

جامعة البحرين

قسم القانون الخاص

كلية الحقوق



حماية البيانات الشخصية في ضوء التطورات التكنولوجية المعاصرة

"دراسة مقارنة في ظل أحكام النظام الأوروبي العام لحماية البيانات"

أطروحة مقدمة كجزء من متطلبات الحصول على درجة الماجستير

في القانون الخاص

إعداد

سجى خيرالله خلف

الرقم الجامعي: 20170040

إشراف

د. حنان محمد المولى

الأستاذ المساعد في القانون المدني والملكية الفكرية - جامعة البحرين

مملكة البحرين

مارس 2023



جامعة البحرين
University of Bahrain

كلية الحقوق

قسم القانون الخاص

برنامج الماجستير

نموذج رقم (2)

صفحة الاعتماد من قبل لجنة التحكيم

ناقشت الطالبة سجي خير الله خلف الحديثي ، الرقم الجامعي (20170040)، الأطروحة التي استكملت بها متطلبات الحصول على درجة الماجستير في القانون الخاص والمعنونة بـ (حماية البيانات الشخصية في ضوء التطورات التكنولوجية المعاصرة - دراسة مقارنة في ظل أحكام النظام الأوروبي العام لحماية البيانات).

وذلك في يوم الثلاثاء الموافق 28 مارس 2023.

وتوصي اللجنة بمنحها درجة الماجستير في القانون الخاص، بتقدير (B+)

(لجنة المناقشة)

الاسم	التوقيع
د. حنان محمد المولى	مشرفاً
أ.د. صالح احمد اللهيبي	ممتحناً خارجياً
د. خليل محمد مصطفى	ممتحناً داخلياً

الختم



ملخص الدراسة

تتركز دراستنا حول الحماية القانونية للبيانات الشخصية للأشخاص الطبيعيين وذلك من خلال قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018 بالمقارنه مع النظام الأوروبي العام لحماية البيانات، و نظراً للاستعمال الواسع للتكنولوجيا الحديثة وتطبيقات أنترنت الأشياء في معالجة البيانات الشخصية وسهولة الحصول على البيانات وتداولها، تزايدت أهمية وضع نظام فاعل للحماية ، وفرض إجراءات قانونية صارمة تحمي الأشخاص الطبيعيين في مجال البيانات الشخصية من الانتهاكات ، وعلى غرار المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات فقد سعى المشرع البحريني إلى اعتماد إطار قانوني وتنظيمي ملائم لحماية البيانات الشخصية يسمح بتحديد أوجه الحماية للفرد ولبياناته الشخصية بدءاً من تكريس المبادئ الأساسية لحماية البيانات الشخصية، والاجراءات الخاصة بعملية المعالجة الآلية للبيانات واحترام حقوق الأشخاص المعنيين بالمعالجة كالحق في الاعلام والحق في الولوج والحق في التصحيح والحق في الاعتراض ووفق آلية مؤسساتية تتمثل في إنشاء هيئة حماية البيانات الشخصية المنصوص عليها، ووضع جزاءات جنائية ومدنية تردع المخالفين لقواعد معالجة البيانات الشخصية ، وهو ما تعرضنا له بالتحليل والمناقشة في دراستنا لهذا الموضوع .

الإهداء

إلى أمي وأبي أطال الله في عمرهما وأمدهما بالصحة والعافية

إلى زوجي الحبيب

إلى أخوتي وكل من ساعدني لأتم هذا البحث.

شكر وتقدير

أشكر الله عز وجل على عظيم فضله وعلى النعمة التي من بها علي في إتمام هذا البحث العلمي، وأتوجه بالشكر الجزيل لكل من أسهم في تقديم يد العون لإنجاز هذا العمل ولجميع المعنيين في جامعة البحرين هذا الصرح العلمي الرائد وعلى رأسهم الدكتورة حنان المولى والشكر موصول لأساتذتي الأفاضل أعضاء هيئة التدريس في قسم القانون الخاص ولجنة التحكيم الكريمة. كما يشرفني أن أشكر زوجي وأمي وأبي، على دعواتهم وصدق مشاعرهم ودعمهم المستمر وتشجيعهم الدائم. والشكر أيضًا للزميلات والزملاء الأعزاء حيث تشاركنا مقاعد الدراسة والكثير من الأمنيات.

قائمة المحتويات

رقم الصفحة	الموضوع
أ	اعتماد لجنة المناقشة
ب	ملخص الدراسة
ج	الإهداء
د	الشكر والتقدير
هـ	قائمة المحتويات
1	مدخل إلى الدراسة
1	مقدمة
2	مشكلة البحث
3	أسئلة البحث
3	منهجية الدراسة
4	أهداف الدراسة
4	أهمية الدراسة
4	أسباب اختيار الموضوع
6	الفصل الأول البيانات الشخصية والحق في الخصوصية والتنظيم القانوني لمعالجة البيانات الشخصية
7	المبحث الأول - ماهية البيانات الشخصية والحق في الخصوصية في عالم المعلوماتية
7	المطلب الأول : مفهوم البيانات الشخصية
17	المطلب الثاني : مفهوم الحق في الخصوصية في عالم المعلوماتية
36	المبحث الثاني - التنظيم القانوني لمعالجة البيانات الشخصية في عالم المعلوماتية
37	المطلب الأول : تعريف معالجة البيانات والمبادئ المرتبطة بها

54	المطلب الثاني: شروط مشروعية معالجة البيانات الشخصية
75	الفصل الثاني ضوابط حماية البيانات الشخصية في عالم المعلوماتية
76	المبحث الأول - الحقوق والالتزامات المرتبطة بمعالجة البيانات الشخصية
76	المطلب الأول: حقوق صاحب البيانات الشخصية
99	المطلب الثاني: التزامات معالج البيانات الشخصية
120	المبحث الثاني - آليات الحماية ومعوقات التطبيق
121	المطلب الأول: آليات حماية خصوصية البيانات الشخصية
156	المطلب الثاني: معوقات تطبيق قواعد حماية البيانات الشخصية
159	الخاتمة
159	نتائج الدراسة
160	توصيات الدراسة
161	قائمة المصادر والمراجع
73	ملخص الدراسة باللغة الانجليزية

مدخل إلى الدراسة

مقدمة

يعد الحق في الحياة الخاصة من الحقوق والحريات الأساسية ، وسعت أغلب التشريعات إلى تنظيم هذا الحق وجعله حقاً دستورياً تجب حمايته من أي انتهاك ، وكان التشريع الإسلامي هو أول تلك التشريعات، فنهى عن التجسس وأخذ الأخبار وتتبع العورات والأخطاء في قوله تعالى { وَلَا تَجَسَّسُوا وَلَا يَغْتَبَ بَعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْنَاهُ وَإِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ }¹، وتم تكريس هذا الحق من خلال المواثيق والاتفاقيات الدولية التي انعكست بدورها على التشريعات الوطنية للدول .

وتبعاً لذلك يعتبر احترام الحق في الحياة الخاصة من الحقوق الملازمة للشخص الطبيعي بصفته الإنسانية، لذلك حرصت الدول الديمقراطية على حمايته من خلال تشريعاتها، ويعد هذا الحق الأساس الذي يقوم عليه الحق في حماية البيانات الشخصية وحماية الحقوق والحريات الخاصة.

وقد أدى انتشار وسائل التكنولوجيا الحديثة والاتصالات وتقنية المعلومات وزيادة اعتماد الأفراد عليها في حياتهم اليومية -كالهواتف الذكية وأجهزة أنترنت الأشياء والمساعدات الشخصية والأجهزة التي تعمل بالأوامر الصوتية- إلى تضاعف حجم البيانات الشخصية وأشكال وأغراض معالجتها، ما أدى إلى تعاظم حجم التهديدات التي تمس خصوصية الإنسان، و أصبحت البيانات أكثر عرضة للسرقة وسوء الاستخدام من أي وقت مضى ، فكان لابد أن يسعى المجتمع الدولي لتكثيف الجهود لمواجهة المخاطر والتحديات التي تفرضها الثورة التكنولوجية ، وهذه الغاية لا يسهل تحقيقها في ظل سرعة التطور الذي تشهده التقنية المعلوماتية.

وفي ضوء ما سبق شُرعت القواعد الدولية و الوطنية بهدف حماية البيانات الشخصية، وتعتبر مملكة البحرين من الدول السبّاقة التي أولت اهتماماً كبيراً بهذا الموضوع، لذا قامت بسن قانون خاص بحماية البيانات الشخصية هو القانون رقم 30 لسنة 2018 بإصدار قانون حماية البيانات الشخصية، الذي دخل حيز التنفيذ في شهر أغسطس 2019، وبموجب هذا القانون تم إنشاء هيئة عامة تسمى هيئة حماية البيانات الشخصية لتتولى عملية الإشراف والمراقبة على عملية معالجة البيانات.

¹ سورة الحجرات، الآية 12

وتجدر الإشارة إلى إن الإطار القانوني لحماية البيانات الشخصية في مملكة البحرين قد تأثر بأحكام النظام الأوروبي العام لحماية البيانات الشخصية (General Data Protection Regulation GDPR) رقم 2016/679 ، وعلى الرغم من حداثة التشريعات المعنية بالبيانات الشخصية إلا أن التطور العلمي والتكنولوجي في الفترة الأخيرة شكل تحدياً حقيقياً بالنسبة للمشرعين وأصبحت مواكبة التشريعات لهذه التطورات مسألة غاية في الصعوبة، وعلى الرغم مما تضمنته هذه التشريعات من أحكام تفصيلية توجب حماية الحق في الخصوصية من الانتهاك ، إلا أنها لا تزال عاجزة عن توفير الحماية اللازمة في ظل تجدد وتنوع التقنيات المستعملة لانتهاك هذا الحق. وعليه، سوف تخصص هذه الدراسة للبحث في نصوص قانون حماية البيانات الشخصية البحريني للوقوف على مدى نجاح المشرع في معالجة الإشكاليات القانونية المصاحبة لحماية البيانات الخاصة بالأشخاص وكيفية جمعها وتخزينها وتداولها والحق في الخصوصية في ظل التطورات التكنولوجية أمام عجز النصوص التقليدية عن حماية البيانات الشخصية وذلك بالمقارنة مع تجربة الاتحاد الأوروبي من خلال توضيح نقاط الالتقاء والاختلاف أينما وجدت.

مشكلة البحث

يشكل التطور التكنولوجي بصوره ومظاهره المختلفة خطورة فعلية على البيانات الشخصية، وفي ظل سرعة هذا التطور أصبح من الصعب السيطرة على الانتهاكات والتجاوزات وتحديد مصدرها ومرتكبها، وباتت خصوصية الفرد مهددة بصورة دائمة.

وفي ظل عدم كفاية النصوص التشريعية العامة لتوفير الحماية المطلوبة، تدخل المشرعون - ومنهم المشرع البحريني - لسن تشريعات خاصة غايتها توفير الحماية اللازمة، إلا إن سرعة عجلة التطور التكنولوجي وضعت هذه التشريعات أمام تحديات واقعية وفعلية تستدعي البحث. وعليه تتمثل مشكلة البحث فيما يلي :

- هل توفر نصوص القانون رقم 30 لسنة 2018 ضمانات فعلية لحماية البيانات الشخصية في ظل المستجدات التكنولوجية الحالية؟
- هل الوضع التشريعي الراهن كافياً لمجاراة الأحداث التكنولوجية في عالم اليوم، أم إنه يتعين على المشرع البحريني التدخل مجدداً وإعادة النظر في هذه النصوص واستحداث نصوص خاصة؟

أسئلة البحث

تهدف هذه الدراسة لتقديم إجابات لعدة تساؤلات يطرحها الموضوع محل الدراسة وهي

كالتالي:

- ماذا يقصد بالبيانات الشخصية وماهي أنواعها وما علاقتها بالحق في الخصوصية؟
- كيف وازن المشرع البحريني بين حق الوصول إلى المعلومة وحق احترام خصوصية الأفراد؟
- هل الضمانات القانونية التي نص عليها المشرع البحريني في قانون البيانات الشخصية كافية لتوفير الحماية اللازمة في ضوء ما تتعرض له خصوصية الأفراد من انتهاكات بسبب التطورات التكنولوجية؟
- ما مضمون النظام الأوروبي العام لحماية البيانات الشخصية؟ وهل عالج المشرع الأوروبي من خلال هذا النظام أو التوجيهات الأوروبية الأخرى موضوع البيانات الشخصية في تطبيقات إنترنت الأشياء؟
- كيف يمكننا الاستفادة من التجربة الأوروبية على الصعيد الوطني؟

منهجية الدراسة

لقد اعتمدت هذه الدراسة على المنهج التحليلي المقارن لتناسبه مع موضوع البحث وغاياته. فالغاية من هذه الدراسة هي البحث فيما إذا كانت النصوص التشريعية الراهنة توفر الحماية القانونية اللازمة للبيانات الشخصية في ظل التطورات التكنولوجية الحالية وظهور تطبيقات إنترنت الأشياء. وتحقيقاً لهذه الغاية، سيتم الرجوع لقانون حماية البيانات الشخصية البحريني باعتباره القانون المعني بموضوع البحث، لتحليل نصوصه وبيان مدى كفايتها لمعالجة الجوانب المتصلة بهذا الموضوع من جهة، ومقارنة موقف التشريع الوطني مع تجربة الاتحاد الأوروبي الذي نجح في التوصل إلى نظام موحد يطبق في الدول الأعضاء كافة لحماية البيانات الشخصية، ومما لا شك فيه أن نجاح التجربة الأوروبية يشكل عاملاً مشجعاً لدول مجلس التعاون لدول الخليج العربية لدراسة إمكانية توحيد قوانينها الوطنية بموجب نظام موحد على غرار النظام الأوروبي العام مع تقادي الإشكاليات وأوجه القصور التي سيتم إبرازها من خلال هذه الدراسة.

أهداف الدراسة

تهدف هذه الدراسة لبيان ما إذا كان المشرع البحريني قد وفر الحماية القانونية الكافية للبيانات الشخصية والحق في الخصوصية وذلك في ظل التطورات التكنولوجية الحالية وبروز تطبيقات إنترنت الأشياء، ومقارنة ذلك مع أحكام النظام الأوروبي العام لحماية البيانات بغية التوصل لحلول تشريعية عند الحاجة إليها.

كما تهدف هذه الدراسة لوضع خارطة طريق للمعنيين بهذا الموضوع من الجانب القانوني ولتكون بداية لدراسات تخصصية معمقة مستقبلا.

أهمية الدراسة

إن حماية البيانات الشخصية تعد من المسائل التي أثارت الكثير من الجدل في ظل التطورات التكنولوجية المعاصرة ، حيث زادت عمليات الإعتداء على البيانات الشخصية مع انتشار التكنولوجيا الحديثة وإنترنت الأشياء "Internet of Things - IoT"، وبالتالي أصبحت هناك حاجة لتوفير حماية للبيانات الشخصية للمستخدمين، فكان لابد من تناول موضوع حماية البيانات الشخصية في ظل التطورات التكنولوجية المعاصرة من وجهة نظر المشرع البحريني، فتكمن الأهمية النظرية في تناول هذا الموضوع في ندرة المراجع والأحكام القضائية التي تعالج هذا الموضوع في المكتبة القانونية العربية، وعدم وجود دراسات قانونية تتناول موضوع حماية البيانات الشخصية في ظل التطورات التكنولوجية المعاصرة من وجهة نظر المشرع البحريني. أما الأهمية العملية، فتكمن في إيجاد أفضل الطرق والوسائل لمعالجة موضوع حماية البيانات الشخصية في ظل التطور التكنولوجي، من خلال التوصيات التي يمكن تقديمها بشأن التعديلات التشريعية اللازمة لمعالجة أوجه القصور التي تعاني منها النصوص التشريعية على أرض الواقع.

أسباب اختيار الموضوع

يحظى موضوع حماية البيانات الشخصية بأهمية كبيرة بفعل التطور التكنولوجي الذي أصبح يشكل أكبر تهديد لخصوصية الأفراد، الأمر الذي يستلزم توفير ضمانات كافية لحماية البيانات الشخصية وحماية خصوصية الأفراد من الاعتداء الواقع عليها ، فتم اختيار هذا الموضوع بسبب حدائته وأهميته على الصعيد الوطني والدولي.

بالإضافة لتقييم تجربة المملكة في مجال حماية البيانات الشخصية لتقرير مدى توافقها مع التوجهات الدولية وإبراز دورها في توفير الأمن المعلوماتي والاجتماعي بما يساهم في تطوير التنمية الاقتصادية في المملكة.

وأيضاً المساهمة في نشر الوعي القانوني ببيان المخاطر الراهنة والمحتملة التي من المتصور أن تنتج عن استخدام الصور المختلفة للتطور التكنولوجي وعلى وجه التحديد تطبيقات إنترنت الأشياء.

الفصل الأول

البيانات الشخصية والحق في الخصوصية والتنظيم القانوني لمعالجة البيانات الشخصية

يعد الحق في الخصوصية وحماية البيانات الشخصية أمراً مقراً ومعتبراً به في التشريعات العربية والغربية، وقد تثار المشكلة في تحديد مفهوم البيانات الشخصية وعلاقتها بالحق في الخصوصية في عالم المعلوماتية نتيجة الخلط بين مفهوم الحياة الخاصة أو الحق في الخصوصية وبين مفهوم البيانات الشخصية. كما أن المشكلة تثار عند تحديد نطاق البيانات الشخصية ومدى الحماية المقررة لها وإطارها القانوني ، فلا توصف كل البيانات بأنها بيانات شخصية وبالتالي لا يمكن القول بوجوب إدخال كافة البيانات تحت مظلة الحماية القانونية للبيانات الشخصية ، وعليه نتناول الآتي:

المبحث الأول: ماهية البيانات الشخصية والحق في الخصوصية في عالم المعلوماتية

المبحث الثاني: التنظيم القانوني لمعالجة البيانات الشخصية في عالم المعلوماتية

المبحث الأول

ماهية البيانات الشخصية والحق في الخصوصية في عالم المعلوماتية

إن الإلمام بماهية البيانات الشخصية والحق في الخصوصية في عالم المعلوماتية لا يتم إلا من خلال التعرف على مفهوم البيانات الشخصية وتوضيح المصطلحات ذات الصلة، وعليه نقسم هذا المبحث لمطلبين، نتناول في الأول مفهوم البيانات الشخصية ونخصص الثاني لمفهوم حق الخصوصية.

المطلب الأول

مفهوم البيانات الشخصية

في ظل تطور تكنولوجيا المعلومات أصبح التعامل مع البيانات الشخصية يحظى بأهتمام كبير ، سواء على مستوى المعالجة والنشر ، أو على مستوى التدفق عبر الحدود ، بالإضافة إلى عدد الأشخاص المعنيين وحجم المعلومات الهائل الذي يتم تداوله عبر الأنترنت.

كما أصبحت عملية معالجة البيانات الشخصية تشكل خطورة على الأفراد وعلى مصالح الدول الحيوية وأمنها، بما يمس حقوق وحرقات الأفراد كالحق في الخصوصية والحق في التعبير، ولأن وضوح المفاهيم و تأطيرها من حيث مجالات تطبيقها وحدودها، أمر مهم للتطبيق السليم لأي قاعدة قانونية، يجعل من المهم التوقف هنا لتحديد مفهوم البيانات الشخصية، وذلك من خلال بيان تعريفها، ثم بيان المخاطر التي يواجهها المستخدم في عالم المعلوماتية مخصصين فرعاً لكل من هذين الموضوعين على التوالي:

الفرع الأول: تعريف البيانات الشخصية وأنواعها

حتى يتم تعريف البيانات الشخصية على وجه الدقة ، لا بد من التفرقة بين البيانات الشخصية المشمولة بالحماية القانونية و البيانات غير المشمولة بهذه الحماية. ولاشك أن وضع القوانين الوطنية تعريفات محددة للبيانات الشخصية، من شأنه أن ييسر مهمة القائمين

على أعمال جمع ومعالجة البيانات، وفي هذا الصدد، تجدر الإشارة إلى تعدد أنواع البيانات الشخصية، فهي لا تقع تحت حصر، وتختلف تبعاً للمعيار الذي ينظر إليها من خلاله².

وتبعاً لما سبق سوف نتناول تعريف البيانات الشخصية المشمولة بالحماية القانونية أولاً ، ثم نتعرض لتعريف البيانات غير الشخصية المستبعدة من نطاق الحماية القانونية ثانياً ، وأخيراً سوف نتناول أنواع البيانات الشخصية.

1- تعريف البيانات الشخصية:

تعرف البيانات الشخصية على إنها المعلومات التي تحدد هوية الفرد ، مثل الاسم والعنوان ورقم الهاتف والوظيفة وكذلك الحالة الاجتماعية ، والتي تعتبر جميعها بيانات موضوعية مجردة وتعد أيضاً من مميزات الشخصية لمن تتعلق به المعلومة ، وقد تكون المعلومات ذاتية عبارة عن آراء شخصية³.

كما عرف المشرع البحريني البيانات الشخصية في المادة الأولى من قانون حماية البيانات الشخصية رقم 30 لسنة 2018 على أنها : " أية معلومات في أية صورة تخص فرداً مُعرّفاً، أو قابلاً بطريق مباشر أو غير مباشر لأن يُعرّف، وذلك بوجه خاص من خلال رقم هويته الشخصية أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية. ولتقرير ما إذا كان الفرد قابلاً لأن يُعرّف، تراعى كافة الوسائل التي يستخدمها مدير البيانات أو أي شخص آخر، أو التي قد تكون متاحة له".

وأما المشرع الأوروبي فقد عرفها في المادة الرابعة من النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) على أنها: " ... إي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد (صاحب البيانات) ، والشخص الطبيعي القابل للتحديد هو الشخص الذي يمكن تحديد هويته بشكل مباشر أو غير مباشر ، بوجه خاص إلى الرجوع إلى محدد للهوية (معرف شخصي) (an identifier) مثل الاسم أو رقم الضمان الاجتماعي أو بيانات الموقع أو المعرف عبر الإنترنت (عنوان IP أو عنوان البريد الإلكتروني) أو لوحد أو أكثر من العناصر المميزة

² Stephen Allison, The Concept of Personal Data under the Data Protection Regime, Edinburgh Student Law Review, Volume 1, Issue 1, 2009, p.2. accessible at: [edinstudentlawreview](http://edinstudentlawreview.com) .

³ جواهر قوادري صامت، الضوابط القانونية لمعالجة البيانات الشخصية إلكترونياً، جامعة حسيبة بو علي الشلف، مجلة الدراسات القانونية، المجلد 06، العدد 02، 2020، الجزائر، ص 468.

للهوية الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي⁴.

أما بالنسبة للمشرع السعودي فقد عرف البيانات الشخصية بأنها " كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي"⁵.

ومن خلال ما تقدم نجد أن تعريف المشرع البحريني يتفق إلى حد كبير مع التعريف الذي نص عليه النظام الأوروبي العام في المادة الرابعة - المشار إليه أعلاه-، والجدير بالذكر أن المشرع البحريني عرف الفرد بصورة صريحة في ذات المادة ونص على أنه أي شخص طبيعي . وفي حال لم تكن هذه البيانات متعلقة بشخص محدد ولا توجد أية إمكانية لتحديد شكل مباشر أو غير مباشر فلا يمكن اعتبار هذه البيانات بيانات شخصية، وذلك لأن المشرع اشترط أن تكون البيانات متعلقة بشخص محدد أو يمكن تحديده لاعتبارها بيانات شخصية.

2- تعريف البيانات غير الشخصية:

يقصد بالبيانات غير الشخصية " Non-personal data " البيانات التي لا يمكن معرفة هوية الشخص من خلالها، مثل المعلومات التي تخص نوع الجنس أو نوع السيارة التي يفضلها وغيرها، كما أن بيانات الشخص الاعتباري تعتبر بيانات غير شخصية⁶.

4 Art (4) GDPR DEFINITIONS:

I. '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."

ويمكن الرجوع للتعريف ذاته لدى حسن عبد الحميد، دراسة نقدية لقانون حماية البيانات الشخصية المصري رقم (101) لسنة 2020، كلية القانون الجامعة البريطانية، (الطبعة لا يوجد)، مصر، 2020، ص32.

5 المادة الأولى من نظام حماية البيانات الشخصية السعودي الصادر بموجب مرسوم ملكي رقم (م/19) وتاريخ 1443/2/9.

⁶ حسن عبد الحميد، المرجع السابق، ص32.

وبهذا تكون البيانات غير الشخصية ليست مشمولة بالحماية القانونية، إلا أن ذلك لا يعني عدم وجود حماية توفرها لها التشريعات الحديثة إزاء عمليات المعالجة، من ذلك على سبيل المثال البيانات الحكومية المشمولة بالحماية بموجب تشريعات أخرى، وهو ما سنأتي على توضيحه لاحقاً في هذه الدراسة.

كما تجدر الإشارة هنا إلى إن المشرع البحريني في قانون البيانات الشخصية قد قصر الحماية القانونية على عمليات المعالجة الخاصة بالبيانات الشخصية دون غيرها من البيانات في إطار قانون حماية البيانات، وبالتالي فإن هذه البيانات غير الشخصية لا تكون مشمولة بالحماية القانونية تحت مظلة هذا القانون، حيث اقتصر تعريف المشرع البحريني في المادة الأولى من قانون حماية البيانات الشخصية على تعريف البيانات الشخصية واستثنى من نطاق تطبيق أحكامه البيانات غير الشخصية.

3- أنواع البيانات الشخصية

البيانات الشخصية وفقاً لهذا التقسيم تنقسم إلى نوعين هما :

أولاً: البيانات الشخصية الحساسة

تعد البيانات الشخصية الحساسة أهم أنواع البيانات الشخصية، وقد عرفها المشرع البحريني في المادة الأولى من قانون حماية البيانات الشخصية رقم (30) لسنة 2018 على أنها " أية معلومات تكشف بشكل مباشر أو غير مباشر عن أصل الفرد العرقي أو الأثني أو أرائه السياسية أو الفلسفية أو معتقداته الدينية أو انتمائه النقابي أو سجل السوابق الجنائية الخاص به أو أية بيانات تتعلق بصحته أو حالته الجنسية".

أي إن نطاق هذه الفئة أضيق من نطاق البيانات الشخصية، وأغلب القوانين ، تمنع جمعها، لأنها ترتبط بشكل مباشر بحقوق إنسانية وحريات أساسية، كما أن التشريعات لم تختلف في مفهومها⁷، فعلى سبيل المثال عرف المشرع المغربي في المادة الأولى المعطيات الحساسة على أنها " تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما في ذلك المعطيات الجينية"⁸.

⁷ عيشاوي أمال ، مستلزمات الحماية القانونية للمعطيات ذات الطابع الشخصي بعد جائحة كورونا (المعلومات الطبية نموذجاً)، جامعة البليدة 2، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58، العدد 02، الجزائر، 2021، ص737.

⁸ قانون حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي المغربي رقم 09.08 ، الصادر في 18 فبراير 2009، الجريدة الرسمية، عدد 5711.

أما بالنظر للنظام الأوروبي العام لحماية البيانات الشخصية فنجد من خلال نصوصه أنه لم يأت بتعريف عام للبيانات الحساسة، ولكنه عرف بعض البيانات الخاصة ذات الطبيعة الحساسة من ذلك البيانات الجينية ، وبيانات الشخصية، والقياسات الحيوية "البيومترية" ، والبيانات الصحية. فعرفت الفقرة (14) من المادة الرابعة من النظام الأوروبي العام بيانات القياسات الحيوية "البيومترية" Biometric Data "على أنها "تعني البيانات الشخصية الناتجة عن معالجة تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أو تؤكد التحديد الفريد لهذا الشخص الطبيعي، مثل البيانات الخاصة بالبصمة "Dactyloscopic data"9.

كما عرف أيضاً "البيانات المتعلقة بالصحة" "Data concerning health" في الفقرة (15) من ذات المادة على أنها "البيانات الشخصية المتعلقة بالصحة الجسدية أو العقلية لشخص طبيعي ، بما في ذلك توفير خدمات الرعاية الصحية ، والتي تكشف عن معلومات حول حالته الصحية"10.

وعلى الرغم أن المشرع الأوروبي قام بتوضيح المقصود بهذه البيانات إلا أنه لم يجمعها تحت مسمى البيانات الحساسة، بل جعل مسألة تحديد ما إذا كان بيان ما حساس من عدمه، هو أمر تقدره التشريعات الوطنية بدول الاتحاد11.

ومن خلال ما تقدم نلاحظ أن المشرع البحريني في قانون حماية البيانات الشخصية رقم 30 لسنة 2018 لم يعم بتحديد المقصود بكل من البيانات التي ألحق بها صفة الحساسية وتركها على عموميتها وهذا خلافاً للنظام الأوروبي العام لحماية البيانات الشخصية الذي كان أكثر توضيحاً للمصطلحات الفنية الواردة في تعريف البيانات الحساسة، فعدم التوضيح

⁹ [Art. 4 GDPR – Definitions - General Data Protection Regulation \(GDPR\) \(gdpr-info.eu\)](https://gdpr-info.eu/art-4-gdpr-definitions-general-data-protection-regulation-gdpr/) “‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”.

¹⁰ Art 4 GDPR Definition

¹⁵ “Data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.”

النظام الأوروبي العام لحماية البيانات الشخصية رقم 2016/679 - الموقع الرسمي لتشريعات الاتحاد الأوروبي: [GDPR Archives - GDPR.eu](https://gdpr.eu/)

¹¹ حسن عبد الحميد، المرجع السابق، ص34.

لهذه المصطلحات الفنية من قبل المشرع البحريني ، قد يؤدي إلى صعوبة في فهم وتفسير النص - تضيقاً أو توسيعاً- عند تطبيقه عملياً ، على اعتبار أن مجالات البيانات الحساسة متنوعة منها ما يرتبط بالحالة الصحية أو المالية وغيرها من المجالات، ومن ذلك على سبيل المثال " البيانات البيومترية" و" البيانات الجينية" هذه العبارات ليست واضحة للعامة الناس وغير مفهومة بالتالي يجب توضيحها من أهل التخصص حتى يتمكن من تحديد طبيعة الحماية الممنوحة لهذه البيانات.

ثانياً: البيانات الشخصية غير الحساسة

يمكن أن تأخذ البيانات الشخصية العديد من الصور حسب طبيعتها ويمكننا تقسيمها على النحو الآتي:

1- البيانات الاجتماعية:

البيانات من الناحية الاجتماعية هي التي تتناول الجانب المدني من حياة الأفراد ، وهي تعد من أهم المعلومات الخاصة التي يسعى الإنسان لإبعادها عن أنظار الغير، لكون هذه المعلومات حساسة جداً في حال عرفت عنه، وهي بذلك تجعل حركة الفرد مقيدة في المجتمع ، وبالأخص في حال إذا كانت هذه المعلومات مخزنة، وسهلة التداول دون ضمانات¹².

ومن أمثلة هذه البيانات الاسم وهو الذي يميز شخصاً عن غيره . ويقصد به الاسم الشخصي، أو اللقب أو اسم الأسرة. وهناك أنواع أخرى للاسم يحميها القانون إذا استعملت بصفة مستمرة وحمايتها تكون بقدر حماية الاسم المدني من ذلك اسم الشهرة والاسم المستعار والاسم التجاري. كذلك الموطن هو المكان الذي يقطنه أو يستخدمه الفرد لإدارة نشاط معين وغالباً مايتكون من رقم العقار واسم الشارع والمنطقة والمحافظة¹³. ومن ضمن هذه البيانات أيضاً السن أو تاريخ الميلاد وشهادة الميلاد، أرقام التلفون، الحالة الاجتماعية سواء كان (أعزب، متزوج، مطلق) ، أرقام بطاقات تعريف الهوية مثل بطاقات الرقم الوطني وجواز السفر ورقم التأمين الاجتماعي،

¹² سوز حميد مجيد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، دراسة تحليلية مقارنة، جامعة السليمانية، السنة السادسة، العدد 11، العراق ، 2018، ص174.

¹³ نصت المادة (12) من القانون المدني البحريني رقم (19) لسنة 2001 على " أن الموطن المختار هو الذي يتخذ لعمل قانوني معين، ويجب إثبات الموطن المختار كتابة. ويكون الموطن المختار لتنفيذ عمل قانوني معين هو الموطن بالنسبة لكل مايتعلق بهذا العمل بما في ذلك إجراءات التنفيذ الجبري، مالم يشترط غير ذلك صراحة".

الديانة، الجنس ، الانتماء السياسي لدولة معينة سواء كان الارتباط بها بالدم أو بالميلاد ، وكذلك الآراء ووجهات النظر سواء في مواضيع عامة أو شخص بعينه¹⁴.

2- البيانات الصحية:

إن حماية البيانات الصحية ، لها أهمية خاصة ، لكونها مرتبطة بخصوصية كل شخص طبيعي، لا يمكن الكشف عنها، إلا لشخص محل ثقة ، وهي ترتبط أيضاً بسلامته الجسدية، وربما النفسية، والعقلية أيضاً، ويمكنها أن تؤثر، على مستقبله المهني، وحالته العائلية، أو الاجتماعية¹⁵. لذلك حرصت جميع الأنظمة القانونية على أخضاعها للحماية القانونية الخاصة وذلك لأنها تعد من فئات البيانات الحساسة لارتباطها بالحق الإنساني الذي أقرته مختلف القوانين والمواثيق الدولية، والبيانات الصحية حظر المشرع البحريني معالجتها إلا بموافقة صريحة من صاحبها ولكنه استثنى من هذا الحظر بموجب المادة (5) من قانون حماية البيانات الشخصية " المعالجة الضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو تقديم الرعاية الصحية أو العلاج أو إدارة خدمات الرعاية الصحية من قبل مرخص له بمزاولة أي من المهن الطبية، أو أي شخص ملزم بحكم القانون بالمحافظة على السرية" . الأمر الذي يثير التساؤل حول ما إذا كان نطاق هذا الاستثناء يتسع ليشمل معالجة البيانات الصحية التي يتم الحصول عليها والمتعلقة بالجائحة العالمية فيروس كورونا (COVID-19).

والأصل إن البيانات الصحية محمية وفقاً للقانون لا يمكن معالجتها دون موافقة مسبقة. إلا إنه ولغايات حماية الصحة العامة خرج المشرع عن الأصل وأجاز معالجة هذه البيانات لتمكين المختصين من البحث عن اللقاحات وتقديم الرعاية الطبية لمن يحتاجها مع مراعاة مصالح الأفراد بطبيعة الحال وعدم انتهاكها. و مع انتشار فيروس كورونا (COVID-19)، قامت العديد من الدول بجمع وتوزيع المعلومات والبيانات الإحصائية والبيانات الخاصة التي يتم تبليغها من المرافق الصحية والمؤسسات الإستشفائية إلى الجهات المخولة قانوناً بمتابعة ومكافحة الفيروس للتمكن من اتخاذ الإجراءات الوقائية وتتبع المصابين أو الذين يشتبه بكونهم حاملين للفيروس من خلال مخالطتهم لأشخاص مصابين. كما قامت العديد من الدول المتقدمة في مجال المعلوماتية باتخاذ تدابير عاجلة ، فقامت بعمل تطبيقات تكنولوجية تحمل على الهاتف النقال يمكن من خلالها تحديد موقع الأشخاص المصابين، وعلى إثر ذلك يتم تعقب الحالات وتنبيه باقي المواطنين بمواقع

¹⁴ مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، القاهرة، 2016، ص83-84.

¹⁵ منى أبو أشقر جبور و محمود جبور، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد، الطبعة الأولى ، لبنان، 2018، ص106.

المرضى و بؤر الوباء، وكما يسمح للجهة المعنية اتخاذ الإجراءات القانونية المتعلقة بالحجر والحد من الحركة والتباعد وغيرها من التدابير الوقائية في كل منطقة 16 .

الفرع الثاني: المخاطر التي يواجهها المستخدم في عالم المعلوماتية

مع ظهور المعلوماتية واعتماد الهيئات العامة والخاصة على الأجهزة الإلكترونية في أداء جميع الأنشطة وتقديم الخدمات ، إلى جانب شيوع استخدام تكنولوجيا المعلومات في مختلف المجالات الإدارية والمالية والصحية، تضاعف حجم المعطيات الشخصية وأشكال وأغراض معالجتها، وبالتالي تعاظمت المخاطر التي تهدد الحياة الخاصة للأفراد من خلال معالجة معطياتهم الشخصية، حيث تمكن تقنية المعلومات الجديدة من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي تم تجميعها من قبل المؤسسات والدوائر الحكومية والشركات الخاصة، كما يمكن معها أيضاً مقارنة البيانات المخزنة في ملف معالج آلياً بمعلومات في قاعدة بيانات أخرى، و يمكن نقلها عبر البلدان في ثوان وبتكاليف منخفضة، وهذا يكشف بوضوح حجم التهديدات والمخاطر على الحق في الخصوصية الذي يمكن توضيحه على النحو الآتي:

أولاً: البيانات التي تجمعها المؤسسات الخاصة والحكومية

اهتمت الشركات التجارية والمؤسسات الخاصة والحكومية في الآونة الأخيرة بتجميع بيانات عديدة ومنفصلة تتعلق بالوضع المادي والصحي والتعليمي والعائلي والاجتماعي والوظيفي للأفراد ، كما يتم استخدام البيانات في تخزين المعلومات وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، الأمر الذي سهل الوصول إلى البيانات على نحو غير مأذون به ويسر إمكانية استخدامها أو توجيهها توجيهاً منحرفاً أو خاطئاً، بقصد مراقبة الأفراد وانتهاك خصوصيتهم¹⁷، ناهيك عما تتميز به بنوك المعلومات من خاصية عدم النسيان وعدم التقادم، لذا يصعب توقع أوجه استخدام تلك البيانات المخزنة عليها مستقبلاً، وهو ما يمثل أحد الأخطار التي تهدد الحياة الخاصة للأفراد¹⁸.

¹⁶ هشام بخوش، المرجع السابق ، ص237. وتجدر الإشارة إلى أن الحكومة البحرينية أتخذت تدرجياً سلسلة من الإجراءات العامة لاحتواء إنتشار فايروس كورونا ،ومنها إنشاء لجنة وطنية لرصد ومتابعة الفيروس ، وقامت بعمل تطبيق مجتمع واعى للتباعد المصابين والمخالطين للمرضى. لقراءة المزيد يمكنك زيارة الموقع الرسمي لوزارة الصحة في مملكة البحرين: moh.gov.bh.

¹⁷ عفيفي كامل عقيقي، جرائم الكمبيوتر ، منشورات الحلبي ، بيروت، 2003 ، ص629.

¹⁸ نعيم مغيب، مخاطر المعلوماتية والانترنت، منشورات الحلبي، الطبعة الثانية ، بيروت ،2008، ص163.

ثانياً: شيوع النقل الرقمي للبيانات

لقد أدى شيوع النقل الرقمي للبيانات إلى إحداث مشاكل أمنية كبيرة ، فباتت عملية استراق السمع والتجسس الإلكتروني أكثر سهولة وذلك بسبب عدم مقدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل من خلالها من بيانات ومعلومات، إضافة إلى إمكانية استعمال تلك البيانات بطريقة غير مشروعة ، وكذلك إمكانية اختراق ذاكرة الحواسيب عن بعد ، ولا يقتصر الاختراق على مجرد الاطلاع على حاوية الذاكرة من بيانات ومعلومات ، بل يصل الأمر إلى الاستنساخ أو الإتلاف وإساءة الاستخدام¹⁹.

لذلك نجد أنه وعلى عكس الطرق التقليدية، أصبح بإمكان أي شخص وإن كان يملك قدرًا ضئيلاً من المعرفة التقنية، أن يصل للمعلومات والبيانات ببسر وسهولة ، مما يشكل انتهاكاً لخصوصية الأفراد، ومع تزايد مظاهر الاعتداء ظهرت مشكلة أخرى تتعلق بوسائل الأمان التقنية حيث إنها عاجزة عن توفير الحماية في مواجهة التعديات الواقعة على البيانات الشخصية ، وعلى الرغم من التقدم في مجال التكنولوجيا إلا أن حياة الأفراد وأسرارهم في بيئة النقل الرقمي لاتزال معرضة للانتهاك لعدم توفر الحماية الكافية لها²⁰.

ثالثاً: انتشار بنوك ومراكز المعلومات الشخصية المنشأة من قبل الدول

تقوم العديد من الدول بإنشاء بنوك أو مراكز معلومات تجمع فيها قدرًا هائلاً من البيانات والمعلومات الشخصية عن الأفراد، حيث تقوم بمقارنة ما تسلمه شركات الاتصال الكبرى، وما تجمعها الإدارات والأجهزة الحكومية، من بيانات ولوائح ومعلومات، والقيام بتحليلها والربط بينها واثم تخزينها في النظام المعلوماتي مما يتيح للدول فرض الرقابة على المواطنين ومعرفة تفاصيل حياتهم بمجرد استخدام الرقم الوطني²¹. ومع انتشار الأجهزة المتصلة بالإنترنت وظهور إنترنت الأشياء والحوسبة السحابية تضاعفت تهديدات الحق في الحفاظ على الحياة الخاصة، وذلك لتوسع آفاق الرقابة فأصبحت الرقابة شاملة "Mass Surveillance" ، بحيث تقوم الدول من خلال برامج الرقابة بمراقبة الأفراد واتصالاتهم وتحركاتهم وما يتم تبادلها من صور بينهم عن طريق هواتفهم وببريدهم الإلكتروني . وكما كشفت الاستخبارات البريطانية في مستندات سرية إمكانية التجسس من

¹⁹ محمد محمد القطب، الحماية المدنية للمعلومات الشخصية في مواجهة الثورة التكنولوجية لوسائل الاتصال والتواصل، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة ، مصر ، 2018 ، ص818.

²⁰ عبد الصبور قوي، المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، مصر 2012، ص77.

²¹ محمد محمد القطب، المرجع السابق ، ص818.

خلال برامج الألعاب خاصة عندما تسمح بتحديد موقع الشخص وبياناته مما يشكل تهديداً للحياة الخاصة و الحريات المدنية والحقوق الشخصية الأخرى²². كما اعتبر القضاء الأمريكي هذا النوع من الرقابة الشاملة تعدياً صريحاً على الحريات، ففي قضية مرفوعة من قبل الاتحاد الأمريكي للحريات المدنية ضد عدد من الأجهزة الأمنية والاستخباراتية ووزير الدفاع على خلفية التنصت على المواطنين الأمريكيين ، والقيام بجمع بيانات اتصالاتهم وبياناتهم الشخصية ، اعتبرت محكمة المقاطعة الجنوبية في نيويورك أن هذا العمل لا يدخل ضمن الصلاحيات الممنوحة لهذه الهيئات في إطار مهمتها لحفظ الأمن القومي ومخالف أيضاً للتعديلات الأولى والثاني من الدستور ، اللذين يقران بحرية التعبير ، وحق الشخص في عدم انتهاك حرمة مسكنه دون حق²³. وما تقدم يدل على أهمية توفير الحماية للبيانات الشخصية منعا للاساءة لحقوق الأفراد.

رابعا: الاختراق والتنصت على البريد الإلكتروني

اختراق البريد الإلكتروني يقصد به " الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات عن طريق انتهاك الإجراءات الأمنية"²⁴. وعادة يتم الاختراق باستخدام البرامج المختصة في سرقة كلمات السر وفكها عن طريق مهارات فنية معينة وهو يحدث عن طريق أمرين: البرنامج المسيطر ويعرف بالعميل (client) و الخادم (server) الذي يسهل الاختراق²⁵.

وتتم عملية الاختراق للبريد الإلكتروني من خلال برامج ووسائل متنوعة مثل:

- أحصنة طروادة (Trojan Horses)²⁶ ويكون مصدرها البريد الإلكتروني والمواقع المشبوهة التي يكون ضررها متمثل في إمكانية التجسس والتعرف على كلمات المرور.

²² منى أبو أشقر جبور و محمود جبور، المرجع السابق ، ص42.

²³ American Civil Liberties Union v. James Clapper, No. 13-3994 (S.D. New York December 28, 2013), 959 F.Supp.2d 724.

²⁴ ابراهيم بن داود وأشرف شعت ، الاطلاع على البريد الإلكتروني بين متطلبات النظام العام والحق في سرية المراسلة، جامعة الغريردي ، دفاثر السياسة والقانون، الإمارات العربية المتحدة، 2017، ص28.

²⁵ محمد محمد القطب، المرجع السابق ، ص835.

²⁶ أحصنة طروادة " فيروس حصان طروادة هو نوع من البرامج الضارة التي يتم تنزيلها على جهاز كمبيوتر متكرر كبرنامج شرعي. عادة ما ترى طريقة التسليم مهاجما يستخدم الهندسة الاجتماعية لإخفاء التعليمات البرمجية الضارة داخل البرامج المشروعة لمحاولة الوصول إلى نظام المستخدمين باستخدام برامجهم". What Is a Trojan Horse?:available at Trojan Virus and Malware Explained | Fortinet (Last visit 17 December 2022).

- أوعن طريق IP Address فيتم الاختراق من خلال قيام شخص بالدخول إلى حاسوب شخص آخر أو بربط جهازين مع بعضهما عن طريق المودم وباستخدام البروتوكول IP /TCP حيث يمكن السيطرة على الجهاز الآخر بالتخفي أو بشكل ظاهر ويمكن إرسال ملفات أو تحميل ملفات وإجراء محادثة أو مسح بيانات الطرف الآخر²⁷.

أما بالنسبة للتنصت على البريد الإلكتروني فهو من أكثر صور الاعتداء شيوعاً وخطورةً، ويقع غالباً من قبل السلطات الرسمية من أجل التصدي لقضايا الأمن العام أو قضايا الإرهاب أو للحفاظ على النظام العام . وهو المبرر الذي استندت إليه الولايات المتحدة الأمريكية عند إصدارها لقانون التنصت الأمريكي (The National Security Surveillance Act 2006) للسماح للاستخبارات الأمريكية بمراقبة المكالمات الهاتفية والبريد الإلكتروني الخاص بالأجانب المقيمين في الولايات المتحدة الأمريكية دون إذن قضائي ويمنح ذلك السلطات الأمريكية الحق في التجسس ولكنه كان مشروع قانون ولم يحصل على الأصوات اللازمة لتمريره في مجلس الشيوخ. وكما لا يقتصر التنصت على الحكومات بل يشمل أيضاً مزودي الخدمة القائمين على الإنترنت إلا أن الفرق هنا هو أن الاعتداء يقع بموافقة صاحب البريد الذي يسمح بذلك عند إنشائه للبريد من دون علم منه أو دراية²⁸.

المطلب الثاني

مفهوم الحق في الخصوصية في عالم المعلوماتية

يعد الحق في الخصوصية أحد الحقوق الأساسية للصيقة بشخصية الإنسان، وتم الاعتراف به كحق مستقل في بداية القرن التاسع عشر، ومع التطور التكنولوجي وظهور الثورة المعلوماتية زادت الحاجة إلى توفير الحماية لهذا الحق ، حيث أصبح الحق في الخصوصية أكثر عرضة للانتهاك من أي وقت مضى، فهناك العديد من المخاطر التي باتت تهدد الحياة الخاصة للأفراد ومعلوماتهم وأسرارهم، خاصة تلك التي ترتبط ببياناتهم الشخصية. الأمر الذي يجعل البحث في

²⁷ عبدالله بن ناصر أحمد العمري ، الحماية الجنائية للبريد الإلكتروني، رسالة ماجستير، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض ،2010، ص61.

²⁸ محمد محمد القطب، المرجع سابق ، ص836.

مفهوم الحق في الخصوصية من حيث تحديد تعريفه و البحث في طبيعته القانونية أمراً مهماً للغاية وذلك حتى يتمكن من تحديد العلاقة بين مفهوم الحق في الخصوصية والبيانات الشخصية.

الفرع الأول: تعريف الحق في الخصوصية

إن تعريف الحق في الخصوصية يتطلب منا التطرق لستة مواضيع وهي كالآتي:

- المفهوم اللغوي للحق في الخصوصية.
- المفهوم الإصطلاحي للحق في الخصوصية.
- موقف المشرع البحريني من الحق في الخصوصية.
- الطبيعة القانونية للحق في الخصوصية.
- العلاقة بين مفهوم البيانات الشخصية والحق في الحياة الخاصة.

أولاً: المفهوم اللغوي للحق في الخصوصية

يُراد بالحق في اللغة إحكام الشيء وصحته وصوابه، والثابت الذي لا يمكن إنكاره، أو ضد الباطل، وهو مصدر فعل حق يحق حقوقاً وحققاً يقال حق الشيء يحق حقاً بمعنى ثبت وصدق وصح ووجب وجوباً²⁹، وهو كما في قوله عز وجل: ﴿لِيُحَقَّ الْحَقَّ وَيُبْطَلَ الْبَاطِلُ وَلَوْ كَرِهَ الْمُجْرِمُونَ﴾³⁰.

ويقصد بالخصوصية في اللغة حالة الخصوص، فيقال خصه بالشيء فيقال خصه خصاً، واختصه أي أفرد به دون غيره، ويقال اختص فلان بالأمر وتخصص له إذا انفرد به³¹.

ثانياً: المفهوم الإصطلاحي للحق في الخصوصية

تشمل الخصوصية على إطلاقها خصوصية البيانات، وخصوصية الاتصالات في مواجهة أنشطة الرقابة والتجسس، وخصوصية المكان وحرمة في مواجهة أنشطة الاعتداء المادية، وهي مسائل حرمة المسكن وحرمة الشخص من التفتيش غير القانوني، وأيضاً خصوصية المراسلات ومن ضمنها المراسلات الإلكترونية، فالخصوصية بالعموم تتطوي على حماية مظاهر مادية ومعنوية ومعلوماتية³².

29 محمد بن مكرم بن منظور، تهذيب لسان العرب، الطبعة الأولى، دار الكتب العلمية، لبنان، 1993، ص 290.

30 سورة الأنفال، الآية 8.

33 ابن منظور، لسان العرب، دار صادر للطباعة والنشر، جزء 8، بيروت، 2000، ص 290.

32 بن حيدة محمد، المرجع السابق، 2011، ص 112-128.

وعليه كان من الصعب إيجاد تعريف محدد ودقيق للحق في الخصوصية ، فتعددت التعريفات واختلف الفقهاء في ضبط وتحديد مفهوم واحد لها .
ولا يسعنا المقام هنا لتناول تفاصيل الخلاف الواسع في الفقه حول مدلول الخصوصية ، لما تمتاز به الفكرة من مرونة لاحدود لها، ولاختلافها من مجتمع لآخر، لذا سوف نذكر موقف الفقه والقضاء من تعريف الحق في الخصوصية بشكلًا مختصر:

1- موقف الفقه من الحق في الخصوصية

حيث ذهب جانب من الفقه الأمريكي إلى تعريف الحق في الخصوصية بأنه الحق في الخلوة، فعرّفها الفقيه (Wisten) بأنها "رغبة الإنسان في الوحدة والألفة والتخفي والتحفّظ"³³. وكذلك ذهب الفقيه الفرنسي بادنتر إلى تعريف الحق في الخصوصية من خلال مفهوم الحياة العامة "بأنه كل ما ليس له علاقة بالحياة العامة". وهذا التعريف يتطلب إيجاد معيار يفصل بين الحياة الخاصة والحياة العامة³⁴.

و عُرف الحق في الخصوصية على إنه " انسحاب إرادي ومؤقت للفرد من المجتمع إلى حالة من العزلة، أو الاقتصار على مجموعة صغيرة يألف إليها، أو حتى وسط مجموعات أكبر، لكن يكون في حالة لاتعرف فيها شخصيته ويلتزم بالتحفظ". أو هو حق الشخص في أن يترك في هدوء و سكون، على اعتبار أن كل إنسان لديه خصوصية، لا يجوز للغير أن يدخل إليها دون استئذان، و إما الخلوة تعني أن يبتعد الفرد عن المجتمع و يعيش وحده فترة من الوقت³⁵.

وفي ظل تباين التعاريف الفقهية المذكورة بشأن الحق في الخصوصية ، أصبح من الصعب التوصل إلى مفهوم قانوني محدد لهذا الحق لوجود ازدواج في حياة الإنسان العامة والخاصة. لذلك أخذ الفقه بالعدول تدريجيا عن البحث عن تعريف الحق في الحياة الخاصة واتجه إلى وضع قائمة للقيم التي تعطيها فكرة الخصوصية، وهذا ما فعله الفقهاء الفرنسيون فحاولوا وضع قائمة بالحالات التي تدخل في إطار الحياة الخاصة فذكروا الحياة العائلية، والحياة المهنية ، والحرية في الصورة، وكشف الراتب، وكشف الضرائب، والمرض، وأماكن قضاء أوقات الفراغ ، والموارد المالية³⁶.

33 بارق منتظر عبد الوهاب، المرجع السابق ، ص14.

34 سليم جلال، المرجع السابق، ص13.

35 حسان أحمد محمد، المرجع السابق، ص19، 12.

36 ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي ،دار الثقافة للنشر والتوزيع ،1996، القاهرة ، ص، 26، 288.

2- موقف القضاء من الحق في الخصوصية

أما بالنسبة لموقف القضاء من الحق في الخصوصية، فقد تردد القضاء بداية في إقرار الحق في الخصوصية، حيث أنكر القضاء البريطاني - في المراحل الأولى - الحق في الخصوصية واتجه لعدم إقراره دون تدخل تشريعي، وفي مرحلة لاحقة قام القضاء الفرنسي بإقرار الحق في الخصوصية. ويعتبر القضاء الفرنسي أول من اعترف بحماية الحياة الخاصة فجعل الحماية تشمل الحماية المادية والمعنوية من مختلف صور المساس بالحياة الخاصة³⁷.

أما بالنسبة لموقف القضاء الأمريكي، فقد تباين موقفه من هذا الحق، حيث لم يعترف بداية بالحق في الحياة الخاصة كحق عام على أساس التعديل الرابع للدستور الذي جعل حماية الحياة الخاصة مقتصرة على الحماية المادية فقط³⁸.

ومن ناحية أخرى فلم يضع القضاء تعريفاً محدداً لماهية الحياة الخاصة، واكتفى ببحث العناصر المرتبطة بالحياة الخاصة لكل حالة على حدة وتوفير الحماية والحل المناسب لها³⁹. ومن خلال ماسبق نجد أن فكرة الحياة الخاصة متغيرة من مجتمع إلى آخر ، لذلك من الصعب تحديد أبعادها في نصوص تشريعية جامدة، من الأفضل أن تترك للفقه والقضاء لتحديد ماهيتها حسب الظروف والوقائع، وعلى أن يتمحور نطاقها حول أمرين الأول يشمل حق الفرد في اختيار أسلوب حياته دون تدخل من الغير في حدود النظام العام، والثاني حق الفرد في سرية ماينتج عن هذه الحرية في اختيار أسلوب حياته من معلومات أو وقائع دون معرفة أي شخص كان، إذ أن السرية هي ما يميز الحياة الخاصة للفرد وتضمن له الاحترام لذاته الشخصية وتمنحه الشعور بالسكينة والأمان⁴⁰.

ثالثاً: موقف المشرع البحريني من الحق في الخصوصية

المشرع البحريني لم يعرف المقصود بالحق في الخصوصية ولكنه اتجه إلى الاعتراف بفكرة الحق في الخصوصية فنص على مجموعة من النصوص في مقدمتها الدستور ، فنص فيه على بعض الصور ولم يستعمل فيه مصطلح الحياة الخاصة كحق مستقل للأفراد وكفل الحماية

37 الشيخ يوسف، حماية الحياة الخاصة في القانون الجنائي المقارن، رسالة دكتوراه جامعة القاهرة، دار الثقافة للنشر والتوزيع، الأردن، 1996، ص200.

38 بارق منتظر عبد الوهاب، المرجع السابق ، ص17.

39 صفية شاتن ، الحماية القانونية للحياة الخاصة ، دراسة مقارنة ، جامعة مولود معمري، رسالة دكتوراه، الجزائر ، 2012، ص69.

40 سليم جلال، المرجع السابق، ص19.

المناسبة لها في المواد من (18-31) من الدستور البحريني ، حيث نص المشرع على أن حرية الفرد الشخصية تكون مكفولة فلا يجوز القبض عليه أو توقيفه أو حبسه أو تفتيشه أو تحديد إقامته أو تقييد حريته في الإقامة أو التنقل إلا وفق أحكام القانون وبرقابة من القضاء ، وكما لا يجوز حجزه أو حبسه في غير الأماكن المخصصة لذلك في قوانين السجون المشمولة بالرعاية الصحية والاجتماعية والخاضعة لرقابة السلطة القضائية ، كذلك منع إيذاء المتهم معنوياً وجسدياً وجعل حق التقاضي مكفول له قانوناً. منح حرية التعبير عن الرأي والبحث العلمي، منح الحق في تكوين الجمعيات والنقابات ، عقد اجتماعات خاصة ، جعل للمساكن حرمة لايجوز دخولها وعدم جواز تفتيشه إلا بمقتضى إذن صادر عن الجهات القضائية المختصة وفي حدود القانون والاحترام المطلوب لخصوصيته، جعل لكل فرد الحق في مخاطبة السلطات العامة كتابة وبتوقيعه ، بالإضافة إلى ذلك منح الحرية في المراسلة البريدية والبرقية والهاتفية والإلكترونية وكفل - حماية حرمة المنزل العائلي باستثناء الحالات التي تستدعي حماية المصلحة العامة، كجواز إسقاط حرمة المنزل لضرورة مكافحة الجريمة وتحقيق العدالة. وهذا التدخل هو الذي ينص عليه القانون الوطني بما يتوافق مع أحكام العهد الدولي الخاص بالحقوق المدنية والسياسية ومراميه وأهدافه، بأن يكون متناسباً مع الغرض المنشود وأن يكون ضرورياً في ظروف أي قضية معينة بصرف النظر عن جنسية أو موقع الأفراد الذين تخضع اتصالاتهم لمراقبة مباشرة⁴¹.

ومن خلال ماسبق يتضح لنا أن المشرع البحريني عندما منح هذه الحقوق والحريات للأفراد بموجب الدستور وذلك حماية للحق في الخصوصية وبالتالي ضمان عدم إصدار أية نصوص عضوية أو عادية أو تنظيمية مخالفة للأحكام الدستورية السابقة ، مع ضمان سلامة المصالح الفردية والجماعية من الضرر المترتب عن التمتع المتعسف بالحق في الخصوصية.

إلى جانب تعارض التداخل مع مقتضيات المواد من (93-95) من قانون الإجراءات الجنائية البحريني رقم (46) لسنة 2004. حيث سبل الانتصاف الفعالة تتطلب إلغاء الإجراء المتخذ المتعارض مع أحكام القانون، وذلك استناداً إلى القاعدة الماثورة (ما بني على باطل فهو باطل).

كما منح المشرع في القانون المدني البحريني⁴² في المادة (162) الحق في طلب التعويض عن العمل غير المشروع الضرر ولو كان أدبياً، مبيناً صور الضرر الأدبي التي تشمل "...ما يلحق الشخص من أذى جسماني أو نفسي نتيجة المساس بحياته أو بجسمه أو بحريته أو بعرضه

41 دستور مملكة البحرين الصادر بمرسوم بقانون رقم (5) لسنة 2002.

42 القانون المدني البحريني مرسوم بقانون رقم (19) لسنة 2001.

أو بشرفه أو بسمعته أو بمركزه الاجتماعي أو الأدبي أو باعتباره المالي . كما يشمل الضرر الأدبي كذلك ما يستشعره الشخص من الحزن والأسى". فنلاحظ من هذا النص أن المشرع البحريني لم ينص صراحة على الحق في الخصوصية في القانون المدني ، وعلى الرغم من ذلك من الممكن أن تكون هذه المادة سند لإقرار الحق في الخصوصية إلى جانب الدستور .

وفي ظل ما تقدم من أحكام يمكن القول إن الضرر الناتج عن الاعتداء على خصوصية الأفراد يستوجب التعويض سواء كان الضرر مادياً أم أدبياً، فمواقع التواصل الاجتماعي وتطبيقات إنترنت الأشياء (IoT) وتكنولوجيا الذكاء الاصطناعي تثير إشكالية خصوصية المستخدمين، وبالتالي يجب حمايتها من أي اعتداء ، وعند حدوث أي انتهاك للخصوصية ، يجب على المعتدي أن يعرض المتضرر عما أصابه من ضرر أي ما لحقه من خسارة وما فاتته من كسب نتيجة هذا الاعتداء .

