جامعة العربي التبسي - تبسة
كلية الحقوق والعلوم السياسية
قسم الحقوق

أطروحة مقدمة ضمن نيل شهادة دكتوراه الطور الثالث حقوق

تخصص: قانون جنائي اقتصادي

الحماية الجزائية للمستهلك في المعاملات الإلكترونية

إعداد الطالب:
جفالي حسين

إشراف الأستاذة:
الطاهر دلول

لجنة المناقشة:

الاسم واللقب		الرتبة العلمية	الجامعة الأصلية	الصفة في البحث
دنيا زاد ثابت		أستاذ محاضر ــ أ ــ	جامعة العربي التبسي ــ تبسة	رئيســـــــــا
الطاهر دلول		أستـــــــــــــاذ	جامعة العربي التبسي ــ تبسة	مشرفـــا ومقـــررا
لخضر بوكحيل		أستـــــــــــــاذ	جامعة باجي مختار ــ عنابة	عضوا مناقشا
سعاد نويري		أستاذ محاضر ــ أ ــ	جامعة العربي التبسي ــ تبسة	عضوا مناقشا
حبيبة عبدلي		أستاذ محاضر ــ أ ــ	جامعة عباس لغرور ــ خنشلة	عضوا مناقشا
هشام بخوش		أستاذ محاضر ــ أ ــ	جامعة محمد الشريف مساعدية ــ سوق أهراس	عضوا مناقشا

السنة الجامعية: 2020/2019

إهداء

إلى أمي الحبيبة و قرة عيني **مسعود اليامنة**

إلى أحبائي إخوتي و أخواتي و أولادهم

إلى كل أحبتي و أصدقائي

إلى أساتذة و عمال كلية الحقوق و العلوم السياسية

إلى كل من ساعدني في إنجاز هذا البحث

كلمة شكر

بمقتضى واجب التقدير و العرفان أن أتوجه

بالشكر الجزيل إلى أستاذي الفاضل

الأستاذ الدكتور دلول الطاهر

الذي شرفني بإشرافه على إنجاز هذه الأطروحة

و على كل توجيهاته و إرشاداته و نصائحه...

كما لا يسعني إلا أن أتقدم بجزيل الشكر و الاحترام

لأعضاء لجنة المناقشة

جزا الله الجميع كل خير

مقدمة

أدت ثورة تكنولوجيا الاتصال و المعلومات أو ما يعرف بالثورة الرقمية، و ما رافقتها من تطور علمي و تقني كبير لتغييرات كبيرة مست أغلب القطاعات و المجالات، و زحما فكريا لم تقف حدوده على البعد التقني بل كان له تأثيره الاقتصادي و القانوني أيضا، و لعل أهم هذه التطورات التي غيرت وجه عالم التعاقدات و الأعمال و خلقت فرصا متنامية للمعاملات الإنسانية أجهزة الحاسوب.

إذ شهد عالم الحاسبات الآلية تطورات واسعة النطاق، انتهت بإمكانية ربط بعضها مع بعض عن طريق شبكات حاسوبية بين المحلي و العالمي، تصل بين حواسيب حول العالم بتقنيات مختلفة لتصنع طفرة في عالم وسائل الاتصال المسماة شبكة الإنترنت العالمية[1]، مما سهل تبادل المعلومات و توفرها في أي جزء من أجزاء المعمورة، و هو ما أفضى إلى تغير من المفاهيم التقليدية للتجارة و أبرزت شكل آخر لمجتمع المعلومات و هو ما يعرف بالمعاملات التجارية الإلكترونية[2].

[1] - تعرف الإنترنت لغة بأنها كلمة جديدة في القاموس اللغوي لمختلف لغات العالم، و هيا كلمة إنجليزية مركبة و مختصرة من مقطعين (inter) و هي اختصار (international) و تعني دولي، و (net) و هيا اختصار لكلمة net) (work و التي تعني الشبكة. و بجمع الكلمتين أي international network فإن المعنى الكامل المتحصل عليه هو الشبكة الدولية. و تعرف على أنها شبكة عالمية تجمع بين وسائل الاتصالات و الحواسيب، و هيا مخصصة لتبادل البريد الإلكتروني للمعلومات المتعددة الوسائل و الملفات، و هي تشتغل وفقا لبروتوكول مشترك، يسمح بسيرورة إرسال الرسائل المنقسمة إلى طرود مستقلة. **أنظر هروال هبة نبيل، جرائم الأنترنت دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2014، ص 02.**

[2] - تعددت التعريفات لمصطلح التجارة الإلكترونية ، فمنها من عرفها على بالنظر لأطراف العلاقة التجارية على أنها "تنفيذ بعض أو كل المعاملات التجارية في السلع أو الخدمات، التي تتم بين مشروع تجاري و آخر، أو بين مشروع تجاري و مستهلك، و ذلك باستخدام تكنولوجيات المعلومات و الاتصالات". **أنظر**

Alain BENSOUSSAN: Le commerce électronique: aspects juridiques, Editions Hermès, Paris 1998.

و اعتمد جانب آخر في تعريفه على الوسيلة المستخدمة في العملية التجارية فعرفت كما يلي " تلك الأنشطة التجارية التي تدار عبر شبكة دولية متصلة إلكترونيا بأجهزة كمبيوتر". **أنظر**

Jérôme HUET: La problématique juridique du commerce électronique, Colloque « Droit et Commerce », Deauville, 2000, p 2.

فأصبحت المعاملات الإلكترونية أحد الركائز الأساسية للتبادل التجاري و للنمو الاقتصادي في معظم دول العالم في هذا القرن، كما تعد أيضا أحد دعائم الاقتصاد الرقمي، فمعظم الشركات التجارية الكبرى تبنت أسلوب التجارة الإلكترونية[3]، حيث يم استخدام الوسائط الإلكترونية لعرض السلع و الخدمات، و إجراء البيع و الشراء من خلال شبكة الأنترنت، و تنفيذ عمليات الدفع لقيمتها عن طريق البطاقات و النقود الإلكترونية، أو بغيرها من وسائل النقل الإلكتروني للأموال[4].

و بذلك اصبح بإمكان المستهلك، أن يقوم بطلب السلع و الخدمات عن طريق شبكة الأنترنت بسهولة و يسر، و أن يدفع ثمنها إلكترونيا، و يتلقى الشروحات الوافية حول مواصفاتها و أنواعها عبر شاشة الحاسوب الخاص به، و هذا دون مغادرة مكان الجلوس، و هذا ما يسمى بالتعاقد عن بعد. حيث يتم ذلك عن طريق تلاقي إرادة المهني، و إفراغها في عقد يكون على شكل مستند أو محرر معد نموذجه مسبقا في غالب الأحيان، أو يعد بعد إرسال المستهلك لبياناته و معلوماته الشخصية، و التوقيع عليه إلكترونيا فيما بعد، مما يتطلب توفير الثقة و الأمان فيه، و تنفيذ الالتزامات المتفق عليها تطبيقا لمبدأ حسن النية.

إلا أنه و بالرغم من الأهمية الكبيرة للمعاملات الإلكترونية، و ما توفره من مزايا و امتيازات للمستهلك الإلكتروني من أجل تلبية حاجياته المختلفة عبر شبكة الإنترنت، إلا أن ذلك لا يخلو من المخاطر العديدة، إذ يعتمد هذا النوع من المعاملات على عرض السلع و الخدمات بواسطة الإعلانات التجارية الإلكترونية، و التي يشوبها في أغلب الأحيان الكذب و التضليل من أجل التأثير على نفسية المستهلك و دفعه إلى التعاقد، كما يعتمد أيضا على

---

[3] - تستطيع الشركات من خلال موقعها على الإنترنت تحقيق تسويق أفضل لمنتجاتها و أكثر فاعلية من خلال الوصول إلى عدد هائل من المستهلكين على مستوى العالم و في مدة 24 ساعة، حيث يمكنها تلقي طلبات المستهلكين في أي ساعة من ساعات الليل أو النهار و الرد عليها في الحال.

[4] - الدفع الإلكتروني: هو منظومة متكاملة من النظام و البرامج التي تهدف إلى تسهيل إجراءات الدفع الإلكتروني و هو المال أو العملة التي تتبادل بصفة إلكترونية. و تعمل هذه المنظومة تحت مظلة من القوانين التي تضمن سرية تأمين و حماية إجراءات الشراء و ضمان وصول الخدمة. **خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2012، ص 8.**

تقديم البيانات الشخصية للمستهلك لإتمام إجراءات التعاقد، حيث يمكن أن تتعرض هذه البيانات إلى الاعتداء عليها سواء من قبل التاجر أو من طرف الغير.

كما تعتمد المعاملات الإلكترونية أيضا على التوقيع عليها بنفس النمط من أطرافه حتى يكتسب الصفة و الحجية القانونية، أين يمكن أن يتعرض هذا التوقيع الإلكتروني إلى الاعتداء، بالإضافة إلى أن المستهلك في المعاملات الإلكترونية لا يملك فرصة الاطلاع على السلع أو نوعية الخدمة إلا بعد الوصول إليه، فإن ذلك من شأنه أن يسمح لبعض المنتجين و البائعين باللجوء إلى الغش من أجل تحقيق الربح، و لو بتعريض صحة المستهلك و امنه إلى الخطر.

لذا أصبحت هذه الاعتداءات تشكل هاجسا كبيرا يهدد مكاسب الثورة الرقمية ليس فقط بالنسبة للمستهلكين، أو في إطار محلي محدود، بل على مستوى واسع و في فضاء دولي مفتوح، بسبب تطورها و ازدياد حجمها بعلاقة طردية مع تطور المعلوماتية جعلها تأخذ طابعا جرميا لمساسها بمصالح محمية جنائيا.

إذ تعتبر ظاهرة الاعتداءات الماسة بالمستهلك في المعاملات الإلكترونية من الظواهر التي افرزها النظام العالمي الجديد، حيث بدأت في الظهور و الانتشار و ارتبطت بتكنولوجيا متطورة هي تكنلوجيا الحاسبات الآلية، و نتيجة تميزها بمجموعة من السمات و الخصائص جعلتها تختلف عن غيرها من الجرائم الأخرى مما ترتب عليه ضرورة التعامل معها بما يتلاءم مع هذه المميزات، لذلك تكتسي حماية المستهلك جزائيا في المعاملات الإلكترونية أهمية في مختلف التشريعات المقارنة الصادرة في هذا الشأن، حيث كرست مبدا حماية المستهلك من المخاطر التي يتعرض لها في المعاملات الإلكترونية[5].

[5] - قامت لجنة الأمم المتحدة للقانون التجاري الدولي بإصدار القانون النموذجي للتجارة الإلكترونية سنة 1966، كقانون استرشادي يمكن من خلاله الاستفادة منه كأساس عند إصدار التشريعات الوطنية للتجارة الإلكترونية، بما فيها حماية المستهلك. كما أصدر الاتحاد الأوربي مجموعة من التوجيهات كالتوجيه الأوروبي رقم 97-07 المتعلق بحماية المستهلك في العقود عن بعد.
كما اهتمت بعض الدول بحماية المستهلك في المعاملات الإلكترونية كقانون المبادلات و التجارة التونسي لعام 2000.

أهمية الموضوع

تكتسي دراسة موضوع الحماية الجزائية للمستهلك في المعاملات الإلكترونية أهمية بالغة باعتبارها من أهم أنواع الحماية التي يلجأ إليها المشرع كلما عجزت أنواع الحماية الأخرى عن حماية حق أو مصلحة ما، و باعتبارها الحماية الأنجع لتأمين المصالح و الحقوق و فرض الاحترام لها، و بالتالي من شأن تحديد أبعادها في ظل البيئة الرقمية التي تجري من خلالها العمليات التجارية الإلكترونية، أن تصبح هذه الأخيرة محور التعامل الدولي، و هو أمر لا يخلوا من الأهمية سواء العلمية أو العملية.

فالفائدة العملية من موضوع البحث ، تتبلور في ارتباط الموضوع بنوع من التجارة تتنامى و تتزايد يوما بعد يوم، و باتت واقعا ملموسا في حياة الأفراد و الدول على حد سواء، كونها أضحت المنفذ الهام للتجارة المحلية و الدولية هذا جهة، و مكانة المستهلك، باعتباره الطرف الضعيف في العلاقة الاستهلاكية و ما يتعرض له من مخاطر كبيرة، فكثيرا ما يتعرض للغش عند إبرام العقود الإلكترونية، نظرا لأن اغلب عقود التجارة الإلكترونية تكون خارج إقليم الدولة مما يجعله عرضة لهذه المخاطر.

و أما الأهمية العلمية و إن صح التعبير القانونية، فتتمثل في استيعاب المسائل القانونية لمثل هذه المعاملات، و ذلك على المستوى الجنائي، و حل إشكالياتها التي قد تمثل عقبات أمام استخدام الأنترنت في العمليات التجارية، هذا كله من ناحية، و من ناحية أخرى تسليط الضوء على هذا الجانب الهام من المعاملات على الأنترنت و هو المستهلك الإلكتروني لما يترصد به من مخاطر و أهمية في مجال التجارة بوجه خاص و الاقتصاد بوجه عام و محاولة وضع حماية جنائية له، خاصة مع وجود تنظيم قانوني وطني ينظم هذه المسألة حديث النشأة، بالرغم أن معظم دول العالم الأجنبية بل و العربية قد سبقتنا في هذا المجال.

أهداف الدراسة

و من خلال الأهمية التي تنبثق منها هذه الدراسة، نهدف للبحث في موضوع الحماية الجزائية للمستهلك في المعاملات الإلكترونية إلى:

-بيان النطاق التشريعي لحماية المستهلك الإلكترونية من الجرائم الواقعة عليه في المعاملات الإلكترونية.

-تحديد الجرائم الماسة بالمستهلك في المعاملات الإلكترونية ضمن قانون العقوبات و القوانين المكملة له.

- تحديد الجهات القضائية المختصة في متابعة الجرائم الماسة بالمستهلك في التعاملات الإلكترونية

-تبيان طرق الحصول على الدليل الخاص بالكشف على الجرائم الماسة بالمستهلك في المعاملات الإلكترونية.

-تبيان مدى مشروعية هاته الأدلة المتحصل عليها أما القضاء الجنائي.

إشكالية البحث:

مما لا شك فيه أن هذا النوع الحديث من المعاملات عبر شبكة الإنترنت أحدث قلقا تشريعيا على المستوى الدولي و المستوى الداخلي على حد سواء، و بات التساؤل عن كيفية مواجهة هذه التحديات التي تطال المستهلك أمر لا غنى عنه، و أصبحت إعادة النظر لنظمنا التقليدية ضرورة ملحة إزاء ثورة معلوماتية غيرت أنماط حياة الأفراد، و عودتهم على اتباع طرق و أساليب في المعاملات لم تكن معلومة لديه من قبل.

لذلك سنحاول حصر دراستنا للموضوع في إطار بحث **ما مدى نجاعة التشريع الجزائي لتقرير و إرساء حماية جزائية للمستهلك في المعاملات الإلكترونية.**

أسباب اختيار الموضوع

و دفعنا لاختيار موضوع الحماية الجزائية للمستهلك في المعاملات الإلكترونية عدة أسباب يمكن إرجاعها إلى أسباب ذاتية و أخرى موضوعية.

فالأسباب الذاتية في اختيار موضوع الحماية الجزائية للمستهلك في المعاملات الإلكترونية تكمن في عامل الحداثة، و هذا راجع لحداثة تبني المشرع الجزائري لهذا النوع المستحدث من المعاملات، الذي أردنا من خلاله كشف مواطن القوة و الضعف في النصوص المرتبطة بحماية المستهلك جنائيا في المعاملات الإلكترونية.

أما الأسباب الموضوعية فتكمن في الخطر الذي يتعرض له المستهلك في هذا النوع المستحث من المعاملات، كون المستهلك عاجزا عن فحص البضاعة و معاينتها، و جاهل تمام لهوية المهني، هذا من جهة، و من جهة أخرى قد يتغاضى هذا الأخير عن سلامة و أمن المستهلك بإيهامه بمزايا غير حقيقية في إنتاجه مما يجعله عرضة للتلاعب بمصالحه، كما يكون مصدر الخطر غير صاحب الخدمة من خلال اختراق الشبكات الإلكترونية المخزنة عليها البيانات و سرقة هذه المعلومات و إعادة استخدامها على نحو يضر بالمستهلك ، فأصبحت الحاجة ملحة لوجود تشريع جنائي لمواجهة كل الاعتداءات الواقعة على المستهلك و مسايرة التطور السريع اللامحدود و اللامتناهي، فالثقة في هذه المعاملات أكثر ما يحتاج إليه المستهلك في سبيل تلبية احتياجاته الشخصية.

منهجية البحث

نظرا لخصوصية الموضوع و أهميته و تشعب القضايا التي يتطرق لها، فقد اعتمدنا لخوض غماره على المنهج التحليلي بصفة أساسية، و الذي يقوم على جمع المعلومات و النصوص القانونية و الآراء الفقهية و وضعها تحت مجهر التقييم و النقد، و لما له من خاصية فهم النصوص القانونية خاصة في المواضيع التي تخلو منها الدراسة.

و نظرا لاحتواء الموضوع على العديد من المصطلحات و المفاهيم الجديدة فسيتم الاستعانة بالمنهج الوصفي لتوضيح هذه المفاهيم و المصطلحات و بيان موقف الفقه و التشريع منها، كما أنا سنلجأ في كثير من الأحيان إلى الاعتماد على المنهج المقارن ، محاولة منا لكشف محاسن و عيوب النصوص الجنائية الحامية للمستهلك و معرفة موقف التشريعات المقارنة منها .

صعوبات البحث

و من خلال دراستنا لموضوع الحماية الجزائية للمستهلك في المعاملات الإلكترونية واجهتنا العديد من الصعوبات يتعلق بعضها بحصر نطاق الموضوع كون الجرائم الماسة بالمستهلك متنوعة و تتوزع بين عدة قوانين، الأمر الذي يتعذر معه الوصول بسهولة إلى تقسيم مناسب لهذه الجرائم.

و من أكثر التحديات التي واجهتنا تلك المتعلقة بالحماية الموضوعية للمستهلك في المعاملات الإلكترونية نظرا لحداثة تنظيم المشرع الجزائري لهذا التطور الحاصل في مجال المعاملات الإلكترونية، هذا من جهة و من جهة أخرى حداثة المصطلحات المتعلقة بالمعاملات الإلكترونية و ذلك لاتصالها بجوانب فنية و تقنية تتسم بالدقة، و تستوجب الإحاطة ببعض المعارف و المعلومات المتخصصة للحصول على حد أدنى من المعرفة التقنية بنظم المعلوماتية و الحواسيب، و بالتالي الوصول إلى تصور صحيح و إجاد حلول للمشاكل القانونية التي تطرحها الحماية الجزائية للمستهلك في هذا النوع المستحدث من المعاملات.

ثم إن قلة البحوث التي عالج تدخل القانون الجنائي في مجال حماية المستهلك في المعاملات الإلكترونية خلق صعوبات أخرى، و إن كنا لا ندعي السبق في طرح هذا الموضوع إلا أن الخوض في معالجة الإشكاليات التي تثيرها الجرائم الماسة بالمستهلك في المعاملات الإلكترونية و فك التداخل بين نصوصها قابله قلة الدراسات السابقة أو كانت معالجة بشكل غير تام.

خطة البحث

للإلمام بموضوع الدراسة و تحقيقا لأهدافها، و إجابة على الإشكالية التي وضعناها للموضوع. فقد رأينا تقسيمه إلى بابين على النحو التالي:

الباب الأول: الحماية الجزائية الموضوعية للمستهلك في المعاملات الإلكترونية

الفصل الأول: الحماية الجزائية الموضوعية للمستهلك من الغش التجاري في المعاملات الإلكترونية

المبحث الأول: الحماية الجزائية الموضوعية للمستهلك قبل إبرام العقد الإلكتروني

المبحث الثاني: الحماية الجزائية الموضوعية للمستهلك في مرحلة ما قبل التعاقد الإلكتروني

الفصل الثاني: الحماية الجزائية الموضوعية لمتطلبات المستهلك في المعاملات الإلكترونية

المبحث الأول: الحماية الجزائية للبيانات الشخصية للمستهلك في المعاملات الإلكترونية

المبحث الثاني: الحماية الجزائية لتوقيع المستهلك في المعاملات الإلكترونية

الباب الثاني: الحماية الجزائية الإجرائية للمستهلك في المعاملات الإلكترونية

الفصل الأول: تنظيم قواعد الاختصاص لنظر الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

المبحث الأول: انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

المبحث الثاني: التعاون الدولي كألية لانعقاد الاختصاص في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

الفصل الثاني: إثبات الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

المبحث الأول: إجراءات ضبط الجرائم الماسة بالمستهلك في العاملات الإلكترونية

المبحث الثاني: حجية الدليل الإلكتروني في إثبات الجرائم الماسة بالمستهلك في العاملات الإلكترونية

الباب الأول: الحماية الجزائية الموضوعية للمستهلك في المعاملات الإلكترونية

مع بداية انتشار الأنترنت وتنامي استخدامه في المعاملات التجارية الإلكترونية، ازدادت مع الوقت الجرائم المصاحبة لاستعمال الشبكة وتعددت صورها وأشكالها الإلكترونية، وشاعت طائفة جديدة أو مستحدثة من الإجرام المعلوماتي خاصة تلك التي تستهدف فئة المستهلكين، سواء تلك المتعلقة بتداول السلع و الخدمات أو بمتطلبات هذا الأخير في إتمام المعاملة الإلكترونية، و هو ما يفند في النهاية أهم وأخطر التحديات و المسائل الجنائية التي تواجه المعاملات الإلكترونية، والذي يؤثر سلبا من الناحية الاقتصادية على حجم هذه المعاملات.

و لما كان هذا النوع المستحدث من الجرائم المعلوماتية يشكل تهديدا و تحديا خطيرا على اقتصاد الدول بصفة عامة و مصالح المستهلك الإلكتروني خاصة، كان لازما على المشرع الوطني توفير الحماية للمستهلك الإلكتروني و ذلك بوضع نصوص تجرم كل اعتداء عليه في هذا النوع من المعاملات الإلكترونية، باعتبار التجريم و العقاب هو الآلية القانونية التي توفر أكبر قدر من الحماية، و بوصفه آلية ردعية لما تحمله من جزاءات تمس بحريات الأفراد و ذمتهم المالية.

وعليه سنبحث في هذا الباب الحماية الجزائية الموضوعية التي أقرها المشرع الوطني للمستهلك في المعاملات الإلكترونية من خلال الحماية الجزائية الموضوعة للمستهلك من الغش التجاري في المعاملات الإلكترونية (الفصل الأول)، الحماية الجزائية الموضوعية لمتطلبات المستهلك في المعاملات الإلكترونية (الفصل الثاني).

الفصل الأول: الحماية الجزائية الموضوعية للمستهلك من الغش التجاري في المعاملات الإلكترونية

يعتبر الغش التجاري الإلكتروني أحد أشكال الظواهر الإجرامية المستحدثة التي انتشرت في الآونة الأخيرة، و قد أصبحت تهدد أمن الأفراد، و هذا بسبب التطور المتسارع في وسائل التقنية الحديثة، و تزداد استخدام العديد من الحكومات و الأفراد لهذه التقنية كعنصر أساسي في إتمام المعاملات الإلكترونية، مما يشكل فرصة سانحة و بيئة خصبة أما المجرمين للقيام بعمليات الغش.

و إزاء ما يتميز به التعاقد الإلكتروني من مراحل يتبعها المستهلك الإلكتروني[1] لإتمامه، ظهرة أشكال متعددة من الغش التجاري، كتسليم سلعة غير المتفق عليها أو معيبة، أو عدم إعلام المستهلك بجميع عناصرها، أو عدم تنفيذ بنود الضمان المتفق عليها، أو خداع المستهلك فيها...الخ.

و عليه سوف نحاول دارسة حماية المستهلك من الغش التجاري في المعاملات الإلكترونية من خلال تقسيم مراحل التعاقد إلى حماية المستهلك من الغش التجاري في مرحلة ما قبل التعاقد الإلكتروني (المبحث الأول)، و حماية المستهلك من الغش التجاري في مرحلة إبرام العقد الإلكتروني (المبحث الثاني).

[1]– اختلف الفقه في وضع تعريف للمستهلك ، فهناك من وسع في تعريفه و منهم من ضيقه، فالمستهلك حسب التعريف الموسع هو كل شخص يتعاقد بهدف الاستهلاك أي بهدف استعمال أو استخدام مال أو خدمة. أما التعريف الضيق للمستهلك فهو كل شخص يتعاقد لأجل إشباع حاجته الشخصية أو العائلية ، غير مرتبطة بنشاط مهني. **أنظر رمزي بيد الله على حجازي، الحماية المدنية للمستهلك بعد التعاقد الإلكتروني، منشورات الحلبي الحقوقية، لبنان، 2016، ص 19–21.**

و لقد أخذ المشرع الجزائري بالمفهوم **الضيق للمستهلك الإلكتروني** من خلال المادة 06 من قانون التجارة الإلكتروني، فالمستهلك حسب هذا القانون هو كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الاتصالات الإلكترونية من المورد الإلكتروني بغرض الاستخدام النهائي.

المبحث الأول: الحماية الجزائية الموضوعية للمستهلك من الغش التجاري الإلكتروني في مرحلة ما قبل التعاقد الإلكتروني

اهم ما يحتاجه المستهلك في المرحلة السابقة لإبرام العقد، هو ذلك الكم من المعلومات و البيانات الخاصة بالسلع أو الخدمة المطلوبة للوقوف على حقيقة مصالحه، و ما ينتج من ذلك من آثار إيجابية في إعادة التوازن النسبي للعلاقة العقدية. و من أجل ذلك فإن التزام المهني بإعلام المستهلك يعد ابرز الآليات القانونية في مجال حماية المستهلك، و الأكثر إلحاحا في مجال عقود التجارة الإلكترونية[1]، التي يتم التعاقد فيها عن بعد.

و من ناحية أخرى، فالمنتج الإلكتروني عادة ما يعتمد أساليب ترويجية لتسويق منتجاته و أهمها الإشهار الإلكتروني، إذ يعتبر هذا الإشهار أداة لتعريف المستهلك بالسلع و الخدمات الحديثة، و طرق الوصول إليها و أماكن تواجدها، إلا أنها قد تعرض المستهلك في أغلب الأحيان لعمليات تضليل، و تجره إلى شراء منتجات لا تلبي رغباته بالقدر الذي تم الإشهار عنها، فيعتبر الإشهار الإلكتروني في هذه الحالة غير مشروع، كما أن عدم المشروعية في الإشهار لا يتوقف على تضليل المستهلك حول المنتجات، بل

---

[1]- **عرف العقد الإلكتروني** التوجيه الأوروبي رقم 97/07 المؤرخ في 20 ماي 1997 المتعلق بحناية المستهلك في العقود المبرمة عن بعد بأنه " عقد متعلق بالسلع و الخدمات يتم بين مورد و مستهلك من خلال الإطار التنظيمي الخاص بالبيع عن بعد أو تقديم الخدمات التي ينظمها المورد، و الذي يتم باستخدام واحد أو أكثر من وسائل الاتصال الإلكترونية حتى إتمام العقد".

أما فقهيا فقد عرف بأنه " التقاء إيجاب صادر من الموجب بشأن عرض مطروح بطريقة إلكترونية سمعية أو مرئية أو كليهما على شبكة الاتصالات و المعلومات، بقبول مطابق له صادر من الطرف المقابل بذات الطرق بهدف تحقيق عملية أو صفقة معينة يرغب الطرفان في إنجازها. **أنظر خالد ممدوح إبراهيم العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2005، ص 51.**

أما المشرع الجزائري فقد نص على تعريفه من خلال المادة 06 من قانون التجارة الإلكترونية ، على أنه كل عقد بمفهوم القانون 04-02 و يتم إبرامه عن بعد دون الحضور الفعلي و المتزامن لأطرافه باللجوء حصريا لتقنية الاتصالات الإلكترونية. و بالرجوع إلى القانون 04-02 المحدد للقواعد المطبقة على الممارسات التجارية نجد أن المادة 03 منه تعرف العقد على أنه كل اتفاق أو اتفاقية تهدف إلى بيع سلعة أو تأدية خدمة حرر مسبقا من أحد أطراف الاتفاق مع إذعان الطرف الآخر بحيث لا يمكن لهذا الأخير إحداث تغيير حقيقي فيه.

يتعدى ذلك من خلال التصدي للإشهار الإلكترونية غير المرغوب فيه الذي يتم عبر البريد الإلكتروني، لما تسببه من مضايقة للمستهلك و اعتداء على حياتهم الخاصة[1].

ومن هنا فقد أضحت حماية المستهلك جنائيا من الغش التجاري في المرحلة السابقة للتعاقد الإلكتروني من الأولويات المهمة في المعاملات التجارية الإلكترونية، و التي سعى المشرع الجزائري كغيره من التشريعات المقارنة لتوفيرها للمستهلك، و ذلك من خلال إقرار المسؤولية الجزائية للمورد الإلكتروني عن نشره لإشهارات إلكترونية غير مشروعة (المطلب الأول). كما ألزام المورد الإلكتروني بإعلام المستهلك في المعاملات الإلكترونية و قيام مسؤوليته عند مخالفة هذا الالتزام (المطلب الثاني).

[1] – د/ أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني ، دراسة مقارنة، دار الكتب القانونية، مصر، 2008، ص 99.

المطلب الأول: الحماية الجنائية للمستهلك من الإشهار التجاري الإلكترونية غير المشروع.

عادة ما تكون الأعمال التجارية الإلكترونية مسبوقة بشكل من أشكال الإشهار الإلكتروني، حيث يسعى المتدخل عادة لدى إبرام عقد التجارة الإلكترونية إلى ترويج منتوجاته، بهدف تعريف المستهلك بمزايا منتوجاته و خدماته.

غير أن لحرية الإشهار التجاري الإلكتروني حدود لا ينبغي تخطيها فإذا اختار المتدخل ترويج منتوجاته، فإنه ملزم بأن يكون الإشهار صادقا، و ألا يكون مخالفا للقوانين، و إلا أصبح يشكل مصدر خطورة حقيقية على المستهلك.

و لأهمية الإشهار التجاري في المعاملات الإلكترونية سعى المشرع الجزائري إلى تنظيمه مفردا له الفصل السابع من القانون 18-05 المتعلق بالتجارة الإلكترونية[1]، و نظرا لما يؤدي إليه الإشهار التجاري الإلكترونية غير المشروع من خداع ومساس بمصالح المستهلك الاقتصادية و سلامته، أقر المشرع المسؤولية الجزائية للمورد الإلكتروني الذي يخالف هذا التنظيم معتبرا إياه إشهار إلكترونيا غير مشروع. و من أجل تحديد هذه الحماية الجنائية للإشهار الإلكتروني غير المشروع وجب تحديد الإشهار التجاري الإلكتروني بصورة عامة (الفرع الأول)، وتحديد صور التجريم الواقعة على الإشهار التجاري الإلكتروني غير المشروع (الفرع الثاني).

الفرع الأول: ماهية الإشهار التجاري الإلكتروني

لقد أصبح الإشهار التجاري الإلكتروني أحد أهم صور الثورة المعلوماتية، إذ أن الأعمال التجارية الإلكترونية بصفة عامة تكون مسبوقة بشكل من أشكال الدعاية، حيث يحتوي الإشهار التجاري عن التعريف بمنتجات وخدمات و يدعو المستهلكين للتعاقد، مما دعا التشريعات و رجال الفقه لوضع مفهوم له (الفقرة الأولى)، كما أن لهذا النوع من الإشهار التجاري عدة أشكال تصل بها للمستهلكين (الفقرة الثانية).

[1]- قانون رقم 18-05 مؤرخ في 10 مايو سنة 2018، يتعلق بالتجارة الإلكترونية، جريدة رسمية، عدد 28، صادرة في 16 مايوا 2018.

الفقرة الأولى: مفهوم الإشهار التجاري الإلكتروني

يعد التسويق باستخدام الإشهار الإلكتروني من أهم وأفضل الطرق التي قد تستخدمها الشركات لتنفيذ خططها التسويقية، فيستخدم الإشهار الإلكتروني كوسيلة ترويجية لمختلف السلع و الخدمات التي تعرضها الشركات عبر الأنترنت، لذلك سعت التشريعات و رجال الفقه إلى تعريف وتحديد خصائصه. وعليه سوف نتطرق لتعريف الإشهار الإلكتروني (أولا) و نحدد خصائصه (ثانيا).

أولا: تعريف الإشهار التجاري الإلكتروني

تعددت التعريفات المنصبة على الإشهار التجاري الإلكتروني سواء على مستوى التشريعات أو من طرف رجال الفقه، و سنحاول تبيان كل منهما على النحو التالي:

1-التعريف التشريعي للإشهار التجاري الإلكتروني:

عرف الإشهار في التوجيه الأوربي رقم 450/84 الصادر بتاريخ 1984/09/10، الخاص بالتقارب بين النصوص التشريعية و اللائحية والإدارية للدول الأعضاء بأنه " كل شكل من أشكال الاتصال الذي يتم في مجال الأنشطة التجارية أو الصناعية والحرفية أو المهنية وتهدف إلى تشجيع الإقبال على السلع والخدمات بما في ذلك العقارات و الحقوق والالتزامات المرتبطة بها"[1].

و ذات الأمر في التوجه الخاص بالإعلانات المضللة والمقارنة الصادر في أكتوبر 1998 ، حيث عرف في المادة 1/2 منه بأنه" كل شكل من أشكال الاتصال يتم في نطاق الأنشطة التجارية و الصناعية و الحرفية بهدف الترويج عن السلع والخدمات بما فيها الحقوق غير المالية و الحقوق والالتزامات"[2].

[1] – خميخم محمد، الحماية الجنائية للمستهلك في عقود التجارة الإلكترونية – دراسة مقارنة– ، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2017، ص 27.

[2] – شريف محمد غنام النظام القانوني للإعلانات عبر شبكة الأنترنت، دار الجامعة الجديدة ، الإسكندرية، مصر، 2008، ص 26

فالملاحظ تبنى التوجيه الأوربي الصادر عام 1984 و المعدل بالتوجيه رقم 55 لسنة 1997 بالمفهوم الموسع للإعلانات التجارية، فلكل منهما نطاق عام وينطبقان من ثم على الإعلان الإلكتروني.

و قد حرص التوجيه الأوربي الخاص بالتجارة الإلكترونية الصادر سنة 2000 على تبني ذات المفهوم عند استخدام مصطلح الاتصال التجاري، وعرف الإعلان المتعلق بالتجارة الإلكترونية في المادة الثانية بأنه" كل البيانات والمعلومات التي تقدمها الشركات والمؤسسات أو حتى الأفراد متى تعلقت بسلع وخدمات، و كانت هذه المعلومات تتضمن ترويجا للسلع و الخدمات بهدف جذب أكبر قدر من العملاء و حثهم على شرائها". وقد اشترط التوجه الأوربي ارتباط هذه البيانات والمعلومات بأنشطة المؤسسة أو الفرد حتى تكون إعلانا أما اذا ارتبطت بشخصه لا تعد إعلانا[1].

أما التشريعات الوطنية فقد اختلفت في إعطاء تعريف للإشهار التجاري الإلكتروني، حيث نص المشرع البلجيكي في المادة 22 من قانون التجارة الإلكترونية و حماية المستهلك الصادر في 14 يوليو 1991، على أن الإعلان التجاري هو " كل دعاية تهدف بصفة أساسية إلى تشجيع بيع المنتجات و الخدمات ... أيا كانت هذه الدعاية أو الوسيلة المستخدمة. متبنيا بذلك المفهوم الموسع للإعلان و ذلك باعتباره كل شكل من أشكال الدعاية يؤدي إلى تشجيع بيع المنتجات و الخدمات[2].

في حين عرفته المادة 35 من القانون 40 لسنة 1998 التونسي بأنه[3] " كل عملية اتصال تهدف بصفة مباشرة أو غير مباشرة إلى تنمية بيع منتوج أو سداد خدمات مهما كان المكان أو وسائل الاتصال المعتمدة." .

---

[1] – علاء عمر محمد الجاف، الآليات القانونية لحماية المستهلك في التعاملات الإلكترونية، منشورات الحلبي الحقوقية، لبنان، 2017، ص160.

[2] – مصطفى موسى العطيات، الجوانب القانونية لتعاملات التجارة الإلكترونية، دار وائل للنشر و التوزيع، عمان، الأردن، 2010، ص 49.

[3] – القانون 40 لسنة 1998 المتعلق بطرح البيع و الإشهار التجاري التونسي، الرائد الرسمي، العدد 44، مؤرخ في 2 جوان 1998.

أما المشرع الجزائري فقد عرف الإشهار التجاري الإلكتروني من خلال نص المادة 6 من قانون 18-05 المتعلق بالتجارة الإلكترونية، على أنه " كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع سلع أو خدمات عن طريق الاتصال الإلكتروني[1]."

و الملاحظ أن هذا التعريف لم يأتي بالجديد، حيث أن قانون الممارسات التجارية رقم 04-02 المحدد للقواعد المطبقة على الممارسات التجارية، قد أورد نفس التعريف[2] و أوسع منه نطاقا، حيث أنه لم يحدد وسائل الإشهار بل جعلها بكل وسائل الاتصال المستعملة، و بذلك يشمل كل من الوسائل التقليدية و وسائل الاتصال الإلكترونية و كل وسيلة قد تظهر مسايرة لتقدم التكنلوجي.

كما أن المشرع الوطني لم يعرف الإشهار التجاري الإلكتروني ذاته، و إنما عرف الهدف منه و هو ترويج لبيع سلعة أو خدمة، غير أن القانون رقم 14-04 المؤرخ في 2014/02/24 و المتعلق بالنشاط السمعي البصري[3] أتي بتعريف حقيقي للإشهار، على أنه أي شكل مصمم أو رسالة محررة أو صوتية أو سمعية بصرية تبث مقابل أجر أو تعويض، سواء من أجل ترقية تقديم سلع أو خدمات في إطار نشاط تجاري أو صناعي أو حرفي أو مهنة حرة أو من أجل ضمان ترقية تجارية لمؤسسة[4].

---

[1] – لم يعرف قانون 18-05 المتعلق بالتجارة الإلكترونية الاتصال الإلكترونية، على غرار قانون 18-07 المتعلق بحماية الأشخاص الطبعيين عند معالجة معطياتهم الشخصية الذي أعطى له تعريف من خلال نص المادة 3 منه، و هو " كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية."

[2] – المادة 3 من قانون 04-02 المؤرخ في 23 يونيو 2004، يحدد القواعد المطبقة على الممارسات التجارية ، جريدة رسمية عدد 41، الصادرة بتاريخ 27 يونيو 2004، على أنه " كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع السلع و الخدمات مهما كان المكان أو وسائل الاتصال المستعملة.

[3] – القانون رقم 14-04 المتعلق بالنشاط السمعي البصري، المؤرخ في 2014/02/24، جريدة رسمية، عدد 16 الصادرة بتاريخ 2014/03/16.

[4] – أنظر المادة 28/1 من قانون 14-04 المتعلق بالنشاط السمعي البصري.

و عليه فإن مفهوم الإشهار التجاري الإلكتروني في التشريع الجزائري هو كل شكل مصمم أو رسالة محررة أو صوتية أو سمعية بصرية تبث بمقابل أو مجانا تهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع سلع و خدمات عن طريق الاتصال الإلكتروني.

و خلاصة التعريفات التشريعية السابقة، إنها ذكرت وسائل عديدة للإشهار لكنها أهملت ذكر الهدف الرئيسي منه، و هو البعد النفسي للمستهلك و التأثير عليه لأجل دعوته إلى التعاقد على تلك السلع و الخدمات المعروضة عليه عن طريق الإعلان.

2-التعريف الفقهي للإشهار التجاري الإلكتروني:

اختلف الفقه في تناول تعريف الإشهار التجاري، فعرفه جانب من الفقه ، بأنه" طريقة متخصصة من طرق ترويج المبيعات ينطوي على مجهودات و أنشطة من جانب المعلن لإقناع المستهلك النهائي و التأثير على سلوكه و توجيه هذا السلوك في اتجاه محدد تتفق و الأهداف التسويقية المنظمة، و ذلك من خلال وسائل الإعلام المختلفة مقابل دفع ثمن معين[1].

كما عرف الإشهار التجاري الإلكتروني بأنه " إخبار أو إعلام تجاري أو مهني القصد منه التعريف بمنتج أو خدمة معينة عن طريق إبراز المزايا و امتداح المحاسن بهدف خلق انطباع جديد يؤدي إلى إقبال الجمهور على هذا المنتج أو هذه الخدمة"[2].

و يعرف الإشهار التجاري كذلك بأنه " معلومات تجارية، صناعية أو مهنية موجهة للإعلام و التعريف بعلامة أو منتج و ذلك بالتضخيم في الجودة بغرض خلق صورة أو البيع و يكون للإعلان طابع مديحي عندما يكون هدفه أن يعلن عن علامة أو منتج، و قد يكون إعلاما اذا كان مرتبطا ارتباط وثيقا بإنتاج يكون له أن يعلم بصفاته و

[1]- محمد شرايرية، الحماية الجنائية للمستهلك، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامع عنابة، الجزائر،2011 ، ص 122.

[2]- كوثر سعيد عدنان خالد، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الإسكندرية مصر، 2016، ص 115.

كمياته و الثمن، و يكون من ثم تحريضيا، إذ أنه في الغالب يكون هدفه العمل على البيع[1].

و حسب رأينا فان أشمل تعريف للإشهار التجاري الإلكتروني هو " كل وسيلة تهدف إلى التأثير نفسيا على الجمهور، القصد منها التعريف بمنتج أو خدمة معينة عن طريق إبراز المزايا و امتداح المحاسن بهدف خلق انطباع جيد يؤدي إلى إقبال الجمهور على هذا المنتج أو هذه الخدمة تتم بوسائل الاتصال الحديثة".

فمن خلال هذا التعريف نخلص إلى أن الإشهار التجاري الإلكتروني لا يختلف كثيرا عن الإشهار التجاري التقليدية، إلا من حيث كون هذه الأخيرة يتم بوسائل الاتصال الحديثة مثل شبكت الأنترنت، فالأنترنت ليست سوى فضاء يتم فيه الإشهار، حيث شمل هذا التعريف كل الوسائل المستعملة للإعلان من وسائل تقليدية و وسائل إلكترونية المستخدمة في الإشهار، و شمل أيضا تأثير الإشهار للجانب النفسي للمستهلك بغرض حثه على التعاقد، و أخيرا وضح الغاية التي من أجلها اقدم المعلن على استخدام الإشهار التجاري لسلعته و هو الحصول على مكاسب تجارية.

ثانيا: خصائص الإشهار التجاري الإلكتروني

من خلال التعريفات السابقة يمكن تحديد خصائص الإشهار التجاري الإلكتروني، و تتمثل هذه الخصائص فيما يلي:

1-الإشهار التجاري موجه إلى جمهور المستهلكين:

توجه الرسائل الإشهارية الإلكترونية إلى المستهلكين عامة ، فيجب على الإشهار التجاري الإلكتروني أن يوجه إلى مجموعة من المستهلكين لا إلى شخص معين[2].

[1]- رمزي بيد الله على حجازي، المرجع السابق، ص 156.

[2]- شريف محمد غنام، المرجع السابق، ص 29.

2-الإشهار الإلكتروني يخبر المستهلكين بمزايا السلع و الخدمات:

حيث ينصب على بيان مزايا السلع و الخدمات المعلن عنها، فيتضمن مدحا لهذه المنتجات و إظهار محاسنها[1]، و لكن لا يجوز أن يغالي أو يبالغ صاحب المنتجات في بيان مزايا سلعهم و خدماتهم مما يؤدي إلى تضليل المستهلك.

3-الإشهار الإلكتروني يحفز المستهلكين على التعاقد:

يسعى أصحب السلع و الخدمات من خلال الإشهار التجاري إلى جذب جمهور المستهلكين على التعاقد و إقبالهم عليه، فإذا تخلفت فكرة حث الجمهور على التعاقد لا نكون بصدد إشهار[2]، فهدف الإشهار إحداث تأثير نفسي لدى الجمهور المتلقي له، من خلال إقناعه بمزايا السلع أو الخدمات و ما يمكن أن تحققه من فوائد[3].

4-الإشهار الإلكتروني ذو طبيعة تجارية:

ليس كل إشهار يتم عبر الأنترنت هو تجاري، و معيار كون الإشهار تجاري هو هدف تحقيق الربح من ورائه، فكل إشهار يستهدف من ورائه المعلن تحقيق الربح فهو إشهار تجاري.

5-الإشهار الإلكتروني يتم بوسيلة إلكترونية:

و هو الشيء الذي يميز الإشهار الإلكتروني عن التقليدي، فالإشهار الإلكتروني يتم من خلال الوسائل الإلكترونية، كالأنترنت مثلا التي هي الوسيلة الأكثر استعمالا مما تعمل على جذب أكبر عدد ممكن من المستهلكين لإقناعهم بالسلع و الخدمات[4].

---

[1]- دمانة محمد، "**الإشهار الإلكتروني التجاري و المستهلك**"، مجلة الفكر، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، العدد 17، جوان 2018، ص 292.

[2]- عبد الفضيل محمد احمد، الإعلان عن المنتجات و الخدمات من الوجه القانوني، مكتبة الجلاء الجديدة، بدون تاريخ نشر، ص 22.

[3] - خالد ممدوح إبراهيم، حماية المستهلك في التعاملات الإلكترونية، الدار الجامعية، الإسكندرية، مصر، 2008، ص 72.

[4] - دمانة محمد، المقال السابق، ص 293.

الفقرة الثانية: أشكال الإشهار التجاري الإلكتروني

يعد الإشهار التجاري الإلكتروني من أهم و أفضل الطرق التي قد يستخدمها أصحاب المنتجات لترويج عن مختلف السلع و الخدمات خاصة عبر الأنترنت، و نظرا لكثرة استخدام هذه الأخيرة بطرق متعددة تنوعت معها أشكال الإشهار التجاري باعتبار الأنترنت مجال خصب لجذب أكبر عدد من جمهور المستهلكين. و تتمثل هذه الأشكال للإشهار الإلكتروني في مواقع الأنترنت (أولا)، الشرائط الإعلانية (ثانيا)، الرسائل البينية (ثالثا)، البريد الإلكتروني (رابعا)، منتديات المناقشة و المحادثة (خامسا).

أولا: مواقع الأنترنت

تعددت و تنوعت مواقع الأنترنت أو صفحات الأنترنت بحيث يمكن القول بأنه من الصعب حصر المواقع المستخدمة في الإشهار عن السلع و الخدمات، حيث نجد أن المؤسسات و الشركات أو حتى الأشخاص الطبيعية تملك موقعا إلكتروني على شبكة الأنترنت يمكن من خلاله المستخدم من الاطلاع على كل ما يتعلق بالسلع و الخدمات كالنوع و الخصائص و السعر و غيرها من العناصر، و تسمح هذه المواقع بتكوين اتصال مباشر بين المنتج و المستهلك[1].

و يعد الإشهار التجاري عبر المواقع الإلكترونية الأكثر استعمالا و هذا نظرا لسهولة البحث و التصفح الذي يتمتع به، و أقلها تكلفة مقارنة بالوسائل الأخرى[2]، حيث يقوم أصحاب المواقع التجارية الإلكترونية بتصميم الإشهار بأسلوب و طريقة تجذب المستهلكين، مثل استعمال أصوات و أشكال مؤثرة و جذابة، و كذلك استعمال عبرات

[1] – خالد ممدوح إبراهيم، أمن المستهلك الإلكتروني، الدار الجامعية، الإسكندرية، مصر، 2008، ص 117.

[2]– Lama Akouche , La Loi Applicable Aux Contrats , Diplôme D'études Approfondies , Droit Interne et International Des Affairés ; Faculté de Droit et Des Sciences , Université Libanaise , Beyrouth,.2005, p72.

مكتوبة لجذب و تحفيز جمهور المستهلكين مثل عبارة اكسب أو أربح رحلة في حالة شرائك أكثر من منتوج[1].

و عليه فإن المواقع التي يتوافر فيها الإعلانات التي تتضمن بيع منتوجات تعد بمثابة دعامة إشهارية، أما المواقع التي تقدم من خلالها المؤسسات أو الجهات الحكومية بيانات أو معلومات عن الأنشطة التي تقدمها الدولة أو الجهات الرسمية لا تعد إشهارا تجارية ، لأنها لا تتضمن بيانات عن سلع و خدمات و لا تهدف إلى حث الجمهور على شرائها[2].

ثانيا: الشرائط الإعلانية (اللافتة الإعلانية الإلكترونية)

الشريط الإعلاني هو مستطيل صغير الحجم و يتواجد بصفة عامة أعلى أو أسفل الصفحة، و يظهر بشكل تلقائي دون أن يطلبه مستخدم الموقع ، فالمعلن يستطيع أن يستخدم عن طريق هذه الشرائط بعض المؤثرات الصوتية أو الحركية التي تحث المستخدم للضغط عليه و الدخول إلى الموقع الذي يشير إليه، و تتخذ هذه الشرائط عدة أشكال مختلفة منها الشرائط الثابتة و شرائط الرسوم المتحركة[3].

إذ أن الهدف التجاري للشريط الإعلاني ليس محل شك، إذ أن هدفه هو دعوة الزائر إلى زيارة الموقع الخاص بالمعلن عن طريق النقر عليه، و يتم الأخذ بالوصف التجاري إذا كانت العملية تعمل على تسويق منتجات أو سمعة شخص له نشاط تجاري[4].

ثالثا: الرسائل البينية

و يقصد بها تلك الرسالة التي تظهر بين صفحتين أو أكثر من صفحات الأنترنت عندما ينتقل المستخدم بين هذه الصفحات، و يستخدمها المعلنون في إشارات سريعة إلى

---

[1] – حمادة مصطفى عزب، الجوانب القانونية للإعلان عن المنتجات و الخدمات عبر الإنترنت، دار النهضة العربية، مصر، بدون تاريخ نشر، ص 34.

[2] – شريف محمد غنام، المرجع السابق، ص 36.

[3] –Lama Akouche , **op–cit** ,p68.

[4] – VERBIEST Thibault :la protection juridique cyber–consommateur. èd litec.2002.p 13.

مواقعهم أو إلى السلع و الخدمات التي يقدمونها أو إلى البريد الإلكتروني الذي يمكن للمستخدم مخاطبتهم عليه، و إذا أراد المستخدم الدخول إلى تلك المواقع أو الاستعلام عن هذه السلع و الخدمات فما عليه سوى الضغط على هذه الرسالة[1].

رابعا: البريد الإلكتروني

يعد البريد الإلكتروني وسيلة لنقل الرسائل إلكترونيا إلى شخص أو عدة أشخاص لهم عناوين بريد إلكترونية مجانا، و هو من أكثر الخدمات المستخدمة في الأنترنت و هو يشبه البريد العادي من الناحية الوظيفية، لكنه يمتاز عنه بالسرعة و المرونة و سهولة الاستخدام[2]، و قد عرفه قانون الثقة في الاقتصاد الرقمي الفرنسي الصادر في 21 يونيه 2004 البريد الإلكتروني في مادته الأولى على أنه " كل رسالة ، أيا كان شكلها نصية ، أو صوتية، أو مصحوبة بصور و أصوات، يتم إرسالها عبر شبكة عامة للاتصالات، و يتم تخزينها على أحد خوادم هذه الشبكة أو في المعدات الطرفية للمرسل إليه حتى يتمكن هذا الأخير من استعمالها".

إذ نجد أن العديد من الشركات تستخدم البريد الإلكتروني كوسيلة فاعلة للتسويق و الإعلان عن السلع و الخدمات التي تقدمها لمستخدم أو مجموعة مستخدمين، حيث يتيح للمعلن فرصة الاتصال المباشر بالعملاء دون انتظار قدومهم إليه و جذب انتباههم بالوسائل الأخرى[3].

خامسا: منتديات المناقشة و المحادثة:(الشبكات الاجتماعية)

منتدى المناقشة مكان افتراضي لتبادل المعلومات و الأفكار حول مسالة معينة بين أكثر من شخص، و يتم الحوار بين الجميع بشكل مكتوب أو شفوي من خلال برنامج معين يربط بينهم. أما المحادثة عبر الأنترنت فهي شبيهة بالمحادثة التي تتم عبر التليفون

---

[1] – VERBIEST Thibault :la protection juridique cyber-consommateur .op. cit. p 13

[2] – كوثر سعيد عدنان، المرجع السابق، ص 124.

[3] – د/ أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الأنترنت، دار النهضة العربية، مصر، 2003، ص 8.

إلا أنها تكون مكتوبة، و يمكن أن تضم المحادثة أكثر من شخصين و في هذه الحالة تتشابه بمنتديات المناقشة[1].

إذ يمكن استخدام مساحات إعلانية لترويج السلع و الخدمات بواسطة هذه المنتديات بشكل دائم أو مؤقت، و يستوي في هذه الحالة أن يكون المعلن صاحب المنتدى أو شخصا من الغير. فوجود موقع ثابت لهذه المنتديات يضمن وصول الرسالة الإعلانية إلى عدد كبير من الأشخاص، مما يضفي على الرسالة الإعلانية وصف العمومية. و عليه تعد الرسالة الإعلانية التي تظهر على المنتديات تجارية متى كانت تتضمن عرضا أو ترويجا لسلع و خدمات تقدم للجمهور بمقابل[2].

الفرع الثاني: صور تجريم الإشهار التجاري الإلكتروني غير المشروع.

بتنظيم المشرع الجزائري التجارة الإلكترونية من خلال قانون التجارة الإلكترونية، أصبح الإشهار الإلكتروني منظم بنصوص خاصة، سواء من حيث شروطه، أو من حيث بعض الالتزامات التي تقع على عاتق المهني (المورد الإلكتروني[3])، و هيا بمثابة حماية تقنية للمستهلك من الإشهار الإلكتروني غير المشروع.

و لقد اعتبر المشرع الجزائري مخالفة الإشهار التجاري الإلكتروني لهذا التنظيم إشهارا غير مشروع و معاقب عليه قانونا من خلال نص المادة 40 من قانون التجارة الإلكترونية، و عليه سنحاول تحديد صور تجريم الإشهار الإلكتروني غير المشروع من خلال جريمة مخالفة شروط الإشهار الإلكتروني (فقرة أولى) و جريمة الإشهار الإلكتروني غير المرغوب فيه (فقرة ثانية) .

[1] – مريم بن خليفة، التسويق الإلكتروني و آليات حماية المستهلك، دار الفكر و القانون، مصر، 2017، ص 50.

[2]– VERBIEST Thibault: la protection juridique cyber-consommateur .op. cit. p 15.

[3]– المورد الإلكتروني هو كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير السلع أو الخدمات عن طريق الاتصالات الإلكترونية. **أنظر المادة 06 من قانون 18-05 المتعلق بالتجارة الإلكترونية.**

الفقرة الأولى: جريمة مخالفة شروط الإشهار التجاري الإلكتروني

وضع المشرع الوطني من خلال قانون التجارة الإلكترونية مجموعة من الشروط الواجب توافرها في الإشهار التجاري الذي يتم عن طريق وسائل الاتصال الإلكترونية، و التي يجب على المورد الإلكتروني الالتزام بها عند الإشهار عن منتوجاته، و مخالفة الإشهار لهذه الشروط يعد إشهارا غير مشروع معاقب عليه بموجب المادة 40 من نفس القانون[1]. و جريمة مخالفة شروط الإشهار التجاري الإلكتروني كغيرها من الجرائم تقوم بتوفر كل من ركنها المادي (أولا) و المعنوي (ثانيا)، كما أقر لها المشرع عقوبة تتماشى مع جسامتها (ثالثا).

أولا: الركن المادي لجريمة مخالفة شروط الإشهار الإلكتروني

تعد جريمة مخالفة شروط الإشهار الإلكتروني من الجرائم الشكلية التي لا يتطلب لقيامها حدوث نتيجة معينة، فمجرد إتيان السلوك الإجرامي تقوم الجريمة، و السلوك الإجرامي لها يتمثل حسب المادة 40 من قانون التجارة الإلكترونية في مخالفة المورد الإلكتروني لنص المادة 30 من نفس القانون. إذ ألزمت هذه الأخيرة أن يتوفر في الإشهار الإلكتروني مجموعة من الشروط[2]، و مخالفة المورد الإلكتروني لواحد من هذه الشروط أو كلها يعد إشهار تجاري إلكتروني غير مشروع. و عليه سنحاول تحديد صور السلوك الإجرامي لهذه الجريمة على النحو التالي :

---

[1]– المادة 40 من قانون 18–05 المتعلق بالتجارة الإلكترونية " دون المساس بحقوق الضحايا في التعويض، يعاقب بغرامة من 50.000دج إلى 500.000دج كل من يخالف أحكام المواد 30...".

[2] – المادة 30 من قانون رقم 18–05 المتعلق بالتجارة الإلكترونية " دون المساس بالأحكام التشريعية و التنظيمية المعمول بها في هذا المجال، كل إشهار أو ترويج أو رسالة ذات طبيعة أو هدف تجاري تتم عن طريق الاتصالات الإلكترونية يجب أن يلبي المقتضيات الآتية:

–أن يكون محدد بوضوح كرسالة تجارية أو إشهارية.

–أن تسمح بتحديد الشخص الذي تم تصميم الرسالة لحسابه.

–ألا تمس بالآداب العام و النظام العام.

–أن تحدد بوضوح ما إذا كان هذا العرض التجاري يشمل تخفيضا أو مكافآت أو هدايا، في حالة ما إذا كان هذا العرض تجاريا أو تنافسيا أو ترويجيا.

التأكد من أن جميع الشروط الواجب استيفاؤها للاستفادة من العرض التجاري، ليست مضللة و لا غامضة."

1- عدم وضوح الإشهار الإلكتروني:

وفقا للفقرة 2 من المادة 30 من قانون التجارة الإلكترونية يجب على المورد الإلكتروني أن يظهر بوضوح الطابع التجاري للرسالة الإشهارية الإلكترونية التي صدرت منه، إذ يلتزم المعلن على ذكر كلمة إعلان أو إشهار بصورة واضحة و مقروءة على رأس كل إعلان أو إشهار إلكتروني[1]. كما يتعلق الأمر هنا بمحتوى الرسالة الإشهارية، و التي يجب أن تكون كل عبارة واضحة الدلالة عما يقصد المعلن توصيله للمستهلك، فلا يستخدم المعلن عبارات **غامضة أو مبهمة أو تحمل أكثر من معنى**[2]. و لذلك يجب أن يستخدم المعلن عبارات سهلة و بسيطة في الإشهار الإلكتروني مع مراعات فئة المستهلكين الذين يخاطبهم الإشهار.

كما يجب لتحقيق الوضوح في الرسالة الإشهارية الصدق، فالصدق هو الإخبار بالشيء على ما هو عليه، فمحتوى الإشهار هو مجموعة من المعلومات التي تتناول الصفات المميزة للشيء المعلن عنه، فيجب أن تكون تلك المعلومات صادقة، بحيث تكون كل صفة يذكرها التاجر أو مقدم الخدمة موجودة بالفعل في السلعة أو الخدمة[3].

كما يجب أيضا لوضوح الرسالة الإشهارية ألا يركز المعلنون فقط على بعض العبارات التي تكشف و تترجم هذه الادعاءات، فيجب كذلك أن يأخذوا في الاعتبار الإشهار الإلكتروني في مجمله بما يتضمن من عبارات مكتوبة و صور و أرقام و غيرها. إذ يقتضي وضوح البيانات الواردة في الإشهار أنه إذا كان يستخدم في الرسالة الإعلانية أصوات عبر الموقع، فيجب أن تكون الأصوات عالية، و يستخدم فيها لغة مفهومة و تعبيرات سهلة[4].

---

[1] – محمد بودالي، حماية المستهلك في القانون المقارن، دراسة مقارنة، دار الكتب الحديثة، مصر، 2006، ص171.

[2]– VERBIEST Thibault: commerce èlectronique : le nouveau cadre juridque . éd LARCIER . 2004.P 60.

[3] – كوثر سعيد عدنان، المرجع السابق، ص 150.

[4] – شريف محمد غنام، المرجع السابق، ص 61.

و يتنافى مع مبدأ وضوح البيانات الواردة في الإشهار التجاري الإلكتروني أن يستخدم المعلنون في التعبير عن إرادتهم عبارات صغيرة الحجم بالمقارنة لحجم إجمالي الإشهار. فلا يجب أن يقدر المعلنون أن مستخدمي الأنترنت سوف يقرؤون كل الصفحات الواردة بالإشهار، أو كل العبارات و الكلمات المستخدمة فيه، و من ثم يجب التركيز على الكلمات و البيانات المهمة و إبرازها بحجم مناسب[1].

كما يؤخذ في وضوح الإشهار التجاري الإلكتروني موضع البيانات الواردة فيه، إذ يجب أن توضع البيانات الواردة فيه بالقرب من كل موضوع من موضوعات الإشهار، و ذلك إذا كان الإشهار الإلكتروني يتضمن مسائل عديدة. هذا التقارب في المكان بين البيانات المهمة يعطي للمستهلك فرصة لرؤية هذه البيانات و ربطها بالموضوع الكلي[2].

و لمعرفة إذا كانت البيانات الواردة في الإشهار التجاري الإلكتروني واضحة و ملفتة للنظر أم لا، فإنه ذلك يقاس بمدى أثر الإشهار في مجمله على المستهلك، و ما يتركه من انطباع إجمالي عليه[3].

و لقد أكد على هذا الشرط المادة السادسة في فقرتها (أ)من توجيه التجارة الإلكترونية رقم 31/2000 الصادر في 8 يونيه 2000 و التي تنص على أنه "يجب أن تكون الاتصالات التجارية قابلة للتحديد بطريقة واضحة باعتبارها كذلك".

و كذلك تنص المادة 20 من القانون الخاص بالثقة في الاقتصاد الرقمي الفرنسي الصادر في 21 يونيه 2004 على أن " كل إعلان أيا كان شكله، يقدم عن طريق خدمة الاتصال عبر الخط، يجب أن يكون واضحا... ".

كما اشترط المشرع الجزائري وضوح الإشهار الإلكتروني إذا كان يحتوي على تخفيض أو على مكافاة أو هدايا[1]، حيث يلتزم المعلن الإلكتروني بتحديد نوع الإشهار

---

[1]– BOCHURERG Laudon: internet et commerce électronique. Ed encvclopédie . DELMAS. 1999. P 142.

[2] – شريف محمد غنام، المرجع السابق، ص 62.

[3]– BOCHURERG Laudon: op. cit. p 144.

الإلكترونية في هذه الأنواع من العروض، إذ يعتبر هذا الشرط من أهم المبادئ التي أتى بها توجيه التجارة الإلكترونية رقم 31/200 [2]، حيث أن التجار أو المهنيين كثيرا ما يضللون المستهلكين و يخدعوهم من خلال الإشهار عن تلك البيوع.

و عليه فإن عدم التزام المعلن الإلكتروني بوضوح الرسالة الإشهارية التجارية الإلكترونية يؤدي لقيام الركن المادي لجريمة مخالفة شروط الإشهار الإلكتروني وفقا للمادة 40 من قانون التجارة الإلكترونية.

2- عدم تحديد الشخص الذي تم تصميم الرسالة لحسابه:

اعتبرت الفقرة الثالثة من المادة 30 من قانون التجارة الإلكترونية أن تحديد شخصية المعلن في الرسالة الإشهارية شرط من شروط الإشهارية التجاري الإلكترونية. و يعد هذا الشرط من أهم الضمانات الحديثة و التي أقرتها أغلب التشريعات في المعاملات الإلكترونية، لأن تحديد شخصية المعلن يوفر عنصر الأمان للمستهلك[3].

غير أن المشرع الجزائري لم يحدد ماهيا المعلومات الواجب أن تتضمنها الرسالة الإشهارية لتحديد شخصية صاحبها، غير أنه بالرجوع إلى المادة 10من نفس القانون فإن البيانات الخاصة بالمعلن تتمثل في : رقم التعريف الجبائي، العناوين المادية و الإلكترونية، و رقم هاتف المورد الإلكتروني، رقم التسجيل التجاري، أو رقم البطاقة المهنية للحرفي[4].

و لقد أكد على هذا الشرط المادة السادسة في فقرتها (ب)من توجيه التجارة الإلكترونية رقم 31/2000 الصادر في 8 يونيه 2000 و التي تنص على أنه "يجب أن يكون الشخص المعنوي أو الطبيعي الذي يتم الاتصال التجاري لحسابه قابلا للتحديد بسهولة".

---

[1] – أنظر الفقرة 4 من المادة 30من قانون18-05 المتعلق بالتجارة الإلكترونية.

[2] – انظر الفقرة (ج) من المادة السادسة من توجيه التجارة الإلكتروني رقم 31/2000.

[3] – د/ خالد ممدوح إبراهيم، أمن المستهلك الإلكتروني ، المرجع السابق، ص 82.

[4] – أنظر المادة 10 من قانون 18-05 المتعلق بالتجارة الإلكترونية.

و كذلك تنص المادة 20 من القانون الخاص بالثقة في الاقتصاد الرقمي الفرنسي الصادر في 21 يونيه 2004 على أن " كل إعلان أيا كان شكله، يقدم عن طريق خدمة الاتصال عبر الخط، يجب أن يكون واضحا. و يجب أن يوضح فيه كذلك الشخص الطبيعي أو المعنوي الذي يتم لحسابه هذا الإعلان".

و عليه وجب على المعلن أن يضع في الرسالة الإشهارية الإلكترونية البيانات المتعلقة به بشكل واضح، بحيث يتمكن كل مستخدم (المستهلك) للموقع أو المرسل إليه عبر بريده الإلكتروني من رؤيتها و قراءتها بسهولة و وضوح. و مخالفة هذا الالتزام يؤدي لقيام الركن المادي لجريمة مخالفة شروط العقد الإلكتروني وفقا للمادة 40 من قانون التجارة الإلكترونية سابقة الذكر.

3- مخالفة محتوى الرسالة الإشهارية للآداب العامة و النظام العام:

يعتبر المشرع الوطني من خلال الفقرة الرابعة من المادة 30 من قانون التجارة الإلكترونية أن الإشهار التجاري الإلكتروني يجب أن لا يكون مخالفا للآداب العامة و النظام العام، إذ يجب على المورد الإلكتروني أن يكتفي بلفت نظر المتلقي و اهتمامه بمحتوى الرسالة الإشهارية و كذلك ترغيبه بالشيء المعلن عنه و ذلك عن طريق الإشهار المهذب و المتخلق[1].

و يمكن حصر المبادئ المتعلقة باحترام الآداب و النظام العام فيما يلي:

-خلو الإشهار من كل ابتذال، و احترام الإشهار للقيم الوطنية و العلمية.

-عدم اللجوء إلى مشاهدة عنيفة أو قصد المجازفة و تأكيد فاعلية المواد المشهر عنها في الإعلانات أو يشع على الخرفات و الشعوذة.

[1] - عبد الله على محمود، حماية المستهلك من الغش التجاري و الصناعي، دار النهضة الغربية، القاهرة، 2002، ص 80.

-ألا يتضمن الإشهار الموجه للأطفال و القصر أية مشاهدة أو صور يمكنه أن تلحق بهم ضرر أو أن تدعوا للمجازفة للتأكيد فاعلية المواد المشهر عنها[1].

و إذا كان مفهوم الآداب العامة مختلفا من دولة إلى أخرى، فلا يجوز أن يستند المعلنون إلى ذلك و إلى أن إشهارهم موجهة إلى الجمهور العالمي عبر الشبكة العالمية. فلا يجوز أن تحرض الإعلانات على التمييز العنصري أو تحرض على الكراهية لجنس معين، أو تبث مفاهيم دينية معينة، أو تدعوا إلى العلاقات غير المشروعة، أو تتضمن إعلانا على مواقع إباحية[2]. فيجب أن تتطور قواعد آداب المهنة الإعلانية الوطنية و الدولية و المطبقة حاليا لتلائم الأنترنت، نظرا لطبيعتها العابرة للحدود غير المادية و التفاعلية.

و لقد أوجبت المادة 1/8 من توجيه التجارة الإلكترونية على الدول الأعضاء أن تراعي أن يكون استعمال الاتصالات التجارية تحت تحفظ احترام القواعد المهنية، الهادفة بصفة خاصة إلى استقلال و كرامة و شرف المهنة و كذلك السر المهني[3]. كما نشر غرفة التجارة الدولية تقنينا دوليا للتطبيقات الدولية الصادق في موضوع الإعلان، و هذا التقنين يعتد بجميع الوسائط بما في ذلك الرسائل الإلكترونية، إذ يتطلب في الإعلان أن يتفق مع القانون[4].

4- التضليل أو الغموض في شروط الواجب استفائها للاستفادة من العرض التجاري في الإشهار الإلكتروني:

تعتبر شروط الاستفادة من العرض التجاري من المسائل المهمة لتمكين المستهلك من الحصول أو الاستفادة من العرض التجاري الذي يحتوي عليه الإشهار التجاري

[1] - خميخم محمد، الرسالة السابقة، ص 41.

[2]- VARILLE larrieu : PUBLICITé sur internet. Droit et déontologie. Gaz-pal. Vendredi 21. Samedi 22 november 1997. P 7.

[3] - أنظر المادة 1/8 توجيه التجارة الإلكترونية رقم 31/2000 الصادر في 8 يونيه 2000.

[4] - BOCHURERG Laudon: op. cit. p 144.

الإلكتروني[1]، لذلك جعل المشرع الوطني عدم الغموض و التضليل في الشروط الواجب استفائها للاستفادة من العرض التجاري المعروض عن طريق الإشهار الإلكتروني من الشروط الواجب توافرها في هذا الأخير و هو ما نصت عليه الفقرة الأخيرة من المادة 30 من قانون التجارة الإلكترونية[2].

غير أن المشرع الوطني لم يحدد هذه الشروط التي يتم بموجبها الاستفادة من العرض التجاري، و حسب رأينا فإن هذه الشروط تتمثل في مدة الإشهار، و طرق الولوج إلى المستندات المحفوظة في مختلف مراحل التعاقد، و طرق الدفع و مراحل التعاقد، و مدة تسليم الطلبية. لذلك يجب أن تكون هذه الشروط غير مضللة أو غامضة.

و التضليل في الإشهار الإلكتروني هو ذلك الإشهار الذي يكون من شأنه خداع المستهلك، أو يمكن أن يؤدي إلى ذلك، أي أن يستخدم المعلن ألفاظ و عبارات كاذبة من شأنها أن تؤدي إلى خداع المستهلك و تدفعه إلى التعاقد، أو تزيد من الإقبال عليه[3]، و تمس هذه الألفاظ الشروط الواجب استفائها للاستفادة من العرض التجاري الإلكتروني.

أما الغموض فهو على غرار التضليل لا يحمل عبارات كاذبة و إنما يورد المعلن الإلكتروني عبارات صادقة لكنها تحمل أكثر من معنى، لذا يجب عليه أن تكون كل عبارة واضحة الدلالة عما يقصد المعلن توصيله للمستهلك، و ذلك باستخدام عبارات سهلة و بسيطة في الإشهار مع مراعات فئة المستهلكين الذين يخاطبهم الإشهار[4].

و عليه فإن خلو الإشهار التجاري الإلكتروني من أي تضليل هو شرط من شروط الإشهار النزيه، و مخالفته يؤدي لقيام الركن المادي لجريمة مخالفة شروط الإشهار الإلكتروني حسب نص المادة 40 من قانون التجارة الإلكترونية.

---

[1] – د/ علاء عمر محمد الجاف، المرجع السابق، ص 160.

[2] – أنظر الفقرة الأخيرة من المادة 30 من قانون 18-05 المتعلق بالتجارة الإلكترونية

[3] – سوالمي أحمد، الحماية الجنائية من الدعاية التجارية الكاذبة، رسالة ماجستير، كلية الحقوق، جامعة الجزائي1، 2014، ص 44.

[4] – VERBIEST Thibault : commerce èlectronique : le nouveau cadre juridque. Op. cit. p 60.

ثانيا: الركن المعنوي لجريمة مخالفة شروط الإشهار التجاري الإلكتروني

يتميز الركن المعنوي في هذا النوع من الجرائم بتقلصه إلا أن الجريمة لا تقوم بطبيعة الحال إلا بوجوده، و بالرجوع إلى المادة 40 من قانون التجارة الإلكترونية و التي جرمت الإشهار الإلكتروني غير المشروع خاصة صورة مخالفة شروط الإشهار المنصوص عليها في المادة 30 من نفس القانون و التي تشمل كل الكذب و التضليل في الإشهار الإلكتروني، نجدها لا تحدد الركن المعنوي بوضوح، حيث أثار التضليل و الكذب في الإشهار الإلكتروني العديد من النقاشات الفقهية، و هذا نظرا لطبيعة هذا السلوك و آثاره المباشرة على المستهلك .

فبعد استبعاد سوء النية لدى المعلن في جريمة الإشهار الذي يحتوي على تضليل[1]، انقسم الفقه إلى عدة آراء و كل رأي له حجته، و هذا ما سوف نحاول تبيانه فيما يلي:

الرأي الأول: يرى أن الجريمة تبقى عمدية و يشترط لقيامها الركن المعنوي مع قيام قرينة قانونية أن المسؤولية تقع على عاتق المعلن و افتراض سوء النية و ذلك تيسيرا للإثبات، حيث أعفى سلطة الاتهام من الإثبات و وجود سوء النية لدى المعلن، فالهدف من نقل عبء الإثبات هو تحقيق حماية فعالة للمستهلك وردع اكثر للمعلن.

الرأي الثاني: يرى أن عنصر التضليل في الإشهار الإلكتروني يقوم مت انصرفت إرادة الجاني إلى القيام بالنشاط المادي المعاقب عليه حتى و لو لم تنصرف إرادته إلى تحقيق النتيجة، و من هنا فان الركن المعنوي يتوفر بمجرد مخالفة القانون، و هذا سواء تعمد المخالفة أو وقعت بسبب إهمال أو عدم حيطة أو عدم مراعاة للأنظمة من طرفه.

و الواقع أن الرأي القائل بامتداد نطاق الاكتفاء بالخطأ غير العمدي راجع إلى فكرة أن المصلحة التي اقر المشرع باستحقاقها الحماية الجنائية يجب أن تحمى ليس فقط ضد

[1] – كان المشرع الفرنسي ينص صراحة على وجوب توافر النية لدى المعلن في قانون 2 جويلية 1963 مما أدى إلى إفلات العديد من العقاب في حالة عجز النيابة عن إقامة الدليل، و لذلك أصدر المشرع الفرنسي القانون 1973 المتعلق بتوجيه النشاط التجاري، و الذي لم يعد يشترط إثبات سوء النية في الركن المعنوي لجريمة الإشهار المضلل، حيث نصت المادة 44 منه على إلغاء اشتراط سوء النية لدى المعلن. **انظر محمد بودالي، حماية المستهلك في القانون المقارن، المرجع السابق، ص 172.**

الاعتداءات العمدية، و إنما أيضا ضد الاعتداءات العائدة للأعمال أو عدم الاحتياط أو غيرها من صور الخطأ

الرأي الثالث: يرى أن التضليل في الإشهار الإلكتروني قائم بمجرد توافر الركن المادي لها، و لا تقوم بالبحث عن توفر الركن المعنوي، حيث تتضمن الجريمة وقوع العناصر المكونة للركن المادي دون النظر إلى الركن المعنوي، فهي تعتبر من قبيل الجرائم المادية البحتة.

فحسب رأي هذا الاتجاه أن المستهلك يتضرر من الإعلان الإلكتروني غير المشروع سواء كان المعلن سيء النية أو حسنها[1].

و من هنا فإن الركن المعنوي في جريمة مخالفة شروط الإشهار التجاري الإلكتروني يتوفر بمجرد مخالفة القانون، لأن فعل ارتكاب المخالفة ينطوي في حد ذاته على خطأ، و مؤدي ذلك اندماج الركن المعنوي في الركن المادي، فليس للمعلن أن يثبت أنه لم يرتكب خطأ، بل يتعين إدانته بمجرد ارتكابه، فمرتكب المخالفة لا يفترض من أنه مخطئ بل هو مخطئ فعلا.

ثالثا: العقوبة المقررة لجريمة مخالفة شروط الإشهار التجاري الإلكتروني

تعتبر العقوبات المالية أهم العقوبات التي جاء بها قانون التجارة الإلكترونية و من بينها جرائم الإشهار التجاري غير المشروع باعتبارها جرائم اقتصادية، و مرجع ذلك أن أغلب هذه الجرائم ترتكب بدافع الطمع و الربح غير المشروع، فكان من الملائم فرض عقوبات مالية تصيب الجناة في ذمتهم المالية لردعهم، و بما يكفل احترام قوانين حماية المستهلك[2].

[1] – أنور محمد صدقي المساعدة، المسؤولية الجزائية عن الجرائم الاقتصادية، دار الثقافة للنشر و التوزيع ، عمان، الطبعة1، 2007، ص 251.

[2] – د/ محمود محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، الجزء الأول، مطبعة جامعة القاهرة و الكتب الجامعية، 1979، ص 157.

و لقد عرفت الغرامة على أنها إلزام المحكوم عليه بدفع مبلغ من المال إلى الخزانة العامة للدولة[1]، و هيا بذلك عقوبة تتوافر فيها كل مقومات و خصائص العقوبة الجزائية، باعتبارها إيلاما مقصودا ينال من الحقوق المالية للمحكوم عليه بها[2].

و لقد كيف قانون التجارة الإلكترونية رقم 18-05 جريمة مخالفة شروط الإشهار التجاري الإلكتروني على أساس جنحة و ذلك بموجب المادة 40 منه، و أفرد له عقوبة مالية تتراوح بين 50.000 دج إلى 500.000 دج. أما في حالة العود فتضاعف العقوبة حيث تصبح غرامة من 100.000دج إلى 1.000.000دج[3].

كما أجاز قانون التجارة الإلكترونية المصالحة في الجرائم المتعلقة بالإشهار الإلكتروني غير المشروع عامة بما فيها جريمة مخالفة شروط الإشهار التجاري الإلكتروني[4]، حيث أن القاعدة العامة في تحديد غرامة الصلح في قانون التجارة الإلكترونية هيا الحد الأدنى لعقوبة الغرامة المقررة للجريمة، و هو ما نصت عليه المادة 46 من نفس القانون. و عليه فإن غرامة الصلح في جريمة الإشهار الإلكتروني غير المرغوب فيه تساوي 50.000دج.

كما منح المشرع الوطني للمورد الإلكتروني الذي قبل بغرامة الصلح المقترحة من طرف الإدارة المعنية (مصالح التجارة) بتخفيض في غرامة الصلح قدره 10 بالمئة[5].

---

[1] – سليمان عبد المنعم، نظرية الجزاء الجنائي، المؤسسة الجامعية للدراسات و النشر و التوزيع، بيروت، 1999، ص 54.

[2] – روسم عطية موسى نو، المرجع السابق، ص 307.

[3] – المادة 48 من قانون18-05 المتعلق بالتجارة الإلكترونية " يضاعف مبلغ الغرامة في حالة تكرار نفس الجريمة خلال مدة لا تتجاوز اثنى عشر (12) شهر من تاريخ العقوبة المتعلقة بالجريمة السابقة".

[4] – المادة 45 من قانون18-05 المتعلق بالتجارة الإلكترونية " دون المساس بحقوق الضحايا في التعويض، تؤهل الإدارة المكلفة بحماية المستهلك بالقيام بإجراءات الصلح مع الأشخاص المتابعين بمخالفة أحكام هذا القانون".

[5] – المادة 46 من قانون 18-05 المتعلق بالتجارة الإلكترونية " مبلغ غرامة الصلح هو الحد الأدنى من الغرامة المنصوص عليها في أحكام هذا القانون".

الفقرة الثانية: جريمة الإشهار التجاري الإلكتروني غير المرغوب فيه.

إن الإشهار عبر البريد الإلكتروني يثير بعض المشاكل، و خاصة ظاهرة الإغراق بالرسائل[1]، أو ما يعرف بالرسائل الإشهارية غير المرغوب فيها[2]. إذ أن الغالبية العظمى من المستهلكين يرفضون تلك الإشهارات، فهي لا تحقق فائدة لهم بقدر ما تحمله من عيوب، إذ ينفق الكثير من الوقت في فتح الرسائل و التحقق من محتواها ثم إزالتها، و يتحمل في نفس الوقت مصاريف استلام هذه الرسائل و البقاء على خدمة الأنترنت، و من جهة أخرى تشكل هذه الرسائل خطر على البيانات الشخصية للمستهلك ، حيث يقوم المورد الإلكتروني بتحويل هذه البيانات إلى جهة أخرى[3].

و عليه فإن كثرة تلقي تلك الرسائل بهذا الشكل يؤدي إلى زعزعة ثقة المستهلك في التجارة الإلكترونية، مما دعا المشرع الجزائري إلى التصدي لمثل هذا النوع من الإشهارات الإلكترونية، من خلال إلزام المورد الإلكتروني باتباع نظامين قانونيين نصت عليهما قانون التجارة الإلكترونية.

و لقد اعتبر المشرع الجزائري مخالفة هاذين النظامين جريمة معاقب عليها قانونا من خلال نص المادة 40 من قانون 18-05 المتعلق بالتجارة الإلكترونية، مما يستدعي تبيان هذه الجريمة من خلال دراسة كل من ركنها المادي (أولا) و ركنها المعنوي (ثانيا)، و تحديد العقوبة المقررة لها (ثالثا).

---

[1] – يلجأ بعض التجار إلى استخدام قائمة العناوين الإلكترونية للمستهلكين المحتملين، ثم يرسلون إليهم الدعايات و الإعلانات التجارية إلى صناديقهم الإلكترونية دون موافقتهم المبدئية، إذ أن هناك شركات متخصصة تهيء قوائم العملاء المستهلكين لسلعة أو خدمة معينة، و تباع هذه القوائم على التجار و الشركات التجارية المتخصصة في إنتاج هذه السلع و الخدمات. **أنظر صابر عبد العزيز سلامة، العقد الإلكتروني، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2007، ص 22.**

[2] – عرف الإعلان الإلكتروني غير المرغوب فيه بأنه تلك الرسائل التي تمت بواسطة إلكترونية و توجه إلى شخص أو مجموعة من الأشخاص بدون تمييز و بغير طلب من جانبهم، و دون رضاهم . **أنظر د/ عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني ، دار النهضة العربية، القاهرة، بدون تاريخ نشر ، ص 81.**

[3] – د/ أسامة أحمد بدر، المرجع السابق، ص98.

أولا: الركن المادي لجريمة الإشهار التجاري الإلكتروني غير المرغوب فيه

جريمة الإشهار التجاري الإلكتروني غير المرغوب فيه من الجرائم الشكلية التي لا تتطلب لقيامها توافر نتيجة معينة، فبمجرد مخالفة المورد الإلكتروني للالتزامات المنصوص عليها في المادتين 31 و 32 من قانون التجارة الإلكترونية تقوم الجريمة. و عليه فإن الركن المادي لهذه الجريمة يمتثل في:

1- عدم أخذ موافقة المستهلك في تلقي رسائل الاستبيان المباشر:

ألزم المشرع الوطني من خلال المادة 31 من قانون التجارة الإلكتروني المعلن الإلكتروني قبل استعمال بيانات المستهلك الإلكتروني في الاستبيان المباشر أخذ الموافقة المسبقة للمستهلك قبل إرسال هذا الاستبيان المباشر إليه[1]، إذ اشترط المشرع على صاحب الإشهار الإلكتروني قبل إرسال الاستبيان المباشر[2] للمستهلك أن تكون الموافقة صريحة و هو ما يعرف بمخالفة نظام الرضاء المسبق من طرف المستهلك، و يقصد بهذا النظام حظر قيام المرسل بإرسال الرسائل الإلكترونية غير المرغوب فيها إلى المرسل إليه إلا إذا أعطى موافقته المسبقة على إرسال مثل هذه الرسائل[3]، إذ يلزم هذا النظام على المرسل أن يقوم بإرسال رسالة إلكترونية إلى المستهلك يطلب فيها قبوله باستلام الإعلانات التجارية التي يرسلها إليه[4]. غير أن المشرع الوطني قد اقتصر تطبيق هذا

---

[1] – المادة 31 من قانون 18-05 المتعلق بالتجارة الإلكترونية " يمنع الاستبيان المباشر اعتمادا على إرسال الرسائل عن طريق الاتصالات الإلكترونية باستعمال معلومات شخص طبيعي، بأي شكل من الأشكال، لم يبد موافقته المسبقة لتلقي استبيانات مباشرة عن طريق الاتصال الإلكتروني".

[2] – لم يعرف المشرع الوطني من خلال قانون 18-05 المتعلق بالتجارة الإلكترونية الاستبيان المباشر، غير أنه بالرجوع إلى قانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي ، نجده قد أورد تعريفا له من خلال نص المادة 3 منه، و يعرف على أنه " إرسال أي رسالة مهما كانت دعامتها و طبيعتها، موجهة للترويج المباشر أو غير المباشر لسلع أو خدمات أو لسمعة شخص يبيع سلعا أو يقدم خدمات."

[3] – د/ عبد الهادي فوزي العوضي، المرجع السابق، ص 87.

[4] – و هناك نوع جديد متطور من نظام opt-in قد ظهر في الحياة العملية يؤمن حماية أكبر للمستهلك هو نظام double opt-in و يقوم هذا النظام الجديد ليس فقط على رضا المستهلك عند استلام إعلان spam و لكن يتطلب تأكيد الرضا عندما يصدر من المستهلك، **أنظر شريف محمد غنام، المرجع السابق، ص 109.**

النظام على رسائل الاستبيان المباشر فقط. و هذا للموازنة بين احترام مبدأ حرية التجارة من ناحية و حماية بيانات المستهلك من ناحية أخرى.

و عليه يمكن للمورد الإلكتروني بعد موافقة المستهلك أن يستعمل عنوان البريد الإلكتروني الذي قدمه له المستهلك بمناسبة الاستبيان المباشر بخصوص البيع السابق أو أداء الخدمة السابقة، غير أنه لا يجوز استعمال عنوان بريد إلكتروني غير ذلك الذي سبق له استعماله و لو كان خاص بذات المستهلك[1].

و هو ما نص عليه التوجيه الأوروبي رقم 58 لسنة 2002 المتعلق بالاتصالات و الحياة الخاصة، حيث تنص المادة 13 منه على انه " لا يجوز استخدام البريد الإلكتروني أو البيانات الشخصية للمستهلكين في الإعلانات التجارية أو التسويق المباشر إلا بعد الحصول على رضائه المسبق"

كما اعتمد قانون الاستهلاك الفرنسي على نظام الموافقة المسبق، فيما يخص الإعلانات أو التسويق التجاري عبر البريد الإلكتروني دون طلب[2]، و ذلك من خلال المادة 5/20/121 التي منعت الاجتذاب المباشر من قبل المهنيين، الذي يحصل بواسطة اتصال آلي أو فاكس، للمستهلك الذي لم يعلن موافقته على تلقي مثل هذه الاتصالات.

و عليه تعد إرسال رسائل الاستبيان المباشر للمستهلك عبر بريده الإلكتروني دون موافقته المسبقة إشهار إلكتروني غير مرغوب فيه، معاقب عليه وفقا للمادة 40 من قانون التجارة الإلكترونية.

---

[1] – د/ أسامة أبو الحسن مجاهد، الوسيط في قانون المعاملات الإلكترونية، الكتاب الأول، دار النهضة العربية، القاهرة، 2007، ص193.

[2] – كما تعرض قانون الثقة في الاقتصاد الرقمي الفرنسي لهذا الأمر، حيث تنص المادة 22 منه على أن استخدام عناوين الرسائل الإلكترونية لأغراض تجارية دعائية يتطلب الرضا المسبق من الأشخاص المعنيين، **انظر علاء عمر محمد الجاف، المرجع السابق، ص 165.**

2- عدم تمكين المستهلك من الاعتراض على الرسائل الإلكترونية المرسلة إليه:

إن الرسائل الإشهارية التجارية الإلكترونية التي تتم عبر البريد الإلكتروني للمستهلك غير تلك المتعلقة بالاستبيان المباشر، لا تحتاج إلى موافقة المستهلك المسبقة على تلقيها، غير أن المشرع ألزم المورد الإلكتروني بتمكين المستهلك من الاعتراض عليها[1].

فعدم تمكين المستهلك من الاعتراض على الإشهارات الإلكترونية المرسلة إليه وفقا للمادة 32 السابق ذكرها، يقوم على أساسين، فالأول يتمثل في عدم توفير المعلن نظام يسمح للمستهلك بتسجيل اعتراضه على وصول الإشهار الإلكتروني إليه، أما الثاني فهو عدم احترام رغبة المستهلك في عدم إرسال الإشهارات التجارية إليه. و سنحاول تحديد كل منهما على النحو التالي:

أ-عدم توفير نظام يسمح للمستهلك بالاعتراض على إرسال الإشهارات الإلكترونية:

تقوم الجريمة وفق لهذه الصورة بمجرد عدم توفيره المورد الإلكتروني لنظام يسمح للمستهلك بالاعتراض على إرساله للإشهارات الإلكترونية[2]، و هذا ما يعرف بنظام قائمة الرفض أو الاعتراض، و طبقا لهذا النظام يقوم المعلن بإرسال إعلاناته إلى بريد المستهلك دون أن يسأله عن موافقته على الإرسال، فإذا لم يرغب المستهلك في تلقي المزيد من الإعلانات، عليه أن يرسل هذه الرغبة إلى المرسل، و الذي بدوره يقوم بإعداد قائمة يسجل فيها عناوين البريد الإلكتروني الذين اعترضوا على وصول الإعلانات إليهم[3].

إذ يشترط المشرع الجزائري على المورد الإلكتروني عملا بهذا النظام أن يزود المرسل إليه (المستهلك) بالوسائل الإلكترونية و التقنية التي تسمح لهم بتسجيل اعتراضهم

---

[1] - المادة 32 من قانون 18-05 المتعلق بالتجارة الإلكترونية " يجب على المورد الإلكتروني أن يضع منظومة إلكترونية يسمح من خلالها لكل شخص بالتعبير عن رغبته في عدم تلقي أي إشهار منه عن طريق الاتصالات الإلكترونية، دون مصاريف أو مبررات".

[2] - أنظر الفقرة الأولى من المادة 32 من قانون18-05 المتعلق بالتجارة الإلكترونية .

[3] - VERBIEST (TH) : commerce èlectronique : le nouveau cadre juridque. Op. cit.p 44.

على ما يتسلموه من إشهارات تجارية إلكترونية غير مرغوب فيها، و عليه فإن عدم توفير هذه الآلية أو الوسيلة للمستهلك لإبداء اعتراضه هو سلوك مجرم يعاقب عليه المشرع الجزائري وفقا للمادة 40 من قانون التجارة الإلكترونية.

ب-عدم احترام رغبة المستهلك في عدم استقبال الرسائل الإلكترونية:

لا يكفي توفير المورد الإلكتروني نظام يسمح للمستهلك بالاعتراض على تلقي الإعلانات التجارية الإلكترونية، بل وجب على هذا الأخير احترام رغبة المستهلك عند اعتراضه على وصول هذه الإشهارات الإلكترونية إليه، و ذلك من خلال تسليم وصل استلام عن طريق الاتصال الإلكتروني يؤكد من خلاله للمستهلك تسجيل طلبه، مع اتخاذ التدابير اللازمة لتلبية رغبة المستهلك في غضون 24 ساعة[1].

و الملاحظ على المشرع الوطني هنا، أنه لم يحدد المدة الزمنية لتسليم وصل الاستلام الذي يؤكد من خلاله للمستهلك تسجيل طلبه، كما لم يوضح لحظة بداية احتساب مدة 24 ساعة، و عليه يجب على المشرع تحديد هذين الالتزامين بدقة، و الراجح لنا أن مدة 24 ساعة تبدا من لحظة تسجيل المستهلك لاعتراضه سواء تم تسليم وصل استلام من طرف المورد الإلكتروني أم لا.

و عليه فإن ارسل المورد الإلكتروني أي رسالة إشهارية إلكترونية أخرى بعد مرور 24 ساعة من لحظة تسجيل المستهلك لاعتراضه يعد إشهار غير مشروع وفقا للمادة 40 من قانون التجارة الإلكترونية.

فالمشرع الجزائري لا يعد إرسال الإشهار التجاري الإلكتروني إلى المستهلك أمرا غير مشروع، إذا تم قبل اعتراض المستهلك على هذا الإشهار الإلكتروني، و لكنه يعد كذلك إذا لم يمكن المستهلك من الاعتراض على هذه الإشهارات، أو لم يحترم رغبة المستهلك بعد 24 ساعة من هذا الاعتراض.

[1] - انظر المادة 2/32 من قانون 18-05 المتعلق بالتجارة الإلكترونية .

ثانيا: الركن المعنوي لجريمة الإشهار الإلكتروني غير المرغوب فيه

أما الركن المعنوي لهذه الجريمة، فبالنظر إلى الطبيعة المادية لجريمة الإشهار الإلكتروني غير المرغوب فيه، فإن الركن المعنوي غير متطلب بحيث يكفي توافر السلوك المادي المجرم. فالجريمة تتوافر إما لارتكاب خطأ عمدي في صورة سوء النية أو لارتكاب فعلا غير عمدي لمجرد إهمال بسط أو عدم الحيطة[1] التي تترتب عن عدم أخذ موافقة المستهلك في الاستبيان المباشر أو عدم تمكينه من الاعتراض على الرسائل الإشهارية الإلكترونية.

ثالثا: العقوبة المقررة لجريمة الإشهار التجاري الإلكتروني غير المرغوب فيه

كيف قانون التجارة الإلكترونية رقم 18-05 جريمة الإشهار التجاري الإلكتروني غير المرغوب فيه على أساس جنحة و ذلك بموجب المادة 40 منه، و أفرد له عقوبة مالية تتراوح بين 50.000 دج إلى 500.000 دج [2]. أما في حالة العود فتضاعف العقوبة حيث تصبح غرامة من 100.000دج إلى 1.000.000دج[3].

كما أجاز قانون التجارة الإلكترونية المصالحة في الجرائم المتعلقة بالإشهار الإلكتروني غير المشروع عامة بما فيها جريمة مخالفة شروط الإشهار التجاري الإلكتروني[4]، حيث أن القاعدة العامة في تحديد غرامة الصلح في قانون التجارة الإلكترونية هيا الحد الأدنى لعقوبة الغرامة المقررة للجريمة، و هو ما نصت عليه المادة 46 من نفس القانون. و عليه فإن غرامة الصلح في جريمة الإشهار الإلكتروني غير المرغوب فيه تساوي 50.000دج. كما منح المشرع الوطني للمورد الإلكتروني الذي قبل

---

[1] – روسطم عطية موسى نو، الحماية الجنائية للمستهلك من الغش في مجال المعاملات التجارية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2014، ص 260.

[2] – أنظر المادة 40من قانون18-05 المتعلق بالتجارة الإلكترونية .

[3] – المادة 48 من قانون18-05 المتعلق بالتجارة الإلكترونية " يضاعف مبلغ الغرامة في حالة تكرار نفس الجريمة خلال مدة لا تتجاوز اثنى عشر (12) شهر من تاريخ العقوبة المتعلقة بالجريمة السابقة".

[4] – المادة 45 من قانون18-05 المتعلق بالتجارة الإلكترونية " دون المساس بحقوق الضحايا في التعويض، تؤهل الإدارة المكلفة بحماية المستهلك بالقيام بإجراءات الصلح مع الأشخاص المتابعين بمخالفة أحكام هذا القانون".

بغرامة الصلح المقترحة من طرف الإدارة المعنية (مصالح التجارة) بتخفيض في غرامة الصلح قدره 10 بالمئة[1].

[1] – المادة 46 من قانون 18-05 المتعلق بالتجارة الإلكترونية " مبلغ غرامة الصلح هو الحد الأدنى من الغرامة المنصوص عليها في أحكام هذا القانون".

المطلب الثاني: الحماية الجنائية لحق المستهلك في الإعلام الإلكتروني

أظهر التقدم العلمي و التكنولوجي وسائل عديدة للاتصال تجمع المهني بالمستهلك، و أنواع كثيرة من السلع و المنتجات يتفاوت علم المستهلك و درايته الفنية بها، و أمام الخبرة المتواضعة للمستهلك العادي مقارنة بالمهني المتخصص، وجب على هذا الأخير تزويد المستهلك بكل المعلومات المتعلقة بالسلعة أو الخدمة[1].

و إن كان هذا الالتزام عاما يخص كل عقود الاستهلاك، فيتسع نطاقه و تعظم أهميته في عقود الاستهلاك الإلكترونية، لأن التعاقد يتم عن بعد دون التقاء حقيقي بين طرفيه، و دون تمكين المستهلك من تفحص المبيع محل التعاقد، لذا حرصت المشرع الجزائري على تنظيم و تطبيق هذا الالتزام في هذا النوع من المعاملات الإلكترونية من خلال قانون 18-05 المتعلق بالتجارة الإلكترونية، و رتب المسؤولية الجزائية عند مخالفته . و من أجل تحديد هذه الحماية الجنائية و جب تحديد ماهية الالتزام بالإعلام الإلكتروني (الفرع الأول)، و تحديد صور الحماية الجنائية المقررة لهذا الالتزام (الفرع الثاني).

الفرع الأول: ماهية الالتزام بالإعلام الإلكتروني.

الالتزام بالإعلام أحد أهم الوسائل التي أقرتها التشريعات لحماية الطرف الضعيف في العلاقة العقدية (المستهلك) في مواجهة الطرف الأقوى (المهني أو المورد الإلكتروني)، فمعظم عقود الاستهلاك تتم بين منتجين محترفين و مستهلك يفتقر للمعلومات الكافية عن السلعة أو الخدمة لا سيما إذا كان هذا التعاقد عن بعد[2].

---

[1] – د/ هدى عبد الله، النظام القانوني للفترة السابقة للتعاقد، دراسة مقارنة، المنشورات الحقوقية، بيروت، لبنان، 2004، ص3.

[2] – كراشي ليلى، "**حماية رضا المستهلك في ظل قواعد حماية المستهلك**" ، حوليات جامعة الجزائر، العدد 31، الجزء الرابع، ص 106

لذا نظم المشرع الوطني هذا النوع من الإلتزامات من خلال قانون 18-05 المتعلق بالتجارة الإلكترونية ، و لتعرف على ماهية حق المستهلك في الإعلام الإلكتروني لابد لنا أن نبحث في مفهومه (الفقرة الأولى) و تحديد مضمونه (الفقرة الثانية).

الفقرة الأولى: مفهوم الالتزام بالإعلام الإلكتروني

الالتزام بالإعلام هو احد ابرز الآليات القانونية في مجال حماية المستهلك، فان كان هذا الالتزام مهما في التعاقدات التقليدية فهو اكثر أهمية في التعاملات الإلكترونية، حيث أن هذا التعاقد يتم دون التقاء حقيقي بين أطراف التعاقد، إذ أن معاينة الشيء محل التعاقد معاينة غير مادية. لذلك وجب تهديد مفهومه و ذلك من خلال تعرفه (أولا)، و تحديد الأهداف المرجوة منه (ثانيا).

أولا: تعريف الالتزام بالإعلام الإلكتروني

بالرغم من التنظيم القانوني للالتزام بالإعلام في قانون التجارة الإلكترونية إلا أن المشرع الوطني لم يضع تعريفا له، غير أنه بالرجوع إلى بعض المراسيم التنظيمية خاصة المرسوم التنفيذي رقم 13-378 المحدد للشروط و الكيفيات المتعلقة بإعلام المستهلك[1] نجده يعرف حق المستهلك في الإعلام بأنه " كل معلومات متعلقة بالمنتوج موجهة للمستهلك على بطاقة أو أي وثيقة أخرى مرفقة به أو بواسطة أي وسيلة أخرى بما في ذلك الطرق التكنلوجيا الحديثة أو من خلال الاتصال الشفهي"[2].

أما فقها فقد تنوعت التعريفات لهذا الالتزام بغض النظر عن التسميات المختلفة التي أطلقت عليه[3]، و أن كانت تستند إلى أرضية مشتركة، تتمثل في أنها التزام عام يتوافر بصفة أساسية في المرحلة السابقة على التعاقد في عقود الاستهلاك، من أجل تنوير

[1] – مرسوم تنفيذي رقم 13-378 مؤرخ في 9 نوفمبر سنة 2013، يحدد الشروط و الكيفيات المتعلقة بإعلام المستهلك، جريدة رسمية، عدد 58، صادرة في 18 نوفمبر سنة 2013.

[2] – أنظر المادة 15/3 من المرسوم التنفيذي رقم 378/13 المتعلق بشروط و كيفيات إعلام المستهلك.

[3] – أطلقت تسميات أخرى لهذا الالتزام ، فسماه البعض الالتزام بالتبصير، و البعض الآخر الالتزام بالأخبار، في حين يرى آخرون أنه التزام بالإفضاء بالبيانات و المعلومات. **أنظر علاء عمر محمد الجاف، المرجع السابق، ص 190.**

المستهلك. فيعرف الالتزام بالإعلام بأنه التزام أحد طرفي العقد بتقديم البيانات و المعلومات كافة، الكفيلة بمساعدة الطرف الآخر على إبرام العقد أو تنفيذه، فضلا عن تحذيره و لفت نظره إذا تطلب الأمر ذلك[1]، و يعرف أيضا بأنه التزام قانوني عام يسبق إبرام العقد، و يضع على عاتق المدين التزاما بإعلام الدائن في ظروف معينة إعلاما صحيحا و صادقا بكل ما يتعلق من معلومات جوهرية بالعقد المراد إبرامه، و التي يعجز عن الإحاطة بها بوسائله الخاصة ليبني عليها رضاه الخاص[2].

و هناك من يرى بأنه التزام سابق على التعاقد يلتزم به أحد المتعاقدين، بأن يقدم للمتعاقد الآخر عند تكوين العقد، البيانات اللازمة لإيجاد رضاء سليم كامل و مستنير، إذ يصبح للمتعاقد الآخر على علم بتفصيلات هذا العقد كافة، و ذلك بسبب ظروف و اعتبارات قد تعود إلى طبيعة العقد أو صفة أحد طرفيه أو طبيعة محله[3]. أو أنه وضع المستهلك في بر الأمان ضد مخاطر المنتج الذي يشتريه سواء كان سلعة أو خدمة و هو ما يفرض على المهني التزاما بإعلام المستهلك بكل ظروف العقد و ملابساته[4].

أما تعريف الالتزام بالإعلام الإلكتروني، فإنه لا يختلف كثيرا عن سابقه إلا فيما يتعلق بالوسائط الإلكترونية، و قد عرف بأنه التزام قانوني سابق على إنشاء العقد الإلكتروني، يلتزم بموجبه أحد الطرفين الذي يكلك معلومات جوهرية متعلقة بالعقد المراد إبرامه، و تقديمها بوسائل إلكترونية في الوقت المناسب و بكل وضوح و أمانة للطرف الآخر الذي لا يستطيع العلم بها بوسائله الذاتية[5].

---

[1] – د/ محمد مرسي زهرة، الحماية المدنية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2008، ص 172.

[2] – د. خالد جمال احمد حسن، الالتزام بالإعلام قبل التعاقد، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999 ، ص 82.

[3] – د./ نبيل احمد صبيح، حماية المستهلك في التعاملات الإلكترونية، الدار الجامعية، بيروت، 2008، ص 206.

[4] – د/ خالد جمال احمد حسن، المرجع السابق، ص 83.

[5] – السيد محمد السيد عمران، الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الأنترنت، الدار الجامعية بيروت، 2006 ، ص 29.

و يعرف بأنه التزام عام يغطي المرحلة السابقة على التعاقد في جميع العقود الإلكترونية[1]، كما يعرف أيضا بأنه التزام يقع على عاتق الطرف المقابل للمستهلك في عقود التجارة الإلكترونية[2].

كما يقول البعض أن الالتزام بالإعلام لا ينصب فقط على الشيء المبيع، بل كذلك على أمانة تحديد الشخصية الحقيقية للمتدخل سواء في البيع العادي أو الإلكتروني، حتى يكون للمستهلك على بينة من أمره، أي مع من يتعاقد، لذا فلا بد من تحديد مركز البائع القانوني، و مكان تواجده، و كذلك توضيح التزاماته و مدى إمكانية تنفيذها، لأن البائع يعتبر عنصر أمان للمشتري المتعاقد، خاصة في مجال التعاقد الإلكتروني[3].

و في ضوء ما تقدم يمكن تعريف الالتزام بالإعلام الإلكتروني بأنه " التزام عام ينتهي عند إبرام العقد الإلكتروني، يرد على البيانات و المعلومات الجوهرية التي يجهلها المستهلك الإلكتروني، و يصعب الحصول عليها بوسائله الخاصة دون تدخل الإيجابي للمهني من اجل تكوين إرادة حرة و سليمة قادرة على إبرام العقد".

ثانيا: الهدف من الالتزام بالإعلام الإلكتروني

يعد الالتزام بالإعلام الإلكتروني بصفة خاصة السبيل الأساسي لإعلام المستهلك في التعاقد عبر التجارة الإلكترونية، و لعله الوسيلة الأفضل للوصول إلى المساوات بين المتعاقدين، فضلا عن تحقيق التوازن العقدي و هما الهدفان الرئيسيان لوجود الالتزام بالإعلام الإلكتروني قبل التعاقد[4].

إن التفكير في تطبيق المساوات بصورة منهجية في العقود، يقودنا بالضرورة إلى تحقيق العدالة العقدية، التي تقتضي تحقيق التوازن بين الالتزامات المتولدة عن العقد

---

[1] – د./غازي أبوا عرابي، "**الالتزام بالإعلام قبل التعاقد عبر شبكة الأنترنت**"، مجلة علوم الشريعة و القانون، المجلد الرابع و الثلاثون، الجامعة الأردنية، 2007، ص 566.

[2] – د/ خالد ممدوح إبراهيم، حماية المستهلك في العقد الإلكتروني، طبعة1 ، دار الفكر الجامعي، الإسكندرية، 2008، ص 34.

[3] – د/ السيد محمد السيد عمران، المرجع السابق، ص84.

[4] – د/ علاء محمد الجاف، المرجع السابق، ص 204.

بحيث لا تطغى مصلحة على أخرى أو يتربح طرف فيه على حساب الآخر دون وجه حق[1].

إن عدم المساوات في العلم بين المنتج أو التاجر أو المهني من جهة و بين المشتري أو المستهلك من جهة أخرى هو المبرر الأساسي إلى وجود و بلورة الالتزام بالإعلام الإلكتروني في التعاقد في عقود التجارة الإلكترونية، و خاصة عبر شبكة الأنترنت بهدف تحقيق المساوات في العلم أو تضييق الفجوة في المعرفة بين المتعاقدين[2]، الفجوة التي جاءت نتيجة التقدم العلمي و الصناعي و التقني، و ما رافق هذا التطور من انتشار وسائل الاتصال الحديثة عبر الهواتف النقالة أو عبر شبكة الأنترنت[3]، لذلك كان من المحتم أن ينتج عن هذا التطور بشأن السلع و الخدمات المعلن عنها عبر وسائل الاتصال المختلفة، خاصة مع وجود أنواع كثيرة و جديدة من السلع و الخدمات و المنتجات التي من الصعب الإحاطة بكل تفصيلاتها و بياناتها و الدراية بطرق استعمالها و أسلوب تفادي أضرارها و خطورتها[4].

إن التباين في المعرفة و انعدام المساوات في المعاملات بين المتعاقدين الخاصة بمحل و شروط العقد، هي في المرتبة نفسها التي يحتلها عدم توازن العقد عند وجود اختلاف في المراكز القانونية، في ضوء استغلال الطرف القوي للطرف الضعيف، كون الأول صاحب الخبرة و المعرفة و الدراية الفنية[5].

من الواضح أن اختلال التوازن المعرفي لمصلحة المهني أو الحرفي، يجعل المستهلك حينما يقدم على إبرام العقد، يفتقر إلى المعلومات و البيانات الرئيسية التي تحدد أوصاف و خصائص السلع و الخدمات محل العقد، و تقري مدى ملائمة هذه السلع و

---

[1] – حسن عبد الباسط جميعي، حماية المستهلك (الحماية الخاصة لرضا المستهلك في عقود الاستهلاك) دار النهضة العربية، القاهرة، 1996، ص 21.

