ISSN : 2543-3938 - EISSN : 2602-7771

صعوبات التحقيق في الجرائم الالكترونية

Difficulties in investigating cyber-crimes

ط.د. عماد بلغيث [1]*، أ.د. جغلولي يوسف [2]

[1] مخبر سوسيولوجية جودة الخدمة العمومية، جامعة محمد بوضياف المسيلة (الجزائر)،
imad.belghit@univ-msila.dz

[2] مخبر سوسيولوجية جودة الخدمة العمومية ، جامعة محمد بوضياف المسيلة (الجزائر)،
youcef.djaghlouli@univ-msila.**dz**

تاريخ الإستلام: 25/ 08/ 2021 **تاريخ القبول**: 20/ 09/ 2021 **تاريخ النشر**: 30/ 09/ 2021

ملخص:

تعتبر الجريمة الالكترونية من الجرائم الخطيرة التي ظهرت في العصر الحديث وأصبحت تشكل مشكلة كبيرة للدول بصفة عامة والافراد بصفة خاصة ، خاصة مع التطور السريع الذي يشهده هذا العصر في مجال التكنولوجيا والمعلومات ، حيث ان كل دول العالم تسعى جاهدة لإيجاد السبل والحلول اللازمة للحد من انتشار مثل هاته الجرائم والبحث في السبل الكفيلة للوقاية منها ، رغم الصعوبات الكبيرة التي تعترض الجهات المختصة، الا انها في كل مرة تصدر قوانين وإجراءات تحكم هاته الجرائم رغم التطور الرهيب لوسائل وكيفيات ارتكاب مثل هاته الجرائم العابرة للحدود الدولية .

وقد اسفرت هاته الدراسة على مجموعة من النتائج أهمها: ان هناك صعوبات كبيرة تعترض طريق المحققين بداية من التحقيق الاولي لمسرح الجريمة مرورا بجمع الأدلة والتي تعتبر المرحلة الأهم في الإيقاع بمرتكبي هاته الجرائم الناعمة ، كما نجد ان الطرق التقليدية التي يعتمد عليها المحققين اثناء التحقيق في الجرائم الالكترونية لا تجدي نفعا ولا توصل الى النتائج المرجوة .

الكلمات المفتاحية: الجريمة؛ الجريمة الالكترونية؛ المجرم المعلوماتي؛ الدليل الرقمي؛ التحقيق، الضحية.

***

Abstract:

Cyber-crime is considered one of the serious crimes that have emerged in the modern era and has become a major problem for countries in general and individuals in particular, Especially with the rapid development witnessed by this era in the field of technology and information, As all countries of the world are striving to find the necessary ways and solutions to curb the spread of such crimes, and search for ways to prevent them. Despite the great difficulties faced by the competent authorities, However, every time laws and procedures are issued to govern these crimes, despite the terrible development of the means and methods of committing such crimes across international borders. **Keywords:** *the crime; cyber-crime; cyber-criminal; digital directory; Investigation, the victim.*

* **المؤلف المرسل**

I. مقدمة

يعتبر التطور التكنولوجي من اهم خصائص العصر الحديث، خاصة في مجال المعلومات والاتصال حيث ساهم هذا التطور بشكل كبير في ربط وتعزيز التواصل بشتى انواعه ثقافيا، اجتماعيا، سياسيا، اقتصاديا، مما ساهم في كسر الحواجز امام التواصل بين الافراد والمجتمعات، حيث اصبح بفضل هاته النقلة النوعية في المجال التكنولوجي والمعلوماتي العالم عبارة عن قرية صغيرة كل هذا بفضل الانترنت التي أصبحت جزءا كبيرا من حياة الافراد والمجتمعات، فبفضل هاته التقنية (الانترنت)، أصبحت الاحداث التي تقع في كل بقاع العالم في أي زمان سهلة المتابعة في لحظة وقوعها لحظة بلحظة .

وان كان ما سبق ذكره هو الجانب الإيجابي الذي تحقق بفضل الثورة التكنولوجية في جميع ميادين الحياة المعاصرة، الا انه صاحبها جانبا سلبيا خطيرا الا وهو سوء استغلال هاته التقنية استغلال غير مشروع وبطرق أصبحت تلحق ضررا كبيرا بالدول بصفة عامة والافراد بصفة خاصة، وهذا ما أدى الى ظهور أنماط جديدة من الجرائم تختلف اختلافا كليا عن الجرائم التقليدية، وهي ما تعرف بالجرائم الالكترونية .

