جامعة عبد الرحمان ميرة ـ بجاية ـ

كلية الحقوق والعلوم السياسية

قسم: القانون الخاص

الحماية الجنائية للحياة الخاصة عبر الأنترنت

مذكرة التخرج لنيل شهادة الماستر في الحقوق

قسم: القانون الخاص/ تخصص: القانون الخاص والعلوم الجنائية

إعداد الطالبين:

ـ إتوشن ساسي

ـ سليماني بوبكر

تحت إشراف:

ـ عبد الرحمان خلفي

لجنة المناقشة:

.....رئيسا

عبد الرحمان خلفي أستاذ محاضر.....مشرفا

.....ممتحنا

السنة الجامعية: 2012/ 2013

بسم الله الرحمن الرحيم

"...و ما توفيقي إلا بالله عليه توكلت و إليه أنيب"

(سورة هود الآية 88)

كلمة شكر

نتقدم بجزيل الشكر الأستاذ المشرف:

د/ عبد الرحمن خلفي

على كل توجيهاته ونصائحه القيمة التي كانت عونًا لنا في إنجاز هذه المذكرة خاصة التصويبات العديدة التي قام بها في جميع مراحل إنجازها

- ✓ إتوشن ساسي
- ✓ سليماني بوبكر

إهداء

الى من كرمهما الله في كتابه..

إلى الوالدين العزيزين،أطال الله في عمرهما و أمدّهما بالصّحة

و العافيّة.

إلى إخوتي وأخواتي الذين ساندوني وكانوا خير عون لي أسأل الله

تعالى أن يحفظهم ويسدد خطاهم ويديم شملهم

إلى كل من ساعدني من أساتذتي الكرام،

إلى جانب كل من تحمل معي مشقة إنجاز هذا العمل المتواضع

و إلى كل زملائي وزميلاتي

إلى جميع هؤلاء أهدي ثمرة جهدي هذا.

✓ ساسي

إهداء

الى من كرمهما الله في كتابه..

إلى الوالدين العزيزين،أطال الله في عمرهما و أمدّهما بالصّحة

و العافيّة.

إلى إخوتي وأخواتي الذين ساندوني وكانوا خير عون لي أسأل الله

تعالى أن يحفظهم ويسدد خطاهم ويديم شملهم،

الى خطيبتي صبرينة و عائلتها،

إلى كل من ساعدني من أساتذتي الكرام،

إلى جانب كل من تحمل معي مشقة إنجاز هذا العمل المتواضع

و إلى كل زملائي وزميلاتي

إلى جميع هؤلاء أهدي ثمرة جهدي هذا.

✓ بوبكر

قائمة المختصرات:

أولا: باللّغة العربيّة:

ج،ر: الجريدة الرَسمية.

د،د،ن: دون دار النشر.

د،س،ن: دون سنة النَشر.

د،ط: دون طبعة.

ص: الصَفحة.

ص، ص: من الصّفحة إلى الصّفحة.

ط: الطَبعة.

ق،ع،ج: قانون العقوبات الجزائري.

ق،إ،ج،ج: قانون الإجراءات الجزائية الجزائري.

ثانيا: باللغة الفرنسية:

CRID : Centre de Recherche et d'Informations pour le Développement.

GILC: Global Internet Liberty Campigny.

JORF: Journal Officiel de la République Française.

P : Page.

مقدّمة:

إنّ الفرد بحكم طبيعته الإنسانيّة لا يتماثل مع غيره من الأفراد، فالتّماثل القائم بين الأفراد هو مجرد مظهر خارجي فقط لا يحول دون وجود اختلاف عميق فيما بينهم سواء في طباعهم أو أحاسيسهم أو آرائهم أو أسلوبهم في الحياة، إلى غير ذلك من أوجه الاختلاف بين الأفراد، وينعكس هذا الاختلاف على حياتهم الخاصّة، وتقتضي طبيعة هذه الحياة أن تتسم بأسرار تنبع من ذاتية صاحبها، فمن حق الفرد أن يحتفظ بأسرار حياته بعيدا عن إطّلاع الغير.

وقد شهد العالم خلال النّصف الثّاني من القرن العشرين ثورة هائلة في مجال تقنيّة المعلوماتية، كان من أهم إفرازاتها ظهور الحاسب الآلي الذي غزى كل أوجه النّشاط الإنساني، وأضحى حاجة أساسيّة لكل بيت متطوّر أو مدرسة أو مصنع أو غير ذلك من المرافق والمؤسّسات، وتوّج التطوّر المتلاحق في تقنيّة المعلومات بظهور الانترنت التي خلقت بيئة افتراضية تتدفّق فيها المعلومات والاتّصالات عبر الحدودما يؤدي عادة إلى الاعتداء على حقّ الإنسان في سمعته وشرفه و اعتباره[1].

إلا أنّ هذا الجانب المشرق لتطوّر وانتشار تقنيّة المعلومات والانترنت، صاحبه جانب آخر اتّسم بالأنانيّة والظّلمة، والاعتداء غير المشروع على مصالح وقيم ماديّة ومعنويّة، كانت ومازالت موضع اهتمام القانون الجنائي، فقد أصبح الانتشار الكبير والتطوّر المتلاحق في تقنيّة المعلومات يشكّل خطرا مستمرّا على الحقّ في الحياة الخاصة، ويهدّد بانتهاك حرماتها وتعرية أسرارها.

(1) –سعد حمد صالح القبائلي، الجرائم الماسّة بحق الإنسان في السّمعة والشّرف والاعتبار عبر الانترنت، بحث مقدم إلى المؤتمر المغاربي حول المعلوماتية والقانون، ليبيا، بين 28 و29 أكتوبر 2009.

إنّ ما قدّمته الانترنت من مزايا في مجال النّشر، وما أعطته للخبر من سرعة للانتشار وعدد أكبر من القرّاء ساهم في انتشار جرائم القذف والسب عبر الانترنت، ووسّع من نطاق تعرية حياة الإنسان وتهديد سكينته وطمأنينته، ورافق انتشار استخدام البريد الالكتروني في مجالات الحياة المختلفة، عدم قدرة الانترنت على توفير أمان مطلق أو كامل لسريّة ما ينقل عبرها من بيانات، مما سهّل من نطاق وطرق الاعتداء على سريّة المراسلات، كما أدى شيوع استخدام تقنيّة المعلومات وبشكل خاص الانترنت في أوجه الحياة المختلفة للمجتمع، – لما لها من قدرة فائقة على جمع وحفظ واسترجاع و نقل بيانات خاصة بأفراد المجتمع وتزايد الاتجاه من قبل الحكومات والهيئات والشركات والأفراد نحو نشر وتخزين الملفات والبطاقات الخاصة بهم على حواسيبهم الآلية المتصلة بالأنترنت– إلى استحداث أساليب جديدة للتّعدي على الحياة الخاصّة للأفراد، وهو ما أدّى إلى التّساؤل حول مدى انطباق النصوص التقليدية للحماية الجنائية للحياة الخاصة على الاعتداءات المرتكبة عبر الانترنت ؟

وتنبثق عن هاته الإشكالية جملة من التساؤلات الفرعية تتمحور أساسا حول مدى تحقق ركن العلانية في جرائم القذف والسب عبر الانترنت، ومدى انطباق الأحكام الخاصة بجرائم الاعتداء على سرية المراسلات الالكترونية المكتوبة.

كما تطرح تساؤلات أخرى تتمثل أساسا في: ما هي الاعتداءات المستحدثة بفعل الانترنت على الحياة الخاصة للأفراد؟ وهل تكفي حماية البيانات الخاصة بالأفراد الواردة في التشريعات المقارنة لحماية البيانات الشّخصية من هذه الاعتداءات؟

ودفعنا لاختيار هذا الموضوع مجموعة من الأسباب والدّوافع ويمكن إيجازها فما يلي:

1 – الانتشار الهائل لاستخدام الانترنت في مجالات الحياة المختلفة، كالبحث العلمي، الاتّصالات، الإعلام، التّجارة، الاستهلاك والخدمات الاتّصالية وغيرها من أوجه نشاطات الحياة المختلفة .

2 – قصور غالبية التشريعات العربية في التعرّض لموضوع الحماية الجنائية للحياة الشخصية عبر الانترنت، وهو ما يقتضي مواكبة التطوّرات التّشريعية الحديثة في القانون المقارن، ذلك أنه مع الاستفادة من تطور تقنيّة المعلومات يجب المحافظة على حقوق الأفراد وحريّاتهم، فالفائدة موجودة والضرر مصاحب وحتى لا نتخلف عن العالم المتقدم لا بدّ أن نواجه المشكلة ونستفيد مما يصاحبها من فائدة .

وتكتسي دراسة موضوع الحماية الجنائية للحياة الشّخصية عبر الانترنت جانبا كبيرا من الأهميّة، يتمثل في القيمة المزدوجة لموضوع حماية الحياة الشخصية في مجال الانترنت وما أثاره انتشار استخدامها من إشكاليّات قانونية.

كما أن دراسة موضوع الحماية الجنائية للحياة الشّخصية عبر الانترنت، يأتي منسجما مع المنطق الذي يصف النشاط الإجرامي وصفا قانونيا دقيقا يتلاءم والنصوص الحاضرة في التشريع الجنائي، ولا يحيد في الوقت ذاته عن مبادئه الّراسخة حيث لا جريمة ولا عقوبة إلا بقانون ولا قياس لغايات التّجريم، خاصة وأن التّشريعات المقارنة لا تتضمن نصوصا صريحة مستقلّة، تنظم موضوع الحماية الجنائية للحياة الشّخصية عبر الانترنت.

ونظرا لطبيعة الموضوع فقد اعتمدنا في هذه الدّراسة على المنهج الإستقرائي، لأنه المناسب للتحليل.

وللإجابة على الإشكالية الرئيسية للموضوع، مع ما ينبثق من تساؤلات فرعية، قمنا بتقسيم الدراسة إلى مقدمة وفصلين وخاتمة.

سنتطرّق في الفصل الأول إلى دراسة مفهوم الحق في الحياة الشّخصية في مجال الانترنت من خلال مبحثين: ندرس في المبحث الأول المخاطر الحديثة للحق في الحياة الشّخصية فنبيّن في هذا المبحث الحق في الشّرف والاعتبار والصّورة، والحق في سريّة المراسلات والبيانات الشّخصية في مجال الانترنت، وفي المبحث الثاني ندرس عناصر المسؤوليّة الإلكترونية وذلك ببيان المقصود بالضرر الإلكتروني، طبيعته، تطبيقاته، وتبيان علاقة السّببية في المسؤولية الإلكترونية، ونذكر التعويض عن الضّرر الإلكتروني.

أمّا الفصل الثاني والأخير فنخصّصه لوسائل حماية الحياة الشّخصية في مجال الانترنت في مبحثين: نتناول في المبحث الأوّل النّظام القانوني لحماية البيانات الشّخصية في مجال الانترنت، فنحاول تبيان مبادئ حماية البيانات الشخصية من مخاطر الانترنت في بعض الدول الغربيّة، وكذا على صعيد بعض الدول العربيّة بالإضافة إلى التحدّيات القانونية لضبط أدلة جرائم الاعتداء على الحياة الشّخصية عن طريق تفتيش شبكة الانترنت بالإشارة إلى المشكلات المتعلقة بسلطات الاستدلال والتحقيق، أما في المبحث الثاني فنتطرق فيه إلى الوسائل التقنيّة والتنظيميّة لحماية الحياة الشخصية من مخاطر الانترنت.

الفصل الأول

مفهوم الحق في الحياة الشّخصيّة عبر الانترنيت

إنّ الدّراسات القانونية التي عنيت بالخصوصية وبحقوق الإنسان في ضوء التطورات التقنيّة محدودة بشكل عام، ويمكن القول أن نهاية الستّينات وبداية السّبعينات شهدت انطلاق مثل هذه الدّراسات، وأنّ هذه الفترة تحديدا هي التي أثير فيها لأول مرّة وبشكل متزايد مفهوم خصوصيّة المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية [1].

وعصر المعلوماتيّة الذي نعيشه الآن يتيح المجال لكل شخص يعيش على أرض المعمورة الحق في الاتّصال بغيره وتبادل المعلومات معه كحقّ من حقوق الإنسان وحريّاته الأساسية وبالتّالي فإن شبكة الانترنيت أظهرت من الحقوق القدر الكثير فلا حدود ولا قيود قانونية، بعبارة أخرى ليس لها شخصيّة قانونية معنويّة فهي عبارة عن اتحاد فيدرالي للشّبكات في مجموعها تغطي تقريبا كل دول العالم وعليه فالمخاطر المنبعثة كثيرة ومتشعبة[2] خاصة فيما يتعلق بالحياة الشخصيّة للأفراد وذلك لسهولة التعرض لحياتهم الخاصة وسرعة انتقال المعلومات المتعلّقة بهم.

وهذا ما سندرسه في هذا الفصل والذي قسّمناه إلى مبحثين تناولنا في الأول المخاطر الحديثة التي تمسّ بالحياة الشخصيّة، أما في الثاني فقد تناولنا عناصر المسؤولية الإلكترونية فبيّننا الضرر الإلكتروني والعلاقة السببيّة فيها.

المبحث الأول

المخاطر الحديثة للحق في الحياة الشخصيّة

حظيت الحياة الشّخصيّة للأفراد بحماية دستوريّة وقانونيّة في مختلف تشريعات الدّول المتقدّمة لما لخصوصيّة الأفراد من أهميّة قصوى على كيان الفرد والمجتمع معا، والحق في الحياة الشّخصيّة هو أحد الحقوق اللّصيقة التي تثبت للإنسان، والتي غالبا ما يصعب حصر

---

[1]– بوليون أنطونيس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، لبنان، 2009، ص– ص 56–57.

[2]–علي أحمد عبد الزغبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، ط1، المؤسسة الحديثة للكتاب، لبنان، 2006، ص–ص 323– 324.

الجوانب المختلفة لها والتّمييز بحدود واضحة بين ما يعد من الحياة الشّخصيّة للأفراد وما يعد من الحياة العامّة لهم.

ولمّا كانت الحياة الشّخصيّة للأفراد بصورتها المستحدثة والمتمثّلة في بنوك المعلومات المرتبطة بالتّكنولوجيا مهدّدة بالعديد من الانتهاكات والاعتداءات ولاسيما بظهور شبكة الانترنيت والطّريقة السريعة لانتقال المعلومات عبرها وبذلك سهولة المساس بالحياة الشّخصية للأفراد عن طريق النّشر وهذا ما يمس بحرمة الحياة الشّخصية وهذا ما سنتعرّض له في هذا المبحث من خلال مطلبه الأول بعنوان "حرمة الشّرف والاعتبار والصّورة، وفي المطلب الثّاني حق الشخص في حماية سرّيّة المراسلات الالكترونية.

المطلب الأول

حرمة الشّرف والاعتبار والصّورة

إن الحق في حرمة الحياة الشّخصية هي إحدى حقوق الإنسان الرّئيسية التي تتعلّق بكرامته وبقيم مادية ومعنوية أخرى، وقد أصبح الحقّ في حرمة الحياة الشّخصية واحدا من أهم حقوق الإنسان في العصر الحديث، وجرى الاعتراف به ضمن أنظمة غالبية الدول وحتّى في الدّول التي لم تتضمن دساتيرها أو قوانينها اعترافا بهذا الحق، فإن المحاكم فيها قد أقرّت هذا الحق استناد إلى الاتّفاقيات الدّولية التي اعترفت به حينما تكون الدولة عضوا فيها[1].

الفرع الأول

الحق في الشرف والاعتبار

للشّخص الحق في الشّرف، الذي يكفل له احترام سمعته وشرفه وكرامته واعتباره من التعدي والإيذاء، ويقصد بالشّرف والاعتبار مجموع القيّم التي يضفيها الشّخص على نفسه وسمعته التي تستتبع تقدير النّاس له.

وتتعدد أوجه نواحي الشّرف والاعتبار من الجانب الشّخصي الذي يعكس كرامة الإنسان الى الجانب الاجتماعي الذي يتكون من تقدير الجمهور للمواطن في مجال نشاطه السياسي أو المهني أو الفني أو العلمي.

---

(1) – بوليون أنطونيوس أيوب، المرجع السابق، ص219 .

ويتمثل الإخلال بالشّرف الحط من مكانة الإنسان وتعريضه لاحتقار النّاس وازدرائهم عن طريق الأقوال والتّشهير أو نسب أفعال معيّنة له، ولا شك أن هذه تتسم بالنّسبية حيث تختلف حسب الظروف والأشخاص، والمحاكم هي التي تقدّر في النّهاية ما اذا كان هناك عدوان على الشّرف من عدمه، وينبغي ألّا يتسم التقدير بالجانب الشّخصي المحض، بل يجب الارتكاز على معيار موضوعي قائم على النّظر إلى شخص مماثل للمضرور[1].

ومن صور التعدي على الشّرف والاعتبار نجد:

أوّلا: القذف

لقد نصّ كل من المشرعين المصري والجزائري على جريمة القذف ضمن أحكام قانون العقوبات خلافا للمشرّع الفرنسي الذي نصّ على جريمة القذف ضمن أحكام قانون الإعلام.

تنصّ المادّة 302 ق ع المصري "يعدّ قذفا كل من أسند لغيره بواسطة إحدى الطرق المبيّنة بالمادّة 171 من هذا القانون، أمورا لو كانت صادقة لا أوجبت عقاب من أسندت إليه بالعقوبات المقرّرة قانونا أو أوجبت احتقاره من أهل وطنه" وعرّف المشرع الجزائري القذف في المادة 296 من قانون العقوبات بأنه "كل إدّعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به و إسنادها إليهم وإلى تلك الهيئة، ويعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو عن طريق إعادة النشر حتى لو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم، ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصّراخ أو التّهديد أو الكتابة أو المنشورات أو الإعلانات موضوع الجريمة".

فيما نصّت المادّة 144 مكرّر و146 على أن القذف الموجّه إلى رئيس الجمهوريّة والهيئات العمومية قد يكون بأية آلية تبث الصوت أو الصورة أو بأي وسيلة إلكترونيّة أو معلوماتيّة أو إعلاميّة أخرى.

فالادّعاء يحمل معنى الرّواية عن الغير، أو ذكر الخبر محتملا الصّدق أو الكذب، بينما الإسناد يفيد نسبة الأمر إلى شخص المقذوف على سبيل التّأكيد سواء أكانت الوقائع المدّعى بها صحيحة أو كاذبة وعلى ذلك فإن الإدّعاء أو الإسناد في القذف يتحقّق بكل صفة كلامية أو كتابيّة توكيديّة وبكل صفة ولو تشكيكيّة من شأنها أن تلقي في أذهان الناس

[1]– محمد حسين منصور، المسؤولية الإلكترونية، د، ط، دار الجامعة الجديدة، مصر 2003، ص 362.

عقيدة ولو وقتيّة أو ظنّا أو احتمالا ولو وقتيّين في صحة الأمور المدّعاة ويجب أن ينصبّ الادّعاء أو الإسناد على واقعة معيّنة ومحدّدة من شأنها المساس بالشّرف والاعتبار وهي حالة موضوعيّة يرجع تقديرها إلى قاضي الموضوع[1].

ولا يشترط القانون الجزائري أن تكون الواقعة المسندة صحيحة، فالقانون يعاقب على مجرد الإسناد سواء أكانت الوقائع صحيحة أو كاذبة وهذا ما يميّز التشريع الجزائري عن التشريعين المصري والفرنسي اللذان يشترطان –عدا حالات خاصة– عدم صحة الوقائع المسندة[2]، وكذلك لابد من تعيين الشخص أو الهيئة المقذوفة، إذ يجب أن يكون المقذوف معيّنا وليس من الضّروري أن يكون معينا بالاسم، وانما يكفي لقيام القذف أن تكون عبارة موجّهة على صورة يمكن معها فهم المقصود منها ومعرفة الشخص الذي يعنيه القاذف وهذه مسألة وقائع تفصل فيها محكمة الموضوع.

ولا يعاقب القانون على القذف إلّا إذا تمّ إدّعاء أو إسناد الواقعة المتضمّنة له في صورة علنيّة إذ يتحقّق حينئذ التّشهير بالمجني عليه ثم ذيوعه مما يستتبع الهبوط بمكانته الاجتماعيّة وهو علّة تجريم القذف.

كما يعدّ ركن العلانيّة الركن المميّز لجنحة القذف، فإذا غاب هذا الركن أصبحت الجريمة مجرد مخالفة ويعاقب عليها قانون العقوبات الجزائري في الفقرة الثانية من المادة 463 بعنوان السّب غير العلني، وهكذا فقيام جنحة القذف يتطلّب توفر العلانية إما بالقبول أو الفعل أو الكتابة أو الصّورة.

ثانيّا: السّب

عرّف المشرّع المصري السّب في المادّة 306 من قانون العقوبات على أن كل سب لا يشتمل على إسناد واقعة معيّنة، بل تتضمن بأي وجه من الأوجه خدشا للشرف أو الاعتبار، يعاقب عليه في الأحوال المبيّنة في المادة 171 بالحبس مدة لا تتجاوز سنة وبغرامة لا تقل عن ألف جنيه ولا تزيد على خمسة ألاف جنيه أو بإحدى هاتين العقوبتين".

---

[1]– أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، ج1، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2008، ص، ص،198،195 .

[2]– المرجع نفسه، ص، 198.

وعرّفه المشرع الجزائري في المادة 297 بأنه "كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة".

يستخلص من المادة 297 من قانون العقوبات الجزائري أن جريمة السّب تقوم على ثلاثة أركان وهي: التعبير المشين أو البذيء، العلانية والقصد الجنائي.

يقوم السّب أساسا على التعبير، ويشترط فيه أن يكون مشينا أو يتضمن تحقيرا أو قدحا، فهو على خلاف القذف لا يشترط فيه إسناد واقعة معيّنة للشّخص، كما لا يشترط أن تكون العبارات المستعملة تنطوي على عنف أو أن يكون الكلام ماجنا أو بذيئا، فالسب يتوافر بكل ما يمس بقيمة الإنسان عند نفسه أو يحط من كرامته أو شخصيته عند غيره.

ويتعين على المحكمة أن تذكر في حكمها ألفاظ السّب وإلا كان حكمها باطلا لقصور الأسباب ويجب أن يوجّه السّب إلى شخص أو أشخاص معيّنين سواء إلى أشخاص طبيعيّين أو معنويّين، وتبعا لذلك، لا تقوم الجريمة إذا كانت ألفاظ السب عامة أو موجهة إلى أشخاص خياليّين ولا عبرة بالوسيلة أو الأسلوب الذي تصاغ به عبارات السب فهو يتحقق بكل صيغة توكيدية أو تشكيكيّة صريحة أو ضمنية[1].

أما بالنسبة لركن العلانية، فمثلما هو الحال في القذف تشترط جنحة السب العلانية، وهي نفس العلانية التي يقتضيها القذف، وتتحقق بالقول أو الكتابة أو الفعل أو الصّورة، وإذا كان المشرّع الجزائري لم يشر صراحة إلى العلانيّة في نص المادة 297 من قانون العقوبات خلافا لما هو عليه الحال في القانون الفرنسي والمصري الذي اشترط هذا العنصر في الجنحة، فإنّ ما نصّت عليه المادة 463 من ق ع ج ومؤداها أن كل من ابتدر أحد الأشخاص بألفاظ سباب غير علنيّة دون أن يكون قد استفزّه يعاقب بغرامة من 30 إلى 100 دج ويجوز أن يعاقب أيضا بالحبس لمدة ثلاثة أيام على الاكثر"، يدل على أن عدم الإشارة إلى العلانيّة مجرد سهو وبالتالي انعدام العلنيّة يحول الجريمة من جنحة السّب الى مخالفة السّب غير العلني المعاقب عليها بموجب الفقرة الثانية من المادة 463 من ق ع ج، وبالنّسبة للقصد الجنائي، يشترط في جريمة السّب القصد الجنائي العام، ويتوفّر لمجرد الجهر بالحكم بالألفاظ المشينة مع العلم بمعناها.

[1]– أحسن بوسقيعة، المرجع السابق، ص، 198.

ثالثا: صور القذف والسّب عبر الانترنيت

تتنوع صور القذف والسّب عبر الانترنيت بتنوع الغرض من استخدام الانترنيت والطّريقة التي يستخدم لها، وفي كل الحالات ترتكب هذه الصّور عبر الانترنيت من خلال المبادلات الإلكترونيّة والتي قد تكون بين طرفي انترنيت متصلة بين الحواسيب الآلية[1]، متمثّلة أوّلا في البريد الإلكتروني الذي هو من أقدم التطبيقات في شبكة الانترنيت وأكثرها انتشارا حيث أصبح يشكل وسيلة اتصال لا غنى عنها في الكثير من مجالات العمل، وقد كانت بداية الانترنيت تهدف إلى تقديم خدمات البريد الإلكتروني للباحثين في مراكز البحث العلمي، ثم أصبح اليوم وسيلة للمراسلة بين مستخدمي الانترنيت كافة، ويمكن تعريفه بأنه رسالة يتم إرسالها من حاسب آلي لآخر عبر شبكة الانترنيت وإلى أيّ مستخدم في أيّ مكان، ففي نظام البريد الإلكتروني صندوق خاص لكل مشترك والذي يعرف بواسطة عنوانه الإلكتروني، وفي واقع الأمر فإن صندوق البريد الإلكتروني ما هو إلاّ ساحة مخصّصة ضمن وحدة التّخزين في أحد الحواسب المزوّدة بشبكة الانترنيت لصاحب هذا الصّندوق تحمل عنوانه وتحفظ فيها الرّسائل الإلكترونية الواردة لهذا المشترك.

ويستطيع الجاني من خلال البريد الإلكتروني أن يخدش شرف واعتبار أيّ شخص، سوا من خلال إسناد أو إدّعاء واقعة محدّدة تستوجب عقاب أو احتقار من أسندت إليه أو من دون أن يتضمن ذلك أي إسناد لأيّ واقعة.

وبما أنّ الكتابة تشكّل الاستخدام الأكثر للانترنيت، فإن القذف والسّب الخطّي يشكلان الصّورة الغالبة لمثل هذا النوع من الجرائم.

ويقع القذف والسّب عبر البريد الإلكتروني لمّا يوزّع على المتعاملين مع الانترنيت الكتابات أو الرّسوم أو الصّور الاستهزائيّة أو مسودّات الرّسوم أو الرّسائل الصّوتية بحيث يتسلّمها عدد غير محدود من الناس[2].

