

جامعة عمار ثلجي الاغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق

الحق في الخصوصية في العصر الرقمي

مذكرة تخرج ضمن مقتضيات نيل شهادة الماستر

تخصص: قانون دولي عام

إشراف الأستاذ الدكتور:

عبيدي محمد

إعداد الطالبين:

تونسسي سعيد

دلماجي أسامة

أعضاء لجنة المناقشة:

رئيسا	بوغفالة بوعيشة
مشرفا ومقررا	عبيدي محمد
ممتحنا	مسعودي محمد لمين

السنة الجامعية: 2024/2023

شكر وعرفان

الحمد والشكر العظيمين لله تعالى الذي أعاننا بتوفيقه ورضاه على إتمام هذا العمل.

فالحمد لله حمدا طيبا كما يحب ويرضى والصلاة والسلام على سيدنا محمد نبي الهدى والرحمة وسيد المرسلين وعلى آله وصحبه ومن تبعه بإحسان إلى يوم الدين.

نتقدم بخالص الشكر والعرفان الجزيل إلى الأستاذ الدكتور عبيدي محمد على ما قدمه لنا من جهد ورعاية متواصلة، ولم يبخل علينا بعلمه ووقته في توجيهنا وتشجيعنا، وما لمسناه منه من حسن خلقه وتواضعه وحرصه الشديد على إتمام العمل في أحسن صورة، فكان لنا نعم المشرف ونعم المعلم، زاده الله علما ورفعة، بارك الله فيه وجزاه خير الجزاء.

كما نتقدم بالشكر الجزيل إلى السادة أعضاء لجنة المناقشة لتفضلهم بتكبد عناء مناقشة المذكرة لملاحظاتهم أثرا كبيرا في إثراء وجودة هذا العمل.

وبأسمى عبارات الحب نهدي عملنا وخلاصة جهدنا وصبرنا إلى كل من ساهم في انجاز هذا العمل ولو بكلمة أو نصيحة أو دعاء بظهر الغيب.

مقدمة:

لقد أحدثت تقنيات الاتصالات ثورة في الطريقة التي يتفاعل بها البشر، وأن العصر الرقمي يمثل أكبر حركة تحرير عرفها العالم، كما شكل التدخل انتهاكا لحق الإنسان في الخصوصية. ومن الثورة التكنولوجية التي مكنت الدولة من الوصول إلى عمق هذه القيمة المجتمعية المتعلقة بالخصوصية، أن عمليات المراقبة قد يكون لها تأثير حقيقي على حقوق الإنسان المكفولة للناس، ومما لا شك فيه أن كل تطور تقني له انعكاساته على المستوى القانوني، فكل المفردات الحديثة للتكنولوجيا أضحت تثير مسألة توافق إيجابياتها مع سلبياتها على بعض الحقوق التي تحتاج إلى الحماية، سواء في إطار النصوص التقليدية أو باستحداث النصوص الملائمة لطبيعتها والدور الذي تؤديه في مختلف مجالات الحياة.

وفي ظل التطور الدائم والمستمر لتكنولوجيا المعلومات ظهرت مشكلة تأثيرها في حياة الغير من خلال توسع استخدام شبكة الانترنت في أغراض مختلفة ودخول جميع فئات المجتمع إلى قائمة المستخدمين، ونقل معه النشاطات الاجتماعية والثقافية والاقتصادية والسياسية من عالم واقعي ملموس إلى بيئة افتراضية تقتقد إلى المرئية، فلقد أثبتت الدراسات تضاعف مستخدمي الانترنت من 360 مليون نسمة عام 2000 إلى ما يقارب 2.7 مليار نسمة في عام 2013 وتوسع تفاعل الأشخاص مع الشبكة وأضحى أكثر تأثيرا في حياتهم اليومية من خلال انتقال الحياة اليومية للأفراد من مجالها الحقيقي إلى فضاءات رقمية كمواقع التواصل الاجتماعي والبريد الإلكتروني وبرز ظاهرة التسوق الإلكتروني وغيرها من المجالات التي أضحت ضرورة لا اختيارا يستغنى عنه، وأصبحت تشكل نقطة تماس مع خصوصية الأفراد بشكل مباشر، مما فتح المجال أمام ظهور نوع جديد من الإجرام المعلوماتي ينصب في أحد أبرز صوره في انتهاك تلك الخصوصية واستباحة حق السرية والهدوء للحياة الخاصة للأفراد¹.

أسباب اختيار الموضوع:

- رغبتنا الشخصية في دراسة الموضوع.
- طبيعة تخصصنا في مجال القانون الدولي.
- خطورة ظاهرة انتهاك الحق في الخصوصية الرقمية وانتشارها من خلال الاستعمال السيئ لتكنولوجيا المعلومات وأثره السلبي على خصوصيات الأفراد.

¹ - كريم عاطف، الخصوصية الرقمية بين الانتهاك والغياب التشريعي، ورقة بحث صادرة في إطار سلسلة أوراق الحق في المعرفة الصادرة عن مركز دعم تقنية المعلومات، القاهرة، 2013، ص3.

أهمية الدراسة:

تظهر أهمية الدراسة في طبيعة الموضوع الذي نتناوله من خلال إبراز مخاطر التكنولوجيا الرقمية على الحق في حرمة الحياة الخاصة الرقمية، لأن التماذي في ابتكار تقنيات انتهاكها دون وازع ولا رادع قد تتحول من خلالها من الدولة المدنية إلى مجتمعات لا إنسانية، فستر خصوصية الفرد هي فطرة طبيعية فرضتها قوانين الطبيعة، وكثرة ضحايا هاته التكنولوجيا في المجتمعات، مع كثرة حالات الانتقام ممن انتهكوا حقهم المقدس في حرمة حياتهم الخاصة، مما يؤدي إلى تزايد عدد الجرائم.

أهداف الدراسة:

من بين الأهداف التي نسعى إلى الوصول إليها، التعريف بالحق في حماية الخصوصية الرقمية، وكذلك تبيان أشكال الاعتداءات والانتهاكات التي تتعرض لها الخصوصية الرقمية في ظل التطور الهائل الذي تشهده تكنولوجيا المعلومات والاتصال.

صعوبات الدراسة:

لقد واجهتنا عدة صعوبات أبرزها:

قلة المراجع التي تناولت الموضوع وذلك نظرا لحدثته.

إشكالية الدراسة:

وترجع مسألة ظهور الاعتداء على الحق في الخصوصية في العالم الرقمي من خلال مساهمة التكنولوجيا في جمع البيانات الشخصية وتنظيمها ودمجها بسهولة وسرعة غير مسبوقين، كذا كثرة نقل وتداول البيانات في إطار الباب الواسع للمعاملات الإلكترونية قد شكلت في مجموعها تهديدا لحدود الحق في الحياة الخاصة، الأمر الذي لزم معه تسييج قنوات التعامل الإلكتروني من خلال ضمان آليات وسبل قانونية تحيط الحياة الخاصة وتحول دون عرضة الخصوصية للكشف والتشهير والاستغلال من قبل الآخرين. وهذا ما يدفعنا للتساؤل عن ماهية الحق في الخصوصية الرقمية؟ وفيما تتمثل مخاطر التقنيات الحديثة على هذا الحق وكذا آليات حمايته؟

منهج الدراسة :

اقتضت منا طبيعة الموضوع اتباع المنهج الوصفي من خلال التعريف بالخصوصية الرقمية.

خطة الدراسة:

وللإجابة على هذه الإشكالية المطروحة، ارتأينا تقسيم الدراسة إلى فصلين، يتناول الفصل الأول دراسة الإطار المفاهيمي للخصوصية الرقمية، وذلك في بحثين، خصصنا الأول لماهية الحق في الخصوصية الرقمية، أما المبحث الثاني أثر تكنولوجيا المعلومات على هذا الحق. وخصصنا الفصل الثاني لدراسة حماية الحق في الخصوصية الرقمية والذي احتوى بحثين، في المبحث الأول تطرقنا لأشكال الاعتداء الإلكتروني على الحق في الخصوصية الرقمية، أما في المبحث الثاني آليات حماية الحق في الخصوصية الرقمية.

الفصل الأول

الإطار المفاهيمي

للخصوصية الرقمية

الفصل الأول: الإطار المفاهيمي للخصوصية الرقمية

الحق في الخصوصية هو حق أساسي من حقوق الإنسان منصوص عليه في العديد من القوانين الدولية والوطنية. ومع ذلك ، ويظهر التقنيات الرقمية ، أصبح الحق في الخصوصية معقدًا بشكل متزايد ويصعب حمايته.

لذا تحرص المجتمعات خاصة الديمقراطية منها على كفالة هذا الحق، وتعتبره حقًا مستقلًا بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعى إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دورا كبيرا وفعالا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم، ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أو من جانب الدساتير أو النظم القانونية.

ومع تزايد التقنيات الحديثة وتطورها المستمر زادت المخاطر على الخصوصية، لاسيما مع بداية خضوع المعطيات الشخصية لنظام تحكم مركزي للإدارة العمومية، مما أثار تخوفات شديدة على حماية البيانات التي تتصل بالأفراد وحياتهم الخاصة¹.

نظرا للانتهاكات المتكررة لحرمة الحياة الخاصة، أولى القانون الدولي لحقوق الإنسان والتشريعات الوطنية ذات الصلة، عناية خاصة بحياة الأشخاص الخاصة.

فقد نص الإعلان العالمي لحقوق الإنسان على انه " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، أو لحملات على شرفه وسمعته، لكل شخص الحق في حماية القانون من مثل هذا التدخل أو هذه الحملات "².

ولتعزيز هذا الحق في عدم التعرض للحياة الخاصة للأشخاص أكد العهد الدولي للحقوق المدنية والسياسية بأنه " لا يجوز لأي شخص على نحو تعسفي أو غير قانوني التدخل في خصوصياته أو شؤون أسرته أو بيئته أو مراسلاته ولا لأي حملات غير قانونية تمس شرفه أو سمته"³ ويشير هذا العهد الدولي أيضا في مادته 17 إلى أن " من حق كل شخص أي يحميه القانون من مثل هذا التدخل أو المساس".

¹ - فريد هديكيت، الخصوصية في عصر المعلومات، مركز الأهرام للترجمة والنشر، القاهرة، ص 123.

² - المادة 12 من الإعلان العالمي لحقوق الإنسان لعام 1948.

³ - المادة 17 من العهد الدولي للحقوق المدنية والسياسية لعام 1966.

وتعرف الخصوصية بأنها حق المستخدم في ضمان عدم التصرف في بياناته الشخصية من قبل الغير دون إذنه، ويشمل ذلك تخزين معلوماته الخاصة وتقاسمها مع جهات أخرى دون علمه أو عرضها على العموم. وتعرف أيضا بأنها حق الأفراد في السيطرة والتأثير على المعلومات التي تخصهم، بحيث يمكنهم تجميع وتخزين وتحديد من وإلى من يمكنهم الاطلاع عليها¹. ويعرفها البعض الآخر بحق الفرد في الحفاظ على معلوماته الشخصية وحياته الخاصة بشكل اختياري وحر، ومنع الحصول عليها بطريقة غير طوعية. وتشمل هذه المعلومات على سبيل المثال كل من المعلومات الطبية والصور والمكالمات والبيانات البنكية وأسلوب الحياة والأخلاقيات ورؤية الذات والآخر". فالخصوصية هي رسم للحدود التي تنظم قدرة المجتمع على التدخل في حياة الأفراد، ولها أربعة حدود أساسية، الأول: خصوصية المعلومات الشخصية وجمعها ومعالجتها. الثاني: خصوصية الجسد من التدخل الفيزيائي. والثالث: خصوصية الاتصال والتواصل وأمن المراسلات بكافة أشكالها. والرابع: خصوصية الحيز المكاني الذي يتواجد فيه الفرد.

واللخصوصية وجهان أساسيان:

الأول: الحق في حرية الحياة الخاصة والثاني: الحق في سرية هذه الحياة ". وقد ساهم الانتقال والتحول إلى العصر الرقمي في تآكل الخصوصية المعلوماتية للمستخدمين لتكنولوجيا المعلومات والاتصال، فالكلم الكبير من البيانات المتوفرة في الفضاء الرقمي جعل هذه البيانات تنتقل من الملكية الخاصة إلى الملكية العامة "

وتعرف البيانات الشخصية، على إنها أي معلومات لها علاقة بالأفراد، والتي يمكن من خلالها التعرف عليهم بشكل مباشر. على سبيل المثال: البريد الإلكتروني، الموقع الجغرافي، الجنس، العرق، الدين والمعتقد، الصورة، معلومات التصفح الخاصة بالمواقع، الآراء السياسية، الأسماء المستعارة والكنية ونمط الحياة وطريقة التفكير ومجالات التحرك، وغيرها مما يمكن اعتباره من البيانات الشخصية التي قد تساعد في التعرف على هوية شخص بعينه".

ومن خلال هذا الفصل سنتناول ماهية الحق في الخصوصية الرقمية ضمن المبحث الأول، وفي المبحث الثاني أثر تكنولوجيا المعلومات على الحق في الخصوصية.

¹ - عبيدي محمد، مقال موسوم: "تكنولوجيا المعلومات والاتصالات وحتمية التحول الرقمي " منشور في كتاب جماعي موسوم: "القانون والتكنولوجيا الحديثة" صادر عن مخبر القانون والتنمية المحلية بجامعة احمد دراية ادرا، ط1، 2021، ص 15.

المبحث الأول: ماهية الحق في الخصوصية الرقمية

مع تزايد التقنيات الحديثة زادت المخاطر على حق الإنسان في خصوصيته، فأصبح الفرد مقيدا في تعاملاته من خلال رصد البيانات الشخصية كتقنيات المراقبة والتجسس والمساس بالمعطيات الخاصة للأفراد وهي جميعها تمثل تهديدا مباشرا على الخاصة والحريات الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات، لا سيما إذا استغلت تلك المعلومات والبيانات لغايات خارجة عن إرادة وعلم أصحابها.

المطلب الأول: مفهوم الحق في الخصوصية الرقمية

الفرع الأول: تعريف الحق في الخصوصية الرقمية

الحق في الخصوصية¹ الرقمية مفهوم يقتزن بالمعلوماتية ومختلف استخداماتها، وكون هذه الأخيرة اليوم تحتل جانبا هاما من الحياة الخاصة للأفراد فقد طفا هذا المفهوم على السطح منذ الستينيات من القرن الماضي.

ينعقد شبه إجماع بين الفقه والتشريع على عدم إيجاد تعريف جامع مانع للحق في الخصوصية وهذا يترجم من خلال التعدد التعريفي لهذا المفهوم في إطار النظام القانوني الواحد، ولعل هذه الصعوبة في توحيد المفهوم يرجع إلى طبيعة الحق التي تكتسب صفة المرونة وعدم التحديد والضبط في إطار محدد وتختلف باختلاف المجتمعات الإنسانية والحقب الزمنية عبر العصور².

أولا: الحق في الخصوصية في وجهه التقليدي

وبهذا فقد ذهب العديد من الفقه لإيجاد تعريف الحق في الخصوصية كل وفق توجهاته ومنطلقاته الفكرية على اعتبار أن المكونات المنطقية للخصوصية تتسم باضطرادها المستمر في كل حقبة زمنية فعلى سبيل المثال قد بدأت بلورة مفهوم الخصوصية سابقا في إطار المراسلات التقليدية الورقية ومن

1 - ورد تعبير "الحق في الخصوصية the right to privacy" لأول مرة في مقال نشر عام 1890 لبرانديس ووارن Brandies/Warren في مجلة هارفرد الحقوقية في الولايات المتحدة الأمريكية، وهو مفهوم يرتبط بكيان الإنسان أو بحيزه الخاص الذي يسعى من خلاله إلى حماية مشاعره وأفكاره وأسراره الخاصة تجسيدا لكيونته الفردية.

وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط1، بيروت، 2017، ص 37.

2 - الذهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية، أدرار، العدد 08، المجلد 01، 2017، ص 142.

ثم بدأت الفكرة تتطور إلى حين وصولها إلى الحياة في العالم الرقمي وهنا يتشكل الفرق في جوهر مفهوم الخصوصية.

فوفقاً للفقهاء EDWARD BLOUSTEIN أن الخصوصية هي الحق في حماية الحياة الشخصية للأفراد وضمان عدم الاعتداء عليها واستقلالها¹.

أما وفقاً للفقهاء GAVISON Ruth فلقد بني مفهوم الحق في الخصوصية وفق 3 عناصر: السرية، العزلة والتخفي بحيث اعتبر أنه الحق في الحماية ضد التدخل في الحياة الخاصة وشؤون عائلتهم بوسائل مادية مباشرة أو عن طريق نشر المعلومات» كما يرجع الفقيه هشام محمد فريد رستم قيام مفهوم الحق في الخصوصية بتوافر وجهين أحدهما مادي وقوامه عدم إقحام الشخص في خصوصيات الآخرين، والثاني إعلامي مقتضاه ألا تكون الشؤون الخاصة بالفرد محلاً للحق في الإعلام بالنسبة للآخرين مما يستتبع معه عدم استغلال الآخرين لتلك المعلومات بالنشر أو التشهير².

ثانياً: حق الخصوصية في العالم الرقمي

وهنا يسند أغلب الفقه والتشريعات فكرة الحق في الخصوصية إلى النطاق الحديث الذي تتناول فيه، والتي يتشكل مفهومها في حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم مدى وصول المعلومات المرتبطة بحياتهم الخاصة للآخرين، وبأن يضبط عملية حصر المعلومات الشخصية ومعاملتها اليا، واستخدامها في صنع القرار الخاص أو المؤثر في حياتهم³.

وبهذا دل التعريف إلى مفهوم الاستحداث في التعاملات بين الأفراد من خلال معالجة المعلومات الخاصة بهم إلكترونياً وضمان تلك الخصوصية التي تتبع من حصر فكرة الاطلاع على البيانات الشخصية وعدم التطاول عليها من قبل الآخر.

من الأوائل الذين كتبوا في موضوع الخصوصية في ظل استخدامات المعلوماتية نجد الفقيه آلان واستن AlenWsten في العام 1967، الذي عبر عنه بـ "خصوصية المعلومات" وعرفه بأنه: "حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنه للآخرين⁴.

1 - عبد الله عبد الكريم، جرائم المعلوماتية والانترنت في الجرائم الالكترونية، منشورات الحلبي الحقوقية، بيروت، 2007، ص 36.

2 - محمد هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1992، ص 176.

3 - حسام الدين الأهواي، الحق في احترام الحياة الخاصة (الحق في الخصوصية)، دراسة مقارنة، دار النهضة العربية، ط2، 2002، ص 132.

4 - توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير، الأمم المتحدة، منشورات اليونسكو، فرنسا، 2013، ص 02.

فهي شكل مستحدث للخصوصية لها علاقة مباشرة بالمعلومات، لأن جانباً مهماً من المعلومات الحساسة والخاصة بالأفراد قد أضحى اليوم متاحاً عبر الأنظمة المعلوماتية والانترنت خاصة، بحيث يصعب تعقبه أو استرجاعه أو جعله قابلاً للنسيان. لذلك فإن الفقيه ميلر Miller يعرفها بأنها "قدرة الأفراد على التحكم بدورة المعلومات المتعلقة بهم"¹. أي تمكين المستخدمين وحدهم من منع الآخرين أو السماح لهم بالاطلاع على أو التصرف في المعلومات المتعلقة بحياتهم الخاصة.

ويظهر بهذا أن مفهوم الحق في الخصوصية الرقمية هو امتداد لمفهوم الحق في الخصوصية عموماً، إلا أنه يختلف عن الأخير بكونه يتصل على وجه التحديد بالمعلومات الخاصة ويمدّ قدرة الأفراد على التحكم في تدفقها عبر تكنولوجيات الاعلام والاتصال.

في حين جاء تعريف الفقيه ميلر في كتابه «الاعتداء على الخصوصية» أكثر عمقا إذ عرفها بأنها قدرة الأفراد على التحكم في سرية المعلومات المتعلقة بهم².

وبهذا فقد نجد أن الحق في خصوصية المعلومات الشخصية يتوقف على فكرة الاعتداء عليها إلكترونياً من قبل الآخر، واستخدامها وفقاً لأغراض خارجة عن القانون بدون علم أو إرادة صاحبها. وبالارتكاز على منحي الخصوصية في وجهها المستحدث نجد التعريف الصادر عن مركز دراسات البيانات المجتمعية والذي أرجع الحق في الخصوصية إلى إمكانية الفرد بالتصرف بشكل قانوني دونما وجود عائق يحول هذا التصرف³.

وبهذا فإن المعنى العميق لمفهوم الخصوصية يتجلى في تبني تلك الرخصة في حرية التصرف وضمان عدم التدخل أو التطفل من الغير تحت أي ظرف وهنا نستشف تلك الإضافة التي جاء بها هذا التعريف من خلال تسييج الخصوصية ضد أي خروق تصدر من الأفراد أو حتى من الدولة في إطار ما يعرف بالمراقبة الإلكترونية⁴.

ثالثاً: المفهوم التشريعي للحق في الخصوصية الرقمية

بداية إن مفهوم الخصوصية قد بني في مختلف التشريعات المقارنة تحت إطار ضمان الحد الأدنى في حق الفرد بعدم التدخل أو المساس بالحياة الشخصية أو الأسرية أو خرق لسرية المعاملات

1 - توبي مندل وآخرون، مرجع سابق ص 13.

2 - محمود إبراهيم الغازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص 272.

3 - السيد عتيق، جرائم الانترنت، دار النهضة العربية، مصر، 2002، ص 61.

4 - عبد الفتاح حجازي، الحماية الجنائية المعلوماتية للحكومة الإلكترونية، دار الكتاب القانونية، مصر، 2007، ص 33.

أو الحقائق التي تحيط بحياته، وأما الدستور الجزائري قد قرر هذا الحق من خلال نص المادة 39 التي تنص على: "لا يجوز انتهاك حرمة حياة المواطن وحرمة شرفه ويحميها القانون "سرية المراسلات والاتصالات بكل أشكالها مضمونة"

أما عن نص المادة 39 فلقد كان النص واضحا مباشرا في تكريس الحماية لحق الخصوصية أما عن نص المادة 40 فقد كانت الإشارة ضمنية تكفل خصوصية الأفراد بعدم خرق حقهم في أن يكونوا آمنين على أنفسهم ضد أي تعسف في التفتيش أو الاحتجاز أو اقتحام المساكن غير مبني على أسس قانونية وهو مظهر من مظاهر الحماية للحياة الخاصة.