ومن اكثر الجرائم الالكترونية انتشارا جرائم القرصنة الالكترونية وجرائم الابتزاز الالكتروني، كما ان سبل وقوانين مواجهة هذا النوع من الجرائم اصبح شبه عاجز عن مجابهة مثل هاته الجرائم فالقوانين التي تحد من خطورة الجرائم الالكترونية لا تتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الحديثة (فلا عقوبة على جرم لم يأت عليه بنص قانوني) (عبيد الكعبي، د س، القاهرة،ص32)

ولان الجريمة الالكترونية لها طبيعة خاصة بعناصرها ووسائل ارتكابها، يجب على المشرعين وأصحاب الاختصاص الى إعادة النظر في الكثير من الإجراءات خاصة فيما يتعلق بمسالة تشريع القوانين التي تحكم هاته الجرائم ، ومحاولة إيجاد حلول للصعوبات التي تعترض المحققين اثناء التحقيق في الجرائم الالكترونية .

ومن خلال ما سبق التطرق اليه سنحاول التعرف على اهم الصعوبات التي تعترض المحققين اثناء محاولة فك شيفرة هاته الجرائم وهذا ما يقودنا الى طرح الاشكال التالي : ماهي الجريمة الالكترونية؟، **ماهي اهم الصعوبات التي يوجهها المحققين في اثبات الجريمة الالكترونية ؟**

- أسباب واهداف الدراسة :

. من بين الأسباب التي دفعتنا للبحث في هذا الموضوع هو ان البحوث في هذا الموضوع قليلة جدا، محاولة معرفة اهم العراقيل والصعوبات التي تواجه المختصين في محاولة إيجاد حلول ووضع قوانين تحكم هاته الجرائم العابرة للقارات .

. اختلاف الجرائم الالكترونية عن الجرائم التقليدية من ناحية الوسائل وطرق ارتكابها .

. تقديم بعض التوصيات والحلول لمواجهة الجريمة الالكترونية بمختلف اشكالها .

. إعادة النظر في مختلف الآليات والاستراتيجيات التي قد تساهم في الوقاية من الجريمة الالكترونية .

أولا: تحديد المفاهيم:

1- تعريف الجريمة:

1-1لغة: الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه وجرمه الرجل على قومه واليهم، ذنب وجنى جنتة (ابن منظور ، 1997، ص 90)

1-2 فقهيا : عرفها الدكتور عبد الله سلمان بانها كل سلوك يمكن اسناده الى فاعله يضر او يهدد بالخطر مصلحة اجتماعية محمية بجزاء جنائي (سلمان، 1998، ص، 59).

عرفها الدكتور مامون سلامة بانها الواقعة التي ترتكب اضرار بمصلحة حماها المشرع في قانون العقوبات ورتب عليها اثرا جنائيا متمثلا في العقوبة (لحسن ، 2002، ص31)

التعريف الاجتماعي: وهي سلوك إنساني سلبا او إيجابا يتعارض مع قيم المجتمع التي توارثتها المجتمعات الإنسانية وهي سلوك غير سوي يحدث اضطرابا في عناصر الاستقرار والأمن الاجتماعيين (مصطفى محمد، 2008، ص 50).

اتفق الكثير من علماء الاجتماع على أن الجريمة ظاهرة اجتماعية وان ما اعتبر جريمة ناتج عن تشريع الجماعة لبعض أعمال أفرادها سواء عاقب عليها القانون أو لم يعاقب إي أن المعيار الاستقامة من عدمه راجع إلى المعيار الاجتماعي لا المعيار القانوني (محمد زكي، 1981، صفحة 33).

-ويعرف أنصار العوامل الاجتماعية بأنها سلوك مضاد للمجتمع وهو ما يضر بالمصلحة الاجتماعية للمجتمع كما تعرف الجريمة اجتماعيا بأنها رد يخالف الشعور العام للجماعة وأنها كل فعل فردي او جماعي يشكل خرقا لقواعد الضبط الاجتماعي التي اقرها المجتمع والذي يمكن التعبير عنه بمجموعة القيم التقاليد والأعراف السائدة في المجتمع (عبيد، 1993، صفحة 93).

تعريف "جاروفالو"Garofalo: ان المجتمع هو الأساس لتجريم اي فعل يرتكب اي انه اعتمد في تعريفه للجريمة غلى معيار اجتماعي ومن تحليله لعواطف المجتمع التي تظهر من خلال تصرفات الإنسان، وقد خرج بنوعين من الجرائم

الأولى جرائم طبيعية متفق على تجريمها من المجتمعات في كل زمان ومكان، بتعارضها مع عاطفة الشفقة وعاطفة الأمانة مثل الاعتداء على الأشخاص وجرائم الاعتداء على الأموال

والأخرى جرائم مصطنعة وهي جرائم ضد العواطف الغير ثابتة وهي العاطفة القابلة للتحول كالعواطف الدينية والشعوب بالحياء وحب الوطن (القهواجي، 1985، الصفحات 13-14).

ومن الناحية السيكولوجية: هي سلوك معاد للمجتمع ويمكن القول أنها سلوك شاذ يحتاج الى علاج حيث يرى علماء النفس ان وراء كل جريمة صراعات نفسية أدت إلى وقوع الجريمة وهي نتيجة للصراع بين غريزة الذات والشعور الاجتماعي (محمد نصر، 2012، صفحة 43).

التعريف الأخلاقي: هي كل فعل او امتناع يتعارض مع القيم والأفكار والمبادئ السائدة في المجتمع كما ان الجريمة تعتبر انتهاكا للقيم الأخلاقية المتفق عليها (السيد، 2008، صفحة 100).

إجرائيا: هي كل سلوك او فعل يخرج عن المعايير والقيم التي وضعها المجتمع يترتب عليها أضرار مادية او معنوية يتعرض فاعلها للعقاب.

2- الجريمة الالكترونية:

تعددت التعاريف حول موضوع الجريمة الالكترونية، كما تعددت المصطلحات المستخدمة للدلالة عليها، فالبعض استخدم مصطلح جرائم استخدام الحسابات او جرائم المعالجة الالية والبعض الاخر اطلق عليهااسم الاجرام المعلوماتي، وغيرها من التعاريف التي تتعلق بهذا الموضوع وفيما يلي تفصيل لهذه الجريمة:

2- تعريف الجريمة الالكترونية فقها وقانونا:

2-1_ التعريف الفقهي: كان لتعريف الجريمة الالكترونية محلا لاجتهادات الفقهاء، لذا ذهب الفقهاء في تعريفها الى مذاهب شتى ووضعوا تعريفات مختلفة، تتباين بين الجرائم التي ترتكب بواسطة الحاسوب الى الجرائم التي ترتكب بأي نوع من المعدات الرقمية

ويذهب انصار هذا الاتجاه الى حصر الجريمة الالكترونية في الحالات التي تتطلب قدرا كثيرا من المعرفة التقنية في ارتكابها، اي ان الجريمة الالكترونية حسب انصار هذا الاتجاه هي كل فعل غير مشروع يكون ذو صلة بتكنولوجيا الحاسبات الالية بقدر كبير لارتكابه من ناحية وملاحقته وتحقيقه من ناحية اخرى

هناك من عرفها على انها الجرائم ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال استخدام الاجهزة الالكترونية ينتج منها حصول المجرم على فوائد مادية او معنوية، مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من اجل السرقة او اتلاف المعلومات الموجودة في الاجهزة، ومن ثم ابتزاز الاشخاص باستخدام تلك المعلومات .(بوزيدي ، 2017، ص09)

ويرى الاستاذ MASS ان المقصود بالجريمة الالكترونية هي اعتداءات ترتكب بواسطة المعلومات هدفها تحقيق الربح .

كما عرفها الاستاذ PARKER بأنها كل فعل اجرامي متعمد ايا كان، ذو صلة بالمعلوماتية ينشأ عنها خسارة تحلق بالمجني عليه او كسب يحققه فاعله .(الشوايكة، 2009،ص8)

وعرفها اخرون بأنها نشاط غير مشروع لنسخ او تغيير او حذف او الوصول الى المعلومات المخزونة داخل الحاسب او التي تحول عن طريقه، وعرفت كذلك بأنها غش غير مشروع يتعلق بالمعلومات المعالجة ونقلها (الشكري، 2008، ص113)

2-2-التعريف القانوني: عرفت الجريمة الالكترونية حسب ما جاء به المشرع الجزائري بموجب المادة 02 من القانون 09-04 على انها" جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات، واي جرائم اخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام الاتصالات الالكترونية"

ويلاحظ من خلال هذا التعريف ان المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية، وهو نظام الاتصالات الالكترونية.

ثانيا: اركان الجريمة الالكترونية

تنهض الجريمة على ركنين رئيسيين هما الركن المادي والركن المعنوي، فالأول يمثل كيانها الملموس ويعبر عن ارادة الفاعل والاخير يعبر عن ارادة المجرم المعلوماتي

1_ الركن المادي للجريمة الالكترونية:

لابد من فعل او امتناع يمكن اثباته اذ لا عبرة بما في خلد الانسان من افكار لانها لا تدخل دائرة التجريم، ويختلف الركن المادي هنا من حال لاخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف او تهديد او تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر، وهذا لا يسبب اشكالا، اذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكات التقليدية، الا ان هناك انواعا من السلوك يتطلب التمييز بينها وبين سابقتها، وهذا ما يدعو للتدخل التشريعي(بوضياف ، 2018، ص7)

يتكون الركن المادي للجريمة الالكترونية من السلوك الاجرامي والنتيجة والعلاقة السببية، علما انه تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها.

2_ الركن المعنوي للجريمة الالكترونية:

تعد الجرائم المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم والارادة) لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون ان يسبقه القصد العام، اما عن وجود قصد خاص في الجرائم المعلوماتية فهذا يرجع بالدرجة الاولى الى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع او ارتكاب الجريمة(بوضياف ، 2018، ص7).

يتكون الركن المعنوي للجريمة الالكترونية من عنصرين هما العلم والارادة

- العلم هو ادراك الفاعل للأمور
- اما الارادة فهي اتجاه السلوك الاجرامي لتحقيق النتيجة

الفاعل في الجريمة الالكترونية يوجه سلوكه الاجرامي نحو ارتكاب فعل غير مشروع او غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتقاء علمه كركن للقصد الجنائي العام

اذن فالقصد الجنائي العام متوافر في جميع الجرائم الالكترونية دون اي استثناء ولكن هذا لا يمنع ان بعض الجرائم الالكترونية تتوافر فيها القصد الجنائي الخاص(مثل جرائم تشويه السمعة عبر الانترنت، وجرائم نشر الفيروسات عبر الشبكة..) وفي كل الاحوال يرجع الامر للسلطة التقديرية للقاضي(بوضياف ، 2018، ص8)

خصائص الجريمة الالكترونية:

للجريمة الالكترونية مجموعة من الخصائص التي تنفرد بها عن الجرائم التقليدية، ومن اهم هذه الخصائص ان الجرائم الالكترونية تتطلب وجود جهاز الكتروني ومعرفة كيفية استخدامه، وان الهدف من هذه الجرائم الكيانات المعنوية لهذا الجهاز، وهي جريمة لا حدود لها، وهذه الجرائم صعبة الاثبات والاكتشاف، لذلك تعد مغرية بالنسبة للمجرمين، وعلى ضوء ما سبق ذكره سنتناول هذه الخصائص في ما يلي:

1- انها جريمة عابرة للحدود الدولية:

الجريمة الالكترونية ذات بعد دولي، اي انها عابرة للحدود، فهي قد تتجاوز الحدود الجغرافية بسبب ان تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الاحيان تحديات قانونية ادارية فنية، كما ينتج عنه صعوبات سياسية بشأن مواجهتها لا سيما فيما يتعلق بإجراءات الملاحقة الجنائية(عطايا، العدد 30، ص374)

2- الجريمة الالكترونية صعبة الاكتشاف والاثبات:

تتميز الجريمة الالكترونية عن الجرائم التقليدية بأنها صعبة الاثبات، وهذا راجع الى افتقاد وجود الاثار التقليدية للجريمة وغياب دليل ملموس(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل وتدميره قصير، بالإضافة الى نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين الردعية القائمة

كما هو واضح ان الجريمة الالكترونية لا تحتاج الى اي عنف او سفك للدماء او اثار اقتحام لسرقة الاموال، وانما هي بيانات ومعلومات تغير او تعدل او تمحى كليا او جزئيا من السجلات المخزونة في ذاكرة الحاسب الالكتروني، لذا يكون من الصعب اكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبها (الشكري، ص116)

3- يتطلب ارتكابها وجود جهاز الالكتروني والاحاطة بتقنيات استخدامه:

مما لا شك فيه ان ما يميز الجرائم الالكترونية عن غيرها هو انها تتطلب اجهزة الإلكترونية والحاسوب بصفة خاصة كما يتطلب وجود علم كافي بالجوانب الفنية كالتقنية لاستخدام الحاسوب والانترنت.، وكلما زادت خبرة لدى الافراد بمعرفة تقنية الحاسوب كلما زاد احتمال استغلال خبرتهم بشكل غير مشروع

4- الجريمة الالكترونية جرائم الاذكياء:

ففي الغالب مرتكب هذا النوع من الجرائم شخص يتميز بالذكاء والدهاء، ذو مهارات عالية ودراية بالأسلوب المستخدم في مجال انظمة الحاسب وكيفية تشغيله وتخزين المعلومات والحصول عليها، في حين ان مرتكب الجريمة التقليدية في الغالب شخص امي(بوضياف اسمهان، ص10)

أصناف المجرمين الالكترونين :

الهواة:**P ranksters** وتظم هذه الطائفة الأشخاص الذين يرتكبون الجريمة الالكترونية بغرض التسلية والمزاح دون ان تكون لديهم نية في احداث أية اضرار بالمجني عليهم ونجد من بين هاته الفئة من لم يبلغ السن القانوني وهم غالبا ما يكونون في مرحلة المرهقة وعلى الرغم من صغر سنهم الا اننا نجدهم انهم قادرين على اختراق كافة الأنظمة المعلوماتية ، وقد اثارت هاته الفئة الكثير من الجدل لدى رجال القانون ، وهذا راجع لمخافة ان تتحول هاته الفئة الى قراصنة محترفين واستغلالهم في اعمال إجرامية خطيرة (سامي الشوا،1993، ص 525)

فئة القراصنة او المخترقون : وتنقسم هاته الفئة الى نوعين :

الهاكار (**Les Hakers**): هم المتطفلون الذين يتحدون امن النظم المعلوماتية والشيكات من خلال الدخول الى أنظمة الحاسبات الالية غير المصرح لهم الدخول اليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وفي الغالب لا يكون لديهم دوافع تخريبية او إجرامية وانما بغرض التحدي واثبات الذات واكتساب الخبرة (موسى،دس ،ص15)

الكراكر: ا (**Les crakers**): وهم الأشخاص الذين يقومون بالتسلل الى أنظمة المعالجة الالية للاطلاع على المعلومات المخزنة بها لإلحاق الضرر بها او العبث بها او سرقتها ، وغالبا ما يكون هدف هاته الفئة هو جمع المال والشهرة .

فئة المحترفين : وتعتبر هاته الفئة الأخطر من المجرمين حيث يكون هدفهم من الاعتداء تحقيق مكاسب مالية لهم او للجهات التي يعملون لها ، فضلا عن تحقيق أغراض سياسية او التعبير عن مواقف او قضية معينة كما انهم يقومون باستعمال العنف المعلوماتي في تنفيذ جرائمهم كتحطيم كل الأنظمة المعلوماتية ، كما انهم يتمتعون بالكفاءة العالية في مجال المعلوماتية ويعملون بطرقة منظمة بحيث يمكن اطلاق مصطلح الجريمة المنظمة على افعالهم .

فئة الحاقدين : وهم فئة خطيرة جدا تختلف عن الأنواع التي تم ذكرها بحيث انهم يهدفون الى الانتقام من صاحب العمل او من جهات معينة .

خصائص المجرم المعلوماتي :

يتميز المجرم المعلوماتي عن غيره بعدة صفات جعلته محل العديد من الدراسات ومن بين هاته الصفات مايلي:

1/ الذكاء : يعتبر الذكاء من اهم صفات مرتكبي الجريمة الالكترونية لان ذلك يتطلب منه معرفة التقنية وكيفية الدخول الى أنظمة الحاسب الالي والقدرة على التغير والتعديل والتحكم في البرامج ، لذلك عادة مايطلق على الاجرام المعلوماتي اجرام الاذكياء وذلك بالمقارنة مع المجرم التقليدي الذي يميل للعنف فهذا المجرم لايمكن ان ينتمي الى طائفة المجرمين الاغبياء ، فمن يستعين بجهاز حاسوب للاستلاء على اسرار بنك او شركة لابد ان يتميز بمستوى ذكاء خارق (غنام، 2003، ص05)

2/ المهارة: تعد المهارة من ابراز خصائص هذا المجرم والتي يكتسبها من خلال الدراسة المتخصصة في هذا المجال او من خلال الخبرة المكتسبة في مجال تكنولوجيا المعلومات او بمجرد التفاعل الاجتماعي مع الاخرين ، ومستوى المهارة التي يكون عليها المجرم الالكتروني هي التي تحدد نوع الجريمة المرتكبة ، بحيث اذا كان المجرم على قدر ضعيف من المهارة نجد ان الجرائم التي يرتكبها لا تتعدى مستوى نسخ البيانات او اتلافها ، اما اذا كان المجرم على قدر كبير من المهارة فان أسلوب ارتكاب الجرائم يختلف ، اذ يمكنه عن طريق الشبكات الالكترونية بالدخول الى أنظمة الحاسب الالي سرقة الأموال وارتكاب جرائم التجسس وزرع الفيروسات في الأنظمة (إبراهيم ، 2003، ص88)

3/ التنظيم والتخطيط: تتميز الجريمة الالكترونية عادة بوجود اكثر من فاعل للنشاط الاجرامي الواحد، اذ ترتكب اغلب الجرائم الالكترونية من عدة اشخاص لكل منهم نشاط محدد ، ويتم العمل بينهم وفق خطة محددة مسبقا على ارتكاب الجريمة ،فقد تحتاج جريمة نسخ برامج الحاسب الالي مثلا الى من يقوم نسخ البرامج والى من يقوم بعملية بيعها ، كما انه من الملاحظ ان الأشخاص الذين يقومون بتعديل البرامج لأغراض غير مشروعة ليسوا دائما المستفيدين بطريقة مباشرة من النشاط الاجرامي ، فجرائم المعلوماتية تتطلب في غالب الأحيان شخصين على الأقل احدهم متخصص في الحاسبات الالية يقوم بالجانب الفني للعملية الاجرامية وشخص اخر من المحيط ذاته او من خارجه لتغطية عملية التلاعب وتحويل المكاسب **(فريد فورة، 2005، ص 58).**

مواجهة الجريمة الالكترونية في التشريع الجزائري:

نتيجة لتأثر الجزائر بما افرزته ثورة تقنية المعلومات من اشكال جديدة للإجرام طالت مصالح غير التي لها قوانين تحميها ، فقد تطرق المشرع الجزائري الى تجريم أفعال المساس بأنظمة المعالجة الالية للمعطيات من خلال تعديل قانون العقوبات بموجب قانون رقم 15/04 والذي تضمن ثمانية مواد عمد من خلالها المشرع الى حماية سرية وسلامة المعلومات ونظم معالجتها وذلك من خلال المواد 394 مكرر الى 394 مكرر 07 ، اين جرم الدخول والبقاء الغير مشروع في نظام المعالجة الالية للمعطيات او في جزء منه الماد (394 مكرر) .

- الادخال بطريق الغش معطيات في نظام المعالجة الالية او الازالة بطريق الغش لمعطيات يتظمنها نظام المعالجة(394 مكرر1)
- الاتجار في معطيات مخزنة ومعالجة او مرسلة عن طريق منظومة معلوماتية
- حيازة او انشاء او نشر المعطيات المتحصل عليها بارتكاب احد الجرائم المنصوص عليها في هذا المجال .

والملاحظ ان تخصيص المشرع الجزائري لهذه الجرائم قسما خاصا في قانون العقوبات دليل على على انها ظاهرة مستجدة ومتميزة عن الجرائم التقليدية الأخرى من حيث المصالح التي تطالها وكذا من حيث طبيعتها ومحلها ، ومن ثم لا يمن ادراجها تحت أي نوع من الجرائم التقليدية (بوبكر ،2021،ص65)،

كما انه لم يميز في وضعه لهذه النصوص القانونية نوعية المعلومات التي تطالها الجريمة فيما إذا كانت معلومات تتصل بمصالح اقتصادية او مالية او مسائل امنية، وذلك سعيا من المشروع الجزائري الي تعميم الحماية للمعلومات بكافة أنواعها ما عدى تشديد العقوبة اذا كانت المعلومات المستهدفة متعلقة بالدفاع الوطني او الهيئات و المؤسسات الخاضعة للقانون العام.

و في الحقيقة فانه قبل هذا القانون نجد ان المشرع الجزائري قد حاول مواجهة الجريمة المعلوماتية من خلال قانون الملكية الأدبية و الفنية وهو الامر 14/73 المؤرخ في 1973/04/03 المعدل و المتمم بمقتضى الامر 10/97 المؤرخ في 1997/03/06 و المعدل و المتمم بالامر 05/03 المؤرخ في 2003/07/19 و المتعلق بحق المؤلف و الحقوق المجاورة، حينما ادمج بموجب هذين الامرين الأخيرين برامج الاعلام الالي ضمن المصنفات الاصلية التي تشملها الحماية القانونية و قرر للاعتداء عليها عقوبة الحبس و الغرامة.

و تجدر الإشارة الى ان هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الامرين 10/97 و 05/03 تعود لاسباب أهمها انه من شروط الانضمام الى المنظمة العالمية للتجارة هو المصادقة على اتفاقية "بيرن" وهو ما فعلته الجزائر بموجب المرسوم الرئاسي (341/97) بالإضافة الى تبني احكام اتفاق جوانب الملكية الفكرية المتعلق بالتجارة، و الذي ورد في نص المادة 10 منه ان برامج الاعلام الالي سواء كانت في صورة برنامج مصدر او صورة منقوشة فهي محمية على أساس انها مصنفات أدبية، كما ان الاتفاقية الدولية حول الاجرام المعلوماتي نصت على تجريم الاعتداءات على حق المؤلف و الحقوق المجاورة اذا ارتكبت هذه الاعتداات عن طريق نظام معلوماتي في نطاق تجاري.

- التشريع في الولايات المتحدة الامريكية: يعد قانون فلوريدا لجرائم الحاسوب الصادر عام 1978 اول قانون في الولايات المتحدة الامريكية يخاطب الجريمة المعلوماتية، حيث يعتبر هذا القانون ان كل دخول الى الحاسوب غير مصرح به هو بمثابة جريمة، حتى ولو لم تكن هماك نية عدائية من هذا الدخول اما على الصعيد الفدرالي فقد صدر عام 1984 قانون الاحتيال و سوء استخدام الكمبيوتر computer fraudand abuseACT وقد تعديله مؤخرا عام 2001 بمقتضى القانون الوطني المؤرخ في 2001/10/26 وتم ادراجه في القسم 1030 من باب 18 من القانون الفدرالي للولايات المتحدة الامريكية. وقد عاقبت المادة 1030 من هذا القانون كل من يقوم بالدخول عمدا الى حاسوب مشمول بالحماية دون ان يكون

مصرحا له بذلك او يتجاوز التصريح الممنوح له اذا كان الغرض من هذا الدخول هو الحصول على شيء ذي قيمة عن طريق الاحتيال.

وما يمكن الإشارة اليه ان التشريع الفدرالي الأمريكي قبل عام 1986 لم يكن يحتوي على تجريم اتلاف المعلومات و البرامج وانما اقتصر التجريم على إعاقة أنظمة الحسابات الالية، فقد جرمت الفقرة الثالثة من المادة1030 من القانون الفدرالي لجرائم الحاسبات الالية الصادر عام 1984 اتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الالية وفي عام 1986 و نتيجة لكثير من الانتقادات التي وجهت لهذا القانون فقد تم تعديله و أصبحت الفقرة الثالثة من المادة 1030 تتناول فقط الدخول غير المصرح به الى حاسب الي تستعمله الحكومة متى أعاق الدخول هذا الاستعمال. و أضيفت فقرة خامسة للمادة 1030 تتناول جريمة الاتلاف العمدي و غبر المصرح به لمعلومات يحتوي عليها حاسب الي تابع للحكومة و ادارتها او حاسب الي غير تابع للحكومة الا انه يتم استخدامه من طرفها او لصالحها، او إعاقة هذا الحاسب عن أداء المهام المختلفة التي تباشرها الحكومة بواسطته، و بصدور قانون حماية بنية المعلومات القومية لعام 1996 تم تعديل المادة السابقة بشكل جوهري، وقد شمل هذا التعديل التوسع في نطاق حماية أنظمة الحاسبات الالية، فوفقا للفقرة الثانية من المادة 1030 لم تعد الحماية مقصورة على الحاسبات الالية التابعة للحكومة و ادارتها او التي يتم استخدامها من قبلها، و انما اتسعت الحماية لتشمل جميع الحاسبات التي يتم استخدامها من قبل المؤسسات الاقتصادية او التي تستخدم في التجارة و الاتصالات وهو ما اطلق عليه بالحاسبات التي تتمتع بالحماية.(الحن، 2011،ص104).

ثانيا: الصعوبات التي تواجه المحققين في الكشف عن الجريمة الالكترونية:

1/ صعوبات استخراج الدليل الرقمي : يتسم التحقيق في الجرائم الإلكترونية العديد من الصعوبات فنظرا لوقوع الجريمة الالكترونية ضمن بيئة رقمية كامنة في أجهزة الحاسب الالي والخوادم والشبكات بمختلف أنواعها أدت الى ظهور نوع من التحدي للأجهزة المختصة بالبحث والتحري، في تطبيق القواعد الإجرائية التي نظمت مسالة استخلاص الدليل الرقمي وتضعف قيمتها في مكافحة هذا النوع من الجرائم وتؤثر على عملية التحقيق وتؤدي الى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في أجهزة التحقيق وقد تصل الى ابعد من ذلك حين يعتقد المجرم ان الجهات الأمنية غير قادرة على اكتشاف امره وان خبرة القائمين على مكافحة الجرائم الالكترونية والتحقيق فيها لا تجاري خبرته، الامر الذي يعطيه ثقة اكبر في ارتكاب المزيد من هذه الجرائم (الحلبي ، 2011،ص220).

وهذه الصعوبات تنوعت وتباينت مابين صعوبات تتعلق بطبيعة الدليل الرقمي ، وأخرى متعلقة بجهات التحقيق ، وأخرى متعلقة بالجهات المتضررة من الجريمة الالكترونية بالإضافة الى صعوبة تحديد الجاني ، وهذا ما سنحاول ان نتطرق اليه بالتفصيل من خلال العناصر الاتية :

أولا: الصعوبات التي تتعلق بطبيعة الدليل الرقمي :

1/ الدليل الرقمي دليل غير مري: من مميزات الدليل الرقمي انه دليل غير مرئي، وهو عبارة عن نبضات مغناطسية أي الكترونية تتكون من سلسلة طويلة من الأرقام أي انه ذو طبيعة ثناية (1-0) لا تفصح عن الشخصية المعنوية .

ودئما ما يكون الدليل في الجريمة التقليدية ذو طبيعة مادية مرئية بحيث يمكن للمختصين في عملية التحقيق بمعاينة مسرح الجريمة، وضبط أي دليل يفيد في الكشف عن الجريمة، ولكن الجريمة الالكترونية تقع في بيئة تختلف عن البيئة التقليدية ، وذلك لان الأدلة فيها عبارة عن نبضات مغناطسية تشكل بيانات رقمية في العالم الافتراضي ، ومنه فعدم رؤية الدليل الرقمي يشكل العديد من المعوقات والصعوبات من خلال جمعه وتحليله مما يستوجب ان يكون المحققين الفنيين على دراية كافية في التعامل مع هذا النوع من الأدلة (حجازي،2007،ص 69).