كما نص المشرع البحريني في نصوص متفرقة من قانون العقوبات البحريني على مجموعة من الحالات التي تشكل انتهاكاً للخصوصية وفرض المشرع على مرتكبها عقوبة الحبس أو الغرامة ومن هذه المواد، نجد في المادة (370) نص على أنه " يعاقب بالحبس مدة لا تزيد عن ست شهور وبالغرامة التي لا تجاوز خمسين ديناراً أو بإحدى هاتين العقوبتين من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد إذا كان من شأن نشرها الإساءة إليهم". بالإضافة إلى ذلك نص قانون العقوبات البحريني في المادة (371) على " أنه يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة التي لا تجاوز مائة دينار من كان بحكم مهنته أو حرفته أو وضعه أو فنه مستودع سر فأفشاه في غير الأحوال المصرح بها قانوناً أو استعمله لمنفعته الخاصة أو لمنفعة شخص آخر، وذلك ما لم يأذن صاحب الشأن في السر بإفشائه أو استعماله وتكون العقوبة السجن مدة لا تزيد على خمس سنين إذا كان الجاني موظفاً عاماً أو مكلفاً بخدمة عامة واستودع السر أثناء أو بسبب أو بمناسبة تأديته وظيفته أو خدمته" وإما المادة (372) نصت على أنه "يعاقب بالغرامة التي لا تجاوز عشرين ديناراً من فض رسالة أو برقية بغير رضا من أرسلت إليه أو استرق السمع في مكالمات تليفونية. ويعاقب الجاني بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة التي لا تجاوز خمسين ديناراً إذا أفشى الرسالة أو البرقية أو المكالمات لغير من وجهت إليه ودون إذنه متى كان من شأن ذلك إلحاق ضرر بالغير"⁴³.

⁴³ قانون العقوبات الصادر بالمرسوم بقانون رقم (15) لسنة 1976.

ويتبين من نصوص المواد السابقة من قانون العقوبات البحريني أراد المشرع من خلالها أن يؤكد على مبدأ سرية الحياة الخاصة، ويقصد بالسرية واقعة أو صفة ينحصر نطاق العلم بها بعدد محدود من الناس ، في حالة ما إذا كان هناك مصلحة يقرها القانون لشخص أو لأكثر حتى يظل العلم محصورا في ذلك النطاق⁴⁴. كما يجب أن تكون المعلومات أو البيانات ذات صلة بالشخص ولها تأثير مادي ومعنوي عليه، لكي تعتبر سرا يستوجب حمايته⁴⁵.

ويتمثل حرص القضاء البحريني على الحفاظ على سرية الحياة الخاصة في القضية الجنائية التي حكم فيها مؤخرا ، وهي تتعلق بموظف مرتشي بالمباحث تحصل على رشوة لمدة 3 سنوات بواقع 300 دينار شهريا و قام مقابل ذلك بإبلاغ بنك بالمعلومات الجنائية السرية حول العملاء المتقدمين بطلبات الحصول على القروض متناهية الصغر، حتى تم اكتشاف الواقعة من قبل مصرف البحرين المركزي. وجاء حكم محكمة الكبرى الجنائية الأولى بشأن ذلك بسجن الموظف المرتشي 5 سنوات وبتعريمه مبلغ 10600 دينار قيمة رشوة ، وأستندت المحكمة في حكمها على المادة (371) من قانون العقوبات الأنفة الذكر ، وكما قامت المحكمة بتبرئة الرئيس التنفيذي للبنك من تهمة الاشتراك مع الموظف المرتشي لكونه لم يكن يعلم بوظيفته لدى وزارة الداخلية، كما برأت الرئيس التنفيذي للبنك وأعفت مديره وأوقفت حبس موظفين⁴⁶.

رابعا: الطبيعة القانونية للحق في الخصوصية

إن تحديد الطبيعة القانونية للحق في الخصوصية كان محل خلاف بين الفقهاء وعلى وجه الخصوص في الفقه الفرنسي، وانقسموا بشأنه إلى اتجاهين، يرى أصحاب الاتجاه الأول أن الحق في الحياة الخاصة حق عيني على اعتبار أن الإنسان مالك لحياته الخاصة، أما الاتجاه الثاني فيرى بأن الحق في الحياة الخاصة هو حق الشخصية باعتباره يهدف إلى حماية الحرية الشخصية وترقية القيم المكونة لها، وكل عناصره ومظاهره يشكلان عناصر الشخصية، ونبين هذين الموقفين على التفصيل الآتي:

⁴⁴ محمود نجيب حسني ، شرح قانون العقوبات القسم الخاص ، دار النهضة العربية ، الطبعة السادسة، مصر، 2019، ص 891 .
⁴⁵ عماد محمد، الاعتداء على حرمة الحياة الخاصة في قانون الجرائم الإلكترونية رقم 27 لسنة 2015 ،مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والدراسات الاستراتيجية، الأردن، 2016 ،ص 17.
⁴⁶ تفاصيل الحكم السابق غير متاحة عبر وسائل البحث عن الأحكام القضائية في الموقع الرسمي للمجلس الأعلى للقضاء، ولكن جاء بيان التفاصيل السابقة في صحيفة الأيام، العدد، 12306، البحرين ، 2020 وللمزيد من التفاصيل حول وقائع القضية يرجى زيارة الموقع التالي لصحيفة الأيام : <https://alay.am/p/2txi> (آخر زيارة: 2022/12/17)، وكذلك راجع صحيفة البلاد ، قضية رشوة موظف و4 متهمين محليين ، العدد 4130 ، البحرين ، 2020. و للتعرف على المزيد حول تفاصيل حكم القضية الصادر حكمها في 26 فبراير 2022 يرجى زيارة الموقع التالي لصحيفة البلاد: <https://albiladpress.com/news/2020/4130/bahrain/624430.html> (آخر زيارة: 2022/12/17).

1- الحق في الخصوصية حق عيني

يرى هذا الإتجاه أن الحق في الحياة الخاصة هو يعتبر حقاً عينياً وذلك لأن الإنسان يعد مالكاً لحياته الخاصة وله السلطة على أعضاء جسمه، وهذه الأعضاء تجتمع وتتجسد في الصورة التي تعد من سمات الملكية، وبالتالي فإن علاقة الشخص بصورته وسلطته عليها هي التي تمثل الحياة الخاصة⁴⁷.

ووفقاً لهذا الإتجاه يكون الشخص الطبيعي مالكا لجسده، وله سلطات المالك على الشيء في التصرف والاستغلال والاستعمال، فعلى سبيل المثال يستطيع الشخص أن يتصرف بصورته ويضعها في الإعلانات مقابل مبلغ من المال أو يقوم ببيع مذكراته التي تحتوي على أغلب أسراره. ومن الآثار المترتبة على الأخذ بهذا الإتجاه أن يكون للشخص الحق في رفع دعوى استرداد بقصد الاعتراف بحقه في الملكية وأيضاً من أجل وقف التعدي. دون الحاجة لإثبات الضرر المادي أو المعنوي، وذلك إعمالاً لحقوق المالك⁴⁸.

إلا أن هذا الإتجاه كان عرضة للانتقاد على اعتبار أن الحق العيني يفترض وجود صاحب حق ووجود موضوع يمارس عليه سلطاته، وحتى يصلح التصرف فيه لا بد أن ينفصل صاحب الحق عن موضوع الحق، أما إذا اتحد صاحب الحق مع موضوع الحق فيستحيل أن يكون محلاً للملكية، كما إن الحق في الملكية محله الشيء المادي في الغالب لذلك يركز على صورة الشخص، في حين نجد أن الحق في الحياة الخاصة يجمع جانبين مادي ومعنوي للشخصية الأمر الذي يجعلنا نستبعد طبيعته كحق عيني⁴⁹.

2- الحق في الخصوصية حق لصيق بالشخصية

نظراً للانتقادات الموجهة إلى الاتجاه الأول، ذهب أغلب الفقه والقضاء الفرنسي الحديث إلى اعتبار الحق في الخصوصية من ضمن الحقوق الشخصية التي تلازم الإنسان والتي تهدف بدورها لحماية الحرية الشخصية والمحافظة على كيان الإنسان المادي والمعنوي وهذا ما يتمتع به الحق في الخصوصية بجمعه بين الجانب المادي والمعنوي للشخصية كما أنه يثبت للأشخاص كافة.

47 ممدوح خليل بحر، المرجع السابق، ص269.

48 حسام الدين الأهواني، المرجع السابق، ص144، 142.

48 عبد القادر عمير، المرجع السابق، ص442.

ورتب الفقه على هذا الرأي نتائج أهمها منح صاحب الحق في الخصوصية سبيل اللجوء للقضاء لوقف الاعتداء أو منعه دون انتظار وقوع الضرر والالتزام بإثبات عنصر الخطأ والضرر فتكون الحماية بذلك أكثر قوة وفعالية ، مما لو تركت مسألة الحماية لقواعد المسؤولية المدنية التي يشترط فيها إثبات عناصرها الثلاث الضرر والخطأ وعلاقة السببية بين الخطأ والضرر، إضافة إلى أن إثبات المسؤولية لا يوفر إلا الحماية اللاحقة للحق من الاعتداء عليه، والتعويض لا يفلح دائما في محو كل أثر للضرر ولكن الحماية القوية تكون عن طريق الوقاية من الاعتداء على الخصوصية، وهذا لا يتحقق إلا من خلال الاعتراف بالحق في الخصوصية باعتباره حق شخصي. كما إن فكرة الحقوق الشخصية تتميز بأنها توفر الحماية القانونية التي تلزم الكافة في احترام حق الشخص في حرمة حياته الخاصة دون التجسس عليها وعدم نشر أي شيء يتعلق بها. كما لا يحق لأي شخص الاطلاع على أسرارها إلا بموافقة مسبقا⁵⁰.

3- طبيعة الحق في الخصوصية في التشريع البحريني

لقد تبين من خلال التطرق لطبيعة الحق في الخصوصية، إن الفقه والقضاء المقارن سلكا اتجاهين مختلفين، فذهب الأول إلى أن الحق في الحياة الخاصة حق ملكية، وأما الثاني وهو الاتجاه الغالب فكيّفه على أنه من الحقوق الملازمة للشخصية. المشرع البحريني أخذ بالاتجاه الثاني ضمنا ، واعتبر الحق في الحياة الخاصة أو الخصوصية من الحقوق الملازمة للشخصية، ويطلق عليها كذلك الحريات العامة ، وتشمل حقوق الشخصية طائفة من الحقوق كحق الإنسان في الحياة وسلامة بدنه وشرفه، وحقه في العمل والزواج والتنقل والإقامة، وحرية الرأي والعقيدة والاجتماع وحرمة المال وحرمة المسكن وعدم انتهاك أسرارها الشخصية، وهي كلها حقوق أساسية لا يمكن أن يعيش الإنسان بدونها . وهذه الحقوق أفرد لها المشرع البحريني حماية دستورية خاصة وخصها بتنظيم خاص في المواد (17-31) ماعدا المادة (30) الدستور البحريني المعدل لسنة (2002).

كما منح المشرع بعضا من الحقوق بموجب قانون حماية حقوق المؤلف البحريني ومنها الحق في الصورة وهو لم ينص عليه كحق مستقل في القانون وإنما يجد أساسه ضمن المادة (2) والمادة (24) من قانون حماية حقوق المؤلف والحقوق المجاورة البحريني ومنحه المشرع الحماية اللازمة 51، وبالإضافة إلى المادة (4) من قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018، التي بموجبها منحت الشخص الحق في عدم معالجة بياناته الشخصية دون موافقته

⁵⁰ بن حيدة محمد، المرجع السابق، ص42، 41.

⁵¹ قانون حماية حق المؤلف والحقوق المجاورة ، قانون رقم (22) لسنة 2006.

الصريحة. وتعرف الصورة بأنها عبارة عن تمثيل إما لشخص أو شئ من خلال أحد الفنون مثل النقش والنحت أو تصوير فوتوغرافي أو فيلم. ويتحدد مضمون هذا الحق بموجب المادة السابقة بأنه لايجوز إنتاج صورة بدون رضا صاحبها وإلا سيكون ممارسة هذا الحق غير مشروع⁵²، وبناء على ذلك يحق للشخص بأن يعترض لغير المرخص له صراحة أو ضمناً في حال تم أخذ صورة له أو تصوير فيديو بغير رضاه ، كما له الحق أن يعترض في حال تم نشر صورته من قبل جهة أخرى دون إذنه من أجل استخدامها مثلاً كوسيلة للمساس بالشرف والإعتبار لأنه سيعد بذلك مساساً بحق غير مشروع من الحقوق الملازمة للشخصية ، طالما هذا النشر لم يكن للمصلحة العامة⁵³.

كما منح المشرع الحق في الأسم ويعرف بأنه مايميز الشخص عن غيره من الأشخاص فهو يعد من ضرورات التنظيم داخل المجتمع لأن كل قانون يلزم الأفراد بأن يكون لكل شخص أسم ولقب ولأهمية ذلك كفله المشرع بالحماية وذلك وفقاً لقانون حقوق المؤلف والحقوق المجاورة في المادة (5) منه ، حيث "منح المشرع للمؤلف الحق في نسبة المصنف إليه، وبوجه خاص حقه في وضع اسمه على جميع نسخ المصنف - عندما يكون ذلك ممكناً - بالطريقة المألوفة وكذلك الحق في أن يبقى اسمه مجهولاً أو أن يستعمل اسماً مستعاراً".

بالإضافة إلى ذلك هناك حق منحه المشرع بموجب قانون حقوق المؤلف والحقوق المجاورة البحريني وهو الحق المعنوي للمؤلف، فهو يعتبر مظهر من مظاهر الشخصية الإنسانية يعبر عن شخصية صاحبه وهو من الحقوق الملازمة للشخصية أو الحريات العامة مشتق من حرية الرأي والتعبير والعقيدة ولايدخل في الذمة المالية، وهذا الحق يهدف لحماية شخصية المؤلف بسبب العلاقة اللصيقة بينه وبين إنتاجه الفكري⁵⁴، ومنح المشرع الحق للمؤلف بموجب المادة (5) من قانون حماية حقوق المؤلف والحقوق المجاورة رقم (22) لسنة 2006 ونص على الاتي "الحق في تقرير نشر مصنفه لأول مرة، وتحديد طريقة هذا النشر وموعده. وكذلك الحق في منع طرح مصنفه للتداول وفي سحبه من التداول رغم سبق تصرف المؤلف في حقوقه المالية، وذلك إذا طرأت أسباباً جدية تبرر المنع أو السحب، ويجب في هذه الحالة أن يستصدر المؤلف من المحكمة المختصة حكماً بمنع طرح مصنفه للتداول أو بسحبه منه، وتقضي المحكمة في حالة إجابته إلى طلبه بإلزامه ، بدفع مقدماً تعويضاً عادلاً لمن آلت إليه الحقوق المالية خلال أجل تحدده المحكمة وإلا أعتبر الحكم كأن لم يكن".

52 سعيد جبر، الحق في الصورة، دار النهضة العربية، القاهرة، 1986، ص1 و2.

53 يوسف بوجمعة، الحقوق الملازمة للشخصية وتقسيماتها دراسة على ضوء الفقه والقانون والقضاء، مجلة الدراسات القانونية، جامعة المدييه، المجلد الرابع ، العدد الأول، 2018، ص348.

54 محمد حسنين، الوجيز في الملكية الفكرية، (لايوجد سنة طبع)، المؤسسة الوطنية للكتاب، الجزائر، 1985، ص109.

وكذلك نجد أن المشرع البحريني عندما أصدر قانون حماية الطفل رقم (37) لسنة 2012 ضمن حق الطفل في عدم تعرضه للاستغلال الاقتصادي في أي عمل يعتبر ضاراً لصحتهم ونموهم العقلي والبدني والنفسي⁵⁵. وفي قانون العمل الأهلي رقم (36) لسنة 2012 وتعديلاته اهتم المشرع البحريني في مجال إشراك من هم دون الـ 18 بمناحي العمل المختلفة وفقاً للمواثيق الدولية التي تسمح بتوظيف الأحداث وذلك ضمن شروط ومعايير محددة، حيث نجد أنه في المادة (28) منه قام بتصنيف 42 مهنة حظر توظيف الأحداث فيها لانتفاء تعرضهم للاستغلال البدني أو النفسي أو الجنسي⁵⁶.

ومن خلال ماتقدم نجد أنه مع التطور التكنولوجي الذي نشهد حالياً ، وإزدياد المخاطر التي تهدد خصوصية الإنسان أدى ذلك لظهور فكرة الحقوق الملازمة للإنسان أو مايسمى " بحقوق الشخصية" بإعتبارها وسيلة لحماية خصوصية الإنسان ، وهذا جعل جل التشريعات العربية ومنها المشرع البحريني أن يولي اهتماماً بهذه الحقوق ويكفل لها الحماية القانونية اللازمة لحماية الحق في الخصوصية .

خامساً: العلاقة بين مفهوم البيانات الشخصية ومفهوم الحق في الحياة الخاصة

من خلال تحديدنا لمفهوم الحق في الخصوصية ، و مفهوم البيانات الشخصية، يمكن أن نحدد العلاقة بين كلا المفهومين. ونلاحظ مما تقدم، أن مجموعة من عناصر الحق في الحياة الخاصة كالصوت والصورة والآراء السياسية وغيرها، تتقاطع مع مضمون البيانات الشخصية وهو ما يؤدي للقول بأن البيانات الشخصية هي حياة خاصة في المجال المعلوماتي أو ما يطلق عليه بالخصوصية المعلوماتية التي تُعرف على إنها " حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين"⁵⁷.

ويتبين لنا من خلال التعريف السابق إن تحديد مفهوم الحياة الخاصة في المجال المعلوماتي هو أمر شاق نظراً لصعوبة إيجاد تعريف للحياة الخاصة جامع مانع كما أسلفنا. فالتعريفات متباينة ومتعددة و مرتبطة بالقيم المجتمعية والتوجهات السياسية والاقتصادية لكل مجتمع وهي متغيرة بتغير الأزمان ، مع ذلك يمكن تحديد الطبيعة القانونية للبيانات الشخصية باعتبارها جزءاً من مفهوم الحياة الخاصة المتعلق بالجانب المعلوماتي، ويمكن القول إن المعالجة المعلوماتية للبيانات

55 قانون حماية الطفل البحريني رقم (37) لسنة 2012 .

56 قانون العدالة الإصلاحية للأطفال وحمايتهم من سوء المعاملة رقم (4) لسنة 2021.

57 هذا التعريف للفقيه الأمريكي (ويستن) وتم الإشارة له في مرجع : عايشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث ، المجلد الثاني ، العدد 5، جامعة عبد الحميد بن باديس- مستغانم، المغرب ، 2016، ص40.

الشخصية قد تشكل تهديداً مباشراً للحقوق والحريات خاصة أثناء معالجة البيانات الشخصية الحساسة التي تتعلق بالآراء السياسية أو المعتقدات الدينية والبيانات الطبية للأفراد⁵⁸.

وبخلاصة ما تقدم أنه ومن خلال تحديد العلاقة بين البيانات الشخصية والحياة الخاصة، وإدراج البيانات الشخصية في إطار الحق في الخصوصية في الجزء المتعلق بالمعلوماتية، يمكن القول إن الحق في حماية البيانات الشخصية هو حق في الخصوصية المعلوماتية أو هو حق في الحياة الخاصة في المجال المعلوماتي، والمساس به هو مساس مباشر بحقوق وحريات الأفراد⁵⁹.

الفرع الثاني: التحديات التي يفرضها عالم المعلوماتية على الحق في الخصوصية

في ظل الثورة المعلوماتية وظهور التقنيات التكنولوجية الحديثة أصبح هناك تحديات جسيمة تفرض أمام الخصوصية ، حيث أصبحت الأخيرة مهددة بالزوال في عالم يكاد أن يكون تحت المراقبة، تجمع فيه الأجهزة ملايين المعلومات كل لحظة وتقوم الآلات الذكية بتحليلها، وبهذا يصبح التنبؤ بسلوك الأفراد ممكناً بسبب الكم الضخم من البيانات المتوافرة عنهم، وفي ضوء ما سبق ندرك تنوع المداخل والطرق لأختراق خصوصية الأفراد والتي نوضحها فيما يلي:

أولاً: الهواتف الذكية

نظراً لتزايد استخدام المستهلكين للهواتف الذكية ، فإن الأجهزة المحمولة تجمع وترسل مجموعة كبيرة من البيانات. تحتوي هذه الأجهزة على مجموعة من أجهزة استشعار توليد البيانات، وأجهزة استشعار الحركة ، والكاميرات ، بما في ذلك نظام التموضع العالمي أو ما يعرف اختصاراً بـ (GPS)⁶⁰، وكما يمكن أن تنقل بيانات تحديد الموقع عبر الإنترنت أو الشبكات الأخرى. حيث تحتوي العديد من الأجهزة المحمولة على مستشعر (GPS) يسجل موقع المستخدم الجغرافي ، ولكن حتى بدونه، يمكن معرفة المواقع التقريبية وذلك من خلال مراقبة الشبكات اللاسلكية المتاحة، نظراً لأن بيانات الموقع تربط العالم عبر الإنترنت بالبيئة المادية للمستخدم ، فغالباً ما تُعتبر هذه البيانات حساسة بشكل خاص. كما تحتوي العديد من هذه الأجهزة أيضاً على كاميرات تستخدم لالتقاط الصور يمكن اعتبارها كمستشعرات ، وقد تكون البيانات التي تنتجها خاصة بالنسبة لأجهزة الاستشعار مثل الكاميرات ، يُفترض أن يكون المستخدم على علم عند تشغيلها ، وتعتمد الخصوصية

58 عبد المجيد كوزي ، الحماية القانونية للبيانات و المعطيات ذات الطابع الشخصي، رسالة دكتوراة ، جامعة سيدي محمد بن عبد الله، فاس، المغرب ، 2014-، 2015 ص58.

59 حسن الحافظي ، المرجع السابق ، ص35-34.

60 Global Positioning System

على هذه المعرفة. أما بالنسبة إلى كاميرات الويب ، فيشير الضوء عادةً إلى ما إذا كانت الكاميرا قيد التشغيل ، ولكن قد يحدث تلاعب بهذا الضوء بواسطة البرامج الضارة. فأصبحت الهواتف الذكية اليوم مصممة بطريقة تمكنها من القيام بعدة مهام أكثر من جهاز رقمي في السابق، وهي تكون دوماً على اتصال بالإنترنت، فضلاً عن تطوير قدراتها على نقل البيانات بسرعة هائلة. وتبدو أنظمة تشغيل هذه الهواتف مصممة أساساً للحصول على معلومات المستخدمين، حيث تكون الإعدادات التلقائية دائماً بإتجاه التشارك والإتاحة إلا عند تعديلها من قبل المستخدم الذي لا يكون على معرفة أصلاً بذلك، وهي البيانات التي تستحوذ عليها التطبيقات التي يقوم بتحميلها المستخدم ويقوم بالتنازل لها طوعاً عن بياناته من خلال موافقته على شروط الاستخدام ، فضلاً عن تسلل برمجيات الدعاية والتجسس⁶¹.

ثانياً: وسائل التواصل الاجتماعي

تأتي قضية استغلال معلومات 87 مليون مستخدم فيما عرفت بفضيحة " كامبريدج أناليتكا" ضمن سلسلة طويلة من الفضائح الرقمية التي تؤكد على أن الخصوصية أصبحت مهددة بشكل كبير، ففي عام 2018 اتهم مستخدمو فيسبوك الموقع بانتهاك قواعد الخصوصية من خلال مشاركة بياناتهم مع أطراف ثالثة ، من بينها شركة " كامبريدج أناليتكا" والتي أرتبطت بحملة دونالد ترامب الرئاسية لعام 2016 ، وقامت شركة " كامبريدج أناليتكا" في ذاك الحين بجمع البيانات الشخصية لـ 87 مليون مستخدم على فيسبوك واستغلالها من دون موافقتهم ، وقامت باستخدامها لتطوير برمجيات لتوجيه الناخبين الأميركيين للتصويت لصالح ترامب . تم بعد ذلك استجواب " مارك زوكربيرج" مؤسس فيسبوك أمام الكونجرس الأمريكي ، وقام بالاعتراف بهذه الانتهاكات ، وهي القضية التي تم تسويتها بتغريم فيس بوك خمس مليارات دولار من جانب المفوضية الفيدرالية للتجارة بالولايات المتحدة بالإضافة لرقابة مستقلة على إدارة بيانات فيسبوك⁶². ولعل ما حصل في هذه القضية يوضح مدى الخطورة التي تتعرض لها الخصوصية في مواقع التواصل الاجتماعي ، حيث تساهم المعلومات الشخصية التي يتيحها المستخدمون عن أنفسهم على مواقع التواصل الاجتماعي وتطبيقاتها بما تحتويه من التفاصيل عن الحالة المادية والحالة المعنوية الخاصة بحياتنا ، ويمكن تحليل هذا العدد الضخم من البيانات مجتمعة للتوصل لمعلومات أكثر عمقاً

⁶¹ Privacy and Information Technology, Stanford Encyclopedia of philosophy, published Thu Nov 20, 2014 [Privacy and Information Technology \(Stanford Encyclopedia of Philosophy/Summer 2020 Edition\)](#) (last visit:28 May2022).

⁶² Mike Isaac, Cecilia Kang, Facebook Expects to Be Fined Up to \$5 Billion by F.T.C. Over Privacy Issues, The New York Times, accessible at: [Facebook Expects to Be Fined Up to \\$5 Billion by F.T.C. Over Privacy Issues - The New York Times \(nytimes.com\)](#).(last visit: 28 May 2022) .

وشمولاً عن المستخدمين وحياتهم الشخصية. و شبكات التواصل الاجتماعي لاتجمع بيانات المستخدمين فقط ولكنها تسمح بنشر معلومات عن أشخاص آخرين. كما إن الشركات الكبرى تقوم باستخدام البيانات التي يشاركها مستخدمي وسائل التواصل الاجتماعي للحصول على الإعلانات وتحقيق المزايا المالية . وفي السياق ذاته، لا تقوم مواقع التواصل الاجتماعي بجمع البيانات فقط وإنما تقوم أيضاً باستغلال موافقة المستخدمين على أحكام استخدام تطبيقاتها للاستحواذ على بياناتهم المخزنة على هواتفهم وأجهزتهم الذكية.

ثالثاً: تقنيات الذكاء الاصطناعي

يعرف الذكاء الاصطناعي (Artificial intelligence) بأنه أحد فروع علم الحاسوب حيث يشمل العديد من التقنيات والتكنولوجيا المتطورة التي تمكن الآلات من محاكاة القدرات العقلية البشرية، سواء كان ذلك في طريقة التعبير عن المشاعر أو في التفكير أو في طريقة اتخاذ القرارات بناءً على معطيات الظروف من حولهم ، ومن الأمثلة التي يتمثل فيها الذكاء الاصطناعي هي السيارات ذاتية القيادة والطائرات المسييرة بدون طيار وبرمجيات الترجمة أو الاستثمار وغيرها الكثير من التطبيقات المنتشرة في حياتنا⁶³.

ويعد الذكاء الاصطناعي ثورة في عالم التغير الرقمي الذي من شأنه التأثير بشكل كبير على خصوصية المستخدمين، حيث شكلت هذه التقنيات تهديدا للخصوصية والشفافية والسلامة بالإضافة للتأثير المتوقع على الأشغال والوظائف. فعلى سبيل المثال، تقنية التعرف على الوجوه المستندة إلى الذكاء الاصطناعي يمكنها تطوير خبرة مستخدمي مواقع التواصل الاجتماعي وتوفير خدمات مميزة لهم ، ولكن في الوقت ذاته يمكن لهذه التقنيات أن تصبح وسيلة للمراقبة وعدم امتلاك القدرة على حجب الهوية، الأمر الذي يزيد من المخاوف بشأن شفافية عمليات جمع البيانات ومدى امتلاك القدرات اللازمة للمحاسبة وتقويم الممارسات والجهات التي تقوم بذلك لاسيما في ظل رغبة الحكومات في الولوج لتلك البيانات من أجل أغراض أمنية، ما يستوجب معه وضع قواعد أخلاقية وقانونية لمواجهة تقنيات الذكاء الاصطناعي وانتشارها⁶⁴.

⁶³ مركز البحوث والمعلومات، الذكاء الاصطناعي ، الغرفة التجارية الصناعية في أبها ، 2016، ص 5 .

المزيد من التفاصيل الرجاء الإطلاع على : <https://www.abhacci.org.sa> (آخر زيارة 2022/12/17).

⁶⁴ Internet Society Global Internet Report: Paths to Our Digital future (2017), report , p. 32 available at: www.internetsociety.org (last visit:17 December 2022).

رابعاً : تطبيقات إنترنت الأشياء

يقصد بـ (إنترنت الأشياء) أو ما يسمى (Internet of Things – IoT) عملية ارتباط أي شيء بالإنترنت عن طريق مجموعة من البروتوكولات الخاصة، و هي عبارة عن شبكة من الأشياء المادية، ولا يمكن اعتبار (IoT) شبكة من أجهزة الكمبيوتر فقط ، ولكنها تطورت حالياً لتصبح شبكة من الأجهزة بمختلف الأنواع والأحجام مثل الهواتف والأجهزة المنزلية ولعب الأطفال والكاميرات والأدوات الطبية والأنظمة الصناعية ، الحيوانات ، الناس ، المباني ، كل شيء متصل على أساس البروتوكولات المنصوص عليها من أجل تحقيق إعادة تنظيم لمختلف الاتصالات والعلاقات⁶⁵.

ومع ظهور تطبيقات إنترنت الأشياء وتزايد استخدامها أصبحت كل تفاصيل حياتنا اليومية مترابطة على شبكة واحدة ضخمة، الأمر الذي ينذر بمخاطر متعددة في حال تعرض خصوصية البيانات للانكشاف وهو ما يستوجب تطوير ممارسات الأمن الرقمي وسلامة البيانات الشخصية. وتوفير الحماية للخصوصية في مثل هذه التقنيات أمراً مهماً جداً ، نظراً لارتباطها بالعديد من الأدوات والأجهزة مثل الأدوات الطبية والسيارات والأجهزة المنزلية ولعب الأطفال، كما أن هذه التقنيات تمتلك قدرة على تسجيل ونقل ومعالجة البيانات عن طريق استخدام نماذج للتصميم تجمع بين إنترنت الأشياء والحوسبة السحابية وتقنيات الذكاء الاصطناعي، مثل "مكنسة رومبا"⁶⁶ وهيمكنسة روبوتية ذاتية القيادة تتنظف المنازل من الغبار، والتي أطلقت إصداراً جديداً في سبتمبر 2018 يمتلك القدرة على تسجيل صور للمنزل وتخزين خريطة له على شبكة الإنترنت وتذكرها. ويشمل هذا الأمر أيضاً التقنيات القابلة للارتداء (Wearables) وهي التي يمكن ارتداؤها مثل النظارات والأساور والساعات الذكية، والتي انتشرت انتشاراً سريعاً وكل هذه التقنيات تمثل تهديداً للخصوصية ، وإن لم يكن بإمكاننا أحياناً ملاحظة قدراتها على تسجيل ونقل البيانات. فعلى سبيل المثال نظارة جوجل تحمل كاميرا صغيرة -من الصعب ملاحظتها- إلا إنها قادرة على النقاط الصور والفيديو، مما جعل جوجل تطرح نظارتها على المستوى الصناعي فحسب وعدم إتاحتها للتداول التجاري، فيما تبدو "نظارة سبيكتاكليس" التي طرحتها سناب شات أشبه بنظارة

⁶⁵ Carlos Salazar, Sunil Patel and Keyur K Patel (2016), *International Journal of Engineering Science and Computing*, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, volume 6 , p 6122, available at: https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges (last visit: 31 May 2022)

⁶⁶مكنسة رومبا للإطلاع على المزيد من التفاصيل حولها الرجاء زيارة الموقع التالي: [Roomba® Robot Vacuum](https://www.ROOMBA.com). Cleaners | iRobot®

شمس عادية ولكنها مزودة أيضا بكاميرا مقاومة للمياه تمكنك من التقاط الفيديو والصور بجودة فائقة وبثها عبر الإنترنت⁶⁷.

ومع انتشار تطبيقات إنترنت الأشياء إزدادت معدلات التعدي على الخصوصية. وذلك لأن بيانات المستخدمين المخزنة في هذه التطبيقات يتم ربطها بالعديد من الآلات والأشياء المادية التي تتفاعل مع بعضها البعض عبر الإنترنت. وينتج عن ذلك كمية هائلة من البيانات مما يتطلب توافر قدرات عالية من آليات التخزين لتتمكن من إدارة هذا الحجم الهائل من البيانات. وعليه كان من اللازم العمل على وضع معايير موحدة عالميا للإنترنت بالإضافة للعمل على دراسة آليات تشفير البيانات بصورة جيدة لضمان الحفظ الآمن لها ولوسائل النقل والتراسل الفعال⁶⁸.

خامسا: الحوسبة السحابية والحوسبة الكمية

عرف المشرع البحريني الحوسبة السحابية على أنها " نظام لتمكين النفاذ، عند الطلب بشكل متاح على نحو واسع ومريح، عبر شبكة لمجموعة مشتركة من موارد الحوسبة القابلة للتهيئة (مثل الشبكات، الخوادم، ومعدات التخزين والتطبيقات والخدمات) يتييسر توفيره وإطلاقه بسرعة عالية وبدرجة منخفضة من الجهد الإداري أو التفاعل مع مزود الخدمة"⁶⁹.

- وتقدم برامج الحوسبة السحابية العديد من المزايا والخدمات للمستهلكين منها⁷⁰:
- إمكانية الاستفادة منها في حفظ وتخزين معلومات دائمة في حاسبات خادمة متصلة بالإنترنت، إضافة إلى الحفظ والتخزين المؤقت على الأجهزة الطرفية المرتبطة بها .
- تقديم منصات عمل رخيصة ومضمونة عند الطلب، مع إتاحة إمكانية الوصول إليها بطرق سهلة، ومن ثم توفير الجهد، وكذلك الكثير من المال الذي ينفق على شراء البرمجيات .

⁶⁷ فاطمة زهراء المفتاح، ملامح الخصوصية والأنكشاف في عصر التقنيات الذكية، دراسات المستقبل ، العدد 7 ، الإمارات، 2019، ص17.

⁶⁸ أحمد محمد علي عبد المختار، توظيف تقنيات أنترنت الأشياء في تطوير خدمة المكتبات الأكاديمية، جامعة المنيا مصر، مجلة ببلوفيليا لدراسات المكتبات والمعلومات، المجلد 3، العدد 10 ، مصر ، 2021، ص230.

⁶⁹ المادة (1) من مرسوم بقانون رقم (56) لسنة 2018 بشأن تزويد خدمات الحوسبة السحابية لأطراف أجنبية

⁷⁰ أمين بن سعيد، ونادية عبد الرحيم، وأحمد مخلوف، مستقبل نظم المعلومات المحاسبية في ظل تكنولوجيا الحوسبة السحابية، مجلة الميادين الاقتصادية، المجلد 01، العدد 01، الجزائر، 2018، ص15-16. لمزيد من التفاصيل حول موقف المشرع البحريني من الحوسبة السحابية راجع: نور أحمد العوضي، التنظيم القانوني لعقد الحوسبة السحابية، رسالة ماجستير، جامعة البحرين، 2021.

- تمكين المستخدم من الولوج الآمن، والاستفادة من الخوادم الضخمة في إجراء عمليات معقدة، قد تتطلب أجهزة بمواصفات عالية، حتى لو كان هذا المستخدم لا يمتلك الخبرة المعرفية الكافية .
- ضمان الصيانة وتوافر التحديث بشكل دائم من خلال الطرف الثالث، والذي تمثله الشركات المستضيفة وعلى الرغم مما تقدم من مزايا ولكن قد يشكل استخدام الحوسبة السحابية تهديداً ضد الخصوصية، حيث يتم تخزين البيانات في جهاز ثالث يتحمل المسؤولية عن حمايتها، بما يحمله ذلك من مخاطر، مثل إمكانية تعرض بيانات المستخدم للسرقة من قبل المخترقين. ولمواجهة مخاطر استعمال الحوسبة السحابية سعت مملكة البحرين إلى التعاقد مع شركة أمازون على الصعيد الاستراتيجي، وذلك لتوفير ونشر البنية التحتية للخدمات السحابية والاستفادة منها، عن طريق استضافتها لشركة أمازون التي توفر خدماتها في ثلاث نطاقات بمنطقة الخليج سواء للقطاعين العام أو الخاص⁷¹.

وأما الحوسبة الكمية فيقصد بها الحوسبة التي تعمل وفق نظم معقدة ومتعددة قادرة على إجراء عدة عمليات في وقت واحد وفقاً لمبادئ النظرية الكمية، بما يمكنها من حل المسائل الرياضية المعقدة المستخدمة في عمليات التشفير، وهو ما يحمل مخاوف بشأن معايير الأمن الرقمي. ويختلف الكمبيوتر الكمي عن الكمبيوتر العادي، حيث يعتمد الأخير على رقائق السيليكون التي تقوم بتخزين البيانات بعد تحويلها إلى النظام الرقمي وفقاً للمنظومة الثنائية "صفر أو واحد"، في حين يعتمد الكمبيوتر الكمي على تفكيك وإعادة بناء الذرة أو الجزيء للتخزين، وهو ما يتيح سرعات غير مسبقة تتجاوز بكثير قدرات الكمبيوتر العادي، ويقول الخبراء إنه خلال فترة تتراوح بين 10 و15 سنة يمكن إنتاج أجهزة كمبيوتر كمي قادرة على اختراق ما نعتبره الآن بيانات مؤمنة، مثل البيانات المصرفية وبيانات الرعاية الصحية لدى القطاع الخاص، وكذلك المعلومات شديدة الحساسية الخاصة بالحكومات والمؤسسات العسكرية⁷².

⁷¹ لمزيد من التفاصيل حول تعاقد حكومة مملكة البحرين مع خدمات أمازون للإنترنت يمكنك زيارة الموقع الرسمي للمملكة البحرين:

www.bahrain.bh

⁷² فاطمة زهراء المفتاح، المرجع السابق، ص20.

سادسا: برمجيات القرصنة والاختراق

إن مخاطر برمجيات القرصنة والاختراق عديدة فهي لا تشكل خطورة على خصوصية الحقوق الفردية والبيانات الشخصية فحسب، وإنما ذلك يشمل مخاطر اختراق قواعد بيانات المؤسسات، خاصة مع الاتجاه حالياً من قبل الدول لبناء الحكومات الرقمية، وتقديم الخدمات الإلكترونية السحابية، وغيرها ، الأمر الذي يثير المخاوف حول ما قد يحدث من مخاطر جسيمة قد تتعرض لها هذه البيانات، والتي أصبحت تعتمد على الإنترنت في عمليات الحفظ والتبادل والتخزين عبر الشبكات، وأصبحت بذلك معرضة لهجمات القرصنة والاختراق التي تكون مدفوعة بأهداف اقتصادية بغرض الاتجار، أو الأبتزاز كبرمجيات الفدية، أو أهداف أمنية كالإرهاب، كما أن الدراسات قد حذرت من هجمات تستهدف الاستحواذ على بيانات حساسة أو سرية، عن طريق الولوج لقواعد بيانات مستشفى والتلاعب ببيانات المرضى ما يؤدي بحياة المئات، بالإضافة لبرمجيات التجسس⁷³، فقد تتعرض الوسائط الرقمية لهجمات الاختراق من قبل ما يسمى ببرمجيات الدعاية (Adware)، هي عبارة عن برامج ضارة تقوم بجمع المعلومات عن المستخدم من غير موافقته . وهذا يتم عن طريق سجل التصفح ونتائج البحث وأيضاً عن طريق الإعلانات التي تظهر في واجهة مستخدم البرنامج أو على الشاشة أثناء عملية تثبيت أحد البرامج، كما يمكن أن تحتوي هذه الإعلانات حتى على أحصنة طروادة وبرامج التجسس. و قد يتم أيضاً دمج هذه البرامج الإعلانية مع برنامج أو ألعاب يتم تنزيلها مما يشكل ذلك خطراً على المستخدم⁷⁴.

وبرمجيات الدعاية تختلف عن برمجيات التجسس (spyware) ، وهي عبارة عن نوع من البرامج الضارة التي تصيب جهاز الكمبيوتر أو الجهاز المحمول وتجمع معلومات عن المستخدم، وذلك من خلال المواقع التي يزورها أو الأشياء التي يقوم بتنزيلها وأسماء المستخدمين وكلمات المرور وكذلك رسائل البريد الإلكتروني حيث ترسل وتنتقل. فإن برامج التجسس تجد طريقها إلى جهاز الكمبيوتر بشكل مستتر دون علم المستخدم أو إذنه ، وتربط نفسها بنظام التشغيل ، وقد يسمح المستخدم بدون قصد لبرامج التجسس هذه بالتثبيت وذلك عندما يوافق على شروط وأحكام برنامج يبدو أنه شرعي دون قراءة التفاصيل الدقيقة ، مما يؤدي ذلك إلى تعرضه للاختراق وانتهاك خصوصيته⁷⁵.

⁷³ C. Bryan Foltz, Cyberterrorism, computer crime, and reality, Information Management & Computer Security, Vol. 12 Issue 2, 2004, p. 159.

⁷⁴ <https://www.cisco.com/c/en/us/products/security/adware-vs-spyware> (last visit: 12 December 2022).

⁷⁵ [What is Spyware | Spyware Removal and Protection | Malwarebytes .html](https://www.malwarebytes.com/what-is-spyware) (last visit: 12 December 2022).

وحتى نتقادی خطر هذه الأنواع من البرمجيات الضارة يجب الحرص على تثبيت برامج الحماية من الفيروسات وكذلك عدم تثبيت أي برامج غير موثوقة وكذلك تجنب الضغط على هذه الإعلانات المنتبقة عند زيارة أي متصفح حتى لا يتم انتهاك خصوصية المستخدم وكذلك من الممكن اللجوء لبعض الشركات المختصة حتى يتم إزالة هذه البرمجيات.

سابعا :الشركات المزودة لخدمة الإنترنت

إن مزود خدمة الإنترنت يقوم بتسجيل المعلومات التي لها علاقة بالحساب الشخصي مثل عنوان البروتوكول (IP Address) الخاص بالإنترنت، و التاريخ والوقت عند تسجيل الدخول أو الخروج من الحساب، وعنوان جهاز التوجيه (Media Access Control -MAC) وكمية البيانات، التي قام بتنزيلها، أو تحميلها، والقيام بالاحتفاظ بمعلومات حول عدد الزيارات، مثل العناوين التي زارها أو الأماكن التي تصفحها (Uniform Resource Locator – URL) . كما إن الشركات التي تقدم الخدمات للهواتف المحمولة لاتسجل فقط المكالمات والرسائل ، بل أيضا تحدد الموقع عن طريق تحديد موقع نقاط التقاط الإشارة ، وفي الولايات المتحدة الأمريكية قامت إحدى الشركات باستخدام الكوكيز الفائقة أو ماتسمى بملفات التعريف الفائقة⁷⁶ ، فلا تسجل فقط بيانات التصفح مثل الكوكيز المعروفة، ولكنها غير قابلة للمسح من خلال اختيار مسح الكوكيز بالمتصفح ، حيث تقوم الشركة التي توفر الخدمة بدمجها في رأس (http) لنقل النص الفائق⁷⁷.

⁷⁶ ملف تعريف الارتباط الفائق هو نوع من ملفات تعريف الارتباط للتعقب يتم إدخالها في رأس HTTP بواسطة مزود خدمة الإنترنت (ISP) لجمع البيانات حول محفوظات وعادات تصفح الإنترنت للمستخدم. يُعرف أيضًا باسم رأس المعرف الفريد ، وهو ملف تعريف ارتباط فائق ليس من الناحية الفنية ملف تعريف ارتباط HTTP ، ولكنه معلومات يتم حقنها في الحزم المرسل من جهاز المستخدم والخدمة التي يتصل بها. عندما يكتشف مزود خدمة الإنترنت (ISP) حركة مرور HTTP للمستخدم ، فإنه يُدرج رأس HTTP إضافيًا في الحزم بعد مغادرته لجهاز كمبيوتر المستخدم. ينظر في: [What is supercookie? - Definition from WhatIs.com \(techtarget.com\)](http://WhatIs.com/techtarget.com/WhatIsSuperCookie)

⁷⁷ Privacy and Information Technology, Stanford Encyclopedia of philosophy, published Thu Nov 20, 2014 [Privacy and Information Technology \(Stanford Encyclopedia of Philosophy/Summer 2020 Edition\)](http://PrivacyandInformationTechnology(StanfordEncyclopediaofPhilosophy/Summer2020Edition))

المبحث الثاني

أحكام معالجة البيانات الشخصية في عالم المعلوماتية

مع التطور التكنولوجي للمعلومات والاتصالات وظهور تكنولوجيا إنترنت الأشياء والحوسبة السحابية والذكاء الاصطناعي ازداد حجم جمع المعلومات وتبادلها ومعالجتها إلكترونياً، مما سمح للشركات والمؤسسات العامة والخاصة باستخدام البيانات الشخصية للأفراد، حيث قدمت هذه البيانات ميزة تنافسية للشركات إذ تقوم بتحليلها والاستفادة منها اقتصادياً وتجارياً . وبناء على ذلك قامت العديد من الشركات العالمية والدول المتقدمة بوضع خطط مستقبلية وبناء مراكز بيانات متخصصة (Data Centers) للاستفادة من تلك البيانات، مثل مشروع وكالة الأمن القومي (NSA) لتطوير قاعدة بيانات وطنية أطلق عليه مشروع (Utah Data Center) ، وهو يهدف إلى تحليل بيانات مستخدمي شبكات الإنترنت والاتصالات في العالم لفهم سلوكياتهم ونشاطاتهم. كما لا يقتصر تأثير البيانات على الشركات الضخمة أو الشركات التقنية، بل هناك مجموعة من القطاعات التقليدية والحكومات، وشركات خدمة المستهلكين وشركات التوريد والتصنيع التي تستفاد من مخرجات تحليل هذه البيانات. ومن ذلك الاستفادة منها في تطوير الخدمات الحكومية، حيث أصبح بإمكان المختصين تطوير الخدمات الحكومية عن طريق رصد ما مدى رضا المواطنين عن الخدمات الحكومية المقدّمة لهم، وعلى ضوء النتائج المحللة يمكن استنتاج ما يلزم عمله للتطوير والتحسين، كذلك ساهمت هذه البيانات في زيادة أرباح الشركات وفي تقديم خدمات أفضل للزبائن، و أُناحت هذه البيانات الفرصة لمؤسسات الأعمال في زيادة أرباحها بشكل كبير وتعزيز وضعها التنافسي. وذلك عن طريق توجيه الإعلانات الترويجية لمستخدمي المواقع الإلكترونية. فعلى سبيل المثال خدمة قوغل «AdSense» ، تعمل على تحليل رغبات المستخدم من خلال المدخلات التي يقوم بإدخالها سابقاً في محركات البحث، فتقوم تلك المواقع برصد الكلمات وتخزينها في قواعد بيانات خاصة، ليتم تحليلها وتوجيه الدعايات التي تتناسب مع هذه الاهتمامات والرغبات، بصرف النظر عن الموقع الذي تتم زيارته. ومن الأمثلة أيضاً، قيام شركات البيع بالتجزئة باستغلال تلك المعلومات بحيث تصبح قادرة على اكتشاف الأيام التي يتوافد المستهلكون فيها إلى المحلات التجارية، وتحلل كيفية إنفاق الناس على البضائع، وذلك بهدف زيادة الربحية واتباع الطرق الأمثل للتسويق المستهدف (Targeted Marketing) ، فأصبحت بذلك البيانات الشخصية نتيجة التطور الحالي هي الأساس في الدعاية والتسويق لما لها من قيمة مادية ومصدراً للربح. حيث تتم معالجة هذه البيانات ويستفاد منها دون علم أصحابها ، الأمر الذي شكل اعتداءً على خصوصية البيانات الشخصية، وهو ما دفع المشرعين في مختلف البلدان للتدخل ووضع تنظيم قانوني لمعالجة البيانات الشخصية.

ووفقاً لذلك، سوف نتناول أحكام معالجة البيانات الشخصية في قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018 ونقارنه بما نص عليه النظام الأوروبي العام (GDPR) فيما يتعلق بمعالجة البيانات ونقسم هذا المبحث إلى مطلبين :

المطلب الأول : تعريف معالجة البيانات والمبادئ المرتبطة بها.

المطلب الثاني : شروط مشروعية معالجة البيانات الشخصية.

المطلب الأول

تعريف معالجة البيانات والمبادئ المرتبطة بها

يتطلب الخوض في موضوع معالجة البيانات الفهم الصحيح لبعض المصطلحات، ولا سيما أنها مصطلحات تقنية أكثر منها قانونية، ولعل أبرزها مصطلح المعالجة. كما يتطلب أيضاً إيضاح المبادئ التي يتعين على المسؤول عن المعالجة الالتزام بها، وذلك ضماناً لسلامة عملية المعالجة ومنها مشروعية المعالجة، وشفافيتها، وأمانتها، ونزاهتها، وضرورتها. وانطلاقاً من هذه الأهمية وحرصاً على سلامة عملية المعالجة أقرت القوانين الخاصة بحماية البيانات الشخصية ومنها قانون حماية البيانات الشخصية البحريني والنظام الأوروبي العام لحماية البيانات الشخصية (GDPR) عدداً من المبادئ التي يفترض بالمسؤول عن المعالجة احترامها، كي لا ينتج عنها أي إساءة إلى أصحاب البيانات، أهمها مبدأ الشفافية، وتوفير الإعلام الكافي عن عملية المعالجة، إضافة إلى ضرورة إتاحة الفرصة لصاحب البيانات كي يتمكن من ممارسة حقوقه. إلا أن الأحكام الخاصة بالمبادئ والموجبات تداخلت، واختلف تنظيمها بين تشريع وآخر، وهذا ما سوف نتناوله في الفرعين التاليين:

الفرع الأول: تعريف المعالجة والمصطلحات المرتبطة بها

الفرع الثاني: المبادئ المرتبطة بالمعالجة

الفرع الأول: تعريف المعالجة والمصطلحات المرتبطة بها والقائمون بالمعالجة

سوف نتناول في هذا الفرع الآتي:

أولاً: تعريف المعالجة

ثانياً: المصطلحات الأخرى المرتبطة بالمعالجة

ثالثاً: القائمون على عمليات المعالجة

أولاً: تعريف المعالجة

وضع المشرع البحريني تعريفاً لمعالجة البيانات الشخصية في المادة الأولى من قانون حماية البيانات الشخصية رقم 30 لسنة 2018، حيث عرف المعالجة بأنها "أية عملية أو مجموعة عمليات يتم إجراؤها على بيانات شخصية بوسيلة آلية أو غير آلية، ومن ذلك جمع تلك البيانات أو تسجيلها أو تنظيمها أو تصنيفها في مجموعات أو تخزينها، أو تحويلها أو تعديلها، أو استعادتها أو استخدامها أو الإفصاح عنها، من خلال بثّها أو نشرها أو نقلها أو إتاحتها للغير، أو دمجها أو حجبها أو مسحها أو تدميرها".

وقد عرف المشرع السعودي المعالجة في نظام حماية البيانات الشخصية في المادة (1) منه بأنها تعني "أي عملية تجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر، والمشاركة في البيانات أو الربط البيني، والحجب، والمسح، والإتلاف"⁷⁸.

ومن ناحية أخرى عرف النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) رقم 2016/679، المعالجة في المادة (4) الفقرة (2) منه على أنها "أي عملية أو مجموعة من العمليات التي يتم إجراؤها على البيانات الشخصية أو على مجموعات من البيانات الشخصية، سواء بوسائل آلية أم لا، مثل الجمع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو التحويل أو

⁷⁸ نظام حماية البيانات الشخصية السعودي 1443 هـ، الصادر بموجب مرسوم ملكي رقم (م/19) يرجى الاطلاع على [تفاصيل النظام](#)

التغيير أو الاسترداد، أو الاستخدام أو الإفصاح عن طريق الإرسال أو النشر أو الإتاحة أو التنسيق أو الدمج أو التقييد أو المسح أو التدمير⁷⁹.

ونجد من خلال التعريفات السابقة أن المشرع البحريني والسعودي والأوروبي توسعوا في تعريف معالجة البيانات الشخصية ، كما أشارت التعريفات السابقة لمجموعة من الإجراءات المتعلقة بمعالجة البيانات الشخصية، ويظهر من صياغتها إن ما ذكره المشرعون لم يكن على سبيل الحصر وإنما على سبيل المثال، ويمكن استنتاج ذلك لأن المشرعين البحريني والسعودي قد استخدموا في التعريف عبارة (ومن ذلك) عتد تعريفهما المعالجة بأنها " أية عملية أو مجموعة عمليات يتم إجراؤها على بيانات شخصية بوسيلة آلية أو غير آلية.... الخ⁸⁰.

أما النظام الأوروبي العام لحماية البيانات الشخصية فقد كان أكثر وضوحاً من خلال استعماله لكلمة (مثل) التي تدل بشكل قاطع على أن ماورد ذكره من صور لعمليات المعالجة إنما جاء على سبيل المثال ، وذلك عندما عرف المعالجة على أنها " أي عملية أو مجموعة من العمليات التي يتم إجراؤها على البيانات الشخصية أو على مجموعات من البيانات الشخصية، سواء بوسائل آلية أم لا، مثل الجمع أو التسجيل أو التنظيم أو الهيكلة... الخ.

ويمكن القول إن المعالجة هي السبب الرئيسي في ظهور الحماية القانونية للبيانات طال شخصية بحسب النظام الأوروبي العام (GDPR) وبأقي التشريعات المقارنة التي جعلت منها محلاً للحماية، على اعتبار أن البيانات الشخصية ليست عرضة للخطر مادامت لا تتم معالجتها.

⁷⁹ Art 4 GBDR definition : " 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

⁸⁰ سامح عبدالواحد التهامي، ضوابط معالجة البيانات الشخصية: دراسة مقارنة بين القانون الفرنسي والكويتي، مجلة كلية القانون الكويتية العالمية، العدد 1، الكويت ، 2021، ص 404.

ثانيًا: المصطلحات الأخرى المرتبطة بالمعالجة

هناك بعض المصطلحات التي قد تختلط بمفهوم معالجة البيانات، وهي التتميط والتسمية المستعارة وهذه المفاهيم لم يتطرق إليها المشرع البحريني في قانون حماية البيانات الشخصية على عكس نظيره الأوروبي، حيث عرف التتميط (Profiling) تعريفاً خاصاً ويعني به بحسب ما جاء في المادة (4) من الفقرة (4) من النظام أنه "أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتكون من استخدام البيانات الشخصية لتقييم جوانب شخصية معينة تتعلق بشخص طبيعي، وبخاصة لتحليل أو توقع الجوانب المتعلقة بأداء هذا الشخص الطبيعي في العمل والوضع الاقتصادي والصحة والشخصية، أو التفضيلات أو الاهتمامات أو الموثوقية أو السلوك أو الموقع أو الحركات"⁸¹.

كذلك عرف المشرع البحريني مصطلح (منظومة ملفات) في المادة الأولى من قانون حماية البيانات الشخصية على نحو مقارب لتعريف النظام الأوروبي، فنص على أنه يقصد بـ (منظومة ملفات) " أية مجموعة بيانات شخصية لا تعالج بواسطة جهاز يعمل آلياً بناءً على تعليمات تُعطى له ولكنها مرتبة على نحو يتيح الحصول منها على معلومات عن الأفراد الذين تحضهم هذه البيانات"

وفي المقابل عرف النظام الأوروبي العام نظام الملفات (Filing system) في الفقرة السادسة من المادة (4) منه على أنه "مجموعة منظمة من البيانات الشخصية التي يمكن الوصول إليها وفقاً لمعايير محددة، سواء مركزية أو غير مركزية أو على أساس وظيفي أو جغرافي"⁸².

ويجدر القول أنه وإن كانت عمليات التتميط غير مجرمة في حد ذاتها، فإنه يجب أن تتبع الضوابط التي تضعها التشريعات لمعالجة البيانات، وللدلالة على أهمية اتباع الضوابط التي تضعها التشريعات فيما يتعلق بنظام الإيداع والتتميط نجد أن شركة H&M (Hennes & Mauritz) لم تلتزم باتباع الإجراءات القانونية اللازمة عند إجراء عمليات المعالجة وتحديد التتميط، ما كلفها

⁸¹ Art. 4 GDPR *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 analyze or predict aspects concerning";

⁸² Art.4 GDPR "'filing system' "means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis".

مبالغ طائلة مؤخراً في أكتوبر من عام 2020 حيث فرض مفوض هامبورج لحماية البيانات الشخصية وحرية المعلومات غرامة قدرها 35.3 مليون يورو على الشركة بسبب انتهاكاتها للبيانات الشخصية لموظفيها، حيث جمعت الشركة واحتفظت بتسجيلات لموظفيها تحتوي على بيانات على مستوى عال من الخصوصية لفترات زمنية طويلة. كما تم استخدام تلك البيانات في تقييم أداء العاملين وعمل ملفات تعريفية مفصلة لهم تستخدم وتؤثر في اتخاذ قرارات تجاههم. والجدير بالذكر إن الموظفين لم تكن لديهم أدنى فكرة عن ذلك إلا حين حدث خطأ فني في أنظمة حواسيب الشركة، ما جعل هذه البيانات متاحة عدة ساعات في أكتوبر من العام الماضي (2021)⁸³.

ومن ناحية أخرى فقد عالج النظام الأوروبي العام ما يسمى بالبيانات المستعارة أو التسمية المستعارة للبيانات في المادة (4) الفقرة (5) منه، وأخرجها من نطاق الحماية المقررة في النظام كونها لا تؤدي إلى التعريف بصاحب البيانات، وعرفها على أنها: "معالجة البيانات الشخصية بطريقة لا يمكن بعدها ربط البيانات الشخصية بشخص محدد هو موضوع تلك البيانات من دون استخدام معلومات إضافية، شريطة الاحتفاظ بهذه المعلومات الإضافية بشكل منفصل، وأن تكون تلك البيانات الإضافية خاضعة لتدابير تقنية وتنظيمية لضمان عدم انتسابها إلى شخص طبيعي معرف أو قابل للتعريف"⁸⁴.

ونلاحظ مما سبق وجود بعض الاختلافات بين تعريفات المعالجة، الأمر الذي يستوجب توضيح معنى مصطلح المعالجة من خلال تناول بعضاً من الأحكام القضائية الصادرة عن محكمة العدل الأوروبية التي تناولت المقصود بالمعالجة وموقف التشريعات العربية منها، وذلك بغية توضيح مدلول هذا المصطلح ونطاقه.

تطرقت محكمة العدل الأوروبية في العديد من أحكامها لتفسير مصطلح المعالجة وحددت الأعمال التي تعد من قبيل معالجة البيانات الشخصية، وجاء أول توضيح من المحكمة لتعريف المعالجة عام 2008 في قضية (Lindqvist) حين أوضحت المحكمة إن مفهوم معالجة البيانات يشمل العمليات الآلية وغير الآلية التي يكون محلها البيانات الشخصية للأفراد، وإن نشر

⁸³ Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre; [Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre | European Data Protection Board \(europa.eu\)](https://european-data-protection-board.europa.eu/en/hamburg-commissioner-fines-h&m-35.3-million-euro-for-data-protection-violations-in-service-centre) (Last visit: 28 April 2022).

⁸⁴ Art4 GBDR 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

هذه البيانات على صفحة الإنترنت يعد انتهاكا للحق في الخصوصية و لقانون حماية البيانات الشخصية. وتتمثل وقائع القضية في أن السيدة (Lindqvist) كانت تقوم بعمل تطوعي كمعلمة في السويد ، وذلك إلى جانب مهنتها الأساسية، ولتمكين الطلاب في الحصول على المعلومات بشكل أكثر سهولة قامت بإنشاء صفحة رئيسية على الأنترنت تحتوي على معلومات حول نفسها وزوجها وبيانات عن زملائها مثل هوياتهم ووظائفهم وفي بعض المرات يتم توضيح الظروف الأسرية، وكانت الصفحة يمكن الوصول إليها من قبل الكنيسة السويدية التي تم تعيين ارتباط بها بناء على طلب السيدة (Lundqvist)، فقامت بمعالجة بيانات زملائها بدون الحصول على موافقتهم على معالجة البيانات، وعند معرفتها بعدم رضا زملائها بخصوص معالجة بياناتهم قامت بإلغاء الصفحة الرئيسية، إلا أنها وعلى الرغم من ذلك حوكت على اعتبار أنها عالجت البيانات بوسائل تلقائية دون تقديم إخطار كتابي مسبق، وقبلت السيدة (Lindqvist) بالحقائق التي أدعى المدعي العام بصحتها، كما استئنفت السيدة في وقت لاحق ، لكن المحكمة التي تنظر القضية رفضت هذا الاستئناف⁸⁵.

