وزارة التعليم العالي والبحث العلمي

جامعة أحمد دراية أدرار

كلية الحقوق والعلوم السياسية

قسم الحقوق

جامعة أحمد دراية.أدرار-الجزائر
Université Ahmed Draia.Adrar -Algérie

الحماية الجزائية للمعاملات الإلكترونية
[دراسة مقارنة]

رسالة مقدمة لنيل شهادة الدكتوراه علوم فـي الحقوق

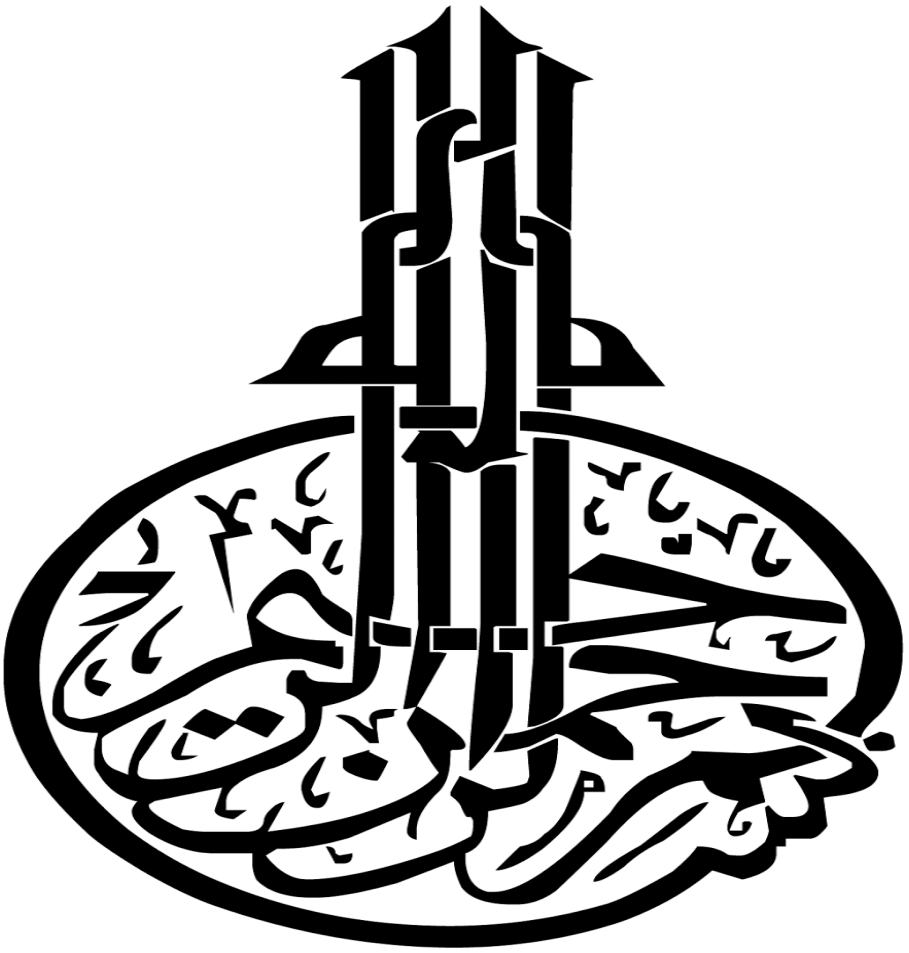
إعـداد الطالبـة: الدهـبي خـدوجـة

إشـراف الأسـتاذ الدكـتور: باخـــويا دريـس

أعضاء لـجنـة المناقـشة:

أ.د/ بومـديـن مـحمد	أسـتاذ التـعلـيم الـعالي	جامـعة أدرار	رئـــيســـاً
أ.د/ باخـويا دريـس	أسـتاذ التـعلـيم الـعالي	جامـعة أدرار	مشرفـاً ومقـرراً
د/ مايـنو جـيلالـي	أسـتاذ مـحاضـر "أ"	جامـعة بشار	منـاقـــشاً
د/ بـوشـي يـوسف	أسـتاذ مـحاضـر "أ"	جامعة تيارت	منـاقـــشاً

الموســم الجامعي: 2019/2018



قائمة المختصرات:

أولاً– باللغة العربية:

– ب د ن	– بدون دار نشر.
– ب س ن	– بدون سنة نشر.
– ج ر ج	– الجريدة الرسمية الجزائرية..
– ص	– صفحة.
– ص ص	– من الصفحة إلى الصفحة
– ط	– طبعة.
– ق ع ج	– قانون العقوبات الجزائري
– ق م ج	– القانون المدني الجزائري
– ق.إ.ج.ج	– قانون الإجراءات الجزائية الجزائري

ثانياً– باللغة الفرنسية:

– **Op.Cit**	– **.citatis opère)Ouvrage précité**
– **Crim .Cass**	– **cassation arrêts des chambers criminelle de la cour de**
– **Chron**	– **chronique**
– **Éd**	– **.édition**
– **I.G.T**	– **.instance Tribunal de grande**
– **Pal .Gaz**	– **.palais gazette du**
– **P .C .J**	– **.juridique mainese ,classeur périodique –jurais**
– **D. S**	– **.date sans**
– **Tribu**	– **.tribunal**
– **J. D .G .L**	– **.jurisprudence de et droit de générale librairie**
– **P**	– **. page**
– **N**	– **.numéro**
– **Rev**	– **revue**
– **d.n.ass.Rev**	– **.Droit Revue de La association nationale en**
– **Doct**	– **Doctorat**
– **CE**	– **Européen Conseil**

شكر وتقدير

بسم الله الرحمان الرحيم:

" ولئــن شكرتم لأزيـــــــدنكم."

صدق الله العظيم

بادئاً أشكر الله تعالى وأحمده على جزيل فضله ونعمه، وتوفيقه لنا في إنجاز هذه الأطروحة.

وأتقدم بوافر الامتنان إلى الأستاذ الفاضل البروفسور: "باخـويا دريـس" على قبوله الإشراف على هذا العمل وتنقيحه، والذي لم يبخل علينا بالملاحظات والتوجيهات القيمة التي أنارت لنا طريق البحث والتقصي.

فله منا أسمى عبارات الشكر والتقدير.

إلى كل من دعمني لإتمام هذا العمل ولو بكلمة تشجيع ، جزيل الشكر.

الطالبة:

الدهبي خدوجة

إهـــــــداء

إلى من لا يمكن أن أنكر أن سبب أي نجاح في حياتي هو من سر دعائهما ورضائهما، ووجودهما هو النبع الذي استقيت منه الصبر والكد في إتمام هذه الأطروحة

والدتي .. والدي .. أطال الله في عمرهما

إلى الإخوة والأخوات و كل العائلة الكريمة

إلى كل أصدقائي وأحبابي

إلى كل من مد لي يد العون في إنجاز هذا العمل من قريب أو بعيد

أهدي هذا العمل المتواضع.

الطالبة:

الدهبي خدوجة

مقدمـــــة

مقدمـــــة:

يشهد العالم منذ منتصف القرن العشرين غزواً تكنولوجياً هائلاً في كافة نواحي الحياة الاقتصادية والاجتماعية والسياسية، الأمر الذي ترتب عنه تغيير جذري في سير حياة المجتمعات المتقدمة منها والنامية، إذ أصبحت تلك الأخيرة تعرف نمطاً حديثاً من الثورات أصطلح عليها بالثورة المعلوماتية أو الثورة "الصناعية الثالثة"، والتي يعد قوامها استغلال أجهزة الكمبيوتر والشبكات المتصلة بها، وعلى رأسها شبكة الانترنت[1]، وما نتج عنها من تحول المعمورة إلى مجرد قرية إلكترونية صغيرة تتدفق المعلومات بين أرجائها في سهولة وسرعة، ويتم فيها التبادل والتحصيل المعرفي بطرق يعجز الإنسان بقدراته العادية عن متابعتها والإلمام بها، لدرجة أصبح معها العصر الحالي عصر المعلومات الفائق السرعة؛ نظراً لانعكاس التحول الجذري لركائز المشاريع الكبرى والمحددات الاقتصادية الاستراتيجية من القيم المادية إلى القيم المعنوية، كالمعلومات والبيانات التي تتبلور في شكل جديد من التعاملات؛ تعرف بالمعاملات الإلكترونية.

وبلا شك، تعتبر المعاملات الإلكترونية واحدة من سمات هذا العصر التكنولوجي؛ نظراً لما رافقها من تغيير في شتى المستويات، ونظراً لما توفره من مزايا لأطرافها التي ترتكز بشكل أساسي على طبيعة الوسط الذي تجرى من خلاله.

إن التعامل الإلكتروني يأخذ معنى التبادل أو التراسل أو التعاقد، أو أي إجراء آخر يبرم أو ينفذ بشكل كلي أو جزئي بوسيلة إلكترونية، كما أنها تعد وسيلة توظيف لأداء معين باستخدام الوسائط والأساليب الإلكترونية, يعبر عنها بآليتي الحاسب الآلي والانترنت"، والتي يقوم من خلالهما تبادل ونقل المعلومات والخدمات، وكذا آليات انتاجها المتمثلة بالبريد والرسائل والتوقيعات والعقود الإلكترونية[2].

---

1 ظهرت الانترنت في الستينات من هذا القرن، عندما قررت المؤسسة العسكرية الأميركية أنها تحتاج إلى وسائل آمنة لتحريك معلوماتها عبر العالم، وأعدت سلسلة من الوصلات الحاسوبية تعرف بـ: (ARPA Net)، جعلتها تستغني عن الاعتماد على طريق واحد لاستعلاماتها أو استخباراتها، وعرفها البعض بأنها شبكة عالمية على نطاق عالمي من الشبكات الحاسوبية المختلفة المتصلة ببعضها البعض بواسطة وصلات بعيدة، وهذه الشبكة مكونة من منظمات ومؤسسات متنوعة تشمل الحكومية والجامعات والشركات التجارية التي قررت للآخرين بالاتصال بحواسيبها ومشاركتهم المعلومات، ويعود إلى كل مؤسسة أو منظمة أمر تحديد حجم المعلومات أو البيانات التي ترغب في عرضها للآخرين وتحديد أسس عرض هذه المعلومات ، مقابل ذلك يمكن لهؤلاء المؤسسات استعمال معلومات مؤسسات ومنظمات أخرى. **انـــظر**: عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية، دار وائل للنشر والتوزيع، الطبعة الأولى، عمان، سنة 2003، ص 19.

2 جليل الساعدي، مشكلات التعاقد عبر الانترنت، مكتبة السنهوري للنشر والتوزيع، بغداد، سنة 2011، ص 230.

إن المعاملات الإلكترونية قد تحوي مفهوماً واسعاً لشتى المستويات اعتماداً على استخدام الوسائل الإلكترونية في معالجة المعطيات وتبادلها، عكس اتجاه البعض الذي يحصر مفهومها في إطار التبادل التجاري الإلكتروني[1] فحسب، وهو ما ينافي المعنى الحقيقي لها، بحيث أن المعاملات الإلكترونية تتسع لتشمل جميع الأنشطة الإدارية، الاقتصادية، الانتاجية، المالية، والخدماتية، الأمر الذي صاحبه ظهور مفاهيم عديدة لأنماط التعامل الإلكتروني الحديث كالتجارة الإلكترونية، والإدارة الإلكترونية، والحكومة الإلكترونية، والدفع الإلكتروني، والعمليات المصرفية الإلكترونية وغيرها.

هذا وقد أصبح نظام المعاملات الإلكترونية في نهاية القرن الماضي من لوازم الحياة الضرورية، وأضحت الدول تعتبره نقطة تحدٍ ورهان لفتح آفاق جديدة في ظل التطور الحاصل والمتنامي بين الدول على جميع الأصعدة، بالرغم من أن هذا التطور له بعض الانعكسات الجنائية السلبية التي قد تمس بمصالح وحقوق الأفراد، الأمر الذي يستلزم توفير الحماية القانونية لهذه المصالح والحقوق سواء في إطار النصوص التقليدية، أو باستحداث النصوص الملائمة لطبيعتها, والدور الذي تؤديه في الحياة كياناً أو نشاطاً.

وبناءً عليه, أضحت المعاملات الإلكترونية مجالاً خصباً لظهور أشكالاً عديدة من الاعتداءات التي استوجبت المواجهة التشريعية تبعاً لآثارها الوخيمة على الفرد والمجتمع، وهذا انطلاقاً من النمط التقليدي للجرائم التي وجدت تطبيقاً حديثاً لها في حيز المعاملات الإلكترونية الاقتصادية بشكل خاص، بحيث ظهرت بعض الأساليب المشكلة للجرائم الواقعة على الأموال في بيئة غير مادية؛ كالسرقة والاحتيال وخيانة الأمانة، ومنها ما قد يمس بآليات تنفيذ المعاملات الإلكترونية كتزوير المحررات الإلكترونية، وهنا تفرض مسألة البحث في قواعد الحماية الجنائية من هذه الجرائم، إسقاطا لشروط وأركان الجريمة في وجهها التقليدي على المجال أو الحيز اللامادي في التعامل الإلكتروني، والخروج بأحكام تتناسب وطبيعة قيام النشاط الإجرامي، وفرض الجزاء المناسب له، بالموازاة مع عدم الخروج عن القواعد والمبادئ التي يقوم عليها الحكم التشريعي الجنائي؛ وعلى رأسها مبدأ المشروعية.[2]

---

1 لقد جاء المشرع الجزائري بتعريف محدد للتجارة الإلكترونية في نص المادة السادسة من القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي 2018 يتعلق بالتجارة الإلكترونية بحيث عرفها: "التجارة الإلكترونية: النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني عن طريق الاتصالات الإلكترونية". وهنا يظهر أن التعامل الإلكتروني هو أوسع نطاقاً من التعامل التجاري الإلكتروني بحيث قد يحوي التجارة الإلكترونية وغيرها من النشاطات والتعاملات في المجال الإلكتروني.

2 يقصد بمبدأ المشروعية أن لاجريمة ولا عقوبة إلا بنص، هذا المبدأ الذي يعد من أقدس ما توارثته الإنسانية في عهدها الجديد وعلى أعتابها دانت رقاب الفساد والطغاة والاستبداد وتحكم القضاة، الأمر الذي حدا إلى تطبيق هذا المبدأ تطبيقاً جامداً في بداية عهده في

وتبعاً لذلك, قد تأخذ الجريمة طابعاً نابعاً من طبيعة التعامل الإلكتروني، فيبرز نوع مستحدث من الجرائم أخذ قوامه من خلال نطاق المعاملات الإلكترونية وآليات نشوئها وتنفيذها، وهو ما يظهر بدقة في الجرائم الماسة بالنظام المعلوماتي؛ باعتباره يمثل أساس نشوء التعاملات الإلكترونية وذلك من خلال المساس بالبيانات والمعلومات الإلكترونية، أو الاعتداء عليها بأي شكل ينال من أمن وسرية المعطيات الشخصية أو المعلومات الرقمية الخاصة ببطاقات الدفع الإلكتروني، وكذا الأنشطة الإجرامية التي تمس مضمون التعاملات الإلكترونية كأساليب التعدي على نظام التوقيع الإلكتروني؛ الذي يعد أهم آليات تنفيذ التعامل الإلكتروني، والذي يرتبط بدوره بشكل مباشر بتحديد مصداقية الأداء للأعمال الإلكترونية, ومدى حجيتها القانونية، وكذا نظام الدفع الإلكتروني الذي يشكل الوسيلة الملائمة لتنفيذ المعاملات المالية والتجارية، والذي يتماشى وحاجيات التعامل عبر الوسائط الإلكترونية, فهو يشمل جملة من الأنماط التي تؤدي الوفاء والتحويل المالي الإلكتروني بين أطراف المعاملات الإلكترونية بشكل يتناسب وطبيعة التعامل والبيئة التي يؤدى من خلالها.

إن المعاملات الإلكترونية ترتبط بشكل رئيسي بخدمة الانترنت التي تمنح المستخدمين فرص تسهيل التواصل الإلكتروني، وتسيير المصالح عبر قنوات الشبكة، وهو مايقع على عاتق الوسطاء الفنيين لخدمة الإنترنت لما لهم دور مباشر في تحقيق آلية عمل المعاملات الإلكترونية، وذلك من خلال الأدوار المساهمة في إصدار المعلومة الإلكترونية وتداولها، وهذا الأمر يستلزم الوقوف ضد أي تجاوزات ذات التأثير السلبي على النشاط الاقتصادي للأشخاص أو الهيئات .

ونظراً لكون الحماية الجنائية للمعاملات الإلكترونية لا تقتصر على الشق الموضوعي فقط، بل تتعداه لفرض قواعد الحماية على المستوى الإجرائي؛ على اعتبار أن الجرائم الواقعة في مجال التعامل الإلكتروني تقوم على التقنية العالية، ونظراً لكونها جرائم عابرة للحدود، ، فإن هذا النوع من التجريم أضفى على مسألة الإجراءات الجنائية تعقيدات كثيرة، وجملة من الصعوبات والإشكالات العملية التي تقف حجر عائق أمام أجهزة العدالة في مواجهتها لهذه الطائفة من الجرائم، ولا سيما أجهزة الضبط والتحري، وكذا الإشكاليات المثارة حول وسائل الإثبات في البيئة الإلكترونية، بالإضافة إلى خصوصية الدليل الإلكتروني، وما قد يصاحب الحصول عليه من خطوات معقدة، وما يثيره من إشكالات على مستوى تقديره من قبل القاضي

ظل المدرسة التقليدية مما حرم القاضي من أي سلطة تقديرية وضعت التشريعات في ظل العقوبات الواحدة، ثم أصبح هذا المبدأ ملازماً للتشريعات لا يفارقها، أما بالنسبة للجرائم الواقعة على المعاملات الإلكترونية، فالأمر قد أوقع القضاء أمام تصادم بين فتح الباب أمام القضاة للعمل بالقياس أو التفسير الواسع للنص مما يهدر مبدأ الشرعية. **للمزيد انظر**: محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، مصر، سنة 2009، ص 54.

الجنائي، وكذا إبراز أهم الأساليب القانونية التي تؤسس المبادئ الملائمة للإختصاص القضائي في المجال الإلكتروني، وحل مسألة التنازع بشكل يحقق الغرض من الحد من هذه الجريمة، وضمان متابعة الجناة وتوقيع الجزاء.

إن التوجه نحو تبني شكل المعاملات الإلكترونية في نمط حياة الأفراد أصبح يتزايد بشكل غير مسبوق، حيث فتحت تقنيات شبكة الانترنت آفاقاً جديدة، ومجالات مبتكرة امتدت حتى شملت مختلف المستويات والعديد من الأنشطة، خاصة الاقتصادية منها، بالرغم من الأخطار المترتبة عن هذا التطور الذي جاء إفرازاً لواقع المجتمعات التي نشأت فيه بما تتضمنه من تناقضات، وهو ما أظهر أساليب إجرامية موازية في تطورها وحداثتها لتلك المعاملات، وأضحى القائمون على تطبيق القوانين أمام مأزق حقيقي بين تطبيق النصوص العقابية القائمة، أو التدخل لسن تشريعات جديدة لمواجهة النقص التشريعي، وهو ما سعى إليه المجتمع الدولي من خلال جملة من التشريعات الجزائية التي تشكل سياجاً ضد الاعتداءات على أساليب التعامل الإلكتروني، وبالأخص على شبكة الانترنت في إطار ما يعرف بالجريمة الإلكترونية، وهذا ما جسد من خلال الاتفاقية الأوروبية لمكافحة الإجرام التقني لعام 2001 في بودابست؛ وهي من بوادر التشريعات التي أنشأت أحكاماً تشريعية دولية شاملة هادفة إلى الحد من الجريمة في الفضاء الإلكتروني في خضم التسارع والحرفية في الجريمة، وتطور خطورتها عبر السنوات بشكل لافت.

وأما على المستوى الإقليمي العربي فقد أدركت الدول ضرورة التكافل لوضع نظام جزائي إقليمي يأخذ على عاتقه مهمة إيجاد قواعد شاملة تجرم الاعتداءات الإلكترونية، وتجسد مبادئ الحماية الجنائية للمعاملات الإلكترونية، فتم ميلاد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010 بالقاهرة[1]، رغبة منها في تعزيز التعاون بين الدول العربية لمكافحة جرائم تقنية المعلومات التي تهدد أمنها، واقتناعاً بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم المعلومات، ونبهت الاتفاقية إلى ضرورة التزام كل دولة طرف وفقاً لنظمها وقوانينها الداخلية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية.

وهذا ما جعل العديد من التشريعات تسير على نهج الاتفاقات الإقليمية أو الدولية، وتساهم بدورها في مكافحة الجريمة المرتكبة عبر التعامل الإلكتروني، ووضع لبنة أساسية لحماية أهم المصالح في نطاق

1 الإتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010: حررت هذه الاتفاقية باللغة العربية في مدينة القاهرة بجمهورية مصر العربية في 01/15/ 1432 هـ الموافق 2010/12/21 من أصل مودع بالأمانة العامة لجامعة الدول العربية ونسخة مطابقة للأصل تسلم للأمانة العامة لمجلس وزراء الداخلية العرب.

المعاملات الإلكترونية؛ لذلك نجد بأن المشرع الفرنسي قد تأثر باتفاقية بودابست، وعمل على إصدار قانون خاص بحماية الثقة في الاقتصاد الرقمي رقم 2004-575 وهو نتاج الرؤية المؤسسة على خلق آليات جنائية ذات أبعاد مهمة على مستوى التجريم في مجال التجارة الإلكترونية وغيرها من التعاملات الإلكترونية، كما أدخل عدة تعديلات على التشريع العقابي الفرنسي ليحقق نظام جنائي فعال ضد الجريمة الإلكترونية عبر شبكة الانترنت.

النظام الأنجلوسكسوني بشكل عام، والتشريع الأمريكي والإنجليزي بشكل خاص عملا على رصد مختلف الأنشطة الإجرامية الإلكترونية, والتصدي لها بقوانين خاصة تفي بغرض الحماية الجنائية لمثل هذه الجرائم، ومدعمة أسس التعامل الإلكتروني الآمن والسليم بفرض جزاءات رادعة في هذا الصدد.

وأما التشريعات العربية الداخلية لم تبقَ في منأىً عن هذا الحراك التشريعي، فنجد أغلبها قد تحرك اتجاه تعديل أو سن تشريعات عقابية من أجل مواجهة مخاطر الجريمة الماسة بالمعاملات الإلكترونية؛ من بينها المشرع الإماراتي بإصدار القانون الاتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، والمشرع الأردني بقانون الجرائم الإلكترونية رقم 27 لسنة 2015، والقانون السعودي من خلال نظام مكافحة الجرائم المعلوماتية وغيرها .

المشرع الجزائري بدوره لم يقف موقفا سلبياً، إنما أدخل عدة تعديلات على التشريعات العقابية سواء في شقيها الموضوعي والإجرائي، في مجال مكافحة الجريمة الإلكترونية، وبسط حماية قانونية ضد الاعتداءات على شتى أنواع التعامل الإلكتروني التي سبق وأن اعترف بها في عدة ميادين قانونية، وهو ما جسده من خلال القانون 04-15 المعدل لقانون العقوبات، والذي كرس من خلاله قواعد حماية فاعلة ضد أشكال التعدي على المنظومة المعلوماتية، ثم أتم هذه الخطوة بإصدار القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وهو أول قانون خاص يهدف إلى إرساء قواعد تشريعية جنائية لمواجهة جرائم تقنية المعلومات في النطاق الإلكتروني، وخاصة على شبكة الإنترنت.

وفي ظل الحركة التطورية التي تشهدها أساليب الاعتداء في المجال الإلكتروني، تظهر أهمية المواجهة التشريعية في خضم التشريعات السابقة؛ وبالأخص الجانب الجنائي، ما يفرض معه ضرورة تنامي التوجه التشريعي نحو مواكبة تطور الجريمة الإلكترونية, والتفاعل مع المستجدات التي تظهر في هذا الميدان لتحقيق معاملات إلكترونية في بيئة آمنة وسليمة.

وفي ضوء التقدم التكنولوجي وما يترتب عليه من تنوع في المعاملات الإلكترونية وسرعة انتشارها، وكذا خلق وسائل حديثة لتنفيذها، الأمر الذي وسع الهوة بين أطراف التعامل من حيث القدرة والخبرة والمعرفة لصالح شخص على حساب آخر، ولذلك فإن أساس إيجاد آليات قانونية لحماية الفرد في المعاملات الإلكترونية يكمن في حالة الضعف المسيطرة على جهل التقنيات والثغرات التي قد يتسلل منها المعتدي، ومن ثم يمكن القول أن تكريس الحماية الجنائية لها دور فعال وبارز في تجريم الفعل وتوقيع العقاب، بحيث لا يهدف فقط إلى حماية الفرد ضد سلوكات إجرامية، وإنما تهدف بطريقة واضحة إلى حماية المجتمع ككل.

إن البيئة الإلكترونية التي ينشأ من خلالها التعامل الإلكتروني، تدعم ضرورة وجود حماية خاصة للمستهلك في عقود التجارة الإلكترونية ومختلف المعاملات المالية والاقتصادية، وذلك لقصور القواعد العامة التي تحمي الفرد في عقود المعاملات التقليدية عن توفير الحماية المنشودة للمتعامل الإلكتروني، فالسمة البارزة للمعاملات الإلكترونية أنها تتم في ظل الغياب المادي لأطراف التعامل، كما أن طبيعة البيئة الإلكترونية وخاصة في شبكة الانترنت المفتوحة عالمياً، والمتاحة لجميع الأشخاص، تجعل من الشخص رهينة الوقوع فريسة سهلة للغش والتدليس والاحتيال.

إن فكرة التعاقد في عقود المعاملات المالية الإلكترونية تثير مسألة أمن المتعامل، فقد يتطلب التعاقد أن يُقَدِّم الشخص معلومات شخصية كرقم بطاقة الائتمان، أو عنوان البريد الإلكتروني، مما يعرضه لخطر إساءة استعمالها من قبل قراصنة الإنترنت، وهو ما يمثل انتهاكاً لخصوصية المستهلك، وتهديداً لمصلحته المادية والمعنوية، ومن هنا بدت الحاجة لوضع آليات قانونية لحماية المتعامل في البيئة الإلكترونية، فالثقة في التعامل المالي الإلكتروني من أبرز ما يحتاج إليه الفرد في سبيل تلبية احتياجاته الشخصية، وبذلك تظهر ضرورة توافر السبل القانونية الجنائية لضمان قيام مبادلات إلكترونية آمنة وسليمة؛ لأن تهيئة مناخ تسوده الثقة في بيئة الإنترنت أمر ضروري للتنمية الاقتصادية والاجتماعية.

ونتيجة لذلك سارع الاتحاد الأوروبي إلى إصدار النظام رقم 2014–910 المتعلق بتحديد الهوية الإلكترونية وبث الثقة في التعاملات الإلكترونية في السوق الداخلية[1]، بحيث جاء في ديباجته: "أن الغرض

1 RÈGLEMENT (UE) No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Disponible sur le site suivant: *https://eur-lex.europa.eu/legal-content/FR/TXT/HTML*.

من هذا النظام هو خلق ثقة أكبر في التعاملات الإلكترونية داخل السوق الداخلية من خلال توفير أساس مشترك للتفاعلات الإلكترونية الآمنة بين المواطنين والشركات والهيئات العامة، وبالتالي زيادة فعالية الخدمات العامة عبر الإنترنت والخاصة، وكذلك النشاط الاقتصادي والتجارة الإلكترونية في الاتحاد"[1].

إن مبررات الحماية الجنائية من المنظور التقني تفرض نفسها؛ من خلال أن التطور التقني يمثل واقعاً علمياً، يحمل العديد من المستجدات الدائمة، والتي تقود إلى تحسين وتسهيل أشكال التعامل بين الأفراد بهدف الحصول على أفضل أداء للممارسات الإلكترونية، غير أن الجانب السلبي لهذا التطور يجسد أضرار التعاقد عبر شبكة الانترنت، مما يفرض معها ضمان الوقاية ضد المخاطر التي يفرزها هذا النمط الحديث من المعاملات.

إن التطور الهائل في مجال التجارة الإلكترونية، أفرز معه توجه المستهلك نحو المواقع التجارية الإلكترونية لتعدد الخدمات المعروضة، مع المزايا المتعددة في العرض والأسعار، فأهمية الخدمات الإلكترونية على شبكة الانترنت زادت من إقبال المستهلكين على هذه الخدمات، وجعلت منها محور طلب للكثير منهم، ومن هنا كانت الحاجة للبحث عن حماية المستهلك بصفته نموذجاً للمتعامل الإلكتروني .

وعلاوة على ما ذكر, فإن كشف النقاب عن قصور القواعد القانونية التقليدية في إيجاد حماية فعالة للمتعامل الإلكتروني في مجال الجرائم ذات الطابع التقليدي المرتكبة في النطاق الإلكتروني، والتي يجب أن تتماشى وحكم المسائل الجديدة التي ولدتها الثورة السريعة في مجال الاتصالات والمعلومات، قد ولد الحاجة إلى وضع نظام قانوني مرن يوفق بين المبادئ العامة لحماية الأشخاص وتطويعها في سبيل حمايتهم، أو وضع منظومة تشريعية سواء في الجانب الموضوعي أو الإجرائي، قادرة على تعويض قصور القواعد التقليدية عن إيجاد الحلول الملائمة في نطاق التعامل الإلكتروني، وقادرة على سد الثغرات التي قد تتسبب في إفلات الجاني من العقاب.

وأمام الجدل القانوني الذي يثار من خلال كيفية إتمام الجوانب الإجرائية للمعاملات الإلكترونية بدءاً بخصوصية وسائل الإثبات الجنائي في البيئة الإلكترونية، ومدى توفير التشريع المقارن لأحكام تخص إجراءات التحري والتحقيق وتفعيل دورها في كشف معالم الجريمة، ولما كانت هذه الجرائم ذات طبيعة خاصة، انعكس

1 "Le présent règlement vise à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur en fournissant un socle commun pour des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques et en accroissant ainsi l'efficacité des services en ligne publics et privés, ainsi que de l'activité économique et du commerce électronique dans l'Union."

هذا الأمر على مراحل التحقيق والتحري في هذه الجرائم؛ نظراً لكونها مرحلة ذات أهمية يكشف فيها النقاب عن أمر الجريمة الواقعة، ويُمَهد فيها الطريق لحسم أمر تحريك الدعوى العمومية من عدمه من قبل سلطة الإدعاء، الأمر الذي طرح عدة إشكالات تستوجب إيجاد حلول قانونية من قبل رجال الفقه، ويستنير بها المشرع الإجرائي عند سنه القوانين، وكذا إلهام القضاء بإيجاد أحكام منطقية تتماشى وطبيعة الجريمة، وكذا الحكم التشريعي الذي ينظم المسألة، بالإضافة إلى تحديد الاختصاصات والهياكل التي تقوم على البحث والتحري في الجرائم, ومدى خصوصية المهام الموكلة لديها في هذا النوع من الجرائم بالمقارنة مع الجرائم التقليدية، فضلاً عن حل إشكال الاختصاص القضائي بتنازع عدة مبادئ ومعايير تطبق على الجريمة العابرة للحدود، وتخرج بحل إيجاد التشريع الجنائي المناسب لمتابعتها وتوقيع العقاب على مرتكبيها.

ونتيجة لذلك فإن مسألة التصدي للإشكالات القانونية الناتجة عن الحماية الجزائية للمعاملات الإلكترونية أصبحت أمراً ضرورياً يستوجب مواجهته للخروج بأزمة التشريع الجزائي لهذا النوع من الجرائم.

ففي ظل التوسع نحو اتخاذ المعاملات الإلكترونية كأساس في الأنشطة الحياتية للأفراد على كل المستويات، وفي إطار البحث عن الخيارات والحلول التشريعية التي تقي المتعاملين خطر التواجد في البيئة الإلكترونية، وقصد ضمان الحماية الجنائية الكافية لهم يمكن طرح الإشكالية الرئيسية التالية :

إلى أي مدى ساهمت التشريعات المقارنة في تأسيس أنظمة حماية جزائية فعالة في شقيها الموضوعي والإجرائي ضد الجرائم المرتكبة في مجال المعاملات الإلكترونية ؟

ويتفرع عن هذه الإشكالية تساؤولان اثنان هما:

- ما مدى إمكانية تطويع النصوص الخاصة بالجرائم التقليدية لتشمل حماية المعاملات الإلكترونية المستحدثة ؟
- وهل تعتبر التعديلات التشريعية الخاصة بالجانب الإجرائي في مجال الجريمة المعلوماتية كافية للتطبيق على شتى أنواع جرائم المعاملات الإلكترونية ؟

ومن أجل الإجابة عن الإشكالية المذكورة, تم الإعتماد على مجموعة من المناهج, يمكن بيان أوجه توظيفها كما يلي:

المنهج الوصفي: ويتجلى توظيف هذا المنهج من خلال بيان الأحكام الخاصة بالجرائم الواقعة في التعامل الإلكتروني وطرح المفاهيم والمصطلحات القانونية والفقهية المتعلقة بها، وكذا بيان القواعد الخاصة بالجوانب الإجرائية بسرد الأحكام النظرية العامة للإثبات الجنائي.

المنهج التحليلي: والذي يقوم أساساً على جمع وتحليل ونقد النصوص القانونية والآراء الفقهية, والبحث في الأحكام المؤطرة لحماية المعاملات الإلكترونية، وإيضاح المفاهيم التي يكتنفها الغموض من الجانب التشريعي والفقهي, وهو المنهج الذي تعتمده الدراسة في أغلب جوانبها.

المنهج المقارن: وذلك من خلال المقارنة بين بعض الأنظمة التشريعية, والتي من بينها التشريع الفرنسي لما له من تأثير في التشريع الجزائري, وكذا التشريع الإنجليزي والأمريكي وذلك لخصوصيتهما في تبني بعض الأحكام الجنائية في المجال الإلكتروني، كما تمت الإستعانة بنماذج عن بعض التشريعات العربية والتي لم نوردها بشكل حصري، إنما تم التطرق إلى الأحكام الواردة فيها وفقاً لكل مسألة.

ومن أجل معالجة الموضوع, تم تقسيم الدراسة إلى بابين اثنين؛ خصص الباب الأول للحماية الجزائية الموضوعية للمعاملات الإلكترونية، والذي قسم بدوره إلى فصلين؛ تم التطرق في الفصل الأول إلى الحماية الجزائية للمعاملات الإلكترونية في إطار الجرائم التقليدية، أما الفصل الثاني فخصص للحماية الجزائية للمعاملات الإلكترونية في إطار الجرائم المستحدثة.

وأما الباب الثاني فقد خصص لأحكام الحماية الجزائية الإجرائية للمعاملات الإلكترونية، والذي قسم هو الآخر إلى فصلين؛ تم التطرق في أولهما إلى الحماية الجزائية للمعاملات الإلكترونية في مرحلتي التحقيق الابتدائي والإثبات، أما الثاني فخصص إلى الحماية الجزائية للمعاملات الإلكترونية في مرحلة المحاكمة.

الباب الأول:
الحماية الجزائية الموضوعية للمعاملات الإلكترونية

الباب الأول:
الحماية الجزائية الموضوعية للمعاملات الإلكترونية

مع التوجه الحديث لتقنية المعلومات وتأثيرها المباشر على مجال المعاملات الفردية والحكومية لتنشأ عالماً خاصاً مليئا بالتطور والسرعة والحداثة، إلا أنه يحوي معه العديد أيضاً من المخاطر التي تحيط بشكل المعاملات الإلكترونية وطبيعتها، مما فرض على المستوى الدولي التصدي لتلك المخاطر, وأضحت مسألة الحماية الجزائية أمراً ضرورياً وعاجلاً.

ومن هنا كانت البداية من المواجهة التشريعية للجرائم التقليدية في مجال المعاملات الإلكترونية، وبناء على ذلك اتجه الفقه والتشريع لمحاولة تطبيق النصوص التقليدية المتعلقة بنصوص جرائم الأموال, مع ظهور تدخل تشريعي واسع بتعديل النصوص العقابية لتتماشى مع نشوئها في مجال المعاملات الإلكترونية (الفصل الأول)، ثم توالت إشكالية ظهور المخاطر الحديثة التي لها ارتباط أساسي بتطور المعاملات الإلكترونية والتي واجهتها التشريعات المقارنة بموجب نصوص خاصة ومستحدثة (الفصل الثاني).

الفصل الأول:

الحماية الجزائية من الجرائم التقليدية الواقعة في إطار التعامل الإلكتروني

الفصل الأول:

الحماية الجزائية من الجرائم التقليدية الواقعة في إطار التعامل الإلكتروني.

مما لاشك فيه أن التطور التكنولوجي المعاصر قد أثر على شكل المعاملات بين الأفراد، وجعلها تأخذ حلة حديثة في شكلها الإلكتروني الذي يتسم بالسرعة في الإنجاز والتقليل من التكاليف، ونتيجة لذلك أثبت الواقع أن هذه المعاملات تحمل في طياتها جملة من المخاطر التي أعطت منحى جديد للجرائم التقليدية في إطار التعامل الإلكتروني، لدرجة أوجبت النظر إلى صيغة الحماية الجنائية من الجرائم التقليدية في مجال المعاملات الإلكترونية، وهذا ما حاولنا دراسته من خلال العناصر الأساسية لقيام الجرائم التقليدية الأكثر تداولاً في النطاق الإلكتروني، وعرض الإشكالات التي تعترض تكييف القواعد العامة للجريمة التقليدية مع القواعد الخاصة بالفعل الإجرامي في شكله الحديث، ومدى توافق الأحكام العامة وصلاحيتها لتحقيق حماية جنائية فعالة للمعاملات الإلكترونية.

وبهذا تم تقسيم الفصل إلى أربعة مباحث، تم تخصيص كل مبحث إلى دراسة الحماية الجنائية لأكثر الجرائم التقليدية شيوعاً في نطاق المعاملات الإلكترونية بحيث تم تخصيص (المبحث الأول) للحماية الجزائية من جريمة السرقة في مجال المعاملات الإلكترونية, أما (المبحث الثاني) فتناولنا فيه الحماية الجنائية من جريمة الاحتيال في إطار المعاملات الإلكترونية، وأما (المبحث الثالث) فخصص للحماية الجنائية من جريمة خيانة الأمانة في إطار المعاملات الإلكترونية، كما تمت دراسة الحماية الجنائية من جريمة التزوير في إطار المعاملات الإلكترونية (المبحث الرابع).

المبحث الأول:

الحماية الجزائية من جريمة السرقة في مجال المعاملات الإلكترونية

إن طبيعة الجرائم الواقعة في مجال المعاملات الإلكترونية تحمل طبيعة خاصة ومتميزة، وأن محل الجريمة في هذا المجال قد ينصب على الأنظمة المعلوماتية سواء ما يقع عليها، أو ما يقع باستخدام أدوات مادية من أجهزة وبطاقات ممغنطة، ونظراً لتمحور هذا الفصل على الجرائم التقليدية التي تتعلق بالاعتداء على المال أو المعلومات في مجال المعاملات الإلكترونية، فإنه وجب بيان جريمة السرقة من حيث قيامها في إطار التعامل الإلكتروني، نظراً لما تتسم به أحكام هذه الجرائم من تعقيد، ونظراً لما تتطلبه من تحليل لعناصر الأموال والمعلومات المتداولة إلكترونياً، ومدى قابيلة هذه العناصر أيضاً إلى الحماية المقررة لجريمة السرقة، خاصة في ظل قصور التشريع الجزائري وباقي التشريعات المقارنة؛ والتي لم تتعرض بشكل دقيق إلى الحلول التشريعية في سرقة المال المتداول إلكترونياً.

لذلك لزاماً الربط بين العناصر المكونة لجريمة السرقة وفقاً للنص الجنائي التقليدي، وبين عناصر السرقة في مجال المعاملات الإلكترونية، وطرح إشكاليات جوهرية حول مدى تطبيق النص الجنائي التقليدي على سرقة الأموال أو المعلومات إلكترونياً، نظراً لضرورة بيان مدى تطابق القواعد القانونية العامة لجريمة السرقة مع القواعد الخاصة للسرقة في إطار المعاملات الإلكترونية، وسوف يتم التطرق لمحل جريمة السرقة في إطار المعاملات الإلكترونية (المطلب الأول)، ثم لأركان جريمة السرقة في إطار المعاملات الإلكترونية (المطلب الثاني).

المطلب الأول: محل جريمة السرقة في إطار المعاملات الإلكترونية.

من المقرر أن محل جرائم الأموال في التشريعات المختلفة ينصب على مال منقول للغير, وفي هذا الإطار تنص المادة 350 من قانون العقوبات الجزائري: "كل من اختلس شيئاً غير مملوكاً له يعد سارقاً"، وهو نفس الحكم المقرر في التشريع الفرنسي بمقتضى المادة 311-1 والتي جاء فيها: " كل من اختلس بسوء قصد شيئاً لا يملكه يكون مسؤولاً عن سرقته"[1].وتقابل هذه المادة نص المادة 382 من قانون العقوبات الإماراتي التي تنص على أن: "تقع السرقة التعزيرية باختلاس مال منقول مملوك للغير"[2].

وبهذا يقوم فعل السرقة وفقاً للأحكام التشريعية السابقة إذا ما تم الاعتداء على ملكية الأموال المنقولة المملوكة للغير.

ومن الواضح أن المسألة لا تثير إشكالاً في حال تطبيق هذا المفهوم على الأموال المنقولة المادية التقليدية، فالحديث عن حماية المعاملات الإلكترونية وفقاً للقواعد المقررة في جريمة السرقة بمفهومها التقليدي هو أمر محسوم سلفاً، وذلك في حال الاعتداء على المكونات المادية للنظام المعلوماتي[3]، ذلك أن الاستيلاء على المعلومات المخزنة في وسائل التخزين ذات الكيان المادي المحسوس كالدعامات والأشرطة والأقراص الممغنطة لا تثير أية صعوبة قانونية؛ لأن الدعامات المادية تعتبر مالاً منقولاً يخضع للحماية الجنائية بموجب النصوص العامة.[4]

إلا أن الإشكال الذي يطرح هو حالة وقوع هذه الجرائم على المادة المعلوماتية المكونة في شكل بيانات أو معلومات مخزنة داخل الجهاز أو التابعة للنظام المعلوماتي، وهي تأخذ شكلاً معنوياً غير ملموس، والأمر يتضح من خلال البيانات الإلكترونية المتعلقة بالمعاملات الإلكترونية المبرمة عبر شبكة الانترنت عبر وسائط الحاسوب[5]، فهنا تُثار إشكالية مفهوم المال المعلوماتي بسبب الطبيعة الخاصة لهذا الأخير، وتظهر مسألة الشك حول مدى اعتبار المال المعلوماتي الإلكتروني كشرط مسبق في جريمة السرقة؟

---

1 Article 311/1: le vol est la soustraction frauduleuse de la chose d'autrui" Code pénal français .

2 **نقلاً عن**: محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، الطبعة 2، 2009، ص 198.

3 Henri crose et yves Bismuth, le droit de l'informatique, Paris expertice.1984. p 151

4 نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقة)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2005، ص 158.

5 شيماء عبد الغني عطالله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، 2007، ص 45.

وفي الواقع نجد أن هذه الإشكالية القانونية قد أخذت نصيبها من الجدل على المستوى القضائي من خلال تدرج الأحكام القضائية الصادرة في هذا الصدد، والتي كانت تمثل المصدر الحقيقي لوجود أحكام تشريعية لاحقة، ولم يهمل الفقه بدوره دراسة هذه الفكرة ما بين معارض ومؤيد، وأما على المستوى التشريعي فقد ارتأت بعض التشريعات المقارنة وضع أحكام صريحة تترجم موقفها بشكل واضح من المسألة، بينما ظلت بعض التشريعات الأخرى يكتنفها الغموض مما استدعى وجود أحكام خاصة تبين موقفها من مسألة الاعتراف بقابلية المادة المعلوماتية كأموالاً معنوية منقولة تندرج تحت مظلة الحماية الجنائية المقررة وفقاً لنصوص العقوبات.

الفرع الأول: مدى اعتبار المعلومات والأموال الإلكترونية محلاً لجريمة السرقة على المستوى القضائي.

تبنت النصوص التشريعية جملة من الأحكام الصادرة عن القضاء والمتعلقة بتلك المسائل المستحدثة التي طفت على سطح النزاعات القانونية، فكانت الأحكام القضائية الصادرة فيها هي المصدر الرئيسي لترجمتها كقواعد تشريعية منظمة للمسائل المشابهة لها.

وهذا ما نستشفه من خلال التطور القضائي المتعلق بفكرة قابلية اعتبار المعلومات الإلكترونية أموالاً معنوية قابلة للتجريم في إطار القواعد التقليدية المنظمة لجرائم الأموال، وكذا مسألة تطبيق وصف المنقول على البيانات والمعلومات الإلكترونية حتى تتخذ وصف التجريم أيضاً, ومن ثم إسباغ الحماية الجنائية على مختلف المعاملات الإلكترونية التي تقع أساساً وفقاً لتداول تلك البيانات والمعلومات على المستوى الإلكتروني، فإلى أي مدى اعتبرت تلك المعلومات محلاً لجريمة السرقة وفقاً لأحكام القضاء؟

أولاً: رفض فكرة الاعتراف بقابلية المعلومات الإلكترونية لأن تكون محلاً لجريمة السرقة.

من خلال استقراء أحكام القضاء الفرنسي الصادرة في هذا الصدد، نجد أن أغلبها قد تبنى موقفاً رافضاً لاعتبار المنقولات المعنوية كمحل لجريمة السرقة، ولقد برز هذا الموقف من خلال الحكم الصادر عن محكمة استئناف باريس التي رفضت التماثل بين سرقة التيار الكهربائي وفك شفرة البرامج، ذلك لاعتبار التيار الكهربائي يحتاج إلى دعامة مادية للانتقال من خلالها، بينما يرد فك الشفرة على موجات عبر الأثير، وبالتالي ليس لها أي دعامة مادية لذلك أقرت المحكمة: "أن سرقة الكهرباء وسرقة البيانات المعلوماتية تفترض وجود دعامة مادية أيا كانت، الأمر الذي لا يتوافر في موضوع الدعوى"[1].

1 Cass. crim.3 Aout1918 ,bul. crime.N 450, cass. crim.8 janvier 1958, bul.crim N33.

ولقد ظل القضاء الفرنسي ولفترة غير قصيرة متبنياً للموقف الرافض لفكرة وصف الأموال على المعلومات المتداولة إلكترونياً واعتبارها بذلك محلاً لجريمة السرقة، وتأكيداً لذلك أقرت محكمة "غرونوبل" "Grenoble": "بعدم وجود ما يسمح بقيام جريمة سرقة الديسكات لعدم وجود أي دعامة مادية للمعلومات"[1].

يتبين من هذا الحكم أن القضاء الفرنسي يؤكد على ضرورة وقوع فعل الاختلاس على أشياء ذات صبغة ملموسة مادية ملموسة كي يقع عليها فعل الاستيلاء من طرف الجاني، رافضاً حكم التجريم على محل السرقة المتمثل في ملفات ومعلومات غير منسوخة على دعامة مادية، مع العلم أن المحكمة ذهبت في الدعوى السابقة إلى عدم استبعاد وقوع جرم التقليد في حالة نسخ تلك الملفات، بشرط توافر عنصر جريمة التقليد كالأصالة.

ثانياً: الاعتراف بفكرة سرقة المعلومات الإلكترونية.

لم تستمر أحكام القضاء الفرنسي على موقفها، حيث لوحظ تغير موقف القضاء من هذه القضايا، ولعل من أبرز أحكام النقض الفرنسي في هذا الصدد، المتعلقة بتجريم أحد المتهمين في قضية "لوجابكس" وهو أحد الذين تم فصلهم من أحد الشركات، بحيث قام المتهم بالدخول إلى مقر الشركة بغية تصوير مستندات خاصة بالشركة تثبت مدى استقرار المركز المالي والتجاري للشركة، وبالتالي إثبات الفصل التعسفي الذي مس العامل، وبهذا كانت الانطلاقة على مستوى الأحكام القضائية باطرادها على إقرار جريمة السرقة في حالة التصوير الفوتوغرافي للمستندات، وهو الحكم الذي ساد في القضاء البلجيكي باعتبار المعلومات الخاصة بالحاسب الآلي من قبيل الأموال التي تصلح محلاً لوقوع جريمة السرقة[2].

وبعد صدور جملة من الأحكام القضائية التي تعترف بقابلية المعلومات محلاً لجريمة السرقة نجد أن أحكام القضاء الفرنسي قد استقرت إلى موقف صريح من خلال حكمي "Bourquin" و"Antonioli"، الحكم الأول يتعلق بقضية عاملين بمطبعة "Bourquin" قاما بنسخ سبعة وسبعين قرصاً ممغنطاً يحتوي على معلومات بالغة الأهمية بغية إنشاء مؤسسة منافسة، وتم تأييد محكمة النقض للحكم الصادر عن محكمة

مشار إليه لدى: نائلة قورة، المرجع السابق، ص 145

1 Cass. Grenoble.4 mai 2000; Michel VIVANT et autre ,op. cite, p 1835

مشار إليه لدى :شيماء عطاالله عبد الغني، المرجع السابق، ص 62

2 Lucas (André); Deveze (Jean), Frayssinet (Jean), Droit de l'informatique et de l'internet, 2001, p 711.

الاستئناف القاضي بإدانتهما بسرقة المعلومات المخزنة على الأقراص الممغنطة، ويعد هذا الحكم واضحاً وجلياً من حيث تحديد المحل الذي تنصب عليه جريمة السرقة؛ ألا وهو المعلومات، وهو ما يعتبر سابقة قضائية تختلف عن جملة الأحكام السابقة التي اكتنفها الغموض في مسألة تجريمها لسرقة المستندات المادية أو المعلومات المخزنة داخل تلك المستندات كما في قضية "لوجابكس"[1].

أما الحكم الثاني فيتعلق بقضية "Antonioli" وهو محاسب إداري لدى إحدى المؤسسات، قام بتسليم الرسوم لإنشاء مؤسسة منافسة، وبهذا تمت إدانته من قبل محكمة الاستئناف بجريمة السرقة لقيامه باختلاس المعطيات التي تحتوي عليها المستندات, والتي تعد أموالاً معنوية مملوكة لرب العمل وتسليمها للغير[2].

وبناءً على ما ذكر، نرى أن الحكمين السابقين يشكلان ثورة فيما يتعلق بسرقة المعلومات ذاتها، فحكم محكمة النقض الصادر في قضية "Bourquin" واضح الدلالة على وقوع التجريم على المعلومات وحدها، دون الاستناد إلى الدعامة المادية، وهذا لوقوع فعل السرقة على المحتوى المعلوماتي للأقراص الممغنطة، كما يتضح لنا ذات الأمر بالنسبة للحكم الصادر في قضية "Antonioli" بالرغم من عدم وضوح ما إذا كان الحكم يتعلق بسرقة المعلومات، أو المستند المادي الذي احتوى المعلومات، إلا أن الملاحظ أن كلا الحكمين يشتركان في إشارتهما إلى أن المعلومات التي تم نقلها كانت ملكاً خالصاً لأصحاب المؤسسات، وبهذا نصل إلى أن المعلومات وحدها كانت محلاً لجريمة السرقة في الحكمين.

أما على المستوى التشريعي فلقد كان للطابع المعنوي لبعض المعلومات التي اعتبرت لها وزن قيم في المعاملات التجارية وراء إيجاد نصوص خاصة لتجريم التعدي على سر الصنعة والأعمال، ومثالها ما ورد في المادة 156-17 من قانون العمل الفرنسي والتي جاء فيها:" كل وسيلة للصناعة تقدم ميزة عملية أو تجارية أعدها صاحب الصنعة واحتفظ بها لنفسه بعيدا عن معرفة المنافسين له". وبذلك أورد تقرير اللجنة الأوروبية للمشكلات الجنائية التابعة للمجلس الأوروبي طلب تجريم الحصول بوسائل غير مشروعة أو إفشاء أو نقل أو استعمال بدون وجه حق لسر تجاري أو صناعي بنية إحداث ضرر اقتصادي للشخص صاحب السر[3].

1 أحمد حسام طه تمام، الجرائم الناشة عن استخدام الحاسوب، رسالة طنطا، مصر، 2001، ص 457.

2 عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2001، ص 156, نقلاً عن:

- P.Catala, les transformatique de droit par l'informatique émergence du droit de l'informatique et des parques, 1983, p264.

3 عبد الله حسين علي محمود، المرجع السابق، ص 261.

ونفس الحكم تبناه المشرع الألماني بمقتضى المادة 17-2 من قانون الجرائم الاقتصادية والتي نصت على أن: "يعاقب أي شخص حصل بدون إذن على سر تجاري أو صناعي وذلك بالاستعانة بوسائل فنية", وهذا كله يبرر ضرورة تدخل مجموعة من التشريعات بنصوص خاصة لإسباغ الحماية الجنائية للأموال ذات الطابع المعنوي، وخاصة أنها لم تحدد أنواع المعلومات محل الجريمة، وتركت الأمر مفتوحاً ليشمل حتى فكرة المعلومات الإلكترونية[1].

الفرع الثاني: مدى اعتبار المعلومات الالكترونية محلاً لجريمة السرقة على المستوى الفقهي.

إن الاعتداد بمفهوم الحماية الجزائية للمعاملات الإلكترونية يتأسس على مدى اعتبار المعلومات الإلكترونية ذات طبيعة تمكنها من الاعتداء عليها, لذلك ثار جدل فقهي كبير حول الحماية القانونية للمعلومات في حد ذاتها بمعزل عن الوسيط المادي الذي يمكن أن تندمج فيه، وقد أدى هذا الجدل المتقدم للتشكيك في توافر الحماية اللازمة لهذه المعلومات على الرغم من أنها تمثل العماد الرئيسي الذي تقوم عليه جملة التعاملات الإلكترونية, فهي الوسيلة التي تخلق التواصل وانتاج الصفقات والعقود عبر شبكة الانترنت، وبهذا الصدد انقسم الفقه بين مؤيد ومعارض لفكرة قابلية المعلومات باعتبارها محلاً يمكن الإعتداء عليه.

وقبل الخوض في الحديث عن الاتجاهات الفقهية التي تصدت لهذه الفكرة, يتوجب لزاماً إبراز الشروط اللازمة في نظر الفقه لتوفير الحماية القانونية للمعلومات الإلكترونية .

أولاً: شروط توفير الحماية القانونية للمعلومات الإلكترونية.

يعرف بعض الفقه القانوني[2] المعلومة بأنها: " مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلاً للتبادل والاتصال أو للتفسير أو التأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها ونقلها بوسائل وأشكال مختلفة".

تشريعياً نصت المادة الأولى من قانون الإمارات العربي الإسترشادي لمكافحة تقنية المعلومات وما في حكمها[1] أن المعلومة هي:" كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وغيرها."

1 محمد محمد شتا، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الاسكندرية، 2001، ص 23.

2 علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المكتبة القانونية، القاهرة، 1999، ص 58.

وحتى تتمتع المعلومات بالحماية القانونية لابد أن تتوافر بها –سواء كان التعبير عنها يتم من خلال وسيط مادي أم بمعزل عن هذا الوسيط – مجموعة من الشروط تتمثل فيما يلي:

1- **شرط التحديد:** تفتقد المعلومة لمصداقيتها في حالة افتقارها لعنصر التحديد، ذلك أن المعلومة هي تعبير وصياغة محددة تجعل الرسائل قابلة للتبليغ والتبادل عن طريق علامات أو إشارات، وتحديد المعلومات يرسم حدود التعاملات وجوانبها وهو يعتبر ضرورياً في حالة الاعتداء على الأموال؛ لأن الاعتداء يجب أن يقع على شيء محدد.

2- **شرط الابتكار:** إن أصل الحماية القانونية تقع على شرط ابتكار المعلومة؛ وذلك بأن ينسب إلى شخص محدد أو مجموعة من الأشخاص، وفي حالة افتقاد هذا الشرط يجعل من المعلومات المتداولة إلكترونياً ملكاً للجميع ولا يمكن الاحتجاج بمسألة الاعتداء على هذه المعلومات.

3- **شرط السرية والاستئثار:** إن اتسام المعلومة بالسرية يجعل منها محددة المجال، وبالتالي انحصارها في قالب خاص بالأفراد المتعاملين بتلك المعلومات، وبالتالي الإحتفاظ بخصوصيتها بعيداً عن الأفراد الآخرين ، وهذا يمكن من حيازتها من قبل الأفراد الناشئة عندهم فحسب وفي حالة خروج تلك المعلومة عن المجال المحدد لها فهي تفتقر إلى أهم الشروط الواجبة للتمتع بالحماية القانونية.[2]

وتعد خاصية الاستئثار بالمعلومة أمراً هاماً يجعل توافر هذا الشرط سلطة الشخص الفردية في التصرف بتلك المعلومات، وتحقق رابطة بينها وبين صاحبها، فتصبح المعلومات كأنها ملكاً خاصاً لأصحابها، لأن مختلف الجرائم التي تنطوي على اعتداء قانوني على الأموال، يعتدي فيها الجاني على حق يخص الغير على سبيل الاستئثار[3].

وبذلك نلاحظ أن توفر الشروط المذكورة يبين تقدير تلك المعلومات، الذي ينعكس غالباً على القيمة الاقتصادية لها، مما يكسبها قيمة مالية تصبح معها واجبة الحماية، بغض النظر عن الطبيعة المعنوية لها، وهو ما توافق عليه أغلب الفقهاء بالرغم من وجود اتجاه معارض لهذه الفكرة وهو ما سنحاول إبرازه فيما يلي:

---

1 قانون الإمارات العربي الاسترشادي لمكافحة تقنية المعلومات وما في حكمها, اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم 495- د 19- 2003/10/8 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 147- د 2004/21.

2 محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الاسكندرية، 2003، ص 46.

3 محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الأسكندرية، الطبعة الأولى، سنة 2014، ص 451.

ثانياً: الإتجاه الرافض لاعتبار المعلومات أموالاً تصلح لأن تكون محل لجريمة السرقة.

يتبنى هذا الإتجاه جانب من الفقه الفرنسي الذي يؤيد فكرة تطبيق المنهج التقليدي الذي يكسب صفة المال على الشيئ المادي وحده، وبالتالي ينفي أن تكون المعلومات المتداولة إلكترونياً محلاً لجريمة السرقة مسلماً بالطبيعة الذاتية لها[1]. ولقد برر أنصار هذا الاتجاه رفضهم بأن جريمة السرقة يجب أن ترد على حق الملكية وفعل الاختلاس يكون بالاعتداء على الحقوق المستأثرة للأفراد، والمعلومات في الأصل أنها ملكية عامة لا يمكن نسبتها لأحد[2].

وعلاوة على ذلك، يأخذ المحل في جريمة السرقة في الأصل طبيعة مادية، والخاصية المادية للأشياء هي التي تكسبها فرصة الاستغلال والاعتداء وانتقال الحيازة؛ أي أن الأشياء المادية المعنوية بطبيعتها غير المحسوسة يصعب الاعتراف بإسقاط السلطات المادية عليها كالملكية والحيازة.

ويزيد هذا الاتجاه من تبرير رفضهم قابلية المعلومة للسرقة من خلال افتراض وقوع فعل الاختلاس المكون في انتقال الحيازة من شخص لآخر، ولا يتصور بنظرهم ذلك إلا إذا وقع على الوسيط أو الإطار المادي الذي يتم تخزين المعلومات عليه، والحصول على المعلومة بطريقة غير مشروعة، ودون إذن صاحبها يبرر قيام جريمة التقليد، وهو ما يتطلب تجريمها بنص خاص يجرم فعل النسخ غير المشروع بعيداً عن فكرة الحيازة غير المشروعة.[3]

ثالثاً: الإتجاه المؤيد لاعتبار المعلومات أموالاً تصلح لأن تكون محلاً جريمة السرقة.

من خلال الجدل القضائي الذي تم عرضه سابقاً، تبين أن العديد من الأحكام القضائية قد تبنت فكرة قابلية المعلومات لأن تكون محلاً لجريمة السرقة من خلال الإعتراف بإعادة انتاج المعطيات المعلوماتية أو الاعتداء على المحتوى المعلوماتي للمستندات بشكل سلبي وغير شرعي المكون لجريمة السرقة، ومن وجهة نظر أنصار هذا الاتجاه أن الثورة التي أحدثتها تلك الأحكام تستند إلى جملة من الأسانيد:

- أن الاعتراف بفكرة تجريم سرقة المعلومات الإلكترونية لا يمثل اعتراضاً على مبدأ الشرعية الجنائية بل تأكيد لها، ففعل الاختلاس الواقع على المعلومات إنما يتحدد وفقاً لطبيعة الشيء محل السرقة، وهذا ما

1 Bertrand (R), la criminalité informatique, les délits relatifs au matérie,Receuil Dalloz-Sirey.n 62, expertise, 2001, p149.

2 مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، سنة 2001، ص 32.

3 عمر الفاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، ورقة بحثية قدمت في مؤتمر الكمبيوتر والانترنت، جامعة الإمارات (1-3 ماي 2000)، ص 32.

أكده القضاء الفرنسي، والاستيلاء على المعلومات قد يتحقق بالإطلاع أو النسخ غير المشروع ودون الرجوع إلى إذن صاحبها، وبذلك يكون الاعتداء موافقاً لطبيعة محل الجريمة[1].

- بعض التشريعات أقرت هذه المسألة من خلال الأحكام التي نصت على تعريف جريمة السرقة، كما هو حال المشرع الفرنسي والبلجيكي الذي أورد مصطلح "شيء" وهو الأمر الذي يوضح مرونة هذا المصطلح واتساعه ليضم معنى الأشياء المادية وغير المادية كالمعلومات, وبالتالي يتضح عدم ضرورة اعتبار محل جريمة السرقة أشياء مادية فحسب.
- يبرر أنصار هذا الرأي أن تطبيق النص الخاص بجريمة السرقة على المعلومات مجردة عن الوسيط المادي هو نتيجة منطقية للتطور القانوني لفعل السرقة، وترى الأستاذة "Delyssac" إذا استمرت فكرة النظر إلى قيام فعل الاختلاس في جرم السرقة بوجهها التقليدي الذي يقوم على فكرة انتقال الحيازة المادية من يد المالك إلى الجاني[2]، بالإضافة إلى أن فعل الاختلاس لا يقع إلا على الأشياء المادية دون غيرها؛ فإن ذلك يمثل قصوراً للفكر القانوني وتخلفاً عن ركب التطور الذي مس الأفعال الإجرامية بصفة عامة، وبالفعل المتعلق بجريمة السرقة بصفة خاصة، فالقواعد القانونية التقليدية المتعلقة بجريمة السرقة قد وضعت في وقت وظرف لاتقبل فيها إلا الشكل المادي لمحل السرقة[3].

ولكن مع تطور الوقت، ظهرت أساليب حديثة غيرت من تطبيقات السرقة، فنشأ مفهوم "سرقة المنفعة"، بحيث لم يعد الاختلاس يتم بمقتضى استئثار الجاني بشكل غير مشروع على جميع سلطات المالك على الشيء، وعلى إثرها ظهرت فكرة الاعتداء على المعلومة دون تحقق الوصف المادي للاعتداء على الحيازة[4].

ويبرر أنصار هذا الاتجاه أيضاً رأيهم من خلال نشوء فكرة حق الملكية على المعلومات الإلكترونية منفصلة عن الوسيط المادي، وهذا من خلال تمتع المعلومات بقيمة اقتصادية تترجمها في وصف المال، مثال ذلك جريمة سرقة بطاقة العملاء، التي اعتبرت من قبيل البضائع، وعليه تكتسب القيمة المالية نتيجة ما

1 هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، المرجع السابق، ص 52.

2 P.Catala, Op.Cite, p 509.

3 علي عبد القادر قهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر، جامعة الإمارات، العين، (1-3 ماي 2000)، ص 30.

4 محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، الأردن، سنة 2004، ص 197.

تحتويه من معلومات، وبالتالي تأخذ تلك المعلومات قيمة الأشياء المادية التي تكون محلاً لجريمة السرقة في التعاملات التجارية.[1]

بناءً على ذلك، نرى بأن فكرة الاعتراف بقابلية أخذ المعلومات وصف الأموال، هو من الرأي الصواب، فالواقع يثبت أن الأحكام القانونية التي تجرم الأفعال غير المشروعة يجب أن تأخذ فاعليتها وفقاً لأسلوب وشكل الفعل الإجرامي، وبهذا كان لزاماً النظر إلى جريمة سرقة المعلومات على أنها تمثل منحى خطير في ارتكاب الجريمة، مما يستدعي معه توافر حماية جنائية فعالة ضد أركان جريمة السرقة من فعل الاختلاس، ونية التملك في مجال المعاملات الإلكترونية، وهو ما ستتم دراسته في المطلب الثاني.

المطلب الثاني: أركان جريمة السرقة في إطار المعاملات الإلكترونية.

إن بلورة مفهوم أركان جريمة السرقة في إطار المعاملات الإلكترونية يستلزم بيان ركن الاختلاس الممثل للنشاط المادي الجريمة، بالإضافة إلى بيان خصوصية الركن المعنوي من خلال عنصري القصد الجنائي العام والخاص.

الفرع الأول: مفهوم الاختلاس كركن في جريمة السرقة في إطار المعاملات الإلكترونية:

ذهب العديد من الفقهاء إلى تعريف الاختلاس في جريمة السرقة بأنه انتقال حيازة المال محل السرقة من المالك إلى يد المجني عليه ويقتضي ذلك حرمان المالك من حيازة وملكية المال[2]، وبالتالي قد يأخذ فعل الاختلاس صفة الأخذ عنوة أو خلسة أو حتى الحصول على المال عن طريق اليد العارضة بتغير نية الجاني في الاستيلاء وتملكه، وهنا يظهر الجاني في مظهر صاحب السيطرة الفعلية على المال محل السرقة.

إن المفهوم الوارد أعلاه يتعارض مع فكرة سرقة المعلومات الإلكترونية؛ وذلك نظراً لصعوبة الاعتراف بانتقال حيازة المعلومات من يد إلى أخرى، ففعل الاختلاس في مجال المعاملات الإلكترونية يأخذ أساليب خاصة تتحقق بفعل الالتقاط الذهني للبيانات، وهو ما ينشأ عن حفظ وتخزين المعلومات بمجرد البصر أو السمع، أو الالتقاط الهوائي للبيانات المعالجة أو المنقولة, وهو ما يتماشى وطبيعة عمل ونظام أجهزة الحاسوب, وما يتصل بها من توابع تصدر أثناء تشغيلها بإشعاعات كهرومغناطيسية يمكن التقاطها وترجمتها

1 عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم اللكترونية)، منشورات الحلبي الحقوقية، سنة 2007، ص 15.

2 مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، سنة 2001، ص 146.

إلى بيانات مرئية، وكذا عملية نسخ ونقل المعلومات من النظام المعلوماتي، وهو ما يترجم فعل الأخذ من خلال اتخاذ فكرة النسخ للمعلومات المخزنة على الدعامات المادية.[1]

إن القول بسرقة المعلومات بفعل النسخ يوسع مفهوم فكرة الاختلاس التي لا تقتصر على الحرمان، وإنما تشكل اعتداء على حق صاحب المعلومة في الاستئثار بما يتضمنه من سرية وخصوصية لتلك المعلومات.

البند الأول: موقف القضاء من الإعتراف بركن الاختلاس.

إن من أولى المواقف التي استقرت عليها أحكام القضاء الاعتراف بفعل الاختلاس الوارد على المعلومات نظراً لصعوبة إثبات فعل انتقال الحيازة، ورفض اعتبار النسخ أو الاطلاع على المعلومات المسجلة بالحاسب الآلي مشكلاً لجريمة من جرائم الأموال، القضاء الأمريكي أصدر أحكاماً يستبعد فيها وقوع جريمة السرقة على عملية نسخ بيانات سرية تخص مرضى إحدى المستشفيات، وجاء الحكم مستنداً إلى عدم اعتبار الومضات الإلكترونية من قبل الأشياء المادية التي يرد عليها فعل السرقة[2]، وكذلك قضت محكمة استئناف باريس بأن استعمال جهاز التليماتك بدون وجه حق لا يصلح اعتباره فعلاً يشكل اختلاساً وبالتالي وقوع جرم سرقة الكهرباء[3].

لقد تردد القضاء الفرنسي في الإجابة على التساؤل الخاص بمدى توافر ركن اختلاس المعلومات الإلكترونية في قيام جريمة السرقة، ثم ما لبث أن طرأ تطوراً كبيراً في مفهوم الاختلاس يتلائم مع طبيعة المعلومات، وهذا بعد الحكم الصادر في قضية "لوجابكس"، بحيث يعد هذا الحكم من الأحكام الهامة التي اعترفت بسرقة المعلومات الإلكترونية, وتتلخص هذه القضية في قيام مهندس يعمل بمؤسسة "لوجابكس" الذي قام بنسخ مستندين على درجة كبيرة من السرية يتعلقان بالمؤسسة ثم قام بتقديم هذه الصور فيما بعد كدلائل في دعوى ضد المؤسسة، وحوكم المتهم بتهمة السرقة، إلا أن الحكم الصادر عن محكمة أول درجة ومحكمة الاستئناف قد أسستا حكمهما على عدم تحقق أركان جريمة السرقة؛ بحيث أنها لا ترى تحقق شرط الاختلاس الواقع على المنقول المادي، والذي رفضت معه انتقال حيازة المستندات إلى يد الجاني، وإنما

1 عبد الله حسين علي محمود، المرجع السابق، ص 261.

2 Cass. Crim 28 mars 1994, N 93-81.061, LAMY, ibid

3 P.Jean spreutels,les crimes informatique et d'autre crimes dans le domaine de la technologie informatique en Belgique, rev.int pénal.1993 p255

أسست الحكم على فكرة إعادة انتاج المستندات، وبالتالي تخلف الركن الخاص بطبيعة انتقال المستندات من يد المؤسسة إلى يد المتهم وظلت في حيازتها[1].

وعلى خلاف ذلك أقرت محكمة النقض الفرنسية إثبات تهمة السرقة على الجاني واستندت في ذلك إلى حكم المادة 379 من قانون العقوبات، فكيفت تصوير المستندات لأغراض شخصية ضد إرادة وعلم المؤسسة على أنه فعل يمثل الاختلاس على محل الجريمة، فيكون الأمر بنظر المحكمة استيلاء على المعلومات أثناء إعادة نسخ المستندات.

واعتبر الفقه أن الحكم الصادر بقضية "لوجابكس" هو استحداث لفرع جديد من جرائم السرقة؛ اصطلح عليه تسمية "سرقة المنفعة", ولقد اطردت محكمة النقض على مجموعة من الأحكام المشابهة التي أسست فيها تجريم فعل الاختلاس القائم على الحيازة الوقتية لإعادة الاستعمال[2].

البــند الثاني: الــموقف الفقهي مــن الإعتراف بركن الاختلاس.

لم تكن فكرة اختلاس المعلومات محل اتفاق بين الفقه، فقد أيده البعض وعارضه البعض الآخر، وجاء انقسام الفقه الفرنسي متماشياً مع التعارض القضائي السالف الذكر.

أولاً: قابلية المعلومات الإلكترونية للإختلاس.

استند أنصار هذا الاتجاه إلى قبول فكرة صلاحية وقوع الاختلاس على المعلومات الإلكترونية، والسبب في ذلك يرجع إلى تقبلهم فكرة اعتبار المعلومات أموالاً معنوية قابلة للتملك والحيازة، وبالتالي فهي قابلة أيضاً للأخذ والاختلاس والاعتداء عليها بأشكال أخرى، غير أن التمعن في هذا الرأي يرجعنا إلى سند منطقي آخر يبرر فكرة اختلاس المعلومة من خلال تشبيهها بسرقة الكهرباء التي تمثلها الومضات الكهربائية من خلال الأسلاك، وبهذا يمكن تحديد قيمة وكمية المعلومات المختلفة من خلال الدعامة المادية؛ وبالتالي يصلح فعل الاختلاس وتقوم كمحل لجريمة السرقة[3].

---

1 أحمد حسام طه تمام، المرجع السابق، ص 457.

2 مدحت عبد الحليم رمضان، المرجع السابق، ص 146.

3 نصت بعض التشريعات المقارنة بموقف صريح على اعتبار الطاقة الكهربائية كمحل لجريمة السرقة، واعتبرتها في حكم الأشياء المنقولة ومن ذلك قانون العقوبات الإيطالي في نص المادة 6/624 منه على أنه : (في تطبيق احكام قنون العقوبات يعتبر في حكم الشيئ المنقول الطاقة الكهربائية أو أية طاقة أخرى يكون لها قيمة اقتصادية)، وقانون العقوبات السوداني نص في المادة 320 من على أنه:" يعتبر مرتكبا لجريمة السرقة كل من يختلس أو يحاول أو يستهلك أو يستعمل الكهرباء أو أي تيار كهربائي بسوء قصد". **انظر:** محمد الكعبي، المرجع السابق، ص 207.

ولقد برر مؤيدو هذا الاتجاه القائل بفعل الاختلاس على المعلومة باعتقادهم وقوع فعل الاختلاس المؤقت الذي جاء وفقاً لنظرية الفقيه"Garçon"، والتي تقوم على أساس قيام فعل السرقة في أي حالة يتم فيها حرمان المالك أو الحائز بالانتقال المادي، ويكتفي في ذلك المساس بمحتوى المعلومات ليتحقق الانتقاص من قيمتها المعنوية، وهو ما يؤسس فكرة "سرقة الاستعمال أو المنفعة"، والذي يبرر الاعتراف بوقوع النشاط الإجرامي وفقاً لطبيعة المال المختلس، وبهذا فإن فعل الاختلاس الخاص بالمعلومات هو في الحقيقة الاعتداء على حق صاحبها في الاحتكار باستغلالها[1].

وبالنظر إلى طبيعة المعلومات كأموال معنوية لأمكن القول أن ذلك فرضاً يخلق مبرراً لوقوع فعل الاختلاس من جنس الشيء محل الاختلاس، فالأشياء المعنوية يمكن اختلاسها باستخدام نشاط مادي كعملية النسخ أو التصوير الذي يتم عن طريقها انتقال المعلومة من الأصل إلى الصورة، كما قد يتوفر نشاط الاختلاس المعلوماتي الذي يتم بواسطة وسائل النظم المعلوماتية، أو تعديل المعلومات الموجودة فيها أو مسحها، وذلك بغية تحقيق العناصر الإيجابية في الذمة المالية للجاني، وبالتالي تتحقق سيطرة الجاني على الأموال بإخراجها من ذمة المالك وإدخالها ذمته، من خلال النظر إلى ما تملكه تلك المعلومات أو البرامج أو البيانات من قابلية للانتقال، واستحواذها على قيمة اقتصادية أو مالية كبيرة تطرح للتداول في السوق مثلها مثل السلع والبضائع[2]، وبهذا تتحقق وجهة النظر القائلة بأن رفض إضفاء وصف الاختلاس على شيئ له قيمة اقتصادية؛ هو بلا جدال رفض مبني على البعد عن الواقع, وبالتالي يعتد بالمعلومة كأموال معلوماتية واجبة الحماية جنائياً من كل أفعال الاعتداء الواقعة عليها.

ثانياً: عدم قابلية المعلومات للاختلاس.

يستند أنصار الإتجاه الرافض لقابلية المعلومات للاختلاس إلى الفكرة المادية للاختلاس، والتي تقوم عليها جرائم السرقة في وجهها التقليدي، بحيث يرون ضرورة تحقق الفعل المادي المتمثل في نقل الشيء أو أخذه أو نزعه من مالكه، متضمناً تغييراً في الحيازة القانونية، وحتى في الحالات التي يتحقق فيها الاختلاس دون نزع الشيء من مالكه؛ لأنه تحت اليد العارضة للجاني لا ينفي ذلك عن المحل صفته المادية، فاليد العارضة تفترض وجود الشيء بين يد الشخص, ويعد ذلك دليلاً على ماديته[3].

1 عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة (دراسة مقارنة)، جامعة الاسكندرية، سنة 2000، ص 135.

2 أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، الطبعة 2، 2006, ص 255.

3 جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، الطبعة 1، 1992، ص 69.

ونجد في الحكم الصادر عن المحكمة العليا بكندا المتعلق بقضية "Stewart" سنداً للرأي المتقدم، حيث قضت المحكمة أن: "اختلاس المعلومات منفصلة عن إطارها المادي، سواء تم ذلك عن طريق تخزينها في الذاكرة أو طباعتها، فإن المالك المزعوم لهذه المعلومات لا يتجرد من حيازتها، ولا من جميع السلطات التي له عليها، فكل ما يفقده هو سرية تلك المعلومات، ولهذا فإن المعلومات لا يمكن أن تكون محلاً للاختلاس"[1].

كما أن افتراض فعل الاختلاس يفترض حتماً مع وجود المادية توافر صفة المنقول، وبهذا ففي إطار التعاملات الإلكترونية تأخذ المعلومات أشكالاً عديدة من حيث تناولها, بالرغم من أن مسألة انتقال تلك المعلومات تفترض دائماً وجود دعامات مادية، وإلا كان الأمر متعلقاً بالاعتداء على الخدمات وليس الأموال، حتى لو استعمل في الاعتداء وسائل لاعتراض تلك المعلومات كسرقة كلمة السر أو استخدام أساليب احتيال أو غش، فالمعلومات المخزنة في النظام المعلوماتي لا تأخذ صفة المنقول؛ لأنه لا يتصور نقلها من يد لأخرى[2].

وبتحليل وجهتي النظر السابقتين، نميل للاعتقاد القائل بقابلية وقوع المعلومات تحت جرم الإختلاس، وهذا إذا عمقنا النظر في طبيعة وحداثة الجرم في حد ذاته الذي يفرض مواكبة هذا الأسلوب الحديث بالجريمة، إيجاد حلول تتماشى وهذا النمط، وهو ما يدفعنا إلى التسليم بالخروج عن القواعد التقليدية من حيث الرجوع إلى الشرط والنتيجة، والإعتراف بالحلول التي تضمن لنا تفعيل الحماية الجزائية دون التعصب للقاعدة التقليدية، ونتجاهل ما هو أهم؛ والمتمثل في ضرورة التحديث بالتوازن مع مبدأ عدم التوسع في الشرعية الجنائية، وهو ما حاول أغلب التشريعات فعله من خلال استحداث قواعد تجريم الاعتداء على المعلومات في مجال المعاملات الإلكترونية من خلال صبها في قالب القواعد التقليدية، مع إيجاد حكم يتماشى وطبيعتها في نفس الوقت.

ونجد أن المشرع الجزائري قد جاء بنص المادة 350 قانون العقوبات الذي أقر فيه مصطلح "شيء" الذي يعتبر مفهوماً مرناً يتماشى مع الأموال المعلوماتية, وكذا استحداث نص المادة 394 مكرر من قانون العقوبات الذي جاء بحكم تجريم الاعتداء على البيانات والمعلومات المعالجة آلياً، والتي تهدف أساساً إلى

1 A. Bensoussan,le vol programmés et des fichiers, un grand malentendu, exparties ,février, 1981, p 15.

2 Jean Pradel, les infractions relatives à linformatique, revue international de droit comparé vol. 42 n 2 avril juin 1990.Etudes de droit contemporain, p 822.

حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق كذلك وبصورة غير مباشرة حماية للمعلومات في حد ذاتها.

الفرع الثاني: الركن المعنوي في جريمة السرقة في مجال المعاملات الإلكترونية.

من بين ما تنص عليه القواعد العامة لجريمة السرقة هو ضرورة توافر الركن المعنوي والمتمثل في القصد الجنائي، حيث يتحقق القصد العام في جريمة السرقة في إطار المعاملات الإلكترونية بتوافر عنصري العلم والإرادة، فيجب أن يعلم الجاني بأن المال ليس ملكاً له، وأن تتجه إرادته إلى ارتكاب فعل الحيازة وتحقيق النتيجة الإجرامية، ذلك أن عدم توافر عنصر الإرادة ينفي القصد الجنائي، ولا تقع جريمة السرقة إلا بتوافر نية حرمان المالك من سلطاته الفعلية كمالك، وحلول الجاني محله في ممارسة هذه السلطات، وتتحقق مظاهر هذه النية بقيام المتهم بممارسة السلطات التي لا تصدر إلا من مالك؛ وهي سلطة الاستئثار بالشيء وسلطة التصرف، عندئذٍ يكون المتهم قد ظهر على الشيء بمظهر المالك وتجسدت لديه نية التملك[1].

ويذهب رأي[2] إلى أن سحب العميل مبالغ تجاوز رصيده لا يعتبر سرقة على أساس أن البنك قد فتح اعتماداً لمصلحة العميل لاعتقاده أنه ملكه، فهو بذلك لم يتوافر لديه القصد الجنائي في تملك أموال غير مستحقة.

بالإضافة إلى جملة الصعوبات المتعلقة بالنشاط الإجرامي الواقع في مجال المعاملات الإلكترونية تثار صعوبة أخرى تخص الركن المعنوي في جريمة السرقة، ويتعلق الأمر بمدى توافر القصد الخاص المتمثل في نية التملك للمعلومات أو الأموال الإلكترونية، وفي الواقع فإن النية المقصودة هنا هي اتجاه إرادة الجاني إلى الإستيلاء على المعلومات الخاصة بالمعاملات الإلكترونية بغية الاحتفاظ بها من أجل استخدامها لأغراض غير مشروعة تضر بمصلحة المجني عليه[3].

وبهذا فإن الرجوع إلى القصد الخاص في إطار جرائم السرقة التقليدية لا يثير أي صعوبة؛ على اعتبار أن محل السرقة هو أشياء مادية قابلة للتملك والحيازة، وفعل الاختلاس الذي يصدر من الجاني يصب في اتجاه نيته السيئة بالاستيلاء على الأشياء محل السرقة، وحرمان صاحب الحق من أوجه السيطرة عليها، بالإضافة إلى عنصري العلم والإرادة.

1 غنام محمد غنام، شرح قانون العقوبات (القسم الخاص)، منشورات جامعة المنصورة، مصر، سنة 2004، ص 458.

2 محمود محمود مصطفى، شرح قانون العقوبات (القسم الخاص)، دار النهضة العربية، القاهرة، 1984، ص 480.

3 هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، سنة 1992، ص 235.

لكن وبإسقاط ذلك على بيئة المعاملات الإلكترونية، وتعمقنا في تصور قيام الجريمة على المستوى الافتراضي بغياب التواجد المادي بين أطراف المعاملات؛ فإننا نصطدم بفكرة مدى قيام نية الشخص في الاعتداء على المعلومات والبيانات المتعلقة بالمعاملة الإلكترونية بغرض التملك، وحرمان المجني عليه منها، مع العلم أن مجرى الفعل الإجرامي في الإطار الإلكتروني هو في الحقيقة اعتداء ضبابي لا يظهر بمظهره الحقيقي, ولا يكشف مسار الفعل الإجرامي لمرتكب الفعل، فغالب الاعتداءات تتمحور في فعل اختلاس المعلومات مع بقاء المعلومة لدى المجني عليه، فالاعتداءات المشكلة في سرقة أرقام بطاقات الدفع أو الائتمان هي لا تظهر نية الشخص في تملك المعلومة على اعتبار أن الجاني يستولي عليها دون الانتقاص من فكرة حيازتها أو ملكيتها للمجني عليه[1].

وبالرغم من ذلك، إلا أن الفقه الجنائي يتجه إلى الاعتراف بوجود وقيام القصد الخاص لجريمة السرقة من خلال النظر إلى الجريمة بطبيعتها؛ التي تفرض النظر إلى المعلومات الخاصة بالمعاملات الإلكترونية على أنها ذات أهمية مالية واقتصادية كبيرة لأصحاب تلك المعاملات، ونية الشخص في التملك تظهر من خلال الاعتداء على ملكية حق الاستئثار بتلك المعلومات، ومن ثم التوجه إلى استغلالها بالشكل الذي يضر مصلحة المجني عليه[2].

وهذا الفرض في الحقيقة يتماشى مع عين المنطق التي تقر بقيام الفعل الإجرامي أولاً في ركنه المتعلق بالنشاط الإجرامي؛ المتمثل في اختلاس المعلومة، والذي يكمله الركن المعنوي باتجاه الجاني إلى الاستيلاء على المعلومات بكامل علمه وإرادته، ضف إلى ذلك النية في تملك تلك المعلومات، وهو الهدف من ارتكاب الجريمة أصلاً، فلا مجال للحديث عن قيام الركن المادي دون أن يكمله الركن المعنوي.

إن النظر إلى توافر القصد الخاص في الجرائم المتعلقة بالمعاملات الإلكترونية يبرز لنا مدى سهولة إثباته, على اعتبار أن نية التملك هي ظاهرة بشكل واضح في المجال الإلكتروني، بحيث تبدأ الجريمة بالبقاء داخل الأنظمة المعلوماتية، ومن ثم الاعتداء على البيانات والمعلومات الخاصة بالمعاملات الإلكترونية، وهو ما يفسر سلوك الشخص بالاستحواذ على تلك المعلومات فيما بعد[3].

1 محمد حماد مرهج الهيتي، المرجع السابق، ص 199.

2 هدى حامد قشقوش، المرجع السابق، ص 62.

3 أحمد خليفة الملط، المرجع السابق، ص 274.

المبحث الثاني:

الحماية الجزائية من جريمة الاحتيال في إطار المعاملات الإلكترونية.

إن جريمة الاحتيال الواقعة في مجال المعاملات الإلكترونية؛ أو ما يطلق عليه أغلبية الفقهاء بمصطلح "الاحتيال الإلكتروني"، هي من أهم الجرائم الواقعة على الأموال، والأكثر انتشاراً نظراً لتشعب أساليب ارتكابها، وارتباطها بقضايا عديدة ذات طابع واقعي، وعلى هذا الأساس ذهبت العديد من التشريعات المقارنة إلى إصدار تشريعات خاصة لمواجهة هذا النوع من الجرائم، فهي قائمة على ذات العناصر والأركان التي تقوم عليها جرائم الاحتيال التقليدية، مع الاختلاف في أساليب وأدوات ارتكابها، بالمقابل يوجد بعض التشريعات التي أغفلت إصدار نصوص تتماشى وتنظيم هذه الجريمة في إطار المعاملات الإلكترونية، ومن بينها المشرع الجزائري، فكان لزاماً دراسة مدى إمكانية تطبيق نصوص التجريم التقليدية على هذه الجريمة، والبحث والتمحيص في المشكلات التي يثيرها هذا التطبيق من خلال تبيان الجدل الفقهي والقضائي في هذا الصدد.

المطلب الأول: مضمون جريمة الاحتيال الإلكتروني.

تعد جريمة الاحتيال الإلكتروني من أبرز الجرائم التي صاحبت التطور التكنولوجي والتي مست بشكل كبير مجال التعامل الإلكتروني؛ نظراً لتشعب صورها وتعدد وسائل ارتكابها، وقد عرفت انتشاراً كبيراً في البيئة الإلكترونية نظراً لمساهمة طبيعة هذه الأخيرة في وجود آليات وسبل ارتكاب الاحتيال بشكل يضمن معه الجاني التخفي والسرعة في طمس معالم الجريمة, وهوما يجعل من مسألة المكافحة التشريعية لها أمراً ضرورياً وهذا ما سيتم دراسته من خلال الفروع التالية:

الفرع الأول: تعريف جريمة الإحتيال في مجال المعاملات الإلكترونية.

تأتي جريمة الاحتيال من خلال كل السلوكات التي تنطوي على خداع المجني عليه بغرض الاستيلاء على أمواله، وتتنوع صور تلك السلوكات بين كذب، أو تضليل للحقيقة، أو تزييف مصحوب بوقائع خارجية تفسر نية الجاني في إيقاع المجني عليه في غلط، أو إيهام يغير الواقع حتى يتسلم المال المملوك لديه[1].

يذهب الشيخلي في تعريفه للاحتيال إلى الحيازة وليس التملك، فيعرف جريمة الاحتيال على أنها توصل الشخص إلى تسليم أو نقل أو حيازة مال منقول مملوك للغير إلى حيازة شخص آخر، وذلك باستخدام طرق احتيالية، أو باتخاذ اسم كاذب، أو حمل آخر على تسليم أو نقل حيازة سند محدد أو إبراء[2].

ومع تطور المنهج المؤدي إلى السرعة اللامتناهية في حدود الإجرام بدأ يأخذ جرم الاحتيال شكلاً يتماشى وما أقرته التكنولوجيا والتطور التقني في المجال الافتراضي، ليبزغ الاحتيال الإلكتروني إلى الوجود عاصفاً بالقواعد والأسس التقليدية للجريمة[3].

الفقه الجنائي بدوره حاول الإحاطة بمفهوم الجريمة معتبرين إياها أحد أصعب أنماط الجرائم التقليدية التي أخذت بعداً كبيراً في المجال الإلكتروني؛ كونها الأكثر تعقيداً، والأسرع تطوراً، والأكثر شيوعاً. فيعرفه "آل

---

1 تيسير أحمد حسين الزعبي، الاحتيال الإلكتروني، رسالة ماجيستر في القانون العام، كلية الحقوق، جامعة جدارا، الأردن، 2009-2010، ص 14.

2 عبد القادر الشيخلي، التشريعات العربية لمواجهة جرائم الاحتيال المعاصرة، ورقة بحثية مقدمة لمركز الدراسات والبحوث،جامعة نايف العربية للعلوم الأمنية، الرياض، 2015، ص 28.

3 بدر بن أحمد بن محمد الزهراني، جريمة الاحتيال الإلكتروني في النظام السعودي، رسالة ماجيستر في الشريعة والقانون، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2015، ص 23.

ديبس" بأنه:" كل تظاهر أو إيحاء يكون صالحاً لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي", وهنا تؤسس جريمة الاحتيال الإلكتروني على ما انطلت عليه حيلة الجاني باستخدام الحاسب الآلي وشبكة الانترنت فيتحقق عنصري الخداع وتسليم المال[1].

وبتمعن المفهوم السابق نجد أنه قد حصر مكونات جريمة الاحتيال على عناصرها التقليدية، مع إدخال الوسيلة المستحدثة والمستخدمة فيها، والمتمثلة في جهاز الكمبيوتر وشبكة الانترنت، مع العلم أن ماهية الاحتيال الإلكتروني تقوم بالاعتماد على خصوصية المجال الافتراضي الذي تقع من خلاله، فالنمط التقليدي يفترض وجود احتيال واقع بين أشخاص، بينما الاحتيال الإلكتروني يحمل معنى أوسع وأشمل؛ يتمثل في خداع الأشخاص مروراً بخداع الأنظمة المعلوماتية بوجه كامل.

ومن المستقر عليه في التشريعات المقارنة أن الهدف من وضع نصوص تشريعية تجرم هذا الفعل هو حماية حق الملكية حيث يتمثل الاعتداء في نية سلب ثروة الغير كلها أو بعضها، وبالإضافة إلى حماية حق الملكية يذهب المشرع بتجريمه للاحتيال لتحقيق مصلحة أخرى هي حرية الإرادة وسلامتها، وتتمثل حمايته لسلامة الإرادة في تجريمه أسلوب الاحتيال الذي يلجأ إليه الجاني، فيوقع به المجني عليه في الغلط، فيسلمه المال محل الجريمة تحت سيطرة الغلط.[2]

وبالمقارنة بين الاحتيال في صورته التقليدية وبين الاحتيال في صورته المستحدثة التي تتمثل في الاحتيال الإلكتروني، نجد أن جوهرهما واحد؛ ففي كلتا الحالتين يمارس الجاني وسائله الاحتيالية للاستيلاء على مال الغير، بينما يكمن الفرق بينهما في محل السلوك الإجرامي من ناحية، وفي نوع الوسائل الاحتيالية التي يلجأ إليها الجاني من ناحية أخرى.

أما بالنسبة لمحل الاحتيال الإلكتروني فيتمثل في جملة المعلومات والبيانات التي تمثل قيمة مالية أو اقتصادية داخل نظام إلكتروني لمعالجة البيانات، وترتكز أغلب حالات الاحتيال الإلكتروني بالتلاعب بمثل هذه المعلومات المتعلقة بالفواتير والأرصدة البنكية والحسابية، وأرقام الأرباح المتعلقة بالصفقات المالية والتجارية والتي أصبحت تمثل مجالات خصبة للنصب، خاصة بعد اتجاه الدول المتقدمة إلى ما يسمى

1 Voir : Raymons gassin, le droit pénale de l'informatique, Dalloz, Paris,1986, p 40.

2 إبراهيم بشارة عواد السويلمين، جريمة الاحتيال عبر الشبكة الدولية (دراسة مقارنة)، أطروحة دكتوراه في القانون العام، جامعة عمان العربية للدراسات العليا، عمان، 2009، ص 45.

"بمجتمع اللانقود" حيث أصبح نظام الدفع سواء في قطاع المال أو الأعمال أو حتى محيط الأفراد يعتمد أساساً على ما يسمى بأوامر تحويل الأموال[1].

ويلاحظ أن ما يميز الاحتيال في مجال المعاملات الإلكترونية هو الاستعانة بأجهزة الحاسوب كوسيلة للاحتيال وكمحل له، وكذا جميع الوسائط التي تسهل تنقل المعلومات الإلكترونية من خلالها كشبكة الانترنت التي كان لها الدور الفاعل في خلق بيئة مرنة وسهلة التفاعل مع هذا النوع من الجرائم، لذلك لجأت الكثير من التشريعات المقارنة لتضمين تشريعاتها نصوصاً خاصة تعاقب على الغش المعلوماتي، غير تاركة الأمر للقواعد العامة، تحذوها الرغبة في إزالة الشك حول تطابق تجريم الاحتيال مع الاحتيال الإلكتروني والرغبة في تشديد الجزاء.

ولقد أشار المشرع الجزائري إلى جريمة الاحتيال من خلال نص المادة 372 من قانون العقوبات حيث نص: " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو الحصول على أي منها أو شرع في ذلك بالاحتيال لسلب كل ثروة الغير أو الشروع فيه"، ويتضح من خلال هذا التعريف أن المشرع قد أفضى إلى تحديد النشاط الإجرامي لجريمة الاحتيال من خلال حصر السلوكات المشكلة لهذه الجريمة في استلام أو التوصل لمال الغير، الذي تختلف طبيعته من نقدية أو تصرفات أو ووعود أو مخالصات أو إبراء أو التزامات، كما ذهب إلى تحديد الوسائل التي تم بها الحصول على المال محل النصب بتحديد أشكال الاحتيال التي تقوم من خلالها الجريمة، وبالرغم من أن هذا التوسع يساعد في تفسير السلوك الإجرامي في مجال المعاملات الإلكترونية، بالرغم أن النص لم يتطرق مباشرة للاحتيال الواقع بأحد الأساليب غير التقليدية.

وهو نفس موقف المشرع الفرنسي الذي جاء تعريفه أوسع لجريمة الاحتيال؛ حيث نص في المادة 313-1 من قانون العقوبات بأنه :"الفعل الذي يتم باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعمال غير المشروع لصفة صحيحة، أو باستعمال الطرق الاحتيالية، وذلك لخداع شخص طبيعي أو معنوي، وحمله على تسليم نقود أو قيم أو مال أو تقديم منفعة، أو قبول تصرف ينطوي على التزام أو مخالصة، وذلك إضرارا بالمجني عليه أو الغير"[2].

1 محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، بيروت، الطبعة الاولى، سنة 2011، ص 62.

2 Article 313-1 du CPF: " L'escroquerie est le fait; soit par l'usage d'un faux nom ou d'un fausse qualité,soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la determiner ainsi, a son prejudice d'un tiers, a

ومن هنا نلاحظ توجه المشرع الفرنسي إلى التوسع في حكم جريمة النصب بعدم اقتصارها على عنصر المال لتشمل عنصر الخدمات، ضف إلى أن استخدام المشرع لمفهوم "القيم" هو دلالة اتجاه المشرع لإسقاط الحكم على القيم المادية أو المعنوية على حد سواء، ما دام قد ترك المصطلح موسعاً، ومن هنا يصلح تطبيق مصطلح القيمة على العناصر ذات الطبيعة المعنوية والقيمة الاقتصادية أو المالية ما يسمح بإسقاط الحكم على المعاملات الإلكترونية.

ولقد نجح مفهوم جريمة الاحتيال الإلكتروني في جذب انتباه العديد من الباحثين والدارسين في مجال الجريمة الإلكترونية[1]، ويرجع السبب في ذلك إلى عدد من العوامل يأتي في مقدمتها الارتفاع المستمر في معدلاتها، ما أدى إلى حدوث خسائر ضخمة تقدر بحوالي 2.5 بليون دولار في عام 2017 بزيادة تتمثل في 30% مقارنة بمعدل عام 2015 وذلك حسب ما نشرته وكالة "إيمس" في نشرتها الدولية بالو.م .أ[2]

الفرع الثاني: صور الاحتيال في مجال المعاملات الإلكترونية.

لكي تتضح معالم الاحتيال في مجال المعاملات الإلكترونية، نوضح بعض أنواع أساليب الاحتيال الواقعة في المجال الافتراضي، خاصة تلك التي يتم فيها الاستناد إلى شبكة الانترنت للمساعدة في تسهيل عمليات تداول المال والأعمال، مع العلم أنه من العسير حصر أساليب الاحتيال عبر الانترنت ولكن يمكن تصنيف أبرز صور هذا الاحتيال؛ كالاحتيال التجاري، والاحتيال عن طريق البريد الالكتروني، والاحتيال الواقع على أموال المصارف والاستثمارات.

والحقيقة أن هناك صورة بارزة من صور الاحتيال الإلكتروني؛ هي الاحتيال عن طريق بطاقات الدفع الإلكتروني، إلا أننا ارتأينا إرجاء دراستها للفصل الثاني على اعتبار أنها نوع من جرائم الاحتيال المستحدثة التي برزت أساساً نتيجةً لظهور المعاملات الإلكترونية واستخدام شبكة الانترنت.

---

remettre des fonds, des valeurs ou un bien quelconque a fournir un service ou consenter un acte apérant obligation ou décharge l'escroquerie est puni de cinq ans d'emprisonnement et de 75000 euros d'amande".

1 نائلة قورة، المرجع السابق، ص 174. **انظر أيضاً:**

- Linat De Bellefonds(xavier) et Hollande (Allain), Droit de l'informatique et de la télématique, Ed des parques, 1983, p 52

2 جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002، ص 32.

أولاً: الاحتيال التجاري المباشر.

تتم المعاملات التجارية الإلكترونية عبر شبكة الانترنت وفق خاصية السرعة والكفاءة، بالرغم من المخاطر المحيطة بمثل هذه المعاملات، فغالباً ما يتيح عنصر السرعة في إجراء الصفقات التجارية على الخط، تسهيلات لحدوث أفعال احتيالية، وذلك نتيجة لعدم وجود فرص انتظار بين أطراف المعاملات، مما ينتفي معه دليل مؤكد على أهمية الموضوع أو تعريف كافي للطرف الآخر في الصفقة[1].

وطبقاً لإحصائيات لجنة التجارة الفيدرالية ولجنة مراقبة الاحتيال عبر الانترنت، فإن هذه الطريقة في الاحتيال تعد الأكثر انتشاراً في العالم الافتراضي.

وفي قضية شهيرة تمت في مقاطعة جورجيا الأميركية، أدانت المحكمة أربعة متهمين وذلك لقيامهم بأفعال احتيال عبر موقع e-bay حيث قاموا باستخدام الموقع لبيع إطارات السيارات، وقام الزبائن بالتفاوض على السعر والدفع عن طريق تحويل الأموال عبر الانترنت، أو عبر موقع "ويسترن يونين" ولكن البضائع لم ترسل للضحايا، ومنذ عام 2013 حتى عام 2016 دفع حوالي 215 شخصاً للمتهمين ما يعادل 539,000 دولار ثمنا لبضائع لم يتم إرسالها[2].

ولتفادي عمليات الاحتيال عند الشراء عبر الانترنت، فإن هذه الشبكة تقدم خدمة يطلق عليها "Escrow House"، وهي عبارة عن مؤسسات مالية تتكفل بمهمة تسلم الأموال من المشترين من مواقع تجارية عبر الانترنت وتجميدها لديها، حتى يصلها إخطار من المشترين يؤكد تسلم المنتجات المطابقة للمواصفات المطلوبة، وبهذا تعمل المؤسسات على تحويل الأموال إلى المواقع التي تم الشراء منها، وفي حالة عدم وصول المنتجات التي طلبها الزبون أو كانت غير مطابقة للمواصفات، فإنه يمكن استرداد تلك الأموال[3].

ثانياً: الاحتيال المصرفـــي.لقد أتاحت الانترنت لعملاء المصارف والبنوك الاطلاع على حساباتهم وإجراء تحويلات المالية من خلال المواقع الإلكترونية العائدة لهذه المصارف، بالرغم من هذه المعاملات لم تسلم من أيدي قراصنة الانترنت من خلال اقتحام تلك المواقع والاعتداء على كشوف وحسابات العملاء،

---

1 محمد شناوي، جرائم النصب المستحدثة، دار الكتب القانونية، القاهرة، 2008، ص 88.

2 Richard Hillman, securities fraud, the internet poses challenges to Regulaters and Inverstors, United States General Accountig office, 2017, p5

- **مشار اليه لدى:** محمد طارق الخن، المرجع السابق، ص 52.

3 أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر، الأردن، 2009، ص 136.

ونقل تلك الأموال إلى حساباتهم الشخصية، وهذا من خلال الحصول على بعض الوسائل المرتبطة بحماية المعلومات مثل كلمات المرور، وتفاصيل الحسابات، والتي يتمكن من خلالها المحتالون من الوصول إلى قواعد البيانات الخاصة بشركات الأعمال والمؤسسات المالية.

ثالثاً: الاحتيال في الأســـــهم والاستثمار.

أدى النمو السريع للتعاملات الإلكترونية بعد انتشار شبكة الانترنت إلى تغييرات هامة في مجال المال والأعمال، بحيث يستخدم الانترنت حالياً بشكل أكثر تنظيماً في كافة أنشطة الشركات التي تتسع من مجرد تقديم العروض والتجارة في الأسهم، ويلاحظ المراقبون تزايد شعبة الانترنت عند المستثمرين، لأنها تسمح لهم ببيع وشراء الأسهم عن طريق حواسيبهم الشخصية مع نسب منخفضة من العمولات التجارية[1].

إن هذا النوع من التعاملات أفرز أنماطاً جديدة من الاحتيال ترتبط بسوق الأسهم، ويعد الأسلوب الأكثر انتشاراً في هذا النوع من الاحتيال هو استخدام الانترنت لنشر معلومات وهمية لجذب المستثمرين، فيعمل المحتالون على نشر معلومات كاذبة عن أسهم بعض الشركات لكي يزيدوا من شراء المستثمرين، وهذه الزيادة في الطلب تزيد من قيمة الأسهم، وغالباً ما يكون هؤلاء المحتالون يملكون كميات كبيرة من هذه الأسهم، حيث يحصلون على ربح سريع عند بيعها بسعر مرتفع, وبالمقابل فإن المستثمرين الذين اشتروا هذه الأسهم بناء على المعلومات الوهمية سيواجهون خسارة فادحة عندما يقومون بالبيع[2].

ومن أمثلة هذا الأسلوب من الاحتيال أن أحد سماسرة البورصة، أطلق إعلاناً يحث فيه الزبائن لوضع أموالهم للاستثمار؛ نظراً لأنه قادر على تحقيق أرباح ضخمة، وذلك باستخدام برنامج حاسوب سري يعمل ضمن الحاسوب الضخم في بورصة "وول ستريت"، وبالرغم من أنه لم يكن لديه البرنامج المزعوم للدخول إلى الحاسوب المذكور، قفد اقتنع مئات الزبائن باستثمار لا يقل عن 100,000 دولار لكل منهم[3].

رابعاً: الاحتيال الـهرمـــي.

يعتبر الاحتيال الهرمي من أبرز أنواع الاحتيال الإلكتروني التي برزت في السنوات الأخيرة، وهي عبارة عن برامج تسويقية واستثمارية احتيالية، يتم بموجبها مكافأة المشاركين عند إقناعهم لأشخاص آخرين بالإنضمام لهذه البرامج التسويقية، ويتشكل هذا الهرم عند قيام شخص واحد من الأشخاص بجمع أموال

1 خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، رسالة ماجيستر، جامعة نايف للعلوم الأمنية، 2009، ص 138.

2 محمد سامي الشوا، ثورة المعلومات وانعكساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998، ص 123.

3 محمد طارق الخن، المرجع السابق، ص 56.

من مشتركين آخرين، مع الطلب منهم إقناع آشخاص آخرين، لتبدأ سلسلة من الاشتراكات، وتعتبر مجموعة أول المشاركين هي الحلقة الأولى من سلسلة الاحتيال، وترتكز هذه المشاريع التسويقية الهرمية على تبادل الأموال، ولا يتعلق الأمر ببيع سلع أو منتجات، وإنما هو غطاء فقط لمثل هذه الأنشطة الاحتيالية التي يسعى من خلالها هؤلاء المجرمين إلى الاستيلاء على أموال الغير[1].

المطلب الثاني: مـحل جريمة الاحتيال في إطار المعاملات الإلكترونية.