كما تنطوي ضمن المبادلات الإلكترونية التي يكون بين طرفي انترنيت متصلة، الويب العالمية والتي تعتبر من بين الأنظمة المعلوماتيّة الأكثر تطوّرا على الانترنيت وهي

---

[1]– محمد أمين أحمد الشوابكة، جرائم الحاسوب و الانترنت و الجريمة المعلوماتية، ط1 دار الثقافة للنشر و التوزيع، الأردن، 2009.

[2]– المرجع نفسه، ص 34.

نظام فرعي من الانترنيت، لكنها النّظام الأكبر من الأنظمة الأخرى، فهي النّظام الشامل باستخدام الوسائل المتعدّدة كونها تدمج أغلب الخدمات المتوفّرة على الانترنيت.

ويمكن تعريفها بأنّها عبارة عن كمّ هائل من المستندات المحفوظة في شبكات الحاسب الآلي والتي تتيح لأيّ شخص أو أيّ جهة الاطلاع على معلومات تخصّ جهات أخرى أو أشخاص آخرين قاموا بوضع هذه الخدمة حيث تقدم خدمة معلومات واسعة النطاق.

ولكل مستخدم على شبكة الانترنيت أن ينشئ موقعا له على شبكة المعلومات العالمية، يتضمن معلومات يمكن إعادة تخزينها والتي يمكن لأي مستخدم في جميع أنحاء العالم استقبال هذه المعلومات من خلال نظم الاستقبال.

يرتكب القذف والسّب على شبكة الويب العالمية من خلال أيّة مادة كتابيّة، أوسمعيّة، أو سمعيّة بصريّة تسيء إلى شرف واعتبار الأشخاص، سواء من خلال إسناد أو ادعاء واقعة محدّدة تستوجب احتقار من أسندت إليه، وهو غالبا ما يتخذ صور القذف أو السّب الخطّي حيث يتم على صفحات الويب نشر وإذاعة الكتابات أو الرّسوم أو الصّور الاستهزائية والمكاتب المفتوحة وبطاقات البريد التي تسيء للمعتدى عليه.

كما يمكن ارتكاب أفعال سب وقذف عبر شبكة "مجموعات الأخبار"[1] متى كان كل من الجاني والمجني عليه يتبادلان الرّسائل عبر مجموعات الأخبار، أو في صدد تعليقاتهم أو مشاركتهم على موضوع معين، كما يمكن القيام بأفعال قذف وسب من خلال ما ينشر بين الناس عبر حلقات النقاش هذه، أو كما يوزع على فئة منهم على شكل كتابات أو صور استهزائيّة.

[1] – تعد مجموعات الأخبار أشكال من المناقشة عبر إنترنت حيث يجتمع مجموعة من الناس لديهم اهتمامات مشتركة للحديث عن كل شيء بداية من البرامج إلى القصص الكوميدية والشئون السياسية. على خلاف رسائل البريد-الإلكتروني، التي تكون ظاهرة فقط للمرسل والمستلمين الذين تم تحديدهم، يمكن قراءة رسائل مجموعة الأخبار بواسطة أي شخص يقوم بعرض المجموعة التي يتم نشر هذه الرسائل فيها. تكون مجموعة الأخبار دولية النطاق، ويستخدمها شركاء من كافة نواحي العالم.

كما يمكن أن تتدرج ضمن صور القذف والسب عبر الانترنيت التي تكون بين طرفي انترنيت متصلة التي تكون عبر غرف المحادثات والدّردشة chat rooms[1] ، وفي الواقع عندما تتخاطب عبر الانترنيت فإنّ ما يحدث هو أنّك تكتب رسالة باستخدام لوحة المفاتيح حيث يمكن للآخرين رؤية ما تكتب ويمكن القيام بأفعال قذف وسب عبر غرف المحادثات والدّردشة بخدش شرف واعتبار أي شخص سواء من خلال إسناد أو ادعاء أي واقعة محددة تستوجب عقاب أو احتقار من أسندت إليه أو من دون أن يتضمن ذلك أيّ إسناد لأيّ واقعة وذلك من خلال الكتابات أو الصّور الاستفزازيّة أو الرّسوم أو مسودّات الرّسوم[2].

كما يرتكب القذف والسّب عبر الانترنيت من خلال المبادلات الإلكترونيّة عبر طرفي انترنيت منفصلة، والتي تتمثل في كل التقنيّات العلمية الحديثة عبر الانترنيت (استعمال الحاسب الآلي) تسمح بصورة مباشرة أو غير مباشرة بالتّبادل الإلكتروني للبيانات وهي ما يعرف بتسمية الشريك الإلكتروني e-partner.

حيث لم تعد الثّورة الرّقمية مقصورة على التّبادل الإلكتروني للبيانات عبر الشّبكة المحلّية حتّى في نطاق الشّبكة العالميّة بين الحواسيب الآلية فقط، بل أصبح من الممكن التجوّل في شبكة الانترنيت والانتفاع بالخدمات المتاحة وإجراء المبادلات الإلكترونية من خلال أجهزة الهواتف الخلوية، حيث يمكن من خلال الهاتف النقال استقبال أو إرسال البيانات من وإلى أيّ بريد إلكتروني، وكذلك يمكن الاتصال بأيّ موقع في شبكة الانترنيت للاستفسار عن أيّة معلومات يريدها المستخدم، والهاتف النّقال عند استعماله كطرفي انترنت منفصلة، شأنه شأن الانترنيت قد يساء استخدامه في غير الغرض المخصص له لاقتراف أفعال مختلفة تكون محرّمة أو غير محرمة وتعد جرائم القذف والسّب أحد صور إساءة استخدام هذه الأجهزة وتتم وفق حالتين:

---

[1] – تستخدم غرفة الدردشة أو غرف المحادثة في المقام الأول عن طريق وسائل الاعلام لوصف أي شكل من اشكال المقابلات علي الإنترنت التي تكون علي هيئة مؤتمرات متزامنة (أي التحدث والمناقشة في نفس الوقت) أو تكون أحيانا غير متزامنة (كما في المنتديات).وبالتالي يمكن أن يعني هذا المصطلح أي تكنولوجيا تتراوح بين الدردشة عبر الإنترنت والتي يتوافر بها عنصر رؤية الاشخاص لبعضهم البعض أثناء التحدث.

[2] – محمد أمين أحمد الشوابكة المرجع السابق، ص، ص، 45،48.

الحالة الأولى: تتعلق بالمراسلات الإلكترونيّة المتضمّنة مواد القذف والسّب من شبكة الانترنيت بواسطة خدماتها المتاحة إلى الهاتف النّقال، سواء كانت كتابيّة أو رسوم أوصور ورسائل صوتية.

الحالة الثانية: تتعلق بإرسال المراسلات الإلكترونيّة من الهاتف النّقال إلى شبكة الانترنيت من خلال خدماتها المتاحة، "البريد الإلكتروني، الويب أو غرف المحادثات".

الفرع الثاني

حماية الحق في الصّورة

ليست صورة الإنسان على ما يقول الفيلسوف الفرنسي جان بول سارتر J P Sarter هي ذلك التّشابه والتّداخل بين الخطوط والألوان فحسب، وإنما هي في الواقع شبه شخص quasi–personne مع شبه وجه quasi–visage أو على حد تعبير الفقيه الإيطالي فرانسوا ديني François Degni، سمة مميّزة لفرديّة الشّخص وبصمة خارجية لأناه.

فتعبيرات وجه الإنسان ومدى التقارب أو التباعد الجسدي بينه وبين غيره والواقع والأوضاع التي يتخذها أثناء تصويره كلّها أمور قد تكشف من حيث لا يدري عن كوامن نفسه لذا قيل بحق أن صورة الإنسان هي المظهر المرئي l'apparence tangible للرّوح التي تسكن الجسد، فهي تجسّد الأنا وتكشف مشاعره وانفعالاته، وتظهر أفراحه وأحزانه[1].

يقصد بالحق في الصّورة أنّ للإنسان سلطة منع النقاط صورة له دون موافقته، وكذا حضر نشرها رغما عن إرادته، ولقد اختلف الفقه الفرنسي بشأن مدى اعتبار الحق في الصورة أحد عناصر الحق في الخصوصية إلى ثلاث آراء[2].

1- **الحق في الصّورة أحد عناصر الحق في الخصوصيّة:** إذ ذهب أنصار هذا الرأي إلى أن حق الشّخص في صورته هو أحد عناصر الحق في الحياة الشخصية وأساس من أسس هذه الحياة، ويرتبط بها، فلا يتصور وجود شخص بلا وجه، وأهميّة الحق في الصّورة تفوق حياة الشّخص العائليّة والعاطفيّة.

---

[1]- هشام محمّد فريد، الحماية الجنائيّة لحق الإنسان في صورته، د ط، مكتبة الآلات الحديثة، مصر، د.س.ن، ص 5.

[2]- محمّد محمّد الدّسوقي الشهاوي، الحماية الجنائيّة لحرمة الحياة الخاصة، رسالة دكتوراه، جامعة القاهرة، مصر، د،س، ن، ص،201.

كما أضاف البعض أن التقاط صورة معناه أخذ جزء من ذات الشّخص، وعلّة ذلك الصّلة القويّة بين الصّورة وألفة الإنسان، والحق في الصورة يعد أحد عناصر الحق في الحياة الشخصية.وبناءا على ما تمّ ذكره، فإن أيّ اعتداء عل حق الإنسان في صورته يمثّل انتهاكا لحرمة الحياة الشخصية، وله صفة الاعتداء الفاضح الذي لا يمكن أن يتسامح المجني عليه عنه.

وقد أكّدت محكمة باريس على احترام الحقّ في الصّورة، بحسبان أنّه من ضمن عناصر الحقّ في الخصوصيّة، حيث ورد في أحد أحكامها أنّ الإنسان له صلاحية إقامة دعوى يختصم فيها عن من قام بنشر صورة له دون الحصول على رضاء صاحب الصّورة.

2- الحقّ في الصّورة حقّ مستقلّ: يرى أصحاب هذا الرأي أن الحقّ في الصّورة لا يعدّ عنصرا من عناصر الحق في الحياة الشّخصية، بل هو حقّ منفصل. فإذا تم التقاط صورة للشّخص حال ممارسته لحياته العامة وتم نشرها فهو أمر مقبول، شريطة ألّا يسيء هذا النّشر للشّخص، أو يقلّل من وضعه، وإذا تم ذلك ونتج عن النّشر إساءة للفرد عدّ ذالك اعتداء على حق الشّخص في الصّورة وليس على حقّه في الخصوصية بحسبان أن حقه في الحياة الخاصة لم يلحقه أي ضرر.

وقد اعتنق القضاء الفرنسي هذا الاتّجاه في بعض أحكامه، حيث قضى بان حق الشّخص في الصورة قد يكون موضعا للاعتداء حال ممارسة الفرد لحياته العامة دون أي مساس بالحق في الحياة الخاصة.

3- الحقّ في الصّورة ذو طبيعة مزدوجة: يرى أنصار هذا الرّأي أن الحقّ في الصّورة يكون قائما بذاته مستقلاّ في بعض الأحيان عن الحقّ في الخصوصّية، وأحيانا أخرى يعدّ عنصرا من عناصر الحق في الحياة الخاصة، ويكون في الحالة الأولى، إذا تمّ التقاط ونشر صورة للفرد في مكان عام وهنا يكون أساس فرض الحماية هو الحقّ في الصّورة بصفة منفردة[1].

ويكون في الحالة الثّانية إذا ما تعلقت الصورة بحياة الشّخص، ومثال ذلك إذا كانت صورته تعبر عن جزء من حياته العاطفيّة، وهنا إذا تم نشرها دون موافقة صاحبها عدّ ذلك انتهاكا لحرمة الحياة الشخصية.

[1] - محمّد محمّد الدّسوقي الشّهاوي، المرجع السابق، ص، ص، 202، 203.

وعلى ذلك فإن تصوير الشخصية العامة عن طريق وكالة متخصصة بقصد النشر في الصحافة جائز بشرط أن يكون لذلك علاقة بنشاطه، ويعد من قبيل الخطأ استعمال الصورة في غرض آخر غير المتصل بالتصوير، كالإشغال التجاري، فإذا كان من الجائز عرض صورة الفنان بمناسبة انتقاد نشاطه الفني، فإنه لا يجوز استغلال الصورة للإعلان عن منتج أو خدمة دون إذن كتابي منه.

ولا يجوز التّصوير في الأماكن الخاصة للشّخصيات العامّة دون إذن منهم، إلّا انّه من الممكن أن يمتدّ التّصوير إلى كافة الأماكن العامّة، سواء كانت خاصّة بالعمل أو غيره كالمطاعم والشّوارع والشّواطئ، حيث يعدّ ذلك جزءا من تبعات المهنة والنّشاطات المرتبطة بالحياة العامّة.

ولا يجوز عرض الصّور العامّة عبر الانترنيت على سبيل السّخرية واللهو أو التّسلية من خلال عمل تركيب لها، حيث يعد ذلك تعدّيا على حقّ صاحبها، ومن ثمّ تقع تلك الأفعال تحت طائلة المساءلة القانونيّة المدنيّة والجنائيّة[1].

المطلب الثّاني

الحقّ في سريّة المراسلات عبر الانترنيت

تعتبر المراسلات مجالا هامّا لإيداع أسرار الأفراد سواء تعلقت بالمرسل أو بالمرسل إليه أو بالغير، ولا عبرة بشكل المراسلة فيستوي أن تكون خطابا أو برقية تلكس أو غير ذلك من الأشكال التي تستحدثها التّكنولوجيا طالما أن الواضح من قصد المرسل أنه لم يقصد إطلاع الغير عليها بغير تمييز.

ولقد رافق الاستخدام المتزايد والانتشار الواسع للانترنيت في مختلف مجالات الحياة، زيادة الاعتماد على البريد الإلكتروني كوسيلة اتصال بشكل أصبح يهدّد فيه وجود البريد التّقليدي لاسيما أنه يتيح إرسال واستقبال الرّسائل من وإلى أيّ مكان في العالم وفي ثوان معدودة وبتكلفة بسيطة، فالبريد الإلكتروني يعد أحد أشهر الخدمات التي يقدّمها الانترنيت وأكثرها انتشارا.

[1] – محمد حسين منصور، المرجع السابق، ص، ص، 326، 328.

وكفلت القوانين الجنائيّة المقارنة الحماية لحق سرّية المراسلات إلا أن التساؤل أصبح يثور حول ما إذا كانت حماية هذه السّرّية تطبّق على المراسلات الإلكترونية المكتوبة؟

ونقصد بالمراسلات الإلكترونية المكتوبة كافّة الرّسائل المكتوبة التي يتم تبادلها بطريق تقنية المعلومات سواء تلك التي تتم باستخدام نظام البريد الإلكتروني أو غيره من برمجيات تبادل البيانات إلكترونيا.

وسنتطرّق في هذا المطلب إلى بيان المقصود بالحقّ في سرّيّة المراسلات وصور التّعدي عليه ثم نتعرض إلى الحماية الجنائيّة لسريّة المراسلات الإلكترونيّة في التّشريع الجزائري والتّشريعات المقارنة.

الفرع الأول

صور التعدي على سرية المراسلات

يعدّ الحقّ في سرّيّة المراسلات من أهمّ الحقوق التي تندرج في إطار الحقوق الشّخصية، فهو مظهر لحق سرّيّة الحياة الشّخصية التي ازدادت أهمّيتها في الوقت الحاضر كما أنّه امتداد لحريّة الفكر لأنّ من يخشى انتهاك سرّيّة رسائله لا يجرؤ على أن يعبّر عن ذلك بحريّة، فهو يعبّر عن تبادل الأفكار والعاطفة بهذه الوسائل.

عرّف المشرع الجزائري المراسلات في البند السّادس من المادّة 09 من قانون البريد والمواصلات السّلكية اللاّسلكية[1] بأنها اتّصال مجسّد بشكل كتابي عبر مختلف الوسائل الماديّة، التي يتم توصيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ولا تعتبر الكتب والمجالاّت والجرائد واليوميّات كمادّة للمراسلات.

والملاحظ أنّ نص المادّة 39 من الدّستور الجزائري كان صريحا في حماية الحقّ في سرّيّة المراسلات بل ذهب بعيدا في هذا المجال متجاوزا حتّى دساتير الدول التي تدعي الدّيمقراطية وحماية حقوق الإنسان، حين استعمل عبارة "والاتّصالات الخاصة بكل أشكالها"[2] فهو بذلك ينصّ على كل أنواع المراسلات التي استعملها ويستعملها الإنسان حاضرا ومستقبلا، خاصة مع التّطورات التكنولوجيّة الحديثة في مجال الاتّصالات

---

[1] – المادة 9/6 من القانون 2000–03، المؤرخ في 5 أوت 2000، يحدّد القواعد العامّة المتعلّقة بالبريد والمواصلات السّلكية واللاسّلكية، ج ر، عدد 48، الصادرة بتاريخ، 6 أوت 2000.

[2] – دستور 1996.

والمعلومات كالانترنيت أو الأقمار الصناعيّة ووسائل التجسّس السمعيّة والبصريّة الدّقيقة الحجم والسّهلة في التّمويه.

ومن ثمّ فإنّ مبدأ السّريّة الإلكترونيّة قائم أيضا بالنّسبة للملفّات والبطاقات والبريد الإلكتروني والاتّصالات عبر الانترنيت وهذا المبدأ يتعيّن احترامه من قبل الحكومات والأفراد.

ويقصد بالحقّ في سرّيّة المراسلات، عدم جواز الكشف عن محتويات المراسلات بين الأفراد ذلك أنها بمثابة الوعاء المادّي للأفكار. وتعدّ الرسائل ترجمة مادّية لأفكار شخصية أو لرأي خاص، لا يجوز لغير طرفي هذه المراسلة معرفتها، وبالتالي انتهاكها للحياة الشّخصية فللمراسلات حرمة ومفاد هذه الحرمة أنه لا يجوز الاطّلاع على المراسلات، إلاّ من مرسلها أو المرسل إليه بصرف النّظر عمّا تحتوي عليه هذه المراسلات حتى لو تضمّنت معلومات لا تتعلّق بالحياة الشّخصية للمرسل أو للمرسل إليه.

ومنه فإنّه ليس حتى للسّلطات الحكومية مراقبة المراسلات والاتصالات الإلكترونيّة إلّا لضرورة تتعلّق بالنّظام أو الأمن القومي أو للوقاية من الجرائم أو لحماية حريّات وحقوق الغير، ولا يتمّ الكشف عن المعلومة أو الرّسالة أو الاتّصال إلّا عن طريق السّلطة القضائيّة أو السّلطة الإداريّة لأسباب مشروعة[1].

وإذا قام أحد الأفراد بمراقبة الاتّصال على الانترنيت أو محتوى البريد الإلكتروني أو الملف الذي يمرّ فيه فإن ذلك يعد جريمة يعاقب عليها جنائيّا وذلك ما أشارت إليه المادة 127 من القانون 2000-03 المتضمّن القواعد العامّة المتعلّقة بالبريد والمواصلات السّلكيّة واللّاسلكيّة والتي تنصّ على تطبيق العقوبات الواردة في المادّة 137 من قانون العقوبات على كلّ شخص مرخّص له بتقديم خدمة البريد السريع الدّولي أو كل عون يعمل لديه والذي في إطار ممارسته، يفتح أو يحوّل أو يخرّب البريد أو ينتهك سرّيّة المراسلات أو يساعد في ارتكاب هذه الأفعال.

وتسري نفس العقوبات على كل شخص مرخّص له بتقديم خدمة مواصلات سلكيّة ولاسلكيّة وكلّ عامل لدى متعاملي الشّبكات العموميّة للمواصلات السّلكيّة واللّاسلكيّة والذي في إطار ممارسة مهامه وزيادة على الحالات المقررة قانونا، ينتهك بأيّ طريقة كانت سريّة

[1] – محمّد حسين منصور، المرجع السابق، ص، 370.

المراسلات الصّادرة أو المرسلة أو المستقبلة عن طريق المواصلات السّلكيّة واللاّسلكيّة أو الذي أمر أو ساعد في ارتكاب هذه الأفعال ويعاقب بالحبس من شهرين إلى سنة وبغرامة مالية من 50.000 إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، كلّ شخص غير الأشخاص المذكورين في الفقرتين السابقتين ارتكب أحد الأفعال المعاقب عليها بموجب هاتين الفقرتين.

علاوة على العقوبات المنصوص عليها في الفقرات 1، 2، 3 المشار إليها أعلاه يمنع المخالف من ممارسة كلّ نشاط أو مهنة في قطاع البريد أو في قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين سنة إلى خمس سنوات. وبالعودة لنص المادّة 137 من قانون العقوبات والتي أحالت إليها المادّة 127 من القانون 2000-03 أنّها تنص على معاقبة كلّ موظف أو عون من أعوان الدولة أو مستخدم مندوب عن مصلحة للبريد يقوم بفض أواختلاس أو إتلاف رسائل مسلّمة إلى البريد أو يسهّل فضّها أو اختلاسها أو إتلافها، يعاقب بالحبس من 3 أشهر إلى 5 سنوات وبغرامة من 30.000 إلى 50.000 دج[1].

ويعاقب بنفس العقوبة كلّ مستخدم أو مندوب في مصلحة البرق يختلس برقيّة أو يذيع محتواها، ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العموميّة من 5 إلى 10 سنوات.

ويرد على مبدأ حماية المراسلات الإلكترونيّة بعض الاستثناءات في التشريعات الأوربيّة أهمّها هي:

- مورّدوا الخدمات المعلوماتيّة، حيث لا تقوم في حقّهم جريمة إفشاء سرّيّة الرّسائل الإلكترونيّة استنادا إلى أنّ تدخّلهم أو تطفّلهم تبرّره الضّرورة الفنيّة.

- صاحب العمل الّذي يراقب استخدام العاملين لديه للانترنيت استنادا إلى رضاهم المفترض بسياسة الرّقابة الخاصّة بمصلحة المشروع[2].

كما نجد أنّ المشّرع الجزائري قد سمح في المادّة 65 مكرر 5 هن قانون الإجراءات الجزائيّة باعتراض المراسلات التي تتّم عن طريق وسائل الاتّصال السلكيّة واللاّسلكيّة وذلك

---

[1] – المادّة 37 من القانون رقم 09-01 المتضمّن تعديل قانون العقوبات الجزائري.

[2]– محمّد حسين منصور، المرجع السّابق، ص، 371.

إذا اقتضت ضرورة التّحري في الجريمة المتلبّس بها أو التّحقيق الابتدائي في جرائم المخدّرات أو الجريمة المنظّمة العابرة للحدود الوطنيّة أو الجرائم الماسّة بأنظمة المعالجة الآليّة للمعطيات أو جرائم تبّييض الأموال أو الإرهاب أو الجرائم المتعلّقة بالتّشريع الخاص بالصّرف وكذا جرائم الفساد وذلك بعد إذن وكيل الجمهوريّة المختص[1].

ويذكر كذلك أنّ التّشريعات المقارنة تجيز التنصّت على شبكات الاتّصالات –بما في ذلك الانترنيت–، متى كانت هناك ضرورة لذلك، فقانون الاتّصالات الفرنسي الصادر في 10 يوليو 1991 يجيز اعتراض الاتّصالات البصرية بما في ذلك شبكات تبادل المعلومات وفي هولاندا يجوز لقاضي التّحقيق أن يأمر بالتنصّت على شبكات اتصال الحاسب الآلي متى كانت هناك جرائم خطيرة وكان المتّهم ضالعا فيها ولحماية المراسلات الإلكترونيّة عبر الانترنيت مما قد يلحق بها من اعتداءات على سرّيّتها تم إيجاد بعض البرامج التي تعمل على تفعيل الحماية[2].

ومن صور الاعتداء على حقّ سرّيّة المراسلات في ميدان الانترنيت نجد التنّصت على المراسلات ويتحقّق ذلك عن طريق وسيط إلكتروني قد يكون مكبّر صوت يلتقط المعلومات والبيانات المعالجة وهذا النّوع من الالتقاط حسب الخبراء يعد أكثر الأفعال غير المشروعة ارتكابا وأسهلها من حيث التّنفيذ.

الفرع الثاني

صور الإعتداء على سرّيّة البيانات الشّخصية

إنّ تطوّر الحواسيب الرّقمية وتكنولوجيا الشّبكات، وبشكل خاص الانترنيت أتاح نقل النّشاط الاجتماعي والتّجاري، والسّياسي والثّقافي والاقتصادي من العالم المادّي إلى العالم الافتراضي، ويوما بعد يوم تتكامل الشّبكات العالميّة للمعلومات مع مختلف أنشطة الحياة، وبنفس الوقت فإنّ التّطور الثّقافي في توظيف التقنيّة رافقه توجّه واسع بشأن حماية خصوصيّة الأفراد.

---

[1]– المادّة 65مكرّر05 من الامر06–22، المؤرّخ في، 20 ديسمبر 2006، المتضمّن تعديل قانون الإجراءات الجزائيّة الجزائري، ج ر عدد 84، الصّادرة بتاريخ، 24 ديسمبر 2006.

[2]– عبد الفتّاح بيّومي حجازي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النّموذجي، "دراسة معمّقة في القانون المعلوماتي"، ط1، دار الفكر الجامعي، مصر، 2006، ص 657.

ففي العالم الرّقمي وعالم شبكات المعلومات العالميّة، يترك المستخدم آثارا ودلالات كثيرة تتصل به بشكل سجلات رقميّة حول الموقع الذي زاره والوقت الذي قضاه على الشّبكة والأمور التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بطلب شرائها.

كما أنّ العديد إن لم نقل كافّة المواقع التّفاعلية على شبكة الانترنيت، تطلب من المستخدم تقديم وتعبئة نموذج يتضمّن معلومات مختلفة، وتتضمّن مادّة هذه المعلومات اسم المستخدم وعنوانه للعمل والمنزل وأرقام الهاتف والفاكس وعنوان البريد الإلكتروني ومعلومات عن السّن والجنس والحالة الاجتماعيّة ومكان الإقامة والدخل الشّهري أو السّنوي، وأما بالنّسبة لمواقع البيع والشّراء على الانترنيت والمواقع التي تمّ فيها إجراء عمليّات دفع فإنّها تطلب رقم بطاقة الاعتماد ونوعها وتاريخ انتهائها[1].

