الحق في الخصوصية الرقمية في مواجهة مقتضيات حماية الأمن الوطني

خالد خليف / طالب دكتوراه / القانون الدولي العام
جامعة باجي مختار عنابة

الحق في الخصوصية الرقمية في مواجهة مقتضيات حماية الأمن الوطني

خالد خليف / طالب دكتوراه / القانون الدولي العام
جامعة باجي مختار-عنابة

ملخص:

يتم رصد عديد صور انتهاك الحق في الخصوصية بمقتضى حماية الأمن الوطني تصل لدرجة التجسس الإلكتروني على الحياة الخاصة وافشاء البيانات الرقمية و التسلل لخصوصيات الأفراد، برغم أنه يفترض الاستناد الى شروط والتقيد بإجراءات من قبل الحكومات و الدول في ممارسة حقها في حماية الأمن الوطني أمام حق الأفراد في حماية خصوصياتهم مثل تشريع قوانين ذات مواصفات محددة لهذا الغرض ، والحصول على أذون قضائية في عمليات التجسس الالكتروني وكذا مراعاة قواعد حقوق الانسان ذات الشأن.

الكلمات المفتاحية:

الخصوصية الرقمية، الأمن الوطني، حقوق الانسان

Abstract:

Numerous forms of violation of the right to privacy are monitored under the protection of national security, amounting to electronic espionage on private life, disclosure of digital data, and infiltration of individual privacy. Although it is assumed to be based on conditions and adherence to procedures by governments and countries in exercising their right to protect national security against the right of individuals to protecting their privacy, such as enacting laws with specific stipulations for this purpose, obtaining judicial permits in electronic espionage operations, as well as observing relevant human rights rules.

The key words:

Digital privacy, national security, human rights

مقدمة

بالنظر للتطور الرهيب للجريمة الالكترونية في العالم تسعى الدول والحكومات لتأمين أمنها القومي عبر سن وتشريع قوانين تنظم وتراقب حدود استعمال التكنولوجيات الرقمية في صورته الشخصية أو المؤسساتية مع اصدار آليات وبرامج تهدف أساسا لردع الجريمة الالكترونية بشتى أشكالها، وبالتالي ستكون هذه الحكومات والدول في مواجهة نقيضين متضادين، فهي تصبوا لتأمين وحماية أمنها الوطني من كل أشكال الاجرام الداخلي والخارجي الالكتروني من جهة، كما أنها تسعى لإحترام وضمان حقوق الأفراد في التمتع بخصوصيتهم الرقمية من جهة أخرى، غير أن هذا لا ينفي ما تبرره الحكومات والدول في وضع برامج الرقابة على الحياة الرقمية والتعرض لخصوصية الأفراد وانتهاكها بأسباب ترتبط بعنوان عريض هو حماية الأمن القومي، ومن أكثر صور انتهاك الحق في الخصوصية المرتبطة بحماية الأمن الوطني تلك التي تتعلق بمراقبة وتعقب اتصالات الأفراد وتسجيلها بلا إذن منه أو بلا علمه وتقفي أثر تحركاته عبر الأنترنت ووسائل التواصل وتسجيل ذلك رقميا، ما يمكن من الاطلاع على أسراره الخاصة وإفشائها بلا مسوغ أو دون أمر من سلطة مختصة قضائية او إدارية. كما يوجد نوع أخر يتمثل في الاختراق ويأخذ معنى العدوان على الحق في الخصوصية عبر استنساخ وتدمير الأجهزة الخاصة بالاتصال او تخزين المعلومات او استرجاعها او تحوير مضمونها او تغييره بلا إذن.

بقي الجدل قائما حول تحقيق معادلة عادلة تحفظ للفرد التمتع بالحق في الخصوصية وتسمح للحكومات بممارسة حق حماية الأمن الوطني من الأخطار المفترضة، وعليه ظهر اتجاه يرى أن الرقابة الالكترونية التي تكون محددة الهدف للاتصالات الرقمية هي تدبير ضروري وفعال لأجهزة الأمن وهيئات إنفاذ القوانين في أي دولة لحماية أمنها الوطني بغض النظر عن موقف القانون الدولي والمحلي تحت مبرر أن تكنولوجيات الاتصالات الرقمية يمكن استغلالها لأهداف إجرامية تمس بالأمن الوطني وبالتالي فان المراقبة لسبب يرتبط بالأمن القومي أو لمنع الإرهاب أو غيره من الجرائم تشكل «هدفاً مشروعاً» حتى لو كان الحق في الخصوصية الرقمية للأفراد عرضة للانتهاك.

