قانون حماية البيانات الشخصية

د. عبد القادر ورسمه غالب

البيانات الشخصية من الأمور الحساسة، وقد أصدرت البحرين قانون "حماية البيانات الشخصية" الذي يبدأ سريانه اعتبارا من أغسطس هذا العام، ولذا لزم التنويه. وللأهمية نشير إلى أن القانون البحريني جاء متضمنا لأهم المبادئ القانونية العامة الخاصة بحماية هذه الحقوق الشخصية وبهذا فإن المشرع البحريني قصد أن يضع البحرين في مستوي المعايير الدولية التي ينادي بها العالم.

كأمثلة لهذا، ووفق القانون البحريني، فإن البيانات الشخصية تشمل (أية معلومات في أية صورة تخص "فردا معرفا" أو قابلا بطريق مباشر أو غير مباشر لأن يعرف، 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 قابلا لأن يعرف، تراعى كافة الوسائل التي يستخدمها مدير البيانات أو أي شخص آخر، أو التي قد تكون متاحة له)، وهذا تعريف شامل بدون لبس للبيانات الشخصية. وهناك خطوة اضافية بتعريف البيانات الشخصية الحساسة وهي (أية معلومات شخصية تكشف على نحو مباشر أو غير مباشر عن أصل الفرد العرقي أو الإثني أو آرائه السياسية أو الفلسفية أو معتقداته الدينية أو انتمائه النقابي أو سِجِل السوابق الجنائية الخاص به أو أية بيانات تتعلق بصحته أو حالته الجنسية)، وجميع هذه البيانات الشخصية يحميها القانون المعني.

ولحماية جميع "البيانات الشخصية"، فإن القانون ينظم كيفية التعامل مع هذه البيانات عبر "المعالجة" التي حددها القانون صراحة وتشمل، (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 تحويرها أو تعديلها، أو استعادتها أو استخدامها أو الإفصاح عنها، من خلال بثِّها أو نشرها أو نقلها أو إتاحتها للغير، أو دمجها أو حجبها أو مسحها أو تدميرها). واضافة لهذا، هناك شروط يجب أن تراعى بشأن البيانات الشخصية التي تتم معالجتها، منها:

- أن تكون المعالجة منصفة ومشروعة،
- أن تكون قد جمعت لغرض مشروع ومحدد وواضح،
- ألا تتم معالجتها لاحقاً،

- ألا يتم إجراء معالجة لاحقة لها على نحو لا يتوافق مع الغرض الذي جمعت من أجله، ولا تعد معالجة غير متوافقة مع الغرض الذي جمعت من أجله البيانات المعالجة اللاحقة لها التي تتم حصرا لأغراض تاريخية أو إحصائية أو للبحث العلمي، بشرط ألا تتم لدعم اتخاذ أي قرار أو إجراء بشأن فرد محدد،
- أنْ تكون كافية وذات صلة وغير مفرطة بالنظر للغرض من جمعها أو الذي تمت المعالجَة اللاحقة لأجله،
- أن تكون صحيحة ودقيقة، وتخضع لعمليات التحديث عندما يكون لذلك مقتضى،
- ألا تبقى في صورة تسمح بمعرفة صاحب البيانات بعد استنفاد الغرض من جمعها أو الذي تتم المعالجَة اللاحقة لأجله.
- تحفظ البيانات التي يتم تخزينها لفترات أطول لأغراض تاريخية أو إحصائية أو للبحث العلمي في صورة مجهولة بتحويرها، بوضعها في صورة لا تمكن من نسبة هذه البيانات إلى صاحبها. ويتعين إن تعذر ذلك تشفير هوية أصحابها.

و"الاشتراطات العامة" للمعالجَة المشروعة تحظَر معالجَة البيانات الشخصية دون موافقة صاحبها، ما لم تكن هذه المعالجَة ضرورية في حالات معينة كتنفيذ عقد يكون صاحب البيانات طرفاً فيه، اتخاذ خطوات بناء على طلب صاحب البيانات بهدف إبرام عقد، تنفيذ التزام يرتبه القانون، خلافاً لالتزام عقدي أو صدور أمر من محكمة مختصة أو النيابة العامة، حماية المصالح الحيوية لصاحب البيانات، مباشرة المصالح المشروعة لمدير البيانات أو أي طرف ثالث يفصح له عن البيانات، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية لصاحب البيانات.