وجدير بالملاحظة أن المحكمة الأوروبية رفضت في حكمها الصادر عام 2014 اعتبار التحليل القانوني الذي تقوم به جهة ما للرد على طلب تقدم به صاحب البيانات لها من قبيل المعالجة للبيانات الشخصية، و أوضحت في حكم سابق إن تسليم البيانات الشخصية الذي يتم استجابة لطلب حصول على تلك البيانات يعد من قبيل أعمال المعالجة⁸⁶. وكان هذا الحكم بشأن موظف في هولندا قام بتقديم طلب تصريح إقامة موظف إلى المسؤول في دائرة الهجرة والتجنيس الهولندية وتطلب الأمر إصدار مستند داخلي ليكون بمثابة مشروع قرار للمراجعة أو مذكرة تفسيرية لتبرير القرار. و يحتوي هذا بشكل عام على معلومات حول مسؤول الدائرة والبيانات الشخصية لمقدم الطلب والأحكام القانونية المعمول بها والتحليل القانوني. ثم قام الموظف بطلب نسخة من المحضر الذي أعقب رفض طلبه للحصول على تصريح إقامة بموجب قانون اللجوء ، وتم تزويده بملخص للبيانات الشخصية الواردة في الوثائق ، وأصل البيانات وتفاصيل الهيئات التي حصلت عليها البيانات تم الكشف عنها. ولكن الموظف قام بالطعن في رفض الوزير الكشف عن نسخة من المحضر في المحاكم الهولندية، التي أحالت خمسة أسئلة إلى محكمة العدل للاتحاد الأوروبي الأسئلة المشار إليها كمرجع أولي تتعلق بنطاق وتفسير ``البيانات الشخصية " بموجب المادة 2

⁸⁵ ECR, Case C-01/101, 6th November 2003, Bodil Lindqvist v. Göta hovrätt (Sweden)

ويمكن الاطلاع على تفاصيل الحكم باللغة الإنجليزية من خلال الموقع الرسمي لمحكمة العدل الأوروبية:
<https://gdprhub.eu/index.php?title=CJEU - C-101/01 - Bodil Lindqvist>

⁸⁶ C-28/08, Commission V. Bavarian Lager CO., 29.6.2010 ("BAVARIAN LAGER").

(أ) من التوجيه الأوروبي، لا سيما ما إذا كان التحليل القانوني يشكل بيانات شخصية ، وما إذا كان رفض تقديم نسخة من المحضر ينتهك حق المتقدمين في الوصول إلى البيانات الشخصية⁸⁷.

ثالثاً: القائمون على عمليات المعالجة

تضمن قانون حماية البيانات الشخصية البحريني والنظام الأوروبي العام لحماية البيانات الشخصية تعريفات لكل من مدير البيانات ومعالج البيانات ومراقب حماية البيانات والطرف الثالث (الغير) الذين يتولون مهام معالجة البيانات الشخصية. حيث عرف المشرع البحريني مدير البيانات في المادة الأولى من قانون حماية البيانات الشخصية بأنه "الشخص الذي يقرر، بمفرده أو بالاشتراك مع الآخرين، أغراض ووسائل معالجة بيانات شخصية معينة. وفي الحالات التي تكون فيها هذه الأغراض والوسائل مقررة بموجب القانون يُعد مديراً للبيانات الشخص المنوط به الالتزام بالقيام بالمعالجة"⁸⁸.

أما النظام الأوروبي العام لحماية البيانات الشخصية فاستبدل مصطلح مدير البيانات بمصطلح المتحكم (controller) وعرفه بأنه "يعني الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي هيئة أخرى تحدد، بمفردها أو بالاشتراك مع آخرين، أغراض ووسائل معالجة البيانات الشخصية، وعندما يتم تحديد أغراض ووسائل مثل هذه المعالجة بموجب قانون الاتحاد أو الدول الأعضاء، يجوز تحديد المتحكم أو المعايير المعتمدة لتحديده وفقاً لقانون الاتحاد أو قانون الدول الأعضاء"⁸⁹.

ومن خلال التعريفين السابقين نجد أن المشرع البحريني اتبع نهج المشرع الأوروبي في تحديد المقصود بالمتحكم، حيث يعد المتحكم هو صاحب القرار الرئيسي، وتكون له السيطرة على عملية جمع البيانات وعلى وسائل وطرائق معالجتها. وفي حالة وجود أكثر من متحكم بالبيانات يكونون متضامنين في المسؤوليات والالتزامات القانونية، ويتشاركون في الهدف من جمع البيانات

⁸⁷ Joined Cases C-141/12 AND c372/12 YS v. Minister Voor Immigratie Integratie en Asiel and Minister Voor Immigratie, Integre en Asiel V. M, S (2014).

للاطلاع على تفاصيل الحكم باللغة الإنجليزية يمكن زيارة الموقع الرسمي لمحكمة العدل الأوروبية:

<https://curia.europa.eu/juris/document/document.jsf?docid=155114&doclang=EN>

⁸⁸ قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018

⁸⁹ Art 4 GBDR '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;

والتحكم بها. وفي هذا الصدد أشار النظام الأوروبي العام لحماية البيانات الشخصية في المادة (26) منه إلى مسألة التحكم المشترك (Joint controllers) حيث نص على أنه "عندما يقوم اثنان أو أكثر من المتحكمين بشكل مشترك بتحديد أغراض ووسائل المعالجة، يجب أن يكونا متحكمين مشتركين، وتحدد بطريقة شفافة مسؤوليات كل منهما عن الامتثال للالتزامات بموجب هذا النظام، وخاصة فيما يتعلق بممارسة حقوق صاحب البيانات وواجبات كل منهما في تقديم المعلومات المشار إليها في المادتين (13،14)، عن طريق الوسائل والتنظيم بينهما ما لم يتم تحديد مسؤوليات كل متحكم بموجب قانون الاتحاد أو قانون الدول الأعضاء الذي يخضع له المتحكمون، ويتم كذلك تخصيص نقطة اتصال للوصول إلى المتحكم بدلا من وضع هذا العبء على الشخص المعني بالبيانات"⁹⁰.

كما يبدو أيضًا أن المشرع البحريني قد سبق أن أشار إلى مسألة التحكم المشترك في المادة (1) من قانون حماية البيانات الشخصية، لكنه لم يشر إلى الشروط الخاصة بالتحكم المشترك، ولم ينص على إمكانية تعيين نقطة اتصال لتسهيل الوصول إلى المتحكم بدلا من وضع هذا العبء على الشخص المعني بالبيانات، وهذا على خلاف النظام العام الأوروبي لحماية البيانات الشخصية الذي تعرض بإيجاز لوجوب تحديد المسؤولية بين المتحكمين المشتركين.

وحتى نحدد معيار وجود تحكم مشترك في تشارك كيانيين أو أكثر في تحديد أغراض ووسائل عملية المعالجة، فإن التحكم المشترك من الممكن أن يكون في شكل قرار مشترك يتخذه كيانات أو أكثر، أو ينتج عن قرارات متقاربة من قبل كيانيين أو أكثر، لكي تكون القرارات مكتملة لبعضها البعض وتكون ضرورية للمعالجة، بحيث يكون لها تأثير على تحديد أغراض ووسائل المعالجة. إضافة إلى ضرورة مشاركة كلا الطرفين في المعالجة، وأن تشمل عملية التحكم المشترك على تحديد الأغراض من جهة وتحديد الوسائل من جهة أخرى⁹¹.

ونخلص مما سبق إلى أن المتحكم في البيانات أو من يسمى مدير البيانات هو الشخص الذي يحصل على البيانات وفقًا لطبيعة عمله، ويحق له تحديد طريقته وأسلوب الاحتفاظ بها ومعالجتها، على أن يكون ذلك في حدود الغرض المعلن والمحدد، الأمر الذي يحدده أيضًا المتحكم سواءً أكان متحكمًا واحدًا أم أكثر من متحكم مجتمعين.

90 Chapter 4 Art 26: "1. where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them..."

91 Guidelines 07/2020 on the concepts of controller and processor in the GDPR European Data Protection Board Report (2020).

كما أن هناك طرفاً آخر لمعالجة البيانات وهو معالج البيانات، حيث عرفه المشرع البحريني في قانون حماية البيانات الشخصية "بأنه الشخص الذي يتولى معالجة البيانات لحساب مدير البيانات ونياية عنه، ولا يشمل ذلك كل من يعمل لدى مدير البيانات أو معالج البيانات"⁹².

وهذا على غرار ما جاء في النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) حيث عرف المعالج في المادة (4) الفقرة (8) على أنه "الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي هيئة أخرى تقوم بمعالجة البيانات الشخصية نيابة عن المتحكم"⁹³.

ومن خلال ما تقدم يتضح أنه يوجد قدر من الاختلاف الجزئي بين تعريف القانون البحريني وتعريف النظام الأوروبي العام لحماية البيانات الشخصية بشأن المعالج، حيث يجيز القانون البحريني للمعالج أن يقوم بعملية المعالجة لصالحه ولصالح المتحكم، بينما يحصره تعريف النظام الأوروبي العام لحماية البيانات الشخصية في قيامه بالمعالجة نيابة عن المتحكم. ما يعني بمفهوم المخالفة قيام مسؤولية المعالج في حال قيامه بعملية المعالجة لصالحه، وليس بناءً على تعليمات المتحكم.

وبشكل عام، نجد أن القانون البحريني والنظام الأوروبي العام لحماية البيانات الشخصية كلاهما يتفقان على أن علاقة المتحكم أو مدير البيانات والمعالج تحدد من خلال تحديد من تكون له سلطة اتخاذ قرار تحديد غرض وطريقة المعالجة فيما يتعلق بمعالجة البيانات الشخصية. وبناءً على ذلك يجب على المعالج ألا يقوم بمعالجة البيانات خلافاً لتعليمات المتحكم أو مدير البيانات، وللمتحكم السلطة المطلقة في تحديد أغراض المعالجة، الأمر الذي يساعد المعالج في اختيار أنسب الوسائل التقنية والتنظيمية لخدمة الغرض الأساسي الذي يتم تجميع البيانات من أجله.

ويظهر الفرق بين المعالج والمتحكم أو من يسمى مدير البيانات عند التعامل مع بيانات العملاء من أجل تقديم الخدمات المصرفية، فعلى سبيل المثال نجد أن شركة بنفث في مملكة البحرين التي تقدم خدمة مصرفية بمقتضى العقد الذي بينها وبين العميل تعد في هذه الحالة متحركة بالبيانات، بينما نجد أن معالجة البيانات الائتمانية لا تتم من قبل نفس الشركة وإنما عن طريق مركز البحرين للمعلومات الائتمانية الذي تتعاقد معه شركة بنفث كمعالج من الباطن، ويعد في هذه الحالة معالجاً للبيانات فقط دون أن يكون متحكماً بها⁹⁴.

⁹² المادة 1 من قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018

⁹³ Art 4 GDPR 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"

⁹⁴ للمزيد من المعلومات الرجاء الاطلاع على الرابط الآتي : <https://benefit.bh/ar/personal/bcbr> المتعاقد من الباطن، هو من يقوم بتنفيذ تعليمات المسؤول عن المعالجة، أقله ما يتعلق منها، بتحديد أهداف المعالجة، والعناصر الأساسية ووسائلها. علماً أن القانون يترك لهذا المتعاقد بعض الحرية في اختيار الوسائل الأنسب، باعتباره مفوضاً، ويعمل لخدمة مصلحة شخص ثالث هو من فوضه، وعليه أن يؤدي هذه الخدمة دون أن يتجاوز حدود التفويض الممنوح له حتى لا يصبح نشاطه غير قانوني.

وقد يكون للغير أو من يعد طرفاً ثالثاً دور في عملية معالجة البيانات، والغير هو من ليس طرفاً في العقد أو خلفاً عاماً أو خاصاً لأحد المتعاقدين⁹⁵، وقد حدد النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) المقصود بالغير أو ما أطلق عليه مسمى "الطرف الثالث" في المادة (1) فقرة (10) وعرفه بأنه "يعني شخصاً طبيعياً أو اعتبارياً أو سلطة عامة أو وكالة أو هيئة أخرى غير موضوع البيانات أو المتحكم أو المعالج أو الأشخاص المخولين، تحت السلطة المباشرة للمتحكم أو المعالج، بمعالجة البيانات الشخصية"⁹⁶. وعليه، لا يعد "الشخص المعني" و "المسؤول عن المعالجة" و "المتعاقدين من الباطن"، أو من يعمل لحسابهما، من الغير، فموظفو وكالة السفر التي تعالج البيانات الشخصية لزبائنهم ليسوا جهة ثالثة، بينما يعتبر العاملون لمؤسسة أخرى كذلك، وإن كانت هذه الأخيرة مملوكة للمجموعة نفسها، صاحبة وكالة السفر.

وأما بالنسبة للقوانين العربية فلم يتطرق المشرع السعودي ولا الإماراتي إلى تحديد من هم الأغيار في نظام حماية البيانات الشخصية، وذلك على عكس المشرع البحريني في قانون حماية البيانات الشخصية رقم 30 لسنة 2018، حيث استخدم على غرار المشرع الأوروبي مصطلح الطرف الثالث في المادة الأولى من القانون، ونص على أنه "أي شخص خلافاً لأي مما يأتي:

- صاحب البيانات.
- مدير البيانات.
- معالج البيانات.
- مراقب حماية البيانات.
- أي شخص يعمل تحت إشراف مدير البيانات أو معالج البيانات ومصرح له بمعالجة البيانات لحساب مدير البيانات أو معالج البيانات".

رابعاً: أشكال المعالجة

إن تجميع البيانات الأولية من مصادرها، وتنظيمها في جداول البيانات، يجعلان من السهل إجراء العمليات اللازمة على هذه البيانات للحصول على المعلومات المطلوبة، وهذه العمليات قد تكون عمليات حسابية للأرقام، أو عمليات ترتيب تسلسل تصاعدي أو تنازلي طبقاً لرغبة المستخدم

95 يقصد بالغير هنا كل شخص أجنبي عن العقد أي كل من لم يوجد في العقد بنفسه أو بواسطة من يمثله ومن لا يعتبر من الخلف الخاص أو من الخلف العام . راجع : عبد الرزاق السنهوري ، نظرية العقد ، مرجع سابق ، ص554.

96 ART4 GBDR 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

أو المستفيد. أو عمليات تصنيف عن طريق تقسيم البيانات في مجموعة متماثلة طبقاً لخواص مشتركة، لها معنى محدد للمستفيد، مثل تصنيف الموظفين ذكوراً وإناثاً، ويدخل كل ما سبق ضمن مفهوم معالجة البيانات، وطبقاً لحجم البيانات المتوافرة وتنظيمها فإنه يمكن معالجتها والحصول على المعلومات التي يمكن الاعتماد عليها في اتخاذ القرارات⁹⁷.

ويعكس تعداد العمليات وذكرها على سبيل المثال لا الحصر رغبة المشرع في توسيع مفهوم المعالجة لتشمل الصور التي يمكن أن تظهر مستقبلاً بفضل التقنيات المتجددة في عصر الثورة التقنية اليوم، وذلك لضمان الحماية ضد أي فعل أو عملية قد تمس الحريات الشخصية تحت حجة غياب النص القانوني. وقد سارع المشرع الأوروبي على النهج ذاته من خلال التعريف الذي جاء به النظام الأوروبي الجديد، حيث فتح المجال أمام عمليات جديدة لم تنص عليها لائحة حماية البيانات الشخصية الأوروبية لسنة 1995، وتركها أيضاً على سبيل المثال في انتظار ظهور أشكال جديدة في زمن تكنولوجي رقمي يتجدد ويتطور بسرعة وباستمرار⁹⁸.

الفرع الثاني: المبادئ المرتبطة بالمعالجة

إن المبادئ التي ترتبط بالمعالجة المنصوص عليها في القوانين المعنية بحماية البيانات الشخصية تشكل المصدر الأساس لحقوق الشخص المعني وموجبات المعالج، وكل من هو معني بالوصول إليها، أو بعملية المعالجة. كما أن قوانين الحماية تركز بشكل أساسي على احترام مبادئ حقوق الإنسان، وحماية الحق في الخصوصية، لذلك كان لا بد من أجل ضمان سلامة عملية المعالجة إقرار عدد من المبادئ التي تلزم المسؤول عن المعالجة، مثل مشروعية المعالجة، وشفافيتها، وأمانتها، ونزاهتها، وضرورتها. كما إن القوانين قد حظرت معالجة البيانات الشخصية بطريقة تمس بحقوق أصحابها، أو بحرياتهم الخاصة والعامة، أو تسيء إليهم، وتشهر بهم⁹⁹.

وقد تبين المشرع البحريني هذه المبادئ في قانون حماية البيانات الشخصية وذلك في المادة (3) منه تحت عنوان "الضوابط الخاصة بجودة البيانات"، وكذلك أوردها المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية في المادة (5) من الفصل الثاني تحت عنوان "المبادئ المتعلقة بمعالجة البيانات الشخصية".

⁹⁷ جوهري قوادري صامت، الضوابط القانونية لمعالجة البيانات الشخصية إلكترونياً، مجلة الدراسات القانونية المقارنة، المجلد 06، العدد 02، الجزائر، 2020، ص 470.

⁹⁸ حسن الحافظي، المرجع السابق، ص 39-42.

⁹⁹ منى أبو أشقر جبور و محمود جبور، مرجع سابق، ص 120-121.

وفيما يلي سوف نتناول هذه المبادئ ومواقف القوانين منها تباعاً:

أولاً : مبدأ مشروعية ونزاهة المعالجة

يشترط عند معالجة البيانات الشخصية أن تتم بطريقة نزيهة ومشروعة (lawfulness) and (fairness) ويقصد بالمشروعية أن تتم كل معالجة للبيانات الشخصية وفقاً للمقتضيات القانونية¹⁰⁰، ويعني هذا لكي تكون معالجة البيانات الشخصية قانونية ، يجب تحديد أسباب محددة للمعالجة ("الأساس القانوني") وفي حال لم يتم تطبيق أي أساس قانوني ، فإن المعالجة تكون غير قانونية وتنتهك هذا المبدأ. كما تعني الشرعية أيضاً أن المتحكمين والمعالجات لا يمكنهم فعل أي شيء بالبيانات الشخصية وهو أمر غير قانوني بمعنى أكثر عمومية. وهذا يشمل التزامات القانون الأساسي والقانون العام ، سواء كانت جنائية أو مدنية. إذا كانت المعالجة تنطوي على ارتكاب جريمة جنائية ، فمن الواضح أنها ستكون غير قانونية. ومع ذلك ، قد تكون المعالجة غير قانونية أيضاً إذا أدت إلى خرق لقوانين الخصوصية المعمول بها ، انتهاك لقانون حقوق التأليف والنشر ، خرق اتفاق تعاقدية واجب النفاذ ، أو خرق للتشريعات أو اللوائح الخاصة بالصناعة ، عندما تقوم الكيانات بمعالجة البيانات بشكل غير قانوني ، يمنح قانون حماية البيانات الأفراد الحق في محو تلك البيانات أو تقييد المعالجة¹⁰¹. إما فيما يتعلق بمصطلح النزاهة وهو مرادف لمصطلح الأنصاف الذي استخدمه المشرعان الأوروبي والبحريني فيعني عدم معالجة البيانات بطريقة ضارة بشكل غير مناسب أو غير متوقعة أو مضللة للأفراد المعنيين¹⁰². و من أفضل الطرق لتحديد ما إذا كان يتم انتهاك مبدأ النزاهة هو البحث عن ضرر يلحق بفرد أو مجموعة من الأفراد. يجب الحذر بشكل خاص عند جمع المعلومات الشخصية التي تتعلق بفئة محمية مثل العرق أو الجنس. على سبيل المثال ، عند نقوم بتشغيل خدمة تجميع السيرة الذاتية وجمع الموافقة من المستخدمين للحصول على جنسهم كجزء من استكمال ملفهم الشخصي. تقدم امرأة موضوع البيانات الحق في الاعتراض على الطلب بعدم منحها مقابلة لوظيفة شعرت أنها مؤهلة لها ، وقد تقرر أن الخوارزمية التي تستخدمها خدمة التجميع الخاصة بنا لمطابقة المتقدمين بأصحاب العمل متحيزة ضد النساء عن غير قصد. إن وجود ضرر لمجموعة من الأفراد من شأنه أن ينتهك مبدأ النزاهة في جمع تلك البيانات. يمكن أيضاً تحديد أنه ليس عدلاً في التجميع في المعالجة إذا كنت قد قادت الفرد إلى

¹⁰⁰ و جدي صبرينه، حماية المعطيات الشخصية في قانون 7-18 تعزيز الثقة بالإدارة الإلكترونية وضمان لفعاليتها" مداخلة بالملتقي الوطني: النظام القانوني العام للمرفق العام الإلكتروني واقع- تحديات- آفاق، المسيلة، 6 نوفمبر 2018 النظام العام القانوني للمرفق العام الإلكتروني واقع - تحديات - آفاق (univ-msila.dz) (آخر زيارة 5-9-2022)

¹⁰¹ <https://medium.com/golden-data/what-does-lawfulness-fairness-and-transparency-mean-under-eu-dp-law-a385d249d754> (last visit: 5 April 2023).

¹⁰² <https://keepabl.com/news/7-principles-of-gdpr/> (last visit: 5 April 2023).

الاعتقاد بأن جنسه يتم جمعه لأغراض إعلامية فقط ولم يكن من المفترض أن يتم تغذيته كمعامل لخوارزمية مطابقة استئناف. حتى في حالة عدم وجود ضرر ، فإن هذا من شأنه أن ينتهك مبدأ النزاهة حيث تم استخدام أساليب خادعة لجمع المعلومات ، مما يخفي القصد الحقيقي لاستخدامها. و على الرغم من احتمال وجود ضرر ، إلا أن ذلك لا يشكل بالضرورة أساساً لانتهاك مبدأ النزاهة¹⁰³. لذلك فإن مبدأ النزاهة منطوي على تقدير معنوي وأخلاقي ويبقى خاضعاً لتقدير القضاء. وجاءت المادة (1/3) من القانون البحريني لحماية البيانات الشخصية مؤكدة بذلك على هذا المبدأ بنصها على "أنه يجب أن تكون معالجة البيانات منصفة ومشروعة". وهذا المبدأ يعني أنه يجب على الشركات أن تقوم بمعالجة البيانات الشخصية بشكل عادل ولأغراض مشروعة ونزيهة، ويجب استخدام المعلومات فقط في حدود القانون. ويمكن أن تشمل القوانين المعمول بها قوانين التوظيف أو مكافحة الاحتكار أو الصحة أو الضرائب. وحتى يكون هناك إنصاف يجب أن يكون مالكو البيانات على دراية بحقيقة أنه سيتم معالجة بياناتهم الشخصية، بما في ذلك كيفية جمع البيانات والاحتفاظ بها واستخدامها، للسماح لهم باتخاذ قراراتهم حول ما إذا كانوا يوافقون على هذه المعالجة وتمكينهم من ممارسة حقوق حماية البيانات الخاصة بهم.

كما أكد المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية في المادة (5) منه على وجوب أن تتم معالجة البيانات بشكل قانوني وعادل وشفاف فيما يتعلق بموضوع البيانات (الشرعية والإنصاف والشفافية)¹⁰⁴. ويقصد هنا بمصطلح الشفافية الذي نص عليه المشرع الأوروبي ، بأنه يجب توفير جميع المعلومات التي يتطلبها " النظام الأوروبي العام لحماية البيانات" لأصحاب البيانات الفردية حول ما تخطط للقيام به ببياناتهم الشخصية¹⁰⁵.

ولم يقتصر الأمر على ذلك فحسب ، وإنما تم التأكيد على أهمية الالتزام بمبدأ المشروعية والأنصاف والشفافية من خلال القرارات التنفيذية البحرينية بشأن حماية البيانات الشخصية ، حيث نجد أن المشرع البحريني نص في القرار رقم (43) لسنة 2022 بتحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية ونص في المادة (2) منه فيما يتعلق بالتدابير الفنية والتنظيمية الواجب تطبيقها عن المعالجة فإنه يجب عند القيام بمعالجة البيانات باتخاذ هذه التدابير إحاطة الموظفين المعنيين بهذه المعالجة . وكما نص في المادة (4) منه أنه في حال وقع خرق أو انتهاك للبيانات يجب على مدير البيانات أخبار صاحب البيانات

¹⁰⁴ Art. 5 GDPR Principles relating to processing of personal data

1. "Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

¹⁰⁵ <http://www-personal.umich.edu/~jdlitman/classes/cyber/cases/Lindqvist.pdf> (last visit:5 April 2023).

بذلك فيقوم بفتح قنوات اتصال للتواصل مع أصحاب البيانات لأبلاغهم بذلك . ولكن هناك حالات هو غير ملزم بأبلاغ أصحاب البيانات بحدوث هذا الخرق أو الانتهاك وذلك ، في حال كانت البيانات التي تم اختراقها غير مفهومة مشفرة ، أو في حال اتخذ المدير تدابير تضمن عدم احتمال ظهور مخاطر عالية على حقوق وحريات أصحاب البيانات، إذا كان إخطار صاحب البيانات يتطلب بذل جهد غير عادي ففي هذه الحالة يكون الإخطار بشكل علني لصاحب البيانات. كما نص في المادة (7) منه عند معالجة البيانات من قبل أكثر من مدير بيانات " يجب الإفصاح لأصحاب البيانات عن معالجة بياناتهم بصورة مشتركة من قبل أكثر من مدير بيانات لضمان وتعزيز الشفافية"¹⁰⁶.

وفي قرار رقم (45) لسنة 2022 بتحديد قواعد وإجراءات معالجة البيانات الشخصية الحساسة ، نص المشرع البحريني في المادة (2) منه بأنه تحظر معالجة البيانات الشخصية الحساسة إلا بعد الحصول على موافقة مسبقة من صاحب البيانات ، وأن كان المشرع البحريني قد استثنى بعض الحالات التي لاتستوجب الموافقة عليها لمعالجة هذا النوع من البيانات التي ذكرناها سابقاً وهي المادة (5) من قانون حماية البيانات الشخصية البحريني¹⁰⁷.

وكذلك نجد القرار رقم (51) لسنة 2022 بشأن شروط إنشاء سجلات البيانات الشخصية المتاح للجمهور الأطلاع عليها ، نص المشرع في المادة (1) منه على "إي سجل يتضمن بيانات شخصية متاح للجمهور الإطلاع عليه سواء بمقابل أو غير مقابل "، وكذلك في المادة (2) من القرار نص على "أنه يجب أخذ موافقة صاحب البيانات عند إدراج أي بيانات في السجلات وذلك بعد إحاطة صاحب البيانات بكافة المعلومات المتعلقة بإدراج البيانات والغرض من السجل، وفي حال الحصول على البيانات من إحدى الوسائل العلنية فيقتصر التزام مدير البيانات على إحاطة صاحب البيانات بإدراج بياناته في السجل وكذلك الغرض من أنشائه . وأية معلومات ضرورية ، ولايشترط الحصول على موافقة صاحب البيانات أو إخطاره قبل إدراج بياناته في السجل إذا كان إدراج تلك البيانات متعلقة بتنفيذ التزام قانوني أو أمر من المحكمة أو النيابة العامة أو تنفيذاً لعقد يكون صاحب البيانات طرفاً فيه"¹⁰⁸.

¹⁰⁶القرار الوزاري رقم (43) لسنة 2022 بتحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية ، الجريدة الرسمية ، العدد 3593 ، البحرين ، 2022 ، ص92-96

¹⁰⁷قرار رقم (45) لسنة 2022 بتحديد قواعد وإجراءات معالجة البيانات الشخصية الحساسة ، الجريدة الرسمية ، العدد 3593 ، البحرين، 2022، ص102.

¹⁰⁸قرار رقم (51) لسنة 2022 بشأن شروط إنشاء سجلات البيانات الشخصية المتاح للجمهور الأطلاع عليها ، الجريدة الرسمية ، العدد 3593، البحرين ، 2022، ص122.

ثانياً: مبدأ الغائية من جمع ومعالجة البيانات الشخصية

أكده كلا المشرعين البحريني والأوروبي على مبدأ الغائية، حيث نص المشرع البحريني في المادة (3) من قانون حماية البيانات الشخصية رقم 30 لسنة 2018 على أنه يجب أن يتم جمع المعلومات لغرض مشروع ومحدد وواضح، وألا تتم معالجتها لاحقاً، وألا يتم إجراء معالجة لاحقة لها على نحو لا يتوافق مع الغرض الذي جُمعت من أجله. إلا أن النظام الأوروبي العام لحماية البيانات الشخصية قد بين في المادة (5) منه إنه لا تعد معالجة غير متوافقة مع الغرض الذي جُمعت من أجله البيانات المعالجة اللاحقة لها التي تتم حصراً لأغراض تاريخية أو إحصائية أو للبحث العلمي، بشرط ألا تتم لدعم اتخاذ أي قرار أو إجراء بشأن فرد محدد¹⁰⁹.

ووفقاً لهذا يعد مبدأ الغاية من تجميع البيانات الشخصية ومعالجتها هو أحد محاور حماية البيانات الشخصية وتطبيقاً لفكرة الشفافية، ويتم التعبير عن هذه الغاية في القانون البحريني في أخذ موافقة صاحب البيانات مسبقاً وأيضاً القيام بإعلام الشخص الذي يتم تجميع بياناته عن كل ما يحدث لبياناته¹¹⁰. حيث نص قرار رقم (48) لسنة 2022 بشأن حقوق صاحب البيانات في المادة (4) منه " بأنه يلتزم مدير البيانات بالحصول على موافقة مكتوبة أو بوسائل إلكترونية على موافقة صريحة من صاحب البيانات قبل البدء في معالجة البيانات وذلك في الحالات التي يتم فيها الحصول على البيانات من صاحبها مباشرة". وكذلك نصت المادة (5) من ذات القرار على أنه " لا يعتد بموافقة صاحب البيانات إذا كانت جدران ملفات الارتباط (cookies wall) تلزم صاحب البيانات بالموافقة المسبقة قبل تصفح المواقع الإلكترونية " ¹¹¹. فلا يجوز أن يتم تجميع البيانات الشخصية إذا كان من يقوم به لا يعلم بالهدف من وراء التجميع وكذلك بدون موافقته . فلا بد من أن يكون التجميع قد تم لغايات محددة ومعلنة ومشروعة، وأن تكون كل معالجة لاحقة متناسبة مع هذه الغايات، وبناءً على ذلك لا يجوز استخدام المعلومات للمعالجة وجمعها، لأهداف أخرى غير تلك التي يتم الإعلان عنها¹¹². فلا يجوز على سبيل المثال، أن يتم استخدام البيانات التي جمعت لإدارة شؤون الزبائن بهدف توجيه إعلانات تسويقية إليهم. وإنما يجب أن تكون الأهداف

¹⁰⁹ Art. 5 GDPR Principles relating to processing of personal data

"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')."

¹¹⁰ سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، الكويت . العدد 9، السنة 3، 2015، ص 407 .

¹¹¹ قرار رقم (48) لسنة 2022 بشأن حقوق صاحب البيانات للمزيد الاطلاع على

http://www.pdp.gov.bh/assets/pdf/executive-decisions/rights_of_the_data_subject.pdf

¹¹² فتحية حزام، إجراءات المعالجة الآلية للمعطيات ذات الطابع الشخصي وفقاً لأحكام القانون 07-18، جامعة محمد بوقرة- بومرداس الجزائر، 2021، ص 348-349.

مثل العمل على تحسين نوعية الخدمات، وإدارة شؤون الموظفين، والعملاء، والزبائن، وحماية المصالح المالية للشركة. ففي عملية معالجة ملفات زبائن وكالة نقلات، لا يوجد سبب يستدعي طلب رقم بطاقة الضمان الصحي من الزبون، أو معلومات عن محيطه العائلي، والمهني. كما أن القيام بتحديد الهدف يساعد على تحديد مدة الاحتفاظ بالبيانات، حيث يفترض أن يتم محو معلومات الأشخاص الذين تركوا عضوية نادٍ، أو جمعية، أو تركوا المؤسسة، إلا متى كان هذا الأمر ضروريًا، لحاجات إثبات قانونية، تفرضها القوانين المرعية. ومن ناحية أخرى يجب الحرص على عدم جمع البيانات التي تكون حساسة بطبيعتها، والتي تمنع معالجتها، إلا بصورة استثنائية، بموجب إجراءات إدارية خاصة، ولأهداف محددة قانونًا¹¹³.

ثالثًا: مبدأ التناسبية ومبدأ تأقيت التخزين

يستلزم مبدأ التناسبية أن تكون البيانات الشخصية مناسبة بالنظر إلى الغايات التي تم على أساسها جمعها ومعالجتها، حيث يلزم في كل معالجة أن تقوم على بيانات تجمعها علاقة مباشرة بالغايات التي حددت ابتداءً للمعالجة ويلزم بالإضافة إلى ذلك أن تكون غير مفرطة بالمقارنة مع الغايات المذكورة، وكذلك أن تكون دقيقة وصحيحة، ما يضمن عدم إصدار حكم، أو تقييم خاطئ على صاحبها من جهة، ويضمن مصداقية نتائج المعالجة من جهة أخرى¹¹⁴. كما يلزم عدم جمع البيانات التي تعتبر حساسة، والتي تمنع معالجتها، إلا بصورة استثنائية، بموجب إجراءات إدارية خاصة، ولأهداف محددة قانونًا. إلا أنه يمكن معالجة هذه البيانات، فيما لو كانت قد نشرت بصورة عامة، ووضعت في متناول الجمهور، أو في حال موافقة صريحة، وخطية، ومحددة، من صاحبها، أو بهدف الحفاظ على حياة إنسان، أو كان استخدامها مرخصًا به بحسب القانون، خدمة لمصلحة عامة، أو كان أصحابها أعضاء في جمعيات أو مجموعات عرقية، أو سياسية، أو دينية، أو إثنية. ويضاف إلى ذلك ضرورة الانتباه إلى المعلومات المتعلقة بالجنايات والجرائم، التي تنظم معالجتها ضمن أطر قانونية¹¹⁵.

ولقد نص المشرع البحريني في الفقرة (3) و(4) من المادة (3/3) من قانون حماية البيانات الشخصية رقم 30 لسنة 2018 على مبدأ التناسبية حيث نص على أنه "يجب" أن تكون البيانات كافية وذات صلة وغير مفرطة بالنظر إلى الغرض من جمعها أو الذي تمت المعالجة اللاحقة لأجله. والمادة (4/3) نصت على أنه يجب" أن تكون البيانات صحيحة ودقيقة، وتخضع للتحديث

منى أبو أشقر جبور و محمود جبور، المرجع السابق، ص122-123

¹¹⁴ تومي يحيى، "الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07 دراسة تحليلية"، مجلة الأستاذ لباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 4، العدد 02، الجزائر، 2019، ص1535.

¹¹⁵ منى أبو أشقر جبور و محمود جبور، المرجع السابق، ص123.

عندما يكون لذلك مقتضى". وقد أكد النظام الأوروبي العام لحماية البيانات الشخصية على هذا المبدأ في المادة (5) منه .

أما بالنسبة للمبدأ الآخر وهو مبدأ تأقيت التخزين، فيعني أنه يجب أن تكون البيانات الشخصية محفوظة خلال مدة لا تتجاوز المدة الضرورية لإنجاز الغايات التي من أجلها تم جمعها ومعالجتها. ويقتضي هذا ألا يتم حفظ البيانات على وجه نهائي ودائم بملفات آلية، حيث يجب أن تتحدد مدة الحفظ بشكل مؤقت في ضوء الغايات المرتبطة بكل ملف، إلا إذا تم الحصول على إذن بحفظ هذه البيانات بعد المدة المحددة، نظرًا إلى طبيعة البيانات وبناءً على طلب من المسؤول عن المعالجة لمصلحة مشروعة، وهذا لأغراض تاريخية أو إحصائية أو علمية¹¹⁶.

ومثال على ذلك، نجد أن مدة الاحتفاظ بالمعلومات التي تجمع عن الموظفين تختلف عن تلك التي تجمع عن زوار المباني، بهدف الحفاظ على الأمن، ومراقبة مداخل الأبنية، أو تلك التي تجمع في المجال الطبي، لمتابعة المرضى، أو لدراسة انتشار الأوبئة، لهذا تستقل حدود مدة الاحتفاظ بالبيانات عن زمن تحقيق الهدف في كل مرة، ولا يكون ممكنًا تحديد وقت الإفادة منها، كأن تكون هذه البيانات وسيلة إثبات علاقات عمل، أو التزامات، أو عقود.

ولقد أخذ المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية بمبدأ تأقيت التخزين في المادة (5) فقرة (e) فنص على أن يتم الاحتفاظ بالبيانات في شكل يسمح بتحديد موضوعات البيانات لمدة لا تزيد عما هو ضروري للأغراض التي تتم معالجة البيانات الشخصية من أجلها؛ فقد يتم تخزين البيانات الشخصية فترات أطول بقدر ما تتم معالجة البيانات الشخصية لأغراض الأرشفة فقط للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية وفقًا للمادة (89) (1) مع مراعاة تنفيذ الإجراءات الفنية والتنظيمية المناسبة¹¹⁷.

وعلى غرار المشرع الأوروبي، نص المشرع البحريني في قانون حماية البيانات الشخصية في المادة (3) فقرة (4) ، (5) على أنه يجب ألا تبقى البيانات بشكل يكون معه من السهل معرفة صاحب البيانات منها بعد استنفاد الغرض من جمعها أو الذي تتم المعالجة اللاحقة لأجله، وتحفظ البيانات التي يتم تخزينها فترات أطول إما لأغراض تاريخية أو إحصائية أو للبحث العلمي في صورة مجهولة، وذلك بوضعها في صورة لا يمكن معها نسبة هذه البيانات إلى صاحبها. ويتعين إن تعذر ذلك تشفير هوية أصحابها.

¹¹⁶ تومي يحي، المرجع السابق، ص1536.

¹¹⁷ Art. 5 GDPR Principles relating to processing of personal data

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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific .."

ووفقاً لما سبق يعد مبدأ تقييد مدّة حفظ البيانات أحد أهم الآليات الكفيلة باحترام البيانات الشخصية بوجه عام، ناهيك عن أهميته في تدعيم الحق في النسيان الرقمي وحمايته، إذ إن حفظ البيانات الشخصية ولا سيما تلك التي تتدرج في صميم الحياة الخاصة للإنسان لمدة زمنية محدودة وغير دائمة يترتب عليه إتلافها أو محوها فيما بعد، ويمنع الرجوع إليها مهما كانت الأسباب، ما يساهم بشكل كبير في تحقيق النسيان الرقمي.

المطلب الثاني

شروط مشروعية معالجة البيانات الشخصية

لم يحظر كل من المشرع البحريني والأوروبي معالجة البيانات الشخصية بشكل مطلق، ووضعاً شروطاً يجب أن تتحقق لكي تتصف المعالجة بالمشروعية، وفي حالة لم تتم مراعاة أحد هذه الشروط ستكون عملية المعالجة غير مشروعة. وهذه الشروط المبدئية يجب أن تتوافر في كل عملية معالجة للبيانات حتى توصف بأنها مشروعة، كما أن هذه الشروط لا تنفي الالتزامات التي تكون على عاتق من يقوم بالمعالجة؛ لأنه سوف يلتزم بها عند قيامه بعملية المعالجة على الرغم من تحقق الشروط.

وتعتبر الشروط التي أقرت للسماح بمعالجة البيانات الشخصية، في القوانين العربية ومنها مملكة البحرين، سواء من حيث الأصول الإدارية المفروضة، أم من حيث ضرورة احترامها حقوق صاحب البيانات، منسجمة مع النظام الأوروبي العام لحماية البيانات الشخصية¹¹⁸. وهذا ما سوف نستعرضه من خلال ثلاثة فروع:

نتناول في الأول: الشروط الخاصة بجمع البيانات

وفي الثاني: الشروط الخاصة بحفظ البيانات

وفي الثالث: الشروط الخاصة بإجراءات المعالجة الأخرى

¹¹⁸ منى أبو أشقر جبور و محمود جبور ،، المرجع السابق، ص 95، 96.

الفرع الأول: الشروط الخاصة بجمع البيانات

أورد المشرعان البحريني والأوروبي شروطاً خاصة بجمع البيانات الشخصية حتى تتصف عملية الجمع بالمشروعية وهي كالآتي:

أولاً: جمع البيانات بطريقة مشروعة

يتطلب التجميع المشروع للبيانات إخبار صاحب البيانات عن وجود هذا التجميع، وعن طريقته وكذلك الغرض منه وما هي أنواع البيانات التي تم تجميعها¹¹⁹. وقد نص القرار الوزاري البحريني رقم (48) لسنة 2022 والمتعلق بحقوق صاحب البيانات الشخصية في المادة (3) منه نص على أهمية إطلاع صاحب البيانات على قرار المعالجة الآلية، وكذلك في المادة (4) إلزم المشرع مدير البيانات بالحصول على موافقة صاحب البيانات قبل البدء بعملية المعالجة بطريقة مكتوبة أو إلكترونية وذلك للموافقة على المعالجة ونطاق التطبيق. وكذلك نجد قرار الوزاري رقم (45) لسنة 2022 بشأن تحديد قواعد وإجراءات معالجة البيانات الحساسة ، حيث تطلب المشرع في المادة (2) منه بالحصول على الموافقة المسبقة من قبل صاحب البيانات قبل بدء عملية المعالجة إلا في الحالات التي تم استثناءها كما ذكرناها انفا لاحتجاج إلى موافقة من قبل صاحب البيانات.

وفيما يتعلق بالاشتراطات العامة للمعالجة المشروعة نصت المادة (4) من قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018 على أنه لا يمكن معالجة البيانات الشخصية دون الحصول على موافقة من صاحبها، ولكن يمكن معالجتها وفق استثناءات نص عليها القانون، وهي كالآتي:

- إذا كانت المعالجة ضرورية من أجل تنفيذ عقد يكون صاحب البيانات طرفاً فيه.
- اتخاذ خطوات بناءً على طلب صاحب البيانات بهدف إبرام عقد.
- تنفيذ التزام يترتب عليه القانون، خلافاً لالتزام عقدي.
- صدور أمر من محكمة مختصة أو النيابة العامة.
- لحماية المصالح الحيوية لصاحب البيانات.
- وأخيراً لمباشرة المصالح المشروعة لمدير البيانات أو أي طرف ثالث يُفصح له عن البيانات، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية لصاحب البيانات.

¹¹⁹ سامح عبد الواحد التهامي، المرجع سابق، ص 404.

وكذلك حظر المشرع البحريني في المادة (5) معالجة البيانات الحساسة من غير الحصول على موافقة صاحبها، وأشار إلى عدة استثناءات، منها:

1. المعالجة التي تتطلب قيام مدير البيانات بالتزاماته بمباشرة حقوقه. وذلك في حال كان صاحب الالتزام ملتزم بالالتزام قانوني مثل تنفيذ العقد.
2. إذا كانت ضرورية لحماية المصالح الحيوية للشخص المعني ومن ضمن هذه المصالح كتلك المتعلقة بسلامته الجسدية أو مسألة الحياة والموت.
3. إذا كانت البيانات الشخصية معلنة للجمهور بمعنى أنه بمجرد نشر هذه البيانات فذلك يعد بمثابة الموافقة من قبل صاحب البيانات على المعالجة .
4. المعالجة الضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو أي شخص ملزم بحكم القانون بالمحافظة على السرية". هذا الاستثناء يتعلق بالصحة العامة مثل البيانات التي تم استخدامها في التطبيقات الصحية عند انتشار وباء كورونا على الرغم من حساسية هذه البيانات إلا أنه استثناء تم معالجتها للتوصل للمصابين وكذلك الاستفادة منه في اخذ اللقاحات وغيرها.
5. المعالجة التي تتم في أنشطة الجمعيات بأنواعها والنقابات وغيرها من الجهات التي لا تهدف إلى تحقيق ربح، وذلك بشرط الالتزام بعدة أمور، منها:
 - "المعالجة تتم وفقاً لما هو ضروري للغرض الذي أنشئت الجمعية أو النقابة أو الجهة من أجله.
 - أن تكون المعالجة لبيانات خاصة بأعضاء الجمعية أو النقابة أو لأفراد لهم اتصال منتظم معها بحكم طبيعة نشاطها.
 - ألا يتم الكشف عن البيانات لأي شخص ما لم يوافق صاحب البيانات على ذلك.
 - وأيضاً المعالجة التي تتم من قبل جهة عامة مختصة بالقدر الذي يقتضيه تنفيذ المهام المنوطة بها قانوناً.
 - معالجة بيانات تتعلق بالأصل العرقي أو الإثني أو الديني إذا كانت ضرورية للوقوف على مدى توافر المساواة في الفرص أو المعاملة لأفراد المجتمع الذين ينحدرون من أصول عرقية أو إثنية أو دينية مختلفة، وبشرط مراعاة الضمانات المناسبة لحقوق وحرية أصحاب البيانات المقررة قانوناً. وعلى مجلس الإدارة أن يصدر قراراً بتحديد القواعد والإجراءات التي يتعين على مديري البيانات الالتزام بها بشأن المعالجة".

هذا الاستثناء لم يشمل الحظر من المعالجة لكون أنشطة هذه الجمعيات أو النقابات تعد مشروعة غير ربحية وكذلك سوف تكون هناك موافقة مسبقه من صاحب البيانات الأمر الذي يسمح بمعالجتها.

وفي الاتجاه نفسه نص النظام الأوروبي العام لحماية البيانات الشخصية (GDPR)، في الفقرة (أ) من المادة (5) الخاصة بالمبادئ المتعلقة بمعالجة البيانات الشخصية، على أن تكون البيانات قد تمت معالجتها بطريقة مشروعة (lawfully) وعادلة (fairly) وبطريقة شفافة (manner transparent) بالنسبة لصاحب البيانات¹²⁰.

كما نص النظام الأوروبي لحماية البيانات الشخصية في المادة (6) منه على الاشتراطات العامة للمعالجة المشروعة وهي كالآتي:

- 1- إعطاء الموافقة من صاحب البيانات على معالجة بياناته الشخصية لغرض واحد أو أكثر من الأغراض المحددة .
- 2- تكون المعالجة ضرورية لأداء عقد يكون موضوع البيانات طرفاً فيه أو من أجل اتخاذ خطوات بناءً على طلب صاحب البيانات قبل الدخول طرفاً في العقد.
- 3- المعالجة ضرورية للامتثال للالتزام القانوني الذي يخضع له المتحكم
- 4- المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر
- 5- المعالجة ضرورية لأداء مهمة يتم تنفيذها للمصلحة العامة أو في ممارسة السلطة الرسمية المخولة للمراقب.
- 6- المعالجة ضرورية لأغراض المصالح المشروعة التي يسعى إليها المتحكم أو طرف ثالث، باستثناء الحالات التي يتم فيها تجاوز هذه المصالح من خلال المصالح أو الحقوق والحريات الأساسية لموضوع البيانات التي تتطلب حماية البيانات الشخصية ، ولا سيما عندما تكون البيانات الموضوع طفل.
- 7- لا تنطبق النقطة (و) من الفقرة الفرعية الأولى على المعالجة التي تقوم بها السلطات العامة في أداء مهامها.

¹²⁰ ART 5 GBDR Principles relating to processing of personal data Personal data shall be:

1. "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

يجوز للدول الأعضاء الاحتفاظ أو إدخال أحكام أكثر تحديدًا لتكييف تطبيق قواعد هذا النظام فيما يتعلق بالتجهيز للامتثال للنقطتين (ج) و (هـ) من الفقرة 1 من خلال تحديد متطلبات أكثر دقة للمعالجة والتدابير الأخرى ضمان المعالجة القانونية والعادلة بما في ذلك حالات المعالجة المحددة الأخرى على النحو المنصوص عليه في الفصل التاسع. وكذلك يجب وضع أساس المعالجة المشار إليه في النقطة (ج) و (هـ) من الفقرة 1 من خلال:

1. قانون الاتحاد أو قانون الدولة العضو الذي يخضع له المراقب.
2. يجب تحديد الغرض من المعالجة في ذلك الأساس القانوني أو ، فيما يتعلق بالمعالجة المشار إليها في النقطة (هـ) من الفقرة 1 ، يجب أن تكون ضرورية لأداء مهمة يتم تنفيذها في المصلحة العامة أو في ممارسة المسؤول السلطة المخولة للمراقب. قد يحتوي هذا الأساس القانوني على أحكام محددة لتكييف تطبيق قواعد هذا النظام ، من بين أمور أخرى: الشروط العامة التي تحكم شرعية المعالجة من قبل المراقب ؛ أنواع البيانات التي تخضع للمعالجة ، موضوعات البيانات المعنية ، الكيانات والأغراض التي قد يتم الكشف عن البيانات الشخصية من أجلها ، تحديد الغرض ، فترات التخزين وعمليات المعالجة وإجراءات المعالجة ، بما في ذلك التدابير اللازمة لضمان المعالجة القانونية والعادلة مثل تلك الخاصة بحالات المعالجة المحددة.

3. يجب أن يلبي قانون الاتحاد أو قانون الدول الأعضاء هدف المصلحة العامة وأن يكون متناسبًا مع الهدف المشروع المنشود.

عندما لا تعتمد المعالجة لغرض آخر غير ذلك الذي تم جمع البيانات الشخصية من أجله على موافقة صاحب البيانات أو على قانون الاتحاد أو الدولة العضو الذي يشكل تدبيرًا ضروريًا ومتناسبًا في مجتمع ديمقراطي لحماية الأهداف المشار إليها في المادة 23 (1) ، يجب على المراقب ، من أجل التأكد مما إذا كانت المعالجة لغرض آخر متوافقة مع الغرض الذي تم جمع البيانات الشخصية من أجله في البداية ، أن يأخذ في الاعتبار ، من بين أمور أخرى:

1. أي رابط بين الأغراض التي تم جمع البيانات الشخصية من أجلها وأغراض المعالجة الإضافية المقصودة
2. السياق الذي تم فيه جمع البيانات الشخصية ، لا سيما فيما يتعلق بالعلاقة بين موضوعات البيانات والمراقب
3. طبيعة البيانات الشخصية ، لا سيما ما إذا كانت تتم معالجة فئات خاصة من البيانات الشخصية ، وفقًا للمادة 9 ، أو ما إذا كانت البيانات الشخصية المتعلقة بالإدانات الجنائية والجرائم تتم معالجتها ، وفقًا للمادة 10 ؛ العواقب المحتملة

للمعالجة الإضافية المقصودة لموضوعات البيانات، دوجود الضمانات المناسبة ،
والتي قد تشمل التشفير أو أسماء مستعارة¹²¹.

ونستنتج مما سبق أن كلا المشرعين الأوروبي والبحريني حرصا في نصوص المواد على
التأكيد على مبدأ العدالة والأنصاف والشفافية وهذا يكون من خلال الحصول على موافقة صاحب
البيانات على عملية المعالجة وتحديد الغرض أو اغراض محددة لهذه المعالجة عند البدء بعملية
الجمع لهذه البيانات خاصة حتى تتصف عملية جمع البيانات بالمشروعية.

ثانياً: جمع البيانات لغايات واضحة ومحددة ومشروعة

نص المادة (3) الفقرة الثانية من قانون حماية البيانات الشخصية البحريني متوافقاً مع ما جاء
في المادة (5) من النظام الأوروبي لحماية البيانات الشخصية. ومفاد هذين النصين أنه يجب أن
يكون لجمع البيانات ومعالجتها أغراض وأهداف مشروعة ومحددة وواضحة وألا يتم إجراء معالجة
لاحقة لها على نحو لا يتوافق مع الغرض الذي جُمعت من أجله، ولا تُعدُّ معالجة غير متوافقة مع
الغرض الذي جُمعت من أجله البيانات المعالجة اللاحقة لها التي تتم حصراً لأغراض تاريخية أو
إحصائية أو للبحث العلمي، بشرط ألا تتم لدعم اتخاذ أي قرار أو إجراء بشأن فرد محدد.

إذاً يتبين مما سبق أن الهدف من هذا الشرط هو تقييد معالجة البيانات بالهدف الذي تم
جمع البيانات من أجله، فينسجم أسلوب معالجة البيانات مع الغاية من جمعها، ويبقى الهدف من
جمع هذه البيانات حاكماً لكل إجراء من إجراءات معالجة البيانات الشخصية. لذلك أي إجراء يتعلق
بالبيانات الشخصية يجب أن يكون متلائماً من جمع البيانات؛ فعندما يقوم شخص بالتعامل مع
جهة معينة وتطلب الجهة منه بعض البيانات الشخصية لتقديم خدمة معينة له، فإنه لا يجوز إجراء
أي معالجة لهذه البيانات الشخصية إلا من أجل تحقيق الهدف وهو تقديم الخدمة له، أما إذا تمت
معالجة هذه البيانات لأي هدف آخر غير ذلك فتكون المعالجة غير مشروعة، ومع ذلك يجوز
معالجة البيانات في غير الأغراض التي جمعت من أجلها في بعض الحالات كاستثناء، ويتحقق
ذلك، مثلاً، في حالة نشرت للجمهور بصورة عامة، أو في حالة المعالجة التي تتم بناءً على موافقة
صريحة وخطية معتمدة من قبل الشخص المعنى بالأمر. أو كان استخدامها مرخصاً به بحسب

121 ART 6 GDPR Lawfulness of processing. Processing shall be lawful only if and to the extent that at least one of the following applies:

1. “The data subject has given consent to the processing of his or her personal data for one or more specific purposes....”

القانون، لخدمة مصلحة عامة، ويضاف إلى هذا ضرورة الانتباه إلى المعلومات المتعلقة بالجرائم والجنایات التي يتم تنظيمها ضمن أطر قانونية خاصة¹²².

ومن ناحية أخرى نص المشرع السعودي في نظام معالجة البيانات الشخصية في المادة (11) منه على وجوب أن يكون للغرض من جمع البيانات الشخصية علاقة مباشرة بأغراض جهة التحكم، وألا يتعارض مع أي حكم مقرر نظاماً. وكذلك يجب ألا تتعارض الطرق المستخدمة في جمع البيانات الشخصية والوسائل مع أي حكم مقرر نظاماً، ويجب أن تكون البيانات ملائمة لظروف صاحبها، ومباشرة وواضحة وآمنة، وخالية من أساليب الخداع أو التضليل أو الابتزاز¹²³. كما يعد هذا الشرط من الشروط الجوهرية التي يجب أن تتوافر في المعالج أو المتحكم أو الغير الذي ترسل إليه البيانات، ويجب أن يظل هذا الشرط قائماً خلال فترة الجمع أو المعالجة أو الاحتفاظ بالبيانات، كما يجب أن يظل متوافراً أيضاً بعدها¹²⁴.

الفرع الثاني: الشروط الخاصة بحفظ البيانات

وفقاً للمادة (3) من قانون حماية البيانات الشخصية البحريني والمادة (5) من النظام الأوروبي العام فيلزم ليكون حفظ البيانات مشروعاً أن تتوافر فيه الشروط الآتية:

أولاً: أن يتم حفظ البيانات بطريقة تحدد هوية صاحبها

حيث نجد أن المشرع البحريني نص في المادة (3) من قانون حماية البيانات الشخصية على أنه يجب "ألا تبقى في صورة تسمح بمعرفة صاحب البيانات بعد استنفاد الغرض من جمعها أو الذي تتم المعالجة اللاحقة لأجله. وتُحفظ البيانات التي يتم تخزينها لفترات أطول لأغراض تاريخية أو إحصائية أو للبحث العلمي في صورة مجهولة بتحويرها، وذلك بوضعها في صورة لا تُمكن من نسبة هذه البيانات إلى صاحبها. ويتعين إن تعذر ذلك تشفير هوية أصحابها". وهذا يعني أنه يجب حفظها بطريقة مجهولة بعد استنفاد الغرض من معالجتها ولكن أثناء عملية المعالجة يتم حفظها بصورة تحدد هوية صاحبها وذلك حرصاً من المشرع البحريني على الحق في الخصوصية فتطلب عدم إيضاح هوية صاحب البيانات بعد استنفاد الغرض حتى

¹²² عمرو طه بدوي، التنظيم القانوني لمعالجة البيانات الشخصية، دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية، أكاديمية أبوظبي القضائية، الإمارات، 2017، ص 110.

¹²³ نظام حماية البيانات الشخصية السعودي 1443 هـ، مرسوم ملكي رقم (م/19) وتاريخ 9/2/1443 هـ.

يرجى زيارة تفاصيل النظام (boe.gov.sa) .

¹²⁴ سامح عبدالواحد التهامي، المرجع السابق، ص 415 وما بعدها.

لا يمكن أحد من الوصول إليها والقيام باستغلالها ، وخاصة فيما يتعلق بالبيانات التي تخزن فترات طويلة لأغراض تاريخية أو إحصائية أو للبحث العلمي.

أما بالنسبة للمشرع الأوروبي في المادة (5) نص على أنه يتم الاحتفاظ بالبيانات بشكل يسمح بتحديد موضوعات البيانات لمدة لاتزيد عما هو ضروري للأغراض التي تتم معالجة البيانات الشخصية من أجلها، كما قد يتم تخزين البيانات الشخصية لفترات أطول بقدر ماستتم معالجة البيانات الشخصية لأغراض الأرشفة فقط للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية.

ونستنتج مما تقدم أن المشرع البحريني حرص على حفظ البيانات بطريقة مجهولة أو بطريقة مشفرة للبيانات بعد استنفاد الغرض منها وانتهاء عملية المعالجة ، خاصة بالنسبة للبيانات التي يتم تخزينها فترات طويلة مثل بيانات لأغراض الأرشفة أو البحث العلمي ، وهذا على غرار المشرع الأوروبي نص على أن يتم حفظ البيانات بشكل يسمح بتحديد موضوعاتها بطبيعة الحال حتى يتمكن صاحب البيانات من الدخول إليها والإطلاع عليها ولكن يجب ان لاتزيد المدة عن الفترة الضرورية لتحقيق الغرض منها.

وهذا يعني أن حفظ البيانات يجب ألا يكون عشوائياً، وإنما يجب أن تحدد هوية صاحب البيانات، حتى يخول له ممارسة حقوقه على بياناته بالدخول إليها وتعديلها وتصحيحها¹²⁵.

ثانياً: حفظ البيانات للمدة اللازمة فقط لتحقيق الغرض الذي تم تجميع البيانات من أجله

سبق أن ذكرنا أنه يجب أن يتم تجميع البيانات وفقاً لغرض واضح ومحدد ومشروع، ووفقاً لما نص عليه المشرع البحريني في قانون حماية البيانات الشخصية في المادة (3) فيجب " ألا تبقى في صورة تسمح بمعرفة صاحب البيانات بعد استنفاد الغرض من جمعها أو الذي تتم المعالجة اللاحقة لأجله. وتُحفظ البيانات التي يتم تخزينها لفترات أطول لأغراض تاريخية أو إحصائية أو للبحث العلمي في صورة مجهولة بتحويلها، وذلك بوضعها في صورة لا تُمكن من نسبة هذه البيانات إلى صاحبها. ويتعين إن تعذر ذلك تشفير هوية أصحابها".

أما بالنسبة للنظام الأوروبي العام لحماية البيانات الشخصية نص في المادة (5) فقرة (ب)، " فمن الضرورة أن تتم معالجة البيانات في شكل يسمح بتحديد هوية صاحب البيانات لمدة معينة، لا تزيد عما هو ضروري للأغراض التي تتم معالجة البيانات الشخصية من أجلها. ومع ذلك أجازت المادة نفسها لأغراض معالجة البيانات الشخصية تخزين البيانات الشخصية فترات أطول، لأغراض الأرشفة من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو

¹²⁵ Alexandre manias and Sophie des courts, High standards apply to personal data processing , Art online at www.juriscom.net, (last visit: 30 April 2022)

الأغراض الإحصائية، مع مراعاة التنفيذ الفني والتنظيمي المناسب واتخاذ التدابير المطلوبة للحفاظ على حقوق وحرقات صاحب البيانات¹²⁶.