تنطوي جريمة الاحتيال في مفهومها التقليدي على اتصال بين الجاني والضحية التي يمارس حيالها النشاط الإجرامي، إلا أنه في حالة إسقاط حالات النصب والخداع في المجال الإلكتروني يصعب التسليم بوجود احتيال ممارس من طرف شخص في مواجهة شخص آخر، بل يمكن القول أن اتصال الجاني يكون مع الأنظمة الحاسوبية مستعيناً في ذلك بجملة من الوسائل الاحتيالية المطبقة على المعلومات والبيانات المدرجة في المعاملات الإلكترونية، والسيطرة عليها بما يسهل فعله الإجرامي في تحقيق عملية تسليم المال محل الإحتيال.

ويبدو ذلك واضحاً في الحالات التي يتم فيها الإستعمال غير المشروع لبطاقات الائتمان لسحب الأموال أو الحالات التي يتم فيها تحويل الأموال إلكترونياً دون تدخل أي عنصر بشري. وهنا ثار جدل كبير حول مسألة مدى تحقق وصف النشاط الإجرامي المتمثل في الاحتيال على الأجهزة الحاسوبية ؟ وبصيغة أدق؛ هل يمكن تصور قابلية مكونات النظام المعلوماتي من أموال ومعلومات متداولة إلكترونياً أن تكون محلاً لجريمة الاحتيال ؟

وللإجابة عن ذلك، سلك الفقه الجنائي والتشريع المقارن ثلاث اتجاهات رئيسية نوردها تباعاً:

الفرع الأول: الإتجاه الرافض لفكرة الاحتيال على الأنظمة المعلوماتية.

وفقاً لرؤية هذا الاتجاه، وجب ضرورة توجيه أفعال الاحتيال لأشخاص طبيعية، نافياً التصور القائم على إمكانية خداع الأنظمة المعلوماتية، وبالتالي رفض تطبيق نصوص جريمة الاحتيال في مجال المعاملات الإلكترونية.

وبناءً على ما ذكر فإن الاحتيال في هذه الحالة ينصرف إلى الإنسان الذي يوجد خلف الحاسوب، إذ أن جريمة الاحتيال تتطلب خداعاً من الجاني يؤثر على المجني عليه بصورة تحمله على تسليم المال، والقول

1 مركز البحوث والدراسات، الغش التجاري في المجتمع الإلكتروني، ورقة عمل مقدمة إلى الندوة الرابعة لمكافحة الغش والتقليد في دول مجلس التعاون الخليجي، جامعة البحرين، 2014، ص 17.

بوجود هذا التأثير على إرادة المجني عليه وخداعه في حالة التلاعب ببرامج الحاسوب هو قول بعيد عن الواقع، ويعد توسعاً في تطبيق قانون العقوبات، ولا يتفق مع مبدأ الشرعية الجنائية[1].

وتعد قضية "R.V.Gold" في المملكة المتحدة واحدة من أبرز القضايا في هذا الصدد، حيث تمكن المتهم وشريكه من الحصول على شفرة تمكنهم من الدخول إلى نظام للمعلومات توفره هيئة الاتصالات البريطانية "Britich Telecom" لمهندسيها نظير دفع رسم محدد، بالإضافة إلى مبلغ آخر يتحدد حسب نوع المعلومات التي تم الحصول عليها، وقدم المتهمان للمحاكمة إلا أن المحكمة رفضت تطبيق النص الخاص بجريمة الحصول على ممتلكات أو خدمات بطريق الاحتيال، وهو ما لا يتصور في مواجهة عقل بشري لإيقاعه في الغلط للحصول على الممتلكات أو الخدمات[2].

ويستند بعض الفقهاء الفرنسيين منهم "Catala Pierre" في تبرير هذا الرأي إلى أن نظام معالجة البيانات –العقل الإلكتروني– يفتقر إلى خاصية التفكير، فهو ينفذ أوامر يتلقاها مسبقاً أو يتلقى أسلوب معالجتها، علاوة على أن معطيات الحاسوب ذات طبيعة معنوية، وتفتقر إلى كونها مالاً منقولاً ذات طبيعة مادية، وهو ما اشترطه المشرع في محل جريمة الاحتيال.

الفرع الثاني: الإتجاه الـمؤيد لفكرة الاحتيال الإلكترونـــي.

يرى أنصار هذا الاتجاه[3] إمكانية تطبيق النصوص الخاصة بجريمة الاحتيال في مجالات المعاملات الإلكترونية على الأنظمة المعلوماتية، باعتبارها الوسيلة التي يتم من خلالها تجسيد الفعل المجرم، بحيث يميل رأي من الفقه الفرنسي إلى القول أن الإحتيال على الأنظمة المعلوماتية لسلب المال يتحقق من خلال توافر سلوكات الفعل الإجرامي المتمثلة في الأكاذيب التي تدعمها وقائع خارجية؛ تتمثل في المعلومات والبيانات التي يتم إدخالها عبر جهاز الحاسوب، وذلك على اعتبار أن الحقيقة تكمن في أن الأساليب إنما هي موجهة نحو شخص آخر يقف وراء هذا الجهاز، ويمكن القول بامتداد تلك الأفعال والحيل لتمتد عبر الوسائط الإلكترونية وتخاطب عقل المجني عليه من خلال رسم صورة غير حقيقية، توهمه بأشياء غير موجودة, وبالتالي تسلب إرادته عن طريق إيقاعه في الغلط الذي يدفعه نحو التعامل مع الجاني.

---

[1] أخذ بهذا الرأي جانب من الفقه الفرنسي وبعض أحكام المحاكم الفرنسية. **مشار إليه لدى:**

- **Catala (Pierre),** Informatique et droit penal; Travaux de l'nstitute de scieces criminelle de poitiers, édition cujas,1983, p 267.

2 Lucas de leyssac, op. cit, p 49-50

3 Linat de Bellfond, Op. Cit, p 113

ويستند أنصار هذا الرأي إلى مجموعة من الأحكام القضائية الصادرة عن القضاء الفرنسي؛ ومنها قضية المتهم الذي عمل على تحويل مبالغ مالية من الشركة التي يعمل بها لحساب شركة أخرى يسيطر عليها، وذلك لصبها في حسابه الخاص، واعتبرت المحكمة هذا النشاط نوعاً من أنواع الاحتيال على أجهزة الحاسوب، ولقد استقر القضاء بعد ذلك على وقوع جريمة الاحتيال في حالة سحب الجاني لمبالغ مالية من حساب شخص باستخدام أي نوع من أنواع الاتصال الإلكتروني، وحتى في حالات السحب عن طريق بطاقات السحب الآلي[1].

لذلك، يتبين اتجاه المحاكم إلى توسيع القبول بفكرة الاحتيال، لتطال الوسائل الإلكترونية باختلافها من خلال الاعتماد على أجهزة الحاسوب، وكذا شبكة الانترنت كوسيط يتم من خلاله تلك المعاملات، ومن ذلك ما قضت به محكمة النقض الفرنسية من وقوع جريمة الاحتيال بالاستعانة بوسيلة إلكترونية معتبرة إياها في عداد المظاهر الخارجية والمادية فترى المحكمة: "إن الأوراق تشكل مظهراً خارجياً إذا كانت طبيعتها أن تولد الاقتناع بوجود ائتمان غير حقيقي ما دامت تأتي من استعمال وسيلة إلكترونية للحساب أو الإدارة تضفي عليها مصداقية"[2].

كما تعترف بإتيان جرم الاحتيال في حالة أوامر التحويل عن طريق الكمبيوتر من حساب في بنك إلى آخر، فاتجهت إلى اعتبار أن أي تلاعب في مستندات البنوك يشكل وسيلة احتيالية سواء كانت المعلومات مادية أو متداولة إلكترونياً، لما لهذه الملفات من مصداقية يترتب عليها تسليم المال في هذه الجريمة[3].

ويرى أنصار هذا الرأي بأن التطور الحديث في مجال تكنولوجيا المعلومات، يدفع للبحث عن معيار جديد غير معيار مادية الشيء، يمكن من خلاله إسباغ صفة المال على الشيء المعنوي، لذلك لجأ اصحاب هذا الاتجاه إلى تبني معيار القيمة الاقتصادية للشيء، حيث يعتبر الشيء مالاً بالنظر إلى قيمته الاقتصادية، لا بالنظر إلى ما له من كيان مادي[4].

---

1 Cass. Crim; 17 octobre 1992. Bull. crim; No : 252, p 594.

2 محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 138.

3 Michel Vivant et autres, Op. Cit, p 812.

- **مشار إليه لدى:** نائلة قورة، المرجع السابق، ص 119- 120.

4 هشام محمد فريد رستم، المرجع السابق، ص 249.

وهنا نرى ضرورة الاعتراف بإمكانية تجسيد الطرق والوسائل الاحتيالية على المعاملات التي تتم عبر الأجهزة الإلكترونية من كمبيوتر أو أجهزة سحب آلي، وهو تسليم ضمني بتوجه تلك السلوكات الاحتيالية نحو شخص يقع تحت التغليط العمدي من خلال المعاملات غير المباشرة التي تؤدى عن طريق وسائط آلية أو إلكترونية.

الفرع الثالث: اتــجاه القانون الفيدرالــي الأمريكي.

يتجه أنصار هذا الرأي[1] إلى تحديد فكرة الاحتيال الإلكتروني في مجال البريد والاتصالات السلكية وبشتى أنواع الاحتيال الواقعة على التعاملات البنكية، وهنا نجد أن بعض الدول منها الو.م.أ قد عملت على تبني تشريعات تمنح تفسيراً واسعاً للأموال, فتنظر إليها من منظور كل الأشياء التي تنطوي على قيمة, وهنا يفسح المجال لإدخال كل العناصر المادية والمعنوية لتشمل بذلك أساس المعاملات الإلكترونية القائمة على تداول المعلومات والبيانات المعالجة آلياً.

وعلى النطاق الفيدرالي أيضاً، تقدمت الحكومات الأمريكية بمشروع قانون يستهدف مباشرة حالة الغش المعلوماتي، والذي يعاقب كل من يقوم باستخدام أي أسلوب احتيالي سواء بتصميم الخطط، أو الحيلة بغرض ارتكاب غش أو الاستيلاء على مبالغ مالية، أو حتى في حالة ولوج أو محاولة الولوج لأجهزة الحاسوب بغرض تنفيذ أو محاولة ارتكاب أفعال احتيال[2].

وبهذا فقد شمل مضمون مشروع القانون المذكور أعلاه كل من الوسائل المستخدمة في حالات الاحتيال الإلكتروني، والتي تحوي جميع المكونات الإلكترونية والكيانات المنطقية، وكل قيمة أخرى ذات طابع مادي أو معنوي.

بدورنا نؤيد الإتجاه القائل بصلاحية وقوع الاحتيال على الأنظمة المعلوماتية، على اعتبار أن الهدف من التجريم بالإضافة للسبب التقليدي المتمثل في حماية كل من حق الملكية وحرية الإرادة وسلامتها، هو تجنب القصور عن مواكبة التطورات التكنولوجية المتلاحقة، والتي جعلت الاحتيال الإلكتروني أمراً غير مألوف يتماشى وطبيعة الجرم المرتكب، والوسائل المستخدمة التي تفرض البحث في دائرة التجريم، وإيجاد الحل لمواجهة هذه السلوكات غير المشروعة، خاصة في ظل غياب النص الخاص لمعالجتها، وهو الأمر الذي

1 John (T), Thomas (F) , Jr. Heidi M. Brissette, Computer Technology and Law, Shepard's/ Mc Graw-hill, 1993, p 348.

2 محمد أمين الشوابكة، المرجع السابق، ص 115.

حاولت بعض التشريعات تداركه؛ كالمشرع الإنجليزي الذي جرم مسألة غش الكمبيوتر عام 1990 الذي يعاقب على الاستعانة بمعلومات مبرمجة كاذبة أو إدخال هذا النوع من المعلومات في نظام الكمبيوتر لشخص آخر للحصول لنفسه أو للغير على ربح غير مشروع.

المطلب الثاني: أركان جريمة الاحتيال في إطار المعاملات الإلكترونية.

إن بيان أركان جريمة الاحتيال الإلكتروني تستوجب دراسة الركن المادي الذي يرتكز على عنصري النشاط الإجرامي لجريمة الاحتيال، القائم على جملة الأفعال الاحتيالية التي يتكون بها جرم الاحتيال، والتي تبرز لها خصوصية في مجال المعاملات الإلكترونية، مع التطرق إلى النتيجة الإجرامية المتمثلة في تسليم الضحية المال محل الجريمة، مع بيان القصد الجنائي المتمثل في الركن المعنوي.

الفرع الأول: النشاط الإجرامي (فعل الاحتيال).

لقد بين الفقه الجنائي في القواعد العامة أن أساس الطرق الاحتيالية هو الكذب البالغ لدرجة الاحتيال الذي يكون صالحاً لإيقاع المجني عليه في الغلط، بطريقة تؤدي إلى الإقناع بالمظهر المادي الخارجي للجاني فيخدع به المجني عليه ويفضي به إلى تسليم المال.

ويجدر بنا تبيان بعض الملاحظات المتعلقة بالنشاط الجرمي لجريمة الاحتيال في إطار المعاملات الإلكترونية على النحو التالي:

- لزوم مباشرة نشاط تقني لارتكاب جريمة الاحتيال الإلكتروني، على اعتبار أن النشاط الإجرامي يبدأ من استخدام الحاسوب الذي يوفر النفاذ إلى الشبكة المعلوماتية، وممن ثم يجب أن يتمتع الجاني بالقدر الكافي من المعرفة التقنية لارتكاب هذه الجريمة[1].
- إن الدخول المصرح به إلى نظام معلوماتي يخص الغير، يعد أحد العناصر الضرورية لبعض أساليب جريمة الاحتيال الإلكتروني، كمن يخترق النظام المعلوماتي لأحد المصارف عبر الانترنت، ليقوم بإجراء تحويلات مالية لصالحه، وفي أغلب التشريعات قد يشكل الدخول غير المصرح به جريمة في حد ذاته، إضافة إلى كونه الوسيلة إلى ارتكاب جرائم أخرى مثل الاحتيال.
- تقدم تقنية الانترنت للمحتالين القدرة على الاتصال الإلكتروني بملايين الضحايا حول العالم، وذلك بكلفة أقل بكثير من وسائل الاتصال التقليدية.

1 عبد الله عبد الكريم عبد الله، المرجع السابق، ص 63.

إن المشكلة في تحديد النشاط الإجرامي لجرم الاحتيال في إطار المعاملات الإلكترونية، يرجعه الفقه إلى التلاعب في البيانات أو البرامج، باستخدام الطرق الاحتيالية على النظام العلوماتي؛ الذي هو أساس ممارسة فعل الاحتيال[1]، ولقد ثار خلاف بين الفقه حول مسألة التلاعب في البيانات باستخدام الطرق الاحتيالية, وهو ما سنبينه كالآتي:

- ذهب رأي[2] إلى أن التلاعب المعلوماتي هو تلاعب في البرامج والبيانات للتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها، الأمر الذي يجعله يسلم بها ، وبالتالي يمكن انطباق النص المتعلق بالجرائم الاحتيالية على التلاعب المعلوماتي باعتباره أحد أساليب الاحتيال وأن النظام المعلوماتي يستخدم كوسيط للتحايل.
- يتوجه جانب من الفقه الجنائي إلى إمكانية استخدام الأساليب الفنية في الاحتيال على النظام المعلوماتي عن طريق استخدام النظام كأداة سلبية, ومثالها دخول الجاني إلى النظام باعتباره المستخدم الشرعي عن طريق الحصول على الرقم السري للمستخدم الأصلي للاستيلاء على الأموال، فهنا يكون النشاط الإجرامي للجاني قائم على استخدام إحدى الطرق الاحتيالية المنصوص عليها قانوناً.
- أما جانب ثالث من الفقه يرى إمكانية استخدام النظام المعلوماتي كأداة إيجابية عن طريق التدخل المباشر في المعطيات وإدخال معطيات وهمية, أو تعديل برامج أو خلق برامج صورية, وهي جميعها طرق احتيالية ومثالها التزوير في الفواتير، وهو ما قامت به شركة تأمين أميركية في إعداد 64000 وثيقة تأمين وهمية[3].

ومن جهتنا نرى صلاحية كل الأساليب السابقة في قيام النشاط الإجرامي لجريمة الاحتيال الإلكتروني، فالطبيعة الخاصة التي يكتسبها هذا النوع من الجرائم تجعل من الجناة يلجأون إلى اختيار الطرق المناسبة لارتكاب الجريمة وفقاً لمعطيات كل جريمة ونوع الضحايا المرتكبة ضدهم.

1 محمد علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديثة ، ط1، مصر، سنة 2004، ص 174.

2 محمد سامي الشوا، المرجع السابق، ص133.

3 محمد فريد رستم، المرجع السابق، ص 282.

الفرع الثاني: عنصر التسليم في جريمة الاحتيال الإلكترونـــي.

لقيام جريمة الاحتيال يجب أن تؤدي وسائل الاحتيال التي نص عليها المشرع إلى إيقاع المجني عليه في غلط يحمله على تسليم ماله إلى الجاني، ويعد هذا التسليم بمثابة النتيجة الإجرامية في جريمة الاحتيال، ولا يختلف الأمر بشكل عام بخصوص الاحتيال الإلكتروني، فالأساليب التي يستخدمها الجاني يجب أن تسفر عن نتيجة مفادها الاستيلاء على مال الغير، وذلك بتسلمه من المجني عليه تحت تأثير الغلط الذي أحدثه فعل الاحتيال، إلا أن الإشكال الذي يثار في هذا المقام هل يمكن أن يقع فعل التسليم الإلكتروني للأموال من قبل الحاسب الآلي؟

وفي الواقع نجد أن التسليم هو سلوك صادر من الجاني يتم بمقتضى الخداع والتضليل الممارس على المجني عليه، وبالنظر أيضاً إلى بعض الحالات التي تندرج تحت وصف الاحتيال الإلكتروني نجد أن الحاسب الآلي يقوم بفعل التسليم بالمفهوم المادي للكلمة، وذلك بقيام التسليم تحت فعل المناولة اليدوية كما هو حال الاحتيال الذي ينطوي على استعمال غير مشروع لبطاقات الائتمان. أما في الحالات الأخرى فقد يتم من خلال تسليم المال بصورة غير مادية، وهنا يمكن القول أن التسليم لا يجوز النظر إليه على أنه واقعة مادية تتمثل في مناولة يدوية، ولكن يتعين النظر إليه على أنه عمل قانوني عنصره الجوهري إرادة المجني عليه المعيبة بالخداع, وليست المناولة سوى مظهر مادي لهذا العمل[1].

وفي حالة الأخذ بهذا المعنى للتسليم، فهنا لا يُثار أي إشكال في حالات الاحتيال في مجالات المعاملات الإلكترونية التي لا تنطوي في مجملها على التسليم المادي للأموال، وإنما قد يتم في صورة التسليم المعنوي الذي يتماشى وطبيعة هذا النوع من المعاملات.

ونرى في هذا الشأن، أن الاحتيال الإلكتروني قد لايختلف عن الاحتيال في وجهه التقليدي في حالة ما تمت المناولة اليدوية للمال محل الجريمة، إلا أن قيام التسليم المعنوي في جريمة الاحتيال الإلكتروني لا يقوم أساساً على انتفاء المناولة اليدوية، وإنما جوهر التسليم هنا يتبلور في اتجاه إرادة المجني عليه في وضع المال في يد الجاني، وهذا بقيام الأفعال الاحتيالية التي مارسها الأخير عبر الحاسب الآلي.

ولا يقع إشكال في حالة ما إذا كان الاستيلاء الناشئ عن الاحتيال في المعاملات الإلكترونية قائم على تسليم أموال منقولة مادية؛ كأن يتم التلاعب في البيانات المدخلة أو المعطيات الآلية التي تقوم عليها المعاملة عن طريق استخراج باسمه بعض الحسابات أو الشيكات أو الفواتير بمبالغ غير مستحقة, والاستيلاء

1 شيماء عطاالله، المرجع السابق، ص 98.

عليها، ولكن الإشكال يثور بصدد فكرة تسليم الأموال في جريمة الاحتيال الإلكتروني في حالة ما إذا كان محل الاحتيال نقوداً كتابية أو بنكية؛ كأن يتم التلاعب من قبل الجاني بالبرامج والمعلومات المصرفية بهدف تحويل الأموال من حسابات أصحابها إلى حسابه الخاص، فهل يتحقق التسليم هنا ؟

تختلف الإجابة عن هذا الإشكال بحسب مواقف التشريع المقارن من مسألة النقود الكتابية، وهنا يمكن التمييز بين اتجاهين:

إن معظم التشريعات المقارنة اعتبرت النقود الكتابية من قبيل الديون، ولم تعترف لها بصفة المال المادي، وبالتالي لا تصلح لأن تكون محلاً لجريمتي السرقة أو الاحتيال، وذهبت بعض التشريعات الأخرى أمثال كندا وهولندا وسويسرا وفي معظم الولايات المتحدة الامريكية وإنجلترا إلى اعتبار النقود الكتابية من قبيل الأموال التي تصلح للاستيلاء عليها.

ففي الولايات المتحدة الأمريكية سبقت الإشارة إلى أن القوانين الفيدرالية قد عرفت المال بأنه: " كل شيئ يمثل قيمة، بحيث يشمل جميع الأموال الكتابية أو المصرفية"[1].

ويلحق بهذه الدول فرنسا، حيث ابتدع القضاء الفرنسي نظرية "التسليم المعادل" التي أقرتها محكمة النقض الفرنسية؛ إذ اعتبرت بأن الدفع الذي يتم عن طريق القيد الكتابي يعادل تسليم النقود، وبناءً على هذه النظرية فإن المادة 313 من قانون العقوبات الفرنسي والمتعلقة بالاحتيال تنطبق على جميع أفعال التلاعب في عملية البرمجة أو في البيانات المدخلة إلى الحاسوب والمنقولة عبر الانترنت.

فجميع عمليات التحويل غير المشروع؛ أي الدخول إلى أنظمة المصارف والتلاعب بها، والتي يترتب عليها الاستيلاء على كل أو بعض الأرصدة العائدة للغير، يعد فيها التسليم محققاً ومعادلاً لتسليم النقود[2].

ويدعم اتجاه القضاء الفرنسي جانب من الفقه المصري الذي يرى أن التسليم في جريمة الاحتيال يقع بوضع المال تحت تصرف الجاني، وتتحقق الحيازة بدون أي عوائق.ونؤيد بدورنا ما ذهبت إليه التشريعات التي اعترفت بالاستيلاء على الأموال الكتابية أو الإلكترونية، وهذا لأن القيام بالأفعال الاحتيالية المتمثلة في التلاعب في البيانات, والتي تفضي إلى انتقال المال من الغير إلى الجاني هي نتيجة مماثلة لتحويل الأموال بشكلها التقليدي، إلا أن الضرروة العملية تقتضي النظر إلى طبيعة الجرائم الخاصة بالاحتيال في مجال المعاملات الإلكترونية، والتي تلح إلى الخروج عن مبدأ القياس مع القواعد التقليدية، والتوجه إلى إصدار

1 علي عبد القادر القهوجي، المرجع السابق، ص 73.

2 نائلة قورة، المرجع السابق، ص 175.

تشريعات خاصة تضمن الحماية الجنائية لمثل هذه الجرائم بشكل خاص، وبالتالي التكريس الأمثل لمبدأ الشرعية الجنائية.

الفرع الثالث: الركن المعنوي لجريمة الاحتيال في إطار المعاملات الإلكترونية.

يقيم العديد من الفقهاء مفهوم القصد الجنائي العام لجريمة الاحتيال على أساس توافر الإرادة السيئة للجاني في إيقاع الجرم من خلال تحقق حرية الاختيار، مع توفر العلم بأضرار الفعل الإجرامي الذي يسلكه، بحيث أن المشرع يهدف أساساً من خلال تجريم أفعال الاحتيال إلى حماية حق الملكية, وضمان التأكد من سلامة إرادة الضحية بالتصرف في أمواله بإرادة سليمة، بعيدة عن كل وسائل التضليل والخداع[1].

ويذهب بعض الفقه الفرنسي إلى تحديد بعض صور الركن المعنوي في جريمة الاحتيال الإلكتروني:

- أن يقوم الجرم الاحتيالي على عمليات التخطيط لتنفيذ عمليات احتيالية بغرض الاستيلاء على أموال الغير دون وجه حق.
- كذا توافر نية قصد الاحتيال الالكتروني من خلال استخدام الوسائل الإلكترونية كالبريد الإلكتروني أو المواقع الإلكترونية من أجل إتمام المخطط الاحتيالي.
- تعمد تضليل المجني عليه والتأثير على إرادته من خلال الاستعانة بأساليب معينة أو إخفاء وقائع مادية ملموسة[2].

أما بخصوص القصد الجنائي الخاص لجريمة الاحتيال الإلكتروني فيتمحور حول نية الجاني في تملك مال الضحية وممارسة كل حقوق الملكية عليه من تصرف واستئثار، وبهذا تنشأ جريمة الاحتيال بدافع الجاني القائم على حرمان المجني عليه من المال بصفة نهائية وبهذا ينتفي جرم الاحتيال في حالة ثبوت عدم توافر نية الشخص في الاطلاع أو الانتفاع المؤقت مع إرجاعه لصاحبه.

وبالرجوع إلى تطبيق جريمة الاحتيال في مجال المعاملات الإلكترونية نجد أن أساس الأفعال الاحتيالية المرتكبة من طرف الجُناة هي قائمة على وجود قصد مسبق في الدخول في تعاملات غير مشروعة يهدف من خلالها الجناة تصيد أموال الضحايا، باستخدام وسائل غير مشروعة كإيقاع الضحايا بعد سلسلة من

1 أحمد خليفة الملط، المرجع السابق، ص 275.

2 Michel Vivant et autres, Op. Cit, p 522.

الأكاذيب وتزييف وانتحال للشخصيات وإيقاع الضحايا في وَهمٍ يدفعهم إلى تسليم أموالهم تحت طائلة الخديعة والتضليل.[1]

ويختلف القصد الجرمي في جريمة الاحتيال الالكتروني وفقاً لنوع الجرائم المرتكبة، وعلى الأساليب المتبعة فيها، فنية الجاني في الاستيلاء على مال الضحية عن طريق استهداف الحسابات المالية الشخصية والمعلومات الخاصة ببطاقات الائتمان، هو التوصل إلى سحب تلك الأموال وتحويلها إلى رصيده الخاص، بينما الاعتداء على مواقع الاستثمار، والاعتداء على سرية المعلومات الخاصة بها يهدف إلى نية الجاني في خداع المستثمرين والاستيلاء على أموالهم.[2]

وأما بخصوص مسألة إثبات القصد الجنائي في مجال المعاملات الإلكترونية فيستند إلى القرائن، وذلك من خلال تفتيش أداة الجريمة المتمثلة في الحاسوب، وترصد المواقع المتصفحة من قبل الجاني، وكذا الاتصالات التي قام بها بغية الوصول إلى دليل إدانته في جريمة الاحتيال.

ولقد نص المشرع الإماراتي في المادة 11 من القانون الاتحادي رقم 5 لسنة 2012 لمكافحة جرائم أنظمة المعلومات[3] الإماراتي بمعاقبة الجاني في حالة استيلائه لنفسه أو لغيره بغير حق على مال منقول أو منفعة، أو توقيع سند، وذلك بالاستعانة بأي طريقة احتيالية، أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات[4].

ونرى أن حكم المادة السابق يقوم على نفس مفهوم الركن المعنوي لجريمة الاحتيال التقليدي، عدا ما يخص الوسيلة المستخدمة والمتمثلة في الشبكة المعلوماتية أو نظام معلومات إلكتروني، أو أي وسيلة تقنية المعلومات، وهذا وبتوسيع محل الجريمة ليشمل المال أو المنفعة أو توقيع سندات، وهو الأمر الذي يفسرتغطية كل الاحتمالات القائمة في مجال التعامل الإلكتروني ليكون هذا الحكم موسعاً أو مشدداً يفي بتكريس حماية فعالة للضحايا.

1 تيسير الزعبي، المرجع السابق، ص 70.

2 حسن فريجة، الجرائم الإلكترونية والانترنت، مجلة المعلوماتية، السعودية، العدد 36، سنة 2012، ص 5.

3 مرسوم بقانون اتحادي لمكافحة جرائم أنظمة المعلومات الإماراتي رقم 5 لسنة 2012 الصادر عن قصر الرئاسة بأبوظبي بتاريخ 25 رمضان 1433هـ الموافق 13 أوت 2012.

4 محمد عبيد الكعبي، المرجع السابق، ص 236.

المبحث الثالث:

الحماية الجنائية من جريمة خيانة الأمانة في إطار المعاملات الإلكترونية.

هناك شبه إجماع بين التشريعات العقابية المقارنة على تعريف جريمة خيانة الأمانة بأنها استيلاء شخص على منقول يحوزه بناء على عقد من عقود الأمانة المحددة قانوناً، وبهذا يأخذ هذا المفهوم معنى خيانة الثقة المودوعة في المتعاقد بمقتضى العقد، بتحويل صفته من حائز لحساب مالكه إلى صاحب ملكية فعلية.

المشرع الجزائري بدوره عرف جريمة الخيانة بأنها: "كل من اختلس أو بدد بسوء نية أوراقاً تجارية أو نقود أو بضائع أو أوراقاً مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاماً أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين، وذلك إضراراً بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكباً لجريمة خيانة الأمانة ويعاقب بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 500 إلى 20.000 دج"[1], وتقابلها المادة 404 من قانون العقوبات الإماراتي والمادة 1/314 من قانون العقوبات الفرنسي الجديد[2].

ولبيان أهم الأحكام الخاصة بوقوع جريمة خيانة الأمانة في إطار المعاملات الإلكترونية يجدر بنا التنويه إلى إغفال التشريعات المقارنة مسألة إدراج الأحكام الخاصة بهذه الجريمة في مجال التعامل الإلكتروني.

وفي هذا الإطار يستوجب بيان أهم العناصر المكونة لفكرة الحماية الجنائية في نطاق هذه الجريمة من خلال التعرض للجدل الفقهي الخاص بمحل جريمة خيانة الأمانة في مجال التعاملات الإلكترونية (المطلب الأول)، إضافة إلى إسقاط الأحكام الخاصة بأركان هذه الجريمة في إطار المعاملات الإلكترونية (المطلب الثاني).

1 انظر المادة 376 من قانون العقوبات الجزائري.

2 Article 314-1 du CPF: " L'abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les représenter ou d'en faire un usage déterminé.l'abus de confiance est puni de trois ans d'emprisonnement et de 375000 euros d'amnde".

المطلب الأول: محل جريمة خيانة الأمانة في إطار المعاملات الإلكترونية.

بالرجوع للحكم التشريعي المنظم لجريمة خيانة الأمانة في التشريعات المقارنة يتبين أن محل الجريمة يتمثل في المال المنقول المملوك للغير، المسلم للجاني على سبيل إحدى العقود المحددة بنص القانون، لذا نجد أن مسألة بيان محل جريمة الخيانة في مجال المعاملات الإلكترونية يستوجب البحث في إشكالية طبيعة المال محل الجريمة، ومدى الاعتراف بفكرة وقوع فعل الخيانة على المعلومات أو الأموال المتداولة إلكترونياً, وكذا البحث في مدى تحقق واقعة التسليم التي تقع على المعلومات أو الأموال الإلكترونية.

الفرع الأول: طبيعة المال المعنوي كمحل لجريمة خيانة الأمانة في إطار التعاملات الإلكترونية.

بالرجوع إلى المفهوم الذي تقوم عليه جريمة خيانة الأمانة، نجد تطابق الأحكام الخاصة بهذا الجرم في حالة قيام المجني عليه بتسليم الجاني الوسيط المادي الذي يمثل محلاً للجريمة، بحيث لم يجد القضاء الفرنسي أي صعوبة في تطبيق النصوص الخاصة بهذه الجريمة، فعلى سبيل المثال صدر حكم عن محكمة الاستئناف "Grenoble" في 23 ماي 2004 بإدانة أحد الأشخاص بتهمة خيانة الأمانة لقيامه بإخراج أحد الأقراص الممغنطة واستخدامها في إطار خارج عن عمله[1].

إلا أنه بالنظر إلى التعاملات الإلكترونية نجد أنه بالإضافة إلى الأموال الإلكترونية المادية هناك نوع آخر من الأموال الإلكترونية اللامادية، هاته الأخيرة التي تشكل جوهر العلاقة التعاقدية الإلكترونية، فحساب العميل في البنك يشمل بيان إلكتروني بمبلغ معين، وهذا البيان يفتقد إلى الصفة الحسية المادية. لذلك، يتوجب الإجابة عن إشكالية هامة تتعلق بمدى تحقق فعل خيانة الأمانة إذا انصب الفعل على المعلومات أو الأموال الإلكترونية محل المبادلات الإلكترونية، وذلك في معزل عن أي وسيط مادي.

البند الأول: الموقف الفقهي من فكرة قابلية الأموال والمعلومات الإلكترونية كمحل لجريمة خيانة الأمانة.

في بداية التصور الذي أقامه العديد من الفقهاء على إمكانية وقوع جريمة خيانة في مجال المعاملات الإلكترونية، اتجه جانب كبير إلى رفض الفكرة حيث اعتبروا أن الطبيعة المعنوية للمعلومات أو الأموال المتداولة إلكترونياً تفتقد إلى المادية التي هي شرط أساسي في المال المنقول محل الجريمة[2].

1 CASS. Crim. 24 mai 2004, Bull crim, n 315. 2004. p 465.

2 عفيفي كامل عفيفي، المرجع السابق، ص 174.

بينما يرى اتجاه محدود من الفقه الفرنسي ضرورة الاعتراف بإمكانية أن تكون الأموال أو المعلومات الإلكترونية منفصلة عن إطارها المادي، واستدلوا بعبارة "التسليم لأداء عمل بأجر أو بدون أجر"، الواردة بالمادة 408 من قانون العقوبات ليمتد نطاق تطبيقها ليشمل المعلومات، وذلك في حالة تجاوز الجاني حدود التعاقد أو التعامل المتفق عليه، وهو ما يفسر صلاحية المعلومات للاستخدام بشكل غير مشروع، والذي يترتب عنه خيانة الثقة الممنوحة في أحد طرفي المعاملات الإلكترونية بشكل يحاول معه تحويل الحيازة الناقصة إلى حيازة كاملة بنية الاستيلاء غير الشرعي لتلك المعلومات أو الأموال[1].

وترى الأستاذة "De Leyssac" أن مادية المحل ليست شرطاً لقيام الجريمة، وأن اشتراط هذه المادية ما هو إلا انعكاس لفكرة أن يكون التسليم حقيقياً؛ أي عن طريق المناولة المادية الفعلية للمال المنقول محل الجريمة، إلا أنه قد يكون اعتبارياً في حالة تصور وقوع المتعامل إلكترونياً الذي يبرر سلوك اعتداءه على الوسيلة التي يتم من خلالها ترجمة القيمة الحقيقية للمال المعتدى عليه، أو المعلومات المتداولة إلكترونياً، والتي تعكس قيمة اقتصادية معينة، وذلك إما بالخروج عن أساس الاتفاق بالحفاظ على القيمة المعنوية للمال أو المعلومة الإلكترونية، والتي تمثل في جوهرها قيمة مادية[2].

البند الثاني: الموقف القضائي من فكرة قابلية الأموال والمعلومات الإلكترونية كمحل لجريمة خيانة الأمانة.

لقد سعى القضاء الفرنسي في العديد من أحكامه إلى التحرر من فكرة المادية لوقوع جريمة خيانة الأمانة في مجال التعاملات الإلكترونية، وهذا استناداً إلى المنطق الذي أقرته أحكام المادة 1/314 من قانون العقوبات الجديد، والتي تجنبت من ناحية التعداد الوارد في المادة 408 للأشياء التي يفترض أن تكون محلاً لجريمة خيانة الأمانة من بضائع أو نقود أو سندات، أو أي أشكال أخرى تشتمل على مخالصات أو إبراء ليحل محل هذا التعداد عبارة أكثر اتساعاً؛ وهي النقود والقيم والأموال أياً كانت. ومن ناحية أخرى فإن المادة 1/314 لم تُشِر إلى عقود الأمانة التي وردت في القانون القديم، والتي جاءت على سبيل الحصر، لتعوض بحكم آخر يتجه إلى عدم تسمية العقد مكتفياً بالإشارة إلى وقوع فعل الاختلاس على شيء يتم تسليمه للجاني بشكل مؤقت في إطار تعاقدي[3].

1 نائلة قورة، المرجع السابق، ص 170.

2 Lucas de leyssac, Op. Cit, p50-51

3 شيماء عطاالله، المرجع السابق، ص 85.

ولعل أهم الأحكام الصادرة في هذا الصدد؛ هو قضاء محكمة النقض الفرنسية بتوافر خيانة الأمانة بخصوص رقم كارت السحب من البنك، وذلك لأن أحكام المادة 1/314 من قانون العقوبات تسري على كل مال أياً كانت طبيعته، وليس فقط على المال المادي، فيكفي لوقوع جريمة خيانة الأمانة أن يكون المال المسلم قد خصصه صاحبه لاستعمال معين، فيخرجه الأمين عن ذلك الاستعمال مستولياً على مال الغير.

وقد قضت ذات المحكمة بأن جريمة خيانة الأمانة وقعت جراء قيام مدير أحد البنوك بتحويل مبلغ من أحد حسابات العملاء؛ ومؤدى ذلك أن جريمة خيانة الأمانة يمكن أن تقع بوسيلة من الوسائل الإلكترونية شأنها في ذلك شأن غيرها من الوسائل[1].

إن الأحكام السابقة تدل على توجه القضاء الفرنسي نحو التخفيف من الطابع المادي للمنقول محل جرائم الأموال ليكون ذات طابع معنوي ما دام أنه ينجم عنها قيمة مالية مادية، ضف إلى ذلك قيام الأمين باستعمال الشيئ المسلم إليه بناءً على العقد على نحو يخالف فيه الاتفاق، ولعل تحول القضاء الفرنسي إلى الإعتراف بعدم مادية الشيئ محل جريمة خيانة الأمانة في إطار التعاملات الإلكترونية، يرجع إلى الضرورة العملية التي فرضتها مثل هذا النوع من المعاملات والتي ألحت بضرورة التعامل معها وفقاً للخصوصية التي تفرزها المعاملات الإلكترونية، وضرورة التصدي لمجال الجريمة وفقاً للطبيعة الخاصة للتعامل الإلكتروني.

الفرع الثاني: توافر عقود الأمانة كشرط لقيام جريمة خيانة الأمانة في مجال المعاملات الإلكترونية.

إن قيام جريمة خيانة الأمانة في إطار المعاملات الإلكترونية لا تخرج في مضمونها العام عن الأساس الذي تقوم عليه في شكلها التقليدي، بحيث أن التشريعات المقارنة قد عملت على إدراج شرط توافر عقود الأمانة التي تنشأ في ظلها هذه الجريمة، بقيام أحد العقود المحددة والتي تعكس فكرة الخروج عن وصف الأمانة الممنوح في ظل هذه العقود.

فذهب المشرع الجزائري إلى تحديد عقود الأمانة في كل من عقد الوديعة أو الإيجار أو الرهن أو عارية الاستعمال أو الوكالة، وأخذ المشرع الفرنسي بنفس الحكم من خلال المادة 408 من قانون العقوبات القديم، والمشرع المصري بمقتضى المادة 341 من قانون العقوبات.

1 R. OTTENHOF, Infraction contr les biens, Rev.sc.crim, 2001, p 386, Abus de confiance incorporal, crim 14/11/2000.

وفي هذا الصدد فإن مسألة الحديث عن جريمة خيانة الأمانة في نطاق المعاملات الإلكترونية تستلزم البحث في مدى توافر أنواع العقود المحددة على سبيل الحصر في إطار المبادلات الإلكترونية، خاصة وأن هذا المجال يفرض طبيعة خاصة للمعاملات والعقود المبرمة في نطاقه، والتي تفتقد إلى المرئية، بحيث تجعل من إمكانية تطبيق هذه العقود أمراً صعباً، أضف إلى ذلك أن الاعتراف بوجود هذه العقود يستدعي فتح المجال لأنواع أخرى من التعاقدات التي تفرزها تلك الطبيعة الخاصة للمعاملات الإلكترونية.

وفي هذا الصدد ثار جدل فقهي فيما يخص فكرة ضرورة توافر عقود الأمانة كشرط لقيام جريمة خيانة الأمانة في إطار المعاملات الإلكترونية.

1- الاتجاه القائل بضرورة توافر عقود الأمانة كشرط لقيام جريمة خيانة الأمانة في إطار المعاملات الإلكترونية:

يذهب هذا الإتجاه إلى عدم نفي فكرة ضرورة توافر العقود المحددة في إطار جريمة خيانة الأمانة، وخاصة ما تعلق بعقود العمل سواء بأجر أو بغير أجر، وكذا عارية الاستعمال، والتي يمكن أن تأخذ مجال التطبيق في إطار الغش المعلوماتي في حالة خروج أحد المتعاملين إلكترونياً عن قواعد الأمانة التي تفرضها طبيعة العقد، وهذا بالحصول على المعلومات أو التلاعب بغية تحويل صفة الحيازة عليها من حائز عرضي إلى حائز فعلي[1]، ولعل ذلك يظهر بشكل جلي في إطار العلاقة البنكية بين العميل والبنك، بحيث أن هذه العلاقة تقوم على عقد عارية الاستعمال الذي يتوجب فيه العميل الحفاظ على بطاقات الائتمان وردها إلى البنك في حالة انتهاء مدة استعمالها، ويعتبر قيام العميل بأي تصرف يظهر من خلاله رفضه إرجاع بطاقات الائتمان في حالة انتهاء صلاحيتها يعد دليلاً على قيام جريمة خيانة الأمانة في حقه[2].

2- الإتجاه الرافض لضرورة توافر عقود الأمانة في إطار المعاملات الإلكترونية:

يرفض أنصار هذا الاتجاه فكرة ضرورة توافر عقود الأمانة المحددة في التشريعات العقابية لقيام جريمة خيانة الأمانة في نطاق التعامل الإلكتروني، ويستندون في ذلك على أن وقوع جريمة خيانة الأمانة وفقاً للعقود المحددة على سبيل الحصر لا المثال أمر مجافي للمنطق؛ على اعتبار أن الجريمة تقوم بالرغم من بطلان

1 Yvonne Muller-Lagarde, La protection pénale de la relation de confiance: Observations sur le délitd'abus de confiance, Revue de Science Criminelle et de Droit Pénal Comparé, Dalloz, 2006. hal-01743321, p8.

2 مدحت عبد الحليم رمضان، المرجع السابق، ص 154.

العقد سواء كان هذا البطلان مطلقاً أو نسبياً، وهنا تظهر مسألة استقلالية القانون الجنائي على القواعد المدنية، فما يفرض العقوبة على الجريمة ليس تنفيذاً للعقد، وإنما هو الاعتداء على الملكية بالخروج عن الثقة الممنوحة في الجاني[1]. محكمة النقض الفرنسية أيدت هذا الرأي من خلال حكمها المتضمن بأن خيانة الأمانة لا تفترض بالضرورة أن المبلغ المختلس قد تم تسليمه بمقتضى عقد، وقد أصدرت هذا الحكم في إطار قضية تتعلق برد عربون دفعه المشتري في إطار المعاملات التجارية الإلكترونية بالرغم من توافر أحد أسباب بطلان عقد البيع[2].

وقد أكد هذا الرأي اتجاه قانون العقوبات الفرنسي بمقتضى أحكام المادة 314 والتي لم تلزم توافر عقد معين من عقود الأمانة المحددة سلفاً في القانون القديم، مما يترتب عنه التزام القاضي الجنائي بإضفاء وصف قانوني معين للعقد.

ولقد اتجه القضاء الفرنسي إلى تبرير فكرة عدم ضرورة توافر عقود الأمانة، باتخاذ موقف يوسع من مجال تطبيق جريمة خيانة الأمانة في نطاق المعاملات الإلكترونية، حيث رأت إمكانية الخروج على أنواع العقود المحددة في التشريع لتشمل أنواعاً أخرى قد تدخل في إطار المعاملات الإلكترونية، وهو ما أثبته حكم صادر عن محكمة جنح باريس في 12 أكتوبر 1988 والتي أدانت أحد العاملين التابعين لشركة توظيف الأموال الموضوعة تحت تصرفه, والذي قام العامل بتحويل الأموال المجمدة للعملاء إلى حسابات أخرى[3].

ونحن نميل بدورنا إلى الاتجاه القائل بضرورة توسيع مجالات العقود المحددة لقيام جريمة خيانة الأمانة في إطار المعاملات الإلكترونية، وهذا لاعتبارين أساسين أولهما : يتعلق بضرورة الأخذ بعين الاعتبار الخصوصية العقدية في هذا المجال, والتي تفرض الخروج عن الأنماط التقليدية للعقود المحددة في إطار جريمة خيانة الأمانة بشكلها التقليدي. وثانيهما: هو ضمان توفير حماية جنائية فعالة في مجال المعاملات الإلكترونية من خلال منح المتعاملين مساحة أوسع من الثقة في التعاملات الإلكترونية وضمان عدم الاعتداء على أموالهم.

1 أحمد خليفة الملط، المرجع السابق، ص 395.

2 CASS. Crim 9 mars 1987, n 48-97, jcp 1998 p 213 .

3 Cass. Crim 12 octobre 1988. N : 84-97. JCP.1988 P 384.

المطلب الثاني: أركان جريمة خيانة الأمانة في إطار المعاملات الإلكترونية.

يقوم البحث في أركان جريمة خيانة الأمانة في إطار المعاملات الإلكترونية على إشكالية رئيسية تتمثل في مدى تطابق الأحكام العامة المتعلقة بكل من الركن المادي والمعنوي لجريمة خيانة الأمانة على التعاملات الإلكترونية؟

الفرع الأول: الركن المادي لجريمة خيانة الأمانة في نطاق المعاملات الإلكترونية

بينت التشريعات المقارنة من خلال النصوص المتعلقة بتحديد مفهوم جرم خيانة الأمانة صور النشاط الإجرامي, ومنها المشرع الجزائري من خلال نص المادة 376 من قانون العقوبات والتي جاء فيها: "كل من اختلس أو بدد بسوء نية أوراقاً تجارية أو نقوداً أو بضائع..."، وهو نفس الحكم الذي أخذ به المشرع الفرنسي من خلال نص المادة 408 قانون العقوبات الجديد، والمشرع الإماراتي في نص المادة 404، بحيث يتضح من هذه الأحكام بيان لصور النشاط الإجرامي لجريمة خيانة الأمانة، مع الملاحظ أن المشرع الجزائري قد اكتفى بصورتي الاختلاس والتبديد، على عكس المشرع الإماراتي الذي أدرج الصور الثلاثة المتمثلة في الإختلاس، التبديد، والإستعمال.

أما بالنسبة للمشرع الفرنسي فقد اقتصر على ذكر صورتي الاختلاس والتبديد؛ فحسب القانون القديم يعتبرهما الصورتين اللتين يتخذهما الركن المادي في جريمة خيانة الأمانة، ثم جاء النص الجديد ليخلو من صورة التبديد ويقتصر على الاختلاس فقط، ونخلص من ذلك أن القانون الفرنسي لم يعرف الاستعمال بوصفه صورة من صور الركن المادي لجريمة خيانة الأمانة, وقد حذا المشرع الجزائري حذو المشرع الفرنسي في هذه المسألة[1].

وفي كل الأحوال نجد أن العناصر الثلاثة التي تشكل قيام الركن المادي، والتي تهدف إلى تحويل الحيازة الناقصة للجاني إلى حيازة كاملة، يستطيع من خلالها السيطرة التامة على المال محل الجريمة والتصرف فيه تصرف المالك الحقيقي. ونحن بصدد البحث في مدى تحقق الاحكام الخاصة بصور النشاط الاجرامي لجريمة خيانة الأمانة والتي تفرض بحث كل عنصر على حدى وهذا ما سيتم بيانه في الآتي:

1 محمود إبراهيم غازي، المرجع السابق، ص 452.

أولاً: الإختلاس.

يقصد بمفهوم الاختلاس في جريمة خيانة الأمانة: " كل تصرف سلبي يقع من الجاني يمتنع فيه عن رد المال إلى صاحبه بحيث تتحول سيطرة الجاني على المال سيطرة كاملة"[1], وبإسقاط هذا المفهوم على جريمة خيانة الأمانة في إطار المعاملات الإلكترونية، انقسم الفقه الجنائي إلى الاتجاهات التالية:

ذهب رأي فقهي[2] إلى أن فعل الاختلاس في إطار جريمة خيانة الأمانة على مستوى التعاملات الإلكترونية يتمثل في الحالة التي يمتنع فيها العميل عن رد بطاقة الائتمان في حالة طلبها من جانب البنك أو الجهة المصدرة لها، وهذا بعد انتهاء مدة صلاحيتها أو إلغائها أثناء مدة صلاحيتها كجزاء لسوء استعمالها من جانب العميل، وهذا لارتكاب العميل لفعل الاختلاس بالتعدي على البطاقة والسيطرة عليها خارج حدود العقد المبرم بيه وبين البنك.

ويرى جانب آخر من الفقه[3] أن مفهوم الإختلاس يأخذ مفهوماً موسعاً عن مفهوم الإختلاس في جريمة السرقة، فالإختلاس في جريمة خيانة الأمانة يتم باتجاه إرادة الجاني إلى تغيير الحيازة من حساب الغير إلى حسابه الخاص، وهنا قد يقوم الاختلاس دون ضرورة تحقق عملية النقل أو الاستيلاء، وهو الأمر الذي يتماشى مع الطبيعة الخاصة لجريمة خيانة الأمانة في إطار المعاملات الإلكترونية.

كما أن فعل الاختلاس يتمثل في استخدام المال المؤتمن عليه في غايات أخرى خلاف المنصوص عليها في العقد، وأن مجال اختلاس الأموال أو المعلومات المتداولة إلكترونياً تتبلور غالباً في أساليب الغش والاحتيال القائم وفق الأنظمة الإلكترونية.

ثانياً: التبديد.

يقصد بمفهوم التبديد ذلك السلوك الذي يأتيه الأمين على المال بالتصرف فيه بما يخرجه عن حيازته بشكل نهائي وكأنه صادر عن المالك الحقيقي، ولقد ذهب جانب من الفقه الفرنسي[4] إلى أنه يمكن تطبيق صورة التبديد على البرامج والأنشطة ومعدات الأجهزة بما تحويه من ذاكرة تحوي المعلومات المتداولة إلكترونياً, وتكون مسلمة إلى الجاني على عقد قانوني بغرض الاستعمال أو بحيازتها, ثم يقوم باستعمالها استعمالاً يتسبب في تبديدها.

1 جميل عبد الباقي الصغير ، المرجع السابق، ص 127.

2 عمرو إبراهيم الوقاد، الحماية الجنائية للمعلوماتية، بدون دار نشر، مصر، 2016، ص 85.

3 محمد سامي الشوا، المرجع السابق، ص 141.

4 MICHEL Vivant et autres, Op.Cit, p 815

ثالثاً: الاستعمال.

يقصد بالاستعمال الفعل الذي يستخدم به الأمين المال أو الشيء المسلم إليه استخداماً يستنزف قيمته كلها أو بعضها، ويتحقق عنصر الاستعمال من خلال رد الشيئ إلى صاحبه بعد استنفاذ غرضه. وبخصوص مسألة تحقق عنصر الاستعمال في مجال المعاملات الإلكترونية اختلفت الرؤى الفقهية, والمتمثلة في:

1. الإتجاه الأول: الاستعمال التعسفي للمال محل الجريمـــة:

يذهب القضاء الفرنسي إلى رفض فكرة الاستعمال التعسفي للمال المؤتمن كصورة من صور النشاط الإجرامي لجريمة خيانة الأمانة، بينما يتجه الفقه إلى وضع قيدين على عدم العقاب على الاستعمال:

أولاً: استعمال المال مخالفاً للغرض المتفق عليه.

وهنا يأتي استعمال الشيئ مخالفاً للغاية التي خصصت من أجله، ويستوي هذا الحكم في حالة استغلال محلل النظم المعلوماتية فرصة ولوجه في النظام الإلكتروني المخزنة على بطاقات, أو على شرائط ممغنطة شكلاً يخالف ما هو متفق عليه, وذلك بنقلها إلى الغير[1].

ثانياً: استعمال الشيء على نحو يخالف الغاية من الحق.

ويتحقق هذا النوع من الاستعمال في حالة ممارسة الشخص أفعال تمكنه من استغلال المال لمصلحته الشخصية, ويمثل خروجاً عن المصلحة المحققة له، وهنا يتجه بعض الفقه[2] أن فعل الخيانة ينطبق على فعل الجاني الذي يضع فجوات في برامج النظام المعلوماتي، بحيث يسمح له باستخدام الجهاز بطريقة الغش.

2. الاتجاه الثاني: استعمال الآلـــة.

يرى جانب من الفقه[3] أن الاستعمال الواقع بفعل الآلة لا يدخل تحت جرم خيانة الأمانة، وهذا الاستعمال ينسب إلى الشخص الذي يغتصب جهد النظام المعلوماتي لتحقيق غايات شخصية، طالما أن الشخص الذي أوتمن على استعمال الآلة لم يغير من حيازته على الجهاز من حيازة ناقصة إلى حيازة كاملة، ولم يؤدي الاستعمال إلى إتلاف النظام المعلوماتي إتلافاً كلياً أو جزئياً، ولم ينقص من قيمته الحقيقة.

---

1 هدى حامد قشقوش، المرجع السابق، ص 175.

2 Fillon (Bernard), la réception de l'innovation technoloque endroit pénal, R.s.c 1990, p 274-281

3 هدى حامد قشقوش، المرجع السابق، ص 32.

إلا أن البعض الآخر[1] رأى ضرورة تجريم كل الأفعال التي تقوم على استعمال الجهاز بغية استخدامه خارج أوقات العمل، أو أن يكون الولوج إليه بطريقة غير مشروعة، وهنا يواجه الجاني بفعل خيانة الأمانة, على عكس الرأي الأول الذي يدرج هذا الفعل تحت مفهوم السرقة قياساً على اعتداء مال الغير واستخدامه دون رضا صاحبه في غير الغرض المخصص له قياساً على سرقة المعلومات المتداولة إلكترونياً.

3. الاتجاه الثالث: استعمال بطاقات الائتمان.

لقد صنف العديد من الفقهاء مسألة إساءة استخدام بطاقات الائتمان التي تصدر عن البنوك من أهم أوجه جريمة خيانة الأمانة في إطار التعاملات الإلكترونية، إذ يرى جانب من الفقه أن الاستخدام التعسفي لبطاقات الائتمان، كحالة سحب المبالغ المالية من قبل العميل بموجب بطاقات الائتمان والتي تفوق الرصيد الممنوح له وقت السحب, يعد أهم صور خيانة الأمانة على اعتبار خروج العميل على المبدأ المتفق عليه في إطار التعاقد مع البنك بموجب استخدام بطاقات الائتمان، وهنا يأتي الفعل مترجماً لسوء استعمال العميل لبطاقات الائتمان تحت إطار خيانة الإتفاق المبرم بينه وبين البنك، ومن ثم تقوم في حقه المساءلة الجنائية[2].

مع العلم أن هناك توجه آخر[3] قد ارتأى عدم الاعتراف بقيام جريمة خيانة الأمانة وفقاً للاستعمال المبين سلفاً على أساس أن العميل لم يبدد البطاقة التي تسلمها من البنك على سبيل عارية الاستعمال، ولكن قد أساء استخدامها بسحب أكثر من الرصيد، وهذا ما يقيم في حقه المسائلة العقدية بالإخلال بالالتزام التعاقدي.

وهذا الفرض قد أقره حكم المادة 4/462 من القانون الفرنسي رقم 19 لسنة 1988 المتعلق بالغش المعلوماتي[4], والتي رأت إدخاله تحت طائلة الإدخال العمدي لمعلومات إلى النظام المعلوماتي بحيث أن البنك بإعطاء بطاقة الائتمان للعميل لاستخدامها في السحب يكون قد سمح له الدخول إلى النظام، فإذا عمل

1 محمد عبد الرحيم سلطان، جرائم الانترنت والاحتساب عليها، ورقة بحثية قدمت في مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات، العين، ماي 2000، ص 17.

2 Hanachowiz (Lionel), Les cartes bancaires (irregularités) et fraude, Thése doctorat; université Lyon iii 1985, P 342

3 Fillon Bernard, Op, Cit, P 320

4 Loi No :88-19 du 5 janvier 1988 relative à la fraude informatique, P 231

العميل على تغيير أو تعديل معطيات النظام بغية صرف مبالغ تتجاوز رصيده، فيكون بذلك قد أضر بمصلحة البنك، وتحقق في حقه إساءة التصريح بالدخول إلى النظام المعلوماتي.

الفرع الثاني: الركن المعنوي لجريمة خيانة الأمانة في إطار المعاملات الإلكترونية.

تتحقق جريمة خيانة الأمانة بتوافر أحد صور النشاط الإجرامي التي تمت دراستها سابقاً، غير أن قيام الجريمة يستوجب استكمال الركن المعنوي المبني على عنصري القصد العام والخاص للجريمة، وهنا يُثار إشكال بخصوص مدى ضرورة توافر كل القصد العام والخاص في مجال التعامل الإلكتروني؛ نظراً للخصوصية التي تميز العناصر المكونة للنشاط الإجرامي.

أولاً: القصد العام.

يتكون القصد العام من خلال توافر عنصري العلم والإرادة، ويتمثل العلم في القصد العام والمقصود به أن يعلم الجاني أنه تسلم الشيئ تسلماً ناقلاً للحيازة الناقصة، فإذا اعتقد أنه تسلم الأموال أو المعلومات المتداولة وفق المعاملات الإلكترونية تسلماً يمكنه من تملك المال، فهنا ينتفي قيام الجرم على اعتبار انتفاء العلم بتحقق التسلم المؤقت، وأنه سلم على سبيل أحد عقود الأمانة التي تجعل من الشخص مالكاً مؤقتاً للمال، وعلاوة على ذلك يجب أن يتوفر علم الجاني بالضرر الذي يلحق الأمين أو المتعاقد أو المتعامل معه إلكترونياً، وهنا ذهبت محكمة السين بفرنسا إلى إصدار حكم يرفض إدانة العميل الذي يجعل ضرورة رد البطاقة الائتمانية إلى البنك بعد انتهاء صلاحيتها[1]، كما أن القضاء الفرنسي نص على أن القصد الجنائي يتوافر متى انصرفت إرادة الجاني إلى إضافة الأموال إلى ملكه بالتصرف فيه تصرف المالك بسوء نية أي بتوافر عنصر العلم والإرادة.

ثانياً: القصد الخاص.

لا تتوقف جريمة خيانة الأمانة على عنصر العلم والإرادة بالتصرف المنشئ لفعل خيانة الأمانة بناء التزام تعاقدي، بل يجب توافر نية خاصة تترجم اتجاه الجاني إلى تملك الشيء محل الجريمة.

ويرى الفقه الجنائي أن تطبيق ذلك في إطار المعاملات الإلكترونية يؤدي إلى توافر القصد الجنائي في حق الجاني الذي يعمل على الاحتفاظ بالأموال والمعلومات المتداولة إلكترونياً، وتغير صفة الحيازة من ناقصة إلى كاملة بغرض تملكها، فإذا كان قصد الجاني ينصرف إلى مجرد استعمال المال فقط ثم رد الشيئ إلى مالكه الحقيقي فهنا ينفي قيام فعل خيانة الأمانة، بالرغم من وجود توجه فقهي يرى ضرورة توافر القصد العام

1 Hanachowiz (Lionel), Op, Cit, P 572

فحسب، فالركن المادي المتمثل في صوره الثلاث يحمل معنى النية في تغيير الحيازة, ومن هنا فإن نية التملك تتخلل النشاط الإجرامي[1].

ونرى بدورنا أن مجال التعامل الإلكتروني قد يفتح مجالاً للتوسع في أساليب وصور النشاط الإجرامي، إلا أن كل تلك الأساليب تترجم نية الجاني في استعمال أو تبديد الأموال المتداولة إلكترونياً, وهو ما يفسر ضمنياً وجود نية التملك لتلك الأموال، وبهذا قد يفسر توافر القصد العام بتحقق ضمني للقصد الخاص.

[1] علي حسن الطوالبة، المرجع السابق، ص 165.

المبحث الرابع:

الحماية الجنائية من جريمة التزوير في إطار المعاملات الإلكترونية.

تعد جريمة التزوير في المحررات من أهم الجرائم التقليدية التي أولاها التشريع اهتماماً خاصاً لخطورة هذا الأسلوب الإجرامي ودوره في هدم مبدأ الثقة في المعاملات، ولما كان الاتجاه في العصر الحالي هو مسايرة للتطور العلمي وانتشار الحاسب الآلي وحلوله محل الأوراق والوثائق الورقية، فإن الجريمة أصبحت تأخذ منحى أخطر مما كانت تعرف عليه في شكلها التقليدي، الأمر الذي ألزم التشريعات المقارنة إلى السعي نحو تعديل تشريعاتها العقابية لتنظيم الحماية الجزائية من هذه الجريمة أو العمل على استحداث نصوص خاصة تتماشى وهذا النمط الحديث من الجرائم.

وتعد جريمة التزوير الإلكتروني من أخطر طرق الغش التي ظهرت في مجال المعاملات الإلكترونية, على أساس انتشار المعاملات الإلكترونية في شتى المجالات مثل عمليات الدفع وطلبات البضائع, وتحويل الأموال من بنك إلى آخر, ومما يزيد من خطورة الجريمة هو صعوبة اكتشاف وإثبات التزوير في هذا المجال[1].

ولعل التشريعات هي الضمانة الأولى والأبرز لحماية المحررات الإلكترونية، بحيث لم تجدي اجتهادات الفقه والقضاء فائدة في مواجهة التزوير إذا ما اقترف في إطار المعاملات الإلكترونية, مما كان له أثره في ظهور ضرورة لحماية هذه المعاملات تشريعياً.

وفي هذا الإطار يثار إشكال رئيسي مفاده: ما مدى كفاية القواعد التقليدية للتصدي لمعالجة التزوير الإلكتروني ؟

وللإجابة على هذا الإشكال ارتأينا إلقاء الضوء على جوانب هذه الجريمة في تناول جملة من العناصر الأساسية من خلال المطالب التالية:

1 محمد حسام محمود لطفي، الإطار القانوني للمعاملات الإلكترونية، دار النهضة العربية، القاهرة، سنة 2002، ص 40.

المطلب الأول: محل جريمة التزوير في إطار المعاملات الإلكترونية.

قبل التطرق لدراسة أهم العناصر المتعلقة بمحل جريمة التزوير الإلكتروني (الفرع الثاني)، توجب بيان تعريف جريمة التزوير الإلكتروني (الفرع الأول) على النحو التالي:

الفرع الأول: تعريف جريمة التزوير الإلكتروني

لقد تباينت التشريعات المقارنة في مسألة تعريف التزوير، فإذا كانت بعض التشريعات قد أوردت تعريفاً للتزوير في نصوصها كقانون العقوبات الأردني الذي جاء في نص المادة 260 منه كالآتي: "يعد التزوير تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطط يحتج بهما، نجم أو يمكن أن ينجم عنها ضرر مادي أو معنوي او اجتماعي"[1].

فهناك تشريعات أخرى لم تتناول مسألة تعريف التزوير, ومن بينها المشرع الجزائري الذي اقتصر على ذكر طرق التزوير والعقاب عليها، ولعله برأينا اتجاه سليم، ذلك أن المشرع الجزائري قد عمل على ترك الباب مفتوحا لدخول أنماط مستحدثة من الأفعال التي قد تعد تزويراً بخلاف الاتجاه الأول المقيد[2].

ومن بين التعريفات السائدة والمستقرة فقهاً التعريف الذي جاء به الفقيه Garçon والذي جاء فيه أن: "التزوير ما هو إلا تغيير للحقيقة مقترن بقصد الغش يقع في محرر بإحدى الطرق التي بينها القانون, ويكون من شأنه أن يسبب ضرراً للغير، ويجب أن يقترن بنية استعمال المحرر المزور وفقاً لما أعد له"[3].

إن هذا التعريف مُنتقد من ناحيتين: الأولى؛ أنه يوحي من جهة بامتداد جريمة التزوير إلى تغيير الحقيقة في جميع أنواع المحررات، وهذا الأمر غير صحيح على اعتبار أن التجريم لا يقع إلا على المحررات المشمولة بالحماية القانونية. وثانياً: أن هذا التعريف يضيف شرطاً جديداً لقيام جريمة التزوير وهو عنصر الضرر بالرغم أنه لايفترض واقعياً اشتراط الأمر.

وعلى هذا الأساس نرى بأن التزوير يراد به تغيير الحقيقة بقصد الغش بإحدى الطرق المقررة قانوناً في محرر محمي قانوناً.

---

1 تم تنظيم الجرائم التي تنطوي على التزوير في الباب الخامس بالجرائم المخلة بالثقة العامة في قانون العقوبات الأردني في المواد من 236-273 ولقد نص قانون العقوبات الليبي من خلال الباب السابع منه المعنون بالجرائم المخلة بالثقة العامة وأبرزها التزوير في نص المادة 326. **انــظر**: محمود أحمد عبابنة، المرجع السابق، ص 107.

2 أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني (دراسة مقارنة)، بحث مقدم إلى المؤتمر العلمي حول الجوانب القانونية والأمنية للعمليات الإلكترونية، جامعة دبي الإمارات العربية المتحدة, 26-27 أفريل 2003، ص 331.

3 السيد عتيق، جرائم الانترنت، دار النهضة العربية، القاهرة، سنة 2000، ص 119.

وبناءً على ما ذكر, فإن الإشكال الذي يتبادر إلى أذهاننا هو بيان محل جريمة التزوير المتمثلة في المحررات في مجال المعاملات الإلكترونية، على اعتبار أن المحرر الإلكتروني يأخذ طبيعة ومفهوم خاصين، يستلزم معه إيجاد أحكام خاصة تضبطه تختلف عن تلك التي تنظم المحررات التقليدية.

الفرع الثاني: محل جريمة التزوير في إطار المعاملات الإلكترونية.

لقد ثبت عملياً ضيق النصوص التقليدية بشأن مواجهة جريمة التزوير الذي يقع في مجال المعاملات الإلكترونية, وحماية الثقة الواجب توافرها في المحررات الإلكترونية, خاصة مع تعاظم الاعتماد على تلك المحررات في تسيير أمور وشؤون المجتمع الحديث، إلا أن هذا الواقع قد خلق تعارضاً ما بين تطبيق النص الجنائي لجريمة التزوير على التلاعب في البيانات والمعطيات, وعقبة وجود محرر في إطار هذه المعاملات, وقد تباين موقف الفقه والتشريع المقارن بخصوص كيفية تجاوز هذه العقبة؛ أو بعبارة أخرى ما مدى اعتبار المحرر الإلكتروني من قبيل المحررات التقليدية التي يسري عليها النص الجنائي الخاص بجريمة التزوير؟

وقبل الخوض في هذا الجدل توجب بيان موقف الفقه الجنائي والتشريعات المقارنة من مفهوم المحررات الإلكترونية (**أولاً**)، ثم دراسة إشكالية الحجية القانونية للمحررات الإلكترونية (**ثانياً**).

أولاً: مفهـــوم المحررات الإلكترونية.

كما سبق بيانه استقر الفقه والقضاء بأن التزوير هو تغيير الحقيقة في محرر، ويعد هذا المحرر هو عماد جريمة التزوير, ويقصد بالمحرر في شكله التقليدي: "كل وثيقة مكتوبة تتضمن مجموعة مترابطة من الأفكار والمعاني الصادرة عن أشخاص معينين؛ أي يجب أن يكون للمحرر مضمون ومصدر ينسب إليه"[1].

أما بخصوص تعريف المحرر الإلكتروني فلقد ذهب البعض من الفقه[2] إلى تعريفه بأنه:" كل جسم منفصل أو يمكن أن يتم فصله عن نظم المعالجة الآلية للمعلومات، وقد سجلت عليه معلومات معينة سواء أكان معد للاستخدام بواسطة نظام المعالجة الآلية للمعلومات أم مشتق من هذا النوع".

يتبين من هذا المفهوم أن الفقه سعى إلى إيجاد مفهوم للمحررات الإلكترونية من خلال التفرقة بين مفهوم المعطيات الموجودة داخل النظام الإلكتروني، وبين تلك المعطيات الموجودة على المستندات خارج النظام الإلكتروني والتي تشمل المعطيات المخزنة على الدعامات المادية والشرائط الممغنطة.

1 أحمد حسام طه تمام، المرجع السابق، ص 391.

2 Raymons Gassin, la protection pénale d'un nouvelle univers de fait en droit français le systémes de traitement automaste de donnes, actulaire legislataire, Dalloz. 1980, P 15.

إلا أنه أعيب على أنصار التفرقة بين المفهومين أن المشرع لم يتوجه إلى التفريق بينهما صراحة، كما أنه لم يستطع إقامة تفرقة واضحة بين مصطلح المستندات والمعلومات، وهنا ظهر توجه آخر يوسع من مفهوم المحرر الإلكتروني ليشمل إلى جانب المعطيات الموجودة بالنظام الإلكتروني تلك الخارجة عنه أيضاً، ومن ثم فإن جريمة التزوير الإلكتروني يمكن أن يكون محلها المحررات الإلكترونية المتضمنة المعلومات الموجودة داخل النظام الإلكتروني[1].

إلا أن هذا التوجه لم يسلم من النقد؛ لأنه قام على تحليل خاطئ يقوم على أساس ربط المحتوى المعلوماتي للمستند بالسند المادي للمعلومات.

وبهذا ذهب رأي آخر[2] إلى ربط المحررات بالماديات حتى يمكن إضفاء وصف المحرر على المعلومات لا بد أن تكون مخزنة على دعامة مادية كالشرائط الممغنطة، سواء كانت تلك المعلومات موجودة داخل النظام الإلكتروني أم خارجه، المهم أن تكون مؤيدة بعناصر مادية محددة ومرئية.

ثانياً: الحجية القانونية للمحررات الإلكترونية.

اختلفت آراء الفقهاء والتشريعات المقارنة، وتضاربت أحكام القضاء حول فكرة إعطاء المحرر الإلكتروني الحجية القانونية، ومن ثم ثار الجدل حول صلاحية إعمال النصوص الخاصة بالتزوير في شكله التقليدي على المحررات الإلكترونية، وما تحويه من خصوصية في إطار المعاملات الإلكترونية.

ولقد انقسمت الآراء فقهاً وتشريعاً وقضاءً بين مؤيد ومعارض:

1- الموقف القضائي من الحجية القانونية للمحررات الإلكترونية:

لقد كان القضاء أول من طرح الإشكالية الخاصة بالمحرر الإلكتروني في مفهوم جريمة التزوير، وقد تعرض قبل هذا إلى إشكالية البحث في مدى القوة القانونية للمحررات المرسلة بالأجهزة الحديثة، فذهب القضاء في بعض الدول إلى رفض تطبيق فكرة التزوير في المحررات الإلكترونية، ففي فنلندا قضت المحكمة العليا في سنة 1985 بأن تسجيل البيانات الإلكترونية أو المغناطيسية في شكل غير مرئي في ذاكرة نظام كمبيوتر لا تتماشى مع فكرة المحرر في مفهوم جريمة التزوير[3].

1 علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، المرجع السابق، ص 23.

2 هشام فريد رستم، المرجع السابق، ص 333.

3 Crim 2 déc.1997, Juris, P192.

وانتهى القضاء الفرنسي إلى الاعتداد بها في الإثبات في المواد المدنية، فقد قضت محكمة النقض الفرنسية (الدائرة التجارية) بجواز التمسك بالنسخة المرسلة عبر الفاكس, وبالتالي فقد أقرت بحجتها في الإثبات[1].

وقد ذهب القضاء الفرنسي-قبل تدخل المشرع بنص صريح- إلى توافر صفة المحرر في الكتابة الإلكترونية، فجاء حكم محكمة جنح باريس بتوافر وصف المحرر في مفهوم جريمة التزوير. كما تبنت أحكام القضاء السويسري فكرة التزوير على الكتابة الإلكترونية, وانتهت إلى إصدار أحكام أخرى تتعلق بإعمال وصف المحرر على الشرائط الممغنطة في بعض الحالات التي تصلح أن تكون فيها حجة للتمسك بها[2].

2- الموقف الفقهي من الحجية القانونية للمحررات الإلكترونية:

لقد انقسم الفقه بين مؤيد ومعارض لفكرة صلاحية المحررات الإلكترونية للخضوع لأحكام جريمة التزوير.

أ. الاتجاه المؤيد:

ويرى أنصار هذا الاتجاه أن المحررات الإلكترونية تعتبر من قبيل المحررات الخاضعة لجريمة التزوير وحجتهم في ذلك:

- إن المحرر يستند إلى مفهوم يتضمن أية فكرة أو معلومات مكتوبة على أوراق، أو من خلال صوت أو صورة، وبهذا يأخذ المحرر الإلكتروني المفهوم الحديث للمحرر في جريمة التزوير.
- ذهبت بعض التشريعات إلى عدم اشتراط صيغة محددة للمحررات مما يفسر توجه المشرع إلى الاعتراف بقابلية المحررات الإلكترونية إلى أن تكون محل جريمة التزوير[3].

ولقد جاء تعريف المنظمة الدولية للمواصفات والمقاييس (ISO) متوافقاً مع هذا الإتجاه؛ بحيث عرف المحررات بأنها :" مجموعة من المعلومات والبيانات المدمجة على دعامة مادية بشكل دائم، بحيث يسهل قراءتها مباشرة عن طريق الإنسان أو باستخدام آلة مخصصة لذلك".

1 **نقلاً عـــــن**: محمود إبراهيم غازي، المرجع السابق، ص 494.

2 Rymons.Gassin (R) , Op. Cit, P 29

3 محمد سامي الشوا، المرجع السابق، ص 15.

ويرى أصحاب الرأي القائل بضرورة أن الكتابة المؤلفة من علامات أو رموز مرئية بوصفها شرطاً مفترضاً لجريمة التزوير في المحررات تمثل عقبة تحول دون إمكانية نشوء هذه الجريمة في حالة التلاعب في البيانات المسجلة على دعامة مادية، بحيث أنه يمكن التغلب على هذه العقبة إذا ما سمح بتغليب روح النص على اللفظ واعتبار أن ما يظهر على الشاشة أنماط مستحدثة للمحرر يمكن أن يقع عليه التزوير[1].

ب. الإتجاه المعارض:

يرفض هذا الاتجاه التكييف السابق لمؤيدي فكرة قابلية التزوير في المحررات الإلكترونية، ويستندون في ذلك أن المشرع عند جرم تزوير المحررات اشترط وجود الكتابة المادية، أما عملية الكتابة التي تتم إلكترونياً، ما هي إلا عبارة عن ومضات كهرومغناطيسية مشفرة لا تقرأ بشكل مباشر تقرأ من الحاسوب مع افتقادها لخاصية الثبات.

كما أن جريمة التزوير لاتقع إلا إذا توافرت نية استعمال المحرر المزور من أجل ما حرر فيه، وهذه النية لا يمكن أن تتواجد في البيانات التي لا تزال مبرمجة ذلك أنها غير معدة أصلاً لتقديمها للتعامل[2].

ونرى أن الحماية الجنائية مقررة لمصلحة العامة التي ترتبط بالثقة في المحررات, وبالتالي فإن الاعتراف بالحجية القانونية للمحررات الإلكترونية في الإثبات هو الموقف الأسلم لإسباغ الحماية الجنائية على المعاملات الإلكترونية، وخاصة إذا نظرنا إلى تركيبة المحررات الإلكترونية, والتي تقوم على الخصائص التي تمنحها القوة القانونية خاصة بعد انتشار وسيلة التعاملات الإلكترونية وذيوعها في شتى المجالات.

ثالثاً: الموقف التشريعي من الحجية القانونية للمحررات الإلكترونية.

بعد التطرق للجدل العميق بصدد مسألة الاعتراف بالحجية القانونية للمحررات الإلكترونية, ومدى قابليتها لأن تكون صالحة كمحل لجريمة التزوير بشكله التقليدي، يأتي دور التشريع الذي يعد السبيل الوحيد لإزالة هذا الجدل بتبني موقف واضح، وعلى هذا الأساس سنتناول الموقف التشريعي من المسألة بداية من موقف التشريعات الدولية كالقانون التجاري الدولي "الأونيسترال"، ثم قانون التجارة الإلكترونية في ظل المشروع الأوروبي، ثم نستعرض بعض المواقف التشريعية المقارنة.

1 محمود أحمد عبابنة، المرجع السابق، ص 111.

2 شيماء عبد الغني عطاالله، المرجع السابق، ص 82.

1- موقف القانون التجاري الدولي "الأونيسترال":

تنص المادة 11 من القانون النموذجي للتجارة الإلكترونية[1] على أنه: "في سياق تكوين المحررات وما لم يتفق الطرفان على غير ذلك، يجوز استخدام رسائل البيانات للتعبير عن العرض وقبول العرض، وعند استخدام رسالة البيانات في تكوين المحرر، ولا يفيد المحرر صحته أو قابليته للتنفيذ لمجرد استخدام رسالة بيانات لذلك الغرض".

وتعني "رسالة البيانات" ذلك البديل الإلكتروني للمحرر المكتوب وتعريف الرسالة في المادة 1/2 من الأونيسترال بأنها: "المعلومات التي يتم إنشاؤها مشابهة أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو وسائل مشابهة بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية, أو البريد الإلكتروني أو التلكس أو النسخ الورقي".

وبهذا ساوى القانون المذكور بين الكتابة الإلكترونية والكتابة التقليدية, حيث نص في المادة 6-1 على أنه: "يشترط القانون أن تكون المعلومات مكتوبة تستوفي رسالة البيانات ذلك الشرط إذا تيسر الاطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا".

2- موقف قانون التجارة الإلكترونية في ظل المشروع الأوروبـــي:

لقد عمل المشرع الأوروبي على إدراك ضرورة الحاجة إلى التدخل التشريعي لتفعيل الإثبات بالمحررات الإلكترونية، والتنسيق بين التشريعات وذلك لطبيعة المعاملات ومالها من تأثير على نوع المعاملات ذات العنصر الأجنبي، وذلك بعدم انتاجها آثارها المنشودة في التعامل في حالة عدم اعتماد هذا النوع من المعاملات أو الاعتراف بحجية المحررات الإلكترونية خاصة في إطار التجارة الإلكترونية.

ولقد تأثر المشروع الأوروبي لقانون التجارة الإلكترونية[2] بالقانون الموحد للتجارة الإلكترونية "الأونيسترال" الذي أعد بمعرفة الأمم المتحدة، فاعترف ذلك المشروع بقبول المحررات الإلكترونية, وتحديد حجيتها في الإثبات، وهذا من خلال أخذه بمبدأ المساواة بين المحرر الإلكتروني والأدلة الكتابية, وهو ما يعرف بمبدأ المساواة الوظيفية في الإثبات ودون الاعتداد بشكل أو وسيلة الإثبات[3].

---

1 القانون النموذجي للتجارة الإلكترونية "اليونسترال" الذي اعتمدته لجنة الأمم المتحدة للقانون التجاري الدولي بناءً على القرار الذي اتخذته الجمعية العامة 2205 (د.21) المؤرخ في 1996/12/17.

2 محمد سامي الشوا، المرجع السابق، ص 15.

3 د.عمر الفاروق الحسيني، المرجع السابق، ص 83 وما بعدها.

3. موقف التشريعات المقارنة:

لقد حسم المشرع الفرنسي الأمر بعد الجدل الكبير على مستوى المحاكم القضائية؛ فنص صراحة على الاعتداد بالمحرر الإلكتروني في جريمة التزوير, وهذا من خلال توسيع مفهوم التزوير ليمتد إلى المحررات الإلكترونية، ويظهر هذا من خلال حكم المادة 1/441 الواردة في القسم الأول من الكتاب الرابع من قانون العقوبات الفرنسي تحت عنوان "الاعتداءات ضد الثقة العامة" [1].

وبالتالي اعتبر النص الأخير أن الوثيقة محل التزوير تشمل أيضاً إلى جانب الشكل التقليدي لها كل وسيط آخر للتعبير عن فكرة أو معاني معينة، لكن يجب أن يكون لها قيمة ثبوتية؛ أي أن تصلح أن تكون دليلاً لإثبات حق أو واقعة لها آثار قانونية وفقاً للقانون، وبهذا فإن النص قد أتاح فرصة احتمال معاني أوسع عن النمط التقليدي للأوراق الورقية ومنها الدعامات المادية كالأقراص الإلكترونية أو البطاقات أو الشرائح الممغنطة مع توافر شرط صلاحيتها لإثبات حق محمي قانوناً.

مع العلم أن المشرع الفرنسي قد نص وفقاً للقانون الخاص رقم 19/88 المؤرخ في 1988/01/05 الخاص بالجرائم المعلوماتية، ومن خلال نص المادة 5/462 حيث يقوم مضمون النص على تجريم تزوير الوثيقة المعالجة آلياً مهما كان شكلها بشرط أن تسبب ضرراً للغير، وهو توجه من المشرع بإفراد نص خاص خارج عن قانون العقوبات لمواجهة تزوير المحررات الإلكترونية.

إلا أنه بعد التعديل الذي مس قانون العقوبات الفرنسي، والذي غطى على الأخذ بمضمون المادتين 4/462 و5/462 من القانون السالف الذكر، على اعتبار أن المادة المستحدثة في نص قانون العقوبات (1/441) قد أعطت مفهوماً موسعاً للمحررات المزورة لتشمل المحررات الإلكترونية[2].

كما أن المادتين قد لاقتا اعتراضاً من مجلس الشيوخ عند مناقشة القانون لما تضمن محتواهما من مساواة بين المعطيات المعلوماتية بصفة عامة وبين المحررات من حيث القيمة القانونية، كما نصت المادة

[1] **Article n 441/1 du CPF**: constitue un faux toute altération frauduleuse de la vérité, de nature a causer un préjuduce et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peyt avoir pour effet d'établir la preuve d'un droit ou d'un44 faut ayant des consequences juridique

2 أشرف توفيق شمس الدين، المرجع السابق، ص 343.

1316 من القانون المدني الفرنسي على أن المحرر الإلكتروني له القوة في الإثبات مثله مثل المحرر الورقي بشرط تحديد هوية الشخص مصدر المحرر، وأن يتم تدوينه والاحتفاظ به في ظروف تسمح بضمان سلامته[1].

وبما أن المشرع الأوروبي دعى الدول الأعضاء إلى تبني تشريعات تنظم مسألة حجية المحررات الإلكترونية في الإثبات، فلقد أصدر المشرع الفرنسي القانون رقم 230 لسنة 2000 والصادر في 13 مارس 2000، وكان من شأن ذلك القانون تطوير قانون الإثبات حتى يتماشى مع تكنولوجيا المعلومات والتوقيع الإلكتروني[2].

ونظراً للأهمية البالغة للجرائم المعلوماتية والمحررات الإلكترونية، فلقد جاء موقف المشرع الأمريكي صريحاً من خلال إصداره لجملة من التشريعات المتعلقة بجرائم الكمبيوتر والجرائم الملحقة بها، ولقد أجاز المشرع الأمريكي من خلال القانون الاتحادي للتوقيع الإلكتروني العالمي قبول استخدام التوقيع والمحررات الإلكترونية في التعاملات التجارية الدولية، وإعمالاً لنصوص هذا القانون يتم الاعتراف بالمحررات الإلكترونية كمحل لجريمة التزوير؛ بحيث أنها تعتبر منتجة لنفس الآثار القانونية الناشئة عن المحررات الإلكترونية.

ولقد اعترف المشرع الجنائي السويسري من خلال تعديل المشرع لمفهوم المحرر ليشمل المحررات الإلكترونية حيث نص على أن الكتابة على دعامات للبيانات ودعامات الصور تعتبر في حكم المحررات، وبالتالي قد أصبح مفهوم المحرر يتسع ليشمل المحررات الإلكترونية.

ولقد حذا المشرع المصري نفس حذو التشريعات المقارنة بالاعتراف بفكرة المحرر الإلكتروني من خلال إصدار قانون التوقيع الإلكتروني[3] رقم 15 لسنة 2004 في المادة 15 والتي جاء فيها:"للكتابة الإلكترونية والمحررات الإلكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية متى استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون".

---

1 (D) Mangnot, Droit de la preuve et technologies nouvelles, droit de la preuve formation permanete,Cup.vol xix.oct 1997, P 99.

– **مشار إليه لدى:** محمود إبراهيم غازي، المرجع السابق، ص 517.

2 Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve au technologies de l'information et relative à la signature électronique (J.O du 14 mars 2000, P 3968).

3 قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 المؤرخ في 2004/11/10 الجريدة الرسمية عدد 71 الصادرة بتاريخ 2004/11/10.

وجاءت المادة 16 من ذات القانون لتؤكد على أن: "الصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي حجة على الكافة بالقدر التي تكون فيها مطابقة لأصل هذا المحرر، وذلك ما دام المحرر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين على الدعامة الإلكترونية"[1].

ولقد جاء موقف المشرع الإماراتي مجسداً في القانون الاتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات, والذي جرم فعل تزوير المستندات الإلكترونية, وخص هنا المحررات الإلكترونية الخاصة بالهيئات الحكومية أو المؤسسات العامة أو استعمال هذه الملفات مع العلم بتزويرها، كما قد عرف المحرر الإلكتروني من نفس القانون السابق الذكر والتي جاءت في إطار تعريف للمصطلحات المستخدمة في القانون, وعرف بأنه: "سجل أو بيان معلوماتي يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط"[2].

وأما عن موقف المشرع الجزائري فلقد اتخذ نفس الموقف التشريعي للدول السابقة من خلال الاعتراف بحجية الكتابة الالكترونية، وبالتالي الاعتراف بالمحررات الإلكترونية في الإثبات, وهذا من خلال النص المستحدث 323 مكرر 1 بموجب القانون 05-01 المتضمن تعديل القانون المدني, والتي جاءت صيغتها كالتالي: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

وبالرغم من ذلك, إلا أنه لم يصدر أي نص صريح يتعلق بالتزوير في نصوص العقوبات، ولعل ذلك يستوجب استكمال موقف المشرع باستحداث نصوص جنائية خاصة تتضمن الاعتراف بالتزوير في المحررات الإلكترونية.

المطلب الثاني: أركان جريمة التزوير في نطاق المعاملات الإلكترونية.

تقوم جريمة التزوير شأنها شأن الجرائم الأخرى بتوافر الركن المادي المتمثل في السلوك الإجرامي الذي يترجم في صور النشاط الإجرامي، وهنا تأخذ جريمة التزوير خصوصية تكمن في تقسيم النشاط الإجرامي إلى صنفين؛ أولهما تغيير الحقيقة في المحرر، وثانيهما يتمثل في طرق التزوير المنصوص عليها قانوناً، أما الركن

1 أحمد حسام طه تمام، المرجع السابق، ص 253.

2 انظر المادة 01 والمادة 06 من القانون الاتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الإماراتي، السابق الذكر.

المعنوي فهو الشق القائم على استكمال السلوك الإجرامي بتوافر الإرادة والعلم في ارتكاب الجرم مع النية في استعمال المحرر الإلكتروني المزور.

الفرع الأول: الركن المادي لجريمة التزوير في نطاق المعاملات الإلكترونية.

أرجع العديد من الفقه قيام الركن المادي لجريمة التزوير عموماً إلى ثلاث عناصر: أولها تغيير الحقيقة, وثانياً: أن يقع التغيير على محرر, وثالثاً: أن يتم التغيير وفقاً للطرق التي حددها القانون.

أولاً: تغيير الحقيقــة.

وهو السلوك الإجرامي الذي يمثل عماد الركن المادي في جريمة التزوير؛ لأنه يقع على محرر، ويتمثل في تغيير الكتابة في المحرر على نحو مخالف للحقيقة، فإذا لم يحدث فعل التغيير ينتفي معه جرم التزوير ولو كان الفاعل يعتقد أنه يثبت غير الحقيقة.

ويقصد بتغيير الحقيقة ذلك التغيير الذي يترتب عليه المساس بالمركز القانوني للغير دون رضائه، وقد يقع هذا التغيير على جزء من المحرر كما قد يقع على المحرر بأكمله، وتشترط التشريعات المقارنة أن يقع على محرر سواء كان المحرر متواجداً من قبل ثم أدخل عليه التغيير أم أنشئ بأكمله من أجل تغيير الحقيقة به[1].

ويرى بعض الفقه[2] وجوب أن تكون الكتابة في المحرر مركبة من حروف وإن لم تتوافر شكل الكتابة المعروفة مثل الكتابة المختزلة والشفرة السرية، وهذا ينطبق على البيانات الموجودة على الحاسب الآلي على الذاكرة المعالجة آلياً، فإذا وقع عليها الاعتداء وخرجت في صورة محرر مكتوب توافرت جريمة التزوير, ولا عبرة بالدعامات التي استندت إليها الكتابة سواء كانت على ورق أو أسطوانات أو ديسكات.

ولقد واجه المشرع الفرنسي مسألة تغيير الحقيقة كنشاط رئيسي لوقوع جريمة التزوير في إطار المعاملات الإلكترونية ليعالج قصور قانون العقوبات في نصوصه العامة في مواجهة المستجدات في مجال المعاملات، ثم تدخل مرة بتعديل لاحق في سنة 1994 في المادة 3/333 من قانون العقوبات الفرنسي الجديد وهي المقابلة للمادة 4/462 من القانون رقم 19 لسنة 1988، ولم تكن هذه الصورة الوحيدة لتجريم تغيير الحقيقة أو التعديل بغير حق في البيانات التي تحتويها النظم الآلية لمعالجة المعلومات، بل توقع المشرع أن تحدث هذه النتيجة لغير قصد كنتيجة اقتحام هذه النظم بطريق الغش، فجاء ذلك في نص الفقرة الثانية من

1 هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، سنة 1999، ص 16.

2 محمد سامي الشوا، المرجع السابق، ص 156؛ **انـــظر ايضاً**: هشام فريد رستم، المرجع السابق، ص 337.

المادة 1/133 من قانون العقوبات الفرنسي الجديد وهي التي كانت تقابل المادة 1/462 من القانون رقم 19 لسنة 1988.

ثانياً: طرق جريمة التزوير في نطاق المعاملات الإلكترونية.

لا يكفي وقوع التزوير في المحرر طبقاً للتشريعات المقارنة، وإنما يجب أن يقع بإحدى الطرق التي يحددها التشريع، والتزوير من حيث ارتكابه ينقسم إلى نوعين : التزوير المادي والتزوير المعنوي.

1- طرق التزوير المادي:

إن ما يهم في إطار بيان طرق التزوير المحددة بموجب القانون هو التعرف على الطرق التي يلجأ إليها مرتكبوا جرائم التزوير في المحررات الإلكترونية عن طريق التدخل بصور مختلفة من خلال النظام الإلكتروني، فتغيير المحررات يمكن أن يتم عن طريق الحذف بإزالة كلمة أو رقم أو رمز معين، ويمكن أن يتم عن طريق الإضافة بزيادة رقم على مبلغ أو بإضافة عبارات أو بيانات غير صحيحة أو عن طريق الإبدال بحذف شيئ من المحرر وإثبات شيئ آخر بدلاً منه[1].

ومثالها قضية مشرف تشغيل الحاسب الآلي بأحد البنوك الأمريكية الذي كان يعمل على تزوير حسابات أصدقائه في البنك، بحيث يزيد من أرصدتهم وبالتالي يمكنهم من سحب تلك المبالغ، ولقد قرر التوقف عن هذا الفعل قبل المراجعة الدورية لحسابات البنك إلا أن طمع أصدقائه أجبره على الاستمرار إلى أن تم اكتشافه من قبل برنامج لتفعيل أمان الحسابات في البنك, وبالتالي تم القبض عليه[2].

ومما لاشك فيه أن البدء التدريجي في التحول إلى الحكومات الإلكترونية سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك مما يسهل الدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة وتزوير البيانات لخدمة أهدافهم الإجرامية.

2- طـــرق التزوير المعنوي:

يقع التزوير المعنوي من خلال التدخل في النظام الإلكتروني لتسجيل بيانات لم تصدر عن أطراف المعاملات أو أولي الشأن أو إثبات وقائع كاذبة غير معترف بها، أو إغفال معلومة أو إيرادها على وجه غير صحيح, مما يسبب تحريفاً للحقيقة في المحررات الإلكترونية، وإذا كانت طرق التزوير هي الأكثر وقوعاً بالنسبة للمحررات الإلكترونية بالحذف أو بالإضافة وكذلك الإصطناع، فإن المشرع قد يخرج بعض تلك

1 هلالي عبد اللاه أحمد ، تفتيش نظم الحاسوب وضمانات المتهم المعلوماتي، درا النهضة العربية، القاهرة، سنة 1997، ص 214.

2 عمرو وقاد، المرجع السابق، ص 99.

المحررات –كما في حالة بطاقات الائتمان الممغنطة– من إطار قواعد التزوير في النصوص العامة لتحكمها نصوص خاصة، ومثال ذلك القانون الفرنسي الصادر في 30 ديسمبر 1991 الذي يتضمن نصاً يعاقب على اصطناع أو تزوير بطاقات الدفع أو السحب، ويعد هذا النص الخاص مقيداً للنص العام[1].

ونرى أن الطبيعة الخاصة للمعاملات الإلكترونية قد تجعل الطرق التقليدية للتزوير غير مناسبة للتطبيق في هذا المجال بسبب طبيعة البيانات الإلكترونية؛ ذلك أن بعض السلوكات كتغيير كلمة المرور أو استبدالها قد لا يمكن تصنيفه ضمن أعمال تزوير المحرر الإلكتروني، وبالتالي فإن الأمر يحتاج من التشريعات التدخل بنصوص خاصة تعاقب على الجريمة أو إدخال تعديلات على النصوص العقابية التقليدية تنص على التجريم على مثل هذه الأنماط من الطرق المستحدثة في إطار جريمة التزوير.

الفرع الثاني: الركن المعنوي لجريمة التزوير في إطار المعاملات الإلكترونية.

لا يمكن الإعتراف بتوقيع العقوبات وفقاً للتشريعات العقابية إلا طبقاً للمسؤولية الجنائية، ولن تكون هنا جريمة إن لم يثبت قيام إرادة الجاني لارتكابها، وبالتالي تطلب إدراكه بالنشاط الجرمي المكون للجريمة.

والقصد الجنائي في جريمة التزوير لا يخرج عن أمرين: الأول هو علم الجاني بارتكابه للجريمة بجميع عناصرها؛ وهنا نقصد به إدراك الجاني بقيامه بفعل تغيير الحقيقة في المحرر الإلكتروني, ومن شأن هذا التغيير الإضرار بالغير. والثاني هو القصد الذي يخص الجريمة في حد ذاتها فيتمحور في فكرة استعمال المحرر المزور فيما زور من أجله مع العلم تماما بتوافر التزوير في هذا المحرر[2].

أولاً: القصد الجنائي العام لجريمة التزوير الإلكترونــي.

تعد جريمة التزوير من الجرائم العمدية التي لاتقوم إلا بقيام القصد العام، ويتطلب ذلك العلم بمكونات الجريمة، ومن بينها المحرر وانصراف إرادة الجاني إلى تغيير الحقيقة بإحدى الطرق المبينة قانوناً مع توقعه احتمال حدوث ضرر مادي أو أدبي جراء هذا الفعل، وينتفي القصد الجنائي العام لدى الشخص الذي يعمل على تغيير الحقيقة سواء على المحررات الورقية أو الإلكترونية مع عدم علمه بالمساس بالمحررات المتمتعة بحماية القانون[3].

1 Rymons Gassin .Op. Cit, p 49.

2 عمر الفاررق الحسيني، المرجع السابق، ص 83.

3 جميل عبد الباقي الصغير، المرجع السابق، ص 165.

ولقد ذهب جانب من الفقه الجنائي إلى الاعتراف بقيام جريمة التزوير متى انصرفت إرادة الجاني إلى تغيير الحقيقة في المحررات الإلكترونية مهما كانت الطريقة المستخدمة لإيقاع التغيير وهذا بعدم حصر الطرق في مجال المعاملات الإلكترونية كماهو الحال بالنسبة للمحررات الورقية.

ولعل هذا الإتجاه قد أعطى مرونة في الصيغة التشريعية لتجريم التزوير بما ينسجم مع طبيعة المعاملات الإلكترونية التي تقوم على التعداد التقني لأشكال المحررات الإلكترونية ووسائل التغيير, وكذلك التطور الحاصل فيها.

ثانياً: القصد الجنائي الخاص في جريمة التزوير الإلكترونــي.

والمقصود بالقصد الجنائي الخاص لجريمة التزوير؛ اتجاه نية الجاني لاستعمال المحررات المزورة للحصول على أهداف شخصية من شأنه تحقيقها بالمحرر مع العلم بتزويره.

ونجد أن كلاً من المشرع الفرنسي والمصري لم يتعرضا إلى تعريف جريمة التزوير، إلا أننا نجد النص على عبارات مثل "نية الإضرار" و"نية الغش" التي تمثل القصد الجنائي الخاص، وقد ترددت نفس العبارات في قررات المحاكم وآراء الفقهاء، فقد جاء في قرار لمحكمة النقض النقض المصرية أن القصد الجرمي في جريمة التزوير إنما يعني تعمد تغيير الحقيقة في محرر من شأنه أن يسبب ضرراً للغير أو نية استعمال هذا المحرر فيما زور من أجله[1].

وتعتبر الصيغة التشريعية للنص الفرنسي في تجريم التزوير واضحة في تطلب هذا القصد حيث يشير النص إلى ضرورة وقوع التزوير بنية الغش؛ أي أن المشرع اشترط إلى جانب القصد العام لدى الجاني توافر قصد خاص قوامه غرض الجاني في استعمال المحرر للتأثير في إثبات حق أو واقعة قانونية. ولقد نصت اتفاقية بودابست حول الإجرام المعلوماتي من خلال نص المادة السابعة (07) منها إلى الإشارة إلى القصد الخاص بإتاحتها للدول الأطراف أن يشترطوا في قوانينهم الداخلية نية الغش في تغيير الحقيقة أو نية الإضرار بالغير[2].

1 **نقلاً عــن:** أحمد خليفة الملط، المرجع السابق، ص 484.

2 شيماء عطاالله عبد الغني، المرجع السابق، ص 81.

الفصل الثانـــي:

الحماية الجزائية من الجرائم المستحدثـــة في إطار التعامل الإلكتروني

الفصل الثاني:

الحماية الجزائية من الجرائم المستحدثة في إطار المعاملات الإلكترونية.

إن الواقع العملي أثبت أن خطورة الجرائم المتعلقة بمجال المعاملات الإلكترونية لم تقتصر على أنماط الجرائم التقليدية، بل تعدتها إلى ظهور سلوكات إجرامية مستحدثة نشأت تبعاً للطبيعة الخاصة للتعامل الإلكتروني، وهي تمس بشكل خاص الإطار الخاص بنظم المعالجة الآلية للمعطيات التي يقوم عليها قوام التعاملات الإلكترونية (المبحث الأول)، وكذا ظهور نوع آخر من التعدي على آليات التعامل الإلكتروني كنظامي الدفع الإلكتروني والتوقيع الإلكتروني والمساس بخصوصيتهما (المبحث الثاني)، من جانب آخر تحتاج التعاملات الإلكترونية إلى إحاطة أعمال الوسطاء الفنيين القائمين على تزويد مستخدمي الشبكة بخدمة الانترنت والخدمات الملحقة بها بجملة من الأحكام التشريعية ضد التجاوزات والخروقات الناجمة عن أنشطتهم الفنية والتي تؤثر بشكل واضح على سلامة وأمن التعامل الإلكتروني (المبحث الثالث).

ولهذا استدعت الضرورة استحداث نصوص خاصة لمواجهة هذه الجرائم لتحقيق الفعالية التشريعية لحماية المعاملات الإلكترونية، وهذا ما حاول الفكر القانوني الدولي تجسيده من خلال الإستقرار على ضرورة وجود نصوص خاصة بالمال المعلوماتي، وهو التوجه الذي سار إليه المشرع الجزائري باستحداث نصوص خاصة بتجريم هذا النوع من السلوكات في ظل تعديل قانون العقوبات بموجب الأمر 04-15، والذي تناول فيه جملة من الأحكام الهادفة لمواجهة الإجرام المعلوماتي.

المبحث الأول:

الحماية الجزائية من الجرائم المتعلقة بتداول البيانات وسلامة المواقع الإلكترونية.

يعد النظام المعلوماتي حقلاً للقيام بالمعاملات الإلكترونية المختلفة التي تجري على عدة مستويات، والتي مكنت الأفراد من الاستعانة بهذا النظام في ظل تبنيها للأنماط الحديثة في التعاملات على مستوى الأجهزة الحاسوبية وشبكة الانترنت، بالرغم من أن الواقع أثبت خطورة الاعتداءات الإلكترونية الماسة بالأنظمة المعلوماتية كوجه مستحدث للجرائم الإلكترونية، بحيث تكمن هذه الخطورة في شتى الانتهاكات الواقعة على البيانات المتداولة إلكترونياً (المطلب الأول)، التي تشكل سلسلة متكاملة إلى حد بعيد ومتصلة بجوانب التعاملات الإلكترونية، الأمر الذي يتطلب إسباغ الحماية الجنائية على ذلك النظام مما قد يتعرض له من مساس بسلامة وسرية البيانات الخاصة بالمعاملات الإلكترونية (المطلب الثاني).

ولقد ترجمت هذه الحماية على مستوى التشريعات المقارنة التي تدخلت لتجريم جملة من الأفعال الواقعة على البيانات الإلكترونية والنظام المعلوماتي، وبهذا كان من مقتضى الحال التعرض لهذه الجرائم وتبيان معالم الحماية المقررة في هذا المجال وفقا لما يأتي:

المطلب الأول: الجرائم الواقعة على نظم المعالجة الآلية للمعلومات وتداول البيانات الإلكترونية.

إن مفهوم الحماية الجنائية من الجرائم المستحدثة يرتكز أساساً على طائفة الجرائم المرتكبة بواسطة تكنولوجيا المعلومات، وتحمل مفهومها المعاصر في نظم المعالجة الآلية للمعلومات، إضافة إلى البيانات المتداولة عبر المعاملات الإلكترونية.

ونظراً للانتشار الواقع لتكنولوجيا المعلومات والتدفق الدولي للمعلومات عبر شبكة الانترنت، بات من الضروري ضمان أمن البيانات نظراً لأهميتها المتزايدة، وازدياد اعتماد الأفراد والدول عليها في شتى المعاملات الإلكترونية[1]،ومن هنا طغت فكرة وجوب الحماية الجنائية لنظم المعالجة الآلية للمعلومات من الاعتداءات (الفرع الأول)، وكذا الحد من الانتهاكات الواقعة على تبادل البيانات الإلكترونية (الفرع الثاني).

الفرع الأول: الحماية الجنائية من الجرائم الماسة بسلامة الأنظمة المعلوماتية والبيانات الإلكترونية.

يرى الفقيه حسام الدين الأهوائي نقلاً عن الفقيه الفرنسي "لوكا" بأن أنظمة المعالجة الآلية للمعطيات؛ يراد بها: "مجموعة العمليات التي تتم آليا أي باستخدام الحاسب الآلي، وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات الاسمية، ومجموعة العمليات التي تتم آلياً بغرض استغلال المعلومات، وخصوصاً عمليات الربط أو التقريب وانتقال المعلومات الاسمية ودمجها مع بيانات أخرى، أو تحليلها للحصول على معلومات ذات دلالة خاصة"[2].

ويتبين من هذا المفهوم بأن المعالجة الآلية للمعلومات هي عبارة عن مجموعة من العمليات المتسلسلة التي تبدأ بجمع البيانات داخل الحاسب الآلي وتطبيق المعالجة عليها وإخراجها بصورة معلومات.

أما بخصوص مفهوم نظام المعالجة الآلية للمعلومات فلقد أغفله التشريع الفرنسي، وكذلك المشرع الجزائري وفقاً للقانون رقم 04-15 المعدل لقانون العقوبات، بحيث اكتفى بتحديد الاعتداءات التي تمثل جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ولم يورد تعريفاً خاصاً بنظام المعلومات حتى إصدار القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3]

1 محمود أحمد عبابنة، المرجع السابق، ص 121.

2 حسام الدين الأهوائي، الحق في احترام الحياة الخاصة (الحق في الخصوصية): دراسة مقارنة، دار النهضة العربية، ط2، 2002، ص 145.

3 القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج رج عدد 47 المؤرخة في 2009/08/16، ص 5.

وفقا لنص المادة 02 التي جاءت بجملة من المفاهيم المنصوص عليها في هذا القانون، بحيث عرف المنظومة المعلوماتية بأنها:" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[1]. وبذلك يكون المشرع الجزائري قد ساير المفهوم الوارد في الاتفاقية الدولية للإجرام المعلوماتي "بودابست" في تعريفها للمنظومة المعلوماتية[2]. ونفس الموقف للمشرع المصري الذي تدارك مسألة إدراج مفهوم النظام المعلوماتي وهذا من خلال القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات في نص المادة الأولى منه والتي نصت على :" النظام المعلوماتي: مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية".[3]

البند الأول: الجرائم الخاصة بنظم المعالجة الآلية للمعطيات وآليات الحماية المكرسة لها.