[2] – خليفي مريم، "**الالتزام بالإعلام الإلكتروني و شفافية التعامل في مجال التجارة الإلكترونية**"، مجلة دفاتر السياسة و القانون، العدد الرابع، 2011، ص 116.

[3] – علاء محمد الجاف، المرجع السابق، ص 205.

[4] – د/ حسن عبد الباسط الجميعي، المرجع السابق، ص 21.

[5] – د/ علاء عمر محمد الجاف، مرجع سابق، ص 205.

الخدمات لرغباته و ميولته[1]، فضلا عن كفايتها لإشباع رغباته، لذلك فإن هذا الفرق بالعلم يبرر تقرير الالتزام بالإعلام على عاتق الطرف الذي يعلم، سواء الحرفي أو صاحب الخبرة و الدراية من المهنيين.

و من الملاحظ أن وجود هذا الالتزام يرتبط بجهل المستهلك و عدم خبرته، و أن هذا الجهل الذي يبرر قيام الالتزام بالإعلام هو الجهل المشروع و ليس الجهل غير المقبول، و استنادا إلى ذلك فإن الجهل و عدم الخبرة الذي من المفروض و جوده هو "الجهل المشروع و المبرر قانونا"[2].

الفقرة الثانية: مضمون الالتزام بالإعلام الإلكتروني

يهدف الالتزام بالإعلام إلى تحقيق التوازن العقدي بين أطرافه، و لذلك يتوجب على المورد الإلكتروني تنوير إرادة المستهلك بمجموعة من المعلومات المتعلقة بالمنتوج، و بالرجوع إلى التشريع الجزائري لا سيما المادة 11 و 12 من قانون التجارة الإلكترونية و بعض المراسيم التنفيذية الصدارة في هذا المجال[3]، و بعد الاطلاع على بعض القوانين المقارنة و منها قانون الاستهلاك الفرنسي نجد أن المعلومات التي يتوجب على المتدخل الإدلاء بها تتمثل في المعلومات الخاصة بالبائع الإلكتروني (أولا)، المعلومات المتعلقة بالصفات الأساسية للسلعة أو الخدمة المعروضة إلكترونيا (ثانيا)، المعلومات المتعلقة بثمن المنتوج أو الخدمة المعروضة إلكترونيا (ثالثا)، المعلومات المتعلقة بالشروط العامة للتعاقد (رابعا).

أولا: المعلومات الخاصة بالبائع الإلكتروني.

إن أكثر ما يهم المستهلك عند إبرامه لعقود التجارة الإلكترونية بشكل عام و عبر شبكة الأنترنت بشكل خاص، هو معرفة شخصية البائع (المورد الإلكتروني) الذي يتعامل

[1] – د. عبد المنعم موسى إبراهيم، حماية المستهلك ، دراسة مقارنة، طبعة1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص 327.

[2] – د/ حسن عبد البسط جميعي، حماية المستهلك، مرجع سابق، ص 22.

[3] – لا سيما المرسوم التنفيذي رقم 13–378 المتعلق بالشروط و الكيفيات إعلام المستهلك.

معه، و ذلك أن طبيعة التعاقد الإلكتروني تتطلب الوضوح في جميع خطواته[1]، و لعل الأهم ما فيها هو معرفة و تحديد شخصية البائع أو المورد الإلكتروني بشكل قاطع لا يقبل الشك، و من منطق الحرص على ديمومة الثقة و الشفافية التي تسمح بتشجيع المعاملات التجارية الإلكترونية مع المستهلكين، فإن البائع يلتزم في نطاق الثقة المشروعة و مبدأ حسن النية بالكشف عن هويته إذ يتضمن عرضه جميع العناصر التي تحدد شخصيته بصورة قاطعة[2]. و قد نص على ذلك التوجيه الأوروبي رقم 7/97 الصادر في 20 مايو 1997 بشأن حماية المستهلكين في العقود عن بعدفي مضمون الفقرة الأولى من المادة الرابعة بأن تتضمن المعلومات التي يتم تزويدها للمستهلك في العقود المبرمة عن بعد هوية المورد المتعامل معه و عنوان[3].

كما نص على ذاك القانون الفرنسي رقم 2004-575 الصادر في 21 يونيو بشأن الثقة في الاقتصاد الرقمي حماية المستهلك و بصفة خاصة المعلومات التي يتعين على البائع إيصالها لعلمه. حيث فرضت المادة 19 منه على الممارسين للتجارة الإلكترونية أن يبرزوا على مواقع الأنترنت التجارية، المعلومات المتعلقة بهوية البائع عبر الشبكة، بأن يبين أسمه و لقبه إذا كان شخصا طبيعيا و عنوان الشركة إذا كان شخصا معنويا ، و يشير إلى عنوان منشأته و عنوان بريده الإلكتروني، و رقم هاتفه. إضافة إلى ذلك يجب إذا كان خاضعا لإجراءات القيد في سجل التجاري و الشركات أو في جدول مهني أن يبرز رقم قيده، و رأس مال الشركة، و مركز إدارتها، و إذا كان يمارس نشاط يخضع لترخيص فعليه أن يظهر على الموقع اسم و عنوان السلطة التي منحت هذا الترخيص[4].

أما في قانون المبادلات و التجارة الإلكترونية التونسي لسنة 2000 فنص المشرع في المادة 25 منه على الزام البائع في المعاملة التجارية الإلكترونية أن يوفر للمستهلك

---

[1] – رمزي بيد الله على الحجازي، الحماية المدنية للمستهلك بعد التعاقد الإلكتروني، منشورات الحلبي الحقوقية، لبنان، 2006، ص 89.

[2] – د. تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الأنترنت، دراسة مقارنة، ط1، بهجات للطباعة، 2009، ص 68.

[3] – أنظر المادة 1/4 من التوجيه الأوروبي رقم 7/97 بشأن حماية المستهلك في العقود المبرمة عن بعد.

[4] – غازي أبو عرابي، المقال السابق، ص 569.

بطريقة واضحة و مفهومة قبل إبرام العقد هوية و عنوان و هاتف البائع أو مؤدي الخدمات[1].

أما المشرع الجزائري فقد ألزم المورد الإلكتروني أن يعرف بالمورد الإلكتروني في العرض التجاري الإلكتروني بالبيانات التالية: رقم التعريف الجبائي، و العناوين المادية و الإلكترونية، و رقم الهاتف ، بالإضافة إلى رقم السجل التجاري أو رقم البطاقة المهنية للحرفي[2]. و الملاحظ أن المشرع لم بين بصورة واضحة و صريحة ماهية المعلومات الخاصة بالمورد الإلكتروني، و قد كان أكثر وضوحا في بيان التزام مقدم الخدمة بوضع البيانات الخاصة بتحديد شخصيته في المرسوم التنفيذي رقم 13-378 المتعلق بالإعلام، من اسم مقدم الخدمة و معلوماته الخاصة و عنوانه أو إذا تعلق الأمر بشخص معنوي عنوان شركته، و مقر شركته و عنوان المؤسسة المسؤولة عن الخدمة إذا كان مقدم الخدمة شخصا آخر، على أن يتم ذلك بأي طريقة تتناسب مع طبيعة التعامل[3].

ثانيا: المعلومات المتعلقة بالصفات الأساسية للسلعة أو الخدمة المعروضة إلكترونيا

يقصد بالصفات الأساسية للسلعة أو الخدمة، المسائل التفصيلية التي يجب أن تصل إلى علم المستهلك، حتى يمكنه إصدار قبول بحرية تامة و دون ضغط أو تضليل، و هو ما يتحقق بوصف المنتج وصفا دقيقا و شاملا يتحقق معه علم المستهلك بالمبيع محل التعاقد علما كافيا نافيا للجهالة[4].

---

[1] – د/ عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، دار الفكر الجامعي، 2004، ص 309.

[2] – أنظر المادة 11 مطة 1 و 2 من قانون 18-05 المتعلق بالتجارية الإلكترونية .

[3] – المادة 55 من المرسوم التنفيذي 13-378 "يجب على مقدم الخدمة أن يعلم المستهلك بكل الوسائل الملائمة حسب طبيعة الخدمة بالمعلومات الآتية: اسم مقدم الخدمة و معلوماته الخاصة و عنوانه أو إذا تعلق الأمر بشخص معنوي عنوان شركته، و مقر شركته و عنوان المؤسسة المسؤولة عن الخدمة إذا كان مقدم الخدمة شخصا آخر...".

[4] – خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2012، ص271.

و في هذا الإطار ألزم التوجيه الأوروبي رقم 7/97 الصادر في 20 مايو 1997 بشأن حماية المستهلك في العقود عن بعد في نص المادة الرابعة الموردين بإعلام المستهلكين ببيان الأوصاف الأساسية للسلع و الخدمات[1].

أما المشرع الفرنسي و من خلال نص المادة 18/121 من تقنين الاستهلاك المعدلة بالمرسوم 741/2001 في 23 أغسطس 2001 فرض على كل مهني إعلام المستهلك الإلكتروني بالمعلومات الواردة في المادة 1/111 من نفس القانون، و بمقتضى المادة 1/111 " يجب على كل مهني بائع للسلع أو مقدم للخدمة قبل إبرام العقد أن يخبر المستهلك بالخصائص الأساسية للسلعة أو الخدمة"[2].

أما المشرع الجزائري فقد فرض على المورد الإلكتروني من خلال قانون التجارة الإلكترونية تزويد المستهلك بالمعلومات المتعلقة بالصفات الأساسية للسلعة أو الخدمة في العرض التجاري الإلكتروني[3] . غير أن المشرع من خلال قانون التجارة الإلكترونية لم يحدد بوضوح طبيعة و خصائص المنتوج ، و بالرجوع إلى المرسوم التنفيذي رقم 13-378 المتعلق بالإعلام و الذي ينص على الإعلام في المعاملات الإلكترونية من خلال المادة 5 منه فإن البيانات الضرورية لإعلام المستهلك حول الصفات الأساسية للسلعة أو الخدمة المعروضة إلكترونيا تتمثل في:

1- البيانات المتعلقة بالصفات الأساسية للسلعة المعروضة إلكترونيا:

فرق المرسوم التنفيذي رقم 13-378 المتعلق بإعلام المستهلك بين المواد الغذائية و غير الغذائية في البيانات الواجب على المتدخل ذكرها في الوسم، فالبيانات الواجب ذكرها في المواد الغذائية حسب المادة 12 من هذا المرسوم هيا: (تسمية البيع للمادة الغذائية. قائمة المكونات، الكمية الصافية المعبر عنها حسب النظام المتري الدولي، التاريخ الأدنى للصلاحية أو التاريخ الأقصى للاستهلاك، الشروط الخاصة بالحفظ و / أو

[1]- أنظر المادة 1/4 من التوجيه الأوروبي رقم 7/97 بشأن حماية المستهلك في العقود المبرمة عن بعد.

[2] - غازي أبوا عرابي، المقال السابق، ص 570.

[3] - أنظر المادة 11 مطة 3 من قانون 18-05 المتعلق بالتجارة الإلكترونية..

الاستعمال، الاسم أو التسمية التجارية و العلامة المسجلة و عنوان المنتج أو الموضب أو الموزع أو المستورد اذا كانت المادة مستوردة، بلد المنشأ و / أو بلد المصدر اذا كانت المادة مستوردة.

بيان حصة الصنع و /أو تاريخ الصنع أو التوضيب، طريقة الاستعمال و احتياطات الاستعمال في حالة ما اذا كان إغفاله لا يسمح باستعمال مناسب للمادة الغذائية، تاريخ التجميع أو التجميد المكثف بالنسبة للمواد الغذائية المعتبة، المكونات و المواد المبينة في المادة 27 من هذا المرسوم و مشتقاتها التي تسبب حساسية أو حساسية مفرطة و التي استعملت في صنع أو تحضير المواد الغذائية و مازالت موجودة في المنتوج النهائي و لو بشكل مغاير، الوسم الغذائي، بيان" نسبة حجم الكحول المكتسب" بالنسبة للمشروبات التي تحتوي على اكثر من 1.2 بالمئة من الكحول حسب الحجم، مصطلح "حلال" للمواد الغذائية المعتبة، إشارة إلى رمز إشعاع الأغذية المحدد في الملحق الثالث من المرسوم مصحوب بإحدى البيانات التالية: مؤين أو مشع عندما تكون المواد الغذائية معالجة بالقرب من اسم الغذاء). و على الرغم من إجبارية ذكر هذه البيانات في الوسم إلا أن المشرع قد نص على استثناءات في بعض المواد الغذائية فيما يخص بيانات الوسم[1].

أما بالنسبة للبيانات الواجب ذكرها في وسم المواد غير الغذائية سواء كانت أداة أو وسيلة أو جهاز أو آلة أو مادة موجهة للاستعمال الخاص أو المنزلي، فحسب المادة 38

[1] – نظم المرسوم التنفيذي 13-378 بيانات الواجب ذكرها في بعض المواعد الغذائية ، حيث تضمنت المادة 16 منه أن القار ورات الزجاجية الموجهة لإعادة الاستعمال و المطبوعة بطريقة يتعذر محوها و التي لا تحمل بطاقة و لاختما و لا معلقة، تكون بياناتها الإلزامية كالتالي:(تسمية البيع للمواد الغذائية، قائمة المكونات، المكونات و المواد المذكورة في المادة 27 ، و مشتقاتها التي تسبب حساسيات أو حساسيات مفرطة و المستعملة في صنع أو تحضير المادة الغذائية و التي تبقى موجودة في المنتوج النهائي و لو بشكل مغاير، الكمية الصافية، التاريخ الأدنى للصلاحية أو التاريخ الأقصى للاستهلاك، الوسم الغذائي، بيان الحصة و / أو تاريخ الصنع).
و تضمنت المادة 17 أيضا البيانات الإلزامية للوسم الواجب توافرها في بعض المواد الغذائية باستثناء التوابل و الأعشاب العطرية و التي تكون تغليفاتها أو أوعيتها تقل مساحتها عن عشرين سنتمتر مربع، و هذه البيانات هيا (تسمية البيع للمواد الغذائية، الكمية الصافية، التاريخ الأدنى للصلاحية أو التاريخ الأقصى للاستهلاك).

من المرسوم التنفيذي رقم 13-378 المتعلق بإعلام المستهلك، أنه بالإضافة إلى البيانات المنصوص عليها في التشريع و التنظيم المعمول بهما[1] يجب أن يشمل الإعلام ما يلي : (تسمية البيع للمنتوج، الكمية الصافية للمنتوج، المعبر عنها بوحدة النظام المتري الدولي، اسم أو عنوان الشركة أو العلامة المسجلة و عنوان المنتج أو الموضب أو الموزع أو المستورد عندما يكون المنتج مستوردا، بلد المنشأ ة / أو المصدر عندما يكون المنتوج مستوردا، طريقة استعمال المنتوج، تعريف الحصة أو السلسلة و / أو تاريخ الإنتاج، التاريخ الأقصى للاستعمال، الاحتياطات المتخذة في مجال الأمن، مكونات المنتوج و شروط التخزين، علامة المطابقة المتعلقة بالأمن، بيان الإشارات و الرموز التوضيحية للأخطار المذكورة في الملحق الرابع بهذا المرسوم).

2-البيانات المتعلقة بالصفات الأساسية للخدمة المعروضة إلكترونيا:

أما بالنسبة للبيانات الخاصة بالخدمات، فقد ألزم المشرع على مقدمو الخدمات إلكترونيا قبل إبرام العقد أن يعلم المستهلك بصفة واضحة و دون لبس المعلومات التالية: الخصائص الأساسية للخدمة المقدمة[2]، اسم مقدم الخدمة و معلوماته الخاصة و عنوانه أو إذا تعلق الأمر بشخص معنوي عنوان شركته و مقر شركته و عنوان المؤسسة المسؤولة عن الخدمة اذا كان مقدم الخدمة شخصا آخر، رقم القيد في السجل التجاري أو في سجل الصناعة التقليدية و الحرف، رقم و تاريخ الرخصة و اسم و عنوان السلطة التي سلمتها بالنسبة للنشاطات التقنية، كيفيات التنفيذ و الدفع، مدة صلاحية العرض و سعره،

[1] – من بين المواد الغير غذائية التي صدر تنظيم خاص بها مواد التجميل ، حيث وردت البيانات الخاصة بها في المادة 10 من المرسوم التنفيذي 37/97 المؤرخ في 1997/01/14 المتعلق بصياغة مواد التجميل و التنظيف البدني، جريدة رسمية عدد 4، و من بين هذه البيانات (تسمية المبيع، الاسم التجاري، الكمية الإسمية، وقت التوضيب، تاريخ الانتهاء، الظروف الخاصة بالحفظ، تاريخ الصنع، التركيب و الشروط الخاصة بالاستعمال و المخاطر).

و من بين المواد الغير الغذائية أيضا اللعب، التي ذكرت بيناتها في المرسوم التنفيذي رقم 494/97 المؤرخ في 1997/12/21 المتعلق بالوقاية من أخطار اللعب جريدة رسمية عدد 85. و من بين البيانات الإجبارية التي يجب أن تتضمنها اللعبة (تسمية المنتوج، طريقة الاستعمال، التحذير، الاسم التجاري،...).

[2] – انظر المادة 53 من المرسوم التنفيذي رقم 13-378. المتعلق بالشروط و الكيفيات الأساسية بإعلام المستهلك.

المدة الدنيا للعقد المقترح، عندما يتضمن تزويدا مستمرا أو دوريا للخدمة، البنود المتعلقة بالضمان، شروط فسخ العقد[1].

ثالثا: المعلومات المتعلقة بثمن المنتوج أو الخدمة المعروضة إلكترونيا

الثمن هو المقابل المادي للحصول على السلعة أو الخدمة، و الذي يلتزم المهني بإعلامه للمستهلك، و يعد الثمن أحد البيانات الجوهرية التي يتعين على المهني تضمينها للعرض، كما لا يمكن الجزم بأن إرادة المستهلك أصبحت مستنيرة بشكل كافي لإبرام العقد بمجرد التعرف على خصائص السلع و شخصية المتعاقد، بل إن هذه المعلومة تدخل ضمن أولوياته لمعرفة مدى تناسب الثمن المعلن مع المواصفات الخاصة بالسلعة أو الخدمة، و كذلك مدى ملائمة الثمن مع إمكانياته المادية للتعاقد، و بناء عليه قد يقدم المستهلك على التعاقد أو ينصرف عنه[2].

لذلك ألزمت معظم التشريعات المهني بأن يضمن العرض المقدم للمستهلك ثمن السلعة أو الخدمة المتاحة. فتجد المشرع الفرنسي ينص على ضرورة إعلام المستهلك بثمن السلع و الخدمات من خلال المادة 17/121 من تقنين الاستهلاك المعدلة بالمرسوم رقم 2001-741 الصادر بتاريخ 23 أغسطس 2001 إلى المواد 1/111 و 3/113 و 3/214 التي تنظم الالتزام بالإعلام حول الخائص الأساسية للسلعة أو الخدمة و الإعلام حول الثمن التي تطبق على البيع عن بعد كما تطبق على كل بيع[3]، و بمقتضى المادة 3/113 من تقنين الاستهلاك، و التي تنص على أن " كل بائع لمنتج و كل مقدم لحدمة يجب عليه، أن يعلم المستهلك بالأسعار، و الحدود المحتملة الخاصة بالمسؤولية التعاقدية و الشروط الخاصة بالبيع، عن طرق الإعلانات أو الملصقات، أو علامات على الطريق

[1] – أنظر المادة 55 من المرسوم التنفيذي رقم 13-378. المتعلق بالشروط و الكيفيات الأساسية بإعلام المستهلك.

[2] – CALAIS-AULOY: droit de la consommation. Ed dalloz. 5 éd. 2000. P343.

[3] – أنظر المادة 17/121 من تقنين الاستهلاك الفرنسي.

أو أي طريقة يمكن الإعلام بها و تلك الأسعار و الشروط تكون حسب طرق محددة بقرار رسمي من وزير الاقتصاد، بعد استشارة المجلس القومي للاستهلاك[1].

كما ألزم المشرع الجزائري المورد الإلكتروني بأن يتضمن عرضه التجاري الإلكتروني ثمن السلع و الخدمات المعروضة إلكترونيا من خلال المادة 11 من قانون التجارة الإلكتروني، فالثمن لا يقتصر على سعر السلع و الخدمات فقط، بل يحدد بجميع العناصر المكونة للأسعار و التعريفات الواجب دفعها، كمصاريف التسليم و ضريبة و رسوم الواجب دفعها، كذلك طريقة حساب الأسعار عندما لا يمكن مسبقا[2].

رابعا: المعلومات المتعلقة بالشروط العامة للتعاقد

إن المعلومات المتعلقة بالصفات الأساسية للمنتوج أو ثمنه غير كافية لإعلام المستهلك الإلكتروني ، بل يجب أن يكتمل علمه بمعرفة شروط التعاقد التي تسمح بتوضيح العلاقة العقدية بين طرفي العقد، و التزامات كل منهما، مما يحول دون حدوث نزاعات محتملة[3]، مما جعل التشريعات من بينهم التشريع الجزائري تعطي أهمية خاصة لشروط العقد، لذلك نجد أن المشرع الجزائري يلزم المورد الإلكتروني بذكر جميع البيانات المتعلقة بشروط التعاقد في العرض التجاري الإلكتروني، و هو ما نصت عليه المادة 11 من قانون التجارة الإلكترونية، و المتمثلة على سبيل المثال في : شروط و كيفيات التسليم، شروط الضمان و التجربة و خدمة ما بعد العقد، شروط فسخ العقد، شروط و كيفيات الدفع، البنود المتعلقة بحماية البيانات الشخصية، حالة توفر السلعة أو الخدمة، وصف كامل لمختلف مراحل تنفيذ المعاملة الإلكترونية، مدة صلاحية العرض، شروط و آجال العدول، طريقة تأكيد الطلبية، موعد التسليم، طريقة إرجاع المنتوج و الاستبدال أو التعويض[4].

---

[1] – أنظر المادة 3/113 من تقنين الاستهلاك الفرنسي

[2] – أنظر المادة 11 مطة 8 من قانون18-05 المتعلق بالتجارة الإلكترونية .

[3] – CALAIS-AULOY: op. cit. p 345.

[4] – أنظر المادة 11 من قانون 18-05 المتعلق بالتجارة الإلكترونية.

و في هذا الاطار ألزم التوجيه الأوروبي رقم 7/97 الصادر في 20 مايو 1997 بشأن حماية المستهلك في العقود عن بعد في نص المادة الرابعة سابقة الذكر الموردين بإعلام المستهلك بالمعلومات الخاصة بالعقد كبيان الائتمان و كيفية الدفع و التسليم و التنفيذ، إقرار حق العدول للمستهلك، و مدة صلاحية الإيجاب[1].

هو ما أكدت عليه المادة 19/121 من تقنين الاستهلاك الفرنسي المضافة بالمرسوم رقم 2001-741 الصادر في 23 أغسطس 2001 على المورد أن يقدم للمستهلك معلومات حول شروط و طرق ممارسة حق الرجوع في التعاقد، و المعلومات المتعلقة بالخدمة بعد البيع، و الضمانات التجارية، و شروط فسخ العقد[2].

[1] – أنظر المادة 1/4 من التوجيه الأوروبي رقم 7/97 بشأن حماية المستهلك في العقود المبرمة عن بعد.

[2] – أنظر المادة 19/121 من تقنين الاستهلاك الفرنسي.

الفرع الثاني: صور التجريم الواقعة على حق المستهلك في الإعلام الإلكتروني

يعتبر الحق في الإعلام من أهم الآليات القانونية التي أقرها المشرع الوطني لحماية المستهلك في التعاملات الإلكترونية، حيث ألزم قانون التجارة الإلكترونية المورد الإلكتروني بضرورة ذكر جميع البيانات سواء الخاصة بمواصفات السلع و خصائصها أو المتعلقة بالأسعار، و بجميع شروط البيع و مراحله في العروض الإلكترونية التي يقدمها، غير أن إعلام المستهلك الإلكترونية لا يتوقف عند المواصفات الأساسية للسلع و الخدمات، أو أسعار و شروط البيع، بل يتعدى ذلك إلى تحديد مراحل التعاقد بدقة و ضرورة احترامها، حتى يتحقق إعلام كاف للمستهلك قبل إبرام العقد الإلكتروني.

و كل هذه الالتزامات أقر لها المشرع عقوبة عند مخالفتها وفقا للمادة 39 من نفس القانون[1] سواء ما تعلق بمخالفة النظام القانوني للعرض التجاري الإلكتروني، أو عدم احترام مراحل التعاقد. و عليه سنحاول تحديد صور الحماية الجنائية لحق المستهلك الإلكتروني في الإعلام، و التي تشمل كل من جريمة مخالفة شروط العرض التجاري الإلكتروني (الفقرة الأولى)، و جريمة مخالفة مراحل التعاقد الإلكتروني (الفقرة الثانية).

الفقرة الأولى: جريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني

اشترط المشرع أن تكون المعاملات التجارية الإلكترونية مسبوقة بعرض إلكتروني[2] حتى يتحقق إعلام المستهلك بهذا العرض، كما حدد مجموعة من الالتزامات التي ينبغي على المورد الإلكتروني احترامها فيه و هو ما نصت عليه المادة 11 من قانون التجارة

[1] – المادة 39 من القانون رقم 18-05 المتعلق بالتجارة الإلكترونية " يعاقب بغرامة مالية من 50.000 دج إلى 500.000 دج، كل مورد إلكتروني يخالف إحدى الالتزامات المنصوص عليها في المادتين 11 و 12 من هذا القانون، كما يجوز للجهة القضائية التي رفعت أمامها الدعوى أن تأمر بتعليق نفاذه إلى جميع منصات الدفع الإلكتروني، لمدة لا تتجاوز 6 أشهر".

[2] – المادة 10 من قانون18-05 المتعلق بالتجارة الإلكترونية " يجب أن تكون كل معاملة تجارية إلكترونية مسبوقة بعرض تجاري إلكتروني..."

الإلكترونية[1]، و مخالفة هذه الالتزامات يعد مخالفة لنظام العرض التجاري الإلكتروني وفقا للمادة 39 من نفس القانون[2]. و هو بذلك اعتداء على حق المستهلك في الإعلام.

و حتى تقوم جريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني وجب توافر كل من أركانها، و سنحاول تحديد كل من ركنها المادي (أولا) ثم ركنها المعنوي (ثانيا)، و العقوبة المقررة لها (ثالثا).

أولا: الركن المادي لجريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني

من خلال استقرائنا للمادتين 39 و 11 من قانون التجارة الإلكترونية فإن جريمة مخالفة النظام القانوني للعرض التجاري من الجرائم الشكلية، التي تقوم بمجرد إتيان السلوك الإجرامي، و صور السلوك الإجرامي المكونة للركن المادي لهذه الجريمة تختلف باختلاف صور الالتزامات المفروضة على المورد الإلكتروني، فمنها ما يتعلق ببيانات العرض التجاري الإلكتروني، و منها ما يتعلق بشروطه، و سنحاول توضيح ذلك على النحو التالي:

1- إغفال أحد البيانات الإلزامية التي يتطلبها القانون في العرض الإلكتروني:

يتحقق السلوك المجرم في هذه الحالة بمجرد امتناع المورد الإلكتروني عن ذكر أحد البيانات الإلزامية و الإجبارية الخاصة بالمعاملة الإلكترونية في العرض التجاري

---

[1] – المادة 11 من قانون 18-05 المتعلق بالتجارة الإلكترونية "يجب أن يقدم المورد الإلكتروني العرض التجاري الإلكتروني بطريقة مرئية ومقروءة ومفهومة، ويجب أن يتضمن على الأقل، و ليس على سبيل الحصر ما يلي:
– رقم التعريف الجبائي و العنوان المادي و الإلكتروني ، و رقم هاتف المورد الإلكتروني . رقم السجل التجاري أو رقم البطاقة المهنية للحرفي، طبيعة و خصائص و أسعار السلع و الخدمات المقترحة مع احتساب كل الرسوم، حالة توفر السلعة أو الخدمة، كيفيات ومصاريف وآجال التسليم، الشروط العامة للبيع لاسيما البنود المتعلقة بحماية المعطيات ذات الطابع الشخصي، شروط الضمان التجاري وخدمة ما بعد البيع، طريقة حساب السعر، عندما لا يمكن تحديده مسبقا، كيفيات وإجراءات الدفع، شروط فسخ العقد عند الاقتضاء، مدة صلاحية العرض، عند الاقتضاء، شروط وآجال العدول، عند الاقتضاء، طريقة تأكيد الطلبية، المسبقة وكيفيات إلغاء الطلبية المسبقة، عند الاقتضاء.'

[2] – المادة 39 من قانون 18-05 المتعلق بالتجارة الإلكترونية " يعاقب بغرامة من 50.000دج إلى 500.000دج كل مورد إلكتروني يخالف أحد الالتزامات المنصوص عليها في المادتينن11.و 12..، كما يجوز للجهات القضائية التي رفعت أمامها الدعوى أن تأمر بتعليق نفاذه إلى جميع منصات الدفع الإلكتروني لمدة لا تتجاوز ستة أشهر".

الإلكتروني المقدم[1]، و المنصوص عليها على سبيل المثال في المادة 11 من قانون التجارة الإلكترونية و مثال ذلك عدم ذكر البيانات المتعلقة بطبيعة و خصائص المنتوج ، أو سعر الخدمة و شروط العقد أو شروط الضمان أو الخدمة ما بعد البيع أو كيفيات و مصاريف التسليم...إلخ[2] .

و عليه فعدم قيام المورد الإلكتروني بذكر أحد البيانات الإجبارية المتعلقة بالعرض الإلكتروني السابق ذكرها، يؤدي إلى قيام الركن المادي لجريمة مخالفة شروط العرض التجاري الإلكتروني وفقا للمادة 39 من قانون التجارة الإلكترونية.

2- مخالفة شروط العرض التجاري الإلكتروني:

في الواقع أن التزام المورد الإلكتروني بإعلام المستهلك لا يتوقف على ذكر البيانات الجوهرية المتعلقة بالعرض التجاري الإلكتروني، و إنما يرتبط أيضا بشروط عديدة تتعلق بتقديم هذا العرض، و يتمثل عدم الالتزام بهذه الشروط النشاط الإيجابي للركن المادي لهذه الجريمة، و هو إقدام المتدخل بتقديم عرض دون مراعة لشروطه. إذ أوجب المشرع أن يقدم العرض التجاري الإلكتروني **بطريقة مقروءة، فضلا عن كونه مرئيا و مفهوما**[3].

فاشتراط أن يكون العرض مفهوم مرتبط ارتباط وثيقا باللغة التي يفهمها المستهلك، فاللغة التي يفهمها المستهلك من بين الوسائل المهمة لحمايته، و التي أوجدتها المبادئ القانونية المعاصرة لكي يستطيع هذا الأخير فهم و معرفة مضمون العرض الذي يريد التعاقد بشأنه[4]. غير أن المشرع من خلال المادة 11 من قانون التجارة الإلكترونية لم

---

[1] – يعد هذا السلوك من قبيل النشاط السلبي للركن المادي، و يعرف النشاط السلبي على انه إحجاف الشخص عن إتيان واجب قانوني يلزمه بهذا الفعل. **انظر عبد الحليم بوقرين، الحماية الجنائية للمعاملات التجارية، رسالة دكتوراه، جامعة تلمسان، الجزائر، سنة ، ص 303.**

[2] – أنظر المادة 11 من قانون18-05 المتعلق بالتجارة الإلكترونية.

[3] – تنص المادة 11 /1 من قانون 18-05 المتعلق بالتجارة الإلكترونية على أنه " يجب أن يقدم المورد الإلكتروني العرض التجاري الإلكتروني بطريقة مرئية ، و مقروءة و مفهومة"

[4] – محمد إبراهيم أبوا الهجاء، عقود التجارة الإلكترونية، طبعة1، دار الثقافة للنشر و التوزيع، الأردن، 2005، ص 47.

ينص على لغة العرض التجاري مما يفتح المجال أمام جميع اللغات بشرط أن تكون مفهومية لدى المستهلك.

غير أنه بالرجوع إلى الأحكام العامة المتعلقة بحماية المستهلك و بالتحديد المادة 18 من قانون حماية المستهلك و قمع الغش، فقد الزم المشرع المتدخل عند تنفيذ الالتزام بالإعلام حول المنتوجات أن تكون بيانات أو معلومات المنتجات المراد التعاقد حولها بالغة العربية و هي اللغة الوطنية و الرسمية التي يفهمها المستهلك، كما أجاز كتابة بيانات الوسم بلغات أخرى على سبيل الإضافة مع بقاء اللغة العربية هيا الأساس بشرط أن تكون مفهومة لدى المستهلكين[1]. و هو ما جسدته المادة 07 من المرسوم التنفيذي رقم 13-378 المحدد لشروط و الكيفيات المتعلقة بإعلام المستهلك سواء التقليدي أو الإلكتروني[2].

و يبدو من المنطقي لنا، أن مسألة اعتماد اللغة الوطنية في العروض التجارية الإلكترونية أو التعاقد الإلكتروني لا تخلو من الصعوبة، و تبعا لذلك لا نستطيع اشتراط اللغة العربية في ذلك، اعتمادا على طبيعة شبكة الأنترنت بوصفها شبكة عالمية، و العقد الإلكتروني غالبا ما يكون عقدا دوليا، إلا أنه من الممكن الاشتراط على المورد الإلكتروني الوطني اعتماد اللغة العربية بالأساس في عرضه التجاري الإلكتروني ضمن حدود الدولة الجزائرية.

أما بالنسبة لشرط القراءة و المرئية، فيجب أن يكون العرض و خاصة البيانات الإلزامية متواجدة في مساحة تسمح بأن تقع عليها الرؤية مباشرة، و كذا أن تكون مكتوبة بحروف تتماشى مع خلفية الصفحة الرئيسية على الموقع الإلكتروني ذاته بشأن حجم

[1] – المادة 18 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش " يجب أن تحرر بيانات الوسم و طريقة الاستخدام و دليل الاستعمال و شروط ضمان المنتوجات و كل معلومة أخرى منصوص عليها في التنظيم الساري المفعول باللغة العربية أساسا، و على سبيل الإضافة، يمكن استعمال لغة أو عدة لغات أخرى سهلة الفهم من المستهلكين، و بطريقة مرئية و مقروءة و متعذر محوها".

[2] – المادة 07 من المرسوم التنفيذي رقم 13-378 سابق الذكر " يجب أن تحرر البيانات الإلزامية لإعلام المستهلك باللغة العربية أساسا و على سبيل الإضافة يمكن استعمال لغة أو عدة لغات أخرى سهلة الاستيعاب لدى المستهلك و تسجل في مكان ظاهر و بطريقة مرئية و مقروءة بوضوح و متعذر محوها".

الكتابة و الخطوط المستعملة، و بألوان لا تصعب القراءة، بالإضافة أن لا تكون البيانات مخفية أو مستترة بواسطة بيانات أو إشارات أو صور[1].

و عليه فإن خالف المورد الإلكتروني هذه الالتزامات سواء المتعلقة بالبيانات أو بشروط العرض التجاري الإلكتروني قامت الجريمة وفقا للمادة 39 من قانون التجارة الإلكترونية.

ثانيا: الركن المعنوي لجريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني

تعد جريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني من الجرائم التي يقوم ركنها المعنوي بتوافر السلوك المادي المجرم. فالجريمة تتوافر إما لمجرد إهمال بسط أو عدم الحيطة التي تترتب عن عدم كفاية المراقبة الذاتية للعرض الإلكتروني من حيث توفر البيانات الإلزامية التي يتطلبها القانون فيه أو عدم وضوحه.

ثالثا: العقوبة المقررة لجريمة مخالفة شروط العرض التجاري الإلكتروني

لقد عاقب المشرع الوطني على هذه الجريمة من خلال المادة 39 من قانون التجارة الإلكترونية بعقوبة مالية تتراوح بين 50.000 دج إلى 500.000دج، أما في حالة العود فتضاعف العقوبة حيث تصبح غرامة من 100.000 دج إلى 1.000.000 دج[2].

كما أجاز قانون التجارة الإلكترونية المصالحة في الجرائم الماسة بحق المستهلك في الإعلام [3]، حيث أن القاعدة العامة في تحديد غرامة الصلح في قانون التجارة الإلكترونية هيا الحد الأدنى لعقوبة الغرامة المقررة للجريمة، و هو ما نصت عليه المادة 46 من نفس

[1] – محمد شرايرية، الرسالة السابق، ص 106.

[2] – المادة 48 من قانون التجارة الإلكترونية " يضاعف مبلغ الغرامة في حالة تكرار نفس الجريمة خلال مدة لا تتجاوز اثنى عشر (12) شهر من تاريخ العقوبة المتعلقة بالجريمة السابقة".

[3] – المادة 45 من قانون 18-05 المتعلق بالتجارة الإلكترونية " دون المساس بحقوق الضحايا في التعويض، تؤهل الإدارة المكلفة بحماية المستهلك بالقيام بإجراءات الصلح مع الأشخاص المتابعين بمخالفة أحكام هذا القانون".

القانون[1]. و عليه فإن غرامة الصلح في جريمة مخالفة مراحل التعاقد الإلكتروني تساوي 50.000دج.

كما منح المشرع الوطني للمورد الإلكتروني الذي قبل بغرامة الصلح المقترحة من طرف الإدارة المعنية (مصالح التجارة) بتخفيض في غرامة الصلح قدره 10 بالمئة.

بالإضافة إلى العقوبة الأصلية أجاز المشرع للقاضي أن يحكم بعقوبة تكميلية، و تتمثل هذه العقوبة في عقوبة النشر الحكم على جميع منصات الدفع الإلكتروني لمدة لا تتجاوز الستة أشهر[2].

[1] – المادة 46 من قانون18-05 المتعلق بالتجارة الإلكترونية " مبلغ غرامة الصلح هو الحد الأدنى من الغرامة المنصوص عليها في أحكام هذا القانون".

[2] – أنظر المادة 39 من قانون 18-05 المتعلق بالتجارة الإلكترونية.

الفقرة الثانية: جريمة مخالفة مراحل التعاقد الإلكتروني

إن إعلام المستهلك الإلكترونية لا يتوقف عند المواصفات الأساسية للسلع و الخدمات، أو أسعار و شروط البيع، بل يتعدى ذلك إلى تحديد مراحل التعاقد الإلكتروني بدقة و ضرورة احترامها، حتى يتحقق إعلام كاف للمستهلك قبل إبرام العقد الإلكتروني[1]، و هو ما أستحدثه المشرع الوطني من خلال نص المادة12 من قانون التجارة الإلكترونية[2]. و التي أقر عند مخالفته المسؤولية الجزائية وفقا للمادة 39 من نفس القانون. و هذه الجريمة كغيرها من الجرائم تقوم بتوافر كل من ركنها المادي (أولا) و ركنها المعنوي (ثانيا)، كما أقر لها المشرع عقوبة(ثالثا).

أولا: الركن المادي لجريمة مخالفة مراحل التعاقد الإلكتروني

من خلال استقرائنا للمادتين 39 و 12 من قانون التجارة الإلكترونية فإن صور الاعتداءات المكونة للركن المادي لهذه الجريمة تتمثل في مخالفة المورد الإلكتروني لمراحل التعاقد، و التي تعد متكاملة فيما بينها حتى يتحقق علم كاف لدى المستهلك، بدأ بمرحلة وضع للشروط في متناول المستهلك التي تليها مرحلة تمكين المستهلك من مراجعة الطلبية و آخرها مرحلة تمكين المستهلك من تأكيد الطلبية. و عليه سنحاول تحديد السلوك المجرم في كل مرحلة على حدى على النحو التالي:

1- عدم وضع الشروط التعاقدية في متناول المستهلك:

إن عرض السلع في مجال التجارة الإلكترونية تختلف عما هو موجود في التجارة التقليدية فهذه الأخيرة يتمتع فيها المستهلك بحرية معاينة المنتوج و حتى تجربته، أما في مجال التجارة الإلكترونية حيث تكون السلع معروضة على شكل صور أو فيديوهات فإنه

[1] – كوثر سعيد عدنان خالد، المرجع السابق، ص 270.

[2] – المادة 12 من قانون 18-05 المتعلق بالتجارة الإلكترونية الجزائري "تمر طلبية منتوج أو خدمة عبر ثلاث مراحل إلزامية: وضع شروط التعاقد في متناول المستهلك...، التأكد من تفاصيل الطلبية من طرف المستهلك ...، تأكيد الطلبية الذي يؤدي إلى تطوين العقد..."

يصعب في كثير من الأحيان على المستهلك الإلكتروني قراءة بياناتها و بالتالي معرفة شروط التعاقد حول المنتوج المعروض للبيع عبر شبكة الأنترنت[1].

و على هذا الأساس فإن المشرع يرى أن عرض البائع في المواقع التجارية لا يكفي لإعلام المستهلك لإبرام العقود الإلكترونية، و إنما يجب على البائع وضع شروط العقد في متناول المستهلك كخطوة أولى لإبرام العقد[2]. و الهدف من تقرير المشرع الجزائري لهذا الحق هو تمكين المستهلك الإلكتروني من التعاقد عبر وسائل الاتصال الإلكترونية بعلم و دراية تامة بكل شروط التعاقد المقدم عليها.

و تتعلق شروط العقد حسب المادة 13 من قانون التجارة الإلكترونية الواجب على المورد الإلكتروني أن يضعها تحت تصرف المستهلك الخصائص التفصيلية للسلع و الخدمات، شروط و كيفيات التسليم، شروط الضمان و خدمات ما يعد البيع، شروط فسخ العقد الإلكتروني، شروط و كيفيات الدفع، شروط و كيفيات إعادة المنتوج، كيفيات معاجلة الشكاوى[3].

و الملاحظ أن تعبير المشرع " **وضع الشروط التعاقدية في متناول المستهلك**" جاء غامضا من حيث الكيفية فقد يكون من خلال إرسالها إلى المستهلك عبر وسائل الاتصال الإلكترونية كالبريد الإلكتروني أو عن طريق عرضها في صفحة مستقلة مع ضرورة التنويه عليها في صفحة العرض الرئيسية أو بتخصيص مكان لها في صفحة العرض. إذ يقع على عاتق المورد الإلكتروني إثبات أنه التزم بوضع شروط العقد تحت تصرف المستهلك.

و عليه فإن امتناع المورد الإلكتروني من وضع الشروط التعاقدية تحت تصرف المستهلك كخطوة أولى لإبرام العقود الإلكترونية يؤدي إلى قيام الركن المادي لهذه الجريمة وفقا للمادة 39 من قانون التجارة الإلكترونية.

---

[1] – عبد الحليم بوقرين، الرسالة السابقة، ص 204.

[2] – أنظر المادة 1/12 من قانون 18-05 المتعلق بالتجارة الإلكترونية.

[3] – أنظر المادة 13 من قانون 18-05 المتعلق بالتجارة الإلكترونية.

2- عدم تمكين المستهلك من مراجعة الطلبية:

ألزم المشرع الجزائري المورد الإلكتروني قبل إبرام العقد و بعد وضع شروط العقد في متناوله تمكين المستهلك من المراجعة النهائية لجميع اختياراته المتعلقة بالطلبية سواء كانت سلعة أو خدمة، و هو ما يعرف بحق المراجعة أو التفكير، باعتباره المرحلة الثانية لإبرام العقد الإلكتروني ، و مهما كانت التسمية فإن هذا الحق هدفه تمكن المستهلك من التفكير و التروي مليا قبل التسرع في التعاقد، إما بتعديل الطلبية أو إلغائها أو بتصحيح الأخطاء، و ذلك من خلال مراجعة تفاصيل الطلبية، و التي ذكرها المشرع على سبيل المثال و تشمل كل من طبيعة المنتوجات و الخدمات المطلوبة و السعر الإجمالي و الوحدوي، الكميات المطلوبة، و ذكر هذه العناصر نظرا لأهميتها حتى لا يقع خطا في الطلبية أو حصول أي تغير في الأسعار من طرف المورد الإلكتروني[1]، و ما دامت هذه العناصر على سبيل المثال فإنه يحق له مراجعة شروط العقد أيضا.

و الحقيقة أن هدف المشرع من هذا التدخل هو القضاء على ظاهرة شائعة عمليا تتمثل برفض بعض المهنيين تسليم نماذج العقود للمستهلكين إلا بعد التوقيع عليها بما يفيد التعاقد، و هذا يؤدي إلى حرمان المستهلك من أي إمكانية للتفكير المسبق في الطلبية و شروط العقد قبل إبرامه، لهذا أصبح تسليم نماذج العقود إلى المستهلك قبل إبرام العقد أمرا الزاميا[2].

و الملاحظ أن المشرع لم يحدد أجلا لممارسة حق المراجعة مما يحد بصفة فعلية من نجاعة مثل هذا الحق، حيث أن عدم تحديد المدة التي يمكن أن يأخذها المستهلك للتفكير قد تحمله على التسرع في التعاقد، حيث أن عدم تحديد المدة التي يمكن للمستهلك فيها مراجعة اختياراته فإنه سيتم تحديدها من طرف المورد الإلكتروني الذي يعتبر في مركز قوة بالنسبة للمستهلك الإلكتروني، كما أنه ستكون هناك صعوبة بالنسبة للقاضي

---

[1] – أنظر الفقرة الثانية للمادة 12 من قانون رقم 18-05 المتعلق بالتجارة الإلكترونية .

[2] – غازي خالد أبو عرابي، "**حماية رضا المستهلك، دراسة مقارنة في قانون حماية المستهلك الإماراتي و تقنين الاستهلاك الفرنسي و مشروع قانون حماية المستهلك الأردني**"، مجلة دراسات علوم الشريعة و القانون الأردنية، العدد الأول، 2009، ص 191.

لتقدير المدة الكافية لفحص الطلبية من طرف المستهلك الإلكتروني[1]. و من جهة أخرى فإن عدم تحديد المدة يمكن أن تحمل البائع على تغيير المعطيات التي وضعها من قبل حيث يمكنه أن يرفع في الثمن أو ينقص من بعض الامتيازات التي قدمها سابقا خلال تلك المدة التي اتخذها المستهلك الإلكتروني للتفكير و ذلك على خلاف التوصية الأوروبية المؤرخة في 11 ديسمبر 1998 و التي تمنع من خلال الفقرة الأولى من الفصل الثالث المهني من تغيير المعطيات التي قدمها لمدة 14 يوم، و هو ما يستنتج منه أن المستهلك له الحق في مراجعة اختياراته خلال تلك المدة، كما تترك الفقرة الثانية من نفس الفصل إمكانية الزيادة في هذه المدة من قبل الأطراف[2].

و عليه فإن امتناع المورد الإلكتروني من تمكين المستهلك الإلكتروني في مراجع الطلبية، خاصة فيما يتعلق بطبيعة المنتوجات و الخدمات المطلوبة و السعر الإجمالي و الوحدوي، و الكميات المطلوبة، يؤدي إلى قيام الركن المادي لهذه الجريمة وفقا للمادة 39 من قانون التجارة الإلكترونية.

3- عدم تمكين المستهلك من تأكيد الطلبية:

أعتبر المشرع الوطني أن تأكيد الطلبة هيا المرحلة الثالثة و الأخيرة لإتمام المعاملة الإلكترونية و التي بموجبها يتكون العقد[3]، غير أنه لم يحدد الكيفية التي يمكن بها ممارسة حق المستهلك في تأكيد الطلبية، غير أن المشرع جعل على عاتق المورد الإلكتروني إلزامية إعلام المستهلك بطريقة تأكيد الطلبية. مما يجعل عبئ إثبات هذا الالتزام يقع على عاتق المورد الإلكتروني. و بذلك فإن لم يمكن المستهلك من تأكيد طلبيته سواء تعلقت باقتناء سلعة أو تقديم خدمة ، تقوم المسؤولية الجزائية في حق المورد الإلكترونية لمخالفته التزام تمكين المستهلك من تأكيد الطلبية.

---

[1] – زوبيدة سميرة، الأحكام القانونية المستحدثة لحماية المستهلك المتعاقد، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو ، الجزائر، 2016، ص 39.

[2] – زوبيدة سمير، الرسالة نفسها، ص 62.

[3] – انظر الفقرة الثالثة من المادة 12 من قانون18-05 المتعلق بالتجارة الإلكترونية.

و عليه فإن أقدم المورد الإلكتروني على مخالفة إحدى المراحل السابق ذكرها يحمله المسؤولية الجزائية وفقا للمادة 39 من قانون التجارة الإلكترونية

ثانيا: الركن المعنوي لجريمة مخالفة مراحل التعاقد الإلكتروني

بالنظر إلى الطبيعة المادية لجريمة مخالفة أو عدم احترام مراحل التعاقد الإلكتروني، فإن الركن المعنوي غير متطلب بحيث يكفي توافر السلوك المادي المجرم. فالجريمة تتوافر إما لمجرد إهمال بسط أو عدم الحيطة التي تترتب عن عدم احترام مراحل التعاقد الإلكتروني التي يتطلبها القانون في المعاملات الإلكترونية[1].

ثالثا: العقوبة المقررة لجريمة مخالفة مراحل التعاقد الإلكتروني

لقد عاقب المشرع الوطني من خلال المادة 39 من قانون 18-05 على هذه الجريمة بعقوبة مالية تتراوح بين 50.000 دج إلى 500.000دج، أما في حالة العود فتضاعف العقوبة حيث تصبح غرامة من 100.000 دج إلى 1.000.000 دج[2].

كما أجاز قانون التجارة الإلكترونية المصالحة في الجرائم الماسة بحق المستهلك في الإعلام [3]، حيث أن القاعدة العامة في تحديد غرامة الصلح في قانون التجارة الإلكترونية هيا الحد الأدنى لعقوبة الغرامة المقررة للجريمة، و عليه فإن غرامة الصلح في جريمة مخالفة مراحل التعاقد الإلكتروني تساوي 50.000دج. كما منح المشرع الوطني للمورد الإلكتروني الذي قبل بغرامة الصلح المقترحة من طرف الإدارة المعنية (مصالح التجارة) بتخفيض في غرامة الصلح قدره 10 بالمئة[4].

---

[1] – أنور محمد صدقي المساعد، المرجع السابق، ص 275.

[2] – المادة 48 من قانون 18-05 المتعلق بالتجارة الإلكترونية " يضاعف مبلغ الغرامة في حالة تكرار نفس الجريمة خلال مدة لا تتجاوز اثنى عشر (12) شهر من تاريخ العقوبة المتعلقة بالجريمة السابقة".

[3] – المادة 45 من قانون 18-05 المتعلق بالتجارة الإلكترونية " دون المساس بحقوق الضحايا في التعويض، تؤهل الإدارة المكلفة بحماية المستهلك بالقيام بإجراءات الصلح مع الأشخاص المتابعين بمخالفة أحكام هذا القانون".

[4] – المادة 46 من قانون18-05 المتعلق بالتجارة الإلكترونية " مبلغ غرامة الصلح هو الحد الأدنى من الغرامة المنصوص عليها في أحكام هذا القانون".

بالإضافة إلى العقوبة الأصلية أجاز المشرع للقاضي أن يحكم بعقوبة تكميلية، و تتمثل هذه العقوبة في عقوبة النشر الحكم على جميع منصات الدفع الإلكتروني لمدة لا تتجاوز الستة أشهر[1].

[1] – أنظر المادة 39 من قانون 18-05 المتعلق بالتجارة الإلكترونية.

المبحث الثاني: الحماية الجزائية الموضوعية للمستهلك من الغش التجاري في مرحلة التعاقد الإلكتروني

يتميز عقد الاستهلاك بشكل عام بمبدأ انعدام التوازن العقدي بين طرفيه المستهلك و المهني، و يتجلى هذا المبدأ بشكل خاص إذا أبرم العقد بوسائل إلكترونية، حيث لا يكون الحضور ماديا بين الطرفين، مما يسمح بتعرضه للخداع عن طريق استعمال وسائل احتيالية بغرض إيقاع المستهلك في غلط يدفعه للتعاقد.

كما أن العقود الإلكترونية وسيلة لتمكين المستهلك من توفير حاجياته التي تعاقد بشأنها، و التي لم تكن له الفرصة الكافية لمعاينها و فحص مواصفاتها، فيقبل الشراء فقط من خلال ذكر المورد الإلكتروني لمواصفات السلع أو مشاهدة صورها عبر العرض الإلكتروني، مما دعي جل التشريعات لاستحداث التزام جديد يقع على عاتق البائع الإلكتروني يتمثل في الحق في ضمان المنتوجات و أمنها.

و عليه سنحاول تحديد الحماية الموضوعية للمستهلك في مرحلة التعاقد الإلكتروني من خلال تحديد الحماية الجنائية لحق المستهلك في ضمان منتوجاته و امنها (المطلب الأول)، كما سنتطرق لحمايته من الخداع و التزوير في هذا النوع من المعاملات (المطلب الثاني).

المطلب الأول: الحماية الجنائية لحق المستهلك في ضمان المنتوجات و أمنها في المعاملات الإلكترونية

يعد عقد البيع وسيلة لتمكين المشتري من الحيازة المادية للمبيع، و ذلك في البيع العادي أو الإلكتروني، لذلك يجب أن تكون هذه الحيازة ملبية لغرض استعمال المشتري، فلا يجب أن يكون الشيء المبيع سلعة أو خدمة غير مطابقة للمواصفات التي اتفقا عليها في العقد أو مشوبا بعيب يؤثر في قيمة الانتفاع به، لذا لقد خص المشرع أحكاما إلزامية فعالة يتضمنها التزام هام من التزامات عقد الاستهلاك، و هو الالتزام بضمان المنتوجات، و الذي ارتقى به لقيام المسؤولية الجزائية عند مخالفته.

و نظرا للطفرة التكنلوجية الكبيرة التي فرضت وجودها في هذا القرن، دفع المنتجين لتطوير إنتاجهم، و ممارسة تقنيات مختلفة لإنتاج و صناعة منتجات و مبيعات مستحدثة تتماشى و متطلبات المستهلك. غير أن هذه القفزة النوعية في التصنيع و التقدم رافقتها مخاطر كثيرة و كبيرة برزت بعد استعمال بعض المنتوجات، فأدت إلى إصابة المستهلك بالأضرار في جسمه و ماله، مما استدعى ضرورة وضع التزام جديد على المتدخلين سواء في البيع التقليدية أو الإلكترونية كضمانة للمستهلك من هذه الأخطار، مما دعا تدخل المشرع الجزائري إلى إحداث التزاما جديد على عاتق المتدخل يدعى ضمان أمن المنتوجات أو ضمان السلامة، و إقرار المسؤولية الجزائية عند مخالفته.

و عليه فإن مخالفة البائع الإلكتروني لاحد الإلتزامات السابقة يعد جريمة معاقب عليها تتمثل الأولى في جريمة مخالفة حق المستهلك في ضمان عيب المنتوجات في المعاملات الإلكترونية (الفرع الأول) أما الثانية فهيا جريمة مخالفة حق المستهلك في ضمان الأمن في المعاملات الإلكترونية (الفرع الثاني).

الفرع الأول: جريمة مخالفة حق المستهلك في ضمان عيب المنتوجات في المعاملات الإلكترونية

أهم التزامات البائع في العقود، هو ضمان المنتوجات في المبيع، حيث أن القاعدة العامة يكون البائع ملتزما بالضمان[1] إذا لم يتوفر في المبيع وقت التسليم الصفات التي ضمن للمشتري وجودها فيه أو إذا كان بالمبيع عيب ينقص من قيمته أو من نفعه بحسب الغاية المقصودة منه[2]. و قد نص المشرع الجزائري على هذا الالتزام في قانون حماية المستهلك و قمع الغش[3].

و لقد أكد المشرع على ضرورة الالتزام بضمان السلع و الخدمات في المعاملات الإلكترونية من خلال المرسوم التنفيذي رقم 327/13 المؤرخ في 26 سبتمبر سنة 2013 و الذي يحدد الشروط و الكيفيات وضع ضمان للسلع و الخدمات حيز التنفيذ[4]، إذ تطبق أحكام هذا المرسوم على السلع أو الخدمات المقتناة المنصوص عليها في أحكام المادة 13 من القانون رقم 03/09 مهما كانت طريقة و تقنية البيع المستعملة[5]، إذ أن المشرع فتح المجال في عملية البيع بكل الطرق و الوسائل بما في ذلك البيع الإلكتروني، و أنه يتعين على كل متدخل تسليم المستهلك سلعة أو خدمة مطابقة لعقد البيع و يكون مسؤولا عن العيوب الموجودة أثناء تسليمها أو تقديم الخدمة[6].

---

[1] – المادة 03 /19 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش "الضمان: التزام كل متدخل خلال فترة زمنية معينة في حالة ظهور عيب بالمنتوج باستبدال هذا الأخير أو إرجاع ثمنه أو تصليح السلعة أو تعديل الخدمة على نفقته...".

[2] – د. محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر عمان الأردن، 2006، ص 111.

[3] – المادة 13 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش " يستفيد كل مقتن لأي منتوج... من الضمان بقوة القانون..."

[4] – مرسوم تنفيذي رقم 13-327 مؤرخ في 26 سبتمبر 2013، يحدد شروط و كيفيات وضع ضمان للسلع و الخدمات حيز التنفيذ، الجريدة الرسمية، عدد 49، صادرة في 2 أكتوبر 2013.

[5] – أنظر المادة 02 من المرسوم التنفيذي 13-327 يحدد شروط و كيفيات وضع ضمان للسلع و الخدمات التنفيذ.

[6] – أنظر المادة 04 من المرسوم التنفيذي 13-327 يحدد شروط و كيفيات وضع ضمان للسلع و الخدمات حيز التنفيذ.

و لقد جرم المشرع الجزائري مخالفة المتدخل لحق المستهلك في ضمان المنتوجات من خلال المادة 75 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش. و هذه الجريمة كغيرها من الجرائم يقوم بتوافر كل من ركنها المادي (القرة الأولى) و ركنها المعنوي كما لأقر لها المشرع عقوبة تتناسب مع جسامتها(الفقرة الثانية).

و تتحقق هذه المخالفة إما عن طريق عدم الالتزام بالضمان، أو عن طريق عدم تنفيذ الضمان[1]. و عليه سوف نحدد كل من جريمة عدم الالتزام بالضمان (الفقرة الأولى)، و جريمة عدم تنفيذ الضمان (الفقرة الثانية).

الفقرة الأولى: الركن المادي لجريمة مخالفة حق المستهلك الإلكتروني في ضمان عيب المنتوجات

تعد جريمة عدم مخالفة حق المستهلك الإلكتروني في ضمان منتوجاته من الجرائم الشكلية، التي يكفي توافر السلوك المجرم دون حدوث نتيجة معينة، و تتحقق هذه المخالفة بتحقق احد السلوكين إما عن طريق عدم الالتزام بالضمان ذاته، أو عن طريق عدم تنفيذ الضمان[2]. و عليه تتحقق هذه الجريمة سواء بعدم الالتزام بضمان المنتوجات (أولا) أو عند عدم تنفيذ هذا الضمان (ثانيا).

أولا: عدم الالتزام بضمان المنتوجات

الالتزام بالضمان المعاقب على مخالفة في هذه الصورة، هو ذلك الالتزام الذي يتزامن مع عملية التعاقد، أي لحظة الإقدام على اقتناء منتوج، أو طلب الخدمة، يلتزم بمقتضاه المنتج أو البائع بأن يصلح الشيء المبيع أو يقوم باستبداله أو رد ثمنه أو تعديل الخدمة على نفقته إذا ظهر عيبا بها في زمن معين[3].

---

[1] – المادة 75 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش " يعاقب ...كل من يخالف إلزامية الضمان أو تنفيذ ضمان المنتوج المنصوص عليه في المادة 13 من هذا القانون".

[2] – المادة 75 من قانون 09-03 المتعلق بحماية المستهلك الجزائري " يعاقب ...كل من يخالف إلزامية الضمان أو تنفيذ ضمان المنتوج المنصوص عليه في المادة 13 من هذا القانون".

[3] – أنظر المادة 13 /1 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

و يتحقق عدم الالتزام بضمان المنتوجات في عدم تقديم شهادة الضمان[1]، إذ ألزم المشرع المتدخل تقديم شهادة الضمان كوسيلة قانونية تحمي المستهلك في جميع عمليات البيع مهما كان الطريقة و الوسيلة المستعملة في البيع[2]، بما في ذلك تقنية الاتصال عن بعد، و التي عرفتها المادة 3 من المرسوم التنفيذي رقم 378/13 على أنها" كل وسيلة بدون الحضور الشخصي و المتزامن للمتدخل و المستهلك ، يمكن استعمالها لإبرام العقد بين هذين الطرفين". و الهدف منها هو وفاء المتدخل بالتزاماته في حالة ظهور عيب في المنتوج خلال فترة الضمان.

و عليه فإن شهادة الضمان هيا التي تؤخذ بعين الاعتبار في قيام جريمة عدم الالتزام بالضمان من عدمها، و التي لم يعرفها المشرع و إنما نص على البيانات التي يجب توافرها فيها من خلال المادة 6 من المرسوم التنفيذي رقم 327/13 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ.

و تتمثل هذه البيانات فيما يلي[3]: اسم أو اسم شركة الضمان و عنوانه و رقم سجله التجاري و كذلك العنوان الإلكتروني عند الاقتضاء، اسم و لقب التقني، رقم و تاريخ الفاتورة أو تذكرت الصندوق أو قسيمة الشراء و/ أو كل وثيقة أخرى متماثلة، طبيعة السلعة المضمونة، لاسيما نوعها و علامتها و رقمها التسلسلي، سعر السلعة المضمونة، مدة الضمان، اسم و عنوان الممثل المكلف بتنفيذ الضمان عند الاقتضاء.

غير أن المشرع الجزائري استعمال بيانات الضمان سابقة الذكر عند الاقتضاء في مجال تقديم الخدمات إما عن طريق بند تعاقدي أو في الفاتورة أو في قسيمة الشراء أو في

---

[1] – تنص المادة 5 من المرسوم التنفيذي رقم 13-327 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ على " يسري مفعول الضمان، ابتداء من تسليم السلعة أو تقديم خدمة. و يتجسد هذا الضمان عن طريق تسليم شهادة الضمان للمستهلك بقوة القانون".

[2] – أنظر المادة 02 من المرسوم التنفيذي 13-327 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ.

[3] – نظر المادة 6 من المرسوم التنفيذي رقم 327/13.المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث –التنفيذ.

وثيقة إثبات أخرى منصوص عليها في التشريع المعمول به[1]. مما يفهم أنه في حالة عدم وجود شهادة الضمان القانونية فإنه وجب على الأقل أن ينص المتدخل على بيانات الضمان في أحد الوثائق بما فيها الشكل الإلكتروني[2].

و عليه تقوم جريمة عدم الالتزام بالضمان في المعاملات الإلكترونية بمجرد امتناع المتدخل على تسليم شهادة الضمان أو ذكر بيانات الضمان كما تم تبيانه سابقا عند إبرام العقد الإلكتروني، أي عدم تمكينه من وثيقة تثبت أنه ضامن لمنتوجه من أي عيب قد يظهر لاحقا خلال مهلة الضمان و عند تسليم المنتوج، دون النظر إلى المنتوج من حيث سلامته أو عدم سلامته[3]، دون تطلب أي ضرر يلحق بالمستهلك، حيث يعبر تسليم شهادة الضمان للمستهلك عند تسليم السلعة أو تقديم الخدمة التزاما قانونيا و تجسيدا لحق المستهلك في الضمان بقوة القانون[4].

ثانيا: عدم تنفيذ الضمان

الالتزام بتنفيذ الضمان المعاقب على مخالفة في هذه الصورة، هو ذلك الالتزام الذي يقوم متى ظهر عيب بالمنتوج بعد إبرام العقد و تسليم الشيء المبيع أو عند استعماله، بالطرق المنصوص عليها قانونا، و أن يكون في حدود آجال الضمان التي حددها القانون[5]. و عليه فإن هذه الصورة تشترط أن يتوفر في المنتوج شروط تنفيذ الضمان و عم تنفيذه بالطرق القانونية.

---

[1] – انظر المادة 7 من المرسوم التنفيذي رقم 13–327 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ.

[2] – و هذا ما تأكد عليه المادة 2 من المرسوم التنفيذي رقم 13–327 سالف الذكر عند تعريفها للضمان حيث تنص " الضمان المنصوص عليه في النصوص التشريعية،... كل بند تعاقدي أو فاتورة أو قسيمة شراء أو قسيمة تسليم أو تذكرة صندوق أو كشف تكاليف، أو كل وسيلة إثبات أخرى منصوص عليها في التشريع و التنظيم المعمول به...".

[3] – تنص المادة 11 من المرسوم التنفيذي رقم 13–327 سابق الذكر على أنه " يمكن المستهلك أن يطالب تجريب المنتوج المقتني، طبقا للتشريع و الأعراف المعمول بها دون إعفاء المتدخل من إلزامية الضمان".

[4] – محمد شرايرية، المرجع السابق، ص 180.

[5] – المادة 3/13 من القانون 09–03 المتعلق بحماية المستهلك و قمع الغش " يجب على كل متدخل خلال فترة الضمان المحددة، و في حالة ظهور عيب بالمنتوج، استبداله أو إرجاعه ثمنه أو تصليح المنتوج أو تعديل الخدمة...".

1- شروط تنفيذ المتدخل لالتزامه بالضمان:

يشترط المشرع في المنتوج لكي يلتزم المتدخل بتنفيذ الضمان أن يلحقه عيبا ما، و أن يكون هذا العيب في فترة الضمان، و هذا ما نصت عليه المادة 13 فقرة 3 سالفة الذكر من قانون حماية المستهلك و قمع الغش، غير أن المادة 21 المرسوم التنفيذي رقم 13-327 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ نصت على شرط آخر وهو ضرورة إبلاغ المتدخل بالعيب[1]. و عليه سنتناول هذه الشروط كالتالي:

أ-أن يظهر بالمنتوج عيب ما:

يشترط في المنتوج لكي يكون محلا للضمان أن يلحقه عيبا ما، غير أنه و بالرجوع إلي النصوص القانونية التي نصت على ذلك[2] فإنه يلاحظ على هذه النصوص أنها لم تعط تعريفا للعيب، و إنما نصت على شروط العيب، و عليه سوف نحاول تحديد مفهوم العيب الموجب لضمان و شروطه على النحو التالي:

- مفهوم العيب الموجب للضمان:

تطرق الفقه لتعريف العيب[3]، و لقد ظهر مفهومان له أحدهما تقليدي يعرفه على أنه الآفة الطارئة التي تخلو منها الفطرة السليمة للمبيع، أي أنه العيب الذي يطرأ في الشيء بعد تكوينه[4]، و قد أنتقد هذا التعريف لأنه حصر مفهوم العيب في الآفة الطارئة دون

---

[1] – المادة 21 من المرسوم التنفيذي رقم 327/13 سالف الذكر " لا يستفيد المستهلك من الضمان إلا بعد تقديم شكوى كتابية، أو عن طريق أي وسيلة اتصال أخرى مناسبة، لدى المتدخل".

[2] - و لاسيما المواد 3/13 و المادة 03 من القانون رقم 03/09 المتعلقة بحماية المستهلك و قمع الغش، و المادة 3 و المادة 4 من المرسوم التنفيذي رقم 327/13 المحدد لشروط و كيفيات وضع النتوج و الخدمة حيز التنفيذ،

[3] – العيب لغة هو الوصمة، و جمع عيب عيوب، فهو مصدر الفعل عاب، أي صار ذا عيب، فهو معيب، كما ورد أنه النقيصة، و ما يخلو عنه أصل الفطرة السليمة. انظر **معزوز دليلة، الضمان في عقود البيع الكلاسيكي و الإلكتروني، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، الجزائر، 2014، ص 182.**

[4] – لعجال لامية، حماية المستهلك في معاملات التجارة الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر، 2016، ص131 .

سواها في حين أن العيب يتعدى الفطرة السليمة للمبيع لأنه يمكن أن يكون آفة خلقية تطرأ مع تكوين الشيء، و قد عرف العيب أيضا في ظل المفهوم التقليدي بأنه "تلك النقائص الموجودة في المبيع و التي لا تظهر عند الفحص و الكشف عليه، تحول دون استعمال المبيع للغاية التي أعد من أجلها". فالعيب وفق هذا التعريف يعرف بشروطه المتمثلة في التأثير و الخفاء، و عموما انتقدت هذه التعريفات لأنها لم تعط تعريفا للعيب و إنما عددت صوره أو شروطه[1].

أما المفهوم الحديث للعيب فإنه نقص السلامة و الأمن في المنتوج، و هو نفس المفهوم في العيب في البيع الإلكتروني، فكثير ما يعرف أنه مبيع مجرد من الأمان و السلامة، أو مبيع يسبب خطورة و أضرار للمشتري[2]، و هذا ما تبناه قانون حماية المستهلك و قمع الغش حيث نصت المادة 11/3 منه على أنه " منتوج سليم و نزيه وقابل للتسويق: منتوج خال من أي نقص و / أو عيب خفي يضمن عدم الإضرار بصحة و سلامة المستهلك و /أو مصالحه المادية و المعنوية" و أكدته كذلك الفقرة 12 من نفس المادة[3].

و عليه فإن مفهوم العيب الموجب للضمان في ظل قانون حماية المستهلك و قمع الغش يختلف عن العيب في ظل مفهومه التقليدي، فهو في هذا الأخير يقتصر على الآفة، بينما أصبح يعرف في ظل المفهوم الحديث بأنه كل ما يجعل من المنتوج غير سليم و غير قابل للتداول، فيترتب نقصا خفيا يؤثر في وظيفة المنتوج و في الصفات التي تعهد المتدخل بوجودها[4]، كما يعد عيبا في ظل هذا المفهوم كل ما من شأنه أن يمس

---

[1] – بن زايد نسرين، حماية المستهلك من خلال الالتزام بالضمان، مذكرة ماجستير، جامعة الجزائر، 2015، ص 43.

[2] – معزوز دليلة، الرسالة السابقة، ص 189.

[3] – تنص الفقرة 12 من المادة 3 من قانون09-03 المتعلق بحماية المستهلك و قمع الغش أنه " منتوج مضمون: كل منتوج في شروط استعماله العادية أو الممكن توقعها بما في ذلك المدة، لا يشكل أي خطر أو يشكل أخطار محدودة في أدنى مستوى تتناسب مع استعمال المنتوج و تعتبر مقبولة بتوفير مستوى حماية عالية لصحة و سلامة الأشخاص".

[4] – على حساني، الاطار القانوني لالتزام بالضمان في المنتوجات –دراسة مقارنة–، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان ، الجزائر، 2012.

بالسلامة المادية و المعنوية للمستهلك، و يعد من العيوب أيضا كل النقص في الاستعمال يخالف الاتفاق و التنظيم، و عموما يمكن القول أنه يعد عيبا كل ما يلحق المستهلك من ضرر نتيجة وجود خطر، أو يجعل من المنتوج خطيرا بعد أن كان آمنا، أو سيزيد من خطورته بعد أن كان أقل خطورة في أية مرحلة من أحد مراحل التصنيع أو التصميم[1].

- شروط العيب الموجب للضمان:

لا يضمن المتدخل العيب في منتوجه، إلا بتوفر شرطين أساسين، يتمثل الأول في تأثير العيب على المنتوج أما الثاني فيجب أن يرتبط هذا العيب بصناعة المنتوج.

فشرط التأثير العيب على المنتوج وفقا لقانون حماية المستهلك و قمع الغش يتحقق بجعل المنتوج غير صالح للاستعمال المعد له كليا أو جزئيا أو أن يجعل منه منتوجا لا يتوافق مع ما كان متفقا عليه، و يتمثل تأثير العيب في جعل المنتوج خطيرا يمس بسلامة المستهلك الإلكتروني[2]. و هذا ما أشارت إليه المادة 3 من قانون حماية المستهلك و قمع الغش و كذا المادة 10 من المرسوم التنفيذي المتعلق بشروط و كيفيات وضع ضمان للسلع و الخدمات حيز التنفيذ. و عليه يمكن القول بأن العيب يكون مأثرا إذا كان جسيما لو علم به المستهلك لما أقدم على الاقتناء فيستبعد من الضمان النقص التافه الذي جرى العرف على التسامح فيه[3].

أما عن شرط ارتباط العيب بصناعة المنتوج حتى يضمنه المتدخل، فهو لا يضمن العيب الخارجي كالعيب الناجم عن سوء استخدام المنتوج[4]، لأن الضمان قاصر

---

[1] – خالد ممدوح إبراهيم، أمن المستهلك الإلكتروني، المرجع السابق، ص 165.

[2] – سامي بلعابد، ضمان المحترف لعيوب منتجاته، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة قسنطينة، الجزائر، 2005، ص 39.

[3] – محمد لبيب شنب و مجدي صبحي خليل، شرح أحكام عقد البيع، دار النهضة العربية، القاهرة، 1968، ص 259.

[4] – YVED (PICOD) ET Héléne (DAVO) : droit de la consommation. Eition armand COLIN .belgique. 2005. P 203.

على عيوب التصنيع، فهو لا يضمن إلا خطأ المتدخل، فيستبعد من نطاقه خطأ المستهلك الإلكتروني و الغير. و يقدم ضمان المنتوجات ميزة هامة للمستهلك الإلكتروني، هي إعفاؤه من عبء إثبات عدم صلاحية المبيع للعمل[1]، و بالتالي فحدوث العيب أثناء فترة الضمان، يعد قرينة على أن هذا مرتبط بصناعة الجهاز أو تصميمه[2].

ب- أن يكون في آجال الضمان:

اشترط المشرع أن يوفي المتدخل بالتزام تنفيذ الضمان عند ظهور العيب في مدة الضمان، أي أنه حتى يتقرر تنفيذ الضمان لابد من حدوث العيب ضمن هذه المدة و هو ما تضمنته المادة 2/13 من القانون رقم 09-03 المتعلق بحماية المستهلك و قمع الغش[3]. و تختلف تلك المدة حسب طبيعة السلعة أو الخدمة على ألا تقل عن ستة (6) أشهر، تبدأ من يوم تسليم السلع الجديدة أو تقديم الخدمة، بما في ذلك للبرامج الإلكترونية بكل أنواعها و التي تسلم عن طريق الأنترنت[4]، و لا يمكن أن تقل مدة الضمان عن ثلاثة أشهر بالنسبة للمنتجات المستعملة، و عموما يتم تحديد مدة الضمان بحسب طبيعة السلعة، سواء تعلق الأمر بالسلعة المستعملة أو غير المستعملة بقرار من الوزير المكلف بحماية المستهلك و قمع الغش أو بقرار مشترك منه و من الوزير المعني[5].

---

[1] – janinie revel." La coexistence du droit commun de la loi relative a la responsabilité du fait des produits défectueux. Droit de la responsabilité et responsabilités des entreprise".REVUE TRIMESTRIELLE DE DROIT ECONOMIQUE.N 2 DALLOZ. 1999.P320.

[2] – محمد حاجة بن علي، **'مسؤولية المحترف عن أضرار و مخاطر تطور منتجاته المعيبة"**، مجلة الأكاديمية للدراسات الاجتماعية و الإنسانية ، جامعة حسيبة ين بو على، الشلف، عدد 02، 2009، ص 45.

[3] – المادة 2/13 من القانون 09-03 المتعلق بحماية المستهلك و قمع الغش "" يجب على كل متدخل خلال فترة الضمان المحددة، و في حالة ظهور عيب بالمنتوج...".

[4] – أنظر المادة 16 من المرسوم التنفيذي رقم 13-327 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيز التنفيذ

[5] – انظر المادة 2/16 و المادة 2/17 من المرسوم التنفيذي رقم 13-327. المحدد لشروط و كيفيات وضع ضمان.

ج- ضرورة إبلاغ المتدخل بأن المنتوج قد لحقه عيب:

ألزم المشرع المستهلك بضرورة إبلاغ المتدخل بأن المنتوج قد لحقه عيب ما حتى تقوم الجريمة، إذ يمكن أن يكون التبليغ في شكل شكوى مكتوبة أو عن طريق أي وسيلة اتصال أخرى مناسبة لدى المتدخل[1]، مما يفهم منه إمكانية إخطار المتدخل عن طريق وسائل الاتصال عن بعد بما فيهم الأنترنت من خلال مراسلته عن طريق البريد الإلكتروني الخاص به و الذي ذكره في شهادة الضمان سالفة الذكر.

بعد إخطار المتدخل يتعين عليه تنفيذ الضمان في أجل 30 يوم من تاريخ استلام الشكوى من طرف المستهلك، أما في حالة تقصير المتدخل يقوم المستهلك بإعذار المتدخل عن طريق رسالة موصى عليها مع إشعار بالاستلام أو بأي وسيلة أخرى مطابقة للتشريع المعمول به، و في هذه الحالة على المتدخل القيام بتنفيذ الضمان في اجل ثلاثين (30) يوم ابتداء من تاريخ التوقيع على الإشعار بالاستلام[2].

2- طرق تنفيذ المتدخل لضمان:

لا يختلف تنفيذ الضمان المقرر لمصلحة المستهلك في البيع التقليدي ، عن البيع عبر شبكة الأنترنت، فإذا تم البيع بهذا الأسلوب و اكتشف في المبيع عيب ما وجب على المتدخل تنفيذ الضمان لصالح المستهلك، حيث يقوم المتدخل استنادا لطلب الضمان الموجه له من طرف المستهلك لوجود عيب موجب لضمان، بتنفيذ هذا الأخير طالما أن تنفيذ الضمان هو التزام قانوني، و التي يتوجب عند عدم تنفيذه قيام الجريمة، و التي لا يتخلص منه إلا بإثبات عدم إخطاره من طرف المستهلك، فإن المادة 3/13 من قانون حماية المستهلك و قمع الغش حددت طرق معينة لتنفيذ هذا الالتزام تتمثل في أنه : "يجب على كل متدخل... في حالة ظهور عيب بالمنتوج ، استبداله أو إرجاع ثمنه، أو تصليح المنتوج أو تعديل الخدمة على نفقته".

---

[1] - تنص المادة 01/21 من المرسوم التنفيذي 13-327 أنه " لا يستفيد المستهلك من الضمان إلا بعد تقديم شكوى كتابية أو عن طريق أي وسيلة اتصال أخرى مناسبة، لدى المتدخل."

[2] - انظر المادة 02/21 من المرسوم التنفيذي رقم 327/13 . المحدد لشروط و كيفيات وضع ضمان السلع

يفهم من خلال استعمال المشرع لعبارة "أو" أن الخيار راجع للمتدخل في كيفية تنفيذ التزامه، و أن تنفيذ احد الالتزامات الثلاثة يغنيه عن تنفيذ الآخر، غير أنه باستقراء المواد 12 و 15 من المرسوم التنفيذي رقم 327/13 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ ، يتبن لنا أنه قصد الموالات.

و يظهر ذلك بوضوح من خلال المادة 15 من نفس المرسوم حين نصت على أنه "إذا تعذر على المتدخل القيام بإصلاح المنتوج، فانه يجب عليه استبدالها أو رد ثمنها في اجل ثلاثين (30)يوما، ابتداء من تاريخ التصريح بالعيب".

و عليه فإن أول طريقة لضمان المنتوجات و غالبا ما يفضلها المستهلك هي إصلاحه، و الذي يتم مجانا و دون أعباء إضافية[1]، أما في حالة لم يقم المتدخل بإصلاح العيب في الآجال المتعارف عليها مهنيا، حسب طبيعة السلعة، فانه يمكن للمستهلك القيام بهذا الإصلاح، أن امكن ذلك عن طريق مهني مؤهل من اختياره و على حساب المتدخل[2].

أما في حالة فشل إصلاح المنتوج، أو كثرة الأعطاب فيه و تكرره فإنه يجب على المتدخل استبداله، و اذا تعذر استبدال المنتوج ، فيجب عليه رد ثمنه دون تأخير[3].

و عليه فإن امتناع المتدخل عن تنفيذ الضمان بالطرق التي حددها القانون كما سبق بيانه، يؤدي إلى قيام المسؤولية الجزائية للمتدخل بموجب المادة 75 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش، سواء في العقود التقليدية أو الإلكترونية.

---

[1] – انظر المادة 12 من المرسوم التنفيذي 13-327 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ.

[2] – انظر المادة 13 من المرسوم التنفيذي رقم 327/13 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ.

[3] – انظر المادة 12 فقرة 2 من المرسوم التنفيذي رقم 327/13 المحدد لشروط و كيفيات وضع ضمان السلع و الخدمات حيث التنفيذ .

الفقرة الثانية: الركن المعنوي لجريمة مخالفة حق المستهلك الإلكتروني في ضمان عيب المنتوجات و العقوبات المقررة لها

يتحقق الركن المعنوي لهذه الجريمة بتوفر القصد الجنائي، و القصد الجنائي المتطلب هنا هو القصد العام، و هو علم المتدخل أن سلوكه السلبي المتمثل في الامتناع عن تسليم المستهلك شهادة الضمان أو أي وثيقة تثبه التزامه بالضمان يشكل جريمة، و تذهب إرادته إلى تحقيق هذا السلوك، فتقوم الجريمة ويعاقب المتدخل على هذا السلوك.

أما بالنسبة للسلوك الثاني و المتمثل في عدم تنفيذ الضمان فالجريمة تتشكل دون التفات إلى الركن المعنوي، حيث يكفي امتناع المتدخل عن تنفيذ التزاماته لضمان المنتج خلال فترة الضمان المحددة قانونا حتى تتشكل الجريمة.

و لقد عاقب المشرع من خلال المادة 75 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش كل متدخل أخل بإلزامية ضمان المنتوجات بصورتيه السابقتين، بعقوبة مالية تتمثل في الغرامة تتراوح بين 50.000دج و 500.000دج.

أما في حالة العود فتضاعف العقوبة لتصبح غرامة تتراوح بين 100.000دج إلى 1.000.000دج[1]، بالإضافة إلى العقوبة الأصلية أجاز المشرع للقاضي الحكم بعقوبة تكميلية في حالة العود تتمثل في الشطب من السجل التجاري، إذ تعتبر هذه العقوبة التكميلية خاصة تتعلق بالتجار فقط سواء شخص طبيعي أو معنوي، فتكون هذه العقوبة من العقوبات التي تحقق الردع الخاص كما لها تأثير على سمعة التاجر و سبب في تراجع ذمته المالية، و في ذلك تحقيق لقاعدة الجزاء من جمس العمل.

[1]- أنظر المادة 85 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

الفرع الثاني: جريمة مخالفة حق المستهلك في ضمان أمن المنتوجات في المعاملات الإلكترونية

جرم المشرع الجزائري مخالفة التزام المتدخل ضمان أمن المنتوجات[1] من خلال المادة 73 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش[2]، و التي بدورها تجرم كل متدخل على مخالفة التزام أمن المنتوجات المنصوص عليه في المادة 10 من نفس القانون[3].

و لقد تأكدت فكرة ضرورة الالتزام بالأمن من قبل المتدخل في مواجهة المستهلك في المعاملات الإلكترونية في التشريع الجزائري، من خلال المرسوم التنفيذي رقم 12-203 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات[4]، حيث نصت المادة الثانية من هذا المرسوم على أنه " تطبيق أحكام هذا المرسوم على السلع و الخدمات الموضوعة للاستهلاك...، مهما كانت تقنيات و طرق البيع المستعملة". إذ يتبين أن المشرع قد ألزم

---

[1] – لم يعرف المشرع الجزائري مصطلح أمن المنتوجات، غير أن الفقه تصدى لهذا المصطلح و عرفه البعض بمصطلح السلامة بأنه " ذلك الالتزام الذي يحرص فيه المتدخل سواء كان بائعا أو صانعا أو مقدم خدمات على تنفيذ العقد دون أن يلحق المبيع أضرارا بالدائن ، أي المستهلك د. **عمر خالد رزيقات، عقد البيع عبر الأنترنت، دراسة تحليلية، ط1بعة، دار الحامد للنشر، عمان، الأردن، 2007، ص 343.**

و عرفه البعض الآخر على أنه "الالتزام الذي يتطلب توافر في كل منتج ضمانات ضد كل المخاطر التي من شأنها أن تمس صحة المستهلك، و أمنه أو تضر بمصالحه المالية". **أنظر: د. خالد ممدوح إبراهيم، حماية المستهلك في التعاملات الإلكترونية، المرجع السابق، ص 193.**

[2] – المادة 73 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش " يعاقب بغرامة ...كل من يخالف إلزامية أمن المنتوجات المنصوص عليها في المادة 10 من هذا القانون".

[3] – حيث ألزمت المادة 10 من قانون 09-03 على كل شخص طبيعي أو معنوي يتدخل في عملية عرض المنتجات للاستهلاك أن يحترم إلزامية آمن المنتوج من حيث مميزاته و تأثيره على المنتوجات الأخرى، و كذلك عرضه و وسمه و التعليمات الخاصة به مع مراعات المنتجات الموجهة خصيصا للأطفال.

[4] – مرسوم تنفيذي رقم 12-203 مؤرخ في 14 جمادى الثاني عام 1433 الموافق 6 مايو سنة 2012، يتعلق بالقواعد المطبقة في مجال أمن المنتوجات، جريدة رسمية العدد 28، الصادرة في 9 مايو سنة 2012. حيث نصت المادة 5 منه على هذا الالتزام ،" يجب أن تستجيب السلعة و /أو الخدمة بمجرد وضعها رهن الاستهلاك، للتعليمات التنظيمية المتعلقة بها في مجال أمن و صحة المستهلكين و حمايتهم، لا سيما فيما يتعلق...".

المتدخل بضمان أمن المنتوجات في عملية البيع بكل الطرق و الوسائل بما في ذلك البيع عن طريق وسائل الاتصال عن بعد.

و باستقرائنا للمواد 73 من قانون حماية المستهلك و قمع الغش و المرسوم التنفيذي رقم 203/12 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات، نجد أن مخالفة إلزامية ضمان أمن المنتوجات تتحقق بقيام الركن المادي، و ركن معنوي .و سنحاول تحديد كل من الركن المادي (فقرة أولى) و الركن المعنوي (الفقرة الثانية).

الفقرة الأولى: الركن المادي لجريمة مخالفة حق المستهلك في ضمان أمن المنتوجات

تعد جريمة مخالفة ضمان أمن المنتوجات من الجرائم الشكلية، يقوم ركنها المادي بإتيان السلوك المجرم دون توفر نتيجة معينة، و حسب المادة 73 من قانون حماية المستهلك و قمع الغش و المرسوم التنفيذي رقم 203/12 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات فإن السلوك المجرم يقوم بإحدى الصورتين، الأولى تتعلق بعدم الالتزام بالمقاييس التنظيمية لإنتاج المواد (أولا) و الثاني تتعلق بعدم الالتزام بالإفضاء عن مخاطر هذه المنتوجات (ثانيا).

أولا: عدم الالتزام بالمقاييس التنظيمية للإنتاج

يقوم الركن المادي لجريمة عدم الالتزام بضمان المنتوجات وفقا لهذه الصورة بمجرد مخالفة المقاييس التنظيمية لإنتاج المواد، حيث يتوجب على المورد الإلكتروني في عملية وضع المنتوج للاستهلاك تحت طائلة العقوبات[1] تحديد أمن المنتوجات وفقا للتنظيمات و المقاييس الخاصة المتعلقة بها، و المستوى الحالي للمعارف و التكنلوجيا، و كذا الأمن الذي يحق للمستهلك انتظاره، بالإضافة إلى الاستعمالات المرتبطة بحسن السير في

[1] – المادة 23 من المرسوم التنفيذي رقم 213/12 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات " تطبق العقوبات المنصوص عليها في التشريع المعمول به، لاسيما أحكام قانون 09-03 ..على كل مخالفة لأحكام هذا المرسوم".

مجال الأمن أو الصحة[1]. و عموما يعتبر المنتوج آمنا عندما لا يشكل خطورة على صحة المستهلك و لا يعرض سلامته للخطر.

و قد نصت المادة 5 من المرسوم التنفيذي رقم 12-203 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات على مجموعة من المعايير التي يجب احترامها لاعتبار المنتوج آمن، حيث نصت على أنه "يجب أن تستجيب السلعة أو الخدمة بمجرد وضعها رهن الاستهلاك، للتعليمات التنظيمية المتعلقة بها في مجال أمن و صحة المستهلك و حمايتهم، لا سيما فيما يتعلق بما يأتي:

-مميزات السلعة من حيث تركيبها و شروط إنتاجها و تجميعها و تركيبها و استعمالها و صيانتها و إعادة استعمالها و تدويرها من جديد و نقلها.

-شروط النظافة التي يجب أن تتوفر في الأماكن المستعملة للإنتاج و الأشخاص الذين يعملون بها.

-مميزات و تدابير الأمن الأخرى المرتبطة بالخدمة و بشروط وضعها في متناول المستهلكين.

-التدابير الملائمة الموضوعة قصد ضمان تتبع مسار السلعة أو الخدمة."

-التدابير المتعلقة برقابة مطابقة السلعة أو الخدمة المتطلبات الأمن المطبقة عليها.

و في إطار رقابة مطابقة أمن السلع و الخدمات يؤخذ بعين الاعتبار على وجه الخصوص مميزات السلعة أو الخدمة، بما في ذلك شروط استعمالها و تأثير السلعة أو الخدمة على الجوار و عرضها و الإنذارات و التعليمات المحتملة الخاصة باستعمالها، و كذا كل البيانات الأخرى بها، و حتى فئات المستهلكين المعرضين لحالات خطر عند استعمال السلعة أو الخدمة[2].

[1] – انظر المادة 6 من المرسوم التنفيذي رقم 213/12 يتعلق بالقواعد المطبقة في مجال أمن المنتوجات.

[2] – انظر المادة 8 من المرسوم التنفيذي رقم 203/12 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات.

و عليه فإن عدم الالتزام بالمقاييس التنظيمية السابق ذكرها يعد مخالفة لضمان المستهلك في منتوج آمن، و هو فعل معاقب عليه وفقا للمادة 73 من قانون حماية المستهلك و قمع الغش.

ثانيا: عدم الالتزام بالإفضاء(عدم الالتزام بإعلام بالتحذيرات و إرشادات الاستعمال)

إن عدم الالتزام بتوفير الأمن في المنتوجات لا يتوقف عند تركيب أو تصنيع أو إنتاج منتوجات بالمخالفة للتنظيم المحدد لعناصرها و مواصفاتها القياسية فقط، بل يتوجب على المتدخل أن يضع في متناول المستهلك كل المعلومات الضرورية التي تسمح له بتفادي الأخطار المحتملة و المرتبطة بالاستهلاك أو باستعمال السلعة أو الخدمة المقدمة[1]، و هو ما يطلق عليه بالالتزام بالإفضاء، الذي يقوم عندما يكون محل التعامل أشياء تنطوي على خطورة[2] سواء من ناحية استعمالها أو حفظها أو بطبيعتها، مما يستوجب على المتدخل الإفضاء بمكامن هذه الخطورة، حتى تتحقق السلامة للمستهلك[3].

و هذا الالتزام نص عليه المشرع بوضوح في المادة 10 من المرسوم التنفيذي رقم 213/12 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات، حيث نصت على أنه" يجب على المنتجين و المستوردين و مقدمي الخدمات وضع في متناول المستهلك كل المعلومات الضرورية التي تسمح له بتفادي الأخطار المحتملة و المرتبطة بالاستهلاك و / أو باستعمال السلعة أو الخدمة المقدمة و ذلك طيلة مدة حياته العادية أو مدة حياته المتوقعة بصفة معقولة.

---

[1] – عبد الحليم بوقرين، الرسالة السابقة، ص 312.

[2] – عرف المشرع الجزائري المنتوج الخطير في المادة 03 من قانون حماية المستهلك 09-03 على أنه المنتوج الذي في ظروف استعماله العادية أو المتوقعة يشكل خطرا يهدد سلامة و صحة المستهلك..، و قد عرف الفقه الشيء الخطير على أنه " ذلك الذي تتطلب حراسته عناية خاصة نظرا لما تمثله من خطورة حتى و إن كان يمثل خطورة بطبيعته"، أنظر **عامر قاسم أحمد القيسي، الحماية القانونية للمستهلك، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2002، ص 117.**

[3] – د. محمد جمال الدين زكي، مشكلات المسؤولية المدنية، الجزء الأول، طبعة 1،جامعة القاهرة، 1999، ص 442.

و لضمان تنفيذ الالتزام بالإفضاء اشترط المشرع على المنتجين و المستوردين الإشارة على غلاف المنتوج و التوضيب لهوياتهم و عناوينهم و مرجع المنتوج ورقم حصته و /أو تاريخ صنعه و بلده الأصلي، و كذلك إعلام المتدخلين القائمين على التوزيع بشأن متابعة منتوجاتهم، و الأكثر من ذلك اشترط المشرع مسك سجل خاص بالشكاوى عند الاقتضاء[1].

و عليه يظهر السلوك الإجرامي في هذا النوع من الاعتداءات في شكل عدم الإفضاء بكيفية الاستعمال[2]، و يتحقق هذا السلوك عند قيام المتدخل بتسليم السلعة الخطيرة أو المعقدة الاستعمال إلى المستهلك و لكن دون أن يرفقها بالبيانات المتعلقة بكيفية الاستعمال أو دليل الاستعمال[3].

و مع ذلك فإن معرفة كيفية الاستعمال لا تحقق الحماية الكافية للمستهلك ما لم يلحقها تحذير و تنبيه عن الأخطار التي يمكن أن يحتويها المنتوج أو يتسبب فيها، و على هذا الأساس فإن هذا السلوك يكون متحققا إذا لم يقم المتدخل بتحذير المستهلك عن المخاطر التي يمكن أن يتعرض لها و كذا الاحتياطات الواجب إتباعها للوقاية من الأخطار[4]، فيظهر الاعتداء في صورة الإفضاء غير الكامل أو غير الواضح ، و يكون التحذير غير كامل إذا لم يحط بجميع الأخطار التي يمكن أن تلحق المستهلك من جراء استعماله للمنتوج أو حيازتها أو من حيث كيفية الوقاية من الأخطار الخاصة به[5].

---

[1] – انظر المادة 11 من المرسوم التنفيذي رقم 203/12 المتعلق بالقواعد المطبقة في مجال أمن المنتوجات.

[2] – غير أن الجريمة لا تقع إذا قام المنتج بالإفضاء الصحيح عن طريق استعمال المنتوج، لكن المستهلك تجاهل هذه التعليمات و استعمل المنتج بطريقة خاطئة أو في غير الغرض المحدد لها، و بهذا يعفى المنتج من المسؤولية. **انظر محمد شكري سرور، مسؤولية المنتج عن الأضرار التي تسببها منتوجاته الخطيرة، الطبعة الثالثة، دار الفكر العربي، القاهرة، ، 1983، ص 32.**

[3] – عبد الحليم بوقرين، الرسالة السابقة، ص 314.

[4] – عامر قاسم أحمد القيسي، المرجع السابق، ص 126.

[5] – محمد شكري سرور، المرجع السابق، ص .32

الفقرة الثانية: الركن المعنوي لجريمة مخالفة حق المستهلك في ضمان امن المنتوجات و العقوبات المقررة لها

تعد جريمة مخالفة ضمان أمن المنتوجات من الجرائم التي يتحقق الركن المعنوي فيها بمجرد أن يتحقق عنصر من العناصر المكونة للركن المادي لها، كمخالفة المقاييس التنظيمية للإنتاج أو عدم تحذير المستهلك من الأخطار المحتملة للمنتوج، دون أن تكون نية المتدخل قد اتجهت إلى إحداث النتيجة، حتى يمكن القول بتوافر القصد الجنائي.

و الجدير بالذكر أن معيار تحديد عدم أمن المنتوجات حددت المادة 9 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش، و التي تنص على أنه " يجب أن تكون المنتوجات الموضوعة للاستهلاك مضمونة و تتوفر على الأمن بالنظر إلى الاستعمال المشروع المنتظر منها، و أن لا تلحق ضررا بصحة المستهلك و أمنه و مصالحه، و ذلك ضمن الشروط العادية للاستعمال أو الشروط الأخرى الممكن توقعها من قبل المتدخل". فالمعيار الذي اعتمده المشرع الجزائري –الاستعمال المشروع المنتظر–[1].

و يرى أغلب الفقه أن الرغبة المشروعة لمستعمل المنتوج لا يجب أن تقدر تقديرا شخصيا[2]، فلا يجب على القاضي أن يأخذ بعين الاعتبار الرغبة الخاصة Inconcreto بمستعمل المنتوج الضار و لكن تقدر تقديرا مجردا In abstracto من خلال المستهلك المتوسط، فهي رغبة تتغير حسب درجات السن، الجنس، و ثروات المستهلك[3].

و هناك من يرى أن الرغبة المشروعة أو المتوقعة أمر من شأن المستهلكين فقط، إذ ليس من حق المهنيين أن يحددوا ما هو حسن أو رديء لعملائهم. و في ذات الوقت ليس

---

[1] – لم يعرف المشرع الجزائري الرغبة المشروعة للمستهلك، و يمكن تعريفها أنها" مفهوم نفسي يتعلق بالحياة الذهنية و تصورات الفرد". **أنظر محمد شرايرية، الرسالة السابقة، ص 272.**

[2] – BRIGITTE HESS-FALLON et SIMON ANNE-MARIE. Droit commercial et des affaires. 9 édition. sirey. 1995. P 138.

[3] – NATHALIE RZEPECKI. Droit de la consommation et théorie géniral du contrat. Presse universitaire daix-marseille. 2002. P 212.

من حق المستهلك أيضا أن ينتظر أو يتوقع إلا ما هو معقول، في ضوء الظروف الاقتصادية، و الحالة التقنية القائمة[1].

و عليه و من خلال ما سبق يتوجب على المتدخلين تقديم منتجات لا تشكل خطرا عند الاستعمال العادي أو المتوقع من طرفهم، و هذا ما نصت عليه المادة 3 و 9 من قانون حماية المستهلك و قمع الغش، و كذلك المرسوم التنفيذي رقم 213/12 في المادة 10 منه، و مخالفة ذلك يؤدي لقيام المسؤولية الجزائية وفقا للمادة 73 من قانون حماية المستهلك و قمع الغش.

أما بالنسبة للعقوبات المقررة لهذه الجريمة فإن المشرع لم ينص على عقوبة واحدة لجريمة مخالفة حق المستهلك الإلكتروني في ضمان أمن المنتوجات، و إنما اختلفت العقوبة المقررة لها باختلاف جسامتها بين جنحة و جناية، و سنحاول تبيان ذلك بنوع من التفصيل كالتالي:

-جريمة مخالفة إلزامية ضمان أمن المنتوجات بوصفها جنحة:

عاقب المشرع على مخالفة أمن المنتوجات سواء من حيث عدم احترام المقاييس و التنظيم، أو من حيث عدم الالتزام بالتحذيرات و إرشادات الاستعمال –دون أن ينجر عليها ضرر– من خلال المادة 73 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش، و الذي يعتبر النص التجريمي الأساسي لهذه الجريمة، و التي تكيف الفعل على أنه جنحة ، وقررت لها عقوبة الغرامة قدرها من 200.000 إلى 500.000 دج[2].

أما في حالة العود فتضاعف العقوبة لتصبح غرامة تتراوح بين 400.000دج إلى 1.000.000دج[3]، بالإضافة إلى العقوبة الأصلية أجاز المشرع للقاضي الحكم بعقوبة

[1] – زوبيدة سميرة، الرسالة السابقة، ص 221.

[2] – تنص المادة 73 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش بانه " يعاقب بغرامة من مائتي ألف دينار (200.000 دج) إلى خمسمائة الف دينار (500.000 دج) كل من خالف إلزامية امن المنتوجات المنصوص عليها في المادة 10 من هذا القانون".

[3] – أنظر المادة 85 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

تكميلية في حالة العود تتمثل في الشطب من السجل التجاري، إذ تعتبر هذه العقوبة التكميلية خاصة تتعلق بالتجار فقط سواء شخص طبيعي أو معنوي، فتكون هذه العقوبة من العقوبات التي تحقق الردع الخاص كما لها تأثير على سمعة التاجر و سبب في تراجع ذمته المالية، و في ذلك تحقيق لقاعدة الجزاء من جمس العمل.

غير أنه حينما يترتب على انتفاء عنصر الأمن في المنتوج بمخالفة أحد الالتزامات المتطلبة المذكرة سابقا مرضا أو عجز عن العمل للمستهلك فإن العقوبة نصت عليها المادة 83 من القانون رقم 09-03 ، و التي أحالت بدورها إلى العقوبة المنصوص عليها في المادة 432 من قانون العقوبات[1]، حيث تكون العقوبة هيا الحبس من خمس (5) سنوات إلى عشرة (10) و غرامة مالية من 500.000دج إلى 1.000.000[2].

-جريمة مخالفة إلزامية ضمان أمن المنتوجات بوصفها جناية:

تكون جريمة مخالفة التزام ضمان امن المنتوجات بوصفها جناية وفقا للفقرة الثانية و الثالثة من المادة 83 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش، إذا تسبب المنتوج الغير آمن في مرض غير قابل للشفاء أو في فقدان استعمال عضو أو في حالة الإصابة بعاهة مستديمة، و تكون العقوبة السجن من 10 سنوات إلى 20 سنة و غرامة مالية من 1.000.000 دج إلى 2.000.000 دج . أما إذا تسبب هذا المرض في وفاة شخص أو عدة أشخاص تكون العقوبة السجن المؤبد[3].

و الملاحظ أن تكييف هذا الاعتداء يثير إشكالية تعدد أوصاف الفعل الواحد، إذ يمكن أن يدرج ضمن الإخلال بواجب الإعلام ، و أمام هذا الوضع ما على رجال القضاء

---

[1] – تنص المادة 83 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش انه " يعاقب بالعقوبات المنصوص عليها في الفقرة الأولى من المادة 432 من قانون العقوبات، كل من يغش أو يعرض أو يضع للبيع أو يبيع منتوج مزور أو فاسد أو سام أو لا يستجيب لالتزامات الأمن المنصوص عليها في المادة 10 من هذا القانون. إذا ألحق هذا المنتوج بالمستهلك مرضا أو عجزا عن العمل".

[2] – أنظر المادة 1/83 من الأمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966، المتضمن قانون العقوبات، المعدل و المتمم.

[3] – انظر الفقرة 2 و 3 من المادة 83 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

أي قضاة بما فيهم قضاة الموضوع إلا اختيار الوصف الأشد عند وقوع فعل تحت عدة أوصاف[1].

[1] – ذلك تطبيقا للمادة 32 من قانون العقوبات التي تنص " يجب أن يوصف الفعل الذي يحتمل عدة أوصاف بالوصف الأشد من بينها".

المطلب الثاني: الحماية الجنائية للمستهلك من الخداع و التزوير الصناعي في المعاملات الإلكترونية

يتعرض المستهلك أثناء إبرام عقود التجارة الإلكترونية إلى مخاطر متعددة يمكن أن تمس بصحته و سلامته من بينها الخداع و التزوير في المنتوجات من طرف البائع باعتباره الطرف الثاني في العملية التعاقدية، حيث تكون فرصة التعرض للخداع و التزوير خلال التعاقدات الإلكترونية كبيرة في ظل انعدام معاينة السلعة أو الخدمة مباشرة.

و نظرا لخطورة هذه الجرائم على حياة المستهلك كان لازما على المشرع الجزائري توفير حماية جنائية من هذه الجرائم، إذ جرم كل فعل من هذه الأفعال من خلال قانون 09-03 المتعلق بحماية المستهلك و قمع الغش. و عليه سنحاول تناول الحماية الجنائية للمستهلك من جريمة الخداع في التعاملات الإلكترونية (الفرع الأول)، و الحماية له من جريمة التزوير في المعاملات الإلكترونية (الفرع الثاني).

الفرع الأول: جريمة خداع المستهلك في المعاملات الإلكترونية

يعرف الخداع[1] على أنه القيام بأعمال أو أكاذيب من شأنها إظهار الشيء على غير حقيقته، أو إلباسها مظهرا يخالف ما هو عليه في الحقيقة[2]، و على هذا الأساس فإن الخداع يقع على المستهلك و ليس على المنتوج، و نظرا لكون المستهلك الطرف الضعيف في العقد لقلة خبرته و قلة معلوماته في إبرام العقود حاول المشرع الوطني حمايته من خداع المهني المحترف ، و ذلك بتجريم الخداع وفقا للمادة 68 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش[3].

---

[1] – الخداع في اللغة مصدره خدع و المخادعة إظهار غير الحقيقة، خدع فلان أي أظهر له خلاف ما يخفي، و ألحق به المكروه من حيث لا يعلم. **أنظر قاموس المحيط للفيروز أبادي، دار الجليل، بيروت، ج2، ص 292.**

[2] – أنظر محمد بودالي، شرح جرائم الغش في بيع السلع و التدليس في المواد الغذائية و الطبية ، دار الفجر للنشر و التوزيع ، القاهرة، 2005، ص 8.

[3] – المادة 68 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش " يعاقب بالعقوبة المنصوص عليها في المادة 429 من قانون العقوبات، كل من يخدع أو يحاول أن يخدع المستهلك، بأية وسيلة أو طريقة كانت حول:

-كمية المنتوجات المسلمة.

-تسليم المنتوجات غير تلك المعينة سابقا.

-فابلية استعمال المنتوج.

و حسب المادة 68 السابق ذكرها نجد أن هذه الجريمة تتحقق عن طريق تغليط المستهلك بشأن كمية المنتوجات أو نوعيتها أو طرق الاستعمال...إلخ، و في حقيقة الأمر كل هذه **الأفعال يمكن أن تقع في مجال المعاملات الإلكترونية** أين يعتمد البائع الإلكتروني إلى محاولة تغليط المستهلك بشأن العناصر السابقة، و على هذا الأساس فإنه يمكن تطبيق النصوص المتعلقة بالخداع على الخداع الإلكتروني، خاصة و أن المشرع لم يحدد الوسيلة التي يتم بها هذا الخداع و إنما نصت المادة 68 أنه **يعاقب على الخداع أو محاولة الخداع بأي وسيلة**، و تعتبر الأنترنت إحدى وسائل الخداع، و هو ما أكده المشرع من خلال القانون المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها[1].

و عليه سنحاول تحديد جريمة الخداع في المعاملات الإلكترونية من خلال تحديد الركن المادي لها (الفقرة الأولى)، و توضيح الركن المعنوي لهذه الجريمة و العقوبة المقررة لها (الفقرة الثانية).

الفقرة الأولى: الركن المادي لجريمة الخداع في المعاملات الإلكترونية

يتحقق الركن المادي لهذه الجريمة بخداع المستهلك، غير أن المشرع الوطني لم يعرف فعل الخادع[2]، و لقد تصدى الفقه لذلك، إذ يعرف الخداع بأنه القيام بأعمال أو أكاذيب من شأنها إظهار محل المعاملة على غير حقيقتها، أو إلباسه مظهرا يخالف ما هو عليه في الحقيقة[3].

-تاريخ أو مدة صلاحية المنتوج.

-النتائج المنتظرة من المنتوج.

-طرق الاستعمال أو احتياطات اللازمة لاستعمال المنتوج."

[1] – أنظر المادة 02 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[2]– يتميز الخداع عن التدليس المدني في كون هذا الأخير ينصب على الإرادة عند تكوين العقد، أما الخداع فيقع بعد تكوين العقد أو خارجا عنه، كما يختلفان من حيث التدليس المدني يكفي لقيامه مجرد الكتمان بشرط أن يكون هو الدافع للتعاقد، في حين لا يكفي ذلك في الخداع، و يختلف الخداع عن الغش في كون هذا الأخير يقع على المنتوج المعد للبيع في حين أن الخداع يقع على المتعاقد، كما أن الغاية من تجريم الخداع هو الحفاظ على الثقة و العقود عموما أما الهدف من تجريم الغش هو الحفاظ على الصحة العامة. **أنظر حليم بوقرين، الرسالة السابقة، ص 16.**

[3] – د/ محمد بودالي، شرح جرائم الغش في بيع السلع و التدليس في المواد الغذائية و الطبية، المرجع السابق، ص 8.

