مؤسسة حرية الفكر والتعبير
Association for Freedom of Thought and Expression

قانون حماية البيانات الشخصية في ضوء المعايير الدولية

ورقة عن

قانون حماية البيانات الشخصية في ضوء المعايير الدولية

إعداد وكتابة: آلاء كليب

الباحثة بوحدة الأبحاث بمؤسسة حرية الفكر والتعبير

الناشر
مؤسسة حرية الفكر و التعبير

info@afteegypt.org
www.afteegypt.org

قائمة المحتويات:

المنهجية ٤

المقدمة ٤

أولًا: نظرة على القانون المصري لحماية البيانات ٦

ثانيًا: المعايير الدولية خارطة طريق لتشريع قوانين حماية البيانات الشخصية ٧

ثالثًا: القانون المصري تحت مجهر المعايير الدولية ٩

١. ضمان إجراء مفاوضات شفافة وشاملة لجميع الأطراف ٩

٢. تعريف قائمة مبادئ لحماية البيانات تكون ملزمة وتضمينها في الإطار القانوني ٩

٣. تحديد الأساس القانوني الذي يسمح بمعالجة البيانات ١٠

٤. إدراج قائمة بحقوق المستخدمين الملزمة في القانون ١٠

٥. تحديد نطاق واضح للتطبيق ١٠

٦. إنشاء آليات ملزمة وشفافة لنقل البيانات بشكل آمن إلى بلدان ثالثة ١١

٧. حماية أمن ونزاهة البيانات ١١

٨. تطوير آليات منع انتهاك البيانات والإبلاغ عنها ١٢

٩. إنشاء سلطة مستقلة وإنشاء آليات قوية لإنفاذ القانون ١٢

١٠. مواصلة حماية البيانات والخصوصية ١٣

رابعًا: موقف القانون من قاعدة البيانات التي تحتفظ بها شركات الاتصالات ١٤

الخاتمة والتوصيات ١٥

المنهجية:

تعتمد الورقة على تحليل ودراسة قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، وذلك اعتمادًا على اللائحة الخاصة بالاتحاد الأوروبي التي تتعلق بحماية البيانات الشخصية «GDPR"، إضافة إلى دليل الدروس المستفادة من القانون الدولي لحماية البيانات والمعطيات الشخصية الذي أطلقته مؤسسة أكسس ناو.

وتستهدف من خلال ذلك تقديم قراءة أولية عن مدى تطبيق القانون المصري، حديث الإصدار، للمعايير الدولية المستخلصة.

مقدمة:

في ظل انتشار التعاملات الإلكترونية اليومية ومشاركة الأفراد معلوماتهم الشخصية سواء مع جهات عامة أو خاصة، وفي ظل توجه الحكومة إلى التحول الإلكتروني بدلًا من المعاملات الورقية، تتجلى قيمة الأمن الرقمي وأهمية الحفاظ عليه بوضوح أكبر، وتظهر بالتالي أوجه الخلل التي قد تصيب هذا الأمان، وتخلق مستفيدين بشكل غير قانوني من البيانات الشخصية سواء بطريق مباشر، أو بيعها لشركات تجارية وغيرها من الكيانات.

وفي ١٨ أغسطس عام ٢٠١٨ صدَّق الرئيس السيسي على قانون جرائم تقنية المعلومات، وفي ٢٧ أغسطس من نفس العام تم التصديق على قانون تنظيم وسائل الإعلام، والتي أدت إلى تقنين مراقبة الحياة الإلكترونية وبالتالي تقييد الحريات الرقمية[1]، وبصدور قانون حماية البيانات الشخصية والتصديق عليه في يوليو عام 2020[2] تسعى الحكومة المصرية بخطًى متسارعة إلى فرض سيطرتها على المجال الرقمي وتداول البيانات، وهو الأمر الذي ينبغي أن يتم وفقًا للمعايير الدولية والحقوق الأساسية المنصوص عليها ضمن الدستور وبقية التشريعات المصرية، وذلك للحفاظ على حق الأفراد في التعبير، وكذلك ضمانًا للحقوق والحريات الشخصية، وحتى لا يتم استخدام تلك البيانات بشكل غير قانوني من قِبل السلطات المصرية.

تحاول هذه الورقة بناءً على ذلك تقديم قراءة أوَّلية للقانون المصري المعني بحماية البيانات الشخصية

---

١. مؤسسة حرية الفكر والتعبير، بيان قانوني "مكافحة الجريمة الإلكترونية" وتنظيم الصحافة والإعلام في مصر انتهاك للحق الأساسي في حرية التعبير،٦ سبتمبر ٢٠١٨
https://afteegypt.org/press_releases/2018/09/06/15762-afteegypt.html

٢. الجريدة الرسمية تنشر قانون حماية البيانات الشخصية، المصري اليوم ، ٢٠٢٠/٧/١٧
https://n9.cl/u7ev

ومدى اتساقه مع المعايير الدولية المعنية بذلك. ويأتي ذلك ضمن اهتمام مؤسسة حرية الفكر والتعبير بحماية وتعزيز الحقوق الرقمية في مصر.