إضافة لهذا فهناك "الاشتراطات الخاصة" بمعالجة البيانات الشخصية الحساسة، كـ :

- حظر معالجَة البيانات الشخصية الحساسة دون موافقة صاحبها، ويستثنى من هذا الحظْر ما يأتي المعالجة التي يقتضيها قيام مدير البيانات (معرف في القانون) بالتزاماته ومباشرة حقوقه المقررة قانونا في مجال علاقة العمل التي تربطه بالعاملين لديه،
- المعالجة الضرورية لحماية أي 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 طبقاً للقانون.
- معالجة البيانات التي أتاحها صاحبها للجمهور،
- المعالجة الضرورية لمباشرة أي من إجراءات المطالبة بالحقوق القانونية أو الدفاع عنها، بما في ذلك ما يقتضيه التجهيز لهذا الأمر والاستعداد له،

- المعالجة الضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو تقديم الرعاية الصحية أو العلاج أو إدارة خدمات الرعاية الصحية من قَبل مرخص له بمزاولة أي من المهن الطبية، أو أي 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 بأن تتم المعالجة في حدود ما هو ضروري للغرض الذي أنشئت الجمعية أو النقابة أو الجهة من أجله،
- أن ترد المعالجة على بيانات تخص أعضاء تلك الجمعية أو النقابة أو الجهة أو لأفراد لهم اتصال منتظم معها بحكم طبيعة نشاطها،
- ألا يتم الإفصاح عن البيانات لأي شخص آخر ما لم يوافق صاحب البيانات على ذلك،
- المعالجَة التي تتم من قبل جهة عامة مختصة بالقدر الذي يقتضيه تنفيذ المهام المنوطة بها قانونا،
- معالجة بيانات تتعلق بالأصل العرقي أو الاثني أو الديني إذا كانت ضرورية للوقوف على مدى توافر المساواة في الفرص أو المعاملة لأفراد المجتمع الذين ينحدرون من أصول عرقية أو اثْنية أو دينية مختلفة، وبشرط مراعاة الضمانات المناسبة لحقوق وحريات أصحاب البيانات المقرَّرة قانوناً.

يتضح من هذه الشروط القانونية أن البيانات الشخصية يحميها القانون منعا لاختراقها وسوء التعامل بها لأي غرض، وللأهمية سنتطرق للالتزامات القانونية الأخرى تباعا.

ملامح قانون الاتحاد الأوربي لحماية البيانات

إن انتهاك البيانات الشخصية واستخدامها في أنشطة مختلفة دون رضاء أصحابها، أصبح دافعا لتبني قوانين جديدة لحمايتها وصيانتها.

يعتبر القانون الأوربي لحماية البيانات الشخصية الذي دخل حيز التنفيذ أخيرا، من أهم هذه القوانين وهو لا يميز ويلزم الجميع بالتنفيذ التام لحماية البيانات والخصوصية داخل أوروبا. وبذا، فالقانون يهدف لمنح المواطنين والمقيمين السيطرة على بياناتهم الشخصية وخصوصيتهم. وعبر هذا الدور الهام، تلعب القوانين دورا مفصليا في تشكيل علاقة الفرد بالآخر والمجتمع ككل، وهكذا يتطور نمط الحياة وفق ضوابط قانونية متطورة.

ويتضمن هذا القانون الشروط المتعلقة بمعالجة البيانات الشخصية التي يمكن التعامل معها، وفي جميع الأحوال، يجب:

- اتمام العمليات التجارية عند التعامل مع البيانات الشخصية حسب التصميم وبشكل افتراضي،
- تخزين البيانات الشخصية باستخدام اسم مستعار أو إخفاء الهوية بالكامل، مع استخدام أعلى درجات الخصوصية بحيث لا تكون البيانات متاحة بشكل عام "لأي عين أو أذن"،
- لا يجوز معالجة البيانات الشخصية ما لم يتم ذلك بموجب القانون أو الموافقة الصريحة من صاحبها.
- على معالج البيانات الشخصية أن يكشف عن البيانات التي يجمعها، وكيف يجمعها، ولماذا يتم معالجتها، وكم من الوقت يتم الاحتفاظ بها، وما إذا يتم مشاركتها مع أي طرف ثالث.
- يحق للشخص طلب نسخة من البيانات التي يجمعها المعالج،
- كذلك له الحق في طلب مسح البيانات.
- يتوجب على السلطات العامة والشركات التي تعالج البيانات الشخصية، توظيف مختص لتأكيد الامتثال بالقانون.
- يجب على الشركات الإبلاغ عن أي خرق للبيانات في غضون ثلاثة أيام، إذا كان لها تأثير سلبي. ولذا، الآن من الأمور الروتينية أن نسمع من الشركات بالاختراقات، وسابقا كان من الأمور السرية للغاية خوفا من العواقب.

