استباحة الحياة الخاصة باسم القانون،

قانون مكافحة جرائم المعلومات واستباحة خصوصية مستخدمي الاتصالات والإنترنت

ANHRI

استباحة الحياة الخاصة باسم القانون،
قانون مكافحة جرائم المعلومات واستباحة خصوصية مستخدمي الاتصالات والإنترنت

تقديم

تأسست مفاهيم الحريات والحقوق الفردية تاريخيا في مواجهة تغول الدول على حقوق وحريات مواطنيها، ونشأ مفهوم المواطن صاحب الحقوق اللصيقة بذاته، تاريخيا بعد صراع طويل لتقليص الصلاحيات غير المحدودة للدولة.

ومنذ البدء كانت المساحة الشخصية التي تحدها جدران منزل كل إنسان، وتمتد بصفة خاصة إلى تواصله الشخصي مع الآخرين هي موضع اهتمام التشريعات المختلفة التي سعت إلى حماية المواطنين من التدخل في حياتهم الشخصية. وقد تعرضت هذه التشريعات إلى الإضافة والتعديل طيلة الوقت حيث طرأت على تكنولوجيات حفظ البيانات الشخصية والتواصل بين الأفراد تطورات هائلة، صاحبها دائما قدر أكبر من مخاطر تعرض هذه البيانات والاتصالات للتدخل من أطراف خارجية، تأتي أجهزة الدولة في مقدمتها.

وفي ظل التطور الكبير لوسائل الاتصالات الإلكترونية وبصفة خاصة شبكة الإنترنت وتطبيقاتها المختلفة التي لم يعد استخدامها مقصورا على أجهزة الكمبيوتر الشخصية بل توسعت لتشمل الهواتف الذكية التي تجعل كل منا على اتصال مستمر بالشبكة، وتتيح لنا أن نحفظ أغلب بياناتنا بشكل إلكتروني وأن نتبادل مثل هذه البيانات مع أشخاص وجهات مختلفة طيلة الوقت؛ تظهر الحاجة إلى حماية خصوصية كل منا من تعرض هذا القدر من البيانات والاتصالات للتدخل من آخرين، قد يستخدمونها لإلحاق الأذى بنا بطريقة أو أخرى. في المقابل فإن الأجهزة الأمنية في الدولة قد تحتاج في ظروف خاصة إلى الاطلاع على بيانات ومراسلات شخصية لجمع أدلة وقرائن تساعد على إدانة مرتكبي الجرائم المختلفة أو كشف مخططات لأعمال إجرامية تستهدف الأمن القومي وبصفة خاصة الجرائم الإرهابية. ومن ثم فإن أي تشريع يحمي خصوصية حفظ البيانات والمراسلات الخاصة ينبغي أن يأخذ في الاعتبار الحالات التي يمكن لأجهزة الأمن فيها النفاذ إلى هذه البيانات والمراسلات، والضمانات التي تحول دون أن يمثل ذلك إباحة عامة وغير مقيدة لكافة البيانات والاتصالات الشخصية للمواطنين، مما يعرض أمنهم وسلامتهم للخطر ،أن تكون هذه الحالات مقيدة حصرا وتحت رقابة وبأوامر قضائية.

هذه الورقة:

تستعرض هذه الورقة باختصار مواد القانون رقم 175 لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، ذات الصلة بحماية بيانات واتصالات المواطنين وصلاحيات الأجهزة الأمنية وتحديدا ما أسماه القانون أجهزة الأمن القومي، في النفاذ إلى هذه البيانات والاتصالات والاطلاع عليها.

وتهدف الورقة إلى:

1- إطلاع المواطنين على مدى الحماية القانونية المتوافرة لبياناتهم الشخصية في ظل هذا القانون،

2- إلى بيان مدى تحقيق القانون للتوازن المطلوب بين متطلبات المصلحة العامة والأمن القومي وبين حماية حق الأفراد في الخصوصية وما يستتبعه من حماية أمنهم وسلامتهم.

الإطار الحقوقي والدستوري

ينص الإعلان العالمي لحقوق الإنسان على أن لكل فرد الحق في الحياة والحرية وفي الأمان على شخصه، وأنه لا يجوز تعريض أحد لتدخل تعسفي في الحياة الخاصة، أو في الشؤون الأسرية، أو في المسكن، أو في المراسلات. وليس ذلك فحسب بل أعطى الإعلان العالمي لحقوق الإنسان الحق في وجود قوانين تحمي البشر من تلك التدخلات، وأقر بحق وجود نظام اجتماعي ودولي يحقق الحقوق والحريات المنصوص عليها في ذلك الإعلان.