ومن ناحية أخرى نجد أن المشرع السعودي قد نص في المادة (18) من نظام حماية البيانات الشخصية على أنه يجب على المتحكم أن يتلف البيانات الشخصية عند انتهاء الغرض من جمعها، إلا أنه أجاز الاحتفاظ بالبيانات بعد انتهاء الغرض من جمعها إذا تمت إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد وفق الضوابط التي تحددها اللوائح". وحدد المشرع السعودي حالتين يمكن من خلالهما الاحتفاظ بالبيانات الشخصية بعد انتهاء الغرض من جمعها، وذلك في حالة وجود سبب يوجب الاحتفاظ بها مدة محددة، وفي هذه الحالة يجب إتلافها بعد انتهاء هذه المدة أو انتهاء الغرض من جمعها، أيهما أطول وكذلك في حالة ما إذا كانت البيانات الشخصية متصلة اتصالاً وثيقاً بقضية منظورة أمام جهة قضائية، وكان الاحتفاظ بها مطلوباً لهذا الغرض، وفي هذه الحالة تتلف البيانات بعد استكمال الإجراءات القضائية الخاصة بالقضية¹²⁷.

أما المشرع الكويتي، وبخلاف موقف المشرع البحريني والأوروبي، لم يشترط في قانون المعاملات الإلكترونية سوى حفظ البيانات بطريقة مشروعة دون أن يضع شروطاً لكيفية حفظ البيانات الشخصية، ودون تحديد المدة التي يتم من خلالها حفظ البيانات، وهذا يمنح معالج البيانات الحق في حفظ البيانات إلى أي وقت يشاء حتى بعد انتهاء الغرض منها، فكان الأولى به أن يربط حفظ البيانات بالغاية من جمعها مثلما فعل المشرعان الأوروبي والبحريني؛ فالاحتفاظ بالبيانات لا يجوز أن يكون أبدياً، بل يكون مؤقتاً ومحدداً لمدة معينة، ويعني ذلك أنه يتعين على المعالج أن يقوم بحفظ البيانات التي تمت معالجتها لمدة زمنية معينة بحيث لا تتجاوز المدة المطلوبة للأغراض التي جمعت من أجلها، وذلك حفاظاً على خصوصيتها¹²⁸.

¹²⁶ Art. 5 GDPR Principles relating to processing of personal data:

b. "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')"

¹²⁷ نظام حماية البيانات الشخصية السعودي 1443 هـ .

¹²⁸ القانون الكويتي رقم 20 لسنة 2014 في شأن المعاملات الإلكترونية. يمكن الاطلاع عليه :

[#https://e.gov.kw/sites/kgArabic/Pages/eServices/LegalPortal/Legal.aspx](https://e.gov.kw/sites/kgArabic/Pages/eServices/LegalPortal/Legal.aspx)

الفرع الثالث: الشروط الخاصة بإجراءات المعالجة الأخرى

كما ذكرنا آنفاً أن تجميع البيانات وحفظها يعتبران من إجراءات معالجة البيانات الشخصية، وقد وضع المشرعان البحريني والأوروبي لهذين الاجرائين شروطاً خاصة، وذلك لأهمية عملية تجميع البيانات على اعتبار أنها أول إجراء من إجراءات معالجة البيانات، ولأهمية إجراء الحفظ على اعتبار أن البيانات الشخصية تحفظ مدة طويلة من الزمن. أما أي إجراء آخر من الإجراءات الأخرى للمعالجة فيخضع لثلاثة شروط، وهي كما يأتي:

أولاً: إعطاء العلم

وفقاً للمادة (5) من النظام الأوروبي العام لحماية البيانات الشخصية والمادة (3) من قانون حماية البيانات الشخصية البحريني يشترط عند القيام بأي إجراء من إجراءات المعالجة أن يتم بطريقة مشروعة، وذلك حتى ينسجم مع تجميع البيانات الذي اشترط فيما سبق أن يتم بطريقة مشروعة. ولكي يتصف أي إجراء من إجراءات المعالجة للبيانات الشخصية بالمشروعية يجب إحاطة صاحب البيانات بجميع المعلومات اللازمة قبل الشروع بعملية المعالجة¹²⁹.

وحتى تتصف إجراءات المعالجة للبيانات الشخصية بالمشروعية يتطلب ذلك أن يتم إخطار صاحب البيانات بوجود معالجة لبياناته الشخصية، ونوع الأساليب التي سوف تستخدم في عملية المعالجة لبياناته وطريقتها وأيضاً الهدف منها، وهذه المعلومات يجب إخبار صاحب البيانات الشخصية بها قبل البدء بعملية المعالجة لبياناته الشخصية، بالإضافة إلى ذلك يجب أن تكون المعلومات التي يحصل عليها صاحب البيانات دقيقة بقدر الإمكان وواضحة، ومفهومة، وشفافة، وسهلة الاستيعاب¹³⁰.

وتحقيقاً لهذه الغاية، يتعين استخدام تعابير سهلة وواضحة، لا تثير الشك، وهذا الأمر شددت عليه جميع القوانين، ولهذا من الممكن أن تكون المعلومات مكتوبة أو شفوية كما يمكن أن تكون رقمية. كما يجب على مسؤول المعالجة أن يجيب عن أي سؤال يطرحه صاحب البيانات حول عملية المعالجة، وأهدافها وذلك وفق فترة زمنية معقولة، ووفقاً لطبيعة وحجم نشاط الجهة

¹²⁹ سامح عبدالواحد التهامي، المرجع السابق، ص410.

¹³⁰ منى الأشقر جبور ومحمود الأشقر جبور، مرجع سابق، ص135.

المسؤولة عن المعالجة ، ففي حال قيام المسؤول عن المعالجة بأي إجراء من إجراءات المعالجة للبيانات الشخصية دون أن يعلم صاحبها عد ذلك غير مشروع قانوناً¹³¹.

وهذا ما أكدته المشرع البحريني في المادة(4) من قانون حماية البيانات الشخصية حيث نص على الاشتراطات العامة للمعالجة المشروعة وهي كالآتي:

" تُحظر معالجة البيانات الشخصية دون موافقة صاحبها، ما لم تكن هذه المعالجة ضرورية لأي مما يأتي:

- 1- تنفيذ عقد يكون صاحب البيانات طرفاً فيه.
- 2- اتخاذ خطوات بناءً على طلب صاحب البيانات بهدف إبرام عقد.
- 3- تنفيذ التزام يرتبه القانون، خلافاً لالتزام عقدي، أو صدور أمر من محكمة مختصة أو النيابة العامة.
- 4- حماية المصالح الحيوية لصاحب البيانات.
- 5- مباشرة المصالح المشروعة لمدير البيانات أو أي طرف ثالث يُفصح له عن البيانات، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية لصاحب البيانات".

المادة (5) من القانون نصت على الاشتراطات الخاصة بمعالجة البيانات الحساسة وبموجب المادة لايجوز معالجة البيانات الحساسة بالإموافقة صاحب البيانات، ماعدا حالات استثنائية نص عليها القانون لانتطلب الحصول على موافقة صاحب البيانات وذلك عندما تكون المعالجة ضرورية أو تقوم بها جهة عامة أو كانت تتعلق معالجة البيانات بالأصل الديني أو العرقي أو الأثني.

المادة (9) من القانون نصت كذلك على سرية المعالجة مدير حيث أوجبت هذه المادة على مدير البيانات أن يقوم بالحصول على موافقة صاحب البيانات قبل أن يقوم بالإفصاح عن أية بيانات شخصية ، وكذلك يمكنه أن يفصح عنها في حال كان ذلك تنفيذاً لأمر صادر من المحكمة المختصة أو النيابة العامة أو قاضي التحقيق أو من النيابة العسكرية.

المادة (17) من قانون حماية البيانات الشخصية ذكرت المعلومات الواجب إحاطة صاحب البيانات بها وهي كالآتي :

¹³¹ منى الأشقر جبور ومحمود الأشقر جبور ، المرجع السابق، ص136.

"1- في الحالات التي يتم فيها الحصول على البيانات من صاحبها مباشرة، على مدير البيانات إحاطته عند تسجيل هذه البيانات بما يأتي:

- (أ) اسم مدير البيانات كاملاً ومجال نشاطه أو مهنته، بحسب الأحوال، وعنوانه.
- (ب) الأغراض التي من أجلها يُعْتَرَم معالجة البيانات.
- (ج) أية معلومات ضرورية أخرى، بحسب ظروف كل حالة، يكون من شأنها أن تكفل جعل المعالجة منصفة بالنسبة لصاحب البيانات، ومن ذلك ما يأتي:
 - (1) أسماء متسلمي البيانات أو فئاتهم.
 - (2) بيان ما إذا كانت الإجابة على أية أسئلة توجّه إلى صاحب البيانات إجبارية أو اختيارية، وعند الاقتضاء توضيح العواقب التي تترتب على الامتناع عن الإجابة.
 - (3) بيان حق صاحب البيانات في أن يتم إخطاره، إذا ما طلب ذلك، بالبيانات الخاصة به كاملة وبحقه في أن يتم تصحيحها.
 - (4) بيان ما إذا كان سيتم استخدام البيانات لأغراض التسويق المباشر.
 - (5) أية معلومات أخرى تلزم صاحب البيانات لمباشرة حقوقه المقررة بموجب أحكام هذا القانون.

(2) في حالة الحصول على البيانات من غير صاحبها، على مدير البيانات إحاطة صاحب البيانات خلال خمسة أيام من البدء في تسجيل هذه البيانات بما يأتي:

- (أ) المعلومات المشار إليها في الفقرة (1) من هذه المادة.
- (ب) الأغراض التي تم من أجلها جمع البيانات.
- (ج) أية معلومات ضرورية أخرى، بحسب ظروف كل حالة، يكون من شأنها جعل المعالجة منصفة بالنسبة لصاحب البيانات، ومن ذلك ما يأتي:
 - (1) المعلومات المشار إليها في الفقرة (1/ج) من هذه المادة.
 - (2) فئات البيانات.

(3) مصدر البيانات، وذلك باستثناء الحالات التي يقتضي واجب المحافظة على أسرار المهنة المقرّر قانوناً عدم الإفصاح عن المصدر.

(3) لا يسري حكم الفقرة (2) من هذه المادة في حال كانت معالجة البيانات لأغراض تاريخية أو إحصائية أو للبحث العلمي، وكانت إحاطة صاحب البيانات بالبيانات المشار إليها متعذرة أو تتطلّب بذل جهود مرهقة غير عادية. وعلى مجلس الإدارة أن يُصدر قراراً يحدّد بموجبه شروط توافر هذه الحالات، وأوضاعها. و إذا كانت معالجة البيانات تتم لغرض تنفيذ التزام يرتبه القانون، خلافاً لالتزام عقدي، أو أمر من محكمة مختصة أو النيابة العامة أو قاضي التحقيق، أو النيابة العسكرية".

ومن ناحية أخرى نجد أن القرارات التنفيذية في البحرين أكدت بدورها على أهمية إحاطة صاحب البيانات بكل ماسوف يجري في عملية المعالجة ومن ضمن هذه القرارات قرار (48) لسنة 2022 بشأن حقوق أصحاب البيانات ، حيث نص المشرع في المادة (4) منه يجب على مدير البيانات الحصول على موافقة كتابية أو إلكترونية من صاحب البيانات قبل مباشرة عملية المعالجة.

القرار رقم (51) لسنة 22022 بشأن شروط إنشاء سجلات البيانات الشخصية المتاح للجمهور الاطلاع عليها نصت المادة (2) على أنه يجب أن لا يتم وضع إي بيانات في السجلات إلا بعد أن يتم الحصول على الموافقة من صاحب البيانات وبعد أن تتم إحاطته بكافة المعلومات بإدراج البيانات وكذلك الغرض من السجل.

القرار رقم (43) لسنة 2022 بشأن الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية بموجب المادة (4) يجب على مدير البيانات أن يخطر أصحاب البيانات بوجود خرق أو انتهاك فيقوم بفتح قنوات الاتصال بينه وبين أصحاب البيانات أو من ينوب عنهم قانونا . ومن الممكن في حالات استثنائية لايُزَم باخطار صاحب البيانات بهذا الخرق أو الانتهاك في حال كانت البيانات التي تم اختراقها غير مفهومة أو استطاع المدير ان يتلافى مخاطرها العالية أو كان إخطار صاحب البيانات يتطلب منه بذل جهود مرهقة غير عادية.

أما بالنسبة للمشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية حدد في المادة (13) المعلومات التي يجب إخبار من يتم معالجة بياناته الشخصية بها، وعلى من يقوم بمعالجة البيانات الالتزام بالإخبار بها، وهي كالآتي:

- هوية وتفاصيل الاتصال الخاصة بالمراقب أو (مراقب حماية البيانات) وفقا للمشرع البحريني، وعند الاقتضاء ممثل المراقب وهذا شرط أساسي لصاحب البيانات حتى يتمكن من الاتصال بوحدة التحكم - ويرادفها في القانون البحريني مسمى (مدير البيانات)- وممارسة صاحب البيانات حقه في الحصول على المعلومات والوصول إليها عند الضرورة.

- تفاصيل الاتصال بمسؤول حماية البيانات عند الاقتضاء، ففي بعض الحالات يجب على وحدة التحكم تعيين مسؤول لحماية البيانات، من واجبه الإشراف على أنشطة المعالجة التي تجريها وحدة التحكم والعمل كنقطة اتصال لأصحاب البيانات.
- تقديم الأغراض التي من أجلها تتم معالجة البيانات الشخصية، وكذلك تحديد الأسس القانونية المختلفة التي يعتمد عليها المتحكمون في معالجة البيانات الشخصية وربطها بالغرض من المعالجة.
- المصالح المشروعة التي يتبعها المتحكم أو طرف ثالث، فعندما يتبع المتحكم مصلحة مشروعة في معالجة البيانات الشخصية يجب إبلاغ صاحب البيانات بشكل صريح عن طبيعة تلك المصلحة المحددة، على سبيل المثال التأكد من أن المنتجات على موقع الويب متاحة ويمكن تسليمها في بلد صاحب البيانات، ويمكن النظر إلى المصلحة المشروعة على أنها شرط مسبق حتى يكون صاحب البيانات قادرًا على ممارسة حقوق أخرى، مثل الحق في الاعتراض على المعالجة.
- المتسلمون أو فئات المستفيدين من البيانات الشخصية، إن وجدت، هذا يعني أنه يجب تغطية كل من الأشخاص الداخليين أو الخارجيين، سواء كانوا موظفين أو وكلاء أو مزودًا خارجيًا للمراقب. على سبيل المثال يجب تحديد جميع متسلمي بيانات الموظف مثل مدير الموارد البشرية لتلك الشركة أو مزود خدمة كشوف المرتبات الخارجي. ومن ناحية أخرى في حال وجود متسلمي الطرف الثالث يجب على وحدة التحكم تسمية متسلمي الطرف الثالث ذوي الصلة، بحيث يكون صاحب البيانات على دراية بالأشخاص الذين ستتم مشاركة بياناتهم معهم خارجيًا، وهذا من خلال تضمين إشارة إلى الأنشطة التي يقومون بها وموقع المتلقين.
- يجب على المراقبين إبلاغ أصحاب البيانات بشأن عمليات نقل البيانات الشخصية إلى المنظمات الدولية أو دول ثالثة، وذلك من خلال تسمية جميع البلدان ذات الصلة، وتحديد الإجراءات الوقائية التي تعتمد عليها. على سبيل المثال إذا نقلت وحدة تحكم بيانات شخصية إلى شريك تجاري موجود في اليابان فيجب أن تدرج اليابان على أنها أحد مواقع النقل.

كما نصت المادة (13) من النظام الأوروبي العام لحماية البيانات الشخصية من الفقرة الثانية على مجموعة من المعلومات الإضافية التي يجب على المراقبين تقديمها إلى أصحاب البيانات عند القيام بجمع البيانات الشخصية، وهي كالآتي¹³²:

- إبلاغ صاحب البيانات بالفترة التي سيتم فيها تخزين البيانات الشخصية (أي فترة الاحتفاظ أو فترة التخزين).
 - إبلاغ صاحب البيانات حول مصدر حقوق أصحاب البيانات، ولا سيما حقه في الوصول والتصحيح والمسح وتقييد المعالجة وإمكانية نقل البيانات وحقه في الاعتراض، ولا يكفي مجرد إبلاغه بحقوقه، وإنما أيضًا تضمين ملخص عما يتضمنه كل حق وأيضًا إعطاؤه خطوات كيف لصاحب البيانات ممارسة كل حق، وهذا يمكن بيانه من خلال إشعار الخصوصية.
 - يجب على المراقب إبلاغ صاحب البيانات بوجود الحق في سحب الموافقة في أي وقت عندما يكون الأساس القانوني لمعالجة البيانات هو موافقة صاحب البيانات.
 - إبلاغ صاحب البيانات على وجه التحديد بوجود الحق في تقديم الشكوى من بين الأمور الأخرى، إلى السلطة الإشرافية في الدولة العضو في المكان المعتاد لصاحب البيانات أو مكان عمله.
 - إبلاغ صاحب البيانات ما إذا كان توفير البيانات الشخصية مطلبًا قانونيًا أو تعاقدًا، أو شرطًا ضروريًا لإبرام عقد، وكذلك ما إذا كان موضوع البيانات ملزمًا بتقديم البيانات الشخصية والعواقب المحتملة لعدم توفير هذه البيانات.
 - إبلاغ صاحب البيانات بوجود آلية صنع القرار الآلي (بما في ذلك التنميط).
- و عندما ينوي المتحكم معالجة البيانات الشخصية لغرض لم يتم تصوره في المقام الأول، يجب إبلاغ صاحب البيانات بالغرض الجديد قبل مباشرة تلك المعالجة الإضافية من الناحية العملية،

¹³² Art. 13 GDPR Information to be provided where personal data are collected from the data subject
Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- a. "the identity and the contact details of the controller and, where applicable, of the controller's representative.
- b. the contact details of the data protection officer, where applicable.
- c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing."

وهذا يعني أنه يجب على المتحكمين تحديث إشعار الخصوصية الخاص بهم، وهذا الإخطار
سيمكن أيضًا صاحب البيانات من تحقيق الهدف الجديد.

ثانيًا: ألا تتم معالجة البيانات بطريقة لا تتلاءم مع الغاية من تجميعها

الهدف من هذا الشرط هو أن يتم تقييد معالجة البيانات الشخصية بالهدف الذي تم جمع
هذه البيانات من أجله، بحيث ينسجم أسلوب معالجة هذه البيانات مع الغاية من جمعها، فيبقى
الهدف من جمع هذه البيانات حاكمًا ومقيّدًا لكل إجراء من إجراءات معالجة البيانات الشخصية
بعد ذلك. فإن أي إجراء يتعلق بمعالجة البيانات الشخصية يجب أن يكون متلائمًا مع الهدف من
جمع هذه البيانات. فعندما يتعامل شخص مع جهة معينة وتطلب منه الجهة بعض البيانات
الشخصية لتقديم خدمة معينة له، فإنه لا يجوز إجراء أي معالجة لهذه البيانات الشخصية إلا في
إطار تحقيق ذلك الهدف وهو تقديم هذه الخدمة له. أما إذا تمت معالجة هذه البيانات لأي هدف
آخر غير ذلك كانت المعالجة غير مشروعة. وهذا الشرط يعتبر مهمًا لأنه يؤدي إلى عدم استخدام
البيانات الشخصية بعد جمعها استخدامًا غير مبرر، فإن الاستخدام غير المبرر هو استخدام غير
متوافق مع الغاية من جمع البيانات¹³³.

من ناحية أخرى نظمت المادة (3) من قانون حماية البيانات الشخصية البحريني والمادة
(5) من النظام الأوروبي العام لحماية البيانات الشخصية القواعد العامة الخاصة بجودة البيانات،
على أنه يجب أن تكون البيانات قد جمعت لغرض مشروع ومحدد وواضح ويجب ألا تتم معالجتها
لاحقًا، كما لا يجوز أن تتم المعالجة لاحقًا بما لا يتوافق مع الغرض الذي جمعت البيانات من
أجله، ويجدر التذكير بأن المعالجة الإضافية لأغراض تاريخية أو إحصائية أو للبحث العلمي لا
تتعارض - وفقًا للتشريعين- مع الأغراض الأولية¹³⁴.

من خلال نص المادتين السابقين نجد أن كلا من المشرعين حرصا على مبدأ تحديد
الغرض حيث أنه لا يجوز معالجة البيانات الشخصية إلا لهدف واحد أو أكثر من الأغراض

¹³³ سامح عبد الواحد التهامي ، المرجع السابق ،ص411.

¹³⁴ Art. 5 GDPR Principles relating to processing of personal data:

“...collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Art 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);”

المحددة. ولا يمكن استخدام البيانات الشخصية التي تم جمعها لغرض ما بحرية لأي غرض آخر. على سبيل المثال لايجوز لطبيب أن يستعمل البيانات التي حصل عليها من قبل المريض بهدف العلاج ، في أن يقوم بأفشاء هذه المعلومات بين الجمهور ، لأن الغرض هنا من إعطاء المريض لمعلومات عنه كان بهدف العلاج، ولكن الطبيب استخدم هذه المعلومات في أغراض أخرى كالترفيه عن الجمهور ، وذلك لأنه وفقاً لنص القانون لايجوز استخدام البيانات بعد جمعها في غير الغرض المحدد لها ويجب أن يحدد الغرض من تجميع البيانات ابتداءً بشكل صريح وليس ضمني فهذا يعتبر الخطوة كذلك يجب عدم استخدام البيانات بعد جمعها لأغراض لا تتوافق مع الغرض (الأغراض) الأصلي المحدد. جمعت يجب تحديد الغرض في اللحظة التي يتم فيها "جمع" البيانات الشخصية لأول مرة بواسطة المتحكم يجب فهم التجميع على أنه الخطوة الأولى في أي عملية معالجة. كما .يمتد مبدأ تحديد الغرض إلى "المعالجة الإضافية" من قبل جميع المستلمين الذين تم الكشف عن البيانات الشخصية لهم والغرض من ذلك هو قصر عمليات المعالجة على هدف محدد ومحدد مسبقاً، يمكن لوحدة التحكم تسمية أغراض متعددة ولكن يجب أن لا تكون الأغراض عامة للغاية لأنه من شأنها أن تقوض الحماية التي يحاول مبدأ تحديد الغرض تأسيسها. مثال كأن. يقوم صاحب العمل بمراقبة موظفيه "لأسباب تتعلق بالكفاءة". يحظر قانون العمل المحلي المراقبة بالفيديو في مكان العمل دون موافقة مجلس العمال. الغرض هنا يعد غير مشروع¹³⁵.

ثالثاً: موافقة صاحب البيانات

يعتبر الرضاء الصريح للشخص المعنى بالبيانات شرطاً أساسياً حتى تتصف عمليات المعالجة للبيانات الشخصية بالمشروعية، سواء لجمع البيانات أو معالجتها أو إفشائها، ما لم ينص القانون على غير ذلك¹³⁶.

ثم يجب لتوافر الرضاء في الشخص وجود الإرادة وأن يعبر عنها بصورة صريحة جازمة تُعبر عن موافقته على عمليات المعالجة لبياناته الشخصية. لذلك لا يعتد بالتعبير الضمني ولا بالموافقة المعلقة على شرط، وبهذا تعد موافقة الشخص هي الأساس القانوني للمعالجة، ومرجع ذلك هو أن بياناته تمس خصوصيته، وقد تمتد إلى حياته العائلية التي يحرص أن تكون بعيدة عن الأنظار.

وقد تطلب المشرع البحريني صراحة في المادة (5) و (6) من قانون البيانات الشخصية البحريني رقم 30 لسنة 2018 وجود موافقة صاحب البيانات على جمع ومعالجة البيانات حيث

¹³⁵ https://gdprhub.eu/index.php?title=Article_5_GDPR#28b.29_Purpose_limitation (last visit:6 April2023)

¹³⁶ حسن عبد الحميد، المرجع السابق، ص51.

نص المشرع البحريني في المادة (5) بشأن الأشرطاطات الخاصة بمعالجة البيانات الحساسة حيث " تُحظر معالجة البيانات الشخصية الحساسة دون موافقة صاحبها، ويُستثنى من هذا الحظر ما يأتي:

- (1) المعالجة التي يقتضيها قيام مدير البيانات بالتزاماته ومباشرة حقوقه المقررة قانوناً في مجال علاقة العمل التي تربطه بالعاملين لديه.
 - (2) المعالجة الضرورية لحماية أيّ إنسان إذا كان صاحب البيانات -أو الوصي أو الولي أو القيم عليه - غير قادر قانوناً على إعطاء موافقته على ذلك، وبشرط الحصول على تصريح مسبق من الهيئة طبقاً للمادة (15) من هذا القانون.
 - (3) معالجة البيانات التي أتاحها صاحبها للجمهور.
 - (4) المعالجة الضرورية لمباشرة أيّ من إجراءات المطالبة بالحقوق القانونية أو الدفاع عنها، بما في ذلك ما يقتضيه التجهيز لهذا الأمر والاستعداد له.
 - (5) المعالجة الضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو تقديم الرعاية الصحية أو العلاج أو إدارة خدمات الرعاية الصحية من قبل مرخص له بمزاولة أيّ من المهن الطبية، أو أيّ شخص ملزم بحكم القانون بالمحافظة على السرية.
 - (6) المعالجة التي تتم في سياق أنشطة الجمعيات بأنواعها والنقابات وغيرها من الجهات التي لا تهدف إلى تحقيق ربح، وذلك بشرط الالتزام بما يأتي:
 - أ) أن تتم المعالجة في حدود ما هو ضروري للغرض الذي أنشئت الجمعية أو النقابة أو الجهة من أجله.
 - ب) أن ترد المعالجة على بيانات تخص أعضاء تلك الجمعية أو النقابة أو الجهة أو لأفراد لهم اتصال منتظم معها بحكم طبيعة نشاطها.
 - ج) ألا يتم الإفصاح عن البيانات لأيّ شخص آخر ما لم يوافق صاحب البيانات على ذلك.
 - (7) المعالجة التي تتم من قبل جهة عامة مختصة بالقدر الذي يقتضيه تنفيذ المهام المنوطة بها قانوناً.
 - (8) معالجة بيانات تتعلق بالأصل العرقي أو الإثني أو الديني إذا كانت ضرورية للوقوف على مدى توافر المساواة في الفرص أو المعاملة لأفراد المجتمع الذين ينحدرون من أصول عرقية أو إثنية أو دينية مختلفة، وبشرط مراعاة الضمانات المناسبة لحقوق وحرّيات أصحاب البيانات المقررة قانوناً.
- وعلى مجلس الإدارة أن يُصدر قراراً بتحديد القواعد والإجراءات التي يتعيّن على مدراء البيانات الالتزام بها بشأن المعالجة المشار إليها".

أما في المادة (6) من القانون نص المشرع البحريني على معالجة البيانات لأغراض الصحافة أو الأداب أو الفنون حيث " لا تسري أحكام المواد (3) و(4) و(5) من هذا القانون على معالجة البيانات الشخصية التي تتم حصراً للأغراض الصحفية أو الفنية أو الأدبية، بشرط: أ) أن تكون البيانات صحيحة ودقيقة وتخضع لعمليات التحديث والتصحيح. ب) توافر تدابير تكفل عدم استخدام البيانات لأية أغراض أخرى خلافاً للأغراض الصحفية أو الفنية أو الأدبية. ج) عدم الإخلال بالتشريعات المعمول بها بشأن تنظيم الصحافة والطباعة والنشر".

وهو عين ما أخذ به النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) في المادة (6) منه، كما حددت المادة (7) من النظام شروط الموافقة (Conditions for consent) 137. كما عرفت المادة 4 / 11 من النظام الأوروبي العام موافقة صاحب البيانات (consent of the data subject) بأنها تعني أي إشارة صريحة ومحددة وواضحة لا لبس فيها، تدل على رضا صاحب البيانات والتي يشير من خلالها إلى الموافقة على معالجة البيانات الشخصية المتعلقة به أو بها، من خلال بيان أو بعمل إيجابي واضح. بينما لم يشر المشرع البحريني إلى تعريف "موافقة الشخص المعني بالبيانات" صراحة في نصوصه ولكن يمكن اعتبار الموافقة هنا تصريحاً من صاحب البيانات لكي يقوم مدير البيانات بمعالجة بياناته بناء على هذه الموافقة. ونجد هنا أن المشرع البحريني كان من الأفضل أن يضع تعريفاً للموافقة على معالجة البيانات الشخصية على غرار ما فعل المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية، وذلك في اللائحة التنفيذية لقانون حماية البيانات الشخصية البحريني.

إذاً يتبين لنا مما سبق أنه على من يقوم بعملية معالجة البيانات الشخصية الحصول على موافقة من تتم معالجة بياناته، وهذا قبل القيام بأي إجراء من إجراءات المعالجة للبيانات الشخصية، وبالإضافة إلى ذلك يقتضي منه أن يخبر صاحب البيانات بكل ما يتعلق بإجراءات المعالجة التي سوف يقوم بها،

¹³⁷ Art. 7 GDPR Conditions for consent

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..."

ونجد أن المشرع البحريني في المادة (24) من قانون حماية البيانات الشخصية اشترط وحدد للاعتداد بموافقة صاحب البيانات عدة أمور ومنها :

" أ) أن تكون صادرة عن شخص كامل الأهلية.

وعلى الرغم من هذا الشرط إلا أن المشرع البحريني لم يبين بنص خاص أهلية من يصدر عنه الرضاء بشأن جمع ومعالجة بياناته ، ومفاد ذلك بأنه يتعين علينا الرجوع إلى المبادئ العامة إي بلوغ إحدى وعشرين سنة ميلادية كاملة.

ب) أن تكون مكتوبة وصريحة وواضحة ومحددة بمعالجة بيانات معينة.

وهذا يعني أن المشرع البحريني اشترط أن يتم إفراغ الموافقة في شكل مكتوب لمعالجة البيانات الشخصية، لضمان نسبتها لصاحبها وتيسيراً لإثباتها، وغالباً ما يتم إعداد نماذج محددة لإفراغ هذه الموافقة وفق الضوابط التي يتطلبها القانون. ولكن تتبغى الإشارة هنا إلى أن اشتراط إفراغ الموافقة في شكل مكتوب لا يغير من طبيعة العقد كونه عقدا رضائيا، أي إن الكتابة شرطاً للإثبات وليست ركناً في العقد، ومفاد ذلك إن الموافقة غير المكتوبة يجوز إثباتها بالإقرار أو اليمين في حال تعذر الكتابة¹³⁸. أما في حال كانت الكتابة ركناً شكلياً في العقد فإن العقد غير المكتوب هو عقد يفتقر لأحد أركانه ما يعني بطلانه حتى مع الإقرار واليمين.

ج) أن تكون صادرة بناءً على إرادته الحرة بعد إحاطته تماماً بغرض أو أغراض معالجة البيانات، وإحاطته، عند الاقتضاء، بالعواقب التي تترتب على عدم موافقته.

وهذا يعني بأنه لا يكفي مجرد وجود رضاء الشخص المعني بالبيانات، إنما يجب أن يكون صحيحاً، وهو يكون كذلك متى توافرت الإرادة، فإذا انعدمت الإرادة انعدم الرضاء، واستحال توافره نتيجة لانعدامه، وعلى ذلك لا يتوافر الرضاء إلا إذا توافرت الأهلية لدى الشخص المعني بالبيانات، والأهلية المطلوبة هنا هي أهلية الأداء أي صلاحية الشخص لاستعمال الحق، أو بمعنى آخر قدرة الشخص على أداء التصرفات القانونية لحساب نفسه، ومناطها التمييز أو الرشد، إذ تتأثر بالسن والعقل، فيجب أن يصدر التعبير من شخص اكتملت مداركه ونضجت، فأصبح يقدر الآثار المترتبة على تصرفاته¹³⁹.

2) إذا كان صاحب البيانات ناقص الأهلية أو عديمها، فيُعتد في هذه الحالة بموافقة الولي أو الوصي أو القيم في الحدود التي رسمها القانون، ووفقاً للشروط المشار إليها في البند (1/ب،ج) من هذه المادة.

¹³⁸ عبد الرزاق أحمد السنهوري، المرجع السابق، ص154.

¹³⁹ عبدالرزاق السنهوري، المرجع السابق، ص 224.

3) لصاحب البيانات، بموجب إخطار يُصدّره لمدير البيانات، أن يسحب في أيّ وقت موافقته على معالجة بياناته الشخصية. ويُصدّر مجلس الإدارة قراراً يحدد بموجبه إجراءات تقديم طلب السّحب والبتّ فيه من قِبَل مدير البيانات".

وهذا يماثل ما جاء في المادة (7) من النظام الأوروبي العام لحماية البيانات الشخصية فيما يتعلق بشروط الموافقة، حيث نصت على أنه يجب أن تكون الموافقة على معالجة البيانات في سياق مكتوب وتقدم بطريقة يمكن تمييزها بوضوح عن الأمور الأخرى، في شكل واضح يسهل الوصول إليه، وباستخدام لغة بسيطة¹⁴⁰.

وكذلك نص المشرع الأوروبي في المادة (8) منه على اعتبار معالجة بيانات الطفل في إطار خدمات مجتمع المعلومات مشروعة، حين يكون سن الطفل ستة عشر (16) عاماً على الأقل، أما إذا كان سنه لا يتجاوز ذلك، فإن المعالجة لا تكون مشروعة، إلا إذا صدر الرضاء من قبل صاحب السلطة الأبوية على الطفل أو من ينوب عنه قانوناً. ويجوز للدول الأعضاء تخفيض هذا السن بشرط ألا يقل بأي حال من الأحوال عن ثلاثة عشر (13) عاماً. ووفقاً للمادة (8) يُقصد بخدمة مجتمع المعلومات أي خدمة يتم تقديمها عادةً مقابل أجر ، عن بُعد ، بواسطة الوسائل الإلكترونية وبناءً على الطلب الفردي لمتلقي الخدمات. ومن خلال هذا التعريف يتضح لنا أن الخدمة تقدم عن بعد دون حضور الأطراف فعلياً ، وكذلك عن طريق الوسائل الإلكترونية ، أي إن الخدمة يتم إرسالها واستلامها في وجهتها من خلال المعدات الإلكترونية التي تعالج البيانات وتخزنها ، فضلاً عن إرسالها ونقلها واستلامها بالكامل عن طريق الأسلاك أو الراديو أو الوسائل البصرية أو غير ذلك. وكما أن الخدمة يتم تقديمها من خلال نقل البيانات بناءً على طلب فردي. ويترتب على ذلك أنه إذا كانت الخدمة لا تفي بالمتطلبات المذكورة أعلاه ، فلن يتم تطبيق المادة (8) من النظام الأوروبي العام لحماية البيانات (وضماناتها)¹⁴¹.

¹⁴⁰ Art. 7 GDPR Conditions for consent

^{2,1}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. ²Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding."

¹⁴¹Society Service definition it available at

https://gdprhub.eu/index.php?title=Article_8_GDPR#Information_Society_Service (last visit: 16 December 2022)

الفصل الثاني

ضوابط حماية البيانات الشخصية في عالم المعلوماتية

بعد أن تبينا مخاطر عالم المعلوماتية والتطور التكنولوجي على الحق في الخصوصية، لا بد من أن نقف عند ضوابط الحماية القانونية التي كفلها القانون البحريني والنظام الأوروبي العام لحماية خصوصية البيانات الشخصية لمواجهة تلك المخاطر التي تهدد خصوصية الأفراد، ومدى ملاءمتها، لمواجهة جميع صور الاعتداء على البيانات الشخصية.

كما أن كلا المشرعين البحريني والأوروبي لم يكتفِ بوضع هذه الضوابط، بل أيضًا أعطى الشخص بعض الحقوق على بياناته، ليتمكن من ممارستها في مواجهة من يقوم بمعالجة البيانات، وهي الحق في الإعلام والاعتراض والحق في التصحيح والحجب والحق في المسح.

ومن ناحية أخرى، حتى تكتمل منظومة الضوابط التي تحاط بها معالجة البيانات الشخصية لم يكتفِ المشرعان الأوروبي والبحريني بوضع شروط لمشروعية معالجة البيانات الشخصية في الفصل الأول بل ألقيا أيضًا ببعض الالتزامات على عاتق القائم بعملية المعالجة، وهي الالتزام بتقديم طلب التصريح المسبق والالتزام بتأمين البيانات الشخصية والالتزام بعدم إفشاء البيانات.

هذا بالإضافة إلى أن كلا من المشرعين قد وضع آليات لحماية خصوصية البيانات الشخصية، وذلك عن طريق إنشاء سلطة وطنية معنية بحماية البيانات الشخصية، وأيضًا وضع الجزاءات المناسبة عند انتهاك خصوصية البيانات الشخصية. وحتى نتناول هذه الحقوق والالتزامات وآليات الحماية بشيء من التفصيل، سنقوم بتقسيم هذا الفصل لمبحثين:

نتناول في المبحث الأول الحقوق والالتزامات المرتبطة بمعالجة البيانات الشخصية

ونخصص المبحث الثاني لبحث آليات الحماية ومعوقات التطبيق.

المبحث الأول

الحقوق والالتزامات المرتبطة بمعالجة البيانات الشخصية

أقر المشرع البحريني والمشرع الأوروبي مجموعة من الحقوق لأصحاب البيانات، والهدف من ذلك هو إعطاء الأشخاص المعنيين إمكانية السيطرة على بياناتهم، وكذلك توفير الحماية لهم في مواجهة الاعتداء على البيانات الخاصة بهم، بالإضافة إلى ذلك تم فرض مجموعة من الالتزامات على عاتق المسؤول عن المعالجة والجهات الثالثة التي يتم التعاقد معها، وذلك حماية للبيانات الشخصية الخاضعة للمعالجة. ولذلك نتناول هذه المسائل من خلال مطلبين:

نخصص الأول لحقوق أصحاب البيانات الشخصية

والثاني التزامات معالج البيانات الشخصية

المطلب الأول

حقوق صاحب البيانات الشخصية

حدد قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018 في المادة (17) منه عدة حقوق لأصحاب البيانات، يمكن تلخيصها في ما يأتي:

1. العلم بالبيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.
2. الحق في الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.
3. الحق في العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها، وكذلك المطالبة بالتصحيح والحجب والمسح أو الإضافة أو التحديث للبيانات الشخصية وتخصيص المعالجة في نطاق محدد.
4. العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

ويتضح مما سبق أن المشرع البحريني قد حدد حقوق صاحب البيانات على سبيل المثال وليس الحصر أي بما يتيح المجال أمام وجود حقوق أخرى لصاحب البيانات، سواء وردت في نصوص أخرى من قانون حماية البيانات الشخصية أو في قوانين أخرى.

وقد عالج النظام الأوروبي العام لحماية البيانات الشخصية حقوق صاحب البيانات (Rights of the data subject) في الفصل الثالث منه في المواد (12-23)، والاعتراف لصاحب البيانات ببعض الحقوق على بياناته هو غاية أساسية يسعى لها القانون، هادفاً بذلك توفير حماية قانونية فعالة له باعتباره المقصود أساساً من هذه الحماية.

وفي ضوء ما تقدم يمكننا أن نلخص الحقوق والضمانات التي توفرها التشريعات للشخص الطبيعي حماية لحقه في الخصوصية، ولنتناول هذه الحقوق نقسم هذا المطلب إلى ثلاثة فروع:

الفرع الأول: الحق في الإعلام والاعتراض

الفرع الثاني : الحق في التصحيح والحجب

الفرع الثالث :الحق في النسيان الرقمي

الفرع الأول: الحق في الإعلام والاعتراض

على صعيد حقوق الأفراد، أشار القانون البحريني في المادة (17) من قانون حماية البيانات الشخصية رقم (30) لسنة 2018 إلى البيانات التي يجب على مدير البيانات إحاطة صاحب البيانات بها وهي كالآتي:

(1) " في الحالات التي يتم فيها الحصول على البيانات من صاحبها مباشرة، على مدير البيانات إحاطته عند تسجيل هذه البيانات بما يأتي:

أ) اسم مدير البيانات كاملاً ومجال نشاطه أو مهنته، بحسب الأحوال، وعنوانه.

ب) الأغراض التي من أجلها يُعْتَرَم معالجة البيانات.

ج) أية معلومات ضرورية أخرى، بحسب ظروف كل حالة، يكون من شأنها أن تكفل جعل المعالجة منصفة بالنسبة لصاحب البيانات، ومن ذلك ما يأتي:

(1) أسماء متسلّمي البيانات أو فئاتهم.

(2) بيان ما إذا كانت الإجابة على أية أسئلة توجّه إلى صاحب البيانات إجبارية أو

اختيارية، وعند الاقتضاء توضيح العواقب التي تترتب على الامتناع عن الإجابة.

(3) بيان حق صاحب البيانات في أن يتم إخطاره، إذا ما طلب ذلك، بالبيانات الخاصة به كاملة وبحقه في أن يتم تصحيحها.

(4) بيان ما إذا كان سيتم استخدام البيانات لأغراض التسويق المباشر.

(5) أية معلومات أخرى تلزم صاحب البيانات لمباشرة حقوقه المقررة بموجب أحكام هذا القانون.

(2) في حالة الحصول على البيانات من غير صاحبها، على مدير البيانات إحاطة صاحب البيانات خلال خمسة أيام من البدء في تسجيل هذه البيانات بما يأتي:

أ) المعلومات المشار إليها في البند (1) من هذه المادة.

ب) الأغراض التي تم من أجلها جمع البيانات.

ج) أية معلومات ضرورية أخرى، بحسب ظروف كل حالة، يكون من شأنها جعل المعالجة منصفة بالنسبة لصاحب البيانات، ومن ذلك ما يأتي:

(1) المعلومات المشار إليها في البند (1/ج) من هذه المادة.

(2) فئات البيانات.

(3) مصدر البيانات، وذلك باستثناء الحالات التي يقتضي واجب المحافظة على أسرار

المهنة المقرر قانوناً عدم الإفصاح عن المصدر.

(3) لا يسري حكم البند (2) من هذه المادة في الحالتين التاليتين:

أ) إذا كانت معالجة البيانات لأغراض تاريخية أو إحصائية أو للبحث العلمي، وكانت إحاطة صاحب البيانات بالبيانات المشار إليها متعذرة أو تتطلب بذل جهود مرهقة غير عادية. وعلى مجلس الإدارة أن يُصدر قراراً يحدّد بموجبه شروط توافر هذه الحالات، وأوضاعها.

ب) إذا كانت معالجة البيانات تتم لغرض تنفيذ التزام يرتبّه القانون، خلافاً لالتزام عقدي، أو أمر من محكمة مختصة أو النيابة العامة أو قاضي التحقيق، أو النيابة العسكرية.

(4) لا يترتب على عدم مباشرة صاحب البيانات لحقه المقرر بموجب حكم أيٍّ من البند (1) من هذه المادة أو المادة (20) من هذا القانون سقوط لأيٍّ من الحقوق المقررة لمصلحته".

كما نص المشرع في المادة (18) من القانون على وجوب إبلاغ صاحب البيانات بكل المعلومات اللازمة والوافية عن الجهة التي سوف تقوم بالإطلاع على بياناته وذلك وفقاً للآتي:

(1) "على مدير البيانات، بناءً على طلب من صاحب البيانات مشفوع بما يثبت هويته، إخطار مقدّم الطلب دون مقابل خلال ميعاد أقصاه خمسة عشر يوم عمل من تاريخ الطلب، عما إذا كان مدير البيانات يعالج بيانات شخصية خاصة بصاحب الطلب، وفي حالة وجود معالجة

من أي نوع لهذه البيانات يلتزم مدير البيانات بإخطار صاحب البيانات في صورة مفهومة بما يأتي:

- (أ) البيانات موضوع المعالجة، كاملة.
- (ب) أية معلومات تتوافر لدى مدير البيانات أو متاحة له عن مصدر البيانات، وذلك باستثناء الحالات التي يفرض فيها القانون واجب المحافظة على سرية المصدر.
- (ج) الغرض من معالجة البيانات.
- (د) أسماء متسلمي البيانات أو فئاتهم.
- (هـ) في الحالة التي يُعترَم فيها اتخاذ قرار ما، بناءً على هذه البيانات دون غيرها، على نحو يمس مصلحة شخصية ومباشرة لصاحب البيانات، يتعين بيان الطريقة التي سوف تُستخدم في هذا الشأن بأسلوب واضح للشخص العادي ودون المساس بأية حقوق ملكية فكرية أو أسرار تجارية تتعلق بهذه الطريقة.
- (2) لمدير البيانات خلال فترة لا تتجاوز عشرة أيام من تسلمه طلباً تم تقديمه استناداً للبند (1) من هذه المادة أن يُخطر مقدّم الطلب باستيفاء أيّ نقص في طلبه.
- (3) لمدير البيانات عدم قبول الطلب المشار إليه في البند (1) من هذه المادة، إذا لم يكن مستوفياً، بشرط الالتزام بمتطلبات البند (2) من هذه المادة وفوات مدة الإعذار. وله رفضه إذا تضمن تعسفاً لاستعمال صاحب البيانات لحقه في المعرفة. وعلى مدير البيانات في هذه الحالة إخطار مقدّم الطلب خلال ميعاد أقصاه خمسة عشر يوم عمل من تاريخ تسلم طلبه بعدم قبول الطلب أو رفضه، بحسب الأحوال، وأسباب ذلك.
- (4) في حالة رفض الطلب المشار إليه في البند (1)، أو انقضاء المدة المحددة للاستجابة له دون أن يصل إلى صاحب البيانات أيّ إخطار بما تم بشأن طلبه، يكون لصاحب البيانات تقديم شكوى إلى الهيئة ضد مدير البيانات".

وجوب إبلاغ صاحب البيانات بكل المعلومات اللازمة والوافية عن الجهة التي ستقوم بالاطلاع على بياناته، والسبب الموجب لحصولها على تلك البيانات والطريقة التي ستتم معالجتها بها، و يتعين على مدير البيانات أن يحيط صاحب البيانات بمجموعة من العناصر طبقاً للمادة (17) وهي كالآتي:

- اسم مدير البيانات ونشاطه ومهنته وعنوانه.
- أغراض القيام بمعالجة البيانات.
- بالإضافة لتزويده بكل معلومة إضافية مفيدة في معالجة البيانات ولا سيما:
- أسماء متسلمي البيانات وفئاتهم.

- مدى إلزامية الرد والنتائج المترتبة على ذلك.
- بيان حق صاحب البيانات في أن يتم إخطاره، إذا ما طلب ذلك، وبحقه في أن يصحح البيانات.
- بيان ما إذا كان سيتم استخدام البيانات لأغراض التسويق المباشر.
- أي معلومات أخرى تلزم صاحب البيانات لمباشرة حقوقه.

وبقراءة نص المادة (17،18) نلاحظ أن مقتضيات الحق في الإعلام تختلف بين ما إذا كان جمع البيانات الشخصية لدى الشخص المعني (لدى صاحب البيانات) أم لدى الغير، ففي الحالة الأولى يلزم المشرع المسؤول عن المعالجة أو من ينوب عنه بوجوب إعلام صاحب البيانات عند الاتصال به من أجل تجميع بياناته، أي قبل عملية تجميع هذه البيانات. أما في الحالة الثانية عندما لا يكون تجميع البيانات لدى صاحب البيانات فيجب على المسؤول عن المعالجة أو من ينوب عنه في هذه الحالة إعلام صاحب البيانات قبل تسجيل هذه البيانات قبل إرسالها إلى الغير.

كما نجد إن المشرع البحريني قد استثنى من نطاق الحق في الإعلام مجموعة من الحالات على سبيل الحصر. وذلك في حالة تعذر على مدير البيانات إحاطة صاحب البيانات بالبيانات المشار إليها آنفاً، أو تطلب ذلك منه بذل جهود مرهقة غير عادية ويجب على مجلس إدارة الهيئة أن يصدر قراراً يحدد بموجبه شروط توافر هذه الحالات، أو قد تكون المعالجة تمت تنفيذاً لالتزام قانوني، أو تمت المعالجة لغرض تاريخي أو إحصائي أو للبحث العلمي.

أما النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) فقد أطلق عليه تسمية الحق في الوصول من قبل صاحب البيانات (Right of access by the data subject) ، وذلك في المادة (15) منه، ويفترض هذا الحق إمكانية الاطلاع على البيانات والمعلومات من قبل صاحبها، الذي يحق له أن يطلب نسخة من المسؤول عن معالجتها، ومعرفة ما إذا كانت بياناته داخلة في عملية المعالجة، وأهداف هذه العملية، وفئات البيانات المعالجة، والجهات التي تسلم، أو تنتقل إليها، ولا سيما في حال انتقال هذه البيانات إلى دولة أخرى أو شركات في هذه الدول، حيث يتعين على المعالج أو المتحكم بالبيانات أن يبلغ صاحب البيانات بالضمانات المناسبة وفقاً للمادة (46)¹⁴² من النظام.¹⁴³ كذلك يتم تحديد الفترة التي سيتم خلالها تخزين البيانات الشخصية، أو

¹⁴² Article 46 Transfers subject to appropriate safeguards:

"1-In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal .."

¹⁴³ منى الأشقر جبور و محمود جبور، المرجع السابق، 2018، ص150.

إذا لم يكن ذلك ممكناً، معرفة المعايير المستخدمة لتحديد تلك الفترة، كما له الحق أيضاً في طلب تصحيح أو مسح البيانات الشخصية لدى المتحكم أو تقييد معالجة البيانات الشخصية المتعلقة بصاحب البيانات أو الاعتراض على هذه المعالجة¹⁴⁴.

وفي السياق نفسه، نجد إن هناك حق آخر منحه المشرع البحريني والمشرع الأوروبي لصاحب البيانات، وهو الحق في الاعتراض على معالجة البيانات، فيكون لصاحب البيانات الاعتراض على معالجة بياناته الشخصية، وفقاً لأسباب مشروعة، فلا يجوز ممارسة هذا الحق دون مبرر مشروع، ولم يحدد كلا المشرعين البحريني والأوروبي المقصود بالمبرر المشروع، وعليه فإن تقدير مدى مشروعية المبرر هي من مسائل الواقع التي تستقل محكمة الموضوع بتقديرها. والهدف من اشتراط مشروعية المبرر هو ألا يتم التوسع في استعمال الحق في الاعتراض، وأي مساس بالحياة الخاصة لصاحب البيانات يعتبر مبرراً مشروعاً للاعتراض على معالجة البيانات. ويمكن ممارسة الحق في الاعتراض في أي وقت، فيمكن أن يتم الاعتراض في مرحلة جمع البيانات، وذلك عن طريق رفض الإفصاح عن البيانات أو في مرحلة لاحقة بعد أن يتم الإفصاح عن البيانات¹⁴⁵. ومن حق صاحب البيانات الاعتراض على استعمال البيانات المتعلقة به لأغراض دعائية وخاصة التجارية منها من قبل المسؤول عن معالجة البيانات، ولا يكون مجبراً على تقديم أي تبرير لذلك، فلكل شخص من حيث المبدأ حق تقرير طريقة استخدام بياناته، بحيث يرفض إدراجها ضمن ملفات إلكترونية معينة، أو نقلها إلى جهات ثالثة. كما له عند طرح الأسئلة عليه بخصوص بياناته الشخصية خلال عملية التجميع أن يرفض الإجابة عنها لكونها غير ملزمة. كذلك له الحق في أن يرفض إعطاء موافقته الخطية التي تعد إلزامية عند معالجة البيانات الحساسة. وله أن يرفض طلب محو بياناته من الملفات ذات الأهداف التجارية. أما بالنسبة للرفض اللاحق بعد عملية المعالجة فيتم ذلك عن طريق الاتصال بمسؤول المعالجة أو التواصل عن طريق البريد الإلكتروني، وعلى المسؤول أن يجيبه خلال مدة يحددها القانون، ولا يمكن أن يبرر تأخيره بالرد بسبب عدم وضوح الطلب المقدم له، أو بأي عذر آخر. فلا بد من أن يرجع المسؤول في هذه

¹⁴⁴ Art. 15 GDPR Right of access by the data subject.

"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 to the personal data and the following information:
the purposes of the processing;
the categories of personal data concerned...."

¹⁴⁵ سامح عبدالواحد التهامي، المرجع السابق، ص 427-428.

الحالة إلى مقدم الطلب لكي يحصل على توضيحات أو معلومات ضرورية لكي يتم بناء الاستجابة على أساسها¹⁴⁶ .

ووفقاً لما سبق أشارت المواد (20-22) من قانون حماية البيانات الشخصية البحريني إلى حق الشخص المعني بالبيانات في الاعتراض على معالجة البيانات لأغراض التسويق المباشر، ومنحته كذلك الحق في الاعتراض على المعالجة التي تُلحق بصاحب البيانات أو غيره ضرراً مادياً أو معنوياً، وأيضاً الحق في الاعتراض على القرارات التي تتم معالجتها آلياً. و استثنى المشرع من ذلك الحالة التي تكون قد تمت فيها المعالجة وفقاً لالتزام قانوني على عاتق صاحب البيانات أو في حال تنازل المسؤول عن المعالجة صراحةً عن ممارسة هذا الالتزام، ما يترتب عليه فقدانه الحق في الاعتراض¹⁴⁷.

أما بالنسبة للنظام الأوروبي العام لحماية البيانات الشخصية فقد منح صاحب البيانات الحق في الاعتراض (Right to object) في المادة (21) منه، وفقاً لحالات محددة، وهي كالآتي¹⁴⁸:

1. لصاحب البيانات الحق في الاعتراض في أي وقت على معالجة بياناته الشخصية، وقد يرفض المتحكمون هذا الاعتراض عندما يظهرون أسباباً مشروعة مقنعة لنشاط المعالجة الذي يتجاوز مصالح صاحب البيانات وحقوقه وحرياته، أو لإنشاء المطالبات أو ممارستها أو الدفاع عنها.
2. لصاحب البيانات الحق في الاعتراض في حالة معالجة البيانات لأغراض التسويق المباشر.
3. الاعتراض على القرارات التي تتم معالجتها آلياً.

¹⁴⁶ منى الأشقر جبور ومحمود الأشقر جبور ، المرجع السابق، ص148.
¹⁴⁷ نعيم السعيداني، حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، مجلة الباحث للدراسات الأكاديمية، المجلد 8، العدد 1، 2021، الجزائر، ص12.

¹⁴⁸ Art. (21) of GDPR. Right to object

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”

4. لصاحب البيانات الحق في الاعتراض عند معالجة البيانات الشخصية لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية، ما لم تكن المعالجة ضرورية لأداء مهمة تم تنفيذها لأسباب تتعلق بالمصلحة العامة¹⁴⁹.

الفرع الثاني: الحق في التصحيح والحجب "Right to rectification"

حرص المشرع الأوروبي في المادة (16) من النظام الأوروبي العام لحماية البيانات الشخصية¹⁵⁰ والمشرع البحريني في المادة (23) من قانون حماية البيانات الشخصية على منح صاحب البيانات، أو كل ذي صفة، الحق في تصحيح البيانات الشخصية غير الدقيقة المتعلقة به أو حجبها أو مسحها، دون تأخير مبرر، في حال كانت البيانات تعالج بالمخالفة لأحكام القانون، أو إذا كانت البيانات غير صحيحة أو ناقصة أو غير محدثة، أو إذا كانت معالجتها غير مشروعة. ويجب أن تتم الاستجابة لطلب صاحب البيانات دون مقابل، ما لم يكن هناك مبرر مقبول قانوناً لعدم الاستجابة من قبل مدير البيانات. ووفقاً للمشرع البحريني يجب أن تكون مدة الاستجابة للطلب خلال عشرة أيام عمل من تاريخ تسلم الطلب، وهذا على خلاف المشرع الأوروبي الذي لم يحدد المدة التي يتعين فيها على معالج البيانات أن يجيب من تخصه البيانات لطلبه، إلا أنه يمكن القول إن معالج البيانات يجب أن يقوم بذلك دون تأخير خلال مدة معقولة¹⁵¹. ومن ناحية أخرى نجد أن المشرع التونسي¹⁵² قد أقر ممارسة هذا الحق في مواجهة السلطات العامة، في المادة (55) منه، حين نص على حق الشخص المعني، أو ورثته، في التقدم بطلب التصحيح، وفرضه كموجب على السلطات العمومية، والجماعات المحلية، والمؤسسات

¹⁴⁹ Art. 89 GDPR Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. "Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place order to ensure respect for the principle of data minimization. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that meaning...."

¹⁵⁰ Art. 16 GDPR Right to rectification

"1-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. 2-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...."

¹⁵¹ منى الأشقر جبور و محمود جبور، المرجع السابق ، ص149.

¹⁵² قانون حماية المعطيات الشخصية التونسي الأساسي، عدد 63، لسنة 2004، مؤرخ في 27 جويلية 2004، منشور في الرائد الرسمي للجمهورية التونسية 30 جويلية 2004 عدد 61 صفحة 2084.

العمومية، التي تعالج بيانات شخصية عائدة للأمن العام، أو الدفاع الوطني، أو الملاحقات الجزائية. وتماشياً مع ما تقدم، تنظر السلطات المذكورة في الطلب المقدم، لتعديل البيانات، أو استكمالها، أو شطبها، في حال تم إعلامها، عن وجود شوائب فيها، وذلك بأية وسيلة تترك أثراً كتابياً.

الفرع الثالث: الحق في النسيان الرقمي

" فكرة الحق في النسيان لا تعتبر جديدة بل حظت باهتمام الشريعة الإسلامية منذ الأزل ، حيث نجد أن الشريعة الإسلامية قسمت النسيان الى نوعين نسيان ترك ونسيان سهو وكذلك نجد أن السنة النبوية مليئة بمثل هذا النوع وأشهرها الحديث النبوي الشريف أن شيخاً عجوزاً جاء إلى النبي صلى الله عليه وسلم فقال " أرأيتَ مَنْ عمل الذنوبَ كُلَّها ولم يتركْ منها شيئاً وهو في ذلك لم يترك حاجةً ولا داجةً إلا أتاها ، فهل لذلك من توبةٍ ؟ قال : فهل أسلمتَ ؟ قال : أما أنا فأشهدُ أن لا إله إلا الله ، وأنتَ رسولُ الله قال : تفعل الخيراتِ ، وتترك السيئاتِ ، فيجعلنَّ الله لك خيراتٍ كُلَّهنَّ قال وغدَرتي وفجَرتي ؟ قال : نعم قال : الله أكبرُ ، فما زال يُكَبِّرُ حتى تَوَارَى . " ¹⁵³ ، بعد ذلك أصبح هناك مسميمات جديدة لهذه الفكرة نتيجة لظهور التطور التكنولوجي والتقني الذي ساهم إلى حد كبير في تطور فكرة الحق في النسيان الرقمي.

ومع تزايد استخدام مواقع التواصل الاجتماعي وتطبيقات إنترنت الأشياء، أصبح النسيان الطبيعي أمراً صعب المنال، لأن معلومات المستخدمين أصبحت تحفظ وتخزن مدة غير محددة، مع إتاحة هذه البيانات والمعلومات في أي مكان في العالم لكل من يريد، ولو كان هناك احتمال في أن تكون ناقصة أو قديمة أو مغلوطة فهي تبقى متاحة على الدوام، ما يصعب على المستخدم مسح وإزالة ماضيه الإلكتروني، وهذا الأمر من شأنه أن يشكل انتهاكاً لخصوصية صاحب البيانات، ويسبب له أضراراً نفسية أو مادية. وهو ما دعا الفكر القانوني إلى البحث عن حلول لهذه المشكلة لحماية خصوصية الأشخاص، ووجد ضالته في مفهوم "الحق في النسيان" في البيئة الرقمية، باعتباره أحد الحقوق المرتبطة بحرمة الحياة الخاصة للإنسان ¹⁵⁴.

أولاً: تعريف الحق في النسيان الرقمي

لقد اختلف الفقه في تحديد مفهوم الحق في النسيان الرقمي الجامع المانع، فمنهم من عرفه التعريف الضيق بأنه "الحق الذي يمنح الأشخاص الوسائل القانونية التي تمكنهم من الحصول على

¹⁵³ الراوي : شطب الممدود أبو الطويل | المحدث : الألباني | المصدر : صحيح الترغيب ص 3164 خلاصة حكم المحدث : صحيح.

¹⁵⁴ حسن عبد الحميد، المرجع السابق ، ص46.

حقهم في النسيان عبر الإنترنت، وذلك من خلال الحد من الاحتفاظ بالبيانات الرقمية الشخصية¹⁵⁵، ومنهم من تبني المفهوم الواسع لهذا الحق وعرفه بأنه "حق يخول الشخص الطبيعي أو الاعتباري مكنة محو معلومة تخصه أو طلب التوقف عن نشرها بعد مرور فترة زمنية"¹⁵⁶.