يمكن أن يقع الاعتداء على أحد المراحل المذكورة سابقاً في نظم المعالجة الآلية للمعلومات، وبهذا نجد أن الاعتداءات قد تأخذ صورتين؛ أولاها تقع على وظائف نظام المعالجة الآلية للمعلومات، والتي يمكن بلورتها في عمليات الإتلاف والمساس بالبيانات الداخلة في إطار سير الأنظمة, مما يحدها عن القيام بمهمة المعالجة، والصورة الثانية تقتصر على عمليات الاستعمال غير المشروع لنظام المعالجة من خلال بعض السلوكيات التي تأخذ شكلاً غير إجرامياً في الأصل، ثم تتعداه لتشكل خطورة على سير النظام وسلامة البيانات وسريتها؛ والمتمثلة في فعل الدخول أو البقاء غير المشروع لأنظمة المعالجة الآلية للمعلومات.[4]

1 انظر المادة 2 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السابق الذكر.

2 **Article 01 du coversation Bodabast**: "Systéme informatique: désigne tout dispositif isolé ou ensemble de dispositif interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme , un traitement automatisé de données" disponible sur ligne suivant : *www.eastlaw.blogspot.com/2010/03/23-11-2001.html.*

3 قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات المؤرخ في 14 اوت 2018 الجريدة الرسمية العدد 32 مكرر ج ص 03.

4 عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في التشريعات العربية، دراسة مقارنة ، دار النهضة العربية، ط1، مصر ، سنة 2009، ص 22.

أولاً: جريمة إتلاف البيانات الإلكترونية.

يتمثل فعل الإتلاف في كل السلوكيات التي تؤدي إلى التعييب أو التأثير على مادة الشيء على نحو يُذهب أو يُقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له، مما يحقق شكل الاعتداء المعاقب عليه قانوناً[1].

وتتم جريمة إتلاف البيانات المعالجة إلكترونياً بأي فعل يؤدي إلى محو المعلومات أو البرامج كلياً أو تدميرها إلكترونياً، أو أن يتم تشويه المعلومات أو البرامج على نحو يؤدي إلى إتلافها وجعلها غير صالحة للاستعمال[2].

وبناءً على ماذكر يمكن القول أن جريمة إتلاف البيانات المعالجة إلكترونياً تعد من جرائم الغش المعلوماتي؛ لما تنطوي عليه من تلاعب في الأنظمة المعلوماتية من خلال البرامج المعالجة المعالجة آلياً، وبهذا فإن جل الأفعال الممثلة لعملية الإتلاف إلكترونياً تكون من خلال المساس بسلامة المعلومات التي يقوم عليها التعامل إما بالمحو أو التعديل، مما يؤدي إلى ضياع قيمتها وجعلها غير صالحة للغرض الذي خصصت من أجله.

1- أركان جريمة إتلاف البيانات الإلكترونية:

بما أن فعل إتلاف البيانات يؤدي إلى منع نظام المعالجة الآلية من القيام بوظائفه الاعتيادية حسب ما ذكر سابقاً، فإن محل الإتلاف يتمثل في تدمير المعلومات والمعطيات الموجودة داخله, والمقصود بالتدمير هنا إما محو تعليمات البرامج أو البيانات ذاتها، وليس مجرد الحصول على منفعة من النظام المعلوماتي أياً كان شكل الاعتداء، وكيفما كانت النتيجة؛ سواء استيلاء على نقود أو الاطلاع على معلومات[3]، وهنا يتجسد النشاط الإجرامي للركن المادي لهذه الجريمة في أفعال الإدخال أو المحو أو التعديل، فلا يشترط اجتماعها، بل يكفي توافر إحداها لقيام جريمة إتلاف البيانات الإلكترونية.

وتبعاً لذلك نوضح الأفعال المكونة للنشاط الإجرامي لجريمة إتلاف البيانات المعالجة إلكترونياً فيما يلي:

---

1 شيماء عبد الغني، مكافحة جرائم المعلوماتية في المملكةالعربية السعودية، مقال متاح على الموقع التالي:
https://www.mohamah.net/law تم الاطلاع بتاريخ: 2017/11/12 على الساعة 18:45.

2 هبة حسين زايد، الحماية الجنائية للصفقات الالكترونية، دار الكتب القانونية، مصر، سنة 2016، ص 75.

3 علي عبد القادر القهوجي، المرجع السابق، ص 59.

أ) **فعل الإدخال:**

يقصد بفعل الإدخال بوجه عام إضافة معطيات جديدة على الدعامة التي تحمل البيانات، سواء كانت خالية أو تحتوي على بيانات سابقة، وذلك بغرض التشويش على صحة البيانات داخل النظام المعلوماتي[1]. وقد ثبت تنوع الأساليب التي تحقق فعل الإدخال، خاصة بعد التطور التكنولوجي والفترة النوعية في مجال المعلوماتية التي ساعدت على بروز هذه الأساليب ومنها:

- **الفيروسات:** يعتبر إدخال الفيروسات إلى نظام معالجة البيانات بالحاسب الآلي بهدف إتلاف البيانات وتشويهها من أكثر الوسائل انتشاراً وخطورةً، حيث أنها تستخدم في الوقت الراهن على نطاق واسع وتتسبب في خسائر اقتصادية فادحة بمختلف القطاعات العامة والخاصة.

وقد عرف البعض[2] الفيروسات:"بأنها مجموعة من البرامج مشفرة مصممة بقدرة الانتشار من نظام لآخر، بحيث يمكنها الانتقال عبر الحدود وإلى أي مكان في العالم، وتصيب الأنظمة المعلوماتية بالشلل التام، ويتمثل نشاطها التدميري في إتلاف البيانات المخزنة ومسحها وتشويهها".

وبناءً عليه يبدو أن تعطيل وإفساد البرامج لا يمكن أن يتم إلا بواسطة إدخال معطيات أو معلومات أو بيانات جديدة، أو محو أو تعديل البيانات، وهذا يرتبط بتشغيل النظام بشكل كلي أو جزئي، ولا يتحقق إلا من خلال إدخال الفيروسات .

- **فعل المحو:** وهو إزالة جزء من المعطيات المسجلة على دعامة، والمتواجدة داخل النظام المعلوماتي، أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[3]. ومن أمثلته الواقعية قيام مجموعة من الأشخاص بالاستيلاء على مبلغ 60,000 دولار كان قد قدم من قبل إحدى شركات التأمين لصالح أحد المراكز الطبية، وقاموا بفتح حسابات وهمية خاصة بهم ووضعوا فيها المبلغ،

1 محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية- رسالة دكتوراه- دراسة مقارنة جامعة القاهرة، قسم الحقوق، سنة 2009، ص 201.

2 نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كوسيلة لأمن المعلومات- ورقة عمل مقدمة إلى المؤتمر الدولي لأمن المعلومات الإلكترونية بعنوان (معاً نحو تعامل رقمي آمن) المنعقد في الفترة 18-2005/12/20 مسقط عمان، ص 30.

3 هشام محمد فريد رستم، المرجع السابق، ص 160.

وحتى تكتمل العملية قاموا بمسح حسابات من سجلات الحاسب الآلي للمركز الطبي بشكل يجعلها غير قابلة للتحصيل وحذفها من الملفات[1].

- **التـــعديل:** يتحقق تعديل البيانات المعالجة إلكترونياً بإجراء نوع من التغييرات غير المشروعة التي تمس النظام المعلوماتي من خلال استبدال معلومات بمعطيات أخرى عن طريق أسلوب المصيدة، أو تلك الفجوات الخالية المتروكة في البرامج، مما يمكن من الولوج إلى البيانات المخزنة بالحاسب الآلي[2]، ومن أمثلة ذلك ما يعرف بالسرقة الإلكترونية، بحيث ثبت في قضية في الو.م.أ التي قام من خلالها أحد القراصنة باستبدال الرسائل الإلكترونية الموجهة للبنوك وتزويرها، بحيث يتم دفع المبلغ لحسابه الشخصي ثم يتجه لسحب المبلغ نقدياً من البنك ويختفي قبل أن يُكتشَف أمره[3].

ولقد أقر قانون العقوبات الفرنسي فعل التعديل أو التغيير الواقع على البيانات كنشاط إجرامي مكون لجريمة التزوير، وهذا على أساس تغيير الحقيقة الذي يترتب عليه إلحاق ضرراً بالغير، وهذا من خلال نص المادة 5/462، إلا أنه بعد صدور قانون العقوبات لسنة 1994 أورد المشرع نصاً جديداً المتمثل في المادة 1/141 لتختص بحالة التزوير المعلوماتي، وبهذا فصل المشرع بين التزوير في البيانات المسجلة في ذاكرة الحاسب الآلي وبين التزوير لمحررات نظام المعالجة الآلية للمعلومات، ولقد تبنت المادة السابعة (7) من اتفاقية بودابست نفس الحكم باعتبار أن أفعال تعديل البيانات وتغييرها يشكل جريمة التزوير، وعلى اعتبار أنها تخل بمبدأ الثقة في البيانات التي تقوم عليها المعاملات الإلكترونية[4].

ب) الركن المعنوي لجريمة إتلاف البيانات الإلكترونية:

يتطلب القصد الجنائي لجريمة إتلاف البيانات المعالجة إلكترونياً، أن تتجه إرادة الجاني إلى إتيان كل سلوك من شأنه تخريب أو محو أوتعديل نظم المعالجة الآلية للمعطيات، مع توقعه للنتيجة المتوصل إليها من نشاطه الإجرامي، والتي تمثل الأساس النفسي النابع من إرادته الكاملة[5].

---

1 Doon. B. Parker, Fighting Computer Crime, (a New Framework for protection information), job wily sons, New York ,2014, P 90.

2 عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة متعمقة في القانون المعلوماتي)، ط1، دار الفكر الجامعي، الاسكندرية، 2006، ص 384.

3 Vergutch pascal, La repression des délits informatique dans une prespective international, Thése, Université de Monttlier1, 1996, P 230

4 محمد أمين الشوابكة، جرائم الحاسب والانترنت، ط1، عمان، دار الثقافة للنشر والتوزيع، 2004، ص 232.

5 طعباش أمين، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الاسكندرية، سنة 2012، ص 69.

مع اشتراط أن تدخل كل النتائج الحاصلة من نشاط الاعتداء في إطار ما يرسمه القانون، وبهذا يخرج من دائرة التجريم أي فعل لا يتجه إلى توقع الآثار غير المباشرة التي تدخل في تحديد النتيجة الإجرامية وفقاً لما هو محدد قانوناً، وإلا انتفى بذلك الركن المعنوي لجريمة إتلاف البيانات الإلكترونية.

ولقد اختلف في مسألة مدى توافر القصد الجنائي في الاعتداء على مشتملات نظام المعالجة داخلياً كما هو موضح سابقا، والمتمثل في أفعال الإدخال أو المحو أو التعديل أو تلك الخارجة عن النظام، والتي تؤدي دوراً فيه، بالرغم من أن موقف المشرع الجزائري كان واضحاً من خلال نص المادة 394 مكرر من قانون العقوبات، بحيث جاء المفهوم مرناً وواسعاً ليشمل كل السلوكات الماسة بتسيير نظام المعالجة وسلامته داخلياً وخارجياً من أفعال التصميم وتجميع وتوفير، أو نشر أو الإتجار في البيانات الإلكترونية واستغلالها لأي غرض خارج عن القانون، وهو ما يوضح نية الغش المتمثلة في سوء الاستخدام والاعتداء على النظام في كل مراحله، مما يثبت الركن المعنوي للجريمة.

البند الثاني: جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعلومات.

مواصلة للحماية المقررة لنظم المعالجة الآلية تتجه أغلب التشريعات العقابية المقارنة في تبني جريمة الدخول أو البقاء في النظام المعلوماتي بشكل غير مشروع، ولعل ذلك يرجع إلى رؤية المشرع الجنائي في تعليق أهمية واضحة لحماية نظم المعلومات على اعتبار أن أفعال الاعتداء على البيانات الإلكترونية قد يفتح لها الباب الواسع من خلال توافر أفعال الدخول أو البقاء غير المشروع[1].

وبهذا نجد أن الهدف من التجريم في هذه الجريمة هو اقتحام نظم المعالجة الآلية للمعلومات بحد ذاته، ولذلك فإن قيام الجريمة يكتمل بالنشاط الإيجابي الذي يصدر من الجاني دون أن يتطلب تحقق نتيجة مادية منفصلة عنه[2].

ولقد تباينت التشريعات المقارنة في مسألة تجريم الدخول غير المشروع لأنظمة المعالجة؛ بحيث استقر البعض منها على تقييد التجريم بقيد يتعلق بتوافر قصد خاص لدى الجاني وهو إحداث الضرر من جراء الدخول، وذلك بالتأشير في البيانات الإلكترونية الواردة بالنظام المعلوماتي، من ذلك القانون الألماني والكندي والياباني[3]، ومنها ما ساير الرأي الأول باشتراط توافر نية الغش في الاستيلاء على أموال الغير، ما

1 شيماء عبد الغني محمد عطاالله، المرجع السابق، ص 94.

2 سمية عكور، الجرائم المعلوماتية وطرق مواجهتها (قراءة في المشهد القانوني والأمني)، مداخلة ملقاة بالملتقى العلمي للجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية– كلية العلوم الاستراتيجية، عمان، الأردن، خلال الفترة: 2/4/ 2014/9، ص 15.

3 نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 159.

طرحه القانون الفيدرالي الأمريكي بشأن الغش وإساءة استعمال الكمبيوتر، وهو ما يكرس فكرة الدخول غير المصرح به لأنظمة معينة كالأجهزة الحكومية أو أجهزة المؤسسات المالية، أو الأجهزة التي تتضمن معلومات تتعلق بالأمن القومي أو العلاقات مع الدول الأجنبية[1].

وأما البعض الآخر فيورد التجريم بشكل مطلق دونما اشتراط نية خاصة، ودونما قيد معين يتعلق بالركن المادي كاتجاه التشريع الفرنسي؛ والذي جاء فيه الحكم مطلقاً بتجريم الدخول والبقاء غير المشروعين، بغض النظر عن نية المتهم في إحداث جريمة معينة أو الوصول إلى أهداف محددة[2].

أولاً: الركن المادي لجريمة الدخول في أنظمة المعلوماتية.

استدل الفقه على ربط مدلول النشاط المادي لفعل الدخول لأنظمة المعالجة وفقاً لعملية الدخول بشكله المعنوي، وهذا يتحقق بأي فعل من أفعال التعدي المباشر أو غير المباشر، ولا يسبغ فعل الإجرام على فعل الدخول المجرد وإنما يكتسب ميزة النشاط الإجرامي انطلاقاً من كونه تم بدون وجه حق، أو بدون تصريح مسبق من الجهة صاحبة الحق في ذلك، أو قد يحدث فعل الدخول وفقاً للتجاوز في الحق في حد ذاته، بحيث يعمد الجاني إلى مخالفة التصريح الممنوح له في الدخول إلى جزء من النظام المعلوماتي وهذا الأمر يتصور وقوعه بالنسبة للعاملين في المؤسسات المعتمدة على الأنظمة المعلوماتية[3].

وبناءً على تحليل النشاط الإجرامي لفعل الدخول، نجد أن الركن المادي يتحقق بالسعي إلى إقامة اتصال للدخول للنظام بأي طريقة كانت، وعادة ما تتم بغاية الوصول إلى المعلومات المخزنة بالنظام المعلوماتي، وفي أي حالة يتمكن فيها الجاني من الولوج إلى الأنظمة المعلوماتية؛ إما عن طريق قيامه بعملية التوصيل عمداً إلى النظام بأحد الطرق التقنية، أو عن طريق شبكة الانترنت، وسواء كان هذا النظام محمياً بكلمة سر أو بأحد الطرق التقنية أو لم يكن[4].

وتعتبر التقنيات الأكثر استخداماً في وقوع فعل الدخول هي التي تعتمد على شفرات خاصة أو استخدام فيروس يتم إدماجه في إحدى البرامج الأصلية للحاسب الآلي، كما يمكن استخدام برامج متخصصة لكسر أنظمة الحماية الفنية التي توفر الحماية ضد أي اتصال غير مشروع بالبيانات الإلكترونية في

1 محمد عبيد الكعبي، المرجع السابق، ص 459.

2 آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة الجزائر، سنة 2007، ص 110.

3 Emmanual cauvin, Vers une nouvelle cite électronique, Books on Demand, Paris, 2016 , P182.

4 نعيم مغبغب، حماية برامج الكمبيتوتر (الأساليب والثغرات)، منشورات الحلبي الحقوقية، لبنان، 2006، ص 235.

الأنظمة المعلوماتية، فتعمل تلك البرامج على تخطي حواجز الحماية الفنية وتعمل على خلق حالات اختلال لوظيفة الأنظمة واختراقها بسهولة[1].

وهناك طرق فنية احتيالية ظهرت على يد بعض القراصنة لتمكنهم من عملية الولوج والتي تعتمد على فكرة القناع، وهي أساليب فنية يعتمدها المحتال ليوهم النظام المعلوماتي بإمكانية الدخول وكأنه شخص مصرح له بذلك، وتتم هذه الطريقة بناءً على استغلال نقاط الخلل والضعف داخل الأنظمة[2]،ومثالها حالة الموظف السابق بأحد البنوك، حيث تمكن من الحصول على كلمة السر من زميل سابق له ونجح في التقاط المعلومات المالية المخزنة في النظام ونقلها لرئيسه في الوظيفة الجديدة لكي يستفيد منها، وكذا قضية الطالب الجامعي الذي عمل على التقاط معلومات خاصة بطلبية بضاعة باستخدام النظام المعلوماتي، واستولى على معدات تساوي قيمتها مليون دولار من إحدى الشركات بولاية كاليفورنيا، وقد تمكن من ذلك عن طريق وساطة شركة أخرى أنشأت خصيصاً لغرض بيع المعدات المختلسة.[3]

ويتضح من الأمثلة السابقة أن جريمة الدخول غير المشروع لا تتوقف على هيئة أو صفة الجاني سواء كان خبيراً في مجال الأنظمة أو خارجها، أو له الإمكانية من الاستفادة من الولوج من عدمه، بل يقتصر على انعدام حقه في الدخول إلى النظام، أو تعدي الشكل القانوني الذي تنظمه اللوائح والأنظمة التي تنظم عمليات الدخول إلى النظام المعلوماتي، وهذا الموقف تدعمه اتفاقية بودابست في المادة الثانية (02) التي جرمت مجرد الدخول إلى نظام المعالجة الآلية للمعطيات سواء كان لكامل النظام أو جزء منه، وحرصت الاتفاقية على منح الدول الأطراف حرية الاشتراط في القوانين الداخلية مسألة ربط تجريم الدخول غير المشروع باختراق التدابير الأمنية من عدمه[4].

ثانياً: جريمة البقاء غير المشروع داخل النظام المعلوماتــي.

إذا كان فعل الدخول يتحقق بإتيان المجرم سلوكاً إيجابياً بدخوله المتعمد إلى نظام المعالجة، فإن فعل البقاء داخل النظام يمثل الجانب الموسع في التجريم من خلال اعتماد السلوك السلبي المتمثل في البقاء بشكل غير قانوني، حتى ولو لم تتجه نية الجاني إلى ولوجه كوجوده عرضاً أو بطريق الخطأ إلا أنه بإمكانه مغادرته،

1 عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية (الكتاب الثاني)، دار الكتب القانونية، مصر، سنة 2007، ص 28.

2 طعباش أمين، المرجع السابق، ص 52.

3 محمد سامي الشوا، المرجع السابق، ص 67.

4 المادة 2 من اتفاقية بودابست: "..حيثما كان ذلك لازماً لاعتبار الولوج إلى كل أو جزء من نظام حاسب دون وجه حق جريمة مؤثمة طبقاً لقانونه الداخلي إذا ما ارتكبت عمداً ..."

أو في حالة دخول الشخص بطريق مشروع ولكنه استمر بعد الوقت المحدد لبقائه فيه، وهذا يحدث في حالة استعمال النظام المحدد بوقت معين نظير أجر مالي، فيتخطى الجاني هذا الوقت وهو ما يعبر عنه "بسرقة وقت الحاسب الآلي"[1].

ويميل غالبية الفقه الفرنسي[2] إلى بسط الحماية الجنائية الواردة بالمادة 2/311 من قانون العقوبات الفرنسي المتعلقة بسرقة المنفعة على سرقة وقت الآلة، وقد اتجهت بعض التشريعات المقارنة إلى تبني نصوص خاصة تجرم أفعال الحصول على معلومات دون وجه حق من الحاسب.

وبناءً على هذا فإن الركن المادي لا يتمثل بالسعي إلى إقامة اتصال للدخول إلى النظام، الأمر الذي تتطلبه جريمة الدخول غير المشروع، إنما يتمثل في ضرورة قيام الجاني بنشاط إيجابي يقطع به الاتصال الذي تحقق عن طريق الخطأ، وامتناعه عن القيام بهذا الواجب يحقق صور السلوك الإجرامي[3].

ويتضح مما سبق أن جريمة الدخول هي جريمة مؤقتة، أما جريمة البقاء فهي ذات طبيعة مستمرة وهذا يبين فارق السلوك الإجرامي في كلتا الحالتين، فإذاً لم يكن من الممكن بناء العقاب في الجريمة الأولى إذا بادر الشخص وقام بقطع الاتصال على العكس في حالة استمراره؛ فهنا يعبر عن القصد في البقاء في النظام المعلوماتي، ولقد ذهب البعض من الفقه الجنائي إلى اعتبار فعل الدخول إلى النظام المعلوماتي والبقاء فيه من قبيل التعدد المعنوي، كما يرى البعض الآخر أنه مجرد تعدد مادي وأن سلوك الجاني يختلف في الحالتين وكلاهما غير مرتبط بالآخر[4].

ثالثاً: الركن المعنوي لجريمتي الدخول أو البقاء غير المشروع في الأنظمة المعلوماتية.

تصنف جريمتي الدخول أو البقاء غير المشروع داخل النظام المعلوماتي من الجرائم العمدية، يحيث يلزم توافر القصد الجنائي لقيامها، ففي حالة دخول الجاني إلى النظام عن طريق الخطأ واستمرار البقاء فيه فإنه يمكن القول بأن جريمة الدخول لا تحدث لانتفاء القصد الجنائي لحالة الدخول، بينما تقوم جريمة البقاء في هذا الفرض[5].

1 عبد الله حسين محمود، المرجع السابق، ص 312.

2 Lucas (André); Deveze (Jean), Op.Cit, P 715

3 أحمد حسام طه تمام، المرجع السابق، ص 299.

4 علي عبد القادر القهوجي، المرجع السابق، ص 52.

5 محمد عبيد الكعبي، المرجع السابق، ص 482.

ويتحقق القصد الجنائي سواء في الدخول أو البقاء بغض النظر عن الباعث، فإذا كان قصد المتهم من الدخول إلى نظام معين هو مجرد إثبات قدراته في مجال الاختراق، فإن هذا يعتبر من قبل البواعث التي لا تنفي القصد الجنائي، وتطبيقاً لذلك فإن وقوع جريمة من مهندس للكمبيوتر أراد أن يثبت لأحد البنوك قدراته الفنية على اختراق أنظمة البنك حتى يفوز بعقد تدريب كوادر البنك، بحيث قام بالولوج إلى الأنظمة المعلوماتية الخاصة بالبنك المشمولة بحماية فنية عالية، وقضي بتجريم سلوك الجاني بالنظر إلى النتيجة التي أحدثها, وبناءً على توافر نية الولوج عمداً لا عن طريق الخطأ أو الصفة العرضية[1].

وبهذا تذهب العديد من التشريعات إلى اشتراط نية الغش بجانب الركن المادي؛ وذلك بأن يباشر الفاعل سلوكه عن طريق الإحتيال والخديعة، ولا يشترط توافر قصد جنائي خاص ما لم يُشترط أن يترتب على دخول الجاني إلى نظام المعلومات لتحقيق نتيجة محددة[2].

ونرى أنه يمكن للقاضي الجنائي الإستدلال بمسألة اختراق الحماية الفنية والأمنية لأنظمة المعلومات كدليل لتوافر القصد الجنائي، بحيث يعتبر انتهاك نظام الحماية وسيلة إثبات سوء نية الجاني.

وبالرغم من ذلك إلا أن بعض التشريعات ذهبت لأبعد من ذلك واعتبرت مسألة الحماية الفنية شرط ضروري لفعل الدخول أو البقاء وتأتي فكرة الربط بين الحماية الفنية والجنائية للنظام المعلوماتي على أساس المنطق والعدالة التي تفرض هذا الربط؛ بحيث أن القانون الجنائي غير مُلزم بحماية الأنظمة التي لم يأخذ أصحابها الاحتياط اللازم، فوجود نظام حماية يكون التزاماً مفروضاً بنص القانون كل من يتولى إدارة نظام معلوماتي، ومن ثم لا يُفترض وقوع الجريمة إلا من قبل أشخاص قادرون على تجاوز أنظمة الحماية الفنية للنظام المعلوماتي.

الفرع الثاني: المواجهة التشريعية لــجرائم الاعتداء على أنظمة المعلومات.

لاكتمال معالم الحماية الجنائية ضد الانتهاكات الماسة بالنظام المعلوماتي وسلامة البيانات الإلكترونية، عملت التشريعات المقارنة على تكريس جملة من القوانين ضمنتها قواعد خاصة حاولت من خلالها تغطية هذه الحماية.

1 Alain Bensoussan, Op.Cite, P199.

2 محمد أمين الرومي، المرجع السابق، ص 103.

البند الأول: المواجهة التشريعية في القوانين الغربية.

يعتبر التشريع الفرنسي من أبرز التشريعات المقارنة التي سارعت بوضع منظومة حمائية تشريعية ضد جرائم تقنية المعلومات، بحيث أدمج المشرع الفرنسي للقانون الجديد رقم 1336 لسنة 1992 مجموعة من المواد جاءت تحت عنوان: "الاعتداءات على نظم المعالجة الآلية" من المادة 323-1 إلى المادة 323-7 وذلك لشعوره بأهمية البيانات الإلكترونية وقيمتها، وحرصاً لتجسيد تلك الحماية فلقد أورد قواعد خاصة ضد جريمة إتلاف البيانات الإلكترونية، وكذا جريمة الدخول والبقاء غير المشروع على الأنظمة المعلوماتية[1]، والتي عاقب عليها بموجب المادة 1/323 بسنتين حبس وغرامة ثلاثون ألف (30.000) أورو، واعتبر الإتلاف الواقع على المعطيات الموجودة داخل النظام جريمة يُعاقب عليها بالحبس لمدة (3) سنوات, وغرامة خمسة وأربعون ألف (45.000) أورو، ليأتي حكم الفقرة الثالثة (3) من نفس المادة لتجريم فعل الإتلاف المعلوماتي للبيانات الإلكترونية وذلك بارتكاب أفعال إدخال أو محو أو تعديل البيانات التي يحتوي عليها النظام بطريق الغش، وعاقب مرتكبها بالحبس لمدة خمس سنوات (5) وغرامة قدرها خمسة وسبعون ألف (75.000) أورو[2].

وأما بخصوص التشريع الأمريكي فلم يحتو التشريع الفيدرالي بشأن جرائم الحاسب الآلي على تجريم إتلاف المعلومات بصورة عامة, وإنما اقتصر التجريم على الإتلاف الذي يترتب عنه إعاقة أنظمة الحاسب الآلي عن العمل.

ولقد جاء مفهوم نص الفقرة 3 من المادة 1030 من ذات التشريع على تجريم عملية الدخول أو البقاء غير المشروع من خلال المعاقبة بالحبس لمدة لا تزيد عن سنة (1), وغرامة لا تزيد عن 5000 دولار أمريكي كل من توصل عن علم وبدون تصريح إلى نظام الحاسب الآلي، أو استغل فرصة توصله لتحقيق أغراض لا يمتد التصريح الممنوح إليه، وكذا من تمكن بهذا السلوك من استخدام أو تعديل أو تدمير أو كشف المعلومات المخزنة داخله[3].

وتدخل المشرع الأمريكي بالحماية ضد الإتلاف المعلوماتي في مجال الدفاع الوطني سنة 1994 حيث نص في الفصل 105 من المادة 2155 على معاقبة الأشخاص الذين يرتكبون أفعال عمدية تحدث تشويشاً،

1 محمود أحمد عبابنة، المرجع السابق، ص 87.

2 نهلا عبد القادر المومني، المرجع السابق، ص 156.

3 شيماء عبد الغني، المرجع السابق، ص 78.

أو تعترض البيانات الخاصة بالدفاع الوطني سواء بالتعييب أو التدمير بالسجن لمدة عشر (10) سنوات وغرامة لا تزيد عن عشرة آلاف دولار(10.000) دولار[1].

ثم صدر قانون حماية المعلومات القومية سنة 1996 الذي جاء به تعديل للمادة 1030 السالفة الذكر، وقام بتوسيع نطاق حماية أنظمة المعلوماتية، فلم تعد قاصرة على الأنظمة التابعة للحكومة وإدارتها، وإنما اشتملت على الأنظمة التابعة للمؤسسات الاقتصادية والمستخدمة في التجارة والإتصالات المحلية أو الإتصالات الدولية[2].

ويلاحظ أن القانون الأمريكي لم يجرم الدخول غير المصرح به كسلوك مادي قائم بحد ذاته، بل اشترط توافر القصد الجنائي، وذلك بخلاف القانون الفرنسي الذي نص في المادة 323-1 على عقاب كل من يدخل أو يبقى في كل أو جزء من نظام المعالجة الآلية للمعلومات، فالقانون الفرنسي عاقب على مجرد الدخول غير المرخص به أو البقاء داخل النظام بصورة غير قانونية, أما في التشريع الأمريكي فيشترط أن يتم الدخول بسوء نية وبأغراض محددة قانوناً، وبذلك يكون القانون الفرنسي أكثر توفيقاً؛ وذلك لكونه أحاط نظام المعالجة بضمانات فعالة لضمان عدم اختراق الأنظمة.

البند الثاني: المواجهة التشريعية المقررة في التشريعات العربية.

لقد اتجهت العديد من التشريعات العربية نحو إصدار منظومة خاصة بمكافحة الاعتداءات التي تمس المعاملات الإلكترونية، ومن ثم تجريم الانتهاكات الماسة بالأنظمة المعلوماتية وسلامة البيانات الإلكترونية التي تعتبر عماد التعامل الإلكتروني، وفيما يلي نتطرق لموقف بعض التشريعات العربية والتي من بينها المشرع الجزائري.

فنجد المشرع الإماراتي من خلال نص المادة (2) الثانية من القانون الاتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات[3] قد جرم فعل الدخول أو البقاء لأي موقع إلكتروني، أو نظام معلوماتي أو شبكة معلومات، أو وسيلة تقنية معلومات بدون تصريح أو بتجاوز حدود التصريح أو البقاء

1 نائلة عادل محمد قورة، المرجع السابق، ص 217

2 أهم ما جاء في التعديل المادة 1030 والخاص بإتلاف البيانات الإلكترونية هو نص الفقرة 5 من هذه المادة التي جرمت تعديل البيانات والشفرات والأوامر داخل أنظمة الحاسبات الآلية، وكذلك الفقرة 8 من ذات المادة فقد حددت المقصود بالأضرار التي تلحق بالحاسبات الآلية بأنها: " كل إتلاف أو إفساد لسلامة المعلومات والبرامج وأنظمة الحاسبات الآلية". **راجـــع في ذلك**: نائلة محمد قورة، المرجع السابق، ص 219.

3 القانون الاتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات السابق الذكر.

فيه بصورة غير مشروعة ، وعاقب مرتكب الأفعال السابقة بالحبس والغرامة التي لا تزيد عن ثلاثمائة ألف (300.000) درهم إماراتي.

ويأتي في نص الفقرة 2 من نفس المادة تشديد العقوبة في حالة ما إذا ترتب عن الأفعال المذكورة سابقاً إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر بيانات أو معلومات، وكذا المعاقبة بالسجن المؤقت والغرامة التي لا تزيد عن 1 مليون و50 ألف درهم إذا وقعت الأفعال السابقة على بيانات تابعة لإدارات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية[1].

ويؤكد المشرع الإماراتي في نص المادة العاشرة (10) من القانون السالف الذكر على تجريم عمليات الإتلاف الواقعة على المواقع الإلكترونية أو الأنظمة أو البيانات التي تتضمنها، من خلال إدخال برامج معلوماتية إذا ما أدى ذلك إلى تعطيلها أو تدميرها أو مسح أو تعديل البيانات أو المعلومات بداخلها.

ونجد أن المشرع الإماراتي أيضاً نص على الاستخدام غير المشروع لأنظمة المعلوماتية من خلال نص المادة 142 من نفس القانون السابق، بحيث جرم عمليات الإعداد أو التصميم أو الانتاج أو البيع أو الشراء، أو استيراد أو عرض للبيع أي برنامج معلوماتي أو الترويج لروابط إلكترونية بغية ارتكاب أو تسهيل أو تحريض لارتكاب الجرائم المنصوص عليها في هذا القانون.

أما المشرع السعودي فلقد قرر من خلال نظام مكافحة الجرائم المعلوماتية[2] بالمعاقبة بالسجن مدة لاتزيد عن سنة (01), وبغرامة لا تزيد على خمسمائة ألف (500.00) ريال، أو بإحدى هاتين العقوبتين كل شخص يعمل على الدخول غير المشروع لأنظمة الحاسب الآلي بغية تغيير تصاميم موقع إلكتروني أو إتلافه أو تعديله، وكذا المعاقبة بالسجن مدة لاتزيد على أربع سنوات وبغرامة لا تزيد ثلاثة ملايين (3.000.000) ريال أو بإحدى هاتين العقوبتين كل فعل للدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو إتلافها أو تغييرها أو إعادة نشرها.

وهنا نرى أن المشرع السعودي فرق في جريمة الدخول غير المشروع للنظام المعلوماتي بين نوعين أحدهما يقع على المواقع الإلكترونية وتجريم الانتهاكات التي تمس بسلامة الموقع وسيره, والثانية تتعلق بالبيانات الإلكترونية على مستوى الأنظمة المعلوماتية، ويعتبر هذا الحكم قد عمَل على توسيع دائرة تجريم الدخول غير المشروع لتشمل المواقع والأنظمة والبيانات على حد سواء، من جانب آخر نلاحظ إهمال

1 المادة 4 من نفس القانون.

2 المادتين الثالثة (03) والخامسة (05) من نظام مكافحة الجرائم المعلوماتية السعودي.

المشرع لتجريم فعل البقاء داخل النظام أو الموقع الإلكتروني، ولعل المشرع السعودي رأى أن النص على الأفعال التي تعتبر أثراً سلبياً لفعل الدخول هو أمر يكفي لعدم النص على فعل البقاء فقد يحتوي هذا الحكم برأيه على تجريم أفعال الدخول والبقاء معاً.

وأما المشرع المصري فقد أورد بنص المادة 14 من القانون رقم 175 لسنة 2018 :" يعاقب بالحبس مدة لاتقل عن سنة وبغرامة لا تقل عن 50 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً ، أو دخل بخطأ غير عمدي، وبقي بدون وجه حق ، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه" واما الفقرة الثانية من نفس المادة تضمنت جريمة الإتلاف الإلكتروني من خلال نصه على :" فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير او نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس لمدة لا تقل عن سنتين، وغرامة لا تقل عم مئة ألف جنيه، ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين".

وأما عن جريمة الإتلاف المعلوماتي نص المشرع في حكم الفقرة الثانية من المادة الخامسة (05) والتي ضمنت تجريم كل أفعال الاعتداء التي تؤدي إلى إيقاف الشبكة المعلوماتية أو تعطيلها أو مسح البرامج أو البيانات الموجودة فيها أو حذفها أو تسريبها أو تعديلها، ونجد أن هذا الحكم يضم أفعال الاعتداء على النظام المعلوماتي، وكذا البيانات الإلكترونية التي يتضمنها النظام بداخله.

أما بالنسبة للمشرع المصري فقد امتنع عن إصدار قانون خاص بمكافحة الجرائم المعلوماتية، وكذا عدم وجود تعديل خاص في قانون العقوبات يكرس عقوبات لتلك الجرائم، وإنما اكتفى بإصدار مشروع خاص بقانون التجارة الإلكترونية يتضمن جملة من الأحكام العقابية في حالة الاعتداءات الواقعة على المعاملات التجارية الإلكترونية فجاء حكم تجريم أفعال الدخول غير المشروع لأنظمة المعلومات في نص المادة 26 من مشروع القانون، إلا أنه من الملاحظ أن المشرع قد خص تجريم الدخول غير المشروع والبقاء فيه بالنسبة لأنظمة المعلومات وقواعد البيانات التي تتعلق بالتوقيعات الإلكترونية، وقرر عقوبة الحبس وبالغرامة التي لا تقل عن ثلاثة آلاف (3000) جنيه أو بإحدى العقوبتين، ويعاقب بنفس العقوبة في حالة الاتصال أو البقاء داخل نظام المعلومات أو قاعدة البيانات بصفة غير مشروعة[1].

كما تضمنت أحكام المادتين 29 و31 تجريم الأفعال التي تكون في مجموعها جريمة الإتلاف الإلكتروني للبيانات الخاصة بالمعاملات التجارية الإلكترونية, وهذا باستخدام نظام أو برنامج للحيلولة دون إتمام تلك

1 محمود إبراهيم غازي، المرجع السابق، ص 378-379.

المعاملات؛ وذلك بالتعديل فيها أو محو بياناتها أو إفسادها أو تدميرها، كما عاقب بالحبس لمرتكب أفعال إدخال بعمد أو بإهمال فيروس إلى نظام معلوماتي بدون موافقة مالك النظام أو حائزه الشرعي.

وأما عن المشرع الأردني فينص في قانون الجرائم الإلكترونية على تجريم فعل الدخول العمدي لنظام أو شبكة المعلومات بأي وسيلة وبدون تصريح أو بما تجاوز التصريح الممنوح له وهذه العقوبة لا تزيد عن ثلاثة (3) أشهر حبساً, وبغرامة لا تقل (100) دينار ولا تزيد عن (200) دينار أردني[1].

كما جرمت الأفعال التي تتحقق كأثر للدخول غير المشروع وتؤدي لإلغاء أو حذف أو إضافة أو تدمير أو إتلاف البيانات الإلكترونية أو تعطيل للشبكة المعلوماتية, بالحبس لمدة أقصاها سنة (01) وبغرامة أقصاها ألف (1000) دينار أردني[2].

كما ورد تجريم أفعال الإتلاف الواقع على البيانات الإلكترونية أو النظام المعلوماتي، وذلك باستخدام برنامج عن طريق الشبكة أو النظام لأجل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تعديل بيانات إلكترونية، أو إعاقة أو تعطيل عمل النظام المعلوماتي أو الوصول إليه، أو تغيير موقع إلكتروني أو إتلافه بالحبس لمدة أقصاها سنة، وغرامة أقصاها مائة ألف (100.000) دينار أردني[3].

وبهذا نلاحظ أن المشرع الأردني قد فتح مجال تجريم أفعال الإتلاف لتشمل البيانات الإلكترونية والأنظمة المعلوماتية وكذا المواقع الإلكترونية، وهو الأمر الذي يكرس حماية أكثر فعالية ضد شتى أنواع الاعتداءات التي يمكن تصور وقوعها في مجال التعامل الإلكتروني.

البند الثالث: موقف المشرع الجزائري من الجرائم الواقعة على نظم المعالجة الآلية وسلامة البيانات الإلكترونية.

لم يعتمد المشرع الجزائري منظومة تشريعية خاصة بمكافحة جرائم تقنية المعلومات بمدلولها الخاص، وإنما اكتفى بإدخال بعض التعديلات على القوانين العقابية، ومن أبرزها القانون رقم 04-15 الذي استحدث من خلاله جملة من المواد التي عالجت جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وهذا من خلال 8 مواد (394 مكرر- 394 مكرر 7) تضمنت أساساً جريمة الدخول أو البقاء غير المشروع لنظام

1 المادة 1/3 من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015.

2 المادة 2/3 من نفس القانون.

3 المادة 3/3 من نفس القانون.

المعالجة، وكذا جريمة إتلاف البيانات الإلكترونية والاستخدام غير المشروع لنظام المعلومات أو البيانات الإلكترونية.

فنجد نص المادة 394 مكرر جرمت فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات، وعاقبت عليها بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من خمسين ألف (50.000) إلى مائة ألف (100.000) دينار جزائري.

وجاء نص الفقرة الثانية منها يشدد العقوبة من ستة (6) أشهر إلى سنتين، وبغرامة من خمسين ألف (50.000) إلى خمسمائة ألف (500.000) دينار جزائري في حالة ترتب عن فعال الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة.

يتضح من النص السابق أن المشرع سعى إلى تجريم كل من فعل الدخول بطريق الغش إلى منظومة المعالجة الآلية، وكذا فعل البقاء داخل النظام في حالة تحقق الاتصال، على الرغم من علم الجاني بعدم مشروعيته وهو ما يفسره لفظ "الغش"، فالملاحظ أن صيغة النص قد جاءت عامة فيما يتعلق بالركن المادي للجريمة الذي يتحقق بالدخول غير المشروع إلى نظام المعالجة، والذي يتحقق بأي صورة من صور التعدي سواء كان مباشراً أو غير مباشراً, وبغض النظر عن الوسيلة المستخدمة سواء تمثلت في استعمال كلمة سر حقيقية، أو عن طريق استخدام برنامج أو شفرة خاصة، وسواء كان هذا النظام محمي أو غير محمي.

كما أن المشرع الجزائري قد استخدم لفظ "الدخول" مثله مثل غالبية التشريعات المقارنة، ونرى أنه يفضل استبدال لفظ "الدخول" بـ: "الاتصال" على اعتبار أن مدلول اللفظ الثاني أعمق وأدق في حالة الحديث عن النظام المعلوماتي، فالدخول قد يمثل المرحلة المادية الأولية للنشاط الإجرامي، أما لفظ "الاتصال" فهو يأخذ دلالة المعنى الأدق بحيث أن السلوك الإجرامي غير المشروع يبنى على انعدام حق الشخص في الاتصال بهذا النظام سواء كان الأمر يتعلق بالإتصال بكامل النظام أو جزء منه.

أما بخصوص جريمة إتلاف البيانات الإلكترونية فلقد نص عليها المشرع بموجب نص المادة 394 مكرر1، وهذا من خلال تجريم أفعال إدخال معلومات بطريق الغش في نظام المعالجة الآلية, وكذا إزالة أو تعديل المعطيات التي يتضمنها النظام.

وذهب المشرع الجزائري إلى تفعيل الحماية الجنائية لينص على تجريم العديد من الأفعال التي تمثل أوجه الإستخدام غير المشروع للنظام المعلوماتي، أو البيانات التي يحتويها من خلال نص المادة 2/394 والمتمثلة في التصميم أو البحث أو التجميع أو توفير أو نشر أو الاتجار في البيانات، وكذا حيازة أو إفشاء أو استعمال لأي غرض كان تلك المعطيات التي يتحصل عليها الجاني من جرائم الدخول أو البقاء أو الإتلاف

الإلكتروني لأنظمة المعالجة، ويعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات, وبغرامة من مليون (1.000.000) إلى خمسة ملايين (5.000.000) دينار جزائري.

ويذهب المشرع الجزائري إلى تشديد العقوبات السابقة في حالة استهدفت الجرائم السابقة هيئة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، فتم تشديد عقوبة الغرامة بـ: 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي بالنسبة للجاني الذي يكتسب صفة الشخص المعنوي، كما تم النص على نفس العقوبات الأصلية بالنسبة لحالتي الإشتراك أو الشروع في الجرائم المذكورة سابقاً.

وذهب المشرع إلى تبني عقوبات تكميلية تقتضي بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي كانت محلاً للجرائم، علاوة على إغلاق المحل أو المكان المستغل لارتكابها في حالة توافر علم مالكها.

المطلب الثاني: جريمة انتهاك سرية وخصوصية البيانات الشخصية في المعاملات الإلكترونية.

ترجع مسألة ظهور الاعتداء على حرمة البيانات الشخصية في المعاملات الإلكترونية من خلال مساهمة التكنولوجيا في جمع تلك البيانات وتنظيمها ودمجها بسهولة وسرعة غير مسبوقين، بالإضافة إلى أن كثرة نقل وتداول البيانات في إطار الباب الواسع للمعاملات الإلكترونية قد شكلت في مجموعها تهديداً لحدود البيانات الشخصية، الأمر الذي لزم معه تسييج قنوات التعامل الإلكتروني من خلال ضمان آليات وسبل قانونية تحيط بالبيانات الشخصية، وتحول دون عرضة الخصوصية للكشف والتشهير والاستغلال من قبل الآخرين. وهذا ما يدفعنا للتساؤل عن مفهوم جريمة انتهاك سرية وخصوصية البيانات في المعاملات الإلكترونية وعن الآليات التشريعية المقررة داخليا ودولياً لحماية هذا الحق ؟

الفرع الأول: الإطار المفاهيمي لحماية البيانات الشخصية في المجال الإلكترونـي.

مع تزايد التقنيات الحديثة زادت المخاطر المشكلة تهديداً على حق الانسان في خصوصيته، فأصبح الفرد مقيداً في تعاملاته من خلال رصد البيانات الشخصية كتقنيات المراقبة والتجسس والمساس بالمعطيات الخاصة للأفراد، وهي جميعها تمثل تهديداً مباشراً على الحياة الخاصة والحريات الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات، لا سيما اذا أُستغِلَت تلك المعلومات والبيانات لغايات خارجة عن إرادة وعلم أصحابها.

أولاً: تعريف البيانات الشخصية.

ينعقد شبه إجماع بين الفقه والتشريع على عدم إيجاد تعريف جامع مانع للحق في حماية البيانات الشخصية، وهو ما يترجَم من خلال التعدد التعريفي لهذا المفهوم في إطار النظام القانوني الواحد، ولعل هذه الصعوبة في توحيد المفهوم يرجع الى طبيعة الحق التي تكتسب صفة المرونة وعدم التحديد والضبط في إطار محدد، وتختلف باختلاف المجتمعات الإنسانية والحقب الزمنية عبر العصور.

1- الوجه التقليدي لحماية البيانات الشخصية:

ذهب العديد من الفقهاء لإيجاد تعريف لحماية البيانات الشخصية كل وفق توجهاته ومنطلقاته الفكرية, على اعتبار أن المكونات المنطقية لها تتسم باضطرادها المستمر في كل حقبة زمنية، فعلى سبيل المثال بدأت بلورة مفهوم البيانات الشخصية سابقاً في إطار المراسلات التقليدية الورقية، ومن ثم بدأت الفكرة تتطور إلى حين وصولها إلى الحياة في العالم الرقمي، وهنا يتشكل الفرق في جوهر مفهوم الخصوصية.

فوفقاً للفقيه"EDWARD Bloustein" فإن حماية البيانات الشخصية هي الحق في حماية المعلومات الشخصية للأفراد وضمان عدم الاعتداء عليها واستقلالها"، أما الفقيه"GAVISON Ruth" فلقد بنى مفهوم حماية البيانات الشخصية وفقاً لثلاث عناصر هي: السرية والعزلة والتخفي, بحيث اعتبر أنه الحق في الحماية ضد التدخل في الحياة الخاصة وشؤون عائلتهم بوسائل مادية مباشرة، أو عن طريق نشر المعلومات".[1]

كما يرجع الفقيه هشام محمد فريد رستم قيام مفهوم حماية البيانات الشخصية بتوافر وجهين؛ أحدهما مادي قوامه عدم إقحام الشخص في خصوصيات الآخرين، والثاني إعلامي مقتضاه ألا تكون المعلومات الخاصة بالفرد محلاً للحق في الإعلام بالنسبة للآخرين[2]، مما يستتبع معه عدم استغلال الآخرين لتلك المعلومات بالنشر أو التشهير.

2- الوجه الحديث لحماية البيانات الشخصية:

وهنا يستند أغلب الفقه والتشريعات المعاصرة إلى أن فكرة حماية البيانات الشخصية يتشكل مفهومها في:"حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم مدى وصول المعلومات المرتبطة بحياتهم الخاصة للآخرين، وبأن يضبط عملية حصر المعلومات الشخصية ومعاملتها آلياً، واستخدامها في صنع القرار الخاص أو المؤثر في حياتهم"[3]، ليدل بذلك هذا التعريف إلى مفهوم الإستحداث في التعاملات

1 **نقلاً عــن:** عبد الله عبد الكريم ، المرجع السابق، ص 36.

2 محمد هشام فريد رستم، المرع السابق، ص 176.

3 حسام الدين الأهوائي، المرجع السابق، ص 132.

بين الأفراد من خلال معالجة المعلومات الخاصة بهم إلكترونياً وضمان تلك الخصوصية التي تنبع من حصر فكرة الاطلاع على البيانات الشخصية وعدم التطاول عليها من قبل الآخر.

ولقد اتجه غالبية الفقه إلى ربط حماية البيانات الشخصية بمخاطر تقنية المعلومات المحيطة بمسألة حماية بنوك المعلومات وعمليات المعالجة الآلية للبيانات الشخصية، وبناءً على ذلك فقد عرفها الفقيه الأمريكي "ويستن Alan Westin" في كتابه المعنون بـ: "الخصوصية والحرية" بأنها: "خصوصية المعلومات تعني حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين"، في حين جاء تعريف الفقيه "ميلر Meler" في كتابه "الاعتداء على الخصوصية" أكثر عمقاً، إذ عرفها بأنها:"قدرة الأفراد على التحكم في سرية المعلومات المتعلقة بهم"[1]. وبهذا نجد أن حماية المعلومات الشخصية تتوقف على فكرة الإعتداء عليها إلكترونياً من قبل الآخر، واستخدامها وفقاً لأغراض خارجة عن القانون بدون علم أو إرادة صاحبها.

وبالارتكاز على منحى الخصوصية في وجهها المستحدث نجد التعريف الصادر عن مركز دراسات البيانات المجتمعية, والذي أرجع حماية البيانات الشخصية إلى إمكانية الفرد بالتصرف بشكل قانوني دونما وجود عائق يحول هذا التصرف[2]، وبهذا فإن المعنى العميق لمفهوم الخصوصية يتجلى في تبني تلك الرخصة في حرية التصرف وضمان عم التدخل أو التطفل من الغير تحت أي ظرف، وهنا نستشف تلك الإضافة التي جاء بها هذا التعريف من خلال تسييج الخصوصية ضد أية خروق تصدر من الأفراد أو حتى من الدولة في إطار ما يعرف بالمراقبة الإلكترونية[3].

3- المفهوم التشريعي لحماية البيانات الشخصية:

بداية إن مفهوم حماية البيانات الشخصية قد بني في مختلف التشريعات المقارنة تحت إطار ضمان الحد الأدنى في حق الفرد بعدم التدخل أو المساس بالحياة الشخصية أو الأسرية، أو خرق لسرية المعاملات أو الحقائق التي تحيط بحياته، وهو ما كرسه الدستور الجزائري بمقتضى نص المادة 39 التي تنص على أنه:"لا

1 **نقلاً عـــن**: محمود إبراهيم غازي، المرجع السابق، ص 272.

2 السيد عتيق، المرجع السابق، ص 61.

3 عبد الفتاح حجازي، الحماية الجنائية المعلوماتية للحكومة الإلكترونية، دار الكتب القانونية، مصر، 2007، ص 33.

يجوز انتهاك حرمة حياة المواطن وحرمة شرفه ويحميها القانون. سرية المراسلات والاتصالات بكل أشكالها مضمونة "[1].

ويتبين من ذلك أن نص المادة 39 كان واضحاً مباشراً في تكريس الحماية لحق الخصوصية بخلاف نص المادة 40 فقد كانت الإشارة ضمنية تكفل خصوصية الأفراد بعدم خرق حقهم في أن يكونوا آمنين على أنفسهم ضد أي تعسف في التفتيش أو الاحتجاز، أو اقتحام المساكن غير المبني على أسس قانونية، وهو مظهر من مظاهر الحماية للحياة الخاصة، وهو نفس الموقف الذي تبناه المشرع الإماراتي من خلال الباب الثالث في المواد 25-44 من الدستور الإتحادي.

ثانياً: مبررات ونطاق حماية البيانات الشخصية في المجال الإلكتروني.

مع تزايد التقنيات الحديثة زادت المخاطر على الحق في الحياة الخاصة، وأضحى الفرد مقيداً في تعاملاته من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة الوسائل المعلوماتية كتقنيات المراقبة أو التجسس والمساس بالمعطيات الخاصة بالأفراد، وهي جميعاً تمثل تهديداً مباشراً على الحياة الخاصة والحريات الفردية بصورتها المستحدثة والمتمثلة في بنك المعلومات، لا سيما إذا استغلت لغايات خارجة عن إرادة صاحبها ودون علمهم.

1- مبررات حماية البيانات الشخصية:

إن مبررات حماية المعلومات الشخصية للأفراد في المعاملات الإلكترونية ترتكز على جملة من النقاط نبينها فيما يأتي:

أ) اتساع شبكة الانترنت:

إن الواقع يثبت أن أهم التقنيات التي تتحكم في مجموع التعاملات الإلكترونية تعتمد على شبكة الإنترنت، وهذه الأخيرة ليست بمنأى عن ولوج أي متطفل أو معتدي يستغل شتى الاتصالات التي تترك أثراً حتى دون علم مستخدم الشبكة، فتدفق المعلومات والاتصالات عبر الحدود دون أي اعتبار للحدود الجغرافية، يمكن الأفراد من تبادل المعطيات الخاصة بهم لجهات مختلفة وفي قنوات عديدة داخلية وخارجية، وربما جهات ليس لها محل معنون، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها الحماية القانونية للبيانات الشخصية[2].

1 الدستور الجزائري المؤرخ في 8 ديسمبر 1996 (ج رج رقم 76) والمعدل بآخر تعديل وفقاً للقانون رقم 16-01 المؤرخ في 26 جمادى الأولى عام 1437 الموافق 6 مارس سنة 2016 المتضمن التعديل الدستوري.

2 جميل عبد الباقي الصغير، المرجع السابق، ص 40.

ب) الطبيعة الخاصة لقنوات التعامل الإلكترونـــي:

هذه الطبيعة الافتراضية التي تفتقد إلى المادية تجعل من الشخص وهو بصدد استخدام شبكة الانترنت يتوقع قدراً من الخفية في نشاطاته أكثر مما هو عليه الحال في العالم الواقعي، بينما الواقع يثبت عكس ذلك على اعتبار أن التعاملات الإلكترونية تترك آثاراً ودلالات على شكل سجلات رقمية حول الموقع المزار، والأمور التي بحث عنها والمواد التي قام بتنزيلها، والوسائل التي أرسلها والخدمات والبضائع التي قام بشرائها، مما يجعله عرضة للقرصنة ثم الاستغلال غير المشروع لها.[1]

ج) فقدان المركزية وآليات السيطرة في قنوات التعامل الإلكترونـي:

يكتسب حق الخصوصية في إطار العالم الرقمي نوعاً من التميز ذلك أن إقرار قانون فاعل يكرس من وجود استراتيجية ملائمة لحماية حق الأفراد بعيدا عن العالم الرقمي، قد يُكوِّن نوعاً من السهولة بحيث يمكن للدولة وضع رقابة على الاعتداءات المختلفة، إلا أن الأمر لن يكون بذات السهولة إذا ما تعلق الأمر بحماية حق الخصوصية المعلوماتية؛ لأن لها ارتباط مباشر بعالم افتراضي شاسع يرتبط بشبكة الانترنت اللامتناهية الحدود، وهنا يحتدم الصراع على السيطرة على الانترنت من خلال الصعوبة في التحكم في مركزية أسماء النطاقات وعناوين المواقع وغيرها، وهو ما يوسع من دائرة اختراق حق الأفراد ويصعب من الحماية ضد أي انتهاك لخصوصياتهم[2].

2- نطاق حماية البيانات الشخصية في المعاملات الإلكترونية:

يتحدد نطاق حماية البيانات الشخصية في مجال التعاملات الالكترونية بين حدين متناقضين؛ يتمثل أولاهما في حق الأفراد في الحياة الخاصة، وثانيها موجبات الإطلاع على المعلومات الخاصة بالأفراد وما تفرضه الضرورة على الدول والحكومات في توفير حد أدنى من خط الأمان, وكبح للجريمة المرتكبة عبر الانترنت، ويتضح هذا النطاق وفق المعالم التالية:

- إيجاد تناسق بين الحق في خصوصية البيانات الشخصية وحق الدولة في الإطلاع على هذه البيانات في إطار تنظيم الحياة الاجتماعية على نحو أفضل، وهذا لا يتعارض في مفهومه مع التعرض للحياة الخاصة للأفراد بأي حال، إلا في حالة استخدام البيانات الشخصية لأغراض تتنافى مع صونها واحترامها[3].

1 عمر محمد أبو بكر يونس، المرجع السابق، ص 398.

2 أحمد حسام طه تمام، المرجع السابق، ص 359.

3 هشام محمد فريد رستم، المرجع السابق، ص 180.

- إيجاد تناسق بين حق الفرد في عدم الكشف عن أي معطيات أو بيانات تتعلق بخصوصيته مع المصلحة في الكشف عن هذه المعطيات لجني فوائد عملية، إذ أنه يتبين عدم وجود تعارض بين الحق في السرية والكشف الإرادي عن هذه الخصوصية، إلا أن الفكرة تخص مسألة تفادي أي احتمال لاستغلال تلك المعلومات المكشوف عنها إرادياً ليتم استغلالها في أغراض تهدد حرمة الفرد وانتهاك لحرمة حياته الشخصية[1].
- رسم خط توازي بين استخدام فكرة بنوك المعلومات[2] كآلية لجمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد، والتي خلقت آثاراً إيجابية عريضة في مجال تنظيم تعاملات الأفراد إلكترونياً، فبفعل الكفاءة العالية لوسائل التقنية الحديثة والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات إلكترونياً، اتجهت أغلبية دول العالم بمختلف هيئاتها إلى إنشاء قواعد بيانات تساهم في هذه العملية[3]، إلا أنه ظهر بشكل سريع الشعور بخطورة تقنية المعلومات وتهديدها للخصوصية، ومكمن المخاوف يبرز في أن الوضع الحديث لتقنية المعلومات أضحى يمس بالجوانب الشخصية بتخزينها لتلك المعلومات وجمعها لفترة غير محددة والرجوع إليها بكل سهولة، مع خطر تدفق تلك البيانات التي تنتج عن المعاملات الإلكترونية ويجعلها عرضة للقرصنة والتملك والاستغلال، مما يخلق حالة قلب لإيجابية تلك التقنية الحديثة إلى خطر يهدد استقرار الحياة الخاصة وسريتها[4].

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

2 تعرف بنوك المعلومات بأنها قاعدة بيانات تم إنشاؤها ومعالجتها بواسطة أجهزة الحاسبات ألإلكترونية، وذلك لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة ، وقد تكون بنوك المعلومات مقصورة على بيانات تتصل بقطاع معين، وقد تكون معدة للاستخدام على المستوى الوطني كمراكز وبنوك المعلومات الوطنية او تستخدم في مجال قطاع الأعمال. **انظر**: حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، 2012، ص 60.

3 أسامة قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات: دراسة مقارنة في القانون الفرنسي والأمريكي وفقاً لآخر التعديلات التشريعية، دار النهضة العربية، مصر، سنة 2008، ص 48.

4 Piérre TRUCHE; Jean –paul Faugére et Patrice FLICHHY: Administration électronique et protection des données personnelles livre Blanc, rapport au ministre de la fonction public et de la réforme de l'Etat, Paris, la documentation française, 2002, P 77. Disponible sur le ligne suivante: *https://www.ladocumentationfrancaise.fr/rapports-publics/024000100/index.shtml*

الفرع الثاني: المخاطر الواقعة على البيانات الشخصية والمواجهة التشريعية المقررة لها.

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

البند الأول: المخاطر الماسة بالبيانات الشخصية.

يمكن تأصيل المخاطر الإلكترونية التي تمس البيانات الشخصية في صورتين؛ أولاهما: انتهاك سرية البيانات الشخصية، وثانيها الإعتداء على سلامة البيانات المتداولة في مختلف التعاملات الإلكترونية.

1- الجرائم الواقعة على سرية البيانات الشخصية:

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

أ- المعالجة غير القانونية للبيانات الشخصية:

تعد البيانات الشخصية قوام الحق في الخصوصية، فهي تمثل في مجموعها المعطيات والمعلومات الخاصة بالفرد والتي تكتسب صفة السرية، وعملية المعالجة غير المشروعة لجملة البيانات هي أبرز صور الإنتهاك لتلك السرية من خلال مخالفة القائمين على عملية المعالجة للشروط والأساليب القانونية المنصوص عليها داخلياً[1] كعدم منح الترخيص من الجهات المختصة أو إلغائه أو انتهاء مدته، وهذا يشكل في جوهره اعتداءً على حق الدولة في الرقابة على تداول ونقل البيانات الممنوحة للأشخاص المعنوية المصرح لها بذلك قانوناً، ولقد أحاط التوجيه الأوروبي[2] رقم ce/46/95 بتعريف للبيانات الشخصية محل المعالجة الآلية في نص

1 محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، مصر، سنة 2016، ط1، ص 92.

2 -Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

المادة الثانية منه بأنها: "كل شخص طبيعي معرف أو قابل للتعريف والذي يمكن معرفته بصفة مباشرة أو غير مباشرة عند الرجوع إلى جملة من الميزات أو الخصائص الفيزيولوجية أو الاجتماعية أو الاقتصادية".

ولقد نوه المشرع الجزائري وفقاً لنص المادة الثانية من القانون 18-07 الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1]: "بأنه يجب أن تتم عملية معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم"، وبهذا تنشأ مخاطر تحول دون مهمة القائمين على تلك الرقابة في التكفل عدم الاعتداء على الحياة الخاصة، ومن ثم تغييب دور الدولة في ضبط مجال الرقابة على البيانات وحمايتها من شتى أنواع الجريمة الإلكترونية[2].

ومن جانب آخر فإن فكرة المعالجة غير المشروعة للبيانات الشخصية تقوم على مسألة الاعتداء على حق الأفراد في الاستئثار بمعالجة البيانات الشخصية، الأمر الذي يعد ضرورياً في التفرقة بين البيانات القابلة لمعالجتها من قبل الغير غير القابلة لذلك[3].

ب- الإفشاء غير المشروع للبيانات الشخصية:

إن مسألة الإفشاء غير المشروع للبيانات الشخصية كأحد صور انتهاك لحق الخصوصية قد تأخذ مظهرها في بعض المهن التي تعتمد على سرية البيانات كمهنة المحاماة والطب أوعمال البنوك، بحيث يفترض احتفاظ صاحب المهنة بسرية البيانات الشخصية للزبون أو العميل بحكم التعامل القائم بينهما.

وتعد أكثر البيانات عرضة للإفشاء غير المشروع تلك الخاصة بتعاملات البنوك الإلكترونية وهذا ما ثبت من خلال قضية بنك (جزل تشافت) السويسري التي حاول خلالها عملاء فرنسيين تابعين لإدارة خدمات الرقابة على التعاملات التجارية والمالية فك شفرة بيانات شخصية لمواطنين فرنسيين تحمل حسابات لدى البنك، وذلك للاستعانة بها في أعمال البحث والتقصي التي تجرى بشأن التهرب الضريبي[4].

---

1 قانون رقم 18-07 المؤرخ في 25 رمضان عام 1439هـ الموافق 10جوان سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي (ج رج عدد 34، ص 11) المؤرخة في 10 جوان 2018.

2 Jean-jacques Hyest: la fraude informatique vue par le nouveau code pénale, exertises des systémes de l'information ,Février. 2010. N 147.

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

4 **نقلا عن**: هشام محمد فريد رستم، المرجع السابق، ص 195.

2- التجسس الإلكتروني:

لقد أثبتت التجربة الواقعية أن خطورة استخدام شبكة الانترنت تكمن أساساً في ضعف الوسائل المستخدمة في حماية انتقال البيانات عبر الشبكة، ضف إلى ذلك صعوبة الوصول إلى الأشخاص القائمين بالإعتداء، وبهذا فقد ظهر التجسس الإلكتروني كأخطر صور الاعتداءات التي تحدث في إطار التعاملات الإلكترونية؛ نظراً لارتباطه بشكل مباشر باغتصاب سرية المحادثات الشخصية وجل المراسلات والتعاملات التي تتم عبر شبكة الانترنت في كل المستويات.

ولقد عُرِّف التجسس الإلكتروني في مجال المحادثات الشخصية بأنه: "عملية التنصت أو التقاط البيانات التي تنتقل بين جهازين عن بعد عبر شبكة الانترنت، أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى بيانات وذلك باستخدام أي وسيلة من الوسائل التقنية"[1].

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

ضف إلى ذلك فإن خطورة التجسس الإلكتروني أضحت تأخذ صورة أوسع مما كانت عليه سابقاً خاصة في ظل العولمة والتقنيات الحديثة، بحيث لم تعد تقتصر على السلطات أو دوائر المخابرات، بل قد أصبحت وسائل التجسس متاحة إلى الأفراد العاديين خاصة في الدول المتقدمة على عكس الدول العربية التي ما زالت حركة تسويق أجهزة التجسس من الأمور المستصعبة والتي لا يمكن تداولها بشكل حر ويسير[2].

ولقد اختلفت الوسائل المتبعة في إطار التجسس الإلكتروني وهذا تبعاً لاختلاف ثقافة مستخدمي هذه الوسائل، ومن أبرزها اتباع تقنية اعتراض الاتصال الشبكي التي تقوم على الاعتماد على برامج لتنفيذها، فيتم التدخل من قبل أحد الأشخاص الخارج عن الاتصالات الشبكية المقامة عبر الانترنت كتبادل النصوص أو الأحاديث الصوتية فيتم التقاط البيانات أو الصور أو التنصت على الأحاديث الصوتية واعتراض المحادثات المقامة بالصوت والصورة عن طريق الكاميرات أثناء الاتصال[3].

---

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

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

3 محمد عزت عبد العظيم، المرجع السابق، ص 101.

3- اختراق الحاسبات الآلـــية:

ذهب البعض من الفقه[1] إلى تعريف جريمة الاختراق بأنها: "عملية دخول غير مصرح بها إلى حاسب الآخر عن طريق استخدام برامج متطورة تحت تقنية وخبرة عاليين"[2]، كما ربط البعض الآخر[3] فكرة الاختراق بالمعالجة غير المشروعة للبيانات فعرفه بأنه: "الولوج غير المصرح به قانونا إلى نظام معالجة البيانات باستخدام الحاسوب".

وبهذا نجد أن عمليات الإختراق لا تقل خطورة عن النماذج السابقة على اعتبار أن الحاسب الشخصي أضحى يمثل أهم الوسائل المتاحة للاتصالات الحديثة بين الأفراد، وأضحى يعتمد عليه كلياً كآلية للمراسلات والمعاملات التي تصدر في إطار التعاملات الإلكترونية، وبهذا فإن فكرة اختراق الحاسب الشخصي تقوم على أساس الإعتداء على خصوصية وسرية المعاملات وتسخيرها واستغلالها في شتى الأغراض غير المشروعة التي تلحق بالفرد عدة خسائر على المستوى المادي والمعنوي، وهذا ما عبر عنه في السنوات الأخيرة من خلال ما يعرف بالاختراق الأسود أو "مخترقي القبعة السوداء"؛ وهي مجموعة من المجرمين الإلكترونيين الذين اعتمدوا أسلوب اختراق الحاسبات الشخصية للأفراد بالدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة وتعديل وتحريف وإتلاف البيانات بغرض الاستفادة المادية أو إحداث الضرر المعنوي للضحية، وقد تدخل هذه التصرفات في غالب الأحيان في إطار العداءات الشخصية أو السياسية أو الدينية أو القيام بتلك الأفعال لحساب جهات منافسة أو معادية.[4]

4- جريمة اختراق البريد الإلكتروني:

يعتبر البريد الإلكتروني من أحد الوسائل الحديثة في إطار المعاملات الإلكترونية التي تقدمها شبكة الانترنت، فهي تدخل في إطار تسهيل الاتصال الإلكتروني عن طريق تبادل الرسائل الفوري، وبهذا يعد اختراق البريد الإلكتروني من أهم المخاطر التي تواجه حق الخصوصية وتعرض الفرد إلى انتهاك سرية المعاملات والمراسلات التي تدخل في شتى المجالات، وبهذا فإن المقرر وفق القواعد العامة تكريس ضمانات

1 عمر محمد أبو بكر بن يونس، المرجع السابق، ص 331.

2 خالد ممدوح إبراهيم ، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، سنة 2004، ص 242.

4 محمد سامي الشوا، المرجع السابق، سنة 1994، ص 56.

لحماية سرية المراسلات في حدود وضوابط معينة بغض النظر عن الأساليب المستخدمة سواء كانت تقليدية أو حديثة[1].

البند الثاني: المواجهة التشريعية للمخاطر الـماسة بالبيانات الشخصية.

لقد أضحت التكنولوجيا الحديثة سلاحاً ذو حدين خاصة في المجال الإلكتروني، فبقدر التطور الهائل الذي مس حياة الأفراد وأسبغ عليه يسر ومرونة في التعامل والاتصال عبر شبكة الانترنت، إلا أن هذا الأمر قد حمل في ثناياه مخاطر عديدة مست بخصوصيات الأفراد, مما استدعى بذل الكثير من الجهود سواء على مستوى التشريعات الداخلية أو على المستوى الدولي، لإرساء آليات الحماية ضد انتهاك البيانات الشخصية، وهنا يثار التساؤل حول معالم الحماية التي رسمتها القواعد الدولية في ظل الاتفاقيات والمؤتمرات الدولية الرامية لحمايتها، أو الجهود الداخلية للدول في مسار تفعيل القواعد العامة العقابية بما يتماشى وحماية البيانات الشخصية في المجال الإلكتروني, أو استحداث تشريعات خاصة تغطي هذه الحماية.

أولاً. الحماية الدولية للبيانات الشخصية:

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

أ- حماية البيانات الشخصية في إطار المؤتمرات الدولية والإقليمية:

لقد تبنت الجمعية العامة للأمم المتحدة توصيات المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الأفراد المنعقد في طهران عام 1986، بحيث خرج بجملة من التوصيات التي تبرز خطر الحاسبات الإلكترونية على المعلومات الشخصية، وضرورة إيجاد آليات على المستوى الإقليمي أو الدولي لمحاربة أجهزة التجسس[2].

وأما على مستوى الإقليم العربي فلقد انعقدت العديد من المؤتمرات الدولية التي عنيت بمكافحة الجرائم المعلوماتية خاصة انتهاك سرية البيانات الشخصية ومن أبرزها:

1- المؤتمر الدولي لأمن المعلومات الإلكترونية المنعقد بمسقط سنة 2005:

1 عمر محمد أبو بكر يونس، المرجع السابق، ص 339.

2 يونس خالد عرب، جرائم الحاسوب (دراسة مقارنة)، رسالة ماجيستر، جامعة الاردن، عمان، 1994، ص 125.

ركز المؤتمر على بحث ودراسة أهم التهديدات الإليكترونية، والمخاطر التي تمس باقتصاديات الدول وتحد من التنمية، وعمل على الخروج بتوصيات خاصة بالتأكيد على التعاون الدولي لمكافحة الجريمة ووضع سياسات مشتركة للقضاء على الآثار السلبية لتكنولوجيا المعلومات التي تهدد البيانات الشخصية[1].

2- المؤتمر الدولي الأول لمكافحة جرائم تقنية المعلومات المنعقد بالشارقة بالإمارات العربية المتحدة سنة 2006:

يعتبر هذا المؤتمر شاملاً من حيث دراسة وبحث إشكالية الجرائم المعلوماتية من حيث المفهوم والمكافحة على المستوى الوقائي والعلاجي وفتح النقاش لدراسة التوجهات المستحدثة في هذا المجال والسعي لتبادل الخبرات في مجال مكافحة جرائم تقنية المعلومات[2].

ب- حماية البيانات الشخصية في إطار الاتفاقيات الدولية:

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

1- الإتفاقية الأروبية لحماية الأفراد في مجال المعالجة الآلية للبيانات الشخصية:

جاءت الاتفاقية الأوروبية لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية رقم 108 المنعقدة في 28 يناير 1981 في ظل الإنفتاح الواسع للانترنت الذي أتاح التبادل الواسع لمختلف أنماط المعلومات، وخلق بيئة للاستثمار والأعمال فيما يعرف بالأسواق الافتراضية أو بيئة الأعمال الإلكترونية، وبحيث أن التقارير الصادرة عن هيئات حماية الخصوصية قد أثبتت عدم أمان العمليات الإلكترونية الصادرة عن الأفراد، خاصة في إطار تجميع وتحليل المعلومات الشخصية كحزمة واحدة للوصول إلى حقائق عن الشخص تساهم في تنفيذ الاعتداء على تلك المعلومات، فلقد كفلت الاتفاقية ضمان حقوق الفرد بغض النظر عن الجنسية أو الإقامة واحترامها في مواجهة الاستخدام الآلي للمعلومات ذات الطابع الشخصي[3].

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

2 أسماء حسن سيد محمد، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه، جامعة القاهرة، سنة 2013، ص 433.

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

2- اتفاقية بودابست لسنة 2001 المتعلقة بالإجرام المعلوماتـي:

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

أقرت الاتفاقية في المذكرة التفسيرية لها بالدور الذي تسعى من خلاله مكافحة الجرائم الناشئة عن الأثر السلبي لتكنولوجيا المعلومات، لتخصص في الباب الثاني من الاتفاقية بعض النماذج البارزة للاعتداء على البيانات الشخصية في المعاملات الإلكترونية[1]، تجسدت في الباب الثاني المعنون: "الإجراءات الواجب اتخاذها على المستوى الإقليمي"، وعلى سبيل المثال ما جاء في فحوى المادة الثانية (2) التي نظمت مسألة الولوج غير القانوني لأجهزة الحاسوب بدون وجه حق، ونصت على الشروط الواجب توافرها لقيام هذه الجريمة باعتبارها تنطوي على تهديد لسرية وسلامة النظم والبيانات الشخصية المعلوماتية للأفراد، كما أقرت ضرورة تكريس التشريعات الداخلية لمجموعة من القواعد في النظم العقابية الخاصة بها بغية وضع إجراءات أمنية فعالة ضد تلك الانتهاكات[2].

من جانب آخر نصت الاتفاقية في نفس المادة على جريمة الإعتراض غير القانوني باستخدام الوسائل الفنية للبيانات المتداولة إلكترونياً بين الحواسيب عبر شبكة الانترنت، واختصت المادة الرابعة (04) بالنص على ضرورة توحيد أطراف الاتفاقية للجهود بغية تبني الإجراءات التشريعية التي تجرم الاعتداء على سلامة البيانات من أجل ضمان سلامة المنظومة البيانية للاتصالات الإلكترونية[3].

3- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010:

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

1 خالد ممدوح إبراهيم، المرجع السابق، ص 276.

2 محمد عزت عبد العظيم، المرجع السابق، ص 161.

3 هلالي عبد اللاه أحمد، جرائم المعلوماتية العابرة للحدود (أساليب المواجهة وفقا لاتفاقية بودابست)، دار النهضة العربية، مصر، ط1، سنة 2007، ص 22.

ولقد أكدت الاتفاقية على التزام الأطراف بتجريم شتى أساليب الاعتداء على حقوق الأفراد في المجال الإلكتروني المنصوص عليها الفصل الثاني منها والمعنون "بالتجريم"، والذي ركزت فيه على تجريم الدخول غير المشروع وكذا الاعتراض غير القانوني للبيانات الشخصية، والاعتداء على سلامتها، في نصي المادتين السابعة (07) والثامنة (08) منها.[1]

ثانياً. حماية البيانات الشخصية في ظل الحماية الداخلية للتشريعات المقارنة:

بعد الحراك التشريعي الدولي الساعي إلى ترسيخ المبادئ الأساسية لمكافحة جرائم تقنية المعلومات بشكل عام ومحاربة الاعتداء الماس بسرية وخصوصية البيانات الشخصية في المجال المعلوماتي بشكل خاص، جاء دور التشريعات الداخلية للدول لتأخذ على عاتقها تأسيس قواعد حمائية ضد تلك الانتهاكات.

وإن كان من الواضح بعد استقراء العديد من النصوص التشريعية العقابية في مجال مكافحة الاعتداء على البيانات الشخصية نجد أن طائفة من التشريعات قد عملت على تبني نصوص خاصة لتكفل حمايتها بعيداً عن النصوص العقابية في القواعد العامة، أما البعض الآخر فقد اكتفى بتعديل التشريع العقابي بما يتوافق ومحاربة جرائم تقنية المعلومات المرتكبة عبر شبكة الانترنت بشكل عام وسرية البيانات الشخصية بشكل خاص.

1- المواجهة التشريعية للجرائم الماسة بالبيانات الشخصية في ظل التشريعات الغربية:

عمل التشريع الفرنسي على التصدي لجرائم انتهاك الخصوصية في المجال المعلوماتي بعد إصدار جملة من التشريعات التي تبناها في مجال نظم المعالجة الآلية للمعلومات, والتي مرت على مرحلتين:

- **المرحلة الأولى**: بموجب القانون رقم 78-17 الصادر في 1978/01/06 الخاص بحماية البيانات الاسمية للمواطنين في مواجهة نظم المعالجة الآلية للمعلومات[2]؛ وعرف هذا القانون باسم قانون المعلوماتية والحريات، وقد ضم أربعة جرائم خص الجريمة الثالثة منها بتجريم إفشاء البيانات الاسمية غير المشروع وذلك في المادة 43 التي نصت على أن: " يعاقب بالحبس من شهرين إلى ستة أشهر وغرامة من 2000 أورو إلى 20.000 أورو أو بإحدى هاتين العقوبتين كل من حاز بمناسبة تسجيله أو تصنيفه أو نقله لأي شكل من أشكال المعالجة الإلكترونية لبيانات اسمية يشكل إفشاؤها اعتداء على الشرف أو الاعتبار أو

1 أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه،كلية الحقوق، جامعة المنصورة، مصر، سنة 2006/2005، ص 198.

2 Loi N°:78-17 du 06 janvier 1978 Relative à l'informatque,aux fichiers et aux libertés (JO.R.F du 07 /01/1978, p 227).

حرمة الحياة الخاصة دون تصريح من صاحب الشأن، أو بنقله عمداً إلى علم شخص غير مختص بهذه البيانات وفقاً للأحكام المنصوص عليها في هذا القانون".

- **المرحلة الثانية:** القانون رقم 88-19 الصادر في 88/01/05 بشأن جرائم الغش المعلوماتي, ولقد حرص المشرع في كلا القانونين على النص على الحلول المناسبة لمواجهة الجرائم الناشئة عن الحاسبات الإلكترونية وخطورتها على الحريات العامة والفردية[1].

ولقد حرص المشرع الفرنسي على مواصلة مكافحة الاعتداءات الواقعة على البيانات الشخصية في إطار التشريعات العقابية بحيث كرس جملة من المواد بموجب قانون العقوبات الجديد رقم 92-684[2]، ثم ألحق تعديلاً آخر بموجب القانون رقم 2011-801 المعدل لقانون العقوبات[3]، كما أضاف المادة 226-17-1 بموجب المادة 39 من الأمر رقم 2011-1012 المتعلق بالاتصالات الإلكترونية[4].

وتضمن القانون أحكاماً جديدة لمواجهة ظاهرة الإجرام المعلوماتي تحت عنوان: "الاعتداء على نظم المعالجة الآلية للمعلومات". وتحديداً من خلال نص المادة 226-22 منه، والتي نصت على أن: "يعاقب بالحبس لمدة خمس (5) سنوات وغرامة 300.00 أورو كل شخص كان قد استقبل أو تلقى بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الآلية معلومات اسمية, من شأن إفشائها الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة وقام بنقلها إلى شخص آخر، وإذا وقع هذا الإفشاء للمعلومات الاسمية بطريق الإهمال تكون العقوبة هي الحبس من ثلاث (3) سنوات الغرامة 100.00 أورو[5].

كما جرم المشرع الفرنسي من خلال المادة 14 وما يليها من قانون 78-17 وما يليها أعمال المعالجة الآلية للمعطيات الشخصية دون مراعاة الشكليات القانونية، والتي تتمثل في احترام إجراء التصريح السابق تحت رقابة اللجنة القومية للمعلوماتية والحريات واستخدام رقم التسجيل الخاص بالمعطيات الشخصية دون

---

1 أحمد فتحي سرور، الحق في الحياة الخاصة، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، جامعة القاهرة، كلية الحقوق السنة 54، 2016، ص 30.

2 قانون العقوبات الجديد رقم 92-684 الصادر في 1992/07/22 والذي دخل حيز التنفيذ ابتداءً من 03/01/، 1994.

3 La loi No: 2004-801 du 6 out 2004 relative à la protection des personnes physique à légard des traitements de données à caractére personnel et modifiantt la loi No:78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

4 Ordonnance No: 2011-1012 du 24 out 2011 relative aux communications électroniques (JORF N 197 DU 26 OUT 2011).

5 Jean –Jaques Hyest, "La Fraude Informatique vue par le nouveau code pénale, Expertises des systéme de l'information , février 1992, p 150

ترخيص التي نظمها المشرع في القسم الرابع من ذات القانون[1]، وهو نفس الموقف الذي نظمه القانون رقم 2004-801 السابق الذكر، ولقد تم تضمين نفس الجريمة لقانون العقوبات من خلال نص المادة 226-16 وعاقب عليها المشرع في المادة 226-31 من قانون العقوبات بالحبس (5) سنوات وغرامة 30.000 أورو بالإضافة إلى العقوبات التكميلية.

ولقد جرم المشرع أفعال المساس باليانات الشخصية تحت عنوان الاعتداء على الحياة الشخصية، فنجده خطى خطوة سباقة في مجال حماية البيانات الشخصية من خلال توفير آليات الحماية الوقائية التي تهدف إلى منع الاعتداء على الحق، بالإضافة إلى الحماية العلاجية وعلى رأسها حماية الضحايا وفقاً لدعاوى التعويض، ثم عمل المشرع الفرنسي على الحرص من أجل تطوير الآليات الخاصة بحماية البيانات الشخصية، خاصة في ظل تنامي دور التشريعات الأوروبية الصادرة عن المجلس الأوروبي التي وضعت نصوص حديثة لتأسيس هذه الحماية، ومثالها التوجيه الأوروبي CE66/97 بشأن معالجة المعطيات الشخصية، وحماية الخصوصية في قطاع الاتصالات والتوجيه رقم CE58/ 2002 [2] بشأن معالجة المعطيات الشخصية وحماية الحياة الخاصة في إطار الانترنت، والتوجيه الأوروبي رقم CE 136/2009 بشأن حماية حقوق الأفراد مستخدمي شبكات الاتصالات الإلكترونية والخدمات.[3]

1 Ibrahim coulibaly, la protection des données à caractére personnel dans le domaine de la recherche scientifique, Thése pour obtenir le grade doctorat de l'université de Grenoble.2011. p18.

2 Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications Journal officiel n° L 024 du 30/01/1998 p. 0001 – 0008.

- **Voir aussi** :
- DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),
- IRECTIVE 2009/136/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

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

كما جاء المشرع ليواصل اهتمامه بتسييج الحماية للمعطيات الشخصية من خلال المعاملات الإلكترونية، وقام باستحداث نص خاص يجرم انتحال الهوية الرقمية، وهي الجريمة التي تقوم أساساً على جمع المعطيات الشخصية للأفراد وانتحالها شخصيتها من أجل استخدامها في أعمال احتيالية مالية وهذا من خلال الاعتداء على أرقام بطاقات الأتمان أو كلمة السر، وهو الأمر الذي جسده المشرع من خلال استحداث نص المادة 226-14 من قانون العقوبات المضافة بالمادة الثانية من قانون الأمن الداخلي[1]؛ حيث تنص على أن كل من يقوم بانتحال هوية الغير أو باستخدام واحدة أو أكثر من معطيات من أي نوع تسمح بتحديد هويته، وذلك بهدف بعث القلق لدى الآخرين والمساس بشرفهم، ويعاقب على ذلك بالحبس سنة وادة وغرامة 15 الف أورو مع إمكانية القضاء بالعقوبات التكميلية المنصوص عليها في المادة 226-31 من قانون العقوبات.

أما على المستوى التشريعات الأنجلوسكسونية فلقد حذت حذو التشريعات اللاتينية في مجال مكافحة الاعتداء على البيانات الشخصية، بحيث أصدر المشرع الإنجليزي قانون حماية البيانات منذ 1984 الذي حث على تأمين الحصول على البيانات الشخصية المخزنة لأغراض المعالجة بأسلوب صحيح ولتحقيق أغراض مشروعة، وكذا المشرع الأمريكي الذي سعى إلى تكريس هذه الحماية وفق جملة من الإصدارات التشريعية على رأسها قانون الخصوصية سنة 1974 بحيث قرر من خلاله الكثير من الضمانات في مواجهة المخاطر التي تتعرض لها بنوك المعلومات، وكذا نجد القضاء الأمريكي قد تأثر بجملة التعديلات الدستورية، فأعطى للمحاكم مساحة واسعة لتفسير نصوص الدستور في نطاق حماية الحقوق والحريات, وبالأخص الحق في الخصوصية.[2]

2- حماية البيانات الشخصية في إطار التشريعات العربية:

سعت تشريعات الدول العربية كغيرها من التشريعات الدولية نحو إصدار قوانين خاصة بحماية المعطيات الشخصية لتحقيق الانسجام مع توجهات المنظمات والاتفاقيات الدولية، إلا أنه يؤخذ عليها أنها تسير بخطوات متواضعة وبطيئة في مجال التصدي لاختراق وسرقة البيانات الشخصية وعمليات التجسس على الحياة الخاصة للأفراد، واستخدام المعلومات الشخصية لأغراض غير مشروعة وغيرها من الاعتداءات الإلكترونية على سرية وخصوصية البيانات الشخصية في العالم الرقمي، وهو ما يعزى لضعف الإرادة

1 Loi No: 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

2 جميل عبد الباقي الصغير، المرجع السابق، ص 117.

التشريعية في مواكبة المستجدات في مجال التشريع الإلكتروني، وفي هذا الإطار سنتطرق لموقف التشريع الجزائري وبعض التشريعات العربية المقارنة.

أ) موقف التشريعات العربية المقارنة من حماية البيانات الشخصية من الاعتداءات الإلكترونية:

لقد عملت العديد من التشريعات العربية على التصدي للاعتداء على البيانات الشخصية، بحيث اكتفت غالبية التشريعات بمحاولة تطويع النصوص العقابية التقليدية على الأنماط المستحدثة من الجرائم المعلوماتية, وعلى رأسها انتهاك سرية البيانات الشخصية، إلا أنه بالمقابل سعت بعض التشريعات الأخرى في مجال مكافحة المخاطر الواقعة عليها بإصدار تشريعات خاصة بحماية البيانات المعالجة آلياً أو تخصيص قوانين لمحاربة جرائم تقنية المعلومات، وإعطاء مساحة لمسألة الحماية الجنائية ضد الاعتداءات على تلك الخصوصية في المجال الرقمي، فلقد أصدر المشرع السعودي قانون مكافحة الجرائم المعلوماتية لسنة 2007 وتضمن القانون جملة من المواد تتعلق بحماية البيانات الشخصية المعالجة آلياً[1].

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

وكذا نص المشرع الإماراتي من خلال القانون الاتحادي الإماراتي رقم 1 لسنة 2006 المتضمن قانون المعاملات والتجارة الإلكترونية في المادة 28 /1 على أنه: "يعاقب بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن 20.000 درهم ولا تزيد عن 200.000 درهم أو بإحدى هاتين العقوبتين كل شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات أو مستندات أو مراسلات إلكترونية وأفشى أيا من هذه المعلومات".

وأما بخصوص المشرع التونسي فقد جرم عملية إفشاء البيانات الإلكترونية الشخصية في إطار خدمات التصديق الإلكتروني، وهذا بمعاقبة كل مورد أو مزود الخدمات الإلكترونية وأعوانه الذين يفشون أو

1 نظام مكافحة لمكافحة جرائم المعلوماتية السعودي لسنة 2007 الصادر بقرار مجلس الوزراء رقم 79 المؤرخ في 7 ربيع الأول 1428 وتمت المصادقة عليه بموجب المرسوم الملكي رقم 17 المؤرخ في 8 ربيع الأول 1428.

يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم بالسجن مدة تتراوح بين شهرين وغرامة تتراوح بين 1000 و10.000 دينار أو بإحدى هاتين العقوبتين.

كما عمل المشرع التونسي على إصدار قانون خاص ألا وهو القانون رقم 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية البيانات الشخصية, وضمنه حماية شاملة للمعطيات الشخصية من خلال جملة من الجرائم، بحيث ينص في الفصل 90 على جريمة المعالجة الآلية بطرق غير مشروعة, وكذا الإفشاء غير المشروع للمعطيات الشخصية, ويعاقب عليها بالسجن مدة عام وبخطية قدرها خمسة آلاف (5000) دينار كل من :

- يتعمد معالجة المعطيات الشخصية دون تقديم التصريح المنصوص عليه بالفصل السابع (7) أو الحصول على الترخيص المنصوص عليه بالفصلين 15 و69 من هذا القانون، أو يستمر في معالجة المعطيات بعد منع المعالجة أو سحب الترخيص.
- يقوم بنقل المعطيات الشخصية إلى الخارج دون ترخيص الهيئة.
- يحيل المعطيات الشخصية دون موافقة المعني بالأمر، أو موافقة الهيئة في الصور المنصوص عليها بهذا القانون.

كما جرم على فعل المعالجة للمعطيات الشخصية رغم اعتراض المعني في الفصل 91 بحيث يعاقب بالسجن مدة عام وبخطية قدرها خمسة (5000) آلاف دينار المسؤول عن المعالجة أو المناول الذي يواصل معالجة المعطيات الشخصية رغم اعتراض المعني بالأمر وفق أحكام الفصل 42 من هذا القانون.

كما أصدر المشرع البحريني القانون رقم 60 لسنة 2014 في شأن جرائم تقنية المعلومات[1], وتضمن القانون تجريم عدة صور للاعتداء على حق الخصوصية وخاصة في إطار إساءة استخدام البيانات الشخصية للأفراد بقصد التشهير والابتزاز[2].

ب) الحماية الجزائية للبيانات الشخصية من الاعتداءات الإلكترونية في ظل التشريع الجزائري:

عمل المشرع الجزائري كغيره من التشريعات المقارنة على الاعتراف بحماية البيانات الشخصية بشكل عام كمبدأ دستوري من خلال نص المادة 39 بنص صريح: "سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

1 القانون البحريني رقم 60 لسنة 2014 في شأن جرائم تقنية المعلومات المؤرخ في 6 ذي الحجة 1435 الموافق 30 سبتمبر 2014 ، منشور بالجريدة الرسمية للقانون البحريني المؤرخة في 9 اكتوبر 2014، العدد 3178، ص 5.

2 محمد عزت عبد العظيم، المرجع السابق، ص 220.

وقد كرس مبدأ الحماية الجنائية بموجب نص المادة 303 من قانون العقوبات التي نصت على أن: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات كل من تعمد المساس البيانات الشخصية بأي تقنية كانت وذلك:

- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه".

ويعتبر هذا النص قد حمل في طياته الحماية المرنة التي تمتد إلى أي طبيعة لحق الخصوصية أو الحديث وهذا باستخدام عبارة "أي تقنية كانت".

وعلى الرغم من النص غير المباشر على حماية البيانات الشخصية إلكترونياً، إلا أن المشرع اكتفى بمواكبة محاربة جريمة المساس بالبيانات الشخصية في العالم الرقمي بموجب القانون رقم 04-15 المتضمن تعديل قانون العقوبات في القسم المعنون بـ:" المساس بأنظمة المعالجة الآلية للمعطيات" من خلال نص المادة 39 فعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) أو بغرامة من 50 ألف إلى 100 ألف كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

وكذا جرم عمليات تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو إفشاء أو استعمالها لأي غرض كل المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم.

ولقد وفر المشرع الحماية الجنائية لحق الخصوصية بموجب المادة 4 من القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]، وهذا بضمان عدم المساس بالبيانات الخاصة للأفراد في حالة قيام السلطات المختصة بالقيام بعمليات المراقبة لكل الإتصالات الإلكترونية بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة.

وتعتبر الحماية الجنائية للبيانات الشخصية قد تناولها المشرع بشكل مرحلي؛ ولعل أهم مرحلة هي إصدار التشريع الخاص بحماية البيانات الشخصية من جانب المعالجة الآلية من خلال القانون 18-07 والذي ضمنه أحكام عديدة تتعلق بتجريم وحظر شتى الأساليب الماسة بسلامة وسرية البيانات الشخصية في إطار المعالجة الآلية، فقد جاء في نص المادة 38 منه أنه يجب على المسؤول عن المعالجة وضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو

1 القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها, ج ر ج العدد 47، المؤرخة في 2009/08/16، ص 5.

الضياع العرضي أو التـلـف أو النشر أو الـولـوج غيـر المرخصين، خصوصاً عندما تستوجب المعالجة إرسال معطيات عبر شبكة معينة وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة.

وقد عاقب المشرع على خرق أحكام المعالجة الآلية للمعطيات وفقاً للمبادئ المنصوص عليها المادة الثانية (02) من هذا القانون، بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج. ويعاقب بالحبس من سنة (1) إلى ثلاث سنوات وبغرامة من 100.000 دج إلى 300.000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقاً لأحكام السرية والموافقة القبلية للشخص المعني وفقاً للمادة السابعة (7) من هذا القانون.

يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، كل من قام، دون الموافقة الصريحة للشخص المعني وفي غير الحالات المنصوص عليها في هذا القانون، بمعالجة المعطيات الحساسة.

يعاقب بالحبس من سنة (1) إلى ثلاث سنوات وبغرامة من 100.000 دج إلى 300.000 دج، كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة.

يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون، والمتمثلة في احترام إجراءات سابقة على عملية معالجة البيانات الشخصية وذلك باستصدار تصريح أو ترخيص سابقين من السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

كما عمل المشرع على استحداث هيئة وطنية تختص بحماية البيانات الشخصية بموجب المادة 22 من ذات القانون, تكلف بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة, ومن أبرز صلاحيتها:

- منـح التـراخيص وتـلـقي التـصريـحـات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفق الشروط المنصوص عليها في هذا القانون.

- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي محل المعالجة.

وبهذا يعد التشريع الجزائري قد واكب التشريعات المقارنة في خلق أحكام خاصة بحماية البيانات الشخصية, وضمان حق الأفراد في إيجاد حماية جزائية موضوعية أو إجرائية ضد مختلف الأنشطة الإجرامية التي تمس بسلامة وسرية البيانات الشخصية، وكذا ضمان المعالجة الآلية لتلك المعطيات وفق أسس وشروط قانونية.

المبحث الثاني:

الحماية الجزائية من الجرائم المتعلقة بمضمون المعاملات الإلكترونية.

لا تتوقف الحماية الجزائية للمعاملات الإلكترونية من الجرائم المستحدثة على ما تعلق فقط بحماية النظام المعلوماتي وسلامة البيانات الإلكترونية من شتى أنواع الاعتداء, بل تتعداها إلى الحماية التي تتعلق بمضمون المعاملات وفحواها؛ وهي الجرائم التي تدخل في صميم هذه المعاملات، وتشمل الاعتداءات التي تتعلق بجوهر التعامل الإلكتروني.

والواقع أن المعاملات الإلكترونية تنشأ وفق العديد من الآليات التي أصبحت تعد من بين الركائز الأساسية لقيام تلك المعاملات، وفي هذا الصدد سنركز في المبحث على دراسة أهم الاعتداءات الواقعة على مضمون المعاملات الإلكترونية، والتي ترتبط أساساً بالجرائم المتعلقة بالتوقيع الإلكتروني في المعاملات الإلكترونية (المطلب الأول)، ثم الحماية الجزائية من الاعتداءات الواقعة على نظام الدفع الإلكتروني في المعاملات الإلكترونية (المطلب الثاني).

المطلب الأول: الحماية الجزائية من الجرائم الواقعة على التوقيع الإلكترونــي.

مع انتشار التبادل والتعاقد عبر الانترنت ووسائل الاتصال الحديثة، نشأ تغيير جذري على مستوى شكل الجرائم التي تمس هذا النوع من المعاملات، وهو الذي يؤثر خاصة على الثقة في الصفقات التجارية التي تتم عبر الانترنت، والتي أضحت تؤثر على مسألة التوقيع الإلكتروني باعتباره أهم الآليات المستحدثة في مجال المعاملات الإلكترونية, والتي تمثل عاملاً عاماً في إتمام التعاملات الإلكترونية في المجال التجاري والمصرفي وكافة أنواع العقود الإلكترونية، ولقد حرصت العديد من الدول على وضع أسس للحماية الجنائية وفق تشريعاتها الداخلية تنسيقاً مع التشريعات الدولية في مجال مكافحة الجرائم الماسة بهذه الآلية، ولذا نجد أغلب التشريعات المقارنة قد عملت على تناول مسألة الحماية بدءاً من ضبط القواعد القانونية التي تنظم آلية التوقيع الإلكتروني (الفرع الأول)، مروراً بتحديد أشكال الاعتداء الواقع عليه (الفرع الثاني)، ثم الوصول إلى تكريس آليات للحماية الجنائية الملائمة لتلك الجرائم (الفرع الثالث).

الفرع الأول: الإطار المفاهيمي للتوقيع الإلكترونــي.

لقد شهدت المعاملات الإلكترونية تطوراً كبيراً وسريعاً واكب الثورة المعلوماتية التي تطلبت تدخلاً سريعاً لمواجهة التحديات التي فرضتها سواءً داخلياً أو دولياً، الأمر الذي دعى المشرع إلى التدخل التشريعي للنص على التوقيع والتصديق الإلكترونيين من خلال التعريف والأهمية داخل نطاق المعاملات الإلكترونية, وكذا مسألة حجية التوقيع الإلكتروني في الإثبات.

البند الأول: تعريف التوقيع والتصديق الإلكترونيين.

إن التوقيع الإلكتروني قد ظهر بفضل ضغط الثورة المعلوماتية التي أثرت على شكل المعاملات، ومن ثم ألحت الضرروة على وجود شكل جديد للتوقيع يلائم التطورات القانونية الأمر الذي دعى إلى اللجوء إلى التوقيع الإلكتروني لتلافي العيوب التي أحاطت بالتوقيع التقليدي، بحيث عرفه جانب من الفقه[1] بأنه:"مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف، ويصدر التوقيع بمناسبة استخدام معادلات خوارزمية متناسقة تتم معالجتها إلكترونياً تنتج شكلاً معيناً يدل على شخصية صاحب التوقيع".

1 منير محمد الجنيهي, وممدوح محمد الجنيهي، الطبيعة القانونية للعقد الإلكتروني، دار الفكر الجامعي،مصر، سنة 2007، ص 195.

كما عرفته لجنة التجارة الدولية التابعة للأمم المتحدة في القانون الصادر عام 1996 بشأن العقود الإلكترونية بأنه:"عبارة عن مجموعة أرقام تمثل توقيعاً على رسالة معينة، ويتحقق التوقيع من خلال اتباع بعض الإجراءات الحسابية المرتبطة بمفتاح رقمي خاص بالشخص المرسل".

ولقد تصدى قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية والتجارة الإلكترونية لعام 2001 لتحديد تعريف له بحيث اعتبره أنه يمثل جملة من البيانات التي تأتي في شكل إلكتروني مدرجة في رسالة بيانات أو مرفقة بها أو مرتبطة بها منطقياً يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[1].

فالتوقيع الإلكتروني وسيلة حديثة لتحديد هوية صاحب المعاملة الإلكترونية ويعكس رضاؤه بالتصرف القانوني الموقع عليه ومن ثم يقوم بذات وظيفة التوقيع التقليدي مع الفرق في الوسيط الإلكتروني الذي ينشأ من خلاله التوقيع، وذلك استجابة لنوعية المعاملات التي تتِم إلكترونياً.

ولقد عرفه القانون رقم 01 لسنة 2006 بشأن التجارة الإلكترونية الإماراتي بأنه:"توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام أو معالجة ذو شكل إلكتروني، وملحق أو مرتبط منطقياً برسالة إلكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة"[2]، وأما التوجه الأوروبي رقم 93/99 الصادر عن المجلس الأوروبي فعرفه بأنه عبارة عن معلومات أو معطيات في شكل إلكتروني ترتبط أو تتصل منطقياً بمعطيات إلكترونية أخرى وتستخدم كوسيلة لإقرارها".

وبهذا نجد أن هذه التعاريف تحدد شروطاً لصحة التوقيع الإلكتروني تقوم أساساً على تخصيصه لصاحبه دون غيره، وأن يكون دال على صاحبه على أن يتم بوسائل تمكن صاحبه من الاحتفاظ به تحت سيطرته وحده[3].

أما بالنسبة للمشرع المصري فلقد أناطه بأهمية خاصة بحيث أفرد له تعريف على مستوى مشروع قانون التجارة الإلكترونية المصري لسنة 2000 وعرفه بأنه:"حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره"[4].

---

1 المادة 1/2 من قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.

2 المادة 15 من قانون رقم 01 لسنة 2006 بشأن التجارة الإلكترونية الإماراتي.

3 ثروت عبد الحميد، التوقيع الإلكتروني (ماهيته- مخاطره- حجيته في الإثبات)، دار الجامعة الجديدة، سنة 2007، ص 173.

4 **نقلاً عن:** محمد حسام محمود لطفي، الإطار القانوني للمعاملات القانونية (دراسة مقارنة) في قواعد الإثبات في المواد المدنية والتجارية، القاهرة، دار النهضة العربية، سنة 2002، ص 131.

كما عرفه قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 بأنه:"ما يوضع على محرر إلكتروني، ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون لها طابع منفرد يسمح بتحديد شخصية الموقع ويميزه عن غيره.[1]

أما المشرع التونسي فلم يَصُغ للتوقيع الإلكتروني تعريفاً خاصاً من خلال قانون رقم 83 للمبادلات والتجارة الإلكترونية التونسي الصادر سنة 2000 بل حدده بمجموعة من المفاهيم كمنظومة إحداث الإمضاء.

وأما المشرع الفرنسي فقد تناول مسألة التوقيع الإلكتروني وفقاً للقانون الخاص بالتوقيع الإلكتروني رقم 230 لسنة 2000 بشأن الإثبات المتعلق بتكنولوجيا المعلومات واعتماد التوقيع الإلكتروني، وجاء هذا القانون في إطار تعديل للنصوص المتعلقة بالإثبات الواردة في القانون المدني بإضافة نصوص حديثة تتوافق مع التطور الحديث في المعاملات وتقنية المعلومات، وتضمن أربعة (4) مواد تتعلق بالإثبات المعلوماتي، وكذا مساواة التوقيع الإلكتروني بالتوقيع التقليدي طبقاً لنص المادة 1316-4 من القانون المدني والمضافة بموجب القانون 2000-230 الخاص بالتوقيع الإلكتروني حيث عرفته بأنه:"التوقيع الضروري لاكتمال التصرف القانوني الذي يميز هوية صاحبه كما يعبر عن رضا الأطراف وبالالتزامات الناشئة عنه"[2].

وأما بالنسبة للتشريع الأمريكي فلقد اعترفت بعض الولايات الأميريكية بالتوقيع الإلكتروني واهتمت بوضع نصوص داخلية لتنظيمه، إلا أنها اتجهت نحو خلق إطار تشريعي متناسق بين التشريعات الاتحادية، ونتاجاً لذلك تم إصدار قانون التوقيع الإلكتروني لسنة 2000 الذي جاء لِيُطبق على التصرفات القانونية بين الولايات الداخلية أو مع دول أجنبية، وهذا يدخل في إطار تدعيم التشريع الأمريكي للأسس التي تقوم عليها التصرفات والمعاملات الإلكترونية وتدعيم الثقة في هذا المجال، ويظهر ذلك في الاعتراف بمسألة التوقيع الإلكتروني في مختلف المجالات الاقتصادية والمدنية وتثبيت الحجة القانونية للتوقيع الإلكتروني كعامل لدعم الشرعية والصفة القانونية له في مجال التعاملات المالية والتجارية[3].

وأما بخصوص المشرع الجزائري فلقد حذا حذو التشريعات المقارنة العربية والغربية فيما يخص تنظيم التوقيع الإلكتروني من خلال القانون 15-04 الذي يحدد القواعدالقواعد المتعلقة بالتوقيع والتصديق

1 المادة 03 من قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2015.

2 Jonathan Rosenar; Cyber-Law, the law of the internet; ed springer.1997. p 237

3 سند حسن سالم صالح، التنظيم القانوني للتوقيع الإلكتروني وحجيته في الإثبات المدني، دار النهضة العربية، القاهرة، سنة 2010، ص 96.

الإلكترونيين[1], وجاء بتعريف خاص به في نص المادة الثانية (2) من نفس القانون بحيث عرفته بأنه:"بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق"، وعمل المشرع وفقاً للقانون 05-10 المعدل للقانون المدني باستحداث نص المادة 2/327، والتي نصت على أنه يعتد بالتوقيع الإلكتروني وفقاً للشروط المذكورة في المادة 323 مكرر"، ويتضح أن النص أضفى الحجية القانونية على المحررات بالاعتراف بالتوقيع الإلكتروني، من جانب آخر نجد بأن المرسوم التنفيذي 07-162 جاء بتعريف غير مباشراً للتوقيع الإلكتروني بحيث عرفه بأنه:"معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر 1 من القانون المدني"، وبالتالي يربط بين التوقيع الإلكتروني والمحررات الإلكترونية وحجيتها في الإثبات، وهو موقف أراد منه المشرع الجزائري التعريف بالتوقيع الإلكتروني كآلية فعالة لتوثيق العمليات الإلكترونية.

