

# المظاهر القانونية لاختراق الخصوصية في العالم الرقمي

ورقة بحثية مقدمة من الدكتور: حميداني سليم

رئيس قسم العلوم السياسية - جامعة 8 ماي 1945 قالمة-الجزائر

ضمن فعاليات:

الملتقى الوطني الأول: الحق في الخصوصية في مواجهة التحديات

الناشئة عن التكنولوجيا الرقمية. (واقع الحماية واعتبارات التقييد)

25-26 فيفري 2019

## ملخص:

يتجه العالم إلى أن يُضيق المسافات ويتجاوز الاختلافات بين شعوبه المتعددة على تنوع ثقافتهم وميولاتهم، ووسيلته في ذلك هي الثورة المتسارعة في ميدان التقنية والمعلوماتية، وهذه الثورة وإن كانت قد سهّلت أمور الحياة المختلفة، فإنها أبرزت إلى الواجهة المخاوف المتعلقة بالحريات الشخصية، وحظوظ الأفراد في أن يتمتعوا بحياة خاصة وخصوصية أبعد ما تكون عن الفضولية والانتهاك، وأن تكون بياناتهم ومعلوماتهم الشخصية بمنأى عن القرصنة والاستغلال غير المشروع، والتوظيف السيء لها، والنشر غير الموافق عليه من أصحابها.

تقتضي هذه المخاوف تحركات جادة وحماية قانونية للخصوصية، وان تتصدى الهيئات القانونية بصرامة لجرائم النشر المقترنة بانتهاك الخصوصية، وأن يجري تدريب العاملين في المجال الإلكتروني والمعلوماتي على تطوير آليات الحماية ونظم التشفير، والنقل الآمن للبيانات، وأن يحدث تكاتف مجتمعي في سبيل إنجاح هذا المسعى، وان تنرسخ ثقافة احترام الخصوصيات ومراعاة الشأن الخاص.

**الكلمات المفتاحية:** الخصوصية؛ جرائم النشر؛ التشفير؛ كلمة السر، المعلوماتية؛ نظم الاتصالات؛

الانترنت.

## Abstract

The world tends to narrow distances and transcend differences among peoples, regardless of their cultures and intellectual tendencies, depending on the accelerating revolution in the field of technology and informatics, and this revolution, although it facilitated the various things of life, It brought concerns about personal freedoms, and individuals' chances of enjoying private life far from curiosity and privacy violation, And that their personal data and information are free from piracy and illegal exploitation, bad using or unauthorized publication by their owners.

These concerns require serious action and legal protection of privacy, And the need for legal institutions to strictly confront publication offenses associated with a violation of privacy, also training of workers in the field of electronic and information on the development of protection mechanisms and encryption systems, safe data transfer, cooperate in order to ensure the success of this endeavor.

**Keywords:** Privacy; Publishing Crimes; Encryption; Password; Informatics; Communication Systems.

## مقدمة

ساهمت الثورة المعلوماتية في إعادة تشكيل العالم، ليصبح في بنيته بمثابة قرية عالمية صغيرة، أساسها التداخل والترابط، ومحورية الأنشطة الالكترونية وسرعة التداولات، ولقد اقتضى ذلك صياغة نمط جديد للتعامل مع هذا الواقع المستجد، خصوصا وأنّ مناحي التغيير شملت جوانب الاقتصاد والسياسة والثقافة وحركة الأفراد العلاقات الاجتماعية، كما أتاحت هذه الآفاق الجديدة المنبثقة عن ثورة الاتصالات والمعلومات نوعًا جديدًا وخطيرًا من أنواع التجسس، وهو التجسس الإلكتروني الذي أدركت الدول أهميته وسعت جاهدة للتفوق فيه.

صُمّمت الإنترنت كشبكة مفتوحة تتدفق خلالها المعلومات في صيغة صريحة، لذا فكل ما ينساب عبرها يمكن اعتراضه والاطلاع عليه بسهولة، إذا لم يتم تحصين الحسابات الشخصية، وإيجاد آليات تأمين فعال للمعلومات والبيانات المهمة، لذا فإن أكثر ما يشغل مستخدمي هذه الشبكة؛ هو حماية الخصوصية والهوية الرقمية والبيانات الشخصية والمعاملات المالية، خصوصا وأنّ التقاعس أو التفريط في ذلك قد يؤدي إلى آثار سلبية على المتضرر، أقلها اطلاع الآخرين على كل ما يخصه، فيما يسعى هو إلى جعله غير متاح إلى ذلك، ووصولاً إل الخسارة المالية وتراجع مستويات الثقة والارتباط إذا كان المتضرر شركة أو مؤسسة مالية أو مؤسسة خدمات، يفترض فيها ممارسة الحد الأقصى من الانضباط والدقة وحماية بيانات المتعاملين.

إنّ محاولة جعل مسألة انتهاك الخصوصية في العالم الرقمي مجرد إشكال قانوني صرف، هو أمر يتجاوز حقيقة أن للأمر جوانب متعلقة بأخلاقيات التعامل الإلكتروني، وبمعطيات اقتصادية تتصل بالاستثمار في نظم الحماية الالكترونية وبتقنيات التشفير وتخزين المعلومات، والأكثر من ذلك وجود مظلة سياسية تمثل إرادة الأنظمة في أن تكون سابقة عن مواطنيها أو المقيمين على بلادها؛ دوماً بخطوات في سبيل ترسيخ الأمّ الشامل كهدف معلن تسعى له الحكومات جميعاً، دون أن تعترف بتفاصيل

فعل ذلك، وبالتالي فإنّ هذه الاشتقاقات والشبكية المقترنة بتداخل الأدوار والأضرار حول مسألة انتهاك الخصوصية في المجال الرقمي، إنما تحفّز البحث حول الإشكالية التي تعالجها هذه الورقة، والتي يمكن صياغتها في التساؤل الموالي:

كيف يمكن إخراج موضوع انتهاك الخصوصية في المجال الرقمي، من نطاق المخاوف والغموض إلى نطاق التعامل الفعّال والتوعية البناءة بشأن مكافحة هذا الانتهاك، والنظر إليه كثغرة في سلامة التداولات والاتصالات يجدر إنهاؤها بأفضل شكل؟

للتعامل مع هذه الإشكالية، تتبنى هذه الورقة البحثية الدراسة الاستكشافية للموضوع والطابع التحليلي في ذلك، ومستعينة بالطرح القانوني في تأصيل موضوع انتهاك الخصوصية كأحد أشكال الجريمة الحديثة، ويمكن هذا المنهج من الوصول إلى تبني معطيات التعامل الفعّال مع هذا الوضع؛ الذي يظل تحدياً في مستقبل المعلوماتية.

## I - مفهوم الخصوصية الشخصية في المجال الإلكتروني :

تعني خصوصية المعلومات حق الأفراد في تحديد متوكيفو الأيديمتصل المعلومات عنهم لأخرين، لذا تُعرّف الخصوصية الرقمية بأنها عدم التعدي على البيانات الشخصية عبر الانترنت، أو أي وسيط مماثل، بالمعالجة أو الاستيلاء أو الاستخدام.<sup>(1)</sup>

تتزايد مخاطر التقنيات الحديثة على حماية الخصوصية، وكثيرة هي الابتكارات التكنولوجية التي أصبحت اليوم تقيّد الفرد في تنقلاته، وترصد أعماله وحركاته، وتجمع المعلومات الشخصية حوله وتخزنها وتعالجها بواسطة الوسائل المعلوماتية كتقنيات المراقبة بالفيديو، ورقابة البريد الإلكتروني والاتصالات وقواعد البيانات وغيرها، وهي جميعها تؤلف تهديداً مباشراً وجديداً على الخصوصية، وعلى الحريات الفردية خاصة بصورتها المستحدثة والمتمثلة في بنوك المعلومات، لاسيما إذا استغلت المعلومات والبيانات

المجمعة لغايات وأغراض مختلفة، بدون رضا أصحابها؛ الذين قد لا يكونون أصلا على علم بحدوث ذلك. (2)

إنّ انتهاك الحق في الخصوصية على شبكة الإنترنت لا يخرج عن أربع صور، وهي: اقتحام عزلة الشخص، والكشف عن أسرار الشخص الخاصة، وادعاء الأكاذيب، والاستخدام غير المصرح به لاسم الشخص أو لصورته. (3)

تعرف الخصوصية الرقمية-والتي يطالب بها المتعاملون بالتكنولوجيات الحديثة- بأنها وصف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائل رقمية، وتتمثل البيانات الشخصية في البريد الإلكتروني، والحسابات البنكية، والصور الشخصية، ومعلومات العمل والمسكن، وكذا البيانات التي يجري استخدامها في التفاعل على شبكة الإنترنت بواسطة الحاسبات الآلية والهاتف المحمول، أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية (4)، والتي صار لا غنى عنها لدى ملايين المستخدمين.

يمكن الآن-وبفضل تطور الوسائل الإلكترونية- أن تكون فكرة عن أشخاص لم يحدث الاتصال أو الالتقاء بهم مطلقا، وهم على بعد جغرافي يحول دون الاحتكاك بهم، وفي هذا الإطار يقول توماس

فريدمان Thomas Friedman الصحفي بجريدة نيويورك تايمز The New York Times:

إن هناك جانبا آخر لجلب المعلومات يجب أن يعتاده الناس، وهو قدرة الآخرين على جلب المعلومات بأنفسهم عنك، حيث تُسطح محركات البحث العالم، بإزالة ما كان الناس يختفون داخله أو وراءه أو تحته، لكي يخفوا سمعتهم أو أجزاء من ماضيهم، وفي العالم المسطح لا يمكنك الهرب، ولا يمكنك الاختباء، فيما يزداد البحث ضيقا، عش حياتك بأمانة، لأن كل ما تفعله، وكل ما ترتكبه من أخطاء، ستصبح يوما ما قابلة للبحث. (5)

تتصل الخصوصية في العصر الرقمي بنمطين هما:

01- خصوصية المعلومات الشخصية Information Privacy Personal

تتضمن هذه الخصوصية القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية وهي المحل الذي يتصل عادة بمفهوم حماية البيانات<sup>(6)</sup> ، *Data Protection* ، ويظل التشكيك واردا بشأن احتفاظ المواقع والتطبيقات بما تجر به من معاملات، بدءاً من المعاملات البنكية وخدمات الصراف الآلي وأعمال التسوق، وكذا خدمات الاطعام والنقل، ومرورا بالخدمات الصحية والسياحية، ووصولاً للنشاطات المهنية والتداولات المالية، وهو ما يجعل التساؤل ينصب حول مصير البيانات والمعلومات الشخصية بعد تقديم الخدمة وانقضائها، واحتمال استخدامها فيما بعد بشكل قد يسبب لصاحبها ضرراً معنوياً أو مادياً.

## 02- خصوصية الاتصالات Telecommunications Privacy

يشير هذا المفهوم إلى شعور المشترك أوكل من يجري اتصالاً، أنه بمأمن عن التنصت والتجسس، بصرف النظر عن المكان أو التوقيت الذي يجري فيه اتصاله، ولطالما كان الامر في الماضي مقترنا بالمحادثات الهاتفية كمحور لهذه الخصوصية، ومع تطور وسائل الاتصال الحديثة، اتسع الأمر ليشمل وسائل الاتصال المنبثقة عن تطور شبكة الانترنت والخدمات التي توفرها في التراسل النصي والمصور<sup>(7)</sup>، ويتصل القسم الأكبر من مشاكل الخصوصية في هذا الاطار، من ما يتعرض له مستخدمو مواقع التواصل الاجتماعي والهواتف المحمولة والانترنت بشكل عام، والتي تؤدي إلى انتهاك خصوصياتهم، باستخدام هؤلاء الأفراد أو أصحاب المواقع الشركات والمصالح الرسمية كلمة سر ضعيفة؛ تساعد من المتلصقين الالكترونيين على كشف خصوصية الضحية، وبسبب عدم الاهتمام بشكل كاف بإعداد كلمة سر قوية لحماية الخصوصية والبيانات الشخصية، تزيد احتمالية وقوع مخاطر ومشاكل رقمية.

## **II أساليب الحكومات في انتهاك الخصوصية الرقمية**

تجسد كثير من الأنظمة السياسية في العالم المعاصر؛ الأجواء المضامينية لرواية "1984" الشهيرة للكاتب الانكليزي جورج أورويل George Orwell، وهي الرواية التي تثير في جانب منها مسألة اقتحام الخصوصية، تحت شعار المراقبة للحماية، إلى درجة يفقد فيها الفرد كل حرياته، وتصير كل فترات يومه ونشاطاته متاحة للجهات التي تراقبه، ويبلغ السعي إلى كشف خصوصية الافراد مستويات غير معقولة في بعض الدول، ومن ذلك مثلاً أنّ كوريا الشمالية تحدد للأفراد ما ينبغي أن يشاهدوه أو يستمعون إليه، حيث يجري تسويق أجهزة التلفزيون والراديو وهي مبرمجة مسبقاً على استقبال ترددات البث الحكومي حصراً، ومختومة بتحذير يمنع تغييرها، ويعد التلاعب بتلك الأجهزة لاستقبال بث خارجي بمثابة جريمة يعاقب عليها القانون، خصوصاً مع إجراءات التحقق من الأختام الموضوعة على الأجهزة، كما جرى سنة 2003م، حين باشرت السلطات حملة للتأكد من ذلك.<sup>(8)</sup>

إن التطاول على حقوق الأفراد في التمتع بالحياة الخاصة، وعدم احترام خصوصياتهم شاع في فترة الحرب الباردة، وضمن البلدان ذات الأنظمة السياسية المغلقة، والتي كانت تحرص عبر أجهزتها الأمنية على التحوط من أي تحركات أو أفكار تتصل بالحرية السياسية ومطالب التغيير السياسي والتداول على السلطة، وترى في انتهاك خصوصيات الأفراد؛ إجراء استباقياً مطلوباً تبرره الاحتياجات الأمنية للدولة، وظلّ الاعتقاد أنه في الدول الأخرى التي هي على النقيض من الدول الاستبدادية، فإن هناك مجالاً واسعاً للحرية واحترام خصوصية الأفراد، ويكفل ذلك جملة من التشريعات والقوانين وحرية الاعلام في فضح الانتهاكات التي قد تطال تلك الخصوصية والحرية الشخصية التي لها قدر عال من التقديس، غير أن السنوات الأخيرة أبانت عن حقائق صادمة بشأن مدى احترام الخصوصية المتعلقة بالمواطنين والمقيمين بدول الغرب، وأنه يجري فعلاً التنصت على الاتصالات والتجسس على الملفات الشخصية، وقرصنة المعلومات، وكل ذلك تحت مبرر الدواعي الأمنية ومكافحة الإرهاب.

تأتي في مقدمة الدول التي تمارس تلك الانتهاكات للخصوصية-خاصة منذ أحداث 11 سبتمبر 2001م- الولايات المتحدة الأمريكية التي لم يعد خافيا هيمنتها على منظومة الاتصالات والمعلوماتية العالمية، على نحو يمكنها الوصول لبيانات ومعلومات ملايين المستخدمين للتكنولوجيا الحديثة، كما يتأتى لها تفعيل نظم المراقبة والتصوير والتجسس الذي يطال ملايين الأفراد في مناطق مختلفة من العالم، وفي هذا الإطار؛ كشف إدوارد سنودن Edward Snowden-الموظف السابق لدى وكالة المخابرات المركزية الأمريكية والمقيم حالياً في روسيا-معلومات؛ تفيد بأن وكالة الأمن القومي في الولايات المتحدة ومقر الاتصالات العامة في بريطانيا طوّرا معاً تكنولوجياً تسمح بالوصول إلى الكثير من حركة الإنترنت العالمية، وسجلات المكالمات، ودفاتر العناوين الإلكترونية للأفراد، وأحجام هائلة من محتوى الاتصالات الرقمية الأخرى.<sup>(9)</sup>

في ذات السياق؛ أظهرت التقارير أن السلطات الأسترالية قد قامت باختراق سجلات المواقع الإلكترونية الأسترالية في العام 2014 بواسطة مزودين خدمة الإنترنت في استراليا للوصول إلى معلومات تتعلق بالأفراد، أما في الصين فهناك برنامج مُعلن عنه لهذه الغايات يطلق عليه GoldenShieldProject وهو برنامج مخصص لمراقبة الأفراد ضمن وزارة الأمن القومي الصينية حيث اعتمد في العام 1998 وبدأ العمل فيه في العام 2003.<sup>(10)</sup>

يجب أن نسجل في هذا الإطار ملاحظة متعلقة بمسألة الوصول إلى المعلومات السرية، وتضرر أصحابها من هذا الفعل، حيث أنه وفي الماضي كان الضغط أكثر نحو مطالبة الحكومات، بأن تحمي خصوصية الأفراد، وأن تكفل قانوناً واضحاً وفعالاً لتأمين ذلك، ومتابعة من ينتهك تلك الخصوصية على اعتبار أن ذلك أحد واجباتها، إلا أن حدة التطور العلمي في مجال الاتصالات خاصة، جعل الحكومات نفسها عاجزة عن تحصين معلوماتها وبياناتها حتى السرية منها، وهو ما يجعل التساؤل يطرح بشأن الجهة

وكذا التقنية القادرة على توفير ذلك، والآليات القانونية التي تمكّن ضحايا انتهاك الخصوصية من التعويض عن الضرر الذي لحقهم جراء ذلك.

إنه وتقديراً منها لأهمية الخصوصية، وخطر الانتهاكات التي قد تطالها، فقد تم وضع مجموعة من المبادئ من طرف منظمة التعاون الاقتصادي والتنمية بشأن الخصوصية، والتي تتمثل فيما يلي:

- مبدأ حدود جمع البيانات، وأن يكون جمعها بوسائل مشروعة ويعلم وموافقة صاحبها؛
- مبدأ جودة البيانات، من خلال وجوب أن تكون على علاقة بالغرض الذي جُمعت لتستخدم فيه، وأن تكون محدّثة ودقيقة وكاملة؛
- مبدأ تحديد الغرض، حيث يجب ان تحدد أغراض جمع البيانات الشخصية، والإطار الزمني للجمع والاستعمال؛
- مبدأ حدود الاستخدام، إذ يجب ألا يتم الكشف عن البيانات الشخصية، أو أن تتاح أو تستخدم لأغراض غير تلك المحددة مسبقاً، وبموافقة صاحب البيانات أو بسلطة القانون؛
- مبدأ الحماية الأمنية؛ حيث يجب حماية البيانات الشخصية عن طريق ضمانات أمنية معقولة ضد المخاطر، مثل فقدان البيانات أو الدخول غير المصرح به عليها، أو تدميرها أو استخدامها أو تعديلها، أو الكشف عنها؛
- مبدأ المساءلة، بوجود أن يكون المتحكم في البيانات خاضعاً للمساءلة بشأن الامتثال للإجراءات التي تطبق المبادئ المذكورة سابقاً.<sup>(11)</sup>

### III- الخصوصية في حقل المعلوماتية كاهتمام قانوني

يعود الاهتمام القانوني الحديث بالحق في الخصوصية إلى عام 1890، وذلك من خلال المقال الشهير الحق في الخصوصية *THE RIGHT TO PRIVACY* الذي تم نشره في مجلة كلية الحقوق بجامعة هارفارد *Harvard Law Review*، والذي ذهب فيه كل من صامويل وارن *Samuel D. Warren*

ولويس برانديس *Louis D. Brandeis* بحق كل إنسان في الانفراد بنفسه، بحيث لا يزعجه أحد، ولقد وصف القاضي برانديس الحياة الخاصة بأنها الحق في أن يترك المرء وشأنه، وذلك من أهم الحقوق وأكثرها قيمة لدى الأفراد المتحضرين. (12)

ان الدفع بالحرية كشكل من أشكال التملص من المتابعة القانونية بشأن انتهاك الخصوصية، يرسخ الاعتقاد بأن عددا من الممارسات التي جرى الاعتقاد أنها عادية، وأن مرتكبيها يعملون بشكل صحيح تماماً، هي ممارسات لا تقع تحت طائلة القانون، ولا متابعة أو تعويضاً بشأنها، وأنتصرف منتهاك الخصوصية المعلوماتية، هو تصرف قانوني تماماً وضمن شروط الخدمة.

نتار المساءلة الجنائية كثيراً في نشر الصورة أو الفيديو، حتى في إثبات التقصير أو تبادل التهم في نزاعات الطلاق والحضانة، فالنشر الافتراضي لا يشترط أحياناً الإرسال لجمهور كبير، فالتهديد بنشر الفيديو أو الصورة يعد أيضاً انتهاكاً، وقد يكون الاعتداء بفعل الانتحال أو المنازعة على أسبقية التسجيل. (13)

لقد تمت إثارة مسألة الخصوصية سنة 2015م على نحو واسع في الفضاء المعلوماتي؛ مع تفجر فضيحة تسريب بيانات 37 مليون مستخدم من عملاء موقع آشلي ماديسون *Ashley Madison* المتعارف بكونه يغطي على أعمال الخيانة الجنسية، ويوفر مجالاً لهذا النوع من الممارسات الاجتماعية المرفوضة، وهذا التسريب لبيانات عدد من المعنيين بما يوازي سكان دولة من دول العالم، فتح الجدل بشأن تأمين البيانات المفترض بقاؤها سرية أو حذفها بشكل يمنع استعادتها بعد انتهاء الخدمة المطلوبة، وبالنسبة لموقع آشلي ماديسون فقد جرى الاحتجاج بأن الموقع لم يحذف ما يدل على هؤلاء العملاء من قاعدة بياناته، رغم تسديد القيمة المالية المطلوبة من هؤلاء الزبائن والمتعاملين عبره. (14)

أصبح تتبع قضايا انتهاك الخصوصية مثاراً لسجال قانوني ما فتئ يحدث بشكل مستمر، ويدفع الأطراف المتضررة من ذلك إلى طلب تعويضات كبيرة، وفي هذا الشأن توصلت شركة فيس بوك

Facebook مثلاً؛ إلى تسوية بشأن قضية خصوصية رفعت ضدها عام 2011م؛ والتزمت بدفع 20 مليون دولار بعد دعوى أشارت إلى أنّ برنامج الإعلانات الجانبية أو ما يعرف بـ *Sponsored Stories* قام بانتهاك خصوصية المشتركين، وتعود القضية إلى ممارسات فيس بوك من حيث استخدام إعجابات المستخدمين كأداة إعلانية، بحيث تعرض صورة ملفاتهم الشخصية وبجانب الصفحة المعلن عنها على أنه قام بالإعجاب بها، وبالتالي تشجيع المستخدمين الآخرين من أصدقائه بالإعجاب بالصفحة، في حين أنّ هناك قانوناً مدنياً في كاليفورنيا يعتبر استخدام الإعجابات كأداة إعلانية بدون موافقة صريحة من المستخدم عملاً غير شرعي.<sup>(15)</sup>

في قضية متعلقة أيضاً بانتهاك خصوصية المستخدمين لخدمات البحث الإلكتروني عبر الإنترنت؛ تعرضت شركة غوغل *Google* إلى تغريم قدره 1.22 مليون دولار من قِبَل لجنة الرقابة لحماية البيانات في إسبانيا؛ لجمعها واستخدامها البيانات الشخصية للمستخدمين فيما يُعدّ ذلك طريقة غير قانونية. وكان التحقيق حول ما قامت به قوغل من ثلاثة انتهاكات خطيرة لقوانين خصوصية البيانات الإسبانية، بعد أن جمعت بيانات شخصية لأكثر من 100 منتج وخدمة هناك، ومن الواضح أن عملاق البحث لم يحصل على موافقة صريحة لاستخدام بيانات المستخدمين<sup>(16)</sup>.

بالعودة إلى التكييف القانوني لكثير من دعاوى انتهاك الخصوصية، ومطالبة الضحايا بالتعويض عما لحقهم من ضرر خاصة المعنوي منه، وما فاتهم من مكاسب مادية، فإنه هذه الدعاوى تسقط إزاء قوة المبدأ القانوني القائل بأنه لا يعذر بجهل القانون، وأن القانون لا يحم المغفلين، وشركات التواصل الاجتماعي مثل التي ابتكرت خدمات وتطبيقات التراسل المكتوبة والمسموعة، عملت من خلال شروط الاستخدام وسياسة الخصوصية التي فرضتها على استغلال المستخدم، أو الاستفادة من عدم تمكنه من فهم ما بين السطور، إما بسبب عدم قراءة شروط الاستخدام التي تتسم دوماً بالطول والتعقيد، أو بسبب اللغة، وبشكل أو بآخر تسعى هذه الشركات إلى إغراء العملاء باستخدام التطبيق، مجاناً مقابل المتاجرة

بأهم شيء يملكونه وهو علاقاتهم، ومراسلاتهم وبياناتهم الشخصية<sup>(17)</sup> ، وبالتالي فإنه وفي الواقع يعلم الكثير من المستخدمين لتطبيقات التواصل الاجتماعي مثلا؛ أنه غالبا من بين أهم شروط استخدام التطبيقات، أن الشركة تستطيع الاستفادة من كل المحتويات الشخصية وبالتالي يمكنها نشرها أو تقديمها لأي جهة.

لقد دأبت منظمات حماية الحقوق الفردية والحريات على الإنترنت، مثل منظمة "سييتيزنز إلكترونيك رايثس"*Citizens Electronic Rights*، على رفع صوت التحذير من عواقب مراكمة المعلومات الشخصية على صفحات شبكات التواصل الاجتماعي، ولا تتوقف الصحف عن نشر الأخبار والقصص التي تدور حول محور وحيد، هو انكشاف الأفراد بأثر من المعلومات والصور والأشرطة التي يضعونها على هذه المواقع.<sup>(18)</sup>

هناك دوما شكاوى متكررة بشأن الفضاء السيبراني من ضعف في نُظم الحماية، ما يجعله مساحة مستهدفة من قبل المتطفلين الإلكترونيين، الذين لا يتورع بعضهم عن استعمال المعلومات وسيلةً لابتزاز أصحابها، أو لإيقاعهم في مشاكل أو توريطهم في أفعال إجرامية، تستدعي متابعتهم قضائيا، ومن ذلك ما يحدث في العالم العربي بشكل متكرر، بل وكان من ورائه شخصيات في مناط بها حماية الأمن المعلوماتي للأفراد ضمن الدولة، ومن ذلك مثلا قبل مدة قصيرة ما تعلق في لبنان بقضية المقدم سوزان الحاج، التي كانت تشغل سابقا منصب مديرة مكتب مكافحة الجرائم المعلوماتية في قوى الأمن الداخلي اللبناني، والتي أوقفت على ذمة التحقيق، بناء على إشارة قضائية للاشتباه بأنها استعانت بقرصان معلوماتية لتلفيق تهمة التواصل مع فتاة إسرائيلية للممثل زياد عيتاني الذي جرى اعتقاله قبل ذلك تحت تهمة التخابر مع إسرائيل.<sup>(19)</sup>

أمام الإصرار على تقييد مجال خصوصية الأفراد والاحتجاج بالضرورات الأمنية، فقد جرى إضعاف الموقف القانوني في عديد القضايا التي رفعت تحت عنوان متابعة انتهاك الخصوصية، وظهر ذلك

خاصة في مجال التراسل الإلكتروني النصي، حيث دأبت الجهات الأمنية على تتبع خيوط وملابسات الاجرام الإلكتروني انطلاقا من رزنامة وفحوى الاتصالات التي تم إجراؤها من أجهزة ذات صلة بواقعة إجرامية ما، مع السعي لتجاوز القيد الإلكتروني المتعامل به في نظم الاتصالات، والمتمثل في نظم التشفير التي تزداد درجة تعقيدها، مع تطور وسائل الاتصالات ، وتحت إلهام الزبائن الذين يطلبون أمانا وسرية أكبر لمعاملاتهم الإلكترونية، واتصالاتهم اليومية بعيد عن القرصنة والتجسس الإلكترونيين، ولهذا يصير التأمين الصارم للخصوصية المعلوماتية هو الأصل، والانتهاك له هو الاستثناء المقيد والمرفوض من شركات الاتصالات ومن الزبائن أنفسهم.

#### IV- رهانات تأمين الخصوصية الإلكترونية في المستقبل

إنّ وجود سابقة في انتهاك الخصوصية لدواع أمنية، والاحتجاج بأنّ فك التشفير هو مطلب استعجالي وحالة خاصة ومحددة، من بين الملايين من المستخدمين الذين يملكون هواتف أو حواسيا في دول العالم المختلفة، لا يرسل رسائل طمأنة بشأن ضمانات حماية الخصوصية، لذا فقد تمسكت شركة آبل بموقفها الرافض لطلب المباحث الفيدرالية في فك تشفير هاتف C5؛ جرى التحفظ عليه في قضية تتعلق بالإرهاب سنة 2016م، وكان من شأن موافقتها على هذا الطلب أن تهتر ثقة عملاء الشركة عبر العالم في نظامها المتعلق بتأمين أجهزة الاتصالات التي تسوقها، ولقد بررت الشركة رفضها بكونه مرتكزا على حقوق الافراد في حماية الخصوصية، وبالتالي كانت تشرك تدفع باتجاه حماية الخصوصية كي تحمي سوقها وسمعتها التكنولوجية، في حين كانت الحكومة الأمريكية تضغط في اتجاه انتهاك الخصوصية بدعوى حماية الأمن القومي، لاسيما وأنها قد تواجه المشكلة ذاتها في سياق جرائم أخرى في المستقبل.(20)

إنّه ومن منظور تقني؛ يظل من الصعب حماية البيانات ذات الشكل الإلكتروني، خصوصا إذا كانت محفوظة على حواسيب متصلة بالإنترنت، ممّا يعرضها للاختراق والقرصنة، بل إنّ الوسائط التي كانت تعد آمنة؛ صارت دون ذلك، مع تطوير طرق لفك التشفير أو نقل المعلومات عن بعد بشكل مشابه

لنمط عمل الواي فاي WiFi، يضاف إلى هذه الحقيقة أنّ هوس الأفراد بالانخراط في الحياة الافتراضية الموازية، يجعلهم غير مدركين لحجم انتهاك خصوصياتهم، وأنهم جزء من منظومة معقدة من الترحيب الإلكتروني المتصاعد، الذي يجعل الفرد المعتقد بأنه يستفيد من الخدمة المجانية للتواصل والتراسل، في حين أنّه ذاته السلعة محور هذا الترحيب، وردا على هذه الحقيقة؛ قال ألكسندر كوغان Aleksandr Kogan-مطور تطبيق كامبريدج أناليتيكا Cambridge Analytica- بأنّ على المستخدمين أن يكونوا واعيين بأن بياناتهم يتم مشاركتها وبيعها لأغراض إعلانية، حيث أن بيع بيانات المستخدمين هي سياسة من فيسبوك لعملية الإعلانات. (21)

فيما لم تجد أستاذة علوم الكمبيوتر مارغو سيلتزر Margo Seltzer إلا القول بأن الخصوصية التي عرفناها في الماضي، أصبحت أمراً مستحيلاً الآن، مضيئة: التقنيات الموجودة بالفعل الآن، مثل بطاقات الائتمان وشبكة الإنترنت والرادارات على الطرق السريعة، وكاميرات مراقبة الشوارع ومواقع التواصل الاجتماعي والبريد الإلكتروني، كل ذلك يترك أثراً رقمياً هائلاً يمكن تتبعنا من خلاله. (22)

يظل التحدي الأبرز لحماية الخصوصية المعلوماتية للأفراد، هو التطور الهائل لأساليب التجسس وأنماط القرصنة الإلكترونية، بشكل يفوق تطور نظم الحماية الإلكترونية، ويبرز ذلك من خلال تطوير آلاف الفيروسات الإلكترونية التي يجري إطلاقها في الشبكة المعلوماتية الدولية، وقد أجرت شركة كاسبرسكي لاب Kaspersky Lab سنة 2014م دراسة في مجال مكافحة الفيروسات وحماية الأجهزة الإلكترونية من هجمات قرصنة الكمبيوتر المعروفين بالهاكرز Hackers، وأظهرت أنّ نحو 315 ألف تطبيق خبيث يحاول اختراق أجهزة الاتصالات الإلكترونية يومياً، واعتبرت الدراسة أن المواقع والصفحات الزائفة المصممة لسرقة البيانات الشخصية على شبكة الإنترنت، أصبحت تهديداً إلكترونياً شاملاً يشكّل خطراً على جميع المستخدمين، بغض النظر عن نوع الجهاز ونظام التشغيل الذي يعمل به، وقد تمّ سنة

2014م رصد وتسجيل أكثر من 137 ألف صفحة تصيدية؛ تدفع مستخدمي الإنترنت إلى تسليم بياناتهم الشخصية والمالية إلى المجرمين الإلكترونيين.<sup>(23)</sup>

صار التحدي الآن وفي المستقبل ، ليس إيجاد مكان لتخزين المعلومات الشخصية، وإنما حمايتها واستغلالها على نحو آمن، وهو ما يتطلب دخولا آمنا لها، وحفظها بشكل يبتعد بمضمونها السري عن إطلاع الآخرين وانتهاك الخصوصية المعلوماتية للأفراد والشركات التي يهتز وضعها بمجرد كشف كلمة المرور السرية وإتاحتها على نحو متوقع للقراصنة المعلوماتيين، ولهذا فإنه ولتجنب الوقوع في هذا الاحتمال، ينصح باستعمال كلمة السر التي تكون قوية، وحتى تصبح كذلك؛ يجب أن تكون كلمة طويلة، فكلما كانت أطول؛ كلما زاد مستوى الحماية، كما يجب أن تكون هذه الكلمة مركبة من أحرف وأرقام ورموز، وغير متعلقة ببيانات شخصية؛ مثل الاسم وتاريخ الميلاد ورقم هاتف المحمول، ومن المهم تغيير كلمة السر بعد فترة استعمال، ومن الخطر استخدام نفس كلمة السر ذاتها لحسابات الفرد المختلفة.

في جانب آخر؛ فإنه يجدر إدخال البيانات الخاصة من الأجهزة الشخصية، بشكل يجعلها مؤمنة بشكل كافٍ، يضمن عدم تعرضها للسرقة، ومن ذلك تجنب المنصات العمومية للإنترنت، أو ما تعرف بمقاهي الإنترنت، ويدخل في هذا الإطار استعمال أجهزة إلكترونية غير شخصية، قد تحتفظ بأثر الدخول، وتكون بذلك طريقة فعالة للنصب والاحتيال، وأقل مستوياتها انتهاك الخصوصية الشخصية، والاطلاع على بيانات لا يريد أصحابها إطلاع غيرهم عليها.

## خاتمة

في ختام هذه الورقة البحثية؛ نخلص إلى جملة من الاستنتاجات بشأن حماية الخصوصية في مجال المعلوماتية والاتصال، وإيلاء ذلك الأمر قدرا عاليا من الاهتمام، وهذه الاستنتاجات نعرضها على النحو التالي:

- ضرورة التوفيق بين الضرورات الأمنية التي يقتضيها الأمن الوطني، وسلامة الأراضي والمنشآت والمصالح من جهة، وحق الأفراد في أن يحظوا باحترام صارم لخصوصياتهم، وأن تمر كل الإجراءات التي تمس بتلك الخصوصية بمتابعة قضائية، وبإخطار للجهات المعنية مع حفظ كامل الحقوق للمعنيين بالمساس بخصوصياتهم.

- العمل على برمجيات متطورة تراعي مفهوم السرية *Confidentiality*، والتي تعني التأكد من أن المعلومات لا تكشف، ولا يمكن الاطلاع عليها من أشخاص آخرين غير مخولين بذلك.

- ضرورة تأصيل المسؤولية التقصيرية لمستخدمي شبكة الإنترنت؛ من المستخدم العادي إلى موصل الخدمة وصاحب الموقع الإلكتروني.

- نشر الوعي بأهمية الخصوصية المعلوماتية، وتعويد الأفراد على احترام خصوصيات بعضهم، بدءاً من الفئات العمرية المتدنية، وعبر مؤسسات التنشئة والتعليم، واستهجان كل انتهاك للخصوصية، باعتباره عملاً غير أخلاقي تستهجنه قيم المجتمع وعاداته.

- منح مجال واسع لحرية الفكر والتعبير، بما يدفع للانطلاق في الابداع والتطوير، ويغني عن التردد والفضولية ورغبة التريح على حساب الآخرين.

- الفصل بين مفهوم الخصوصية المعلوماتية والشأن العام، وذلك بالتفرقة بين الشخص ونشاطه أو المؤسسة التي يعمل بها أو السلطة التي يمثلها، والصلاحيات المتاحة لها، حيث يمكن تتبع مسار عمله على نحو من المحاسبة والمساءلة، وبشكل شفاف وعبر المؤسسات القانونية المنتخبة، ووسائل الاعلام المحترفة.

- تفعيل منظومة قانونية وقضائية صارمة تقف بمسؤولية وفاعلية أمام أي انتهاك للخصوصية، ويدخل في هذا الإطار تتبع نشاط شركات المعلوماتية، وكذا مواكبة إدخال الأجهزة الحديثة، وضرورة تتبع كل

الثغرات التي قد يتم الدخول منها للملفات والمعلومات الشخصية، ويكون الأسلوب الرادع بالغرامات الرادعة والتعويض المجزي خيارا مناسباً، للحد من انتهاكات الخصوصية.

في العالم العربي نحن بحاجة لأن نتجاوز القيود الفكرية والتنظيمية حول مفهوم الأمن المعلومات، وأن يتم تشجيع الكفاءات على الابداع، والربحية والاستثمار في هذا المجال، والسعي للتعامل بصرامة مع أنظمة التسويق والاتصالات والمعلوماتية الأجنبية والمحلية، التي مازالت تستثمر في العجز العربي عن تفعيل نظم الحماية الالكترونية، ويضاف إلى ذلك أنه يجدر رفع الوعي لدى الأفراد العرب بشأن مسائل انتهاك الخصوصية، واحداث تدريب في المؤسسات التنشئة والتعليم على احترام الخصوصيات الشخصية وسبل تأمينها، وأن لا يكون الامر مناطاً فقط باستيراد نظم التأمين والحماية الالكترونيين من الخارج.

## الهوامش

(1)- مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، (مصر: القاهرة، مركز الدراسات العربية للنشر والتوزيع، ط01، 2016)، ص100.

(2)-أسامة السيد محمود، الخصوصية وحرية تداول المعلومات على مواقع الويب دراسة تحليلية، في: أسامة السيد محمود(محرر)، الاتجاهات الحديثة في المكتبات والمعلومات ، ج01، (القاهرة: المكتبة الأكاديمية، ط01، 2011)، ص309.

(3)-يعقوب عبد العزيز الصانع، انتهاك الحق في الخصوصية عبر الإنترنت، جريدة القبس، الكويت، العدد 16022، 2017/01/08، ص12.

(4)-مركز هردولد عمالتعبير الرقمي، انتهاك الخصوصية الرقمية في الصحافة المهنية الصحفية والحياة الشخصية، القاهرة، 2017، ص05.

(5)- توماس فريدمان، العالم مسطح: تاريخ موجز للقرن الواحد والعشرين، تر: عمر الأيوبي، (لبنان: بيروت، دار الكتاب العربي، ط01، 2006)، ص179.

- (6)- محمد عبد الله شاهين، التجارة الإلكترونية العربية بين التحديات وفرص النمو، (القاهرة، دار حميترا ، ط1، 2017)، ص265.
- (7)-محمد نور الدين، "الحماية الجنائية في خصوصية المكالمات الهاتفية"، مجلة دراسات، علوم الشريعة والقانون، المجلد 43، ملحق04، 2016، ص1689.
- (8)-Susan Chun, **Radio gives hope to North and South Koreans**, February 27, 2008, see : 12/04/2018  
<http://edition.cnn.com/2008/WORLD/asiapcf/02/27/cho.dissidentradio/index.html>
- (9)- جاسم محمد، داعش والجهاديون الجدد، (الأردن: عمان، دار الياقوت للنشر، ط01، 2014) ص61.
- (10)-رزق سلمودي وآخرون، الموقف المعاصر لقواعد القانون الدولي العام من الحقائق الخصوصية في العصر الرقمي، مجلة الجامعة العربية الأمريكية للبحوث، مجلد(3)، العدد(2)، 2017، ص03.
- (11)- ريموند واكس، الخصوصية: مقدمة قصيرة جدا، تر: ياسر حسن، (القاهرة، كلمات عربية للترجمة والنشر، ط01، 2013)، ص ص 116-118.
- (12)-Samuel D. Warren,Louis D. Brandeis, **THE RIGHT TO PRIVACY**, **Harvard Law Review**. Vol. IV, No. 5, December 15, 1890, downloaded from :  
[http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy\\_brand\\_warr2.html](http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html)
- (13)- يعقوب عبد العزيز الصانع، انتهاك الحق في الخصوصية عبر الإنترنت، جريدة القبس، الكويت، العدد 16022، 2017/01/08، ص12.
- (14)- رامي عبود، ديجيتولوجيا: الانترنت، اقتصاد المعرفة، الثورة الصناعية الرابعة...المستقبل، (القاهرة: العربي للنشر والتوزيع، ط01، 2016)، ص61.
- (15)-محمد حبش، فيس بوك تدفع 20 مليون دولار غرامة انتهاك الخصوصية، منشور بتاريخ 2013/08/27، اطلق عليه بتاريخ: 2018/04/02، متوفر على الرابط الالكتروني:
- <https://goo.gl/BTs9Ry>
- (16)-تامر عمران، في مسلسل انتهاك الخصوصية: لجنة الرقابة الإسبانية تُغرم قوقل 1.2 مليون دولار، منشور بتاريخ 2013/12/21، اطلع عليها بتاريخ 2018/04/03، متوفر على الرابط الالكتروني:
- <https://goo.gl/ZMCMDY>
- (17)- تزي منصور، الأرباح بالملايين عبر شبكات التواصل الاجتماعي أين أهمية الدور والوظيفة في العالم الافتراضي؟، مجلة الجيش، لبنان، العدد 347، أيار 2014، ص ص 78-82.
- (18)- أحمد مغربي، شكوك حول قدرة الموقع الاجتماعي على حماية خصوصية المعلومات الشخصية، جريدة الحياة، لندن، العدد 17607، 2011/06/19، ص18.
- (19)-يستند عمل مكافحة الجرائم المعلوماتية في حماية الأمن اللبناني على عدم التعارض مع قانون التخابر رقم 140 الصادر في 27 أكتوبر 1999 الذي ينصّ في مادته الأولى على صيانة الحق في سرية التخابر الجاري داخلياً وخارجياً بأي وسيلة من وسائل الاتصال السلكية أو اللاسلكية الأجهزة الهاتفية الثابتة، والأجهزة المنقولة بجميع أنواعها بما فيها الخليوي، والفاكس، والبريد الالكتروني....
- ويشددّ على أن التخابر لا يخضع لأي نوع من أنواع التنصت أو المراقبة أو الاعتراض أو الإفشاء إلا في الحالات التي ينص عليها هذا القانون، وبواسطة الوسائل التي يحددها ويرسم أصولها. أنظر: شفيق السامرائي، حقوق الانسان في الموثيق والاتفاقيات الدولية، (الأردن: عمان، دار المعتز للنشر والتوزع، ط01، 2015)، ص336.
- (20)-رامي عبود، مرجع سابق، ص ص 60،61.
- (21)- Harry Davies, **How academicat centre of Facebook scandaltried – and failed – to spin personal data into gold**, The Guardian, Tue 24 Apr 2018.
- (22)-سلمان الدوسري، التعايش مع انتهاك الخصوصية، جريدة الشرق الأوسط، 2017/03/09، العدد 13981.
- (23)- ندين البلعة خير الله، 315 ألف تطبيق خبيث يحاول اختراق أجهزتك الإلكترونية!، مجلة الجيش، لبنان، العدد 356، شباط 2015، ص 75.