ونجد أن التعريف الموسع للحق في النسيان قد يُنتقد لأنه يشمل الشخص الطبيعي والاعتباري، إلا أنه أكثر دقة وشمولية وضماناً لحق الأفراد في أن تدخل بياناتهم طبي النسيان، وذلك لإلزامه المسؤول عن المعالجة بمحو هذه البيانات بعد انتهاء الغرض منها¹⁵⁷.

وفي ضوء ما سبق نرى أنه إن كان الحق في النسيان بصورته العامة هو حق الفرد سواء كان شخصاً طبيعياً أو اعتبارياً في بقاء ماضيه محاطاً بسياج من الكتمان وعدم خروجه بعد مرور فترة زمنية معينة إلى العلن، فإنه يقصد به في العالم الرقمي حق الشخص المعني في الحفاظ على خصوصية بياناته الشخصية، فله أن يطلب حذف وإلغاء جميع البيانات على مواقع التواصل الاجتماعي وتطبيقات إنترنت الأشياء وعدم الاحتفاظ بها إلكترونياً خلال فترة زمنية محددة سواء أثناء الاستخدام أو في حالة ترك الموقع أو عدم استخدام التطبيق بشكل نهائي. حيث عادة ما يقوم مدير البيانات بالاحتفاظ بها أطول فترة ممكنة، وهذا يتعارض مع حق الشخص المعني في أن يطلب حذف بياناته أو حسابه الشخصي، لهذا يجب على مدير البيانات أو مقدم الخدمة اتخاذ التدابير اللازمة دون إطلاع باقي المستخدمين على بياناته¹⁵⁸.

ثانياً: طبيعة الحق في النسيان الرقمي

ما إن ظهرت فكرة الحق في النسيان الرقمي إلى العلن بوصفها حقاً يتم الاستناد إليه أمام القضاء من أجل المطالبة بمحو وإزالة البيانات المتاحة على شبكة الإنترنت عبر مختلف مواقعها وخدماتها، حتى تساءل الفقه حول طبيعة هذا الحق، فهل يعتبر هذا الحق وجهاً من أوجه الحياة

¹⁵⁵ معاذ سليمان الملا، فكرة الحق في الدخول في طبي النسيان الرقمي في التشريعات الجزائرية 2 الإلكترونية الحديثة دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائري الكويتي، مجلة كلية القانون الكويتية العالمية - أبحاث المؤتمر السنوي الدولي الخامس 9 - 10 مايو 2018، ص 119.

¹⁵⁶ الزين بوخلوط، الحق في النسيان الرقمي، مجلة العلوم الإنسانية - جامعة محمد خيضر بسكرة، العدد 46، جامعة عنابة، الجزائر، 2017، ص 335.

¹⁵⁷ بشيخ محمد حسين وبن ديدة نجا، الحق في النسيان كآلية لحماية المعطيات الشخصية، مجلة القانون العام الجزائري والمقارن، المجلد الثامن، العدد 01، الجزائر، 2022، ص 569.

¹⁵⁸ محمد عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، مصر، 2020، ص 68-69.

الخاصة؟ أم أن له من الخصائص والمقومات ما يجعله ينفرد بخصوصيات تتأى به عن كل الحقوق المعروفة سلفاً فيعتبر مستقلاً عنها؟ وانقسم الفقهاء في إجابتهم عن هذا التساؤل إلى مذهبين، على النحو الآتي:

1. الاتجاه الأول: الحق في النسيان الرقمي أحد عناصر الحق في الحياة الخاصة

يرى أنصار هذا الرأي أن الحق في النسيان الرقمي هو حق مرتبط بالحياة الخاصة وعنصر من عناصرها، ومن شأن ذلك أن يتسع ليشمل كل العناصر الشخصية حتى لو كانت البيانات عامة، وهذا على اعتبار أن ما كان عامًا من بيانات تم نشرها في السابق سيصبح في المستقبل من قبيل الأسرار ويدخل في طي النسيان وذلك بعد مرور فترة زمنية عليه¹⁵⁹. وفي حالة تم الكشف والإعلان عن هذه الأسرار سوف يشكل هذا اعتداءً واضحاً على الحياة الخاصة للأشخاص وهذا مجرم قانوناً، كما أن الحق في النسيان لا يعد مستقلاً عن الحياة الخاصة كاستثناء، إلا بالنسبة لوقائع الحياة العامة، فيمكن نشرها دون إذن باعتبارها تخدم المصلحة العامة ونشر الخصوصية في حالة الوفاة¹⁶⁰.

وقد تبني القضاء الفرنسي هذا التوجه عندما قضت محكمة باريس الابتدائية في الحكم الصادر في 15 فبراير 2012 في قضية تتلخص وقائعها في وجود مقطع فيديو قديم حدد فيه هوية الشاكية، وذلك بسبب قيام شخص مجهول بنشر هذا المحتوى على مواقع إباحية، وظهر لها ذلك من خلال نتائج البحث في محرك البحث Google، الأمر الذي تسبب لها في ضرر لحياتها وعملها، فطالبت المدعية محرك البحث Google بإلغاء فهرسة المحتوى، ورفض الأخير مسبباً ذلك بعدم تمتعه بالصلاحية لإدارة المحتوى، في حين أن المحكمة وجدت أن محرك البحث Google قد ساهم في وقوع هذا الضرر، وسببت المحكمة قرارها أنه من حق المدعية أن تنسى ما مضى من حياتها¹⁶¹.

2. الاتجاه الثاني: الحق في النسيان الرقمي هو حق مستقل

¹⁵⁹ أيمن عبدالله فكري، جرائم نظام الحاسوب، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007، ص 89.

¹⁶⁰ فيصل بن وقليل، الحماية الجنائية للحق للدخول في طي النسيان الرقمي، دراسة مقارنة بين التشريع الجزائري والفرنسي، جامعة يحيى فارس (المدينة)، المجلد 08، العدد 01، الجزائر، 2020، ص 733.

¹⁶¹ حكم محكمة باريس الابتدائية في 15 فبراير 2012، ديانا ومحرك قوقل، مشار له لدى: أمين الخنتوري، معالم تنظيم الحق في النسيان الرقمي في التشريع المغربي، جامعة سيدي محمد بن عبدالله بن فاس، مجلة الصدى للدراسات القانونية والسياسية، العدد الخامس، المغرب، 2020، ص 34. وللاطلاع على الحكم باللغة الفرنسية راجع: [Legalis | L'actualité du droit des nouvelles technologies | Tribunal de grande instance de Paris Ordonnance de référé 15 février 2012](https://www.legalis.fr/actualite/nouvelles/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-15-fevrier-2012)

على الرغم من أنهما قد يتطابقان معا في حالة عدم موافقة صاحبيهما، إلا إنهما يختلفان من حيث البعد الزمني ومن حيث النطاق الموضوعي. فمن حيث البعد الزمني فإن الحق في الخصوصية لا يقتصر فقط على الوقائع الحديثة، بل أيضا يشمل الوقائع التي مر عليها فترة من الزمن. أما من حيث الطبيعة أو النطاق الموضوعي فإن الحق في النسيان يعد أكثر اتساعا من الحق في الحياة الخاصة، فالأول يدخل ضمنه الوقائع والأحداث سواء كانت عامة أو خاصة أو سرية¹⁶². وهذا يعكس الهدف من الحق في النسيان ألا وهو حماية الهوية الإنسانية. أما بالنسبة للحق في الحياة الخاصة فإنها لا تتعلق بالوقائع أو الأحداث العامة لأن صفة الخصوصية في هذه الحالة سوف تنتفي لنشرها مسبقا على الجمهور سواء تم ذلك بناء على موافقة أصحابها أو لأسباب مرتبطة بالمصالح العامة كالحقائق المتعلقة بالجرائم والقضايا والأحداث التاريخية¹⁶³.

ومن جانبنا نميل إلى رأي المذهب الثاني ونرى إن الحق في النسيان يعد بمثابة حق مستقل عن الحق في الحياة الخاصة شأنه شأن الحقوق الشخصية الأخرى، وهذا استنادا للتبريرات التي أخذ بها هذا المذهب وهي أنه لا يجوز الاستناد إلى وقائع مضى عليها مدة معينة طواها الزمن. كذلك نرى أن فكرة الحق في الحياة الخاصة بدأت تنحسر؛ وذلك بسبب التطورات الرقمية والتكنولوجيا التي تطلبت منا كمستخدمين الكشف عن بياناتنا الشخصية من أجل الحصول على الخدمات المختلفة عبر شبكة الإنترنت. الأمر الذي جعل مسألة تحكم المستخدمين ببياناتهم أكثر صعوبة وقد تكون مستحيلة، وذلك بسبب نشر البيانات على الإنترنت وتداولها عن طريق تطبيقات تقنية المعلومات، وبالتالي يصبح أمر محوها أو حذفها أمرا صعبا.

ثالثا: موقف المشرع الأوروبي والبحريني من الحق في النسيان الرقمي

لقد حظي الحق في النسيان الرقمي باهتمام بالغ في أوروبا، وعرف ظهورا واسعا خاصة بعد صدور حكم محكمة العدل الأوروبية الصادر بتاريخ 13 مايو 2014 في قضية (ماريو

¹⁶² محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، 2005، ص218.

¹⁶³ عبدالهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الإنترنت، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2013، ص76.

كوستيغا) ضد (محرك البحث غوغل إسبانيا)¹⁶⁴. ولقد أكدت المحكمة في هذا الحكم على أنه وفقاً لشروط معينة، يحق للشخص الطبيعي أن يطلب من محرك البحث إزالة نتائج البحث المتعلقة ببياناته في حال كانت غير دقيقة وقديمة، حتى لو كان المحتوى صحيحاً ومنشوراً بشكل قانوني، طالما كانت هناك رغبة لدى الشخص في نسيانها. فضلاً عن ذلك، فقد أكد هذا الحكم على إنه على الشخص أن يتقدم بطلبه في المقام الأول إلى محرك البحث، ويجب على الأخير النظر في طلب رفع اسمه من عمليات البحث على النحو الواجب على أساس موضوعي، وفي حالة عدم الاستجابة لطلبه فإن على السلطة الإشرافية أو القضائية في الدولة العضو تحديد التدابير التي يجب اتخاذها¹⁶⁵.

وكان الحكم السابق هو الدافع الرئيس لقيام المشرع الأوروبي باستبدال اللائحة رقم 95/46 بالتوجيه رقم 679/2016، والذي أصبح ساري المفعول بتاريخ 28 مايو 2018، حيث اعترف المشرع الأوروبي صراحة بحق الفرد في أن يطالب بحذف بياناته الشخصية من قبل المسؤول عن المعالجة دون تأخير غير مبرر، متى كانت البيانات غير ضرورية أو تم الانتهاء من معالجتها¹⁶⁶. وبموجب المادة (17) من النظام الأوروبي العام لحماية البيانات الشخصية الذي أطلق عليه عنوان الحق في النسيان أو الحق في المحو (Right to be forgotten or Right to erasure)، نلاحظ أن النظام الأوروبي العام لم يجعل الحق في المحو حقاً مطلقاً بل قيده بضرورة توافر حالة من الحالات المنصوص عليها في الفقرة الأولى من المادة نفسها، وهي كما يأتي:¹⁶⁷

الحالة الأولى: إذا لم تعد البيانات الشخصية ضرورية لتحقيق الأغراض التي تم تجميع البيانات لأجلها. ووفقاً لهذا النص يجوز لصاحب البيانات أن يطلب من محرك البحث تتبع البحث

¹⁶⁴ C-131/12 Google Spain v AEPD and Mario Costeja González

¹⁶⁵ الصالحين محمد العيش، التنظيم القانوني لاستخدام البيانات الشخصية في الإعلام الجديد، مجلة الحقوق، العدد 2، المجلد 13، كلية الحقوق جامعة بنغازي، ليبيا، (لا يوجد سنة)، ص 17.

¹⁶⁶ معاذ سليمان الملا، المرجع سابق، ص 122.

167 Art. 17 GDPR Right to erasure ('right to be forgotten')

"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:

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
2. 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;....."

الذي تم إجراؤه على أساس اسمه وإزالة المحتوى من نتائج البحث الخاصة به، وهذا في حالة أصبحت البيانات غير ضرورية فيما يتعلق بأغراض المعالجة بواسطة محرك البحث.

الحالة الثانية: إذا قام الفرد صاحب البيانات بسحب رضاه على عملية المعالجة التي تم تأسيسها عليه وفقاً للمادتين 6 (1) و 9 (2) من النظام، إلا إذا كان هناك أساس قانوني آخر للمعالجة. وفي هذه الحالة من حق صاحب البيانات طلب الإزالة بأنه لم يعد يوافق على المعالجة التي يقوم بها مشغل المحرك البحث لبياناته الشخصية؛ لأنه من الناحية العملية يجب على مشغل المحرك أن يطلب من صاحب البيانات موافقته الصريحة قبل معالجة البيانات لأغراضه الشخصية.

الحالة الثالثة: ممارسة صاحب البيانات حقه في الاعتراض على معالجة بياناته الشخصية وفقاً للفقرتين (1،2) من المادة (21) من النظام الأوروبي العام لحماية البيانات الشخصية. حيث منح المشرع الأوروبي صاحب البيانات وفقاً للفقرة (1) من المادة حق الاعتراض لأسباب تتعلق بوضعه الخاص، في أي وقت على معالجة بياناته الشخصية والتي تستند إلى النقطة (هـ) أو (و) من المادة (6) اللتين تتعلقان بما يأتي:

1. أن تكون المعالجة ضرورية للمصلحة العامة أو ضمن نطاق الممارسة الرسمية المخولة للمراقب أو طرف ثالث.

2. عندما تكون المعالجة ضرورية لأغراض المصالح المشروعة التي ينتهجها المراقب أو طرف ثالث دون إهدار للحقوق والحريات الأساسية لصاحب البيانات التي تتطلب حماية البيانات الشخصية، وخاصة إذا كان صاحب البيانات طفلاً. ولا ينطبق هذا الحكم على المعالجة التي تقوم بها السلطات العامة في أداء مهامها.

وأما بالنسبة للفقرة الثانية من المادة (21)، فعند معالجة البيانات الشخصية لأغراض التسويق المباشر، يكون لصاحب البيانات الحق في الاعتراض في أي وقت على معالجة البيانات الشخصية الخاصة به في مثل هذا التسويق، والتي تشمل التمييز إلى الحد الذي ترتبط به هذه المعلومات مباشرة بالتسويق¹⁶⁸.

¹⁶⁸ Art. 21 GDPR Right to object

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. 2The 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...”.

وبناءً على ما سبق عندما يقدم صاحب البيانات طلباً لإزالة البيانات الخاصة به لمزود محرك البحث، فاستناداً للحالة الخاصة بصاحب البيانات، يجب على مزود محرك البحث أن يوافق على هذا الطلب فوراً ما لم يكن بإمكانه أن يظهر أسباباً مشروعة ملحة للإدراج في نتائج البحث، وهي أسباب تتخطى المصالح المشروعة والحريات الخاصة لصاحب البيانات. فتتم الموازنة بين الأسباب المتعلقة بالحالة الخاصة بصاحب البيانات والمبررات القانونية المقنعة لمزود محرك البحث

الحالة الرابعة: إذا كانت عملية معالجة البيانات غير مشروعة وفقاً للأسس التي بينها النظام بشأن مشروعية المعالجة التي سبق توضيحها. وبالعودة إلى المادة (5) من النظام الأوروبي العام لحماية البيانات الشخصية نجدها قد نصت على أنه يجب أن تتسم معالجة البيانات الشخصية بالمشروعية والإنصاف والشفافية. وكذلك بالعودة إلى المادة (6) من النظام، نجد أنها حددت الحالات التي تتم فيها المعالجة القانونية، وبذلك تكون معالجة البيانات غير قانونية إذا رفض صاحب البيانات معالجة بياناته، أو في حال كانت المعالجة غير ضرورية للامتثال لالتزام قانوني يخضع له المراقب، أو إن المعالجة غير ضرورية لحماية المصالح الحيوية، أو إنها غير ضرورية لأداء مهمة تتم للمصلحة العامة أو لأغراض المصالح المشروعة التي ينتهجها المراقب أو طرف ثالث.

الحالة الخامسة: إذا كان هناك التزام قانوني وفقاً للقانون الاتحادي أو قوانين الدول الأعضاء التي يخضع لها المراقب تفرض على المراقب إزالة البيانات الشخصية، وينشأ الالتزام القانوني نتيجة أمر قضائي أو طلب صريح لمحو البيانات، أو يكون هناك خرق من قبل صاحب البيانات فيما يتعلق بفترة الاحتفاظ بالبيانات، حيث يتم تحديد فترة للاحتفاظ بها عن طريق النص ويتم عدم الالتزام به.

الحالة السادسة: إذا كانت المعالجة على أساس الفقرة (1) من المادة (8) من النظام والتي تتعلق بمعالجة البيانات الخاصة بالأطفال. حيثما تنطبق الفقرة (أ) من المادة (6) / 1 من النظام والتي تنص على أن معالجة البيانات لا تكون قانونية إلا إذا وافق صاحب البيانات على معالجة بياناته لغرض محدد أو أكثر. أما فيما يتعلق بعرض خدمات مجتمع المعلومات على الطفل مباشرة، فيجب أن تكون البيانات الشخصية للطفل مشروعة بحيث يكون عمر الطفل ستة عشر سنة على الأقل، وإذا كان عمر الطفل أقل من ستة عشر عاماً، فإن المعالجة لن تكون مشروعة للبيانات إلا إذا منح المباشرة للمسؤولية الأبوية الموافقة أو التصريح، كما يجوز للدول الأعضاء أن تنص على سن أقل للأغراض بشرط ألا يقل عن ثلاثة عشر سنة.¹⁶⁹

¹⁶⁹ Art. 8 GDPR Conditions applicable to child's consent in relation to information society services

” 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

ومن خلال ما تقدم يمكن القول إن نص المادة السابق يعكس تشدد المشرع الأوروبي في توفير الحماية للأطفال في البيئة الرقمية، وبناءً على هذا يجب على محررات البحث أن تمنح أهمية لكل طلب يتعلق بالمحو إذا كانت معالجة البيانات تستند إلى الموافقة المقدمة من الطفل، كما تجب مباشرة هذا الأمر في حال لم يعد صاحب البيانات طفلاً، لأن الطفل لم يكن على دراية كاملة بالمخاطر التي تنطوي عليها المعالجة في وقت المعالجة.

ونلاحظ هنا إن الحالات السابقة التي أوردناها والمتعلقة بطلب محو البيانات والتي حددتها المادة (17) فقرة (1) من النظام الأوروبي العام لحماية البيانات الشخصية وردت على سبيل الحصر، فلا يجوز مطلقاً محو البيانات إلا إذا توافرت إحدى الحالات السابقة. كما يمكن تقديم طلب المحو إلى مزود محرك البحث لكي يقوم بدوره بمحو البيانات.

وفي الإطار نفسه قررت الفقرة (2) من المادة (17) أنه إذا كان مراقب البيانات قد عمل على جعل البيانات الشخصية عامة أو متاحة للجمهور، وجب عليه -فضلاً عن الالتزام بمحوها- في ضوء التكنولوجيا المتاحة والتكاليف المعقولة، اتخاذ ما هو ضروري بما في ذلك التدابير التقنية اللازمة، بغية إخطار المراقبين الآخرين الذين يقومون بمعالجة البيانات بإزالة بياناته الشخصية، بمعنى إزالة هذه البيانات والروابط التي تساهم في الوصول إليها فضلاً عن كل ما من شأنه تكرار إتاحة البيانات الشخصية مرة أخرى¹⁷⁰. ونصت الفقرة الثالثة من المادة نفسها على تعطيل الالتزام بمحو البيانات في حال توافرت القيود التي تبرر الاحتفاظ بالبيانات الشخصية، وهذا عندما تكون معالجة البيانات ضرورية، كما لا يسري على هذه الحالات ما جاء في الفقرة (1) والفقرة (2) من المادة نفسها، وهذه الحالات هي كالآتي:¹⁷¹

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 authorized by the holder of parental responsibility over the child.”

¹⁷⁰“Art. 17 GDPR Right to erasure (‘right to be forgotten’)

2- Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.....”

¹⁷¹ Art. 17 GDPR Right to erasure (‘right to be forgotten’)

“Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

for exercising the right of freedom of expression and information;

for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;..”

for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or....”

الحالة الأولى: عندما تكون المعالجة ضرورية لممارسة الحق في حرية التعبير والوصول إلى المعلومات، وهو ما يعكس التخوفات التي أبدتها النظام الأوروبي العام لحماية البيانات الشخصية فيما يتعلق بمدى تأثير الحق في المحو على الحق في حرية التعبير والوصول إلى المعلومات، وبالتالي كان يجب على النظام الأوروبي العام لحماية البيانات الشخصية مواجهة هذه المخاوف عند صياغته لنص الفقرة (1) من المادة (17) التي تتعلق بالحالات المستثناة من تطبيق الحق في المحو، حيث نص على أنه إذا توافرت الشروط المنصوص عليها في هذه المادة فإنه يتعين على المتحكم في البيانات أن يلتزم بحذف البيانات الشخصية دون تأخير لا مبرر له، وعلى الرغم من ذلك فإن التوازن بين حماية حقوق الأطراف المعنية وحرية التعبير بما في ذلك حرية الوصول إلى المعلومات هو أمر جوهري في نص المادة (17).

وبالرجوع إلى حكم محكمة العدل الأوروبية في قضية (Google Spain)، نجد أن المحكمة قد سعت لتحقيق هذا التوازن، وذلك من خلال ما ذكرته في حيثيات الحكم من أن المعالجة التي يجريها مزود الخدمة يمكن أن تؤثر بشكل كبير على الحقوق الأساسية للخصوصية وقانون حماية البيانات عند إجراء البحث بواسطة اسم صاحب البيانات. وقامت المحكمة أيضا بذكر مجموعة من المعايير التي توضح الموازنة بين كل من الحق في الخصوصية والحق في الوصول إلى المعلومات وحرية التعبير، ومنها طبيعة المعلومات المراد محوها وحساسيتها بالنسبة للحياة الخاصة لصاحب البيانات وتأثيرها على مصلحة الجمهور في الحصول على المعلومات، وهي تختلف بحسب الدور الذي يلعبه صاحب البيانات في الحياة العامة.

كما نص النظام الأوروبي العام لحماية البيانات الشخصية بدوره على ضرورة تحقيق الموازنة بين الحق في البيانات الشخصية والحقوق الأخرى في المادة (4) من النظام، حيث يتعين أن تكون معالجة البيانات الشخصية مصممة لخدمة البشرية، كما إن الحق في حماية البيانات الشخصية لا يعد حقا مطلقا، وإنما يجب أن ينظر إليه وفقا لمبدأ التناسب فيما يتعلق بوظيفته في المجتمع، وأن يكون متوازنا مع الحقوق الأساسية الأخرى، كما يحترم النظام ويراعي جميع الحريات والحقوق والمبادئ المعترف بها في المواثيق والمعاهدات بما في ذلك حرية التعبير، والمعلومات وحرية ممارسة الأعمال التجارية والمحاكمة العادلة والتنوع الثقافي والديني واللغوي.

كذلك نص النظام الأوروبي العام لحماية البيانات الشخصية على حكم مهم في المادة (85) التي جاء فيها:

1. الدول الأعضاء تسهر على الحق في حماية البيانات الشخصية مع الحق في حرية التعبير والمعلومات، بما في ذلك المعالجة للأغراض الصحفية أو الأكاديمية أو التعبير الفني أو الأدبي.

2. على الدول الأعضاء أن تنص على إعفاءات أو استثناءات متى ما كانت المعالجة ضرورية للأغراض الصحفية أو الأكاديمية أو للتعبير الفني أو الأدبي، وذلك بقصد الموازنة بين الحق في حماية البيانات الشخصية والحق في حرية التعبير والمعلومات.
3. كل دولة عضو يجب أن تخطر اللجنة بأحكام قانونها أو أي تعديل عليه دون إبطاء¹⁷².

المعلومات قد أكدته مجموعة من الأحكام القضائية السابقة على صدور الحكم في قضية (Google Spain)، كما أكد النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) الموازنة بين الحق في حماية البيانات الشخصية والحقوق الأخرى من خلال النص صراحة على ذلك، وهذا عن طريق إعطاء كل دولة عضو في الاتحاد الأوروبي الحق في أن تنص في قوانينها على استثناءات أو إعفاءات لأغراض صحفية أو أكاديمية أو لأغراض التعبير الفني أو الأدبي.

الحالة الثانية: الامتثال للالتزام قانوني يتطلب معالجة البيانات بموجب قانون الاتحاد أو قانون الدول الأعضاء الذي يخضع له المراقب أو لأداء مهمة تتم للمصلحة العامة أو في ممارسة السلطة الرسمية للمراقب. و وفقاً للفقرة (1) من المادة (6) من النظام الأوروبي العام لحماية البيانات الشخصية لا تكون المعالجة قانونية إلا إذا كانت ضرورية للامتثال للالتزام قانوني يخضع له المراقب، وأن تكون المعالجة ضرورية لأداء مهمة تتم للمصلحة العامة أو ضمن السلطة الرسمية المخولة للمراقب، ثم بعد ذلك نصت في الفقرة (3) من المادة على أن أساس المعالجة المشار إليها يحدد وفقاً لقانون الاتحاد أو قانون الدول الأعضاء الذي يخضع له المراقب¹⁷³. وعند النظر إلى خصائص مزودي محركات البحث نجد أنه من غير المرجح أن يتم منحهم من قبل الدول الأعضاء صفة السلطات العامة، أو أن يُعتبر نشاطهم أو جزءاً منه ضرورياً لتحقيق مصلحة عامة قانونية. وعلى الرغم من ذلك وفي حال منح قانون أي من الدول الأعضاء لمحركات البحث صفة السلطة العامة أو ربط نشاطها بتحقيق مصلحة عامة، فإنهم في هذه الحالة يستفيدون من الاستثناء المنصوص عليه في المادة (17) فقرة (3) (ب) من النظام الأوروبي العام لحماية البيانات

¹⁷² Art. 85 GDPR Processing and freedom of expression and information

"Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.."

¹⁷³ Art. 6 GDPR Lawfulness of processing

"1-Processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes; 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..."

الشخصية ويستلزم لتطبيق الاستثناء أن يتم تحديد ما إذا كان الحفاظ على المعلومات في نتائج البحث ضروريا لتحقيق المصلحة العامة.

الحالة الثالثة: أسباب تتعلق بالمصالح العامة في مجال الصحة العامة

لقد استتنت المادة (17) (3) من النظام الأوروبي العام لحماية البيانات الشخصية الالتزام بمحو البيانات الشخصية المتعلقة بالمصلحة العامة في مجال الصحة العامة. وبالرجوع إلى المادة (9) من النظام الأوروبي العام لحماية البيانات الشخصية نجد أنها حظرت معالجة فئات خاصة من البيانات الشخصية:

- البيانات التي تكشف عن الأصل العرقي أو المعتقدات الدينية.
 - البيانات المتعلقة بالصحة وغيرها.
- إلا أن الفقرة (2) من المادة أوضحت أن الحظر على معالجة بعض البيانات الشخصية، التي من بينها البيانات الصحية:
- لا ينطبق في حالة كانت المعالجة ضرورية لأغراض الطب الوقائي أو المهني، لتقييم القدرة على العمل للموظف والتشخيص الطبي، وأيضا توفير الرعاية الصحية أو الرعاية الاجتماعية أو العلاج وخدمات الرعاية الصحية أو الاجتماعية على أساس قانون الاتحاد أو الدول الأعضاء أو بموجب عقد مع اختصاصي صحي.
 - لا ينطبق حظر معالجة البيانات الصحية في حالة كون المعالجة ضرورية لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة، مثل ضمان سلامة وجودة الرعاية الصحية والمنتجات والأجهزة الطبية على أساس الاتحاد أو قانون الدول الأعضاء الذي يحتوي على تدابير محددة ومناسبة لحماية حقوق وحرقات صاحب البيانات وخاصة السرية المهنية¹⁷⁴.

ومن ناحية أخرى فقد أوضحت الفقرة (45) التمهيدية من النظام الأوروبي العام لحماية البيانات الشخصية إن معالجة البيانات الشخصية قد تكون ضرورية في بعض

¹⁷⁴ Art. 9 GDPR Processing of special categories of personal data

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.

Paragraph 1 shall not apply if one of the following applies:

الحالات لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة دون موافقة صاحب البيانات، وفي هذا الشأن أوضحت أنه يجب تفسير مصطلح الصحة العامة وفقا لما تم النص عليه في اللائحة رقم 1338 لسنة 2008 أي جميع العناصر التي تتعلق بالصحة والتي تشمل الحالة الصحية، بما في ذلك العجز واحتياجات الرعاية الصحية والموارد المخصصة للرعاية الصحية والإنفاق على الرعاية الصحية وتمويلها.

الحالة الرابعة: لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية.

نصت المادة (17) (3) من النظام الأوروبي العام لحماية البيانات الشخصية على حماية البيانات الشخصية لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية، ووفقا للمادة (17) فقرة (1) يحق لصاحب البيانات أن يحصل من المراقب على حق محو البيانات الشخصية الخاصة به دون تأخير لا مبرر له.

وبالعودة إلى نص الفقرة (1) من المادة (89) نجد إنها قد نصت على أن تخضع عملية أغراض الأرشفة للمصلحة العامة، أو لأغراض البحث العلمي أو التاريخي، أو الأغراض الإحصائية للضمانات المناسبة وفقا لهذا النظام، وتضمن هذه الضمانات وجود تدابير تقنية وتنظيمية على وجه الخصوص من أجل ضمان احترام مبدأ "تقليل البيانات" (Data minimization)¹⁷⁵ إلى الحد الأدنى.

ووفقا لهذا الاستثناء يجب على مزود محرك البحث أن يكون قادراً على إثبات محتوى معين على صفحة النتائج، الذي قد يمثل عقبة أمام تحقيق أغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية، وفي هذه الحالة يتم إعفاؤه من محو البيانات.

الحالة الخامسة: إنشاء المطالبات القانونية أو ممارستها أو الدفاع عنها.

من غير المحتمل أن يستخدم مزود محرك البحث هذا الإعفاء لرفض الطلبات المقدمة لهم لمحو البيانات، وخاصة أن طلب المحو يعني منع نتائج البحث التي يقدمها موفر محرك البحث عند استخدام اسم صاحب البيانات عادة كمعيار للبحث، ولكن تبقى المعلومات متاحة عند استخدام مصطلحات أخرى للبحث عنها.

¹⁷⁵ يحد مبدأ تقليل البيانات من المبادئ المهمة في النظام الأوروبي العام لحماية البيانات، ويقصد به أنه يتعين على الشركات قصر جمع البيانات الشخصية وتخزينها واستخدامها على البيانات ذات الصلة الملائمة والضرورية لتنفيذ الغرض الذي تتم معالجة البيانات من أجله.

وعلى غرار المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية، حظي الحق في النسيان باهتمام المشرع البحريني وعالجه تحت مسمى الحق في المسح. حيث نص المشرع البحريني على هذا الحق صراحة في المطالبة بالتصحيح والحجب والمسح، وذلك في المادة (23) من قانون حماية البيانات الشخصية، وذلك إذا كانت معالجة البيانات المطلوب مسحها قد تمت بالمخالفة لأحكام القانون وتكون المعالجة كذلك على وجه الخصوص :

1- إذا كانت البيانات التي تمت معالجتها غير صحيحة مثلا إذا كان يوجد خطأ في بياناته الأسمية أو مهنته أو بيانات تضر في سمعته فيحق لصاحب البيانات في هذه الحالة أن يطالب بتصحيحها أو حجبها أو المسح.

2- إذا كانت البيانات ناقصة في هذه الحالة من حق صاحب البيانات أيضا أن يطالب بإدخال تعديل على هذه البيانات لكي يتم تصحيحها وبالتالي حتى لا يؤثر هذا النقص على مصلحة صاحب البيانات ويلحق به الضرر.

3- إذا كانت البيانات غير محدثة مثلا في حال صدر عليه حكم قضائي بالعفو أو البراءة ولم تحدث بياناته على هذا الأساس بل لازالت البيانات قديمة تفيد بأنه عليه حكم في السجن هذا ممكن أن يشكل له ضرراً في حال إراد التقديم على وظيفة معينة .

4- إذا كانت البيانات غير مشروعة مثلا تكون البيانات تتعلق بمواد إباحية لشخص ما وهذا الشخص سوف يتضرر على المدى البعيد منها سوف تؤثر على سمعته فمن حق صاحب البيانات في هذه الحالة المطالبة بمسح هذه البيانات لعدم مشروعيتها.

ويجب على مدير البيانات في حال لم يكن لديه سبب مقبول قانونا، أن يوافق على طلب محو البيانات دون مقابل، ويكون ذلك خلال عشرة أيام من تاريخ تقديم الطلب.

واستثنى المشرع البحريني من حكم المادة السابقة السجلات التي تكون متاحة للجمهور للاطلاع عليها، وذلك في حال تطلب القانون المنشئ للسجل إجراءات معينة للتصحيح أو الحجب أو المسح. كما بينت المادة عدم جواز معالجة البيانات التي يتم حجبها، إلا بموافقة من صاحب البيانات أو لغرض الإثبات أو لحماية حقوق طرف ثالث. وحدد المشرع البحريني مدة (15) يوما يتعين خلالها على مدير البيانات من تاريخ استجابته كليا أو جزئيا لطلب قدم إليه، أن يخطر أي طرف ثالث أفصح له عن تلك البيانات عن التصحيح أو المسح أو الحجب الذي تم نتيجة الطلب، ما لم يكن متعذرا ولا يمكن تحقيقه بحسب الأحوال.

ومن خلال ما سبق نجد أن قانون حماية البيانات الشخصية البحريني لم يتبنى صراحة مسمى (الحق في النسيان الرقمي)، وهو المصطلح الذي تبناه النظام الأوروبي العام، ولكن هذا لا ينفي وجود الحق كفكرة قانونية ، و حماية للحق في خصوصية البيانات الشخصية وتماشيا مع مسلك المشرع الأوروبي حرص المشرع البحريني على إصدار قانون حماية البيانات الشخصية رقم (30) لسنة 2018، وعالج مضمون الحق في النسيان الرقمي في نصوصه، فمنح مجموعة من الحقوق لصاحب البيانات عند معالجة بياناته تحت مسمى (الحق في المسح)، ومنها الحق في الحجب والحذف والتصحيح والحق في المسح، ومن خلال ذلك نرى أنه كان من الأجدر أن ينص على الحق في المسح صراحة ويفصل في أحكامه، على اعتبار أنه أصبح من الحقوق الأساسية الرقمية الحديثة، والتي تبلورت أهميتها خاصة في ظل التطور الرقمي الذي نشهده.

وأما فيما يتعلق بالقيد المذكور في الفقرة (2) من المادة (17) من النظام الأوروبي العام لحماية البيانات الشخصية، وهو قيد الأخذ بالتكنولوجيا عند طلب محو البيانات الشخصية من قبل مراقب البيانات، فنجد أنه على غرار المشرع الأوروبي أخذ المشرع البحريني بهذا القيد وذلك لمواكبة التطورات التكنولوجية والرقمية في اتخاذ أحدث التدابير الفنية والتقنية التي تكفل الحماية المناسبة للبيانات الشخصية ، حيث نص المشرع البحريني في المادة (8) من قانون حماية البيانات الشخصية تحت عنوان أمان المعالجة ، على أنه يجب على مدير البيانات أن يطبق التدابير الفنية والتنظيمية الكفيلة بحماية البيانات. ويجب أن تكفل هذه التدابير توفير مستوى مناسب من الأمان بمراعاة ما وصلت إليه أحدث أساليب الحماية التقنية، وعلى الرغم من هذا ، فعند الرجوع إلى الفقرة (2) من المادة (17) من النظام نجد أن المشرع الأوروبي منح مدير البيانات إستثناء لم ينص عليه المشرع البحريني وهو إمكانية عدم محو بياناته إذا كانت الإمكانات التكنولوجية غير متاحة في الحالة التي تكون فيها المعالجة ضرورية أما لممارسة الحق في حرية التعبير والإعلام، أو الامتثال لالتزام قانوني يتطلب المعالجة بموجب قانون الاتحاد أو قانون الدول، أو لأداء مهمة يتم تنفيذها للمصلحة العامة أو في ممارسة السلطة الرسمية المخولة للمراقب، أو لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة، ولأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي، أو عند إنشاء المطالبات القانونية أو ممارستها أو الدفاع عنها.

رابعا: إشكاليات الحق في النسيان الرقمي

إن التطبيق العملي للحق في النسيان الرقمي يواجه العديد من الإشكاليات العملية، إذ قد تكون المعلومات المتاحة على صفحة خاصة بمستخدم آخر له الحق في حرية التعبير على صفحته والاحتفاظ بالمعلومات ضمن حق حماية الحق في التعبير، فلا يجوز في هذه الحالة إجبار الشخص على إزالة البيانات التي تم وضعها من قبل بعض متابعيه، على الرغم من وجود بعض المواقع التي تمنح المستخدم إمكانية حذف بياناته أو ما قام بوضعه على صفحة مستخدم آخر طالما وافق هذا المستخدم على منح خاصية الحذف للمتابعين عند بداية الاشتراك مثل الفيسبوك، وهذا على خلاف مواقع التواصل الاجتماعي الأخرى التي تستلزم موافقة صاحب الصفحة التي تم وضع البيانات عليها أو منها ما يسمح بحذفها ولا يراها إلا صاحبها فقط، وتبقى موجودة على الصفحة المملوكة للغير. كما أن هناك إشكالية أخرى متعلقة بالبيانات الشخصية الخاصة بالشخص غير المستخدم لمواقع التواصل الاجتماعي وهي وجود تعارض بين الحق في النسيان الرقمي مع الحق في الاحتفاظ بالبيانات؛ فقد لا يملك المستخدم منع المستخدمين الآخرين من القيام بالبحث عما يبيده من آراء طالما وافق في البداية على علانية النشر. فإذا ما كان يسمح بهذا الحق للجميع من رؤية بياناته ومنشوراته فلا يجوز بعد علانيتها وتعلق بعضها بحق شخص آخر في التعبير أن يطلب حذفها. حيث إنه من ناحية يعتدي على الحق في التعبير وحرية الرأي، ومن ناحية أخرى يكلف شركات التواصل الاجتماعي جهداً فائداً وتكلفة مالية عالية للبحث عن المعلومات المطلوب حذفها¹⁷⁶.

ومن المواقع التي تعمل على الموازنة بين الحق في النسيان والحق في التعبير عن الرأي موقع تويتر، حيث يقوم عند إلغاء المستخدم حسابه بوقف الوصول إلى بيانات المستخدم فوراً ويمحوها خلال ثلاثين يوماً والتي يمكن خلالها إعادة تفعيل الحساب ويلتزم موقع فيسبوك بمحو جميع المعلومات العائدة إلى الحساب الملغى خلال 90 يوماً، ولكن تبقى بعض المعلومات عن المستخدم الذي ألغى حسابه وهي تلك المنسوخة أو الظاهرة على حسابات أخرى أو البيانات المجمعة عنه خارج إطار حسابه¹⁷⁷.

ونحن نؤيد تبني التشريعات العربية للحق في النسيان الرقمي بصورة صريحة، ذلك إن التقدم العلمي والتكنولوجي المتسارع وتزايد استخدام تطبيقات إنترنت الأشياء أتاحت الفرصة للاطلاع على البيانات الشخصية وتبادلها، كما أصبحت البيانات الشخصية محلاً للتداول، الأمر الذي من شأنه الإضرار بأصحابها واستغلالها في أغراض غير مشروعة، فكان لا بد من وضع

¹⁷⁶ وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، المركز العربي للبحوث القانونية والقضائية، ط1، لبنان، 2017، ص92.

¹⁷⁷ معاذ سلمان الملا، المرجع السابق، ص133.

إطار لحماية البيانات الشخصية وإرساء القواعد الضرورية والمبادئ القانونية التي تتم وفقاً لها معالجة هذه البيانات من أجل احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة.

المطلب الثاني

التزامات معالج البيانات الشخصية

يؤدي كل من المتحكم والمعالج دوراً بالغ الأهمية في نطاق معالجة البيانات الشخصية، إلى درجة يمكن معها القول أنهما في قلب القانون الجديد وجوهر أحكامه. وفضلاً عن ذلك اشترط القانون على الممثل القانوني للشخص الاعتباري لأي متحكم أو معالج تعيين شخص يكون مسؤولاً عن حماية البيانات الشخصية، وألقى المشرع على عاتقه جملة من الالتزامات. الأمر الذي يتطلب في فرعين :

الفرع الأول : التزامات المتحكم والمعالج في إطار حماية البيانات
الفرع الثاني: المسؤولية عن حماية البيانات الشخصية.

الفرع الأول: التزامات المتحكم والمعالج في إطار حماية البيانات

أشار قانون حماية البيانات الشخصية البحريني إلى الالتزامات التي تقع على عاتق المتحكم والمعالج في نصوص متفرقة، ولم يختلف الأمر في النظام الأوروبي العام لحماية البيانات الشخصية حيث جاء النص على التزامات المتحكم في نصوص متفرقة منه، كما بين المبدأ العام لمسؤوليته في الفقرة (1) من المادة (24). ويبدو من الالتزامات الملقاة على عاتق المتحكم أو المعالج أنه يعتبر المسؤول الأساسي عن ضمان إجراء عملية المعالجة وفقاً للقواعد المنصوص عليها في النظام، ويقع على عاتقه مسؤولية إثبات اتخاذ الإجراءات اللازمة لامتثال لقواعد النظام، ويمنحه النظام إرشادات حول كيفية إثبات قانونية أنشطة المعالجة التي يقوم بالإشراف عليها. ومن ثم يكون المتحكم هو المسؤول عن توفير الإجراءات التقنية والتنظيمية والمعايير الكافية التي تسمح لصاحب البيانات بأن يمارس حقوقه المنصوص عليها في النظام بسهولة كافية.

وسوف نتناول التزامات المتحكم والمعالج في إطار معالجة البيانات الشخصية فيما يلي:

أولاً: طلب التصريح المسبق

ثانيا : الالتزام بتأمين البيانات الشخصية
ثالثا:الالتزام بالمحافظة على سرية البيانات الشخصية

أولاً: طلب التصريح المسبق

التصريح المسبق هو عبارة عن موافقة مسبقة من الهيئة لكي يتمكن من القيام بالمعالجة، ويتم السماح لمقدم التصريح بأن يباشر عمله، وذلك عند استلامه وصل الإيداع، ويجب أن يتضمن مجموعة من البيانات، مثل الاسم وعنوان المسؤول عن المعالجة، وعند الاقتضاء اسم وعنوان من يمثله، كذلك طبيعة المعالجة وذلك قبل القيام بهذا التجميع، ويجب أن يكون الإخبار صريحاً ولا يحتمل اللبس، ويقع هذا الالتزام على عاتق كل من المسؤول عن المعالجة أو من يمثله ولا يسقط إلا في الحالة التي يكون فيها الشخص المعني على علم مسبق بالعناصر اللازم إخباره بها، بالإضافة إلى ذلك قد تقرر بعض القوانين عقوبات جزائية، بسبب عدم التقيد بالإجراءات الإدارية. ومثال على ذلك في حالة نسي المسؤول عن المعالجة التصريح، أو أن يكون قد قصد عدم القيام به¹⁷⁸.

وبموجب هذا الالتزام أشار قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018 إلى قاعدة أساسية وهي عدم جواز الحصول على البيانات الشخصية أو معالجتها دون الحصول على موافقة كتابية صريحة من صاحب البيانات وإلا سوف تكون المعالجة غير مشروعة، باستثناء الحالات التي نص عليها المشرع صراحة لاتحتاج إلى موافقة مسبقة وذلك في المادة (4) من قانون حماية البيانات الشخصية ، فإن موافقة الشخص المعني لا تكون واجبة إذا كانت المعالجة ضرورية لحماية حياة الشخص المعني أو لتحقيق مصلحة مشروعة من قبل المسؤول أو لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن مهام السلطة العمومية. وكما نصت المادة (5) من القانون على أنه يجب الحصول على موافقة مسبقة عند معالجة البيانات الحساسة ولكن هناك استثناءات نص عليها المشرع تجيز معالجتها في بعض الحالات بدون الحصول على الموافقة من صاحب البيانات ، وهي في حالة " المعالجة التي يقتضيها قيام مدير البيانات بالتزاماته ومباشرة حقوقه المقررة قانوناً في مجال علاقة العمل التي تربطه بالعاملين لديه. كذلك المعالجة الضرورية لحماية أيّ إنسان إذا كان صاحب البيانات -أو الوصي أو الولي أو القَيم عليه - غير قادر قانوناً على إعطاء موافقته على ذلك، 3 معالجة البيانات التي أتاحها صاحبها للجمهور، المعالجة الضرورية لمباشرة أيّ من إجراءات المطالبة بالحقوق القانونية أو الدفاع عنها، بما في ذلك ما يقتضيه التجهيز لهذا الأمر والاستعداد له.، المعالجة الضرورية لأغراض الطب الوقائي أو

¹⁷⁸ حسن الحافظي، المرجع السابق، ص123.

التشخيص الطبي أو تقديم الرعاية الصحية أو العلاج أو إدارة خدمات الرعاية الصحية من قِبَل مرخص له بمزاولة أيٍّ من المهن الطبية، أو أيِّ شخص ملزم بحكم القانون بالمحافظة على السرية..، المعالجة التي تتم في سياق أنشطة الجمعيات بأنواعها والنقابات وغيرها من الجهات التي لا تهدف إلى تحقيق ربح، وذلك بشرط الالتزام بما يأتي:

- 1- أن تتم المعالجة في حدود ما هو ضروري للغرض الذي أنشئت الجمعية أو النقابة أو الجهة من أجله..
- 2- أن ترد المعالجة على بيانات تخص أعضاء تلك الجمعية أو النقابة أو الجهة أو لأفراد لهم اتصال منتظم معها بحكم طبيعة نشاطها.
- 3- ألا يتم الإفصاح عن البيانات لأيِّ شخص آخر ما لم يوافق صاحب البيانات على ذلك.
- 4- المعالجة التي تتم من قِبَل جهة عامة مختصة بالقدر الذي يقتضيه تنفيذ المهام المنوطة بها قانوناً.
- 5- معالجة بيانات تتعلق بالأصل العرقي أو الإثني أو الديني إذا كانت ضرورية للوقوف على مدى توافر المساواة في الفرص أو المعاملة لأفراد المجتمع الذين ينحدرون من أصول عرقية أو إثنية أو دينية مختلفة، وبشرط مراعاة الضمانات المناسبة لحقوق وحرّيات أصحاب البيانات المقررة قانوناً. وعلى مجلس الإدارة أن يُصدر قراراً بتحديد القواعد والإجراءات التي يتعيّن على مدراء البيانات الالتزام بها بشأن المعالجة المشار إليها".

كما اشترط المشرع البحريني في قانون حماية البيانات الشخصية الحصول على موافقات خاصة لبعض حالات معالجة البيانات، ومنها في المادة (12) حيث نصت على عدم جواز نقل البيانات خارج مملكة البحرين من دون موافقة خاصة من صاحبها، إلا إذا كان ذلك بتصريح خاص من وزارة العدل والشؤون الإسلامية. كما نص القانون في المادة (15) على وجوب الحصول على تصريح كتابي مسبق من وزارة العدل والشؤون الإسلامية؛ حتى يتم استخدام المعالجة الآلية لربط البيانات الشخصية بين أكثر من جهة، كأن يتم ربط البيانات الشخصية للعملاء في شركتين مختلفتين، أو أن تستخدم المعالجة الآلية للبيانات القياسات الحيوية (Biometrics) للتعرف على الشخصية، كتلك التي تستخدم من خلال التطبيقات الإلكترونية على الأجهزة الذكية، أو تستخدم المعالجة التي تكون عبارة عن تسجيل بصري لأغراض المراقبة، كوضع كاميرات للمراقبة عن بُعد.

هذا ونص القرار رقم (42) لسنة 2022 بشأن نقل البيانات الشخصية إلى خارج البحرين في المادة (5) منه على يكون تقديم طلب الحصول على تصريح من الهيئة لنقل البيانات الشخصية إلى خارج المملكة وفقاً للآتي: "يتم تقديم طلب التصريح من خلال الموقع الإلكتروني

على الانموذج المعد لذلك متضمن البيانات التالية ، وهي أسم مدير البيانات وعنوانه واسم معالج البيانات وعنوانه ان وجد، البلد او الإقليم الوجهة النهائية له ويقوم ببيان مايتوفر بتلك البلدان أو الاقاليم من تدابير لحماية البيانات الشخصية، أن يرفق بالانموذج بيان الاتفاقيات والتشريعات ذات العلاقة بالبلد أو الأقليم، وأن يرفق بيان بالانموذج إذا كان البلد سوف يوفر مستوى كاف لحماية البيانات الشخصية المراد نقلها". وكذلك المادة (4) من القرار أنه في حال سوف يتم نقل البيانات لأقليم أو بلدان لم يتضمنها الكشف فيجب على مدير البيانات أن يحصل على موافقة مسبقة من أجل معالجتها¹⁷⁹.

ونجد أن المشرع أيضا القرار الوزاري رقم (44) لسنة 2022 بشأن قواعد وإجراءات تقديم الإخطار لهيئة حماية البيانات الشخصية¹⁸⁰ وطلب التصريح المسبق للمعالجة والبت فيه في المادة (3) منه المتعلقة بطلب التصريح المسبق من الهيئة، حيث يقدم مدير البيانات طلب التصريح المسبق على الأنموذج المعد على الموقع الإلكتروني للهيئة، ويجب أن يتضمن طلب التصريح البيانات ذاتها التي يجب أن يتضمنها الإخطار الذي يتعين تقديمه وفقاً للفقرة (2) من المادة (14) من قانون حماية البيانات الشخصية البحريني السابق ذكرها، وكذلك وفقاً للمادة (15) من القانون ذاته، حيث يتم البت في الطلب من قبل الهيئة خلال خمسة أيام من تاريخ تسلم الطلب، ويجب على مدير البيانات استيفاء أي نقص في البيانات خلال خمسة أيام التالية للعمل من تاريخ الطلب، وإلا تعين على الهيئة البت في الطلب بناءً على ما تضمنه من معلومات.

ووفقاً للمادة (4) من القرار الوزاري رقم (44) لسنة 2022 المتعلقة بالبت في طلب التصريح المسبق، تمنح الهيئة التصريح المسبق عند توافر الاشتراطات في الطلب المقدم لها، ويكون للهيئة البت بالتصريح وإخطار مدير البيانات بالنتيجة خلال ثلاثين يوماً من تاريخ تقديمه، وإذا لم يتسلم صاحب البيانات رداً من الهيئة يعد رفضاً ضمناً للطلب. كما تناولت المادة (5) من القرار ذاته التزامات المصريح له بالمعالجة، والتي من ضمنها التزامه بمراعاة الشفافية أثناء المعالجة ويشمل ذلك إعلام أصحاب البيانات بكيفية معالجة البيانات.

ويتطلب هذا الالتزام من المتحكم القيام بالتأكد من موافقة الشخص المعني بالبيانات وإثبات هذه الموافقة، وقد وضع المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) التزاماً مماثلاً على عاتق المتحكم، وذلك في المادة (7) منه، وبموجبه يتعين أن يكون المتحكم قادراً على إثبات أن صاحب البيانات قد وافق على معالجة بياناته الشخصية. إذا كانت موافقة صاحب البيانات مقدمة في شكل إعلان مكتوب يتعلق أيضاً بأمر أخرى، فيجب تقديم

179 القرار رقم(42) لسنة 2022 بشأن نقل البيانات الشخصية إلى خارج البحرين، الجريدة الرسمية ، العدد3593، 2022،

¹⁸⁰ القرار رقم (44) لسنة 2022، بشأن قواعد وإجراءات تقديم الإخطار لهيئة حماية البيانات الشخصية وطلب التصريح المسبق للمعالجة والبت فيه، الجريدة الرسمية، العدد 3594، 2022، البحرين، ص99-100.

طلب الموافقة بطريقة يمكن تمييزها بوضوح عن الأمور الأخرى، وفي شكل واضح يسهل الوصول إليه، وباستخدام لغة واضحة ومفهومة، وأي جزء من هذا الإعلان يشكل انتهاكاً لهذا النظام لن يكون ملزماً. كما يحق لصاحب البيانات سحب موافقته في أي وقت، ولن يؤثر سحب الموافقة على قانونية المعالجة، طالما كان هناك موافقة سابقة¹⁸¹.

وتجدر الإشارة هنا إلى إنه يوجد اتفاق بين مسلك المشرع الأوروبي والبحريني، فتنص المادة (4) من قانون حماية البيانات الشخصية البحريني على وجوب الحصول على موافقة الشخص المعني بالبيانات عند معالجة البيانات، وأكدت المادة (5) من القانون على وجوب الحصول على موافقة الشخص المعني بالبيانات عند معالجة البيانات الحساسة. ولصاحب البيانات، بموجب المادة (24) من القانون، أن يسحب في أي وقت موافقته على معالجة بياناته الشخصية بموجب إخطار يُصدره لمدير البيانات. ويُصدر مجلس الإدارة قراراً يحدد بموجبه إجراءات تقديم طلب السحب والبت فيه من قبل مدير البيانات.

ثانياً: الالتزام بتأمين البيانات الشخصية

إن الالتزام بتأمين سلامة البيانات الشخصية يعد مكملاً لموجب سرية البيانات، من الناحية المادية، وكذلك يعتبر من الموجبات الأساسية، للمسؤول عن المعالجة، فمن الضروري الحفاظ على أمن المعلومات، ومنع تسريبها، والحد كذلك من مخاطر انكشافها. وهذا يتطلب من المسؤول عن المعالجة بأن يقوم باتخاذ التدابير والإجراءات الضرورية لتحقيق ذلك، سواء كانت تقنية، أو إدارية، أو تنظيمية، فيقوم بوضع قواعد، وحدوداً، للاطلاع عليها، حتى يمنع من وصول المعالجين إليها، إلا في حدود ما هو ضروري منها¹⁸².

وحرص المشرع البحريني في قانون حماية البيانات الشخصية على أن ينص على الالتزام بتأمين البيانات الشخصية وذلك في المادة (8) وألزم مدير البيانات بأن يقوم بتطبيق التدابير الفنية والتنظيمية الكفيلة بحماية البيانات من الإتلاف غير المقصود أو غير المصرح به، أو من الفقد العرَضِي، أو مما هو غير مصرح به من التغيير أو الإفصاح أو النفاذ أو أي من الصور الأخرى للمعالجة. ويجب أن تكفل هذه التدابير توفير مستوى مناسب من الأمان بمراعاة ما وصلت

¹⁸¹ Art. 7 GDPR Conditions for consent

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...."

¹⁸² منى الأشقر جبور ومحمود الأشقر جبور، المرجع السابق، ص131.

إليه أحدث أساليب الحماية التقنية، والتكلفة المترتبة على ذلك، وطبيعة البيانات موضوع المعالجة، والمخاطر التي قد تنشأ من هذه المعالجة. ويجب أن تكون التدابير الفنية والتنظيمية مدونة ومتاح الاطلاع عليها من ذوي الشأن ومن الهيئة ومدير البيانات ومعالج البيانات.

وفي المادة (9) من القانون ، نصت على " أنه " يُحظر على مدير البيانات أن يفصح عن اي بيانات إلا بعد الحصول على موافقة صاحب البيانات، أو يكون تنفيذاً لأمر قضائي صادر من محكمة مختصة أو النيابة العامة أو قاضي التحقيق أو النيابة العسكرية. وكما يحظر أيضاً ان يعالج مدير البيانات اية بيانات بالمخالفة لأحكام القانون. وفي جميع الأحوال، يُحظر على أي فرد من المتاح لهم النفاذ إلى بيانات شخصية القيام بأية معالجة لها إلا بعد الحصول على موافقة من قبل مدير هذه البيانات أو تنفيذاً لأمر قضائي صادر من محكمة مختصة أو قاضي التحقيق أو النيابة العامة أو النيابة العسكرية، كما يُحظر عليهم استخدامها لمنفعتهم الخاصة أو لمنفعة الغير، ويستمر هذا الحظر بعد انتهاء علاقة العمل أو مدة العقد".

ولزم المشرع الكويتي في المادة (35) من قانون المعاملات الإلكترونية الكويتي "...الجهات الحكومية أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية باتخاذ التدابير المناسبة لحماية البيانات الشخصية الموجودة في أنظمة المعالجة الإلكترونية الخاصة بها من كل ما يعرضها للفقْد أو التلف أو الإفشاء أو استبدالها ببيانات غير صحيحة أو إدخال معلومات عليها خلافاً للحقيقة"¹⁸³.

وأما بالنسبة للنظام الأوروبي العام لحماية البيانات الشخصية فنص في المادة (32)¹⁸⁴ على أمان المعالجة، حيث حددت المادة مجموعة من التدابير الفنية والتنظيمية اللازمة التي يجب على المنظمات تنفيذها لحماية جميع البيانات الشخصية التي تخزنها بشكل مناسب، ولكنها لم تحدد الشكل الذي يجب أن تبدو عليه هذه العمليات، لأن أفضل الممارسات -وخاصة عندما يتعلق الأمر بالتكنولوجيا- تتغير بسرعة وما يعد مناسباً الآن لن يكون كذلك بمرور السنوات. ومع ذلك يجب أن تركز أي إجراءات يتم تنفيذها على أمان المعالجة، وهذا يعني أنه يجب النظر في كيفية وطرائق تخزين البيانات الشخصية وحمايتها وخاصة في منع انتهاكات البيانات، وكذلك حدوث

¹⁸³ القانون الكويتي رقم 20 لسنة 2014 في شأن المعاملات الإلكترونية. يمكن الاطلاع عليه من خلال البوابة الإلكترونية الرسمية لدولة الكويت: <https://e.gov.kw/sites/kg0Arabic/Pages/eServices/LegalPortal/Legal.aspx>.

¹⁸⁴ Art. 32 GDPR Security of processing

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate....."

الحوادث المادية والتقنية، ومن ناحية أخرى يجب على مراقبي البيانات أن يأخذوا في الاعتبار عوامل معينة لتحديد ما إذا كان عنصر تحكم أمني معين مناسباً في الظروف المعنية أم لا. ومن ضمن العوامل اللازمة لاتخاذ الإجراءات التنظيمية والفنية المناسبة الآتي:

1- حالة التقنية القائمة (state of the art) - والتي تشير إلى أفضل ممارسات الصناعة.

كما يقر النظام الأوروبي العام لحماية البيانات بأن الأمن هو مجال من مجالات الخبرة المهنية، و يترك الأمر لمراقبي البيانات والمعالجات للنظر في أفضل ممارسات الصناعة أثناء وضع ضوابط أمنية مناسبة في موقف معين.

2- تكاليف التنفيذ: أي يتعين أن تأخذ الضوابط الأمنية بنظر الاعتبار تكاليف التنفيذ في حالة معينة. وهذا يعني أن مراقبي البيانات والمعالجات ليسوا مطالبين بتنفيذ ضوابط باهظة الثمن. ويجب أن تظل المنظمات مُحَدَّدة للتكلفة، وأن تضع في الاعتبار أفضل الممارسات الصناعية وأن تنفذ الضوابط الأمنية المناسبة لوضعها وظروفها.

3- طبيعة المعالجة ونطاقها وسياقها وأغراضها، لتحديد الضوابط المناسبة: يجب على المؤسسات مراعاة طبيعة البيانات المراد معالجتها، وكذلك السياق الذي تتم فيه المعالجة وأغراض المعالجة ونطاق التجهيز. وستتطلب الاحتمالات الأعلى أو التهديدات ذات التأثير العالي أن تستخدم المؤسسات ضوابط أكثر صرامة، وخاصة أثناء معالجة البيانات الشخصية الحساسة.

4- المخاطر على حقوق وحريات الأشخاص الطبيعيين، لتحديد الضوابط المناسبة: يجب على المنظمات إجراء تقييمات للمخاطر لتحديد أي تهديدات ومخاطر معقولة يمكن توقعها لموضوعات البيانات. ويجب أن يكون التحكم الأمني مناسباً للمخاطر المحددة.