ووفقا للقانون الأوروبي فإن "**البيانات الشخصية هي أي معلومات تتعلق بفرد، سواء كانت تتعلق بحياة خاصة به أو مهنية أو عامة. يمكن أن تكون أي شيء من اسم أو عنوان منزل أو صورة أو عنوان بريد إلكتروني أو تفاصيل المصرف، أو عنوان كمبيوتر وبقية (أنماط البيانات – آي بي – المشاركات) على مواقع الشبكات الاجتماعية أو المعلومات الطبية ...**". وبعد تعريفها، فإن حماية هذه البيانات يتطلب "تصميم تحكم" خاص لحماية البيانات المتعلقة بتطوير العمليات الخاصة بالمنتجات والخدمات. لذا:

- يجب تحديد الخصوصية على مستوى عال بشكل افتراضي.
- اتخاذ التدابير التقنية والإجرائية من قبل وحدة التحكم للتأكد من أن المعالجة، وطوال فترة المعالجة، تتم وفق اللوائح، مع تنفيذ آليات لضمان عدم معالجة البيانات الشخصية ما لم تكن ضرورية للغرض المحدد.

وللمزيد من الخصوصية الأوربية، فإنه لا يجوز الاعتراف بأي حكم من محكمة وبقرار يصدر من سلطة إدارية لبلد ثالث يطلب جهاز تحكم أو معالج لنقل البيانات الشخصية أو الإفصاح عنها بأي طريقة ما لم يستند ذلك لاتفاق دولي، أو معاهدة مساعدة قانونية سارية المفعول بين الدولة والاتحاد الأوروبي أو دولة عضو. وحماية

البيانات أيضا تتضمن توجيها منفصلا لحماية البيانات في قطاع الشرطة والعدالة الجنائية ويوفر قواعد لتبادل البيانات الشخصية على المستويات الوطنية والأوروبية والدولية.

سيستفيد المستخدم من هذا القانون من عدة نواحي، أولها أن بياناته لم تعد سلعة رخيصة تستخدم في أي شيء على الإنترنت، ويمكنه المطالبة بحذفها من خوادم الشركات التي يتعامل معها وعليها أن تقوم بذلك في فترة قصيرة. من جهة أخرى سيعرف كل البيانات التي تجمع عنه وبهذا يمنع البيانات، عن حياته الخاصة والمهنية، التي لا يريد مشاركتها مع الآخرين. وستنطبق مجموعة واحدة من القواعد على جميع أعضاء الاتحاد الأوربي وهذا سيخلق قاعدة كبيرة جدا على مستوي العالم للحماية.

ويمنح القانون حق الوصول للبيانات والمعلومات الشخصية وحق معرفة كيفية معالجة هذه البيانات، وهو ما بدأت الشركات توفيره مثل فيسبوك وجوجل وغيرها. إضافة لما سبق، يضمن القانون الجديد للمستخدمين إعلامهم في أقل من ٧٢ ساعة بعد اختراق أي خدمة من الخدمات التي يستخدمونها. ومن المعلوم أن الاختراقات التي تحصل عادة ما تؤدي إلى تسريب البيانات وسوء استخدامها لأي غرض أو بيعها في السوق السوداء، لكن مع القانون الجديد سيتم إشعار المتضررين بالاختراق، ويجب على الشركات توفير النصائح والتوصيات التي تساعد المستخدمين على حماية أنفسهم من تداعيات الاختراق.

من الواضح، أن القانون يضع سياجا قويا حول البيانات الشخصية وفي هذا حماية للجميع ولخصوصيتهم. ولكن، من دون شك نقول، القانون وحده لا يكفي لتغطية كل الحالات. ولهذا، على كل منا أن يكون الحامي الأول لبياناته وخصوصيته لأنه يشكل العتبة الأولى للاختراق أو الصد.

ولنحرص على حماية أنفسنا من كل متطفل يأتي متخفيا عبر الأثير.