الفرع الثاني: التطور التاريخي لحماية الحق في الخصوصية:

يكتسب الحق في الخصوصية أهميته وخطورته من تكريم الله للإنسان وتفضيله له على كثير ممن خلق، فالمستعرض لتاريخ الإنسانية الفكري يجد أن فكرة الحقوق الطبيعية المستمدة من فكرة القانون الطبيعي من أولى الفكر التي نادي بها الفلاسفة والمفكرون وهي التي أقرت للإنسان حقوقا طبيعية في المقدمة منها حقه في الحياة لكونه الأساس الذي يركز عليه بقية حقوقه، ويرى الكثير من الباحثين أن حقوق الإنسان عامة هي نتاج الفكر الأوربي الحديث ووليدة تربته التي ائبعت بالثورة الانجليزية عام 1688 والثورة الفرنسية عام 1789 وما تمخض عنها من مبادئ الاهتمام بحقوق الإنسان وحرية¹ أهمها الإعلانات والمواثيق الدولية والإقليمية حيث نصت المادة 12 من الإعلان العالمي لحقوق الإنسان الذي أقرته الجمعية العامة لمنظمة الأمم المتحدة عام 1948م، على حماية الحق في الحياة الخاصة بنصها " لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلته."

ونصت المادة 17 من العهد الدولي للحقوق المدنية والسياسية التي وافقت الجمعية العامة للأمم المتحدة عليها سنة 1966 على أنه لا يجوز التدخل بشكل تعسفي أو غير قانوني بخصوصيات أحد أو بعائلته أو بينه أو مراسلته"، كما اعترفت الاتفاقية الأوروبية لحقوق الإنسان التي تم التوقيع عليها عام 1950 بالحق في الحياة الخاصة فنصت في المادة 08 على أن "الكل شخص الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلته، ولا يجوز للسلطة العامة التدخل في مباشرة هذا الحق إلا إذا كان هذا التدخل بنص عليه القانون، ويعد إجراء ضروريا في مجتمع ديمقراطي لحماية الأمن الوطني العام أو

1 - عمراوي مارية - حجاج مليكة، حماية الحق في الخصوصية عبر الانترنت دراسة وصفية تحليلية وفق قانون العقوبات الجزائري، دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، مجلد 12، عدد 3، جويلية 2020، السنة الثانية عشر، جامعة زيان عاشور، الجلفة، ص 3.

الرفاهية الاقتصادية للدولة، أو لحماية النظام أو لمنع الجرائم أو لحماية الصحة أو الآداب أو لحماية حقوق الغير وحرياتهم¹.

وقد شهد العالم خلال النصف الثاني من القرن العشرين ثورة هائلة في تقنية المعلومات. كان من أهم إفرازاتها ظهور الحاسب الآلي الذي غزا أوجه كل النشاط الإنساني وأضحى حاجة أساسية لكل بيت متطور أو مدرسة أو مصنع أو غير ذلك من المرافق والمؤسسات، وتوج التطور المتلاحق في تقنية المعلومات بظهور الإنترنت التي خلفت بيئة افتراضية لتدفق فيها المعلومات والاتصالات عبر الحدود، ودون أي اعتبار للحدود أو السيادة، وسهلت عن طريق استخدامهما المختلف للاتصالات وسرعة الحصول على المعلومات في أي مكان في العالم وسهولة سرعة تبادل الأبحاث والمعلومات، واحتل البريد الإلكتروني أهمية بالغة في انتشار استخدام الإنترنت في المراسلات والاتصالات على كافة المستويات، وإلى تطور العلاقة بين وسائل الإعلام والفرد الذي لم يعد متلقي بل طرفا في العلاقة الإعلامية، فله أن ينشر ما يريد وأن يعبر عن رأيه إلى جميع مستخدمي الإنترنت في شتى أنحاء العالم، مما أعطى للخير سرعة أكبر في الانتشار وعدد أكبر من القراء وجعل من الفرد العادي محررا ورئيس تحرير، وناشرا وطابعا وموزعا².

إلا أن هذا الجانب المشرق لتطور وانتشار تقنية المعلومات والإنترنت، والاستفادة من خدماتها وميزاتها صاحبه جانب آخر اتسم بالأنانية والظلمة، والاعتداء غير المشروع على مصالح وفهم مادية ومعنوية، كانت ومازالت موضع اهتمام القانون الجنائي، فقد أصبح الانتشار الكبير والتطور المتلاحق في تقنية المعلومات بشكل خطرا مستمرا على الحق في الحياة الخاصة، وهدد بانتهاك حرمتها وتعرية أسرارها، وتهديد سكينة الإنسان وطمأنينته خاصة أمام عدم قدرة الإنترنت على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات³ خاصة عقب كشف العالم ادوارد سندوق سنة 2013 من برنامج لجسم أطلقته وكالة الأمن القومي على شركات الإنترنت بتفويض من جورج بوش بعد هجمات الحادي عشر سبتمبر سنة 2001.

1 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 326.

2 - عمراوي مارية - حجاج مليكة، المرجع نفسه، ص 326.

3 - عمراوي مارية - حجاج مليكة، المرجع نفسه، ص 326.

الفرع الثالث: محل الحق في الخصوصية الرقمية

كشفت دراسة صادرة عن لجنة التجارة الفيدرالية (FTC)¹ عام 1999 أن 92.08 % من مواقع الويب كانت جمعت على الأقل نوعا واحدا من بيانات الهوية، (identifying information) على غرار الاسم، العنوان البريدي، عنوان البريد الإلكتروني².

وغيرها من المعلومات ذات الطبيعة الخاصة والشخصية المتداولة عبر الانترنت، والممثلة تمثيلا رقميا، تسمى بالبيانات الشخصية، لذلك فإن هذه الأخيرة تعتبر المحل الذي ينصب عليه موضوع الحق في الخصوصية الرقمية.

أولا: تعريف البيانات الشخصية

البيان يجد مرادفه في اللغة الانجليزية Data وفي اللغة الفرنسية، Donnée ويقصد به من الناحية الفنية، كل تمثيل يمكن أن تخزن فيه المعلومة، يمكن أن يكون نصا أو جدولا أو رسما بيانيا، كما يمكن أن يكون منديلا أو لونا أو إشارة أو أية رموز أخرى، تكون ذات دلالة ومعنى لدى معالج المعلومة³.

وتقوم مختلف الأنظمة المعلوماتية اليوم في أدائها على تمثيل البيانات تمثيلا رقميا، باستعمال الرقمين 0 و 1 فقط يشار لها أيضا بالمعطيات ذات الطابع الشخصي، أو البيانات الاسمية.

ف نجد المشرع رقم الفرنسي مثلا، قد استخدم عبارة البيانات الاسمية بشكل أساسي في القانون، (78/17) وهو القانون المتعلق بالمعلوماتية والحرية الصادر في 6 جانفي 1978) في نسخته الأولى، واستخدم عبارة البيانات الشخصية في مواضع معينة من هذا القانون، بينما استخدمت الاتفاقية الأوروبية لحماية الأشخاص اتجاه المعالجة الآلية لسنة 1981 وكذا التوجيه الأوروبي رقم 95/46 المتعلق بحماية الأفراد فيما يتصل بمعالجة البيانات وحرية انتقالها، عبارة "البيانات ذات الطابع الشخصي الأمر الذي دفع المشرع الفرنسي إلى استبدال عبارة البيانات الاسمية بعبارة البيانات ذات الطابع الشخصي، استجابة للتوجيه الأوروبي لتعميم استخدام هذه التسمية، وتبني تعريف أوسع للمعطيات الشخصية حيث جاء

¹ - Federal Trade commission.

² - Winnie Chung and John Paynter : Privacy Issues on the Internet, Departement of Management Science and Information Systeme, School of Business, The University of Auckland, Private Bag 92019, Auckland, New Zealand. Proceedings of the 35th Hawaii International Conference on Systeme Science – 2002. IEEE.

³ - كيث دفلين، الإنسان والمعرفة في عصر المعلومات، ترجمة: شادن اليافي، مكتبة العبيكان، السعودية، ط 1، 2001م، بتصرف.

التعديل بموجب قانون 04/801 الصادر في 6 أوت 2004،¹ الذي عرفها في المادة 02: "تشكل معطيات ذات طابع شخصي كل معلومة متعلقة بشخص طبيعي معرف أو يمكن التعرف عليه، بصفة مباشرة أو غير مباشرة، بالرجوع إلى رقم تعريف أو إلى عنصر أو عدة عناصر مميزة له".

ولتحديد ما إذا كان الشخص قابلاً للتعرف عليه، يلزم الأخذ بالاعتبار مجموع الوسائل التي من شأنها التمكين من تعريفه² وبنفس الصيغة تقريباً عرف المشرع المغربي المعطيات الشخصية³.

بينما عرفها المشرع التونسي في القانون الأساسي عدد 63 المتعلق بحماية المعطيات الشخصية، بنص الفصل 04: "تعتبر معطيات شخصية على معنى هذا القانون كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصاً طبيعياً معروفاً أو قابلاً للتعريف بطريقة مباشرة أو غير مباشرة، باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانوناً"، وجاء في نص الفصل 05 من نفس القانون: "يعد قابلاً للتعريف الشخص الطبيعي الذي يمكن التعرف عليه بصورة مباشرة أو غير مباشرة من خلال مجموعة من المعطيات أو الرموز المتعلقة خاصة بهويته أو بخصائصه الجسمية أو الفيزيولوجية أو الجينية أو النفسية أو الاجتماعية أو الاقتصادية أو الثقافية"⁴.

يعد هذا التعريف، تعريفاً وظيفياً يرمي القانون من ورائه إلى حماية جانب من الحياة الخاصة من زحف المعرفة، للحد من الانتهاكات التي تأتي على مكامن الذات الإنسانية، فكل معلومة تتعلق أو تخص فرداً معروفاً أو يمكن التعرف عليه بشكل مباشر أو غير مباشر تشكل معطيات شخصية، فمتى وجد رابط أو صلة بين المعلومة والشخص المتعلقة به، وكان بالإمكان التعرف عليه، شكلت هذه المعلومة إحدى المعطيات الشخصية، ما يعني أن المعطيات المجهولة أو التي تم تجهيلها les données (anonymes ou anonymisées) لا يشملها مفهوم المعطيات الشخصية⁵.

1 - صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، التواصل في الاقتصاد والإدارة والقانون، ص 127.

2 - صبرينة جدي، المرجع نفسه، ص 127.

3 - القانون المغربي رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذ الظهير الشريف رقم 15-09 المؤرخ في 18 فبراير 2009، منشور بالجريدة الرسمية رقم 5711، بتاريخ 23 فبراير 2009.

4 - القانون الأساسي رقم 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية، الرائد الرسمي للجمهورية التونسية، الصادر بتاريخ 30 جويلية 2004، النص الكامل للقانون على الموقع الإلكتروني: www.legislation.tn.

5 - أشرف البكوش، حماية الحياة الخاصة في القانون الجنائي، مذكرة ماجستير، كلية الحقوق والعلوم الاقتصادية والسياسية بسوسة، 2006/2007، ص 59.

ومن الناحية القانونية - وغير بعيد عن هذا المعنى- فقد أورد المشرع الجزائري تعريفا للبيانات الرقمية، حيث عبر عنها بـ "المعطيات المعلوماتية" وعرفها بأنها: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"¹.

أما البيانات الشخصية فلم يورد لها تعريفا خاصا بها، وهي بحسب اللجنة الوطنية للمعلوماتية والحريات "CNIL"²: كل معلومة تتعلق بشخص طبيعي معروف الهوية أو ممكن التعرف على هويته بصفة مباشرة أو غير مباشرة بالرجوع إلى رقم تعريفه أو إلى واحد أو مجموعة من العناصر التي تخصه..."³.

أو كما تعرفها اتفاقية 108⁴ "كل معلومة تتعلق بتحديد هوية الفرد، أو بفرد محدد".

ثانيا: أنواع البيانات الشخصية

يتبين من التعريف أنه يعد من قبيل البيانات أو المعطيات الشخصية، كل معلومة كيفما كان شكلها وبغض النظر عن دعامتها متى تعلقت بشخص طبيعي معرف أو يقبل التعريف، لتشمل كل المعطيات الفردية والمدنية والصحية والمالية.. الخ، بعضها يوصف بالمعطيات الحساسة، كتلك التي تظهر بشكل مباشر أو غير مباشر الأصل العرقي أو المعطيات المتعلقة بالآراء السياسية، والمعتقدات الدينية، أو الانتماء النقابي، وكذا المعطيات المتعلقة بالصحة أو الحياة الجنسية، تضاف إليها البيانات المتعلقة بالأحكام الجزائية، والتي تستوجب مستوى أعلى من الحماية⁵، ولأنه لا يمكن حصر كل البيانات أو المعطيات التي تعتبر شخصية، نذكر منها:

1.البيانات الشخصية المحددة للهوية

بالنظر إلى الوسائل والتقنيات المعلوماتية المتعلقة بتحديد هوية الأشخاص، نجد أن البيانات المحددة للهوية تنقسم إلى نوعين من البيانات:

1 - القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية / العدد 47.

2 - Commission Nationale de l'Informatique et Libertés.

3 - المادة الثانية من قانون 78-17 المؤرخ في 06 جانفي 1978 المتعلق بالمعلوماتية، الملفات والحريات.

4 - المادة 108 الفقرة الثانية من الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية، المجلس الأوروبي ستراسبورغ 1981.

5 - العربي جنان، معالجة المعطيات ذات الطابع الشخصي الحماية القانونية في التشريع المغربي والمقارن، مراكش، 2010، ص 41.

يتمثل النوع الأول في الحروف والأرقام والرموز، والتي تتمثل أهمها في كلمات المرور التي تسمح أو تمنع المستخدم من الولوج إلى الحاسوب الشخصي أو قاعدة البيانات أين يعمل أو الولوج إلى البريد الإلكتروني أو البيانات التي يقتضيها إتمام معاملة من معاملات التجارة الإلكترونية، أو تسجيل الدخول إلى منتدى أو حساب شخصي على موقع إلكتروني.

فيما يتمثل النوع الثاني في القياسات الحيوية، على غرار بصمة الإصبع، بصمة القزحية، البصمة الصوتية، بصمة أبعاد الكف، خط اليد (التوقيع)، بصمة الوجه... إلخ¹.

2. البيانات الشخصية الخاصة

يتعلق هذا النوع من البيانات بالحياة الخاصة للأفراد وتشمل كل البيانات التي من شأنها الكشف عن الأصل العرقي أو الآراء السياسية أو المعتقدات الدينية أو غيرها، وكذلك البيانات الشخصية المتعلقة بالصحة أو الحياة الجنسية، أو السوابق العدلية² المخزنة لدى المؤسسات العامة والخاصة في شكل قواعد بيانات، أو في خوادم الشبكات المعلوماتية³. وتعتبر قواعد البيانات لمختلف المنظمات مصدرا هاما لهذا النوع من البيانات، كذلك المواد الإعلامية المنشورة على صفحات شبكات التواصل الاجتماعي، والبيانات التي تقوم وكالات التحقيق والاستخبارات بتقصيها وجمعها.

الفرع الرابع: الأساس القانوني لحق الخصوصية في العالم الرقمي

لقد أضحت التكنولوجيا الحديثة سلاحا ذو حدين خاصة في مجال الحق الخصوصية، فبقدر التطور الهائل الذي مس حياة الأفراد وأسبغ عليه يسر ومرونة في التعامل والاتصال عبر شبكة الانترنت إلا أن هذا الأمر قد حمل في ثناياه مخاطر عديدة مست بخصوصيات الأفراد مما استدعى بذل الكثير من الجهود سواء على مستوى التشريعات الداخلية أو على المستوى الدولي الإرساء آليات الحماية ضد انتهاك حق الخصوصية، وهنا يثار التساؤل حول معالم الحماية التي رسمتها القواعد الدولية في ظل الاتفاقيات والمؤتمرات الدولية الرامية لحماية هذا الحق، أو الجهود الداخلية للدول في مسار تفعيل القواعد

1 - منصور بن محمد الغامدي، البيانات الحيوية، البصمة الصوتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، ط1، 2005، ص 06.

2 - المادة 108 الفقرة السادسة من الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية، مرجع السابق.

3 - إيان ليه: الإشراف على استخدام البيانات الشخصية، مقال متاح على الرابط:

www.dcaf.ch/content/download/.../1/...Tool_6_intel_over_AR.pdf.

العامة العقابية بما يتماشى وحماية حق الخصوصية في المجال الإلكتروني أو استحداث تشريعات خاصة تغطي هذه الحماية.

وعلى غرار التشريعات المقارنة افرد القانون الجزائري حماية جنائية ومدنية لكل من تتعرض حياتهم الخاصة للانتهاك. كما أكد الدستور الجزائري على انه لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه وسرية مراسلاته واتصالاته وحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي¹. وقد جرم قانون العقوبات المساس بحرمة الحياة الخاصة للأشخاص، بالنص في المادة 303 مكرر على عقوبة الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج، على كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت بدون إذن صاحبها ورضاه.

أولاً: حق الخصوصية في ظل الحماية الدولية

مما لا شك فيه أن الحماية الدولية لحقوق الإنسان قد أخذت أهمية واسعة نظراً للدور الذي تقوم الوثائق والمؤتمرات الدولية في ترسيخ تلك الحقوق ودعمها على المستوى الإقليمي في ظل النظام القانوني للدول.

1-حماية حق الخصوصية في ظل المؤتمرات الدولية والإقليمية

لقد تبنت الجمعية العامة للأمم المتحدة توصيات المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الأفراد المنعقد في طهران عام 1986، بحيث خرج بجملته من التوصيات التي تبرز خطر الحاسبات الإلكترونية على الحياة الخاصة وضرورة إيجاد آليات على المستوى الإقليمي أو الدولي لمحاربة أجهزة التجسس².

وأما على مستوى الإقليم العربي فلقد انعقد العديد من المؤتمرات الدولية التي عنت بمكافحة الجرائم المعلوماتية ومنها انتهاك حق الخصوصية ومن أبرزها:

-المؤتمر الدولي الأمن المعلومات الإلكتروني المنعقد بمسقط سنة 2005 ركز المؤتمر على بحث ودراسة أهم التهديدات الإلكترونية والمخاطر التي تمس باقتصاديات الدول وتحد من التنمية، وعمل على الخروج

¹ - محمد عبيدي، مرجع سابق.

² - يونس خالد عرب، جرائم الحاسوب (دراسة مقارنة)، رسالة ماجستير، جامعة الأردن، 1994، ص 125.

بتوصيات خاصة بالتأكيد على التعاون الدولي لمكافحة الجريمة ووضع سياسات مشتركة للقضاء على الآثار السلبية لتكنولوجيا المعلومات التي تهدد الحياة الخاصة¹.

-المؤتمر الدولي الأول لمكافحة جرائم تقنية المعلومات المنعقد بالشارقة بالإمارات العربية المتحدة سنة 2006 يعتبر هذا المؤتمر شاملا من حيث دراسة وبحث إشكالية الجرائم المعلوماتية من حيث المفهوم والمكافحة على المستوى الوقائي والعلاجي وفتح النقاش لدارسة التوجهات المستحدثة في هذا المجال والسعي لتبادل الخبرات في مجال مكافحة جرائم تقنية المعلومات².

يصنف البعض البيانات في العصر الرقمي بمثابة الذهب لقيمتها السوقية والتي قد تستغلها الشركات التجارية للترويج لمنتجاتها واستقطاب اكبر عدد ممكن من الزبائن وبالنظر لحساسية بعض البيانات التي يعد جمعها وتقاسمها دون موافقة صاحبها، انتهاكا لحقه في حماية خصوصيته، أشار تقرير صادر عن مجلس حقوق الإنسان التابع للأمم المتحدة، إلى أن نقل المعلومات الشخصية وتبادلها عن طريق الوسائل الالكترونية، لاسيما في إطار التعاملات التجارية التي يجريها المستهلك للحصول على سلع أو خدمات، ينبغي أن تتم في سياق " تسوية واعية، يقدم الأفراد بموجبها طوعية معلومات عن أنفسهم وعلاقاتهم مقابل الوصول الرقمي إلى السلع والخدمات والمعلومات. ولكن تثار أسئلة خطيرة عن مدى معرفة المستهلكين حقا، لأي بيانات يتقاسمونها وكيف ومع من يتقاسمونها وكيف ستستخدم³. وحذر ذات التقرير من أن البيانات الكبيرة التي يتم جمعها من الصعب أن يبقى مصدرها مجهولا، وانه لا فرق بين تلك البيانات التوصيفية التي تعطي نظرة عن سلوك الفرد وعلاقاته الاجتماعية وافضلياته الخاصة وهويته التي تسمح بالتوصل إلى استنتاجات دقيقة بشأن الحياة الخاصة للأشخاص الذين احتفظ ببياناتهم، وبين بيانات الاتصالات التي يتم التقاطها وجمعها والاحتفاظ بها فكلهما " يعد بمثابة تدخل في الخصوصية سواء أتم الاطلاع على تلك البيانات واستخدامها لاحقا أو لا، وحتى مجرد احتمال التقاط معلومات الاتصالات ينشئ تدخلا في الخصوصية⁴.

¹ - ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1983، ص 90.

² - محمود إبراهيم غازي، مرجع سابق، ص 204.

³ - تقرير صادر عن مجلس حقوق الإنسان موسوم بـ: "الحق في الخصوصية في العصر الرقمي " - رمز التقرير A/HRC/27/37 بتاريخ 2014/06/30، ص 7.

⁴ - نفس المرجع - ص 9.

وتوجد العديد من الأساليب والطرق التقنية القادرة على جمع وتحليل واستخدام البيانات الشخصية ولعل الطريقة الأكثر انتشارا هي تقنية ملفات الارتباط (Cookies) التي تقوم بمتابعة المستهلك عبر الانترنت، فهي تمكن المواقع الالكترونية من جمع المعلومات عن المستخدمين، الخاصة بنوع الجهاز والمعالج ورقم IP الخاص بالمستخدم وطريق الاتصال بالإنترنت والمواقع التي قام بزيارتها وعدد الساعات التي يستغرقها المستهلك في تصفح هذه المواقع وطبيعة اهتماماته وماهية الأشياء التي يبحث عنها وما يقوم بشرائه عبر المنصات الرقمية، لاسيما بواسطة الهاتف الخليوي، مما يساهم في تزويد المعلنين والمسوقين بمعلومات تستغل في توجيه الإعلانات والإشارات، بما يناسب مع رغبات واختيارات المستهلكين، مما قد يشكل انتهاكا لحق المستهلك في عدم التعرض لخصوصيته¹.