أما بخصوص آلية التصديق الإلكتروني فهو عبارة عن وسيلة فنية آمنة تساهم في التحقق من صحة التوقيع الإلكتروني أو المحرر الإلكتروني حتى يمكن نسبته إلى شخص او كيان معين، يصدر عن جهة موثوقة أو طرف محايد يسمى مقدم خدمات التصديق.

ولقد عرفه المشرع الجزائري وفقاً لنص الفقرة 15 من المادة 2 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين بأنه:"مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين". ولقد عرف قانون الأونيسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001 جهة التصديق أو مقدم خدمات التصديق بنص المادة (2-e) بأنه الشخص الذي يصدر الشهادات الإلكترونية، ويمكن أن يقدم خدمات أخرى مرتبطة بالتوقيعات الإلكترونية".

ولجهات التصديق الإلكتروني أدوار يمكن عرضها في النقاط التالية:

- التحقق من هوية الشخص الموقع: بحيث تقوم جهات التوثيق الإلكتروني بإصدار شهادة توثيق إلكترونية تفيد التصديق على التوقيع الإلكتروني في تعاقد معين تشهد بموجبها بصحته ونسبته إلى من صدر عنه.
- إثبات مضمون التبادل الإلكتروني حيث تتولى جهة التوثيق كذلك التحقق ممن مضمون التبادل الإلكتروني بين الأطراف وسلامته وجديته وبعده عن الاحتيال والغش، فضلاً عن إثبات وجود مضمونه.

1 القانون رقم 15-04 المؤرخ في 2015/02/01 الموافق 11 ربيع الثاني 1436 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين (ج ر ج العدد 06).

كما أن شهادة التصديق عرفت من قبل الأونيسترال النموذجي المتعلق بالتوقيعات الإلكترونية بأنها: "رسالة بيانات أو سجلاً آخرا يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع".

وقد عرفها جانب من الفقه[1] بأنها:"الشهادات التي تصدرها جهات التوثيق المرخص لها من قبل الجهات المسؤولة في الدولة لتشهد بصحة التوقيع الإلكتروني واستيفائه لكافة الشروط والضوابط المطلوبة فيه كونه دليل إثبات يعول عليه".

أما المشرع الجزائري فبقد عرفها بموجب المادة 7/2 من القانون 15-04 بأنها:"وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع".

ثانياً: الحجية القانونية للتوقيع الإلكترونـــي.

اهتمت العديد من التشريعات بتنظيم مسألة الحجية القانونية للتوقيع الإلكتروني في الإثبات خاصة بعد استحداثه كأحد الآليات الضرورية لاكتمال المعاملات المدنية والتجارية الإلكترونية، ومن بينها التشريع التونسي من خلال نص المادة 4 من قانون المبادلات والتجارة الإلكترونية لعام 2000، والذي أورد فيه حكم يعترف من خلاله بالمساواة في حجية التوقيع الإلكتروني الذي تتضمنه وثيقة إلكترونية وحجية التوقيع التقليدي في المعاملات الورقية، باحتفاظ كل من المرسل بالوثيقة التي أرسلها واحتفاظ المرسل إليه بالوثيقة التي استلمها على حامل إلكتروني، وذلك للاطلاع على محتواها ومدة صلاحيتها و بشكلها النهائي بطريقة تضمن سلامة محتواها وتاريخها ومكان إرسالها واستلامها، كما منح ذات القانون حجية كاملة للشهادات التي يمكن مصادقتها في الخارج نفسها التي تمنح للتوقيع الإلكتروني[2].

وهذا الموقف تبناه أيضاً المشرع الإماراتي من خلال القانون الاتحادي للإثبات رقم 36 لسنة 2006 وبالتحديد في نص المادة 17 مكرر التي اعتبرت أن للتوقيعات الإلكترونية ذات الحجية المقررة للتوقيعات التقليدية بشرط مراعاة الأحكام المقررة في قانون المعاملات والتجارة الإلكترونية[3].

---

1 سند حسن سالم صالح، المرجع السابق، ص 98.

2 المادة 23 من القانون التونسي المتعلق بالمبادلات والتجارة الإلكترونية.

3 هذه الأحكام هي التي تحدد شروط الاعتراف بالتوقيع الإلكتروني وحمايته قانونا والتي تقع أساسا على:" أن ينفرد به الشخص الذي استخدمه- إثبات هوية الشخص المستخدم له- أن يكون تحت سيطرته التامة سواء بالنسبة لإنشائه أو وسيلة استعماله وقت التوقيع- ويرتبط بالرسالة الإلكترونية ذات الصلة به بطريقة توفر تأكيدا يعتمد عليه في سلامة التوقيع. **ينظر في ذلك:** ثروت عبد الحميد، المرجع السابق، ص 103.

أما التشريع المصري فلقد أفرد حكماً خاصاً يعترف من خلاله بالحجية القانونية للتوقيع الإلكتروني في إثبات المعاملات المدنية والتجارية، وهذا تحديداً في نص المادة 14 من القانون رقم 15 لسنة 2004 الخاص بالتوقيع الإلكتروني التي جاء فيها:"للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة في أحكام قانون الإثبات المصري في المواد المدنية والتجارية, إذا روعي في إنشاءه وإتمامه الشروط المنصوص عليها في هذا القانون, والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون"، ونصت المادة 18 من ذات القانون بأن: "يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات".

وبالرجوع إلى أحكام المادة 2/327 من القانون المدني الجزائري نجد أن المشرع قد اعترف بالحجية القانونية للتوقيع الإكتروني من خلال المساواة الوظيفية بينه وبين التوقيع التقليدي، وهذا وفقاً للشروط المذكورة في المادة 23 مكرر1 من نفس القانون؛ والتي نستشف من فحواها عدم التمييز بين الإثبات بالكتابة في الشكل الإلكتروني ونظيرتها على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها، وهنا نجد أن المشرع قد ربط حكم الحجية القانونية للتوقيع الإلكتروني على حكم الكتابة الإلكترونية, وأعطى حكماً مباشراً للإعتراف بالحجية القانونية للتوقيع الإلكتروني.

أما التشريع الفرنسي فلقد اهتم بمسألة حجية التوقيع الإلكتروني من خلال نص المادتين 13 و16 التي جاءت بعد التعديل الذي استحدثه القانون الخاص بالتوقيع الإلكتروني رقم 230 لسنة 2000 بشأن الإثبات المتعلق بتكنولوجيا المعلومات واعتماد التوقيع الإلكتروني، وركز المشرع على استحداث مبدأ المساواة وعدم التمييز بين التوقيع سواء جاء على دعامة مادية أو غير مادية, أو من خلال وسيط ورقي أو آخر إلكتروني، فالأمر لا يجب أن يكون سبباً لعدم الاعتراف بها.

ودعمت ذات الموقف بحكم صريح ينص على مبدأ المساواة الوظيفية بين التوقيع التقليدي والإلكتروني طالما أن هذا الأخير يميز صاحبه ويحدد هويته، وقد تم إنشاؤه وحفظه بطريقة تجعله سليماً من التحريف أو التعديل[1]. أما بخصوص التشريع الاتحادي الأمريكي فقد اعترف بدوره بحجية المحررات الإلكترونية والتوقيع الإلكتروني دون اشتراط الحصول على موافقة الشخص أو ترخيص من جهة معينة[2].

1 هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية، القاهرة، سنة 2000، ص 22.

2 سند صالح، المرجع السابق، ص97.

وفي الواقع نرى أن جل التشريعات المقارنة التي تبنت فكرة الاعتراف بالحجية القانونية للتوقيع الإلكتروني قد رأت ضرورة النص على هذا الحكم لإكمال الصورة التشريعية للاعتراف بالمحررات الإلكترونية ودورها في إنشاء المعاملات الإلكترونية، وهو الحكم الذي عملت التشريعات الداخلية انتهاجه وفق ما جاء به قانون الأونيسترال النموذجي, والذي حدد أيضاً شروطاً خاصة للاعتراف بالحجية القانونية, وهو نفس الحكم التي تناولته التشريعات المنظمة للتوقيع الإلكتروني.

الفرع الثاني: الجرائم الواقعة على التوقيع الإلكتروني وآليات الحماية المقررة لها.

لقد اختلفت التشريعات حول مسألة توحيد صور الإجرام التي تقع على التوقيع الإلكتروني، فالبعض منها قرر تجريم الأفعال التي تشكل أكثر خطورة وتمس بمصداقية وحقيقة التوقيع كفعل التزوير ومزاولة نشاط التصديق الإلكتروني بدون ترخيص مسبق، وكذا تم اعتماد بعض القوانين الخاصة من قبل التشريعات المقارنة شملت بها أغلب الاعتداءات الواقعة على التوقيع الإلكتروني، ابتداءً من النظام المعلوماتي للتوقيع، وكذا آليات وإصدار التوقيعات واستعماله، ونجد البعض الآخر قد اكتفى بإصدار تشريعات متناثرة تأخذ في أغلبها صور تعديلات على التشريعات العقابية, ليأخذ حكم تجريم الاعتداء على التوقيع الإلكتروني من أصل تجريم الاعتداءات الماسة بنظم المعالجة الآلية للمعطيات والممارسات غير المشروعة في مجال المعاملات الإلكترونية، وفي هذا الصدد ارتأينا إلقاء الضوء على أهم الأحكام التي تضمنتها بعض التشريعات الأجنبية والعربية في مجال مكافحة الاعتداءات الواقعة على نظام التوقيع الإلكتروني، وهذا وفق جملة من الجرائم المنصوص عليها في القواعد العامة أو نصوص خاصة بتنظيم التوقيع الإلكتروني.

البند الأول: جريمة الاعتداء على النظام المعلوماتي للتوقيع الإلكتروني.

لقد عنيت أغلب التشريعات المقارنة بوضع نظام حمائي ضد المخاطر التي تحيط بمجال المعاملات الإلكترونية, مركزة على نطاق الحماية المتعلق بشكل المعاملات التي تتم من خلال البيانات الإلكترونية، وفي إطار الجرائم المستحدثة ظهرت الحاجة إلى حماية التوقيع الإلكتروني في الإطارين الشكلي والموضوعي, وعلى رأس تلك الجرائم ما يتعلق بجرائم الدخول عن طريق الغش لأنظمة المعلومات الخاصة بالتوقيع الإلكتروني، وكذا صنع أو حيازة برنامج لإعداد توقيع إلكتروني, وكذا العمليات المؤدية إلى إتلاف التوقيع الإلكتروني.

البند الثاني: جريمة الدخول بطريق الغش إلى قاعدة بيانات تتعلق بالتوقيع الإلكتروني

تعتبر جريمة الدخول بطريق الغش إلى قاعدة البيانات المتعلقة بالتوقيع الإلكتروني هي أحد فروع جريمة المساس بالنظام المعلوماتي، ولقد تصدت لها أغلب التشريعات العقابية المنظمة للتوقيع الإلكتروني إما بنص خاص, أو الاكتفاء بتجريم عمليات الدخول أو البقاء داخل الأنظمة المعلوماتية بصفة عامة[1].

أجمعت غالبية التشريعات وكذا الآراء الفقهية على إدماج صورتي الدخول والاتصال عن طريق الغش للنظام المعلوماتي الخاص بالتوقيع الإلكتروني، ولا يفترض تحديد طرق الدخول والاتصال بالنظام أو قاعدة البيانات لافتراض حدوث ذلك بمختلف الوسائل التقنية، فقد تقع عملية الدخول باستعمال أجهزة خاصة تمكن الجاني من التعدي على شفرات البيانات, أو بسرقة الشفرة الصحيحة لشخص آخر واستعمالها في عملية الدخول وبهذا فقد تتعدد الوسائل المستعملة[2].

والنشاط الإجرامي يتحدد بمجرد صدور فعل الدخول أو الاتصال دون ضرورة إحداث ضرر أو إتلاف, بل يكفي اشتراط عدم مشروعية الوسيلة المستعملة أو حدوثها بشكل غير قانوني كاستخدام التدليس أو الاحتيال، ويفترض وقوع هذه الأفعال من قبل أشخاص تتوفر لهم الإمكانية بولوج النظام بشكل قانوني ومعتاد، أو من قبل الأشخاص الذين لا يحق لهم الدخول إلى النظام المعلوماتي الخاص بالتوقيع الإلكتروني.

وتتحقق جريمة الدخول أو الاتصال غير المشروع بالنظام المعلوماتي للتوقيع الإلكتروني بتوافر القصد العام الذي يتطلب علم الجاني بولوجه إلى قاعدة البيانات بشكل غير قانوني، وكذا اتجاه إرادته إلى إحداث ذلك، فمن المنطق أن يتم تنافي بقاء الجاني على الاتصال بالنظام المعلوماتي للتوقيع الإلكتروني عن طريق المصادفة أو التجريب فحسب، ولكن فعل البقاء يدل على تعمده الاعتداء عن طريق الغش أو التدليس الذي يعكس سوء نيته.

وبخصوص المواجهة التشريعية لجريمة الدخول أو الاتصال غير المشروع بالنظام المعلوماتي للتوقيع الإلكتروني, فقد سعى المشرع الفرنسي لتوفير الحماية الجنائية للنظام المعلوماتي للتوقيع الإلكتروني وفق المواد الخاصة بحماية أنظمة المعالجة الآلية في المواد 1/323 إلى 7/323 من قانون العقوبات, على اعتبار أن التوقيع الإلكتروني يمثل نظاماً معلوماتياً يشتمل على بيانات إلكترونية, فمن هذا المنطلق تنطبق عليه نصوص

1 شيماء عبد الغني عطاالله، المرجع السابق، ص 161.

2 محمود إبراهيم غازي، المرجع السابق، ص 339.

الحماية المقررة، واعتبر أن أفعال الدخول والبقاء أو الاتصال بنظام التوقيع الإلكتروني بطريق غير مشروع من قبل الجرائم التي عاقب عليها المشرع الفرنسي وفقاً لنص المادة 1/323 من قانون العقوبات بالحبس لمدة سنتين (02) وغرامة تقدر بـ: 30 ألف أورو.[1]

أما المشرع الأمريكي فقد اعتمد وفقاً للقانون الاتحادي الخاص بجرائم الحاسوب، وتحديداً من خلال نص المادة 3/1030 على تجريم عمليات الدخول أو البقاء غير المشروع من خلال معاقبة كل من توصل بصفة غير قانونية إلى الأنظمة المعلوماتية للتوقيع الإلكتروني، واستغل فرصة وصوله لتحقيق أغراض غير مشروعة، وقرر إزائها عقوبة بالحبس لمدة لا تزيد عن سنة (1) واحدة وغرامة لا تزيد عن 5 آلاف دولار أمريكي[2].

أما بخصوص التشريعات العربية فجاء على رأسها المشرع المصري الذي أفرد حكماً خاصاً يتعلق بتجريم الدخول بطريق الغش أو التدليس لقاعدة بيانات تتعلق بالتوقيع الإلكتروني، وهذا من خلال أحكام نص مشروع قانون التجارة الإلكترونية في نص المادة 26 منه حيث عاقب الجاني بالحبس وبغرامة لا تقل عن 3000 جنيه، ويعاقب بنفس العقوبة من أبقى الاتصال بنظام المعلومات بصورة غير مشروعة.

وضَمَّن القانون الإتحادي الإماراتي رقم 5 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات, وبالتحديد من خلال نص المادة الثانية (02) منه تجريم فعل الدخول أو البقاء لأي نظام إلكتروني أو نظام معلوماتي بدون حق مشروع أو تصريح مسبق أو تجاوز التصريح الممنوح بالبقاء داخل النظام المعلوماتي للتوقيع الإلكتروني، وقد حددت نفس المادة عقوبة للجاني بالحبس والغرامة التي لا تزيد 300 ألف درهم إماراتي.

وحاول المشرع السعودي توسيع دائرة تجريم الأفعال المؤدية إلى الاعتداء على الأنظمة المعلوماتية الخاصة بالتوقيع الإلكتروني؛ وهذا من خلال قانون نظام مكافحة جرائم المعلوماتية، والذي أورد به نص يتعلق بتجريم الدخول أو البقاء أو الاتصال بطريق غير مشروع لأي نظام داخل الحاسب الآلي، وبهذا فقد

1 محمد مرسي الزهرة، مدى حجية التوقيع الالكتروني في الاثبات، دراسة مقارنة، مجلة الشؤون الاجتماعية، القاهرة، العدد 48، السنة 12، 2015، 85 وما بعدها.

2 محمد السيد عرفة، التجارة الالكترونية عبر الانترنت، مؤتمر "القانون والكمبيوتر"، كلية الشريعة والقانون، الإمارات العربية المتحدة، سنة 2000، ص 13.

شمل الحكم تجريم الاعتداء على نظام التوقيع الإلكتروني، وعاقب على هذه الأفعال بالسجن مدة لا تزيد عن أربع (4) سنوات وبغرامة لا تزيد عن ثلاثة (3) ملايين ريال سعودي أو بإحدى هاتين العقوبتين[1].

وجاء المشرع السعودي من خلال أحكام نظام المعاملات الإلكترونية ليضع حكماً خاصاً وأكثر وضوحاً لتجريم الدخول لمنظومة التوقيع الإلكتروني لشخص آخر دون تفويض صريح أو نسخه أو إعادة تكوينه أو الاستيلاء عليه[2]، وعاقب على تلك الأفعال بغرامة لا تزيد عن خمسة (5) ملايين ريال أو بالسجن لمدة لا تزيد عن خمس (5) سنوات أو بالعقوبتين مجتمعتين مع جواز مصادرة الأجهزة أو البرامج المستخدمة في ارتكاب الجريمة[3].

وتناول المشرع الأردني من خلال قانون الجرائم الإلكترونية رقم 27 لسنة 2015 تجريم أفعال الدخول أو البقاء غير المشروع لنظام معلوماتي يتعلق بالتوقيع الإلكتروني بأي وسيلة كانت وبدون تصريح مسبق, أو بتجاوز التصريح الممنوح، وعاقب عليها بالحبس لمدة لا تزيد عن ثلاثة (3) أشهر وبغرامة لا تقل عن مائة (100) دينار ولاتزيد عن مائتين (200) دينار أردني[4].

أما عن موقف المشرع الجزائري فلم يورد نص خاص في القانون 15-04 يجرم من خلاله الدخول أو البقاء غير المصرح به لنظام معلوماتي متعلق بالتوقيع الإلكتروني، وإنما انتهج منهجاً غير مباشرٍ في تجريم فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المنظومة المعالجة الآلية للمعطيات المنصوص عليها بموجب القانون رقم 04-15 المعدل لقانون العقوبات ، وبالرجوع إلى مفهوم منظومة المعالجة الآلية للمعطيات نجده يستوعب مفهوم النظام المعلوماتي للتوقيع الإلكتروني، وبالتالي اعتبار هذا الحكم غير مباشر سعى من خلاله المشرع بتصنيف تلك الأفعال في مصاف الجنحة المعاقب عليها بالحبس من ثلاثة (3) أشهر إلى سنة (01) وبغرامة من 50 ألف دينار إلى 100 ألف دينار جزائري.

البند الثالث: جريمة إتلاف أو تعييب التوقيع الإلكتروني.

تقع جريمة إتلاف التوقيع الإلكتروني بإتلاف أو تعييب التوقيع في حد ذاته، أو قد يمتد إلى المحرر أو الوسيط الإلكتروني الذي يؤثر بشكل سلبي على سير المعاملات الإلكترونية وإعاقتها، وهنا ذهب بعض

1 المادة 5 من قانون مكافحة جرائم المعلوماتية السعودي.

2 المادة 8/23 من نظام المعاملات الإلكترونية السعودي.

3 المادة 24 من نظام المعاملات الإلكترونية السعودي.

4 المادة 3 من قانون مكافحة الجرائم الإلكترونية الأردني رقم 27 لسنة 2015.

الفقه[1] إلى تحديد معنى الإتلاف بعملية إفقاد البرنامج المعلوماتي الخاص بالتوقيع الإلكتروني قدرته على العمل كلياً باستخدام أية وسيلة كانت، أما التعييب فهو الإفقاد الجزئي لهذا البرنامج الخاص بالتوقيع الإلكتروني.

ويتمثل النشاط الإجرامي لهذه الجريمة في إقبال الجاني بإتلاف النظام المعلوماتي للتوقيع الإلكتروني على نحو يؤدي إلى عدم قدرته على العمل بشكل نهائي، أو تعييب هذا النظام بحيث ينقص من صلاحية التوقيع الإلكتروني للاستعمال، وبهذا تركت العديد من التشريعات المقارنة مسألة تحديد وسائل الإتلاف أو التعييب مما يجعل الأمر مفتوحاً لاحتمال كل الوسائل المعروفة أو المكتشفة في وقت لاحق.

ولا يكفي لقيام جريمة إتلاف التوقيع الإلكتروني بحدوث السلوك الإجرامي وفقاً للمعنى المحدد سابقاً بل يجب توافر عنصري العلم والإرادة اللذان يتخذهما الجاني كأساس للاعتداء واتجاه إرادته في إحداث ضرر لصاحب التوقيع الإلكتروني[2].

أما بخصوص المواجهة التشريعية لجريمة إتلاف التوقيع الإلكتروني, فلم تتجه أغلب التشريعات المقارنة إلى النص بشكل مباشر على تجريم عمليات الإتلاف أو التعييب التي تمس التوقيعات الإلكترونية، بل اكتفت بحظر الإتلاف المعلوماتي الذي يقع على البيانات أو النظام المعلوماتي ككل، وهو حكم عام يشمل الخاص ويغطي حماية التوقيع الإلكتروني، فالمشرع الفرنسي اعتمد من خلال نصوص قانون العقوبات الجديد وفقاً لنص المادة 323-3 تجريم أفعال الإدخال أو محو أو تعديل البيانات التي تحتويها الأنظمة المعلوماتية, مما يشكل إتلاف لعمل النظام المعلوماتي الخاص بالتوقيع الإلكتروني, وعاقب عليها بالحبس لمدة (**5**) سنوات وغرامة قدرها **75** ألف أورو[3].

بدوره التشريع الأمريكي جاء بتعديل هام من خلال نص المادة 1030 والخاصة بإتلاف الأنظمة المعلوماتية، وتحديداً نص الفقرة الخامسة منها التي جرمت كل إتلاف أو إفساد لسلامة المعلومات والبرامج وأنظمة الحاسبات الآلية، ويعتبر هذا الحكم يشمل أيضاً حماية نظام التوقيع الإلكتروني بما يحتويه من بيانات أو شفرات إلكترونية، فيعتبر أي مساس بالتعديل أو التعييب سلوكاً يُعاقَب عليه بالحبس لمدة سنة (1) وغرامة لا تزيد عن 5000 دولار أمريكي.

---

1 فتوح شاذلي، المواجهة التشريعية للجرائم المستحدثة، بحث مقدم لمؤتمر "الأمن والسلامة", المنعقد من قبل وزارة الداخلية بأبوظبي في 06-08 أكتوبر 2015، الإمارات العربية المتحدة، ص 205.

2 ثروت عبد الحميد، المرجع السابق، ص 185.

3 Leclercq (jean); Prevue et Signature électronique de la loi 13 mars 2001, au decret du mars 2001.

ويعتبر المشرع الأمريكي سباقاً في إيجاد نص خاص يتعلق بتجريم أفعال الإتلاف التي تمس التوقيع الإلكتروني من خلال نص المادة 2/23 من القانون الاتحادي لسنة 2000؛ بحيث نص على معاقبة كل شخص صدر منه فعل الإتلاف أو تعييب توقيع، أو وسيط أو محرر إلكتروني بالحبس وبغرامة لا تقل عن 10 آلاف دولار ولا تجاوز 100 ألف دولار أو بإحدى هاتين العقوبتين[1].

ويأتي المشرع الإماراتي في القانون الاتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بالنص على تجريم عمليات الإتلاف الواقعة على الأنظمة المعلوماتية, والتي تؤدي إلى تعطيلها أو تدميرها أو مسح أو تعديل البيانات التي بداخلها، وعاقب عليها بالسجن لمدة لا تقل عن (5) سنوات وغرامة لا تجاوز 500 ألف درهم.[2]

البند الرابع: جريمة إصدار شهادات التوقيع أو التصديق الإلكتروني بدون ترخيص.

يبنى التوقيع الإلكتروني على جملة من الإجراءات التي يفرضها المشرع في إطار القوانين المنظمة للمبادلات الإلكترونية أو التشريعات التي تخصص لتنظيم التوقيع الإلكتروني بشكل منفرد، ومن أهمها ضرورة احترام آليات وشروط عملية التصديق الإلكتروني، وهذا نظراً للانتشار الواسع والسريع لاستخدام التكنولوجيا التقنية، ومن ثم ضرورة وجود آليات لإكساب التوقيع الإلكتروني المصداقية الكافية من أجل حث المتعاملين على الإقبال على التعامل في مجال العقود الإلكترونية بكل طمأنينة وثقة، وبهذا تأتي المصادقة الإلكترونية على التوقيع الإلكتروني من قبل أجهزة حددت صلاحيتها وشروط اعتمادها بدقة من قبل التشريع.

وعملت أغلب التشريعات المقارنة إلى التصدي إلى كافة أنواع السلوكيات الإجرامية التي تقع في إطار مخالفة شروط آلية التصديق الإلكتروني؛ ومن أهمها جريمة إصدار شهادة التصديق الإلكتروني دون ترخيص أو في حالة سحبه.

1- البناء القانوني لجريمة إصدار شهادة التصديق الإلكتروني بدون ترخيص:

تقوم جريمة إصدار شهادة التصديق الإلكتروني بدون ترخيص على انتحال الجاني صفة مزود خدمات التصديق المرخص له من قبل الجهة الوصية بالتصديق، بحيث يعمل على إصدار شهادة التصديق الإلكتروني دون الحصول على الترخيص المسبق الذي يحدد للأفراد الذين يتوجهون لعملية التصديق الإلكتروني شروطاً

1 ثروت عبد الحميد، المرجع السابق، ص 173.

2 المادة 10 من القانون الاتحادي الإماراتي في شأن مكافحة جرائم تقنية المعلومات.

قانونية يتوجب توافرها في الشخص الطبيعي أو المعنوي، إعطاؤه بموجبها رخصة إصدار شهادات التصديق المعترف بها في إطار التوقيع الإلكتروني، أو قد يتمثل سلوك الجاني أيضا في مزاولة نشاط منح شهادة التصديق الإلكتروني مع انتهاء مدة صلاحية الرخصة الممنوحة له مسبقاً، وبهذا تعتبر كل عمليات المصادقة الإلكترونية التي تتم في هذه الفترة غير قانونية وترتب المسؤولية الجنائية في حق مزود الخدمة[1].

وبهذا يرتبط النشاط الإجرامي لجريمة إصدار شهادة التصديق بدون ترخيص بمخالفة أولاً المفهوم القانوني الذي يضعه المشرع لشهادة التصديق في حد ذاته، فنجد المشرع المصري يعرف شهادة التصديق الإلكتروني بموجب المادة 1 من قانون التوقيع الإلكتروني رقم 15 لسنة 2004 بأنها:"الشهادة التي تصدر من الجهة المختصة بالتصديق وتثبت الإرتباط بين الموقع وبيانات إنشاء التوقيع"، ويمكن أن تصب الجريمة كذلك في إطار مخالفة المدلول لعملية التصديق الإلكتروني الذي يعتبر آلية فعالة تصدر عن جهات مختصة تعمل على تسييج عملية التوقيع الإلكتروني ضد مخاطر القرصنة والاعتداء على النظام المعلوماتي للتوقيعات الإلكترونية، ويضمن إصدار التوقيع وفق الشروط والإجراءات المحددة لإنشاء آلية التوقيع المؤمن، ويتوجب توافر الإرادة الكاملة لدى الجاني عند إقباله على إصدار التصديق على نحو غير مشروع، وكذا العلم بعدم شرعية نشاطه وما يترتب عنه من نتائج سلبية وأضرار ترجع على صحة وأمان التوقيع الإلكتروني[2].

وترتيباً لما سبق, تعد كل السلوكات التي تصدر من الجاني تخالف مبدأ إصدار شهادة التصديق الإلكتروني والمساس بمصداقية الشروط والإجراءات المحددة قانوناً والتي تعيق بسلامة وأمن المعاملات الإلكترونية عموماً.

2- المواجهة التشريعية لجريمة إصدار شهادة التصديق الإلكتروني بدون ترخيص:

واجه المشرع المصري بموجب قانون التوقيع الإلكتروني وفقاً لحكم المادة 23 الفقرة الأولى منها التي جرمت كل إصدار لشهادة التصديق الإلكتروني دون الحصول على ترخيص مسبق بمزاولة النشاط من الهيئة المختصة بذلك.

وهو نفس موقف المشرع التونسي الذي الذي أقر من خلال الفصل 46 من قانون التجارة والمبادلات الإلكترونية حماية خاصة ضد أي سلوك يهدف منه ممارسة نشاط مزود خدمات المصادقة الإلكترونية بدون

1 سند صالح، المرجع السابق، ص 96-97.

2 جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، المرجع السابق، ص 134.

الحصول على ترخيص مسبق طبقاً للفصل 11 من ذات القانون, ويعاقب عليها بالحبس لمدة تتروح بين شهرين وثلاث (3) سنوات, وبغرامة تتروح بين ألف دينار و10 آلاف دينار.

وأما عن المشرع الأردني فقد أورد بالقانون رقم 5 لسنة 2015 المتعلق بالمعاملات الإلكترونية نص المادة 26 منه الذي ينص على معاقبة كل من يمارس نشاط جهات التوثيق الإلكتروني داخل المملكة دون الحصول على ترخيص أو اعتماد وفقاً لأحكام هذا القانون، ويعاقب عليها بغرامة لا تقل عن 50 ألف دينار ولا تزيد على 100 ألف دينار.

وأما عن المشرع السعودي فمن خلال الفصل التاسع من نظام المعاملات الإلكترونية المتعلق بالمخالفات والعقوبات، وبالتحديد في نص الفقرة الأولى من المادة 23 منه ضمن حكم يجرم ممارسة نشاط مقدم خدمات التصديق دون الحصول على ترخيص من الهيئة، وعاقب عليها بغرامة لا تزيد عن خمسة (5) ملايين ريال، أو بالسجن مدة لا تزيد عن خمسة (5) سنوات أو بالعقوبتين معاً، ويجوز الحكم بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب الجريمة.

وأما عن المشرع الجزائري فعاقب كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو يستأنف أو يواصل نشاط المصادقة بالرغم من سحب الترخيص بالحبس من (1) سنة إلى (3) سنوات وبغرامة من 200 ألف دينار إلى 2 ملاين دينار أو بإحدى هاتين العقوبتين، كما نص على مصادرة التجهيزات المستعملة لارتكاب الجريمة[1].

البند الخامس: جريمة تزوير التوقيع الإلكترونـــــي.

تمثل جريمة تزوير التوقيع الإلكتروني أهم صور الجرائم الواقعة على منظومة التوقيع الإلكتروني باعتبارها تشكل تهديداً كبيراً على نمو ومستوى المعاملات الإلكترونية من خلال إضعاف ثقة مستخدمي مجال التجارة والمبادلات الإلكترونية، الأمر الذي يفرض ضرورة إيجاد منظومة حماية كافية تعول على تنظيم الحماية الجزائية ضد جريمة التزوير بضبط التزامات كل الأطراف الفاعلة في هذه المنظومة من مزودي ومالكي التوقيع والوسطاء في العملية, من أجل كفالة أكبر قدر من الثقة الكافية في إبرام كافة المعاملات الإلكترونية عبر الانترنت ووسطاء التكنولوجيا الحديثة، دون أدنى خوف من أي عمليات تزوير للتوقيعات الإلكترونية، وهنا يجدر بيان البناء القانوني لجريمة تزوير التوقيع الإلكتروني ورصد المواجهة التشريعية لهذه الجريمة على مستوى التشريعات المقارنة.

1 المادة 72 من القانون 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

أولاً: البناء القانونـــي لجريمة تزوير التوقيع الإلكتروني.

بالرجوع إلى مفهوم التزوير المعلوماتي المشار إليه سابقاً فهو تغيير الحقيقة في محرر إلكتروني بإحدى الطرق التي حددها القانون تغييراً من شأنه أن يرتب ضرراً للغير أو بنية استعماله فيما أعد له. وبإسقاط مفهوم التزوير على التوقيع الإلكتروني نجد أن مفهوم تزوير التوقيع الإلكتروني يبنى على أساس إحداث تغيير أو تعديل على منظومة التوقيع الإلكتروني، يترتب عليه إحداث ضرر لمالك التوقيع وزعزعة الثقة في مجال التعامل الإلكتروني القائم على صحة التوقيع الإلكتروني.

وهنا تطرح أهمية بيان الأركان العامة لجريمة تزوير التوقيع الإلكتروني وبالنظر إلى خصوصية الجريمة مستقلة على جريمة التزوير الإلكتروني على أساس أن التوقيع الإلكتروني يمثل جزء لا يتجزء من المحرر الإلكتروني.

1- الركن المادي لجريمة تزوير التوقيع الإلكتروني:

يتمثل السلوك الإجرامي المكون لهذه الجريمة في قيام الجاني بتغيير حقيقة التوقيع الإلكتروني بإحدى الطرق التي يحددها القانون كالاصطناع أو التقليد أو التحوير أو بطريق آخر، ويترتب عن صدور النشاط الإجرامي لجريمة التزوير وفقاً لمفهومها السابق أن ينسب المزور التوقيع الإلكتروني إلى شخص لم يصدر عنه، وبالتالي هو اعتداء على رمز شخصية الموقع على المحرر الإلكتروني على اعتبار أن التوقيع الإلكتروني هو الدليل على امتلاك الموقع للتوقيع, وحجية على اتجاهه لتبني مضمون المحرر الإلكتروني الذي عبر عن بالتوقيع الإلكتروني[1].

وبخصوص إمكانية وقوع أساليب تزوير التوقيع الإلكتروني من تعديل أو حذف أو اصطناع أو تقليد فهو أمر متاح بالنظر إلى طبيعة المعاملات الإلكترونية التي تتم وفقاً لجهاز الحاسب الآلي وشبكة المعلومات التي تقوم أساساً على تداول بيانات ومعلومات إلكترونية، وهنا يمثل التوقيع الإلكتروني أحد نماذجها، وهنا تعتبر المعلومات الخاصة بالتوقيع الإلكتروني ذات قيمة في ترتب حق معين أو أثر قانوني يتم التأثير في مصداقيتها من خلال المساس بأحد الأساليب الموضحة سابقاً[2].

فوفقاً لما قضت به محكمة النقض المصرية:"جريمة التزوير تتحقق بمجرد تغيير الحقيقة بطريق الغش بالوسائل التي نص عليها القانون ولو لم يتحقق عنه ضرر يلحق شخصاً بعينه لأن هذا التغيير ينتج عنه

1 أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني (دراسة مقارنة)، دار النهضة العربية، الطبعة 1، القاهرة، سنة 2006، ص 116.

2 علي عبد القادر القهوجي، المرجع السابق، ص 176.

حتماً حصول ضرر بالمصلحة العامة لما يترتب عليه من عيب ينال من قيمته وحجيته"[1], وبالتالي يكفي فعل التغيير دون اشتراط حدوث ضرر ينتج عن هذا التزوير، وسيتم توضيح الأساليب التي يقوم عليها تزوير التوقيع الإلكتروني فيما يأتي:

أ- تغيير أو تحريف التوقيع الإلكترونـــي:

يعتبر التغيير أو التحريف الواقع على التوقيع الإلكتروني هو أحد أبرز الطرق التي يعتمدها الجاني لتحقيق جريمة التزوير؛ ذلك أن الحاسب الآلي حين يتلقى البيانات والمعلومات داخل نطاقه المعلوماتي يتم معالجتها آلياً، وهنا يمثل جهاز الحاسب الآلي معبر تلك البيانات بمساعدة التقنيات الحديثة, ويمكن إزاء ذلك تعرض التوقيع الإلكتروني لأي اعتداء, أو تزويده بكامل معطياته من خلال وضع بيانات غير حقيقية، بالإضافة إلى إمكانية وضع صورة ضوئية للتوقيع الإلكتروني ونقلها إلى جهاز الحاسب الآلي, واستغلالها لاحقاً بشكل غير مشروع[2].

ب/اصطناع أو إتلاف التوقيع الإلكترونـــي:

يمثل أسلوب اصطناع إنشاء لبيانات ووقائع غير موجودة؛ خلق معلومات ونسبها إلى شخص لا صلة له بها أو إلى أي سلطة لم يصدر عنها، وأما عن اصطناع التوقيع الإلكتروني فيقع من خلال إدخال الجاني للمعلومات والبيانات الخاصة إلى جهاز الحاسب الآلي ونسبها إلى شخص آخر أو جهة لا علاقة لها بها[3].

ولقد توسعت الأنظمة القانونية في مجال حماية المعاملات الإلكترونية وبالخصوص فيما يتعلق بالحماية الجنائية من جريمة التزوير التوقيع الإلكتروني، واعتبرت أن أفعال الإتلاف التي تمس بالتوقيع الإلكتروني سواء في الشكل الجزئي أو الكلي, وهذا من خلال محاولة لمحو أو طمس معالم التوقيع بطريقة لا يمكن معها تمييز ما كان يدل عليه هذا التوقيع، وهو ما يدخل في إطار المساس بحقيقة التوقيعات الإلكترونية والتأثير على حجيتها في إثبات المعاملات الإلكترونية[4].

---

1 هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، دراسة مقدمة إلى مؤتمر كلية الشريعة والقانون بجامعة الإمارات العربية "القانون والكمبيوتر والانترنت"، الفترة ما بين 1-3 ماي 2000، الإمارات، ص 583.

2 عبد الفتاح حجازي، المرجع السابق، ص 243.

3 خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، دراسة تحليلية مقارنة، رسالة ماجيستر، جامعة نايف العربية للعلوم الأمنية، السعودية، سنة 2009، ص 183.

4 حفصي عباس، جرائم التزوير الإلكترونية، أطروحة دكتوراه في العلوم الإسلامية (شريعة وقانون)، جامعة وهران "أحمد بن بلة"، الموسم الجامعي 2014-2015، ص 120.

2- الركن المعنوي لجريمة تزوير التوقيع الإلكتروني:

يعتبر تزوير التوقيع الإلكتروني من أهم المخاطر التي تؤثر على إنشاء وفاعلية المعاملات الإلكترونية بما يشكله لزعزعة ثقة المتعاملين، وبهذا صنفت هذه الجريمة من الجرائم العمدية التي يتخذ ركنها المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة، بحيث يجب توافر علم الجاني بقيامه لتزوير توقيع إلكتروني مملوك للغير وذلك بتغيير حقيقته بطريقة من الطرق المحددة قانوناً، واتجاه إرادته لارتكاب هذا الجرم دون اشتراط تطلب قصد خاص، وسواء تم استعمال هذا التوقيع فيما أعد له أم دون ذلك[1].

ثانياً: المواجهة التشريعية لجريمة تزوير التوقيع الإلكترونـي.

عمل المشرع المصري على تجريم فعل التزوير الواقع على التوقيع الإلكتروني من خلال نصوص قانون التجارة الإلكترونية وفقاً لنص المادة 28 منه والتي عاقبت بالحبس مع الشغل كل من زور أو قلد محرراً أو توقيعاً إلكترونياً أو شهادة اعتماد لتوقيع إلكتروني، كما جرم قانون التوقيع الإلكتروني المصري في الفقرة الثانية من المادة 23 منه كل عملية تزوير للتوقيعات او الوسائط أو المحررات الإلكترونية بطريق الإصطناع أو التعديل أو التحوير أو بأي أسلوب آخر, وعاقب عليها بالحبس والغرامة التي لا تقل عن 10 آلاف جنيه ولا تجاوز 100 ألف جنيه أو بإحدى هاتين العقوبتين[2].

وتصدى المشرع التونسي لجريمة تزوير التوقيع الإلكتروني من خلال حكم المادة 47 من قانون التجارة الإلكترونية سواء وقعت من قبل صاحب التوقيع أو شخص آخر، وهذا بتجريم كل تصريح عمدي لمعطيات خاطئة لمزود خدمات التصديق الإلكتروني ولكافة الأطراف المقدم لها التوقيع الإلكتروني في إطار التعامل الإلكتروني، وعاقب على ذلك بالسجن لمدة تتراوح بين ستة (6) أشهر وسنتين (2) وبغرامة تتراوح بين 1000 و 10 آلاف دينار أو بإحدى هاتين العقوبتين، كما عاقب بمقتضى نص المادة 48 من ذات القانون بنفس العقوبة السابقة كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء الغير[3].

واعتمد المشرع الإماراتي تجريم عملية تزوير التوقيع الإلكتروني وفقاً لتجريم أساليب تصب في إطار وقوع فعل التزوير، والأمر يتضح من خلال نص المادة 29 التي جرمت كل عمليات إنشاء أو نشر شهادة أو بيانات غير صحيحة لأي غرض احتيالي أو أي غرض غير مشروع وهنا يدخل مفهوم تزوير التوقيع

1 محمود ابراهيم غازي، المرجع السابق، ص 346.

2 هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، المرجع السابق، ص 580.

3 عبد الفتاح حجازي، التوقيع الإلكتروني في النظم المقارنة، دار الفكر الجامعي، مصر، سنة 2010، ص 19.

الإلكتروني، ويعاقب على هذه الأفعال بالحبس والغرامة التي لا تتجاوز 250 ألف درهم أو بإحدى هاتين العقوبتين.

وجاء كذلك في نص المادة 30 من قانون المعاملات الإلكترونية تجريم التصريح العمدي للبيانات غير الصحيحة لمزودي خدمات التصديق بغرض طلب أو استصدار أو إلغاء شهادة التصديق الإلكتروني، وهي الأفعال التي تؤدي بالنتيجة إلى ثبوت التوقيعات الإلكترونية المزورة والمساعدة في استعمالها بشكل غير مشروع، وعاقب عليها المشرع بالحبس لمدة لا تزيد عن 6 أشهر وبغرامة لا تجاوز 100 ألف درهم أو بإحدى هاتين العقوبتين.

وأورد المشرع السعودي حكم صريح بتجريم تزوير التوقيع الإلكتروني أو شهادة تصديق رقمية أو استعمال أي من ذلك مع العلم بتزويرها، وجاء نفس القانون بتجريم جملة من السلوكات التي تصب في إطار تسهيل وقوع جريمة تزوير التوقيع الإلكتروني منها:

- إفشاء مقدم خدمات التصديق الإلكتروني للمعلومات التي يطلع عليها بحكم عمله دون إذن صاحب الشهادة كتابياً أو إلكترونياً.
- إنشاء شهادة رقمية أو توقيع إلكتروني أو نشرهما أو استعمالهما لغرض غير مشروع.
- تقديم معلومات خاطئة عمداً إلى مقدم خدمات التصديق أو تقديم معلومات خاطئة عمدا على التوقيع الإلكتروني إلى أي من الأطراف الذين وثقوا بالتوقيع بموجب النظام[1].

وعاقب المشرع على الأفعال السابقة بالغرامة التي لاتزيد عن خمسة (5) ملايين ريال أو بالسجن لمدة لا تزيد عن خمسة (5) سنوات أو بالعقوبتين مجتمعتين مع النص على عقوبة تكميلية تتمثل في مصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب الجريمة.[2]

أما المشرع الجزائري فلم يعتمد نص صريح لتجريم تزوير التوقيع الإلكتروني، إلا أنه وبالرجوع لأحكام القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين يضمن جملة من السلوكات التي تمثل أفعال تمهيدية أو مسهلة لوقوع التزوير، وخاصة عند صدورها ممن لهم علاقة بحماية التوقيع الإلكتروني كمؤدي خدمات التصديق فنجده في المادة 66 من القانون 15-04 تعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاثة (3) سنوات

1 المادة 23 من نظام المعاملات الإلكترونية السعودي.

2 المادة 24 من نظام المعاملات الإلكترونية السعودي.

وبغرامة من 20 ألف إلى 200 ألف دينار كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة.

وكذا تجريم كل عمليات الإستعمال أو إفشاء بيانات إنشاء توقيع إلكتروني خاص بالغير ومعاقبة مرتكبها بالحبس من (3) أشهر إلى (3) سنوات وبغرامة من (1) مليون إلى (5) ملايين دينار أو بإحدى هاتين العقوبتين، وحظر جملة من الأفعال بالنسبة لمؤدي خدمات التصديق الإلكتروني بحيث ألزم كل مؤدي خدمات التصديق بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة في إطار ذلك, وفي حالة مخالفة هذا الالتزام يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين وبغرامة من مائتي (200) ألف دينار إلى مليون (1) دينار جزائري.[1]

كما يلزم القانون 15-04 في نص المادة 43 بجمع البيانات الشخصية الضرورية فقط لمنح وحفظ شهادة التصديق الإلكتروني وحظر استعمالها لأغراض أخرى، والتي قد يدخل فيها تزوير التوقيع، ويعاقب على مخالفة هذا الالتزام في المادة 71 بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من (200) ألف إلى اثنين (2) مليون دينار جزائري، أو بإحدى هاتين العقوبتين.

المطلب الثاني: الحمايـــة الجنائية لنظام الدفع الإلكتروني.

يشهد العصر الحالي تطورات هائلة في مجال المعاملات الإلكترونية مست بشكل مباشر مجال المؤسسات المصرفية والمالية والتجارية التي أضحت تعتمد على التقنيات الحديثة في مجال تداول المال، لما لهذه الأخيرة من تأثير في سرعة إنجاز التعاملات المالية واختصار في بذل المجهود، وبهذا ظهرت وسائل الدفع الإلكتروني وتعددت وفقاً للمتطلبات المرجوة منها في هذا المجال، ومن تلك الوسائل بطاقات السحب المصرفي وبطاقات الائتمان, وغيرها من البطاقات الذكية التي شكلت انتشاراً واسعاً وأضحت تمثل أهم الوسائل المعتمدة في التعامل المالي الإلكتروني, التي تمكن المتعاملين من السرعة في شراء السلع والخدمات مع توافر ائتمان قصير المدى, وهي الخصائص التي تتماشى وصيغة الحياة العصرية للأفراد.

إلا أن هذا التميز في وسائل الدفع الإلكتروني يصاحبه عدة مخاطر تتمثل في جملة من الاعتداءات الواقعة على تلك الوسائل فتؤثر على النظام الاقتصادي بشكل عام والنظام المصرفي بشكل خاص، ومن هنا يجدر إيجاد نظام قانوني محكم يجرم كل أشكال الاعتداءات، ويضع حداً لكل الأفعال التي تضعف من ثقة التعامل في تلك الوسائل من تزوير في بطاقات الدفع وسرقتها وإساءة استخدامها من قبل الحامل أو الغير.

1 المادة 70 من القانون رقم 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين الجزائري السالف الذكر.

وتأسيساً على ما سبق, وانطلاقاً من الأساس الذي نشأ منه نظام الدفع الإلكتروني وفكرة الحماية الجنائية للمتعامل في المجال الإلكتروني، تفرض الدراسة البحث في الإطار المفاهيمي للدفع الإلكتروني (الفرع الأول)، ثم دراسة الجرائم التي تمس نظام الدفع الإلكتروني والعقوبات المقررة لها تشريعياً (الفرع الثاني).

الفرع الأول: الإطار المفاهيمي للدفع الإلكترونـــي.

يلتزم المستهلك بأداء الثمن؛ وهو المقابل للحصول على السلعة أو الخدمة محل التعاقد، وإذا كان دفع الثمن في التعاقد التقليدي يتم بإحدى وسائل الوفاء المعروفة إما نقداً، أو بشيك، أو حوالة، أو غيرها من وسائل الدفع التجارية، فإن الوفاء بالثمن في عقد التجارة الإلكتروني له صور عديدة أيضاً، فقد يتم باستخدام بطاقات الدفع الإلكترونية, أو التحويل المصرفي, أو الأوراق التجارية الإلكترونية[1]، ويثير الدفع الإلكتروني بعض التساؤلات عن مفهومه، استوجبت الإجابة عنها دراسة مفهوم الدفع الإلكتروني (البند الأول)، فالطبيعة القانونية للدفع الإلكترونـي (البند الثاني), وصولاً لخصائص الدفع الإلكترونـــي (البند الثالث).

البند الأول: مضمون الدفع الإلكترونـــي.

إذا كان ظهور المعاملات الإلكترونية وانتشارها يرجع إلى التقدم العلمي في وسائل الاتصال والمعلومات، وبصفة خاصة عبر شبكة الانترنت، حيث يتم الدفع من خلال قنوات إتصال إلكترونية، ولا جدال في أن استخدام نظام الدفع الإلكتروني يؤدي إلى سرعة وسهولة تسوية الوفاء، وتقليص الحاجة إلى وسائل الدفع الكلاسيكية, الأمر الذي يساعد بشكل خاص على التوسع في مجال التبادل التجاري الإلكتروني[2].

وفي إطار تحديد مفهوم الدفع الإلكتروني, أصدرت لجنة الإتحاد الأوروبي في 08 ديسمبر 1987 توصية تسمى بالقواعد الأوروبية للتعامل السليم في مجال الدفع الإلكتروني، ووفقاً لهذه التوصية يقصد بالدفع الإلكتروني كل عملية وفاء تتم بواسطة بطاقة ذات أشرطة ممغنطة، أو تلك التي تحتوي على دوائر إلكترونية لدى جميع شبكات الدفع المزودة بآلات الدفع الحديثة (T.P.V) (T.P.E)[3].

---

1 كوثر سعيد عدنان، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الاسكندرية، سنة 2012، ص 550.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 106.

3 يقصد بـ: T.P.V اختصار لكلمة Terminal de Paiement de vente وكلمة T.P.E اختصار لكلمة Terminal de Paiement électronique وهي أجهزة آلية تستطيع فحص البطاقة من حيث صلاحيتها أو عدم وجودها على قائمة الاعتراضات

ويلاحظ على التعريف أنه ركز على الدفع الإلكتروني باستخدام البطاقات بالرغم من وجود طرق أخرى للدفع الإلكتروني، ربما كان سبب ذلك يرجع إلى أن هذه التوصية صدرت سنة 1987 أي قبل ظهور وسائل الدفع الأخرى.

من جانب آخر نجد أن القانون النموذجي للتحويلات الدولية للأموال الصادر في عام 1992 عن لجنة الأمم المتحدة "الأونسيترال"، يعرف الدفع الإلكتروني تحت مسمى التحويل المصرفي بأنه:"مجموعة العمليات التي تبدأ بأمر الدفع الصادر عن الآمر بهدف وضع قيمة الحوالة تحت تصرف المستفيد"[1].

أما مشروع قانون التجارة الإلكترونية المصري فقد عرف الدفع الإلكتروني بأنه:"وفاء بالتزام نقدي بوسيلة إلكترونية كالشيكات والكمبيالات الإلكترونية وبطاقات الدفع الممغنطة وغيرها"[2].

ويلاحظ أن الوسائل التي حددها هذا التعريف للدفع الإلكتروني واردة على سبيل المثال لا الحصر، بحيث يتسع التعريف ليشمل أية وسائل أخرى تستحدث للدفع الإلكتروني، ويعيب النص أنه لم يوضح بأن الوفاء يكون نتيجة التزام بالدفع لعملية تجارية تتم عن بعد.

أما عن التعريف الفقهي، فعرف البعض من الفقه[3] الدفع الإلكتروني بأنه تصرف قانوني يكون الهدف من ورائه تسوية دين ثابت في ذمة شخص ما لصالح شخص آخر، كنتيجة لوجود معاملة تجارية تجري بينهما عبر شبكة الانترنت، وذلك باستخدام وسائل دفع تتوافق وحاجات التجارة الإلكترونية.

كما ذهب البعض[4] إلى تعريفه بأنه: "جملة المعاملات المصرفية الإلكترونية التي تجرى في إطار التجارة الإلكترونية عن طريق البنوك باستخدام جهاز الحاسوب الآلي".

(حالتي السرقة أو الضياع) بطريقة آلي. **مشار إليه لدى:** نبيل محمد أحمد صبيح، بعض الجوانب القانونية لبطاقات الوفاء والائتمان المصرفية، مجلة الحقوق، مجلس النشر العلمي، جامعة الكويت، مارس 2003، ص 220.

1 واقد يوسف، النظام القانوني للدفع الإلكتروني، رسالة لنيل شهادة الماجيستر(القانون العام)، كلية الحقوق، جامعة مولود معمري بتيزي وزو، الموسم الجامعي لسنة 2011، ص 19.

2 كوثر سعيد عدنان، المرجع سابق، ص 551.

3 سامي عبد الباقي أبو صالح، الوفاء الإلكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 22.

4 نبيل محمد أحمد صبيح، حماية المستهلك في التعاملات الإلكترونية، مجلة الحقوق، مجلس النشر العلمي، جامعة الكويت، جوان 2008، ص 230.

كما اتجه فريق آخر[1] إلى تعريف الدفع الإلكتروني بأنه:"نظام الدفع الآلي عبر الشبكة المعلوماتية، وهو نتيجة إلزامية للتطور التكنولوجي على إثر الاتساع الانفجاري لشبكة الانترنت، وفي إطار الوفاء بمبلغ من النقود". وبهذا قسموا تعريف الدفع الإلكتروني إلى معنيين: واسع وضيق .

ويقصد بالدفع الإلكتروني بالمعنى الواسع كل عملية دفع لمبلغ من النقود تتم بأسلوب غير مادي لا يعتمد على دعامات ورقية، بل الرجوع إلى آليات إلكترونية، أما الدفع الإلكتروني بمعناه الضيق؛ فينحصر فقط في عمليات الوفاء التي تتم دون وجود اتصال مباشر بين الأشخاص الطبيعيين[2].

أما عن موقف التشريع الجزائري من تعريف نظام الدفع الإلكتروني، فيعتبر الأمر 03-11 المعدل والمتمم الموافق عليه بموجب القانون رقم 03-15 المتعلق بالنقد والقرض أول قانون جزائري تضمن التعامل الإلكتروني الحديث في القطاع المصرفي، ويلاحظ ذلك من خلال نص المادة 69 التي نصت على مايلي:"تعتبر وسائل الدفع كل الأدوات التي تمكن الشخص من تحويل أموال مهما يكون السند أو الأسلوب التقني المستعمل". ويتبين من خلال النص نية المشرع الانتقال من وسائل الدفع التقليدية إلى وسائل حديثة إلكترونية[3].

وبعد صدور الأمر 05-06 المؤرخ بتاريخ أوت 2005 المتعلق بمكافحة التهريب وبالضبط في نص المادة الثالثة (03) منه استعمل المشرع مصطلح "وسائل الدفع الإلكتروني"، حيث اعتبرها من بين التدابير والإجراءات الوقائية لمكافحة التهريب[4].

وبذلك نلاحظ أن المشرع قد انتقل من عبارة "مهما يكن السند أو الأسلوب التقني المستعمل" الواردة في نص المادة 69 من الأمر 03-11 المتعلق بالنقد والقرض، إلى مصطلح أكثر دقة والمتمثل في "وسائل الدفع الإلكتروني" المذكور في نص المادة الثالثة من الأمر 05-06 المتعلق بمكافحة التهريب.

---

1 سامي عبد الباقي أبو صالح، المرجع السابق، ص 32.

2 ناجي الزهراء، التجربة التشريعية الجزائرية في تنظيم المعاملات الإلكترونية المدنية والتجارية، المؤتمر العلمي المغاربي حول المعلوماتية والقانون، أكاديمية الدراسات العليا طرابلس، 28-29 أكتوبر سنة 2009 ، ص 15.

3 الأمر رقم 03-11 المؤرخ في 27 جمادى الثانية 1424 الموافق 26 أوت 2003 المتعلق بالنقد والقرض, ج رج عدد 52، السنة 40، ص 3-22, الموافق عليه بالقانون 03-15 المؤرخ في 29 شعبان 1424 الموافق 25 أكتوبر 2003, ج رج العدد 64، السنة 40، ص 05, المعدل والمتمم.

4 الأمر 05-06 المؤرخ في 18 رجب 1426 الموافق 23 أوت 2005 المتعلق بمكافحة التهريب, ج رج العدد 59، السنة 42، ص3-8, الموافق عليه بالقانون رقم 05-17 المؤرخ في 29 ذي القعدة 1426 الموافق 31 ديسمبر 2005، ج رج العدد 02، السنة 43، ص 03.

ونجد المشرع الجزائري قد استحدث أخيراً مفهوم الدفع الإلكتروني بشكل خاص في مجال التجارة الإلكترونية من خلال القانون الجديد رقم 18-05 المتعلق بالتجارة الإلكترونية[1], وتحديداً في نص المادة السادسة (06) منه والتي عرفت وسيلة الدفع الإلكتروني بأنها كل وسيلة دفع مرخص بها طبقاً للتشريع المعمول به, تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة إلكترونية.

وبهذا ونظراً لطبيعة المعاملات التجارية الإلكترونية، والتي تتم بانعدام التقابل المادي لأطراف التعاقد، وتتسم أيضاً بالسرعة مع استخدام التقنيات التكنولوجية الحديثة، بالإضافة إلى تراجع دور الوسائل التقليدية التي لم تعد صالحة لتسهيل التعامل في هذا المجال الإلكتروني، فكان لا بد من تطور وسائل الدفع لتتناسب وطبيعة تلك المعاملات, فتطورت الأوراق التجارية لتصبح عبارة عن أوراق تجارية إلكترونية, كما استحدثت وسائل دفع حديثة كالنقود الإلكترونية والتحويل الإلكتروني[2].

البند الثاني: الطبيعة القانونية للدفع الإلكترونـــي.

يعتبر الدفع الإلكتروني أسلوب مستحدث من أساليب الوفاء, لذلك يثور التساؤل حول طبيعته القانونية ؟

وللإجابة عن ذلك, اتجه رأي[3] إلى اعتبار الدفع الإلكتروني عمل مختلط، إذ أن الوفاء هو اتفاق بين طرفين على تسوية دين معين، فهو تصرف قانوني يجب أن تتوافر فيه الشروط القانونية، كما أنه يهتم بكيفية التنفيذ المادي للالتزام بالوفاء.

وهناك اتجاه آخر[4]، فرق في بيان الطبيعة القانونية للوفاء الإلكتروني بين وسائل الدفع، فالبنسبة للدفع الإلكتروني باستخدام بطاقات الائتمان فاعتبروه أنه عملية مصرفية حديثة تتضمن أداة دفع ووسيلة ائتمان في ذات الوقت، ولها طابع مميز وخصائص معينة تفرضها هذه الطبيعة الخاصة، أما الدفع الإلكتروني من خلال شبكة الانترنت باستخدام النقود الإلكترونية فيذهب هذا الرأي إلى القول بأن هذه النقود لايقتصر

1 القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي 2018 يتعلق بالتجارة الإلكترونية, ج ر ج عدد 28، السنة 55، ص 4, المؤرخة في 30 شعبان 1439 الموافق 16ماي 2018.

2 محمد حسين منصور ، أحكام البيع التقليدية والإلكترونية والدولية وحماية المستهلك، دار الفكر الجامعي، الاسكندرية، سنة 2006، ص 408.

3 خالد عبد التواب عبد الحميد أحمد، نظام بطاقات الدفع الإلكتروني من الناحية القانونية، رسالة دكتوراه، كلية حقوق حلوان، مصر، سنة 2005-2006، ص 339.

4 سامي عبد الباقي أبو صالح، المرجع السابق، ص 15.

قبولها إلا على بعض التجار، بالإضافة إلى أنه يتوقف إصدارها على حصول مصدرها على مقابل سابق من المستهلك وهو ما لا يتصور في النقود العادية.

والرأي الراجح فقهاً[1]، يذهب للقول بأن الدفع الإلكتروني تصرفاً قانونياً، وهو يقوم على توافر عنصريين؛ عنصر مادي يتمثل في واقعة تسليم مبلغ من النقود، والعنصر الإرادي وهو توافر الإرادة في تسليم النقود بقصد البراءة من التزام قائم.

وعلى هذا يتطلب أن يتوافر في الدفع الإلكتروني شروط التصرف القانوني، بأن يكون صادراً عن إرادة حرة وموجهة نحو إحداث أثر قانوني معين وهو الوفاء، وأن يكون صادراً من شخص ذي أهلية، وأن تتوافر شرعية محل وسبب الوفاء[2].

البند الثالث: خصائص الدفع الإلكترونـــي.

يعتبر الدفع الإلكتروني وسيلة لتسوية المعاملات التي تتم عن بعد، على اعتبار أن المعاملات الإلكترونية تتم في بيئة غير مادية تغيب فيه الدعائم الورقية، ونظراً لدولية شبكة الانترنت، فوسائل الدفع الإلكتروني تأخذ الطبيعة الدولية أيضاً، كذا أن طبيعة التعامل التجاري الإلكتروني تطبع خصوصية أدوات الدفع الخاصة بها من حيث الجهة التي تقوم بخدمة الدفع الإلكتروني، وكذا من حيث توفير وسائل الأمان الفنية[3].

1- الدفع الإلكترونـي ذا طبيعة دوليـــة:

تضفي صفة الدولية على العقد الذي يتم عبر شبكة الانترنت، الذي يفترض تباعد أطرافه، بحيث يغيب فيه الحضور المادي على مائدة المفاوضات؛ أو ما يسمى بمجلس العقد، فوسيلة الدفع الإلكتروني تستجيب لهذه السمة، حيث أنها تكون وسيلة دفع لتسوية معاملات دولية التي تتم عن بعد، فيصدر الدفع من خلال إعطاء أمر يتم وفقاً لمعطيات إلكترونية تسمح بالاتصال المباشر بين أطراف العقد[4]، ويتميز نظام الدفع بأنه يدمج تنوعاً غنياً ووفيراً للتسهيلات الوظيفية، وذلك في أنظمة الترخيص والتفويض مثل تبادل

1 خالد عبد التواب عبد الحميد أحمد، المرجع السابق، ص 341.

2 إسماعيل قطاف، العقود الإلكترونية وحماية المستهلك، مذكرة لنيل شهادة الماجيستر فرع "المسؤولية المهنية"، جامعة الجزائر، الموسم الجامعي 2005-2006، ص 83.

3 فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة للنشر، مصر، سنة 2002، ص 125.

4 فاروق محمد أحمد الأباصيري، المرجع سابق، ص127.

الشيكات وتصفية الحسابات بين مختلف البنوك، وأنظمة التسديد والتسوية دون الاصطدام بالحاجز الجغرافي[1].

2- تخصص الجهة القائمة بالدفع الإلكترونـــي:

تفرض الطبيعة الخاصة لنظام الدفع الإلكتروني تواجد ارتباط بمؤسسات مصرفية أو مالية مسبقاً من قبل أطراف التعاقد لتتيح عملية الدفع من خلالها، وبالتالي توفر أجهزة تقوم بإدارة عمليات الوفاء عن بعد، ومن شأنها أن توفر الثقة للمتعاملين بهذه الوسيلة، ويرتبط الدور بصفة أصلية بالبنوك وغيرها من المنشآت التي تعمل لهذا الغرض، حيث أن إدارة وسائل الدفع في البلاد الأوروبية عدا فرنسا غير مقتصر على البنوك بغرض تسهيل تبادل وتقديم الخدمة بين البلدان الأوروبية[2], وهو ما توخاه المشرع الجزائري وفقا لنص الفقرة الثانية من المادة 27 من القانون 18-05 المتعلق بالتجارة الإلكترونية[3].

3- توافر الأمان في وسائل الدفع الإلكترونـــي.

يتم الدفع من خلال فضاء معلوماتي مفتوح، وبهذا يبقى خطر التعامل بهذه الوسائل قائم بشكل كبير وخاصة باستعمال شبكة الانترنت وغيرها، باعتبارها فضاء يستقبل جميع الأفراد من مختلف دول العالم باختلاف أهدافهم ونواياهم، وبهذا يستلزم هذا النظام أن يكون مصحوباً بوسائل أمان فنية من شأنها منح قدرا من الحماية للمستهلك بتوفير برامج تساعد على تسييج طرفي المعاملة التجارية الإلكترونية ووضع برامج خاصة لتحقيق هذا الغرض، كما يتم وضع أرشيف للمبالغ التي يتم السحب عليها بحيث استخدام هذه الطريقة يكون من السهل الرجوع إليها[4].

---

1 محمد سعيد أحمد إسماعيل، الحماية القانونية لمعاملات التجارة الإلكترونية (دراسة مقارنة)، منشورات الحلبي الحقوقية، ط1، بيروت، سنة 2009، ص 302.

2 سامي عبد الباقي أبو صالح، المرجع السابق، ص27، **انظر أيــضاً**: فاروق محمد الأباصيري، نفس المرجع السابق، ص 100.

3 المادة 2/27 من القانون 18-05 المتعلق بالتجارة الإلكترونية: "عندما يكون الدفع إلكترونياً، فإنه يتم من خلال منصات دفع مخصصة لهذا الغرض، منشأة ومستغلة حصرياً من طرف البنوك المعتمدة من قبل بنك الجزائر وبريد الجزائر وموصولة بأي نوع من أنواع محطات الدفع الإلكتروني عبر شبكة المتعامل العمومي للمواصلات السلكية واللاسلكية. ويتم الدفع في المعاملات التجارية العابرة للحدود حصرياً عن بعد، عبر الاتصالات الإلكترونية".كما نصت المادة 28 من نفس القانون على أنه: "يجب أن يكون وصل موقع الانترنت الخاص بالمورد الإلكتروني بمنصة الدفع الإلكتروني مؤمناً بواسطة نظام تصديق إلكتروني".

4 وهو ما نصت عليه المادة 28 من القانون 18-05 المتعلق بالتجارة الإلكترونية على أنه: "يجب أن يكون وصل موقع الانترنت الخاص بالمورد الإلكتروني بمنصة الدفع الإلكتروني مؤمناً بواسطة نظام تصديق إلكتروني". وكذا نص المادة 29 من نفس القانون: "تخضع منصات

الفرع الثاني: وسائل الدفع الإلكتروني.

نتج عن التطور الذي جاءت به التجارة الإلكترونية وسائل دفع حديثة يتم بموجبها تنفيذ الالتزامات المترتبة عن العلاقات التجارية القائمة عبر شبكة الانترنت، والتي لاقت تطبيقاً عملياً واسعاً، ويمكن في هذا الصدد التمييز بين أنواع تقليدية كانت معروفة من قبل، وتم تطويرها وتطويعها إلكترونياً أهمها السفتجة الإلكترونية والشيك الإلكتروني (أولاً)، كما ظهرت صور أخرى مستحدثة لم تكن معروفة من قبل مثل النقود الإلكترونية، بطاقات الدفع الإلكترونية، التحويل الإلكتروني (ثانياً).

أولاً: وسائل الدفع الإلكترونية الـمطورة.

من خلال النقاط الموالية، ستقتصر الدراسة على أهم الوسائل التقليدية للدفع في مجال التعامل التجاري، والتي تم معالجتها إلكترونياً للتحول من الصورة العادية لها كدعائم ورقية إلى وسائل دفع إلكترونية[1]، وبهذا سيتم دراسة كل من السفتجة الإلكترونية (أولاً)، وكذا الشيك الإلكتروني (ثانياً).

1- السفتجة الإلكترونية :

تعرف السفتجة الإلكترونية بأنها محرر شكلي ثلاثي الأطراف معالج إلكترونياً بصورة كلية أو جزئية، يتضمن أمراً من شخص يسمى الساحب إلى شخص آخر يسمى المسحوب عليه بأن يدفع مبلغاً من النقود لشخص ثالث يسمى المستفيد في تاريخ معين[2].

وتنقسم السفتجة الإلكترونية حسب بعض الفقه[3] إلى نوعين:

أ) **السفتجة الورقية المعالجة إلكترونياً:** وهي السفتجة الورقية العادية التي يقوم الساحب بتحريرها ويقوم بالتوقيع عليها وتقديمها إلى بنكه بتظهيرها، ليقوم هذا الأخير بتحويل البيانات الواردة في السفتجة العادية إلى دعامة ممغنطة، والذي يقوم بتحصيل قيمتها من خلال المقاصة مع بنك المسحوب عليه.

الدفع الإلكتروني المنشأة والمستغلة طبقاً لنص المادة 27 أعلاه، لرقابة بنك الجزائر لضمان استجابتها لمتطلبات التشغيل البيئي، وسرية البيانات وسلامتها وأمن تبادلها".

1 محمد عمر ذوابة، أكرم ياملكي، عقد التحويل المصرفي الإلكتروني (دراسة قانونية مقارنة)، دار الثقافة للنشر والتوزيع، الأردن، سنة 2006، ص 09.

2 مصطفى كمال طه, ووائل أنور بندق، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، سنة 2005، ص 345.

3 مصطفى كمال طه, ووائل أنور بندق، نفس المرجع، ص 55.

ب) **السفتجة الإلكترونية الممغنطة:** يحرر هذا النوع من السفتجة من قبل الساحب على دعامة ممغنطة يتسلمها الساحب من بنكه، ويدون على تلك الدعامة بيانات السفتجة، ويسلمها إلى بنك المستفيد الذي يتولى تحصيل قيمتها عن طريق بنك المسحوب عليه[1].

إن مسار نظام الدفع عن طريق السفتجة الإلكترونية يمتاز بالدقة مقارنة بنظام استخدام السفتجة التقليدية التي تعتمد على الدعامة الورقية، كما أنه يختلف عنه من حيث تكوين الأثر، وبهذا فإن تقديم السفتجة الإلكترونية عمل تقوم به مباشرة مؤسسة الساحب التي تستخدم نظامها الرقمي الخاص، ويكفي أن يكون لدى الساحب الكلمات السرية الرقمية ما بين البنوك، وهي معلومات تقدم من البنك الذي يتعامل معه الساحب[2].

2- الشيك الإلكترونـــي:

يعرف الشيك الإلكتروني بأنه محرر إلكتروني موثق ومؤمن يحرره مصدر الشيك لصالح مستلم الشيك (حامله)، ليعتمده ويقدمه للبنك الذي يعمل عبر الانترنت[3]، ليقوم البنك أولاً بتحويل قيمة الشيك المالية لحساب حامل الشيك، والشيك الإلكتروني عبارة عن وثيقة تحتوي على البيانات التالية: رقم الشيك، واسم الساحب، ورقم حسابه، واسم المستفيد، ورقم حسابه، واسم البنك، وقيمة الشيك التي ستدفع، ووحدة العملة، والتوقيع الإلكتروني[4].

تعتمد أنظمة الشيك الإلكتروني على وجود وسيط يقوم بعملية التحقق والدفع الإلكتروني للشيك، وغالباً مايكون هذا الوسيط أحد البنوك الإلكترونية[5] التي تعمل من خلال شبكة الانترنت، ومع ذلك فإن

---

1 واقد يوسف، المرجع السابق، ص 62.

2 JEANTIN MICHEL, & PAUL CANNU, Droit Commercial, instruments de paiement et crédit entreprise en difficulté, 5 éme éd, Dalloz, Paris, 1999, p 277.

3 لذلك يرى بعض الفقه أنه يخضع للقواعد نفسها التي تحكم الشيك التقليدي، كما يخضع لأحكام قانون الصرف في المسائل التي لا يوجد نص يحكمها، أنظر نبيل محمد أحمد صبيح، حماية المستهلك في التعاملات الإلكترونية، المرجع السابق، ص 244.

4 أحمد سفر، أنظمة الدفع الإلكترونية، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، سنة 2008، ص 44.

5 تعرف البنوك الإلكترونية بأنها مؤسسات مالية ضخمة مجهزة بأحدث التقنيات الرقمية لتقديم الخدمات المصرفية المتاحة على شبكة الانترنت، ويطلق على هذه المؤسسات المالية عدة تسميات منها المصاريف الافتراضية أو المصارف عبر الانترنت، وإن نشاطات البنوك الإلكترونية تشمل بالضرورة تبادل المعلومات والبيانات بواسطة الفاكس أو الهاتف أو الحاسوب، وإن الحصول على الخدمات التي تقدمها هذه المصارف تتطلب من العميل أن يفتح حساباً مع أحد المؤسسات المالية، ويكون مسبوقا عادة بتوقيع عقد مكتوب حيث يتم تنفيذه شخصياً أو إلكترونياً. **للمزيد انظر:** محمد سعيد أحمد إسماعيل، المرجع السابق، ص 323.

هذه الأنظمة المؤمنة والموثقة قد تم تصميمها بشكل خاص ليتم توظيفها كأنظمة تشغيل للشيك الإلكتروني والاستفادة من البنية التحتية الرقمية للبنوك الإلكترونية التي تقدم خدماتها مباشرة على شبكة الانترنت[1].

ولقد استحدث التشريع الجزائري هذا النوع المطور من الأوراق التجارية بموجب القانون رقم 05-02 المؤرخ في 06 فيفري 2005 المتضمن القانون التجاري، بحيث أضاف فقرة ثالثة لنص المادة 414 في وفاء السفتجة, وتنص على مايلي: "... يمكن أن يتم التقديم أيضاً بأي وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما"، ولقد تم إضافة نفس الفقرة إلى نص المادة 502 بمناسبة تقديم الشيك للوفاء[2].

وتتنوع أنظمة الدفع الخاصة بالشيك الإلكتروني[3]، إلا أنها تصب كلها في مجال العمل على وجود وسيط بين المتعاملين يقوم بإجراء عملية المقاصة، وغالباً ما يكون أحد البنوك، وتتطلب عملية الوفاء بواسطة الشيكات الإلكترونية أن يكون لكل من البائع والمشتري حساباً لدى بنك محدد، وبالتالي يكون لكل منهما توقيعاً إلكترونياً معتمداً ومحفوظاً في قاعدة البيانات الخاصة بالبنك, وعند إجراء عملية الدفع يقوم المشتري الساحب بتحرير شيكاً إلكترونياً للمستفيد، ويوقع عليه إلكترونياً, ويرسله بالبريد الإلكتروني[4].

وبعد التحقق من قيمة الشيك من قبل التاجر وكذا التوقيع عليه كمستفيد، يرسله عبر البنك لمراجعة الشيك والتحقق من التوقيعات والبيانات المدرجة عليه وتوافر الرصيد الكافي، ومن ثم يقوم البنك بخصم قيمة

---

1 محمد سعيد أحمد إسماعيل، نفس المرجع السابق، ص 323-324.

2 القانون رقم 05-02 المؤرخ في 27 ذي الحجة 1425 الموافق 06 فبراير 2005, ج رج العدد 11، السنة 42، ص 8, يعدل ويتمم الأمر رقم 75-59 المؤرخ في 20 رمضان 1395 الموافق 26 سبتمبر سنة 1975 المتضمن القانون التجاري.

3 من بين أنظمة الدفع للشيكات الإلكترونية نظام (FSTC)، حيث يقتضي نقل الشيك من شكله العادي إلى النطاق غير الملموس، بحيث يمكن العميل من الحصول على دفتر الشيكات الإلكترونية، واستعين في هذا النظام بالتشفير لضمان عملية تسوية الدين بالوفاء، وقد ساعد في اعتماده كأسلوب وفاء للشيك عبر الانترنت العدد المتزايد من المستفيدين منه مما أدى إلى اعتراف الحكومة الأمريكية به وانخراط مجلس الخزانة الأمريكي في هذا النظام واستعماله للشيك الإلكتروني أول مرة في 30 جوان 1998، أما النظام الآخر فهو نظام NETCHEX، طرح هذا النظام من قبل شركة NETCHEX، ويقتضي وجود تسجيل مسبق لمستخدم النظام والتاجر لدى هذا الوسيط، وترتكز إجراءات الأمان لهذا النظام على نقطة أساسية تتمثل في عدم إظهار المعلومات المصرفية على الوثيقة، وتتأكد هذه الشركة من صحة وأصالة الوثيقة بواسطة قاعدة بيانات الأعضاء المنتمين لها، ثم ينقل الشيك بخطوط خاصة إلى الشبكة المصرفية حيث يتم التعامل معه بنفس الطريقة التي يعامل بها الشيك التقليدي. للمزيد انظر: عدنان إبراهيم سرحان، الوفاء الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، بتاريخ 10-12 ماي سنة 2003، المجلد الأول، ص 270-271.

4 مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الانترنت، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، سنة 2010، ص 426-427.

الشيك من رصيد المستهلك وإضافته إلى رصيد التاجر ويخطر البنك كل من المستهلك والتاجر بعملية التسوية[1].

ثانياً: وسائل الدفع الإلكترونية الحديثــة.

لقد عمل التطور التكنولوجي في مجال المعلوماتية والاتصال في التجارة الإلكترونية على وضع أدوات وفاء حديثة تتماشى ونمط التعامل التجاري الإلكتروني، ولم يكتف عند حد المعالجة الإلكترونية لوسائل الدفع التقليدية، وبهذا فقد حظيت هذه الوسائل باهتمام خاص من طرف المتعاملين بها، مما جعلها محل دراسة ونقاش لتنظيم آليات التعامل بها وتأطيرها في مختلف الدول[2].

وفي هذا الصدد سيتم إلقاء الضوء على أهم هذه الوسائل من خلال بحث المقصود بأدوات الدفع الإلكترونية الحديثة، وكذا بيان آليات استعمالها والدور الذي تلعبه في ظل المعاملات التجارية الإلكترونية.

1- بطاقات الدفع الإلكترونيــة:

لقد تعددت مفاهيم بطاقة الدفع الإلكترونية ما بين تعريفات شكلية[3] وفنية وقانونية، فذهب البعض[4] إلى تعريفها:"بأنها عبارة عن قطعة من البلاستيك بأبعاد قياسية مدون عليها بيانات ومعلومات مرئية وغير مرئية، يصدرها البنك لحساب لشخص طبيعي أو معنوي بناءً على عقد بينهما، يمكنه من سحب أو تحويل مبالغ مالية من حسابه وفاء لما يحصل عليه من سلع وخدمات من التجار الذين يرتبطون مع البنك المصدر بعقد يتعهدون فيه بقبول البطاقة في الوفاء بمشتريات حامل البطاقة على أن تتم عملية التسوية بين البنوك أو الأطراف وفقاً لنظام الدفع الإلكتروني".

ولقد اتجه المجمع الفقهي لمنظمة المؤتمر الإسلامي في دورته السابعة بجدة عام 1993 إلى تعريف بطاقة الدفع الإلكترونية بأنها:"مستند يعطيه مصدره لشخص معين بناءً على عقد بينهما، يمكنه من شراء السلع

---

1 محمد أمين الرومي، التعاقد الإلكتروني عبر الانترنت، دار المطبوعات الجامعية، الطبعة الأولى الاسكندرية،سنة 2004، ص 145-146.

2 عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 111.

3 فمن حيث الشكل تعرف البطاقة الإلكترونية بأنها تتضمن بيانات رقمية تظهر بأحرف بارزة تحدد الجهة المصدرة لها، وهوية الشخص حاملها، ونطاق صلاحيتها، وبموجب العقد يتسلم الحامل بطاقة الائتمان من الجهة المصدرة ليستعملها كأداة ائتمان في الوفاء بقيمة مشترياته. **انظر في ذلك:** موسى رزيق، رضا حامل البطاقة الائتمانية بالعقد والحماية التي يقررها المشرع له، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الامارات العربية وغرفة تجارة وصناعة دبي، بتاريخ 10-12 ماي 2003 المجلد الخامس، ص 1083.

4 خالد عبد التواب عبد الحميد أحمد، المرجع السابق، ص 49.

والخدمات ممن يعتمد المستند دون دفع الثمن حالاً لتضمينه التزام المصدر بالدفع، مما يمكن سحب النقود من المصارف"[1].

ولقد أضاف المشرع الجزائري بموجب القانون 05-02 المتضمن القانون التجاري في الباب الرابع، الكتاب الرابع والمعنون بالسندات التجارية، الفصل الثالث منه يتضمن بطاقات السحب والدفع وتحديداً في نص المادة 543 مكرر 23 حيث نصت على مايلي:"تعتبر بطاقة الدفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانوناً، وتسمح لصاحبها بسحب أو تحويل الأموال"[2].

ويلاحظ من التعريفات السابقة أن بعضها يخلط بين بطاقة الوفاء الإلكتروني وبطاقة الائتمان، والبعض[3] ينظر طبيعة العلاقة الناشئة عن إصدار البطاقة واستخدامها، وما نريد التركيز عليه هو بطاقة الدفع الإلكتروني المستخدمة لوفاء ثمن المشتريات وأداء الخدمات التي تتم من خلال شبكة الانترنت، وهي مايطلق عليه بطاقة الانترنت.

وبهذا ذهب جانب من الفقه[4] إلى تعريف بطاقة الانترنت: "بأنها بطاقة ممغنطة تصدرها البنوك المرخص لها في ذلك بمبلغ معين، بمقتضى عقد مبرم مع البنك تتيح لحاملها شراء السلع والحصول على الخدمات من خلال شبكة الانترنت، والوفاء باستخدامها في حدود المبلغ الذي صدرت به"، وتحتل بطاقة الانترنت مكانة كبيرة بين طرق الدفع الإلكتروني، فيستخدمه أكثر من 80 % من المستهلكين في الوفاء بمشترياتهم على شبكة الانترنت.

يتم الدفع عن طريق بطاقة الانترنت بقيام المستهلك بالتعاقد مع التاجر على شراء سلعة أو خدمة من الموقع التجاري الإلكتروني، فيرسل المستهلك بيانات بطاقة الانترنت الخاصة به عن طريق صفحة الويب المحمية، ويقوم التاجر بالتوثيق من البطاقة للتأكد من أنها سارية وغير مسروقة، ويمكن للتاجر التأكد من مصدر البطاقة لضمان وجود المبلغ وحجزه، ثم تتم عملية التسوية بعد شحن المشتريات للمستهلك وانتقال

1 واقد يوسف، المرجع السابق، ص 69.

2 القانون رقم 05-02 المتضمن القانون التجاري السابق الذكر.

3 محمد أمين الرومي، المرجع السابق، ص 136.

4 محمد خليل بحر، بطاقات الائتمان والآثار القانونية المترتبة بموجبها، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية وغرفة تجارة وصناعة دبي، يتاريخ 10-12 ماي 2003، ص 989.

المبلغ إلى حساب التاجر عبر النظم المصرفية، وهذا يفترض أن يكون للتاجر حساب لدى بنك لتتم إضافة المبلغ إلكترونياً بطريقة المقاصة أو الحوالة[1].

2- النقود الإلكترونيـــــة:

يستخدم مصطلح النقود الإلكترونية للإشارة إلى الأنظمة الحديثة المؤمنة على برامج حاسوبية لتبادل المعلومات, وتحويل الوحدات النقدية الإلكترونية بشكل رقمي عبر شبكة الانترنت، وقد استخدمت عدة تسميات للإشارة للنقود الإلكترونية، مثال ذلك: النقود أو العملة الرقمية، النقود الائتمانية الإلكترونية، النقود المغناطيسية[2].

ولقد اتجه بعض الفقه[3] إلى تعريف النقود الإلكترونية بأنها:" تسجيل لقيمة العملة الموثقة والمقيدة في شكل إلكتروني".

وعرفها البنك المركزي الأوروبي بأنها:"مخزون إلكتروني لقيمة نقدية على وسيلة إلكترونية مثل بطاقة بلاستيكية، قد تستخدم في السحب النقدي أو تسوية المدفوعات لوحدات إقتصادية أخرى غير تلك التي أصدرت البطاقة"[4].

أما بالنسبة لآلية استخدام النقود الإلكترونية؛ فإن المستهلك يقوم بالحصول على وحدات نقدية إلكترونية ذات قيم مختلفة من البنك المتعامل معه، وفي حالة تعاقده على السلع والخدمات، فيمكنه الوفاء باستخدام هذه النقود بإصدار أمر من حاسوبه الشخصي، وإرسالها عبر الانترنت إلى التاجر، ويقوم التاجر بالاستفادة منها بعد التحقق من وجود حساب للمستهلك بالنقود الإلكترونية لدى البنك، ومن صلاحية النقود للاستعمال في الدفع، ويتم بعد ذلك تحويل النقود الإلكترونية إلى نقود عادية في حسابه الخاص، أو يبقي عليها كنقود إلكترونية ويودعها في حسابها لدى نفس البنك المتعامل معه أو بنك آخر[5].

1 كوثر سعيد عدنان، المرجع السابق، ص 575.

2 أمير فرج يوسف، عالمية التجارة الإلكترونية وعقودها وأساليب مكافحة الغش الإلكتروني، المكتب الجامعي الحديث، الاسكندرية، بدون طبعة، سنة 2009، ص 111.

3 محمد سعيد أحمد إسماعيل، المرجع سابق، ص 332.

4 VERCILLE (V), BOUBILA (S) et FABRE(R) : La monnaie électronique: enjeux micro-économique et macro-économique, éd université des sciences sociales des toulous1, Maitrise de sciences économiques, 1998-1999, p 08.

5 عدنان إبراهيم سرحان، المرجع السابق، ص 196-197.

3- التحويل الإلكترونـــــي:

إذا كان تعريف التحويل المصرفي العادي بأنه:"مجموعة من العمليات التي تبدأ بأمر الدفع الصادر عن الآمر بهدف وضع قيمة الحوالة، تحت تصرف المستفيد"[1]. فتعريف التحويل المصرفي الإلكتروني لا يختلف عن التحويل المصرفي العادي سوى بوجود وسائل إلكترونية، تسمح بالقيام بالعملية عن بعد، والتي تتم بعلاقة عقدية بين المؤسسات المالية[2].

وبذلك اهتم قانون تحويل الأموال الإلكترونية الأمريكي بتعريف التحويل المصرفي الإلكتروني, فيرى بأنه:"عملية تحويل للأموال تبدأ أو تنفذ من خلال وسيلة إلكترونية، كالهاتف، الحاسوب أو شريط مغناطيسي يهدف أمر أو توجيه أو تفويض منشأة مالية بإجراء قيد دائن أو مدين في الحساب"[3].

وتنشأ آلية التحويل المصرفي الإلكتروني بتوجيه العميل (المستهلك) أمره إلى بنكه بتحويل مبلغ نقدي من حسابه إلى حساب شخص آخر (التاجر)، وهو المستفيد من أمر التحويل, ويقوم البنك بالتأكد من كفاية الرصيد، ثم يقوم بعملية نقل المبلغ عن طريق القيد من حساب العميل إلى حساب التاجر الآخر وهذا في حالة إذا كان الطرفان عميلان لنفس البنك، أما إذا كانا يتعاملان مع بنكيين مختلفيين فقد يكون هناك حساب قائم بين البنكين، وهنا يتم تنفيذ الأمر مباشرة بينهما عن طريق المقاصة، وقد يحتاج الأمر إلى تدخل بنك ثالث يكون لكل من البنكين حساب فيه[4].

المطلب الثاني: الجرائم الماسة ببطاقات الدفع الإلكترونـــي والمواجهة التشريعية المقررة لها.

يثير نظام الدفع الإلكتروني العديد من المشكلات القانونية التي تتنافى وأمان المعاملات الإلكترونية، وذلك ناتج عن طبيعة هذا النظام حيث يتم في بيئة إلكترونية، وكذلك يتم على نطاق عالمي، مما يشكل خطورة كبيرة تتمثل في عدم كفاية القواعد القانونية الحالية لتنظيم هذه الآلية الحديثة في الوفاء، ولعل أبرز الآليات المستخدمة في هذا النظام تتمثل في بطاقات الدفع الإلكتروني على اختلاف أنواعها والتي تعتبر أكثر الوسائل انتشاراً إن كان في مجال السحب الآلي للأموال أو الاستخدام عبر شبكة الانترنت، وإن اعتبرت بطاقة الدفع الإلكتروني من أبرز الوسائل التي تحمل امتيازات في طريقة الاستعمال, إلا أن هذه

1 محمد خليل بحر، المرجع السابق، ص 990

2 سميحة القليوبي، الأسس القانونية لعمليات البنوك، دار النهضة العربية، القاهرة، الطبعة الثانية، سنة 2003، ص 105. **انظر أيضاً**: أحمد سفر، المرجع السابق، ص 72.

3 يوسف وقاد، المرجع السابق، ص 98.

4 محمد عمر ذوابة, وأكرم ياملكي، المرجع السابق، ص 26.

الميزات حفتها مخاطر وسلوكات إجرامية تؤثر على فكرة الأمان في أدائها، الأمر الذي استلزم إصدار قواعد قانونية خاصة تضبط مجال الحماية الجنائية لبطاقات الدفع الإلكتروني سواءً على المستوى الداخلي أو الدولي[1].

وبناءً على ذلك يتم التطرق للجرائم الماسة ببطاقة الدفع الإلكتروني (الفرع الأول)، ثم المواجهة التشريعية الجنائية المقررة لها (**الفرع الثاني**).

الفرع الأول: الجرائم الماسة ببطاقة الدفع الإلكترونـــــي.

فيما يتعلق ببطاقات الدفع الإلكترونية فإنها تثير مشكلات قانونية متنوعة، بداية من حماية المعلومات والبيانات الشخصية من جرائم التزوير والسرقة، إلى التنظيم القانوني لمختلف الاستعمالات الخاصة بها، مما خلق تأثيراً على سعة انتشارها وقبولها من قبل المتعاملين الإلكترونيين[2].

وتتنوع تلك الجرائم بين مخاطر ناتجة عن الاستخدام غير المشروع لبطاقات الدفع الإلكترونية من قبل حاملها الشرعي (البند الأول), والاستخدام غير المشروع لبطاقات الدفع الإلكترونية من قبل الغير (البند الثاني) .

البند الأول: الاستخدام غير المشروع لبطاقات الدفع الإلكتروني من قبل حاملها.

قد يقع المستهلك فريسة الاستخدام غير المشروع لبطاقة الدفع الإلكتروني الخاصة من قبل التاجر المتعامل معه في عقد التجارة الإلكترونية، وذلك في حالة تبليغ المستهلك التاجر برقم البطاقة عن طريق الاتصال الإلكتروني، أو من خلال كتابة الرقم في خانة ضمن بنود العقد على موقع التاجر، ويلتزم التاجر عند حصوله على الرقم السري للبطاقة أن يحيطه بالسرية والتأمين، كما يجب أن لا يسحب من البطاقة أكثر من قيمة المبلغ المتفق عليه وفاء لثمن السلعة أو الخدمة، إلا أن بعض التجار يمارسون بعض أساليب الغش والاحتيال بالسحب أكثر من المبلغ المستحق أو استخدام الرقم السري للبطاقة في غير إطاره الشرعي بما يمثل إضراراً بمصلحة المستهلك[3].

---

1 أمير فرج يوسف، المرجع السابق، ص 308.

2 إبراهيم سيد أحمد، المرجع السابق، ص 87.

3 فتحية محمد قوراري، الحماية الجنائية للمعاملات المصرفية الإلكترونية (دراسة تطبيقية) على بطاقات الائتمان المغنطة في القانون الإماراتي والمقارن، مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الاسكندرية، جويلية سنة 2005، ص ص 257-

كما قد يصدر الاستخدام غير المشروع للبطاقات الإلكترونية من الغير وهو طرف خارج عن عملية التعاقد، وذلك بحصوله على بطاقة الدفع عن طريق سرقتها أو الحصول عليها بعد فقدها من حاملها الشرعي، أو الحصول على الرقم السري بأية وسيلة غير مشروعة، كأن يقوم الغير بتزوير البطاقة عن طريق إنشاء بطاقة خاصة ببنك معين لبعض العملاء على الشبكة واستغلالها بالحصول على السلع والخدمات[1].

وقد يحصل الغير على الرقم السري للبطاقة أيضاً عن طريق الاختراق غير المشروع لمنظومة خطوط الاتصال العالمية التي تربط جهاز الحاسوب الخاص بالمستهلك بالحاسوب الخاص بالتاجر.

وبهذا تتعدد وسائل الاحتيال في استعمال بطاقات الدفع الإلكتروني وتتنوع باختلاف البطاقة نفسها وما تقدمه من وظائف أو خدمات لحاملها، ولذا فإننا نرى ضرورة التفرقة بين البطاقات المختلفة من حيث أداء وظائفها عند تناول صور الاستخدام غير المشروع؛ وهنا نفرق بين الاستعمال غير المشروع لبطاقات الدفع الإلكتروني كأداء وفاء, وبين استخدامها بشكل غير قانوني في سحب النقود ثم الاستخدام غير المشروع كأداة ضمان للشيكات، وأخيرا استخدام البطاقة الدفع من قبل حاملها بعد إلغائها أو انتهاء صلاحيتها[2].

أولاً: الاستخدام غير المشروع لبطاقات الدفع الإلكتروني كأداة وفاء.

تسمح بعض بطاقات الدفع الإلكتروني لحاملها الشرعي فرصة الحصول على السلع والخدمات من قبل الجهات المقبولة من البنك المانح لها، وتمنح هذه البطاقات حاملها الحق في اتخاذ الإجراءات اللازمة لخصم المبلغ الذي يحدده –لمصلحة جهة التعامل– من حسابه لدى البنك المانح للبطاقة.

ويمكن أن تتجلى إساءة استخدام البطاقة السليمة في هذا المجال، عندما يستعملها حاملها الشرعي للحصول على سلع وخدمات، وهو يعلم أن رصيده في البنك غير كافٍ، ويمكن أن يتجاوز بذلك الحد الأقصى الذي يضمنه هذا البنك أو لا يتجاوزه، ففي حالة تجاوز الحامل للرصيد المضمون لدى البنك من أجل الوفاء يكون المجني عليه هو التاجر أو مقدم الخدمة، إذ أن البنك غير ملزم بتسديد ما زاد على هذا الحد من مبالغ ثمنا للسلع أو الخدمات التي اقتناها المتعامل، وهذا ما دعا بعض الفقهاء[3] للقول بتطابق

---

259. **انظر أيضاً:** عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص 127. **وانظر أيضاً:** محمد سعيد أحمد إسماعيل، المرجع السابق، ص 343.

1 إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، سنة 2007، ص 111.

2 Tronche, La monaie electrinique, Rev .ass n. D, No. 42, 1982, p 18.

3 DEVEZE (j) , La fraude informatique- Aspects juridiques, J.C.P 2007,doct. 3289, No: 9.

تكييف الإحتيال عليها؛ لأن إقبال حامل البطاقة على تقديمها للتاجر يعد حسب رأيهم وسيلة احتيالية تم من خلالها إقناع الحامل له بوجود رصيد وهمي.

ولقد تبنى القضاء الفرنسي هذا الرأي في بعض أحكامه، بحيث اعتبر أن تقديم البطاقة مع العلم بعدم كفاية الرصيد وعدم توجه حامل البطاقة إلى تزويد الرصيد بالمبلغ الذي استخدم البطاقة للوفاء به، إنما يشكل وسيلة احتيالية تهدف إلى إقناع التاجر بوجود رصيد وهمي[1]، ويدعم القضاء الفرنسي وجهة نظره بأن استخدام بطاقة الوفاء على الرغم من عدم كفاية الرصيد هو في الحقيقة استعمال تعسفي لمستند صحيح، استعان به حامل البطاقة لتدعيم أكاذيبه وإقناع التاجر بوجود رصيد وهمي[2].

ويمكن تفسير هذا التوجه للقضاء الفرنسي في أنه قد غلب فكرة الاحتيال على غيرها، من أجل حماية أموال البنك من السلب بهذه الوسيلة، وذلك تأسيساً على أن حامل البطاقة كان يعلم وقت شرائه السلع أو حصوله على الخدمة أنه لن يقوم بتسديد قيمتها لهذا البنك.

في حين انتقد آخرون[3] هذا التوجه، فمن جهة لا تحقق الأساليب الاحتيالية بمجرد تقديم البطاقة للتاجر أو مقدم الخدمة، أي لا يمكن القول إن الاستعانة بالبطاقة كان دعماً لادعاءات كاذبة، ومن جهة أخرى يفترض أن لدى التاجر أومقدم الخدمة علماً مسبقاً بالحد الأقصى الذي يضمنه البنك بموجب بطاقة الوفاء التي منحها للعميل.

ونحن نميل إلى هذا الرأي، لأن وسائل الاحتيال هي أكاذيب مدعمة بمظاهر خارجية، ولقيام جريمة الاحتيال بحق المتهم لابد من استعانته بأشياء تتخذ أشكال هذه المظاهر الخارجية لتدعيم أكاذيبه، ويشترط لصحة المظهر الخارجي أن يكون مستقلاً عن هذه الأكاذيب، بحيث يمكن القول أن المتهم قام بسلوكين مختلفين أما إذا كان الشيء مندمجاً في موضوع الكذب بحيث لم تكن الإشارة إليه غير ترديد للكذب أو تأكيد له فإن الوسائل الاحتيالية لا تقوم بذلك[4].

أما في الحالة التي لم تتجاوز فيها عملية الوفاء الحد الذي يضمنه البنك، فإن الرأي يتجه إلى عدم اعتبار حامل البطاقة قد ارتكب فعلاً يستحق العقاب عليه جزائيا؛ لأن التاجر أو مقدم الخدمة في هذه

1 Cour d'appele de paris, No: 3 mars 2008 ;Gaz. pal. II. p 721.JEANDIDIER (W), Les truques et usages frauduleuse de cartes magnétiques, J.C.P 2012 doct .789.

2 JEANDIDIER (W), Les truques et usages frauduleuse de cartes magnétiques, J.C.P 2012 doct .789.

3 Cabrillac (M) et Mouly (c): Droit pénal de la banque et du crédit , MASSON, Paris, S.D, N 356.

4 جميل عبد الباقي الصغير، المرجع السابق، ص 37.

الحالة لم يتضرر ما دام البنك المانح للبطاقة ملتزماً بتسديد قيمة الفاتورة؛ أي لا يستطيع التاجر أو مقدم الخدمة التذرع بأن الحامل قد استخدم وسائل احتيالية لإقناعه بوجود رصيد وهمي. وكذلك من غير المنطق معاقبة الحامل على تجاوزه رصيده لدى البنك، ما دامت عملية الوفاء كانت ضمن الحد الذي يضمنه هذا البنك، إذ أن تضرر البنك من عملية الوفاء نتيجة التزامه بتسديد النفقات الناجمة عن استخدام البطاقة الصادرة عنه لا يبرر اعتبار سلوك حامل البطاقة جريمة معاقباً عليها[1].

ويذهب رأي في الفقه الفرنسي[2] إلى أنه من المتعذر تجريم إساءة استخدام البطاقة الائتمانية كأداة وفاء سواء تجاوز الحامل الحد الأقصى الذي يضمنه البنك أم لم يتجاوزه، وإن كان سلوك الحامل في هذه الحالة هو أقرب إلى خيانة الأمانة منه إلى الاحتيال، حتى ولو لم يكن العقد المبرم بين الحامل والجهة المانحة للبطاقة لا يدخل ضمن عقود الأمانة التي حددها قانون العقوبات.

ويميل القضاء الفرنسي في بعض أحكامه إلى هذا التوجه، فقد جاء في حكم:"أن العقد المبرم بين البنك وحامل البطاقة الزرقاء يحمل هذا الأخير فوائد متفقاً عليها تضاف إلى المبالغ التي تستخدم البطاقة للوفاء بها إذا لم يوجد رصيد يقابلها، وهو ما يعطي العميل ضمنياً الحق في تجاوز الحد الذي يضمنه البنك، ويترتب على ذلك أنه لا يمكن القول أن حامل البطاقة قد لجأ إلى استخدام أساليب احتيالية في مواجهة البنك لإقناعه بوجود رصيد وهمي، وكذلك لا يمكن التسليم بتحقق الأساليب الاحتيالية في مواجهة التاجر لإقناعه بوجود رصيد وهمي، وذلك لأن الرصيد الذي يقدمه البنك للعميل حقيقي، وعلى البنك أن يتحمل المخاطر الناجمة عن إصداره البطاقة للعميل[3].

والملاحظ أن هذا التوجه يغلب فكرة الائتمان على سواها، فعندما يستخدم الحامل البطاقة للوفاء بثمن السلع أو الخدمات التي حصل عليها من التاجر متجاوزاً رصيده لدى البنك, فإنه لا يتعدى كونه مستديناً لم يقم بتسديد دينه لهذا البنك، ومن ثم لا يشكل سلوكه جريمة، ومما يدعم وجهة النظر هذه أنه

1 HANACHOWICZ (L), Les cartes bancaires (Irrégularités et Fraudes), Thése doctorat, Université LYON III, 2008, p111.

2 Cabrillac (M) et Mouly (c), Op.Cit, p 356.

3 Cour d'appel de Colmar; 9 mai 2012; Rcueil Juridique; p 95.

قد جرى العمل لدى الجهات المانحة لبطاقات الوفاء على عدم خصم المبالغ التي استخدمت البطاقة في الوفاء بها إلا بعد مدة معينة وهو ما يعد من قبيل التسهيلات المصرفية[1].

ثانياً: جريمة إساءة استخدام بطاقة الدفع كأداة سحب.

يمكن القول بشكل عام أن جميع البطاقات الائتمانية تقوم بوظيفة سحب النقود، حيث أن هذه الوظيفة تعد أساساً لعمل البطاقات الائتمانية المختلفة، إلا أن هناك بطاقات ينحصر دورها في وظيفة سحب النقود فقط، ويبنى هذا الدور بناءً على العقد المبرم بين الجهة المانحة للبطاقة وبين حاملها والذي ينص على التزام هذا الأخير– عند عملية سحب أي مبلغ من النقود من جهاز توزيع النقود– بالتأكد من كفاية رصيده، كما يمكن أن يتضمن أيضاً العقد نصاً يقضي بتعرض حامل البطاقة للعقوبات التي ينص عليها القانون في حالة الاستخدام غير المشروع لها.

وتظهر بصورة أساسية مشكلة إساءة استخدام البطاقة الائتمانية عندما يتم السحب من أجهزة توزيع النقود التي لا ترتبط مباشرة بحساب العميل في البنك؛ أي عندما تعتمد الأجهزة على نظام " Off line", وذلك على عكس الأجهزة التي تعتمد على نظام "On line" حيث يرتبط الجهاز مباشرة بحساب العميل في البنك، ومن ناحية أخرى فإن وسائل الرقابة على صلاحية بطاقات السحب جعلت الاستخدام غير المشروع لهذه البطاقات في مواجهة أجهزة السحب يقتصر على الحالات التي يتم فيها السحب بما يجاوز رصيد الحامل، ولا يضمن استعمال بطاقة سحب انتهت مدة صلاحيتها أو تم إلغاؤها، حيث يتم سحب هذه البطاقات بطريقة آلية عن طريق الأجهزة التي تمت برمجتها للقيام بهذا العمل بعد تزويدها بالذاكرة اللازمة لذلك، كما أنه يجب التنويه أيضاً إلى أنه مع تطور أجهزة السحب الآلي أصبحت الحالات التي تنطوي على سحب يجاوز رصيد الحامل تتسم بالندرة، فهذه الأجهزة وهي عبارة عن نهايات طرفية أصبحت تمارس نوعاً من الرقابة على البطاقات المستخدمة وذلك باتصالها بمركز الإرسال الذي يعطي الموافقة على عملية السحب في حدود ما يسمح به رصيد الحامل[2].

[1] Christian Gavalda, Jean Stoufflet,Instruments de Paiement et de Credit; 7 éme ed; LexisNexisSA, Paris, 2009, p10.

[2] BRUNO KAROUBI, La criminalité favorise-t-elle l'aacceptation de la carte bancaire? Revue économique. 2015/6, Vol 66, P1180.

ويرى جانب من الفقه الجزائي[1] أن استخدام بطاقة الدفع في سحب مبالغ تزيد عن الرصيد لا يشكل جريمة تستحق العقاب، وإنما يعد إخلالاً بالتزامات الحامل التعاقدية اتجاه الجهة المانحة للبطاقة تقوم به المسؤولية المدنية لا الجزائية.

وقد اتجهت محكمة النقض الفرنسية إلى هذا الرأي في قرار لها:"أن قيام حامل البطاقة بسحب مبلغ من النقود من أحد أجهزة التوزيع الآلي، متجاوزاً رصيده الدائن في الحساب، ينظر إليه على أنه مخالفة لشروط التعاقد بين البنك والعميل، ولا يدخل تحت أي نص من نصوص قانون العقوبات"[2].

في حين يرى جانب من الفقه[3] أن استخدام البطاقة الائتمانية في هذه الحالة يعد جريمة تستحق العقاب، لأنه عندما يقوم حاملها بالسحب على الرغم من عدم وجود رصيد له في الحساب أو السحب بما يزيد على الحد المسموح به من قبل البنك، فإن سلوكه يتصف بعدم المشروعية ولا يجوز القول أنه يعد فقط من قبيل الإخلال بشروط العقد المبرم بين البنك وحامل البطاقة؛ أي أن سلوكه ينطوي على إخلال بشروط التعاقد من جهة، ويتصف من جهة أخرى بعدم المشروعية.

وبتقديرنا أن هذا الخلاف في أوساط الفقه الجزائي يعود إلى صعوبة إعطاء التكييف القانوني الدقيق لحالة السحب الإلكتروني على الرغم من وجود رصيد، وذلك وفقاً لنصوص قانون العقوبات التقليدية، وهذا ما يفسر لنا إخفاق محاولات القضاء الفرنسي في تطبيق الأحكام العامة المتعلقة بالسرقة والاحتيال وخيانة الأمانة على هذه الحالة.