وفي جميع الأحوال يجب أن تكون الأسبقية في اتخاذ التدابير للمنظمات التي توفر الضمانات المناسبة لجميع البيانات التي تم جمعها. ونظراً إلى مدى ديناميكية عالم خصوصية البيانات، فمن المفترض أن تضمن المؤسسات ديناميكية وحداثة ممارساتها وإجراءاتها الأمنية وتوافقها مع المعايير الحديثة وأفضل الممارسات الصناعية.

وأما بالنسبة لأهم التدابير الفنية التنظيمية الصريحة المذكورة في النظام الأوروبي العام لحماية البيانات الشخصية في المادة (32) منه فهي كالآتي:¹⁸⁵

¹⁸⁵ Art 32 Security of processing

“1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and

1. اسم مستعار للبيانات: الغرض من اتخاذ هذا الإجراء هو ضمان الحد الأدنى من مخاطر البيانات المعالجة المكشوفة. ويمكن إجراء تحديد هوية مستعارة للبيانات عن طريق استبدال أسماء موضوعات البيانات والمعرفات الفريدة باستخدام معلومات إضافية مثل الأرقام المرجعية. يمكن بعد ذلك استخدام هذه المعلومات الإضافية للإحالة المرجعية وتتبع بيانات المستخدمين. ويقلل استخدام الأسماء المستعارة من المخاطر التي يتعرض لها الأشخاص المعنيون بالبيانات. وتعتبر البيانات ذات الأسماء المستعارة أيضًا بيانات شخصية بموجب النظام الأوروبي العام لحماية البيانات ، وبالتالي ستخضع لمتطلبات حماية البيانات الواردة في النظام.

2. تشفير البيانات: التشفير هو عنصر تحكم صريح آخر في النظام الأوروبي العام لحماية البيانات الشخصية. عندما يتم تشفير البيانات تصبح غير قابلة للقراءة دون تشفير أو دون الوصول إلى مفتاح فك التشفير. كما يجعل التشفير البيانات الشخصية غير مفهومة لأي شخص غير مصرح له بالوصول إلى البيانات، وهو بذلك يخفف من المخاطر الكامنة في نشاط معالجة البيانات.

3. القدرة على ضمان استمرار سرية ونزاهة وتوافر ومرونة البيانات الشخصية: الأسماء المستعارة والتشفير هي الضوابط الوحيدة الصريحة المذكورة في النظام الأوروبي العام لحماية البيانات الشخصية. ويتطلب النظام من مراقبي البيانات والمعالجات تنفيذ ضوابط أمنية تضمن السرية المستمرة والنزاهة والتوافر والمرونة لأنظمة المعالجة والخدمات. كما تشير السرية إلى أن الوصول إلى البيانات مسموح به على أساس الحاجة إلى المعرفة. وأما النزاهة فتعني أن البيانات تظل دقيقة وكاملة. والتوافر يعني أن البيانات تظل متاحة عند الحاجة لنشاط تجاري.

4. استعادة توافر البيانات والوصول إليها: لنفترض أن منظمة ما تتخذ جميع الاحتياطات اللازمة ولديها أفضل بروتوكولات الأمان، إلا إنه وعلى الرغم من ذلك تقع حادثة بيانات، فلا شك إنه في

freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;.....”

المزيد من التفاصيل فيما يتعلق بالتدابير الفنية والتنظيمية المتعلقة بأمان المعالجة التي نصت عليها المادة (32) من النظام الأوروبي العام لحماية البيانات الشخصية يرجى لإطلاع على الموقع التالي:

[GDPR Article 32: Your guide to the requirements - IT Governance UK Blog](https://www.uk.gov.uk/government/publications/gdpr-article-32-your-guide-to-the-requirements)

:

مثل هذه الحالة ستدخل العديد من خطط الطوارئ حيز التنفيذ. وتهدف هذه الخطط إلى استعادة الوصول إلى البيانات الشخصية في أقرب وقت ممكن في حالة حدوث خرق.

ومن خلال ما سبق نتوصل إلى أنه لا يمكن توفير الحماية القانونية للبيانات الشخصية بدون تأمين هذه البيانات من جانب المعالج لها، حيث تزداد المخاطر الخاصة بالاعتداء على هذه البيانات من الأشخاص غير المرخص لهم بالاطلاع عليها، بحيث يمكن لهؤلاء التعديل عليها أو إفشاؤها.

كما قضت محكمة العدل الأوروبية في حكمها الصادر بتاريخ ٥ يونيو ٢٠١٨ بأن المدير أو مشرف صفحة المعجبين مسؤول مسؤولية تضامنية مع الفيسبوك عن معالجة بيانات المستخدمين على صفحة هذه المجموعة بحيث يستطيع المتضرر من معالجة البيانات الشخصية أن يرفع دعوى على مدير صفحة الفيسبوك، وكذلك في مواجهة الشركة التابعة للفيسبوك في البلد نفسه. وتتلخص وقائع الدعوى بقيام شركة ألمانية بالنشر عبر صفحتها على الفيسبوك أنها متخصصة في مجال خدمات التدريب والتعليم من خلال أداة على الفيس بوك متوافرة مجاناً لمدير الصفحة؛ وبحيث يستطيع هذا الأخير أن يقوم بجمع بيانات عن زوار الصفحة (مع اختلاف العمر والجنس... إلخ)، ومع الأخذ بعين الاعتبار أن جمع هذه البيانات يكون من خلال ملفات تعريف يرتبط كل منها برمز مستخدم وحيد فعال لمدة عامين ويتم حفظه بواسطة فيسبوك على القرص الصلب للكمبيوتر أو أي وسيلة أخرى لزوار الصفحة. وأكدت محكمة العدل الأوروبية على إنه ينبغي اعتبار الفيسبوك المسؤول عن معالجة البيانات الشخصية التي تم تجميعها. وكذلك انتهت المحكمة إلى أن مدير الصفحة يعتبر مسؤولاً على أساس استخدام منصة أقامت فيسبوك من أجل الاستفادة من الخدمات التي تقدمها. وبالنسبة للإجراءات التقنية يمكن استعمال مجموعة من التقنيات مثل الترميز، أو التشفير، أو الولوج الشخصي، أو الولوج التسلسلي، أو صد الفيروسات المعلوماتية ومحاولة الدخول بدون إذن، أو عرقلة أنظمة تعديل البيانات¹⁸⁶.

كما جاء القرار رقم (43) لسنة 2022¹⁸⁷ بتحديد الاشتراطات التي يجب أن تتوفر في التدابير الفنية والتنظيمية لحماية البيانات الشخصية، ومن ضمنها المادة (2)، حيث اشتملت على

¹⁸⁶ أحمد محمد العدوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، جامعة بنها، العدد الثالث والثلاثون - الجزء الرابع، مصر، 2020، ص 1995-1993.

¹⁸⁷ القرار الوزاري رقم (43) لسنة 2022، تحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية، الجريدة الرسمية، العدد، 3594، 2022، البحرين، ص 92.

أهم التدابير الفنية والتنظيمية التي يجب تطبيقها عند القيام بعمليات المعالجة، وذلك وفقاً لطبيعة نطاق المعالجة أو سياقها أو أغراضها أو مخاطرها، وهي كالاتي:

- تطبيق تصميم لحماية الخصوصية (Design by Privacy)¹⁸⁸ عند إعداد وتصميم واختيار واستخدام التطبيقات والخدمات والمنتجات القائمة على معالجة البيانات بأنواعها.
- وضع أطر حماية الخصوصية (Privacy framework)، وذلك من خلال الهيكلية والممارسة والتعليمات المتعلقة بحماية البيانات في ضوء القانون والقرارات المعمول بها.
- الالتزام بتطبيق تدابير فعالة للحد من مخاطر انتهاك الخصوصية في مواجهة عمليات أو محاولات الاختراق، ومنها على سبيل المثال تنظيم وضمان الوصول إلى البيانات المحفوظة، وحماية كلمات المرور، واستخدام برامج مكافحة الفيروسات وتطبيقات جدران الحماية (firewalls) والبرمجيات، وتنظيم مدة الحفظ بالبيانات ومحوها، والامتثال للتراخيص، ووضع بروتوكولات تقنية ملائمة تكفل الوصول إلى المواقع الفعلية والنظم الافتراضية.
- إجراء تقييم لمكامن الضعف والاختراق للبرامج الآلية (Assessment and Vulnerability) وذلك من خلال صورة دورية للتحقق من كفاءة التدابير الأمنية المعمول بها، وقياس مدى فاعليتها لتصحيح أي ثغرات أمنية والحد منها.
- وضع خطة فعالة لمواجهة الحوادث والاختراقات الفجائية في أنظمة معالجة البيانات بما يسمح باستمرار تنفيذ أعمال المعالجة دون انقطاع.
- تحديد نطاق الصلاحية الممنوح لكل موظف كل بحسب اختصاصه والمهام المكلف بها، بغرض توفير حماية وخصوصية عاليتين للبيانات محل المعالجة. وعلى مدير البيانات إحاطة الموظفين المعنيين بالمعالجة وبالتدابير المذكورة في الفقرة السابقة، وذلك على نحو يكفل الامتثال لأحكام القانون والقرارات الصادرة تنفيذاً له.

ثالثاً: الالتزام بالمحافظة على سرية البيانات الشخصية

سرية البيانات الشخصية تحفز الاستقلال والكرامة الإنسانية. وفي ظل عدم الإجماع على تعريف موحد تعتبر السرية حق تحديد، متى، وكيف، وإلى أي مدى، يمكن مشاركة المعلومات،

¹⁸⁸ تصميم لحماية الخصوصية: هو طريقة نظامٍ لو معالجة البيانات تسعى لتوفير أقصى درجات الخصوصية بشكل استباقي من خلال ضمان حماية البيانات تلقائياً في النظام التكنولوجي أو الممارسة التجارية، وتطبيق تدابير الأمان في جميع مراحل المعالجة بشكل يتوقع مشاكل الخصوصية ويمنعها قبل حدوثها. يرجى الاطلاع على : القرار الوزاري رقم (43) لسنة 2022، تحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية، الجريدة الرسمية، العدد، 3594، 2022، البحرين، ص92. كذلك منى الأشقر جبور ومحمود الأشقر جبور، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد، مرجع سابق، ص

التي تم الاطلاع عليها، وهي هنا البيانات الشخصية مع الآخرين. وبحسب هذا الموجب المفروض لحماية البيانات الشخصية لا يجوز للمسؤول عن المعالجة السماح بالوصول إلى هذه البيانات، إلا للأشخاص المعنيين بمعالجتها، وللمدة الضرورية، لإنجاز الهدف الأساسي من جمعها. فلا يجوز لفندق مثلاً، الاستمرار في حفظ البيانات الشخصية، ورقم بطاقة الانتماء العائدة للزبون، بعد انتهاء مدة إقامة هذا الأخير لديه، وإتمامه موجب دفع المستحقات. بل يفترض بالفندق، إما محو البيانات، وإما تشفيرها، وإما اللجوء إلى تقنية إخفاء تحديد الهوية من خلالها، بحيث لا يعود تحديد الشخص المعني ممكناً، فعندها فقط، يسمح للفندق الاحتفاظ بها، لأغراض إحصائية، أو غيرها¹⁸⁹.

ومن أجل توفير الحماية اللازمة للبيانات والمعلومات الشخصية من الاعتداء عليها، نص المشرع البحريني في قانون حماية البيانات الشخصية في المادة (9) المتعلقة بسرية المعالجة على أنه "يحظر على مدير البيانات الإفصاح عن أي بيانات شخصية إلا بموافقة صاحب هذه البيانات، أو تنفيذاً لأمر قضائي صادر عن محكمة مختصة أو النيابة العامة أو قاضي التحقيق أو النيابة العسكرية. كما يحظر على مدير البيانات معالجة أي بيانات شخصية بالمخالفة لأحكام هذا القانون. وفي جميع الأحوال يحظر على أي فرد من المتاح لهم النفاذ إلى بيانات شخصية القيام بأية معالجة لها إلا بموافقة مدير هذه البيانات أو تنفيذاً لأمر قضائي صادر عن محكمة مختصة أو قاضي التحقيق أو النيابة العامة أو النيابة العسكرية، كما يحظر عليهم استخدامها لمنفعتهم الخاصة أو لمنفعة الغير، ويستمر هذا الحظر بعد انتهاء علاقة العمل أو مدة العقد".

وفي السياق نفسه أكد المشرع الأوروبي في المادة (28) من النظام الأوروبي العام لحماية البيانات الشخصية (GDPR) على أهمية أن يضمن المعالج التزام الأشخاص المصرح لهم بمعالجة البيانات الشخصية بالسرية أو أنهم يخضعون لالتزام قانوني بالسرية¹⁹⁰.

وكذلك نص المشرع الكويتي في المادة (32) من قانون المعاملات الإلكترونية لسنة 2014 على أنه "لا يجوز في -غير الأحوال المصرح بها قانوناً- للجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين بها الاطلاع دون وجه حق أو إفشاء أو نشر أي بيانات أو معلومات شخصية مسجلة في سجلات أو أنظمة المعالجة الإلكترونية المتعلقة بالشؤون الوظيفية أو بالسيرة الاجتماعية أو بالحالة الصحية أو بعناصر الذمة

¹⁸⁹ منى الأشقر جبور و محمود الأشقر جبور، المرجع السابق، ص 129-130.

¹⁹⁰ Art 28 GDPR Processor:

B." ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality....."

المالية للأشخاص أو غير ذلك من البيانات الشخصية المسجلة لدى أي من الجهات المبينة في هذه المادة أو العاملين بها بحكم وظائفهم ما لم يتم ذلك بموافقة الشخص المتعلقة به هذه البيانات أو المعلومات أو من ينوب عنه قانوناً، أو بقرار قضائي مسبب. وتلتزم الجهات المبينة في الفقرة الأولى من هذه المادة ببيان الغرض من جمع البيانات والمعلومات المذكورة، وأن يتم جمع تلك البيانات والمعلومات في حدود ذلك الغرض".

ونجد مما سبق إن كل من المشرع البحريني والكويتي والأوروبي قد ألقى على عاتق معالج البيانات الالتزام بعدم إفشاء البيانات الشخصية أو نشرها إلا بموافقة الشخص نفسه أو بإذن قضائي.

الفرع الثاني: دور مسؤول حماية البيانات الشخصية والتزاماته

إن قانون حماية البيانات الشخصية قد استحدث مفهوم "مسؤول حماية البيانات الشخصية"، وهو الشخص الطبيعي الذي يعنى بمباشرة مهام حماية البيانات الشخصية داخل المؤسسة أو الجهة. وقد تناول كل من المشرع البحريني والأوروبي هذا الموضوع في نصوص القانون المتعلقة بحماية البيانات الشخصية. وباستقراء تلك المواد يتضح لنا أن مسؤول حماية البيانات هو الشخص المسؤول داخل كل مؤسسة عن تطبيق أحكام القانون، ويضطلع بمعظم المسؤوليات في هذا الصدد. ولبيان التحديات المتعلقة بمسؤول حماية البيانات سوف نوضح كيفية تعيينه وتحديد التزاماته في القانون البحريني والنظام الأوروبي العام لحماية البيانات الشخصية فيما يأتي:

أولاً: تعيين مسؤول حماية البيانات

أجاز المشرع البحريني في قانون حماية البيانات الشخصية رقم 30 لسنة 2018 من المادة (10) منه لمدير البيانات أن يعين مراقباً لحماية البيانات، ومع ذلك يجوز لمجلس الإدارة أن يصدر قراراً يلزم بموجبه فئات معينة من مديري البيانات بأن يعينوا مراقباً لحماية البيانات. وفي جميع الأحوال، يجب على مدير البيانات إخطار الهيئة بالتعيين المشار إليه خلال ثلاثة أيام عمل من قيامه بذلك. كما نص القرار رقم (46) لسنة 2022 البحريني بشأن مراقبي حماية البيانات الشخصية البحريني من المادة (2) منه أنه يجوز لمدير البيانات أن يعين مراقب حماية بيانات داخلياً وخارجياً ويمكن لمجلس الإدارة أن يصدر قراراً يلزم بموجبه فئات معينة من مديري البيانات بتعيين مراقب لحماية البيانات، وذلك وفقاً لنوع العمل وطبيعة النشاط أو حجم المعاملات التي يقوم بها مدير البيانات أو إن كان أسلوب معالجته للبيانات الشخصية يتطلب ذلك، ومن ثم يجب على

مدير البيانات أن يخطر الهيئة بالتعيين خلال ثلاثة أيام عمل من قيامه بذلك¹⁹¹، وهذا الالتزام يهدف إلى ضمان مزيد من التنسيق والامتثال لأحكام القانون، وفي ذات الوقت يخدم المتحكم والمعالج ذاتهما بأن يوزعا الأدوار ويرفعا من على كاهلها بعض المسؤوليات¹⁹².

كذلك ألزمت المادة (37) من النظام الأوروبي العام لحماية البيانات الشخصية المتحكم والمعالج بتعيين مسؤول حماية البيانات وفقا للحالات الآتية:¹⁹³

1- عندما تتم المعالجة من قبل سلطة أو هيئة عامة.

أ- لم يحدد النظام الأوروبي العام لحماية البيانات الشخصية في هذه المادة ما الذي يشكل سلطة أو هيئة عامة، ومع ذلك ذكرت الهيئة الاستشارية الأوروبية المستقلة في المادة (29) من (DPOs)¹⁹⁴ إن هذه المسألة هي ضمن اختصاص القانون الوطني. وعلى الرغم من أن السلطات والهيئات العامة قد تشمل السلطات الوطنية والإقليمية والمحلية، فقد يمتد المصطلح أيضًا ليشمل الهيئات الأخرى التي يحكمها القانون العام. وفي مثل هذه الحالات، يكون تعيين مسؤول حماية البيانات إلزاميًا. كما يجب تعيين مسؤول حماية البيانات حتى في الحالات التي يمارس فيها شخص طبيعي أو اعتباري مهمة عامة. كما توصي الهيئة الاستشارية الأوروبية المستقلة أيضًا بأنه في الحالات التي تقوم فيها المؤسسات الخاصة بتنفيذ مهام عامة، فإنها تقوم أيضا بتعيين مسؤول لحماية البيانات.

ب- في حال تضمنت الأنشطة الأساسية لوحدة التحكم أو المعالج عمليات معالجة تتطلب بحكم طبيعتها ونطاقها أو أغراضها، مراقبة منظمة ومنتظمة لأصحاب البيانات على نطاق واسع. ومن خلال هذا النص يتبين لنا أن السلطات القضائية مستثناة من شرط وجود مسؤول حماية البيانات، والسبب في ذلك هو مبدأ أن القضاء يجب أن يكون مستقلاً عن أحكام إنفاذ النظام العام الأوروبي لحماية البيانات، ومع ذلك لا ينطبق هذا الاستثناء في الحالات التي تتم فيها معالجة البيانات الشخصية من قبل إدارات المحاكم

¹⁹¹ القرار البحريني رقم (46) لسنة 2022، بشأن مراقبي حماية البيانات الشخصية، الجريدة الرسمية، العدد، 3594، 2022، البحرين، ص104.

¹⁹² د. حسن عبد الحميد، المرجع السابق، ص56.

193 Art. 37 GDPR Designation of the data protection officer

“The controller and the processor shall designate a data protection officer in any case where....”

194 تم إنشاء مجموعة العمل هذه بموجب المادة 29 من التوجيه EC. 46/95 / وهي هيئة استشارية أوروبية مستقلة بشأن حماية البيانات والخصوصية. مهامها موصوفة في المادة 30 من التوجيه EC 46/95 / والمادة 15 من التوجيه EC.58/2002 / .

WP29, Guidelines on Data Protection Officers (“DPOs”), WP 243 rev.01, 5 April 2017 (available at [ARTICLE29 - Guidelines on Data Protection Officers \('DPOs'\) \(wp243rev.01\) \(europa.eu\) \(last .visit:17December 2022\)](https://ec.europa.eu/art29/wp243rev01_en.pdf))

عندما تتصرف كسلطات عامة بطريقة مرتبطة بولايتها القضائية. ويلاحظ من هذه المادة أنها قامت بذكر مفهوم "المراقبة المنظمة والمنظمة" لموضوعات البيانات، ويتضمن "جميع أشكال التتبع والتميط على الإنترنت، بما في ذلك لأغراض الدعاية السلوكية". ويمكن أيضًا أن تتم مراقبة موضوعات البيانات خارج سياق بيئة الإنترنت. على وجه التحديد، كما فسرت الهيئة الاستشارية الأوروبية المستقلة كلمة "منتظم" على أنها تعني: مستمر أو يحدث في فترات زمنية معينة لفترة معينة، متكرر أو متكرر في أوقات محددة، بشكل مستمر أو دوري. وفسرت "منهجي" على أنه يحدث وفق نظام مرتب مسبقًا أو منظم أو منهجي، يجري كجزء من خطة عامة لجمع البيانات تُنفذ كجزء من إستراتيجية. وتتضمن الأمثلة المعطاة لأنشطة المعالجة المنظمة والمنظمة تشغيل شبكة اتصالات، والتسويق القائم على البيانات، وتتبع الموقع، وغيرها من أمور أخرى.

ج - عندما تتكون الأنشطة الأساسية لوحدة التحكم أو المعالج من معالجة على نطاق واسع من فئات البيانات الخاصة وفقًا للمادة (9) والبيانات الشخصية المتعلقة بالإدانات الجنائية والجرائم المشار إليها في المادة (10) من النظام.

ومن هذه المادة يلاحظ أنه بطريقة مماثلة للمادة (37) (1/ب)، تفرض المادة (37) (1/ج) من النظام الأوروبي العام لحماية البيانات الشخصية التزامًا بتعيين مسؤول لحماية البيانات على وحدات التحكم أو المعالجات التي تتضمن أنشطتها الأساسية على نطاق واسع معالجة الفئات الخاصة من البيانات بموجب المادة (9) من النظام الأوروبي العام لحماية البيانات أو البيانات المتعلقة بالإدانات الجنائية والجرائم بموجب المادة (10) من النظام ذاته، ومن الواضح أن هذا المطلب مرتبط بأهمية وجود شخص ما داخل الهيكل التنظيمي للمراقب الذي يفهم حساسية البيانات التي تتم معالجتها، وهو على دراية جيدة بما تتضمنه معالجة هذا النوع من البيانات.

ونجد أن المادة (37) (1/ب) والمادة (37) (1/ج) من النظام الأوروبي العام لحماية البيانات الشخصية قد وسعت من متطلبات تعيين مسؤول حماية البيانات للمتحمكين أو المعالجين الذين تتطلب أنشطتهم الأساسية المراقبة المنظمة والمنظمة لموضوعات البيانات على نطاق واسع، كما توضح المادة (10) من النظام الأوروبي العام لحماية البيانات أن الأنشطة الأساسية لوحدة التحكم هي تلك المتعلقة "بالأنشطة الأساسية ولا تتعلق بمعالجة البيانات الشخصية باعتبارها أنشطة إضافية". كما أوضحت الهيئة الاستشارية الأوروبية المستقلة أن فكرة "الأنشطة الأساسية" يمكن اعتبارها "العمليات الرئيسية اللازمة لتحقيق أهداف وحدة التحكم أو المعالج". ومع ذلك لا ينبغي تفسير "الأنشطة الأساسية" بطريقة تستبعد عمليات المعالجة التي تشكل جزءًا لا يتجزأ من أنشطة

وحدة التحكم أو المعالج. ومثال ذلك المستشفى الذي يوفر الرعاية الصحية. هنا سيحتاج المستشفى إلى معالجة البيانات الصحية حتى يتمكن من توفير الرعاية الصحية بشكل فعال. وفي هذه الحالة يجب اعتبار معالجة البيانات جزءًا من الأنشطة الأساسية للمستشفى، وبالتالي سيكون المستشفى ملزمًا بتعيين مسؤول حماية البيانات.

كما يلاحظ من هذه المادة إنها لم تعرف مصطلح "واسع النطاق" فيما يتعلق بالمعالجة، ومع ذلك، نجد إن المادة (91) من النظام الأوروبي العام لحماية البيانات الشخصية قد ألقت بعض الضوء على ما قد يعنيه هذا المصطلح، مع ملاحظة أن عمليات المعالجة "واسعة النطاق" قد تهدف إلى "معالجة قدر كبير من البيانات الشخصية على المستوى الإقليمي أو الوطني أو فوق الوطني" وقد "تؤثر على عدد كبير من البيانات المواضيع" في هذا الصدد، كما حددت الهيئة الاستشارية الأوروبية المستقلة أربعة معايير يمكن من خلالها تقييم طبيعة وسعة النطاق لعمليات المعالجة وهي:

- (1) عدد موضوعات البيانات المعنية.
- (2) حجم ونطاق البيانات التي تتم معالجتها.
- (3) مدة المعالجة أو استمرارها.
- (4) النطاق الجغرافي لأنشطة المعالجة. وتشمل مثلاً المعالجة المنتظمة لبيانات المرضى في المستشفيات، أو معالجة البيانات عن طريق الهاتف أو مزودي خدمة الإنترنت. في المقابل، فإن معالجة البيانات الشخصية من قبل طبيب فردي، على سبيل المثال، لن تعتبر معالجة على نطاق واسع.

بالإضافة إلى ما سبق، تتم المعالجة من قبل سلطة أو هيئة عامة، باستثناء المحاكم التي تعمل بصفقتها القضائية، وتتكون الأنشطة الأساسية لوحدة التحكم أو المعالج من عمليات المعالجة التي تتطلب، بحكم طبيعتها ونطاقها أو أغراضها، مراقبة منتظمة لموضوعات البيانات على نطاق واسع، أو تتكون الأنشطة الأساسية لوحدة التحكم أو المعالج من المعالجة على نطاق واسع من الفئات الخاصة من البيانات وفقاً للمادة (9) من النظام أو البيانات الشخصية المتعلقة بالإدانات الجنائية والجرائم المشار إليها في المادة (10) من النظام¹⁹⁵.

¹⁹⁵ Art. 37 GDPR Designation of the data protection officer

1. "The controller and the processor shall designate a data protection officer in any case where:
 1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;...."

وعلى الصعيد الوطني، فقد اشترطت المادة (4) من القرار الوزاري رقم (46) لسنة 2022 بشأن مراقبي حماية البيانات أنه يجب على كل من يرغب في تعيين مراقب لحماية بيانات داخلي أو خارجي أن يقيّد اسمه في السجل. وهذا ما نص عليه أيضاً المشرع البحريني في قانون حماية البيانات الشخصية رقم 30 لسنة 2018 في المادة (10) بأنه حتى يتم اعتماد مراقب حماية البيانات لا بد من أن يكون مقيّداً في هذا السجل. ويُصدر مجلس الإدارة قراراً بتنظيم أعمال مراقبي حماية البيانات، وكذلك يحدد الشروط اللازم توافرها فيمن يقيّد في السجل المشار إليه وبإجراءات القيد ومدة سريانه وتجديده. وبموجب المادة (3) من القرار الوزاري السابق، يتكون السجل من قسم خاص لقيد مراقبي حماية البيانات الخارجيين وقسم خاص لقيد مراقبي حماية البيانات الداخليين أيضاً ويتم نشر السجل على الموقع الإلكتروني للهيئة. كما حددت المادة (5) من هذا القرار شروط قيد مراقب حماية البيانات الخارجي في السجل حيث يشترط الآتي:

1. بالنسبة للشخص الطبيعي:

يجب أن يكون كامل الأهلية، وأن يكون كذلك حاصلًا على درجة البكالوريوس في تقنية المعلومات أو شهادة مهنية في الأمن المعلوماتي، أو التدقيق على الأمن المعلوماتي، أو الأمن الإلكتروني، أو أن يتمتع بخبرة لا تقل عن سنتين في أي من المجالات المشار إليها، وأن يكون حسن السيرة والسلوك وألا يكون سبق الحكم عليه بعقوبة جنائية أو في جريمة مخلة بالشرف والأمانة، ما لم يكن رد إليه اعتباره، وألا يكون قد سبق فصله من عمله بموجب حكم أو قرار تأديبي، أو سبق أن شطب قيده أو ألغي أو أوقف الترخيص الصادر بمزاولة مهنته الأصلية بموجب حكم أو قرار تأديبي.

2. بالنسبة للشخص الاعتباري:

أن يكون مرخصاً له بالعمل في مملكة البحرين، وأن يكون مجال عمله مرتبطاً بتقديم الاستشارات القانونية، أو التدقيق، أو تقنية المعلومات، أو إدارة الأعمال، أو المحاسبة، أو إدارة المخاطر، أو أن يكون ثلاثة من موظفيه على الأقل ممن تنطبق عليهم الشروط المذكورة لقيد الشخص الطبيعي بالسجل المنصوص عليها في الفقرة (1)، كذلك يتم القيد على أي شروط تحددها الإدارة¹⁹⁶.

ووفقاً لهذه المادة يلتزم الممثل القانوني للشخص الاعتباري لأي متحكم أو معالج بأن يعين داخل كيانه القانوني وهيكله الوظيفي موظفاً مختصاً مسؤولاً عن حماية البيانات الشخصية، وذلك

¹⁹⁶ القرار الوزاري رقم (46) لسنة 2022، بشأن مراقبي حماية البيانات الشخصية، الجريدة الرسمية، العدد، 3594، الخميس 17 مارس 2022.

بقيده في سجل مسؤولي حماية البيانات الشخصية بالمركز، ويعلن عن ذلك، ويكون الشخص الطبيعي المتحكم أو المعالج هو المسؤول عن تطبيق أحكام هذا القانون.

وأما المادة (9) من هذا القرار فقد نصت على الشروط الواجب توافرها عند قيد مراقب حماية البيانات الداخلي في السجل، حيث يشترط بالإضافة إلى الشروط السابق ذكرها فيما يتعلق بالشخص الطبيعي في البند (1) من المادة (5) أنه يجب أن يكون من بين العاملين لدى مدير البيانات أو لدى شركة تابعة له أو أحد أفرعها أو ضمن مجموعة إقليمية أو دولية ذات ملكية واحدة، وأن تكون إقامته داخل مملكة البحرين.

ومن ناحية أخرى نجد أن المادة (37) فقرة (2) وكذلك المادة (37) (3) من النظام الأوروبي العام لحماية البيانات الشخصية بتعيين مسؤول حماية بيانات واحد لمجموعة من التعهدات أو العديد من الهيئات أو الهيئات العامة. حيث تنص الفقرة (2) من المادة (37) على أنه يمكن تعيين مسؤول حماية بيانات واحد للعديد من التعهدات، طالما أن مسؤول حماية البيانات يمكن الوصول إليه بسهولة من كل مؤسسة. و أوضحت الهيئة الاستشارية الأوروبية المستقلة أن فكرة الوصول هذه تشير إلى أن مسؤول البيانات ليس فقط بمثابة نقطة اتصال لموضوعات البيانات، ولكن أيضًا نقطة اتصال داخلية للمؤسسة نفسها. وهو ما أكدته مضمون المادة (39) (1) من النظام الأوروبي العام لحماية البيانات الشخصية، فنصت على إن إحدى مهام مسؤول حماية البيانات هي "إبلاغ وحدة التحكم والمعالج والموظفين الذين ينفذون معالجة التزاماتهم وفقًا لهذا النظام وتقديم المشورة لهم". ويتعين أيضًا التأكد من أن تفاصيل الاتصال بمسؤول حماية البيانات متاحة على الصعيدين الخارجي والداخلي.

واتخذت المادة (37) فقرة (3) من النظام الأوروبي العام لحماية البيانات نهجًا مشابهًا، حيث نصت على أنه يجوز للسلطات أو الهيئات العامة المتعددة أيضًا تعيين مسؤول حماية بيانات واحد، بمجرد أخذ هيكلها التنظيمي وحجمها في الاعتبار. وعليه، فإذا كان سيتم تعيين مسؤول حماية واحد لمجموعة متنوعة من المهام عبر هذه الكيانات، فإن مهمة وحدة التحكم أو المعالج هي التأكد من أن مسؤول حماية البيانات يمكنه أداء أنشطته بكفاءة. بعبارة أخرى، يجب ألا يعيق تصرفهم بصفتهم كيانات متعددة، التنفيذ الفعال لمهامهم، لضمان فاعلية مسؤول حماية البيانات. كما توصي الهيئة الاستشارية الأوروبية المستقلة بأن تكون موجودة داخل الاتحاد الأوروبي، بغض النظر عما إذا كانت وحدة التحكم والمعالج نفسه قد تم إنشاؤهما أيضًا في الاتحاد.

كما تنص المادة 37 (4) من النظام الأوروبي العام لحماية البيانات الشخصية على أنه في حالات أخرى غير تلك المشار إليها في المادة (37) (1)، قد يظل من الموصى به أو اللازم

بموجب قانون الدولة العضو أن يقوم المتحكم أو المعالج، أو مجموعات من هذا القبيل، بتعيين مسؤول حماية البيانات. وقد يعمل مسؤول حماية البيانات هذا بعد ذلك نيابة عن هذه الجمعيات أو الهيئات الأخرى التي تمثل وحدات التحكم أو المعالجات، على سبيل المثال، كما يمكن أن يكون مسؤول حماية البيانات في هذا السياق مفيداً في تقديم المشورة لمجموعات وحدات التحكم أو المعالجات بشأن المشكلات التي يتم مواجهتها بشكل متكرر، ويمكن أن يعمل أيضاً كقناة اتصال بين وحدات التحكم والمعالجات المماثلة.

وتحدد المادة (37) (5) من النظام الأوروبي العام لحماية البيانات الشخصية أنه يجب تعيين مسؤول حماية البيانات على أساس الصفات المهنية ومعرفة الخبراء بقانون حماية البيانات، على وجه الخصوص، ويشير هذا الحكم إلى المادة (39) من النظام الأوروبي العام لحماية البيانات، التي توضح بالتفصيل مهام مسؤول حماية البيانات. وتشمل هذه، على سبيل المثال لا الحصر:

- مهام مثل إبلاغ المراقب والمعالج بالتزاماتهما بموجب النظام الأوروبي العام لحماية البيانات الشخصية.
- مراقبة الامتثال للنظام الأوروبي العام لحماية البيانات الشخصية والمساعدة في تحديد المسؤوليات وتدريب الموظفين المشاركين في عمليات المعالجة.
- تقديم المساعدة في تقييمات تأثير حماية البيانات¹⁹⁷ (DPIAs) عند الحاجة، ومراقبة الامتثال لها، وأخيراً التعاون مع إدارة الشؤون السياسية والعمل كقناة اتصال.

كما أعطت المادة (37) (6) من النظام الأوروبي العام لحماية البيانات الشخصية مسؤول حماية البيانات المعين أن يكون إما مراقباً أو موظفاً لدى المعالج، أو بدلاً من ذلك يتم تعيينه على أساس عقد الخدمة. ويمكن تفسير هذا الحكم على أنه يوفر مرونة إضافية لوحدة التحكم أو المعالج في تحديد أفضل طريقة لتوظيف مسؤول حماية البيانات لمنظمتهم. والأهم من ذلك أنه لا يتطلب أيضاً أن يكون مسؤول حماية البيانات هيئة محايدة تماماً وغير مرتبطة بوحدة التحكم أو المعالج، تماماً مثل المدقق المستقل. ومع ذلك من الضروري أن يستوفي مسؤول حماية البيانات (Data Protection Officer - DPO) المتطلبات المعمول بها في المادة (4) من النظام الأوروبي العام لحماية البيانات، ومنها على سبيل المثال، عدم وجود تضارب في المصالح لديهم.

أخيراً تتطلب المادة (37) (7) من النظام الأوروبي العام لحماية البيانات الشخصية، أن يقوم المتحكم أو المعالج بنشر تفاصيل الاتصال الخاصة بمسؤول حماية البيانات، وإبلاغ إدارة

¹⁹⁷ Data Protection Impact Assessments

حماية البيانات (Data Protection Authority- DPA) ذات الصلة بها. ويمكن للمرء أن يفسر غاية هذا الحكم ألا وهي تسهيل الاتصال والشفافية بين صاحب البيانات أو إدارة حماية البيانات ومسؤول حماية البيانات.

ومع ذلك، لا يتطلب الحكم السابق نشر اسم مسؤول حماية البيانات، بمعنى آخر، قد تتضمن تفاصيل الاتصال عنوان البريد الإلكتروني لجهة الاتصال، ولكن لا يلزم بالضرورة أن تؤدي إلى نشر أي بيانات شخصية.

وأما فيما يتعلق بإجراءات القيد في سجل مسؤولي حماية البيانات فقد حددها القرار البحريني رقم (46) لسنة 2022 المتعلق بإجراءات قيد مراقب حماية البيانات الخارجي في المادة (6) حيث يجب أن يتم تقديم طلب إلكتروني من خلال الموقع الإلكتروني الخاص بذلك مشفوعاً بالمستندات الثبوتية والبيانات أيضاً، ويتطلب من الشخص الطبيعي عدة أمور منها:

شهادة الخبرة، وشهادة حسن سيرة وسلوك، ونسخة من بطاقة الهوية أو جواز السفر، وصورة شخصية، والعنوان وبيانات الاتصال، والمؤهلات العلمية والسيرة الذاتية وهي مماثلة للاشتراطات الواجب توافرها عند قيد مراقب حماية البيانات الداخلي المنصوص عليها في المادة (10).

أما بالنسبة للشخص الاعتباري فالشروط الواجب توافرها فيه عند قيده كمراقب حماية بيانات خارجي هي توافر نسخة من السجل التجاري والترخيص، والعنوان وبيانات الاتصال¹⁹⁸.

ومن خلال ما سبق نجد أن تعيين مسؤول حماية بيانات يحتمل أحد أمرين: إما أن يتم تعيين شخص في الشركة يتفرغ لهذه الوظيفة في الشركة فحسب، أو أن يتم إسناد هذه الوظيفة لشخص غير متفرغ خارج الشركة. وجاء موقف المشرع البحريني مماثلاً لأحكام النظام الأوروبي العام لحماية البيانات الشخصية، حيث يسمح بأن يكون مسؤول حماية البيانات تابعاً لهيئة العاملين في الجهة أو المؤسسة، كما قد يتولى ذلك الموقع بناءً على عقد خدمة، أي دون تفرغ وذلك وفقاً للفقرة (6) من المادة (37) من النظام ، حتى إنه من الممكن تعيين مسؤول حماية بيانات لأكثر من جهة في ذات الوقت بموجب الفقرة (2) من المادة ذاتها¹⁹⁹.

ومن الملاحظ في هذا الصدد إن قانون حماية البيانات الشخصية البحريني قد صمت عن ضمانات عمل مسؤول حماية البيانات، إذ يفترض أن يتمتع مسؤول حماية البيانات بقدر من

¹⁹⁸ القرار الوزاري رقم (46) لسنة 2022، بشأن مراقبي حماية البيانات الشخصية، الجريدة الرسمية، العدد، 3594، الخميس 17 مارس 2022.

¹⁹⁹ Art. 37 GDPR Designation of the data protection officer

1. “The controller and the processor shall designate a data protection officer in any case where.....”

الاستقلال في ممارسة مهامه، وهو ما يستدعي ألا يتلقى أي توجيهات من رؤوسيه بخصوص عمله وأن يقوم بوظيفته وفقاً للقانون وتعليمات مركز حماية البيانات فحسب.

ثانياً: التزامات مراقب حماية البيانات

تناولت المادة (10) من القانون البحريني لحماية البيانات الشخصية رقم (30) لسنة 2018 الالتزامات الواقعة على مسؤول حماية البيانات الشخصية، وقامت في هذا الصدد برسم إطار عام وطرح أمثلة خاصة للالتزامات التي يتحملها مراقب حماية البيانات، وهو ما يعني أن تلك الالتزامات المذكورة في المادة جاءت على سبيل المثال وليس الحصر. وقد أجملت المادة (10) سאלفة الذكر في فقرتها الأولى طبيعة التزامات مراقب حماية البيانات في العموم قبل أن تفصل بعضها، حيث يتولى مراقب حماية البيانات ما يأتي:

- مساعدة مدير البيانات في مباشرة حقوقه والالتزام بواجباته المقررة بموجب أحكام هذا القانون.
- التنسيق بين الهيئة ومدير البيانات بشأن قيام الأخير بتطبيق الأحكام الخاصة بمعالجة البيانات الشخصية.
- التَّحَقُّق من قيام مدير البيانات بمعالجة البيانات وفقاً لأحكام هذا القانون، ويتعيَّن عليه إذا قامت لديه دلائل على وقوع أية مخالفة في هذا الشأن إخطار مدير البيانات بذلك فوراً لإزالة أسباب المخالفة أو إجراء التصحيح اللازم في أقرب وقت.
- إخطار الهيئة بالمخالفات التي قامت لديه دلائل جدية على وقوعها ولم يبادر مدير البيانات بإزالة أسبابها أو إجراء التصحيح اللازم لها رغم مُضي فترة تجاوز عشرة أيام على إخطاره بذلك. ومسك سجل بعمليات المعالجة التي يتعيَّن على مدير البيانات إخطار الهيئة بها وفقاً لأحكام المادة (14) من هذا القانون.
- يلتزم مدير البيانات بمسك السجل في حالة عدم تعيين مراقب لحماية البيانات. ويجب أن يشتمل هذا السجل -كحد أدنى- على البيانات التي يتعيَّن تقديمها وفقاً لأحكام المادة المشار إليها، وعلى مراقب حماية البيانات إخطار الهيئة بنسخة محدَّثة من هذا السجل مرة واحدة كل شهر. كما يتولى مراقب حماية البيانات مباشرة مهامه في استقلال وحيدة.

هذا بالإضافة إلى القرار الوزاري رقم (46) لسنة 2020 المتعلق بمراقبة حماية البيانات حيث قام بوضع مجموعة من الالتزامات التي تقع على عاتق مراقب حماية البيانات الخارجي والداخلي في المادة (13) منه، وهي كالآتي:

- أن يفصح لمدير البيانات عما يكون من شأنه تعارض مصالح كمراقب حماية بيانات أو قد يؤثر على استقلاله، أو إذا كان معيناً أو سبق له التعيين كمراقب حماية بيانات خارجي مع مدير بيانات منافس أو كانت تربطه به مصالح شخصية قد تؤثر أو تتعارض مع قبول مهمته عند مدير البيانات. ويجب القيام بتجديد الإفصاح فوراً كلما حدث عليه تغيير.
- كما يجب عليه أيضاً أن يلتزم بعدم إفشاء أي معلومات أو بيانات تتعلق بمدير البيانات أو بطبيعة العمل أو بأسراره التي وصلت إليه أو كانت تحت بصره أو كان متاحاً له الوصول إليها بحكم عمله كمراقب حماية بيانات. أو استخدام أي من المعلومات أو البيانات لمصلحته الشخصية أو لمصلحة الغير دون وجه حق. كما تشمل هذه المعلومات والبيانات أسرار العمل وبيانات العملاء والموظفين، وكذلك المتعاملين مع مدير البيانات وبيانات الأنظمة المعلوماتية والتقنية والفنية وغير ذلك من المعلومات.

كما أشار النظام الأوروبي العام لحماية البيانات الشخصية إلى مجموعة من الالتزامات التي تقع على عاتق مسؤول حماية البيانات وفقاً للمادة (39). فيجب أن يتولى مسؤول حماية البيانات المهام التالية على الأقل من الالتزامات التي تقع على عاتق مراقب حماية البيانات الداخلي وهي إبلاغ وحدة التحكم أو المعالج والموظفين الذين يقومون بمعالجة بياناتهم وفقاً لهذا النظام، وبنود حماية البيانات الأخرى في الاتحاد أو الدول الأعضاء لمراقبة الامتثال لهذا النظام مع أحكام حماية البيانات الأخرى في الاتحاد أو الدول الأعضاء ومع سياسات وحدة التحكم أو المعالج فيما يتعلق بحماية البيانات الشخصية، بما في ذلك إسناد المسؤوليات وزيادة الوعي وتدريب الموظفين المشاركين في معالجة البيانات وعمليات التدقيق ذات الصلة، وذلك لتقديم المشورة عند الطلب فيما يتعلق بتقييم تأثير حماية البيانات ومراقبة أدائها وفقاً للمادة (35)، و للتعاون مع السلطة الإشرافية، للعمل كنقطة اتصال للسلطة الإشرافية بشأن القضايا المتعلقة بالمعالجة، بما في ذلك التشاور المسبق المشار إليه في المادة (36)، والتشاور عند الاقتضاء فيما يتعلق بأي مسألة أخرى. وكذلك يجب على مسؤول حماية البيانات في أداء مهامه أن يولي اهتماماً للمخاطر المرتبطة بعمليات

المعالجة، مع مراعاة طبيعة المعالجة ونطاقها وسياقها وأغراضها²⁰⁰. كما يلتزم أيضاً بالسرية فيما يتعلق بأداء مهامه، وفقاً لقانون الاتحاد أو قانون الدول الأعضاء²⁰¹.

أما بالنسبة لالتزام مراقب حماية البيانات في مواجهة الشخص المعني بالبيانات فتجيز المادة (4/38) من النظام الأوروبي العام لحماية البيانات الشخصية لأصحاب البيانات الاتصال بمسؤول حماية البيانات فيما يتعلق بجميع القضايا المتعلقة بمعالجة بياناتهم الشخصية وممارسة حقوقهم بموجب هذا النظام²⁰².

المبحث الثاني

آليات الحماية ومعوقات التطبيق

لجأت أغلب التشريعات إلى حماية البيانات الشخصية وفق آليات حماية قانونية محددة، ومنها قانون حماية البيانات الشخصية البحريني والنظام الأوروبي العام لحماية البيانات الشخصية، حيث تضمنت هذه القوانين مجموعة من القواعد التي تكفل الحماية القانونية للبيانات الشخصية، وذلك نتيجة للتطور التكنولوجي وتزايد استخدام تطبيقات إنترنت الأشياء، ما جعل البيانات الشخصية للمستخدمين عرضة للاعتداء، الأمر الذي تطلب وضع العقوبات الرادعة لمرتكبيها، كما تم إسناد صلاحية الرقابة للسلطة الوطنية ليتم التأكد من التطبيق السليم للقانون، وتحقيق الحماية للبيانات الشخصية، وعلى الرغم من الجهود المبذولة لفرض آليات قانونية للعديد من المخاطر الماسة بعمليات المعالجة، فإنها ما زالت تعاني من العديد من نقاط الضعف التي تحد من فاعليتها

²⁰⁰ Art. 39 GDPR asks of the data protection officer
The data protection officer shall have at least the following tasks:

a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;.....”

²⁰¹ Art. 38 GDPR Position of the data protection officer:

1. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

²⁰² Art. 38 GDPR Position of the data protection officer:

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.”

في مواجهة مخاطر تقنية المعلومات التي تتطور يوماً بعد يوم. وسوف نتناول هذا الموضوع في مطلبين:

المطلب الأول: آليات حماية خصوصية البيانات الشخصية

المطلب الثاني: معوقات تطبيق حماية البيانات الشخصية

المطلب الأول

آليات حماية خصوصية البيانات الشخصية

لقد استحدث النظام الأوروبي العام لحماية البيانات الشخصية وقانون حماية البيانات الشخصية البحريني آلية مؤسساتية من أجل السهر على مراقبة وحماية البيانات الشخصية المتمثلة في الجهة الوطنية المعنية بحماية البيانات الشخصية، كما أقر كل من المشرع الأوروبي والمشرع البحريني مجموعة من العقوبات الردعية ضد كل مسؤول عن المعالجة ينتهك أحكام هذا القانون. وسوف نتناول هذه الآليات القانونية على الشكل الآتي:

الفرع الأول: الجهة الوطنية المعنية بحماية البيانات الشخصية

الفرع الثاني: محدودية الآليات المؤسساتية لحماية البيانات الشخصية

الفرع الأول: الجهة الوطنية المعنية بحماية البيانات الشخصية

لا تعتبر الأطر القانونية فعالة إلا إذا تم توفير آليات وإمكانات للتنفيذ الفاعل، والمراقبة على التطبيق السليم للقانون. لهذا حرص المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية وكذلك المشرع البحريني على إسناد مهمة الرقابة للهيئة الوطنية المختصة بحماية البيانات الشخصية، حيث يقوم هذا الجهاز الإداري بالإشراف على تطبيق قواعد وأحكام القانون، وفقاً للمبادئ والأهداف المعلنة فيه. كما إن إنشاء هذا الجهاز الإداري يدل على النية الجدية في الحماية، وكذلك على وعي الحكومة المعنية بخصوصية مسألة حماية البيانات الشخصية، وخاصة مع التطور الرقمي والتكنولوجي، ما يستوجب إضافة إلى وجود القانون والإلزام بمبادئه، إماماً بتقنيات البرامج، والتطبيقات الرقمية، ورؤية واضحة وشاملة. ويترجم ذلك عملياً

بتشكيل الهيئة من عدد من الأعضاء من خلفيات مهنية وعلمية وخبرانية يمكنها التعامل، مع التطورات التكنولوجية والتقنية المختلفة، لظاهرة معالجة البيانات الشخصية²⁰³.

ووفقاً لذلك، نص المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية في المادة (51) منه على أنه يجب على كل دولة عضو في الاتحاد الأوروبي أن تنشئ سلطة إشرافية واحدة على الأقل تمارس مهماتها باستقلالية تامة، وذلك لتأمين حماية فعالة للأفراد، في مواجهة معالجة البيانات الشخصية في ظل التطورات التكنولوجية²⁰⁴.

كما أقر المشرع البحريني إنشاء هيئة تخضع لذات المعايير التي نص عليها النظام الأوروبي العام لحماية البيانات الشخصية، وذلك بموجب المادة (27) من قانون حماية البيانات الشخصية رقم (30) لسنة (2018)، حيث أسندت إلى هيئة حماية البيانات الشخصية مهمة الإشراف والرقابة على تطبيق أحكام القانون، ولهذه الهيئة شخصية اعتبارية واستقلال مالي وإداري، وتكون خاضعة لرقابة الوزير.

وكذلك فعل المشرع الإماراتي الذي أنشأ "مؤسسة بيانات دبي" بموجب نص المادة (3) من قانون إنشاء مؤسسة بيانات دبي، وأعطى لهذه المؤسسة الشخصية الاعتبارية، والأهلية القانونية اللازمة لمباشرة الأعمال والتصرفات القانونية²⁰⁵.

أولاً: نشأة الجهة الوطنية المعنية بحماية البيانات الشخصية

1. الطبيعة القانونية للجهة الوطنية المعنية بحماية البيانات الشخصية

الهيئة، أو السلطة الوطنية المختصة بحماية البيانات، تنشأ كجهاز إداري مستقل بموجب مرسوم، وذلك نظراً إلى طبيعة مهامها ودورها القيادي، والإشرافي، والتوعوي والقضائي. وتمنح لها صلاحيات من أجل أن تحقق هدفها في حماية البيانات الشخصية التي تكون محفوظة إما في ملفات ورقية، أو رقمية، في القطاعين العام والخاص. بالإضافة إلى ذلك، يجب أن تتخذ الهيئة قراراتها، وتصدر توصياتها بشكل مستقل عن أية سلطة يمكن أن تؤثر عليها. واستقلالية الهيئة تكون في عدم خضوع أعضائها للهرمية الوظيفية والإدارية

²⁰³ منى الأشقر جبور و محمود جبور، المرجع السابق، ص151.

²⁰⁴ Art. 51 GDPR Supervisory authority

"1-Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority')..."

²⁰⁵ قانون إنشاء مؤسسة بيانات دبي رقم (2)، حكومة دبي، الجريدة الرسمية، العدد (397)، 2016.

المتبعة في الوزارات، كما أنهم لا يتلقون أوامر، أو آراء أو تعليمات من أية وزارة، فلا يجوز لرئيس الهيئة أو لأعضائها أن يكونوا من الموظفين، أو من أصحاب المصالح في المؤسسات، أو الشركات العاملة في مجال الاتصالات ومعالجة البيانات. كما لا يجوز أن تتوافر لهم أية مصالح في مؤسسة تمارس هذه الأنشطة، سواء أكان ذلك بصورة مباشرة، أم غير مباشرة²⁰⁶.

ولقد أكد النظام الأوروبي العام لحماية البيانات الشخصية في المادة (51) منه على إنفاذ مبدأ الاستقلال فيما يتعلق بالجهات المنوط بها الرقابة على حماية البيانات، ويفترض وفقاً للنظام الأوروبي العام أن تتمتع السلطة الرقابية باستقلال تام في ممارسة نشاطها. ومن أجل أن يتحقق ذلك يجب مراعاة عدة أمور، وهي كالآتي:²⁰⁷

- يجب أن تعمل كل سلطة إشرافية باستقلالية تامة في أداء مهامها وممارسة صلاحياتها وفقاً للنظام.
- يجب على كل عضو أو أعضاء كل سلطة إشرافية عند أداء مهامهم وممارسة سلطاتهم عدم التأثير خارجياً، سواء كان مباشراً أو غير مباشر. وعدم طلب أو تلقي أي معلومات من شخص آخر. كذلك يجب أن يمتنعوا عن أي عمل لا يتوافق مع واجباتهم، ولا يجوز لهم خلال فترة ولايتهم الانخراط في أي مهنة غير متوافقة، سواء أكانت مربحة أم لا.
- ويجب أن تضمن كل دولة عضو تزويد كل سلطة إشرافية بالموارد البشرية والتقنية والمالية والمباني والبنية التحتية اللازمة لأداء مهامها بفاعلية وممارسة صلاحياتها، بما في ذلك تلك التي يتعين القيام بها في سياق المساعدة المتبادلة، والتعاون والمشاركة في مجلس الإدارة. وأيضاً التأكد من أن كل سلطة إشرافية تختار من يمثلها، وأن يكون لديها موظفوها الخاصون الذين يخضعون للتوجيه الحصري للعضو أو أعضاء السلطة الإشرافية المعنية. وكذلك التأكد من أن كل سلطة إشرافية تخضع للرقابة المالية التي لا تؤثر في استقلاليتها، وأن لديها ميزانيات سنوية منفصلة وعامة، والتي قد تكون جزءاً من الميزانية العامة للدولة أو الميزانية الوطنية.

²⁰⁶ خالدي فتيحة، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كآلية لحماية الحق في الخصوصية في ظل القانون 07-18، جامعة أكلي محند أو لحاج- البويرة، مجلة الحقوق والعلوم الإنسانية، المجلد 13 ، العدد 04،

²⁰⁷ Art. 51 GDPR Supervisory authority

“1-Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’). ...”

ومن ناحية أخرى نجد أن النظام الأوروبي العام لحماية البيانات الشخصية نص في المادة (53) منه على أنه يجب على الدول الأعضاء أن تنص على تعيين كل عضو في سلطاتها الإشرافية عن طريق إجراء شفاف إما من برلمانهم أو حكومتهم أو رئيس دولتهم أو هيئة مستقلة يعهد إليها التعيين بموجب قانون الدول الأعضاء. ويجب أن يتمتع كل عضو بالمؤهلات والخبرة والمهارات، ولا سيما في مجال حماية البيانات الشخصية اللازمة لأداء واجباته وممارسة صلاحياته. وتنتهي واجبات العضو في حال انتهاء مدة المنصب أو الاستقالة أو التقاعد الإجباري، وفقاً لقانون الدولة العضو المعنية ولا يجوز فصل العضو إلا في حالات سوء السلوك الجسيم أو إذا لم يعد العضو يستوفي الشروط المطلوبة لأداء الواجبات²⁰⁸.

كما نصت المادة (54) من النظام الأوروبي العام لحماية البيانات الشخصية على مدة ولاية العضو أو أعضاء كل سلطة إشرافية بأنها لا تقل عن أربع سنوات، باستثناء التعيين الأول بعد 24 مايو 2016، والتي قد يتم جزء منها لفترة أقصر، حيث يكون ذلك ضرورياً لحماية استقلالية السلطة الإشرافية عن طريق إجراء تعيين متدرج²⁰⁹.

ووفقاً لما سبق نجد أن النظام الأوروبي العام لحماية البيانات الشخصية حرص على تمتع السلطة الإشرافية باستقلالية تامة، وهذا ما سار عليه المشرع البحريني، بالرجوع إلى المادة (27) من قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018، نجد أن المشرع قد منح الشخصية الاعتبارية للهيئة الوطنية المعنية بحماية البيانات، حيث يكون لها الاستقلال المالي والإداري، ولكن أخضعها لرقابة الوزير المختص بشؤون العدل. و وفقاً للمادة (28) من القانون، يتولى الوزير متابعة مدى التزام الهيئة بأحكام هذا القانون وبسياسة الدولة في مجال عمل الهيئة، ومدى قيامها بمباشرة مهامها بكفاءة وفاعلية في حدود الاعتمادات المالية المتاحة لها. مع عدم الإخلال بما تتمتع به الهيئة من استقلال في مباشرة مهامها وصلاحياتها وفقاً لأحكام هذا القانون. كما نص المشرع البحريني في المادة (29) على تخصيص ميزانية مالية مستقلة للهيئة حرصاً منه على استقلاليتها.

²⁰⁸ Art. 53 GDPR General conditions for the members of the supervisory authority

"1-Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

– their parliament;

– their government;..."

²⁰⁹ Art. 54 GDPR Rules on the establishment of the supervisory authority

"the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure.."

ونلاحظ من خلال ما سبق أن النص القانوني تكررت فيه عبارة الاستقلالية الإدارية مرتين، وهو ما يعكس -بحسب نظرنا- عزم المشرع البحريني وتأكيد على استقلالية هذه السلطة رغم التناقض الذي وقع فيه في النص نفسه، حيث أخضع المشرع الاستقلالية المالية والإدارية لرقابة الوزير، ما يدل على أن الاستقلالية هنا نسبية وليست مطلقة، وهذا ما يعكس تبعية السلطة الوطنية وعدم استقلاليتها عن السلطة التنفيذية، الأمر الذي قد ينعكس سلبيًا على أداء السلطة لمهامها كجهاز يهدف إلى حماية البيانات الشخصية²¹⁰.

2- مهام وصلاحيات الجهة الوطنية المعنية بحماية البيانات الشخصية

لقد خول قانون حماية البيانات الشخصية البحريني والنظام الأوروبي العام لحماية البيانات الشخصية الجهة الوطنية أو ما يسمى بمركز حماية البيانات الشخصية مجموعة من الأدوار التي يمكن القيام بها من أجل حماية البيانات الشخصية. وقد تنوعت الأدوار التي يفترض اضطلاع المركز بها، بين ما يمكن تقسيمه إلى أدوار استشارية، وأخرى رقابية. وبالرجوع إلى قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018، نجد أن المشرع قد منح الهيئة بموجب المادة (30) منه سلطات واسعة تتعدى السلطات الممنوحة للهيئات الإدارية التقليدية، والتي يمكن تلخيصها فيما يلي:

1. إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، ويشمل الحق في الإعلام، والإعلام المسبق للمعني بهوية المسؤول عن المعالجة والهدف منها، وكل معلومة إضافية مفيدة ولا سيما المرسل إليه، ومدى إلزامية الرد والآثار المترتبة على ذلك وحقوقه ونقل البيانات إلى بلد أجنبي، وفي حال استعمال المعلومات في شبكة مفتوحة يجب إعلام المعني أنه يمكن تداول هذه المعلومات في الشبكات دون ضمانات السلامة، وأنها قد تتعرض للقراءة والاستعمال غير المرخص من طرف الغير.
2. القيام بالرقابة والتفتيش على أعمال مديري البيانات المتعلقة بمعالجة البيانات الشخصية للتحقق من التزامهم بأحكام هذا القانون، وتشجيعهم على وضع الأنظمة الكفيلة بحماية تلك البيانات على نحو يتفق وأحكام هذا القانون.

²¹⁰ في ذات السياق راجع: عبد العالي بالة، السلطة الوطنية لحماية حماية المعطيات ذات الطابع الشخصي بين الاستقلال والتبعية، جامعة خنشلة، المجلة الجزائرية للأمن الإنساني، المجلد 06، العدد 01، الجزائر، 2021، ص 788-789.

3. مراقبة الإجراءات المسبقة للمعالجة، إذ تقوم الهيئة الوطنية بإمساك السجل الوطني لحماية البيانات الشخصية وتقيّد فيه التصريحات المقدمة لها، والتراخيص والتصاريح المسلمة من طرفها؛ فالشخص القائم بالمعالجة يلزم بضرورة حصوله على تصريح أو ترخيص من الهيئة الوطنية من أجل معالجته للبيانات الشخصية.
4. تتولى الهيئة الوطنية تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة البيانات الشخصية أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.
5. بالإضافة إلى ذلك يكون للهيئة وفقاً للمادة (47) من القانون سلطة مباشرة التحقيق سواء من تلقاء نفسها أو بناءً على طلب الوزير أو بناءً على البلاغات والشكاوى الجدية التي قدمت لها، للتحقق من أن مدير بيانات أو مراقب حماية بيانات قد ارتكب مخالفة لأيٍّ من أحكام هذا القانون من عدمه²¹¹.

