمستخدمين بإنشاء صفحتهم الخاصة بهم والتي تحتوي على بعض المعلومات الشخصية مثل تاريخ الميلاد ومكان التواجد والاهتمامات والاسم، ويمكن بعد ذلك للمستخدمين الارتباط مع أصدقاء سيتمكنون عندئذ من رؤية معلومات بعضهم البعض، وتنتشر مواقع التواصل الاجتماعي بشكل كبير مع استقطاب مئات الآلاف من المستخدمين بينهم. مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 20.

[237] الحجار. (2017). مرجع سابق. ص: 8.

[238] الحجار. (2017). مرجع سابق. ص: 9.

[239] إحصائيات السوشيال ميديا في 2020: https://www.dimofinf.net/blog/s/2020

مستخدم شهري، ويصل العدد إلى أكثر من مليار مستخدم نشط على انستغرام[240]. ويتزايد القلق بشأن انتهاك البيانات الشخصية التي تسببت فيها هذه المواقع، وبصورة خاصة لأنّ الكثير من مستخدمي هذه المواقع غير مدركين لمخاطر انكشاف بياناتهم الشخصية ومعالجتها، فلا يمارس الكثير من المستخدمين أي قيود في عرض بياناتهم الشخصية، من معلومات تفصيلية عن حياتهم، وصور شخصية أو عائلية، بل والسماح لأي شخص برؤيتها، بالإضافة لتكوين صداقات مع أفراد لا يعرفونهم مطلقًا أو لا يعرفونهم بشكل كافٍ.

4. محركات البحث: تقوم محركات البحث بدور حيوي كوسيط على الإنترنت يسمح للأفراد بالبحث عن المحتويات والاطلاع عليها، وتقوم بجمع قدر هائل من البيانات الشخصية، بما في ذلك عناوين بروتوكول الإنترنت وطلبات البحث والوقت والتاريخ والمكان الذي قدم فيه الجهاز طلب البحث، ويمكن أن تكون هذه البيانات قابلة لتحديد الهوية الشخصية، ويمكن أن تكشف عن أجزاء حساسة من المعلومات مثل المعتقدات السياسية للشخص أو ميوله الجنسية أو معتقداته الدينية أو حالته الصحية، وعادة تُستخدم هذه المعلومات لأغراض التسويق[241].

إنّ التفاعلات الاجتماعية التي تحدث عبر شبكة الإنترنت، ولا سيما في منصات وسائل التواصل الاجتماعي ومحركات البحث، والتقنيات الأُخرى أتاحت قدرة فائقة على جمع المعلومات، ومع أنّها أوجدت بعض الفوائد لكنها أيضًا هددت حقوق الإنسان وحرياته الأساسية، وفي إطار هذا البحث هددت الحق في حماية البيانات

---

[240] 100 Social Media Statistics for 2019. https://statusbrew.com/insights/social-media-statistics-2019/

[241] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). ص: 21.

الشخصية، وهو ما هيأ الفرصة لزيادة المخاطر على حقوق الإنسان، إذا جمعت هذه البيانات بطريق غير مشروع، أي في الأحوال التي تكون البيانات مما لا يجوز جمعها بحكم القانون أو بدون موافقة صاحبها.

وفي ظل عدم وجود قواعد قانونية فإنّ جمع بيانات مستخدمي شبكة الإنترنت يؤدي إلى تسليع هذه البيانات واستخدامها لخدمة مصالح أصحاب هذه المواقع، دون اعتبار لحقوق أصحابها، مما يحرم مستخدمي الشبكة من حقهم في حماية بياناتهم الشخصية، التي تعبّر عن شخصيتهم الإنسانية، ويجعل احتمال انتهاك حقوق مستخدمي الشبكة وحرياتهم الأخرى، ولا سيما الحق في الحياة الخاصة، أكثر من السابق.

الفرع الثاني: دور الإنترنت في تسهيل استخدام البيانات الشخصية في المراقبة والأعمال التجارية

كثيرًا ما كانت معالجة البيانات الشخصية جزءًا لا يتجزأ من التفاعل البشري، إلا أنّها اتخذت أبعادًا وإمكانات غير مسبوقة في عصرنا الحالي، فأصبحت معالجة البيانات الشخصية تستخدم في خطط المراقبة وتنمية الأعمال التجارية، فعلى سبيل المثال يعتمد اقتصاد الإنترنت على الأشخاص الذين يقدمون بياناتهم في مقابل خدمات مجانية من حيث الظاهر، وفي الوقت نفسه تزداد شهية الحكومات للحصول على المعلومات، وهذا الأمر أكثر وضوحًا مع المراقبة التي تمارسها الأجهزة الأمنية، كما يتضمن تقديم الخدمات للأفراد من قبل الحكومات على معالجة مكثّفة للبيانات الشخصية، وقد سوغت المعالجة المكثفة للبيانات من أجل ضمان تقديم الخدمات إلى المواطنين الذين يحتاجون إليها أو المؤهلين قانونًا بالحصول عليها، وكان لهذا التسويغ دور بارز في رغبة الهيئات

الحكومية لمعرفة المزيد من البيانات عن مواطنيها[242]. وفيما يأتي مناقشة للتحديات الناشئة عن معالجة البيانات الشخصية واستخدامها في المراقبة والأعمال التجارية.

أولًا: استخدام البيانات الشخصية في المراقبة.

مع تطور وسائل الاتصال ولا سيما الإنترنت، وظهور الاتصالات الرقمية التفاعلية غير المكلفة، وتصاعد استخدام الأجهزة المتصلة بالإنترنت كالهواتف الخلوية وغيرها الكثير من الأجهزة الأُخرى، تدفقت البيانات الشخصية وأصبحت القدرة على مراقبة الأفراد أسهل وأقل كلفة وأكثر فعالية، مقارنة بالوقت السابق على وجود الإنترنت حيث كانت مراقبة الأفراد معقدة ومكلفة جداً[243]. كما أتاحت الإنترنت القدرة على معالجة البيانات الشخصية وعلى هذا الأساس ازدادت المخاطر التي تواجهها هذه البيانات، الأمر الذي مثّل تهديدًا بانتهاك البيانات الشخصية. فالسلطات في العالم تقوم بأكثر من مجرد تخزين البيانات، فهي تستخدم البيانات للرقابة والتمييز والحد من حرية التعبير، كما تستخدم الشركات المراقبة للتلاعب ليس فقط بالمقالات الإخبارية والإعلانات التي نراها ولكن أيضًا بالأسعار التي تقدمها عبر شبكة الإنترنت. ويشارك كلا الجانبين هذه المعلومات مع بعضهما البعض، أو ربما الأسوأ من ذلك، يفقدانها أمام مجرمي الإنترنت في خروقات ضخمة للبيانات. والكثير من هذه الرقابة تحدث بصورة طوعية، فنحن

[242] Bygrave. (2014). Previous reference. P: 4.

[243] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 13.

نتعاون مع مراقبة الشركات لأنها تعدنا بالراحة، ونخضع للمراقبة الحكومية لأنها تعدنا بالحماية، والنتيجة هي مجتمع مراقب جماعيًا[244].

1. البيانات الشخصية والرقابة الحكومية.

إنّ جمع البيانات الشخصية واستخدامها من قبل الحكومات ليست ظاهرة حديثة، بل هو أحد أسباب اعتماد الجيل الأول من قوانين حماية البيانات، وهي أقدم مجموعة من التشريعات والتي اعتمدتها بعض الدول مثل ألمانيا والسويد والولايات المتحدة الأمريكية وكندا وفرنسا في سبعينيات القرن الماضي، بعد أن أثارت قواعد البيانات الكبيرة التي تملكها وتحتفظ بها الحكومات قلقًا بين المدافعين عن الخصوصية والمواطنين أيضًا، وذلك عندما استخدمت الحكومات المعلومات الشخصية لأغراض أخرى غير تلك التي جمعت المعلومات من أجلها في البداية، بالإضافة إلى أنّ الإدارة السيئة للبيانات الشخصية، أدّت إلى اختراق قواعد البيانات الحكومية، والوصول إلى البيانات الشخصية بطرق غير مشروعة ولأغراض شائنة، وبالتالي فإن المخاوف الناتجة عن تخزين البيانات الشخصية واستخدامها من قبل الحكومة، أدت إلى اعتماد تشريع يحاسب الحكومة على انتهاكات هذه البيانات[245].

لقد كانت الحكومات تستفيد أقصى ما يمكنها من تقنيات المراقبة، ولكن منذ أحداث الحادي عشر من أيلول، تحول تهديد الإرهاب إلى دافع في الكثير من البلدان لزيادة استخدام أساليب المراقبة[246]. وقامت العديد من

---

[244] Data and Goliath, The Hidden Battles to Collect Your Data and Control Your World. A Book by Bruce Schneier. Last updated: 20\5\2021. Available at: https://www.schneier.com/books/data_and_goliath/

[245] Stefanick. (2011). Previous reference. P: 43.

[246] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 18.

الحكومات بزيادة برامج المراقبة الخاصة بها ووسعت ممارساتها في جمع المزيد من البيانات عن الأفراد[247]، ومما لا شك فيه أنّ الوصول إلى المعلومات الشخصية للأفراد أمر بالغ الأهمية في هذا الصدد. ولكن تصاعد حركة إنشاء السجلات الحكومية، وعملية جمع البيانات الشخصية، أدت إلى ظهور بعض الممارسات والقوانين، التي تميل إلى ترجيح كفة الأمن، على كفة مصالح الأفراد لاسيما تلك المتعلقة بحماية حقوقهم وحرياتهم بحجة حماية الأمن ومواجهة الإرهاب[248]. والمثال الذي يمكن إثارته في هذا الصدد، عن التشريعات التي وضعت تحت عنوان مكافحة الإرهاب، فقد أقرّت الولايات المتحدة الأميركية صلاحيات واسعة للحكومة، وأعطَت هامشًا أوسع للتحقيق، واستبعدت المسؤولية عن أشخاص القانون الخاص، في حال إفشائهم معلومات للحكومة، وقد أعرب البرلمان الأوروبي عن قلقه إزاء الأثر الذي يمكن للإجراءات الهادفة لحماية الأمن أن تتركه على الحقوق والحريات[249].

كما استطاعت بعض الحكومات أن تستخدم هذه التقنيات في مراقبة أعمال المواطنين، ولا سيما المعارضين بشكل أكثر كثافة من السابق، وتمكّنت الحكومات من الحصول على البيانات الشخصية من مصادر جديدة، ففي بعض الحالات، يطلب المسؤولون الحكوميون من مزودي خدمة الإنترنت تقديم معلومات عن مستخدم الإنترنت المشتبه بارتكابه عملًا إجراميًا، وفي حالات أخرى، يخضع أعضاء المعارضة للمراقبة بشكل غير قانوني، وهو ما يعد انتهاكًا لحقوقهم الإنسانية[250]. ومن الممارسات الأخرى استخدام قوائم المراقبة السرية، حيث يقوم المسافرون

---

[247] Lloyd. (2011). Previous reference. P: 17-18.

[248] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص18.

[249] جبور الأشقر؛ جبور. (2018) مرجع سابق. ص: 38.

[250] Hirsch, Dennis. D. (2011). The law and policy of online privacy: Regulation, self-regulation or co-regulation? Seattle University Law Review. Vol 34. P. 451

بتقديم البيانات الشخصية كونه شرط من شروط السفر، وعند التحقق من هذه المعلومات تقارن بقواعد البيانات من مصدر آخر، وتستخدم هذه البيانات في إنشاء قوائم للأفراد المصنفين على أنّهم تهديد للأمن، وتعمم القائمة على الدول الأخرى، ثم يُمنع الأفراد من السفر أو يخضعون إلى تدابير أمنية معززة، وقد تبين احتواء هذه القوائم على أخطاء، الأمر الذي أدى إلى تشويه سمعة بعض الأفراد، وأحياناً تحفظ القوائم سراً ما يعني حرمان بعض الأفراد من التأشيرة دون إدانتهم بالضرورة بأي شيء، ودون منحهم الفرصة للدفاع عن أنفسهم[251]. وبالإضافة لما سبق تستخدم العديد من الدول، برامج رقابة متطورة، وتقارن بين ما تسلمها إياه شركات الاتصال الكبرى، وما تجمعه الإدارات والأجهزة الحكومية من بيانات ومعلومات، نتيجة تعقب الأفراد عبر تطبيقات تحديد المواقع، وبيانات الاتصال والبيانات الجغرافية الموجودة على الصور، التي يتبادلونها في مواقع التواصل الاجتماعي من هواتفهم وبريدهم الإلكتروني، ولوائح أصدقائهم وأفراد عائلتهم. وقد أشارت أجهزة الاستخبارات البريطانية في مستندات سرية، إلى أنّ القدرة على التجسس، موجودة في برامج الألعاب الأكثر انتشارًا، ولاسيما عندما تسمح بتحديد موقع الشخص وعمره وجنسه، وغير ذلك من بياناته الشخصية، وما يمثله هذا الواقع من تهديد جدي للحريات المدنية وحقوق الشخصية الأخرى[252]. وكان قد أشار التقرير المعني بمكافحة الإرهاب وحقوق الإنسان إلى أمثلة عن ممارسات المراقبة في ألمانيا وكولومبيا وبنجلاديش والولايات المتحدة الأمريكية، والتأثير المثبط للمراقبة على مستخدمي شبكة

[251] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 18.

[252] الأشقر جبور، جبور. (2018). مرجع سابق. ص: 41-42.

الإنترنت وخشيتهم من زيارة بعض مواقع الأنترنت والتعبير عن آرائهم أو الاتصال بأشخاص آخرين مخافة أن تطالهم العقوبات[253].

وفي هذا الإطار تحتل أخبار انتهاك البيانات الشخصية الصفحات الأولى في وسائل الإعلام، وتنتشر أخبار تعامل الأجهزة الحكومية المختلفة مع البيانات الشخصية، من منطلق ضرورة الرقابة والسيطرة، الأمر الذي يؤكد لجوء الحكومات إلى ممارسة الرقابة الشاملة، وعلى استغلال البيانات الشخصية، في عمليات رقابة شاملة ورصد التحركات، لم يسبق لها مثيل، أثارت موجة من الاستياء حول العالم بلغت ذروتها، مع الفضيحة التي فجرها إدوارد سنودين عام (2013)، حول الرقابة التي تقوم بها أجهزة الاستخبارات الأميركية، فالتحول إلى الرقابة الشاملة، والتحكم بوسائل الاتصالات المختلفة، وجمع البيانات لتعقب الأفراد[254]، تهدد الحقوق والحريات إضافة إلى تقويضه لأسس أي نظام سياسي يحترم حقوق الإنسان. وفي كل ما تقدم، دليل على أهمية البيانات الشخصية وضرورة حمايتها، لمنع استخدامها في المساس بحقوق الأفراد، فقد أصبح واضحًا للعالم، أن التقدم التكنولوجي لا يمرّ دون مخاطر جديدة تشكل تهديداً على الحريات والحقوق لا يمكن للمشرع تجاهلها، لذا لا بد من رسم حدود واضحة لا يمكن للدولة أن تتجاوزها، منعًا للاعتداء على حقوق الأفراد وحرياتهم.

---

[253] الجمعية العامة للأمم المتحدة، مجلس حقوق الإنسان، البند الثالث من جدول الأعمال، تعزيز كافة حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية. تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، السيد مارتين شاينين. تاريخ آخر اطلاع 2022/6/15. على الموقع الآتي:
http://hrlibrary.umn.edu/arabic/AR-HRC/AHRC13-127.pdf

[254] الأشقر جبور، وجبور. (2018). مرجع سابق. ص: 42-45.

2. البيانات الشخصية ورقابة الجهات الخاصة.

إنّ الحكومات أو الجهات العامة لا تمارس وحدها تقنيات المراقبة، وإنما أيضًا الجهات الخاصة تستخدم تقنيات المراقبة بشكل أكبر، فعلى المستوى المحلي يرصد سلوك أفراد الأسرة والموظفين. فبدلاً من مراقبة الموظفين الذين يظهرون سلوكاً مريباً، يقوم أصحاب العمل بمراقبة دائمة لمكان العمل، وهناك ابتكار وتطوير دائم لتقنيات جديدة تساعد أصحاب العمل على مراقبة الموظفين[255]. كما تبرز شبكات التواصل الاجتماعي، بوصفها شكل جديد من أشكال التحكم الاجتماعي، حيث يمكن لأي شخص، مراقبة نشاط شخص آخر وتحركاته. وتتم هذه الرقابة، على مستويين، الأول مرئي ويقوم به أصدقاء ومعارف وعائلة الشخص المعني بالبيانات، أو متتبعو نشاط هذا الشخص عمومًا، والثاني غير مرئي وتقوم به البرامج والتطبيقات المتخصصة في رصد وتحليل الاهتمامات الشخصية، والتي تستخدمها المواقع المختلفة، ومحركات البحث[256].

ثانيًا: استخدام البيانات الشخصية في الأعمال التجارية.

تظهر أهمية البيانات الشخصية في الأعمال التجارية من حاجة الشركات لمعرفة المزيد عن عملائها من أجل تحسين الخدمات المقدمة لهم، فالشركات تحتاج إلى معلومات شخصية عن المستهلكين فيما يتعلق باختيارهم وتفضيلاتهم لغرض الإعلان المستهدف والتسويق المباشر[257]. فالشركات الكُبرى تستخدم البيانات الشخصية في مجال تطوير المنتجات والإعلانات، عبر تحليلها وتحليل ميول الأشخاص الطبيعيين، وتحديد حاجاتهم وعاداتهم

[255] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 19.

[256] الأشقر؛ جبور، (2018). مرجع سابق. ص: 34.

[257] Birnhack. (2008). Previous reference. P: 510.

الاستهلاكية واهتماماتهم[258]. فاقتصاد الإنترنت يعتمد على الأشخاص الذين يقدمون بيانات عن أنفسهم سواء عن قصد أو عن غير قصد، في مقابل خدمات مجانية من حيث الظاهر[259].

وتعدّ المواقع على شبكة الإنترنت والمعلنين على الشبكة مستخدمين رئيسيين للمعلومات الشخصية على الإنترنت. فالمعلنون على الشبكة مسؤولون عن الإعلانات التي يراها المستخدمون عند زيارة الموقع، ويدخلون في علاقات تعاقدية مع مالكي المواقع لتزويدهم بالبيانات الشخصية، وبالإضافة إلى المواقع على شبكة الإنترنت والمعلنين عبرها، هناك مستخدمون آخرون للبيانات الخاصة مثل سماسرة البيانات والمستخدمين الثانويين[260].

1. القيمة المالية للبيانات الشخصية.

تمثل بيانات المستخدم قيمة اقتصادية كبيرة[261]، ولذلك ليس من المستغرب وصف البيانات الشخصية بأنّها النفط الجديد للإنترنت والعملة الجديدة للعالم الرقمي[262]. فالبيانات الشخصية بالإضافة إلى كونها سلعة في حد ذاتها، فإنّها المحرك والوقود في مجتمع المعلومات[263]. ويُشار إلى البيانات الشخصية بأنّها أهم سلعة في السوق في أيامنا هذه، وهي أكثر قيمة من الذهب، فنحن الأصل الذي تريده كل شركة وحكومة[264]. فهي مورد جديد للقيمة

[258] الأشقر جبور، جبور. (2018). مرجع سابق. ص: 29-30.

[259] Bygrave. (2014). Previous reference. P: 4.

[260] Hirsch. (2011). Previous reference. P: 447.

[261] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 19-20.

[262] Kuneva, Meglena. Roundtable on Online Data Collection, Targeting and Profiling: "Personal data is the new oil of the internet and the new currency of the digital world". Last updated: 20\5\2021. Available at: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

[263] Lloyd. (2011) Previous reference. p: 15.

[264] Craig, Terence, Ludloff, Mary.E. (2011). Privacy and big data. Published by O'Reilly Media. United States of America. Back cover page.

في القرن الحادي والعشرين، تظهر على أنّها فئة أصول جديدة تمس جميع جوانب المجتمع[265]. فقد نتج عن الإنترنت كم هائل من الأنشطة الاقتصادية، وتقدر دراسة أجراها مؤخراً معهد (McKinsey) أن التأثيرات الاقتصادية المباشرة وغير المباشرة للإنترنت تمثل (3.4%) من إجمالي الدخل القومي في (13) دولة خضعت للدراسة[266].

فالتحول الرقمي للمعلومات وتوقع حرية الدخول يجعل من الأشكال التقليدية لتحقيق الدخل أمراً أكثر تعقيداً على الإنترنت، ومن ثم تقوم الشركات بالتنقيب عن البيانات الشخصية حتى تستهدف المستخدمين بدعاياتها، ولهذا يوجد حافز اقتصادي مباشر وقوي لتأمين البيانات الشخصية والاحتفاظ بها ومشاركتها[267]. ومع التحول الرقمي الذي تطبقه الحكومات، سواء في تقديم الخدمات أو في إنشاء البنية التحتية، وتصاعد دور الاقتصاد الرقمي في نمو الاقتصاد العالمي، أصبح للبيانات قيمة أكبر من أي عهد مضى في خلق الوظائف ودعم عملية الإبداع والابتكار، وأصبحت من ضمن ركائز القوة الاقتصادية للدولة[268].

2. المخاوف المتعلقة باستثمار البيانات الشخصية لمستخدمي شبكة الإنترنت

تعتمد جل الأنشطة الاقتصادية على شبكة الإنترنت اعتماداً متزايداً على وسطاء الإنترنت[269]، للوصول إلى البيانات ومعالجتها، ونشأ عن القوة المتزايدة لوسطاء الإنترنت وتحكمهم في البيانات الشخصية، عدداً من

---

[265] World Economic Forum (WEF). (2011) .Personal data: The emergence of a new asset class.. P. 34. Last updated: 21/3/2021. P: 5. Available At: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

[266] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 19.

[267] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 15.

[268] عبد الصادق. (2019/4/14). الثورة الصناعية الرابعة. مرجع سابق.

[269] مجموعة من أصحاب المصلحة والخدمات والتطبيقات التي تسهل من التعاملات بين الأطراف الأخرى على الإنترنت بما في ذلك على سبيل المثال محركات البحث ومزودي خدمات الإنترنت. مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 20.

المخاوف المتعلقة فيما إذا كانت القوانين السارية كافية لحماية الأشخاص، فشركات الإنترنت مثل غوغل وفيسبوك تتمتع بحرية الوصول إلى كم هائل من البيانات، وهي أكثر شركات الإنترنت التي لديها قواعد مستخدمين هائلة، وتعتمد نماذج عملها في تقدم الكثير من الخدمات، على جمع معلومات المستخدم وتستخدمها بصورة رئيسية لغرض التسويق[270].

إنّ التضخم الهائل في حجم البيانات الشخصية واستخدامها للأغراض التجارية، هو أحد أهم القضايا المثيرة للجدل[271] على شبكة الإنترنت التي لا حدود لها، والتي أتاحت التدفق الحر للبيانات عبر الحدود الوطنية[272]. فالبيانات الشخصية الرقمية التي تم تنشأ بوساطة الأشخاص وعنهم، تولّد موجة جديدة من الفرص لخلق قيمة اقتصادية واجتماعية، ولكن تزايد أهمية تدفق البيانات من أجل تعزيز التجارة الدولية أبرز تحديات جديدة، فظهرت الحاجة إلى تنظيم حدود لتدفق البيانات الشخصية عبر الحدود الوطنية[273].

وفي هذا الإطار، تحتل أخبار الاتجار بالبيانات الصفحات الأولى، في وسائل الإعلام والمثال الذي يمكن طرحه هنا مساءلة مارك زوكربيرغ، مالك فيسبوك، عن فضيحة استثمار البيانات الشخصية لمستخدمي الموقع، ونقلها إلى جهات ثالثة، قد أثارت انتباه العالم، حول خطورة الاعتداءات على بيانات مستخدمي شبكة الإنترنت، ومدى اجتياحها لحياتهم، ولاسيما عندما تجمع هذه البيانات دون علم صاحبها ودون موافقة صريحة منه، ودون

---

[270] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 19-20.

[271] Kuneva. Previous reference.

[272] Council of Europe. Protection of personal data and privacy. Last updated 15/12/2021. Available at: https://www.coe.int/en/web/portal/personal-data-protection-and-privacy

[273] World Economic Forum (WEF). (2011). Previous reference. P: 5.

مسوغات قانونية. هذا عدا عن إضاءتها للتهديدات التي يشكلها قطاع الإعلانات الرقمية، ولاسيما عندما يلجأ إلى أساليب تحليل البيانات لمعرفة علاقات صاحبها واهتماماته، وتحديد ما يمكن أن يثير اهتمامه من خدمات، ومنتجات وبضائع ومعلومات. وتصبح الأمور مقلقة أكثر، فيما لو نظرنا إلى حجم البيانات، التي يجمعها محرك البحث غوغل، ومدى متابعته حركة المبحرين على الإنترنت، وتسجيل الوقت الذي يمضونه على المواقع المختلفة، وفي استخدام التطبيقات، وبعض المنصات الرقمية[274].

إنّ القطاع الخاص يمثل تحديًا أكبر بكثير للبيانات الشخصية من الحكومة، لأن الشركات على عكس الحكومة، يتصف استخدامها للبيانات الشخصية بالشمولية، كما أنّه لا يقتصر على استعمال محدد، فقد أصبح للبيانات الشخصية قيمة للأغراض التجارية أكثر من أي غرض آخر، فكل ما يفعله مستخدم شبكة الإنترنت ينتج بيانات، وهذه البيانات قيّمة للغاية للقطاع الخاص، وأهميتها بالنسبة له أكثر منها للحكومة، فالحكومة في الأوقات العادية، تهتم فقط بأن يلتزم مستخدم الشبكة بالقوانين، لكن القطاع الخاص مهتم بأكثر من ذلك، على سبيل المثال كيف ينفق مستخدم شبكة الإنترنت أمواله، والبيانات توضح ذلك. ومع وجود كميات هائلة من البيانات حول ما يفعله مستخدم شبكة الإنترنت وما يقوله، يزداد التسويق بطريقة مباشرة وفعّالة، فعلى سبيل المثال يقوم (Gmail) بمعالجة البيانات الموجودة في بريدك الإلكتروني لمعرفة ما يجب أن يحاول بيعه، وهناك قائمة لا حصر لها من الكيانات التي ترغب في معرفة المزيد عن مستخدمي الشبكة، على الأقل لخدمة مصالحها بشكل أفضل[275].

---

[274] الأشقر جبور، جبور. (2018). مرجع سابق. ص: 30-31.

[275] Lessig, Lawrence. (2006). Code version 2.0. Published by Basic Books. United States of America: New York .p: 216.

إن للمعلومات الشخصية قيمة اقتصادية في المجتمع الذي تحركه تكنولوجيا المعلومات، ومع ذلك، فإن المخاطر المرتبطة بمعالجة البيانات الشخصية غير المنظمة تتجاوز بكثير قيمتها الاقتصادية والتجارية[276]. وتتشكل مصادر الخطر على البيانات الشخصية، نتيجة الاستخدام غير القانوني للبيانات الشخصية، دون اعتبار لحقوق أصحابها، وهذا هو السبب في إيلاء اهتمام كبير للبيانات الشخصية لضمان توفير الحماية القانونية الكافية لها.

المطلب الثاني: التحديات المتعلقة بقصور نماذج الحماية وغياب الأطر التشريعية والتنظيمية الملائمة

لم تحظَ البيانات الشخصية بالحماية الدستورية والتشريعية الكافية في سورية، فالدستور السوري الذي صدر في العقد الثاني من القرن الحادي والعشرين، لم يتضمن نصًا صريحًا يعترف بحق الأفراد في حماية بياناتهم الشخصية في ظل مخاطر التطور التكنولوجي الراهن. كما لا توجد حماية كافية في التشريعات السورية الحالية، ولم يسن المشرع إلى الآن قانونًا خاصًا بحماية البيانات الشخصية. في حين توظف الحكومة التكنولوجيا في جمع كم هائل من البيانات الشخصية[277]، وغالبًا ما تحظى الأجهزة الأمنية بحرية الوصول إلى البيانات الشخصية للمواطنين دون قيد أو شرط، وتستغل الشركات الخاصة هذه المعلومات لأهداف ربحية دون علم أصحابها أو موافقتهم على ذلك[278].

---

[276] World Economic Forum (WEF). Previous reference. P. 8.

[277] أكسس ناو. (يناير 2021). عرضه للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال أفريقيا. ص: 3. تاريخ التحميل (2022/1/25) متاح على الرابط:
https://www.accessnow.org/cms/assets/uploads/2021/03/AR_Data-Protection-MENA.pdf

[278] أكسس ناو. (يناير 2021). مرجع سابق. ص: 3.

وفي ظل الفراغ التشريعي في سورية من قانون خاص بحماية البيانات الشخصية، كان لا بد من مراجعة التشريعات السورية ذات العلاقة بحماية البيانات الشخصية؛ لتوضيح مدى قصورها في تقديم حماية كافية للبيانات الشخصية؛ وأهمية وجود قواعد خاصة لتنظيم معالجة البيانات الشخصية، في ظل التطور التكنولوجي والاستخدام الواسع للبيانات الشخصية على شبكة الإنترنت[279]. من خلال البحث في حماية البيانات الشخصية ضمن نطاق حماية الخصوصية (الفرع الأول)، وحماية البيانات الشخصية ضمن نطاق حماية سرية البيانات والمعلومات (الفرع الثاني).

الفرع الأول: حماية البيانات الشخصية ضمن نطاق حماية الخصوصية

إنّ الوثائق المتعلقة بحقوق الإنسان وحرياته الأساسية، وأبرزها الإعلان العالمي لحقوق الإنسان لعام (1948)، والعهد الدولي الخاص بالحقوق المدنية والسياسية لعام (1966)، والاتفاقية الأوروبية لحقوق الإنسان لعام (1950)، تشكّل الأساس الرسمي للقوانين والسياسات المتعلقة بحماية البيانات الشخصية. ويمكن القول إن مجموعة واسعة من الحقوق والحريات في هذه الوثائق الدولية تلهم المبادئ الموجودة في قوانين حماية البيانات

[279] وتجدر الإشارة إلى أنّ أوّل قانون عربي لحماية البيانات الشخصية صدر في تونس عام (2004)، ولاحقاً أصدرت دول عربية قوانين مماثلة، في الإمارات عام (2007)، والمغرب عام (2009)، وقطر عام (2016)، ومصر عام (2020). أنظر: عزام، إسماعيل (2018/3/3). الأمية الرقمية تجعل خصوصية العرب على الإنترنت وهمًا كبيرًا. 2020/9/20.
https://www.dw.com/ar/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9/s-9106
وتشير الإحصاءات العالمية الحديثة، أنّ نحو (137) دولة من أصل (194) دولة اعتمدت تشريعات لتأمين حماية البيانات والخصوصية، في جميع أنحاء العالم، أي بنسبة تعادل (70%) من دول العالم، وتبذل دول أخرى جهودًا من خلال صياغة مشاريع قوانين بنسبة تعادل (9%). أما نسبة الدول التي ليس لديها أي تشريعات أو مشاريع قوانين لحماية البيانات الشخصية فتعادل فقط (15%) من دول العالم. أنظر:
UNCTAD. Data Protection and Privacy Legislation Worldwide. Last updated: 24\4\2022. Available at:
https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

الشخصية، ومع ذلك فإن الحق في الخصوصية أو الحياة الخاصة هو الذي يُنظر إليه عمومًا على أنه يشكل الأساس المركزي لمبادئ حماية البيانات الشخصية[280].

ومن هنا، ولعدم وجود حماية خاصة بالبيانات الشخصية في المنظومة التشريعية السوريّة، كان من المنطقي بحث الحماية القانونية للخصوصية في القانون السوري (أولًا)، لتوضيح مدى قصورها في تأمين الحماية للبيانات الشخصية (ثانيًا).

أولًا: الحماية القانونية للخصوصية في القانون السوري

حظيت الخصوصية بحماية دستورية وقانونية كبيرة في سورية وشهدت السنوات الأخيرة استجابة تشريعية على مستويات مختلفة لدواعي هذه الحماية، فقد اعترف المشرع السوري بحق الأفراد في الخصوصية وحماية حياتهم الخاصة ليس فقط بمقتضى النصوص القانونية العادية، بل من خلال الاعتراف بالحق في الحياة الخاصة أو الخصوصية على أنّه حق دستوري، وأضحى انتهاك الحياة الخاصة من قبل الأفراد أو الدولة مخالفًا لأحكام الدستور، حيث تقر المادة (1/36)[281] بحرمة الحياة الخاصة، كما عدّت المادة (54)[282] أنّ الاعتداء على حرمة الحياة الخاصة جريمة، وهو تأكيد للحماية التي أولاها الدستور لخصوصية الأفراد. ولم يقتصر الأمر عند هذه النقطة فقد أفرد الدستور عدداً من المواد لحماية مظاهر الحياة الخاصة، فنص على حرمة المساكن في المادة (2/36)[283]،

---

[280] Bygrave. (1998). Previous reference. P: 247-249.

[281] الدستور السوري النافذ بتاريخ (27) شباط لعام (2012) المادة (1/36): "للحياة الخاص حرمة يحميها القانون".

[282] الدستور السوري المادة (54): "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".

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

وعلى سرية المراسلات البريدية والاتصالات السلكية واللاسلكية في المادة (37)[284]، وبهذا يكون الدستور السوري قد نص على الحق في الحياة الخاصة على أنَّه حق مستقل، كما نصّ على تطبيقات عملية في إطار حماية هذا الحق. بالإضافة إلى النص على حماية حرية الاعتقاد في المادة (1/42)[285]، وحماية الحرية الشخصية وكرامة وأمن المواطنين في المادة (1/33)[286]. وما يعنينا في هذا الموضع هو عرض الحماية القانونية للخصوصية لكشف مدى ملاءمتها لإضفاء الحماية للبيانات الشخصية.