وبالرّغم من المنافع الكبيرة التي أفرزتها تكنولوجيا المعلومات وشبكات المعلومات العالميّة فإنّها أيضا أوجدت خطرا حقيقيا تمثّل في إمكانية جمع المعلومات وتخزينها والاتّصال بها والوصول إليها بعدّة طرق غير مشروعة وغير قانونيّة، بدون علم أو معرفة صاحب المعلومات ونذكر منها:

أوّلا: انتحال الشّخصية:

تعتبر جريمة الألفيّة الجديدة، كما سمّاها بعض المختصّين في أمن المعلومات، وذلك نظرا لانتشار ارتكابها خاصة في الأوساط التجارية وتتمثل هذه الجريمة في استخدام هويّة شخصيّة أخرى بطريقة غير شرعيّة وتهدف إمّا لغرض الاستفادة من مكانة تلك الهويّة أو لإخفاء هويّة شخصيّة المجرم لتسهيل ارتكابه لجرائم أخرى، وأنّ ارتكاب هذه الجريمة على شبكة الانترنيت أمر سهل، وهذا من أكبر سلبيّات الانترنيت الأمنيّة[2].

كما يمكن أن يحصل التّعدي من خلال أشخاص أو عن بعد، ويجب أن تمنع إجراءات السّلامة انتحال صفة الآخرين بقصد الدّخول إلى نظام الحاسب، ومن أنواع هذه

---

[1] – يونس عرب، المخاطر التي تهدد الخصوصيّة وخصوصية المعلومات في العصر الرّقمي، ص 11، 12.
Alyasser.net/vb/showthead.php? t:10932.
تاريخ الزيارة: 27 ماي 2013

[2] – عمرو عيسى الفقّى، الجرائم المعلوماتيّة، جرائم الحاسب الآلي والانترنيت في مصر والدّول العربيّة، د،ط، المكتب الجامعي الحديث، مصر، د،س،ن، ص، ص، 102، 103.

التعدّيات الدّخول إلى نظام حماية التّشغيل فمن الممكن أن يستخدم المجرم هويّة مزوّرة للدّخول إلى المناطق المحظورة أو الدّخول إلى مبنى مركز المعلومات، أو الحاسب، ويمكن استخدام أسلوب التظاهر، وهو أن يحمل الفرد معدّات الحاسب ويظهر بمظهر الذي ينتمي للمكان لكي يتمكن من الدخول، ويمكن استخدام الانتحال الإلكتروني من خلال استخدام كلمات المرور أو الدّخول أو الرّقم الشّخصي أو رمز الهاتف (الصوت)...إلخ، ولفهم كيف تتم عمليّات الانتحال لابد من فهم كيفيّة التّعرف على الهويّة من قبل نظام الحاسب.

والهويّة طريقة تخبر النّظام فيها من أنت؟ مثل أن تدخل رقم الحاسب أو كلمة المرور...إلخ وهناك ثلاث طرق لإثبات من أنت وهي:

- شيء تعرفه كرقم الهوية، أو كلمة المرور.
- شيء تملكه، مثل مفتاح المبنى، أو البطاقة الذكية.
- شيء منك، أو تفعله، مثل الصفات الفيزيولوجية، كبصمة اليد أو بصمة الصوت، أو توقيعك.

ثانيا: جمع أو معالجة بيانات حقيقيّة دون ترخيص

على الرّغم من اعتراف بعض الدول بمبدأ حرّية الاتصال ونقل المعلومات فإنّها قد تأخذ بنظام التّرخيص، وبمقتضاه يلزم صدور ترخيص سابق بإقامة أو استعمال المنشآت والأجهزة التي تستخدم في بث أو نقل المعلومات الشخصية أو معالجتها، ويطلق بعضهم على هذه العمليّة عقود نقل التكنولوجيا، أي من حق صاحب البرنامج التّصرف في البرنامج واستغلاله واستعماله، وفي الغالب أن يتنازل صاحب البرنامج عن حقوقه المتفرّعة عن الملكية "كلها أو بعضها" للغير ببيعها أو بمنح ترخيص باستغلالها وتظلّ له جميع حقوق المؤلف التي يحميها حق المؤلف، إذ لا يتلقى الغير سوى النّفسية المادّية للبرنامج، ولكن إذا تلقّى الغير ملكيّة هذه النّسخة والحقّ في استغلالها فإنّ له حق استخدامها في تشغيل الحاسوب بغرض معالجة المعلومات ونقلها داخل الدّولة أو خارجها عن طريق شبكات الاتصال وفقا للشّروط التي بمقتضاها تلقّى ملكيّة البرنامج أو الحق في استغلاله[1].

[1] – علي أحمد عبد الزّغبي، المرجع السابق، ص 346.

حيث يحدث أن يستخدم لجمع أو تخزين البيانات أساليب تتسم بعدم المشروعيّة ممّا يمثّل بلا أدنى شك تهديدا للحياة الشّخصية للفرد إذا كان محل هذه الأعمال بيانات شخصيّة.

ومن قبيل هذه الأساليب غير المشروعة: التقاط الارتجاجات التي تحدثها الأصوات في الجدران الإسمنتيّة للحجرات ومعالجتها بحاسب مزوّد ببرنامج خاص لترجمتها إلى كلمات وعبارات ومراقبة واعتراض وتفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني وتوصيل أسلاك بطريقة خفيّة إلى الحاسب الذي يخزّن داخله البيانات والتوصّل بطريق غير مشروع إلى ملفات تخص الآخرين، وغير ذلك من الأساليب التي من شأنها جمع بيانات بصورة غير مشروعة كالتّدليس والغش أو التنصّت على الهاتف أو التّسجيل دون سبق الحصول على إذن من القضاء[1].

ويتمثّل الرّكن المادي لهذه الجريمة بقيام الجاني بتسجيل البيانات الاسميّة، ويتخذ هذا التّسجيل كل ما يقوم به المتّهم من أفعال ومنها قيامه بالمعالجة الإلكترونيّة للبيانات الشّخصيّة مع عدم وضع الضّمانات الواجبة للحفاظ على سرّيّة هذه البيانات مما قد يؤدي إلى تشويه أو إتلاف أو إطلاع الغير عليها دون حصوله على تصريح يسمح له بذلك.

كما تتحقّق الجريمة بقيام المتّهم بتجميع البيانات دون سبب مشروع أو بمخالفة القانون باستخدام طرق الغش والتنصّت والتّسجيل دون الحصول على إذن من المحكمة المختصة.

أمّا الركن المعنوي فيتحقّق بصورتين إما عن طريق العمد أو عن طريق الخطأ، فأمّا العمد فيقوم بتحقّق القصد الجنائي بعنصريه، العلم والإرادة، ويتمّ ذلك من خلال قيام الجاني بتجميع إحدى البيانات الشّخصيّة بطرق عمديّة، أما الخطأ فيتحقّق بقيام المتهم بعمليّة المعالجة الإلكترونيّة للبيانات الشّخصيّة دون وضع الضوابط والاحتياطات اللاّزمة لسلامة وأمن هذه البيانات[2].

---

[1] – فتّوح الشّاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلّف والمصنّفات الفنيّة ودور الشّرطة والقانون، "دراسة مقارنة"، ط2، منشورات الحلبي الحقوقية، لبنان، 2007، ص 277.

[2] – محمّد محمّد الدّسوقي الشّهاوي، المرجع السّابق، ص 295، 296.

بالرّغم من الصّعوبة التي تكتنف عملية التّمييز بين ما هو من البيانات ذات الطابع الشّخصي وبين ما لا يعد كذلك إلّا أن البعض يرى أنّ من شأن استخدام الحواسيب كبنوك للمعلومات، التوصل بشكل أو بآخر إلى السّمات الأساسيّة التي يتميّز بها الفرد الذي تخصّه هذه البيانات، مما يمثل بلا شك تهديدا غير مسبوق لخصوصيّة الفرد حتى ولو لم يتم جمع معلومات شخصيّة كاملة عن الشّخص من خلالها، حيث يمكن من خلال جمع معلومات جزئيّة عن شخصيّة الفرد مثل المعلومات الخاصّة بحالته الصّحية أو التعليميّة أو الماليّة أو الانتمائيّة... وغيرها التّوصل إلى صورة تقريبيّة للشّخص.

وهو الأمر الذي دعا الفقيه "T.F.Fry" إلى القول بأن من شأن استخدام الحواسيب كبنوك للمعلومات جعل حياة الأفراد ككتاب مفتوح من السّهل لشخص لديه إمكانيّة التّوصّل إليها للإطلاع عليه.

ثالثا: إفشاء بيانات بصورة غير شرعية:

على الرّغم من تعدّد بنوك المعلومات وكثرة البيانات المخزّنة، غير أنّ تلك البيانات تحظى بحرمة وقدسيّة كباقي صور الخصوصيّة، قد تشمل أسرارهم الشّخصيّة أو أوضاعهم الذّاتيّة في مختلف الاتّجاهات، والحفاظ عليها من العلن مهّمة ذات طابع إنساني وأخلاقي، وقد جسد المشرّع الفرنسي هذه الحماية للبيانات أي كان نوعها (صور، كتابات، أصوات) من الإفشاء والنّقل والنّشر كما في المادّة 43 من قانون المعالجة المعلوماتيّة والحرّيات لسنة 1978 كما أورد المشرّع الفرنسي في المادّة 226/22 من قانون العقوبات الجديد، تحريم كل فعل يرتكبه شخص من شأنه الكشف عن بيانات شخصيّة، بمناسبة تسجيل أو فهرسة أو نقل أو أي شكل من أشكال معالجة البيانات الشّخصيّة التي يترتب عن كشفها الاعتداء على الشّخصيّة الاعتباريّة لصاحب الشّأن أو حرمة حياته الشّخصيّة في هذه المعلومات[1].

كما أن المشرّع الفرنسي نصّ أنّ جميع المعلومات التي تجمع وتحفظ بوسائل غير قانونية، محرمة، كما يمنح لكلّ شخص طبيعي حق المعارضة لأسباب شرعية، عن كل جمع للمعلومات محل التخزين في الكمبيوتر[2].

---

[1] – علي أحمد عبد الزّغبي، المرجع السّابق، ص 355.

[2] – فوزي أوصديق، اشكاليّة المعلوماتيّة بين حق الخصوصيّة وإفشاء الأسرار المهنيّة (السّر البنكي نموذجا).
http://isegs.com/forum/shouthead.phpi=3537
تاريخ الزيارة:28 ماي 2013

إلّا أنّ المحافظة على الحياة الشّخصيّة أو الخصوصيّة لا تمنع السّلطات الرّسميّة من إفشاء البيانات التي تخزنها في برامجها، لكن هنا وجب التحديد، فإن كانت البيانات تتناول الحياة الحميمية للفرد كحياته العاطفيّة أو شرفه أو كل ما يتعلق بسمعته، فلا يحقّ للسّلطات الرّسمية نشرها إذا كان من شأنها عدم المساهمة في كشف القضيّة التي هي موضوع بحث، فطالما أنّ الكشف عن مثل هذه المعلومات لا شأن له بما هو متداول، فلا يجوز إفشاؤها لا من قبل السّلطات الرّسمية ولا من قبل الغير، أما إذا كان لهذه المعلومات صلة وثيقة بالقضيّة المثارة فلا مانع من إفشائها توصّلا لكشف الحقيقة لأنّه في مثل هذه الحالة يجب تقديم المصلحة العامّة على المصلحة الخاصة الآيلة بالمحافظة على المعلومات الحميمة وعدم كشفها، وفي هذا السيّاق اعتبرت المحكمة الأمريكيّة أن كشف أو إفشاء البيانات الخاصة بمستحقات المدعي إلى إدارة معوّقي الحرب في إطار برنامج المقارنة أمر مباح لأن هذه الإدارة ملزمة بوضع هذه المستحقّات في الاعتبار[1].

من خلال التّحليل القانوني لهذه الجريمة يتضح أن موضوعها بيانات شخصيّة (رسميّة) على النّحو المذكور آنفا، كما يتضح أنّ هذه الجريمة تقترب في حقيقتها من جريمة إفشاء الأسرار التي يعاقب عليها قانون العقوبات، فعلى الرّغم من وجود اختلاف بينهما في الأركان والموضوع، إلّا أنّهما يتّفقان في العلّة التّشريعيّة، وهي حماية البيانات أو المعلومات الشّخصيّة، وعليه تقوم هذه الجريمة على ركنين هما:

أ- **الرّكن المادي:** وهو الذي يكون في شكل القيام بفعل الحيازة للبيانات سواء بقصد تصنيفها أو نقلها أو لعلاجها، وفعل الإفشاء، أي للشخص الآخر غير المختص أو المخوّل له تلقي هذه المعلومات، وكما ينبغي لقيام الرّكن المادّي تحقّق النّتيجة الإجرامية وهو أنّ يترتّب عن فعل الإفشاء أضرارا للشخص أو اعتداءا على حرمة خصوصيّته أو شرفه أو اعتباره وأنّ ترتبط هذه النّتيجة بالفعل بعلاقة سببية، وعليه فإنّه يتطلّب لقيام الرّكن المادّي في هذه الجريمة توافر الشّروط الثّلاثة الآتية:

- أن يكون من طبيعة فعل الإفشاء اعتداءا على الشّرف أو الحياة الشّخصيّة، كما يستوي في نظم القانون أنّ تكون هذه البيانات صحيحة أو مزوّرة طالما أنّ إفشاؤها يمثّل اعتداءا.

---

[1]- نعيم مغبغب، حماية برامج الكمبيوتر، "دراسة في القانون المقارن" ط2، منشورات الحلبي الحقوقية، لبنان، 2009.

– أن يكون الإفشاء لشخص أو أشخاص ليس له أو لهم حقّ الاطلاع على هذه البيانات.

– بالإضافة إلى انتفاء رضا المجني عليه.

ب– الرّكن المعنوي: يختلف الرّكن المعنوي لهذه الجريمة عنه في الجرائم السّابقة إذ تتّخذ إحدى الصّورتين، إمّا العمد أو الخطأ، فالصّورة الأولى (العمد) تتمثل في عنصري العلم والإرادة، أي علم الجاني بأنّ البيانات التي يعالجها هي بيانات شخصّية، يمثّل إفشاؤها اعتداءا على الشّرف أو الاعتبار أو حرمة الحياة الشّخصيّة، مع علمه أنّه يفشي هذه البيانات إلى شخص غير جائز له قانونا الإطّلاع عليها، وزيادة على ذلك تتجه إرادته إلى ارتكاب فعل الإفشاء، أيّا كانت صورته أو وسيلته.

أما الصّورة الثّانية (الخطأ)، فمستفاده مما أشار إليه المشرع الفرنسي من العقاب على الإفشاء إذا وقع نتيجة إهمال أو رعونة أو ترك للبيانات الشّخصيّة[1].

أمّا عقوبة هذه الجريمة فإنّ المشرّع الفرنسي فرّق في العقاب على أساس الرّكن المعنوي سواء في قانون المعالجة الإلكترونيّة والحريّات أو في قانون العقوبات الجديد.

إذ جعل المشّرع الفرنسي عقوبة هذه الجريمة في حالة ارتكابها عن عمد عقوبة الحبس من شهرين إلى 6 أشهر بالإضافة إلى غرامة مالية من 2000 إلى 20000 ألف فرنك أو بإحدى هاتين العقوبتين.

أمّا إذا وقعت الجريمة ذاتها عن خطأ نتيجة رعونة أو إهمال أو ترك للبيانات الشّخصيّة فإنّ العقوبة تقتصر على الغرامة دون الحبس، وكذا فعل المشرّع في قانون العقوبات إذ جعل عقوبة الجريمة عن عمد هي الحبس مدة سنة وغرامة ب 100 ألف فرنك أما إذا وقعت الجريمة ذاتها نتيجة إهمال أو عدم احتياط أي بصورة غير عمدية فإن العقوبة تكون الغرامة فقط ومقدارها هو 50 ألف فرنك.

رابعا: الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية:

من أبلغ الأخطار أو المضار التي تصيب الفرد في خصوصيّة معلوماته بوصفها من أهم أوجه الحياة الشّخصيّة المقصودة من معنى هذا الحقّ عند اتّصاله بالانترنيت، هو أنّ المعلومات التي تجمع عن فرد من الأفراد لغرض معين ومحدد إبتداءا، تستخدم لدى تخزينها

[1] – علي أحمد عبد الزغبي، المرجع السابق، ص، ص، 356،359.

في الحاسب الآلي استخدامات عديدة تتجاوز الهدف الذي جمعت من أجله في الأساس، فالانحراف في مجال المعالجة الإلكترونية هو الخروج عن الغرض أو الغاية الأساسية التي من أجلها تم الفعل، إلى غرض أو غاية غير مقرّرة قانونا، ويتمثّل ذلك الغرض أو الغاية بالإساءة إلى سمعة الفرد ومراقبته أو بتوحيد ومحو الشّخصيّة أو بالاستغلال التّجاري أو من أجل الضّغط أو الابتزاز السّياسي ونحوهما، ولذلك فإنّ جميع هذه الاستخدامات غير المتوقّعة من أيّة جهة كانت، يؤدي إلى إيذاء الفرد وتقليل فرص تمتّعه بحقوقه على وجهها الأكمل، بل وتصبح قيدا على حرّيته فيما يريد القيام به من الأمور؛ و مما لا جدال فيه أن نوع المعلومات التي يعطيها الإنسان عن نفسه وحجمها تختلف من جهة إلى أخرى وذلك وفقا للهدف الذي دفع هذا الفرد إلى إعطاء تلك المعلومات.

وبناءا على ما تقدّم فقد عمل المشرّع أكثر من أي وقت مضى للتّدخل من أجل تنظيم هذا الموضوع بما يصون حقوق الأفراد وحرّياتهم في مواجهة هذه التهديدات سواء كان مصدرها الأجهزة الحكوميّة وهو في الأغلب المؤسّسات والشّركات الخاصة ومما لا شك فيه أنّ هذه الحماية التّشريعية إنّما تراعي مصلحة قرّرها الدّستور من جهة ومن جهة أخرى تمكّن السّلطة الإداريّة من الهيمنة والإشراف على الأنشطة التي تمسّ حقوق الأفراد وحرّياتهم بصرف النّظر عن الجهة التي تقوم بهذا النشاط[1].

وأركان هذه الجريمة هي:

أ- الرّكن المادي: يتوفّر هذا الرّكن إذا ما انحرف الجاني عن الغاية أو الهدف من المعالجة الإلكترونيّة للبيانات، ولا يفرّق القانون بين حيازة الفرد للبيانات بقصد تصنيفها أو نقلها أو علاجها بأية وسيلة[2].

و يتحقّق هذا الرّكن بمجرد الانحراف عن الهدف من معالجة البيانات الاسمية والغاية هي موضوع المعالجة الإلكترونية، أي الغرض المتوخى من معالجة البيانات الاسميّة.

ب- الرّكن المعنوي: جريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونيّة للبيانات الاسمية عمدية، يتخذ فيها الركن المعنوي صورة القصد الجنائي العام، فيجب أن

---

(1) – علي أحمد عبد الزغبي، المرجع السابق، ص 259، 260.

(2) – محمّد محمّد الدّسوقي الشّهاوي، المرجع السابق، ص 298.

يعلم الجاني أن ما يأتيه من أفعال يؤدي إلى الانحراف عن الهدف أو العرض من معالجة البيانات كما يجب أن تتجه إرادته إلى الوصول إلى ذلك الهدف.

فقيام أحد الأشخاص بمعرفة مصادر ثروة الآخر من خلال قيامه بالانحراف عن الغاية من المعالجة الإلكترونية للبيانات الاسمية الخاصة بالمجني عليه يتحقق به الرّكن المعنوي لهذه الجريمة.

أما العقوبة المقرّرة لهذه الجريمة فقد شدّد المشرع الفرنسي عقوبة هذه الجريمة سواء في قانون المعالجة الإلكترونيّة والحرّيات أم في قانون العقوبات الجديد لما تمثله هذه الجريمة من اعتداء جسيم على خصوصيّة البيانات الشّخصيّة، إذ جعل عقوبة هذه الجريمة في قانون المعالجة الإلكترونيّة والحرّيات هي الحبس من سنة إلى 5 سنوات والغرامة من 20 ألف إلى 200 ألف فرنك.

بيد أنه جعل العقوبة اشد في قانون العقوبات الجديد إذ جعل العقوبة الحبس لمدة 5 سنوات والغرامة 200 ألف فرنك.

بمعنى أنه لم يضع حدا أدنى أو حتى أقصى للعقوبة، أو أنه لم يترك للقاضي سلطة تقديرية للحكم بعقوبة أقل من ذلك[1].

وعلى غرار المشرّع الفرنسي نجد المشرّع الجزائري تناول الحقّ في سرّيّة البيانات الشّخصيّة بموجب القانون رقم 04-15 المؤرّخ في العاشر من نوفمبر 2004 الموافق ل السّابع والعشرين من رمضان لسنة 1425 هجريّة المعدّل والمتمّم للأم رقم 66-156 المتضمن قانون العقوبات، والذي افرد القسم "السّابع مكرر" منه تحت عنوان، المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن ثمانية مواد، ونصّ على عدّة جرائم منها ما نصّت عليه المادّة 394 مكرر 2 من قانون العقوبات: "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة مالية من 1000000 دج إلى 5000000 دج كل من يقوم عمدا وعن طريق الغش بما يلي:

1- تصميم أو بحث أو توفير أو نشر أو الاتّجار في معطيات مخزّنة أو معالجة أو مرسلة عن طريق منظومة معلوماتيّة يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

[1]- محمّد محمّد الدّسوقي الشّهاوي، المرجع السّابق، ص 362.

2- حيازة أو إفشاء أو نشر أو استعمال، لأي غرض كان، المعطيات المتحصل عليها من احدى الجرائم المنصوص علها هذا القسم"[1].

كما شدّدت العقوبة الى الضّعف إذا استهدفت الجريمة الدّفاع الوطني أو المؤسسات العموميّة، وشدّدت عقوبة الغرامة على الشّخص المعنوي إلى خمس مرات الحد الأقصى المقرّر للشّخص الطّبيعي، وذلك يعد إقرارا من المواد 18 مكرر، 18 مكرر01، و51 مكرر من التّعديل نفسه لمسؤوليّة الشّخص المعنوي بوجه عام.

كما عاقبت تلك المواد على الاشتراك في مجموعة أو في اتفاق يتألّف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم.

ونصّ هذا التعديل ايضا على عقوبة مصادرة وسائل ارتكاب الجريمة وإغلاق المواقع التي تكون محلا لها، وإغلاق المحل أو المكان الذي ارتكبت فيه الجريمة.كما عاقب التعديل أيضا على الشروع في جرائم هذا القسم[2].

المبحث الثّاني

عناصر المسؤوليّة الإلكترونيّة

تعّرضنا فيما سبق (المبحث الأوّل) لمفهوم الحقّ في الحياة الشّخصيّة في مجال المعلوماتيّة بذكر أهمّ المخاطر الحديثة، وسنحاول فيما يلي (المبحث الثّاني) دراسة عناصر المسؤوليّة الإلكترونيّة وهي: الضّرر (المطلب الأوّل) وعلاقة السّببيّة (المطلب الثّاني) بذكر إثباتها بالإضافة إلى التّعويض.

المطلب الأّول

الضّرر الإلكتروني

---

[1]- المادة 394 مكرر2 من القانون 04-15 المعدل لقانون العدل للأمر، 66-156 المتضمّن قانون العقوبات الجزائري.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر، 2007، ص 62-63.

الضّرر هو الرّكن الجوهري في المسؤوليّة المدنيّة لأنّه محل الالتزام بالتّعويض، وهو ذلك الإخلال بمصلحة محقّقة مشروعة للمضرور في ماله أو شخصه، أو في أيّ حقّ من حقوقه، ووقوع الضّرر مسألة موضوعيّة لا رقابة فيها للمحكمة ولكنّ الشروط الواجب توافرها في الضّرر مسألة قانونيّة تخضع لرقابتها.

الفرع الأوّل

طبيعة الضّرر الإلكتروني

الضّرر قد يكون ماديّا وقد يكون أدبيّا يصيب المضرور في قيمة غير مالية كشعوره أو عاطفته أو سمعته أو غير ذلك من القيم، وتتنوّع صور وتطبيقات الضّرر في المجال الإلكتروني، فهو لا يتّسم بطبيعة واحدة.

وينبغي الإشارة في البداية إلى أن المسؤوليّة الإلكترونيّة قد تكون عقديّة وقد تكون تقصيريّة، وتظهر أهميّة ذلك في التّعويض، ففي الأولى (العقديّة) يقتصر التّعويض على الضّرر المتوقّع، إلّا في حالتيّ الغشّ والخطأ الجسمي حيث يشمل التّعويض الضّرر غير المتوقّع، أمّا في الثّانية (التقصيريّة)، فإنّ التّعويض يشمل كل الأضرار النّاجمة عن العمل غير المشروع، سواء كان متوقّعا أو غير متوقّع، ما دام الضّرر مباشرا[1].

الفرع الثّاني

تطبيقات الضّرر الإلكتروني

الصّورة الغالبة للضّرر الإلكتروني المادّي هو تدمير الثّروة المعلوماتيّة في البرامج وقواعد المعلومات وما يمكن أن ينجم عن ذلك من نتائج على المشاريع والإنتاج والأجهزة والخدمات، ويبدو ذلك أيضا في حالة الفيروس بأغراضه التّدميرية المختلفة للحاسب وبرامجه وما ينجم عن ذلك من أضرار ماديّة تتمثّل في الخسارة الّتي تلحق المضرور وما فاته من كسب، بل والأضرار المستقبليّة المحقّقة الوقوع، فبعض الفيروسات تنتشر وتتفاقم آثارها مع مرور الزمن، والضّرر النّاجم عن تفويت الفرصة مثل عرقلة المشروع عن الاشتراك في مسابقة إنتاج أو معرض معين.

[1]– محمد حسن منصور، المرجع السابق، ص.399.

وما يهمّنا هنا من صور الضّرر الإلكتروني (الأولي) حالة انتهاك السّريّة المعلوماتيّة والبيانات الشّخصيّة وحرمة الحياة الخاصّة، وذلك عن طريق التّجسّس الإلكتروني والذي يتمّ بواسطته الحصول على المعلومات الشّخصيّة، والتي قد يساء استعمالها،[1] أو عن طريق اختراق أجهزة الحاسب وبرامجه وقواعد المعلومات، ومثاله أيضا الأضرار النّاجمة عن البثّ الفضائي للبرامج التي تتضمّن مساسا بأمن وكرامة الأفراد والقيم السّائدة لديهم، وما قد تنطوي عليه من إهانات وتجريح لحرمة وخصوصيّة الآخرين، وذلك عن طريق ما تحمله من أساليب دعائيّة مغرضة أو عرض الوقائع الكاذبة والأنباء المحرفّة[2].

المطلب الثّاني

علاقة السّببيّة

لا يكفي مجرّد ثبوت الخطأ ووقوع الضّرر لقيام المسؤوليّة بل يلزم أن يكون هذا الضّرر ناتجا عن ذلك الخطأ، أي وجود علاقة مباشرة بينهما، وهذا ما يعرف بركن السّببيّة كركن ثالث من أركان المسؤوليّة.

