جامعة زيان عاشور -الجلفة-
Zian Achour University of Djelfa
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

قسم الحقوق

# الجرائم المتعلقة بانتهاك الأحكامة الاجرائية المقررة لحماية الحق في الخصوصية الرقمية في الجزائر

مذكرة ضمن متطلبات
نيل شهادة الماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية

إعداد الطالب :
- بن سيد سمير
-

إشراف الأستاذ:
-د. طعيبة عيسى

لجنة المناقشة

| | |
|---|---|
| -د/أ. ضيفي نعاس | رئيسا |
| -د/أ. طعيبة عيسى | مقررا |
| -د/أ. سبع زيان | ممتحنا |

الموسم الجامعي 2020/2019

**اهداء**

بسم الله و الحمد لله الذي وهبنا التفكير و حسن التوكل عليه و الذي أنار لنا السبيل لإنجاز هذا العمل المتواضع.

أهدي ثمرة جهدي المتواضع إلى أغلى ما أملك التي لا أرد جميلها بأي إهداء إلى هدية السماء و منبع الورود و الوفاء إلى من رفع الله من رتبها و جعل الجنة تحت أقدامها إلى أمي الغالية رعاها الله و حفظها لي،

إلى والدي العزيز أطال الله في عمره

الى زوجتي و أبنائي

إلى من ساندوني و ووقفوا بجانبي في مشواري الدراسي

إلى كل أصدقائي

# شكر وعرفان

الشكر العظيم إلى الله تعالى الذي أعاننا بتوفيقه ورضاه على إتمام هذا العمل.

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

أتقدم بخالص الشكر والعرفان الجزيل إلى الأستاذ الدكتور طعيبة عيسى على ما قدمه لي من جهد ورعاية متواصلة، ولم يبخل علي بعلمه ووقته في توجيهيوتشجيعي، وما لمسته منه حسن خلقه وتواضعه وحرصه الشديد على إتمام العمل في أحسن صورة، فكان نعم المشرف ونعم المعلم، زاده الله علما ورفعة، بارك الله فيه وجزاه خير جزاء.

كما أتقدم 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

## مقدمة

يعيش العالم اليوم عصر ثورة المعلومات، بما تعنيه من يسر وسرعة في انتقال المعلومة وأداء المعاملات الإلكترونية، وما نتج عنه بروز مظاهر العالم المعلوماتي، بحيث أضحى من لوازم الحياة الضرورية على المستوى العام والخاص، ومما لا شك فيه أن كل تطور تقني له انعكاساته على المستوى القانوني، فكل المفرزات الحديثة للتكنولوجيا أضحت تثير مسألة توافق إيجابياتها مع ما تخلفه من آثار سلبية على بعض المصالح والحقوق التي تحتاج إلى الحماية الجنائية لها 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 تفتقد إلى المرئية، فلقد أثبتت الدراسات تضاعف مستخدمي الانترنت من 360 مليون نسمة عام 2000 إلى ما يقارب2.7 مليار نسمة في عام 2013 وتوسع تفاعل الأشخاص مع الشبكة وأضحي أكثر تأثيرا في حياتهم اليومية من خلال انتقال الحياة اليومية للأفراد من مجالها الحقيقي إلى فضاءات رقمية كمواقع التواصل الاجتماعي والبريد الالكتروني وبروز 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 للأفراد.[1]

**أسباب اختيار الموضوع :**

- الرغبة الشخصية في دراسة الموضوع
- طبيعة تخصصي في مجال القانون الجنائي
- خطورة الظاهرة و انتشارها
- الوجه السيئ لتكنولوجيا المعلومات و أثره 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، ص 3

**أهمية الدراسة**

تظهر أهمية الدراسة في طبيعة الموضوع الذي نتناوله من خلال إبراز مخاطر التكنولوجية الرقمية على الحق في حرمة الحياة الخاصة الرقمية ، لأن التمادي في ابتكار تقنيات التجسس دون وازع ولا رادع قد نتحول من خلالها من الدولة المدنية إلى مجتمعات لاإنسانية، فستر خصوصية الفرد هي فطرة طبيعية فرضتها قوانين الطبيعة، وكثرة ضحايا تكنولوجيا الإعلام والاتصال في المجتمع الجزائري، مع كثرة حالات الانتقام ممن انتهكوا حقهم المقدس في حرمة حياتهم الخاصة، مما يؤدي كل هذا إلى تزايد عدد الجرائم؛

**اهداف الدراسة**

من بين الأهداف التي اسعى الى الوصول التعريف بالحق في حماية الخصوصية الرقمية في التشريع الجزائري، وكذلك تبيان أشكال الاعتداءات على الخصوصية الرقمية و الانتهاكات التي تتعرض لها الخصوصية الرقمية في ظل التطور الهائل الذي تشهده تكنولوجيا الاعلا م و الاتصال

**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 أن 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 الجرائم الماسة بالأحكام الاجرائية المقررة لحماية الحق في الخصوصية الرقمية في الجزائر؟

**منهج الدراسة :**

اقتضت مني طبيعة الموضوع اتباع المنهج الوصفي من خلال التعريف بالخصوصية الرقمية ، و كذلك المنج التحليلي من خلال تحليل النصوص التشريعية التي أقرها المشرع الجزائري لحماية الخصوصية الرقمية

**خطة الدراسة:**

وللإجابة على هذه الإشكالية المطروحة ، ارتأت تقسيم الدراسة الى فصلين ، يتناول الفصل الأول بالدراسة الاطار المفاهيمي للخصوصية الرقمية الخصوصية ، وذلك في مبحثين ، خصصنا الأول

لأثر تكنولوجيا المعلومات على الحق في الخصوصية. أما المبحث الثاني مفهوم حق الخصوصية الرقمية المعلوماتية،

وأفردنا الفصل الثاني لدراسة آليات حماية خصوصية الرقمية و الذي احتوى مبحثين ، خصص المبحث الأول لأشكال الاعتداء الإلكتروني على الحق في الخصوصية أما المبحث الثاني : آليات الحماية للخصوصية الرقمية في التشريع الجزائري

**صعوبات الدراسة**

ولقد واجهتني عدة صعوبات أبرزها :

الازمة الوبائية و التي ألقت بظلالها على الدراسة، حيث أغلقت الجامعات و المكتبات ، نتيجة لتطبيق إجراءات الحجر الصحي ، إضافة الى قلة المراجع التي تناولت الموضوع

# الفصل الأول : الاطار المفاهيمي للخصوصية الرقمية

## الفصل الأول: الاطار المفاهيمي للخصوصية الرقمية

لا نزاع اليوم في أن الخصوصية تعد من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الانسانية كأصل عام، فهي تعد أساس بنيان كل مجتمع سليم، ويعتبر من الحقوق السابقة عن وجود الدولة ذاتها.

لذا تحرص المجتمعات خاصة الديمقراطية منها على كفالة هذا الحق، وتعتبره حقا مستقلا بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعى إلى ترخيصة 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 الخاصة.[1]

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

[1] – فريد هدكيت، الخصوصية في عصر المعلومات، مركز الأهرام للترجمة والنشر، القاهرة، 1999، ص 123.

## المبحث الأول: أثر تكنولوجيا المعلومات على الحق في الخصوصية.

تعتمد المجتمعات الحديثة كليا على تكنولوجيا المعلومات، في تسيير الشؤون العامة والخاصة، فلا يمكن للأفراد في هذا العصر الاستغناء عن هذه التقنية؛ فالبريد الإلكتروني، وبطاقات التعريف الالكترونية ووسائل الدفع الإلكترونية، والتواصل والحوار الإلكتروني والتسلية كذلك، فلهذه التكنولوجية الحديثة أثرها على مختلف مناحي الحياة الاجتماعية والاقتصادية والثقافية ... الخ ، ويبدو أنّ لها أثرا خاصا على الحق في الحياة الخاصة، يمكن تبينه في ظهور مفهوم جديد للخصوصية هو الخصوصية المعلوماتية، إلى جانب المفاهيم التقليدية، كما أنّ إساءة استخدام هذه التكنولوجيا، أوجد مخاطر غير مسبوقة وجدت في البيئة الالكترونية 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 الشخصية.[1]

تغيّر 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 و تداولها دون علم أصحابها، بهدف توجيه الدعاية أو لقياس المؤشرات

[1] – يونس عرب، موسوعة القانون وتقنية المعلومات الجزء2: الخصوصية و حماية البيانات في العصر الرقمي، منشورات اتحاد المصارف العربية، 2002، ص60.