بينما يرى اتجاه أخر ان الرقابة الالكترونية تحت بند حماية الأمن الوطني له معنى فضفاض قد يتخذ أشكالا منافية للحق في الخصوصية في ضوء القانون الدولي و الوطني كما انها قد تأخذ طابعا تعسفيا وتشكل انتهاكا صارخا لحق الأفراد في الخصوصية بكل أنواعها خاصة الالكترونية. وهو ما يحتم علينا طرح التساؤل التالي: ماهي أشكال انتهاك الحق في الخصوصية في ظل سعي الحكومات حماية أمن أوطانها؟ وماهي الشروط الواجب التقيد بها لحماية الحق في الخصوصية في مقابل واجب الدولة في

حماية أمنها الوطني؟

وعليه سنحاول الإجابة عما سبق طرحه من خلال مطلب أول نستعرض فيه صور انتهاك الحق في الخصوصية بمقتضى حماية الأمن الوطني ثم نستعرض الشروط الواجب الاستناد اليها في تقييد واجب الحكومات في حماية الأمن الوطني أمام حق الأفراد في حماية خصوصياتهم في مطلب ثان.

المطلب الأول: صور انتهاك الحق في الخصوصية باسم الأمن الوطني

يأخذ انتهاك الحق في الخصوصية طرقا عديدة وأشكالا متنوعة تحت مسمى مقتضيات حماية الأمن الوطني يمكن أن نوجزها فيمايلي:

أولا: جمع وتخزين بيانات شخصية صحيحة على نحو غير مشروع

إذ يحدث أن تقود الجهات الأمنية حملة بحث عن مشتبه فيهم افتراضيين دون الرجوع الى سلطة قضائية لمنحها الإذن في مباشرة ترصد وتعقب الأفراد وبالتالي يكون أمام فعل واضح لإنتهاك الحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة عنهم، لكن على نحو غير مشروع وغير قانوني، ويستمد هذا الجمع أو التخزين صفته فجوة غير المشروعة.

ومن بين تلك الأساليب ما يلي:

مراقبة أو اعتراض والتقاط وتفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني.

توصيل أسلاك بطريقة خفية إلى الحاسب الآلي الذي تخزن داخله البيانات المطلوب الاستيلاء عليها.

ثانيا: التجسس الإلكتروني على الحياة الخاصة

وذلك باستعمال التقريب والمقابلة بين المعلومات واستعمال برامج الإحصائيات وإدماج البيانات في نطاق امني مشترك ثم ربطها ببعضها البعض ومنه الحصول على ترجمة فورية لحياة الفرد مثل الحصول على رقم رصيده البنكي عمولاته وتواريخ تذاكر سفره رقم التامين الاجتماعي الخاص مع إمكانية وقوع هذه المعلومات في ايدي غير مختصة او مرتبطة بأجهزة الأمن لانه في بعض الأحيان تستعمل هذ الأجهزة عملاء مدنيين او مؤقتين او الاستعانة بشركات امنية خاصة.

وتزداد الأمور تعقيدا عندما يتم التطفل على البريد الالكتروني من الجهات الرسمية بداع التصدي لقضايا حماية الأمن الوطني أو الحفاظ على النظام العام، وعلى سبيل المثال نجد أنه صدر قانون التنصت الأمريكي الذي يسمح لوكالة الاستخبارات الأمريكية بمراقبة المكالمات الهاتفية فيه والبريد الالكتروني الخاص بالأجانب وبالمقيمين في الولايات المتحدة الامريكية دون إذن قضائي ويمنح السلطات الأمريكية حق التجسس على كل المكالمات.

ثالثا: الإفشاء غير المشروع للبيانات وإساءة استعمالها

إن الطرق والأساليب التي تستخدمها أجهزة الامن الحكومية تعتمد في غالبها على نشر البيانات المحصل عليها رقميا على أوسع نطاق مما يجعل هذه الأجهزة تقع تحت طائلة إفشاء غير المشروع لبيانات رقمية لعديد الأفراد ومن المتصور في هذه الحالة أن يتم الجمع والتخزين والمعالجة لبيانات شخصية بصورة مشروعة ولكن على العكس من ذلك يتم إفشائها من قبل القائمين على حفظها بصورة غير مشروعة أو قد يساء استخدامها من قبلهم بشكل أو بآخر.

رابعا: عدم الإلتزام بالقواعد الاجرائية في عملية جمع ومعالجة ونشر البيانات الشخصية

فقد تضطر الحكومات إلى الاستعانة بقطاعات أخرى اقتصادية أو إدارية لها صلاحيات معالجة بيانات رقمية شخصية للمواطنين أو غير مواطني تلك الدولة فتأخذ هذ البيانات وتعالجها رغم ان القانون قد يوجب ضرورة قيام الجهات الراغبة في جمع وتخزين ومعالجة بيانات شخصية ضرورة الحصول على ترخيص مسبق لممارسة هذا النشاط قبل مزاولتها إياه. وعليه فأي عدم التزام بما تنص عليه القوانين ذات الصلة بالخصوصية للبيانات الشخصية ستعتبر انتهاكا صارخا لحق الخصوصية للأفراد والجماعات.

خامسا: التسلل الالكتروني

حيث تمارس بعض الدول بحجة حماية الامن القومي عن طريق التسلل داخل بيانات الشركات والمؤسسات العامة والخاصة بغية أخذ معلومات شخصية تمس حياة الموظفين والعمال والاطلاع على ملفاتهم دون اذن بذلك، فإذا انطوت المراقبة على ممارسة الدولة للسلطة أو للسيطرة الفعلية فيما يتعلق بالهياكل الأساسية للاتصالات الرقمية، يجب على الدول أن تتقيد بالتزاماتها المتعلقة بحقوق الإنسان كلما قامت بهذه المراقبة.

ويشمل ذلك مثلاً، التصنت المباشر على الهياكل الأساسية للاتصالات أو اختراقها، وممارسة الدولة للولاية التنظيمية على طرف ثالث يتحكم مادياً في البيانات. ونسخ كل البيانات الرقمية والمعلوماتية لهذه الشركات والمؤسسات واستغلالها في عمليات أبحاث أمنية أو استخباراتية.

المطلب الثاني: الشروط الواجب الاستناد إليها في تقييد واجب حماية الأمن الوطني أمام الحق في الخصوصية

لعله من المناسب الإشارة الى ان تأثر الحق في الخصوصية بمقتضى حماية الأمن الوطني له انعكاسات أخرى على حقوق جماعية غير تلك المتعارف عليها مثل الحق في الارتباط بالاتصالات الرقمية وجمع البيانات الشخصية بل تتعداه الى انتهاك حقوق اخرى مثل الحق في حرية الرأي والتعبير والحق في الوصول للمعلومة وتلقيها وإذاعتها

والحق في حرية التجمع السلمي وتكوين الجمعيات والحق في الحياة العائلية وهي حقوق كلها ترتبط ارتباطاً وثيقاً بالحق في الخصوصية.

وبالتالي فقيمة الحق في الخصوصية اذا استلزمت مقتضيات الأمن الوطني تقييده فيجب ان يكون ذلك وفق شروط واضحة ومعايير محددة يمكن ان نوجزها كالآتي:

أولا: أن تستند المراقبة الالكترونية على قانون ذي مواصفات محددة

من أهم ما ركز عليه اغلب من تناول الحق في الخصوصية في مواجهة حماية الأمن الوطني هو التأكيد على مبدأ التناسب، أشارت ألى ان التدابير المراد أخذها في مجال الرقابة الالكترونية يجب أن تتناسب مع أهمية المصالح ذات الصلة مصلحة الدولة في اتخاذ التدبير ومصلحة الفرد في الخصوصية.