ومنحت المادة (47) للهيئة الحق في أن تفحص الشكاوى المقدمة والمستندات المؤيدة لها، للوقوف على مدى جديتها ويجوز أن تطلب تزويدها بأي بيانات تراها ضرورية. وفي حال عدم كفاية الأدلة للتحقيق في الشكاوى للهيئة أن تقرر حفظها. وفي حال قبلت الهيئة الشكاوى فإنها تقوم بإخطار الأطراف المشكو في حقهم وجميع الأطراف ذوي الصلة بموضوع الشكاوى، ويجب أن يتضمن الإخطار الأدلة والقرائن والمعلومات التي تملكها الهيئة المتعلقة بالمخالفات. ومن حق الهيئة الرد على الإخطار خلال سبعة أيام عمل من تاريخ وصوله إليها، ويجب أن يشتمل الرد على دفاعهم وملاحظاتهم. وللهيئة، بعد دراسة الرد على الإخطار، أن تأمر بحفظ الموضوع أو بالبدء في إجراءات التحقيق، وعليها إخطار الأطراف المعنية بالأمر الصادر عنها في أيٍّ من الحالتين. كما لها أن تباشر التحقيق بنفسها أو تشكل لذلك لجنة ثلاثية من ذوي الاختصاص من داخل الهيئة أو خارجها، أو تكلف أيٍّ شخص مؤهل للقيام بذلك²¹².

ومن ناحية أخرى يحق للجنة التحقيق أن تتدب أيًا من مأموري الضبط القضائي، وذلك في سبيل إنجاز عملها أو من غيرهم للقيام بأعمال التفتيش للتحقق من تنفيذ أحكام القانون، وكذلك المفتشين الذين يصدر قرار بتحديدهم من الوزير المختص بشؤون العدل، وصفة مأموري الضبط القضائي تكون بالنسبة للجرائم المنصوص عليها في هذا النظام والتي تقع في دائرة اختصاصهم وتكون متعلقة بأعمال وظائفهم، وعندما

²¹¹ جاء تحديد الإجراءات والقواعد الخاصة بتقديم الشكاوى في القرار التنفيذي رقم (49) بشأن الإجراءات والقواعد الخاصة بتقديم الشكاوى عن مخالفة أحكام قانون حماية البيانات الشخصية، الجريدة الرسمية، العدد: 3593، 2022.

²¹² القرار الوزاري رقم (49) لسنة 2022 بشأن الإجراءات والقواعد الخاصة، الجريدة الرسمية، العدد 3593، 2022.

يتم إنهاء إجراءات التحقيق يجب على لجنة التحقيق أن تصدر تقريراً مسبباً بالنتائج التي توصلت إليها، ويجب أن ترفق معه ملف التحقيق كاملاً وتسلمه للرئيس التنفيذي خلال فترة لا تتجاوز ستة أشهر من تاريخ بدء إجراءات التحقيق، ويمكن للجنة التحقيق أن تطلب من الرئيس التنفيذي تمديد الفترة قبل انتهائها لمدد أو لمدة إضافية ولكن يجب ألا تتجاوز في مجموعها ستة أشهر، وذلك في الحالات التي يكون التأخير فيها لأسباب خارجة عن إرادة اللجنة.

6. إجراء البحوث والدراسات ودعمها في هذا المجال، والعمل على الاستفادة من نتائجها.
7. تنظيم دورات وبرامج تدريبية وتنقيفية بهدف التوعية بأحكام هذا القانون، ونشر ثقافة حماية البيانات الشخصية.
8. تمثيل المملكة في المؤتمرات الدولية، باعتبارها الجهة المختصة بحماية البيانات الشخصية²¹³.

ومن ناحية أخرى فقد حدد النظام الأوروبي العام لحماية البيانات الشخصية المهام التي أسندتها للهيئة وذلك بموجب المادة (57) منه، وهي كالآتي:²¹⁴

- تلتزم الهيئة بمراقبة وتنفيذ النظام الأوروبي العام لحماية البيانات الشخصية.
- تعزيز الوعي العام، حيث منح النظام الأوروبي العام لحماية البيانات الشخصية الهيئة مهمة القيام بتوعية الجمهور، ليس فقط بالمخاطر المرتبطة بمعالجة البيانات، ولكن أيضاً بالضمانات والحماية التي يوفرها النظام الأوروبي العام لحماية البيانات الشخصية لموضوعات البيانات والأطفال.
- تقديم المشورة للدول الأعضاء، حيث لا تقوم هيئات حماية البيانات فقط برفع مستوى الوعي العام، ولكنها توفر أيضاً إرشادات محددة حول ممارسة حقوق النظام الأوروبي العام لحماية البيانات الخاصة بهم. ويشمل مصطلح "الحقوق" الحقوق المادية (مثل الحق في النسيان، وكذلك الحقوق الإجرائية وخيارات الإنفاذ القانوني).
- تعزيز وعي وحدات التحكم والمعالجات، فلا ينبغي أن تسلط الهيئة الضوء على المقترحات التشريعية والتدابير الإدارية فحسب، بل يجب أن تسلط الضوء أيضاً على الجهات الفاعلة التي يحكم أعمالها النظام الأوروبي العام لحماية البيانات الشخصية. وفي الممارسة العملية،

²¹³ المادة رقم 30 قانون حماية البيانات الشخصية رقم 30 لسنة 2018.

²¹⁴ Art. 57 GDPR Tasks

“Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(A) monitor and enforce the application of this Regulation.

(B) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention...”

يمكن تنفيذ هذه المهمة، على سبيل المثال من خلال الدورات التدريبية والبيانات الرسمية، وكذلك من خلال الاتصالات المباشرة مع الأطراف الملزمة في حال وجود صعوبات واضحة في تفسير الأحكام الجديدة.

- التعامل مع الشكاوى والتحقيق فيها، فيتم التعامل مع الشكاوى المقدمة من صاحب البيانات، أو بواسطة هيئة أو منظمة أو جمعية، والتحقيق قدر الإمكان في موضوع الشكاوى، وإبلاغ صاحب الشكاوى بالتقدم في التحقيق وبناتجها في غضون فترة معقولة، ولا سيما إذا كان من الضروري إجراء مزيد من التحقيق أو التنسيق مع سلطة إشرافية أخرى، حيث نص المشرع الأوروبي في المادة (56) فقرة (3) من النظام على أنه تكون كل سلطة إشرافية مختصة بمعالجة الشكاوى المقدمة إليها أو انتهاك محتمل لهذا النظام، إذا كان الموضوع يتعلق فقط بمؤسسة في الدولة العضو بها أو يؤثر بشكل كبير على مواضيع البيانات فقط في الدولة العضو فيها . كما يجب على السلطة الإشرافية دون تأخير النظر بشأن هذه المسألة في غضون ثلاثة أسابيع²¹⁵.
- التعاون مع هيئات الإشراف الأخرى، بما في ذلك تبادل المعلومات وتقديم المساعدة المتبادلة، بهدف ضمان الاتساق في تطبيق النظام الأوروبي العام لحماية البيانات الشخصية وإنفاذه²¹⁶.
- القيام برصد التطورات ذات الصلة، ما يكون له تأثير في حماية البيانات الشخصية، ولا سيما تطوير تكنولوجيا المعلومات والاتصالات والممارسات التجارية للقيام بذلك، كما يجب أن يتم توفير الموارد البشرية والتقنية الملائمة.
- اعتماد بنود تعاقدية قياسية (Standard Contractual Clauses – SCCs)، وهي عبارة عن بنود حماية بيانات نموذجية موحدة ومعتمدة مسبقاً تسمح للمراقبين والمعالجين بالامتثال لالتزاماتهم بموجب بيانات الاتحاد الأوروبي من النظام الأوروبي العام لحماية البيانات الشخصية. يمكن دمجها من قبل وحدات التحكم والمعالجات في ترتيباتهم التعاقدية مع الأطراف الأخرى، ويمكن استخدام البنود على أساس طوعي لإثبات الامتثال لمتطلبات حماية البيانات، ويكون لهذه البنود قوة إلزامية باعتبارها التزاماً تعاقدياً. كما تتمتع المفوضية

²¹⁵Art. 56 GDPR Competence of the lead supervisory authority

"3- In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. 2Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

216Art. 63 GDPR Consistency mechanism "In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section....".

الأوروبية بسلطة اعتماد البنود التعاقدية القياسية لتنظيم العلاقة بين وحدات التحكم والمعاملات، وكذلك لنقل البيانات الشخصية إلى دول خارج المنطقة الاقتصادية الأوروبية²¹⁷.

- يجب على السلطة الإشرافية بموجب الفقرة (4) من المادة (35) إنشاء ونشر قائمة متعلقة بنوع عمليات المعالجة التي تخضع لمتطلبات تقييم تأثير البيانات، وكذلك الحفاظ عليها²¹⁸.
- التشجيع على وضع مدونات لقواعد السلوك وإبداء الرأي والموافقة على قواعد السلوك تلك التي توفر ضمانات كافية، ووفقاً للمادة (40) من النظام يجب على الدول الأعضاء والسلطات الإشرافية والمجلس والمفوضية تشجيع وضع قواعد السلوك التي تهدف إلى المساهمة في التطبيق السليم لهذا النظام، مع مراعاة السمات المحددة لقطاعات المعالجة المختلفة والاحتياجات الخاصة للمؤسسات الصغيرة والشركات الكبيرة والمتوسطة، ويجوز للجمعيات والهيئات الأخرى التي تمثل فئات من وحدات التحكم أو المعاملات إعداد قواعد سلوك، أو تعديل أو توسيع هذه القواعد²¹⁹. كما يمكن وفقاً للمادة (41) من النظام العام القيام بمراقبة قواعد السلوك من قبل هيئة تتمتع بمستوى مناسب من الخبرة²²⁰.
- بموجب المادة (36) من النظام، يجب على وحدة التحكم استشارة السلطة الإشرافية قبل المعالجة، حيث يشير تقييم تأثير حماية البيانات بموجب المادة (35) إلى أن المعالجة

217 لمزيد من التفاصيل حول البنود التعاقدية القياسية، يمكنك زيارة الموقع الرسمي للمفوضية الأوروبية عبر الرابط التالي:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en .

²¹⁸ Art. 35 GDPR Data protection impact assessment

"1-Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. 2A single assessment may address a set of similar processing operations that present similar high risks..."

²¹⁹ Art. 40 GDPR Codes of conduct

"1-The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises..."

²²⁰ Art. 41 GDPR Monitoring of approved codes of conduct

"1-Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority..."

ستؤدي إلى مخاطر عالية في ظل غياب التدابير التي يتخذها المراقب للتخفيف من المخاطر.

إذا رأت السلطة الإشرافية إن المعالجة من شأنها أن تنتهك النظام الأوروبي العام لحماية البيانات، ولا سيما في حال عدم تحديد المراقب أو التخفيف من المخاطر بشكل كافٍ، وجب عليها في غضون فترة ثمانية أسابيع من استلام طلب التشاور، تقديم المشورة المكتوبة إلى وحدة التحكم، وعند الاقتضاء إلى المعالج، كما يمكن تمديد هذه الفترة لمدة ستة أسابيع أخرى، مع الأخذ في الاعتبار مدى تعقيد المعالجة المقصودة، كما يجب على السلطة الإشرافية إبلاغ وحدة التحكم، وعند الاقتضاء، المعالج، بأي تمديد من هذا القبول في غضون شهر واحد من استلام طلب التشاور مع بيان أسباب التأخير. ويمكن تعليق هذه الفترات حتى تحصل السلطة الإشرافية على المعلومات التي طلبتها لأغراض التشاور. كما يجب على المراقب عند استشارة السلطة الإشرافية تزويدها بما يأتي:

1. عند اللزوم، المسؤوليات الخاصة بوحدة التحكم ووحدات التحكم المشتركة والمعالجات المشاركة في المعالجة، ولا سيما للمعالجة داخل مجموعة من التعهدات.
2. أغراض ووسائل المعالجة المقصودة.
3. التدابير والضمانات المقدمة لحماية حقوق وحريات الأشخاص المعنيين بالبيانات وفقاً للنظام عند الاقتضاء.
4. تفاصيل الاتصال بمسؤول حماية البيانات.
5. تقييم تأثير حماية البيانات، وأي معلومات أخرى تطلبها السلطة الإشرافية.

وبالإضافة إلى ذلك يتعين على الدول الأعضاء استشارة السلطة الإشرافية أثناء إعداد اقتراح لإجراء تشريعي يعتمد البرلمان الوطني، أو إجراء تنظيمي قائم على مثل هذا الإجراء التشريعي، والذي يتعلق بالتجهيز. وقد يتطلب قانون الدول الأعضاء من المتحكمين التشاور مع السلطة الإشرافية والحصول على إذن مسبق منها فيما يتعلق بالمعالجة من قبل وحدة تحكم لأداء مهمة يقوم بها المتحكم في المصلحة العامة، بما في ذلك المعالجة فيما يتعلق بالحماية الاجتماعية والصحة العامة²²¹.

²²¹ Art. 36 GDPR Prior consultation

"1-The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk..."

- ويجب على الدول الأعضاء والسلطات الإشرافية والمجلس والمفوضية التشجيع على وضع آليات لإصدار شهادات حماية البيانات وأختام وعلامات حماية البيانات، لغرض إثبات امتثال عمليات المعالجة من قبل وحدات التحكم والمعالجات لأحكام هذا النظام. كما يؤخذ في الاعتبار الاحتياجات الخاصة للمؤسسات متناهية الصغر والصغيرة والمتوسطة. كما يتم أيضًا الموافقة على معايير التصديق²²².
- صياغة ونشر معايير إنشاء هيئة لرصد مدونات السلوك عملاً بالمادة (41) من النظام، حيث يجوز إنشاء هيئة ذات خبرة لرصد مدونات قواعد السلوك، على أن يراعى تحقق الآتي:
 1. أن تظهر الهيئة استقلاليتها وخبرتها فيما يتعلق بموضوع المدونة بما يرضي السلطة الإشرافية المختصة.
 2. أن يكون هناك إجراءات تسمح للهيئة بتقييم أهلية وحدات التحكم والمعالجات المعنية.
 3. مراقبة امتثالها لأحكامها ومراجعة عملها بشكل دوري.
 4. أن تظهر الهيئة للسلطة الإشرافية المختصة أن مهامها وواجباتها لا تؤدي إلى تضارب في المصالح.
 5. يجب على الهيئة أن تراعي الضمانات المناسبة، عند اتخاذ الإجراء المناسب في حالات انتهاك المدونة من قبل مراقب أو المعالج، كما يجب على الهيئة إبلاغ السلطة الإشرافية المختصة بهذه الإجراءات وأسباب اتخاذها.
- ولا تنطبق هذه المادة على المعالجة التي تجريها الهيئات العامة²²³.
- وفقًا للمادة (43) من النظام، يجب على الهيئة أن تقوم بإصدار وتجديد الشهادات التي تتمتع بمستوى مناسب من الخبرة فيما يتعلق بحماية البيانات، بعد إبلاغ السلطة الإشرافية من أجل السماح لها بممارسة صلاحياتها²²⁴.

²²² Art. 40 GDPR Codes of conduct

"1 Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises..."

²²³ Art. 41 GDPR Monitoring of approved codes of conduct

"1- Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority..."

²²⁴ Art. 43 GDPR Certification bodies

"1-Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection

- عند الاقتضاء إجراء مراجعة دورية للشهادات الصادرة.
- الموافقة على قواعد الشركة الملزمة وفقا للمادة (47) من النظام، حيث توافق السلطة الإشرافية المختصة على قواعد الشركة الملزمة وفقاً لآلية الاتساق المنصوص عليها في المادة (63) من النظام، شريطة أن تكون ملزمة قانوناً وسارية وتنفذ من قبل كل عضو معني في مجموعة التعهدات²²⁵ أو مجموعة الشركات العاملة في نشاط اقتصادي مشترك، بما في ذلك موظفوها، كما تمنح صراحة الحقوق واجبة الإنفاذ لأصحاب البيانات فيما يتعلق بمعالجة بياناتهم الشخصية²²⁶.

- المساهمة في أنشطة المجلس.
- الاحتفاظ بسجلات داخلية لانتهاكات هذا النظام وللتدابير المتخذة في المادة (58) فقرة (2) من النظام.
- القيام بأي مهام أخرى متعلقة بحماية البيانات الشخصية²²⁷.

ونستطيع أن نستنتج مما سبق أن هناك مجموعة من الضوابط التي يتعين على الجهة الوطنية التقيد بها عند قيامها بمهامها المختلفة، وهي كالآتي:

- 1- يجب على رئيس وأعضاء الجهة الوطنية الالتزام بالحفاظ على الطابع السري للبيانات الشخصية التي اطلعوا عليها، ولو بعد انتهاء مهامهم.
- 2- لا يجوز لأعضاء الجهة الوطنية أن يملكو مصالح في أي مؤسسة تمارس نشاطاتها في مجال البيانات الشخصية.

shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. 2Member States shall ensure that those certification bodies are accredited by one or both of the following....”

²²⁵ غالباً ما تتكون مجموعة التعهدات من تعهد يمكن يمارس تأثيراً مهيماً على شركة أخرى أو مشروع خاضع للرقابة، على سبيل المثال، الملكية أو المشاركة المالية أو القواعد التي تحكمه أو سلطة تطبيق قواعد حماية البيانات الشخصية. يجب اعتبار التعهد الذي يتحكم في معالجة البيانات الشخصية في المؤسسات التابعة لها، جنباً إلى جنب مع تلك التعهدات، كمجموعة من التعهدات.

Recital 37Group of undertakings available at : [\(Recital 37 - Group of undertakings - General Data Protection Regulation \(GDPR\) \(gdpr-info.eu\)](https://gdpr-info.eu/Recital-37-Group-of-undertakings-General-Data-Protection-Regulation-(GDPR)) (last visit:12 December 2022).

²²⁶ Art. 47 GDPR Binding corporate rules

“1-The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees...”

²²⁷ Art. 57 GDPR Tasks

“1- Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

monitor and enforce the application of this Regulation.

promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention...”

3- يجب إنشاء سجل وطني لحماية البيانات الشخصية، تقيد فيه مختلف الملفات موضوع المعالجة من قبل السلطات العمومية، كما يتم تقييد جميع التصريحات المقدمة للجهة الوطنية والتراخيص المسلمة وغيرها من البيانات الضرورية المخول للأشخاص الاطلاع عليها وفق الإجراءات المحددة قانونا أو تنظيما.

3- تشكيل الجهة الوطنية المعنية بحماية البيانات الشخصية

أولاً: تشكيل مجلس الإدارة

تتشكل الجهة الوطنية المعنية بحماية البيانات الشخصية عن طريق تعيين أعضائها، وأنظمة التعيين قد تختلف باختلاف المهام المطلوبة من أعضاء الهيئة، على سبيل المثال تخضع الهيئة المستقلة لسيطرة البرلمان، وتكون له سلطة الاعتراض أو حتى النقض المسبب ضد قرار الحكومة عند تعيين الأعضاء. وتعطى صلاحية تعيين رئيس الهيئات المستقلة في قوانين بعض الدول مثل إيطاليا إلى رئيس الدولة²²⁸. كما يمكن أن تكون التعيينات سياسية كما هو الحال في الولايات المتحدة الأمريكية، وهذا النوع من التعيينات قد يؤدي إلى تعيين أعضاء ليس لديهم الكفاءة المطلوبة فلا يكون للدولة الحق في الاختيار، وكل دورها ينحصر في الموافقة فقط. بينما في إنجلترا يتم تعيين الأعضاء ممن يملكون الخبرة، وتكون شخصياتهم مستقلة عن السلطة السياسية التي تتولى الحكم. بينما هناك بلدان أخرى تقوم بتعيين شخصيات سياسية، لا تكون مؤيدة بالضرورة للسلطة الحاكمة، كوزراء، أو برلمانيين سابقين. وبشكل عام تميل الدول إلى تعيين الأعضاء، من بين الأشخاص الذين يقدمون ضمانا للاستقلالية، ويستوفون الشروط المطلوبة، لممارسة أعلى الوظائف الإدارية أو القضائية، و يملكون خبرات وكفاءات تمكنهم من إنجاز المهام المطلوب منهم تنفيذها وفق معايير موضوعية، دون انحياز، استنادا إلى قاعدة استقلالية القرار. كما يمكن للنظام المعتمد للتعين أن يكون مرنا، فيتم التعيين من قبل السلطتين التشريعية والتنفيذية، بناء على اقتراحات من الإدارات المختصة، إضافة إلى طريقة أصيلة ومباشرة عبر الانتخاب من أعضاء هيئة معينة، أو من بقية الأعضاء كما يحصل في بعض القوانين، مع اختيار رئيس هيئة الرقابة على حماية البيانات. وبشكل عام، من المفترض اختيار الأعضاء بناء على انتمائهم المهني، أو الوظيفي، أو المهارات المتوافرة، ويعزز هذا الأمر من خلال التشاور مع الجهات، التي ينتمي إليها المعنيون²²⁹.

²²⁸ غزال نسرين، حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، كلية الحقوق، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 59، العدد 1، 2019، الجزائر، ص 126.

²²⁹ منى الأشقر جبور ومحمود جبور، المرجع السابق، ص 156.

وبالعودة لنصوص المشرع البحريني، نجد إن أعضاء هيئة حماية البيانات الشخصية يتكونون من سبعة أعضاء من بينهم رئيس المجلس، يعينون بموجب مرسوم من قبل السلطة التنفيذية، كما يؤدي أعضاء الجهة الوطنية اليمين قبل تنصيبهم أمام المجلس الأعلى للقضاء، وهم كآلاتي²³⁰:

- عضو يرشحه رئيس الوزراء.
- عضو ترشحه جامعة البحرين من بين أعضاء هيئة التدريس بدرجة لا تقل عن أستاذ مشارك في تخصص مناسب لمجال عمل الهيئة.
- عضو ترشحه هيئة تنظيم الاتصالات من بين شاغلي الوظائف العليا بها.
- عضو يرشحه مصرف البحرين المركزي من بين شاغلي الوظائف العليا.
- عضو ترشحه غرفة تجارة وصناعة البحرين.
- عضو ترشحه الجهة التي يقدر الوزير، بعد التشاور مع محافظ مصرف البحرين المركزي، أنها الأوسع تمثيلاً لأصحاب الأعمال في قطاعات المؤسسات المالية.
- عضو ترشحه الجهة التي يقدر الوزير أنها الأوسع تمثيلاً للمختصين في مجال تقنية المعلومات.
- كما يحدد المرسوم مدة العضوية في مجلس الإدارة أربع سنوات قابلة للتجديد لمدة مماثلة مرة واحدة، إلا أنه بالنسبة لمجلس الإدارة الأول فإن عضوية رئيس المجلس وثلاثة من أعضائه تكون لمدة أربع سنوات، ومدة الباقين ثلاث سنوات.

ومن جهة أخرى نص النظام الأوروبي العام لحماية البيانات الشخصية في المادة (68) على كيفية تشكيل مجلس الإدارة، حيث يتم إنشاء مجلس حماية البيانات الأوروبي "مجلس الإدارة" كهيئة تابعة للاتحاد، وله شخصية قانونية مستقلة. ويتم تشكيله كآلاتي:

- يتم تمثيل المجلس برئيسه.
- كما يتألف المجلس من رئيس سلطة إشرافية واحدة لكل دولة عضو ومن مشرف حماية البيانات الأوروبي،²³¹ أو من ممثليهم المعنيين.
- عندما يكون في دولة عضو بها أكثر من سلطة إشرافية واحدة تكون مسؤولة عن مراقبة تطبيق الأحكام وفقاً لهذا النظام، يتم تعيين ممثل مشترك وفقاً لقانون تلك الدولة العضو.

²³⁰ المادة رقم 39 من قانون حماية البيانات الشخصية رقم 30 لسنة 2018.

²³¹ مشرف حماية البيانات الأوروبي (EDPS) هو سلطة حماية البيانات المسؤولة عن ضمان امتثال المؤسسات الأوروبية لقانون حماية البيانات الأوروبي.

ويلاحظ هنا أن المشرع الأوروبي لم ينص على قواعد تعيين ممثل مشترك بل ترك ذلك للقانون الوطني للدولة العضو.

• كما يحق للجنة المشاركة في أنشطة المجلس واجتماعاته دون الحق في التصويت، وكذلك تقوم بتعيين ممثل، ويقوم رئيس المجلس بإبلاغ اللجنة بأنشطة المجلس²³².
و كما أشرنا سابقا إلى أن المشرع الأوروبي منح الاستقلالية لمجلس الإدارة لحماية البيانات الشخصية عند قيامه بمهامه أو عند ممارسة صلاحياته.

ومن الجدير بالملاحظة من التشكيلة السابقة للسلطة الوطنية، إن المشرع البحريني قد حرص في قانون حماية البيانات الشخصية على دعم التشكيلة بالأساتذة والجامعيين ومن لهم خبرة في مجالات مختلفة، مثل الاتصالات والبنوك والمؤسسات المالية وغيرها، من أجل الاستفادة من خبراتهم في هذا المجال، أما المشرع الأوروبي وعلى خلاف المشرع البحريني، اكتفى بأن يمثل المجلس رئيس سلطة إشرافية واحدة ومن المشرف الأوروبي على حماية البيانات وممثليهم. ومن وجهة نظرنا فإن مسلك المشرع البحريني بالنسبة لتشكيلة الهيئة الوطنية كان أفضل من مسلك المشرع الأوروبي، وذلك على اعتبار أن المشرع البحريني حرص على شرط توافر الاختصاص القانوني والتقني في ممثلي السلطة الوطنية على عكس المشرع الأوروبي كما ذكرنا، الذي لم يضمن التنوع في تشكيلة المجلس، ما يدل على اهتمام المشرع البحريني بهذا الجهاز والسعي لتفعيله، وخاصة في ظل التطورات التكنولوجية والتقنية المتسارعة اليوم وظهور تطبيقات إنترنت الأشياء، وقد ساهم كل ذلك في تطوير وتفعيل آليات الحماية من أجل توفير الحماية الكافية للبيانات الشخصية.

ثانيا: مهام وصلاحيات مجلس الإدارة

ولقد قام المشرع البحريني باسناد مهام وصلاحيات إلى مجلس الإدارة مثلما فعل المشرع الأوروبي، وذلك وفي المادة (40) من القانون، فيتولى مجلس الإدارة مهمة رسم السياسة العامة التي تدير الهيئة عليها، وكذلك يقوم بالرقابة على أعمال الهيئة، وله اتخاذ ما يكفل لها مباشرة مهامها وصلاحياتها. كما أن له على وجه الخصوص:

²³² Art. 68 GDPR European Data Protection Board

"The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

The Board shall be represented by its Chair.

The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives..."

- أن يقوم بإصدار القرارات واللوائح، وكذلك يتخذ التدابير اللازمة لتنفيذ أحكام القانون.
- القيام باعتماد الهيكل التنظيمي وإصدار لوائح داخلية لتنظيم شؤون موظفي الهيئة.
- اعتماد الميزانية السنوية للهيئة، وكذلك حسابها الختامي المدقق.
- قبول الموارد المالية.
- يقوم مجلس الإدارة بدراسة التقارير الدورية التي تقدم له من قبل الرئيس التنفيذي عن سير العمل في الهيئة وتقرير ما يلزم بشأنها.
- القيام بكافة المهام والصلاحيات الأخرى التي تقرّر أحكام هذا القانون اختصاصه بها.
- من الجائز أن يعهد مجلس الإدارة إلى لجنة أو أكثر تشكّل من بين أعضائه، أو إلى رئيس المجلس، أو أيّ من أعضائه، أو الرئيس التنفيذي، القيام بمهام محددة، ماعدا إصدار اللوائح والقرارات التي تقرّر أحكام هذا القانون اختصاص مجلس الإدارة بإصدارها.

وكما منح المشرع الأوروبي بموجب المادة (70) مجلس الإدارة مهام وصلاحيات، حيث يحرص مجلس الإدارة على ضمان التطبيق المتسق لهذا النظام، وتحقيقاً منه لهذه الغاية يقوم المجلس بمبادرة منه أو عند الاقتضاء، بناءً على طلب اللجنة على وجه الخصوص بما يأتي:

- مراقبة وضمان التطبيق الصحيح لهذا النظام، دون الإخلال بمهام سلطات الإشراف الوطنية.
- تقديم المشورة في أي مسألة تتعلق بحماية البيانات الشخصية في الاتحاد، وكذلك في شأن تقديم أي تعديل مقترح لهذا النظام.
- تقديم المشورة للجنة فيما يتعلق بشكل وإجراءات تبادل المعلومات بين المراقبين والمجهزين والسلطات الرقابية بشأن قواعد الشركات الملزمة.
- القيام بإصدار مبادئ توجيهية وتوصيات وأفضل الممارسات بشأن إجراءات محو الوصلات أو نسخ أو تكرار البيانات الشخصية من خدمات الاتصالات المتاحة للجمهور.
- أن تقوم بدراسة، سواء بمبادرة منها، أو بناء على طلب أحد أعضائها أو بناء على طلب اللجنة، أي مسألة تغطي تطبيق هذا النظام، وإصدار مبادئ توجيهية وتوصيات من أجل التشجيع على التطبيق المتسق للنظام.
- إصدار مبادئ توجيهية وتوصيات وأفضل الممارسات، من أجل مواصلة تحديد معايير وشروط القرارات المستندة للمادة (22) فقرة (2) من النظام.

- إصدار مبادئ توجيهية وأفضل الممارسات، وذلك لتحديد خروقات البيانات الشخصية وتحديد التأخير غير المبرر. و الظروف التي يحتمل أن يؤدي فيها خرق البيانات الشخصية إلى حدوث خطر كبير على حقوق وحريات الأشخاص الطبيعيين.
- مواصلة تحديد معايير ومتطلبات نقل البيانات الشخصية استنادًا إلى قواعد الشركات الملزمة التي يلتزم بها المراقبون والقواعد المؤسسية الملزمة التي تلتزم بها المعالجات والمتطلبات الإضافية اللازمة لضمان حماية البيانات الشخصية لأصحاب البيانات. ولوضع إجراءات مشتركة للإبلاغ عن الأشخاص الطبيعيين المتهمين بانتهاك النظام.
- التشجيع على وضع مدونات لقواعد السلوك وإنشاء آليات لإصدار شهادات حماية البيانات وأختام وعلامات حماية للبيانات وفقا للمادة (45) السابقة الذكر.
- القيام باعتماد هيئات لإصدار الشهادات، والاحتفاظ بسجل دوري للهيئات المعتمدة ولأجهزة التحكم أو المعالجات المعتمدة المنشأة في بلدان ثالثة.
- تحديد المتطلبات اللازمة، من أجل اعتماد هيئات لإصدار الشهادات.
- تزويد اللجنة برأي بشأن متطلبات التصديق، و بشأن الأيقونات المشار إليها في المادة (12) فقرة (7) من النظام، حيث نصت على تقديم المعلومات التي يتعين تقديمها إلى أصحاب البيانات عملاً بالمادتين (13) و(14) بالاقتران مع أيقونات موحدة من أجل إعطاء نظرة عامة ذات مغزى عن المعالجة المقصودة بطريقة سهلة الرؤية ومفهومة ومقروءة بوضوح. وحيثما تعرض الرموز إلكترونياً يجب أن تكون قابلة للقراءة آلياً. وأيضاً تزويدها بالرأي من أجل تقييم مدى كفاية مستوى الحماية في بلد ثالث أو منظمة دولية أخرى، بما في ذلك تقييم ما إذا كان بلد ثالث أو إقليم أو قطاع محدد أو أكثر داخل هذا البلد الثالث، أو منظمة دولية لم تعد تضمن مستوى مناسباً من الحماية. وتحقيقاً لهذه الغاية يجب على اللجنة تزويد المجلس بجميع الوثائق اللازمة، بما في ذلك المراسلات مع حكومة البلد الثالث، فيما يتعلق بذلك البلد الثالث أو الإقليم أو مع منظمة أخرى.
- إصدار آراء بشأن مشاريع مقررات السلطات الإشرافية عملاً بآلية الاتساق التي أشرنا إليها مسبقاً في المادة (64) من النظام، بشأن المسائل المقدمة، وإصدار قرارات ملزمة.
- تعزيز التعاون والتبادل الفعال والمتعدد الأطراف للمعلومات وأفضل الممارسات بين السلطات الإشرافية.
- تعزيز برامج التدريب المشتركة وتسهيل تبادل الموظفين بين السلطات الإشرافية والسلطات الإشرافية في البلدان الثالثة أو مع المنظمات الدولية، عند الاقتضاء.

- تعزيز تبادل المعارف والوثائق المتعلقة بتشريعات وممارسات حماية البيانات مع السلطات الإشرافية لحماية البيانات في جميع أنحاء العالم.
- إصدار آراء بشأن مدونات السلوك الموضوعة على مستوى الاتحاد.
- الاحتفاظ بسجل إلكتروني متاح للجمهور بالقرارات التي تتخذها السلطات الإشرافية والمحاكم بشأن القضايا التي يتم التعامل معها في آلية الاتساق.
- عندما تقوم اللجنة بطلب مشورة من المجلس يجب مراعاة الحد الزمني، ومدى أهمية المسألة.
- يحول المجلس آراءه ومبادئه التوجيهية وتوصياته وأفضل الممارسات إلى اللجنة وإلى لجنة القانون العام لحماية البيانات ويجعلها عامة.

كما يتشاور المجلس عند الاقتضاء، مع الأطراف المهمة ويمنحهم الفرصة للتعليق خلال فترة معقولة، ويقوم المجلس بإتاحة نتائج التشاور للجمهور²³³.

ثالثاً: تعيين الرئيس التنفيذي ومهامه

وبموجب القانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018، نصت المادة (43) منه على كيفية تعيين الرئيس التنفيذي وأجره وكذلك حالة خلو المنصب، حيث يكون للهيئة الوطنية أن تقوم بتعيين رئيس تنفيذي لها، وذلك بموجب مرسوم لمدة ثلاث سنوات، ويتم ذلك عن طريق ترشيح مجلس الإدارة له ولا يجوز أن تتم إعادة تعيينه أكثر من مرتين متتاليتين. كما أن مجلس الإدارة هو من يحدد الأجر الذي يستحق الرئيس التنفيذي الحصول عليه، ويتضمن ذلك العلاوات والمزايا الأخرى. وأما في حالة خلو منصب الرئيس التنفيذي لأي سبب، فيعين محله بذات الطريقة التي عين بها شخص آخر، حيث يجوز لمجلس الإدارة أن يصدر قراراً بتعيين نائب للرئيس التنفيذي يحل محله في حال غيابه أو قيام مانع لديه أو خلو منصبه، ويباشر نائب الرئيس التنفيذي المهام الموكلة إليه من قبل مجلس الإدارة أو الرئيس التنفيذي، ويُنشر قرار التعيين في الجريدة الرسمية.

²³³ Art. 70 GDPR Tasks of the Board

"1-The Board shall ensure the consistent application of this Regulation. 2To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular: monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities."

أما بالنسبة لتعيين الرئيس في النظام الأوروبي العام لحماية البيانات الشخصية، فيتم عن طريق انتخاب المجلس رئيساً ونائبين له من بين أعضائه بأغلبية بسيطة، وتكون مدة ولاية الرئيس ونوابه خمس سنوات قابلة للتجديد مرة واحدة²³⁴.

بالإضافة إلى ذلك منح قانون حماية البيانات الشخصية البحريني والنظام الأوروبي العام عدة مهام للرئيس، فنصت المادة (44) من قانون حماية البيانات الشخصية البحريني على المهام والصلاحيات التي يقوم بها الرئيس التنفيذي، فيكون الرئيس التنفيذي ممثلاً عن الهيئة أمام مجلس القضاء وفي علاقتها مع الغير، ويكون مسؤولاً أمام مجلس الإدارة عن سير أعمال الهيئة فنيا وإداريا ومالياً، وله أن يمارس جميع صلاحيات الهيئة ماعدا الصلاحيات التي تكون لمجلس الإدارة، وله أن يتولى بوجه خاص ما يأتي:

- إدارة الهيئة وتصريف شؤونها، والإشراف على موظفيها وتسيير العمل فيها.
 - ينفذ القرارات الصادرة عن مجلس الإدارة.
 - يجب أن يقوم بإعداد ميزانية الهيئة وعمل تقرير بشأنها، وعرضهما على مجلس الإدارة قبل انتهاء السنة المالية خلال فترة لا تتجاوز الشهرين.
 - إعداد الحساب الختامي للهيئة وعمل تقرير بشأنه، وعرضهما على مجلس الإدارة خلال شهرين بعد انتهاء السنة المالية للهيئة لإقرارهما.
 - أن يقوم بإعداد تقرير سنوي عن نشاط الهيئة، خلال السنة المالية السابقة وعرضه من أجل أن يتم إقراره على مجلس الإدارة خلال ثلاثة أشهر على الأكثر من تاريخ انتهاء السنة المالية، وإرفاق نسخة مدققة من الحسابات للهيئة عن ذات السنة المالية.
 - أن يقوم بإعداد مشروع الهيكل التنظيمي للهيئة، ويعرضه على مجلس الإدارة لاعتماده.
 - إعداد تقارير دورية وعرضها كل ثلاثة أشهر على مجلس الإدارة عن نشاط الهيئة وسير العمل بها، تتضمن بوجه خاص ما تم إنجازه وفقاً للخطط والبرامج الموضوعة. وتحدد معوقات الأداء -إن وجدت- والحلول المقترحة لتفاديها، وذلك ما لم يقرر مجلس الإدارة مدة أقل لتقديم هذه التقارير.
 - القيام بالمهام والصلاحيات الأخرى التي يختص بها وفقاً لأحكام هذا القانون.
- يجوز للرئيس التنفيذي أن يفوض كتابة من يراه من موظفي الهيئة في مباشرة بعض مهامه.

²³⁴ Art. 73 GDPR Chair

“1- The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.
2-The term of office of the Chair and of the deputy chairs shall be five years and be renewable once...”

ونلاحظ مما سبق إن المشرع البحريني قد وسع من صلاحيات الرئيس التنفيذي، وهذا على عكس المشرع الأوروبي، الذي حدد صلاحياته بثلاث مهام، وهي²³⁵:

- يعقد اجتماعات المجلس، ويعد جدول أعماله.
 - إخطار السلطة الإشرافية الرئيسية والسلطات الرقابية المعنية بالقرارات التي يعتمدها المجلس.
 - أداء مهام المجلس في الوقت المناسب، وخاصة فيما يتعلق بآلية الاتساق.
- ويقوم المجلس بتوزيع المهام بين الرئيس ونوابه في نظامه الداخلي

وترى الباحثة إن المشرع البحريني قد وُفق في تبنيه مسلك توسعة نطاق المهام الممنوحة للرئيس التنفيذي، وذلك بغية منح الهيئة الوطنية آلية أكثر فاعلية لحماية البيانات الشخصية، ويتطلب ذلك تضافر الجهود من جميع الجهات، الأمر الذي جعل المشرع البحريني على عكس المشرع الأوروبي يوسع من صلاحيات الرئيس التنفيذي ليتمكن بدوره من تمثيل الهيئة بأفضل صورة والقيام بأكثر من مهمة، وذلك نظراً إلى المستجدات الحالية وظهور التكنولوجيا الحالية ومواجهة خطر الاعتداء على خصوصية البيانات الشخصية بتوفير الحماية القانونية اللازمة لها.

رابعاً: أمانة المجلس

بموجب المادة (75) من النظام الأوروبي العام لحماية البيانات الشخصية ، أوجب المشرع على المشرف الأوروبي حماية البيانات الشخصية وتوفير مجلس أمانة ليؤدي هذا المجلس مهامه بتعليمات من رئيس المجلس، كما يساهم المشرف الأوروبي في تقديم الدعم التحليلي واللوجستي والإداري إلى المجلس، بالإضافة إلى مسؤولية مجلس الأمانة بوجه خاص عن عدة أمور، منها:

- الأعمال اليومية للمجلس.
- الاتصال بين أعضاء المجلس ورئيسه واللجنة.
- التواصل مع المؤسسات الأخرى والجمهور.
- استخدام الوسائل الإلكترونية للاتصالات الداخلية والخارجية.
- ترجمة المعلومات ذات الصلة.

²³⁵ Art. 74 GDPR Tasks of the Chair

1-"The Chair shall have the following tasks:

to convene the meetings of the Board and prepare its agenda.

to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned...."

- إعداد اجتماعات المجلس وتتابعها.
- إعداد وصياغة الآراء والقرارات المتعلقة بتسوية المنازعات بين السلطات الإشرافية والنصوص الأخرى التي يعتمدها المجلس²³⁶.

الفرع الثاني : جزاءات انتهاك خصوصية البيانات

تشكل الأطر القانونية والتنظيمية جزءاً أساسياً من منظومة حماية البيانات الشخصية، لا يمكن الاستغناء عنه، ومن هذا المنطلق قام كل من المشرع البحريني في قانون حماية البيانات الشخصية، والمشرع الأوروبي في النظام الأوروبي العام، بمنح الهيئة الوطنية صلاحية اتخاذ الإجراءات الإدارية والجزائية في حق المسؤول عن المعالجة في حالة انتهاكه أحكام القانون.

أولاً: الإجراءات والعقوبات الإدارية

لقد أنشأ المشرع البحريني والنظام الأوروبي -كما ذكرنا- سلطة إدارية مستقلة تتمتع بالشخصية الاعتبارية والاستقلال المالي والإداري، توكل إليها مهمة حماية البيانات الشخصية، ولها في سبيل ذلك الاستعانة بضباط وأعوان الشرطة القضائية، وكذلك بعض أعوان الرقابة في حالة البحث ومعاينة الأفعال.

1- العقوبة الإدارية

لقد منح المشرع البحريني طبقاً للقرار رقم (49) لسنة 2022 بشأت الإجراءات والقواعد الخاصة بتقديم الشكاوى مخالفة أحكام قانون حماية البيانات الشخصية الصادر بالقانون رقم 30 لسنة 2018 والبت فيها في المادة (2) منه الحق لكل صاحب صفة أو مصلحة أن يقوم بتقديم شكوى للهيئة في حال حمله الاعتقاد في وقوع مخالفة لأحكام قانون البيانات الشخصية أو كان يعتقد بأن شخصاً ما يقوم بمعالجة البيانات خلافاً لأحكام القانون. وإما بالنسبة لإجراءات تقديم الشكاوى فنص القرار في المادة (3) منه على "أنه الشكاوى يجب أن تقدم على الانموذج المعد لذلك من خلال الموقع الإلكتروني للهيئة حيث يجب أن يتضمن عدة أمور أسم مقدم الشكاوى وصفته وعنوانه ومعلومات للتواصل معه وكذلك اسم المشكو في حقه وعنوانه والمعلومات اللازمة للتواصل معه. وكذلك الوقائع المتصلة بالمخالفة وأية مستندات تؤيد الشكاوى. وبعد تقديم الشكاوى يتم فحصها ورافق

²³⁶ Art. 75 GDPR Secretariat

"1-The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2-The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board..."

المستندات المتعلقة بها للتأكد من جدية هذه الشكاوى ، ويمكن للهيئة أن تطلب تزويدها بأي بيانات ضرورية وفي حال كانت الأدلة غير كافية للتحقيق الشكوى كما للهيئة الحق في حفظها". إما فيما يتعلق بمباشرة التحقيق حيث منح المشرع البحريني في المادة (47) الحق للهيئة في أن تقوم بمباشرة إجراء التحقيق ، ويمكن أن تجري الهيئة هذا التحقيق من تلقاء نفسها أو بطلب من الوزير أو بناء على الشكاوى والبلاغات المتلقاة. كما ويجب على الهيئة قبل البدء في إجراءات التحقيق أن تخطر مدير البيانات أو مراقب حماية البيانات المعني. بحسب الأحوال، بالأسباب التي دفعتها إلى الاعتقاد بوقوع المخالفة أو أنها على وشك الوقوع، ويجب أن يتضمن الإخطار الأدلة والقرائن التي تدل على وجود المخالفة. ومع ذلك، في المادة (48) من القانون والمادة (5) من القرار الوزاري رقم (49) قيجوز وطبقاً يُصدره رئيس المجلس إجراء المراحل الأولية من التحقيق التي يحددها القرار دون توجيه الإخطار إذا قامت دلائل جدية يُخشى بسببها عدم التوصل للحقيقة أو تعثر التحقيق، وعلى الهيئة توجيه الإخطار عند زوال الأسباب المشار إليها. و لمدير البيانات أو مراقب حماية البيانات المعني حق الرد على الإخطار خلال سبعة أيام عمل من تاريخ وصوله إليه، ويجب أن يشمل الرد على دفاعه وملاحظاته وأن يكون مشفوعاً بما لديه من المستندات والأوراق وأية أدلة أو قرائن تؤيد وجهة نظره. وللهيئة، بعد دراسة الرد على الإخطار، أن تأمر بحفظ الموضوع أو بالبدء في إجراءات التحقيق، وعليها إخطار الأطراف المعنية بالأمر الصادر منها في أيٍّ من الحالتين. كما لها أن تباشر التحقيق بنفسها أو تشكل لذلك لجنة ثلاثية من ذوي الاختصاص من داخل الهيئة أو خارجها، أو تكلف أي شخص مؤهل للقيام بذلك ". وعند مباشرة التحقيق من قبل اللجنة من حقها أن تطلب البيانات والمعلومات والإبضاحات اللازمة والضرورية وكذلك ارفاق المستندات المناسبة خلال مدة تعين لذلك . ووفقا لقرار (49) من المادة 6 تتولى الهيئة البت في الشكوى ويجب على الهيئة أن تمسك سجلا بموجب المادة (7) منه وتسجل فيه معلومات تقديم الشكوى التاريخ وأسم المشكو في حقه وموضوع الشكوى.

ومن ناحية أخرى يحق للجنة التحقيق أن تتدب أيا من مأموري الضبط القضائي ، وذلك في سبيل إنجاز عملها وهم بموجب المادة (36) من القانون "المفتشين الذين يندبهم الرئيس التنفيذي من بين موظفي الهيئة أو من غيرهم للقيام بأعمال التفتيش للتحقق من تنفيذ أحكام القانون وكذلك المفتشين الذين يصدر قراراً بتحديدهم من الوزير المختص بشؤون العدل بالاتفاق مع الوزير ، صفة مأموري الضبط القضائي بالنسبة للجرائم المنصوص عليها في هذا القانون والتي تقع في دائرة اختصاصهم وتكون متعلقة بأعمال وظائفهم ، منحهم القانون سلطة القيام بالتحريات اللازمة ومعاينة الأماكن التي لها صلة باختصاص الهيئة والأطلاع على الملفات والسجلات والدفاتر والمستندات والبيانات الموجودة بها. كما يحق لهم سماع أقوال كل من يشتبه له صلة في الموضوع".

عند إنهاء إجراءات التحقيق يجب على لجنة التحقيق أن تصدر تقرير مسبب بالنتائج التي توصلت لها ، ويجب أن ترفق معه ملف التحقيق كاملاً وتسلمه للرئيس التنفيذي خلال فترة لا تتجاوز 6 أشهر من تاريخ بدء إجراءات التحقيق، ويمكن للجنة التحقيق أن تطلب من الرئيس التنفيذي تمديد الفترة قبل أنتهاؤها لمدة أو لمدة إضافية ولكن يجب أن لا تتجاوز في مجموعها الستة أشهر وذلك في الحالات التي يكون التأخير فيها لأسباب خارج عن إرادة اللجنة.

كما أعطى المشرع البحريني هيئة حماية البيانات الشخصية صلاحية اتخاذ الإجراءات الإدارية في حق المسؤول عن المعالجة في حال خرقه أحكام القانون طبقاً للمادة (55)، في شكل قرارات قابلة للطعن أمام مجلس الدولة المتمثل بالمجلس الأعلى للقضاء، وتتمثل هذه الإجراءات بالآتي:

- القيام بسحب التصريح في حال وقعت مخالفة تتعلق بالتصريح المسبق الصادر عن الهيئة.
- يتم إيقاع غرامة تهيديّة تحتسب على أساس يومي لكي يتوقف المخالف عن المخالفة ويزيل سببها وآثارها، وذلك بما لا يجاوز 1000 دينار يومياً عند ارتكابه المخالفة أول مرة، و 2000 دينار يومياً في حال ارتكابه مخالفة أخرى خلال ثلاث سنوات من تاريخ إصدار قرار في حقه عن المخالفة السابقة.
- توقيع غرامة إدارية بما لا يجاوز 20000 دينار، ويجب عند تقدير الغرامة مراعاة جسامته المخالفة، والعنت الذي بدا من المخالف والمنافع التي جناها صاحب البيانات والأضرار التي أصابته نتيجة لذلك.
- للهيئة، بناءً على قرار مجلس الإدارة، أن تنشر بياناً بالمخالفة التي ثبت وقوعها من قبل مدير البيانات أو مراقب حماية البيانات، وذلك بالوسيلة والكيفية اللتين يحددهما القرار بما يتناسب مع جسامته المخالفة. على أنه يجب ألا يتم النشر إلا بعد فوات ميعاد الطعن في قرار الهيئة بثبوت المخالفة أو صدور حكم باتّ بثبوت المخالفة، وذلك بحسب الأحوال 237. بالإضافة إلى ذلك منح المشرع البحريني الرئيس التنفيذي في الحالات المستعجلة، بناءً على طلب صاحب الشأن، إذا قامت لديه أدلة قوية تجعله يظن أن الاستمرار في معالجة البيانات على نحو معين قد يؤدي إلى تعدي على حقوق وحريات مقدّم الطلب المقررة قانوناً ما يتعدّر تداركه فيما بعد، أن يقوم بإصدار قرار مسبب بالوقف المؤقت عن معالجة البيانات كلياً أو جزئياً وبالحجب المؤقت للبيانات كلياً أو جزئياً.

ويصدر الرئيس التنفيذي القرار بعد أن يطلع على الأوراق ويسمع أقوال كل من صاحب الشأن ومدير البيانات المعني، ويقوم بإتاحة الفرصة لهما لمناقشة آرائهما وتقديم ما يؤيد وجهة نظرها مثل مستندات أو أوراق أو أدلة أو قرائن، وذلك كله في المواعيد ووفقاً للإجراءات التي يصدر بتحديدھا قرار من مجلس الإدارة. كما يحق للهيئة أو لصاحب الشأن أن يستصدر أمراً على عريضة 238 من المحكمة الكبرى المدنية بتنفيذ أي قرار يصدر وفقاً مؤقتاً لحكم الوقف الكلي أو الجزئي. ويجوز للمحكمة أن تُصدر الأمر على وجه الاستعجال دون استدعاء مدير البيانات، ولمدير البيانات أن يعترض على الأمر إلى المحكمة التي أصدرته خلال ثمانية أيام من صدوره، وللمحكمة أن تؤيد الأمر أو تعدّله أو تلغيه. وفي حال صدور قرار بشأن الوقف المؤقت، يلتزم الرئيس التنفيذي في هذه الحالة خلال سبعة أيام عمل من تاريخ صدور القرار بأن يحيل أية مخالفة تكشف له إلى التحقيق 239.

ثانياً: الجزاء المدني

تقوم المسؤولية المدنية على قاعدة كل خطأ سبب ضرراً للغير يُلزم محدثه بالتعويض²⁴⁰. وبناء على ذلك، فإن أركان المسؤولية المدنية هي الخطأ والضرر وعلاقة السببية، وأيضاً نجد أن المشرع البحريني نص في المادة (57) من قانون حماية البيانات الشخصية على أنه "مع عدم الإخلال بأحكام القانون المدني، يجوز لمن لحقه ضرر نشأ عن معالجة بياناته الشخصية من قبل مدير البيانات، أو عن إخلال مراقب حماية البيانات بأحكام هذا القانون، الحق في مطالبة مدير البيانات أو مراقب حماية البيانات، بحسب الأحوال، بالتعويض الجابر للضرر". والغاية من ذلك هو ضمان الضرر الذي تسبب فيه مرتكب فعل الإضرار وحصول المضرور على التعويض الجابر للضرر.

وعليه، نتناول فيما يلي أركان المسؤولية المدنية في إطار الاعتداء على البيانات الشخصية دون البحث في النظريات العامة والمبادئ القانونية المستقرة المرتبطة بهذه الأركان والتي لا يسعنا المقام هنا لتناولها:

1- الخطأ

²³⁸ تجدر الإشارة هنا إلى صدور قانون جديد للتنفيذ في مملكة البحرين وهو المرسوم بقانون رقم (22) لسنة 2021 بإصدار قانون التنفيذ في المواد المدنية والتجارية.

²³⁹ المادة 65 من قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018.

²⁴⁰ المادة 158 من القانون المدني البحريني، المرسوم بقانون رقم (19) لسنة 2001.

يعرف الخطأ بأنه عمل غير قانوني يتم استخدام الحاسب الآلي فيه كأداة أو كموضوع للاعتداء على البيانات الشخصية للمستخدمين²⁴¹. أي ينصب الخطأ هنا على كل فعل غير مشروع يمثل اعتداءً على البيانات في انسيابها وتدفقها، ولا شك حتى يتحقق الخطأ كشرط أولي لتحقيق المسؤولية المدنية فإن ذلك يتم عن طريق استخدام حاسب آلي متصل بشبكة الإنترنت، ثم يقوم المعتدي بتحميل الجهاز ببرامج فيروسات من أجل أن يقوم ببثها، حتى تمكنه من الاعتداء على خصوصية المستخدم، فيقوم من خلال ذلك بخداعه بالدخول إليها ومن ثم يقوم المعتدي بسرقة البيانات الخاصة بالمستخدم. وأيضاً قد يحدث أن يتم التنصت على المحادثات عن طريق مواقع التواصل الاجتماعي، فيقوم المعتدي باستخدام برنامج معين لهذا يفتح على جهاز المضرور، فيتمكن بالتالي من الاستماع لجميع المحادثات، والاطلاع أيضاً على كافة المراسلات الصادرة والواردة إلى حساب المضرور، كما يتمكن من قراءة بياناته الشخصية. لذلك لا بد من أن تتوفر التقنية العالية لدى القائمين على عمليات تجميع البيانات، والقيام بتوعيتهم بالمسؤولية الملقة على عاتقهم، من أجل الحفاظ على كافة البيانات والمعلومات المتعلقة بالمستخدمين، ومن أجل منع المتطفلين من الوصول إليها، وكذلك عدم وضعها في التداول بدون إذن من صاحب البيانات²⁴².

كما يجب أن يكون هناك معيار لمعرفة مدى تحقق الخطأ في انتهاك البيانات، فيتم النظر في هذه الحالة إلى التقني على أنه متميز. وبالتالي العناية التي يجب أن يبذلها التقني في هذا المجال هي عناية من نوع خاص، فيجب أن يبذل ما في وسعه من أجل أن يحافظ على سرية البيانات الشخصية، على اعتبار أنه متخصص ومتمكن من تقنيات الحماية التي تحول دون تعدي الغير على البيانات الشخصية. كما أن المعيار الذي يطالب به التقني هو معيار المهني البقظ، في حال حدث أي خطأ في إيراد أي معلومة، وإن كانت بسيطة أو قدم بيانات دون أن يلتزم بالسرية، فيعد هذا خطأ يوجب المسؤولية. كما نجد أن الخطأ في مجال البيانات الشخصية وارد حدوثه عند تجميع أو تخزين معلومات دون إخطار صاحبها، وفي ظل عدم وجود الاحترام الكافي لسرية البيانات، فإن تداول البيانات ونشرها على الإنترنت، وسهولة الحصول عليها بطريقة غير مشروعة، يعد من صور الخطأ الأكثر شيوعاً. ومن ناحية أخرى فإن الخطأ يجب إثباته من قبل المضرور في المجال التقني، إلا أن هناك عدة صعوبات ناتجة عن خصوصية الخطأ، وهي تعود إلى عدة أسباب:

1- سرعة ارتكاب الخطأ واختفائه وهذا معناه إن الاعتداء على الخصوصية أو نشر البيانات يتم خلال ثوانٍ معدودة بمجرد ضغط زر، والخطأ بالنظر إلى خصوصية

²⁴¹ ذياب موسى البداينة، جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، جامعة

نايف للعلوم الأمنية، الرياض، 1420هـ، ص102.

²⁴² = محمد محمد القطب، المرجع السابق، ص895.

محل الاعتداء قد لا يتطلب وجود المعتدي مادياً، بل يقوم بضبط بعض البرامج التي تساهم وتساعد في حصول الاعتداء وتقوم بنشر البيانات من تلقاء نفسها²⁴³.

2- خصوصية محل ارتكاب الخطأ، ويتم عادة الاعتداء على البيانات الشخصية وانتهاك خصوصية المضرور عبر الإنترنت، وهو يعتبر عالمًا افتراضياً، بالتالي من الصعب التعامل معه، حيث يستلزم هذا توافر معرفة تقنية وفنية لاكتشاف الاعتداء وتحديد، وهذا الأمر لا يتوافر عند جميع المستخدمين لمواقع التواصل الاجتماعي أو التطبيقات التكنولوجية المختلفة.

3- تعدد مرتكبي الخطأ: قد يتم في هذه الحالة الاعتداء من قبل شخص قام بالعمل الفني وآخر ساهم في استخدام البيانات بطريقة غير مشروعة وآخر تلاعب بها، ومع هذا التعدد يصبح من الصعب تحديد شخصية مرتكب الخطأ.

4- تنفيذ الخطأ عن بعد، وذلك من خلال استعمال التكنولوجيا عن بعد، فيكون المعتدي على خصوصية البيانات مقيماً في دولة أخرى.

5- عدم وضوح الاعتداء وصعوبة إثباته: قد يحدث أن يتم الاعتداء على المضرور كأن يقوم بسرقة مبلغ من الحساب البنكي ويحصل على أمواله، فيستطيع المعتدي حينها محو أدلة الاعتداء وتدميرها، الأمر الذي سيؤدي إلى صعوبة إثبات خطأ المعتدي بعد أن قام بإزالة آثاره. وفي ظل هذه الصعوبة التي تحيط بمسألة إثبات الخطأ في هذا المجال التقني المعقد وتعذر تحديد شخصية المعتدي المنتهك لخصوصية البيانات، قد يُحرم المضرور من الحصول على التعويض، فهنا يمكن أن تقام المسؤولية المدنية عن أضرار مواقع التواصل في حالات تعذر تحديد شخصية المعتدي الحقيقية والحصول منه على التعويض، على أساس الخطأ في الحراسة، حيث من الممكن أن تحدد أماناً الشخص المسؤول عن التعويض تلك الأضرار في حال قصر في واجب الرقابة والحراسة، وهذا الواجب يلقي على عاتق مدير مواقع التواصل الاجتماعي أو مالكه، وعلى عاتق وسطاء الإنترنت ومصممي تقنيات الاتصال²⁴⁴.

-2

-3

²⁴³ علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، مطابع جاد للأوفست، الرياض، 1436 هـ، ص 63.

²⁴⁴ محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003، ص 363.

4- الضرر

تتحقق المسؤولية المدنية عن الأضرار التي تلحق بالبيانات الشخصية عندما يتم استخدام مواقع التواصل الاجتماعي أو تطبيقات إنترنت الأشياء أو التطبيقات التكنولوجية المختلفة، بطريقة تسبب الضرر لبعض المستخدمين لها. وهذا عن طريق انتهاك خصوصية بياناتهم الشخصية.

ويعرف الضرر بأنه "الإخلال بحق أو مصلحة ذات قيمة مالية للمضرور"²⁴⁵ ويعرف أيضا "ما يصيب الشخص في حق من حقوقه أو بمصلحة مشروعة له"²⁴⁶.