الاقتصادية، أو مراقبة الأفراد ورصد مختلف سلوكاتهم لأغراض أمنية. ما أكد أنّ الحياة الخاصة للأفراد إلى جانب باقي الحقوق والحريات بحاجة للحماية في عصر المعلومات.[1]

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 و مدى سيطرتهم عليها.[2]

وجّهت العناية إلى موضوع حماية المعطيات المتعلقة بالأفراد من خطر استخدام أنظمة المعالجة الآلية في مطلع الستينيات من القرن الماضي، كأولى الموضوعات التي أثيرت حول 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 firoodom لصاحبه Alan Westin سنة 1967.[3]

الثاني: الاعتداء على الخصوصية The Assault on privacy لمؤلفه Miller Arthr Raphael سنة 1971.[4]

عرف الأول خصوصية المعلومات على أنّها: "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

[1] – علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة – دراسة مقارنة، منشورات زين الحقوقية، بيروت،2013، ص 408 و ص 409.

[2] – العربي جنان، معالجة المعطيات ذات الطابع الشخصي الحماية القانونية في التشريع المغربي والمقارن، مراكش، 2010، ص 17 و 18.

[3] – صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، التواصل في الاقتصاد والإدارة والقانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار – المجلد 24 – العدد 02 – أوت 2018 ،ص 126.

[4] –المرجع نفسه، ص 126.

التقنية الحديثة، حيث استعرض الصعوبات والتباينات الثقافية في استخدام المصطلح واختلاف المفهوم القانوني للخصوصية في المعلومات بين النظم القانونية.[1]

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 عليها "[2]، مع ملاحظة أنّه من الشائع استخدام مصطلح الخصوصية مستقلا ومنفردا دون إلحاقه بالبيانات في البيئة الإلكترونية للدلالة على حماية البيانات، وكذلك في الدراسات الأكاديمية والتقنية، دون أن يعني ذلك ترادفا أو تطابقا 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 المكان.[3]

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 1967، معبرا عن قلقه من ما يمكن أن يحدثه الحاسوب بالحياة الخاصة، وهي المقولة التي تتكرر دائما عند الحديث عن الخصوصية والمعلوماتية، والتي تعبر عن وضعية الحياة الخاصة في عصر تكنولوجيا المعلومات: " إن الحاسب بشراهته 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 رأسا على عقب، ليخضع فيه الأفراد لنظام رقابة

[1] – صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، التواصل في الاقتصاد والإدارة والقانون، ص126.

[2] –أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، رسالة دكتوراه، جامعة المنصورة،2005/ 2006، ص 470 و471.

[3] – يونس عرب، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات – نادي المعلومات العربي – 16–17 أكتوبر 2002 – عمان – الأردن تحت عنوان: دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، لصاحبها ، ص 19.

صارم يتحول المجتمع بذلك إلى عالم شفاف تصبح فيه بيوتنا و معاملاتنا المالية وحالتنا العقلية والجسمانية عارية لكل مشاهد عابر....[1] 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، فاتسع على نحو كبير استخدام الحاسبات لتجميع و تخزين ومعالجة البيانات الشخصية، لأغراض متعددة فيما يعرف ببنوك المعلومات أو المراكز الوطنية للمعلومات.

بنوك المعلومات مجموعة من البيانات أو المعلومات المنظمة بطريقة خاصة، في سجلات أو ملفات تسمح برامج الحاسوب من البحث عنها، واسترجاعها ومعالجتها، و تمكن من الوصول إلى محتواها، وإدارتها وتحديدها بسهولة، والتي تكون قاعدة بيانات، و يتكون بنك المعلومات الواحد من مجموعة من قواعد البيانات.[2]

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، تعتزم تأسيس بنوك للمعلومات، من خلال جمع بيانات عديدة ومفصلة عن الأفراد: كالوضع الصحي والتعليمي والعائلي والقانوني.[3]

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 التوجيه الخاطئ لمراقبة الأفراد، وتعرية خصوصياتهم.

كما أنّ بنوك المعلومات تجعل المعلومات الشخصية، التي كانت منعزلة ومتفرقة التوصل إليها صعبا أو متعذرا، مجمعة ومتوافرة بشكل كامل، وسهلة المنال يمكن تحميلها وتخزينها في

[1] – صبرينة جدي، مرجع سابق، ص128.

[2] – نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2008، ص 167.

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

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 وتصويبها.[1]

**الفرع الثاني: تصفح المواقع الالكترونية 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 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 برتوكول 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 صفحة.[2] أما المواقع التفاعلية ومنتديات الحوار فتتطلب من المستخدم ملا 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 خطرا أكبر على خصوصية الفرد، فهي تسمح بتواصل وتبادل المعلومات ونشر الصور والتعليقات، وتوثيق العديد من الأحداث والممارسات اليومية، التي يتم جمعها ومعالجتها

[1] – أيمن عبد الله فكري، المرجع السابق، ص 502 و 503.

[2] – محمود إبراهيم الغازية الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص 20 و ص 21.

وتخزينها، ما يفقد صاحبها سيطرة عليها بمجرد عرضها على الموقع، كما قد تستخدم للحكم عليه أو تصنيفه ضمن فئة معينة.[1]

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 في تطوراتها اللاحقة عدت وسيلة لتتبع الأشخاص وكشف حياتهم بل وإهدار توقعهم في التخفي؛ إذ تستخدم كوسيلة لبناء الدراسات التسويقية وملاحقة الزبائن[2]، مما يثير التساؤل حول مدى مشروعيتها ومدى مساسها بخصوصية الأفراد ؟

**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 و تتم 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 يتهدد 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 المتعامل يصرح ببيانات

[1] – عبد الهادي فوزي العوضي، الحق في الدخول في طي النسيان على شبكة الانترنت، دار النهضة العربية، القاهرة، 2014 ، ص 93 و 94

[2] – صبرينة جدي، مرجع سابق، ص 130.

شخصية، يتم تداولها مع المؤسسات المالية و مقدمي السلع أو الخدمات والوسطاء، بشكل قد يتيح الاستيلاء عليها لأغراض إجرامية.[1]

**الفرع الرابع: تقنيات التتبع والمراقبة وتحديد المواقع.**

أفرز التقدم العلمي انظمة وتقنيات جديدة، كان الغرض منها تسهيل عمليات التعقب 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 و السيارات . فإساءة استخدامه لتتبع الأشخاص ومراقبتهم كابوس حقيقي يهدد خصوصية الفرد، كذلك الأمر بالنسبة للرقائق RFID وهي اختصار لد Radio – frequency identificatio ، وهي تقنية تستخدم لتتبع المواشي أو البضائع حول العالم. يستخدم الكثير من المصنعين رقائق التتبع لمعرفة موقع كل منتج يصنعونه منذ لحظة إنتاجه، والتقاطه ووضعه 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 علمنا.[2]

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

[1] – عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الجزء الثاني: الحماية الجنائية، دار الفكر العربي، الإسكندرية، 2002 ، ص 56 و مايليها.

[2] – صبرينة جدي، مرجع سابق، ص130.

يساعد على القبض على الجناة والفارين، إلا أنها قد تتحول إلى أنظمة رقابة خانقة على الحريات، متى أسيئ استخدام تلك التسجيلات.[1]

مع ضرورة الإشارة في هذا المقام؛ أن تكنولوجيا المعلومات تعرض على المستخدمين تقنيات، وبرامج التأمين وحماية البيانات الشخصية؛ كبرامج التشفير وبرمجيات الجدار الناري، وخاصية التعرف على المستخدم، كما يوصي المختصون بسلوكيات معينة للحيلولة دون الوصول إلى البيانات الشخصية للأفراد[2]، وتوخي الحذر عند التعامل مع تقنية المعلومات عموما، والانترنت خصوصا، 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

## المبحث الثاني: الإطار المفاهيمي لحق الخصوصية الرقمية

مع تزايد التقنيات الحديثة زادت المخاطر على حق الانسان 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 اذا 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 الخصوصية [1] الرقمية مفهوم يقترن 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 الى طبيعة الحق التي تكتسب صفة المرونة وعدم التحديد والضبط في إطار محدد وتختلف باختلاف المجتمعات الانسانية والحقب الزمنية عبر العصور [2].

**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

---

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

وسيم شفيق الحجار: **النظام القانوني لوسائل التواصل الاجتماعي**، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط1، بيروت ،2017، ص37

[2] – الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الإليكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية – أدرار، العدد الثامن، المجلد الأول، 2017، ص 142.