وتنتفي العلاقة السّببيّة إذا كان الضّرر راجعا إلى سبب أجنبي، كما تنتفي أيضا إذا لم يكن الخطأ هو السّبب المباشر أو السّبب المنتج، ويتوفّر السّبب الأجنبي إذا كان الضّرر راجعا إلى قوّة قاهرة أو حادث مفاجئ أو إلى خطأ المضرور أو خطأ الغير.

إنّ تحديد العلاقة السّببيّة في المجال الإلكتروني يعدّ بالأمر الصّعب لكون المسائل الإلكترونيّة معقّدة وتتغيّر حالاتها وخصائصها وعدم وضوح الأسباب، فقد ترجع أسباب الضّرر إلى عوامل بعيدة أو خفيّة، أو القوّة القاهرة أو الحادث الفجائي، يؤدّي إلى قطع رابطة السّببيّة إذا كان غير متوقّع ويستحيل ردّه، مما يجعل تنفيذ الالتزام مستحيلا، وبالتّالي لا محلّ للتّعويض.

كما أنّ تقدير مدى اعتبار الواقعة قوّة قاهرة هو تقدير موضوعي تملكه محكمة الموضوع، وينبغي لقيام القوّة القاهرة أن تكون الواقعة معلومة، فإذا لم يتّضح سبب الضّرر

---

[1] – فتّوح الشاذلي، المرجع السابق، ص.325.

[2] – محمد حسن منصور، المرجع نفسه، ص.400.

لبقاء بعض الظّروف التي أحاطت بوقوعها مجهولة، فإن المدّعى عليه المسؤول لا يستطيع التّمسك بالسّبب الأجنبي لعدم مسؤوليته[1].

كما ينفي خطأ المضرور علاقة السّببيّة، إذا كان هو وحده السّبب في وقوع الضّرر، ويؤدي إلى إنقاص التّعويض، إذا ساهم مع خطأ المسؤول في وقوعه بقدر نسبة الخطأ، كما أنّ الأصل أن خطأ المضرور لا يخفّف من المسؤولية إلّا إذا تبيّن من ظروف الحادث أن هذا الخطأ هو العامل الرّئيسي في وقوع الضّرر وأنّه بلغ قدرا من الجسامة بحيث يستغرق خطأ المسؤول.

ومن أمثلة خطأ المضرور عدم تعاون المتعاقد أو المستخدم الإلكتروني مع المنتج أو مقدّم الخدمة في تنفيذ الالتزام، أو عدم تقديم المعلومات الكافية أو عدم تقديم احتياجاته بوضوح، بالإضافة إلى مخالفة تعليمات استخدام الجهاز أو البرنامج إذا كانت واضحة ومحدّدة وغير تعسفيّة[2].

ويقطع خطأ الغير رابطة السّببيّة إذا كان هو السّبب الوحيد في إحداث الضّرر، ولا يعتبر من الغير الأشخاص الذين يسأل عنهم المدّعي عليه مدين مثل التّابع ومن يتولّى المسؤول رقابتهم، كما قد يكون الخطأ مشتركا في حالة وقوع الضّرر نتيجة أكثر من خطأ، فإذا تعدّدت الأخطاء التي تقوم بينها وبين الضّرر علاقة سببيّة، ولم يكن من بينها خطأ مستغرقا للأخطاء الأخرى، ثم توزيع المسؤوليّة بين المخطئين كلّ حسب نسبة الخطأ الّذي ارتكبه، فإذا ساهم المضرور في الخطأ فإن حقّه في التّعويض قبل المدّعى عليه يتمّ إنقاصه بقدر مساهمته في الخطأ.

والقاعدة أنّه إذا استغرق أحد الخطأين الخطأ الآخر، لم يكن للخطأ المستغرق من أثر، فإذا استغرق خطأ المدّعي عليه خطأ المضرور قامت مسؤوليّة المدّعى عليه كاملة ولا يؤثّر فيها خطأ المضرور، أما إذا استغرق خطأ المضرور خطأ المدّعى عليه، وكل ذلك بشرط أن يكون الخطأ المستغرق كافيا بذاته لإحداث النّتيجة أي الضّرر[3].

---

(1) – محمد حسين منصور، المرجع السابق، ص402.

(2) – محمد حسين منصور، المرجع السابق، ص.402.

(3) – المرجع نفسه، ص.403.

بالإضافة إلى ذلك يمكن أن يؤدّي الخطأ الواحد إلى سلسلة من الأضرار المتعاقبة، واحدا بعد الآخر، هنا يثور البحث حول مدى مسؤولية المدّعى عليه مرتكب الخطأ عن هذه الأضرار المتوالية، هل يسأل عنها جميعا أم تقتصر مسؤوليّته على البعض منها دون البعض الآخر؟.

يستقرّ الفقه والقضاء المقارن على أنّ المسؤول يلتزم بالتّعويض عن الضّرر المباشر فقط، وهذا ما ينطبق على كلّ من المسؤوليّة العقديّة والمسؤوليّة التقصيريّة، فالضّرر غير المباشر لا يستلزم التّعويض عنه، إذ ينبغي تعويض الضّرر الّذي يكون نتيجة طبيعيّة للخطأ الذي أحدث ضررا مباشرا، أما إذا لم يكن الضرر نتيجة للخطأ فإنّ العلاقة السّببيّة تنتفي وبالتّالي انتهاء المخطئ بتقديم التّعويض.

كما قد يقع الضّرر نتيجة فعل شخص غير محدّد من بين مجموعة معيّنة من الأشخاص، يحدث ذلك كثيرا في مجال الانترنيت ونظم المعلومات والبرامج، حيث يمكن اكتشاف السّكان أو الجهة الّتي وقع منها الخطأ دون تحديد الشّخص المسؤول بالذّات.

لا تثور صعوبة في حال توافر المسؤوليّة عن فعل الغير، حيث تقوم مسؤوليّة المتبوع عن وقوع الضّرر من أحد التّابعين ولو لم يتمّ تحديده، مثال ذلك قيام أحد العاملين بشركة المعلوماتيّة بإفشاء أسرار أو زرع الفيروس، وكذلك الحال بالنّسبة لمتولّي الرقابة مثل عبث أحد الأبناء بالانترنيت.

وإذا حدث الضّرر بفعل الشيء الواقع تحت الحراسة المشتركة لعدّة أشخاص في نفس الوقت، إذا كانت لهم سلطات مماثلة في استعماله وادارته وتوجيهه، هنا يعتبر الجميع أو كل مشارك في النّشاط بحسب الأحوال، حرسا ويسألون مسؤوليّة تضامنية، ونفس الحكم في حالة الخطأ الشّخصي الصادر من أحد الباحثين القائمين على نشاط معين، كما هو الحال في مجال البرامج والمعلومات[1].

[1] – كذلك الحال بمناسبة النشاط المشترك الذي يقوم به عدة أشخاص بصورة متوازنة، وينطبق ذلك على كل صور النشاط الجماعي.

الفرع الأوّل

إثبات المسؤوليّة

تقضي القواعد العامّة بأنّ المدّعى (المضرور) هو الّذي يقع عليه عبء إثبات عناصر المسؤوليّة من خطأ وضرر وعلاقة سببيّة.

وإن كان إثبات الضّرر لا يثير الكثير من الصّعوبات، إلّا أنّ الأمر يختلف فيما يتعلّق بإثبات الخطأ ورابطة السّببيّة في المجال الإلكتروني.

الاصل أنّ يتم إثبات الخطأ بكافّة الطّرق لأنّ الأمر يتعلّق بواقعة ماديّة، ومن ثم يقع على عاتق المضّرور عبء الإثبات، أيّ الانحراف عن السّلوك المألوف للشّخص العادي، وقد يرد الإثّبات على تصرّف قانوني يلزم إثباته بالكتابة، وقد يكون الخطأ في الإخلال بالتزام بتحقيق نتيجة، وهنا يكفي إثبات عدم تحقّق النّتيجة.

ومن المسائل المتعارف عليها أن استخلاص الخطأ الموجب للمسؤوليّة يعدّ من المسائل الموضوعيّة الّتي تدخل في السلطات التّقديريّة لقاضي الموضوع الّتي يستمدّها من وقائع الدّعوى، ويقع عبء إثبات رابطة السّببيّة على عاتق المضرور، إلّا أنّ القضاء يتساهل في هذا الصّدد ويقيم قرينة المضرور، إذا كان من شأن هذا الخطأ أن يحدث عادة مثل هذا القرار، وعلى المسؤول نفي هذه القرينة، فمتى أثبت المضّرور الخطأ والضّرر كان من شأن ذلك الخطأ أن يحدث عادة هذا الضّرر فإنّ القرينة على توافر علاقة السّببيّة بينهما تقوم لصالح المضرور، وللمسؤول نقض هذه القرينة بإثبات أن الضّرر قد ينشأ عن سبب أجنبي لا يد له فيه[1].

وقيام رابطة السّببيّة بين الخطأ والضّرر هو من مسائل الواقع الّتي تستقل بها محكمة الموضوع بشرط أن تورد الأسباب المؤديّة إلى ما انتهت إليه.

ومما لاشك فيه أنّ وسائل الإثبات الحديثة ستلعب دورا هامّا وحاسما في هذا الصّدد ولعلّ أبرزها، المصفرات الفيلمية Microfilm، حيث يتمّ تصوير المسندات وتصغيرها وتحزينها واسترجاعها في الوقت المناسب، وتقديم صور منها، وهناك ذاكرات الحاسبات

[1] – محمد حسين منصور، المرجع السابق، ص.407.

الآليّة التّي يتمّ التّعبير عنها بمخرجات ودعامات معينة، وأسطوانات الفيديو والشّرائط الممغنطة[1].

وتظهر أهميّة المحرّرات الإلكترونيّة والتّوقيع الإلكتروني كأدّلة إثبات المعاملات في المجال الإلكتروني، وبصفة خاصّة يصدر عمليات البنوك والوفاء النّقدي، وهي تأخذ طابع الشّفرات السّريّة حيث تتكوّن من حروف أو أرقام أو رموز أو إشارات، ذات طابع منفرد تسمح بتحديد الشّخص صاحبها وتميّزه عن غيره، وظهرت وسائل أخرى حديثة لتمييز الأشّخاص بدلا من التّوقيعات مثل بصمة قرنية العين وبصمة الصّوت والشّفاه وتحليل الحامض النّووي.

ويقتضي قبول تلك المعطيات التّقنيّة الحديثة في الإثبات تعديلا تشريعيا[2] ولا شك أنّ التقدّم العلمي حافز هام لتطوير قانون الإثبات والتّوسيع في أعمال الخبرة، الاهتمام الكبير بالبحث عن الحقيقة الموضوعيّة من خلال استخدام الوسائل العلميّة الجديدة ولاشك أنّ للقضاء دورا هامّا في قبول تلك الوسائط وإضفاء الحجيّة عليها بقدر ما تحمله من يقين والدّلالة على الحقيقة وانتفاء شبهة التّزوير أو التّلاعب بصددها.

ولقاضي الموضوع السّلطة المطلقة في استنباط القرائن القضائيّة الّتي يعتمد عليها في تكوين قناعته، فلا رقابة عليه، فيما يتحصّل عليه من شهادة الشّهود، ولا فيما يتناوله من قرائن، وله أن يأخذ لما يطمئنّ إليه من دلائل تاركا ما عداه ولو كان محتملا متى أقام قضاءه على أسباب مشروعة.

وإذا كان من السّهل على القاضي أن يتبيّن الخطأ بنفسه فيما يتعلّق بالأعمال العاديّة، إلّا أنّ ذلك يبدو عسيرا بالنّسبة للأعمال والتّصرفات في المجال الإلكتروني، لذلك فعلى القاضي إمكانيّة الاستعانة بأهل الخبرة، فله أن يندب خبير أو أكثر للتحقّق من وقائع الدّعوى وإبداء الرّأي في المسألة الفنيّة التي يصعب عليه استقصاء مضمونها بنفسه.

وينبغي ملاحظة أنّ الخبير وإن كان يساعد القاضي في استنباط الخطأ، إلّا أنّه يستقلّ بالتّكييف القانوني للسّلوك الفنّي، لذلك فهو ليس ملزما بالأخذ برأي الخبراء، إذ قدّر

(1) - La loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J0 14 mars 2000).

(2)- Décret n° 2001. 277 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code cube et relatif à la signature électronique (J0 31 mars 2001 ;p.5070).

أنّه ظاهر الفساد أو أنّه يتعارض مع وقائع أخرى أكثر إقناعا من النّاحية القانونيّة، ولكن للقاضي أن يأخذ بتقارير الخبراء إذا اقتنع بأنّها واضحة الدّلالة على الخطأ.

ولا يلزم في القرينة المستمدّة من تقارير الخبراء أن تكون قاطعة الدّلالة على هذا الخطأ، بل يكفي أن تكون واضحة في التّدليل عليه[1].

الفرع الثّاني

التّعويض عن الضّرر الإلكتروني

يترتب على قيام المسؤوليّة التزام المسؤول بتعويض المضرور عن الضّرر الّذي لحقه، فالتّعويض هو جبر الضّرر الّذي يلحق المضرور، وتقدير التّعويض قد يتم مباشرة عن طريق المشرع وهو ما يعرف بالتّعويض القانوني، وقد يقدّر بالإتّفاق، وهو ما يصطلح عليه بالتّعويض الاتّفاقي وقد يتولّى القاضي تقديره، عند توافر شروط المسؤوليّة بالتّقدير اللّازم لجبر الضّرر.

كما قد يكون التّعويض عينيّا ويتمثّل في إعادة الحال إلى ما كانت عليه قبل وقوع العمل غير المشروع، فهو يزيل الضّرر النّاشئ عنه، ويجوز في بعض الظّروف أن يحكم القاضي بأداء أمر معيّن متّصل بالعمل غير المشروع كنشر الحكم في الصّحف على نفقه المحكوم عليه لتعويض ضحيّة القذف والسّب عن الضّرر الأدبي الّذي أصابه، وإن كان مثل هذا التّعويض لا هو بالعيني ولا هو بالنّقدي، ولكنه قد يكون أنسب ما تقتضيه الظّروف في بعض الصّور.

ويتعيّن على القاضي أن يحكم بذلك إذا كان هذا ممكنا وبناءا على طلب المضّرور والتّنفيذ العيني هو الأصل في المسؤوليّة العقديّة بصدد المعاملات الإلكترونيّة، حيث يلتزم

[1] – أخذا بمبدأ حرية القاضي في تكوين اقتناعه، فله أن يقبل جميع الأدلة التي يقدمها الخبير، وله أن يستبعد أي دليل لا يطمئن إليه، فلا وجود لأدلة مفروضة عليه.

المنتج أو مقدّم الخدمة بتنفيذ التزامه، مثل تقديم البرنامج المناسب أو السّلعة أو الخدمة المتّفق عليها أو إزالة الفيروس أو تقديم أسلوب التحصّن منه[1].

وقد يكون التّعويض بمقابل، وبصفة خاصّة في صورة نقديّة وهو الأنسب والأصل في مجال المسؤوليّة التّقصيريّة، حيث يتّفق وطبيعة الضّرر ويفضّله المضرور عادة في حالات الضّرر الأدبي والجسماني حيث يستحيل التّنفيذ العيني، وتلك هي الصّورة الغالبة في المسؤوليّة الإلكترونيّة عند اختراق الجهاز المعلوماتي أو تدميره أو التّعدي على حقوق الملكية الفكرية أو حقوق الشّخصيّة مثل إفشاء الأسرار أو المساس بالحقّ في الخصوصيّة، والمساس بسمعة المشروع أو الشّخص عبر صفحات الويب، وقد يرى القاضي بالإضافة إلى التعّويض النّقدي إلزام المسؤول بنشر تصحيح أو اعتذار بنفس الطّريقة الّتي تمّ بها التّعدي.

ويشمل التّعويض كلّ ما لحق المضرور من خسارة، وما فاته من كسب بالإضافة إلى تعويض الضّرر الأدبي، كما يحيط التّعويض بكل الضّرر المباشر، دون تفرقه بين الضّرر المتوقّع وغير المتوقّع، فكلاهما يوجب التّعويض عنه، بخلاف الحال في المسؤوليّة العقديّة.

إنّ الهدف من المسؤوليّة المدنيّة هو جبر الضّرر، وذلك بإعادة المضرور إلى الوضع الّذي كان عليه قبل حدوث الضّرر، أي إعادة التّوازن الّذي اختلّ نتيجة للضّرر، وذلك على نفقة المسؤول، ويتحقّق ذلك بالتّعويض الكامل للضّرر، فالتّعويض يجب ألّا يتجاوز قدر الضرر من جهة، وألا يقل عنه من جهة أخرى.

ولا يوجد في القانون نصّ معيّن يلزم باتّباع معايير معيّنة لتقدير التّعويض، لذلك فلقاضي الموضوع السّلطة التّامة في تقديره، بشرط أن يكون التّقدير قائما على أسس مشروعة لها ما يبرّرها، ويجوز للمحكمة القضاء بتعويض إجمالي عن كافّة عناصر الضّرر، دون تحديد ما يخصّ كلّ عنصر على حدا.

مثال ذلك إلزام المنتج بإزالة الفيروس من البرنامج، وتحمّل تكاليف إدخال البيانات الّتي تمّ مسحها منه، بالإضافة إلى التّعويض عن كلّ ما أصابه من ضرر وما فاته من كسب نتيجة لإصابته بالفيروس، وعلى القاضي أن يراعي في ذلك الظّروف الملابسة

[1] – هناك صعوبة بالنّسبة للتّعويض المدني عن ارتكاب أحد جرائم الإنترنيت حيث يرجع في ذلك لأحكام القانون الدّولي الخاصّ وما تثيره من صعوبات واتجاهات فقهيّة وتشريعيّة متعارضة.

للمضرور كمهنته وموارده ومدى تأثير الإصابة عليه، وطبقا لمصادر دخله وإمكانيّاته الاقتصاديّة.

وتبدوا أهميّة ذلك في مجال التّعويض عن الضّرر الأدبي الّذي يتفاوت تقديره بحسب الوضع المادّي والاجتماعي للمضرور، كما في حالة اختراق الجهاز المعلوماتي للبنك والتّلاعب بحساباته والتّأثير البالغ لذلك على مركزه المالي وسمعته وثقة العملاء فيه[1].

إذا كان الحقّ في التّعويض أيّ الحقّ في إصلاح الضّرر ينشأ منذ استكمال أركان المسؤوليّة وبصفة خاصّة منذ وقوع الضّرر، إلّا أنّ هذا الحقّ لا يتحدّد إلّا بصدور حكم القاضي، فهذا الحكم لا ينشئ الحقّ بل يكشف عنه، فهو الّذي يحدّد عناصره وطبيعته ويجعله مقوما بالنّقد.

ويثير تقدير التّعويض عن الضّرر الإلكتروني، أحيانا، صعوبات خاصّة فيما يتعلّق بالوقت الّذي يتمّ فيه هذا التّقدير، إذ أنّ الضّرر الواقع قد يكون متغيّرا وقد لا يتيسّر تعيين مداه تعيينا نهائيا وقت النّطق بالحكم.

لذلك فمن المقرّر أنّه إذا لم يتيّسر للقاضي وقت الحكم أن يعيّن مدى التّعويض تعيينا نهائيا، فله أن يحتفظ للمضرور بالحقّ في أن يطالب خلال مّدة معينة بإعادة النّظر في تقديره.

وإذا كان الضّرر متغيّرا فإنّه يتعيّن على القاضي النّظر فيه لا كما كان عندما وقع، بل كما صار إليه عند الحكم، مراعيا التّغيير في الضّرر ذاته، من زيادة راجع أصلها إلى خطأ المسؤول أو نقص كائنا ما كان سببه، ومراعيا كذلك التّغيير في قيمة الضّرر بارتفاع ثمن النّقد وانخفاضه وبزيادة أسعار المواد اللّازمة لإصلاح الضّرر أو نقصها، ذلك أنّ الزّيادة في ذات الضّرر التي يرجع أصلها إلى الخطأ والنّقص أيّا كان غير منقطعي الصّلة به، أمّا التّغيير في قيمة الضّرر فليس تغييرا في الضّرر ذاته، فحقّ المضرور وإن كان ينشأ من يوم تحقق الضّرر إلّا أنّ تجسيده في حقّ دائنيه مقدّر بالنّقد تقديرا دقيقا لا يتمّ إلّا من يوم الحكم[2].

---

[1] – محمد حسين منصور، المرجع السابق، ص.412.

[2] – المرجع نفسه، ص.413.

الفصل الثّاني

وسائل حماية الحياة الشّخصيّة في مجال الانترنت

إنّ الخصوصيّة هي أحد حقوق الإنسان الرّئيسية التي تتعلّق بكرامته وبقيم ماديّة ومعنويّة أخرى، وقد أصبح الحقّ في الخصوصيّة واحدا من أهم حقوق الإنسان في العصر الحديث وجرى الاعتراف بالخصوصيّة في ثقافات وأنظمة غالبية الدول، فجرت حمايتها في الإعلان العالمي لحقوق الإنسان، وفي غالبية اتفاقيّات حقوق الإنسان الدولية والإقليميّة وفي معظم الدّساتير الحديثة، وحتىّ في الدّول التي لم تتضمن دساتيرها أو قوانينها اعترافا بالخصوصيّة، فإنّ المحاكم فيها قد أقرّت هذا الحق استنادا إلى الاتفاقيّات الدوليّة التي اعترفت بهذا الحق.

ومع شيوع استخدام شبكة الإنترنيت التي تشكوا نقصا فادحا في مستوى الأمن الفعلي فيها، نتيجة أسباب متعدّدة أبرزها أنّها كشبكة دولية لا تخضع لآيّة رقابة ولائيّة للسّلطة المركزيّة التي تدير التبادل المعلوماتي الحاصل بين مئات الملايين من المستخدمين المنتشرين حول العالم أو تراقبه، برزت حاجة المتعاملين في شبكة الإنترنيت، لاسيما الاختصاصيّن منهم إلى ابتكار وسائل تكنولوجيّة متطوّرة – إلى جانب القانون تساعد على تأمين وظائف الأمن والسّريّة والإثبات والفعلية للكثير من البيانات الحساسة المتبادلة.

لكن سرعان ما جوبهت هذه الوسائل التكنولوجية باعتراضات شديدة ، قد تؤدي مستقبلا إلى حضر البعض منها كّليا على الشّبكة[1].

وقد سبق وأن عالجنا في الفصل الأول مفهوم الحق في الحياة الشخصية وصورها لذلك سنعمد في هذا الفصل إلى معالجة وسائل حماية الحياة الشخصية من مخاطر المعلوماتية وذلك من خلال مبحثين أولهما النظام القانوني لحماية البيانات الشخصية في مجال المعلوماتية وثانيهما، الوسائل التقنية والتنظيمية لحماية الحياة الشخصية من مخاطر المعلوماتية.

[1] – بوليون أنطونيوس أيوب ، المرجع السابق، ص، 219–220.

المبحث الأول

النّظام القانوني لحماية البيانات الشّخصية من مخاطر الانترنت

تختلف القوانين السّائدة من بلد إلى أخر بشكل كبير، فقوانين بعض الدول الأوروبيّة مثل هولندا تسمح بتعاطي المخدرات، فيما تعتبر دول أخرى هذا الأمر غير مشروع ومخالف للقانون وتقرّر العقوبات المناسبة له، وتصنّف عدد كبير من بلدان العالم القمار ضمن الأمور المشروعة، فيما تعدّه بلدان أخرى مخالفا للقانون.

وإذا كان بالإمكان لبلد ما أن يطبّق قوانينه في إطار حدوده الجغرافيّة، فالأمر مختلف بالّنسبة للجريمة في فضاء الانترنيت حيث لا حدود جغرافية بين الدول.

ولذلك فالحل في قانون دولي يصدر في صورة اتفاقية دولية، ويمثل الحد الأدنى لمتطلبات كل دولة حتى يتم مواجهة ظاهرة الجريمة في فضاء الانترنيت ولذلك يرى الخبراء في مجال الانترنيت المتعلّقة بالمساس بالحياة الشّخصية أنّ الطّابع الدولي لمتطلبات فضاء الانترنيت يتطلّب تطوير استراتيجيات جديدة من أجل مكافحة النّشاط الإجرامي خاصة في جانب اخر من العالم، ذلك أنّ الجريمة العابرة للحدود عبر الانترنيت تتطوّر وتتزايد بسرعة، وقد يكون من أسباب ذلك الاختلافات الكبيرة في الأنظمة القانونية والقيم والأولويّات على مستوى العالم والصّورة المثلى لذلك التّعاون الدولي يكون في صورة اتفاقية دولية في هذا الصدد.

بالإضافة إلى دعوة كلّ دولة على حدى إلى تجريم أنشطة مواطنيها غير المشروعة في مجال الانترنيت حتى ما دعيت الدّولة للاشتراك في معاهدة أو اتفاقية دولية أو التصديق عليها تكون مهيأة لمثل ذلك، سيما وأنّ جريمة الانترنيت جريمة لا تعرف الحدود الدّولية[1].

ومن ناحية أخرى يمكن تعزيز العلاقات الدّولية في وضع قوانين جزائية لحماية الحياة الشّخصية وهذا ما سنتطرق إليه من خلال مطلبين: أوّلهما: مبادئ حماية البيانات الشّخصية من مخاطر الانترنت وثانيهما: التحدّيات القانونيّة لضبط أدلة جرائم الاعتداء على الحياة الشّخصية عن طريق تفتيش شبكة الانترنيت.

---

[1] – عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنيت، د،ط، دار الكتب القانونية، مصر ، 2007.

المطلب الأول

مبادئ حماية البيانات الشّخصية من مخاطر الانترنت

بما أنّ صور انتهاك الخصوصية في شبكة لا تتمتع بأمان كامل أو مطلق لسرّيّة ما ينقل عبرها من بيانات، فإنّ إمكانية مراقبة واعتراض وتفريغ الرّسائل المتبادلة عن طريق البريد الالكتروني والتّوصل بطريق غير مشروع إلى الملفّات بيانات تخص الآخرين، أصبح عرضة للعديد من الانتهاكات، مما يثير التّساؤل حول الجهود المبذولة لموجهة خطر انتهاك خصوصيّات الإفراد، والتي أصبحت تزداد بازدياد مستخدمي ومشتركي شبكة الانترنيت[1].

كما أنّ مختلف التّشريعات لم تتّفق على طريقة موحّدة لحماية الحياة الشّخصيّة ضمنيا، فمنها من أفرد قوانين خاصة بها وأخرى لم تفاعل واكتفت بالنّصوص القائمة في القوانين التّقليدية.