وينقسم الضرر إلى نوعين: ضرراً مادياً يصيب الذمة المالية للمضرور، وضرراً معنوياً يتمثل في المعاناة التي تصيب عاطفة المضرور، وفي الحالتين لا يوجد خلاف في الفقه على شمول التعويض لكلا النوعين من الضرر. ولقد أكد المشرع البحريني في القانون المدني على ذلك في المادة (158) منه حين نص على إن "كل خطأ سبب ضرراً للغير يلزم من أحدثه بتعويضه"، كما أقرت المادة (162) حق المضرور في التعويض عن الضرر المادي والأدبي، حيث يتحقق كلا النوعين من الضرر للمعتدي عليه عادة، عن طريق التعدي على بياناته الشخصية عبر مواقع التواصل الاجتماعي أو من خلال استخدام التطبيقات التكنولوجية المختلفة، والتي يقوم المعتدي من خلالها بالكشف والاطلاع على البيانات الشخصية والأمور السرية الخاصة بصاحب الحساب أو البريد الإلكتروني، وهو ما يسبب ضرراً لصاحب البيانات، فيقوم المعتدي بنشر هذه البيانات على الشبكة، وتصبح متاحة لعدد غير محدود، ما قد يؤدي لإصابة صاحب البيانات بأضرار بالغة في سوق العمل نتيجة رفض التعامل معه، أو عدم الموافقة على طلب دخوله في مناقصة أو مسابقة بسبب ما نشر عنه من بيانات ومعلومات، وقد يكون الضرر المادي متمثلاً في خسارته لبعض أمواله نتيجة سرقة كلمات مرور سرية لحساباته البنكية وبالتالي سرقة أمواله. أما بالنسبة للضرر الأدبي فهو يحدث نتيجة انتهاك الخصوصية والاعتداء على بياناته الشخصية في انتهاك حرمة الحياة الخاصة للمستخدمين، وما يتبع ذلك من مساس بشخصيته الاجتماعية، ونشر معلوماته وأسراره الخاصة، وإهانته أو تجريحه تبعاً لذلك²⁴⁷.

وفيما يتعلق بشروط الضرر الموجب للتعويض وفقاً للقانون المدني، فيجب أن يكون الضرر محققاً، أو أن يكون قد وقع بالفعل، أو أن تكون احتمالية وقوعه في المستقبل أمراً حتمياً. وتتوافر تلك الشروط بالنسبة للضرر الناشئ عن الاعتداء على خصوصية البيانات الشخصية

²⁴⁵ عبدالرزاق السنهوري، الوسيط في المسؤولية المدنية، الجزء الأول، ف571، ص856.

²⁴⁶ سليمان مرقص، الوافي في شرح القانون المدني، الفعل الضار، الجزء الثالث، دار المنشورات الحقوقية، بيروت، 1998، ص133.

²⁴⁷ منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلومات السعودي، جامعة نايف للعلوم الأمنية، الرياض، 2010، ص103.

سواء من خلال استخدام مواقع التواصل الاجتماعي أو التطبيقات التكنولوجية المختلفة، فيكون بهذه الحالة الضرر محققاً لأن الضرر الاحتمالي غير متصور على صعيد انتهاك الخصوصية والسرية المعلوماتية، فعند الاعتداء على البيانات الشخصية والاطلاع على الأسرار الشخصية لصاحب الحساب يصبح الضرر محققاً. وحتى يكون الضرر محققاً يلزم في الضرر أن يمس بمصلحة مشروعة للمضرور، وهذا يتحقق عندما يتم التعدي على خصوصية صاحب البيانات من خلال مواقع التواصل الاجتماعي أو استخدام التطبيقات التكنولوجية المختلفة، فتعتبر خصوصيته وحرمة بياناته الشخصية والسرية والحرص على الحفاظ عليها، من أهم المصالح المشروعة لمستخدمي هذه المواقع.

كما يلزم أن يكون الضرر مباشراً، والضرر المباشر في المسؤولية المدنية وحده الذي يمكن التعويض عنه، والضرر يكون مباشراً في حال كان نتيجة طبيعية للاعتداء الحاصل على خصوصية المعتدى عليه، ولم يكن بالإمكان تفادي حدوثه بجهد معقول²⁴⁸.

5- علاقة السببية

بالإضافة إلى الخطأ والضرر يجب أن تتوافر علاقة السببية بين الخطأ الذي تمثل بالاعتداء على خصوصية البيانات الشخصية لصاحب الحساب عن طريق مواقع التواصل الاجتماعي أو عن طريق تطبيقات إنترنت الأشياء، وبين الضرر المادي أو الأدبي الذي لحقه. فلا يسأل المدعى عليه عن كل ضرر وقع، وإنما يسأل فقط عن الضرر الذي وقع نتيجة ارتكابه فعل الإضرار.

أما بالنسبة لإثبات رابطة السببية، فليس من اليسير على المضرور أن يثبت الخطأ الذي تقوم عليه المسؤولية، وهذا يعود إلى صعوبة تفسير أو تمييز الخطأ أو تحديد مصدره أو وقت حدوثه، وذلك بسبب تعدد مراحل تنفيذ الاعتداء على بياناته الشخصية²⁴⁹. وطبقاً لذلك وطبقاً لذلك أن السببية التقليدية لم تعد كافية لمعالجة مثل هذه الفرضيات لذلك أتجه القضاء المقارن إلى خلق نظريات جديدة جميعها تصب في مصلحة المضرور والتخفيف عليه لإثبات هذه السببية ومنها على سبيل المثال:

أولاً: السببية الاحتمالية وتقسم إلى :

- أ- الاحتمالية الأقرب لليقين وأخذ بها بعض القضاء الألماني .
- ب- الاحتمالية الراجحة وهو ما يميل اليه القضاء الأمريكي.
- ج- الاحتمالية الممكنة ويأخذ بها القضاء الفرنسي حيث يقوم بتفسير الشك لمصلحة المضرور .

²⁴⁸المادة (161) من القانون المدني البحريني، وكذلك: محمد محمد القطب، المرجع السابق ، ص909-910.

²⁴⁹منصور بن صالح السلمي، المرجع السابق، ص111.

ثانياً: السببية العلمية وهي تعتمد على إثبات السببية بطريقة سلبية ، بمعنى ان الضرر إن لم يكن له تفسير سوى واقعة ما فهو كافي للقول بوجود السببية .

ثالثاً: السببية المفترضة

من الآثار المترتبة على وجود العلاقة السببية في المسؤولية المدنية هو ضمان الضرر إي جبر الضرر المحقق بتعويض المضرور. والتعويض يدور وجوداً وعدمًا مع الضرر. وإن قامت المسؤولية في بعض الحالات دون اللجوء لفكرة الخطأ، إلا إنها لا تقوم إذا انعدم الضرر، وبناءً عليه يعد الضرر أساس التعويض. فلما كان الضرر ركناً من أركان المسؤولية. وينشأ الحق في المطالبة بالتعويض من الوقت الذي يصبح فيه الضرر محقق الوقوع وليس من وقت وقوعه فعلاً، ولا من وقت وقوع الخطأ. والقاعدة إن المدعي ملزم بإثبات وقوع الضرر استناداً لقاعدة البينة على من ادعى، واستثناء من ذلك، افترض القانون الخطأ في حالات محددة بموجب قرينة قانونية لصالح المضرور، كما يصح الاتفاق على مثل هذه القرينة فتكون القرينة في هذه الحالة بإرادة الطرفين. ومفاد ما تقدم، تكتمل أركان المسؤولية بوقوع الضرر، وتخلّف ركن من أركان المسؤولية يعني عدم جواز الحكم بالتعويض.

ولا شك إن التطور التكنولوجي وزيادة استخدام مواقع التواصل الاجتماعي وتطبيقات إنترنت الأشياء، جعلت فهم المستخدم العادي لفحواها أمراً معقداً، ما يجعل من الصعب التمسك بقواعد المسؤولية التقليدية التي تتطلب إثبات الخطأ. فمسألة إثبات حدوث تعدي على صاحب البيانات من خلال اختراق صفحته الإلكترونية، يحتاج إلى قدر من التخصص في مجال البرمجة والإلكترونيات، ومع هذا التعقيد التقني المصاحب لشبكة الإنترنت والتكنولوجيا، يكون من اللازم تطويع القواعد التقليدية بما يتناسب وطبيعة هذه الموضوعات، فيكون من مصلحة المستخدم العادي أن يعرض بمجرد وقوع الضرر وإن لم يكن بالإمكان إثبات الخطأ، ويمكن الرجوع في هذه الحالة إلى وسطاء الشبكة إذا ثبت ضلوعهم في الضرر الذي حدث وانتقت بشأنهم حالات الإغفاء من المسؤولية المحددة، أو الرجوع إلى مالك موقع التواصل، فيتم تحميلهم مسؤولية التعويض بمجرد أن يحدث الضرر..

وأما بالنسبة لأنواع التعويض عن الضرر فهي تختلف باختلاف نوع الضرر الذي لحق بالمضرور سواء كان مادياً أو أدبياً، ومبلغ التعويض وفقاً لنص المادة (161) من القانون المدني البحريني يجب أن يشمل ما فات المضرور من كسب، وما لحق به من خسارة. ويعتبر التعويض النقدي هو الأصل شريطة أن يكون ذلك نتيجة طبيعية للاعتداء، أما التعويض العيني فالحكم فيه جوازي للقاضي، وهو ما نوضحه على النحو الآتي:

• التعويض النقدي: يقدر القاضي هذا النوع من التعويض بمبلغ من النقود، يكفي لجبر الضرر، ويحاول القاضي من خلال هذا النوع من التعويض أن يجبر ويصلح الأذى الذي أصاب المضرور بفعل تطبيقات التكنولوجيا الحديثة، نتيجة الاعتداء على حرمة البيانات الشخصية الخاصة بالمستخدم. ولا يمثل التقدير النقدي للتعويض عن الضرر المادي الذي لحق المضرور أي صعوبات؛ لأنه يكون عادة مقدراً بقدر الضرر، ولكن الصعوبة تكمن عندما يقوم القاضي بتقدير التعويض النقدي عن الضرر الأدبي الذي لحق بالمضرور نتيجة التعدي على خصوصياته، وتكون في هذه الحالة المصلحة الأدبية غير قابلة للتقدير بثمن، لكن رغم ذلك أجمع الفقه على أهمية فرض التعويض النقدي عنها أيضاً، على اعتبار أنها على الأقل تقدم ترضية ولو بسيطة للمضرور. ورغم ذلك مازال الفقه يسعى للاجتهاد من أجل الوصول إلى تقدير التعويض بمبلغ يتوافق مع مقدار الأضرار وفقاً للظروف المناسبة²⁵⁰.

• التعويض العيني: هذا التعويض يهدف إلى إعادة الحال إلى ما كان عليه قبل التعدي، أو إزالة الأثر الضار الذي ترتب على الاعتداء، لذلك قد يرى القاضي عند وجود ضرر لحق بالمضرور أن التعويض العيني هو بمثابة ترضية مناسبة للمضرور، فيحكم به بناءً على طلب من المضرور.²⁵¹ وقد يحدث هذا عندما يكون هناك مثلاً تعدي قد وقع يتمثل في سرقة بيانات المضرور أو صور له والقيام بنشرها على مواقع غير أخلاقية، أو عن طريق نشر المعلومات بطريقة تسيء لصاحبها، يحكم القاضي عندئذ بوقف التعدي، ثم إزالة الصور والبيانات المتعلقة بالمضرور من الموقع، ونشر تصحيح واعتذار يزيل الأثر الضار الذي رتبته التعدي.

وخلاصة ما تقدم إن الضرر المباشر هو مناط التعويض، والتعويض إن كان في صورة عينية أو نقدية، مقسطاً، أو إيراداً مدى الحياة، يقدر بمقدار الضرر المباشر الذي أحدثه الخطأ أو التعدي، سواء كان الضرر مادياً أو أدبياً، وسواء كان متوقعاً أو غير متوقع، وسواء كان حالاً أو مستقبلاً.

من ناحية أخرى منح المشرع البحريني في قانون حماية البيانات الشخصية لمن لحقه ضرر نتيجة معالجة بياناته الشخصية من قبل مدير البيانات، أو بسبب إخلال مراقب حماية البيانات بأحكام هذا القانون، الحق في مطالبة مدير البيانات أو مراقب حماية البيانات، بحسب

²⁵⁰ محمد محمد القطب، المرجع السابق، ص 940.

²⁵¹ سامح عبدالواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها (دراسة في القانون الإماراتي)، مجلة البحوث القانونية والاقتصادية، المجلد 8، العدد 67، جامعة الشارقة، الإمارات، 2018، ص 659.

الأحوال، بالتعويض الجابر للضرر 252. وأعطى المشرع الأوروبي بموجب المادة (82) من النظام الحق لكل من يعاني من ضرر مادي أو غير مادي بسبب انتهاك النظام، بأن يحصل على تعويض من المراقب والمعالج عن الأضرار التي لحقت به. وتتحمل أيضا أي وحدة تحكم تشارك في المعالجة المسؤولية عن الأضرار الناجمة عن المعالجة التي تنتهك هذا النظام، ويكون المعالج مسؤولاً عن الضرر الناجم فقط في الحالات التي لا يمثل فيها لالتزامات هذا النظام، أو يكون قد تصرف خارج نطاق التعليمات القانونية لجهاز التحكم أو مخالفاً لها، وقد يعفى المتحكم أو المعالج من المسؤولية إذا ثبت أنه ليس مسؤولاً بأي شكل من الأشكال عن الحدث الذي أدى إلى حدوث الضرر. أما في حال وجود أكثر من وحدة تحكم أو معالج يشاركون في المعالجة نفسها، فتكون كل وحدة تحكم أو معالج مسؤولة عن الضرر بأكمله من أجل ضمان تعويض فعال لصاحب البيانات. كما يحق لكل وحدة تحكم أو معالج وقعت عليها المسؤولية بالتعويض عن الضرر بأكمله نتيجة مشاركتها في عملية معالجة نتج عنها الضرر لصاحبها أن تطالب مرة أخرى من وحدات التحكم أو المعالجات الأخرى المشاركة في المعالجة نفسها بذلك الجزء من التعويض المقابل للجزء الخاص بهم من المسؤولية عن الضرر 253.

وبموجب المادة (79) من النظام ترفع دعاوى المحكمة لممارسة الحق في الحصول على تعويض أمام المحاكم المختصة بموجب قانون الدولة العضو التي يوجد بها جهاز تحكم أو معالج، وبدلاً من ذلك يمكن عرض هذه الإجراءات على محاكم الدولة العضو التي يكون فيها الشخص المعني بالبيانات محل إقامته المعتاد، ما لم يكن المتحكم أو المعالج سلطة عامة لدولة عضو تعمل في ممارسة سلطاتها العامة.

ثالثاً: الجزء الجنائي

اتجه المشرع البحريني في قانون حماية البيانات الشخصية إلى تنويع أدواته العقابية، ليشمل لنفسه المرونة في مواجهة الاعتداءات المختلفة على البيانات الشخصية. لهذا تضمن القانون نوعين من العقوبات على اختلاف الجرائم، وهي عقوبات مالية تتمثل في الغرامة مختلفة المقدار، والعقوبة السالبة للحرية وهي الحبس.

²⁵² المادة (57) من قانون حماية البيانات الشخصية البحريني لسنة 2018.

²⁵³ Art. 82 GDPR Right to compensation and liability

“1- Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered....”.

وأخذ المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية بالغرامة الإدارية، واشترط لإيقاعها ما يلي²⁵⁴:

- يجب مراعاة طبيعة الانتهاك وخطورته ومدته مع الأخذ بعين الاعتبار نطاق أو غرض المعالجة المعنية، وكذلك عدد الأشخاص المعنيين بالبيانات ومستوى الضرر الذي لحق بهم. والطابع المتعمد أو الإهمال للانتهاك و يمكن من خلال ذلك تقييم مدى تصرف وحدة التحكم أو المعالج بمسؤولية بعد حدوث الانتهاك. والإجراءات التي تتخذها وحدة التحكم أو المعالج، للتخفيف من الأضرار التي يتعرض لها أفراد البيانات. ومراعاة درجة مسؤولية وحدة التحكم أو المعالج، إضافة للتدابير الفنية والتنظيمية التي تنفذها. ومراعاة أي انتهاكات سابقة ذات صلة بوحدة التحكم أو المعالج. كذلك يجب معرفة درجة التعاون مع السلطة الإشرافية، وهذا من أجل معالجة الانتهاك والتخفيف من الآثار الضارة المحتملة للانتهاك. ومعرفة فئات البيانات الشخصية المتأثرة بالانتهاك. وكذلك معرفة الطريقة التي أصبح فيها الانتهاك معروفاً للسلطة الإشرافية.
- الالتزام بمدونة السلوك المعتمدة أو آليات التصديق المعتمدة.
- مراعاة أي عامل مشدد أو مخفف آخر ينطبق على ظروف الحالة، مثل المنافع المالية المكتسبة أو الخسائر التي يتم تجنبها، بشكل مباشر أو غير مباشر من الانتهاك. وفي حال انتهاك المعالج أو المتحكم عن قصد أو إهمال النظام العام، فإن المبلغ الإجمالي للغرامة الإدارية يصل إلى عشرة ملايين يورو، أو في حالة التعهد بما يصل إلى 2 بالمئة من إجمالي قيمة التداول السنوية في السنة المالية السابقة أيهما أعلى. وكذلك في حال تم خرق التزامات وحدة التحكم والمعالج، والتزامات هيئة إصدار الشهادات، والتزامات هيئة المتابعة كلها يخضع خرقها لغرامات إدارية تصل إلى عشرين مليون يورو، أو في حالة التعهد بما يصل إلى 4 بالمئة من إجمالي قيمة التداول السنوية في السنة المالية السابقة أيهما أعلى. كما تفرض نفس الغرامة في حال عدم الامتثال لأمر أو قيد مؤقت أو نهائي على معالجة أو تعليق تدفقات البيانات من جانب السلطة الإشرافية.
- معرفة المبادئ الأساسية للمعالجة بما في ذلك شروط الموافقة وبيان حقوق أصحاب البيانات، وخاصة عند نقل البيانات الشخصية إلى متسلم في بلد ثالث أو منظمة دولية.

²⁵⁴ Art. 83 GDPR General conditions for imposing administrative fines" 1- Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive..”.

- دون الإخلال بالسلطات التصحيحية الإشرافية، يجوز لكل دولة عضو أن تضع القواعد بشأن ما إذا كان يجوز فرض غرامات إدارية على السلطات العامة والهيئات المنشأة في تلك الدولة. كما أنه في الحالات التي لا ينص فيها النظام القانوني للدولة العضو على الغرامات الإدارية، من الممكن تطبيق هذه المادة على نحو تقوم فيه السلطة الإشرافية المختصة بتقديم الغرامة المالية وتفرضها المحاكم الوطنية المختصة. مع ضمان أن تكون تلك السبل القانونية فعالة ولها تأثير يماثل الغرامات الإدارية التي تفرضها السلطات الإشرافية، وفي جميع الأحوال تكون الغرامات المفروضة فعالة ومتناسبة وراعية. وتخطر تلك الدول الأعضاء اللجنة بأحكام قوانينها التي تعتمد عليها دون تأخير.
- تخضع ممارسة السلطة الإشرافية لضمانات إجرائية مناسبة وفقاً لقانون الاتحاد وقانون دول الأعضاء، بما في ذلك سبل الانتصاف القضائية الفعالة ومراعاة الأصول القانونية.

وعلى غرار ذلك حددت المادة (58) من قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018 مجموعة من الأفعال التي تشكل اعتداء على البيانات الشخصية أثناء معالجتها وخصها بعقوبات محددة:

- 1- الحبس مدة لا تزيد على سنة وبالغرامة التي لا تقل عن ألف دينار ولا تتجاوز عشرين ألف دينار، أو بإحدى هاتين العقوبتين لمن قام بالأفعال التالية :
- في حال تم معالجة بيانات شخصية حساسة، بالمخالفة للشروط المتطلبة لمعالجتها.
 - كل من قام بنقل بيانات شخصية خارج المملكة إلى بلد أو إقليم خلافاً لحكم أيٍّ من المادتين (12) و(13) من هذا القانون²⁵⁵.

²⁵⁵ المادة (12) نقل البيانات الشخصية إلى بلدان وأقاليم توفّر مستوى كافياً من الحماية حيث يُحظر على مدير البيانات نقل البيانات الشخصية إلى خارج المملكة في غير الحالات الآتية:

"أن يكون النقل إلى بلد أو إقليم مدرج في كشف تتولى الهيئة إعداده وتحديثه يتضمن أسماء البلدان والأقاليم التي تقرّر الهيئة أنّ لديها تشريعات أو أنظمة معمولاً بها تكفل مستوى كافياً من الحماية للبيانات الشخصية، ويُشر هذا الكشف في الجريدة الرسمية..."

مادة (13) الاستثناءات

"استثناءً من أحكام المادة (12) من هذا القانون، يجوز لمدير البيانات نقل بيانات شخصية خارج المملكة إلى بلد أو إقليم لا يوفر مستوى كافياً من الحماية للبيانات في أيٍّ من الحالات الآتية:

- في حال تم علاج بيانات شخصية من غير إخطار الهيئة بذلك، يعد ذلك لحكم الفقرة (1) من المادة (14) من هذا القانون والتي توجب على مدير البيانات ضرورة حصوله على إخطار من قبل الهيئة قبل بدء عملية المعالجة.
- كل من لم يقدّم بإخطار الهيئة بالتغييرات التي طرأت على البيانات بعد أن سبق إخطار الهيئة بها.
- من قام بمعالجة البيانات الشخصية دون الحصول على تصريح مسبق من الهيئة، ويعد هذا مخالفة لحكم المادة (15) من هذا القانون والتي توجب الحصول على تصريح كتابي من قبل الهيئة قبل عملية المعالجة.
- في حال قدم المعالج للهيئة أو صاحب البيانات بيانات كاذبة أو مضلّة أو خلاف الثابت في السجلات أو البيانات أو المستندات التي تكون تحت تصرّفه.
- أخفى عن الهيئة أي بيانات أو معلومات أو سجلات أو مستندات من تلك التي يجب عليه تزويد الهيئة بها أو تمكينها من الاطلاع عليها، للقيام بمهامها المقررة بموجب هذا القانون.
- في حالة التسبب في عرقلة عمل مفتشي الهيئة أو أيّ تحقيق تكون الهيئة بصدد إجرائه.
- في حال قام المعالج بالإفصاح عن أي بيانات أو معلومات من المتاح له الوصول إليها بحكم عمله أو استخدامها لمنفعته أو لمنفعة الغير، وذلك بدون وجه حق وخلافاً لأحكام هذا القانون.

2- الغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تتجاوز عشرين ألف دينار:

- على كل من خالف حكم أيّ من الفقرتين (1) أو (2) من المادة (32) من القانون²⁵⁶، وإذا تم الحكم بالإدانة للمحكمة أن تقضي بمصادرة المبالغ المتحصّلة من الجريمة.

1- إذا وافق صاحب البيانات على هذا النقل.

2- إذا كان هذا النقل لبيانات مستخرجة من سجل تم إنشاؤه وفقاً للقانون بغرض توفير معلومات للجمهور...

²⁵⁶ المادة (32) من قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018 نصت على:

"1 - لعضو مجلس الإدارة لدى نظر المجلس لأيّ موضوع يكون لهذا العضو فيه مصلحة شخصية مباشرة أو غير مباشرة تتعارض مع مقتضيات منصبه، أن يُفصح عن ذلك كتابة حال علمه بعزم المجلس نظر هذا الموضوع، ولا يجوز لهذا العضو حضور مناقشات المجلس بشأن ذلك الموضوع أو التصويت عليه.

3- الحبس مدة لا تزيد على شهر وبالغرامة التي لا تقل عن مئة دينار ولا تتجاوز خمسمئة

دينار، أو بإحدى هاتين العقوبتين:

كل من يستعمل دون وجه حق شعار الهيئة أو رمزاً أو إشارة مماثلة أو مشابهة له.

ونشير هنا إلى أن الغرامات التي نص عليها قانون حماية البيانات الشخصية البحريني تختلف من حيث طبيعتها عن تلك التي تضمنها النظام الأوروبي العام، حيث إن الغرامة في القانون البحريني تعتبر عقوبة جنائية، بينما هي غرامة إدارية وفقاً للنظام الأوروبي العام لحماية البيانات الشخصية، وهو ما يترتب عليه اختلاف الاختصاص بتوقيع الغرامة في كل من النظامين. ففي أوروبا تختص مراكز حماية البيانات بتقدير الغرامة وتوقيعها وتخفيفها، بينما ينعقد الاختصاص للمحكمة في مملكة البحرين.

ويعني ذلك أيضاً خضوع الغرامات في مملكة البحرين باعتبارها غرامات جنائية لكافة قواعد العقوبات الجنائية، فهي تخضع لمبدأ الشرعية، ولمبدأ شخصية العقوبة، وتتعدد بتعدد الفاعلين، وهو ما يعني إمكانية خضوع أكثر من متحكم أو حائز للغرامة كل على حدة عن الفعل نفسه. كما نجد أن النظام الأوروبي العام لحماية البيانات الشخصية تضمن تقسيماً وحيداً للغرامات، ووفقاً لهذا التقسيم يكون الحد الأقصى للغرامة هو عشرة ملايين يورو أو 2% من الدخل السنوي الإجمالي للجهة في حالات معينة، وترتفع الغرامة في حالات أخرى لتصل إلى 20 مليون يورو أو 4% من الدخل الإجمالي كحد أقصى، أما بالنسبة للقانون البحريني فقد أثر المشرع أن يكون أكثر تفصيلاً في هذا الصدد، فجعل نطاق العقوبة يتفاوت بحسب كل فعل أو مجموعة أفعال دون أن يضع نطاقاً عاماً لكافة الانتهاكات.

في إطار تحديد نطاق الغرامات يلاحظ أن القانون البحريني قد أغفل ذكر معايير لتحديد قيمة الغرامة، فترك الأمر لسلطة القاضي والتفريد القضائي للعقوبة دون إعطائه معايير يسترشد بها، وهو مسلك يخالف ما جاء في المادة (83) من النظام الأوروبي العام لحماية البيانات الشخصية، إذ تحدد مجموعة عوامل تساعد على تقدير الغرامة بحسب طبيعة الانتهاك الواقع وجسامته، وما إذا كان عمدياً، ومحاولات المتحكم أو المعالج لتدارك الخرق وغيرها²⁵⁷. كذلك لم

2- يُحظر أن يكون للرئيس التنفيذي أو لأي من موظفي الهيئة مصلحة مباشرة أو غير مباشرة في مجال عمل الهيئة تتعارض مع مقتضيات الوظيفة، وعلى كل منهم الإبلاغ كتابة فوراً عن أية مصلحة تنشأ له في هذا الشأن خلال فترة شغل الوظيفة لدى الهيئة. ويكون إبلاغ الرئيس التنفيذي لمجلس الإدارة، وما عداه من موظفي الهيئة فيبلغ الرئيس التنفيذي".

²⁵⁷ Art. 83 GDPR General conditions for imposing administrative fines

يتميز القانون البحريني في المعاملة العقابية بين المؤسسات الكبيرة والصغيرة، فلم يمنح الأخيرة أي إعفاءات أو وضع أحكاماً مخففة أو نطاق غرامات أقل. وعلى ذلك يكون قد ترك أمر التدرج في العقوبة للقاضي.

المطلب الثاني

معوقات تطبيق قواعد حماية البيانات الشخصية

تأتي مساهمة مملكة البحرين في الجهود الدولية لحماية البيانات الشخصية نتيجة لإيمان المملكة بأن القواعد القانونية التقليدية قاصرة عن تنظيم المجال المعلوماتي، وهو ما يتطلب خلق إطار قانوني ملائم لتحديات العصر الرقمي، ثم العمل على بلورة قواعد على أرض الواقع من خلال خلق آليات قانونية (قانون حماية البيانات الشخصية رقم 30 لسنة 2018)، وآليات مؤسساتية (الهيئة الوطنية المعنية بحماية البيانات) تضمن التطبيق الفعال بغية تحقيق غايات وأهداف المشرع البحريني سواء في بعدها الحقوقي أو الاقتصادي. بناء على ذلك سوف نتناول التالي:

الفرع الأول: محدودية الآليات القانونية لحماية البيانات الشخصية

الفرع الثاني: محدودية الآليات المؤسساتية لحماية البيانات الشخصية

الفرع الأول: محدودية الآليات القانونية لحماية البيانات الشخصية

يتوقف تطبيق قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018 على مدى وعي ومعرفة المسؤولين عن المعالجة والمعنيين بأمرها وبأهمية الحقوق والضمانات التي منحها هذا القانون، والنتائج المترتبة على مخالفتها. ولا يمكننا أن نتغاضى عن أثر التطور التكنولوجي المستمر الذي يضع النصوص القانونية في موقف العاجز أمام ثورة التقنية المعلوماتية. وأظهرت لنا هذه الدراسة إن نصوص القانون البحريني جاءت مقاربة ومتأثرة بشكل كبير بنصوص النظام الأوروبي العام لحماية البيانات الشخصية، ومن المتوقع أن يتأثر المشرع البحريني بما يدخله المشرع الأوروبي من تعديلات على نظامه، فستجد البلدان المتعاملة اقتصاديا مع الاتحاد الأوروبي ومن بينها مملكة

“Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

1Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). 2When deciding whether to impose an administrative fine and deciding on the amount of the administrative ..”

البحرين، نفسها مضطرة إلى التحرك من أجل الملاءمة السريعة حتى لا تفقد سوقا تجاريا وزبائن مهمين²⁵⁸.

كما إن ارتباط عمليات المعالجة بالتقنية والتكنولوجيا يجعلها تتدرج ضمن الجرائم المعلوماتية التي يصعب اكتشافها وإثباتها، ولذلك يتم اكتشاف هذا النوع من الجرائم عادة بمحض الصدفة، فهي عبارة عن أرقام وبيانات تتغير أو تمحى تمامًا من السجلات المخزونة في ذاكرة الحسابات الآلية. و يمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى أمرين:

1. أن الجريمة لا تترك أي أثر خارجي لها بصورة مرئية .
2. تمكن الجاني من ارتكاب هذه الجريمة في عدة دول وقارات أخرى على غرار الشركات العالمية في مجال الإنترنت، مثل فيسبوك وغوغل. بالإضافة لما سبق، أن مسألة إثبات هذه الجرائم أمر صعب، لأنه يتم ارتكابها دون وجود أي أثر مادي لها، بالإضافة إلى وسائل الإثبات التي جاء بها قانون حماية البيانات الشخصية البحريني والمتمثلة في المحاضر لا تتماشى مع خطورة هذه الجرائم الماسة بالحق في الخصوصية، فمحاضر ضبطية الشرطة القضائية تتقصها الخبرة والتكوين، ومحاضر هيئة حماية البيانات الشخصية تتقصها الحجية الصريحة²⁵⁹.

الفرع الثاني : محدودية الآليات المؤسسية لحماية البيانات الشخصية

أورد قانون حماية البيانات الشخصية البحريني رقم (30) لسنة 2018 العديد من الأحكام القانونية، التي تعكس الدور الكبير الذي تضطلع به هيئة حماية البيانات الشخصية، وعلى الرغم من ذلك فلا تملك هيئة حماية البيانات الشخصية سلطة فرض عقوبات زجرية ، وتقتصر سلطاتها على ما تتخذه من قرارات إدارية و تأديبية²⁶⁰.

كما أن السلطة المالية والإدارية للهيئة وإن كانت مستقلة فهي تخضع لرقابة الوزير المختص بشؤون العدل ما يجعلها لا تكتسب حجية مطلقة، وهو ما يؤكد محدودية دورها في ضمان تطبيق حقيقي وفعال لقواعد حماية البيانات الشخصية ، وكما إن تواصل هيئة حماية البيانات

²⁵⁸ حسن الحافظي، المرجع السابق، ص190.

²⁵⁹ رصاع فتية الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل ماجستير في القانون العام، كلية الحقوق والعلوم

السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012، ص45.

²⁶⁰ عبد المجيد كوزي، الحماية القانونية للبيانات و المعطيات ذات الطابع الشخصي، أطروحة لنيل الدكتوراه في القانون الخاص، جامعة سيدي محمد بن عبد الله، فاس، 2015، ص358.

الشخصية مع أفراد المجتمع لنشر ثقافة قانونية وحقوقية في هذا المجال ضعيف جدا حتى هذه اللحظة، وذلك على الرغم من محدودية معلومات فئات المجتمع البحريني بخطورة وأبعاد هذا الموضوع، وعدم استيعاب تطورات ونتائجه على حقوقهم وحررياتهم، خاصة إن قانون حماية البيانات الشخصية البحريني لا يزال تشريعاً حديثاً فلا بد من إيضاحه للناس عامة²⁶¹.

أما بالنسبة للقضاء ، فهو يعد الضامن الأساسي للحقوق والحریات، ويقوم بالرقابة على أعمال الهيئة الوطنية لمراقبة حماية البيانات الشخصية، وتعتبر أهم مظاهر محدودية دور القضاء في تطبيق قواعد القانون وضمان تحقيق غاياته وأهدافه متمثلة في ضعف الخبرة والتكوين في مجال الجرائم المعلوماتية بشكل عام، وجرائم المعالجة للبيانات الشخصية بشكل خاص، مما يخلق نوعاً من الارتباك في ضمان تطبيق فعال يتماشى مع غاية المشرع من قانون حماية البيانات الشخصية البحريني والقوانين ذات الصلة بمجال حماية البيانات الشخصية²⁶².

²⁶¹ حسن الحافظي، مرجع سابق، ص 191.

²⁶² عبد المجيد كوزي، المرجع السابق، ص 358.

الخاتمة

في ختام هذه الدراسة نجد أن التطور التكنولوجي في مجال المعلومات و وسائل الاتصال، والاستعمال المكثف و المفرط للبيانات الشخصية المرتبطة بالحياة الخاصة للأفراد، من خلال عمليات المعالجة الآلية للبيانات الشخصية، قد خلق صعوبات كبيرة مرتبطة بمسألة التحكم فيها و مراقبتها مقارنة بالمعالجة التقليدية اليدوية، مما أدى إلى انتشار المخاوف من تلاشي الحق في الخصوصية، خاصة وأنّ البيانات الشخصية أصبحت اليوم من أهم عناصر الحق في الحياة الخاصة و بالتالي عنواناً لكرامة الإنسان و حقوقه وحرياته، وتقوم الحاجة لحمايتها على أساس أنها حق من حقوق الإنسان التي يسعى المجتمع الدولي للحفاظ عليها ، و هو ما دفع المشرع البحريني للتحرك من أجل وضع إطار قانوني قادر على خلق التوازن بين استعمال التكنولوجيا و الحرص على القيم الأساسية و على رأسها الحريات الأساسية و الشخصية في ظل قصور القواعد القانونية التقليدية عن تنظيم المجال المعلوماتي.

وبعد الانتهاء من دراسة موضوع حماية البيانات الشخصية في ضوء التطورات التكنولوجية المعاصرة، نستخلص حصيلة هذه الدراسة في (النتائج) ومن ثم نستعرض ما توصلنا له من (توصيات).

أولاً: النتائج

خلصت هذه الدراسة التي تناولت موضوع الحماية القانونية للبيانات الشخصية والتي قارنت بين التشريع البحريني و النظام الأوروبي العام لحماية البيانات الشخصية إلى مجموعة من النتائج وهي كالآتي:

1. إن الحق في الخصوصية يعتبر حقاً دستورياً لا يقل أهمية عن الحقوق والحريات العامة التي نص عليها الإعلان العالمي لحقوق الإنسان والعهديين الدوليين.

2. ترتبط مسألة حماية البيانات الشخصية في الفضاء الرقمي بالحق في الخصوصية الذي بات اليوم عرضة لانتهاكات صارخة خاصة عند استخدام التطبيقات التكنولوجية والتقنية المختلفة.

3. لم يعرف المشرع البحريني الحق في الخصوصية ، واكتفى بسرد صور الحياة الخاصة في الدستور البحريني ، واعتبر الحق في الخصوصية من الحقوق الملازمة للشخصية.
4. قام المشرع البحريني، وعلى غرار المشرع الأوروبي، بتعداد صور عمليات المعالجة على سبيل المثال لا الحصر، رغبة منه في التوسع بمفهوم المعالجة لتشمل الصور التي يمكن أن تظهر مستقبلاً بفضل التقنيات المتجددة في عصر الثورة التقنية اليوم، وذلك لضمان الحماية ضد أي فعل أو عملية قد تمس الحريات الشخصية تحت حجة غياب النص القانوني.
5. يعد مبدأ تقييد مدة حفظ البيانات أحد أهم الآليات الكفيلة باحترام البيانات الشخصية بوجه عام، كما يشكل أهمية في تدعيم الحق في النسيان الرقمي وحمايته، إذ إن حفظ البيانات الشخصية ولا سيما تلك التي تتدرج في صميم الحياة الخاصة للإنسان لمدة زمنية محدودة وغير دائمة يعني وجوب إتلافها أو محوها فيما بعد، ومنع الرجوع إليها مهما كانت الأسباب، ما يساهم بشكل كبير في تحقيق النسيان الرقمي.
6. لم يحظر كل من المشرع البحريني والأوروبي معالجة البيانات الشخصية بشكل مطلق، ووضعاً شروطاً يجب أن تتحقق لكي تتصف المعالجة بالمشروعية، وفي حالة لم تتم مراعاة أحد هذه الشروط ستكون عملية المعالجة غير مشروعة.

ثانياً: التوصيات

نوصي من خلال هذه الدراسة بالآتي:

- 2- يعتبر قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018 بشكله الحالي وبصياغته المقاربة للنظام الأوروبي العام لحماية البيانات الشخصية ، غير كاف للوصول إلى الغاية من إصدار هذا القانون وذلك ، بسبب قصور بعضاً من مواد القانون الحالية فنجد أن المشرع البحريني لم يضع الضوابط اللازمة لممارسة الحقوق التي منحها لصاحب البيانات ، كذلك لم يأت بتعريف عام للبيانات الحساسة، ولم يعرف البيانات التي ألحق بها صفة الحساسية (مثل البيانات البيومترية أو الجينية)، بالإضافة أنه لم يحدد سن الأهلية.
- 3- في ظل التطورات التكنولوجية والتقنية التي نشهدها يجب أن تعمل هيئة حماية البيانات الشخصية على نشر الثقافة القانونية والوعي الرقمي لدى الأفراد ، وذلك بهدف توعيتهم بمدى أهمية بياناتهم الشخصية ، مع تنبيههم بالمخاطر التي تحيط بها والأضرار التي قد تصيبهم من جراء التفريط بها.

- 4- يتعين على القائمين على معالجة البيانات الشخصية التقيد بأن تكون عملية الجمع مشروعة وضمن الأغراض والغايات التي يتطلبها القانون.
- 5- تضافر الجهود دول مجلس التعاون الخليجي من أجل العمل على إصدار تشريع قانوني موحد لحماية البيانات الشخصية ، وذلك نظرا لنجاح تجربة المشرع الأوروبي الذي وحد شرع نظام موحد بين دول الاتحاد لحماية البيانات الشخصية،
- 6- على الرغم من معالجة المشرع البحريني للحق في النسيان الرقمي ، إلا أنه بحاجة لمعالجة هذا الحق بنصوص أكثر تفصيلاً وذلك على غرار مافعل المشرع الأوروبي في النظام الأوروبي العام لحماية البيانات الشخصية، وذلك لأهمية تفعيل هذا الحق لحماية خصوصية البيانات الشخصية من الانتهاك .

قائمة المراجع

(المراجع العربية)

أولاً: المعاجم

- ابن منظور، لسان العرب، دار صادر للطباعة والنشر ، جزء 8، بيروت ، 2000.
- محمد بن مكرم بن منظور، لسان العرب ، دار المعارف، القاهرة، جزء 2، مصر، (لا يوجد سنة).
- شطب الممدود أبو الطويل ، الألباني ، صحيح الترغيب .

ثانياً: الكتب

- الكتب العامة
- عبدالرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء الأول، نظرية الالتزام بوجه عام مصادر الالتزام، تنقيح المستشار حمد مدحت المراغي، طبعة نادي قضاة مجلس الدولة، مصر، 2008.
- محمود نجيب حسني ، شرح قانون العقوبات القسم الخاص ، دار النهضة العربية ، الطبعة السادسة، مصر، 2019.

1. الكتب المتخصصة

2. أيمن عبدالله فكري، جرائم نظام الحاسوب، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007.
- سليمان مرقص، الوافي في شرح القانون المدني، الفعل الضار، الجزء الثالث، دار المنشورات الحقوقية ، بيروت ، 1998.
- سعيد جبر، الحق في الصورة، دار النهضة العربية، القاهرة، 1986.
- علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، مطابع جاد للأوفست، الرياض، 1436 هـ.
- عبدالهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الإنترنت، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2013.
- عدنان سرحان، المصادر غير الإرادية للالتزام، دراسة معززة بأحدث توجهات القضاء الإماراتي، مكتبة الجامعة، الشارقة، الطبعة الأولى، 2010.
- حسام الدين كمال الأهواني، الحق في احترام الحياة الخاصة - الحق في الخصوصية- دراسة مقارنة ، دار النهضة العربية، القاهرة ، مصر ، 1978.
- حسان أحمد محمد، نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدول والافراد ، دار النهضة العربية، القاهرة، 2001.
- محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، 2005.
- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003.
- محمد عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، مصر، 2020.
- مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، الطبعة الاولى، القاهرة ، 2016.
- ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي ،دار الثقافة للنشر والتوزيع ، القاهرة ، 1996.

- منصور بن صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلومات السعودي، جامعة نايف للعلوم الأمنية، الرياض، 2010.
- منى أبو أشقر جبور و محمود جبور، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد ، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، الطبعة الأولى، لبنان، 2018.

ثالثاً: المجالات العلمية والبحوث

- إبراهيم بن داود و أشرف شعت، الاطلاع على البريد الإلكتروني بين متطلبات النظام العام والحق في سرية المراسلة ، مجلة دفاتر السياسة والقانون التي تصدرها جامعة الغرير في دبي، الإمارات العربية المتحدة ، العدد 16، 2017.
- أحمد محمد العداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، جامعة بنها، العدد الثالث والثلاثون – الجزء الرابع، مصر، 2020.
- أحمد محمد علي عبد المختار، توظيف تقنيات أنترنت الأشياء في تطوير خدمة المكتبات الأكاديمية، جامعة المنيا مصر، مجلة ببلوفيليا لدراسة المكتبات والمعلومات، المجلد 3، العدد 10 ، مصر ، 2021 .
- الزين بوخلوط، الحق في النسيان الرقمي، مجلة العلوم الإنسانية – جامعة محمد خيضر بسكرة، العدد 46، جامعة عنابة، ، الجزائر، 2017.
- الصالحين محمد العيش، التنظيم القانوني لاستخدام البيانات الشخصية في الإعلام الجديد، مجلة الحقوق ، العدد 2 ، المجلد 13 ، كلية الحقوق جامعة بنغازي ، ليبيا ، (لايوجد سنة).
- أمين الخنتوري، معالم تنظيم الحق في النسيان الرقمي في التشريع المغربي، جامعة سيدي محمد بن عبد الله بن فاس، مجلة الصدى للدراسات القانونية والسياسية، العدد الخامس، المغرب، 2020.
- أمين بن سعيد و نادية عبد الرحيم و أحمد مخلوف، مستقبل نظم المعلومات المحاسبية في ظل تكنولوجيا الحوسبة السحابية، مجلة الميادين الاقتصادية، المجلد 01، العدد 01، الجزائر ، 2018.

- بارق منتظر عبد الوهاب، جريمة إنتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني، دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، عمان ، الأردن، 2017.
- بشيخ محمد حسين وبن ديدة نجاه، الحق في النسيان كآلية لحماية المعطيات الشخصية، مجلة القانون العام الجزائري والمقارن، المجلد الثامن، العدد 01، الجزائر، 2022.
- تومي بن يحي، "الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07 دراسة تحليلية"، مجلة الأستاذ لباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 4 ، العدد 02 الجزائر، 2019.
- جوهر قوادي صامت، الضوابط القانونية لمعالجة البيانات الشخصية الكترونيا، جامعة حسيبة بو علي الشلف، المجلد 06 ، العدد 02 الجزائر، 2022.
- حسن عبد الحميد، دراسة نقدية لقانون حماية البيانات الشخصية المصري رقم (101) ، كلية القانون الجامعة البريطانية، (الطبعة لا يوجد) ، مصر، 2020.
- سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية العدد 9، السنة 3، الكويت ، 2015.
- سامح عبدالواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها (دراسة في القانون الإماراتي)، مجلة البحوث القانونية والاقتصادية، المجلد 8، العدد 67، جامعة الشارقة، الإمارات، 2018.
- سوز حميد مجيد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، دراسة تحليلية مقارنة، جامعة السليمانية، السنة السادسة، العدد 11، العراق ، 2018.
- عائشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث ، المجلد الثاني ، العدد 5، جامعة عبد الحميد بن باديس-مستغانم، المغرب ، 2016.
- عبد العالي بالة، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بين الاستقلال والتبعية، جامعة خنشلة، المجلة الجزائرية للأمن الإنساني، المجلد 06، العدد 01، الجزائر ، 2021.
- عبد الصبور قوي، المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، مصر، 2012.

- عبد القادر عمير، تأثير تكنولوجيا المعلومات على الحق في الحياة الخاصة، حوليات جامعة الجزائر 1، المجلد 34، العدد 1، الجزائر، 2020.
- عفيفي كامل عقيقي، جرائم الكمبيوتر، منشورات الحلبي، بيروت، 2003.
- عماد محمد، الاعتداء على حرمة الحياة الخاص في قانون الجرائم الإلكترونية رقم 27 لسنة 2015، مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والدراسات الاستراتيجية، الأردن. 2016.
- عمرو طه بدوي، التنظيم القانوني لمعالجة البيانات الشخصية، دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية، أكاديمية أبوظبي القضائية، الإمارات، 2017.
- عشاوي أمال، مستلزمات الحماية القانونية للمعطيات ذات الطابع الشخصي بعد جائحة كورونا (المعلومات الطبية نموذجا)، جامعة البليدة 2، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد: 58، العدد: 02، الجزائر. 2021.
- غزال نسرين، حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، كلية الحقوق، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 59، العدد 1، 2019، الجزائر.
- فاطمة زهراء المفتاح، ملامح الخصوصية والأنكشاف في عصر التقنيات الذكية، دراسات المستقبل، العدد 7، الإمارات. 2019.
- فتحية حزام، إجراءات المعالجة الآلية للمعطيات ذات الطابع الشخصي وفقاً لأحكام القانون 07-18، جامعة محمد بوقرة- بومرداس الجزائر، 2021.
- فيصل بن وقليل، الحماية الجنائية للحق للدخول في طبي النسيان الرقمي، دراسة مقارنة بين التشريع الجزائري والفرنسي، جامعة يحيى فارس (المدية)، المجلد 08، العدد 01، الجزائر، 2020.
- محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، 2005.
- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003.
- محمد محمد القطب، الحماية المدنية للمعلومات الشخصية في مواجهة الثورة التكنولوجية لوسائل الاتصال والتواصل، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 67، مصر، 2018.

- محمد نواورية، الحماية القانونية للخصوصية المعلوماتية ، مجلة الدراسات القانونية المقارنة، جامعة ممد الشريف مساعدية (سوق أهراس) ، المجلد 06، العدد 02، الجزائر، 2020.
- نعيم السعيداني، حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، مجلة الباحث للدراسات الأكاديمية، المجلد 8، العدد 1 ، الجزائر، 2021،
- نعيم مغيب، مخاطر المعلوماتية والانترنت، منشورات الحلبي، ، الطبعة الثانية، بيروت، 2008،
- هشام بخوش، الجرائم الماسة بسلامة المعطيات ذات الطابع الشخصي وفقا للقانون 07-18 معالجة معطيات فيروس كورونا- نمونجا-، مجلة ابحاث قانونية وسياسة، جامعة محمد الشريف مساعدية المجلد 6، العدد 1، ، سوق أهراس، الجزائر، 2021 .
- وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، دراسة قانونية مقارنة حول الحرية الشخصية والمسؤولية والاختصاص، المركز العربي للبحوث القانونية والقضائية، طبعة 1، لبنان، 2017 .
- يوسف بوجمعة، الحقوق الملازمة للشخصية وتقسيماتها دراسة على ضوء الفقه والقانون والقضاء، مجلة الدراسات القانونية، جامعة المدييه، المجلد الرابع ، العدد الأول، 2018،

رابعا: رسائل الماجستير والدكتوراة

- الشيخ يوسف، حماية الحياة الخاصة في القانون الجنائي المقارن، رسالة دكتوراه، جامعة القاهرة، دار الثقافة للنشر والتوزيع، الأردن، 1996.
- بن حيدة محمد، حماية الحق في الحياة الخاصة في التشريع الجزائري، رسالة دكتوراه، جامعة أبي بكر بلقايد، الجزائر، 2016-2017.
- حسن الحافظي، الحماية القانونية للمعطيات ذات الطابع الشخصي بين التشريع الوطني والاتفاقيات الدولية، رسالة ماجستير، جامعة مولاي أسماعيل، المغرب ، 2017-2018.
- سليم جلاّد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، رسالة ماجستير، جامعة وهران، الجزائر، 2013.
- صفية شاتن ، الحماية القانونية للحياة الخاصة - دراسة مقارنة - ، جامعة مولود معمري، رسالة دكتوراه، الجزائر، 2012.

- عبدالله بن ناصر أحمد العمري ، الحماية الجنائية للبريد الإلكتروني، رسالة ماجستير، كلية الدراسات العليا جامعة نايف العربية للعلوم الامنية، الرياض ،2010.
- عبد المجيد كوزي ، الحماية القانونية للبيانات و المعطيات ذات الطابع الشخصي، رسالة دكتوراة ، جامعة سيدي محمد بن عبد الله، فاس، المغرب، 2014 - 2015 .
- رصاع فتيحة الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، ، تلمسان، 011-2012 .
- نور أحمد العوضي، التنظيم القانوني لعقد الحوسبة السحابية، رسالة ماجستير، جامعة البحرين، 2021.

خامسا: أوراق العمل والندوات

- حسين بن سعيد الغافري، الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الإلكترونية العماني، ورقة مقدمة لمؤتمر "أمن المعلومات الخصوصية في ظل قانون الانترنت" ، القاهرة ،أيام 2-4 يونيو 2008 .
- نيا ب موسى البداينة، جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، جامعة نايف للعلوم الأمنية، الرياض، 1420هـ.
- معاذ سليمان الملا، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الإلكترونية الحديثة دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائي الكويتي، مجلة كلية القانون الكويتية العالمية - أبحاث المؤتمر السنوي الدولي الخامس 9 - 10 مايو 2018.

سادسا: القوانين والتشريعات

1. القوانين والتشريعات الوطنية

- مملكة البحرين، مرسوم بقانون رقم (14) لسنة 2002 دستور مملكة البحرين المعدل.
- مملكة البحرين، مرسوم بقانون رقم (19) لسنة 2001 القانون المدني البحريني.

- مملكة البحرين ، مرسوم بقانون رقم (15) لسنة 1976 قانون العقوبات البحريني.
- مملكة البحرين ، قانون رقم (4) لسنة 2021 قانون العدالة الإصلاحية للأطفال وحمايتهم من سوء المعاملة,
- مملكة البحرين ، قانون رقم (37) لسنة 2012 قانون حماية الطفل البحريني.
- مملكة البحرين ، قانون رقم (22) لسنة 2006 قانون حماية المؤلف والحقوق المجاورة.
- مملكة البحرين، قانون رقم (30) لسنة 2018 المتعلق بحماية البيانات الشخصية .
- مملكة البحرين، مرسوم بقانون رقم (56) لسنة 2018 بشأن تزويد خدمات الحوسبة السحابية لأطراف أجنبية .
- مملكة البحرين، مرسوم بقانون رقم (7) لسنة 1986 قانون الولاية على المال.
- مملكة البحرين، مرسوم بقانون رقم (22) لسنة 2021 قانون التنفيذ المعدل الجديد.
- مملكة البحرين، مرسوم بقانون رقم (42) لسنة 2022 قرار بشأن نقل البيانات الشخصية إلى خارج مملكة البحرين.
- مملكة البحرين، مرسوم بقانون رقم (43) لسنة 2022 قرار بشأن الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات.
- مملكة البحرين، قرار رقم (44) لسنة 2022 بشأن قواعد وإجراءات تقديم الإخطار لهيئة حماية البيانات الشخصية وطلب التصريح المسبق للمعالجة والبت فيه.
- مملكة البحرين، قرار رقم (45) لسنة 2022 قرار بتحديد قواعد وإجراءات معالجة البيانات الشخصية الحساسة.
- مملكة البحرين، قرار رقم (46) لسنة 2022 بشأن مراقبي حماية البيانات.
- مملكة البحرين، قرار رقم (47) لسنة 2022 بتحديد رسوم القيد في سجل مراقبي حماية البيانات ورسوم تجديد القيد وحالات الإعفاء منها وردها،
- مملكة البحرين، قرار رقم (48) لسنة 2022 بشأن حقوق صاحب البيانات الشخصية.
- مملكة البحرين، مرسوم بقانون رقم (49) لسنة 2022 قرار بشأن الإجراءات والقواعد الخاصة بتقديم الشكاوى عن مخالفة أحكام قانون حماية البيانات الشخصية.
- مملكة البحرين، قرار رقم (50) لسنة 2022 قرار بتحديد ضوابط و ضمانات المحافظة على سرية البيانات المتعلقة برفع الدعوى الجنائية وبالأحكام الصادرة فيها.
- مملكة البحرين، قرار رقم (51) لسنة 2022 قرار بشأن شروط إنشاء سجلات البيانات الشخصية المتاح للجمهور الاطلاع عليها.
- الكويت، قانون رقم (20) لسنة 2014 في شأن المعاملات الإلكترونية.
- الإمارات، قانون رقم (2) لسنة 2016 المتعلق بإنشاء مؤسسة بيانات دبي.

- المملكة العربية السعودية، مرسوم ملكي رقم (م/19) وتاريخ 9/2/1443هـ والمتعلق بحماية البيانات الشخصية.
- المغرب، قانون رقم (08.09) لسنة 2009 والمتعلق بحماية الأشخاص الذاتيين تجاه معالجة البيانات ذات الطابع الشخصي.
- تونس، قانون رقم (63) لسنة 2004 والمتعلق بحماية المعطيات الشخصية.

2. القوانين والتشريعات الأجنبية

- 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)

سابعا: المواقع الالكترونية

- موقع وزارة الصحة البحريني فيما يتعلق بفايروس كورونا : [19وزارة الصحة \(moh.gov.bh\)](https://moh.gov.bh)
- الموقع الرسمي لتويتر: القوانين والسياسات: <https://help.twitter.com/ar/rules-and-policies>
- صحيفة الأيام، قضية رشوة موظف وتسريب بيانات بنكية للعملاء، العدد، 12306، البحرين، 2020 <https://alay.am/p/2txi>
- صحيفة البلاد، قضية رشوة موظف و4 متهمين محليين، العدد 4130، البحرين، 2020 <https://alay.am/p/2txi>
- مركز البحوث والمعلومات، الذكاء الاصطناعي، الغرفة التجارية الصناعية في أبها، 2016، ص5 للمزيد من التفاصيل الرجاء الإطلاع على : <https://www.abhacci.org.sa>
- مكنسة رومبا للإطلاع على المزيد من التفاصيل حولها الرجاء زيارة الموقع التالي [Roomba® Robot Vacuum Cleaners | iRobot®](https://www.irobot.com/Roomba)

ثامنا: الأحكام القضائية (العربية)

- حكم المحكمة الجنائية الكبرى الأولى الجلسة المنعقدة بتاريخ 26/20152/2 - رقم الدعوى غير مذكور

(المراجع الأجنبية)

Journal Articles

- Carlos Salazar, Sunil Patel and Keyur K Patel (2016), *International Journal of Engineering Science and Computing*, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, volume 6 , p 6122 Retrieved from :https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges
- Internet Society Global Internet Report: Paths to Our Digital future (2017), report , p. 32 available at: www.internetsociety.org.
- Stephen Allison, The Concept of Personal Data under the Data Protection Regime, *Edinburgh Student Law Review*, Volume 1, Issue 1, Scotland, 2009 accessible at : edinstudentlawreview .
- Global Internet Report: Paths to Our Digital future, (VA: Internet Society, 2019, USA, p. 32 accessible at. InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf .

Websites

- AMAZON :[Now Open – AWS Middle East \(Bahrain\) | AWS News Blog \(amazon.com\)](https://aws.amazon.com/middle-east/bahrain/) (last visit 18 October 2022.)
- Definition of Super cookie: [What is super cookie? - Definition from WhatIs.com \(techtarget.com\)](https://www.techtarget.com/whatis/definition/super-cookie) (last visit: 11 December 2022)
- Definition of Trojan Horse: [What Is a Trojan Horse? Trojan Virus and Malware Explained | Fortinet](https://www.fortinet.com/resources/white-papers/what-is-a-trojan-horse-trojan-virus-and-malware-explained)
- Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre; accessible at [Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre](https://www.hamburg.de/3530000/Hamburg-Commissioner-Fines-H-M-35-3-Million-Euro-for-Data-Protection-Violations-in-Service-Centre/)

[Protection Violations in Service Centre | European Data Protection Board \(europa.eu\)](#) (Last Visit: 28 of April 2022.).

- Mike Isaac, Cecilia Kang, Facebook Expects to Be Fined Up to \$5 Billion by F.T.C. Over Privacy Issues, The New York Times, accessible at: [Facebook Expects to Be Fined Up to \\$5 Billion by F.T.C. Over Privacy Issues - The New York Times \(nytimes.com\)](#).(last visit 28 MAY 2022.)
- Privacy and Information Technology, Stanford Encyclopedia of philosophy, *published Thu Nov 20, 2014* [Privacy and Information Technology \(Stanford Encyclopedia of Philosophy/Summer 2020 Edition\)](#) (last visit 11 November 2022)
- Society Service definition it available at :https://gdprhub.eu/index.php?title=Article_8_GDPR#Information_Society_Service (last visit: 16 December2022)
- Technologies, *volume 6* , p 6122, available at: https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges (last visit: 31 May 2022
- WP29, Guidelines on Data Protection Officers (“DPOs”)”, WP 243 rev.01, 5 April 2017 (available) at [ARTICLE29 - Guidelines on Data Protection Officers \('DPOs'\) \(wp243rev.01\) \(europa.eu\)](#) (last visit:3November 2022) (last visit: 9 December 2022).

Caselaw

- American Civil Liberties Union v. James Clapper, No. 13-3994 (S.D. New York December 28, 2013), 959 F.Supp.2d 724..
- ECJ, Case C-73/07, 16th of December 2008, Tietosuoja-valtuutettu [Finnish data protection ombudsman] v. Satakunnan Markkinapörssi Oy and Satamedia Oy, 16.12.2008 ("Tietosuoja-valtuutettu").
- C-28/08, Commission V. Bavarian Lager CO., 29.6.2010 ("BAVARIAN LAGER").
- C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO
- GOOGLE VS. DIANA Judgment of the Paris Court of First Instance on 15 February 2012, Diana and Google Drive.
- C-131 Google Spain v AEPD and Mario Costeja González N12.

- COSTEJA GONZALEZ, 13.5.2014 ("GOOGLE"), Paragraphs 26-31"
- Joined Cases C-141/12 AND c372/12 YS v. Minister Voor Immigratie Integratie en Asiel and Minister Voor Immigratie, Integrate en Asiel V. M, S (2014).
- C-291/12, Schwarz v. Bochum, 17.10.2014 ("Schwarz"), Para 28-29

Abstract

This study examines the legal protection of personal data of natural persons from a comparative perspective. It compares and analyses the legal provisions of Bahrain Personal Data Protection Law No. 30 of 2018 (PDP), and the European General Data Protection Regulation (GDPR). The widespread use of modern technology and applications of Internet of Things (IoT) in the processing of personal data and the ease of obtaining and trading data, meant that establishing an effective system to protect personal data against violations has become a necessity. In the light of GDPR provisions, the Bahraini legislator sought to adopt an appropriate legal and regulatory framework to provide the needed protection. The Bahraini (PDP) law identifies the fundamental principles for protection of personal data, the procedures for the automated processing of data, the rights of the persons concerned with the processing, such as the right to information, the right to access, the right to rectification and the right to object. In addition to that, the law established the national authority for the protection of personal data and has enacted criminal and civil sanctions that deter violators. The study attempts to compare the provisions of the two legal systems to determine if the current legal provisions provide adequate legal protection or if further steps are needed from the Bahraini legislator.

UNIVERSITY OF BAHRAIN

College of Law

**Department of Private
Law**



**Protection of Personal Data in the light of
Technological Developments
"A Comparative Study on EU General Data
Protection Regulation"**

A Thesis Submitted in Partial Fulfillment of the Requirements for the
Master Degree in in Private Law

Submitted by
Saja kherallah khalaf
201700040

Supervised by
Dr. Hanan Mohamed Almawla
Assistant Professor of Civil Law and IP Law
College of Law

Kingdom of Bahrain
March 2023