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

فوفقا للفقيه « EDWARD BLOUSTEIN » أن الخصوصية هي الحق في حماية الحياة الشخصية للأفراد وضمان عدم الاعتداء عليها واستقلالها.[1]

أما وفقا للفقيه « GAVISON Ruth » فلقد بني مفهوم الحق في الخصوصية وفقا ل 3 عناصر السرية والعزلة والتخفي بحيث اعتبر أنه الحق في الحماية ضد التدخل في الحياة الخاصة وشؤون عائلتهم بوسائل مادية مباشرة او 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 الاخرين ، والثاني إعلامي مقتضاه ألا تكون الشؤون الخاصة بالفرد محلا للحق في الإعلام بالنسبة للآخرين مما يستتبع معه عدم استغلال الآخرين لتلك المعلومات بالنشر أو التشهير.[2]

**ثانيا : 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 الأنفسهم مدى وصول المعلومات المرتبطة بحياتهم الخاصة للآخرين، وبأن يضبط عملية حصر المعلومات الشخصية ومعاملتها اليا، واستخدامها في صنع القرار الخاص أو المؤثر في حياتهم.[3]

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

---

[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، سنة 1992، ص 176

[3] – حسام الدين الأهوائي، الحق في احترام الحياة الخاصة ( الحق في الخصوصية، دراسة مقارنة، دار النهضة العربية، ط2، 2002، ص 132

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 للآخرين[1]. فهي شكل مستحدث للخصوصية لها علاقة مباشرة بالمعلومات، لأن جانبا مهما من المعلومات الحساسة والخاصة بالأفراد قد أضحى اليوم متاحا عبر الأنظمة المعلوماتية والانترنت خاصة، بحيث يصعب تعقبه أو استرجاعه أو جعله قابلا للنسيان. لذلك فإن الفقيه ميلر Miller يعرفها بأنها "قدرة الأفراد على التحكم بدورة المعلومات المتعلقة بهم[2]. 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 عموما، إلا أنه يختلف عن الأخير بكونه يتصل على وجه التحديد بالمعلومات الخاصة وبمدى 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 بهم.[3]

وبهذا فقد نجد أن الحق في خصوصية المعلومات الشخصية يتوقف على فكرة الاعتداء عليها إلكترونيا من قبل الآخر، واستخدامها وفقا 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 التصرف،[4] وبهذا فإن المعنى العميق لمفهوم الخصوصية يتجلى في تبني تلك الرخصة في حرية التصرف وضمان عم التدخل أو التطفل

---

[1] –توبي مندل وآخرون: **دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير**، الأمم المتحدة، منشورات اليونسكو، فرنسا ،2013، ص02.

[2] المرجع نفسه، ص13

[3] – محمود إبراهيم غازي، مرجع سابق، ص 272

[4] – السيد عتيق، جرائم الانترنت، دار النهضة العربية، مصر، 2002، ص 61

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 الإلكترونية.[1]

**ثالثا : المفهوم التشريعي للحق في الخصوصية الرقمية**

بداية إن مفهوم الخصوصية قد بني في مختلف التشريعات المقارنة تحت إطار ضمان الحد الأدني في حق الفرد بعدم التدخل أو المساس بالحياة الشخصية أو الأسرية أو خرق لسرية المعاملات 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 أواقتحام 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 يرتكز عليه بقية حقوقه، ويرى الكثير من الباحثين أن حقوق الإنسان عامة هي نتاج الفكر الأوربي الحديث ووليدة تربته التي اينعت بالثورة الانجليزية عام 1688 والثورة الفرنسية عام 1789 وما تمخض

[1] – عبد الفتاح حجازي، الحماية الجنائية المعلوماتية للحكومة الالكترونية، دار الكتب القانونية، مصر، 2007، ص 33

عنها من مبادئ الاهتمام بحقوق الإنسان وحريته[1] اهمها 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 الأتفافية الدولية 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 مراسلاته "، كما اعترفت الاتفاقية الأوربية 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 ومراسلاته، ولا يجوز للسلطة العامة التدخل في مباشرة هذا الحق إلا إذا كان هذا التدخل بنص عليه القانون، وبعد إجراءا ضروريا في مجتمع ديمقراطي لحماية الأمن الوطني العام أو الرفاهية الاقتصادية للدولة، أو لحماية النظام أو لمنع الجرائم أو لحماية الصحة أو الأداب أو لحماية حقوق الغير وحرياتهم. [2]

وقد شهد العالم خلال النصف الثاني من القرن العشرين ثورة هائلة في مجال تقنية المعلومات. كان من أهم إفرازاتها ظهور الحساب الألي الذي غزا أوجه كل النشاط الإنساني وأضحي حاجة أساسية لكل بيت متطور أو مدرسة أو مصنع أو غير ذلك من المرافق والمؤسسات، وتوج التطور المتلاحق في تقنية المعلومات بظهور الأنترنت التي خلفت بيئة افتراضية لتدفق فيها المعلومات والاتصالات عبر الحدود، ودون أي اعتبار للحدود أو السيادة، وسهلت عن طريق استخدامها المختلف الاتصالات وسرعة الحصول على المعلومات في أي مكان في العالم وسهولة سرعة تبادل الأبحاث والمعلومات، واحتل البريد الالكتروني أهمية بالغة في انتشار استخدام الانترنت في المراسلات والاتصالات على كافة المستويات، والى تطور العلاقة بين وسائل الإعلام والفرد الذي لم يعد منلقي بل طرفا في العلاقة الإعلامية ،

[1] –عمراوي مارية–حجاج مليكة، حماية الحق في الخصوصية عبر الانترنيت 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، ص3.

[2] – عمراوي مارية–حجاج مليكة، مرجع سابق، ص 326

فله أن ينشر ما يريد وأن يعبر عن رأيه إلى جميع مستخدمي الانترنت في شتى أنحاء العالم، مما أعطى للخير سرعة أكبر في الانتشار وعدد أكبر من القراء وجعل من الفرد العادي محررا ورئيس تحرير، وناشرا وطابعا وموزعا[1].

إلا أن هذا الجانب المشرق لتطور وانتشار تقنية المعلومات والانترنت، 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 حرماتها وتعرية أسرارها، وتهديد سكينة الإنسان وطمأنينته خاصة أمام عدم قدرة الإنترنت على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات[2] خاصة عقب كشف العالم ادوارد سندون سنة 2013 من برنامج لجسم أطلقته وكالة الأمن القومي على شركات الانترنت بتفويض من جورج بوش بعد هجمات الحادي عشر سبتمبر سنة 2001.

### الفرع الثالث : محل الحق في الخصوصية الرقمية

كشفت دراسة صادرة عن لجنة التجارة الفيديرالية( FTC)[3]عام 1999 أن 92.08 % من مواقع الويب كانت جمعت على الأقل نوعا واحدا من بيانات الهوية ( identifyinginformation)، على غرار الاسم، العنوان البريدي، عنوان البريد الالكتروني[4]. 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.

---

[1] – عمراوي مارية–حجاج مليكة ،مرجع سابق، ص 326

[2] – عمراوي مارية–حجاج مليكة ،مرجع سابق ، ص 326.

[3] Federal Trade Commission–

[4] Winnie Chung and John Paynter: **Privacy Issues on the Internet**, Department –of Management Science and Information Systems, School of Business, The University of Auckland, Private Bag 92019, Auckland, New Zealand. Proceedings of the 35th Hawaii International Conference on System Sciences – 2002. IEEE.

## 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 المعلومة[1].

وتقوم مختلف الأنظمة المعلوماتية اليوم في أدائها على تمثيل البيانات تمثيلا رقميا، باستعمال الرقمين 0 و1 فقط .

يشار لها أيضا بالمعطيات ذات الطابع الشخصي، أو البيانات الاسمية. فنجد المشرع الفرنسي مثلا، قد استخدم عبارة البيانات الاسمية بشكل أساسي في القانون رقم 17/78، ( 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 التعديل بموجب قانون 801/2004 الصادر في 6 أوت 2004،[2] 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

[1] كيث دفلين ،**الإنسان والمعرفة في عصر المعلومات**، ترجمة: شادن اليافي، مكتبة العبيكان، السعودية، ط: 1، 2001م، بتصرف

[2] – صبرينة جدي، مرجع سابق، ص127

إذا كان الشخص قابلا للتعرف عليه، يلزم الأخذ بالاعتبار مجموع الوسائل التي من شأنها التمكين من تعريفه"[1] وبنفس الصيغة تقريبا عرّف المشرع المغربي المعطيات الشخصية.[2]

بينما عرّفها 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 شخصا طبيعيا معرفا أو قابلا للتعريف بطريقة مباشرة أو غير مباشرة، باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانونا"، وجاء في نص الفصل 05 من نفس القانون:" يعد قابلا 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".[3]

يعد هذا التعريف، تعريفا وظيفيا 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 فردا معروفا 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 المجهلة أو التي تم تجهيلها (les données anonymes ou anonymisees) لا يشملها مفهوم المعطيات الشخصية.[4]

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

---

[1] –المرجع نفسه، ص127

[2] – القانون رقم 08–09 المتعلق ب حماية 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

[3] –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 الالكتروني: . www legislation . tn

[4] – أشراف البكوش، حماية الحياة الخاصة في القانون الجنائي، مذكرة ماجستير ،كلية الحقوق و العلوم الاقتصادية و السياسية بسوسة، 2007 / 2006 ، ص 59

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 تعريفي أو إلى واحد أو مجموعة من العناصر التي تخصه..."[3].

أو كما تعرفها اتفاقية 108 [4]" 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 الإثني والمعطيات المتعلقة بالآراء السياسية، والمعتقدات الدينية، أو الانتماء النقابي، وكذا المعطيات المتعلقة بالصحة أو الحياة الجنسية، تضاف إليها البيانات المتعلقة بالأحكام الجزائية، والتي تستوجب

---

[1] القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 5 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية/ العدد 47.