ولتناول موقف التّشريعات بخصوص هذه المسألة سنعرض في الفرع الأوّل، التدابير التّشريعية الغربيّة لحماية البيانات الشّخصيّة من مخاطر الانترنت ثم التدابير التّشريعيّة العربيّة لحماية البيانات الشّخصيّة من مخاطر الانترنت في الفرع الثاني.

الفرع الأول

التّدابير التشريعية الغربيّة لحماية البيانات الشّخصيّة من مخاطر الانترنت

أمام كل المخاطر والتّعدّيات التي ولّدتها تقنيّة الانترنت، نرى أنّ الدّراسات القانونيّة الأكاديمية التي عنيّت بالخصوصيّة وبحقوق الإنسان في التّطورات التكنولوجيّة محدودة بشكل عام.

ويمكن القول أنّ نهاية الستّينات والسّبعينات من القرن الماضي شهدت انطلاق مثل هذه الدّراسات وأنّ هذه الفترة تحديدا هي التي أثير فيها لأوّل مرة وبشكل متزايد مفهوم خصوصيّة المعلومات[2].

---

(1) - محمد أمين أحمد الشوابكة، المرجع السابق، ص، 27.

(2) - بوليون أنطونيوس أيوب، المرجع السابق، ص، 308.

ومن خلاصة هذه الدّراسات الأكاديمية في الفترة المشار إليها يمكن القول أنّ الخصوصيّة من حيث مفهومها جرى التعامل معها كحق لمنع إساءة استخدام الحكومة للبيانات التي يصار لمعالجتها آليّا أو الكترونيّا أو تقييد استخدامها وفق القانون فقط.

ففي معظم الدّول الغربيّة جرى تطوير هذه الفكرة ضمن مجموعة شاملة من مبادئ السّلوك والممارسات المقبولة، أهمّها تأكيد الاستخدام العادل والمنصف للبيانات الشّخصية، وتقييد وتضييق أغراض استخدام البيانات وحصر الاستخدام في غرض الجمع، ففي فرنسا أصدر المشّرع القانون رقم 17 لسنة 1978 الخاص بالمعالجة الآلية للبيانات والحرّيات، وتضمّن الباب الأوّل من ذلك القانون مجموعة من المبادئ القانونيّة التي أشارت إلى أنّ المعالجة الالكترونيّة للبيانات" يجب أن تكون لخدمة المواطن فقط، ولا يجوز أن تتضمّن اعتداءات على شخصيته أو حياته الخاصة وحرّياته، وفي الباب الثّاني من ذلك القانون انشأ ما أطلقت عليه اللّجنة القومية الخاصة لمراقبة تنفيذ أحكام هذا القانون ووجوب استشارة اللّجنة قبل معالجة البيانات، وتطبيقا لذلك قضت محكمة Nantes بتاريخ 1985/12/16 بإدانة شخص قام بإجراء معالجة الكترونيّة للبيانات الشّخصية دون الإخطار السّابق لهذه اللّجنة[1]. بالإضافة إلى المعالجة التّشريعية في ميدان حماية البيانات في ولاية هينس (ألمانيا)، لكن هذه المعالجة لا تعدّ قانونا متكاملا لاعتبارات عديدة أهمّها أنّه ليس قانون دولة، وقد تبعه سن أوّل قانون وطني متكامل في السّويد عام 1973، ثمّ الولايات المتّحدة الأمريكيّة عام 1974، ثم في ألمانيا على المستوى الفيدرالي عام 1977، وفي عام 1981 وضع مجلس أوروبا اتفاقيّة حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية ووضعت كذلك منظّمة التعاون الاقتصادي والتّنمية دليلا إرشاديا لحماية الخصوصيّة ونقل البيانات الخاصة، والذي قرّر مجموعة قواعد تحكم عمليات المعالجة الالكترونيّة للبيانات وتهدف إلى تأمين حمايتها في كلّ مراحل الجمع والتخزين والمعالجة والنّشر.

ثمّ وفي خطوة متطوّرة على المستوى التّشريعي الإقليمي أصدر الاتحاد الأوربّي الأمر التّشريعي لعام 1995 الخاص بحماية البيانات ونقلها عبر الحدود، الذي مثّل مرحلة جديدة في إعادة تنظيم خصوصيّة المعلومات، وهذا ما دفع العديد من دول أوروبّا والعالم إلى وضع

(1) – محمود أحمد عبابنة ، المرجع السابق ، ص، 76.

تشريعات جديدة أو تطوير تشريعاتها القائمة في هذا الحقل، سواء الدّستورية أو القانونيّة، نظرا لما تضمّنه هذا الأمر التّشريعي من معايير في حقل نقل البيانات عبر الحدود.

الفرع الثّاني

التدابير التشريعية العربيّة لحماية البيانات الشّخصية من مخاطر الانترنت

نظرا لأنّه يوما بعد يوم تّتجه جميع دول العالم نحو تأمين النّظم المعلوماتيّة من ناحية الاختراق وسرقة البيانات وإفشاء الأسرار والاعتداء على الحياة الخاصة والبرمجيات ونشطة التجسّس وتحريف وتدمير البيانات باستخدام الفيروسات وأنشطة تعطيل الأنظمة المعلوماتية عبر هجمات القراصنة واعتداءاتهم واختراقاتهم للنظم والمواقع، كل ذلك من أجل منع الاعتداء على المعلوماتية والبيانات الموجودة داخل النظام المعلوماتي والمنقولة عبر الشّبكات العالميّة[1].

ويقع اختيارنا على الدول العربيّة كي نعالج بعضا من تجاربها نتيجة أنّ الثورة المعلوماتيّة في هذه الدّول مستحبّة ومستحدثة وبدأت تداهم كل مناحي الحياة، وعلى سبيل المثال نذكر بعض التّجارب العربيّة:

أوّلا: التّجربة المصريّة

مصر على سبيل المثال لا الحصر لم تعمل على سن قوانين جديدة خاصة بها في هذا المجال ولم تقم حتى بتعديل ما لديها من قوانين جديدة تستوعب المستجدّات الإجراميّة[2].

ولقد جاء تأسيس الجمعية المصريّة لمكافحة جرائم المعلوماتيّة والانترنيت كبداية لدعوة المؤتمر التّأسيسي لجمعيات ومنظمات قانون الانترنيت من جانب نخبة من القضاة ووكلاء النّائب العام والمحامون والمحاسبون والمصرفيّون والإعلاميّون ومهندسي تكنولوجيا

---

[1] - أحمد خليفة الملط، الجرائم المعلوماتيّة (دراسة مقارنة)، د،ط، دار الفكر الجامعي، مصر، 2005، ص، 178.

[2] - منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنيت والحاسب الآلي و وسائل مكافحتها، د.ط، دار الفكر الجامعي، مصر، 2005.

المعلومات والاتصالات، كما تعتبر الجمعيّة منظمة غير حكوميّة خاضعة للقانون المصري ومشهرة تحت رقم 2176 لسنة 2005، وصدر قرار إشهارها بتاريخ 2005/08/05[1].

ومن المعروف أنّ المشرّع المصري لم يصدر قانون خاص بالجرائم المعلوماتيّة، بل إنّه لجأ في بعض القوانين والتّشريعات الخاصة إلى إضافة بعض المواد التي تهمّ البيانات كما هو الحال في قانون الحماية المدنيّة الجديد رقم 143 لسنة 1994، وتعديل بعض أحكام القانون رقم 354 لسنة 1954 الخاص بحماية حق المؤلّف[2].

وقد أضاف المشرّع المادّة: 309 مكرر إلى قانون العقوبات بموجب القانون رقم(37) لسنة 1982 والتي تعاقب بالحبس مدّة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، كذلك أضاف المشرّع المصري جريمة جديدة ضمّنها المادتين 21-22 من القانون رقم(92) لسنة 1992 بشأن تنظيم سلطة الصّحافة حيث جاء فيها عقاب الصحفي الذي يتعرض للحياة الشّخصية للمواطنين وفرض عقوبة الحبس سنة والغرامة التي لا تقل من 5000 جنيه ولا تزيد عن 13000 جنيه أو بأحدهما[3].

كما نجد القانون رقم 10 لسنة 2003 المتعلّق بتنظيم الاتّصالات وقانون حماية الملكية الفكريّة الذي ينص في المادة 140 منه على حماية برنامج الحاسوب الآلي[4].

ثمّ صدور القانون المصري رقم 15 لسنة 2004 في شأن التوقيع الالكتروني ورتب عقوبة جنائية لأي شخص يسيء استخدام البيانات الاسميّة أو يقوم بنشرها متى كانت تتعلق بالتّوقيع الالكتروني وذلك بدون أي وجه حق أو بدون رضاء صاحب الشأن نفسه[5].

ثانيا: التّجربة التّونسية

أفرد المشرّع التّونسي حماية خاصة للمعطيات الشّخصيّة في مواجهة التطور التّقني في المواد من (38-42) من قانون التّجارة الالكترونيّة لعام 2000، وفرض عقوبات أصليّة وعقوبات تكميليّة على الأفعال التي تقع بالمخالفة لتلك المواد، فتنص المادّة 38 على أنّه:

---

(1) - عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت (الجرائم الالكترونية)، دراسة مقارنة في النّظام القانوني لمكافحة جرائم المعلوماتيّة والانترنيت مع الإشارة إلى جهود مكافحتها محليا و عربيا و دوليا، ط1، منشورات الحلبي الحقوقية لبنان 2007.

(2) - أحمد خليفة الملط ، المرجع نفسه، ص، 182

(3) - محمود أحمد عبابنة ، المرجع السّابق، ص، 79-80.

(4) - زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى للطباعة والنّشر والتّوزيع، الجزائر، 2011.

(5) - عبد الفتاح بيومي حجازي ، المرجع السابق، ص، 668.

"لا يمكن لمزوّد خدمات المصادقة الالكترونيّة معالجة المعطيات الشّخصيّة إلاّ بعد موافقة صاحب الشهادة المعني" و تنص المادّة 39 على أنّه: "باستثناء موافقة صاحب الشّهادة لا يمكن لمزوّد الخدمات المصادقة الالكترونيّة أو لأحد أعوانه جمع المعلومات الخاصّة بصاحب الشّهادة إلاّ ما كان منها ضروري لإبرام العقد وتحديد محتواه وتنفيذه وإعداد وإصدار الفاتورة، لا يمكن استعمال المعطيات المجمّعة طبقا للفقرة الاولى من هذا الفصل لغير الغاية المذكورة أعلاه من قبل المزوّد أو غيره إلاّ اذا تم اعلام صاحب الشّهادة بذلك ولم يعارضه[1].

وتنص المادّة 40 على أنه: "يمنع على مستعملي المعطيات الشّخصيّة المجمّعة طبقا للفصل 39 من هذا القانون، إرسال الوثائق الالكترونية إلى صاحب الشّهادة الذي يرفض صراحة قبولها".

ويتعيّن على صاحب الشّهادة إعلام الوكالة الوطنيّة للمصادقة الالكترونيّة باعتراضه بواسطة رسالة مضمونة الوصول مع اعلام بالبلوغ، ويعتبر هذا الاعلام قرينة قاطعة على معرفة كل المزوّدين والغير لهذا الاعتراض.

أمّا المادّة (41) فتنص على أنّه "يتعيّن على مزوّد خدمات المصادقة الالكترونيّة، قبل كل معالجة للمعلومات الشّخصيّة، إعلام صاحب الشّهادة بواسطة إشعار خاص بالإجراءات المتّبعة في مجال حماية المعطيات الشّخصيّة.

وكذلك تنص المادّة (42) على أنّه "يمكن لصاحب الشّهادة في كل وقت بطلب ممضي بخطّ اليد أو الكترونيا النفاذ إلى المعلومات الشّخصيّة المتعلّقة به وتعديلها، ويشمل حق النّفاذ والتّعديل الدخول على جميع المعطيات الشّخصية المتعلّقة بصاحب الشهادة.

ويتعيّن على المزوّد وضع الإمكانيات التقنيّة اللاّزمة لتمكين صاحب الشّهادة من إرسال مطلبه الممضي لتعديل المعلومات أو فسخها بطريقة الكترونية[2].

---

[1] - علي جبار الحسيناوي، جرائم الحاسوب و الانترنيت، د.ط، دار اليازوري العلمية للنّشر والتوزيع، الأردن، 2009، ص، 171.

[2] - محمد أمين الشوابكة، جرائم الحاسوب و الانترنيت " الجريمة المعلوماتية "، ط1، الإصدار الثالث، دار الثقافة للنشر و التوزيع الأردن، 2009، ص، 82-83 .

كما يحدّد القانون التونسي الخاص بالمبادلات والتّجارة الالكترونيّة رقم 83 والمؤرّخ في 09 أوت 2000 بعض الإحكام الخاصة بجرائم المعلوماتية والانترنيت[1].

فالفصل 48 من القانون المشار اليه ينص على أنه يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصيّة متعلّقة بإمضاء غيره بالسّجن لمدة تتراوح بين 06 أشهر وعامين وبخطيّة تتراوح من 1000 أو 10000 دينار أو لأحدى هاتين العقوبتين.

أما الفصل 52 فينص على أن يعاقب طبقا لأحكام الفصل 254 من المجلّة الجنائية مزوّد خدمات المصادقة الالكترونيّة وأعوانه الذين يفشون أو يبحثون أو يشاركون في افشاء المعلومات التي عهدت في اطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشّهادة كتابيا أو الكترونيا في نشرها أو الاعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل[2].

ثالثا: التّجربة الجزائريّة

إنّ الجزائر لا تزال متأخّرة في مواكبة التطوّر الحاصل في المجال المعلوماتي فهي تحتل المرتبة 121 ضمن البلدان الأعضاء في منظّمة الأمم المتحدة التي شملها المسح والبالغ عددها 192 دولة، هذا فضلا عن مشروع انجاز بطاقة التعريف الالكترونية[3].

ظهور المعلوماتيّة و تطبيقاتها المتعدّدة أدى إلى بروز مشاكل قانونيّة جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية ولما كان القاضي الجزائي مقيّد عند نظره في الدّعوى الجنائيّة بمبدأ شرعيّة الجرائم فإنّه لن يستطيع أن يجرّم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة، وعلى مستوى عال من الخطورة الإجرامية.

إن البحث عن حماية الحق في الحياة الخاصة في القانون الجزائري، يستوجب الإشارة إلى حماية الدّستور لهذا الحق باعتباره قمّة التسلسل الهرمي في التنظيم الداخلي، وهذا ما يعدّ وسيلة فعّالة لضمان حمايته، ولقد سار المشرّع في وضع الاحكام التشرّيعية التي

---

[1] - عبد الفتاح حجازي ، مقّدمة في التّجارة الالكترونيّة العربيّة ، الكتاب الأول ، شرح المبادلات والتّجارة الالكترونيّة التّونسي، دار الفكر الجامعي، مصر، 2004، ص 255.

[2]- عبد الله عبد الكريم عبد الله، المرجع السّابق، ص، 85-86

[3] - زبيحة زيدان، المرجع السابق، ص، 20-21.

تعالج مسألة حماية الحياة الخاصة بصورة تتفق مع نص الدّستور لصبغ صفة الشّرعيّة عليها استنادا الى المصالح الأساسية المشروعة العامّة منها والفردية، وسنقتصر في هذا المجال بما ورد في كل من قانون الإجراءات الجزائية وقانون العقوبات والقانون المدني وبعض القوانين الخاصّة.

1 – الحماية الدّستورية :

لقد كفل المؤسّس الدّستوري الجزائري حماية الحق في الحياة الخاصّة، بهدف وضع نظام للحياة الاجتماعيّة تصان فيه الكرامة الإنسانيّة، وتحمى فيه الأسرار وتستر فيه العورات، وتأكيدا للقيمة الدّستورية لهذا الحق، فقد حرص نص التّعديل الدّستوري لسنة 1996 على كفالتها وحمايتها، حيث اقرّ في الفصل الرابع تحت عنوان "الحقوق والحرّيات" بموجب نص الفقرة الأولى من المادّة 39 منه على أنّه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميهما القانون" وبهذا يكون هذا الحق قد ارتفع إلى مصاف الحقوق الدّستوريّة التي لا يجوز المساس بها سواء من قبل الدولة أو الافراد.

ولم يكتف المؤسّس الدّستوري بإقرار هذا المبدأ العام الذي أورده قي تلك الفقرة، بل أورد له بعض التّطبيقات، ومن ذلك ما نصّت عليه الفقرة الثّانية من نفس المادّة على أن "سرّيّة المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"[1].

2– الحماية التّشريعيّة:

إنّ إقرار الحق في الحياة الخاصّة كحق عام في الحقيقة استتبع التّدخل التّشريعي ليوفّر مستويات من الحماية الجزائية أو حماية تطبيقات معيّنة تتّصل بتكريس هذا الحق، وردع الاعتداءات التي تطاله.

أ– **قانون العقوبات:** نجد نصوص ومواد جزائية تعاقب صراحة على انتهاك الحق في الحياة الشخصية، وذلك في نص المادّة 303 مكرر من قانون العقوبات: "يعاقب بالحبس من ستة

[1] - بيو خلاف، تطور حماية الحياة الخاصة للعامل، مذكرة لنيل شهادة الماجستير في الحقوق، جامعة قاصدي مرباح، ورقلة ، 2011.

6 أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمّد المساس بحرمة الحياة الخاصة بالأشخاص، بأيّة تقنية كانت وذلك:

– بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرّيّة، بغير إذن صاحبها أو برضاه.

– بالتقاط او تسجيل أو نقل صور لشخص في مكان خاص، بغير إذن صاحبها أو برضاه.

ب– **في القانون المدني:** لم يفصل المشرّع الجزائري صراحة في مسألة الحق في الحياة الشّخصيّة على نحو ما فعل المشرع الفرنسي في المادة 09 من القانون المدني، غير أنّه اعترف صراحة بالحقوق الملازمة لشخصية الإنسان، فبالرجوع إلى المادة 47 من القانون المدني الجزائري نجد أنها تنص "لكل من وقع عليه الاعتداء غير مشروع في الحق من الحقوق الملازمة لشخصيّته، أن يطلب وقف هذا الاعتداء والتّعويض عما لحقه من ضرر" وإذا كانت هذه الحقوق اللصيقة بالشّخصيّة تشمل كذلك حرمة الحياة الشّخصيّة، فتعتبر هذه الأخيرة، حقّا بالضّرورة تتمتع بما تتمتع به الحقوق الاخرى من حماية.

ج– **في قانون الإعلام:** نصت المادة 03 منه على أنه "يمارس حق الإعلام بحرّية مع احترام الكرامة الشّخصيّة الإنسانية..." كما نصت المادة 36 فقرة 4 على أنه: "حق الوصول إلى مصادر الخبر لا يجيز للصحافي أن ينشر أو يفشي المعلومات التي من طبيعتها أن تمس بحقوق المواطن وحرّياته الدّستورية".

ونصّ المرسوم التّنفيذي رقم 98– 257 المتعلّق بشروط وضبط كيفيات إقامة خدمات الانترنيت واستغلالها في المادة 14/02 على أنه: "يلزم مقدم خدمات الانترنيت خلال ممارسته نشاطاته بما يلي: المحافظة على سرّية كل المعلومات المتعلّقة بحياة مشتركيه الخاصة، وعدم الإدلاء بها إلاّ في الحالات المنصوص عليها في القانون[1].

ومما سبق يمكن القول أنّ أغلب التّشريعات العربيّة لم تفرد قانونا خاصا حماية خصوصيّة الإنسان في جال الانترنت كما فعلت بعض التشريعات الغربيّة، بل تناثرت الاحكام التي تتعلق بالخصوصيّة في قوانين العقوبات والإجراءات والشّركات التّجارية وقوانين

[1] - المرسوم التنفيذي رقم 98–257، المؤرخ في 25 أوت 1998، المتعلق بشروط وضبط كيفيات إقامة خدمات الانترنيت و استغلاله، ج.ر عدد 63، الصادرة بتاريخ 26 أوت 1998.

الاتّصالات والبريد وبمجمل هذه النصوص لم نجد نصّا تشريعيا واحدا يتعلق بحماية الحياة الشّخصيّة من مخاطر الحاسب الآلي وبنوك المعلومات[1].

المطلب الثّاني

التحدّيات القانونيّة لضبط أدلّة جرائم الاعتداء على الحياة الشّخصيّة عن طريق تفتيش شبكة الانترنيت

في الجريمة الالكترونية يستطيع المجرم استعمال اسمه وأسماء أخرى لارتكاب نفس الجريمة التي كان قد ارتكبها عدّة مرات ومن الصّعوبة بمكان اكتشافه، حيث أصبح التعامل يتمّ بواسطة أرقام ومن الصّعب اكتشاف المعلومات المتوفّرة كبراهين، علما أنّه يمكن محوها بسهولة وعدم ترك أيّ دليل على هذه الجريمة مما يجعل التحرّيات أكثر صعوبة كما انه في الجرائم المتعلّقة بشبكات الانترنيت لا يتأذى أحد مباشرة من الناحية الجسديّة، وأنّ الفعل الإجرامي ينتهي بمجرد ادخال الاوامر عليه، لذلك لا نجد عند بعض المجرمين ما يسمى الشّعور بالذّنب بالإضافة إلى قصور النصوص القانونية المجرّمة لمثل هذه الأفعال التي تقع بواسطة شبكة الانترنيت[2].

ومن هنا سوف نتناول مطلبنا هذا في فرعين يخصّص الأوّل لدراسة كيفية الحصول على الدّليل الرقمي من الأجهزة والنّظم والشّبكات، ونتناول في الثاني المشكلات المتعلّقة بسلطات الاستدلال والتّحقيق في مجال التعدّي على الحياة الشّخصيّة.

الفرع الأوّل

كيفية الحصول على الدّليل الرّقمي من الأجهزة والنّظم والشّبكات

قد يكون مرتكب الجريمة الالكترونيّة أكثر فطنة وحذرا مما تتصوّره سلطات التحري والتحقيق، فيقوم بمسح البيانات أو اتلاف الاقراص الالكترونية أو زرع فيروسات أو برامج تدميريّة لإخفاء ومحو الدّليل الرّقمي حال إحساسه بالمداهمة، لذا وجب على رجال الضّبطية القضائية في مرحلة التّحرّي وقاض التّحقيق في مرحلة التّحقيق الابتدائي أن يتوخوا الحيطة وأن يكونوا أكثر دهاءا.

---

[1] - محمود أحمد عبابنة، المرجع السابق، ص، 80.

[2] - نعيم مغبغب، المرجع السابق، ص، 225.

ويتم الحصول على الدّليل الرّقمي بفحص الحاسوب والبيانات المادّية والمعنويّة وكذلك بالتّفتيش في مراسلات البريد الالكتروني وتعقب المرسل.

أوّلا : فحص الحاسوب و البيانات المادّية و المعنويّة المتّصلة به

إنّ مكوّنات الحاسب الآلي يصف عليها وصف الشيء المنقول وذلك على أساس أنّه بالإضافة إلى إمكانية نقل هذه المكوّنات من مكان إلى أخر، فإنّه يمكن نقل المكوّنات المعنويّة المتمثّلة في البيانات المعالجة الكترونيا أو المعلومات عن طريق ارسالها من حاسب إلى حواسيب أخرى عبر الانترنيت[1].

لذا قد تضطرّ جهة التحقيق إلى ضبط الحاسوب وحجزه، وإلى ضبط القطع الصّلبة المتّصلة به والبرمجيات المخزّنة فيه ومحاولة الحصول على الدّليل من خلالها وبذلك يتم فحص ما يلي:

1- فحص القرص الصّلب: (Disk Dure) يحتوي القرص الصّلب على مجموعة البيانات الرّقمية ذات الطابع الثنائي (1.0) ويمكن إجراء الفحص الكلّي أو الجزئي على القرص الصّلب، من أجل التّعرّف على محتوى البيانات، سواءا أكانت مكتوبة أو عبارة عن أصوات أو صور كما تتيح من خلالها استعراض ملفات النّسخ والتي تظهر كل الصّفحات التي تم تصفّحها حتىّ تاريخ قد يصل إلى ستة أشهر، وكل الملفّات التي قام مستخدم الجهاز بتنزيلها، وغيرها من الملفّات، وكذلك ما تم حذفه من بيانات وبرمجيات.

وفحص القرص الصّلب لا يعني ايلاء أهمّية خاصة لمادة القرص فهي لا تساوي شيئا بمعزل عن البرمجيات المخزّنة فيه، و عن حركة البيانات بحرية داخل القرص[2].

2- فحص البرمجيات: ويكون من خلال الفحص الدّاخلي والخارجي لبرامج البرمجيات، ففي الفحص الدّاخلي يتمّ التّأكّد من إعداد خطوات التّسلسل المنطقي وكتابة البرنامج بناءا عل

---

[1]- محمد فتحي محمد أنور عزت، تفتيش شبكة الانترنيت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبار (دراسة مقارنة)، د،ط، 2011،د.د.ن، ص 453.

[2] - عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص، 245.

هذه الطريقة، وبالتالي المقارنة بين النّسخة الأصلية والمقّلدة مما يعني قيام جريمة تقليد البرمجيات[1].

3 – فحص النظام المعلوماتي: من المعلوم أنّ الرّسالة الالكترونيّة ذات طابع خاص، لكنها لا تختلف عن الرّسالة الورقيّة من حيث أنّ مآلها من حيث حفضها أو الاستغناء عنها وإهمالها لكن ما يميّز الأولى (الرسالة الالكترونية) سواء المهملة أو المحفوظة يمكن الوصول إليها عن طريق صناديق البريد أو الملفّات المحفوظة أو الرجوع إلى سلة المهملات، فالتّحقيق الذي يجري بغرض ضبط المراسلات الالكترونيّة يكون أمام ثلاثة خيارات بعد الولوج الى البريد الالكتروني (Email)[2].

فبعد تحديد صندوق البريد الالكتروني للمتّهم المشكو منه يتمحور العمل حول ثلاث عناصر وهي: الوارد والصادر، الحفظ، وسلة المهملات فبذلك يمكن مراجعة قائمة الرّسائل التي وصلت المشكو منه من الوارد والعكس، وكذا الشأن بالنسبة للرّسائل المحفوظة أو المهملة[3].

وإذا كان الحاسوب يحتاج إلى كلمة مرور، فيجب فكّها قبل الشّروع في الفحص، علما أن بعض الانظمة أعدت لتقوم بتدمير نفسها ذاتيا إذا حاول أيّ مستخدم الولوج إلى نظام الجهاز بطرق ملتوية.