كما أن العهد الدولي الخاص بالحقوق المدنية والسياسية والذي يعمل به في مصر كقانون داخلي منذ العام 1981 ، قد أقرفي المادة 17 منه ، بعدم جواز التعرض لأي شخص بالتدخل في خصوصياته، أو شؤون أسرته، أو بيته، أو مراسلاته، وكذلك أن لكل شخص الحق في الحماية القانونية من مثل هذا التعرض.

حيث جاء في المادة 17 نصا:

" 1. لا يحوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.

2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس."

أما الدستور المصري فقد نص على حرمة الحياة الخاصة، وحرمة المراسلات البريدية والبرقية والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال، وحرم مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة ، في المادتين 57 ، 58 منه.

كذلك تحدث الدستور عن أن الحياة الآمنة حق لكل إنسان، وأن الدولة ملزمة بتوفير الأمن والطمأنينة لمواطنيها، ولكل مقيم على أراضيها.

القانون 175 والخصوصية

أولا: تعريض خصوصية المواطنين للخطر بصفة عامة

ينصالقانون رقم 175لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، في مادة (2)على أن "يلتزم مقدمو الخدمة" أي الشركات مقدمة خدمات الاتصالات والإنترنت بعدة أمور منها:

1 - حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة مائة وثمانون يومًا متصلة. وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي:

(أ) البيانات التي تمكن من التعرف على مستخدم الخدمة.

(ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل، متىكانت تحت سيطرة مقدم الخدمة.

(جـ) البيانات المتعلقة بحركة الاتصال.

(د) البيانات المتعلقة بالأجهزة الطرفية للاتصال.

(هـ) أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

تعرض هذه المادة خصوصية المواطنين للانتهاك لعدة أسباب:

1. تلزم مقدمي الخدمة بالاحتفاظ ببيانات تتخطى ما تحتاجه في إتمام عملها بشكل كفؤ، علما بأن هذه البيانات لا تخص مقدمي الخدمة وليست مملوكة لها بأي شكل، وإنما هي خاصة بمستخدمي الخدمة ومملوكة لهم بشكل كامل.
2. تلزم مقدمي الخدمة بالاحتفاظ بهذه البيانات لمدة طويلة، وكلما طالت هذه المدة، كانت هذه البيانات عرضة لأن يصل إليها من لا يحق له الاطلاع عليها،أو التعامل معها بشكل تجاري أو خارج القانوني مما ينتهك خصوصية المواطنين ، وبشكل يصعب معه تحديد المنتك، سواء كان من القائمين على النظام المعلوماتي التابع لمقدم الخدمة، أو كان من خارجه وتمكن من اختراقه بأية وسيلة.
3. تسمح لجهة إدارية غير تشريعية أو قضائية بتحديد أنواع إضافية غير معلومة وغير محددة ودون ضوابط، من البيانات التي تلزم مقدمي الخدمة بالاحتفاظ بها، وفي هذا إخلال جسيم بحق مستخدم أي خدمة من معرفة البيانات الخاصة به والتي سيحتفظ بها مقدم الخدمة، مقدما وعلى وجه التفصيل.

ثانيا: الصلاحيات الممنوحة لأجهزة الأمن القومي

على الرغم من أن القانون ألزم الشركات مقدمة الخدمة بالحفاظ على سرية تلك البيانات التي تم حفظها وتخزينها، وألزمهم بعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، إلا أن ذات القانون جعل لأجهزة "الأمن القومي" التي عرفها وحددهما القانون بأنها رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية؛ الحق في الاستفادة من ذلك القرار القضائي المسبب فأصبح من حقهم الآتي:

- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه.
- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط.
- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني.

ويعيب مواد القانون فيما يخص هذه الصلاحيات عدة أمور أساسية:

1. عدم الاتساق، فبعض المواد تلزم أن يكون النفاذ إلى البيانات بأمر قضائي، والبعض يمنح صلاحية تقديرية لجهة تحقيق لم يعرفها، والآخر يمنح صلاحيات لأجهزة الأمن القومي نفسها دون اشتراطات الحصول على أمر قضائي أو من جهة تحقيق.
2. لم يبين القانون أية ضوابط فيما يتعلق أولا، الأسباب والظروف التي يمكن في ظلها إصدار أمر قضائي بالنفاذ إلى بيانات مستخدمي نظام معلوماتي، ثانيا، ماهية البيانات التي يمكن أن يشملها مثل هذا الأمر القضائي، في المطلق أو فيما يتعلق بالحالة التي يُسمح فيها بالنفاذ إليها.
3. منح القانون جهة مجهولة الحق في التظلم من الأمر القضائي، مع أنه لم يلزم بإخطار صاحب الشأن (المستخدم) بصدور الأمر القضائي، ولم يحدد فترة زمنية تسمح بالتظلم من الأمر قبل تنفيذه فعليا، كما لم ينص القانون على أية سبل لجبر الضرر أو التعويض في حال كانت أسباب طلب النفاذ إلى البيانات غير كافية أو غير صحيحة، وترتب عليها الإضرار بمصالح صاحبها أو غيره أو سلامتهم بأي شكل.
4. الأخطر هو أن المواد المذكورة تسمح لأجهزة الأمن القومي بالنفاذ إلى كامل البيانات الموجودة على النظام المعلوماتي ولا تقصرها أصلا على تلك الخاصة بمستخدم أو مستخدمين بعينهم يتعلق بهم الأمر

القضائي (حين تشترط الحصول عليه)، وبالتالي فإن بيانات جميع مستخدمي النظام المعلومات تصبح مباحة دون أي مبرر أو مسوغ قانوني ودون أية ضوابط.

ثالثا: ترهيب مقدمي الخدمة

وضع القانون مسئولية جنائية على عاتق مقدمي الخدمة،فإذا امتنع أي منها عن تنفيذ القرار الصادر بتسليم ما لديها من بيانات أو معلومات أو ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه لأجهزة الأمن القومي،أو لم تسمح لأجهزة الأمن القومي بالبحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية،تعاقب الجهة مقدمة الخدمة بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرين ألف جنيه، ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين.

خاتمة وتوصيات

يضرب القانون 175 لسنة 2018، عرض الحائط بالضمانات الدستورية والحقوقية للخصوية وحرمة الحياة الخاصة، حيث أنه عمليا يجعل البيانات الإلكترونية لمستخدمي خدمات الاتصالات الإنترنت مستباحة بشكل كامل لأجهزة الأمن القومي على تعددها ، دون رقابة قضائية واضحة أو ضوابط ودون سبل حقيقية للتظلم لتجنب الضرر الناتج عن تلك الاستباحة أو جبره والتعويض عليه حال وقوعه.

ومن ثم فان هذه الورقة توصي بتعديل القانون 175 لسنة 2018 بحيث تلتزم مواده بشكل كامل بنص الدستور وكذلك بالمواد ذات الصلة من مواثيق وعهود حقوق الإنسان الدولية التي صدقت عليها مصر وأصبحت ملزمة لها، وينبغي بصفة خاصة أن تشمل هذه التعديلات ما يلي:

1. عدم إلزام مقدمي الخدمة أو السماح لهم بالاحتفاظ لأي فترة ببيانات تتخطى تلك المطلوبة لأداء وظيفتها وللفترة الضرورية لأداء تلك الوظيفة. حيث ينبغي أن ينص القانون صراحة على ماهية تلك البيانات وعلى قصر ضرورة إفصاح مقدم الخدمة عنها لجهات قضائية حصرا ، و لمستخدميه مع ترتيب عقوبات حال احتفاظ مقدم الخدمة ببيانات تتخطى تلك التي حصل على موافقة مستخدميه على الاحتفاظ بها.
2. في حال حاجة التحريات والتحقيقات في جريمة بعينها إلى النفاذ إلى بيانات مستخدم لخدمات الاتصالات والإنترنت، أو الاحتفاظ بها لفترة معينة، فإن ذلك لابد من أن يتم من خلال التقدم إلى جهة قضائية مستقلة، وينبغي أن ينص القانون على ضوابط هذا الطلب، والذي لابد أن تشمل بين أمور أخرى النص صراحة على الشخص/الأشخاص المطلوب النفاذ إلى بياناتهم، ومبررات ذلك، والبيانات المطلوب النفاذ إليها على وجه التحديد مع بيان مبرر الحاجة إليها، وإذا كان الطلب بالاحتفاظ بالبيانات لفترة (وهو مماثل لوضع شخص تحت المراقبة) لزم تحديد هذه المدة وبيان مبررها.
3. لا ينبغي أن ينص القانون على إلزام مقدمي الخدمة بمنح أية جهة حكومية أو غير حكومية نفاذا كاملا إلى أنظمتها المعلوماتية، تحت أي ظرف، وإنما يقتصر ذلك على بيانات يحددها أمر قضائي مسبب وعن فترة محددة .