[2] – Commission Nationale de l'Informatique et Libérés

[3] –المادة الثانية من قانون 6 جانفي 1978 المتعلق بالمعلوماتية، الملفات والحريات.

Loi n° 78-17 du 6 janvier 1978, modifiée le 6 août 2004

https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive annotee.pdf

خالد ممدوح إبراهيم: **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص50.

[4] –المادة الثانية من **الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة آالية للبيانات الشخصية 108**، المجلس الأوربي ستراسبورغ 1981.

Convention for the Protection of Individuals with regard to Automatic Processing of PersonalData

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?d

ocumentId=0900001680078b37

مستوى أعلى من الحماية،[1] 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. يتمثل النوع الأول في الحروف والأرقام والرموز. والتي تتمثل أهمها فيكلمات المرور التي تسمح أو تمنع المستخدم من الولوج إلى الحاسوب الشخصي أو قاعدة البيانات أين يعمل أو الولوج إلى البريد الالكتروني أو البيانات التي يقتضيها اتمام معاملة من معاملات التجارة الالكترونية. أو تسجيل الدخول إلى منتدى أو حساب شخصي على موقع الكتروني.فيما يتمثل النوع الثاني في القياسات الحيوية، على غرار بصمة الإصبع، بصمة القزحية، البصمة الصوتية ،بصمة أبعاد الكف، خط اليد(التوقيع)، بصمة الوجه... إلخ[2].

**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 العدلية[3] المخزنة لدى المؤسسات العامة والخاصة في شكلقواعد بيانات، أو في خوادم الشبكات المعلوماتية[4]. 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.

---

[1] – العربي جنان، معالجة المعطيات ذات الطابع الشخصي الحماية القانونية في التشريع المغربي والمقارن، مراكش، 2010، ص 41.

[2] – منصور بن محمد الغامدي: **البيانات الحيوية، البصمة الصوتية**، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض ،ط1، 205، ص 06.

[3] –المادة السادسة من **الاتفاقية حول حماية الأفراد المتعلقة بالمعالجة آللية للبيانات الشخصية 108**، المرجع السابق.

[4] –إيان ليه: **الإشراف على استخدام البيانات الشخصية**، مقال متاح على الرابط:
www.dcaf.ch/content/download/.../1/.../Tool_6_intel_over_AR.pdf

## الفرع الثالث: 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 يسرومرونة 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 العامة العقابية بما يتماشى وحماية حق الخصوصية في المجال الإلكتروني أو استحداث تشريعات خاصة تغطي هذه الحماية

### أولا: حق الخصوصية في ظل الحماية الدولية

مما لا شك فيه أن الحماية الدولية لحقوق الإنسان قد أخذت أهمية واسعة نظرا للدور الذي تقوم المواثيق 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 بجملة من التوصيات التي تبرز خطر الحاسبات الإلكترونية على الحياة الخاصة وضرورة إيجاد آليات على المستوى الإقليمي أو الدولي لمحاربة أجهزة التجسس[1]

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

**- المؤتمر الدولي الأمن المعلومات الإليكترونية المنعقد بمسقط سنة 2005**

ركز المؤتمر على بحث ودراسة أهم التهديدات الإليكترونية والمخاطر التي تمس باقتصاديات الدول وتحد من التنمية، وعمل على الخروج بتوصيات خاصة بالتأكيد على التعاون الدولي

[1] – يونس خالد عرب ، جرائم الحاسوب (دراسة مقارنة) ، رسالة ماجيستر، جامعة الأردن، 1994، ص 125.

المكافحة الجريمة ووضع سياسات مشتركة للقضاء على الآثار السلبية لتكنولوجيا المعلومات التي تهدد الحياة الخاصة.[1]

**- 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 لدراسة التوجهات المستحدثة في هذا المجال والسعي لتبادل الخبرات في مجال مكافحة جرائم تقنية المعلومات.[2]

**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 الإليكترونية.

**- 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 للانترنت 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 الشخصي.[3]

---

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

[2] – محمود ابراهيم غازي، المرجع السابق ، ص 204

[3] – Daniel Kaplan, Informatique, libertées, identities, Fyp Edition 1" avril.2010,P10.

**- 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 الرقمي[1]، 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 تنطوي على تهديد لسرية وسلامة النظم والبيانات المعلوماتية للأفراد، كما أقرت ضرورة تكريس التشريعات الداخلية المجموعة من القواعد في النظم العقابية الخاصة بها بغية وضع إجراءات أمنية فعالة ضد تلك الانتهاكات.[2]

وكذا جاءت الاتفاقية في نص المادة على النص على جريمة الاعتراض القانوني غير القانوني باستخدام الوسائل الفنية للبيانات المتداولة إلكترونيا 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 الإلكترونية.[3]

**- 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

[1] –خالد ممدوح إبراهيم، المرجع السابق، ص 276

[2] – محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، سنة 2016، ط1، ، ص 161.

[3] – هلالي عبد الله احمد، جرائم المعلوماتية العابرة للحدود ( أساليب المواجهة وفقا لاتفاقية بودابست)، دار النهضة العربية ، مصر، ط 1، سنة 2007، ص 22

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 وحفاظا 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 المعلومات.[1]

**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 حمائية ضد الاعتداءات الماسة بهذا الحق.

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 17-78 الصادر في10/06/ 1978 الخاص بحماية البيانات الاسمية للمواطنين في مواجهة نظم المعالجة الآلية للمعلومات.

[1] – محمود إبراهيم غازي ، المرجع السابق، ص 235

**والثاني:** القانون رقم 19-88 الصادر في 01/05/ 88 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 والفردية.[1]

وحرص المشرع الفرنسي على مواصلة مكافحة الاعتداءات الواقعة على حق الخصوصية في إطار التشريعات العقابية بحيث كرس جملة من المواد بموجب قانون العقوبات الجديد رقم92- 684 الصادر في7/22/ 1992 والذي دخل حيز التنفيذ ابتداءا من 03/01/ 1994

وتضمن القانون أحكاما جديدة لمواجهة ظاهرة الإجرام المعلوماتي تحت عنوان : الاعتداء على نظم المعالجة الآلية للمعلومات.[2]

ولقد جرم المشرع أفعال المساس بالحق في حرمة الحياة الخاصة تحت عنوان الاعتداء على الحياة الشخصية فنجده 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 التعويض.[3]

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 الإصدرات 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

---

[1] – احمد فتحي سرور، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، السنة 54، 1984، ص 30

[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 ابو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونيا، أطروحة دكتوراه، جامعة القاهرة، 2009، ص163.

مساحة واسعة لتفسيرنصوص الدستور في نطاق حماية الحقوق والحريات وبالأخص الحق في الخصوصية.[1]

### ثالثا: 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 الإليكترونية 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.

### رابعا : 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:

– التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

– التقاط 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".[2]

[1] – جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، مصر، سنة 2000، ، ص 117

[2] - الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الإليكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ص153.

وعلى الرغم من النص غير المباشر على حق الخصوصية إلكترونيا نجد المشرع لم يتجه إلى إصدار قانون بالحماية للخصوصية في المجال الإلكتروني، إلا أن المشرع اكتفي بمواكبة محاربة جريمة المساس بالحق في الخصوصية في العالم الرقمي بموجب القانون رقم 04-15 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 الف إلى 100 الف كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك»

وكذا جرم عمليات تجميع او 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 القانون09- 04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]، وهذا بضمان عدم المساس بالحياة الخاصة للأفراد في حالة قيام السلطات المختصة بالقيام بعمليات المراقبة لكل الاتصالات الاليكترونية بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة.

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

[1] – القانون 09-04 المؤرخ 08/05/ 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جرعدد 47 المؤرخة في08/16/ 2009

الجرائم المعلوماتية لسنة 2007 وتضمن القانون جملة من المواد تتعلق بحماية البيانات الشخصية المعالجة آليا.[1]

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

كما أصدر المشرع البحريني القانون رقم 60 لسنة 2014 في شان جرائم تقنية المعلومات وتضمن القانون تجريم عدة صور للاعتداء على حق الخصوصية وخاصة في إطار اساءة استخدام البيانات الشخصية للأفراد بقصد التشهير والابتزاز.[2]

## المطلب الثاني: مبررات حماية حق الخصوصية الرقمية

مع تزايد التقنيات الحديثة زادت المخاطر على الحق في الحياة الخاصة وأضحى الفرد مقيدا في تعاملاته من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة الوسائل المعلوماتية كتقنيات المراقبة أو التجسس والمساس بالمعطيات الخاصة بالأفراد وهي جميعها تمثل تهديدا مباشرا 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 التي تترك أثرا 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

[1] – عمر ابو الفتوح عبد العظيم، المرجع السابق، ص 179.

[2] – محمد عزت عبد العظيم، المرجع السابق، ص 220

معنون وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها الحماية القانونية للبيانات الشخصية.[1]

**2- الطبيعة الخاصة لقنوات التعامل الإلكتروني**

هذه الطبيعة الافتراضية التي تفتقد 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 المزاروالأمور التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بشرائها، مما يجعله عرضة للقرصنة ثم الاستغلال غير المشروع لها.[2]

**3- فقدان المركزية وآليات السيطرة في قنوات التعامل الإلكتروني**

يكتسب حق الخصوصية في إطار العالم الرقمي نوعا من التميز إذ أن إقرار قانون فاعل يكرس من وجود استراتيجية ملائمة لحماية حق الأفراد بعيدا عن العالم الرقمي قد يكون نوعا 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، وهوما يوسع من دائرة اختراق حق الأفراد ويصعب من الحماية ضد أي انتهاكات لخصوصياتهم.[3]

[1] – جميل عبد الباقي الصغير، مرجع سابق ، ص 40

[2] – عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الانترنت ( الأحكام الموضوعية والجوانب الاجرائية)، دار النهضة العربية مصر، سنة 2004، ص398

[3] – أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، مصر، سنة 2000، ص 359

# الفصل الثاني : آليات حماية  خصوصية الرقمية

## الفصل الثاني : آليات حماية خصوصية الرقمية

مع التقدم العلمي والتكنولوجي المعاصر برزت أساليب إجرامية بتقنيات حديثة أثرت بشكل كبير على مسألة حماية الحقوق والحريات عبر العالم الرقمي، وزاد الاهتمام بالحق في حرمة الحياة الخاصة في ظل التطور المستمر لتكنولوجيا المعلومات، حيث مكنت تلك التكنولوجيا من انتهاك خصوصية الأفراد والاطلاع على أسرارهم واستغلالها بشكل غير قانوني، مما ألزم التدخل التشريعي على المستوى الدولي والداخلي للحد من هذه الاعتداءات.

وبناء عليه سنتناول في هذا الفصل أشكال الاعتداء الإلكتروني على الحق في الخصوصية في المبحث الأول ، و آليات الحماية في المبحث الثاني

## المبحث الأول: أشكال الاعتداء الإلكتروني على الحق في الخصوصية

لما شقت التكنولوجيا طريقها إلى حياة الأفراد، أضحت الإعتداءات المرتكبة إلكترونيا تتسم بالحداثة 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 الإقليمية والوطنية لإيجاد مبادئ وقواعد من شانها 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 الإطلاع 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 واحترامها.[1]

– 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 تفادي أي احتمال لاستغلال تلك المعلومات المكشوف عنها إراديا ليتم استغلالها في أغراض تهدد حرمة الفرد وانتهاك لحرمة حياته الشخصية.[2]

[1] – هشام محمد فريد رستم، المرجع السابق، 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 المعلومات[1] كآلية لجمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد والتي خلقت آثارا إيجابية عريضة في مجال تنظيم تعاملات الافراد 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. ومكمن المخاوف يبرز في أن الوضع الحديث التقنية المعلومات أضحى يمس بجوانب حياة الأفراد الشخصية بتخزينها التلطك 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 وسريتها.[3]

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.

---

[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 الطفي، الحماية القانونية لبرامج الحاسب الآلي ، دار الثقافة للطباعة والنشر، 1987، ص 60

[2] – اسامة 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 Faugére et Patrice FLICHHY : Administration électronique et protection des données personnelles livre Blanc, rapport au ministre de la fonction public et de la réforme de bEtat, Paris, la documentation française, 2002,P 77

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 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 الشخصية[1] .

**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 بيئته[2].

ومن الناحية البنيوية، فإن النظام يتكون من مجموعة من المكونات المترابطة بحيث يمكنها التفاعل فيما بينها. كل مكون هو نظام آخر قائم بذاته[3].

وانطلاقا من التعريف التقني أمكن لرجال القانون اعتماد التعريف القانوني للنظام المعلوماتي، حيث جاء في المادة الأولى من اتفاقية بودابست حول الجريمة السيبيرانية: "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 ب: "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 معين[5].

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

---

[1] –توبي مندل وآخرون: المرجع السابق، ص19.

[2] –Jerome H. Saltzer& M. FransKaashoek**: Principles of Computer System Design**. Morgan Kaufmann Publishers - Elsevier-.USA.2009. p6

[3] – FernardLone Sang. **Protection des systemes informatiques contre les attaques par entrees-sorties**. Doctorat de l'Uinivercite de Toulouse. Directeurs de these : Yves Deswarte et Vincent Nicomette. 2012.p06

[4] – **Convention On Cybercrime**. Budapest, 23.XI.2001. Article 1

[5] –المادة الأولى من القانون رقم 10-05 المؤرخ في 01 نوفمبر 3110 حول المساس بأنظمة المعالجة الآلية. الجريدة الرسمية للجمهورية الجزائرية، العدد 20. السنة الواحدة والأربعون.

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 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 فيها البيانات الشخصية وتعالج وتخزن ويتم تبادلها .يمكن لها اليوم أن تحتوي صور الأشخاص ومذكراتهم. كما تعتبر أهم وسيلة لإجراء الاتصالات الشخصية، والمحادثات السرية، والتقاط الصور الخاصة... وبظهور 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 تتيحهما تكنولوجيات الاعلام والاتصال. أهمها: البريد الالكتروني والسكايب.

أما البريد الالكتروني فهو عبارة عن رسالة يتم إرسالها من نظام معلوماتي(حاسوب شخصي، هاتف دكي...) 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 الصحيح.[1]

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 تحققه عبر وسائل الاتصالات وشبكة الانترنت، باعتبار وجود طرف ثالث يمكن من خلاله التعقب والاطلاع على المعلومات التي

[1] http://www.halifaxpubliclibraries.ca/assets/files/handouts/Email.pdf

يرغب أصحابها في 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 وبتحميله والتعليق عليه وتعديله[1]. 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، وبتحديثه (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 وجنسيتهم 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 فيسبوك[2].

**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 الطبية[3].وفي هذا الخصوص قضت محكمة الدرجة الأولى في باريس بتاريخ 2013/11/6 بإلزام غوغل، بالاستناد إلى الحق في حرمة الحياة الخاصة، بوقف عرض صور تكشف الحياة الجنسية لأحد الأشخاص[4].

---

[1] – وسيم شفيق الحجار: المرجع السابق، ص15.

[2] المرجع نفسه، ص49.

[3] توبي مندل وآخرون: المرجع السابق ،ص32

[4] –وسيم شفيق الحجار: المرجع السابق، ص 32-43.

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 دائما 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 | الاشعاربغرض التجميع | الاشعارعن 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 الالكترونية[1]

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 PRISM [2]الذي يستهدف جميع بيانات مستخدميخدمات الانترنت لشركات [3] PalTalk,AOL,Yahoo, Microsoft, Appele, Google في جميع أنحاء العالم

**خامسا: الحوسبة السحابية**

[1] :Winnie Chung and John Paynterالمرجع السابق

[2] – كشف عنه إدوارد سنودن، فني سابق بوكالة الاستخبارات الأمريكية لصحيفة الجارديان في يونيو 2013.

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

[3] –المرجع نفسه.

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 للأف راد 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 wordوspreadsheet على الانترنت وتشتمل بعض الخدمات الأخرى على منصات تعاونية تسمح للمستخدمين بحرية الوصول إلى المستندات بشكل فوري مثل منصات wiki ومستندات 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 المستخدمين.[1]

## 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 ابتداءا من المعالجة غير المشروعة للبيانات أو عملية الإفشاء 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 البيانات هي أبرز صور انتهاك لتلك السرية من خلال مخالفة القائمين على

[1] –كريم عاطف المرجع السابق.

عملية المعالجة للشروط والأساليب القانونية المنصوص عليها داخليا كعدم منح الترخيص[1] 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 الإلكترونية.[2]

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 لذلك.[3]

**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 أوعمال 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 الضريبي.[4]

**الفرع الثاني: التجسس الإلكتروني**

---

[1] – محمد عزت عبد العظيم، مرجع سابق، ص 92

[2] – Jean–Jacques Hyest: la fraude informatique vue par le nouveau code pénale, exertises des systèmes de linformation Fvrier.1992.N 147.

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

[4] – هشام محمد فريد رستم، المرجع السابق، ص 195.

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 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 التقاط 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 التقنية.[1]

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 أودوائر 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 المستصعبة والتي لا يمكن تداولها بشكل حرويسير.[2]

ولقد اختلفت الوسائل المتبعة في إطار التجسس الإلكتروني وهذا تبعا لاختلاف ثقافة مستخدمي هذه الوسائل ومن أبرزها اتباع تقنية اعتراض الاتصال الشبكي التي تقوم على الاعتماد على برامج لتنفيذها ، فيتم التخل من قبل أحد الأشخاص الخارج عن الاتصالات

[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.