1. الحماية المدنية للخصوصية في إطار حماية حقوق الشخصية: اعترف المشرّع السوري في القانون المدني المادة (52)[287] بوجود طائفة من الحقوق هي الحقوق الملازمة لشخصية الإنسان، والحق في الخصوصية يدخل في نطاق هذه الحقوق التي ترتبط بكيان الشخص وآدميته، التي إذا أهدرت تنعدم صفته الإنسانية[288]. ويصبح الحق في الخصوصية، بما أنه حقًا من حقوق الشخصية، أحد المقومات الأساسية اللازمة كي يعيش الإنسان في سكينة وأمان. وقد وضع المشرع السوري ضمانات لحماية هذا الحق؛ فأقرّ إمكانية طلب وقف الاعتداء دون حاجة لإثبات الضرر، وتوحي عبارة وقف الاعتداء بأن الحماية لا تكون فقط في حالة الاعتداء الذي ينشأ عنه الضرر، وإنما يكفي مجرد الاعتداء بصرف النظر عن الضرر. كما نص المشرع السوري على حماية بعض مظاهر هذه

---

[284] الدستور السوري. المادة (37): "سرية المراسلات البريدية والاتصالات السلكية واللاسلكية وغيرها مكفولة وفق القانون".

[285] الدستور السوري. المادة (1/42): "حرية الاعتقاد مصونة وفقًا للقانون".

[286] الدستور السوري. المادة (1/44): "الحرية حق مقدس وتكفل الدولة للمواطنين حريتهم الشخصية وتحافظ على كرامتهم وأمنهم".

[287] القانون المدني السوري. الصادر بالمرسوم التشريعي رقم (84) بتاريخ (1949/5/18). 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".

[288] واصل، محمد. (1995). الحقوق الملازمة للشخصية، دراسة مقارنة، دمشق، الطبعة الأولى. ص: 251.

الفئة من الحقوق، كالحق في الاسم الذي من شأنه أن يكفل تمييز الشخص ويمنع اختلاطه بغيره من الأفراد وذلك في المادتين (40 و53)[289].

2. الحماية الجزائية للخصوصية: وفي إطار حماية الخصوصية جرّم قانون العقوبات السوري[290] إفشاء الأسرار في المادة (565)[291]. ويقتضي فعل الإفشاء أن يكون قد جرى الإفضاء بالسر إلى طرف ثالث لا ينتمي إلى الفئة التي ينحصر فيها نطاق العلم بالواقعة أو بالمعلومات السرية. ويتبين من نص المادة أنّ هناك شروطًا يفترض توافرها مجتمعة للقول بوقوع جريمة إفشاء الإسرار، فلا بد أن يتصل هذا السر أو المعلومة بوضع أو مهنة أو فن شخص ما، أي يجب أن يكون نطاق العلم بالسر محصورًا بأشخاص يُفترض توافر عنصر الثقة بهم، بسبب مكانتهم الاجتماعية بالنسبة لصاحب السر أو مركزهم العملي أو المهني، ويفترض علمهم بهذا السر أو المعلومة بسبب هذه المكانة الاجتماعية أو المركز العملي أو المهني، وبالتالي يفترض أن تكون الواقعة معلومة لعدد محدود من الأشخاص المميزين، وإلا انتفى عنها صفة السر وبالتالي تنتفي عنها الحماية، ويجب أن يكون إفشاء السر من دون سبب مشروع أو استعمله لمنفعته الخاصة أو منفعة غيره، أي أن يكون لصاحب السر مصلحة مشروعة في عدم إفشائه، كما تشترط المادة أن يسبب الإفشاء ضررًا ماديًا أو معنويًا بصاحب السر.

---

[289] القانون المدني السوري. المادة (40): "يكون لكل شخص اسم ولقب، ولقب الشخص يلحق أولاده". المادة (53): "لكل من نازعه الغير في استعمال اسمه بلا مبرر، ومن انتحل الغير اسمه أو لقبه أو كليهما دون حق، أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر".

[290] قانون العقوبات السوري الصادر بالمرسوم التشريعي رقم (148) لعام (1949).

[291] قانون العقوبات السوري. 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".

كما جرّم الاطلاع أو إتلاف أو اختلاس الرسائل أو البرقيات البريدية أو إفشاء مضمونها إلى غير المرسل إليه أو إفشاء مخابرة هاتفية في المواد (565-566-567)[292] وقد اكتفى المشرع بهذه النصوص لحماية خصوصية منزل الإنسان وأسراره ورسائله وبرقياته ومكالماته الهاتفية، التي كانت كافية قبل التطور التكنولوجي الذي صاحب نهايات القرن العشرين.

3. تطوير الحماية القانونية للخصوصية: عرفت حماية الخصوصية تطورًا ملحوظًا، بالنص صراحة على وجوب حماية خصوصية الأفراد في عدد من القوانين الجديدة، التي استحدثها المشرع السوري لمواكبة التطور الحاصل في مختلف ميادين الحياة، تأكيدًا على الأهمية القصوى للخصوصية على كيان الفرد والمجتمع معًا، واستجابة لدستورية هذا الحق ومشروعيته التي لا تقبل أي معارضة له. فأكّد المشرع في قانون الاتصالات[293] على خصوصية الاتصالات بين المستخدمين في المادة (50/أ)[294]، وذكرت المادة (4/4)[295] من قانون الإعلام السوري[296]، أنّ

---

[292] قانون العقوبات السوري. المادة (566) على: "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". وتنص المادة (567) على: " 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".

[293] قانون الاتصالات السوري. الصادر بالقانون رقم (18) بتاريخ (1/6/ 2010).

[294] قانون الاتصالات السوري. المادة (50/أ) على: ب-يتخذ كل مرخص له جميع الإجراءات الكفيلة بضمان سرية وخصوصية بيانات المشتركين لديه".

[295] قانون الاتصالات السوري. المادة (4) من قانون الإعلام السوري على: "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: 1.احترام حرية التعبير على أن تمارس هذه الحرية بوعي ومسؤولية. 2.حق الإعلامي في الحصول على المعلومات واستخدامها مع مراعاة الأحكام الواردة في هذا القانون. 3. الالتزام بالصدق والأمانة والنزاهة والدقة والموضوعية في نقل المعلومات. 4. احترام خصوصية الأفراد وكرامتهم وحقوقهم والامتناع عن انتهاكها بأي شكل من الأشكال. 5.احترام ميثاق الشرف الصحفي الصادر عن اتحاد الصحفيين. 6. منع احتكار الوسائل الإعلامية على اختلاف أنواعها".

[296] قانون الاعلام السوري الصادر بالمرسوم التشريعي رقم (108) لعام (2011).

إحدى مبادئ العمل الإعلامي هو احترام خصوصية الأفراد وكرامتهم وحقوقهم والامتناع عن انتهاكها بأي شكل من الأشكال، وأكد على حظر التعرض لحياة الأفراد الخاصة بأي شكل[297]. وفي قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (17)[298]، أتي المشرع على ذِكر حماية خصوصية المستخدمين وبياناتهم الشخصية في المادة (3/أ)[299]، فسمح لمقدم خدمات النفاذ إلى الشبكة بعملية تخزين المعلومات المتبادلة عن طريقه بتخزينها بشرط ألا يؤدي ذلك إلى انتهاك خصوصية المستخدمين أو بياناتهم الشخصية، ويبدو أن المشرع السوري يرى أن هناك فرقًا بين الخصوصية والبيانات الشخصية، والحماية الممنوحة لأحدهما لا تغطي الثانية ومع ذلك لم يميّز في الحماية بينهما، وهذا يتضح عندما جرّم في المادة (23)[300] نشر معلومات عن طريق الشبكة تنتهك خصوصية أي شخص، لكنه لم يجرّم العمليات التي تنتهك البيانات الشخصية. وفي قانون الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17) الذي حلّ محل قانون تنظيم التواصل على الشبكة ومكافحة على الشبكة ومكافحة الجريمة المعلوماتية رقم (17)، لم يأتِ المشرّع على ذِكر التزام مقدم خدمات النفاذ إلى الشبكة بعدم انتهاك

---

[297] قانون الاعلام السوري. المادة (13) على أنه: "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".

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

[299] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (17). المادة (3/أ): يجوز لمقدم خدمات النفاذ إلى الشبكة تخزين المعلومات المتبادلة عن طريقه تخزينا مؤقتاً مباشرة أو عن طريق العهدة بذلك إلى الغير شريطة ان يكون ذلك بغرض تحسين تقديم الخدمة وألا يؤدي إلى انتهاك خصوصية المستخدمين أو بياناتهم الشخصية وعليه ألا يقوم بأي تغيير على المحتوى المخزن لديه وأن يتخذ جميع الاجراءات اللازمة لضمان عدم الوصول غير المشروع إلى هذا المحتوى المخزن والعمل على إتلافه فور انتفاء الحاجة إليه.

[300] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (17). المادة (23): "يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه، حتى لو كانت تلك المعلومات صحيحة".

خصوصية المستخدمين أو بياناتهم الشخصية، وجرّم فقط انتهاك الخصوصية بنشر معلومات على الشبكة تتعلق بالخصوصية من دون رضا صاحبها، حتى لو كانت تلك المعلومات صحيحة[301].

ثانيًا: قصور الحماية القانونية للخصوصية عن حماية البيانات الشخصية

على الرغم من الحماية المقررة للخصوصية والأسرار لدى بعض الأشخاص والكيانات، نجد أن هذه الحماية تقوم بحماية البيانات الشخصية بصورة جزئية ومحدودة، فمفهوم الخصوصية لا يمتد ليشمل جميع أنواع البيانات الشخصية، فهناك طائفة كبيرة من البيانات الشخصية لا تمس الخصوصية ولا تصنف أنها تتعلق بحياة الأفراد الخاصة وبالتالي تخرج من نطاق الحماية كمعالجة البيانات المتعلقة بالحياة العملية والنشاطات العامة أو اسم الشخص وكنيته، فحماية البيانات لا تتعلق بمدى تعلّق البيانات الشخصية بالخصوصية، وإنما بتعلقها بالشخص الطبيعي وبقدرتها على تحديده والدلالة عليه، وبالتالي فإن مفهوم الخصوصية قاصر عن الإحاطة بمفهوم البيانات الشخصية كما أنّ حماية البيانات الشخصية تؤدي إلى حماية أكبر لجميع أنواع البيانات الشخصية.

1. قصور مفهوم الخصوصية عن الإحاطة بمفهوم البيانات الشخصية: يرتبط مفهوم الخصوصية بمفاهيم المجتمع وعاداته وتقاليده، أي أن لها بعدًا اجتماعيًا، ولذلك ليس غريبًا أن تختلف من بلد إلى آخر ومن مدينة إلى أخرى ومن وقت لآخر[302]، كما أن تعدد التعاريف الفقهية وعدم الاتفاق على تعريف محدد للخصوصية تؤكد فكرة نسبية

[301] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (21): "يعاقب بالحبس من شهر إلى ستة أشهر وغرامة من (500,000) ل.س إلى (1,000,000) ل.س، كل من قام بواسطة إحدى وسائل تقانة المعلومات بنشر معلومات على الشبكة تتعلق بالخصوصية من دون رضا صاحبها، حتى لو كانت تلك المعلومات صحيحة".

[302] الشماط، كندا. (2004–2005). الحق في الحياة الخاصة. رسالة لنيل درجة الدكتوراه في الحقوق. ص: 97–99.

الخصوصية وغموض مفهومها، الأمر الذي يؤدي إلى عدم استقرار قانوني. وفيما يتعلق بالتعريف التشريعي للخصوصية، فقد ذكرها المشرع السوري في قوانين عدة بصورة متشابهة تقريبًا، فعرّفها في المادة الأولى في قانون الإعلام لعام (2011) بأنها: "حق الفرد في حماية أسراره الشخصية والعائلية ومراسلاته وسمعته وحرمة منزله وملكيته الخاصة وفي عدم اختراقها أو كشفها دون موافقته" كما عرّفها في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (17) لعام (2012) بأنّها: "حق الفرد في حماية أسراره الشخصية والملاصقة للشخصية والعائلية ومراسلاته وسمعته وحرمة منزله وملكيته الخاصة وفي عدم اختراقها او كشفها دون موافقته". أما في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) لعام (2022) فعرّف الخصوصية بأنها: "حق الفرد في حماية أسراره الشخصية أو الملاصقة للشخصية أو العائلية أو مراسلاته أو سمعته ونشاطاته على الشبكة". ومن هذه التعاريف يتضح بأن حماية الخصوصية تتعلق بحماية المعلومات السرية المتعلقة بحياة الفرد الشخصية أو الملاصقة للشخصية أو العائلية أو مراسلاته أو سمعته، أو نشاطات الفرد على الشبكة على سبيل الحصر، وبذلك تخرج معلومات الأفراد الشخصية على خلاف ما ذُكر من نطاق الحماية التي منحها المشرع للخصوصية، ويتضح من التعاريف ارتباط مفهوم الخصوصية بحماية الأسرار، وفي هذا الإطار يعّرف الفقه القانوني السر بأنّه: "أمر ما يتعلق بشخص المرء ويمس الدائرة الشعورية الحساسة من نفسه بحيث يكون في البوح به حرج كبير"[303]، وعرّف جانب من الفقه الفرنسي السر بأنّه: "النبأ الذي يجب إخفاؤه حتى ولو لم يترتب على إفشائه

[303] بهنام، رمسيس. (1999). قانون العقوبات القسم الخاص. الطبعة الأولى. منشأة دار المعارف. مصر: الإسكندرية. ص: 1088. أشار إليه: الفتلاوي، سلام عبد الزهرة عبد الله، وفليح، حسام جادر. (2017/3/31). مفهوم التزام المحامي بعدم إفشاء السر المهني: دراسة مقارنة. مجلة المحقق الحلي للعلوم القانونية والسياسية، مج. 9، ع. 1، ص: 161.

إضرار بالسمعة أو الكرامة، وكان غير مشين بمن يريد كتمانه أو مزريًا بل قد يكون مشرّفًا لمن يريد كتمانه"[304]. فالنبأ أو المعلومة أو الواقعة محل الالتزام بالكتمان يقتصر على ما يكون منها ذا طبيعة سرية، فما كان منها شائعًا على وجه التأكيد لا يدخل ضمن الأسرار المشمولة بالحماية[305]. والسر قد يكون معلومة عن الحياة الخاصة، وقد يكون بيانًا شخصيًا يتصف بدرجة كبيرة من السرية[306]. أما مفهوم البيانات الشخصية فهو مفهوم قانوني واضح ومحدد في القوانين، وإن كان بعضها قد ينطبق عليها صفة المعلومات الخاصة أو السرية، ولكن في غالب الأحيان لا تتضمن معلومات لها علاقة بخصوصية الأفراد أو أسرارهم، وهي في معظمها معلومات معروفة عن الفرد في محيطة كاسمه ومعلومات الاتصال به.

2. الحماية الخاصة بالبيانات الشخصية تعطي حماية أكبر للبيانات الشخصية من حماية الخصوصية وحماية الأسرار؛ فحماية البيانات الشخصية تشمل في طياتها جميع المعلومات المتعلقة بالأفراد، سواء كانت سرية أم غير سرية، وسواء تعلقت البيانات الشخصية بحماية خصوصية أسرار الفرد الشخصية أو العائلية أو بمراسلاته أو بنشاطاته على الشبكة أم لم تتعلق بذلك، فقد يبدو أن لا قيمة كبيرة لبعض البيانات الشخصية، كالاسم الأول، أو اسم العائلة، أو البيانات المتعلقة بمشاركة الشخص في النشاطات العامة، ولكن بعد معالجتها أو ربطها ببعضها يمكن الحصول على معلومات شخصية ذات قيمة للأشخاص وربما تمس خصوصية الأفراد وأسرارهم.

---

[304] E . GARCON "code penal annote" 1956, ART 378. NO. 30

أشار إليه: الفتلاوي، وفليح. (2017). المرجع السابق. ص: 161.

[305] ويمكن تعريف السر أيضًا بأنّه: "كل معلومة ذات طبيعة سرية، ينحصر نطاق العلم بها في عدد محدد من الأشخاص، يلتزم من توصل إليها بكتمانها حماية لمصلحته المشروعة". الفتلاوي، سلام عبد الزهرة عبد الله، وفليح، حسام جادر. (2017/3/31). المرجع السابق. ص: 161.

[306] فكري. (2007). مرجع سابق. ص:740.

كما أنّ حماية الأسرار في قانون العقوبات تقدم حماية جزئية للبيانات الشخصية لأنّها من جهة؛ تحمي الأسرار الموجودة لدى بعض الأشخاص أو الجهات المحددة، بموجب نص القانون الذي حصرهم بوضع الشخص أو مهنته أو فنه، والمبدأ أنه لا يجوز القياس في المواد الجزائية، وبالتالي لا يجوز تطبيق النص وفرض التزام المحافظة على السر على شخص أو جهة ما خارج الفئات المذكورة، في حين أنّ حماية البيانات الشخصية تكون بمواجهة كل من يتحكم بالبيانات ويقوم بمعالجتها، ومن جهة أُخرى؛ فإنّ الحماية المقررة محدودة، فهي مقتصرة على الإفشاء من دون سبب مشروع أو الاستعمال لمنفعة الشخص المؤتمن على السر أو منفعة غيره، وبالتالي فإن الحماية لا توفر الحماية البيانات الشخصية من مخاطر المعالجة الأخرى، التي حولت بيانات الأفراد والتي قد تكون بذاتها غير ضارة، إلى معلومات قد تشكل تهديدًا حقيقيًا لخصوصية الأفراد، بفعل عمليات جمع البيانات المتفرقة ومعالجتها وتحويلها إلى سجل تفصيلي عن حياة الأفراد.

إنّ حماية الخصوصية على الإنترنت تتقاطع مع حماية البيانات، وفي الواقع جزء كبير من حماية الخصوصية هي حماية للبيانات الشخصية، ولكن البيانات الشخصية لا تتعلق جميعها بالخصوصية، فالبيانات التي تتعلق بالنشاطات العامة للفرد تشكل بيانات شخصية، لكنها لا تدخل ضمن مفهوم الخصوصية، كما لا تحلّ حماية البيانات الشخصية محل حماية الأسرار وطمأنينة الفرد واستقلاليته، لكنها تكملها وتؤمن تفعيلها في وجه مخاطر الإنترنت[307]. وهنا لا بد من الاستشهاد باجتهاد محكمة العدل الأوروبية التي أقرت أن المعلومات المتعلقة بأسماء الخبراء، جنبًا إلى جنب مع رأي كل خبير من الخبراء تشكل بيانات شخصية، فبقدر ما تتيح هذه المعلومات

[307] الحجار، وسيم شفيق. (2017). مرجع سابق. ص: 59.

الاتصال بخبير معين أو بتعليق معين، فإنها تتعلق بالأشخاص الطبيعيين المحددين، وبالتالي، تشكل مجموعة من البيانات الشخصية، فتقديم المعلومات على أنّها جزء من نشاط مهني، لا يعني أنّه لا يمكن وصف هذه المعلومات بأنها بيانات شخصية، والإعلان عن هوية الخبراء المعنيين والتعليقات المقدمة على موقع الهيئة العامة للرقابة المالية على الإنترنت، لا يعني أن المعلومات المعنية لم يعد من الممكن تمييزها على أنّها بيانات شخصية، وبالتالي فإن الادعاء بأن هذه المعلومات لا تدخل في نطاق الحياة الخاصة غير مجدي، فينبغي عدم الخلط بين مفاهيم البيانات الشخصية والبيانات المتعلقة بالحياة الخاصة[308].

الفرع الثاني: حماية البيانات الشخصية ضمن نطاق حماية سرية البيانات والمعلومات

وحيث لا يوجد في المنظومة التشريعية السورية تشريع خاص بحماية البيانات الشخصية بصورة مباشرة، كان لا بد من مراجعة القوانين السورية والبحث عن المواد القانونية المتعلقة بحماية المعلومات والبيانات، لتوضيح

[308] Judgment of the Court (Second Chamber) of 16 July 2015. (ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority). Case C-615/13 P. Paragraph (29): " In so far as that information would make it possible to connect to one particular expert or another a particular comment, it concerns identified natural persons and, accordingly, constitutes a set of personal data…" Paragraph (30): "… the fact that information is provided as part of a professional activity does not mean that it cannot be characterised as a set of personal data…" Paragraph (31): " Likewise, the fact that both the identity of the experts concerned and the comments submitted on the draft guidance document were made public on the EFSA website does not mean that the information at issue could no longer be so characterized". Paragraph (32): "" … the claim made by ClientEarth and PAN Europe in this case that the information at issue does not fall within the scope of the private life of the experts concerned is ineffective". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2015:489

مدى قصورها في تقديم حماية كافية للبيانات الشخصية في ظل التطور التكنولوجي والاستخدام الواسع لها على شبكة الإنترنت.

أولًا: حماية سرية البيانات والمعلومات الشخصية في القانون السوري

مع أنّ المشرّع لم يعرّف البيانات الشخصية كما لم يعرّف البيانات ولم يميزها عن المعلومات، كما أشار البحث في موضع سابق، إلا أنّه وبمراجعة بعض القوانين السورية نجد أنّ المشرّع السوري نصّ على حماية معلومات وبيانات محددة من بعض أشكال المساس بها، وسيوضح البحث ذلك فيما يأتي.

1. في قانون الأحوال المدنية[309] خصّ بالحماية بيانات الأفراد التي تحويها سجلات الأحوال المدنية فأكّد في المادة (3/5)[310]، على سرية السجل المدني وما يتضمنه من بيانات ومعلومات فلا يجوز الاطلاع عليها إلا من قبل العاملين المختصين، كما أكّدت المادة (7) على وجوب اتخاذ سائر الإجراءات اللازمة للحفاظ عليها وتأمين سلامتها وحمايتها من الضياع أو التلاعب والتلف واستخدام أفضل الوسائل التقنية لحفظها وتصنيفها وإعداد نسخ احتياطية منها[311]. وعاقب في المادة (72/ج)[312]، كل عامل مُخوّل بالدخول لنظام السجل المدني المؤتمت، وبدأ

---

[309] قانون الأحوال المدنية السوري رقم (13) لعام (2021).

[310] قانون الأحوال المدنية السوري. المادة (3/5): " الحفاظ على سرية السجل المدني وما يتضمنه من بيانات ومعلومات وعدم جواز الاطلاع عليها إلا من قبل العاملين المختصين ضمن حدود صلاحياتهم، وإذا اقتضى الحال في دعاوى التزوير الاطلاع على هذه السجلات ومستنداتها فيجب أن يتم هذا الاطلاع في مكان السجلات بواسطة هيئة المحكمة أو من تنتدبه لهذا الغرض ".

[311] قانون الأحوال المدنية السوري. المادة (7):" تعد السجلات المدنية وبرامجها من الوثائق الوطنية الأساسية الدائمة، ويتوجب اتخاذ سائر الإجراءات اللازمة للحفاظ عليها وتأمين سلامتها وحمايتها من الضياع أو التلاعب والتلف واستخدام أفضل الوسائل التقنية لحفظها وتصنيفها وإعداد نسخ احتياطية منها. "

[312] قانون الأحوال المدنية السوري. المادة (72/ج): " يعاقب بالحبس من شهر إلى ستة أشهر، وبغرامة من /25000/ ل.س خمسة وعشرين ألف ليرة سورية إلى /50000/ ل.س خمسين ألف ليرة سورية، كل عامل مُخوّل بالدخول لنظام السجل المدني المؤتمت، وبدأ بالعمل عليه بشكل مخالف للتعليمات الخاصة بصلاحيات عمله على نظام السجل المدني المؤتمت، ويقدر ذلك من اللجان المختصة."

بالعمل عليه بشكل مخالف للتعليمات الخاصة بصلاحيات عمله على نظام السجل المدني المؤتمت. كما عاقب في المادة (72/د)[313] كل من دخل، وهو غير مخول بالدخول إلى بيانات السجل المدني المؤتمت، بقصد حذف أو إضافة أو تعديل بياناته، وضاعف العقوبة إذا كان من قام بالفعل أحد العاملين سواء أكان مخوّلاً أو غير مخوّل بالدخول بقصد التزوير. فجاءت الحماية في مواجهة بعض أنواع المخاطر التي تتعرض لها البيانات وهي تعديل البيانات بالحذف أو الإضافة أو التعديل عليها أو التزوير.

2. في قانون السرية المصرفية الخاص بالمؤسسات المالية[314]، أكدت المادة (2)[315] على سرية بيانات العملاء مثل هويتهم وحساباتهم وموجوداتهم ومعاملاتهم مع المؤسسات المالية العملاء، وحظر إفشائها على كل من اطلع من الأشخاص بحكم وظيفته أو صفته أو ما تسمح القوانين بإفشائه للجهات المسموح لها، وجاءت الحماية في مواجهة بعض المخاطر التي تتعرض لها وهي إفشاء المعلومات المشار إليها في المادة (2) أو الشروع به، وذلك بموجب المادة (9)[316] من هذا القانون.

---

[313] قانون الأحوال المدنية السوري. المادة (72/د): " يعاقب بالسجن من ثلاث إلى خمس سنوات، كل من دخل وهو غير مُخّول بالدخول إلى معلومات السجل المدني المؤتمت، بقصد تعديل بياناته (حذف، إضافة، تعديل) أو برامجه، وتضاعف العقوبة إذا كان من قام بالفعل عاملاً، سواء أكان مخولاً أم غير مُخوّل بالدخول بقصد التزوير".

[314] قانون السرية المصرفية السوري الصادر بالمرسوم التشريعي رقم (30) بتاريخ (2010/4/15).

[315] قانون السرية المصرفية السوري. المادة (2): "أ–تعتبر معلومات سرية في معرض تطبيق هذا المرسوم التشريعي المعلومات التي تتعلق بهوية العملاء وحساباتهم وموجوداتهم ومعاملاتهم مع المؤسسات المالية بما في ذلك الحالات المذكورة في المادة (3) من هذا المرسوم التشريعي. 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".

[316] قانون السرية المصرفية السوري. 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".

3. في قانون التوقيع الإلكتروني وخدمات الشبكة[317] أكّد المشرّع على سرية بيانات إنشاء التوقيع الإلكتروني والمعلومات التي تقدم إلى مزود خدمات التصديق الإلكتروني وذلك في المادة (4/ب)[318]، وتتضمن الحماية البيانات والمعلومات الشخصية التي يتعلق بها التوقيع الإلكتروني، وجاءت الحماية في مواجهة مخاطر محددة وهي؛ تزوير أو تحريف بيانات إنشاء التوقيع الإلكتروني وذلك في المادة (31/أ/2)[319]، أو الحصول عليها بغير حق وبأي وسيلة كانت أو اختراقها أو اعتراضها أو تعطيلها عن أداء وظيفتها في المادة (31/أ/4)[320]، أو إفشاء العاملين لدى مزود خدمات التصديق الإلكتروني بيانات تتعلق بالتوقيع الإلكتروني أو التحقق من عائديته، أو استخدامها في غير الغرض الذي قدمت لأجله (المادة 31/أ/6)[321].

---

[317] قانون التوقيع الإلكتروني وخدمات الشبكة السوري الصادر بالقانون رقم (4) بتاريخ (2009/2/25).

[318] قانون التوقيع الإلكتروني وخدمات الشبكة السوري. 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".

[319] قانون التوقيع الإلكتروني وخدمات الشبكة السوري. 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."

[320] قانون التوقيع الإلكتروني وخدمات الشبكة السوري. 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."

[321] قانون التوقيع الإلكتروني وخدمات الشبكة السوري. 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".

4. في قانون الاتصالات[322] جاءت الحماية في مواجهة مخاطر محددة وهي إفشاء المعلومات أو استخدامها في غرض مختلف عن الغرض الذي قدمت من أجله أو العبث بها؛ وذلك في المادة (13)[323] التي جاءت تحت عنوان "واجب السرية المفروض على العمل في الهيئة"، وحظرت 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 حتى بعد ترك الوظيفة، والمادة (27/أ)[324] التي جاءت تحت عنوان "واجب السرية المفروض على المرخص لهم" وحظرت على المرخص لهم أو العاملين لديه استخدام أي معلومات تخص مرخص له آخر دون موافقته؛ كما نصت المادة (27/ب)[325] على أن العبث ببيانات المشتركين في خدمات الاتصال أو استخدامها لأي غرض آخر غير الغرض الذي حصل عليها أو إفشاءها دون رضا المشترك محظور على المرخص له، أو على العاملين لديه، وكان من واجب المشرع توضيح ما المقصود بالعبث ببيانات المشتركين وتحديد هذه العمليات. وفي الباب الثاني عشر الذي جاء بعنوان "حماية البيانات والخصوصية والأمن الوطني"، نصّ المشرّع بعبارات عامة ومبهمة على واجب المرخّص له باتخاذ الإجراءات الكفيلة بضمان سرية وخصوصية بيانات المشتركين(50/ب)[326]، مما يعني أن الحماية مقتصرة على فئات محدد على سبيل الحصر من البيانات الشخصية،

---

[322] قانون الاتصالات السوري الصادر بالقانون رقم (18) بتاريخ (1/6/ 2010).

[323] قانون الاتصالات السوري. 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".

[324] قانون الاتصالات السوري. المادة (27/أ) من قانون الاتصالات: "أ-يحظر على المرخص له، أو العاملين لديه، استخدام أي معلومات تخص مرخص له آخر لأي غير الغرض الذي حصل عليها من أجله، أو إفشاؤها بأي طريقة كانت، دون الحصول على موافقة المرخص له صاحب تلك المعلومات".

[325] المادة (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".

[326] المادة (50/ب) على: أ-... للاتصالات بين المستخدمين صفة الخصوصية.".

وبالتالي لا يجوز مد الحماية المقررة لهذه الفئات إلى فئات أخرى. ثم أحال المشرع تحديد شروط حماية خصوصية بيانات الحركة وبيانات الموقع إلى اللائحة التنفيذية لقانون الاتصالات[327].

وقد وردت هذه الشروط في الباب التاسع من اللائحة[328]، الذي جاء بعنوان حماية البيانات والخصوصية. وجاءت حماية بيانات الحركة في المادة (36)، التي سمحت للمرخص له بحفظ بيانات الحركة واستخدامها بهدف إصدار الفواتير من غير تحديد القدر الملائم والمدة الكافية لذلك (36/أ)[329]، كما سمحت باستخدامه بيانات الحركة بغية القيام بأبحاث السوق وأنشطة المبيعات المتعلق بخدماته ما لم يبد المشترك صراحة، في أي وقت، عدم رغبته بذلك، أي دون الموافقة المسبقة للمشترك (36/ب)[330]. هذه الشروط غير ملائمة لحماية بيانات الحركة للمشتركين، فيجب تحديد مدة حفظ بيانات المشتركين، وأخذ موافقتهم المسبقة قبل القيام بأي استخدام غير ضروري لبياناتهم الشخصية

وجاء في تحديد شروط حماية بيانات الموقع في المادة (37/أ)[331]، جواز المرخص له استخدام بيانات الموقع التي لا تنتمي إلى فئة بيانات الحركة إذا رغب بتقديم خدمات القيمة المضافة ما لم يبد المشترك صراحة،

---

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

[328] اللائحة التنفيذية لقانون الاتصالات الصادرة بالمرسوم رقم (261) لعام 2010.

[329] اللائحة التنفيذية لقانون الاتصالات الصادرة بالمرسوم رقم (261) لعام 2010. المادة (36/أ): "يسمح للمرخص له بحفظ واستخدام بيانات الحركة بالقدر الذي يلزم لإصدار الفواتير، ولمدة كافية تسمح بجباية الفواتير والنظر في اعتراضات المشتركين".

[330] اللائحة التنفيذية لقانون الاتصالات الصادرة بالمرسوم رقم (261) لعام 2010. المادة (36/ب): "يسمح للمرخص له باستخدام بيانات الحركة بغية القيام بأبحاث السوق وأنشطة المبيعات فيما يتصل بخدماته، أو تقديم خدمات القيم المضافة، ما لم يبد المشترك صراحة، في أي وقت، عدم رغبته بذلك".

[331] اللائحة التنفيذية لقانون الاتصالات الصادرة بالمرسوم رقم (261) لعام 2010. المادة (37/أ): "يجوز للمرخص له استخدام بيانات الموقع التي لا تنتمي إلى فئة بيانات الحركة عند رغبته بتقديم خدمات القيمة المضافة، ما لم يبدِ المشترك صراحة، في أي وقت، عدم رغبته بذلك. وعلى المرخص له في جميع الحالات جعل تلك البيانات مغفلة الاسم".

في أي وقت، عدم رغبته بذلك، أي دون الموافقة المسبقة للمشترك. وأيضًا هذه الشروط غير ملائمة لحماية بيانات الموقع للمشتركين، فيجب أخذ موافقة المشتركين المسبقة قبل القيام بأي استخدام غير ضروري لبياناتهم الشخصية. وجعل بيانات الموقع مغفلة الاسم لا يكفي لضمان حماية الأشخاص أصحاب هذه البيانات، فقد تحدد هذه البيانات أصحابها عند معالجتها بشكل أو بآخر. وترى الباحثة أن شروط حماية خصوصية بيانات الحركة وبيانات الموقع في اللائحة التنفيذية لقانون الاتصالات تجيز للمرخص له باستخدام البيانات دون رضا المشترك، لذلك يجب وضع قواعد أكثر دقة وتحديدًا.