ويعتبر القانون العام الأوروبي الخاص بالخصوصية وحماية البيانات الشخصية (GDPR) الذي اقر عام 2018، الإطار الأكثر مصداقية لحماية الخصوصية ومحاولة تمكين المستخدمين من السيطرة على بياناتهم الشخصية والرقمية. وقد حدد هذا القانون سبعة مبادئ لحماية البيانات الشخصية والمساءلة عن خرقها وانتهاكها وهي²:

- التعامل مع البيانات الشخصية بصورة قانونية، شرعية وشفافة وعادلة تجاه صاحب البيانات،
- تحديد الغرض المباشر والدقيق من معالجة البيانات وإعلام صاحب البيانات به بعد جمعها،
- تقليل حجم البيانات التي تجمع واقتصارها على المعلومات الضرورية للغرض المحدد،
- الحفاظ على دقة البيانات الشخصية وتحديثها، بحيث لا تكون مغلوطة ومضللة،
- وضع قيود واضحة وصارمة على تخزين البيانات الشخصية، الذي يكون للضرورة المحددة بغرض،
- الالتزام بالنزاهة والسرية التامة في معالجة البيانات بما يضمن الأمان والسلامة كالتشفير،
- مساءلة مراقب البيانات، المسؤول عن جمع وحفظ ومعالجة البيانات، أمام القانون.

¹ - دراسة استكشافية عن واقع الخصوصية وحماية البيانات الرقمية في فلسطين، المركز العربي لتطوير الإعلام

الاجتماعي، أوت 2021، ص 10.

² - نفس المرجع، ص 12 و 13.

2- حماية حق الخصوصية في ظل الاتفاقيات الدولية

تعتبر الاتفاقيات الدولية ذات دور مهم في مسألة التنسيق بين التشريعات المختلفة للدول والجدير بيان أبرز صور التعاون الدولي في مجال حماية حق الخصوصية في المجال الرقمي من الاعتداءات الإلكترونية.

-الاتفاقية الأوروبية لحماية الأفراد في مجال المعالجة الآلية للبيانات الشخصية.

جاءت الاتفاقية الأوروبية لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية رقم 108 المنعقدة في 28 يناير 1981 في ظل الانفتاح الواسع للإنترنت الذي أتاح التبادل الواسع لمختلف أنماط المعلومات وخلق بيئة للاستثمار والأعمال فيما يعرف بالأسواق الافتراضية أو بيئة الأعمال الإلكترونية، وبحيث أن التقارير الصادرة عن هيئات حماية الخصوصية قد أثبتت عدم أمان العمليات الإلكترونية الصادرة عن الأفراد وخاصة في إطار تجميع وتحليل المعلومات الشخصية كحزمة واحدة للوصول إلى حقائق عن الشخص تساهم في تنفيذ الاعتداء على حق الخصوصية، فلقد كفلت الاتفاقية ضمان حقوق الفرد بغض النظر عن الجنسية أو الإقامة واحترامها في مواجهة الاستخدام الآلي للمعلومات ذات الطابع الشخصي¹.

اتفاقية بودابست لسنة 2001 المتعلقة بالإجرام المعلوماتي

تعد هذه الاتفاقية أول اتفاقية ذات طابع دول يتبناها المجلس الأوروبي في هذا المجال، بحيث ضمت العديد من الدول الأوروبية وغير الأوروبية، وقد دخلت حيز التنفيذ في سنة 2004.

أقرت الاتفاقية في المذكرة التفسيرية لها بالدور الذي تسعى من خلاله مكافحة الجرائم الناشئة عن الأثر السلبي لتكنولوجيا المعلومات، لتخصص في الباب الثاني من الاتفاقية بعض النماذج البارزة للاعتداء على حق الخصوصية في العالم الرقمي²، تجسدت في الباب الثاني المعنون «الإجراءات الواجب اتخاذها على المستوى الإقليمي» وعلى سبيل المثال ما جاء في فحوى المادة 2 التي نظمت مسألة الولوج غير القانوني لأجهزة الحاسوب بدون وجه حق، ونصت على الشروط الواجب توافرها لقيام هذه الجريمة باعتبارها تتطوي على تهديد لسرية وسلامة النظم والبيانات المعلوماتية للأفراد، كما أقرت ضرورة

¹ - Daniel Kaplan, Informatique, libertés, identities, Fyp Edition 1^{er} Avril 2010, P10

² - خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص 276.

تكريس التشريعات الداخلية المجموعة من القواعد في النظم العقابية الخاصة بها بغية وضع إجراءات أمنية فعالة ضد تلك الانتهاكات¹.

وكذا جاءت الاتفاقية في نص المادة على النص على جريمة الاعتراض القانوني غير القانوني باستخدام الوسائل الفنية للبيانات المتداولة إلكترونياً بين الحواسيب عبر شبكة الانترنت، واختصت المادة الرابعة بالنص على ضرورة توحيد أطراف الاتفاقية للجهود بغية تبني الإجراءات التشريعية التي تجرم الاعتداء على سلامة البيانات من أجل ضمان سلامة المنظومة البيانية للاتصالات الإلكترونية².

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010

تبنت جامعة الدول العربية أول اتفاقية عربية لمكافحة جرائم تقنية المعلومات في 21 يناير 2010، وجاءت الاتفاقية في إطار تعزيز التعاون ودعم الدول العربية لبعضها البعض في مجال مكافحة تقنية المعلومات بحيث سارت الاتفاقية على نهج الاتفاقية العالمية بودابست من خلال إقرارها في الفصل الأول بالهدف من الاتفاقية المتمثل في تعزيز التعاون والدعم بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم وحفاظاً على أمن الدول العربية في هذا المجال.

ولقد أقرت الاتفاقية على التزام الأطراف بتجريم شتى أساليب الاعتداء على حقوق الأفراد في المجال الإلكتروني المنصوص عليها الفصل الثاني منها والمعنون «بالتجريم» والذي ركزت فيه على تجريم الدخول غير المشروع وكذا الاعتراض غير القانوني للبيانات الشخصية والاعتداء على سلامتها، لتأتي في نص المادة 14 منها وتنص بشكل مباشر على تجريم الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات³.

حق الخصوصية في ظل الحماية الداخلية للتشريعات المقارنة

بعد الحراك التشريعي الدولي الساعي إلى ترسيخ المبادئ الأساسية لمكافحة جرائم تقنية المعلومات بشكل عام ومحاربة الانتهاكات الماسة بحق الخصوصية في المجال المعلوماتي بشكل خاص، جاء دور التشريعات الداخلية للدول لتأخذ على عاتقها تأسيس قواعد حماية ضد الاعتداءات الماسة بهذا الحق.

1 - محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، سنة 2016، ط1، ص 161.

2 - هلالى عبد الله أحمد، جرائم المعلوماتية العابرة للحدود (أساليب المواجهة وفقاً لاتفاقية بودابست)، دار النهضة العربية، مصر، ط1، سنة 2007، ص 22.

3 - محمود إبراهيم غازي، مرجع سابق، ص 235.

وإن كان من الواضح بعد استقراء العديد من النصوص التشريعية العقابية في مجال مكافحة الاعتداء على الحق في الحياة الخاصة نجد أن طائفة من التشريعات قد عملت على تبني نصوص خاصة لتكفل حماية هذا الحق بعيدا عن النصوص العقابية في القواعد العامة، أما البعض الآخر فقد اكتفى بتعديل التشريع العقابي بما يتوافق ومحاربة جرائم تقنية المعلومات المرتكبة عبر شبكة الانترنت بشكل عام وحق الخصوصية بشكل خاص.

ثانيا: حق الخصوصية في العالم الرقمي في ظل التشريعات الغربية عمل التشريع الفرنسي على التصدي لجرائم انتهاك الخصوصية في المجال المعلوماتي بعد إصدار جملة من التشريعات التي تبناها في مجال نظم المعالجة الآلية للمعلومات والتي مرت على مرحلتين:

الأول: بموجب القانون رقم 78-17 الصادر في 1978/10/06 الخاص بحماية البيانات الاسمية للمواطنين في مواجهة نظم المعالجة الآلية للمعلومات.

الثاني: القانون رقم 88-19 الصادر في 88/01/05 بشأن جرائم الغش المعلوماتي ولقد حرص المشرع في كلا القانونين على النص على الحلول المناسبة لمواجهة الجرائم الناشئة عن الحاسبات الإلكترونية وخطورتها على الحياة الخاصة والحريات العامة والفردية¹.

وحرص المشرع الفرنسي على مواصلة مكافحة الاعتداءات الواقعة على حق الخصوصية في إطار التشريعات العقابية بحيث كرس جملة من المواد بموجب قانون العقوبات الجديد رقم 684 - 92 الصادر في 1992/7/22 والذي دخل حيز التنفيذ ابتداء من 1994/03/01.

وتضمن القانون أحكاما جديدة لمواجهة ظاهرة الإجرام المعلوماتي تحت عنوان: الاعتداء على نظم المعالجة الآلية للمعلومات².

ولقد جرم المشرع أفعال المساس بالحق في حرمة الحياة الخاصة تحت عنوان الاعتداء على الحياة الشخصية فنجدته خطى خطوة سباقة في مجال حماية الحياة الخاصة من خلال توفير آليات الحماية الوقائية التي تهدف منع الاعتداء على الحق بالإضافة إلى الحماية العلاجية وعلى رأسها حماية الضحايا وفقا لدعاوى التعويض³.

1 - أحمد فتحي سرور، الحق في الحياة الخاصة، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، السنة 54،

2 - أسامة فايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة في القانون الفرنسي والأمريكي وفقا لآخر التعديلات التشريعية، دار النهضة العربية، مصر، سنة 2008، ص 86.

3 - عمر أبو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونيا، أطروحة دكتوراه، جامعة القاهرة، 2009، ص 163.

أما على المستوى التشريعات الأنجلوسكسونية فلقد حذت حذو التشريعات اللاتينية في مجال مكافحة الاعتداء على الحق في الخصوصية، بحيث أصدر المشرع الإنجليزي قانون حماية البيانات منذ 1984 الذي حث على تأمين الحصول على البيانات الشخصية المخزنة الأغراض المعالجة بأسلوب صحيح ولتحقيق أغراض مشروعة، وكذا المشرع الأمريكي سعى إلى تكريس هذه الحماية وفق جملة من الإصدارات التشريعية على رأسها قانون الخصوصية سنة 1974، بحيث قرر من خلاله الكثير من الضمانات في مواجهة المخاطر التي تتعرض لها بنوك المعلومات، وكذا نجد القضاء الأمريكي قد تأثر بجملة التعديلات الدستورية فأعطى للمحاكم مساحة واسعة لتفسير نصوص الدستور في نطاق حماية الحقوق والحريات وبالأخص الحق في الخصوصية¹.

ثالثاً: الحق في الخصوصية في إطار التشريعات العربية

سعت تشريعات الدول العربية كغيرها من التشريعات الدولية نحو إصدار قوانين خاصة بحماية الحق في الخصوصية لتحقيق الانسجام مع توجهات المنظمات والاتفاقيات الدولية، إلا أنه يؤخذ عليها أنها تسير بخطوات متواضعة وبطيئة في مجال التصدي لاختراق وسرقة البيانات الشخصية وعمليات التجسس على الحياة الخاصة للأفراد واستخدام المعلومات الشخصية لأغراض غير مشروعة وغيرها من الاعتداءات الإلكترونية على الحياة الخاصة في العالم الرقمي، ولا ربما يرجع ذلك لضعف الإرادة التشريعية في مواكبة المستجدات في مجال التشريع الإلكتروني، وفي هذا الإطار سنتطرق لموقف التشريع الجزائري وبعض التشريعات العربية المقارنة.

رابعاً: موقف المشرع الجزائري من حماية حق الخصوصية

من الاعتداءات الإلكترونية عمل المشرع الجزائري كغيره من التشريعات المقارنة على الاعتراف بحق الخصوصية بشكل عام كمبدأ دستوري من خلال نص المادة 39 بنص صريح: (لا يجوز انتهاك حرمة المواطن الخاصة وحرمة شرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة).

وقد كرس مبدأ الحماية الجنائية بموجب نص المادة 303 من قانون العقوبات التي نصت على من يعاقب بالحبس من 6 أشهر إلى 3 سنوات كل من تعمد المساس بحرمة الحياة الخاصة بأي تقنية كانت وذلك:

¹ - جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، مصر، سنة 2000، ص 117.

-النقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

-النقاط أو تسجيل أو نقل صورة الشخص في مكان خاص بغير إذن صاحبها أو رضاه ويعتبر هذا النص قد حمل في طياته الحماية المرنة التي تمتد إلى أي طبيعة الحق الخصوصية أو الحديث وهذا باستخدام عبارة أي "تقنية كانت"¹.

وعلى الرغم من النص غير المباشر على حق الخصوصية إلكترونياً نجد المشرع لم يتجه إلى إصدار قانون بالحماية للخصوصية في المجال الإلكتروني، إلا أن المشرع اكتفى بمواكبة محاربة جريمة المساس بالحق في الخصوصية في العالم الرقمي بموجب القانون رقم 15-04 المتضمن تعديل قانون العقوبات في القسم المعنون: «المساس بأنظمة المعالجة الآلية للمعطيات» من خلال نص المادة 39 « يعاقب بالحبس من 3 أشهر إلى سنة أو بغرامة من 50 ألف إلى 100 ألف كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك»، وكذا جرم عمليات تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو إفشاء أو استعمالها لأي غرض كل المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم.

ولقد وفر المشرع الحماية الجنائية لحق الخصوصية بموجب المادة 4 من القانون 04 - 09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال²، وهذا بضمان عدم المساس بالحياة الخاصة للأفراد في حالة قيام السلطات المختصة بالقيام بعمليات المراقبة لكل الاتصالات الإلكترونية بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة.

خامساً: موقف التشريعات العربية المقارنة من حماية حق الخصوصية من الاعتداءات الإلكترونية

لقد عملت العديد من التشريعات العربية على التصدي لجريمة الاعتداء على حق الخصوصية بحيث اكتفت غالبية التشريعات محاولة تطويع النصوص العقابية التقليدية على الأنماط المستحدثة من الجرائم المعلوماتية وعلى رأسها انتهاك حق الخصوصية، إلا أنه بالمقابل سعت بعض التشريعات الأخرى على خطو خطوات واسعة في مجال مكافحة الجريمة الواقعة على هذا الحق بإصدار

1 - الذهبي خدوجة، مرجع سابق ص 153.

2 - القانون 04-09 المؤرخ 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، عدد 47 المؤرخة في 2009/08/16.

تشريعات خاصة بحماية البيانات المعالجة آلياً أو تخصيص قوانين لمحاربة جرائم تقنية المعلومات وإعطاء مساحة لمسألة الحماية الجنائية ضد الاعتداءات على الحق في الخصوصية في المجال الرقمي، فلقد أصدر المشرع السعودي قانون مكافحة

الجرائم المعلوماتية لسنة 2007 وتضمن القانون جملة من المواد تتعلق بحماية البيانات الشخصية المعالجة آلياً¹.

كذا أصدر المشرع الإماراتي المرسوم رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بحيث جرم هذا الأخير في بعض مواد الأفعال التي تتعلق بالمساس بالبيانات الشخصية المعالجة آلياً ومثاله المادة 21 بحيث عاقبت مستخدم الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً إما عن طريق الاعتراض أو التسجيل أو نشر صور أو بيانات شخصية.

كما أصدر المشرع البحريني القانون رقم 60 لسنة 2014 في شأن جرائم تقنية المعلومات وتضمن القانون تجريم عدة صور للاعتداء على حق الخصوصية وخاصة في إطار إساءة استخدام البيانات الشخصية للأفراد بقصد التشهير والابتزاز².

المطلب الثاني: مبررات حماية حق الخصوصية الرقمية

مع تزايد التقنيات الحديثة زادت المخاطر على الحق في الحياة الخاصة وأضحى الفرد مقيداً في تعاملاته من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة الوسائل المعلوماتية كتقنيات المراقبة أو التجسس والمساس بالمعطيات الخاصة بالأفراد وهي جميعها تمثل تهديداً مباشراً على الحياة الخاصة والحريات الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات لا سيما إذا استغلت لغايات خارجة عن إرادة صاحبها ودون علمها، وعلى هذا الأساس نجد أن مبررات حماية الحق في الخصوصية في المجال الرقمي وهي على الآتي:

1- اتساع شبكة الانترنت

إن الواقع يثبت أن أهم التقنيات التي تتحكم في مجموع التعاملات الإلكترونية تعتمد على شبكة الانترنت وهذه الأخيرة ليست بمنأى عن ولوج أي متطفل أو معتدي يستغل شتى الاتصالات

¹ - عمر أبو الفتوح عبد العظيم، مرجع سابق، ص 179.

² - محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، ط 1، ص 220.

التي تترك آثار حتى دون علم مستخدم الشبكة، فتدفق المعلومات والاتصالات عبر الحدود دون أي اعتبار لحدود جغرافية أو سياسية، بحيث يعمل الأفراد على تبادل المعطيات الخاصة بهم لجهات مختلفة وفي قنوات عديدة داخلية وخارجية، وربما جهات ليس لها محل معنون وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها الحماية القانونية للبيانات الشخصية¹.

2- الطبيعة الخاصة لقنوات التعامل الإلكتروني

هذه الطبيعة الافتراضية التي تنفذ إلى المادية تجعل من الشخص وهو بصدد استخدام شبكة الانترنت يتوقع قدرا من الخفية في نشاطاته أكثر مما هو عليه الحال في العالم الواقعي، بينما الواقع يثبت عكس ذلك على اعتبار أن التعاملات الإلكترونية تترك آثارا ودلالات على شكل سجلات رقمية حول الموقع المزار والأمر التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بشرائها، مما يجعله عرضة للقرصنة ثم الاستغلال غير المشروع لها².

3- فقدان المركزية وآليات السيطرة في قنوات التعامل الإلكتروني

يكتسب حق الخصوصية في إطار العالم الرقمي نوعا من التميز إذ أن إقرار قانون فاعل نوعا يكرس من وجود إستراتيجية ملائمة لحماية حق الأفراد بعيدا عن العالم الرقمي قد يكون من السهولة بحيث يمكن للدولة وضع رقابة على الاعتداءات المختلفة، إلا أن الأمر لن يكون بذات السهولة إذا ما تعلق الأمر بحماية حق الخصوصية المعلوماتية لأن لها ارتباط مباشر بعالم افتراضي شاسع يرتبط بشبكة الانترنت اللامتناهية الحدود، وهنا يحتدم الصراع على السيطرة على الانترنت من خلال الصعوبة في التحكم في مركزية أسماء النطاقات وعناوين المواقع وغيرها، وهو ما يوسع من دائرة اختراق حق الأفراد ويصعب من الحماية ضد أي انتهاكات لخصوصياتهم³.

¹ - جميل عبد الباقي الصغير، مرجع سابق ص 40.

² - عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية)، دار النهضة العربية، مصر، سنة 2004، ص 398.

³ - أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، مصر، سنة 2000، ص 395.

المبحث الثاني: أثر تكنولوجيا المعلومات على الحق في الخصوصية.

تعتمد المجتمعات الحديثة كلياً على تكنولوجيا المعلومات، في تسيير الشؤون العامة والخاصة، فلا يمكن للأفراد في هذا العصر الاستغناء عن هذه التقنية؛ فالبريد الإلكتروني، وبطاقات التعريف الإلكترونية ووسائل الدفع الإلكترونية، والتواصل والحوار الإلكتروني والتسليم كذلك، فهذه التكنولوجيا الحديثة أثرها على مختلف مناحي الحياة الاجتماعية والاقتصادية والثقافية... الخ، ويبدو أن لها أثراً خاصاً على الحق في الحياة الخاصة، يمكن تبيينه في ظهور مفهوم جديد للخصوصية هو الخصوصية المعلوماتية، إلى جانب المفاهيم التقليدية، كما أن إساءة استخدام هذه التكنولوجيا، أوجد مخاطر غير مسبقة وجدت في البيئة الإلكترونية فضاء خصبا لانتهاك الحياة الخاصة قد لا يدرك البعض خطورتها.

المطلب الأول: ظهور مفهوم الخصوصية المعلوماتية (خصوصية المعلومات)

ارتبط ظهور مفهوم الخصوصية المعلوماتية في السبعينيات، مع ما تقوم به الجهات الحكومية من جمع وتخزين البيانات الشخصية على أجهزة الحاسوب، باعتبارها الوحيدة التي كانت تملك تلك الأجهزة وقتها؛ فانتشر الحديث عن الخطر الكبير الذي يتهدد الحريات العامة، وزاد التخوف من الانتهاكات والاعتداءات المحتملة؛ بسبب المقدرة الهائلة لنظم المعالجة الإلكترونية في الوصول إلى المعلومات المتعلقة بالأفراد، واستغلالها في غير الأغراض التي تجمع من أجلها، ما أطلق عليها بالقوى الرقابية المحتملة على المعلومات الشخصية¹.

تغير الواقع التكنولوجي منذ الثمانينيات، فيما يتعلق بالجهات التي تملك وتسيطر على نظم الحاسوب؛ بسبب إطلاق الحواسيب الشخصية وانتشارها، وظهور شبكات المعلومات كنتيجة للاندماج بين تكنولوجيا المعلومات والاتصالات؛ لتصبح المعالجة الآلية للمعلومات المتعلقة بالأفراد تتم من قبل هيئات عامة وخاصة ولأغراض مختلفة، بل تحولت هذه المعلومات إلى سلعة يتم جمعها وتداولها دون علم أصحابها، بهدف توجيه الدعاية أو لقياس المؤشرات الاقتصادية، أو مراقبة الأفراد ورصد مختلف سلوكياتهم لأغراض أمنية. ما أكد أن الحياة الخاصة للأفراد إلى جانب باقي الحقوق والحريات بحاجة للحماية في عصر المعلومات².

¹ - يونس عرب، مرجع سابق ص 60.

² - علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة - دراسة مقارنة، منشورات زين الحقوقية، بيروت، 2013، ص 408 و 409.

ارتبطت ولادة مفهوم الخصوصية المعلوماتية بالخشية من مخاطر جمع، ومعالجة المعطيات المتعلقة بالأفراد الأغراض غير معلنة أو غير مشروعة، أو إساءة استعمالها أو تحويلها إلى جهات أخرى، وحقوق أصحاب المعطيات ومدى سيطرتهم عليها¹.

وجهت العناية إلى موضوع حماية المعطيات المتعلقة بالأفراد من خطر استخدام أنظمة حول المعالجة الآلية في مطلع الستينيات من القرن الماضي، كأولى الموضوعات التي أثارت مسألة تكنولوجيا المعلومات وخضوعها للنظام القانوني.

يعود الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات إلى مؤلفين أمريكيين هامين في هذا المجال هما:

الأول: الخصوصية والحرية privacy and freedom لصاحبه Alan Westin سنة 1967².

الثاني: الاعتداء على الخصوصية The Assault on privacy لمؤلفه Miller Arthur Raphael سنة 1971³.

عرف الأول خصوصية المعلومات على أنها: "حق الفرد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين"، بينما عرفها الثاني ب: قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم."

إلى جانب الدراسة التي قام بإعدادها Michel James سنة 1994 تحت إشراف اليونسكو بعنوان "الخصوصية وحقوق الإنسان"، privacy and human rights والتي تعد إحدى أوسع الدراسات بشأن المسائل المتصلة بالخصوصية وحقوق الإنسان في ضوء التطورات التقنية الحديثة، حيث استعرض الصعوبات والتباينات الثقافية في استخدام المصطلح واختلاف المفهوم القانوني للخصوصية في المعلومات بين النظم القانونية⁴.

فالمقصود بخصوصية المعلوماتية أو خصوصية المعلومات: "حق الفرد على بياناته الشخصية أو البيانات ذات الطبيعة الشخصية مما يسمح بمواجهة الاعتداءات الواقعة عليها، وتنظيم الحق على البيانات الشخصية وسيطرة صاحبها عليها⁵"، مع ملاحظة أنه من الشائع استخدام مصطلح الخصوصية مستقلاً ومنفرداً دون

1 - العربي جنان، مرجع سابق ، ص 17 و18.

2 - صبرينة جدي، مرجع سابق ، ص 126.

3 - صبرينة جدي، مرجع سابق، ص 126.

4 - صبرينة جدي، المرجع نفسه ، ص 126.

5 - أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، رسالة دكتوراه، جامعة المنصورة، 2006/2005، ص

إحاقه بالبيانات في البيئة الإلكترونية للدلالة على حماية البيانات، وكذلك في الدراسات الأكاديمية والتقنية، دون أن يعني ذلك ترادفاً أو تطابقاً بين خصوصية المعلومات والحق في الخصوصية، فالأولى لا تشكل إلا إحدى صور الثانية فإلى جانب خصوصية البيانات نجد:

1- الخصوصية الجسدية أو المادية: والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم.

2- خصوصية الاتصالات.

3- الخصوصية المكانية أو خصوصية المكان¹.

فموضوع الخصوصية المعلوماتية هي البيانات أو المعطيات الشخصية.

المطلب الثاني: مخاطر تكنولوجيا المعلومات على الخصوصية المعلوماتية.

لا يمكن إنكار الآثار الإيجابية العديدة لاستخدام الحاسوب وشبكات الاتصال على جميع الأصعدة وفي مختلف المجالات، لكنها لا يجب أن تلهينا عن مخاطره.

صرح الفقيه Miller Arthr سنة 1967معبراً عن قلقه من ما يمكن أن يحدثه الحاسوب بالحياة الخاصة، وهي المقولة التي تتكرر دائماً عند الحديث عن الخصوصية والمعلوماتية، والتي تعبر عن وضعية الحياة الخاصة في عصر تكنولوجيا المعلومات: " إن الحاسب بشرأته التي لا تشبع للمعلومات، والسمعة التي ذاعت حول عدم وقوعه في الخطأ، وذاكرته التي لا يمكن لما يختزن فيها أن ينسى أو يضيع، قد يقلب حياتنا رأساً على عقب، ليخضع فيه الأفراد لنظام رقابة صارم يتحول المجتمع بذلك إلى عالم شفاف تصبح فيه بيوتنا ومعاملتنا المالية وحالتنا العقلية والجسمانية عارية لكل مشاهد عابر....² فمصدر الخطر ليس تكنولوجيا المعلومات وتطبيقاتها، وإنما إساءة استخدامها هو مصدر الخطر، والذي يتجلى في ما يأتي:

الفرع الأول: بنوك المعلومات وقواعد البيانات.

اتجهت أغلب الدول بمختلف هيئاتها ومؤسساتها إلى إنشاء قواعد للبيانات لتنظيم عملها، فانتسح على نحو كبير استخدام الحاسبات لتجميع وتخزين ومعالجة البيانات الشخصية، لأغراض متعددة فيما يعرف ببنوك المعلومات أو المراكز الوطنية للمعلومات.

1 - يونس عرب، مرجع سابق، ص 19.

2 - صبرينة جدي، مرجع سابق، ص 128.

بنوك المعلومات مجموعة من البيانات أو المعلومات المنظمة بطريقة خاصة، في سجلات أو ملفات تسمح برامج الحاسوب من البحث عنها، واسترجاعها ومعالجتها، وتمكن من الوصول إلى محتواها، وإدارتها وتحديثها بسهولة، والتي تكون قاعدة بيانات، ويتكون بنك المعلومات الواحد من مجموعة من قواعد البيانات¹.

تستخدم هذه التقنية في مجال تنظيم الدول الشؤون الأفراد، الاقتصادية والاجتماعية وغيرها، التي قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع معين؛ كبنوك المعلومات القانونية، أو بنوك عامة، وإما مهيأة للاستخدام الوطني العام أو مستخدمة على نحو خاص، كمراكز وبنوك المعلومات للشركات المالية، كما قد تكون محلية أو عالمية، فالكثير من المؤسسات الحكومية التابعة لوزارات العدل، أو الداخلية أو الصحة، تعتمد تأسيس بنوك للمعلومات، من خلال جمع بيانات عديدة ومفصلة عن الأفراد: كالوضع الصحي والتعليمي والعائلي والقانوني².

الأمر الذي يجعل فرصة الوصول إلى هذه البيانات على نحو غير مشروع، أو استخدامها في غير الغرض الذي جمعت من أجله، ويفتح المجال واسعا لإساءة استخدامها، أو توجيهها للتوجيه الخاطئ لمراقبة الأفراد، وتعرية خصوصياتهم.

كما أن بنوك المعلومات تجعل المعلومات الشخصية، التي كانت منعزلة ومتفرقة التوصل إليها صعبا أو متعذرا، مجمعة ومتوافرة بشكل كامل، وسهلة المنال يمكن تحميلها وتخزينها في بضع ثوان، لتزيد شبكات الاتصال الطريق السريع للمعلومات الأمر سوءا بما تسمح به من اختراق وتجسس إلكتروني، عند عمليات الربط بقواعد البيانات أو عند عملية نقل وتحويل البيانات، إلى جانب خطر آخر لبنوك المعلومات على الحياة الخاصة، والمتمثل في احتوائها على بيانات غير دقيقة أو معلومات غير كاملة لم يتم تحديثها، بما يكفل تعديلها وتصويبها³.

الفرع الثاني: تصفح المواقع الإلكترونية على الانترنت.

إن المتصفح للمواقع الإلكترونية على شبكة المعلومات يتوقع قدرا من الخفية أو السرية أكثر مما يتوقعه في الواقع المادي، حيث يمكن ملاحظة وجوده ومراقبته من قبل الآخرين، فطالما لم يقدم بيانات تخصه أو استعمل اسم مستعارا، فإنه لا أحد يمكن أن يتعرف عليه أو يكتشف ما يفعل، لكن الأمر

1 - نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 167.

2 - عمدت الجزائر إلى إنشاء العديد من قواعد البيانات كالسجل الوطني الآلي للحالة المدنية بموجب القانون رقم 08-14 المعدل والمتمم للأمر 20-70 المتعلق بالحالة المدنية، والسجل الوطني الآلي للسوابق القضائية بموجب نص المادة 620 مكرر قانون الإجراءات الجزائية، وقواعد بيانات الضمان الاجتماعي وتعتمد إنشاء قاعدة للبيانات الجينية ... الخ

3 - أيمن عبد الله فكري، مرجع سابق، ص 502 و 503.

على غير ذلك، فنظام الخوادم وبرامج إدارة الشبكة تعمل على تسجيل قدر كبير من المعلومات عن كل مستخدم أو مشترك وعن كل حركة داخل فضاء الشبكة، فالإبحار على الشبكة يترك لدى كل موقع تتم زيارته كما من المعلومات، تسمح بالتعرف على المستخدم، تعرف بمعلومات رأس الصفحة، وهي التي يزود بها حاسوب المستخدم الحاسوب الخادم أو مستضيف الموقع عند كل اتصال، وتتضمن:

- عنوان بروتوكول الانترنت الخاصة بالمستخدم (IP) وهو رقم يحدد هوية كل جهاز. معلومات عن نظام التشغيل والتجهيزات المادية المستخدمة.

- وقت وتاريخ الزيارة - مواقع الانترنت التي تمت زيارتها - والوقت الذي تم قضاؤه في كل صفحة¹.

أما المواقع التفاعلية ومنتديات الحوار فتتطلب من المستخدم ملأ نموذج أو استمارة تتضمن معلومات مختلفة كالاسم والعمر، والجنسية ومكان الإقامة، والمستوى التعليمي، وعنوان البريد الالكتروني وحتى هواياته واهتماماته، سواء كان ذلك للاشتراك بخدمة معينة أو للانضمام إلى مجموعة حوار أو حتى لإجراء تعليق، كما تشكل مواقع التواصل الاجتماعي وأشهرها الفيسبوك خطراً أكبر على خصوصية الفرد، فهي تسمح بتواصل وتبادل المعلومات ونشر الصور والتعليقات، وتوثيق العديد من الأحداث والممارسات اليومية، التي يتم جمعها ومعالجتها

وتخزينها، ما يفقد صاحبها سيطرة عليها بمجرد عرضها على الموقع، كما قد تستخدم للحكم عليه أو تصنيفه ضمن فئة معينة².

إلى جانب أشهر الوسائل التقنية التي تستخدم لتتبع المعلومات الشخصية، ما يعرف بملفات الكعك المحلي، cookies التي تنتقل إلى نظام المستخدم بمجرد دخوله للموقع في مرحلة أولى، ولتتمكن من تسجيل بيانات تخص المستخدم في مرحلة ثانية، ومع أنها وسيلة اعتمدت في البداية لغرض غير جرمي، هدفها إرسال بريد الكتروني للمستخدمين في إطار الأنشطة الدعائية للشركات التجارية، إلا أنها في الوقت ذاته تسمح بالكشف عن بيانات قد لا يرغب الشخص الكشف عنها، وهي تطوراتها اللاحقة عدت وسيلة لتتبع الأشخاص وكشف حياتهم بل وإهدار توقعهم في التخفي؛ إذ تستخدم كوسيلة لبناء الدراسات التسويقية وملاحقة الزبائن³.

1 - محمود إبراهيم الغازي، مرجع سابق، ص 20 و 21.

2 - عبد الهادي فوزي العوضي، الحق في الدخول في طبي النسيان على شبكة الانترنت، ص 93 و 94.

3 - صبرينة جدي، مرجع سابق، ص 130.

الفرع الثالث: التجارة الالكترونية ووسائل الدفع الالكتروني

تسمح وسائل الاتصال الجديدة القيام بجميع الأعمال التجارية، كبيع وشراء البضائع، وعرض الخدمات والمعلومات... الخ، من خلال استخدام المواقع الالكترونية، حيث تعرض السلع وتتم أعمال التداول في الفضاء الرقمي، وبمناسبة ذلك يتم تبادل بيانات شخصية على قدر كبير من الأهمية، فالتجارة تتطلب نموذجية: أن يثق الزبائن بالتاجر، عند تقديم بيانات حساسة، مثل أرقام بطاقات الاعتماد، وعناوين البريد، والمعلومات الشخصية، والتي تكون جميعها قابلة للاستيلاء، والاستغلال غير المشروع. ما يجعل المعاملات التجارية الالكترونية، مصدرا آخر للخطر الذي يهدد الحياة الخاصة. وفي ذات الوقت يعد موضوع الخصوصية والاعتداءات الواقعة عليها عائقا أمام انتشار التجارة الالكترونية.

أما عن وسائل الدفع الالكتروني فهي المصدر الأخطر، فما تتيحه من سرعة في التعاملات المالية، يقابله تهديد لسرية هذه التعاملات، الأمر الذي يجعل التعامل يصرح ببيانات شخصية، يتم تداولها مع المؤسسات المالية ومقدمي السلع أو الخدمات والوسطاء، بشكل قد يتيح الاستيلاء عليها لأغراض إجرامية¹.

الفرع الرابع: تقنيات التتبع والمراقبة وتحديد المواقع.

أبرز التقدم العلمي أنظمة وتقنيات جديدة، كان الغرض منها تسهيل عمليات التتبع وتحديد المواقع، إلا أن تغلغلها في حياتنا اليومية جعل منها مصدرا آخر للخطر، فنظام التتبع وتحديد الموقع GPS توسعت تطبيقاته لتشمل عدة مجالات، إذ أصبح أحد التطبيقات المستخدمة في الحواسيب، والهواتف النقالة والسيارات. فإساءة استخدامه لتتبع الأشخاص ومراقبتهم كابوس حقيقي يهدد خصوصية الفرد، كذلك الأمر بالنسبة للرقائق RFID وهي اختصار لـ: Radio - frequency identification وهي تقنية تستخدم لتتبع المواشي أو البضائع حول العالم.

يستخدم الكثير من المصنعين رقائق التتبع لمعرفة موقع كل منتج يصنعه منذ لحظة إنتاجه، والتقاطه ووضع في سلة المشتريات. هذه التقنية أيضا تستخدم في تتبع السيارات، والمسافرين والمرضى المصابين بالزهايمر، وقريبا سوف تتبع هذه الرقائق ما تفضله من أطعمة أو أجهزة أو أي شيء. وجهت الكثير من الانتقادات لهذه التقنية، التي أصبحت تشكل جزءا كبيرا من حياتنا دون أن نعرف، وأي تفاصيل من حياتنا يتم تتبعها دون علمنا².

1 - عبد الفتاح بيومي حجازي، مرجع سابق ص 56 وما يليها.

2 - صبرينة جدي، مرجع سابق، ص 130.

تستخدم هذه التقنية في جوازات السفر الالكترونية البيومترية، ومختلف وثائق التعريف الالكترونية وبطاقات السحب ما يوفر حماية لصاحب الوثيقة، ويحول دون سرقة هويته، بتخزينها للبيانات ومنع تغييرها أو تعديلها، لكنها تعتبر معالجة الكترونية لبيانات الشخصية، تسمح بجمع معلومات على قدر كبير من الحساسية، مع إمكانية عرضها والاطلاع عليها واستخدامها ما يطرح التساؤل حول تأمينها وحمايتها.

يضاف إلى ذلك كاميرات المراقبة، التي أصبحت أداة مهمة بيد مصالح الأمن، لرصد الكثير من الجرائم المرتكبة في الأماكن العمومية كالطرق والمطارات ومحطات ووسائل النقل، ما يساعد على القبض على الجناة والفارين، إلا أنها قد تتحول إلى أنظمة رقابة خانقة على الحريات، متى أسيء استخدام تلك التسجيلات¹.

مع ضرورة الإشارة في هذا المقام؛ أن تكنولوجيا المعلومات تعرض على المستخدمين تقنيات، وبرامج التأمين وحماية البيانات الشخصية؛ كبرامج التشفير وبرمجيات الجدار الناري، وخاصة التعرف على المستخدم، كما يوصي المختصون بسلوكيات معينة للحيلولة دون الوصول إلى البيانات الشخصية للأفراد²، وتوخي الحذر عند التعامل مع تقنية المعلومات عموماً، والانترنت خصوصاً، لكن تبقى الحماية التقنية غير كافية، فتوفير الحماية القانونية مطلب رئيسي.

1 - عن كاميرات المراقبة وأنظمة التجسس، انظر: بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد تكنولوجيا الإعلام والاتصال، رسالة دكتوراه، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، 2014/2015، ص 107 وما يليها.

2 - بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، لبنان، 2009، ص 227 وما يليها.

خلاصة الفصل الأول:

يعد الحق في الخصوصية أو الحق في الحياة الخاصة من أكثر الحقوق تعلقا بالشخصية وأشدها ارتباطا بالكرامة وذلك لجمعه بين الجوانب المادية والمعنوية لشخصية الإنسان وعلاقته الوثيقة بالحقوق والحريات الأخرى، ويشمل الحق في الحياة الخاصة حرمة المسكن، سرية الاتصالات الخاصة، حماية المعلومات والمعطيات ذات الطابع الشخصي فضلا عن تأثره الشديد بالمخاطر التي فرضها التطور العلمي والتكنولوجي لوسائل المعلومات والاتصال ، فنستخلص ان الحق في الخصوصية هو حق أساسي من حقوق الإنسان منصوص عليه في العديد من القوانين الدولية والوطنية. ومع ظهور التقنيات الرقمية ، أصبح الحق في الخصوصية معقدًا بشكل متزايد ويصعب حمايته كليا ولكن وجب العمل على ذلك.

وهذا كله أشرنا إليه في الفصل الأول من هذه الدراسة، بحيث استعرضنا فيه الاطار المفاهيمي للحق في الخصوصية الرقمية وكذا اثر تكنولوجيا المعلومات على هذا الحق من خلال مبحثين وكل مبحث يحوي مطالب وفروع فصلت المراد توضيحه ودراسته.

الفصل الثاني:

آليات حماية

الخصوصية الرقمية

الفصل الثاني: آليات حماية خصوصية الرقمية

أصبح بالكاد يمر يوم لا يعبر فيه الأفراد عن قلقهم بشأن خصوصياتهم المهددة بالاختراق، وهذا القلق المتزايد بشأن اختراق الخصوصية مستوحى من الثورة التكنولوجية التي مكنت الدول، أكثر من أي وقت سبق، من الوصول إلى عمق هذه القيمة المجتمعية المتعلقة بالخصوصية، في الوقت ذاته يرى البعض أن الدفاع عن هذه القيمة في الحق في الخصوصية يشكل في بعض جوانبه إضعاف لقيمة مجتمعية أخرى تتمثل في أمن المجتمع، فمراقبة الأفراد من قبل الدولة بالاعتماد على الوسائل التكنولوجية الحديثة ينبع من التهديد المتنامي الذي تواجهه الدولة من ارتكاب الجرائم على اقليمها والتي تشكل تهديداً مباشراً لأمن المجتمع، إلى ذلك أصبحت المراقبة الإلكترونية والردع والتصدي لهاته الانتهاكات عاملاً حاسماً في متابعة الجرائم قبل وقوعها ما ينعكس إيجاباً على أمن الفرد واستقرار المجتمع برمته

وبناء عليه سنتناول في هذا الفصل أشكال الاعتداء الإلكتروني على الحق في

الخصوصية في المبحث الأول، وآليات الحماية للخصوصية الرقمية في المبحث الثاني

المبحث الأول: أشكال الاعتداء الإلكتروني على الحق في الخصوصية

لما شقت التكنولوجيا طريقها إلى حياة الأفراد، أضحت الاعتداءات المرتكبة إلكترونياً تتسم بالحدثة والتطور، بحيث أدى الاعتماد على الحواسيب وشبكة الانترنت ودورها في جمع البيانات الشخصية ومعالجتها إلى تهديد خصوصية الأفراد ووقوع الحياة الخاصة فريسة الجريمة المعلوماتية ومن ثم أضحت حياة الأفراد شبه عارية أمام تكنولوجيا المعلومات، هذا ما نمى الشعور بمخاطر تقنية المعلومات وحرك الجهود الداخلية والدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد من شأنها مراعاة الحماية لحق الخصوصية في العالم الرقمي.

المطلب الأول: نطاق حماية حق الخصوصية الرقمية

يتحدد نطاق الحق في الخصوصية في مجال التعاملات الالكترونية بين حدين متناقضين يتمثل أولاهما في حق الأفراد في الحياة الخاصة وثانيها موجبات الاطلاع على شؤون الأفراد وما تفرضه الضرورة على الدول والحكومات في توفير حد أدنى من خط الأمان وكبح للجريمة المرتكبة عبر الانترنت، ويتضح هذا النطاق وفق المعالم التالية:

-إيجاد تناسق بين الحق في الخصوصية وحق الدولة في الاطلاع على هذه الخصوصية في إطار تنظيم الحياة الاجتماعية على نحو أفضل، وهذا لا يتعارض في مفهومه مع التعرض للحياة الخاصة للأفراد بأي حال، إلا في حالة استخدام البيانات الشخصية لأغراض تتنافى مع صونها واحترامها¹.

-إيجاد تناسق بين حق الفرد في عدم الكشف عن أي معطيات أو بيانات تتعلق بخصوصيته مع المصلحة في الكشف عن هذه الخصوصية لجني فوائد عملية، إذ أنه يتبين عدم وجود تعارض بين الحق في السرية والكشف الإرادي عن هذه الخصوصية، إلا أن الفكرة تخص مسألة نقادي أي احتمال لاستغلال تلك المعلومات المكشوف عنها إرادياً ليتم استغلالها في أغراض تهدد حرمة الفرد وانتهاك لحرمة حياته الشخصية².

1 - هشام محمد فريد رستم، مرجع سابق، ص 180.

2 - منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، سنة 2013، ص 19.

-رسم خط توازي بين استخدام فكرة بنوك المعلومات¹ كآلية لجمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد والتي خلقت آثارا إيجابية عريضة في مجال تنظيم تعاملات الأفراد إلكترونيا، فبفعل الكفاءة العالية لوسائل التقنية الحديثة والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات إلكترونيا، اتجهت أغلبية دول العالم بمختلف هيئاتها إلى إنشاء قواعد بيانات تساهم في هذه العملية،² إلا أنه ظهر بشكل سريع الشعور بخطورة تقنية المعلومات وتهديدها للخصوصية.

وممكن المخاوف يبرز في أن الوضع الحديث لتقنية المعلومات أضحى يمس بجوانب حياة الأفراد الشخصية بتخزينها لتلك المعلومات وجمعها لفترة غير محددة والرجوع إليها بكل سهولة، مع خطر تدفق تلك البيانات التي تنتج عن المعاملات الالكترونية ويجعلها عرضة للقرصنة والتملك والاستغلال مما يخلق حالة قلب لإيجابية تلك التقنية الحديثة إلى خطر يهدد استقرار الحياة الخاصة وسريتها³.

وإذا كانت البيانات الشخصية هي المحل الذي ينشأ حوله الحق في الخصوصية الرقمية باعتبارها مصدرا للمعلومات الخاصة، فإن نطاق هذا الحق واسع ومتعدد باعتبار البيانات الشخصية تتواجد في أكثر من نطاق عبر مختلف الأنظمة المعلوماتية.

وبالنظر إلى استخدامات الأنظمة المعلوماتية المتاحة اليوم، يمكن القول إن الحق في الخصوصية الرقمية يتعلق على وجه الخصوص بالبيانات الشخصية المخزنة في قواعد البيانات والأنظمة المعلوماتية للمؤسسات والإدارات كالملفات الطبية والقضايا المسجلة في المحاكم، وقوائم العمال والموظفين، كما يتعلق الحق في الخصوصية الرقمية بالاتصالات والمراسلات عبر الشبكات والانترنت.

كما تظهر الكثير من سمات الانترنت أنه من الصعب أن يتحكم المستخدم في بياناته الشخصية، لذلك فقد أدى التوتر بين الحقوق والقدرة الفعلية لمستخدمي الانترنت على التحكم في بياناتهم الشخصية إلى الكثير من الجدل حول الخصوصية على الانترنت. ويركز هذا الجدل في العادة على عدم قدرة المستخدم على التحكم وتمكينه من أن يقرر كيفية استخدام بياناته، مع التركيز على دور المؤسسات

1 - تعرف بنوك المعلومات بأنها قاعدة بيانات تم إنشاؤها ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية، وذلك لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة، وقد تكون بنوك المعلومات مقصورة على بيانات تتصل بقطاع معين، وقد تكون معدة للاستخدام على المستوى الوطني كمراكز وبنوك المعلومات الوطنية أو تستخدم في مجال قطاع الأعمال. انظر د. حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، 1987، ص 60.

2 - أسامة فايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة في القانون الفرنسي والأمريكي وفقا لآخر التعديلات التشريعية، دار النهضة العربية، مصر، سنة 2008، ص 48.

3 - Pierre TRUCHE; Jean-Paul FAUGERE et Patrice FLICHHY : Administration électronique et protection des données personnelles livre blanc, rapport au ministre de la fonction public et de la réforme de l'état, Paris, la documentation française, 2002, P 77.

في مراقبة وإدارة البيانات الشخصية. فضلا عن ذلك دائما تكون سيطرة الجهات الخاصة في مقارنة سيطرة الجهات العامة والتي تعتبر غير قادرة أو غير راغبة في تنفيذ الحماية الفعلية لبيانات المستخدمين الشخصية¹.

أولا: الأنظمة المعلوماتية

يعرف النظام من الناحية التقنية بأنه مجموعة من الأجزاء المترابطة فيما بينها بحيث ينتظر منها أداء سلوك يمكن مشاهدته على الواجهة مع بيئته².

ومن الناحية البنيوية، فإن النظام يتكون من مجموعة من المكونات المترابطة بحيث يمكنها التفاعل فيما بينها. كل مكون هو نظام آخر قائم بذاته³.

وانطلاقا من التعريف التقني أمكن لرجال القانون اعتماد التعريف القانوني للنظام المعلوماتي، حيث جاء في المادة الأولى من اتفاقية بودابست حول الجريمة السيبرانية: "النظام المعلوماتي يعني أي جهاز أو مجموعة من الأجهزة المتصلة أو المترابطة بحيث واحد من بينها أو أكثر يقوم بالمعالجة الآلية للبيانات وفقا لبرنامج"⁴.

أما المشرع الجزائري فقد عبر عنه بـ: "المنظومة المعلوماتية" وعرفه بأنه أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين⁵.

ويعد جهاز الحاسوب بمختلف أشكاله أهم الأنظمة المعلوماتية، بالإضافة إلى الألواح والهواتف الذكية، والصراف الآلي، والأنظمة المدمجة، وغيرها. هذه الأجهزة يمكن أن تكون مفصولة عن غيرها من الأجهزة والأنظمة، كما يمكن أن تكون موصولة بأنظمة معلوماتية أخرى لتشكل نظاما معلوماتيا أوسع يعرف بالشبكة المعلوماتية. هذه الأخيرة بدورها يمكن أن تكون منفصلة أو موصولة بغيرها من

¹ - توبي مندل وآخرون: مرجع سابق، ص 19.

² - Jerome H. Saltzer & M. Frans Kaashoek: Principles of Computer system Design. Morgan Kaufmann Publishers – Elsevier-. USA. 2009. P6.

³ - Fernard Lone SANG. Protection des systèmes informatiques contre les attaques par entrées-sorties. Doctorat de l'Université de Toulouse. Directeurs de thèse: Yves DESWARTE et Vincent NICOMETTE. 2012. P06.

⁴ - Convention On Cybercrime. 23. XI. Article 1.

⁵ - المادة الأولى من القانون رقم 10-05 المؤرخ في 01 نوفمبر 2010 حول المساس بأنظمة المعالجة الآلية. الجريدة الرسمية للجمهورية الجزائرية، العدد 20، السنة الواحدة والأربعون.

الشبكات. لتشكل نظاما أكثر اتساعا، وهكذا إلى أن تكون منفصلة عن أو متصلة بشبكة الشبكات المعروفة بشبكة الانترنت والتي تعتبر أوسع الأنظمة المعلوماتية.

وتدخل الأنظمة المعلوماتية في نطاق الحق في الخصوصية الرقمية باعتبارها البيئة التي تولد لها وفيها البيانات الشخصية وتعالج وتخزن ويتم تبادلها. ويمكن اليوم أيضا أن تحتوي صور الأشخاص ومذكراتهم، كما تعتبر أهم وسيلة لإجراء الاتصالات الشخصية، والمحادثات السرية، والتقاط الصور الخاصة...

ويظهر الحكومة الالكترونية، أصبح تسيير مختلف المؤسسات يتم عبر الأنظمة المعلوماتية، ما يتطلب تبني قواعد البيانات التي تحتوي على بيانات شخصية تعود لعمال أو موظفين أو تلاميذ، أو مرضى في المستشفيات، أو متابعين قضائيا في المحاكم، وهي كلها بيانات تستحق الحماية.

ثانيا: وسائل الاتصال الرقمية (البريد الالكتروني والسكايب)

يتم اليوم إجراء جانب كبير من الاتصالات والمراسلات عبر الخدمات التي تتيحها تكنولوجيا الإعلام والاتصال. أهمها: البريد الالكتروني والسكايب.

أما البريد الالكتروني فهو عبارة عن رسالة يتم إرسالها من نظام معلوماتي (حاسوب شخصي، هاتف ذكي...) نحو آخر عبر شبكة الانترنت. ولتتم العملية لا بد من تحقق أمرين: الأول أن يكون كلا من جهاز المرسل والمرسل إليه موصولا بالإنترنت، والأمر الآخر هو وجود العنوانين الالكترونيين للطرفين، تمنحهما إحدى الشركات التي تملك خوادم بريد. وهي عبارة عن أجهزة كمبيوتر خاصة تستطيع إيصال البريد الالكتروني إلى العنوان الصحيح¹.

وفيما تسمح خدمة البريد الالكتروني بتبادل الرسائل الالكترونية (النصية غالبا) عبر شبكة الانترنت، فإن خدمة السكايب وفضلا عن ذلك تتيح للمستخدمين إمكانية إجراء المحادثات المسموعة والمرئية بحيث يتم تبادل الصوت والصورة بين الطرفين عبر الانترنت.

وهو ما قد يهدد الخصوصية باعتبار أن جوهرها يتمثل في "قدرة الأشخاص على التحكم في دورة المعلومات التي تتعلق بهم". الأمر الذي يصعب تحقيقه عبر وسائل الاتصالات وشبكة الانترنت، باعتبار وجود طرف ثالث يمكن من خلاله التعقب والاطلاع على المعلومات التي يرغب أصحابها في

¹ - <http://www.halifaxpubliclibraries.ca/assets/files/handouts/Email.pdf>

حجبها عن الغير. ذلك أن البيانات المتبادلة تمر عبر خوادم الانترنت قبل الوصول إلى المرسل أو المرسل إليه.

ثالثا: وسائل التواصل الاجتماعي

وسائل التواصل الاجتماعي هي إحدى تطبيقات الويب، التي تسمح لكل شخص ليس فقط بالوصول إلى المحتوى على الانترنت، بل بتحرير المحتوى وبتمويله والتعليق عليه وتعديله¹.

ويرتكز تعريف وسائل التواصل الاجتماعي على ثلاثة عناصر: إنشاء سيرة ذاتية من قبل المستخدم، وجود أدوات تسمح بإنشاء لائحة المعارف والتفاعل معهم، تمكين المستخدم من وضع المحتوى الخاص به على الشبكة، وتحديثه (نصوص، رسوم، صور، صوت، أغاني، أفلام...). وما ينشر قد يكون مفتوحا للعموم، أو خاصا أو مختلطا، وقد يكون مفتوحا لفئات مختلفة.

وقد أثبتت الدراسات حول حسابات طلاب على موقع فيسبوك أن 88% يفشون كامل تاريخ ولادتهم وجنسياتهم لوسيلة التواصل الاجتماعي، وينشر أيضا 45.8% منهم عنوان سكنهم. وهذه المعلومات هي كافية لتحديد هوية الشخص. كما تمكن طلاب من جامعة أم أي تي MIT من الوصول إلى 70 ألف سيرة على موقع الفيسبوك من خلال برنامج ابتكروه.

وبالتالي، فمن المنطقي القول إنه من غير الصعب على فنيين محترفين تجاوز إعدادات الخصوصية لموقع فيسبوك².

رابعا: محركات البحث

تقوم محركات البحث على غرار Google في العادة بجمع قدر هائل من البيانات الشخصية بما في ذلك عناوين بروتوكولات الانترنت IP وطلبات البحث والوقت والتاريخ والمكان الذي قدم فيه جهاز الكمبيوتر الطلب. يمكن أن تكون المعلومات قابلة لتحديد الهوية الشخصية ويمكن أن تكشف عن أجزاء حساسة من المعلومات مثل المعتقدات السياسية للشخص أو ميوله الجنسي أو معتقداته الدينية أو المسائل الطبية³. وفي هذا الخصوص قضت محكمة الدرجة الأولى في باريس بتاريخ 2013/11/6 بالإلزام

1 - وسيم شفيق الحجار: مرجع سابق، ص 15.

2 - وسيم شفيق الحجار: المرجع نفسه، ص 49.

3 - توبي مندل وآخرون: مرجع سابق، ص 32.

قول، بالاستناد إلى الحق في حرمة الحياة الخاصة، بوقف عرض صور تكشف الحياة الجنسية لأحد الأشخاص¹.

وبالانتشار المتزايد للمعاملات التجارية الالكترونية، تقوم معظم الشركات بجمع البيانات الشخصية عبر مواقعها على شبكة الانترنت. وكما هو موضح في الجدول (1) فإنها لا تصرح دائماً عن الأغراض من تجميع البيانات الشخصية، كما أنها لا تلتزم بإشعار المستخدمين بالتجميع عن طريق بيان سياسة الخصوصية التي يفترض أن يتبناها الموقع.

القطاع	عدد المواقع الالكترونية	البيانات الشخصية المجمعة	الاشعار بغرض التجميع	الاشعار عن طريق بيان الخصوصية
البنوك	9	%100	%44	%33
السفر	7	%57	%25	%25
السيارات	14	%50	%14	%14
بيع التجزئة	13	%100	%69	%62
الرياضة	15	%33	%40	%20
الموضة	5	%80	%0	%0
الزراعة	11	%55	%67	%83
مجالات أخرى	48	%63	%50	%47

الجدول يبين تجميع البيانات الشخصية عبر مختلف المواقع الالكترونية²

بالإضافة إلى ذلك، تقوم الحكومات بالتجسس الرقمي اتجاه الأفراد برصد أداء الأشخاص وتفاعلاتهم اليومية عبر الانترنت، وقد يتوسع هذا التجسس ليطال مواطني دول أخرى.

ومن الأمثلة الفعلية على ذلك التفويض الذي أعطاه الرئيس الأمريكي الأسبق جورج بوش إلى وكالة الأمن القومي بعد هجمات الحادي عشر من سبتمبر لتطوير آليات للتجسس، وإطلاق برنامج الرقابة PRISM³ الذي يستهدف جميع بيانات مستخدمي خدمات الانترنت لشركات⁴ في جميع أنحاء العالم العالم PalTalk , AOL , Microsoft , Yahoo , Apple , Google ,

1 - وسيم شفيق الحجار: مرجع سابق، ص 32-43.

2 - Winnie Chung and John Paynter: مرجع سابق.

3 - كريم عاطف: الخصوصية الرقمية بين الانتهاك والغياب التشريعي، مركز دعم لتقنيات المعلومات، القاهرة، مقال متاح على الرابط: info@sitcegypt.org.

4 - كريم عاطف: المرجع نفسه.

خامسا: الحوسبة السحابية

الحوسبة السحابية عبارة عن هيكل شبكات ناشئ يتم من خلاله تخزين البيانات أو طاقة المعالجة أو البرامج في أجهزة خادم عن بعد، على خلاف الأجهزة الشخصية. وتكون متاحة من خلال الانترنت. تتوفر أشكال مختلفة من الحوسبة السحابية وتوفر مجموعة كبيرة من الخدمات ويمكن للأفراد أو المنظمات تأجير القدرة الحاسوبية بشكل فعال من مزودي الخدمة عن بعد.

فمثلا تسمح خدمة تطبيقات جوجل Google's Apps للأفراد بإنشاء وحفظ مستندات معالجة spreadsheet و word على الانترنت وتشتمل بعض الخدمات الأخرى على منصات تعاونية تسمح للمستخدمين بحرية الوصول إلى المستندات بشكل فوري مثل wiki ومستندات منصات. Google docs.

وتثير الحوسبة السحابية كذلك العديد من المخاوف من منظور الخصوصية. حيث يتم تخزين البيانات في جهاز طرف ثالث يتحمل المسؤولية عن حمايتها ويفقد المستخدم قدرته على التحكم فيها. يضاف إلى ذلك أن القوانين التي تغطي الحوسبة السحابية غير محددة بما يكفي فليس هناك ما يضمن خصوصية بيانات المستخدمين¹.

المطلب الثاني: الاعتداء على الخصوصية في العالم الرقمي

يمكن تأصيل المخاطر الإلكترونية التي تمس حق الخصوصية في صورتين أولاهما: انتهاك سرية البيانات الشخصية وثانيها الاعتداء على سلامة البيانات المتداولة في مختلف التعاملات.

الفرع الأول: الجرائم الواقعة على سرية البيانات الشخصية

تتعدد صور الاعتداء على سرية البيانات الشخصية ابتداء من المعالجة غير المشروعة للبيانات أو عملية الإقضاء غير المشروع لتلك البيانات أو تعرض المحادثات الشخصية للأفراد للتجسس عبر شبكة الانترنت وكذا عمليات اختراق البريد الإلكتروني.

أولا: المعالجة غير القانونية للبيانات الشخصية

تعد البيانات الشخصية هي قوام الحق في الخصوصية فهي تعد تمثل في مجموعها المعطيات والمعلومات الخاصة بالفرد والتي تكتسب صفة السرية، وعملية المعالجة غير المشروعة لجملة

¹ - كريم عاطف، مرجع سابق.

البيانات هي أبرز صور انتهاك لتلك السرية من خلال مخالفة القائمين على عملية المعالجة للشروط والأساليب القانونية المنصوص عليها داخليا كعدم منح الترخيص¹ من الجهات المختصة أو إلغائه أو انتهاء مدته وهذا يشكل في جوهره اعتداء على حق الدولة في الرقابة على تداول ونقل البيانات الممنوحة للأشخاص المعنوية المصرح لها بذلك قانونا. وبهذا ينشأ مخاطر تحول دون مهمة القائمين على تلك الرقابة في التكفل عدم الاعتداء على الحياة الخاصة، ومن ثم تغييب دور الدولة في ضبط مجال الرقابة على البيانات وحمايتها من شتى أنواع الجريمة الإلكترونية².

كذا أن فكرة المعالجة غير المشروعة للبيانات الشخصية تقوم على مسألة الاعتداء على حق الأفراد في الاستئثار بمعالجة البيانات الشخصية، الأمر الذي يعد ضروريا في التفرقة بين البيانات القابلة لمعالجتها من قبل الغير وتلك غير القابلة لذلك³.

ثانيا: الإفشاء غير المشروع للبيانات الشخصية

إن مسألة الإفشاء غير المشروع للبيانات الشخصية كأحد صور انتهاك لحق الخصوصية قد تأخذ مظهرها في بعض المهن التي تعتمد على سرية البيانات مهنة المحاماة والطبيب أو عمال البنوك، بحيث يفترض احتفاظ صاحب المهنة بسرية البيانات الشخصية للزبون أو العميل بحكم التعامل القائم بينهما. وتعد أكثر البيانات عرضة للإفشاء غير المشروع هي الخاصة بتعاملات البنوك الإلكترونية وهذا ما ثبت من خلال قضية بنك (جزل تشافت) السويسري التي حاول خلالها عملاء فرنسيين تابعين لإدارة خدمات الرقابة على التعاملات التجارية والمالية فك شفرة بيانات شخصية المواطنين فرنسيين تحمل حسابات لدى البنك، وذلك للاستعانة بها في أعمال البحث والتقصي التي تجرى بشأن التهرب الضريبي⁴.

الفرع الثاني: التجسس الإلكتروني

لقد أثبتت التجربة الواقعية أن خطورة استخدام شبكة الانترنت تكمن أساسا في ضعف الوسائل المستخدمة في حماية انتقال البيانات عبر الشبكة، ضف إلى ذلك صعوبة الوصول إلى الأشخاص القائمين بالاعتداء وبهذا فقد ظهر التجسس الإلكتروني كأخطر صور الاعتداءات التي تحدث في إطار

¹ - محمد عزت عبد العظيم، مرجع سابق، ص 92.

² - Jean-Jacques Hyst: La fraude informatique vue par le nouveau code pénal, expertises des systèmes de l'information, Février 1992, N 147.

³ - يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخليوي، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخليوي، اتحاد المصارف العربية، عمان، الأردن، 2002، ص 519.

⁴ - هشام محمد فريد رستم، مرجع سابق، ص 195.

التعاملات الإلكترونية وهذا لارتباطه بشكل مباشر باغتصاب سرية المحادثات الشخصية و جل المراسلات والتعاملات التي تتم عبر شبكة الانترنت في كل المستويات.

ولقد عرف التجسس الإلكتروني في مجال المحادثات الشخصية بأنه: "عملية التنصت أو النقاط البيانات التي تنتقل بين جهازين عن بعد عبر شبكة الانترنت"، أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى بيانات وذلك باستخدام أي وسيلة من الوسائل التقنية¹.

وما يجدر الإشارة إليه أن التجسس الإلكتروني الذي يصدر في سياق خارج عن القانون والممارس من طرف سلطات الدولة يعد من الأساليب المحرمة دوليا وداخليا لانتهاك حق الأفراد، وهذا في حالة ثبوت حصول فعل التجسس بدون إذن مسبق من المحكمة وهذا يدخل في إطار التعسف في استعمال حق الدولة في المساس بحقوق الأفراد تحت مظلة الأمن القومي أو العام.

أضف أن خطورة التجسس الإلكتروني أضحت تأخذ صورة أوسع مما كانت عليه سابقا خاصة في ظل العولمة والتقنيات الحديثة، بحيث لم تعد تقتصر على السلطات أو دوائر المخابرات بل قد أصبحت وسائل التجسس متاحة إلى الأفراد العاديين خاصة في الدول المتقدمة على عكس الدول العربية التي ما زالت حركة تسويق أجهزة التجسس من الأمور المستعصبة والتي لا يمكن تداولها بشكل حر وبسيير².

ولقد اختلفت الوسائل المتبعة في إطار التجسس الإلكتروني وهذا تبعا لاختلاف ثقافة مستخدمي هذه الوسائل ومن أبرزها إتباع تقنية اعتراض الاتصال الشبكي التي تقوم على الاعتماد على برامج لتنفيذها، فيتم التخل من قبل أحد الأشخاص الخارج عن الاتصالات الشبكية المقامة عبر الانترنت كتبادل النصوص أو الأحاديث الصوتية فيتم التقاط البيانات أو الصور أو التنصت على الأحاديث الصوتية واعتراض المحادثات المقامة بالصوت والصورة عن طريق الكاميرات أثناء الاتصال³.

الفرع الثالث: اختراق الحاسبات الآلية والبريد الإلكتروني

ذهب البعض من الفقه غلى تعريف جريمة الاختراق بأنها «عملية دخول غير مصرح بها إلى حاسب الآخر عن طريق استخدام برامج متطورة تحت تقنية وخبرة عاليين»⁴.

1 - يأتي هذا التعريف وفقا لما ورد في نص المادة 3 من اتفاقية بودابست لسنة 2001 المتعلقة بمكافحة الإجرام المعلوماتي.

2 - نديم عبده، أمن الكمبيوتر (الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي)، دار الفكر للأبحاث والدراسات، بيروت، ط1، 1991، ص 86.

3 - محمد عزت عبد العظيم، مرجع سابق، ص 101.

4 - عمر محمد أبوبكر يونس، مرجع سابق، ص 331.

كما ربط البعض الآخر فكرة الاختراق بالمعالجة غير المشروعة للبيانات فعرفه بأنه الولوج غير المصرح به قانونا إلى نظام معالجة البيانات باستخدام الحاسوب¹.

وبهذا نجد أن عمليات الاختراق لا تقل خطورة عن النماذج السابقة على اعتبار أن الحاسب الشخصي أضحى يمثل أهم الوسائل المتاحة للاتصالات الحديثة بين الأفراد وأضحى يعتمد عليه كليا كآلية للمراسلات والمعاملات التي تصدر في إطار التعاملات الإلكترونية وبهذا فإن فكرة اختراق الحاسب الشخصي تقوم على أساس الاعتداء على خصوصية وسرية المعاملات وتسخيرها واستغلالها في شتى الأغراض غير المشروعة التي تلحق بالفرد عدة خسائر على المستوى المادي والمعنوي، وهذا ما عبر عنه في السنوات الأخيرة من خلال ما يعرف بالاختراق الأسود أو «مخترقتي القبعة السوداء» وهي مجموعة من المجرمين الإلكترونيين الذين اعتمدوا أسلوب اختراق الحاسبات الشخصية للأفراد بالدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة وتعديل وتحريف وإتلاف البيانات بغرض الاستفادة المادية أو إحداث الضرر المعنوي للضحية، وقد تخل هذه التصرفات في غالب الأحيان في إطار العداءات الشخصية أو السياسية أو الدينية أو القيام بتلك الأفعال لحساب جهات منافسة أو معادية².

ثانيا: جريمة اختراق البريد الإلكتروني

يعتبر البريد الإلكتروني من أحد الوسائل الحديثة في إطار المعاملات الإلكترونية التي تقدمها شبكة الانترنت في تدخل في إطار تسهيل الاتصال الإلكتروني عن طريق تبادل الرسائل الفوري، وبهذا يعد اختراق البريد الإلكتروني من أهم المخاطر التي تواجه حق الخصوصية وتعرض الفرد إلى انتهاك سرية المعاملات والمراسلات التي تدخل في شتى المجالات وبهذا فإن المقرر وفق القواعد العامة تكريس ضمانات لحماية سرية المراسلات في حدود وضوابط معينة بغض النظر عن الأساليب المستخدمة سواء كانت تقليدية أو حديثة³.

1 - خالد ممدوح إبراهيم مرجع سابق، ص 242.

2 - محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، مصر، 1994، ص 56.

3 - عمر محمد أبوبكر يونس، مرجع سابق، ص 339.

المبحث الثاني: آليات حماية الحق في الخصوصية الرقمية

من خلال هذا المبحث نبين آليات الحماية الموضوعية للحق في الخصوصية الرقمية في المطلب الأول، والحماية الإجرائية في المطلب الثاني، وأخيرا في المطلب الثالث تقييم هذه الآليات.

المطلب الأول: الحماية الموضوعية للحق في الخصوصية الرقمية

بعد بيان مفهوم الحق في الخصوصية الرقمية، نركز في هذا الجزء من البحث على استقصاء الحماية الجنائية للحق في الخصوصية الرقمية في قانون العقوبات الجزائري، وتحديد الخصوصية المعلوماتية، والخصوصية عبر وسائل الاتصال والمراسلات، ومواقع التواصل الاجتماعي.

الفرع الأول: الحماية الموضوعية لخصوصية الأنظمة المعلوماتية

عبر المشرع الجزائري عن الأنظمة المعلوماتية بـ "منظومة للمعالجة الآلية للمعطيات"، وعبر عن البيانات الرقمية بـ "المعطيات"، كما نفتت إلى الحماية الجنائية للبيانات بصفة عامة، دون تحديد للبيانات الشخصية، أو إفرادها بنصوص خاصة. حيث جرم جملة من الأفعال الموصوفة في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات¹، منها ما تعلق بسلامة الأنظمة والبيانات، ومنها ما تعلق بإتاحة الأنظمة والبيانات، فيما يتعلق جانب منها بخصوصية الأنظمة وسرية البيانات وهو ما يعنينا في هذا المقام.

أولا: تجريم الولوج إلى أو البقاء غير المصرح بهما في نظام معلوماتي

يعتبر الولوج غير المصرح به إلى النظام المعلوماتي أحد أهم الجرائم الماسة بالحق في الخصوصية، إذ أضحت الحواسيب الشخصية للأفراد تحتل جانبا كبيرا من حياتهم الخاصة، لذلك فإن الولوج غير المصرح به إلى الأنظمة المعلوماتية يشكل جريمة في معظم التشريعات الحديثة، بما فيها التشريع الجزائري الذي ينص في المادة 394 مكرر من قانون العقوبات² على أنه: "يعاقب بالحبس من ثلاثة أشهر إلى سنة، وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"

من خلال النص يتضح أن الركن المادي للجريمة يكون إما بالولوج إلى النظام المعلوماتي وإما بالبقاء فيه.

¹ - القانون رقم 04-15 مرجع سابق.

² - المرجع نفسه.

1.الولوج غير المصرح به إلى نظام معلوماتي

يمكن تعريف الولوج غير المصرح به إلى نظام معلوماتي بأنه أي نشاط يقوم به الشخص عمداً، وبدون رضى صاحب النظام، يجعله في حالة تسمح له بالاتصال الحسي مع النظام أو بالتحكم في نظام التشغيل ولو جزئياً. يمكن أن يكون فعل الولوج غير المصرح به بسيطاً وبالاتصال الحسي المباشر مع النظام. إلا أنه في الكثير من الحالات يتم عن بعد وباستخدام أساليب وتقنيات القرصنة المعقدة.

ولاكتمال الركن المادي اشترط المشرع أن يتم الفعل بطريق الغش وهو ما يمكن أن يعبر عن أحد أمرين: الأمر الأول هو عدم رضا صاحب النظام بفعل الولوج. والأمر الآخر هو اللجوء إلى استخدام تقنيات وأساليب فنية لاقتحام النظام. وهو ما يتصور في حال كون النظام مؤمناً بالأدوات اللازمة على غرار كلمة السر والجدران النارية وغيرها من أنظمة الحماية ضد البرمجيات الخبيثة التي تستعمل في التجسس والتحكم في عمل النظام، فضلاً عن اقتحامه.

وفي اشتراط كون النظام المعلوماتي مؤمناً حتى يتمتع بالحماية ينقسم الفقه إلى رأيين¹:

الرأي الأول يرى عدم اشتراط انتهاك نظام الحماية الفنية لتجريم فعل الولوج غير المشروع، بحجة أن التمسك بهذا الشرط يؤدي إلى قصر نطاق الحماية الجنائية على الأنظمة المعلوماتية المحمية فقط. ما يعني زيادة حالات الإفلات من العقاب.

فيما يرى الجانب الآخر على ضرورة وجود نظام أمان، استناداً إلى أن المنطق والعدالة يستلزمان ذلك - بحسب هؤلاء- لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياطات اللازمة والمتطلب من إنسان متوسط الذكاء.

أما المشرع الجزائري فواضح من خلال نص المادة أعلاه أنه لا يشترط وجود هذه الحماية الفنية حتى يتمتع النظام المعلوماتي بالحماية الجنائية. وهو ما يمكن الاستدلال عليه بكون المشرع جرم فعل البقاء داخل النظام، وهو ما يتصور حدوثه في حالة الولوج بطريق الخطأ، أي دون أدنى صعوبة، ثم التماذي بالبقاء بعد التقطن لذلك. فكون النظام غير مؤمن بكلمة المرور مثلاً يجعل من الولوج إليه أمراً غاية في البساطة، لكن في حال حدوث ذلك خطأ، فإن الفاعل مسؤول جنائياً عن البقاء غير المصرح به.

¹ - دلخار صالح بوتاني: الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2015، ص 200.

عبد العال الديربي، محمد صادق إسماعيل: الجرائم الالكترونية، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012، ص 189.

2.البقاء غير المصرح به في نظام معلوماتي

يلحق المشرع الجزائري بفعل الولوج غير المصرح به، فعل البقاء غير المصرح به. ويقصد به التواجد داخل النظام المعلوماتي ضد إرادة من له الحق في السيطرة على هذا النظام¹. ويتصور وقوع هذا الفعل في إحدى حالتين²:

الحالة الأولى: تتحقق إذا تم الدخول إلى النظام عن غير قصد كالخطأ أو السهو، أي بدون قصد جنائي، ولكنه وبعد تقطنه للأمر يختار البقاء في النظام، أي بعد تكون العلم والإرادة اللازمين لتشكيل القصد الجنائي.

الحالة الثانية: تتحقق إذا تم الدخول بتصريح من صاحب الحق على النظام، ولكن بتصريح مشروط بمدة محددة أو بجزء محدد من النظام، فيتجاوز الحدود المسموح بها من خلال التصريح، وهذه الحالة توافق ما ينص عليها المشرع الأمريكي صراحة في القانون الفيدرالي CFAA³.

أما بالنسبة للركن المعنوي: فالجريمة تعتبر تامة ومرتبطة للجزاء متى توفر القصد العام أي اتجاه إرادة الفاعل نحو إتيان السلوك مع العلم بنتيجة هذا السلوك، وهو التواجد داخل نظام معلوماتي دون إذن صاحبه. وبغض النظر عن البواعث والنوايا. فإن الجريمة تعتبر تامة وإن كان الغرض منها هو التعلم والفضول العلمي البحث، وبهذا فإن جريمة الولوج غير المشروع في القانون الجزائري هي من الجرائم الشكلية، حيث يشكل فعل الولوج المجرد دون تصريح من صاحب النظام جريمة ولو لم ينتج عنه أي ضرر مادي أو معنوي ملموس⁴، لكن الجزاء يضاعف في حال إحداث ضرر بالحذف أو التغيير⁵، أما الضرر الناتج عن الحيازة أو الإفشاء فقد اعتبرها جريمة مستقلة.

1 - محمود أحمد طه: المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، ط1، 2017، ص 30.

2 - محمود أحمد طه: المرجع نفسه.

3 - Computed Fraud and Abuse Act، صدر عن الكونغرس لأول مرة عام 1986 وتم تنقيحه عدة مرات على مدى العقود الثلاثة التالية. كان الهدف الأساسي من هذا القانون هو حماية الأنظمة المعلوماتية التي تعود إلى إحدى الفئات التالية: الكيانات الاتحادية، المؤسسات المالية ومؤسسات التجارة الداخلية والخارجية. تعدل القانون أربع مرات في: 1986، 1994، 1996، 2001.

4 - مجرد الولوج غير المصرح به لا يشكل جريمة في القانون الأمريكي، إلا إذا حصل الفاعل بعد فعل الولوج على بيانات تتمتع بالحماية القانونية موجودة في النظام. المادة 1030 في الباب 18 من القانون الأمريكي المتعلق بالاحتيال وإساءة استخدام الحاسوب CFAA.

5 - الفقرة الثانية من المادة 394 مكرر من قانون العقوبات الجزائري .

ثانيا: تجريم إدخال معطيات إلى النظام المعلوماتي أو إزالتها أو تعديلها

تنص المادة 394 مكرر 1: "يعاقب بالحبس من ستة 6 أشهر وثلاث 3 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

ما يعنينا في هذا المقام هو المساس بحرمة الحياة الخاصة. والمشرع أطلق لفظ المعطيات ولم يقيد بصنف معين. والمعطيات من الناحية الفنية وحتى القانونية لفظ يتسع ليشمل جملة من الأصناف. فهي يمكن أن تكون برامج خبيثة (فيروسات) يقوم الفاعل بإدخالها إلى النظام بهدف التجسس وجمع البيانات الخاصة. كما يمكن أن تكون غير ذلك. يمكن مثلا أن تكون مواد إباحية يتعارض وجودها داخل النظام مع إرادة مالكه أو المسؤول عنه، يكون القصد من إدخالها هو الإزعاج أو إحداث أي ضرر معنوي آخر. ولا شك في أن هذا يتعارض وحرمة الحياة الخاصة.

كذلك هو الشأن مع أفعال تعديل البيانات الشخصية المخزنة داخل النظام أو إزالتها دون علم صاحبه. والواقع يثبت - من الناحية النظرية على الأقل - أن فعل التعديل يمكن أن يمس بالحقوق في الخصوصية. يتصور هذا مثلا في حال تعديل أو حذف يتم في قاعدة بيانات تخص موظفين أو مرضى أو أي فئة أخرى من الأشخاص.

فكل من أفعال الإدخال والتعديل والإزالة هي جريمة شكلية، وتعتبر تامة بغض النظر عن حدوث ضرر من عدمه، وبغض النظر عن البواعث وحجم الضرر الناتج، ويعاقب عليها المشرع بالعقوبة نفسها، مهما كانت طبيعة البيانات والحقوق أو المصالح المستهدفة. والمشرع وإن لم يعبر صراحة عن المعطيات الشخصية فإن النص يستغرقها كونه عاما في حماية المعطيات، وكون المعطيات (البيانات) الشخصية صنفا من المعطيات.

ثالثا: تجريم حيازة أو إفشاء أو نشر أو استعمال البيانات الشخصية

تنص المادة 394 مكرر 2 في فقرتها الثانية على المعاقبة بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 500.000 دج كل من يقوم عمدا وبطريق الغش ب: حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

وعلى غرار المادة السابقة فإن المشرع أطلق لفظ "المعطيات"، دون أن يخص المعطيات الشخصية بعبارة خاصة، لكن هذا لا يمنع من إمكانية سحب النص وتطبيقه لحماية البيانات الشخصية باعتبارها صنفا من البيانات، هذا إذا ما أخذنا بعين الاعتبار أن الولوج أو البقاء غير المصرح بهما في النظام المعلوماتي هو جريمة من الجرائم المنصوص عليها في هذا القسم، أي القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، والتي يمكن أن ترتكب بهدف حيازة بيانات شخصية أو إفشائها أو نشرها أو التصرف فيها بأي شكل آخر، كما أن هذه الجرائم شكلية وتعتبر تامة متى حصل الفعل ولا يشترط توافر قصد خاص مهما كان الباعث والغرض من حيازتها أو إفشائها أو نشرها أو استعمالها بأي شكل آخر.

الفرع الثاني: الحماية الموضوعية لخصوصية الاتصالات والمراسلات والصور الشخصية

في الواقع يمكن لجملة من الأفعال المهددة للخصوصية أن ترتكب عبر خدمات التراسل والاتصالات التي تقدمها الانترنت، تتمثل هذه الأفعال أساسا في الاطلاع على محتوى الرسائل، والالتقاط (الاعتراض)، والتسجيل، والتجميع وغيرها من الأفعال التي يجرمها المشرع الجزائري في سياق حماية الحق في الخصوصية، بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006¹ المعدل والمتمم لقانون العقوبات .

أولا: تجريم فض وإتلاف الرسائل والمراسلات

للتوسيع نطاق التحريم ولضمان حماية الحق في الخصوصية جرم المشرع الجنائي بموجب المادة 303 من قانون العقوبات كل من يفضي أو يتلف رسائل أو مراسلاتها موجهة إلى الخير وذلك بسوء نية إلا ومحل جريمة فض وإتلاف الرسائل والمراسلات الواردة في هذه المادة هو الرسائل أو المراسلات، وبالرجوع إلى قانون البريد والمواصلات السلكية واللاسلكية يقصد بالرسائل وفقا لما ورد في البندين 05 و 16 من المادة 09 من قانون البريد والمواصلات السلكية واللاسلكية أنها " كل أوتسال لا يتعدى وزنا معيناً تسمح مواصفاته التقنية بالتكفل به في الشبكة البريدية وغالبا ما تأخذ الرسائل الظروف" أنها وبذلك لا تدخل المراسلات الإلكترونية المكتوبة في مضمون الرسائل المحددة طبقا للبندين 15 و 16 من المادة 09 من قانون البريد، والمواصلات السلكية واللاسلكية، كونها لا يتم التكفل بها من الشبكة البريدية².

1 - قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية / العدد 84.

2 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 328.

وبالنسبة للمراسلات فلقد عرفت المادة التاسعة في الفقرة السادسة من قانون البريد والمواصلات السلكية واللاسلكية على أنها "اتصال مجسد بشكل كتابي عبر مختلف الوسائل المادية التي يتم توصيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه ولا تعتبر الكتب والمجلات والجرائد واليوميات كمادة للمراسلات، كما عرف قانون البريد والمواصلات السلكية واللاسلكية الجزائري في البند 21 من المادة 08 الاتصالات بأنها "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات، أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية، وبذلك فإن مفهوم المراسلات يتحدد طبقا للمفهوم السابق للاتصالات بأنها المعلومات المتبادلة بين طرفي الاتصال المجسدة بشكل كتابات أو صور عبر مختلف الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ويدخل في نطاق هذا المفهوم المراسلات الإلكترونية المكتوبة، وهو ما يجعل الحماية الجنائية المقررة لسرية المراسلات بموجب المادة 303 من قانون العقوبات الجزائري تنطبق على المراسلات الإلكترونية المكتوبة¹.

واضح من خلال نص المادة 303 من قانون العقوبات على أن: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر إلى سنة وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط"².

أن التجريم عام ليستغرق كافة الرسائل والمراسلات، دون تقييد لشكل الرسائل والمراسلات، فهو لا يتعلق فقط بالورقية منها بل يشمل أيضا - بمفهوم العموم - رسائل البريد الإلكتروني والرسائل الإلكترونية المرسلة عبر السكايب أو أي تقنية اتصال أخرى.

إلا أن السؤال المطروح الذي يمكن طرحه هنا يتعلق بأفعال القرصنة والاقتحام المرتكبة ضد البريد الإلكتروني وحساب السكايب الشخصي، ومدى إمكانية اعتبارها من قبيل الفض المنصوص عليه في المادة 303، ونشير في هذا المقام إلى أن نص المادة 303، وإن كان ينطبق على المراسلات الإلكترونية المكتوبة، إلا أنه قاصر على حمايتها من صورة واحدة من صورة التعدي على سريتها وهي

1 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 329.

2 - قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون العقوبات، الجريدة الرسمية الجزائرية / العدد 84.

الاختلاس ذلك أن الحماية المقررة في المادة 303 من قانون العقوبات تقتصر على أفعال الفض والإتلاف وأن فض المراسلات يشمل فقط الرسائل داخل الظروف الخاصة بها¹.

وفي إطار الصور التجريبية التي أوردها المشرع الجزائري لحماية الحق في الخصوصية عبر الإنترنت تجريم الاحتفاظ وإفشاء واستخدام بيانات شخصية في ظل النظام المعلوماتي باعتباره الليبية التي تولد فيها البيانات الشخصية وتعالج والخزن ويتم تبادلها كما تعتبر أهم وسيلة لإجراء الاتصالات الشخصية والمحادثات السرية والتقاط الصور الخاصة خاصة بظهور الحكومة الالكترونية أصبح لتسيير مختلف المؤسسات يتم عبر الأنظمة المعلوماتية ما يتطلب تبني قواعد البيانات التي تحتوي على بيانات شخصية تعود لعمال وموظفين أو تلاميذ، أو مرضي في المستشفيات، أو متابعين قضائيا في المحاكم وفي كلها بيانات تستحق الحماية التي نصت المادة 303 مكرر 1 من قانون العقوبات يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدام بأي وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون والملاحظ أن الأفعال المجرمة في هذه المادة تشمل التسجيلات - السمعية والسمعية البصرية والصور والوثائق وغيرها من البيانات الشخصية المتحصل عليها جراء إحدى الجرائم المنصوص عليها في المادة 303 مكرر من هذا القانون، ويكتمل الركن المادي بإتيان أحد أفعال الاحتفاظ أو الوضع في متناول الجمهور أو الغير أو الامتناع عن منع وضعها في متناول الجمهور أو الغير أو الاستخدام

بأية وسيلة كانت، وبالتالي فالمشرع أطلق عنان التجريم ولم يهتم بالوسيلة المستخدمة في نشر البيانات الشخصية عبر المواقع الالكترونية والأنظمة المعلوماتية².

ثانيا: تجريم التقاط وتسجيل ونقل بيانات شخصية

نظمت هذه الصورة المادة 303 مكرر من قانون العقوبات بمعاقبتها كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت للالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية دون إذن صاحبها أو رضاه ويتحقق المساس بالمكالمات والأحاديث الخاصة بأي وسيلة كانت سواء التقليدية أو حديثة من خلال استخدام المشرع مصطلح تقنية بدل وسهلة وهذا دليل على أن الحماية جاءت منصبة على التقنيات الحديثة لأن مصطلح تقنية ينصب على الوسائل والآليات التكنولوجية

1 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 329.

2 - عمراوي مارية - حجاج مليكة، المرجع نفسه، ص 329.

المتطورة فضلا على الوسائل التقليدية، ولعل من أهم المكالمات التي تتم عن طريق التواصل بين الأفراد بشكلها الحديث المكالمات التليفونية والتي يعاقب القانون على كل الاعتداءات الواقعة عليها ونستشف ذلك من خلال تحليل الفقرة الأولى من المادة 303 مكرر حيث نلاحظ أن المشرع استعمل مصطلح المكالمات التي تدور عادة بين شخصين أو أكثر، ولقد انتقد الفقه تقصير الاعتداء على المكالمات التي تتم بين شخصين وإنما يجب أن لمدد الحماية الجنائية إلى حديث النفس المسموح وهو الحديث الفردي الذي ينطق به الشخص اعتمادا على أنه في مأمن من أن يسمعه آخر كما في حالة قيام الشخص بالتسجيل الصوتي لمذكراته أو لأفكاره كما أن المشرع لم يشترط أن تكون المكالمات أو المحادثات الملتقطة أو المسجلة أو المنقولة قد تمت في مكان خاص¹.

وبالنظر إلى الإمكانيات التقنية التي تسمح بتسجيل الصورة والحدث عبر كاميرات الهواتف الذكية والقدرة على نقلها مباشرة إلى جمهور غير محدود عبر الانترنت فإن موضوع الخصوصية يصبح مطروحا بإلحاح، وفي إطار حماية خصوصية الاتصالات والحق في خصوصية الصورة الملتقطة من مكان خاص، لأسباب غير مشروعة، تنص المادة 303 مكرر² من قانون العقوبات على أنه: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

- 1- بالنقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو سرية، بغير إذن صاحبها أو رضاه.
 - 2- بالنقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.
- يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة. ويضع صفح الضحية حدا للمتابعة الجزائية."

ولقد أدرج المرسوم الرئاسي 15-261 المحدد التشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المكالمات الهاتفية ضمن الاتصالات الإلكترونية التي تشملها المراقبة، وذلك بموجب المادة الخامسة التي عرفت الاتصالات الإلكترونية بأنها "كل ترسال أو إرسال أو استقبال الأصوات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت والنقال"³.

1 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 327.

2 - القانون رقم 06-23، مرجع سابق.

3 - عمراوي مارية - حجاج مليكة، المرجع نفسه، ص 327.

الشاهد هنا أن التجريم يقع مهما كانت الوسيلة أو التقنية المستخدمة في ارتكاب الفعل، وبالرغم من أن التقنيات المتاحة اليوم يمكن أن تسهل من ارتكاب هذه الأفعال، فجميع الحواسيب الشخصية والهواتف مجهزة بكاميرا ولواقط الصوت، إلا أن المشرع لم يشدد أو يخص الأفعال المرتكبة عبر هذه التقنيات الحديثة بنصوص خاصة.

أما الاعتداء على الأحاديث الخاصة فيعد من أكثر الأمور ارتباطاً بشخصية الإنسان، إذ الإحساس بالأمن الشخصي الذي يستولي على المرء وهو بصدد مكالمات الهاتفية أو محادثاته الشخصية هو ضمان هام لممارسة الحق في الحياة الخاصة.

وتعرف الأحاديث الخاصة بأنها كل صوت له دلالة التعبير عن معنى أو مجموعة معالي من الأفكار المترابطة سواء كانت مفهومة لجمهور الناس أو لفئة قليلة، من خلالها يطلق الفرد العنان لنفسه ويبوح لما يدور في كوامن نفسه ولا يشترط لغة معينة يجري بها الحديث¹.

وبالرجوع إلى نص المادة 303 مكرر من قانون العقوبات نلاحظ أن المشرع لم يحدد الوسيلة التي يتم بها السلوك الإجرامي إلا أنه حدد على سبيل الحصر صور التي يمكن للجاني أن يرتكبها أو ينتهك بها حرية الحديث أو الأحاديث الخاصة وليس هناك ما يحول دون اجتماع هذه الصور ولكن القيام بارتكاب صورة واحدة منها كاف للحقيقي الجريمة، ويقصد بالتقاط الأحاديث الخاصة الحصول على ما جري بين الأشخاص من كلام أو ما تشوه الفرد به سرا ودون علم صاحب الشأن أم التسجيل فيعني حفظ الحديث على جهاز أو أي وسيلة أخرى معدة لذلك بقصد الاستماع إليه فيما بعد أو نقله إلى مكان آخر غير الذي تم تسجيله فيه، أما النقل فيقصد به نقل الحديث أو المكالمة الذي تم الاستماع إليهما أو تسجيلهما من المكان الذي تم فيه هذا الاستماع أو التسجيل إلى مكان آخر غيره وذلك بأية تقنية كانت².

وتتحقق النتيجة الإجرامية المعاقب عليها بموجب نص المادة 303 مكرر من قانون العقوبات بحصول الجاني على المكالمات أو الأحاديث الخاصة وإن كانت ذات المادة بموجب الفقرة الثالثة اعتبرت أن مجرد الشروع والبدء بالتنفيذ وعدم حصول النتيجة تعطل في الجهاز أو ضبط الجاني الأسباب خارجة عن إرادته يعاقب هذا الأخير بعقوبة الجريمة التامة وهذا الاحترام كيان الإنسان وتقديس حياته الخاصة التي حاول أن يضيفي عليها حماية أكثر ورعاية أكبر³.

1 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 328.

2 - عمراوي مارية - حجاج مليكة، المرجع نفسه، ص 328.

3 - عمراوي مارية - حجاج مليكة، المرجع نفسه، ص 328.

ثالثا: تجريم الاحتفاظ وإفشاء واستخدام بيانات شخصية

تنص المادة 303 مكرر 1 من قانون العقوبات¹: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون"

تستهدف الأفعال المجرمة في هذه المادة، التسجيلات (السمعية والسمعية البصرية)، والصور والوثائق، وغيرها من البيانات الشخصية المتحصل عليها جراء إحدى الجرائم المنصوص عليها في المادة 303 مكرر (الالتقاط أو التسجيل أو النقل).

ويكتمل الركن المادي بإتيان أحد أفعال: الاحتفاظ، أو الوضع في متناول الجمهور، أو الغير، أو الامتناع عن منع وضعها في متناول الجمهور أو الغير، أو الاستخدام بأية وسيلة كانت.

وعلى غرار المادة 303 مكرر السابقة، فالمشرع أطلق التجريم ولم يلتفت إلى الوسيلة المستخدمة في ارتكاب الجريمة، وبذلك فإن نشر البيانات الشخصية الذي يتم عبر المواقع الالكترونية والأنظمة المعلوماتية عموما أو استخدامها بأي وسيلة كانت يمثل جريمة تستغرقها المادة القانونية. أما الركن المعنوي فيتمثل في توافر القصد الجنائي العام (العلم والإرادة)، ولم يشترط المشرع القصد الجنائي الخاص.

ومن خلال نص المادة 394 مكرر 2 من قانون العقوبات الجزائي والتي أن المشرع الجزائي أقر مسؤولية الأشخاص المعنوية إذا ثبت ضلوعها في نلاحظ من خلالها أن المشرع أطلق لفظ المعطيات دون أن يخص المعطيات الشخصية بعمارة خاصة، لكن هذا لا يمنع من إمكانية سحب النص وتطبيقه لحماية البيانات الشخصية باعتباره صنفا من البيانات، وهذا إذا ما أخذنا بعين الاعتبار أن الولوج أو البقاء غير المصرح بها في النظام المعلوماتي هو جريمة من الجرائم المنصوص عليها في القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، والتي يمكن أن ترتكب بها في حيازة بيانات شخصية أو إفشاءها أو نشرها أو التصرف فيها بأي شكل².

1 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 328..

2 - عمراوي مارية - حجاج مليكة، المرجع نفسه، ص 329.

والملاحظ أن صور النشاط الجرمي الماسة بالحق في الخصوصية عبر الانترنت المنصوص عليها في قانون العقوبات لن يكتمل بناءها القانوني إذا لم تتوفر فيها قوام القصد الجرمي العلم والإرادة.

الفرع الثالث: الحماية الموضوعية للحق في الخصوصية عبر مواقع التواصل الاجتماعي

إذا كان سحب قواعد الخصوصية على الأنظمة المعلوماتية ووسائل المراسلات والاتصالات ممكننا ومقبولا فإن سحبها على وسائل التواصل الاجتماعي يمكن أن يكون مع الكثير من التحفظ، نظرا لطبيعة هذه التكنولوجيا والإشكالات التي تثيرها. لذلك فإنني وقبل الخوض في موقف المشرع الجزائي اتجاه خصوصية مستخدمي وسائل التواصل الاجتماعي، أجد من المهم بيان الإشكالات المتعلقة بهذه الوسائل.

أولا: إشكاليات الحماية الموضوعية للحق في الخصوصية عبر وسائل التواصل الاجتماعي

تختلف وسائل التواصل الاجتماعي عن وسائل الاتصال الأخرى (الهاتف والسكايب والبريد الإلكتروني...). ويمكن القول إن موضوع الحماية القانونية للخصوصية عبر وسائل التواصل الاجتماعي لا يزال يثير الجدل، ولم يستقر الاجتهاد بعد حول العديد من المسائل في هذا الجانب، خاصة ما تعلق منها بملكية البيانات الشخصية المتداولة عبر هذه الوسائل، ومدى قدرة الأشخاص على التحكم في دورة ما ينشرونه من محتويات عبرها، كذلك مسألة تعارض الخصوصية عبر هذه الوسائل مع حرية التعبير والحق في التجمع والوصول إلى المعلومة.

هذا بالإضافة إلى العنصر الدولي الذي تتسم به مواقع التواصل الاجتماعي وخدمات الانترنت عموما والعديد من المسائل الأخرى التي تدفعنا للتساؤل أولا عن مدى إمكانية تطبيق القواعد القانونية العامة المتعلقة بحماية الحق في الخصوصية، أم أن موضوع الخصوصية عبر وسائل التواصل الاجتماعي يحتاج إلى إيجاد القواعد الخاصة، ثم التساؤل عن جدوى وفاعلية هذه النصوص الخاصة، إذا ما نظرنا إلى الإشكالات التي تحول دون تطبيقها.

1- الملكية والقيمة التجارية للبيانات الشخصية المتداولة عبر مواقع التواصل الاجتماعي

خلافا للشعور العام لدى المستخدمين بمجانية وسائل التواصل الاجتماعي، فهي ليست منشأة على وجه مجاني، ولها هدف مادي هو الربح، وتدخل ضمن إطار اقتصاد الويب الاجتماعي الذي يستند على تمويل الخدمات المقدمة من خلال الإعلانات الموجهة، وبالتالي من خلال استثمار البيانات

الشخصية للمستخدمين. عمالة الانترنت المجانية كفيسبوك ووقول، تحول البيانات الشخصية لمستخدميها إلى أموال، لاسيما ما تعلق بعاداتهم الاستهلاكية ومحو اهتماماتهم وبنمط حياتهم.

وتشكل القيمة الإجمالية للبيانات الشخصية للمواطنين الأوروبيين 330 مليار يورو في السنة من خلال الزيادة في الإنتاج والوصول إلى أسواق جديدة، وذلك وفق ما ورد في دراسة بوستن كونسلتينغ قروب Bosten consulting Group لعام 2012¹.

فوسائل التواصل الاجتماعي تعرض خدمات مبتكرة، مجانية بالعموم، لكن غالبا متاحة مقابل الاستخدام التجاري للبيانات الشخصية للمستخدمين، وقد اعتبرت محكمة التمييز الفرنسية أن تجميع البيانات الشخصية على الانترنت هو عمل غير مشروع، ويرى بالتالي البعض أنه قد يظن المستخدمون أنهم يملكون البيانات الشخصية العائدة لهم، وفي الحقيقة لا أحد يملك الحقائق، فحقائق المعلومات هي مستبعدة من نطاق الحماية بموجب قوانين الملكية الفكرية التي تحمي فقط الابتكار، أما القوانين المتعلقة بأسرار التجارة فهي تحمي المعلومات التي تبقىها الشركات سرية إذا كانت ذات قيمة اقتصادية، ولا تشكل البيانات الشخصية على مواقع التواصل الاجتماعي من هذا القبيل من المعلومات، وعندما تجمع شركات التواصل الاجتماعي معلومات حول ميول المستخدمين واستخدامهم للخدمات، لها وحدها حق المطالبة بملكية هذه الأسرار التجارية وليس المستخدمين، كذلك يمكن حماية قواعد البيانات ومحتواها من البيانات الشخصية بموجب القوانين الأوروبية المتعلقة بقواعد البيانات كونها عائدة لشركات التواصل الاجتماعي ولكن ليس كونها عائدة للمستخدمين². ومع أن مواقع التواصل الاجتماعي قد أقرت بحاجة المستخدمين لديها إلى الخصوصية ووضعت آليات لها، إلا أنها ومنذ البداية قد وضعت السياسات المطبقة لحماية صناعة وسائل التواصل الاجتماعي ولتأمين ازدهارها ومصالحها وليس لخصوصية الأفراد عليها، فإفشاء معلومات أكثر يؤمن مدخولا أكبر³.

2- التعارض مع حرية التعبير والحق في الوصول إلى المعلومة

إن الحق في الخصوصية يتقاطع مع غيره من الحقوق والحريات التي تمارس على شبكة الانترنت، لذلك فقد أشار قرار الجمعية العامة للأمم المتحدة رقم 167/68 إلى هذا التقاطع وشدد على علاقة

1 - وسيم شفيق الحجار: المرجع السابق، ص 68.

2 - وسيم شفيق الحجار: المرجع نفسه، ص 66.

3 - وسيم شفيق الحجار: المرجع نفسه، ص 53.

الحق في الخصوصية مع ثلاثة حقوق على وجه الخصوص، وهي الحق في حرية التعبير، والحق في التجمع والحق في الوصول إلى المعلومات والعمل ضد الدعاية المروجة للجريمة والإرهاب¹.

وفي هذا الخصوص، اعتبرت محكمة الدرجة الأولى في باريس في قرارها تاريخ 2013/11/13 أن حق الشخص باحترام حياته الخاصة قد ينحصر أمام متطلبات حرية التعبير عن الرأي، ويتم تقدير ذلك في ضوء مجموعة من الظروف تتعلق بالضحية وبصفاتها وبتصرفها السابق وبموضوع النشر وبمحتواه وبشكله وكذلك في ضوء سوء النية ومدى التعرض لكرامة الشخص والمشاركة في نقاش ذات اهتمام عام.

وتعتمد المحاكم إلى موازنة الحقوق المتعلقة بالخصوصية بالحقوق المدنية، ولا سيما تلك المتعلقة بالحق في التعبير الحر وفي المعلومات، ويتفوق الحق في حرية التعبير وفي المعلومات، المعترف بهما في الدساتير واتفاقيات حقوق الإنسان على الحق في الخصوصية².

3- مسؤولية المستخدم اتجاه حقه في الخصوصية

يعتبر الكثيرون أن مفهوم المساحة الخاصة على وسائل التواصل الاجتماعي كفيسبوك، لم يعد لها معنى بالنظر لطبيعة هذه الوسائل، فهي أدوات للاتصال، يمكن لكل مستخدم إعادة إرسال المحتوى أو المعلومات التي يتلقاها، فما نقوله لأصدقائنا عليها يمكن نقله إلى أصدقاء الأصدقاء وهكذا دواليك دون وجود طريقة فعالة للتحكم في حركة المعلومات³.

كما أن المستخدم نفسه مسؤول عن انتهاك حيزه الخاص، سواء اتجاه شركات الإنترنت أو اتجاه المستخدمين، فالكثير من المستخدمين يتقبل رقابة تجارية مستمرة من طرف شركات الانترنت، والعديد منهم يهملون وضع إعدادات الخصوصية بالنظر لتعقيدها وصعوبة إجرائها، ونرى أن الكثير منهم، وإن كانوا يعلنون عن حرصهم على خصوصيتهم، لا يقومون بما هو مطلوب منهم لجهة إعدادات الخصوصية على مواقع التواصل الاجتماعي لضمان هذه الخصوصية، بالإضافة إلى ذلك، قد يهمل مستخدمون كثر إجراء هذه الإعدادات أو لا يهتمون أصلاً بها لاعتقادهم أن ما ينشرونه ليس بذي أهمية ولا يشكل خطراً عليهم أو لرغبتهم في نشر صورهم وتعليقاتهم للجمهور ولأكبر عدد من الناس رغبة في

1 - وسيم شفيق الحجار: مرجع سابق، ص 41.

2 - وسيم شفيق الحجار: المرجع نفسه، ص 40 و 42.

3 - وسيم شفيق الحجار: المرجع نفسه، ص 51.

التباهي بما يملكونه أو بمواهبهم أو بشكلهم.. ويبدو أن أغلبية مستخدمي وسائل التواصل الاجتماعي لا يحسنون ضبط إعدادات الخصوصية¹.

وبموجب القوانين المتعلقة بحماية البيانات، على شركات وسائل التواصل الاجتماعي أخذ موافقة المستخدمين بخصوص معالجة بياناتهم ومشاركتها مع الغير أو استعمالها في الإعلانات. فالمادة السابعة من التوجه الأوروبي لعام 1995 تسمح بمعالجة البيانات الشخصية في حال موافقة الشخص المعني بها، وعندما يسجل الفرد، يمكن لمشغل الموقع إبلاغه بالتعليمات المتعلقة بالخصوصية والحصول على موافقته، إلا أن معظم المستخدمين يكسبون على الفأرة لإعطاء الموافقة على شروط الخصوصية دون فهمها أو قراءتها حتى، وتتعلق هذه الشروط في الأساس بمعالجة البيانات التي تجمعها وسائل التواصل الاجتماعي من المستخدمين من خلال التسجيل عليها أو الكعكات.

كما أن العلنية هي عدو الخصوصية بمعنى أن ما يكون علنيا على وسائل التواصل الاجتماعي لا يحترم بطبيعة الحال خصوصية الفرد، والمستخدم بإطلاق التصريحات بشكل علني على موقع التواصل الاجتماعي، يكون قد تخلى عن أي حق باعتبار هذه التصريحات كخاصة².

لذلك فالمعلومات الشخصية التي يشاركها مع أشخاص آخرين على مواقع التواصل الاجتماعي هي معفية من القيود بموجب القوانين الأوروبية المتعلقة بالبيانات الشخصية، فهذه القوانين هي معدة لتحمي الأفراد اتجاه الحكومات والشركات التجارية وليس لتقليص الاتصالات بين الأفراد وتجميع المعلومات من قبلهم، وهذه القوانين لا تحمي الفرد من نفسه ولا من أصدقائه، لأن المستخدم ذاته هو من يضع معلومات متعلقة بحياته الخاصة بتصرف الجمهور، والاجتهاد مستقر على حرمان البيانات الشخصية من الحماية عندما يفشي الشخص المعني ذاته ببياناته الشخصية، وفي هذا الاتجاه، قضت المحكمة الأوروبية لحقوق الإنسان في قرارها بتاريخ 2009/7/23 بأن المعلومات، في حال إيصالها لمعارف الجمهور من قبل الشخص المعني ذاته، فإنها تتوقف عن كونها سرية وتصبح متاحة بحرية³.

ثانيا: الحق في الخصوصية عبر وسائل التواصل الاجتماعي في قانون العقوبات الجزائري إن الأفعال التي تتعرض للخصوصية على وسائل التواصل الاجتماعي هي مشابهة لتلك المرتكبة في العالم الحقيقي، ولا تختلف عنها إلا بطريقة حصولها عبر وسائل التواصل الاجتماعي والاتصالات وعن بعد مقارنة بالوسائل

1 - وسيم شفيق الحجار: مرجع سابق، ص 47 و 55.

2 - وسيم شفيق الحجار: المرجع نفسه، ص 50 و 60.

3 - وسيم شفيق الحجار: المرجع نفسه، ص 70 و 72.

الشفهية أو المادية المباشرة والحاصلة في مجلس واحد، وبالتالي يمكن -بحسب البعض- تطبيق القواعد القانونية ذاتها على هذه الأفعال لا سيما إذا لم يحدد المشرع وسيلة ارتكابها¹.

إلا أنه وبالنظر إلى الاعتبارات المذكورة أعلاه والتي تحول دون حماية فعلية للحق في الخصوصية عبر وسائل التواصل الاجتماعي فإنني أرى أنه من المستبعد ومن غير المنطقي أن تعيد المحاكم تفسير القوانين الخاصة بالخصوصية لتطبيقها على ما يحدث عبر وسائل التواصل الاجتماعي، لذلك فإنه يتوجب على المشرع الجزائري (التشريعات الوطنية) أن يبتكر قوانين جديدة للخصوصية على وسائل التواصل الاجتماعي المستجدة².

أما فيما يتعلق بحماية هذا الحق اتجاه شركات الانترنت والحكومات الأجنبية، فإن المسألة تحتاج إلى أكثر من ذلك، وفي هذا الصدد يمكن أن نذكر الاتفاق الذي توصلت إليه المفوضية الأوروبية عام 2016 مع الإدارة الأمريكية المسمى "Privacy Shield" والذي يسمح باحترام الحريات الأساسية للمواطنين الأوروبيين عند معالجة بياناتهم الشخصية في الولايات المتحدة الأمريكية، وهذا الاتفاق يعطي المواطنين الأوروبيين الحقوق المنصوص عليها في التوجيه الرئاسي حول الحياة الخاصة الصادر عام 2014 وكذلك في القانون الأمريكي لعام 1974 حول الخصوصية المسمى "Privacy Act" والذي ينص على حق الأمريكيين بالاطلاع وبالطعن - ما خلا حالة الأمن الوطني - في حال استعمال بياناتهم بصورة غير مشروعة، مع العلم أن البيانات الشخصية المجمعة في أوروبا، وفي الجزائر وفي أية دولة عبر العالم من قبل وسائل التواصل الاجتماعي الأمريكية، كفيسبوك يتم تخزينها في الواقع في الولايات المتحدة الأمريكية³.

المطلب الثاني: الحماية الإجرائية للحق في الخصوصية الرقمية

بالإضافة إلى موازنة الحق في الخصوصية مع الحق في التعبير والوصول إلى المعلومات، توازن التشريعات والمحاكم بين حق الشخص في الخصوصية ومبررات حماية الأمن الوطني في الدولة لجهة استخدام المراقبة الرقمية على الأفراد لرصد الجرائم وتعقب مرتكبيها.

بالرجوع إلى قانون الإجراءات الجزائية الجزائري، وتحديدا إلى القانون رقم 09-04 المؤرخ في 05/08/2009⁴ الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

1 - وسيم شفيق الحجار: مرجع سابق ، ص 53.

2 - وسيم شفيق الحجار: المرجع نفسه ص 45.

3 - وسيم شفيق الحجار: المرجع نفسه ، ص 71.

4 - القانون رقم 09-04 المؤرخ في 5 أوت 2009.

والاتصال ومكافحتها، نجد أنه يعطي صلاحيات للسلطات القضائية المختصة وضباط الشرطة القضائية بمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية، وهو الأمر الذي قد يتعارض مع الحق في الخصوصية، كون هذه القواعد تنص على السماح بمراقبة الاتصالات الالكترونية وجمع البيانات وحجزها، سواء من طرف السلطات الداخلية أو الأجنبية في إطار التعاون الدولي والمساعدة القضائية. كما تنص أيضا على إلزام مقدمي خدمات الانترنت بحفظ بيانات المستخدمين التي تمكن من التعرف عليهم مثل مكان المرسل والمرسل إليه وعناوين المواقع الالكترونية المطلع عليها¹.

إلا أن اهتمام المشرع بحماية الحق في الخصوصية ليس مغيبا تماما في هذا القانون، حيث يمكن أن نلمس إرادته بالتوفيق بين تبتي القواعد الإجرائية الناجعة لمكافحة جرائم المعلوماتية والوقاية منها وبين تكريس هذا الحق.

من مظاهر تكريس الحق في الخصوصية يمكن أن نسجل ما يلي:

- التأكيد على سرية المراسلات والاتصالات من خلال المادة الثالثة حيث تنص على أنه: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام والآداب العامة أو لمستلزمات التحريات أو التحقيقات القضائية الجارية... وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"
- تحديد الحالات التي يلجأ فيها إلى هذه الإجراءات، حتى تنص عليها المادة الرابعة وهي على سبيل الحصر:
- الوقاية من الأفعال الموصوفة بجرائم الإرهاب.
- في حالة وجود معلومات تقيد احتمال وقوع اعتداء على منظومة معلوماتية اعتداء يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- إذا تعذر الوصول إلى نتيجة بعد استيفاء كافة آليات التحريات والتحقيقات القضائية المتاحة
- إذا كانت في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة
- اشتراط إذن مكتوب من السلطة القضائية المختصة بإجراء عمليات مراقبة الاتصالات الالكترونية
- تقيد مجال استعمال المعلومات المتحصل عليها حيث تنص المادة التاسعة على أنه:

¹ - القانون رقم 09-04 المرجع نفسه.

"تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية"

- إلزام مقدمي خدمات الانترنت وتحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها¹.
- تحديد مدة الاحتفاظ بالبيانات المحجوزة بمدة سنة واحدة من تاريخ التسجيل².

المطلب الثالث: تقييم آليات لحماية الحق في الخصوصية الرقمية وفق قانون العقوبات الجزائري

تباينت سياسية المشرع في تسليط العقوبات المقررة لمجابهة المساس بالحق في الخصوصية عبر الانترنت فبالرجوع إلى الحماية الجنائية لخصوصية الاتصالات والمحادثات والمراسلات والصور الشخصية والتي تناولتها المواد من 303 إلى 303 مكرر 3 من قانون العقوبات حيث عاقب على جنحة الفض أو إتلاف رسائل، أما العقوبات التكميلية الوجوبية فتناولتها المادة 394 مكرر 6 والمتمثلة في مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المحل أو مكان الاستغلال³.

كما أن المشرع الجزائري أقر مسؤولية الشخص المعنوي في حالة ارتكابه الجرائم المنصوص عليه في القسم السابع مكرر السالف الذكر وعاقبه بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وهذا نظرا لأهمية وقدسية الحياة الخاصة للإنسان، والملاحظ أن العقوبات المقررة على الشخص الطبيعي الماسة بالمعالجة الآلية للمعطيات غير كافية مقارنة بالفعل المرتكب، ومن جهة أخرى نلاحظ أن المشرع الجزائري لم يتبع سياسة التحفيز للإبلاغ عن هذا النوع من الجرائم بالتخفيض والإعفاء، وإن كان من الأجدر تبني هذه السياسة لكشف الغطاء عن المجرمين خاصة وأن مثل هذه الجرائم تتم في طي السر والكتمان فضلا على صعوبة معرفة مرتكبيها وإلقاء القبض عليهم.