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 الاتصال.[1]

### 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»[2]

كما ربط البعض الآخر فكرة الاختراق بالمعالجة غير المشروعة للبيانات فعرفه بأنه الولوج غير المصرح به قانونا إلى نظام معالجة البيانات باستخدام الحاسوب.[3]

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 معادية.[4]

### 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

---

[1] – محمد عزت عبد العظيم، المرجع السابق، ص 101.

[2]–عمر محمد أبو بكر بن يونس، مرجع سابق، ص 331

[3] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، سنة 2004، ص 242 .

[4] – محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، مصر، سنة 1994، ص 56.

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 حديثة.[1]

[1] – عمر محمد أبو بكر يونس، المرجع السابق، ص 339

## المبحث الثاني: آليات الحماية للخصوصية الرقمية في التشريع الجزائري

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

### المطلب الأول: الحماية الموضوعية للحق في الخصوصية الرقمية في القانون الجزائري

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. وتحديدا الخصوصية عبر الأنظمة المعلوماتية، والخصوصية عبر وسائل الاتصال والمراسلات، ومواقع التواصل الاجتماعي .

#### الفرع الأول: الحماية الموضوعية لخصوصية الأنظمة المعلوماتية

عبر المشرع الجزائري عن الأنظمة المعلوماتية ب"منظومة للمعالجة الآلية للمعطيات". وعبر عن البيانات الرقمية ب" المعطيات"، كما التفت إلى الحماية الجنائية للبيانات بصفة عامة، دون تحديد للبيانات الشخصية، أو إفرادها بنصوص خاصة. حيث جرم جملة من الأفعال الموصوفة في المواد من 394مكرر إلى 394 مكرر7 من قانون العقوبات[1]، 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 394مكررمن قانون العقوبات [2]على أنه: "يعاقب بالحبس من ثلاثة أشهر إلى سنة، وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ."

[1] – القانون رقم 04-15، المرجع السابق.

[2] – المرجع نفسه.

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

**1. الولوج غير المصرح به إلى نظام معلوماتي**

يمكن تعريف الولوج غير المصرح به إلى نظام معلوماتي بأنه أي نشاط يقوم به الشخص عمدا، وبدون رضى صاحب النظام، يجعله في حالة تسمح له بالاتصال الحسي مع النظام أو بالتحكم في نظام التشغيل ولو جزئيا. يمكن أن يكون فعل الولوج غير المصرح به بسيطا 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 مؤمنا بالأدوات اللازمة على غرار كلمة السر والجدران النارية وغيرها من أنظمة الحماية ضد البرمجيات الخبيثة التي تستعمل في التجسس والتحكم في عمل النظام، فضلا عن اقتحامه.

وفي اشتراط كون النظام المعلوماتي مؤمنا حتى يتمتع بالحماية ينقسم الفقه إلى رأيين[1] :الرأي الأوليرى 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 جانب آخر من الفقه ضرورة وجود نظام أمان، استنادا إلى أن المنطق والعدالة يستلزمان ذلك. فالقانون الجنائي –بحسب هؤلاء– لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم والمتطلب من انسان 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

---

[1] – دلخار صالح بوتاني: **الحماية الجنائية الموضوعية للمعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1، 2015، ص200.

عبد العال الديربي، محمد صادق إسماعيل: **الجرائم الالكترونية**، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012، ص189.

المشرع جرم فعل البقاء داخل النظام، وهو ما يتصور حدوثه في حالة الولوج بطريق الخطأ، أي دون أدنى صعوبة، ثم التمادي بالبقاء بعد التفطن لذلك. فكون النظام غير مؤمن بكلمة المرور مثلا يجعل من الولوج إليه أمرا غاية في البساطة، لكن في حال حدوث ذلك خطأ، فإن الفاعل مسؤول جنائيا عن البقاء غير المصرح به .

**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 النظام[1]. ويتصور وقوع هذا الفعل في إحدى حالتين[2]:

**الحالة الأولى:** تتحقق إذا تم الدخول إلى النظام عن غير قصد كالخطأ أو السهو، أي بدون قصد جنائي، ولكنه وبعد تفطنه للأمر يختار البقاء في النظام، أي بعد تكون العلم والإرادة اللازمين لتشكل 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 الفيديرالي CFAA[3].

أما بالنسبة للركن المعنوي: فالجريمة تعتبر تامة ومرتبة للجزاء متى توفر القصد العام أي اتجاه إرادة الفاعل نحو إتيان السلوك مع العلم بنتيجة هذا السلوك، وهو التواجد داخل نظام

---

[1] – محمود أحمد طه: **المواجهة التشريعية لجرائم الكمبيوتر والانترنت**، دار الفكر والقانون، المنصورة، ط1، 2017، ص30.

[2] – المرجع نفسه ص31.

مدحت محمد عبد العزيز إبراهيم: **الجرائم المعلوماتية الواقعة ضد النظام المعلوماتي**، دار النهضة العربية، القاهرة، ط1، 2015، ص84

[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، و2001.

معلوماتي دون إذن صاحبه. وبغض النظر عن البواعث والنوايا. فإن الجريمة تعتبر تامة وإن كان الغرض منها هو التعلم والفضول العلمي البحت .

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 ملموس[1]. لكن الجزاء يضاعف في حال احداث ضرر بالحذف أو التغيير[2]. أما الضرر الناتج عن الحيازة أو الافشاء فقد اعتبرها جريمة مستقلة .

**ثانيا: تجريم ادخال 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 يقيده 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 المس ؤول عنه، يكون القصد من إدخالها هو الازعاج أو احداث 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 بالحق 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 الب واعث وحجم الضرر الناتج، ويعاقب عليها

[1] ـ 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 الحاسوبCFAA.

[2] ـ الفقرة الثانية من المادة 394 مكرر نفسها.

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 افشاء 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 افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى 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 افشائها 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 افشائها 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 2006[1] المعدل والمتمم لقانون العقوبات .

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

**أولا: تجريم فض واتلاف الرسائل والمراسلات**

للتوسيع نطاق التحريم ولضمان حماية الحق في الخصوصية جرم المشرع الجنائي بموجب المادة 303 من قانون العقوبات كل من يفضي او يتلف رسائل او مراسلاتها موجهة إلى الخير وذلك بسوء نية الا ومحل جريمة فض واتلاف 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 والموصلات السلكية واللاسلكية أنها " كل اوتسال لا يتعدي وزنا معينا تسمح موصفاته التقنية بالتكفل به في الشبكة البريدية وغالبا ما تأخذ الرسائل الظروف" اتها وبذلك لا تدخل المراسلات الإلكترونية المكتوبة في مضمون الرسائل المحددة طبقا للبندين 15 و16 من المادة 09 من قانون البريد، والمواصلات السلكية واللاسلكية، كونها لا يتم التكفل بها من الشبكة البريدية.[1]

و بالنسبة للمراسلات فلقد عرفتها المادة التاسعة في الفقرة السادسة من قانون البريد والموصلات 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 والموصلات 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 المرسلات بموجب المادة 303 من قانون العقوبات الجزائري تنطبق على المراسلات الإلكترونية المكتوبة.[2]

[1] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 328

[2] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 329.

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 1 إلى سنة1 وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط".[1]

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 الالكتروني والرسائل الالكترونية المرسلة عبر السكايب أو أي تقنية اتصال أخرى. إلا أن السؤال المطروح الذي يمكن طرحه هنا يتعلق بأفعال القرصنة والاقتحام المرتكبة ضد البريد الالكتروني وحساب السكايب الشخصي، ومدى إمكانية اعتبارها من قبيل الفض المنصوص عليه في المادة303

ونشير في هذا المقام إلى أن نص المادة 303، وان كان ينطبق على المراسلات إلكترونية المكتوبة، إلا أنه قاصر على حمايتها من صورة واحدة من صورة التعدي علي سريتها وهي الاختلاس ذلك أن الحماية المقررة في المادة 303 من قانون العقوبات تقتصر على أفعال الفض والإتلاف وأن فض المراسلات بشمل فقط الرسائل داخل الظروف الخاصة بها.[2]

وفي إطار الصور التجريمية التي أوردها المشرع الجزائي لحماية الحق في الخصوصية عبر الأنترنت تجريم الاحتفاظ وإفشاء واستخدام بهانات شخصية في ظل النظام المعلوماتي باعتباره الليبية التي تولد فها البيانات الشخصية وتعالج والخزن ويتم تبادلها كما تعتبر أهم وسيلة لإجراء الاتصالات الشخصية والمحادثات السرية والتقاط الصور الخاصة خاصة بظهور الحكومة الالكترونية اصبح لسهير 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 الذ نصت المادة 303 مكرر 1 من قانون العقوبات بعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع او سمع بان توضع في متناول الجمهور أو الغير، أو استخدام

[1] ـ 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 329

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 احدى الجرائم المنصوص عليها في المادة 303 مكرر من هذا القانون، ويكتمل الركن المادي بإنيان 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 المعلوماتية.[1]

**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 والأليات التكنولوجية المتطورة فضلا على الوسائل التقليدية، ولعل من أهم المكالمات التي تتم عن طريق التواصل بين الأفراد بشكلها الحديث المكالمات التيليفونية 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 الإعتداء 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 أخر كما في حالة قيام الشخص بالتسجيل الصوتي المذكراته أو لأفكاره كما أن المشرع لم يشترط أن تكون المكالمات أو المحادثات الملتقطة أو المسجلة أو المنقولة قد تمت في مكان خاص ".[2]

[1] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 329

[2] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 327

وبالنظر إلى الإمكانات 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 303مكرر[1] من قانون العقوبات على أنه:" يعاقب بالحبس من ستة أشهر6 إلى ثلاث3 سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1. بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو سرية، بغير إذن صاحبها أو رضاه.