5. في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17)، ألزم المشرع مُقدم خدمات النفاذ إلى الشبكة[332]، بضمان سرية بيانات الحركة مثل الرقم الخلوي والثابت، ووقت وتاريخ بدء ونهاية الحركة وحجم الحركة الرقمية المتبادل[333]، وحفظها لمدة معينة تحددها الهيئة الناظمة لجميع مشتركيه وهو ما أوردته المادة (3/أ/1)[334]، كما ألزم مقدم خدمات الاستضافة[335] بحفظ نسخة من بيانات الحركة والمحتوى الرقمي المستضاف لديه، وعدم تغيير أو تعديل أو حذف أي محتوى رقمي مخزن أو مستضاف لديه، إلا

[332] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (1). مُقدم خدمات النفاذ إلى الشبكة: مُقدم الخدمات الذي يتيح للمشتركين لديه خدمة النفاذ إلى الشبكة والوصول إلى الخدمات والمعلومات المتوفرة.

[333] التعليمات التنفيذية للقانون رقم (20) لعام 2022 لتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية. الصادرة بتاريخ (2022/5/22).

[334] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (1) التزامات مقدم خدمات النفاذ إلى الشبكة. أ–يلتزم مقدم خدمات النفاذ إلى الشبكة بالآتي: 1. ضمان سرية وحفظ بيانات الحركة لجميع مشتركيه لمدة زمنية تحددها الهيئة الناظمة."

[335] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (1). مُقدم خدمات الاستضافة: مُقدم الخدمات الذي يقدم بتوفير نظم المعلومات اللازمة لإتاحة استضافة المعلومات أو الخدمات على الشبكة.

في حالات حددها القانون (المادة 4)[336]. وكذلك ألزم مقدم خدمات التطبيقات على الشبكة[337] بحفظ نسخة من المحتوى الرقمي[338] المتبادل لديه مع بيانات الحركة[339] التي تحدد هوية من يساهم في وضع هذا المحتوى (المادة 5)[340]. وجرّم إقدام مقدمي الخدمات على الشبكة الامتناع عن حفظ نسخ المحتوى الرقمي أو المعلومات[341] أو بيانات الحركة (المادة 6)، أو إفشاءها (المادة 7)، أو تغييرها أو تعديلها أو حذفها (المادة 9)، أو الامتناع عن حذف محتوى رقمي غير مشروع (المادة 8).

كما جرم أيضًا كل من دخل إلى نظام معلومات، أو موقع إلكتروني أو حساب شخصي بشكل مشروع فتجاوز حدود هذا الدخول، وجرّم أيضًا نسخ المعلومات أو استخدمها أو أفشاءها، أو حذفها، أو تعديلها، ونسخ المعلومات التي وصل إليها وحذفها (المادة 11)، كما جرم أيضًا كل من دخل بطريقة غير مشروعة إلى نظام

---

[336] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (4): التزامات مقدم خدمات الاستضافة على الشبكة. أ–يلتزم مقدم خدمات الاستضافة على الشبكة بالآتي: 1. حفظ نسخة من بيانات الحركة والمحتوى الرقمي المستضاف لديه، وتضع الهيئة الناظمة أو الهيئة الوطنية كل حسب اختصاصه بطبيعة المحتوى الرقمي والخدمات المقدمة، الضوابط الخاصة لعمل مقدم الخدمة. 2. عدم تغيير أو تعديل أو حذف أي محتوى رقمي مُخزّن أو مُستضاف لديه."

[337] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (1). "مُقدم خدمات التطبيقات على الشبكة: مُقدم الخدمات الذي يقوم بتقديم خدمات المحتوى الرقمي والخدمات الأخرى للمستخدمين بطريقة تفاعلية عبر الشبكة".

[338] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (1). "المحتوى الرقمي: المعلومات المخزنة التي يمكن الوصول إليها وتداولها عبر الشبكة".

[339] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (1). "بيانات الحركة: معلومات يجري تداولها عبر الشبكة تشير بوجه خاص إلى مصدر الاتصال والوجهة المرسل منها وإليها، ومساره، وساعته وتاريخه، وحجمه، ومدته، ونوع الخدمة".

[340] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (5): التزامات مقدم خدمات التطبيقات على الشبكة. يلتزم مقدم خدمات التطبيقات على الشبكة بالآتي: أ–حفظ نسخة من المحتوى الرقمي المتبادل لديه مع بيانات الحركة التي تُحدد هوية من يساهم في وضع هذا المحتوى وتضع الهيئة الناظمة أو الهيئة الوطنية، كل حسب اختصاصه، الضوابط الخاصة لعمل مقدم الخدمة."

[341] قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17). المادة (1). "المعلومات: هي العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة الرقمية التي تتم معالجتها لتصبح ذات معنى أو مغزى معين وترتبط بسياق محدد".

معلومات، أو موقع إلكتروني أو حساب شخصي، وجرّم أيضًا نسخ المعلومات أو استخدمها أو أفشاءها، أو حذفها، أو تعديلها، ونسخ المعلومات التي وصل إليها وحذفها (المادة 12).

ونلاحظ أن الحماية القانونية للبيانات والمعلومات بما فيها البيانات الشخصية جاءت في مواجهة بعض أنواع التهديدات، التي نستطيع حصرها في إفشاء المحتوى أو البيانات أو المعلومات المخزنة الإفشاء، والتغيير والتعديل والحذف، والامتناع عن الحذف، بالإضافة إلى النسخ.

6. أما في قانون المعاملات الإلكتروني[342] فقد ألزم المشرّع أطراف النشاط الاقتصادي بالوسائل الإلكترونية، بحماية جميع المعلومات العائدة لباقي الأطراف فلا يجوز لهم التصرف بالمعلومات أو التعامل بها بصورة تلحق ضررًا ماديًا أو معنويًا بأصحاب هذه المعلومات[343]. وبغض النظر عن غموض مفهوم التصرف والتعامل، وما قصد المشرّع بهما وعلى ماذا يشتملان، وفيما كان يقصد المشّرع بهما المعالجة، نستطيع القول إن حماية البيانات في هذا القانون تقتصر على البيانات المتبادلة بوسائل إلكترونية، في أثناء القيام بنشاط اقتصادي، كما أن الحماية المقررة جاءت مشروطة بإلحاق الضرر، وبمفهوم المخالفة يجوز التصرف والتعامل بهذه المعلومات إذا لم يلحق ذلك ضررًا بأصحابها.

---

[342] قانون المعاملات الإلكترونية السوري رقم (3) الصادر بتاريخ (2014/3/4).

[343] 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".

ثانيًا: قصور الحماية القانونية لسرية البيانات والمعلومات في حماية البيانات الشخصية

بعد عرض أهم المواد القانونية في القوانين السوريّة، المتعلقة بحماية سرية البيانات والمعلومات وسلامتها لدى بعض الأشخاص والجهات، نستنتج:

1. أنّ تدابير المشرّع في حماية البيانات والمعلومات قاصرة عن حماية البيانات الشخصية، فحماية سرية البيانات الشخصية في قانوني الأحوال المدنية والسرية المصرفية؛ حماية جزئية مقتصرة على بيانات الأفراد المخزنة لدى هذه الجهات بالذات، وبالتالي لا تشمل البيانات الشخصية التي تجمعها وتخزنها الجهات الأخرى العامة والخاصة، كما أنّها حماية محدودة في مواجهة بعض أنواع المخاطر التي تتعرض لها هذه البيانات، والتي اقتصرت في قانون الأحوال المدنية على تعديل البيانات بالحذف والإضافة والتعديل أو تزويرها، واقتصرت في قانون السرية المصرفية على الإفشاء أو الشروع به.

2. أنّ تدابير المشرّع في حماية البيانات والمعلومات الإلكترونية، بما فيها البيانات والمعلومات الخاصة بالأفراد، تقدم حماية جزئية ومحدودة للبيانات الشخصية فهي مقتصرة على البيانات والمعلومات الخاصة بالأفراد المخزنة لدى الجهات المحددة التي سبق عرضها من جهة، وعلى بعض فئات البيانات الشخصية من جهة ثانية، وفي مواجهة بعض أنواع المخاطر من جهة ثالثة، وبالتالي فهي حماية محدودة لأنها لا تغطي المفهوم الواسع للبيانات الشخصية، كما لا تغطي العمليات التي تقع عليها التي يتضمنها المفهوم الواسع للمعالجة، فمحل الحماية في قوانين حماية البيانات الشخصية هو أي معلومة متعلقة بشخص طبيعي، تخضع لأي عملية من عمليات المعالجة، بغض النظر عن ماهية أو مكان الكيان متسلّم البيانات. كما أنّ الحماية في النصوص السابقة تهدف بالدرجة الأولى إلى

الوفاء بالتزام المحافظة على السرية، أما حماية البيانات الشخصية فتهدف بالدرجة أولًا إلى احترام جميع حقوق الأفراد وحرياتهم ولا سيما حقهم في حماية بياناتهم الشخصية، التي أصبحت محلًا لعمليات المعالجة في قواعد البيانات لدى مختلف الجهات العامة والخاصة دون تحديد، وقواعد البيانات المنتشرة عبر الإنترنت، سواء في حالة جمعها بداية أو معالجتها بأي طريقة أخرى في خطوة لاحقة، وما يرافق ذلك من مخاطر المراقبة والتجسس على الأفراد، والاتجار غير المشروع بهذه البيانات كاستعمالها في الإعلانات التجارية وتطوير الأعمال التجارية للشركات أو إساءة استغلالها بأي شكل آخر، الأمر الذي يشكّل اعتداءً صارخًا على حقوق الأفراد وحرياتهم الأساسية.

إن هذه الحماية التي سبق عرضها، لا تتناسب مع دخول المجتمع السوري عصر التكنولوجيا الحديثة، ومع التحديات التي أوجدها على البيانات الشخصية، لذلك يجب على المشرّع السوري تحديث حماية البيانات الشخصية وتعزيزها وتوسيعها لمواجهة هذه المستجدات، والاعتراف بحق الأفراد في حماية بياناتهم الشخصية، وذلك بالنص عليه في الدستور، وإصدار تشريع خاص بحماية البيانات الشخصية، يحدد المفاهيم المتعلقة بهذه الحماية، وينظم مبادئ هذه الحماية، ويحدد حقوق أصحاب البيانات والتزامات القائمين على عملية المعالجة، للحيلولة دون التعدي على حقوق أصاحب البيانات.

خلاصة الفصل الأول

هدف الفصل الأول من البحث إلى التعريف بمفهوم البيانات الشخصية والتحديات التي تواجهها على شبكة الإنترنت ولهذه الغاية عرض المبحث الأول مفهوم البيانات الشخصية ومعالجة البيانات، وأهداف حمايتها في إيجاد توازن بين حماية حق الأفراد في البيانات الشخصية وحقوقهم وحرياتهم الأُخرى، كالحق في الخصوصية، من جهة، وضمان التدفق الحر للبيانات الشخصية لحماية المصالح التجارية، من جهة أخرى، ثم عرض المبحث الثاني التحديات التي تواجه البيانات الشخصية على شبكة الإنترنت، وعالج ذلك من خلال، التحديات المتعلقة بطبيعة شبكة الإنترنت التي تسهل انتاج البيانات الشخصية جمعها ومعالجتها، وتوفر قدرات جديدة لمعالجة البيانات الشخصية وإعادة استخدامها؛ والتحديات المتعلقة بقصور نماذج الحماية وغياب الأطر التشريعية والتنظيمية الملائمة في التشريعات السورية، وبالنظر إلى عدم وجود تنظيم قانوني خاص بحماية البيانات الشخصية في سورية، كان لا بد من مراجعة التشريعات السورية ذات العلاقة، بهدف إظهار ملامح الحماية المتاحة في هذه التشريعات، ومن ثم توضيح مدى قصورها في تقديم حماية كافية للبيانات الشخصية، وفي مسايرة التطور التكنولوجي والاستخدام الواسع للبيانات الشخصية على شبكة الإنترنت، وبيّن البحث أنّ القواعد القانونية الخاصة بحماية الخصوصية وحماية سرية المعلومات والبيانات لا تؤمن حماية كافية للبيانات الشخصية ولا تتوافق مع المخاطر التي أوجدتها شبكة الإنترنت، وتبقى تلك النصوص القانونية نصوصًا متفرقة قد تقدّم الحماية لبعض أنواع البيانات الشخصية لكنها تعجز عن تقديم الحماية للجزء الأكبر منها.

الفصل الثاني: تطور حماية البيانات الشخصية في التشريعات الدولية والتنظيم القانوني لحمايتها

ظهرت المبادرات الأولى التي تحث على ضرورة وجود حماية قانونية للبيانات الشخصية منذ ستينيّات القرن العشرين، من خلال المؤتمرات الأكاديمية المتخصصة بحماية حقوق الإنسان وحرياته، ففي مرحلة أولى كان لمؤتمر ستوكهولم المنعقد عام (1967)، برعاية اللجنة الدولية للقانونيين، بما طرحه من مسائل تتعلق بمخاطر التطور العلمي والتكنولوجي على حياة الأفراد الشخصية[344]، دور رئيسي في التأكيد على ضرورة اتخاذ الوسائل القانونية الفاعلة لحماية الأفراد، كما كان له دور في توجيه اهتمام منظمة الأمم المتحدة العالمية إلى أثر التطور التكنولوجي على انتهاك حقوق الأفراد وحرياتهم، وتبلورت المرحلة الثانية في المؤتمر الدولي لحقوق الإنسان المنعقد في طهران عام (1968)، الذي جاء تلبية للمتغيرات غير المسبوقة التي أتاحها التقدم التكنولوجي، الذي يعدّ باكور جهود الأمم المتحدة في ميدان حماية حقوق الأفراد وحريات من مخاطر التكنولوجيا[345]، وقد نبه المؤتمر في الإعلان[346] الذي أصدره، من مخاطر التقدم التكنولوجي على الحقوق والحريات الأساسية، فكان محركًا أساسيًا حول تأثير التطور التكنولوجي على حقوق الإنسان وحرياته[347].

---

[344] مغبغب، نعيم. (1998) مخاطر المعلوماتية والإنترنت، المخاطر على الحياة الخاصة، دراسة في القانون المقارن. ص: 97.

[345] أيوب. (2009). مرجع سابق. ص: 300.

[346] إعلان طهران، أصدره المؤتمر الدولي لحقوق الإنسان في طهران رسميًا بتاريخ (1968/5/13). متاح على الموقع الآتي: http://hrlibrary.umn.edu/arab/b006.html

[347] إعلان طهران، الفقرة (18): "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".

وهنا تجدر الإشارة، إلى أنّ أول اعتراف قانوني بتوفير حماية خاصة للبيانات الشخصية بعيدًا عن الحق في الخصوصية كان على المستوى الوطني، ولم يكن على المستوى الدولي، وقد أدت الدول الأوروبية دورًا رائدًا في هذا المجال. فمنذ مطلع سبعينيّات القرن الماضي، وعلى أثر مؤتمر الأمم المتحدة لحقوق الإنسان المنعقد في طهران عام (1968)، ومناقشة مخاطر تكنولوجيا المعلومات على الخصوصية، ظهرت أول معالجة تشريعية وطنية لحماية البيانات الشخصية في ولاية هيس في ألمانية الاتحادية التي أصدرت قانون حماية البيانات في عام (1970)، مع أنّه لا يعدّ قانونًا متكاملًا لاعتبارات أهمها أنّه ليس قانون دولة. كما كان للسويد دور مهم في الاعتراف بالحق في البيانات الشخصية، فسنت أول قانون وطني متكامل لحماية البيانات عام (1973)[348].

ولم تكن الريادة بحماية البيانات الشخصية في ألمانيا والسويد من قبيل المصادفة، فقد كان للجوانب الإيجابية أو السلبية للنظام السياسي دور أساسي في إبرازها؛ ففي ألمانيا أدّت تجربة إساءة استخدام البيانات الشخصية من قبل الحكومات الشمولية، سواء في ظل النظام النازي في ألمانيا الغربية أو في ظل النظام الشيوعي في ألمانيا الشرقية آنذاك، إلى محاولة لوضع قيود على قدرة هيئات القطاعين العام والخاص على معالجة البيانات الشخصية؛ أما في السويد، فقد كان الوضع مختلفًا، فلم يكن هناك نظام شمولي يسيء استخدام البيانات الشخصية، ولكن كان هناك تقليد قديم في حرية المعلومات وبموجبه ربما تصنف أي معلومة تحتفظ بها الهيئات العامة على أنها ضمن المجال العام، وقد توسع نطاق مفهوم حرية المعلومات ليشمل القطاع الخاص، وبالتالي يستطيع الأفراد الوصول إلى سجلات البيانات، وهذا يوضح الدور الاختياري في حماية البيانات في السويد[349]. وقد تبعت ولاية

[348] أيوب. (2009). مرجع سابق. ص: 309-310.

[349] Lloyd. (2011). Previous reference. P: 22.

هيس ودولة السويد دول أخرى مثل الولايات المتحدة وألمانيا بقوانين على المستوى الفدرالي في عامي (1974) و (1977) على التوالي، كما سنّت فرنسا القانون المعروف باسم "قانون المعلوماتية والحريات" عام (1978)[350].

ومن ثم بدأت المنظمات والهيئات الدولية في تطوير قوانين حماية البيانات منذ ثمانينيّات القرن العشرين، كدليل منظمة التعاون الاقتصادي والتنمية لحماية الخصوصية والبيانات الشخصية عام (1980). الذي كان له أثّر مهم على مجلس أوروبا، الذي وضع بدوره اتفاقية حماية البيانات من مخاطر المعالجة الآلية رقم (108) لعام (1981). وكان من الطبيعي أن تتطور أدوات الحماية لدى الأمم المتحدة فتجاوزت المؤتمرات إلى الإعلانات، وقامت بإصدار القرار رقم (95/45)، المعروف بدليل الأمم المتحدة المتعلق بملفات البيانات الشخصية المؤتمتة لعام (1990). كما بذل الاتحاد الأوروبي جهودًا حثيثة لحماية بيانات مواطنيه، فأصدر التوجيه الأوروبي رقم (EC/46/95) لعام (1995)، لحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية انتقالها عبر الحدود. ولاحقًا أصدر الاتحاد الأوروبي في (14) نيسان (2016) نظام قانوني أوروبي جديد باسم النظام العام أو اللائحة العامة لحماية البيانات الشخصية (General Data Protection Regulation)، لتحل محل الإرشاد السابق رقم (EC/46/95)، ومحل جميع القوانين الوطنية للاتحاد الأوروبي.

وأيضًا على المستوى الوطني، ازداد اهتمام الدول في الوقت الحالي، في سنّ تشريعات خاصة لحماية بيانات الأفراد الشخصية، وردع الاعتداءات التي تطالها، تماشيًا مع ازدياد التطور التكنولوجي في وسائل الاتصال،

[350] أيوب. (2009). مرجع سابق. ص: 309-310.

ولا سيما ظهور شبكة الإنترنت. فسنّت مئات الدول في جميع أنحاء العالم قوانين لحماية البيانات، وهناك بلدان تنظر حاليًا في تشريعات حماية البيانات[351].

ومن أجل عرض تطور حماية البيانات الشخصية في التشريعات الدولية والتنظيم القانوني لحمايتها، يقدم هذا المبحث عرضًا وتحليلًا لأهم الجهود الدولية والإقليمية، التي كان لها دور أساسي في تطوير الحماية القانونية الخاصة بالبيانات الشخصية، (المبحث الأول) المعنون بتطور الحماية القانونية للبيانات الشخصية على الصعيد الدولي؛ ومن ثم مراجعة التشريعات السورية ذات العلاقة لتبين ملامح حماية البيانات الشخصية في هذه التشريعات ولتوضيح مدى ملاءمتها وقدرتها على تقديم حماية كافية للبيانات الشخصية في ظل التطور التكنولوجي والاستخدام الواسع للبيانات الشخصية على شبكة الإنترنت، وهو ما سيُعرض في المطلب الثاني المعنون بالحماية القانونية للبيانات الشخصية في التشريعات السورية.

المبحث الأول: تطور الحماية القانونية للبيانات الشخصية في التشريعات الدولية

إذا كانت التكنولوجيا قد قامت بدور مهم في مجال معالجة البيانات الشخصية، فإن الفكر والقانوني والحقوقي استشعر أثر الجانب السلبي لمخاطر التكنولوجيا، التي عرفت بدورها تطورًا نوعيًا، ومدى إمكانية استغلالها كآليات ووسائل متطورة لانتهاك حقوق الإنسان وحرياته الأساسية، كواحدة من أهم القيم الأساسية للوجود الإنساني،

[351] أكسس ناو. (2018). مرجع سابق. ص:3.

التي صارع الفكر الإنساني والقانوني لسنوات من أجل حمايتها. فكان لبعض المنظمات، دور مهم في حماية البيانات الشخصية، وهو ما سيُعرض البحث في المطلبين الآتيتين.

المطلب الأول: جهود المنظمات الدولية في حماية البيانات الشخصية

ظهر اهتمام دولي لوضع تنظيم قانوني لحماية بيانات الأفراد الشخصية، وأبرز المنظمات الدولية التي نظمت هذه الحماية هي منظمة التعاون الاقتصادي والتنمية (OECD) ومجلس أوروبا (CoE) ومنظمة الأمم المتحدة (UN)، وفيما يأتي عرض لمساهماتهم.

الفرع الأول: جهود منظمة التعاون الاقتصادي والتنمية في حماية البيانات الشخصية

منظمة التعاون الاقتصادي والتنمية، من أوائل المنظمات الدولية التي تعاملت بشكل صريح مع البيانات الشخصية[352]، فقد قامت لعقود عدة بدور مهم في تعزيز حماية البيانات على أنّها قيمة أساسية وشرط للتدفق الحر للبيانات الشخصية عبر الحدود[353].

1. الجهود الأولية لمنظمة التعاون الاقتصادي والتنمية: بدأت منظمة التعاون الاقتصادي والتنمية الاهتمام بحماية البيانات في عام (1969) مع بدء برنامج استخدام الكمبيوتر في القطاع العام، وفي أوائل عام (1978) أُنشأت

[352] De Hert, Paul, Papakonstantinou, Vagelis. (2013). Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency? I/S: A Journal of Law and Policy for the Information Society. Vol. 9:2. P: 276.

[353] OECD work on privacy. Last updated: 1/6/2021. Available at: http://www.oecd.org/sti/ieconomy/privacy.htm.

مجموعة خبراء لوضع إرشادات تحكم تدفق البيانات عبر الحدود وحماية البيانات الشخصية والخصوصية وتسهيل تنسيق التشريعات الوطنية[354]. ووضعت المجموعة إرشادات منظمة التعاون الاقتصادي والتنمية لحماية الخصوصية وتدفق البيانات الشخصية عبر الحدود، في شكل توصية وأُرفقت بمذكرة توضيحية، وأصبحت سارية بتاريخ (1980/9/23)[355].

2. دور إرشادات منظمة التعاون الاقتصادي والتنمية لعام (1980) في حماية البيانات الشخصية: أكدت منظمة التعاون الاقتصادي والتنمية، بوجوب أن تأخذ الدول 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 فيما بينها من أجل تنفيذ ما تضمنه الدليل[356]. وتضم إرشادات

---

[354] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Explanatory memorandum to the Guidelines. Activities of the OECD. Last updated: 1/6/2021. Available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum

[355] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Explanatory memorandum to the Guidelines. INTRODUCTION. Last updated: 1/6/2021. Available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[356] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data:

• 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;

منظمة التعاون الاقتصادي والتنمية مبادئ تشكل حجر الأساس لحماية البيانات، وقد قسمت التوصية المبادئ إلى؛ مبادئ أساسية للتطبيق الوطني وحددتها بثمانية مبادئ وهي مبدأ جمع البيانات، ومبدأ جودة البيانات، ومبدأ تحديد الغرض، ومبدأ تقييد الاستخدام، ومبدأ الحماية الأمنية، ومبدأ الانفتاح، ومبدأ المشاركة الفردية، ومبدأ المساءلة[357]؛ ومبادئ أساسية للتطبيق الدولي وهي مبدأ التدفق الحر للبيانات والقيود القانونية على هذا المبدأ[358].

• That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

[357] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Annex to the Recommendation of the Council of 23rd September 1980: Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. Part two. Basic principles of national application. "Collection Limitation Principle: 7. there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Data Quality Principle: 8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. Purpose Specification Principle: 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. Use Limitation Principle: 10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law. Security Safeguards Principle: 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. Openness Principle: 12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. Individual Participation Principle: 13. An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. Accountability Principle: 14. A data controller should be accountable for complying with measures which give effect to the principles stated above."

[358] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Annex to the Recommendation of the Council of 23rd September 1980: Guidelines governing the Protection of Privacy and

3. توصية منظمة التعاون الاقتصادي والتنمية بشأن التعاون عبر الحدود في إنفاذ القوانين التي تحمي الخصوصية لعام (2007): العمل الآخر المهم الذي قامت به منظمة التعاون الاقتصادي والتنمية بشأن حماية البيانات، هو التوصية بشأن التعاون عبر الحدود في إنفاذ القوانين التي تحمي الخصوصية. تشجع هذه التوصية البلدان الأعضاء على اتخاذ خطوات من أجل؛ تحسين أطرها المحلية لإنفاذ قانون الخصوصية لتمكين سلطاتها بشكل أفضل من التعاون مع السلطات الأجنبية؛ ووضع آليات دولية فعالة لتسهيل التعاون عبر الحدود في مجال إنفاذ قانون الخصوصية؛ وتقديم المساعدة المتبادلة لبعضهم البعض في إنفاذ القوانين التي تحمي الخصوصية، بما في ذلك من خلال الإخطار وإحالة الشكاوى والمساعدة في التحقيق وتبادل المعلومات مع مراعاة الضمانات المناسبة؛ وإشراك أصحاب المصلحة المعنيين في المناقشات والأنشطة التي تهدف في المقام الأول إلى تعزيز التعاون عبر الحدود في إنفاذ القوانين التي تحمي الخصوصية[359].

Transborder Flows of Personal Data. Part two. Basic principles of international application. Free flow and legitimate restrictions. " 15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data. 16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure. 17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection. 18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

[359] OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (12 June 2007). Last updated: 2/6/2021. Available at: http://www.oecd.org/internet/ieconomy/38770483.pdf

4. تطوير إرشادات منظمة التعاون الاقتصادي والتنمية لحماية الخصوصية وتدفق البيانات الشخصية عبر الحدود لعام (1980): في عام (2013) نقّحت منظمة التعاون الاقتصادي والتنمية مبادئها التوجيهية، لمواكبة التطورات التكنولوجية السريعة، وأضافت توصية جديدة لمجلس منظمة التعاون الاقتصادي والتنمية بشأن المبادئ التوجيهية التي تحكم حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود. وهذا التحديث هو أول تحديث رئيسي للمبادئ التوجيهية منذ عام (1980)[360]. وقد أدى النص المنقّح إلى تحديث نهج منظمة التعاون الاقتصادي والتنمية في نواحي مهمة وتعزيز تكامله، وهناك موضوعان أساسيان في الإرشادات المحدثة؛ الأول هو التركز على التنفيذ العملي لحماية الخصوصية من خلال منهج قائم على احتواء المخاطر أو إدارتها، والثاني الاعتراف بالحاجة إلى بذل جهود أكبر من أجل معالجة البعد العالمي للخصوصية من خلال تحسين إمكانية العمل المتبادل[361].

الفرع الثاني: جهود مجلس أوروبا في حماية البيانات الشخصية

كان لمجلس أوروبا دور مهم في حماية البيانات الشخصية، وفيما يأتي استعراض لهذه الجهود.

1. الجهود الأولية لمجلس أوروبا في حماية البيانات الشخصية: في عام (1968)، وجّه مجلس البرلمان في مجلس أوروبا إلى اللجنة الوزارية في المجلس التوصية رقم (509)، طالب فيها فحص إذا ما كانت الاتفاقية الأوروبية لحقوق الإنسان والقوانين المحلية للدول الأعضاء، يوفرون حماية كافية للحق في الخصوصية تجاه التكنولوجيا الحديثة، وأظهرت الدراسة التي أجريت أنّ التشريعات الوطنية الحالية لا توفر حماية كافية لخصوصية الأفراد،

---

[360] OECD. Work on privacy. Previous reference.

[361] OECD. The OECD privacy framework. (2013). P: 4. last updated: 1/6/2021. Available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf,

وغيرها من حقوق ومصالح الأفراد فيما يتعلق ببنوك البيانات الآلية[362]. وعلى أساس هذه النتائج، اعتمدت اللجنة الوزارية في عامي (1973) و (1974) قرارين بشأن حماية البيانات؛ الأول، القرار رقم (22) الذي أرسى مبادئ حماية البيانات في القطاع الخاص[363]، والثاني القرار (29) فعل الشيء نفسه بالنسبة للقطاع العام[364]. وقد أوصى كلا القرارين بضرورة احتواء القوانين الوطنية على مبادئ تتعلق بممارسات عادلة للمعلومات، ولا سيما متطلبات المعالجة القانونية والوصول الفردي، هذه المبادئ تدعم قوانين حماية البيانات إلى الآن، ولكن مع مرور الوقت، كشف التقدم في تكنولوجيا المعلومات عن أوجه القصور في هذين القرارين[365]، فلم تنص القرارات على الوسائل التي ينبغي للدول الأعضاء تفعيل المبادئ من خلالها، وبالتالي كان هناك تناقضات واسعة النطاق في قوانين حماية البيانات في الدول الأعضاء، كما أنّ القرارين ومعظم قوانين حماية البيانات اللاحقة لهما، تستند على فكرة وجود متحكم واحد يحتفظ بالبيانات بجهاز كمبيوتر واحد. وهذا بعيد عن البيئة المتصلة بشبكة الإنترنت اليوم، فبمجرد أن تجد البيانات طريقها إلى الإنترنت، لا يمكن التراجع عن الضرر أبدًا في ظل عدم وجود الضوابط التفاعلية الكافية. وقد أدى ذلك إلى التحرك نحو معاهدة لضمان مواءمة أفضل للقوانين الوطنية[366].

---

[362] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Strasbourg, 28.I.1981). p2. Last updated: 10/6/2021. Available at: https://rm.coe.int/16800ca434

[363] Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in Private Sector. (26 September 1973). Last updated: 10/6/2021. Available at: https://www.legislationline.org/documents/id/6498

[364] Resolution (74) 29 on the Protection of Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector. (20 September 1974). Last updated: 10/6/2021. Available at: https://www.legislationline.org/documents/id/6499

[365] Lloyd. (2011). Previous reference. P: 25.

[366] Lloyd. (2011). Previous reference. P: 25.

2. دور اتفاقية مجلس أوروبا رقم (108) لحماية الأفراد من المعالجة الآلية للبيانات الشخصية: في خطوة لاحقة أصدر مجلس أوروبا اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (اتفاقية مجلس أوروبا) رقم (108) بتاريخ (1981/1/28)[367]، كأول نص دولي ملزم، يتعين بموجبه على الدول الأعضاء، اتخاذ الخطوات اللازمة على المستوى التشريعي، لتطبيق المبادئ التي تحددها الاتفاقية[368]. وتهدف هذه الاتفاقية، كما جاء في ديباجتها، إلى التوفيق بين احترام حقوق الإنسان وحرياته الأساسية ولا سيما احترام الحق في الخصوصية لجميع الأشخاص دون استثناء، وبين حرية تبادل المعلومات عبر الحدود، وتوفير الحماية القانونية للأفراد فيما يتعلق بالمعالجة الآلية لبياناتهم الشخصية[369]. 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

---

[367] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Strasbourg, 28.I.1981). Last updated: 10/6/2021. Available at: https://rm.coe.int/1680078b37

[368] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Strasbourg, 28.I.1981). 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".

[369] Preamble: The member States of the Council of Europe, signatory here to. 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".

نطاق عالمي وليس وطنيًا فقط[370]. وكان من المقرر أن تدخل حيز التنفيذ عند التصديق من قبل خمس دول أعضاء وهو ما حدث في تاريخ (1\10\1985)[371].

وضعت اتفاقية مجلس أوروبا مبادئ أساسية تمثل الحد الأدنى لحماية البيانات، التي ينبغي على الدول الأعضاء تضمينها في تشريعاتها الوطنية، وجاءت هذه المبادئ متقاربة مع المبادئ التوجيهية التي أقرتها منظمة التعاون الاقتصادي والتنمية، كما أضافت مبادئ تتعلق بحماية أصناف خاصة من البيانات متعلقة بالأصل العرقي أو الآراء السياسية والمعتقدات الدينية والإيديولوجية وبيانات الحياة الصحية والجنسية أو المتصلة بالأدلة الجنائية[372]. وتغطي الاتفاقية جميع ملفات البيانات الشخصية المؤتمتة في القطاعين الخاص والعام[373].

كما تنطبق الاتفاقية على جميع فئات البيانات الشخصية الآلية، مع إتاحة إمكانية أن تستثني الدول الأعضاء فئات معينة من البيانات الشخصية[374]، كما تنطبق الاتفاقية على الأشخاص الطبيعيين، ومع ذلك، يجوز

---

[370] أيوب (2009). مرجع سابق، ص: 315-316.

[371] CoE. Chart of signatures and ratifications of Treaty 108. Last updated: 21/3/2021. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108

[372] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Strasbourg, 28.I.1981). Article (6): "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions".

[373] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article (3/1): " The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors".

[374] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article (3/2/b): " 2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe: that it will not apply this Convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new

للدول الأعضاء توسيع نطاق تطبيق الاتفاقية لتشمل معالجة البيانات المتعلقة بالأشخاص الاعتباريين كالجمعيات والمؤسسات والشركات والنقابات وأي هيئات أخرى تتكون بشكل مباشر أو غير مباشر من الأفراد، سواء كانت هذه الهيئات تمتلك شخصية اعتبارية أم لا[375]. كما يقتصر نطاق الاتفاقية أيضًا على المعالجة الآلية أو المحوسبة للبيانات الشخصية ولا يشمل المعالجة اليدوية، ومع ذلك، يجوز للدول الأعضاء توسيع نطاق تطبيق الاتفاقية ليشمل المعالجة غير الآلية أو اليدوية للبيانات الشخصية[376].