وبيّنت أنه بزيادة أهمية مصلحة الفرد في الخصوصية، يجب أن تزداد دقة تصميم التدبير المتخذ. وأشارت إلى السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان، التي منحت الدول هامشاً معقولاً للتقدير، لا سيما في مجال الأمن القومي، يتيح لها أن تحدد على أساس كل حالة على حدى التدابير الضرورية والمتناسبة مع تحقيق مصلحة معينة للدولة، وأشارت السيدة كليفلاند أيضاً إلى أهمية الضمانات الإجرائية التي تضعها الدولة لضمان سلامة تطبيق نظام المراقبة.

وأشارت إلى الحاجة إلى وضع ضمانات قانونية لتحديد النظام، فضلاً عن الإشراف وسبل الانتصاف بأثر رجعي، للتأكد من عدم إساءة استعمال النظام.

ثانيا: أن يكون صادرا عن جهة مختصة

أي أن يتكفل الترخيص للأجهزة المختصة بمهمة حماية الأمن الوطني جهة قضائية أو سلطة إدارية مخولة قانونا مع السرية ويحق تامين الحكومات لأوطانها وحماية أمنها الوطني بوسائل فعالة تحت إشراف قضائي وبالتالي لا يتم التعرض لخصوصيات الأفراد إلا بترخيص قضائي وأن يكفله نص قانوني مثل ما نص عليه القانون الفرنسي يجيز القانون الصادر في 10جويلية1990 إذا توافرت شروط منها:

- إذا كان الاعتراض تفرضه ضرورة التحقيق
- أن يكون القرار صادرا من قاضي التحقيق باعتراض المراسلات المكتوبة أو من الجهة القضائية المخولة بذلك
- أن يكون الأمر بالضبط مسببا متضمننا لكل العناصر اللازمة لتحديد الاتصال المراد اعتراضه وتكون مدة صلاحية القرار أربعة أشهر قابلة للتجديد بنفس الشروط.

ثالثا: أن لا يكون مخالفا لقواعد القانون الدولي لحقوق الإنسان

وهو ما نص عليه قرار الجمعية العامة للأمم المتحدة 167/68 لعام 2013 الخاص بالحق في الخصوصية في العصر الرقمي لعام 2013 الذي استند على تقرير المفوض

السامي لحقوق الإنسان في العام 2014 حول تقرير الحق بالخصوصية في العصر الرقمي يصب في نتيجة مبدئية واحدة تتمثل في أن مصطلح الحق في الخصوصية يتسع للوسائل التكنولوجية الحديثة غير تلك المتعارف عليها سابقا.

حيث أقر تقرير المفوض السامي الى ضرورة كما انه لا يبدو من الضروري ولا من المتناسب الاحتفاظ الإلزامي بالبيانات لدى طرف ثالث - حيث يطلب من شركات الهاتف ومقدمي خدمات الأنترنت تخزين بيانات وصفية عن الاتصالات التي يجريها عملاؤها لكي تتمكن هيئات إنفاذ القانون وأجهزة الاستخبارات من الوصول إلى هذه البيانات في وقت لاحق.

رابعا: أن يكون مؤقتا

أي ان لا تتجاوز مدة تثبيت المراقبة الإلكترونية الشخصية المدة الزمنية المحددة قانونا او التي قدرتها جهة قضائية و بالتالي في فان أي تمديد او زيادة باي شكل من الأشكال يعتبر نوعا من انواع التدخل «التعسفي» أو «غير القانوني» في الخصوصية، فالمتفق عليه ان مراقبة الدولة لبيانات الاتصالات الإلكترونية قد تكون تدبيراً مشروعاً لإنفاذ القانون، إذا أُجريت وفقاً للقانون. غير أن الدول يجب أن تثبت أن تلك المراقبة ضرورية ومتناسبة مع الخطر المحدد الذي تجري مواجهته وبمدة محددة سلفا.

خامسا: أن لا يكون فيه تمييز بين المراقبين

كأن يتم توجيه الرقابة الالكترونية التي تنتهك الحق في الخصوصية على أساس التمييز بناء على اتجاهات سياسية معينة أو فكر إيديولوجي محدد او عن طريق التمييز الديني وغيره من أشكال التمييز المنبوذة قانونا وأخلاقا.

كما لا يجب أن يكون التمييز موجها ضد جنسية مقيمين في دولة بعينهم وهذا الشكل من أشكال انتهاك الحق الخصوصية موجود بكثرة في دول أوربا او تمارس حكومات أوربية يمينية متطرفة ضد المهاجرين.

ان الشروط السابقة الذكر رغم أهميتها تبقى غير كافية حيث انها تستلزم وضع أطر وآليات للموازنة بين قيمتين مجتمعيتين، وهما حق الأفراد في الخصوصية وواجب الدولة في درء وقوع الجرائم وتعقبها تحت مظلة حماية الأمن الوطني. في هذا الإطار خلص تقرير مفوضية الأمم المتحدة حول الحق في الخصوصية إلى أن مثل هذا التوازن ممكن في الحالة التي تستند فيها المراقبة الإلكترونية على قانون ذي مواصفات محددة وسلطة مختصة دون خرق للتشريعات ذات الصلة ودون تعسف.

خاتمة

أمام المخاطر التي استحدثتها الثورة المعلوماتية في مجال الرقمنة وتكنولوجيات الاتصال الرقمي والأنترنت واتساع دائرة التواصل في الفضاءات المفتوحة مع ما خلقه

ذلك من تفشي للجريمة الالكترونية ستكون الحكومات والدول في مهمة تحقيق هدفين مزدوجين الأول يتعلق بواجب كبح وردع كل صور وأشكال جرائم المعلوماتية لتأمين وحماية الأمن القومي، أما الثاني فيرتبط بضمان الحق في الخصوصية الرقمية للأفراد أو المؤسسات، وبالتالي يمكن القول أن التقدم التكنولوجي، بقدر ما عزز من قدرة الأفراد على التواصل بشكل سريع وفعال غير أنه خلق مجالا و مساحة لممارسة نوع اخر من الجرائم الحديثة الضارة بالأمن القومي للدول، في نفس الوقت تعززت قدرة الحكومات والدول على إجراء عمليات مراقبة للأفراد والتعرض لخصوصيتهم الحياتية خاصة ما تعلق بمراسلاتهم والمعلومات الخاصة المتعلقة بهم، فقد أصبح بإمكان سلطات الدولة باسم حماية الأمن الوطني أكثر من أي وقت مضى تتبع ومراقبة المراسلات بين الأفراد بشكل سري مستخدمين بذلك برامج الكترونية مخصصة لهذا الغرض سواء كان ذلك من خلال التسجيل للمكالمات أو من خلال التصنت أو التسجيل المرئي لمراسلات الأفراد وحركاتهم الإلكترونية وهو ما يضع الحكومات أمام واجب تحمل مسؤولياتها في احترام قواعد القانون الدولي الذي يقدم إطاراً واضحاً للحق في الخصوصية، على النحو المنصوص عليه في المادة 12 من الإعلان العالمي لحقوق الإنسان والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

وعلى ما سبق ذكره يمكن اقتراح بعض التوصيات التالية:

1. خلق توازن في اتخاذ التدابير والبرامج المرتبطة بحماية الأمن الوطني في مواجهة الحق في الخصوصية الرقمية.
2. ضرورة إعمال الحق في الخصوصية الرقمية في تشريعات وطنية واضحة ومحددة.
3. واجب التقيد بما تمليه وتنص عليه التشريعات الدولية في مجال حماية الحق في الخصوصية الرقمية.
4. إضفاء مزيد من الشفافية والوضوح على عمليات المراقبة الالكترونية التي تكون تحت مقتضيات حماية الأمن الوطني.

المراجع

راجع مقال انتهاك الخصوصية الرقمية الصحافة عن مركز هردو لدعم التعبير الرقمي مصر لعام2017- www.hrdoegypt.org : ص7 على رابط الموقع

تقرير المفوضية السامية لحقوق الانسان، الحق في الخصوصية في العصر الرقمي مؤرخ 30جوان2014 - a/HRC/27/37 الصفحة 10 فقرة 24 رقم الوثيقة

بارق منتظر بد الوهاب، جريمة إنتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الاردني،رسالة- ماجستير، جامعة الشرق الأوسط2017 الصفحة 113

سوزان عدنان ، صفاء أوتاني، انتهاك حرمة الحياة الخاصة عبر الإنترنت دراسة مقارنة، مجلة جامعة - .دمشق للعلوم القانونية و الاقتصادية المجلد 29 العدد3 لسنة2013 ص435

أ.د. إبراهيم بن داود أ.د أشرف شعت، الاطلاع على البريد الإلكتروني بين متطلبات النظام العام والحق - .في سرية المراسلة، دفاتر السياسة و القانون العدد16 جانفي2017 الصفحة29

بارق منتظر بد الوهاب، جريمة إنتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الاردني، رسالة - ماجستير، جامعة الشرق الأوسط2017 الصفحة 115

بارق منتظر بد الوهاب، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، رسالة - .ماجستير، جامعة الشرق الأوسط2017 الصفحة 116

مثال: القانون الفرنسي الخاص بالمعالجة الإلكترونية للبيانات الاسمية الصادر سنة 1978 ينص في المادة- :41 على أنه

يعاقب بعقوبة الحبس من ستة أشهر إلى ثلاث سنوات وبالغرامة من 14 الف فرنك أو أحدى هاتين العقوبتين) لكل من يجري أو يقوم بإجراء او المعالجة الإلكترونية للبيانات الشخصية دون ترخيص من اللجنة المختصة بذلك) ووفقا لذات القانون، فللمحكمة أن تأمر بنشر الحكم كله أو ملخصه في جريدة أو اكثر بالشروط التي .(يحددها الحكم

تقرير المفوضية السامية لحقوق الانسان، موجز حلقة نقاش بشأن الحق في الخصوصية بتاريخ 19 - A/HRC/28/39ديسمبر2014 صفحة5 الفقرة 12 رقم الوثيقةَ

سوزان عدنان ، صفاء أونتلي، جريمة انتهاك الحياة الخاصة عبر الأنترنت دراسة مقارنة، مجلة جامعة - .دمشق للعلوم القانونية و الاقتصادية المجلد 29 العدد3 ، لسنة2013 ص436

تقرير المفوضية السامية لحقوق الانسان، الحق في الخصوصية في العصر الرقمي الصفحة 6 فقرة 14 - a/HRC/27/37 رقم الوثيقة

تقرير المفوضية السامية لحقوق الإنسان، موجز حلقة نقاش بشأن الحق في الخصوصية بتاريخ 19 - A/HRC/28/39ديسمبر2014 صفحة 10 الفقرة27 رقم الوثيقةَ

أ.د. براهيم بن داود أ.د. أشرف شعت، الاطلاع على البريد الإلكتروني بين متطلبات النظام العام والحق - .في سرية المراسلة، دفاتر السياسة و القانون العدد16 جانفي2017 الصفحة 38

تقرير المفوضية السامية لحقوق الانسان، موجز حلقة نقاش بشأن الحق في الخصوصية بتاريخ 19 - A/HRC/28/39ديسمبر2014 صفحة5 الفقرة 9و10 رقم الوثيقةَ

تقرير المفوضية السامية لحقوق الانسان، موجز حلقة نقاش بشأن الحق في الخصوصية بتاريخ 19- A/HRC/28/39ديسمبر2014 صفحة5 الفقرة 10 رقم الوثيقةَ

كما ذات جاء في التقرير لمفوضية حقوق الانسان :››لا يجيز القانون الدولي لحقوق الإنسان التدخل في- حق الفرد في الخصوصية إلا إذا لم يكن هذا التدخل تعسفياً ولا غير قانوني. وأوضحت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم أن مصطلح «غير قانوني» يعني عدم إمكان حدوث أي تدخل «إلا في الحالات التي ينص عليها القانون. ولا يجوز أن يحدث التدخل الذي تأذن بها الدول إلا على أساس القانون، الذي يجب ‹‹ هو نفسه أن يكون متفقاً مع أحكام العهد ومراميه وأهدافه