يهدف قانون حماية البيانات الشخصية إلى وضع إطار تشريعي يكفل للمستخدم حماية بياناته التي خضعت للمعالجة الإلكترونية، وذلك من خلال الحفاظ على عدة حقوق فرعية، مثل: الحق في معرفة طبيعة البيانات التي يمتلكها الحائز على البيانات والمعالج لها، كما يسمح للمعني بالبيانات بتقديم شكوى ضد مستخدمي البيانات، ومقاضاتهم إذا استدعى الأمر، كما يخاطب القانون الشركات والمؤسسات التي تتعامل مع قواعد البيانات الخاصة بالمستخدمين، ويحدد على أساس ذلك المعايير التي تحكم العلاقة بين المستخدمين والشركات الرقمية، ومن هذا المنطلق نص القانون على إنشاء مركز حماية البيانات الرقمية لتكون مهامه الرقابة على تنفيذ القانون، وإصدار التراخيص والتصاريح والاعتمادات للشركات التي تقوم بمعالجة واستخدام البيانات الشخصية للمستخدمين، وكذلك توجيه الإرشادات اللازمة لتوجيه القانون، وهو ما نراه تطورًا محمودًا يواكب التطور الإلكتروني في الحياة العامة والخاصة، ولكن هل يحافظ القانون على الحريات الرقمية بشكل كامل؟ هذا ما نسعى إلى معرفته من خلال هذه الورقة.

نشرت عدة صحف إلكترونية أن القانون المصري جاء محاكيًا للقوانين العالمية وعلى رأسها اللائحة المنصوص عليها من قبل الاتحاد الأوروبي[٣] "General Data Protection Regulation" مع إضافة تعديلات ومعايير تساهم في تعزيز حماية البيانات الشخصية. وبالاطلاع على مجموعة من المعايير الدولية لإنشاء قانون حماية البيانات الرقمية وكذلك المبادئ التي أشارت إليها مؤسسة أكسس ناو[4] والتي اعتبرتها مقياسًا للدروس السابقة من القوانين المعنية بحماية البيانات الشخصية، يمكن من خلال ذلك قياس مدى فاعلية القانون المصري في حماية بيانات المستخدمين مع حماية الحق في الخصوصية باعتباره حقًّا مرتبطًا بشكل أساسي بالبيانات الشخصية، مع الأخذ في الاعتبار أن تلك الورقة تعتبر بمثابة قراءة أولية للقانون إلى حين صدور اللائحة التنفيذية الخاصة به.

---

٣. اليوم السابع، ضوابط بقانون حماية البيانات الشخصية للتسوق الإلكترونى.. تعرف عليها، نورا فخري ، 16 مارس 2020
shorturl.at/hpzB6

٤. أكسس ناو، دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الأوروبي، ٢٠١٨
https://www.accessnow.org/cms/assets/uploads/2019/01/Updated-version-BOOKlet

أولًا: نظرة على القانون المصري لحماية البيانات الشخصية

يتكون القانون رقم ١٥١ الصادر سنة ٢٠٢٠ من ٤٩ مادة تتوزع على أربعة عشر فصلًا، بالإضافة إلى التصدير الذي يتكون من سبع مواد. يختص الفصل الأول بالتعريفات التي يتأسس عليها القانون، مثل البيانات الشخصية «أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة.. إلخ"، أما البيانات الشخصية الحساسة فهي «البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية، أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية... وتعد بيانات الأطفال من البيانات الشخصية الحساسة».

أما المعالجة فهي «أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها... أو استرجاعها أو تحليلها باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيًا أو كليًا".

ومن خلال بقية الفصول يؤسس القانون الإطار الذي يحدد العلاقة بين المعني بالبيانات من جهة، ومستخدمي البيانات من جهة أخرى، كالحائز والمتحكم والمعالج، وذلك من خلال تفنيد حقوق المعني بالبيانات وشروط جمع ومعالجة البيانات، والتزامات المتحكم والمعالج، وإجراءات إتاحة البيانات الشخصية، وطبيعة استخدام البيانات الشخصية الحساسة، وكذلك البيانات الشخصية عبر الحدود، واستخدام البيانات الشخصية في التسويق الإلكتروني المباشر. كما يؤسس القانون بدايةً من الفصل التاسع ووصولًا إلى الفصل الأخير لإنشاء مركز حماية البيانات الشخصية الذي تتحدد مهامه في الرقابة على إنفاذ قانون حماية البيانات الشخصية وإصدار التراخيص والتصاريح والاعتمادات لمزاولة الشركات، وجمع ومعالجة بيانات المستخدمين، كما يخصص القانون حق الضبطية القضائية لأفراد معينة من المركز، ويحدد كذلك الجرائم والعقوبات في الفصل الأخير من القانون.