وبالرجوع إلى العقوبات المقررة في القسم السابع مكرر من قانون العقوبات والمقررة في حالة المساس بأنظمة المعالجة الآلية للمعطيات نجد أن المشرع عاقب الشخص الطبيعي بعقوبة أصلية تتمثل في ثلاثة أشهر إلى سنة حبس و 50.000 دج إلى 100.000 دج غرامة - في حالة الدخول أو

1 - المادة 3/10 من القانون رقم 04-09 ، مرجع سابق.

2 - المادة 11 من المرجع نفسه.

3 - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 330.

البقاء - وقد تشدد العقوبة في حالة الحذف أو تغيير المعطيات حيث تصبح العقوبة من ستة أشهر إلى سنتين حبس، وغرامة من 50.000 دج إلى 150.000 دج، وفي حالة الإقضاء أو النشر أو استعمال المعطيات تقرر على الفاعل عقوبة الحبس من شهرين إلى ثلاث سنوات وبغرامة من 100.000 دج إلى 500.000 دج ، ومراسلات الحبس من شهر إلى سنة وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى العقوبتين والملاحظ أن العقوبة غير كافية مقارنة بالفعل خاصة إذا اكتفي القاضي بالغرامة فقط دون تقرير العقوبة السالبة للحرية. من جهة أخرى نلاحظ أن المشرع الجنائي رفع العقوبة بموجب نصي المادة 303 مكرر، و 303 مكرر 1 بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة من خمسين ألف إلى ثلاثمائة ألف دينار جزائري كل من تعمد المساس بحرمة الحياة الخاصة، وبالتالي فإن للقاضي سلطته في تقدير العقوبة فضلا عن الغرامة المالية المقررة، ونظر لخطورة المساس بالحق في الخصوصية أجاز المشرع للمحكمة أن تحظر على المحكوم عليه من أجل الجرائم المنصوص عليها في المادتين 303 مكرر و 303 مكرر 1 ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 وأكد على ضرورة مصادرة الأشياء التي استعملت لارتكاب الجريمة.

كما أن المشرع الجزائري أقر مسؤولية الأشخاص المعنوية إذا ثبت ضلوعها في ارتكاب الأفعال السالفة الذكر والماسة بالحق في الخصوصية وذلك بتطبيق عقوبات الغرامة المالية فضلا عن العقوبات التكميلية التي قد تصل إلى حل الشخص المعنوي وحسنا فعل المشرع الجزائري بإقرار المسؤولية الجنائية للأشخاص الاعتبارية لأنه في الكثير من الأحيان تنشط أشخاص معنوية والتخصص في المساس بالحياة الخاصة والتعامل مع هيئات أخرى للكشف عن هوية وبيانات شخصية لبعض الأشخاص كالمشاهير ورجال الأعمال مما يعد تعدي صارخ للحق في الخصوصية¹.

¹ - عمراوي مارية - حجاج مليكة، مرجع سابق، ص 330.

خلاصة الفصل الثاني:

ولكل ما تطرقنا إليه نجد انه أصبح لازماً فهم موقف القانون من هذا التقدم التكنولوجي خاصةً عندما يتعلق الأمر باستخدام التكنولوجيا في عملية مراقبة الأفراد, على وجه التحديد والتصدي للانتهاكات الماسة بحقهم في الخصوصية وهذا ما جاء به موقف قواعد القانون الدولي العام ومنها اتفاقيات القانون الدولي لحقوق الإنسان وكذا ممارسات الدول لمعرفة مدى توافق برامج المراقبة مع ما تتضمنه هذه الاتفاقيات من حقوق للأفراد وأبرزها الحق في الخصوصية ومدى التزام الدول بواجباتها تنفيذاً لهذه الالتزامات على الصعيد الداخلي لحماية هذه الحقوق.

وهذا ما جاءت به دراستنا من خلال استعراض الفصل الثاني مفصلاً في بحثين من خلال اظهار أشكال الاعتداء الإلكتروني على الحق في الخصوصية ، وكذل التطرق الى آليات الحماية للخصوصية الرقمية.

الخاتمة

الخاتمة:

في الختام نصل إلى أن مسألة احترام الحياة الخاصة الرقمية وحماية المعلومات الشخصية، ليست موضوعاً جديداً للبحث. إلا أن التقدم التكنولوجي والمعلوماتي أعطى له بعداً جديداً، ولعل هذا ما يفسر سعي التشريعات المقارنة إلى توفير الحماية القانونية لمختلف صور الخصوصية، ووقوف القوانين العقابية في وجه كل منتهك لحرمة الحياة الخاصة بأي شكل أو وسيلة بما تفرضه من قواعد، تجرم كل الاعتداءات القديمة والمستجدة، حتى تواكب ما استحدثته التكنولوجيات الجديدة من مفاهيم وقيم تحتاج الحماية.

فالحق في الخصوصية حق قديم، له أبعاد جديدة، وذلك نتيجة التطورات التكنولوجية في مجال المعلوماتية، فحماية الخصوصية المعلوماتية على جانب من الأهمية لا يمكن إنكاره، ووضع تشريع لحماية المعطيات الشخصية ضرورة وحتمية، على المشرع الجزائري إرساؤه في أقرب الآجال، تكريساً لأحكام الدستور الذي أقر حق الأفراد في الحماية، فيما يتعلق بمعالجة معطياتهم الشخصية، وتجريم كل الانتهاكات التي تقع عليها.

خاصة إذا علمنا أن الغرض من تبني تشريعات لحماية المعطيات الشخصية، يتجاوز حماية حقوق الإنسان أو حرمة الحياة الخاصة، فهي لازمة لتشجيع التجارة الالكترونية والاندماج في المجتمع الرقمي، فلا يمكن للأفراد الإقدام على التعاملات الالكترونية في غياب حماية قانونية لمعطياتهم الشخصية. يعد الحق في الخصوصية في العصر الرقمي قضية معقدة ومتطورة تطرح العديد من التحديات للأفراد والحكومات والشركات. في حين أن التقنيات الرقمية جعلت من السهل أكثر من أي وقت مضى جمع واستخدام المعلومات الشخصية، فمن الضروري التأكد من أن الأفراد قادرون على التحكم في معلوماتهم الشخصية وأن حقوق الخصوصية محمية. من خلال سن قوانين خصوصية قوية واحترام حقوق الخصوصية في العصر الرقمي، يمكننا ضمان أن الأفراد قادرون على المشاركة الكاملة في المجتمع وأن التقنيات الرقمية تُستخدم بطرق تعزز، بدلاً من تقويض، كرامة الإنسان وحرية.

إن المواجهة الفعالة لكافة صور الجرائم المعلوماتية خاصة الواقعة منها على الحياة الخاصة، تتطلب استنفار كافة الجهود على كافة المستويات وهذا من خلال سعي الأجهزة الوطنية والدولية تكريس مفهوم الاستخدام الآمن للتكنولوجيا المعلومات، وتوفير الإمكانيات المادية والبشرية التي تسوغها من امتلاك مهارات ومقومات المواجهة للتطور المتسارع للإجرام المعلوماتي.

يمكن إجمال أهم النتائج المتوصل إليها من خلال هذا البحث، في النقاط التالية:

■ الحق في الخصوصية الرقمية مفهوم مستحدث يعبر عن قدرة الأشخاص على التحكم في تدفق بياناتهم الشخصية عبر الأنظمة المعلوماتية ومختلف تكنولوجيات الإعلام والاتصال الحديثة.

وبالرغم من كونه امتدادا لمفهوم الخصوصية التي نعرفها منذ القدم فإن لهذا المفهوم المستحدث محلا ونطاقا مختلفين.

■ تمثل البيانات الشخصية بنوعها المحددة للهوية والبيانات الشخصية الخاصة محلا للحق في الخصوصية الرقمية، باعتبارها الدعامة الالكترونية للمعلومات الشخصية التي يحق للأشخاص التمتع بها وعدم إعلانها للغير، لذلك فقد حظيت بالكثير من الجهود التشريعية على المستويين الدولي والوطني في سبيل تنظيمها وحمايتها.

■ تمثل الأنظمة المعلوماتية البيئية الالكترونية حيث تخلق البيانات وتعالج وتخزن وتتدفق، لذلك فهي تمثل نطاق الحق في الخصوصية بمختلف أنواعها، بدء بالحواسيب الشخصية والهواتف الذكية والشبكات المعلوماتية ووصولاً إلى مواقع الانترنت، وخدمات البريد الالكتروني والسكايب ووسائل التواصل الاجتماعي. فجميعها تمثل بدورها نطاقا للحق في الخصوصية الرقمية.

■ على غرار معظم الدول المتقدمة، فقد كفل المشرع الجزائري حق الأفراد في الخصوصية من خلال الدستور، وسعى إلى تكريس هذا الحق من خلال صياغة قواعد جنائية على المستويين الموضوعي والإجرائي من شأنها ضمان الحماية الجنائية لهذا الحق. إلا أنه وبخلاف الكثير من التشريعات الداخلية-على غرار فرنسا وتونس مثلا- لا يخصص البيانات الشخصية بتشريع خاص يكفل لها الحماية الجنائية رغم كونها تمثل محل وجوه الحق في الخصوصية الرقمية.

■ يقدم القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 حول المساس بأنظمة المعالجة الآلية، حماية موضوعية للحق في الخصوصية عبر الأنظمة المعلوماتية، بتجريم جملة من الأفعال الماسة بالبيانات عموما دون أن يخص البيانات الشخصية بحماية خاصة، بل هي تدخل في عموم النصوص المتعلقة بحماية الأنظمة المعلوماتية والبيانات بصفة عامة.

تتمثل جملة الأفعال الماسة بالحق في الخصوصية الرقمية أساسا في:

- الولوج إلى أو البقاء غير المصرح بهما في نظام معلوماتي

- إدخال معطيات إلى النظام المعلوماتي أو إزالتها أو تعديلها.

- حيازة أو إفشاء أو نشر أو استعمال البيانات الشخصية.

■ يقدم القانون رقم 23-06 المؤرخ في 20 ديسمبر 2006، حماية موضوعية لخصوصية الاتصالات والمراسلات والصور الشخصية، بتجريم جملة من الأفعال أهمها:

-فض واتلاف الرسائل والمراسلات.

-تجريم التقاط وتسجيل ونقل بيانات شخصية.

-تجريم الاحتفاظ وإفشاء واستخدام بيانات شخصية.

■ فيما تثير وسائل التواصل الاجتماعي العديد من المسائل التي قد تحول دون خلق القواعد الجنائية اللازمة لحماية الحق في الخصوصية عبرها. تتمثل أهم هذه الاشكالات في:

-تعارض الحق في الخصوصية عبر وسائل التواصل الاجتماعي مع حرية التعبير والحق في الوصول إلى المعلومة.

-الملكية والقيمة التجارية للبيانات الشخصية المتداولة عبر مواقع التواصل الاجتماعي.

-الطبيعة العلنية للإنترنت وبالتالي، مسؤولية المستخدم اتجاه حقه في الخصوصية عبر هذه الوسائل.

بالإضافة إلى تدفق البيانات والمحتويات الشخصية عبر وسائل التواصل الاجتماعي لتستقر خارج الحدود السياسية للدول، لذلك فإنه من الصعب خلق قواعد جنائية على المستوى الداخلي فقط.

ولا بد من التعاون وإبرام اتفاقات دولية لتنظيم وخلق الإطار القانوني لحركة البيانات الشخصية المتدفقة عبر الانترنت.

■ إلى جانب الحماية الموضوعية، يقدم القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 الحماية الإجرائية للحق في الخصوصية الرقمية. تظهر من خلال عمل المشرع الجزائري منها على إيجاد التوازن بين تبتي القواعد الإجرائية الناجعة لمكافحة جرائم المعلوماتية والوقاية وبين تكريس هذا الحق.

وبهذا نخرج بالجملة التالية من الاقتراحات:

-تعميق دور الشراكة المؤسسية والمجتمعية من خلال اضطلاع المؤسسات ومنظمات المجتمع المدني بدورها المحوري في عقد الندوات والمؤتمرات بغية التوصل لحلول جذرية تعتمد على وسائل متطورة لمواجهة الجريمة الماسة بالحق في الحياة الخاصة إلكترونيا.

-ضرورة إصدار تشريع جنائي معلوماتي ينظم كافة الاعتداءات والجرائم الواقعة على مستوى العام الرقمي واستخدامات شبكة الانترنت.

-ضرورة الدعوة إلى اعتماد قواعد وحلول تنظيمية مشتركة إقليميا أو عربيا للمسائل والإشكالات المطروحة عن جرائم الاعتداء على حق الخصوصية عبر الانترنت وبذل جهود التعاون وتبادل الخبرات للاستفادة من التجارب الواقعية للدول في هذا المجال.

قائمة المصادر والمراجع

القوانين والمراسيم:

-المادة 12 من الإعلان العالمي لحقوق الإنسان الذي أقرته الجمعية العامة لمنظمة الأمم المتحدة عام 1948م

-المادة 17 من العهد الدولي للحقوق المدنية والسياسية التي وافقت الجمعية العامة للأمم المتحدة عليها سنة 1966

-المادة 39 و 40 من الدستور الجزائري.

-قانون رقم 23 - 06 المؤرخ في 20 ديسمبر 2006. المعدل والمتمم لقانون العقوبات. الجريدة الرسمية للجمهورية الجزائرية، العدد 84.

-القانون 04- 09 المؤرخ 05 / 08 / 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جر عدد 47 المؤرخة في 16/08/2009.

-القانون الأساسي رقم 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية، الرائد الرسمي للجمهورية التونسية، الصادر بتاريخ 30 جويلية 2004.

-القانون رقم 08 - 09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذ الظهير الشريف رقم 15 - 09 المؤرخ في 18 فبراير 2009، منشور بالجريدة الرسمية المغربية رقم 5711، بتاريخ 23 فبراير 2009.

الكتب:

-احمد فتحي سرور، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، سنة 1984.

-اسامة فايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة في القانون الفرنسي والأمريكي وفقا لآخر التعديلات التشريعية، دار النهضة العربية، مصر، سنة 2008.

-بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، لبنان، 2009.

-جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، مصر، 2000.

-حسام الدين الأهوائي، الحق في احترام الحياة الخاصة "الحق في الخصوصية"، دراسة مقارنة، دار النهضة العربية، ط 2، 2002.

-حمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، مصر، 2000.

-خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط 1، 2009.

-دلخار صالح بوتاني: الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، ط 1، 2015.

-السيد عتيق، جرائم الانترنت، دار النهضة العربية، مصر، 2002.

-عبد العال الديربي، محمد صادق إسماعيل: الجرائم الالكترونية، المركز القومي للإصدارات القانونية، القاهرة، ط 1، 2012.

-عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الجزء الثاني: الحماية الجنائية، دار الفكر العربي، الإسكندرية، 2002.

-عبد الفتاح حجازي، الحماية الجنائية المعلوماتية للحكومة الالكترونية، دار الكتب القانونية، مصر، 2007.

-عبد الله عبد الكريم، جرائم المعلوماتية والانترنت في الجرائم الالكترونية، منشورات الحلبي الحقوقية، بيروت، 2007.

-عبد الهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الانترنت، دار النهضة العربية، القاهرة، 2014.

-العربي جنان، معالجة المعطيات ذات الطابع الشخصي الحماية القانونية في التشريع المغربي والمقارن، مراكش، 2010.

-علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة - دراسة مقارنة، منشورات زين الحقوقية، بيروت، 2013.

-عمر ابو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونياً، أطروحة دكتوراه، جامعة القاهرة، 2009.

-عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية)، دار النهضة العربية مصر، 2004.

-فريد هديت، الخصوصية في عصر المعلومات، مركز الأهرام ، القاهرة، 1999.

-كيث دفلين ،الإنسان والمعرفة في عصر المعلومات، ترجمة: شادن اليافي، مكتبة العبيكان السعودية، ط1، 2001.

-محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية مصر، 1994.

-محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، ط1 ، 2016.

-محمد هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة مصر، 1992.

-محمود إبراهيم الغازية، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، 2014.

-محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، ط 1، 2017.

-مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة ضد النظام المعلوماتي، دار النهضة العربية، القاهرة، ط 1، 2015 .

-ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1983.

-منصور بن محمد الغامدي، البيانات الحيوية، البصمة الصوتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، ط 1، 2005.

-نديم عبده، أمن الكمبيوتر (الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي)، دار الفكر للأبحاث والدراسات، بيروت، ط 1، 1991.

-نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008.

-هلاي عبد الله أحمد، جرائم المعلوماتية العابرة للحدود (أساليب المواجهة وفقا لاتفاقية بودابست)، دار النهضة العربية ، مصر، ط 1، 2007.

رسائل ومذكرات التخرج:

-أشرف البكوش، حماية الحياة الخاصة في القانون الجنائي، مذكرة ماجستير، كلية الحقوق والعلوم الاقتصادية والسياسية بسوسة، 2007 / 2006.

-أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، رسالة دكتوراه، جامعة المنصورة، 2006 / 2005.

-سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد تكنولوجيا الإعلام والاتصال، رسالة دكتوراه، جامعة الحاج لخضر - باتنة، كلية الحقوق والعلوم السياسية ، 2014/2015.

-يونس خالد عرب ، جرائم الحاسوب (دراسة مقارنة) ، رسالة ماجستير، الأردن، 1994.

المقالات والمنشورات العلمية:

- الذهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الإلكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية - أدرار، 2017.
- صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، التواصل في الاقتصاد والإدارة والقانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، المجلد 24، 2018.
- عبيدي محمد، مقال موسوم: "تكنولوجيا المعلومات والاتصالات وحتمية التحول الرقمي " منشور في كتاب جماعي موسوم: "القانون والتكنولوجيا الحديثة" صادر عن مخبر القانون والتنمية المحلية بجامعة احمد دراية ادرار، ط1، 2021.
- عمراري مارية - حجاج مليكة، حماية الحق في الخصوصية عبر الانترنت دراسة وصفية تحليلية وفق قانون العقوبات الجزائري، دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، ، السنة الثانية عشر، جامعة زيان عاشور، الجلفة مجلد 12، عدد 3، جويلية 2020.
- كريم عاطف، الخصوصية الرقمية بين الانتهاك والغياب التشريعي، ورقة بحث صادرة في إطار سلسلة أوراق الحق في المعرفة الصادرة عن مركز دعم تقنية المعلومات، القاهرة، 2013.
- منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، سنة 2013.
- وسيم شفيق الحجار: النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط 1، بيروت، 2017.
- يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخليوي اتحاد المصارف العربية ، عمان، الأردن، 2002.

المراجع باللغة الأجنبية:

- Pierre TRUCHE ; Jean-Paul Faugère et Patrice FLICHHY : Administration électronique et protection des données personnelles livre Blanc, rapport au ministre de la fonction public et de la réforme de l'Etat, Paris, la documentation française, 2002,
- Jerome H. Saltzer & M. Frans Kaashoek: Principles of Computer System Design. Morgan Kaufmann Publishers - Elsevier-.USA.2009.
- Fernard Lone Sang. Protection des systèmes informatiques contre les attaques par entrees- sorties. Doctorat de l'Université de Toulouse. Directeurs de thèse : Yves Des warte et Vincent Nicomette. 2012.
- Jean-Jacques Hyest: la fraude informatique vue par le nouveau code pénale, expertises des systèmes de l'information Fvrier.1992.N 147.
- Daniel Kaplan, Informatique, libertés, identities, Fyp Edition 1" avril.2010,P10.

المواقع الالكترونية:

- <https://florc.uk/2023/04/23/%D8%A7%D9%84%D8%AD%D9%82-%D9%81%D9%8A-%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D9%81%D9%8A-%D8%A7%D9%84%D8%B9%D8%B5%D8%B1-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A/>
- https://www.researchgate.net/publication/369142868_alhqwg_alrqmyt_w_alhq_fy_alkhsysyt
- <https://dspace.univ-oran1.dz/items/e211935b-ebbd-43e7-831f-f0b2d2a63188/full>

فهرس المحتويات

شكر وعرفان

مقدمة

أ

2	الفصل الأول: الإطار المفاهيمي لحق الخصوصية الرقمية
4	المبحث الأول: ماهية الحق في الخصوصية الرقمية
4	المطلب الأول: مفهوم الحق في الخصوصية الرقمية
4	الفرع الأول: تعريف الحق في الخصوصية الرقمية
7	الفرع الثاني: التطور التاريخي لحماية الحق في الخصوصية
9	الفرع الثالث: محل الحق في الخصوصية الرقمية
12	الفرع الرابع: الأساس القانوني لحق الخصوصية في العالم الرقمي
21	المطلب الثاني: مبررات حماية حق الخصوصية الرقمية
23	المبحث الثاني: أثر تكنولوجيا المعلومات على الحق في الخصوصية
23	المطلب الأول: ظهور مفهوم الخصوصية المعلوماتية
25	المطلب الثاني: مخاطر تكنولوجيا المعلومات على الخصوصية المعلوماتية
25	الفرع الأول: بنوك المعلومات وقواعد البيانات
26	الفرع الثاني: تصفح المواقع الالكترونية على الانترنت
28	الفرع الثالث: التجارة الالكترونية ووسائل الدفع الالكتروني
28	الفرع الرابع: تقنيات التتبع والمراقبة وتحديد المواقع
30	خلاصة الفصل الاول
32	الفصل الثاني: حماية الحق في الخصوصية الرقمية
33	المبحث الأول: أشكال الاعتداء الإلكتروني على الحق في الخصوصية

33	المطلب الأول: نطاق حماية حق الخصوصية الرقمي
39	المطلب الثاني: الاعتداء على الخصوصية في العصر الرقمي
39	الفرع الأول: الجرائم الواقعة على سرية البيانات الشخصية
40	الفرع الثاني: التجسس الإلكتروني
41	الفرع الثالث: اختراق الحاسبات الآلية والبريد الإلكتروني
43	المبحث الثاني: آليات حماية الخصوصية الرقمية
43	المطلب الأول: الحماية الموضوعية للحق في الخصوصية الرقمية
43	الفرع الأول: الحماية الموضوعية لخصوصية الأنظمة المعلوماتية
47	الفرع الثاني: الحماية الموضوعية لخصوصية الاتصالات والمراسلات والصور الشخصية
53	الفرع الثالث: الحماية الموضوعية للحق في الخصوصية عبر مواقع التواصل الاجتماعي
57	المطلب الثاني: الحماية الإجرائية للحق في الخصوصية الرقمية
59	المطلب الثالث: تقييم آليات لحماية الحق في الخصوصية الرقمية
61	خلاصة الفصل الثاني
63	الخاتمة
68	قائمة المصادر والمراجع
74	فهرس المحتويات