و لقد حدد المشرع من خلال المادة 68 موضوع الخداع، و التي لا يمكن التوسع فيها أو القياس عليها، رغم أن الصيغة التي وردت بها من الشمولية بحيث تشمل جميع مظاهر و صفات الخداع[1]، و تتمثل في:

أولا: الخداع في كمية المنتوج المسلمة

يقع الخداع في هذه الحالة وفقا للفقرة الأولى من المادة 68 من قانون حماية المستهلك و قمع الغش حول كمية المنتوج إما على العدد أو المقدار أو المعيار أو القياس أو الكيل أو طاقتها[2]، و يرى البعض أن كل هذه الألفاظ تدور حول معنى المقدار[3].

و لا يتحقق الخداع التجاري بالانقاص من وزن أو حجم البضاعة فقط، و إنما بالإضافة أيضا، إذ تم إضافة مواد غريبة عن السلعة لزيادة وزنها أو حجمها، و في هذه الحالة يوصف الفعل بأنه خداع في كمية المنتوج.

ثانيا: خداع المستهلك بشأن هوية المنتوج

و يتحقق الخداع في هوية المنتوج بتسليم سلعة أو خدمة غير تلك المتفق عليها، و تقوم هذه الجريمة سواء تم التسليم فعليا أو حكميا، و يتحقق التسليم الفعلي بوضع المبيع تحت تصرف المشتري و يأخذ صورتين: صورة التسليم المادي حيث يستولي المستهلك على المبيع، و الصورة الثانية التسليم الرمزي و هو التسليم القانوني، كان يعهد غليه بمفتاح التشفير الخاص بتحميل البرنامج المعلوماتي، أما التسليم الحكمي فيتم عن طريق الاتفاق على تغيير صفة الحائز للشيء المبيع دون تغيير الحيازة الفعلية التي تبقى تحت يد البائع[4].

ثالثا: الخداع في طبيعة المنتوج و صفاته الجوهرية

لقد نص المشرع الوطني على هذا النوع من الخداع في المادة 69 فقرة 03 من قانون حماية المستهلك و قمع الغش ، بقابلية استعمال المنتوج، و يدخل في قابلية المنتوج للاستعمال كل ما له علاقة بالعناصر الجوهرية له و طبيعته، فالخداع في طبيعة الشيء

---

[1] – د/ محمد شرايرية، الرسالة السابقة، ص 215.

[2] – ناصر حمد الصقير، مرجع سابق، ص 83 ..

[3] – احمد محمد محمود على، المرجع السابق، ص 180.

[4] – عبد الحليم بوقرين، الرسالة السابقة، ص 19.

هو إعطاء صورة مغايرة عن خصائص السلعة، بحيث يتحول إلى شيء ذو طبيعة أخرى[1]، أما في ما يخص الصفات الجوهرية[2] للمنتوج فهي تلك الصفات التي تقوم عليها القيمة الحقيقية للبضاعة في نظر المتعاقد، و هي مسالة تختلف باختلاف الأشخاص و العقود.

رابعا: الخداع في صلاحية المنتوج

تعد صلاحية المنتوج من أهم الصفات الجوهرية للمنتوج أو السلعة بل تعد أحيانا أساس المعاملة التجارية، و غاليا ما تحدد صلاحية المنتوج بتاريخ فيكون المنتوج غير صالح للاستعمال اذا تخطى هذا الأخير، و المقصود بتاريخ الصلاحية تلك الفترة التي تظل فيها السلعة محتفظة بتركيبتها و خواصها الطبيعية و قدرتها و هذه الفترة تختلف باختلاف المنتوجات، و يتم الخداع في التاريخ إما بتقديم سنة الصنع أو الإنتاج[3]، أو تأخير سنة الصلاحية. و التي ميز فيها المشرع بين ثلاث حالات، الأولى تتمثل في التاريخ الأقصى للاستهلاك[4]، و الثانية التاريخ الأدنى للصلاحية أو من المستحسن استهلاكه قبل[5]، و الثالثة هيا التاريخ الأقصى للاستعمال[1].

---

[1] – أحمد محمد محمود على، المرجع السابق، ص 175.

[2] – اختلف الفقه في تحديد مفهوم الصفات الجوهرية، فمنهم من عرفها على أساس موضوعي، فهيا تقوم على تحديد هذه الصفات من الناحية المجردة و طبقا للشروط التي وجب توافرها في الشيء عادة، أما أصحاب المفهوم الشخصي، فانهم الصفات الجوهرية تتجاوز مجرد الخصائص المادة و الكيماوية بل تتعداها لتشمل ما يضعه المتعاقدون في الاعتبار عند التعاقد. **انظر اكثر تفصيلا محمد شرايرية، الرسالة السابقة، ص 217 و 218.**

[3] – عرفة المادة 03 من المرسوم التنفيذي رقم 13-378 يحدد الشروط و الكيفيات المتعلقة بإعلام المستهلك تاريخ الصنع أو الإنتاج بأنه: التاريخ الذي يصبح فيه المنتوج مطابقا للوصف الذي وضع له. كما حددت المادة 29 فقرة 3 من نفس المرسوم تاريخ الصنع بانه : يعرف تاريخ الصنع بيوم الصنع أو يوم التوضيب أو يوم التجميد المكثف بالنسبة للمواد الغذائية المجمدة تجميدا مكثفا أو بيوم التجميد بالنسبة للمواد الغذائية المجمدة.

[4] – التاريخ الأقصى للاستهلاك: التاريخ المحدد تخت مسؤولية المتدخل المعني، الذي تكون بعده المواد السريعة التلف قابلة لتشكيل خطر فوري على صحة الإنسان أو الحيوان، و يجي ألا تسوق المادة بعد هذا التاريخ. **أنظر المادة 3 من المرسوم التنفيذي رقم 13-378 يحدد الشروط و الكيفيات المتعلقة بإعلام المستهلك.**

[5] – التاريخ الأدنى للصلاحية أو من المستحسن استهلاكه قبل: تاريخ نهاية الآجال المحددة تحت مسؤولية المتدخل المعني، الذي تبقى المادة الغذائية خلاله صالحة كليا للتسويق و محافظة على كل مميزاتها الخاصة المستندة إليها صراحة أو ضمنيا، ضمن شروط التخزين المبينة إن وجدت، و يجب أن تسحب المادة الغذائية من التسويق بعد هذا

خامسا: الخداع في المطابقة الوظيفية

هذا الخداع نصت عليه كل من الفقرتين الخامسة و السادسة من المادة 68 من قانون حماسية المستهلك و قمع الغش، و يقصد بها صلاحية المنتوج المبيع و ملائمته للاستعمال العادي أو التجاري و مدى كفاية البيانات و المعلومات المتعلقة بالاستعمال و الحصول على منافعه و كيفية صيانته[2]. فالنتائج المرجوة من المنتوج، هيا عبارة عن النتائج التي على أساسها قام المستهلك بالتعاقد على المنتوج و لولاها لما اقدم على التعاقد، و بذلك يصبح المتدخل مسؤولا عن تحقيق هذه النتائج.

أما بالنسبة لطريقة استعمال المنتوج و الاحتياطات اللازمة للاستعمال، فتعني جميع البيانات التي تساعد المستهلك على استعمال المنتوج و طيفية الاستفادة منه، بما ذلك التعليمات التعليمات لإعادة تشكيل بعض المنتوجات الغذائية[3]. و كيفية الوقاية من الأخطار الناتجة عن استعماله، و التغليط بشأن هذه العناصر سوف يؤدي إلى عدم الحصول على الفائدة المرجوة من المنتوج.

و الملاحظ على أن التغليط أو الكذب بشأن هذه العناصر خاصة الخداع حول طريقة استعمال المنتوج و الاحتياطات اللازمة للاستعمال يؤدي إلى تعدد التكييفات بين جريمة الخداع و جرائم أخرى كالإخلال بحق المستهلك في الإعلام و الإخلال بإلزامية أمن المنتوجات.

و الجدير بالذكر أن المشرع عاقب على الشروع في خداع المستهلك، و الذي يشترط فيه أن يكون الكذب أو التغليط في مقام تعاقد، بحيث يؤدي إلى قبول التعاقد، و بدونها لما اقدم المستهلك على ذلك[4]، مما يؤدي ذلك إلى قيام جريمة مخالفة إلزامية

الأجل حتى لو بقيت صالحة كليا بعد التاريخ. **أنظر المادة 3 من المرسوم التنفيذي رقم 13-378 يحدد الشروط و الكيفيات المتعلقة بإعلام المستهلك .**

[1] – التاريخ الأقصى للاستعمال: التاريخ المحدد تحت مسؤولية المتدخل المعني الذي من المحتمل أن يفقد بعده المنتوج غير الغذائي خصائصه الأساسية و لا يلبي الرغبات المشروعة للمستهلك. **أنظر المادة 3 من المرسوم التنفيذي رقم 13-378 يحدد الشروط و الكيفيات المتعلقة بإعلام المستهلك.**

[2] – أنظر المادة 5/68و6 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

[3] – أنظر المادة 35 من المرسوم التنفيذي رقم 13-378 يحدد الشروط و الكيفيات المتعلقة بإعلام المستهلك.

[4] – د/ رؤوف عبيد، المرجع السابق، ص 391.

الإعلام السابق التطرق إليها، و التي تقوم قبل إبرام العقد، مما ينبغي على المشرع تعديل نص المادة 68 من قانون حماية المستهلك حتى يتجنب تعدد التكييف، و حسب رأينا يكون التعديل بحذف عبارة" **المحاولة في الخداع**"، لأنها جريمة قائمة بذاتها و هيا مخالفة إلزامية إعلام المستهلك.

الفقرة الثانية: الركن المعنوي لجريمة الخداع في المعاملات الإلكترونية و العقوبة المقررة لها

تعد جريمة الخداع في المعاملات الإلكترونية من الجرائم العمدية التي يتطلب لقيامها توافر القصد الجنائي، على الرغم أن المشرع الوطني لم يشر إلى وجوب توافر القصد الجنائي في هذه الجريمة، و مع ذلك فان القصد الجنائي شرطا عاما في الجريمة، و لا تقوم مسؤولية الجاني إلا به و هو ما أكدة عليه محكمة النقض المصرية صراحة في أحد أحكامها " جريمة خداع المشتري هي من الجرائم العمدية التي يجب لتوافرها ثبوت القصد الجنائي"[1]، كما تعتبر أن الإهمال حتى و لو كان جسيما فانه لا يعبر عن سوء النية[2]. و بناء عليه وجب على القاضي أن يثبت في حكم الإدانة توافر هذا الركن.

غير أن محكمة النقض الفرنسية أجازت استخلاص القصد الجنائي من مجرد الإهمال[3]، مما يؤدي إلى أن عدم قيام الجاني بالتحريات اللازمة لمطابقة المنتوج معبرا عن مسؤوليته في جريمة الخداع. إلا أن هذا الموقف غير ثابت إذ تقضي بعض الأحكام الأخرى إلى عدم اعتبار الإهمال معبر عن سوء النية إذا كان العيب راجع إلى صعوبة فنية في الصناعة يتعذر اكتشافها[4].

---

[1] – نقض 1950/11/27، قواعد محكمة النقض، ج2، رقم 13، رقم 879 .**انظر عبد الحليم بوقرين، الرسالة السابقة، ص 21.**

[2] – إذا قضي بأن خطأ الفاعل مهما كان عظيما لا يجعله مسؤولا جنائيا. أنظر نقض 26 فبراير 1916 الشرائع س3، ص423 **مشار إليه عند أحمد محمد محمود على، المرجع السابق، ص 184.**

[3] – قضت محكمة النقض الفرنسية بأنه يتوجب على القضاة أن يلتمسوا مسؤولية الجاني بين عناصر الدعوى و الظروف المحيطة. قرار صادر عن محكمة النقض الفرنسية صادر في 4 جانفي 1977 ، **أنظر محمد بودالي، شرح جرائم الغش، المرجع السابق، ص 22.**

[4] – د/ محمد بودالي، شرح جرائم الغش..، المرجع السابق، ص 22 و 23.

و عليه يجب أن يتوافر القصد الجنائي بعنصريه وقت إبرام العقد إذا كان الخداع تاما، أو حين تقدم البضاعة أو عرضها إذا كان الخداع في مرحلة الشروع، كما أن الإهمال البسيط أو انعدام الرقابة لا يكفيان للقول بتوافر سوء النية.

أما بالنسبة للعقوبة المقررة لجريمة خداع المستهلك في المعاملات الإلكترونية، فبالرجوع إلى المادة 68 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش و التي تحيل بدورها على المادة 429 قانون عقوبات فإن العقوبات المقررة تتمثل في عقوبات سالبة للحرية، فيعاقب على الخداع البسيط الذي لم يخلف ضررا بالحبس من شهرين (2) إلى ثلاث (3) سنوات، بالإضافة إلى عقوبة الغرامة التي تحتل مكانة متميزة في الجرائم الاقتصادية بصفة عامة و الجرائم الماسة بالمستهلك بصفة خاصة، و تكون الغرامة من 2000 إلى 20.000 دج. أو بإحدى هاتين العقوبتين سواء كانت الجريمة تامة أو شرع في ارتكابها.

أما بالنسبة لتشديد هاذه العقوبة فقد نصت المادة 69 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش على مجموعة من الوسائل إذ تم الخداع باستعمال أحداها ترفع العقوبة على النحو التالي[1]: بالنسبة للعقوبة السالبة للحرية يرفع الحد الأقصى إلي 5 سنوات أي يكون الجبس من شهرين إلى خمس سنوات. أما الغرامة فيرفع الحد الأقصى لها إلى 500.000 دج و تكون عقوبة الغرامة من 2.000 إلى 500.000 دج.

و تعتبر الوسائل المذكورة في نص المادة 69 السابق ذكرها ظروف تشديد قانونية، فإن تم الخداع بواسطتها وجب على قاضي الموضوع الحكم بالعقوبة المشددة و إلا كان

---

[1] – المادة 69 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش "ترفع العقوبات المنصوص عليها في المادة 68 أعلاه إلى خمس (5) سنوات حبسا و غرامة قدرها 500.000 دج غذا كان الخداع أو محاولة الخداع قد ارتكبت بواسطة:

-الوزن أو الكيل أو بأدوات أخرى مزورة أو غير مطابقة.

-طرق ترمي إلى التغليط في عمليات التحليل أو المقدار أو الوزن أو الكيل أو التغيير عن طريق الغش في تركيب أو وزن أو حجم المنتوج.

-إشارات أو ادعاءات تدليسية.

-كنيبات أو منشورات أو نشرات أو معلقات أو إعلانات أو بطاقات أو أية تعليمات أخرى."

حكمه باطلا، و هذه الوسائل مذكورة على سبيل الحصر. و نلاحظ في هاذا الأخير أن الإعلان أو الإشهار الكاذب و المضلل بما فيها الإشهار الإلكتروني المخالف لشروطه المنصوص و المعاقب عليه وفقا للمادة 40 من قانون التجارة الإلكترونية يعتبر ظرف تشديد في جريمة الخداع، و يشكل جريمة مستقلة في قانون التجارة الإلكترونية، إلا أن جريمة الخداع تتطلب وجود تعاقد و هو ما لا يشترط في جريمة الإشهار الإلكتروني المخالف لشروطه، و يرى البعض أن جريمة الخداع المشددة تتطلب و جود مجني عليه، أي يجب أن يكون هناك عقد أو الشروع في التعاقد بينما تكون جريمة الإشهار الإلكتروني المخالف لشروطه موجهة للجمهور و لا تتطلب و جود متعاقد .

و خلاصة القول أن المشرع لا يتطلب وجود وسائل معينة في هذه الجريمة إذ يكفي الكتمان أو الكذب أو حتى الإيماء الذي يوحي بخلاف الحقيقة، إلا انه جعل من اللجوء إلى بعض الوسائل ظرفا مشددا، و على هاذا الأساس فان الخداع يقع على المستهلك و ليس على السلعة، **و كل هاذه الأفعال يمكن أن تقع في مجال المعاملات و التجارة الإلكترونية.**

غير أن الخداع في مجال المعاملات الإلكترونية لا يقتصر فقط على العناصر السالفة الذكر و إنما يتعداه إلى عناصر أخرى ذات أهمية بالغة في إتمام المعاملة الإلكترونية، و منها الخداع بخصوص طريقة الدفع و وسائل الدفع و طريقة التسليم و جهة التسليم، فكل هذه الأفعال لا تشملها المادة 68 سالفة الذكر، و لذلك يكون من الضروري إحداث نص جديد يجرم الخداع الإلكتروني أو تعديل نص المادة 68 على نحو يحتوي كل خداع من الممكن أن يتصور في المعاملات الإلكترونية.

الفرع الثاني: جريمة التزوير التجاري و الصناعي في المعاملات الإلكترونية

تعتبر ظاهرة التزوير التجاري و الصناعي[1] من المظاهر التي تمس المستهلك، و نظرا لما تخلفه من آثار خطيرة على حياته، فقد اهتم المشرع الوطني بها، و نص على تجريمها و معاقبة مرتكبيها من خلال نص المادة 70 من قانون حماية المستهلك و قمع الغش.

إذ يجب أن ينصب التزوير على محل يحميه القانون جنائيا و قد ورد المحل الذي يحميه القانون في المادة 70 من قانون حماية المستهلك و قمع الغش. فإن كانت المادة 431 قانون عقوبات قد عددت الأشياء التي تكون محلا للغش[2] فإن المادة 70 من قانون حماية المستهلك و قمع الغش قد عاقبت على كل غش في أي منتوج دون تحديد، فيستوي أن يكون مواد غذائية أو غير غذائية أو طبية أو صناعية أو حتى **برامج إلكترونية** .

إذ يمكن أن يتحقق التزوير التجاري و الصناعي عبر شبكة الأنترنت و ذلك عند استلام المستهلك لمنتوجات مغشوشة أو غير مطابقة للمواصفات أو غير آمنة أو فاسدة، كما يمكن أن يتصور ذلك إلكترونيا و ذلك في حالة المبيعات الإلكترونية مثل البرامج، فقد يشتري المستهلك برنامجا معينا و عند إرساله من طرف البائع يكتشف المستهلك أن

---

[1] – لم يعرف المشرع الوطني التزوير التجاري و الصناعي، و هذا بالرغم من تجريمه و النص على كافة صوره و أنواعه، على غرار المشرع السعودي و الليبي ، حيث عرفه المشرع السعودي على أنه " كل منتج دخل عليه تغيير أو عبث به بصورة ما مما أفقده شيئا من قيمته المادية أو المعنوية، سواء كان ذلك بالإضافة أو بالانقاص أو بالتصنيع أو بغير ذلك، في ذاته أو طبيعته أو جنسه أو نوعه أو شكله أو عناصره أو صفاته أو متطلباته ...".

أما المشرع الليبي فقد عرفه على أنه " كل إظهار أو محاولة إظهار سلعة أو خدمة ما بغير مظهرها الحقيقي، سواء أكان ذلك بإدخال الغش على المنتج ذاته، أو بصناعة أو حيازة أو استعمال أدوات أو آلات أو أساليب تساعد على الغش، لتحقيق عائد أو مكسب مادي. **أنظر روستم عطية ، المرجع السابق، ص 51 ، 52 .**

كما عرفته محكمة النقض الفرنسية بانه " اللجوء إلى التلاعب أو المعالجة غير المشروعة التي لا تتفق مع التنظيم و تؤدي بطبيعتها إلى تحريف في التركيب المادي للمنتوج. **أنظر محمد بودالي، حماية المستهلك في القانون المقارن، المرجع السابق، ص 317.**

[2] – نصت المادة 431 من قانون العقوبات الجزائري على أنواع معينة و على سبيل الحصر حول السلع التي تكون محل لجريمة الغش التجاري و الصناعي، و تتمثل في: أغذية الإنسان و الحيوان و المشروبات، المواد و المنتجات الطبية.، المنتجات الفلاحية.

البرنامج معيب أو غير صالح أو منتهي الصلاحية، كما يمكن حدوثه في العديد من المنتجات التي يتم بيعها عبر الأنترنت كالمجلات أو الصور أو الفيديوهات أو الألعاب و غيرها.

و عليه سنحاول تحديد جريم تزوير التجاري و الصناعي في المعاملات الإلكترونية من خلال كل من ركنها المادي (الفقرة الأولى) و الركن المعنوي و العقوبة المقررة لها (الفقرة الثانية).

الفقرة الأولى: الركن المادي لجريمة التزوير التجاري و الصناعي في المعاملات الإلكترونية

لم يبين المشرع الجزائري كيف يتم التزوير في قانون حماية المستهلك و قمع الغش، و اكتفى بتحديد مجموعة من الأفعال أو الصور المكونة لهذه الجريمة، و عليه يتم التزوير بإتيان سلوك إيجابي من طرف الصانع أو المنتج أو المتدخل و ذلك بتغيير عناصر المنتوج أو خلطه بمادة أخرى أو عدم احترام للتنظيم المعمول به. و وفقا لما نصت عليه المادة 70 من قانون حماية المستهلك فإن هذه الأفعال هي:

أولا: تزوير منتوجات

و يقصد بالغش أو التزوير هنا كل تغيير أو تشويه متعمد يتم إدخاله على جوهر المنتوج أو تكوينه الطبيعي، فالتحريف للصفة الجوهرية للمنتوج هم العنصر الفعال في الجريمة، و يجب أن يكون المنتج محل الجريمة موجه للاستهلاك أو الاستعمال البشري أو الحيواني. و وفقا للمعنى المتقدم فإن الغش أو التزوير يتحقق بواحد أو أكثر من الوسائل التالية:

1-التزوير بالإضافة:

و تعد هذه الوسيلة من أشهر الوسائل و أكثرها شيوعا في ارتكاب جريمة التزوير نظرا لسهولتها من الناحية العملية، فهي لا تتطلب في الكثير من الأحيان اتباع طرق فنية دقيقة

فالتزوير بالإضافة يتحقق إما عن طريق إدخال عناصر جديدة أو خلطها بأخرى مختلفة عنها أو من ذات طبيعتها، و لكن من صنف رديء أو اقل جودة[1]، و هذا من أجل خلق الاعتقاد بأن السلعة من نوعية رفيعة أو جيدة أو بغرض إخفاء عيوبها أو رداءة نوعيتها، و هذا بشرط أن لا تكون هذه الإضافة أو الخلط مسموح و مرخص به عن طريق القانون أو مطابق للأعراف و العادات التجارية المعمول بها[2]، كالإضافات التي تكون ضرورية لحفظها من التلف كالمواد المضافة إلى المواد الغذائية، و غما لتحسين النوعية[3].

2-التزوير بالانقاص:

يتحقق الغش بهذه الوسيلة بانقاص أو سلب أو نزع كل من العناصر الحقيقية المكونة للمنتج أو جزء منه مع احتفاظها بنفس التسمية و المظهر الخارجي الذي يوهم بأنها هي المنتج الحقيقي[4]. و يهدف هاذا النوع من الغش لتشويه المنتج الحقيقي و ليس فقط إخفاء ضعف المادة، الأمر الذي من أثره نزع بعض جوهر المادة ذاتها، و لكن لا يصل إلى الاستفادة الكاملة أو الإلغاء الكلي لهذه المادة[5].

3-التزوير بالصناعة:

يتحقق التزوير بالصناعة عند قيام المتدخل بصناعة سلعة، أو مادة دون أن يدخل في تركيبها بعض المواد الواجب إدخالها طبقا للأنظمة أو العرف التجاري و الصناعي[6]، و بذلك يمكن أن يكون الغش بهذه الطريقة جزئيا، و ذلك في حالة افتقاد السلعة لبعض

---

[1] – روستم عطية موسى نو، المرجع السابق، ص 56.

[2] – السيد محمد السيد عمران، حماية المستهلك أثناء تكوين العقد، دار الجامعة الجديدة للنشر، الإسكندرية، 2003، ص 72.

[3] – روستم عطية موسى نو، المرجع السابق، ص 57.

[4] – ناصر محمد الصقير، الحماية الجنائية للمستهلك من الغش التجاري، مذكرة ماجستير في قانون حماية المستهلك و المنافسة، كلية الحقوق، جامعة الجزائر، 2016.، ص 98.

[5] – روستم عطية موسى نو، المرجع السابق، ص 58.

[6]– Combaldieu Raoul: La fraude en matiére alimentaire. Revue internationale de droit compare. Vol 26. N3. Juilley. 1974 . p 521.

العناصر التي يتكون منها المنتج الحقيقي، و قد يكون كليا في حالة ما إذا افتقدت السلعة جميع العناصر المكونة للمنتج الحقيقي[1].

و ما يميز هاذه الصورة من صور الغش عما عداها أنها تتطلب وجود تشريع يحدد العناصر الداخلة في تركيب السلعة المصنعة و الطبيعية، ذلك أن المشرع يحرص أحيانا على توافر بعض العناصر في السلعة عند الإنتاج و من ثم افتقارها لهذه العناصر أو خلوها منها يعرض سلامة المستهلك للخطر[2].

ثانيا: التعامل في السلعة المزورة أو السامة أو الفاسدة أو الخطيرة

لا يتحقق غش المستهلك بمجرد تغيير أو تحريف في جوهر السلعة أو الخدمة أو تكوينها الطبيعي سواء بالإضافة أو الانقاص أو التصنيع فقط، بل اعتبر المشرع في الفقرة الثالثة من المادة 70 من قانون حماية المستهلك و قمع الغش أن طرح أو عرض أو بيع سلعة مزورة أو فاسدة أو سامة صورة من صور التزوير[3]. و عليه سوف نوضح صور هذا النوع من التزوير التجاري، و تحديد محل الذي تقع عليه هذه الصور على النحو التالي:

1- محل التعامل في المنتج المزور أو السام أو الخطير أو الفاسد:

يتحقق التزوير التجاري وفقا للفقرة الثالثة من المادة 70 من قانون حماية المستهلك و قمع الغش، عندما يقوم المتدخل بالعرض أو الوضع للبيع أو بيع منتوج مزور أو فاسد أو خطير أو خطير، و سنحاول تحديد كل من هذه الأنواع السابقة للمنتج محل التجريم كالتالي:

المنتوجات المزورة سبق و أن عرفناها، أما المنتجات السامة فيقصد بها تلك المنتجات التي قد تؤدي إلى الموت في بعض الأحيان أو تؤدي إلى تقيئات و اضطرابات

---

[1] – غزيوي هندة، "**المسؤولية الجزائية للشركات التجارية عن جرائم الغش التجاري**" ، مجلة التواصل في الاقتصاد و الإدارة و القانون، ع 39، سبتمبر، 2014. ، ص 121.

[2] – روستم عطية موسى نو، المرجع السابق، ص 59.

[3] – أنظر المادة 3/70 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

في الأمعاء، و هيا منتجات مضرة بصحة المستهلك بالضرورة، أو التي تشكل خطرا من نوع خاص[1].

أما المنتجات الفاسدة فهيا منتجات تم اعتمادها طبقا للقوانين، لكن يشوبها درجة من التغيير الطارئ أو التلقائي الذي يغير من مكوناتها الطبيعية أو الخواص الموجودة بها سواء من حيث الطعم أو الرائحة أو اللون نتيجة التحلل الكيماوي و الميكروبي، مما يجعلها غير صالحة للاستعمال[2].

2- صور التعامل في السلع المزورة أو السامة أو الفاسدة أو الخطرة:

حسب الفقرة الثالثة من المادة 70 من قانون حماية المستهلك و قمع الغش فإن السلوك المجرم لهذا النوع من الغش يتكون من ثلاث تصرفات:

-**البيع:** يتحقق هذا النوع من الغش في حالة البيع إذا تم اقتران إيجاب المتدخل مع قبول المستهلك من اجل شراء المنتوج المزور أو الفاسد أو الخطير[3]، حيث يشمل جميع أنواع البيع بما فيها البيوع الإلكترونية التي تتم عبر وسائل الاتصال الحديثة، و التي نص عليها المشرع من خلال مشروع قانون التجارة الإلكترونية.

-**العرض للبيع:** يعني عرض سلعة للجمهور للإقبال عليها و التعامل بشأنها، و هو يتحقق بوضع البضاعة في محل أو أي مكان آخر مخصص للبيع فيه تحت تصرف المشترين المحتملين حتى و لو لم يراها هؤلاء فعلا، إذ أصفر العرض عن إقبال مشتري على السلعة المغشوشة[4]. مما يسمح باستغراق العرض الإلكتروني المنصوص عليه في المادة 11 من 18-05 المتعلق بقانون التجارة الإلكترونية.

-**الطرح للبيع:** يتحقق بمجرد وضع البضاعة تحت نظر المشتري في مكان مفتوح للجمهور لرؤيتها أو فحصها أو شرائها، كان توضع البضاعة على واجهة المحل[5].

---

[1] – روستم عطية موسى نو، المرجع السابق، ص 110.

[2] – عبد الحليم بوقرين، الرسالة السابقة، ص 28.

[3] – ناصر محمد الصقير، المذكرة السابقة، ص 109..

[4] – روستم عطية موسى نو، المرجع السابق، ص 110.

[5]– Combaldieu Raoul: op cit. p 522. .

و عليه فالعرض للبيع أعم من الطرح للبيع، إذ أنه يتضمن حالة جعل البضائع اكثر عرضة للبيع من حالة الطرح للبيع، و ذلك لما ينجم عن العرض من إغراء المارة في الطرقات أو الذين يدخلون المحل. مما يدخل في هذه الصورة الإشهار الإلكتروني فهو بمثابة دعوى للتعاقد و تعريف المنتجات لدى جمهور المستهلكين.

و عليه يلزم لقيام هذه الجريمة أن تكون المنتجات مطروحة أو معروضة بقصد البيع، أما اذا كانت موجودة لدى شخص قصد الاستعمال الشخصي فلا تقوم الجريمة. كما نشير إلى أن قيام هذه الجريمة لا يتطلب توافر عقد أو مجني عليه، و بالتالي فان تجريم فعل التزوير أعم منه في حالة الخداع، حيث أنه في جريمة الخداع ترتكب الجريمة بواسطة التصريح أو الإدلاء ببيان كاذب مع بقاء مادة الشيء كما هيا صالحة للاستهلاك، أما في جريمة التزوير فلا تتحقق إلا بالمساس بمادة الشيء و لذل فهيا اشد خطر من جريمة الخداع[1].

ثالثا: التعامل في مواد تستعمل في التزوير

لم يكتف المشرع بتجريم أفعال الغش و التعامل في المنتوجات المغشوشة أو الفاسدة أو السامة، بل جرم أيضا التعامل في المواد التي تستعمل في الغش و ذلك بموجب الفقرة الرابعة من المادة 70 قانون حماية المستهلك و قمع الغش، و هدف المشرع من تجريم التعامل في مواد تستعمل في ارتكاب الغش هو تكريس مبدأ الحماية الوقائية لصحة المستهلكين، و بالتالي حماية الثقة في التجارة عن طريق استبعاد كل الوسائل التي من شأنها أن تسهل للتاجر أو المتدخل ارتكاب الغش.

و عليه تقوم هذه الجريمة عن طريق عرض أو الوضع للبيع أو بيع أدوات و أجهزة أو أي مادة خاصة تستعمل في غش المنتوجات، و لا يشترط المشرع أن يكون الشيء محل التعامل ممنوع في حدي ذاته وقت التعامل و إنما يكفي أن يكون المنتج قابل لاستخدامه في الغش و هاذا ما نصت عليه المادة 70 فقرة 04 بعبارة "... من شأنها أن تؤدي...".

[1] – د/ أحمد محمد خلف، الحماية الجنائية للمستهلك، دراسة مقارنة، المكتبة العصرية للنشر و التوزيع، المنصورة، مصر، 2008، ص 233.

الفقرة الثانية: الركن المعنوي لجريمة التزوير التجاري أو الصناعي في المعاملات الإلكترونية و العقوبة المقررة لها

التزوير التجاري جريمة عمدية ، يستلزم لقيامها توافر القصد الجنائي، وذلك بعلم الجاني أن أفعاله سوف تؤدي إلى غش السلعة أو المنتجات و أن ما يعرض أو يطرح للبيع أو يبيعه مغشوش أو فاسد أو مسموم أو خطير ، ثم اتجاه إرادته إلى تحقيق ذلك بنية خداع المستهلك.

و جريمة التزوير الصناعي من الجرائم الوقتية التي تقع بمجرد ارتكاب أحد الأفعال السابق ذكرها و بالتالي ينبغي توافر القصد الجنائي في وقت معاصر لوقوع الجريمة ، أما جرائم الطرح أو العرض للبيع أو البيع فهي من الجرائم المستمرة و بالتالي يجب أن يتوافر القصد الجنائي في أي وقت تحقق فيه علم الجاني بالتزوير .

و يعد البحث في توافر القصد الجنائي أو عدم توافر العلم بالتزوير من المسائل التي يستقل بتقديرها قاضي الموضوع، و هاذا الأمر أكدته محكمة النقض الفرنسية من أنه يجب على قضاة الموضوع التأكد من قيام الغش[1]. كما اعتبر المشرع الفرنسي أن التاجر أو الصانع مسؤول عن الغش الواقع في مصانعهم أو محلاتهم سواء بفعلهم أو بفعل تابعيهم، حيث يتوافر القصد بالنسبة للصانع أو المنتج من العلم بالصفة غير المشروعة لعملية الغش، و يستدل على ذلك بالقرائن، و يكفي لقيام مسؤولية الجنائية إثبات قيامه بتغيير المنتوج إلى منتوج مغشوش و العلم بأن هاذا المنتوج موجه للبيع. أما بالنسبة للبائع فيستلزم لقيام القصد الجنائي إثبات توافر العلم فعلا لدى البائع مع استبعاد العلم بالقرائن[2].

أما بالنسبة للعقوبة المقررة لهذه الجريمة فتنص المادة 70 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش و التي تحيل بدورها على المادة 431 من قانون العقوبات بعقوبة سالبة للحرية و هيا الحبس من سنتين (2) إلى خمس (5) سنوات و

[1] – محمد بودالي، شرح جرائم الغش، المرجع السابق، ص 44.

[2] – محمد بودالي، حماية المستهلك في القانون المقارن، المرجع السابق، ص 327.

بغرامة من 20.000 إلى 100.000 دج، و لم يعاقب المشرع على هذه الجريمة في حالة الشروع، لأن جريمة التزوير جريمة شكلية لا يتنظر حدوث النتيجة.

و تشدد العقوبة طبقا للمادة 432 عقوبات اذا ألحقت المواد المغشوشة أو الفاسدة بالشخص مرضا أو عجزا عن العمل عند تناولها أو تقديمها له و تكون العقوبة الحبس من سنتين إلى عشر سنوات و غرامة من 500.000 دج إلى 1.000.000 دج.

و تتحول هذه الجريمة من جنحة إلى جناية اذا ترتب عن المادة مرض غير قابل للشفاء أو فقد عضو أو عاهة مستديمة ، فتكون العقوبة السجن من عشر سنوات إلى عشرين سنة ، و بغرامة من 1.000.000 دج إلى 2.000.000 دج ، أما اذا تسببت تلك المادة في موت إنسان تكون العقوبة بالسجن المؤبد[1].

و في الأخير وإن كان يسهل التعرف على التزوير في الحالات ذات الطبيعة المادية منه، فإنه يتعذر ذلك في مجال التعاملات الإلكترونية التي لا تتوفر في الكثير من الأحيان على تلك الطبيعة المادية، و بالرغم من ذلك فإن جميع الحالات التي ذكرتها المواد سالفة الذكر يمكن أن تتم عبر شبكة الأنترنت، و يتحقق ذلك عند استلام المستهلك الإلكتروني لمنتوجات مغشوشة أو غير مطابقة للمواصفات أو غير أمنة أو فاسدة.

كما يتصور أن يتحقق ذلك إلكترونيا في حالة المبيعات الإلكترونية مثل البرامج، فقد يشتري المستهلك برنامجا معينا و عند إرساله من طرف البائع يكتشف أن البرنامج معيب أو غير صالح أو منتهي الصلاحية.

و إن كان يمكن تطويع النصوص المتعلقة بجريمة التزوير لتشمل صور الغش في مجال المعاملات الإلكترونية كون الأنترنت وسيلة فقط للتعاقد، أما التزوير فيقع بمحل التعاقد و هو المنتجات، و مع ذلك يكون من الأفضل إحداث نص جديد يحدد أركان هذه الجريمة و صورها و نطاقها.

[1] – أنظر المادة 432 من قانون العقوبات المعدل و المتمم.

الفصل الثاني: الحماية الجزائية الموضوعة لمتطلبات المستهلك في المعاملات الإلكترونية

أدى التطور السريع لتبادل المعلومات إلكترونيا إلى نمو التعاقدات التجارية في العالم بأسره، و انعكس ذلك على تزايد المعاملات الإلكترونية عبر شبكة الأنترنت و ممارستها بشكل ملحوظ سريع و فعال، إذ تلزم المعاملات الإلكترونية على المستهلك تبادل بياناته الشخصية مع صاحب السلع أو مقدم الخدمة، كما تتطلب أيضا هذه المعاملات الإلكترونية لإتمامها توقيع الأطراف المتعاقدة بما فيها المستهلك الإلكتروني، إذ تستلزم عقود التجارة الإلكترونية توقيعا يتلاءم حسب طبيعتها و هو التوقيع الإلكتروني.

و نظرا لأهمية هذه المتطلبات في إتمام المعاملات الإلكترونية جعلت الفكر القانوني يستقر و يقتنع بضرورة وضع نصوص قانونية خاصة لحمايتها من الاعتداء عليها خاصة في ظل التحديات الرقمية. و هو ما جسده المشرع الجزائري من خلال مجموعة من النصوص سواء منها التعلق بحماية البيانات الشخصية للمستهلك الإلكتروني (المبحث الأول) أو تلك المتعلقة بالتوقيع الإلكتروني للمستهلك (المبحث الثاني).

المبحث الأول: الحماية الجنائية للبيانات الشخصية للمستهلك في المعاملات الإلكترونية

تلزم المعاملات الإلكترونية على المستهلك تبادل بياناته الشخصية مع صاحب السلع أو مقدم الخدمة، الأمر الذي أدى إلى إمكان تعرض تداول بيانات أطراف المعاملة الإلكترونية عامة و المستهلك خاصة للاعتداء عليها.

و هو ما جعل المشرع الجزائري يضفي حماية خاصة لهذه المعطيات الشخصية، و ذلك من خلال قانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي عند معالجتها إلكترونيا[1]، إذ تضمن هذا القانون مجموعة من الأحكام الجزائية التي من شأنها أن توفر حماية جنائية للبيانات الشخصية بصفة عامة، و التي تتضمن حماية لبيانات المستهلك الإلكتروني[2]، سواء ما تعلق بالجرائم المتعلقة بالجوانب الموضوعية للمعالجة (المطلب الأول)، أو تلك المتعلق بالجوانب الشكلية لها (المطلب الثاني).

[1] – قانون رقم 18-07 مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، عدد 34، الصادرة في 10 يونيو 2018.

[2] – نص المشرع الجزائري من خلال المادة 03 من قانون 18-07 سالف الذكر على أن الشخص المعني هو كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة. و عليه فالمستهلك مشمول بالحماية وفقا لهذا القانون لأنه يتعامل بمعطياته الشخصية في المعاملات الإلكترونية.

المطلب الأول: الجرائم المتعلقة بالجوانب الموضوعية لمعالجة البيانات الشخصية للمستهلك الإلكتروني

جرم المشرع الجزائري من خلال قانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي مجموعة من الأفعال التي تشكل خرقا للقواعد الموضوعية التي يلزم مراعاتها عند القيام بكل معالجة إلكترونية للمعطيات الشخصية بما فيها المتعلقة بالمستهلك الإلكتروني، سواء تعلقت هذه القواعد بتسيير المعطيات ذات الطابع الشخصي(الفرع الأول)، وكذا المتعلقة بحقوق الشخص المعني-المستهلك-(الفرع الثاني).

الفرع الأول: الجرائم المتعلقة بتسيير المعطيات الشخصية للمستهلك الإلكترونية

نظرا لأهمية البيانات الشخصية[1] للمستهلك في المعاملات الإلكترونية و ارتباطها بحياته الخاصة، أوجب المشرع على ضرورة تسييرها بطريقة نزيهة و مشروعة و متوافقة مع المقتضيات القانونية، إذ يلزم في كل معالجة لهذه البيانات الإلكترونية أن يكون الجمع مشروعا و متوافقة مع الأغراض المصرح بها أو المرخص لها، و من ثم فإن كل معالجة لا تستجيب لما سبق يشكل جريمة المعالجة الغير مشروعة للمعطيات الشخصية للمستهلك (الفقرة الأولى)، كما يلزم كل مسؤول عن المعالجة أن يتقيد بالاستعمال المشروع لهذه المعطيات و كل خروج عن ذلك يشكل جريمة الاستعمال غير المشروع

[1]- عرف المشرع الجزائري من خلال المادة 03 من قانون 18-07 سالف الذكر المعطيات ذات الطابع الشخصي على أنها "هيا كل المعلومات بغض النظر عن دعامتها متعلقة بشخص معروف أو قابل للتعرف على صاحبها بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية" ، و هو تعريف أساسه التوجيه الأوروبي رقم 95/46 الصادر في 24 أكتوبر 1995 الخاص بحماية الأشخاص في مواجهة المعالجة الآلية للمعطيات ذات الطابع الشخصي، حيث عرفها في المادة 2/أ على أنها " المعطيات ذات الطابع الشخصي هي كل معلومات متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه (الشخص المعني)، يعد قابل للتعرف عليه بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع رقم تعريف أو إلى عنصر أو عدة عناصر خاصة، مميزة لهويته الطبيعية، الفزيولوجية، النفسية، الاقتصادية، الثقافية"..

للمعطيات الشخصية للمستهلك الإلكتروني (الفقرة الثانية)، كما يعد تحويل البيانات الشخصية للمستهلك إلى الخارج فعل محضور (الفقرة الثالثة).

الفقرة الأولى: جريمة المعالجة غير المشروعة للمعطيات الشخصية للمستهلك الإلكترونية

تقتضي المعالجة المتعلقة بالمعطيات الإلكترونية[1] الشخصية أن تكون قائمة على أساس مشروع من أجل ضمان احترام حقوق و حريات الأشخاص بما فيهم المستهلك الإلكتروني، لذا جرم المشرع كل معالجة غير مشروعة للمعطيات الشخصية في مختلف مراحل هذه المعالجة من خلال المادتين 58 من قانون 18-07 ، و التي تجرم كل إنجاز أو استعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها[2]، و المادة 59 من نفس القانون التي تعاقب على كل جمع معطيات ذات طابع شخصي بطريقة تدليسيه أو غير نزيهة أو غير مشروعة[3].

[1] – معالجة المعطيات هيا كل عملية أو مجموع عمليات منجزة بطرق أو وسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني و كذلك و التشفير أو المسح أو الإتلاف. **أنظر المادة 3 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي** . و الملاحظ أن المشرع الوطني وسع من طرق المعالجة إذ تسمل كل تكنولوجيات الإعلام المعلوماتية، و شبكات الاتصال عن بعد، فالعبرة إذن ليست بالآلة في حد ذاتها و إنما بان تكمن هذه الأخيرة من معالجة آلية للمعطيات ذات الطابع الشخصي، و من ثم فإن قانون 18-07 يشمل مجال تطبيقه الأجهزة الآلية للمعالجة الموجودة حاليا، و تلك التي من الممكن أن تظهر في المستقبل.

[2] – المادة 58 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب بالحبس من ستة أشهر إلى سنة و بغرامة من 60.000 دج إلى 100.000دج أو بإحدى هاتين العقوبتين فقط، كل من قام بإنجاز أو باستعمال معالجة لأغراض أخرى غير تلك المصرح بها أو المرخص بها".

[3] – المادة 59 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب بالحبس من سنة إلى ثلاث سنوات و بغرامة من 100.000دج إلى 300.000دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة".

و جريمة المعالجة غير المشروعة للمعطيات الشخصية للمستهلك الإلكتروني تتطلب لقيامها إتيان كل من ركنها المادي (أولا) و المعنوي (ثانيا)، كما أقر لها المشرع عقوبة تتناسب مع جسامتها (ثالثا).

أولا: الركن المادي لجريمة المعالجة غير المشروعة للمعطيات الشخصية للمستهلك الإلكتروني

انطلاقا من المادتين 58 و 59 من قانون 18-07 المتعلق بحماية المعطيات الشخصية فإن المعالجة غير المشروعة للمعطيات الشخصية تأخذ صورتين، فالأولى تتمثل في إنجاز أو استعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها و المنصوص عليها بموجب المادة 58 السابق ذكرها، أما الصورة الثانية فتتمثل في جمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة المنصوص عليها بموجب المادة 59 من قانون 18-07 المتعلق بحماية المعطيات الشخصية.

1- إنجاز أو استعمال معالجة معطيات إلكترونية شخصية لأغراض أخرى غير تلك المصرح بها أو المرخص لها:

تتحقق جريمة المعالجة غير المشروعة للمعطيات الإلكترونية الشخصية في هذه الصورة وفقا للمادة 58 سابقة الذكر **بإنجاز** معالجة للمعطيات الإلكترونية الشخصية متنافية مع الغايات المحددة و المعلنة و المشروعة التي تم ذكرها في التصريح المقدم إلى السلطة الوطنية[1]، أو تم إيرادها في الترخيص الممنوح من قبل هذه الأخيرة بناء على طلب المسؤول عن المعالجة[2]. فالهدف من تحديد الغاية من معالجة البيانات الشخصية

[1] – ألزم المشرع الجزائري على المسؤول عن المعالجة أن يتضمن التصريح طبيعة المعالجة و الغرض أو الأغراض المقصودة منها. أنظر المادة 14 /2 من القانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة بياناتهم الشخصية.

[2] – ألزم المشرع الجزائري أن يتضمن طلب الترخيص المعلومات المنصوص عليها في المادة 14 ، و التي تتضمن ذكر الغرض من المعالجة. أنظر المادة 20 من 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة بياناتهم الشخصية.

الإلكترونية هو تحقيق الرقابة لتجنب إساءة استخدام هذه المعطيات الإلكترونية من أي طرف كان[1].

فتجميع المعطيات ذات الطابع الشخصي يتم لغايات محددة بدقة و معلنة و مشروع، حيث يلزم في كل تجميع لهذه المعطيات أن يكون ضروريا من أجل الوصول إلى الأهداف المسطرة و المعلن عنها مسبقا من قبل الجهة المسؤولة عن تجميعها، دون أن تخرج هذه الأهداف المحددة و المعلنة عن المشروعية ، حيث يلزم أن تكون الغايات المجمعة على أساسها المعطيات الشخصية الإلكترونية مشروعة.

و عليه فإن كل معالجة للمعطيات الشخصية الإلكترونية للمستهلك تكون وفق الغايات التي تم على أساسها تجميع هذه المعطيات، حيث يلزم كل مسؤول على المعالجة عند معالجته عدم الخروج عن الأهداف التي تم على أساسها جمع المعطيات الشخصية الإلكترونية في البداية.

كما تتحقق أيضا هذه الجريمة **باستعمال** المعالج البيانات الشخصية الإلكترونية في غير الأغراض التي جمعت من أجلها، عن طريق إجراء معالجة لاحقة تتنافى مع الغايات التي سبق أن أجريت من أجلها المعالجة السابقة، و هيا الغايات التي يلزم أن يصرح بها أو مرخص لها من قبل السلطة الوطنية[2].

2-جمع المعطيات الإلكترونية الشخصية بطريقة تدليسيه أو غير نزيهة أو غير مشروعة:

فبمقتضى هذه الصورة يعد مرتكبا لجريمة المعالجة غير المشروعة للمعطيات الشخصية للمستهلك، كل من قام بجمع هذه الأخيرة بطريقة تدليسيه أو غير نزيهة أو

[1] – محمد على سالم و حسون عبيد هجيج، البطاقة الائتمانية و الأساس القانوني لحمايتها من التزوير، مجلة المحقق المحلي للعلوم القانونية و السياسية، ع2، 2015، ص 97.

[2] – أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة و بنوك المعلومات، دار النهضة العربية، القاهرة، 1988، ص 98.

غير مشروعة، أي الحصول عليها عن طريق الاحتيال و الغش[1]. و تعد المواقع الوهمية على شبكة الأنترنت من أخطر وسائل الاحتيال لجمع بيانات شخصية عن المستهلك، و ذلك عن طريق التجسس، حيث تقوم بعض الشركات الوهمية بوضع إشهارات تجارية و وعود مغرية للمستهلكين و هذا لكي يقوم بشراء سلعها و يقدم معلومات تعبر عن شخصيته من خلال نموذج العقد[2].

كما تتحقق عدم المشروعية في الحصول على المعطيات الشخصية للمستهلك بعدة طرق أخرى من بينها مراقبة و اعتراض و تفريغ الرسائل المتبادلة بواسطة البريد الإلكتروني ، أو ربط الحاسوب المخزنة داخله المعطيات بأسلاك بشكل خفي...ألخ[3]، إذ أن المجال المعلوماتي يحفل بالعديد من هذه الأساليب التي تعتمد بدورها على التقنية المعلوماتية و تتطور بشكل كبير جدا.

ثانيا: الركن المعنوي لجريمة المعالجة غير المشروعة للمعطيات الشخصية للمستهلك الإلكتروني

تعتبر جريمة المعالجة غير المشروعة للمعطيات الشخصية الإلكترونية للمستهلك من الجرائم العمدية التي تطلب توفر القصد الجنائي العام بعنصريه العلم و الإرادة، و ذلك بأن يعلم الجاني بالطبيعة الشخصية للمعطيات الإلكترونية و نشاط معالجتها و بأن الأفعال التي يأتيها من جمع لمعطيات إلكترونية شخصية بطريقة تدليسيه أو غير نزيهة أو غير مشروعة، أو إنجاز معالجة تتنافى مع الأغراض المصرح بها أو المرخص لها، أو استعمالها لغير أغراضها المنصوص عليها في التصريح أو الترخيص، كما يلزم أن تتجه إرادته إلى القيام بهذه الأفعال بذاتها، و إلا انتفى القصد لدى الجاني و من ثم الركن

---

[1] – عبد الفتاح بيومي حجازي، التجارة الإلكترونية و حمايتها القانونية، الكتاب الثاني، دار الكتب القانونية، مصر، 2007، ص 74.

[2] – شنين صالح، "**الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري**"، المجلة الأكاديمية للبحث القانوني، كلية الحقوق، جامعة عبد الرحمان ميرة، بجاية، ع01، 2010، ص 690.

[3] – هشام محمد فريد رستم، قانون العقوبات و مخاطر تقنية المعلومات ، مكتبة الآلات الحديثة، أسيوط، دون سنة نشر، ص 187.

المعنوي للجريمة. و نشير إلى أن الركن المعنوي لهذه الجريمة يقوم بمجرد توافر القصد الجنائي العام فقط دون حاجة إلى القصد الخاص[1].

ثالثا: العقوبة المقررة لجريمة المعالجة غير المشروعة للمعطيات الشخصية للمستهلك الإلكترونية

عاقب المشرع على جريمة المعالجة غير المشروعة للمعطيات الإلكترونية الشخصية للمستهلك أو المحاولة[2] بعقوبة أصلية و أخرى تكميلية، تتمثل الأصلية في الحبس أو الغرامة أو هما معا حسب كل فعل من الأفعال المكونة لها، فانطلاقا من المادة 58 من القانون 18-07 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي فإن العقوبة المقررة لكل من قام بإنجاز أو استعمال معالجة معطيات إلكترونية شخصية لأغراض أخرى غير تلك المصرح بها أو المرخص لها تكون الحبس من ستة (6) أشهر إلى سنة (1) و بغرامة من (60.000 دج) إلى (100.000دج) أو بإحدى هاتين العقوبتين فقط، أما من قام بفعل الجمع لمعطيات إلكترونية ذات طابع شخصي بطريقة تدليسيه أو غير نزيهة أو غير مشروعة فتكون العقوبة حسب نص المادة 59 من نفس القانون الحبس من سنة (1) إلى ثلاث (3) سنوات و بغرامة من(100.000دج) إلى (300.000دج).

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر ، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[3]، فتكون عقوبة

---

[1] – أيمن عبد الله فكرى، الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية و الأجنبية، ط1، مكتبة القانون و الاقتصاد، الرياض، السعودية، 2015، ص 692.

[2] – المادة 73 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب على محاولة ارتكاب إحدى الجنح المنصوص عليها في هذا القانون بنفس العقوبات المقررة للجريمة التامة".

[3] – المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة بياناتهم الشخصية " يعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون وفقا للقواعد المنصوص عليها في قانون العقوبات"

الشخص المعنوي بالنسبة لفعل إنجاز أو استعمال معالجة معطيات إلكترونية شخصية لأغراض أخرى غير تلك المصرح بها أو المرخص لها (100.000دج) إلى (500.000دج)، أما بالنسبة لفعل الجمع غير المشروع لمعطيات إلكترونية ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة فتكون العقوبة غرامة تتراوح بين (300.000دج) إلى (1.500.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[1]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[2]، أو أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[3].

[1] – المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي." يصادر محل الجريمة بغرض إعادة تخصيصه أو تدميره في إطار احترام التشريع المفعول.
يتحمل المحكوم عليه مصاريف إعادة التخصيص أو التدمير"

[2] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

[3] – المادة 71 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي." يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات.
كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة و التي نتج عنها ارتكاب الجريمة".

الفقرة الثانية: جريمة الاستعمال غير المشروع للمعطيات الشخصية للمستهلك الإلكتروني

جرم المشرع الجزائري استعمال المعطيات الشخصية الإلكترونية للمستهلك بطريقة غير مشروعة من خلال المادة 69 من قانون 18-07 المتعلق بحماية المعطيات الشخصية[1]، حيث ترتكب هذه الجريمة من قبل أشخاص معينين، يتسبب في الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستعملة أو تسهيل ذلك، أو أن يتم إيصالها لغير المؤهلين لذلك. و عليه سنحدد صفة الجاني باعتباره ركنا مفترضا (أولا)، و كل من ركنها المادي (ثانيا) و المعنوي (ثالثا)، و تحديد العقوبة المقررة لها (رابعا).

أولا: الركن المفترض (صفة الجاني) لجريمة الاستعمال غير المشروع للمعطيات الشخصية للمستهلك الإلكتروني

حددت المادة 1/69 من قانون 18-07 الأشخاص المسؤول عن هذه الجريمة، حيث ترتكب من قبل المسؤول عن المعالجة أو المعالج من الباطن، أو الشخص المكلف بحكم مهامه بمعالجة معطيات شخصية.

فبالنسبة للمسؤول عن المعالجة فهو كل شخص طبيعي أو معنوي عمومي أو خاص يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات و وسائلها[2].

أما المعالج من الباطن فهو كل شخص طبيعي أو معنوي، عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة[1].

---

[1] – المادة 69 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي "يعاقب بالحبس...كل مسؤول عن المعالجة و كل معالج من الباطن و كل شخص مكلف، بالنظر إلى مهامه، بمعالجة معطيات ذات طابع شخصي يتسبب أو يسهل، و لو عن إهمال الاستعمال التعسفي أو التدليسي للمعطيات أو المستعملة أو يوصلها إلى غير المؤهلين لذلك".

[2] – أنظر المادة 3 من القانون 18-07 . المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي

و فيما يتعلق بالشخص المكلف بمعالجة المعطيات ذات الطابع الشخصي بحكم مهامه، فيمكن القول بأنه كل شخص يتدخل في عملية المعالجة سواء بشكل مباشر أو غير مباشر دون أن يتعلق الأمر بمسؤول عن المعالجة أو معالج من الباطن، مثل موظفي المصالح التي تقوم بمعالجة المعطيات الشخصية، و الذين يكونوا خاضعين للسلطة المباشرة للمسؤول عن المعالجة أو للمعالج من الباطن.

ثانيا: الركن المادي لجريمة الاستعمال غير المشروع للمعطيات الشخصية للمستهلك الإلكتروني

يقوم الركن المادي لجريمة الاستعمال غير المشروع للمعطيات الشخصية بإتيان السلوك الإجرامي، إذ يتعلق الأمر بمجموعة من الأفعال و التصرفات التي يأتيها الفاعل، فتؤدي إلى استعمال تعسفي أو تدليسي للمعطيات المعالجة أو المستلمة، و إما القيام بإيصالها لغير المؤهلين لذلك[2].

فبالنسبة **للتسبب** في الاستعمال التعسفي للمعطيات الشخصية الإلكترونية أو التدليسي أو المستلمة أو تسهيل ذلك، فإذا كان فعل التسبب يفيد هنا قيام رابطة قوية بين الفعل الذي يأتيه الجاني، و بين الفعل المكون للاستعمال التعسفي أو التدليسي، فان فعل التسهيل يشمل كل فعل يمكن أن تكون له علاقة بفعل الاستعمال التعسفي أو التدليسي مهما كانت درجة هذه العلاقة[3]. و كما يمكن أن يرتكب التسبب أو التسهيل بفعل إيجابي فإنها يمكن أن يرتكبها بفعل سلبي.

و في ما خص الاستعمال التعسفي أو التدليسي فإننا نشير إلى أن هذا النص يطرح صعوبة أمام عدم دقة هذين المصطلحين، و يمكن القول بأن الاستعمال يكون تعسفيا أو

---

[1] – أنظر المادة 3 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي..

[2] – أنظر المادة 69 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي..

[3] – إبراهيم عيد نايل، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي ، دار النهضة العربية، القاهرة، 2000، ص 70.

تدليسيا حينما يتم الانحراف عن الغرض أو الغاية من معالجة المعطيات الشخصية، و ذلك على اعتبار أن هذه المعالجة تكون من أجل غاية أو غرض محدد دون غيره يحدد بشكل مسبق إما في النص التشريعي الذي يرخص بالمعالجة أو في التصريح أو الإذن بها[1]، و لما كان هذا التحديد يهدف إلى ضمان حماية للشخص المعني في مواجهة الأشخاص المسؤولين عن معالجة المعطيات الشخصية المكلفين بذلك، فان كل معالجة لا تندرج ضمن هذه الغاية تشكل تعسفا في استعمال المعطيات الشخصية[2].

و من جانب آخر يجب أن ينصب الاستعمال التعسفي أو التدليسي على المعطيات المعالجة أو المستلمة، فينصرف مصطلح المعطيات المعالجة إلى المعطيات التي تمت عليها عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها، مثل الجمع أو التسجيل...إلخ[3]، أما المعطيات المستلمة فيراد بها المعطيات التي حصل عليها أو تسلمها أحد الأشخاص السالف ذكرهم و لو يقم بأية عملية من عمليات المعالجة لهذه المعطيات الشخصية.

أما فيما يخص إيصال المعطيات الإلكترونية ذات الطابع الشخصي لغير المؤهلين لذلك، فيتحقق ذلك بقيام المسؤول عن المعالجة أو المعالج من الباطن أو كل شخص مكلف بحكم مهامه بمعالجة المعطيات الشخصية بإرسال هذه الأخيرة إلى أشخاص يمنع القانون إيصالهم بالمعطيات المذكورة، إذ يكون هنا الفاعل قد خرق الالتزام بالمحافظة على سرية المعطيات و استعمالها وفق الغايات المجمعة من أجلها[4]. و لا يشترط في قيام

---

[1] – بولين أنطنيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، لبنان، 2009، ص 62.

[2] – و في هذا السياق قضت محكمة ألمانية بوقف إحصاء للسكان سنة 1984 بعدما ثبت لها أن وزارة الداخلية استطاعت من خلال استمارات الإحصاء الحصول على عناوين مجموعة متطرفة إرهابية، حيث اعتبرت المحكمة ذلك من قبيل إساءة لاستخدام البيانات التي جمعت من اجل غاية معينة، و هو الإحصاء السكاني، و يشكل اعتداء على الحياة الخاصة للأفراد و انتهاكا لسرية البيانات الشخصية. **أنظر أسامة عبد الله قايد، المرجع السابق، ص53.**

[3] – المادة 3 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " المعالجة: كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل..."

[4] – بولين أنطنيوس أيوب، المرجع السابق، ص 63.

هذا العنصر الأضرار بالحياة الخاصة للشخص المعني بل تقوم الجريمة هنا بمجرد إيصال المعطيات الشخصية إلى أشخاص غير مؤهلين باستلامها و لو لم يترتب أي ضرر عن ذلك، و يكون الشخص غير مؤهل باستلام المعطيات عندما لا يخوله القانون الحق في الاطلاع عليها.

ثانيا: الركن المعنوي لجريمة الاستعمال غير المشروع للمعطيات الشخصية للمستهلك الإلكتروني

يتطلب لقيام الركن المعنوي لجريمة الاستعمال غير المشروع للمعطيات الشخصية الإلكترونية الخاصة بالمستهلك توفر قصدا جنائيا يوحي بعلم و إرادة الجاني لارتكاب هذه الجريمة، و يتضح من خلال المادة 69 من قانون 18-07 بأن جريمة الاستعمال غير المشروع للمعطيات الشخصية يمكن أن ترتكب عن طريق القصد، كما يمكن أن ترتكب عن طريق الخطأ، فانطلاقا من التنصيص على مجموعة الأفعال التي لا يمكن أن ترتكب إلا إذا كان للفاعل قصد، و هي التسبب و التسهيل، و الإيصال، و يستلزم في القصد هنا أن يكون الجاني عالما بأن الأفعال التي يقوم بها من شأنها أن تسبب أو تسهل الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة، أو أن أفعاله تشكل إيصالا لغير المؤهلين بذلك، و زيادة على ذلك يجب أن تتجه إرادة الجاني إلى القيام بهذه الأفعال.

أما بالنسبة للخطأ في هذه الجريمة فيتضح من خلال استعمال المشرع لعبارة " و لو عن إهمال"، و هو يفيد بأن كل فعل يرتكبه الجاني عن طريق الخطأ يؤدي إلى التسبب في الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو إلى تسهيل ذلك، يعد مكونا للركن المعنوي لجريمة الاستعمال غير المشروع للمعطيات الشخصية، و لا يلزم أن يكون الخطأ المرتكب في صورة إهمال فقط، بل يمكن أن يكون بأي صورة أخرى من صور الخطأ[1].

[1] – أسامة عبد الله قايد، المرجع السابق، ص 54.

رابعا: العقوبة المقررة لجريمة الاستعمال غير المشروع للمعطيات الشخصية للمستهلك الإلكتروني

عاقب المشرع من خلال المادة 69 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي على جريمة الاستعمال غير المشروعة للمعطيات الإلكترونية الشخصية للمستهلك أو المحاولة[1] بعقوبة أصلية و أخرى تكميلية، تتمثل الأصلية في الحبس من سنة (1) إلى خمس (5) سنوات و بغرامة من 100.000دج إلى 500.000دج. و الملاحظ أن المادة 69 من قانون 18-07 سالف الذكر قد سوت بين عقوبة الفعل المرتكب بشكل عمدي، و بين عقوبة الفعل المرتكب عن طريق الخطأ، و هو نهج غير سليم في نظرنا على اعتبار اختلاف الخطورة الإجرامية لدى مرتكب الفعل في الحالتين.

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[2]، فتكون عقوبة الشخص المعنوي الغرامة من (500.000دج) إلى (2.500.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[3]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[4]، أو

---

[1] – أنظر المادة 73 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – أنظر المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – أنظر المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[1].

الفقرة الثالثة: جريمة تحويل المعطيات الشخصية للمستهلك الإلكتروني نحو الخارج

جرم المشرع الجزائري تحويل المعطيات الشخصية المعالجة إلكترونية بما فيها الخاصة بالمستهلك نحو دولة أجنبية و ذلك من خلال نص المادة 67 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي[2]، و هذه الجريمة كغيرها من الجرائم تقوم بتوفر كل من ركنها المادي (أولا) و ركنها المعنوي (ثانيا)، كما أقر المشرع عقوبة تتماشى مع خطورتها (ثالثا).

أولا: الركن المادي لجريمة تحويل المعطيات الشخصية للمستهلك الإلكتروني نحو الخارج

يتمثل الركن المادي لهذه الجريمة وفقا للمادة 67 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي في نقل المعطيات الشخصية المستهلك من قبل المسؤول عن المعالجة الإلكترونية لدولة أجنبية دون توفر الشروط المنصوص عليها في المادة 44 من نفس القانون، و تتمثل هذه الشروط في موافقة الهيئة الوطنية لحماية المعطيات الشخصية، و إذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة و الحريات و الحقوق الأساسية للأشخاص

[1] – المادة 71 من قانون 18-07. المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات.

كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة و التي نتج عنها ارتكاب الجريمة".

[2] – المادة 67 من قانون 18-07 "يعاقب المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي بالحبس ...كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادة 44 من هذا القانون".

إزاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها. حتى و إن لم يترتب على هذا النقل أي ضرر[1].

غير أن المشرع الجزائري أجاز للمسؤول عن معالجة البيانات الشخصية نقلها لدولة أجنبية دون مراعات للشروط السابق ذكرها، و ذلك في حالات نصت عليها المادة 45 على سبيل الحصر، و تتمثل هذه الحالات في: الموافقة الصريحة للشخص المعني، إذا كان النقل ضروريا، إذا تم النقل تطبيقا لاتفاق ثنائي أو متعدد الأطراف تكون الجزائر طرفا فيه، بناء على ترخيص السلطة الوطنية، إذا كانت المعالجة في إطار احترام الكرامة الإنسانية و الحياة الخاصة و الحريات العامة و ألا تمس بحقوق الأشخاص و شرفهم و سمعتهم[2].

و عليه فإن تحويل القائم بالمعالجة للبيانات الشخصية المتعلقة بالمستهلك الإلكتروني نحو دولة أجنبية دون مراعات للشروط المنصوص عليها في المادة 44 من قانون 18-07 سابق الذكر، و في غير الحالات المنصوص عليها في المادة 45 من نفس القانون، يعد فعل معاقبا عليه وفقا للمادة 67 من نفس القانون.

ثانيا: الركن المعنوي لجريمة تحويل المعطيات الشخصية للمستهلك الإلكتروني نحو الخارج

إن جريمة نقل المعطيات الشخصية المعالجة إلكترونيا من الجرائم العمدية تأخذ صورة القصد الجنائي العام بعنصريه العلم و الإرادة، فتقوم متى علم الجاني بأن المعطيات شخصية و أن فعل نقلها لدولة أجنبية هو فعل معاقب عليه و انصرفت إرادته نحو ذلك[3].

---

[1] – أنظر المادة 44 من قانون 18-07. المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[2] – أنظر المادة 45 من 18-07. المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[3] – شنين صالح، المقال السابق، ص 209.

ثالثا: العقوبة المقررة لجريمة تحويل المعطيات الشخصية للمستهلك الإلكتروني نحو الخارج

عاقب المشرع الجزائري من خلال المادة 67 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي على جريمة تحويل المعطيات الإلكترونية الشخصية للمستهلك نحو دولة أجنبية أو المحاولة[1] بعقوبة أصلية و أخرى تكميلية، تتمثل الأصلية في الحبس من سنة (1) إلى خمس (5) سنوات و بغرامة من 500.000دج إلى 1.000.000دج.

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[2]، فتكون عقوبة الشخص المعنوي الغرامة من (500.000دج) إلى (5.000.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[3]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[4]، أو

---

[1] – أنظر المادة 73 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – أنظر المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – أنظر المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[1].

الفرع الثاني: الجرائم المتعلقة بحقوق الشخص المعني(المستهلك الإلكتروني)

خول المشرع للأشخاص المعنيين[2] بمعالجة معطياتهم الإلكترونية الشخصية بما فيهم المستهلك الإلكتروني، مجموعة من الحقوق في مواجهة المسؤول عن المعالجة، و ذلك بغية تمكينهم من حماية حياتهم الخاصة من كل اعتداء يمكن أن يطالها من جراء معالجة معطياتهم الشخصية إلكترونيا، و تبعا لذلك فإن كل معالجة يجريها المسؤول عن المعالجة دون موافقة مسبقة من الشخص المعني –المستهلك الإلكتروني– تشكل جريمة معاقب عليها (الفقرة الأولى)، و في نفس الإطار فإن كل اعتداء على حقوق الشخص المعني الخاصة –المستهلك الإلكتروني– المنصوص عليها قانونا يشكل هو الآخر فعلا مجرما(الفقرة الثانية).

الفقرة الأولى: جريمة معالجة المعطيات الشخصية دون موافقة المستهلك الإلكتروني

نظرا للطابع الخاص الذي تتميز به المعطيات الشخصية الإلكترونية منح المشرع للشخص المعني –المستهلك الإلكتروني– حق الموافقة المسبقة على معالجتها مما يعد التزاما واقع على المسؤول عن المعالجة، و مخالفة هذا الالتزام يعد جريمة معالجة دون

[1] – المادة 71 من قانون 18–07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي." يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات.

كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة و التي نتج عنها ارتكاب الجريمة".

[2] – الشخص المعني كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي به موضوع معالجة". انظر المادة 3 من قانون 18–07 و عليه فهذا التعريف يشمل المستهلك في التعاملات الإلكترونية لأنه يتعامل بعطياته الشخصية.

موافقة الشخص المعني وفقا للمادة 55 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة بياناتهم الشخصية[1].

و جريمة معالجة المعطيات الشخصية دون موافقة الشخص المعني –المستهلك الإلكتوني– كغيرها من الجرائم تتطلب لقيامها توافر كل من الركن المادي (أولا) و المعنوي (ثانيا)، كما أقر لها المشرع عقوبة تتماشى مع جسامتها (ثالثا).

أولا: الركن المادي لجريمة معالجة المعطيات الشخصية دون موافقة المستهلك الإلكتروني

يقوم الركن المادي لجريمة المعالجة دون موافقة الشخص المعني –المستهلك الإلكتروني– وفقا للمادة 55 من قانون 18-07 المتعلق بحماية المعطيات الشخصية في مجال معالجة المعطيات الشخصية بقيام المسؤول عن المعالجة بمعالجة المعطيات الشخصية دون موافقة مسبقة من الشخص المعني بما فيها المستهلك الإلكتروني وفقا لما نصت عليه المادة 07 من نفس القانون، كما تظهر عدم الموافقة أيضا عند اعتراضه. و سنحاول تبيان كل سلوك على النحو التالي:

1- القيام بالمعالجة دون موافقة الشخص المعني:

ألزم المشرع من خلال الفقرة الأولى من المادة 7 من قانون 18-07 كل مسؤول عن المعالجة أخذ الموافقة المسبقة للشخص المعني عند معالجة معطياته ذات الطابع الشخصي[2]، و موافقة الشخص تعني كل تعبير عن الإرادة المميزة يقبل بموجبه الشخص المعني أو ممثله الشرعي معالجة المعطيات الشخصية المتعلقة به بطريقة يدوية أو

---

[1] – المادة 55 من قانون 18-07 سالف الذكر " يعاقب بالحبس...كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من هذا القانون.

و يعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخصي المعني، عندما تستهدف هذه المعالجة لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب شرعية".

[2] – المادة 1/7 من قانون 18-07 " لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بموافقة الصريحة للشخص المعني".

إلكترونية[1]. فهذا الأخير يحل كل خلاف يمكن أن ينشأ بين المسؤول عن المعالجة و الشخص المعني، إذ أن ممارسة كل منهما لحقوقه و واجباته تتوقف على قبول الشخص المعني.

إذ تفرض الموافقة المسبقة على المسؤول على المعالجة ضرورة تنظيم عملية تجميع المعطيات بعد الاتصال بالشخص المعني و بشكل واضح و مقنع، كما يفرض استبعاد الرضا الضمني ، و يلزم في الرضا أن يكون واضحا لا يدع مجالا للشك، و هذا ما يفترض أن يكون له رابطة مطابقة للإعلام المسبق الذي يقوم به المسؤول عن المعالجة.

كما يلزم الحصول على هذا الرضى كذلك في كل إطلاع للغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة و المتعلقة بإنجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة و المرسل إليه[2].

غير أنه يمكن القيام بمعالجة معطيات شخصية دون موافقة الشخص المعني، و ذلك متى كانت المعالجة تدخل ضمن المعالجات الضرورية، و يتعلق الأمر بمجموعة من الحالات التي ترتبط فيها المعالجة بتحقيق مصالح مشروعة للشخص المعني (المستهلك) أو المسؤول عن المعالجة، و كذلك مصالح مرتبطة بالصالح العام، و هيا حالات محددة على سبيل الحصر نصت عليهم المادة 07 في فقرتها الخامسة، و تشمل كل من[3]:

-لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة: و تنصرف عبارة الالتزام القانوني إلى كل التزام يستمد مصدره من القانون سواء تعلق الأمر بنص تشريعي أو تنظيمي.

---

[1] – انظر المادة 03 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[2] – أنظر المادة 4/7 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – أنظر المادة 5/7 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

-لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه: فيما يتعلق بتنفيذ العقد فإن هذا المقتضى لا يثير إشكالات كبيرة، فمن الواضح أن المعطيات المطلع عليها في إطار عقد شراء يتم عبر الأنترنت تصلح أو تعين على المعالجة الضرورية للتسليم أو الأداء. فتحصيل الرضا يكون هنا ضمنيا و لا حاجة من ثم إلى تعبير صريح عن الإرادة، و يسري هذا المقتضى على كافة أنواع و أشكال العقود[1].

أما بالنسبة للإجراءات السابقة للعقد، فإنه تجدر الإشارة إلى أن مفهوم هذه الإجراءات يبقى غير محدد و يمكن أن يفسر وفق مفهوم واسع، و يجد هذا المقتضى تطبيقه بشكل خاص في عدد من المعاملات التي تتم عن بعد و عبر شبكة الأنترنت[2]، و يدخل في هذا الإطار بعض الإجراءات التي تتم في إطار التجارة الإلكترونية، كالتسجيلات أو الاشتراكات أو طلبات و الوثائق[3].

-للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه: تعد عبارة المصالح الحيوية التي جاء بها المشرع الوطني واسعة و غير دقيقة و هي نفس العبارة التي جاء بها التوجيه الأوروبي

"Intérét vital (م7/د)، و هي عبارة ذات أصل أنجليزي حيث جاءت من الترجمة الحرفية لكلمة vital interest [4]، و حقيقة الأمر أنها تشكل مصدر لبس و غموض، و

---

[1] - Christiane féral-schuhl: Cyber droit. Le a l'épreuve de l'internet. 2éme éd 2000. Dalloz. Dunod. Chapiter 7. P 100 .

[2] -Thierry Piette-Coudol et André Bertrand. Internet et la loi. Ed. dalloz. Paris 1997. P109.

[3] - عفيف كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت، 2003، ص 276.

[4] - André lucas. Jean Deveze et Jean Freyssinet. Droit de l'informatique et de l'internet. Presses univerditaires de France. Economies. Paris 2001. P131.

إن كانت الحيثية 31 من التوجيه الأوروبي حددتها في المصلحة الأساسية لحياة الشخص المعني[1].

و يلاحظ أن المشرع الجزائري تميز عن التوجيه الأوروبي في أنه استلزم في الشخص المعني (المستهلك الإلكتروني) المراد المحافظة على مصالحه الحيوية أن يكون من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه.

-لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم اطلاعه على المعطيات: بمقتضى هذه الحالة لا يكون رضى الشخص المعني ضروريا أو لازما في المعالجة التي تكون ضرورية لتنفيذ إحدى المهام التي تدخل ضمن الصالح العام أو ضمن ممارسة السلطة العمومية التي يقوم بها المسؤول عن المعالجة أو أحد الأغيار عندما يتم اطلاعه على المعطيات الشخصية، و يتعلق الأمر أساسا بالمعالجات التي تكون ضرورية لسير مجموعة من المصالح العامة، و مصالح السلطات العمومية، و غيرها من الوظائف و المهام التي يقوم بها الأشخاص المنتمون للقانون العام، كمصالح الجمارك و الضرائب، و مصالح المؤسسات العمومية كالوكالة الوطنية للمحافظة العقارية[2].

-لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و / أو حقوقه و حرياته الأساسية: يلاحظ أن هذا المقتضى يبقى غامضا إذ أن المشرع الوطني على غرار التوجيه الأوروبي لم يضع معيارا يمكن من تحديد المصلحة المشروعة و التي تتعارض مع حقوق و حريات الشخص المعني، و قد اكتفت الحيثية 30 من التوجيه الأوروبي بتعداد مجموعة من الأمثلة التي تدخل في هذا الإطار و هي: التسيير الجاري بالمقاولات أو الهيئات الأخرى، الاستقراء

---

[1] – Christiane Féral-schuhl. Op.cit. P144.

[2] – PIERRE Kayser. La protection de la vie privée par le droit. Protection du secret de la vie privée. Economica marseille.1995. P 430.

التجاري أو الاستقراء عن طريق جمعية[1]. و يبقى أي تقييم للمصلحة المشروعة للمسؤول عن المعالجة أو المرسل إليه مقرونا بترجيح مصلحة الشخص المعني و كذا حقوقه و حرياته الأساسية

و هكذا فكل عملية معالجة يجريها المسؤول عن المعالجة على المعطيات الإلكترونية ذات الطابع الشخصي المتعلقة بالمستهلك، دون موافقة صادرة عن هذا الأخير و في غير الحالات التي يجيز فيها القانون ذلك يعد جريمة معاقب عليها وفق للمادة 55 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

2- إجراء المعالجة رغم اعتراض الشخص المعني:

تتحقق هذه الصورة عند مواصلة معالجة المعطيات الشخصية الإلكترونية رغم اعتراض الشخص المعني وفق المقتضيات القانونية المنصوص عليها[2]، فيشترط أن يكون الاعتراض مبنيا على أسباب مشروعة، و ذلك حسب ما يتبين للشخص المعني (المستهلك الإلكتروني) على كمعالجة معطياته بطريقة غير نزيهة أو أنه تم معالجها خارج الغرض أو الأغراض التي جمعت من أجلها أو أنه المسؤول عن المعالجة جمع معطيات غير مناسبة و مبالغ فيها بالنظر إلى الغايات التي جمعت من أجلها أو معالجتها، أو أنها غير صحيحة ...إلخ[3]، على أن يخضع تقدير مشروعية هذه الأسباب لمحكمة الموضوع .أما إذا كان الاعتراض منصبا على معالجة تستهدف الإشهار التجاري، ففي هذه الحالة لا يلزم أن يكون الاعتراض مبنيا على سبب مشروع.

---

[1] - A RIANE Mole: « le nouveau droit des flux transfornteres des données personnelles »revde. Soc.n12 déc.2004.p 1072. .

[2] - المادة 2/55 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " و يعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخصي المعني، عندما تستهدف هذه المعالجة لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب شرعية".

[3] - Michel Bibent. Le droit du tratement de l'informatique. Nathany/HER.Paris.2000. P44.

و عليه فإن كل معالجة يجريها المسؤول عن المعالجة على المعطيات الشخصية الإلكترونية للمستهلك رغم تقديم اعتراض وفق إحدى الحالتين السالفتين الذكر، يشكل جريمة معاقب عليها وفق المادة 55 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

و نشري في الأخير إلى أن جريمة معالجة معطيات شخصية بدون موافقة أو اعتراض الشخص المعني جريمة شكلية لا يتوقف قيامها على تحقق نتيجة معينة، في صورة إضرار بالحياة الخاصة للشخص المعني[1]، بل تتوافر هذه الجريمة بمجرد معالجة معطيات شخصية دون الموافقة المسبقة للشخص المعني، أو إجراء المعالجة رغم اعتراضه.

ثانيا: الركن المعنوي لجريمة معالجة المعطيات الشخصية دون موافقة المستهلك الإلكتروني

أما فيما يخص الركن المعنوي لهذه الجريمة فيلزم وجود القصد الجنائي، على اعتبار أن هذه الجريمة عمدية لا تقوم بمجرد الخطأ، و يتحقق القصد إذا كان الشخص عالما بأنه يقوم بفعل يشكل معالجة للمعطيات الشخصية، و أن هذه المعالجة يجريها بدون موافقة مسبقة للشخص المعني، و دون أن تندرج معالجته ضمن المعالجات الضرورية التي رخص فيها المشرع على سبيل الحصر بإنجاز معالجة و لو دون موافقة مسبقة من الشخص المعني، و أنه يعالج معطيات على الرغم من اعتراض صاحبها المبني على أسباب مشروعة أو المنصب على المعالجة التي يجريها الجاني من أجل القيام بأعمال الإشهار التجاري، بالإضافة إلى عنصر العلم يلزم أن تتجه إرادة الجاني إلى القيام بهذه الأفعال[2].

[1] – هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دراسة مقارنة، دار الكتب القانونية، مصر، 2015، ص 50.

[2] – آدم عبد البديع آدم حسين، المرجع السابق، ص 578.

ثالثا: العقوبة المقررة لجريمة معالجة معطيات شخصية دون موافقة المستهلك الإلكتروني

عاقب المشرع الجزائري من خلال المادة 55 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي على جريمة معالجة المعطيات الشخصية دون موافقة الشخص المعني -المستهلك الإلكتروني- أو المحاولة[1] بالحبس من سنة (1) إلى ثلاث (3) سنوات و بغرامة مالية من 100.000دج إلى 300.000دج[2].

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[3]، فتكون عقوبة الشخص المعنوي الغرامة من (300.000دج) إلى (1.500.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[4]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[5]، أو

---

[1] – أنظر المادة 73 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[2] – أنظر المادة 55 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – أنظر المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] – أنظر المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[5] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[1].

الفقرة الثانية: جريمة مخالفة الحقوق الخاصة بالمستهلك الإلكتروني

يتمتع الشخص المعني –المستهلك الإلكتروني– بمعالجة معطياته و بياناته الشخصية بمجموعة من الحقوق و ضمانات توفر له الحماية اللازمة و تمثل نوع من الرقابة على معطياته الشخصية الخاضعة للمعالجة، و قد أفرد المشرع لهذه الحقوق الباب الرابع من القانون 18–07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي تحت تسمية حقوق الشخص المعني بما فيها المستهلك الإلكتروني، و هيا مجموعة من الحقوق المتكاملة فيما بينها، و التي يمكن ممارستها في كل وقت، و كل خرق لهذه الحقوق يعد جريمة معاقب عليها بموجب المادة 64 من نفس القانون[2].

و جريمة مخالفة الحقوق الخاصة بالشخص المعني –المستهلك الإلكتروني– كغيرها من الجرائم تقوم بتوفر كل من ركنها المادي (أولا) و ركنها المعنوي (ثانيا)، كما أقر لها المشرع عقوبة (ثالثا).

أولا: الركن المادي لجريمة مخالفة الحقوق الخاصة بالمستهلك الإلكتروني

يتحقق الركن المادي لهذه الجريمة وفقا للمادة 64 من قانون 18–07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي برفض

---

[1] – المادة 71 من قانون 18–07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي." يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات.

كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة و التي نتج عنها ارتكاب الجريمة".

[2] – المادة 64 من قانون 18–07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب بالحبس ...كل مسؤول عن المعالجة يرفض دون سبب مشروع حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض المنصوص عليها في المواد 32 و 34 و 35 و 36 من هذا القانون".

المسؤول عن المعالجة تمكين الشخص المعني –المستهلك الإلكتروني– من حقوقه. إذ يمكن القول أن هذه الحقوق تعبر عن شكل جديد من حقوق الإنسان المعاصرة ، و ذلك في حقه في الإخبار و الحق في الشفافية[1]، و هيا كذلك تعبر عن حقه في حماية هوية الأشخاص و إصلاح كل ضرر يمكن أن يلحق بها جراء تعدي الغير عليها[2]. و تتمثل هذه الحقوق حسب المادة 64 السابق ذكرها في حق الإعلام و الولوج و التصحيح و الاعتراض. و سنحاول التطرق لكل منها بشكل من التفصيل على النحو التالي:

1- رفص الحق في الإعلام:

الزم المشرع من خلال المادة 32 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي إعلام الأشخاص المعنيين الذين يتم الاتصال بهم لجمع المعطيات بمجموعة من العناصر، و ذلك قبل القيام بهذا التجميع، و يتوجب أن يكون الإعلام صريحا و لا يحتمل اللبس.

و يقع هذا الالتزام على عاتق كل من المسؤول عن المعالجة أو من يمثله و لا يسقط إلا في الحالة التي يكون فيها الشخص المعني (المستهلك الإلكتروني) على علم مسبق بالعناصر اللازمة لإعلامه بها، و تتمثل هذه العناصر في:

–هوية المسؤول عن المعالجة و عند الاقتضاء هوية ممثله.

–أغراض المعالجة.

– كل معلومة إضافية مفيدة، لاسيما المتعلقة بالمرسل إليه و مدى إلزامية الرد و الآثار المترتبة عن ذلك و حقوقه و نقل المعطيات إلى بلد أجنبي[3].

---

[1] – André lucas. Jean Deveze et Jean Freyssinet. Op cit. p 99.

[2] – PIERRE Kayser. La protection de la vie privée par le droit.. op cit. p 491.

[3] – أنظر المادة 1/32 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

أما في حالة تجميع المعلومات عن طريق شبكة مفتوحة، و يتعلق الأمر هنا بصفة خاصة بشبكات الاتصال الإلكترونية العالمية (الأنترنت)، فيلزم المسؤول عن المعالجة أو ممثله بإعلام الشخص المعني بجميع المعلومات السابقة، و إعلامه ما لم يكن على علم مسبق بأن معلوماته الشخصية يمكن أن تتداول في الشبكات دون ضمانات السلامة و أنها قد تتعرض للقراءة و الاستعمال من طرف الغير[1].

و إن كان المبدأ هو أن المعطيات ذات الطابع الشخصي يمكن أن يتم تجميعها لدى الشخص المعني بهذه المعطيات، فإنه في بعض الحالات يمكن أن يتم تجميع المعطيات المتعلقة بهذا الأخير لدى شخص آخر. لكن رغم ذلك فإن الشخص الذي يتم تجميع معطياته يبقى له الحق في الإعلام، حيث يبقى على عاتق المسؤول عن المعالجة أو الشخص الذي يمثله إعلام الشخص المعني بالمعلومات المذكورة سابقا[2]، غير أنه يتم هذا الإعلام قبل تسجيل المعطيات أو قبل إيصالها للغير، غير أن المسؤول عن المعالجة أو ممثله يمكن أن يتحلل من الالتزام بالإعلام إذا كان هذا الأخير على علم مسبق بالمعلومات المتوجب إخباره بها[3].

و سواء تعلق الأمر بتجميع مباشر أو غير مباشر للمعطيات الشخصية للمستهلك، فإن تقديم المعلومات من المسؤول عن المعالجة أو ممثله القانوني يمكن أن يتم بأي وسيلة تحقق هذه الغاية، و من بين هذه الوسائل رسالة إلكترونية أو دعامة ورقية، عرض

---

[1] – انظر المادة 3/32 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – يتعلق الأمر في هذه الحالة بتجميع غير مباشر للمعطيات، و هو بمثابة التزام غير مرن مكلف، معقد من حيث القيام به، كما انه يخلق تضييقا بالنسبة لعدد من القطاعات ، و هو ذا أهمية من الناحية الإقتصادية بالنسبة لمن يحوز ملفات تحتوي على معطيات للغير أنظر....13 **lucas. Jean Deveze et Jean Freyssinet. Op cit. p André.**

[3] – انظر المادة 2/32 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات

أو نموذج إلكتروني[1]. و في الأخير فإن هذا الالتزام يبقى أساسيا عند القيام بعمليات التسويق المباشر و المعاملات و التجارة الإلكترونية[2].

و لقد استثنى المشرع الجزائري بعض الحالات و هيا على سبيل الحصر من نطاق الحق في الإعلام، حيث لا يكون للشخص المعني بتجميع معطياته الإلكترونية الشخصية فيها الحق في الإعلام، فالحالة الأولى تتعلق بتعذر إعلام الشخص المعني لاسيما في حالة المعالجة لأغراض إحصائية أو تاريخية أو علمية، إذ يأتي استبعاد تطبيقه في هذه الحالة بسبب استحالته من الناحية العلمية، لذلك و من أجل حماية حقوق الشخص المعني يلزم المسؤول عن المعالجة إشعار السلطة الوطنية بهذه الاستحالة مع تقديم السبب الذي يبررها[3]. و نشير هنا إلى أن قانون 18-07 استبعد تطبيق الحق في الإعلام سواء تم التجميع لدى الشخص المعني أو لدى شخص آخر، و ذلك على عكس التوجيه الأوروبي (م2/11) الذي استبعدها في الحالة الثانية دون الأولى.

أما الحالة الثانية فقد استبعد المشرع من الحق في الإعلام كذلك الحالة التي ينص فيها القانون على تجميع و معالجة المعطيات ذات الطابع الشخصي، أو إذا تمتمت المعالجة حصريا لأغراض صحفية أو فنية أو أدبية[4].

و الملاحظ أن المشرع الجزائري لم يوفق إلى تعداد هذه الحالات على خلاف التوجيه الأوروبي في المادة 13 الذي ذكر حالة تتعلق بالدفاع الوطني و الأمن الداخلي أو الخارجي للدولة أو للوقاية من الجريمة، و كذلك في حالة المصلحة الاقتصادية أو المالية للدولة في الميادين النقدية[5]. كما أنه قد ساهم في حصر و تضييق نطاق الحق في الإعلام و هيا سياسة تضعف من الحماية التي جاء بها قانون 18-07 المتعلق بحماية

---

[1] – Michel Bibent. Le droit du tratement de l'informatique. Op ciy. P 47.

[2] – André lucas. Jean Deveze et Jean Freyssinet. Op cit. p 13.

[3] – أنظر الفقرة 1 من المادة 33 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] – أنظر الفقرة 2 و 3 من المادة 33 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[5] – Marie-Claire Ponthoreau. Op. cit. p 125.

الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي من أجل ضمانها.

و عليه وبناء على ما سبق يتحقق رفض الإعلام إذا لم يعلم المسؤول عن المعالجة أو ممثله الشخص المعني بالمعلمات السابق ذكرها في المادة 32 من قانون 18-07 قبل جمعها عندما يتعلق الأمر بالشخص المعني أو قبل تسجيها أو نقلها للمرسل إليه إذا تعلق الأمر بالغير، أو كان هذا الإعلام غير صريح. على ألا تدخل المعالجة في الحالات التي يستثني فيها القانون عدم الإعلام كما تم توضيحه سابقا. مما يؤدي إلى قيام جريمة مخالفة الحقوق الخاصة للشخص المعني –المستهلك الإلكتروني-.

2-رفض الحق في الولوج:

بالإضافة إلى الحق في الإعلام منح المشرع كذلك للشخص المعني –المستهلك الإلكتروني- الحق في الولوج من خلال المادة 33 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهو حق لا يتوقف الاستفادة منه على ضرورة الاستفادة من الأول، إذ يتمتع الشخص المعني بمعالجة المعطيات بمقتضاه في مواجهة المسؤول عن المعالجة بالحق في العلم بمجموعة من العناصر أولها التأكيد على كون المعطيات الشخصية المتعلقة به تعالج إلكترونيا أو لا تعالج، و يشمل كذلك على المعلومات المنصبة على غايات المعالجة الإلكترونية و فئات المعطيات المتعلقة بها، و المرسل إليهم أو فئات المرسل إليهم الذين أوصلت إليهم المعطيات ذات الطابع الشخصي[1].

و عليه يتحقق رفض الحق في الولوج، برفض المسؤول عن المعالجة تمكين الشخص المعني من المعلومات السابق بيانها كما يتحقق الرفض أيضا عند إحاطته بالمعطيات الخاضعة للمعالجة و بكل معلومة متاحة خاصة بمصدر المعطيات و ذلك بطريقة غير مفهومة.

[1] – انظر المادة 34 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

غير أن المشرع الجزائري أجاز للمسؤول عن المعالجة رفض طلبات الولوج التعسفية، لاسيما من حيث عددها و طابعها المتكرر، إذ يقع على عاتق المسؤول عن المعالجة إثبات الطابع التعسفي لهذا الطلب[1].

و الملاحظ أن المشرع الجزائري عند نصه و تنظيمه لهذا الحق اغفل كيفية ممارسة حق الولوج و الإجراءات المتبعة لذلك، غير انه بالرجوع إلى التوجيه الأوروبي[2] نجد أن ممارسة الحق في الولوج يمارس من قبل الشخص المعني فقط، الذي يمكنه أن يختار مستشارا لمساعدته كما يمكن أن يفوض شخصا آخر بصفة وكيل خاص، أما بالنسبة للقاصر فإنه يمارس حقه عن طريق وليه القانوني، و يكون ذلك أمام الجهة التي تقوم بتجميع المعطيات الشخصية المتعلقة بالشخص المعني، أو أمام الجهة التي تحوز هذه المعطيات حسب الأحوال. **أما عن طريقة ممارسته فبطبيعة الحال يكون عن طريق طلب كتابي** و ذلك إما بطريقة تقليدية أو إلكترونية، و يقدم في هذه الحالة إلى المسؤول عن المعالجة و يكون محدد بدقة [3].

أما في الحالة التي يكون فيها الملف أو الملفات التي تحتوي على المعطيات الشخصية خاضعة لإدارة مشتركة لعدة مسؤولين، فانه يمكن مباشرة حق الولوج إلى المعطيات لدى أي منهم، ما عدا إذا كانت مسؤولية إدارة الملفات يتحملها مسؤول واحد فقط[4].

---

[1] – انظر الفقرة الثانية من المادة 34 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – لم ينص المشرع الوطني على استثناءات على ممارسة الحق في الولوج على غرار التوجيه الأوروبي الذي جعل نفس الاستثناءات المتعلقة بالحق في الإعلام تسري كذلك على الحق في الولوج .**أنظر Marie-Claire Ponthoreau. Op. cit. p 126.**

[3] – Marie-Claire Ponthoreau. Op. cit. p 127

[4] – PIERRE Kayser. La protection de la vie privée par le droit.. op cit. p 492.

3-رفض الحق في التصحيح:

يرتبط الحق في التصحيح برابطة وظيفية مع الحق في الولوج، إذ أن ممارسة الأول تتوقف بشكل كبير على الثاني، و يشكل الحق في التصحيح ضمانة أساسية لحماية الحياة الخاص, للأفراد، حيث يتيح لهؤلاء سلطة حقيقية لمراقبة مختلف المعالجات التي يمكن أن تكون معطياتهم الشخصية محلا لها، و من ثم فهو يشكل بالمقابل التزاما على عاتق المسؤول عن المعالجة الذي يلزمه تصحيح أو إكمال المعطيات المعالجة ، و تظهر أهمية الحق في التصحيح في أن استعماله يبقى مفتوحا في وجه كل شخص معني بمعالجة معطياته و ذلك بشكل حر و في كل وقت، و بدون أي شرط و دون أن يتوقف على وجود نزاع حقيقي[1].

إذ ألزم المشرع كل مسؤول عن المعالجة أن يمكن الشخص المعني أو ورثته مجانا من تصحيح المعطيات الشخصية التي يتم معالجتها، و يشمل هذا التصحيح تحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية في الحالة التي تكون فيها معالجة هذه المعطيات غير قانونية كعدم اكتمالها أو عدم صحتها، أو لكون معالجتها ممنوعة، و ذلك خلال 10 أيام [2].

و عليه يتحقق رفض الحق في التصحيح عند رفض الطلب أو عدم الاستجابة داخل 10 أيام ، و في هذه الحالة يحق للشخص المعني إيداع طلب تصحيح لدى اللجنة الوطنية، حيث تكلف أحد أعضائها من أجل القيام بالتحقيقات المفيدة و العمل على إجراءات التصحيحات اللازمة في أقرب الآجال، و حماية لحقوق الشخص المعني يجب إبقاؤه على إطلاع بالنتائج المتوصل إليها، و يكون ذلك عن طريق إخباره كتابة بالتدابير المتخذة[3].

---

[1] – André lucas. Jean Deveze et Jean Freyssinet. Op cit. p 112.

[2] – أنظر المادة 35/أ /1من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي..

[3] – أنظر المادة 35/أ/2 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

كما يعد أيضا رفض لحق في التصحيح، عدم تبليغ الغير الذي أوصلت إليه المعطيات الشخصية بكل تحيين أو تصحيح أو مسح أو إغلاق للمعطيات ما لم يكن ذلك مستحيلا[1].

و يلاحظ هنا أن المشرع الجزائري من خلال عبارة" **استحالة**" التبليغ لم يضع ضابطا دقيقا لتحديد ما إذا كان التبليغ ممكنا أو متعذرا، و يبقى تحديد ذلك من اختصاص السلطة التقديرية لقضاء الموضوع بحس كل جالة على حدة.

و الجدير بالذكر أن تبليغ الأغيار لا يطرح صعوبات كبيرة على شبكة الأنترنت إذ يمكن تبليغ ملفات ضخمة في مختلف مناطق العالم بمجرد نقرة واحدة على الحاسوب، فقد أصبح تدفق المعلومات سهلا و سريعا[2].

4-رفض الحق في الاعتراض:

ألزم المشرع الجزائري من خلال المادة 36 من قانون 18-07 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي المسؤول عن المعالجة تمكين الشخص المعني –المستهلك الإلكتروني- بمعالجة معطياته الشخصية من ممارسة حق التعرض، إذ يمثل الحق في التعرض أحد الحقوق الأساسية التي منحها المشرع للشخص المعني بغية حماية حياته الخاصة، حيث يعد بمثابة سلطة في مواجهة استعمال معطياته الشخصية من قبل المسؤول عن المعالجة أو الغير[3].

غير أن المشرع اشترط على الشخص المعني عند ممارسة هذا الحق أن يبين الأسباب المشروعة التي يستند إليها عند تعرضه على معالجة معطياته الشخصية[4]، و لا شك أن هذا الشرط يطرح مجموعة من الإشكالات حول كيفية تقدير و تطبيق الحق في

---

[1] – المادة 36/ب من قانون 18-07 ا المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – Christiane féral-schuhl: Cyber droit. Le a l'épreuve de l'internet. Op. cit. p 105.

[3] – André lucas. Jean Deveze et Jean Freyssinet. Op cit. p 114.

[4] – أنظر المادة 36-1 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في معالجة المعطيات الشخصية .

التعرض و كذا حول الجهات المؤهلة للترجيح بين مصالح الشخص المعني و مصالح المسؤول عن المعالجة ، ثم حول العناصر التي يستند إليها هذا الأخير لرفض الاستجابة لطلب التعرض، و يبقى القضاء في كل الأحوال الجهة الوحيدة المختصة لحل كل نزاع يمكن أن ينشأ ، و ذلك بحسب ظروف كل حالة على حدة و عن طريق التوفيق بين الوقائع و النص القانوني.

بالإضافة إلى شرط مشروعية أسباب التعرض، فإن الشخص المعني لا يمكنه أن يمارس الحق في التعرض إذا كانت المعالجة تستجيب لالتزام قانوني، أو إذا كان الشخص المعني قد تنازل صراحة عن الحق في التعرض في المحرر الذي يأذن بالمعالجة[1].

أما إذا استعملت معطيات الشخصية للشخص المعني –المستهلك الإلكتروني– لأغراض دعائية خاصة التجارية، فإنه يمكن لهذا الأخير أن يوجه طلب التعرض في كل وقت و دون مصاريف إلى المسؤول عن المعالجة الحالي، أو كل مسؤول عن المعالجة اللاحق دون أن يكون ملزما بتبرير هذا التعرض، حيث تخضع ممارسة هذا الحق للسلطة التقديرية الواسعة للشخص المعني[2]. و لا شك أن توسيع المشرع لممارسة الحق في التعرض على المعالجات التي تتخذ لأغراض دعائية يشكل واجبا على المسؤولين عن هذا النوع من المعالجة، ضرورة احترام رضى الشخص المعني، حيث يمنع عليهم استعمال بيانات شخص لم يعبر عن رضاه المسبق بشأن استقبال المسائل الدعائية و التي من أهمها الاستقراءات المباشرة، التي تستعمل فيها آلية اتصال أو جهاز الاستنساخ البعدي أو بريد إلكتروني أو وسيلة تستخدم تكنولوجيات ذات طبيعة مماثلة.

و نشير في الأخير إلى أن جريمة الاعتداء على حقوق الشخص المعني جريمة شكلية لا يتوقف قيامها على تحقيق نتيجة معينة، في صورة إضرار بالحياة الخاصة له، بل تتوافر هذه الجريمة بمجرد رفض حقوق ممارسة الشخص المعني لحقوقه.

---

[1] – أنظر المادة 3/36 من قانون 18–07 المتعلق بحماية الأشخاص الطبعيين في معالجة المعطيات الشخصية.

[2] – أنظر المادة 2/36 من قانون 18–07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ثانيا: الركن المعنوي لجريمة مخالفة حقوق المستهلك الإلكتروني

تتطلب هذه الجريمة ركنا معنويا لقيام الجاني بجريمة الاعتداء على حقوق الشخص المعني –المستهلك الإلكتروني–، إذ يجب أن يتوافر لدى المسؤول عن المعالجة قصدا لارتكابها، باعتبار أن الجريمة عمدية، و يتحقق القصد العمدي لدى الجاني بعلمه أنه يرتكب أفعالا تشكل رفضا للحق في الإعلام أو الولوج، أو الحق في التصحيح، أو الحق في الاعتراض، كما يلزم أن يكون لدى الجاني الإرادة للقيام بهذا الفعل دون غيره.

ثالثا: العقوبة المقررة لجريمة مخالفة حقوق المستهلك الإلكتروني

انطلاقا من المادة 64 من قانون 18-07 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي فإن جريمة مخالفة حقوق الشخص المعني بمعالجة بياناته الشخصية وقع لها المشرع عقوبة الحبس من شهرين (2) إلى سنتين (2) و غرامة من 20.000دج إلى 200.000دج، أو بإحدى هاتين العقوبتين فقط.

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر ، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[1]، فتكون عقوبة الشخص المعنوي الغرامة من (200.000دج) إلى (1.000.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[2]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية

[1] – أنظر المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – أنظر المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[1]، أو أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[2].

[1] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

[2] – أنظر المادة 71 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

المطلب الثاني: الجرائم الماسة بالقواعد الشكلية لمعالجة المعطيات الشخصية للمستهلك الإلكتروني

يقتضي القيام بمعالجة المعطيات الإلكترونية ذات الطابع الشخصي للأشخاص بما فيهم المستهلك الإلكتروني ضرورة احترام مجموعة من القواعد الشكلية التي نص عليها المشرع من خلال قانون 18-07 المتعلق بحماية الأشخاص الطبعيين عند معالجة معطياتهم الشخصية بهدف حماية الأشخاص في مواجهة هذه المعالجة، حيث يلزم المسؤول عن المعالجة قبل إجرائها، ضرورة القيام ببعض الشكليات المسبقة، التي تخوله معالجة المعطيات الإلكترونية الشخصية و من ثم فإن مخالفة هذه الشكليات يعد جريمة معاقب عنها(الفرع الأول)، و من أجل ضمان سلامة المعطيات الإلكترونية الشخصية و حمايتها من مختلف المخاطر التي يمكن أن تتعرض لها و خاصة انتهاك سريتها، فرض المشرع على المسؤول عن المعالجة ضرورة اتخاذ مجموعة من التدابير لضمان أمنها، كما ألزمه ضرورة احترام التعاون مع السلطة الوطنية و إلا اعتبر مرتكبا لجرائم معاقب عنها(الفرع الثاني).

الفرع الأول: الجرائم المتعلقة بالشكليات المسبقة لمعالجة المعطيات الشخصية للمستهلك الإلكتروني

يلزم قبل إجراء معالجة للمعطيات الشخصية الإلكترونية للأشخاص بما فيهم للمستهلك الإلكتروني، ضرورة تقديم المسؤول عن المعالجة تصريحا بذلك أو الحصول على ترخيص من قبل السلطة الوطنية، و ذلك وفقا لمقتضيات المادة 12 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، و من ثم فإن كل معالجة يجريها المسؤول في غياب التصريح أو الترخيص تعد جريمة معاقب عنها (الفقرة الأولى)، و في نفس الإطار يلزم المسؤول عن المعالجة قبل إجراء المعالجة على معطيات حساسة ضرورة الحصول على الموافقة المسبقة للشخص المعني لهذه المعالجة و إلا كانت معالجته معاقب عليها (الفقرة الثانية).

الفقرة الأولى: جريمة معالجة المعطيات الشخصية للمستهلك بدون تصريح أو ترخيص

تلزم المعاملات الإلكترونية على المستهلك تبادل بياناته الشخصية مع صاحب السلع أو مقدم الخدمة[1]، و نظرا لأهمية و قيمة هذه البيانات فقد فرض الحصول على ترخيص كإجراء سابق على تداول تلك البيانات، تمنحه جهة مختصة يناط بها هذا دون غيرها من الجهات الأخرى[2]. و مخالفة هذا الالتزام يعد جريمة معالجة بدون ترخيص أو تصريح وفقا للمادة 56 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي[3]. و هذه الجريمة كغيرها من الجرائم تقوم بتوفر كل من ركنها المادي (أولا) و ركنها المعنوي (ثانيا)، كما أقر لها المشرع عقوبة (ثالثا).

أولا: الركن المادي لجريمة معالجة معطيات شخصية للمستهلك بدون تصريح أو ترخيص

يتحقق الركن المادي لهذه الجريمة حسب المادة 56 السابق ذكرها بمجرد **إنجاز** أو **الأمر** بإنجاز معالجة لبيانات إلكترونية شخصية دون تصريح أو الحصول على ترخيص من الجهة المختصة حتى و إن لم يترتب على ذلك أي نتيجة إجرامية[4]، كما يتحقق الركن المادي أيضا عند مواصلة المعالجة بعد سحبهما. و سنحاول تبيان كل سلوك على النحو التالي:

---

[1] – هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، مصر، 2005، ص 37.

[2] – هبة حسين محمد زايد، المرجع السابق، ص 49 .(فرنسية)

[3] – المادة 56 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة بياناتهم الشخصية " يعاقب بالحبس ...كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون".

[4] – هروال هبة نبيلة، جرائم الأنترنت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2014، ص 281.

1- إنجاز أو الأمر بإنجاز معالجة معطيات ذات طابع شخصي دون تقديم تصريح أو الحصول على ترخيص:

و يتعلق الأمر هنا بإنجاز أو الأمر بإنجاز عملية أو أكثر من عمليات المعالجة على المعطيات ذات الطابع الشخصي، دون تقديم تصريح لسلطة الوطنية، أو تلقي ترخيصا منها، إذ ألزم المشرع كل مسؤول عن معالجة معطيات ذات طابع شخصي أن يقدم تصريح بذلك أو الحصول على إذن من طرف السلطة الوطنية لحماية المعطيات الشخصية[1]، و عليه فإن السلوك المجرم في هذه الصورة يتمثل في عدم تقديم تصريح للسلطة الوطنية أو عدم توفره على ترخيص منها عند المعالجة . و سنحاول تحديد كل منها على النحو التالي:

أ-عدم تقديم التصريح:

تخضع كل معالجة للمعطيات ذات الطابع الشخصي إلى تصريح مسبق يقدمه المسؤول عن المعالجة أو ممثله للسلطة الوطنية، و ذلك قبل كل معالجة آلية كلية أو جزئية أو مجموع المعالجات التي لها غاية واحدة أو غايات مرتبطة، و الذي يتضمن التزاما بإجراء المعالجة طبقا لمقتضيات القانون[2]. و تتمثل الغاية من التصريح المسبق في تكمين السلطة الوطنية من ممارسة مهامها التي يخولها لها القانون من أجل مراقبة و التحقق من كل معالجة للمعطيات الشخصية.

و الجدير بالذكر أن المشرع الجزائري ميز بين ثلاث أنواع من التصريحات المسبقة التي يقدم المسؤول عن المعالجة الآلية الكلية أو الجزئية أو مجموع المعالجات التي لها غاية واحدة أو غايات مرتبطة قبل معالجة المعطيات الشخصية و هي:

[1] – انظر المادة 12 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – انظر الفقرة الأولى و الثانية من المادة 13 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

-**التصريح العادي:** و هو النوع الذي يشكل القاعدة و الذي يشمل مجموعة من البيانات الإلزامية المنصوص عليها في المادة 14 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1].