4 – فحص الطّابعة: الطّابعات الحديثة تتمتع بميزة تخزين أخر مجموعة من الصّفحات التي تمّ طباعتها حتىّ عدد معين، وإذا كانت تلك الملفّات قد تعرضت لأمر إلغاء فبرمجيات الاسترجاع المتخصّصة يمكنها الاستعانة بنظام الحاسوب لإعادتها وتحديد عدد النّسخ المطبوعة وتاريخ طباعتها وساعة الطّباعة، مما يساعد في التّحقيق ومعرفة المتهم ومواجهته بالدّلائل.

5– فحص المودام : يحتوي المودم هو الاخر رقم تم الاتصال به، وقد يحتوي على أرقام أخرى، ويمكن لرجال الضبطية القضائية أن يقوموا من أجل الحصول على الأدلة بفعل

---

(1) – خثير مسعود ، الحماية الجنائية لبرامج الكمبيوتر، (أساليب و ثغرات)، د ط، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2010، ص، 74.

(2) – يعرف بأنه: إرسال واستقبال الرسائل الالكترونية عن طريق شبكة الانترنيت.

(3) – زبيحة زيدان، الرجع السابق، ص، 128.

تمديد المودم الموصولة بجهاز المشتبه به إيصاله بجهازهم لكي يتم الحصول على المعلومات العميل الداخلية[1].

ثانيا: التفتيش في مراسلات البريد و تعقب المرسل

يعتبر البريد الالكتروني من أهم الوسائل الحديثة للاتّصال في مجال الانترنيت، وهو أكثر استخداما في هذا المجال نظرا لما يتسم به من سرعة ويسر في الاستخدام، بل يمكن القول أنّ البريد الالكتروني أضحى مجالا خصبا للرّبط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون عائق.

ولكن لم يسلم البريد الالكتروني والذي يعتبر المستودع الأساسي للأسرار الشّخصية في البيئة الافتراضية من الاقتحام من قبل مجرمي الانترنت بل يعتبر الميدان الخصب لتدخّلاتهم والفضاء الذي يجد فيه هواة الإجرام ظالتهم لما يوفره لهم من إمكانيات وتقنيات حديثة ومميزة[2].

ويتمتّع البريد الالكتروني أيضا بخدمة "قائمة التّراسل" وهو نظام تراسل جماعي يمنح صلاحيات بث رسالة إلى مجموعة من الاشخاص المسجّلين في هذه القائمة، ولا شك أن هذا النظام تم تطويره لتشجيع العمل الجماعي وتبادل الأفكار والخبرات.

1- الأصول القانونية المتبعة في تفتيش البريد الالكتروني:

يتمّ ضبط البريد الالكتروني الخاص بالضّحية كالأتي: يطلب المحقّق أو رجل الضّبطية القضائيّة من الضّحيّة الولوج إلى بريده باستخدام اسم المستخدم و كلمة السّر ثم يذهب إلى قائمة الاستقبال (Boite de Reception)، وينقر على الرّسالة التي تتضمّن الأسانيد الجارحة في جريمة التشهير أو عبارات السّب أو تشويه صورته أو سمعته، أو كلّ ما يتعلق بالحياة الشّخصيّة، ثم يقوم بطبع الرسالة بصورة تظهر صندوق العرض، وفيه اسم المرسل وعنوان بريده الالكتروني، وعنوان بريد الضّحية، وكذلك مادّة الرّسالة والمستند الالكتروني مادام عبّر عن فكرة وكان في الإمكان قراءته و إدراك معناه وفهم مضمونه فإنّه

[1] – عادل عزّام سقف الحيط، المرجع السابق، ص، 249.

[2] – زبيحة زيدان ، المرجع السابق ، ص، 160.

يعدّ محرّرا ومن ثم يحوز الحجّية وفقا لطبيعة الشّخص المنسوب إليه إصداره، ولمن وضع عليه توقيعه الالكتروني[1].

ويترتّب على اعتبار الرّسائل الالكترونيّة المتولّدة من البريد الالكتروني بمثابة رسائل شخصيّة، أنّه يجب حماية خصوصيتها، تماما كالمراسلات الورقيّة المغلقة والطّرود، فلا يجوز التّي نصّت عليها أو الاطّلاع على الأسرار التي تحتويها إلاّ بذات الطرق التي تنص عليها قوانين الإجراءات الجزائية، ولا يجوز للضّبطيّة القضائيّة دون إذن تفتيش من اختراق صندوق البريد الالكتروني أو الدخول إلى أنظمة الحاسوب، المخزّن فيه الرّسائل البريديّة الالكترونيّة، إلاّ بإتباع الإجراءات المنصوص عليها في القوانين الإجرائية، وبعد ضبط مادة الجريمة، يجري تتبّع مصدرها عن طريق تعقّب مسار بروتوكول الانترنيتIP ADRESSE التّابع للجهاز الذي أرسلت منه الرّسالة، وهو كالبصمة يعرف بها الجهاز في أيّ مدينة وأيّ حي بل في أيّ مقهى إنترنيت أو بيت أو مكتب.

2- تعقب الأفراد لمرسل رسائل البريد الالكتروني:

كلّ رسالة الكترونيّة يظهر فيها معلومات عامّة، مثل تاريخ إنشاء الرّسالة، وتاريخ تلقّيها وكذلك عنوان المرسل، وعنوان المرسل إليه، وهذه المعلومات ليست كافية لمعرفة المرسل، فمرسل الرّسالة بإمكانه إطلاق رسائله من حسابات بريد مسجّلة بأسماء وهميّة، كما هناك وسائل تتيح للمرسل أن يرسل رسالته دون أن يظهر فيها عنوان بريده الالكتروني الصّحيح لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الالكتروني.

وفيما يأتي تفصيل لخطوات متابعة البريد الالكتروني، المتضمن إزعاجات أو عبارات الذم والقدح أو تلطيخ سمعة وصورة الضحية، وما يتعلق بحياته الشخصية، وخطوات كشفه، وطلب وقف رسائله أو حجب الخدمة عنه من مزوّد الخدمة.

أ/ المعلومات المطلوبة للكشف عن المرسل :

كل جهاز حاسوب متّصل بشبكة الانترنيت له حتما رقم تعريف خاص به و يطلق على هذا الرقم IP Addresse أو بروتوكول الانترنيت، هذا الرقم أشبه ما يكون برقم

[1] – عادل عزام سقف الحيط، المرجع السابق، ص، 250-251.

الهاتف ويتخذ هيئة تتكون من مجموعة أرقام مفصولة بنقاط مثل23.041.973.10 أو 365.25.485.589، وعادة ما يكون هذا الرّقم متغيّرا، ورغم هذا التغيّير إلاّ أنّ مزوّد الخدمة يمكنه التّعرف على الجهاز الموصول بالبروتوكول عند معرفة الوقت الذي كان فيه الجهاز متصلا بالانترنيت، وتسهل عمليّة الكشف عن صاحب رقم**IP** عندما يكون متّصلا بالانترنيت من خلال شبكة محلية، مثل شبكات بعض الشّركات أو المؤسسات أو الجامعات، لأنّ أجهزة الحاسوب فيها تتّصل بالانترنيت باستخدام رقم غير متغير[1].

ب/ الكشف عن هويّة المرسل :

بعد التعرّف على رقم **IP** الخاص بالمرسل من حاشية المعلومات، يصبح من السهل الحصول على المزيد من المعلومات عن المرسل، وذلك بإدخال رقم**IP** في بعض المواقع التي تقوم بالكشف عن مصدر الرّسالة والمكان الجغرافي الذي أرسلت منه الرّسالة (البلد)، وكذلك عن مزوّد خدمة الانترنيت الذي يتعامل معه مرسل الرّسالة[2].

جـ/ الطلب من الجهة المزودة بالخدمة وقف الازعاجات:

ان تضمّنت الرّسائل البريديّة إزعاجا أو إعلانات ماجنة أو رسائل تضمّ عبارات قدحيّه وتمس بالشّرف والاعتبار، يمكن الحصول على المعلومات السابقة عن المرسل، بعد كتابة شكوى رسمية إلى الجهة المزوّدة بخدمة الانترنيت، وتزويدها بالمعلومات الأساسيّة مثل رقم IP الخاص بمرسل الرّسالة، ووقت إرسالها، ويشكل طريقة مبسطة لتعقب مرسلي البريد الالكتروني، ويقتضي التنويه هنا إلى إمكانية قيام قراصنة محترفين بالتّلاعب في حاشية معلومات البريد الالكتروني وإتّباعهم أساليب تجعل عملية الكشف عن أرقام IP الخاصة بهم صعبة بل معقّدة.

كما أن بعض الجهات المزوّدة بخدمة الانترنيت قد تستعين بشركات خارج بلدانها ومن ثم قد تظهر النتيجة أن الرّسالة من خارج بلد المرسل الفعلي، ومع ذلك، هناك وسائل أكثر تطورا لتعقب البريد الالكتروني تتجاوز تلك الثغرات.

---

[1] - عادل عزام سقف الحيط، المرجع السابق، ص، 256.

[2] – المرجع نفسه، ص، 257.

الفرع الثاني

المشكلات المتعلقة بسلطات الاستدلال والتحقيق

لا شك أن الجريمة المعلوماتية كغيرها من الجرائم الأخرى تمر بذات مراحل الاستدلال والتحقيق الجنائي المتكامل، وإجراء التحقيق الجنائي العام هي الركيزة في تحقيق جرائم الحاسب الآلي وجريمة التعدي على الحياة الشخصية عبر الانترنيت، وذلك من سماع الشهود ومعاينة وقبض وتفتيش واستجواب، ولكن إجراءات التحقيق الأخرى العملية والفنية والنفسية توقف استخدامها على ظروف كل جريمة على حدة مع مراعاة الخصوصية التي تتسم بها الجريمة المعلوماتية[1].

وهناك العديد من المشكلات والصّعوبات العملية والإجرائيّة التي تظهر عند ارتكاب أحد جرائم المساس بالحياة الشخصية عبر الانترنيت ومن بين هذه المشكلات نذكر:

أولا: صعوبة إثبات وقوع الجريمة

في الغالب من الأحيان يتم الفعل الإجرامي دون معرفة المجني عليه بحدوث اعتداء وقع عليه، ومثال ذلك أن يتم إدخال فيروس إلى جهازه عن طريق الاتصال بشبكة الانترنيت ويظل ذلك الفيروس داخله حتى لحظة معينة ثم يقوم بالنّشاط وتدمير البرامج وسرقة المعلومات الشّخصية والتجسّس عليها، فهنا المجني عليه لا يدري الوقت الذي تمّ فيه إصابته بالفيروس، بالإضافة إلى إمكانية تدمير الفيروس لنفسه بحيث لا يعرف نوعية الفيروس أو من قام بإدخاله[2].

ثانيا: صعوبات مصدرها الإحجام عن الإبلاغ

تبقى جريمة المساس بالحياة الشخصية عبر الانترنت مخفية ما لم يتم الإبلاغ عنها، ومن ثمّ عدم تحريك الدعوى الجنائية كما أنّ الصّعوبة التي تواجه أجهزة الأمن والمحقّقين هي أنّ هذه الجرائم لا تصل إلى علم السّلطات المعنيّة بالصورة العادية، كما هو الحال في الجريمة التقليدية، ذلك لصعوبة اكتشافها من قبل الأشخاص العاديين أو حتى الشركات

---

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص، 67.

[2] – عمرو عيسى الفقي ، المرجع السابق ، ص، 140.

والمؤسسات التي وقعت مجنيا عليها في هذه الجرائم، أو لأن هذه الجهات تحاول درأ الأثر السلبي للإبلاغ لما وقع لها و حرصا على ثقة العملاء[1].

ومن أجل تفعيل عملية الإبلاغ عن هذه الجريمة، ومن ثمة المساهمة بطريقة ايجابية في منع وقوعها أو سرعة تحصيل الدليل المتعلّق بها، ما طالب البعض به في الولايات المتّحدة الأمريكية، وذلك أن تتضمن القوانين المتعلّقة بجرائم الحاسب والمعلومات نصوصا تلزم موظفي الجهة المجني عليها أيّا كانت بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلّق بهذا المجال[2].

ثالثا: صعوبة التوصّل إلى الجاني

كثيرا ما يقوم الجاني بالدّخول إلى شبكة الانترنيت عن طريق مقاهي الانترنيت، الأمر الذي يصعّب التعرّف على موقعه، بالإضافة إلى إمكانية الدخول باستخدام اسم مستعار وبالتالي صعوبة التعرف عليه[3].

رابعا : صعوبة إلحاق العقوبة بالجاني المقيم بالخارج

الصّعوبة تكمن إذا تمّ ارتكاب الجريمة من شخص أجنبي مقيم في الخارج و وقعت الجريمة ببلد أخر، و بالتالي صعوبة الوصول إليه و إلحاق العقوبة به[4].

وبالتالي ضرورة تدخل الشّرطة الدولية الانتربول التي بدأت تهتم بمكافحة جرائم الانترنت بكافة أشكالها، وأنشأت لديها فرقة خاصة لهذا الغرض، هي على اتصال دائم بفرق مكافحة الجريمة المعلوماتية في أوروبا والولايات المتّحدة الأمريكية واستراليا إضافة إلى تبادل المعلومات حول كيفية اكتشاف هذا النّوع من الجرائم –الإبلاغ– وتعزيز الإجراءات الأمنية في مجال الجرائم التي تقع بواسطة الانترنيت والتي تمس بالحياة الشّخصيّة[5].

خامسا: صعوبة السّيطرة على أدلّة الجريمة

قد يقع أفراد الضّبطيّة القضائيّة حينما يتوجّهون للقبض على الجاني وبالتالي جمع أدلّة إثبات التّهمة ومنها جهاز الكمبيوتر المستخدم في الاتّصال بالشّبكة وبالتالي ما يحتوي

---

(1)– عبد الفتاح بيومي حجازي، المرجع السابق، ص، 68.

(2) – المرجع نفسه، ص، 75.

(3) – محمد أمين الرومي، المرجع السابق، ص، 140.

(4) – عمرو عيسى الفقي، المرجع السابق، ص، 91.

(5) – عب الفتاح بيومي حجازي، المرجع السابق، ص، 76.

عليه من برامج ومعلومات، في مشكلة معرفة الرّقم السري الذي بدونه لا يعمل جهاز الكمبيوتر، وفي هذه الحالة لا يمكن إجبارهم للمتهم على الإفشاء على الرقم السّري لأنّ ذلك يعدّ إجراءا غير قانوني، كذلك قد يتمكن الجاني من تدمير البيانات الموجودة والمخزّنة في لحظات قليلة أثناء إجراء التفتيش، وهنا تكون الصّعوبة في جمع الأدلّة الماديّة التي تثبت ارتكاب جرائم الانترنيت[1].

سادسا: تنازع القوانين الجنائيّة من حيث المكان وافتراض العلم بالقوانين

هناك مبادئ تحكم تطبيق القانون الجنائي ومنها مبدأ إقليميّة القانون الجنائي وشخصيّته و عينيّته و تثور المشكلة إذا ارتكب الفعل الإجرامي في الخارج ونتيجته تحقق ببلد أخر فأيّ القوانين الجنائيّة تنطبق؟، وقد يكون الفعل المرتكب بتلك الدّولة مباحا ولكنه يشكل جريمة في الدّولة التي حدثت بها النّتيجة لذلك فالشّخص الذي ينوي ارتكاب جريمة من جرائم المساس بالحياة الشّخصيّة عبر الانترنيت، أمر يخضع معه لقانون تلك الدّولة التي حدثت النّتيجة الإجرامية فيها، الأمر الذي يجد الشخص نفسه خاضعا لقانون دولة لا يعرف عنه شيئا، وهو ما يعد أمرا غير مقبول[2].

سابعا: صعوبات مصدرها نقص خبرة سلطات الاستدلال والتحقيق

كذلك من الصّعوبات التي تواجه عملية استخلاص الدّليل في جريمة التّعدي على الحياة الشّخصيّة في مجال الانترنت، نقص الخبرة لدى رجال الضّبط القضائي أو أجهزة الأمن بصفة عامّة، وكذلك في القضاة، سواء في مرحلة الاتّهام أو التّحقيق الابتدائي، وذلك فيما يتعلّق بثقافة الحاسب الآلي والإلمام بعناصر الجرائم المعلوماتية و كيفية التعامل معها، وذلك على الأقل في البلدان العربيّة كونها متأخّرة في تجربة الاعتماد على الحاسب الآلي والانترنيت، بالإضافة إلى عدم مواكبة الحركة التّشريعية أو الثقافة الأمنيّة أو القانونية مع سرعة انتشار الجريمة المعلوماتية وسرعة تقدّم التقنيّة.

---

[1] – عمرو عيسى الفقي، المرجع السابق، ص، 92-93

[2] – محمد أمين الرومي، المرجع السابق، ص، 142.

وهذا الفارق في التّقدم والتّطور ينعكس سلبا على فنّيّة إجراء التّحقيقات في الدّعوى الجنائية عن الجريمة المهدّدة للحياة الشخصية عبر الانترنت.

ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات الأمن وجهات التّحقيق والادّعاء والحكم في شأن هذه الجرائم [1].

وكخطوة أولى يتعيّن منح صفة الضّبطية القضائيّة للعاملين في مجال المعلومات الأمنيّة سواء أكانوا من أفراد الأمن أو في القطاعات ذات العلاقة بجهاز الحاسب الآلي وسواء كانوا فنّيّين أو خبراء، وذلك من أجل التّمكن من ضبط جرائم الانترنت في نطاق عملهم، ولكن المشكلة لا تثور في منح صفة الضّبطيّة، وإنّما نقص الثّقافة في جريمة الانترنت واكتشافها والتوصّل إلى فاعليها وملاحقتهم قضائيا، لا يتطلب فقط الإلمام بأصول البحث الجنائي أو قواعد التحقيق القانونية، فذلك أمر مفترض لكن يجب الإلمام بأصول التحقيق الجنائي الفنّي في الجرائم التقليديّة بالإضافة إلى مهارات خاصة تسمح باستيعاب تقنيّات الحاسب الآلي من حيث برامجه، وأنظمته وطبيعة الجريمة الواقعة بواسطته.

ونخلص مما سبق أنه يجب على كافة أجهزة التّحقيق مواكبة المتغيّرات التكنولوجيّة في مجال برامج طموحة للتدريب، وإدارات متخصصة للاستدلال في جرائم الانترنت، وأجهزة تحقيق متخصصة في مثل هذه الجرائم[2].

---

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص، 82.

[2] – المرجع نفسه، ص، 91.

المبحث الثّاني

الوسائل التّقنيّة والتّنظيميّة لحماية الحياة الشخصيّة من مخاطر الانترنت

إنّ تطبيقات تقنيّة المعلوماتية والاتصالات في حقل حماية الحياة الشّخصيّة تعرف على نطاق واسع بتقنيات تعزيز الخصوصيّة وتعرف بأنها معايير أنظمة تقنيات الاتصالات والمعلومات المتكاملة التي تحمي الخصوصيّة عن طريق ازالة أو تخفيض البيانات الشّخصيّة غير الضّروريّة أو غير المرغوب بها دون التّأثير على كفاءة أداء نظام البيانات.

وعليه فأنّ مختلف الوثائق الدّولية والإقليميّة وكذلك القوانين الوطنيّة تتطلب من جهات المعالجة أن تعتمد وسائل حماية تقنيّة ملائمة لحماية عمليات معالجة البيانات الشّخصيّة.

إن شبكة الانترنيت التي صمّمت لان تكون في الأساس وسيلة لتبادل المعلومات على نطاق محدود، أخذت تتحوّل بوتيرة متسارعة إلى فضاء جديد لتبادل المعلومات بكافة أشكالها على النّطاق الكوني، لكن في موازاة هذا التحول، فإنّه سرعان ما نمت الحاجة إلى إيجاد الوسائل التقنيّة والتنظيميّة، إضافة إلى الوسائل التشريعيّة التي تضمن أمن التبادل والمتبادلين على حد سواء، وتقي من الاعتداءات والتّعديات المحتملة على الحقوق فيها، وتوجد الضّوابط الكفيلة بمراقبة الدّفق المعلوماتي العابر في هذه الشّبكة والمتجول بداخلها، ولتحقيق ذلك تمّ تعميم تقنيّات متطوّرة أوجدها المتعاملون في هذه الشّبكة لاسيما الاختصاصيّون منهم، تساعد على تأمين وظائف الحماية الوقائيّة – وهي حماية مسبقة من شأنها منع وقوع الاعتداءات على الحياة الشّخصيّة– التقنيّة والتنظيميّة المطلوبة بإلحاح من أجل تبادل البيانات الحسّاسة عبر الانترنيت.

ونؤكد هنا أنّ الوسائل التقنيّة والتنظيميّة لحماية الحياة الشّخصيّة في عصر المعلوماتيّة مسألة أساسيّة وعنصر جوهري لنمو الإعمال الالكترونيّة والتّجارة الالكترونية ونؤكّد أنّ حماية الحياة الشّخصيّة تتطلب الوعي والشفافية والفاعلية وبنفس الوقت تبني الحلول التكنولوجيّة الملائمة والشاملة[1].

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 223– 224.

وسنقف في هذا المقام على تقنيّات الحماية من حيث بيان الأدوات والوسائل واستخداماتها واستراتجيات توظيفها، فنعرض في المطلب الأوّل الوسائل التقنيّة ونتعرض في المطلب الثاني إلى عرض وسائل الحماية التنظيميّة.

المطلب الأول

الوسائل التقنيّة لحماية الحياة الشّخصية عبر الانترنت

ضمن نطاق عمليّات التبادل المعلوماتي الرّقمية التي تتزايد في شبكة الانترنيت يوما بعد يوم، وفي ظل انعدام أي مرتكز ورقي للعمليات المتبادلة يصبح من الضّروري تعميم تقنيّات متطوّرة أوجدها المتعاملون في هذه الشبكة تساعد على تامين وظائف الحماية والأمن والسّرية المطلوبة بإلحاح من أجل تبادل البيانات الحسّاسة عبر الانترنيت وقد اخترنا البحث في اثنتين من هذه التّقنيات وهما تقنيّة التشفير المعلوماتي وتقنية الغفلية.

الفرع الأول

التشفير المعلوماتي

تصنّف تقنيّات التّشفير في مقدّمة الوسائل في مجال توفير أمن وسلامة وسرّية المعلومات والحياة الشّخصيّة في شبكة الإنترنيت. ومبرّر هذا التّصنيف يكمن في أنّ تقنيّات التّشفير لا تقتصر فقط على تأدية وظائف الحماية والسّرية للرّسائل الرقمية المتبادلة وحدها بل تتعدّاها لتشمل أيضا وظائف أخرى تساهم بنسبة كبيرة في تدعيم الإثبات المعلوماتي[1].

أبرزها التّحقق من هوية مطلق الرّسائل والمصادقة على مضمونها وعلى توقيع أصحابها إلكترونيّا عليها، والتأكّد من سلامتها.

حيث تأمين هذه الوظائف، يصير في الإمكان تبادل الكثير من البيانات الشّخصيّة الحسّاسة في هذه الشّبكة العالميّة المفتوحة ذات الطابع المتجاوز للحدود وحيث المبادلات الجارية سهلة الاعتراض والالتقاط دون الخشية على ضياعها أو من تسربها أو تحريفها أو الاستيلاء عليها والمقصود بالبيانات الحساسة تلك التي تطال الحياة الشخصية والتي تستوجب بطبيعتها قدرا معيّنا من الحمايّة والأمن والسّرية مثل الرّسائل والصّور الشّخصيّة والمعلومات المهنيّة والماليّة والمصرفيّة أو الأسرار الصناعيّة والتّجارية، ومجمل العمليات

(1) - René MONTERO : les responsabilités liées a la diffusion d’information illicites ou inexactes sur intente face au droit, cahiers du CRID, France 1997.

والمعاملات الداخلة في نطاق التجارة الالكترونيّة و وسائل الدّفع الالكتروني الآمن عن بعد وغيرها.

ومع نمو شبكة الانترنيت وانتشارها الواسع بدأت الكتابة المشفّرة تخرج تدريجيا من دائرة الحضر – بعدما كانت في الماضي حكرا على الاستخبارات العسكريّة والدبلوماسيّة إلى حد أن الكثير من الدّول صنفها ضمن عناصر أمنه الداخلي. وحضر استخدامها والتعامل بها كليا – لكي تفرض ذاتها كوسيلة مهمّة لا غنى عنها في توفير أمن وسرّية وسلامة المبادلات والصفقات الجارية من قبل جمهور المستخدمين لا يتوقف عن النمو والازدياد.

أولا: تعريف التّشفير المعلوماتي

وردت تعريفات عديدة لأدوات التّشفير المستخدمة في ميدان الانترنت، فقد عرّفها القانون الفرنسي بأنّها تشمل جميع التّقديمات التي ترمي بفضل بروتوكولات سرّيّة، إلى تحويل معلومات مفهومة الى معلومات وإرشادات غير مفهومة أو القيام بالعملية المعاكسة وذلك بفضل استخدام معدّات أو برامج مصمّمة لهذه الغاية [1].

ومن التّعريفات التي أوردها الفقه، أنّ التّشفير أو التّرميز هو آلية يتمّ بمقتضاها ترجمة معلومة مفهومة الى معلومة غير مفهومة، عبر تطبيق بروتوكولات سرّيّة قابلة للانعكاس، أي يمكن إرجاعها لحالتها الأصلية.

كما يقصد بعملية تشفير البياناتّ كتابتها برموز سرّيّة بحيث يصبح فهمها متعذرا على من لا يحوز مفتاح الشفرة[2].

يمكن تصنيف تقنيّات التّشفير في ميدان الانترنت إلى فئتين رئيسيتين:

هناك أولا: تلك التي تستخدم المفتاح الخصوصي (Cryptographie à une clé privée) وتسمى تقنية التشفير المتماثل (Cryptage à clé symétriques) وهناك ثانيا: تلك التي

---

[1] - حسب تعريف المادة 1/28 من القانون رقم 90 – 1170 الصادر يوم 29 كانون الأول 1990 حول تنظيم الاتصالات عن بعد ، منشور في الجريدة الرسمية الفرنسية الصادرة يوم 3 كانون الأول 1990.

[2] – فتوح الشاذلي و عفيفي كامل عفيفي، المرجع السابق، ص، 336.

تستخدم المفتاح العمومي (cryptographie à une clé publique) وتسمى تقنية التشفير غير المتماثل (cryptographie à clé asymétrique) [1].