ثالثاً: جريمة إساءة استخدام بطاقة الدفع كأداة ضمان شيكات.

تسمح بطاقة ضمان الشيكات لحاملها بالوفاء بقيمة بضائع أو خدمات للتاجر أو مقدم الخدمة بواسطة شيك تضمنه البطاقة وذلك بحد أقصى يحدده البنك المصدر، فإذا قام حامل البطاقة بإصدار شيك يتجاوز هذا الحد ولا يوجد رصيد يقابله، فهل يمكن مساءلته عن جريمة الاحتيال لتقديمه البطاقة لضمان الشيك ؟

1 جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة (دراسة تطبيقية في القضاء الفرنسي والمصري)، دار النهضة العربية، مصر، 2010، ص 40.

2 Cass .Crim 24 Novembre 2012. Bul Crim No 315; p810

3 PRADEL (j), FEUILLARD (ch): Les Infractions Commises au Moyen de l'ordinateur Rev .pen .Crim ,Juillet, 2014.

تقترب هذه الحالة التي سبقت الإشارة إليها، والتي يتم فيها استعمال البطاقة والشيك معاً لإجراء عمليات سحب، وقد اعتبرت بعض الأحكام استخدام البطاقة في هذه الحالة من قبيل الطرق الاحتيالية حيث قضت محكمة استئناف باريس أن استعمال البطاقة هو بمثابة استعمال مستند صحيح لتدعيم ادعاءات كاذبة للإيهام بوجود رصيد وهمي.

ويرفض جانب من الفقه[1] هذا التكييف، فكيف يمكن- في تقديرهم- أن يوصف استعمال البطاقة بأنه تدعيم لأكاذيب تتحقق به الأساليب الاحتيالية، في حين أن البنك المصدر قد أعطى لحامل البطاقة بموجبها تصريحاً للوفاء بديونه، ولا يتحقق ذلك بطبيعة الحال إذا كانت البطاقة التي تم استخدامها لضمان الشيك قد انتهت صلاحيتها أو تم إلغاؤها، حيث يرجع البعض في هذه الحالة أنه يمكن تكييفها بأنها جريمة احتيال.

رابعاً: استخدام بطاقة الدفع الإلكتروني بعد انتهاء صلاحيتها أو إلغاؤها.

يحكم العلاقة بين الجهة المانحة لبطاقة الدفع الإلكتروني وحاملها اتفاق يشبه عقد الإذعان، إذ يقدم العميل طلباً ممهوراً بتوقيعه إلى البنك أو المؤسسة المصرفية من أجل الحصول على البطاقة طبقاً للشروط الموضوعة سلفاً من قبل البنك أو تلك المؤسسة وغير قابلة للتفاوض، وبعد فحص حالة العميل يتم قبول طلبه الذي يعد بمنزلة عقد مبرم بينهما, ومدة هذا العقد تكون غالباً سنة تبدأ من تاريخ إصدار البطاقة وهي قابلة للتجديد بشكل دوري، وللجهة المانحة للبطاقة الحق في سحبها أو إلغائها إذا أساء الحامل استخدامها[2].

وبالتالي ينتهي العمل ببطاقة الدفع إما بانتهاء مدة صلاحيتها التي تبدأ من تاريخ إصدار البطاقة وهي قابلة للتجديد، أو وقف العمل بها بسحبها أو إلغائها، وعلى أساس ذلك يبدو لنا أن هناك إشكالية تتعلق بتصرفات حامل البطاقة الشرعي وهي وجوب التفريق بين استعمال البطاقة من قبل حاملها بعد إلغائها، واستعمالها بعد انتهاء مدة صلاحيتها، وأهمية هذه التفرقة وإن كانت تعود لأمر بسيط هو اختلاف العلاقات القانونية التي تنشأ عن الوضعين، واختلاف الجهات التي يصيبها الضرر من تصرف حامل البطاقة ومدى تجريمه ومساءلة حامل البطاقة عنه بالنسبة للعلاقة التي تنشأ بين حامل البطاقة والجهة المصدرة

1 عطية سالم عطية، الصور المستحدثة لجرائم بطاقة الدفع الإلكتروني، مركز البحوث بأكاديمية الشرطة، القاهرة، سنة 2011، ص 232.

2 علي عباس، مخاطر استخدام بطاقة الدفع الإلكتروني عبر شبكة الانترنت، مؤتمر القانون والانترنت، جامعة الامارات، سنة 2002، ص 17

للبطاقة، أو باتجاه التاجر الذي تم استعمال ابطاقة بمواجهته حيث اشترى البضاعة منه، ببطاقة ملغاة، أو منتهية الصلاحية هذا من جانب[1].

ومن جانب آخر ينعكس ذلك على حقيقة القصد الجنائي الذي يمكن أن يتحقق بحق حامل البطاقة بالنسبة للجريمة التي تنسب له إن تم إقرار مساءلته، ووجه إنعكاس ذلك على القصد هو إمكان احتجاج حامل البطاقة بعدم العلم، وبالتالي نفي القصد بانتفاء علمه بإلغاء البطاقة في حين أنه لا يمكنه ذلك في حالة انتهاء مدة صلاحية البطاقة، إذ يعد عالماً أو يفترض فيه ذلك، أي ينبغي عليه العلم بذلك عند استعمالها خارج نطاق مدة صلاحيتها خلاف الأمر بالنسبة لاستعمالها عند إلغائها، إذ قد يحتج بعدم علمه بذلك لعدم إبلاغه أو إخطاره أو لأي سبب آخر. وهنا يتوجب بيان أحكام المسؤولية الجنائية لاستخدام بطاقات الدفع من قبل حاملها في حالتي الإلغاء أو انتهاء مدة صلاحية كل منها بشكل مستقل[2].

1- استخدام بطاقة الدفع الإلكتروني بعد إلغائها

في نطاق العلاقة الجنائية التي تنظم حالة استخدام بطاقة الدفع الإلكتروني بعد إلغائها يثار فرض بصدد هذا الوضع مفاده أن حامل البطاقة قد يستخدم البطاقة على الرغم من إلغائها، حيث يقدمها للتاجر للوفاء بمشترياته، أو أن يتولى استعمالها في سحب النقود.

وفي إطار الإجابة على ذلك وتحديد ما يمكن أن يثار بشأن حامل البطاقة وحتى التاجر فإن ما ينبغي الإشارة له, أو ما ينبغي أخذه بنظر الاعتبار في نطاق الحالة الأولى هو أن يكون التاجر قد قبل البطاقة باعتبارها بطاقة لا زالت سارية المفعول، أي لم يتم إلغاؤها، بمعنى أخص ينبغي ألا يكون التاجر على علم بأن البطاقة قد تم إلغاؤها، وهذا يحصل في حالة استخدام البطاقة بطريقة (off line) ذلك لأن كون التاجر عالماً بإلغائها ومع ذلك يقبلها له حكم مختلف على الصعيد الجنائي، فهذا الوضع ونقصد كونه عالماً بإلغائها لا يمكن أن يجعل التاجر بمنأى عن المسؤولية الجنائية في نطاق قواعد القانون الجنائي، حيث يمكن أن يعتبر شريكاً لحامل البطاقة وتم وصف فعله تحت وصف جرمي معين باعتباره عالماً بإلغاء البطاقة ومع ذلك باشر بقبولها[3].

1 جميل الصغير، الانترنت والقانون الجنائي، المرجع السابق، ص 38.

2 رياض فتح الله بصلة، جرائم بطاقة الائتمان، ب. د .ن، القاهرة، سنة 2007، ص 81.

3 محمد الشوابكة، المرجع السابق، ص 198.

وبناءً على ذلك فإن جوهر هذا الفرض يعالج حالة أن العميل فقط هو من يعلم بإلغاء البطاقة ويقدمها لتاجر يجهل ذلك للوفاء بقيمة مشترياته فيقبلها الأخير. فهل بالإمكان مساءلة حامل البطاقة ؟ وعن أي جريمة يمكن مساءلته, لا سيما أنه قد اعتدى على الذمة المالية للجهة المصدرة للبطاقة, والذي أنهى العمل بالبطاقة بإلغائها استناداً إلى حقه في ذلك، وسعى كذلك من خلالها في الحصول على البضائع والخدمات من جهة يصور بها وجوب قبول البطاقة كونها ما زالت نافذة ويتم العمل بها خلافا للحقيقة ؟

يذهب الفقه الجنائي في الإجابة على هذا الفرض باتجاهين: الأول يرى بعدم إمكان إسناد جرم الاحتيال بحق حامل البطاقة, أما الاتجاه الثاني فيرى بإمكان إسناد جرم الاحتيال باعتبار أن حامل البطاقة قد استخدم طرقاً احتيالية. وسنتولى عرض كلا الاتجاهين فيما يلي:

أ. انعدام المسؤولية الجنائية عن استخدام بطاقة الدفع الإلكتروني بعد إلغائـــها:

يذهب جانب من الفقه[1] في صدد الإجابة على التساؤل المطروح آنفاً –بخصوص إمكانية قيام المسؤولية الجنائية لحامل بطاقة الدفع الإلكتروني باستخدامها بعد إلغائها– إلى القول بأن حامل البطاقة لا يمكن إسناد المسؤولية إليه، ذلك أن نشاطه في مثل هذا الفرض لا يمكن أن يندرج تحت طائلة الأفعال المجرمة بشكل عام, ولا ينطبق عليه وصف جرم الاحتيال أو النصب بشكل خاص.

ويعلل هذا الإتجاه مذهبه استناداً إلى جملة من المبررات التي يسوقها في هذا الإطار، ومنها:

- إن الصفة المزيفة التي استعملها حامل البطاقة، والتي تتمثل بأن صاحب البطاقة قد عرض بطاقة الدفع على أساس أنها فاعلة، ليست هي الدافع الذي أخذ به البنك أو المؤسسة التي أصدرت البطاقة للوفاء بقيمة الخدمات أو المشتريات، وإنما الدافع الحقيقي وراء قيامها بذلك هو الشرط العقدي الذي يلزمه بذلك, لا الحالة التي كان عليها أو ظهر بها مع المتعامل، وعلى أساس ذلك فإن إرادة المجني عليه (البنك أو المؤسسة المصدرة البطاقة) صحيحة ولا يشوبها أي عيب نتيجة الخداع أو الاحتيال الذي قام به الحامل[2].
- أن الركن المادي في جريمة الاحتيال يتطلب علاقة سببية تربط بين فعل الاحتيال والنتيجة التي أفضى إليها فعل النصب الأمر الذي يكون وراء تشويه إرادة المجني عليه نتيجة الغلط الذي وقع فيه، وهو ما يُفتقد في هذا الفرض.

1 عفيفي كامل عفيفي، المرجع السابق، ص 158.

2 جلال الزعبي, أسامة المناعة, وصايل الهواوشة، جرائم الحاسوب والانترنت، دار وائل، عمان سنة 2001، ص 188.

- ويستمر أنصار هذا الرأي في دعم وجهة نظرهم بقولهم أن نسبة المسؤولية الجنائية لحامل البطاقة عن جريمة الاحتيال فيه تحميل للنصوص الجنائية أكثر مما تحتمل، الأمر الذي يتطلب استحداث نص خاص يواجه به ازدياد استعمال بطاقات الوفاء وما قد تنطوي عليه في مثل هذه الفروض من اعتداء على الذمة المالية للبنك[1].

وفي إطار مناقشة الحجج التي استند إليها هذا الاتجاه؛ فنجد أولاً أن ما يعاب على التوجه أن بنى تصوره ووجه انتقاداته لعلاقة لا يمكن أن تنشأ بصورة مباشرة عند استعمال بطاقة تم إلغاؤها، فالعلاقة التي تنشأ ابتداء عند استعمال بطاقة تم إلغاؤها ستكون في مواجهة التاجر الذي يقع عليه عبء التحقق من كونها بطاقة صحيحة إلى جانب كونها بطاقة نافذة، لم يتم إلغاؤها ولا انتهاء صلاحيتها، أما العلاقة التي يشير إليها أنصار هذا الاتجاه فأنه لا يمكن إنكارها, غير أنها تنشأ بالتبعية لعلاقة حامل البطاقة بالتاجر الذي يقبل الوفاء بها, الأمر الذي كما –أشرنا سابقاً– ينبغي التفريق في نطاقها بين علمه أو عدم علمه بإلغاء البطاقة.

أما بالنسبة لاستناده في رفضه لفكرة المساءلة الجنائية لحامل البطاقة على أساس عدم وجود ترابط بين الصفة غير الصحيحة وقيام جرم الاحتيال، فإننا ننتقد هذه الحجة على اعتبار أن الصفة التي ظهر بها حامل البطاقة أمام التاجر بأنها ما زالت سارية المفعول ولها نفاذ في مواجهة البنك يكون قد مارس طرقاً احتيالية[2]، وبنفس الوقت أنه قد استعان بمستندات صادرة عن شخص ثالث لإيهام التاجر بأنه ما زال يتمتع بتلك الصفة, فقدم له دليلاً على شكل خطاب مادي صادر من جهة لها محل ثقة واطمئنان لدى التاجر، وعزز بموجبه مزاعمه وكذبه، الأمر الذي أوقع التاجر بالغلط الذي دفعه لكي يقدم خدماته أو بضائعه لحامل البطاقة.

ب. قيام المسؤولية الجنائية لاستخدام بطاقة الدفع الإلكتروني بعد إلغائـــها:

لقد أنكَرَ الاتجاه السابق جرم الاحتيال بحق حامل البطاقة عندما استعمالها بعد إلغائها من قبل الجهة المصدرة لها، وبهذا ظهر اتجاه آخر[3] يتصدى لهذا الطرح من خلال الاعتراف بقيام المسؤولية الجنائية لصاحب البطاقة كون فعله قد جلب عليه النفع من غير وجه حق، وقد أثرى على حساب جهات معينة،

1 جلال الزعبي, أسامة المناعة, وصايل الهواوشة، نفس المرجع، ص 190.

2 جميل الصغير، القانون الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص 102.

3 محمد الشوابكة، المرجع السابق، ص 210.

إذ أنّه حصل على أموال الغير بطرق وأساليب غير قانونية, وبالتالي حصل على السلع والخدمات دون أن يتولى سداد أثمانها, لذا فإنه يتحمل المسؤولية الجنائية عن جريمة الاحتيال.

وينطلق هذا الاتجاه في تبرير مذهبه هذا من نقطة أساسية هي أن استعمال حامل البطاقة للبطاقة الملغاة يشكل صورة من صور النشاط الذي تتحقق به جريمة الإحتيال، وهذه الصورة هي أن حامل البطاقة ظهر باعتباره صاحب صفة غير حقيقية أو غير صحيحة خلافاً للواقع, لا سيما أن إلغاء البطاقة يخلع عنها قيمتها كأداة وفاء[1]، ويزيل أي صفة عن الشخص الذي يستخدمها وفي تقديمها بعد إلغائها تأكيد لصفة زالت بعد الإلغاء.

غير أن جريمة الاحتيال إذا كان ينبغي لتحققها إحدى الوسائل التي حددها المشرع، فإن هذا الاتجاه وفي هذا الإطار يعتبر استعمال البطاقة الملغاة بمثابة انتحال لصفة غير صحيحة يكفي لتحققها مجرد الادعاء بهذه الصفة, وعدم اشتراط أن يؤيد هذه المزاعم بمظاهر خارجية, الأمر الذي تتطلبه جريمة الاحتيال في حال استعمال الطرق الاحتيالية[2]، حيث يشترط لتحقق هذا الأسلوب في الاحتيال أن يعزز الكذب بمظاهر خارجية تؤيده يهدف من ورائها الجاني إقناع المجني عليه، حيث أن مجرد الأقوال والادعاءات الكاذبة لا تكفي لوحدها لتكوين الطرق الاحتيالية, وهو في نطاق موضوعنا إيهام التاجر بوجود ائتمان وهمي لا وجود له في الواقع، هذا من جانب.

ومن جانب آخر إن حامل البطاقة الذي يعلم بإلغاء البطاقة ويتقدم للتاجر بالبطاقة لتسوية معاملاته فهو يستعين بالكذب للاحتيال، وبما أنه لا يعتد بالكذب المجرد في نطاق جريمة الاحتيال فهو يدعمه باستعمال إحدى الوسائل الاحتيالية التي حددها التشريع لقيام الجريمة, وهذه الوسيلة تتمثل في إظهار مستندات منسوبة للغير، ويستخدمها كمستند لإيهام التاجر بأنها ما زالت سارية المفعول، وإيهامه بأن الجهة التي أصدرتها ما زالت ملتزمة أمامه بقبولها بالوفاء على خلاف حقيقتها، وأن حامل البطاقة قد استولى استناداً لذلك على السلع والخدمات دون وجه حق، وهذا كله يعزز تحقق جريمة الاحتيال[3].

وما يؤيد الأخذ بهذا الطرح هو موقف القضاء الفرنسي الذي استقر على أن استخدام بطاقات الدفع الملغاة وكذا المنتهية الصلاحية يكون جريمة احتيال في مواجهة حامل البطاقة، وكذا التاجر الذي تعهد

1 فتحية محمد قوراري، المرجع السابق، ص 28.

2 سامي محمد الشوا، المرجع السابق، ص 107.

3 غنام غنام، الحماية الجنائية لبطاقة الائتمان الممغنطة، ورقة بحثية مقدمة بمؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، سنة 2003، ص 168.

بقبول تلك البطاقة بشرط أن يكون مصدر البطاقة قد أخطره بسحب هذه البطاقة من الاستعمال. وهذا ما أبرزه الحكم القضائي الصادر عن محكمة النقض الفرنسية بشأن قضية إمرأة قامت بتسديد فواتير عن طريق استخدام بطاقة ائتمان صادرة بموجب حساب بنكي قد تم إغلاقه من قبل السداد، وهذا يقيم جريمة الاحتيال لتوافر الطرق الاحتيالية المستخدمة للإقناع بوجود رصيد وهمي.[1]

وبرأينا نؤيد ونأخذ بالمبررات التي ساقها أنصار هذا الاتجاه في قيام جريمة الاحتيال بحق حامل البطاقة الملغاة، فلا شك أن الإقرار بتحمل حامل البطاقة للمسؤولية الجنائية عن جريمة الاحتيال يعد أمراً مقبولاً، حيث أنه أوهم التاجر بكون البطاقة لا زالت صالحة في حين أنها فقدت قيمتها القانونية، وأنه ظهر بصفة غير صحيحة باعتباره يملك استعمالها في الوقت الذي لا يملك ذلك، الأمر الذي يحقق انخداع التاجر لا سيما أن ما يحدث في الناحية العملية أن التاجر لا يرجع للجهة التي أصدرت البطاقة، أو لمؤسسة الوساطة المالية التي تتولى التوسط بين التاجر والجهة التي أصدرت البطاقة في تحصيل قيم السلع أو الخدمات التي يستفيد منها حاملوا بطاقات الدفع الإلكتروني للتأكد من صحة فاعلية البطاقة للعمل في كل عملية شراء، وهذا بدوره يهدد الثقة التي تبنى عليها مثل هاته العمليات ويمس بمبدأ الأمانة الذي يربط بين التاجر والمؤسسة المصدرة للبطاقة، وبالتالي يستوجب النظر برؤية أكثر حزم لتسييج هذه المعاملات ضد أي نوع من الأعمال الإحتيالية حتى لوكانت صادرة من حامل البطاقة بحد ذاته وتغليب فرض التجريم على دونه.

2. استخدام بطاقة الدفع الإلكتروني بعد انتهاء صلاحيتها:

من المعلوم أن من أهم الالتزامات التي تترتب على حامل البطاقة بعد إبرامه عقد طلب بطاقة الدفع الإلكتروني هو أن يتم استخدامها خلال فترة زمنية معينة تمثل مدة صلاحيتها قانوناً، وإذا تمت هذه المدة فإنه يكون ملزماً بردها إلى الجهة التي أصدرتها، إلا أنه يظهر في هذا الإطار أمر مفاده حكم احتفاظ صاحب البطاقة بعد مدة انتهاء صلاحيتها، وتطرح الإشكالية مدى تكييف هذا الفعل كفعل جنائي يستدعي تجريمه أم أنه يدخل في خانة الإخلال ببنود الالتزام في العقد فحسب, ولا يرقى الاعتداد به كجريمة توجب المسؤولية الجنائية ؟

وفي هذا الصدد تناقض رأيين في الفقه حول مسألة تجريم استخدام بطاقة الدفع الإكتروني بعد انتهاء صلاحيتها بين موجب للمسؤولية الجنائية، وبين معارض لقيامها بحق حامل البطاقة, خاصة بارتباط هذه الإشكالية بمسألة قيام الجهات المصدرة بواجباتها القانونية التي تلزمها من حيث المنطق أن تتولى إعلام التجار

1 HANACHOWICZ (L), Op. Cit; p 225

والمتعاملين الإلكترونيين بعملية إلغاء بطاقات الدفع الإلكتروني بعد انتهاء مدة صلاحيتها، الأمر الذي يساعد في الحد من الوقوع في هذا الإشكال أصلاً[1].

إلا أنه بالرجوع إلى الواقع العملي يتضح أن المؤسسات المالية قد لا تتتبع آليات موحدة في إجراء عمليات التعميم على البطاقات المنتهية الصلاحية، وأن التبليغ السريع الذي يتم بمختلف الطرق الحديثة قد يستخدم في حالات محددة فقط هي حالة سرقة البطاقة أو فقدها، إلى جانب أن هذه الإجراءات لا تتم عن طريق الجهة المصدرة للبطاقة، إنما تتم عن شركات خدمات الدفع بالأمر الذي قد يؤدي إلى أن تحتاج بدورها لوقت غير قصير للتعميم على التجار الذين يقبلون الوفاء بهذه البطاقات، الأمر الذي يساهم في تحقق فرضية استخدام بطاقة منتهية الصلاحية؛ وذلك من خلال استغلال الفترة الزمنية بين انتهاء صلاحية البطاقة وبين إجراء عملية التعميم على تلك البطاقات وإحاطة التجار بذلك[2].

وبالرجوع إلى الإشكال الرئيسي وما يخص الاتجاهيين الفقهيين في مسألة تحقق قيام المسؤولية الجنائية عن استخدام بطاقة الدفع الإلكتروني بعد انتهاء تاريخ الصلاحية، وهنا يدخل بشكل مهم البحث في مدى تحقق جريمة الاحتيال عن قيام مثل هذه الفعل، وهذا من حيث تكييف هذا الفعل وتطابقه مع مفهوم هذه الجريمة من حيث النشاط الإجرامي والقصد الجنائي, وعلى هذا الأساس نوضح كل اتجاه على حدىً ونبرز مبرراته وفقاً لما يأتي:

أ. عدم قيام المسؤولية الجنائية في حالة استخدام بطاقة الدفع الإلكترونية المنتهية الصلاحية:

يذهب جانب من الفقه[3] في صدد الإجابة على الفرض الذي نحن بصدده – والذي يتمثل في قيام حامل البطاقة بتقديم البطاقة للتعامل بها بعد انتهاء صلاحيتها، وما يترتب عليه قانوناً رفض المؤسسة المالية المصدرة لها بتغطية قيمة الصفقة التي أجراها المتعامل (حامل البطاقة)– إلى القول بعدم قيام المسؤولية الجنائية بحق العميل حامل البطاقة حتى وإن كان من شأن هذا الفعل أن يسبب اعتداء على الذمة المالية للتاجر، ويستندون في تبرير هذا الرأي على أساس أن العقد المبرم بين البنك والتاجر, يلزم من خلال شروطه التاجر بفحص البطاقة، والتأكد ظاهرياً من صحة وفاعلية المعلومات والبيانات المدونة عليها.

ويأتي شرط فحص تاريخ بداية وانتهاء العمل بالبطاقة في مقدمة هذه الشروط، وحيث أن التاجر قد أهمل في تنفيذ هذا الالتزام, فهنا تسقط المسؤولية على حامل البطاقة الذي قدم بطاقة قد انتهت

1 سامي محمد الشواء، المرجع السابق، ص 110.

2 عماد خليل، الحماية الجزائية لبطاقة الوفاء، دار وائل، عمان، الأردن، سنة 2000، ص 10.

3 جميل الصغير، الانترنت والقانون الجنائي، المرجع السابق ، ص 43.

صلاحيتها، الأمر الذي يحتم انتباه التاجر وحرصه على اكتشافه، إلى جانب أن مناط التجريم في نطاق قانون العقوبات إنما ينطلق من خطورة الفعل الذي يرتكبه الجاني, بحيث يعكس نفسية إجرامية خطيرة توجب مواجهتها بالعقوبة الرادعة، ولما كان فعل تقديم البطاقة المنتهية الصلاحية هو أمر ساذج وبسيط يفترض أن لا ينخدع به أوسط الناس احتياطاً وحرصاً, فلا مجال لقيام المسؤولية الجنائية عن طريق جريمة الاحتيال[1].

وبرأينا فإنه من المنطقي قبول هذا الرأي في حالة واحدة وهي كون البطاقة تحمل تاريخ انتهاء الصلاحية حيث يجب على التاجر التأكد من التاريخ وعدم قبول العمل بها، وإلا انقلب نشاطه إلى نشاط مجرم في حالة قبوله الوفاء ببطاقة منتهية الصلاحية باعتباره شريكاً لحامل البطاقة بعد تاريخ انتهاء صلاحيتها، والذي يمثل إضراراً بالجهة المصدرة لها، الأمر الذي على ضوئه يمكن القول بضرروة التمييز بين أن يكون التاجر قد ارتكب خطأ أم لم يرتكب أي خطأ، بحيث أن التاجر الذي لا ينسب له أي خطأ بشأن التحري عن صلاحية البطاقة للاستعمال لا يمكن أن يجعل حامل البطاقة بمنأىً عن المسؤولية, خلاف التاجر الذي ارتكب خطأ وتهاون في التحري عن صلاحية البطاقة، إذ يكون بهذا قد أسقط حقه، الأمر الذي يترتب عليه عدم إلزام الجهة المصدرة للبطاقة بسداد قيمة التعامل بالبطاقة.

ب. قيام المسؤولية الجنائية في حالة استخدام بطاقة الدفع الإلكترونية المنتهية الصلاحية:

ينطلق هذا الاتجاه من شروط تطبيق نصوص جريمة الاحتيال لبيان مدى إمكان إعمال تلك النصوص على الفرض الذي ينادي به، وهو القول بتحقق جريمة الاحتيال بحق حامل البطاقة الذي يستخدمها بعد انتهاء فترة صلاحيتها، ومن هنا نناقش رأي هذا الاتجاه ابتداءً من مدى تحقق جريمة الاحتيال وفقاً لأسلوب استخدام بطاقة الدفع الإلكتروني المنتهية الصلاحية ودوافعه ومطابقتها للوصول إلى تحقق فرض قيام المسؤولية الجنائية بحق حاملها[2].

وعلى أساس ذلك فإن جريمة الاحتيال إذ كانت تقوم على الركن المادي المتمثل في استخدام أحد الوسائل المحددة قانوناً, ومن أهمها وسائل الكذب والخداع التي قد تحيط بمظاهر وأعمال تجعل المجني عليه يعتقد بصحة الأمر، والنتيجة تتمثل في الاستيلاء على مال مملوك للغير أو الحصول على نفع غير مشروع لمصلحة الجاني، وهنا يذهب أنصار هذا الاتجاه للقول بعدم إسقاط المسؤولية الجنائية عن حامل البطاقة؛

1 عمر الحسيني، صور الحماية الجنائية لنظام الحاسب الآلي، اتحاد المصارف العربية، القاهرة، سنة 2010، ص 27.

2 عماد خليل، المرجع السابق، ص 22.

بحيث لا يمكن أن يكون نشاطه مشروعاً كون فعل حامل البطاقة المنتهية الصلاحية يشكل صورة من صور النشاط الذي تتحقق به جريمة الاحتيال، وهذه الصورة مؤداها قيام الحامل بظهوره بصفة غير حقيقية، يهدف من خلاله إقناع المجني عليه بوجود ائتمان وهمي لا وجود له في الواقع، ولا سيما أن انتهاء مدة صلاحيتها يخلع عنها قيمتها كأداة وفاء[1].

وما يؤيد ذلك هو أن الجهة المصدرة للبطاقة قد نفذت التزاماتها خلال فترة العقد الأمر الذي يجعل من مستعمل البطاقة بعد هذا التاريخ يكذب على التاجر ويوهمه بأن العقد ما زال ينتج آثاره خلاف الحقيقة، أضف إلى ذلك انتهاز فرصة عدم علم التاجر وإقناعه بتسوية قيمة المعاملة يمثل مظاهر خارجية تعزز الكذب, مدعومة باستعمال إحدى الوسائل الاحتيالية التي حددها التشريع لقيام جريمة الاحتيال، ولعل ما يساهم في تسهيل فعل الاحتيال هو أن البطاقة يتوافر فيها شرط الإقناع الظاهري الذي لا يحتاج إلى تدليل، والذي يولد الإقناع بمجرد استعماله ألا وهو تحقق صدورها عن الجهة المصدرة التي ما زالت ملزمة بالوفاء, وأن الاعتماد المالي ما زال سارياً حتى لحظة الاستعمال[2].

فحامل البطاقة بمسلكه هذا يحقق أمرين؛ الأول الإدعاء بوجود العقد المبرم بينه وبين مصدر البطاقة الذي يستند إليه تبرير وجود البطاقة في حيازته، وإيهامه من جهة ثانية بأن الجهة المصدرة ما زالت ملتزمة أمام حاملها بقبولها الوفاء بقيمة المعاملة, وهو الأمر الذي يدفع التاجر بقبول البطاقة وإتمام تسوية المعاملة استناداً على مظاهر تخالف الحقيقة.

البند الثاني: الاستخدام غير المشروع لبطاقات الدفع الإلكتروني من قبل الغير.

تصب مسألة البحث في إشكالية الاستخدام غير المشروع لبطاقات الدفع الإلكتروني في رافدين مهمين؛ أولهما ما يتعلق بجريمة تزوير بطاقات الدفع الإلكتروني, والتي أضحت تشكل أخطر الأساليب في الاعتداء على نظام الدفع الإلكتروني، وهذا لانتشارها وتطور أساليب ارتكابها من فترة لأخرى (أولًا)، وثانيها البحث في ما يتعلق بأحكام جريمة سرقة أو استخدام بطاقات الدفع الإلكتروني المسروقة أو المفقودة في مجال التعامل الإلكتروني، والتي لا تقل خطورة عن جريمة التزوير من حيث الآثار, وحتى الأساليب

1 خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب، دار الثقافة للنشر والتوزيع، عمان، الأردن، سنة 2011، ص 125.

2 علي سالم، الأساس القانوني لحماية بطاقة الائتمان من الاحتيال، مجلة المحقق المحلي للعلوم القانونية والسياسية، جامعة الكويت، كلية الحقوق، العدد الثاني، السنة السابعة، سنة 2015، ص 122.

المستخدمة في تحقيقها، مما يستدعي ضرروة إيجاد الآليات التشريعية الكافية لبسط الحماية الجنائية والحد من استفحالها (ثانياً).

أولاً: أحكام الحماية الجنائية لجريمة تزوير بطاقات الدفع الإلكترونـــي.

لقد تم في فحوى الفصل الأول من الدراسة[1] رصد ماهية التزوير الإلكتروني، وهو تغيير الحقيقة في محرر بإحدى الطرق المنصوص عليها قانوناً تغييراً من شأنه إلحاق الضرر بالآخرين، وإذا كانت بطاقات الدفع الإلكتروني تأخذ مدلولها في مجال التعامل الإلكتروني باعتبارها محررات إلكترونية ذات طبيعة خاصة؛ باعتبارها وسيلة دفع إلكترونية تهدف بالقيام من العديد من الخدمات المصرفية من سحب ووفاء للنقود وتحويلها، فإن ذلك قد جعل من مجرمي المعلوماتية يتخذون عدة أساليب للاعتداء عليها بالتزوير بغية سلب أموال الغير بطريقة غير مشروعة.

وتبدو أهمية المحرر بالنسبة لجريمة التزوير الإلكتروني بشكل عام من أن المحرر ليس باعتباره محل السلوك أو موضوعه فحسب، وإنما يمثل وعاء الثقة التي توضع فيه، والتي يشملها القانون بحمايته، بحيث أنه إذا وقع تغيير الحقيقة على محل آخر لا تهتز الثقة به لا يعد تزويراً كالأمر الذي يصاحب التغيير في بعض المحررات، إلى جانب ما قد يؤدي إلى التهاون في عدم العقاب أو بساطته إلى اهتزاز الثقة التي يسعى المشرع تركيزها في المحررات، سواء التي تصدر أو يتعامل بها الأفراد أو الدولة[2].

1- مدلول تزوير بطاقات الدفع الإلكترونيـــة:

ويتم التعدي على بطاقات الدفع الإكتروني إما بتزويرها كلياً أو جزئياً، فالتزوير الكلي يأخذ معنى خلق بطاقة جديدة من العدم، ويطبق عليها الجاني عمليات تقليد للشكل والرسوم والكتابة المتواجدة على البطاقة الأصلية، ويستخدم نفس طريقة التغليف ووضع الشريط الممغنط والشريحة الرقائقية والتوقيع كل بحسب تواجده في البطاقة الأصلية، ثم تأتي مرحلة طباعة الحروف النافرة المتضمنة للمعلومات التي تحصل الجاني عليها بطرق خاصة، وهنا يتحقق مفهوم التزوير الكلي بمحاولة الجاني اصطناع بطاقات دفع إلكترونية جديدة عن طريق تقليد في كل محتويات البطاقة وتفاصيلها[3].

---

1 بحيث تم تناول التزوير الإلكتروني من خلال المبحث الرابع للفصل الأول من الباب الأول من الأطروحة.

2 عماد خليل، المرجع السابق، ص 37.

3 ممدوح بن رشيد العنزي، الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير، المجلة العربية للدراسات الأمنية والتدريب، المجلد 31 العدد 62، الرياض، سنة 2015، ص 28.

أما التزوير الجزئي لبطاقات الدفع الإلكتروني، فيتطلب تطبيق عملية التقليد على بطاقات دفع سابقة تكون سارية المفعول أو منتهية الصلاحية، إذ يقوم من خلالها الجاني باستبدال أرقام جديدة محل الأرقام القديمة يتم الحصول عليها بطرق غير مشروعة كاختراق قواعد البيانات أو الدخول لشبكة الحاسب الخاصة بالبنوك، أو باستخدام تقنية الاختراق من شبكة الانترنت، أو يقوم الجاني بتقليد الشريط الممغنط بمحو بيانات الشريط الأصلي وإعادة تشفيره بمعلومات أخرى صحيحة يتم الحصول عليها بطرق أيضاً غير مشروعة، ويلجأ الجاني إلى تزوير التوقيع بمحوه آلياً أو باستخدام مواد كيميائية واستبدال الصورة الحقيقة للحامل بصورة أخرى، وقد أثبتت التجربة اكتشاف عمليات التزوير الجزئي من خلال انهيار جزء من شريط التوقيع، أو ظهور اختلافات في الأرقام والحروف والصورة المثبة على البطاقة المزورة عنها في البطاقة الحقيقية.

2- أركان جريمة تزوير بطاقة الدفع الإلكتروني.

يعرف التزوير الإلكتروني حسب اتفاقية بودابست بأنه: "التزوير المرتبط بالحاسب الآلي والذي يتكون عند خلق أو تعديل غير مصرح به للبيانات في سياق المعاملات الإلكترونية، بتغيير صحة البيانات المستخرجة التي تكون موضوعا لخداع المصالح القانونية المحمية"[1].

وحيث أن بطاقة الدفع الإلكتروني بشكل عام تتشكل من نوعين المكونات؛ إحداهما ذات طبيعة مادية تتمثل بجسم البطاقة المادي الذي يتكون من ورق صلب مسطح أومن مادة كلوريد الفنيل (PVC) أي البلاستيك غير المرن يتم تثبيت مجمل البيانات التي تتعلق بالجهة مصدرة البطاقة حتى البيانات التي يتم تثبيتها بشكل بارز، وكذلك تثبيت الجسم الذي يضم الكيان غير المادي أو المعنوي, أو ما يعرف بالشريط الممغنط، والثاني ذو طبيعة غير مادية يتكون من مجموع البيانات والمعلومات التي يتم دمجها في الشريط الممغنط, والتي تمثل البيانات والمعلومات المشفرة, والتي لا يستطيع استطلاعها واستطلاع مدلولها إلا الأجهزة الإلكترونية[2].

فإن هذه الطبيعة وتلك المكونات ينبغي أخذها بنظر الاعتبار عند معالجة تزوير البطاقة؛ لأن التلاعب والتغيير الذي يمكن أن تتعرض له يمكن أن يصيب الكيان غير المادي أو المعنوي كما يمكن أن يصيب الكيان المادي، وذلك لأن الجناة كما يمكن أن يقوموا بالتغيير للكيان المادي الذي تتكون منه البطاقة يمكن أن يتوجهون بفعل التغيير إلى الكيان المعنوي لا سيما أنهم من الممكن أن يحصلوا على الكيان

1 محمد الشوابكة، المرجع السابق، ص 201.

2 غنام غنام، المرجع السابق، ص 174.

المادي للبطاقة بسهولة بصورة أو بأخرى كالحصول على البطاقات المنتهية الصلاحية أو الملغاة، ويتم ذلك بمساعدة موظفي المؤسسة المصدرة للبطاقة، أو أن تتم سرقتها فيقوم الجناة بنسخ المعلومات التي يتم دمجها بالشريط الممغنط, وتكون للبطاقة بذلك أكثر من نسخة، وتعد هذه الطريقة من أخطر طرق التلاعب بالبطاقة المصرفية .

لذلك فإن البحث في الإشكاليات التي يواجهها التزوير وبالتالي تطبيق النصوص القانونية المنظمة لجريمة التزوير في نطاق البطاقة المصرفية يتعلق بالمحل الذي يرد عليه فعل التزوير، وفي نطاق دراستنا هو بطاقة الدفع الإلكترونية، ٌويثار التساؤل بشأن مدلول المحرر والبيانات التي يتضمنها، فإلى أي مدى بالإمكان تطبيق وصف المحرر على المعلومات والبيانات التي تتضمنها بطاقة الدفع الإلكترونية, وبالتحديد البيانات والمعلومات التي تتضمنها الأشرطة الممغنطة ؟

وعلى أساس ذلك ينبغي في إطار معالجة تزوير البطاقة النظر إلى التغيير الذي ينصب على جسم البطاقة المادي والتغيير الذي ينصب على مكوناتها المعنوية المتمثل بالبيانات والمعلومات المدمجة إلكترونياً على الأشرطة الممغنطة، وحيث أن الأخيرة يضمها كيان مادي يتمثل بالأشرطة الممغنطة, لذلك ينبغي النظر إليها ومحلها إن أصابها التغيير، ومن هذا المنطلق فإن قوام جريمة التزوير يقوم على المساس بصحة البيانات الموجودة ببطاقة الدفع الإلكتروني, سواء هذا المساس نال من الأرقام الموجودة عليها أو الإمضاءات أو تغيير بالكتابة أو التوقيع عليها[1].

3. مدى إسقاط وصف المحرر على بيانات بطاقة الدفع الإلكترونـــــي:

ما ينبغي بيانه في إطار تطبيق نصوص جريمة التزوير على التغيير أو التلاعب الذي يصيب الكيان المادي لبطاقة الدفع الإلكترونية، واستناداً إلى التصور الذي طرحناه هو مدى إمكان وصف التغيير الذي يقع الكيان المادي للبطاقة والتلاعب الذي يمكن أن يصيب بياناتها محققاً لجريمة التزوير الواقع على محرر؟ بمعنى أخص مدى إسقاط وصف المحرر على البطاقة بحيث يكون التغيير الذي يقع عليها أو على البيانات التي تتضمنها محققاً للتغيير المتطلب في جريمة التزوير؟

ومن خلال استطلاع موقف الفقه نجده ينقسم بين رأيين متناقضين: الأول يرى بعدم إمكان إسقاط وصف المحرر على بطاقة الدفع الإلكتروني, وبالتالي عدم إمكان تطبيق نصوص جريمة التزوير على

1 محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الائتمان الممغنطة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، سنة 2009، ص 447.

التغيير الذي ينال من المكونات المادية لبطاقة الدفع الالكتروني. والثاني يرى بإمكانية إسقاط وصف المحرر على بطاقة الدفع الإلكتروني ومتابعة الجناة وفقاً لقواعد وأحكام جريمة التزوير.

أ- عدم ملائمة وصف المحرر على بطاقة الدفع الإلكترونـي:

على الرغم من اتفاق الفقه على عدم أهمية المادة التي يتم تحرير المحررات أو المستندات عليها، إلا أن جانباً من الفقه[1] حاول أن يخالف هذه الحقيقة, ويستند إلى المدلول الذي يعتقد أن المشرع قد صرح عن طبيعة المحرر ويرفض على أساسه إسقاطه على بطاقات الدفع الإلكتروني، وأساس ذلك هو اختلاف طبيعة البطاقة عن طبيعة المحرر الورقية، وعزز اتجاهه بقوله بتبني أغلب التشريعات المقارنة للطبيعة الورقية للمحررات محل جريمة التزوير، وبالتالي استبعاد غيرها من المحررات ذات طبيعة مغايرة عن ذلك, خاصة وأن المشرع جاء بعبارات ونصوص صريحة توضح أن وعاء التزوير يجب أن يتمثل في أوراق أو تقارير أو سجلات أو دفاتر ورقية، وإلى جانب ذلك أن المشرع قد جاء بنصوص محددة ومختلفة عما سبق ذكره عندما أراد بتوقيع العقاب على التزوير الواقع على غير الأوراق؛ أي أن المشرع لما سعى إلى تجريم التزوير الواقع على وعاء آخر يختلف عن الأوراق, جاء بنصوص محددة وقاطعة كتخصيص نصوص لتجريم تزوير العملات النقدية، كما أنه جاء بنصوص خاصة ومحددة بشأن التزوير الواقع على الأختام [2].

كما أن تطبيق نصوص جريمة التزوير يتطلب أن يتخذ محل الجريمة مظهر المحرر الذي يحتج أو يمكن الاحتجاج به قانوناً بخصوص ما يتضمنه من بيانات أو وقائع يراد إثباتها، الأمر الذي لا يمكن أن يتوافر في البطاقة، إذ أنها ليست محرراً معداً للإثبات وفقاً للقانون؛ لأنها ليست معدة للتداول بين الناس، إذ الغرض منها أنها خاصة بصاحبها فقط، بل أنها لا تستخدم في بعض الأحيان إلا بتقديم مستند أو وثيقة رسمية كالهوية الشخصية التي ينبغي أن تتطابق البيانات الواردة فيها مع البيانات الواردة في بطاقة الدفع الإلكتروني[3].

ب – إمكانية إسقاط وصف المحرر على بطاقة الدفع الإلكترونـي:

تتجه طائفة من الفقه[4] إلى تأييد تطبيق نصوص جريمة التزوير على التغيير الواقع على الشكل المادي لبطاقة الدفع الإلكتروني، فإذا كان الغالب في المحرر أن يتم تثبيته على الورق باعتباره الوسيلة الأسهل

1 فتحية محمد قوراري، المرجع السابق، ص 158.

2 أحمد حسام طه تمام، المرجع السابق، ص 543.

3 هدى حامد قشقوش، المرجع السابق، ص 65-66.

4 عفيفي كامل عفيفي، المرجع السابق، ص 170.

والأكثر مرونة لنقل الأفكار من شخص لآخر، إلا أن هذا لا يمنع أن يكون المحرر ذا طبيعة غير ورقية، فلا يمنع من حيث المبدأ وجود حائل قانوني أو فني من أن تكون المادة التي يتم تثبيت البيانات أو المعلومات عليها مصنوعة من البلاستيك أو المعدن أو أي مادة أخرى، والأمر كذلك بالنسبة للأشرطة أو الأسطوانات أو الأقراص الممغنطة المرنة أو الصلبة, بحيث تصلح لأن تكون وعاء للمحرر الذي يتضمن الفكرة التي ينبغي نقلها إلى الغير.

فإذا كان ما يمكن التوصل إليه مما تقدم هو أن الشكل المادي للبطاقة ذو الطبيعة غير الورقية يصلح من حيث المبدأ لأن يكون وعاء للمحرر شأنه شأن أي طبيعة أخرى، فإن ما يترتب على ذلك وكنتيجة منطقية للأمر فإن التغيير الذي يقع على المحررات المصنوعة من مواد أخرى, يمكن أن يحقق التغيير المتطلب في جريمة التزوير متى تم استخدامها كمادة يصنع منها المحرر، الأمر الذي يمكن القول على أساسه أن ينطبق وصف المحرر على المادة المصنوعة منها البطاقة[1].

غير أن وصف المحرر لا يتوقف على المادة التي يصنع منها، فإلى جانب ذلك لا بد أن يحتوي على مضمون تحدده الكتابة والمعلومات التي يتضمنها, والتي ينبغي أن تتوافر فيها صفات منها أن تكون معبرة عن فكرة قانونية، وأن يتم إدراكها بصورة مباشرة؛ أي قابليتها للقراءة البصرية وليس عن طريق الآلة إلى جانب إمكانية التعرف على شخص واضعها[2].

إن تطبيق هذه المواصفات على الشكل المادي لبطاقة الدفع الإلكتروني يؤدي بنا إلى القول بأننا لا نعتقد أن الشكل المادي للبطاقة يخرج عن هذه المواصفات بما فيه من بيانات تعبر عن فكرة قانونية، ويمكن قراءتها بصورة مباشرة دون أن تتدخل الآلة في ذلك, إلى جانب أنه من الممكن التعرف على الجهة التي أصدرتها، حيث يعد ذلك من البيانات الأساسية التي تحرص الجهات التي تصدرها على وضعه بشكل واضح.

ويذهب جانب آخر من الفقه[3] بشأن التغيير الذي ينال من بطاقة الدفع الإلكتروني إلى القول بأن وصف المحرر المتطلب توافره بشأن جريمة التزوير باعتباره المحل الذي يقع عليه التغيير أو التلاعب ينطبق على بطاقات الدفع الإلكتروني لجملة من الأسباب:

1 **Jean Devèze**, Instruments de paiement et de credit, disponible en lingne á l'adresse suivante: http://197.14.51.10:81/pmb/COURS%20ET%20TUTORIAL/DROIT/Droit%20Prive/Instrumets%20de%20paiement%20et%20de%20credit.

2 غنام غنام، المرجع السابق، ص 180.

3 محمد الشوابكة، المرجع السابق، ص 202.

- **أولًا:** كونها تنطوي على معلومات وبيانات يتطلب الأمر أن يقع عليه التغيير الذي ينال من المحرر.
- **ثانياً:** إلى جانب أن بطاقة الدفع الإلكتروني عبارة عن قطعة من البلاستيك تصدر عن إحدى المؤسسات المالية، وتحمل بيانات خاصة بالحامل ورقماً خاصاً, وتاريخ معين يبين تاريخ صلاحيتها.
- **ثالثاً:** إن المساس بالبيانات الخاصة ببطاقة الدفع الإلكتروني يشكل الركن المادي لجريمة التزوير.

وبهذا فإن شكل البطاقة ينطبق عليه وصف المحرر؛ لأنه يحمل بيانات في مجملها تجعل البطاقة مستنداً يمكن استخدامه فيما أعد له، لذلك نصل إلى نتيجة مهمة هي أن التغيير الذي يمس بيانات البطاقة أو يتعرض لشكلها وإن كانت مصنوعة من مادة بلاستيكية في الغالب, من شأنه أن يحقق التغيير المتطلب لتحقق جريمة التزوير؛ لأنه ليس هناك ما يمنع من إسقاط وصف المحرر عليها, لذلك يعد مرتكباً للتغيير المحقق لجريمة التزوير في محرر من يقوم بأي عملية شطب أو حذف أو تغيير للأرقام, أو المعلومات التي تتضمنها البطاقة شأنها في ذلك شأن التزوير في المحررات الورقية[1].

الفرع الثاني: المواجهة التشريعية لمكافحة جريمة تزوير بطاقة الدفع الإلكتروني.

يتحدد الإطار القانوني لجريمة تزوير بطاقة الدفع الإلكتروني وفق مجموعة من النصوص الواردة في الاتفاقيات الدولية والتشريعات الداخلية لإضفاء الحماية الجزائية ضد كل الاعتداءات المحققة للتغيير والتزييف في حقيقة البطاقات، وهذه الحماية شملت المجال الدولي على مستوى الاتفاقيات المبرمة على المستوى الدولي أو الإقليمي، وكذا التشريعات الداخلية المقارنة التي عملت عل محاربة هذه الجريمة لما لها من انعكاسات خطيرة على مستوى المعاملات المالية الإلكترونية.

أولاً: الإطار القانوني لحماية بطاقة الدفع الإلكتروني من جريمة التزوير على المستوى الدولي:

تعد جريمة التزوير من الجرائم التي أولاها المشرع الدولي أهمية بالغة, بحيث خصص لها مساحة واسعة من التشريع ضمن النصوص الواردة في الاتفاقيات والتوصيات الناتجة عن المؤتمرات الدولية، وهذا التوسع في التشريع الجنائي ضد جريمة تزوير بطاقة الدفع الإلكتروني يجد مبرره من خلال انتشار المعاملات الإلكترونية التجارية والمالية، واستغلال فئة من العصابات الدولية هذا الفضاء للاعتداء على الأموال من خلال تزوير بطاقة الدفع الإلكتروني على نطاق واسع, وهو ما يدخل في إطار الجريمة المنظمة، والتي يعمل فيها الجناة على الحصول على البيانات الخاصة لبطاقات الدفع الإلكتروني من دولة ثم تزويرها في دولة أخرى، وترويجها

1 محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الائتمان الممغنطة، المرجع السابق، ص 538.

للتعامل في دولة ثالثة للحيلولة دون ملاحقتهم، لذا بادرت منظمات دولية لمكافحة هذا النوع من الجريمة تبعاً للصفة الدولية التي تخولها متابعة نشاط هؤلاء الجناة، وبهذا استلزام وجود أساس قانوني دولي تعتمد عليه هذه المنظمات في توفير الحماية القانونية, وهذا ما سنبينه وفقاً لما يأتي:

1. موقف اتفاقية بودابست في مواجهة تزوير بطاقات الدفع الإلكترونـــي:

تعتبر اتفاقية بودابست الاتفاقية الخاصة بمكافحة الإجرام الافتراضي، ولقد تضمنت ديباجتها إشارة لجريمة تزوير بطاقة الدفع الإلكتروني (إن ظهور الثورة الإلكترونية في عالم المعلومات ضاعف من ارتكاب الجرائم الاقتصادية ومنها الغش والاحتيال والتزوير في بطاقات الائتمان, فالأصول المالية التي يتم تداولها بواسطة الحاسب الآلي أصبحت هدفاً للتداول).

كما أن الإتفاقية أشارت إلى مدلول جريمة التزوير من خلال نص المادة السابعة (07) منها بأنه: "إدخال أو إفساد أو تعطيل أو محو أو شطب عن قصد وبدون وجه حق ولقد حددت الاتفاقية أساليب التزوير في طرق معينة كالإدخال أو إفساد أو تعطيل أو شطب البيانات الإلكترونية وبدون وجه مشروع"[1].

وأما المادة الثامنة فقد وضعت التزاماً على عاتق كل دولة طرف في الاتفاقية باتخاذ الإجراءات التشريعية, أو أي إجراءات أخرى ضرورية لتأسيس الحماية الجنائية ضد الجرائم التي تسبب في إحداث ضرر مالي للغير عن عمد وبشكل غير مشروع، وحددت أساليب ارتكاب تلك الجرائم وفقاً لما يلي:

- الإدخال أو الإتلاف أو المرور ضمن نشاطات الحاسب الآلي بغية تغيير حقيقة البطاقة وتزويرها؛
- اعتماد أي شكل من أشكال الاعتداء على الحاسب الآلي بنية الغش, أو أي نية إجرامية مشابهة للغش من أجل الحصول بدون وجه حق على منفعة اقتصادية لمرتكب الفعل[2].

وإن كان ما يلاحظ أن أحكام الاتفاقية قد أغفلت النص على أسلوب التغيير في المعطيات الإلكترونية لبطاقة الدفع الإلكتروني، إلا أنها منحت الأطراف الحرية في النص في تشريعاتها الداخلية على أساليب التجريم وفق ما يتماشى مع هدف الاتفاقية ومضمونها، وهذا ما يجعل التشريعات المقارنة ملزمة بضبط أساليب التزوير بشتى أشكالها, وعلى رأسها فعل التغيير الذي يمثل النشاط الإجرامي الأساسي لجريمة تزوير بطاقات الدفع الإلكتروني.

1 علي سالم، المرجع السابق، ص 136.

2 جميل الصغير، الانترنت والقانون الجنائي، المرجع السابق، ص 43.

2. موقف الاتفاقيات الدولية تحت رعاية الانتربول من جريمة تزوير بطاقة الدفع الإلكتروني:

تعد منظمة الشرطة الدولية (الانتربول) من أهم المنظمات الدولية الفعالة في مجال مكافحة الإجرام الدولي بصفة عامة والإجرام الإلكتروني على وجه خاص، وهذا لتكوين المنظمة من فروع وأقسام خاصة كشعبة الإجرام الاقتصادي والمالي وشعبة التقصي الآلي وتحليل المعلومات، ويظهر دورها الفعال أيضاً عن طريق التعاون المتبادل في مجال مكافحة ومنع استفحال الجريمة المنظمة بتبني خطط مستمرة ودائمة لمتابعتها.

ولقد عملت المنظمة في إطار مكافحة الجرائم الواقعة على وسائل الدفع الإلكتروني, وبالأخص بطاقة الدفع الإلكتروني، وهذا بناءً على توصيات هامة استخلصت من المؤتمرات الدولية الخاصة بمكافحة الاحتيال والغش في البطاقات الإلكترونية الائتمانية، وتبلورت أهم التوصيات فيما يلي:

- إنشاء مجموعات عمل من الشرطة الدولية ذات خبرة في مجال التصدي لجرائم الغش والتزوير على المستوى الدولي، ووضع أسس خاصة بالتبادل المعلوماتي بين الدول المهتمة بمكافحة الظاهرة للحد منها.
- تحسيس الدول بضرورة مراجعة التشريعات الداخلية في مجال تنظيم الحماية الجنائية لبطاقة الدفع الإلكتروني بتجريم كل أفعال التصنيع, أو امتلاك أي معلومات غير قانونية تم الحصول عليها بسبل غير مشروعة واستخدامها في نظام بطاقة الدفع الإلكتروني.
- كما عملت المنظمة على خلق مبادرات تعاون فيما بينها وبين المنظمات الراعية لإصدار بطاقات الدفع الإلكتروني لمكافحة الجرائم الواقعة عليها، وهذا ما تمخض عنه جملة من التوصيات الصادرة في إطار خمس اتفاقيات دولية.

3. موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 من تزوير بطاقة الدفع الإلكترونـــــي:

تعتبر الإتفاقية العربية لمكافحة جرائم تقنية المعلومات من أهم الاتفاقيات على المستوى الإقليمي التي حددت جملة من الأهداف في الحد من جرائم المعلومات والآثار السلبية لها، ومن خلال الرجوع إلى أحكام الاتفاقية نجد أنها جرمت الاعتداءات الواقعة على البيانات والمعلومات بصفة عامة وجرمت التزوير الإلكتروني بوجه خاص فنجدها أقرت في نص المادة العاشرة (10) منها تعريفاً خاصاً بالتزوير الإلكتروني, حيث عرف بأنه:"استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر ونية استخدامها كبيانات صحيحة".

واتبعت الاتفاقية العربية نهجاً مسايراً للتشريعات الدولية في مجال الاستخدام غير المشروع لوسائل تقنية المعلومات من أجل تغيير الحقيقة، وركزت بشكل خاص على تزوير بطاقات الدفع الإلكتروني التي خصصت له حكم في نص المادة 18 منها والتي جاءت كالآتي:

1- كل تزوير أو اصطناع أو وضع أي أجهزة أو مواد تساعد على التزوير أو تقليد أي أداة من أدوات الدفع الإلكتروني بأي وسيلة كانت.

2- تجريم الاستيلاء على البيانات أو أي أداة من أدوات استعمالها أو تقديمها للغير أو تسهيل الحصول عليها.

3- كذا استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في التوصل إلى أرقام أو بيانات تخص بطاقات الدفع الإلكتروني بشكل غير مشروع، وحتى أن الاتفاقية ضمنت تجريم قبول أي شخص بإحدى وسائل الدفع الإلكتروني المزورة مع علمه بذلك.[1]

وتعتبر الإتفاقية قد تصدت لتجريم أغلب أنواع النشاط الإجرامي في مجال الدفع الإلكتروني ومن بينها بطاقة الدفع الإلكتروني من خلال أبرز أساليب التزوير الماسة بشكل ومضمون بطاقة الدفع الإلكتروني، والحد من الآثار السلبية التي تنتجها على المستوى الاقتصادي والمالي، وهو ما يضع أيضاً التزاماً على الدول العربية بضرورة متابعة ورصد الظواهر الإجرامية في إطار الجريمة المنظمة, وتطبيق ما جاء في الفصل الرابع من الاتفاقية الخاص بمجال التعاون التشريعي والقضائي في هذا الصدد.

ثانياً: الإطار القانوني للحماية الجنائية من جريمة تزوير بطاقة الدفع الإلكتروني على المستوى الداخلي:

سنتعرض في هذا المقام لبيان موقف بعض التشريعات المقارنة التي تصدت للجرائم الواقعة إلى بطاقات الدفع الإلكتروني، وبالأخص جريمة التزوير وعلى رأسها التشريع الفرنسي والمشرع السعودي والإماراتي.

1. المواجهة التشريعية للمشرع الفرنسي لجريمة تزوير بطاقة الدفع الإلكترونــي:

لم يأت موقف المشرع الفرنسي من الاعتداءات التي تتعرض لها بطاقات الدفع الإلكتروني بالوضع الذي هو عليه دفعة واحدة، إنما جاء على مراحل وبنصوص شهدت تطوراً ملموساً لا يمكن للمتمعن فيها

1 محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الائتمان الممغنطة، المرجع السابق، ص 540.

إلا أن يكتشف تغيير وجهة نظر المشرع الفرنسي من القواعد التقليدية التي يحتويها قانون العقوبات ويمكن أن تحكم الاعتداءات التي تعترض تلك البطاقات, والاتجاه إلى القواعد الخاصة[1].

فموقف المشرع الفرنسي من جريمة تزوير بطاقة الدفع الالكتروني وليد التطور الحديث، حيث اعتبرها جريمة يجب أن تستقل عن نصوص جريمة تزوير المحررات العادية, فجاء بالقانون رقم 88/19 الصادر في 05 يناير 1988 والخاص بالغش المعلوماتي بالنص على تزوير واستعمال الوثائق المعلوماتية المزورة، وذلك حسب ما جاء بالفقرتين الخامسة (05) والسادسة (06) من المادة 462 التي أضافها القانون المذكور إلى قانون العقوبات الفرنسي قبل إلغائه حتى وصل إلى ماهو عليه.

وعلى أساس ذلك يعد قانون الغش المعلوماتي أول تشريع يتصدى فيه المشرع الفرنسي لجرائم الحاسب الآلي والجرائم المرتبطة بها، والذي يعد بذات الوقت القانون الذي أغلق باب الاجتهاد الفقهي وتناقض الأحكام القضائية الخاصة بتطبيق نصوص قانون العقوبات، أو النصوص العقابية التقليدية إن صح التعبير على التصرفات الإجرامية التي تستند على تسخير تقنية المعلومات، ويعاقب فيه المشرع بصفة خاصة على تزوير بطاقات الدفع الإلكتروني واستعمالها أهم الوثائق المعلوماتية المعالجة آلياً[2].

وقد جاء المشرع من خلال قانون أمن الشيكات وبطاقات الوفاء رقم 91/1382, وتحديداً من خلال نص المادة 68 التي تنص على أنه:"يعاقب بالحبس من سنة إلى سبع سنوات وبالغرامة من 3600 أورو إلى 500 ألف أورو أو إحدى هاتين العقوبتين كل من:

– استعمل أو حاول استعمال بطاقة وفاء أو سحب مقلدة أو مزورة وهو يعلم ذلك"[3].

وتعد خطوة المشرع هذه الخطوة التي أغفلت كل خلاف واستحكمت في بناءها على كل تناقض للأحكام، وخاصة أن المشرع الفرنسي في إطار قانون غش المعلوماتية لم يصرح بتطبيقها على البطاقات الممغنطة مثل ما فعل المشرع في هذا القانون الذي أشار صراحة لبطاقات الدفع، الأمر الذي تميز به عن القانون الخاص بغش المعلوماتية, ما دفع الفقه[4] إلى الاستنتاج بأن المشرع عالج ما تتعرض له بطاقات الدفع الإلكتروني حينذاك بصورة غير مباشرة.

---

1 علي عباس، المرجع السابق، ص 22.

2 HANACHOWICZ (L), Op. Cit, p 223.

3 Loi n° 91-1382 du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement (J.O du 1er janvier 1992 p12).

4 HANACHOWICZ (L), Op. Cit, p 223.

وما يلاحظ على اتجاه المشرع هو أنه كما جرم تزوير بطاقة الدفع الإلكتروني أو السحب جرم استعمال البطاقة المزورة، حيث جعل جريمة استعمال البطاقة المزورة أو المقلدة جريمة مستقلة عن جريمة التقليد أو التزوير، وهذا من شأنه أن يرتب نتيجة مهمة هي أن مرتكب جريمة تقليد أو تزوير البطاقة المزورة يسأل عن جريمة استعمال بطاقة مقلدة أومزورة حتى ولو لم يكن له في تزويرها ولم يساهم في ذلك أو يشترك فيه.

وإلى جانب ذلك، وفي نطاق تجريمه لاستعمال البطاقة المزورة أو المقلدة فقد جرم المشرع صورة هي بين الأعمال التحضيرية وبين البدء بالتنفيذ المحقق للشروع؛ تلك هي صورة المحاولة، وأعطاها ذات الحكم الذي أقره بشأن الجريمة التامة، فمن يحاول استعمال البطاقة المزورة، وعلة التشدد هذه هو حرص المشرع على حماية هذه الوسائل الحديثة في الوفاء بالمشتريات, بحيث يجرم مجرد المحاولة لاستعمالها بعد تزويرها.

2. المواجهة التشريعية للمشرع السعودي لجريمة تزوير بطاقة الدفع الإلكترونـــي:

عالج المشرع السعودي الاعتداءات التي تتعرض لها بطاقات الدفع الإلكتروني، وبالتحديد ضد تزويرها واستعمالها بعد التلاعب بها بنص خاص تضمنه نظام مكافحة التزوير المعدل بالمرسوم الملكي رقم 16 لسنة 2005, الذي أضاف المادتين الثالثة عشرة (13) والرابعة عشر (14) إلى النظام المذكور، وقد جاءت المادة الثالثة عشر (13) من المرسوم السابق تجرم كل شخص قام بعملية تزوير بطاقة الدفع أو السحب الصادرة عن البنوك أو المؤسسات المالية، وهذا عن طريق الاصطناع أو التقليد أو تغيير بياناتها، وجرمت كذلك أفعال الاشتراك عن طريق التحريض أو الاتفاق أو المساعدة أو استعمال البطاقة المزورة مع علمه بذلك، وكذا استخدامها آلياً حتى لو لم يتحقق الغرض من الاستخدام، وعاقبت نفس المادة الجاني بمدة لاتزيد عن 10 سنوات أو بغرامة لا تزيد عن 50 ألف ريال أو بهما معاً[1].

وما يمكن ملاحظته على اتجاه المشرع السعودي هو أنه في الوقت الذي اتفق مع المشرع الفرنسي على تجريم تزوير بطاقات الدفع واستعمالها مع العلم بتزويرها، وكذا تجريمه لجريمة الشروع في استعمالها الأمر الذي يستفاد من عبارة "أو استخدمها آليا ولو لم يتحقق الغرض من الاستخدام.."، غير أنه اختلف عنه بأمر مهم يحتسب نقصاً تشريعياً ينبغي تداركه؛ ألا وهو عدم تجريمه لفعل التاجر الذي يقبل الدفع ببطاقة مزورة, وهو ما يمثل امتدادا لجريمة التزوير يستوجب العقاب عليه.

3. المواجهة التشريعية للمشرع الإماراتي لجريمة تزوير بطاقة الدفع الإلكتروني:

1 علي عبد القادر القهوجي، المرجع السابق، ص 64 وما بعدها.

يعاقب المشرع الإماراتي بالحبس والغرامة لا تقل عن 500 ألف درهم ولا تجاوز 2 مليون درهم, أو بإحدى هاتين العقوبتين على كل عمليات تزوير أو تقليد أو نسخ بطاقة ائتمانية أو بأي وسيلة أخرى من وسائل الدفع الإلكتروني, وذلك باستخدام تقنية المعلومات أو برنامج معلوماتي.

ويذهب المشرع إلى تحديد نفس العقوبة السابقة لكل من قام بعملية صنع أو تصميم وسيلة من وسائل تقنية المعلومات بقصد تسهيل أي فعل من أفعال التزوير أو التقليد المحددة سابقاً، وكذا استخدام بطاقة ائتمانية أو إلكترونية أو أي وسيلة من وسائل الدفع الإلكتروني بدون تصريح, بقصد الحصول لنفسه أو لغيره على أموال أو أملاك الغير، أو الاستفادة مما تتيحه من خدمات يقدمها للغير، وذهب المشرع لأبعد من ذلك بأن جرم قبول التعامل بالبطاقات المزورة أو المقلدة أو غيرها من وسائل الدفع الإلكتروني مع العلم بعدم مشروعيتها[1].

ثالثاً: أحكام الحماية الجنائية لجريمة سرقة أو استعمال بطاقات الدفع الإلكتروني المسروقة أو المفقودة.

ابتداءً تجب الإشارة إلى أن البطاقة مالاً يصلح من حيث المبدأ أن يكون محلاً للسرقة أو الاستيلاء عليه بوجه آخر، إذ أنها من حيث كونها بطاقة ذات طبيعة مادية وذات قيمة اقتصادية وأنها لا تخرج عن دائرة التعامل لا بحكم طبيعتها ولا بحكم القانون، مما يجعل طبيعتها المادية صالحة من حيث المبدأ في أن تكون محلاً لجرائم الأموال بشكل عام مهما تضاءلت قيمتها, وتم الاعتراض على ذلك لو تم النظر إليها من حيث مكوناتها المادية فحسب.

ولقد اتجه جانب من الفقه[2] إلى ضرورة التمييز بين استعمال البطاقة المسروقة أو استعمالها بعد فقدها من قبل حاملها الشرعي، وبرروا وجهة نظرهم بأن الاستيلاء على بطاقة بفعل جنائي أصلاً يختلف في الوصف والعقاب على فعل ينقلب إلى فعل جنائي بعد تحقق حالة ليس لإرادة الشخص الحائز دور في السعي إلى تحققها أصلاً, وإن كانت قد تحققت واقعة الحيازة بفعله.

كما أن سرقة بطاقة الدفع الإلكتروني يشكل فعلاً جنائياً بأصله كون الإرادة تنصرف فيه إلى تحقيق حالة الحيازة من خلال الوسائل التي استخدمها، الأمر الذي لا يتحقق في حالة استيلاء عليها بعد فقدانها، حيث أن الجاني عند العثور عليها وإن كان قد استعان بوسائل جعلت البطاقة في حيازته, إلا أنها تختلف في

1 المادة 13من القانون الاتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي السابق الذكر.

2 عماد خليل، المرجع السابق، ص 105.

مدى العلم والإرادة التي أنشأت هذه الحيازة حيث أنه لم يسع عن الوسائل التي تنشأ له هذه الحيازة بل إنها تحققت بصورة عرضية، وأساس هذه الدعوة إلى التمييز بين سرقة البطاقة وبين الاستيلاء عليها بعد فقدانها هو النتائج القانونية التي تترتب على مسؤولية الشخص في الحالتين، فحيث ينبغي أن يخضع فعل الجاني في حالة سرقة البطاقة إلى النصوص الخاصة بجريمة السرقة، حيث يعاقب الجاني بموجب النصوص الجنائية الواردة في قانون العقوبات ولا حاجة إلى نص خاص يجرم هذا الفعل[1]، وينبغي أن يخضع فعل الجاني في حالة الاستيلاء على بطاقة مصرفية مفقودة أو ضائعة إلى الأحكام الجنائية الخاصة بالأموال المفقودة التي جرمتها بعض التشريعات بنص خاص وألحقتها بجريمة خيانة الأمانة, كونها أقرب لفكرة الاعتداء على الائتمان من غيره.

1. أحكام المسؤولية الجنائية لجريمة سرقة بطاقة الدفع الإلكتروني:

على اعتبار أن بطاقة الدفع الإلكتروني هي مزيج من الشكل المادي للبطاقة والمكونات المعنوية المتمثلة في البيانات والمعلومات التي يتم دمجها بالشريط الممغنط، فإن الإشكال المثار في إطار أحكام جريمة سرقة بطاقة الدفع الإلكتروني يقوم على أساس بحث مدى تطبيق نصوص جريمة السرقة على الاستيلاء على الشكل المادي البطاقة بما يحوي من شريط ممغنط، وكذا الاستيلاء على المعلومات أو البيانات الخاصة ببطاقة الدفع الإلكتروني؟

وإن كان الرجوع إلى تحليل فعل الجاني الذي ثبت حصوله على بطاقة الدفع الإلكتروني بعد ضياعها من حاملها الشرعي، يذهب بنا إلى ضرورة عدم مساءلة الجاني عن جريمة سرقة البطاقة لانتفاء القصد الجرمي المتمثل في نية التملك، وهو المعيار لقيام جريمة السرقة، بحيث أن الحيازة العرضية أو المؤقتة لا تكفي لتحقق القصد الجنائي للجريمة.

إلا أن جانب من الفقه الجنائي[2] رأى ضرورة التوجه في مجال التشديد في الحماية الجنائية, إذ يؤكد على عدم التفريق بين مجرد الانتفاع بالشيئ بشكل غير مشروع وبين سلب قيمته، بحيث أن حيازة البطاقة المفقودة بنية استعمالها وإرجاعها إلى صاحبها، لا ينزع عنه فعل استنزاف قيمتها, الأمر الذي يجعل من البطاقة عديمة القيمة.

1 فتحية محمد قوراري، المرجع السابق، ص 50.

2 أحمد حسام طه تمام، المرجع السابق، ص 204.

كما أن اقتران حيازة البطاقة مع استعمالها واستنزاف قيمتها يشكل في الحقيقة قوام فعل الاختلاس على اعتبار أن المال محل السرقة هو قيمة البطاقة المستعملة، هذا بالإضافة إلى توافر القصد الجنائي حتى وإن اتجهت نية الجاني إلى استعمال البطاقة وإعادتها إلى صاحبها, فهذا لا ينفي اتجاه إرادته في امتلاك قيمة البطاقة وهو ما يشكل جريمة السرقة.

2. قيام المسؤولية الجنائية لسرقة المكونات المادية لبطاقة الدفع الإلكترونـي:

إن بطاقة الدفع الالكتروني عبارة عن قطعة بلاستيكية مكتوب عليه بحروف نافرة اسم حاملها وتاريخ إصدارها وتاريخ انتهاء صلاحيتها، بالإضافة إلى رقمها التسلسلي، وتحمل معلومات عن اسم الجهة المصدرة وشعارها، ويوجد خلف أغلبها شريط ممغنط وفي بعضها رقاقة حاسوبية تسجل عليها بعض المعلومات المهمة حسب عمل المؤسسة ونوعية البطاقة.

وهذا الكيان المادي قد يثير الاستيلاء عليه مشاكل قانونية سواءً بثبوت صفة المال لها أو في نطاق صلاحيتها لفعل الاختلاس ولو كانت ذات قيمة بسيطة, فهي بكل الأحوال غير مجردة من القيمة، وأنها ذات طبيعة مادية منقولة، وهو الأمر الذي يتطلبه تحقق جريمة السرقة, والذي يشترطه جانب من الفقه[1] في الأموال التي تصلح أن تكون محلاً لجريمة السرقة، فحسب رأيه أن شكل البطاقة المادي شأنه شأن أي منقول مادي آخر.

وإن كان التوغل في فكرة الاستيلاء على المكونات المادية للبطاقة يجعلنا نتوصل إلى أن سرقة تلك المكونات لا يعطي المحل الذي وقعت عليه أفعال الاستيلاء طابعاً خاصاً، مما يعني أنه تبقى الأفعال الموجهة ضد المكونات المادية في نطاق الجرائم العادية, ولا يمكن إعطاؤها وصفاً خاصاً على اعتبار أنها مال منقول ذات طبيعة خاصة، ولا يمكن أن يحدث تميز بشأن القواعد القانونية التي يمكن أن تنطبق على جريمة سرقتها لا من حيث التكييف ولا من حيث ظروف تشديد العقاب، بل إن الخطورة تكمن في الباعث من سرقتها؛ أي فيما تحتويه هذه البطاقات من معلومات تمكن الجاني من استخدامها في الأغراض التي سعى عليها.

3. قيام المسؤولية الجنائية لجريمة سرقة المكونات المعنوية لبطاقة الدفع الالكتروني:

أضحى الدفع الإلكتروني يشكل شرياناً هاماً في مجال المعاملات الإلكترونية بين المؤسسات والأفراد والمتعاملين الإقتصاديين، وبهذا أصبحت بطاقة الدفع الإلكتروني تمثل آلية هامة لقيام عمليات الشراء والبيع

1 خالد عياد الحلبي، المرجع السابق، ص 133.

عبر مواقع الانترنت, وهذا بتزويد التاجر رقم البطاقة الخاصة بالزبون ومعلومات أخرى لتصله بذلك السلعة أو الخدمة المطلوبة خلال الفترة الزمنية المتفق عليها، ثم يأتي دور المؤسسة المالية كوسيط لاقتطاع قيمة المعاملة وتحويلها إلى رصيد التاجر مع احتساب الفوائد والعمولات وفقاً للاتفاقيات المبرمة بين أطراف المعاملة الإلكترونية[1].

وهنا تُثار إشكالية وقوع جريمة سرقة المكونات المعنوية لبطاقات الدفع الإلكتروني فيما يخص الرقم السري والرصيد المحتوى ضمن بطاقة الدفع الإلكتروني، ومن ثم إمكانية التلاعب في هذه المكونات والاستيلاء على الأموال التي تتضمنها هذه البطاقة في التعاملات المالية.

وبالرغم من ميزة التعامل ببطاقة الدفع الإلكتروني، إلا أنها شكلت مجالاً خصباً لفئة من مجرمي المعلوماتية والقراصنة لسلب أموال الأفراد بطرق إجرامية حديثة تعكس مواطن الضعف التي تكتنف أنظمة الدفع الإلكترونية، وهنا نبين بعض الأساليب المنتشرة للاستيلاء على المكونات المعنوية لبطاقة الدفع الإلكتروني:

أ- تقليد المواقع التجارية الإلكترونية:

يلجأ الجناة من خلال هذا الأسلوب لاستهداف المواقع التجارية الإلكترونية لسرقة أرقام البطاقات السرية والمعلومات الخاصة بطريقة التعامل بها، بحيث يقوم هذا الأسلوب على إنشاء مواقع مبيعات مقلدة مماثلة لمواقع ويب حقيقية للبيع، والتشابه بينها قد يكون كبيراً إلى حد التماثل من خلال التخطيط والبيانات والنماذج والرسومات, وهذا بغرض تمويه المستهلكين والحصول على معلومات وبيانات بطاقات الائتمان وأرقامها السرية الخاصة بهم .

فبعد إنشاء هذه المواقع، يعمل قراصنة الانترنت بعرض منتوجات عامة بأسعار منخفضة ومبهرة لإغراء المستهلكين وحثهم على إرسال طلبات الشراء، التي يتبعها عملية الإرسال لمعلوماتهم الائتمانية، وهذا الأسلوب يطلق عليه بعض الفقه بالصنارة أو الفخ[2].

ب- الاختراق غير المشروع لأنظمة خطوط الاتصالات العالمية:

وهو أسلوب اختراق غير قانوني لمنظومة الخطوط التي تربط الحاسب الآلي لأطراف المعاملة الإلكترونية، ويعد الجاني هنا كمتنصت على مكالمة هاتفية، بحيث يستخدم الجناة في هذا الأسلوب برامج

1 محمد الشوابكة ، المرجع السابق، ص 202.

2 محمد أمين أحمد الشوابكة، المرجع السابق، ص 144.

تمكنهم من الاطلاع على البيانات والمعلومات الخاصة بالأفراد والمؤسسات المالية المصدرة لبطاقة الدفع الإلكتروني على شبكة الانترنت، وهذا الأسلوب يمثل أخطر الطرق المهددة لنظم التقنية والتفوق على الحماية المقررة لها وتعقيداتها.

وعلى الرغم من صعوبة تحديد شخصية المخترقين لأنظمة خطوط الاتصالات، إلا أنه من الممكن تحديد كيفية الاختراق وتوقيته، وذلك من خلال الملفات التأمينية الخاصة بنظام الدخول بما يسمح جمع أكبر عدد من الأدلة لتقصي أثر الجناة واكتشافهم.[1]

ج- تقنية تفجير المواقع التجارية الإلكترونية:

يستند مجرمو الانترنت على تقنية تفجير المواقع التجارية المستهدفة، وذلك بضخ مئات آلاف من الرسائل الإلكترونية (E-mils) من جهاز الحاسوب الخاص بالمجرم إلى الجهاز المستهدف بهدف التأثير على السعة التخزينية، بما يؤدي إلى تفجير الموقع العامل على الشبكة، وتشتت المعلومات الخاصة به[2]، ليتمكن هؤلاء القراصنة من التجول بحرية في هذه المواقع والحصول على جميع المعلومات المتضمنة بيانات وبطاقات الدفع الإلكتروني وجميع أسرار المعاملات التجارية أو المالية القائمة عن طريق التحويل الإلكتروني أو أي أسلوب آخر من وسائل الدفع، وبهذا تكون مصلحة الأفراد معرضة للتعدي نتيجة هذه التصرفات الإجرامية.[3]

رابعاً: المواجهة التشريعية لجريمة سرقة أو استعمال بطاقة الدفع الإلكتروني المسروقة أو المفقودة:

اتجه المشرع السعودي كغيره من بعض التشريعات المقارنة التي حرصت على ضبط الحماية الجنائية لبطاقات الدفع الإلكتروني، وهذا ما أكده نص المادة الرابعة من نظام مكافحة الجرائم المعلوماتية السعودي بحيث حظرت الوصول دون مسوغ قانوني إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات.

---

1 علي عباس، المرجع السابق، ص 17.

2 إيهاب فوزي السقا، المرجع السابق، ص115.

3 ومن هذه الطرق ما ذكر على أحد رؤساء مجلس إدارة أحد المصارف السويسرية الشهيرة، الذي وقع ضحية هؤلاء القراصنة ، بحيث أن رئيس مجلس الإدارة أراد أن يوجد تقنية شراء آمنة عبر شبكة الانترنت، فحشد طاقات فنية هائلة متخصصة في تطوير برمجيات الحاسوب، وعند نجاحه في إيجاد التقنية، ومحاولته لعرضها للتجربة من خلال مؤتمر صحفي، تبين أن هذه المجموعة قد اخترقت الخط الآمن، وأجرت حركة واحدة بسقف بطاقة رئيس مجلس الإدارة كاملا والبالغ 80 ألف دولار أمريكي من خلال أحد مراكز التسوق الكبرى في لندن. **للمزيد انظر:** كوثر سعيد عدنان، المرجع السابق، ص 600.

ولعل النص لم يشر إلى بطاقة الدفع الإلكتروني بشكل مباشر، إلا أنه ضمن الحماية الشاملة للبيانات الائتمانية أو البنكية, وهذا ما يتضمن في فحواه كل وسائل الدفع الإلكتروني المستخدمة في المعاملات الإلكترونية وتأمين البيانات والمعلومات المتعلقة بملكية أموال أو خدمات، وكذا إن مصطلح "الوصول دون مسوغ قانوني" المستخدم في النص هو مصطلح مرن يسمح بإدخال شتى أفعال الاستيلاء أو الاختلاس المكونة لجريمة سرقة المكونات المعنوية لجريمة سرقة بطاقة الدفع الإلكتروني، وكما أن المشرع قد حدد عقوبة السجن التي لا تزيد مدتها عن ثلاث سنوات, وبغرامة لا تزيد عن اثنين (2) مليون ريال أو بإحدى العقوبيتين لكل شخص يرتكب الأفعال المبينة سابقاً.

وأما المشرع الإماراتي فقد عاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق عن طريق استخدام الشبكة المعلوماتية أو نظام معلومات إلكتروني, أو بإحدى وسائل تقنية المعلومات إلى أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية، وتكون عقوبة الحبس مدة سنة وبغرامة لا تقل عن (100) ألف درهم, ولا تجاوز ثلاثمائة (300) ألف درهم أو بإحدى هاتين العقوبتين, إذا قصد من ذلك استخدام البيانات والأرقام في الحصول على أموال الغير أو الاستفادة مما تقدمه خدمات.

فإذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير فيعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (200) ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين، ويعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من نشر أو أعاد نشر أو أرقام أو بيانات بطاقة الدفع الإلكتروني للغير.

بدوره المشرع الأردني يعاقب كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الدفع الإلكتروني أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار.

وأما المشرع التونسي فقد اهتم بتنظيم مسألة الالتزامات الواقعة على صاحب البطاقة والجهة المصدرة لها بعد سرقة بطاقة الدفع الإلكتروني أو استعمالها في الفصل 37 من قانون المبادلات والتجارة الإلكترونية لسنة 2000، بتحديد التزام يقع على حامل البطاقة بإعلام الجهة المصدرة لها بواقعة سرقتها أو ضياعها او سرقة الوسائل التي تمكن من استعمالها، كما أن المشرع ألزم صاحب البطاقة بتحمل مسؤولية نتائج سرقة أو

ضياع البطاقة أو استعمالها المزيف من قبل الغير وهذا قبل فترة إعلام الجهة المصدرة بجريمة سرقتها أو فقدانها، ولا يتحمل أي مسؤولية عن ذلك فور إعلام الجهة المصدرة للبطاقة.

المبحث الثالث:

الحماية الجزائية المقررة من خلال أعمال مقدمي خدمات الانترنت.

بعدما أضحى الانترنت وسيلة مفتوحة لانسياب وتدفق المعلومات ونقطة انطلاق لإقدام الأشخاص على شتى التعاملات، فإن الواقع العملي يُثبت أن قيام المعاملات الإلكترونية عبر شبكة الإنترنت بحاجة إلى تعاضد جهود الأشخاص القائمين على إدارتها، والذين تتنوَّع مهامهم وأنشطتهم في تشغيلها، فحتى يتمكن مستخدموا الإنترنت من الدخول إلى الشبكة، والوصول إلى ما يصبون إليه من معلومات أو بثِّها، لا بُدَّ من وجود عدَّة أشخاص، يُطلق عليهم عادةً مصطلح "مقدمي خدمات الإنترنت"، أو "الوسطاء في خدمات الإنترنت"، يتولُّون عملية إيواء المعلومات، وبثِّها، وعرضها. وهذا التنوُّع في أدوارهم والتعدُّد في أنشطتهم يجعل من اليسير عليهم تتبُّع النشاط المعلوماتي غير المشروع وكشفه، إلاَّ أن تحقيق ذلك يبقى رهن قيد ضوابط قانونية تُحدِّد حقوق أطراف النشاط الإلكتروني والتزاماته في مواجهة بعضهم البعض من جهة، وفي مواجهة المجتمع الذي يعيشون فيه من جهةٍ أُخرى.

لذا بدت الحاجة ماسة لإيجاد تنظيم تشريعي متكامل يُحدد المركز القانوني لمقدمي خدمات الإنترنت، ويُبين في نفس الوقت مسؤولية كلٍّ منهم عمّا يُرتكب من مخالفات عبر الشبكة، الأمر الذي لا يُمكن تحقيقه إلا بتضافر تشريعي على الصعيدين: الوطني والدولي، من هنا تبدو أهمية بيان الحماية الجزائية المقررة من خلال تحديد المسؤولية الجنائية لمقدمي خدمات الانترنت، والذي سنستعين في إيضاحها بتجارب الدول التي سبقتنا في تنظيم هذا المجال، بخاصَّةٍ موقف التشريع الأوروبي والفرنسي، ثم آراء الفقه وكذا التشريعات العربية المقارنة المهتمة بتنظيم المسألة.

وتأسيساً على ما تقدم، نتناول دراسة "النظام القانوني لمقدمي خدمات الإنترنت" من خلال مطلبين؛ نخصص الأول لماهية مقدمي خدمات الانترنت، أما المطلب الثاني فيخصص لأحكام المسؤولية الجنائية لمقدمي خدمات الإنترنت.

المطلب الأول: مفهوم مقدمي خدمات الانترنت.

إن قيام المعاملات الإلكترونية عن طريق شبكة الانترنت يستدعي تداخل جملة من الأنشطة لعدة جهات تبدأ من مرحلة تزويد خدمة الانترنت للمتعامل الإلكتروني, والذي يتولاه ما يطلق عليه باسم "مقدم خدمة الانترنت" أو "متعهد الوصول" أو "مزود الخدمة"، بحيث تأخذ طبيعة عمله صفة فنية بحتة على اعتبار أنه يمثل أداة ربط بين المستخدم وخدمة الانترنت عن طريق عقود اشتراك تؤمن لهم الدخول إلى هذه الخدمة، ثم يأتي دور الوسطاء الفنيين في خدمة الانترنت، والذين تتشعب أدوارهم حسب نمط الخدمة المقدمة.

وهنا نجد التشريعات المقارنة قد حددت الأنماط الثلاثة من الوسطاء؛ وهم "متعهد خدمة التوصيل" fournisseur d'accés و"متعهد الإيواء" fournisseur d'hébergement، و"مقدم المضمون" contenu ou fournisseur Editeur وفي هذا الصدد سيتم بيان تعريف لكل من هؤلاء الوسطاء وتحديد الالتزامات المنوطة بكل فئة وفقاً للتشريعات الدولية والمقارنة فيما يأتي:

الفرع الأول: تعريف مقدمي خدمات الانترنت.

لبيان مفهوم مقدمي خدمة الانترنت، ينبغي التطرق إلى تعريف متعهد الوصول أو مزود خدمة الانترنت, وكذا بيان مفهوم وسطاء تقديم خدمة الانترنت من متعهد الإيواء وناقل المضمون.

البند الأول: تعريف مزود أو متعهد خدمة الانترنت.

يعرف مزود خدمة الانترنت (ISP) وهي اختصار لكلمة (Internet Service rovider) بأنه شركة تقدم خدمة توصيل للانترنت, فهو الممر الالزامي لوصول المستخدم إليها، فهو يلتزم تقنياً بوصل المستخدمين بالشبكة من خلال أجهزة المودم[1]. ولقد جاء المشرع الأوروبي من خلال التوجيه الأوروبي رقم 2000-31 الخاص ببعض الأوجه القانونية لخدمات شركات المعلومات وبصفة خاصة التجارة الإلكترونية[2] بمفهوم

1 Valérie Sédallian, Droit de l'internet: Réglemetation, Responsabilité, Contras, Collection Association des utilisateurs d'internet, Net press.1997, p123.

2 Directive 2000/31/CE du 08 juin 2000 relative à certains aspects juridiques de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (J.O n° L 178 du 17 juillet 2000), p.1-16

المتعهد خدمة الانترنت في نص المادة 12/ب على أنه :"أي شخص طبيعي أو معنوي يقدم خدمة الانترنت في مجتمع الخدمات المعلوماتية".

ولقد عرفه المشرع الفرنسي وفقاً لنص المادة 9 من القانون رقم 575-2004 المتعلق بالثقة في الاقتصاد الرقمي على أنه: "الشخص الذي يؤمن نشاطه خدمة التوصيل بشبكة اتصالات إلكترونية".

وعرفه المشرع الجزائري بموجب الفقرة "د" من المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات".

من خلال المفاهيم السابقة نستطيع القول بأن مزود الخدمة أو متعهد خدمة الانترنت هو شخص طبيعي أو معنوي متمثلاً بشركات الانترنت, تقتصر مهمتها على دور تقني بحت يتمثل في توصيل المستخدم بخدمة الانترنت، وهو غير مسؤول عن انتقال المعلومات أو المحتويات.

البند الثانـــي: متعهد خدمة الإيواء.

إن مصطلح الإيواء بمعناه الإلكتروني الواسع يشمل وضع الوسائل التقنية المعلوماتية بمقابل أو بالمجان, تحت تصرف الزبائن ليتمكنوا من الدخول إلى شبكة الانترنت في أي وقت لبث مضمون معين من نصوص أو صور أو أصوات للجمهور[1]، وبهذا يأخذ متعهد الإيواء أهمية لافتة من قبل التشريع نظراً لحساسية طبيعة المهام التي يقوم عليها، فهو المشرف الأول على تأمين مساحة نشر المضامين والمعلومات المتداولة إلكترونياً عبر الانترنت, وعن مدى مشروعيتها من عدمه.

ولقد عرفته المادة 14 من التوجيه الأوروبي حول التجارة الإلكترونية رقم 2000-31 بأنه:"عبارة عن نشاط يُمارسه شخص طبيعي أو معنوي، يهدف إلى تخزين مواقع إلكترونية وصفحات ويب (web pages) على حاسباته الآلية الخادمة بشكل مباشر ودائم مقابل أجر أو بالمجان، ويضع من خلاله تحت تصرف عملائه الوسائل التقنية والمعلوماتية التي تُمكنهم في أي وقت من بث ما يريدون على شبكة الإنترنت، من نصوص وصور وأصوات، وتنظيم المؤتمرات والحلقات النقاشية (forum de discussion)، وإنشاء روابط معلوماتية مع المواقع الإلكترونية الأخرى (liens hypertexts), ومن الوسائل التي يقدمها متعهد الإيواء لعملائه تخصيص مساحة قرص أو شريط مرور لبث المعلومات التي يرغبون بنشرها على شبكة الإنترنت،

1 Guide Permanent Droit et Internet, E 3.3 Hébergement du site, précité, nº 1 et 4, p. 4 et 5, Voir aussi: H. LANGLOIS, "La responsabilité des intermédiaires en matière de commerce électronique", Petites Affiches, 6 février 2004, n° 27, p. 28

وتزويد العميل بحساب خاص يتضمن مفتاح دخول (code d'accès) للتعريف به، وتزويده ببرنامج خاص يُمكنه من الاتصال بمتعهد الإيواء، وإضافة، أو حذف، أو تغيير ما يريد من معلومات[1].

ولقد جاء المشرع الفرنسي بمفهوم له في نص المادة 6 من القانون 2004-575 حيث عرفه بأنه: "كل شخص طبيعي أو معنوي الذي – حتى بدون مقابل– يتيح للجمهور عن طريق خدمات اتصالات عامة على الإنترنت تخزين الإشارات أو الكتابات أو الصور أو الأصوات أو الرسائل أياً كانت طبيعتها لفائدة مستعملي هذه الخدمات"[2].

أما المشرع الجزائري فقد عرفه بموجب الفقرة 2/د من المادة 2 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه: "أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال أو لمستعمليها".

البند الثالث: مقدم المحتوى المعلوماتـــي.

تعد مسألة توريد المعلومات عبر شبكة الانترنت للمستخدمين هي نشاط صادر عن مورد المعلومات باعتباره أحد وسطاء خدمة الانترنت، بحيث يقوم بتقديم المعلومة بصورة متعاقبة ومنتظمة، ولقد عرفه جانب من الفقه[3] بأنه كل شخص طبيعي أو معنوي يقوم ببث المعلومات والرسائل المتعلقة بموضوع معين على الانترنت، بحيث يتمكن مستخدم الشبكة التوصل إليها بمقابل أو مجاناً، بينما عرفه البعض الآخر[4] بأنه: "الشخص الذي يزود الوسطاء الآخرين بالمعلومات والبيانات التي تبث على الموقع فهو المسؤول عن تحديد مضمون ما يبث على المواقع، والبيانات التي يحددها هذا المورد في شكل نصوص مكتوبة أو صور أو قطع

1 Article 14/1 du Directive 2000/31/CE:" En cas de fourniture d'un service de la société de l'information consistant à stoker des iinformations fournies par un distinaire du service".

2 Article6/2 du lois n 2004-575 du 21 juin 2004 pour la connfiance dans l'économie numérique . Modifié par LOI n°2018-898 du 23 octobre 2018 - art. 29. dispose que:" Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services".

3 Feral-Schuhl christian; cyber droit, le droit à l'épreuve de l'internet,3 éd, Dunod,Paris, 2002, p129.

– **مشار إليه لدى:** عبد الفتاح محمود كيلاني، مدى المسؤولية القانونية لمقدمي خدمة الانترنت، بحث منشور على الانترنت متوفر على الموقع التالي:. *http://www.flaw.bu.edu.eg/flaw/images/part2.pdf*

4 Stowel (A) et Ide (N), Respnsibilité de intermidiares: Actualités législatives et jurisprudantilles, Droit et Nouvelle Teccchnologies, 10 Octobre 2000, p 1 .Disponible à l'adresse suivante*: //www.droit-technologi.org*

موسيقية أو علامات تجارية يعلن عنها، ويعرف مقدم المحتوى المعلوماتي باسم الناشر الإلكتروني الذي يتمثل في الشخص المحرر للرسالة ويضعها على الانترنت، مستخدماً خدمات الاتصال المختلفة وخاصة منها الانترنت التي عرفته بأنه:" الشخص الذي يشارك في إنشاء المحتوى أو أحد عناصره".

الفرع الثاني: التزامات مقدمي خدمات الانترنت.

تتجسد التزامات مقدمي خدمات الانترنت في المهام الموكلة للوسطاء الفنيين لخدمة الانترنت بمختلف أنواعهم من متعهد الوصول وناقل للمعلومات ومورد للمعلومات، والتي تتراوح بين الربط المادي لشبكات الاتصال عن بعد من أجل تسهيل عملية نقل المعلومات، وكذا تمكين مستخدمي الشبكة من الوصول إلى المادة المعلوماتية المتداولة عبر الانترنت.

إن استقبال رواد الانترنت للمعلومات المنشورة عبر شبكة الانترنت، يتم عبر مرحلة ربط الحاسبات الآلية بالمواقع الإلكترونية، وهو ما يقتضي توافر الربط مادياً عن طريق جهة مختصة وتتمثل غالباً في الهيئات العامة للاتصال، والتي تأخذ دور الناقل المادي للبيانات الذي يربط بالوسطاء الآخرين لخدمة الانترنت[1]، وهذا الالتزام يتولاه ناقل المعلومات الذي تشبه مهمته بساعي البريد الذي ينحصر التزامه في تأمين النقل المادي للمعلومات بين الأطراف المختلفة، وهو ما يميزه عن غيره من مقدمي خدمات الانترنت كمتعهد الإيواء ومورد المعلومات، فهو لا يتولى عملية التخزين المباشر الدائم للمادة المعلوماتية، وإنما جل عمله ينصب على عملية نقلها مادياً من وحدة لأخرى دون أن يكون مكلف بمراقبتها أو بمعرفة مضمونها.[2]

كما يتضح أن الالتزام المؤدى من قبل متعهد الوصول أو مزود الخدمة يتم عبر عقد اشتراك في الانترنت هو أشبه بعقد المقاولة يلتزم بمقتضاه متعهد الوصول بتقديم خدمة التوصيل لقاء مقابل يلتزم طالب الخدمة بدفعه، والملاحظ أن نشاط متعهد الوصول مختلف من حيث الطبيعة عن عمل متعهد الإيواء ومورد المعلومات واللذان يتحملان مسؤولية مراقبة مشروعية المعلومات والتحكم بها.

كما أن متعهد الإيواء يقدم لزبونه جملة من المعلومات ويضعها تحت تصرفه لمدة معينة وبمقابل معين، ويعتبر ذلك التصرف بمثابة عقد إيجار الأشياء، إذ يعرض إيواء صفحات ويب مقابل أجر معلوم ، ويكون

1 آلاء يعقوب النعيمي، الوكيل الإلكتروني مفهومه طبيعته، مجلة جامعة الشارقة للعلوم الشرعية والقانونية،الإمارات، المجلد 7، العدد 2، جوان 2010، ص 52.

2 أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الانترنت (دراسة تحليلية مقارنة)، مجلة المنارة، العدد 9، المجلد 13، سنة 2007, كلية الدراسات الفقهية و القانونية، جامعة آل البيت، الأردن، ص329.

للمستأجر نشر ما يشاء من نصوص أو صور وغيرها[1]، وبهذا يعد عقد الإيواء مهما لتحديد التزامات مزود الخدمة، بالإضافة لالتزام متعهد الإيواء الأصلي المتمثل بتقديم الوسائل التقنية والمعلوماتية التي تمكن المستخدمين من بث ما يرغبون من معلومات، فقد يقع على المتعهد التزامات تتمثل في بعض الخدمات الإضافية كتقديم المساعدة الفنية للزبائن أو المساعدة على إنشاء مواقع إلكترونية أو تقديم خدمات البريد الإلكتروني وأنظمة البحث الآلي[2].

كما أن التشريعات المقارنة قد أولت اهتماماً لتحديد الالتزامات الخاصة بمقدمي خدمات الانترنت فيما يخص مجال التحقيق والتحريات في ارتكاب الجريمة عبر الانترنت، وهو اعتمده كل من التشريع الجزائري والفرنسي، وهو ما نرجأه إلى أحكام الباب الثاني من الحماية الجزائية الإجرائية للمعاملات الإلكترونية.

المطلب الثاني: أحكام المسؤولية الجنائية لــمقدمي خدمات الانترنت.

تنشأ المسؤولية الجنائية عن أعمال مقدمي خدمات الانترنت عن نشر المعلومات والبيانات غير المشروعة عبر الانترنت، وهذا حسب الطرف المقدم لتلك الخدمة، إلا أن مسألة تحديد تلك المسؤولية أضحت أمراً لتقديم تلك الخدمة عبر فضاء غير مادي، وهو ما جعل موقف الاجتهاد الفقهي غير موحد، وفتح المسألة على عدة اتجاهات، البعض منها يدعو إلى إعفاء مقدمي خدمة الانترنت عن ترتيب المسؤولية الجنائية على عاتقهم لكون أن وظيفتهم المقدمة ذات طبيعة فنية تقنية مع استحالة تحقيق مراقبة لكل المعلومات المقدمة عبر شبكة الانترنت[3]، إلا أن البعض الآخر قد اتجه إلى القول بتحقيق المسؤولية ضدهم في كل الحالات، ولقد اتجهت أيضا الاجتهادات القضائية في الخوض في هذه المسألة طويلاً واتخذت أحكاماً قضائية مختلفة، لكن جلها كان يصب في إيجاد أساس لتحقيق المسؤولية الجنائية وفقاً لطبيعة تقديم

1 بوخالفة حدة، النظام القانوني لمتعهد الإيواء عبر الانترنت، مجلة المفكر، كلية الحقوق، جامعة محمد خيضر، بسكرة، العدد 14، ص 293.

2 عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة، 2011، د.ط، ص 95.

3 Pierre TRUDEL, La responsabilité sur Internet, texte préparé pour le séminaire Droit et Toile, Bamako, organisé par l'UNITAR (Institut des Nations unies pour la formation et la recherche), en association avec OSIRIS (Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal) et l'INTIF (Institut francophone des nouvellestechnologies de l'information et de la formation) de l'Agence intergouvernementale de la Francophonie Bamako, 27 mai 2002, p17.disponible en lingne á l'adresse suivante: *http://pierretrudel.chairelrwilson.ca/cours/drt6929f/Resp.internet-trudel.pdf*

تلك الخدمات عبر شبكة الانترنت، وأما عن التشريعات الدولية والداخلية فاتخذت حراكاً واسعاً نحو تأسيس أحكام خاصة تنظم عن مسؤولية مقدمي خدمات الانترنت لما لها من أثر للحد من انتشار المعلومات غير المشروعة عبر المعاملات الإلكترونية وحث الوسطاء الفنيين على الحرص على فرض الرقابة الذاتية على المعلومات لدرء المسؤولية عنهم.[1]

الفرع الأول: انتهاج المسؤولية التتابعية كأساس لقيام المسؤولية الجنائية لمقدمي خدمات الانترنت.

أثير التساؤل في فرنسا حول القانون الواجب التطبيق على الرسائل التي يتم تداولها عن طريق الانترنت حول إمكانية تطبيق قانون النشر الصحفي على أعمال مقدمي خدمات الانترنت، والتي ترتكز على مبادئ المسؤولية التتابعية، فإلى أي مدى نجح هذا التوجه في إرساء المسؤولية الجنائية لمقدمي خدمات الانترنت؟

على المستوى الفقهي نرصد اتجاهين؛ الأول يأخذ بفكرة إعمال قانون النشر الصحفي على أعمال مقدمي خدمة الانترنت، على اعتبار أن عمل مقدم الخدمة شبيه بدور مدير التحرير في الصحف المتمثل في عملية النشر، من ثم يأتي تطبيق المسؤولية الجنائية وفقاً لمبادئ المسؤولية التتابعية، وهو ما جاء به قانون الصحافة بفرنسا لسنة 1881، وبناءً عليه رتبوا على ذلك نتيجة مهمة هي تطبيق المادة 42 من قانون الصحافة[2]، بحيث يسأل مدير التحرير في حالة النشر الصحفي، ومدير البرنامج في حالة الاتصالات السمعية البصرية، وإن لم تقع على المسؤولية على المدير فيقع على المؤلف، وإن لم تتوافر على المؤلف تأتي على عاتق الطابع، وإن لم يكن فالبائع أو الموزع أو ملصق الإعلانات بصفتهم فاعلين أصليين، أو قد يتابع رئيس التحرير أو الناشر كفاعل أصلي ويسأل باعتباره شريكاً[3]. أما عن قانون الإتصالات السمعية البصرية

1 Olivier cachard , droit du commerce electronique , RDAI, N 3, 2004, P 394.

2 Art 42 du Loi du 29 juillet 1881 sur la liberté de la presse , dispose que: "Seront passibles, comme auteurs principaux des peines qui constituent la répression des crimes et délits commis par la voie de la presse, dans l'ordre ciaprès, savoir :

1- Les directeurs de publications ou éditeurs, quelles que soient leurs professions ou leurs dénominations, et, dans les cas prévus au deuxième alinéa de l'article 6, de les codirecteurs de la publication ;

2- A leur défaut, les auteurs ;

3 -A défaut des auteurs, les imprimeurs

4- A défaut des imprimeurs, les vendeurs, les distributeurs et afficheurs.

3 Art 43 du Loi du 29 juillet 1881 sur la liberté de la presse Modifié par Ordonnance du 26 août 1944, art 15 v. init., Modifié par Loi n°52-336 du 25 mars 1952 - art. 5 JORF 26 mars 1952.

رقم 82-652 فقد نص بمقتضى المادة 93-3 منه[1] على بيان تتابع المسؤولية الجنائية في إطار المجال السمعي البصري ابتداءً من مدير البرامج إلى مؤلف الرسالة فالمنتج، وبهذا استند أنصار هذا الاتجاه لهذا التسلسل في تشبيه عمل مقدم خدمة الانترنت باعتبارها نظام سمعي بصري، بشرط توافر التخزين المسبق أي عدم بثها مباشرة مما يسقط مسؤولية مدير البرنامج على رقابة المحتوى ويسأل صاحب الرسالة باعتباره فاعلاً أصلياً.

وجاء رأي مخالف من قبل بعض الفقه[2] المعارض لفكرة مساءلة مقدم خدمة الانترنت وفقاً للمسؤولية التتابعية المطبقة في قانون الصحافة والنشر, مستندين في ذلك لمخالفتها لقرينة البراءة على اعتبار أن مبادئ هذه المسؤولية تقوم على فكرة الإدانة القاطعة الواقعة بالتسلسل، كما أن الأمر لا يتعلق بقرينة قانونية على المسؤولية، ولكن يتعلق باستخلاص للركن المعنوي من الركن المادي؛ أي من واقعة نشر المعلومات غير المشروعة، فلا يمكن لمن تكون مهمته مديراً للتحرير أن يجهل بعدم مشروعية تلك المعلومات وبالتالي السماح بنشرها.[3]

وأما على مستوى الاجتهاد القضائي فقد أبدى مجلس الدولة الفرنسي تقديراً بشأن الانترنت والخطوط الرقمية الموافق عليه من قبل الجمعية العمومية للمجلس في 1998/07/02 والذي تضمن في فحواه رفض المسؤولية التتابعية لمقدمي خدمات الانترنت وتطبيق الأحكام العامة الخاصة بالمسؤولية الجنائية

1 Art 93-3 duLoi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle dispose que: " Au cas où l'une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication au public par voie électronique, le directeur de la publication ou, dans le cas prévu au deuxième alinéa de l'article 93-2 de la présente loi, le codirecteur de la publication sera poursuivi comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public .

A défaut, l'auteur, et à défaut de l'auteur, le producteur sera poursuivi comme auteur principal .

Lorsque le directeur ou le codirecteur de la publication sera mis en cause, l'auteur sera poursuivi comme complice .Pourra également être poursuivie comme complice toute personne à laquelle l'article 121-7 du code pénal sera applicable .Lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message .

2 شيماء عبد الغني، المرجع السابق، ص169.

3 Olivier cachard, Op. Cit, p 399.

فحسب، وهذا بالنظر على توافر القصد الجنائي من خلال التحقق بمعرفة محتوى المعلومات غير المشروعة المقدمة عبر الانترنت، وتحقق الإجراءات الكافية لمراقبة طرح تلك المعلومات[1].

وأما على مستوى محكمة الاستئناف الفرنسية بباريس سنة 1999 فقد اتجهت إلى موقف مخالف لما جاء به مجلس الدولة، والتي أقرت بمساءلة متعهد الإيواء للمعلومات عبر الانترنت مقرة بالتماثل بينها وبين تلك الخدمات المقدمة سمعياً وبصرياً وفقاً للتتابع في المسؤولية الجنائية في إطار قانون الصحافة[2].

وتشكل المسؤولية التتابعية برأينا إخلالاً لمبدأ أصل البراءة، مادام أنها تقيم قرينة قاطعة غير قابلة لإثبات العكس على مسؤولية مدير التحرير وما يليه في سلم التسلسل، وهو ما لا يعبر عن أي تحقيق للعدالة في حالة الأخذ بذات المسألة في مجال أعمال مقدمي خدمات الانترنت؛ نظراً لتعقد مهام الوسطاء الفنيين وتداخلها مع صعوبة تحديد الرقابة على المعلومات وحصر مشروعيتها من عدمها في نطاق غير مادي.

أما على المستوى التشريعي فقد رأى المشرع الفرنسي ضرورة وضع حكم خاص من خلال القانون رقم 2000–719 المعدل للقانون رقم 86-1067 المتعلق بحرية الاتصالات، منظم للمسؤولية الجنائية لمقدمي خدمات الانترنت, وهذا تحديداً من خلال المادة 43-8 التي نصت على عدم تقرير المسؤولية الجنائية أو المدنية لمقدم خدمات الانترنت عن محتوى هذه الأخيرة، والذي يقوم بتقديمها بمقابل أو بدون مقابل أو بالتخزين المباشر والمستمر لها، أو يضع تحت تصرف الجمهور إشارات أو كتابة أو صور أو أصوات أو رسائل كيفما كانت طبيعتها، باستثناء حالتين؛ الأولى تتعلق بعدم تنفيذ الأمر القضائي الصادر بإلزامه بمنع الوصول إلى هذا المضمون، والثانية في حالة تقدير الغير وجود محتوى غير مشروع من شأنه الإضرار بالمتعامل الإلكتروني وتنبيه مقدم الخدمة إلى ذلك، وعدم اتخاذ الإجراءات اللازمة لمنع نشر هذا المحتوى[3].

1 Conseil d'État: INTERNET ET LES RÉSEAUX NUMÉRIQUES, Etude adoptée par l'assemblée générale du Conseil d'État, section du rapport et des études, le 2 juillet 1998. Paris : La Documentation française, 1998, p 266. (Les Études du Conseil d'État). ISBN 2-11-004102-1. ISSN 1152-4561. 95 F. voir le site: *HTTP://BBF.ENSSIB.FR/CONSULTER/BBF-1999-01-0125-009.*

2 CA paris, 10 février 1999, D.1999,jur.389,note Nathalie mallet –pourjol:disponible en lingne á l'adresse suivante: *http//fr.jurispedia.org/index.php/Responsabilit%C3%A9_des_interm%C3%A9diaires_techniques_de_l'internet.*

3 Art. 43-8.du LOI no 2000-719 du 1er août 2000–dispose que: Les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images de sons ou de messages de toute nature

الفرع الثاني: موقف التشريعات الدولية والتشريعات المقارنة من المسؤولية الجنائية لمقدمي خدمات الانترنت.

نظراً لدقة وصعوبة دور مقدمي خدمات الانترنت، بدأ إدراك تلك الصعوبة وبدت الحاجة الماسة لإنشاء نظام قانوني خاص يتكفل بمسألة تنظيم المسؤولية الجزائية لهؤلاء الفئة في مجال التعامل الإلكتروني بأحكام خاصة، وهذا ما سعت إليه أغلب التشريعات إن كان على المستوى الإقليمي أو الداخلي، وهو ما أدى بالبرلمان الأوروبي لإصدار التوجيه الأوروبي رقم 31-2000 في 08 جوان 2000 المتعلق ببعض الأوجه القانونية لخدمات شبكات المعلومات وبصفة خاصة التجارة الإلكترونية في السوق الداخلية، والذي أولى اهتماماً بالمسألة، بحيث خصص القسم الرابع من التوجيه لتنظيم المركز القانوني للوسطاء في خدمة الانترنت.

وتعتبر تلك الأحكام مصدر إلهام لبعض التشريعات الأوروبية وعلى رأسها التشريع الفرنسي، خاصة أن التوجيه حث الدول الأعضاء على تبني أحكام خاصة بتحديد المسؤولية الجنائية والمدنية لهذه الفئة، وهذا ما أدى بالمشرع الفرنسي إلى السير على خطى التوجيه الاوروبي وإصدار القانون 2004-575 المؤرخ في 21 جوان 2004 حول الثقة في الاقتصاد الرقمي, مخصصاً المواد من 5-9 في الفصل الثاني منه لتظيم المسؤولية المستقلة لمقدمي خدمات الانترنت في فرنسا[1].

البند الأول: موقف التوجيه الأوروبي من المسؤولية الجنائية لمقدمي خدمات الانترنت.

أورد التوجيه الأوروبي رقم 2000-31 في نص المادة 12 إعفاءً من المسؤولية للوسطاء الذين يقدمون الخدمات عبر شبكة الانترنت، والذين يلعبون دوراً سلبياً يتمثل في نقل المعلومات فقط التي تأتي من الغير، ثم جاء في نص المادة 14 لينص على عدم مسؤولية متعهد الإيواء عن مضمون المعلومات التي يتم بناؤها على طلب المتعامل، وذلك ما لم يثبت علمه بالمضمون غير المشروع, سواء علماً فعلياً أو من خلال

accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que: "si, ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu; ayant été saisies par un tiers estimant que le contenu qu'elles hébergent est illicite ou lui cause un préjudice, elles n'ont pas procédé aux diligences appropriées."

1 D. MELISON, "Responsabilité des hébergeurs : une unité de régime en trompe l'œil", juriscom.net 25 avril 2005, disponible á l'adresse suivante:www.juriscom.net, p 11 .

الملابسات والظروف، كما أن للدول الأعضاء وفقاً للفقرة 3 من المادة 14 أن تلزم مقدمي خدمات الانترنت سواء عن طريق القضاء أو السلطة التنفيذية باتخاذ كل ما يلزم لوقف الاعتداء أو اجتناب حدوثه.

هذا الحكم ينسجم مع ما جاءت به الفقرة الأولى من المادة 15 التي حظرت على الدول الأعضاء أن تفرض على مقدم الخدمات التزاماً عاماً بمراقبة المعلومات التي يقومون بنقلها أو بتخزينها أو للبحث عن الوقائع وظروف النشاط غير المشروع، وأما فيما يخص بدور ناقل المعلومات والذي يقوم دوره على عملية تخزين للبيانات بشكل مؤقت على أجهزته، فهنا نصت المادة 13 من التوجيه الأوروبي على عدم مساءلته إلا في حالة ثبوت أنه هو مصدر المحتوى المعلوماتي غير المشروع، أو قام بعمليات التغيير عليه أثناء عملية النقل والتخزين بشكل جعل منه يظهر في صفة غير مشروعة، أو في حالة تقاعسه عن وقف بث المحتوى غير المشروع رغم علمه بذلك.

كما أن التوجيه لم يُلقِ المسؤولية على متعهد الوصول إلا في حالة رفض التعاون مع السلطات القضائية في الدولة في حالة طلبها ذلك منه بصورة قانونية، كما ألزمت المادة 12 متعهد الوصول المبادرة إلى شطب المحتوى الإلكتروني غير المشروع أو منع الوصول إليه بعد علمه بذلك أو إخطاره من قبل السلطات القضائية أو من قبل الشخص المتضرر من ذلك المحتوى.

كما أن التوجيه أورد أحكاماً صريحة وعامة خارج الفصل الخاص بمسؤولية وسطاء الانترنت، وذلك من خلال المادة 43 التي نفت المسؤولية على مقدم الخدمات في حالة ما إذا كان عمله يقتصر على النقل أو التخزين، فهنا يعتبر غير مسؤول على فحوى المعلومات المنقولة ولا يملك أي سلطة على تعديلها، بحيث أن العمل التقني البحت لا يشكل تغييراً في المعلومات، أما الشخص المكلف بخدمة تخزين المعلومات فإنه ملزم بمتضى المادة 46 من التوجيه بسحب تلك المعلومات ومنع الوصول إليها في حالة العلم بعدم مشروعيتها[1].

البند الثاني: موقف المشرع الفرنسي من المسؤولية الجنائية لمقدمي خدمات الانترنت.

جاء حكم المشرع الفرنسي من خلال القانون 2004-575 وتحديداً في نص المادة 3/6 متوافقاً مع التوجيه الأوروبي 2000-31 بوضع مبدأ عام قائم على عدم مسؤولية مقدمي خدمات الانترنت, إلا في حال معينة وتوافر شروط محدد، والتي جاء في مضمونها: "أن أفعال مقدمي خدمات الانترنت الخاطئة لا

1 سعيد بن محمد الغافري، التعويض في التعامل الإلكتروني دراسة في النظام السعودي مع التأصيل والمقارنة، أطروحة الدكتوراه فلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2012، ص 152.

يمكن أن تدخل في نطاق التجريم إلا إذا ثبت علمهم بالمضمون الإلكتروني غير المشروع، وعلى الرغم من ذلك لم يتخذوا الإجراءات اللازمة لشطبه أو على الأقل منع الوصول الجمهور إليه"[1].

فكل دولة في هذا الشأن تنتظر بالتأكيد من مقدمي خدمات الإنترنت الذين يُمارسون أنشطتهم من على أراضيها، وفيما لا يُجاوز في حدِّه الأعلى الشروط السابقة، مساعدة السلطات العامة فيها على مُحاربة الجريمة الإلكترونية، وبخلاف ذلك سيجدون أنفسهم تحت طائلة المسؤولية الجزائية كمتدخِّلين في الجريمة، أو كمشتركين فيها. غير أنه وبالرجوع إلى نصوص قانون العقوبات الفرنسي نجد بأنه لا يُمكن أن يُدان شخص بجريمة التدخُّل أو بالاشتراك الجرمي ما لم يثبت علمه بالأفعال المرتكبة[2]؛ وتطبيقاً لذلك فإن القصد الجرمي لمقدمي خدمات الإنترنت ينتفي في حال ثبت عدم علمهم الفعلي بالمضمون الإلكتروني غير المشروع، أو إذا ما قاموا بمجرد علمهم بعدم مشروعية هذا المضمون، بشطبه، أو بمنع وصوله للجمهور.

كما اهتم القانون الفرنسي المتعلق بالثقة في الاقتصاد الرقمي بتنظيم المسؤولية الجنائية الواقعة على عاتق متعهد الوصول ومتعهد الإيواء بشكل خاص، فقرر في نص المادة السادسة (06) إعفاء متعهد الإيواء من المسؤولية المدنية والجنائية عن المحتوى غير المشروع الذي يأويه إذا انتفى علمه بحقيقة ذلك المضمون، وقام المتعهد بكل ما يلزم حيال شطب ذلك المحتوى ومنع وصوله إلى المستخدمين فور علمه بأسباب عدم مشروعيته, أو بالملابسات والظروف التي تضفي عليه عدم المشروعية.

ويأتي المشرع الفرنسي مبيناً وسيلة إثبات علم متعهد الإيواء بمشروعية المحتوى غير المشروع من عدمه، فنص في المادة السادسة (06) على أن هذا العلم يثبت بمجرد تقديم شكوى من الشخص المتضرر من هذا المحتوى، ويقدم دلائل على عدم مشروعيته، ضف إلى ذلك تحديد تاريخ التبليغ، وهنا يشترط المشرع قيام المسؤولية اتجاه متعهد الإيواء في حالة توافر شرطين: الأول يتعلق بتسليمه إخطار من الطرف

1 Article 6-3 du LCEN Modifié par Loi n°2018-898 du 23 octobre 2018 - art. 29, dispose que "Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible."

2 Ch. HUGON, "La responsabilité des acteurs de l´internet dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l´économie numérique", Contrats, Concurrence, Consommation, Études, novembre 2004, n° 18 et s., p. 9.

المتضرر من المحتوى الإلكتروني، وهذا ما يقيم عليه قرينة العلم بعدم مشروعية المضمون، وكذا منحه فرصة من أجل السعي لإيقاف نشر المحتوى غير المشروع.

ولكن كيف بالإمكان ضمان جدِّية التبليغ، وبالتالي تجنُّب التبليغات التعسُّفية أو الكيدية؟ أجابت على هذا التساؤل المادة 4/6 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، والتي نصَّت على أن كل من بلَّغ مقدمي خدمات الإنترنت بوجود مضمون إلكتروني غير مشروع، من أجل شطبه أو منع الجمهور من الوصول إليه، مع علمه المسبق بعدم صحَّة تبليغه، يُعاقب بالسجن لمدة عام وبغرامة مقدارها خمس عشرة ألف (15.000) يورو[1].

كما أن المشرع قد أورد بنص المادة التاسعة (09) من ذات القانون أحكاماً خاصة بكل من متعهد الوصول وناقل المعلومات، فنصت على عدم إمكانية مساءلتهم مدنياً أو جزائياً إلا في حالة إثبات أنهم مصدر المحتوى غير المشروع، أو أنهم عملوا على إدخال تغييرات عليه، وساهموا في إيصاله إلى المستخدمين عبر شبكة الانترنت، وهذا ما يخالف مبدأ الحياد الذي يفترض أن تقوم عليه مهامهم، وهذا الحكم مستمد من أحكام المادتين 12 و13 من التوجيه الأوروبي رقم 200-31.

البند الثالث: موقف المشرع الأمريكي من المسؤولية الجنائية لمقدمي خدمات الانترنت.

من جهته حصر القانون الأمريكي (DMCA)[2] مساءلة مقدمي خدمات الإنترنت جزائياً في حدود الاعتداء على حقوق الملكية الفكرية في نطاق الإنترنت، فأقام مسؤوليتهم فقط في حال علمهم بعدم مشروعية المضمون المعلوماتي الإلكتروني الذي يقومون بنقله أو تخزينه، ويثبت علمهم هذا في حالتين؛ الأولى: أن تكون عدم المشروعية ظاهرة إلى حدٍّ لا يُمكن تجاهلها، والثانية: قيام السلطات الأمريكية المختصة أو الشخص المتضرر من نشر المضمون المعلوماتي بإبلاغ مقدم الخدمة بوجه عدم المشروعية، فإذا ما تحقق علمه بعدم المشروعية، وعلى وجه الخصوص بالعمل المقلَّد أو المنسوخ بصورة غير شرعية، توجب

1 Article 6/4 dispose que:" Le fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 Euros d'amende".

2 القانون الأمريكي الصادر في 28 تشرين الأول 1998 والمسمَّى: Digital Millenium Copyright Act (DMCA) (Public Law n° 105-304, 112 sat, 2860, 28 oct. 1998.)، يُمكن أيضاً الإطِّلاع على نصوص هذا القانون على الموقع الإلكتروني للمكتب الأمريكي لحقوق النشر وذلك على العنوان التالي *http://lcweb.loc.gov/copyright*، تم الاطلاع بتاريخ: 2018/11/12، على الساعة: 12.33.

عليه المبادرة إلى اتخاذ موقف إيجابي بشطب المضمون الإلكتروني غير المشروع، أو منع وصوله لجمهور مستخدمي الشبكة، وبخلاف ذلك، يُعدُّ مقدم الخدمة مُخلاً بالتزاماته، مع قيام مسؤوليته[1]. ونلاحظ في هذا الصدد تطابق حالات قيام المسؤولية وانتفائها في التشريعات الثلاث: الأوروبي، والفرنسي، والأمريكي.

ولكي تنتفي مسؤولية مقدمي خدمات الإنترنت الجزائية بشكلٍ كُلِّي، وفي إطار مساعدتهم للسلطات العامة في الدولة في مُحاربة جرائم انتهاك حقوق الملكية الفكرية، وحرمة الحياة الخاصة وقداسة الأديان وجرائم الحث على المشاعر العنصرية، والاعتداء الجنسي على الأطفال، فإنهم مُطالبون أيضاً وفقاً لنص الفقرة الثالثة من المادة 6-7/2 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"[2]، والتي جاءت متفقةً مع الاتجاه العام للمواد 13 و14 من التوجيه الأُوروبي حول "التجارة الإلكترونية"، ومع المادة 3/g/512 من القانون الأمريكي (DMCA)، والخاصة بالتعدي على حقوق الملكية الفكرية في نطاق الإنترنت، بأن يضعوا تحت تصرُّف عملائهم الوسائل اللازمة لتسهيل عملية التبليغ عن أيِّ مخالفات قد تتم عبر الشبكة. وبعد تحقق مقدم الخدمات من صحة موضوع التبليغ ومن عدم مشروعية المضمون الإلكتروني عليه أن يُبادر فوراً إلى إبلاغ السلطات العامة في الدولة عن هذه الواقعة، وذلك من أجل استصدار أمرٍ إداريٍّ أو قضائيٍّ بشطب هذا المضمون، أو منع وصوله لمستخدمي الشبكة.[3]

---

1 حول القانون الأمريكي (DMCA) انظر:

- M. GUILLARD, "Responsabilité des acteurs techniques de l´internet", précité, p. 29,A. STROWEL, "Responsabilité des intermédiaires: actualité législatives et jurisprudentielles", 10/10/2000, p. 17, article disponible à l'adresse : *www.droit -technologie.org*, V. SÉDALLIAN, "La responsabilité des prestataires techniques sur Internet dans le Digital Millenium Copyright Act américain et le projet de directive européen sur le commerce électronique", Cahiers Lamy, Droit de l'informatique et des réseaux, n° 110, janvier 1999, p. 1.

2 Article 6/7/2 dispose que": Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième, septième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 222-33, 225-4-1, 225-5, 225-6, 227-23 et 227-24 et 421-2-5 du code pénal."

3 أحمد قاسم فرح، المرجع السابق، ص 354.

البند الرابع: موقف المشرع الجزائري من المسؤولية الجنائية لمقدمي خدمات الانترنت.

بالرجوع لنصوص التشريع الجزائري نجد أن المشرع قد منح أهمية واسعة لمسألة المسؤولية الجنائية لمقدمي خدمات الانترنت, ابتداءً من وضع نصوص تحيط بالالتزامات الواقعة على عاتق هذه الفئة من خلال المرسوم التنفيذي رقم 98-257 المتضمن شروط وكيفيات إقامة خدمات الانترنت واستغلالها، حيث نصت المادة 14 منه على فرض التزامات على مقدمي خدمة الانترنت منها تسهيل النفاذ إلى خدمات الانترنت، حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك باستعمال أنجح الوسائل التقنية، وكذا احترام قواعد حسن السيرة بالامتناع عن استعمال أي وسائل غير مشروعة سواء اتجاه المستعملين أو اتجاه مقدمي خدمات الانترنت، كما يقع على عاتق مقدم خدمة الانترنت تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها ويأويها، واتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة للمستخدمين قصد منع النفاذ إلى الموزعات التي تحوي معلومات تتعارض مع النظام العام أو الأخلاق.

ونجد القانون رقم 09-04 المتعلق بجرائم تكنلوجيات الإعلام والاتصال من خلال نص المادة 12 منه يفرض التزامين رئيسيين على الوسيط الفني يتعلق الأول منهما على: التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، وأما التزام الثاني فيتأتى بوضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المستخدمين لديهم بوجودها وهو نفس موقف المشرع الفرنسي من خلال نص المادة 6 من القانون 2004-575 المتعلق بالثقة بالاقتصاد الرقمي.

والملاحظ أن المشرع قد أحسن عملاً في تحديد تلك الالتزامات التي تمثل بشكل واضح خضوع مقدمي خدمات الانترنت لواجب المراقبة والحرص على المحتوى الإلكتروني، والعمل على حظر انتشار المضامين غير المشروعة، إلا أن المشرع لم يكمل دوره من خلال فرض الالتزامات دون تقرير الجزاء المترتب على مخالفتها وهو ما يفقد فاعلية هذه الأحكام خاصة أن الهدف من تقرير المسؤولية الجنائية هو فرض الجزاء الرادع الذي يحول دون التهاون في التمسك بالالتزامات المفروضة في هذا الصدد وبالتالي الحد من الجرائم المرتكبة في هذا النطاق.

إلا أن المشرع عمل على تدارك هذا النقص من خلال نص القانون 16-02 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، بحيث أورد نص المادة 394 مكرر 8 التي نصت على فرض عقوبة الحبس من سنة إلى ثلاث (3) سنوات وبغرامة من 2.000.000 دج إلى 10.000.000 دج أو بإحدى هاتين العقوبتين فقط لكل مقدم خدمات الانترنت بمفهوم المادة 2 من القانون 09-04 الذي لا يقوم رغم إعذاره من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] أو صدور أمر أوحكم قضائي يلزمه :

- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانوناً.
- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة أ أو جعل الدخول إليها غير ممكن.

والملاحظ من هذا الحكم أن المشرع الجزائري ارتأى ربط تقرير المسؤولية الجنائية لمقدمي خدمات الانترنت بناءً على مخالفة أمر أو حكم الجهات القضائية, أو الإعذار الموجه من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بالقيام بأي نوع من الإجراءات التي تحول دون نشر المحتوى الإلكتروني غير المشروع ومنع وصوله إلى الجمهور، ولعل هذا الربط يعد أمراً منطقياً؛ نظراً لأن مسألة تقرير المسؤولية الجنائية يفترض صدورها من الهيئة التي تملك سلطة التقدير في مخالفة تلك الإلتزامات وآثارها الوخيمة على التعامل الإلكتروني, والتي تتمثل في السلطة القضائية باعتبارها جهة حكم، وكذا اتجاه المشرع لاعتبار محتوى المعلومات غير شرعي بصفة غير موضوعية؛ أي صادر بموجب حكم قضائي يقضي بعدم شرعية ذلك المحتوى، أو من خلال صدور إعذار من الهيئة المنشئة لغرض إيجاد وسائل تشريعية وقائية من شتى الأعمال التي تمثل اعتداء في مجال التعاملات الإلكترونية.

1 تحدد المادة 14 المهام الموكلة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته وهي:
أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.
ب – مساعدة السلطات القضائية ومصالح بشأن الشرطة القضائية في التحريات التي تجريها على الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.
ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الباب الثاني:
الحماية الجزائية الإجرائية للمعاملات الإلكترونية

الـباب الثانـــــي:
الحماية الـجنائية الإجرائيـــة للمعاملات الإلكترونيـــة.

بعد الوقوف على أهم فصول الحماية الجنائية الموضوعية للمعاملات الإلكترونية, نجد أن الدراسة تقف عند منحى آخر؛ وهو الجانب الإجرائي الذي يمثل استكمالاً لمفهوم تلك الحماية وشموليتها، ويعزز القواعد الموضوعية، فالجوانب الإجرائية للحماية الجنائية من جرائم المعاملات الإلكترونية هي التي تنقل نص التجريم من حالة الركود إلى جانب الحركة، فعلى فرض أن المشرع استطاع أن يحيط بالقاعدة الموضوعية للجرائم المتعلقة بالمعاملات الإلكترونية، فإن نجاحه سيبقى مرهوناً بمدى إمكانية تطبيق هذه النصوص على أرض الواقع، ويظل محصوراً في دائرة نظرية ضيقة ما لم يكفل التنظيم الإجرائي الفعال ليضمن تحقيق الهدف من العقاب، مع مراعاة ما يحتاجه هذا التطبيق من إمكانيات تقنية تختلف بحسب مستوى التقدم التقني والتكنولوجي في كل دولة.

وعند الانتقال إلى دائرة التطبيق العملي للحماية الجنائية للمعاملات الإلكترونية، تظهر التحديات التي تبدأ من أولى مراحل التحقيق وجمع الأدلة التي ولدت مشكلات وعقبات عملية, وقفت كحجر عائق أمام السلطات والهيئات المختصة قانوناً في مواجهة هذه الطائفة من الجرائم من جهة، ومن جهة أخرى فإن الطبيعة الخاصة للمعاملات الإلكترونية ولدت مشكلة السيطرة على الدليل غير المادي, وغموض مسرح الجريمة الافتراضي الذي أثر على وسائل وآليات التحقيق والإثبات.

ونتيجة لهذه الخصوصية فإن الأهداف الأساسية من الدراسة في هذا الباب ترتكز على إيجاد إجابة عن إشكالية رئيسية مفادها: ما مدى قابلية القواعد الإجرائية التقليدية للتطبيق على الجرائم الماسة بالمعاملات الإلكترونية ؟ وهنا يجدر بنا بيان التصورات العملية الممكنة ومناقشة الإشكاليات على الصعيد الإجرائي للوصول للحلول المناسبة في هذا الإطار من الجانب التشريعي والفقهي والقضائي المقارن.

وبناءً على ماسبق سيتم تقسيم هذا الباب إلى فصلين مستقلين يخصص الأول منهما لبيان الحماية الجنائية للمعاملات الإلكترونية من خلال الإجراءات الجنائية السابقة على المحاكمة المتمثلة في مرحلتي التحقيق الابتدائي والإثبات (الفصل الأول)، ثم دراسة أهم القواعد الإجرائية الجنائية لحماية المعاملات الإلكترونية في مرحلة المحاكمة من بيان اختصاص المحكمة, وتقدير الدليل الرقمي من قبل القضاء (الفصل الثاني).

الفـصل الأول:
الحماية الجزائية للمعاملات الإلكترونية في مرحلتي التحقيق الإبتدائي والإثبات

الفصل الأول:

الحماية الجنائية للمعاملات الالكترونية في مرحلتي التحقيق الإبتدائي والإثبات.

لا يعتبر تحريك الدعوى العمومية من الفراغ، بل لا بد أن يبنى على أسباب معقولة تبدأ من اكتشاف النشاط الإجرامي ومعرفة الجاني وجمع الأدلة الخاصة بالجريمة، وعند اكتمال هذه العناصر يمكن للنيابة العامة ممارسة سلطتها التقديرية في إقامة الدعوى العمومية أو عدم إقامتها، ومن هنا تظهر أهمية أعمال التحقيق أو الاستدلال، التي تبدأ منذ وقوع الجريمة وتستمر حتى تحريك الدعوى العمومية.

وفي مجال الجرائم الواقعة على المعاملات الإلكترونية وسائر الجرائم المرتكبة في العالم الافتراضي، فإن أهمية هذه المرحلة تبلغ أعلى مستوياتها؛ لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم الحصول عليه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة، قد لا يبقى متاحاً بعد مرور وقت قصير على ارتكابها، والسبب يعود إلى الطبيعة التقنية لهذه الجرائم.

والمرجع الأساسي في مشكلة إثبات جرائم المعاملات الإلكترونية أنه يصعب اكتشافها وضبطها وتحديد هوية مرتكبيها الذين يتسمون في مجملهم بصفتي الدهاء والذكاء في ارتكاب هذه النوعية من الجرائم، ويقابل ذلك عدم ملائمة الأدلة التقليدية في اثباتها، علاوة على قلة خبرة القائمين على التحقيق في تلك الجرائم، مما يزيد من صعوبة اتخاذ اجراءات التحقيق الجنائي على الوجه الأكمل وصولاً إلى مرتكبي هذه الجرائم.

كل هذا يقودنا إلى محاولة تحليل القواعد الخاصة باستكمال إجراءات التحقيق الابتدائي, وبيان الخصوصية التي تطبعها على المستوى العملي من خلال التشريعات المقارنة التي عملت على تنظيم هذا الشق في تشريعاتها العقابية، والبحث في مدى ملائمة النصوص التقليدية لتلك الخصوصية بالنسبة للتشريعات التي لم تخط خطوة نحو استحداث تشريعات تنظم هذا النوع من الجرائم (المبحث الأول)، لتأتي مسألة بيان قواعد الإثبات في الجرائم الماسة بالمعاملات الالكترونية, واستظهار الصعوبات والعقبات التي تعتريها نظراً لتباين المسرح الإجرامي في الجريمة التقليدية والجريمة في المجال الرقمي (المبحث الثاني).

المبحث الأول:

التحقيق الإبتدائي في الجرائم الواقعة على المعاملات الإلكترونية.

إن الجرائم المرتكبة في مجال المعاملات الإلكترونية ترتبط بأنماط ودرجات من التكنولوجيا, مما يتطلب معه أن لا يقتصر تحقيقها على قواعد وأساليب التحقيق الابتدائي المعروفة، بل تحتاج إلى قواعد وتقنيات خاصة وفريدة أو غير مسبوقة، وبهذا فإن القواعد الفنية التي يوصى بالإسترشاد بها في إجراءات التحقيق الناجح هي التي تتماشى مع الطبيعة الخاصة لتلك الجرائم.

كما أن العمل على مستوى الجريمة الافتراضية يختلف من حيث الجهات المكلفة بالبحث والتحري فيها نظراً لتقنية الأساليب المتخذة في ارتكاب الجريمة، مما يستلزم تجنيد أفراد على مستوى من الخبرة والمهارة لكشف حقيقة السلوك الإجرامي وتعقبه في بيئة غير مغلقة وشاسعة ويصعب السيطرة عليها، وهو ما ذهبت إليه أغلب التنظيمات التشريعية المقارنة التي استحدثت أجهزة خاصة بمجال مكافحة الجرائم ذات طبيعة إلكترونية، أو التي تقع في مجال شبكة الانترنت.

وبناء على ما ذكر أعلاه, نبين في هذا المبحث الأجهزة المختصة بالتحقيق الإبتدائي في الجرائم الماسة بالمعاملات الإلكترونية (المطلب الأول), على نحو نستطيع من خلاله بيان آليات وإجراءات التحقيق الابتدائي في الجرائم الماسة بالمعاملات الإلكترونية (المطلب الثاني).

المطلب الأول: الأجهزة المختصة بالتحقيق الإبتدائي في الجرائم الماسة بالمعاملات الإلكترونية.

وقبل بيان الأجهزة المختصة بالبحث والتحقيق الجرائم الماسة بالمعاملات الإلكترونية على الصعيد الداخلي أو الدولي أو الإقليمي, يجدر بيان المبادئ التي تحكم الضبطية القضائية المختصة في مكافحة جرائم المعلوماتية، بحيث يحكم الضبط القضائي في ظل البحث والتنقيب مجموعة من المبادئ تتمثل في:

- يشترط أن تكون هذه الفئة ممن تتمتع بفن الضبط القضائي؛ أي أنه يجب أن تكون متخصصة في إدراك كيفية عمل الضبط القضائي وموضوعاته لكي تكون مستعدة دائماً للتعامل مع هذه النوعية من الجرائم، وذلك عن طريق تدريبها وتكوينها في أمور تقنية الحوسبة والانترنت وكيفية التعامل مع العالم الافتراضي.
- يجب إعادة النظر وضبط مفهوم المشروعية في أعمال الضبط المناط بها شرطة الضبطية القضائية نظراً لمواجهة هذه الفئة لأفعال واقعة عبر شبكة الانترنت مثل التخفي عبر الاتصالات وإمكانية انتحال أسماء وهمية وغيرها.[1]
- كما يجب التزام الشرطة القضائية في هذا المجال بالتقيد بكل واجبات العمل القانوني وفق الشروط والإجراءات المقررة قانوناً من تحرير محاضر تثبت الإجراءات المتخذة في الكشف عن الجريمة، والالتزام باستصدار إذن من السلطات المختصة للقيام بالإجراءات الماسة والمقيدة لحرية الأشخاص كالتفتيش والضبط والقبض، وكذا توافر شرط الاختصاص المكاني والزماني والموضوعي للقيام باختصاصاتها المحددة قانونا.[2]

وأمام التزايد المستمر للاعتداءات في مجال التعامل الإلكتروني، اضطرت أجهزة الضبط القضائي للسير نحو تحديث الإطار الهيكلي للتعامل مع هذا النوع من الجرائم ومحاربتها، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة مختصة في هذا المجال، بالرغم من أنها حملت تسميات مختلفة منها شرطة الانترنت، الضبطية القضائية لمكافحة جرائم المعلوماتية, أو درك الانترنت وغيرها.

وتختلف هذه الأجهزة عن الأجهزة المختصة بضبط الجرائم التقليدية من حيث طريقة التكوين، فهي لا تعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الشرطة، وإنما تعتمد على البناء العلمي

1 محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، ط1، منشورات الحلبي الحقوقية، بيروت، سنة 2011، ص 231.
2 خالد عياد الحلبي، المرجع السابق، ص 168.

والتكنولوجي لأفرادها، وهي تتولى مهمة التحري عن جرائم العالم الافتراضي لكشف النقاب عنها[1]. ولا يقتصر دور هذه الأجهزة على المستوى الوطني، بل هناك أجهزة مختصة على المستوى الدولي والأوروبي وهو ما سيتم بيانه من خلال النقاط التالية:

الفرع الأول: الأجهزة المختصة بمكافحة الجرائم الماسة بالمعاملات الإلكترونية على المستوى الداخلي.

ظهرت العديد من الأجهزة المختصة بمكافحة جرائم المعاملات الإلكترونية على المستوى الوطني، سواء على صعيد الدول الأجنبية أم على صعيد الدول العربية.

البنــد الأول: الأجهزة المختصة بمكافحة الجرائم الماسة بالمعاملات الإلكترونية على صعيد الدول الأجنبيــة.

ذهبت غالبية الدول الأجنبية لاستحداث أجهزة خاصة على مستوى الضبطية القضائية تتكفل بمكافحة الجرائم الواقعة في المجال المعلوماتي، والتي تشكل خطراً على التعاملات بين الأفراد في كل المستويات، وترتبط مكافحة جرائم المعاملات الإلكترونية بمدى تقدم الدول من الناحية التقنية، وبمدى توفر الإمكانيات المادية اللازمة لإنشاء هذه الأجهزة.

أولاً: الأجهزة المتخصصة على مستوى الولايات المتحدة الأمريكية.

قامت الولايات المتحدة الامريكية بإنشاء عدة أجهزة لمكافحة جرائم الانترنت ومنها:

1- **شرطة الويب:** وهي نقطة مراقبة على الانترنت إضافة إلى أنها تقوم بتلقي الشكاوى عن مستخدمي الشبكة، وملاحقة الجناة القراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة. وتعمل هذه الفئة خصيصاً في مجال محاربة جرائم الاحتيال التي تقع عبر صفحات الويب وغرف الدردشة والبريد الإلكتروني من خلال متابعة قضايا عرض السلع والخدمات الوهمية على المستهلكين, أو تزويدهم بعرض غير حقيقي أو احتيالي، أو تحويل أموال المجني عليهم عبر سرقة أو تزوير بطاقات الدفع الإلكتروني للضحايا[2].

1 محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 235.

2 مصطفى محمد مرسي، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، الطبعة الاولى، سنة 2009، ص 325.

2- كما أنشأ مكتب التحقيقات الفيدرالي (FBI) مركزاً لتلقي شكاوى الإنترنت سنة 2000، والذي تم دمجه مع مركز شكاوى الإحتيال عبر الانترنت، وخصص له موقعاً على شبكة الانترنت، لتلقي بلاغات الاحتيال على شبكة الانترنت، وأسندت مهمة السهر على تحقيق أهداف محددة من خلال تسيير الموقع لأجهزة متخصصة, وتتمثل تلك الأهداف فيما يلي:

- منع الخسائر الاقتصادية أو الحد منها، وتوفير أرشيف تحليلي للمعلومات عن الاحتيال الإلكتروني.
- وكذا تطوير استراتيجية على مستوى الولايات المتحدة الأمريكية لمواجهة الاحتيال عبر الانترنت، وملفات تتضمن معلومات تتعلق بالشكاوى المجموعة والتي يتم تحويلها إلى الأجهزة المختصة بتطبيق القانون.
- تلقي وتحويل وتحليل جميع الأنشطة الإجرامية الاحتيالية التي يتم تحديدها عبر الانترنت، وتحديد الاتجاه الحالي للجرائم المرتكبة عبر الانترنت وتطوير وسائل التحقيق في المشكل الجنائية التي يجرى تحديدها.[1]

3- نيابة جرائم الحاسوب والاتصالات CTC وتتألف من مجموعة من قضاة النيابة العامة الذين تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات، وتم منحهم صلاحيات واسعة في مجال الاستعانة بغيرهم من خبراء وزارة العدل[2].

ثانياً: الأجهزة المتخصصة على مستوى بريطانيا.

ونجدها كغيرها من الدول التي يهددها هذا النوع المستحدث من هذا الإجرام، قد خصصت وحدة تجمع نخبة من رجال الشرطة المتخصصين في البحث والتنقيب عن الجرائم الواقعة في المجال الإلكتروني، وتضم هذه الوحدة 80 مفتشاً من رجال الشرطة والجمارك, وأفراداً من مصلحة الإستعلامات متمركزين في لندن وفي جميع المفتشيات الإقليمية التقليدية المتواجدة في انجلترا، 40 منهم يشتغلون في لندن ضمن الوحدة الوطنية لمكافحة جرائم التقنية العالية و46 مقسمون على الوحدات المحلية[3].

---

1 نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، سنة 2006، ص 108-109.

2 مصطفى محمد مرسي، المرجع السابق، ص 327.

3 Cyber police contre cyber-crimes: La Grande Bretagne lance une unité de "cyber-policiers". disponible en ligne suivant :*http://www.stratégique.free.fr*

- تم الاطلاع بتاريخ: 2018/12/13 على الساعة 19:12.

ثالثاً: الأجهزة المتخصصة بمكافحة جرائم المعاملات الإلكترونية في فرنسا:

لقد أنشأت عدة وحدات ومراكز متخصصة وغير متخصصة ضمن الشرطة والدرك الوطني في فرنسا لمكافحة هذا الإجرام المستحدث بجميع صوره، وهذا ما أشارت إليه الاتفاقية الأوروبية لمكافحة جرائم الانترنت, والتي وقعت وانضمت وصادقت على سريانها على أراضيها، ومن أبرز هذه الوحدات:

1- على مستوى مصالح الشرطة: نجد:

أ. **القسم الوطني لقمع جرائم المساس بالأموال والأشخاص:** ويتكون هذا القسم من مجموعة من المحققين المتخصصين في مجال التحقيق في الجرائم الواقعة في البيئة الإلكترونية، ولقد بدأ هذا القسم مهامه سنة 1997، وهو يشهد منذ ذلك التاريخ ارتفاعاً هائلاً في عدد الشكاوى التي تصل إليه من جراء الجرائم الإلكترونية، إذ وصل عدد الشكاوى إلى 3000 شكوى سنة 2014.

ويقوم أفراد هذا القسم بمعالجة حوالي 10% من الجرائم المبلغ عنها، مع إحالة القضايا الأخرى التي يكون المشتبه فيها معروفاً إلى الجهات المختصة. وتجدر الإشارة إلى أن الشكاوى التي تصل إلى القسم تكون نتيجة للحجز على عناوين الـ "IP" وأرقام بطاقات الائتمان من قبل السلطات الأجنبية التي تحيلها بدورها إلى السلطات الوطنية عن طريق قنوات التعاون القضائي الدولي[1].

ب. المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات:

يعتبر هذا المكتب من أهم الوحدات الفرنسية في مكافحة الجرائم الماسة بالمعاملات الإلكترونية، تم إنشاؤه بموجب مرسوم وزاري مشترك رقم 00-405 المؤرخ في 2000/05/15 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية، ويساعد في نشاطاته كل من وزارة الدفاع ووزارة الاقتصاد والمالية والمديرية العامة للمنافسة والاستهلاك وقمع الاحتيال[2]. وهو يتمتع كغيره من المكاتب المتخصصة باختصاص وطني يتحدد نطاقه في الجرائم الخاصة والمرتبطة بتكنولوجيا المعلومات والاتصالات, سواءً كانت تلك التكنولوجيا محلاً للاعتداء، أو وسيلة لارتكاب أوتسهيل ارتكاب ذلك الاعتداء[3].

---

[1] Thierry Breton: Chantier sur la lutte contre la cybercriminalité; disponible en ligne suivant: *http://www.réseaux-telecoms.com*.

2 وهذا ما تنص عليه المادة 1 من المرسوم رقم 00-405 المؤرخ في 2000/05/15 المتضمن إنشاء المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات.

3 المادة 2 من المرسوم رقم 00-405 المؤرخ في 2000/05/15 المضمن انشاء المكتب المركزي لمكافحة الاجرام المرتبط بتكنولوجيا المعلومات والاتصالات.

كما يعتبر المكتب مكلفاً وفقاً للمادة الثالثة من المرسوم السابق الذكر بتنشيط وتنسيق عمليات ملاحقة مرتكبي الجرائم الواقعة في مجال الإتصالات الإلكترونية، وتقديم يد المساعدة لمصالح الشرطة الوطنية والدرك الوطني في حالة وقوع تلك الجرائم، ومن بين هذه المساعدات تلك التي تقدمها في إجراءات الضبط والتفتيش وفحص وحدات الحاسب الآلي كالأقراص الصلبة أو البيانات المتحصل عليها من الاتصال عبر الانترنت.

وتجدر الإشارة إلى أن هذا المكتب يمثل نقطة الإتصال المركزية في التبادلات الدولية، فهو من جهة يشارك على المستوى الوطني في تحريك وتنسيق الأعمال التحضيرية اللازمة، ومن جهة أخرى فهو يشارك في نشاطات المنظمات الدولية[1].

أما فيما يتعلق بالوحدات غير المتخصصة في مكافحة الجرائم الواقعة عبر المعاملات الإلكترونية في النظام الفرنسي نجد الإدارات الإقليمية للشرطة القضائية؛ وهي إدارات تابعة للمديريات الجهوية للشرطة, تساهم في التحقيق في جرائم الانترنت وملاحقة مرتكبيها والقبض عليهم, إما بناء على إذن من النيابة العامة، أو بناء على سلطاتها بشرط انعقاد اختصاصها الإقليمي.

2. على مستوى مصالح الدرك الوطني:

وينعقد اختصاص رجال درك الانترنت في مكافحة هذا النوع من الإجرام على مستويين:

أ. **على مستوى الإختصاص الوطني:** نجد:

- قسم الانترنت للمصلحة التقنية للبحوث القانونية والوثائقية، وهو يختص بجمع الأدلة الرقمية ويجعل المعلومات المستخلصة من التحقيق سهلة البلوغ للقضاة، ويعمل على تأمين الرقابة على شبكة الانترنت عن طريق البحث والتنقيب عن الجرائم الماسة بالبروتوكولات الأساسية للانترنت[2].

- وكذا القسم المعلوماتي الإلكتروني التابع لمعهد البحوث الجنائية للدرك الوطني الذي تم إنشاؤه منذ سنة 1992, ويعمل على تحليل البيانات المدمجة في الحواسيب الآلية في إطار التحقيقات القضائية، والمتعلقة بالأعمال الاقتصادية والمالية خاصة تلك المرتبطة بأرصدة المؤسسات وكذا أعمال القرصنة، وهو بالتالي يقوم بتقديم المساعدة التقنية لمختلف مصالح الدرك.

1 نبيلة هبة هروال، المرجع السابق، ص 126.

2 عمر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، مصر، سنة 2004، ص 812.

البند الثاني: الأجهزة المختصة بمكافحة الجرائم الماسة بالمعاملات الإلكترونية على صعيد الدول العربية.

لم تنأى الدول العربية كغيرها من دول العالم عن فكرة استحداث هيئات وأجهزة متخصصة لمكافحة الجرائم الواقعة في المجال الإلكتروني وعلى شبكة الانترنت؛ نظراً للضرورة العملية التي تستوجب تخصص هيئات ضبطية قضائية في مجال التحري والتحقيق عن مرتكبي هذه الجرائم، وكشف أساليب ارتكابها التي تعتمد على تقنيات فنية حديثة، ففيما تتمثل هيئات الضبطية القضائية لمكافحة جرائم الانترنت على مستوى الدول العربية عموما والجزائر خاصة ؟

أولاً: الأجهزة المتخصصة لمكافحة جرائم المعاملات الإلكترونية في مصر

كلفت جمهورية مصر العربية جهات وإدارات معينة بتلك المكافحة منها:

1- الإدارة العامة لمباحث الأموال العامة:

والتي تضطلع بمكافحة الجرائم الاقتصادية التقليدية بصفة عامة والمستحدثة بصفة خاصة, باعتبارها إحدى الروافد الرئيسية لقطاع الأمن الاقتصادي, ومن أكثر تلك الجرائم مكافحة جرائم تزوير العملات الورقية التي يكون الحاسب الآلي أداة لارتكابها[1].

2- الإدارة العامة للتوثيق والمعلومات:

تعتبر هذه الإدارة من أكبر الإدارات بوزارة الداخلية تعاملاً مع الجرائم المعلوماتية، وهي في ذلك تختص بعمليات المتابعة الفنية لكثير من الجرائم، ويبدأ عملها من خلال المتابعة الفنية والتحري عن الجرائم المبلغ عنها من الإدارات الأخرى, وذلك من خلال استخدام شبكة الانترنت هذا من جهة، ومن جهة أخرى فهي تقوم بتحديد المتهم من خلال عملية التتبع، ويعتمد أسلوب عمل هذه الإدارة في معرفة شخص مرتكب الجريمة على استخدام البرامج الحديثة وذلك عن طريق الاعتماد على رقم (IP) الذي يتعامل من خلاله الشخص مع شبكة الانترنت[2].

وحرصاً على مواكبة أجهزة الشرطة المصرية التطور الذي تنتهجه بلدان العالم المتقدم من ضرورة الاهتمام بمكافحة ما يستجد من صورة حديثة في ارتكاب الجرائم, فقد تم إنشاء الإدارة العامة لمكافحة

1 نبيلة هبة هروال، المرجع السابق، ص 110.

2 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، 2009، ص 185.

جرائم الحاسبات وشبكات المعلومات سنة 2002، وهي تابعة للإدارة العامة للمعلومات والتوثيق، وتتكون من ضباط على أعلى درجة من التخصص والحرفية في تكنولوجيا الحاسبات وشبكة الانترنت, مقسمين على أجهزة مختصة منها قسم العمليات، وقسم التأمين، وقسم البحوث والمساعدات الفنية.

ثانياً: الأجهزة المتخصصة لمكافحة جرائم المعاملات الإلكترونية في الإمارات العربية المتحدة:

لم تقم الإمارات العربية المتحدة بإنشاء جهاز متخصص بمكافحة جرائم الانترنت، وإنما قامت بإحكام الرقابة على شبكة الانترنت عن طريق ما يعرف بنظام الرقيب "proxy"، الذي يقوم بمراجعة الخدمات المقدمة على الشبكة، فهو يقوم بمراجعة المواقع الممنوعة أو المحظورة، ومنع الولوج إليها بعد وصول إشارة إلى الرقيب تنبهه من ذلك[1].

وبرأينا يؤخذ على النظام الإماراتي عدم استحداثه لجهاز خاص بالبحث والتحري في جرائم المعلوماتية, خاصة بعد إصدار قانون خاص بمكافحة جرائم المعلوماتية على اعتبار أن نظام الرقيب يمثل دور وقائياً، وتبقى مسألة المعالجة البعدية التي لا تتم إلا عن طريق جهاز خاص بالبحث والتحري والكشف عن مرتكب الجريمة ومحاكمته، لأنه لا يمكن اعتبار أن نظام الرقيب فعالاً بالمطلق, بل يمكن أن تقع جرائم عبر الإنترنت قد تفلت من قبضة هذا النظام، وتحتاج إلى مكافحة بعدية عن طريق جهاز متخصص في هذا الغرض.

ثالثاً: الأجهزة المتخصصة في مكافحة الجريمة المعلوماتية في النظام الجزائري:

في ظل التطور الحاصل في مجال مواجهة الجرائم الماسة بالمعاملات الإلكترونية، أحدثت هذه الأخيرة حالة من الطوارئ في أجهزة القضاء وأجهزة الضبط القضائي في مجال التحري والتحقيق، مما جعل الجزائر تتجه إلى تبني جملة من الهيئات الخاصة بمواجهة هذا الإجرام المستحدث، وكذا تطوير عمل الهيئات التقليدية للشرطة القضائية لمواكبة وتدارك المواجهة الفعالة للجريمة الإلكترونية، وسيتم بيان هذه الهياكل وفقاً لما يلي:

1- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

أُنشأَت هذه الهيئة بموجب المادة 13 من القانون 09-04 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ثم جاء المرسوم رقم 15-261 المؤرخ في 8

1 جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 78.

أكتوبر 2015 الخاص بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها, ليبرز كيفية تكوين وسير هذه الهيئة، بحيث نص على أن تتشكل هذه الهيئة من لجنة يرأسها الوزير المكلف بالعدل, وثلاث مديريات, ومركز للعمليات التقنية, وملحقات جهوية, كما يتمثل أعضاؤها في الوزير المكلف بالداخلية، والوزير المكلف بالبريد والتكنولوجيا، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا[1].

ومن مهام هذه الهيئة تفعيل التعاون القضائي والأمني الدولي، وإدارة وتنسيق العمليات الوقاية من هذه الجرائم، وتعمل على مساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[2].

2- الأقطاب القضائية الجزائية المتخصصة:

تم استحداث هيئات قضائية متخصصة في مجال مكافحة الجريمة المعلوماتية بموجب القانون رقم 14/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الاجراءات الجزائية، تختص بمكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقاً للمواد 37 و39 و40 من قانون الإجراءات الجزائية الجزائري، ولقد منحها القانون اختصاص إقليمياً موسعاً طبقاً للمرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/5 بحيث تنظر في القضايا المتصلة بجرائم المعلوماتية المرتكبة في الخارج حتى لو كان مرتكبها أجنبياً إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني[3].

3- المعهد الوطني للأدلة الجنائية وعلم الجرائم:

يتفرع المعهد الوطني للأدلة الجنائية وعلم الجرائم إلى إحدى عشر (11) دائرة متخصصة في مجالات مختلفة، تختص بإنجاز الخبرة، والتكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي والإلكتروني

1 المادة 6 و7 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

2 انظر المادة 14 من القانون 09-04 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

3 هواري عياش، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ،مداخلة ملقاة بالملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، كلية الحقوق، بتاريخ سنة 2016، ص 14.

مكلفة بمعالجة وتحليل وتقديم الأدلة الرقمية المساعدة للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات[1].

4- المديرية العامة للأمن الوطنـــي:

يأخذ دور المديرية العامة للأمن الوطني شكلاً توعوياً من خلال برمجة جملة الدروس التوعوية في مختلف الأطوار الدراسية، وكذا المشاركة في الملتقيات والندوات الوطنية, وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة البرامج الإلكترونية.

وفي إطار البعد الدولي لمكافحة الجرائم الواقعة على المعاملات الإلكترونية فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية التي تتيح مجالات التبادل المعلوماتي الدولي، وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الإنابات القضائية الدولية ونشر أوامر القبض للمجني عليهم دولياً[2].

الفرع الثاني: الأجهزة المتخصصة في مكافحة الجريمة المعلوماتية على المستوى الدولي والإقليمي.

لما كانت الجرائم الواقعة على المعاملات الإلكترونية يمكن أن تمتد آثارها حيزاً خارج حدود الدولة الواحدة، وهذا نظراً لخصوصية الوسيلة الإلكترونية المستخدمة فيها وشبكة الانترنت ذات الصبغة العالمية، فإن ملاحقة مرتكبيها وتقديمهم للمحاكمة وتوقيع العقاب عليهم، يتطلب ضرورة التعاون فيما بين الدول لإلقاء القبض على الجناة أو لجمع الأدلة أو سماع الشهود أو اللجوء إلى الإنابة القضائية, أو تقديم المعلومات التي يمكن أن تساهم في تحقيق ذلك، وهذا ما نصت عليه الاتفاقية الأوروبية لجرائم الانترنت، لكونه أصبح يمثل إحدى الضرورات اللازمة لمواجهة هذه الأنشطة الإجرامية المستحدثة على نحو يتكامل مع دور القوانين الداخلية[3].

وبهذا لم ينظر إلى التعاون باعتباره يخلق سيادة فوق الدول بقدر ما أصبح يعني التعاون بين سيادات دول مختلفة، ترمي جميعها إلى تشديد وتفعيل حلقات مكافحة الجريمة بوجه عام والجريمة العابرة للحدود بشكل خاص.

1 حملاوي عبد الرحمان، دور المديرية العامة للامن الوطني في مكافحة الجرائم الالكترونية، مداخلة ملقاة بالملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، كلية الحقوق، سنة 2016، ص 52.

2 عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999، ص 120.

3 هواري عياش، المرجع السابق، ص 17.

وما يهمنا في هذا الصدد هو التعاون الشرطي الدولي الذي يمثل أهم صور التعاون الدولي في مكافحة الجريمة الواقعة عبر التعامل الالكتروني وشبكة الانترنت، ذلك لكونه منظم للدخول إلى مركز المصادر التي تقدم المساعدات اللازمة في مجال التقريب والبحث وتبادل المعلومات بين سلطات التحقيق المختلفة للدول، ويساهم في تسهيل مكافحة الجرائم عن طريق تقديم حصيلة خبراتها إلى سلطات التحقيق.

ومن جهة أخرى, فإن أجهزة هذا التعاون تقوم بتحقيق الأهداف التي لا يمكن للشرطة الداخلية تحقيقها بمفردها, والتي منها تسهيل الدخول إلى المحتويات غير المشروعة المتواجدة في إقليم دولة أخرى بناءً على قرار قضائي واجب النفاذ، وتحديد مستخدميها وملاحقة المشتبه فيهم, وهو ما يدفعنا للتساؤل عن أنواع الأجهزة الدولية والإقليمية المختصة في مجال التعاون الدولي لمكافحة جرائم المعاملات الإلكترونية ؟

البند الأول: الأجهزة الدولية المختصة في مكافحة جرائم المعاملات الإلكترونية.

تعد المنظمة الدولية للشرطة الجنائية (الانتربول)[1] من أهم الوحدات المتخصصة في مكافحة جرائم الانترنت التي تتخذ باريس مقراً لها، وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون المتبادل بين سلطات الشرطة في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة، وإقامة وتنمية النظم التي من شأنها أن تسهم على نحو فعال في منع ومكافحة الجرائم الدولية.

وتباشر المنظمة دورها من خلال وظيفتين: **الأولى** هي القيام بتجميع كافة البيانات والمعلومات المتعلقة بالجريمة والجاني، من خلال المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة في إقليم الدول الأعضاء. أما الوظيفة **الثانية** فتتمثل في التعاون في ضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدولة التي تطلب تسليمهم، وهي في ذلك متخصصة بمكافحة الجرائم ذات الطابع الدولي خاصة تلك المتعلقة بالمساس بالأشخاص والأموال[2].

وتحقيقاً للأهداف المرجوة من إيجاد هذه المنظمة، والتوصيات الصادرة عن السكرتارية والمدير التنفيذي لها في عدة مؤتمرات دولية, دعت لضرورة تكثيف التعاون الدولي في مجال التحقيق في الاجرام الحديث الخاص بالمعاملات الالكترونية. وبهذا أنشأت المنظمة الدولية للشرطة الجنائية (الانتربول) وحدة

1 تضم هذه المنظمة 177 عضواً وهي تتكون وفقاً لنص المادة 5 من دستورها من خمس أجهزة: الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، وجهاز المستشارين والمكاتب المركزية الوطنية.

2 جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 76.

لمكافحة جرائم التكنولوجيا، بالإضافة إلى وضع استراتيجيات محكمة لمواجهة هذه الجرائم بالتعاون مع المجموعة الثمانية (G8) وذلك من خلال:

- إنشاء مركز اتصالات أمني عبر الشبكة يعمل 24 ساعة على 24 ساعة وفي كل الأيام على مستوى مصالح الشرطة للدول الأطراف.
- استخدام وسائل حديثة في تلك المكافحة كاستخدام تلك القاعدة من البيانات المركزية للدول الأطراف التي تستخدم برامج مقاربة وتحليل لتلك البيانات المساعدة على كشف الجرائم والتحقيق فيها[1].

البند الثاني: الوحدات المتخصصة في مكافحة جرائم الواقعة على المعاملات الالكترونية على المستوى الإقليمـــي.

على المستوى الأوروبي ظهرت مجموعة من الأجهزة المختصة في مكافحة جرائم الانترنت, ومن أبرزها الأوروبول, وجهاز الأورجست .

1- الأوروبول أو مركز الشرطة الأوروبية[2]:

هو أحد الأجهزة المتواجدة على المستوى الأوروبي, والتي تتخذ من لاهاي-هولندا مقراً لها, وهي تعمل على الوقوف في وجه الإجرام المستحدث عبر شبكات الانترنت عن طريق معالجة المعلومات المرتبطة بالأنشطة الاجرامية على مستوى الاتحاد الأوروبي، ودعم وتشجيع سلطات التحقيق, وذلك بتكميل ووسائلهم وتحديثها من أجل مكافحة جميع أنواع المنظم الدولي الخطير، وكذا بتسهيل تبادل تلك المعلومات عن طريق عن طريق تزويد المحققين بتحاليل عملية واستراتيجية، وبدعمهم بخبراته ومدهم بمساعداته التقنية.

وتجدر الإشارة إلى أن ملفات التحليل الثرية بالمعلومات المبلغة من قبل سلطات التحقيق التابعة للدول الأطراف في الاتحاد الأوروبي تمثل وسيلة هامة في عمل هؤلاء المحققين, وفي مكافحتهم للشبكات الإجرامية.

---

1 نبيلة هروال، المرجع السابق، ص 123.

2 تم إنشاء الأوروبول من قبل المجلس الأوروبي في لكسمبورغ سنة 1991 وهي منظمة عن طريق الاتفاقية الأوروبية الموقعة في 1995/07/26 والتي تحدد مهامها، والمسماة باتفاقية ماسترخت واتفاقية الاتحاد الاوروبي. وترجع فكرة إنشاء هذا الجهاز إلى اقتراح تقدم به المستشار الالماني Helmut khol أثناء قمة لكسمبورغ في 1991 بحيث يكون هذا الجهاز على نموذج الشرطة الفيدرالية الألمانية أي بمثابة مكتب فيدرالي أوروبي. انظر في ذلك: جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 79.

2- جهاز الأورجست:

يتواجد على المستوى الأوروبي إلى جانب الأوروبول جهاز الأورجست الذي يمثل أحد الوحدات المساعدة على التعاون القضائي والشرطي ومكافحة جميع أنواع الجرائم الخطيرة، وتنعقد اختصاصاته عندما يمس ذلك الإجرام دولتين على الأقل من أعضاء الاتحاد الأوروبي، أو دولة عضو مع دولة من دول العالم الثالث, أو دولة عضو مع الرابطة الأوروبية.

وهو يمثل دعامة في فعالية التحقيقات والملاحقات المتبعة من قبل السلطات القضائية الوطنية, وخصوصاً فيما يتعلق بالأنشطة المرتبطة بجرائم الانترنت، وهو في ذلك على علاقة وثيقة مع الأوروبول؛ إذ يمدها بالتحليلات اللازمة للقيام بالتحقيقات في الجرائم المنظمة، وهو يتكون من نواب عامين ومستشارين ومأموري ضبط قضائي للدول الأعضاء في الاتحاد الأوروبي ذوي الاختصاص، والمندوبين من قبل كل دولة عضو في الإتحاد وفقاً لنظامها القانوني.

وتتمثل أهم أهدافه في:

- تحسين التنسيق بين السلطات القضائية المختصة للدول الأطراف.
- تبادل المعطيات بين دول أعضاء الاتحاد الأوروبي وكذا التحفظ عنها.
- كما أنه يمكن أن يطلب من الوكلاء العامين ذوي الاختصاص الوطني إجراء تحقيقات أو إجراء ملاحقات أو التبليغ عن الجرائم إلى السلطات المختصة للدول الأطراف.

المطلب الثاني: آليات وإجراءات التحقيق الإبتدائي في الجرائم الماسة بالمعاملات الإلكترونية.

تعتبر إجراءات التحقيق هي مجموعة الإجراءات التي تهدف إلى التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه، وتهدف هذه الإجراءات في الجرائم الماسة بالمعاملات الإلكترونية إلى جمع وفحص الأدلة الإلكترونية القائمة على وقوع الجريمة ونسبتها إلى فاعلها، وتعتبر إجراءات التحقيق في مثل هذا النمط من الجرائم لا تخرج عن الأساليب المقررة في القواعد التقليدية, مع استحداث بعض الآليات الخاصة التي استلزمت التجربة الواقعية إيجادها لمحاربة صيغ وأشكال النشاط الإجرامي المستحدث الخاص بالجريمة المعلوماتية، وهذا على اعتبار أن الجرائم في المجال الإلكتروني تتميز بصعوبة اكتشافها وإثباتها بسبب ارتكابها بتقنيات كثيرة التعقيد, بالإضافة إلى سهولة محو وتدمير المعلومات الخاصة بارتكابها، وأنها تمتلك أيضاً صفة الدولية بحيث تتعدى الحدود والفواصل الجغرافية لعدة دول، ولقد أثبتت الدراسة المقامة من قبل شركة (Symantec) وهي شركة متخصصة في حماية الأنظمة والبرامج المعلوماتية سنة 2010، بينت فيها أن

الاعتداءات على الأنظمة المعلوماتية وإصلاحها سنوياً يسبب خسارة مالية قدرها 114 مليار دولار في العالم, وأن هذه الاعتداءات مست 431 مليون شخص[1].

وهنا يتضح أن مسألة المكافحة الإجرائية في مجال التحقيق والتحري عن ارتكاب هذه الجرائم قد أنشأ تحديات على مستوى التشريعات المقارنة التي سعت إلى مواكبة التطور الحاصل في المجال الإجرائي، ابتداءً من تعديل الأحكام الخاصة بالإجراءات الجنائية لتتماشى وهذا النمط من الجريمة، أو إصدار قوانين خاصة في مجال الإجراءات استحدثت من خلالها آليات جديدة تتعلق بمكافحة الجريمة المعلوماتية, وهي تستمد من الطبيعة الخاصة للنشاط الإجرامي الذي تتميز به هذه الجرائم.

وفي هذا الصدد يستوجب إبراز الآليات والإجراءات المتخذة في التشريعات الجنائية التقليدية عامة والتشريع الجزائري خاصة، وكذا الآليات وإجراءات التحري المستحدثة في هذا الصدد.

الفرع الأول: آليات التحقيق التقليدية في الجرائم الواقعة على المعاملات الإلكترونية.

إن التشريع الجنائي يفرض واجباً أولا على عاتق الشرطة القضائية هو استقصاء الجرائم والتحري عنها، فالتحقيق في الجرائم هو البحث عن جريمة لم يثبت وقوعها فعلاً، إما بناءً على شكوى أو إبلاغ، أو بناءً على تكليف من النيابة العامة، أو بناءً على معلومات وصلت إلى أعوان الضبطية القضائية من أي مصدر كان، أما الواجب الثاني وهو إثبات الجرائم؛ ويقصد به جمع الأدلة على وقوع الجريمة ومعرفة مرتكبها وإلقاء القبض عليه.

وفي سبيل قيام أعوان الضبطية القضائية بهذين الواجبين؛ لهم أن يسلكوا كل السبل المجدية لكشف الجريمة، فالقانون لم يحدد شكلاً خاصاً لاستقصاء الجرائم وجمع أدلتها، لذلك كان من حقهم أن يستعينوا بكل الوسائل المشروعة للتحري عنها، دون انتظار توجيه أو أمر مسبق.

ومن المؤكد أن قيام رجال الضبطية القضائية بأعمال الاستقصاء وإثبات الجرائم، إنما يهدف إلى مساعدة النيابة العامة على اتخاذ قرارها بتحريك الدعوى العمومية أو عدم تحريكها، وبهذا تعد إجراءات التحقيق الإبتدائي ذات أهمية سواء أكانت تتعلق بجرائم تقليدية أو مستحدثة، إلا أن الخصوصية الإجرائية في النوع الثاني تبرز بشكل جلي للفارق في أسلوب ارتكابها ونطاق وقوعها وتميز شخصية الجناة المرتكبين لها، هذا كله أعطى للآليات التقليدية المتخذة في مجال التحري والتحقيق الابتدائي للجرائم الواقعة في مجال المعاملات الإلكترونية طابع خاص, وهذا ما سيتم بيانه في النقاط التالية:

1 هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة)، مكتبة الآلات الحديثة، مصر، سنة 1994، ص 57.

البند الأول: المعاينة كآلية للبحث والتحري في الجرائم الواقعة على المعاملات الإلكترونية.

يعتبر إجراء المعاينة من أهم العقبات التي تواجه عملية التحقيق في الجرائم المرتكبة على المستوى الإلكتروني, ومن حيث المبدأ فإن المعاينة تأخذ مفهوم الرؤية بالعين لمكان أو شخص أو شيئ لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة، وعرفها البعض[1] بأنها إجراء يتم بمقتضاه انتقال المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها.

وتعد المعاينة كإجراء يجوز اللجوء إليه في كافة الجرائم، إلا أنها ليست إجراء مجدي أو صالح لكشف الحقيقة في الجرائم كلها، فهي ليست إجراء تلقائي في مباشرتها بل إجراء هادف غايته الكشف عن العناصر المادية التي تتعلق بالجريمة وتفيد في التحقيق الجاري بشأنها[2].

أولاً: أهمية المعاينة كإجراء تقليدي في الجرائم الإلكترونية.

للمعاينة أهمية كبيرة في كشف غموض الكثير من الجرائم التقليدية, فيما عدا الحالات الإستثنائية كما هو الحال في جريمة التزوير المعنوية وجريمة السب التي تقع في وضع غير علني، إلا أن دورها في مجال كشف غموض الجرائم الإلكترونية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها, لا ترقى إلى نفس الدرجة من الأهمية نظراً للاعتبارات التالية:

1. أن الجرائم في المجال الإلكتروني قلما يتخلف عن ارتكابها آثار مادية، وما ينتج عنها من أدلة يتمثل في بيانات غير مرئية يصعب معاينتها.
2. كذا تردد العديد من الأشخاص على مسرح الجريمة خلال الفترة الفاصلة بين بين ارتكاب الجريمة واكتشافها, مما يفسح المجال لحدوث إتلاف أو تغيير أو عبث بالآثار المادية، مما يضعف من قوة الدليل المستمد من المعاينة.
3. إمكانية تلاعب الجاني في البيانات عن بعد، أو محوها عن طريق التدخل من خلال وحدة طرفية، لذلك ينبغي على المشرع أن يقرر جزاءات جنائية على كل من يقوم بإجراء تغيير أو تعديل في المعلومات المخزنة في ذاكرة الحاسوب أو في بنك المعلومات أو قاعدة البيانات قبل قيام سلطة التحقيق بإجراء المعاينة، وهو مانص عليه كل من المشرع الجزائري في المادة 43 من قانون الإجراءات الجزائية, والمشرع الفرنسي من خلال نص المادة 1/55 من قانون الاجراءات الجنائية الفرنسي, وذلك حرصاً منهما على

1 محمد زكي أبو عامر، الاجراءات الجنائية، دار الجامعة الجديدة، الاسكندرية، ط7، سنة 2002، ص 233.

2 هشام محمد فريد رستم، المرجع السابق، ص 57.

المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، والملاحظ أن أحكام هذه النصوص وإن كانت تنصرف إلى أغلب الجرائم التقليدية، إلا أنه يمكن تطبيقها عند معاينة مكونات الحاسوب ذات الطابع المادي كأشرطة الحاسوب والأقراص، بخلاف معاينة المكونات غير المادية التي تتطلب إجراءات خاصة[1].

ثانـــياً: آلية تنفيذ المعاينة في التحقيق في الجرائم الإلكترونية.

تتم المعاينة في الجرائم الواقعة على التعامل الإلكتروني كأي جريمة أخرى عن طريق الإنتقال إلى محل الواقعة الإجرامية، إلا أن الإنتقال هنا لا يكون إلى العالم المادي، وإنما إلى العالم الافتراضي بحيث يستطيع أحد عناصر الشرطة القضائية الانتقال إلى معاينة ارتكاب الجريمة من خلال الحاسوب الخاص به أو مقهى الانترنت, أو إلى مقر مزود خدمة الانترنت الذي يعتبر أفضل موقع يمكن من خلاله إجراء المعاينة[2].

وتتخذ المعاينة في الجرائم الواقعة في المجال الإلكتروني عدة أشكال, وذلك حسب نوعية الجريمة المرتكبة، إلا أن هناك طرقاً عامة تتوافق مع طبيعة النظام الإلكتروني مثل عملية تصوير الحاسوب بواسطة آلة تصوير تقليدية، أو عن طريق استخدام برمجية حاسوب متخصصة في أخذ صورة لما يظهر على الشاشة, وهو ما يعرف بطريقة تجميد الشاشة، أو أن يكون ذلك عن طريق حفظ الموقع باستخدام خاصية الحفظ المتوفرة في نظام التشغيل.

البند الثاني: إجراء التفتيش كآلية للتحقيق في الجرائم الواقعة على المعاملات الإلكترونية.

يعد إجراء التفتيش من أخطر الإجراءات المتخذة في مرحلة التحقيق وجمع الاستدلالات في الجرائم لمساسه بالأسرار الخاصة بالأفراد، فهو يعرف بأنه:"إجراء تقوم بمقتضاه جهات التحقيق البحث عن أدلة مادية لارتكاب الجريمة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص في حد ذاته، وذلك وفقاً للإجراءات القانونية المقررة"[3].

ونرى من خلال هذا التعريف أن التفتيش ما هو إلا وسيلة للإثبات المادي، ذلك لأنه إجراء يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد كشف الحقيقة, وغايته دوماً هي الحصول على الدليل المادي، وهذا ما يتنافر مع الطبيعة غير المادية للبيانات الإلكترونية، وهنا يجدر بنا التساؤل عن مدى صحة

1 نبيلة هبة هروال، المرجع السابق، ص 217.

2 جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 28.

3 قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الاسكندرية، سنة 2005، ص 15.

تطبيق أحكام التفتيش كإجراء تقليدي في التحقيق الجنائي على الجرائم الواقعة في المجال الإلكتروني؟ وبيان الإجراءات المستحدثة بخصوص إجراء التفتيش في مثل هذا النوع من الجرائم لتلائمها مع طبيعة الجريمة.

أما محل التفتيش في الجرائم الواقعة على المعاملات الإلكترونية وعبر الانترنت, فيمكن أن ترد على الحاسوب بمكوناته المادية والمعنوية كالبرامج وأنظمة التشغيل والبيانات المخزنة عليه، لأنه يعتبر وسيلة النفاذ إلى العالم الافتراضي، وقد يقع التفتيش على شبكة الإنترنت بما تشمل من مكونات برامجية وملحقات تقنية.

والتفتيش هنا وسيلة للبحث والتحري لكشف الجرائم فهو ليس غاية في حد ذاته، لأنه يهدف إلى ضبط الأشياء المادية المتعلقة بالجريمة، والتي تفيد في إظهار الحقيقة، والواقع أن تفتيش مكونات الحاسوب المادية لا تثير أي إشكال نظراً لطبيعتها المادية التي تقبل التفتيش والبحث واستخراج ما بداخلها من مخفيات, على عكس الحال بالنسبة لمسألة تفتيش المكونات المعنوية أو البرامج للحاسوب بحثاً عن الأدلة الرقمية التي تفيد في كشف الجريمة أو كيفية ارتكابها[1].

ولقد تنازع الفقه المقارن في اتجاهين مختلفين حول مدى صحة اعتبار البحث عن أدلة الجريمة في العالم الافتراضي نوعاً من التفتيش ويخضع لأحكامه في الشكل التقليدي, وذلك كما يلي:

1. **الإتجاه الأول:** ويجسده موقف بعض التشريعات المقارنة التي رفضت تطبيق أحكام التفتيش التقليدية على الجريمة المستحدثة، على اعتبار أن آلية التفتيش لا تتماشى وطبيعة البيانات الإلكترونية، وبهذا حثت على سن تشريعات جزائية حديثة قادرة على مواجهة التقنية الإجرامية التي صاحبت ظهور الحاسب الآلي وشبكة الانترنت، وأفردت جانباً كبيراً من تلك القوانين أحكام خاصة بإجراء التفتيش؛ منها القانون البريطاني من خلال قانون إساءة استخدام الحاسب الآلي لسنة 1990؛ إذ نص على إجراءات تفتيش نظم الحاسب الآلي في جرائم الولوج غير المصرح به على الأنظمة الإلكترونية، طالما كان هدف الولوج ارتكاب أفعال غير مشروعة عن قصد، أما إذا كان الولوج مجرداً ودون نية ارتكاب أفعال غير مشروعة فإن التفتيش يستلزم إذن قضائي.

1 هلال عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص 201.

وإلى جانب القانون البريطاني يوجد القانون الأمريكي الذي نظم إجراء التفتيش والضبط في بيئة الحاسب الآلي، وذلك من خلال القوانين الإجرائية الفيدرالية بشأن جرائم الكمبيوتر، ونجد أن فرنسا تبنت نفس الموقف من خلال الإتفاقية الأوروبية لجرائم الانترنت في نص المادة 19 منها[1].

2. **الإتجاه الثانـــي**: ويستند أنصار هذا الاتجاه إلى عمومية نصوص التفتيش التقليدي للتوسع في تفسيرها من أجل مد حكمها إلى البيانات الإلكترونية في الأنظمة المعلوماتية، ولقد أخذ بهذا الاتجاه خاصة المشرع الكندي من خلاله توسعه في تفسير نص المادة 487 من قانون العقوبات الكندي, ليشمل تفتيش وضبط بيانات الحاسب الآلي بغض النظر عن المكونات المادية كالأقراص والأسطوانات الممغنطة[2].

ونرى من مقام الموازنة بين الاتجاهين أن التشكيك في الطبيعة المادية للبيانات الإلكترونية على النحو الذي ذهب إليه أنصار الاتجاه الأول, أو الاعتراف بصلاحية التفتيش على البيانات الإلكترونية بشكل مطلق كما يراه أنصار الاتجاه الثاني هو أمر قد لا يكون له ما يسوغه، إذا لم يتم أولاً التمييز بين المعلومات من جهة, والبيانات الإلكترونية من جهة ثانية، فالأولى هي عبارة عن عملية أو علاقة تقوم بين الذهن البشري وبين أنواع المثيرات الناتجة عن الاتصال الإلكتروني, وهي بالرغم من تجسدها على ركيزة مادية تحتويها لتنتقل بواسطتها إلى الغير, ومن ثم لا مجال لأن يرد التفتيش عليها، أما البيانات الإلكترونية فهي نبضات أو ذبذبات إلكترونية قابلة لأن تسجل وتخزن على وسائط معينة، ويمكن نقلها وبثها وحجبها واستغلالها, فهي من حيث المبدأ لا تتشابه مع الحقوق والآراء والأفكار, بل هي شيئ له في العالم الواقعي وجود مادي, ومن ثم يصح قانوناً أن يرد عليها التفتيش.

أولاً: إجراءات التفتيش في الجرائم الواقعة على المعاملات الإلكترونية.

لقد تم بيان أن التفتيش في وجهه التقليدي يفترض أن ينصب على المكونات المادية بأوعيتها المختلفة للوقوف على الأدلة المثبة للجرم المرتكب وفقاً للشروط والإجراءات القانونية، إلا أن هناك حالات خاصة لإجراء التفتيش في الجرائم الواقعة على المعاملات الإلكترونية, وهذا ما سنبينه فيما يأتـي:

1 شيماء عبد الغني، المرجع السابق، ص 279.

2 تقضي المادة 487 من قانون العقوبات الكندي بإمكانية إصدار أمر قضائي وضبط أي شيئ... تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة، أو أنه سينتج دليلاً على وقوع الجريمة.

1- شروط التفتيش الإلكتروني:

تحرص أغلبية القوانين على إحاطة التفتيش بشروط وضمانات أساسية، بوصفه إجراء يمس بالحرية الشخصية، والغرض منها تحقيق الموازنة الضرورية بين مصلحة المجتمع في القصاص من المجرم وردعه, وبين حريات الأفراد، ومن الضمانات التي يجب توافرها منها ما هو موضوعي ومنها ما هو شكلي، وعلى هذا الأساس يتم بيانها فيما يلـي:

أ. الشروط الموضوعية للتفتيش الإلكترونـــي:

يقصد بالشروط الموضوعية للتفتيش بصفة عامة في الجرائم التقليدية, وبصفة خاصة في جرائم الانترنت الشروط اللازمة لقيام تفتيش صحيح، وهي سابقة له في المعتاد، ويمكن حصرها في توافر السبب والمحل والسلطة المختصة بإجرائه.

أ) سبب التفتيش الإلكترونـــي:

من المتفق عليه في الحالات التقليدية أن سبب التفتيش إنما يعني السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث، ويمكن إجماله بصورة مختصرة في وقوع جريمة تقع عبر التعامل الإلكتروني, وتتمثل إما في صورة جنحة أو جناية, واتهام أشخاص معينين بارتكابها أو المشاركة فيها، وفي قيام قرائن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة سواء بشخصه أو مسكنه أو بشخص غيره أو مسكنه[1]، وبتطبيق مفهوم سبب التفتيش الإلكتروني، لا بد أن نكون بصدد جريمة ارتكبت عبر الوسائل الإلكترونية واقعة بالفعل سواء أخذت وصف الجناية أو الجنحة، وتورط أشخاص معينين بارتكابها أو المشاركة فيها، وبتوافر قرائن قوية على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم.

ب) محل التفتيش الإلكترونـــي:

يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، ومحل التفتيش في الجرائم الواقعة عبر التعامل الإلكتروني هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الانترنت على العالم، والشبكة التي تشمل في مكوناتها المزود الآلي والملحقات التقنية.

1 وهذا ما أقرته محكمة النقض المصرية في إحدى أحكامها، إذ أقرت بأن:"الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة –جناية أو جنحة– واقعة بالفعل وترجحت نسبتها إلى متهم معين، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية". نقض 1967/10/16 مجموعة أحكام النقض، س 18، ق 37، رقم 195، ص 997.

ويعتبر هذا المحل غير قائم بذاته، وإنما يشمله مكان أو عقار أو يكون في ذمة مالكه أو حائزه؛ أي أن الحرز الذي يوجد فيه الحاسب الآلي هو بطبيعته حرز مادي أو شخصي، ولذلك وجب على الضبطية القضائية عند استصدار إذن التفتيش أن يحدد محل ذلك الإجراء تحديداً دقيقاً, وكذا الغرض منه وإلا وقع تحت طائلة البطلان[1].

ج) السلطة المختصة بالتفتيش الإلكتروني:

نظراً لخصوصية التفتيش الإلكتروني باعتباره أحد إجراءات التحقيق الابتدائي التي تمس بحريات الأفراد كما أسلفنا سابقاً، فإن المشرع الجزائري يحرص على إسنادها لجهة قضائية تكفل تلك الحقوق والحريات، وتتمثل هذه الجهة في قاضي التحقيق أو النيابة العامة باختلاف التشريعات كسلطة أصلية، واستثناءً في رجال الضبط القضائي[2]، وإذا كان الأصل أن يقوم قاضي التحقيق أو النيابة العامة بإجراء التفتيش بنفسه، غير أنه يمكن لمأمور الضبط أن يقوم استثناء في حالتي التلبس التي يجوز فيها تفتيش شخص المتهم في الجنايات والجنح المعاقب عليها، وكذا في حالة الإنتداب من قبل المحقق المختص لتفتيش منزل أو شخص المتهم. وفي هذه الحالة يجب أن يحدد في إذن الندب بالتفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها، والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الإستكشافي، بحيث لا يترك لصاحب الاختصاص في التفتيش أي سلطة تقديرية في ذلك.[3]

ب. الشروط الشكلية للتفتيش الإلكتروني:

لا يختلف الأمر في هذا النوع من الجرائم المستحدثة عن الجرائم التقليدية في كون أن إجراء التفتيش يجب توافر الشروط الشكلية لقيامه والتي تختلف من تشريع جنائي لآخر، إلا أنها تجتمع معظمها في الشروط الآتية:

أ) الحضور الضروري لبعض الأشخاص أثناء قيام إجراء التفتيش في جرائم المعاملات الإلكترونية:

والأصل أن يتم حضور المتهم، وهذا الشرط يكون قائماًحتماً في تفتيش الأشخاص طالما يعتبرون محل التفتيش، غير أنه في حالة تفتيش المساكن قد يغيب المتهم وتذهب التشريعات إلى اشتراط وجود من

1 هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، أسيوط، 2000، ص 30.

2 هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط 2، دار النهضة العربية، مصر، سنة 2008، ص 78.

3 خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الاسكندرية، سنة 2009، ص 222.

ينوب عنه وإذا تعذر ذلك يجوز أن يحضر التفتيش شاهدين من أقارب المتهم البالغين أو القاطنين معه بالمسكن[1].

ويلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم 06-22 من المادة 45 منه استغنى المشرع من خلاله عن ضمانة حضور الأشخاص المحددين في الفقرة الأولى من هذه المادة في جرائم معينة منها المساس بأنظمة المعالجة الآلية للمعطيات.

ب) الميقات الزمني لإجراء التفتيش في الجرائم الإلكترونيــة:

ويقصد بضمانة الميقات في التفتيش أن يجريه القائم به خلال فترة زمنية يحددها المشرع، وذلك حرصاً على تضييق نطاق الاعتداء على الحرية الفردية، في حين نجد بعض التشريعات الإجرائية تركت أمر تحديد ذلك التوقيت للقائم بالتفتيش, ومن ثم يقوم به في كل الأوقات سواء ليلاً أو نهاراً, ومن بين تلك التشريعات قانون الإجراءات الجنائية المصري، وعلى العكس من ذلك نجد القانون الجزائري والفرنسي يحددان التفتيش في ميقات زمني معين، إلا أنه يرد استثناء على هذا المبدأ في جرائم محددة يصح فيها إجراء التفتيش في كل الأوقات[2].

فالبنسبة للمشرع الجزائري بالإضافة إلى جريمتي المخدرات والإرهاب التي أجاز فيها المشرع الجزائري للضبطية القضائية إجراء التفتيش في كل ساعة من ساعات النهار أو الليل، أضاف قائمة من الجرائم وذلك من خلال المادة 10 من القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، وتتمثل هذه الجرائم في الجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

وهنا نجد أن المشرع قد أدرك طبيعة الجرائم الواقعة في المجال الإلكتروني, ومدى خطورة قابلية الدليل الإلكتروني للمحو والتدمير في وقت قياسي، لذلك إرجاء التفتيش في الموعد القانوني قد يعرقل السير الطبيعي لمجريات التحقيق.

2. آلية تنفيذ إجراء التفتيش التقليدي على الجرائم الواقعة في التعاملات الإلكترونية:

وهنا يلزم التمييز بين حالات تنفيذ إجراء التفتيش كعملية هادفة للبحث وضبط الأدلة المادية وهي:

1 فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه حقوق (القانون الجنائي والعلوم الجنائية)، كلية الحقوق، جامعة الجزائر1، سنة 2010-2011، ص 330.

2 نبيلة هروال، المرجع السابق، ص 134.

أ. **الحالة الأولى:** في حالة الولوج إلى المكونات المادية للحاسوب بحيث تخضع إلى الإجراءات الخاصة بالتفتيش مراعاة لمكان وجود الحاسب أثناء مباشرة ذلك الإجراء، فيما إذا كان عاماً أو خاصاً، ذلك لأن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا تواجد في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له نفس الحكم, فلا يجوز تفتيشه إلا وفقاً لنفس شروط وضمانات تفتيش المسكن في التشريعات المقارنة المختلفة[1].

ب. **الحالة الثانية:** إذا كانت مكونات الحاسب الآلي محل الجريمة متصلة بحاسوب أو نهاية طرفية في مكان آخر غير مسكن المتهم، ففي هذه الحالة الأخيرة يتعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش الأماكن، أما إذا تعلق الأمر بتفتيش الحاسب الآلي ذا نهاية طرفية في دولة أجنبية, فقد نصت بعض التشريعات على طرق أخرى للتحقيق في الجرائم, وهي التنصت والمراقبة الإلكترونية لشبكات الحاسوب بقصد التعرف على مضمونها.

ج. **الحالة الثالثة:** وفي حالة تواجد مكونات الحاسوب المادية في الأماكن العامة كالمطاعم وسيارات الأجرة, فإن تفتيشها يكون وفقاً للحالات التي يتم فيها تفتيش الأشخاص, وبنفس الضمانات والقيود المنصوص عليها في مختلف التشريعات[2].

ثانياً: تفتيش الشبكات أو الأنظمة المعلوماتيــة:

من أهم المشكلات العملية التي تنشأ عن إجراء التفتيش في مجال الأنظمة المعلوماتية هو مشكلة اتصال الحاسوب موضوع التفتيش بحاسوب آخر موجود داخل أو خارج إقليم الدولة، فكثيراً ما يثبت بعد التحقيقات عملية تخزين المعلومات من قبل الجاني في حواسيب أخرى بهدف عرقلة التحقيقات، ونتساءل في هذه الحالة عن إمكانية أن يشمل التفتيش الحواسيب الأخرى المرتبطة بالحاسوب المطلوب تفتيشه. وهنا انقسم الرد إلى حالتين:

أ. **الحالة الأولى:** أن يكون حاسوب الجاني محل الجريمة مرتبط بحاسوب آخر موجود في مكان آخر داخل الدولة, وهناك جانب من الفقه الألماني يرى ضرورةأن يمتد التفتيش إلى المعلومات والبيانات المخزنة في

1 وهو ما يتضح من خلال نص المادة 46 من قانون الإجراءات الجزائية ،بحيث يشترط المشرع الجزائري للقيام بهذا الإجراء الحصول على رضا صريح من صاحب ذلك المسكن، ويجب كتابته بخط يد صاحب الشأن وتوقيعه ويجب مراعاة التوقيت بين الساعة الخامسة صباحاً والثامنة مساءً.

2 أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الاسكندرية، سنة 2015، ص 143.

حاسوب آخر غير الحاسوب محل التفتيش، وذلك استناداً إلى القسم 103 من قانون الإجراءات الجزائية الألماني. وهو نفس الموقف الذي اتجه إليه المشرع الهولندي في نص المادة 25 من مشروع قانون الحاسوب الذي أجاز أن يمتد التفتيش في هذه الحالة إلى نظم المعلومات والبيانات المتواجدة في حاسوب آخر بشرط ان تكون هذه المعطيات ضرورية لإظهار الحقيقة[1].

أما الفقرة الثانية من المادة 19 من اتفاقية بودابست فقد سمحت بتفتيش نظام حاسوب آخر أو جزء منها إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تم تخزينها في نظام ذلك الحاسوب، بشرط أن يكون نظام الحاسوب الآخر ضمن النطاق الإقليمي للدولة.

ب. **الحالة الثانية** وهي تعنى بتواجد الحاسوب محل الجريمة مرتبطا بنظام حاسوب آخر خارج إقليم الدولة الواحدة، في هذه الحالة يرى جانب آخر من الفقه الألماني استرجاع المعلومات والبيانات التي يتم تخزينها في الخارج يعتبر انتهاكا لسيادة الدول الأخرى، أما المادة 32 من اتفاقية بودابست فقد سمحت بتفتيش حاسوب موجود في دولة أخرى بشرط أن يتعلق التفتيش ببيانات متاحة للجمهور, وأن يتم التفتيش برضى صاحب البيانات[2].

ففي إحدى قضايا الاحتيال عبر الانترنت وبعد إجراء التحقيق تبين أن حاسوب المتهم الموجود في ألمانيا متصل بحواسيب أخرى في سويسرا؛ حيث تم تحريف المعلومات في هذه الحواسيب الخارجية، وعندما رغبت السلطات الألمانية الحصول على هذه المعلومات لم تستطع ذلك إلا من خلال طلب المساعدة المتبادلة[3].

وعلى ذلك نرى أن امتداد التفتيش إلى نظم الحاسوب الواقعة في بلد أجنبي له أهميته في إمكانية الحصول على الدليل عن بعد وفي بضع ثواني، إلا أن بعض الفقه يتحفظ على القيام بذلك لأنه يعتبر انتهاك لسيادة الدول الأجنبية، وإذا اقتضت ضرورة التحقيق القيام به ينبغي مراعاة العديد من الضمانات

1 **نقلاً عـــن**: محمد طارق الخن، المرجع السابق، ص 283.

2 هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 121.

3 عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الاسكندرية، سنة 2006، ص 383.

المتفق عليها سلفاً عن طريق اتفاقيات ومعاهدات في المجال، وهذا ما يؤكد أهمية التعاون الدولي في مكافحة مثل هذا النوع من الجرائم.

ثالثاً: موقف المشرع الجزائري من إجراء تفتيش الأنظمة المعلوماتيـة.

قرر المشرع الجزائري أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار الحالات المنصوص عليها في المادة الرابعة (04) من القانون 09/ 04 السالف الذكر إمكانية تفتيش منظومة معلوماتية أو المعطيات المخزنة عليها، ففي حالة ثبوت أسباب تدعو إلى الاعتقاد بأن المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى, يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطات القضائية مسبقاً بذلك[1].

وإذا تبين بأن المعطيات محل التحقيق والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج إقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل، ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية وخبرة بعمل المنظومة المعلوماتية محل التحقيق أو بالتدابير المتخذة لحماية المعطيات التي تتضمنها قصد مساعدتها, وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[2].

البند الثالث: إجراء ضبط البيانات الإلكترونيـــة.

يتجه أغلب الفقه[3] إلى تعريف الضبط بأنه وضع اليد على أي شيئ يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبها، والهدف الذي تسعى إليه سلطة التحقيق من القيام بالتفتيش هو ضبط الأدلة والمستندات والأشياء التي تفيد في كشف الجريمة وتحقيق العدالة، ولذلك ينبغي التقيد بالقواعد الإجرائية التي تحدد الأماكن التي يجوز تفتيشها أو الأشخاص الذين يجري تفتيشهم.

وضبط الأدلة الإلكترونية أو ما يتعلق بجرائم الحاسوب والانترنت يتصل بضبط المكونات المادية لأنظمة الحاسوب، وضبط المكونات المعنوية والبرمجيات، وضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط بالحاسبات معاً وما يتصل بها، وباعتبار مكونات نظام الحاسوب المادية من الأشياء، فإنها في الأصل ماديات يجوز ضبطها وتحريرها، وأما بالنسبة للشبكات فإن ما يعني التحقيق في

1 المادة الخامسة من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

2 عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، سنة 2007، ص 181.

3 خالد عياد الحلبي، المرجع السابق، ص 168.

الغالب المعطيات المستخرجة من الخوادم والأجهزة التي تحكم وتسيطر على هذه الشبكات، فإن تحصلت عليها جهات التحقيق من الجهة المعنية وفق ما يقرره القانون وما يجيزه ليس ثمة مشكلة، أما إن لم يتم تحصيلها وتوافر الموجب لضبط خادم الشبكة أي النظام المتحكم بالشبكة وأجاز القانون والقضاء ذلك، فإن ما يضبط قد يمتد إلى النظام المادي كله بما يتضمنه من معطيات وبرامج[1].

1- مدى صلاحية ضبط الأدلة الناتجة عن الجرائم الواقعة في المعاملات الإلكترونية:

يعتبر من حيث الأصل في الجرائم التقليدية قيام جهات التحقيق بضبط الأدلة المادية الناتجة عن وقوع الجريمة, والتي لا تثير أي إشكالاً بخصوص مدى خضوعها لعمليات التفتيش والضبط، إلا أن الأمر يختلف فيما يخص وقوع جرائم عبر التعامل الإلكتروني أو عبر شبكات الانترنت، بحيث أن الأدلة الناتجة عنها تأخذ طبيعة معنوية وغير محسوسة كالبيانات الإلكترونية، وبهذا اختلفت التشريعات الإجرائية والاتجاهات الفقهية حول مسألة ضبط الأدلة ذات الطبيعة المعنوية, والتي لا تصلح بطبيعتها محلاً لوضع اليد، وهي مجردة من أي دعامة مادية مثبتة عليها، ونشأ عن هذا الخلاف رأيين :

يرى البعض[2] أن بيانات الحاسوب لا تصلح لأن تكون محلاً للضبط، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفتوغرافي، أو بنقلها على دعامة مادية أو غيرها من الوسائل المادية، ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة، فالقانون الجنائي الألماني يجعل من الضبط إجراء يقع على الأشياء المادية المحسوسة حسب المادة 94 من قانون الإجراءات الجزائية، وأن البيانات المعالجة إلكترونياً لا يمكن ضبطها مجردة إلا إذا تم تحويلها إلى كيان مادي أو عن طريق التصوير الفتوغرافي، ويرى الإتجاه الثاني[3] أن البيانات المعالجة إلكترونياً ماهي إلا ذبذبات إلكترونية أوموجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة انتاجها، فوجودها المادي لا يمكن إنكاره.

ولقد كان الرأي لدينا هو تأييد خضوع الكيانات المعنوية المتمثلة في البيانات الإلكترونية وغيرها لإجراء الضبط، فالواقع يثبت أن القيمة الفعلية للبيانات الإلكترونية في تحديد وقائع الجريمة تفرض حمايتها

1 يونس عرب، المرجع السابق، ص 519.

2 علي الطوالبة، المرجع السابق، ص 138.

3 عفيفي كامل عفيفي، المرجع السابق، ص 353.

قانونياً، ومن ثم الاعتراف بها كالأدلة ذات الطبيعة المادية وإخضاعها لنفس الإجراءات دون تمييز حتى تتأتى النتيجة من ذلك وهي كشف حقيقة ارتكاب الجريمة الإلكترونية.

أما عن المشرع الجزائري فلقد قرر بموجب المادة 06 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أنه في حالة اكتشاف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، فإنه ليس من الضروري حجز كل المنظومة, بل يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية، ولقد عمل المشرع الفرنسي على تعديل قانون الإجراءات الجزائية بموجب قانون الأمن الداخلي رقم: 2003/239 واستحدث الفقرة الثالثة من المادة 57 التي تنص على المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة يتعين نسخها على دعامات التخزين المعلوماتية، ويتم تحريزها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون[1].

2- آليات تنفيذ الضبط الإلكتروني:

إن تنفيذ إجراء الضبط الواقع على الأدلة المستخرجة من ارتكاب الجرائم الواقعة عبر التعامل الإلكتروني قد يقع على جهاز الحاسوب وملحقاته بشكل أولي، ذلك أنه يمثل الأداة الرئيسية لارتكاب الجريمة وكذا جميع المعدات الملحقة به أو المستخدمة بالاتصال بشبكة الانترنت كالمودم، وكذا جميع وسائط التخزين المتحركة كالاقراص المدمجة والأقراص المرنة والأشرطة المغناطيسية وغيرها، ولقد حدد المشرع الجزائري من خلال القانون 09-04 وسيلتين لضبط الأدلة الإلكترونية؛ **الأولى** عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون هذه الأخيرة قابلة للحجز ووضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية، وأما الوسيلة **الثانية** تكون باستعمال التقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى البيانات

1 جاء هذا التعديل استجابة لا تفاقية بودابست التي نصت على ضبط الدليل الإلكتروني في الفقرة الثالثة من المادة 19 من القسم الرابع باعتبارها أنه من سلطة كل دولة طرف أن تتخذ الإجراءات التالية:

– أن تضبط نظام الكمبيوتر أوجزء منه أو المعلومات المخزنة على وسيط من وسائط التخزين الخاصة بالكمبيوتر وأن تحافظ على سلامة تلك المعلومات المخزنة.

الإلكترونية التي تحتويها والقيام بنسخها, وهذا في حالة استحالة ضبط هذه المعطيات لأسباب تقنية وفقاً للوسيلة الأولى.

ويحوز الدليل في هذه الجرائم خصوصية متميزة فهو عبارة عن معطيات مخزنة في نظام معلوماتي أو إلكتروني، ولذلك كان من الواجب أن يكون المحقق في مثل هذه الجرائم مؤهلاً ومدرباً على التعامل مع تلك الأدلة وإلا فإنه قد يساعد على إتلافها وإفساد دلالتها، لذلك كان تأمين ضبطها أمراً لازماً، وهو ما حرص على تقريره المشرع الجزائري من خلال الفقرة الثالثة من نص المادة السادسة من القانون 09-04، حيث ألزم السلطات القائمة على تنفيذ إجراء الضبط أن تحرص على سلامة المعطيات في المنظومة المعلوماتية، وأن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات، وهو نفس الموقف الذي أقرته الهيئة الدولية لدليل الحاسب الآلي التي وضعت عدة ضوابط لعملية ضبط الدليل الإلكتروني؛ منها ألا تكون الإجراءات المتخذة في تحريز الدليل الإلكتروني سبباً في تغيير طبيعة هذا الدليل, وأن تكون جميع الأنشطة المتعلقة بتحريز الوثائق الإلكتروونية أو الدخول إليها أو نقلها موثقة توثيقاً كاملاً, مع المحافظة عليها وتوفيرها للمراجعة، وهو الأمر الذي أوردته الفقرة الثالثة من المادة 19 من اتفاقية بودابست.

الفرع الثاني: آليات التحقيق المستحدثة في الجرائم الواقعة على المعاملات الإلكترونية:

لم تسلم طرق وإجراءات الإثبات من تأثيرات المعلومات والتكنولوجيا، فالتناغم المطلوب تحقيقه دائماً بين طبيعة الدليل وطبيعة الجريمة التي يولد منها، أفرز إلى حيز الوجود نوعاً جديداً من الإجراءات التي تتماشى مع طبيعة الجرائم، وهذا لأن الجرائم المرتكبة عبر التعامل الإلكتروني تحتاج إلى وسائل وسبل تقنية تتناسب مع طبيعتها؛ بحيث يمكن اكتشاف الأدلة الإلكترونية من خلال خلق أفكار تساعد على الولوج إلى الحاسب أو شبكة الانترنت، ومن ثم وضع اليد على معالم الجريمة وكشف الجناة وفقاً لنفس المنهج المتبع في ارتكابها, وهذا ما يفسره استحداث التشريعات المقارنة لأسلوب التسرب أو الاختراق الإلكتروني, وكذا المراقبة الإلكترونية كإجرائين فعالين في مرحلة التحقيق الابتدائي, ومصدر هام للأدلة الإلكترونية .

البند الأول: أسلوب الاختراق أو التسرب عبر الانترنت.

وفي هذا البند نتطرق لمفهوم أسلوب التسرب عبر الإنترنت (أولاً), ثم شروط صحة إجراء التسرب (ثانياً) على النحو التالي:

أولاً: مفهوم أسلوب التسرب عبر الإنترنت:

تتمثل آلية التسرب في تلك العملية الأمنية المنسق لها من قبل جهات الضبط القضائي، وهي هدف إلى ولوج أحد عناصر الشرطة داخل جماعة إجرامية والتوغل داخلها من أجل اكتساب ثقتها, ومن ثم كشف حقيقة الخطط الإجرامية المرتكبة من طرفها وجميع تحركاتها لتسهيل عملية القبض عليها من طرف السلطات الأمنية[1]. ولقد عرفه المشرع الجزائري على أنه: "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف للفعل الإجرامي"[2].

ويتميز نظام الاختراق في الجرائم التقليدية عنه في الجرائم المستحدثة هو أن المخترق في الجرائم التقليدية غالباً ما يكون من الغير؛ أي ليس من أعوان الشرطة، أما المخترق في الجرائم المستحدثة فمن الممكن أن يكون دائماً من عناصر الشرطة، إذ أن الأمر لا يتطلب منه سوى الحصول على إذن رسمي من رؤساءه للقيام بهذه المهمة، ثم يلج بواسطة حاسوبه إلى شبكة الانترنت، حيث يستغل حلقات الدرشة والنقاش عبر الشبكة لاستدراج الجناة، وإيقاعهم في فخ التصريح بخططهم ومشاريعهم الإجرامية كالكشف عن آليات الاعتداء على أرقام بطاقات الائتمان بصورة احتيالية، أو إعداد مواقع لبيع المسروقات، أو مواقع تجارية وهمية لخداع المستهلكين والحصول على أموالهم، أو تزوير مواقع إلكترونية لها تعامل مع البنوك أو البورصات أو غيرها، ويمكن أن يطرح المرشد في مهمته أسئلة عديدة على الجاني للحصول على أكبر عدد من المعلومات التي يستفيد منها أعوان الضبطية المكلفة بالتحقيق في تعقب الجاني, والقاء القبض عليه[3].

ومن أمثلة التسرب والاختراق، قيام مكتب التحقيقات الفيدرالي FBI بضبط أفراد عصابة "فاستلان" Fastlan المنتشرين حول العالم الذين امتهنوا قرصنة البرمجيات وتحميلها على مواقع للهكرة، وجنوا أرباحاً وصلت إلى مليون دولار في فترة زمنية قصيرة، حيث تم إلقاء القبض على تسعة منهم في الولايات المتحدة الأمريكية، وتمت إدانتهم أمام هيئة المحلفين العليا في شيكاغو، وقد استعملت المباحث الفيديرالية في هذه القضية أسلوب التسرب، عندما دست أحد عناصرها في هذه العصابة إلى أن تم إلقاء القبض عليهم[4].

1 عمر بن يونس، المرجع السابق، ص 838.

2 المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري.

3 خالد ممدوح إبراهيم، المرجع السابق، ص 396.

4 شيماء عبد الغني، المرجع السابق، ص 383.

ثانياً: شروط صحة إجراء التسرب:

نظراً لخصوصية إجراء التسرب وما يحويه من مساس بحرمة الحياة الخاصة للمتهم فقد اشترط المشرع ضمانات معينة يتعين مراعاتها عند اللجوء إلى هذا الإجراء، وهي تنقسم إلى نوعين شكلية وموضوعية:

1. الشروط الشكلية لإجراء التسرب.

تنحصر الشروط الشكلية لقيام إجراء التسرب في صدور إذن من الهيئة المختصة، فلا يمكن بأي حال أن يباشر ضابط الشرطة القضائية هذه العملية بمفرده دون أن يكون له الإذن المسبق بذلك, وهو ما نصت عليه المادة 65 مكرر 11 بحيث يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن حسب الحالة بمباشرة عملية التسرب.

وعلى هذا الأساس فإن منح إذن التسرب يكون إما من قبل وكيل الجمهورية أو قاضي التحقيق، ويشترط أن يكون الإذن مكتوباً وإلا بطل إجراء التسرب طبقاً لنص المادة 65 مكرر 5 ، ومن جهة أخرى فإن إصدار الإذن في شكله الكتابي يجب أن يتضمن معلومات جوهرية تتمثل في ذكر هوية الضابط التي تقوم عملية التسرب تحت مسؤوليته، بالإضافة إلى تحديد المدة المطلوبة في عملية التسرب والتي لا تتجاوز أربعة (4) أشهر، ويمكن تجديدها حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي أذن بهذا الإجراء أن يأمر في أي وقت إيقافه قبل انقضاء المدة المحددة.

2. الشروط الموضوعية لإجراء التسرب.

تحدد أغلب التشريعات الجزائية جملة الجرائم التي يطبق من خلالها إجراء التسرب، بحيث يشترط القانون الجزائري لإجراء عملية التسرب في إطار جرائم محددة لا يمكن الخروج عنها وهي محددة في جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية، وجرائم تبييض الأموال، والجرائم الإرهابية وجرائم الفساد، والجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1]. كما أنه يشترط تسبيب إجراء عملية التسرب من خلال بيان العناصر التي أدت بالجهات القضائية المختصة لمنح الإذن، وكذا العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء والذي يكون ضمن طلبه الإذن.

1 المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري.

وتجدر الإشارة إلى أن المشرع الجزائري قد أسند مهمة إصدار إذن التسرب إلى وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية؛ أي أن المشرع خرج عن الأصل العام في التحقيق القائم على الفصل بين سلطتي الاتهام والتحقيق، ذلك أن المهمة الأساسية لوكيل الجمهورية هي تقديم المتهم للعدالة ومن الصعوبة أن يتجرد عن مهمته في الاتهام عندما يقوم بإصدار الترخيص بالتسرب، خاصة وأن طبيعة عملية التسرب فيها نوع من الخطورة على حرمة الحياة الخاصة للأفراد.

البند الثاني: المراقبة الإلكترونيـــة.

ونتطرق في هذا البند لمفهوم المراقبة الإلكترونية (أولاً), ثم لموقف المشرع الجزائري من آلية المراقبة الإلكترونية (ثانياً).

أولاً: مفهوم المراقبة الإلكترونية.

يقصد بالمراقبة الالكترونية ذلك العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع المعلومات عن المشتبه به، سواء أكان شخصاً أم مكاناً أم شيئاً وذلك لتحقيق غرض أمني[1]، فالمشتبه به الإلكتروني يمكن أن يكون شخصاً، أو موقعاً أو بريداً إلكترونياً مخالفا للقانون، وتشمل المراقبة الإلكترونية جميع تحركات المشتبه به عبر الانترنت بما في ذلك بريده الإلكتروني.