-**التصريح البسيط** : و لقد تطرقت لهذا التصريح المادة 15 من قانون 18-07 سابق الذكر، و هو يتعلق بمجموعة من المعالجات التي لا تلحق ضررا بحقوق و حريات الأشخاص، و ذلك بالنظر إلى المعطيات التي ستتم معالجتها، و لم يحدد المشرع فئات هذه المعالجة و إنما أسندت مهمة تحديد قائمتها إلى السلطة الوطنية[2].

و يشمل هذا النوع من التصريحات سوى بعض البيانات فقط من بين تلك المنصوص عليها في المادة 14 سابقة الذكر (اسم و عنوان المسؤول عن المعالجة، طبيعة المعالجة و خصائصها و الغرض منها، وصف فئة و فئات الأشخاص المعنيين، المرسل إليهم أو فئات المرسل إليهم، طبيعة المعطيات المراد إرسالها إلى الخارج، مدة حفظ البيانات)[3]. و تندرج في إطار هذه المعالجات مختلف المعالجات الآلية في إطار المواقع الإلكترونية.

---

[1] – حددت المادة 14 من قانون 18-07 البيانات التي يتضمنها التصريح و هيا: (1-إسم و عنوان المسؤول عن المعالجة و عند الاقتضاء اسم و عنوان ممثله، 2-طبيعة المعالجة و خصائصها و الغرض أو الأغراض المقصودة منها،3- وصف فئة أو فئات الأشخاص المعنيين و المعطيات أو فئات المعطيات ذات الطابع الشخصي المتعلقة بهم،4- المرسل إليهم أو فئات المرسل إليهم الذين قد توصل إليهم المعطيات، 5-طبيعة المعطيات المعتزم إرسالها إلى دول أجنبية، 6-مدة حفظ المعطيات،7- المصلحة التي يمكن الشخص المعني عند الاقتضاء، أن يمارس لديها الحقوق المخولة له بمقتضى أحكام هذا القانون و كذلك الإجراءات المتخذة لتسهيل ممارسة هذه الحقوق، 8-وصف عام يمكن من تقييم أولي لمدى ملائمة التدابير المتخذة من اجل ضمان سرية و أمن المعالجة، 9-الرابط البيني أو جميع أشكال التقريب الأخرى بين المعطيات، و كذا التنازل عنها للغير أو معالجتها من الباطن، تحت أي شكل من الأشكال، سواء مجانا أو بمقابل.

[2] – أنظر المادة 15 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – يشتمل التصريح البسيط إلا على البيانات المنصوص عليها في 1، 2،3،4،5،6 من المادة 14. **أنظر الفقرة الأولى من المادة 15 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.**

غير أنه هناك بعض الحالات التي لا يكون فيها تقديم التصريح إلى الهيئة الوطنية إلزاميا، و يتعلق الأمر بالمعالجات التي يكون الغرض منها فقط مسك سجل مفتوح ليطلع عليه الجمهور أو التي يثبت فيها الشخص مصلحة مشروعة، غير أنه في هذه الحالة يتم كشف عن هوية المسؤول عن المعالجة و تبليغها للسلطة الوطنية، و أن يوصل إلى كل شخص قدم طلبا بذلك المعلومات المتعلقة بالغاية من المعالجة و المرسل إليهم[1].

و هكذا فإن إنجاز معالجة آلية كليا أو جزئيا أو مجموع المعالجات التي لها غاية واحدة أو غايات مرتبطة للمعطيات الشخصية دون تقديم تصريح مسبق مهما كان نوعه إلى الهيئة الوطنية يشكل جريمة المعالجة دون تصريح[2].

ب-عدم الحصول على ترخيص:

اشترط المشرع ضرورة الحصول على ترخيص مسبق تسلمه السلطة الوطنية للقيام بالمعالجة في مجموعة من الحالات المحددة على سبيل الحصر[3]، لحماية المعطيات ذات الطابع الشخصي بناء على طلب المسؤول عن المعالجة[4]، و تتمثل هذه الحالات التي تشترط حصول المسؤول على المعالجة على ترخيص مسبق في:

---

[1] – أنظر المادة 16 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة بياناتهم الشخصية..

[2] – و قد قضت محكمة النقض الفرنسية في قرار لها بتاريخ 30 أكتوبر 2001، بان محكمة الاستئناف كانت على صواب حينما قضت بتوافر جميع أركان الجريمة المنصوص عليها في المادة 16/226 من قانون العقوبات. فيما يخص غياب التصريح ، و ذلك بعدما استخلصت من نتائج تحقيقها بان المتهمين استعملوا نظام للمعالجة الآلية للمعلومات الإسمية بدون إجراء أي تصريح مسبق إلى اللجنة الوطنية للمعلومات و الحريات كما هو منصوص عليه في المادة 16 من قانون 6 يناير 1978. **انظر إبراهيم عيد نايل، المرجع السابق، ص 81.**

[3] – أنظر المادة 1/17 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] – يجب أن يتضمن طلب الترخيص المعلومات المنصوص عليها في المادة 14 من هذا القانون، و تتخذ السلطة الوطنية قرارها بقول الطلب و منح الإذن في أجل شهرين (02) من تاريخ إخطارها، كما يمكن أن تمدد هذه المدة إلى شهرين آخرين بقرار مسبب من طرف رئيسها، و يعتبر عدم رد السلطة الوطنية في الآجال المذكورة رفضا للطلب. **أنظر المادة 20 من قانون 18-07. المتعلق بحماية الأشخاص الطبعيين في مجال معالجة بياناتهم الشخصية.**

-إذا تبين للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي عند دراسة التصريح المقدم لها، أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على احترام و حماية الحياة الخاصة و الحريات و الحقوق الأساسية للأشخاص[1].

-المعالجة التي تخص المعطيات الحساسة[2]: كقاعدة عامة منع المشرع معالجة المعطيات الحساسة[3]، غير أنه أجاز الترخيص بمعالجتها إذا تعلق الأمر بالمصلحة العامة، شرط أن تكون ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة، أو إذا تعلق الأمر بمعالجة معطيات حساسة لشخص معين بناء على موافقته الصريحة[4].

-المعالجة التي تهدف إلى الربط البيني لملفات[5] تابعة لشخص أو عدة أشخاص معنوية يسيرون مرفقا عموميا، و ذلك عندما تكون غايات المصلحة العامة لديهم مختلفة مرتبطة بالمنفعة العامة، أو الربط البيني لملفات تابعة لأشخاص طبيعية، الذي يتم لأغراض مختلفة[6].

---

[1] – أنظر المادة 1/17 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – المعطيات الحساسة هيا كل معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية. **أنظر المادة 3 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.**

[3] – الفقرة الأولى من المادة 18 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] – الفقرة الثانية من المادة 18 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[5] – الربط البيني هو أي شكل من أشكال المعالجة التي تتمثل في إقامة ترابط بين معطيات معالجة لغاية محددة مع معطيات أخرى يمسكها مسؤول أو مسؤولون آخرون عن المعالجة أو يمسكها نفس المسؤول لنفس الغرض أو الأغراض الأخرى. **أنظر المادة 03 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة بياناتهم الشخصية..**

[6] – أنظر المادة 19 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الطابع الشخصي.

-المعالجة التي تهدف إلى تحقيق مصلحة عامة للبحث أو الدراسات أو التقييم في مجال الصحة، في إطار احترام المبادئ المنصوص عليها في هذا القانون، و بالنظر إلى المصلحة العامة التي تهدف إلى تحقيقها الدراسة أو البحث أو التقييم[1].

و عليه فإن كل معالجة تهم الحالات السالفة الذكر يتم إجراؤها، دون الحصول على إذن مسبق من طرف السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، تعد معالجة بدون ترخيص معاقب عليها بموجب المادة 56 من قانون 18-07 سابق الذكر.

2- مواصلة المعالجة بعد سحب التصريح أو الترخيص:

يتحقق الركن المادي في هذه الصورة عند قيام المسؤول عن المعالجة بمواصلة نشاط معالجة المعطيات ذات الطابع الشخصي رغم سحب وصل التصريح أو الترخيص[2]. و تعد السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي الجهة الوحيدة المختصة بسحب وصل التصريح أو الترخيص الممنوح من قبلها، باعتبارها الجهة التي تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي للقانون، و ضمان عدم انطواء استعمال تكنولوجيات الإعلام و الاتصال على أي أخطار تجاه حقوق الأشخاص و الحريات العامة و الحياة الخاصة[3].

أما عن حالات سحب هذا الوصل أو الترخيص، فقد جعلها المشرع عند مخالفة المسؤول عن المعالجة لأحكام قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي [4]، أو إذا تبين بعد إجراء المعالجة

---

[1] - أنظر المادة 21 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] - أنظر المادة 2/56 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] - أنظر المادة 1/25 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] - المادة 1/46 من القانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " تتخذ السلطة الوطنية في حق المسؤول عن المعالجة في حالة خرق لأحكام هذا القانون الإجراءات

موضوع التصريح أو الترخيص أنها تمس بالأمن الوطني أو أنها منافية للأخلاق أو الآداب العامة[1]. و يلاحظ أن السلطة الوطنية تملك إمكانات واسعة لممارسة صلاحية سحب وصل التصريح أو الترخيص، و ذلك أمام اتساع و عدم دقة المجالات التي تمارس فيها هذه الصلاحية.

و في كافة الأحوال فإن كل مسؤول عن معالجة المعطيات ذات الطابع الشخصي تم سحب وصل التصريح أو الترخيص الذي يخوله القيام بهذه المعالجة، و يواصل القيام بأنشطة المعالجة المعنية بهذا السحب، يكون قد ارتكب جريمة المعالجة بدون تصريح أو ترخيص وفقا للمادة 56 من نفس القانون.

ثانيا: الركن المعنوي لجريمة معالجة معطيات شخصية دون تصريح أو ترخيص

تعد جريمة المعالجة بدون تصريح أو ترخيص من الجرائم العمدية حيث يلزم أن يكون الجاني على علم بكون الأفعال التي يأتيها تشكل معالجة لمعطيات ذات طابع شخصي، و أنه لم يقدم تصريحا لهذا النشاط لسلطة الوطنية أو لم يتحصل منها على ترخيص، أو أنه يواصل نشاط المعالجة رغم سحب وصل التصريح أو الترخيص، و إضافة إلى العلم بالأفعال التي يأتيها الجاني، فإن القصد يستلزم أن يكون لدى الجاني إرادة لارتكاب هذه الأفعال.

و نشر في الأخير أن هذه الجريمة تتحقق بمجرد القصد الجنائي العام فقط، دون القصد الخاص، حيث يعاقب عنها مهما كانت نيته، أو الباعث سواء كان الإضرار المادي بالشخص، أو استغلال معطياته من أجل الإساءة لسمعته، أو كان ذلك لمجرد الفضول و حب الاستطلاع[2].

الإدارية الآتية: الإنذار، الإعذار، السحب المؤقت لمدة لا تتجاوز سنة أو السحب النهائي لوصل التصريح أو الترخيص..."

[1] – أنظر المادة 48 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – إبراهيم عيد نايل، المرجع السابق، ص 91.

ثالثا: العقوبة المقررة لجريمة معالجة معطيات شخصية دون تصريح أو ترخيص

نظرا لخطورة الأفعال التي تحملها هذه الجريمة على حقوق و حريات الأشخاص بما فيهم المستهلك الإلكتروني من جراء معالجة معطياتهم الشخصية دون تصريح أو ترخيص، فإن المشرع الجزائري أفرد لها عقوبة مشددة في المادة 56 من قانون 18-07 بالنظر إلى بقية الأفعال الجريمة الأخرى، حيث أقر لها عقوبة سالبة للحرية تتمثل في الحبس من سنتين (2) إلى خمس (5) سنوات و غرامة مالية تتراوح بين 200.000دج و 500.000دج أو بإحدى هاتين العقوبتين فقط.

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[1]، فتكون عقوبة الشخص المعنوي الغرامة من (500.000دج) إلى (2.500.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[2]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[3]، أو

[1] – أنظر المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – أنظر المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[1].

الفقرة الثانية: جريمة التعامل في معطيات حساسة دون موافقة المستهلك الإلكتروني أو تكليف

تقوم هذه الجريمة حسب نص المادة 57 و 68 من قانون 18-07 بمعالجة المسؤول عن المعالجة لمعطيات حساسة دون موافقة الشخص المعني-المستهلك الإلكتروني- أو لمعطيات ذات طابع شخصي متعلقة بمخالفات أو إدانات أو تدابير أمن من غير الرخص لهم قانونا. و سنحاول تبيان كل من الركن المادي (أولا) و المعنوي لهذه الجريمة (ثانيا) و العقوبة المقررة لها (ثالثا)

أولا: الركن المادي لجريمة التعامل في معطيات حساسة دون موافقة الشخص المستهلك الإلكتروني أو تكليف

يتحقق الركن المادي لجريمة التعامل في معطيات حساسة دون موافقة الشخص المعني -المستهلك الإلكتروني- أو تكليفه في صورتين هما: إما معالجة معطيات حساسة دون موافقة الشخص المعني المنصوص عليها في المادة 57 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، أو وضع أو حفظ معطيات شخصية متعلقة بمخالفات أو إدانات أو تدابير أمن من غير المخول لهم قانونا ذلك وفقا للمادة 68 من نفس القانون.

1-معالجة معطيات حساسة دون موافقة المستهلك الإلكتروني:

اشترطت المادة 57 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي لقيام الركن المادي في هذه الصورة أن تجري معالجة معطيات حساسة بدون الموافقة الصريحة لشخص المعني -المستهلك

[1] - أنظر المادة 71 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي

الإلكتروني–[1]، و لقد حددت المادة 03 من نفس القانون هذه المعطيات الحساسة بأنها " معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية".

و يأتي تجريم هذا النوع من المعطيات (المعطيات الحساسة) ذات الطابع الشخصي بدون موافقة الشخص المعني –المستهلك الإلكتروني– انسجاما مع الغاية الخاصة التي أعطاها المشرع الجزائري للأشخاص المعنيين بهذا النوع من المعطيات، لكونها ترتبط بجوانب ذات أهمية كبيرة للحياة الخاصة للأشخاص، حيث تضم معطيات يمكن أن تؤدي إلى أشكال متنوعة من التمييز، كما يمكن أن تؤثر على سرية بعض جوانب حياتهم الخاصة[2]، و تتأكد هذه الغاية من استلزام المشرع ضرورة خضوع معالجة المعطيات الحساسة إلى إذن يمنح بموجب القانون الذي يحدد شروطها، و يتم منح الإذن المذكور بناء على رضى الصريح للشخص المعني.

و لا يلزم في المعطيات الحساسة أن ترتبط بشكل مباشر بالشخص المعني – المستهلك الإلكتروني–، بل يدخل فيها كذلك تلك التي ترتبط به بشكل غير مباشر. كما يمكن أن تتعلق المعالجة بجانب واحد من الجوانب المذكورة ، فانه يمكن أن ترتبط بجانبين أو اكثر[3].

و يستثنى من نطاق ارتكاب هذه الجريمة بعض المعالجات التي تخضع لها المعطيات الحساسة، حيث يمكن للمسؤول عن المعالجة إجراء معالجات للمعطيات

---

[1] – المادة 57 من قانون 18–07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة من 200.000 إلى 500.000، كل من قام دون الموافقة الصريحة للشخص المعني و في غير الحالات المنصوص عليها في هذا القانون بمعالجة المعطيات الحساسة".

[2] – André lucas. Op cit. p 140.

[3] – قضت محكمة النقض الفرنسية في قرار لها بتاريخ 4 مارس 1997، أن عناصر الجريمة تعد متوافرة بالقيام بدون موافقة صريحة للمعني، بالتخزين الآلي لمعلومات إسمية تظهر على وجه الخصوص، الآراء السياسية ، الفلسفية أو الدينية. . **أنظر .Yves Mayausd.code penal. 14éme éd. Dalloz. 2009.p 683**

الحساسة و لو في غياب هذه الموافقة، و هو ما أكدته المادة 57 من قانون 18-17 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " ... كل من قام دون الموافقة الصريحة للشخص المعني **و في غير الحالات المنصوص عليها في هذا القانون**، بمعالجة المعطيات الحساسة"، و تشمل هذه الحالات ما نصت عليه المادة السابعة في فقرتها الخامسة من هذا القانون[1].

فإجراء المعالجة في مختلف هذه الحالات دون الحصول على الموافقة المسبقة للشخص المعني –المستهلك الإلكتروني–، لا يشكل جريمة و لا يخضع القائم بها للعقوبة المنصوص عليها في المادة 57 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

2-وضع أو حفظ في الذاكرة الآلية معطيات شخصية متعلقة بمخالفات أو إدانات أو تدابير امن من غير المخول لهم قانونا:

يتحقق السلوك الإجرامي في هذه الصورة وفقا للمادة 68 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي عند قيام المسؤول عن المعالجة أو الغير بوضع أو حفظ في الذاكرة الآلية معطيات ذات طابع شخصي متعلقة بالجنايات أو الجنح أو المخالفات المرتكبة من قبل شخص معين، و بالإدانات الصادرة بشأنها من طرف القضاء و كذلك تدابير الأمن المتخذة من قبله، فكل وضع أو حفظ في الذاكرة الآلية لهذه المعطيات تعرض صاحبها للعقوبة[2].

---

[1] – لمادة 5/7 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " غير أن موافقة الشخص المعني لا تكون واجبة إذا كانت المعالجة ضرورية في:

– لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة.

–لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه.

–للحفاظ على المصالح الحيوية للشخص المعني.

–لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة الوطنية.

–لتحقيق مصلحة مشروعة من قبل المسؤول على المعالجة أو المرسل إليه..."

[2] – المادة 68 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة مالية من 60.000 إلى 300.000 كل من قام

إذ أن معالجة هذا النوع من المعطيات يعد ممنوعا، و لا تختص بمعالجته إلا من قبل السلطات القضائية و السلطات العمومية و الأشخاص المعنويين الذين يسيرون مصلحة عمومية، و مساعدي العدالة في إطار اختصاصهم القانوني[1].

فمن غير الجهات المذكورة سابقا، يعد كل وضع أو حفظ في الذاكرة الآلية لمعطيات شخصية تتعلق بمخالفات أو إدانات أو تدابير أمن جريمة معاقب عليها.

و في الأخير فإن كل معالجة للمعطيات الحساسة دون موافقة الشخص المعني – المستهلك الإلكتروني– أو حفظ معطيات متعلقة بمخالفات أو عقوبات أو تدابير أمن من دون الأشخاص المخولين بذلك يؤدي لقيام الركن المادي لجريمة التعامل في معطيات حساسة دون موافقة أو تكليف.

ثانيا: الركن المعنوي لجريمة التعامل في معطيات حساسة دون موافقة المستهلك الإلكتروني أو تكليف

تعد جريمة معالجة المعطيات الحساسة بدون موافقة الشخص المعني –المستهلك الإلكتروني– جريمة عمدية لا تقوم إلا بتوافر القصد العام لدى الجاني و ذلك بعنصريه العلم و الإرادة، حيث يلزم أن يعلم الجاني بأن الأفعال التي يقوم بها تشكل معالجة لمعطيات ذات طابع شخصي، و أن المعطيات التي يعمل على معالجتها تشكل معطيات حساسة، و انه يجري المعالجة المذكورة دون موافقة صريحة من الشخص المعني – المستهلك الإلكتروني–. أما بالنسبة للفعل الآخر، فيلزم أن يعلم الجاني بأنه يقوم بوضع أو حفظ معطيات ذات طابع شخصي تتعلق بمخالفات أو إدانات أو تدابير أمن و هو غير مكلف بذلك قانونا، فضلا عن ذلك يستوجب القصد أن تكون للجاني إرادة للقيام بكل هذه الأفعال من أجل تحقيق نتيجتها.

في غير الحالات المنصوص عليها قانونا، بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن".

[1] – أنظر المادة 10 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ثالثا: العقوبات المقررة لجريمة التعامل في معطيات حساسة دون موافقة المستهلك الإلكتروني أو تكليف

عاقب المشرع الجزائري على جريمة التعامل في معطيات حساسة دون موافقة الشخص –المستهلك الإلكتروني– أو التكليف أو المحاولة[1] بعقوبة أصلية وأخرى تكميلية، تتمثل الأصلية في الحبس أو الغرامة أو هما معا حسب كل فعل من الأفعال المكونة لها، فانطلاقا من المادة 57 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي فإن العقوبة المقررة لكل من قام بمعالجة معطيات حساسة دون موافقة الشخص المعني بالحبس من سنتين (2) إلى خمس سنوات (5) وبغرامة من (200.000 دج) إلى (500.000دج) ، أما من قام بفعل الحفظ في ذاكرة آلية معطيات متعلقة بمخالفات و جرائم و إدانات أو تدابير أمن من غير الأشخاص المكلفين بذلك فتكون العقوبة حسب نص المادة 68 من نفس القانون الحبس من ستة أشهر إلى ثلاث (3) سنوات و بغرامة من(60.000دج) إلى (300.000دج).

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[2]، فتكون عقوبة الشخص المعنوي بالنسبة لكل من قام بمعالجة معطيات حساسة دون موافقة الشخص المعني الغرامة من (500.000دج) إلى (2.500.000دج)، أما بالنسبة لفعل الحفظ في ذاكرة

[1] – المادة 73 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب على محاولة ارتكاب إحدى الجنح المنصوص عليها في هذا القانون بنفس العقوبات المقررة للجريمة التامة".

[2] – المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون وفقا للقواعد المنصوص عليها في قانون العقوبات"

آلية معطيات متعلقة بمخالفات و جرائم و إدانات أو تدابير أمن من غير الأشخاص المكلفين بذلك فتكون العقوبة غرامة تتراوح بين (300.000دج) إلى (1.500.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[1]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[2]، أو أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[3].

الفرع الثاني: الجرائم المتعلقة بشكليات الحماية و التعاون مع اللجنة الوطنية

ألزم المشرع الجزائري كل مسؤول عن معالجة المعطيات ذات الطابع الشخصي بضرورة اتخاذ مجموعة من التدابير بهدف حماية هذه المعطيات من المخاطر التي يمكن أن تلحق بها، و عليه فإن كل إغفال أو تقصير في اتخاذها يشكل جريمة معاقب عليها(الفقرة الأولى)، كما أنه من أجل تمكين السلطة الوطنية من ممارسة مهامها، ألزم المشرع المسؤول عن المعالجة بالاستجابة لمختلف الالتزامات التي تتطلب منه للتعاون مع هذه الأخيرة، و كل إخلال بهذه الالتزامات يعرضه للعقوبة (الفقرة الثانية).

---

[1] – المادة 72 من قانون 18-07 " المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي" يصادر محل الجريمة بغرض إعادة تخصيصه أو تدميره في إطار احترام التشريع المفعول.
يتحمل المحكوم عليه مصاريف إعادة التخصيص أو التدمير"

[2] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

[3] – أنظر المادة 71 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

الفقرة الأولى: جريمة عدم اتخاذ تدابير حماية المعطيات الشخصية للمستهلك الإلكتروني

نظرا لما تتميز به المعطيات الشخصية للأشخاص بما فيهم المستهلك الإلكتروني من طابع السرية و الحرص على عدم تداولها من غير المرخص لهم ألزم المشرع المسؤول عن المعالجة بتوفير التدابير اللازمة لحماية سرية و سلامة هذه المعطيات. إذ يهدف المشرع من خلال هذه الالتزامات تأمين نظام المعالجة المعلوماتية للمعطيات الشخصية لدرء خطر الاطلاع عليها من أشخاص غير مخول لهم ذلك. و مخالفة هذا الالتزام يعد جريمة معاقب عليها بموجب المادة 65 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي [1].

و لقيام جريمة عدم اتخاذ تدابير حماية المعطيات الشخصية يجب توافر كل من ركنها المادي (أولا) و ركنها المعنوي (ثانيا)، كما أقر لها المشرع عقوبة تتماشى مع جسامتها (ثالثا).

أولا: الركن المادي لجريمة عدم اتخاذ تدابير حماية المعطيات الشخصية للمستهلك الإلكتروني

يتحقق الركن المادي لجريمة مخالفة تدابير حماية المعطيات عند قيام المسؤول عن المعالجة بمعالجة معطيات شخصية دون اتخاذ تدابير و إجراءات الحماية المنصوص عليها في المادتين 38 و 39 المتعلقة بالإجراءات التقنية و التنظيمية، أو الاحتفاظ بها خارج الآجال القانوني. و سنحاول تحديد كل سلوك على النحو التالي:

1-عدم اتخاذ التدابير و الإجراءات التقنية و التنظيمية:

[1] – المادة 65 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع ساري المفعول، يعاقب بغرامة من 200.000دج إلى 500.000دج المسؤول عن المعالجة الذي يخرق الالتزام المنصوص عليه في المادتين 38 و 39 من هذا القانون".

ألزم المشرع الجزائري عند معالجة المعطيات الشخصية كل مسؤول عن المعالجة و عند الاقتضاء ممثله، و المعالج من الباطن اتخاذ كافة الإجراءات التقنية و التنظيمية المناسبة و الملائمة لتوفير الحماية لها، و ذلك في مواجهة كافة المخاطر التي يمكن أن تهددها، و بصفة خاصة الإتلاف العرضي أو غير المشروع، الضياع العرضي ، التلف أو النشر و الولوج غير المرخص به، و على وجه الخصوص إذا استوجبت المعالجة إرسال معطيات عبر شبكة معينة بما في ذلك شبكة الأنترنت، كما يلزم في هذه الإجراءات أن توفر حماية في مواجهة كافة أوجه المعالجة غير المشروعة[1].

و يلزم في الإجراءات المذكورة أن توفر مستوى ملائما من الحماية على أساس الأخذ بالاعتبار عند اتخاذ هذه الإجراءات مختلف مخاطر المعالجة و طبيعة المعطيات التي تتطلب الحماية من جهة ثانية[2]. ففي الحالة التي تكون فيها المعطيات المعنية تمكن على سبيل المثال من إعادة استعمال بطاقة الائتمان الخاصة بالمستهلك يغير علمه، فإنه يلزم توفير درجة كبيرة من الحماية[3].

فبالنسبة للإجراءات التقنية يمكن استعمال مجموعة من التقنيات مثل الترميز، أو التشفير أو الولوج الشخصي، أو الولوج التسلسلي، أو صيد الفيروسات المعلوماتية أو عرقلة أنظمة تعديل المعلومات، أما فيما يتعلق بالإجراءات التنظيمية، فمن بينها، حماية الولوج إلى بعض الأماكن، أو صيانة المعدات و برامج الحاسوب، أو إعداد معدات

---

[1] – المادة 1/38 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يجب على المسؤول عن المعالجة وضع التدابير التقنية و التنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين، و كذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة.

[2] – المادة 2/38 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي "و يجب أن تتضمن هذه التدابير مستوى ملائما من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة و طبيعة المعطيات الواجب حمايتها".

[3] – Thibault Verbiest et Etienne Wery. Le droit de l'internet et de la société de l'informatique. Droit européen. Belge et francais. Lacier. Bruxelles. Belgique. 2001. P 414.

احتياطية من أجل تعويض تلك التي يلحقها الضرر خلال المعالجة. و يلزم على القاضي اللجوء إلى الخبرة الفنية قبل البت في كل نزاع يتعلق بمدى ملائمة الإجراءات التقنية و التنظيمية لحماية المعطيات الشخصية بالنظر إلى مخاطر المعالجة و طبيعة المعلومات[1].

كما يتحمل المسؤول عن المعالجة بالتزام سلامة المعطيات حتى و لو لم يقم بالمعالجة شخصيا، ففي هذه الحالة التي تجري فيها المعالجة لحساب المسؤول عن المعالجة، فإن هذا الأخير يلزمه اختيار معالج من الباطن[2] يقدم ضمانات كافية لإجراءات السلامة المتعلقة بالمعالجة التي يلزم القيام بها، كما يتحمل مسؤولية ضمان هذه الإجراءات[3].

و عليه فإن القيام بمعالجة المعطيات ذات الطابع الشخصي دون اتخاذ الإجراءات التقنية و التنظيمية السالف الذكر يعتبر مكونا لجريمة مخالفة تدابير حماية المعطيات الشخصية للمستهلك[4].

---

[1] – André lucas. Jean Deveze et Jean Freyssinet. Droit de l'informatique et de l'internet. Op cit. p 164.

[2] – تنظم عملية المعالجة من الباطن بموجب عقد أو سند قانوني يربط المعالج من الباطن بالمسؤول عن المعالجة، و ينص خصوصا على ألا يتصرف المعالج من الباطن إلا بناء على تعليمات المسؤول عن المعالجة و على تقيده بالالتزامات المنصوص عليها في المادة 38 . **أنظر المادة 2/38 من قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة بياناتهم الشخصية.**

[3] – المادة 1/39 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " عندما تجري المعالجة لحساب المسؤول عن المعالجة، يجب على هذا الأخير اختيار معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية و التنظيمية للمعالجات الواجب القيام بها و يسهر على احترامها".

[4] – في هذا الإطار اعتبرت محكمة النقض الفرنسية في قرارها الصادر بتاريخ 30 أكتوبر 2001، بأن محكمة الاستئناف كانت صائبة عند تقريرها بتوافر جميع العناصر المكونة للجريمة المنصوص عليها في المادة 17/226 من قانون العقوبات-جريمة عدم اتخاذ التدابير الحمائية- بعدما اثبت تان المتهمين استعملوا نظاما للمعالجة الآلية للمعلومات الاسمية بدون اتخاذ كافة الاحتياطات اللازمة لمنع الاطلاع علي المعلومات الطبية بالنسبة للموظفين

2-حفظ المعطيات الشخصية لمدة تزيد عن المدة القانونية:

يتحقق السلوك المجرم في هذه الصورة عندما يحتفظ المسؤول عن المعالجة المعطيات الشخصية فوق المدة المطلوبة للحفظ ، إذ يقتضي هذا أن لا يتم حفظ المعطيات على وجه نهائي و دائم لمعطيات شخصية ، حيث يتوجب أن تحدد مدة الحفظ بشكل مؤقت على ضوء الغايات المرتبطة بكل ملف يتم تكوينه لغايات معينة. و تحدد هذه المدة من خلال التصريح أو الترخيص المقدم من طرف السلطة الوطنية لحماية المعطيات الشخصية[1]،

إذ أن عدم الاحتفاظ النهائي للمعطيات الشخصية يحتل أهمية كبيرة في نطاق شبكة الإنترنت، حيث تكون فيها التكلفة الاقتصادية لحفظ المعطيات غير ذات أهمية، مما يسهل مدة الحفظ غير محددة المدة، و المعمول به عند تجميع المعطيات الشخصية في العلاقات التعاقدية الإلكترونية يجب أن لا تتجاوز مدة الاحتفاظ بهذه المعلومات مدة وجود أو تنفيذ العقد[2].

و من ثم فإن كل حفظ للمعطيات الشخصية للمستهلك الإلكتروني يتجاوز المدة المنصوص عليها قانونا أو المنصوص عليها التصريح أو الترخيص الممنوح من طرف السلطة الوطنية، يعتبر حفظا غير مشروع للمعطيات الشخصية و مخالف لتدابير حماية هذه المعطيات وفقا للمادة 65 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الإداريين غير المرخص لهم، و لا سيما بدون أن يكون المتهمين بشكل مستقل مذكرات إدارية، تأمن الإعلام الكافي و بشكل تام وظيفة النظام. **انظر إبراهيم عيد نايل، المرجع السابق، ص 98.**

[1] – أنظر المادة 2/65 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – hibault Verbiest et Etienne Wery. Op cit. p 445.

ثانيا: الركن المعنوي لجريمة عدم اتخاذ تدابير حماية المعطيات الشخصية للمستهلك الإلكتروني

يقوم الركن المعنوي لهذه الجريمة بتوفر القصد الجنائي العام بعنصريه العلم و الإرادة، أي أن يعلم المسؤول عن معالجة للبيانات الشخصية أن فعله يشكل جريمة عدم اتخاذ تدابير حماية المعطيات الشخصية، و أن تتجه إرادته نحو تحقيق ذلك الفعل المجرم[1].

كما يمكن تصور قيام الركن المعنوي لهذه الجريمة عن طريق مجرد الخطأ، إذ اعتبر الفقه الفرنسي بأن هذه الجريمة يمكن قبول ارتكابها عن طريق الإهمال أو عدم التبصير[2].

و هكذا فإن جريمة عدم اتخاذ تدابير حماية المعطيات الشخصية يمكن أن تقوم عن طريق العمد، أي بعلم الجاني بأنه يعالج معطيات ذات طابع شخصي دون أن يكون قد أنجز تدابير حماية سرية و سلامة المعطيات كما يلزمه بذلك القانون، و كذلك بإرادة تحقيق هذا الفعل، أما الجريمة عن طريق مجرد الخطأ، فيتمثل في إجراء معالجة للمعطيات الشخصية دون اتخاذ كل الإجراءات اللازمة لحماية سلامة المعطيات، سواء بإهمال هذه الإجراءات أو عدم التبصر بشأنها[3].

ثالثا: العقوبة المقررة لجريمة عدم اتخاذ تدابير حماية المعطيات الشخصية للمستهلك الإلكتروني

عاقب المشرع الجزائري في المادة 65 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي على جريمة عدم

---

[1] – هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2005، ص 42.

[2] – إبراهيم عيد نايل، المرجع السابق، ص 100.

[3] – مدحت رمضان عبد الحليم، جرائم الاعتداء على الأشخاص و الأنترنت، دار النهضة العربية، القاهرة، 2000،ص 101.

اتخاذ إجراءات حماية المعطيات الشخصية بعقوبة مالية فقط، تتراوح بين 200.000دج و 500.000 دج.

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر من قانون العقوبات، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[1]، فتكون عقوبة الشخص المعنوي الغرامة من (500.000دج) إلى (2.500.000دج).

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[2]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[3]، أو أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[4].

[1] – أنظر المادة 70 من قانون رقم 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – أنظر المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة من قانون العقوبات.

[4] – أنظر المادة 71 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

الفقرة الثانية: جريمة عدم التعاون مع السلطة الوطنية

ألزم المشرع المسؤول عن المعالجة التعاون مع السلطة الوطنية و ذلك من خلال اتخاذ بعض الإجراءات تهدف إلى حماية المعطيات الشخصية و تسهيل أداء مهامها في مراقبة المعالجة على هذه المعطيات و ضرورة إعلامها بكل اعتداء عليها، و عدم احترام هذه الالتزامات يؤدي لقيام المسؤولية الجزائية للمسؤول عن المعالجة.

و تتحقق هذه الجريمة كغيرها من الجرائم بتوافر ركنها المادي (أولا) و بتوفر قصد جنائي لمرتكبها(ثانيا)، كما أقر لها المشرع عقوبة تتناسب مع جسامتها(ثالثا).

أولا: الركن المادي لجريمة عدم التعاون مع السلطة الوطنية.

يتحقق الركن المادي لهذه الجريمة بإتيان أحد السلوكين ، يتمثل الأول في عرقة عمل السلطة الوطنية المنصوص عليه في المادة 61 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1]، أما الثاني فهو عدم إعلام السلطة الوطنية عن كل انهاك للمعطيات الشخصية المنصوص عليه في المادة 66 من نفس القانون[2]. و سنحاول تحديد مل سلوك على النحو التالي:

1- عرقة عمل السلطة الوطنية:

كلف المشرع الجزائري السلطة الوطنية بالسهر على مطابقة معالجة المعطيات الشخصية لأحكام القانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي و ضمان عدم انطواء استعمال تكنولوجيات الإعلام و

[1] – المادة 61 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب بالحبس ...كل من عرقل عمل السلطة الوطنية ..."

[2] – المادة 66 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي " يعاقب بالحبس ...مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية و الشخص المعني عن كل انتهاك للمعطيات الشخصية خلا لأحكام المادة 43 من هذا القانون".

الاتصال على أخطار تجاه حقوق الأشخاص و الحريات العامة و الحياة الخاصة[1]، لذلك وجب تتحقق عرقة السلطة الوطنية عن أداء مهامها عند قيام المسؤول عن المعالجة أو المعالج من الباطن بأحد الأفعال التالية:

أ-الاعتراض على إجراء عملية التحقيق في عين المكان:

يتحقق الاعتراض بإتيان فعل يحول دون قيام السلطة الوطنية بمهمة الرقابة، سواء عن طريق القيام بأفعال إيجابية، أو عن طريق مجرد الامتناع عن القيام بفعل معين.

و ينصب الاعتراض على مجموعة مهام المراقبة التي تختص بها السلطة الوطنية، و التي تخول لها مراقبة كافة الأنشطة المرتبطة بمعالجة المعطيات ذات الطابع الشخصي التي منها لها قانون 18-07، و من بين هذه المهام ما نصت عليه المادة 35 من نفس القانون، حيث يمكن للسلطة الوطنية بناء على طلب التصحيح المودع لديها من قبل المعني بالأمر بعد رفض طلبه أو عدم الاستجابة له خلال الأجل من قبل المسؤول عن المعالجة القيام بتكليف أحد أعضائها من أجل إجراء كل لتحقيقات المفيدة و إدخال التصحيحات اللازمة في أقرب الآجال.

ب-رفض تزويد أعضاء السلطة الوطنية بالمعلومات و الوثائق الضرورية أو إخفاءها أو إزالتها:

يتضمن هذا السلوك عدم الاستجابة للالتزام القانوني بضرورة تمكين السلطة الوطنية من جميع الوثائق أو المعلومات التي تطلبها هذه الأخيرة، و يتجسد هذا الرفض في عدم القيام بإرسال هذه الوثائق أو المعلومات ، مهما كانت طبيعة الوثائق و المعلومات و كيفما كانت دعائمها، كما جعل المشرع إخفاء و إزالة الوثائق و المعلومات من قبيل أفعال الإعاقة، و عدم تقديم المساعدة للسلطة الوطنية.

[1] – أنظر المادة 25 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ج-إرسال معلومات غير مطابقة أو تقديمها بشكل غير واضح:

يتضمن هذا العنصر قيام أي شخص يخضع في نشاط معالجة المعطيات ذات الطابع الشخصي لرقابة السلطة الوطنية، و قيامه بإرسال معلومات تحتوي على أخطاء عمدية أو مغلطة، و ذلك وقت تقديم طلب إرسالها في الآجال و طبقا لكيفيات محددة من قبلها، أو إرسال معلومات لمحتوى تسجيلات غير واضحة.

2-عدم إعلام السلطة الوطنية بكل انتهاك للمعطيات الشخصية.

ألزم المشرع من خلال نص المادة 43 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي مقدم الخدمات[1] بضرورة إعلام السلطة الوطنية على الفور و الشخص المعني إذا أدت معالجة المعطيات الشخصية في شبكات الاتصال الإلكترونية المفتوحة للجمهور إلى إتلاف أو ضياع أو إفشاء أو الولوج غير المصرح به لهذه المعطيات، مما يشكل مساسا بحياتهم الخاصة[2].

و عليه فإن عدم إعلام المسؤول عن المعالجة السلطة الوطنية و الشخص المعنوي عن كل مساس بالمعطيات الشخصية محل المعالجة في الشبكات المفتوحة يعد جريمة معاقب عليها قانونا وفقا للمادة 66 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

---

[1] – مقدم الخدمات هم كل كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو أنظمة الاتصال، أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة لفائدة خدمة الاتصال المذكورة أو للمستعملين. **أنظر المادة 03 من قانون 18-07 . المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة بياناتهم الشخصية.**

[2] – المادة 43 من قانون 18-07 المتعلق بحماية المعطيات الشخصية " إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الاتصال الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، يعلم مقدم الخدمات فورا السلطة الوطنية و الشخص المعني، إذ أدى ذلك إلى المساس بحياته الخاصة..."

ثانيا: الركن المعنوي لجريمة عدم التعاون مع السلطة الوطنية

يتضح من خلال المادتين 61 و 66 من قانون 18-07 المتعلق بحماية المعطيات الشخصية أن الركن المعنوي لجريمة عدم التعاون مع السلطة الوطنية، لا يتحقق إلا عن طريق القصد، و يظهر ذلك من طبيعة الأعال المعاقب عنها، و التي لا يمكن تصور ارتكابها عن طريق الخطأ، حيث يلزم أن يكون لدى الجاني القصد العام لارتكابها، و ذلك من خلال علمه بكون الأفعال السالف ذكرها التي يرتكبها تعد عرقلة لممارسة السلطة الوطنية لمهامها في الرقابة، و عدم إعلام هذه الأخيرة بكل انتهاك للمعطيات الشخصية من طرف مقدم الخدمات، بالإضافة إلى ذلك يلزم أن تتجه إرادة الجاني إلى القيام بهذه الأفعال.

ثالثا: العقوبة المقررة لجريمة عدم التعاون مع السلطة الوطنية

عاقب المشرع الجزائري على هذه الجريمة بعقوبة أصلية و أخرى تكميلية، تتمثل العقوبات الأصلية حسب كل فعل على حدى ، فبالنسبة لفعل عرقلة عمل السلطة الوطنية فان العقوبة حسب المادة 61 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي هي الحبس من ستة أشهر إلى سنتين و بغرامة من 60.000دج إلى 200.000دج أو بإحدى هاتين العقوبتين، أما بالنسبة لفعل عدم إعلام مقدم الخدمة السلطة الوطنية فقد قرر لها المادة 66 عقوبة الحبس من سنة إلى ثلاث سنوات و غرامة من 100.000دج إلى 300.000دج أو بإحدى هاتين العقوبتين فقط.

أما الشخص المعنوي فإن العقوبة المقررة له تكون وفقا للقواعد العامة المقررة في قانون العقوبات و المنصوص عليها وفقا للمادة 18 مكرر، إذ تقدر الغرامة بمضاعفة من واحد إلى خمس الحد الأقصى للغرامة المقرر للشخص الطبيعي[1].

[1] – أنظر المادة 70 من قانون رقم 18-07 ا المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

بالإضافة إلى العقوبات الأصلية نص المشرع على عقوبات تكميلية منها الإلزامية و الجوازية، إذ ألزم القاضي بمصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة الجاني[1]، كما أجاز المشرع للقاضي أن يحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات كالتوقيف عن النشاط أو غلق المؤسسة...إلخ[2]، أو أن يأمر بمسح كل أو جزء من المعطيات الشخصية التي هيا محل معالجة و التي نتج عنها ارتكاب الجريمة[3].

[1] – أنظر المادة 72 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] – العقوبات التكميلية المقررة للشخص الطبيعي نصت عليها المادة 09 من قانون العقوبات، أما العقوبات التكميلية المقررة للشخص المعنوي فقد نصت عليها المادة 18 مكرر من قانون العقوبات.

[3] – المادة 71 من قانون 18-07 المتعلق بحماية الأشخاص الطبعيين في معالجة المعطيات ذات الطابع الشخصي.

المبحث الثاني: الحماية الجنائية لتوقيع المستهلك في العاملات الإلكترونية

أفضى التعاقد الإلكتروني إلى ظهور بعض المعوقات، تتمثل أساسا في افتقار المعاملات الإلكترونية إلى عنصر الأمن و السرية إلى حد كبير، نتيجة أعمال القرصنة و التدخلات غير المشروعة التي تتعرض لها، بالإضافة إلى صعوبات إثبات تلك التعاملات و التأكد من محتواها و صدورها عمن نسبت إليه دون تحريف أو تغيير، لذلك ظهرت وسائل حديثة تستجيب لمقتضيات و خصوصية العقود الإلكترونية، فحلت السندات التوقيعات الإلكترونية محل التوقيعات التقليدية، و الذي أصبح أحد الوسائل الأساسية في تنظيم المعاملات الإلكترونية[1].

و تماشيا مع منطق الثقة في التجارة الإلكترونية نظم المشرع الجزائري هذا النوع من التوقيعات من خلال قانون خاص و هو القانون رقم 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين[2]، و الذي من خلاله مجموعة من النصوص تحديد نظامه القانوني، كما أفرد له نصوص حمائية من كل اعتداء عليه لخلق الثقة و الأمان في التعاملات الإلكترونية.

و عليه سنحاول دراسة الحماية الموضوعية لتوقيع المستهلك الإلكتروني من خلال تحديد نظامه القانوني (المطلب الأول)، ثم تبيان صور حماية توقيع المستهلك الإلكتروني (المطلب الثاني).

[1] – إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، لجنة التأليف و التعريب النشر جامعة الكويت، 2003، ص 177.

[2] – القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، المؤرخ في 1 فبراير 2015، جريدة رسمية، عدد 06، الصادرة بتاريخ 10 فبراير 2015.

المطلب الأول: النظام القانوني للتوقيع المستهلك الإلكتروني

نظرا لتطور الذي حدث في مجال المعلوماتية و قطاع الاتصالات و ما لها من انعكاسات على التبادل التجاري الذي يتم عبر شبكة الاتصال الحديثة، لم يعد التوقيع التقليدي ملائما للمعاملات الإلكترونية، لذلك ظهر التوقيع الإلكتروني كبديل عن التوقيع التقليدي ليتوافق و طبيعة المعاملات الإلكترونية.

و نظرا للأهمية التوقيع الإلكتروني في المعاملات الإلكترونية، و الذي بدونه لا يصبح للعقد الإلكتروني أي قيمة قانونية، فإن المشرع الجزائري قد نظم هذا النوع المستحدث من التوقيعات، و الذي حدد نظامه القانوني بدأ بماهيته من مفهوم و شروط (الفرع الأول) و كذلك كيفية المصادقة عليه (الفرع الثاني).

الفرع الأول: ماهية التوقيع الإلكتروني للمستهلك

لقد ظهر التوقيع الإلكتروني كبديل عن التوقيع التقليدي لإثبات صحة عقود التجارة الإلكترونية، بحيث يعتبر ذو فائدة كبيرة، فهو يختصر المسافات و الزمن، فيكفي أن يضع الشخص توقيعه لإتمام معاملاته الإلكترونية دون الحاجة إلى تنقله، كما يستطيع من خلاله الأطراف المتعاملون بنظام التبادل الإلكتروني للبيانات و الرسائل الإلكترونية توثيق معاملاتهم، و التأكد من أن الرسائل قد جاءت من مصدرها دون تعرضه لأي تغيير أثناء عملية التنقل.

و بالنظر لأهمية الدور الذي يؤديه التوقيع الإلكتروني في معاملات التجارة الإلكترونية، و حاجته إلى تبيان ماهيته باعتباره وسيلة لضمان الثقة و الأمان بين المتعاملين إلكترونيا، سعت التشريعات و من بينها المشرع الجزائري بوضع مفهوم له (الفقرة الأولى)، و تحديد الشروط اللازمة لإعطاء التوقيع الإلكتروني فعاليته الكاملة (الفقرة الثانية) .

الفقرة الأولى: مفهوم التوقيع الإلكتروني

نظرا للتطور الهائل في مجال المعلوماتية و اتساع مجال المعاملات الإلكترونية التي تستوجب توقيع الأطراف المتعاقدة إلكترونيا سعت جل التشريعات سواء الدولية أو الداخلية من بينها المشرع الجزائري لوضع مفهوم لهذا النوع الجديد من التوقيعات، و ذلك من خلال تعريفه (أولا) و أشكاله المعمول بها في المعاملات التجارية الإلكترونية (ثانيا).

أولا: تعريف التوقيع الإلكتروني

تباينت العريفات المعطاة للتوقيع الإلكتروني بين تعريفات فقهية و التعريفات المدرجة ضمن القوانين الدولية و القوانين الداخلية للدول، و عليه سنتطرق إلى تعريفه التشريعي و كذلك الفقهي له.

1-التعريف التشريعي للتوقيع الإلكتروني

حظى تعريف التوقيع[1] الإلكتروني باهتمام معظم التشريعات التي تناولت تنظيمه سواء على المستوى الدولي أو الوطني، إذ عرفته قانون "الأونستيرال" النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 بأنه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا يجوز أن تستخدم لتعيين هوية الموقع بالنسبة لرسالة البيانات، و لبيان موافقة الموقع على المعلومات الواردة في الرسالة."[2]

و يلاحظ على هذا التعريف أنه لم يحدد أنواع التوقيع الإلكتروني المستخدم، تاركا للدول إصدار تشريعات خاصة بتحديد أنواعه و كيفية استخدامه للدلالة على شخصية الموقع و التزامه بالمحرر أو المستند الإلكتروني، إضافة إلى أن هذا التعريف قام بتحديد

---

[1] – التوقيع لغة من فعل "وقع" أي بين في إيجاز رأيه بالتابة، و توقيع العقد أو السند و نحوه أن يكتب الكاتب اسمه في ذيله إمضاء له أو إقرارا له، و منها عرفت التوقيعات على أنها " التأشيرات التي تعبر عن رأي صاحبها". **المعجم الوسيط، الطبعة الرابعة، مكتبة الشروق الدولية، القاهرة، 2004، ص 1050.**

[2] – أنظر المادة الثانية من قانون الأنستيرال النموذجي بشأن التوقيع الإلكتروني لسنة 2001. **مشار إليه عند مصطفى هنشور وسيمة، "النظام القانوني للتوقيع الإلكتروني في التشريع الجزائري"، مجلة الحقوق و العلوم الإنسانية ، كلية الحقوق و العلوم السياسية، جامعة مستغانم، العدد 24 المجلد الثاني، ص 409.**

الوظائف التي يقوم بها التوقيع و هي تعيين هوية الموقع و رسالة البيانات، و دلالته على التزامه و موافقته على المعلومات الواردة فيه، و هي نفس الوظائف التي يقوم بها التوقيع العادي.

كما جاء التوجيه الأوربي رقم 93-1999 الصادر بتاريخ 1999/02/13 بشأن التوقيع الإلكتروني بتعريف له، فالتوقيع الإلكترون عبارة عن بيان أو معلومة معالجة إلكترونيا ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرى (رسالة أو محرر) و التي تصلح كوسيلة لتمييز الشخص و تحديد هويته[1].

أما على الصعيد الوطني، لم يصدر المشرع الفرنسي تشريعا خاصا بالمحررات الإلكترونية أو التوقيع الإلكتروني، و إنما عدل قواعد الإثبات في القانون المدني، بما يتلاءم مع الأخذ بهذه الوسائل الحديثة في الإثبات[2]. حيث أصدر المشرع الفرنسي القانون رقم 230 لسنة 2000 المعدل للقانون المدني، و الذي ينص في المادة 4/1316 " ... التوقيع الذي ينتج عن استخدام أي وسيلة مقبولة موثوق بها لتحديد هوية الموقع و تكفل اتصال التوقيع بالعمل أو المستند المرتبط به". فالمشرع الفرنسي لم يعرف التوقيع الإلكتروني، و لم يحدد الطريقة التي يتم بها إنشاء التوقيع الإلكتروني، و لكنه اشترط أمرين، الأمر الأول و هو أن تكون هذه الطريقة موثوقة، أما الثانية فيجب أن تكون الكتابة الإلكترونية تعبر عن الشخص الذي صدرت عنه قانونا، مساويا بذلك بين التوقيع الإلكتروني و الكتابة على الورق في الحجية كدليل إثبات.

و عرف القانون المصري رقم 15 لسنة 2004 التوقيع الإلكتروني بأنه" ما يوضع على محرر إلكتروني و يتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها و يكون له طابع منفرد يسمح بتحديد شخص الموقع و يميزه عن غيره"[3].

---

[1] – أنظر المادة الثانية من التوجيه الأوروبي رقم 93-1999 بشأن التوقيع الإلكتروني، الصدار بتاريخ 1999/02/13.

[2] – د/ آزاد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2016، ص 42.

[3] – المادة 1/ج من قانون رقم 15 لسنة 2004 الخاص بتنظيم التوقيع الإلكتروني المصري.

أما المشرع الجزائري و لمواكبة التطورات الحاصلة على مستوى التعاملات الإلكترونية، و قصد التكفل بالمتطلبات القانونية و التنظيمية و التقنيات التي تسمح بإحداث جو من الثقة و لتعميم و تطوير المبادلات الإلكترونية صدر القانون رقم 04/15 المؤرخ في أول فبراير 2015 و الذي يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، الذي يعد قفزة نوعية في مجال المعاملات الإلكترونية على مستوى هذا النوع الحديث من التعاملات[1].

فبصدور هذا القانون أصبح هاذا النوع من التوقيع منظم قانونا بموجب قانون خاص، و عرفه على أنه " بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة للتوثيق"[2].

يلاحظ على هاذا التعريف أن المشرع لم يحدد صور التوقيع الإلكتروني، بل اكتفى بأن يكون التوقيع في شكل إلكتروني فقط أيا كان هاذا الشكل، و هذا ما يفتح المجال أمام الاعتراف بجميع صور التوقيع الإلكتروني، كما ركز على الغرض من التوقيع الإلكتروني و المتمثل في توثيق هوية الموقع، و كذا توثيق مختلف الوثائق الإلكترونية الصادرة من الأطراف.

2-التعريف الفقهي للتوقيع الإلكتروني:

قد عرف بعض الفقه التوقيع الإلكتروني بأنه" مجموعة من الإجراءات و الوسائل التي يتبع استخدامها، عن طريق الرموز أو الأرقام إخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونيا، يجري تشفيرها باستخدام خوارزم المفتاح، أحدهم معلن عنه و الآخر خاص بصاحب الرسالة[3].

---

[1]- حابت أمال، التجارة الإلكترونية في الجزائر، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، الجزائر، 2015، ص 98.

[2] – المادة 02 من القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[3] – لملوم كريم، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية و الدولية، رسالة ماجستير، جامعة تيزي وزو، الجزائر، 2011، ص 121.

و يذهب اتجاه آخر إلى تعريفه بأنه " بيان مكتوب بشكل إلكتروني، يتمثل بحرف أو رقم أو رمز أو إشارة أو صوت أو شفرة خاصة و مميزة، ينتج عن اتباع وسيلة آمنة، و هذا البيان يلحق أو يرتبط منطقيا ببيانات المحرر الإلكتروني للدلالة على هوية الموقع على المحرر و الرضا بمضمونه"[1]. فهذا التعريف يقوم على أساس تحديد وسيلة التوقيع الإلكتروني، و الوظيفة المنوطة به و هي تحديد هوية الموقع و التأكد على قبوله مضمون الوثيقة الإلكترونية التي قام بالتوقيع عليها.

ثانيا: أنواع التوقيع الإلكتروني

يتخذ التوقيع الإلكتروني أشكالا عدة بحسب الوسيلة أو التقنية التي تستخدم في إنشائه[2]، لاسيما و أن القوانين التي نظمته و من بينها التشريع الجزائري لم تنص على شكل معين له، ولقد ظهرت العديد من أشكال للتوقيع الإلكتروني في المعاملات الإلكترونية، أهمها التوقيع باستخدام البطاقة الممغنطة، و التوقيع البيومتري، و التوقيع بالقلم الإلكتروني، و التوقيع الرقمي.

1- التوقيع باستخدام البطاقات الممغنطة المقترنة بالرقم السري:

يعد التوقيع باستخدام الرقم السري و البطاقة الممغنطة أول شكل أظهرته التقنيات التكنولوجية للتوقيع الإلكتروني و هو أكثرها شيوعا، و هذه الطريقة لتوقيع أفرزتها التقنيات التي استخدمت من أجل الإسراع في إنجاز المعاملات البنكية[3]، فقد درجت البنوك على إصدار بطاقات إلكترونية مصحوبة برقم سري تمنحها لعملائها لاستخدامها في سحب و إيداع النقود أو لسداد ثمن السلع و الخدمات، تسحب النقود أو تدفع من خلال جهاز آلي تؤمنه البنوك للعملاء كجهاز الصراف الآلي أو أجهزة الدفع الإلكتروني الموجودة في المحلات التجارية[4].

---

[1] – مصطفى هنشور وسيمة، المقال السابق، ص 407.

[2] – ثروت عبد الحميد، التوقيع الإلكتروني، دار النيل للطباعة و النشر، المنصورة، مصر، 2001، ص 47.

[3] – عيسى غسان ربضي، القواعد الخاصة للتوقيع الإلكتروني، دار الثقافة للنشر و التوزيع، عمان، 2012، ص 58.

[4] – آزاد دزه يي، المرجع السابق، ص20.

2- التوقيع بالقلم الإلكتروني:

من الأشكال الأخرى للتوقيع الإلكتروني التي يمكن استخدامها في توثيق التصرفات القانونية التي تبرم على الوسائط الإلكترونية التوقيع باستخدام قلم خاص، و هو عبارة عن قلم إلكتروني حسابي يمكن من خلاله الكتابة على شاشة الحاسب الآلي الخاص بالموقع[1].

إذ يحتوي الحاسب الآلي المتصل به القلم الإلكتروني برنامج خاص مثبتا على قاعدة بياناته، و هو المحرك لعملية التوقيع، إذ يقوم هذا البرنامج بوظيفتين أساسيتين هما:

-**الوظيفة الأولى:** وظيفة التقاط التوقيع

بداية يدخل الموقع بياناته الخاصة كالاسم و العمر و الوظيفة على البرنامج الموجود على قاعدة بيانات حاسبه الآلي، و بعد إدخال هذه البيانات تظهر على شاشة الحاسوب مجموعة من التعليمات لينفذها الموقع، و بعد الانتهاء من تنفيذها تظهر تعليمات أخرى على الشاشة مفادها " على الشخص المستخدم كتابة توقيعه داخل المربع الذي سيظهر على الشاشة بواسطة القلم الإلكتروني" ، و بمجرد تنفيذ الموقع هذه التعليمات يرى توقيعه على الشاشة بذات الشكل الذي كتب به. و يجمع البرنامج جميع بيانات الموقع و يدمجها مع شكل التوقيع الموافق عليه ثم يشفرها و يحتفظ بها لحين الحاجة إليها[2].

- **الوظيفة الثانية:** وظيفة التحقق من صحة التوقيع

عند حاجة الشخص إلى التوقيع لتوثيق التصرف القانوني الذي عزم على القيام به يرجع إلى البرنامج الذي حفظ التوقيع به، و لكي تتم عملية التوثيق يطلب الحاسب الآلي من الشخص كتابة توقيعه على الشاشة داخل مربع معين، هنا تظهر وظيفة البرنامج إذ

[1] - د. حجازي عبد الفتاح بيومي، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص 198.

[2] - د. أبو هبة نجوى، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2002 ،ص43.

يجري مقارنة بين خصائص التوقيع الموجودة على الشاشة و تلك الخصائص المحفوظة على قاعدة البيانات [1]، فإذا تم التطابق بين الخصائص التوقيع يصدر الحاسب الآلي تقريرا بالنتيجة التي توصل إليها.

و من مزايا هذا النوع من التوقيعات الإلكترونية صعوبة سرقة التوقيع و انتحال السارق صفة صاحب التوقيع بسهولة، و ذلك لصعوبة أو استحالة قيام السارق بالحركات و الانحناءات انفسها التي قام بها صاحب التوقيع الأصلي و المداخل و المخارج و الحروف و إحجامها و دقة قياسها[2].

أما الصعوبات التي تواجه هذا النوع من التوقيعات انه لابد لإتمام التوقيع بالقلم الإلكتروني من وجود حاسب ذي مواصفات خاصة، كاحتوائه على وحدة القلم الإلكتروني و الشاشة الحساسة و هذا إضافة إلى أنه غالي الثمن[3].

3- التوقيع البيومتري:

من التطورات التكنولوجية المبتكرة حديثا و التي تستخدم في التعاقدات التي تتم عبر الوسائط الإلكترونية تقنية الاعتماد على الخواص الفزيائية و الطبيعية و السلوكية للإنسان أطلق عليها التوقيع البيومتري[4]. إذ يقوم هاذا النوع من التوقيعات الإلكترونية على أساس المميزات الفردية بكل شخص، و التي تعتمد على تكنولوجيا و الخواص الحيوية أو الطبيعية التي يتميز بها الأشخاص عن بعضهم البعض[5].

يتطلب استخدام هذه الطريقة في التوقيع الإلكتروني، أخذ صورة دقيقة من الخواص مثل بصمة الإصبع ، بصمة الشفاه، نبرة الصوت، شبكة قرنية العين، ملامح الوجه و

---

[1] – يقوم البرنامج بقياس خصائص التوقيع كالحجم و الشكل و المنحنيات و النقاط و الخطوط و الالتواءات، و درجة الضغط على القلم. **أنظر عيسى غسان ربضي، المرجع السابق، ص 65.**

[2] – آزادة دزه يي، المرجع السابق ، ص71.

[3] – أبو هبة نجوى، المرجع السابق، ص 50.

[4] – د/ عمر خالد رزيقات، عقد البيع عبر الأنترنت، المرجع السابق، ص256

[5] – جميعي حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الأنترنت، دار النهضة العربية، القاهرة، 2000، ص 41.

غيرها من الصفات الجسدية و السلوكية، ثم يقوم بتخزينها بصورة مشفرة بذاكرة الحاسوب، حيث يستطيع صاحب الشأن و عند رغبته استعمال هذه الصورة لإبرام تصرف قانوني معين الرجوع إليها و توثيق تصرفه[1].

و يؤخذ على هذا النوع من التوقيع أنه يحتاج إلى تكاليف عالية و جهد كبير حتى يمكن التعامل بها على أساس من الموثوقية، كما يذهب البعض أنه بالرغم من دقته و الأمان و الثقة المتوافرة به إلا أنه ليس بعيدا عن التزوير، فيمكن تسجيل بصمة الصوت ثم إعادة بثها، كذلك تزوير بصمة العين بتقليدها عن طريق بعض أنواع العدسات اللاصقة... بل إن هناك إمكانية خضوع الذبذبات الحاملة للصوت أو الصورة للنسخ و إعادة الاستعمال مما يؤدي لافتقادها للأمن و السرية[2].

4- التوقيع الرقمي:

من الأشكال الأخرى للتوقيع الإلكتروني التي تستخدم في إبرام التصرفات القانونية عبر الوسائط الإلكترونية خاصة تلك المعاملات التي تتم عبر شبكة الاتصال الحديثة "الأنترنت" التوقيع الرقمي، و يعتمد هذا التوقيع على نظام التشفير لذى سما بنظام التوقيع القائم على التشفير[3]، و هو التوقيع الإلكتروني الأوسع نطاقا و الأكثر استخداما نظرا لطابع الأمان و الثقة الذي يوفرها، إذ يضمن سلامة البيانات الإلكترونية و تأمينها ضد أي عبث أو تلاعب أو تعديل، و قد عرفت المنظمة الدولية للمواصفات و المقاييس التوقيع الرقمي بأنه" بيان أو معلومة تتصل بمنظومة بيان أخرى، أو صياغة منظومة في صورة مشفرة و الذي يسمح للمرسل إليه إثبات مصدرها[4].

---

[1] – مشيمش ضياء أمين، التوقيع الإلكتروني، المنشورات الحقوقية، بيروت، 2003، ص 129.

[2] – جميعي حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الأنترنت، المرجع السابق، ص43.

[3] – على محمود أبوا العز، التجارة الإلكترونية و أحكامها في الفقه الإسلامي، طبعة1 ، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2008، ص 323.

[4] – آزاد دزه يي، المرجع السابق ص .72

يتضح أن التوقيع الرقمي من أهم صور التوقيع الإلكتروني و أفضلها على الإطلاق ، لما يتمتع به من تحديد هوية الموقع و تمييزه بدقة و درجة عالية من الثقة و الأمان في استخدامه و تطبيقه، و بذلك يكون له ذات القوة التي يتمتع بها التوقيع التقليدي ما لم تكن قوته أفضل.

الفقرة الثانية: الشروط الواجب توافرها في توقيع المستهلك الإلكتروني

نصت جل التشريعات التي نظمت التوقيع الإلكتروني على مجموعة من الشروط، يجب أن تتوافر فيه حتى يتمتع بالحجية الكاملة[1]، و يرى المشرع الجزائري أن التوقيع الإلكتروني الموصوف وحده يكون مساوي للتوقيع الكتابي[2].

و التوقيع الإلكتروني الموصوف هو ذلك التوقيع الإلكتروني الذي تتوفر فيه مجموعة من الشروط التي نص عليها المادة 07 من القانون رقم 04/15 سالف الذكر، و تتمثل هذه الشروط في ما يلي[3]:

[1] – سماه التوجيه الأوروبي حسب المادة الثانية بالتوقيع المتقدم و أشترط فيه : أن يرتبط و بشكل منفرد بصاحب التوقيع.، أن يتيح كشف هوية صاحب التوقيع، أن ينشأ من خلال وسائل موضوعة تحت سيطرة الموقع، أن يرتبط بالمعلومات التي وضع عليها التوقيع إلى درجة أن أي تعديل لاحق للبيانات يمكن كشفه. أما المشرع الفرنسي فقد نصت المادة 1316 من القانون 230 لسنة 2000 المعدل للقانون المدني على توفر شرطين في التوقيع الإلكتروني حتى يكون مساويا للتوقيع الكتابي، الأمر الأول و هو أن تكون هذه الطريقة موثوقة، أما الثانية فيجب أن تكون الكتابة الإلكترونية تعبر عن الشخص الذي صدرت عنه قانونا .

[2] – المادة 8 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين " يعتبر التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب ، سواء كان لشخص طبيعي أو معنوي".

[3] – المادة 7 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين " التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات التالية:

–أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.

–أن يرتبط بالموقع دون سواه.

–أن يمكن من تحديد هوية الموقع.

–أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.

–أن يكون مصمما بواسطة آلية تكون تحت التحكم الحصري للموقع.

أولا: أن يرتبط بالموقع دون سواه

اشترط المشرع ارتباط التوقيع الإلكتروني بالموقع وحده دون سواه تحقيقا للوظيفة القانونية للتوقيع، و هي تحديد هوية صاحب التوقيع و تمييزه عن غيره من الأشخاص، و التعبير عن إرادته في الالتزام بمضمون المحرر الإلكتروني الذي وقع عليه[1]. و ارتباط التوقيع الإلكتروني بالموقع وحده دون سواه يكون باستناد هذا التوقيع إلى منظومة إنشاء توقيع إلكتروني مؤمنة، و التحقق من صحة التوقيع الإلكتروني[2].

ثانيا: استناد التوقيع إلى آلية مؤمنة لإنشاء التوقيع الإلكتروني

الآلية المؤمنة لإنشاء التوقيع الإلكتروني تتمثل في جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني[3]، و التي تتوفر فيها المتطلبات التالية[4]:

-ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، و أن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد.

-ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج و أن يكون هذا التوقيع محمي من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد.

-عدم تعديل البيانات محل التوقيع، و أن تعرض البيانات على الموقع قبل عملية التوقيع.

-أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.

-أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

[1] – فاروق إبراهيم جاسم، الجوانب القانونية للتجارة الإلكترونية، دار السنهوري، بيروت، 2016، ص 88.

[2] – محمد محمد سادات ، خصوصية التوقيع الإلكتروني، دراسة مقارنة، دار الفكر و القانون للنشر و التوزيع، المنصورة، مصر، 2011، ص 165.

[3] – أنظر المادة 4/2 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[4] – أنظر المادة 11 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

ثالثا: التحقق من صحة التوقيع الإلكتروني

يتم التحقق من صحة التوقيع الإلكتروني عن طريق بيانات التحقق من التوقيع الإلكتروني و المتمثلة في " رموز أو مفاتيح التشفير العمومي أو أي بيانات أخرى مستعملة من أجل التحقق من التوقيع الإلكتروني" [1]، بواسطة منظومة أو آلية موثوقة[2].

و آلية التحقق من التوقيع الإلكتروني الموثوقة هيا جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع ، تتوفر فيها المتطلبات التالية[3]:

-أن تتوافر البيانات المستعملة للتحقق من التوقيع الإلكتروني مع بيانات إنشاء التوقيع المعروضة عند التحقق من التوقيع.

-أن يتم التحقق من التوقيع الإلكتروني بصفة مؤكدة و أن تكون نتيجة هذا التحقق معروضة عرضا صحيحا.

-أن يكون مضمون البيانات الموقعة اذا اقتضى الأمر محددا بصفة مؤكدة عند التحقق من التوقيع الإلكتروني.

-أن يتم التحقق بصفة مؤكدة من موثوقية و صلاحية شهادة التصديق الإلكتروني المطلوبة عند التحقق من التوقيع الإلكتروني.

-أن يتم عرض نتيجة التحقق و هوية الموقع بطريقة واضحة و صحيحة.

رابعا: أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع

تطلبت المادة 7 من قانون التوقيع و التصديق الإلكترونيين لصحة التوقيع الإلكتروني، و حتى يتمتع بالحجية الكاملة في الإثبات بأن يكون للموقع وحده -دون غيره- سيطرة على الوسائل التي أنشأ بواسطتها. و الوسائل التي ينشأ بواسطتها التوقيع

[1] - أنظر المادة 5/2 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[2] - أنظر المادة 12 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[3] - أنظر المادة 13 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

الإلكتروني هيا بيانات إنشاء التوقيع الإلكتروني و المتمثلة في بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني[1].

فحيازة الموقع لبيانات إنشاء التوقيع الإلكتروني تجعله مسيطرا عليها، أما اذا فقد الموقع سيطرته على هذه البيانات أصبحت غير سرية، بحيث يعلمها أشخاص آخرون غير الموقع، فإن التوقيع الإلكتروني لا يعتبر حجة في الإثبات، لأن تحديد شخصية الموقع و هويته بالرجوع إلى هذا التوقيع يكون مشكوكا فيه[2].

خامسا: أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات

ينبغي –فضلا عما تقدم– لصحة التوقيع الإلكتروني أن يكون متاحا من الناحية الفنية أمكانية كشف أي تعديل أو تبديل في بيانات التوقيع الإلكتروني، و هنا يظهر دور جهة التصديق الإلكتروني في المعاملات الإلكترونية، و هيا الجهة التي يناط بها تسجيل التوقيع الإلكتروني لديها و تصدر أنماط مختلفة من هذه التوقيعات، و تمنح شهادات تفيد صحة توقيع العميل أو صحة نسبة التوقيع إلى صاحبه، كتوثيق هوية الأشخاص المستخدمين للتوقيع الإلكتروني و تأكيد نسبة المفتاح العام المستخدم إلى صاحبه، و أن الموقع يملك المفتاح الخاص، فضلا من أنها تقوم بإصدار شهادات تصديق إلكتروني تثبت الارتباط بين الموقع و بيانات إنشاء التوقيع[3] .

و نظرا لأهمية شهادة التصديق الإلكتروني فقد جعل المشرع ضرورة استصدارها شرط من شروط التوقيع الإلكتروني الموصوف، و هو ما يعرف بالتصديق الإلكتروني.

---

[1] – أنظر المادة 3/2 من قانون 15–04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[2] – د/ فاروق إبراهيم جاسم، المرجع السابق، ص 89.

[3] – د/ محمد محمد سادات، المرجع السابق، ص 167.

الفرع الثاني: التصديق على توقيع المستهلك الإلكتروني

يتطلب استخدام التوقيع الإلكتروني بطريقة آمنة و موثوق بها تدخل شخص ثالث، لإعطاء التوقيع الإلكتروني فعاليته الكاملة[1]، فهذه الجهة تصدر شهادات إلكترونية للمصادقة على صحة التوقيع الإلكتروني و معرفة صاحب التوقيع، و منع التلاعب به أو بمحتوى البيانات الإلكترونية[2]، و عليه سنبين الجهة المختصة بالتصديق على التوقيع الإلكتروني (الفقرة الأولى) ، ثم نحدد مفهوم شهادة التصديق على التوقيع الإلكتروني (الفقرة الثانية).

الفقرة الأولى: الجهة المختصة بالتصديق على التوقيع الإلكتروني

حدد المشرع الجزائري الجهة المختصة بالتصديق على التوقيع الإلكتروني و اطلق عليها تسمية مؤدي خدمات التصديق الإلكتروني، و كذا الشروط التي يجب أن تتوفر فيهم من خلال قانون 04/15 سالف الذكر. و عليه سنحاول تحديد مفهوم هذه الجهة (أولا)و الشروط الواجب توافرها فيهم حتى يمارسوا نشاط التصديق على التوقيع الإلكتروني (ثانيا).

أولا: مفهوم مؤدي خدمات التصديق الإلكتروني

اختلفت التسميات التي اطلقت على جهة التصديق على التوقيع الإلكتروني، حيث عرفها قانون اليونسترال النموذجي للتوقيع الإلكتروني الصادر سنة 2001 باسم مقدم خدمات التصديق بانه" شخص يصدر الشهادات و يجوز أن يقدم خدمات أخرى ذات صلة بالتوقيع الإلكتروني"[3].

---

[1] – د/ نادر شافي، " **التوقيع الإلكتروني، الاعتراف التشريعي و تعريفه**"، مجلة الجيش اللبناني، العدد 239، 2006.

[2] – د/ محمد محمد سادات، المرجع السابق، ص 36.

[3] – المادة 2 بند هـ من قانون اليونستيرال النموذجي للتوقيع الإلكتروني الصادر سنة 2001.

أما المشرع الفرنسي فقد عرف جهات التصديق على التوقيع الإلكتروني أو مقدم خدمة التصديق على أنها كل شخص طبيعي أو معنوي يصدر شهادات أو خدمات متعلقة بالتوقيع الإلكتروني[1].

و عرفه المشرع التونسي في الفصل الثاني من قانون 83 لسنة 2000 المتعلق بالمبادلات و التجارة الإلكترونية بانه" كل شخص طبيعي أو معنوي يحدث ويسلم و يتصرف في شهادات المصادقة، و يسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني"[2].

وقد عرف المشرع المصري جهات التصديق الإلكتروني بأنها الجهات المرخص لها بإصدار شهادات التصديق الإلكتروني و تقدم خدمات تتعلق بالتوقيع الإلكتروني[3].

أما المشرع الجزائري فقد استعمل مصطلح " مؤدي خدمات التصديق الإلكتروني"، و عرفه في المادة الثانية من القانون 04/15 المتعلق بالتوقيع و التصديق الإلكترونيين بأنه " كل شخص طبيعي أو معنوي، يقوم بمنح شهادات تصديق إلكتروني موصوفة، و يقدم خدمات أخرى في مجال التصديق الإلكتروني".

و عليه فإن مؤدي خدمات التصديق الإلكتروني هو الشخص (طبيعيا أو اعتباريا) المسؤول عن إصدار شهادة تتضمن تحديد هوية الموقع و تثبت صلته بالتوقيع الإلكتروني، إذ يعد بمثابة حلقة وصل في مجال المعاملات القانونية الإلكترونية بين المرسل و المرسل إليه[4]، كما يقدم خدمات أخرى في مجال التصديق الإلكتروني[5].

---

[1] – آزاد دزه يي، المرجع السابق ص .75.

[2] – الفصل الثاني من قانون 83 لسنة 2000 المتعلق بالمبادلات و التجارة الإلكترونية التونسي

[3] – زهيرة كيسي، "**النظام القانوني لجهات التوثيق الإلكتروني**"، مجلة دفاتر السياسة و القانون، العدد السابع، 2012، ص 35.

[4] – مشيمش ضياء أمين، المرجع السابق، ص 73 .

[5] – من بين الخدمات الأخرى التي يقدمها مؤدي خدمات التصديق الإلكتروني: إصدار تواقيع رقمية عن طريق إصدار المفاتيح الإلكترونية (المفتاح الخاص او العام) التي يتم بمقتضاها تشفير الرسائل و التواقيع الإلكترونية أو فكها، التحقيق من صحة التواقيع الإلكترونية و نسبتها إلى أصحابها، مسك سجلات خاصة بالشهادات الصادرة عنه، و

ثانيا: شروط ممارسة نشاط مؤدي خدمات التصديق الإلكتروني

حدد المشرع الجزائري الشروط الواجب توافرها في مؤدي خدمات التصديق الإلكتروني، و التي يمكن تقسيمها إلى شروط تتعلق بنشاط تأدية خدمة التصديق الإلكتروني و شروط تتعلق بمؤدي خدمة التصديق الإلكتروني، و سنحاول تبيان كل منها كالتالي:

1-شروط تتعلق بنشاط تأدية خدمات التصديق الإلكتروني:

أدرج المشرع الجزائري نشاط التصديق الإلكتروني في المجال الاقتصادي ضمن نظام الترخيص، تمنحه السلطة الاقتصادية لتصديق الإلكتروني[1].

حيث يقوم مؤدي خدمة التصديق الإلكتروني بوضع طلب لدي هذه الأخيرة مبين فيه سياسة التصديق الإلكتروني المعتمدة من قبله، و في حالة وضع الطلب يمنح شهادة التأهيل قبل الحصول على الترخيص[2] لمدة سنة واحدة قابلة للتجديد مرة واحدة، خلال 60 يوما ابتداء من تاريخ استلام الطلب المثبت بإشعار بالاستلام، لتهيئة كل الوسائل اللازمة لتأدية خدمات التصديق الإلكتروني، و حصوله على شهادة التأهيل لا يمكنه من تادية خدمات التصديق إلا بعد الحصول على الترخيص[3].

تصنيفها من حيث تلك الصالحة للاستعمال و الشهادات الملغاة و تاريخ الإلغاء، تعقب المواقع التجارية على الأنترنت للتحري عنها و عن جديتها و مصداقيتها، فإذا تبين عدم أمنها، يقوم بتوجيه رسائل تحذيرية للمتعاملين عن عدم مصداقية الموقع. **أنظر د/ دريس كمال فتحي، "آلية التصديق الإلكتروني كضمانة للتعاملات التجارية بالوسائل الحديثة "، مجلة البحوث و الدراسات، العدد 24، 2017، ص 164.**

[1] – المادة 33 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين " يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنه السلطة الاقتصادية للتصديق الإلكتروني".

[2] – المادة 10/02 من القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين الترخيص: نظام استغلال خدمات التصديق الإلكتروني و الذي يتجسد في وثيقة رسمية ممنوحة لمؤدي الخدمات بطريقة شخصية، تسمح له بالبدء الفعلي في توفير خدماته.

[3] – أنظر المادة 35 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

و يمنح الترخيص لصاحب شهادة التأهيل لمدة 5 سنوات، و يجدد عند انتهاء صلاحيته وفقا للشروط المحددة في دفتر الأعباء الذي ترفقه السلطة الاقتصادية للتصديق الإلكتروني بشهادة الترخيص[1].

و في حالة الرفض طلب شهادة التأهيل و الترخيص وجب على السلطة الاقتصادية تسبيب الرفض و يتم تبليغه مقابل إشعار بالاستلام[2]، كما يمنح الترخيص بصفة شخصية لا يمكن التنازل عنها للغير و بمقابل مالي يحدد مبلغه عن طريق التنظيم[3].

2-شروط تتعلق بطالب ترخيص تأدية خدمات التصديق الإلكتروني:

بالإضافة لشرط الحصول على الترخيص، يجب أن تتوفر في مؤدي خدمات التصديق الإلكتروني مجموعة من الشروط الفنية و التقنية، كأن يكون خاضع للقانون الجزائري في حالة ما إذا كان شخص معنوي أو يتمتع بالجنسية الجزائرية إذا كان شخص طبيعي، و التمتع بقدرة مالية كافية و بمؤهلات و خبرة ثابتة في ميدان تكنلوجيا الإعلام و الاتصال للشخص الطبيعي أو المسير للشخص المعنوي، وأن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاطه، بالإضافة[4].

[1] – انظر المادة 40 من قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين.

[2] – أنظر المادة 37 من قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين.

[3] – أنظر المادة 39 من قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين.

[4] – أنظر المادة 34 من قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين.

الفقرة الثانية: شهادة التصديق الإلكتروني

يمارس مؤدي خدمات التصديق وظائفهم عن طريق إصدار شهادات، سماها البعض "شهادات التوثيق الإلكتروني، و البعض الآخر استعمل مصطلح " الشهادات المعتمدة"، و آخرون استعملوا عبارة "شهادات التصديق أو المصادقة الإلكترونية"، و رغم اختلاف التشريعات في تسمية هذه الشهادة إلا أنها أجمعت على أنه وسيلة لبعث الثقة في التعاملات الإلكترونية و الحفاظ على سريتها و توفير الأمان لأطراف العقود الإلكترونية عامة و للمستهلك خاصة، الأمر الذي يستدعي البحث عن مفهومها من خلال تعريفها(أولا)، و البيانات الواجب توافرها فيها(ثانيا).

أولا: تعريف شهادة التصديق الإلكتروني

نظرا لأهمية هذه الشهادة في إثبات هوية الموقع و صحة التوقيع، فقد نصت معظم التشريعات المنظمة للتجارة الإلكترونية على تعريفها. فقد عرفها قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية بأنها" الشهادة التي تصدر من الجهة المرخص لها بالتصديق و تثبت الارتباط بين الموقع و بيانات إنشاء التوقيع"[1].

وعرفها المشرع الفرنسي بأنها" مستند في شكل إلكتروني تثبت توافر الرابط بين بيانات التحقق من صحة التوقيع الإلكتروني و بين الموقع"[2].

و عرفها المشرع المصري بأنها" الشهادة التي تصدر من الجهة المرخص لها بالتصديق، و تثبت الارتباط بين الموقع و بين إنشاء الشهادة"[3].

أما المشرع الجزائري فقد عرف شهادة التصديق الإلكتروني بأنها " وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقيق من التوقيع الإلكتروني و الموقع"[4].

---

[1] – أنظر المادة 2/ب من قانون الأنستيرال النموذجي بشأن التوقيع الإلكتروني لسنة 2001.

[2] – مشيمش ضياء أمين، المرجع السابق، ص 73.

[3] – أنظر المادة 1/و من قانون التوقيع الإلكتروني المصري.

[4] – أنظر 7/2 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

و يلاحظ من التعريفات السابقة أنها ركزت على الجانب الوظيفي لشهادة التصديق الإلكتروني، المتمثل أساس في إثبات هوية الموقع و أنه صادر عمن نسب إليه، و أن توقيعه صحيح، بما في ذلك البيانات الموقع عليها و أنه لم يطرأ عليها حذف أو إضافة أو تغير.

ثانيا: بيانات شهادة التصديق الإلكتروني

لا يكون لشهاد التصديق الإلكتروني الحجية، و لا تستطيع أداء مهامها في تأكيد صدور الرسائل و التوقيعات الإلكترونية عن أصحابها، لتحقيق الثقة و الأمان فيها، إلا إذا تضمنت بيانات معينة[1]، و قد نص المشرع الوطني على تلك البيانات في المادة 15 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين و أطلق على هذه الشهادة تسمية شهادة التصديق الإلكتروني الموصوفة. حيث يمكن تقسيم هذه البيانات إلى ثلاث مجموعات كالتالي:

1- المعلومات المتعلقة بشهادة التصديق الإلكتروني: و التي تتضمن ما يلي:

-الإشارة إلى ما يدل أن هذه الشهادة منحت على أساس أنها شهادة تصديق إلكتروني موصوفة[2]: ينبغي أن تتضمن شهادة التصديق الإلكتروني ما يفيد أنها منحت بوصفها شهادة تصديق إلكتروني" موصوفة"، و تكمن هذه الإشارة إلى ضمانة الشفافية في المعاملات

-مدة صلاحية الشهادة[3]: و يعد هذا البيان من البيانات المهمة للمستهلك كطرف متعاقد، فهو يحقق له الثقة في التعامل مع صاحب الشهادة، إذ تشير أن تتضمن الشهادة تاريخ صلاحيتها و تاريخ انتهائها. حيث تحدد مدة صلاحية الشهادة وفقا لسياسة التصديق المقدمة من طرف مقدم خدمة التصديق الإلكتروني و التي وافق عليها السلطة

[1] - حجاز عبد الفتاح بيومي، التوقيع الإلكتروني في النظام القانوني المقارن، دار الفكر الجامعي، الإسكندرية، 2005، ص 295.

[2] - أنظر المادة 15/1/أ من قانون 15/04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[3] - أنظر المادة 15/3/و من قانون 15/04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

الاقتصادية للتصديق الإلكتروني[1]، أو في حالة إلغائها في الحالات التي نص عليها القانون[2].

-حدود استخدام الشهادة و قيمة المعاملات المالية[3]: أوجب المشرع عند الضرورة أن تتضمن شهادة التصديق الإلكتروني على حدود استعمال هذه الشهادة و كذا قيمة المعاملات التي قد تستعمل من أجلها هذه الشهادة[4].

-الرقم التسلسلي للشهادة التصديق الإلكتروني: اعتبر المشرع الجزائري هذا البيان من البيانات الضرورية في شهادة التصديق الإلكتروني[5].

2- المعلومات و البيانات المتعلقة بصاحب التوقيع: و تشمل هذه البيانات على ما يلي:

-هوية صاحب التوقيع الإلكتروني و صفته: ينبغي أن تشمل الشهادة على ما يحدد شخصية الموقع و انه صاحب الشهادة التي تصدر من مقدم خدمة التصديق الإلكتروني، و ذلك من خلال بيان اسم الموقع الأصلي أو اسمه المستعار الذي يسمح بتحديد هويته، كما يمكن إدراج صفة خاصة للموقع عند الاقتضاء و ذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني[6] .

-بيانات تتعلق بالتحقيق من صحة التوقيع الإلكتروني: كما يلزم المشرع وضع بيانات التحقيق من صحة التوقيع الإلكتروني في هذه الشهادة[7].

---

[1] – أنظر المادة 1/45 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[2] – أنظر المادة 2/45 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[3] – أنظر المادة 45 /3/ي من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[4] – أنظر المادة 3/45/ط من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[5] – أنظر المادة 3/15/ز من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[6] – أنظر المادة3/15/ج من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[7] – أنظر المادة 3/15/ه من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

-**الإشارة إلي الوثيقة التي تثبت** تمثيل شخص طبيعي أو معنوي آخر عند الاقتضاء[1].

3- المعلومات و البيانات المتعلقة بمقدم خدمات التصديق الإلكتروني: و تشتمل على ما يلي:

-**هوية مقدم خدمات التصديق الإلكتروني**[2]: أشار المشرع الجزائري إلى أن تتضمن شهادة التصديق الإلكتروني اسم و عنوان الجهة المرخص لها إصدار هذه الشهادة، و كذلك البلد الذي يقيم فيه.

-**التوقيع الإلكتروني الموصوف للجهة المرخص لها إصدار شهادة التصديق الإلكتروني**[3]: ينبغي أن تحتوي شهادة التصديق الإلكتروني على التوقيع الإلكتروني لمقدم لمقدم خدمة التصديق الإلكتروني أو الطرف الثالث الموثوق الذي يمنح هذه الشهادة.

و عليه فإذا ما توفرت هذه البيانات في شهادة التصديق الإلكتروني، يمكن التعويل عليها في إبرام العقود و المعاملات الإلكترونية، باعتبار أن ما ورد فيها موثوق و يمكن الأطراف من التعامل في كل أمان. و تكون محل حماية قانونية.

[1] – أنظر المادة 3/15/ك من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[2] – أنظر المادة 3/15/ب من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[3] – أنظر المادة 3/15/ح من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

المطلب الثاني: صور الحماية الجنائية لتوقيع المستهلك الإلكتروني

تتم التعاقدات الإلكترونية عن طريق وسيط إلكتروني يتبادل من خلاله أطراف التعاقد المعلومات و البيانات المعالجة إلكترونيا و يتم التوقيع على هذا التعاقد عن طريق التوقيع الإلكتروني، و نظرا لأهمية و قيمة هذه التوقيع في توفير سرية المعاملات الإلكترونية، فقد فرضت على المشرع الوطني ضرورة فرض حماية جنائية خاصة له، سواء من خلال قانون العقوبات أو بموجب نصوص قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين.

و سنحاول تحديد هذه الحماية من خلال قانون العقوبات (الفرع الأول) و الحماية المقررة بموجب قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين (الفرع الثاني).

الفرع الأول: الحماية المقررة لتوقيع المستهلك الإلكتروني في ظل قانون العقوبات

تتم العقود الإلكترونية عن طريق التوقيع عليها، و يتم التوقيع عن طريق منظومة إنشاء توقيع إلكتروني، الأمر الذي يؤدي إلى اختصار الزمن و هو ما يبحث عنه المستهلك في عملية التعاقد الإلكتروني، غير أن استخدام شبكات الاتصال قد يعرض بيانات هذا التوقيع لعمليات التطفل الأمر الذي يؤدي في النهاية إلى قرصنتها و السطو عليها[1].

و نظرا للتطور الحاصل في بيئة الأعمال الإلكترونية شرع المشرع الجزائري إلى تعديل قانون العقوبات و ذلك بموجب الأمر رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات، إذ أضاف فصلا كاملا تحت عنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

و يقصد بنظام المعالجة الآلية وفق التعريف الوارد في الفقرة (ب) من المادة 2 من القانون رقم 09-04 بشأن الوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال و

[1] – سليم عبد الله الخيوري، الحماية القانونية لمعلومات شبكة الأنترنت، طبعة1، منشورات الحلبي الحقوقية، لبنان، 2011، ص 318.

مكافحتهما[1] بأنه " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ".

ووفقا لهذا التعريف الموسع فإن المحل الذي ينصب عليه سلوك الجاني في جرائم المساس بأنظمة المعالجة الآلية للبيانات يتسع لاستيعاب المعلومات في نظام المعالجة الآلية خلال مرحلة المعالجة و التخزين و الاسترجاع، النظام الذي يتضمنها فضلا عن الشبكات ذاتها أو المعلومات المنقولة عبرها، و بالتالي يشمل تجريم اعتراض عملية نقل المعلومات سواء من خلال الدخول إلى الشبكة الاتصالات أو من خلال التقاط الإشارات التي يحدثها جهاز إلكتروني من خلال وسائل التقاط إلكترونية، و يترتب على ذلك أن تصبح هذه الإشارات محلا ينصب عليه سلوك الجاني في هذه الجرائم[2].

و عليه فإن منظومة إنشاء التوقيع الإلكترونية هيا جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني[3]، إذ يتم فيها تبادل البيانات بين طرفي (صاحب التوقيع و مؤدي خدمات التصديق الإلكتروني أو المورد الإلكتروني) من خلال الحاسب الآلي و باستخدام أنظمة و برامج معينة، مما يجعلها منظومة معلوماتية وفق لتعريف السابق، و عليه تكون محلا للحماية الجنائية المقررة لأنظمة المعالجة الآلية . و سنحاول التطرق لأهم الجرائم الماسة بهذا النظام و هيا جريمة الدخول أو البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني (الفقرة الأولى)، و جريمة التلاعب في بيانات إنشاء التوقيع الإلكتروني (الفقرة الثانية) باعتبارها أنظمة معالجة آلية.

[1] – قانون رقم 09-04 مؤرخ في 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال و مكافحتها، الجريدة الرسمية عدد 47، الصادرة في 16 أوت سنة 2009.

[2] – رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012، – ص223.

[3] – أنظر المادة 4/2 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

الفقرة الأولى: جريمة الدخول أو البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني

يتحقق الاعتداء على التوقيع الإلكتروني بالاعتداء على النظام المعلوماتي له من خلال الدخول أو البقاء غير المشروع[1]، و لقد جرم المشرع الوطني فعل الدخول أو البقاء غير المشروع في المادة 394 مكرر ق ع ج [2]. و هذه الجريمة كغيرها من الجرائم يجب لقيامها توافر كل من ركنها المادي (أولا) و ركنها المعنوي (ثانيا)، كما أقر لها المشرع عقوبة تتماشى مع جسامتها (ثالثا).

أولا: الركن المادي لجريمة الدخول أو البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني

يتحقق الركن المادي لهذه الجريمة بمجرد إتيان السلوك المجرم دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر المتطلب فيها حصول ضرر للمجني عليه[3]، و السلوك المجرم وفقا للمادة 394 مكرر من قانون العقوبات يتمثل في فعل الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات –من بينها منظومة إنشاء توقيع إلكتروني– أو جزء منه، و فعل البقاء غير المشروع فيه أو في جزء منه. و هو ما يقتضي منا تبيان كل من الدخول و البقاء غير المشروعين و ذلك كالتالي:

1-الدخول غير المشروع إلى النظام:

لم يعرف المشرع الوطني فعل الدخول في النظام باعتبارها ظاهرة حديثة تتعلق بأشياء غير ملموسة أي غير مادية. غير أن الفقه الفرنسي تصدى لهذا المصطلح و وضع مدلولين، مدلول معنوي، بحيث يشبه الدخول إلى النظام بمثابة ذلك إلى ذاكرة الإنسان، و مدلول مادي، يتمثل في أن الشخص قد يكون حاول أو دخل بالفعل إلى النظام المعلوماتي[4]. و وفقا للتصور المعنوي لفكرة الدخول، فإنه يتحقق بأي صورة من

---

[1] – على عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، الدار الجامعية للطباعة و النشر، بيروت، 1999، ص 128.

[2] – المادة 394 مكرر " يعاقب بالحبس... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..."

[3] – شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 97.

[4] – خليفي مريم، "**الحماية الجنائية لمواقع التجارة الإلكترونية**"، مجلة العلوم القانونية، عدد 2، 2011، ص 170.

صور التعدي، أي يستوي أن يكون التعدي مباشرا أو غير مباشر، علما بأن الدخول في ذاته –حسب أنصار المدلول المعنوي– يعد مسالة وقتية، و أن تخلف عنها بعض الآثار التي تستمر حيزا من الزمن[1].

و يتم الدخول بأي وسيلة تقنية حيث أن المشرع الجزائري لم يحدد ذلك[2]، كما أنها جريمة يمكن أن يقترفها الشخص أيا كانت صفته، بشرط ألا يكون فقط ممن هم مخول لهم بالدخول إلى النظام، و أن يكون هذا الدخول مخالفا لإرادة صاحب النظام أو من له الحق في السيطرة عليه[3]، لذلك تعد من صور الدخول غير المشروع أيضا أن يكون صاحب النظام قد وضع قيودا للدخول إلى ذلك النظام، و لم يحترم الجاني هذه القيود، أو عن طريق استخدام برامج القرصنة[4].

و عليه فإن المشرع في هذه الجريمة يعاقب على مجرد الدخول إلى النظام المعلوماتي كنظام إنشاء التوقيعات الإلكترونية عند إبرام العقود الإلكترونية ، حتى و إن لم يترتب على دخوله ضررا، طالما أن الدخول كان بطريقة غير مشروعة، و يتحقق فعل الدخول إلى أنظمة إنشاء بيانات التوقيع الإلكترونية إذا دخل الجاني إلى النظام كله أو جزء منه، كالدخول على الحاسب الآلي أو شبكة الاتصال أو البرامج ، كما يتحقق الاعتداء بالدخول غير المشروع، متى كان مسموح للجاني بالدخول لجزء معين في البرنامج و تجاوزه إلى جزء آخر غير مسموح له بالدخول له[5]. لذلك يخرج من نطاق الدخول غير المشروع الدخول إلى برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه. كما لا تتوافر الجريمة أن اقتصر دور الجاني على مجرد قراءة الشاشة، إذ بهذه الأفعال لا تقوم جريمة الدخول غير المشروع إلى نظام المعالجة[6].

---

[1] – محمد عبيد كعبي، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، دون سنة نشر، ص 34.

[2] – لم يحدد المشرع الجزائري في المادة 394 مكرر وسيلة معينة للدخول و هو أمر قد وفق فيه مما يفتح المجال في العقاب على كل طريقة أو وسيلة لتحقيق الدخول.

[3] – د/ مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص و الأنترنت، المرجع السابق، ص 60 .

[4] – عبد الحليم بوقرين، الرسالة السابقة، ص 126.

[5] – رشيدة بوكر، المرجع السابق، ص 228.

[6] – د/ محمد عبيد كعبي، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص 335 .

2-البقاء غير المشروع في النظام:

يتحقق هذا السلوك المجرم بتواجد الجاني داخل نظام إنشاء توقيع إلكتروني بدون رضا من له الحق في التحكم بالنظام[1]. إذ أن الهدف من تجريم فعل البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني، هو معاقبة كل شخص كان دخوله إلى النظام بطريقة الصدفة البحتة و أنتفى لديه القصد الجنائي، و ذات الحكم ينصرف إلى من هو مسموح له بالدخول إلى جزء من النظام، ثم يدخل إلى جزء آخر غير مصرح له الدخول فيه[2].

فيرى جانب من الفقه أن هذه الجريمة تقوم بسلوك سلبي، إذ رغم دخول الجاني مصادفة و رغم علمه بأن ذلك غير مشروع، فهو يرفض الخروج من النظام، و بمعنى آخر يمتنع عن الخروج من النظام[3]. و يعرف هذا الجانب من الفقه فعل البقاء على أنه " التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في سيطرته على هذا النظام، و وفقا لهذا الرأي يعد من صور فعل البقاء المعاقب عليه، أن يظل الجاني باقيا داخل النظام بعد المدة المحددة له بالبقاء داخله، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له بالرؤية و الاطلاع فقط[4].

و خلاصة القول أن فكرة الدخول الغير مشروع على أنظمة المعالجة الآلية للمعطيات بما فيها أنظمة إنشاء التوقيع الإلكتروني تحدد بعدة معايير أو دلائل، أهمها المعايير المكانية و الزمانية و الفنية، دلالة المكان، و تعني التسلل داخل النظام المعلوماتي، و دلالة الزمان، و تتمثل في تجاوز حدود التصريح أو الترخيص داخل النظام و الممنوع لفترة زمنية محددة عن طريق تجاوز هذه الفترة الزمنية[5] و عادة ما تتحقق لدى مؤدي خدمات التصديق الإلكتروني الذينِ وكل لهم مهمة إنشاء هذا النوع من التوقيعات الإلكترونية، حيث يكونون على علم بشفرة الدخول وقت إنشاء التوقيع و تسليمه

---

[1] – رامي عبد الحليم، "جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات"، مجلة دراسات و أبحاث ، جامعة زيان عاشور الجلفة، عدد1، 2009.

[2] – د/ السيد عتيق، جرائم الأنترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص 299

[3] – د/عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الإلكترونية، الكتاب الثني، الحماية الجنائية للتجارة الإلكترونية، دار الفكر العربي، مصر، 2002، ص 31.

[4] – د/عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الإلكترونية، المرجع السابق، ص 32.

[5] – د/ مدحت عبد الحليم رمضان، المرجع السابق، ص 251.

إلى المستهلك أو الشخص المعني عند الطلب. أما الدلائل الفنية، فيتحدد مضمونها بالدخول الذي يتم بصورة مختلفة، منها الاعتداء على البرنامج أو المعطيات أو المكونات المادية أو الوصلات الخاصة بالحاسب الآلي، سواء عن طريق الغش المعلوماتي بأداة إلكترونية مصطنعة، و عن طريقها يتم التقاط معلومات أو التنصت عليها [1]، كما تتحقق هذه الجريمة أيضا بالالتقاط غير المشروع للمعطيات، أو الاطلاع الغير مشروع عليها أو التنصت عليها، و هيا كلها أمور بالغة الخطورة في المعاملات الإلكترونية[2].

ثانيا: الركن المعنوي لجريمة الدخول أو البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني.

تعد هذه الجريمة من الجرائم العمدية التي تقوم بالقصد الجنائي العام الذي يتكون من عنصري العلم و الإرادة، حيث يتوجب أن يكون الجاني عالما بعدم أحقيته في دخول النظام أو البقاء فيه، و أن هذا الفعل مخالف لإرادة صاحب النظام، و مع ذلك يقدم عل الدخول على هذا النظام أو يبقى فيه بإرادة حرة[3].

و الملاحظ أن المشرع الوطني اشترط في المادة 394 مكرر أن يتم **الدخول أو البقاء عن طريق الغش**، و يقصد بطريق الغش في هذه الحالة أن الجاني يجب أن يكون سيء النية عند دخوله للنظام أو البقاء فيه، و يستخلص سوء النية في غالب الأحيان عندما يخترق الجاني نظام الحماية الخاص بنظام التوقيع الإلكتروني[4]، أما بالنسبة لعنصر البقاء فيستنتج من خلال العمليات و التصرفات التي قام بها الجاني داخل النظام، و مع ذلك فإن سوء النية يظهر أيضا من خلال الدخول أو البقاء دون وجه حق[5]، حيث يرى جانب من الفقه بأن الدخول يكون مشروعا و بالتالي تنتفي الجريمة متى كان

---

[1] – د/ السيد عتيق، المرجع السابق، ص 230.

[2] – شيماء عبد الغني، المرجع السابق، ص 122.

[3] – عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2004، ص 350.

[4] – نصت المادة 2 من اتفاقية بودابست للإجرام المعلوماتي أنه يحق للدول الأعضاء أن تشترط بأن الجريمة ترتكب عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة داخله.

[5] – أمال قارة، المرجع السابق، ص 123.

بطريق الصدفة أو السهو أو الخطأ، بشرط أن ينسحب الشخص متى علم باعتدائه أو خطئه و إلا توافر في حقه القصد الجنائي لارتكاب هذه الجريمة و يعاقب بعقوبتها[1].

و متى توافر القد الجنائي بعنصريه –العلم و الإرادة– فإنه لا محل للباعث على ارتكاب الجريمة، باعتبار أن الباعث عليها لا أثر له على قيامها، و لذلك تقوم الجريمة في حق الجاني بتوافر القصد الجنائي، حتى ولو كان باعثه للدخول إلى النظام أو البقاء فيه، هو الفضول أو التنزه أو إثبات القدرة في الانتصار على النظام[2].

ثالثا: العقوبة المقررة لجريمة الدخول أو البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني

اعتبر المشرع الجزلئري جريمة الدخول أو البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني من قبيل الجنح و قرر لها عقوبة الحبس من ثلاثة أشهر إلى سنة و غرامة مالية من 50.000دج إلى 200.000دج.

أما إذا ترتب على الدخول أو البقاء محو البيانات التي يحتويها نظام التوقيع الإلكتروني أو أدى إلى فقدان النظام لقدرته على أداء وظيفته المتمثلة في توقيع المحررات و قبول مضمونها في المعاملات الإلكترونية تصبح العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 100.000دج إلى 400.000دج[3].

أما الشخص المعنوي الذي يرتكب هذه الجريمة فقد قرر له المشرع من خلال المادة 394 مكرر4 عقوبة مالية تقدر بمضاعفة خمس مرات الحد الأقصى للعقوبة المالية المقررة للشخص الطبيعي[4].

---

[1] – حنان ريحان مبارك المضحكي، الجرائم المعلوماتية (دراسة مقارنة)، طبعة1،منشورات الحلبي الحقوقية، لبنان، 2014، ص 107.

[2] – حمودي ناصر، الحماية الجنائية للتجارة الإلكترونية، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2015، ص 85.

[3] – المادة 394 مكرر قانون عقوبات المعدل و المتمم فقرة الثانية " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ، و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة..."

[4] – المادة 394 مكرر4 من قانون العقوبات المعدل و المتمم " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

كما أقر المشرع الجزائري المعاقبة على مجرد المحاولة أو الشروع في ارتكاب هذه الجريمة، أي أنها من الجرائم الجائز العقاب على الشروع فيها، و هو ما أكد عليه المشرع من خلال المادة 394 مكرر7 التي قررت العقاب على الشروع بخصوص الجرائم المتعلقة بالاعتداء على نظم المعالجة الآلية للمعطيات[1].

و عليه فإن المشرع الجزائري قد احسن في صياغة هذه المادة من خلال أنها تحمل أو يدخل في مجالها أي نظام للمعالجة الآلية سواء تعلق بإنشاء توقيع إلكتروني أو تعلق بإنشاء شهادة تصديق إلكتروني أو خاص بمنصات الدفع الإلكتروني أو مواقع التجارة الإلكتروني، و لكن يعاب عليه أن العقوبة المقررة لهذه الجريمة تبدو غير كافية لردع هذه الجريمة خاصة في مجال المعاملات التجارية الإلكترونية، مما ينبغي التدخل و رفع الغرامة المقررة لها.

[1] – المادة 394 مكرر7 من قانون العقوبات المعدل و المتمم " يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

الفقرة الثانية: جريمة التلاعب في بيانات نظام إنشاء توقيع إلكتروني

بتجرم المشرع الجزائري أفعال الاعتداء على أنظمة المعالجة الآلية للبيانات من بينها أنظمة إنشاء توقيع إلكتروني، من دخول غير مشروع إلى النظام أو جزء منه أو البقاء فيه، أورد نصا آخر يعاقب على كل اعتداء على البيانات ذاتها الموجودة بالنظام. و هيا الأفعال التي يعاقب عليها المشرع الجزائري بموجب المادة 394مكرر 1 من قانون العقوبات[1]، والتي تعاقب على التلاعب في بيانات نظام إنشاء توقيع إلكتروني، المتمثلة في : إدخال معلومات في النظام، أو إزالتها أو تعديلها بطريق الغش دوما، و هيا الأفعال المشكلة للركن المادي لهذه الجريمة.

أولا: الركن المادي لجريمة التلاعب في بيانات نظام إنشاء توقيع إلكتروني

انطلاقا من نص المادة 394 مكرر 1 من قانون العقوبات الجزائري يتضح أن الركن المادي لجريمة التلاعب الغير مصرح به للمعلومات التي يتضمنها نظام إنشاء توقيع إلكتروني يتم بسلوك إجرامي يرتكبه الجاني دون أن يستهدف تحقيق نتيجة معينة.

إذ ينحصر السلوك الإجرامي المكون للركن المادي لهذه الجريمة في أفعال الإدخال أو التعديل أو إزالة معلومات داخل نظام إنشاء توقيع إلكتروني مع عدم وجود تصريح، و التي لا يشترط توافرها جميعا، بل يكفي قيام أحدها ليقوم الركن المادي لهذه الجريمة[2]. و عليه فإن صور السلوك الإجرامي في هذه الجريمة تتعدد مما يقتضي الأمر بيان كل صورة منها على حدى بنوع من التفصيل الموجز لتتضح الأمور.

1-فعل الإدخال:

عرفه الفقه فعل الإدخال على أنه "تغذية النظام بالمعلومات المراد معالجتها، أو بتعليمات لازمة لعملية المعالجة"[3]، أو أنه " إضافة خصائص ممغنطة جديدة في الدعامة

---

[1] – المادة 394 مكرر1 قانون عقوبات المعدل و المتمم " يعاقب من ستة أشهر (6) إلى ثلاث (3) سنوات و بغرامة مالية من 500.000دج إلى 4.000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

[2] – محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية– دراسة مقارنة– رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2009، ص 212.

[3] – رشيدة بوكر، المرجع السابق، ص 251.

الموجودة سواء كانت فارغة غير مشغولة ، أو كانت تحتوي على خصائص ممغنطة قبل هذا الإدخال"[1]. و عليه فإن فعل الإدخال بوجه عام يكون بإضافة معطيات جديدة لم تكن موجودة من قبل على الدعامة الخاصة، و ذلك بهدف التشويش على صحة البيانات و المعلومات الموجودة داخل نظام إنشاء التوقيع الإلكتروني[2].

و إدخال المعلومات المحرفة إلى نظام إنشاء توقيع إلكتروني أمر سهل القيام به من قبل مؤدي خدمات التصديق الإلكتروني، حيث يكون من السهل تغذية النظام بمعلومات مغلوطة أو زائفة فيه لم تكن موجودة في السابق أو أحد العاملين على التدقيق المنصوص عليهم في المادة 16/2 من قانون التوقيع و التصديق الإلكترونيين رقم 15-04، الأمر الذي يؤثر على سلامة المعلومات الموجودة فيه و قيمتها و سلامة المعاملة الإلكترونية[3].

كما يمكن للغير إدخال المعلومات المحرفة لنظام إنشاء توقيع إلكتروني، إذ تتنوع الطرق و الأساليب في تحقيق فعل الإدخال و أهمها إدخال البرامج الخبيثة إلى نظام توقيع إلكتروني بهدف إتلاف المعلومات و تشويهها و تدميرها، و من الوسائل انتشارا و خطورة على المعلومات برامج الفيروسات و القنابل المنطقية و الزمنية[4].

2-فعل التعديل:

يقصد بالتعديل إجراء نوع من التغيير غير المشروع للمعلومات و البيانات المحفوظة داخل النظام، و استبدالها ببيانات و معلومات أخرى جديدة و ذلك باستخدام احدى وظائف الحاسب الآلي[5]. فالتعديل يعني تغيير البيانات و المعلومات المعالجة آليا

---

[1] – د/ عبد الفتاح بيومي حجاز، جرائم الكمبيوتر و الأنترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية 2006، ص 378.