ثانيًا: المعايير الدولية خارطة طريق لتشريع قوانين حماية البيانات الشخصية

يلتصق الحق في حماية البيانات الشخصية بالحق في الخصوصية الرقمية وهو «التسليم بحق الأفراد في التمتع بفسحة للتنمية الذاتية تقوم على مبدأي التفاعل والحرية، أو حقهم في مجال خاص يتسع لهم فيه التفاعل أو عدم التفاعل مع الآخرين، دون الخضوع لتدخل الدولة أو تدخل زائد يمارسه أفراد آخرون بلا دعوة»، وذلك وفقًا للتقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان عن الحق في الخصوصية في العصر الرقمي[٥]، يشمل التقرير أيضًا الحياة الإلكترونية للأفراد، مساحة البيانات الشخصية التي تقع تحت بند الخصوصية. وأكد على ذلك الإعلان العالمي لحقوق الإنسان في المادة ١٢[٦] وكذلك العهد الدولي الخاص بالحقوق المدنية والسياسية في المادة[٧] 17.

وأشار التقرير أيضًا إلى التدخلات من قبل الحكومات وكذلك مؤسسات الأعمال التي تقوم بجمع مليارات البيانات الشخصية لمستخدمي المعاملات الإلكترونية، بالإضافة إلى سماسرة المعلومات الذين يتاجرون بالبيانات الشخصية للمستخدمين، الذين يجدون أنفسهم في موقف يستحيل من خلاله تتبع مسار بياناتهم الشخصية والمعلومات المتعلقة بهم وكذلك مسار استخدامها، خاصةً أننا أمام قدرة فائقة لتحليل البيانات، وتدوينها، وتتبع مسار الحياة اليومية للمستخدمين والتفاصيل الخاصة بحياتهم التي قد لا يريدون الإفصاح عنها.

جاء التقرير الخاص بمفوضية الأمم المتحدة لحقوق الإنسان وتعزيز الحقوق المدنية والسياسية بتوضيح أثر التكنولوجيا[٨] في تعزيز حقوق الإنسان وخاصة الحقوق المتعلقة بالمجتمع والاحتجاجات السلمية وألقى الضوء علي ضرورة تقوية المجتمعات الديمقراطية لمبدأ حماية البيانات الشخصية المتعلقة بالأفراد وخاصة ذات التوجه السياسي، حيث تقوم الحكومات الهشة بتتبع الأفراد ذوي النشاط السياسي سواء عن طريق البريد أو الهواتف أو المواقع الخاصة بهم، ومن ثم يؤكد على أهمية ترسيخ حماية البيانات الشخصية داخل القانون وخاصة إذا كان المجتمع يريد الحفاظ على هويته الديمقراطية.

---

٥. التقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان عن الحق في الخصوصية في العصر الرقمي، الدورة التاسعة والثلاثين لمجلس حقوق الإنسان، ٣ أغسطس ٢٠١٨ https://undocs.org/ar/A/HRC/٣٩/٢٩

٦. الإعلان العالمي لحقوق الإنسان،
https://www.un.org/ar/udhrbook/#٢٩

٧. العهد الدولي الخاص بالحقوق المدنية والسياسية،
https://www.nhrc-qa.org/wp-content/uploads/٢٠١٤/٠١/العهد-الدولي-الخاص-بالحقوق-المدنية-والسياسية.pdf

٨. التقرير السنوي بمفوضية الأمم المتحدة السامية، أثر التكنولوجيا الجديدة في تعزيز حقوق الإنسان وحمايتها في سياق التجمعات، بما فيها الاحتجاجات السلمية، ٣ يوليو ٢٠٢٠ https://undocs.org/ar/A/HRC/٤٤/٢٤

بالإضافة إلى ذلك تستند صناعة القوانين الخاصة بحماية البيانات الشخصة إلى المعايير الدولية كأساس ومرجع لها، مثل الاتفاقية ١٠٨، والمبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي، واللائحة العامة لحماية البيانات الخاصة باللائحة الاوروبية «GDPR" والتي أصبحت أخيرًا ضمن المراجع المستند إليها في صياغة قوانين حماية البيانات الشخصية.

تهدف اللائحة العامة لحماية البيانات التي أصدرها البرلمان الأوروبي والمفوضية الأوروبية "GDPR" اختصارًا لـGeneral Data Protection Regulation إلى تقنين عملية استخدام بيانات الأفراد من قبل الشركات الكبرى أو التي تقوم على حيازة أو معالجة بيانات الأفراد، وذلك من خلال وضع الإطار القانوني الذي يؤسس تلك العلاقة ويحميها من الخلل، كما يشرع لوجود سلطة مستقلة تراقب تنفيذ الآليات بشكل سليم وتسعى إلى تطوير حماية بيانات الأفراد وكذلك الحق في الخصوصية، بالتوازي مع حرية حركة البيانات.