2. بالتقاط 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 الالكترونية بأنها "كل ترسال أو إرسال أو استقبال الأصوات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية بما في ذلك وسائل الهاتف الثابت والنقال"[2]

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 ارتباطا 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.

[1] -القانون رقم 06-23، المرجع السابق.

[2] – عمراوي مارية-حجاج مليكة ، مرجع سابق ، ص327

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 الحديث.[1]

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 كانت.[2]

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 يضفي عليها حماية أكثر ورعاية أكبر.[3]

**ثالثا: تجريم الاحتفاظ وإفشاء واستخدام بيانات شخصية**

تنص المادة 303 مكرر 1 [4]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 استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون. "

[1] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 328

[2] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 328

[3] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 328.

[4] – المرجع نفسه

تستهدف الأفعال المجرمة في هذه المادة، التسجيلات (السمعية والسمعية البصرية)، والصور والوثائق، وغيرها من البيانات الشخصية المتحصل عليها جراء احدى 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 المادة303 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 الجزائري والتي أن المشرع الجزائري اقر مسؤولية الاشخاص المعنوية اذا ثبت ضلوعها في نلاحظ من خلالها أن المشرع أطلق لفظ المعطيات دون أن يخص المعطيات الشخصية بعمارة خاصة. لكن هذا لا يمنع من امكانية 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 افشائها أو نشرها أو التصرف فيها بأي شكل.[1]

والملاحظ أن صور النشاط الجرمي الماسة بالحق في الخصوصية عبر الانترانت المنصوص عليها في قانون العقوبات لن يكتمل بناءها القانوني اذا 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

[1] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 329

التحفظ، نظرا لطبيعة هذه التكنولوجيا والاشكالات التي تثيرها. لذلك فإنني وقبل الخوض في موقف المشرع الجزائري اتجاه خصوصية مستخدمي وسائل التواصل الاجتماعي، أجد من المهم بيان الإشكالات المتعلقة بهذه الوسائل.

**أولا: اشكاليات الحماية الموضوعية للحق في الخصوصية عبر وسائل التواصل الاجتماعي**

تختلف وسائل التواصل الاجتماعي عن وسائل الاتصال الأخرى (الهاتف والسكايب والبريد الالكتروني...). 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. عمالقة الانترنت المجانية كفيسبوك وغوغل، تحول البيانات الشخصية لمستخدميها إلى أموال، لاسيما ما تعلق بعاداتهم الاستهلاكية ومحور اهتماماتهم وبنمط حياتهم.

وتشكل القيمة الاجمالية 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 غروب Bosten consulting Group لعام 2012[1].

[1] وسيم شفيق الحجار: المرجع السابق، ص68.

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 تبقيها 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 للمستخدمين .[1] 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 أكبر.[2]

**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 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 والإرهاب[3].

وفي هذا الخصوص، اعتبرت محكمة الدرجة الأولى في باريس في قرارها تاريخ 2013/11/13 أن حق الشخص باحترام حياته الخاصة قد ينحصر امام متطلبات حرية

[1] وسيم شفيق الحجار: مرجع سابق ، ص66.

[2] المرجع نفسه، ص53.

[3]: المرجع نفسه ،ص41.

التعبير عن الرأي، ويتم تقدير ذلك في ضوء مجموعة من الظروف تتعلق بالضحية وبصفتها وبتصرفها السابق وبموضوع النشر وبمحتواه وبشكله وكذلك في ضوء سوء النية ومدى التعرض لكرامة الشخص والمشاركة في نقاش ذات اهتمام عام. وتعمد 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 الانسان على الحق في الخصوصية[1].

**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 المعلومات[2].

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 لتعقيداتها 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 أصلا بها لاعتقادهم أن ما ينشرونه ليس بدي أهمية ولا يشكل خطرا عليهم أو لرغبتهم في نشر صورهم وتعليقاتهم للجمهور ولأكبر عدد من الناس رغبة في التباهي بما يملكونه أو بمواهبهم أو بشكلهم. ويبدو أن أغلبية مستخدمي وسائلالتواصل الاجتماعي لا يحسنون ضبط إعدادات الخصوصية[3].

وبموجب القوانين المتعلقة بحماية البيانات، على شركات وسائل التواصل الاجتماعي أخذ موافقة المستخدمين بخصوص معالجة بياناتهم ومشاركتها مع الغير أو استعمالها في

[1] وسيم شفيق الحجار: مرجع سابق ،ص40..42 بتصرف.

[2] المرجع نفسه ،ص51

[3] وسيم شفيق الحجار: مرجع سابق ، ص ،55، 47. بتصرف.

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 يكبسون 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 كخاصة[1].

لذلك فالمعلومات الشخصية التي يشاركها مع أشخاص آخرين على مواقع التواصل الاجتماعي هي معفية من القيود بموجب القوانين الأوربية 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 بياناته الشخصية. وفي هذا الاتجاه ،قضت المحكمة الأوروبية لحقوق الانسان في قرارها تاريخ 2009/7/23 بأن المعلومات، في حال إيصالها لمعارف الجمهور من قبل الشخص المعني ذاته، فإنها تت وقف عن كونها سرية وتصبح متاحة بحرية[2].

## 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 الشفهية أو المادية المباشرة والحاصلة في

[1] المرجع نفسه ،ص50، 60. بتصرف.

[2] وسيم شفيق الحجار: مرجع سابق ، ص ،70، 72. بتصرف

مجلس واحد. وبالتالي يمكن –بحسب البعض–تطبيق القواعد القانونية ذاتها على هذه الأفعال لا سيما إذا لم يحدد المشرع وسيلة ارتكابها.[1]

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 لتطبقها على ما يحدث عبر وسائل التواصل الاجتماعي. لذلك فإنه يتوجب على المشرع الجزائري (التشريعات الوطنية) أن يبتكر قوانين جديدة للخصوصية على وسائل التواصل الاجتماعي المستجدة[2].

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 2016مع 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 الأمريكية[3].

### 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.

[1] – المرجع نفسه، ص53.

[2] – وسيم شفيق الحجار: مرجع سابق ص45. بتصرف.

[3] – وسيم شفيق الحجار: المرجع السابق ص71. بتصرف.

بالرجوع إلى قانون الإجراءات الجزائية الجزائري، وتحديدا إلى القانون رقم 09-04 المؤرخ في 5 أوت 2009، [1]الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام 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 عليها[2].

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:

ـ 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 تفيد 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.

[1] القانون رقم 09-04 المؤرخ في 5 أوت 2009

[2] ـ المادة 11 من القانون رقم 09-04،المرجع السابق.

- إذا كانت في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

▪ اشتراط إذن مكتوب من السلطة القضائية المختصة بإجراء عمليات مراقبة الاتصالات الالكترونية

▪ تقييد مجال استعمال المعلومات المتحصل عليها حيث تنص المادة التاسعة على أنه: "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 وكدا المعلومات المتصلة بها[1].

▪ تحديد مدة الاحتفاظ بالبيانات المحجوزة بمدة سنة واحدة من تاريخ التسجيل.[2]

## 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 الاستغلال.[3]

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

[1] – المادة 3/10 من القانون رقم 09-04،المرجع السابق.

[2] ـ المادة 11 من المرجع نفسه.

[3] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 330.

مقارنة بالفعل المرتكب، من جهة أخرى نلاحظ أن المشرع الجزائري لم يتبع سياسة التحفيز للإبلاغ عن هذا النوع من الجرائم بالتخفيض والإعفاء، وان 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 الالية للمعطيات نجد أن المشرع عاقب الشخص الطبيعي بعقوبة اصلية تتمثل في ثلاثة اشهر الى سنة حبس و 50.000 دج الى 100.000 دج غرامة– في حالة الدخول أو البقاء – وقد تشدد العقوبة في حالة الحذف أو تغيير المعطيات

حيث تصبح العقوبة من ستة أشهر إلى سنتين حبس، وغرامة من 50.000دج إلى 150.000دج، وفي حالة الإفشاء 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 بالحبس من شهر إلى سنة وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى العقوبتين والملاحظ أن العقوبة غير كافية مقارنة بالفعل خاصة اذا اكتفي القاضي بالغرامة فقط دون تقرير العقوبة السالبة للحرية. من جهة اخرى نلاحظ أن المشرع الجنائي رفع العقوبة بموجب نصي المادة 303 مكرر، و303 مكررا 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 فان 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 و303 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 أنّ المشرع الجزائري أقرّ 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 اشخاص 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 الخصوصية. [1]

[1] – عمراوي مارية–حجاج مليكة ، مرجع سابق ، ص 330.

# الخاتمة

## الخاتمة:

في الختام نصل إلى أن مسألة احترام الحياة الخاصة الرقمية وحماية المعلومات الشخصية، ليست موضوعا جديدا للبحث. إلا أن التقدم التكنولوجي والمعلوماتي أعطى له بعدا جديدا، 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، تكريسا 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.

كما أن فرص التعاون أو التبادل الاقتصادي أو الثقافي مع دول الاتحاد الأوروبي مستقبلا يتطلب الانسجام مع ما تقره و تضعه من معايير لحماية الخصوصية، فعلى المشرع الجزائري أن يستفيد من التجارب التشريعية في مجال حماية البيانات الشخصية، ليرسي نظاما قانونيا متكاملا يسمح بالإدارة والتحكم في البيانات الشخصية بشكل لا يعرضها للاعتداء، ويصون ويحمي حقوق أصحاب هذه البيانات، واقتراح المسارعة بوضع قانون خاص لحماية البيانات الشخصية ينظم عمليات المعالجة الآلية للبيانات الشخصية، يحدد حقوق أصحاب البيانات وكذا الإجراءات الواجب اتباعها من طرف الجهات القائمة بأعمال المعالجة، وتعيين دقيق لهذه الجهات، خاصة عندما يتعلق الأمر بالبيانات الحساسة، مع ضرورة تجريم مختلف أشكال الاعتداء على البيانات الشخصية، سواء تلك التي تلحق بها ضررا أو تهددها بخطر، والتي ترتكب عمدا أو خطأ، مع فرض عقوبات تتناسب وخطورة الأفعال الإجرامية سوء كان مرتكبها شخصا طبيعيا أو معنويا.

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 الأمن التكنولوجيا المعلومات، وتوفير الإمكانيات المادية والبشرية التي تسوغها من امتلاك مهارات ومقومات المواجهة للتطور المتسارع للإجرام المعلوماتي.

كذا أن الإشكالية الحقيقية التي ينبثق عنها مسألة الحماية الجزائية للحق في الخصوصية هو التحدي الأكبر الذي يواجه هذا الحق في التشريع الداخلي خاصة بعد تأسيس قاعدة حمائية عريضة على مستوى المواثيق والاتفاقيات الدولية وهو ما يضع التشريع الجزائري محل رهان مع التحديات المستحدثة لمخاطر التكنولوجيا وعلى رأسها الحق في الخصوصية.

كما أن الحق في الخصوصية في العالم الرقمي يكتسب ميزة عنه في شكله التقليدي مما يلزم التنسيق بين أشكال الحماية التشريعية والتقنية والتنظيمية.

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 التكتم عنها وعدم إعلانها للغير. لذلك فقد حظيت بالكثير من الجهود التشريعية على المستويين الدولي والوطني في سبيل تنظيمها وحمايتها.
- تمثل الأنظمة المعلوماتية البيئة الالكترونية حيث تخلق البيانات وتعالج وتخزن وتتدفق، لذلك فهي تمثل نطاق الحق في الخصوصية بمختلف أنواعها، بدء بالحواسيب الشخصية والهواتف الذكية والشبكات المعلوماتية ووصولا 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 يخص البيانات الشخصية بتشريع خاص يكفل لها الحماية الجنائية رغم كونها تمثل محل وجوهر الحق في الخصوصية الرقمية .

- يقدم القانون رقم 04–15المؤرخ في 10نوفمبر 2004حول 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
  - ادخال معطيات إلى النظام المعلوماتي أو إزالتها أو تعديلها.
  - حيازة أو افشاء أو نشر أو استعمال البيانات الشخصية .
- يقدم القانون رقم 06–23 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 وابرام اتفاقات دولية لتنظيم وخلق الإطار القانوني لحركة البيانات الشخصية المتدفقة عبر الانترنت .

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

وبهذا نخرج بالجملة التالية من التوصيات:

-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 العالم 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 المراجع

**أولا : الكتب**


- احمد فتحي سرور، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، السنة 54، 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،
- أسامة 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، ص 227
- توبي مندل وآخرون: دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير، الأمم المتحدة، منشورات اليونسكو، فرنسا ،2013،
- جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، مصر، سنة 2000،
- حسام الدين الأهوائي، الحق في احترام الحياة الخاصة ( الحق في الخصوصية، دراسة مقارنة، دار النهضة العربية، ط2، 2002،
- حسام الطفي، الحماية القانونية لبرامج الحاسب الآلي ، دار الثقافة للطباعة والنشر، 1987، ص 60
- حمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، مصر، سنة 2000
- خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009
- دلخار صالح بوتاني: الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2015،
- السيد عتيق، جرائم الانترنت، دار النهضة العربية، مصر، 2002،
- عبد العال الديربي، محمد صادق إسماعيل: الجرائم الالكترونية، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012،

- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الجزء الثاني: الحماية الجنائية، دار الفكر العربي، الإسكندرية، 2002 ، ص 56
- 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،
- 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 إلكترونيا، أطروحة دكتوراه، جامعة القاهرة، 2009،
- عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الانترنت ( الأحكام الموضوعية والجوانب الاجرائية)، دار النهضة العربية مصر، سنة 2004،
- فريد هدكيت، الخصوصية في عصر المعلومات، مركز الأهرام للترجمة والنشر، القاهرة، 1999
- كيث دفلين ،الإنسان والمعرفة في عصر المعلومات، ترجمة: شادن اليافي، مكتبة العبيكان، السعودية، ط: 1، 2001م،
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، مصر، سنة 1994،
- محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، سنة 2016، ط1، ،

- محمد هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة مصر، سنة 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، ط1، 2017،
- مدحت محمد عبد العزيز إبراهيم: الجرائم المعلوماتية الواقعة ضد النظام المعلوماتي، دار النهضة العربية، القاهرة، ط1، 2015، ص84
- 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 ،ط1، 205،
- نديم عبده، أمن الكمبيوتر (الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي)، دار الفكر للأبحاث والدراسات، بيروت، ط1، 1991
- نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2008
- هلالي عبد الله احمد، جرائم المعلوماتية العابرة للحدود ( أساليب المواجهة وفقا لاتفاقية بودابست)، دار النهضة العربية ، مصر، ط 1، سنة 2007،

**رسائل ومذكرات التخرج**

- أشراف البكوش، حماية الحياة الخاصة في القانون الجنائي، مذكرة ماجستير ،كلية الحقوق و العلوم الاقتصادية و السياسية بسوسة، 2007 / 2006
- أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، رسالة دكتوراه، جامعة المنصورة،2005/ 2006
- 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 ماجيستر، جامعة الأردن، 1994،

**المقالات و المنشورات العلمية**


- الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الإليكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية،
- الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الإليكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية – أدرار، العدد الثامن، تاريخ ، المجلد الأول، 2017،
- صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، التواصل في الاقتصاد والإدارة والقانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار – المجلد 24 – العدد 02 – أوت 2018
- عمراوي مارية–حجاج مليكة، حماية الحق في الخصوصية عبر الانترنيت 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،
- 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، ط1، بيروت ،2017،
- يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي، اتحاد المصارف العربية ، عمان، الأردن، سنة 2002،


**القوانين و المراسيم**


- القانون رقم 08–09 المتعلق ب حماية 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

- القانون 09-04 المؤرخ 08/05/ 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جرعدد 47 المؤرخة في08/16/ 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 .
- قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006. المعدل والمتمم لقانون العقوبات .الجريدة الرسمية للجمهورية الجزائرية/ العدد 84.
- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 5 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية/ العدد 47.

## المراجع باللغة الأجنبية

- Pierre TRUCHE; Jean-paul Faugére et Patrice FLICHHY : Administration électronique et protection des données personnelles livre Blanc, rapport au ministre de la fonction public et de la réforme de bEtat, Paris, la documentation française, 2002,

–Jerome H. Saltzer& M. FransKaashoek: Principles of Computer System Design. Morgan Kaufmann Publishers - Elsevier-.USA.2009.

– FernardLone Sang. Protection des systemes informatiques contre les attaques par entrees-sorties. Doctorat de l'Uinivercite de Toulouse. Directeurs de these : Yves Deswarte et Vincent Nicomette. 2012

- Jean-Jacques Hyest: la fraude informatique vue par le nouveau code pénale, exertises des systèmes de linformation Fvrier.1992.N 147.

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

Daniel Kaplan, Informatique, libertées, identities, Fyp Edition 1" avril.2010,P10.

## المواقع الالكترونية

http://www.halifaxpubliclibraries.ca/assets/files/handouts/Email.pdf

https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive annotee.pdf

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

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

# فهرس المحتويات