ففي التّقنية الأولى أي التّشفير المتماثل يستعمل نفس الرّمز السّري أو نفس المفتاح في تشفير الرّسائل وفي فكها – أي فك الشّفرة – بمعنى أنّ نظام الكتابة المشفرة بالمفتاح الخصوصي يعمل بواسطة مفتاح واحد يملكه كل من المرسل والمرسل إليه[2].

أمّا في التّقنية الثّانية أي التّشفير غير المتماثل أو بالمفتاح العمومي، فقد برزت هذه التكنولوجيا في نهاية السّبعينات، على إثر أبحاث قام بها العالمان الأمريكيّان (Diffie) و(Helman) وقد أثبتت فاعليتها في مجال توفير أمن الرّسائل والبيانات المتعلقة بالحياة الشّخصية في مجال الانترنت وأول نظام تشفيري من هذا النّظام أطلقه في عام 1978 كل من Leonard Adelman, Adi Shamir , Ronald Rinest.

وهم ثلاثة باحثين من جامعة (MIT) الأمريكية اسموه نظام (RSA) وهو يتحكم اليوم بسوق خوارزميات وتقنيات التشفير.

وارتكازا على نظام (RSA) انطلقت معظم مجموعات برامج التّشفير المعروفة في شبكة الإنترنيت اليوم لاسيما البرنامج المسمى (Pretty Good Privacy) الذي صمّمه الأمريكي(Phil Zimmerman) في العام 1991، ويعتبره البعض أنه برنامج يستحيل خرقه[3].

ويحمي التّشفير خصوصيّة الاتّصالات والبيانات الخاصّة ولكن الأهم أنّه يمكّن من التعبير الحر عن الأفكار والمعلومات خاصّة إذا كان يوجد سجل لدى الحكومة خاص بمراقبة الاتّصالات، وبضمان خصوصيّة الاتّصالات وعدم تحديد هوية القائم بالاتّصال، فإنّ

---

(1) - htpp // www .versign .com / docs/pk-intro.html .

تاريخ الزيارة: 21ماي 2013

(2) - Christiane feral, cybendroit ,à l'épreuve de l'internet , chapitre 7, p 100 et s, 2eme edition , dalloz drunod, France, 2000.

(3) - طوني عيسى، التنظيم القانوني لشبكة الانترنيت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، منشورات صادر، د.ب.ن، 2008، ص، 360.

التّشفير يمكّن من التّبادل الحر للمعلومات في الفضاء الافتراضي وهو أمر مهم وحقّ تقليدي في ظل الظّروف الرّاهنة للعولمة.

وبينما توجد مخاوف قانونيّة شرعيّة يجب أن تأخذ في الحسبان في أية سياسة وطنيّة حول التّشفير، إلاّ أنّه لا يوجد ثمّة مبرّر لحظر استخدام الأفراد أو التّصريح للأفراد باستخدام برامجه[1] بغية حماية حياتهم الخاصّة من الاعتداءات النّاتجة عن استخدام شبكة الانترنيت، حيث يجب النّظر للتّشفير كناقل للتّعبير مثل اللّغة، وبالتّالي يجب أن لا يتمّ إلزام الأفراد بالحصول على تصريح من السّلطات لكي يرسلوا أو يستقبلوا اتّصالات مشفّرة لضمان أمن وسلامة حقهم في حياتهم الشّخصيّة وبياناتهم الخاصة.

إنّ حق تشفير الرّسائل يعدّ ذات أهميّة خاصة لحماية حقوق الإنسان وما يتعلق بحياتهم الخاصّة، وفي عديد من البلدان تستخدم منظّمات حقوق الإنسان برامج التّشفير لحماية هوية الشّهود والضّحايا عند إرسال البيانات إلكترونيا، فجماعات حقوق الإنسان في جواتيمالا، إثيوبيا، هايتي، المكسيك، جنوب إفريقيا وتركيا من بين تلك الجماعات التي تستخدم التشفير، وفقا للمسح الذي أجرته منظمة (GILC)[2].

وتستخدم بعض الجماعات أساليب التّشفير للتّوقيع الكترونيا على الرسائل التي ترسلها عبر الانترنيت لضمان سلامتها، وقد يقوم التّشفير بفعالية بإخفاء مضامين الرسائل ويحجب الغير من الاطّلاع على المعلومات والبيانات المتعلّقة بالحياة الخاصة للأفراد، ولكنه لا يخفي الحقيقة بأنّ ثمّة شيئا قد تمّ تشفيره، وقد يؤدي هذا وحده إلى عواقب وخيمة إذا رغبت السّلطات في معاقبة المرسل أو المستقبل أو إجباره على إفشاء مضمون الرّسالة أو مفاتيحها الخاصّة (Private Keys) وإذا حصلت السّلطات على المفاتيح الخاصّة بالشّفرة فإنّها تستطيع حينئذ قراءة كل رسالة يقوم المرسل بتشفيرها كما يمكن لها كذلك الاطّلاع على بياناته ومعلوماته الخاصة التي قام بتشفيرها .

---

[1] – شريف درويش اللبان، الانترنيت، التشريعات والأخلاقيات، ط1، دار العلم العربي مصر، 2001، ص، 232.

[2] – منظّمة الحملة العالميّة لحرية الانترنت GLIC .

الفرع الثّاني
تقنيّة الغفليّة

إنّ شبكة الانترنيت التي تشكو نقصا فادحا في مستوى الأمن الفعلي فيها، تؤلّف عنصر تهديد أساسي لمفهوم الحياة الشّخصيّة، وبشكل خاص حق مستخدم الشّبكة بأن تحترم سريّة الاتّصالات و المبادلات التي يجريها بواسطة هذه الشبكة.

إن جدّية هذه المخاطر دفعت إلى ابتكار تقنيّات متطوّرة تؤمّن لمستخدمي هذه الشّبكة اتّصالهم بها بصورة مغفلة وذلك من خلال استخدام معدّات يطلق عليها تسمية معاودة الإرسال بشكل مغفل، وتقوم هذه الخدمة بإعادة بث البريد الالكتروني دون تحديد الهوية وتسمى بالانجليزيّة(Anonymous Remailers) وبالفرنسيّة(Reexpediteur Anonymes) [1].

وغالبا ما توفّر هذه التقنيّة لدى مورّدي خدمات الانترنيت ويعرضونها بمثابة خدمات إضافيّة للمشتركين ومن ثمّة ترسلها إلى مقاصدها بعناوين مجهولة أو مغفلة[2].

كثيرة هي التّطبيقات في شبكة الانترنيت، حيث يمكن للغفليّة فيها أن تمنح الحماية لحياة المستخدمين الشّخصية في هذه الشّبكة والحريصين على أن تبقى اتّصالاتهم في هذه الشّبكة سريّة قدر الإمكان ومستترة، ونورد على سبيل المثال أهميّتها في منتديات المناقشة والمجموعات الإخباريّة المخصصّة لطرح ومناقشة المواضيع الطبيّة أو النفسيّة، إذ من المعلوم أنّ المداخلات والحوارات فيها تبقى موثّقة ومحفوظة، بحيث يمكن لمن يشاء وبكيفيّة بسيطة العثور على أسماء وعناوين أصحاب الرّسائل المرسلة منذ عدة أشهر.

في إطار المداخلات والحوارات التي تجري داخل المنتديات والمجموعات الإخباريّة قد يرغب الفرد بإبقائه مغفلا أو مستترا لأسباب مبدئية تتّصل بالمفهوم العام للحياة الشّخصيّة لاسيما لجهة الحق بالسّريّة وبالخصوصيّة، وحتى أحيانا لأسباب شخصية ووجيهة كأن يكون المتدخّل في هذه الحوارات، مثلا وقع ضحية اعتداء جنسي أو يكون مصابا بداء فقدان المناعة....إلخ.

ولتقنية الغفلة كتقنية التشفير ميزات وعيوب:

---

[1] – شريف درويش اللبان، المرجع السابق، ص، 234.

[2] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 250.

أولا: ميزات تقنية الغفليّة:

في الحالات السّابقة الذّكر، تكون للغفليّة منافع وإيجابيات عديدة تنصبّ مباشرة في خانة حماية الحياة الشّخصيّة للفرد في مجال الانترنت، لاسيما حقّه بأن لا تجمع أو تحلّل أو تستغل المعلومات المتعلقة بشخصه أو بعائلته أو بمسكنه وسائر البيانات التي تسمح بالتّعرف عليه، بدون رضاه وموافقته الصّريحة. وفي هذا المجال، يعتبر الكثيرون بأن الغفليّة هنا أيضا أداة فعّالة في متناول مستخدمي شبكة الانترنيت لمجابهة مثل هذه الممارسات[1].

ثانيا: عيوب الغفليّة

حتى وإن كانت الغفليّة في شبكة الانترنيت تتضمّن قدرا معيّنا من الحماية لمفهوم الحياة الشّخصيّة، فإنّ لها مظاهر سلبيّة خطيرة إذا أسيئ استعمالها، لا يمكن التغاضي عنها أو التّساهل بشأنها على الإطلاق، أبرز هذه المظاهر السلبيّة أنّها تسهل، وبنسبة كبيرة، النّشاطات الإجرامية وغير الشّرعية في شبكة الانترنيت، عن طريق حجب هوية مرسلي الرّسائل الضّارة، كأن تستخدم الغفليّة في الحثّ على الحقد العرقي أو التحّريض على العنف أو في القدح أو الذّم، أو في التّشهير أو تفشّي الإباحية...الخ بحيث يجد مرتكبو الجرائم أنفسهم، مع هذه الغفليّة، مدفوعين بشعور انعدام المعاقبة [2].

وقد ساهمت المظاهر السّلبية للغفليّة، في اتّساع حجم الأصوات المنادية بوجوب حظر استخدام الأجهزة والمعدّات والبرامج التي تؤمّن الغفليّة للمستخدمين في شبكة الانترنيت، لكن الحلول التي ينبغي اعتمادها في مجال الغفليّة، –التي يجب أن لا ننكر منافعها وإجابتيها الكثير– لا يمكن أن تكون مطلقة أي أنّه لا يكفي التّذرع بالسّلبيات أعلاه لتبرير منع الغفليّة في هذه الشّبكة. لكن لا يمكن الحكم مسبقا بهذا الخصوص سلبا أم ايجابا دون فهم وإدراك حقيقيّين لتركيبة شبكة الانترنت ولطريقة عملها. فبمقتضى بروتوكول الانترنت (IP) الذي يختصّ بعنونة البيانات في الشّبكة يمكن دائما معرفة الموزّع (Serveur) الذي استعمله مستخدم الشّبكة للاتّصال بالمواقع الأخرى الموصولة بشبكة الانترنت، وهو

---

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 251.

[2] – طوني عيسى، المرجع السابق، ص، 401.

غالبا ما يكون مورّد خدمة الاتّصال بالشّبكة، وذلك بفضل تقنيّات مبتكرة تسمح بتتبّع المسار الذي يكون قد سلكه الاتّصال المقصود بغية التّوصل للموقع الجغرافي للموزّع (أو لمورّد خدمة الاتّصال) الذي أمّن له الدّخول إلى الشّبكة[1].

ومن هذا الأخير، يمكن بالطّبع معرفة الهويّة الحقيقيّة لمستخدم الشّبكة الذي أجرى الاتّصال، باعتبار أنّ هذا المورّد يفترض أنه قد وقّع معه عقد اشتراك وحصل منه على المعلومات الضّرورية للتّعريف عنه، فطالما يمكن دائما تتبّع مسار الرّسالة المطلقّة والتوصل بالنّتيجة إلى تعيين موضع تمركز الموزّع أو مورّد خدمة الاتّصال الذي أطلقها حتىّ لو توسل صاحبها الغفليّة، فإننا لا نجد مبدأ خطر الأجهزة المعاودة للإرسال المغفل بحد ذاته مبرّرا، وبالتالي يمكن الوصول إلى الشّخص المرسل أو الذي قام بالاعتداء على البيانات الخاصة أو الحياة الشّخصيّة للغير ولو كان مغفلا.

أما بالنسبة للغفليّة المطلقة أي الغير القابلة للتتبّع l'anonynat absolu ou intractable فهي التي تعني أن يستخدم مورّد خدمات الاتّصال أجهزة معيدة للإرسال المغفل، من النّوع الذي يحقق غفليّة كاملة، فهي لا تحتفظ بأية بيانات أو معلومات تسمح بتعريف أصحاب الرّسائل، ولا تترك أيّ أثر لأيّ عنوان أو لمنشأ هذه الرّسائل قبل أن تعيد إرسالها.

وبالتالي فيستحيل من خلالها التّعرّف على الهوية الحقيقيّة لأصحابها حتى و لو كان مورد الخدمات.

وفي هذا المجال أخذت الولايات المتّحدة الأمريكية المبادرة حيث أضافت تعديلات واسعة إلى قانون الاتّصالات لديها بموجب قانون المساعدة الاتّصالية لتطبيق القانون رقم 411-103 لعام 1994، الذي يعتبر بأنّ إجراء اتّصال هاتفي أو استعمال وسيلة اتّصالات أخرى، ومن بينها طبعا شبكة الانترنيت دون الكشف عن هوية المتّصل و بنيّة إزعاج أو تهديد، أو التّعدي على الشّخص الذي يتلقى الاتصال، يشكّل جرما جزائيّا معاقب عليه.

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 253.

ويختم بالقول أنّ الغفليّة بنوعيها المطلقة والنّسبية تتطلب نظاما قانونيا يراعي الجوانب التقنية[1].

إنّ التّشديد على وجوب وضع اطار تنظيمي وقانوني ملائم لاستخدام الأجهزة المعيدة للإرسال المغفل التي تؤمّن غفليّة نسبيّة وقابلة للتتبع نابع بشكل أساسي من الحاجة العمليّة إلى تفادي احتمالات امتناع مورّدي خدمات الاتّصال، الذين يملكون المعلومات التعريفيّة المطلوبة عن هوية أصحاب الرّسائل المغفلة، عن البوح بها، متذرعين بأسباب وحجج مختلفة.

فالبوح بالمعلومات الشّخصيّة العائدة إلى المشتركين التي يكون مورّد خدمات الاتّصالات بالانترنيت حائزا عليها، يمكن أن يعتبر تعرّضا لمفهوم الحياة الخاصة والشّخصيّة، وبشكل خاص لحق الفرد في ستر اسمه والحق في سّرية عنوانه أو مكان سكنه، هي حقوق تكرّسها العديد من القوانين الوضعية والاتّفاقيات الدّولية، ويؤكّدها الاجتهاد، ويكاد الفقه يجمع عليها.

ونظرا لأنّ الحق في الحياة الشّخصية ليس مطلقا إذ قد يصطدم بمقتضيات ردع الافعال ذات الطّابع الجرمي ومعاقبتها، لهذا السبب ينبغي تنظم الاصول والحمالات التي يجوز خلالها إلزام مورّد خدمات الاتصال بالكشف عن المعلومات التعريفيّة الشخصية التي يملكها عن المشتركين.

ولعلّ الإشكال الأبرز الذي تطرحه شبكة الانترنيت في هذا المجال يتمثّل بأن تبقى دولة واحدة مثلا موصولة بهذه الشّبكة وتعتمد سياسة متحرّرة إزّاء الاتّصالات المغفّلة بما في ذلك أجهزة معاودة الإرسال من النّوع الذي يؤمّن غفليّة مطلقة وغير قابلة للتتبّع عندما يصبح التّحايل على التشّريعات المتشدّدة في هذا الشّأن لدى الدّول الأخرى أمرا ممكنا وسهلا.

وهذا ما يدفعنا إلى بحث الوسائل التّنظيمية لحماية الحياة الشّخصيّة في مجال الانترنيت.

---

[1] – بوليون أنطونيوس أيوب ،المرجع نفسه، الصفحة 256.

المطلب الثّاني

الوسائل التّنظيميّة لحماية الحياة الشّخصيّة عبر الانترنت

إنّ عدم ثقة المستخدمين بالانترنيت نظرا للمخاطر التي تتعرّض لها حياتهم الشّخصية دفع باتّجاه ظهور عشرات المبادرات للتّنظيم الذّاتي كوسيلة قانونيّة تحظى باحترام المستهلكين والأفراد وتقوم على وضع مدوّنات سلوك ملزمة لقطاع معيّن، وفق رؤية هذا القطاع، كما أنّه في ظل هذا الواقع، أصبح من المتّفق عليه بين مختلف قطاعات الاعمال والمواقع على الانترنيت أن وضع سياسة خاصة بشأن الخصوصيّة على المواقع أمر ضروري لبناء الثّقة بين مستخدمي الانترنيت وبين الموقع نفسه وبالتالي بين المستخدمين والانترنيت ككل وغرض هذه السّياسات إبلاغ المستخدم عما يجري جمعه من بيانات شخصيّة عنه خلال تفاعله مع الموقع وسياسة الموقع بشأن التعامل معها واستخدامها ونقلها.

فسياسة الخصوصيّة بوجه عام هي عبارة عن وثيقة أشبه بالعقد تتضمن التزامات المستخدم والتزامات الموقع، وتصلح مصدرا لالتزامات الطرفين، يتيح الإخلال بها من أيّهما تحريك المسؤوليّة العقديّة في مواجهة المخل[1]. وبالتالي لا يمكن أن نغفل الدور الذي تلعبه الاستراتيجيات التّنظيميّة في حماية الحياة الخاصة في بيئة الانترنيت وهذا ما سنتناوله في هذا المطلب وذلك بتبيين الدور الذي تلعبه الوسائل التّنظيميّة من تنظيم ذاتي وعقد في حماية الحياة الخاصة في مجال الانترنيت.

الفرع الأوّل

التّنظيم الذّاتي

إزاء عجز القانون والتّشريعات المختلفة عن توفير أمن قانوني بالكامل، نظرا لاختلاف مستويات الحماية للبيانات الشّخصيّة بين دولة وأخرى، برزت الحاجة إلى تجاوز النّظام التقليدي وإلى تصوّر أدوات وآليات قانونيّة وتنظيميّة أخرى تراعي طبيعة شبكة الانترنيت وتسمح بالإحاطة بالوضعيّات المتعدّدة التّمركز على المستوى الجغرافي، وقد بدأت تظهر مؤشّرات عدّة في هذا الاتّجاه وذلك من خلال ما يسمى بالتّنظيم الذّاتي الذي يعتمد كوسيلة

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 259.

لحماية البيانات الشّخصيّة المعالجة إلكترونيّا في شبكة الانترنيت، والاهتمام بحرمة وسّرية الحياة الشّخصيّة لا تقتصر فقط على الأفراد وحدهم، فقد ظهر اتّجاه عريض ومتزايد لدى قطاعات الأعمال، وأصبحت تأخذ موضوع الحياة الشّخصيّة على محمل الجدّ وأحيانا كعامل خطر يهدّد أعمالها باعتبار أنّ عدم الثّقة بالتّجارة الالكترونيّة بسبب الخشية على الخصوصيّة يمثل عائقا فعّالا لرواج التجارة الالكترونيّة ذاتها في البيئة المعلوماتيّة.

فالتّنظيم الذّاتي في شبكة الانترنيت هو بشكل أساسي الأعراف والقواعد السّلوكيّة المتكوّنة ضمن القطاعات المهنيّة والتّجاريّة المختلفة في معرض مزاولة أنشطتها عبر الشّبكة حيث نجد المهتمّين وأرباب العمل في قلب مهنة معيّنة يتبعون أحيانا قواعد سلوكيّة ذاتيّة تحكم علاقاتهم المهنيّة وتنظيمها[1].

ويرى الكثيرون في طرح التّنظيم الذّاتي لشبكة الانترنيت حلاّ مثاليا وآلية مبتكرة في تنظيم استخدام هذه الشّبكة وهم يعتبرون أن العادات والأعراف عندما تتركّز وتتكوّن تدريجيا على المستوى العالمي، تمتاز قدرتها على أن تلعب دورا مرجعيا متجاوزا للحدود وبالحدّ الأدنى من المشقّة والعناء على الصّعيد القانوني، فهي تتمتّع عموما بالمرونة والفعاليّة فيما تقدّمه من حلول بشأن حماية الخصوصيّة وحرمة الحياة الشّخصيّة في مجال الانترنت، فهي تتيح لقوى السّوق والقطاعات الصناعيّة تزويد حلول متميزة في هذا الحقل.

وفي رأينا أنّ التنظيم الذاتي هو وسيلة لتنظيم موضوعات تقنيّات المعلومات عموما، وأداة مكمّلة لا متناقضة مع التّشريع وأصبح وسيلة أوّلية تسبق التّشريعات كلما وجدت صعوبة لإصدار التّشريع أو الحاجة إلى وقت لإصداره. ويمكن القول أنّ النّموذج الأمريكي للتعامل مع تقنيّة المعلومات دعا إلى المزيد من تبني فكرة التّنظيم الذاتي في حقل حماية الحياة الشّخصيّة والبيانات الخاصّة وأمن المعلومات.

مع ذلك فإنّ سياسة التّنظيم الذّاتي لم تظل دون استثناءات بل أحيانا ظهر توجه جديد نحو التّنظيم الحكومي ومثال ذلك إقرار تشريعات في حقل حماية خصوصية الاطفال على الخط لعام 1988 وفي حقل الملكية الفكرية أيضا.

---

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 262.

أما الاتحاد الأوروبيّ فأنه يتجه نحو التّنظيم الحكومي أكثر، لهذا نجد أن منظّماته قد اتّجهت دائما إلى توجيه الدّول الأعضاء إلى إصدار تشريعات تتلاءم مع القواعد المقرّرة في الأدلة الإرسالية والتوجيهية الصادرة عن منظّماته كمجلس أوربّا واللّجنة الأوروبيّة والاتّحاد الأوربيّ بل اتجه إلى التّنظيم التّشريعي الشّامل عبر قوانين البرلمان الأوربيّ وأمام اتّساع المخاطر الأمنيّة التي تستهدف البيانات الخاصة والتطفّلات التي تتعرض للحياة الشّخصيّة للأفراد بات يتحتم على الشّركات العاملة في قطاع المعلوماتيّة توفير حلول وأدوات فعّالة لمواجهة هذه التحدّيات، ومن قبيل تجارب التنظيم الذاتي في بيئة أعمال الانترنيت لتعزيز الخصوصيّة مبادرة الثقة الالكترونية (تروست)Truste[1] ومجلس الأعمال لبرنامج الخصوصيّة على الخط (Better Business Bureau's Online Privacy Program) واتّحاد الخصوصيّة على الخط (Online privacy Alliance) وغيرها.

ومع تزايد الشّركات في بيئة الانترنيت وتزايد الجهات العاملة في حقل الأمن والخصوصيّة، نجد عشرات مبادرات التّنظيم الذّاتي، حتى أنّنا نجد الآن مواقع متعدّدة مثل (Privacy Sensitivity) تشير إلى تقديم منتجات وخدمات تحمي الخصوصيّة والبيانات الحسّاسة كما أنّ كثير من الشّركات التّجارية تستخدم شعارات الخصوصيّة نفسها في خططها التّسويقية ومواردها الإعلانية وتتسابق في إظهار ما تستخدمه من تقنيات لحماية الحياة الشّخصية على الانترنيت[2].

وبرزت في العالم العربي بعض نماذج للتّنظيم الذّاتي لحماية الحياة الشّخصيّة في مجال الانترنيت والتي اعتمدت من قبل الكثير من التّشريعات وأشهرها "ماكافي" إحدى أكثر الشركات الموفّرة لأنظمة الأمن المعلوماتي وحماية خصوصيّة المعلومات، وتظم منتجات "ماكافي"قائمة من أحدث تطبيقات جدران الحماية وبرامج مكافحة فيروسات الكمبيوتر والبريد

(1) – عن موقع www.truste.org :http// تاريخ الزيارة 21 ماي 2013 الساعة 23h00

(2) – موقع www.privacyalliance.org تاريخ الزيارة: 26 ماي 2013 الساعة 11ساو 14 د.

الالكتروني التّطفلي وتطبيقات الحماية ضد محاولات اختراقات الأنظمة المعلوماتية، ويعد برنامج" جدار الحماية الشّخصية" أهم ما تضمّنته هذه القائمة وهو أداة ضروريّة لكافة مستخدمي الكمبيوتر كونه يضمن حماية الاتّصالات الالكترونيّة ويحبط محاولات الوصول غير المرخّص لأجهزة الكمبيوتر والمعلومات الشّخصيّة[1].

وهذه الجهود التي ساهمت في تعزيز الثّقة بالانترنيت لدى كثيرين فإنّها أيضا أثارت تساؤلات وتحدّيات كبيرة، أوّلها التساؤل حول مدى ضمان الالتزام بقواعد التنظيم الذاتي في بيئة غير مركزية كالانترنيت لا تتحكم بها سلطة تنفيذية.

وقد برزت أراء كثيرة ومتناقضة في إطار تقييم التّنظيم الذاتي كوسيلة لتنظيم موضوعات تقنيّة المعلومات بشكل عام، بما تنطوي عليه من حماية للبيانات والحياة الشّخصيّة، الذي يعتبر من أوّل وأهم المواضيع التي طرحت على بساط البحث في هذا العصر عصر المعلوماتية .

ونظرا لاختلاف الأنظمة القانونية بين الدّول، يرى الكثيرون أن طرح التّنظيم الذاتي لشبكة الانترنيت حلاّ مثاليا والية مبتكرة في تنظيم استخدام هذه الشبكة.

ويدعم هذا التّوجه ويؤكّده فريق واسع من الفقهاء الأمريكيين، كما يروج له بشكل أساسي أنصار نظرية وضع" شرعة" خاصة بشبكة الانترنيت.

أعتبر البعض من أنصار هذا الموقف أنّ التّنظيم الذّاتي في شبكة الانترنيت هو شبه حتمي ومن غير الممكن الاستغناء عنه تماما كالقوانين الدّاخلية للدّول التي لا يجب أن تتفوق على هذه القواعد التي يضعها مستخدمو الشّبكة أنفسهم إلاّ في أحوال جدّ محدودة ويسميها الانجلوسكسونيون سياسات الاستعمالات المقبولة (Acceptable Uses Polices)

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 264.

التي تلحظ على سبيل المثال الأصول المتعلّقة باحترام الطّابع الخاص للبريد الالكتروني أو احترام الحياة الخاصة[1].

لكن هذا التوجّه لا يلقى إجماعا، إذ يشكّك البعض بجدوى وسيلة التنظيم الذاتي وبفاعليتها، معتبرين أنّه أيّا تكن التّسمية التي قد تعطى لهذا الحل فسوف يبقى ذو تطلعات محدودة وفي أحسن الأحوال سوف يقود إلى تعزيز نظام الرّقابة الحكوميّة على شبكة الانترنيت وعدم خضوعها إلى سلطة محرّرة تديرها.