تتكون اللائحة العامة لحماية البينات من ٩٩ مادة تتوزع على ١١ فصلًا، تختص بإدراج التعريفات العامة وأحكامها، والمبادئ المتعلقة بعملية المعالجة، وحقوق صاحب البيانات، ونقل البيانات الشخصية إلى دول ثالثة أو منظمات دولية، وتؤسس أيضًا لوجود سلطات مستقلة تقوم بالإشراف على العملية القانونية، وذلك بداية من الفصل السادس حتى الفصل الأخير، مع مراعاة إدراج سبل الانتصاف والمسؤوليات، وكذلك آليات دفع الغرامات في حالة المخالفة القانونية.

تركز اللائحة على الشركات التي تقوم بمعالجة البيانات الشخصية للمستخدمين لأغراض مختلفة، فهي لا تعتبر بالأشخاص، وإنما تسعى إلى تقنين عمل الشركات، وهو الأمر الذي يختلف عن القانون المصري الذي ينطبق على الأفراد فضلًا عن الشركات. ورغم اختلاف الديباجات، يشترك القانون المصري واللائحة الأوروبية في اعتبار الآراء السياسية والصحة النفسية وكذلك بيانات الأطفال ذات درجة أعلى من الخصوصية، يصنفها القانون المصري على أنها بيانات شخصية حساسة، أمَّا اللائحة الأوروبية فتقوم بحظر معالجة أو حفظ مثل هذه المعلومات. كما تؤكد كلتا الجهتين: القانون واللائحة، على عدم استحواذ الشركات على بيانات المستخدمين[٩] بدون موافقة مسبقة من الشخص المعني بالبيانات، وحقه في مراجعة البيانات الشخصية التي تستحوذ عليها الشركات، وكذلك حقه في تعديلها أو إلغاء التعاقد مع تلك الشركات. كما ضمَّت اللائحة وأكدت على بعض الحقوق الفرعية التي تضمن حماية البيانات الشخصية كالحق في الخصوصية، والحق في التعامل مع البيانات الشخصية كمسح البيانات أو تعديلها والحق في النسيان، والحق في المعرفة، والحق في الخصوصية حسب التصميم الافتراضي لها، والحق في إمكانية الحصول على البيانات وإمكانية نقلها.

---

٩. المرجع السابق، Definitions ،
https://gdpr-info.eu/art-4-gdpr/

ثالثًا: القانون المصري تحت مجهر المعايير الدولية

قدمت جمعية أكسس ناو، وهي إحدى الجمعيات التي شاركت في الحوار المدني لإصدار اللائحة الأوروبية دليلًا إرشاديًّا يتضمن المبادئ الأساسية التي يمكن للمشرِّع أن يأخذها بعين الاعتبار في صياغته لقانون يقوم على حماية البيانات الشخصية وتنظيم عملية المعالجة بين الأطراف المختلفة، وذكرت أيضًا ما يجب اجتنابه لعدم الوقوع في الأخطاء ذاتها للتجارب السابقة، ومن تلك المعايير الأساسية:

1- ضمان إجراء مفاوضات شفافة وشاملة لجميع الأطراف

ويقصد بها إشراك مؤسسات المجتمع المدني والشركات الخاصة وجمعيات الدفاع عن المستهلك، وذلك عن طريق إقامة اجتماعات معلنة وشفافة بين جميع تلك الطوائف وإشراكها في الحوار الخاص بصياغة القانون على أن تكون تلك المناقشات خالية من أساليب الضغط بأي شكل من الأشكال، وأن تكون على قدر عالٍ من الشفافية والحيادية، وهذا ما اتبعته دول الاتحاد الأوروبي في صياغة اللائحة الخاصة بحماية البيانات الشخصية.

لكن فيما يخص الخطوات المتخذة لإصدار القانون المصري، فإنه تجاهل تلك النقطة المهمة وتجاهل إشراك فئات مختلفة من المجتمع، إذ بعد تقدم ٦٠ عضوًا من البرلمان بمشروع القرار، أعلن وزير الاتصالات والتكنولوجيا عن موافقة الحكومة على مشروع القرار في ٢٠١٩ ومن ثم تمت موافقة مجلس النواب عليه بشكل نهائي[10]. وبهذا الشكل يُظهِر عدم اعتماد المشِّرع على إشراك مختلف فئات المجتمع في صياغة وإعداد القانوناحتمال وجود خلل في أهداف القانون.