ويشترط في المراقبة الإلكترونية أن تكون مشروعة، والغرض من هذه المشروعية هو تحقيق نوع من التوازن بين حق الأفراد في الخصوصية، وحق المجتمع في مكافحة الجريمة بوسائل فعالة حفاظاً على أمنه، وعلى ذلك فيمكن لرجل الضبطية القضائية أن يقوم طبقاً للقانون بمراقبة أحد القراصنة أثناء اختراقه لحاسوب المجني عليه، أو أن يراقب أحد المواقع التي أعدت للاحتيال على الأفراد.

ومن الملاحظ أن أغلبية الدول أخذت بنظام المراقبة الإلكترونية ضمن شروط معينة بهدف رصد الجرائم المستحدثة، ففي الولايات المتحدة الأمريكية نظم قانون خصوصية الاتصالات الإلكترونية ECPA[2] كيفية الحصول على أجهزة العدالة على المعلومات المخزنة في مخدمات مزودي خدمة الانترنت، فأعطى الحق لأعوان الضبط القضائي في الحصول على المعلومات الأساسية للمشترك كالاسم والعنوان وغيرها، أو

1 مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الانترنت (دراسة مقارنة)، سلسة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد الخامس، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، سنة 2003، ص 192.

2 وهو اختصار لـ: the Electronic Communication Privacy Act وقد تم تعديله بموجب القانون الوطني الأمريكي Patriot Act 2001.

المعلومات المتعلقة ببريده الإلكتروني أو بريده الصوتي، بمجرد توجيه أمر من المحكمة إلى مزود خدمة الانترنت تأمره فيه بالكشف عن محتويات الحاسوب[1].

أما الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية "بودابست" فقد سمحت من خلال المادتان 20 و21 منها بمراقبة حركة البيانات ومحتواها أثناء عملية التراسل، وأما عن المشرع الفرنسي فقد أصدر القانون 86-2000 المؤرخ في 2000/8/1 الذي عدل قانون حرية الاتصالات الذي سمح لمزودي الخدمات بمراقبة حركة رواد الانترنت.

ثانياً: موقف المشرع الجزائري من آلية المراقبة الإلكترونية:

لقد تبنى المشرع الجزائري إجراء المراقبة الإلكترونية من خلال نص المادة 4 من القانون 09-04 المتعلق بمكافحة جرائم تكنولوجيا المعلومات والاتصالات، وهذا بالسماح باللجوء إلى آلية المراقبة الإلكترونية في حالات محددة تتعلق بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو الماسة بأمن الدولة، أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

ولقد نص المشرع على آلية المراقبة الإلكترونية في قانون الإجراءات الجزائية في الفصل المتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور من خلال المواد 65 مكرر إلى 65 مكرر10، وقد حصر تطبيق هذا الإجراء على مجموعة من الجرائم كجريمة المخدرات أو الجريمة المنظمة العابرة للحدود، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات, وكذا جرائم الفساد وتبييض الأموال أو الإرهاب والجرائم المتعلقة بالصرف، وبهذا يعتبر إجراء اعتراض المراسلات في إطار التحقيق القضائي خارج هذه الجرائم المحددة أمراً خارجاً عن القانون.

1 محمد طارق الخن، المرجع السابق، ص 253.

المبحث الثاني:

وسائل الإثبات في الجرائم الماسة بالمعاملات الإلكترونيـــة.

كرست معظم الدساتير في العالم مبدأ "المتهم بريء حتى تثبت إدانته" وذلك حفاظاً على كرامة الإنسان إذا لم يقم الدليل القاطع على ارتكاب الجريمة، ويقصد بالإثبات في المسائل الجنائية "إقامة الدليل لدى السلطة الجزائية المختصة على حقيقة واقعة ذات أهمية قانونية وذلك بالطرق المنصوص عليها قانوناً"[1].

والإثبات هو العمود الفقري للعدالة الجزائية، إذ لا يمكن أن تحقق هذه العدالة بدون اللجوء إلى نظام إثبات يضمن تحقيقها، وقد عرفت التشريعات الإجرائية الجزائية نظامين رئيسين؛ **الأول** هو نظام الإثبات المقيد حيث يقوم المشرع في هذا النظام بتحديد طرق الإثبات والقوة الثبوتية لكل دليل من الأدلة بناءً على قناعة المشرع بها، ولا يكون لقناعة القاضي في هذا النظام أي دور في تقدير الأدلة والبحث عنها. أما النظام **الثاني** فهو نظام الإثبات الحر الذي يقوم على أساس حرية الإثبات، أي أن المشرع لا يقوم بتحديد الأدلة، بل يكون للقاضي دور إيجابي في البحث عن الأدلة وتقدير قوتها الثبوتية حسب قناعته بها، والواقع أن الاختلاف بين هذين النظامين لا يشكل سوى التباين في أسلوب اعتراف المشرع بالحقيقة[2].

وتعد مسألة الإثبات في الجرائم الواقعة على المعاملات الإكترونية من المسائل الشائكة لما تتصف به هذه الجريمة من سرعة في ارتكابها، وسهولة في طمس معالمها, ومع ذلك فإن الأدلة التقليدية كالشهادة والقرائن والاعتراف لم تتلاش أمام هذه الجريمة المستحدثة، وإن كان دورها قد تضاءل في عملية الإثبات، الأمر الذي أدى إلى ظهور ما يعرف بالدليل الرقمي الذي يتم الحصول عليه من خلال عملية البحث والتحري في حاسوب الجاني أو المجني عليه، أو في المواقع الإلكترونية.

فالأدلة الرقمية التي تنتج عن هذا الفحص التقني تبقى هي رأس الخيط الذي يوصل إلى تسلسل أحداث النشاط الجرمي، وبناءً على ذلك, تتم دراسة طرق الإثبات التقليدية في الجرائم الواقعة على المعاملات الإلكترونية (المطلب الأول)، ثم لطرق الإثبات المستحدثة (المطلب الثاني).

1 محمد طارق الخن، المرجع السابق، 295.

2 مصطفى محمد موسى، المرجع السابق، ص 196.

المطلب الأول: طرق الإثبات التقليدية في الجرائم الواقعة على المعاملات الإلكترونية.

لم يضمر دور وسائل الإثبات التقليدية في عصر التكنولوجيا والمعلومات، فمع أن هذه الوسائل المعروفة في إثبات الجرائم المادية، إلا أنها تلعب دوراً لا غنى عنه في إطار جرائم المعاملات الإلكترونية والجرائم الواقعة عبر الانترنت، فالشهادة والخبرة والاعتراف وغيرها من وسائل الإثبات التي حافظت على وجودها في عصر الطفرة التكنولوجية والمعلوماتية، وبناءً على ذلك سنلقي الضوء على دور طرق الإثبات التقليدية في إثبات الجرائم الواقعة على المعاملات الإلكترونية وعبر الانترنت من خلال ما يلي:

الفرع الأول: الشهادة كأداة إثبات في الجرائم الواقعة على المعاملات الإلكترونية.

تعرف الشهادة كوسيلة للإثبات بأنها:"الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء تعلق الأمر بثبوت الجريمة وظروف ارتكابها واسنادها إلى المتهم أو برائته منها"[1]. وتعد الشهادة من أقدم وأبرز وسائل الإثبات والحصول على الأدلة حتى أنه لا يخلو منها أي تشريع إجرائي، فلها أهمية بالغة في ميدان الإثبات؛ ذلك أن الجريمة ليست تصرفاً قانونياً بل عمل غير مشروع يحدث فجأة ولا يتيسر عادة إثباته بالكتابة، بل يجتهد الجاني في التكتم عند ارتكابه ويحرص على إخفائه، وبهذا أطلق على الشهود بأنهم عيون القضاء وآذانه.

ولا تقل الشهادة أهمية في الجريمة الواقعة عبر التعامل الإلكتروني عن باقي الوسائل الأخرى المتبعة في الحصول على الدليل الإلكتروني، فالقاعدة العامة تقتضي بأن يلتزم الشاهد بالإفضاء بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها، والإدلاء بكل ما يفيد في كشف الحقيقة من وقائع أخرى، وهنا يجدر بيان مفهوم الشهادة في مجال الجرائم الإلكترونية أو عبر الانترنت.

أولاً: الشاهد في الجريمة الإلكترونية:

يأخذ مفهوم الشاهد في الجريمة الإلكترونية معنىً متميزاً عن الشاهد في الجرائم التقليدية، إذ يقصد به الفني صاحب الخبرة والتخصص في تقنية الحاسب وشبكات الإتصال الذي يكون لديه معلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي ذلك[2].

1 أحمد شوقي الشلفاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 86.

2 د.هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، سنة 2006، ص 23.

ويرى الفقه[1] أن الشاهد المعلوماتي يمكن أن يكون من إحدى الطوائف الآتية:

1- **القائم على تشغيل الحاسوب:** وهو المسؤول عن تشغيل الحاسوب والمعدات المتصلة به، ويجب أن تكون لديه خبرة عالية في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات, كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.

2- **المبرمجون:** وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين هما؛ مخططوا برامج التطبيقات ومخططو برامج النظم، حيث تقوم الفئة الأولى بالحصول على خصائص دقيقة وموثقة لتحقيق هذه المواصفات, أما مخططو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسوب الداخلية؛ أي أنهم يقوموموون بالوظائف الخاصة بتجهيز الحاسوب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائل التخزين, بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج.

3- **المحللون:** وهم الأشخاص الذين يحللون الخطوات ويقومون بتجميع بيانات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات[2].

4- **مديرو النظام المعلوماتي:** الذين توكل إليهم أعمال الإدارة في النظم المعلوماتية، وهناك أشخاص آخرون يعدون بمثابة شهود في الجريمة الإلكترونية، وهذه الفئة لها دور كبير في توصيل المستهلك إلى شبكة الانترنت، من بينهم مقدمو الخدمات الوسطية في مجال المعلوماتية والانترنت.

وتطبيقاً لمفهوم الشهادة في الجرائم الإلكترونية؛ فهي تتمثل في الأقوال التي يدلي بها من أدخلوا البيانات الإلكترونية، أو العاملون في إحدى الشركات الذين تم تكليفهم بإرسال الرسائل الإلكترونية إلى الزبائن, إذا تبين فيما بعد أن هذه الشركة كانت تقصد من وراء هذه الرسائل الاحتيال على الزبائن والاستيلاء على أموالهم دون علم العاملين في الشركة[3].

ثانياً: التزامات الشاهد المعلوماتـــــي: إذا كان يلزم على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يجب من معلومات جوهرية لازمة للولوج في الحاسبات والمواقع الإلكترونية التي تحتوي على المعلومات

1 محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، 1991، ص 33 وما بعدها.

2 أشرف عبد القادر قنديل، المرجع السابق، ص 162.

3 محمد طارق الخن، المرج السابق، ص 305.

التي تشكل جريمة بحثاً عن أدلة تثبتها، فيطرح التساؤل عن مدى التزام الشاهد المعلوماتي بالتعاون مع سلطة التحقيق ؟

خاصة وأن المؤتمر الدولي الخامس عند الجمعية العامة لقانون العقوبات والذي انعقد في "ريو دي جانيرو" بالبرازيل في الفترة مابين 4-9 سبتمبر 2004 فيما يتعلق بالقانون الإجرائي أوصى بالحاجة إلى التعاون الفعال من جانب المجني عليهم والشهود وغيرهم من مستخدمي تكنولوجيا المعلومات، وهنا يقصد بمدلول التعاون الفعال من قبل الشاهد هو قيامه بطبع الملفات المخزنة في ذاكرة الحاسوب، أو الإفصاح عن كلمة المرور، أو الكشف عن الشفرات الخاصة بالبرامج المختلفة التي استعان بها الجاني لارتكاب الجريمة[1]، كذا إن التعاون في مجال الشهادة المعلوماتية له أهمية بالغة، حيث أن من الجهة القضائية قد تجهل الأساليب الفنية التي يمكن اتباعها لوجود الأدلة التي تفيد في كشف الحقيقة, وقد لا يعلمها إلا الشاهد المعلوماتي.

وفي هذا الإطار يتنازع الفقه المقارن بين اتجاهين مختلفين حول مدى إلزام الشاهد في الجريمة الواقعة عبر التعامل الإلكتروني بتقديم دليل فني؛ بحيث يرى البعض[2] أنه ليس من واجب الشاهد وفقاً للالتزامات التقليدية للشهادة أن يقوم بطباعة البيانات المخزنة في ذاكرة الحاسوب, أو تحليل ذاكرة النظام المعلوماتي لكشف آثار البيانات الإلكترونية، وعلى عكس هذا الاتجاه يرى جانب آخر[3] أن من بين الالتزامات التي تقع على الشاهد القيام بالإدلاء بكافة المعلومات الفنية والضرورية وهذا بالقيام بطبع ملفات البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة.

ونجد مشروع قانون الحاسب الآلي في هولندا يساير هذا الرأي؛ إذ يتيح لسلطات التحري والتحقيق إصدار الأمر للقائم بالتشغيل النظام لتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، وهو نفس الرأي لدى بعض الفقة الفرنسي الذين يبررون هذا الموقف على أساس أن المشرع الفرنسي طالما لم ينظم هذه المسألة فإنه لا مناص من تطبيق القواعد العامة للشهادة[4].

1 د.جميل عبد الباقي الصغير، أدلة الإثبات الجنائي في التكنولوجيا الحديثة، دار النهضة العربية، سنة 2002، ص 104.

2 أشرف عبد القادر قنديل، المرجع السابق، ص 166.

3 هلالي عبد الله، التزام الشاهد بالإعلام في الجرائم المعلوماتية، المرجع السابق، ص 66.

4 **نقلاً عــن** : عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 35.

ونرى أنه وفقا للقواعد العامة أن الشاهد لا يلزم إلا بذكر ما يعلمه عن الجريمة ولا يجوز إجباره القيام بعمل معين، إلا أنه تطبيقا لهذا المبدأ على الجريمة الواقعة عبر التعامل الإلكتروني قد تخلق عائقا في مدى إثبات وقائع وأفعال تأخذ طابعاً فنياً، ولها أهمية في مجرى التحقيق والحصول على دليل ارتكاب الجريمة، وهنا يستلزم الخروج على المبدأ العام وتعاون الشاهد في هذا الصدد بكل ما يلزم لتقديم البيانات الإلكترونية التي تفيد ذلك، إلا أنه في حالة وجود بعض التشريعات لا تلزم الشاهد بالإدلاء بالمعلومات، فهنا يستوجب تدارك قصور وسيلة الشهادة في الحصول على الدليل الإلكتروني بضرورة البحث عن وسيلة قانونية جديدة تحقق ما لم تستطع فكرة الالتزام بأداء الشهادة أن تؤديه, وهو الإلتزام بالإعلام في الجريمة المعلوماتية.

الفرع الثانـــي: الخبرة المعلوماتيـــة.

تعتبر الخبرة الفنية إجراء للتحقيق يعهد به القاضي إلى شخص مختص تتعلق بوقائع مادية يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علمياً أو فنياً، فتعتبر هذه الوسيلة عوناً ثميناً لجهة التحقيق والقضاء ولسائر السلطات المختصة في الدعوى الجنائية لكشف الحقيقة، فبدونها يتعذر الوصول إلى الرأي السديد بشأن المسائل الفنية التي يكون على ضوئها كشف جوانب ارتكاب الجريمة من الناحية العلمية والفنية[1].

لذلك اهتمت التشريعات المقارنة بتنظيم أعمال الخبرة ومنها المشرع الجزائري الذي أجاز من خلال قانون الإجراءات الجزائية الاستعانة بالخبراء لكل من مأموري الضبط القضائي والنيابة العامة وقاضي التحقيق، ولم يحظر على المحاكم أن تستعين بالخبراء إما من تلقاء نفسها أو بناءً على طلب الخصوم[2]، وإن كانت للخبرة تلك الأهمية في الجرائم التقليدية, فإن أهميتها تزداد وتصبح ضرورية بل وحتمية في اشتقاق الأدلة الإكترونية لإثبات الجرائم الإلكترونية؛ نظراً لأنها تتعلق بمسائل فنية في غاية التعقيد, وما يزيد من أهميتها كونها تتعلق بأساليب إجرامية واقعة في مجال افتراضي تصبغ بطابع السرعة والغموض، وهنا لا يمكن مواجهة تلك الصعوبات إلا من خبير في مجال المعلوماتية.

والواقع أن الخبرة الفنية بدأت تأخذ حيزاً في مجال إثبات جرائم المعاملات الإلكترونية حتى أصبحت تعرف في الفقه المقارن بمصطلح " الخبرة المعلوماتية الشرعية" ويمكن تعريف المعلوماتية الشرعية بأنها استخدام الطرق العلمية لجمع وتعريف وتحليل وتفسير الدليل الرقمي المأخوذ من مصادر رقمية، والاحتفاظ به وتوثيقه

1 خالد ممدوح ابراهيم، المرجع السابق، ص 283.

2 أشرف عبد القادر قنديل، المرجع السابق، ص 168.

على نحو يسهل بناء الحوادث التي تؤدي إلى اكتشاف الجريمة، فالمعلوماتية الشرعية هي عملية البحث التي يقوم بها الخبير المعلوماتي من أجل الحصول على الدليل الرقمي بغية إعادة بناء مجريات القضية وتوضيحها للمحكمة[1].

أولاً: القواعد القانونية التي تحكم أسلوب الخبرة المعلوماتية.

تعتبر الخبرة المعلوماتية في أغلب التشريعات شأنها شأن الخبرة القضائية في الجرائم التقليدية من حيث القواعد القانونية التي تحكم الخبرة عموماً, سواء من خلال اختيار الخبراء أو من حيث عمليات الخبرة في ذاتها باختلاف الأمور الفنية التي تحكم عمل الخبير التقني.

ولذلك أعطت التشريعات الجزائية الحرية للقاضي الجزائي في الاستعانة بالخبرة لتكوين قناعته الشخصية، فله مطلق الصلاحية في اختيار الخبير المعلوماتي الذي قد يكون شخصاً طبيعياً أو معنوياً كالشركات المختصة في تكنولوجيا المعلومات، ويرى بعض الفقه[2] أنه يمكن للقاضي اختيار الخبير المعلوماتي من بين خيارات معينة كالجهات المختصة بالخبرة, أو جهات الضبط القضائي, أو آلية التعاون الدولي.

ثانياً: الجهات المختصة بالخبرة المعلوماتيــة:

إلى جانب الخبرة الفردية يمكن للقاضي أن يلجأ إلى الشركات المختصة في مجال تكنولوجيا المعلومات والاتصالات التي تضم في الغالب خبراء على مستوى عال من الكفاءة، فهذه الجهات قد تعمد في الغالب إلى التعامل مع خبراء ومختصين لهم ذيع في هذا المجال، ولو لم يكونوا من خريجي الأكاديميات؛ أي أن لديهم الخبرة العملية للتعامل مع الحواسيب وأنظمة الشبكة المعلوماتية فحسب، وهو ما ينطبق على القراصنة في مجال المعلوماتية الذين تتوافر لديهم الخبرة العملية دون تحصلهم على مستوى تعليمي عال أو متميز، ضف إلى ذلك أنه يمكن اللجوء إلى المؤسسات التعليمية المعروفة بإعداد قاعدة قوية في مجال دراسات الحاسوب والانترنت مثل جامعة "ستانفورد" ومعهد التكنولوجيا في ولاية ماساشوستس, اللذين شهدوا تخرج مجموعة من الخبراء ذوي الكفاءة العالية والمتميزة، وبالتالي يمكن للقاضي أن يلجأ إلى هؤلاء الفئات في مجال الخبرة المعلوماتية[3].

1 محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، العدد 30، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 176.

2 عمر بن يونس، المرجع السابق، ص 819.

3 عمر بن يونس، نفس المرجع، ص 1023.

ومن جانب آخر، اتجهت أغلب الدول في العالم إلى إحداث أجهزة مختصة في مجال المعلوماتية الشرعية، فقد أسست الو.م .أ مؤخرا فرعاً تابعاً لمكتب التحقيقات الفيدرالية أطلق عليه "المخبر الإقليمي الشرعي للحاسوب" مقره "بسان دييجو"، حيث يتم من خلاله إعداد الباحثين في المجال المعلوماتي، ويمكن للقاضي اللجوء إلى الخبرة الأجنبية من قبل جهات خارجة عن الدولة، غير أن هذا الأمر يتوقف على مدى نشاط المشرع في كل دولة لإبرام اتفاقيات تعاون في هذا الصدد[1].

ثانياً: آلية تنفيذ الخبرة المعلوماتيـــــة.

يقوم الخبير المعلوماتي بفحص الأجهزة الرقمية المتعلقة بالجريمة سواء كانت عبارة عن حاسوب آلي أو مخدمات لدى مزود خدمة الإنترنت، لذا ثبت أن عمل الخبرة ينحصر في جملة من المراحل التي يجب أن توفر القدرة لدى الخبير على إتمامها وهي:

1- **مرحلة حجز البيانات:** من المعلوم في الفقه الجنائي في مجال الإجراءات الجزائية في مسألة الإثبات أن أي شخص يدخل إلى مسرح الجريمة يجب أن يأخذ منه شيئاً أو أن يترك خلفه شيئاً، وهو ما يتضح من خلال قيام أحد الأشخاص بإرسال رسالة إلكترونية تحمل مضموناً احتيالياً إلى أحد الأفراد، فإن الرسالة سيتم تخزينها على الخادمات الموجودة لدى مزود خدمة الإنترنت مع التاريخ والوقت، بالإضافة إلى مسار الرسالة وعنوان رقم النفاذ، وبهذا يجب على الخبير المعلوماتي أن يقوم بعملية حجز للبيانات المتعلقة بالجريمة لدى مزود الخدمة، إضافة إلى حجز الأجهزة التي تحوي هذه البيانات, والتي تكون بحوزة الجاني أو في مسرح الجريمة[2].

2- **مرحلة حفظ البيانات:** بعد مرحلة حجز البيانات يأتي دور الخبير في حفظها, بحيث يعمل على نسخ تلك البيانات إلى نسختين؛ الأولى تم تخزينها في الأجهزة الرقمية التي تم حجزها مما يضمن بقاؤها كدليل رقمي، والثانية عبارة عن نسخة طبق الأصل يتم عمل الاختبار والفحص عليها.

3- **مرحلة استعادة البيانات:** تجدر الإشارة إلى أنه في حالة حذف البيانات من قبل الجاني، يلزم الخبير باستعادتها, وهو أمر ضروري لاستكمال تقرير الخبرة وبناء القضية، ومثاله أن يستبعد الخبير الرسائل المحذوفة من قبل الجاني عن طريق الأثر الذي تتركه هذه الرسائل على جهاز التخزين.

1 مصطفى محمد موسى، المرجع السابق، ص 222.

2 Eoghan Casey, Digital Evidence and Computer Crime Foreensic, Science, Computers and the Internet, Second Edition, Academic Press An imprint of Elsevier, London 2004. p 260.

4- **مرحلة تحليل البيانات:** يقوم الخبير المعلوماتي بعملية تقييم لمحتوى البيانات الرقمية بحبث يفحصها بدقة من أجل تحديد وسائل الجريمة ودوافعها[1].

وبعدها يتوجه الخبير إلى مرحلة إعادة بناء القضية، وهي العملية التي تلي مرحلة الحجز والحفظ والتحليل من أجل توضيح مجريات أحداث الجريمة وكيفية وقوعها، فالدليل الرقمي المحصل عليه يحوي آثار من سلوك الجاني مثل الكلمات التي استخدمها والمواقع التي تصفحها، فالربط بين هذه السلوكيات يؤدي إلى معرفة وقت ومكان ارتكاب الجريمة والطريقة التي تمت بها.

5- **تحرير تقرير الخبرة المعلوماتية:** يتضمن تقرير الخبرة في محتواه النتائج التي توصل إليها الخبير من خلال عملية البحث، ويجب أن يحوي مواصفات مسرح الجريمة الواقعة في المجال الإلكتروني، مع شرح ملخص عن عملية الفحص التي تم القيام بها، بالإضافة إلى رواية أحداث القضية مع ذكر ملخص النتائج, وكذا اقتراحات الخبير المعلوماتي. ويلزم أن يكون التقرير المعد من قبل الخبير متسلسلاً من حيث الأحداث, وأن يكون مختصراً من الناحية التقنية، ومكتوباً بأسلوب بسيط وواضح حتى تتمكن المحكمة من فهمه.

وإذا رأت المحكمة نقصاً في التقرير، أو كان يحوي على مسائل غامضة وتحتاج إلى توضيح, فيمكن أن تقرر المحكمة من تلقاء نفسها أو على طلب من الخصوم, دعوة الخبير المعلوماتي لحضور الجلسة وتوجيه الأسئلة له لتدارك ذلك النقص, وفك مسائل الغموض[2].

رابعاً: مدى تأثير الـخبرة على قناعة القاضـــي.

يذهب جانب من الفقه[3] بأن الخبير المعلوماتي هو القاضي الحقيقي للدعوى؛ إذ يعتبر كل ما يبديه تقرير الخبرة هو عنوان الحقيقة التي تجبر القاضي على الأخذ بها، فوظيفة الخبير التقنية التي تعتمد على قدراته التقنية والفنية في حل المسائل المعقدة لاستنباط الأدلة الرقمية, لا تترك مجالاً للقاضي لتحديد مسار الدعوى، فالخبير هو الملهم الأساسي في كشف الحقيقة.

ويتجسد هذا الرأي في الدعوى المرفوعة من طرف طلبة يهود ضد شركة "ياهو" بسبب فتحها لمزادات علنية تتعلق بالنازية على إحدى صفحاتها المجانية، ولقد رفعت الدعوى أمام محكمة باريس الابتدائية

1 عبد الناصر محمد محمود فرغلي، محمد عبيد سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، ورقة بحث مقدمة إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2007، ص 35.

2 هشام رستم، المرجع السابق، ص 142.

3 عمر بن يونس، المرجع السابق، ص 967.

بناءً على أن شركة "ياهو" قامت بالتقليل من حادثة "الهولوكست" عندما سمحت بإجراء مثل هذا المزاد على الإنترنت، وقد أصدر القاضي حكمه على شركة "ياهو" بإلزامها بمنع المستخدمين من الدخول إلى هذا المزاد، واعتمد القاضي في حكمه على تقرير الخبرة المعلوماتية الذي يثبت قدرة الشركة على منع المستخدمين من الدخول، وهو الأمر الذي أصرت الشركة على نفيه. وبهذا تعد هذه القضية نموذجاً بارزاً يجسد اعتماد الحكمة على تقرير الخبرة دون مناقشته، بحيث أصدرت المحكمة قرارها بعد أيام من إبداع لجنة الخبراء[1].

ونرى أن اعتماد المحكمة على تقرير الخبرة المعلوماتية لا يعد مساساً بمبدأ قناعة القاضي الشخصية أو التأثير عليها، ولا يجعل من الخبير القاضي الحقيقي للدعوى حتى وإن ثبت عملياً اتجاه القاضي لاعتماد تقارير الخبرة في الأحكام الصادرة عنه، إلا أنه يبقى أمر طبيعي وغير مستحدث على الساحة القضائية، فالقضاء قد يستند في أحكامه إلى الخبرة التي تجري على البصمات أو على الحمض النووي أو على التحاليل النفسية، كما أن بناء الحكم على أساس الخبرة لا يختلف عن الأخذ بأقوال الشهود وبناء الحكم بالبراءة أو الإدانة، فمحكمة الموضوع هي صاحبة القرار في الأخذ بتقرير الخبرة من عدمه.

إلا أنه بالرجوع إلى مجال الخبرة المعلوماتية في إطار الجرائم الإلكترونية, نرى أنه من الواقعي أيضاً إعطاء قوة إلزامية لتقرير الخبير المعلوماتي، وذلك على أساس أن بعض المسائل المعقدة في مجال الجريمة الإلكترونية، قد لا تجد حلاً لها إلا بعد فحص وتحليل من قبل خبير معلوماتي, له الدراية والكفاءة في إيجاد الأدلة الرقمية لحل شيفرات ارتكاب الجرم، وبالإضافة إلى أنه إذا رفض القاضي رأي الخبير فهذا يشكل تعارض مع نفسه، إذ أنه يعني بذلك أنه أراد أن يفصل بنفسه في مسألة سبق وأن اعترف في بادئ الأمر بأن الخبير يتمتع فيها بمعرفة ودراية تفوق معرفته الشخصية.

1 **نقلاً عـــن**: عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 42.

المطلب الثاني: وسائل الإثبات المستحدثة.

لم تسلم وسائل الإثبات من تأثيرات ثورة المعلومات، فالتجانس المطلوب تحقيقه دائماً بين طبيعة الدليل وطبيعة الجريمة التي ينتج عنها, أفرز معه نوعاً جديداً من الأدلة يتماشى مع طبيعة الجرائم الواقعة على المعاملات الإلكترونية أو عبر شبكة الانترنت، وهو مايعرف بالدليل الإلكتروني[1].

ولقد ساهم القضاء المقارن في رسم مفهوم الأدلة الإلكترونية سواء من حيث القيمة القانونية أو الدور في كشف معالم الجريمة الإلكترونية، هذا ما اعتدَّت به المحاكم بناءً على نص تشريعي تارةً وعلى الاجتهاد تارة أخرى، ومن هذا المنطلق سنتناول بالبحث والتفصيل التعريف بالدليل الإلكتروني ومشروعيته (الفرع الأول), وأيضاً وسائل الإثبات الحديثة لإيجاد هذا الدليل (الفرع الثاني)، وتبقى مسألة سلطة القاضي في تقرير هذا الدليل محل بحث في الفصل الثاني على اعتبار أنها تخص مرحلة المحاكمة.

الفرع الأول: مفهوم الدليل الإلكتروني.

وفيه نتطرق لتعريف الدليل الإلكتروني (أولاً), ثم لخصائصه (ثانياً), على نحو يمكننا من معرفة مصادر الدليل الإلكتروني (ثالثاً).

أولاً: تعريف الدليل الإلكتروني.

لقد تعددت التعريفات بشأن الدليل الإلكتروني بين التوسع والتضييق, والمرجع إلى ذلك طبيعة المجال الذي يدور في فلكه وهو المعلوماتية، وعليه ذهب البعض[2] إلى تعريفه بأنه: "كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما".

وهناك من بنى تعريفه على أساس العقل والمنطق في طرق الحصول عليه؛ بحيث يعتبر أنه ترجمة البيانات الإلكترونية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال, ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بالجريمة أو بالجاني[3].

---

1 ولقد آثر ترجيح مصطلح الدليل الإلكتروني على أساس أنه المصطلح المستخدم من طرف المشرع الأوروبي في التوصية رقم 13/95 الخاصة بمشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات, والتي تم اعتمادها من قبل لجنة الوزراء في (1995/09/11)، كذلك تم استعمال المصطلح في الفقرة 2 من المادة 14 من اتفاقية بودابست الموقعة في 2001/11/23.

2 عمر بن يونس، المرجع السابق، ص 969.

3 محمود إبراهيم غازي، المرجع السابق، ص 670.

كما عرفه آخر[1] بأنه: "ذلك الدليل المشتق بواسطة النظم البرامجية المعلوماتية وأجهزة ومعدات الحاسوب أو شبكات الاتصال من خلال إجراءات قانونية وفنية, لتقديمها للقضاء بعد تحليلها علمياً, أو تفسيرها في شكل نصوص مكتوبة لإثبات وقوع الجريمة لتقرير البراءة أو الإدانة فيها". ولقد جاءت المنظمة الدولية لأدلة الحاسوب IOCE بتعريف الدليل الإلكتروني بأنه: "المعلومات المخزنة أو المتنقلة في شكل ثنائي ويمكن أن تعتمد عليها المحكمة في الإثبات"[2].

ومن الملاحظ من التعريفات السابقة أنها وضعت مفهوماً يستوعب المعلوماتية وما يواكبها من تطور سريع، إلا أنه يلاحظ أن البعض منها قد أخلط بين مفهوم الدليل الإلكتروني وبرامج الحاسب الآلي، حيث تم اعتبار الدليل المذكور كبيانات تم إدخالها إلى جهاز الكمبيوتر وذلك لإنجاز مهمة, وهذا يتطابق مع مفهوم برامج الحاسب الآلي، فإذا كانت برامج الحاسب لها دور في تشغيل الحاسب وتوجيهه إلى حل المشاكل, وبدونها لا يعد الحاسب سوى آلة صماء, ومدى نسبتها إلى مرتكبها والتعرف على كل المراحل التي مر بها المجرم في سبيل تحقيق الهدف الإجرامي، كما أن للتعريفات السابقة للدليل الإلكتروني دور في حصر الأدلة في أجهزة الحاسب وملحقاتها, أو ما يعرف بفتح نظم الحاسوبية ونظم الاتصال، إلا أن الواقع العلمي أثبت أن هناك نظم أخرى مدمجة بالحواسيب, قد تحتوي على العديد من الأدلة كالهواتف المحمولة والبطاقات الذكية.

وتأسيساً على التعاريف السابقة واسترشاداً بها, يمكننا القول بأن للدليل الإلكتروني هو: "معلومات مخزنة في أجهزة الحاسوب وملحقاتها أو متنقلة عبر شبكة الانترنت، والتي يتم تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة, بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها".

ثانياً: خصائص الدليل الإلكترونـــي.

إن البيئة الإلكترونية التي ينبثق منها الدليل الإلكتروني تعتبر بيئة متطورة بطبيعتها, فهي تشمل على أنواع متعددة من البيانات الإلكترونية منفردة أو مجتمعة, تصلح لأن تكون دليلاً للإدانة أو البراءة، وقد انعكست هذه البيئة على طبيعة الدليل, مما يجعله يتصف بعدة خصائص تميزه عن الدليل الجنائي التقليدي وهي:

1 عبد النصر محمود فرغلي, وعبيد سعيد المسماري، المرجع السابق، ص 13.

2 Eoghan Casey, Op. Cit. p 271.

1. يعتبر الدليل الإلكتروني دليلاً علمياً يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة ولاتدرك بالحواس العادية، ومن ثم يتطلب إدراكه الإستعانة بأجهزة ومعدات تقنية للتعامل معه، فالدليل الإلكتروني أشبه بالدليل العلمي له منطقه وبيئته التي يتكون فيها لكونه من طبيعة تقنية.
2. كما يمتاز الدليل الإلكتروني بأنه يصعب التخلص منه بشكل نهائي, عكس الأدلة التقليدية التي يمكن التخلص منها بسهولة بدون رجعة، فالدليل الإلكتروني يمكن استرجاعه بعد محوه وإصلاحه بعد إتلافه، وهذا بفضل بعض البرامج والتطبيقات التي تمكن من استعادة البيانات التي تم حذفها أو إلغاؤها[1].
3. كما أن الأدلة الإلكترونية تتميز بقابليتها للنسخ؛ بحيث يمكن استخراج نسخ طبق الأصل ولها نفس القيمة العملية، وهذه الخاصية لا تتوافر في الأدلة التقليدية, مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد التلف أو التغيير، وقد عمل المشرع البلجيكي على تعديل قانون التحقيق الجنائي بمقتضى قانون 2000 من خلال المادة 39 التي سمحت بضبط الأدلة بقصد عرضها على الجهات القضائية[2].

ثالثاً: مصادر الدليل الإلكترونــي.

ويقصد بها المنبع الذي قد تنتج الأدلة الإلكترونية في مجال البحث والتحقيق، والتي قد تكون على مستويين: الأول يتعلق بأنظمة الحاسوب وملحقاتها والثاني على مستوى أنظمة شبكة الاتصال بشبكة الانترنت.

وبهذا تعد الحواسيب مصدراً رئيسياً للأدلة الإلكترونية، وخاصة الحواسيب الشخصية التي تمثل أرشفة لسلوكيات الأفراد نظراً لاحتوائها على الكثير من المعلومات المتعلقة بنشاطاتهم وشخصيتهم، فالنشاط الاعتيادي للأفراد يتم استخراجه بعد تحليل العمليات القائمة على مستوى ملفات النظام وغيرها من الملفات المخزنة عادة في الأقراص الصلبة، والتي تحتوي على معلومات تتعلق بالجريمة وتفيد في عملية التحقيق.[3]

وتعتبر عملية حجز الحاسوب وتفتيشه أول مرحلة للبحث والتحقيق لكشف حقيقة ارتكاب الجريمة الإلكترونية؛ لأنه يمثل وسيلة للنفاذ إلى هذه الشبكة أياً كان شكل الحاسوب، كما أن عملية فحص

1 أشرف قنديل، المرجع السابق، ص 170.

2 **نقلاً عــن:** محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2004، ص 237.

3 فايز محمد راجح غلاب، المرجع السابق، ص 377.

البرمجيات المخزنة يجب أن تطبق بعناية وشكل سليم ومنتظم؛ لأن ذلك يمكن أن ينال من صحة الدليل الإلكتروني المستخلص من عرضه على القضاء[1].

كما يمكن أن تشمل عملية فحص أنظمة الاتصال بالانترنت من عمليات التحميل والتنزيل والنظام الأمني المحاط بالانترنت التي قد ينتج عنها الحصول على دليل إلكتروني يفيد في كشف الحقيقة، ومن بين أهم المسائل المثارة في عملية الإتصال بالإنترنت هي مسألة تحديد مكان الجريمة أو الحاسوب الذي ارتكب بواسطته النشاط الإجرامي, حيث يتم كشفه غالباً بتتبع الحركة العكسية للانترنت.

الفرع الثاني: الإجراءات المستحدثة للحصول على الدليل الإلكترونـــي.

لقد اتضح من خلال دراسة إجراءات التحقيق التقليدية كآليات متبعة للحصول على الأدلة الجنائية لكشف طرق ارتكاب الجرائم الإلكترونية مدى الصعوبات المحيطة بهذه الإجراءات، وهذا ما يسهل للكثير من الجناة الإفلات من العقاب، لذا كان من الضروري أن تواكب التشريعات المقارنة هذا التطور من خلال استحداث إجراءات غير تقليدية معتمدة على التقنية التكنولوجية في تحصيل الدليل الإلكتروني، وبهذا تتجاوز القصور الذي يمس الإجراءات التقليدية، وإعطاء فعالية أكبر من خلال إجراءات حديثة مستقلة قائمة بذاتها. وعلى اعتبار أن مجال البحث عن الأدلة الإلكترونية يتم من خلال التحقيق الجاري على البيانات الإلكترونية داخل النظام المعلوماتي للحاسوب أو أنظمة شبكة الانترنت، والتي تنقسم بدورها إلى نوعين إما بيانات متحركة وأخرى ساكنة[2].

البند الأول: الإجراءات المتعلقة بالبيانات الساكـــنة .

اهتمت اتفاقية بودابست بتحديد الإجراءات المتعلقة بالبيانات الساكنة, والتي قسمتها إلى نوعين؛ الأول يتعلق بالتحفظ المعجل على البيانات المخزنة، والأمر بتقديم بيانات معلوماتية متعلقة بالمشترك ثانياً.

أولًا: التحفظ المعجل على البيانات المخزنـــــة.

نصت اتفاقية بودابست في المادة 16 منها على ضرورة أن يقوم كل طرف بالسماح لسلطاته المختصة أن تأمر أو تفرض على مزود خدمة الانترنت التحفظ المعجل على البيانات المعلوماتية المخزنة, بما في ذلك البيانات المتعلقة بالمرور بواسطة نظام معلوماتي.

1 عمر بن يونس، المرجع السابق، ص 1008.

2 عبد النصر محمود فرغلي, وعبيد سعيد المسماري، المرجع السابق، ص 20.

ويعد إجراء حفظ البيانات من بين الأدوات المستحدثة والمساعدة في مجال التحقيق في الجرائم الواقعة عبر المعاملات الإلكترونية، نظراً لأنه يتلاءم مع طبيعة هذه البيئة، وبهذا يجدر بيان إجراء التحفظ، وقبل ذلك توضيح دور مزودي الخدمات باعتباره الحائز لهذه البيانات في مسألة التعاون مع سلطات التحري والتحقيق[1].

1. المقصود بدور مزودي الخدمات الإلكترونية في مرحلة التحقيق:

تقوم عملية تزويد الخدمة بناءً على الإشراف على الرسائل المتبادلة إلكترونياً بين الأشخاص، فيأخذ المزود دور الوسيط قبل أن تصل الرسالة إلى المرسل إليه وتظل مخزنة لدى المزود، وهنا يكون أمام خيارين؛ إما مسح الرسالة, وإما أن يقوم بتخزينها[2].

وفي هذا الصدد تلزم بعض التشريعات المقارنة كالقانون الفرنسي مزود الخدمات بإزالة البيانات التي يتم تخزينها تلقائياً وتتعلق بالاتصالات الإلكترونية بين مستعملي شبكة الانترنت, والخاصة بهوية المتصلين وميعاد الإتصال, بالرغم من وجود بعض الإستثناءات على هذا الالتزام:

- **الأول:** يتعلق بمتطلبات المحاسبة المالية بين مزودي الخدمات والمشتركين في خدماتهم، حيث يقوم مزودوا الخدمات لبعض هؤلاء المشتركين بعض الخدمات المدفوعة الأجر.
- **والثاني:** يتعلق بمسألة التعاون القضائي؛ بحيث تلزم الجهات القضائية الاحتفاظ بتلك البيانات لمدة لا تزيد عن سنة (1) واحدة، جدير بالذكر أن القانون الفرنسي لم يفرض الإلتزام المتعلق بتقديم المعلومات إلى الجهات القضائية بشكل مطلق، وأدرج عليه استثناءات منها ما يتعلق بسر المهنة, وهو ما جاءت به المادة 18 من قانون الأمن الداخلي الذي عدل قانون الإجراءات الفرنسي بموجب المادة (60-1) منه.

2. مفهوم التحفظ المعجل على البيانات المخزنـــة:

يقع على مزود الخدمة التزام بالاحتفاظ بالبيانات المخزنة عند مرورها في حالة الاتصالات الإلكترونية كما وضحنا سابقاً، إلا أن هذا الخيار قد يصبح التزاماً واقعاً على عاتق المزود في حالة ما تم توجيه السلطة المختصة لمزود الخدمة الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته, أو تحت سيطرته, في انتظار اتخاذ الإجراءات الخاصة بالتحقيق كالتفتيش أو الخبرة.

1 عبد الله حسين علي محمود، المرجع السابق، ص 398.

2 أشرف قنديل، المرجع السابق، ص 156.

وقد جاءت المادة 155 من اتفاقية بودابست بالأسباب التي تدعو لاتخاذ مثل هذا القرار، فنظراً لطبيعة البيانات الإلكترونية ومدى قابليتها للمحو أو الإخفاء أو التغيير من قبل الجاني بهدف طمس أدلة ارتكاب الجريمة، فيأتي إجراء التحفظ كوسيلة متاحة للحفاظ على الدليل الإلكتروني من الضياع، حيث أن إصدار الأمر بالتحفظ يكون مستعجلاً وملزماً لمزود الخدمة, وهذا لتفادي قطع السبل أمام الجهات القضائية في إيجاد دليل تتوصل من خلاله لكشف الحقيقة، وعلاوة على ذلك فإن أسلوب حفظ البيانات يأخذ شكلاً وقائياً نظراً لأن غالبية الجرائم الإلكترونية تتم عن طريق الاتصالات الإلكترونية المقامة عبر شبكة الانترنت[1].

وللإشارة كذلك فإن البيانات المعلوماتية المشمولة بإجراء التحفظ تضمن بيانات المرور المتعلقة باتصالات سابقة، وذلك من أجل تحديد خط سير الإتصال، وهذا ما يسهل مهمة معرفة هوية الأشخاص المرتكبين للجريمة، ولقد كان المشرع الجزائري واضحاً في النص على هذا الالتزام في نص المادة 11 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتي أجبر فيها مزود الخدمة بحفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،
- الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصالات الإلكترونية، وكذا المعطيات التي تسمح بالتعرف على المرسل إليه الاتصال, وكذا عناوين المواقع المطلع عليها.

ثانــياً: الأمر بتقديم بيانات معلوماتية عن المشترك.

لقد أجازت بعض التشريعات لجهات الضبط القضائي بتوجيه أمر لمزودي الخدمة بتسليم ما تحت أيديهم من موضوعات, والتي تطالب تقديمها كدليل, ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزود الخدمة، وهو ما نص عليه القانون الفرنسي رقم 719 لسنة 2000 المعدل لقانون رقم 86/1067 الخاص

1 المادة 155 من اتفاقية بودابست: "عندما تحتوي هذه الاتصالات على محتوى غير قانوني أو دليل على نشاط إجرامي، يحتفظ مقدمي الخدمات بنسخ من هذه الرسائل مثل البريد الإلكتروني، ويعتبر حفظ هذه الاتصالات مهماً من أجل ضمان عدم إتلاف أدلة بالغة الأهمية، ولعل الحصول على نسخ من هذه من هذه الاتصالات السابقة مثل البريد الإلكتروني المخزن الذي تم إرساله من شأنه أن يكشف عن أدلة عن الإجرام".

بحرية الإتصالات[1]، وكذا القانون الأمريكي المتعلق بخصوصية الإتصالات الإلكترونية، فقد أجاز لرجال الضبط القضائي في إطار مهمة التحري والتحقيق الاطلاع على البيانات الموجودة في حوزة مزود الخدمة الخاص بمستخدمي شبكة الانترنت، وهذه المعلومات تشمل البيانات الشخصية الخاصة بالمشترك كالاسم ورقم الهاتف أو المعلومات الشخصية الخاصة بالمتعامل مع المشترك؛ وهو كل من يدخل مع هذا الأخير في أي تعاملات أو صفقات إلكترونية, أو المعلومات المتعلقة بمحتوى البيانات, والمتمثلة في مضمون المحادثات الإلكترونية.

وقد نصت اتفاقية بودابست على هذا الإجراء في نص المادة 18 والتي جاء فيها أنه: "يجوز للدول الأطراف في تلك الاتفاقية تمكين السلطات المختصة بإصدار أمر تقديم البيانات، حيث يسمح لرجال السلطة العامة بإصدار هذا الأمر إذا تعلق الأمر ببيانات المشترك المعلنة للجمهور"، في حين أن بعض الدول تشترط أن يكون هذا الأمر صادراً فقط من السلطات القضائية عند الحاجة للحصول على نوع معين من البيانات المتعلقة بحق الخصوصية؛ مثل رقم بطاقة الائتمان أو حساب بنكي[2].

البند الثاني: الإجراءات المتعلقة بالبيانات المتحركة (اعتراض الاتصالات الإلكترونية).

لقد عملت التشريعات المقارنة على اعتبار أن البيانات المتحركة هي تلك البيانات التي لا يطبق عليها إجراء التفتيش أو التحفظ العاجل، وإنما يستوجب التعامل معها بأسلوب آخر يتماشى وعملية مجرى الاتصالات الإلكترونية لاستنباط الدليل الإلكتروني بشأنها، وهو ما يعرف باعتراض الاتصالات الإلكترونية, بحيث عرفه القانون الأمريكي في المادة الرابعة (04) من قانون خصوصية الاتصالات الإلكترونية بأنه: "اكتساب سماعي أو غيره لمحتوى أي اتصالات سلكية أو إلكترونية أو شفوية وذلك من خلال استعمال أي جهاز, سواء كان هذا الجهاز آلياً أو إلكترونياً أو غير ذلك. وقد قضي بأن معنى الاكتساب هو أن يتم الإلتقاط أثناء الاتصال نفسه, ويترتب على ذلك أن مراقبة الاتصالات المخزنة لا يعتبر اعتراضاً لها، وقد قرر القضاء الأمريكي بذلك بحيث اعتبر أن الدخول إلى الاتصالات الخاصة بالبريد الإلكتروني المخزنة لا يعد اعتراضاً لها[3].

1 Loi n° 2000-719 du 1er Août 2000 Modifiant la Loi n° 86-1067 du 3o Septembre 1986 Relative à la Liberté de Communication.

2 عمر بن يونس، المرجع السابق، ص 998.

3 ياسر الأمير فاروق محمد، مراقبة الأحاديث الخاصة في الإجراءات الجنائية (دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة ص 2008، ص 11.

ويجوز اعتراض الاتصالات الإلكترونية أثناء حدوثها على غرار ما يحدث في الاتصالات الهاتفية بناءً على أمر بذلك، ويتضمن ذلك إجراء تسجيل لتلك الاتصالات إذ تنص المادة 20 من القسم الخامس من اتفاقية الأوروبية لجرائم الانترنت على أنه من حق الدولة الطرف أن تقوم باعتراض وتسجيل الاتصالات الإلكترونية المتداولة في الوقت الحقيقي؛ أي خلال الوقت الذي يتم تداولها فيه[1].

وتميز اتفاقية بودابست بين نوعين من البيانات المعلوماتية محل الاعتراض؛ وهي البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال، فبالنسبة للنوع الأول فإن الإتفاقية قد عرفتها بأنها:" كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي يتم انتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصراً في سلسلة الاتصال"[2].

أما بالنسبة للنوع الثاني الخاص بالبيانات المتعلقة بمحتوى الاتصال فإنه لم يأتِ تعريف لها في الاتفاقية، لكنها تشير إلى المحتوى الإخباري للاتصال؛ بمعنى مضمون الاتصال أو الرسالة أو المعلومات المتنقلة عن طريق الاتصال، ويلاحظ أن هناك نوعاً من التقارب بين هذين النوعين من البيانات من حيث المعنى, إلا أنهما مختلفان من حيث درجة المساس بحق الخصوصية، حيث يكون ذلك أهم بالنسبة لمراقبة محتوى الاتصال[3].

أولاً: نطاق الأخذ بأسلوب اعتراض الاتصالات الإلكترونية.

تسعى التشريعات الجزائية من خلال وضع الأحكام الخاصة بالجرائم إلى إيجاد توازن بين حقوق الإنسان ومصلحة المجتمع في كشف الحقيقة بشأن الجريمة ومعاقبة الجناة، وبهذا فإن حق الخصوصية ليس حق مطلق بل مقيد بالمصلحة العامة. وتطبيقاً لذلك فإن اعتراض الأحاديث والاتصالات الإلكترونية قد تمس بحق الإنسان في الخصوصية وما يتفرع عنه من سرية الأحاديث الخاصة, وهذا الحق أصبح مهدداً بدرجة كبيرة نتيجة للتطور التكنولوجي الذي أدى إلى إفراز أجهزة للمراقبة وتسجيل الاتصالات دون علم الأفراد بها.

1 Article 20 du Convention sur la Cybercriminalité Budabest 2001:" ….pour assure la collecte ou l'enregistrement en temps réel des données au trafic associées à des communication spécifique transmises sur son territoire par l'application de moyens techniques existant sur ce territoire."

2 المادة الأولى من اتفاقية بودبست لمكافحة الإجرام المعلوماتي.

3 أشرف عبد القادر قنديل، المرجع السابق، ص 184.

وبهذا حرصت العديد من التشريعات العقابية على توفير قدر كبير من الأحكام الخاصة بحماية سرية الاتصالات الخاصة للأفراد، ولقد نص المشرع الجزائري على حظر اعتراض الاتصالات السلكية واللاسلكية دون إذن بذلك بموجب القانون رقم 06-23 المعدل لقانون العقوبات الجزائري, وتحديداً في نص المادة 303 مكرر من قانون العقوبات, والتي جاء فيها:"يعاقب بالحبس من ستة (6) أشهر إلى ثلاثة (03) سنوات وبغرامة من خمسين ألف دينار (50.000) دج إلى ثلاثمائة ألف دينار (300.000) دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أور ضاه.

2- بالتقاط أو بتسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه".

أما بالنسبة للمشرع المصري فقد عاقب بالحبس مدة لا تقل سنة كل من اعتدى على حرمة الاتصالات الخاصة من خلال أي فعل يمثل استراق للسمع أو تسجيل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه.

وفي نفس الإطار عملت العديد من التشريعات على إدخال نصوص خاصة تسري على الاتصالات الإلكترونية, ومنها ما تضمنه القانون الأمريكي الذي ينص على عقاب كل من قام باعتراض المراسلات الإلكترونية[1].

ثانياً: أسلوب الاعتراض المشروع للاتصالات الإلكترونيــة.

إذا كان الأصل في حماية الحق في سرية الاتصالات الإلكترونية هو الحفاظ على سريتها وعدم التعرض لخصوصيتها بشكل مطلق، فإن الضرورة التشريعية تستلزم تطبيق الاستثناء الخاص بمشروعية أسلوب الاعتراض للاتصالات الإلكترونية في الحالة التي تواجه فيها خطر الجريمة المرتكبة عبر المعاملات الإلكترونية أو عبر شبكة الانترنت، فكان لزاماً تنظيم هذا الأسلوب كأداة لإثبات تلك الجرائم, أو استخراج الأدلة الإلكترونية المساعدة على كشف الحقيقة.

ولقد مكنت أغلب التشريعات الجزائية الجهات المختصة بالتحري والتحقيق في اعتماد أسلوب اعتراض المحادثات الإلكترونية والتقاط الصور للكشف عن الأدلة وإثبات الجرائم الواقعة عبر التعامل الإلكتروني، وهذا على الرغم من تناقضها مع النصوص المقررة لحماية حق الخصوصية.

1 **نقلاً عـــن**: شيماء عبد الغني، المرجع السابق، ص 218.

ويعد هذا الإجراء الحديث من أهم وسائل تحصيل الدليل الجنائي في الجرائم الإلكترونية، وقد عملت أغلب التشريعات بتطبيقه في حالة جرائم محددة, سواء كانت جنايات أو جنح التي وقعت أو قد تقع في المستقبل يستنبط من خلال أدلة تكشف ضلوع المتهم في ارتكاب الجريمة من خلال تحليل الاتصالات الإلكترونية الصادرة منه أو الواردة إليه, وهو مايفيد في أغلب الأحيان إلى كشف معالم ارتكاب الجريمة.

1- مفهوم إجراء اعتراض المراسلات الإلكترونيـــة:

لقد أورد تقرير صادر عن لجنة الخبراء بالبرلمان الأوروبي "بستراسبورغ" المؤرخ في 2006/20/06 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية تعريفاً لإجراء اعتراض المراسلات بأنها:"عملية مراقبة سرية للمراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم"[1].

ولقد قرر المشرع الجزائري هذا الإجراء من خلال نص المادة 65 مكرر من قانون الإجراءات الجزائية، والذي عرفه بأنه اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للانتاج والتخزين والاستقبال والعرض، ونجد المشرع الفرنسي يكرس هذا الإجراء من خلال نص المادة 100 من قانون الإجراءات الجزائية التي تنص على إمكانية تقرير القاضي لاعتراض وتسجيل ونقل المراسلات التي تتم عن طريق وسائل الاتصال في المواد الجنائية والمواد الجنحية إذا كانت العقوبة تفوق سنتين، وإذا استدعت مقتضيات البحث والتحري ذلك.

ولقد حدد المشرع الجزائري تعريفاً للمراسلات محل الاعتراض من خلال القانون 2000-03 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات, والذي عرفها بأنها:"كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف الراسل نفسه أو بطلب منه"، ويلاحظ من هذا النص عمومية مفهوم المراسلات دون إشارة مباشرة لطبيعة المراسلات محل الاعتراض[2].

إلا أنه بالرجوع إلى نص المادة 303 من قانون العقوبات التي تعاقب كل إتلاف لمراسلات موجهة للغير بأي شكل من الأشكال، فالملاحظ أن المراسلات الخاصة قد تأخذ سواء الشكل المادي المكتوب أو الإلكتروني، وسواء على دعامة ورقية أو إلكترونية، مرسلة لعدد معين ومحدد من المرسل إليهم. وهو ذات

---

1 **مشار إليه لدى:** لوجاني نور الدين، أساليب البحث والتحري الخاصة وإجراءاتها وفقاً للقانون 06-22، مداخلة مقدمة في اليوم الدراسي حول علاقة النيابة العامة بالشرطة القضائية احترام حقوق الانسان ومكافحة الجريمة، وزار الداخلية- المديرية العامة للأمن الوطني منعقد يوم 2007/12/12، بإليزي، ص 08.

2 المادة 6/9 من القانون 2000-03 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات.

الموقف الذي وضحه المشرع من خلال القانون 09-04 بتعريفه للاتصالات الإلكترونية على أنها:"تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[1].

2- شروط تنفيذ أسلوب الاعتراض المشروع للاتصالات الإلكترونيـــة:

أباح المشرع الجنائي اتخاذ هذا الإجراء مقابل وضع ضمانات قانونية لتنفيذه, وهذا دائماً في سبيل التوفيق في التعارض بين حق المصلحة العامة في الكشف عن الجريمة, والحق في احترام حق خصوصية الأفراد. وتتمثل تلك الضمانات في ضرورة إصدار إذن من السلطة المختصة؛ حيث توكل أغلب التشريعات الجنائية مهمة إصدار الإذن الخاص باعتراض وتسجيل الاتصالات الإلكترونية إلى السلطة القضائية المختصة، ويعد ذلك ضمانة لازمة لمشروعية هذا الإجراء، ولم يشترط التشريع المصري أو الفرنسي أن يقوم قاضي التحقيق أو النيابة العامة في حالة صدور إذن من القاضي الجنائي بتنفيذ أمر الاعتراض, بل يمكن أن تعهد بذلك إلى جهات الضبط القضائي، بالرغم من أن المشرع الجزائري خالف ذلك وأجاز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات والاتصالات التي تم عن طريق وسائل الاتصال السلكية واللاسلكية, وتباشر هذه العملية تحت رقابته[2].

ويجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على مضمون الاتصالات الإلكترونية, كما أنه يجب أن يصدر بناءً على ما ينكشف للقاضي من خلال أعمال الاستدلال التي قامت بها جهات الضبط القضائي, ليتبين له من خلالها ضرورة إصدار الإذن بالموافقة لما في ذلك من أهمية في ظهور الحقيقة في الجرائم الإلكترونية[3].

ولقد عمل المشرع الجزائري على تحديد نوع من الجرائم التي يجوز فيها اعتراض المراسلات التي تتم عن طريق وسائل الاتصالات الإلكترونية؛ ومنها جرائم المساس بأنظمة الحاسب الآلي للمعطيات، وذلك إدراكاً منه على عدم كفاية الوسائل التقليدية لجمع الدليل الإلكتروني؛ نظراً لما تتمتع به هذه الجريمة المستحدثة من خصوصية.

كما حرصت معظم التشريعات الجنائية على تحديد مدة معينة للاعتراض منعاً للتعسف وإساءة استعمال السلطة، غير أن هذه التشريعات لم تسر على وتيرة واحدة في شأن هذا الإجراء؛ فمنها من حدد

1 المادة 02 الفقرة 6 من القانون 09-04 المتعلق بمكافحة جرائم الاتصال وتكنولوجيا المعلومات.

2 المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري.

3 نبيلة هروال، المرجع السابق، ص 156.

المدة بأمد قصير كالمشرع المصري؛ حيث حددها بثلاثين يوماً قابلة للتجديد طبقاً لنص المادة 206/95 من قانون الإجراءات الجزائية المصري.

كما تترتب فائدة الإجراء في ظل احترام سائر الضوابط المقدمة في القانون الجنائي, والتي تتعلق بإمكانية الاعتداء بالأدلة الإلكترونية سواء كان بريد إلكتروني, أو المحادثات الفورية الناجمة عن إثبات الجريمة ونسبتها إلى المتهم، بينما يترتب عن عدم مشروعية الإجراء أثراً عكسياً يتمثل في استبعاد الأدلة الناجمة عنها وعدم جواز قبولها في إثبات إدانة المتهم، فضلاً عن تحقق المسؤولية الجنائية عن جريمة الاعتراض غير المشروع, وهو ما سبق بيانه في نطاق ممارسة أسلوب اعتراض وتسجيل الإتصالات الإلكترونية[1].

1 ياسر الأمير فاروق محمد، المرجع السابق، ص 226.

الفـصل الثانـــــي:
الحماية الجزائية للمعاملات الإلكترونية في مرحلة المحاكمـــــــــة

الفصل الثاني:

الحماية الجزائية للمعاملات الإلكترونية في مرحلة المحاكمة.

تكفل الأحكام العامة بالإضافة إلى النصوص الخاصة في التشريعات الإجرائية الحماية الجنائية للمعاملات الإلكترونية في مرحلة المحاكمة، بحيث يؤثر هذا النوع من المعاملات على تلك الأحكام العامة، بل وأصبح له مبرراً لإدخال نصوص خاصة لتنظيم الدعوى الجنائية في مرحلة المحاكمة؛ سواء من حيث تحديد المحكمة المختصة بنظر الجرائم الواقعة على المعاملات الإلكترونية، ومحاولة تطويع المبادئ العامة في مجال تنازع الاختصاص القضائي لبسط حماية فعالة لتلك المعاملات، وكذا محاولة تبني حلول خاصة تساعد بشكل مباشر لحل هذا التنازع (المبحث الأول).

وسواء من ناحية سلطة المحكمة في تقدير الدليل الجنائي في مجال المعاملات الإلكترونية، بحيث أن عملية تقدير الأدلة جوهر الحكم، وليس باستطاعة القاضي إدراكه والوصول إليه إلا بعد ممارسة السلطة التقديرية للأدلة محل الوقائع، فتتوقف سلامة الحكم على صحة تقدير الأدلة الإلكترونية، وهو ما يضع على القاضي الجنائي مسؤولية كبرى في انتقاء الآليات والأسس التي تبنى عليها مسألة تقدير الدليل الجنائي الإلكتروني (المبحث الثاني).

المبحث الأول:

قواعد الاختصاص القضائي في الجرائم الواقعة على المعاملات الإلكترونية.

يحدد مفهوم الاختصاص القضائي بأنه السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها داخل إقليمها، وتعد الجرائم الواقعة عبر التعامل الإلكتروني ذات خصوصية فيما يتعلق بتحديد قواعد الاختصاص القضائي المطبقة بشأنها، ذلك أن السلوك أو النشاط الإجرامي لها لا يعترف بالحدود، فالعالم قد تحول إلى أشبه بقرية صغيرة، وقيام الفعل الإجرامي الإلكتروني تخطى كل الحدود الجغرافية والسياسية للدول لهدمه كل معاني المكانية للجريمة، وأضحت التقنية المعلوماتية المرتبطة بشبكة المعلومات تشكل مسار قيام الجريمة بشكل محدد وقطعي, وأدت إلى إمكانية تعدد المسارح الدولية للجريمة، الأمر الذي قد ينجم عنه تنازع الإختصاص القضائي بين هذه الدول، فقد يحدث أن ترتكب الجريمة المعلوماتية في إقليم دولة معينة, وتتحقق آثارها الجرمية في دولة أخرى، وقد تمر عبر دول أخرى وسيطة بين مكان وقوع الفعل وتحقق النتيجة, ومن ثم يمكن أن تتعدد القوانين التي يمكن أن تحكم هذه الجريمة بتعدد الدول المرتبطة بها[1].

ولذلك فإن الإشكالية بشأن تنازع الاختصاص القضائي للدول تبنى على الاختلاف التشريعي والتباين في النظم العقابية الدولية وأحكامها، ومن هنا تأتي الضرورة لإبراز الحلول المتعلقة بمسألة تحديد القانون الواجب التطبيق الذي يترتب عنه تحديد الولاية القضائية للمحكمة المختصة، وهذا يرجع إلى تبيان المبادئ أو المعايير المعتمدة في تحديد القانون الواجب التطبيق على الجرائم المرتكبة التي تُوصِلُنا إلى تحديد الاختصاص القضائي. وهو ما يطرح إشكالية التساؤل عن القواعد الخاصة بتحديد الاختصاص القضائي للجرائم الواقعة على المعاملات الإلكترونية ؟ وفيما يبرز أثر ذاتية أو خصوصية هذه الجرائم في تحديد الاختصاص القضائي ؟

1 فايز محمد راجح غلاب، المرجع السابق، 375.

المطلب الأول: الأحكام المتعلقة بتحديد القانون الواجب التطبيق على جرائم المعاملات الإلكترونية

إن المبدأ السائد في معظم دول العالم هو مبدأ إقليمية القانون الجنائي, إلا أن هناك استثناءات ترد على هذا المبدأ مردها الحرص على عدم إفلات الجاني من العقاب، خاصة بعد ظهور نوع جديد من الإجرام المستحدث وأخذه لأشكال متعددة، وكثرة العصابات الإجرامية التي يمتد نشاطها في هذا المجال ليشمل عدداً كبيراً من الدول، ومنه اتخذت الجريمة الطابع العالمي ولذلك استوجب وجود نظام يسمح بالعقاب على هذه الجرائم.

فالأخذ بمبدأ واحد لا يعد كافياً لتحقيق الحماية الجنائية داخل وخارج الدولة، وبهذا وجدت مبادئ أخرى أخذت بها التشريعات المقارنة كحلول مساندة ومكملة لمبدأ الإقليمية، بحيث تمكن الدول من تطبيق قوانينها وتوقيع العقاب على الجناة في أي مكان، وكذا الحد من النيل من مصالحها وسيادتها بمتابعة الجاني تحت أي ظرف كان. وهو الأمر الذي يدفعنا إلى دراسة هذه المبادئ المتعلقة بتحديد القانون الواجب التطبيق على الجرائم الإلكترونية, بدءاً بالموقف التشريعي من المبادئ المتعلقة بحل تنازع الاختصاص القضائي في جرائم المعاملات الإلكترونية (الفرع الأول), ثم الموقف الدولي من مسألة الاختصاص القضائي في جرائم المعاملات الإلكترونية (الفرع الثاني), وصولاً لتقييم المبادئ التقليدية لحل تنازع الاختصاص القضائي في الجرائم الإلكترونية (الفرع الثالث).

الفرع الأول: الموقف التشريعي من المبادئ المتعلقة بحل تنازع الاختصاص القضائي في جرائم المعاملات الإلكترونية.

اتجهت أغلب التشريعية الإجرائية المقارنة إلى حل مشكلة تنازع الاختصاص القضائي في مجال الجرائم الواقعة عبر التعامل الإلكتروني بإسقاط الأحكام العامة المتعلقة بتبني المبادئ المقررة لحل تنازع الاختصاص في الجرائم التقليدية، ومن نتائج هذا الإسقاط ظهور عدة نقائص في تبني هذه المبادئ، وقصورها عن حل الإشكال بشكل جذري؛ نظراً لخصوصية الجريمة وكيفية ارتكابها, الأمر الذي استوجب البحث عن بدائل وحلول أخرى تكون أكثر فعالية .

البند الأول: الموقف التشريعي من مبدأ إقليمية النص الجنائي.

تأخذ أغلب التشريعات المقارنة بمبدأ إقليمية النص الجنائي؛ والذي يقصد به خضوع كل الجرائم التي ترتكب على إقليم دولة معينة لقانونها الجنائي الوطني بغض النظر عن جنسية مرتكبيها، بحيث يرجع

الاختصاص القضائي في الفصل في تلك الجرائم إلى محاكمها الوطنية، ولا تخضع لسلطات أي قانون أجنبي، وفي المقابل لا مجال لامتداد سريان القانون الجنائي للدولة خارج نطاق إقليمها وفقاً للحدود المعترف بها، حيث يصطدم بسيادة الدول الأجنبية, إلا في أحوال استثنائية تقتضيها حماية المصالح الجوهرية للدولة, أو متطلبات التعاون الدولي في مكافحة الإجرام[1].

وقد حظي هذا المبدأ بتأييد جانب كبير من الفقه والتشريعات؛ ومنها المشرع الجزائري الذي تبنى مبدأ الإقليمية في نص المادة الثالثة (03) من قانون العقوبات التي نصت على أن:"يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية،كما أخذ بهذا المبدأ المشرع الفرنسي في المادة 2/113 من قانون العقوبات الجديد التي تنص:"يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية".

أما المشرع المصري فلقد تبنى هذا المبدأ في نص المادة الأولى من قانون العقوبات التي تنص على أن:"تسري أحكام هذا القانون على كل من يرتكب في الإقليم المصري جريمة من الجرائم المنصوص عليها فيه".

كما أن الأصل في تحقق الركن المادي للجريمة يكتمل في نطاق إقليم الدولة الواحدة، بحيث يقع النشاط الإجرامي وتترتب آثاره في نفس الإقليم، إلا أن بعض الجرائم قد تأخذ مدىً أوسع من إقليم الدولة الواحدة، بحيث يتجاوز آثارها إلى دول أخرى، وهنا يتجزأ الركن المادي للجريمة ويتوزع على أكثر من إقليم, وهو ما يميز الجرائم العابرة للحدود بالأخص[2].

وهنا يثار التساؤل بشأن مبدأ الإقليمية في هذه الحالة، فهل يعتد بمكان وقوع الجريمة أو الإقليم الذي تترتب فيه آثارها ؟

بالرجوع إلى آلية تطبيق مبدأ الإقليمية على الجرائم الواقعة عبر التعامل الإلكتروني، نجد أن هذه الجرائم تشكل وضعاً خاصاً، وهذا يتجلى بالتحديد في الحالات التي تعتمد بها بعض التشريعات المقارنة انعقاد الاختصاص القضائي لها بمجرد توافر ارتكاب جزء من السلوك الإجرامي على إقليمها وليس كله, وهو نفس موقف المشرع الفرنسي في نص المادة 2/113 التي جاء فيها:"تعتبر الجريمة قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع في هذا الإقليم".

1 عدنان الخطيب، موجز القانون الجزائي (الكتاب الأول)، مطبعة جامعة دمشق، 1963، ص 79.

2 عدنان الخطيب، المرجع السابق، ص 81.

وأما المشرع الجزائري فلقد تناول نفس الحكم في نص المادة 586 من قانون الإجراءات الجزائية الذي ورد فيه أنه: "تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها قد تم في الجزائر".

كما جاء نص المشرع المصري على اعتبار كل من ارتكب في خارج القطر فعلاً يجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها في القطر المصري، وهو نفس موقف المشرع الفرنسي وكذا المشرع الجزائري الذي تبناه في نص المادة 585 من قانون الإجراءات الجزائية, بحيث نص على متابعة كل من كان في إقليم الجمهورية شريكاً في جناية أو جنحة مرتكبة في الخارج، ويحكم عليه بمعرفة جهات القضاء الجزائرية، ويشترط أن تكون الواقعة معاقباً عليها في كلا القانونين الأجنبي والجزائري، وأن تكون تلك الواقعة الموصوفة بأنها جنحة أو جناية قد ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية[1].

وهنا يلاحظ أن التشريعات المقارنة قد عملت على توسيع الأخذ بمبدأ الإقليمية بشكل يضمن معه ملاحقة الجاني والحرص على تطبيق النص الجنائي الوطني في أوسع حالاته، وهو ما يبين فاعلية هذا الحكم بخصوص الجرائم المرتكبة إلكترونياً وعبر شبكة الانترنت, بحيث يلحق تطبيق النص الجنائي الوطني على الشريك في الجريمة المرتكبة كلها أو جزء منها داخل إقليم الدولة الواحدة.

ويلاحظ مما تقدم أن هذا المبدأ يسمح بمتابعة كل من ارتكب أحد العناصر المكونة للركن المادي للجريمة، حتى لو تعلق الأمر بآثار السلوك الإجرامي داخل إقليم الدولة، ولو لم يكن الفعل غير معاقب عليه في بلد المنشأ الأصلي؛ أي بداية السلوك الإجرامي، ومن ثم فإن تنقل البيانات أو المعلومات إلكترونياً في النشاط الإجرامي بين العديد من الدول وبمجرد تحقق جزء من هذا السلوك داخل القطر الوطني، فهنا يقام الإختصاص القضائي الجزائي للمحاكم الوطنية، فلقد اعترفت أحكام القضاء الفرنسي بمبدأ موسع للقضاء الجزائي الوطني متبنية بذلك نظرية كلية الحضور كلما ارتبط الأمر بالإقليم الوطني, وبالقانون الجزائي في حالة أن جزء من الجريمة ارتكب في الإقليم الوطني[2].

غير أن هذا المبدأ قد يصطدم بصعوبات تتعلق بطريقة تطبيقه بالنسبة لهذه الجرائم, وهذا بالنظر لطبيعتها المميزة لها عن الجرائم التقليدية, وخاصة فيما يتعلق بصعوبة تحديد مكان وزمان ارتكابها بدقة. ومثالها ارتكاب أحد الجناة لجريمة الدخول غير المشروع في نظام آلي وتعديل المعطيات به بغرض الحصول

1 جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، سنة 2001، ص 73.

2 Myriam quéméner, yves CHARPENEL, cybercriminalité, droit pénal appliqué .ECONOMICA, Paris, 2010, p158.

على المال، بحيث قد يتواجد الشخص خارج الإقليم الوطني ويقوم عن طريق الإنترنت بالدخول إلى شبكة المعلومات الخاصة بأحد المصارف، ويخترق حساب أحد العملاء ويقوم بالتحويل منه إلى حسابه أو حساب شخص آخر في دولة أخرى، ففي هذه الحالة تكون الجريمة قد توزعت بين إقليم الدولة وأقاليم أخرى لتشعب السلوك الإجرامي المكون لها بين عدة أقاليم وفي عدة أزمنة[1].

وعليه نرى أن تطبيق مبدأ إقليمية النص الجنائي يصطدم بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل، وإن كان المبدأ يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها المادية، فهذا المبدأ يبدو غير ملائم للجريمة المعلوماتية التي تفتقد إلى الطبيعة المادية الثابتة.

البند الثانـــي: مبدأ شخصية النص الجنائي.

يقصد بمبدأ شخصية النص الجنائي هو سريان القانون الوطني الجنائي على الجرائم المرتكبة من أو ضد من يحملون جنسية الدولة، ولهذا المبدأ وجهان؛ وجه إيجابي يطبق فيه النص الجنائي على كل فرد يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها. أما الوجه السلبي فيعني أن يطبق النص الجنائي على كل جريمة يكون المجني عليه منتمياً إلى جنسية الدولة, ولو كان مرتكبها أجنبياً أو ارتكبت خارج إقليم الدولة[2].

ويهدف الوجه السلبي هنا إلى حماية رعايا الدولة إذا ما تعرضوا لاعتداء إجرامي خارج نطاق دولتهم، بينما يهدف الوجه الإيجابي لحماية سمعة الدولة بالخارج, وحتى لاتكون الدولة مرتعاً للمجرمين من مواطنيها إذا ما هربوا من العدالة في الدول التي ارتكبوا عليها الجرائم.

ولقد اعتد المشرع الجزائري على غرار باقي التشريعات بمبدأ شخصية النص الجنائي في شقه الإيجابي لا السلبي؛ وهو ما نص عليه قانون الإجراءات الجزائية الذي نص على أن كل واقعة موصوفة بأنها جناية معاقب عليها في القانون الجزائري, ارتكبها جزائري خارج إقليم الجمهورية يجوز أن يتابع ويحاكم في الجزائر[3]. ولم يأخذ بالشق السلبي للمبدأ نظراً لعدم اعترافه بأي اعتبار لشخصية المجني عليه في تطبيق القانون الجنائي من حيث المكان.

1 أحمد عبد الكريم سلامة، الانترنت والقانون الدولي الخاص، بحث مقدم إلى مؤتمر القانون والانترنت، جامعة الإمارات العربية المتحدة، 1-3 ماي، جزء 3، سنة 2004، ص 54.

2 زكي محمد أبو عامر، المرجع السابق، ص 223.

3 المادة 582 من قانون الإجراءات الجزائية الجزائري.

وهو نفس موقف المشرع المصري الذي نص وفقاً لحكم المادة 3 من قانون العقوبات المصري على أن: "كل مصري ارتكب وهو في خارج القطر فعلاً يعتبر جناية أو جنحة في هذا القانون يعاقب بمقتضى أحكامه وكان الفعل المعاقب عليه بمقتضى قانون البلد الذي ارتكب فيه".

أما المشرع الفرنسي فقد أخذ بمبدأ الشخصية بوجهيه الإيجابي والسلبي، فالوجه الإيجابي نصت عليه المادة 113-6 من قانون العقوبات الفرنسي الجديد بقولها: "يطبق القانون الفرنسي أيضاً على الجنح التي يرتكبها فرنسي خارج فرنسا إذا كانت الوقائع المكونة لها معاقب عليها في قانون الدولة التي تم ارتكابها فيها، وتطبق أحكام هذه المادة حتى لوكان المتهم قد اكتسب الجنسية الفرنسية بعد ارتكاب الواقعة المنسوبة إليه".

أما الوجه السلبي فقد نصت عليه المادة (113-7) لنصها على أن يطبق القانون الفرنسي على أي جناية أو جنحة يعاقب عليها بالحبس يرتكبها فرنسي أو أجنبي في الخارج إذا كان المجني عليه يكون فرنسياً لحظة ارتكاب الجريمة، فوفقاً لنص هذه المادة يكون معيار اختصاص القانون الفرنسي أن المجني عليه يكون فرنسياً، وهو بذلك يهدف إلى حماية رعاياه الفرنسيين الذين ترتكب ضدهم جرائم في الخارج، ويترتب على ذلك أن الجاني في الجريمة الواقعة عبر التعامل الإلكتروني على إقليم دولة أجنبية ضد المواطن الفرنسي يحاكم وفقاً للقانون الفرنسي, حتى لو كان هذا الفعل غير معاقب عليه في البلد الأجنبي, فتسمح قواعد الإختصاص وفقاً لنص المادة 113-7 بحماية المواطن الفرنسي المضرور من الخارج في الجريمة المعلوماتية[1].

وبهذا نجد أن القانون الفرنسي أكثر اتساعاً في تطبيق مبدأ الشخصية من القانون الجزائري والمصري فنأمل من هذين التشريعين الأخذ بمبدأ الشخصية بوجهيه الإيجابي والسلبي لتوفير حماية للرعايا خارج إقليم الدولة, وحتى يتسع نطاق تطبيق نصوص مواده على الجرائم التي يتم ارتكابها عبر الفضاء الإلكتروني.

وبالرغم مما ذكر, إلا أن هذا المبدأ لم يرد بشكل مطلق في التطبيق, وإنما أوردت عليه التشريعات المقارنة قيود معينة، بحيث أن الاختصاص لا ينعقد للمحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع خارج إقليم الدولة, وإنما يجب توافر شرطين مهمين؛ أولاً: عدم جواز تحريك الدعوى الجنائية إلا بمعرفة النيابة العامة, وعدم جواز محاكمة الشخص عن الفعل الواحد مرتين، وهو ما نصت عليه الفقرة الثانية (02) من المادة 582 والمادة 583 من القانون الجزائري الذي ربط مسألة تطبيق مبدأ شخصية النص الجنائي إلا

1 Ann BRISSET-GIUSTINIANI, Aspects juridiques de l'émergence d'une sécurité européenne des réseaux et des systémes d'information, Mémoire D.E.S.S Droit de l'internet administration-entreprises, université PANTHEON SORBON, Paris. 2004. P 222 Disponible sur: *www.univ-paris1 .fr*

بناء على طلب النيابة العامة بعد إخطارها بشكوى من الشخص المضرور، أو ببلاغ من سلطات القطر الذي ارتكبت فيه، ولم يثبت عليه حكم نهائي في الخارج, وأن يثبت في حالة حكم بالإدانة أنه قضى العقوبة أو سقطت عليه بالتقادم أو حصل على العفو عنها.

وهو ما نص عليه التشريع المصري من خلال نص المادة الرابعة (04) من قانون العقوبات المصري الذي نص على أن لا تقام الدعوى العمومية على مرتكب الجريمة أو في الخارج إلا من النيابة العامة، ولا يجوز إقامتها على من يثبت برائته مما أسند إليه, أو بالنسبة لمن حكمت عليه واستوفى عقوبته.

وأما المشرع الفرنسي فقد نص في المادة 8/113 على أنه: "في الجرائم المنصوص عليها في المادتين 6/113 و7/113 لا ترفع الدعوى الجنائية من المجني عليه أو من خلفه أو بناء على بلاغ رسمي من سلطات الدولة التي ارتكبت الجريمة على إقليمها".

كما ثبت وفقاً لنص المادة 9/113 من نفس القانون أنه في نفس الحالات السابقة لا تقام الدعوى الجنائية ضد شخص ثبت أنه حوكم نهائياً في الخارج عن نفس الوقائع, ويثبت في حالة الإدانة أنه نفذ العقوبة أو أنها سقطت بالتقادم.

البند الثالث: مبدأ الاختصاص العينـــي.

ويعني هذا المبدأ سريان القانون الوطني الجنائي على بعض الجرائم التي تمس المصالح الجوهرية للدولة والتي ترتكب خارج إقليمها الوطني، وطبقاً لهذا المبدأ يتمد التشريع الجنائي للدولة ليطبق على الجرائم التي ترتكب في الخارج بغض النظر عن جنسية مرتكبيها، ويستند هذا الامتداد لحق الدولة في الدفاع الذاتي ضد كافة صور الاعتداء على مصالحها الأمنية والمالية ولو وقع هذا الاعتداء خارج إقليمها[1].

وهو بذلك يكون مكملاً لمبدأ الإقليمية، لأنه يسمح بملاحقة الجرائم التي ترتكب خارج إقليم الدولة وتنال من مصلحتها الجوهرية، وبصفة خاصة في الأحوال التي قد لا تهتم الدولة التي وقعت فيها مثل هذه الجرائم بملاحقة الجناة لانعدام النص الجنائي المجرم لمثل تلك الأفعال على إقليمها.

ولقد أخذ المشرع الجزائري بهذا المبدأ في قانون الإجراءات الجزائية الذي نص على متابعة كل فاعل أصلي أو شريك في جناية أو جنحة ارتكبت خارج الإقليم الجزائري وتمس بسلامة الدولة الجزائرية ومصالحها الجوهرية، كما تتم محاكمته إذا حصلت الحكومة على تسليمه من دولة أخرى[2]. وبالرغم من ذلك, إلا أن

1 زكي محمد أبو عامر، المرجع السابق، ص 235.

2 المادة 588 من قانون الإجراءات الجزائية الجزائري.

المشرع قد عمل على استحداث حكم خاص بالجرائم المتعلقة بتكنولوجيا الإعلام والاتصال من خلال القانون 04/09 الواردة في الفصل السادس تحت عنوان التعاون والمساعدة القضائية والاختصاص القضائي، حيث أكد المشرع على مبدأ عينية النص الجنائي المنصوص عليه في قانون الإجراءات الجزائية, بحيث أولى الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال المرتكبة خارج الوطن، عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[1]، وهو موقف يحسب للمشرع الجزائري الذي صرح بتطبيق مبدأ الاختصاص العيني في الجرائم الواقعة عبر التعاملات الإلكترونية.

أما المشرع المصري فلقد أورد تطبيق مبدأ الاختصاص العيني الجنائي بالنسبة لجرائم معينة جاءت على سبيل الحصر في نص المادة 2/2 من قانون العقوبات, والتي رأى أنها تمس بمصالح الدولة الاستراتيجية الاقتصادية؛ كجريمة التزوير وجريمة تزييف أو تقليد عملة وطنية أو إدخالها أو إخراجها من التراب المصري أو حيازتها أو ترويجها أو بعض الجرائم الماسة بأمن الدولة واستقراره كجريمة التخابر, وجريمة تسليم أو إفشاء أسرار الدفاع عن البلاد، وبذلك يكون المشرع المصري قد أغفل النص على الجرائم المتعلقة بالمعاملات الإلكترونية أو الواقعة عبر شبكة الانترنت.

وقد أخذ أيضاً المشرع الفرنسي بمبدأ العينية من خلال نص المادة 10/113 من قانون العقوبات الجزائية بحيث يطبق القانون الفرنسي على الجنايات والجنح التي ترتكب في الخارج, والتي تشكل اعتداءً على المصالح الأساسية للأمة المنصوص عليها, أو أماكن البعثات الدبلوماسية أو القنصلية الفرنسية في الخارج.

الفرع الثاني: الموقف الدولي من مسألة الاختصاص القضائي في جرائم المعاملات الإلكترونية.

إذا كان الموقف الداخلي من مسألة الاختصاص في الجرائم الماسة بالتعامل الإلكتروني غير مجدي عند العديد من التشريعات المقارنة؛ لعدم استحداثها لنصوص خاصة بطبيعة هذا التعامل, أو حتى الإشارة إليها بشكل صريح، فإن عمل التشريعات الدولية جاء مخالف لذلك, بحيث عملت بعض الاتفاقيات على المستوى الدولي والإقليمي لمعالجة مسألة الاختصاص بنصوص صريحة في هذا الشأن, وسنعرضها فيما يلي:

البند الأول: الاتفاقية الأوروبية حول الجريــمة الافتراضية لعام 2001.

أشارت المادة 22 من هذه الاتفاقية إلى المبادئ التي يجب على الدول الأطراف اعتمادها لتحديد الإختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها في هذه الاتفاقية وهي: مبدأ الإقليمية، وأوردت

1 المادة 15 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

من خلاله إمكانية تبني كل دولة طرف في الاتفاقية متابعة الجرائم المنصوص عليها إذا ارتكبت ضمن النطاق الإقليمي للدولة، وعلى سبيل المثال ينعقد الاختصاص للدولة إذا كان نظام الحاسوب للجاني يقع ضمن الإطار الإقليمي، ولو كان المعتدي مقيماً خارج الدولة، كما يعد الاختصاص الإقليمي متوفراً وفق الاتفاقية إذا كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة[1].

وكذا نصت الاتفاقية على مبدأ شخصية القوانين بحيث نصت على هذا الأخير الفقرة الأولى البند الرابع من المادة 22, والتي مكنت الدول الأطراف أن تكون مختصة جزائياً عندما يرتكب مواطنوا أي من هذه الدول جريمة في الخارج إذا كان هذا السلوك يشكل جريمة وفق قانون الدولة التي ارتكبت على أرضها الجريمة. كما جاءت الفقرة الثالثة من المادة 22 من الإتفاقية لتنص على مبدأ العالمية, والتي تقضي بأنه:"في حالة رفض أي دولة طرف في هذه الاتفاقية تسليم مرتكب الجريمة المتواجد على أرضها على أساس مبدأ الشخصية، فيجب على الدولة الرافضة القيام بإجراءات التحقيق والمحاكمة وفقاً لقانونها الوطني".

ولقد سمحت الفقرة الثانية من المادة 22 من الاتفاقية للدول الأطراف التحفظ على هذه المبادئ باستثناء مسألتين هما: مبدأ الإقليمية، والثانية عندما يكون التزام متبادل بين الدول بتسليم المجرمين، كما سمحت الفقرة الرابعة من المادة 22 للدول الأطراف أن تتخذ أشكالاً أخرى من مبادئ الاختصاص على نحو يتناسب مع قانونها الوطني[2].

وإذا كانت الجريمة المرتكبة في العالم الافتراضي تدخل في اختصاص أكثر من دولة من الدول الأطراف مثل جرائم الاحتيال وغيرها، فإنه يجدر على الدول التشاور بينها لتحديد المكان الملائم للمحاكمة حتى يتم تجنب ازدواج الجهود المبذولة أو المنافسة بين السلطات الرسمية في الدول ذات العلاقة[3].

البند الثاني: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود.

جاءت الإتفاقية بحكم خاص فيما يتعلق بتحديد الولاية القضائية للدول في حالة الجرائم الواقعة في المجال الإلكتروني وعبر شبكة الانترنت، فقد حددت المادة 15 من الإتفاقية المعايير التي يمكن للدول الأطراف اتباعها في تحديد الاختصاص القضائي، وبذلك دعت هذه المادة كل دولة طرف في الإتفاقية أن تعتمد ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات التالية:

1 عمر بن يونس، المرجع السابق، ص 181.

2 محمد طارق الخن، المرجع السابق، ص 205.

3 الفقرة الخامسة من المادة 22 من اتفاقية بوداست.

- عندما ترتكب الجريمة في إقليم الدولة,
- عندما ترتكب الجريمة ضد أحد مواطني الدولة,
- عندما يرتكب الجريمة أحد مواطني تلك الدولة, أو شخص عديم الجنسية مكان إقامته المعتاد في إقليمها.

كما نصت الاتفاقية على أنه في حالة ممارسة الاختصاص القضائي تبعاً لأحد المعايير من قبل أي دولة، وتم علمها بإجراء تحقيق أو ملاحقة قضائية بشأن نفس الجريمة من قبل دولة أو دول أخرى، فإنه يجدر التشاور بين هذه الدول للتنسيق فيما بينها لاتخاذ التدابير اللازمة[1].

البند الثالث: القانون العربي الاسترشادي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات لعام 2004.

جاءت معالجة الإختصاص القضائي في هذا القانون في شكل محدود؛ إذ تضمنت نص وحيد يتمثل في المادة 26 منه التي جاءت تحت عنوان "إطار تطبيق القانون"، والتي تضمنت مبدأ الاختصاص العيني بحيث قضت بسريان أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه, حتى لو ارتكبت كلياً أو جزئياً خارج إقليم الدولة متى أضرت بأحد مصالحها, ويختص القضاء الوطني بنظر الدعاوى المترتبة عنها[2].

الفرع الثالث: تقييم المبادئ التقليدية لحل تنازع الإختصاص القضائي في الجرائم الإلكترونية.

تظهر خصوصية الجريمة المرتكبة إلكترونياً بشكل أبرز في حالة النزاع في الاختصاص القضائي بين الدول، وهذا نظراً لصعوبة التحكم في سبل ارتكابها, أو ضبط الوسائل المستخدمة في إنشاء السلوك الإجرامي الراجع إلى طبيعة مسرح الجريمة، ولعل تطبيق المبادئ التقليدية لحل تنازع الاختصاص في مثل هذا النوع من الجريمة قد سد جزء من الإشكالية المترتبة عنها في حالة ما تناسب المبدأ المعتمد مع مجريات ارتكاب الجريمة، وبهذا تكون له فعالية في إيجاد حل لمشكلة الإختصاص بشرط التناسق مع الدول الأخرى التي تعنيها مسألة ارتكاب الجريمة.

1 خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، سنة 2012، ص 58.

2 عبد الله عبد الكريم عبد الله، المرجع السابق، ص 147.

وبهذا ذهب البعض من الفقه[1] إلى إعطاء حلول فيما يخص مسألة التنازع الإيجابي للاختصاص القضائي بين الدول بإعطاء أولوية لأحد المبادئ التي تشكل فعالية وجدوى في الكشف عن الجريمة، وضمان ملاحقة مرتكبيها وتوقيع العقوبات المناسبة عليهم، وهو ما يذهب إلى تبرير قبول مبدأ الإقليمية في بعض الحالات كأفضل المعايير؛ نظراً لاعتماده على فكرة مكان وقوع الإعتداء بشكل كلي أو جزئي، مما يتيح التعرف بشكل أكبر على الأدلة والأجهزة المستخدمة في الجريمة إما في مرحلة بداية السلوك الإجرامي أو آثاره النهائية دون الوقوف عند شخصية الجاني.

كما أن مبدأ شخصية النص الجنائي قد يمثل لدى البعض أحد المعايير المثالية فيما يخص مسألة ضمان توسع تنفيذ القوانين الوطنية خارج الإقليم تبعاً لشخصية الجاني، وبهذا لا يعتد بالحدود الإقليمية بين الدول ومحو العامل الإقليمي كحاجز لتحقيق أفضل للعدالة خاصة فيما يتعلق بهذا النوع من الجرائم التي ألغت بدورها طابع الحدود المكانية.

كما أن مبدأ الاختصاص العيني يمثل دوراً بارزاً في الحفاظ على المصالح الاستراتيجية للدول خاصة إذا كانت الجرائم المرتكبة إلكترونياً تمثل تهديداً مستحدثاً يحمل بين طياته السرعة والخطورة وعدم القدرة على التحكم من قبل السلطات القضائية, وهو ما قد يجد جدواه من خلال تطبيق مبدأ عينية النص الجنائي الذي يهتم بموضوع الجريمة وخطورتها بغض النظر عن الإقليم المرتكبة فيه أو جنسية الجاني[2].

إلا أنه بالمقابل فإن جانب من الفقه الفرنسي[3] يرى عدم فاعلية المبادئ التقليدية للاختصاص القضائي في الجرائم الإلكترونية الواقعة في الخارج وذلك للأسباب التالية:

في ظل الوضع الراهن للأنظمة القانونية وفكرة تدويل الجرائم المرتكبة عن طريق التعامل الإلكتروني تجعل من فكرة العقاب أمراً احتمالياً، حيث أن من الصعب التحكم في حركة السير عبر وسائل الإتصال الحديثة وشبكة الانترنت, مما يتيح للجناة قدرة على التملص من العقاب.

كما أنه قد يصادف تطبيق هذه المبادئ صعوبات يترتب عنها البطء والتعقيد وطول الإجراءات، وقد يصطدم بفكرة صعوبة التنفيذ للأحكام الصادرة في الخارج، أو فكرة تسليم المجرمين نظراً لمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة.

---

1 سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس القاهرة، 1997، ص 425 وما بعدها.

2 Ann BRISSET GIUSTINIANI, Op.Cit. p 89.

3 Myriam quéméner, yves CHARPENEL, Op. Cit, p 125.

المطلب الثاني: حـــلول مشكلة تـــنازع الإختصاص القضائي للجرائـــم الواقعة فـــي إطار المعاملات الالكترونية.

تبقى مسألة حل تنازع الاختصاص القضائي في الجرائم الواقعة عبر المعاملات الإلكترونية رهينة تبني المعيار الأمثل, وهو ما يتجسد في مبدأ العالمية باعتباره يشكل أفضل الحلول وأنجعها، وتناسبها مع طبيعة وكيفية ارتكاب هذه الجرائم (الفرع الأول)، أضف إلى ذلك اعتماد مسألة التعاون القضائي بين الدول، وما تشكله وسائل المساعدة القضائية أو الإنابة القضائية من فرص للتعاون الدولي الإجرائي في الحد من الجريمة الإلكترونية (الفرع الثاني).

الفرع الأول: مبدأ العالمية كحل أمثل لمشكلة تنازع الاختصاص القضائي في الجرائم الإلكترونيـــة.

من المتفق عليه أن الجرائم الماسة بالمعاملات الإلكترونية هي جرائم عابرة للحدود لا تتقيد بظرف المكان ولا الزمان، وكذا إن المعايير المتبناة من قبل التشريعات العقابية قد لا تقدم الحل الأمثل لمشكلة التنازع الإيجابي للإختصاص بين الدول، وهذا ما جعل الفقه والقضاء يسير نحو مبدأ عالمية النص الجنائي لما لهذا المبدأ من أهمية وفاعلية في عقاب المجرمين على المستوى الدولي، ويعني هذا المبدأ أن يطبق القانون الوطني على أي شخص ارتكب جريمة وتم القبض عليه في إقليم الدولة أياً كانت جنسيته أو جنسية المجني عليه[1]، وبالتالي يعطي هذا المبدأ لقانون العقوبات مجالاً متسعاً يشمل العالم كله، فلا يتقيد بمكان ارتكاب الجريمة أو أحد سلوكياتها, ولا بجنسية مرتكبها, ولا بطبيعة الجريمة ومساسها بالسيادة والمصالح الوطنية.

ويُبرَر إقرار مبدأ العالمية لازدياد ظاهرة الإجرام الدولي الذي لا يقتصر على نطاق دولة معينة، وبهذا فهو يسد العجز أو النقص الذي قد يجده المشرع الوطني من تطبيق مبادئ الإقليمية أو الشخصية أو العينية ويضمن عدم إفلات أي مجرم من العقاب في أي مكان في العالم، فالخطورة المتلاحقة والمتنامية للإجرام الدولي الحديث في شكله المتعلق بالاعتداء الحاصل عبر التعاملات الإلكترونية وشبكة الانترنت, أدى إلى إتاحة الفرص لنشوء عصابات دولية ينتمي أفرادها إلى العديد من الدول ويحملون جنسيات مختلفة، وبالتالي فمن الصعب أن تقوم دولة واحدة بمجابهة هذا النوع من الإجرام[2]. وعليه لا بد من تكاثف الدول فيما بينها لتحقيق هذا الهدف، وهو الأساس الذي يقوم عليه مبدأ العالمية بتجسيد فكرة التضامن والإتجاه نحو

1 جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، مرجع سابق، ص 73.

2 مصطفى محمد موسى، المرجع السابق، ص 205.

تأكيد عالمية الجزاء الجنائي، وبهذا فإن التضامن والتعاون بين التشريعات الدولية قد يرتب فرصة التقليل من هروب الجناة من العدالة، ويضمن تطبيق العدالة الجنائية على مرتكب الجريمة في أي مكان في العالم.

وقد أخذت بعض الدول بمبدأ العالمية على سبيل الحصر في بعض الجرائم، ومنها دولة الإمارات العربية المتحدة، حيث نصت المادة 21 من قانون العقوبات الاتحادي على سريان قانون دولة الإمارات على كل من وجد في الدولة بعد ارتكابه في الخارج بوصفه فاعلاً أو شريكاً جريمة تخريب أو تعطيل وسائل الإتصال الدولية وجرائم الاتجار في المخدرات أو النساء أو الصغار أو الرقيق, أو جرائم القرصنة أو الإرهاب الدولي.

والملاحظ أن أغلب التشريعات المقارنة لم تأخذ بمبدأ العالمية على غرار التشريع الجزائري بالرغم من أهميته في إيجاد حل فعال لمشكلة الاختصاص القضائي، ومواجهة خطورة الجريمة المرتكبة عبر التعاملات الإلكترونية والإنترنت، وبهذا نرى وجوب توجه التشريعات المقارنة إلى التوحد ضمن تشريعات دولية اتفاقية تعطي لهذا المبدأ المشروعية والصلاحية في التطبيق في حالة وجود مثل هذا النوع من الجرائم، كما أنه يجب تدعيم هذا المبدأ بتعاون دولي جاد وسريع وإعداد تشريعات وطنية لتجريم الظاهرة، وبالتالي إمكانية توقيع العقاب على الجناة دون النظر إلى جنسية أو إقليم وقوع الجريمة.

الفرع الثانـي: التعاون القضائي الدولـــي في الجرائم الماسة بالمعاملات الإلكترونية.

تبقى إشكالية الإختصاص القضائي في الجرائم الإلكترونية وعبر الانترنت تتشعب على عدة أوجه مما يخلق ضرورة لحلها بما يحقق العدالة الجنائية, وتوقيع العقاب على الجناة والحد من إفلاتهم من قبضة القضاء، وإذا كانت فكرة تبني المعايير الخاصة بمنح الولاية القضائية للدول في مجال ارتكاب الجريمة الإلكترونية، وتوجه التشريعات إلى اعتمادها كحل تقليدي يبقى له نوع من القصور وعدم التدارك المجدي للحد من الجريمة نتيجة اختلاف التشريعات الجنائية في الدول، والناتج عن اختلاف العادات والثقافات يكون من الطبيعي أن نجد بعض الأفعال مشروعة في دولة المنشأ ومجرمة في بلد آخر, وهو ما قد يصطدم مع فكرة تطبيق مبدأ الإقليمية أو الشخصية أو العينية أو العالمية، وهنا تُضاف عقبة أخرى لتطبيق المبادئ وإيجاد حل لفكرة تنازع الإختصاص القضائي في الجرائم الإلكترونية.

وهنا كان لزاماً تدعيم تلك المبادئ بأساليب تشريعية وقضائية لإعطائها أكثر نجاعة, وهذا ما يترجمه أسلوب التعاون القضائي الدولي الذي يقصد به:"مجموعة الإجراءات القضائية التي بها الدولة لتسهيل

مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم، وهذا بتحقيق مساعدة قضائية متبادلة هادفة إلى تحقيق السرعة والفاعلية في إجراء ملاحقة وعقاب مرتكبي الجرائم"[1].

ولقد اشتملت الاتفاقيات الدولية الحديثة مجالاً واسعاً في المساعدة والتعاون القضائي؛ حيث اشتملت على ضرورة الإتجاه إلى أساليب الإنابة القضائية والتسليم بالوقائع الإجرامية، والأحكام القضائية وحضور الشهود والخبراء وتجميع عناصر الأدلة, والقيام بالبحث وتقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية وغيرها[2].

البـــند الأول: المساعدة القضائية.

يأخذ أسلوب المساعدة القضائية صور وأوجه متعددة, تصب في إطار تسهيل إجراءات البحث والتحري في الجرائم الإلكترونية, وهي:

أولاً: تــبادل المعلومات:

يقصد بها قيام الدول المتعاقدة في إطار اتفاقيات دولية بتقديم المعلومات والبيانات التي تطلبها السلطات القضائية بصدد جريمة ما والتبادل فيما بينها، وهذا التبادل قد يشمل التبادل بصفة منتظمة لنصوص التشريعات النافذة والمعلومات المختلفة الخاصة بالتنظيم القضائي، وتعمل على اتخاذ الإجراءات الرامية إلى التوفيق بين النصوص التشريعية والتنسيق بين الأنظمة القضائية لدى الأطراف المتعاقدة حسب ما تقتضيه الظروف الخاصة لكل منها, ومن أمثلتها ما جاءت به اتفاقية الرياض العربية للتعاون القضائي الدولي[3].

ثانـــياً: حق التقاضي وحضور الشهود والخبراء.

بحيث يكون للمواطنين في الدول المتعاقدة حق التقاضي أمام الهيئات القضائية للمطالبة بحقوقهم والدفاع عنها، ولا يجوز أن تفرض عليهم أي ضمانات شخصية أو عينية لكونهم لا يحملون جنسية الأطراف الأخرى في القضايا، أو عدم وجود إقامة لهم خارج إقليم دولتهم، كما أنه يعتبر مسألة تنقل الشهود والخبراء من دولة لأخرى من أهم صور المساعدة القضائية في المجال الجنائي مع إلزامية توافر شروط

1 سالم محمد سليمان الأوجلي، المرجع السابق، ص 430.

2 أحمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، بحث منشور بمجلة الفكر الشرطي، المجلد 17، العدد الرابع، عام 2008، ص 153.

3 اتفاقية الرياض للتعاون القضائي الدولي الموقعة بين عشرين دولة عربية وهم: السعودية- الإمارات العربية- تونس – الجزائر- جيبوتي – السودان- سوريا – الصومال- العراق- عمان- قطر- الكويت- لبنان- ليبيا- المغرب- موريطانيا- اليمن.

محددة، نذكر منها ما جاء في اتفاقية للتعاون القضائي وهي: توافر الإرادة للشهود والخبير للحضور أمام الهيئات القضائية الطالبة لحضوره، ويجب احترام الطرق المحددة قانوناً لحضور الشهود والخبراء وإعطاؤهم حصانة ضد اتخاذ أي إجراءات جنائية بحقهم, كإلقاء القبض أو الحبس أو تنفيذ أحكام سابقة على دخوله إلى إقليم الدولة الطالبة لحضوره أمامها.

ولقد أرست الإتفاقية الأوروبية للإجرام المعلوماتي قواعد المساعدة القضائية والتعاون القضائي؛ حيث قررت في حالة ارتكاب أي نوع من الجرائم الواقعة عبر الوسائل الإلكترونية، فإنه يأخذ بأحكام المادتين 33 و34 المتعلقة بالمساعدة القضائية الخاصة بتجميع حركة البيانات في الزمن الفعلي ومراقبة محتوى البيانات, وهو ما يجعل لجميع الأطراف المتعاقدة في هذه الاتفاقية وجود نطاق مختلف لتطبيق الإجراءات[1].

البند الثانـــي: الإنابة القضائية الدولية.

يقصد بها طلب تتقدم به الدولة الطالبة بغرض اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية في الدولة المطلوب منها لضرورة الفصل في مسألة معروضة على السلطة القضائية للدولة الطالبة, والتي يتعذر عليها القيام بها بنفسها، وهي بذلك تمنح لدولة ما بمباشرة إجراء قضائي يتعلق بالدعوى داخل الحدود الإقليمية لدولة أخرى نيابة عنها وبناءً على طلبها, ووفقاً لما نصت عليه وقررته بنود الإتفاقية الدولية بينهما في هذا الصدد[2].

وتعتبر الإنابة القضائية آلية لتسهيل الإجراءات الجنائية بين الدول بما يضمن سير إجراءات تقديم المتهمين، وتجاوز عقبة السيادة الدولية التي تحول دون ممارسة بعض الدول لبعض الأعمال القضائية داخل إقليم دولة أخرى، وبهذا تمكن الإنابة القضائية السلطات القضائية المختصة من ممارسة الإجراءات في الدولة المطلوب منها التنفيذ دون تدخل أو مشاركة من الأجهزة في الدول الطالبة, مما يساعد هذا التعاون على عدم ضياع الأدلة والآثار المتعلقة بالجريمة وإنجاز التحقيقات الجارية في الدولة الطالبة وحفظ حقوق المتهمين في الإسراع بمحاكمتهم[3].

1 جميل عبد الباقي الصغير، المرجع السابق، ص 80.

2 نبيلة هروال، المرجع السابق، 254.

3 سالم محمد سليمان الأوجلي، المرجع السابق، ص 156.

ونجد التشريع الفرنسي قد أقر بنظام الإنابة القضائية عن الطريق الدبلوماسي، بحيث يتم توجيهها لوزارة العدل طبقاً للإجراءات المنصوص عليها بالنسبة لطلبات تسليم المجرمين في نص المادة 696 من قانون الإجراءات الجزائية الفرنسي والمعدلة بالقانون رقم 204 لسنة 2004 بمقتضى المادة 17 منه.

ونجد الإتفاقية الأوروبية للتعاون القضائي تنص على مسألة تبادل الإنابة بين قرارات العدل مباشرة في حالة الاستعجال يمكن تنفيذها مباشرة من الدول الطالبة إلى الدولة المطلوب منها، ويتم التسليم عن طريق الانتربول، كما يشترط في تنفيذ الإنابة القضائية بين الدول إرسال الملف الخاص بالقضية مع المرفقات من محاضر الاستدلالات ومحاضر التحقيق والمستندات التي أجريت بمعرفة السلطة القضائية في الدولة الطالبة، وكذلك يجب أن يتضمن طلب الإنابة نوع القضية والجهة الصادرة عنها طلب الإنابة والجهة الموجهة إليها طلب التنفيذ, وجميع البيانات والتفاصيل المتعلقة بملف القضية[1].

كما أن الإنابة القضائية تتعدد في شكلها التقليدي من خلال الجهة الطالبة في دولة، والجهة المطلوب منها التنفيذ في دولة أخرى, وذلك في الحالات الآتية[2]:

1. **الطريق الدبلوماسي**: الذي تتم فيه الإنابة القضائية عن طريق طلب مقدم من المحكمة المختصة بنظر الدعوى إلى وزارة الخارجية، والتي تقوم هذه الأخيرة بدورها إلى إرسالها ممثلها الدبلوماسي في البلد الأجنبي.
2. **الطريق القنصلي**: من خلال قيام المحكمة المختصة بإرسال طلب الإنابة إلى قنصلها مباشرة في الدولة المطلوب فيها تنفيذ الإنابة، والذي يقوم بدوره بعد ذلك توجيه الإنابة إلى الجهة المختصة في البلد المطلوب تنفيذ الإنابة فيه.
3. **الطريق القضائي**: وهنا تقوم المحكمة المختصة بتوجيه الإنابة مباشرة إلى المحكمة الأجنبية المطالب منها تنفيذ الإنابة وذلك تنفيذاً لمعاهدة دولية سابقة، أو فقاً لأحكام قانون الدولتين.

وتعد هذه الطرق هي الأنواع التقليدية لتنفيذ الإنابة القضائية، والتي لا قد لا تتماشى في تطبيقها مع طبيعة الجرائم المرتكبة في مجال المعاملات الإلكترونية وعبر الانترنت, التي تتسم بالسرعة والخطورة بالتلاعب في البيانات والتخلص منها, مما يستوجب إبرام اتفاقيات حديثة تشتمل على أساليب حديثة لتنفيذ الإنابة القضائية في مثل هذا النوع من الجرائم، بحيث يشترط توافر عنصر السرعة لتدارك الإجراءات

1 أحمد عبد الحليم شاكر، المرجع السابق، ص 160.

2 محمد أمين الشوابكة، المرجع السابق، ص 68.

بشكل فوري, ومنها مثلاً آلية الاتصال المباشر من الجهتين المختصين بتنفيذ الإنابة القضائية بينها عن طريق الوسائل الحديثة أو التصوير عن بعد في حالة الاستعجال التي من شأنها تحسين التعاون القضائي، ومن أمثلتها الإتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفهياً في حالة الاستعجال، كما تحث إحدى توصيات المجلس الأوروبي المتعلقة بمشاكل الإجراءات الخاصة بالمعلوماتية الدول الأطراف على تيسير الإجراءات وإنشاء نظام للربط بين السلطة القضائية والسلطات الأجنبية بهدف الحصول على الأدلة على وجه السرعة[1].

1 محمد لموسخ، تنازع الاختصاص في الجرائم الإلكترونية، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، العدد 2، السنة 2009، ص 23.

المبحث الثاني:

سلطة المحكمة الجنائية في التعامل مع الدليل الإلكترونـــي.

يأخذ الدليل الإلكتروني نفس المكانة للأدلة التقليدية من حيث التعامل من قبل القاضي في مرحلة المحاكمة، ويخضع لنفس القواعد المقررة لباقي الأدلة سواء كانت هذه القواعد تتعلق بسلطة القاضي الجنائي في قبول الدليل الإلكتروني، أو تتعلق بسلطته في تقدير هذا النوع من الدليل، وبالنظر إلى الطبيعة الخاصة التي يتميز بها الدليل الإلكتروني وما قد يصاحب الحصول عليه من خطوات معقدة، فإن قبوله في الإثبات قد يثير العديد من الإشكالات التي يحرص القاضي الجنائي التعامل بها باحترافية وتمحيص.

ولا تقف الصعوبات التي تواجه الدليل الإلكتروني عند حد كيفية الحصول عليه وإجراءات حفظه، بل تمتد إلى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية القاضي بالإقتناع به من عدمه. لذلك حاول التشريع والقضاء والفقه المقارن التصدي لهذه المسألة وذلك بتحديد الأساس الذي يستند إليه قبول الدليل الإلكتروني، وكذا وضع القيود والشروط التي يجب توافرها في الدليل الإلكتروني أو في المخرجات حتى يمكن قبوله من قبل القاضي الجنائي.

وبناءً على ما تقدم ستناول سلطة القاضي الجنائي في قبول الدليل الإلكتروني بما يتلائم مع القواعد العامة في الإثبات (المطلب الأول)، وكذا سلطة القاضي الجنائي في تقدير الدليل الإلكتروني (المطلب الثاني).

المطلب الأول: سلطة القاضي الجنائي في قبول الدليل الالكترونــي.

يعد قبول الدليل الجنائي الخطوة الإجرائية الأولى التي يمارسها القاضي اتجاه الدليل الجنائي بصفة عامة والدليل الإلكتروني بصفة خاصة، وذلك قبل البدء في تقديره للدليل للتأكد من مدى صلاحيته، وملائمته لتحقيق ما قدم من أجله، ويهدف القاضي الجنائي في هذه المرحلة إلى التيقن من مدى مراعاة الدليل الإلكتروني لقاعدة المشروعية، والتي لا يمكن بدونها أن يترتب على الدليل أي آثار قانونية، بل يثير إهمالها أو مخالفة ما يستلزمه من شروط آثار قانونية إلى بطلانه أمام القضاء.

الفرع الأول: أساس قبول الدليل الإلكترونــي.

يخضع الدليل الإلكتروني إلى طبيعة النظام السائد في الدولة، وتختلف النظم القانونية في موقفها من الأدلة التي تقبل كأساس للحكم بالإدانة بحسب الإتجاه الذي تتبناه، وهناك اتجاهان رئيسيان؛ الأول: نظام مبدأ حرية الإثبات ويقصد به فتح المجال للقاضي في قبول جميع الأدلة، وهنا تكون جميع طرق الإثبات مقبولة ما لم يستبعد المشرع بعضها صراحة (البند الأول)، أما الاتجاه الثاني فهو نظام الإثبات المقيد وتتبناه القوانين الأنجلوسكسونية بحيث يقيد من حرية الإثبات في مرحلة الفصل بالإدانة أو البراءة، وقد تحدد الأدلة القانونية بشكل حصري، فلا يجوز للقاضي اللجوء إلا لأدلة معينة من قبل التشريع سلفاً (البند الثاني), والإستثناء الوارد على الدليل الإلكتروني (البند الثالث).

البند الأول: نظام الإثبات الحر .

لم تُفرِد التشريعات المنتمية إلى العائلة ذات الأصل اللاتيني مثل فرنسا وغيرها من الدول المتأثرة بها كالجزائر، نصوصاً خاصة فيما يتعلق بقبول الدليل الإلكتروني، وذلك على أساس أن هذه الدول تستند لمبدأ حرية الإثبات في المسائل الجنائية[1]، كما أن هذا النظام يخول للقاضي سلطة تقييم الأدلة دون أن يفرض عليه قيداً أو شرطاً، فالقاضي حر في أن يستعين بكل طرق الإثبات للبحث عن الحقيقة، وهو حر في وزن وتقدير كل دليل، وفي التنسيق بين الأدلة التي تتمثل في الحكم بالإدانة أو البراءة. ونتيجة لذلك فإنه يحظر على المشرع إضفاء قوة معينة لأي دليل من شأنه أن يقيد سلطة القاضي في تكوين قناعته، أو يسبغ على بعضها شكاً أو عدم ثقة كي يستبعدها القاضي من تقديره الحر[2].

---

1 نبيل صقر, الوسيط في شرح قانون الإجراءات المدنية والإدارية (الخصومة, التنفيذ, التحكيم), دار الهدى, عين مليلة, الجزائر, 2008, ص: 160.

2 فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، أطروحة دكتوراه ، كلية الحقوق، جامعة بغداد، 1992، ص 60.

وانطلاقاً مما سبق ذكره يتضح لنا مبدئياً أنه يجوز للقاضي الجنائي الإستناد إلى الدليل الإلكتروني لإثبات الفعل الجنائي في سائر الجرائم بشكل عام والجرائم الإلكترونية على وجه الخصوص، وهو ما سنبينه بالتفصيل فيما يلي:

أولاً: مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإلكترونـــي.

تعتبر حرية الإثبات في المسائل الجنائية من المبادئ المستقرة في نظرية الإثبات الجنائي، وذلك بخلاف المسائل المدنية، حيث يحدد القانون سلفاً وسائل الإثبات وقواعد قبولها، وقد استقر مبدأ حرية الإثبات الجنائي القديم على الرغم من أن قانون التحقيقات الجنائية الفرنسي لم يكرسه صراحة وإنما أشير إليه في بعض النصوص، خاصة التعليمة المقررة للمحلفين لدى محكمة الجنايات[1].

وفي الوقت الراهن، فإن قانون الإجراءات الفرنسي قد أقر مبدأ حرية الإثبات الجنائي صراحة بمقتضى المادة 427 من حيث أنه يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناءً على اقتناعه الشخصي، ما لم يرد نص مخالف لذلك، وهذا النص وإن كان مخصصاً لمحاكم الجنح، إلا أن مبدأ حرية الإثبات يطبق أمام جميع المحاكم الجنائية, إلا إذا نص القانون على خلاف ذلك.

وكذلك أقر المشرع الجزائري مبدأ حرية الإثبات الجنائي حيث نص على جواز إثبات الجرائم بأي طريق من طرق الإثبات, ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعاً للاقتناع الشخصي[2].

وتكمن الأسباب الداعية لضرورة إعمال مبدأ حرية الإثبات في نطاق نظرية الإثبات الجنائي فيما يلي:

- أن حرية الإثبات تعد نتيجة منطقية لمبدأ قضاء القاضي بمحض اقتناعه، والتي تستتبع في نفس الوقت السماح للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها لتمكين القاضي من أداء رسالته في إرساء العدالة بين المتقاضين.
- إن الإثبات في الدعوى الجنائية يرد على وقائع قانونية أو مادية يصعب بل يستحيل الحصول على دليل سابق لها، كما أن موضع الإثبات في الدعوى الجنائية يرد على وقائع قانونية تنتمي إلى الماضي، لذلك لا بد للمحكمة أن تستعين بكل الوسائل الممكنة كي تعيد لها الحقائق التي حدثت في الواقع.

1 المادة 342 من قانون التحقيقات الجنائية الفرنسي.

2 المادة 212 من قانون الإجراءات الجزائية الجزائري.

ومن المسلم به أن قرينة البراءة تلقي عبء الإثبات كلية على عاتق سلطة الاتهام مما جعل مهمة هذه الأخيرة جد صعبة، وكذا أن طبيعة المصلحة التي تحميها الدعوى الجنائية تختلف عن تلك التي تحميها الدعوى المدنية، بالإضافة إلى أن مبدأ حرية الإثبات يعد بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية، والتي لو تم حصرها كأدلة إثبات على مواجهة الجرائم المستحدثة ومنها الجريمة الإلكترونية[1].

وعلى ذلك نلاحظ أن الدليل الإلكتروني في نظام الإثبات الحر له نفس شأن الأدلة الأخرى وهو مقبول مبدئياً في الإثبات الجنائي بصفة عامة, والإثبات في الجرائم الواقعة إلكترونياً بصفة خاصة، كما لا تثار مشكلة مشروعية الدليل الإلكتروني من حيث الوجود على اعتبار أن المشرع لا يعهد له سياسة النص على قائمة لأدلة الإثبات، ولذلك فمسألة قبول الدليل الإلكتروني لا ينال منها سوى مدى اقتناع القاضي بها إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي.

ثانـــياً: النتائج المترتبة على تطبيق مبدأ حرية الإثبات الجنائـي.

إن إعمال مبدأ حرية الإثبات يجعل القاضي الجنائي يتمتع بدور إيجابي في توفير وقبول الدليل الجنائي بما في ذلك الدليل الإلكتروني، بحيث يؤدي القاضي دوراً مهماً في عملية الإثبات، وحتى يتضح لنا هذا الدور المهم للقاضي الجنائي يتعين لنا أن نقوم بتحديد مفهوم هذا الدور بداية، ثم نعرض لأهم مظاهر الدور الإيجابي للقاضي.

1- مفهوم الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكترونـــي:

يقصد به عدم التزام القاضي بما يقدمه له أطراف الدعوى من أدلة، وإنما له سلطة وواجب يملي عليه المبادرة من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعلية فيها، وفي 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 وأن يوجه أحد الأطراف إلى تقديم دليل بعينه، بينما القاضي الجنائي لا يتخذ هذا الدور السلبي[2].

والنظام الإجرائي السائد في الدولة هو الذي يحدد دور القاضي الجنائي في هذا الشأن سلبياً، لأن هذا النظام ينظر إلى الدعوى الجنائية على أنها ملك للطرفين؛ الأول هو الإدعاء، ويمثله المضرور من الجريمة،

1 بدرالدين يونس، سلطة القاضي الجنائي في تقدير الدليل الجنائي، أطروحة دكتوراه, كلية الحقوق، جامعة قسنطينة1، 2014، ص 74.

2 علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي, المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد 1، الإمارات العربية المتحدة، 26-28 أفريل 2003، ص 56.

والآخر هو مرتكب الجريمة، أما إذا كان النظام التنقيبي هو المهيمن على الإجراءات الجنائية كالقانون الفرنسي والجزائري والمصري, فحينئذ يكون دور القاضي إيجابياً في صدد تحقيق الدعوى والفصل فيها.

2. مظاهر الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكترونـــي:

أفرد القانون الإجرائي الفرنسي نصاً خاصاً منح بموجبه رئيس محكمة الجنايات سلطة تقديرية خاصة للقيام بجميع الإجراءات التي يقدر فائدتها في كشف الحقيقة وفقاً لمادة 310 من قانون الإجراءات الفرنسي، ولايختلف الوضع في ذلك عند القانون المصري؛ بحيث نصت المادة 291 من قانون الإجراءات الجنائية على أنه للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لظهور الحقيقة. وكذلك يعد من مظاهر الدور الإيجابي للقاضي الجنائي في القانون المصري ما نصت عليه المادة 274 من قانون الإجراءات الجزائية حيث حظرت استجواب المتهم ما لم يقبل هو بذلك، غير أنها أضافت أنه إذا ظهر أثناء المرافعة والمناقشة بعض الوقائع ترى لزوم تقديم إيضاحات عنها من المتهم لظهور الحقيقة, يلفته القاضي إليها ويرخص له بتقديم تلك الإيضاحات[1].

كما أن القاضي الجنائي يستطيع من أجل الوصول إلى الحقيقة أن يوجه أمراً إلى مزود خدمة الإنترنت بتقديم بيانات معلوماتية المتعلقة بمستخدم الانترنت، وكذا يمكن للقاضي البحث في الدليل الإلكتروني من خلال أمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، وكذلك للقاضي الجنائي سلطة الأمر بتفتيش نظم الحاسب الآلي بمكوناته المادية والمعنوية وشبكات الإتصال, متى قدر ضرورة ملائمة هذا الإجراء[2].

وفي مجال البحث عن الدليل الإلكتروني نجد أن الخبرة التقنية تعد من أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات، فهي تؤدي دوراً لا يستهان به, خاصة مع نقص المعرفة القضائية الشخصية لظاهرة الحاسب الآلي ذاته يعد أمراً بالغ التعقيد ويحتاج إلى وجود خبير، لا سيما في حالة التشفير وغيرها من الوسائل الفنية.

1 عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن، د.ط، دار الجامعة الجديدة، الاسكندرية،سنة 2010، ص 268.

2 هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع سابق، 104.

البند الثانـــي: نظام الإثبات المقيد.

إن المشرع وفقاً لهذا النظام يعتبر هو المحدد الأساسي لنظام الإثبات الجنائي، بحيث يعمل على حصر الأدلة التي يمكن للقاضي اللجوء إليها في الإثبات، ويجب أن يتقيد بها الحكم بوجهيه الإدانة أم البراءة، وبهذا يقتصر دور القاضي على مجرد فحص تلك الأدلة للتأكد من توافر الشروط التي حددها القانون سلفاً، ولا سبيل للاستناد إلى أي دليل يخرج عن الأدلة التي لم ينص عليها صراحة ضمن التشريع[1].

ولا يكتفي بتقييد القاضي في الأخذ بالأدلة محل الإثبات، بل يتعداه إلى تحديد دور القاضي في تقدير القيمة الإقناعية للدليل الجنائي، بحيث يمنع إعمال اقتناعه الشخصي أو ميوله نحو الأدلة، فهنا أخذ المشرع دور القاضي في الاقتناع والأخذ بالأدلة، وبالتالي فإن اليقين القانوني يقوم أساساً على افتراض صحة الدليل بغض النظر عن مجريات الدعوى واختلاف حيثيات القضية، ويكبح اجتهاد القاضي اتجاه تقدير الدليل, فالدور الأول والأخير يقتصر على توافرها في الدليل دون الرجوع إلى الاقتناع الشخصي للقاضي[2].

ومن الدول التي تأخذ بهذا النظام هي الدول الأنجلوسكسونية كالو.م.أ وإنجلترا وأستراليا، وبالرجوع إلى آليات تطبيق هذا النظام في هذه الدول نجد أنه يخضع لقواعد خاصة لقبوله أمام المحاكم، وهذا على اعتبار أن هذه الدول تطبق قاعدة استبعاد شهادة السماع من الإثبات الجنائي، وإذا اعتبر الدليل الإلكتروني هو أحد التطبيقات لشهادة السماع لكونه يتضمن أقوالاً وبيانات ومعلومات من انتاج الشخص، وتم حفظها أو وضعها في الحاسوب أو شبكة الانترنت[3]، فهنا يثار الإشكال بموضع الدليل الإلكتروني من هذه القاعدة، وعلى أي أساس تم استبعاده أو قبوله كدليل يعتد به أمام القاضي الجنائي؟

يتضح أن بعض التشريعات المقارنة في النظام الأنجلوسكسوني كالولايات المتحدة الأمريكية وإنجلترا أو كندا وأستراليا لا تعتد بالشهادة السماعية في الإثبات الجنائي، وبما أن الدليل الإلكتروني يصنف ضمن هذه القاعدة فيعتبر في أول وهلة غير مقبول وفقاً لنظام الإثبات هذا، إلا أن الواقع يثبت غير ذلك بحيث اعتمدت هذه الأنظمة حالات استثنائية؛ ومن بينها الإعتراف بالبيانات والمعلومات التي يتم الحصول عليها من الحاسوب كدليل إثبات جنائي[4].

---

1 بربارة عبد الرحمان, بربارة عبد الرحمان, شرح قانون الإجراءات المدنية والإدارية (قانون رقم 08-09 مؤرخ في 23 فيفري 2008), طبعة أولى, منشورات بغدادي, الجزائر, 2009, ص 107.

2 شيماء عطاالله، مرجع سابق، ص 387.

3 عمر أبو بكر يونس، مرجع سابق، ص 960.

4 أشرف عبد القادر قنديل، مرجع السابق، ص 201.

فنجد المشرع الإنجليزي قبل الدليل الإلكتروني في الإثبات الجنائي على أساس أنه استثناء من قاعدة شهادة السماع، وأما المشرع الأمريكي فلقد اعتبر من حيث الأصل أن شهادة السماع لا يعول عليها كدليل، ويرجع السبب إلى عدم الثقة في الشخص الذي يدلي بها مع وجود بعض الحالات التي يتحول فيها هذا النمط إلى وسيلة مقنعة، ومنها قبول البيانات والمعلومات الإلكترونية المستخرجة من الحاسوب, بحيث أنها تمثل تخزين لبيانات بشرية قد دونت بالكتابة على أنظمة معلوماتية وتم التعامل بها كوسيلة مادية لارتكاب الفعل المجرم[1].

وبهذا تخرج عن دائرة الشهادة السماعية لتأخذ قوة ثبوتية أكبر يمكن الاقتناع بها كدليل إثبات جنائي، وهو ما ثبت وفقاً لمحكمة الاستئناف في إنجلترا بالاعتراف بالدليل الإلكتروني في قضية R.V.Pettingreme التي تتلخص وقائعها في واقعة سرقة لأحد البنوك من قبل أحد الجناة، والذي اكتُشِفَ في حيازته لبعض أرقام النقود المسروقة المسجلة على حساب البنك في إنجلترا، حيث أخذت المحكمة بمخرجات الحاسب كأدلة إثبات جنائية تخرج عن قاعدة الشهادة السماعية[2].

البند الثالث: الدليل الإلكترونــي استثناءً من قاعدة الدليل الأفضل.

وفقاً لأنظمة الإثبات في الدول الأنجلوسكسونية المعتمدة لنظام الإثبات المقيد، نجد أن المشرع يقرر تقديم أفضل نموذج للإثبات فيما يتعلق المستندات المكتوبة فيجب أن تكون الأدلة المقدمة أولية وليست ثانوية أصلية لا بديلة، وقد قرر القانون الأمريكي هذه القاعدة بموجب المادة 1002 من قانون الإثبات الأمريكي والتي تقضي أن حجية الكتابة أو التسجيل أو الصورة رهن القبول بتقديم الأصل إلا إذا نص القانون على خلاف ذلك، ومع ظهور المستندات الإلكترونية استدعى الأمر إلى تغيير هذه القاعدة لكي تتلاءم مع عصر المعلومات، وقد استجابت بعض التشريعات كالقانون الأمريكي والإنجليزي لهذه المستجدات، بحيث قام المشرع الأمريكي باستخدام مدلول موسع للكتابة والتسجيلات ليشمل كل من الحروف والكلمات أو الأرقام أو ما يعادلها, مكتوبة وفقاً للشكل التقليدي أو منسوخة إلكترونياً، أو استخرجت على شكل صور مطبوعة، أو اتخذت شكل نبضات مغناطيسة أو تسجيل إلكتروني، أو أي شكل آخر من أشكال تجمع المعلومات، فيتم اعتبار الكتابة الموجودة داخل الجهاز في صورة إلكترونية من

1 رمزي رياض عوض، حماية المتهم في النظام الأنجلوسكسوني، د.ط ، دار النهضة العربية، القاهرة، سنة 2014، ص 34.

2 **نقلاً عــن:** علي محمود علي حمودة، مرجع السابق، ص 76.

قبيل النسخة الأصلية، وبالتالي لا نصطدم بقاعدة الدليل الأفضل، ويعتبر أن المحررات الإلكترونية نسخة أصلية[1].

الفرع الثانـــي: شروط قبول الدليل الإلكتروني أمام القاضي الجنائي.

إن سلطة القاضي الجنائي في قبول الدليل الإلكتروني ليست مجردة من كل قيد، وبهذا لجأت أغلب التشريعات المقارنة إلى رسم ضوابط وأطر معينة، يتعين أن تضع هذه السلطة في نطاقها بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من ورائها، وهو الوصول إلى الحقيقة الفعلية في القضية، وبهذا يتوقف قبول القاضي الجنائي للدليل الإلكتروني وتحقق حجيته في الإثبات بتوافر شروط محددة؛ وهي تحقق مشروعية الدليل الإلكتروني (البند الأول)، وضرورة مناقشة الدليل الإلكتروني (البند الثاني), وضرورة بلوغ الاقتناع القضائي درجة اليقين (البند الثالث).

البند الأول: مشروعية الدليل الإلكترونـــي.

تخضع قواعد الإثبات الجنائي لمبدأ المشروعية؛ والتي مؤداها التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام، وفي انعكاسها على شرعية الإثبات الجنائي في شتى مراحله، ويستلزم أن الدليل الإلكتروني بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية كالحاسوب مثلاً لا يتسم بصفة المشروعية، ومن ثم قبوله كدليل جنائي إلا إذا جرت عملية البحث عنه والحصول عليه، وإقامته أمام القضاء في إطار أحكام القانون واحترام قيم العدالة وأخلاقيتها التي يحرص على حمايتها[2].

ولقد تبنت الإتفاقيات الدولية والدساتير الوطنية والتشريعات الإجرائية المقارنة نصوصاً تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية، ومن ثم فإن مخالفة هذه النصوص في تحصيل الدليل الجنائي يَسِمُه بعدم المشروعية، ومن هنا فإنه لا يجوز للقاضي أن يقبل بدليل إلكتروني تم الحصول عليه من إجراء باطل كإجراء التفتيش خارج الشروط والأطر المحددة قانوناً، أو استخدام الإكراه المادي أو المعنوي أو الغش ضد الجاني في الجريمة المرتكبة من أجل فك شيفرة الخاصة بالدخول إلى النظام، أو التوصل إلى الأدلة المخزنة في الوسائل الإلكترونية[3].

1 شيماء عطاالله، مرجع السابق، ص 391.

2 هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص 104.

3 طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية المنعقد في الفترة بين 28-29-2009، أكاديمية الدراسات العليا، طرابلس، ليبيا، ص 23.

وتطبيقاً للمشروعية في الحصول على الدليل الإلكتروني نجد أن الفقه والقضاء الفرنسي قد ساندا هذا المبدأ باعترافهما بضرورة توافره في مراحل التنقيب، وكذا وجوب التزام القضاء قبل استخدام الوسائل العلمية الحديثة في عملية البحث والتحري عن الجرائم أن يتم الحصول على الأدلة الجنائية, ومن بينها الأدلة الإلكترونية على نحو مشروع ونزيه.

ويعتبر مبدأ مشروعية الحصول على الدليل الإلكتروني أحد المحاور الهامة التي تناولتها الاتفاقية الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات الشخصية، والمصادق عليها من طرف لجنة الوزراء التابعة للمجلس الأوروبي، والتي نصت على ضرورة استخراج البيانات المضبوطة بشكل صحيح وكامل ودقيق وتستمد بطرق مشروعة، كما لا يجوز استعمالها أو إفشاؤها في غير الأغراض المخصصة لها[1].

وبهذا نجد أن هذا المبدأ يكتسب أهمية كبرى نتيجة التقدم الهائل الذي تحقق في السنوات الأخيرة في شأن الوسائل الفنية للبحث والتحقيق، والتي تسمح اختراق مجال الحياة الخاصة للأفراد، وهو ما يثير إشكالين رئيسين في هذا الصدد؛ أولاهما ما مدى إمكانية قبول الدليل الإلكتروني غير المشروع لتحقيق المصلحة العامة على حساب المصلحة الخاصة للأفراد؟ وثانيهما مدى جواز قبول الدليل الإلكتروني غير المشروع في حالة البراءة على مستوى أنظمة الإثبات الجنائي؟

أولاً: مشكلة المصلحة الأولــى بالرعاية.

قد يأخذ الدليل الإلكتروني غير المشروع أثراً للتعدي على الحياة الخاصة، وفي نفس الوقت يعد وسيلة إثبات لجرائم تهدد الأمن ونظام المجتمع الأخلاقي، فيذهب البعض[2] إلى القول بعدم الاعتراف بقبول الدليل الإلكتروني غير المشروع بحجة الحفاظ على النظام العام للمجتمع, لا سيما في بعض الجرائم التي يمثل فيها تقديم هذا الدليل مساساً مباشراً بخصوصية الأفراد، إلا أن البعض الآخر[3] نادى بالإستعانة بمثل هذه الأدلة ولو فقدت مشروعيتها, إلا أنها تعتبر وسيلة إثبات على جرائم تستحق المكافحة والتصدي لها بكل السبل؛ نظراً لتحقيق الغاية في الحفاظ على المصلحة الخاصة للأفراد, خاصة إذا تعلق الأمر بالنظام الأخلاقي الإجتماعي، فلا يمكن استبعاد كل وسيلة لمجرد منافاتها للقواعد العامة دون الوقوف على آثارها العميقة على المجتمع.

1 **مشار إلى ذلك لدى:** علي حسن محمد الطوالبة، مرجع سابق، ص 189.

2 عائشة بن قارة مصطفى، مرجع سابق، ص 264.

3 طارق محمد الجملي، المرجع السابق، ص 25.

ونرى أن الرأي الأخير هو الأقرب إلى الصواب من الناحية المنطقية, ذلك أن الإنتقاص من تطبيق بعض القوانين والإبتعاد عن الإمتثال الأصم للأحكام القانونية، قد يجد مبرره في حالة تحقيق أهداف أسمى وأهم ترعى المصلحة العامة, ولو على حساب المصلحة الشخصية للأفراد.

ثانـــياً: موقف القاضي الجنائي من الدليل الإلكتروني غير المشروع.

إن الوقوف على قيمة الدليل الإلكتروني يأتي من خلال البحث في موقف القاضي من دليل الإدانة أو البراءة على مستوى أنظمة الإثبات الجنائي، وسنبين ذلك فيما يلي:

1. **بالنسبة لدليل الإدانة:**

انطلاقاً من قاعدة الأصل في المتهم هو البراءة، فيجب أن يتم التعامل مع هذا الأمر في كل مراحل الدعوى إلى حين صدور حكم نهائي، وهذا يستدعي أن تكون الأدلة مشروعة سواءً كانت أدلة تقليدية أو ناتجة عن الوسائل الإلكترونية، وترتيباً على ذلك فإن قبول القاضي بأي دليل غير مشروع يبنى عليه حكم إدانته يتم إبطاله، وهذا الحكم تبنته بعض التشريعات الموالية للنظام اللاتنيني كالمشرع المصري بمقتضى نص المادة 336 من قانون الإجراءات المصري[1]، وهو نفس موقف المشرع الجزائري كذلك من خلال نص المادة 191 من قانون الإجراءات الجزائية التي نصت على أن ينظر من قبل غرفة الاتهام في صحة الإجراءات المدفوعة إليها، وإذا اكتشفت سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية كلها أو بعضها[2].

وإذا كانت القاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراء وما يمليه من إجراءات لاحقة مباشرة، فإن هذه القاعدة تثير مسألة في غاية الأهمية تتعلق بماهية المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي, والأعمال التالية له حتى يمتد إليها البطلان.

إلا أنه بالرجوع إلى بعض مواقف التشريعات التابعة للنظام الأنجلوسكسوني نجد أن القانون الإنجليزي قد تبنى قاعدة عامة في نظام الإثبات؛ مدلولها متى كان الدليل منتجاً في الإثبات فهو مقبول أياً كانت الطريقة التي تم الحصول عليه من خلالها؛ أي حتى لو كان بطريقة غير مشروعة[3]، إلا أنه ظهر اتجاه آخر في

1 المادة 336 من قانون الإجراءات الجزائية المصري: "إذا تقرر بطلان أي إجراء فإنه يتناول جميع الآثار التي تترتب عليه مباشرة، ويلزم إعادته متى أمكن".

2 أيمن عبد الله فكري، مرجع سابق، ص 225.

3 عائشة بن قارة مصطفى، مرجع سابق، ص 207.

القضاء يخفف من صرامة وحدة مبدأ قبول الدليل أياً كانت طريقة تحصيله، وهو نفس الموقف الذي دعمه بعد ذلك صدور قانون الشرطة والإثبات الجنائي الإنجليزي حيث جاء ليعالج اختصاص الضبطية وقواعد الإثبات الجنائي على نحو يحقق ضمانات إجرائية هامة تحقق العدالة الإجتماعية, إذ نصت المادة 76 منه تنص على تنظيم قواعد استبعاد الاعتراف بالدليل غير المشروع، وذلك إما لاستعمال وسيلة قسرية ضد المتهم، أو أنه غير حقيقي أو تم الحصول عليه من شخص غير المتهم، أما المادة 78 من نفس القانون فإنها تمنح السلطة التقديرية للقضاء في استبعاد الدليل، حيث يجوز للمحكمة أن ترفض السماح بقبول الأدلة التي قدمها الإدعاء إذا تبين للمحكمة ذلك من خلال تقدير الظروف التي تم فيها تحصيل الدليل الجنائي.

2. **بالنسبة لدليل البراءة:**

لقد ثار خلاف فقهي انعكس على موقف التشريعات المقارنة فيما يخص مدى قبول الدليل غير المشروع في حالة إثبات براءة المتهم، وهذا الخلاف انقسم إلى ثلاث اتجاهات:

الإتجاه **الأول** يتمسك باعتبار المشروعية في تحصيل الدليل الجنائي أمراً لازماً في قبول الدليل سواء لإدانة المتهم أو برائته، وبهذا يبطل كل دليل جنائي تم الحصول عليه بطرق غير مشروعة كالتسجيل أو اللجوء إلى أسلوب المراقبة أو التسرب الإلكتروني دون الحصول على إذن من الهيئة المختصة, وتم الوصول إلى أدلة تقيد ببراءة المتهم، إلا أنه لا يمكن الاعتراف بها لعدم احترام الأطر والشروط القانونية التي تسمح بممارسة هذه الأساليب، وبالتالي يعتبر بطلان الدليل مستمد من مخالفة المشروعية المنصوص عليه سلفاً، كما أن قصر المشروعية على دليل الإدانة دون البراءة قد يخلق آثار سلبية على المجتمع, بحيث لا يصح إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أي تشريع جنائي[1].

أما الاتجاه **الثاني** فيرى أن اشتراط مبدأ مشروعية الدليل الإلكتروني يكون في حالة الإدانة لا البراءة، وبهذا يعتد بالأدلة غير المشروعة المحصل عليها في سبيل تحقيق براءة المتهم، لأن الأصل في الإنسان هو البراءة التي لا يحتاج لإثباتها، والمحكمة لا تحتاج إلى اليقين في إثبات البراءة بل يكفي لذلك الشك، وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع.

أما الاتجاه **الثالث** فيرى ضرورة التفرقة بين ما إذا كان نتيجة الحصول على الدليل غير المشروع تصنف كسلوك إجرامي يعاقب عليها جنائياً، وما إذا تم الحصول عليه وفق سلوك يشكل مخالفة لقواعد إجرائية فحسب، فإذا كان الاحتمال الأول فهنا وجب استبعاد الدليل غير المشروع وعدم الاعتداد به؛ لأن

1 محمد الأمين البشري، مرجع سابق، ص 244.

الأخذ به من قبيل الإعتراف باستثناء بعض الجرائم من العقاب والدعوى إلى ارتكابها, وهو ما لا يستقيم مع العدالة الجنائية[1].

وفي إطار الترجيح بين الاتجاهات السابقة، نتجه لتأيد الرأي الثاني منها الذي يقتصر في مشروعية الدليل الإلكتروني على دليل الإدانة لا البراءة, وهذا للمبررات التالية:

- أن القاعدة الأساسية في الإثبات تفيد بافتراض براءة المتهم حتى يثبت العكس، وبهذا فإن أي دليل يساعد على تحقيق هذه القاعدة وتأكيدها, يجب قبوله دون الإلتفات لأي اعتبار آخر.
- كما أن تطبيق هذا الرأي يحقق نتيجة هامة؛ هي حماية المتهم من احتمال إدانته وهو برئ، وهو أمر يستحق النظر إليه مقارنة مع إفلات المجرم من العقاب استناداً إلى دليل غير مشروع، وبالتالي فإن العدالة لا يضيرها إفلات المجرم من العقاب, بقدر ما يضيرها إدانة متهم برئ بحجة عدم مشروعية دليل البراءة.

البند الثانــي: وجوب مناقشة الدليل الإلكتروني من قبل القاضي الجنائي.

إن من أهم القيود الواردة على حرية قبول الدليل الإلكتروني من قبل القضاء الجنائي هو وضع الأدلة المستخلصة من مراحل البحث والتحري في موضع المناقشة وقت المحاكمة، وهو ما يؤدي معنى المواجهة والشفافية للخصوم في التعرف على الأدلة وتحضير الدفاع وفق الحالة التي يخدم فيها الدليل المتقاضي من عكسه. والأمر له انعكاس على تكوين اقتناع القاضي أيضاً بحيث لا يسوغ للقاضي أن يستند في حكمه إلى دليل ليس له أصل في أوراق الدعوى، ولم يعلن عنه في جلسة المحاكمة للمناقشة من قبل أطراف الدعوى وإبداء آرائهم فيه، وبالتالي يحصل اقتناع معين في شأن قيمة هذا الدليل[2].

وترتيباً على ذلك فإن جميع الأدلة الإلكترونية المتحصل عليها من إجراء التفتيش الإلكتروني وفي أي شكل كانت يستلزم أن تكون محل مناقشة أمام القاضي الجنائي، ولا يكفي النص عليه في ملف الدعوى، وهذا الحكم ينطبق على نتائج الخبرة والمعاينة الواقعة ضمن تحريات البحث في البيئة الإلكترونية, وكذا شهادة الشهود المعلوماتيين يجب إعادة سماعها في جلسة المحاكمة، ومناقشة تلك التقارير التي خلصت عنهم والمعلومات التي صدرت عنهم.

1 أيــمن عبد الله فكري، مرجع سابق، ص 252.

2 أشرف قنديل، المرجع السابق، ص 101.

وأهم النتائج التي تترتب على شرط مناقشة الدليل الإلكتروني هي عدم جواز حكم القاضي استناداً لمعلوماته الشخصية, أو بناء على معلومات مستمدة من الغير باستثناء الخبراء، وهذا الحظر يجد مبرره في التحصل على تلك المعلومات خارج الجلسة أو في غير نطاق المرافعات والمناقشات، ومن ثم يكون الاعتماد عليها مناقضاً لمبدأ الشفوية والمواجهة[1].

جدير بالذكر أنه يستثنى من مسألة القضاء بالمعلومات الشخصية الإستناد إلى المعلومات العامة التي يفترض في كل شخص الإلمام بها، أو استناد القاضي في حكمه إلى رأي يرجع إلى العلم أو يجري به العرف، والحكمة من استلزام وجوب تحرير محضر الجلسة حتى تكون الأدلة التي يستند إليها الحكم قائمة وثابتة بأوراق منعاً للتحكم وتحقيقاً للعدالة.

وبالرجوع إلى خصوصية الدليل الإلكتروني محل المناقشة تُـثار إشكالية مدى محافظة هذا الدليل على أصالته وتأثيرها على مبدأ قبوله من طرف القضاء، وهو ما قد ينتج عن التغييرات التي قد تطرأ على الدليل الإلكتروني في مرحلة البحث من تعرضه للتحريف أو الإلغاء, أو الحصول على مجرد نسخة منه يتم التحصيل عليها وفقاً لإجراء المراقبة الإلكترونية أو التسرب الإلكتروني مثلاً.

وهنا قد نجد أن بعض التشريعات ذهبت لافتراض أصالة الدليل الإلكتروني ومنها المشرع الأمريكي من خلال نص المادة (3/1003) من قانون الإثبات الأمريكي التي قررت أن صور البيانات المخزنة في الكمبيوتر, أو أي وسيلة إلكترونية تأخذ نفس الحجية لأصلها، ولعل الحكمة من افتراض أصالة الدليل الإلكتروني راجعة إلى الطبيعة التقنية لهذا الدليل التي لا تعبر عن قيمته الأصلية بمجرد تحصيله من النظام المعلوماتي، وإنما تبقى من خلال الحصول عليه من أي وسيلة أو مكان آخر[2].

المطلب الثانــي: سلطة القاضي الجنائي في تقدير الدليل الإلكترونــي.

تعتبر مسألة تقدير القاضي الجنائي للدليل الإلكتروني من المسائل المهمة في مجال الإثبات على اعتبار أن أهم المشاكل التي تطرح في إثبات الجرائم الواقعة عبر التعامل الإلكتروني هو ما يقع على القاضي في تقدير الأدلة الإلكترونية ومدى الاقتناع بها، نظراً لأن السلطة التقديرية للقاضي لهذا النوع من الأدلة يثير إشكالاً كبيراً نظراً لتصنيفها كنوع من أنواع الأدلة العلمية التي تعتمد على وسائل تقنية من أجل الوصول إلى

1 نبيلة هروال، المرجع السابق، ص 166.

2 محمد بوبكر بن يونس، المرجع السابق، ص 973.

الحقيقة، أضف إلى ذلك ضرورة توافر شروط معينة في الأدلة الإلكترونية مع بلوغ القاضي إلى درجة الاقتناع اليقيني بهذه الأخيرة، وهو ما استوجب بيانه في النقاط التالية:

الفرع الأول: حرية القاضي الجنائي في تقدير الدليل الإلكترونـــي.

يعتبر تنامي دور الإثبات العلمي مع بروز الدليل الإلكتروني المستحدث في إطار الجرائم الواقعة عبر التعامل الإلكتروني هو عامل هام في مجال الإثبات الجنائي، يستدعي ضرورة تعامل القاضي معه بشكل مخالف عن الأدلة التقليدية، وخاصة مع نقص الثقافة المعلوماتية وتعقد طبيعة الأدلة الإلكترونية وسبل استخدامها في مجال الإجرام الإلكتروني.

وإن كانت العملية القضائية التي يجريها القاضي الجنائي هدفها النهائي هو التوصل إلى الحقيقة الواقعية أي الوقوف على الحقائق كما حدثت، ففي حالة توصل القاضي إلى حالة ذهنية استجمع فيها كافة عناصر الحقيقة وارتاح إليها ضميره، فهنا يمكن القول أن القاضي قد وصل إلى حالة الاقتناع القضائي. ففيما تتمثل ماهية الاقتناع القضائي بالدليل الجنائي الإلكتروني, وما تأثير طبيعة الدليل الإلكتروني على اقتناع القاضي الجنائي؟

البـــند الأول: مفهوم مبدأ الاقتناع القضائـــي.

عرف بعض الفقه[1] الاقتناع القضائي بأنه حالة ذهنية وجدانية يصل إليها القاضي الجنائي وهي عبارة عن محصلة منطقية يستنتجها من وقائع القضية، فأهم مبادئ الإثبات الجنائي مبدأ الاقتناع القضائي والذي يجعل القاضي يقبل جميع الأدلة التي يقدمها إليه أطراف الدعوى مادامت تعدت مرحلة القبول؛ أي امتثالها للشروط المحددة مسبقاً في التشريع، ولها بعد ذلك أن تخضع لمرحلة السلطة التقديرية الكاملة وذلك بوزن قيمة كل دليل على حدى، وفي النهاية سلطة التنسيق بين الأدلة التي قدمت إليه واستخلاص نتيجة منطقية من الأدلة مجتمعة ومتساندة تتمثل في تقدير البراءة أو الإدانة[2].

وذهب البعض الآخر من الفقه[3] إلى تعريف الاقتناع القضائي بأنه حالة ذهنية يتوصل لها القاضي في حالة توافر مجموعة من الأدلة الوضعية ما يكفي لتسبيب تسليمه بالوقائع، ولقد أقرت معظم التشريعات بهذا المبدأ، حيث أخذ به المشرع الفرنسي في قانون الإجراءات الجزائية في المادة 303 التي نصت بأنه:"لا

1 أيمن عبد الله فكري، المرجع السابق، ص 230.

2 محمود إبراهيم غازي، المرجع السابق، ص 644.

3 محمد الأمين البشري، مرجع سابق، ص 250.

يطلب القانون من القضاة حساباً بالأدلة التي اقتنعوا بها، ولا يفرض قاعدة خاصة تتعلق بتمام وكفاية دليل ما، وإنما يفرض عليه أن يتساءلوا في صمت وتدبر، وأن يبحثوا في صدق ضمائرهم أي تأثير قد أحدثته الأدلة الراجحة ضد المتهم ووسائل دفاعه"[1].

أما المشرع الجزائري فلقد كرس المبدأ في قانون الإجراءات الجزائية بحيث نص أنه يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك, وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص..."[2].

وورد ذات المبدأ في نص المادة 1/302 من قانون الإجراءات الجزائية المصري التي نصت على أنه:"يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته".

كما أنه يتحدد مجال تطبيق مبدأ الاقتناع القضائي إما وفق طبيعة القضاء أو من حيث مراحل الدعوى الجنائية، بحيث أنه يمتد تطبيق مبدأ الاقتناع القضائي إلى كل أنواع المحاكم الجنائية سواء كانت محاكم الجنايات أو الجنح أو المخالفات، وهو ما صرح به المشرع الفرنسي من خلال نص المادة 353 من قانون الإجراءات الجزائية التي تنص على تطبيق المبدأ أمام محاكم الجنايات، وأما نص المادة 427 من ذات القانون فتنص على تطبيق هذا المبدأ أمام محكمة الجنح ، أما المادة 536 فهي مخصصة لمحاكم المخالفات.

بينما نجد أن المشرع الجزائري والمصري لم يحددا ذلك صراحة، ومع ذلك فإن عدم النص على تطبيق المبدأ لا يعني الإغفال بالعمل, وخاصة بالنسبة للتشريعات التي تعتنق المذهب الحر في الإثبات الجنائي.

وإن كان اعتبار تطبيق مبدأ الاقتناع القضائي هو مخصص لمرحلة الحكم، إلا أن ذلك لا يعني اقتصاره على تلك المرحلة، بل قد يمتد ليشمل مرحلة التحقيق الابتدائي أمام قضاة التحقيق الذين يقدرون مدى كفاية الأدلة من عدمها دون الخضوع لرقابة محكمة النقض وإنما للاقتناع الشخصي فحسب.

البــند الثانـــي: تأثير طبيعة الدليل الإلكتروني على مسألة الاقتناع القضائي.

إذا كان العلم قد استحدث الكثير من أساليب الإثبات وأمدت سلطات التحقيق بوسائل متطورة، إلا أن اقتناع القاضي الجنائي يأتي على قمة هذه الوسائل، لا كوسيلة من وسائل الإثبات, ولكن كمبدأ يحمي العدالة من سوء استخدام الوسائل العلمية الحديثة، بحيث أن طبيعة الأدلة الإلكترونية التي تجعلها أدلة مستمرة في التطور ومتعددة في التركيب، وتقوم في الأغلب على خاصية علمية تجعلها تكتسب من الدقة

1 المادة 303 من قانون الإجراءات الجزائية الفرنسي

2 المادة 212 من قانون الإجراءات الجزائية الجزائري.

والنتائج المحددة إلى نسبة كبيرة، كل هذا له تأثير مباشر قوي على اقتناع القاضي يتجاوز في تأثيره كل أنواع وسائل الإثبات الأخرى، بحيث تجعله أكثر جزماً ويقيناً، كما تقلل من نسبة الأخطاء القضائية والاقتراب من العدالة بخطوات أوسع, والتوصل إلى درجة أكبر نحو الحقيقة[1].

وإن كانت الأدلة الإلكترونية تخضع إلى تقدير القاضي الجنائي وبالتالي اقتناعه، إلا أن هذا الأمر يكون في إطار خطين متوازيين؛ الأول يتعلق بالقيمة العلمية القاطعة للدليل، والثاني للظروف والملابسات التي وجد فيها الدليل, فتقدير القاضي لا يتناول الأمر الأول؛ وذلك لأن قيمة الدليل تقوم على أسس علمية كما ذكر سابقاً، وبالتالي لا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، ذلك أن مجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم مباشرة سواء بالإدانة أم البراءة دون بحث الظروف والملابسات، فالدليل الإلكتروني ليس آلية معدة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة، وبهذا يبقى للقاضي دور إيجابي في حرية تقدير الدليل الإلكتروني والاقتناع به من عدمه دون أي تأثير صادر من طبيعته، أو من قبل تقارير الخبرة التي تساعد على ثبوتيته وتأكيده[2].

الفرع الثانـــي: بلوغ القاضي درجة الاقتناع اليقيني بالدليل الإلكترونـــي.

إن الحكم الصادر من القاضي الجنائي يبنى على اقتناع القاضي اليقيني بالأدلة الإلكترونية المستخرجة من النظام المعلوماتي أو شبكة الانترنت، وبهذا يتجنب حكم الإدانة أو البراءة بناءً على الشك, فلا مجال لدحض قرينة البراءة أو افتراض عكسها إلا في حالة الجزم واليقين[3]، وعليه إذا كانت الأدلة الإلكترونية التي ساقها القاضي في حكمه قد انتهت به إلى ترجيح وقوع الجريمة من المتهم ، فإن هذا الحكم يوصم بمخالفته للقانون على حسب أن أي شك يتطرق إلى اقتناع القاضي في ثبوت التهمة يجب على المحكمة أن تقضي بالبراءة مهما كان احتمال الثبوت ودرجته، وهو ما يمكن التوصل إليه من خلال ما يعرض من الأدلة الإلكترونية على اختلاف صورها, وتنوع وسائل الحصول عليها، فيأخذ القاضي دور الممحص في الأدلة تمحيصاً حسياً وعقلياً يجعله يشيد قناعته اليقينية بالدليل، مستبعداً ما قد ينطبع في تصوره الذهني من احتمالات أو استضعاف للقوة الثبوتية لأي دليل, مما يؤثر على حقيقة نسبة الجريمة إلى المتهم من عدمه.

1 أشرف عبد القادر قنديل، المرجع السابق، 231.

2 شيماء عبد الغني عطاالله، المرجع السابق، ص 523.

3 علي حسن محمد الطوالبة، المرجع السابق، ص 190.

ومما يساعد بلا شك من تحقق الإقتناع اليقيني للقاضي الجنائي هو خضوع تلك الأدلة للتقسيم الفني بوسائل علمية تمكن من فحصها للتأكد من سلامتها، وكذا صحة الإجراءات المتبعة في تحصيل الدليل الإلكتروني لتجنب الأخطاء التي قد تنال من أصالتها أو قوتها الثبوتية. ويذهب الرأي السائد في الفقه الكندي إلى اعتبار أن مخرجات الحاسب الآلي تحقق اليقين في الأحكام الجنائية، وقد نص التشريع الأمريكي من خلال قانون الإثبات الأمريكي على اعتبار أن نسخ المخرجات الإلكترونية من بيانات ومعلومات من أفضل الأدلة المتاحة للإثبات الجنائي التي تحقق مبدأ اليقين لهذه الأدلة[1].

1 هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 91.

الـــخاتـــمة

الخاتمـــــة:

احتلت التعاملات الإلكترونية الجانب الهام من الحياة اليومية؛ نظراً لارتباطها بعاملي السرعة والسهولة في الإنجاز، وهذا بفضل تطور المجال التكنولوجي والرقمي وشموله لجميع المستويات. ومن خلال الدراسة المعمقة لفصول الحماية الجزائية للمعاملات الإلكترونية, يتضح لنا بالرغم من تنامي هذه التقنية إلا أنه لا يمكن أن نحصر الفائدة المرجوة من هذا النمط من التعاملات, ما لم يقترن بضوابط قانونية تقيم نظام حمائي جزائي ضد المخاطر التي تمس بسلامة وأمن وسرية المعاملات الإلكترونية, ومن ثم تحقيق الثقة في هذه المعاملات من جهة, وتحقيق الاستقرار في هذا النمط من جهة أخرى.

وبهذا لا يتأتى مفهوم الضابط القانوني للحماية الجزائية للمعاملات الإلكترونية إلا باتخاذ جميع السبل الممكنة من قبل التشريعات الجزائية المقارنة في سن تشريعات عقابية, تلبي الحاجة في منع الاعتداء الواقع من قبل الجناة إما ضد الجرائم التقليدية المصاغة في البيئة الإلكترونية, وهذا بتطويعها بأحكام تضمن التصدي لتلك المخاطر، أو باستحداث أحكام تشريعية جديدة تتماشى وطبيعة وخصوصية المعاملات وتتوازى مع تحقيق العقاب الأمثل للجرم المستحدث، كما يجب استكمال هذه الأحكام الموضوعية بأحكام إجرائية على المجال التطبيقي بداية من الهيئات المختصة في مواجهة هذه الجرائم، وكذا سبل الأخذ بالجوانب الإجرائية في مجال التحقيق والتحري وصولاً إلى مرحلة المحاكمة، وضمان وضع أحكام خاصة بالاختصاص القضائي الأمثل لمواجهتها, مع الأخذ بضرورة تنظيم مسألة تقدير الدليل الإلكتروني وتحقيق الجدوى من الاعتراف به كآلية لكشف الجرائم الماسة بالمعاملات الإلكترونية.

لذلك, وبناء على ما تمت دراسته في هذا الموضوع, يمكن طرح النتائج والملاحظات التالية:

- يبدو من خلال الطرح التشريعي أن أهم الإشكالات المتعلقة بحماية المعاملات الإلكترونية في إطار الجرائم التقليدية, تتمحور حول قصور التشريعات المقارنة عن إيجاد معنى واضح للمال المعلوماتي وإدراجه ضمن الأنظمة القانونية، بما يساعد على وضع أحكام جزائية صارمة ضد جرائم السرقة والاحتيال والتزوير الإلكترونية، وهذا ما جعل الحكم التقليدي لمواجهة تلك الجرائم عاجزاً عن سد الطريق على الاعتداءات المختلفة الواقعة على أشكال المعاملات المالية الإلكترونية, خاصة وأن ما يعزز صعوبة إيجاد حلول لهذه الجرائم هو الاختلاف بين شكل الجرائم التقليدية والمستحدثة، والتي تعتمد بشكل كبير على مهارة المجرم الإلكتروني وخبراته في استخدام الأجهزة الحديثة، وكذا وسائل الإثبات التي تتمثل في الأدلة المتحصلة من الأجهزة المستخدمة.

- كما تم التوصل إلى أن اتجاه أحكام القضاء في القانون المقارن قد سعت إلى الخروج من إشكالية الاعتراف بالطبيعة المعنوية للمال المعلوماتي, ومن ثم انتاج أحكام عديدة مساعدة على إيجاد عقوبات ضد الممارسات غير الشرعية في المعاملات الإلكترونية؛ وعلى رأسها الاعتراف بتوافر بفكرة الاختلاس في جريمة سرقة المعلومات, وكذا جرائم النصب وخيانة الأمانة, وهو ما جسده من خلال القانون رقم 2014-1353 المعدل لقانون العقوبات الفرنسي.
- كما أن الاختلاف الفقهي حول إمكانية تطويع النصوص التقليدية لتشمل الجرائم الحديثة, ترتب عنه اتجاه المحاكم القضائية في القانون المقارن إلى الاعتراف بوقوع جرائم السرقة والنصب وخيانة الأمانة باستعمال الوسائل الإلكترونية المساعدة على نقل المال من يد صاحبه إلى الجاني بسهولة وسرعة، الأمر الذي دفع أيضاً التشريعات المقارنة إصدار أحكام مباشرة في النص على أساليب النشاط الإجرامي وتوقيع الجزاء المناسب، في حين أنه يوجد بعض التشريعات الرافضة لبسط الحكم التقليدي على الجرائم المستحدثة, مما يبقي نشاط تلك الجرائم مباحاً من الناحية القانونية محتجة بمبدأ الشرعية الجنائية.
- كما يتبين أن حظر جريمتي الدخول أو البقاء غير المشروع داخل النظام المعلوماتي, بمثابة الاعتراف المباشر من المشرع الجنائي بالحد من أساليب اعتدائية تحقق انتهاك لحرمة النظام المعلوماتي بالاطلاع أو الإلتقاط غير المشروعين على المعلومات الخاصة بالمعاملات الإلكترونية لتلك البيانات أثناء انتقالها، أو البقاء داخل الأنظمة بشكل يتعارض مع علم أو إرادة صاحبها، مما يؤثر على مسألة الخصوصية وسرية المعلومات, وقد كان ذلك موقف جل التشريعات في النظام اللاتيني والأنجلوسكسوني وحتى العربية،كما أن الحماية الجنائية للنظم المعلوماتية تحقق بشكل ضمني حماية لمواقع التعاملات الإلكترونية، الأمر الذي تبنته أغلب التشريعات المقارنة, محاولة منها إدراج الحماية للمعلومة الإلكترونية والنظام المعلوماتي, أو الموقع الحامل لها في آن واحد.
- تعد حماية البيانات الشخصية التي تضمنها التشريع الجزائري في القواعد العامة غير كافية لحماية البيانات الشخصية المخزنة في بنوك المعلومات وقواعد البيانات المنتشرة عبر الانترنت، وذلك إعمالاً للقاعدة التي تقضي بعدم جواز القياس في التجريم، ولعل المشرع قد تدارك الأمر بإصدار القانون 18-07 الخاص بحماية البيانات المعالجة آليا ذات طابع شخصي, والتي حاول من خلالها بلورة أحكام جنائية ضد الأفعال الماسة بسرية وسلامة البيانات الشخصية الإلكترونية, ورصد هيئات وآليات لحمايتها من الجانب الموضوعي والإجرائي.

- كما يتضح سير التشريعات في مجال ترسيخ حماية المعاملات الإلكترونية من خلال آلية التوقيع الإلكتروني التي تبنتها في الأغلب من خلال قوانين خاصة, وهو نفس الموقف الذي تبناه المشرع الجزائري من خلال إصدار القانون 15-04 الذي بالرغم من أنه جاء متأخراً مقارنة مع اعتراف المشرع بحجية التوقيع الإلكتروني والكتابة الإلكترونية، إلا أنها كانت خطوة موفقة حملت معها العديد من الأحكام المنظمة لنظام التوقيع الإلكتروني ووسائل الحماية الجنائية المتعلقة به، بحيث تدارك من خلاله الفراغ التشريعي الذي كان سائداً قبل إصدار هذا القانون, خاصة فيما يتعلق بإسباغ الحجية القانونية الكاملة للتوقيع الإلكتروني أمام القضاء، وتنظيم الجوانب المتعلقة بالتصديق الإلكتروني, وأطر حمايتهما من بعض المخاطر المحتملة الوقوع في إطار التعامل الإلكتروني، إلا أنه يؤخذ على المشرع إغفاله لتنظيم بعض الجرائم التي تمس بآلية التوقيع الإلكتروني كجريمة التزوير والدخول والبقاء غير المشروع لنظام التوقيع الإلكتروني, وكذا جريمة تجريم أفعال الشروع أو التحضير في ارتكاب الجرائم المنصوص عليها, والتي تعد حماية وقائية ضد تلك الجرائم، وهذا ما يترجم عدم كفاية وفعالية وسائل الحماية الجنائية المقررة في القانون رقم 15-04, خاصة في ظل حصرها لجرائم الاعتداء على منظومة التوقيع الإلكتروني في أفعال مؤدي وطالب خدمات التصديق الإلكتروني, متغافلاً عن أعمال إجرامية تقع من القراصنة أو الجناة من غير أطراف المعاملات الإلكترونية.
- كما يتضح أن تقرير الحماية الجزائية لوسائل الدفع الإلكتروني تستمد خصوصيتها من خلال اعتبارها كآلية مستحدثة لقيام المعاملات المالية الإلكترونية, وكذا من خلال تصنيف الجرائم المتعلقة بها في خانة الجرائم الماسة بأنظمة المعالجة الآلية للنظام المعلوماتي، مما يوجب مواجهة التشريع لها بأنظمة قانونية خاصة دون الاعتماد على الأحكام التقليدية في ذلك، وبالرغم من محاولة التشريع الجزائري لمواكبة التشريعات المقارنة في إيجاد أحكام تنظم هذه الوسائل, إلا أنه يتضح عليه القصور في تنظيم أحكام جزائية رادعة بخصوص بعض الاعتداءات الماسة ببطاقات الدفع الإلكتروني المستعملة من قبل الحامل أو الغير.
- ويتبين أن موقف التشريع الجزائري الإجرائي في مجال حماية المعاملات الإلكترونية قد حمل جملة من النقائص منها؛ قصور المشرع الجزائري من حيث عدم تضمينه الاستثناء الخاص بوقت التفتيش والأشخاص المطلوب حضورهم ضمن القانون 09-04، وعدم نصه على صدور إذن بالتفتيش مقتصراً على تفتيش الحاسوب، فإذا كان هذا الأخير متواجداً في مسكن يتعين توافر شروط تفتيش المساكن،

وإذا تواجد الحاسوب في حيازة الجاني فيكفي توافر شروط تفتيش الأشخاص, وهي الحالة التي نص عليها المشرع فقط في حالة التلبس بجناية أو جنحة.

- كما أن توجه التشريعات الإجرائية المقارنة إلى محاولة لتحديث الإجراءات التقليدية بما يتماشى وجرائم المعاملات الإلكترونية يبقى ناقصاً أمام إيجاد حلول مستحدثة تنبع من أصل الإشكال، وتحمل طبيعته لتكون له المواجهة الأكثر فعالية, وهو ما ترجمه استحداث أسلوب المراقبة الإلكترونية والتسرب الإلكتروني, اللذان يحققان أهداف كبيرة في البحث والتقصي والكشف عن الجريمة، وهو ما أدى إلى اتجاه العديد من المؤسسات الضبطية دولياً إلى استخدامه، وذلك عن طريق تجنيد عناصرها للدخول إلى العالم الافتراضي, والتعامل مع الأسلوب الإجرامي بشكل تقني واحترافي, مما يحقق نتائج هامة في الحد من الجريمة وإلقاء القبض على الجناة.
- ويتبين أن مسألة تقدير قيمة الدليل الإلكتروني من قبل القاضي الجنائي تتوقف على أمرين؛ الأول يتعلق بالقيمة العلمية للدليل, والثاني على الظروف والملابسات التي تحيط بالدليل، فالقاضي ليس له أن ينازع فيما أسفرت عليه التكنولوجيا التقنية والعلمية، وهذا الأمر يوجب الإبقاء على سلطة القاضي الجنائي التقديرية في تقديره للأدلة الإلكترونية, وهذا لضرورة حتمية تضمن تنقية الأدلة من الأخطاء، وجعل الحقيقة العلمية حقيقة قضائية، ويبقي للقاضي سلطته في تحديد الحقيقة واستبعاد الأدلة الإلكترونية غير المشروعة.
- كما أن التوسع في الاختصاص الإقليمي في متابعة الجرائم المتعلقة بالتكنولوجيا من طرف التشريع الجزائري من المسائل التي تحسب له؛ نظراً لما يمكن استغلال هذه التكنولوجيا ضد مصالح الأفراد أو المصالح الاستراتيجة للاقتصاد الوطني وخاصة شبكة الانترنت، وما يتبعها من حذف للحدود الإقليمية, مما يؤدي إلى امتداد تلك الجرائم عبر عدة أقاليم، وينشأ التنازع في الاختصاص القضائي لها، كما تُظهِر الحقيقة العملية أن الضوابط والمعايير التقليدية سواء كانت الشخصية منها أو الموضوعية للاختصاص القضائي التقليدي عاجزة عن فض المنازعات القانونية للاختصاص القضائي في المعاملات الإلكترونية؛ لاختلاف وطبيعة وسط كل منهما، وهذا ما يرجح مبدأ العالمية كالمعيار الأنسب والأمثل في حل النزاع؛ نظراً لأنه يضمن متابعة ومحاكمة الجناة في أي وضع كان, بغض النظر عن إقليم أو مكان ارتكاب الجريمة أو جنسية الجناة.

واتساقاً مع ما تم التوصل إليه من نتائج وملاحظات في هذه الدراسة فإننا نختتمها بجملة من التوصيات المتمثلة في:

- نهيب بالتشريعات المقارنة ضرورة الفصل بين جريمة التزوير الواقعة على المحرر الإلكتروني, وبعض الجرائم التي قد تتصل بها الدخول غير المشروع لنظام المعالجة الآلية, وجريمة تعطيل النظام على اعتبار أن الركن المادي لجريمة الاعتداء العمدي على المعطيات يقوم على أفعال الإتلاف أو المحو أو التعديل, وهي نفس الأفعال التي قد تكون النشاط المادي لجريمة تزوير المحرر الإلكتروني, مما يلقي على القاضي الجنائي عبء الفصل والتمييز بينها.
- لزوم توفير أساس قانوني يكفل الحماية اللازمة لمنع وقوع الاعتداء على بطاقات الدفع الإلكتروني لتأثيرها الواضح في الإخلال بالنظام الاقتصادي بشكل عام, والنظام المصرفي بشكل خاص, عن طريق وضع نظام قانوني محكم يجرم كل أشكال الاعتداء على بطقات الدفع الإلكتروني, ويحدد الأفعال التي تضعف من ثقة الأفراد في التعامل بها, سواء كان ذلك الفعل تزويراً أو سرقة أو احتيال أو إساءة استخدام، مع الحاجة لبيان المقصود بكل نوع على حدى من الجانب الإصطلاحي عن طريق تفصيلها من الناحية التشريعية والفقهية لضمان حماية جزائية كافية لكل تلك الأنواع.
- نوصي بتكاملية الحلول القانونية؛ وذلك بتوفير أدوات حماية تقنية تضطلع بتقليص عملية جمع البيانات الشخصية التي تجري دون علم المستخدم, وهو البعد التقني للحماية، فضلاً عن توفير البناء القانوني الملائم لتنظيم مسائل الحماية وتوفير استراتيجيات التعامل مع انتهاكات البيانات الشخصية انطلاقاً من الوعي بمخاطر الاعتداء عليها, والوعي بوسائل تقليلها ومنع حصولها وهو البعد التوعوي للحماية.
- نأمل تدارك المشرع الجزائري للنقص التشريعي الوارد بالقانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين للإحاطة بجملة الجرائم الواقعة عى التوقيع الإلكتروني، والتي تشكل تهديداً كبيراً ومباشراً كجريمة تزوير وإتلاف التوقيع الإلكتروني, والدخول والبقاء غير المشروع داخل نظام التوقيع الإلكتروني.
- ضرورة مراعاة مستخدمي شبكة الانترنت للقواعد الأمنية الواجب تطبيقها, ومنها عدم استخدام البريد الإلكتروني في استقبال أو إرسال أية بيانات مالية هامة قد تعرضها للسرقة, أو تصفح أي مواقع مشبوهة.

- ضرورة إيجاد آليات قانونية تضمن تفعيل التنسيق بين الجانب القانوني والجانب التقني في مجال المعاملات الإلكترونية بغرض ترقية عناصر الأمان والسرية، وبث ثقة أكبر في هذا النوع من التعاملات.
- الدعوة إلى إقامة تعاون كامل بين رجال الضبط القضائي وقضاة التحقيق والخبراء من أجل نجاح عملية ضبط الجريمة وتجميع الأدلة وتحليلها وتقديمها في شكل ينفي أو يثبت إدانة المتهم, ويؤدي إلى اقتناع القاضي بالحكم، على اعتبار أن الإثبات الجنائي في الجرائم الواقعة على المعاملات الإلكترونية تتطلب إلمام رجال الضبط القضائي بالتدابير والإجراءات اللازمة لتأمين مسرح الجريمة، وضبط وتحرير الآثار الجنائية الرقمية ونقلها بالطريقة السليمة.
- نوصي المشرع الجزائري بالنظر بشأن إجراء حفظ المعطيات، وذلك بتحديد الجهة المكلفة بمنح هذا التسخير بشكل أدق، وتحديد مدة الحفظ لها وعدم تركها مفتوحة، وهذا كله في إطار ضمان ضوابط قانونية تحد من التجاوزات التي يمكن لأعوان الضبط القضائي ممارستها في حالة التحريات، وكذا ضمان تعجيل إجراءات المتابعة الجزائية في حالة تحديد المدة القانونية لحفظ المعطيات, وهو ما يجب على المشرع تداركه في هذا الصدد.
- ضرورة توحيد القوانين على المستوى الدولي كما هو معمول به في الاتحاد الأوروبي أو تكتلات دولية أخرى, بالإضافة إلى تكثيف الاتفاقيات الدولية مع دول أجنبية بما فيها المجاورة للجمهورية الجزائرية بهدف تعزيز التعاون والشراكة في المبدأ القضائي، وتسهيل مهمة تسليم مرتكبي الجرائم ومتابعتهم قضائياً.
- الدعوة إلى اعتماد قواعد وحلول تنظيمية مشتركة بين الدول العربية للمسائل والإشكاليات المطروحة، وذلك لمواجهة التحالفات العالمية الكبرى من ناحية، ولسهولة التواصل ووحدة المفاهيم بين الدول العربية، وبهذا تظهر ضرورة التعاون العربي في مجال تبادل الخبرات، وتأهيل وتدريب العاملين في الجهات المختصة للتصدي للجرائم الناشئة عن المعاملات الإلكترونية.
- إن مسألة الوعي والثقافة المطلوبة لدى المتعاملين الإلكترونيين تبقى من أهم آليات الوقاية ضد الجرائم التي تنال من أمن وسلامة التعامل الإلكتروني، وهذا بتحاشي نشر البيانات الخاصة على مواقع الانترنت أو التعامل عبر البريد الإلكتروني, وغيرها من أدوات التواصل الإلكتروني, دون أخذ الحذر من تصيد قراصنة الانترنت ومجرمي المعلوماتية لها, واستغلالها بشكل يضر مستخدميها.

- إن تضاعف الضرورة لإصدار نظام جزائي حمائي خاص بالمعاملات الإلكترونية في الجزائر أضحى أمراً مهماً يُـلقى على عاتق المشرع لمواكبة ذلك الزخم من المخاطر والاعتداءات المتلاحقة لمجال المعاملات الإلكترونية، بالرغم من تثميننا إصدار التشريع 18-05 المتعلق بالتجارة الإلكترونية, ولو أنه جاء متأخراً مقارنة بالتشريعات العربية المقارنة, إلا أنه يعتبر خطوة إيجابية سعى المشرع من خلالها إلى سد جانب من الحماية الجنائية لأحد أنواع المعاملات الإلكترونية، بالرغم من الحاجة إلى إصدار تشريع شامل وضمان القدر الكافي من المرونة في هذا التشريع بما يسمح بمواجهة المستجدات المتعلقة بشتى جوانب التعامل الإلكتروني، والابتعاد عن الإتكال التشريعي في إطار القواعد العامة التقليدية التي لا توفر الوجه الحقيقي للحماية الجزائية في هذا النوع من المعاملات الحديثة.

قائمة المراجع

قائمة المراجـــــع:

أولاً: الكتب والمؤلفات.

أ) الكتب العامـــــة:

1. أحمد شوقي الشلفاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999.
2. أسامة قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دراسة مقارنة في القانون الفرنسي والأمريكي وفقا لآخر التعديلات التشريعية، دار النهضة العربية، مصر، 2008.
3. بربارة عبد الرحمان, بربارة عبد الرحمان, شرح قانون الإجراءات المدنية والإدارية (قانون رقم 08-09 مؤرخ في 23 فيفري 2008), طبعة أولى, منشورات بغدادي, الجزائر, 2009.
4. ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1983.
5. محمد زكي أبو عامر، الاجراءات الجنائية، دار الجامعة الجديدة، الاسكندرية، ط7، 2002.
6. محمود محمود مصطفى، شرح قانون العقوبات (القسم الخاص)، دار النهضة العربية، مصر، 1984.
7. سميحة القليوبي، الأسس القانونية لعمليات البنوك، دار النهضة العربية، القاهرة، الطبعة الثانية، 2003.
8. نبيل صقر, نبيل صقر, الوسيط في شرح قانون الإجراءات المدنية والإدارية (الخصومة, التنفيذ, التحكيم), دار الهدى, عين مليلة, الجزائر, 2008.
9. عدنان الخطيب، موجز القانون الجزائي (الكتاب الأول)، مطبعة جامعة دمشق، 1963.
10. رمزي رياض عوض، حماية المتهم في النظام الأنجلوسكسوني، د.ط ، دار النهضة العربية، القاهرة، 2014.
11. غنام محمد غنام، شرح قانون العقوبات (القسم الخاص)، جامعة المنصورة، مصر، 2004.

ب) الكتب الخاصة:

12. أحمد حسام طه تمام، الجرائم الناشة عن استخدام الحاسوب، رسالة طنطا، 2001.
13. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، الطبعة 2، 2006.

14. أحمد سفر، أنظمة الدفع الإلكترونية، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، 2008.

15. أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني (دراسة مقارنة)، دار النهضة العربية، الطبعة 1، القاهرة، 2006.

16. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الاسكندرية، 2015.

17. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة الجزائر، 2007.

18. أمير فرج يوسف، عالمية التجارة الإلكترونية وعقودها وأساليب مكافحة الغش الإلكتروني، المكتب الجامعي الحديث، الاسكندرية، بدون طبعة، 2009.

19. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007.

20. جلال الزعبي, وأسامة المناعة, وصايل الهواوشة، جرائم الحاسوب والانترنت، دار وائل، عمان, 2001.

21. جليل الساعدي، مشكلات التعاقد عبر الانترنت، مكتبة السنهوري للنشر والتوزيع، بغداد، 2011.

22. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي في التكنولوجيا الحديثة، دار النهضة العربية، 2002.

23. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002.

24. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة (دراسة تطبيقية في القضاء الفرنسي والمصري)، دار النهضة العربية، مصر, 2010.

25. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة،دار النهضة العربية، الطبعة1، 1992.

26. هبة حسين زايد، الحماية الجنائية للصفقات الالكترونية، دار الكتب القانونية، مصر، الإمارات، 2016.

27. هدى حامد قشقوش،الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000.

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

29. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة)، مكتبة الآلات الحديثة، مصر، 1994.

30. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، أسيوط، 2000.

31. هلالي عبد اللاه أحمد، تفتيش نظم الحاسوب وضمانات المتهم المعلوماتي، دار النهضة العربية، مصر، 1997.

32. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، مصر، 1999.

33. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006.

34. هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006.

35. هلالي عبد اللاه أحمد، جرائم المعلوماتية العابرة للحدود (أساليب المواجهة وفقا لاتفاقية بودابست)، دار النهضة العربية، مصر، ط1، 2007.

36. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ط 2، دار النهضة العربية، مصر، 2008.

37. حسام الدين الأهوائي، الحق في احترام الحياة الخاصة (الحق في الخصوصية)، دراسة مقارنة، دار النهضة العربية، ط 2، 2002.

38. حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، 2012.

39. طعباش أمين الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الاسكندرية، ط 1، 2015.

40. كوثر سعيد عدنان، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الاسكندرية، 2012.

41. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط 1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

42. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الاسكندرية، 2003.

43. محمد أمين الرومي، التعاقد الإلكتروني عبر الانترنت، دار المطبوعات الجامعية، الطبعة 1, الاسكندرية، 2004.

44. محمد أمين الشوابكة، جرائم الحاسب والانترنت، ط1، عمان، دار الثقافة للنشر والتوزيع، 2004.

45. محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، مصر، 1987.

46. محمد حسام محمود لطفي، الإطار القانوني للمعاملات الإلكترونية، دار النهضة العربية، مصر، سنة 2002.

47. محمد حسام محمود لطفي، الإطار القانوني للمعاملات القانونية (دراسة مقارنة) في قواعد الإثبات في المواد المدنية والتجارية، القاهرة، دار النهضة العربية، 2002.

48. محمد حسين منصور، أحكام البيع التقليدية والإلكترونية والدولية وحماية المستهلك، دار الفكر الجامعي، الاسكندرية، 2006.

49. محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، الأردن، 2004.

50. محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الائتمان الممغنطة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2009.

51. محمد سامي الشوا، ثورة المعلومات وانعكساتها على قانون العقوبات، دار النهضة العربية، مصر، 1998.

52. محمد سعيد أحمد إسماعيل، الحماية القانونية لمعاملات التجارة الإلكترونية (دراسة مقارنة)، منشورات الحلبي الحقوقية، الطبعة الأولى، دمشق، 2009.

53. محمد شناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، 2008.

54. محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، بيروت، ط1، 2011.

55. محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، الطبعة الاولى، 2011.

56. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت (دراسة مقارنة)، دار النهضة العربية، الطبعة 2، 2009.

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

58. محمد علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديثة، ط1، مصر، 2004.

59. محمد عمر ذوابة، أكرم ياملكي، عقد التحويل المصرفي الإلكتروني (دراسة قانونية مقارنة)، دار الثقافة للنشر والتوزيع، الأردن، 2006.

60. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، 1991.

61. محمد محمد شتا، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، مصر، 2001.

62. محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الأسكندرية، الطبعة الأولى، 2014.

63. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر، الأردن، 2009.

64. مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، مصر، 2001.

65. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001.

66. مصطفى كمال طه, ووائل أنور بندق، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الإسكندرية، 2005.

67. مصطفى محمد مرسي، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، الطبعة الاولى، 2009.

68. مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الانترنت، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2010.

69. منير محمد الجنيهي وممدوح محمد الجنيهي، الطبيعة القانونية للعقد الإلكتروني، دار الفكر الجامعي، مصر، 2007.

70. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقة)، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005.

71. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، 2006.

72. نديم عبده، أمن الكمبيوتر (الفيروسات والقرصنة البمعلوماتية وانعكاساتها على الأمن القومي)، دار الفكر للأبحاث والدراسات، بيروت، ط1، 1991.

73. نعيم مغبغب، حماية برامج الكمبيتوتر (الأساليب والثغرات)، منشورات الحلبي الحقوقية، لبنان، 2006.

74. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008.

75. سامي عبد الباقي أبو صالح، الوفاء الإلكتروني بالديون الناشئة عن المعاملات التجارية، دار النهضة العربية، القاهرة ، بدون سنة نشر.

76. سند حسن سالم صالح، التنظيم القانوني للتوقيع الإلكتروني وحجيته في الإثبات المدني، دار النهضة العربية، 2010.

77. السيد عتيق، جرائم الانترنت، دار النهضة العربية، مصر، 2000.

78. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن، د.ط، دار الجامعة الجديدة، الاسكندرية، 2010.

79. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الاسكندرية، 2006.

80. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة متعمقة في القانون المعلوماتي)، ط1، دار الفكر الجامعي، الاسكندرية، 2006.

81. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية (الكتاب الثاني)، دار الكتب القانونية، مصر، 2007.

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

83. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2007.

84. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في التشريعات العربية، دراسة مقارنة، دار النهضة العربية، ط1، مصر, 2009.

85. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم المقارنة، دار الفكر الجامعي، مصر، 2010.

86. عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة، 2011.

87. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2001.

88. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم اللكترونية)، منشورات الحلبي الحقوقية، بيروت, 2007.

89. عطية سالم عطية، الصور المستحدثة لجرائم بطاقة الدفع الإلكتروني، مركز البحوث بأكاديمية الشرطة، القاهرة، 2011.

90. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة (دراسة مقارنة)، جامعة الاسكندرية، 2000.

91. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المكتبة القانونية، القاهرة، 1999.

92. عماد خليل، الحماية الجزائية لبطاقة الوفاء، دار وائل، عمان، 2000.

93. عمر الحسيني، صور الحماية الجنائية لنظام الحاسب الآلي، اتحاد المصارف العربية، القاهرة، 2010.

94. عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية، دار وائل للنشر والتوزيع، الطبعة الأولى، عمان، 2003.

95. عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت (الاحكام الموضوعية والجوانب الاجرائية)، دار النهضة العربية مصر، 2004.

96. عمرو إبراهيم الوقاد، الحماية الجنائية للمعلوماتية، بدون دار نشر، مصر، 2016.

97. فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة الجديدة للنشر، مصر، 2002.

98. قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشاة المعارف، الاسكندرية، 2005.

99. رياض فتح الله بصلة، جرائم بطاقة الائتمان، دون دار نشر، القاهرة، 2007.

100. شيماء عبد الغني عطالله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية, 2007.

101. ثروت عبد الحميد، التوقيع الإلكتروني (ماهيته- مخاطره-حجيته في الإثبات)، دار الجامعة الجديدة، الإسكندرية, 2007.

102. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب، دار الثقافة للنشر والتوزيع، عمان، 2011.

103. خالد ممدوح إبراهيم ، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2004.

104. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الاسكندرية، 2009.

105. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، 2009.

106. خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012.

ثانياً: الأطروحات والرسائل العلمية.

أ) الأطـــروحات:

107. إبراهيم بشارة عواد السويلمين، جريمة الاحتيال عبر الشبكة الدولية (دراسة مقارنة) ، أطروحة دكتوراه في القانون العام، جامعة عمان العربية للدراسات العليا، عمان، 2009.

108. أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه،كلية الحقوق، جامعة المنصورة، مصر، 2006/2005.

109. أسماء حسن سيد محمد، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه، جامعة القاهرة، 2013.

110. بدر الدين يونس، سلطة القاضي الجنائي في تقدير الدليل الجنائي، أطروحة دكتوراه، كلية الحقوق، جامعة قسنطينة 1، 2014.

111. حفصي عباس، جرائم التزوير الإلكترونية، أطروحة دكتوراه في العلوم الإسلامية (شريعة وقانون)، جامعة وهران "أحمد بن بلة"، الموسم الجامعي: 2014-2015.

112. ياسر الأمير فاروق محمد، مراقبة الأحاديث الخاصة في الإجراءات الجنائية (دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة, 2008.

113. محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة), رسالة دكتوراه, جامعة القاهرة, 2009.

114. سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية (دراسة مقارنة)، رسالة دكتوراه ، جامعة عين شمس القاهرة، 1997.

115. سعيد بن محمد الغافري، التعويض في التعامل الإلكتروني دراسة في النظام السعودي مع التأصيل والمقارنة، أطروحة الدكتوراه فلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

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

117. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه حقوق (القانون الجنائي والعلوم الجنائية)، كلية الحقوق ، جامعة الجزائر1، 2010-2011.

118. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق، جامعة بغداد، 1992.

119. خالد عبد التواب عبد الحميد أحمد، نظام بطاقات الدفع الإلكتروني من الناحية القانونية، رسالة دكتوراه، كلية حقوق حلوان، مصر، 2005-2006.

ب) رسائل الماجستير:

120. إسماعيل قطاف، العقود الإلكترونية وحماية المستهلك، مذكرة لنيل شهادة الماجيستر فرع "المسؤولية المهنية"، جامعة الجزائر، الموسم الجامعي 2005-2006.

121. بدر بن أحمد بن محمد الزهراني، جريمة الاحتيال الإلكتروني في النظام السعودي، رسالة ماجيستر في الشريعة والقانون، جامعة نايف العربية للعلوم الأمنية، الرياض، 2015.

122. واقد يوسف، النظام القانوني للدفع الإلكتروني، رسالة لنيل شهادة الماجيستر (القانون العام)، كلية الحقوق، جامعة مولود معمري بتيزي وزو، 2011.

123. يونس خالد عرب، جرائم الحاسوب (دراسة مقارنة)، رسالة ماجيستر، جامعة الاردن، 1994.

124. تيسير أحمد حسين الزعبي، الاحتيال الإلكتروني، رسالة ماجيستر في القانون العام، جامعة جدارا، 2009-2010.

125. خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، رسالة ماجيستر، جامعة نايف للعلوم الأمنية، 2009.

126. خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، دراسة تحليلية مقارنة، رسالة ماجيستر، جامعة نايف العربية للعلوم الأمنية، السعودية، 2009.

ثالثاً: الـمجلات العلمـية.

127. أحمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، بحث منشور بمجلة الفكر الشرطي، المجلد 17، العدد الرابع، عام 2008.

128. أحمد فتحي سرور، الحق في الحياة الخاصة، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية، السنة 54، 2016.

129. أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الانترنت (دراسة تحليلية مقارنة)، مجلة المنارة، كلية الدراسات الفقهية والقانونية، جامعة آل البيت، الأردن, العدد 9، المجلد 13، سنة 2007.

130. آلاء يعقوب النعيمي، الوكيل الإلكتروني: مفهومه طبيعته، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 7، العدد 2، جوان 2010.

131. بوخالفة حدة، النظام القانوني لمتعهد الإيواء عبر الانترنت، مجلة المفكر، كلية الحقوق، جامعة محمد خيضر، بسكرة، العدد 14.

132. حسن فريجة، الجرائم الإلكترونية والانترنت، مجلة المعلوماتية، السعودية، العدد 36، سنة 2012.

133. محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، العدد 30، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

134. محمد لموسخ، تنازع الاختصاص في الجرائم الإلكترونية، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، العدد 2، سنة 2009.

135. محمد مرسي الزهرة، مدى حجية التوقيع الالكتروني في الاثبات، دراسة مقارنة، مجلة الشؤون الاجتماعية، العدد 48، السنة 12، 2015.

136. مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الانترنت (دراسة مقارنة)، سلسة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد الخامس، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، سنة 2003.

137. ممدوح بن رشيد العنزي، الحماية الجنائية لبطاقات الدفع الإلكتروني من التزوير، المجلة العربية للدراسات الأمنية والتدريب، المجلد 31 العدد 62, الرياض, سنة 2015.

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

139. نبيل محمد أحمد صبيح، بعض الجوانب القانونية لبطاقات الوفاء والائتمان المصرفية، مجلة الحقوق، مجلس النشر العلمي، جامعة الكويت، مارس 2003.

140. نبيل محمد أحمد صبيح، حماية المستهلك في التعاملات الإلكترونية، مجلة الحقوق، مجلس النشر العلمي، جامعة الكويت، جوان 2008.

141. علي سالم، الأساس القانوني لحماية بطاقة الائتمان من الاحتيال، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد الثاني، السنة السابعة، سنة 2015.

142. فتحية محمد قوراري، الحماية الجنائية للمعاملات المصرفية الإلكترونية (دراسة تطبيقية) على بطاقات الائتمان الممغنطة في القانون الإماراتي والمقارن، مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الاسكندرية، جويلية سنة 2005.

رابـعاً: الملتقيات والـــمؤتمرات.

143. أحمد عبد الكريم سلامة، الانترنت والقانون الدولي الخاص، بحث مقدم إلى مؤتمر القانون والانترنت، جامعة الإمارات العربية المتحدة، 1-3 ماي، جزء 3، سنة 2004.

144. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني (دراسة مقارنة)، بحث مقدم إلى المؤتمر العلمي حول الجوانب القانونية والأمنية للعمليات الالكترونية، دبي الامارات العربية المتحدة 26-27 أفريل 2003.

145. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، دراسة مقدمة إلى مؤتمر كلية الشريعة والقانون بجامعة الإمارات العربية "القانون والكمبيوتر والانترنت"، الفترة ما بين 1-3 ماي 2000.

146. هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان: "الجرائم الواقعة في مجال تكنولوجيا المعلومات"، القاهرة 25-28 أكتوبر، 1993.

147. هواري عياش، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، مداخلة ملقاة بالملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، كلية الحقوق، 16-17 نوفمبر 2015.

148. حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، مداخلة ملقاة بالملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، كلية الحقوق، 16-17 نوفمبر 2015.

149. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي.، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية المنعقد في الفترة بين 28-29-2009، أكاديمية الدراسات العليا، طرابلس، ليبيا.

150. لوجاني نور الدين، أساليب البحث والتحري الخاصة وإجراءاتها وفقاً للقانون 06-22، مداخلة مقدمة في اليوم الدراسي حول علاقة النيابة العامة بالشرطة القضائية احترام حقوق الانسان ومكافحة الجريمة، وزارة الداخلية– المديرية العامة للأمن الوطني, المنعقد يوم 2007/12/12 بإليزي.

151. محمد السيد عرفة، التجارة الالكترونية عبر الانترنت، مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، الامارات العربية المتحدة، سنة 2000.

152. محمد خليل بحر، بطاقات الائتمان والآثار القانونية المترتبة بموجبها، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية وغرفة تجارة وصناعة دبي، بتاريخ 10-12 ماي 2003.

153. محمد عبد الرحيم سلطان، جرائم الإنترنت والإحتساب عليها، مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات، العين، ماي 2000.

154. موسى رزيق، رضا حامل البطاقة الائتمانية بالعقد والحماية التي يقررها المشرع له، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون،جامعة الامارات العربية وغرفة تجارة وصناعة دبي، بتاريخ 10-12 ماي 2003.

155. ناجي الزهراء، التجربة التشريعية الجزائرية في تنظيم المعاملات الإلكترونية المدنية والتجارية، المؤتمر العلمي المغاربي حول المعلوماتية والقانون، أكاديمية الدراسات العليا طرابلس، 28-29 أكتوبر 2009.

156. نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كوسيلة لأمن المعلومات, ورقة عمل مقدمة إلى المؤتمر الدولي لأمن المعلومات الإلكترونية بعنوان (معاً نحو تعامل رقمي آمن) المنعقد في الفترة 18-2005/12/20 مسقط عمان.

157. سمية عكور، الجرائم المعلوماتية وطرق مواجهتها (قراءة في المشهد القانوني والأمني)، مداخلة ملقاة بالملتقى العلمي للجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية, كلية العلوم الاستراتيجية، عمان، الأردن، خلال الفترة 4/2- 9-2014.

158. عبد الناصر محمد محمود فرغلي، محمد عبيد سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة، ورقة بحث مقدمة إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2007.

159. عدنان إبراهيم سرحان، الوفاء الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، بتاريخ 10-12 ماي 2003.

160. علي عباس، مخاطر استخدام بطاقة الدفع الإلكتروني عبر شبكة الانترنت، مؤتمر القانون والانترنت، جامعة الامارات، سنة 2002.

161. علي عبد القادر قهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم لمؤتمر القانون والكمبيوتر، جامعة الإمارات، العين، 1-3 ماي 2000.

162. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي, المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد 1، الإمارات العربية المتحدة، 26-28 أفريل 2003.

163. عمر الفاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، بحث مقدم لمؤتمر الكمبيوتر والانترنت، جامعة الإمارات, 1-3 ماي 2000.

164. فتوح شاذلي، المواجهة التشريعية للجرائم المستحدثة، بحث مقدم لمؤتمر الأمن والسلامة المنعقد من قبل وزارة الداخلية بأبو ظبي, 06-08 أكتوبر 2015.

165. غنام غنام، الحماية الجنائية لبطاقة الائتمان الممغنطة، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، سنة 2003.

خامساً: البحوث المتاحة على الانـــترنت:

166. يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي، اتحاد المصارف العربية، عمان، الأردن، سنة 2002, متاح على الرابط التالي: *www.abhatoo.net* .

167. مركز البحوث والدراسات، الغش التجاري في المجتمع الإلكتروني، ورقة عمل مقدمة إلى الندوة الرابعة لمكافحة الغش والتقليد في دول مجلس التعاون الخليجي، 2014, متاح على الرابط التالي: *https://fr.scribd.com*

168. عبد الفتاح محمود كيلاني، مدى المسؤولية القانونية لمقدمي خدمة الانترنت، بحث منشور على الانترنت, متاح على الرابط التالي: *http://www.flaw.bu.edu.eg/flaw/images/part2.pdf*

169. شيماء عبد الغني، مكافحة جرائم المعلوماتية في المملكةالعربية السعودية، متاح على الرابط التالي: *https://www.mohamah.net/law*

سادساً: النصوص التشريعية.

أ) النصوص التشريعية والتنظيمية الوطنية:

170. قانون رقم 18-07 المؤرخ في 25 رمضان عام 1439هـ الموافق 10جوان سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي, ج رج عدد 34، ص 11. المؤرخة في 10 جوان 2018.

171. القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي 2018 يتعلق بالتجارة الإلكترونية, ج ر ج عدد 28، السنة 55، المؤرخة في 30 شعبان 1439 الموافق 16ماي 2018.

172. القانون رقم 15-04 المؤرخ في 2015/02/01 الموافق 11 ربيع الثاني 1436 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين, ج ر ج العدد 06.

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

174. القانون 2000-03 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات.

175. الأمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق 8 جوان 1966 المتضمن قانون العقوبات, ج رج العدد 49، السنة 03، ص 702-753, المتمم بالقانون رقم 16-02 المؤرخ في 14 رمضان 1437 الموافق 19 جوان 2016 ج رج العدد 37 ،ص 4 المؤرخة في 2016/06/22.

176. الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق 8 جوان 1966 المتضمن قانون الإجراءات الجزائية, ج رج العدد 49, المعدل والمتمم بالقانون رقم 18-06 المؤرخ في 25 رمضان 1439 الموافق 10جوان 2018 ج رج العدد 34 ص 4 المؤرخة في 2018/06/10.

177. الأمر رقم 75-58 المؤرخ في 20 رمضان 1395 الموافق في 26 سبتمبر 1975 المتضمن القانون المدني, ج رج العدد 78، السنة 12، ص 990-1055, المعدل والمتمم .

178. الأمر رقم 75-59 المؤرخ في 20 رمضان 1395 الموافق 26 سبتمبر 1975 المتضمن القانون التجاري المعدل والمتمم .

179. الأمر رقم 03-03 المؤرخ في 19 جمادى الأولى 1424 الموافق 19 جويلية 2003, ج رج العدد 43، السنة 40، ص 25-32) المتعلق بمكافحة التهريب الموافق عليه بالقانون رقم 03-12, ج رج العدد 64، المؤرخة في 26 أكتوبر 2003، ص 04, المعدل والمتمم بالقانون رقم 08-12 المؤرخ في 25 جوان 2008, ج رج العدد 36، السنة 45، ص 11-15.

180. الأمر رقم 03-11 المؤرخ في 27 جمادى الثانية 1424 الموافق 26 أوت 2003 المتعلق بالنقد والقرض, ج رج العدد 52، السنة 40، ص 3-22, الموافق عليه بالقانون رقم 03-15 المؤرخ في 29 شعبان 1424 الموافق 25 أكتوبر 2003, ج رج العدد 64، السنة 40، ص 05, المعدل والمتمم.
181. الأمر رقم 05-06 المؤرخ في 18 رجب 1426 الموافق 23 أوت 2005 المتعلق بمكافحة التهريب, ج رج العدد 59، السنة 42، ص 3-8, الموافق عليه بالقانون رقم 05-17 المؤرخ في 29 ذي القعدة 1426 الموافق 31 ديسمبر 2005, ج رج العدد 02، السنة 43، ص 03.
182. المرسوم الرئاسي رقم 261/15 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

ب) النصوص التشريعية العربية:

183. قانون رقم 2000-83 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية التونسي, المنشور في الجريدة الرسمية التونسية العدد 64 المؤرخة في 11 أوت 2000.
184. القانون رقم 01 لسنة 2006 بشأن التجارة الإلكترونية الإماراتي، ج ر رقم 442 يناير2006.
185. القانون الاتحادي الإماراتي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.
186. قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015.
187. قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 المؤرخ في 2004/11/10 الجريدة الرسمية عدد 71 الصادرة بتاريخ 2004/11/10.
188. القانون المصري رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات المؤرخ في 14 اوت 2018 الجريدة الرسمية العدد 32 مكرر ج ص 03.

سابعاً: الـــمراجع باللغـــة الأجنبيـــة.

A. Textes Juridiques:

1. Texte ligislatives et Réglementaires :

189. Code pénal français.
190. Code de procédure pénale français.
191. Loi du 29 juillet 1881 sur la liberté de la presse Modifié par Ordonnance du 26 août
192. Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuell .

193. Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve au technologies de l'information et relative à la signature électronique (J.O du 14 mars 2000, p 3968).
194. Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 3o septembre 1986 relative à la liberté de communication.
195. Loi n° 91-1382 du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement (J.O du 1er janvier 1992, p12).
196. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans -l'économie numérique Modifié par Loi n°2018-898 du 23 obre 2018 (J.O 143 du 22 juin 2004, p 168).
197. La loi n° 2004-801 du 6 out 2004 relative à la protection des personnes physique à légard des traitements de données à caractére personnel et modifiantt la Loi n°:78-17 du 06 janvier 1978relative à l'informatque,aux fichiers et aux libertés (JO.R.F du 07 /01/1978, p 227 .
198. Ordonnance n°: 2011-1012 du 24 out 2011 relative aux communications électroniques (JORF N 197 DU 26 OUT 2011).
199. L a loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
200. The Digital Millenium Copyright Act (DMCA)) Public Law n° 105-304, 112 sat, 2860, 28 oct. 1998 U.S. Copyright Office Summary.

2. Directives:

201. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
202. -Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications Journal officiel n° L 024 du 30/01/1998 p. 0001 – 0008.
203. Directive 2000/31/CE du 08 juin 2000 relative à certains aspects juridiques de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (J.O n° L 178 du 17 juillet 2000).

204. Directive 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).
205. Directive 2009/136/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs .
206. Réglement (UE) No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

B. Les ouvrages:

207. BENSOUSSAN alain, le Consommateur Electronique «Aspect Juridique », Edition Hermes, Paris, 1998.
208. Daniel Kaplan, Informatique, Libertées, Identities, Fyp Edition,1er avril.2010.
209. Doon .B.Parker, Fighting Computer Crime, (a New Framework for protection information (job wily sons, 1998.
210. Eoghan Casey, Digital Evidence and Computer Crime Foreensic, Science, Computers and the Internet, Second Edition, Academic Press An Imprint of Elsevier, London 2004.
211. Henri crose, et yves Bismuth,le Droit de l'informatique, Paris Expertice.1984.
212. JEANTIN MICHEL , PAUL CANNU, Droit Commercial, Instruments de Paiement et Crédit Entreprise en Difficulté, 5 éme édition, Dalloz, Paris, 1999
213. Jonathan Rosenar ; Cyber-Law, the law of the internet; ed Springer.1997.
214. Linat De Bellefonds (xavier) et Hollande (Allain), Droit de l'informatique et de la Télématique, Ed des Parques, 2001.

215. Lucas (André), Deveze (Jean), Frayssinet, Droit de l'informatique et de l'internet, 2001.
216. Michel Vivant et autres , Informatique et Droit Pénale. Les Biens Informatiques, Objets d'une Fraude .Lamy Informatique; 1991
217. Myriam quéméner, yves CHARPENEL, Cybercriminalité, Droit Pénal Appliqué ECONOMICA, Paris, 2010
218. Piérre Catala, les Transformatique de Droit par l'informatique Emergence du Droit de l'informatique et des Parques,1983.
219. Raymons gassin, la Protection Pénale d'un Nouvelle Univers de Fait en Droit Français le Systémes de Traitement Automate de Donnes, Actuaire Legislataire, Dalloz. 1980.
220. Raymons gassin, le Droit Pénale de l'informatique, Dalloz, 1986
221. Valérie Sédallian, Droit de l'internet: Réglementation, Responsabilité, Contras, Collection Association des Utilisateurs d'internet , éd. Net press. 1997.

C. Theses et memoires:

222. Ann BRISSET-GIUSTINIANI, Aspects Juridiques de l'émergence d'une Sécurité Européenne des Réseaux et des Systèmes d'information, Mémoire D.E.S.S Droit de l'internet Administration-Entreprises, Université PANTHEON SORBON, Paris. 2004
223. Hanachowiz (Lionel), Les Cartes Bancaires (Irrégularités) et Fraude, Thèse Doctorat; Université Lyon iii 1985.
224. Ibrahim Coulibaly, la Protection des Données à Caractère Personnel dans le Domaine de la Recherche Scientifique, Thèse pour Obtenir le Grade Doctorat de l'université de Grenoble.2011.

D. Articles:

225. BRUNO KAROUBI, La Criminalité Favorise-t-elle l'acceptation de la Carte Bancaire? Revue économique.2015/6 Vol 66.
226. Bertrand (R), la Criminalité Informatique, les Délits Relatifs au Matériel .Recueil Dalloz -Sirey.n 62, Expertise, 1984
227. Cabrillac (M) et Mouly (c): Droit Pénal de la Banque et du Crédit , MASSON, Paris, 2009, N356.

228. Ch. HUGON, "La Responsabilité des Acteurs de l´internet dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l´économie numérique", Contrats, Concurrence, Consommation, Études, novembre 2004, n° 18.
229. Olivier Cachard , Droit du Commerce Electronique , RDAI, N 3, 2004.
230. PRADEL (j), FEUILLARD (ch) : Les Infractions Commises au Moyen de l'Ordinateur Rev .pen .crim juillet 2014.
231. DEVEZE (j) , La Fraude Informatique- Aspects Juridiques ,J.C.P 2007,doct.3289 n9
232. Dominique Mangenot, Droit de la Preuve et Technologies Nouvelles, Droit de la Preuve Formation Permanete,Cup.vol xix.oct 1997.
233. Jean spreutels, les Crimes Informatique et d'autre Crimes dans le Domaine de la Technologie Informatique en Belgique, rev.int pénal. 2016.
234. Jean DIDIER, Les Truques et Usages Frauduleuse de Cartes Magnétiques, J.C.P 2012.
235. Jean Pradel, les Infractions Relatives à linformatique, Revue International de Droit Comparé vol.42 n 2 Avril - Juin 1990. Etudes de Droit Contemporain.
236. Reynald OTTENHOF, Infraction Contr les Biens, Revue de Science Criminale et de Droit Pénale Comparé, 2001.
237. Yvonne Muller-Lagarde, La Protection Pénale de la Relation de Confiance: Observations sur le Délitd'Abus de Confiance. Revue de Science Criminelle et de Droit Pénal Comparé, Dalloz, 2006.

E. Les articles sur Internet:

238. D. MELISON, "Responsabilité des hébergeurs : une unité de régime en trompe l'œil", juriscom.net 25 avril 2005, disponible en lingne á l'adresse suivante: *www.juriscom.net*
239. Guide Permanent Droit et Internet, E 3.3 Hébergement du site, précité, nº 1 et 4, p. 4 et 5, H. LANGLOIS, "La Responsabilité des Intermédiaires en Matière de Commerce Electronique", Petites Affiches, 6 février 2004, n° 27.
240. Jean-jacques Hyest : la Fraude Informatique Vue par le Nouveau Code Pénale, Expertises des Systémes de l'information , Février 2010.
241. Leclercq (jean); prevue et signature électronique de la loi 13 mars 2001,au decret du mars 2001.

242. Richard Hillman, Securities Fraud, the Internet Poses Challenges to Regulaters and Inverstors, United States General Accountig office, 2017.
243. VERCILLE (V) ,BOUBILA (S) et FABRE(R): La Monnaie Electronique : Enjeux Micro-économique et Macro-économique, éd Université des Sciences Sociales des Toulous1, Maitrise de Sciences Economiques, 1998-1999.
244. Piérre TRUCHE; Jean –paul Faugére et Patrice FLICHHY: Administration Electronique et Protection des Données Personnelles Livre Blanc, Rapport au Ministre de la Fonction Public et de la Réforme de l'Etat, Paris, la Documentation Française, 2002.
245. Pierre. TRUDEL, La Responsabilité sur Internet, Texte Préparé pour le Séminaire Droit et Toile, Bamako, organisé par l'UNITAR (Institut des Nations unies pour la formation et la recherche), en association avec OSIRIS (Observatoire sur les Systèmes d'Information, les Réseaux et les Inforoutes au Sénégal) et l'INTIF (Institut francophone des nouvellestechnologies de l'information et de la formation) de l'Agence Intergouvernementale de la Francophonie Bamako, 27 mai 2002.
246. Pierre Emmanuel, Ombolo, Menogainstrument de Creditet de Paiement; disponible en lingne á l'adresse suivante:
http://lumiairedudroit.centerblog.net/36-instruments-de credit-et-de-paiement.
247. Stowel (A) et Ide (N), Respnsibilité de Intermidiares: Actualités législatives et jurisprudantilles, Droit et Nouvelle Teccchnologies, 10 Octobre 2000.
248. Thierry Breton: Chantier sur la Lutte Contre la Cybercriminalité; Disponible en ligne: *http://www.réseaux-telecoms.com.*
249. V. SÉDALLIAN, "La Responsabilité des Prestataires Techniques sur Internet dans le Digital Millenium Copyright Act américain et le projet de directive européen sur le commerce électronique", Cahiers Lamy, Droit de l'informatique et des réseaux, n° 110, janvier 1999.

F. Sites Internet Divers:

250. www.uncitral.org.
251. www.legifrace.gouv.fr
252. www.joradp.dz
253. http://eur-lex.europa.eu/oj/direct-access.html?locale=fr

254. *www.memoireonline.com*
255. *http://edoctorale74.uni-lille.2.fr*
256. *http://europa.eu/législation-séminaire/international*
257. *www.eastlaw.blogspot.com/2010/03/23-11-2001.html*
258. *http://www.flaw.bu.edu.eg/flaw/images/part2.pdf*
259. *http://pierretrudel.chairelrwilson.ca/cours/drt6929f/Resp.internet-trudel.pdf*
260. *HTTP://BBF.ENSSIB.FR/CONSULTER/BBF-1999-01-0125-009.*
261. *www.jurispedia.org/index.php/Responsabilit_techniques_de_l'inter.net*
262. *http://lcweb.loc.gov/copyright.*
263. *http://www.stratégique.free.fr*
264. *www.univ-paris1 .fr*
265. *www.cairn.info/revue-economique.*

فهرس المحتويات

فهرس المحتويات

الملخص:

تعتبر المعاملات الإلكترونية من أهم الآليات المراهن عليها مستقبلاً في بناء دول مبنية على الحداثة والسرعة في أداء مهامها المجتمعية والاقتصادية، إلا أن هذا التطور قد يحمل معه مخاطر عديدة على مستوى قيام تلك المعاملات خاصة في ظل ارتباطها بشبكة الانترنت.

وهنا كان لزاماً على مختلف التشريعات الدولية والمقارنة في التصدي للنمط الحديث من الجرائم الماسة بالمعاملات الإلكترونية، وهو ما يعزز ظهور جملة من القواعد الموضوعية والإجرائية على المدى البعيد تضمن الحماية الجنائية الفعالة لكل وسائل وأطراف التعاملات الإلكترونية.

الكلمات المفتاحية: المال المعلوماتي- الاحتيال الالكتروني- التجسس الالكتروني- الجرائم الالكترونية- البيانات الشخصية.

Summary:

E-transactions are considered one of the most important mechanisms in the future in building countries based on modernity and speed in the performance of societal and economic tasks, but this development may carry with it many risks to the level of such transactions, especially in light of the Internet connection.

Here, various international and comparative legislation was required to deal with the modern pattern of cybercrime, which reinforces the emergence of a number of objective and procedural rules in the long run to ensure effective criminal protection of all means and parties to electronic transactions.

Key words: informational money - electronic fraud - electronic espionage - cybercrime - personal data.