3. تحديث اتفاقية مجلس أوروبا رقم (108) لحماية الأفراد من المعالجة الآلية للبيانات الشخصية: نظرًا لأهمية تبادل البيانات وتدفقها عبر الحدود الدولية، ومواكبة لهذه التحديات، وتفاديًا لبعض أوجه القصور في اتفاقية مجلس أوروبا رقم (108)، كان من الضروري تقوية الحماية، فخضعت الاتفاقية بمرور الوقت لعدة تحديثات، كان التحديث الأول بالبروتوكول الإضافي رقم (ETS No. 181) الصادر بتاريخ (2001/11/8)، المتعلق بالهيئات المشرفة على حماية البيانات وتدفقات البيانات عبر الحدود، والذي أضاف نقطتين أساسيتين؛ الأولى، إنشاء هيئات وطنية

declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law".

[375] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article (3/2/b): " 2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe: b. that it will also apply this Convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality".

[376] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Article (3/2/c): "Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe: c. that it will also apply this Convention to personal data files which are not processed automatically."

مشرفة على حماية البيانات، ومسؤولة عن ضمان الامتثال للقوانين أو اللوائح المعتمدة بموجب الاتفاقية، فيما يتعلق بحماية البيانات الشخصية وتدفقات البيانات عبر الحدود؛ والثانية، أن يكون البلد المرسل إليه البيانات متمتعًا بمستوى مماثل للحماية المقرة للبيانات الشخصية في البلد المرسل[377].

والتحديث الثاني بالبروتوكول الإضافي رقم (CETS 223) الصادر بتاريخ (2018/10/10)، الذي يوفر إطارًا قانونيًا قويًا ومرنًا، لتسهيل تدفق البيانات عبر الحدود مع توفير ضمانات فعّالة عند استخدام البيانات الشخصية، ومتعدد الأطراف، ليشكل جسراً بين مناطق مختلفة من العالم وأطر معيارية مختلفة، بما في ذلك لائحة الاتحاد الأوروبي التي أصبحت قابلة للتطبيق بالكامل في (25 أيار 2018). وأهم التحديثات الواردة في البروتوكول هي؛ متطلبات أقوى فيما يتعلق بمبادئ التناسب وتقليل البيانات، وقانونية المعالجة، وتوسيع أنواع البيانات الحساسة، لتشمل البيانات الجينية والبيومترية، والعضوية النقابية والأصل العرقي، والالتزام بالإعلان عن انتهاكات البيانات، وشفافية أكبر في معالجة البيانات، وحقوق جديدة لأصحاب البيانات في سياق صنع القرار، ومساءلة أقوى لمراقبي البيانات، وتطبيق مبادئ حماية البيانات على جميع أنشطة المعالجة، بما في ذلك المتعلقة بالأمن القومي، مع استثناءات وقيود محتملة تخضع لشروط تحددها الاتفاقية مع مراجعة وإشراف مستقل وفعّال، ونظام واضح لتدفقات

[377] Council of Europe. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181). Last updated: 21/3/2021. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181

البيانات عبر الحدود، وتعزيز الصلاحيات والاستقلالية لهيئات حماية البيانات وتعزيز الأساس القانوني للتعاون الدولي[378].

الفرع الثالث: جهود الأمم المتحدة في حماية البيانات الشخصية

كان لمنظمة الأمم المتحدة دور في تطوير حماية البيانات، وإن لم يكن دورها جوهريًا مثل المنظمتين الدوليتين السابقتين، إلا أنّه شكّل عاملًا مهمًا لتوجيه الانتباه الدولي إلى ضرورة حماية البيانات الشخصية تماشيًا مع التطور التكنولوجي الحاصل.

1. الجهود الأولية لمنظمة الأمم المتحدة في حماية البيانات الشخصية: كان أول صك للأمم المتحدة يتعامل بشكل مباشر مع حماية البيانات هو القرار الصادر عام (1968) عن الجمعية العامة، يدعو الأمين العام إلى تفحّص عدة أمور من بينها حق الأفراد في الخصوصية في ضوء التطورات التكنولوجية، أدت الدراسة الناتجة التي أجراها الأمين العام إلى نشر تقرير في عام (1976) يحثُّ فيه الدول اعتماد تشريع لحماية البيانات يغطي أنظمة البيانات الشخصية المؤتمتة في القطاعين العام والخاص، وإدراج معايير دنيا لهذه التشريعات[379].

2. دور إرشادات الأمم المتحدة لتنظيم ملفات البيانات الشخصية المؤتمتة لعام (1990) في حماية البيانات الشخصية: في تاريخ (1990/12/14) اعتمدت الجمعية العامة للأمم المتحدة القرار رقم (95/45)، المعروف

---

[378] Council of Europe. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Last updated: 21/3/2021. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223

[379] Bygrave. (2014). Data privacy law: An international perspective. P: 51.

بدليل الأمم المتحدة لتنظيم ملفات البيانات الشخصية المؤتمتة[380]، ويتكون الدليل من شقين؛ يحدد الشق الأول (الجزء أ) المبادئ التي تشكل الحد الأدنى من الضمانات التي يجب إدراجها في قوانين حماية البيانات الوطنية. وهذه المبادئ هي: مبدأ المشروعية والنزاهة (فقرة 1)، ومبدأ الدقة (فقرة 2)، ومبدأ تحديد الغرض (فقرة 3)، ومبدأ وصول أصحاب البيانات إلى بياناتهم (فقرة 4)، ومبدأ عدم التمييز (فقرة 5)، وصلاحية الاستثناء في حالات محددة (فقرة 6)، ومبدأ الأمن (فقرة 7)، ومبدأ الرقابة والعقوبات (فقرة 8)، ومبدأ تدفق البيانات عبر الحدود (فقرة 9)، ومبدأ نطاق التطبيق (فقرة 10)[381]. أما الشق الآخر (الجزء ب) فهو يتعلق بتطبيق الإرشادات على المنظمات الدولية (الحكومية وغير الحكومية)، ومعالجة البيانات الشخصية بطريقة مسؤولة وعادلة[382].

[380] Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990. Last updated: 3\6\2021. Available at: https://www.refworld.org/pdfid/3ddcafaac.pdf

[381] Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990, A. PRINCIPLES CONCERNING THE MINIMUM GUARANTEES THAT SHOULD BE PROVIDED IN NATIONAL LEGISLATIONS.

[382] Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990. B. APPLICATION OF THE GUIDELINES TO PERSONAL DATA FILES KEPT BY GOVERNMENTAL INTERNATIONAL ORGANIZATIONS.

ركّزت إرشادات الأمم المتحدة على بعض الجوانب المهمة، فقد وضعت أحكامًا لتطبيق مبادئ لحماية البيانات من قبل الهيئات الدولية[383]، كما طبقت المبادئ على المعالجة الآلية للبيانات إضافة للمعالجة اليدوية[384]، إلا أن تأثيرها كان أقل أهمية من غالبية الوثائق الدولية الرئيسية المذكورة سابقًا. وربما يعود ذلك إلى طبيعة هذه الوثيقة غير الملزمة، على الرغم من أنّ توصية منظمة التعاون الاقتصادي والتنمية الأكثر تأثيرًا لها الوضع نفسه، وذلك على خلاف اتفاقية مجلس أوروبا[385].

3. قرارات الجمعية العامة للأمم المتحدة بشأن الخصوصية في العصر الرقمي: بذلت الأمم المتحدة مؤخراً المزيد من الجهود، وقامت بدور نشط في مجال حماية البيانات، فأصدرت الجمعية العامة للأمم المتحدة قرارات بشأن

---

[383] Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990. B. APPLICATION OF THE GUIDELINES TO PERSONAL DATA FILES KEPT BY GOVERNMENTAL INTERNATIONAL ORGANIZATIONS." The present guidelines should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization.
Each organization should designate the authority statutorily competent to supervise the observance of these guidelines…"

[384] Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990, A. PRINCIPLES CONCERNING THE MINIMUM GUARANTEES THAT SHOULD BE PROVIDED IN NATIONAL LEGISLATIONS. "10. Field of application: The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals."

[385] Bygrave. (2014). Previous reference. P. 53.

الخصوصية في العصر الرقمي في الأعوام (2013)[386] (2014)[387] (2016)[388] (2018)[389] (2020)[390]، دعت فيها جميع الدول إلى اعتماد تشريعات ولوائح تنظيمية، وتنفيذ سياسات لحماية البيانات، بما فيها بيانات الاتصالات الرقمية، وإنشاء هيئات وطنية مستقلة تكون لها الصلاحيات والموارد اللازمة لرصد الممارسات المتعلقة بحماية البيانات، والتحقيق في الانتهاكات والتجاوزات، وتلقي البلاغات من الأفراد والمنظمات، وتوفير سبل الانصاف المناسبة، ومواصلة إعمال التشريعات واللوائح والسياسات[391]. ودعت الدول إلى حماية الأفراد من أي تجاوزات أو انتهاكات ماسة بالحق في الخصوصية، بما فيها تلك الناجمة عن عمليات جمع البيانات ومعالجتها وتخزينها وتداولها بطرق تعسفية أو غير قانونية[392]. ودعت جميع الدول أن تنظر في وضع تشريعات وتدابير وقائية ووسائل الانصاف اللازمة لمعالجة الضرر الناجم عن معالجة البيانات الشخصية أو استخدامها أو بيعها أو إعادة بيعها لمرات متعددة أو تداولها بشكل آخر بين المؤسسات التجارية دون موافقة الفرد الصريحة والحرة والمتنورة، وأن تواصل مراقبة إعمال التشريعات والتدابير ووسائل الانتصاف[393].

---

[386] قرار الجمعية العامة رقم 167/68 بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 18 كانون الأول/ديسمبر لعام 2013، متاح على الموقع الآتي: https://undocs.org/pdf?symbol=ar/A/RES/68/167 ، تاريخ الدخول إلى الموقع 2021/6/4 الساعة 10 صباحًا.

[387] قرار الجمعية العامة رقم 166/69 بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 18 كانون الأول/ديسمبر 2014، متاح على الموقع الآتي: https://undocs.org/pdf?symbol=ar/A/RES/69/166، تاريخ آخر زيارة 2021/6/4 الساعة 10 صباحًا.

[388] قرار الجمعية العامة رقم 199/71، بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 19 كانون الأول/ديسمبر 2016، متاح على الموقع الآتي: https://undocs.org/pdf?symbol=ar/a/res/71/199، تاريخ آخر زيارة 2021/6/4 الساعة 10 صباحًا.

[389] قرار الجمعية العامة رقم 73/ 179، بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 17 كانون الأول/ديسمبر 2018، متاح على الموقع الآتي: https://undocs.org/ar/A/RES/73/179 ، تاريخ آخر زيارة 2021/6/4 الساعة 10 صباحًا.

[390] قرار الجمعية العامة رقم 176/75، بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 16 كانون الأول/ديسمبر 2020، متاح على الموقع الآتي: https://undocs.org/ar/A/RES/75/176 ، تاريخ آخر زيارة 2021/6/4 الساعة 10 صباحًا.

[391] قرار الجمعية العامة رقم 176/75، لعام 2020، المرجع السابق، (7/ح).

[392] قرار الجمعية العامة رقم 176/75، لعام 2020، المرجع السابق، (7/ن)

[393] قرار الجمعية العامة رقم 176/75، لعام 2020، المرجع السابق، (7/ع).

كما دعت جميع المؤسسات التجارية التي تقوم بجمع البيانات وتخزينها واستخدامها وتداولها ومعالجتها أن تفي بمسؤوليتها عن احترام حقوق الإنسان بما في ذلك الحق في الخصوصية في العصر الرقمي، وأن تبلغ المستخدمين بطريقة واضحة ويسهل الاطلاع عليها بكل ما يمكن أن يمس بحقهم في الخصوصية من جراء جمع بياناتهم واستخدامها وتداولها والاحتفاظ بها[394]. وأن تنفذ ضمانات إدارية وتقنية ومادية لضمان أن تُعالج البيانات على نحو قانوني وأن تكون هذه المعالجة مقتصرة على ما هو ضروري ومشروع ودقيقة ونزيهة وسرية[395]. وأن تكفل للأفراد إمكانية الوصول إلى بياناتهم الشخصية واعتماد التدابير المناسبة التي تتيح إمكانية تعديل الموافقة المتعلقة بالبيانات وتصحيحها وتحديثها وحذفها وسحبها، ولا سيما إذا كانت البيانات غير صحيحة أو غير دقيقة، أو كان الحصول عليها بصورة غير قانونية[396].

المطلب الثاني: جهود الاتحاد الأوروبي في حماية البيانات الشخصية

بدأت جهود الاتحاد الأوروبي(EU)[397]، في تطوير حماية خاصة بالبيانات الشخصية، منذ عام (1976)، عندما أصدر الاتحاد تعليمات خاصة بحماية الأفراد من أنشطة التقويم الآلي للبيانات رقم (76/4/8)، والتعليمات

---

[394] قرار الجمعية العامة رقم 176/75، لعام 2020، المرجع السابق، (8/أ وب).

[395] قرار الجمعية العامة رقم 176/75، لعام 2020، المرجع السابق، (8/ج).

[396] قرار الجمعية العامة رقم 176/75، لعام 2020، المرجع السابق، (8/هـ).

[397] تم إنشاء المجموعة الاقتصادية الأوروبية (EEC) بموجب معاهدة روما لعام 1957 لتحقيق التكامل الاقتصادي في أوروبا من خلال إنشاء سوق مشتركة بين الدول الأعضاء فيها. في عام 1993، أعيدت تسميتها المجموعة الأوروبية (EC) بموجب معاهدة ماستريخت. في عام 2009، خلف الاتحاد الأوروبي (EU) المجموعة الأوروبية من خلال معاهدة لشبونة. الاتحاد الأوروبي هو شراكة اقتصادية وسياسية فريدة من نوعها بين 28 دولة أوروبية تغطي معظم القارة. لقد بدأ في البداية كاتحاد اقتصادي خالص، لكنه وسع نطاقه ليشمل مجالات السياسة مثل التنمية والبيئة. وسوقها الداخلي هو المحرك الاقتصادي للاتحاد الأوروبي. يتيح ذلك للسلع والخدمات والأموال والأشخاص التنقل بحرية عبر معظم أنحاء القارة. في الآونة الأخيرة، وسعت وظائفها لتشمل حقوق الإنسان:

European Parliament. How the European Union works. Last updated: (1/4/2022). Available at: https://www.europarl.europa.eu/factsheets/en/chapter/209/how-the-european-union-works

المتعلقة بحماية الافراد في مواجهة التطور التقني لمعالجة البيانات رقم (79/5/8)، والتعليمات رقم (82/3/9) بذات الموضوع[398]. ثم في وقت لاحق أصدر الاتحاد الأوروبي التوجيه رقم (EC/46/95) لعام (1995)، واستمرّ في تطوير الحماية فأصدر اللائحة العامة لحماية البيانات (GDPR) رقم (679) لعام (2016) التي حلت محل التوجيه السابق، وفيما يأتي عرض لأهم جهود الاتحاد الأوروبي في حماية البيانات الشخصية.

الفرع الأول: توجيه الاتحاد الأوروبي رقم (EC/46/95) لعام (1995)

أصدرت المفوضية الأوروبية[399] في عام (1981)، توصية تدعو البرلمان الأوروبي إلى التوقيع والتصديق على اتفاقية مجلس أوروبا[400]. وبحلول نهاية عام (1981)، بدأت المفوضية العمل على توجيه لحماية البيانات، وفي عام (1990)، أصدرت المفوضية الأوروبية أول اقتراح لها بشأن توجيه حماية البيانات[401]، ومن ثم أصدرت المفوضية اقتراحًا معدلًا في عام (1992)[402]. وبعد مرور ثلاث سنوات وتحديدًا في (1995/10/24)، أصدر

---

[398] أيوب. (2009). مرجع سابق. ص: 306.

[399] المفوضية الأوروبية: مقرها في بروكسل هي هيئة سياسية كبيرة مستقلة، تهتم بالمصالح الإجمالية للاتحاد الأوروبي وتدافع عنها، متجاوزة الحدود القومية. تتمتع المفوضية الأوروبية بسلطة تقديم المقترحات (حق المبادرة) لمختلف الأمور المشتركة والجماعية، كما تعتبر "الساهرة على حماية الاتفاقات"، وتراقب الالتزام بالحقوق العامة المشتركة كما تتمتع بصلاحيات السلطة التنفيذية، فيما يتعلق بالموازنة أو قوانين منع الاحتكار على سبيل المثال. وهي تمثل المصالح الجماعية العليا للاتحاد أمام الأطراف الخارجية.
https://www.deutschland.de/ar/topic/syast/mwssat-alathad-alawrwby-wmhmatha-fy-lmht-sryt

[400] Commission Recommendation of 29 July 1981 relating to the Council of Europe convention for the protection of individuals with regard to automatic processing of personal data (81/679/EEC). Last updated: 5/6/2021. Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31981H0679

[401] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data. (Submitted by the Commission on 27 July 1990). Last updated: 5/6/2021. Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990PC0314(01)&from=HU

[402] Amended proposal for a COUNCIL DIRECTIVE on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (15 October 1992). Last updated: 5/6/2021. Available at: http://aei.pitt.edu/10375/1/10375.pdf

البرلمان[403] ومجلس الاتحاد الأوروبي[404] توجيه حماية الأفراد من معالجة البيانات الشخصية وحرية نقلها رقم (EC/46/95)[405].

1. دور توجيه الاتحاد الأوروبي رقم (EC/46/95) لعام (1995) في حماية البيانات الشخصية: وسّع توجيه الاتحاد الأوروبي من نطاق الحماية الممنوحة للبيانات الشخصية، وغطى مختلف أنواع البيانات الشخصية المعالجة بوسائل آلية كليًا أو جزئيًا[406]. كما عرّف مصطلحات جديدة كالبيانات الشخصية، معالجة البيانات، مراقب المعالجة، المعالج، المتلقي، أصحاب البيانات، واقتصر تطبيق هذا الدليل على عمليات معالجة البيانات الشخصية التي تجري ضمن الاتحاد الأوروبي فقط، مستثنيًا عمليات المعالجة الخاصة بالسلامة العامة والدفاع وأمن الدولة ونشاطات الحكومة في المجال الجزائي[407]. وقد شكل التوجيه نواة الحركة التشريعية الأوروبية الهادفة إلى حماية البيانات الشخصية. ومن حيث مبادئ الحماية المقررة فقد جاءت أوسع وأكثر شمولية من المبادئ التي تضمنتها الوثائق

---

[403] البرلمان الأوروبي: البرلمان الأوروبي هو الهيئة البرلمانية للاتحاد الأوروبي. وهو يتألف من 751 عضوا، يتم انتخابهم من قبل مواطني الدول الأعضاء السبع والعشرين بطريق الانتخاب المباشر لمدة خمس سنوات. ولكل دولة من الدول الأعضاء عدد من المقاعد البرلمانية يتناسب وعدد سكانها. ويتمتع البرلمان بسلطة إقرار القوانين والموازنة وبصلاحيات الرقابة، إلا أنه لا يتمتع بحق الاقتراح (المبادرة) في مجال القوانين. مقر البرلمان في مدينة ستراسبورغ، وتتوزع مكاتب عمله في كل من بروكسل ولوكسمبورغ.
https://www.deutschland.de/ar/topic/syast/mwssat-alathad-alawrwby-wmhmatha-fy-lmht-sryt

[404] مجلس الاتحاد الأوروبي: المجلس الذي يعرف باسم "المجلس الوزاري" هو أهم هيئة تشريعية في الاتحاد الأوروبي. وتشارك كل من الدول الأعضاء في الاتحاد الأوروبي هذا المجلس بوزير مختص. فالمجلس يتقاسم مع البرلمان الأوروبي الصلاحيات التشريعية والمسؤولية عن موازنة الاتحاد الأوروبي. وتتناوب الدول على رئاسة المجلس كل ستة أشهر.
https://www.deutschland.de/ar/topic/syast/mwssat-alathad-alawrwby-wmhmatha-fy-lmht-sryt

[405] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[406] Directive 95/46/EC. Article (3/1): " 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."

[407] الأشقر جبور، منى. (د.ت). السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية. ص: 137.

السابقة[408]، وبقي هذا التوجيه بمثابة المرجعية العامة لحماية البيانات الشخصية في أوروبا ومرجعًا توجيهيًا غير ملزم لباقي دول العالم إلى وقت قريب، انتهى بإصدار الاتحاد الأوروبي اللائحة العامة لحماية البيانات الشخصية.

2. أوجه قصور توجيه الاتحاد الأوروبي رقم (EC/46/95) لعام (1995): على الرغم من أن الاتحاد الأوروبي وافق على التوجيه وألزم الدول الأعضاء في الاتحاد بوجوب تضمين أحكامه في تشريعاتها الوطني خلال ثلاث سنوات من تاريخ إصداره، إلا أنّه ينبغي على كل دولة عضو أن تسن تشريعات وطنية لحماية البيانات ليصبح بموجبها التوجيه نافذًا[409]، كما اقتصر تطبيق قواعد هذا التوجيه على عمليات معالجة البيانات الشخصية التي تجري ضمن الاتحاد الأوروبي[410]. ومع ذلك فإنّ قواعد التوجيه كانت قابلة للتطبيق والتأثير على نطاق واسع؛ ففي عام (1992)، دمج التوجيه في اتفاقية المنطقة الاقتصادية الأوروبية، بحيث تكون الدول الأطراف في اتفاقية المنطقة الاقتصادية الأوروبية، وغير الأعضاء في الاتحاد الأوروبي ملزمة قانونًا بجعل قوانينها متوافقة مع التوجيه[411]. علاوة على ذلك، كان للتوجيه تأثير كبير على البلدان الأخرى خارج الاتحاد الأوروبي، لأسباب ليس أقلها حظر نقل البيانات الشخصية إلى هذه الدول، ما لم توفر مستويات مناسبة من حماية البيانات[412].

---

[408] أيوب. (2009). مرجع سابق، ص321-322.

[409] Directive 95/46/EC. Article (32/1): " 1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption."

[410] Directive 95/46/EC. Article (34): "This Directive is addressed to the Member States."

[411] Bygrave. (2014). Previous reference. P. 54.

[412] Directive 95/46/EC. Article (25/1): "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

الفرع الثاني: لائحة الاتحاد الأوروبي لحماية البيانات (GDPR) رقم (679) لعام (2016)

1. الدعوة إلى وجوب تطوير الحماية القانونية للبيانات الشخصية: بعد أن جلبت التطورات التكنولوجية السريعة والعولمة تحديات جديدة لحماية البيانات الشخصية، وأدت إلى ازدياد حجم جمع البيانات الشخصية وتبادلها، وسمحت لكل من الشركات الخاصة والسلطات العامة باستخدام البيانات الشخصية على نطاق واسع وغير مسبوق من أجل متابعة أنشطتها، بالإضافة إلى قيام الأفراد عمومًا بإتاحة معلوماتهم الشخصية[413]، الأمر الذي أدى إلى أن يطلب المجلس الأوروبي[414] من المفوضية الأوروبية، تقويم أداء الاتحاد الأوروبي بحماية البيانات، وتقديم مبادرات تشريعية إذا دعت الضرورة لذلك، وخلصت المفوضية إلى أنّ الاتحاد الأوروبي يحتاج إلى سياسة أكثر شمولاً وتماسكًا بشأن الحق الأساسي في حماية البيانات الشخصية، وبتاريخ (2012/1/25) قدمت المفوضية الأوروبية إلى مجلس الاتحاد الأوروبي والبرلمان الأوروبي حزمة من المقترحات التشريعية، تتعلق بمشروع لائحة عامة لحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات، لتحل محل التوجيه

---

[413] European Commission. Brussels (25.1.2012). COM (2012) 11 final. 2012/0011 (COD). C7-0025/12. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Last updated: 20\6\2021. Available at: https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf. & GDPR. Recital (6): "Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally…"

[414] المجلس الأوروبي: يمثّل المجلس الأوروبي أرفع مستوى من التعاون السياسي بين بلدان الاتحاد الأوروبي. يضمّ رؤساء دول أو حكومات البلدان الأعضاء ورئيس المجلس الأوروبي ورئيس المفوضية الأوروبية والممثل الأعلى للاتحاد الأوروبي للشؤون الخارجية والسياسة الأمنية. يقرّر المجلس الأوروبي التوجّه العام للاتحاد الأوروبي وأولوياته السياسية. كما يرسم السياسة الخارجية والأمنية المشتركة للاتحاد. أنظر: https://euromedrights.org/ar

(EC/46/95)، وتضع قانونًا موحدًا لجميع أنشطة معالجة البيانات في جميع أنحاء الاتحاد الأوروبي، وتحدّ من الاختلافات الحالية بين القوانين الوطنية[415]. وبتاريخ (24 و2013/10/25) أكّد المجلس الأوروبي على أهمية اعتماد إطار قوي لحماية البيانات الشخصية في الاتحاد الأوروبي، من أجل تعزيز ثقة المواطنين والشركات في الاقتصاد الرقمي[416]. وبعد أربع سنوات من المداولات، وتحديدًا بتاريخ (2016/4/27)، توصلت الهيئات التشريعية في الاتحاد الأوروبي إلى اتفاق بشأن قانون جديد لحماية البيانات، وأصدر الاتحاد الأوروبي اللائحة العامة لحماية البيانات الشخصية رقم (679) في (2016/4/14)[417]، ودخلت حيز النفاذ اعتبارًا من (2018/5/25) لتحل محل التوجيه رقم (EC/46/95)، وقد مثّلت اللائحة العامة لحماية البيانات الشخصية تغيير مهم جدًا في قانون حماية البيانات الأوروبي، منذ اعتماد توجيه حماية البيانات للاتحاد الأوروبي (EC/46/95) عام (1998)[418].

---

[415] European Commission. Brussels (25.1.2012). COM (2012) 11 final. 2012/0011 (COD). C7-0025/12. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Previous reference.

[416] The European Council conclusions and Statement of Heads of State or Government. Brussels. 24/25 October 2013. "8. It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015". Last updated: 20\6\2021. Available at: https://www.eu.dk/-/media/files/topmoeder/2425102013_delkonklusion.ashx

[417] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[418] Kuner, Christopher. (2012). The European Commission's Proposed Data Protection Regulatio: A Copernican Revolution in European Data Protection Law. Privacy & Security Law Report. P: 1. http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf

2. دور اللائحة العامة للاتحاد الأوروبي في حماية البيانات الشخصية: بعد أن غيّر التطور التكنولوجي كلًا من الحياة الاجتماعية والاقتصاد، كان لا بد من تسهيل تدفق البيانات الشخصية عبر الحدود الوطنية، ولكن مع ضمان مستوى عالٍ من حماية البيانات الشخصية[419]، الأمر الذي يتطلب وجود إطار قوي وأكثر تماسك لحماية البيانات الشخصية[420]. وقد عززت اللائحة حماية البيانات الشخصية في أوروبا، وحققت الانسجام بين القوانين الأوروبية وواكبت التطورات المتسارعة في مجال تقنيات المعلومات من جهة أخرى[421]. كما تجاوزت نقاط الضعف في التوجيه الأوروبي السابق من حيث؛ إلزامية قواعدها بصفتها قانونًا عامًا ملزمًا لدول الاتحاد الأوروبي، وليس مجرد إرشادات أو توجيهات أو توصيات كالتوجيه الأوروبي[422]، ومن حيث؛ مجال التطبيق فاللائحة ملزمة لأي كيان يقوم بمعالجة بيانات شخصية لجميع الأفراد المقيمين في الاتحاد الأوروبي حتى لو كان المتحكم أو المعالج موجودًا خارج النطاق الإقليمي لدول الاتحاد الأوروبي[423].

---

[419] European Commission. Brussels (25.1.2012). COM (2012) 11 final. 2012/0011 (COD). C7-0025/12. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Previous reference. & GDPR. Recital (6): " ...Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data."

[420] GDPR. Recital (7): "Those developments require a strong and more coherent data protection framework in the Union..."

[421] الأشقر جبور، وجبور. (2018). مرجع سابق. ص: 55.

[422] GDPR. Article (99): "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"

[423] GDPR. Article (3): "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

وقد أكّدت اللائحة بأنّها تحترم جميع الحقوق الأساسية والحريات والمبادئ المعترف بها في الميثاق على النحو المنصوص عليه في المعاهدات، ولا سيما الحياة الخاصة والعائلية والمنزل والاتصالات وحماية البيانات الشخصية وحرية الفكر والضمير والدين، وحرية التعبير والإعلام، وحرية إدارة الأعمال التجارية، والحق في الحصول على تعويض مؤثر ومحاكمة عادلة، واحترام التنوع الثقافي والديني واللغوي[424]. كما أقرّت عددًا من الحقوق الجديدة للأفراد لإتاحة الفرصة أمام أصحاب البيانات الشخصية باستعادة السيطرة على بياناتهم، وهو ما سيشار إليه في موضع لاحق من البحث. لتصبح اللائحة الأوروبية بداية حقيقة لقواعد عالمية ملزمة في مجال حماية البيانات خارج أوروبا. وتعبّر عن سياسات جديدة تمثل نموذجًا لانتشارها في باقي دول العالم، تعزز معها الانتقال من حالة الفوضى إلى حالة التنظيم، ومن حالة الانفتاح اللامحسوب إلى حالة الانفتاح المنضبط، كما تعبّر عن حالة دولية جديدة للتعامل مع العولمة ومؤسساتها وفاعليها في مواجهة المصالح الوطنية، وعن الانتقال من مرحلة تراجع دور الدولة في مجال الأمن والحماية إلى استعادة دورها مرة أخرى وفق بيئة جديدة[425].

---

in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union. 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."

[424] GDPR. Recital (4): "This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

[425] كتاب البيانات الشخصية: الصراع على نفط القرن الحادي والعشرين. (2018/6/22). الموسوعة الجزائرية للدراسات والاستراتيجية. آخر زيارة: 2020/9/25. متاح على الرابط: https://www.politics-dz.com/

المبحث الثاني: التنظيم القانوني لحماية البيانات الشخصية

يقصد بحماية البيانات الشخصية مجموعة القواعد المتعلقة بمعالجة البيانات الشخصية، التي يجب أن يأخذها المشرع في اعتباره عند صياغة القوانين، ويجب أن يأخذها في الاعتبار أيضًا المتحكمون بالبيانات الشخصية والقائمون على عملية معالجتها، هذه العملية لا تنتهي بوضع القواعد، وإنّما هي عملية مستمرة فمن الضروري تطوير القواعد القانونية في كل مرة تظهر فيها تحديات جديدة بسبب التطورات التكنولوجية الجديدة[426].

لقد جاء الاهتمام بحماية البيانات الشخصية وتطوير تشريعات خاصة لحمايتها نتيجة أربعة عوامل مترابطة؛ العامل الأول الذي أثار القلق هو أنّ أجهزة الكمبيوتر حسنت القدرة على تخزين المعلومات واسترجاعها ونقلها، هذه التحسينات يمكن أن تؤدي إلى خدمات أكثر كفاءة وفعالية من جهة، ولكن من جهة أخرى فإن قدرة الكمبيوتر على تخزين كميات كبيرة من المعلومات تثير أيضًا سؤالًا مهمًا حول جمع المعلومات غير الضرورية وغير ذات الصلة بسبب سعة تخزين الكمبيوتر[427]. أما العامل الثاني هو تزايد القلق بشأن بنوك البيانات الحكومية أو مستودعات البيانات، فالحكومات تجمع مجموعة هائلة من المعلومات حول الأفراد بسبب طبيعة ومدى الخدمات التي يقدمونها، مثل الرعاية الصحية والخدمات الاجتماعية والتعليم والترخيص، ولكن من جهة أُخرى، أثارت قدرة الجهات الحكومية على ربط فئات مختلفة من المعلومات حول الفرد عبر الإدارات الحكومية المختلفة[428]، سؤالًا مهمًا حول إذا كان من الجائز إجراء مقارنات بين قواعد البيانات المختلفة من خلال مطابقة البيانات، وإنشاء ملفات تعريف إلكترونية

---

[426] Stefanick. (2011). Previous reference. P: 43.

[427] Stefanick. (2011). Previous reference. P: 42.

[428] الموسوي؛ وفضل الله. (2013م). مرجع سابق. ص: 12-13.

للأفراد، والتنقيب في البيانات لتحديد اتجاهات وأنماط السلوك[429]؛ والعامل الثالث هو أنّ التجارة الإلكترونية تثير مخاوف بشأن حماية البيانات فيما يتعلق بالإنترنت، فشركات الإنترنت تعمل على تحديد ملفات تعريف المستهلكين وتتبعها وتطويرها، وهو ما يشعر المستهلكون بالقلق إزاء عدم إخفاء الهوية، فضلاً عن البيع المحتمل لمعلوماتهم الشخصية إلى أطراف ثالثة لأغراض متنوعة[430]، وبالتالي لن يقدم مستخدمو شبكة الإنترنت على التجارة الإلكترونية في ظل خشيتهم على بياناتهم الخاصة[431]، ولذلك فإن وجود حماية قانونية للبيانات الشخصية يشجع التجارة الإلكترونية، وفي حالة عدم وجود قانون لحماية البيانات، سيفتقر عامة الناس إلى الثقة للمشاركة في التجارة[432]؛ أما العامل الرابع الذي يسهم في انتشار حماية البيانات الشخصية هو تشريعي، فتشريعات الاتحاد الأوروبي تثير إمكانية فرض عقوبات تجارية ضد الدول التي لم تنظم قوانينها حماية ملائمة للبيانات الشخصية[433]، فإذا لم يكن بالإمكان التأكد من أنّ معلوماتهم الشخصية ستعامل بالاحترام نفسه، كما هو الحال في دولهم، فيبدو من المعقول عدم السماح بعمليات نقل هذه البيانات[434].