2- تعريف قائمة مبادئ لحماية البيانات تكون ملزمة وتضمينها في الإطار القانوني

حسب هذا المبدأ فلا بد أن يحتوي القانون على مفاهيم واضحة للبيانات الشخصية والبيانات الشخصية الحساسة وأن يشمل الإجراءات المتبعة تجاه البيانات الشخصية أثناء الاتصالات، ما يحافظ على خصوصية تلك الاتصالات وخصوصية البيانات التي يتم تبادلها كذلك، كما أكد هذا المبدأ على ضمان القانون المبادئ الثمانية التي جاءت بها المعايير الدولية واتفاقية ١٠٨ والمبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي[11]، وهي الإنصاف والشرعية، وتحديد الغرض، وتقليص البيانات، والدقة، وتحديد مدة

---

١٠. موقع مصراوي، فكرة عمرها ثلاثة أعوام... تفاصيل قانون حماية البيانات الشخصية، ١٨ يوليو ٢٠٢٠، عبد الله مجدي
https://www.elwatannews.com/news/details/4908354

١١. منظمة التعاون والتنمية في الميدان الاقتصادي، سبتمبر ١٩٨٠، المبادئ التوجيهية التي تحكم حماية الخصوصية والتدفقات عبر الحدود للبيانات الشخصية
https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

الاحتفاظ بالبيانات، وحقوق المستخدمين، مثل: الحق في النفاذ إلى المعلومات والحق في حذفها، والنزاهة والسرية، وأخيرًا التلاؤم في نقل البيانات إلى بلاد أخرى أو إقليم آخر يتمتع بمستوًى كافٍ من الحماية.

نص القانون المصري على تعريفات واضحة للبيانات الشخصية والبيانات الشخصية الحساسة، وكذلك نص على تعريف الحائز للمعلومات والمعالج[12]، وسعى إلى الحفاظ على حق المعني بالبيانات، سواء كان المعالج ممثلًا في فرد أو شركة. وذلك من خلال تجريم استخدام بيانات دون علم صاحبها أو التعنت في تمكين صاحب البيانات من حقه في الاطلاع عليها، ولكن لم يشمل هذا التجريم أجهزة الدولة، ولم يحدد مهام عملها كذلك، وذلك عن طريق استثناء الجهات الأمنية وقواعد البيانات التي يستحوذ عليها البنك المركزي والمؤسسات التابعة له من سريان أحكام القانون عليهم.

3- تحديد الأساس القانوني الذي يسمح بمعالجة البيانات

يلزم هذا المبدأ القانون بأن يحدد أساس قانوني لأي جهة تقوم بمعالجة البيانات أن تمتثل أمام القانون بتنفيذ بنود العقد بموافقة المستخدم، وكذلك في جميع حقوق المستخدم، أي أن تعطي للمستخدم حق سحب الموافقة، وهذا ما كفله القانون في المادة ٢ وهو "الحق في العدول عن الموافقة المسبقة على الاحتفاظ بالبيانات الشخصية أو معالجتها".

4- إدراج قائمة بحقوق المستخدمين الملزمة في القانون

وذلك يضمن للمستخدمين التحكم في بياناتهم وفقًا لحقوق أساسية، يجب على القانون أن يذكرها، وهي الحق في الاعتراض والمحو والتصحيح والحق في تلقي المعلومات والحق في الاستفسار، وقد كفل القانون كل هذه الحقوق ولكن وضع مقابلًا ماديًّا لمزاولة تلك الحقوق باستثناء المعرفة في حالة انتهاك البيانات الشخصية، هذا المقابل لا يتجاوز العشرين ألف جنيه ويتولى مركز حماية البيانات إصدار القرارات المتعلقة بتحديد المقابل المادي واستلامه.

5- تحديد نطاق واضح للتطبيق

نظرًا إلى أن الانتهاكات المتعلقة بالحقوق الرقمية وبحماية البيانات الشخصية هي انتهاكات تتعدى الشكل التقليدي لكثير من الجرائم، والذي يرتبط بوقائع محددة الزمان والمكان، وأغلبها داخل الإقليم الجغرافي الذي تقع عليه سيادة الدولة، لكن الأمر هنا مختلف وتنشأ إشكالية عند صياغة قوانين حماية البيانات الشخصية حول العالم، فهناك من يتجه إلى توسيع نطاق التطبيق، ليشمل أي فرد أو كيان على

---

١٢. البيانات الشخصية وفقًا لما أتى به القانون "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى: الاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية.»

البيانات الحساسة «البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية «البيومترية» أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة.»

أرض الدولة، وكذلك أي كيان في أي مكان آخر في العالم سواء كان منتميًا إلى الدولة، أو كان يعالج بيانات مواطنين لها. ولكن في تلك الحالة، تنشأ مزيد من التعقيدات واحتمالات تضارب القوانين. والتي من المهم أخذها في الاعتبار عند صياغة التشريعات.