الفرع الثاني

العقد

إنّ نقل البيانات خارج الحدود، يحتاج بهدف حماية الأفراد، أن يصار إلى معيار متوازن بين حق تدفّق البيانات الشّخصيّة وبين موجبات الحماية. هذا المعيار يتمثّل في ضرورة ضمان أن تتوفّر في الدّولة المنقول إليها البيانات حماية ملائمة للحياة والبيانات الشّخصيّة تكفل عدم إهدار الحق في خصوصية البيّانات.

إلاّ أنّ نقل البيانات لا يجب، أن يؤدّي إلى إفقاد الشّخص الحق في الوصول إلى المعلومة وذلك بالقيد المشدّد على نقل البيانات كما أنّه لا يجوز أيضا أن يطلق إلى الحد الذي يسهل فيه إيجاد ضوابط الحماية فيصار لنقل عمليات المعالجة كلّيا أو جزئيّا ونقل بيانات الأفراد و الاتجار بها.

ونظرا لأنّ عصر المعلومات يستوجب نقل بيانات متعلّقة بالحياة الشّخصيّة وبيانات خاصّة بالأفراد، ولعدم كفاية الحماية التّشريعية في كافة الدّول أو لتفاوتها في دول الإقليم الواحد كما هو الحال في أوروبا والتي توصف أنّها البيئة الخصبة لحماية الخصوصيّة، لذلك فأحد الأدوات التي تتجاوب مع المعيار المتقدّم بشأن نقل البيانات الخاصة وفي نفس الوقت تحل مسألة قصور الحماية التّشريعية تتمثل في عقود نقل البيانات[2].

---

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 266

[2] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 268.

ولابد في هذا الإطار من التطرّق إلى سياسات الخصوصيّة على شبكة الانترنيت والتي يمكن تكييفها من حيث طبيعتها القانونيّة بأنّها عقد نظرا لما تتضمنه من التزامات عقدية[1].

يتيح الإخلال بها إلى ترتيب المسؤوليّة العقديّة على الطرف المخل فقد أصبح من المتّفق عليه بين مختلف قطاعات الأعمال والمواقع على الانترنيت أنّ وضع سياسة خاصة بشأن الخصوصيّة على المواقع أمر ضروري لبناء الثّقة بين المستخدمين والانترنيت ككل وغرض هذه السيّاسات إبلاغ المستخدم عما يجري جمعه من بيانات شخصيّة عنه.

فسياسة الخصوصيّة بوجه عام، هي صفحة أو مجموعة صفحات موجودة على موقع الانترنيت تصف البيانات الشّخصيّة التي يجمعها الموقع و كيفية استخدامها والمواقع التي تتشارك معه في هذه البيانات ونطاق سيطرة المستخدم على استخدام بياناته الشّخصيّة.

إن وضع سياسة للالتزام بالخصوصيّة على مواقع الانترنيت المختلفة وتحديدا تلك التي تطلب بيانات شخصيّة لأغراض التفاعل مع المستخدم (مواقع التجارة الالكترونية، البنوك الالكترونية) لهو أمر ضروري لبناء الثّقة ما بين الموقع والمستخدم، وتوضع هذه السّياسات في الأساس لإعلام المستخدم عما يجمع عنه من بيانات وعن أوجه استخدامها والتزامات الموقع بشأن الحفاظ عليها وقيود نقلها للغير.

وسنبيّن الشكل الذي غالبا ما تتخذه هذه السّياسات وما تحتويه من بنود من شأنها تأمين الحماية للبيانات والحياة الشّخصيّة.

أولا: سياسات الخصوصيّة من حيث الشّكل

بالنّسبة للشّكليّة التي تتخذها سياسة الخصوصيّة فإنّ الخطّ الواضح و تبين محتوى السّياسة يساعد على سهولة قراءتها. و لكنّنا نلاحظ أنّها غالبا ما ترد بشكل لا يشجع على قراءتها كأن تكون طويلة من حيث المتن أو مقسّمة إلى صفحات تتطلب الانتقال من واحدة إلى أخرى أو غير متوفّرة في الصّفحة التي يتم فيها تزويد الموقع بالبيانات أو أنها مكتوبة

[1] – موضوع التعاقد، بيان التزامات مستورد البيانات، بيان التزامات مصدر البيانات، بيان ضمان مستورد البيانات، بيان القانون الواجب التطبيق و جهة الاختصاص القضائي، بيان أحكام تجديد العقد أو فسخه أو إنهائه.

بخط صغير أو في مكان يصعب فيه قراءتها، وهذه الأشياء أو الصّعوبات هو أول ما يلاحظه المرء عند دخوله لدراسة سياسات الخصوصيّة لدى بعض المواقع و الشركات[1].

ولهذا فإنّ هناك أهمّية بالغة لمراعاة عناصر الشّكل أو البناء الشّكلي العام وأهمّيتها أن تكون السّياسة مختصرة بقدر الإمكان دون إخلال بمحتواها، بمعنى التوازن بين موجبات تغطية البناء الموضعي بعبارات واضحة مختصرة بعيدة عن الإسهاب غير اللازم، لكن هذا مفاده أنه لا يجب أن ترد بإيجاز مفرط إلى حد يفقدها قيمتها ومضمونها.

وبهدف تحقيق حماية فعّالة للحياة الشّخصيّة عبر الانترنيت يجب أن تنطلق سياسات الخصوصيّة من مبادئ احترام الخصوصيّة المقرّرة دوليا وإقليميّا ووطنيّا، بمعنى أنه يجب أن تعكس الموقف القانوني من الخصوصيّة في مجال يشعر المستخدم بتوافق الموقع مع المشروعيّة.

وكما سيرد فيما يلي، فإنّ حماية خصوصيّة المعلومات يقوم على مبادئ تحكم عمليات الجمع والمعالجة والتّخزين والاستعمال والتّبادل وهي مبادئ تدور حول الالتزام بعدم جمع البيانات في نطاق أوسع من الغرض المراد من جمعها وهو غرض ضروري ومشروع والالتزام بتحديد الاستعمال في نطاق الغرض والملائمة وعدم إساءة الاستخدام أو تعدّيه أبعد من ذلك أو منح الأفراد حقوقا من اللّحظة الأولى لجمع البيانات تبدأ من إخبارهم بعملية الجمع وغرضها وإتاحة خيار القبول أو الرفض وإتاحة خيار الانسحاب الاختياري من تقديم البيانات أو التّراجع اللاّحق عنه وإتاحة حق الوصول اللاّحق وتصحيح البيانات وتحديثها وإلغائها إضافة إلى مبادئ تتعلّق بالتزامات جهات المعالجة بمعايير أمن وسلامة وسرّيّة البيانات والتّقيد بالقيود القانونيّة في عملية التبادل والنّقل، وبالتّالي فإن مراعاة هذه المبادئ من قبل موقع الانترنيت يتيح تضمين سياسة الخصوصيّة ما يعكس هذه المبادئ التي تتكفّل بحق بناء الثّقة لدى المستخدم[2].

---

(1)- سياسات الخصوصية لدى بعض المواقع و الشركات:

http// : www1.euro.dell.com/content/topic/topic.aspx/emea/topic/footer/privacu ?c =dz 8l=ar. http// www.microsoft.com/products/ceip/ar-sa/privacypolicy.mspx. http//www.nokia.com/sa-ar/privacy/privacy/policy/privacy-policy/.

تاريخ الزيارة 27 ماي2013 على الساعة 11 سا و45 د.

(2) – بولين انطونيوس أيوب ، المرجع السابق ، الصفحة 274.

ثانيا: سياسات الخصوصيّة من حيث المضمون

إنّ المبادئ التي يجب أن تتضمّنها سياسات الخصوصيّة والتي تهدف إلى تأمين حماية فاعلة للحياة الشخصية عبر الانترنت هي ما يلي:

1- المعلومات التي يتم جمعها سواء تلك التي يجري تقديمها مباشرة من المستخدم عن طريق تعبئة استمارات الاشتراك أو الخدمة أو تلك التي يجري جمعها الكترونيا عبر رسائل الكوكيز أو من خلال بروتوكولات الاتصال.

2- أغراض هذا الجمع و الاوجه الضّرورية له بشكل واضح و شامل بعيدا عن العبارات الغامضة وأوجه و طريقة استخدام هذه البيانات بالنّسبة للموقع نفسه والجهات المشتركة معه.

3- الالتزام بعدم نقل البيانات لطرف ثالث دون الموافقة، أو تحديد الطّرف الثالث الذي تنقل اليه البيانات مع تبيان أغراض نقلها الدّقيقة، وبيان التزام الموقع بحماية البيانات مع بيان أغراض نقلها أو عدم مسؤوليته عن هذا النّقل مع إتاحة الخيار عندها لرفض نقل البيانات مستقلا عن بقيّة الشّروط والالتزامات، وفي هذه الحالة يتعين أن تتضمّن السّياسة التزاما واضحا من الموقع باستخدام البيانات لديه وحده وعدم نقلها للطّرف الثّالث في حال عدم الموافقة.

4 - في الحالات التي يريد الموقع استخدام البيانات لأغراض ثانوية غير الغرض المعلن، فإنّ على الموقع بيان هذه الأغراض وإتاحة الحق للمستخدم برفض الاستخدام للأغراض الثّانوية أو قبوله صراحة.

5- بيان ما اذا كان للمستخدم حق الوصول للمعلومات وتحديثها وهذا ما تتيحه مثلا شركة (Google) حيث يمكن للأشخاص الوصول إلى معلوماتهم وتحديثها متى أرادوا ذلك[1] أضف إلى هذا إمكانية تصحيحها أو حذفها[2].

---

(1) - http //www.google.dz/intel/ar/policies privacy/

(2) - http//www.who.int/about/privacy/ar

تاريخ الزّيارة: يوم 27 ماي2013 : 13ساو 54د

6 – بيان المدّة التي سيحتفظ فيها الموقع بالبيانات وما إذا كانت ستحفظ لمدة أطول من الغرض الذي جمعت لأجله.

7 – بيان آلية التّعويض عن الأضرار والمسؤوليّات القانونيّة وبيان الجهة التي يتصل بها المستخدم عند الاعتداء على خصوصيّته أو رغبته بتقديم شكوى أو المطالبة بالتّعويض.

8 – بيان القانون الواجب التّطبيق عند حصول النّزاع وتحديد الاختصاص القضائي بنظر النزاع.

9 – تعيين المسؤول في الموقع عن مسائل الخصوصيّة وتحديد بريده الالكتروني أو عنوانه إشعارا للمستخدم بمزيد من الثقة في التزام الموقع بحماية الخصوصيّة.

باستعراضنا لمختلف النماذج التطبيقية لسياسات الخصوصيّة نجد أنّها بغالبيتها لا تنطوي على المبادئ المذكورة أعلاه بأكملها فتغيب بعض هذه المبادئ عن بعضها، لا بل أنّها قد تنطوي على تناقضات وغموض في أجزاء منها تتعارض مع حماية الحياة الشّخصيّة فبالرّغم من شمولية بعض نماذج سياسات الخصوصيّة وتغطيتها البناء الموضوعي والشكلي، وبالرّغم من انطوائها على التزامات رئيسيّة من قبل الموقع ذاته لحماية الخصوصيّة إلا أنها تنطوي على بعض أوجه الغموض والتناقض التي تخل بمستوى الحماية وتثير التساؤلات [1].

[1] – بوليون أنطونيوس أيوب، المرجع السابق، ص، 277.

خاتمة:

لقد بات من المحتّم على دول العالم مواكبة التّطور التكنولوجي الحاصل في العالم الافتراضي الجديد الذي صارت المعلومة فيه سيّدة دون منازع ومصدرا للقوة، بل وأكثر من ذالك صارت معيارا لتطوّر الشعوب.

وإزّاء التطور العلمي الهائل فإن مزايا الانترنت جلبت معها أيضا مخاطر جمة وصارت سلاحا لا يستهان به لممارسة النشاطات الإجرامية وبهذا ظهرت طائفة جديدة من الجرائم المستحدثة، إضافة إلى إمكانية ارتكاب الجرائم التقليدية بطريقة حديثة.

ومن خلال دراستنا لهذا الموضوع توصلنا في فصله الأول إلى النتائج التالية:

1- لا يشكل الانترنت موضوعا لتشريع خاص مستقل.

2- يمكن تطبيق النصوص العقابية المتعلّقة بجرائم القذف ولسّب الواردة في التشريع الفرنسي والمصري والجزائري في مجال شبكة الانترنت.

3- تختلف صور الاعتداء على سرّية المراسلات المكتوبة الالكترونية عن صور الاعتداء على سرّية المراسلات المكتوبة التقليدية، حيث يتم الاعتداء على هذه الأخيرة بالفتح أوالإخفاء أو الإفشاء أو الاختلاس أو الإتلاف، بينما يتم الاعتداء على المراسلات الالكترونيّة المكتوبة بالاعتراض أو الاختلاس أو الإخفاء أو التّغيير أو الإذاعة أو النّشر أو التّسجيل.

4- تتفاوت الحماية الجنائية لسرية المراسلات الالكترونية المكتوبة في القانون المقارن، وبصفة عامة لا تخلو في مجملها من القصور.

ففي فرنسا تضمّن قانون العقوبات في المادتين226/15 و432/9 حماية لسرية المراسلات التي تتم بطريق الاتّصالات وهي تنطبق على المراسلات الالكترونيّة المكتوبة التي تتم بطريق الانترنت، وقد وجدنا أن هذه الحماية لا تكفي لحماية المراسلات الالكترونيّة المكتوبة من كل صور الاعتداء عليها.

وفي مصر تضمّن قانون تنظيم الاتّصالات حماية جنائيّة لسرّية رسائل الاتصالات في البندين01 و02 من المادة 73 ويمكن تطبيقها على المراسلات الالكترونيّة المكتوبة التي تتمّ في مجال شبكة الانترنت، وقد وجدنا أن هذه الحماية لا توفّر الحماية الكاملة لسرية رسائل الاتصالات، حيث أنها اقتصرت على عقاب الاعتداء على سرّية رسائل الاتصالات

الذي يرتكبه أحد عمّال شبكات الاتصالات، ولا تتضمن حماية من الاعتداءات التي يرتكبها غير هؤلاء.

أمّا المشرع الجزائري فقد نص على حماية جنائيّة لسرّية المراسلات في المادة 303 مكرر و303 مكرر1 من قانون العقوبات ويمكن تطبيقها على المراسلات الالكترونيّة المكتوبة، كما تضمّن قانون العقوبات حماية جنائيّة غير مباشرة للمراسلات الإلكترونيّة المكتوبة بموجب أحكام المادتين 394 مكرر و394 مكرر2، غير أن هذه الحماية التي وردت في قانون العقوبات الجزائري ليست كافية لحماية المراسلات الالكترونيّة المكتوبة من كل صور التّعدي عليها، كما أن الحماية غير المباشرة لسرّية المراسلات الالكترونية المكتوبة لم تكن صريحة، وواضحة بشأن إمكانية تطبيقها على المراسلات الالكترونية المكتوبة وفقا لما يقتضيه مبدأ الشّرعية.

ثم تبيّن لنا من خلال دراسة الفصل الثّاني لهذا البحث قصور قواعد الإجراءات الجزائية في مواجهة التعرّض للحياة الشّخصية عبر الانترنت، كفشلها في مجال الضّبط والتحري، والتحقيق وتفتيش النّظام المعلوماتي واستنباط الأدلّة وإثبات جريمة التّعدي على الحياة الخاصة بالنظر إلى طبيعة الدليل الذي يتحصّل منها، إذ قد يكون هذا الدليل غير مرئي وقد يسهل إخفاؤه أو تدميره، وقد يكون متّصلا بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها. كما وأنّ هذا الإثبات قد يحتاج إلى معرفة علمية وفنيّة قد لا تتوافر لضبّاط الشّرطة القضائية والقضاة.

كما تبيّن لنا كذالك:

1- قصور كلا من الوسائل التقنيّة والتّنظيميّة المستحدثة بغرض حماية البيانات الخاصّة بوجه خاص وبالتالي حماية الحياة الشخصية بوجه عام من مخاطر المعلوماتية.

2- أنّه رغم التّدخل التّشريعي الموضوعي، إلاّ أنّ هناك قصورا في التّشريعات الإجرائيّة، ذلك أنه ما يزال يقف في حمايته للحريّة الشّخصيّة وحرمة الحياة الخاصّة من الوسائل الالكترونيّة متجاهلا بذلك الإجراءات الضّروريّة للحصول على الدّليل في الجريمة المعلوماتية ومعتمدا دائما على الإجراءات التّقليديّة، خاصة منها التّفتيش والخبرة.

3 - أنّ هناك صعوبة تكتنف الدّليل بالنّسبة لهذه الجريمة سواء من حيث طرق الحصول عليه أو من حيث طبيعته، فالحصول عليه قد يحتاج إلى عمليات فنّيّة وعلميّة، كما أن

طبيعته قد تكون غير مرئية، كالذّبذبات والنّبضات، وأنه من السهولة استخدام التقنيّة العلميّة في إخفائه أو إتلافه.

وعلى ضوء هذه النّتائج فإنّنا نقترح ما يلي:

1- تعديل المادتين296 و297 من قانون العقوبات الجزائري لفك الغموض المتعلّق بركن العلانيّة وكذلك لتكون صياغتها واضحة ومحدّدة بشأن انطباقها على جرائم القذف والسّب، المرتكبة بواسطة الأجهزة المستحدثة بفعل التقدم التكنولوجي وتطور تقنيّة المعلومات على النحو الذي وردت به جريمة الإهانة والقذف والسّب الموجّه إلى رئيس الجمهورية في المادّة 144 مكرّر منه.

2- إدراج المشرّع الجنائي الجزائري إلى جانب النصوص العقابيّة التي تحمي سرية المراسلات التقليديّة، نصوصا أخرى تتضمن حماية صريحة لسرّية رسائل الاتصالات من كل صور التّعدي عليها سواء تلك التي يتم ارتكابها من طرف الأفراد، أو من أي عامل في شبكات الاتّصالات.

3- توفير أدوات حماية تقنيّة تعمل على تقليص عمليات جمع البيانات الشّخصيّة التي تتم دون علم المستخدم أو تمنعها، و كذالك تقنيات تتيح للمستخدم التّعامل مع البيئة الرّقمية بقدر من التخفي الملائم لأغراض الاستخدام.

4- ضرورة إيجاد قاعدة تعاون دولي فيما يتعلّق بحماية الحياة الشّخصية في البيئة الافتراضيّة.

5- ضرورة تدخل تشريعي لحماية المعلومات والبيانات الشّخصيّة بنصوص خاصة فلا يكفي التّوسيع من نطاق تطبيق النصوص التقليدية حتى لا يصطدم القاضي بمبدأ الشّرعية ويجد نفسه أمام أفعال وسلوكيات غير مجرّمة فيفلت فاعلوها من العقاب.

6- تخصيص وحدات أمنيّة لديها الإلمام الكافي بتقنيّات الحاسب، وذلك لا يتأتى إلا من خلال تكوين فرق وتعليمهم مبادئ وعلوم الحاسب الآلي وكيفية التعامل مع هذه الأجهزة في الضبط والتّحرّي عن هذه الجرائم، وتطوير وسائل البحث.

7- ضرورة استحداث نصوص قانونيّة جديدة خاصة في قانون الإجراءات الجزائيّة، حتى تتلاءم في مجال الضّبط والتحقيق لعدم ملاءمة الإجراءات التقليديّة في مواجهة هذه الجرائم إضافة إلى تحديث الأساليب الإجرائيّة المتّبعة في الجرائم المعلوماتيّة، دون أن تتعرض حقوق الأفراد وحرّياتهم للخطر عند الإثبات في مجالها.

8- إنشاء لجنة مختصّة على غرار اللّجنة الوطنية للمعلومات والحرّيات في فرنسا تتولى دراسة ظاهرة الإجرام المعلوماتي بكافة جوانبه، وتعمل على صياغة التعديلات التّشريعية اللازمة لاحتواء المشكلة، بالإضافة إلى تكليفها بمراقبة المعالجات الآلية للبيانات، ونشر التوعية لمستخدمي الحاسوب بفوائد ومخاطر التعامل به.

9- ضرورة عقد ملتقيات والتعاون المكثّف بين التّقنيّين والخبراء في الحقول الالكترونيّة مع ضبّاط الشّرطة القضائيّة والقضاة بشكل دوري ودائم، للاستفادة من خبراتهم وإرشاداتهم ابتداء من مرحلة التّحري والاستدلال وجمع الأدّلة وانتهاء بأحكام المحاكم، خاصة فيما يتعلق بالخبرة والشّهادة في المجال المعلوماتي.

وبالتالي فإن آلية حماية الحياة الشّخصيّة في مجال الانترنت تنطلق من:

* معرفة المخاطر التي تهدّد الحياة الشّخصيّة في بيئة الانترنت.
* إدراك السّلوكيات الملائمة و الحد الادنى من المهارات للتّعامل مع مصادر الخطر.
* توظيف وسائل وتقنيّات ملائمة لتفادي التّعدي ومنعه .

-تمّ بحمد الله تعالى-

قائمة المراجع

أولآ: الكتب

1- بوسقيعة أحسن، الوجيز في القانون الجنائي الخاص، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر 2008.

1-بولين أنطنيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة ط1، منشورات الحلبي الحقوقية لبنان 2009.

2-حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة "الحق في الخصوصية" دراسة مقارنة، دار النهضة العربية للنشر والتوزيع مصر 1978.

3-خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للطباعة والنشر والتوزيع، الجزائر 2010.

4-ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر 20111.

5-عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية، مصر 2005.

6-عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي، دراسة معمقة في القانون المعلوماتي ط1، دار الفكر الجامعي، مصر 2006.

7-علي أحمد الزعبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة ط1، المؤسسة الحديثة للكتاب، لبنان 2006.

8-علي جبار الحسيناوي، جرائم الحاسوب والانترنيت، الطبعة العربية، دار اليازوري العلمية للنشر والتوزيع، الأردن 2009.

9-عمرو عيسى الفقي، الجرائم المعلوماتية "جرائم الحاسب الآلي والانترنيت في مصر والدول العربية، المكتب الجامعي الحديث.

10- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط2، منشورات الحلبي الحقوقية، لبنان 2007.

11- محمد أحمد عبابنة جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن 2005.

12- محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية مصر 2004.

13- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنيت والجريمة المعلوماتية ط1، دار الثقافة للنشر والتوزيع، الأردن 2004.

14- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر مصر 2003.

15- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر 2007.

16- منير محمد الجنيهي ومحمود محمد الجنيهي، دار الفكر الجامعي، مصر 2005.

17- نعيم غبغب، حماية برامج الكمبيوتر، ط2، منشورات الحلبي الحقوقية لبنان 2009.

18- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات، ط1، دار الفكر الجامعي، مصر 2007.

19- هشام محمد فريد، الحماية الجنائية لحق الإنسان في صورته، مكتبة الآلات الحديثة، مصر د.س.ن.

قائمة المراجع:

I/ الكتب:

1-منحمد حسين منصور، المسولية الإلكترونية، دار الجامعة الجريدة للنشر، مصر 2003.

2-علي حياز الحسيناوي، جرائم الحاسوب والانترنيت، الطبعة العربية، دار اليازوري العلمية للنشر والتوزيع، الأردن 2009.

3-نعيم مغبغب، حماية برامج الكمبيوتر، ط2، منشورات الحلبي الحقوقية، لبنان 2009.

4-نبيلة هبه هروال، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالاتط1، دار الفكر الجامعي، مصر 2007.

5-عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، ط2، منشورات الحلي الحقوقية، لبنان 2007.

6-خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وشغرات، دار الهدى للطباعة والنشر والتوزيع، الجزائر 2010.

7-هشام محمد فريد، الحماية الجنائية لحق الإنسان في صورته، مكتبة الآلات الحديثة، مصر، د.س.ن.

8-محمد أحمد عبابنة، جرام الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن 2005.

9-محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، مصر 2004.

10- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي في دراسة متعمقة في القانون المعلوماتي، ط1، دار الفكر الجامعي، مصر، 2006.

11- منير محمد الجنيهي ومحمود محمد الجنيهي، دار الفكر الجامعي، مصر 2005.

12- بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، لبنان 2009.

13- علي أحمد الزعبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، ط1، المؤسسة الحديثة للكتاب، لبنان، 2006.

14- محمد خليفة الحماية الجنائية لمعطيات الحاسب الآلي، القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر 2007.

15- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، دراسة متعمقة في جرائم الحاسب الآلي والانترنيت، دار الكتب القانونية، مصر، 2005.

16- محمد أحسين أحمد الشوابكة، جرائم الحاسوب والانترنيت "الجريمة المعلوماتية"، ط1، دار الثقافة للنش والتوزيع، الأردن 2004.

17- عمر وعيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الأولي والانترنيت في مصر والدول العربية، المكتب الجامعي الجديد.

18- بوسقيعة أحسن الفقي، الوجيز في القانون الجنائي الخاص، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر 2008.

19- ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدىللطباعة والنشر والتوزيع، الجزائر، 2011.

20- حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة "الحق في الخصوصية" دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، مصر 1978.

ثانيا: الرسائل والمذكرات الجامعية

1-محمد محمد الرستي الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، رسالة دكتوراه، جامعة القاهرة، مصر د.س.ن

2-بوشكريط ريمة وآخرون، الأمن المعلوماتي، مذكرة تخرج لنيل شهادة الليسانس في ع ق إ، جامعة جيجل 2010، 2011.

ثالثا: المذكرات الإلكترونية

1-فوزي أوصديق، إشكالية المعلوماتية بين حق الخصوصية وإفشاء الأسرار المهنية، بحيث مقدمة لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 1 إلى 12 ماي 2003.

2-راسند بن سالم ليادي، التعدي على الخصوصية وجرائم الأخلاق والآداب العامة، ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الانترنيت، المنعقد في القاهرة بين 4 و 8 يونيو 2008.

3-سعد حماد صالح القبائلي، الجرائم الماسة بحق الإنسان في السمعة والشرف والاعتبار عبر الانترنيت، بحث مقدم إلى المؤتمر المغاربي حول المعلوماتية والقانون، ليبيا بين 28 و 29 أكتوبر 2009.

رابعا: النصوص القانونية

1-الأمر رقم66-156 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل والمتمم ج رسمية، عدد 49 المؤرخة في 11 يونيو 1966.

2-قانون رقم 2000-03 مؤرخ في 5 جمادى الأولى عام 1421 الموافق ل 5 غشت سنة 2000، تحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية،

ج ر عدد 48 المؤرخة في 6 جمادى الأولى عام 1421، الموافق ل 6 غشت سنة 2000.

الفهرس: