جرائم التجارة الإلكترونية "الخصوصية ومتطلبات المواجهة التشريعية" (بحث مقارن)

روسم عطية موسى

عضو هيئة تدريس، كلية القانون، جامعة درنة.

drro6404@gmail.com

استلمت الورقة بتاريخ 2022/6/1
وقبلت بتاريخ 2022/7/22
ونشرت بتاريخ 2022/8/5

الكلمات المفتاحية: تذكر هنا أهم الكلمات المفتاحية (3-5 كلمات)

الملخص

لقد تطرقنا لبحث موضوع **جرائم التجارة الإلكترونية " الخصوصية ومتطلبات المواجهة التشريعية"** متبعين في ذلك المنهج التحليلي الوصفي المقارن, وقد اعتمدنا خطة ثنائية لعرض موضوع البحث تتكون من مبحثين: تضمن المبحث الأول بيان الخصوصية الفنية والإجرائية لجرائم التجارة الإلكترونية. أما المبحث الثاني فقد خصص لتوضيح متطلبات المواجهة التشريعية لجرائم التجارة الإلكترونية على مستوى القواعد الموضوعية والإجرائية.

ويهدف البحث إلى توضيح أهمية المواجهة التشريعية لجرائم التجارة الإلكترونية بنصوص خاصة تتلاءم مع الطابع الفني والتقني الخاص بهذا النمط المستحدث من الاجرام الذي أضحى يشكل تحدياً كبيراً في إطار مكافحته والتصدي له، خاصة في ظل الصعوبات القانونية التي أفرزها التطبيق العملي للقواعد الجنائية التقليدية في نطاق الجرائم الإلكترونية.

وقد توصلنا من خلال بحثنا للموضوع إلى ضرورة استحداث نظام قانوني متكامل يكفل المواجهة الجنائية الفاعلة للجرائم الإلكترونية بشكل عام وجرائم التجارة الإلكترونية بشكل خاص، و تكثيف التعاون الدولي في مجال مكافحة الجرائم المستجدة بفعل التكنولوجيا المعلوماتية.

الكلمات المفتاحية: , جرائم, تجارة إلكترونية , خصوصية , مواجهة تشريعية.

المقدمة

موضوع البحث:

لقد ساهمت ثورة تكنولوجيا الاتصالات والمعلومات التي يشهدها العصر الحديث في تقريب المسافات ونقل المعلومة من مكان إلى أخر في زمن قياسي, فتعددت الشبكات المفتوحة التي قربت القارات بعضها من بعض حتى أمكن القيام بالأعمال اليومية دون تنقل, وظهر ما يعرف بالتعليم عن بعد, والطب عن بعد, والعمل عن بعد ... إلخ, وأفرزت هذه الثورة ما أطلق عليه اسم "الإنترنت" والذي أخذت استخداماته تتطور إلى أن ظهر مصطلح **" التجارة الإلكترونية "**[1].

فالتجارة الإلكترونية هي أحد استخدامات الإنترنت, وتعني مجموعة المبادلات الرقمية ذات الصلة بالأنشطة التجارية التي تقوم على استخدام التقنيات التي وفرتها الثورة المعلوماتية والاتصالات وشبكة الإنترنت عبر التبادل الإلكتروني للبيانات, متجاوزة عنصري الزمان والمكان, وتغطي قطاعات عديدة, وتضع قواعد جديدة لعمليات البيع والتخزين والتوثيق والاستثمار....إلخ.

وككل تطور, فقد فتحت الثورة التكنولوجية أبواباً نحو تجاوزات لم تكن موجودة قبل ظهورها, وحملت بين طياتها جانباً مظلماً أفرزه استعمالها لأغراض غير مشروعة, فاتسمت الجرائم الإلكترونية بسمات الواقع التقني الذي تتم فيه, وسايرت ما يقدمه من تطور, فتميزت عن غيرها من الجرائم بخصائص وتقنيات عديدة ومن ضمنها جرائم التجارة الإلكترونية.

[1] ينقسم مصطلح التجارة الإلكترونية إلى قسمين: **القسم الأول**: التجارة وهو مصطلح معروف ، يعبر عن نشاط اقتصادي يتم من خلال تداول السلع والخدمات،**القسم الثاني**: الإلكترونية وهو نوع من التوصيف لمجال أداء النشاط المحدد في القسم الأول، ويقصد به هنا أداء النشاط التجاري باستخدام الوسائط والأساليب الإلكترونية، ويعد الإنترنت أحد أهم الوسائط الإلكترونية التي يستخدم البيانات الإلكترونية لإبرام المعاملات بين طرفي عقد التجارة الإلكترونية. ينظر : بدر منشيف، حماية المستهلك في العقد الإلكتروني ، المجلة العربية للدراسات القانونية والاقتصادية والاجتماعية ، المغرب ، (ط1)، 2020، ص: 322. منشورة على الموقع الإلكتروني drive . google. com

أهمية البحث:

إن التجارة الإلكترونية تمثل في الوقت الراهن الأساس في عالم التجارة, بل من المتوقع أن تكون هي الأساس الوحيد للتعامل في السنوات القادمة, وبذلك فإن الحاجة تبدو ملحة إلى توفير حماية جنائية فاعلة لها ضد التجاوزات التي قد تقع في نطاقها بشكل يتلاءم مع خصوصيتها الفنية والتقنية والتي شكلت مفارقة عميقة مع القانون الذي يرتكز على خاصيات لا تتجاوز المكان والزمان وإن امتدت فيه, والموجود فعلاً وإن اختلفت فيه .

ويكتسي موضوع البحث أهمية على المستويين النظري والعملي:

- **المستوى النظري**: ينبثق من الطبيعة اللامادية للتجارة الإلكترونية والتنامي المذهل للسلوكيات المنحرفة, وسرعة اكتساحها لكل الميادين واستفحال دائها, وغياب نصوص قانونية خاصة لمواجهتها , كل ذلك من شأنه أن يطرح مسألة ضبط الاختيارات الكبرى, أي السياسة الجنائية المتعلقة بمدى إمكانية إخضاع الانحرافات الجديدة لمبدأ التجريم والعقاب.
- **المستوى العملي:** يتمثل في تطبيق تلك الاختيارات وبلورتها في إطار ميدان العلوم الجنائية, بعد استطلاع ما توصلت إليه الدول المتقدمة في مجال مكافحة الجرائم الإلكترونية لسن تشريعات مناسبة عندما يستشعر المشرع الحاجة لذلك.

نطاق البحث:

ينصب موضوع البحث على جرائم التجارة الإلكترونية في إطار الخصوصية ومتطلبات المواجهة التشريعية, وبذلك يخرج عن نطاقه جرائم التجارة التقليدية, كما ينحصر مفهوم التجارة الإلكترونية في نطاق بحثنا في كونها عنصراً من عناصر العمل الإلكتروني يقتصر فقط على النشاط التجاري, ويتعلق بالتعاقدات التجارية والمبادلات التي تقع في إطار بيئة تقنية, دون التطرق للأعمال الإلكترونية التي تعد أوسع نطاقاً وأشمل من التجارة الإلكترونية.

إشكالية البحث:

يثير البحث إشكالية قانونية تتمثل في الفراغ التشريعي القائم في العديد من الدول في مجال مكافحة جرائم التجارة الإلكترونية, ومدى إمكانية التصدي لها وما يطرحه ذلك من تساؤلات تتمثل في :

- **هل تكفي القواعد الجنائية التقليدية لمواجهة هذا النمط المستحدث من الإجرام مع ما ينفرد به من خصوصية تقنية وأبعاد دولية ؟**
- **في حال عدم كفاية القواعد الجنائية التقليدية لمواجهة هذا النمط المستحدث من الإجرام, هل يتطلب الأمر ضرورة تعديلها بما يتلاءم ومتطلبات المواجهة التشريعية الفاعلة له؟ أم أن خصوصية هذا النمط من الإجرام التقني تقتضي المعالجة بنصوص قانونية خاصة ووفقاً لمعطيات وآليات معينة تتلاءم مع طبيعة المعاملات الإلكترونية محل الحماية الجنائية؟**

أهداف البحث:

يهدف البحث إلى توضيح الآتي:

- **الخصوصية الفنية والإجرائية لجرائم التجارة الإلكترونية.**
- **متطلبات المواجهة التشريعية لمكافحة هذا النمط المستحدث من الإجرام التقني على مستوى القواعد الموضوعية والإجرائية.**
- **أهمية وضع تنظيم تشريعي خاص لمكافحة جرائم التجارة الإلكترونية في إطار التصدي للإجرام الإلكتروني.**

منهج البحث:

سنتبع في بحثنا للموضوع المنهج التحليلي الوصفي المقارن وفقاً للخطة الآتية:

المبحث الأول/ خصوصية جرائم التجارة الإلكترونية.

المطلب الأول/ خصوصية فنية.

المطلب الثاني/ خصوصية إجرائية.

المبحث الثاني/ متطلبات المواجهة التشريعية لجرائم التجارة الإلكترونية.

المطلب الأول/ على مستوى القواعد الموضوعية.

المطلب الثاني/ على مستوى القواعد الإجرائية.

المبحث الأول
خصوصية جرائم التجارة الإلكترونية

تمهيد وتقسيم:

تختلف تقنيات الجرائم الإلكترونية – ويدخل في نطاقها جرائم التجارة الإلكترونية - كثيراً عن أنماط الجرائم التقليدية ويرجع ذلك إلى البيئة الرقمية التي تتم فيها هذه الجرائم وما يتميز به مرتكبيها من سمات خاصة(**مطلب أول**), وما ترتب على ذلك من خصوصية فنية انعكست على الجانب الإجرائي فشكلت تحدياً في إطار مكافحتها(**مطلب ثان**).

المطلب الأول
خصوصية فنية

تمهيد وتقسيم:

تتميز جرائم التجارة الإلكترونية عن الجرائم التقليدية بوسائل اقترافها وطرقها, فهي تنفرد بخصوصية فنية سواءً فيما يتعلق بالتقنيات المستخدمة في ارتكابها(**فرع أول**), أو ما يتعلق بمرتكبيها(**فرع ثان**).

الفرع الأول/ خصوصية التقنيات المستخدمة في جرائم التجارة الإلكترونية.

تختلف تقنيات جرائم التجارة الإلكترونية كثيراً عن أنماط الجريمة التقليدية؛ ويرجع ذلك لأداة الجريمة ألا وهو الحاسوب الذي قد يكون أداة وضحية في الوقت ذاته بحسب الدور الذي يلعبه في ارتكاب الفعل مباشراً كان(**بند أول**), أم غير مباشر(**بند ثان**).

البند الأول/ التقنيات المعتمدة على الحاسوب بشكل مباشر.

أي أن الفعل الإجرامي لا يتم إلا بالحاسوب الذي يحتاجه الجاني لتسهيل جريمته التي قد تتخذ أحد الصور الآتية:

أولاً: التقنيات المستخدمة ضد البيانات:

إن البيانات هي مجموعة من المعطيات التي تهتم بموضوع معين, وهي تتخذ أشكالاً مختلفة في صورة مجموعة أرقام, أو حروف, أو رموز, أو صور, أو أشكال خاصة, وهي تعد مادة خاماً قابلة للتحويل واستخراج معلومات معينة, مثل: (أرقام المبيعات في شركة ما, صورة متلقاه من قمر صناعي للاستشعار عن بعد, أرقام حسابات مصرفية ....). فالبيانات بهذا المعنى تمثل ثروة مهمة يمكن أن تكون عرضة لعدة اعتداءات يسهلها استخدام تقنيات معقدة, وتتمثل خصوصاً في وضع بيانات وهمية, أو تزييف البيانات, أو التجسس على البيانات, أو سرقة البيانات.[1]

ثانياً: التقنيات المستخدمة ضد البرامج.

البرامج هي عبارة عن مجموعة أوامر مجتمعة في ملف أو عدة ملفات تعمل على معالجة معلومات معينة, مثل برامج التطبيق في البنوك التي تعالج الحسابات البنكية للزبائن.

ويعد البرنامج المحرك الرئيس للآلة التي من خلالها يقوم الجاني بجميع عملياته الإجرامية, وتتمثل التقنيات المستعملة ضد البرامج في: تغيير مهمة البرنامج بتحوير يطال مجموعة الأوامر المكونة للبرنامج, ووضع برامج الفيروسات المعلوماتية, ووضع برامج مبتورة, وإعداد برامج وهمية جديدة.[2]

ثالثاً: التقنيات المستخدمة ضد الآلة.

بالإضافة إلى الجرائم التي تستهدف الجانب غير المادي للحاسوب, هناك جرائم تستهدف الجاني المادي للآلة, وتتمثل التقنيات المستخدمة ضدها في: إعداد برامج معلوماتية تخريبية لتدمير الجانب المادي للحاسوب, وإدخال اضطراب على حسن سير العمل العادي للحاسوب.[3]

البند الثاني/ التقنيات المعتمدة على الحاسوب بشكل غير مباشر.

وهنا يكون للحاسوب دور غير مباشر في ارتكاب الجريمة كما يتضح ذلك في الصور الآتية:

أولاً: الجرائم المستهدفة للحاسوب.

ليس بالضرورة لتعرض الجهاز للاعتداء أن يكون في حالة تشغيل, فقد يتعرض الجهاز للاعتداء وهو في حالة سكون وتتحقق ذات النتيجة؛ وذلك بحصول الفاعل على بعض البيانات أو المعلومات بالرجوع إلى علاقة الجهاز ببعض التوابع, كسرقة الحوامل المادية, وسرقة بيانات مضمنة بأشرطة ممغنطة أو بأشرطة عادية, وسرقة بيانات من على وثائق عادية, أو تخريب توابع الحاسوب.[4]

ثانياً: تزييف بطاقات الائتمان (البطاقات الممغنطة).

---

[1] لمزيد من الإطلاع ينظر: شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دراسة مقارنة،(د.ط)،(د.م.ن):برلين للطباعة، 2013، ص:93.

[2] ينظر:هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، (د.ط)، القاهرة: دار النهضة العربية ، 1992، ص: 43.

[3] ينظر:هدى حامد قشقوش، مرجع سابق، ص: 77.

[4] ينظر: ذات المرجع ، ص: 78.

مع ظهور بطاقات الائتمان كوسيلة سهلة في مجال المعاملات التجارية والنقدية, وتداول العملات المالية, ظهر صنف جديد من الجرائم الاقتصادية وتزايدت معدلاته بتزايد عدد العاملين مع آلات الصرف الآلي.[1]

ولم تسلم بطاقات الائتمان من عمليات التزييف والسرقة التي تقف وراءها عصابات دولية متخصصة تستخدم أحدث أساليب التكنولوجيا في ارتكاب جرائمها, وهو ما دفع خبراء المال والاقتصاد إلى إطلاق صيحات التحذير والمطالبة بالبحث عن وسائل حديثة للحد من هذه النوعية من الجرائم.

البند الثالث/ جرائم الاعتداء على مواقع الويب التجارية.

تمثل هذه الجرائم تهديداً مباشراً المعاملات التجارية الإلكترونية, سواء في إطار استغلال خدمات البريد الإلكتروني, أو في الاعتداء على نمط المبادلات التجارية.

أولاً: جرائم البريد الإلكتروني.

من بين الخدمات التي تعتمد عليها المعاملات التجارية الإلكترونية خدمات البريد الإلكتروني وذلك بتمكين حرفائها من الحصول على العقود الإلكترونية التي تتم بها إبرام الصفقات التجارية وكذلك الدفع الإلكتروني, ويكون ذلك بواسطة رسائل إلكترونية في شكل سيل من البيانات تمر عبر الشبكات الوسيطة إلى عناوين محددة مسبقة وهذه الرسائل غالباً ما تكون عرضة لأعمال إجرامية, أو قد تكون بذاتها سبباً في ارتكاب أفعال أخرى.

وتتمثل هذه الأفعال في الناحية الأولى, في تعقب الرسائل الإلكترونية قصد ارتكاب أفعال إجرامية تستهدف محتواها, أما الوجه الثاني لهذه الجرائم, فهي تلك التي تستهدف البريد الإلكتروني بجعله شريكاً متواطئاً في ارتكاب الأفعال, فالجاني قد يستعمل البريد الإلكتروني للمساعدة بإرسال رسالة مسمومة أو ملغمة ووضعها بذلك البريد.[2]

ثانياً: اختراق الشبكات التجارية.

تتمثل هذه الجرائم في الاعتداء على نمط المبادلات التجارية الذي يعتمد وثائق إلكترونية لا مادية, ويعتمد ارتكابها على خبرة الجناة في مجال اختراق الشبكات وحل الشفرات الخاصة بهذه النوعية من المبادلات, وتتعدد الأفعال المرتكبة ضد التجارة الإلكترونية من التحايل عبر إحداث مواقع للتجارة الإلكترونية تكون وهمية قصد سرقة أرقام بطاقات الائتمان, أو سرقة هذه الأرقام عبر التجسس عن بعد وتعقبها.[3]

الفرع الثاني/ خصوصية المجرم الإلكتروني.

يمثل المجرم الإلكتروني بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة قائمة بذاتها, إلا أنه لا يوجد نموذج محدد للمجرم الإلكتروني بل إن هناك عدة نماذج للمجرمين في إطار الجرائم الإلكترونية (**بند أول**), تدفعهم إلى ارتكاب أفعالهم الإجرامية أسباب وعوامل تختلف عن تلك التي تدفع المجرم التقليدي للإجرام (**بند ثان**).

البند الأول/ أصناف الجناة.

إن تصنيف الجناة في إطار الجرائم الإلكترونية يعتمد بالأساس على خصوصيات المجرم في المجال الإلكتروني الراجعة للسمات الخاصة بالجريمة الإلكترونية؛ بحيث يمكن تصنيف هؤلاء المجرمين إلى فئات متعددة نذكر منها[4]:

أولاً: المحترفون:

إن جرائم التجارة الإلكترونية تعد من جرائم التقنية البيضاء التي تتطلب الخبرة والدراية والذكاء, وبالرجوع إلى تصنيف المجرمين حسب ظهور الإجرام يمكن القول إن المجرم المحترف هو المجرم الذي يتخذ من الإجرام حرفة ومهنة يعتمد عليها في معيشته ويعتبرها رسالة في الحياة, وقد يعمل المجرم المحترف بشكل فردي, كما قد يؤسس أو ينضم إلى عصابة إجرامية كبيرة أو صغيرة وقد تكون هذه العصابة ممتدة الفروع داخل دول مختلفة.[5]

والسمة العامة التي تميز هؤلاء المجرمين هي طريقتهم في الحياة التي تعتمد على أحد أمرين: إما الاتجاه إلى كشف هذه الاتجاهات الإجرامية في الوسط المحيط, وإما الاتجاه إلى إخفائها عن ذلك الوسط عن طريق استخدام الأوراق المزورة أو عن طريق استخدام لغة خاصة مع عصابته دلالاتها معروفة فيما بينهم فقط, واللغة الخاصة التي يتبادلها محترفو جرائم التجارة الإلكترونية تتسم بكونها أكثر تعقيداً, وتقوم على الرموز وهو ما يجعل أفعال المجرم المحترف في هذا الميدان على درجة كبيرة من الخطورة, لاسيما إذا ما أخذنا في الاعتبار الصبغة التقنية للجريمة الإلكترونية وتعقد شخصية مرتكبها.

---

[1] ينظر: عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية ، (د.ط)، الإسكندرية، دار الجامعة الجديدة ، 2009، ص:78.

[2] ينظر: شيماء عبد الغني، مرجع سابق، ص: 146- 147.

[3] ينظر: عصام عبد الفتاح مطر، مرجع سابق، ص: 360.

[4] نظراً لكثرة أصناف الجناة في إطار الجرائم الإلكترونية،التي يندرج ضمنها: صنف القراصنة، وصنف المتجسسون والإرهابيون، والعابثون، والموظفون وعدم اتساع المقام لسردها جميعاً فإننا سوف نقتصر على البعض لشيوعها. لمزيد من الإطلاع بالخصوص ينظر: محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، (د.ط) ، القاهرة: دار النهضة العربية، 1994، ص: 37 وما يليها.

[5] ينظر: ذات المرجع ، ص: 44.

ثانياً: الهواة:

هم من عشاق الأنشطة والألعاب الفكرية التي تستخدم فيها الآلة والمغرمين بالمجال الإعلامي, وغالباً ما يكون لديهم مستوى معرفي معين من تقنيات البرمجة والتعامل مع الحاسوب وهم بطبيعة الحال لا يعملون بمقابل بما أنهم غير محترفين.

والمجرم الهاوي قد يكون جهبذاً من ذوي القدرات الذهنية والعقلية الفائقة ومن ذوي الموهبة, وقد يكون من بين عامة الناس, غاية ما هنالك أنه يهوى ملاعبة الحاسوب فيأتي أفعالاً خطيرة من حيث لا يشعر, لا سيما أن جرائم الحاسوب لا تستدعي دائماً وفي كل الأحوال الذكاء الخارق ولا الدراية الكبيرة بل يكفي قدر متوسط من الذكاء لارتكابها.[1]

البند الثاني/ الدوافع الإجرامية.[2]

إن اختلاف صفات المجرم في الجرائم الإلكترونية عنه في إطار الجرائم التقليدية, يستتبع اختلاف الدوافع الإجرامية, وتتمثل الدوافع الأساسية الكامنة وراء الأعمال الإجرامية في نطاق الجرائم الإلكترونية في الآتي:

أولاً: الشغف بالإلكترونات:

الكثير من المجرمين في الميدان الإلكتروني تورطوا من حيث لا يدرون وأجرموا وهم يلعبون, هؤلاء استهواهم عالم الإلكترونات, وشغفهم حتى أصبحوا مدمنين.

وقد يدفعهم هذا الولع إلى إظهار تفوقهم إزاء التقنيات المستحدثة بحيث لا يكون الدافع هو الحصول على الربح المادي, وإنما الرغبة في تحدي الأنظمة التقنية للبرامج المعلوماتية وفك شفرتها بشكل غير مشروع, ويزداد هذا الدافع انتشاراً لدى صغار السن وتكون أداة الجريمة هي الحواسيب الشخصية حيث تكون أداة لكسر حواجز شبكة المعلومات.

ثانياً: الطمع في تكوين ثروة وبلوغ الرفاهية:

تحدث الكثير من الفقهاء على ما يسمى **"بالأموال المعلوماتية"** كصنف جديد من أصناف الأموال وحذر بعضهم من إمكانية تعرضها للاعتداء بحكم خصوصية طبيعتها وبحكم أهميتها في عالم اليوم.

ويكاد يجمع الباحثون والمحللون على أن دافع الاعتداء على المعلومات والحصول عليها هو الطمع في الحصول على الربح وتكديس الثروة, وهذه هي ميزة كل جرائم الأعمال تقريباً والجرائم الإلكترونية من ضمنها.

ثالثاً: دافع جمع المعلومات:

قد يكون الهدف لدى مجرمي الإنترنت الرغبة في الحصول على المعلومة وهم يعتمدون في ذلك على مبدأين؛ **الأول**: أن التطفل على أنظمة الحاسوب الآلي يجعل المتدخل مواكباً لآخر المستجدات والمعلومات. و**الثاني**: أن جمع هذه المعلومات لا يخضع لقيود ويسعون إلى التخصص وتقاسم البرامج والخبرات, بحيث يطبقون ما تعلموه في أنشطة هادفة ولكن بطرق غير قانونية.

المطلب الثاني
خصوصية إجرائية

تمهيد وتقسيم:

إن الطبيعة الخاصة للبيئة التقنية التي تتم فيها جرائم التجارة الإلكترونية انعكست على الجوانب الإجرائية لتتسم بطابع من الخصوصية يضفى عليها طابعاً من الذاتية إذا ما قورنت بإجراءات الدعوى في غيرها من الجرائم التقليدية(**فرع أول**), يتماشى مع طبيعة المعاملات الإلكترونية وتقنية إثباتها بالوسائل الرقمية **(فرع ثان).**

الفرع الأول/ قصور الإثبات بالوسائل التقليدية.

إن الطبيعة اللامادية للجريمة الإلكترونية تشكل تحدياً كبيراً في إطار إثباتها بالوسائل التقليدية سواء على مستوى المعانية والتفتيش والضبط (**بند أول**), أم على مستوى التحقيق(**بند ثان**) .

البند الأول / على مستوى المعاينة والتفتيش والضبط.

تتجلى أهم الصعوبات التي يثيرها اثبات الجرائم الإلكترونية بالوسائل التقليدية على مستوى المعاينة والتفتيش والضبط في الأتي:

أولاً: المعاينة:

عرف الفقه الجنائي المعاينة بأنها: **" رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"** [3], وفي مجال الجرائم الإلكترونية تظهر عدة صعوبات تحول دون فاعلية المعاينة أو فائدتها يمكن تلخيصها في عقبتين رئيستين:

الصعوبة الأولى: تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم الإلكترونية.[4]

---

[1] ينظر: ذات المرجع، ص: 39.

[2] ينظر: ذات المرجع، ص: 47 وما يليها.

[3] ينظر:خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، (ط1)، الإسكندرية: دار الفكر الجامعي، 2010، ص: 148.

[4] ينظر:هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، (د. ط)، أسيوط: مكتبة الآلات الحديثة، 1994، ص: 59.

الصعوبة الثانية: الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالباً ما تكون طويلة نسبياً, ما بين وقوع الجريمة والكشف عنها, الأمر الذي يسمح بحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها, وهو ما يلقي ظلالاً من الشك على الدليل المستمد من المعاينة.[1]

ثانياً: التفتيش:

يغلب على الوسائل المستخدمة لارتكاب الجريمة الإلكترونية الطابع الفني التقني, ويتطلب إثبات هذه الأخيرة اللجوء إلى الفنيين المختصين في هذا الصدد, أو لمأمور الضبط ذاته متى كان مؤهلاً للقيام بهذا العمل.

غير أن الأمر ليس بهذه السهولة, فالمشكلة تكمن في مجموعة الاجراءات والصعوبات العملية التي تعيق خضوع البيانات المخزنة آلياً لقواعد التفتيش التقليدية المنصوص عليها حسب القواعد العامة في قوانين الاجراءات الجنائية, بوصفها الأصل الذي يحكم هذه الاجراءات الجنائية, ومن هذه الصعوبات[2] :

- حالة وجود النظام المعلوماتي داخل أحد المساكن مع وجود النهاية الطرفية له في مكان آخر, الأمر الذي يعطي للجاني فرصة سانحة للتخلص من البيانات التي يستهدفها التفتيش.
- فيما يتعلق بإذن التفتيش فتبدو الصعوبة في هذا الصدد في اشتراط أن يكون هذا الإذن محدداً فيما يخص محله, والأشياء التي يهدف التفتيش إلى ضبطها, وهذا الشرط يتطلب أن يقوم مصدر الإذن بتحديد المواد المراد ضبطها بطريقة فنية, الأمر الذي لا يكون في مقدوره؛ لأنه يتطلب نوعاً من المعرفة الفنية يتجاوز في مداه الثقافة والمعرفة العامة أو السطحية للأمور, وهو ما قد يخرج عن الإمكانات الفنية المؤهل لها سلطة التحقيق أو سلطة مأموري الضبط القضائي.

وقد لجأ المشرع في دول عديدة إلى تقرير بعض القواعد القانونية بهدف التغلب على الصعوبات التي قد تثار عند تفتيش الأنظمة المعلوماتية. منها **كندا**, فيما يتعلق بصعوبة تحديد محل إذن التفتيش والأشياء التي يهدف إلى ضبطها, فيمكن الاعتماد في ذلك على صيغة إذن التفتيش الذي اعتمدته الشرطة التابعة للإدارة الأمنية لمركز المعلوماتية الكندي, والذي استخلصته من واقع خبراتها العملية.[3]

وفي **أمريكا** وبخصوص الصعوبة التي تتعلق بالدخول إلى أنظمة معلوماتية لضبط ما يعد صالحاً من هذه البيانات كدليل أو قرينة لارتكاب جريمة نص على جملة من الإجراءات يجب اتخاذها.[4]

ثالثاً: ضبط الأدلة الرقمية:

عُرف الضبط في البيئة الإلكترونية بأنه: " استخدام البرامج المهمة من أجل الولوج للبيانات المراد ضبطها إلى جانب وضع اليد على تلك الدعائم المادية" .[5]

ويواجه ضبط الأدلة المتحصل عليها في الجرائم الإلكترونية, التي تتميز بأنها ذات طبيعة معنوية عدة صعوبات إلا أنه - وحسبما لاحظ جانب من الفقه- أن المعضلة الأساسية تكمن في مأموري الضبط القضائي القائمين على ضبط دليل الجريمة المعلوماتية, فالأمر يتطلب تأهيل مأموري الضبط القضائي على كيفية التعامل مع جرائم الحاسب الآلي.

ولذلك اتجهت البلدان الأوروبية مثل كندا سنة 1980, وكذلك انجلترا سنة 1957, وفرنسا سنة1983, إلى إعطاء دورات تدريبية لمأموري الضبط القضائي عن كيفية تحقيق جرائم الحاسبات الآلية, وهو ما بدأت الدول العربية تطبيقه, منها مصر ودولة الإمارات العربية المتحدة, ونأمل أن يتم تطبيقه كذلك في الدول التي لم تنظم ذلك.[6]

البند الثاني/ على مستوى التحقيق.

تتميز إجراءات التحقيق في الجرائم الإلكترونية ببعض الخصوصية في طريقة اكتشافها, والتبليغ عنها, والعناية بمسرح الجريمة, وكيفية تكوين فريق الضبط, والتفتيش وخصوصية الأدلة المضبوطة.[7]

فاكتشاف الجرائم الإلكترونية – ومنها جرائم التجارة الإلكترونية- والتبليغ عنها يواجهه إشكال يتمثل في أن الجريمة الإلكترونية لا تصل إلى علم السلطات المعنية بالصورة العادية, وذلك لصعوبة اكتشافها بواسطة الأشخاص العاديين, حتى في المؤسسات المالية والشركات الكبرى لا يتم اكتشاف هذه الجرائم فور وقوعها .

إن الخصوصية التي تتميز بها هذه المرحلة – أي مرحلة تلقي البلاغ - هي أن يكون مصدر البلاغ على درجة من الوعي والقدرة والمعرفة بتفاصيل ما يدلي به من معلومات, ولا يصلح هنا كبلاغ يبرر تحريك الإجراءات

---

[1] ينظر: نبيلة هبه هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، (د.ط)، الإسكندرية: دار الفكر الجامعي، 2006، ص: 117.

[2] ينظر: عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية،(ط1)، الإسكندرية: منشأة المعارف، 2009، ص: 249.

[3] ينظر: هشام محمد فريد رستم، مرجع سابق، ص: 43.

[4] ينظر: نبيلة هبه هروال، مرجع سابق، ص: 225.

[5] ينظر: ذات المرجع، ص: 226.

[6] ينظر: عبد الفتاح بيومي، مرجع سابق، ص:280- 281.

[7] ينظر: ضياء علي أحمد نعمان ، الغش المعلوماتي، الظاهرة والتطبيقات، (ط1)، مراكش: المطبعة والوراقة الوطنية، 2011.، ص:363.

القول بأن هنالك جريمة إلكترونية وقعت, وإنما على المبلغ هنا أن يقدم وصفاً علمياً محدداً للنشاط الإجرامي, ومكان وقوعه, واللغات والبرامج وأنواع الأجهزة المستخدمة قدر المستطاع.

كما تبرز خصوصية إجراءات التحقيق في مجال الجرائم الإلكترونية في أنواع الأدلة المطلوبة, فالجريمة الإلكترونية كغيرها من الجرائم لها أركانها وعناصرها, وتمر بالمراحل التي تمر بها أية جريمة من مرحلة التفكير, والتخطيط, والتحضير, فالتنفيذ, ومن ثم إخفاء المعالم, والتخلص من الآثار.

فالاعتراف في الجرائم الإلكترونية سيد الأدلة, وشهادة الشهود مفيدة, ومطلوبة والقرائن تعضدها, وللآثار بمختلف أنواعها دورٌ في الإثبات ولكن هنالك بعض الأدلة التي لها قيمتها الخاصة في إثبات الجريمة الإلكترونية كالمحرر الإلكتروني وما يتميز به من خصوصيات.

الفرع الثاني / تقنية الإثبات بالوسائل الرقمية.

يمثل الإثبات الرقمي مجموعة البيانات والمعطيات التي يتم جمعها وحفظها بواسطة الأنظمة المعلوماتية أو الإلكترونية, والتي تكون صالحة للاستدلال بها أمام القضاء.

ومن أهم وسائل الإثبات الرقمي هو تقنية تتبع الآثار التي تتركها الجريمة في الفضاء الإلكتروني, والتي تعكس مرور الجاني من خلال العلامات أو البصمات التي يتم رصدها(**بند أول**) والسندات الإلكترونية (**بند ثان**).

البند الأول/ الدليل الرقمي.

يعرف الدليل الرقمي أو الإلكتروني بأنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل نبضات مغناطيسية, أو كهربائية يمكن تجميعها باستخدام برامج تكنولوجية وهي مكون رقمي لتقديم معلومات متنوعة في أشكال متنوعة من النصوص أو الصور وذلك ليتم اعتمادها أمام الجهاز القضائي.[1]

والأدلة الرقمية قد تتمثل في سجلات الكمبيوتر, ومعلومات الدخول, والاشتراك, والنفاذ والبرمجيات, ويثير هذا النوع من الأدلة إشكاليات عديدة من حيث قبولها وحجيتها لدى المحاكم.

<u>ويوجد نوعان من الأدلة الرقمية, أحدهما ذا صلة بالكمبيوتر والآخر ذا صلة بشبكة الإنترنت</u>.

<u>أولاً: الأدلة الرقمية ذات الصلة بالكمبيوتر.</u>

وتشمل:السجلات المحفوظة في الكمبيوتر والوثائق المكتوبة مثل: صفحات المواقع المختلفة (**Web pazes**), والبريد الإلكتروني (**email**),والصور المرئية (**Digitized still image**) , والفيديو الرقمي(**Fils shored on personal computer**)، والملفات المخزنة في الكمبيوتر الشخصي.[2]

<u>ثانياً: الأدلة الرقمية ذات الصلة بالإنترنت.(بروتوكول ICP/IP)</u>

يعتبر هذا البرتوكول من أشهر البروتوكولات المستخدمة في شبكة الإنترنت, وهي تدل بصفة أكيدة على مصدر الجهاز المستخدم في الجريمة وتحديد الأجهزة التي أصابها الضرر جراء ارتكاب الفعل الإجرامي, حيث يحتوي هذا البروتوكول على كافة المعلومات والبيانات المتعلقة بالفعل الإجرامي, إلا أن الإشكاليات العملية المترتبة على قانونية هذا الأسلوب تثير اشكالية مدى حجيتها أمام أجهزة العدالة الجنائية.

البند الثاني/ السندات الإلكترونية.

في إطار تعريف السندات الإلكترونية قامت لجنة الأمم المتحدة للقانون التجاري الدولي (CNUDCI) بمبادرة بقصد تشجيع الدول على تجاوز العراقيل التي قد تقف أمام المراسلات الإلكترونية كوسيلة إثبات, وقد صدر القانون النموذجي الخاص بالتجارة الإلكترونية والذي حدد مفهوم السند الإلكتروني بحيث يأخذ تعريفاً للكتابة في الواقع أياً كان السند التي تتجسد فيه.

كما عرف المشرع الفرنسي السند الإلكتروني بشكل يتلاءم مع تطور تكنولوجيا المعلومات يستوعب جميع أشكال الكتابة, ومن ضمنها شكلها الإلكتروني وذلك بقطع النظر عن السند المادي الذي يحملها وطريقة نقلها.[3]

ويتسم السند الإلكتروني بالعديد من الخصوصيات لا تتوافر في السند التقليدي, أبرزها استخدام لغة ثنائية في إنشائه وإرساله برموز إلكترونية لا يمكن قراءتها مباشرة, ويجب فك ترميزها كي يتمكن الإنسان من قراءتها.

أيضاً عدم وجود دعامة مادية للمستند الإلكتروني, بعكس المستند التقليدي المودع عادةً على دعامة ورقية, وكذلك وجود بيانات وصفية والتي هي عبارة عن بيانات تقنية عن المحررات الإلكترونية غالباً ما تكون مخفية.

كما تتميز السندات الإلكترونية بعدم الارتباط ببنية محددة, نظراً لكون بنيتها معقدة وغير مرئية للمستخدم, كما أنها تدخل في إطار ما يسمى (**البنية المنطقية**) للمحرر, بخلاف السندات التقليدية التي لها بنية مادية ملموسة ومرئية بالنسبة للمستخدم, فهي جزء كامل صحيح من أية وثيقة ورقية, وهي أحد المعايير الأساسية لتقييم موثوقيتها وتقديم الدليل على أنها أصلية.[4]

---

[1] ينظر: ذات المرجع ، ص: 283.

[2] ينظر: خالد ممدوح إبراهيم، مرجع سابق، ص: 275.

[3] ينظر: عز الدين بن عمر، العقد الإلكتروني بين زوال السند المادي عند إبرامه والآثار اللامادية لتنفيذه، ، مجلة القضاء والتشريع ، تصدر عن مركز الدراسات القانونية والقضائية، تونس، ع1،س40، 2001، ص: 96.

[4] ينظر: تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت، (ط1)، الإسكندرية: منشأة المعارف، 2009،ص: 159 وما يليها.

المبحث الثاني
متطلبات المواجهة التشريعية لجرائم التجارة الإلكترونية

تمهيد وتقسيم:

إن جرائم التجارة الإلكترونية لا تقف عند حد معين, بل هي متجددة ومتطورة لوقوعها في نطاق عالم تقني متجدد ومتطور لا يكف عما هو جديد, الأمر الذي يقتضي أن تتم مواجهتها بشكل خاص سواء على مستوى القواعد الموضوعية(**مطلب أول**),أم على مستوى القواعد الإجرائية(**مطلب ثان**).

المطلب الأول
على مستوى القواعد الموضوعية

تمهيد وتقسيم:

سنتطرق لتوضيح متطلبات المواجهة التشريعية لجرائم التجارة الإلكترونية على مستوى القواعد الموضوعية من خلال ضرورة التنظيم التشريعي الخاص لجرائم التجارة الإلكترونية (**فرع أول**), والمعطيات التي يجب مراعاتها لتحقيق حماية جنائية ناجعة(**فرع ثان**).

الفرع الأول/ التنظيم التشريعي الخاص لجرائم التجارة الإلكترونية.

إن مكافحة جرائم التجارة الإلكترونية والتصدي لها يتطلب ضرورة تجريمها بنصوص خاصة لتحقيق الحماية المنشودة التي يسعى إليها المشرع(**بند أول**), مع مراعاة معطيات معينة تقتضيها خصوصية المواجهة لهذا النمط المستحدث من الإجرام (**بند ثان**) .

البند الأول/ ضرورات التجريم بنصوص خاصة.

إن التصدي للجرائم الإلكترونية- بشكل عام – وجرائم التجارة الإلكترونية - بشكل خاص- يتطلب التجريم بنصوص خاصة تتلاءم مع طبيعتها التقنية, ومن ثم فإن الدول التي لم تقم إلى الآن بتنظيم تشريعي خاص لهذه الجرائم, تجد صعوبة في التصدي لها ومكافحتها؛ وذلك لعدة أسباب منها:

أولاً:عدم كفاية القواعد الجنائية التقليدية لحماية المعاملات التجارية الإلكترونية, خاصة في إطار انطباق الأحكام العامة في جرائم الأموال(السرقة,النصب, خيانة الأمانة)على جرائم التجارة الإلكترونية.

وقد أكد أغلب ممثلي الدول المشاركة في الملتقى التحضيري الذي نظمته الجمعية العالمية للقانون الجنائي سنة 1992 بمدينة **Wurtzbourg** الألمانية عدم كفاية النصوص الجنائية بقوانينهم الوطنية للتصدي للجرائم الإلكترونية, لا سيما أن هذه النصوص قد وضعت في فترة لم تكن فيها تقنية الإنترنت قد ظهرت ولم تبرز الإشكاليات القانونية الناشئة عنها.[1]

ثانياً: الاختلاف في التفسير بين المحاكم عندما يتعلق الأمر بتطبيق القواعد العامة في جرائم الأموال في نطاق المعاملات الإلكترونية.

ثالثاً: التغرات القانونية التي قد تظهر عند تطبيق القواعد الجنائية التقليدية في نطاق المعاملات الإلكترونية – ومنها التجارية- وذلك بسبب طبيعتها الخاصة.

البند الثاني/ فاعلية التجريم بنصوص خاصة في تحقيق الحماية المنشودة.

نظراً لانتشار التعاملات من خلال الإنترنت وتزايد التجارة الإلكترونية, فقد أدركت العديد من الدول أهمية إصدار تشريعات خاصة لمواجهة جرائم التجارة الإلكترونية, **منها على مستوى الدول الأجنبية**: انجلترا, حيث صدر قانون التجارة الإلكترونية سنة 2002, كما أصدرت الولايات المتحدة الأمريكية قانوناً خاصاً بالتجارة الإلكترونية سنة 2001, وكذلك فرنسا سنة 2000, وسنغفورة سنة 1998, واليابان سنة 2000.[2]

أما على مستوى الدول العربية, فقد كان للمشرع التونسي فضل السبق في إصدار قانون خاص بالتجارة الإلكترونية, هو القانون رقم (83) لسنة 2000 الصادر في أغسطس سنة 2000 بشأن المبادلات والتجارة الإلكترونية, كذلك أصدرت إمارة دبي في دولة الإمارات العربية المتحدة القانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية, وفي مصر صدر القانون رقم (15) في شأن تنظيم التوقيع الإلكتروني وإنشاء هيأة تنمية صناعة تكنولوجيا المعلومات بتاريخ 22/ 4/ 2004, وتم إعداد مشروع للتجارة الإلكترونية سنة 2000.[3]

وفي ليبيا, على الرغم من صدور مشروع قانون مكافحة الجرائم الإلكترونية سنة 2018, الذي تم اعتماده سنة 2021, إلا أن الأمر يتطلب بذل مزيد من الجهود في إطار مكافحة هذا النمط المستحدث من الإجرام خاصة في نطاق التجارة الإلكترونية.

إن المعالجة التشريعية الخاصة للجرائم الإلكترونية بشكل عام, وجرائم التجارة الإلكترونية بشكل خاص لها أثر كبير في التصدي لها والوقاية من مخاطرها, وإن كانت لا تصل إلى درجة الكفاية في القضاء عليها بشكل نهائي

[1] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، (د.ط)، الإسكندرية: مطابع أبو الخير، 2010، ص: 34.

[2] ينظر: عصام عبد الفتاح مطر، مرجع سابق، ص: 117- 118.

[3] ينظر: شيماء عبد الغني ، مرجع سابق، ص: 7.

– وهو أمر غير متصور حدوثه أيضاً في إطار الجرائم التقليدية - إلا أنها خطوة يحمد لها على أقل تقدير إقرار مبدأ الشرعية الجنائية في إطار الأفعال التي تشكل خطراً على المعاملات الإلكترونية, ومن ثم مواجهة أي تأويل قد يبيحها خاصة في ظل الصعوبات القانونية الناشئة عن تطبيق القواعد الجنائية التقليدية في نطاق المعاملات الإلكترونية.

الفرع الثاني / مراعاة المعطيات اللازمة لتحقيق حماية ناجعة.

إن المواجهة التشريعية الفاعلة لجرائم التجارة الإلكترونية تتطلب – إضافة إلى التجريم بنصوص خاصة- مراعاة معايير معينة في التجريم و العقاب(**بند أول**), وتوظيف التقنيات الحديثة في إطار مكافحة هذه الجرائم (**بند ثان**).

البند الأول/ تحديد معايير التجريم والعقاب.

لابد من توافر بعض المعايير في التجريم كي تكون العقوبة الجنائية هي الحل الأمثل لتحقيق الحماية المطلوبة, والتي نرى تحديدها في إطار الجرائم محل البحث بما يلي:

أولاً: خطورة ما أتاه الفاعل: كي تحقق العقوبة الجنائية غايتها, يجب أن لا تتدخل إلا في الظروف التي تظهر درجة معينة من خطورة الفاعل؛ أي تلك التي تعبر عن فكر سيء النية, لا يستخدم التعاملات الإلكترونية إلا من أجل الحصول على فائدة غير مستحقة.

ثانياً: حجم الضرر وعدد الضحايا: بما أن العقوبة الجنائية تتميز بالخطورة مقارنة مع سائر أنواع العقوبات, لما لها من تأثير يطال الشخص المفروضة عليه, لذلك يجب أن تفرض بخاصة في حال التصرفات غير المشروعة التي ينتج عنها ضرر كبير يطال المجتمع, أو ضرر يطال عدداً كبيراً من الضحايا, خاصة وأن الإجرام المتعلق بالتجارة الإلكترونية يظهر خطوطاً مميزة تتمثل بأن أفعاله ليست مستقلة وإنما مرتبطة بحجم السوق, وتدخل بعض جرائمه في خانة الجرائم الجماعية كون ضررها يمتد إلى عشرات إن لم نقل مئات الأشخاص لينتج عن كل جريمة عدد كبير من الضحايا. وذلك سعياً لتحقيق التوازن بين الفعل المرتكب, والعقوبة المفروضة عليه, بما يؤمن حماية جنائية فعالة.

ثالثاً: جهاز تشريعي متناسق: إن تحقيق العقوبات الجنائية لغرضها الحمائي يتطلب تنظيمها من خلال إنشاء جهاز تنظيم متناسق ومتلائم,وقد يصار إلى ذلك من خلال تنسيق الجرائم وتوفيقها, إضافة إلى وجوب تناغم العقوبات الأساسية والإضافية في إطار الجرائم ذات الطبيعة الواحدة, فمن شأن عدم التنسيق الحد من فاعلية العقوبة, إذ إن مبدأ استمرار القاعدة الجنائية موضوع بخطر, ومن الضروري استكمال النصوص القانونية بلوائح تطبيقية يكون من شأنها تحديد دقائق الأمور, ووضع الأسس الواجب الالتزام بها عند تطبيق النصوص القانونية.

البند الثاني/ توظيف التقنيات الحديثة في مكافحة الجرائم الإلكترونية.

تتعدد وسائل المكافحة التقنية للجرائم الإلكترونية وطرقها, ويأتي في مقدمتها التشفير وبرمجيات كشف الفيروسات .

أولاً: التشفير:

تعد هذه التقنية الوسيلة الأكثر نجاعة لتحقيق وظائف الأمن الثلاثة وهي: السرية , والتكاملية, وتوفير المعلومات.

إن ضمان سرية المعلومات يرتكز على تشفير الملفات والمعطيات وترميزها[1], ويعد التشفير وفي مقدمته التوقيع الإلكتروني تقنية للتثبت عند فكه أن الرسالة الإلكترونية لم تتعرض لأي نوع من التعديل أو التغيير, ويوجد نوعان من التشفير؛ **التشفير التماثلي**: ويعتمد على مفتاح واحد في التشفير أو الفك, وهو ما يستوجب إحالة المفتاح بين الأطراف بطريقة سرية تضمن سلامته, و**التشفير اللاتماثلي**: يعتمد على مفتاحين مترابطين, هما: مفتاح خاص لا يعلمه إلا المعني به, ومفتاح عام وهو معلوم من طرف جميع المتعاملين.

ثانياً: برمجيات كشف الفيروسات:

تعد تقنيات مضادات الفيروسات الأكثر انتشاراً, وهي من وسائل الأمن المتداول في البيئة المعلوماتية, وتوجد عدة أنواع من البرمجيات المخصصة لمكافحة الفيروسات, منها: برمجيات الجدران النارية, والشبكات الافتراضية الخاصة.[2]

وتتمثل برمجيات الجدران النارية الحديثة في إنشاء الشبكات الافتراضية الخاصة ومراقبة محتوى البيانات والوقاية من الفيروسات وإدارة نوعية الخدمة, وهي جدران تقع على طرف الشبكة, وبرزت مؤخراً الجدران النارية الخاصة التي لا تحتاج إلى إعداد من قبل المستخدم حيث يمكن استعمالها دون أي تعديلات على نظام التشغيل. كما ظهر برنامج حماية يسمى " **منطقة الإنذار بالخطر**", وهو من أنجع برامج الحماية؛ حيث يوفر

---

[1] ينظر: حسن الجهاد، المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، جامعة الامارات، 2000، ص: 3.

[2] **فيروسات الحاسب الآلي**: هي عبارة عن خلية كهرومغناطيسية نائمة ومبرمجة بحيث تنشط في وقت محدد لتخريب البرنامج الأصلي، وتنتشر في الأجهزة الأخرى التي تضمنها الشبكة بحيث تفسد ما تحويه من معلومات. ينظر: محمد سامي الشوا، مرجع سابق، ص: 189.

حماية قصوى للأنظمة المعلوماتية, بتشكيل جدار ناري افتراضي يتم وضعه بين القرص الثابت لجهاز الكمبيوتر والإنترنت, فينبه المستخدم بكل محاولة ربط بالإنترنت مما يمكن مستعمل الكمبيوتر من قبول أو رفض النفاذ إلى الشبكة.

المطلب الثاني
على مستوى القواعد الإجرائية

تمهيد وتقسيم:

إن المواجهة التشريعية لجرائم التجارة الإلكترونية, لا تقتصر فقط على الجانب الموضوعي, وإنما تتطلب أيضاً تنظيماً إجرائياً خاصاً سواء في مرحلة الاستدلال(**فرع أول**), أو في مرحلة التحقيق(**فرع ثان**), أو في إطار الإثبات (**فرع ثالث**).

الفرع الأول/ النص على ضبطية قضائية خاصة بالجرائم الإلكترونية.

يقع على عاتق الأجهزة الإجرائية دورٌ مهمٌ في مواجهة الجريمة الإلكترونية, وهو أمر قد تعجز الضبطية العادية عن الاضطلاع به, ويمكن حصر أسباب ذلك في الآتي:

أولاً: أسباب مرتبطة بالجريمة موضوع المخالفة:

- إن الجرائم الإلكترونية من الجرائم المستحدثة التي تستخدم فيها التقنية العالية, كما أنها من الجرائم العابرة للحدود,والتي يصعب اكتشافها أو تحديد مصدرها, خاصة في حالة ارتكابها عن بعد من داخل دولة أجنبية, وصعوبة إيقافها بالنظر إلى سرعة انتشار المعلومات وتسجيلها أوتوماتيكياً على الحاسبات الخادمة الموجودة في الخارج, وهذا يستلزم أن يكون مأمورو الضبط القضائي المضطلعين بضبط هذه الجرائم والتحري عنها مكونين تكويناً علمياً وتكنولوجياً, حتى يتمكنوا من فهمها والكشف عنها وملاحقة مرتكبيها.[1]
- إن هذه الجرائم لها طبيعة خاصة وأدلتها غير محسوسة نظراً لعدم وجود أي وثائق ورقية متبادلة في إجراء وتنفيذ المعاملات الإلكترونية, حيث إن كافة عمليات التفاعل بين طرفي المعاملة تتم إلكترونياً دون استخدام أي ورق, وبالتالي تصبح الرسالة الإلكترونية هي السند القانوني الوحيد المتاح لكلا الطرفين. لذلك فهي تحتاج إلى خبرة فنية وتقنية عالية حتى تتعامل مع هذه الخواص الجديدة والبيئة المعلوماتية والعاملين والمتعاملين فيها.[2]
- إن التحري والتحقيق في الجرائم الإلكترونية يحتاج إلى استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبها, وكيفية ارتكابها مع الاستعانة بوسائل جديدة كذلك لضبط الجاني والحصول على أدلة إدانته. خاصة و أن المجرم الإلكتروني هو مجرم ذو طبيعة خاصة يتعين تفهم كيفية التعامل معه.وهو أمر يفتقر إليه أعضاء الضبط القضائي العاديين.[3]

ثانياً: أسباب مرتبطة بالنصوص المتصلة بموضوع الجريمة منها السرعة والنجاعة التي تسعى إليها هذه النصوص, وكذلك التخصيص الذي تجنح إليه دائماً كسبيل لتحقيق فعاليتها.

الفرع الثاني/ تذليل معوقات التحقيق الابتدائي في الجرائم الإلكترونية.

يتسم التحقيق في الجرائم الإلكترونية, وملاحقة مرتكبيها جنائياً بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق, ومن أهم هذه المعوقات:

أولاً: عوائق تتعلق بالجريمة الإلكترونية[4]:

- خفاء الجريمة, وغياب الدليل المرئي الممكن بالقراءة فهمه.
- افتقاد أكثر الأدلة التقليدية.
- إعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية, كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها, أو ترميزها, أو تشفيرها.
- سهولة محو الدليل أو تدميره في زمن قصير جداً.

ثانياً: عوائق تتعلق بجهات التحقيق[5]:

- بعض هذه المعوقات ترجع إلى شخصية المحقق, مثل التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الإنترنت, بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.
- والبعض الآخر يتعلق بالنواحي الفنية, كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم, ونقص المهارة في استخدام الكمبيوتر والإنترنت.

ثالثاً: عوائق تتعلق بإجراءات الحصول على الدليل الإلكتروني نذكر منها:

[1] ينظر: نبيلة هبه هروال، مرجع سابق، ص: 11.
[2] ينظر: تامر محمد سليمان الدمياطي، مرجع سابق، ص:102 - 103.
[3] ينظر: هشام محمد فريد رستم، قانون العقوبات والمعلوماتية، (د. ط)، القاهرة: دار النهضة العربية، 2005، ص: 94.
[4] ينظر: خالد ممدوح إبراهيم، مرجع سابق، ص: 65.
[5] ينظر: ذات المرجع ، ص:69.

- اعتبارات المعرفة الأساسية لكل من الضابط, والمحقق لماهية الجرائم المعلوماتية, وهل ما قام به يعد جريمة في قانون الدولة التي ينتمون إليها من عدمه, وكذلك قانون الدولة المتواجد بها المشتبه فيه الأمر الذي تنشأ عنه مشكلة أخرى, هو كيفية الحصول على الدليل عبر الحدود, وربما يكون ذلك الدليل غير قائم بالفعل وكيفية اكتشاف الجريمة, وما يجب أن يكون عليه أعضاء النيابة من الدراية الكافية لمعرفة البدء في التحقيقات, وهذا ما يطلق عليه " **الوضع المناسب و الإشارة الصحيحة**" فإذا لم تحدد الجريمة, ولم يتم التحفظ على الدليل, فإن الأثر المباشر لهذا هو عدم وجود الجريمة.[1]
- لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها فحسب, وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة, فإذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة, والتتبع والمساعدة, فمن الصعب عليها التحري بهذه الطرق بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية.

الفرع الثالث/ الاعتراف بحجية الأدلة الإلكترونية.

إن الاعتراف بحجية الأدلة الإلكترونية يعتمد بدرجة كبيرة على مدى المعالجة التشريعية, ومع ذلك فإنه يمكن أن نلمس تطوراً في مجال الاعتراف بحجية للأدلة الإلكترونية في الإثبات من خلال الطرح الآتي:

أولاً: شروط قبول الأدلة الإلكترونية:

أثيرت في فرنسا مشكلة الإثبات لمحاضر المخالفات التي تتم عن طريق جهاز السينموتر, وانتهى القضاء هناك إلى عدم اعتبار محاضر المخالفات المحررة بإثبات المخالفة حجة بذاتها في الإثبات, وإنما ذهب كل من الفقه والقضاء إلى أن أي محضر لا تكون له قوة إثبات إلا إذا أثبت فيه محرره وقائع تدخل في اختصاصه, وأن يكون شاهدها, أو سمعها, أو تحقق منها بنفسه.[2]

ولذلك يمكن القول بأن المخرجات المتحصلة من الوسائل الإلكترونية لا تمثل مشكلة في النظام اللاتيني, حيث يسود مبدأ حرية القاضي الجنائي في الاقتناع.

كما أثار قبول الأدلة المتحصلة من الوسائل الإلكترونية مشكلات عديدة في ظل القواعد الأنجلو أمريكية للإثبات الجنائي, التي تعتنق مبدأ أساسياً الإثبات بالشهادة التي تتعلق بالواقعة محل الإثبات , لذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإلكترونية يجعلها بمثابة أدلة ثانوية وليست أصلية.[3]

وقد صدر في **انجلترا** قانون للإثبات الجنائي سنة 1984, وعمل به بدءاً من سنة 1986.[4]

ونشير إلى أن مخرجات الوسائل الإلكترونية تقبل كوسائل إثبات في **الولايات المتحدة الأمريكية**, وذلك بالنسبة للبرامج والبيانات المخزنة فيها, وبالنسبة للنسخ المستخرجة من البيانات التي يحتويها الحاسب الآلي.[5]

ثانياً: حجية السندات الالكترونية في الإثبات:

نظراً للطبيعة الخاصة للكتابة الإلكترونية, ولكونها أصبحت واقعاً ملموساً لا يمكن تجاهله لانتشار هذه السندات بسبب التطور الهائل في وسائل الاتصال الفوري, فإن تشريعات العديد من الدول المعاصرة تدخلت لتأخذ بالمفهوم الواسع للكتابة.

ففي الولايات المتحدة الأمريكية, صدرت استثناءات منحت بموجبها قواعد الإثبات تفسيراً واسعاً ومتطوراً يراعى فيه اعتماد وسائل التقنية الحديثة التي طرحها التطور التكنولوجي, ومن هذه الاستثناءات ما نصت عليه المادة (803) من قانون الإثبات الفيدرالي, واستقر القضاء على تسميتها باستثناء "السندات التجارية" واعتماداً على هذه الاستثناءات يمكن قبول السندات الإلكترونية في الإثبات بوصفها مساوية في الحجية للأدلة الكتابية التقليدية.[6]

أما في فرنسا ولما كانت حجية السندات الإلكترونية بموجب أحكام قانون 1980 حجية ناقصة, ولم تعد تنسجم مع متطلبات التطور التكنولوجي المتسارع , فقد تدخل المشرع لتعديل قواعد الإثبات, فصدر التعديل التشريعي في 13/ 3/ 2000 والمعدل لنص المادة (1316) من القانون المدني الفرنسي, حيث أعاد المشرع صياغة نص المادة لتستوعب كل صور الكتابة, سواء أكانت بالأساليب التقليدية أم الإلكترونية. و أورد فقرة جديدة لنص المادة تتعلق بالسند الإلكتروني بجعله مساوياً في الإثبات للسند المكتوب.[7]

---

[1] ينظر: ذات المرجع ، ص: 74.

[2] ينظر: جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، (د. ط)، القاهرة: دار النهضة العربية، 2002، ص: 29.

[3] ينظر: خالد ممدوح إبراهيم، الجرائم المعلوماتية، (ط1)، الإسكندرية: دار الفكر الجامعي،2009.، ص: 193.

[4] ينظر: محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، مجلة الحقوق، ، تصدر عن مجلس النشر العلمي، جامعة الكويت، ع2، س36، 2012، ص: 526.

[5] ينظر: خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص:194.

[6] ينظر: ذات المرجع ، ص: 117.

[7] ينظر: هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، (د.ط) ، القاهرة: دار النهضة العربية، 2000، ص72.

وفي مصر دعت الحاجة إلى إصدار قانون لتنظيم التوقيع الإلكتروني والإثبات عن طريق المحررات الإلكترونية, فأصدر المشرع القانون رقم (15) لسنة 2004 بشأن تنظيم التوقيع الإلكتروني, وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ولائحته التنفيذية الصادرة بقرار وزير الاتصالات وتكنولوجيا المعلومات رقم (109) لسنة 2005 [1], إلا أن هذا القانون لم يواجه كافة الصعوبات والمسائل التي تواجه اعتبار المحرر الإلكتروني دليلاً كتابياً كاملاً في الإثبات على قدم المساواة مع المحرر الورقي, إذ يظل من اللازم مواجهة بعض المسائل التقليدية التي قد تثير صعوبات لدى تطبيقها على المحررات الإلكترونية باعتبار أنها وضعت في وقت سادت فيه الكتابة على دعامة ورقية.

[1] ينظر: شيماء عبد الغني، مرجع سابق، ص: 80.

الخاتمة

لقد خلصنا من بحثنا لموضوع **جرائم التجارة الإلكترونية " الخصوصية ومتطلبات المواجهة التشريعية" بجملة من النتائج والتوصيات نوردها فيما يأتي:**

✓ **النتائج:**

أولاً: تميزت الجرائم الإلكترونية - ويدخل في نطاقها جرائم التجارة الإلكترونية- بخصوصية فنية وتقنية ناتجة عن ارتباطها بالتكنولوجيا الرقمية, ووقوعها في نطاق العالم الافتراضي, وقد شكل ذلك تحدياً كبيراً في مجال مكافحتها والحد من آثارها.

ثانياً: إن القواعد الجنائية التقليدية غير كافية لمواجهة هذا النمط المستحدث من الإجرام, خاصة في ظل الصعوبات القانونية التي أفرزها التطبيق العملي لهذه النصوص في نطاق الجرائم الإلكترونية.

ثالثاً: إن مكافحة الجرائم الإلكترونية بشكل عام, وجرائم التجارة الإلكترونية – بعدها سليلة هذا الصنف- بشكل خاص, مرتبط بدرجة كبيرة بالمعالجة التشريعية لهذا التطور التقني, فلئن كان عنصر التطور حقيقة ملموسة تشهدها أغلب دول العالم وستعم حتماً بقية الدول الأخرى عاجلاً أم آجلاً تأسيساً لحضارة الحاسوب والإنترنت, فإن عنصر الضمانات هو الذي بقي تحت المجهر ترتب بمقتضاه درجة نجاعة الأنظمة القانونية, وتحدد بموجبه مصير التجارة الإلكترونية بين النجاح و الفشل.

رابعاً: إن أطر التقنية لم تحظ إلى الآن بتنظيم تشريعي أو حتى لائحي يحدد – على الأقل- حداً أدنى من القواعد المنظمة لعمل مقدمي خدمات الإنترنت, ويضع نظاماً خاصاً لمسؤوليتهم المدنية أو الجنائية, على غرار ما فعل المشرع في الدول المتقدمة.

خامساً: تعقد وسائل الإثبات الخاصة بالجرائم الإلكترونية مقارنة بوسائل الإثبات التقليدية, والتي أصبحت تأخذ شكلاً لا مادياً أو إلكترونياً بعيداً عن المفهوم التقليدي للكتابة والوثائق المادية والورقية.

✓ **التوصيات:**

أولاً: لما كان التدخل التشريعي تقنية أكثر منه هدفاً, فإن هذه التقنية تصعب إذا ما تعلق الأمر بتنظيم على درجة عالية من التطور والتقنية, وهو في إطار بحثنا " التجارة الإلكترونية" التي نأمل بخصوصها ما يلي:

- أن تعمل الدول كافةً والعربية خاصةً على تطوير قوانينها بصورة مستمرة في مواجهة الجرائم المستجدة بفعل التكنولوجيا المعلوماتية.
- إيلاء الاهتمام بالعمليات التجارية التي تتم عبر الإنترنت والتوعية بشأن هذا النمط المستجد في إطار التعاملات التجارية بما يحمله من خصوصية لجهة الوسيلة التي يتم بها- عن بعد- بما يفترض هذا البعد من جوانب خاصة بتنفيذ الالتزامات الناشئة عن هذا التعامل.
- استحداث نظام قانوني متكامل يكفل المواجهة الجنائية الفاعلة لكافة التجاوزات التي أفرزتها ثورة تكنولوجيا الاتصالات والمعلومات, والتي شكلت منعطفاً خطيراً في جوانب الحياة الانسانية كافة في خضم عالم افتراضي, لا يعترف بالضوابط ولا يمكن فرض حدود عليه.
- اعتماد وسائل الإثبات الإلكترونية, وحماية جميع المتعاقدين بهذه الوسائل وضمان سلامة المعاملات الإلكترونية من خلال الاعتراف بالقيمة القانونية للسندات الإلكترونية, وإسنادها الحجية القانونية الحرية بها.

ثانياً: ضرورة تكثيف التعاون الدولي في مجال مكافحة الجرائم الإلكترونية, وعقد الاتفاقيات الدولية للتعاون القضائي في مرحلة التحقيق والمحاكمة والاعتراف بالأحكام الأجنبية وكذلك تسهيل تسليم المجرمين في هذا المجال.

ثبت المراجع

أولاً/الكتب القانونية المتخصصة:

1- تامر محمد سليمان الدمياطي, إثبات التعاقد الإلكتروني عبر الإنترنت,(ط1), الإسكندرية: منشأة المعارف, 2009.

2- جميل عبد الباقي الصغير, الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, (د.ط), القاهرة: دار النهضة العربية, 2002.

3- خالد ممدوح إبراهيم, فن التحقيق الجنائي في الجرائم الإلكترونية, (ط1), الإسكندرية: دار الفكر الجامعي, 2010.

- ــ, الجرائم المعلوماتية,(ط1),الإسكندرية: دار الفكر الجامعي,2009.

4- شيماء عبد الغني محمد عطا الله, الحماية الجنائية للتعاملات الإلكترونية, دراسة مقارنة,(د.ط),(د.م.ن):برلين للطباعة, 2013.

5-ضياء علي أحمد نعمان , الغش المعلوماتي, الظاهرة والتطبيقات, (ط1), مراكش: المطبعة والوراقة الوطنية, 2011.

6-عبد الفتاح بيومي حجازي, الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية,(ط1), الإسكندرية: منشأة المعارف, 2009.

7-عصام عبد الفتاح مطر, التجارة الإلكترونية في التشريعات العربية والأجنبية , (د.ط), الإسكندرية, دار الجامعة الجديدة , 2009.

8-غنام محمد غنام, دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت, (د.ط), الإسكندرية: مطابع أبو الخير, 2010.

9- محمد سامي الشوا, ثورة المعلومات وانعكاساتها على قانون العقوبات, (د.ط) , القاهرة: دار النهضة العربية, 1994.

10- محمد فهمي طلبة, فيروسات الحاسب وأمن البيانات, (د.ط), القاهرة: مطابع المكتب المصري الحديث, 1992.

11- نبيلة هبه هروال, الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات, (د.ط), الإسكندرية: دار الفكر الجامعي, 2006.

12- هشام محمد فريد رستم, الجوانب الإجرائية للجرائم المعلوماتية, (د.ط), أسيوط: مكتبة الآلات الحديثة, 1994.

- ــ, قانون العقوبات والمعلوماتية,(د.ط), القاهرة: دار النهضة العربية, 2005.

13- هدى حامد قشقوش, جرائم الحاسب الإلكتروني في التشريع المقارن, (د.ط), القاهرة: دار النهضة العربية , 1992.

- ــ, الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت, (د.ط), القاهرة: دار النهضة العربية, 2000.

ثانياً/البحوث والمقالات:

1- حسن الجهاد,المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية, بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت, جامعة الامارات, 2000.

2- عز الدين بن عمر,العقد الإلكتروني بين زوال السند المادي عند إبرامه والآثار اللامادية لتنفيذه,مجلة القضاء والتشريع, تصدر عن مركز الدراسات القانونية والقضائية, تونس, ع1,س40, 2001.

3- محمد أحمد المنشاوي, سلطة القاضي الجنائي في تقدير الدليل الإلكتروني, مجلة الحقوق, , تصدر عن مجلس النشر العلمي, جامعة الكويت, ع2, س36, 2012.

4- محمد أمين البشري,التحقيق في جرائم الحاسب الآلي والإنترنت, المجلة العربية للدراسات الأمنية والتدريب, تصدرها أكاديمية نايف للعلوم الأمنية, الرياض, مج 15, ع 30, س15, 2000.

ثالثاً/المراجع الإلكترونية:

1- بدر منشيف, حماية المستهلك في العقد الإلكتروني, المجلة العربية للدراسات القانونية والاقتصادية والاجتماعية,المغرب,(ط1),2020. منشورة على الموقع الإلكتروني drive . google. Com.