[2] – على عبد القادر القهوجي، "**الحماية الجنائية للبيانات المعالجة إلكترونيا**"، بحث مقدم لمؤتمر القانون و الكمبيوتر و الأنترنت، كلية الشريعة و القانون، جامعة الإمارات، مايو 2000، ص 59.

[3] – د/ خالد ممدوح إبراهيم، التقاضي الإلكتروني و إجراءاتها أمام المحاكم ، الطبعة الأولى ، دار الفكر الجامعي، مصر، 2008،ص 329

[4] – رشيدة بوكر، المرجع السابق، ص 251 .

[5] – د/ على عبد القادر القهوجي، المقال السابق، ص 59.

و الموجودة داخل النظام المعلوماتي و استبدالها ببيانات و معلومات أخرى، و عادة ما يتم عن طريق برامج تتلاعب بهذه المعطيات[1].

3-فعل الإزالة:

يقصد بالإزالة محو جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام، أو تحطيم تلك الدعامة أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[2]. و هو فعل أيضا في العادة يرتكب من طرف القائمين على تسيير هذه البرامج كمؤدي خدمات التصديق الإلكتروني أو القائمين بالتدقيق، أو عن طريق برامج الاختراق[3].

و الجدير بالذكر أن الأفعال المكونة للركن المادي لجريمة التلاعب ببيانات نظام إنشاء توقيع إلكتروني مذكورة على سبيل الحصر و عليه لا يدخل ضمن هذه الجريمة فعل نسخ البيانات مثلا أو التخريب[4].

ثانيا: الركن المعنوي لجريمة التلاعب ببيانات نظام إنشاء توقيع إلكتروني.

هذه الجريمة كغيرها من الجرائم السابقة ، تعد جريمة عمدية تتطلب قصد جنائي عام ، و تقوم بمجرد توافر فعل الإدخال أو التعديل أو الإزالة[5]. سيما و أن كان المشرع الجزائري استعمل عبارة" عن طريق الغش" ، مما ينطوي على أن الشخص يعلم بسلوكه المجرم و يريد فعلا النتائج المترتبة عليه، التي قد تكون إدخال البيانات و المعطيات أو إزالتها أو تعديلها[6].

---

[1]– محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، طبعة2، دار النهضة العربية، القاهرة، 1998، ص 74.

[2] – هبة حسين محمد زايد، المرجع السابق، ص 91 .

[3]– محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، الرسالة السابقة، ص 210..

[4]– لتفصيل أكثر أنظر عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2004، ص 51.

[5] – د/ على عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، المقال السابق، ص 60 .

[6] – مدحت رمضان عبد الحليم، المرجع السابق، ص 56.

ثالثا: العقوبة المقررة لجريمة التلاعب ببيانات نظام إنشاء توقيع إلكتروني

اعتبر المشرع الجزائري هذه الجريمة من الجنح و عاقب عليها وفقا للمادة 394 مكرر1 سابق ذكرها بالحبس من ستة أشهر إلى ثلاث سنوات و الغرامة من 500.000دج إلى 4.000.000دج

أما الشخص المعنوي الذي يرتكب هذه الجريمة تضاعف عقوبته خمس مرات الحد الأقصى لعقوبة الغرامة المقررة للشخص الطبيعي طبقا للمادة 394 مكرر4 من قانون العقوبات.

و في الأخير نرى بأن المشرع الجزائري عند تجريمه لمختلف الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، من شأنه أن يضفي حماية جنائية فعالة لمنظومة إنشاء التوقيع الإلكتروني للمستهلك، و حتى غيرها من الأنظمة في مقدمتها أنظمة التصديق الإلكتروني، و ذلك لأن التعامل مع الأنترنت بأي شكل من الأشكال سواء تعلق الأمر بالمعاملات التجارية أو غيرها من المسائل المعلوماتية، لا يمكن أن يتم إلا باتخاذ مواقع على هذه الشبكة تسيرها نظم معلوماتية.

الفرع الثاني: الحماية المقررة لتوقيع المستهلك الإلكتروني في ظل قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين

ظهر التوقيع الإلكتروني ليكون بديلا عن التوقيع التقليدي، ليتوافق و طبيعة التعاقدات القانونية و العقود التي يبرمها المستهلك باستخدام الوسائل و الأجهزة الإلكترونية الحديثة. مما دعا المشرع الوطني لإصدار تشريع خاص و هو القانون 15-04 المحدد للقواعد العامة للتوقيع و التصديق الإلكترونيين لينظم هذا النوع من التوقيعات لتوفير و تعزيز الثقة و الأمان في التعاملات الإلكترونية. و حماية لما يوفره هذا النوع الجديد من التوقيعات من أمان، جرم المشرع مجموعة من الأفعال سواء تلك المتعلقة بتأدية خدمات التصديق الإلكتروني(الفقرة الأولى) أو تلك المتعلقة شهادة التصديق الإلكتروني (الفقرة الثانية)، و أخيرا المتعلقة بالتوقيع الإلكتروني ذاته(الفقرة الثالثة).

الفقرة الأولى: الجرائم المتعلقة بتأدية خدمات التصديق الإلكتروني

منح المشرع الجزائري المؤدي خدمات التصديق الإلكتروني إصدار شهادات التصديق الإلكتروني لبعث الثقة و الأمان في المعاملات الإلكترونية، و ذلك في ظل نظام قانوني ينظم هذا النشاط كما رأيناه سابقا، والذي اتبعه المشرع الوطني بتقرير المسؤولية الجزائية حتى يمنح للأطراف المتعاملة من بينها المستهلك الثقة و الأمان في الشهادات التي يصدرونها و حمايتا لتوقيعاتهم الإلكترونية التي اشترط المشرع أن ترفق بشهادة التصديق. و عليه سنحاول تحديد هذه المسؤولية الجزائية لمؤدي خدمات التصديق الإلكتروني والتي يمكن حصرها في جريمة مزاولة نشاط مؤدي خدمات التصديق الإلكتروني بدون ترخيص (أولا)، وجريمة عدم الإعلام بالتوقف عن نشاط خدمات التصديق الإلكتروني (ثانيا)، وجريمة الجمع الغير المشروع للبيانات الشخصية لطالب شهادة التصديق الإلكتروني (ثالثا).

أولا: جريمة مزاولة نشاط مؤدي خدمات التصديق الإلكتروني بدون ترخيص أو بعد سحب الترخيص

جرم المشرع الجزائري ممارسة نشاط مؤدي خدمات التصديق الإلكتروني بدون ترخيص أو بعد سحب الترخيص من خلال نص المادة 72 من قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين[1]، و تقرير هذه المسؤولية يعد من أهم صور الحماية لتوقيع المستهلك الإلكتروني باعتبار أن مؤدي خدمات التصديق الإلكتروني هو الوسيط أو الطرف الثالث الموثوق في التعاملات الإلكترونية. و عليه سنحاول تحليل هذه الجريمة انطلاقا من ركنيها المادي و المعنوي و تحديد العقوبة المقررة لها.

1-الركن المادي لجريمة مزاولة نشاط مؤدي خدمات التصديق الإلكتروني بدون ترخيص أو بعد سحب الترخيص:

يتمثل الركن المادي لهذه الجريمة حسب نص المادة 72 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين في إتيان مؤدي خدمات التصديق الإلكتروني أحد السلوكين، يتمثل الأول في تقديم خدمات التصديق الإلكتروني دون ترخيص، أو مواصلة تقديم الخدمة بالرغم من سحب الترخيص. و سنحاول تبيان كل سلوك على حدى :

أ- تقديم خدمات التصديق الإلكتروني دون ترخيص:

أوجب المشرع عند مزاولة نشاط مؤدي خدمة التصديق الإلكتروني الحصول على ترخيص مسبق تمنحه السلطة الاقتصادية لتصديق الإلكتروني[2]. و مخالفة هذا الالتزام يعد سلوك مجرما وفقا للمادة 72 السابق ذكرها. و عليه فإن عدم حصول مؤدي خدمات التصديق الإلكتروني للترخيص وفقا لتشرع المعمول به يؤدي لقيام المسؤولية الجزائية.

---

[1]- المادة 72 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين "يعاقب بالحبس... ، كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه".

[2] - أنظر المادة 33 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

و لقد حدد المشرع الإجراءات الواجب اتباعها للحصول على الترخيص و المتمثلة في:

-**تقديم طلب لدى السلطة الاقتصادية للتصديق الإلكتروني:** حيث يقوم مؤدي خدمة التصديق الإلكتروني بوضع طلب لدي السلطة الاقتصادية للتصديق مبين فيه سياسة التصديق الإلكتروني المعتمدة من قبله.

-**الحصول على شهادة التأهيل:** و في حالة وضع الطلب تمنح السلطة الاقتصادية للتصديق الإلكتروني لصاحب الطلب شهادة التأهيل قبل الحصول على الترخيص لمدة سنة واحدة قابلة للتجديد مرة واحدة، خلال 60 يوما ابتداء من تاريخ استلام الطلب المثبت بإشعار بالاستلام، لتهيئة كل الوسائل اللازمة لتأدية خدمات التصديق الإلكتروني. و لا يمكن لحامل هذه الشهادة تأدية خدمات التصديق الإلكتروني إلا بعد الحصول على الترخيص[1].

-**تقديم الترخيص:** إن حصول صاحب الطلب على شهادة التأهيل يمكنه من الحصول على الترخيص، بعد أن يتقدم بطلب إلى السلطة الاقتصادية للتصديق الإلكتروني أو مكتب التدقيق المعتمد بإنجاز تقييم تقييمي، و بهذا التدقيق التقييمي تقرر هذه السلطة منح الترخيص أو رفض الطلب مع التسبيب[2].

و في حالة منح الترخيص يكون صالح لمدة 5 سنوات ، و يجدد عند انتهاء صلاحيته وفقا للشروط المحددة في دفتر الأعباء الذي ترفقه السلطة الاقتصادية للتصديق الإلكتروني بشهادة الترخيص مع دفع مقابل مالي[3]. كما يمنح الترخيص بصفة شخصية لا يمكن التنازل عنها للغير[4].

---

[1] – أنظر المادة 35 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين .

[2] – أنظر المادة 36 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[3] – أنظر المادة 40 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[4] – أنظر المادة 39 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

و عليه فإن عدم الحصول على الترخيص وفقا الإجراءات السابق بيانها يؤدي إلى قيام جريمة مزاولة نشاط مؤدي خدمات التصديق الإلكتروني دون ترخيص من قبل السلطة الاقتصادية للتصديق الإلكتروني.

ب- مواصلة تقديم خدمات التصديق الإلكتروني بالرغم من سحب الترخيص:

تقوم الجريمة في هذه الصورة عندما يسحب ترخيص تأدية الأنشطة المتعلقة بخدمات التصديق الإلكتروني من مؤدي الخدمات ، و يقوم هذا الأخير بمواصلة النشاط، أي انتحال الجاني صفة مؤدي خدمات التصديق الإلكتروني المرخص له بمزاولة العمل و ذلك على خلاف الحقيقة.

و لقد حدد المشرع الحالات التي يسحب فيها الترخيص من قبل مؤدي خدمات التصديق الإلكتروني، و هيا كالتالي:

-**عند التوقف عن النشاط:** أجاز المشرع لمؤدي خدمات التصديق الإلكتروني التوقف عن الأنشطة سواء بمحض الإرادة أو كانت لأسباب خارجة عن إرادته، إلا أنه رتب على وقف الأنشطة المتعلقة بخدمات التصديق الإلكتروني سحب الترخيص[1].

-في حالة عدم احترام مؤدي خدمات التصديق الإلكترونية أحكام دفتر الأعباء أو سياسة التصديق الإلكتروني الخاصة به[2].

-في حالة عدم احترام امتثال مؤدي خدمات التصديق الإلكتروني للأعذار[3].

-في حالة انتهاك مؤدي الخدمات التصديق الإلكتروني للمقتضيات التي يطلبها الدفاع الوطني و الأمن العمومي[1].

---

[1] – أنظر المادة 58 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[2] – أنظر المادة 1/64 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[3] – المادة 64 فقرة 2 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين " و في حالة عدم امتثال مؤدي الخدمات للأعذار، تتخذ ضده السلطة الاقتصادية للتصديق الإلكتروني قرار سحب الترخيص الممنوح له و إلغاء شهادته، حسب الحالة، بعد موافقة السلطة".

و عليه فإن مواصلة تأدية خدمات التصديق الإلكتروني بعد سحب الترخيص من السلطة الوطنية للتصديق الإلكتروني سلوك معالق عليه بموجب المادة 72 من قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين.

2-الركن المعنوي لجريمة مزاولة نشاط مؤدي خدمات التصديق الإلكتروني بدون ترخيص:

يتحقق الركن المعنوي في هذه الجريمة بتوافر القصد الجنائي العام بعنصريه العلم و الإرادة، فيجب أن يعلم الجاني أن سلوكه المتمثل في مزاولة نشاط خدمات التصديق الإلكتروني دون أن يحصل على ترخيص بذلك من الجهة المختصة أو مواصلة العمل مع سحب الترخيص هو سلوك مجرم يعاقب عليه القانون، و أن تتجه إرادته إلى إتيان هذا السلوك و ما يترتب عليه من نتائج[2].

3-العقوبة المقررة لجريمة مزاولة نشاط مؤدي خدمات التصديق الإلكتروني بدون ترخيص:

عاقب المشرع الجزائري مؤدي خدمات التصديق الإلكتروني عند إصدار شهادة التصديق الإلكتروني بدون ترخيص أو مواصلة الخدمة بعد سحب الترخيص بالحبس مدة تتراوح بين سنة (1) واحدة إلى ثلاث (3) سنوات ،و بغرامة مالية من مائتي ألف دينار (200.000 دج) إلى مليوني دينار جزائري (2.000.000 دج) أو بإحدى هاتين العقوبتين فقط، بالإضافة إلى عقوبة تكميلية تتمثل في مصادرة التجهيزات التي استعملت لارتكاب هذه الجريمة[3].

[1] – أنظر المادة 65 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[2] – هدى قشقوش، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 43.

[3] – أنظر المادة 72 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

أما الشخص المعنوي الذي يرتكب هذه الجريمة فقد قرر له المشرع من خلال المادة 75 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين [1] عقوبة مالية تقدر بمضاعفة خمس مرات الحد الأقصى للعقوبة المالية المقررة للشخص الطبيعي لتحدد بغرامة قدرها عشرة ملايين دينار جزائري (10.000.000دج).

ثانيا: جريمة عدم الإعلام بالتوقف عن نشاط خدمات التصديق الإلكتروني

جعل المشرع الجزائري على عاتق مؤدي خدمات التصديق الإلكتروني عند إيقاف نشاطه المتعلق بخدمات التصديق الإلكتروني التزاما بإعلام السلطة الاقتصادية للتصديق الإلكتروني في الآجال المحددة قانونا. و هذا ما نصت عليه المادة 61 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين .و هذه الجريمة كغيرها من الجرائم تتكون من ركن مادي و معنوي و عقوبة تتناسب مع جسامتها.

1-الركن المادي لجريمة عدم إعلام السلطة الوطنية بالتوقف عن نشاط خدمات التصديق الإلكتروني :

يتمثل الركن المادي لهذه الجريمة في عدم إعلام مؤدي خدمات التصديق الإلكتروني السلط الاقتصادية للتصديق بالوقف عن ممارسة الأنشطة المتعلقة بخدمات التصديق في الآجال المحدد قانونا. و قد حدد المشرع الآجال القانوني للتبليغ و ميز بين حالتين:

الحالة الأولى: يلتزم مقدم خدمات التصديق الإلكتروني الراغب في إيقاف نشاطه المتعلق بخدمات التصديق الإلكتروني بإعلام السلطة الاقتصادية للتصديق الإلكتروني في الآجال المحددة في سياسة التصديق الإلكتروني لهذه السلطة [2].

[1] – المادة 75 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين " يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي."

[2] – أنظر المادة 58 من قانون 15-04 المتعلق المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

الحالة الثانية: في حالة إيقاف مقدم خدمات التصديق الإلكتروني أنشطته لأسباب خارجة عن إرادته وجب عليه إعلام السلطة الاقتصادية للتصديق الإلكتروني في" **الحال**" [1].

و عليه فإن عدم إعلام السلطة الاقتصادية للتصديق الإلكتروني عن التوقف عن ممارسة نشاط التصديق الإلكتروني، و في الآجال المحددة قانونا يعتبره المشرع الوطني سلوك مجرم و معاقب عليه بموجب المادة 61 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

2-الركن المعنوي لجريمة عدم إعلام السلطة الوطنية بالتوقف عن نشاط خدمات التصديق الإلكتروني :

تعتبر هذه الجريمة من الجرائم العمدية تقوم بالقصد الجنائي العام بركنيه العلم و الإرادة ، فيلتزم على مؤدي خدمات التصديق الإلكتروني بإعلام السلطة الاقتصادية عند التوقف عن نشاطه في الآجال التي حددها القانون، و أن عدم الإعلام يجرمه القانون و يعاقب عليه، و مع ذلك تتجه إرادته إلى عدم التبليغ و تقبل النتائج التي تترتب عليه[2].

3-العقوبة المقررة لجريمة عدم إعلام السلطة الوطنية بالتوقف عن نشاط خدمات التصديق الإلكتروني :

أقر المشرع من خلال المادة 61 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين أنه عند إخلال مؤدي خدمات التصديق الإلكتروني بإعلام السلطات الاقتصادية بالتوقف عن نشاطه في الآجال المحددة قانون وفقا للمادتين 58 و 59 بالحبس من شهرين (2) إلى سنة (1) واحدة و بغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000دج) ، أو بإحدى هاتين العقوبتين فقط.

[1] – أنظر المادة 59 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين.

[2] – جبيري ياسين، "**الحماية الجنائية للتصديق و التوقيع الإلكتروني –دراسة مقارنة**"، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، العدد 01، المجلد 32، 2018، ص 145.

أما الشخص المعنوي الذي يرتكب هذه الجريمة فقد قرر له المشرع من خلال المادة 75 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين عقوبة مالية تقدر بمضاعفة خمس مرات الحد الأقصى للعقوبة المالية المقررة للشخص الطبيعي، إذ تقدر العقوبة لشخص المعنوي بي خمس ملايين دينار جزائري (5.000.000دج).

ثالثا: جريمة الجمع الغير المشروع للبيانات الشخصية لطالب شهادة التصديق الإلكتروني.

أقرى المشرع الجزائري المسؤولية الجزائية لمؤدي خدمات التصديق الإلكتروني عند قيامه بالجمع الغير مشروع للبيانات الشخصية للمستهلك عند طلب شهادة التصديق الإلكتروني، و هذا ما نصت عليه المادة 71 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، والتي تنص على " **يعاقب ...، كل مؤدي خدمات التصديق الإلكتروني اخل بأحكام المادة 43 من نفس القانون**". و عليه سوف نتطرق إلى أركان هذه الجريمة كالتالي:

1-الركن المادي لجريمة الجمع الغير المشروع للبيانات الشخصية لطالب شهادة التصديق الإلكتروني:

فمن خلال استقرائنا للمادة 71 و المادة 43 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، فإن الركن المادي لهذه الجريمة يتمثل في الجمع الغير مشروع للبيانات الشخصية لطالب الشهادة، و تتحقق عدم المشروعية في صورتين هما:

الصورة الأولى تتمثل في قيام مؤدي خدمات التصديق الإلكتروني بجمع بيانات شخصية تتعلق بطالب الشهادة دون رضاه و هو ما عبر عنه المشرع الجزائري من خلال الفقرة الأول من المادة 43 من نفس القانون و التي تنص على " **لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة**". و عليه اشترط المشرع في هذه الحالة أن تكون الموافقة صريحة لا ضمنية، و يكون ذلك

باللفظ و بالكتابة أو الإشارة المتداولة عرفا كما يكون صريحة أي تكون الموافقة باتخاذ موقف لا يدع أي شك في دلالته على مقصود صاحبه[1].

أما الصورة الثانية لعدم المشروعية فتتمثل في نوع البيانات المراد جمعها، إذ تتحقق الجريمة حتى بعد موافقة طالب الشهادة لمؤدي خدمات التصديق الإلكتروني بالجمع، إذ أن البيانات الشخصية الواجب جمعها هيا البيانات الضرورية لمنح و حفظ شهادة التصديق الإلكتروني [2]، و يبقى للقاضي الجنائي تقدير متى كانت هذه البيانات ضرورية في الغرض الذي جمعت من أجله.

2-الركن المعنوي لجريمة الجمع الغير المشروع للبيانات الشخصية لطالب شهادة التصديق الإلكتروني:

و جريمة جمع مؤدي خدمات التصديق الإلكتروني الغير مشروع لبيانات الشخصية للمستهلك من الجرائم العمدية و التي يتطلب لقيام الركن المعنوي فيها توافر القصد الجنائي العام بعنصريه العلم و الإرادة، فمرتكب هذه الجريمة يسعى بمحض إرادته إلى جمع بيانات خاصة بالمستهلك دون رضاه، أو جمع بيانات غير تلك التي أجاز المشرع جمعها بهدف منح و حفظ شهادة التصديق الإلكتروني، و تتجه إرادته لإتيان هذا السلوك و يقبل الآثار المترتبة عليه[3].

---

[1] – راضية عيمور، "**الحماية الجنائية للمعاملات الإلكترونية، مجلة الدراسات القانونية و السياسية**"، العدد01، ص 135.

[2] – الفقرة الثانية من المادة 43 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين " لا يمكن مؤدي خدمات التصديق الإلكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح و حفظ شهادة التصديق الإلكتروني ، و لا يمكن استخدام هذه البيانات لأغراض أخرى.

[3] – عزيزة لرقط، "**الحماية الجنائية للتوقيع و التصديق الإلكترونيين في التشريع الجزائري**"، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المركز الجامعي لتامنغست، الجزائر، العدد 11، 2017، ص 105.

3-العقوبة المقررة لجريمة الجمع الغير المشروع للبيانات الشخصية لطالب شهادة التصديق الإلكتروني:

اقر المشرع الجزائري مسؤولية مؤدي خدمات التصديق الإلكتروني عند الجمع الغير مشروع للبيانات الشخصية للمستهلك عند طلب شهادة التصديق الإلكتروني من خلال نص المادة 71 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، و تتمثل العقوبة في الحبس من ستة أشهر (6) إلى ثلاث (3) سنوات، و بغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط.

أما الشخص المعنوي الذي يرتكب هذه الجريمة فقد قرر له المشرع من خلال المادة 75 من نفس القانون عقوبة مالية تقدر بمضاعفة خمس مرات الحد الأقصى للعقوبة المالية المقررة للشخص الطبيعي، و عليه تكون العقوبة تساوي خمس ملايين دينار جزائري (5.000.000دج).

الفقرة الثانية: الجرائم المتعلقة ببيانات شهادة التصديق الإلكتروني

نظرا لما تشكله شهادة التصديق الإلكترونية من أهمية في تحقيق الأمن و السرية في المعاملات الإلكترونية، إذ تعد وظيفتها الربط بين الموقع و توقيعه الإلكتروني، فكل شهادة تحتوي على بيانات خاصة بصاحبها كاسمه أو سلطته في التوقيع و أهليته و مهنته...إلخ، مما يمكن المستهلك أو المورد الإلكتروني (المهني) من التحقق من هوية الموقع و صلاحية توقيعه قبل إبرام التصرف بشكل نهائي.

و هو ما جعل المشرع الجزائري يضفي على بيانات شهادة التصديق الإلكتروني حماية جزائرية من خلال قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين، و هيا حماية أساسها حماية التوقيع الإلكتروني للأطراف المتعاقدة عامة و المستهلك خاصة. و تشمل هذه الحماية جريمة التصريح بمعطيات خاطئة لاستصدار شهادة التصديق الإلكتروني (أولا)، و حماية سرية بيانات هذه الشهادة (ثانيا).

أولا: جريمة التصريح بمعطيات خاطئة لاستصدار شهادة التصديق الإلكتروني

نصت المادة 66 من قانون 04/15 المتعلق بالتوقيع و التصديق الإلكترونيين على أنه" يعاقب بالحبس ....، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة". و هذه الجريمة كغيرها من الجرائم لا بد من توافر كل من ركنها المادي و المعنوي على النحو التالي:

1-الركن المادي لجريمة التصريح بمعطيات خاطئة لاستصدار شهادة التصديق الإلكتروني:

يتحقق الركن المادي في هذه الجريمة بمجرد توافر واقعة التصريح بالمعطيات الخاطئة أو الغير صحيحة من جانب الجاني، ذلك أن الجاني أو ممثله القانوني يقدمان معلومات خاطئة أو غير صحيحة كاذبة أيا كان موضوع المعلومات، سواء كانت تتعلق بهوية صاحب الشهادة أو هوية الشخص المفوض، و هي المعلومات التي تحدد شخص

صاحب الشهادة تحديدا دقيقا[1]. و يتعين كذلك الإدلاء بهذه المعلومات و البيانات الكاذبة إلى مؤدي خدمات التصديق الإلكتروني حاصل على ترخيص من الجهة المختصة، و يكون الغرض من ذلك هو استصدار شهادة تصديق إلكتروني موصوفة [2].

2-الركن المعنوي لجريمة التصريح بمعطيات خاطئة لاستصدار شهادة التصديق الإلكتروني:

أما الركن المعنوي لهذه الجريمة، فهيا جريمة من الجرائم العمدية يتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم و الإرادة، فيجب على الجاني أن يعلم بحقيقة سلوكه الإجرامي و أنه يدلي بإقرارات كاذبة إلى مؤدي خدمات التصديق الإلكتروني بهدف الحصول على شهادة تصديق إلكتروني موصوفة، و يعلم أن هذا الفعل محضور قانونا، و مع ذلك تتجه إرادته إلى فعل السلوك الإجرامي المتمثل في الإدلاء بهذه المعلومات غير الصحيحة[3].

3-العقوبة المقررة لجريمة التصريح بمعطيات خاطئة لاستصدار شهادة التصديق الإلكتروني:

أقر المشرع لهذه الجريمة من خلال المادة 66 من قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين عقوبة سالبة للحرية تتمثل في الحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات، و بعقوبة مالية تتمثل في غرامة تتراوح بين عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج). أو إحداهما فقط.

أما الشخص المعنوي الذي يرتكب هذه الجريمة فقد قرر له المشرع من خلال المادة 75 من نفس القانون عقوبة مالية تقدر بمضاعفة خمس مرات الحد الأقصى للعقوبة

---

[1] – د/ عبد الفتاح بيومي حجازي، التجارة عبر الأنترنت، طبعة1، دار الفكر الجامعي ، الإسكندرية، 2008، ص 323.

[2] – هدى حامد قشقوش، التجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، 2000، ص 588.

[3] – د/ عبد الفتاح بيومي حجازي، مقدمة في التجارة العربية ، المجلد الأول، دار الفكر الجامعي، الإسكندرية، 2003، ص 275.

المالية المقررة للشخص الطبيعي. و عليه تكون العقوبة المقررة للشخص المعنوي مليون دينار جزائري (1.000.000دج).

ثانيا: جريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني

جرم المشرع الجزائري انتهاك سرية بيانات شهادة التصديق الإلكتروني من خلال نصي المادة 70 و المادة 73 من قانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، و الملاحظ على هاتين المادتين أن المشرع حمى بموجبهما سرية بيانات شهادة التصديق الإلكتروني، إلا أن الاختلاف يكمن في صفة الجاني، فالمادة الأولى تتعلق بمقدمي خدمات التصديق الإلكتروني، أما الثانية فتتعلق بكل شخص مكلف بالتدقيق. و سنحاول تحديد كل من ركني هذه الجريمة و العقوبة المقررة لها.

1-الركن المادي لجريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني:

يتوافر الركن المادي لهذه الجريمة بمجرد انتهاك سرية و خصوصية تلك المعلومات الخاصة ببيانات شهادة التصديق الإلكتروني حتى و لو لم يترتب على هذا الانتهاك أي نتيجة إجرامية، فهذه الجريمة تعد من الجرائم السلوكية يكفي فيها المشرع مجرد تحقق السلوك الإجرامي دون اشتراط تحقق النتيجة لأن الغرض من التجريم هنا هو الحفاظ على سرية المعلومات و خصوصيتها و ليس تحقيق نتيجة إجرامية[1].

و كشف المعلومات أو البيانات هنا يعني أن الجاني (المكلف بالتدقيق، مؤدي خدمات التصديق الإلكتروني) يطلع على بيانات شهادة التصديق الإلكتروني بحكم وظيفته ، أي أن هذا الاطلاع مبررا[2]، و عقب إطلاع الجاني يقوم بإذاعة هذه البيانات التي اطلع عليها بحكم وظيفته، و يكون هذا الإفشاء أو الإذاعة بأي طريقة كانت سواء بنشرها في الصحف أو الإعلان بوسيلة مرئية أو إذاعية أو بوسيلة إلكترونية أو أي وسيلة أخرى

[1] – أسامة عبد الله فايد، المرجع السابق، ص 77.

[2] – هبة حسين محمد، المرجع السابق ، ص.61

على عدد محدد من الجمهور، المهم أن تفقد بيانات شهادة التصديق الإلكتروني طابع السرية سواء بمقابل أو بدون مقابل[1] .

غير أنه لا يعد من قبيل الإفشاء المعاقب عليه إذا كان السبب يرجع إلى تصريح بنص القانون أو التنفيذ استنادا لإجراءات قضائية كأمر يصدر من إحدى المحاكم الجزائية المختصة[2].

2-الركن المعنوي لجريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني:

أما الركن المعنوي لجريمة انتهاك سرية و خصوصية المعلومات فيقوم بتوافر القصد الجنائي العام بعنصريه العلم و الإرادة، فمرتكب هذه الجريمة (المكلف بالتدقيق، مؤدي خدمات التصديق الإلكتروني) يسعى بمحض إرادته إلى كشف هذه المعلومات المتواجدة لديه بحكم وظيفته مع علمه بسريتها و في غير الأحوال المصرح بها قانونا ، و تتجه إرادته لإتيان هذا السلوك و يقبل الآثار المترتبة عليه[3].

3-العقوبة المقررة لجريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني:

تختلف عقوبة جريمة انتهاك سرية بيانات شهادة التصديق الإلكتروني باختلاف صفة الجاني، فإن كان مرتكب الجريمة مؤدي خدمات التصديق الإلكتروني فإن العقوبة نصت عليها المادة 70 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، و تتمثل في الحبس من ثلاث (3) أشهر إلى سنتين (2) و بغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين فقط. أما بالنسبة للشخص المعنوي فحسب نص المادة 75 من نفس القانون تكون غرامة تساوي خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، و عليه تكون الغرامة خمس ملايين دينار جزائري (5.000.000دج).

---

[1] – عبد الفتاح بيومي حجازي، التجارة عبر الإنترنت، المرجع السابق، ص327.

[2] – فوزي أوصديق، "**إشكالية المعلومات بين الخصوصية و إفشاء الأسرار المهنية**"، مجلة دراسات قانونية، مركز البصيرة للبحوث و الدراسات و الخدامات التعليمية، الجزائر، العدد 12، 2008، ص 49.

[3] – عزيزة لرقط، المقال السابق، ص 105.

أما إذا كان مرتكب الجريمة من بين الأشخاص المكلفون بالتدقيق، فإن عقوبته حددتها المادة 73 من نفس القانون، و تتمثل في الحبس من ثلاثة (3) أشهر إلى سنتين (2) و هيا نفس العقوبة السالبة للحرية المقررة لمؤدي خدمات التصديق الإلكتروني، و غرامة مالية تتراوح بين عشرين الف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج)، أو بإحدى هاتين العقوبتين فقط. أما بالنسبة للشخص المعنوي فالعقوبة تكون غرامة تساوي خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، و عليه فالغرامة المقررة للشخص المعنوي هيا مليون دينار جزائري (1.000.000دج).

الفقرة الثالثة: الجرائم المتعلقة بالتوقيع الإلكتروني ذاته

وضع المشرع مجموعة من الجرائم حتى يتم توفير أكبر قدر من الحماية لأمن و سلامة التوقيع الإلكتروني غير أنه تناول جريمة واحدة تتعلق مباشرة بالتوقيع الإلكتروني و هيا جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف المنصوص و المعاقب عليها بموجب المادة 68 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين. غير أنها تشمل مجموعة من الصور أو السلوكات لا تقل أهميتا من باقي الجرائم السابق ذكرها سواء المتعلقة بخدمة التصديق الإلكتروني أو ببيانات شهادة التصديق . حيث تعد متكاملة فيما بينها لتحقيق حماية التوقيع الإلكتروني للمستهلك . و عليه سوف نحاول تحديد أركان هذه الجريمة و العقوبة المقررة لها .

أولا: الركن المادي لجريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير

تعد جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير من الجرائم الشكلية لا تتطلب لقيامها حدوث نتيجة معية، بل يكفي لقيامها إتيان السلوك المجرم، و يقوم السلوك الإجرامي في هذه الجريمة على ثلاثة صور الحيازة أو الإفشاء أو الاستعمال ، و سنحاول تحديد كل سلوك على حدى :تتمثل

1-حيازة بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير:

وهي حيازة برنامج أو نظام معلوماتي لإعداد توقيع إلكتروني خاصة بالغير دون موافقة صاحبه والحيازة المشروعة لهذا البرنامج أو النظام المعلوماتي لا عقاب عليها طالما أن الشخص مرخص له بهذه الحيازة من الجهة المتخصصة بهدف توثيق هذه التوقيعات طالما لم يثبت أن نيته قد اتجهت إلى استخراج توقيع إلكتروني رغما عن إرادة صاحبة[1].

و يمكن حيازة بيانات التوقيع الإلكتروني عن طريق اختراق بيانات التوقيع الإلكتروني بالدخول غير مشروع للنظام المعلوماتي المتضمن للتوقيع الإلكتروني، أو اعتراضه أو بأي وسيلة كانت[2].

2- إفشاء بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير:

يتمثل هذا السلوك في إفشاء بيانات التوقيع الإلكتروني، أي نشرها و إطلاع الغير عليها، بعد أن كان العلم بها قاصرا على صاحبها. و يكون إفشاء بيانات إنشاء توقيع إلكتروني بالتعدي على البيانات المشفرة أو فض المعلومات المشفرة التي تخص بيانات إنشاء التوقيع الإلكتروني والتي تكون مرتبطة بأجهزة أو برامج معلوماتية[3].

3 – استعمال بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير:

إن استعمال بيانات إنشاء التوقيع الإلكتروني تشبه جريمة تزوير التوقيع العادي، فالتوقيع الإلكتروني لا يمكن تقليده، و أنما يمكن استعماله دون علم مالكه باعتباره يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، فيما

---

[1] – لالوش راضية، أمن التوقيع الإلكتروني، مذكرة ماجستير في القانون العام ، كلية الحقوق ، جامعة مولود معمري ، تيزي وزو،2012، ص154.

[2] – لقد أحسن المشرع الوطني صنعا حينما لم يحدد وسيلة على سبيل الحصر لارتكاب الفعل المجرم في هذه الجريمة، لكنه خلافا لبعض التشريعات لم يجرم محاولة الحيازة على بيانات توقيع إلكتروني.

[3] – بلحسني حمزة ، "**الحماية القانونية و الفنية للتوقيع الإلكتروني في مجال البيئة الرقمية**" ، مجلة العلوم القانونية و الإدارية ، العدد الحادي عشر،2015، ص82.

يتم تزوير التوقيع التقليدي بتقليد توقيع شخص آخر مما يعني أن التوقيع ذاته مختلف عن التوقيع الخاص بصاحبه، و ذلك لأن التوقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي و بالتالي لا يمكن أن و يكون متماثل معه[1].

أما في جريمة استعمال بيانات إنشاء التوقيع الإلكتروني فانه يتم الحصول على منظومة التوقيع الإلكتروني الخاص بشخص آخر، و بالتالي التوقيع الإلكتروني في حد ذاته صحيح لم يطرأ عليه تعديل أو تغيير، بل تم **استخدامه** دون رضا مالكه، حيث يكون الجاني قد تحصل على منظومة التوقيع الإلكتروني بطريقة غير مشروعة بنية استخدامها في توقيع وثيقة معلوماتية، أو كانت حيازته لها مشروعة كالأشخاص الخاصة بتصديق التوقيع الإلكتروني المرخص لهم و استعملوها دون علم و رضا صاحبها.

و لذلك فجريمة تزوير التوقيع التقليدي تختلف عن جريمة تزوير التوقيع الإلكتروني سواء في طريقة التزوير أو في أسلوب اكتشاف هذا التزوير، فطريقة الكشف عن التوقيع التقليدي المزور تكون عن طريق مضاهاة التوقيع المزيف بتوقيع الشخص المنسوب إليه هذا التوقيع، بينما في حالة تزوير التوقيع الإلكتروني لا يمكن استخدام تلك الطريقة لاكتشاف تزوير التوقيع، إذ أن التوقيع سليم لكنه ليس صادرا من الشخص مالك منظومة التوقيع الإلكتروني[2].

ثانيا: الركن المعنوي لجريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير.

تعتبر جريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني خاص بالغير، من الجرائم العمدية حيث يأخذ فيها الركن المعنوي صورة القصد الجنائي العام

[1] – منير محمد الجنيهي، ممدوح محمد الجنيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص 54.

[2] – منير محمد الجنيهي، ممدوح محمد الجنيهي، المرجع السابق، ص 55.

بعنصريه العلم و الإرادة، فلا بد أن يعلم الجاني بانه يحوز بيانات خاصة بالغير ، أو التصرف فيها إما بالإفشاء أو الاستعمال، و أن تتجه إرادته للقيام بالفعل المجرم[1].

ثالثا: العقوبة المقررة لجريمة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير.

أقر المشرع الوطني لهذه الجريمة من خلال نص المادة 68 من قانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين عقوبة الحبس ثلاثة أشهر(03) إلى ثلاث سنوات (03) و غرامة مالية تتراوح بين 100.000 دج إلى 500.000دج. كما أجاز للقاضي حرية النطق بإحدى هاتين العقوبتين فقط.

أما الشخص المعنوي الذي يرتكب هذه الجريمة فقد قرر له المشرع من خلال المادة 75 السابق ذكرها عقوبة مالية تقدر بمضاعفة خمس مرات الحد الأقصى للعقوبة المالية المقررة للشخص الطبيعي، وعليه تكون الغرامة المقررة للشخص المعنوي هيا (2.500.000) دينار جزائري.

[1] – حمزة بلحسني، المقال السابق، ص 84.

خلاصة الباب الأول

إن ظهور المعاملات الإلكترونية هو أحد روافد ثورة التكنولوجيا و المعلومات، و نتيجة حتمية للنمو السريع و المتطور في استخدام شبكة الإنترنت الدولية، غير أن انتشار الأنترنت و تنامي استخدامه في المعاملات التجارية الإلكترونية، ازدادت معه الجرائم المصاحبة لاستعمال الشبكة خاصة المتعلقة بغش المستهلك باعتباره الطرف الضعيف في العلاقة الاستهلاكية، أو تلك المتعلقة بمتطلبات إتمام هذا النوع من المعاملات.

و لما كان هذا النوع المستحدث من الجرائم المعلوماتية يشكل تهديدا و تحديا خطيرا على اقتصاد الدول بصفة عامة و مصالح المستهلك الإلكتروني خاصة، كان لازما على المشرع الوطني توفير الحماية للمستهلك الإلكتروني و ذلك بوضع نصوص تجرم كل اعتداء عليه في هذا النوع من المعاملات الإلكترونية، فمنها ما يتعلق بتجريم الغش التجاري في المعاملات الإلكتروني، و الذي بدوره يمكن تقسيمه إلى غش يرتكب قبل التعاقد الإلكتروني، و غش يرتكب عند التعاقد الإلكتروني.

أما حماية متطلبات المستهلك في المعاملات الإلكترونية، و نظرا لأهمية هذه المتطلبات في إتمام المعاملات الإلكترونية أفرد لها المشرع الوطني من خلال مجموعة من النصوص حماية خاصة سواء منها التعلق بحماية البيانات الشخصية للمستهلك عند معالجتها إلكترونيا أو تلك المتعلقة بالتوقيع الإلكتروني للمستهلك.

الباب الثاني: الحماية الجزائية الإجرائية للمستهلك في المعاملات الإلكترونية

إن المشرع عندما قرر حماية المستهلك في المعاملات الإلكترونية من مختلف الاعتداءات التي تمسه أو الخطر الذي يهدده فإنه سن عدة تشريعات سواء ما كان متعلقا بالغش التجاري في المعاملات الإلكترونية أو حماية متطلباته في هذا النوع الحديث من المعاملات، المنصوص عليها في عدة قوانين بدأ بقانون العقوبات أو القوانين المكملة له كقانون التجارة الإلكترونية أو قانون التوقيع و التصديق الإلكترونية إلى قانون حماية المعطيات الشخصية، و الهدف من خلالها هو معاقبة كل من تسول له نفسه الإضرار بالمستهلك الإلكتروني.

غير أن فاعلية نصوص التجريم و العقاب التي تشكل مضمون حق الدولة في العقاب ترتبط إلى حد كبير بمدى دقة و نجاعة القواعد الإجرائية التي تحدد إجراءات دعوى الحق العام، التي من شأنها أن تضمن اقتضاء الحق المتضمن و المحدد في القواعد الموضوعية، و هو حق الدولة في العقاب، فمن خلالها تقوم ولاية الجهة القضائية المختصة بنظر الجرائم الماسة بالمستهلك الإلكتروني، و عمل جميع السلطات سواء الاستدلالية و الخاصة بالتحقيق، أو ما يعرف بتنظيم قواعد الاختصاص القضائي، كما تعمل هذه النصوص الإجرائية على تحديد وسائل كشف هذه الجرائم و إعطاء حجتها أما مختلف الجهات القضائية.

و عليه سوف نبحث من خلال هذا الباب عن تنظيم قواعد الاختصاص القضائي في نظر الجرائم الماسة بالمستهلك في المعاملات الإلكترونية (الفصل الأول) ونناقش إثبات الجرائم الماسة بالمستهلك في المعاملات الإلكترونية (الفصل الثاني).

الفصل الأول: تنظيم قواعد الإختصاص في نظر الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

تتمتع المعاملات الإلكترونية عبر شبكة الأنترنت بصبغة ذات بعد عالمي، ذلك أنها لا تخضع لدولة أو كيان معين، حيث تقوم هذه المعاملات عبر شبكات عالمية مختلفة، مما يثير إشكالية جوهرية تقوم على تحديد الجهة القضائية المختصة بتطبيق الأوصاف الجزائية التي يمكن أن تأخذها الجرائم المرتكبة على المستهلك الإلكتروني عبر هذه الأخيرة، و تحديد الآليات و القواعد الإجرائية المعتمدة في هذا التطبيق.

الأمر الذي يستدعي بحث المسائل المتعلقة بالاختصاص القضائي عن الجرائم الماسة بالمستهلك الإلكتروني، وعن مدى نجعتها في قمع الجرائم التي تقع على المستهلك في المعاملات الإلكترونية، و ذلك من خلال البحث عن الأحكام الجزائية المتعلقة بانعقاد الإختصاص الجزائي لمثل هذه الجرائم (المبحث الأول)، و البحث عن دور التعاون الدولي في تعزيز قواعد الإختصاص القضائي الوطني للحد من هذه الجرائم تحقيقا لحماية فعالة و متكاملة للمستهلك في المعاملات الإلكترونية (المبحث الثاني).

المبحث الأول: انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

يقصد بقواعد الإختصاص القضائي تلك الضوابط أو النصوص التي يخول بمقتضاها القانون لجهة قضائية معينة سلطة الفصل في دعوى معينة، حيث يحدد بمقتضاها اختصاصات كل من سلطات البحث و التحري والتحقيق و المحاكمة[1]. و قواعد الإختصاص القضائي في المادة الجزائية وفقا لهذا المعنى من النظام العام يترتب على مخالفتها البطلان المطلق فلا يجوز التنازل عنها صراحة أو ضمنا كما أنه لا يمكن تصحيحها بالسكوت عنها أو الرضا بها، و يجوز إثارتها في أي مرحلة كانت عليها الدعوى الجزائية و لو كان ذلك لأول مرة أما المحكمة العليا و من أي طرف كان في الدعوى العمومية، كما يمكن للقاضي الجزائي أن يصح بعدم اختصاصه و من غير طلب الأطراف متى كانت الوقائع المعروضة عليه لا تدخل ضمن اختصاصه الوظيفي تبعا للمبادئ و القواعد التي تحكم الإختصاص الجزائي[2].

و قد أولى المشرع مسألة الإختصاص الجزائي أهمية بالغة فنظم القواعد و المبادئ التي تحكمه (المطلب الأول)، و عالج وسائل إنفاذ هذه القواعد و تطبيق أحكامه (المطلب الثاني).

[1] – مدحت محمد عبد العزيز إبراهيم، القواعد العامة في مسائل الاختصاص لمأموري الضبط القضائي و أعضاء النيابة العامة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2014، ص 11.

[2] – مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، الجزء الثاني، دار الفكر الجامعي، مصر، 1988، ص 59.

المطلب الأول: قواعد الإختصاص القضائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

إن قواعد الإختصاص القضائي في نظر الجرائم الماسة بالمستهلك في المعاملات الإلكترونية تخول بمقتضاها للجهات القضائية سلطة الفصل في الدعاوى المرفوعة بشأن هذه الجرائم، و عليه سنحاول تحديد ضوابط انعقاد الإختصاص القضائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية (الفرع الأول)، و القيود الواردة عليه (الفرع الثاني).

الفرع الأول: ضوابط انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني

ينعقد الإختصاص القضائي بشأن الجرائم الماسة بالمستهلك الإلكتروني بمبادئ عامة تحكم سريان نصوص التجريم على الوقائع محل النظر خاضعة بذلك لمجموعة من المبادئ و و المعايير الإجرائية التي تحكم توزيع الإختصاص الجزائي. و عليه سنحاول تحديد مبادئ انعقاد الاختصاص القضائي بشأن الجرائم الماسة بالمستهلك في المعاملات الإلكترونية (الفقرة الأولى)، ثم تحديد معايير انعقاده (الفقرة الثانية).

الفقرة الأولى: مبادئ انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني

تحكم قواعد الإختصاص القضائي بشأن الجرائم الماسة بالمستهلك في المعاملات الإلكترونية من الناحية المكانية مبادئ عدة أولها أساسي و هو مبدأ إقليمية القاعدة الجزائية، و الأخرى احتياطية –مبدأ الشخصية و مبدأ العينية– يتم اللجوء إيها حالة قصور المبدأ الرئيسي أو عجزه في متابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني. و سنحاول التطرق بشكل من التفصيل لكل هذه المبادئ بدأ بالأساسي و هو مبدأ إقليمية القاعدة الجزائية (أولا) و مبدأ شخصية القاعدة الجزائية (ثانيا)، ثم مبدأ عينية القاعدة الجزائية (ثالثا).

أولا: مبدأ إقليمية القاعدة الجزائية

يقصد بمبدأ الإقليمية أن يخضع كل من يرتكب عمل إجرامي على إقليم[1] الدولة لقانون العقوبات المعمول به لتلك الدولة، و لا فرق في ذلك بيم مواطن أو أجنبين و سواء مصلحة الدولة صاحبة السيادة على الإقليم أو هددت مصلحة لدولة أجنبية[2] ، و تطبيقا لهذا المبدأ نص قانون العقوبات الجزائري في المادة الثالثة منه على أنه " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية..."، بمعنى سريان القانون الجزائري على كافة الجرائم الواقعة على إقليم الجمهورية، بصرف النظر عن جنسية الجاني و المجني عليه فيها سواء كان جزائريا أو أجنبيا، كما هذا المبدأ أساسه في الجرائم الإلكترونية بما فيها الماسة بالمستهلك الإلكتروني من خلال المادة 15 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام و الاتصال، و التي تنص على " زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة ..."

و لمبدأ الإقليمية وجهان، وجه سلبي يتمثل في تطبيق قانون الدولة على جميع الجرائم المرتكبة على إقليمها بغض النظر عن جنسية الجاني أو المجني عليه، و بغض النظر عن المصلحة المستهدفة سواء أكانت مصلحة الدولة أو مصلحة دولة أجنبية، أما الوجه الثاني فهو سلبي، و يعني عدم تطبيق قانون الدولة على الجرائم التي ترتكب خارج إقليمها[3].

و يجد هذا المبدأ مبرراته في كونه مظهر من مظاهر سيادة الدولة، حيث يعتبر تطبيق القانون الجنائي لدولة ما على إقليمها أحد مظاهر سيادتها هاذا من جهة، و من

---

[1] – يشمل إقليم الدولة ثلاث عناصر الإقليم البري و يحدد بالحدود السياسية للدولة، و الإقليم البحري الذي هو جزء من البحر العام الذي يلاصق شواطئ الدولة و المحدد ب 12 ميل، و يشمل كذلك الإقليم الجوي و هو الذي يشمل كل طبقات الهواء التي تعلوا الإقليم الأرضي و البحري. **أنظر د/ محمود نجيب حسني، شرح قانون العقوبات القسم العام، المجلد الأول، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، ص 182.**

[2] – د/ محمود نجيب حسني، شرح قانون العقوبات القسم العام، المرجع السابق ص 189.

[3] – نظام توفيق المجاني، شرح قانون العقوبات القسم العام، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2009، ص 109.

جهة أخرى إن مكان وقوع الجريمة أنسب لمحاكمة المتهم، بسبب توافر أدلة إثبات الجريمة فيه[1].

و ينعقد الإختصاص وفقا لهذا المبدأ بتحقق أحد العناصر المكونة للجريمة سلوكا أو نتيجة[2]، كما أن هذا المبدأ يسمح بمتابعة كل من ارتكب أحد العناصر المكونة للجريمة و لو كان الفعل غير معاقب عليه في بلد المنشأ الأصلي أي بداية السلوك الإجرامي فبمجرد اقتراف أحد سلوكيات الجريمة في القطر الوطني ينعقد الاختصاص للقاضي الوطني[3]، كما يمكن بناء على هذا المبدأ متابعة الجاني خارج القطر الوطني متى كان مساهما أو شريكا في الجريمة التي وقعت داخل القطر لأن العبرة بمكان وقوع الجريمة[4].

غير أن هذا المبدأ يجد صعوبة و إشكالات كبيرة في تطبيقه بالنسبة للجرائم الإلكترونية الماسة بالمستهلك و هذا بالنظر لطبيعتها و الخصائص التي تتميز بها عن الجرائم التقليدية و خصوصا صعوبة تحديد مكان وقوعها و ارتكابها بدقة.

لذا تصدت اتفاقية بودابيست لهذه الإشكالية حيث أشارت في المادة 22 إلى المبادئ التي يجب على الدول الأطراف اعتمادها لتحديد الاختصاص القضائي المتعلق بالجرائم الواقعة في بيئة الأعمال الإلكترونية، حيث أكدت المادة السالفة الذكر على كل دولة طرف بضرورة العقاب على ارتكاب هذه الجرائم حتى و لو كان المجرم خارج إقليم الدولة، فيعد الإختصاص منعقدا إذا كان نظام حاسوب المعتدي داخل إقليم الدولة و هو خارجها، أو كان نظام الحاسوب العائد للضحية ضمن النطاق الإقليمي، أو كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة، كما أشارت الفقرة الرابعة من المادة السالفة الذكر أنه يجوز للأطراف اتخاذ أشكال أخرى من معايير الاختصاص بما يتناسب مع قانونها

[1] – رمسيس بنهام، قانون العقوبات (النظرية العامة للقانون الجنائي)، الطبعة الثالثة، منشأ المعارف، الإسكندرية، 1997، ص 242.

[2] – المادة 586 من قانون الإجراءات الجزائية " تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر".

[3] – هدى طلب على، الإثبات الجنائي في جرائم الأنترنت و الاختصاص القضائي بها، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2012، ص 156.

[4] – محمد زكي أبو عامر، قانون العقوبات القسم العام، دار الجامعة الجديدة للنشر، الإسكندرية، 2015، ص 87.

الداخلي[1]، و إذا كانت الجريمة الواقعة في بيئة الأعمال الإلكترونية تدخل في اختصاص أكثر من دولة فإن هذه الدولة تتشاور فيما بينها لتحديد المكان الملائم للمحاكم حتى يتم تجنب ازدواج التخصص.

و عليه فإنه وفقا لهذا المبدأ ينعقد الإختصاص للقضاء الجزائري لمتابعة الجرائم الماسة بالمستهلك الإلكتروني سواء بتحقيق السلوك الإجرامي لها على الإقليم الوطني ، و يكون ذلك إذا كان نظام حاسوب المعتدي داخل إقليم الدولة و هو خارجها، أو كان نظام الحاسوب العائد للضحية ضمن النطاق الإقليمي، أو كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة ، و بالرغم من هذه الأهمية و هذا الدور الذي يلعبه مبدأ إقليمية النص الجنائي إلا أنه يظل قاصرا عن سريان قانون العقوبات الجزائري و القوانين المكملة عند ارتكاب الجرائم خارج إقليمها خاصة الجرائم الماسة بالمستهلك الإلكتروني التي تتميز بطابعها العابر للحدود ، مما يفرض ضرورة إعمال مبادئ أخرى[2].

ثانيا: مبدأ شخصية القاعدة الجزائية

يعتبر مبدأ الشخصية من أهم المبادئ التكميلية لمبدأ الإقليمية[3]، و ذلك في الحالات التي لا يمكن تطبيق القاعدة الأصيلة (مبدأ الإقليمية) على الجرائم المنصوص عليها في قانون الدولة، فالمواطن الذي يرتكب جريمة في الخارج ثم يعود لوطنه قد يفلت من العقاب

[1] – د/ محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2011، ص 200.

[2] – مصطفى العوجي، القانون الجنائي، منشورات الحلبي الحقوقية، بيروت لبنان، 2006، ص 357.

[3] – قد كان لمبدأ شخصية النص الجنائي أهمية كبيرة فيما مضى، إذ كان الأصل في القوانين كافة أنها شخصية تلاحق رعايا الدولة أينما كانوا، و لكن هذا المبدأ تقلص نفوذه حينما أصبحت سيادة الدولة الحديثة مرتكزة إلى أساس إقليمي لا شخصي، و قد ترتب على ذلك أن أصبح الأصل في النص الجزائي إقليمية، مع بقاء دوره في إعطاء النص الجزائي نطاق أوسع مما يسمح به مبدأ الإقليمية. **أنظر محمود نجيب حسني، شرح قانون العقوبات، المرجع السابق، ص 200-201.**

لأنه لا يخضع لقانون وطنه طبقا لمبدأ الإقليمية بسبب ارتكابه جريمة خارج إقليمها، و لذلك و حتى لا يفلت من العقاب كان لزما الأخذ بمبدأ شخصية القانون الجنائي[1].

و يعني مبدأ الشخصية امتداد القانوني الجنائي للدولة إلى الجرائم المرتكبة خارج إقليمها ممن يرتبط بتك الدولة بعلاقة معينة[2]، و لهذا المبدأ وجهان أحدهما إيجابي يتمثل في استطاعة الدولة تطبيق قانونها على الجرائم التي يرتكبها مواطنوها خراج نطاق حدود إقليمها، أما وجها السلبي استطاعة الدولة أن تعاقب على الجريمة التي يكون المجني عليه فيها من رعياها[3].

و لمبدأ الشخصية في وجهه الإيجابي أهمية واضحة، إذ هو الوسيلة التي تجنب فرار المجرم من العقاب إذا ارتكب جريمته خارج إقليم دولته ثم عاد إليها بعد جريمته، و بيان ذلك أن دولته لا تستطيع وفقا لمبدأ الإقليمية أن تعاقبه، لأنه لم يرتكب جريمة في إقليمها[4]، أما هذا المبدأ في وجهه السلبي، فهو مقتصرة على تمكين الدولة من حماية رعاياها إذا تعرضوا لاعتداء جرمي و هم في خارج إقليمها، فهو صورة لحماية الدولة بعض مصالحها، و هو بذلك اقرب إلى مبدأ عينية النص الجنائي[5].

و لقد نص المشرع الجزائري على هذا المبدأ، و ذلك في المواد 582 و 583 من قانون الإجراءات الجزائية بوجهه الإيجابي و السلبي، إذ يشترط لإعمال هذا المبدأ أن تكون الجريمة من وصف جناية في قانون العقوبات الجزائري، أما إذا كانت جنحة فيشترط أن تكون لهذا الوصف في القانون الجزائري و الأجنبي مع تقديم شكوة، أما الشرط الثاني فيتمثل في أن يرتبط المواطن الذي يحمل الجنسية الجزائرية جريمة في الخارج ثم يعود للوطن، أما الشرط الثالث فيجب أن لا يكون قد حكم عليه في الخارج.

---

[1] – د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2002، ص 57.

[2] – هدى طلب على، المرجع السابق، ص 171.

[3] – د/ زهير الزبيدي، الاختصاص الجنائي الدولي في القانون الدولي، 1980، ص 390.

[4] – إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية، أطروحة دكتوراه، كلية الحقوق و العلوم السياسي، جامعة باتنة، الجزائر، 2016، ص 208.

[5] – محمود نجيب حسني، شرح قانون العقوبات القسم العام، المرجع السابق، ص 202.

و عليه فإن مبدأ الشخصية خاصة في وجهه السلبي يكون القضاء الجزائري مختص في نظر الجرائم الماسة بالمستهلك الإلكتروني الذي تربطه علاقة الجنسية بها حتى و لو ارتكبت عليه في دولة أخرى، غير أن هذا المبدأ قد يجد صعوبة في تطبيقه على هذه الجرائم ، حيث يعتمد بصفة أساسية على كشف هوية الجاني التي تعد صعبة جدا في البيئة الإلكترونية، غذ يستعمل الجناة أساليب التشفير و الأسماء المستعارة.

ثالثا: مبدأ عينية القاعدة الجزائية

يعتبر مبدأ العينية مبدأ مكمل أيضا لمبدأ الإقليمية في تطبيق قانون العقوبات، و يقصد به المبدأ تطبيق القانون الجنائي على الجرائم التي تمس المصالح الأساسية للدولة، و المرتكبة خارج إقليمها، أيا كانت جنسية مرتكبها[1]. و عليه فإن مبدأ العينية يباشر بصفة خاصة أي يقتصر على طائفة معينة من الجرائم تؤدي إلى الإضرار بالمصالح الأساسية أو الجوهرية للدولة، أما من حيث صفة الجاني فيمارس هذا الإختصاص على كل أجنبي بوجه عام أي مهما كانت جنسية الفاعل.

و يجد هذا المبدأ مبرره في أن الجرائم الماسة بالمصالح الأساسية و الجوهرية للدولة عندما ترتكب في الخارج فليس من المؤكد أن تهتم الدول التي ارتكبت هذه الجرائم على إقليمها بمعاقة الجاني عليها[2]، كما يعتبر هذا المبدأ الصيغة العملية التي تتمسك بها الدول للحفاظ على مصالحها الأساسية و الجوهرية من التهديد الموجه ضدها من مصادر خارجية[3].

حيث نصى القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات لسنة 2004 أنه تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه، حتى و

[1] – محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت، المرجع السابق، ص 220.

[2] – د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص 53.

[3] – د/ زهير الزبيدي، مرجع سابق، ص 268.

لو ارتكبت كليا أو جزئيا خارج إقليم الدولة متى أضرت بإحدى مصالحها، و يختص القضاء الوطني بنظر الدعاوى المرتبة عليها[1].

و لقد نص المشرع الجزائري على مبدأ العينية في المادة 588 من قانون الإجراءات الجزائية بحيث يجوز متابعة و محاكمة كل أجنبي سواء فاعلا أو شريك ، إذا ألقي عليه القبض أو حصلت الحكومة على تسليمه وفقا للقانون الجزائري إذا ارتكب جناية أو جنحة ضد سلامة الدولة الجزائرية أو تزييفا للنقود أو أوراق مصرفية وطنية متداولة قانونا ، أو إضرارا بمواطن جزائري.

و أكد المشرع الجزائري أيضا على تطبيق هذا المبدأ في الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال من خلال المادة 15 من قانون الوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، و التي جاء فيها " زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبي و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني".

و عليه فإن اختصاص المحاكم الوطنية وفق مبدأ العينية ينظر حتى في الجرائم الإلكترونية التي تستهدف مصلحة المستهلك باعتبارها حماية للاقتصاد الوطني.

[1] – أنظر المادة 26 من القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات لسنة 2004.

الفقرة الثانية: معايير انعقاد الإختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني

إضافة إلى تحديد المبادئ التي تحكم انعقاد الإختصاص القضائي بشأن الجرائم الماسة بالمستهلك الإلكتروني اتجه المشرع الإجرائي الجزائري نحو ضبط المعايير التي تحكم الاختصاص بظر هذه الجرائم، فوضع قواعد عامة عادية لهذه المعايير (أولا)، كما أجاز الخروج عنها عن طريق ما يعرف بتمديد الإختصاص (ثانيا).

أولا: المعايير العادية لانعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكترونية

ينعقد الإختصاص القضائي بنظر الجرائم الماسة بالمستهلك الإلكتروني جزائيا في الأصل بإعمال ثلاث معايير (المعيار الشخصي و معيار نوعي، و آخر محلي). و سنحاول تحديد كل منها على النحو التالي:

1-المعيار الشخصي:

يقوم المعيار الشخصي على أساس صفة أو حالة خاصة بالمتهم المرفوعة ضده الدعوى الجزائية، أي أن يكون من الأشخاص الخاضعين لسلطة المحكمة[1].

و يحكم هذا النوع من الإختصاص مبدأ عام يتمثل في عدم الاعتداد بشخص المتهم في تحديد الإختصاص، و مفاده خضوع جميع الأشخاص الذين ارتكبوا جريمة لذات القضاء، فلا تفرقة بين الناس تبعا لجنسياتهم أو مراكزهم الاجتماعية من أجل الخضوع لجهات قضائية معينة، و يعد هذا المبدأ نتيجة حتمية لمبدأ المساواة بين

[1] – محمد سعيد نمور، أصول الإجراءات الجزائية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2005، ص 417.

الأفراد[1]. و عليه فإنه وفقا لهذا المبدأ فإن القضاء الجنائي يختص بنظر كل الجرائم الإلكترونية بما فيها الماسة بالمستهلك الإلكتروني مهما كانت صفة مرتكبها.

غير أن هذا المبدأ غير مطلق، إذ يتقيد هذا المعيار أحيانا بصفة المتهم أو حالته وقت ارتكاب الجريمة لا وقت رفع الدعوى، و الأمر هنا يتعلق بتلك الفئة من الأشخاص التي خصها المشرع بمحاكم خاصة، إما بسبب صغر السن و إما بسبب الوظيفة أو الصفة[2].

إذ خص قانون الإجراءات الجزائية الجزائري الأحداث الجانحين بأحكام خاصة في المواد من 442 إلى 494 منه، و ذلك بإنشاء في كل محكمة قسم للأحداث يختص بنظر الجنح و الجنايات التي يرتكبها الأحداث دون سن الثامنة عشر[3]، و هو ما يعني أن المشرع قد ميز الأحداث بتخصيص قضاء معين لمحاكمتهم، بسبب الطابع الخاص لإجرام هذه الفئة سواء من حيث أسبابه أو أساليب علاجه، و هذا يتطلب قضاة لديهم الخبرة في التعامل مع هؤلاء المجرمين، كما يتطلب إجرامهم اتخاذ إجراءات خاصة غير مطبقة في المحاكم العادية حماية لنفسية الطفل و مستقبله[4].

كما يختص القضاء العسكري بمحاكمة العسكريين دون سواه في الجرائم التي يرتكبها العسكريين أو من في حكمهم في الخدمة أو المرتكبة داخل مؤسسة عسكرية أو

---

[1] – د/ محمود نجيب حسني، شرح قانون الإجراءات الجزائية وفقا لأحدث التعديلات التشريعية، الجزء الأول، دار النهضة العربية، القاهرة، 2013، ص 803.

[2] – د/ محمود نجيب حسني، شرح قانون الإجراءات الجزائية وفقا لأحدث التعديلات، الجزء الثاني، دار النهضة العربية، القاهرة، 2013، ص 741.

[3] – أنظر المادة 59 من قانون 15–12 المؤرخ في 15 يوليو 2015 المتعلق بحماية الطفل الجزائري ، جريدة رسمية رقم 39 المؤرخة في 20 يوليوا 2015.

[4] – أجعود سعاد، حماية حق المتهم في محاكمة عادلة في التشريع الجزائي الجزائري، أطروحة دكتوراه، كلية الحقوق، جامعة عنابة، 2016، ص 165.

لدى المضيف[1]، و يستوي في ذلك أن يكون مرتكب الجريمة عسكريا أو مدنيا، فاعلا أصليا أو شريك[2].

وبناء على ما سبق فإن تحديد المحكمة المختصة في الجرائم الماسة بالمستهلك الإلكتروني يتوقف على صفة مرتكبها ، فإن كان مرتكبها الحدث فينعقد الاختصاص لقسم الأحداث في المحاكم وفقا للمادة 451 من قانون الإجراءات الجزائية، أما إذا كان مرتكبها عسكري فإن الإختصاص يؤول للقضاء العسكري، و ما عدا ذلك فالقضاء العادي هو صاحب الولاية في نظرها.

2-المعيار النوعي:

يقصد بالإختصاص النوعي توزيع الإختصاص داخل القضاء الواحد بعد أن ينعقد له الإختصاص الشخصي، و الضابط في توزيع الدعوى ضمن القضاء العادي هو جسامة الجريمة[3]، أي أن الضابط في تحديد الإختصاص النوعي يكون بالنظر إلى الوصف القانوني للجريمة فيما إن كانت تشكل جناية أو جنحة أو مخالفة و لا تكون بالنظر إلى نوع العقوبة التي تقررها المحكمة[4].

إذ يقسم المشرع الجزائري المحاكم إلى نوعين، محاكم الجنايات و التي تختص بالقضايا التي من نوع جناية التي تتعدى عقوبتها السجن 5 سنوات او السجن المؤبد أو الإعدام[5]، كجريمة مخالفة التزام ضمان أمن المنتوجات في المعاملات الإلكترونية، يحث تكون بوصف جناية وفقا للفقرة الثانية و الثالثة من المادة 83 من قانون 09-03 المتعلق

---

[1] – أنظر المادة 28 من الأمر رقم 71 – 28 المؤرخ في 22 أفريل 1971 المتضمن قانون القضاء العسكري، الجريدة الرسمية، عدد 38، المؤرخة في 11 مايو سنة 1971.

[2] – د/ جيلالي بغدادي، التحقيق دراسة مقارنة نظرية و تطبيقية، الديوان الوطني للأشغال التربوية، الجزائر، 1999، ص 105 .

[3] – د/ محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت، المرجع السابق، ص 226.

[4] – إلهام بن خليفة ، الرسالة السابقة ، ص 227.

[5] – انظر المادة 5 من قانون العقوبات المعدل و المتمم.

بحماية المستهلك و قمع الغش، إذا تسبب المنتوج الغير آمن في مرض غير قابل للشفاء أو في فقدان استعمال عضو أو في حالة الإصابة بعاهة مستديمة، و تكون العقوبة السجن من 10 سنوات إلى 20 سنة و غرامة مالية من 1.000.000 دج إلى 2.000.000 دج . أما إذا تسبب هذا المرض في وفاة شخص أو عدة أشخاص تكون العقوبة السجن المؤبد[1]. حيث يكون التحقيق فيها وجوبا أمام قاضي التحقيق و غرفة الاتهام.

أما النوع الثاني فهو محكمة الجنح و المخالفات، التي لا تتعدى عقوبتها الحبس خمس سنوات[2] إذ تعبر اغلب الجرائم الماسة بالمستهلك الإلكتروني من قبيل الجنح سواء ما تعلق بجرائم الغش التجاري في المعاملات الإلكترونية او تلك المتعلقة بمتطلباته في هذا النوع المستحدث من المعاملات التجارية.

3-المعيار المحلي:

إن المعيار الشخصي و النوعي غير كافيين لتحديد الجهة القضائية المختصة في نظر الجرائم الماسة بالمستهلك الإلكتروني، حيث يجب معرفة المحكمة المختص إقليميا بنظر هذه الجرائم و هو ما يعرف بالمعيار المحلي[3]، و يتحدد اختصاص المحكمة إقليميا بموجب ثلاثة ضوابط و هي: مكان وقوع الجريمة، أو مكان إقامة المتهم أو مكان القبض عليه[4].

---

[1] – انظر الفقرة 2 و 3 من المادة 83 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

[2] – انظر المادة 5 من قانون العقوبات المعدل و المتمم.

[3] – محمد سعيد نمور، المرجع السابق، ص 435.

[4] – أما بالنسبة للأحداث فقد حدد المشرع الوطني معايير انعقاد الاختصاص من خلال المادة 60 من قانون 15-12 المتعلق بالطفل، و هيا مكان ارتكاب الجريمة أو التي بها محل إقامة الطفل الجانح، أو ممثله الشرعي أو المحكمة التي عثر فيها على الطفل أو المكان الذي وضع فيه.

أ-اختصاص المحكمة محليا بمكان وقوع الجريمة:

لقد رسخ المشرع الجزائري مكان وقوع الجريمة كاختصاص محلي لمتابعة المتهم سواء كان شخصا طبيعيا أو معنويا[1]، و يجد هذا الضابط مبرره في أن متابعة مرتكب الجريمة الإلكترونية و محاكمته و معاقبته تكون بالمكان الذي أخل فيه بالنظام العام، و أين شعر قاطنوه بآثار النشاط الإجرامي، و مكان ارتكاب الجريمة هو المكان الذي تحققت فيه أحد عناصر الركن المادي من أعمال التنفيذ و البدا في التنفيذ و بصرف النظر عن الأعمال التحضيرية السابقة عليها و النتائج التالية لها ، حيث لا مشكلة إذا كان الركن المادي بأكمله تحقق في دائرة اختصاص محكمة معينة، و لكن تثار المشكلة عندما يتحقق أحد العناصر في دائرة اختصاص محكمة معينة و تحققت باقي العناصر في دوائر اختصاص محاكم أخرى، و لقد قضت محكمة النقض المصرية أن جميع هذه المحاكم تكون مختصة بنظر الجريمة[2].

ب-اختصاص المحكمة محليا تبعا لمحل إقامة الشخص الطبيعي و وجود مقر الاجتماعي للشخص المعنوي:

لقد جعل المشرع الجزائري من محل إقامة الشخص الطبيعي و المقر الاجتماعي للشخص المعنوي أماكن صالحة قانونا لقيام اختصاص المحكمة محليا حين متابعة كلا من الشخصين جزائيا، و يجد هذا الضابط مبرره في أن محاكمة المتهم في محل إقامته فائدة كبرى إذ يسهل الوقوف على سوابقه و ماضيه من نفس الوسط الذي يعيش فيه، و قد يتعذر أحيانا معرفة المحل الذي وقعت فيه الجريمة فيتعين حينئذ محاكمته في محل إقامته[3].

---

[1] – انظر المادة 37 و 40 و 65مكرر1 من قانون الإجراءات الجزائية .

[2] – د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 806.

[3] – د/ جندي عبد المالك، الموسوعة الجنائية ، الجزء الأول،دار المؤلفات القانونية، بيروت لبنان، 1931، ص 362.

ج-اختصاص المحكمة محليا تبعا لمكان إلقاء القبض على المتهم:

مكان إلقاء القبض على المشتبه فيه الذي يفتح المجال لاختصاص المحكمة محليا ، هو مكان القبض الفعلي على المشتبه فيه، و في حالة تعدد المساهمين في الجريمة يكون مكان إلقاء القبض على أحدهم كافيا ليعود الاختصاص المحلي للمحكمة التي تم في دائرتها القبض و لو لسبب آخر[1]، و يتعلق هذا الضابط بالشخص الطبيعي دون المعنوي.

و تحديد مكان إلقاء القبض على المتهم له ما يبرره من حيث انه المكان الذي يكشف عن بعض المعالم التي تساعد القاضي في التحقيق، و انه المكان الذي وقع فيه المتهم في قبضة العدالة و هو يجنب السلطات مشقة و مصاريف نقله[2].

ثانيا: تمديد الإختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني

قد ينعقد الاختصاص لمحكمة جزائية في نظر الجرائم الماسة بالمستهلك الإلكتروني لا تدخل في اختصاصها طبقا لمعيار صفة المتهم أو نوع الجريمة أو المحل، و هو ما نسميه تمديد الاختصاص، و يكون ذلك في حالة تعدد الجرائم المسندة إلى المتهم و التي تضم جنايات و جنح و مخالفات و هذا يعني تعدد المحاكم المختصة بالنظر في كل منها رغم وحدة المتهم، أو في حالة تعدد المتهمين الذين تكون لهم مساهمة في ارتكاب سلوك إجرامي واحد[3]، إذ يخرج بعضهم عن الاختصاص الشخصي للمحكمة المختصة طبقا للقواعد العامة، و يتعين محاكمتهم أمام محكمة أخرى، فتتعدد كذلك المحاكم رغم وحدة الجريمة، إلا أن حسن إدارة العدالة يقتضي أن يتولى الفصل في هذه الجرائم محكمة واحدة تحسن تقدير ظروف و مسؤولية كل من المتهمين و تمكينها من فحص مجموعة من المشروعات الإجرامية ترتبط فيما بينها ارتباط وثيقا، بحيث يفسر بعضها بعضا،

---

[1] – انظر المادة 37 و 40 من قانون الإجراءات الجزائية المعدل و المتمم.

[2] – محمد سعيد نمور، المرجع السابق، ص 437.

[3] – د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 811.

فيخشى إذا توزع الاختصاص بها على عدد من القضاة أو المحاكم، ألا يتاح لأي منهم أن يحدد لما أختص به التقدير الواقعي السليم أو التكييف القانوني الصحيح الذي قد يكون متاحا لقاضي ينظر فيها مجتمعة، كما أن نظر محكمة واحدة فيها جميعا يحول دون أي تعدد للأحكام و تعارضها و يكفل عدالة أسرع و أقل تكلفة[1].

و حتى نكون أما تمديد الاختصاص وجب توفر حالتين من التعدد المادي و هيا التعدد الذي لا يقبل التجزئة و التعدد البسيط، فالتعدد المرتبط ارتباطا لا يقبل التجزئة يعني أن تتعدد الجرائم الماسة بالمستهلك الإلكتروني بتعدد الأركان المادية و المعنوية، و مع هذا التعدد قد يرتبط بعضها ببعض برباط وثيق يجعل كلا منها لا يتجزأ بحيث لا تكون قانونا إلا جريمة واحدة[2]، كما يتحقق عدم التجزئة في تعدد الجناة في ارتكاب جريمة من الجرائم الماسة بالمستهلك الإلكتروني، و علة اعتبار هذا الأخير يدخل ضمن حالة عدم التجزئة هي أن الماديات الإجرامية و ما يرتبط بها من تكييف إجرامي واحدة بالنسبة لجميع المساهمين، و من ثم كان الأقرب للعدالة أن يقدرها في مجموع قاض واحد[3] .

و المشرع الجزائري لم يحدد حالات عدم التجزئة مما يجعلها تخضع لتقدير محكمة الموضوع المحالة إليها الدعوى العمومية عن الجرائم المرتبطة، و في حالة توافرها كان تمديد الاختصاص لازما و هو ما نصت عليه المادة 329 فقرة ثالثة من قانون الإجراءات الجزائية[4].

---

[1] – د/ أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، الطبعة الخامسة، ديوان المطبوعات الجامعية، بن عكنون ، الجزائر، 2010، ص 361.

[2] – جندي عبد المالك، المرجع السابق، ص 366.

[3] – عادل بوزيدة، المسؤولية الجزائية لمتعهدي الإيواء، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تبسة، الجزائر، 2018، ص 136.

[4] – المادة 3/329 من قانون الإجراءات الجزائية المعدل و المتمم " ...كما تختص المحكمة كذلك بالنظر في الجنح و المخالفات غير قابلة للتجزئة أو المرتبطة."

أما الارتباط البسيط فيتحقق بتوفر الصلة التي تجمع عدة جرائم ببعضها كلما وجدت ظروف بينها دون أن تمنع من بقاء كل منها مستقلا عن الأخرى[1]، بمعنى قد ترتبط الأفعال الإجرامية ارتباطا لا يصل إلى حد عدم التجزئة، و لكنه يكون من المفيد نظرها معا بمعرفة جهة قضائية واحدة، و حسب المادة 3/329 من نفس القانون، فإن الجرائم المرتبطة يمكن أن تحال جميعا على محكمة واحدة قد تختص بإحداها و لا تختص بالباقي طبقا للقواعد العامة للاختصاص. و لقد عدد المشرع الجزائري في المادة 188 من قانون الإجراءات الجزائية أربعة حالات للارتباط البسيط و لكن هذا التعداد جاء على سبيل المثال و ليس الحصر[2]. و كمثال دخول الجاني لمنظومة إنشاء توقيع إلكتروني دون موافقته و التعامل في بياناته الشخصية دون موافقته مما يعد استعمال غير مشروع لها.

[1] – جيلالي بغدادي، الاجتهاد القضائي في المواد الجزائية، الجزء الأول، الديوان الوطني للأشغال التربوية، الجزائر ، 2002، ص 54.

[2] – المادة 188 من قانون الإجراءات الجزائية المعدل و المتمم "تعد الجرائم ترتبط في الأحوال الآتية:

أ–إذا ارتكبت في وقت واحد من عدة أشخاص مجتمعين.

ب–إذا ارتكبت من أشخاص مختلفين حتى و لو في أوقات مختلفة و في أماكن مختلفة و لكن على اثر تدبير إجرامي سابق بيتهم.

ج–إذا كان الجناة قد ارتكبوا بعض هذه الجرائم للحصول على وسائل ارتكاب الجرائم الأخرى أو تسهيل ارتكابها أو إتمام تنفيذها أو جعلهم في مأمن من العقاب.

د–أو عندما تكون الأشياء المنتزعة أو المختلسة أو المتحصلة من جناية أو جنحة قد أخفيت كلها أو بعضها".

الفرع الثاني: تقييد الإختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني

الأصل أن القاعدة الإجرائية المنظمة للاختصاص الجزائي خطاب موجه للكافة على إقليم الدولة الواحدة بغض النظر عن جنسياتهم و صفاتهم و هذا الخطاب يتضمن أمر أو نهيا ذو صلة بأحكام التشريع الجزائي الموضوعي و تهديدا لكل من يخرق هذه الأحكام أو يخالفها على إقليم الدولة، غير انه قد تحول بعض العوارض عن السريان المطلق للقواعد القانونية على إقليم الجمهورية أو تعلق العمل بها أمام جهة قضائية جزائية دون أخرى، و ذلك بسبب قيود قد تتعلق بالمركز القانوني لمرتكبي الجرائم الماسة بالمستهلك الإلكتروني (الفقرة الأولى) أو تعلقت العوارض بالاختصاص ذاته (الفقرة الثانية).

الفقرة الأولى: القيود المتعلقة بالمركز القانوني لمرتكب الجرائم الماسة بالمستهلك الإلكتروني

تنصرف هذه القيود إلى العوارض المتعلقة بالمركز القانوني التي يتخذه مرتكب الجرائم الماسة بالمستهلك الإلكتروني متى كان متمتعا بالحصانة النيابية أو كان من أعضاء السلك الدبلوماسي الأجنبي على الإقليم الوطني، أو كان أجنبيا و ارتكب الجريمة على مواطن جزائري –مستهلك إلكتروني– خارج إقليم الوطني، ففي كلتا الحالتين يكون مرتكبي الجرائم الماسة بالمستهلك الإلكتروني في وضعية مانعة لانعقاد الاختصاص القضائي بمساءلته جزائيا، حيث يكون أساس تقييد هذا الاختصاص في الحالة الأولى قواعد قانونية دولية (أولا) و في الثانية قواعد تشريعيا وطنية (ثانيا).

أولا: تقييد سريان القواعد الإجرائية للاختصاص على الإقليم الوطني

يقضي مبدأ الإقليمية بخضوع كل الجرائم التي ترتكب في إقليم الدولة لقانون هذه الدولة، فلا تفرقة بين مرتكبي هذه الجرائم ، تفرقة ترجع إلى جنسياتهم أو طوائفهم أو

مهنهم، و لكن ثمة اعتبارات من المصلحة العامة للمجتمع الوطني و المجتمع الدولي تقضي بعدم تطبيق قانون العقوبات على بعض الأشخاص[1].

فبموجب الاتفاقية الدولية [2] يتمتع بعض الأجانب في الدولة المستضيفة بحصانات تمنع خضوعهم لسلطة القضاء الوطني للدولة المستقبلة بما يتضمن نوعا من التقييد في سريان القانون الجزائي على الإقليم الوطني، مما يرتب عدم متابعة المتمتعين بالحصانة أثناء ارتكابهم للجرائم الماسة بالمستهلك الإلكتروني و ذلك لعدم تحريك الدعوى بخصوص هذه الفئة من الأشخاص إلى حين رفع الحصانة عنهم[3]. غير أن عدم محاكمتهم لا ينفي عدم مشروعية سلوكهم في القوانين الوطنية و هو ما يسمح بإمكان مقاضاتهم في دولهم الأصلية، فهذه الحصانة تعلق الخضوع لولاية القضاء الوطني، و عدم الخضوع لا يمنع الدولة المستضيفة من اتخاذ ما تراه مناسبا من إجراءات و تدابير تسمح بها الأعراف الدبلوماسية. فوفقا للاتفاقيات الدولية يتمتع رؤساء الدول الأجنبية بحصانة سياسية عامة تشمل كل فعل يصدر عنهم و تمتد إلى أفراد أسرهم و حاشيتهم، و علة هذه الحصانة كونهم يمثلون دولا ذات سيادة ، فإخضاعهم لسيادة الدولة التي يوجدون في إقليمها مساس بسيادة الدولة التي يمثلونها[4]،

كما يتمتع أيضا رجال السلك السياسي بحصانة عامة تشمل كل أفعالهم، سواء تعلقت بالعمل الدبلوماسي أم لم تكن متعلقة به، و تمتد الحصانة إلى كل رجال السلك السياسي الأجنبي على اختلاف ألقابهم و درجاتهم[5]، و يتمتع بالحصانة كذلك أعضاء البعثات السياسية الخاصة و ممثلو الهيئات الدولية كهيئة الأمم المتحدة و جامعة الدول

[1] – د/ محمود نجيب حسني، شرح قانون العقوبات القسم العام، المجلد الأول، المرجع السابق، ص 191.

[2] – إن السفراء و الموظفين الدبلوماسيين الأجانب المعتمدين لدى الجزائر يتمتعون بالحصانة الدبلوماسية طبقا لاتفاقية فيانا ل 15 أفريل 1961 و 24 أفريل 1963 التي صادقت عليها الجزائر بموجب المرسوم رقم 84/64 المؤرخ في 04 مارس 1964، انظر في ذلك، الجريدة الرسمية الجزائر رقم 29 لسنة 1964.

[3] – عادل بوزيدة، الرسالة السابقة، ص 137.

[4] – محمد نجيب حسني، شرح قانون العقوبات القسم العام، المجلد الأول، المرجع السابق، ص 192.

[5] – محمود نجيب حسني، شرح قانون العقوبات القسم العام، المجلد الأول، المرجع نفسه، ص 193.

العربية[1]. و علة هذه الحصانة كون رجال السلك السياسي يمثلون دولا ذات سيادة، بالإضافة إلى أن كفالة الحرية و الاستقلال المتطلبين لأداء أعمالهم تقتضي إقرار حصانة أشخاصهم . و يتمتع رجال السلك القنصلي بحصانة محدودة تقتصر على ما يرتكبه القنصل من أفعال أثناء أدائه وظيفته أو بسببها[2].

كما يتمتع رجال القوات الأجنبية الذين يتواجدون في إقليم الدولة بترخيص منها لحصانة تتسع للأفعال التي يرتكبونها أثناء أدائهم أعمالهم أو في داخل المناطق المخصصة لهم، و يعني ذلك أنه إذا ارتكب الفعل في غير عمل رسمي و في غير المناطق التي خصصتها لهم سلطات الإقليمية فلا حصانة لمن يرتكبه[3].

ثانيا: تقييد السلطة القضائية بنظر الجرائم الماسة بالمستهلك الإلكتروني

و يجد هذا القيد أساسه في قانون الإجراءات الجزائية، حيث يمنع مباشرة الجهات القضائية لإجراءات المتابعة ضد مرتكبي الجرائم الماسة بالمستهلك الإلكتروني، و تظهر بالأساس في القيود الواردة على سلطنة النيابة العامة في تحريك الدعوى العمومية و المتمثل في تقديم الشكوى[4]، حيث يشمل هذا القيد الجنح المرتكبة ضد المستهلك الإلكتروني خارج الإقليم الوطني كما قضت به المادة 583 من قانون الإجراءات الجزائية في فقرتها الثالثة، حيث اشترطت البلاغ المكتوب الذي تقدمه هيئة معينة أو المتضرر للنيابة العامة لتحريك الدعوى العمومية ضد مرتكبي الجرائم الإلكترونية الماسة بالمستهلك.

[1] – د/ عبد الله اوهايبية، شرح قانون العقوبات الجزائري، دار هومة، بوزريعة، الجزائر، 2006،، ص 141.

[2] – محمود نجيب حسني، شرح قانون العقوبات القسم العام، المجلد الأول، المرجع السابق، ص 194.

[3] – د/ عبد الله اوهايبية، شرح قانون العقوبات الجزائري، المرجع السابق2006، ص 141.

[4] – عادل بوزيدة، الرسالة السابقة، ص 138.

الفقرة الثانية: القيود المتعلقة بالإختصاص الجزائي ذاته

و تعني تلك الحالات أو الأسباب التي تحول دون ممارسة الجهة القضائية لولايتها بنظر الجرائم الواقعة على المستهلك الإلكتروني بصورة مؤقتة أو نهائية و التي تتخذ شكلا إجرائيا لاتصالها المباشر بتطبيق النصوص التشريعية لمعاقبة مرتكبيها، و تظهر هذه العوارض في صورة حالات قانونية للتنازع في الاختصاص بين الجهات القضائية الجزائية.

إذ قد يحصل متابعة نفس الوقائع الماسة بالمستهلك الإلكتروني على أكثر من محكمة ينتمون إلى نفس المجلس القضائي أو محاكم تنتمي إلى مجالس مختلفة، مما يترتب عليه تنازع إيجابي يتمسك كل واحد منهم باختصاصه دون أن يصدر من أحدهم أمر التخلي لصالح الجهة القضائية الأخرى، أو تنازع سلبي بإعلان كل واحد منهم عدم اختصاصه، رغم أن أحدهم على الأقل مختصا قانونا بنظر الدعوى[1].

و لقد حددت المادة 546من قانون الإجراءات الجزائية طرق رفع طلب النظر في تنازع الاختصاص و الفصل فيها، حيث خولت لكل من النيابة العامة و المتهم و المدعي المدني حق رفع طلب النظر في تنازع الاختصاص ، و ذلك بواسطة عريضة يتم إيداعها لدى كتابة الضبط لغرفة الاتهام في الحالة التي ينشأ فيها التنازع بين جهات قضائية تتبع نفس المجلس القضائي أو الغرفة الجنائية للمحكمة العليا في الحالة التي ينشأ فيها هذا التنازع بين جهات تتبع مجالس قضائية مختلفة، و ذلك خلال شهر اعتبارا من تاريخ أخر مقرر، على أن تعلن العريضة إلى جميع أطراف الدعوى الذين يعنيهم الأمر و لهم مهلة عشرة أيام لإيداع مذكراتهم لدى قلم الكتابة، غير أن هذا الأجل لا يعد من النظام العام إذ يجوز مخالفته اتفاقا، حيث أن المشرع نص عليه علي سبيل الإرشاد و التنظيم فقط و قصد السرعة في حل النزاع.

[1] – محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة العاشرة، دار هومة، الجزائر، 2015، ص 141.

المطلب الثاني: وسائل انفاذ الاختصاص الجزائي بشأن الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

ينصرف مدلول وسائل انفاذ الاختصاص الجزائي بحماية المستهلك في المعاملات الإلكترونية إلى مجموع الآليات والتدابير المرصودة من قبل المشرع لتطبيق قواعد الاختصاص الجزائي، مستهدفا بذلك نقل هذه القواعد من الحال النظرية، إلى الفعالية الإجرائية، و التطبيق العملي، لتحري حقيقة المسؤولية الجزائية الناشئة عن الإخلال بصالح المستهلك في هذا النوع المستحدث من المعاملات، وتقرير مدى توافر شروطها وإمكانية تطبيق أحكامها، تبعا لإجراءات قانونية معينة. ولمناقشة أهم الآليات وسائل انفاذ الاختصاص الجزائري بحماية المستهلك جزائيا في المعاملات الالكترونية. فإننا سنحاول تحديد الجهات القضائية المحتصة بإنفاذ قواعد الاختصاص الجزائي (الفرع الأول) ثم تبيان طرق إنفاذ الاختصاص القضائي في هذا النوع من الجرائك (الفرع الثاني).

الفرع الأول: الجهات القضائية المختصة بإنفاذ قواعد الاختصاص الجزائي في الجرائم الماسة بالمستهلك الإلكتروني

يقصد بالمحكمة المختصة جزائيا بإنفاذ قواعد الاختصاص، لحمايةً المستهلك جزائيا في المعاملات الإلكترونية؛ الجهة المتمتعة بالولاية القضائية – المخولة لها بموجب أحكام القانون –، للنظر والفصل في الدعاوى والوقائع المعروضة عليها والمتصلة بعدم مشروعية الأنشطة المرتكبة عبر مواقع التجارة الإلكترونية، التي يقدمها موردو هذا النمط من الخدمات، و البروج إلى التشريع الوطنب فإنه يمكن تقسم هذه الجهات القضائية إلى جهات عادية (الفقرة الأولى) و الجهات القضائية الجزائية الاستثنائية (الفقرة الثانية).

الفقرة الأولى: الجهات القضائية الجزائية العادية المختصة بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

تشمل هذه الفئة من المحاكم؛ الأجهزة القضائية المختصة بنظر الوقائع ذات الطابع الجزائي، والدعاوى الناشئة عنها، سواء كانت هذه الأجهزة ذات اختصاص عادي أو اختصاص موسع، وتظم هذه الفئة من المحاكم: كلا من محكمة الجنايات ومحكمتي الجنح والمخالفات من جهة (أولا)، والأقطاب الجزائية ذات الاختصاص الموسع من جهة ثانية (ثانيا).

أولا: الجهات القضائية ذات الاختصاص العادي بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

وتدل على جهات الحكم المختصة بنظر وقائع الجرائم الماسة بالمستهلك الإلكتروني، والتي ينعقد اختصاصها الإقليمي تبعا للقواعد العامة المقررة في قانون الإجراءات الجزائية، وتشمل على وجه التحديد كلا من: محكمة الجنايات التي تختص بنظر الجرائم الواقعة على المستهلك الإلكتروني، بأنها جنايات[1]، والجنح والمخالفات المرتبطة بها، وكذا الجرائم الموصوفة بأنها أفعال ماسة بالاقتصاد الوطني، المحالة إليها بقرار نهائي من غرفة الاتهام. وتتشكل محكمة جنايات أول درجة، من عنصر قضائي محترف وآخر غير محترف. فهي تتشكل من: رئيس برتبة رئيس غرفة على الأقل، وقاضيين برتبة مستشار على مستوى المجالس القضائية، ومن لؤبع محلفين؛ ومحكمة الجنح: وهي قسم يتواجد على مستوى المحاكم الابتدائية، يختص بالفصل في الجنح المرتكبة ضد المستهلك الإلكتروني، أو غير القابلة للتجزئة. كما يوجد على مستوى محكمة أول درجة قسم، يختص بالفصل في وقائع الجرائم الإلكترونية، ذات وصف

[1] – أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثالث، ديوان المطبوعات الجامعية، دون طبعة، بن عكنون، الجزائر، 1998، ص، 332

المخالفة. وتتشكل محكمتي الجنح والمخالفات من: قاض فرد ويمثل النيابة العامة أمامها، وكيل الجمهورية، أو أحد مساعديه[1].

ثانيا: المحاكم الجزائية ذات الاختصاص الموسع بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

وهي جهات قضائية منحها القانون اختصاصا اقليميا موسعا، للنظر في بعض الجرائم الخطيرة، بموجب نصوص المواد 37، 40 و 329 من القانون 15 – 04 المعدل لقانون الإجراءات الجزائية والمتمم له[2]، حيث قضت المواد سالفة الذكر، بجواز تمديد الاختصاص المحلي، لجهات الحكم والتحقيق والنيابة العامة المعنية بها إلى دائرة اختصاص جهات قضائية أخرى، عن طريق التنظيم[3]. وتتصل هذه المحاكم بملف الوقائع محل النظر، وفق إجراءات خاصة نصت عليها المواد من 40 مكرر 1 إلى 40 مكرر 5 من قانون الإجراءات الجزائية الجزائري؛ حيث يتعين على جهات الضبط القضائي، إذا رأت بأن الملف المكون من طرفها، يدخل ضمن اختصاص القطب الجزائي المتخصص، أن تخطر وكيل الجمهورية لدى محكمة وقوع الجريمة فورا، مصحوبة بأصل ملف الدعوى مع نسختين، ليقوم وكيل الجمهورية بإرسال نسخة من ملف الدعوى إلى النائب العام لدى مجلس قضاء محكمة القطب ليحيل بدوره الملف إلى وكيل الجمهورية لدى محكمة القطب، متى تبين له انعقاد اختصاص محكمة القطب بالوقائع المتضمنة في الملف محل

[1] – محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، المرجع السابق، ص، 308.

[2] – القانون رقم 04 – 15 المؤرخ في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر سنة 2004 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق لـ 08 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية عدد 71 المؤرخة في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر سنة 2004.

[3] – المرسوم التنفيذي رقم 06 – 348 المؤرخ في12 رمضان عام 1427 الموافق لـ 05 أكتوبر 2006 المتضمن تمديد الاختصاص الحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق الجريدة الرسمية عدد 63 المؤرخة في 15 رمضان عام 1427 الموافق لـ 08 أكتوبر 2006،

الإحالة[1].

الفقرة الثانية: الجهات القضائية الجزائية الاستثنائية بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

لما كان الأصل هو اختصاص جهات القضاء الجزائي عادية كانت، أو أقطابا متخصصة، بنظر وقائع الجرائم الإلكترونية المجرم فالاستثناء، أنْ تعرض هذه الوقائع على جهات أخرى خاصة، وتشمل – هذه الأخيرة – فئتين رئيستين الأولى هي المحاكم العسكرية (أولا)، والثانية هي قضاء الأحداث (ثانيا).

أولا: قضاء الأحداث

تعد محاكم الأحداث من المحاكم الخاصة، التي يتحدد اختصاصها ببعض لجرائم، وبمحاكمة فئة معينة من الجناة، هم الأحداث. وهي تقابل محاكم القانون العام، التي تختص بجميع الجرائم، وجميع المتهمين بارتكابها.

وتعد محاكم الأحداث بدرجاتها المختلفة، نوعا من القضاء الطبيعي بالنسبة للمتهمين، أو الجرائم التي تدخل في اختصاصها، كما تعتبر هذه المحاكم أجهزة قضائية ذات طبيعة مزدوجة، فهي قانونية اجتماعية، لأن القانون هو الذي يحدد سن الحدث، ويحدد الحالات التي يعد الحدث فيها منحرفا، أو تلك التي يكون فيها في خطر معنوي، ويحدد للمحكمة اختصاصها، ويحدد لها الوسائل التقويمية والعلاجية، التي تتفق مع ظروف الحدث، هذا في الوقت الذي يمنح فيه القانون للمحكمة دورا اجتماعيا، يتمثل في ضرورة فحص هذه الحالة من النواحي الاجتماعية، الطبية والنفسية، ليساعدها في اختيار العلاج الذي يقضي على أساس انحراف الطفل. والمحكمة تطبق في ذلك مبادئ الدفاع

[1] – عبد المجيد جباري، دراسات قانونية في المادة الجزائية، على ضوء أهم التعديلات الجديدة، دار هومة، دون طبعة، الجزائر 2012، ص، 73.

الاجتماعي، بنبذه فكرة الردع أو العقوبة وإتباع الوسائل التقويمية، بشأن الأحداث[1].

ولا يمكن لمحاكم الأحداث أن تتصل بوقائع الماس بالمستهلك الإلكتروني مالم يكن للطفل محل المتابعة اضطلاع مباشر بها، وتتحقق هذه الحالة متى باشر الطفل أي صورة من صور الجرائم الماسة بالمستهلك الإلكتروني من غير أن يأخذ وصف المحترف أو المتعامل الاقتصادي كما تعرفه التشريعات والأنظمة القانونية السارية، لتستبعد بذلك هذه الأجهزة – كأصل عام – من الهياكل القضائية المسؤولة عن انفاذ قواعد الاختصاص الجزائي في مادة حماية المستهلك الإلكتروني.

ثانيا: جهات القضاء العسكري

من الثابت أن المحاكم العسكرية كقضاء استثنائي، لا تخضع في قواعد اختصاصها وإجراءات المتابعة أمامها، إلى القواعد الإجرائية نفسها، المتبعة أمام القضاء العادي. وتستمد المحاكم العسكرية طابعها الاستثنائي، من خصوصية الوقائع التي تدخل ضمن اختصاصها، والفئات الخاضعة للمتابعة أمامها[2].

وتخضع هذه الجهات في اختصاصها بنظر الجرائم الماسة بالمستهلك الإلكتروني لضابطين زمنيين: ضابط يحدد اختصاصها في زمن السلم، وضابط يحدد هذا الأخير في زمن الحرب؛ فبالنسبة للضابط الأول: تختص المحاكم العسكرية، بنظر وقائع الإجرام المعلوماتي – بوصفها جرائما من جرائم القانون العام – الواقعة من العسكريين، وأشباه العسكريين أثناء الخدمة، أو داخل المؤسسات العسكرية، أو لدى المضيف[3].

---

[1] – حمدي رجب عطية ، الإجراءات الجنائية بشأن الأحداث في التشريعيين الليبي والمصري في ضوء الأفاق الجديدة للعدالة الجنائية في مجال الأحداث، دار النهضة العربية، دون طبعة، القاهرة، 1999، ص ، 111.

[2] – دمدوم كمال، القضاء العسكري والنصوص المكملة له، دار الهدى، الطبعة الثانية، عين مليلة، الجزائر، 2004، ص: 11.

[3] – لم يرد في قانون القضاء العسكري الجزائري، ما يحدد المقصود بالأوصاف الثلاثة التي يتحدد بموجبها انعقاد اختصاص المحاكم العسكرية، بالجرائم المعلوماتية، غير أن المتواتر عليه فقها، أن المقصود بالجرائم المعلوماتية المرتكبة أثناء تأدية الخدمة، هي: كل الأفعال المعلوماتية، ذات الصلة بخدمات التجارة الإلكترونية عبر شبكة الأنترنت،

أما بالنسبة للضابط الثاني: لاختصاص المحاكم العسكرية في زمن الحرب، فيشمل الجرائم المعلوماتية الموصوفة بأنها اعتداء على أمن الدولة. في حين تخضع جهات القضاء العسكري في اختصاصها الإقليمي لأحكام المادة 30 وما بعدها، من قانون القضاء العسكري الجزائري[1].

المرتكبة من عسكري، أو ممن في حكمه، أثناء تنفيذه أمرا من السلطة السلمية؛ والمقصود بجرائم التجارة الالكترونية المرتكبة داخل مؤسسة عسكرية: تلك التي ترتكب داخل كل المرافق والبنايات الموضوعة تحت تصرف الجيش الوطني الشعبي، لتأدية مهامه؛ أما الجرائم المعلوماتية المرتكبة لدى المضيف فهي: تلك التي تقع لدى كل الأشخاص الطبيعيين، أو المعنويين من غير العسكريين، الذين يسخرون ما في حيازتهم لإيواء عسكريين بمناسبة ظروف معينة أو لأجل القيام بمهمة رسمية. **أنظر كلا من: إبراهيم أحمد عبد الرحيم الشرقاوي، النظرية العامة للجريمة العسكرية، المكتب الجامعي الحديث، دون طبعة الإسكندرية، جمهورية مصر العربية، 2007، ص: 127 وما بعدها؛ صلاح الدين جبار، القضاء العسكري في التشريع الجزائري والقانون المقارن، دار الخلدونية، الطبعة الأولى، الجزائر، 2010، ص: 77.**

[1] – الأمر رقم 71 – 28 المؤرخ في 26 صفر عام 1391 الموافق لـ 22 أفريل 1971 المتضمن قانون القضاء العسكري، الجريدة الرسمية عدد 38 المؤرخة في 16 ربيع الأول عام 1391 الموافق لـ 11 مايو سنة 1971، ص: 566.

الفرع الثاني: طرق إنفاذ الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني

من المعلوم أنه لا يمكن لجهات القضاء الجزائي، أن تتصل من تلقاء نفسها بالدعوى الرامية إلى مباشرة الإجراءات القضائية فيما يتعلق بحماية المستهلكين في خدمات التجارة الإلكترونية، بل هناك سبل وطرق حددها القانون، يتم بمقتضاها تقديم المتهم، والوقائع المحال بها، إلى المحكمة المختصة للنظر، والفصل في دعواه. وقد نظم المشرع الجزائري طرق انفاذ الاختصاص الجزائي و يمكن تقسيمها إلى طرق تقليدية (الفقرة الأولى) و أخرى مستحدثة (الفقرة الثانية).

الفقرة الأولى: الطرق التقليدية بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

نص قانون الإجراءات الجزائية الجزائري، على طرق تقليدية تتيح اتّصال المحكمة المختصة بنظر دعاوى حماية المستهلك في معاملات الإلكترونية، بملف الدعوى. وقد اتجه جانب كبير من الفقه[1]، نحو تصنيف هذه الطرق، وإدراجها تحت نوعين، يشمل الأول الطرق التقليدية العادية، وهي وسائل ينعقد بها اختصاص الجهات القضائية الجزائية، كما أقرته قواعد الاختصاص؛ في حين يشمل الثاني: الطرق الاستثنائية، أو غير العادية لهذا الإتصال.

أولا: الطرق التقليدية العادية بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

يشمل النوع الأول؛ الطرق التقليدية العادية لاتصال المحكمة الجزائية بالوقائع المجرمة، جنحا ومخالفات كانت، أو جنايات؛ فأما اتصال محكمتي الجنح والمخالفات دعاوى حماية المستهلك في معاملات الإلكترونية جزائيا، فيتم بناء على أمر الإحالة الصادر عن قاضي التحقيق[2]، أو بناء على قرار غرفة الاتهام القاضي بإعادة تكييف

[1] – زوليخة تيجاني، نظام الإجراءات أمام محكمة الجنايات، أطروحة دكتوراه، كلية الحقوق، بن عكنون، جامعة بن يوسف بن خدة الجزائر 1، 2013، ص، 71.

[2] – أنظر المادة 164 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

الوقائع من جناية إلى جنحة[1] أو عن طريق التكليف بالحضور أمام محكمة الجنح[2]، متى كانت وقائع توريد خدمات التجارة الإلكترونية تشكل وصف جنحة. أما إذا كانت بوصف مخالفة، فتتصل محكمة المخالفات بالدعوى بأحد طريقين؛ الأول: عن طريق التكليف بالحضور أمام محكمة المخالفات[3]، والثاني بناء على أمر بالإحالة الصادر عن قاضي التحقيق[4]. أما بالنسبة لاتصال محكمة الجنايات بالوقائع المعلوماتية غير المشروعة فيتم بناء على قرار إحالة نهائي، صادر عن غرفة الاتهام، والذي يمثل الوسيلة الإجرائية العملية لاتصال محكمة الجنايات بالوقائع المعلوماتية المجرمة[5]، متى استوفى شروطه القانونية المنصوص عليها بالمواد 198 وما بعدها من قانون الإجراءات الجزائية.

ثانيا: الطرق التقليدية الاستثنائية بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

وتعني هذه الفئة من الطرق: الإجراءات غير العادية التي تتصل من خلالها المحكمة المختصة بالوقائع المعلوماتية المجرمة، وترد هذه الإجراءات ضمن ثلاث طوائف؛ تتصرف الأولى إلى قرارات الإحالة الصادرة عن غرف الاتهام بالمجالس القضائية وتلك الصادرة عن الغرف الجزائية للمحكمة العليا، حال بتها في مسائل التنازع بالاختصاص[6]؛ والثانية إلى الإحالة الصادرة عن الغرفة الجزائية للمحكمة العليا، حال البت في طعن غير عادي بالنقض مع الإحالة[7]؛ أما الثالثة، فتتصرف إلى الحالات التي ينص عليها القانون صراحة، وهي الإحالة لداعي الأمن العمومي، أو لمصلحة سير

[1] – أنظر المادة 196 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[2] – أنظر المادة 333 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[3] – أنظر المادة 394 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[4] – أنظر المادة 164 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[5] – تيجاني زوليخة، الرسالة السابقة، ص: 59.

[6] – محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، المرجع السابق، ص، 147.

[7] – عبد الرحمن خلفي، المرجع السابق، ص، 386.

القضاء، أو لقيام الشبهة المشروعة. على أن تتم الإحالة في حالتي داعي الأمن العمومي وحسن سير القضاء، بناء على أمر يرفعه النائب العام لدى المحكمة العليا، إلى الجهة المعروضة عليها وقائع الإيواء المعلوماتي المجرم، أما إذا كان سبب الإحالة قيام شبهة مشروعة، جاز تقديم العريضة بطلب الإحالة من النائب العام لدى المحكمة العليا، أو من قبل النيابة العامة لدى الجهة القضائية المعنية، أو من المتهم أو المدعي المدني[1].

الفقرة الثانية: الطرق المستحدثة بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني

استحدث المشرع الجزائري، ومن خلال التعديل الذي لحق قانون الإجراءات الجزائية، الصادر تحت رقم 15 – 02 [2]، وسائل إجرائية جديدة، تُعْقَدُ بها ولاية المحكمة الجزائية بنظر الوقائع الجرمية، ومنها الوقائع المعلوماتية المجرمة التي تستوفي الشروط القانونية الواردة ضمن هذا القانون، وتتجلى هذه الطرق بالأساس في نظاميْ المثول الفوري (أولا) و الأمر الجزائي (ثانيا).

أولا: نظام المثول الفوري

يمثل هذا النظام، طريقا جديدا لاتصال المحكمة بالوقائع الجزائية محل النظر. وقد استحدثه المشرع الجزائي، بناء على التعديل المذكور أعلاه، وأحله محل إجراءات التّلبس. ويعد هذا النظام من إجراءات المتابعة، التي تتبعها النيابة العامة تبعا لما تتمتع به من سلطة الملائمة الإجرائية، في إخطار المحكمة بالقضية. والتي تهدف إلى تبسيط إجراءات المحاكمة، في مجال الجنح المتلبس بها[3]. وتحكم هذا النظام، نصوص المواد من: 339 مكرر حتى: 339 مكرر 7 من قانون الإجراءات الجزائية. حيث أحاطه المشرع الإجرائي، بالعديد من الضمانات الشكلية والموضوعية،

[1] – أنظر المادة 549 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[2] – الأمر 15 – 02 المؤرخ في 07 شوال عام 1436 الموافق لـ 23 يوليو سنة 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386الموافق لـ 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40 المؤرخة في 07 شوال عام 1436 الموافق لـ 23 يوليو سنة 2015.

[3] – عبد الرحمن خلفي، المرجع السابق، ص، 339.

والتي أوردها في شكل شروط، تحكم الالتجاء إلى هذا النظام. و سنحاول تحديد هذه الشروط على النحو التالي:

1-شروط صحة هذا الإجراء من الناحية الموضوعية:

أول شرط من الشروط الموضوعية التي وضعها المشرع الوطني هيا أن تكون الوقائع محل الإحالة تحمل وصف جنحة متلبس بها تبعا لما أقرته المادة 41 من قانون الإجراءات الجزائية[1]، شريطة أن تكون معاقب عليها بعقوبة سالبة للحرية، و هو ما يستبعد باقي الجنح المعاقب عليها بعقوبة الغرامة كعقوبة أصلية و كذلك الوقائع الموصوفة جنايات و مخالفات.

كما اشتراط المشرع الوطني أن تكون الوقائع محل النظر، لا تستلزم ولا تخضع من حيث المتابعة فيها لإجراءات تحقيق خاصة[2].

2- شروط صحة هذا الإجراء من الناحية الإجرائية:

أما من الناحية الإجرائية، فيلزم لصحة نظام المثول الفوري، احترام الإجراءات المنصوص عليها قانونا، والمتمثلة في استجواب المتهم من قبل وكيل الجمهورية، وتمكينه من الاستعانة بمحام، مع إحاطة باقي أطراف الدعوى بمثولهم فورا أمام جهات الحكم، ووضع نسخ من ملف القضية تحت تصرف محامي المتهم، وتمكينهما من التواصل على انفراد[3].

---

[1] – نصت المادة 41 من قانون الإجراءات الجزائية على الحالات التي تكون فيها الجرائم متلبس بها و تتمثل في:

– مشاهدة الجريمة حال أو عقب ارتكابها.

– متابعة المجرم بالصياح اثر وقوع الجريمة

– العثور على أشياء في وقت قريب في حوزة الجاني أو دلائل تفرض مساهمته في الجريمة.

–وقوع الجريمة داخل المنزل مع المبادرة بالإبلاغ عنها عقب اكتشافها.

[2] – أنظر المادة 339 مكرر من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[3] – أنظر المادة 339 مكرر 4 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

ثانيا: نظام الأمر الجزائي

ويعد هذا الطريق، أحد أهم التدابير، التي تهدف إلى تقليص الإجراءات في مرحلة المحاكمة، كما يعتبر بديلا، لا يستهان به نظرا للفائدة التي يحققها في مجال إجراءات المحاكمة الجزائية. والأمر الجزائي – بهذا المعنى – نظام خاص يواجه نوعا من الجرائم البسيطة، التي لا تستلزم مراعاة القواعد المقررة للمحاكمات العادية[1] . غير أن المشرع الوطني قد حدد نطاق تطبيق هذا النظام سواء من حيث الموضوع و من حيث الأشخاص.

إذ تخضع لهذا النظام الأفعال التي تحمل وصفة جنحة معاقبا عليها بالغرامة و/ أو بالحبس، لمدة تساوي أو تقل عن سنتين. مع اشتراط أن تكون هوية مرتكبها معلومة، وأن تكون الوقائع محل النّظر بسيطة وغير خطرة، وليس من شأنها أن تثير مناقشة وجاهية[2]. وأن يكون المتهم محل المتابعة شخصا واحدا، باستثناء حالة متابعة الشخص الطبيعي مع الشخص المعنوي، عن الوقائع ذاتها و يستثنى من هذا النظام أيضا، المتهمون الأحداث، وتلك الوقائع المرتبطة بوقائع أخرى لا تحقق الشروط المذكورة، وفي حالة تعدد الجناة والمتابعين على الوقائع ذاتها[3].

[1] – سعاد أجعود، المرجع السابق، ص: 375.

[2] – أنظر المادة 380 مكرر من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[3] – أنظر المادة 381 مكرر 7 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

المبحث الثاني: التعاون الدولي كألية لانعقاد الاختصاص القضائي لمواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

إن الطابع العابر للحدود الذي تتمتع به الجرائم الماسة بالمستهلك في المعاملات الإلكترونية يجعل من الصعب على أي دولة بمفردها و مهما كانت الوسائل و الموارد المتوفرة لديها أن تتصدى لها بشكل كاف دون أن تعتمد على شكل من أشكال التعاون الدولي، و يقصد به تبادل المساعدة و تضافر الجهود المشتركة بين دولتين أو أكثر لتحقيق نفع أو خدمة مشتركة في مجال مواجهة الإجرام، و كل ذلك يكون في إطار إبرام الاتفاقيات الدولية سواء أكانت جماعية أو ثنائية.

كما يشكل التعاون الدولي في مجال تعزيز الإختصاص القضائي بمتابعة مرتكبي الجرائم الماسة بالمستهلك في المعاملات الإلكترونية جزائيا عنصرا أساسيا في مواجهة الاعتداءات المرتكبة على هذا الأخير طالما أن تحقيق العدالة أضحت مسؤولية عامة و مشتركة تتطلب لتحقيقها اتباع نهج متكامل يواءم مع المبادئ و الأهداف المنصوص عليها في الاتفاقيات الدولية.

و انطلاقا من هذا الواقع بات تعزيز التعاون الدولي في مجال حماية المستهلك في المعاملات الإلكترونية ضرورة لمواجهة هذا النوع من المجرمين و التي تتخذ من شبكة الإنترنت وسائل للمساس بمصالح المستهلك الإلكتروني و تنفيذ مخططاتها الجرمية.

و عليه سوف نحاول البحث عن صور التعاون الدولي في تعزيز الإختصاص القضائي لمواجهة الجرائم الماسة بالمستهلك الإلكتروني (المطلب الأول)، و مناقشة الإشكالات التي يطرحها التعاون الدولي (المطلب الثاني).

المطلب الأول: صور التعاون الدولي في تعزيز الإختصاص القضائي لمواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

إن معاملات المستهلك الإلكترونية لا تعرف الحدود الجغرافية و الجرائم المتعلقة بها جرائم وطنية و أغلبها عابرة للحدود، و هو أدى إلى عدم قدرة الجهات القضائية الوطنية من مكافحة هذه الجرائم، ما جعل من التعاون الدولي مطلب الجميع.

لهذه الأسباب سارعت بعض الدول من بينها المشرع الجزائري إلى النص على صور التعاون الدولي في مجال إجراء المتابعة و التحقيق[1]، و إبرام اتفاقيات دولية لتبسيط هذه الإجراءات و توحيد القواعد العامة، و قد نصت اتفاقية بودابست على المبادئ العامة التي تحكم التعاون الدولي في مجال الجرائم التي لها علاقة بالجرائم الواقعة في بيئة الأعمال الإلكترونية[2]. و من بين أهم صور التعاون الدولي المساعدة القضائية (الفرع الأول)، و تسليم المجرمين (الفرع الثاني).

الفرع الأول:المساعدة القضائية المتبادل لتعزيز الاختصاص القضائي في مواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

تعد المساعدة القضائية المتبادلة في المسائل الجنائية من الآليات الفعالة لمواجهة الإجرام بوجه عام لما لتعاون في مجال الإجراءات الجنائية من دور في التوفيق بين حق الدولة في ممارسة اختصاصها الجنائي داخل حدود إقليمها، و حقها في توقيع العقاب[3].

و تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به الدولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم الواقعة في بيئة الأعمال الإلكترونية[4] بما فيها الماسة بالمستهلك الإلكتروني. أو أنها تقديم الدول الأطراف لبعضها

---

[1] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 392.

[2] – بوقرين عبد الحليم، الرسالة السابقة، ص 482.

[3] – سليمان إبراهيم مصطفى، الإرهاب و الجريمة المنظمة، دار الطلائع، القاهرة، 2006، ص 394.

[4] – هلالي عبد الله احمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، 2007، ص 326.

البعض أكبر قدر من المساعدة القانونية المتبادلة في التحقيقات و الملاحقات و الإجراءات القضائية المتصلة بجرائم تحددها الاتفاقيات الدولية[1].

إذ أوصت اتفاقية بودابيست كل طرف تبنى إجراءات تشريعية لأجل الوفاء بالالتزامات المتفق عليها في مجال التعاون الدولي، و أجازت لأي طرف في حالة الاستعجال أن يقدم طلبا للمساعدة المتبادلة...، و في المقابل أوجبت على الدول المقدمة إليها الطلب أن توافق على الطلب أو على الأقل أن ترد عليه بأي وسيلة مستعجلة[2].

و بالرجوع إلى التشريع الجزائري نجد قد تنبه إلى أهمية التعاون الدولي و المساعدة القضائية الدولية، فسمح في إطار التحريات أو التحقيقات القضائية بخصوص الجرائم الواقعة في البيئة الإلكترونية بما فيها الماسة بالمستهلك الإلكتروني بتبادل المساعدة القضائية الدولية بخصوص جمع الأدلة الإلكترونية، بل يمكن في حالة الاستعجال قبول طلبات المساعدة القضائية إذا وردت عن طريق وسائل الاتصال الإلكتروني، و ذلك بقدر ما توفره هذه الوسائل من شروط تضمن أمنها و صحتها[3].

و عليه فإن المساعدة القضائية إجراء قضائي من شأنه ممارسة الاختصاص القضائي في دولة أخرى بصدد جريمة من الجرائم الماسة بالمستهلك الإلكتروني، يلجأ إليه لتحقيق الفعالية و السرعة في إجراءات الملاحقة و العقاب على هذه الجرائم. و تتخذ المساعدة القضائية في المجال الجنائي عدة صور تتمثل في تبادل المعلومات (الفقرة الأولى) و نقل الإجراءات الجنائية (الفقرة الثانية) و الإنابة القضائية (الفقرة الثالثة).

[1] – بوقرين عبد الحليم، الرسالة السابقة، ص 484.

[2] – أنظر المادة 25 من الاتفاقية بودابست لسنة 2001.

[3] – انظر المادة 16 من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

الفقرة الأولى: تبادل المعلومات بين الدول

يشمل تبادل المعلومات في مجال المعاملات التجارية الإلكترونية تقديم المعلومات و البيانات و الوثائق و العناوين المتعلقة بالمتعاملين في مجال التجارة الإلكترونية أو بعض المعلومات عن المنتوجات و السلع التي تطلبها سلطة قضائية أجنبية عند نظر جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج و الإجراءات التي اتخذت ضدهم، و قد يشمل التبادل السوابق القضائية للجناة[1]، و بصفة عامة كل المعلومات المتعلقة بالمعاملة التجارية الإلكترونية.

و لقد أوصت معاهدة الأمم المتحدة بشأن تبادل المساعدة في المسائل الجنائية على أن يقدم كل طرف للآخر أكبر قدر من المساعدة المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة ضمن نطاق اختصاص السلطة القضائية في الدولة الطالبة[2]، و هو الأمر الذي أوصت به كذلك اتفاقية بودابست[3] و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[4].

أما المشرع الجزائري فقد نص في المادة 17 من قانون 04/09 المتعلق بالوقاية من جرائم تكنلوجيا الإعلام و الاتصال على أنه تتم الاستجابة لطلبات المساعدة القضائية الرامية لتبادل المعلومات أو اتخاذ إجراءات تحفظية وفقا لاتفاقية الدولية ذات الصلة و الاتفاقيات الثنائية و مبدأ المعاملة بالمثل.

و يكون تبادل المعلومات بتقديم طلب سواء أكان في شكل خطي أو يمكن أن يكون عاجل عن طريق الفاكس أو البريد الإلكتروني في الحالات الطارئة، شريطة أن تتضمن هذه الاتصالات القدر المعقول من الأمن و المرجعية[5].

---

[1] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 407.

[2] – محمد الأمين البشري و محسن عبد الحميد احمد، معايير الأمم المتحدة في مجال العدالة الجنائية و منع الجريمة، الطبعة الأولى، الأكاديميون للنشر و التوزيع، عمان، 2014ن ص 277.

[3] – أنظر المادة 25 من اتفاقية بودابست لسنة 2001.

[4] – أنظر المادة 1/32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[5] – انظر المادة 2/16 من قانون 04/09 .المتعلقة بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

غير أن المشرع الجزائري وضع قيود على تنفيذ طلبات المساعدة القضائية إذا كان الطلب من شأنه المساس بالسيادة الوطنية أو بالنظام العام، غير أنه يمكن أن يتم الاستجابة لطلبات المساعدة بشروط من بينها المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها خارج حدود ما هو مبين في الطلب[1].

و هو ما أكدت عليه الاتفاقية العربية من خلال المادة 32 سابقة الذكر إذ مكنت الدولة الأطراف أن ترفض طلب المساعدة إذا كان متعلقا بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية أو أن تنفيذ الطلب يشكل انتهاكا لسيادتها أو أمنها أو نظامها أو مصالحه الأساسية. و نصت عليه أيضا اتفاقية بودابست حيث أجازت لكل دولة في حدود قانونها الداخلي –و حتى دون طلب مسبق– أن ترسل لأي دولة طرف معلومات حصلت شريطة الحفاظ على السرية، و إن لم تستطع الدولة الأخرى ضمان السرية فتبلغ الدولة المسلمة بذلك، و التي تقرر بدورها مدى إمكانية تقديم المعلومات، أما إذا قبلت الدولة المرسل إليها شرط السرية، فيجب أن تبقى المعلومات بين الدولتين[2].

الفقرة الثانية: نقل الإجراءات بين الدول

و يتم ذلك عن طريق قيام دولة باتخاذ إجراءات جنائية بمناسبة جريمة معينة قد ارتكبت في إقليم دولة أخرى و لمصلحة هذه الدولة و ذلك بناءا على اتفاقية مبرمة بينهم[3]، و لقد أقرت العديد من الاتفاقيات الدولية هذه الصورة من بينها معاهدة الأمم المتحدة بشأن نقل الإجراءات في المسائل الجنائية التي جاء في مذكرتها الإيضاحية أن هذا الإجراء يسهم في إقامة العدل بصورة فعالة، و في الحد من تنازع الاختصاص بين

[1] – انظر المادة 18 من قانون 04/09 . المتعلقة بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[2] – أنظر المادة 26 من اتفاقية بودابست لسنة 2001.

[3] – د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص 80.

الدول و عليه فيجب تعزيزه باتفاقيات ثنائية أو متعددة الأطراف[1]. و للقيام بنقل الإجراءات بين الدول تنص هذه الأخيرة على بعض الشروط في قوانينها الداخلية أو في الاتفاقيات الدولية نذكر منها:

-أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في كلتا الدولتين.

-أن يكون الإجراء المطلوب اتخاذه مقرر في القانون الداخلي للدولة المطلوب منها الإجراء و هو ما يعرف بشرعية الإجراء.

-أن يكون هذا الإجراء مناسب للوصول إلى الحقيقة المتعلقة بأدلة الجريمة المرتكبة.

-أن يكون الإجراء المطلوب اتخاذه بصدد نقل مجرم في الدولة المطلوب منها الإجراء و كذلك الدولة المطالبة له[2].

و بالرجوع إلى المادة 17 من قانون 04/09 نجد المشرع قد أشار إلى هذا الإجراء تحت عنوان تبادل المعلومات و اتخاذ الإجراءات التحفظية، دون ذكر ماهيا هاذه الإجراءات التحفظية، و تذكر المادة أن هذا الإجراء يتم وفق للاتفاقيات الدولية ذات الصلة و الاتفاقيات الدولية الثنائية و مبدأ المعاملة بالمثل.

بالرجوع إلى اتفاقية بودابست و الاتفاقية العربية بخصوص جرائم تقنية المعلومات نجدها تنص على بعض الإجراءات الوقتية التي يمكن اتخاذها في مجال الجرائم الإلكترونية، و المتمثلة في :

-الحفظ المعجل على المعطيات المخزنة:

نصت اتفاقية بودابست على الحفظ المعجل على المعطيات المخزنة في المادة 29، و كذلك الاتفاقية العربية بخصوص جرائم تقنية المعلومات في المادة 37، و يكون هذا

[1] – د/ عادل عبد العال إبراهيم خراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية و سبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015، ص 35.

[2] – بوقرين عبد الحليم، الرسالة سابقة، ص 485.

الإجراء في شكل طلب تقدمه دولة طرف إلى دولة أخرى بغية الحصول على الحفظ المعجل للمعطيات المخزنة في نظام معلوماتي يقع ضمن إقليمها، و يكون طلب التحفظ متعلقا بما تود الدولة الطالبة أن تقدم طلبا بشأنه للمساعدة المتبادلة للبحث و ضبط المعلومات، و يجب أن يحدد في طلب الحفظ ما يلي:

-السلطة الطالبة للحفظ.

-الجريمة موضوع التحقيق و الإجراءات الجنائية و ملخصا لوقائعها مرفقا.

-كل المعلومات المتاحة التي تحدد شخصية المسؤول عن المعلومات المخزنة أو موقع نظام المعلومات.

-مبررات تدابير الحفظ.

-رغبة الدولة الطرف بتسليم طلب المساعدة القضائية للتفتيش أو الوصول أو الضبط أو كشف البيانات المخزنة[1].

و عند استلام الدولة الطرف الطلب فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل فوري و عاجل بحسب قانونها الداخلي، و لغاية الاستجابة الفورية لا تشترط الاتفاقية التجريم المزدوج للحفظ فيهما يتعلق بالجرائم المتصلة بتكنلوجيا المعلومات.

كما توصي الاتفاقيات على أن أي حفظ ناجم عن الاستجابة للطلب يجب أن يكون لفترة لا تقل عن 60 يوما حتى تتمكن الدولة الطالبة من تسليم طلب التفتيش أو الوصول أو الضبط أو التأمين أو الكشف للمعطيات[2].

[1] – أنظر المادة 29 من اتفاقية بودابست، و المادة 1/37 من الاتفاقية العربية بخصوص جرائم تقنية المعلومات.

[2] – أنظر المادة 2/37 من الاتفاقية العربية بخصوص جرائم تقنية المعلومات.

-الكشف السريع عن المعطيات المحفوظة:

نصت على هذا الإجراء كل من اتفاقية بودابست في المادة 30، و كذلك الاتفاقية العربية بخصوص جرائم تقنية المعلومات في المادة 38، و يتعلق إجراء الكشف السريع عن المعطيات المحفوظة بإجراء طلب الحفظ العاجل و هو من الإجراءات الهامة التي تكشف عن نسيج الجريمة العالق في أكثر من إقليم دولة واحدة، حيث أن الدولة المطلوب إليها حفظ البيانات المخزنة لديها في نظام معلوماتي خوفا من تغيير الحقيقة فيه تغييرا من شأنه إلحاق الضرر و من شأنه المساهمة في إفلات الجناة من العدالة، إذا اكتشف أثناء تنفيذ هذا التحفظ بأن مقدم خدمة في دولة أخرى قد اشترك في بث الاتصال، فيجب عليها أن تعلم الدولة الطالبة بالقدر الكافي من المعلومات حركة السير من أجل تحديد شخصية مقدم الخدمة و مسار بث الاتصال[1].

-حجز أو اعتراض معطيات متعلقة بالمحتوى:

نصت كذاك الاتفاقيات الدولية على ضرورة جمع أو تسجيل فوري و في الحال لمعلومات محتوية في اتصالات معينة تحول بواسطة أنظمة معلوماتية و ذلك بالحد الذي تسمح به القوانين الداخلية المطبقة و المعاهدات[2].

[1] – هلالي عبد الله احمد، اتفاقية بودابست لمكافحة جرائم المعلومات، المرجع السابق، ص 330.

[2] – المادة 34 من اتفاقية بودابست، و المادة 42 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الفقرة الثالثة: الإنابة القضائية على المستوى الدولي

تعد الإنابة القضائية الدولية من بين سبل التعاون القضائي في المجال الجنائي و التي من شأنها أن تساهم في التصدي للجرائم الماسة بالمستهلك الإلكتروني عندما تتجاوز الحدود الوطنية، فهيا تؤدي إلى تمكين دولة من الاستفادة من السلطات القضائية لدولة أخرى في حالة عجزها إقليميا في نفاذ قانونها في اتجاه المجرم[1].

و نظرا لأهمية الإنابة القضائية في انعقاد الإختصاص القضائي في كشف الجرائم و معاقبة مرتكبيها، نظمها المشرع الوطني في قانون الإجراءات الجزائية، حيث يأخذ بمفهوم الإنابة القضائية الدولية و هو القانون المطبق في حالة غياب اتفاقية قضائية مع الدول المرسل إلى سلطاتها القضائية طلب الإنابة القضائية، شريطة المعاملة بالمثل أي عدم التعاون مع الدولة الأجنبية في مجال الإنابة القضائية الدولية في حالة عدم تعاونها هي الأخرى[2]. و عليه سنحاول تبيين مفهوم الإنابة القضائية الدولة (أولا) و الإجراءات المتخذة بشأنها (ثانيا).

أولا: مفهوم الإنابة القضائية الدولية

تعتبر الإنابة القضائية لاسيما في المسائل الجنائية من الإجراءات الهامة التي لا يمكم الاستغناء عن العمل بها خاصة فيما يتعلق بالجرائم الإلكترونية بما فيها الماسة بالمستهلك الإلكتروني، فوجود أدوات الجريمة و مرتكبوها على أكثر من إقليم يرتب اندثار الأدلة و ضياعها، مما يتطلب وجود تعاون فعال من باقي الدول من أجل مساعدة الجهات المختصة، و تمكينها من الأدلة التي بحوزتها[3].

[1] – د/ سليمان احمد فضل، المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007، ص 425.

[2] – انظر المادة 721 من قانون الإجراءات الجزائية المعدل و المتمم.

[3] – عكاشة محمد عبد العال، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 30.

و يقصد بالإنابة القضائية الدولية قيام الجهة أو الدولة الطالبة بتفويض السلطة المختصة في الجهة المطلوب منها لاتخاذ إجراء أو أكثر من إجراءات التحقيق أو من إجراءات تتعلق بالجريمة المطلوب التعاون بشأنها[1].

كما يعرف جانب من الفقه الإنابة القضائية الدولية على أنها " عمل بمقتضاه تفوض الجهة القضائية المختصة جهة أخرى، للقيام مكانها، و في دائرة اختصاصها، بإحدى أو بعض إجراءات التحقيق أو الإجراءات القضائية الأخرى، و التي تعذر عليها مباشرتها بنفسها بسبب بعد المسافة أو أي مانع آخر"[2].

و مما سبق يمكن تعريف الإنابة القضائية الدولية بأنها تفويض سلطة قضائية أجنبية مختصة بموجب إنابة قضائية مكتوبة، لتنفيذ عمليات التفتيش أو الحجز أو إجراء من إجراءات التحقيق من طرف سلطة قضائية أخرى تكون مختصة بذلك التحقيق حتى تتمكن من كشف الجرائم الماسة بالمستهلك الإلكتروني و معاقبة مرتكبها، مع احترام في ذلك القانون الداخلي للدولتين، أو الاتفاقية القضائية التي تجمعهما.

ثانيا: إجراءات قبول و تنفيذ الإنابة القضائية الدولية

قد يتوقف التحقيق في الدعوى الجزائية بخصوص جريمة من الجرائم الماسة بالمستهلك الإلكتروني على إجراء الإجراءات التي تتجاوز الإختصاص الإقليمي للجهة القضائية الوطنية، الأمر الذي يتطلب معه اللجوء إلى الدولة صاحبة الإختصاص من أجل القيام بهذا الإجراء على أراضيها، و يمثل طلب الإنابة القضائية الوسيلة القانونية التي يمكن اللجوء إليها في هذه الحالة من أجل إتمام هذا الإجراء، حيث يتم إرسال هذا الطلب إلى الدولة المطلوب منها القيام بهذا الإجراء عبر الطريق الدبلوماسي، و هذا ما نصت عليه المادة 702 و 703 من قانون الإجراءات الجزائية، لذلك فإنه يتم سلوك هذا

[1] – د/ عادل عبد العال إبراهيم خراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية و سبل التغلب عليها، المرجع السابق، ص 56.

[2] – عكاشة محمد عبد العال، المرجع السابق ص 9.

الطريق في حالة عدم وجود اتفاقية أو في حالة ما اذا سكتت الاتفاقية عن تنظيم طريقة إرسال طلبات الإنابة القضائية، أو أحالت تنظيم ذلك للقانون الداخلي للأطراف[1].

إلا أنه و سعيا وراء الحد من التعقيد و البطء في الإجراءات التي تتميز بها الدبلوماسية، نجد أن بعض المعاهدات و الاتفاقيات تشترط بصدد طلب التعاون القضائي أن تحدد الدولة الأطراف سلطة مركزية أو أكثر تكون مكلفة بإرسال طلبات المساعدة أو إجابتها أو بتنفيذ أو ارسال هذه الطلبات إلى السلطات المعنية لتنفيذها[2].

و إذا تلقت السلطات الداخلية طلبا يتضمن إنابة بشأن إجراء من الإجراءات القضائية، فإن هذا الطلب يجب أن يتوفر على جملة من الشروط، و تتمثل هذا الشروط في[3]:

-أن تكون الجريمة محل المتابعة جريمة غير سياسية.

-يتم تقديم الطلب عن طريق القنوات الدبلوماسية.

-يتولى وزير الخارجية تحويل الطلب بعد فحص الملف، و المستندات المرفقة بالطلب إلى وزير العدل.

-يتحقق وزير العدل من سلامة الطلب ثم يقرر ما يراه لازما بشأن الطلب.

-يتعين أن تكون المستندات و الأوراق التي ترى الدولة الأجنبية أنها ضرورية للتبليغ مترجمة للغة العربية.

و محل الإنابة في القانون الجزائري يتمثل في إجراءات التحقيق عموما كالاستجواب ، أو إجراء معاينة، أو التفتيش، إلا أنه لا يجوز أن تمنح الإنابة القضائية تفويضا عاما للقاضي المناب، إلا إذا نصت الاتفاقية على خلاف ذلك و الملاحظ أن معظم الاتفاقيات

---

[1] – محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2008، ص 101.

[2] – انظر المادة 27 فقرة 2-ا من اتفاقية بودابست، و المادة 34 الفقرة 2-أ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] – انظر المواد 721 و 722 من قانون الإجراءات الجزائية المعدل و المتمم.

المبرمة في هذا الإطار تحيل للقانون الداخلي للطرف متلقي الطلب أولوية التطبيق فيما يتعلق بإجراءات تنفيذ الإنابة[1].

الفرع الثاني: تسليم المجرمين لتعزيز الاختصاص القضائي في مواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

إن الجرائم الواقعة على المستهلك في بيئة الأعمال الإلكترونية تهدد استقرار المعاملات الإلكترونية بصورة عامة و مصالح المستهلك بصفة خاصة، لذا يعد الاتفاق على تسليم المجرمين بين الدول حول هذه الجرائم ضرورة ملحة، و هو ما أكدت عليه اتفاقية بودابست من خلال ضرورة أن تلتزم الأطراف المتعاقدة بإدراج هذه الجرائم بوصفها جرائم تستوجب تسليم المجرمين.

و نظرا لأهمية تسليم المجرمين في معاقبة الجناة فقد نظم المشرع الوطني مسألة التسليم في قانون الإجراءات الجزائية. و عليه سنتطرق إلى مفهوم تسليم المجرمين (الفقرة الأولى) و شروط و إجراءاته (الفقرة الثانية)

الفقرة الأولى: مفهوم تسليم المجرمين

يعبر مصطلح تسليم المجرمين عن إعادة الشخص المطلوب إلى الدولة ذات السيادة و السلطة في محاكمته، و يعكس العمل به تبلور المبدأ الذي يقتضي بضرورة تعاون الدول فيما بينها للقضاء على الجريمة بشتى أشكالها، و هذا النظام يستجيب لاعتبار تحقيق المساواة بين المجرمين في المعاملة و مقتضيات حسن سير العدالة و الصالح العام بجميع الدول. لذلك سنحاول تحديد مفهوم نظام تسليم المجرمين بدأ من تحديد تعريف (أولا) و طبيعته القانونية (ثانيا)، و الخصائص التي يمتاز بها (ثالثا).

أولا: تعريف نظام تسليم المجرمين

يقصد بتسليم المجرمين مجموعة الإجراءات القانونية تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم عليه إلى دولة أخرى لكي يحاكم بها أو ينفذ فيها الحكم الصادر

[1] – إلهام بن خليفة، الرسالة السابقة، ص 358.

عليه من محاكمها[1]. و يعرف أيضا أنه إجراء بمقتضاه تتخلى الدولة عن شخص موجود في إقليمها لدولة أخرى تطالب بتسليمها إليها لمحاكمته عن جريمة منسوبة إليه ارتكبها أو تنفيذ عقوبة مقضي عليه بها من محاكم هذه الدولة[2].

و يقصد به أيضا مطالبة دولة أخرى بتسليمها شخصا ينسب إليه ارتكاب جريمة أو صدر حكم بالعقوبة ضده حتى تتمكن هذه الدولة من محاكمته، و ذلك باعتبار أنها صاحبة الإختصاص الطبيعي باتخاذ الإجراءات الناشئة عن الجريمة أو تنفيذ العقوبة الصادرة ضد الشخص المطلوب تسليمه[3].

و يرى البعض أن التسليم هو الاسترداد، و يعرفه أنه إجراء تعاون دولي تقوم بمقتضاه دولة تسمى بالدولة الطالبة بتسليم شخص يوجد في إقليمها إلى دولة ثانية تسمى بالدولة المطلوب إليها أو جهة قضائية بهدف ملاحقته عن جريمة اتهم بارتكابها أو لأجل تنفيذ حكم جنائي ضده[4].

و الملاحظ من خلال التعريفين السابقين أن التسليم ينصب على فئتين من الأشخاص، تتمثل الأولى في الأشخاص الذين تطالب الدولة تسليمهم من أجل محاكمتهم في محاكمها وفقا لقانونها، أي لم يصدر حكم بالإدانة يثبت ارتكابهم للجرم، أما الفئة الثانية فهم الأشخاص الذين تطلب الدولة تسليمهم إليها من أجل تنفيذ حكم قضائي صدر بحقهم بالإدانة، إذ أن الغاية من التسليم هيا تنفيذ العقوبة المحكوم بها.

ثانيا: الطبيعة القانونية لتسليم الجرمين

اختلفت النظم القانونية الوطنية في تحديد الطبيعة القانونية للتسليم، لذلك يعتبر تحديدها من المشاكل الصعبة التي اختلفت عليها هذه الأنظمة من حيث الطبيعة التي

---

[1] – ذناب آسية، الآليات الدولية لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة ماجستير، كلية الحقوق و العلوم السياسية ، جامعة قسنطينة، الجزائي، 2010 ، ص 177.

[2] – سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دار الجامعة الجديدة، الإسكندرية، 2007، ص 10.

[3] – ذياب آسية، نفس المذكرة، ص 177.

[4] – سليمان إبراهيم مصطفى، الإرهاب و الجريمة المنظمة، دار الطلائع، القاهرة، 2006، ص 332.

تضفيها عليها، فهناك دول ترى أن التسليم عملا من أعمال القضاء يعهد بأمره لجهة قضائية تطبق عليه العديد من القواعد المنظمة للدعاوى القضائية و هناك دول أخرى اعتبرته عملا من أعمال السيادة فيكتسب بهذا الوصف طابعا إداريا أو سياسيا، و من ثم تكون السلطة السياسية هي صاحبة البت فيه من عدمه و أخرى تتبنى نظاما مختلطا[1].

و قد عرف نظام التسليم تطورا ملحوظا فبعد أن كان يعد عملا سياسيا، تتصرف السلطة التنفيذية في البت فيه على هواها دون ضابط، فإنه و بنمو التعاون و التضامن بين الشعوب و تشابك مصالحها فغنه أخذ يتسم بطابع العدالة و القانون و مهما كانت طبيعة التسليم فإنه يلبي مطلبا من مطالب الصالح العام المشترك للأمم المتمدنة في العصر الحاضر، و تستلزمه مقتضيات العدالة و يؤلف حقا من حقوق الدولة[2].

و قد أسهم في إشكالية الطبيعة القانونية للتسليم أمران، أولها ذو طابع سياسي و الثاني ذو طابع قانوني، أما الأول فيتمثل في الارتباك الحاصل في هذه المرحلة من مراحل التطور القانوني بين ظاهرة العولمة و ما تفرضه من مقتضيات التعاون الدولي في مكافحة الجريمة، و بين مفهوم السيادة الوطنية و ما يستلزمه من مقتضيات التقيد بمسلمات و مفاهيم القانوني الجنائي، لا سيما في شقه الجنائي مما يعني إمكانية تنكر الدولة للتسليم باعتباره حقا لها، أما الأمر الثاني فإن الاتفاقيات الدولية لم تبين بشكل واضح ملامح الطبيعة القانونية لتسليم المجرمين، و ما إذا كان يعتبر عملا سياديا أو عملا قضائيا، إذ أن نصوص هذه الاتفاقيات انصرفت جلها إلى تحديد الاطار الموضوعي للتسليم من حيث الشروط الخاصة بالجريمة و محل التسليم، أو الشخص المطلوب تسليمه[3].

و الراجح أن التسليم إجراء قانوني يتم بين دولتين أو أكثر طبقا للقانون الدولي و الاتفاقيات الدولية و التشريعات الوطنية المعنية، فهو إجراء مختلط فمن جانب هو تصرف سياسي لكونه يمس العلاقات الخارجية للدول/ و من جانب فهو تصرف قانوني يمس

[1] – سليمان عبد المنعم، المرجع السابق، ص 43.

[2] – ذنايب آسية، المذكرة السابقة، ص 180.

[3] – سليمان عبد المنعم، المرجع السابق، ص 43.

بالحريات الفردية لذا ينبغي أن ينظمه القانون فلا يترك البت فيه للجهة التنفيذية فقط، و إنما ستقوم المحاكم بتطبيق قواعد و أحكام تسليم المجرمين حيث تخضع إجراءات التسليم لإشراف قضائي يكفل شرعيتها[1].

و عليه فإن الطبيعة القانونية للتسليم تتأرجح بين الطبيعة السيادية و الطبيعة القضائية، و أن الغالب هو الطبيعة السيادية ، فإذا صدر قرار مثلا من القضاء برفض التسليم فإن السلطة التنفيذية تلتزم به غالبا، أما إذا صدر قرار القضاء بقبول التسليم فإن للسلطة التنفيذية الخيار بين قبول التسليم أو عرقلته أو رفض إجراءاته.

ثالثا: خصائص نظام تسليم المجرمين

يتميز نظام تسليم المجرمين بمجموعة من الخصائص يمكن تلخيصها في الآتي:

1-الطابع الإجرائي للتسليم:

إن تسليم المجرمين هو إجراء سواء كان قضائيا في الدول التي تأخذ بالأسلوب القضائي، أو إداريا أو سبه قضائي في الدول التي تأخذ بذلك، لذلك تبدو القواعد المنظمة للتسليم قبيل القواعد الإجرائية فتأخذ أحكامها، كالتطبيق الفوري للقانون الجديد على كافة دعاوى التسليم و لو ناشئة على جريمة و قعت قبل صدور هذا القانون[2].

2-الطابع الدولي للتسليم:

يتم التسليم بين دولة و أخرى، أو بين دولة و جهة قضائية دولية، و بذلك ينعكس الطابع الدولي علة مصادره، إذ تتمثل في الغالب في الاتفاقيات و المعاهدات الدولية، و قد افضى الطابع الدولي إلى عدم النظر إليه كمحض إجراء وطني بل أصبح يكتسي

[1] – بوجمعة لطفي، الإجراءات الخاصة لمكافحة الجريمة الإرهابية، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة عنابة، الجزائر، 2016، ص 232.

[2] – سليمان عبد المنعم، الجوانب الاشكالية في النظام القانوني لتسليم المجرمين، المرجع السابق، ص33.

صبغة دولية تجعله متأثرا أحيانا ببعض أفكار و مفاهيم القانون الدولي كما في مجال قانون المعاهدات و مبدأ المعاملة بالمثل[1].

3-الطابع الطوعي أو التعاوني للتسليم:

التسليم إجراء طوعي تعاوني ينطلق من فلسفة التعاون القضائي بين الدول لمكافحة الجريمة و ملاحقة المجرمين أينما كانوا، لذلك فليس لقواعده نفس درجة الإلزام التي تتمتع بها القواعد القانونية الأخرى على الأقل من حيث الواقع، و هو الأمر الذي يفسر رفض الدول إجراء التسليم في بعض الأحيان دون مساءلتها قانونا، و مع هذا هناك اتجاه دولي يعطي لقواعد التسليم أهمية متنامية قد ترتب المسؤولية الدولية، و من الصعب إنكار تنامي الطابع الإلزامي للتسليم مع إبرام معاهدات دولية عالمية تنشئ لنفسها آليات تطبيق و مراقبة كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[2].

4-الطابع العالمي للتسليم:

يتسم التسليم بطابع "عالمي" يعكس المفاهيم العالمية المشتركة التي تأخذ أكثرية دول العالم في العصر الحالي و المرتبطة بحقوق الإنسان، و من ذلك امتناع التسليم في الجرائم السياسية او حال كون الدولية الطالبة تنص على عقوبة الإعدام ، أو اذا كان الهدف من التسليم محاكمة الشخص الأسباب دينية، عرفية ، عنصرية جنسية أو لآراء سياسية، و بهذا اصبح التسليم مرتبطا بمسألة حقوق الإنسان و مفاهيم الحرية السياسية و حماية الأقليات و كلها تشكل منظومة قيم عالمية بدأت تترك أثارها على القوالب القانونية ، و أن هذا الطابع العالمي قد تولد عن انتشار الاتفاقيات الثنائية و العالمية في مجال التسليم[3].

---

[1] – ذنايب آسية، المذكرة السابقة، ص 183.

[2] – سليمان عبد المنعم، المرجع السابق، ص 35.

[3] – بوجمعة لطفي، الرسالة السابقة، ص 234.

الفقرة الثانية: شروط و إجراءات نظام تسليم المجرمين

نصت الاتفاقيات الدولية و التشريعات الوطنية على عدة شروط لتسليم المجرمين، كما حدد مجموعة من الإجراءات بهدف إتمام هذا التسليم. و سنحاول تحديد شروط تسليم المجرمين (أولا)، و الإجراءات المتبعة بشأنه (ثانيا).

أولا: شروط تسليم المجرمين

وضعت الاتفاقيات الدولية و التشريعات الوطنية عدة شروط لتسليم المجرمين، فمنها ما يتعلق بالشخص المطلوب تسليمه و بعضها الآخر يتعلق بالجريمة محل التسليم و هو ما نوضحه كما يلي:

1-الشروط المتعلقة بالجريمة محل التسليم:

تتمثل الشروط المتعلقة بالجريمة محل التسليم في شرط التجريم المزدوج و، و أن يكون الطلب في جريمة من الجرائم الجائز بشأنها التسليم. و سنحاول تحديد كل منها على النحو التالي:

أ-**التجريم المزدوج:** تشترط معظم الدول ازدواج التجريم للسلوك الذي يطالب بالتسليم من أجله و أن يكون معاقبا عليه في قوانين الدولة طالبة التسليم و الدولة المطلوب إليها[1]. كما يجب أن يكون الفعل على درجة معينة في الجسامة (جناية أو جنحة)، و أن يكون معاقب عليه بعقوبة سالبة للحرية و اشتراط التجريم المزدوج لا يعني اشتراط تماثل التكييف للأفعال المجرمة، فيستوي أن يختلف التكييف طالما الأفعال واحدة[2].

و يتبع ازدواجية التجريم أحكام المسؤولية الجزائية، و كذلك أحكام التقادم أو انقضاء الدعوى بالتقادم، فيفترض في المطلوب تسليمه أن يكون قد بلغ السن الجنائية في الدولة الطالبة و الدولة المطلوبة إليها، أما إذا لم يبلغ هذه السن في الدولة الطالبة فترفض التسليم، و كذلك الحال إذا انقضت الدعوى العمومية بالتقادم وفقا لقانون الدولتين، و يجد

[1] – البريزات محمد، الجريمة المنظمة، الطبعة الأولى، دار الثقافة، عمان، 2008، ص 177

[2] – الفاضل محمد، التعاون الدولي لمكافحة الإجرام، مطبعة المفيد الجديدة، دون بلد نشر، 1967،، ص 84.

ذلك تبريره في أن الهدف من وراء التسليم هو محاكمة المطلوب و معاقبته على أفعاله، فإذا انقضت الدعوى حسب قانون الدولة الطالبة ، فلا يكون هناك من محل للتسليم[1].

و يشترط كذلك أن يكون قانون الدولة طالبة التسليم مختص بنظر الفعل المجرم وفقا لقانون الدولتين، و عدم اختصاصها يعني رفض التسليم، و بالمقابل يتعين ألا يكون قانون الدولة المطلوب منها التسليم مختصا بمحاكمة المطلوب تسليمه عن ذات الفعل المنسوب إليه ارتكابه[2].

أما المشرع الجزائري فقد اعتمد في شرط ازدواجية التجريم، إذ يجب أن تكون الجريمة على درجة معينة من الخطورة جناية أو جنحة[3]، و هو ما يتفق مع مبدأ أن الدولة لا تشارك في معاقبة أفعال لم تكن في نظرها أفعال جنائية[4].

ب-أن يشكل الفعل جريمة من الجرائم الجائز بشأنها التسليم:

اجمع المجتمع الدولي و القوانين الوطنية[5] رفض التسليم بشأن بعض الجرائم من نطاق التسليم، و سنحاول تحديد هاته الجرائم على النحو التالي:

-**الجرائم السياسية:** يثير استبعاد الجريمة السياسية صعوبات كبيرة ، و تكمن هذه الصعوبات في عدم وجود تعريف للجريمة السياسية سواء على المستوى التشريعات الوطنية أو الاتفاقيات الدولية، و بالرجوع إلى الفقه نجد أن هناك مذهبين (المذهب الشخصي، و المذهب الموضوعي) في تعريف الجريمة السياسية.

فالمذهب الشخصي، اعتبر أن معايير تحديد الجريمة السياسية تتمثل في الدافع لارتكاب الجريمة، فإذا كان الدافع سياسيا اعتبرت الجريمة سياسية أيا كان موضوعها و

---

[1] – البريزات محمد، المرجع نفسه، ص 178.

[2] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنيت، المرجع السابق، ص 89.

[3] – تنص المادة 03/697 من قانون الإجراءات الجزائية المعدل و المتمم انه" ... لا يجوز قبول التسليم في أية حالة إذا كان الفعل غير معاقب عليه طبقا للقانون الجزائري بعقوبة جناية أو جنحة".

[4] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع نفسه، ص 89.

[5] – لاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 4/31 و اتفاقية بودابست في المادة 4/24.

أيا كانت المصلحة القانونية المعتدي عليها. أما المذهب الموضوعي فيرى أصحابه أن الاعتماد على طبيعة المصلحة محل الاعتداء و موضوعها، هو المعيار الذي يحدد طبيعة الجريمة، فيرى أصحاب هذا المذهب أن العبرة بطبيعة الجريمة نفسها و وضعيتها الخاصة[1].

إن العلة من إبعاد الجرائم السياسية من نطاق التسليم راجع إلى أنها ليست مظهرا لنفسية خطرة لدى مرتكبها، و إنما الغرض منه اتخاذ إجراءات انتقامية ضد الشخص المطلوب تسليمه، و هو عمل لا يليق بالدولة المطلوب منها التسليم أن تساهم في تنفيذه[2]، و يلقى هذا الاستبعاد إجماعا بلغ حد تكريس مبدأ قانوني، إذ توجب بعض الاتفاقيات رفض التسليم في الجرائم السياسية[3]، كما استثنى المشرع الجزائري التسليم في الجرائم السياسية ، حيث نصت المادة 689 من قانون الإجراءات الجزائية أنه" لا يقبل إذا كانت للجناية أو الجنحة صبغة سياسية أو إذا تبين من الظروف أن التسليم مطلوب لغرض سياسي".

و بالرجوع إلى قانون العقوبات نجد أن المشرع الجزائري لم يفرق بين الجرائم السياسية و العادية، كما أنه لم يميز بين الجرائم السياسية المجردة و تلك المركبة. كما أنه أخذ بالمعيار الشخصي في تحديد الجريمة السياسية من خلال المادة 66 من الدستور، في حين يأخذ قانون الإجراءات الجزائية بالمعيار الموضوعي.

-**الجريمة العسكرية:** تتفق اغلب الاتفاقيات الدولية و التشريعات الوطنية على استبعاد الجريمة العسكرية من نطاق التسليم[4]، و الجريمة العسكرية تلك الجرائم التي تقع من شخص ذي صفة عسكرية بالمخالفة للواجبات العسكرية أو للنظام العسكري التي يفرضها قانون القضاء العسكري و ينعقد الإختصاص فيها للقضاء العسكري، و هي في

[1] – بوجمعة لطفي، الرسالة السابقة، ص 235 و 236.

[2] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 89.

[3] – أنظر المادة 3 من الاتفاقية الأوروبية للتسليم المجرمين .

[4] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 90.

جوهرها صورة من الجريمة التأديبية غير أنها تتميز بخصوصية النظام و خطورة الجزاءات[1].

و يجب التمييز بين الجريمة العسكرية البحتة و التي يرتكبها العسكريون أثناء الخدمة و جرائم القانون العام المرتكبة من قبل العسكريين، لأن الفئة الأولى لا يجوز التسليم بشأنها أما الفئة الثانية فيجوز التسليم بشأنها[2].

2-الشروط المتعلقة بالشخص المطلوب تسليمه:

تتمثل الشروط المتعلقة بالشخص المطلوب تسليمه في كل من مبدأ عدم جواز تسليم الرعايا، و عدم جواز تسليم ممنوحي حق اللجوء السياسي، و كذلك لا يجوز تسليم من تمت محاكمته عن ذات الجريمة المطلوب تسليمه لأجلها. و سنحاول توضيح كل شرط على حدى:

أ-**مبدأ عدم جواز تسليم الرعايا:** يعتبر مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم، من المبادئ المستقر عليها المجتمع الدولي و المنصوص عليها في الاتفاقيات الدولية و القوانين الداخلية للدول[3]، و هو ما نصت عليه المادة 1/4 من معاهدة الأمم المتحدة بشأن تسليم المجرمين و نصت عليه كل من اتفاقية بودابست في المادة 6/24 و الاتفاقية العربية لمكافحة تقنية المعلومات في المادة 6/31 ، و تنص المادة 698 الفقرة الأولى من قانون الإجراءات الجزائية الجزائري " لا يقبل التسليم ... إذا كان الشخص المطلوب تسليمه جزائري الجنسية ...'.

[1] – سليمان عبد المنعم، الجوانب الإشكالية في نظام القانوني لتسليم المجرمين، المرجع السابق، ص 191.

[2] – انظر المادة 3/697 من قانون الجزائية المعدل و المتمم.

[3] – رمزي النويصر، "**التعاون الدولي في مجال مكافحة جرائم الإنترنت**"، مجلة القضاء و التشريع، العدد08، تونس،2011، ص 85.

ب-لا يجوز تسليم من تمت محاكمته عن ذات الجريمة المطلوب تسليمه لأجلها:

يعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمه، و يهدف إلى توفير أكبر قدر ممكن من الحماية القضائية للشخص المطلوب تسليمه في الدولة الطالبة، و ذلك حتى لا يتعرض الطلوب لعقوبة مزدوجة[1].

ثانيا: إجراءات تسليم المجرمين

تتم إجراءات تسليم المجرمين من دولة لأخرى بحسب النظام القانوني المتبع في كل دولة لاسيما بالنسبة للدول المنابة، إلا أن هناك قواعد ثابتة على المستوى الموضوعي و الإجرائي تجمع الدول من حيث المبدأ، و تختلف بالأخذ بها، كما تجمع أغلب الأنظمة على احترام مجموعة من الحقوق للشخص محل التسليم.

1-سير إجراءات تسليم المجرمين:

يعتبر طلب التسليم الأداة التي تحركها الدولة الطالبة من أجل الحصول على الشخص المتهم أو المحكوم عليه في هذه الدولة، حيث يقدم طلب التسليم كتابة، و يحال بمرفقاته و كذلك المراسلات اللاحقة، عبر القنوات الدبلوماسية مباشرة بين وزارتي العدل و أية سلطات أخرى يحددها القانون[2]، إذ يرفق هذا الطلب حسب قانون الإجراءات الجزائية الجزائري، إما بالحكم الصادر بالعقوبة حتى و لو كان غيابيا، و إما أوراق الإجراءات الجزائية التي صدرت بها الأمر رسميا بإحالة المتهم إلى جهة القضاء الجزائي أو التي تؤدي إلى ذلك بقوة القانون، و أما بأمر القبض أو أية ورقة صادرة من السلطة القضائية و لها ذات القوة على أن تتضمن هذه الأوراق الأخيرة بيان دقيقا للفعل الذي صدرت من أجله، و تاريخ هذا الفعل، و على أن تقدم أصول هذه الأوراق أو نسخ رسمية عنها، و

[1] – إلهام بن خليفة، الرسالة السابقة، ص 363.

[2] – د/ محمد أمين البشري، و د/ محمد عبد الحميد احمد، المرجع السابق، ص 306.

كذلك تقدم الدولة الطالبة نسخة من النصوص المطبقة على الفعل المكون للجريمة، و أن ترفق ببيان بوقائع الدعوى[1].

إذ يتولى وزير الخارجية تحويل الطلب و مرفقاته إلى وزير العدل الذي يتحقق من سلامته و يعطيه خط السير الذي يطلبه القانون، و يحيله إلى القضاء ليتخذ إجراءات استجواب المطلوب تسليمه و إبلاغه بالمستند الذي قبض عليه بموجبه، و تحرير محضر بذلك ثم ينقل إلى سجن العاصمة ليحبس فيه، ثم يعاد استجوابه من قبل النائب العام لدى المحكمة العليا، و يحرر محضرا بذلك، ثم ترفع المحاضر إلى الغرفة الجزائية بالمحكمة العليا، و يمتثل المطلوب تسليمه أمامها و يستجوب في جلسة علنيا ما لم يتقرر خلاف ذلك باءا على طلب النيابة أو المطلوب، و تسمع في الجلسة مطالب النيابة العامة و أقوال الشخص المطلوب، و يمكنه أن يستعين بمحام مقبول أمامها و بمترجم، و يجوز الإفراج عنه في كل وقت أثناء الإجراءات[2].

و إذا قرر المطلوب تسليمه قبول تسليمه إلى سلطات الدولة الطالبة فتثبت المحكمة هذا الإقرار و تحول نسخة منه بغير تأخير إلى وزير العدل بواسطة النائب العام ليتخذ ما يراه مناسبا[3].

و في حالة عدم وجود إقرار ، فإن المحكمة تبدي رأيها حول طلب التسليم، فإذا رفضته بسبب وجود خطأ تراءى لها أو أن الشروط القانونية غير مستوفاة فإنها تصدر رأيا مسببا برفض طلب التسليم و الذي يكون نهائي، و لا يجوز معه قبول التسليم بحيث يعاد الملف إلى وزير العدل، و في الحالة العكسية يعرض وزير العدل لتوقيع مرسوما بالإذن بالتسليم، و تبلغ به حكومة الدولة الطالبة، و إذا انقضى ميعاد شهر من يوم

[1] – انظر المادة 702 من قانون الإجراءات المعدل و المتمم.

[2] – أنظر المواد من 703 إلى 707 من قانون الإجراءات الجزائية المعدل و المتمم.

[3] – أنظر المادة 708 من قانون الإجراءات الجزائية المعدل و المتمم.

التبليغ دون أن يقوم ممثلو الدولة الطالبة باستلام المطلوب يفرج عنه، و لا يجوز المطالبة به بعد ذلك لنفس السبب[1].

كما نظم المشرع الجزائري إجراءات طلب التسليم في حالة الاستعجال، يمكن أن يأمر وكيل الجمهورية بالقبض على الأجنبي إذا ورده إخطار من السلطات القضائية للدولة الطالبة سواء بالبريد أو بأي طريقة من طرق الإرسال التي يكون لها أثر مادي يدل على وجود أحد المستندات التي نصت عليها المادة 702 سالفة الذكر، غير أنه يجب على السلطات الطالبة في نفس الوقت أن ترسل إخطارا قانونيا عن الطريق الدبلوماسي أو الريد أو بأي طريق آخر من طرق الإرسال التي يكون لها اثر مكتوب إلى وزارة الخارجية ، و يجب على النائب العام أن يحيط وزير العدل و النائب العام لدى المحكمة العليا بهذا القبض، و يمكن الإفراج عن المطلوب المقبوض عليه إذا لم تبلغ السلطات الجزائرية خلال 45 يوما من تاريخ القبض بالمستندات الواردة في المادة 702 من قانون الإجراءات الجزائية، حيث يتقرر الإفراج عنه بعريضة توجه إلى المحكمة العليا لتفصل فيها خلال 8 أيام بقرار غير قابل للطعن فيه، أما إذا وصلت المستندات فتستأنف الإجراءات السابقة[2].

و الملاحظ من خلال هذه النصوص أن المشرع الجزائري نظم تسليم المجرمين باعتبار أن الجزائر هي الدولة المطلوب منها التسليم فقط، و لم ينص على الإجراءات الواجب اتباعها باعتبار الجزائر هي الدولة الطالبة للتسليم.

و في حالة تعدد طلبات التسليم، فإن الراجح من خلال الاتفاقيات الدولية و التشريعات المقارنة، أن تكون الأولوية في التسليم للدول التي أضرت الجريمة بمصالحها ثم الدول التي ارتكبت الجريمة في إقليمها، ثم للدولة التي ينتمي إليها الشخص المطلوب تسليمه[3].

[1] – انظر المواد من 709 إلى 711 من قانون الإجراءات الجزائية المعدل و المتمم.

[2] – انظر المادتين 712 و 713 من قانون الإجراءات الجزائية المعدل و المتمم.

[3] – الفاضل محمد، المرجع السابق، ص 168.

2-ضمانات الشخص محل التسليم:

تتمثل ضمانات الشخص محل التسليم في كل من احترام حقوق الدفع و عدم جواز المحاكمة على الفعل مرتين، و هو ما سنحاول توضيحه على النحو التالي:

-**احترام حقوق الدفاع:** تحرص الدول أن تتضمن معاهدات التسليم نصوصا تخولها حق رفض طلب التسليم متى كانت المعايير المتعارف عليها دوليا بشأن عدالة المحاكمة و كفالة حقوق الإنسان و سلامة الإجراءات الجنائية غير متوافرة، و تتعرض الدول التي تنتهك هذه الضمانات لإمكانية مسائلتها أمام الآليات الدولية أو الإقليمية المعنية بحماية حقوق الإنسان و مراقب احترام الدول لها[1].

-**عدم جواز ثنائية المحاكمة:** و مفاد ذلك عدم معاقبة الشخص على الفعل مرتين، و من ثمة فإن الدولة المطلوب إليها التسليم أن ترفض الطلب إذا كان الشخص المطلوب قد سبقت محاكمته أما محاكمها، و عليها أن تحترم حجية الحكم الصادر من محاكمها و تمنع تسليمه.

كما تأبى الدولة أن يعاقب الشخص على الفعل مرتين لذلك تنص الاتفاقيات على رفض التسليم إذا كان مبني الطلب أفعال تمت المحاكمة عنها، و من المبررات أيضا تحقيق استقرار المراكز القانونية للأفراد، و احترام الحكم الجنائي ذاته بوصفه عنوانا للحقيقة لا سيما عندما يصير الحكم نهائيا[2].

[1] – د/ محمد امين البشري، و د/ محمد عبد الحميد احمد، المرجع السابق، ص 310.

[2] – سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، المرجع السابق، ص 283.

المطلب الثاني: إشكاليات التعاون الدولي كآلية لانعقاد الإختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني

التعاون الدولي بكافة صوره كآلية مكملة لانعقاد الاختصاص القضائي لمواجهة الجرائم الماسة بالمستهلك الإلكتروني و إن كان يعد مطلبا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، إلا أنه ثمة صعوبات و معوقات تقف دون تحقيقه، سواء تعلقه هذه الإشكاليات بالوضع الداخلي للدول (الفرع الأول) أو كانت ذات بعد دولي (الفرع الثاني).

الفرع الأول: إشكاليات التعاون الدولي على المستوى الوطني في الجرائم الماسة بالمستهلك الإلكتروني

من أهم إشكاليات التعاون القضائي الدولي على المستوى الوطني نجد عدم كفاية و ملائمة القوانين القائمة و اختلاف النظم القانونية الإجرائية و صعوبة إثبات الجريمة الإلكترونية بما فيها الماسة بالمستهلك الإلكتروني. و عليه سنتطرق إلى اشكل عدم كفاية و ملاءمة التشريعات القائمة (الفقرة الأولى)، و اختلاف الأنظمة القانونية الإجرائية في مكافحة الجريمة الماسة بالمستهلك الإلكتروني (الفقرة الثانية)، و الصعوبات المتعلقة بإثبات الجرائم الماسة بالمستهلك الإلكتروني (الفقرة الثالثة).

الفقرة الأولى: عدم كفاية و ملائمة التشريعات القائمة

على الرغم من التطور التكنلوجي في جميع نواحي الحياة و اعتماد الجميع في سائر شؤونهم، و استغلال مجرمي المعلوماتية للتقنية في ارتكاب جرائمهم، فإن هذا التطور لا يقابله تطور بنفس الدرجة في النصوص القانونية.

و بالرغم من إصدار الدول لقوانين تتعلق بمكافحة الجرائم الإلكترونية و انضمامها إلى العديد من الاتفاقيات، فإنه لا يمكن اعتبارها جامعة مانعة ، إذ تشكل نصوص التجريم في مجال المعلوماتية عقبة أما إنفاذ قواعد التعاون الدولي بألياته المختلفة لأسباب متعددة لعل أهماها تلك المبادئ التي أسس التجريم العامة و منها مبدأ قانونية الجرائم و

العقوبات[1] نتيجة لما يخلفه من أوجه للقصور بالأنظمة التشريعية القائمة، و الآثار السلبية الناجمة عن ذلك في السياسات الجنائية المتبعة في مكافحة جرائم الإلكترونية العابرة للحدود و الحد منها[2].

فما يكون مباح في أحد الأنظمة القانونية قد يكون مجرما و غير مباح في نظام آخر، و لعل مبرر هذا التباين راجع إلى الطبيعة القانونية الجديرة بالحماية في هذه الدول، و هو الأمر الذي يؤدي إلى فشل التعاون الدولي نظرا لاشتراط الدول لثنائية التجريم ، لتقف في هذه الحالة الدول عاجزة لأنها أولا لم تجرم الفعل و ثانيا أنه يتبع عدم التجريم عدم تهيئة الوسائل الفنية و الإمكانات اللازمة للتحقيق في الجرائم الإلكترونية، و يترتب على ذلك إغراء مجرمي المعلوماتية على إعداد انفسهم و ارتكابهم للجرائم، دون تقيد بالحدود الجغرافية حيث أن الأمر لا يتوقف عند حد صعوبة التعاون الدولي بل أنه في حالة عدم التجريم الداخلي لكل سلوك جديد تفرزه التكنلوجيا يصعب من مهمة رجال الضبط و القضاء في الدولة في ضبط الجرائم و ملاحقة مرتكبيها و عليه إفلات المجرم من العقاب، و هو ما يتطلب بذل المزيد من الجهود[3].

[1] – إلهام بن خليفة، الرسالة السابقة، ص 369.

[2] – جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعةالأولى، دار النهضة العربية، القاهرة، 1992، ص 190.

[3] – سامي على حامد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 126.

الفقرة الثانية: اختلاف النظم القانونية الإجرائية

بسبب تنوع و اختلاف النظم القانونية الإجرائية، نجد أن طرق التحري و التحقيق و المحاكمة التي تثبت فائدتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية، و التفتيش و غيرها من الإجراءات. فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيقات أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى[1]، و بالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى و إن كان هذا الدليل تم الحصول عليه في ظل اختصاص قضائي و بشكل مشروع[2].

مما لا شك فيه أن أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة و المجرمين هي الحصول على المعلومات و البيانات المتعلقة بهم، و لتحقيق هذا الهدف كان لزما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة[3].

فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة و المعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة و لمجرمين معينين، و بالتالي تنعدم الفائدة من هذا التعاون.

---

[1] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 72.

[2] – محمود إبراهيم غازي، الحماية الجنائية للخصوصية و التجارة الإلكترونية ، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص 59.

[3] – عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، 2006،، ص 104.

و عليه فإن اختلاف النظم القانونية الإجرائية يجعل التعاون الدولي دون جدوى لأنه لم يحقق الغاية المرجوة في التكاتف من أجل عدم بقاء الجاني بدون عقاب، و هو ما يتطلب أيضا تكثيف الجهود في محاولة توحيد النظم الإجرائية و الإجراء الجنائية.

الفقرة الثالثة: معوقات إثبات الجرائم الماسة بالمستهلك الإلكتروني

إن دخول العالم في مجال تكنلوجيا المعلومات و قيام ثورة عالمية في مجال نقل المعلومات و تبادلها عبر الأنظمة الإلكترونية و أهماها الإنترنت، أدى إلى تغيير مفهوم الإثبات تبعا لإمكانية إنشاء الحقوق و الالتزامات بطرق إلكترونية، مما صعب إثبات الجرائم الواقعة في البيئة الإلكترونية، و يمكن حصر هذه الصعوبات في:

أولا: تخلف الآثار المادية للجرائم الماسة بالمستهلك الإلكتروني

إن الجرائم الماسة بالمستهلك في المعاملات الإلكترونية تتم في الغالب ضمن بيئة افتراضية منطقية غير مادية أي غير محسوسة، تتم بأفعال و أو أومر على شكل نبضات إلكترونية غير مرئية، و بالتالي لا تترك هذه الجرائم أي دلائل مادية[1].

فكون الآثار التي تتخلف عن أغلب هذه الجرائم ذات الطبيعة غير المادية، هيا بذاتها تمثل صعوبة أمام إثباتها بل و عقبة أمام ذلك لا يمكن تجاوزها، إلا من خلال اتباع نمط في الإثبات ينسجم و طبيعة هذه الجرائم[2]. غير أن هذا لا يعني أن الجرائم المتقدمة لا تختلف عنها آثار مادية بصورة مطلقة، بل منها ما تخلف هذه الآثار التي تعتمد كدليل على ارتكاب الجريمة، و من ثم يعتمد عليه في نطاق إثباتها[3].

[1] – أسامة احمد المناعسة، صايل فاضل الهواوشة، جرائم الحاسب الآلي و الإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر، 2001، ص 289.

[2] – سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص 50

[3] – أسامة احمد المناعسة، صايل فاضل الهواوشة، المرجع نفسه، ص 289.

ثانيا: نقص فعالية أساليب الحصول على أدلة كشف الجرائم الماسة بالمستهلك الإلكتروني

إن تقديم أدلة إثبات غير تلك التي عهدها القاضي كالمحررات الإلكترونية و وسائل البريد الإلكتروني و التوقيع الإلكتروني، تطرح إشكاليات و ذلك لاختلاف المعايير و المواصفات القانونية لأدلة الإثبات العادية مقارنة مع الإلكترونية.

و على الرغم من استحداث الاتفاقيات الدولية و القوانين الوطنية لإجراءات تتوائم مع هذا الدليل غير أنه توجد عدة معوقات تؤدي إلى عدم فعالية الأساليب و الوسائل المستخدمة في استخلاص الدليل الإلكتروني من جهات التحقيق[1]، أهمها نقص الخبرة لدى جهات التحقيق حيث يتطلب الكشف عن هذه الجرائم اكتساب هذه الأخيرة مهارات خاصة على نحو يساعدهم على مواجهة التقنيات المعلوماتية، إذ يرى المتخصصون في مكافحة الجرائم المعلوماتية أن الأنشطة المعلوماتية و ما يقع عليها من جرائم تعد تحديا هائلا لأجهزة العدالة الجنائية ذلك أن رجال التحقيق غير المختصين و الذين اختصرت معلوماتهم في جرائم قانون العقوبات بصورته التقليدية لن يكونوا قادرين على التعامل مع الجريمة المعلوماتية و التي تقع بطريقة تقنية عالية[2].

و من المعوقات أيضا ندرة البرامج التدريبية اللازمة لتأهيل المحققين و قلة إلمامهم بالبرامج الخاصة بالتعدي و الاختراق و الاحتيال الإلكتروني، و قلة الإمكانيات الفنية اللازمة لإثبات هذه الجريمة التي يحتاج اكتشافها إلى تقنيات تتبع و تسترجع المعلومات[3]، و تتبع مصدر الاختراق و التعدي، و من أهم الصعوبات أيضا عدم ثقة الجهات القضائية بالدليل الإلكتروني لإمكانية تزويره في ضوء تعدد المستخدمين و انتشار تقنيات الاختراق، و عدم الثقة هذه تحول دون قبوله دليل إدانة[4].

---

[1] – خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، الرسالة السابقة، ص 372.

[2] – رشيدة بوكر ، المرجع السابق، ص 461.

[3] – حسن فتحي الحامولي، التعاون الدولي الأمني في تنفيذ الأحكام الجزائية، دون دار نشر، دون بلد نشر، 2015، ص 400.

[4] – خليفي مريم، الرسالة السابقة، ص 372.

فنقص المهرات الفنية في استخدام الكمبيوتر و الإنترنت و عدم توفر المعرفة بأساليب ارتكاب الجريمة الإلكترونية و قلة الخبرة و الوسائل التقنية في مجال التحقيق عن جرائم العالم الافتراضي، عوامل من شأنها أن تضعف دور التعاون الدولي في ردع الجناة ، و على السلطات أن تقوم بتدريب الخبراء و تأهيلهم ليكون لهم خطط و مألات يتبعونها لتأمين البيئة التي ارتكبت فيها الجريمة من التلاعب أو المساس عن بعد، و للحفاظ على الأدلة و ضمان عدم تغييرها و استرجاع الأدلة المدمرة، و ينبغي توفير كل الوسائل التقنية التي تسمح بالحصول على الدليل التقني الذي يعتمد عليه أما القضاء[1].

[1] – حنان ريحان مبارك، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص 375.

الفرع الثاني: إشكاليات التعاون الدولي على المستوى الدولي في الجرائم الماسة بالمستهلك الإلكتروني

إضافة إلى الإشكالات المطروحة على المستوى الوطني، عناك إشكالات أخرى تطرح على المستوى الدولي، فمنها ما يتعلق بمشكلة الاختصاص (الفقرة الأول)، و كذلك إشكالات الإنابة القضائية (الفقرة الثانية)، و تسليم المجرمين (الفقرة الثالثة)، و كذلك ما يتعلق بمجال التدريب (الفقرة الرابعة).

الفقرة الأولى: مشكلة الاختصاص و تنفيذ الأحكام الأجنبية في الجرائم المتعلقة بالمستهلك الإلكتروني

تعد الجرائم الإلكترونية بما فيها الماسة بالمستهلك الإلكتروني من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي أو الدولي و لا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك[1]، و لكن المشكلة تثار بالنسبة للإختصاص على المستوى الدولي حيث اختلاف التشريعات و النظم القانونية و التي قد ينجم عنها تنازع في الإختصاص بين الدول بالنسبة للجرائم الإلكترونية الماسة بالمستهلك التي تتميز بكونها عابرة للحدود[2].

فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا يكون الجريمة خاضعة للإختصاص الجنائي لدولة الأولى استنادا إلى مبدا الإقليمية، و تخضع كذلك لإختصاص الدولة الثانية على أساس مبدأ الإختصاص الشخصي في جانبيه، و قد تكون هذه الجريمة من الجرائم التي تهدد أمن و سلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدا العينية[3].

و تتجلى الصعوبة هنا في مشكلة تطويع النصوص القانونية المجسدة لقواعد الإختصاص و في تعقيد الأنماط الإجرامية في البيئة الإلكترونية، و تعدد الأوصاف و

---

[1] – هذه المعايير الثلاثة هي مكان القبض على المتهم و مكان وقوع الجريمة ، و محل إقامة المتهم.

[2] – محمود إبراهيم غازي، المرجع السابق، ص 60.

[3] – د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، المرجع السابق، ص 73.

التكيفات التي يمكن أن تأخذها هذه الأخيرة، إضافة إلى التباين الذي تعرفه التشريعات الوطنية في تأسيس اختصاصها القضائي دون تجاهل لدور هذه العقبات في تبرير مشكلة التنازع في الإختصاص القضائي الدولي بنظر الجرائم الإلكترونية إيجابا كان أو سلاب حال دفع دولتين أو أكثر بانعقاد اختصاصها القضائي بنظر الوقائع المذكورة أو تنفي ذلك مع اشتراط أن تكون واحدة منها مختصة على الأقل و هو ما يثيره و بكل تأكيد المفهوم التقليدي لمبدأ الإقليمية[1].

أما عن تنفيذ الأحكام الجنائية، فتعتبر الأحكام الوسيلة القانونية التي تعبر عن سلطان الدولة على الأقاليم التي تصدر فيها هذه الأحكام و تتجلى فيها سيادة الدولة بأقوى مظاهرها، و عليه فإن تنفيذ الأحكام الجنائية على إقليم الدولة لا يجد أي صعوبة فيها تطبيقا لمبدأ إقليمية القواعد الجنائية[2]، و الإشكالية هنا في إمكانية تنفيذ الدولة لأحكامها الجنائية على إقليم دولة أخرى، و الحقيقة أن هناك تباين في المواقف التشريعية في عرض هذه المسألة بين مقر بهذه الحجية و رافض لها، و لكل تيار ما يبرر توجهه غير أن هذا التباين في المواقف و الخلاف في الآراء قد أثر سلبا على إنفاذ قواعد التعاون الدولي و سريان آلياته هذا من جهة و من جهة ثانية تظهر الإشكالية المتصلة بإنفاذ هذه القواعد إشكالية شروط سريان الأحكام الأجنبية و آليات إنفاذه خارج أقاليم الإدانة[3].

[1] – عادل بوزيدة، الرسالة السابقة، ، ص 161.

[2] – حمزة سالم، التعاون الدولي في تنفيذ الأحكام الجنائية الأجنبية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2003، ص 09.

[3] – عادل بوزيدة، الرسالة السابقة، ص 162.

الفقرة الثانية: الصعوبات الخاصة بالمساعدة القضائية

نعلم أن الأصل بالنسبة لطلبات الإنابة القضائية الدولية و التي تعد من أهم صور المساعدة القضائية الدولية في المجال الجنائي أن تسلم بالطريق الدبلوماسي و هذا بالطبع يجعلها تتسم بالبطء و التعقيد، و الذي يتعارض مع بيئة الأنشطة الإلكترونية و ما تتميز به من سرعة، الأمر الذي يستحيل معه القيام بإجراءات فعالة تؤدي إلى كشف الجريمة الإلكترونية ونسبتها إلى مرتكبيها، إذ أن الجرائم الماسة بالمستهلك في التعاملات الإلكترونية تستلزم ردود سريعة خشية التلاعب بالبيانات التي قد تشكل دليلا ضد المتهم[1].

كذلك من الصعوبات الكبيرة في مجال المساعدة القضائية الدولية المتبادلة التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة و غيرها من الأسباب[2].

و إذا كانت السرعة هيا أحد المفاتيح الرئيسية لمكافحة الجرائم الإلكترونية بفعالية، فإن تعديل الآليات التقليدية للتعاون الدولي أصبح ضرورة ملحة، و يتم ذلك من خلال إبرام الاتفاقيات الدولية من أجل تسهيل إجراءات تنفيذ الإنابة القضائية بما يتلاءم مع طبيعة هذه الجريمة، حيث تتداول هذه الإنابة مباشرة بين السلطات القضائية[3].

و من الإشكاليات أيضا تزاحم الطلبات أو تعددها و التي تتضمن كلها التماسا بإجراء و مباشرة ألية من آليات التعاون الدولي القضائي في شأن نفس الأشخاص و ذات الوقائع، و اختلاف التشريعات الوطنية في الفصل في هذه المسألة[4]، كما أن عدم الرد على الطلب لا يجد مبررا في مدى إلزامية الدولة في الرد أم لا، فمن التشريعات من يعتبر أن الطلب من قبيل الأعمال الإدارية أو القضائية و اتجاه أنظمة أخرى نحو الجمع

[1] – جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 91.

[2] – محمود إبراهيم غازي، الحماية الجنائية للخصوصية و التجارة الإلكترونية، المرجع السابق، ص 61.

[3] – إلهام بن خليفة، الرسالة السابقة، ص 374.

[4] – / جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع نفسه، ص 63.

بين التكييفين، الأمر الذي يوقع بعض آليات التعاون القضائي بين اعتبار السيادة الوطنية من ناحية و بين مقتضيات التعاون الدولي من ناحية أخرى، فتبعا للاتجاه الأول تعد الآليات القضائية حقا للدولة و لا يمكن إلزامها به أما بالنسبة للاتجاه الثاني تكون هذه الآليات واجبا يقع إنفاذه على عاتق الدولة المطلوب منها[1].

الفقرة الثالثة: الصعوبات الخاصة بتسليم المجرمين

التجريم المزدوج من أهم الشروط الخاصة بتنظيم تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية و الاتفاقيات الدولية المعنية بتسليم المجرمين، و بالرغم من أهميته تلك ، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم الإلكترونية سيما و اذا كان قانون الدولة المطلوب منها التسليم لا يجرم الفعل الذي ارتكبه المطلوب تسليمه[2].

و من إشكاليات تسليم المجرمين أيضا التزاحم في طلب التسليم و هي الحالة التي يصل فيها إلى الدولة المطلوبة منها التسليم أكثر من طلب لتسليم نفس الشخص من عدة دول طالبة سواء أكان الطلب متعلق بنفس الجريمة أو بجرائم أخرى، بمعنى أنه قد يرتكب شخص واحد لجريمة تمس بمصالح أساسية لعدة دول و لهذا تتعد طلبات التسليم على الدولة الموجود على أرضها المطلوب تسليمه[3]. و للقول بالتزاحم لا يكفي مجرد الادعاء أو التصريحات الشفوية أو إبداء الرغبة في استلام الشخص بل لا بد من تقديم الطلب و مرفقاته التي تثبت نسبة الجريمة للمطلوب تسليمه، كما لا يشترط في التزاحم أن تكون الطلبات مرسلة في وقت واحد، بل يكفي تواليها على الدولة المطلوب منها، فالمهم أن يكون المطلوب لم يتم تسليمه بعد إلى أية دولة[4].

---

[1] – عادل يحيى ، التعاون الدولي في تنفيذ الأحكام الأجنبية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2004، ص 38.

[2] – د/ جميل عبد الباقي الصغير، الجوانب الإجرائية، المرجع السابق، ص 91.

[3] – إلهام بن خليفة، الرسالة السابقة، ص 375.

[4] – د/ عادل عبد العالي إبراهيم خراشي، المرجع السابق، ص 65.

الفقرة الرابعة: الصعوبات المتعلقة بمجال التدريب

تتمثل الصعوبات المتعلقة بمجال التدريب في عدم رغبة بعض الدول في تدريب القائمين على الكشف على الجرائم الإلكترونية لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية و ما اكتسبوه من خبرات[1].

و من الصعوبات أيضا و التي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين و تأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة و متكافئة لدى مختلف الأفراد التدربين، سيما في مجال تكنولوجيا المعلومات و شبكات الاتصال حيث أنه يوجد بعض الأشخاص ممن لا يعي في هذا المجال شيء، و على النظر يوجد أناس على درجة كبيرة من المعرفة و الثقافة في هذا المجال[2].

بالإضافة إلى نظرة التدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبئ لا طائل منه تهدد العملية التدريبية برمتها و بالطبع نسف التعاون الدولي في هذا المجال.

أيضا من الصعوبات التي قد تؤثر على العملية التدريبية و على التعاون الدولي فيما يتعلق بالملامح العامة المميزة للبيئة التدريبية و عدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما و متقنا، من حيث ما يدور بها من وقائع و ملابسات و إجراءات، و ما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية[3].

[1] – محمود إبراهيم غازي، المرجع السابق، ص 62.

[2] – حسين فتحي الحامولي، المرجع السابق، ص 450.

[3] – محمود إبراهيم غازي، المرجع السابق، ص 62.

الفصل الثاني: إثبات الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

يشهد العالم ثورة تكنولوجيا المعلومات، قوامها المعلومات و المعرفة التي أصبحت أساس التنمية و زيادة الإنتاج و تحقيق الرفاهية، و هو ما أدى إلى ظهور أنماط جديدة من الجرائم الإلكترونية بما فيها تلك الماسة بالمستهلك الذي يعتمد على المعاملات الإلكترونية لتوفير احتياجاته.

و تطرح الجرائم الماسة بالمستهلك الإلكتروني العديد من المشاكل و التحديات الإجرائية، و من بينها إثبات هذه الجرائم، حيث يحتاج هذا النوع من الجرائم لكشفها أدلة مستخرجة من نفس البيئة التي ارتكبت فيها هذه الجرائم، إذ أصبح الدليل الإلكتروني ضرورة لكشف أنماط هذه الجرائم، كما أن كيفية و مكانة هذا الدليلي يثير نوع من الإشكالات أمام الجهات القضائية باعتباره الوسيلة الوحيدة لإدانة مركب هذا النوع المستحدث من الجرائم.

و عليه سنبحث إثبات الجرائم الماسة بالمستهلك في المعاملات الإلكترونية من خلال تحديد إجراءات ضبط الجرائم الماسة بالمستهلك الإلكتروني (المبحث الأول)، و التطرق إلى حجية الدليل الإلكتروني في إثبات الجرائم الماسة بالمستهلك الإلكتروني (المبحث الثاني).

المبحث الأول: إجراءات ضبط الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

تتميز الجرائم التي تركب على المستهلك في المعاملات الإلكترونية بالسرعة و الذكاء عند ارتكابها، و ذلك نظرا لخصوصية البيئة الإلكترونية التي تعتمد على وسائل و تقنيات إلكترونية، مما يستدعي الكشف عنها اتخاذ إجراءات تتلاءم مع هذه البيئة، و هو ما لا تحققه الإجراءات التقليدية نظرا لسهولة تدمير أدلة ارتكاب هذه الجرائم و سهولة تبخرها.

لهذا حرص المشرع الجزائري من خلال قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و قانون التجارة الإلكترونية من وضع أسس و أساليب جديدة لكشف الجرائم الإلكترونية بصفة عامة و الماسة بالمستهلك الإلكترونية بصفة خاصة، تكون متوافقة مع ما تطلبه مثل هذه الأفعال على الشبكة الرقمية.

و سنحاول التطرق إلى هذه الإجراءات الخاصة بكشف الجرائم الماسة بالمستهلك الإلكتروني سواء المتخذة من قبل الضبطية القضائية (المطلب الأول)، أو تلك المتخذة من قبل جهات خاصة (المطلب الثاني).

المطلب الأول: الإجراءات المتخذة من طرف الضبطية القضائية لكشف الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

إنه من أكثر الأمور صعوبة في ظل الجرائم الإلكترونية هو التوفيق بين مقتضيات كشف الحقيقة عند وقوع الجريمة و بين حرية المتهم التي تصونها النظم القانونية مع الأخذ في الاعتبار ضرورة التحرك السريع لجمع الأدلة دون إبطال أو تأخر.

لذلك خول المشرع الجزائري لضباط الشرطة القضائية اتخاذ مجموعة من الإجراءات لكشف الجرائم الماسة بالمستهلك الإلكتروني تتلاءم و طبيعة الوسط الذي سيتم الحصول فيه على الدليل الإلكتروني ألا و هيا البيئة الإلكترونية، و تتمثل هذه الإجراءات في التفتيش و الضبط (الفرع الأول)، و تسخير أشخاص ذوي كفاءة لتعامل مع هذا النوع من الأدلة إذا تعلق الأمر بمسائل تقنية أو فنية و هو ما يعرف بالخبرة (الفرع الثاني).

الفرع الأول: التفتيش و الضبط لكشف الجرائم الماسة بالمستهلك الإلكتروني

يعد التفتيش إجراء يباشره موظف مختص بهدف البحث عن أدلة لجريمة تحقق وقوعها في محل و ذلك وفق لضمانات و قيود قانونية مقررة، و أن الضبط هو النتيجة الطبيعية التي ينتهي إليها التفتيش.

غير أن التفيش و الضبط الحاصل في البيئة الإلكترونية يقع على محل غير مادي أي هو عبارة عن معطيات رقمية ليس لها أي مظهر مادي محسوس، مما يجعلنا نتساءل عن مدى صلاحية تفتيش الكيان المعنوي للحاسوب أي أنظمة المعالجة الإلكترونية (الفقرة الأولى)، و كيف يتم ضبطها (الفقرة الثانية).

الفقرة الأولى: التفتيش في الجرائم الماسة بالمستهلك الإلكتروني

يعرف التفتيش بوجه عام أنه عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، و ذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة[1].

و يتميز التفتيش عن باقي إجراءات التحقيق الأخرى كالخبرة و المعاينة في إباحة انتهاك الحق في الخصوصية طالما أن هناك مبررا في القانون لهذا الانتهاك، لذلك فهو يعد من بين أهم الصلاحيات التي تمارسها سلطة التحقيق ضد الأشخاص و مساكنهم و يعد أحد مظاهر تقييد الحريات الإنسانية التي سعت التشريعات الدولية و الوطنية للحفاظ عليها، و قررت إبطاله في حالة عدم مراعاة الضمانات و القيود المقررة لإجرائه[2].

أما التفتيش في الجرائم الإلكترونية يختلف عنه في الجرائم التقليدية من حيث المحل ، إذ أن محل التفتيش في الجرائم الإلكتروني يكون الحاسوب أو أنظمة معلوماتية و هيا مجرد برامج و بيانات إلكترونية ليس لها أي مظهر مادي[3]. و من هنا يطرح الإشكال في ما مدى صلاحية مكونات و شبكات الحاسوب كمحل يرد عليه التفتيش (أولا) و ماهية الضوابط التي يجبوا اتباعها في ذلك(ثانيا).

أولا: مدى قابلية مكونات و شبكات الحاسوب للتفتيش

يتكون الحاسوب من مكونات مادية و مكونات منطقية ، كما أن له شبكات اتصالات على المستوى المحلي أو الدولي، إذ أنه لا تثار أدنى صعوبة إذا كان محل الجرائم الإلكترونية مكونات مادية، حيث ينطبق بصددها القواعد التقليدية دون صعوبة

[1] – احمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، الطبعة السابعة، 1993 ص 544.

[2] – جميل عبد الباقي الصغير، الإنترنت و القانون الجنائي، دار النهضة العربية، مصر، 2002، ص 113.

[3] – على عدنان الفيل، إجراءات التحري و التحقيق الابتدائي في الجريمة المعلوماتية ، المكتب الجامعي الحديث، الإسكندرية، 2012، ص 39.

بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه و هل هو من الأماكن العامة أم من الأماكن الخاصة، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش منزله و بنفس الضمانات المقررة قانونا في التشريعات المختلفة[1].

أما إذا كان المحل مكونات غير مادية كبرامج الحاسب أو بياناته أو شبكة الاتصال فقد ثار خلاف كبير في الفقه بين مؤيد و معارض، و لذلك سنحاول تبيان مدى إمكانية تفتيش مكونات الحاسب المعنوية و شبكات الاتصال المتصلة به.

1- مدى إمكانية تفتيش المكونات المعنوية للحاسوب:

يتعلق تفتيش أجهزة الحاسوب المعنوية ببيانات تما التلاعب فيها أو تغييرها، و هذه البيانات ليس لها الطبيعة المادية، مما أثار الخلاف بشأن تفتيش المكونات المعنوية للحاسوب.

فالرأي الأول: يخلص أصحابه إلى جواز تفتيش مكونات الحاسوب المعنوية و يستند في ذلك إلى عمومية نص التفتيش ، وذلك من خلال توسيع تفسير عبارة" **أي شيء** "، و يفسر الفقه عبارة' أي شيء' بأنها تشمل ضبط البيانات المخزنة أو المعالجة إلكترونيا[2].

إذ نصت المادة 487 من القانون الكندي صراحة على إمكانية ضبط أي شيء سواء كان ماديا أو بيانات إلكترونية، إذ تمنح سلطة إصدار إذن الضبط "لأي شيء"

[1] – خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الإنترنت، دار الثقافة للنشر و التوزيع، الطبعة الأولى، 2011 ، ص 159.

[2] – عبد الفتاح بيومي حجاز، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، مصر، 2009، ص 652 .

طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة التي وقعت أو يشتبه في وقوعها أو أن هناك نية في ارتكاب الجريمة بواسطته أو سوف ينتج دليلا على وقوع الجريمة[1] .

و يعاب على هذا الاتجاه، أن النصوص القانونية التي أرست القواعد التي تحكم التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية، فطبيعة البيانات و المعطيات الإلكترونية تتطلب قواعد خاصة تحكمها بدلا من محاولة تطويع القواعد التقليدية و توسيع نطاقها ، فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا يمكن إعمالها مباشرة على أنظمة الحاسوب لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية.

أما الرأي الثاني: فيرى أصحابه عدم إمكانية انسجام و تطبيق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث و تنقيب على الأدلة في برامج الحاسوب و بياناته[2].

كما تدعوا إلى ضرورة مواجهة التطور التكنولوجي للحواسيب و وسائل الاتصال الحديثة بسن نصوص قانونية خاصة غايتها تفتيش و ضبط البيانات المعالجة عن طريق الحواسيب و الأنظمة المعلوماتية ،لأن الغاية من التفتيش في الجرائم التقليدية هو ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة و أن هذا المفهوم المادي لا ينطبق على بيانات الحاسوب الغير المادية، و منه وجب أن تكون الغاية من التفتيش هي البحث عن الأدلة الغير المادية أو بيانات معالجة بواسطة الحاسوب.

فيرى الفقه الفرنسي أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المادية و بالتالي لا تعد شيئا ماديا بالمعنى المألوف للمصطلح و لذا لا يمكن ضبطه[3].

---

[1] – عائشة بن قادة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي (في القانون الجزائري و القانون المقارن)، دار الجامعة الجديدة، الإسكندرية، 2010، ص 91.

[2] – على حسن محمد الطوالبة، التفتيش الجنائي علم نظام الحاسوب و الأنترنت دراسة مقارنة، عالم الكتب الحديث، الأردن، 2004، ص 31.

[3] – عائشة بن قادة مصطفى، المرجع السابق، ص91.

إذ نجد على الصعيد الدولي اتفاقية بودابست قد ناشدت بحق الدول الأعضاء في تفتيش أجهزة الحاسوب المعنوية في إطار الإجراءات الجنائية و ذلك من خلال الفقرة الأولى من المادة 19 ، حيث دعت كل دولة طرف أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى نظام الكمبيوتر أو جزء منه أو المعطيات المخزنة فيه، أو الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزنة في إقليمها. صراحة[1].

و قد استجاب المشرع الفرنسي لهذا الرأي و قام بتعديل نصوص التفتيش بالقانون رقم 545 – 2004 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الاقتصاد الرقمي، حيث أضاف في المادة 94 من قانون الإجراءات الجزائية عبارة **"المعطيات المعلوماتية"** لتصبح المادة كالتالي: يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة[2].

أما موقف المشرع الجزائري من تفتيش المكونات المعنوية لأنظمة الحاسوب فقد خرج عن القواعد العامة للتفتيش المنصوص عليها في قانون الإجراءات الجزائية متدارك هذا القصور من خلال القانون رقم 09 –04 المؤرخ في 5 غشت 2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، حيث أجاز صراحة تفتيش المنظومة المعلوماتية، وذلك بموجب المادة 05 منه، إذ اجاز لسلطة القضائية المختصة و كذا ضباط الشرطة القضائية الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها[3] .

[1] – أنظر المادة 1/19 من اتفاقية بودابست لسنة 2001.

[2] – أنظر المادة 94 من قانون الإجراءات الجزائية الفرنسي.

[3] – أنظر المادة 5 من قانون 09–04 المتعلق بالوقاية من جرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

2- تفتيش الشبكات المتصلة بالحاسوب:

تعرف الشبكة المعلوماتية بأنها مجموعة مكونة من اثنين فأكثر من أجهزة الحاسوب و المتصلة ببعضها اتصالا سلكيا أو لاسلكيا، و قد تكون الأجهزة متواجدة في نفس الموقع و تسمى بالشبكة المحلية ، و قد تكون متوزعة في أماكن مختلفة[1]، و مع التطور التكنلوجي لوسائل الاتصالات لم يعد نطاق الاتصال محدودا في إقليم دولة واحدة ، بسبب ظهور شبكة الأنترنت و التي هي عبارة عن منظومة واسعة من الشبكات المعلوماتية الحاسوبية المتصلة مع بعض بطريقة لا مركزية.

إن إجراء تفتيش شبكات الحاسوب قد يجد صعوبات في الحصول على البيانات التي تحتوي على أدلة لارتباط هذه البيانات بشبكات حاسوبية بعيدة عن الموقع المادي للتفتيش ، فقد يكون الموقع الفعلي للشبكات داخل اختصاص قضائي آخر و حتى في بلد آخر ، و هو ما يزيد المسألة تعقيدا باعتبار أن الشبكة المعلوماتية ممتدة في أرجاء العالم ، بالتالي فإن الحاسوب أو النهاية الطرفية التي يمكن أن ترتكب عليها أو بواسطتها الجريمة الإلكترونية تخضع للقانون الخاص بتلك الدولة.

لذلك يثار التساؤل حول أثر تفتيش الشبكات المتصلة بالحاسوب المأذون تفتيشه إذا تواجدت في دوائر اختصاص مختلفة. و نستطيع أن نميز في هذه الصورة بين احتمالين على النحو التالي:

الاحتمال الأول: أن يكون حاسوب المتهم متصلا بحاسوب أو نهاية طرفية موجودة في مكان آخر داخل الدولة، وهنا يثور التساؤل حول مدى إمكانية امتداد الحق في التفتيش إلى أجهزة الحاسوب المتصلة بجهاز المشتبه فيه أو المتهم.

ففي هذا الصدد نجد أن اتفاقية بودابست لعام2001 في المادة 19 تسمح للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من

[1] – على حسن محمد الطوالبية، المرجع السابق، ص 34.

الأجهزة المرتبطة به في حال الاستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش[1].

أما المشرع الجزائري فقد نص في قانون 09-04 سابق الذكر على إمكانية تمديد التفتيش إلى منظومة معلومات أخرى أو جزء منها انطلاقا من المنظومة الأولى ، و يتم هذا الامتداد وفق لضابطين، أولهما وجود أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلومات أخرى، أما الثاني فيتعلق بإعلام السلطة القضائية المختصة مسبقا[2].

كما أجاز المشرع الفرنسي من خلال المادة 17 من قانون رقم 2003/239 المتعلق بالأمن الداخلي الصادر في 2003/03/18 لرجال الضبط القضائي أن يدخلوا بغرض التفتيش من الجهاز الرئيسي على المعطيات التي تهم عملية التحقيق و المخزنة في أي نظام معلوماتي آخر، بما أن هذه البيانات يتم الدخول إليها أو تكون متاحة انطلاقا من النظام الرئيسي[3].

الاحتمال الثاني: أن يكون حاسوب المتهم متصلا بحاسوب أو نهاية طرفية موجودة في مكان آخر خارج الدولة، من الصعوبات التي تواجه السلطات القضائية في جمع الأدلة و التحقيقات حالة امتداد التفتيش إلى خارج إقليم الدولة التي صدر من جهتها إذن التفتيش، إذ يقوم مرتكبي الجرائم الإلكترونية بصفة عامة بتخزين بياناتهم في أنظمة معلومات خارج الدولة بواسطة شبكا الاتصالات بهدف عرقلة السلطات القضائية في جمع الأدلة و تمسك كل دولة بسيادتها و حدودها الإقليمية[4].

لذا فإن جانب من الفقه يرى أن التفتيش الإلكتروني العابر للحدود لابد و أن يتم في إطار اتفاقيات تعاون ثنائية أو دولية تجيز هذا الامتداد أو الحصول على إذن مسبق

[1] – انظر المادة 19 من اتفاقية بودابست لسنة 2001. .

[2] – أنظر المادة 2/5 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] – انظر المادة 17 من قانون الإجراءات الجزائية الفرنسي.

[4] – عائشة بن قادة مصطفى، المرجع السابق، ص 93.

من الدولة الأخرى[1]، و بالتالي فإنه لا يجوز القيام بذلك التفتيش في ظل غياب تلك الاتفاقية أو عدم الحصول على إذن الدولة الأخرى، و إن الاختراق المباشر يعد انتهاكا لسيادة دولة أخرى و خرقا للقوانين ما لم توجد اتفاقية دولية في هذا الشأن، و هذا يؤكد على أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية.

و هو ما اتخذه المشرع الفرنسي في المادة 1/57-2 من قانون الإجراءات الجزائية المضافة بموجب المادة 2/17 من قانون 2003/239 و التي أجازت للجهات المختصة بالتحقيق أنه في حالة تبين لها أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني و أنه يمكن الدخول إليها انطلاقا من المنظومة الرئيسية فإنه يمكن الحصول عليها مع مراعات الشروط المنصوص عليها في المعاهدات الدولية[2].

أما موقف المشرع الجزائري في هذا الشأن، فقد أجاز تفتيش الأنظمة المتصلة حتى و لو كانت متواجدة خارج الإقليم الوطني، من خلال قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها ، الذي مكن من خلال المادة 5 منه جهات التحقيق تفتيش منظومة معلوماتية تقع خارج الإقليم الوطني إذا تبين مسبقا بأن المعطيات المبحوث عنها متواجدة فيها انطلاقا من المنظومة الأولى ، و يكون الحصول على المعطيات المبحوث عنها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية و وفقا لمبدأ المعاملة بالمثل[3].

و عليه فإن تفتيش الأنظمة المتواجدة على إقليم بلد أجنبي يستلزم بالضرورة وجود اتفاق دولي يضمن التعاون الدولي بين السلطات المختصة، و القول بغير ذلك يجعل من هذا الإجراء مساسا لسيادة الدول. و بالرغم من ذلك أجازت المادة 32 من اتفاقية بودابست لسنة 2001 إمكانية الدخول بغرض تفتيش شبكات تابعة لدولة أخرى بدون

[1] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 205.

[2] – أنظر المادة 2/17 من قانون الإجراءات الجزائية الفرنسي.

[3] – أنظر المادة 3/5 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

إذنها في حالتين: الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، و الثانية إذا رضى صاحب أو حائز هذه البيانات بهذا التفتيش[1].

ثانيا: ضوابط التفتيش في البيئة الإلكترونية

تضمنت معظم التشريعات الإجرائية على ضوابط معينة يجب التقيد بها خلال الإجراءات الماسة بالحريات الشخصية كالتفتيش، و هدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم و بين حقوق الأفراد و حرياتهم[2]. و يمكن تقسيم الضوابط العامة لتفتيش نظم الحاسوب إلى ضوابط موضوعية و أخرى شكلية.

1- الضوابط الموضوعية لتفتيش أنظمة الحاسوب:

يقصد بها بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح، و هي في العادة تأتي سابقة له، و يمكن حصرها في ثلاث شروط أساسية و هي السبب و المحل و السلطة المختصة بالقيام به[3].

أ-سبب التفتيش في البيئة الإلكترونية:

التفتيش هو إجراء من إجراءات التحقيق لا يصلح إصداره إلا للكشف عن جريمة واقعة بالفعل و ترجحت نسبتها إلى متهم معين، و أن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية[4]. و عليه فإن حتى يكون التفتيش صحيحا في عند التحقيق في الجرائم الماسة بالمستهلك الإلكتروني فإنه يجب :

– وقوع جريمة ماسة بالمستهلك الإلكتروني: حتى يكون إجراء التفتيش جائزا لابد من وقوع جريمة بصورة قطعية سواء أكانت جناية أو جنحة[5] و تستبعد المخالفات لضآلة

---

[1] – أنظر المادة 32 من اتفاقية بودابست لسنة 2001.

[2] – د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الأول، المرجع السابق، ص 594.

[3] – رشيدة بوكر، المرجع السابق، ص 405 .

[4] – د/ خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص209.

[5] – انظر المادة 44 من قانون الإجراءات المعدل و المتمم.

خطورتها[1]، و من ثم لا يجوز إجراءه لضبط جريمة مستقبلا أو لمجرد ورود معلومات تشير إلى إمكانية وقوع الجريمة مستقبلا حتى و لو كانت الدلائل كافية على أنها ستقع بالفعل[2].

و عليه فإن المشرع الجزائري فتح المجال في اتخاذ إجراء التفتيش من طرف السلطات المختصة في أي جريمة ترتكب على المستهلك في إطار المعاملات الإلكترونية تكون محل للتفتيش مادامت ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

– اتهام شخص أو أشخاص بارتكاب جريمة ماسة بالمستهلك الإلكتروني أو المشاركة فيها: إن وقوع جريمة من الجرائم الماسة بالمستهلك الإلكتروني غير كاف للقول بصحة إجراءات التفتيش بل ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل[3] كافية تدعوا للاعتقاد بأنه ساهم في ارتكاب جريمة ماسة بالمستهلك الإلكتروني بصفته فاعلا أصليا أو شريكا فيها مما يستوجب اتهامه بها، بحيث أنه إذا لم تتوفر هذه الدلائل كان على الجهة القضائية المختصة أن تصدر أمرا بأن لا وجه لإقامة الدعوى[4].

–وجود أمارات قوية على وجود معطيات أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره: لا يكفي وقوع جريمة و اتهام شخص أو عدة أشخاص لارتكابها، بل يجب أن توافر أمارات و قرائن قوية و كافية تفيد على وجود أدوات استعملت في الجريمة الماسة بالمستهلك الإلكتروني أو أشياء متحصلة منها أو أي مستندات إلكترونية يحتمل أن يكون لها فائدة لإظهار الحقيقة و تكون هاذه الدلائل و

---

[1] – رشيدة بوكر ، المرجع السابق، ص 406.

[2] – نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، الطبعة الاولى، دار الفكر الجامعي، الإسكندرية، 2007، ص 231

[3] – يمكن تعريف الدلائل على أنها مجموعة من المظاهر أو الأمارات المعنية التي تنهض على السياق العقلي و المنطقي و التي تؤيد نسبة الجريمة الإلكترونية إلى شخص معين بوصفه فاعلا أو شريك. **أنظر عبد الفتاح بيومي حجاز، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 662.**

[4] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 210..

الأمارات متواجدة في الأماكن أو لدى الأشخاص المراد تفتيشهم[1]. و تقدير هذه الدلائل و الأمارات المتحصلة من التحريات الجدية التي تسبق التفتيش من المسائل الموضوعية التي يوكل الأمر فيها إلى السلطة المختصة بإصدار إذن التفتيش، فتنسب لشخص معين بقدر يبرر تعرض إجراء التفتيش لحريته الشخصية ولحرمة مسكنه في سبيل إظهار الحقيقة[2].

ب– محل التفتيش في البيئة الإلكترونية:

يقصد بمحل التفتيش المستودع الذي يحفظ فيه الشخص بالأشياء التي تتضمن سره، و محل التفتيش في الجرائم الماسة بالمستهلك الإلكتروني هو جهاز الحاسوب بكل مكوناته المادية و المعنوية و شبكات الاتصال كما سبق بيانه.

د–السلطة المختصة بالتفتيش:

يعتبر التفتيش إجراء من إجراءات التحقيق التي تمس بحقوق و حريات الأفراد، و لهذا تخول التشريعات الإجرائية أمر القيام به لسلطة التحقيق، إلا أنه و بالنظر إلى ضرورات عملية مردها كثرة القضايا و الحرص على سرعة إنجاز أعمال التحقيق فيها، و تسهيله و الاستفادة من قدرات رجال الضبطية القضائية أجيز لسلطة التحقيق تكليف هؤلاء بتنفيذ التفتيش[3].

و يكون هذا التكليف بإذن مكتوب من السلطة القضائية المختصة، حيث ينص المشرع الوطني في المادة 44 من قانون الإجراءات الجزائية أنه" لا يجوز القيام بإجراء التفتيش إلا بإذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق و يشترط في هذا الإذن وجوب استظهاره قبل الدخول إلى المنزل و الشروع في تفتيشه"، و الهدف من هذا

[1] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 213.

[2] – إلهام بن خليفة، الرسالة السابقة، ص 248.

[3] – رشيدة بوكر، المرجع السابق، ص 410.

التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي، بحيث لا يترك لضابط الشرطة القضائية القائم بالتفتيش أي سلطة تقديرية في ذلك[1].

و بالرجوع إلى القواعد الخاصة بإجراء التفتيش في البيئة الإلكترونية المنصوص عليها في قانون 09-04، نجدها لا تنص على استصدار الإذن عن قيام ضباط الشرطة القضائية بإجراء التفتيش في الجرائم الإلكترونية و إنما اكتفى بإعلام السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة أخري[2]، و هذا السكوت لا يعني عدم استصدار إذن من السلطة القضائية المختصة عند القيام بهذا الإجراء، فهذا القانون مكمل لقانون الإجراءات الجزائية حيث تنص المادة 03 من هذا القانون على أنه،" ...أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية و في هذا القانون ... القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية".

و بالرجوع إلى قانون الإجراءات الجزائية نجده يلزم ضباط الشرطة القضائية باستصدار إذن مكتوب من الجهات القضائية المختصة عند التفتيش[3]، **فهل يكفي تفتيش أنظمة الحاسوب فقط بالإذن المتعلق بالمسكن الذي يتواجد فيه الحاسوب؟.**

وطبقا لمعيار الخصوصية التي يحميها المشرع فإن نظام الحاسوب و ما يحتويه من أسرار و خصوصيات الأشخاص، فإنه يخضع لمبدأ عدم جواز الدخول إلى هذا النظام و تفتيشه دون إذن من السلطة القضائية المختصة، و عليه يجب على ضابط الشرطة القضائية عند تفتيش أنظمة الحاسوب استصدار إذن بالتفتيش أولا، و ينص الإذن صراحة على تفتيش أنظمة الحاسوب ثانيا ، بالإضافة إلى تحديد المسكن ثالثا.

[1] – عائشة بن قادة مصطفى، المرجع السابق، ص 106.

[2] – انظر المادة 2/05 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] – انظر المادة 44 قانون الإجراءات الجزائية المعدل و المتمم.

2- الضوابط الشكلية لتفتيش في البيئة الإلكترونية.

بالإضافة إلى الضوابط الموضوعية لصحة إجراء تفتيش نظم الحاسوب و شبكات الاتصال الخاصة به في الجرائم الماسة بالمستهلك الإلكتروني، هناك ضوابط أخرى ذات طابع شكلي يجب التقيد بها عند القيام بهذا الإجراء حماية لحريات الأفراد[1]، و تتمثل هذه الضوابط في:

أ-تسبيب أمر التفتيش في البيئة الإلكترونية:

ينص المشرع الجزائري في المادة 44 من قانون الإجراءات الجزائية أنه لا يجوز القيام بإجراء التفتيش إلا بإذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق و يشترط في هذا الإذن أولا وجوب استظهاره قبل الدخول إلى المنزل و الشروع في تفتيشه و ثانيا أن يتضمن الإذن بيان وصف الجرم موضوع البحث عن الدليل و عنوان الأماكن التي سيتم زيارتها و تفتيشها ...، بمعنى أن يكون مسببا و علة التسبيب هي بيان هدف التفتيش و التحقق من مشروعيته بثبوت أنها الغاية التي حددها القانون، ذلك أن الإذن حسب المادة 44 إذ لم يتضمن التسبيب يقع تحت طائلة البطلان، إذ أن اشتراط المشرع للتسبيب يتيح للقضاء تقدير صحة الأمر بالتفتيش و تقرير بطلانه إذا ثبت أنه يستهدف غاية أخرى غير ما حدده القانون[2] ، و لا يشترط المشرع في التسبيب أن يكون تفصيليا، بل يكفي بيان الجرم بالاستناد إلى الدلائل التي استخلصتها الضبطية من تحرياتها.

ب-الحضور لبعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونية:

يعتبر هذا الشرط من أهم الشروط الشكلية التي تطلبها المشرع الجزائري، إذ أوجب عند إجراء التفتيش المتعلق بالمساكن و ملحقاتها بضرورة حضور المشتبه فيه من طرف الضبطية القضائية، و في حالة تعذره على الحضور يتعين على ضابط الشرطة القضائية

[1] – د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 389.

[2] – د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الأول، المرجع السابق، ص 605.

أن يكلفه بتعيين ممثل له، أما في حالة امتناعه عن حضور التفتيش أو كان هاربا يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش[1].

غير أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم 22/06 استثنى بموجبه شرط حضور المشتبه فيه أو الشاهدين في جرائم معينة منها جرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2]، و الهدف من ذلك هو ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني ، خاصة و أن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله و التلاعب فيه حتى عن بعد، بالإضافة إلى الإسراع في استخلاصه قبل فقدانه.

ج-الميعاد الزمني لإجراء التفتيش في البيئة الإلكترونية:

إن عدم احترام هذه الضمانة يؤدي إلى قيام المسؤولية الجزائية للقائم بالتفتيش خارج الفترة الزمنية المحددة قانونا، و ذلك حرصا على تضييق الاعتداء على الحرية الفردية و حرمة المسكن. إذ أن المشرع الجزائري يحظر تفتيش المساكن و ما في حكمها في أوقات معينة[3]، و الفترة الزمنية المسموح بها لإجراء التفتيش حددها المشرع من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا[4]، إلا أنه عندما يتعلق الأمر بالجرائم الإلكترونية فقد أجاز فيها المشرع لضباط الشرطة القضائية إجراء التفتيش في كل ساعة من ساعات النهار أو الليل [5]، و الهدف من ذلك ميزة هذه الجريمة من حيث قابلية الدليل الإلكتروني فيها للمحو و التدمير و ضرورة المحافظة عليه لسير مجريات التحقيق.

---

[1] – انظر المادة 45 من قانون الإجراءات الجزائية المعدل و المتمم.

[2] – تنص القرة الأخيرة من المادة 45 قانون إجراءات جزائية المعدل و المتمم على أنه لا تطبق هذه الأحكام إذا تعلق الامر بالجرائم المعلوماتية باستثناء الحفاظ على السر المهني و جرد الأشياء و حجز المستندات.

[3] – إلهام بن خليفة، الرسالة السابقة، ص 277.

[4] – انظر المادة 1/47 من قانون الإجراءات الجزائية المعدل و المتمم.

[5] – انظر المادة 2/47 من قانون الإجراءات الجزائية المعدل و المتمم.

الفقرة الثانية: الضبط في الجرائم الماسة بالمستهلك الإلكتروني

إن الهدف الذي تسعى إليه السلطة المختصة بالتفتيش هو ضبط الأدلة و الأشياء المتعلقة بالجريمة و تفيد في الكشف عنها، و منه يمكن تعريف الضبط على أنه وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة و عن مرتكبها [1]. و عليه فإن ضبط الأدلة التي يتم الحصول عليها أثناء التفتيش هي النتيجة الطبيعية التي ينتهي إليها هذا الإجراء.

أما الضبط في البيئة الإلكترونية فيعرف على أنه وضع اليد على الدعائم المادية المخزنة فيها البيانات أو المعلومات التي تتصل بالجريمة الإلكترونية التي وقعت و تفيد في كشف الحقيقة عنها و عن مرتكبها، كما يعرف أيضا بأنه استخدام البرامج الهامة من أجل الولوج للبيانات المراد ضبطها إلى جانب وضع اليد على تلك الدعائم المادية[2].

فمن خلال ما سبق فأن الضبط في الجرائم الماسة بالمستهلك الإلكتروني يختلف عن الضبط في غيره من الجرائم التقليدية من حيث المحل، فالجريمة التقليدية ينصب الضبط فيها على أشياء مادية ملموسة على خلاف الجريمة الإلكترونية التي يكون محل الضبط فيها أشياء مادية و أخرى ذات طبيعة معنوية كالبيانات و المراسلات و الاتصالات الإلكترونية.

و بناء على هذا الاختلاف حول محل الضبط سنحاول البحث في مسألة الضبط في البيئة الإلكترونية من خال تبيان مدى إمكانية ضبط الأدلة الإلكترونية (أولا)، و ماهيا إجراءاته (ثانيا).

[1] – خالد عياد الحلبي، المرجع السابق، ص 168 .

[2] – نبيلة هبا هروال، إجراءات البحث و التحري، المرجع السابق، ص 266.

أولا: مدى صلاحية ضبط الأدلة في البيئة الإلكترونية

يقصد بالضبط في قانون الإجراءات وضع اليد على شيء يتصل بجريمة وقعت و يفيد في كشف الحقيقة عنها و عن مرتكبها[1]، و يشترط أن تكون الأشياء المضبوطة ذو طبيعة مادية، و على هذا الأساس فإن ضبط المكونات المادية للحاسوب لا يثير مشاكل لدي فقهاء القانون في إمكانية ضبط هذه المكونات، أما بالنسبة لضبط مكونات الحاسوب المعنوية المتمثلة في البيانات المعالجة إلكترونيا يثير العديد من الجدل لدى الفقهاء[2].

لقد اختلفت التشريعات الإجرائية و الاتجاهات الفقهية حول مسألة ضبط المكونات المعنوية للحاسوب و التي لا تصلح بطبيعتها محلا لوضع اليد و هي مجردة من دعائمها المادية المثبتة عليها، و انقسمت في ذلك إلى ثلاث اتجاهات:

-**الاتجاه الأول:** يرى أصحابه أنه لا يمكن تصور إجراء الضبط على المكونات المعنوية للحاسوب لانتفاء الكيان المادي عنها، و بالتالي عدم صلاحية البيانات المخزنة آليا لأن تكون محلا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية لانتفاء الطابع المادي عن هذه البيانات في حال تجردها عن الدعامة المادية [3]، و لكن يمكن ضبط المعلومات و البيانات إذا كانت مخزنة على دعامة أو وسيط إلكتروني، أو كانت من مخرجات الحاسوب، كما لو كانت مطبوعة على الورق، أو حالة تصوير أو تجميد شاشة الحاسوب.

-**الاتجاه الثاني:** يرى أنصار هذا الاتجاه أن المعطيات المخزنة آليا كونها مجردة عن الدعائم المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة لأن تكون محلا للضبط المنصوص عليها بمقتضى النصوص التقليدية مستندين إلى الغاية من

---

[1] – خالد عياد الحلبي، المرجع السابق، ص 168.

[2] – محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الأنترنت، المرجع السابق، ص 291 .

[3] – عفيف كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون دراسة مقارنة، منشأة المعارف الإسكندرية، 2010، ص 353.

التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة و بالتالي يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها[1].

-**الاتجاه الثالث:** و يأخذ أنصار هذا الاتجاه الموقف الوسط، و ذلك بدعوتهم إلى ضرورة تدخل تشريعي لتوسيع دائرة الأشياء التي يرد عليها الضبط لتشمل إلى جانب الأشياء المادية الأشكال المختلفة للبيانات الإلكترونية.

و لقد تدخل المشرع الفرنسي لينص على ضبط المكونات المعنوية للحاسوب من خلال قانون الأمن الداخلي رقم 239/ 2003 ، أين نصت الفقرة الرابعة من المادة 57 على أن: " المعطيات التي يتم الدخول إليها بالشروط المنصوص عليها في هذا القانون يمكن نسخها على دعامة، و دعامات التخزين المعلوماتية يمكن ضبطها و وضعها في أحراز بالشروط المنصوص عليها في هذا القانون".

كما تدخل المشرع الجزائري لتدارك القصور التشريعي من خلال قانون رقم 09 – 04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ،إذ نص صراحة في المادة السادسة منه على حجز البيانات المتواجدة في منظومة معلوماتية أو جزء منها و التي تم الكشف عنها جراء التفتيش، شريطة أن تكون مفيدة في الكشف عن الجريمة أو مرتكبيها[2].

و هو ما أكدته اتفاقية بودابست لسنة 2001، إذ الزمت الدول على اتخاذ إجراء ضبط نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين على الخاصة بالحاسوب و أن تحافظ على تلك المعلومات المخزنة[3].

[1] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 235.

[2] – انظر المادة 06 من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] – انظر المادة 19 من اتفاقية بودابست لسنة 2001.

ثانيا: إجراءات ضبط البيانات في البيئة الإلكترونية

تختلف طريقة ضبط البيانات المعالجة في النظم المعلوماتية عما هو متبع عند ضبط الأشياء المادية المحسوسة لأجهزة الحاسوب الآلي و ملحقاته، فضبط البيانات الإلكترونية يتم عن طريق نسخها على دعامات إلكترونية، و تقوم هذه التقنية على أخذ نسخة من محتويات النظام المعلوماتي على دعامات إلكترونية مع المحافظة على سلامة البيانات المنسوخة في الحالة التي تم العثور عليها لحظة الضبط[1].

و لقد نص المشرع الجزائري على ضرورة نسخ البيانات التي تم الكشف عنها عند تفتيش منظومة إلكترونية من خلال نص المادة 06 من قانون 04/09 سابق الذكر، حيث نصت هذه المادة الأخيرة على أن الجهات المختصة بالتفتيش عند ضبطها لمعطيات تم الكشف عنها في منظومة معلوماتية أو جزءا منها بضرورة نسخها على دعامات تخزين إلكترونية و السهر على سلامة تلك المعطيات المضبوطة[2].

أما في حالة عدم إمكانية الوصول لهذه البيانات عن طريق النسخ في دعائم إلكترونية قابلة للحجز، فيتم التعامل معها بطرق تقنية أو أي وسيلة إلكترونية تمنع الدخول إلى هذه البيانات التي تحتويها منظومة معلوماتية أو جزءا منها، و يتمثل هاذا **الإجراء في الحجز عن طريق منع الوصول إلى المعطيات،** حيث نصت المادة 07 من 09-04 سابق الذكر أنه "إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه، لأسباب تقنية على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

و مفاد هذا الإجراء هو منع الغير من المتهم أو غيره من الوصول إلى المعطيات التي تم الدخول إليها و لكن تعذر حجزها أو ضبطها لأسباب تقنية، و ذلك باستعمال

[1] – عائشة بن قادة مصطفى، المرجع السابق، ص116.

[2] – انظر المادة 06 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

وسائل تقنية كترميزها أو تشفيرها عن طريق أي برنامج من البرامج التشفير و الهدف من ذلك هو عدم امتداد يد العابثين إليها لتغيير مجرى التحقيق[1].

كما أجاز المشرع الجزائري للسلطات التي تباشر التفتيش رفع المعطيات من النظام، إذ يتم اللجوء إلى هذا الإجراء إذا كانت البيانات تتضمن خطرا أو ضرر بالمجتمع أو التي يكون فيها محتوى البيانات غير مشرعة[2]، إذ لا يهدف هذا الإجراء لتدمير البيانات بل تستمر في الوجود إلا أنه يتم حرمان الشخص مؤقتا من الولوج إلى هذه البيانات المتواجدة في منظومة معلوماتية أو جزء منها أو نسخها، لكن يمكن إعادتها إليه بعد انتهاء التحقيق الجاري.

كما نص المشرع الفرنسي على هذا الإجراء من خلال قانون الثقة في الاقتصاد الرقمي المؤرخ في 21 جوان 2004 المعدل لقانون الإجراءات الجزائية ، حيث تنص المادة 97 على أنه يجب القيام بإجراء المحو الكامل للدعامة الخارجية أو المعطيات المعلوماتية إن لم توضع بيد القضاء إذا كان محتواها غير قانوني أو خطر على أمن الأشخاص أو الأموال.

و هاذا ما أكدت عليه المادة 19 فقرة 03 من اتفاقية بودابست لسنة 2001 و التي ألزمت الدول الأطراف اتخاذ مثل هاذا النوع من الإجراءات لضبط البيانات في الحالات التي تتضمن خطرا أو ضررا بالمجتمع و على سبيل المثال البرامج التي تحتوي على فيروسات أو الحالات التي يكون فيها محتوى البيانات غير قانوني[3].

و المعروف أن بعد ما يتم ضبط البيانات الإلكترونية يتعين تحريزها لحمايتها فنيا، و هو ما نص عليه المشرع في المادة 06 فقرة الثالثة من قانون 04/09 المتعلق بالوقاية

---

[1] – محمد عبد الرؤوف الخن، المرجع السابق، ص 292.

[2] – المادة 08 من قانون 09-04 " يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك ".

[3] – هلال عبد الله أحمد، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، المرجع السابق، ص 240.

من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها حينما أوجب على السلطات التي تقوم بعملية ضبط الدليل الإلكتروني أن تسهر على سلامة المعطيات في الأنظمة المعلوماتية التي تجري بها العملية، و أن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات[1]. و من هذه الإجراءات على سبيل المثال أخذ نسخ احتياطية عن المعطيات و العمل عليها لضمان عدم المساس بالدليل الأصلي، عدم تنفيذ برنامج على الحاسوب مسرح الجريمة خوفا من إتلاف الأدلة الموجودة عليه أو محو الذاكرة أو الملفات و عدم السماح للمشتبه فيه بالتعامل مع الحاسوب، ضبط الدعائم الأصلية للمعلومات و عدم الاقتصار على ضبط نسخها، عدم تبني القرص لان ذلك يؤدي إلى تلفه و فقدانه للمعلومات المسجلة عليه، عدم تعريض الأقراص الممغنطة و الأشرطة الممغنطة لدرجات حرارة عالية و لا إلى الرطوبة[2].

[1] – أنظر المادة 3/6 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[2] – خالد عياد الحلبي، المرجع السابق ص177.

الفرع الثاني: الخبرة في إثبات الجرائم الماسة بالمستهلك الإلكتروني

لاشك أن القاضي مطالب بالنظر و التحري عن حقيقة الدعاوى التي ينظر فيها و ما يتعلق بها، و لقد أفرز التطور الهائل في مجال تكنلوجيا المعلومات و الاتصال في عصر المعلومات العديد من الأنشطة المستحدثة التي تتم باستخدام الوسائل الإلكترونية، التي قوامها نظم و برمجيات الحاسب الآلي، و الشبكات الحاسوبية و شبكات الاتصالات العالمية (الأنترنت)، و يقود مثل هذا القول في الحقيقة إلى تعاظم دور الإثبات العلمي للدليل و إعلان انضمام الخبرة التقنية إلى عالم الخبرة، من حيث ضرورة الاستعانة بالمتخصص في مجال النزاع.

و تظهر أهمية الاستعانة بالخبير في مجال الجرائم الإلكترونية عامة و تلك الماسة بالمستهلك الإلكتروني خاصة عند غيابه، فقد تعجز الضبطية القضائية عن كشف غموض الجريمة، و قد تعجز هي أو جهة التحقيق عن جمع الأدلة حول الجريمة، و قد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه. مما يقودنا حتما لتبيان دور الخبرة التقنية في عملية الحصول على الدليل، و ذلك من خلال تحديد مفهوم الخبرة (الفقرة الأولى) و التطرق إلى القواعد القانونية و الفنية التي تحكمها (الفقرة الثانية).

الفقرة الأولى: مفهوم الخبرة في البيئة الإلكترونية

الخبرة القضائية عموما هيا الاستشارة الفنية التي يستعين بها رجال القضاء لمساعدتهم في تكوين عقيدتهم نحو المسائل التي يحتاج تقديرها أو درايتها عملية خاصة لا تتوافر لديهم[1].

كما عرفت أيضا بأنها " الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه، و الخبرة الفنية تعتبر من إجراءات التحقيق بحسب الأصل[1].

[1] – أمال عثمان، الخبرة في المسائل الجنائية ، رسالة دكتوراه، كلية الحقوق ، جامعة القاهرة ، مصر، 1964 ص 68.

و للخبرة أهمية بالغة تكمن في تقديم العون لجهات التحقيق أو القضاء و لكامل السلطات المختصة في الدعوى الجنائية في تحقيق العدالة، فبدونها يتعذر الوصول إلى الرأي السديد بشأن المسائل الفنية التي يكون على ضوئها كشف جوانب الحقيقة المبينة على الحقائق العلمية[2]. لذلك اهتم المشرع الجزائري بتنظيم أعمال الخبرة في قانون الإجراءات الجزائية من المواد 143 إلى 156 ، حيث منح لجهات التحقيق أو الحكم الاستعانة بالخبراء في المسائل ذات الطابع الفني إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو بطلب من الخصوم[3].

و إذا كانت ندب الخبراء الفنيين في الجرائم التقليدية ذا أهمية بالغة ، فإن أهميتها تصبح ضرورية بل حتمية في استخلاص الأدلة الإلكترونية لإثبات الجرائم الإلكترونية، حيث تتعلق بمسائل فنية أية في التعقيد و محل الجريمة فيها غير مادي، حيث يجد المحقق صعوبة في جمع الأدلة الإلكترونية لنقص معرفته لهذا النوع من الجرائم المتطورة في أساليب ارتكابها ، و لذاك بات من الضروري الاستعانة بالخبرة الفنية في مجال الجريمة الإلكترونية. و التي تعد أقوى مظاهر التعامل القانوني أو القضائي مع ظاهرة تكنلوجيا المعلومات و الأنترنت[4]

إذ سعت بعض التشريعات إلى تنظيم الخبرة في مثل هذا النوع من الجرائم في نصوص خاصة ، فنجد المشرع الجزائري لم يتخلف عن هذه التشريعات حينما أشار في المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال و مكافحتها أنه يمكن للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية

---

[1] – أنيس حسيب السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية و الرقمية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2016، ص17.

[2] – سيف ابغازي ، السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر ص 440.

[3] – انظر المادة 143 من قانون الإجراءات الجزائيةالمعدل و المتمم.

[4] – عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، دون سنة نشر، دون بلد نشر، 2005، ص 103.

محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

كما أكد المشرع في المادة 8 من نفس القانون على ضرورة الاستعانة بالأشخاص المؤهلين باستعمال الوسائل التقنية من طرف السلطات التي تباشر التفتيش لضبط الأدلة الإلكترونية عن طريق منع الاطلاع على المعطيات التي يشكل محتواها جريمة.

الفقرة الثانية: القواعد القانونية التي تحكم الخبرة القضائية في البيئة الإلكترونية.

نظرا للأهمية البالغة للخبرة و الدور الذي تلعبه في عملية الإثبات في المجال الجنائي، فقد حرصت معظم التشريعات على تنظيم الخبرة و وضع شروط و ضوابط لها ، و من الشروط منها ما يتعلق بالخبير (أولا) و منها ما يتعلق بقرير الخبرة (ثانيا).

أولا: الشروط المتعلقة بالخبير.

يكن حصر الشروط المتعلقة بالخبير في التالي:

أ-أن يتم اختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة دون التزام بترتيب معين، و إذا لم يتضمن الجدول من الخبراء المختصين في مجال الخبرة فإنه يجوز لجهات التحقيق بصفة استثنائية اختيار خبراء ليسوا مقيدين في الجدول[1].

ب-حلف اليمين القانوني: إذ يجب لصحة عمل الخبير أداء اليمين القانوني و ذلك لحمله على الصدق و الأمانة في عمله و بث الطمأنينة في أرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، و لذلك لا يغني عن هذا الإجراء أية ضمانة أخرى من الضمانات ،فلقد أوجب المشرع الجزائري بموجب المادة 145 من قانون

[1] – انظر المادة 144 من قانون الإجراءات الجزائية المعدل و المتمم.

الإجراءات الجزائية أن يحلف الخبير اليمين القانوني قبل أداء مهمته، غير انه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى[1].

ثانيا: الشروط المتعلقة بتقرير الخبرة

أما الشروط المتعلقة بتقرير الخبرة فإن الخبير بعد انتهائه من أبحاثه و فحوصاته يعد تقريرا يضمنه خلاصة ما قام به من أعمال و ما توصل إليه من نتائج[2]، بعد تطبيق الأسس و القواعد الفنية على المسالة محل البحث، و إن كان المشرع لن يحدد اتباع شكل معين في تقرير الخبرة فقد يكون شفويا و قد يكون كتابيا وفقا لما تحدده طبيعة المأمورية[3].

لكن الواقع العملي أثبت أن ما يتم في الغالب هو إيداع الخبير تقرير كتابة، سيما إذا كانت المسالة موضوع الخبرة تتطلب إجراء أبحاث و تجارب و فحوصات علمية و عملية ، و غالبا ما يرفق الخبير بالتقرير ملحقا إيضاحيا بالصورة حتى يسهل على جهة التحقيق فهم الخبرة و على جهة الحكم تكوين عقيدتها و اقتناعها الذاتي بالدليل.

و إذا كان الحال كذلك بالنسبة لموضوعات الخبرة التقليدية فإن أهمية إعداد تقارير فنية مكتوبة و ملاحق توضيحية مصورة تصبح حتمية في حالة الجرائم الإلكترونية، حيث يقتضي الأمر عرض و توضيح و تحليل الدليل الجنائي الإلكتروني و كيفية اشتقاقه و استخلاصه[4].

---

[1] – تنص المادة 145 من قانون الإجراءات الجزائية المعدل و المتمم على أنه "يحلف الخبير اليمين المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتية بيانها:

–اقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه و بكل إخلاص و أن أبدي رأيي بكل نزاهة و استقلال. و لا يجدد القسم مادام الخبير مقيدا في الجدول".

[2] – انظر المادة 1/153 من قانون الإجراءات الجزائية المعدل و المتمم .

[3] – سعيداني نعيم، آليات البحث و التحري عن الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة باتنة، الجزائر، 2013، ص 169.

[4] – عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرجع السابق، ص 106.

و يشترط فيما يتعلق بتقرير الخبرة أن يقوم الخبير بإيداع تقريره خبرته خلال المدة المحددة له في أمر حكم الندب، فإن لم يودع تقريره خلال هذه المدة جاز للقاضي استبداله بغيره ما لم يقدم الخبير طلبا بتمديد المهلة [1]و ذلك نظرا لما تتسم به الإجراءات الجزائية من طابع السرعة سيما إذا تعلق الأمر بالجريمة الإلكترونية.

الفقرة الثالثة: القواعد التقنية التي تحكم الخبرة القضائية في البيئة الإلكترونية

لما كانت عملية تجميع الأدلة الإلكترونية تعد من أهم و أصعب الأمور التي تواجه الخبير التقني، كان لزما عليه أن يتبع عدة خطوات من أجل اشتقاق هذا النوع المستحدث من الدليل ، باستخدام وسائل تتماشى مع الطبيعة الإلكترونية المتواجد فيها، و تتمثل هذه القواعد التقنية في خطوات يقوم بها الخبير لاستخلاص الدليل الإلكتروني (أولا)، و وسائل تقنية تمكنه من استخلاص الدليل الإلكتروني (ثانيا).

أولا: خطوات الخبير في استخلاص الدليل في البيئة الإلكترونية.

لما كانت عملية تجميع الأدلة في الشكل الإلكتروني تعد من أهم و أصعب الأمور التي تواجه الخبير التقني، كان لزما عليه أن يتبع عدة خطوات من أجل اشتقاق هذا الدليل، و تتمثل هذه الخطوات في التالي:

1-خطوات ما قبل التشغيل و الفحص:

و تشمل هذه المرحلة على التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها، كذلك التأكد من صلاحية وحدات النظام للتشغيل، كما تشتمل أيضا على تسجيل معطيات وحدات المكونات المضبوطة، كالنوع و الطراز و الرقم التسلسلي...إلخ[2].

2-خطوات التشغيل و الفحص:

-استكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز.

[1] – انظر المادة 148 من قانون الإجراءات الجزائية المعدل و المتمم .

[2] – انيس حسيب السيد المحلاوى، الخبرة القضائية في الجرائم المعلوماتية و الرقمية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2016، ص 109.

-عمل نسخ من كل وسائط التخزين المضبوطة، و على رأسها القرص الصلب لغجراء عملية الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير، سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برامجية.

-تحديد أنواع و أسماء المجموعات البرامجية، برامج النظام (برامج التشغيل)، برامج التطبيقات، و برامج الاتصال، و ما إذا كان هناك برامج أخرى ذات الدلالة بموضوع الجريمة.

-إظهار الملفات المخبأة و النصوص المخفية داخل الصور.

-استرجاع الملفات التي تم محوها من الأصل، و ذلك باستخدام برامج استعادة المعلومات، و كذلك بالنسبة للملفات المعطلة أو التالفة.

-تخزين هذه الملفات أو المعطيات و عمل نسخ طبق الأصل أخرى من الأسطوانة أو القرص المحتوي لها و لفحصها عن طريق تطبيق الخطوات سالفة الذكر[1].

-يتم إعداد قائمة يجرد فيها الخبير كل الأدلة التي تم الحصول عيها في الديسك الخاص به مع إجراء مراجعة لكل صورة محتفظ بها في الديسك في كمبيوتر آخر للتأكد من سلامة القائمة[2].

-تحويل الدليل التقني إلى هيئة مادية و ذلك عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صور أو نصوص، أو وضعها في أي وعاء آخر حسب نوع المعطيات و المعلومات المكونة للدليل[3].

[1] – سعيداني نعيم، المذكرة السابقة، ص 175.

[2] – رشيدة بوكر، المرجع السابق، ص 431.

[3] – سعيداني نعيم، المذكرة السابقة، ص 170.

3-تحديد مدى الترابط بين الدليل المادي و الدليل التقني:

في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط، و الدليل التقني في شكله المادي المستخرج من جهاز الحاسب الآلي، و من ثم الربط بينهما مما يكسب الدليل الموثوقية و اليقينية، اللتان تؤديان إلى قبوله لدى جهة التحقيق و الحكم[1].

4-مرحلة تدوين النتائج و إعداد التقرير:

حيث يتم إعداد تقرير بجميع خطوات و إجراءات البحث، و يرفق به في الغالب الملاحق الإيضاحية المصورة أو المسجلة و غيرها لاعتمادها ثم تسلم إلى الجهة القضائية التي طلبتها[2].

و في حقيقة الأمر يتطلب في الخبير في المجالات الإلكترونية أن يجمع بين المؤهل العلمي و الخبرة العلمية، و يمكن اعتبار الخبير الإلكتروني الذي عمل فترة طويلة في القواعد الفنية خبيرا حتى و لو تخلف الجانب العلمي لديه، أما من اقتصر على التعمق العلمي دون ممارسة فعلية للعمل فلا يستطيع أن يكون خبيرا. و من ثم يجب أن تتوافر في الخبير الإلكتروني لغات البرمجيات و أنظمة التشغيل الجديدة، تصميم البرامج و تشغيلها و معرفة الجديد منها، طرق تحليل البرامج أو أنظمة التشغيل، و أن يؤمن الخبير بوجود أشخاص آخرين مثله لديهم القدرة على اختراق الشبكة[3].

ثانيا: الوسائل التقنية التي تمكن الخبير من استخلاص الدليل في البيئة الإلكترونية

ان الخبير الإلكتروني أو المعلوماتي و هو في إطار القيام بعمله له أن يستخدم العديد من الوسائل العلمية و البرمجيات التي تمكنه من استخلاص الدليل الإلكتروني و تساعده في الوصول إلى المجرم المعلوماتي، و غالبا ما تكون هذه الوسائل أدوات فنية تستخدم في بيئة إلكترونية، و نذكر منها:

---

[1] – رشيدة بوكر، المرجع السابق، ص 432.

[2] – هشام فريد رستم، الجوانب الإجرائية للجرائم الإلكترونية، مكتبة الالات الحديثة، 1994، ص 143.

[3] – د/ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشركة، القاهرة، 2009، ص 222.

1-بروتوكول الإنترنت IP:

و يعد هذا البروتوكول المسؤول عن تراسل حزم البيانات عبر شبكة الأنترنت و توجيهها إلى أهدافها، و هو يوجد بكل جهاز مرتبط بالأنترنت و يتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، و الجزء الثاني لمزود الخدمة، و الثالث لمجموعة الحسابات المرتبطة، أما الرابع فيحدد الكمبيوتر الذي تم الاتصال منه، مع ملاحظة أن عنوان IP قد يتغير في كل اتصال بشبكة الأنترنت[1].

2-نظام البروكسل PROXY:

يعمل هذا النظام كوسيط بين الشبكة و مستخدميها بحيث يضمن مقدم الخدمة توفير خدمات الذاكرة الجاهز، و تقوم فكرة البروكسل على تلقي مزود البروكسل طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق البروكسل فيما إذا كانت هذه الصفحة قد تم تنزيلها من قبل فيقوم بإرسالها إلى المستخدم دون حاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية و هنا يستخدم البروكسل أحد عناوينIP. و من أهم مزايا هذا النظام أن الذاكرة المتوفرة لديه يمكن أن تتحفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها، و التي تخص المتهم و الموجودة عند مزود الخدمة[2] .

[1] – سعيداني نعيم، المذكرة السابقة، ص 173.

[2] – هشام فريد رستم، المرجع السابق، ص 144.

3-برنامج معالجة الملفات Xtree Progold:

و هو برنامج يمكن من العثور على الملفات في أي مكان في الشبكة أو على القرص الصلب، و يستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم و الأقراص المرنة المضغوطة أو يستخدم لقراءة البرامج في صورتها الأصلية[1].

[1] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 229.

المطلب الثاني: الإجراءات المتخذة من الجهات الخاصة في كشف الجرائم الماسة بالمستهلك الإلكتروني

تتميز البيانات في الأنظمة المعلوماتية بقابليتها للمحو و فقدانها بسرعة أو صعوبة الوصول إليها ، لذلك كان من الضروري استحداث نوع جديد من الإجراءات يتلاءم مع البيئة الإلكترونية يساعد على تثبيت هذه البيانات للحصول على دليل يكشف وقوع الجريمة أو مرتكبها. و أهم هذه الإجراءات ما استحدثه المشرع في قانون 04/09 سواء المتخذة من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال (الفرع الأول)، أو تلك المتخذة من قبل مقدم خدمات الإنترنت (الفرع الثاني) ، أو المنصوص عليها في قانون التجارة الإلكترونية المتخذة من قبل الأعوان التابعين لوزارة التجارة (الفرع الثالث).

الفرع الأول: الإجراءات المتخذة من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها

لمواكبة التطور التكنلوجي في مجال الاتصالات الإلكترونية و الحصول على دليل إلكتروني منها لما يتميز به هذا الأخير من سرعة قابليته للتلف و التغيير، استحدث المشرع الجزائري إجراء مراقبة الاتصالات الإلكترونية كإجراء للوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، كما عهد مباشرة عملية المراقبة الإلكترونية إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، و التي تمارس مهامها تحت رقابة السلطة القضائية المختصة و طبقا لأحكام قانون الإجراءات الجزائية. وعليه سنحاول تحديد مفهوم هذا الإجراء (الفقرة الأولى) و الضوابط التي تحكمه (الفقرة الثانية).

الفقرة الأولى: مفهوم المراقبة الإلكترونية للاتصالات

لم يعرف المشرع الجزائري إجراء مراقبة الاتصالات الإلكترونية، على غرار المشرع الأمريكي الذي عرفه من خلال قانون المراقبة السلكية و اللاسلكية الفيديرالي بأنها " الالتقاط السمعي ، أو أي التقاط لمحتويات أي اتصال سلكي أو إلكتروني أو شفوي باستخدام أي جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر"[1].

و يتضح من هذا التعريف أن المشرع الأمريكي قد أعطى تعريفا موسعا للمراقبة بحيث تشمل المراقبة على الهاتف العادي و المراقبة على أي اتصال إلكتروني سواء أكان عبر أجهزة اللاسلكي أم عبر الأنترنت، وباستخدام أي جهاز له القابلية على القيام بتلك المهمة.

كما عرف الفقه هذا الإجراء على أنه" مراقبة شبكة الاتصالات[2]، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات و معلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ و الوقت) لتحقيق غرض أمني أو لأي غرض آخر[3].

يتبين من استقرائنا للتعرفين الفقهيين، أن المراقبة الإلكترونية هي إجراء من إجراءات جمع البيانات و المعلومات عن المشتبه فيه، يقوم بها مراقب ذي كفاءة تقنية عالية في مجال المعلوماتية، و يستخدم في هذه المراقبة التقنية الإلكترونية عبر شبكة الأنترنت، غير أن هذه التعريفات لم تحدد زمن المراقبة، هل يكون أثناء البث المباشر للاتصال أم لدى الاتصال الذي يكون في حالة تخزين عند بثه.

غير أن القضاء الأمريكي حسم هذا الغموض و قرر أن كلا من الاتصالات السلكية و الإلكترونية تتم مراقبتها فقط عندما يتم التقاطها في زمن البث، فالقائم على

---

[1] – د/ سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية دراسة مقارنة، دار الكتب القانونية، مصر، 2011، ص 283.

[2] – نبيلة هبا هروال ، المرجع السابق، ص 198.

[3] – د/ سامي جلال فقي حسين، المرج نفسه، ص 284.

التفتيش الذي يطلع على نسخة من اتصال مخزن لا يعد عمله هذا مراقبة للاتصال[1]، و هاذا ما أكده المشرع الجزائري من خلال نص المادة الثالثة من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها، إذ أوجب أن تكون مراقبة الاتصالات الإلكترونية و تجميع و تسجيل محتواها في **'حينها"**[2]، أي يكون في مرحلة النقل و التحويل أي في الزمن الفعلي لنقلها بين أطراف الاتصال و ليس الحصول على اتصالات إلكترونية مخزنة.

و الشيء المراقب هو الاتصالات الإلكترونية عبر شبكة الأنترنت، و التي عرفها القانون الفيدرالي الأمريكي للمراقبة السلكية و اللاسلكية الاتصال الإلكتروني بأنها" أي تحويل لمؤشرات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو أي معلومات من أي نوع يتم بثها جزئيا أو كليا أو بواسطة نظام سلكي أو لاسلكي أو كهرومغناطيسي أو كهروضوئي أو ضوئي بصري...)[3].

و لقد وضع المشرع الجزائري تقريبا نفس التعريف للاتصالات الإلكترونية بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[4].

و تعني التقنية الإلكترونية المستخدمة في المراقبة مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات المتعلقة بالمجرمين وفقا لبرنامج موضوع مسبقا لتحديدهم من أجل ضبطهم و جمع الأدلة لإثبات إدانتهم و تقديمهم للمحاكم[5] ، و هناك العديد من هذه التقنيات من أجل ضبط و جمع البيانات و المعطيات التي يتم تبادلها بين الأشخاص عبر شبكة الأنترنت تستخدم على المستوى الدولي لمكافحة الجرائم عبر الوطنية، و من بين هذه التقنيات برنامج كارنيفور لمراقبة البريد الإلكتروني، و هو

---

[1] – عمر بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، مرجع سابق، ص 368.

[2] – أنظر المادة 03 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] – د/ سامي جلال فقي حسين، ص 284

[4] – أنظر المادة1/و من قانون 04/09 المتعلق بالوقاية من جرام تكنولوجيات الإعلام و الاتصال و مكافحتها.

[5] – مصطفى محمد مرسي، التحقيق الجنائي في الجرائم المعلوماتية، مرجع سابق، ص 205 .

برنامج طورته إدارة تكنلوجيا المعلوماتية التابعة لمكتب التحقيقات الفيدرالي الأمريكي، الذي يقوم بتعقب و فحص رسائل البريد الإلكتروني المرسلة و الواردة عبر أي حاسب خادم تستخدمه أية شركة مزودة لخدمات الأنترنت، و يشتبه في أن تيار الرسائل المار عبر خدماته يحمل معلومات عن جرائم أو حوادث جنائية، و تتم هذه العملية بوضع أجهزة تلك الشركة تحت المراقبة[1].

و من التقنيات أيضا برنامج كشف و جمع الأدلة و القرائن من رسائل البريد الإلكتروني، و هي تقنية تختص بالبحث و التحري عن الوثائق الإلكترونية باعتبار أن الوثائق تترك وراءها أثر لا يمحى، و يمكن استعادتها مهما أجتهد الفاعل في محوها على غرار الوثائق المدونة على الورق، و هذه المعلومات تشمل الطريق الذي سلكته الرسالة في البداية من جهاز المرسل مرورا بعدد من الأجهزة، و يتم تجميع المعلومات في أرشيف خاص ليكون جاهزا للاستخدام و متاحا للخبراء و المحققين و رجال التحري و المراقبة[2] .

[1] – د/ سامي جلال فقي حسين، المرجع السابق، ص 297.

[2] – د/ مصطفى محمد مرسي، المرجع السابق، ص 215.

الفقرة الثانية: شروط تنفيذ المراقبة الإلكترونية

يعتبر إجراء المراقبة الإلكترونية للاتصالات من أخطر الإجراءات الماسة بحق الإنسان في الخصوصية التي سعت التشريعات و الاتفاقيات الدولية لحمايتها، فنجد اتفاقية بودابست لسنة 2001 تنص في المادة 15 على ضرورة احترام حقوق الإنسان في مجال الإجراءات الجنائية التي تتخذ عند وقوع جريمة من جرائم السيبر، لذلك وضع المشرع الجزائري من خلال قانون 04/09 سابق الذكر مجموعة من الشروط وجب التقيد بها من الجهات التي تباشر هذا الإجراء تحت طائلة العقوبات، إذ حمى الحق في الخصوصية و ما يتفرع عنه من حرية المراسلات و سرية الأحاديث و ذلك عن طريق تجريمه لكل سلوك من شأنه الاعتداء على حرمة الحياة الخاصة في المادة 303 مكرر من قانون العقوبات، و عليه فإن هذه الشروط تتمثل في سبب اللجوء إلى المراقبة (أولا) و الحصول على إذن من السلطة القضائية المختصة (ثانيا).

أولا: سبب اللجوء إلى المراقبة الإلكترونية

أوجب المشرع الجزائري من خلال نص المادة 04 من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال، اللجوء إلى المراقبة الإلكترونية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية[1]، و عليه فإن المراقبة الإلكترونية إجراء استثنائي تمليه الضرورة لأنه يتضمن اعتداء جسيما على حرمة الحياة الخاصة و حق الإنسان في السرية، فيباح استثناء لمقتضيات التحريات و التحقيقات القضائية التي تتعلق بكشف الجريمة أو العمل على ضبط الجناة في حالة عجز السلطات القضائية عن اكتشافها بوسيلة أخرى غير المراقبة الإلكترونية.

كما أن ضابط الوقاية من وقوع بعض الجرائم يعتبر السند الشرعي المبرر للمراقبة، و من قبل ذلك أن تكون هناك معلومات كافية تنذر باحتمال اعتداء على منظومة

[1] – أنظر المادة 1/4/ج من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، و في هذه الحالة يتم الترخيص بالمراقبة الإلكترونية.

كما أنها تكون لمكافحة الجرائم التي تمس بالمصالح الأساسية في الدولة و الجرائم الموصوفة بأفعال إرهابية أو تخريبية و الماسة بأمن الدولة، و حالة المساعدة القضائية المتبادلة.

ثانيا: الحصول على إذن من السلطة القضائية المختصة

يعد الإذن ضمانة لازمة لمشروعية المراقبة على الاتصالات الإلكترونية و قد نصت المادة 4 في فقرتها الثانية من القانون 09 / 04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها على أن عمليات المراقبة لا تجرى إلا بإذن مكتوب صادر عن السلطة القضائية المختصة[1].

و جاء في الفقرة الثالثة من نفس المادة على أن الحالات المنصوص عليها في البند " أ" من الفقرة الأولى من هذه المادة أن النائب العام لمجلس قضاء الجزائري هو من يمنح الإذن بالمراقبة لمدة 06 أشهر قابلة للتجديد لضابط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من جرائم المتصلة بتكنلوجيا الإعلام و الاتصال و مكافحتها، و يمنح هذا الإذن على أساس تقرير مكتوب يبين فيه طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها[2]، فإن لم تكن المراقبة وفق للحالات التي أجاز فيها القانون اللجوء إليها و المحددة في نص المادة 4 من نفس القانون فإن المراقب يقع تحت طائلة العقوبات المنصوص عليها في المادة 303 مكرر من قانون العقوبات الجزائري[3].

و في الأخير فإن عدم احترام هاذه الضمانات في عملية المراقبة يترتب عنها البطلان و استبعاد الأدلة الإلكترونية المتحصلة منها و عدم جواز قبولها أما المحاكم

[1] – أنظر المادة 2/04 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[2] – أنظر المادة 3/04 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] – انظر المادة 4/04 من قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

الجنائية، فضلا عن تحقق المسؤولية الجنائية عن جريمة المساس بالحياة الخاصة للأفراد وفق لنص المادة 303 مكرر قانون العقوبات.

الفرع الثاني: الإجراءات المتخذة من قبل مؤدي خدمات الأنترنت

نظرا لما يمتاز به الدليل في الشكل الإلكترونية من سرعة في التدمير أو التعديل ، كان لازما على التشريعات الدولية حماية هذا النوع من الأدلة من الضياع أو التشويه من خلال تجميع البيانات لحظة نقلها عبر الاتصال لتتمكن من الرجوع إليها عند الحاجة، و هو ما أكدت عليه اتفاقية بودابست، حيث الزمت الدول الأعضاء أن تتبنى في تشريعاتها الداخلية إجراء التجميع الفوري للمعطيات المتعلقة بحركة المرور، و يلزم بهذا التجميع مزودي الخدمات، بمعنى أن يقوم هذا الأخير بجمع المحتويات المتعلقة بالاتصال في فترة الإنتاج و تجميعها لحظة النقل عبر الاتصال[1].

و لقد نص المشرع الجزائري على هذا الإجراء تحت عنوان التزامات مقدمي الخدمات في المواد 10 و 11 من قانون الوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال و مكافحتها، و تتمثل هذه الالتزامات في حفظ البيانات المتعلقة بحركة السير و مساعد السلطات في تجميع و تسجيل المعطيات، و عليه سنتناول هذه الالتزامات من خلال إعطاء تعريف لمقدمي الخدمات (الفقرة الأولى) ثم تحديد هاذه الالتزامات (الفقرة الثانية).

[1] – هلال عبد الله أحمد، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، المرجع السابق، ص 248.

الفقرة الأولى: تعريف مقدم الخدمة

حسب المادة الأولى فقرة "ج" من اتفاقية بودابست فإن مزود الخدمة هو كل من يقوم بخدمات الاتصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، و قد يكون جهة عامة أو جهة خاصة و قد يقدم خدماته للجمهور أو لمجموعة من المستخدمين الذين يشكلون مجموعة مغلقة[1].

و هو نفس التعريف الذي نص عليه المشرع الجزائري بموجب الفقرة 06 من المادة الثانية من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال، بأنه كل كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات، أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

و عليه فإن المراسلات التي تتم عبر البريد الإلكتروني و التي يتم استقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه و التي لم يطلع عليها بعد، فإنها تستقر في حالة تخزين إلكتروني و تكون في هذه المرحلة النسخة من الاتصال المخزنة تتواجد فقط كإجراء أو وسيط مؤقت في انتظار استقبال المرسل إليه لها من مزود الخدمة، و بمجرد استلام المرسل إليه المراسلة، فإن الاتصال يكون قد وصل إلى وجهاه الأخيرة، و هنا يكون موقف مزود الخدمة يتراوح بين أمرين، إما أن يقوم بمسح تلك الرسالة أو يقوم بالاحتفاظ بها[2].

[1] – أنظر المادة 1/ج من اتفاقية بودابست لسنة 2001.

[2] – رشيد بوكر، المرجع السابق، ص 447.

الفقرة الثانية: التزامات مقدمي الخدمات

حدد المشرع الجزائري التزامات مقدمي الخدمات و التي تمكن الجهات القضائية من جمع الأدلة الإلكترونية لكشف الجرائم و مرتكبيها، في حفظ المعطيات المتعلقة بحركة السير وفقا للمادة 11 من قانون 04/09 (أولا) و في تقديم المعطيات إلى الجهات المختصة بالتحقيق في المادة 10 من نفس القانون (ثانيا).

أولا: التحفظ على البيانات المتعلقة بحركة السير

التحفظ المعجل هو إجراء أولي تأمر به السلطة المختصة بالتحريات القضائية يهدف إلى محاولة الاحتفاظ ببيانات مخزنة لدي مقدم الخدمة قبل فقدانها. و تواجد هذه البيانات أو حركتها في حوزة مقدم الخدمة أو تحت سيطرته تدعي منه ضرورة مساعدة السلطات المكلفة بالتحقيق من خلال ضبط هاذه البيانات في مرحلة أولى حتى لا يطمس أثرها و تقديمها في مرحلة ثانية لسلطات المكلفة بالتحقيقات القضائية[1].

و هو ما أكدت عليه اتفاقية بودابست لسنة 2001 في المادة 16 على ضرورة السماح للسلطات المختصة لكل دولة طرف أن تأمر أو تفرض بطريقة أخرى مزود الخدمة التحفظ العاجل على البيانات المعلوماتية المخزنة بواسطة نظام معلوماتي، و ذلك عندما تكون هناك أسباب تدعوا للاعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير. و البيانات المعلوماتية التي يشملها الأمر بالتحفظ، هيا بيانات المتعلقة بالمرور و المتعلقة باتصالات سابقة و ذلك من أجل تحديد خط سير هذه الاتصالات بمعنى مصدر أو مكان وصول هذه الاتصالات.

و قد عرفت المادة الأولى فقرة "د" من الاتفاقية بيانات المتعلقة بالمرور على أنها" صنف من بيانات الحاسوب التي تشكل محلا لنظام قانوني محدد، حيث يتم توالد هذه البيانات من الحاسوب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة، و بذلك فهيا تشمل طائفة من البيانات تتمثل في : مصدر

[1] – د/ مصطفى محمد مرسي، المرجع السابق، ص 225.

الاتصالات و وجهتها المقصودة، خط السير و وقت أو زمن الاتصالات، حجم الاتصال و مدته و نوع الخدمة .

و لقد حددت المذكرة التفسيرية لاتفاقية بودابست الأسباب التي تدعوا إلى اتخاذ مثل هاذا الإجراء و هيا كالاتي:

-قابلية البيانات الإلكترونية للتلاشي، حيث تكون محل للمحو أو التغيير سواء كان ذلك بدافع إجرامي يهدف إلى طمس معالم الجريمة أو أي عنصر إثباتي لشخص المجرم ، أو بدافع غير إجرامي و ذلك في اطار الحذف الروتيني للبيانات التي لم تعد الحاجة إليها.

-غالبا ما يتم ارتكاب الجرائم الإلكترونية عن طريق نقل الاتصالات عبر نظم معلوماتية، حيث يمكن أن تتضمن هذه الاتصالات محتويات غير مشروعة، فتحديد مصدر هذه الاتصالات يساعد على معرفة هوية مرتكب الجريمة.

-تامين الدليل الإلكتروني من الضياع، حيث يتم نسخ الاتصالات ذات المحتوى غير المشروع أو دليل على نشاط جنائي من قبل مزودي الخدمات ، مثل المراسلات الإلكترونية التي يتم إرسالها أو استقبالها، و من ثم يمكن الكشف عن دليل جنائي للجرائم المرتكبة[1].

و هو ما نص عليه المشرع الجزائري في نص المادة 11 من قانون 04/09 ، إذ الزم مقدمي الخدمات بحفظ المعطيات، و البيانات التي يشملها أمر التحفظ فقد حددها في المعطيات المتعلقة بحركة السير ،حيث عرفتها المادة الأولى من نفس القانون بأنها " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، و الوجهة المرسل إليها، و الطريق

[1] – هلال عبد الله أحمد، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست ، المرجع السابق، ص 252

الذي يسلكه، و وقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة. و عليه فإن المعطيات التي يلتزم مقدم الخدمة بحفظها هيا[1]:

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.

-الخصائص التقنية و كذا تاريخ و وقت و مدة كل اتصال.

-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل اليهم الاتصالات و كذا عناوين المواقع المطلع عليها.

أما بالنسبة للنشاطات المتعلقة بالاتصالات الهاتفية فإنه يتوجب على مقدم الخدمة حفظ المعطيات التالية[2]:

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

-المعطيات التي تسمح بالتعرف على مصدر الاتصال و تحديد مكانه.

و يعتبر إجراء التحفظ إجراء وقتي، إذ حدده المشرع الجزائري في نفس المادة من ذات القانون في فقرته الثالثة بمدة سنة، ابتداء من تاريخ التسجيل، و يأتي هذا التحديد احتراما للحق في الخصوصية، إذ يلتزم مقدم الخدمات بمسح المعطيات التي يتم حفظها بعد مرور هذه المدة، و هو نفس توجه المشرع الفرنسي في قانون الإجراءات الجزائية في المادة 2/60 الفقرة الثانية و المادة 2/1/37 الفقرة الثانية، يحث بمقتضى هذه المواد يلزم مقدمي الخدمات بالدخول لنظام الاتصالات على المباشر و يأخذ كل التدابير لتأمين الحفظ لمدة لا تتجاوز السنة لمحتوى المعطيات المجمعة و المسجلة من قبل مقدمي

[1] – لمادة 11 فقرة 1 من قانون 04/09. المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[2] – انظر الفقرة الثانية من المادة 11 قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

الخدمات[1]. و عدم التزام مقدمي الخدمات بهذا الإجراء رتب عليه المشرع الجزائري قيام المسؤولية الجزائية عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية[2].

ثانيا: تسليم البيانات إلى السلطات المختصة

إلى جانب التزام مقدم الخدمة بحفظ البيانات و المعطيات المتعلقة بحركة السير يتوجب عليهم أيضا تسليم هذه البيانات التي تكون بحوزتهم للسلطات المختصة عند طلبها، و كذلك مساعدتهم في جمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، و هذا ما نصت عليه المادة 10 من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال[3].

إذ أن تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوي الاتصالات في حينها و وضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 تحت تصرفهم عائد لما يمتاز به مزود الخدمات بإمكانه مراقبة و معرفة جميع الخطوات التي يتبعها المستخدم إذ يتاح له معرفة المواقع التي زارها و المعلومات التي خزنها و كل الاتصالات التي أجراها[4]، و من ثم فإنه ملزم بتمكين جهات التحقيق من كل المعلومات التي تبحث عنها، و ذلك بتجميعها أو تسجيلها.

أما بالنسبة للقانون الأمريكي المعروف بقانون خصوصية الاتصالات الإلكترونية، فقد أجاز لرجال الضبط القضائي في اطار ما يقومون به من جمع الاستدلالات، الاطلاع على البيانات الموجودة في حوزة مقدمي الخدمات و التي تخص مستخدمي شبكة الأنترنت، و ذلك من خلال توجيه طلب إلى مزود الخدمات بتقديم تلك المعلومات، و تتمثل البيانات الواجب تقديمها في:

---

[1] – إلهام بن خليفة، الرسالة السابقة، ص 327.

[2] – أنظر المادة 4/11 و 5 من قانون 04/09 المتعلق بالوقاية من جرام تكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] – المادة 10 من قانون 09-04 ' ...و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة'

[4] – إلهام بن خليفة، الرسالة السابقة، ص 328.

-المعلومات الشخصية الخاصة بالمشترك مثل اسمه و رقم تلفونه و عنوانه.

-المعلومات الشخصية الخاصة بالمتعامل مع المشترك(كل من يتصل به او يدخل معه في صفقة).

-المعلومات المتعلقة بمحتوى البيانات (مضمون المحادثة، مضمون الملفات)[1] .

و هو ما أشارت إليه اتفاقية بودابست من أنه يتوجب على كل دولة طرف أن تتخذ الإجراءات الضرورية التي تسمح لسلطاتها المختصة أن تأمر مقدم الخدمات الذي يقدم خدماته على إقليمها من أجل إرسال البيانات التي في حوزته و المتعلقة بالمشتركين و بالخدمات التي يقدمها، و قد حددت الاتفاقية المقصود بتلك البيانات بقولها أنها تتعلق:

-نوع خدمة الاتصال التي يشترك فيها الشخص و الوسائل الفنية لتحقيقها.

-العنوان البريدي أو الجغرافي و رقم تلفون المشترك.

-رقم دخول المشترك للحصول على تلك الخدمات و الفواتير اللاتي ترسل إليه، و أي معلومات تتعلق بطريقة الدفع، أو أي معلومات أخرى تتعلق بأداء الخدمة أو بالاتفاق بين هذا المشترك و مزود الخدمة[2].

[1] - عائشة بن قادة ، المرجع السابق، ص 162.

[2] - أنظر لمادة 18 من اتفاقية بودابست لسنة 2001.

الفرع الثالث: الإجراءات المتخذة من قبل أعوان الرقابة التابعين لمصالح التجارة

نظرا لخصوصية جرائم الغش التجاري في المعاملات الإلكترونية، و ما تتميز به مسائل تقنية و فنية تحتاج لأشخاص ذوي خبرة في المجال الاقتصادي، منح المشرع الوطني للمستخدمين المنتمون إلى الأسلاك الخاصة بالمراقبة التابعون للإدارة المكلفة بالتجارة مهمة القيام بالمعاينة و التحقيق في هذه الجرائم[1]. و تتمثل الإجراءات المعاينة و التحقيق المتخذة من قبل أعوان إدارة التجارة في تفتيش المحلات التجارية الإلكترونية (الفقرة الأولى) و فحص الوثائق المتعلقة بالمعاملات التجارية الإلكترونية (الفقرة الثانية).

الفقرة الأولى: تفتيش المحلات التجارية الإلكترونية

أجازت المادة 34 من قانون حماية المستهلك للأعوان المكلفين بمعاينة الجرائم المتعلقة بقانون حماية المستهلك و قمع الغش دخول الأماكن في أي وقت كان، سواء كان في النهار أو الليل أو أيام العطل، و الأماكن المسموح لهم دخولها غير محددة على سبيل الحصر، بحيث يمكن أن يتم الدخول إلى المحلات التجارية و ملحقاتها، و أمكان التخزين و الشحن...إلخ، غير أن المشرع استثنى من نطاق هذا الإجراء الأماكن المعدة للسكن[2].

و بتنظيم المشرع التجارة الإلكترونية من خلال قانون 18-05 أصبح من الضروري الاعتراف بالمحلات التجارية الإلكترونية، التي تمارس نشاطها من خلال مواقع إلكترونية معترف بها قانونا[3]، و التي يتم من خلالها البيع و تقديم الخدمات للمستهلكين، و التي

[1] – أنظر المادة 36 من قانون 18-05 المتعلق بالتجارة الإلكترونية

[2] – محمد شرايرية، الرسالة السابقة، ص 300.

[3] – المادة 8 من قانون 18-05 المتعلق بالتجارة الإلكترونية "يخضع نشاط التجارة الإلكترونية للتسجيل في السجل التجاري أو سجل الصناعات التقليدية و الحرفية، و لنشر موقع إلكتروني أو صفحة إلكترونية على الأنترنت مستضيفة في الجزائر بامتداد com.dz ".

أصبحت من الأماكن التي مراقبتها من قبال أعوان الرقابة، و التي يجوز لهم الدخول إليها في أي وقت.

و الغرض من دخول المحلات التجارية الإلكترونية و الأماكن الأخرى هو التفتيش و التحري عن الجرائم المنصوص عليها في قانون التجارة الإلكترونية و قانون حماية المستهلك و قمع الغش، حتى و لو لم يوجد ما يحمل على الاعتقاد بأن جريمة معينة من تلك التي تدخل في اختصاصهم قد ارتكبت. و يفيد ذلك أنه يجوز للعون دخول الأماكن المعروضة أو المودعة فيها السلعة و البضائع سواء على مستوى المواقع الإلكترونية أو العادية، و ذلك لضبط جريمة قد وقعت، أو عند توافر القرائن القوية على وقوع مخالفة لأحكام نصوص قانون التجارة الإلكترونية و قانون حماية المستهلك و قمع الغش، أو حتى لمجرد التحقق من عدم وجود مخالفات.

و يختلف دخول الأماكن عن التفتيش الذي نص عليه قانون الإجراءات الجزائية، فإن كان الهدف الرئيسي للتفتيش هو البحث عن أدلة الجريمة و أثارها، فإن دخول الأماكن في مفهوم قانون حماية المستهلك و قمع الغش و قانون التجارة الإلكترونية ليس بالضرورة البحث عن الجريمة و الأدلة المتعلقة بها، و إنما للرقابة على احترام هذا القانون أي معاينة مادية فقط، و لذا لا يعد الدخول من قبيل التفتيش بالمعنى المقصود في قانون الإجراءات الجزائية لكونه لا يهدف إلى ضبط أدلة جريمة محل تحقيق، و إنما هو إجراء إداري[1].

[1] – محمد شرايرية، الرسالة السابقة، ص 301.

الفقرة الثانية: فحص الوثائق المتعلقة بالمعاملات التجارية الإلكترونية

أجازت قانون حماية المستهلك و قمع الغش للأعوان المنوط بيهم معاينة الجرائم المتعلقة بهذا القانون صلاحية طلب الاطلاع على أية وثيقة تقنية أو إدارية أو تجارية أو مالية أو محاسبتيه، و كذلك كل وسيلة مغناطيسية أو معلوماتية، و تحت يد أي كان[1].

و يتم ذلك عادة عند دخول المحلات التي أجاز القانون دخولها لممارسة حق الاطلاع قصد التحقق من عدم وجود مخالفة لأحكام القوانين و الأنظمة، و من شأن هذا الاطلاع أن يفضي إلى حجزها[2]. و في هذه الأحوال يمنع الاحتجاج في مواجهة أعوان قمع الرقابة بأسرار المهنة، لأنه ليس من الخطر تمكين الأعوان من الاطلاع على أسرار المتدخلين في العملية الاستهلاكية لأن هذا من صميم عمله الذي يلزمه بالمحافظة على السر المهني و إلا أعرض للمسائلة[3].

أما بالنسبة للمعاملات الإلكترونية فإنه يمكن أن يتم هذا الإجراء من خلال دخول موقع تجاري إلكتروني و طلب هذه الوثائق السابقة من المتدخل أو المورد الإلكتروني، و الامتثال لهذا الطلب تحت طائلة المسائلة الجزائية، كما أجاز قانون التجارة الإلكترونية للأعوان الولوج إلى تواريخ المعاملات[4].

[1] – أنظر المادة 33 من قانون 09-03 المتعلق بحماية المستهلك و قمع الغش.

[2] – عبد الحليم بوقرين، الرسالة السابقة، ص 405.

[3] – إلهام بن حليفة، الرسالة السابقة، ص 213.

[4] – أنظر المادة 3/36 من قانون18-05 المتعلق بالتجارة الإلكترونية

المبحث الثاني: حجية الدليل الإلكتروني في إثبات الجرائم الماسة بالمستهلك في العاملات الإلكترونية

تستند عملية الإثبات الجنائي على الدليل باعتباره الوسيلة الرئيسية لكشف الجرائم و نسبتها لمرتكبها، و نتيجة للتطور العلمي و ثورة المعلومات، فإن الدليل الجنائي التقليدي أصبح لا يتفق بشكل كامل مع طبيعة الوسط الذي ارتكبت فيه الجريمة حتى يستطيع القاضي أن يبني القناعة الكاملة في الإثبات، و لهذا ظهرت طائفة جديدة من الأدلة تتفق مع طبيعة الوسط الذي ارتكبت فيه الجرائم الماسة بالمستهلك الإلكتروني و هو الدليل الإلكتروني الذي يستطيع القاضي بموجبه أن يبني قناعته و يصدر حكمه.

غير أن البحث في حجية الدليل الإلكتروني في إثبات الجرائم الماسة بالمستهلك الإلكتروني يثير مسألتين الأولى تتعلق بهذا النوع المستحدث من الأدلة التي تختلف عن مفهومها التقليدي و أنها قابلة للاختفاء بسرعة وقابلة للعبث بها، و المسألة الثانية تتعلق بجية هذا الأخيرة أما القاضي الجنائي إذ تطرح مشكلة مدى مشروعيتها خاصة إذا عرفنا أن إجراءات الحصول عليها قد ينطوي على المساس بالخصوصية. و عليه سوف نحاول التطرق إلى هذا الموضوع من خلال تحديد ماهية الدليل الإلكتروني (المطلب الأول)، و تحديد حجيته أما القاضي الجنائي (المطلب الثاني).

المطلب الأول: ماهية الدليل الإلكتروني في إثبات الجرائم الماسة بالمستهلك الإلكتروني

كما أثرت الثورة المعلوماتية على نوعية الجرائم التي صاحبتها و ظهور أنماط مستحدثة من الجرائم فرفت بالجرائم الإلكترونية بما فيها الماسة بالمستهلك الإلكتروني ، فإنها أيضا أثرت على دليل إثباتها فأصبحت تحتاج إلى طرق تقنية تتناسب مع طبيعتها، بحيث يمكنها فك رموزه و ترجمته نبضاته إلى كلمات و بيانات محسوسة و مقروءة تصلح لان تكون أدلة إثبات هذه الجرائم. و هو ما يقتضي منا التطرق لماهية هذا الدليل المستحدث و ذلك من خلال تحديد مفهومه (الفرع الأول)، و تبيان أنواعه و أشكاله (الفرع الثاني).

الفرع الأول: مفهوم الدليل الإلكتروني

يعتبر الدليل الإلكتروني الوسيلة الوحيدة و الرئيسية لإثبات الجرائم الماسة بالمستهلك الإلكتروني، غير انه بسبب طبيعته و خصوصيته الإلكترونية تجعلنا نحاول تحديد مفهومه من خلال تعريفه (الفقرة الأولى) و تبيان خصائصه (الفقرة الثانية).

الفقرة الأولى: تعريف الدليل الإلكتروني

تعددت التعريفات حول الدليل[1] الإلكتروني و تباينت بين التوسع و التضييق، ويرجع ذلك لاختلاف مجال كل باحث، فمنهم من عرفه في مجال التقنية و منهم من عرفه قانونا.

فيعرف الدليل الإلكتروني على أنه" كل بيانات يمكن إعادتها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما. و هناك من يعرفه بأنه الدليل الذي يجد له أساس في العالم الافتراضي و يقود إلى الجريمة[2].

---

[1] – الدليل لغة: هو المرشد و ما يتم به الإرشاد، و ما يستدل به ، و الدليل هو الدال أيضا، و الجمع أدلة او دلالات. **أنظر عائشة بن قادة، المرجع السابق، ص 53.**

[2] – عائشة بن قارة مصطفى، المرجع السابق، ص 53.

و عرف كذلك بأنه معلومات يقبلها العقل و المنطق و يعتمدها العلم ، يتم الحصول عليها بإجراءات علمية و قانونية بترجمة المعلومات و البيانات المخزنة في الحاسوب و ملحقاته و شبكات الاتصال و يمكن استخدامها في أي مرحلة من مراحل التحقيق و المحاكمة لإثبات حقيقة فعل شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه[1].

و كذلك عرف الدليل الإلكتروني بأنه الدليل المأخوذ من أجهزة الحاسوب و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، من الممكن تجميعها و تحليلها باستخدام برامج و تطبيقات خاصة، و يتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء[2]. أو هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، و أجهزة و معدات و أدوات الحاسب الآلي، أو شبكات الاتصال من خلال إجراءات قانونية و فنية ، لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور و أشكال و أصوات لإثبات وقوع الجريمة لتقرير البراءة أو الإدانة فيها[3].

و نلاحظ من خلال التعريفات السابق أنها متقاربة ، حيث حاولت استيعاب هذا النوع المستحدث من الدليل بالرغم من حداثته و ارتباطه بالتقنية الرقمية، إلا أن هناك بعض الملاحظات ينبغي الإشارة إليها و تتمثل في:

-حصرت التعريفات السابقة مصادر الأدلة الإلكترونية في أجهزة الحاسب الآلي و ملحقاتها أو ما تعرف عند التقنيين بفتح النظم المعلوماتية و نظم الاتصال[4]، إلا أن العلم

---

[1] – خالد عياد الحلبي، المرجع السابق، ص 230.

[2] – دوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الحاسوب الآلي و الإنترنت، دار الكتاب القانونية، مصر، ص 88

[3] – عبد الناصر محمود فرغلي، ود/ عبيد سيف عبيد المسماري، **"الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية"**، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي دراسة تطبيقية مقارنة، الرياض ، المنعقدة في الفترة 12-2007/11/14 ،ص 13.

[4] – فتح النظم الحاسوبية تتألف من محركات الأقراص الصلبة و لوح المفاتيح ورصد مثل الحواسيب المحمولة و شاشات الحاسوب و غيرها من النظم التي تحتوي على المعلومات المخزنة. أما نظم الاتصال فتشمل جميع انواع الشبكات بما فيها شبكة الإنترنت التي تتوفر على العديد من المواقع المختلفة. **أنظر على حمود حمودة، "الأدلة**

أثبت أن هناك نظم أخرى مدمجة بالحواسيب قد تحتوي على العديد من الأدلة الإلكترونية كالهواتف المحمولة، و البطاقات الذكية، و المساعد الرقمي الشخصي.

-ألحق البعض من التعريفات مفهوم الأدلة الإلكترونية بمفهوم البرنامج على الرغم من اختلافهما، فالفرق بينهما يكمن في الوظيفة التي يؤديها كل واحد منهما، فبرنامج الحاسب الآلي له دور في القيام بمختلف العمليات التي يحتويها نظام المعالجة الآلية و الذي لا يقوم بعمله إلا عن طريق مجموعة من البرامج تسمح بالقيام بمختلف العمليات عند إعطاء أوامر بذلك، أما الدليل الإلكتروني فله أهمية كبرى و دوره أساسي في معرفة كيفية حدوث الجرائم الإلكترونية بهدف إثباتها و نسبتها إلى مرتكبها.

و تأسيسا على ما سبق يمكن تعريف الدليل الإلكتروني بأنه" **مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات خاصة ، لتظهر في شكل صورة أو تسجيلات صوتية أو مرئية، بهدف إثبات وقوع جريمة و نسبتها إلى مرتكبيها**".

المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، ورقة عمل ، المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية، دبي، 2003، ص 22.

الفقرة الثانية: خصائص الدليل الإلكتروني

إن البيئة الرقمية التي يعيش فيها الدليل الإلكتروني بيئة متطورة بطبيعتها، فهي تشمل أنواع متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكون دليلا للإدانة أو البراءة، و قد انعكس هذا العالم الرقمي على طبيعة هذا الدليل مما جعله يتصف بعدة خصائص ميزته عن الدليل الجنائي التقليدي و هي كالتالي:

أولا: الدليل الإلكتروني دليل علمي

يتكون الدليل الإلكتروني من بيانات و معلومات ذات صفة إلكترونية غير ملموسة لا تدرك بالحواس العادية ، بل يتطلب إدراكها الاستعانة بالحاسوب و الأجهزة الإلكترونية ، و استخدام برامج إلكترونية خاصة بذلك. و هذا يعني أنه كدليل يحتاج إلى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات[1]، و لأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني، فالدليل العلمي له منطقه الذي لا يجب أن يخرج عليه، إذ يستبعد تعارضه مع القواعد العلمية السليمة، فإن الدليل الإلكتروني له ذات الطبيعة فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي و إلا فقد معناه[2].

ثانيا: الدليل الإلكتروني دليل تقني

إن الطبيعة التقنية للدليل تقتضي أن يكون هناك توافق بين الدليل المتحصل عليه و بين البيئة التي يعيش فيها و هي البيئة الرقمية أو التقنية أو ما يطلق عليها بالعالم الافتراضي، و يكمن هذا العالم في أجهزة الحاسوب و الخوادم و المضيفات و الشبكات بمختلف أنواعها، و التي تنتج نبضات إلكترونية تصل إلى درجة التخيلية في شكلها و حجمها و مكان تواجدها غير المعلن، فهيا ذات طبيعة ديناميكية فائقة السرعة تنتقل من

[1] – محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 234.

[2] – د/ عمر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004، ص 977.

مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان و المكان، على عكس ما ينتجه الدليل العادي من أشياء مادية كالاعتراف المكتوب أو بصمة الإصبع أو أي وسيلة مادية أخرى[1].

ثالثا: الدليل الإلكتروني يصعب التخلص منه

إن القاعدة التي تسري على كافة ما يتعلق بتقنية تكنلوجيا المعلومات هي أنه كلما حدث اتصال بتكنولوجيا المعلومات عن طريق إدخال بيانات إلى ذلك العالم ، فإنه من الصعب التخلص منها و لو كان ذلك باستخدام أعلى برامج الإلغاء، و تعد هذه الخاصية من أهم خصائص الدليل الإلكتروني، بل يمكن اعتبار هذه الخاصية مميزة يتمتع بها الدليل الإلكتروني عن الدليل العادي[2]، إذ يمكن التخلص بسهولة من الأوراق و الأشرطة المسجلة إذا حملت في طياتها دليل الجريمة بتمزيقها أو حرقها، كما يمكن أيضا التخلص من بصمات الأصابع بمسحها عن موضعها، كما يمكن التخلص من الشهود بتهديدهم أو قتلهم و كل هذا يجعل عملية التخلص من الأدلة أمرا سهلا، و من إمكانية استرجاعها أو استرداد الدليل المستمد منها أمرا مستحيلا بعد تدميرها، أما بالنسبة للأدلة الإلكترونية فإن الحال غير ذلك، حيث يمكن استرجاعها بعد محوها و إصلاحها بعد إتلافها و إظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منها، كما أن نشاط الجاني في عملية محو الدليل يشكل في حد ذاته دليلا ضد الجاني لأن هذا النشاط يتم تسجيله في الحاسوب و يمكن استخلاصه لاحقا كدليل إدانة ضده[3].

فمحاولة التخلص من الدليل الرقمي باستخدام خصائص التخلص من الملفات لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة إذ تتوافر برمجيات ذات

---

[1] – د/ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم و عبد الله عبد العزيز، **"نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر"**، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة و القانون، المجلد الخامس، المنعقد في 10-12 مايو 2003، ص 224.

[2] – عائشة بن قارة مصطفى ، المرجع السابق، ص 63.

[3] – عمر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص 972.

الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب[1].

رابعا: الدليل الإلكتروني دليل متنوع و متطور

يشمل الدليل الإلكتروني كافة أشكال و أنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها و بين الجريمة رابطة من نوع خاص و تتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها و بين الجاني، و تعني هذه الخاصية أنه على الرغم من أن الدليل الإلكتروني في أساسه متحد التكوين بلغة الحوسبة و الرقمية إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها. كان يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات و الخوادم، كما من الممكن أن يكون بيانات مفهومة كما لو كان وثيقة معدة بنظام المعالجة الآلية[2].

أما عن كون الدليل الإلكتروني دليلا متطور فهي خاصية تكاد تكون تلقائية، نظرا لارتباطه بالطبيعة التي تتمتع بها حركة الاتصال عبر الأنترنت و العالم الافتراضي الذي هو في تطور مستمر لتطور تكنلوجيا الاتصال عن بعد[3].

خامسا: الدليل الإلكتروني قابل للنسخ

حيث يمكن استخراج نسخ للأدلة الإلكترونية مطابقة للأصل و لها نفس القيمة العلمية، و هذه الخاصية لا تتوافر في أنواع الأدلة التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد أو التلف و التغيير عن طريق نسخ طبق الأصل من الدليل[4].

---

[1] – تستخدم لاسترجاع الصور و الملفات المحذوفة من الهاردونواكر .Photorec / recover . **أنظر عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 982.**

[2] – عبد الناصر محمود فرغلي، ود/ عبيد سيف عبيد المسماري، المرجع السابق، ص 14.

[3] – رشيدة بوكر، المرجع السابق، ص 390.

[4] – عبد الناصر محمد محمود و عبيد سيف المسماري، المرجع السابق، ص 15.

الفرع الثاني: أنواع الدليل الإلكترونية و أشكاله

إن أدلة الإثبات في الجرائم الإلكترونية عموما تختلف عن أدلة الإثبات في الجرائم العادية ، لأن الجرائم الإلكترونية تتم في بيئة غير مادية عبر نظام الحاسوب و شبكة الأنترنت، إذ تأخذ هذه الأدلة أنواع عديدة (الفقرة الأولى) كما تأخذ عدة أشكال (الفقرة الثانية).

الفقرة الأولى: أنواع الدليل الإلكتروني

نظرا لما يتميز به الدليل الإلكتروني عن الدليل التقليدي من خصائص، يجعله من هذا الدليل عدة أنواع، حيث يمكن تقسيمها من حيث مصدر الدليل (أولا) و من حيث اعتباره كوسيلة إثبات (ثانيا).

أولا: من حيث المصدر

حاول فريق من الفقهاء تقسيم الدليل الإلكترونية من حيث المصدر إلى، الأدلة الإلكترونية الخاصة بأجهزة الكمبيوتر و شبكاتها، و الأدلة الإلكترونية الخاصة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، و الأدلة الإلكترونية الخاصة بالشبكة العالمية للمعلومات[1].

و يلاحظ أن هذا التقسيم يتطابق تماما مع التقسيم الفقهي للجريمة عبر الحاسوب، و الذي قسمها إلى أربعة أنواع تتمثل في [2]:

النوع الأول جرائم الكمبيوتر: و هي سلوك إنساني يشكل فعلا غير مشروع قانونا و يقع على أجهزة الكمبيوتر سواء وقع هذا السلوك غير المشروع على المكونات المادية أو المكونات المعنوية أو قواعد البيانات الرئيسية.

[1] – رشيدة بوكر، المرجع السابق، ص 385.

[2] – د/ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم و عبد الله عبد العزيز، البحث و التحقيق الجنائي في جرائم الكمبيوتر و الإنترنت، المرجع السابق، ص 88.

النوع الثاني جرائم الشبكة العالمية: و هي أي سلوك إنساني يكون فعلا غير مشروع قانونا و يقع على أي وثيقة أو نص موجود بالشبكة.

النوع الثالث جرائم الإنترنت: و هي سلوك إنساني يشكل فعلا غير مشروع قانونا و تقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات .أما **النوع الرابع فهيا الجرائم التي تتم باستخدام الأنترنت.**

كما يلاحظ أيضا أن هذه التقسيمات للجرائم المعلوماتية تدور حول موضوع واحد ألا و هو الدليل الإلكتروني الخاص بجهاز الحاسوب و شبكاته، كما ميزت بين شبكات الحاسوب و الأنترنت و بروتوكول تبادل المعلومات و الشبكة العالمية للمعلومات التي هي في الأصل واحد ، فاختلاف المصطلحات لا يعني اختلاف في المعنى.

ثانيا: من حيث الإثبات

قسم الفقه الأدلة الإلكترونية من حيث الإثبات إلى أدلة معدة كوسيلة إثبات، و أدلة غير معدة كوسيلة إثبات، و سنحاول تحديد كل نوع على النحو التالي:

1-أدلة أعدت لتكون وسيلة إثبات:

يمكن إجمال الأدلة الإلكترونية التي أعدت لتكون وسيلة إثبات فيما يلي:

أ-**السجلات التي تم إنشاؤها بواسطة جهاز الحاسوب تلقائيا،** و تعتبر هذه السجلات من مخرجات الحاسوب التي لم يساهم الأفراد في إنشائها مثل سجلات الهاتف و فواتير أجهزة الحاسب الآلي[1].

ب-**السجلات التي هي جزء منها تم حفظه بالإدخال و جزء تم إنشاؤه بواسطة الآلة الإلكترونية،** و من أمثلة ذلك البيانات التي تم إدخالها إلى الأدلة و تتم معالجتها من خلال برنامج خاص كرسائل غرف المحادثة المتبادلة[2].

[1] – خالد عياد الحلبي، المرجع السابق، ص 234.

[2] – أمال بن خليفة، الرسالة السابقة، ص 252.

2-أدلة لم تعد لتكون وسيلة إثبات:

و هذا النوع من الدليل الإلكتروني نشأ دون إرادة الشخص و له أثر يتركه الجاني دون أن يكون راغبا في وجوده و يسمى بالبصمة الإلكترونية أو الآثار المعلوماتية الإلكترونية، و هي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي و شبكة الأنترنت بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها و كافة الاتصالات التي تمت من خلال الحاسوب أو شبكة الأنترنت[1]، و الواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من طرف من صدر عنه غير أن الوسائل التقنية الخاصة تمكن من ضبط هذه الأدلة و لو بعد فترة زمنية من نشوئها، فالاتصالات التي تتم عبر المنظومة المعلوماتية المرتبطة بشبكة الأنترنت و كذا المراسلات الصادرة عن الشخص أو التي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك[2].

و تبدوا أهمية التمييز بين هذين النوعين في كون النوع الأول من الأدلة الإلكترونية قد أعد سلفا كوسيلة لإثبات بعض الوقائع التي يتضمنها، لذلك فإن عادة ما يعمد إلى حفظه للاحتجاج به لاحقا و هو ما يقلل من إمكانية فقدانه كما يكون من السهل الحصول عليه، بينما النوع الثاني من الأدلة الإلكترونية فلكونه لم يعد أصلا ليكون أثرا لمن صدر عنه لذا فهو في الغالب ما يتضمن معلومات تفيد في كشف الجريمة و مرتكبها و يكون الحصول عليه باتباع تقنيات خاصة لا تخلو من الصعوبة و التعقيد، و هو على عكس النوع الأول لم يعد ليحفظ مما يجعله عرضة للفقدان بسهولة[3].

---

[1] – ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم و عبد الله عبد العزيز ، المرجع السابق، ص38..

[2] – يتم الاعتماد في ضبط هذا النوع من الأدلة بما يعرف ببروتوكول ل IP و الذي يمكن من خلاله ضبط تحركات مستخدم الإنترنت عبر الجهاز الذي يستعمله من خلال بيانات هذا الجهاز عند مزود الخدمة، و أن كان هذا النظام لا يحدد شخصية مرتكب الجريمة فانه يحدد الجهاز الذي ارتكبت منه، و يرى البعض أن ذلك يصح لان يكون قرينة على اعتبار صاحب الجهاز هو مرتكب الجريمة إلى أن يثبت العكس. **أنظر سعيداني نعيم، المذكرة السابقة، ص 129.**

[3] – طارق محمد الجملي، "**الدليل الرقمي في الإثبات الجنائي**"، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية و القانون، المنعقد في 28-2009/10/29 ، الأكاديمية للدراسات العليا طرابلس، ص 130.

و يلاحظ أن هذا التنوع في الدليل الرقمي يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه و إنما تتعدد الوسائل أيضا، و يضل في كل الأحوال الدليل المستمد بواسطتها إلكترونيا.

الفقرة الثانية: أشكال الدليل الإلكتروني

اعتمد في تقسيم الدليل الإلكتروني من حيث الشكل على أشكال المخرجات الحاسوب، إذ يأخذ الدليل الإلكتروني بحسب هذا التقسيم ثلاث أشكال، المخرجات الورقية (أولا) و المخرجات الإلكترونية (ثانيا)، و مخرجات مرئية (ثالثا).

أولا: المخرجات الورقية

تعتبر مخرجات الكمبيوتر الذي يسجل فيه المعلومات على الورق، أحد الأشكال الرئيسية التي تأخذها هذه المخرجات، و يستخدم في ذلك الطابعات، و الطابعة هيا عبارة عن جهاز يقوم بإنتاج نسخ مطبوعة من البيانات، مثل التقارير و الشيكات و قوائم البيانات و البرامج التي يحتاج إليها المستخدمين، و تتنوع الطابعات الملحقة بأجهزة الحاسوب لإنتاج المخرجات الورقية، من حيث طريقة تشغيلها، و سرعة التشغيل و التطبيق المستهدف و خصائص المخرجات الورقية، فهناك طابعات تصادمية تعمل مثل الآلة الكتابية تعمل عن طريق الشريط المبلل بالحبر، و هناك طابعات غير تصادمية تستخدم المواد الكيمائية أو أشعة الليزر أو الحرارة[1].

ثانيا: المخرجات الإلكترونية

تتزايد في الآونة الأخيرة كميات المعلومات المنتجة على أوعية لا ورقية أو غير مطبوعة ، كالأشرطة و الأقراص الممغنطة و المصغرات الفلمية، و غيرها من الأشكال غير التقليدية للتكنولوجيا التي تتوفر عن طريق الوصول المباشر، حيث يقوم المستخدم

[1] – د/ محمد خالد جمال رستم، التنظيم القانوني للتجارة الإلكترونية و الإثبات الإلكتروني في العالم، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006، ص 199.

بإدخال البيانات و يحصل على المخرجات في نفس الوقت. و سنحاول تبيان المخرجات الإلكترونية بالتفصيل:

1-الشريط المغناطيسي:

عبارة عن شريط بلاستيكي مغطى بمادة معدنية قابلة للمغنطة، و الفكرة التي يبني عليها تسجيل البيانات على الشريط المغناطيسي مماثلة لتلك التي يبني عليها تسجيل الأحاديث على شريط التسجيل الصوتي[1].

إذ تسجل البيانات على شكل نقطة مغناطيسية على الشريط بشفرة خاصة تدل على البيانات المستخرجة من داخل الحاسوب، كما يستطيع هذا الرأس الإحساس بوجود هذه النقطة، و يقوم بإرسال النبضات الكهربائية القابلة لشفرة البيانات داخل الحاسب، و يستخدم الشريط المغناطيسي في تخزين البرامج و الملفات المتتالية، أي التي يلزم لقراءة البيانات فيها قراءة الشريط من بدايته، و تنظم المعلومات على الشريط على شكل وحدات خاصة تسمى كل واحدة منها حزمة[2].

2-الأقراص المغناطيسية:

تعبر الأقراص المغناطيسية من أفضل الوسائط التي يمكن استخدامها للتخزين المباشر أو العشوائي، التي تتميز بقدرتها الاستيعابية العالية، و سرعة تداول المعلومات المخزنة عليها.

و من أهم خواص الأقراص المغناطيسية إمكانية القراءة أو التسجيل على أي قطاع من الأسطح، كذلك يمكن تغيير أو تعديل أي ملف مسجل عليها دون الحاجة لإنشاء ملف جديد، إذ يتم تعديل السجل و هو في موضعه[3]، و توجد أنواع عديدة من الأقراص

---

[1] – عمر بن يونس ، **'مذكرات في الإثبات الجنائي عبر الأنترنت'**، ندوة الدليل الرقمي، بمقر جامعة الدول العربية في الفترة بين 5-2005/03/8، ص 49

[2] – د/ محمد خالد جمال رستم، المرجع السابق، ص 200.

[3] – طارق الحملي، المقال السابق، ص 16.

المغناطيسية لعل من أهمها: القرص المرن، القرص الصلب، قرص الخرطوش أو قرص الكارت ريدج[1]

3-المصغرات الفيلمية:

تعتبر مخرجات الكمبيوتر على الميكروفيلم شكلا مختلفا من تكنلوجيا المخرجات، التي تسجل فيه المعلومات على المصغرات الفيلمية المختلفة، بدلا من تسجيلها على الورق، و هيا عبارة عن أفلام فوتوغرافية يتم استخدامها في تصوير صفحات البيانات، مع تصغيرها بدرجة متناهية في الصغر، عن طريق جهاز تحويل البيانات المسجلة على الأشرطة و الأقراص الممغنطة، و تتنوع سعة مخرجات الكمبيوتر على الميكروفيلم طبقا لأنواع المصغرات الفيلمية و معدلات تصغيرها، و يتم قراءتها عن طريق أجهزة خاصة لقراءة الميكروفيلم يطلق عليها قارئ الميكروفيلم[2].

ثالثا: مخرجات مرئية.

يتمثل هذا النوع في عرض مخرجات المعالجة بواسطة الكمبيوتر على الشاشة الخاصة به، و تسمى أيضا وحدة العرض المرئي، و هيا تعتبر من أهم أجزاء الحاسب استخداما، إذ عن طريقها يتم استعراض أي بيانات أو معلومات تكتب على لوحة المفاتيح

[1] – القرص المرن: يعتبر القرص المرن من أشهر وسائط تخزين البيانات، و ذلك نتيجة سهولة استخدامه و تداوله، يصنع القرص المرن من مادة ريقة جدا من البلاستيك، مغطاة بطبقة من مادة مغناطيسية حساسة من أكسيد الحديد. و توجد فتحة كبيرة فيه تسمى بفتحة القراءة و الكتابة و هذه الفتحة هيا التي تصل من خلالها رأس القراءة و الكتابة بوحدة إدارة الأقراص لتلامس القرص المغناطيسي، حيث تتم عملية القراءة و الكتابة بمعني تخزين المعلومات و استرجاعها، و يمكن مسح البيانات من القرص و إعادة تخزينها عدة مرات دون ان يفقد القرص المرن كفاءته.

القرص الصلب: القرص الصلب عبارة عن قرص معدني رقيق و مغطى بمادة قابلة للمغنطة، و يلاحظ أن طبقة التغطية المغناطيسية لهذا القرص تتم على سطح يتم صنعه من سبائك الألمنيوم، و من خواص هذا القرص السعة التخزينية و كذلك سرعة تجزين و استرجاع البيانات التي تفوة سرعة الأقراص المرنة. كما يتميز القرص الصلب أيضا بعدم إمكانية تحريكه من مكانه.

قرص الخرطوش او قرص الكارت ريدج: قرص هجيني يجمع بين خصائص القرص الصلب من حيث كبر حجم السعة التخزينية، و بين و القرص المرن في إمكانية تغييره من مكانه بقرص آخر. **أنظر محمد خالد جمال رستم، المرجع السابق، ص 202.**

[2] – طارق الحملي، المقال السابق، ص 27.

بواسطة المستخدم، كما يتم استعراض البيانات التي تم إدخالها أو المعلومات الناتجة عن معالجة البيانات في وحدة المعالجة المركزية، و كذلك التعليمات الموجهة للمستخدم بواسطة البرامج التطبيقية[1].

الفقرة الثالثة: مصدر الأدلة في الشكل الإلكتروني

إن مصادر الحصول على الدليل الإلكتروني في البيئة الرقمية التي ارتكبت فيها الجريمة الإلكترونية، تتمثل في أجهزة الحاسوب و ملحقاته (أولا) و أنظمة الاتصال بالإنترنت (ثانيا).

أولا: أنظمة الحاسوب و ملحقاته

تعد الحواسيب مصدرا غنيا بالأدلة الرقمية خاصة منها الحواسيب الشخصية التي تعد بمثابة أرشيف سلوك للأفراد أي أنها تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد و رغباتهم[2]، و عليه يمكن من خلال فحصه الحصول على ما يدل على الواقعة و يفيد في عملية التحقيق حيث يشمل الفحص كل المكونات المادية الصلبة و المكونات المعنوية للارتباط القائم بشكل طبيعي بين مكونات الحاسوب ككل، و عليه تشمل عملية الفحص على ما يلي:

1-فحص القرص الصلب:

يحتوي القرص الصلب بداخله على مجموع البيانات الرقمية ذات الطابع الثنائي و التي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي (1.0)، و تتم

[1] – تختلف شاشة عرض الحاسب الشخصي عن طريقة عمل الطرفيات ، و هي شاشة عرض توضع في أماكن بعيدة عن الوحدة المركزية لجهاز الحاسب، مثل الطرفيات التي تستعمل في مكاتب وكالات السفر، للقيام بعملية حجز و إصدار تذاكر الصفر-و تحتفظ الطرفيات بسجلات البيانات المعروضة على الشاشة بداخلها، و تخاطب هذه الشاشات مع الحاسب المركزي في حالة واحدة فقط و هي عندما يتم الاحتياج إلى بيانات جديدة. هذا الأسلوب يجعل شاشات العرض بطيئة ، بالمقارنة فان شاشات العرض للحاسب الشخصي قريبة من وحدة تشغيلها في هذه الحالة يقوم كل منها بالفعل بتناغم كامل مع الآخر. **أنظر د/ محمد محمد المهدي ، تكنلوجيا المعلومات و تطبيقاتها، دار الشروق، ط1، سنة 1989، ص 79.**

[2] – د/ محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 346.

عملية فحص القرص الصلب إما كليا أو جزئيا، الفحص الجزئي يؤدي إلى التعرف على محتوى البيانات التي يؤدي التعامل معها إلى الكشف عن القيمة الاسترادادية للبيانات المخزونة فيه سواء كانت محتويات مكتوبة ، صورة، أو أصوات...إلخ. بالإضافة إلى إمكانية معرفة ما تم حذفه من بيانات و برامج بالاستعانة ببرمجيات خاصة للقيام بذلك[1].

و للتعرف على محتويات القرص الصلب فإن ذلك يتوقف على مسائل عديدة منها الكيفية التي يتم بها ضبط الحاسوب و مهارات الشخص القائم باستخلاص البيانات دون العبث بمحتوياتها لذلك فإنه عند ضبط جهاز الحاسب الآلي، على المحقق أن ينتزع القرص من الجهاز الخاص به و يحافظ عليه من الارتجاج أو الاصطدام بأي شيء، و عدم محاولة تفريغ أي بيانات متواجدة عليه و ذلك تلافيا لفقد أي بيانات، و تسليمه إلى الفني المختص الذي يقوم بتحليل النسخ التي تصدر من القرص و بعض ما توصل إليه المحقق[2].

و إن من الأشياء التي تظهر بعد عملية فحص أي قرص صلب لأي جهاز تلك البيانات التي كان يستخدمها الجاني، و كذلك المخزنة فيه و عناوين صفحات الأنترنت، و من خلالها يمكن التوصل لصفحات و عناوين مواقع الأنترنت و كذلك رسائل البريد الإلكتروني بالإضافة إلى رؤوس الصفحات المرسلة و المتلقات و مجموع البرامج الجاهزة المتخصصة التي استخدمها الجاني و منها يمكن تحديد شركائه و تحديد كل ما ارتكبوه و ما هو مخطط له[3].

2-فحص البرمجيات:

يتطلب الأمر في مثل هذه الحالة أن نميز بين الفحص الداخلي للبرمجيات و الفحص الخارجي لها، فالفحص الداخلي يتم من خلال البحث في البناء المنطقي للبرمجة بما يوحي بأن هناك مجهودا في إعداده للعمل حين إنزاله على جهاز الحاسوب الآلي من

[1] – عمر بين يونس، مذكرات في الإثبات الجنائي عبر الأنترنت المقال السابق، ص 10-11.

[2] – سعيدان نعيم، المذكرة السابقة، ص 131.

[3] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط1، دار الفكر الجامعي، الإسكندرية، 2009 ، ص 218.

خلال تتبع خطوات منطقية تعبر عن هذا الجهد، و اكثر ما يتم البحث عنه في إطار الفحص الداخلي هو البحث عن مصدر الملفات الموجودة في هذا الإطار، ذلك أن النسخ عبر الأنترنت لا يشبه النسخ باستخدام برمجيات المعالجة، فالأول ننسخ عبر العالم الافتراض و الثاني يتم باستخدام مصنف متداول في العالم المادي[1].

أما في حالة الفحص الخارجي و الذي يتم اللجوء فيه إلى النسخة الأصلية للمقارنة بينها و بين النسخة مجل الاشتباه و ذلك للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة[2].

و في كلتي الحالتين ينبغي التنبيه إلى خطورة البرمجيات المعيبة التي يمكن أن تؤثر على الحاسوب و تجعله محل شك تهتز معه قيمة الدليل، يكون لهذا القصور أثره في عملية تقييم الدليل المستمد من البرمجيات ذاتها[3].

3-فحص النظام المعلوماتي:

إن المهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر التي يمكن أن يقوم بها مستخدم الحاسوب، و تعني عملية فحص النظام المعلوماتي ضبط كافة ما يحتوي جهاز الحاسوب الآلي من معلومات، يمكن استرجاعها عبره تكون مخزنة في ملفات على أي شكل يمكن أن يكون عليها الحركة الإستردادية ما دام موضوعها يشكل جريمة[4].

و الحقيقة أنه على حسب كثرة التعامل بالحاسب الآلي يتكاثر محتوى النظام المعلوماتي مما يزيد من صعوبة فحصه بالنظر إلى الحجم الضخم و الكم الهائل من المعلومات المخزنة فيه[5].

---

[1] – عمر بن يونس، مذكرات في الإثبات الجنائي عبر الأنترنت، المقال السابق، ص 11.

[2] – سعيداني نعيم، المذكرة السابقة، ص 132.

[3] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، ص 219.

[4] – عمر بن يونس، الجرائم الناشئة من استخدام الأنترنت، المرجع السابق، ص 998.

[5] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 222.

ثانيا: فحص أنظمة الاتصال بالأنترنت

يقصد بنظام الاتصال بالأنترنت بالمفهوم الإجرائي هو تلك الإجراءات أو المراحل المتبعة حال استخدام الاتصال بالأنترنت، و من أهم المسائل المثارة في صدد فحص أنظمة الاتصال بالأنترنت سيما وراء البحث عن الدليل هي مسألة تحديد مكان الجريمة أو جهاز الحاسوب الذي انطلق منه النشاط الإجرامي، و ذلك من خلال تتبع الحركة العكسية لمسار الأنترنت أي تتبع الحركة التراسلية للنشاط الممارس من خلال الأنترنت، فالحاسوب بمجرد أن يعرف على المسار يقوم تلقائيا باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات[1].

[1] – عمر بن يونس، الجرائم الناشئة عن الإنترنت، المرجع السابق، ص 999.

المطلب الثاني: حجية الدليل الإلكتروني أمام القضاء الجنائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية

إن مرحلة الجنائية، ذلك أن غاية الدعوى هيا الوصول إلى حكم حاسم لها، و لهذا فإن الحكم يمثل أهم إجراءات هذه الدعوى لأنه يمثل غايتها، و عملية تقدير الأدلة تشكل جوهر هذا الحكم، حيث لا يمكن الوصول إليه و إدراكه ما لم يمارس القاضي سلطته التقديرية على الأدلة محل الواقعة، و في مجال الجرائم الماسة بالمستهلك الإلكتروني يكون الدليل الإلكتروني هو الأوفر، سيما إذا اعتبرنا الحكم هو الكلمة النهائية للقضاء، و سلامة هذا الحكم يتوقف على سلامة تقدير هذه الأدلة. و على ذلك سنحاول تحديد حجية الدليل الإلكتروني أما القاضي الجنائي من خلال تبيان سلطة القاضي الجنائي في قبول الدليل الإلكتروني (الفرع الأول)، و سلطة القاضي الجنائي في تقدير الدليل الإلكتروني (الفرع الثاني).

الفرع الأول: سلطة القاضي الجنائي في قبول الدليل الإلكتروني

يعد قبول الدليل الخطوة الإجرائية الأولى التي يمارسها القاضي اتجاه الدليل الجنائي بصفة عامة و الدليل الإلكتروني بصفة خاصة، و ذلك قبل البدء في تقديره، للتأكد من مدى صلاحيته، و ملائمته لتحقيق ما قدم من أجله، و قبول القاضي الجنائي الدليل الإلكتروني في الإثبات لابد و أن يستند على أساس.

و يهدف القاضي الجنائي في هذه المرحلة إلى التيقن من مدى مراعاة الدليل الجنائي أساسا لقواعد المشروعية و التي لا يمكن بدونها أن يترتب على الدليل أي أثار قانونية، بل يثير إهمالها أو مخالفتها ما يستلزم من شروط آثار قانونية أخرى تكمن أساسا في بطلانه و بطلان ما ترتب عليه من إجراءات.

و عليه سنحاول تحديد سلطة القاضي الجنائي في قبول الدليل الإلكتروني لإثبات الجرائم الماسة بالمستهلك الإلكتروني من خلال تحديد أساس قبول الدليل الإلكتروني (الفقرة الأولى)، و التطرق إلى المشروعية كقيد على حرية القاضي الجنائي في قبول الدليل الإلكتروني(الفقرة الثانية).

الفقرة الأولى: أساس قبول الدليل الإلكتروني في الإثبات الجنائي

إن سلطة القاضي في قبول الدليل الإلكتروني تخضع إلى طبيعة نظام الإثبات السائد في الدولة ، و سنحاول تحديدها من خلال النظام اللاتيني (أولا) ثم التظام الانجلوسكسوني (ثانيا).

أولا: في النظام اللاتيني

لم تفرد التشريعات المنتمية لنظام اللاتيني مثل فرنسا و غيرها من الدول المتأثرة بها كالجزائر نصوصا خاصة فيما يتعلق بقبول الدليل الإلكتروني، و ذلك على أساس أن هذه الدول تستند لمبدأ حرية الإثبات في المسائل الجنائية، إذ أن القانون لا يرسم طرقا محددة للإثبات يتقيد بها القاضي الجنائي، بل يترك حرية الإثبات للخصوم في أن يقدموا ما يرونه مناسبا لإقناع القاضي. هاذا من ناحية، و من ناحية أخرى يترك للقاضي في أن يلتمس تكوين اعتقاده من أي دليل يطرح أمامه، و في أن يقدر القيمة الإقناعية لكل منها، حسبما تتكشف لوجدانه، حيث لا سلطان عليه في ذلك إلا ضميره، كما أنه غير مطالب بأن يبين سبب اقتناعه.

1-مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإلكتروني:

تعتبر حرية الإثبات في المسائل الجنائية من المبادئ المستقرة في نظرية الإثبات الجنائي، و ذلك بخلاف المسائل المدنية حيث يحدد القانون سلفا وسائل الإثبات و قواعد قبولها و قوتها، ويقصد بهذا المبدأ "حرية جميع الأطراف في اللجوء إلى كافة وسائل الإثبات للتدليل على صحة ما يدعونه، فلسلطة الاتهام أن تلجأ إلى أي وسيلة لإثبات وقوع الجريمة على المتهم، و يدفع المتهم كذلك بكل الوسائل، ويستظهر القاضي الحقيقة بكل ذلك أو بغيره من طرق الإثبات"[1].

و قد نصت التشريعات المنتمية إلى النظام اللاتيني على هذا المبدأ، فنجد أن المشرع الفرنسي قد أقرى هذا المبدأ صراحة في المادة 427 من قانون الإجراءات الجزائية

[1] – عائشة بن قادة، المرجع السابق، ص 184.

و التي تنص" ما لم يرد نص مخالف، يجوز إثبات الجرائم بجميع طرق الإثبات، و يحكم القاضي بناء على اقتناعه الشخصي...". وهذا النص إن كان مخصصا لمحاكم الجنح ، إلا أن مبدا حرية الإثبات يطبق أمام جميع أنواع المحاكم الجنائية، إلا إذا نص القانون على خلاف ذلك.

و الواقع أن الفقه الفرنسي يدرس حجية المخرجات الإلكترونية في المواد الجنائية ضمن مسألة قبول الأدلة الناشئة عن الألة، أو الأدلة العلمية مثل الرادار و الأجهزة السينمائية و أجهزة التصوير و أشرطة التسجيل و أجهزة التنصت، حيث حكمت محكمة النقض الفرنسية أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل للإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي، و لا يختلف الأمر بالنسبة لقبول مخرجات الحاسب الآلي[1].

كما أقر أيضا المشرع الجزائري مبدأ حرية الإثبات الجنائي في المادة 212 من قانون الإجراءات الجزائية، و التي تنص" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"[2].

و تكمن الأسباب الداعية لضرورة إعمال مبدأ حرية الإثبات في نطاق الإثبات الجنائي فيما يلي:

-إن حرية الإثبات تعد نتيجة منطقية لمبدأ قضاء القاضي بمحض اقتناعه و التي تستتبع في نفس الوقت السماح للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع و يطمئن إليها لتمكين القاضي من أداء رسالته في إرساء العدالة بين المتقاضين.

---

[1] – د/ هلال عبد الله أحمد، حجية محررات الكمبيوتر في المواد الجزائية، دار النهضة العربية، القاهرة، 2006، ص 251.

[2] – و لقد أكدت محكمة النقض المصرية هذا المبدأ في العديد من أحكامها، و استقرت على ان للقاضي الجنائي حرية الاستعانة بكافة وسائل الإثبات لتكوين اقتناعه حول حقيقة الوقائع المرفوعة عنها الدعوى. نقض 25 يناير 1965، مجموع أحكام محكمة النقض، س16 رقم 21، ص 87.

-إن الإثبات في الدعوى الجنائية يرد على وقائع قانونية -مادية أو نفسية- يصعب أو يستحيل الحصول على دليل مسبق لها[1].

-أن موضع الإثبات في الدعوى الجنائية يرد على وقائع قانونية تنتمي إلى الماضي، لذلك لابد للمحكمة أن تستعين بكل الوسائل الممكنة كي تعيد لها رواية ما حدث.

-من المسلم به أن قرينة البراءة تلقي عبء الإثبات كلية على عاتق سلطة الاتهام مما جعلت مهمة هذه الأخيرة جد صعبة[2].

-مبدأ حرية الإثبات يعد بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية و التي لو حصرها كأدلة إثبات على مواجهة الجرائم المستحدثة و منها الإلكترونية[3].

و على ذلك نلاحظ أن الدليل الإلكتروني شأنه في ذلك شأن الأدلة الأخرى التي تم ذكرها على سبيل المثال في القانون، مقبول مبدئيا في الإثبات الجنائي بصفة عامة، و الإثبات في مجال الجرائم الإلكترونية بصفة خاصة.

2-النتائج المترتبة على تطبيق مبدأ حرية الإثبات الجنائي:

إن إعمال مبدأ حرية الإثبات يجعل القاضي الجنائي يتمتع بدور إيجابي في توفير و قبول الدليل الجنائي بما في ذلك الدليل الإلكتروني[4]، و سوف نتناول دور القاضي الجنائي في توفير و قبول الدليل الإلكتروني على النحو التالي:

[1] – أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2016 ص 196.

[2] – د/ هلال عبد الله أحمد، حجية محررات الكمبيوتر في المواد الجزائية، المرجع السابق، ص 153.

[3] – أشرف عبد القادر قنديل، المرجع السابق، ص 197.

[4] – عائشة بن قادة، المرجع السابق، ص 194.

أ-الدور الإيجابي للقاضي في توفير الدليل الإلكتروني:

يؤدي القاضي الجنائي دورا هاما، بل لعله أكثر الأدوار أهمية في الدعوى الجنائية، و بصفة خاصة في شأن عملية الإثبات، و حتى يتضح لنا هذا الدور المهم للقاضي الجنائي يتعين لنا أن نقوم بتحديد مفهوم هذا الدور بداية، ثم نعرض أهم مظاهر الدور الإيجابي للقاضي الجنائي.

-مفهوم الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكتروني: يقصد به عدم التزام القاضي بما يقدمه له أطراف الدعوى من أدلة، و إنما له سلطة بل و واجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى و الكشف عن الحقيقة الفعلية فيها[1]. و هذا ما أكدته المادة 212 من قانون الإجراءات الجزائية الجزائري.

و في ذلك يختلف دور القاضي الجنائي عن دور القاضي المدني، فإذا كان عمل هذا الأخير مجرد قبول الأدلة المقدمة من الخصوم في الدعوى، فليس له أن يبادر من تلقاء نفسه إلى البحث عن أي دليل أو تقديمه و أن يوجه أحد الأطراف إلى تقديم دليل بعينه، بينما القاضي الجنائي لا يتخذ هذا الدور السلبي[2].

و تجدر الإشارة أن المقصود بالقاضي ليس هو قضاء الحكم فحسب، و إنما يشمل أيضا قضاء التحقيق و كذلك قضاة النيابة العامة باعتبار أن مشكلة الإثبات قد تثور في أي مرحلة تمر بها الدعوى الجنائية، بل يمكن أن تثور قبل ذلك أي في مرحلة جمع الاستدلالات أيضا.

-مظاهر الدور الإيجابي للقاضي في توفير الدليل الإلكتروني: إن القاضي الجنائي من أجل الوصول إلى الحقيقة في الجرائم الإلكترونية، أن يوجه أمرا إلى مزود خدمة الأنترنت بتقديم بيانات و معلومات المتعلقة بمستخدم الأنترنت، كعناوين المواقع التي

[1] – اشرف عبد القادر قنديل، المرجع نفسه، ص 198.

[2] – عائشة بن قادة، المرجع نفسه، ص 194.

زارها وقت الزيارة و الصفحات التي اطلع عليها و الملفات التي أرسلها أو استقبلها و غيرها من المعلومات المتعلقة بكل أفعال المستخدم عندما يتصل بالشبكة[1].

و من مظاهر الدور الإيجابي أيضا للقاضي الجنائي في البحث عن الدليل الإلكتروني، أن يطلب من مقدمي خدمات التصديق الإلكتروني تقديم شهادات التصديق الإلكتروني المنتهية صلاحيتها و البيانات المرتبطة بمنحها[2].

كما يجوز للقاضي الجنائي أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام و الولوج إلى داخله، كالإفصاح عن كلمات المرور و الشفرات الخاصة بتشغيل البرامج المختلفة، كذلك للقاضي الجنائي سلطة الأمر بتفتيش نظم الحاسب الآلي بمكوناته المادية و المعنوية و شبكات الاتصال متى ما قدره ضرورة ملائمة هذا الإجراء[3].

ب-الدور الإيجابي للقاضي في قبول الدليل الإلكتروني:

تعد مرحلة قبول الدليل الإلكتروني الخطوة الثانية بعد البحث عن الدليل و تقديمه من قبل كل من سلطة الادعاء و المتهم و القاضي في حالة ما إذا تطلب أن الفصل في الدعوى يتطلب تحقيق دليل بعينه، و ذلك من أجل خلق حالة اليقين المطلوبة لدى القاضي كأساس لإصدار حكمه بالإدانة أو تأكيد حالة البراءة[4].

و أول شيء ينظر إليه القاضي الجنائي في هذه المرحلة –مرحلة قبول الدليل الإلكتروني– هو التأكد من مشروعية الدليل الإلكتروني، و ذلك قبل الوصول إلى المرحلة الأخيرة ألا و هي مرحلة تقدير الدليل، لأن القاضي الجنائي لا يقدر إلا الدليل المقبول، و لا يكون كذلك إلا إذا كان مشروعا[5].

---

[1] – أنظر المادة 10 من قانون 04/09 المتعلق بجرائم تكنولوجيات الإعلام و الاتصال و مكافحتها.

[2] – أنظر المادة 30 /4 من قانون 04/15 المتعلق بالتوقيع و التصديق الإلكترونيين.

[3] – اشرف عبد القادر قنديل، المرجع نفسه، ص 199.

[4] – عائشة بن قادة، المرجع السابق، ص 195.

[5] – هلال عبد الله أحمد، حجية محررات الكمبيوتر في المواد الجزائية، المرجع السابق: ص 169.

ثانيا: في التشريعات الأنجلوسكسونية

يسود التشريعات الأنجلوسكسونية نظام الإثبات القانوني أو المقيد، و في هذا النظام يحدد المشرع أدلة الإثبات و يقدر قيمتها الإقناعية. و مقتضى ذلك أن يتقيد القاضي في حكمه بالإدانة أو بالبراءة بأنواع معينة من الأدلة، أو بعدد منها طبقا لما يرسمه التشريع المطبق دون أن يأبه في ذلك بمدى اقتناع القاضي بصحة ثبوت الواقعة أو عدم ثبوتها، إذ يقوم اقتناع المشرع بصحة إسناد أو عدم صحته مقام اقتناع القاضي، و هكذا فإن اليقين القانوني يقوم أساسا على افتراض صحة الدليل بصرف النظر عن حقيقة الواقعة أو اختلاف ظروف الدعاوى[1]. و سنحاول تحديد أساس قبول الإثبات بالدليل الإلكتروني في هذه التشريعات الانجلوساكسونية على النحو التالي:

1-الدليل الإلكتروني مقبول استثناء عن قاعد الشهادة المباشرة:

تعتبر هذه التشريعات أو كما يطلق عليها التشريعات العامة أن دليل الشهادة هو المبدأ الأساسي في الإثبات كلما كان متعلق بالدعوى، شريطة أن يدلي الشاهد بما رآه أو سمعه بواسطة حواسه مباشرة، و استبعد الشهادة السماعية التي يشهد فيها الشاهد بما سمعه ممن رأى الواقعة، مما يجعل الدليل الإلكتروني باعتباره من مخرجات الأنظمة الإلكترونية يعتبر شهادة سماع مأخوذة عن سجلات و بالتالي فهو لا يعتد به في الإثبات الجنائي[2]، إلا أن المشرع الأمريكي وضع قائمة من الاستثناءات على قاعدة شهادة السماع و من بينها البيانات و المعلومات التي يتم الحصول عليها من الكمبيوتر، حيث ميز المرشد الفيديرالي الأمريكي لتفتيش و ضبط الحواسب الصادر عام 2002 بين نوعين من الأدلة الإلكترونية فيما يتعلق بمدى اعتبارها شهادة سماعية يعتد بها في الإثبات، و هي السجلات المخزنة في الحاسوب، و سجلات الحاسوب المتوالدة أو المأخوذة عن الحاسوب، و يكمن الفرق بينهما على ما إذا كان الشخص أو الآلة هو من يصنع محتويات هذه السجلات[3]، فسجلات الحاسوب المخزنة و هي تلك البيانات المدونة

[1] – د/ حسنين روف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، مرجع سابق، ص 682.

[2] – د/ اشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، المرجع السابق، ص 201.

[3] – د/ عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرجع السابق، ص 421.

من شخص أو عدة أشخاص و حدث و أن صارت في شكل إلكتروني أو رسائل البريد الإلكتروني و غيرها، فهذه السجلات تتوافق مع قاعدة شهادة السماع لأنها تحتوي على بينات بشرية فإذا تم قبولها للإثبات فإنه يقع على عاتق مزود السجلات أن يبين أن الظروف التي تشير إلى البيانات البشرية الموجودة على السجل موثوقة و يعتد عليها، كما يجب أن تكون صحيحة[1].

أما فيما يتعلق بالسجلات المأخوذة أو المتوالدة عن الحاسوب فهي نتائج برامج الحاسوب أو مخرجاته التي لا دخل للإنسان بإنشائها، فهي ليست من قبيل شهادة السماع ، لا كن يمكن للمحاكم أن تأخذ بها شريطة أن يكون الحاسوب يعمل بطريقة صحيحة و على نحو جيد و سليم[2].

كما أقر المشرع الإنجليزي قبول الدليل الإلكتروني كدليل في الإثبات الجنائي، و ذلك خروجا عن الأصل العام الذي تبناه في عدم قبول الشهادة السماعية، إلا أن هذا القبول مقيد بشروط معينة نصت عليها المادة 69 من قانون البوليس و الإثبات الجنائي لسنة 1984 و هيا عدم وجود أسباب معقولة للاعتقاد بأن البيان يفتقر إلى الدقة بسبب الاستخدام غير المناسب أو الخطأ للحاسب. أن الحاسب كان يعمل في جميع الأحوال بصورة سليمة، و إذا لم يكن كذلك، فإن أي جزء لم يعمل فيه بصورة سليمة أو كان معطلا عن العمل، لم يكن ليأثر في إخراج المستند أو دقة محتوياته. الوفاء بأي شروط متعلقة بالمستند محددة طبقا لقواعد المحاكمة[3].

2- الدليل الإلكتروني مقبول استثناء عن قاعدة الدليل الأفضل:

كما يسود أيضا في دول التشريعات العامة قاعدة الدليل الأفضل أو المستند الأصلي و هو ما أقره القانون الأمريكي بموجب المادة (1002) من قانون الإثبات

[1] – د/ عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، المرجع نفسه ، ص 424.

[2] – إلهام بن خليفة، الرسالة السابقة، ص 263.

[3] – Naughan Bevan and Ken Lidstone- Aguide to the police and criminal evidence act 1984-Bujterworth- London 1985- P497.

الأمريكي و التي تقضي على أن حجية الكتابة أو التسجيل أو الصورة رهن بتقديم الأصل إلا إذا نص القانون على خلاف ذلك، بمعنى أنه حينما يقدم أحد الأطراف دليلا يستند إلى عدة دعائم، فإن عليه تقديم أفضل نموذج، و هو ما يعني أن تكون الأدلة الواجب تقديمها أولية و ليست ثانوية، أصلية لا بديلة[1].

فالدليل الإلكتروني وفقا لقاعدة الدليل الأفضل ليس أفضل دليل متاح لأنه ليس أصلي بل ثانوي منسوخ عن الأصل الموجود في الحاسب أو أي وسيلة إلكترونية، الأمر الذي يثير صعوبات كبيرة حول قبول الأدلة الإلكترونية بحيث يمكن الاعتراض عليها بدعوى أنها نسخ رغم أهميها في إظهار الحقيقة[2].

غير أن المشرع في أمريكا قد حسم الأمر لصالح الدليل التقني بأن نص في قانون الإثبات الفيديرالي في المادة 3/1001 على أنه إذا كانت البيانات المخزنة في الحاسوب أو آلة مشابهة، فإن أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها تعكس دقة البيانات تعد بيانات أصلية".

و يستنتج مما سبق أن القاضي في أنظمة الإثبات الأنجلوساكسونية يمكنه الاستناد في حكمه على الأدلة الإلكترونية طالما تأكد من توافر شروطها القانونية و المتمثلة في الصحة و السلامة و أن يعمل جهاز الحاسوب المستخرجة من الأدلة بكفاءة.

[1] – د/ اشرف عبد القادر قنديل، المرجع السابق، ص 203.

[2] – إلهام بن خليفة، الرسالة السابقة، ص 264.

الفقرة الثانية: المشروعية كقيد على حرية القاضي الجنائي في قبول الدليل الإلكتروني

تخضع قواعد الإثبات الجنائي لمبدأ مشروعية الدليل الجنائي أو مبدأ الشرعية الإجرائية و مقتضاه أن الدليل الجنائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية كالحاسب الآلي مثلا، لا يكون مشروعا و من ثم مقبولا في الإثبات، إلا إذا جرت عملية البحث عنه و الحصول عليه و إقامته أمام القضاء في إطار أحكام القانون[1]، و ذلك باتباع إجراءات صحيحة و سليمة قانونا و استخدام في سبيل الحصول عليه طرق و وسائل مشروعة يقرها العلم بشكل يتضمن تحقيق توازن بين مصلحة المجتمع في العقاب و مصلحة المتهم في احترام كرامته الإنسانية و حقوقه[2].

و لقد وضعت الاتفاقيات الدولية[3] و الدساتير الوطنية[4] و القوانين الإجرائية المختلفة[5] نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية و من ثم فإن مخالفة هذه النصوص في تحصيل الدليل الجنائي يصم هذا الدليل بعدم المشروعية، و من هنا فإنه لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم دليلا إلكترونيا تم الحصول عليه من تفتيش لنظام معلوماتي باطل، كان يكون إذن التفتيش صادر من جهة قضائية غير مختصة ، أو لم تكن الجريمة الإلكترونية محل الإذن قد وقعت بعد، أو عملية المراقبة الإلكترونية إن لم يحسن استخدامها بالكيفية المنصوص عليها قانونا فغنه سوف ينجر عليها مساس بحقوق الأفراد و حرياتهم خاصة ما تعلق منها بالخصوصية[6].

---

[1] – عائشة بن قادة ، المرجع السابق، ص 213.

[2] – محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفق أحدث التعديلات التشريعية، الجزء الأول، المرجع السابق، ص 22.

[3] – انظر المواد (5–7–12) من الإعلان العالمي لحقوق الإنسان لسنة 1948.و المواد (3–8–38) من الاتفاقية الأوربية لحقوق الإنسان و الحريات الأساسية لسنة 1950.

[4] – انظر المواد (46–48–32–34 فقرة 2–35) من الدستور الجزائري لسنة 1996. و انظر أيضا المواد (17–19–27–41–42–44–45–71) من الدستور المصري لسنة 1971.

[5] – انظر المواد (41–44) من قانون الإجراءات الجزائية الجزائري. و انظر أيضا المواد (34–35–91–95–206) من قانون الإجراءات الجنائية المصري.

[6] – إلهام بن خليفة، الرسالة السابقة، ص 266.

و الواقع أن هذا القيد يمثل المقابل لحرية القاضي الجنائي في قبول جميع أدلة الإثبات، بما فيها تلك التي لم ينظمها المشرع، فالمعروف أن القانون قد اقتصر على الإشارة على بعض أهم وسائل الإثبات و أكثرها شيوعا في العمل، و ترك الباب مفتوح أما ما قد يستجد من وسائل أخرى، يكون من شأنها تيسير الوصول إلى الحقيقة، هذا من جهة.

و من جهة أخرى يكتسب هذا القيد أهمية كبيرة نتيجة التقدم الهائل الذي تحقق في السنوات الأخيرة في شأن الوسائل الفنية للبحث و التحقيق و التي تسمح أكثر فاكثر باختراق مجال الحياة الخاصة للأفراد، و إن كان في مقابل ذلك يلبي مقتضيات العدالة الجنائية على مكافحة الجريمة بصفة عامة و الجريمة الإلكترونية بصفة خاصة[1].

و الحقيقة أن مشروعية الدليل تعد قيدا و خطا فاصلا بين حق الدولة في توقيع العقاب لضمان أمن و استقرار المجتمع من جهة، و بين ضمان حقوق الأفراد و حرياتهم من جهة أخرى، لذلك فالسؤال المطروح هنا **ما هو موقف القضاء من الدليل غير المشروع و ما هي قيمته في الإثبات الجنائي؟**، إن هذا التساؤل يقودنا إلى البحث عن قيمة كل من دليل الإدانة و دليل البراءة لمعرفة قيمته في الحالتين:

فبالنسبة لدليل الإدانة: انطلاقا من قاعدة أن الأصل في الإنسان البراءة فإن المتهم يجب أن يعامل على أساس أنه برئ في مختلف مراحل الدعوى إلى أن يصدر بحقه حكم بات، و هذا يقتضي أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة سواء كانت أدلة تقليدية أو ناتجة عن الوسائل الإلكترونية بصفة عامة[2]، و ترتيبا على ذلك فإنه لا يجوز للقاضي القبول بالدليل الإلكتروني تم الحصول عليه من إجراء التفتيش أو المراقبة الإلكترونية جرى القيام به دون مراعاة الشروط الشكلية و الموضوعية للإذن بمباشرة هذا

[1] – د/ هلال عبد الله أحمد، حجية محررات الكمبيوتر في المواد الجزائية، المرجع السابق، ص 265.

[2] – عائشة بن قادة ، المرجع السابق، ص 216.

الإجراء، أو كان الدليل متحصلا عليه عن طريق إكراه المتهم المعلوماتي من أجل فك شفرة الدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملفات المخزنة[1].

و انطلاقا من ذلك فأي دليل يتم الحصول عليه بطريقة غير مشروعة يتم إبطاله بما في ذلك الدليل الإلكتروني، و عدم إنتاج الإجراء الباطل للآثار التي تترتب عليه مباشرة، حيث نصت المادة 191 من قانون الإجراءات الجزائية على أن تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها و إذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به و عند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها..".

و إذا كانت القاعدة أن الإجراء الباطل يمتد إلى الإجراء و الإجراءات اللاحقة له مباشرة ، غير أن هذه القاعدة تثير مسألة في غاية الأهمية تتعلق بماهية المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي و الأعمال التالية له حتى يمتد البطلان، و قد تعددت المعايير التي قال عنها الفقه المقارن[2]، و المعيار الراجح في الجزائر هو أن العمل اللاحق يعتبر مرتبطا بالإجراء السابق إذا كان هذا الأخير مقدمة ضرورية لصحة العمل اللاحق، فإذا أوجب القانون مباشرة إجراء معين قبل آخر بحيث يصبح الأول بمثابة السبب الوحيد للجراء الذي تلاه كان الإجراء الأول شرطا لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه[3].

-**أما بالنسبة لدليل البراءة:** هناك اختلاف حول مدى اشتراط المشروعية بوجه عام في دليل البراءة و يمكن رد هذا الخلاف إلى اتجاهين ثلاثة، و سنحاول تبيان هاته الاتجاهات كالتالي:

---

[1] – د/ اشرف عبد القادر قنديل، المرجع السابق، ص 203.

[2] – حمد فتحي سرور ، نظرية البطلان في قانون الإجراءات الجنائية، رسالة دكتوراه ، كلية الحقوق، جامعة القاهرة، مصر، 1959، ص 182.

[3] – د/ احمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، نفس المرجع، ص 382 و ما بعدها

فالاتجاه الأول: يرى أن المشروعية لازمة في كل دليل سواء أكان إدانة أو براءة، و إثبات البراءة كالإدانة لا يكون إلا من دليل تم الحصول عليه من خلال سبل مشروعة و لا يصح أن يفلت إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أي تشريع[1].

أما الاتجاه الثاني: فيرى أن المشروعية لازمة في دليل الإدانة دون البراءة، تأسيسا على أن المحكمة لا تحتاج إلى اليقين في إثبات البراءة بل يكفي في ذلك الشك و هو ما يمكن أن الوصول إليه من خلال أي دليل و لو كان غير مشروع[2].

و هذا ما أكدته محكمة النقض المصرية بقولها" أن كان يشترط في دليل الإدانة أن يكون مشروعا إذ لا يجوز أن تبني إدانة صحيحة على دليل باطل في القانون، إلا أن المشروعية ليست بشرط واجب في دليل البراءة، ذلك أنه من المبادئ الأساسية في الإجراءات الجنائية أن كل متهم يتمتع بقرينة البراءة حتى يحكم بإدانته نهائيا"[3].

و الاتجاه الثالث: يرى ضرورة التفرقة بين ما إذا كان دليل براءة قد تم الحصول عليه نتيجة سلوك يعد جريمة جنائية و ما إذا كان قد تم الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة إجرائية، فإن كان الأول وجب إهدار الدليل و عدم الاعتداء به، لأن القول بغير ذلك مفاده استثناء بعض الجرائم من العقاب و الدعوى إلى ارتكابها و هو ما لا يجوز و تاباه الشرائع القويمة، أما إذا كان الحصول على الدليل يخاف قاعدة إجرائية فحسب فهنا يصلح الاستناد إلى هذا الدليل في تبرئة المتهم تحقيقا للغاية من تشريع البطلان، و لأن الغرض من البطلان الذي شاب وسيلة التوصل إلى الدليل إنما يرجع إلى فعل من قام بالإجراء الباطل، و بالتالي يصح أن يضار المتهم بسبب لا دخل له فيه[4].

و في إيطار الترجيح بين الاتجاهات الثلاثة نؤيد الاتجاه الثاني و الذي يقتصر المشروعية على دليل الإدانة دون البراءة و ذلك لعدة أسباب:

---

[1] – رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الفكر العربي، 2006، ص 40.

[2] – عائشة بن قادة، المرجع السابق، ص 220..

[3] – نقض 31 يناير 1967، مجموع أحكام النقض ، س 18، رقم 24، ص 128. نقض 15 فبراير سنة 1984، مجموعة أحكام النقض، س 15، رقم 13، ص 153.

[4] – عائشة بن قادة ، المرجع السابق، ص 221.

-أن القاعدة هيا افتراض البراءة في المتهم و من ثم فإن أي دليل يساعد على تأكيد هذه القاعدة يجب قبوله دون الالتفاف لأي اعتبار آخر.

-قيد المشروعية ذاته هو احترام حقوق الدفاع مما يستبعد قصر هذا القيد على دليل الإدانة هو وحده الذي يمس حق الدفاع أما قيد البراءة فلا يخضع لهذا القيد.

-كذلك فإن العدالة لا تضار إذا افلت مجرم من العقاب استنادا إلى دليل غير مشروع، لأنه لا يضير العدالة إفلات مجرم من العقاب بقد ما يضيرها إدانة برئ.

الفرع الثاني: سلطة القاضي الجنائي في تقدير الدليل الإلكتروني

بعد قبول القاضي الجنائي للدليل الإلكتروني فإنه يخضعه لعملية تقديرية، و يعتمد القاضي في هذه العملية على حرية الاقتناع أو ما يعرف بمبدأ الاقتناع الشخصي و الذي يعد جوهر الإثبات الجنائي الحر حيث تكاد تتفرع عنه أغلب قواعد الإثبات[1]، فيثور التساؤل من جهة عن ماهية أو مفهوم هذا المبدأ ، و من جهة أخرى أنه لما كان الدليل الإلكتروني هو أفضل دليل لإثبات الجريمة الإلكترونية و هو دليل يقوى على فهمه سوى الخبير في المجال المعلوماتي لأنه يتحصل عليه من عمليات فنية معقدة ، إذا لا يستطيع القاضي فهمه لنقص ثقافته المعلوماتية و عليه فهل يتضاءل دور القاضي إزاء تقدير هذا الدليل بمعنى ما مدى إعمال القاضي لسلطته في تقدير الدليل في الشكل الإلكتروني ، و هل هذه الحرية في تقدير الأدلة مطلقة أو لا؟

و بناء على ما سبق سوف نتطرق إلى مفهوم حرية القاضي بالاقتناع بالدليل الإلكتروني (الفقرة الأولى)، و نتناول مسألة شروط إعمال القاضي لمبدأ الاقتناع القضائي في الأدلة الإلكترونية (الفقرة الثانية).

الفقرة الأولى: حرية القاضي الجنائي بالاقتناع بالدليل الإلكتروني

تقوم حرية القاضي بالاقتناع بالدليل الإلكتروني من خلال مبدأ الاقتناع الشخصي، و لفهم هذا المبدأ بصورة عامة و شاملة يقتضي التعرض إلى تعريفه (أولا) و مدى إعماله مع الأدلة الإلكترونية (ثانيا).

أولا: تعريف مبدأ الاقتناع الشخصي

يعرف فقهاء القانون الجنائي الاقتناع بأنه حالة ذهنية ذاتية نتيجة تفاعل ضمير القاضي و أدلة الإثبات المطروحة و التي يثيرها الخصوم إما لإثبات أو إنكار إتهام[2]. كما

[1] – د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 846.

[2] – مروك نصر الدين، النظرية العامة للإثبات الجنائي، الجزء الأول، ، دار هومة، الجزائر، 2010، ص 620

عرف الاقتناع الشخصي أيضا بأنه حالة ذهنية ذاتية تنجم هن إمعان الفكر في وقائع معروضة من أجل بحثها و الوصول إلى حالة تطرد الشك و الاحتمال، و يجد هذا المبدأ مناخه الطبيعي الملائم في ظل مذهب الإثبات الحر الذي لا يضع تقديرا مسبقا لأدلة معينة لا يمكن الوصول بغيرها إلى اليقين[1]. و من خلال هذا التعريف فإن الاقتناع الشخصي للقاضي الجزائي يتميز بخاصيتين هما :

-أنها حالة ذهنية مبنية على الاحتمال و أن العبرة ليست بكثر الأدلة و إنما بما تتركه من أثر في نفسية القاضي، لأن هذا التأثير سيلعب دورا في تحديد مصير الدعوى الجزائية بالإدانة أو البراءة.

-و الخاصية الثانية تتمثل في أن القاضي حر في أن يأخذ عقيدته أو اقتناعه من أي دليل لكن يجب التأكد هنا من أن حرية الإثبات في المسائل الجزائية ليست خاصية يتميز بها القاضي الجزائي لتتسع سلطته في الإدانة أو البراءة و لكنها، ترجع إلى أن الإثبات في المسائل الجزائية و الوصول إلى الدليل مسألة جد صعبة و ذلك لاختلاف أساليب ارتكاب الجريمة و أن المجرم عادة ما يسعى إلى إخفاء جريمته، لذلك فالبحث عن الحقيقة من خلال الأدلة الجزائية لا يكون عن طريق منح القاضي الجزائي هامشا عن الحرية لمناقشة الدليل الذي يراه مناسبا في إثبات الجريمة.

و لقد أقرت التشريعات الجنائية اللاتينية بهذا المبدأ، بما في ذلك التشريع الجزائري ، حيث نصت المادة 212 من قانون الإجراءات الجزائية على ما يلي: " يجوز إثبات الجرائم باي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"، و جاء في المادة 307 من نفس القانون أن "... إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي قد وصلوا إلى تكوين اقتناعهم، و لا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، و لكنه يأمرهم أن يسألوا أنفسهم في صمت و تدبر، و أن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة

[1] – سعيداني نعيم، المذكرة السابقة، ص 226.

إلى المتهم و أوجه الدفاع عنها و لم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم : هل لديكم اقتناع شخصي" [1].

فالمشرع ترك للقاضي حرية قبول و تقدير الدليل الجنائي بناء على اقتناعه الخاص، فله في سبيل ذلك أن يطرح ما لا يطمئن إليه ، كما له السلطة في التنسيق بين جمع الأدلة المعروضة عليه لاستخلاص نتيجة منطقية منها مجتمعة[2]، و تبعا لهذا المبدأ فهو يساهم في تحقيق مصلحة الجميع لأن النيابة تلزم بتقديم أدلة بعينها حتى يقتنع القاضي، مكا يساهم في تحقيق مصلحة المتهم من جهة أخرى، و ذلك بطرح الأدلة لمناقشتها في الجلسة و تمكينه من تقدير دفوعاته، و إذ بقي شك في ذهن القاضي فإنه يحكم بالبراءة، و هذا الاقتناع لا يخضع فيه القاضي لرقابة المحكمة العليا، إلا أنه لا يمنع من استمال الحكم على بيان الواقعة و الأسباب التي يبنى عليها[3].

ثانيا: الطبيعة العلمية للدليل الإلكتروني و أثرها على اقتناع القاضي الجنائي

يعتبر الدليل الإلكتروني من الأدلة العلمية أو الفنية التي كشف عنها العلم الحديث، و التي تحتاج في الكشف عنها إلى الاستعانة بالخبير، و هو ما يعرف بنظام الإثبات بالأدلة العلمة، الذي يقوم على الاستعانة بالأساليب الفنية التي كشف عنها العلم الحديث في إثبات الجريمة و نسبتها إلى المتهم، و يعطي الدور الأساسي في الإثبات إلى الخبير في عملية الإثبات مما يغني عن الحاجة إلى العملية الذهنية التي يسعى إليها القاضي وصولا إلى الحقيقة، و يقضي عن إعمال السلطة التقديرية للقاضي الجنائي لمختلق الأدلة العلمية[4].

---

[1] – رشيدة بوكر، المرجع السابق، ص 505.

[2] – د/ فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، مكتبة دار الثقافة، عمان 1999. ص 94.

[3] – مروك نصر الدين، المرجع السابق، ص 622.

[4] – إلهام بن خليفة، الرسالة السابقة، ص 274.

إذ أن الأصالة العلمية لدليل الإلكتروني جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي[1]، إذ أن هناك من يرى أن الدليل العلمي و منه الدليل الإلكتروني له قوته الثبوتية الملزمة حتى للقاضي، مستندين في رأيهم إلى أن هذا الدليل يتسم بالقيمة العلمية القاطعة التي يبلغ معها إلى درجة اليقين، لأنها تقوم على أسس و أصول و حقائق علمية دقيقة تتميز بالثبات و الاستقرار و الثقة في مصدرها العلمي، و هناك من يرى أن مبدأ حرية القاضي في الاقتناع يجب أن يبسط سلطانه على كل الأدلة دون استثناء حتى على الدليل الإلكتروني، معتبرين أن إعطاء الدليل الإلكتروني القوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني. و المشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا[2]، و منح القاضي الجزائي سلطة تقدير الدليل و الحرية في تكوين اقتناعه من أي دليل يطمئن إليه، فهل تتصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي إلى الدليل الرقمي المستخرج من الوسائل الإلكترونية؟

إن الطبيعة العلمية و التقنية للجرائم الماسة بالمستهلك الإلكترونية بصفة خاصة و الجريمة المعلوماتية بصفة عامة غالبا ما تفرض على القاضي الاستناد في تكوين قناعته على الخبرة الفنية و التقيد بالنتيجة المتوصل إليها الخبير في تقرير خبرته و لا يمكن طرحها و استبعادها هذا من القيمة العلمية لدليل الإلكتروني فهي تدخل بطبيعتها في نطاق سلطة القاضي التقديرية، بحيث يكون في مقدوره أن يطرح مثل هذه الأدلة رغم قطعيتها من الناحية العلمية عندما يجد أن الدليل الإلكتروني لا يتسق منطقيا مع ظروف الواقعة و ملابساتها، و عليه فوجود الدليل الإلكتروني لا يعني إطلاقا أن يلزم القاضي بالحكم بموجبه بالبراءة أو الإدانة دون البحث في ظروف و ملابسات القضية، بل يخضع لتقديره، و بأن يؤسس حكمه في النهاية على ما وجد في أصل الدعوى من أدلة و ظروف

[1] – رشيدة بوكر، المرجع نفسه، ص 505-508.

[2] – أنظر المادة 212 من قانون الإجراءات الجزائية المعدل و المتمم.

متساندة و غير متساندة و غير منطوية على تناقض أو غموض و ذلك بعد طرحها في جلسة المرافعات.

الفقرة الثانية: الضوابط التي تحكم إقتناع القاضي الجنائي بالدليل الإلكتروني

إن القاضي الجنائي و إن تمتع بسلطة واسعة في تقديره الأدلة بما في ذلك الدليل الإلكتروني، فله أن يتحرى الحقيقة بكافة الأدلة دون الزامه بقيمة مسبقة لدليل ما حتى و لو كان دليلا علميا كالدليل الإلكتروني، أو تحديده لنوع معين من الأدلة لا يجوز الإثبات بغيرها[1]. إلا أنها ليست مطلقة، إذ وضعت لها قيود، و هذه الأخيرة تكون بمثابة صمام أمان إزاء انحراف القاضي عند ممارسته لها لكي لا تختل الأحكام، و عند الإخلال بها فان الرقابة تتحقق عليه. و عليه سوف نتطرق إلى هذه الضوابط بدءا بالضوابط المتعلقة بمصدر الإقتناع (أولا)، و المتعلقة بالإقتناع ذاته (ثانيا).

أولا: الضوابط المتعلقة بمصدر الإقتناع

يمكن حصر الضوابط المتعلقة بمصدر الإقتناع إلى شروط مقبولية الدليل الإلكتروني و شرط وضعية الدليل الإلكتروني، و سنحاول التفصيل في كل منها على النحو التالي:

1-شرط مقبولية الدليل الإلكتروني:

تعد مشروعية الدليل الإلكتروني ضمانة كبيرة للحرية الفردية و تحقيقا للعدالة، لذلك فالقاضي الجنائي ليس حرا في تقدير الدليل الإلكتروني أي كان، بل حر في تقدير الدليل الإلكتروني المقبول في الدعوى، أي تم الحصول عليه بطريق مشروع[2]، إذ يفرض هذا الشرط أن يستمد القاضي الجنائي إقتناعه الذاتي في مجال إثبات الجرائم الإلكترونية من دليل إلكتروني مشروع، و يستبعد في مقابل ذلك الأدلة الإلكترونية المتحصل عليها من

[1] – د/ فاضل زيدان محمد، نفس المرجع، ص 232.

[2] – د/ اشرف عبد القادر قنديل، المرجع السابق، ص 235.

إجراءات باطلة و إلا أبطل معه الحكم، لأنها لا يمكن أن تكون عنصرا من عناصر تقيره[1].

2-شرط وضعية الدليل الإلكتروني:

من القواعد الأساسية في الإجراءات الجنائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح للمناقشة الخصوم في الجلسة، و هو ما يعبر عنه بوضعية الدليل، و مقتضى ذلك أن يكون للدليل الإلكتروني أصل ثابت في أوراق الدعوى سواء كان على شكل بيانات معروضة على شاشة الكمبيوتر، أو مدرجة في حاملات البيانات أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مستخرجة في شكل مطبوعات، و أن تتاح للخصوم فرصة الاطلاع عليه و مناقشته[2]. و قد أرست هذا الضابط المادة 212 فقرة الثانية من قانون الإجراءات الجزائية الجزائري[3].

و علة هذه القاعدة هي مبدأ الشفوية في المحاكمة الجنائية و هو مبدأ أساسي في الإجراءات الجنائية و تقتضيه أولى بديهيات العدالة[4]، حيث يجعل القاضي غير مكتف في تقدير الأدلة سواء كانت تقليدية أو مستخرجة من الوسائل الإلكترونية، على ما دون في محاضر التحقيق، و إنما يتوجب عليه أن يسمع الشهود و اعتراف المتهم بنفسه و ما يدلي به الخبراء و يطرح جميع الأدلة الأخرى للمناقشة الشفوية، حتى يتمكن القاضي من تكوين قناعته من خلال هذه المناقشات التي تجرى أمامه في الجلسة[5].

و من أهم النتائج المترتبة على قاعدة وضعية الدليل الإلكتروني هي "عدم جواز القاضي أن يقضي استنادا على معلوماته الشخصية أو رأي غيره". و يقصد بالعلم الشخصي للقاضي ، معلوماته الشخصية التي يكون قد حصل عليها من خارج نطاق الدعوى المطروحة عليه، و التي من الممكن أن تؤثر في تكوين قناعته عند تقديره لأدلته،

---

[1] – عائشة بن قادة، المرجع السابق، ص 269

[2] – د/ هلال عبد الله احمد، حجية مخرجات الكمبيوتر في المواد الجنائية، المرجع السابق، ص 103.

[3] – أنظر المادة 212 من قانون الإجراءات الجزائية المعدل و المتمم.

[4] – عائشة بن قادة ، المرجع السابق، ص 270.

[5] – د/ فاضل زيد محمد، المرجع السابق، ص 254.

حيث لا يجوز له أن يكون شاهدا أو قاضيا في آن واحد، و عليه فهو يحكم وفقا لما قام به من تحقيق نهائي في جلسة المرافعات[1].

ثانيا: الضوابط المتعلقة بالاقتناع ذاته

تتعلق الضوابط المتعلقة بالإقتناع ذاته بدرجة اليقين التي يصل غلها القاضي، و كون الاقتناع القضائي متوائم مع مقتضيات العقل و المنطق.

1-بلوغ الإقتناع القضائي درجة اليقين:

إن الهدف من الخصومة الجنائية هو الوصول إلى الحقيقة المطلقة، مما يقتضي أن يصدر حكم القاضي عن إقتناع يقيني بصحة ما ينتهي غليه من وقائع، لا بمجرد الضن و الاحتمال، إذ أن الشك يفسر لصالح المتهم آخذا بقاعدة أساسية أن الأصل في الإنسان البراءة، و شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستند إليها في بناء يقينه تقليدية أو أدلة إلكترونية.

أ-مفهوم اليقين:

يعرف اليقين في اللغة أنه" العلم و زوال الشك و عدم وجود أدنى ريبة"، أما تعريفه اصطلاحا فهو اعتقاد القاضي بأن ما وصل إليه هو الحقيقة، أو هو حالة ذهنية و عقلية تؤكد وجود الحقيقة، و الوصول إلى ذلك اليقين يتم عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال وقائع الدعوة و ما يرتبه ذلك من ذهنية من تصورات ذات درجة عالية من التوكيد[2]،و عندما يصل القاضي إلى هذه المرحلة من اليقين فإنه يصبح مقتنعا بالحقيقة فاليقين هو وسيلة الإقتناع .

[1] – عائشة بن قادة، المرجع نفسه، ص 274، و أيضا د/ فاضل زيدان محمد، المرجع نفسه، ص 258.

[2] – محمد محمد، "**السلطة التقديرية للقاضي الجنائي**"، مجلة البحوث، المركز الجامعي بالوادي، العدد الأول، 2004، ص 23.

ب-كيفية الوصول إلى اليقين:

يلتزم القاضي أن يبني اقتناعه على سبيل اليقين و الجزم، و المطلوب عند الإقتناع ليس اليقين الشخصي للقاضي فحسب، و إنما هو اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قولها في الإقناع[1]، و هو بهذا المفهوم يقوم على عنصرين، أحدهما شخصي و يتمثل في ارتياح ضمير القاضي و اطمئنانه إلى إدانة المتهم على سبيل الجزم و اليقين، و الثاني موضوعي و يتمثل في ارتكان هذا الارتياح و الاطمئنان على أدلة من شأنها أن تفض لذلك وفقا لمقتضيات العقل و المنطق[2].

و إذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالأدلة التقليدية عن طريق المعرفة الحسية التي تدركها حواسه، أو المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل و الاستنتاج، فإن الجزم بوقوع الجريمة الإلكترونية و نسبتها إلى المتهم المعلوماتي تتطلب نوع جيد من المعرفة و هي المعرفة العلمية للقاضي بالأمور المعلوماتية لاسيما و أن القاضي الجنائي يلعب دورا إيجابيا في الإثبات[3].

و يترتب على لزوم بلوغ الإقتناع بالإدانة درجة اليقين أنه إذا لم يدرك القاضي هذه الدرجة من الإقتناع كان معنى ذلك أن اقتناعه يتأرجح بين ثبوت التهمة و مسؤولية المتهم عنها و بين عدم ثبوتها أو عدم مسؤولية المتهم عنها، و هذا الإقتناع المتأرجح يعني الشك في ثبوت التهمة، مما يستوجب على القاضي أن يحكم بالبراءة.

ج-استثناء حالة البراءة من شرط الإقتناع اليقيني:

إذا كان الأصل في الإنسان البراءة، فإنه يجب لإدانته أن يقوم الدليل القاطع على ارتكاب الجريمة سواء كانت تقليدية أو إلكترونية، بحيث يقتنع القاضي إقتناعا يقينيا بارتكابها و نسبتها للمتهم، أما فيما يتعلق بأحكام البراءة ، فيكفي أن يتشكك القاضي في

[1] – د/ احمد فتحي سرور، المرجع السابق، ص 475.

[2] – /محمد عيد غريب ،المرجع السابق ، ص 130.

[3] – عائشة بن قادة، المرجع السابق، ص 273.

صحة استناد المتهم إلى التهمة حتى يقضي بالبراءة، و ذلك إعمالا لمبدا الشك يفسر لصالح المتهم[1].

2-كون الاقتناع القضائي متوائم مع مقتضيات العقل و المنطق:

يجب أن يكون استخلاص القاضي الجنائي لوقائع الدعوى استخلاصا معقولا سائغا، و معيار معقولية الإقتناع هو أن يكون الدليل بما في ذلك الدليل الإلكتروني مؤديا إلى ما رتبه الحكم عليه، من غير تعسف في الاستنتاج، و لا تنافر مع مقتضيات العقل و المنطق[2].

و في ذلك قضت محكمة النقض المصرية بأنه" و إن كان من حق محكمة الموضوع أن تستخلص الواقعة من أدلتها و عناصرها المختلفة، إلا إن شرط ذلك أن يكون هذا الاستخلاص سائغا تؤدي إلى ظروف الوقائع و أدلتها و قرائن الأحوال فيها.."[3]

و مع ذلك، تجدر الإشارة إلى أن تقييد القاضي الجنائي عند تقديره للدليل الإلكتروني بضوابط معينة سواء كانت متعلقة بهذا الدليل ذاته أو متعلقة بالاقتناع، غير كافية لضمانة منع الاستبداد و التحكم، بل لا بد من ضمانة أخرى أشد من سابقيها ، لتجعل سلطة القاضي الجنائي التقديرية تدور في ايطار معتدل بهدف الوصول إلى الحقيقة الواقعية باعتبارها غرض الدعوى الجنائية، و تتمثل هذه الوسيلة في رقابة المحكمة العليا على سلطة القاضي الجنائي التقديرية.

[1] – محمد عيد غريب ،المرجع السابق ، ص 132.

[2] – محمد محمد، المقال السابق، ص 24.

[3] – نقض 30 ابريل سنة 1963، مجموعة القواعد القانونية، الجزء الرابع، رقم 208، ص 385. **أنظر حسنين روف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، مرجع سابق، ص 690.**

خلاصة الباب الثاني

إن فاعلية نصوص التجريم و العقاب التي تشكل مضمون حق الدولة في العقاب ترتبط إلى حد كبير بمدى دقة و نجاعة القواعد الإجرائية التي تحدد إجراءات دعوى الحق العام، التي من شأنها أن تضمن اقتضاء الحق المتضمن و المحدد في القواعد الموضوعية، و هو حق الدولة في العقاب، فمن خلالها تقوم ولاية الجهة القضائية المختصة بنظر الجرائم الماسة بالمستهلك الإلكتروني، و عمل جميع السلطات سواء الاستدلالية و الخاصة بالتحقيق، أو ما يعرف بتنظيم قواعد الإختصاص القضائي، و قد أولى المشرع مسألة الإختصاص الجزائي أهمية بالغة فنظم القواعد و المبادئ التي تحكمه، و عالج وسائل إنفاذ هذه القواعد و تطبيق أحكامه، كما يلعب التعاون الدولي دور كبير في تعزيز قواعد الإختصاص القضائي الوطني لمتابعة مرتكبي هذه الجرائم تحقيقا لحماية فعالة و متكاملة للمستهلك في المعاملات الإلكتروني.

كما تعمل هذه النصوص الإجرائية على تحديد وسائل كشف هذه الجرائم و إعطاء حجتها أما مختلف الجهات القضائية. غير أن الجرائم الماسة بالمستهلك الإلكتروني تطرح العديد من المشاكل و التحديات الإجرائية، و من بينها إثبات هذه الجرائم، حيث يحتاج هذا النوع من الجرائم لكشفها أدلة مستخرجة من نفس البيئة التي ارتكبت فيها هذه الجرائم، إذ أصبح الدليل الإلكتروني ضرورة لكشف أنماط هذه الجرائم، كما أن كيفية و مكانة هذا الدليلي يثير نوع من الإشكالات أمام الجهات القضائية باعتباره الوسيلة الوحيدة لإدانة مركب هذا النوع المستحدث من الجرائم.

الخاتمة

يعتبر موضوع الحماية الجزائية للمستهلك في المعاملات الإلكترونية من أكثر المواضيع القانونية أهمية، و لقد حاولنا في هذه الدراسة استعراض جوانب هذه الحماية الجزائية التي أقرها المشرع الجزائري، و الذي وفق إلى حد بعيد في حماية المستهلك في هذا النوع من المعاملات، سواء منها ما تعلق بالشق الموضوع أو تلك المتعلقة بشقها الإجرائي.

فبالنسبة للحماية الجزائية الموضوعية نجد أن المشرع الجزائري حاول التصدي للجرائم الماسة بالمستهلك في المعاملات الإلكترونية من خلال مجموعة من القوانين سواء منها ما تعلق بالغش التجاري في المعاملات الإلكتروني أو تلك المتعلقة بمتطلباته في هذا النوع المستحدث من المعاملات التجارية. أما الحماية الجزائية الإجرائية فتميزت بطابعها الخاص انطلاقا من تحديد قواعد الاختصاص في متابعة الجرائم الماسة بالمستهلك الإلكتروني، و آليات إثبات هذه الجرائم. **و من خلال دراستنا لهذا الموضوع توصلنا إلى النتائج التالية:**

أولا: تتميز المرحلة السابقة على التعاقد الإلكترونية بحاجة المستهلك للمعلومات الخاصة بالسلع و الخدمات مما ينبغي على المورد الإلكتروني إعلام المستهلك بكل ما يتعلق بهذه السلع و الخدمات عن طريق العرض التجاري الإلكتروني، و هو ما يعرف بحق المستهلك في الإعلام الإلكتروني، و مخالفة هذا الحق يعد جريمة نص عليها قانون التجارة الإلكترونية تتمثل صورتها الأولى في مخالفة النظام القانوني للعرض التجاري الإلكتروني التي يتحقق ركنها المادي بإغفال أحد البيانات الإلزامية التي يطلبها القانون في هذا العرض التجاري، أو مخالفة شروط هذا العرض، غير أن إعلام المستهلك لا يتوقف عند هذا الحد بل ينبغي أن يعلم المستهلك بجميع مراحل التعاقد الإلكتروني، و التي حصرها المشرع في مرحلة وضع شروط التعاقد في متناول المستهلك، و مرحلة مراجعة الطلبية، و أخيرا مرحلة تأكيد الطلبية، و مخالفة الإعلام بهذه المراحل هو الصورة

الثانية لمخالفة حق المستهلك في الإعلام، و التي يقوم ركنها المادي على مخالفة أحد أو كل المراحل الإلزامية السابق ذكرها.

ثانيا: يلجأ المورد الإلكتروني في المرحلة السابقة على التعاقد الإلكترونية إلى ترويج منتوجاته عن طريق الإشهار الإلكتروني، الذي يعد أداة لتعريف المستهلك بالسلع و الخدمات، و الذي نظمه المشرع الوطني من خلال قانون التجارة الإلكترونية و الذي نص من خلاله على مجموعة من الالتزامات ينبغي احترامها حتى تتحقق مشروعيته، و مخالفة هذا الالتزامات يعد إشهار إلكتروني غير مشروع و جريمة معاقب عليها، حيث تتحقق عدم المشروعية في الإشهار الإلكتروني سواء عند مخالفة شروط الإشهار التجاري الإلكتروني أو إذا كان الإشهار الإلكتروني غير مرغوب فيه، و الذي يتحقق عند مخالفة المورد الإلكتروني لنظام الموافقة المسبق الذي يمنع من إرسال إشهار عبر البريد الإلكتروني لغرض الاستبيان المباشر ما لم يكون هناك رضا صريح و مسبق من طرف المستهلك، أو مخالفة نظام الرضا اللاحق، و هو عكس النظام الأول أين يسمح للمورد الإلكتروني من إرسال الإشهار التجاري الإلكتروني عبر البريد الإلكتروني، ما لم يبدي عدم رغبته في تلقي ذلك الإشهار.

ثالثا: أستحدث المشرع الجزائري آليات قانونية جديدة لتوفير أكبر قدر ممكن من الحماية للمستهلك عند إبرام العقود الإلكترونية نتيجة لانعدام التوازن العقدي بين طرفين المعاملة الإلكترونية، تتمثل أساسا في حق المستهلك في ضمان منتوجاته و أمنها.

فضمان المنتوجات يتحقق إذا لم يتوفر في البيع وقت التسليم الصفات التي ضمن المورد الإلكتروني للمستهلك وجودها فيه، أو إذا كان بالمبيع عيب ينقص من قيمته أو من نفعه بحسب الغاية المقصودة منه، و مخالفة المورد الإلكتروني لهذا الالتزام يعد جريمة معاقب عليها، إذ تتحقق هذه المخالفة إما عن طريق عدم الالتزام بالضمان الذي يقوم على أساس تقديم شهادة الضمان عند التعاقد، أو عن طريق عدم تنفيذ الضمان بالطرق المحددة قانونا.

أما بالنسبة للنوع الثاني من الضمان فهو ضمان أمن المنتوجات، و هو ذلك الالتزام الذي يتطلب توافر في كل منتج ضمانات ضد كل المخاطر التي من شأنها أن تمس صحة المستهلك، و أمنه أو تضر بمصالحه المالية، و تقوم مخالفة ضمان الأمن بصورتين أولها تتعلق بعدم الالتزام بالمقاييس التنظيمية للإنتاج، و الثانية تتعلق بعدم الالتزام بالإفضاء عن مخاطر المنتجات.

رابعا: يتعرض المستهلك عند التعاقد الإلكتروني إلى مخاطر عديدة، يمكن أن تمس بصحته و سلامة جسده، و التي تتمثل في الخداع و التزوير التجاري للسلع و الخدمات، مما دعي المشرع الوطني لحمايته من هذه الاعتداءات و ذلك بتجريم كل من الخداع و التزوير التجاري.

فجريمة خداع المستهلك تتحقق عن طريق تغليط المستهلك بشأن كمية المنتوجات أو نوعيتها أو طرق الاستعمال...إلخ ، و في حقيقة الأمر كل هذه الأفعال يمكن أن تقع في مجال التجارة الإلكترونية أين يعتمد البائع الإلكتروني إلى محاولة تغليط المستهلك بشأن العناصر السابقة، و على هذا الأساس فإنه يمكن تطبيق النصوص المتعلقة بالخداع على الخداع الإلكتروني، خاصة و أن المشرع لم يحدد الوسيلة التي يتم بها هذا الخداع و إنما نصت المادة 68 أنه **يعاقب على الخداع أو محاولة الخداع بأي وسيلة،** و تعتبر الأنترنت إحدى وسائل الخداع.

أما بالنسبة لجريمة تزوير المنتجات و إن كانت تنصب على محل مادي، غير أنه يتصور أن يتحقق ذلك إلكترونيا في حالة المبيعات الإلكترونية مثل البرامج، فقد يشتري المستهلك برنامجا معينا و عند إرساله من طرف البائع يكتشف أن البرنامج معيب أو غير صالح أو منتهي الصلاحية. و إن كان يمكن تطويع النصوص المتعلقة بجريمة التزوير لتشمل صور الغش في مجال المعاملات الإلكترونية كون الأنترنت وسيلة فقط للتعاقد.

خامسا: إن الجرائم الماسة بالمستهلك خاصة تلك المتعلقة بالغش التجاري في المعاملات الإلكترونية تتطلب نوعا معينا من العقوبات، بحيث تحقق الردع و لا تؤثر

على استقرار المعاملة و مصالح المتعاملين، و لهذا تتجه التشريعات الحديثة نحو العدول عن تسليط العقوبات السالبة للحرية في المجال الاقتصادي، في مقابل فرض عقوبات مالية مناسبة، حيث تعد العقوبة المالية من ابرز العقوبات بالنسبة للجرائم الاقتصادية، و يعود ذلك إلى أن أكثر هذه الجرائم ترتكب بدافع الربح غير المشروع، و لذا فمن المناسب أن تصيب العقوبة الجاني في ذمته المالية، و قد كرس المشرع الوطني هذا الاتجاه في قانون التجارة الإلكترونية و قانون حماية المستهلك و قمع الغش، حيث عاقب على جرائم الغش التجاري في المعاملات الإلكترونية بغرامات مالية متفاوتة.

سادسا: تلزم المعاملات الإلكترونية على المستهلك تبادل بياناته الشخصية مع صاحب السلع أو مقدم الخدمة، و نظرا لأهمية هذه البيانات في إتمام المعاملات الإلكترونية جعلت الفكر القانوني يستقر و يقتنع بضرورة وضع نصوص قانونية خاصة لحمايتها من الاعتداء عليها خاصة في ظل التحديات الرقمية و هو ما جعل المشرع الوطني يضفي حماية خاصة لهذه المعطيات الشخصية، و ذلك من خلال قانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي عند معالجتها إلكترونيا، إذ تضمن هذا القانون مجموعة من الأحكام الجزائية سواء ما تعلق بالجرائم المتعلقة بالجوانب الموضوعية للمعالجة ، أو تلك المتعلق بالجوانب الشكلية لها.

إذ أن الجوانب الموضوعية للمعالجة تشمل كل ما يلزم مراعاتها عند القيام بكل معالجة إلكترونية للمعطيات الشخصية، سواء تعلقت هذه القواعد بتسيير المعطيات ذات الطابع الشخصي، و التي تلزم أن تكون المعالجة مشروعة و متوافقة مع الأغراض المصرح بها و أن يكون استعمال هذه البيانات مشروعا، و مخالفة هذه القواعد المتعلق بتسيير المعالجة تعد جريمة معاقب عليها. أو تعلقت بحقوق الشخص المعني، و التي وضعها المشرع لتمكين المستهلك من حماية حياته الخاصة من كل اعتداء قد يطالها من جراء المعالجة ، و كل مخالفة لهذه الحقوق يعتبر جريمة معاقب عليها.

أما الجوانب الشكلية للمعالجة فهيا تلك القواعد الشكلية التي وضعها المشرع بهدف حماية البيانات الشخصية في مواجهة هذه المعالجة، حيث ألزم المسؤول عن المعالجة

اتخاذ شكليات مسبقة كالحصول على ترخيص أو تصريح قبل معالجة هذه البيانات، و كذلك اتخاذ مجموعة من التدابير لتوفير أكبر قدر ممكن من الحماية لهذه البيانات، و مخالفة هذه القواعد الشكلية يعد جريمة معاقب عليها.

كما اعتمد المشرع الجزائري من خلال قانون 18-07 المتعلق بحماية الأشخاص الطبعيين عند معالجة معطياته الشخصية سياسة عقابية تتماشى مع خطورة الجرائم الماسة ببيانات المستهلك الشخصية في التعاملات الإلكترونية و ذلك من خلال تقرير عقوبات سالبة للحرية و عقوبات مالية، و التي يلاحظ عليها رفع من قيمة العقوبات المالية سواء بالنسبة للشخص الطبيعي أو المعنوي.

سابعا: نظرا لتطور الذي حدث في مجال المعلوماتية و قطاع الاتصالات و ما لها من انعكاسات على المعاملات التجاري الذي يتم عبر شبكة الاتصال الحديثة، لم يعد التوقيع التقليدي ملائما للمعاملات الإلكترونية، لذلك ظهر التوقيع الإلكتروني كبديل عن التوقيع التقليدي ليتوافق و طبيعة المعاملات الإلكترونية. و نظرا للأهمية التوقيع الإلكتروني في المعاملات الإلكترونية، و الذي بدونه لا يصبح للعقد الإلكتروني أي قيمة قانونية، فإن المشرع الجزائري قد نظم هذا النوع المستحدث من التوقيعات، من خلال قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين، حيث نص على تعريفه و شروط الاعتداد به حتى يكون مساويا لتوقيع الكتابي، كما حدد الجهة التي تصادق عليه و هيا مؤدي خدمات التصديق الإلكتروني، و نظم شهادة التصديق عليه من خلال تضمينها مجموعة من البيانات الواجب أن تشملها هذه الشهادة.

كما حرص المشرع الوطني على تقرير حماية جنائية للتوقيع الإلكتروني سواء من خلال قانون العقوبات الذي يشمل حماية أنظمة إنشاء التوقيع الإلكتروني باعتبارها أنظمة معالجة للمعطيات، أو بموجب قانون 15-04 المحدد للقواعد العامة للتوقيع و التصديق الإلكترونيين، و ذلك بإفراد الفصل الثاني من الباب الرابع منه للعقوبات على الجرائم الماسة به. إذ تنوعت هذه الحماية من خلال تقرير المسؤولية الجزائية لمؤدي خدمات

التصديق الإلكتروني، و منها ما يتعلق بشهادة التوقيع الإلكتروني، و أهمها حماية التعامل الغير مشروع في التوقيع الإلكتروني الموصوف الخاص بالغير.

كما اعتمد المشرع الجزائري من خلال قانون 15-04 المحدد للقواعد العامة للتوقيع و التصديق الإلكترونيين على سياسة عقابية تتماشى مع خطورة الجرائم الماسة بالتوقيع في التعاملات الإلكترونية و ذلك من خلال تقرير عقوبات سالبة للحرية و عقوبات مالية ، و التي يلاحظ عليها رفع من قيمة العقوبات المالية سواء بالنسبة للشخص الطبيعي أو المعنوي.

ثامنا: إن فاعلية نصوص التجريم و العقاب التي تشكل مضمون حق الدولة في العقاب ترتبط إلى حد كبير بمدى دقة و نجاعة القواعد الإجرائية التي تحدد إجراءات دعوى الحق العام، التي من شأنها أن تضمن اقتضاء الحق المتضمن و المحدد في القواعد الموضوعية، و هو حق الدولة في العقاب، فمن خلالها تقوم ولاية الجهة القضائية المختصة بنظر الجرائم الماسة بالمستهلك الإلكتروني، و عمل جميع السلطات سواء الاستدلالية و الخاصة بالتحقيق، أو ما يعرف بتنظيم قواعد الاختصاص القضائي، و قد أولى المشرع مسألة الاختصاص الجزائي أهمية بالغة فنظم القواعد و المبادئ التي تحكمه، و عالج وسائل إنفاذ هذه القواعد و تطبيق أحكامه.

فينعقد الاختصاص القضائي بشأن الجرائم الماسة بالمستهلك الإلكتروني بمبادئ عامة تحكم سريان نصوص التجريم على الوقائع محل النظر، و هيا كل من مبدأ إقليمية النص الجنائي الذي يعد الأصل العام و يقوم سواء بتحقيق السلوك الإجرامي لها أو النتيجة على الإقليم الوطني ، و يكون ذلك إذا كان نظام حاسوب المعتدي داخل إقليم الدولة و هو خارجها، أو كان نظام الحاسوب العائد للضحية ضمن النطاق الإقليمي، أو كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة، و مبدأين مكملين هما الشخصية و العينية.

كما يخضع انعقاد الاختصاص القضائي لمجموعة من المعايير الإجرائية، فمنها قواعد عامة عادية لهذه المعايير، و هيا تتعلق أساس بكل من المعيار النوعي و الشخصي و المكاني، غير أن المشرع أجاز الخروج عنها عن طريق ما يعرف بتمديد الاختصاص.

أما بالنسبة لوسائل إنفاذ قواعد الاختصاص القضائي فقد حدد المشرع الوطني الجهات القضائية فزيادة على المحاكم العادية منح المشرع لجهات قضائية اختصاص محلي موسع للنظر في الجرائم الماسة بالمستهلك الإلكتروني، و هي ما يعرف بالأقطاب المتخصصة. كما حدد طرق إنفاذه ، أي طرق تقديم الجاني و الوقائع إلى المحكمة المختصة للنظر و الفصل في الدعوى، و التي يمكن تقسيمها إلى طرق تقليدية كأمر الإحالة من طرف قاضي التحقيق، أو طرق مستحدثة تتمثل في نظام المثول الفوري أو الأمر الجزائي.

تاسعا: يشكل التعاون الدولي في مجال تعزيز الاختصاص القضائي بمتابعة مرتكبي الجرائم الماسة بالمستهلك في المعاملات الإلكترونية جزائيا عنصرا أساسيا في مواجهة الاعتداءات المرتكبة على هذا الأخير طالما أن تحقيق العدالة أضحت مسؤولية عامة و مشتركة تتطلب لتحقيقها اتباع نهج متكامل يواءم مع المبادئ و الأهداف المنصوص عليها في الاتفاقيات الدولية.

عاشرا: تتميز الجرائم التي تركب على المستهلك في المعاملات الإلكترونية بالسرعة و الذكاء عند ارتكابها، و ذلك نظرا لخصوصية البيئة الإلكترونية التي تعتمد على وسائل و تقنيات إلكترونية، مما يستدعي الكشف عنها اتخاذ إجراءات تتلاءم مع هذه البيئة، و هو ما لا تحققه الإجراءات التقليدية نظرا لسهولة تدمير أدلة ارتكاب هذه الجرائم و سهولة تبخرها.

لهذا حرص المشرع الوطني من خلال قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و قانون التجارة الإلكترونية من وضع أسس و أساليب

جديدة لكشف الجرائم الإلكترونية بصفة عامة و الماسة بالمستهلك الإلكترونية بصفة خاصة، تكون متوافقة مع ما تطلبه مثل هذه الأفعال على الشبكة الرقمية.

فمن بين هذه الإجراءات التفتيش و الضبط في البيئة الرقمية التي خولها المشرع للضبطية القضائية، كما منحها اللجوء إلى الخبرة الفنية في حالة عجزهم عن كشف هذه الجرائم أو في حالة الخوف تدمير أدلة الكشف عنها أو عدم معرفة التعامل معها.

كما خول المشرع الوطني لبعض الجهات الأخرى اتخاذ نوع من الإجراءات للكشف عن الجرائم الإلكترونية عامة كالمراقبة الإلكترونية الذي عهد بمباشرته إلى الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام و الاتصال، أو التحفظ المعجل على البيانات الذي يطلب من مقدمي خدمات الأنترنت، كما خول المشرع للأعوان التابعين لمصالح التجارة تفتيش المحلات الإلكترونية و الاطلاع على الوثائق المتعلقة بكل معاملة تجارية إلكترونية.

حادي عشر: إن الدليل الذي يقوم على إثبات الجرائم الماسة بالمستهلك في المعاملات الإلكترونية يكون من ذات طبيعتها أي أنه دليل في شكل إلكتروني، و هو عبارة على معلومات مخزنة في نظم تقنية المعلومات أو مخرجاته أو متنقل عبرها، و يجمع أو يسجل أو يحفظ و يحلل ببرامج و تطبيقات تكنولوجية خاصة لتظهر في النهاية بشكل مقروء يمكن من كشف الجريمة و نسبتها إلى مرتكبيها.

إن الدليل في الشكل الإلكتروني باعتباره من الأدلة العلمية التي لا يفهم خباياها إلا الخبير التقني، فهذا لا يعني إحلال الخبير محل القاضي لأنه إذا كان العلم يكشف عن الجريمة و يضع شبهات حول شخص معين، فإنه لا يمكن أن يلع الدور المهم في الإثبات، و هو التأكد من نسبة الجرم إلى ذلك الشخص، و هذا الدور يفهمه القاضي بمقتضى اقتناعه الشخصي، إذ يبني حكمه في الإدانة أو البراءة على ما جاء في الدعوى من أدلة و ظروف مجتمعة و متساندة.

إن الملاحظات و النتائج التي توصلنا إليها من خلال دراستنا للحماية الجنائية للمستهلك في المعاملات الإلكترونية تدفعنا لطرح مجموعة من المقترحات نراها ضرورية في تصحيح بعض النقاط حتى تتحقق حماية أكثر فاعلية للمستهلك في هذا النوع المستحدث من المعاملات نذكر منها :

أولا: ينبغي على المشرع الجزائري تحديد المدة الزمنية لتسليم وصل الاستلام من طرف المورد الإلكتروني للمستهلك، الذي يؤكد من خلاله للمستهلك تسجيل طلب عدم رغبته في تلقي الإشهار الإلكتروني المنصوص عليها في المادة 32 من قانون التجارة الإلكترونية، كما يجب تحديد لحظة بداية احتساب مدة 24 ساعة المقررة لتنفيذ طلبه.

ثانيا: ضرورة تحديد المسؤولية الجنائية للمتدخلين في بث الإشهار التجاري غير المشروع، أين يتم تحديد مسؤولية كل من مزود الخدمة أو متعهد الوصول و منظمي منتديات المناقشة.

ثالثا: وجب على المشرع الجزائري حتى يتحقق إعلام مفهوم حول مضمون العرض التجاري الإلكتروني أن يشترط على المورد الإلكتروني الوطني اعتماد اللغة العربية بالأساس في عرضه التجاري الإلكتروني ضمن حدود الدولة الجزائرية. فاللغة التي يفهمها المستهلك من بين الوسائل المهمة لحمايته، و التي أوجدتها المبادئ القانونية المعاصرة لكي يستطيع هذا الأخير فهم و معرفة مضمون العرض الذي يريد التعاقد بشأنه.

رابعا: ضرورة تعديل قانون 09-03 المتعلق بحماية المستهلك و قمع الغش و ذلك بإضافة نصوص قانونية تجرم الخداع و التزوير في المعاملات الإلكترونية أو تعديل النصوص القديمة. على أن يكون نص المادة 68 من هذا القانون و المتعلق بتجريم الخداع الإلكتروني على النحو التالي " يعاقب ... ، كل من يخدع أو يحاول أن يخدع المستهلك بأية وسيلة أو طريقة كانت حتى في المعاملات التي تتم عبر وسائل الاتصال عن بعد حول:

*كمية المنتوج المسلمة.

*تسليم المنتوجات غير تلك المعلنة مسبقا.

*قابلية استعمال المنتوج.

*تاريخ أو مدة صلاحية المنتوج.

*النتائج المنتظرة من المنتوج.

*طرق الاستعمال أو الاحتياطات اللازمة لاستعمال المنتوج.

*طرق دفع ثمن المنتوج أو مقابل الخدمة، أو طريقة التسليم إذا كانت المعاملة تتم عن طريق وسيط إلكتروني".

أو إحداث نص جديد في قانون التجارة الإلكترونية ينص على " دون الإخلال بأية عقوبة أشد يعاقب بغرامة من 10.000دج إلى 100.000دج كل من استغل ضعف أو جهل المتعاقد في إطار المعاملات التجارية الإلكترونية، بغرض دفعه للالتزام حاضرا أو آجلا بأي شكل من الأشكال، و ذلك إذا كان هذا المتعاقد غير قادر على إدراك آثار التزامه أو إذا أثبت انه تحت إكراه ما...".

خامسا: ضرورة تعديل نصوص قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين ليشمل جريمة تزوير التوقيع الإلكتروني و استعمال توقيع إلكتروني موزر، لأن المشرع اعترف بجميع أنواع التوقيعات في الإثبات من خلال المادة 10 منه.

سادسا: ضورة تعديل نصوص التزوير المنصوص عليها في قانون العقوبات لتشمل المحررات الإلكترونية أو إدراج نص جديد في قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين ينص صراحة على تزوير المحررات و العقود الإلكترونية و شهادة التصديق الإلكتروني.

سابعا: إنشاء لجنة مختصة تتولى دراسة ظاهرة الإجرام المعلوماتي بكافة جوانبها، و تعمل على صياغة التعديلات اللازمة.

ثامنا: إنشاء قضاء متخصص للنظر في الجرائم الإلكترونية بصورة عامة بما فيها الماسة بالمستهلك الإلكتروني، و ذلك لصعوبة كشفها و إثباتها و التحقيق فيها، و احتياجها لمعطيات خاصة لا تتوافر في القضاء العادي.

تاسعا: تعزيز التعاون و التنسيق الدولي بين الدول العربية مع بعضها البعض، و بينها و بين باقي الدول خاصة في مجال المساعدة القضائية الدولية و تسليم المجرمين، و العمل على دراسة و متابعة المستجدات على الساحة العالمية خاصة فيما يتعلق بجرائم المعاملات التجارية الإلكترونية.

عاشرا: لإسراع بالانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الأنترنت، خاصة المعاهدات الدولية لمكافحة جرائم المعلومات و الأنترنت.

حادي عشر: توسيع الاختصاص الزماني للجرائم الإلكترونية عامة بما فيها الماسة بالمستهلك الإلكتروني، حيث يتم حساب مدة التقادم من يوم الاكتشاف، و ليس من يوم وقوع الجريمة، و هذا نظرا لخطورتها و إمكانية وقوعها عن بعد و صعوبة اكتشافها و سرعة حدوثها .

"**تمت بحمد الله و فضله**"

"**و آخر دعوانا أن الحمد الله رب العالمين**"

قائمة المصادر و المراجع

أولا: قائمة المصادر

أ-القوانين و التشريعات

1-القوانين الوطنية

- اتفاقية فيانا 15 أفريل 1961 و 24 أفريل 1963 التي صادقت عليها الجزائر بموجب المرسوم رقم 84/64 المؤرخ في 04 مارس 1964، الجريدة الرسمية الجزائر رقم 29 لسنة 1964.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بتاريخ 21 ديسمبر 2010، المصادق عليها بالمرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، جريدة رسمية، عدد 57، الصادرة في 28 سبتمبر 2014.

- الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل و المتمم.

- الأمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966، المتضمن قانون العقوبات، المعدل و المتمم.

- الأمر رقم 71 - 28 المؤرخ في 26 صفر عام 1391 الموافق لـ 22 أفريل 1971 المتضمن قانون القضاء العسكري، الجريدة الرسمية، عدد 38 المؤرخة في 16 ربيع الأول عام 1391 الموافق لـ 11 مايو سنة 1971.

- القانون رقم 04-02 المؤرخ في 23 جوان 2004، المتعلق بالقواعد المطبقة على الممارسات التجارية، جريدة رسمية، عدد 41، الصادر بتاريخ 27 جوان 2004، المعدل و المتمم.

-القانون رقم 09-03 المؤرخ بتاريخ 25 فيفري 2009، جريدة رسمية، عدد 59، صادرة بتاريخ 08 مارس 2009، المعدل و المتمم.

- قانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الاتصال و مكافحتها، جريدة رسمية، عدد 47، الصادرة في 16 أوت سنة 2009.

- القانون رقم 14-04 ، المؤرخ في 24 فيفري 2014، المتعلق بالنشاط السمعي البصري، جريدة رسمية، عدد 16 الصادرة بتاريخ 16 مارس 2014.

- القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق 1 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، جريدة رسمية، عدد 06، الصادرة بتاريخ 10 فبراير 2015.

- قانون 15-12 المؤرخ في 15 يوليو 2015 المتعلق بحماية الطفل الجزائري، جريدة رسمية ، عدد 39، الصادرة في 20 يوليوا 2015.

- قانون رقم 18-05 مؤرخ في 10 مايو سنة 2018، يتعلق بالتجارة الإلكترونية، جريدة رسمية، عدد 28، صادرة في 16 مايوا 2018.

- قانون رقم 18-07 مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية، عدد 34، الصادرة في 10 يونيو 2018.

- مرسوم تنفيذي رقم 13-378 مؤرخ في 9 نوفمبر سنة 2013، يحدد الشروط و الكيفيات المتعلقة بإعلام المستهلك، جريدة رسمية، عدد 58، صادرة في 18 نوفمبر سنة 2013.

- مرسوم تنفيذي رقم 13-327 مؤرخ في 26 سبتمبر 2013، يحدد شروط و كيفيات وضع ضمان للسلع و الخدمات حيز التنفيذ، ج ريدة رسمية، عدد 49، صادرة في 2 أكتوبر 2013.

- مرسوم تنفيذي رقم 12-203 مؤرخ في 14 جمادى الثاني عام 1433 الموافق 6 مايو سنة 2012، يتعلق بالقواعد المطبقة في مجال أمن المنتوجات، جريدة رسمية، العدد 28، الصادرة في 9 مايو سنة 2012.

2-القوانين الأجنبية

- الاتفاقية الأوربية لحقوق الإنسان و الحريات الأساسية لسنة 1950.

- اتفاقية بودابست للإجرام المعلوماتي لسنة 2001.

- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليلي التشريع، منشورات الأمم المتحدة، 2000. متوفر على الموقع: http://www.uncitral.org/uncitral/ar

- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001. متوفر على الموقع: http://www.uncitral.org/uncitral/ar

- التوجيه الأوروربي رقم 95/46 الصادر في 24 أكتوبر 1995 الخاص بحماية الأشخاص في مواجهة المعالجة الآلية للمعطيات ذات الطابع الشخصي. متوفر على الموقع:www.books.dz

- القانون 40 لسنة 1998 المتعلق بطرح البيع و الإشهار التجاري التونسي. متاح على الموقع:www.aradous-aca.com

- القانون التونسي الخاص بالمبادلات و التجارة الإلكترونية رقم 83 لسنة 2000. متاح على الموقع: www.aradous-aca.com

- قانون رقم 15 لسنة 2004 بشأن التوقيع الإلكتروني المصري. متاح على الموقع : www.ar.jurispedia.org/index.ph

- اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، متاحة على الموقع:

www.ar.jurispedia.org/index.ph

--Directive 97/7/CE du 20 mai 1997 sur la protection des consommateurs en matière de contrats à distance, Journal Officiel des Communautés Européennes, N° L 144/19 , 04/06/1997 .

-directive 2000/31/ce du parlement européen et du conseil du 08 juin 2000 relative à certains aspects juridiques des services de la société de l'information ,et notamment du commerce électronique ,dans le marché intérieur « directive sur le commerce électronique » , Journal Officiel des Communautés Européennes , L178, 17/07/2000.

-Loi n°2000-230 du 30 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique , journal officiel Français n°62 du 14 mars 2000.

-Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique , Journal Officiel Français N°134 du 22 juin 2004.

-code de la consommation, version consolidée du code au 24/02/2014

ب-المعاجم

- قاموس المحيط للفيروز أبادي، دار الجليل، بيروت، الجزء الثاني، دون سنة نشر.
- المعجم الوسيط، الطبعة الرابعة، مكتبة الشروق الدولية، القاهرة، 2004.

ثانيا: قائمة المراجع

أ-المراجع باللغة العربية

1-الكتب

***الكتب العامة**

1- إبراهيم أحمد عبد الرحيم الشرقاوي، النظرية العامة للجريمة العسكرية، المكتب الجامعي الحديث، دون طبعة الإسكندرية، جمهورية مصر العربية، 2007.

2- د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، الطبعة الخامسة، ديوان المطبوعات الجامعية، بن عكنون ، الجزائر، 2010.

3- د. أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثالث، ديوان المطبوعات الجامعية، دون طبعة، بن عكنون، الجزائر، 1998.

4- د. احمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، الطبعة السابعة، 1993.

5- د. جندي عبد المالك، الموسوعة الجنائية، الجزء الأول، دار المؤلفات القانونية، بيروت لبنان، 1931.

6- د. جيلالي بغدادي، الاجتهاد القضائي في المواد الجزائية، الجزء الأول، الديوان الوطني للأشغال التربوية، الجزائر ، 2002.

7- د. جيلالي بغدادي، التحقيق دراسة مقارنة نظرية و تطبيقية، الديوان الوطني للأشغال التربوية، الجزائر، 1999.

8- حمدي رجب عطية ، الإجراءات الجنائية بشأن الأحداث في التشريعيين الليبي والمصري في ضوء الأفاق الجديدة للعدالة الجنائية في مجال الأحداث، دار النهضة العربية، دون طبعة، القاهرة، 1999.

9- دمدوم كمال، القضاء العسكري والنصوص المكملة له، دار الهدى، الطبعة الثانية، عين مليلة، الجزائر، 2004.

10- د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الفكر العربي، مصر 2006.

11- رمسيس بنهام، قانون العقوبات (النظرية العامة للقانون الجنائي)، الطبعة الثالثة، منشأ المعارف، الإسكندرية، 1997.

12- د. زهير الزبيدي، الاختصاص الجنائي الدولي في القانون الدولي، دون دار نشر، دون بلد نشر، 1980.

13- سليمان عبد المنعم، نظرية الجزاء الجنائي، المؤسسة الجامعية للدراسات و النشر و التوزيع، بيروت، 1999.

14- د. عبد الله اوهايبية، شرح قانون العقوبات الجزائري، دار هومة، بوزريعة، الجزائر، 2006.

15- صلاح الدين جبار، القضاء العسكري في التشريع الجزائري والقانون المقارن، الطبعة الأولى، دار الخلدونية، ، الجزائر، 2010.

16- عبد المجيد جباري، دراسات قانونية في المادة الجزائية، على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر 2012.

17- مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، الجزء الثاني، دار الفكر الجامعي، مصر، 1988.

18- محمد الأمين البشري و محسن عبد الحميد احمد، معايير الأمم المتحدة في مجال العدالة الجنائية و منع الجريمة، الطبعة الأولى، الأكاديميون للنشر و التوزيع، عمان، 2014.

19- د. محمد جمال الدين زكي، مشكلات المسؤولية المدنية، الجزءالأول، طبعة أولى، جامعة القاهرة، 1999.

20- د. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2008.

21- د. محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة العاشرة، دار هومة، الجزائر، 2015.

22- د. محمد زكي أبو عامر، قانون العقوبات القسم العام، دار الجامعة الجديدة للنشر، الإسكندرية، 2015.

23- محمد سعيد نمور، أصول الإجراءات الجزائية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2005.

24- محمد شكري سرور، مسؤولية المنتج عن الأضرار التي تسببها منتوجاته الخطيرة، الطبعة الثالثة، دار الفكر العربي، القاهرة، ، 1983.

25- محمد لبيب شنب و مجدي صبحي خليل، شرح أحكام عقد البيع، دار النهضة العربية، القاهرة، 1968.

26- د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفق أحدث التعديلات التشريعية، الجزء الأول، دار النهضة العربية، القاهرة 2013.

27- د. محمود نجيب حسني، شرح قانون الإجراءات الجزائية وفقا لأحدث التعديلات، الجزء الثاني، دار النهضة العربية، القاهرة، 2013.

28- د. محمود نجيب حسني، شرح قانون العقوبات القسم العام، المجلد الأول، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت. دون تاريخ نشر.

29- مدحت محمد عبد العزيز إبراهيم، القواعد العامة في مسائل الاختصاص لمأموري الضبط القضائي و أعضاء النيابة العامة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2014.

30- مروك نصر الدين، النظرية العامة للإثبات الجنائي، الجزء الأول، ، دار هومة، الجزائر، 2010.

31- مصطفى العوجي، القانون الجنائي، منشورات الحلبي الحقوقية، بيروت لبنان، 2006.

32- نظام توفيق المجاني، شرح قانون العقوبات القسم العام، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2009.

***الكتب المتخصصة**

1- د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، لجنة التأليف و التعريب، جامعة الكويت ،الكويت، 2003.

2- د. إبراهيم عيد نايل، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الفرنسي ، دار النهضة العربية، القاهرة، 2000.

3- أبو هبة نجوى، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2002.

4- د. أحمد محمد خلف، الحماية الجنائية للمستهلك، دراسة مقارنة، المكتبة العصرية للنشر و التوزيع، المنصورة، مصر، 2008.

5- د. آزاد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2016.

6- د. أسامة أبو الحسن مجاهد، الوسيط في قانون المعاملات الإلكترونية، الكتاب الأول، دار النهضة العربية، القاهرة، 2007.

7- د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الأنترنت، دار النهضة العربية، مصر.2003.

8- أسامة أحمد المناعسة، صايل فاضل الهواوشة، جرائم الحاسب الآلي و الإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر، 2001.

9- د/ أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني ، دراسة مقارنة، دار الكتب القانونية، مصر، 2008.

10- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة و بنوك المعلومات، دار النهضة العربية، القاهرة، 1988.

11- أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2016 .

12- البريزات محمد، الجريمة المنظمة، الطبعة الأولى، دار الثقافة، عمان، 2008.

13- د. السيد عتيق، جرائم الأنترنت، دار النهضة العربية، القاهرة، مصر، 2002.

14- السيد محمد السيد عمران، الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الأنترنت، الدار الجامعية بيروت، 2006.

15- السيد محمد السيد عمران، حماية المستهلك أثناء تكوين العقد، دار الجامعة الجديدة للنشر، الإسكندرية، 2003.

16- الفاضل محمد، التعاون الدولي لمكافحة الإجرام، مطبعة المفيد الجديدة، دون بلد نشر، 1967.

17- أنور محمد صدقي المساعدة، المسؤولية الجزائية عن الجرائم الاقتصادية، الطبعة الاولى، دار الثقافة للنشر و التوزيع ، عمان، 2007.

18- أنيس حسيب السيد المحلاوى، الخبرة القضائية في الجرائم المعلوماتية و الرقمية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2016.

19- أيمن عبد الله فكرى، الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية و الأجنبية، الطبعة الأولى، مكتبة القانون و الاقتصاد، الرياض، السعودية، 2015.

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

21- د. تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الأنترنت، دراسة مقارنة، الطبعة الأولى، بهجات للطباعة، دون بلد نشر، 2009.

22- ثروت عبد الحميد، التوقيع الإلكتروني، دار النيل للطباعة و النشر، المنصورة، مصر، 2001.

23- جميعي حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الأنترنت، دار النهضة العربية، القاهرة، 2000.

24- جميل عبد الباقي الصغير، الإنترنت و القانون الجنائي، دار النهضة العربية، مصر، 2002.

25- د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2002.

26- حسن عبد الباسط جميعي، حماية المستهلك (الحماية الخاصة لرضا المستهلك في عقود الاستهلاك) دار النهضة العربية، القاهرة، 1996.

27- حسن فتحي الحامولي، التعاون الدولي الأمني في تنفيذ الأحكام الجزائية، دون دار نشر، دون بلد نشر، 2015.

28-حمادة مصطفى عزب، الجوانب القانونية للإعلان عن المنتجات و الخدمات عبر الإنترنت، دار النهضة العربية، مصر، دون تاريخ نشر.

29- حمزة سالم، التعاون الدولي في تنفيذ الأحكام الجنائية الأجنبية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2003.

30- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية (دراسة مقارنة)، الطبعة الأولى،منشورات الحلبي الحقوقية، لبنان، 2014.

31- د. خالد جمال احمد حسن، الالتزام بالإعلام قبل التعاقد، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

32- د. خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الإنترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع، ، 2011.

33- د. خالد ممدوح إبراهيم، التقاضي الإلكتروني و إجراءاتها أمام المحاكم، الطبعة الأولى ، دار الفكر الجامعي، مصر، 2008.

34- د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009.

35- د. خالد ممدوح إبراهيم، العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2005.

36- د. خالد ممدوح إبراهيم، أمن المستهلك الإلكتروني، الدار الجامعية، الإسكندرية، مصر، 2008.

37- د. خالد ممدوح إبراهيم، حماية المستهلك في التعاملات الإلكترونية، الدار الجامعية، الإسكندرية، مصر، 2008.

38- د/ خالد ممدوح إبراهيم، حماية المستهلك في العقد الإلكتروني، الطبعة الأولى ، دار الفكر الجامعي، الإسكندرية، 2008.

39- د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

40- دوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الحاسوب الآلي و الإنترنت، دار الكتاب القانونية، مصر.2008.

41- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012.

42- د. رمزي بيد الله على الحجازي، الحماية المدنية للمستهلك بعد التعاقد الإلكتروني، منشورات الحلبي الحقوقية، لبنان، 2006.

43- د. روسطم عطية موسى نو، الحماية الجنائية للمستهلك من الغش في مجال المعاملات التجارية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2014.

45- د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية دراسة مقارنة، دار الكتب القانونية، مصر، 2011.

46- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

47- سليمان إبراهيم مصطفى، الإرهاب و الجريمة المنظمة، دار الطلائع، القاهرة، 2006.

48- د. سليمان احمد فضل، المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007.

49- سليم عبد الله الخيوري، الحماية القانونية لمعلومات شبكة الأنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2011.

50- سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دار الجامعة الجديدة، الإسكندرية، 2007.

51- شريف محمد غنام النظام القانوني للإعلانات عبر شبكة الأنترنت، دار الجامعة الجديدة ، الإسكندرية، مصر، 2008.

52- شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.

53- صابر عبد العزيز سلامة، العقد الإلكتروني، ط2، دار النهضة العربية، القاهرة، مصر، 2007.

54- عائشة بن قادة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي (دراسة مقارنة بين التشريع الجزائري و القانون المقارن)، دار الجامعة الجديدة، الإسكندرية، 2010.

55- د. عادل عبد العال إبراهيم خراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية و سبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015.

56- عادل يحيى، التعاون الدولي في تنفيذ الأحكام الأجنبية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2004.

57- عامر قاسم أحمد القيسي، الحماية القانونية للمستهلك، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2002.

58- د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية و حمايتها القانونية، الكتاب الثاني، دار الكتب القانونية، مصر، 2007.

59- د. عبد الفتاح بيومي حجازي، التجارة عبر الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008.

60- د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظام القانوني المقارن، دار الفكر الجامعي، الإسكندرية، 2005.

61- د. عبد الفتاح بيومي حجاز، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، مصر، 2009.

62 - د. عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2004.

63- د. عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الإلكترونية، الكتاب الثني، الحماية الجنائية للتجارة الإلكترونية، دار الفكر العربي، مصر، 2002.

64- د. عبد الفتاح بيومي حجاز، جرائم الكمبيوتر و الأنترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية 2006.

65- د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

66- د. عبد الفتاح بيومي حجازي، مقدمة في التجارة العربية ، المجلد الأول، دار الفكر الجامعي، الإسكندرية، 2003.

67- د. عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، المجلد الثاني، دار الفكر الجامعي، 2004.

68- د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر في القانون العربي النموذجي، الطبعة الاولى، دار الفكر الجامعي، 2006.

69- عبد الفضيل محمد أحمد، الإعلان عن المنتجات و الخدمات من الوجه القانوني، مكتبة الجلاء الجديدة، بدون تاريخ نشر.

70- د. عبد المنعم موسى إبراهيم، حماية المستهلك ، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

70- عبد الله على محمود، حماية المستهلك من الغش التجاري و الصناعي، دار النهضة الغربية، القاهرة، 2002.

71- د. عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني ، دار النهضة العربية، القاهرة، بدون تاريخ نشر.

72- عفيف كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت، 2003.

73- عفيف كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون دراسة مقارنة، منشأة المعارف الإسكندرية، 2010.

74- عكاشة محمد عبد العال، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، دار الجامعة الجديدة، الإسكندرية، 2007.

75- علاء عمر محمد الجاف، الآليات القانونية لحماية المستهلك في التعاملات الإلكترونية، منشورات الحلبي الحقوقية، لبنان، 2017.

76- علي حسن محمد الطوالبة، التفتيش الجنائي علم نظام الحاسوب و الأنترنت دراسة مقارنة، عالم الكتب الحديث، الأردن، 2004.

77- علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، الدار الجامعية للطباعة و النشر، بيروت، 1999.

78- علي عدنان الفيل، إجراءات التحري و التحقيق الابتدائي في الجريمة المعلوماتية ، المكتب الجامعي الحديث، الإسكندرية، 2012.

79- علي محمود أبوا العز، التجارة الإلكترونية و أحكامها في الفقه الإسلامي، الطبعة الأولى ، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2008.

80- عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، دون دار نشر، دون بلد نشر، 2005.

81- عمر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004.

82- د. عمر خالد رزيقات، عقد البيع عبر الأنترنت، دراسة تحليلية، الطبعة الأولى، دار الحامد للنشر، عمان، الأردن، 2007.

83- عيسى غسان ربضي، القواعد الخاصة للتوقيع الإلكتروني، دار الثقافة للنشر و التوزيع، عمان، 2012.

84- فاروق إبراهيم جاسم، الجوانب القانونية للتجارة الإلكترونية، دار السنهوري، بيروت، 2016.

85- د. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الادلة، الطبعة الاولى، مكتبة دار الثقافة، عمان 1999.

86-كوثر سعيد عدنان خالد، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الإسكندرية مصر، 2016.

87- محمد إبراهيم أبوا الهجاء، عقود التجارة الإلكترونية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2005.

88- د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

89- د. محمد بودالي، حماية المستهلك في القانون المقارن، دراسة مقارنة، دار الكتب الحديثة، مصر، 2006.

90- د. محمد بودالي، شرح جرائم الغش في بيع السلع و التدليس في المواد الغذائية و الطبية، دار الفجر للنشر و التوزيع ، القاهرة، 2005.

91- د/محمد خالد جمال رستم، التنظيم القانوني للتجارة الإلكترونية و الإثبات الإلكتروني في العالم، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006.

92- محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1998.

93- محمد عبيد كعبي، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، دون سنة نشر.

94- د. محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2011.

95- د. محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية، دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر عمان الأردن، 2006.

96- د. محمد مرسي زهرة، الحماية المدنية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2008.

97- د. محمد محمد المهدي ، تكنلوجيا المعلومات و تطبيقاتها، طبعة أولى، دار الشروق، سنة 1989.

98- محمد محمد سادات ، خصوصية التوقيع الإلكتروني، دراسة مقارنة، دار الفكر و القانون للنشر و التوزيع، المنصورة، مصر، 2011.

99- محمود إبراهيم غازي، الحماية الجنائية للخصوصية و التجارة الإلكترونية ، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014.

100- د. محمود محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، الجزء الأول، مطبعة جامعة القاهرة و الكتب الجامعية، 1979.

101- مدحت رمضان عبد الحليم، جرائم الاعتداء على الأشخاص و الأنترنت، دار النهضة العربية، القاهرة، 2000.

102- مريم بن خليفة، التسويق الإلكتروني و آليات حماية المستهلك، دار الفكر و القانون، مصر، 2017.

103- مشيمش ضياء أمين، التوقيع الإلكتروني، المنشورات الحقوقية، بيروت، 2003.

104- د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشركة، القاهرة، 2009.

105- مصطفى موسى العطيات، الجوانب القانونية لتعاملات التجارة الإلكترونية، دار وائل للنشر و التوزيع، عمان، الأردن، 2010.

106- منير محمد الجنيهي، ممدوح محمد الجنيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

107- د. نبيل احمد صبيح، حماية المستهلك في التعاملات الإلكترونية، الدار الجامعية، بيروت، 2008.

108- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.

109- هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دراسة مقارنة، دار الكتب القانونية، مصر، 2015.

110- د. هدى عبد الله، النظام القانوني للفترة السابقة للتعاقد، دراسة مقارنة، المنشورات الحقوقية، بيروت، لبنان، 2004.

111- هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، مصر، 2005.

112- هشام فريد رستم، الجوانب الإجرائية للجرائم الإلكترونية، مكتبة الحلات الحديثة، 1994.

113- د. هلالي عبد الله احمد، إتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، 2007.

114- د. هلال عبد الله أحمد، حجية محررات الكمبيوتر في المواد الجزائية، دار النهضة العربية، القاهرة، 2006.

115- هشام محمد فريد رستم، قانون العقوبات و مخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، دون سنة نشر.

2- الرسائل و المذكرات الجامعية

*** رسائل الدكتوراه**

1- أجعود سعاد، حماية حق المتهم في محاكمة عادلة في التشريع الجزائي الجزائري، أطروحة دكتوراه، كلية الحقوق، جامعة عنابة، الجزائر، 2016.

2- أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، رسالة دكتوراه ، كلية الحقوق، جامعة القاهرة، مصر، 1959.

3- إلهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية، أطروحة دكتوراه، كلية الحقوق و العلوم السياسي، جامعة باتنة، الجزائر، 2016.

4- أمال عثمان، الخبرة في المسائل الجنائية ، رسالة دكتوراه، كلية الحقوق ، جامعة القاهرة، مصر، 1964.

5- بوجمعة لطفي، الإجراءات الخاصة لمكافحة الجريمة الإرهابية، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة عنابة، الجزائر، 2016.

6- حابت أمال، التجارة الإلكترونية في الجزائر، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، الجزائر، 2015.

7- خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2012.

8- خميخم محمد، الحماية الجنائية للمستهلك في عقود التجارة الإلكترونية، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2017.

9- زوبة سميرة، الأحكام القانونية المستحدثة لحماية المستهلك المتعاقد، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو ، الجزائر، 2016.

10- زوليخة تيجاني، نظام الإجراءات أمام محكمة الجنايات، أطروحة دكتوراه، كلية الحقوق، بن عكنون، جامعة بن يوسف بن خدة الجزائر 1، 2013.

11- سيف ابغازي ، السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراه، جامعة القاهرة، مصر.

12- عادل بوزيدة، المسؤولية الجزائية لمتعهدي الإيواء، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تبسة، الجزائر، 2018.

13 - عبد الحليم بوقرين، الحماية الجنائية للمعاملات التجارية، رسالة دكتوراه، جامعة تلمسان، الجزائر، 2014.

14- على حساني، الاطار القانوني لالتزام بالضمان في المنتوجات، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان ، الجزائر، 2012.

15- لعجال لامية، حماية المستهلك في معاملات التجارة الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر، 2016.

16- محمد شرايرية، الحماية الجنائية للمستهلك، مذكرة دكتوراه، كلية الحقوق و العلوم السياسية، جامع عنابة، الجزائر،2011.

17- محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية- دراسة مقارنة- رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2009.

18- معزوز دليلة، الضمان في عقود البيع الكلاسيكي و الإلكتروني، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، الجزائر، 2014.

19- هروال هبة نبيلة، جرائم الأنترنت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، 2014.

*** مذكرات الماجستير**

1- بن زايد نسرين، حماية المستهلك من خلال الالتزام بالضمان، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2015.

2- حمودي ناصر، الحماية الجنائية للتجارة الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2015.

3- ذنايب آسية، الآليات الدولية لمكافحة الجريمة المنظمة عبر الوطنية، مذكرة ماجستير، كلية الحقوق و العلوم السياسية ، جامعة قسنطينة، الجزائي، 2010.

4- سامي بلعابد، ضمان المحترف لعيوب منتجاته، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة قسنطينة، الجزائر، 2005.

5- سامي على حامد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

6- سعيداني نعيم، آليات البحث و التحري عن الجرائم المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق و العلوم السياسية، جامعة باتنة، الجزائر، 2013.

7- سوالمي أحمد، الحماية الجنائية من الدعاية التجارية الكاذبة، رسالة ماجستير، كلية الحقوق، جامعة الجزائر1، 2014.

8- لالوش راضية، أمن التوقيع الإلكتروني، مذكرة ماجستير في القانون العام ، كلية الحقوق ، جامعة مولود معمري ، تيزي وزو،2012.

9- لملوم كريم، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية و الدولية، رسالة ماجستير، جامعة تيزي وزو، الجزائر، 2011.

10- ناصر محمد الصقير، الحماية الجنائية للمستهلك من الغش التجاري، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2016.

11- هدى طلب على، الإثبات الجنائي في جرائم الأنترنت و الاختصاص القضائي بها، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2012.

3- المقالات و البحوث العلمية

***المقالات**

1- بلحسني حمزة ،الحماية القانونية و الفنية للتوقيع الإلكتروني في مجال البيئة الرقمية، مجلة العلوم القانونية و الإدارية ، العدد الحادي عشر،2015.

2- جبيري ياسين، الحماية الجنائية للتصديق و التوقيع الإلكتروني –دراسة مقارنة، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، العدد 01، المجلد 32، 2018.

3-خليفي مريم، "الالتزام بالإعلام الإلكتروني و شفافية التعامل في مجال التجارة الإلكترونية"، مجلة دفاتر السياسة و القانون، العدد الرابع، 2011.

4- خليفي مريم، الحماية الجنائية لمواقع التجارة الإلكترونية، مجلة العلوم القانونية، عدد 2، 2011.

5- د. دريس كمال فتحي، آلية التصديق الإلكتروني كضمانة للتعاملات التجارية بالوسائل الحديثة ، مجلة البحوث و الدراسات، العدد 24، 2017.

6- دمانة محمد، الإشهار الإلكتروني التجاري و المستهلك، مجلة الفكر، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، العدد 17، جوان 2018، ص 292.

7- راضية عيمور، "الحماية الجنائية للمعاملات الإلكترونية، مجلة الدراسات القانونية و السياسية"، العدد01.

8- زهيرة كيسي، "النظام القانوني لجهات التوثيق الإلكتروني"، مجلة دفاتر السياسة و القانون، العدد السابع، 2012.

9- شنين صالح، الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، كلية الحقوق، جامعة عبد الرحمان ميرة، بجاية، ع01، 2010.

10- رامي عبد الحليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجموعة أعمال الملتقى الدولي حول التنظيم القانوني للأنترنت و الجريمة الإلكترونية، مجلة دراسات و أبحاث جامعة زيان عاشور الجلفة، ع1، 2009.

11- رمزي النويصر، التعاون الدولي في مجال مكافحة جرائم الإنترنت، مجلة القضاء و التشريع، العدد08، تونس،2011.

12- عزيزة لرقط، الحماية الجنائية للتوقيع و التصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية و الاقتصادية، المركز الجامعي لتامنغست، الجزائر، العدد 11، 2017.

13- د.غازي خالد أبوا عرابي، الالتزام بالإعلام قبل التعاقد عبر شبكة الأنترنت، مجلة علوم الشريعة و القانون، المجلد الرابع و الثلاثون، الجامعة الأردنية، 2007.

14- غازي خالد أبو عرابي، حماية رضا المستهلك، دراسة مقارنة في قانون حماية المستهلك الإماراتي و تقنين الاستهلاك الفرنسي و مشروع قانون حماية المستهلك الأردني، مجلة دراسات علوم الشريعة و القانون الأردنية، العدد الأول، 2009.

15- غزيوي هندة، المسؤولية الجزائية للشركات التجارية عن جرائم الغش التجاري ، مجلة التواصل في الاقتصاد و الإدارة و القانون، ع 39، سبتمبر، 2014.

16-فوزي أوصديق، إشكالية المعلومات بين الخصوصية و إفشاء الأسرار المهنية، مجلة دراسات قانونية، مركز البصيرة للبحوث و الدراسات و الخدامات التعليمية، الجزائر، العدد 12، 2008.

17- محمد حاجة بن علي، مسؤولية المحترف عن أضرار و مخاطر تطور منتجاته المعيبة، مجلة الأكاديمية للدراسات الاجتماعية و الإنسانية ، عدد 02، جامعة حسيبة ين بو على، الشلف، 2009.

18- محمد على سالم و حسون عبيد هجيج، البطاقة الائتمانية و الأساس القانوني لحمايتها من التزوير، مجلة المحقق المحلي للعلوم القانونية و السياسية، عدد2، 2015.

19- محمد محمد، السلطة التقديرية للقاضي الجنائي، مجلة البحوث، المركز الجامعي بالوادي، العدد الأول، 2004.

20- مصطفى هنشور وسيمة، النظام القانوني للتوقيع الإلكتروني في التشريع الجزائري، مجلة الحقوق و العلوم الإنسانية ، كلية الحقوق و العلوم السياسية، جامعة مستغانم، العدد 24 المجلد الثاني.

21- كراشي ليلى، حماية رضا المستهلك في ظل قواعد حماية المستهلك، حوليات جامعة الجزائر، العدد 31، الجزء الرابع.

22- د. نادر شافي، التوقيع الإلكتروني، الاعتراف التشريعي و تعريفه، مقال منشور في مجلة الجيش اللبناني، العدد 239 في 2006/3/1.

*الاعمال العلمية

1-طارق محمد الجملي، الدليل الرقمي في الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية و القانون، المنعقد في 28-2009/10/29 ، الأكادمية للدراسات العليا طرابلس.

2- عبد الناصر محمود فرغلي، ود/ عبيد سيف عبيد المسماري، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية، دراسة تطبيقية مقارنة، الرياض ، المنعقدة في الفترة 12-2007/11/14.

3-علي حمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل ، المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية، دبي، 2003.

4- علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون و الكمبيوتر و الأنترنت، كلية الشريعة و القانون، جامعة الإمارات، مايو 2000.

5- عمر بن يونسي، مذكرات في الإثبات الجنائي عبر الأنترنت، ندوة الدليل الرقمي، بمقر جامعة الدول العربية في الفترة بين 5-2005/03/8.

ب-المراجع باللغة الأجنبية

1-الكتب:

1- André lucas. Jean Deveze et Jean Freyssinet. Droit de l'informatique et de l'internet. Presses universditaires de France. Paris 2001.

2- Alain BENSOUSSAN: Le commerce électronique: aspects juridiques, Editions Hermès, Paris 1998.

3-BOCHURERG Laudon : internet et commerce électronique. Ed encvclopédie . DELMAS. 1999.

4- BRIGITTE HESS-FALLON et SIMON ANNE-MARIE. Droit commercial et des affaires. 9 édition. sirey. 1995.

5- CALAIS-AULOY: droit de la consommation. Ed dalloz. 5 éd. 2000.

6- Christiane féral-schuhl: Cyber droit. Le a l'épreuve de l'internet. 2éme éd 2000. Dalloz. Dunod.

7- Michel Bibent. Le droit du tratement de l'informatique. Nathany/HER.Paris.2000.

8- NATHALIE RZEPECKI. Droit de la consommation et théorie général du contrat. Presses universitaires d 'aix-marseille. 2002.

9-Naughan Bevan and Ken Lidstone- Aguide to the police and criminal evidence act 1984-Bujterworth- London 1985.

10- PIERRE Kayser. La protection de la vie privée par le droit. Protection du secret de la vie privée. Economica marseille.1995.

11-Thierry Piette-Coudol et André Bertrand. Internet et la loi. Ed. dalloz. Paris 1997.

12- Verbiest Thibault. la protection juridique cyber-consommateur. Litec. 2002.

13- Verbiest Thibault. commerce èlectronique : le nouveau cadre juridque . LARCIER . 2004.

14- Verbiest Thibault et Etienne Wery. Le droit de l'internet et de la société de l'informatique. Droit européen. Belge et francais. Lacier. Bruxelles. Belgique. 2001.

15- YVED PICOD ET Héléne DAVO: droit de la consommation. Eition armand COLIN .belgique. 2005.

2-المذكرات:

1- Lama Akouche , La Loi Applicable Aux Contrats , Diplôme D'études Approfondies , Droit Interne et
International Des Affairés ; Faculté de Droit et Des Sciences , Université Libanaise , Beyrouth,.2005.

3-المقالات:

1-A RIANE Mole: « le nouveau droit des flux transfrontières des données personnelles »revde. Soc.n12 déc.2004.

2- Combaldieu Raoul: La fraude en matiére alimentaire. Revue internationale de droit compare. Vol 26. N3. Juilley. 1974 .

3-janinie revel." La coexistence du droit commun de la loi relative a la responsabilité du fait des produits défectueux. Droit de la responsabilité et responsabilités des entreprise".REVUE TRIMESTRIELLE DE DROIT ECONOMIQUE.N 2 DALLOZ. 1999.

4- VARILLE larrieu : PUBLICITé sur internet. Droit et déontologie. Gaz-pal. Vendredi 21. Samedi 22 november 1997.

5-**Jérôme HUET**: La problématique juridique du commerce électronique, Colloque « Droit et Commerce », Deauville, 2000.

المواضيع	الصفحة
مقدمة	01
الباب الأول: الحماية الجزائية الموضوعية للمستهلك في المعاملات الإلكترونية	10
الفصل الأول: الحماية الجزائية الموضوعية للمستهلك من الغش التجاري في المعاملات الإلكترونية	11
المبحث الأول: الحماية الجزائية الموضوعية للمستهلك من الغش التجاري الإلكتروني في مرحلة ما قبل التعاقد الإلكتروني	12
المطلب الأول: الحماية الجنائية للمستهلك من الإشهار التجاري الإلكترونية غير المشروع.	14
الفرع الأول: ماهية الإشهار التجاري الإلكتروني	14
الفقرة الأولى: مفهوم الإشهار التجاري الإلكتروني	15
الفقرة الثانية: أشكال الإشهار التجاري الإلكتروني	21
الفرع الثاني: صور تجريم الإشهار التجاري الإلكتروني غير المشروع	24
الفقرة الأولى: جريمة مخالفة شروط الإشهار التجاري الإلكتروني	25
الفقرة الثانية: جريمة الإشهار التجاري الإلكتروني غير المرغوب فيه	35
المطلب الثاني: الحماية الجنائية لحق المستهلك في الإعلام الإلكتروني	42
الفرع الأول: ماهية الالتزام بالإعلام الإلكتروني	42
الفقرة الأولى: مفهوم الالتزام بالإعلام الإلكتروني.	43
الفقرة الثانية: مضمون الالتزام بالإعلام الإلكتروني	47
الفرع الثاني: صور التجريم الواقعة على حق المستهلك في الإعلام الإلكتروني	56
الفقرة الأولى: جريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني	56
الفقرة الثانية: جريمة مخالفة مراحل التعاقد الإلكتروني	62
المبحث الثاني: الحماية الجزائية الموضوعية للمستهلك من الغش التجاري في مرحلة التعاقد الإلكتروني	68
المطلب الأول: الحماية الجنائية لحق المستهلك في ضمان المنتوجات و أمنها في المعاملات الإلكترونية	69
الفرع الأول: جريمة مخالفة حق المستهلك في ضمان عيب المنتوجات في المعاملات	70

الإلكترونية	
الفقرة الأولى: الركن المادي لجريمة مخالفة حق المستهلك الإلكتروني في ضمان عيب المنتوجات	71
الفقرة الثانية: الركن المعنوي لجريمة مخالفة حق المستهلك الإلكتروني في ضمان عيب المنتوجات	80
الفرع الثاني: جريمة مخالفة حق المستهلك في ضمان أمن المنتوجات في المعاملات الإلكترونية	81
الفقرة الأولى: الركن المادي لجريمة مخالفة حق المستهلك الإلكتروني في ضمان أمن المنتوجات.	82
الفقرة الثانية: الركن المعنوي لجريمة مخالفة حق المستهلك الإلكتروني في ضمان امن المنتوجات و العقوبات المقررة لها	86
المطلب الثاني: الحماية الجنائية للمستهلك من الخداع و التزوير الصناعي في المعاملات الإلكترونية	90
الفرع الأول: جريمة خداع المستهلك في المعاملات الإلكترونية	90
الفقرة الأولى: الركن المادي لجريمة الخداع في المعاملات الإلكترونية	91
الفقرة الثانية: الركن المعنوي لجريمة الخداع في المعاملات الإلكترونية و العقوبة المقررة لها	95
الفرع الثاني: جريمة التزوير التجاري و الصناعي في المعاملات الإلكترونية	98
الفقرة الاولى: الركن المادي لجريمة التزوير التجاري و الصناعي في المعاملات الإلكترونية	99
الفقرة الثانية: الركن المعنوي لجريمة التزوير التجاري أو الصناعي في المعاملات الإلكترونية و العقوبة المقررة لها	104
الفصل الثاني: الحماية الجزائية الموضوعة لمتطلبات المستهلك في المعاملات الإلكترونية	106
المبحث الأول: الحماية الجزائية للبيانات الشخصية للمستهلك في المعاملات الإلكترونية	107
المطلب الأول: الجرائم المتعلقة بالجوانب الموضوعية لمعالجة البيانات الشخصية للمستهلك الإلكتروني	108
الفرع الأول: الجرائم المتعلقة بتسيير المعطيات الشخصية للمستهلك الإلكتروني	108
الفقرة الأولى: جريمة المعالجة غير المشروعة للمعطيات الشخصية للمستهلك الإلكتروني	109
الفقرة الثانية: جريمة الاستعمال غير المشروع للمعطيات الشخصية للمستهلك الإلكتروني	115

الفقرة الثالثة: جريمة تحويل المعطيات الشخصية للمستهلك الإلكتروني نحو الخارج	120
الفرع الثاني: الجرائم المتعلقة بحقوق المستهلك الإلكتروني	123
الفقرة الأولى: جريمة معالجة المعطيات الشخصية دون موافقة المستهلك الإلكتروني	123
الفقرة الثانية: جريمة مخالفة الحقوق الخاصة المستهلك الإلكتروني	131
المطلب الثاني: الجرائم الماسة بالقواعد الشكلية لمعالجة المعطيات الشخصية للمستهلك الإلكتروني	142
الفرع الأول: الجرائم المتعلقة بالشكليات المسبقة لمعالجة المعطيات الشخصية للمستهلك الإلكتروني	142
الفقرة الأولى: جريمة معالجة المعطيات الشخصية للمستهلك بدون تصريح أو ترخيص	143
الفقرة الثانية: جريمة التعامل في معطيات حساسة دون موافقة المستهلك الإلكتروني أو تكليف	151
الفرع الثاني: الجرائم المتعلقة بشكليات الحماية و التعاون مع اللجنة الوطنية	156
الفقرة الأولى: جريمة عدم اتخاذ تدابير حماية المعطيات الشخصية للمستهلك	157
الفقرة الثانية: جريمة عدم التعاون مع السلطة الوطنية	163
المبحث الثاني: الحماية الجزائية لتوقيع المستهلك في العاملات الإلكترونية	168
المطلب الأول: النظام القانوني للتوقيع المستهلك الإلكتروني	169
الفرع الأول: ماهية التوقيع الإلكتروني للمستهلك	169
الفقرة الأولى: مفهوم التوقيع الإلكتروني	170
الفقرة الثانية: الشروط الواجب توافرها في توقيع المستهلك الإلكتروني	177
الفرع الثاني: التصديق على توقيع المستهلك الإلكتروني	181
الفقرة الأولى: الجهة المختصة بالتصديق على التوقيع الإلكتروني	181
الفقرة الثانية: شهادة التصديق الإلكتروني	185
المطلب الثاني: صور الحماية الجنائية لتوقيع المستهلك الإلكتروني	189
الفرع الأول: الحماية المقررة لتوقيع المستهلك الإلكتروني في ظل قانون العقوبات	189
الفقرة الأولى: جريمة الدخول أو البقاء غير المشروع داخل نظام إنشاء توقيع إلكتروني	191
الفقرة الثانية: جريمة التلاعب في بيانات نظام إنشاء توقيع إلكتروني	197
الفرع الثاني: الحماية المقررة لتوقيع المستهلك الإلكتروني في ظل قانون 15-04 المتعلق بالتوقيع و التصديق الإلكترونيين	201
الفقرة الأولى: الجرائم المتعلقة بتأدية خدمات التصديق الإلكتروني	201

الفقرة الثانية: الجرائم المتعلقة ببيانات شهادة التصديق الإلكتروني	211
الفقرة الثالثة: الجرائم المتعلقة بالتوقيع الإلكتروني ذاته	215
الباب الثاني: الحماية الجزائية الإجرائية للمستهلك في المعاملات الإلكترونية	220
الفصل الأول: تنظيم قواعد الاختصاص في نظر الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	221
المبحث الأول: انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	222
المطلب الأول: قواعد الاختصاص القضائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	223
الفرع الأول: ضوابط انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني	223
الفقرة الأولى: مبادئ انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني	223
الفقرة الثانية: معايير انعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني	230
الفرع الثاني: تقييد الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني	238
الفقرة الأولى: القيود المتعلقة بالمركز القانوني لمرتكب الجرائم الماسة بالمستهلك الإلكتروني	238
الفقرة الثانية: القيود المتعلقة بالاختصاص الجزائي ذاته	241
المطلب الثاني: وسائل انعقاد الاختصاص الجزائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	242
الفرع الأول: الجهات القضائية المختصة بإنفاذ قواعد الاختصاص الجزائي في الجرائم الماسة بالمستهلك الإلكتروني	242
الفقرة الأولى: الجهات القضائية الجزائية العادية المختصة بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني	243
الفقرة الثانية: الجهات القضائية الاستثنائية بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني	245
الفرع الثاني: طرق إنفاذ الاختصاص القضائي في الجرائم الماسة بالمستهلك الإلكتروني	248
الفقرة الأولى: الطرق التقليدية بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني	248
الفقرة الثانية: الطرق المستحدثة بمتابعة مرتكبي الجرائم الماسة بالمستهلك الإلكتروني	250
المبحث الثاني: التعاون الدولي كألية لانعقاد الاختصاص لمواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	253

المطلب الأول: صور التعاون الدولي في تعزيز الاختصاص القضائي لمواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	254
الفرع الأول: المساعدة القضائية المتبادل لتعزيز الاختصاص القضائي في مواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	254
الفقرة الأولى: تبادل المعلومات بين الدول	256
الفقرة الثانية: نقل الإجراءات بين الدول	257
الفقرة الثالثة: الإنابة القضائية على المستوى الدولي	261
الفرع الثاني: تسليم المجرمين لتعزيز الاختصاص القضائي في مواجهة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	264
الفقرة الأولى: مفهوم تسليم المجرمين	264
الفقرة الثانية: شروط و إجراءات نظام تسليم المجرمين	269
المطلب الثاني: إشكاليات التعاون الدولي كآلية لانعقاد الاختصاص القضائي في الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	277
الفرع الأول: إشكاليات التعاون الدولي على المستوى الوطني في الجرائم الماسة بالمستهلك الإلكتروني	277
الفقرة الأولى: عدم كفاية و ملائمة التشريعات القائمة	277
الفقرة الثانية: اختلاف النظم القانونية الإجرائية	279
الفقرة الثالثة: معوقات إثبات الجرائم الماسة بالمستهلك الإلكتروني	280
الفرع الثاني: إشكاليات التعاون الدولي على المستوى الدولي في الجرائم الماسة بالمستهلك الإلكتروني	283
الفقرة الأولى: مشكلة الاختصاص و تنفيذ الأحكام الأجنبية	283
الفقرة الثانية: الصعوبات الخاصة بالمساعدة القضائية	285
الفقرة الثالثة: الصعوبات الخاصة بتسليم المجرمين	286
الفقرة الرابعة: الصعوبات المتعلقة بمجال التدريب	287
الفصل الثاني: إثبات الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	288
المبحث الأول: إجراءات ضبط الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	289
المطلب الأول: الإجراءات المتخذة من طرف الضبطية القضائية لكشف الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	290
الفرع الأول: التفتيش و الضبط لكشف الجرائم الماسة بالمستهلك الإلكتروني	290

الفقرة الأولى: التفتيش في الجرائم الماسة بالمستهلك الإلكتروني	291
الفقرة الثانية: الضبط في الجرائم الماسة بالمستهلك الإلكتروني	304
الفرع الثاني: الخبرة في إثبات الجرائم الماسة بالمستهلك الإلكتروني	310
الفقرة الأولى: مفهوم الخبرة في البيئة الإلكترونية	310
الفقرة الثانية: القواعد القانونية التي تحكم الخبرة في البيئة الإلكترونية	312
الفقرة الثالثة: القواعد التقنية التي تحكم الخبرة القضائية في مجال الجرائم الإلكترونية	314
المطلب الثاني: الإجراءات المتخذة من الجهات الخاصة في كشف الجرائم الماسة بالمستهلك في المعاملات الإلكترونية	319
الفرع الأول: الإجراءات المتخذة من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها	319
الفقرة الأولى: مفهوم المراقبة الإلكترونية للاتصالات	320
الفقرة الثانية: شروط تنفيذ المراقبة الإلكترونية	323
الفرع الثاني: الإجراءات المتخذة من قبل مؤدي خدمات الأنترنت	325
الفقرة الأولى: تعريف مقدم الخدمة	326
الفقرة الثانية: التزامات مقدمي الخدمات	327
الفرع الثالث: الإجراءات المتخذة من قبل أعوان الرقابة التابعين لمصالح التجارة	332
الفقرة الأولى: تفتيش المحلات التجارية الإلكترونية	332
الفقرة الثانية: فحص الوثائق المتعلقة بالمعاملات التجارية الإلكترونية	334
المبحث الثاني: حجية الدليل الإلكتروني في إثبات الجرائم الماسة بالمستهلك في العاملات الإلكترونية	335
المطلب الأول: ماهية الدليل الإلكتروني في إثبات الجرائم الماسة بالمستهلك الإلكتروني	336
الفرع الأول: مفهوم الدليل الإلكتروني	336
الفقرة الأولى: تعريف الدليل الإلكتروني	336
الفقرة الثانية: خصائص الدليل الإلكتروني	339
الفرع الثاني: أنواع الدليل الإلكترونية و أشكاله.	342
الفقرة الأولى: أنواع الدليل الإلكتروني	342
الفقرة الثانية: أشكال الدليل الإلكتروني	345
الفقرة الثالثة: مصدر الأدلة في الشكل الإلكتروني	348
المطلب الثاني: حجية الدليل الإلكتروني أمام القضاء الجنائي في الجرائم الماسة بالمستهلك	352

في المعاملات الإلكترونية	
الفرع الأول: سلطة القاضي الجنائي في قبول الدليل الإلكتروني	352
الفقرة الأولى: أساس قبول الدليل الإلكتروني في الإثبات الجنائي	353
الفقرة الثانية: المشروعية كقيد على حرية القاضي الجنائي في قبول الدليل الإلكتروني	361
الفرع الثاني: سلطة القاضي الجنائي في تقدير الدليل الإلكتروني.	366
الفقرة الأولى: حرية القاضي الجنائي بالاقتناع بالدليل الإلكتروني	366
الفقرة الثانية: الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني.	370
الخاتمة	376
قائمة المراجع و المصادر	387
الفهرس	415

الملخص :

تعتبر ظاهرة الجرائم الماسة بالمستهلك في المعاملات الإلكترونية من الظواهر التي افرزها النظام العالمي الجديد، حيث بدأت في الظهور و الانتشار و ارتبطت بتكنولوجيا متطورة هي تكنلوجيا الحاسبات الآلية، و نتيجة تميزها بمجموعة من السمات و الخصائص جعلتها تختلف عن غيرها من الجرائم الأخرى مما ترتب عليه ضرورة التعامل معها بما يتلاءم مع هذه المميزات، و هو ما جعل المشرع الوطني يتصدى لكل الاعتداءات الماسة بالمستهلك في المعاملات الإلكتروني، و ذلك من خلال مجموعة من القوانين سواء منها ما تعلق بمكافحة الغش التجاري في المعاملات الإلكتروني أو تلك المتعلقة بحماية متطلباته في هذا النوع المستحدث من المعاملات التجارية، كما وضع قواعد إجرائية تحدد الاختصاص القضائي في متابعة الجرائم الماسة بالمستهلك الإلكتروني، و آليات إثبات هذه الجرائم.

الكلمات المفتاحية: المعاملات الإلكترونية، المستهلك الإلكتروني، الحماية الجنائية، الغش التجاري، متطلبات المعاملات الإلكترونية.

Le résumé :

Les nouveaux crimes contre le consommateur dans le cadre des transactions électroniques sont l'un des phénomènes nouvellement apparu avec le nouvel ordre mondial, dont ils ont commencé à apparaître et à se répandre et a s'associer aux technologies de pointe ,En raison de leurs ensemble distinctifs de traits et caractéristiques, ils sont différents des autres crimes, ce qui entraîne la nécessité de les traiter conformément en fonction de ces traits, C'est ce qui a incité le législateur algérien à traiter toutes les atteintes contre le consommateur lors de transactions électroniques, .tout en élaborant et adoptant ensemble de lois, qu'il s'agisse de la lutte contre la fraude commerciale dans les transactions électroniques ou de la protection de ses exigences dans ce nouveau type de transactions commerciales, ainsi que de l'établissement de règles de procédure pour déterminer la compétence en matière de poursuite des infractions contre le consommateur et de mécanismes pour prouver ces infractions.

Les mots clefs : transactions électroniques, le consommateur électronique, la protection pénale, la fraude commerciale, les exigences des transactions électroniques.

Abstract :

The phenomenon of crimes against the consumer in e-transactions is one of the phenomena produced by the new world order ; thus It began to emerge and spread in association with an advanced technology that is computer technology ; and as a result of its distinctive set of features and characteristics made it different from other crimes which led to a need to deal with them in line with these advantages, the national legislator addresses all asaults against the consumer in e-transactions, through a set of laws, whether related to the fight against commercial fraud in e-transactions or those related to the protection of its requirements in this new type of commercial transactions, as well as the establishment of procedural rules to determine the jurisdiction to follow up crimes against the consumer, and mechanisms to prove these crimes.

Keywords: e-transactions, e-consumer, criminal protection, commercial fraud, e-transaction requirements...