أقرّت قوانين حماية البيانات الشخصية مبادئ أساسية لحماية البيانات، وتعدّ هذه المبادئ المصدر الأساسي لحقوق الأشخاص المعنيين بالبيانات، والتزامات القائمين على عمليات المعالجة ومن هنا سيتعرض هذا الفصل

---

[429] Stefanick. (2011). Previous reference. P: 43.

[430] Stefanick. (2011). Previous reference. P: 44.

[431] فكري. (2007). مرجع سابق، ص: 752.

[432] Bygrave. (2014). Previous reference. P: 11.

[433] Stefanick. (2011). Previous reference. P: 45-46.

[434] Stefanick. (2011). Previous reference. P: 47.

لمبادئ حماية البيانات الشخصية (المطلب الأول)، والحقوق والالتزامات في إطار حماية البيانات الشخصية (المطلب الثاني).

المطلب الأول: مبادئ حماية البيانات الشخصية

أقرّت معظم قوانين حماية البيانات الشخصية مجموعة من المبادئ، تعبّر عن معايير دنيا يجب أن تتوافر في أي قانون يسعى لحماية البيانات الشخصية[435]. تشكّل هذه المبادئ نقطة الانطلاق الرئيسية لحماية البيانات الشخصية، فهي تسعى إلى وضع مبادئ أساسية يجب على القائمين على معالجة البيانات الالتزام بها، لتحقيق توازن بين المصالح المتضاربة لأصحاب البيانات من جهة، والقائمين على معالجة البيانات من جهة أخرى، كما وضعت قوانين حماية البيانات الشخصية مجموعة من الاستثناءات على هذه المبادئ، مراعاةً لبعض المصالح الأجدر بالحماية؛ ومن هنا، سيتعرض هذا المطلب لهذه المبادئ (الفرع الأول)، واستثناءاتها (الفرع الثاني)، كما وردت في التشريعات محل الدراسة، وبصورة خاصة اللائحة الأوروبية، مع الأخذ بموقف المشرّع المصري.

الفرع الأول: المبادئ المتعلقة بمعالجة البيانات الشخصية ومشروعيتها

إنّ تجنب المساس بحق الأفراد في حماية بياناتهم الشخصية عند معالجة هذه البيانات، يقتضي وضع مبادئ تكون بمثابة ضمانات لأصحاب البيانات، ويمكن تصنيف هذه المبادئ إلى مبادئ متعلقة بمعالجة البيانات الشخصية، ومبادئ متعلقة بمشروعية معالجة البيانات الشخصية.

---

[435] إكسس ناو. (2018). مرجع سابق. ص: 5.

أولًا: المبادئ المتعلقة بمعالجة البيانات الشخصية

حظرت القوانين الخاصة بحماية البيانات الشخصية معالجة البيانات الشخصية، بطريقة تمس حقوق أصحابها، أو حرياتهم الخاصة والعامة، أو تسيء إليهم وتشهر بهم، ومع أنّ المصدر الأساسي لهذه المبادئ هو المعايير الدولية، ولا سيما إرشاد منظمة التعاون الاقتصادي والتنمية واتفاقية مجلس أوروبا[436]، إلا أنّ هذه المبادئ تداخلت واختلف تنظيمها بين تشريع وآخر، ويمكن تفسير هذا الأمر، بناءً على فلسفة القانون وأهدافه[437]، كما اختلفت القوانين لناحية إعطاء تفاصيل أو إقرار مبدأ عام، وربما يعود هذا الاختلاف إلى تطور مفهوم الحماية ومسايرة القوانين لمستجدات التطور التكنولوجي. ومع الأهمية الكبيرة لهذه المبادئ نجد أنّ المشرّع المصري لم يفرد مادة خاصة بها، وإنما أشار إليها ضمن شروط المعالجة. وفيما يأتي عرض لهذه المبادئ كما وردت في اللائحة الأوروبية.

1. مبدأ الشرعية والانصاف والشفافية: يعني هذا المبدأ أنّ عملية معالجة البيانات الشخصية يجب أن تتم بطريقة قانونية وعادلة وشفافة[438]. مما يعني أنّه يجب جمع البيانات الشخصية التي تخضع للمعالجة بطريقة قانونية أي أن تكون معالجة البيانات وفق أساس قانوني واضح ومن أجل غاية مشروعة، وبطريقة عادلة، فيجب أن يكون

---

[436] أورد دليل منظمة التعاون الاقتصادي والتنمية، مبادئ المعالجة، في الجزء الثاني الذي جاء بعنوان "المبادئ الأساسية للتطبيق الوطني" وفي الجزء الثالث الذي حمل عنوان "المبادئ الأساسية للتطبيق الدولي". بينما وردت في اتفاقية مجلس أوروبا في الفصل الثاني، وعنوانه "المبادئ الأساسية لحماية البيانات"، وأوردها قرار الجمعية العامة للأمم المتحدة رقم 95/45 لعام 1990 لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية، في الفقرة (أ)؛ وأوردها التوجيه الأوروبي لعام 1995، في المادة (6) التي جاءت بعنوان: "المبادئ المتعلقة بجودة البيانات"، وتطرقت إليها اللائحة الأوروبية لعام 2016، في المادة (5) التي جاءت بعنوان: "المبادئ المتعلقة بمعالجة البيانات الشخصية".

[437] الأشقر جبور. مرجع سابق. ص: 121.

[438] GDPR. Article (5/1/a): "1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)"

واضحًا للأشخاص الطبيعيين أن البيانات الشخصية المتعلقة بهم يتم جمعها أو استخدامها أو معالجتها بطريقة أخرى وإلى أي مدى يتم أو سيتم معالجة البيانات الشخصية[439]. ويتطلب مبدأ الشفافية توفير معلومات لأصحاب البيانات حول هوية المتحكم، وأغراض المعالجة، والبيانات المتعلقة بهم التي تعالج، وأن تكون المعلومات حول البيانات الشخصية المعالجة سهلة الوصول والفهم، وأن تستخدم لغة واضحة وواضحة، كما يجب توعية أصحاب البيانات بالمخاطر والقواعد والضمانات، وحقوقهم فيما يتعلق بمعالجة البيانات الشخصية، وكيفية ممارستهم لهذه الحقوق[440]، حتى يتمكن أصحاب البيانات من التعرف بشكل كافٍ على كيفية جمع البيانات الخاصة بهم واستخدامها وتخزينها، وعن الجهة التي تقوم بذلك[441].

2. مبدأ تحديد غرض الجمع: يعني هذا المبدأ أن يكون الغرض من جمع البيانات محددًا ومشروعًا ومعلنًا حتى يتسنى فيما بعد التحقق من أن؛ جميع البيانات الشخصية، التي جُمعت ذات صلة بالغاية المستهدفة، وأنّ أيًا من للبيانات التي جُمعت أو عولجت لغاية معينة لا تستخدم لغاية أخرى لا تتفق مع الغايات المحددة[442]. ويجب أن

---

[439] GDPR. Recital (39): "Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed… ".

[440] GDPR. Recital (39): "…The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…".

[441] إكسس ناو. (2018). مرجع سابق. ص: 5.

[442] GDPR. Article (5/1/b): "(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"

تكون الأغراض المحددة التي تعالج البيانات الشخصية من أجلها صريحة وشرعية ومحددة في وقت جمع البيانات الشخصية[443].

3. مبدأ محدودية جمع البيانات (تقليل جمع البيانات): أي أن يكون جمع البيانات الشخصية ضمن حدود؛ فيجب أن تكون البيانات الشخصية كافية وذات صلة ومتناسبة مع أغراض المعالجة وألا يكون هناك إفراط في ذلك[444]. ويجب أن تقتصر البيانات الشخصية التي تُجمع أو تُستخدم على ما هو ضروري للأغراض المحددة التي تعالج البيانات من أجلها[445]، وهذا يتطلب بصورة خاصة، التأكد من أنّ الفترة التي يتم فيها تخزين البيانات الشخصية محدودة إلى الحد الأدنى، ولا ينبغي معالجة البيانات الشخصية إلا عندما يكون الغرض من المعالجة لا يمكن تحقيقه بوسائل أخرى[446].

---

[443] GDPR. Recital (39): "… the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed…".

[444] إكسس ناو. (2018). مرجع سابق. ص: 5.

[445] GDPR. Article (5/1/c): "(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"

[446] GDPR. Recital (39): "…This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means…".

4. مبدأ دقة البيانات: يعني هذا المبدأ اتخاذ الإجراءات لضمان أن البيانات الشخصية دقيقة، وتراعي الأغراض التي تتم معالجتها من أجلها، بما في ذلك محوها أو تصحيحها دون تأخير[447]. ويجب اتخاذ كل خطوة معقولة لضمان تصحيح أو حذف البيانات الشخصية غير الدقيقة[448].

5. مبدأ قيود التخزين: يوجب هذا المبدأ الاحتفاظ بالبيانات بطريقة تسمح بتحديد أصحاب البيانات، وألا تتجاوز مدة الاحتفاظ بالبيانات الشخصية المدة التي تتيح بلوغ الغاية المحددة من المعالجة[449]. ومن أجل ضمان عدم الاحتفاظ بالبيانات الشخصية لفترة أطول مما يجب، ينبغي أن يحدد المتحكم بالبيانات حدودًا زمنية للمسح أو المراجعة الدورية[450].

6. مبدأ الأمن والسرية: يعني هذا المبدأ أنه ينبغي معالجة البيانات الشخصية بطريقة تضمن الأمان المناسب وسرية البيانات الشخصية، بما في ذلك منع الوصول غير المصرح به إلى البيانات الشخصية[451]، واتخاذ التدابير التقنية أو التنظيمية الملائمة في معالجة البيانات الشخصية لحمايتها ضد المخاطر الطبيعية، مثل فقدها أو تلفها

---

[447] GDPR. Article (5/1/d): "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

[448] GDPR. Recital (39): "…Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted…"

[449] GDPR. Article (5/1/e): (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;… ('Storage limitation').

[450] GDPR. Recital (39): "… In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review."

[451] GDPR. Recital (39): "…Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing".

أو تضررها عرضيًا، أو ضد المخاطر البشرية مثل المعالجة غير المصرح بها أو غير المشروعة، والاطلاع عليها بغير إذن أو استخدام البيانات بشكل غير آمن[452].

7. مبدأ المسائلة: يفرض هذا المبدأ على الأطراف التي تقوم بمعالجة البيانات، المسؤولية عن التزامها بمبادئ معالجة البيانات الشخصية، التي وردت في المادة (1/5) من اللائحة الأوروبية والتي سبق عرضها، وهي؛ مبدأ الشرعية والانصاف والشفافية؛ ومبدأ تحديد غرض الجمع؛ ومبدأ تقليل الجمع؛ ومبدأ دقة البيانات؛ ومبدأ قيود التخزين؛ ومبدأ النزاهة والسرية، من جهة، وأن تكون قادرة على إثبات امتثالها لهذه المبادئ من جهة ثانية[453].

أما قانون حماية البيانات الشخصية المصري فلم ينص على مبادئ معالجة البيانات فقد أوردت المادة (4) عدد من الالتزامات على المتحكم، تتماشى مع التزامه بمبادئ المعالجة التي نصت عليها اللائحة، مثل التزام المتحكم بالتأكّد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها (المادة 2/4)؛ ووضع طريقة وأسلوب ومعايير المعالجة طبقا للغرض المحدد (المادة 3/4)؛ والتأكد من انطباق الغرض المحدد من جمع البيانات (المادة 4/4)؛ ومحو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها (المادة 7/4)؛ وتصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به (8/4).

---

[452] GDPR. Article (5/1/f): (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

[453] GDPR. Article (5/2) "2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

ثانيًا: المبادئ المتعلقة بمشروعية معالجة البيانات الشخصية

وفقًا للمادة (8) من ميثاق الحقوق الأساسية للاتحاد الأوروبي، يجب معالجة البيانات الشخصية بشكل عادل، ولأغراض محددة، وعلى أساس مشروع ينص عليه القانون. وفي هذا الصدد، تحدد المادة (1/6) من اللائحة العامة لحماية البيانات (GDPR) مجموعة من الأسس لتكون المعالجة قانونية. ولتحديد الأساس القانوني المناسب أهمية كبيرة، حيث إنّ تطبيق بعض حقوق أصحاب البيانات قد يختلف اعتمادًا على الأساس القانوني الذي تستند إليه المعالجة، فعلى سبيل المثال، قد تؤدي المعالجة الضرورية لتنفيذ عقد يكون صاحب البيانات طرفًا فيه، أو لاتخاذ خطوات بناء على طلب صاحب البيانات قبل الدخول في عقد إلى الحق في نقل البيانات بموجبه، ولكن لن يؤدي إلى الحق في الاعتراض على المعالجة[454].

وتتعلق مبادئ مشروعية معالجة البيانات بتحديد الأساس القانوني الذي يسمح بمعالجة البيانات الشخصية. ولكي تكون المعالجة مشروعة، يجب معالجة البيانات الشخصية على أساس موافقة صاحب البيانات المعني، أو على أساس شرعي آخر ينص عليه القانون، مثل تنفيذ عقد يكون صاحب البيانات طرفًا فيه، والامتثال لالتزام قانوني يخضع له المتحكم. وقد أشار المشرع المصري لموافقة المعني بالبيانات في المادة (6)[455]، التي جاءت

---

[454] Guidelines 2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects. Adopted on 9 April 2019. N. 1-2. P: 3.

[455] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (6): "تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر إحدى الحالات الأتية: 1. موافقة الشخص المعني بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر".

تحت عنوان شروط المعالجة. ولتكون عملية معالجة البيانات مستندة على أساس قانوني يجب أن تنطبق على حالة واحدة على الأقل من الحالات الآتية.

1. حالة رضا الشخص المعني بمعالجة بياناته الشخصية.

يعدّ رضا الشخص المعني بالبيانات على معالجة بياناته، لغرض محددة وبصورة مسبقة[456]، ومن أجل تحقيق غرض محدد أو أكثر[457]، شرطًا أساسيًا لمشروعية كافة عمليات المعالجة على بياناته الشخصية، سواء بجمع هذه البيانات أو الإفصاح عنها أو نشرها.

أ. تعريف موافقة المعني بالبيانات: عرفت المادة (11/4) من اللائحة الأوروبية موافقة صاحب البيانات بأنّها تعني: أي إشارة صريحة ومحددة وواضحة لا لبس فيها، تدل على رضا صاحب البيانات، يشير من خلالها إلى الموافقة على معالجة البيانات الشخصية المتعلقة به، وذلك من خلال بيان، أو عمل إيجابي واضح[458]. بينما أغفل المشرّع المصري تعريف المعني بالبيانات، لكنه اشترط صراحة وجود موافقة الشخص المعني بالبيانات على جمع بياناته أو معالجتها بصورة صريحة[459]. ووجود الرضا، مشروطة بوجود الإرادة[460] الصادرة عن صاحبها[461].

---

[456] GDPR. Article (6/1/a): "(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes."

[457] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (1/6).

[458] GDPR. Article (4/11): "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

[459] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (2): "لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح أو الافشاء عنها بأية وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانونًا"

[460] أبو العيال، أيمن، صالح، فواز. (2016-2017). القانون المدني، مصادر الالتزام. ص42.

[461] صالح، فواز. (2011-2012). القانون المدني، مصادر الالتزام، الجزء الأول، المصادر الإرادية. ص140.

فموافقة الشخص هـي أساس مشروعية المعالجة، ومرجع ذلك إلـى أنّ بياناته تعبّر عن شخصيته، وقد تمتد إلى حياته الخاصة والعائلية التي يحرص أن تكون بعيدة عن الأنظار[462]، أو تمس أيًا من حقوقه الأخرى.

ب. شروط موافقة المعني بالبيانات على معالجة بياناته الشخصية: يجب لتوافر رضا الشخص بمعالجة بياناته وجود الإرادة، ويجب أن يعبّر عنها بصورة صريحة جازمة، تعبّر عن موافقته على العمليات المزمع القيام بها على بياناته، وبالتالي لا يعتد بالتعبير الضمني عن الموافقة أو الموافقة المعلقة على شرط، كما لا يشكّل الصمت أو المربعات المحددة مسبقًا أو السكون موافقه[463].

ومن ثم يكون للشخص وفقاً للقواعد العامة حرية كاملة في التعبير عن موافقته الصريحة على الوجه الذي يراه، فالتعبير يكون صريحاً إذا قصد به صاحبه إحاطة الغير علماً بإرادته، أياً كان المظهر الذي يتخذه، شفاهه أو الكتابة، أياً كانت عباراتها أو صورتها أو بالإشارة التي لها دلالة بين الناس[464]. ويكون التعبير عن الإرادة بشكل صريح على شبكة الإنترنت بالكتابة الإلكترونية، أو من خلال الضغط على زر الموافقة، أو الكلام في التفاعل المباشر، والصور الأكثر انتشارًا للتعبير عن الإرادة عبر شبكة الإنترنت هي الكتابة الإلكترونية، واتخاذ موقف لا تدع ظروف الحال شكًا في دلالته على حقيقة المقصود من خلال الضغط على أيقونة الموافقة، أمّا الصور الأقل شيوعًا فهي التعبير عن الإرادة بالكلام أو الإشارة المتداولة عرفًا[465].

---

[462] مركز بحوث القانون والتكنولوجيا. (2020). دراسة نقدية لقانون حماية البيانات الشخصية رقم (151) لسنة 2020. مرجع سابق. ص: 51.

[463] GDPR. Recital (32): "... Silence, pre-ticked boxes or inactivity should not therefore constitute consent..."

[464] تنص المادة (1/93) من القانون المدني السوري والتي يقابلها المادة (1/90) من القانون المدني المصري أن: "التعبير عن الإرادة يكون باللفظ وبالكتابة وبالإشارة المتداولة عرفاً كما يكون باتخاذ موقف لا تدع ظروف الحال شكًا في دلالته على حقيقة المقصود".

[465] التهامي، سامح عبد الواحد. (2008). التعاقد عبر الإنترنت، دراسة مقارنة. دار الكتب القانونية. مصر المحلة الكبرى. ص: 80.

ويكون إعطاء الموافقة على معالجة البيانات الشخصية من خلال تصرف إيجابي واضح، يعطي دليلًا محددًا ومستنيرًا لا لبس فيه على موافقة الشخص المعني بالبيانات على معالجة بياناته الشخصية، مثل بيان مكتوب أو شفهي، بما في ذلك عن طريق الوسائل الإلكترونية، ويمكن أن يشمل ذلك وضع علامة في مربع عند زيارة موقع على شبكة الإنترنت، أو سلوك آخر يشير بوضوح إلى قبول صاحب البيانات للمعالجة المقترحة لبياناته الشخصية، لذلك لا ينبغي أن يشكل الصمت أو المربعات المحددة مسبقًا أو السكون موافقة[466]. ويجب أن تشمل الموافقة جميع أنشطة المعالجة المنفذة، ولذلك عندما يكون للمعالجة أغراض متعددة، يجب إعطاء الموافقة عليها جميعًا، وإذا كانت موافقة صاحب البيانات ستعطى بالوسائل الإلكترونية بعد طلبها، فيجب أن يكون الطلب واضحًا وموجزًا ولا يؤدي إلى تعطيل استخدام الخدمة المقدمة من أجلها دون داع[467].

ولضمان منح الموافقة بحرية، ينبغي ألّا تكون الموافقة أساسًا قانونيًا صالحًا لمعالجة البيانات الشخصية في حالة وجود خلل واضح بين صاحب البيانات والمتحكم، ولا سيما عندما يكون المتحكم سلطة عامة، ولذلك فمن المرجح أن الموافقة لم تمنح بحرية، وكذلك يُفترض أن الموافقة على عمليات معالجة البيانات الشخصية لم تمنح

---

[466] GDPR. Recital (32): " Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent…"

[467] GDPR. Recital (32): "… Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

بحرية، إذا لم تسمح بإعطاء الموافقة لعمليات معالجة متعددة، أو إذا كان أداء العقد بما في ذلك تقديم الخدمة، يعتمد على الموافقة، على الرغم من أنّ هذه الموافقة ليست ضرورية لمثل هذا الأداء[468]. ويجب أن يكون صاحب البيانات على علم بحقيقة الموافقة ومداها، لذلك يجب تقديم إعلان الموافقة بشكل واضح، باستخدام لغة واضحة، ويجب ألّا يحتوي على شروط غير عادلة، ويجب أن يكون صاحب البيانات على دراية على الأقل بهوية المتحكم وأغراض المعالجة.

وكذلك لا يتوافر الرضا إلا إذا كان صادرًا من الشخص المعنى بالبيانات ذي الأهلية، والأهلية المطلوبة هنا هي أهلية الأداء أي صلاحية الشخص لاستعمال الحق[469]. أو بمعنى آخر قدرة الشخص على أداء التصرفات القانونية لحساب نفسه، فيجب أن يصدر التعبير من شخص اكتملت مداركه ونضجت، فأصبح يقدّر الآثار المترتبة على تصرفاته[470]. وبحسب اللائحة الأوروبية تكون معالجة البيانات الشخصية للطفل مشروعة عندما يكون عمره (16) عامًا على الأقل، أما إذا كان عمر الطفل أقل من ذلك، فلن تكون هذه المعالجة قانونية إلا إذا منح المسؤول

[468] GDPR. Recital (43): "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

[469] السنهوري، عبد الرزاق أحمد. الوسيط في شرح القانون المدني. نظرية الالتزام بوجه عام. مصادر الالتزام. دار إحياء التراث العربي. بيروت: لبنان. الجزء الأول. ص: 266-268.

[470] مركز بحوث القانون والتكنولوجيا، دراسة نقدية لقانون حماية البيانات الشخصية رقم (151) لسنة 2020. مرجع سابق. ص: 52.

عن الطفل الموافقة أو التصريح بها[471]، وباستقراء نصوص قانون حماية البيانات المصري نجدها تخلو من اشتراط أن يكون الشخص المعنى بالبيانات بالغاً سن الرشد، أو من تحديد آخر يتعلق بالعمر.

ج. العدول عن الموافقة: لا تكون الموافقة ممنوحة بحرية إذا لم يكن لصاحب البيانات خيار حقيقي أو حر أو كان غير قادر على رفض أو سحب الموافقة دون ضرر[472]. ومن ثم فمن الطبيعي أن يكون للشخص الحق في العدول عن هذه الموافقة، أي سحب موافقته في أي وقت، لتعلقها بحقوقه اللصيقة بشخصيته، فقد تطرأ أمور خاصة بصاحب البيانات تستدعي عدم الاحتفاظ بالبيانات أو معالجتها، ويصدر طلب العدول من الشخص أو كل ذي صفة قانونية كالورثة أو من ينوب عنه ويترتب على هذا العدول عدم جواز الاحتفاظ بالبيانات أو معالجتها[473]. ويجوز سحب الموافقة في أي وقت، بيد أن سحب الموافقة لا يؤثر على مشروعية المعالجة التي جرت بناء على الموافقة السابقة على سحبت[474].

---

[471] GDPR. Article (8/1): "1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child."

[472] GDPR. Recital (42): "... a declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

[473] مركز بحوث القانون والتكنولوجيا، دراسة نقدية لقانون حماية البيانات الشخصية رقم (151) لسنة 2020. مرجع سابق. ص: 45.

[474] GDPR. Article (7/3): "3.The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."

د. إثبات الموافقة: عندما تعتمد المعالجة على موافقة صاحب البيانات، يجب أن يكون المتحكم قادرًا على إثبات أنّ صاحب البيانات قد أعطى موافقته على عملية المعالجة[475]، حتى يكون المتحكم بالبيانات قادرًا على الوفاء بالتزامه بإثبات صدور موافقة المعني بالبيانات الشخصية على عمليات جمع البيانات أو معالجتها[476]. وعلى الرغم من عدم اشتراط المشرع إفراغ الموافقة في شكل مكتوب، إلا أن المتحكم سيكون حريصاً على الحصول عليها في صورة مكتوبة لضمان نسبتها لصاحب البيانات وتيسيراً لإثباتها، وغالباً ما يتم إعداد نماذج محددة لإفراغ هذه الموافقة وفق الضوابط التي يتطلبها القانون[477].

2. الحالات المستثناة من الحصول على رضا الشخص المعني.

أجاز المشرع استبعاد الحصول على موافقة الشخص المعني في الأحوال المصرح بها قانوناً. ومن الحالات المستثناة من الحصول على رضا الشخص المعني:

أ. عندما تكون المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر[478]، فتكون المعالجة مشروعة عندما يكون ذلك ضروريًا لحماية مصلحة ضرورية لحياة صاحب البيانات أو حياة شخص طبيعي آخر، وفي حالة معالجة البيانات الشخصية بناءً على المصلحة الحيوية لشخص طبيعي آخر يجب أن تتم

---

[475] GDPR. Recital (42): "Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation…"

[476] GDPR. Article (7/1): "1.Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

[477] مركز بحوث القانون والتكنولوجيا، دراسة نقدية لقانون حماية البيانات الشخصية رقم (151) لسنة 2020. مرجع سابق. ص: 52.

[478] GDPR. Article (6/1/d): "(d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person."

فقط عندما لا يمكن أن تستند المعالجة على أساس قانوني آخر، وقد تخدم بعض أنواع المعالجة كلاً من الأسس المهمة للمصلحة العامة والمصالح الحيوية لموضوع البيانات، على سبيل المثال عندما تكون المعالجة ضرورية للأغراض الإنسانية، بما في ذلك مراقبة الأوبئة وانتشارها أو في حالات الطوارئ الإنسانية، ولا سيما في حالات الكوارث الطبيعية وتلك التي من صنع الإنسان[479].

ب. عندما تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفًا فيه أو لاتخاذ خطوات على طلب صاحب البيانات قبل الدخول في عقد، تكون المعالجة مشروعة عندما تكون ضرورية في سياق عقد أو نية إبرام عقد، أي إذا كانت المعالجة ضرورية لأداء عقد يكون صاحب البيانات طرفًا فيه، أو من أجل اتخاذ خطوات بناء على طلب صاحب البيانات قبل الدخول في العقد[480]، ففي هذه الحالة تكون المعالجة لازمة وضرورية تنفيذاً لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعنى بالبيانات، أو لمباشرة أي من إجراءات المطالبة بحقوقه القانونية أو الدفاع عنها[481].

---

[479] GDPR. Recital (46): "The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters."

[480] GDPR. Article (6/1/b): "(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

[481] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (2/6).

ج. عندما تكون المعالجة ضرورية للوفاء بالتزام قانوني، للمصلحة العامة أو في أثناء ممارسة السلطة الرسمية لمهامها: تكون المعالجة مشروعة عندما تكون ضرورية وفقًا لالتزام قانوني يخضع له المتحكم[482]، أو عندما تكون المعالجة ضرورية لأداء مهمة تنفذ للمصلحة العامة[483]، أو في أثناء ممارسة مهام السلطة الرسمية، ولكن ينبغي أن يكون للمعالجة أساس بنص القانون، يحدد الغرض من المعالجة ويضع مواصفات لتحديد المتحكم بالمعالجة، ونوع البيانات الشخصية التي تخضع للمعالجة، وأصحاب البيانات، والكيانات التي يتعامل معها الأفراد، وفترة التخزين، والتدابير الأخرى لضمان المعالجة القانونية والعادلة[484].

د. عندما تكون المعالجة ضرورية مراعاة لمصالح المتحكم المشروعة: أي عندما تكون المعالجة ضرورية لتمكين المتحكم بالبيانات أو الطرف الثالث ذي الصفة، ممارسة مصالحه المشروعة التي ينتهجها المتحكم أو الطرف

---

[482] GDPR. Article (6/1/c): "(c) processing is necessary for compliance with a legal obligation to which the controller is subject"

[483] GDPR. Article (6/1/e): "(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

[484] GDPR. Recital (45): "Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing…".

الثالث للقيام بالتزاماته، مع مراعاة عدم تعارض ذلك مع مصالح المعني بالبيانات أو حقوقه وحرياته الأساسية التي تتطلبها حماية البيانات الشخصية، على وجه الخصوص حيث يكون موضوع البيانات طفلًا[485].

ويمكن أن توجد هذه المصلحة المشروعة على سبيل المثال عندما تكون هناك علاقة بين صاحب البيانات والمتحكم، كأن يكون صاحب البيانات عميلاً أو موظفًا لدى المتحكم، ووجود مصلحة مشروعة قد يحتاج إلى تقويم دقيق، بما في ذلك ما إذا كان يمكن أن يتوقع صاحب البيانات جمع بياناته الشخصية ومعالجتها، ولكن يمكن أن تطغى الحقوق الأساسية لصاحب البيانات على مصلحة المتحكم بالبيانات، إذا كانت الظروف تدل أنّ صاحب البيانات لم يتوقع معالجة البيانات الشخصية، وتشكل معالجة البيانات الشخصية لأغراض منع الاحتيال أيضًا مصلحة مشروعة للمتحكم بالبيانات المعني، وأيضًا قد يُنظر إلى معالجة البيانات الشخصية لأغراض التسويق المباشر على أنها تمت لمصلحة مشروعة[486].

---

[485] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (4/6). GDPR، Article (f/1/6):
"(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[486] GDPR. Recital (47): "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing… The processing of personal data strictly necessary for the purposes

الفرع الثاني: الاستثناءات على مبادئ حماية البيانات الشخصية

إذا كان المبدأ العام، هو السماح بمعالجة البيانات الشخصية، ضمن حدود تراعي قواعد ومبادئ حمايتها، إلا أنّ لهذا المبدأ استثناء، الأول يقضي باستثناء فئات من البيانات الشخصية من الحماية، والثاني يقضي بتشديد الحماية على فئات أُخرى.

أولًا: البيانات الشخصية المستثناة من قواعد الحماية

كما أشار البحث سابقًا أن البيانات الشخصية تتعلق بالشخص الطبيعي المحدد أو الذي يمكن تحديده، أما إذا كانت هذه البيانات متعلقة بشخص طبيعي غير محدد ولا توجد أيّة إمكانية لتحديده بطريقة مباشرة أو غير مباشرة، أو إذا كان الغرض من معالجة البيانات لا تتطلب أو لم تعدّ تتطلب تحديد هوية صاحب البيانات، ولم يحتفظ المتحكم بمعلومات إضافية، أو يحصل على معلومات إضافية أو يعالجها من أجل تحديد صاحب البيانات[487]، فهذه البيانات لا تعدّ بيانات شخصية، وإن كانت تشير في السابق إلى شخص يمكن تحديده، إلا أنّ

of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

[487] GDPR. Article (11/1): "1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation".

هذا التحديد لم يعد ممكنًا، ولذلك لا تخضع لقواعد حماية البيانات مثل البيانات الإحصائية، ويعتمد تقويم البيانات أنّها مجهولة ولا تسمح بتحديد هوية الفرد على ظروف كل حالة على حده[488].

وتجمع قوانين حماية البيانات على استثناء بعض الفئات من البيانات الشخصية من الحماية المقررة وذلك بغية تحقيق أهداف ومرامي متنوعة لا بد منها، لضمان التوازن المطلوب، بين حماية حقوق الفرد وحرياته الأساسية، من جهة أولى، وحق المجتمع في التمتع بالرفاه والأمن والاستقرار وممارسة الدولة لواجباتها في هذه المجالات من جهة ثانية[489]. ويرى البعض أنّ الاجتهاد مستقر على حرمان البيانات الشخصية من الحماية في حالتين؛ الأولى عندما تطغى مصلحة أجدر بالحماية كالمصلحة العامة، فإن المصلحة العامة أولى بالحماية؛ والثانية عندما يفشي الشخص المعني بياناته الشخصية، فإن الفرد ذاته يتنازل عن حق من حقوق الشخصية الممنوح له[490]. وبالتالي فإن أهم الفئات المستثناة من الحماية:

1. معالجة البيانات الشخصية للمصلحة العامة: خرجت فئات المعلومات الشخصية، التي تجمعها الدولة وتعالجها، في إطار نشاطها المعتاد، كسلطة عامة، مسؤولة عن ضمان الأمن والسلم الوطنيين، عن نطاق هذه القوانين، وكذلك، استثني ما يجمع من بيانات ومعلومات، في إطار الحفاظ على الأمن القومي، وضرورات الدفاع الوطني[491]. كما لا تنطبق مبادئ معالجة البيانات الشخصية على المعالجة التي تقوم بها السلطات المختصة لأغراض منع

---

[488] ARTICLE 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Example No. 1. P: 21.

[489] الأشقر جبور، جبور. مرجع سابق. ص: 93.

[490] الحجار. (2017). مرجع سابق. ص: 66.

[491] الأشقر جبور. مرجع سابق. ص: 94.

الجرائم الجنائية أو التحقيق فيها أو اكتشافها أو مقاضاة مرتكبيها أو تنفيذ العقوبات الجنائية، بما في ذلك الحماية من التهديدات التي يتعرض لها الأمن العام والوقاية منها[492].

2. معالجة البيانات الشخصية من قبل شخص طبيعي في سياق نشاط شخصي أو منزلي[493]. وهي البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير ويقوم بمعالجتها للاستخدام الشخصي[494]. ومن الطبيعي، استثناء معالجة البيانات من قبل شخص طبيعي في إطار الاستعمال الشخصي أو العائلي لأهداف شخصية. أمّا السبب الذي يقدم في تسويغ هذا الأمر، فهو غياب مخاطر انكشاف البيانات الشخصية على نحو يهدد حقوق الأشخاص[495]. فالهدف من التنظيم القانوني هو حماية بيانات الأشخاص من تعرضها للانتهاك والاستغلال من جانب الغير، أمّا في هذه الحالة فمن غير المتصور أن يكون الاستخدام الشخصي محلًا للانتهاك والاستغلال.

وقد توسع المشرع المصري بشكل كبير في استبعاد طائفة كبيرة من البيانات الشخصية من نطاق الحماية الذي يضفيها القانون على البيانات دون مسوغ أو علة، على الرغم من حاجتها للحماية عليها، ومنها البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية[496]، والبيانات الشخصية لدى جهات الأمن

---

[492] GDPR. Article (2/2/d): "This Regulation does not apply to the processing of personal data: (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

[493] GDPR. Article (2/2/c): " 2.This Regulation does not apply to the processing of personal data: (c) by a natural person in the course of a purely personal or household activity."

[494] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، مادة الإصدار (1/3).

[495] الأشقر جبور، جبور. مرجع سابق. ص: 93-94.

[496] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (4/3).

القومي[497]، حيث كان من الأولى وضعها تحت مظلة الحماية وفق ضوابط تراعي خصوصيتها، وليس استبعادها على إطلاقها؛ ومن جهة أخرى، تفتح هذه المادة الباب واسعًا لاستبعاد البيانات لدى جهات الأمن القومي المتعددة، بالإضافة إلى ما تقدره هذه الجهات لاعتبارات أخرى، أي اعتبارات خلاف الأمن القومي وهي بالطبع كثيرة[498]، والبيانات الشخصية لدى البنك المركزي والجهات الخاضعة لرقابته وإشرافه[499].

ثانيًا: البيانات الشخصية المستثناة من القاعدة العامة للمعالجة

إذا كان المبدأ العام هو السماح بمعالجة البيانات الشخصية، في إطار قواعد ومبادئ الحماية، إلا أنّ لهذا المبدأ استثناء، يقضي بتقييد معالجة بعض أنواع البيانات الشخصية. ويبنى الاستثناء من جهة على حساسية هذه البيانات وبالتالي ارتفاع مستوى المخاطر والأضرار التي قد تلحق بالشخص المعني، ومن جهة أخرى على الهدف من المعالجة بقصد حرمان بعض الأشخاص من بعض الحقوق أو الخدمات أو العقود. لذلك كان لا بد من وضع قواعد أكثر تشددًا لمعالجة بعض أنواع البيانات الشخصية، كالبيانات الشخصية الحساسة، أو البيانات الشخصية المتعلقة بارتكاب الجرائم والأحكام الجزائية.

1. معالجة فئات خاصة من البيانات الشخصية: عرّف قانون حماية البيانات المصري البيانات الشخصية الحساسة بأنها: "البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعدُّ

[497] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، مادة الإصدار (5/3).
[498] مركز بحوث القانون والتكنولوجيا. (2020). ص: 25.
[499] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، مادة الإصدار (3).

بيانات الأطفال من البيانات الشخصية الحساسة"[500]. والأصل أنّه يحظر معالجة البيانات التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات السياسية أو الفلسفية أو العضوية النقابية، والبيانات البيومترية بغرض تحديد هوية الشخص الطبيعي بشكل فريد أو البيانات المتعلقة بالصحة والحياة الجنسية للشخص الطبيعي أو الميول الجنسية[501].

ومع أنّ القاعدة هي حظر معالجة هذه الفئة من البيانات الشخصية من العمليات التي حددها المشرع في القانون المصري وهي الجمع أو النقل أو التخزين أو الحفظ أو المعالج أو الإتاحة[502]، لكن استثناءً يجوز معالجة هذه الفئة من البيانات بشرط موافقة الشخص المعني على معالجة بياناته الشخصية الحساسة بصورة صريحة ومكتوبة[503]. في حين أنّ اللائحة الأوروبية نصت على أنّ الحظر يزول في عدة حالات منها؛ إذا أعطى صاحب البيانات موافقة صريحة على معالجة هذه الفئة من البيانات الشخصية[504]، أو عندما تكون المعالجة ضرورية لتنفيذ الالتزامات وممارسة الحقوق في قانون العمل أو الضمان الاجتماعي[505]، أو أنّ المعالجة ضرورية لحماية المصالح الحيوية

---

[500] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (1).

[501] GDPR. Article (9/1): " Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

[502] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (12).

[503] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (12).

[504] GDPR. Article (9/1/a): "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject".

[505] GDPR. Article (9/1/b): "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to

لصاحب البيانات أو لشخص طبيعي آخر حيث يكون صاحب البيانات غير قادر جسديًا أو قانونيًا على منح الموافقة[506]، أو إذا تعلقت المعالجة ببيانات شخصية أعلن عنها صاحب البيانات[507].

2. معالجة البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية: لا تتم معالجة البيانات الشخصية المتعلقة بالإدانات والجرائم الجنائية أو التدابير الأمنية إلا تحت إشراف السلطة الرسمية، أو عند التصريح بالمعالجة من قبل القانون مع وجود ضمانات مناسبة لحقوق وحريات أصحاب البيانات، ويجب الاحتفاظ بأي سجل شامل للإدانات الجنائية تحت سيطرة السلطة الرسمية فقط[508]، ضمن قواعد البيانات القضائية، أو الأمنية التي تديرها السلطات العامة المسؤولة عن مكافحة الجريمة ومعاقبتها ورصدها والوقاية منها[509].

إنّ مبادئ حماية البيانات، لا تكون ذات فعّالية إلا بالنص على مجموعة من الحقوق، لتمكين المعني بالبيانات من حماية حقه في بياناته الشخصية، ومن جهة أُخرى النص على مجموعة من الالتزامات على الجهات التي تقوم بمعالجة البيانات، تلزمهم باحترام حق المعني بالبيانات في حماية بياناته الشخصية، وهو ما سنبحثه فيما يأتي.

Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".

[506] GDPR. Article (9/1/c): "processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent".

[507] GDPR. Article (9/1/e): "processing relates to personal data which are manifestly made public by the data subject".

[508] GDPR. Article (10): "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

[509] الأشقر جبور. مرجع سابق. ص: 94.

المطلب الثاني: الحقوق والالتزامات في إطار حماية البيانات الشخصية

أثارت الإنترنت الجدل حول القدرة الفعلية لمستخدمي الإنترنت على التحكم في البيانات الشخصية، ويركّز هذا الجدل في العادة على وجوب تمكينهم من أن يقرروا كيفية معالجة بياناتهم الشخصية[510]، ولذلك رسّخت قوانين حماية البيانات الشخصية مجموعة من الحقوق لأصحاب البيانات، وهو ما سيُبحث تحت عنوان حقوق الشخص المعني بالبيانات بموجب الحق في البيانات الشخصية (الفرع الأول)، وبالمقابل نصت على مجموعة من الالتزامات على الجهات التي تقوم بمعالجة البيانات وهو ما سيُبحث في التزامات القائمين على معالجة البيانات الشخصية (الفرع الثاني).

الفرع الأول: حق الشخص المعني في حماية بياناته الشخصية

يُعدّ الشخص الطبيعي الذي تُعالج بياناته الشخصية والذي يُعرف بصاحب البيانات أو الشخص المعني بالبيانات، أحد الأطراف الأساسية في عملية معالجة البيانات. لذلك وضعت قوانين حماية البيانات الشخصية عددًا من الحقوق لهذا الشخص، تعبّر عن ضمانات أساسية يجب احترامها والالتزام بها في أثناء عملية معالجة البيانات. وقبل بيان حقوق هذا الشخص لا بد أولًا من التعريف به.

[510] مندل، بوديفات، أواجنر، هوتن، وتوريس. (2012). مرجع سابق. ص23.

أولًا: التعريف بالشخص المعني بالبيانات

الشخص هو محور القانون فالحقوق لا تثبت إلا للأشخاص بالمعنى القانوني. ويقصد بالشخص في لغة القانون كل من يتمتع بالشخصية القانونية، وهو أي كيان له الصلاحية لاكتساب الحقوق وتحمل التزامات، أيًا كان هذا الكيان سواء أكان إنسانًا، أو مجموعة من الأموال أو الأشخاص تهدف إلى تحقيق غرض معين[511]. وما يعنينا في هذه الفقرة التعريف بالشخص المعني بالبيانات.

عرّفت المادة (1/4) من اللائحة الأوروبية الشخص المعني بالبيانات (data subject)، في معرض تعريفها للبيانات الشخصية، بأنّه: الشخص الطبيعي الذي يمكن التعرف عليه بصورة مباشرة 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"[512]. كما عرّفه قانون حماية البيانات المصري في المادة (1) بأنه: "أي شخص طبيعي تُنسب إليه بيانات شخصية معالجة إلكترونيًا تدل عليه قانونًا أو فعلًا، وتمكن من تمييزه عن غيره". ويستفاد من هذه التعريفات أنّ نطاق الحماية للبيانات الشخصية تقتصر من حيث المبدأ على بيانات الشخص الطبيعي المحدد أو القابل للتحديد الذي تكون

[511] نجيدة، علي. (2000-2001). المدخل للعلوم القانونية. الكتاب الثاني. نظرية الحق. الطبعة الثالثة. ص: 132.

[512] GDPR. Article (4/1): ('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.

بياناته الشخصية محلًا لأي عملية من عمليات المعالجة، وهنا سنتعرض بمزيد من البحث والتفصيل لتوضيح المقصود بالشخص الطبيعي، ثم المقصود بالشخص المحدد أو القابل للتحديد.

1. المعني بالبيانات شخص طبيعي

تبيّن مما سبق أنّ الشخص المعني بالبيانات هو كل شخص طبيعي تكون بياناته الشخصية محلًا لأي عملية من عمليات المعالجة، والشخص الطبيعي هو الإنسان، فالشخصية الطبيعية لا تكون إلا للإنسان دون سواه وتظل ملازمة له لا تفارقه ما دام حياً، فكل إنسان مهما كانت حالته يعدّ في نظر القانون شخصاً طبيعياً، إلا أنّ السؤال الذي يثور على الفور هو معرفة متى تبدأ هذه الشخصية ومتى تنتهي. وما هي عناصر هذه الشخصية التي تسمى بحالة الشخصية، حيث تتميز الشخصية باسم ويتأثر مركزه بالجنسية التي يتمتع بها وبحالته السياسية والعائلية، ويكون له موطن يخاطب فيه، ويكون له أهلية تمكنه من اكتساب الحقوق وتحمل الالتزامات، ما يترتب عليها تكوّن الذمة المالية للشخص[513].

تبدأ الشخصية القانونية للإنسان بمجرد ولادته حيًا[514]؛ أي بوجوده بصورة مستقلة، وتمام انفصاله عن أمه ولو فارق الحياة بعد ذلك، بغض النظر عن أي اعتبار آخر. فالشخصية القانونية لصيقة بالشخصية الإنسانية تبدأ معها وتنتهي بنهايتها، فإذا ولد ميتاً لا تثبت له هذه الشخصية، ولا تثبت له أيضاً إذا لم يولد، لذلك لا بد معرفة تاريخ الولادة لمعرفة زمن بدء الشخصية القانونية للمولود، فيصبح صالحًا لاكتساب الحقوق، ويمكن معرفة تاريخ

[513] نجيدة. (2000–2001). مرجع سابق. ص: 133.

[514] القانون المدني السوري الصادر بالمرسوم التشريعي رقم (84) تاريخ 18 أيار 1949، المادة (31/ف1): "تبدأ شخصية الإنسان بتمام ولادته حيًا، تنتهي بموته".

بلوغه سن الرشد أو سن المساءلة الجنائية. وتثبت الولادة بالسجلات الرسمية المعدة لذلك، فإذا لم يوجد هذا الدليل أو تبين عدم صحة ما أُدرج بالسجلات جاز الإثبات بأي وسيلة من وسائل الإثبات القانونية[515]. كما تنتهي الشخصية القانونية بمفارقة الشخص الحياة[516].

ولذلك نستطيع القول، من حيث المبدأ، إن البيانات الشخصية هي معلومات تتعلق بأفراد أحياء محددين أو يمكن تحديدهم والتعرف عليهم. إلا أنّ هذا الاستنتاج يثير بعض التساؤلات حول البيانات التي تتعلق بالمتوفين أو غير المولودين بعد، والبيانات المتعلقة بأشخاص اعتبارية.

أ. المعلومات المتعلقة بالمتوفين: من حيث المبدأ لا تعدّ المعلومات المتعلقة بالمتوفين بيانات شخصية، حيث لم يعد المتوفون أشخاصًا طبيعيين، ومع ذلك قد تعدّ بيانات المتوفى بيانات شخصية في بعض الحالات. فمن ناحية أولى قد تشير المعلومات المتعلقة بالمتوفين إلى أشخاص أحياء. على سبيل المثال، تشير المعلومات التي تفيد بأنّ المرأة المتوفاة عانت من مرض وراثي ما، بأنّ ابنها يعاني أيضًا من المرض نفسه، لأنّه مرتبط بجين موجود في الكروموسوم (X). وبالتالي، عندما يمكن اعتبار المعلومات التي تمثل بيانات عن الأشخاص المتوفين مرتبطة في الوقت نفسه بالأحياء تكون بيانات شخصية، وبالتالي تتمتع البيانات الشخصية للمتوفى بشكل غير مباشر بحماية قواعد حماية البيانات. ومن ناحية ثانية، قد يكون المتحكم بالبيانات في وضع لا يسمح له بالتحقق مما إذا كان

---

[515] القانون المدني السوري الصادر بالمرسوم التشريعي رقم (84) تاريخ 18 أيار 1949، المادة (32): "1. تثبت الولادة والوفاة بسجل الأحوال المدنية. 2. فإذا لم يوجد هذا الدليل، أو تبين عدم صحة ما أدرج بالسجلات، جاز الإثبات بأية طريقة أخرى".

[516] القانون المدني السوري الصادر بالمرسوم التشريعي رقم (84) تاريخ 18 أيار 1949، المادة (31/ف1): "تبدأ شخصية الإنسان بتمام ولادته حيًا، تنتهي بموته".

الشخص الذي تتعلق به البيانات حياً أو ميتًا. وحتى إذا كان بإمكانه التأكد من ذلك، فيمكن للمتحكم بالبيانات معالجة البيانات المتعلقة بالمتوفين بموجب النظام نفسه المطبق على الأحياء دون تمييز، نظرًا لأنّه يخضع لالتزامات حماية البيانات فيما يتعلق ببيانات الأفراد الأحياء، فمن المحتمل أن يكون من الأسهل عليه عمليًا معالجة البيانات الموجودة على المتوفين بالطريقة التي تفرضها قواعد حماية البيانات، بدلاً من فصل مجموعتي البيانات. وثالثًا قد تخضع المعلومات المتعلقة بالأشخاص المتوفين لحماية خاصة تمنحها مجموعة من القواعد بخلاف تشريعات حماية البيانات، فعلى سبيل المثال لا ينتهي الالتزام بالسر الطبي بوفاة المريض، وقد يمنح التشريع الوطني المتعلق بالحق في الصورة والشرف الحماية أيضًا لذكرى المتوفين. ورابعًا، لا شيء يمنع أي دولة من توسيع نطاق التشريع الوطني لتشمل بيانات المتوفين، فمن الممكن أن يقرر بعض المشرعين الوطنيين توسيع أحكام القانون الوطني ليشمل حماية البيانات لتشمل بيانات المتوفين[517].

ب. بيانات الأجنة: إنّ المعلومات المتعلقة بالأجنة لا تعدّ بيانات شخصية، فهم ليسوا أشخاصًا طبيعيين، ومع ذلك قد تعدّ هذه البيانات بيانات شخصية في بعض الحالات؛ فمن ناحية قد تشير المعلومات المتعلقة بالأجنة إلى أشخاص أحياء، فهذه المعلومات تتعلق بالمرأة الحامل بالجنين، حيث يمكنها الكشف عن ظروفها الصحية، لذلك يجب التعامل مع البيانات الطبية والوراثية للأجنة على أنّها بيانات شخصية تتعلق بالمرأة الحامل، كما قد ترتبط المعلومات المتعلقة بالأجنّة بالزوج والزوجة على السواء، وذلك في حالة الأجنة المجمدة؛ ومن ناحية أخرى، في

[517] ARTICLE 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Example No. 1. P: 22.

حال اكتمال الحمل وولادة الطفل على قيد الحياة، سيكون التعامل مع هذه البيانات على أنّها بيانات شخصية ترتبط بشخص طبيعي وهو الطفل القاصر، وعندها يمكن اعتبار المعلومات التي تمثل بيانات الأجنة مرتبطة في الوقت نفسه بالأحياء أيضًا، وتكون بيانات شخصية وبالتالي تتمتع بالحماية القانونية[518].

ج. الأشخاص الاعتبارية: نظرًا لأنّ تعريف البيانات الشخصية يشير إلى الأشخاص الطبيعيين، فإنّ المعلومات المتعلقة بالأشخاص الاعتباريين، لا تعدّ من حيث المبدأ بيانات شخصية، ومع ذلك في بعض الحالات، قد تسري بعض قواعد حماية البيانات بصورة غير مباشرة على المعلومات المتعلقة بالأشخاص الاعتبارية. فيمكن أن تعدّ معلومات الأشخاص الاعتبارية، بأنّها متعلقة بالأشخاص الطبيعيين في الحالة التي يكون فيها اسم الشخص الاعتباري مشتقًا من اسم شخص طبيعي، أو في حالة استخدام موظف البريد الإلكتروني للشركة، أو في حالة تعلق المعلومات بشركة صغيرة قد تصف سلوك مالكها. فعندما يعطي معيار محتوى المعلومات المتعلقة بالشخص الاعتباري، أو معيار الغرض منها أو معيار الناتج عن هذه المعلومات، بأنّها تتعلق بشخص طبيعي، يجب اعتبارها بيانات شخصية، ويجب تطبيق قواعد الحماية على هذه المعلومات. بالإضافة لما سبق، عندما يقوم المتحكم بالبيانات بجمع البيانات عن الأشخاص الطبيعيين والاعتباريين بشكل غير واضح وتضمينهم في نفس مجموعات البيانات، قد يكون من الأسهل على المتحكم تطبيق قواعد حماية البيانات على جميع أنواع المعلومات الموجودة في ملفاته بدلاً من محاولة فرز المعلومات التي تشير إلى الأشخاص الطبيعيين، وتلك التي تشير إلى الأشخاص

---

[518] ARTICLE 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Example No.1. P: 23.

الاعتبارية. كما لا يوجد ما يمنع من توسيع نطاق التشريع الوطني ليشمل بيانات الأشخاص الاعتبارية، وبناءً على ذلك، قامت بعض الدول مثل إيطاليا أو النمسا أو لوكسمبورغ بتوسيع نطاق تطبيق بعض أحكام القانون الوطني لتشمل معالجة البيانات المتعلقة بالأشخاص الاعتبارية[519].

2. المعني بالبيانات محدد أو قابل للتحديد

تتعلق البيانات الشخصية بأي شخص طبيعي محدد أو قابل للتحديد، تكون بياناته الشخصية محلًا لأي عملية من عمليات المعالجة. ويكون الشخص محددًا عندما يكون مميزًا ضمن مجموعة من الأشخاص عن باقي أعضاء المجموعة. وينطوي مفهوم الشخص المحدد في أغلب الأحيان على الإشارة إلى اسم الشخص، ويكون قابلاً للتحديد عند عدم تحديد هوية الشخص بعد ولكن من الممكن تحديده، من خلال أجزاء معينة من المعلومات لها علاقة مميزة ووثيقة بفرد معين[520]. وتجري عملية التحديد بطريقة مباشرة أو غير مباشرة.

أ. تحديد المعني بالبيانات بطريقة مباشرة: في كثير من الحالات يمكن تحديد المعني بالبيانات بصورة مباشرة وبسهولة، من خلال البيانات المسجلة في ملف الموظف لدى مكتب شؤون الموظفين، والبيانات المتعلقة بنتائج الفحص الطبي للمريض الواردة في سجله الطبي لدى إحدى المراكز الطبية، وصورة شخص في مقابلة الفيديو، والمعلومات الواردة في ملف الشركة تحت اسم عميل[521]. ويعدّ اسم الشخص المعرَّف الأكثر شيوعًا في تحديد

---

[519] ARTICLE 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Example No.1. P: 24.

[520] ARTICLE 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. P: 12.

[521] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference. Example No. 1. P: 11.

المعني بالبيانات بطريقة مباشرة، ومن أجل التحقق من هذه الهوية يجب أحيانًا دمج اسم الشخص مع أجزاء أخرى من المعلومات، مثل؛ تاريخ الميلاد، أو أسماء الوالدين، أو العنوان، أو صورة الوجه، لمنع الخلط بين هذا الشخص وبين الأسماء المحتملة[522].

ب. تحديد المعني بالبيانات بطريقة غير مباشرة: كما يمكن تحديد هوية الشخص بطريقة غير مباشرة عن طريق رقم الهاتف أو رقم تسجيل السيارة أو رقم الضمان الاجتماعي أو رقم جواز السفر أو من خلال مجموعة من المعايير الأخرى التي تسمح بتحديد الشخص، من خلال تضييق نطاق المجموعة التي ينتمي إليها مثل العمر، والوظيفة، ومكان الإقامة، والسمات الخارجية للشخص كالطول، ولون الشعر، والملابس[523].

وفي حين أنّ تحديد المعني بالبيانات من خلال الاسم هو أكثر شيوعًا في الممارسة العملية، ولكن قد لا يكون الاسم في حد ذاته ضروريًا في جميع الحالات لتحديد هوية الفرد[524]. ويحدث ذلك عند استخدام معلومات أخرى لتمييز الشخص عن غيره، فالبيانات المرتبطة بالأشياء التي تخص شخص ما، أو التي تقع تحت تأثير معين

---

[522] ARTICLE 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. P: 13.

[523] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference. Example No. 1. P: 12-13

[524] Poullet,Yves, Dinant, Jean-Marc,and Terwangne, Cécile de. CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD), REPORT ON THE APPLICATION OF DATA PROTECTION PRINCIPLES TO THE WORLDWIDE TELECOMMUNICATION NETWORKS, Information self-determination in the internet era, Thoughts on Convention No. 108 for the purposes of the future work of the Consultative Committee (T-PD). Strasbourg. (13/12/2004). P: 33. Last updated: 21/4/2021. 10 a.m. Available at: https://rm.coe.int/168068416a

من قِبله، تتعلق بالشخص بصورة غير مباشرة[525]، وعادةً ما تقوم الملفات المحوسبة على شبكة الإنترنت بتعيين معرّف فريد للأشخاص، لتجنب الخلط بين شخصين في الملف ذاته، ولتسهل أدوات مراقبة حركة المرور على الشبكة، والتعرّف على سلوك الجهاز وبالتالي سلوك مستخدمه[526]. فكل جهاز كمبيوتر أو هاتف نقال أو أي جهاز آخر متصل بالإنترنت يختص بعنوان بروتوكول إنترنت (IP)، يوفر محدد هوية فريد لكل جهاز، مما يعني أنّه يمكن تتبع هذه الأجهزة وتحديد موقع أي جهاز من الأجهزة[527]. ويمكن ربط عنوان بروتوكول الإنترنت بهوية الشخص الفعلية بطرق كثيرة، فقد طورت الكثير من مواقع الإنترنت، ومزودي خدمات الإنترنت أنظمة التحقق من المستخدم، تتضمن الكشف عن الهوية، بصورة خاصة خلال التعاملات التجارية الإلكترونية، كما تتطلب الكثير من التطبيقات عنوان البريد الإلكتروني الشخصي أو أشكال أخرى من تحديد الهوية، وقد تطلب الحكومة من مستخدمي الإنترنت تسجيل عنوان بروتوكول الإنترنت الخاص بهم، ويمكن أحياناً الحصول على الهوية من خلال تحركات الشخص على الإنترنت[528].

ثانيًا: حقوق الشخص المعني بالبيانات بموجب الحق في حماية البيانات الشخصية

مع وعي إمكانات التكنولوجيا ودور الإنترنت وطبيعتها، انصب الاهتمام في قوانين حماية البيانات الشخصية على كيفية مواجهة قدرة التقنيات الحديثة على تهديد حق المعني بالبيانات في حماية بياناته الشخصية،

---

[525] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. Previous reference Example No. 1. P: 9.

[526] Poullet,Yves, Dinant, Jean-Marc,and Terwangne, Cécile de. Previous reference. P: 33.

[527] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 14.

[528] مندل، بوديفات، واجنر، هوتن، وتوريس. (2012). مرجع سابق. ص: 15.

الذي أصبح حقًا أساسيًا بموجب قوانين الاتحاد الأوروبي. ولا يمكن ضمان حماية هذا الحق من دون الاعتراف بمجموعة من الحقوق للشخص المعني بالبيانات، التي تعدّ في صميم الحق الأساسي في حماية البيانات. وفيما يأتي عرض لأهمية الاعتراف بحقوق للشخص المعني بالبيانات على بياناته الشخصية، ومن ثم عرض حقوق الشخص المعني بالبيانات على بياناته الشخصية.

1. أهمية الاعتراف بحقوق الشخص المعني بالبيانات على بياناته الشخصية

تتضح الأهمية الكبيرة لقوانين حماية البيانات، نظرًا لأنّها تسعى إلى تنظيم استخدام البيانات الشخصية بشكل مباشر، وقبل كل شيء حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية، فحماية البيانات عملية يُفترض فيها أنّ الجهات الخاصة والعامة بحاجة لأن تكون قادرة على معالجة البيانات الشخصية، لأنّه غالبًا ما تكون معالجتها ضرورية، وبالتالي فإن حماية البيانات لا تحمينا من معالجة البيانات، أي لا تتمتع بطبيعة مانعة، فأصحاب البيانات لا يمتلكون بياناتهم، وفي كثير من الحالات، لا يمكنهم منع معالجة بياناتهم، فيجوز معالجة البيانات الشخصية المتعلقة بالآخرين، ولكن بصورة قانونية ومتناسبة مع غرض المعالجة المشروعة. فحماية البيانات تنظّم عملية معالجة البيانات[529] لا تمنعها، لكنها من جهة أُخرى تعمل على حماية حق المعني بالبيانات من المعالجة غير المسوغة لبياناته الشخصية. ولتحقيق ذلك اعترفت قوانين حماية البيانات للشخص المعني بالبيانات

[529] De Hert, Gutwirth. (2009). Previous reference. P: 3.

ببعض الحقوق تمكنه من التحكم والسيطرة على بياناته الشخصية، مستندة بذلك إلى حقه في حماية بياناته الشخصية، بهدف توفير حماية فعّالة لحقوق الشخص المعنى بالبيانات كونه المقصود أساسًا من هذه الحماية.

2. حقوق الشخص المعني بالبيانات على بياناته الشخصية

رسّخت قوانين حماية البيانات الشخصية مجموعة من الحقوق للمعني بالبيانات، وهذه الحقوق هي:

أ. حق الشخص المعني بالبيانات في الاطلاع والوصول إلى بياناته: يضمن هذا الحق لصاحب البيانات الاطلاع على بياناته والوصول إليها، وبالتالي يكون لصاحب البيانات الحصول على تأكيد فيما إذا كانت البيانات الشخصية المتعلقة به في طور المعالجة أم لا، وفي حال كانت كذلك فيحق له الوصول إلى البيانات الشخصية المعالجة والحصول على معلومات حول الغرض من المعالجة، وفئات البيانات الشخصية المعنية بالمعالجة، والمستفيدين أو المستلمين الذين كشفت لهم البيانات الشخصية أو ستكشف لهم، وخاصة المستفيدون في بلدان أخرى أو منظمات دولية، والفترة التي ستُخزن خلالها البيانات الشخصية، وإذا لم يكن ذلك ممكنًا المعايير المستخدمة لتحديد تلك الفترة. كما يجب توفير معلومات عن تفاصيل الاتصال بالمتحكّم بمعالجة البيانات وعنوان البريد الإلكتروني. كما يرتبط الحق في الوصول إلى البيانات والاطلاع عليها الحق في الحصول عليها، ويقصد من ذلك حق الشخص المعني في الحصول على نسخة من بياناته بلغة واضحة، ومطابقة لما هو موجود لدى المتحكّم أو غيره من الجهات التي تقوم بمعالجة بياناته[530].

[530] GDPR. Article (15/1): " 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access

ب. حق الشخص المعني بالبيانات في تصحيح البيانات الشخصية: يتضمن هذا الحق صورًا متعددة يسمح للشخص المعني أن يطلب تصحيح بياناته الشخصية، بتعديلها أو استكمالها أو الإضافة عليها أو تحديثها، متى كانت هذه البيانات غير صحيحة أو غير كاملة أو غير مناسبة. ويكون للشخص المعني بالبيانات، أو كل ذي صفة، الحق في طلب تصحيحها إذا ما شاب البيانات أخطاء في أثناء جمعها ومعالجتها. كما يكون له طلب تعديلها سواء بالإضافة إذا كان يشوبها نقص، أو تغييرها متى كانت غير دقيقة أو غير صحيحة أو مضلله أو غامضة، أو طلب تحديثها[531]. ويكون لصاحب البيانات الحق في الحصول من المتحكّم بمعالجة بياناته على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به دون تأخير غير مسوغ، والحق في استكمال البيانات الناقصة بوسائل منها تقديم بيان إضافي[532].

---

to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".

[531] مركز بحوث القانون والتكنولوجيا. (2020). مرجع سابق. ص: 45.

[532] GDPR. Article (16): " The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement".

ج. حق الشخص المعني بالبيانات في محو بياناته الشخصية (الحق في النسيان): إنّ ما تتسم به شبكة الإنترنت؛ من القدرة على جمع وتسجل بيانات ومعلومات مستخدميها، سواء كانت تعليقات أو صورًا أو أخبارًا خاصة أو معلومات؛ وذاكرتها المطلقة التي لا يمكن محو ما تخزنه الخوادم الضخمة؛ وقابلية إتاحة هذه البيانات والمعلومات والاطلاع عليها، للجميع وعلى الدوام وإلى ما لا نهاية، وفي أي وقت أو أي مكان في العالم، جعل النسيان الطبيعي أمرًا صعب المنال إن لم يكن مستحيلًا، بالإضافة إلى ذلك فهناك إمكانية كبيرة أن تكون هذه البيانات والمعلومات قديمة أو مغلوطة أو غير صحيحة، وفي الحالين قد يسبب ذلك أضرارًا بالغة الخطورة للشخص المعني بالبيانات، لذلك نصت قوانين حماية البيانات على حق الشخص في محو بياناته الشخصية تطبيقًا لحقه في النسيان[533].

وقد حظي هذا الحق باهتمام بالغ في أوروبا، وخاصة بعد الحكم الذي أصدرته محكمة العدل الأوروبية ضد محرك البحث (Google)، حيث قضت المحكمة بحق مستخدمي الإنترنت في مطالبة محركات البحث بإزالة نتائج طلبات البحث التي تتعلق ببياناتهم الشخصية، متى كانت الروابط غير كافية أو غير ذات صلة بموضوع البحث أو مبالغ فيها، وحتى لو كان المحتوى صحيحًا ومنشورًا بشكل قانوني، مادام الشخص قد رغب في نسيانه، وقد استندت المحكمة في قرارها إلى أحكام التوجيه الأوروبي رقم 46/95 بشأن حماية معالجة البيانات الشخصية

[533] مركز بحوث القانون والتكنولوجيا. (2020). مرجع سابق. ص: 46.

ونقلها، وأيضًا الاتفاقية الأوروبية لحقوق الإنسان الصادرة عام 1950، والمادتين (7، 8) من ميثاق الاتحاد الأوروبي لعام (2000)[534].

ويسمح هذا الحق لكل فرد في ظروف معينة أن يطلب محو البيانات الشخصية المتعلقة به عند مغادرة الخدمة أو التطبيق[535]، كما يحق للمعني بالبيانات طلب محو بياناته الشخصية دون تأخير لا مسوغ له، إذا لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي جُمعت أو عولجت من أجلها؛ أو عند قيام صاحب البيانات بسحب الموافقة التي استندت إليها المعالجة، أو عند اعتراض صاحب البيانات على المعالجة بدون وجود أسباب مشروعة

[534] Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Judgment of the Court (Grand Chamber). Case C-131/12. operative part: "3. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful. 4. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question." Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

[535] إكسس ناو. (2018). مرجع سابق. ص: 6.

تسوغ المعالجة، أو إذا جرت المعالجة بطريقة غير قانونية، أو عندما يكون محو البيانات استجابة للوفاء بالتزام قانوني، أو إذا جمعت البيانات الشخصية فيما يتعلق بتقديم خدمات مجتمع المعلومات لطفل لم يتجاوز (16) عامًا[536].

د. حق الشخص المعني بالبيانات في تقييد معالجة بياناته الشخصية (تخصيص المعالجة في نطاق محدد): يسمح هذا الحق للفرد في ظروف معينة، طلب تقييد معالجة بياناته الشخصية، ويجوز للشخص طلب ذلك في عدة حالات منها؛ إذا اعترض على دقة معلوماته الشخصية لفترة من الزمن تمكّن الشخص المسؤول من التحقق من دقتها؛ أو إذا كانت المعالجة غير قانونية ورفض الشخص المعني حذف البيانات الشخصية، وطلب بدلًا من ذلك تقييد استخدام البيانات الشخصية؛ أو إذا لم يعد الشخص المتحكّم بالبيانات الشخصية بحاجة إليها لأغراض المعالجة، ولكن الشخص المعني بالبيانات يحتاج إليها لإقامة دعوى أو الدفاع عنها؛ أو إذا اعترض الشخص المعني على

[536] GDPR. Article (17/1): "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)".

المعالجة، ولم يحدد بعد فيما إذا كانت الأسباب المشروعة للمتحكّم تفوق أسباب الشخص المعني بالبيانات بالاعتراض على المعالجة[537].

هـ. حق الشخص المعني بالبيانات في نقل بياناته الشخصية: يمكّن هذا الحق الشخص المعني بالبيانات تلقي بياناته الشخصية التي قدمها إلى المتحكّم، بتنسيق منظم ومعروف وقابل للاستخدام والقراءة الآلية، وبالإضافة إلى ذلك، لديه الحق في نقل هذه البيانات إلى متحكم آخر دون عائق من قبل المتحكم الأول الذي قدمت إليه البيانات الشخصية، وذلك عندما تكون المعالجة قد تمت على أساس موافقه صاحب البيانات، أو كانت ضرورية لأداء عقد يكون صاحب البيانات طرفًا فيه، أو على أساس موافقته الصريحة لمعالجة بياناته الخاصة[538]؛ وعندما تكون المعالجة قد تمت بوسائل آلية[539]. وبممارسة هذا الحق، يكون لصاحب البيانات أيضًا الحق في التحقق من إرسال بياناته الشخصية مباشرة من شخص إلى آخر، مازال ذلك ممكنًا من الناحية التقنية[540]. ولا ينطبق الحق في نقل

---

[537] GDPR. Article (18/1): "1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject".

[538] GDPR. Article (20/a): "1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1)".

[539] GDPR. Article (20/b): "(b) the processing is carried out by automated means".

[540] GDPR. Article (20/2): "2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible".

البيانات الشخصية عندما تكون المعالجة لأغراض المصلحة العامة أو في إطار ممارسة السلطة الرسمية المفوضة للمتحكم بالمعالجة، كما لا تؤثر ممارسة المعني بالبيانات لهذا الحق بحقه في محو البيانات[541]. ولكن لا يجوز أن يؤثر استخدام الشخص المعني بالبيانات حقه في نقل بياناته الشخصية بحقوق أشخاص آخرين أو حرياتهم[542].

و. حق الشخص المعني بالبيانات في الاعتراض على معالجة البيانات الشخصية: يمكّن هذا الحق الشخص المعني بالبيانات، أن يعترض على معالجة بياناته الشخصية في أي وقت، ولو كانت المعالجة ضرورية للمصلحة العامة أو لمصلحة المتحكم بالمعالجة، أو ضمن ممارسة السلطة الرسمية، وذلك لأسباب تنشأ من الوضع الخاص للمعني بالبيانات، ما لم يثبت المتحكّم بمعالجة البيانات أسبابًا مشروعة للمعالجة تتجاوز مصالح وحقوق وحريات صاحب البيانات، أو أن المعالجة تهدف إلى إقامة دعوى أو الدفاع فيها[543]. أما في حالة معالجة البيانات الشخصية لأغراض التسويق، فيكون لصاحب البيانات الحق في الاعتراض في أي مرحلة، سواء في مرحلة جمع البيانات، أو في مرحلة لاحقة ولا يجوز بعدها معالجة بياناته الشخصية لهذه الأغراض[544].

---

[541] GDPR. Article (20/3): "3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

[542] GDPR. Article (20/4): "4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others".

[543] GDPR. Article (21/1): "1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims".

[544] GDPR. Article (21/2 & 3): "2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. 3. Where the data

وعلى الرغم من أن هذه القائمة ليست شاملة، فإن هذه الحقوق ينبغي أن ينص عليها القانون، ولا تترك لتقدير الجهات التي تعالج البيانات، وينبغي أن يكون المستخدمون قادرين على ممارسة أي من هذه الحقوق مجانًا.

الفرع الثاني: التزامات القائمين على معالجة البيانات الشخصية

كفلت قوانين حماية البيانات الشخصية عددًا من الضمانات لحماية البيانات الشخصية، ومن هذه الضمانات الالتزامات التي تقع على عاتق القائمين على عملية معالجة البيانات، وأهمهم المُتحكّمون بمعالجة البيانات والمُعالجون. ولبحث هذه الالتزامات لا بد أولًا من التعريف بالمتحكّم والمعالج (أولًا)، ومن ثم بحث التزامات المتحكّم والمعالج (ثانيًا).

أولًا: التعريف بالمتحكّم والمعالج

يعدّ مفهوما المتحكّم والمعالج من المفاهيم الوظيفية، التي تهدف إلى توزيع المسؤوليات وفقًا للأدوار الفعلية للأطراف، هذا يعني أن الوضع القانوني للمتحكّم أو المعالج يجب أن يُحدد من حيث المبدأ من خلال أنشطته الفعلية في موقف معين، وليس بناءً على تعيينه على أنه مراقب أو معالج في العقد على سبيل المثال، وتوزيع الأدوار يجب أن ينبع عادة من تحليل العناصر الواقعية أو ظروف القضية وبالتالي فهو أمر غير قابل للأخذ

---

subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes".

والرد[545]. وتؤدي مفاهيم المتحكّم والمعالج دورًا حاسمًا في تطبيق قوانين حماية البيانات، لأنّ هذه المفاهيم تحدد من سيكون مسؤولاً عن الامتثال لقواعد حماية البيانات المختلفة، لذلك يجب أن تكون هذه المفاهيم واضحة ودقيقة.

1. التعريف بالمتحكّم

عرّفت اللائحة الأوروبية المتحكّم بأنه "الشخص الطبيعي أو الاعتباري أو السلطة العامة أو المرفق أو أي هيئة أخرى تحدد، بمفردها أو بالاشتراك مع آخرين، أغراض معالجة البيانات الشخصية ووسائلها[546]. وعرّفه المشرّع المصري بأنه: "أي شخص طبيعي أو اعتباري، يكون له –بحكم أو طبيعة عمله – الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكّم فيها طبقًا للغرض المحدد أو نشاطه"[547].

تشير هذه التعاريف إلى مجموعة متنوعة وواسعة من الأشخاص، الذين يمكنهم أخذ دور المتحكّم، فقد يكون المتحكم فردًا أو مجموعة من الأفراد، أو سلطة عامة أو منظمة أو أي هيئة أخرى. وهذا يعني أنّه من حيث المبدأ، لا توجد قيود على الشخصية القانونية التي تأخذ دور المتحكّم، فقد يكون شخصًا طبيعيًا أو اعتباريًا، ولكن من الناحية العملية عادةً ما يكون المقصود بالمتحكّم المنظمة أو الهيئة أو الشركة، وليس الفرد أو الموظف أو

---

[545] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. P. 9. No. 12. Last updated: 1/4/2022. Available at: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

[546] GDPR. Article (4/7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[547] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (1).

عضو مجلس الإدارة، لذلك يجب إيلاء أهمية لموضوع ما إذا كان فرع الشركة يعمل متحكمًا أو معالجًا، عند معالجة البيانات نيابة عن الشركة الأم[548].

وفي بعض الأحيان، تقوم الشركات والهيئات العامة بتعيين شخص مسؤول عن تنفيذ أنشطة المعالجة، أو تقوم بتعيين شخص طبيعي لضمان الامتثال لقواعد حماية البيانات، فهذا الشخص لا يكون المتحكّم، ولكنّه يتصرف نيابة عن الشركة أو الهيئة العامة، التي ستكون مسؤولة في نهاية المطاف في حالة انتهاك القواعد بصفتها المتحكّم. وعلى المنوال نفسه، حتى لو كان قسم في منظمة ما لديها مسؤولية عن معالجتها للبيانات، فهذا لا يعني أنّ هذا القسم أصبح المتحكّم[549].

فالمبدأ أنّ الشخص المعنوي أو المؤسسة أو الشركة أو الإدارة الرسمية أو أية جهة أخرى، تبقى مسؤولة عن عمليات المعالجة التي تنفذها في مجال نشاطها، وتبقى مسؤولة عن احترام مبادئ حماية البيانات، ومراعاة حقوق أصحاب البيانات، وتنفيذ الالتزامات التي يفرضها القانون، حتى في الحالات التي تلجأ فيها إلى تعيين شخص طبيعي لمراقبة تنفيذ عملية المعالجة ومتابعتها[550].

ويمكن تحديد المتحكّم بمعالجة البيانات بوضوح والتمييز بينه وبين غيره من خلال عبارة "تحدد أغراض ووسائل معالجة البيانات الشخصية". فالمتحكّم هو الذي يحدد أغراض المعالجة ووسائلها. ويمكن تحديد المتحكّم

---

[548] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. Previous reference. P. 11. No. 17.

[549] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. Previous reference. P. 11. No. 18.

[550] الأشقر جبور، جبور. (2018). مرجع سابق. ص: 110.

إمّا بموجب القانون وذلك عندما يعيّن المشرّع الكيان الذي يتمتع بقدرة حقيقية على ممارسة السيطرة بصفته متحكّمًا، كأن ينص القانون على أنّ السلطات العامة هي المسؤولة عن معالجة البيانات الشخصية في سياق واجباتها. وفي بعض الحالات الأخرى يمكن تحديد المتحكّم من تحليل العناصر الواقعية أو ظروف القضية[551].

2. التعريف بالمعالج

عرّفت اللائحة الأوروبية المعالج بأنّه: "أي شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو هيئة أخرى تعالج البيانات الشخصية نيابة عن المتحكّم"[552]. وعرّفه المشرع المصري بأنّه: "أي شخص طبيعي أو اعتباري مختص، بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه، أو لصالح المتحكّم بالاتفاق معه ووفقًا لتعليماته"[553].

ونلاحظ أنّ هذه التعاريف تشير إلى مجموعة متنوعة وواسعة من الأشخاص، يمكنهم أخذ دور المعالج، فقد يكون المعالج فردًا أو مجموعة من الأفراد، أو سلطة عامة أو منظمة أو أي هيئة أخرى. وهذا يعني أنّه من حيث المبدأ، لا توجد قيود على الشخصية القانونية التي تأخذ دور المعالج، فقد يكون شخصًا طبيعيًا أو اعتباريًا.

كما نستنتج من التعاريف أنّ هناك شرطين أساسيين يجب أن يحققهما المعالج؛ الأول أن يكون كيانًا منفصلاً بالنسبة للمتحكّم، أي أن المتحكّم يقرر تفويض كل أنشطة المعالجة أو جزءًا منها إلى المعالج، كأن تكون إحدى الشركات معالجًا لشركة أخرى تعمل متحكمًا، حيث أنّ كلا الشركتين كيانان منفصلان، لذا لا يمكن أن يكون

---

[551] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. Previous reference. P. 11. No. 20, 21, 22, 23, 24.

[552] GDPR. Article (4/8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[553] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (1).

القسم داخل الشركة معالجًا لقسم آخر داخل الشركة نفسها[554]. أما إذا قرر المتحكّم معالجة البيانات بنفسه، باستخدام موارده الخاصة داخل مؤسسته، من خلال موظفيه على سبيل المثال، ففي هذه الحالة لا يعدّ معالجًا، ولا يُنظر إلى الموظفين والأشخاص الآخرين الذين يعملون تحت السلطة المباشرة للمتحكّم، على أنّهم معالجين، لأنّهم سيعالجون البيانات الشخصية على أنّها جزء من كيان المتحكّم[555].

والثاني قيامه بمعالجة البيانات الشخصية نيابة عن المتحكّم، وتتطلب معالجة البيانات الشخصية نيابة عن المتحكّم أن يعالج الكيان المنفصل البيانات الشخصية لصالح المتحكّم، وأن تتم المعالجة نيابة عن المتحكّم ولكن تحت سلطته أو سيطرته المباشرة، كما يجب ألّا يقوم المعالج بمعالجة البيانات خلافًا لتعليمات المتحكّم، أو لأغراض خاصة به[556].

ثانيًا: التزامات المتحكم والمعالج

تقابل الحقوق الممنوحة للأشخاص المعنيين بالبيانات، التي تمكنهم من ممارسة حقهم في حماية بياناتهم الشخصية، التزامًا من الجهة المسؤولة عن معالجة بياناتهم، ويؤدي المتحكم والمعالج دورًا مهمًا في نطاق معالجة

---

[554] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. Previous reference. P. 25. No. 73, 76, 77.

[555] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. Previous reference. P. 25. No. 78.

[556] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. Previous reference. P. 26. No. 80, 81.

البيانات الشخصية، لذلك يمكننا القول إنّهما الجهة المسؤولة بصورة أساسية. وقد ميزت قوانين حماية البيانات بين الالتزامات التي تقع على المُتحكم والمُعالج. وهو ما سيُعرض فيما يأتي.

1. التزامات المتحكم

أشارت اللائحة العامة إلى التزامات المتحكم في مواد عدة، في حين وضعت المادة (4) من قانون حماية البيانات المصري عددًا كبيرًا من الالتزامات على عاتق المتحكم (12 التزام)[557]. ويلتزم المتحكم عمومًا بما يأتي:

أ. التزام المتحكم بمبادئ معالجة البيانات، وإمكانية إثبات التزامه: وهو الالتزام الأساسي للمتحكّم كما جاء في المادة (24)[558] من اللائحة الأوروبية، هذا الالتزام ضروري لضمان أنّ عملية المعالجة تتناسب مع طبيعة المعالجة

[557] تنص المادة (4) من قانون حماية البيانات المصري على ما يلي: "مع مراعاة أحكام المادة 12 من هذا القانون (المعنية بالبيانات الحساسة وحظر إجراء أي عملية عليها إلا بإذن مركز حماية البيانات)، يلتزم المتحكم بما يأتي: 1. الحصول على البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونا. 2. التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها. 3. وضع طريقة وأسلوب ومعايير المعالجة طبقا للغرض المحدد، ما لم يقرر تفويض المعالج في ذلك بموجب تعاقد مكتوب. 4. التأكد من انطباق الغرض المحدد من جمع البيانات الشخصية لأغراض معالجتها. 5. القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية إلا في الأحوال المصرح بها قانونا. 6. اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظا على سريتها، وعدم اختراقها، أو إتلافها، أو تغييرها أو العبث بها قبل أي إجراء غير مشروع. 7. محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض فيجب ألا تبقي في صورة تسمح بتحديد الشخص المعني بالبيانات. 8. تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به. 9. إمساك سجل خاص للبيانات، على أن يتضمن وصف فئات البيانات الشخصية لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها، وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود، ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات. 10.الحصول على ترخيص أو تصريح من المركز للتعامل مع البيانات الشخصية. 11. يلتزم المتحكم خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية. 12. توفير الإمكانيات اللازمة لإثبات التزامه بتطبيق أحكام هذا القانون وتمكين المركز من التفتيش والرقابة للتأكد من ذلك".

[558] GDPR. Article (24/1 & 2): Responsibility of the controller. "1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary .2 Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller".

ونطاقها وأغراضها، ويقع على عاتق المتحكم مسؤولية إثبات اتخاذه كافة الإجراءات التقنية والتنظيمية والمعايير اللازمة للامتثال للقواعد المنصوص عليها في القانون، ومن ثم يكون المتحكّم هو المسؤول عن توفير الإجراءات التي تسمح لصاحب البيانات بممارسة حقوقه. كما أوردت المادة مبدأ التناسب (Proportionality)، وهو مبدأ عام في لائحة الاتحاد الأوروبي، مهم، بصورة أساسية، لضمان أنّ معالجة البيانات الشخصية متناسبة مع مستوى الحماية، ولا تؤدي إلى مخاطر على حقوق الأشخاص وحرياتهم، تفوق الغرض والمزايا المحققة من المعالجة[559]. وتمنح المادة للمتحكّم إرشادات حول كيفية إثبات قانونية أنشطة المعالجة التي يقوم بالإشراف عليها.

ويتشابه مضمون هذه المادة مع المادة (12/4) من قانون حماية البيانات المصري، حيث توضح أنّ الالتزام الأساسي للمتحكّم هو وضع طريقة المعالجة وغرضها طبقًا للقانون، ويكون هو المسؤول عن توفير الإمكانات اللازمة لذلك، ولكن بخلاف اللائحة الأوروبية لم يتطرق القانون المصري إلى مبدأ التناسب.

ب. الالتزام بمبادئ مشروعية معالجة البيانات الشخصية: وذلك بالحصول على البيانات الشخصية أو بتزويده بها من الجهات المختصة بعد موافقة الشخص المعنى بالبيانات، أو في الأحوال المصرح بها قانونًا. وقد ورد هذا الالتزام في المادة (7) من اللائحة الأوروبية، حيث نصت على أنّ المتحكّم يجب أن يكون قادرًا على إثبات موافقة صاحب البيانات على معالجة بياناته الشخصية، وذلك عندما تعتمد المعالجة على الموافقة. ويجب تقديم طلب

[559] مبدأ التناسب هو مبدأ عام للائحة الأوروبية يقيد الجهات في ممارسة سلطاتها من خال مطالبتهم بتحقيق التوازن بين الوسائل المستخدمة والهدف المقصود. وفي سياق الحق في حماية البيانات الشخصية، يبدو التناسب هو التبرير لأي قيود على أي من حقوق أصحاب البيانات. الموقع الإلكتروني لمركز حماية البيانات الأوروبي الآتي:
https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

الموافقة بطريقة يمكن تمييزها بوضوح عن الأمور الأخرى، وفي شكل واضح يسهل الوصول إليه، وباستخدام لغة واضحة ومفهومة[560].

كذلك نص القانون المصري على هذا الالتزام في المادة (1\4)، التي تضع على عاتق المتحكّم التزاماً بالحصول على البيانات الشخصية بالطرق المشروعة. وفي هذا الصدد يوجد اتفاق بين مسلك المشرعين المصري والأوروبي، في أنّ الحصول على موافقة الشخص المعنى البيانات على عملية معالجة بياناته، تقع على عاتق المتحكّم.

ج. تأمين معالجة البيانات: يوجب هذا الالتزام على المتحكّم اتخاذ جميع الإجراءات التقنية والتنظيمية المناسبة لضمان معالجة البيانات الشخصية الضرورية فقط، ولغرض محدد من المعالجة، وينطبق هذا الالتزام على كمية البيانات الشخصية التي جُمعت، ومدى معالجتها، وفترة تخزينها، وإمكانية الوصول إليها، ويجب أن تضمن هذه التدابير عدم إتاحة البيانات الشخصية لعدد غير محدد من الأشخاص الطبيعيين[561]. كذلك نص القانون المصري

---

[560] GDPR. Article (7/1 & 2): "1.Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2.If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding".

[561] GDPR. Article (25/1 & 2): Data protection by design and by default. "1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2.The controller shall implement appropriate technical and

في المادة (6\4)، على التزام المتحكّم بتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظًا على سريتها، وعدم اختراقها، أو إتلافها، أو تغييرها أو العبث بها قبل أي إجراء غير مشروع[562].

ويجب على المتحكّم عند قيام المعالج بإجراء المعالجة نيابة عنه، اختيار المعالج الذي يوفر ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة، تضمن حماية حقوق صاحب البيانات. وتتمثل هذه المعايير على سبيل المثال؛ في المعرفة المتخصصة لدى المعالج، كالخبرة الفنية فيما يتعلق بالتدابير الأمنية وخرق البيانات؛ وموثوقية المعالج؛ والتزامه بقواعد السلوك المعتمدة أو آلية الاعتماد[563]. وفي كل الأحوال يجب أن تكون عملية المعالجة عن طريق المعالج بموجب عقد أو بموجب نص القانون[564].

د. مسك سجل خاص بالبيانات: يجب على كل متحكّم الاحتفاظ بسجل لأنشطة المعالجة تحت مسؤوليته، ويجب أن يتضمن هذا السجل، كما جاء في المادة (30) من اللائحة الأوروبية، اسم المتحكّم وتفاصيل الاتصال الخاصة به، وممثل المتحكّم، ومسؤول حماية البيانات، وأغراض المعالجة، ووصف لفئات أصحاب البيانات، وفئات البيانات

---

organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".

[562] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (6/4).

[563] GDPR. Article (28/1): "1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject".

[564] GDPR. Article (28/3): "3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."

الشخصية، وفئات المتسلمين الذين كشفت لهم البيانات الشخصية، أو ستكشف لهم، بما في ذلك المتسلمين في دول ثالثة أو المنظمات الدولية، وعمليات نقل البيانات الشخصية إلى دول ثالثة أو منظمات دولية، بما في ذلك تحديد ذلك البلد الثالث أو المنظمة الدولية، والحدود الزمنية المتوخاة لمحو مختلف فئات البيانات، وصف عام للتدابير الأمنية والتقنية والتنظيمية المتخذة[565].

كما حدد قانون حماية البيانات المصري في المادة (9/4)، ما يجب أن يتضمنه هذا السجل من معلومات تحتوي على؛ وصف فئات البيانات الشخصية لديه، وتحديد لمن سيفصح عن هذه البيانات أو يتيحها لهم، وسنده في ذلك، والمدد الزمنية، وقيودها، ونطاقها، وآليات محو أو تعديل البيانات الشخصية لديه، وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود، ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات[566].

وأيضًا عند قيام المعالج بتنفيذ أنشطة المعالجة نيابة عن المتحكّم، يجب عليه الاحتفاظ بسجل لجميع فئات أنشطة المعالجة المنفذة يحتوي على؛ اسم وتفاصيل الاتصال الخاصة به وبالمتحكّم الذي يعمل المعالج نيابة عنه؛

---

[565] GDPR. Article (30/1): "1.Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a)the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)."

[566] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (9/4).

وفئات المعالجة المنفذة نيابة عن كل متحكم؛ وعمليات نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية، بما في ذلك تحديد ذلك البلد الثالث أو المنظمة الدولية[567]. ويجب أن تكون هذه السجلات مكتوبة، بما في ذلك في شكل إلكتروني، كما يجب إتاحة هذه السجلات للسلطة الرقابية المختصة بحماية البيانات[568].

هـ. الالتزام بالإخطار والإبلاغ عند حدوث انتهاك للبيانات الشخصية: يلتزم المتحكم، حال علمه بوجود انتهاك للبيانات الشخصية لديه، بإبلاغ المركز خلال اثنين وسبعين ساعة من تاريخ علمه به، ويجب وصف طبيعة خرق أو انتهاك البيانات الشخصية، وفئات أصحاب البيانات الشخصية المعنيين والعدد التقريبي لهم، وفئات البيانات الشخصية وسجلاتها، وبيانات مسؤول حماية البيانات الشخصية لديه، والآثار المحتملة لحادث الخرق أو الانتهاك؛ ووصف الإجراءات المتخذة والمقترحة من قبل المتحكّم لمواجهة هذا الخرق أو الانتهاك والتقليل من أثاره السلبية؛ وتوثيق أي انتهاك للبيانات الشخصية، والإجراءات المتخذة لمواجهته؛ وأية وثائق أو معلومات أو بيانات يطلبها المركز أو الهيئة المختصة[569].

---

[567] GDPR. Article (30/2): "2.Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)."

[568] GDPR. Article (30/3 & 4): "3.The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. 4.The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request."

[569] GDPR. Article (33/1): "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the

وفي جميع الأحوال يجب على المتحكّم إخطار المعني بالبيانات، إذا كان من المرجح أن يؤدي خرق البيانات الشخصية إلى مخاطر عالية على حقوقه وحرياته، ويجب أن يتضمن الإخطار ما اتخذه من إجراءات[570]. وعلى خلاف اللائحة الأوروبية، فقد وضع المشرع المصري هذا الالتزام على عاتق المتحكم والمعالج، بحسب الحال[571]. ويبدو من الالتزامات الملقاة على عاتق المتحكم بأنّه المسؤول الأساسي عن ضمان إجراء عملية المعالجة.

2. التزامات المعالج

أشارت اللائحة العامة إلى التزامات المعالج في مواد عدة، في حين وضعت المادة (5) من قانون حماية البيانات المصري عددًا كبيرًا من الالتزامات على عاتق المعالج (12 التزام)[572]. وبالإضافة إلى بعض الالتزامات المشتركة مع المتحكم التي أشارت إليها الفقرة السابقة، ويلتزم المعالج عمومًا بما يأتي:

---

supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

[570] GDPR. Article (34/1): "1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

[571] قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، المادة (7).

[572] تنص المادة 5 من قانون حماية البيانات المصري على ما يلي: مع مراعاة أحكام المادة 12 من هذا القانون (المعنية بالبيانات الحساسة وحظر إجراء أي عملية عليها إلا بإذن مركز حماية البيانات)، يلتزم المعالج بما يأتي: 1 – إجراء المعالجة وتنفيذها طبقًا للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقًا للحالات المشروعة والقانونية وبناءً على التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أي ذي صفة بحسب الأحوال، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها، ونوع البيانات الشخصية، واتفاقها وكفايتها مع الغرض المحدد له. 2 –أن تكون أغراض المعالجة وممارستها مشروعة ولا تخالف النظام العام أو الآداب العامة. 3 –عدم تجاوز الغرض المحدد للمعالجة ومدتها، ويجب إخطار المتحكم أو الشخص المعنى بالبيانات أو كل ذي صفة، بحسب الأحوال، بالمدة اللازمة للمعالجة. 4–محو البيانات الشخصية بانقضاء مدة المعالجة أو تسليمها للمتحكم. 5 –القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانونًا. 6 –عدم إجراء أية معالجة للبيانات الشخصية تتعارض مع غرض أو نشاط المتحكم فيها، إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخال بحرمة الحياة الخاصة. 7 –حماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك

أ. يجب على المعالج إجراء المعالجة وتنفيذها وفق الحالات المشروعة والقانونية، وبناء على التعليمات المكتوبة الواردة إليه من المتحكم أو من أي شخص ذي صفة بحسب الأحوال، بما في ذلك ما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها، ونوع البيانات الشخصية، واتفاقها وكفايتها مع الغرض المحدد له[573]، ونقل البيانات الشخصية إلى دولة ثالثة أو منظمة دولية[574]. فلا يجوز للمعالج أو أي شخص تحت سلطة المتحكّم له حق الوصول إلى البيانات الشخصية، أن يقوم بمعالجة تلك البيانات إلا بناءً على تعليمات من المتحكّم، أو بموجب نص القانون[575]. ويجب أن يوفر المعالج الإمكانات اللازمة لإثبات التزامه بتطبيق أحكام القانون عند طلب المتحكّم للتأكد من التزامه بذلك[576].

وما عليها من بيانات شخصية. 8 –عدم إلحاق أي ضرر بالشخص المعنى بالبيانات بشكل مباشر أو غير مباشر. 9 –إعداد سجل خاص بعمليات المعالجة لديه، على أن يتضمن فئات المعالجة التي يجريها نيابة عن أي متحكم وبيانات الاتصال به ومسئول حماية البيانات لديه، والمدد الزمنية للمعالجة وقيودها ونطاقها وآليات محو أو تعديل البيانات الشخصية لديه، ووصفًا للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة. 10 –توفير الإمكانيات لإثبات التزامه بتطبيق أحكام هذا القانون عند طلب المتحكم وتمكين المركز من التفتيش والرقابة للتأكد من التزامه بذلك 11 –الحصول على ترخيص أو تصريح من المركز للتعامل على البيانات الشخصية. 12 –يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية. ومن ثم يتعين على اللائحة التنفيذية تحديد قواعد وضوابط تعيين ممثل المعالج الذي يقع خارج مصر، حتى يتم التعامل معه من قبل المركز أو الشخص المعنى بالبيانات لأغراض ضمان الامتثال لهذا القانون.

[573] قانون حماية البيانات المصري، المادة (1/5).

[574] GDPR. Article (29): "The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law".

[575] GDPR. Article (28/3/a): "processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest".

[576] قانون حماية البيانات المصري، المادة (10/5).

ب. يجب على المعالج عدم الاستعانة بمعالج آخر دون إذن كتابي مسبق ومحدد من المتحكم، وفي حالة الحصول على إذن كتابي عام، يجب على المعالج إبلاغ المتحكّم بأي تغييرات مقصودة تتعلق بإضافة معالج أو استبداله، مما يمنح المتحكّم الفرصة للاعتراض على هذه التغييرات[577].

ج. يجب على المعالج القيام بعمله بطريقة مشروعة، بناء على عقد أو بموجب نص قانوني، ويحدد المتحكّم موضوع المعالجة ومدتها وطبيعة المعالجة والغرض منها، ونوع البيانات الشخصية وفئات أصحاب البيانات والتزامات وحقوق المتحكّم[578]. ويجب أن يكون هذا العقد أو التصرف القانوني في صورة مكتوبة، بما في ذلك الكتابة في الشكل الإلكتروني[579].

وفي حالة قيام المعالج بإشراك معالج ثانوي للقيام بأنشطة معالجة محددة نيابة عن المتحكّم، تفرض الالتزامات نفسها المنصوص عليها في العقد أو أي تصرف قانوني آخر بين المتحكّم والمعالج الأصلي على المعالج

---

[577] GDPR. Article (28/2): "2.The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes".

[578] GDPR. Article (28/3): "3.Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."

[579] GDPR. Article (28/9): "9.The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form."

الثانوي، وفي حالة إخلال المعالج الثانوي بالوفاء بالالتزامات، يبقى المعالج الأصلي مسؤولاً بصورة كاملة تجاه المتحكّم عن أداء التزامات المعالج الثانوي[580].

د. كما يقع على عاتق المعالج التزام بإخطار المتحكّم دون تأخير حال علمه بحدوث انتهاك البيانات الشخصية[581].

ونستنتج مما سبق أنّ المعالج ملزم قانونًا بالامتثال لتوجيهات المتحكّم، كما أنّ المتحكّم ملزم قانونًا بالتأكّد من امتثال المعالج، فهناك مسؤولية مشتركة فيما بينهما، الأمر الذي يضمن حماية أكبر للبيانات الشخصية.

[580] GDPR. Article (28/4): "Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."

[581] GDPR. Article (33/2): "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

خلاصة الفصل الثاني

هدف الفصل الثاني من البحث إلى إظهار أهمية وجود تنظيم قانوني خاص بحماية البيانات الشخصية، ولهذه الغاية عرض الفصل في المبحث الأول تطور حماية البيانات الشخصية على الصعيد الدولي، وكيف ساير التطور التشريعي المخاطر التي فرضها التطور التكنولوجي، ثم عرض المبحث الثاني التنظيم القانوني لحماية البيانات الشخصية وذلك من خلال عرض المبادئ التي يجب أن تتوافر في أي قانون يسعى إلى حماية البيانات، والحقوق والالتزامات في إطار قوانين حماية البيانات الشخصية.

الخاتمة

يتركز البحث حول حقيقة أن حماية البيانات الشخصية، لا سيما في البلدان النامية مثل سورية، تمثل تحديًا كبيرًا، فالتقدم التكنولوجي، وبصورة خاصة استخدام شبكة الإنترنت، أصبح يترسخ تدريجيًا في المجتمع، ويتغلغل في نسيج حياة الإنسان، ويزداد حضوره في جميع القطاعات، الأمر الذي أثّر تأثيرًا كبيرًا على حقوق الإنسان وحرياته الأساسية. ولذلك فإنّ توفير الحماية للبيانات الشخصية أصبح ضرورة ملحة، لما لهذه الحماية من قيمة نهائية في حماية الحق في البيانات الشخصية، وقيمة وسيطة أو ثانوية في حماية الحقوق والحريات ولاسيما الخصوصية.

وتوفير الحماية للبيانات الشخصية مرهون بإصدار تشريعات تستجيب لمتطلبات العصر الذي نعيشه، وتشكّل القوانين الخاصة بحماية البيانات الشخصية الإطار الأنسب لمواجهة مخاطر معالجة البيانات، فقوانين حماية البيانات تفعّل أكثر بكثير من مجرد تكرار الحق في الخصوصية فيما يتعلق بالبيانات الشخصية. وفي هذا الصدد، سعت قوانين حماية البيانات إلى حماية البيانات الشخصية، التي تضم جميع البيانات والمعلومات المتعلقة بالشخص الطبيعي، من خلال تنظيم عملية معالجة البيانات، التي تشمل كل عملية تجري على البيانات الشخصية، فهي تصوغ الشروط التي بموجبها تكون المعالجة مشروعة. ويستلزم ذلك ضرورة معالجة البيانات بشكل عادل ولأغراض محددة، وعلى أساس موافقة الشخص المعني أو أي أساس شرعي آخر ينص عليه القانون. كما أقرت قوانين حماية البيانات الشخصية مجموعة من الحقوق لأصحاب البيانات تمكنهم من السيطرة على بياناتهم الشخصية، وتفرض بالمقابل على القائمين على عملية المعالجة التزامات لاحترام حق أصحاب البيانات في حماية

البيانات الشخصية. ويبدو جليًا مما تقدم أنّ مسألة حماية البيانات الشخصية باتت مدرجة على سلم أولويات الدول، وبصورة خاصة بعد ازدياد حوادث تسريب البيانات والمتاجرة بها، الأمر الذي أظهر الضرورة الملحة لوجود تنظيم قانوني يحمي البيانات الشخصية.

وبعد الانتهاء من عرض موضوع الحماية القانونية للبيانات الشخصية لمستخدمي شبكة الإنترنت، توصلت الباحثة إلى النتائج والتوصيات الآتية:

النتائج

1. إنّ التغيير الحاصل في الواقع التكنولوجي وبصور خاصة شبكة الإنترنت، واستخدامها على نطاق واسع ومكثّف، سهّل انتاج البيانات الشخصية وجمعها واستخدامها، كما سهل تدفق البيانات الشخصية عبر الحدود الوطنية، مما أدى إلى تفاقم المخاطر التي تحيط بالبيانات الشخصية، فتنامى القلق من مخاطر التكنولوجيا على حقوق الأفراد وحرياتهم، وانعكس ذلك على واقع الحماية القانونية للبيانات الشخصية، فبدأ الاهتمام العالمي بحماية البيانات، ما دفع إلى صدور تشريعات دولية وإقليمية ووطنية لحماية البيانات الشخصية، تؤمن حماية تتناسب وحجم التهديدات التي تتعرض لها البيانات الشخصية.