وقد أوضح القانون المصري في المادة الثانية منه نطاق تطبيقه ليشمل كل من ارتكب إحدى الجرائم المنصوص عليها متى كان الجاني «من المصريين داخل الجمهورية أو خارجها، أو كان من غير المصريين المقيمين داخل الجمهورية، أو كان من غير المصريين خارج الجمهورية، إذا كان الفعل معاقبًا عليه في الدولة التي وقع فيها تحت أي وصف قانوني وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية».[١٣]

6- إنشاء آليات ملزمة وشفافة لنقل البيانات بشكل آمن إلى بلدان ثالثة

وفقًا للائحة الأوروبية يحظر تداول البيانات الشخصية مع أي دولة ثالثة لا تتمتع بقرار الكفاية وهو قرار تصدره المفوضية الأوروبية، يشير إلى أن الدولة التي تمتلك قرار الكفاية، لديها القدر الكافي من الحماية طبقًا لقانونها الداخلي أو وفقًا لالتزاماتها الدولية، وتمتلك المفوضية الأوروبية السلطة لإعطاء إلى دولة ثالثة قرار الكفاية من عدمه وتسعى العديد من الدول إلى الحصول على هذا القرار، ويشمل هذا المبدأ عدم تداول المعلومات الشخصية عبر الوكالات الفضائية أو غيرها مع دول ثالثة إن لم تكن تتمتع بقرار الكفاية، ولا بد أن يذكر القانون الإجراءات التي يتم بها نقل المعلومات إلى تلك الدول.

حذر القانون من نقل البيانات عبر الحدود سواء عن طريق الجمع أو التخزين أو المعالجة أو المشاركة مع دولة أجنبية لا تتمتع بمستوًى من الحماية يقل عن المستوى المنصوص عليه في القانون وذلك بترخيص من مركز حماية البيانات، وترك أمر تحديد السياسات والمعايير والإجراءات والقواعد إلى اللائحة التنفيذية، ولكنه لم يذكر أمرًا يشبه قرار الكفاية.

7- حماية أمن المعلومات ونزاهة عملية المعالجة

يضمن القانون ثقة المستخدمين من خلال وجود قدر كبير من المسؤولية القانونية التي تتعرض لها الجهات المسؤولة عن جمع وتعديل ومعالجة البيانات، فقد نص القانون على العديد من أشكال العقوبات في حالة حدوث أي تجاوز من قبل تلك الجهات أو الأشخاص المعنية بذلك، كما يضمن القانون حماية بيانات المستخدمين بما لا يعرضهم لأي شكل من أشكال الخطر.

ذكر القانون أنه في حالة إثبات جرائم تتعلق بمخالفة أحكام القانون من قبل العاملين بمركز حماية البيانات أن يصدر قرار عن وزير العدل بناءً على اقتراح الوزير المخول له صفة الضبطية القضائية.

---

١٣. المادة ٢ من قانون حماية البيانات الشخصية، ١٥١ لعام ٢٠٢٠.

لكن لم يتناول القانون حالات وضع التظاهر السلمي في ظل التكنولوجيا والمراقبة الإلكترونية، فلم يتطرق القانون إلى حماية البيانات الشخصية لمن يملكون آراء سياسية معارضة أو لديهم مواقف سياسية سابقة، ولم يتطرق إلى حالات التظاهر السلمي وحماية بيانات المتظاهرين من حالات المراقبة الجماعية وحمايتهم هم. رغم إدراج الآراء السياسية ضمن البيانات الحساسة فاستثناء الجهات الأمنية من القانون يعد ثغرة كبيرة تنقض من قيمة البيانات الحساسة.

8- تطوير آليات منع انتهاك البيانات والإبلاغ عنها

يحث هذا المبدأ روح التطوير المستمر تجاه الآليات التي تحمي البيانات وتمنع الانتهاك، وذلك بمواكبة التطورات التكنولوجية والاستعانة بالخبراء في مجال الاتصالات والبيانات والتكنولوجيا لتطوير آليات العمل في المجال الإلكتروني.

وضع القانون في بدايته تعريفًا بخرق البيانات الشخصية وانتهاك المعلومات[14]وأعطى للشخص المعني بالبيانات حق المعرفة في حالة وجود أي اختراق أوانتهاك لبياناته، كما أعطاه الحق في اللجوء إلى القضاء في حالة انتهاك حق حماية بياناته، كما ألزم المعالج أو المتحكم في البيانات بضرورة إخطار المركز خلال ٧٢ ساعة في حالة حدوث خرق أو انتهاك للبيانات الشخصية، ويتم التبليغ فورًا إذا كانت البيانات تمس الأمن القومي، وعلى المركز خلال ٧٢ ساعة من تاريخ علمه أن يقوم بوصف طبيعة وصورة أسباب الانتهاك وتحديد الآثار المحتمل حدوثها نتيجة لهذا، ووصف الإجراءات التي يجب اتخاذها، وعلى المركز إخطار الشخص المعني بالبيانات بتلك الحادثة خلال ٧٢ ساعة من تاريخ الإبلاغ.

وترك القانون الأمر للائحة التنفيذية فيما يتعلق بتحديد الإجراءات الخاصة بالإبلاغ والإخطار، ولكنه لم يذكر على وجه التحديد أي نوع من التطورات التكنولوجية التي يجب الاستعداد لها لتطوير آليات مواجهة الانتهاك والاختراق.

9- إنشاء سلطة مستقلة وإنشاء آليات قوية لإنفاذ القانون

أكد هذا المبدأ على ضرورة وجود سلطة مستقلة تشرف على تطبيق القانون وتنفيذه بشكل حتمي وصارم وتطبيق الغرامات على الشركات، خاصة المتوسطة والصغيرة التي قد لا تلتزم بشكل كافٍ أثناء معالجة البيانات الشخصية بما أتى به القانون والمعايير الدولية.

نص القانون على إنشاء مركز حماية البيانات والذي بموجب القانون له الحق في وضع السياسات والخطط الإستراتيجية والبرامج المعنية بحماية البيانات وتنفيذها، وله الحق في وضع التدابير وتحديد الإجراءات والتنسيق والتعاون مع الأجهزة الحكومية وغير الحكومية والجهات والمبادرات ذات الصلة، وإصدار

---

١٤. تعريف خرق وانتهاك البيانات الشخصية وفقًا لما جاء في القانون: "كل دخـول غير مرخـص بـه إلى بيـانات شخصية أو وصول غير مشروع لها، أو أي عملية غير مشروعة لنسخ أو إرسال أو توزيع أو تبادل أو نقل أو تداول يهدف إلى الكشف أو الإفصاح عن البيانات الشخصية أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها.»

التراخيص والتصاريح والاعتمادات، وتلقي الشكاوى والبلاغات، والحق في إبداء الرأي في مشروعات القوانين والاتفاقيات الدولية التي تنظم العمل على تطوير حماية البيانات الشخصية، والرقابة على اتخاذ الإجراءات التي نص عليها القانون والتحقق من شروط حركة البيانات عبر الحدود واتخاذ القرارات المتعلقة بذلك.

يتكون مجلس الإدارة من ١٠ أفراد، وهم ممثل عن وزارة الدفاع، وممثل عن وزارة الداخلية، وممثل عن جهاز المخابرات العامة، وممثل عن هيئة الرقابة الإدارية، وممثل عن هيئة تنمية صناعة تكنولوجيا المعلومات، وممثل عن الجهاز القومي لتنظيم الاتصالات، والرئيس التنفيذي للمركز، وثلاثة من ذوي الخبرة. ولا يمكن إغفال الطابع النظامي لمجلس الإدارة حيث يتم تعيين سبعة من الأعضاء الذين ينتمون إلى جهات حكومية، فضلًا عن احتواء المجلس على ثلاثة ممثلين عن جهات أمنية، وهي نفس الجهات المستثناة من تنفيذ القانون عليها، وهو ما يعطيهم الأحقية في الاستحواذ على قواعد البيانات دون رقابة أو تقييد قانوني.

كما وضع المشرِّع جهات الأمن كوجهة أساسية في عمليات معالجة البيانات وحدوث أي اختراق وجعلها مرجعية يتحرك إليها المركز، كما ألزم القانون الشخص المعالج أو المتحكم في البيانات بالإبلاغ الفوري لجهات الأمن خلال ٢٤ ساعة.

وبذلك يفقد مركز حماية البيانات استقلاله عن طريق انتمائه شبه الكامل إلى جهات حكومية وغياب أي ممثلين عن المجتمع المدني، فضلًا عن الصلاحيات المفتوحة للأجهزة الأمنية.

10- مواصلة حماية البيانات والخصوصية

هناك توجه عالمي في النص على حماية الحق في الخصوصية في الدساتير الدولية، سواء بأحد المعاني الكلاسيكية لها، والتي يضمها الدستور المصري في المادة ٥٧، إذ ينص على حماية وصيانة الحياة الخاصة. أو بالمعاني الأحدث لها، والتي تضم في النص بشكل واضح، الأمان والخصوصية الرقمية، والبيانات الشخصية.

يأتي إصدار قانون حماية البيانات الشخصية خطوةً مهمة في هذا الإطار، غير أن عدم استقلال المركز القائم على إنفاذ القانون، واستثناء الجهات الأمنية من القانون، يعرقل من تطبيق حقوق المواطنين في الخصوصية والأمان الرقمي.

رابعًا: موقف القانون من قاعدة البيانات التي تحتفظ بها شركات الاتصالات والممارسات المنافية لحماية البيانات الشخصية والحق في الخصوصية

نشرت مؤسسة حرية الفكر والتعبير إصدارًا بعنوان: "سياسات الخصوصية لشركات الاتصال"[15] تناولت فيه وضع شركات الاتصالات الأربع، وكيفية استحواذها على قاعدة عملاقة من البيانات للعملاء مستخدمي الخدمة، وذلك منذ لحظة التعاقد وإمداد الشركة بنسخة من الرقم القومي.

كما أوضح التقرير أن شركة WE الشركة المصرية للاتصالات لم تصرح حتى الآن عن أية معلومات فيما يخص سياسة الخصوصية الخاصة بها، بالإضافة إلى مشاركة الشركات الأربع البيانات الخاصة بالمستخدمين مع أطراف ثالثة سواء كانت جهات إنفاذ القانون أو جهات ذات أغراض تسويقية، ولم تصرح الشركة عن وجود أية التزامات أو آليات لديها لإدارة قواعد البيانات الضخمة التي تستحوذ عليها، بالاضافة إلى إجبار كلٍّ من الشركة المصرية للاتصالات وشركة أورانج مستخدميها على الموافقة على بعض القواعد التي من شأنها أن تحد من حرية التعبير وحرية الوصول إلى المعلومات.

هناك العديد من الممارسات التي تبيح اختراق البيانات الشخصية، منها حوادث تفتيش أجهزة المحمول الخاص بالمواطنين في الميادين الرئيسية من قِبل رجال الأمن خاصة في عقب المظاهرات المعارضة في سبتمبر ٢٠١٩، بالإضافة إلى تسريب البيانات الخاصة بالناجيات[16] من حادثة اعتداءات جماعية واغتصابات جماعية في ميدان التحرير بتاريخ ٣ و٨ يونيو ٢٠١٤ أثناء حلف الرئيس السيسي اليمين، حيث نشرت قناة أون تي في وجريدة اليوم السابع بيانات الناجيات الشخصية وصورهن، ما يعد انتهاكًا صريحًا واعتداءً صارخًا على حقوق الناجيات في الخصوصية وحماية بياناتهن الشخصية مما يعرضهن للخطر والتهديد.

أيضًا ما قام به القائمون على برنامج صبايا الخير الذي تقدمه «ريهام سعيد» حين استضافت الناجية من حادثة المول، وبعد سرد الناجية لأحداث الاعتداء ورفضها التصريح عن هويتها، استباح فريق إعداد البرنامج بعد الحلقة الكشف عن هويتها، وعَرَض صورها وتفاصيل حياتها الشخصية[17]وهو الأمر الذي سبب حالة من الاستياء على مواقع التواصل الاجتماعي، ونتيجة للضغط على البرنامج من خلال وسائل التواصل الاجتماعي، وذلك بتفعيل العديد من الحملات الإلكترونية لوقف البرنامج، استجابت إدارة قناة

---

١٥. سياسة الخصوصية لشركات الاتصالات في مصر، مؤسسة حرية الفكر والتعبير، ٣٠ ديسمبر ٢٠١٨ https://afteegypt.org/digital_freedoms/publications_digital_freedoms/2018/12/10/16365-afteegypt.html

١٦. تسريب البيانات الشخصية للناجيات اعتداء صارخ على خصوصيتهم واستهتار بسلامتهن، مركز القاهرة لدراسات حقوق الإنسان، 26 يونيو 2016 https://n9.cl/1emh

١٧. ما بين انتهاك الخصوصية وحرية الإعلام، مؤسسة حرية الفكر والتعبير، ٢ نوفمبر ٢٠١٥ https://n9.cl/dnhc3

النهار، وقامت بتعليق برنامج صبايا الخير وفتح تحقيق فيما نسب إلى البرنامج من اتهامات، وقامت القناة بحذف الفيديو المنتشر عن الناجية على موقع اليوتيوب.

الخاتمة والتوصيات

يمثل صدور قانون حماية البيانات الشخصية محاولة من السلطات لمواكبة الأحداث، ومحاولة لحماية الحق في الخصوصية باعتباره حقًّا متداخلًا مع حماية البيانات الشخصية، وإن كان يتضمن أوجه قصور تتمثل في غياب النقاش المجتمعي والشفافية في إصدار القانون، وعدم استقلال المركز القائم على تنفيذ القانون.. فلا يزال من الممكن معالجة القصور مع صدور اللائحة التنفيذية، ونأمل أن تكون السلطات على قدر كبير من الوعي بالتطورات التي تحدث في العالم الإلكتروني وأن تكون علي قدر عالٍ من الاستجابة له بشكل يحمي ويعزز حقوق الإنسان الرقمية والمادية فيوقت واحد، بدلًا من انتهاكها أو السماح بذلك.

وفي حالة عدم إمكانية ذلك عن طريق اللائحة التنفيذية فإن هناك حاجة إلى تعديل بعض نصوص القانون، مثل ضرورة النص على الإعفاء المادي من مزاولة الحقوق الأساسية المرتبطة بحماية البيانات، فلا يلزم أن يدفع المستخدمون مالًا مقابل ممارسة حقهم في معرفة البيانات التي تستخدمها الجهات القائمة على معالجة البيانات وجمعها، وأن تخفف كذلك من سلطوية أجهزة الدولة على التحكم في آليات قواعد البيانات والسيطرة عليها، وخلق سلطة مختصة بالرقابة تتميز بالاستقلالية والشفافية، وأن يكون هناك مساحة أوسع لإشراك فئات متنوعة في صياغة اللائحة التنفيذية ما دامت الفرصة لم تُتح في صياغة القانون، كما نأمل أن تفسر اللائحة مصطلح «حرمة الحياة الخاصة» التي ذكرها القانون، دون التطرق إلى تفاصيل تحاول تفسير ذلك المصطلح، حتى لا نجد أنفسنا أمام مصطلحات مبهمة يمكن تأويلها وتفسيرها بأكثر من معنى.