2. هناك قصور تشريعي في القانون السوري فيما يتعلق بحماية البيانات الشخصية. فلا يوجد تشريع خاص بحماية البيانات، كما لا يوجد تعريف للبيانات أو المعلومات الشخصية أو معالجة البيانات في التشريعات السورية، ووجود بعض النصوص المتفرقة لحماية الخصوصية وحماية سرية البيانات والمعلومات لا تؤمن حماية كافية للبيانات

الشخصية، ولا تتوافق مع المخاطر التي أوجدتها شبكة الإنترنت، وتبقى تلك النصوص المتفرقة تحمي نطاق ضيق من البيانات في مجالات محددة وفي مواجهة بعض الانتهاكات. هذا الوضع يوجب على المشرع السوري تفهّم الآثار المترتبة على حقوق مستخدمي شبكة الإنترنت في سورية جراء معالجة بياناتهم الشخصية، وإيلاء قضية حماية البيانات اهتمامًا أكبر.

3. للبيانات الشخصية مكانة سامية بالنسبة للإنسان فهي تعبّر عن شخصيته وترسم صورة واضحة له على هيئة معلومات، بالإضافة إلى القيمة المالية الكبيرة للبيانات الشخصية التي أصبحت سلعة تدر أموالًا طائلة. وبالتالي فإنّ الهدف من حماية البيانات الشخصي هو تحقيق مستوى مكافئ من حماية حقوق الأشخاص الطبيعيين وحرياتهم ولا سيما حقهم في حماية بياناتهم الشخصية من جهة، وضمان التدفق الحر للبيانات الشخصية لحماية المصالح التجارية من جهة أخرى.

4. على الرغم من صعوبة الفصل بين الحق في الخصوصية وحماية البيانات، التي كانت تصنف في القرن الماضي ضمن نطاقها، إلا أنّ المشرع الأوروبي اعترف منذ مطلع هذا القرن بالحق في حماية البيانات الشخصية على أنّها حق مستقل، فحماية البيانات الشخصية وإن كانت تحمي الخصوصية بالدرجة الأولى لكنها تحمي أكثر من ذلك، وتنفرد بنطاق ومعايير وأهداف خاصة تميزها عن الخصوصية.

5. يختلف نطاق الحق في البيانات الشخصية عن نطاق الحق في الخصوصية، فهو يحمي مجموعة أوسع من البيانات، وتقع الإجراءات المتعلقة بالبيانات ضمن نطاقه، كما يختلف أيضًا نطاق الحقوق المحمية فالحق في البيانات الشخصية يحمي حقوقًا أخرى بما فيها الحق في الخصوصية.

6. لتأمين حماية فعالة للبيانات الشخصية، ولضمان سلامة عملية معالجة البيانات، لا بد من الاعتراف بمجموعة من المبادئ تحدد معايير دنيا لحماية البيانات. ولتأمين فعالية هذه المبادئ يجب الاعتراف للشخص المعني بالبيانات بمجموعة من الحقوق تمكنه من السيطرة على بياناته وتتفادى أي إساءة له.

7. كفلت قوانين حماية البيانات الشخصية عددًا من الضمانات لحماية البيانات الشخصية وحماية حقوق أصحاب البيانات، وفقا للمبادئ والأهداف المعلنة فيها، ومن هذه الضمانات الالتزامات التي تقع على كل مُعالج أو مُتحكم أو جهات أخرى تتعاقد معهما، لتنفيذ عمليات إدارة أو تحليل أو أي عملية معالجة أخرى على البيانات الشخصية.

8. الحق في حماية البيانات الشخصية من الحقوق والحريات الأساسية المتعلقة بالذات الإنسانية، لأنّ البيانات الشخصية تتعلق بالشخص وتنتمي إلى كيانه كإنسان، ولذلك لا ينبغي أن تقع معالجتها إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان. وبالنظر إلى التطور التكنولوجي الذي ضاعف من البيانات الشخصية وعمليات المعالجة التي تتعرض لها، فإن المشرع ملزم أكثر من السابق بحماية البيانات الشخصية، والطريقة المثلى لذلك هي، اعتراف المشرع بالحق في حماية البيانات الشخصية في الدستور، وسن تشريع خاص لحماية هذه البيانات، يتصدى ابتداءً لاحتمالية التعدي عليها، يضع الضمانات لمواجه التحديات التي تتعرض لها.

9. إنّ استخدام شبكة الإنترنت على مستوى عالمي أصبح خطرًا جديدًا يهدد حقوق وحريات الأفراد، فقد أتاحت شبكة الإنترنت تدفق البيانات الشخصية خارج الحدود الوطنية، وبالنتيجة ضاعفت التحديات التي تتعرض لها، لذلك فلا بد لحماية البيانات بصورة فعّالة من تظافر الجهود الدولية، والعمل على تشريع عالمي لتنظيم هذه الحماية.

المقترحات

وفي ضوء النتائج التي توصلت إليها، أقترح ما يأتي:

1. ضرورة اهتمام المشرع السوري بحماية البيانات الشخصية لما لها من أهمية كبيرة في حماية الحقوق والحريات، لذلك يجب على المشرّع السوري تحديث حماية البيانات الشخصية وتعزيزها وتوسيعها لمواجهة المستجدات التي أوجدها التطور التكنولوجي والتحديات التي رافقته، وذلك بإصدار تشريع خاص بحماية البيانات الشخصية، يحدد المفاهيم المتعلقة بهذه الحماية، وينظم مبادئ هذه الحماية، ويحدد حقوق أصحاب البيانات والتزامات القائمين على عملية المعالجة، للحيلولة دون التعدي على حقوق أصاحب البيانات، مع الأخذ في الاعتبار التنظيم الذي اتبعته اللائحة الأوروبية العامة كونها قننت تنظيمًا متكاملًا لحماية البيانات الشخصية. والاستمرار في تطوير تشريعات حماية البيانات الشخصية بما يحقق مرونتها ومواكبتها للتطورات التكنولوجية المتسارعة، وضرورة إسناد مهمة صياغة التشريع إلى خبراء في المجال القانوني والتقني.

2. ضرورة اعتراف المشرع السوري بالحق في البيانات الشخصية على أنّه حق مستقل، بالنص عليه في الدستور، بالنظر للنطاق الواسع للبيانات المحمية والإجراءات المتعلقة بها، والنطاق الواسع للحقوق المحمية. كما أنّ الاعتراف بالحق في البيانات الشخصية على أنّه حق مستقل يضيف قيمة مهمة في الاعتراف بمجموعة من الحقوق لأصحاب البيانات على بياناتهم الشخصية، ويفرض مجموعة من الالتزامات على القائمين بمعالجتها.

4. ضرورة التعاون الدولي والإقليمي لحماية البيانات وإيجاد تنظيم قانوني وحلول مشتركة قدر الإمكان، حيث أصبح تدفق البيانات خارج الحدود الوطنية يحتاج لمثل هذا التعاون.

5. تشجيع البحث القانوني المتعلق بالتطور التكنولوجي، وإنشاء قسم متخصص للدراسات العليا في كلية الحقوق يواكب المستجدات العلمية والتكنولوجية ويلبي حاجة المجتمع المحلي والإقليمي والدولي.

6. 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 البيانات الشخصية لمستخدمي شبكة الإنترنت؛ واهتمام وسائل الإعلام المرئية والمسموعة والمقروءة بتنمية الوعي والإدراك بأهمية حماية البيانات الشخصية، وذلك لتمكين أفراد المجتمع من فهم حقيقة ما يجري، من ممارسات تطال بياناتهم الشخصية وتمس حقوقهم كونهم خط الدفاع الأول.

وبعد الانتهاء من عرض البحث، أتمنى أن أكون قد عرضت البحث وناقشته على أكمل وجه، وإن لم يكن التوفيق التام حليفي، فأرجو أن يكون الجهد المبذول في إنجاز هذا البحث خطوة للمزيد من البحث والتعمق في هذا الموضوع المهم.

قائمة المراجع

1-الكتب

1. أبو العيال، أيمن، صالح، فواز. (2016-2017). **القانون المدني، مصادر الالتزام**. منشورات جامعة دمشق. كلية الحقوق. مركز التعليم المفتوح. برنامج الدراسات القانونية. ص: 465.

2. الأشقر جبور، منى، وجبور، محمود. (2018). **البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد**. أبحاث ودراسات (5). الطبعة الأولى. بيروت: لبنان. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب. ص: 171.

3. الأشقر جبور، منى. (د.ت) **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية. ص: 215.

4. أيوب، بولين أنطونيوس. (2009). **الحماية القانونية للحياة الشخصية في مجال المعلوماتية. دراسة مقارنة**. الطبعة الأولى. بيروت: لبنان. منشورات الحلبي الحقوقية. ص: 584.

5. التهامي، سامح عبد الواحد. (2008). **التعاقد عبر الإنترنت**، دراسة مقارنة. دار الكتب القانونية. مصر المحلة الكبرى. ص: 664.

6. الحجار، وسيم شفيق. (2017). **النظام القانوني لوسائل التواصل الاجتماعي (واتساب، فيسبوك، تويتر)**. دراسة قانونية مقارنة حول الخصوصية والحرية الشخصية والمسؤولية والاختصاص. أبحاث ودراسات (4). الطبعة الأولى. بيروت: لبنان. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب. ص: 147.

7. الحسناوي، علي جبار. (2009). **جرائم الحاسوب والانترنت**. الطبعة العربية. الأردن: عمان. دار اليازوري العلمية للنشر والتوزيع، ص: 192.

8. خشبة، محمد السعيد. (1991). **المعالجة الإلكترونية للمعلومات**. سلسلة الحاسبات الإلكترونية وتخطيط البرامج المطورة، الكتاب الثاني، جامعة الأزهر، مصر. المركز الدولي الإسلامي للدراسات والبحوث السكانية. ص: 143.

9. خليفة، محمد. (2007) **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن**. الإسكندرية: دار الجامعة الجديدة للنشر. ص: 251.

10. السنهوري، عبد الرزاق أحمد. **الوسيط في شرح القانون المدني**. نظرية الالتزام بوجه عام. مصادر الالتزام. دار إحياء التراث العربي. بيروت: لبنان. الجزء الأول. ص: 1330.

11. صالح، فواز. (2011–2012). **القانون المدني، مصادر الالتزام**، الجزء الأول، المصادر الإرادية. منشورات جامعة دمشق. كلية الحقوق. ص: 486.

12. عفيفي، عفيفي كامل. (2003). **جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة**. بيروت: لبنان. منشورات الحلبي الحقوقية. ص: 474.

13. فكري، أيمن عبد الله. (2007). **جرائم نظم المعلومات. دراسة مقارنة.** الإسكندرية. دار الجامعة الجديدة للنشر. ص: 841.

14. الكسواني، عامر محمود. (2008). **التجارة عبر الحاسوب، دراسة مقارنة**، الطبعة الأولى. الأردن؛ عمان، دار الثقافة للنشر والتوزيع، ص 304.

15. مغبغب، نعيم. (1998). **مخاطر المعلوماتية والإنترنت، المخاطر على الحياة الخاصة، دراسة في القانون المقارن**. ص: 304.

16. مندل، توبي، بوديفات، أندرو، واجنر، بن، هوتن، ديكسي، وتوريس، نتاليا. (2012). **دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير**. الطبعة الأولى. باريس: فرنسا. سلسة اليونسكو بشأن حرية الإنترنت. ص: 145.

17. نجيدة، علي. (2000-2001). **المدخل للعلوم القانونية**. الكتاب الثاني. نظرية الحق. الطبعة الثالثة. ص: 415.

18. ناصيف، الياس. (2009). **العقود الدولية، العقد الإلكتروني في القانون المقارن**. الطبعة الأولى. بيروت: لبنان. منشورات الحلبي الحقوقية. ص: 624.

19. واصل، محمد. (1995). **الحقوق الملازمة للشخصية**، دراسة مقارنة، دمشق، الطبعة الأولى. ص: 685.

2-القواميس.

1. قاري، عبد الغفور عبد الفتاح. (2000). **معجم مصطلحات المكتبات والمعلومات**. إنكليزي-عربي. السلسلة الثانية. الرياض. مطبوعات مكتبة الملك فهد الوطنية. ص: 349.

2. قشوع، رشدي محمد. (1997). قاموس الكمبيوتر –إنكليزي عربي. جامعة ريدينج –بريطانيا. مراجعة د. خيري الجمل. جامعة كامبرج. ص: 402.

3. عمر، أحمد مختار. (2008). معجم اللغة العربية المعاصرة، المجلد الأول، الطبعة الأولى. القاهرة. منشورات عالم الكتب، ص: 3367

3-المجلات والصحف.

1. التهامي، سامح عبد الواحد، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي. (15-16 شباط 2015). **مجلة كلية القانون الكويتية العالمية**. السنة الثالثة. العدد التاسع. المجلد الأول. ص: 395-444.

2.التهامي، سامح عبد الواحد. (آب 2018). نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها. دراسة في القانون الإماراتي. **مجلة البحوث القانونية والاقتصادية**. العدد السادس. المجلد الثامن. ص: 615-668.

3. داود، إبراهيم. (2017). الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية، دراسة تحليلية مقارنة. **مجلة الحقوق للبحوث القانونية والاقتصادية**. كلية الحقوق-جامعة الإسكندرية، العدد الأول، المجلد الثاني. ص: 315-456.

4. الفتلاوي، سلام عبد الزهرة عبد الله، وفليح، حسام جادر. (2017/3/31). مفهوم التزام المحامي بعدم إفشاء السر المهني: دراسة مقارنة. مجلة المحقق الحلي للعلوم القانونية والسياسية، مج. 9، ع. 1، ص: 157-208.

5. المعداوي، أحمد محمد. (2018). حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي. دراسة مقارنة. **مجلة جامعة الأزهر**. كلية الحقوق. جامعة بنها. المجلد 33، العدد 4، ص: 1926-2057.

6. الموسوي، منى تركي، وفضل الله، جان سيريل. (2013). الخصوصية المعلوماتية وأهميتها ومخاطر التقانات الحديثة عليها. **مجلة كلية بغداد للعلوم الاقتصادية**. العدد الخاص بمؤتمر الكلية. مركز بحوث السوق وحماية المستهلك. جامعة بغداد. ص: 303-355.

4-رسائل الماجستير والدكتوراه.

1. تقوى، أروى. (2013). **المسؤولية المدنية في مجال الاتصال الإلكتروني**، أطروحة دكتوراه، كلية الحقوق، جامعة دمشق، ص:542.

2. الشماط، كندا. (2004-2005). **الحق في الحياة الخاصة**. رسالة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة دمشق: سورية. ص: 621.

5-الدراسات.

1. أكسس ناو. (2018). **دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الأوروبي**. ص19.

2. أكسس ناو. (يناير 2021). **عرضه للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال أفريقيا**. ص 60.

3. مركز بحوث القانون والتكنولوجيا. (2020). **دراسة نقدية لقانون حماية البيانات الشخصية رقم (151) لسنة 2020**، الجامعة البريطانية في مصر، كلية الحقوق، إشراف حسن عبد الحميد. ص 138.

6-المواقع الإلكترونية.

1. أليغرين، مات. (2022/2/12). **حقائق وإحصائيات حول الإنترنت لعام 2022**. Website Rating. 2022/3/25. الرابط:

https://www.websitehostingrating.com/

2. عبد الصادق، عادل. (2019/4/14). **الثورة الصناعية الرابعة: تحديات وفرص الاستحواذ على القوة الجديدة**. المركز العربي لأبحاث الفضاء الإلكتروني. 2020/5/7. الرابط:

http://accronline.com/article_detail.aspx?id=29387

3. **كم عدد سكان العالم 2022؟ الترتيب العالمي للكثافة السكانية**. (2022/2/25). هجرة نيوز. 2022/3/25. الرابط:

https://hijra.news

4. **كتاب البيانات الشخصية: الصراع على نفط القرن الحادي والعشرين**. (2018/6/22). الموسوعة الجزائرية للدراسات والاستراتيجية. 2020/9/25. الرابط:

https://www.politics-dz.com/

5. **أمن تكنولوجيا المعلومات** (د. ت)، الرابط:

http://specto.co/files/Books_Details/Samples/IT_Security_Arabic_SampleLesson.pdf

6. **هذا هو تنظيم الاتحاد الأوروبي. أهم المؤسسات الأوروبية ومهماتها في لمحة سريعة**. (2019/11/1). موقع (Deutschland.de). 2022/11/17.

https://www.deutschland.de/ar/topic/syast/mwssat-alathad-alawrwby-wmhmatha-fy-lmht-sryt

7. **دليل تدريب عبر الإنترنت -الدعوة أمام الاتحاد الأوروبي**. (د.ت) موقع شبكة الأورو-متوسطية للحقوق. 2022/11/18.

https://euromedrights.org/ar/

7-النصوص القانونية.

1. النصوص القانونية السورية.

1. الدستور السوري الصادر بتاريخ (2012/2/27).

2. القانون المدني السوري الصادر بالمرسوم التشريعي رقم (84) بتاريخ (1949/5/18).

3. قانون العقوبات السوري الصادر بالمرسوم التشريعي رقم (148) لعام (1949).

4. قانون التوقيع الإلكتروني وخدمات الشبكة الصادر بالقانون رقم (4) بتاريخ (2009/2/25).

5. قانون السرية المصرفية السوري الصادر بالمرسوم التشريعي رقم (30) بتاريخ (2010/4/15).

6. قانون الاتصالات السوري الصادر بالقانون رقم (18) بتاريخ (1/6/ 2010).

7. اللائحة التنفيذية لقانون الاتصالات الصادرة بالمرسوم رقم (261) لعام 2010.

8. قانون الاعلام السوري الصادر بالمرسوم التشريعي رقم (108) لعام (2011).

10. قانون الأحوال المدنية السوري رقم (13) لعام (2021).

11. قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) الصادر بتاريخ (2022/3/17).

12. التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (20) لعام 2022 الصادرة بتاريخ (2022/5/22).

2. النصوص القانونية العربية.

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010)

2. دستور الجمهورية التونسية الصادر بتاريخ (2014/1/27).

3. قانون حماية البيانات الشخصية المصري رقم (151) لعام (2020).

3. النصوص القانونية الأجنبية والقرارات والتقارير المتاحة باللغة العربية.

1. اتفاقية مجلس أوروبا لحماية الأشخاص اتجاه المعالجة الآلية للبيانات الشخصية. ستراسبورغ (1981/1/28).

2. اتفاقية مجلس أوروبا لمكافحة الجريمة المعلوماتية بودابست (2001/11/23).

3. الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، روما، الصادرة بتاريخ (1950/11/4).

4. إعلان طهران الصادر بتاريخ (1968/5/13).

5. الإعلان العالمي لحقوق الإنسان الصادر بتاريخ (1948/12/10).

6. العهد الدولي الخاص بالحقوق المدنية والسياسية الصادر بتاريخ (1966/12/16).

7. تعليق اللجنة المعنية بالحقوق المدنية والسياسية رقم (16)، على المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية. الدورة الثانية والثلاثون (1988).

8. قرار الجمعية العامة رقم 167/68 بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 18 كانون الأول/ديسمبر لعام 2013.

9. قرار الجمعية العامة رقم 166/69 بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 18 كانون الأول/ديسمبر 2014.

10. قرار الجمعية العامة رقم 199/71، بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 19 كانون الأول/ديسمبر 2016.

11. قرار الجمعية العامة رقم 73/ 179، بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 17 كانون الأول/ديسمبر 2018.

12. قرار الجمعية العامة رقم 176/75، بشأن الحق في الخصوصية في العصر الرقمي المعتمد في 16 كانون الأول/ديسمبر 2020.

13. تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، السيد مارتين شاينين.

References

1-Books

1. Bygrave, Lee. A. (2014**). Data privacy law: An international perspective**. Oxford university press. First Edition. United States of America: New York. (233).

2. Bernal, Paul. (2014). **Internet privacy right, right to protect autonomy**. First Edition. Cambridge University Press. New York. (311).

3. Craig, Terence, Ludloff, Mary.E. (2011). **Privacy and big data**. Published by O'Reilly Media. United States of America. P. (79).

4. Fuster, Gloria. G. (2014). **The emergence of personal data protection as a fundamental right of the EU**. Law, Governance and Technology Series. Springer International Publishing Switzerland. Volume 16. P. 274.

5. Lessig, Lawrence. (2006). **Code version 2.0**. Published by Basic Books. United States of America: New York. (410).

6. Stefanick, Lorna. (2011). **Controlling knowledge: Freedom of information and privacy in a networked world**. AU Press, Athabasca University. Canada. (251).

7. Kuner, Christopher, Bygrave, Lee. A, Docksey, Christopher, Drechsler, Laura. (2020). **The EU General Data Protection Regulation (GDPR)**. Oxford university press. First Edition. United States of America: New York. P. (1393).

8. Lloyd, Ian. j. (2011). **Information technology law**. Sixth Edition. Oxford university press. United States: New York. (597).

9. Ozden, Melik. (June 2011). The right to non-discrimination. Part of a series of the Human Rights Programme of the Europe - Third World Centre (CETIM). Geneva Switzerland. P: 64.

2-Magazines and Newspapers

1. Bygrave, Lee. A. (1998). Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. **International Journal of Law and Information Technology**. Volume 6. (247–284).

2. Birnhack, Michael. D. (2008). The EU Data Protection Directive: An engine of a global regime. **Computer Law & Security Review.** Volume 24. P. (508-520).

3. Blackman, Josh. (2009). Omniveillance, Google, Privacy in Public, and the right to your digital identity: a tort for recording and disseminating an individual's image over the internet. **Santa Clara Law Review**. Vol 49. P: 313-329.

4. De Andrade, Norberto Nuno Gomes. (2012). Oblivion: The Right to Be Different from Oneself - Reproposing the Right to Be Forgotten. Monograph "VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet". Universitat Oberta de Catalunya. IDP. **Revista de Internet, Derecho y Política**. No. 13. p: 122-137.

5. De Hert, Paul, Papakonstantinou, Vagelis. (2013). Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency? **I/S: A Journal of Law and Policy for the Information Society**. Vol. 9:2. (271-324).

6. De Hert, Paul, Gutwirth, Serge. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Editors: Serge Gutwirth. Yves Poullet. Paul De Hert. C´ecile de Terwangne· Sjaak Nouwt. **Reinventing Data Protection?** P: 3-44. Springer.

7. Ferraris, Valeria, Bosco, Francesca, D'Angelo, Elena. (2013). **The impact of profiling on fundamental rights.** P: 1-43. Last updated: 21/4/2022. Available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366753

8. Hirsch, Dennis. D. (2011). The law and policy of online privacy: Regulation, self-regulation or co-regulation? **Seattle University Law Review**. Vol 34. (439-480).

9. Jeske, Margo, Intahchomphoo, Channarong, Landriault, Emily, Bioni, Bruno. (March 2016) The Intersection of Freedom of Information, **Privacy Legislation and Library Services in Canadian Jurisdictions**. P: 1-15. Last updated: 21/12/2021. Available at:

https://www.researchgate.net/publication/298733944_The_Intersection_of_Freedom_of_Information_Privacy_Legislation_and_Library_Services_in_Canadian_Jurisdictions

10. Koops, Bert-Jaap. (2014). The trouble with European data protection law. **International Data Privacy Law.** Vol. 4. No. 4. P: 250-261.

11. Kuner, Christopher. (2009). An international legal framework for data protection: Issues and prospects. **Computer Law & Security Review**. P: 307-317.

12. Kuner, Christopher. (2012). The European Commission's Proposed Data Protection Regulatio: A Copernican Revolution in European Data Protection Law. **Privacy & Security Law Report.** P: 1-15.

13. Lynskey, Orla. (2013). From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis. Editors: Serge Gutwirth, Ronald Lee Nes, Paul de Hert, Yves Poulet. **European Data Protection: Coming of Age**. P: 59-84.

14. Lynskey, Orla (2014). Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. **International and Comparative Law Quarterly**. Vol. (63). Issue (3). 569 – 597.

15. Rouvroy, Antoinette, Poullet, Yves. (2009). The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. Serge Gutwirth. Yves Poullet. Paul De Hert, C´ecile de Terwangne, Sjaak Nouwt, **Reinventing Data Protection?** P: 45-76.

16. Solove, Daniel. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. **Stanford Law Review**. Vol. 53. P: 1393-1426.

17. Solove, Daniel.J. (2002). Conceptualizing privacy. California law review. **California Law Review**. Vol 90. P: 1087-1156.

18. Schartum Dag. W. (2008). Designing and formulating data protection laws. **International Journal of Law and Information Technology**. Vol. 18 No. 1. P: 1-27.

19. Tzanou, Maria. (2013). Data Protection as a fundamental right next to privacy? "Reconstructing" a not so new right. **International Data Privacy Law.** Vol. 3. No. 2. P: 88-99.

3-Reports

1. Article 29 Data Protection Working Party, Opinion 4/2007 on **the concept of personal data**, 01248/07/EN, WP 136, Adopted on 20th June. last updated: 18/4/2021. 11 a.m. Available at:

https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

2. Article 29 Data Protection Working Party, Working document on **data protection issues related to RFID technology**, 10107/05/EN WP 105, January 19, 2005. last updated: 18/4/2021. 10 a.m. Available at:

https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2005/wp105_en.pdf

3. Guidelines 2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects. Adopted on 9 April 2019. Last updated: 1/4/2022. Available at:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

4. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Adopted on 07 July 2021. Last updated: 1/4/2022. Available at:

https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

5. Guidelines 10/2020 on restrictions under Article 23 GDPR. Version 1.0. Adopted on 15 December 2020. Last updated: 1/4/2022. Available at:

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf

6. Poullet,Yves, Dinant, Jean-Marc, & Terwangne, Cécile de, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD), **REPORT ON THE APPLICATION OF DATA PROTECTION PRINCIPLES TO THE WORLDWIDE TELECOMMUNICATION NETWORKS**, Information self-determination in the internet era, Thoughts on Convention No. 108 for the purposes of the future work of the Consultative Committee (T-PD). P. 59. Strasbourg. (13/12/2004). last updated: 21/3/2021. 10 a.m. Available at:

https://rm.coe.int/168068416a

7. World Economic Forum (WEF). **Personal data: The emergence of a new asset class.** (2011). P. 34. Last updated: 21/3/2021. Available At:

http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

4- Websites

1. 100 Social Media Statistics for 2019.

https://statusbrew.com/insights/social-media-statistics-2019/

2. Big Data Statistics & Facts for 2017.

https://waterfordtechnologies.com/big-data-interesting-facts/

3. Data and Goliath, The Hidden Battles to Collect Your Data and Control Your World. A Book by Bruce Schneier. Last updated: 20\5\2021. Available at:

https://www.schneier.com/books/data_and_goliath/

4. European Parliament. How the European Union works. Last updated: (1/4/2022). Available at:

https://www.europarl.europa.eu/factsheets/en/chapter/209/how-the-european-union-works

5. Kuneva, Meglena. Roundtable on Online Data Collection, Targeting and Profiling: "Personal data is the new oil of the internet and the new currency of the digital world". Last updated: 20\5\2021. Available at:

http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

6. OECD work on privacy. Last updated: 1/6/2021. Available at:

http://www.oecd.org/sti/ieconomy/privacy.htm

7. OECD. The OECD privacy framework. (2013). last updated: 1/6/2021. Available at:

http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

8. UNCTAD. Data Protection and Privacy Legislation Worldwide. Last updated: 24\4\2022. Available at:

https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

5-Court ruling.

1. Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist. Case C-101/01. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

2. Judgment of the Court (Grand Chamber) of 16 December 2008. (Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy). Case C-73/07. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0073&qid=1652172677513

3. Court of Justice. Judgment of the Court (Grand Chamber) of 29 June 2010. Case C-28/08 P. (European Commission v The Bavarian Lager Co. Ltd). Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0028

4. Judgment of the Court (Third Chamber). of 30 May 2013. Case C-342/12. (Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)). Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CA0342&qid=1652178526664

5. Judgment of the Court (Fourth Chamber) of 17 October 2013. (Michael Schwarz v Stadt Bochum). Case C-291/12. Available at:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0291

6. Judgment of the Court (Grand Chamber). Of 13 May 2014. (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González). Case C‑131/12. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

7. Judgment of the Court (Fourth Chamber). Of 11 December 2014. (František Ryneš v Úřad pro ochranu osobních údajů). Case C‑212/13. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0212

8. Judgment of the Court (Second Chamber) of 16 July 2015. (ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority). Case C-615/13 P. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli:ECLI:EU:C:2015:489

9. Judgment of the court (Grand Chamber). Of 6 October 2015. (Maximillian Schrems v Data Protection Commissioner). (‘Schrems I’). Case C‑362/14. Operative part (2): "Decision 2000/520 is invalid". Available at:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362

10. Court of Justice. Judgment of the Court (Second Chamber). of 19 October 2016. Case C-582/14. 19. 10. 2016. (Patrick Breyer v Bundesrepublik Deutschland). Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582&qid=1652172799454

11. Judgment of the court (Grand Chamber). Of 16 July 2020. (Data Protection Commissioner V Facebook Ireland Limited and Maximillian Schrems). ('Schrems II'). Case C-311/18. Available at:

https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2789(RSP)

6-Legal texts.

1. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181). Last updated: 21/3/2021. Available at:

https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181

2. Amended proposal for a COUNCIL DIRECTIVE on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (15 October 1992). Last updated: 5/6/2021. Available at:

http://aei.pitt.edu/10375/1/10375.pdf

3. Charter of fundamental rights of the European Union. (2000/C 364/01). Last updated 15/12/2021. Available at:

https://www.europarl.europa.eu/charter/pdf/text_en.pdf

4. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. (2000/520/EC). Available at:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520

5. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

6. Commission Recommendation of 29 July 1981 relating to the Council of Europe convention for the protection of individuals with regard to automatic processing of personal data (81/679/EEC). Last updated: 5/6/2021. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31981H0679

7. Convention (No. 108) for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Strasbourg, 28.I.1981). Last updated: 10/6/2021. Available at:

https://rm.coe.int/1680078b37

8. Convention on the Organization for Economic Co-operation and Development, PARIS 14th December 1960. Last updated: 9/9/2021. Available at:

https://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm

9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

10. Draft Charter of Fundamental Rights of the European Union. Last updated 15/12/2021. Available at:

https://www.europarl.europa.eu/charter/pdf/04473_en.pdf

11. European Commission. ‘A comprehensive approach on personal data protection in the European Union’ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM (2010) 609 final. 5-10. 10/9/2021. Available At:

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

12. European Commission. (25.1.2012). Brussels. COM (2012) 11 final. 2012/0011 (COD). C7-0025/12. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). P: 1. last updated 5/6/2021. Available at:

https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

13. Explanations relating to the Charter of Fundamental Rights. (2007/C 303/02). Last updated: 24/7/2021. Available at:

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF

14. Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Strasbourg, 28.I.1981). Last updated: 10/6/2021. Available at:

https://rm.coe.int/16800ca434

15. Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990. Last updated: 3\6\2021. Available at:

https://www.refworld.org/pdfid/3ddcafaac.pdf

16. Montreux Declaration, The protection of personal data and privacy in a globalized world: a universal right respecting diversities. (14- 16 September 2005). Last updated: 9/9/2021. Available at:

https://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf

17. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Last updated: 1/6/2021. Available at:

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum

18. OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (12 June 2007). Last updated: 2/6/2021. Available at:

https://www.oecd.org/digital/ieconomy/38770483.pdf

19. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data. (Submitted by the Commission on 27 July 1990). Last updated: 5/6/2021. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990PC0314(01)&from=HU

20. Proposal for a Regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). European Commission. Brussels (25.1.2012). COM (2012) 11 final. 2012/0011 (COD). C7-0025/12. Last updated: 20\6\2021. Available at:

https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

21. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Last updated: 21/3/2021. Available at:

https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223

22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at:

https://eur-lex.europa.eu/eli/reg/2016/679/oj

23. Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in Private Sector. (26 September 1973). Last updated: 10/6/2021. Available at:

https://www.legislationline.org/documents/id/6498

24. Resolution (74) 29 on the Protection of Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector. (20 September 1974). Last updated: 10/6/2021. Available at:

https://www.legislationline.org/documents/id/6499

25. The European Council conclusions and Statement of Heads of State or Government. Brussels. 24/25 October 2013. Last updated: 20\6\2021. Available at:

https://www.eu.dk/-/media/files/topmoeder/2425102013_delkonklusion.ashx

26. The Treaty on the Functioning of the European Union. Consolidated versions. (26/10/2012). Last updated 15/12/2021. Available at:

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

27. The Treaty on European Union (TEU). Consolidated versions. (26/10/2012). Last updated (13/1/2022). Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT

28. Treaty establishing the European Community. (Amsterdam consolidated version). (10/11/1997). Last updated 15/12/2021. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:11997E/TXT&rid=1

29. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. Last updated 15/12/2021. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

"Abstract"

The research discusses the legal protection of personal data of Internet users. Research on this subject is extremely important, especially after the Internet has facilitated the production and collection of personal data, and provided new capabilities for the processing and use of personal data, thus multiplying the challenges facing personal data, which made the existence of legal protection of personal data an urgent necessity. Therefore, the research addressed the challenges facing personal data on the Internet from two aspects; the first concerns the challenges posed by the nature of the Internet, and the second concerns the challenges of inadequate protection models and the absence of appropriate legislative and regulatory frameworks. Through the presentation of the foregoing, the legal rules for protecting privacy and protecting the confidentiality of information and data in Syria do not provide sufficient and adequate legal protection for the personal data of Internet users. In order to clarify the importance of having legal protection for personal data the research presented the development of legal protection for personal data in international legislation and the legal regulation of this protection.

Keywords: personal data, data processing, the Internet, the right to protect personal data.

Syrian Arab Republic
Damascus University
Faculty of Law
Department Private law

Legal Protection of Personal Data of Internet Users

A dissertation submitted in partial fulfillment of the requirements for the degree of Master in private law

By

Nelma Alashqer

Supervisor

Dr. Jamal Mathkour

Professor in the private law department

(2021-2022)