2/ سهولة إخفاء الدليل : المجرمين الذين يستخدمون الوسائل الالكترونية في ارتكاب جرائمهم يتميزون بالذكاء والاتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعة الفنية، ولذلك فانهم يتمكنون من إخفاء الأفعال غير المشروعة التي يقومون بها اثناء تشغيلهم لهذه الوسائل الالكترونية ويستخدمون في ذلك التلاعب غير المرئي في النبضات او الذبذبات الالكترونية التي يتم عن طريقها تسجيل البيانات(رستم،1994،ص 17).

كما وان هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الوسائل الالكترونية ويكون امرها حكرا عليهم كالتجسس على ملفات البيانات المخزنة ومعرفة ما بها من اسرار ،كما انهم ينسخون هاته البيانات والملفات بقصد استعمالها تحقيقا لمصالحهم الخاصة، كذلك فانهم يقومون باختراق قواعد البيانات والتغير في محتواها تحقيقا لمارب خاصة، وقد يصل بهم الامر في بعض الأحيان الى القيام بتخريب الأنظمة بقصد التمويه وعدم ترك الاثار، كما لو كان مصدره خطا في البرامج او الأجهزة او أنظمة التشغيل او التصميم الكلي للنظام المعالج اليا للمعلومات ، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب الالي او يعدلون برامجه او يحرفون البيانات المخزنة في داخله دون ينكشف امر هذا التعديل (رستم،1994،ص ص 17،20).

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة عليها من الوسائل الالكترونية انه يمكن محو الدليل في زمن قصير جدا بحيث لا تستطيع الجهات المختصة من تتبعه وكشف الجريمة اذا ما تم اكتشافها او التبليغ عنها (الصغير،1998،ص04) .

3/ صعوبة الحصول على الدليل الرقمي : كثيرا ما يلجا مرتكبي الجريمة الالكترونية الى اهم الوسائل لعرقلة جميع ادلة الإدانة ، ومن بين اهم هذه الوسائل نجد مسالة استخدام تقنية التشفير (حجازي، مرجع نفسه، ص89) ، او لاستخدامهم لمسالة التدابير الأمنية لمنع مشكلة التفتيش والاطلاع على الأدلة او ضبطها ، وذلك باستخدام كلمة السر او القيام بإخفاء هويتهم ، وخاصة عند استخدامهم لشبكة الانترنت وذلك بالاستعانة بالبرامج والتطبيقات التي تعمل على طمس هويتهم في شبكة الانترنت (ممدوح عبد المطلب ، دس، ص 121).

ثانيا : الصعوبات التي تواجه جهات التحقيق : تتعلق هاته الصعوبات بالعامل البشري القائم بالتحقيق في الجريمة الالكترونية ، فاذا كانت السلطات القائمة بالتحقيق من رجال الشرطة والضبطية القضائية بما لهم

من خلفية قانونية تلعب دورا كبيرا في التحري عن الجرائم والبحث عن مرتكبيها في اطار الجريمة التقليدية ، فان وظيفتهم في مكافحة الجرائم الالكترونية لا ترتقي الى نفس الدرجة.

وياتي ذلك بسبب الدليل الرقمي ، فالدليل الرقمي هو دليل يحتوي على مسائل فنية لا يقوى على فهمها الا الخبير المتخصص ، وان كان الدليل الرقمي الناتج عن الجرائم الالكترونية يتحصل عليه من خلال عمليات فنية معقدة عن طريق التلاعب في نبضات وذبذبات الكترونية وعمليات أخرى غير مرئية ، فان الوصول اليه وفهم مضمونه قد يكون في غاية الصعوبة ، فالطبيعة الغير مادية للمعلومات والبيانات المخزنة بالحاسب الالي، والطبيعة المعنوية لوسائل نقل هذه البيانات تثير مشكلات عديدة في الاثبات الجنائي ، ومثال ذلك ان اثبات التدليس والذي قد يقع على نظام المعالجة الالية للمعلومات يتطلب تمكين مأمور الضبط القضائي او سلطة الحقيق من جمع المعطيات الضرورية التي تساعد على إجراءات التحريات و التحقيق من صحتها للتأكد عما اذا كانت هناك جريمة وقعت ام لا ومثل هذا الامر يتطلب إعادة عرض كافة العمليات الالية التي تمت لأجل الكشف عن هذا التدليس (الصغير،1998،ص 113) ، وقد يستعصي هدا الامر فهما على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من القضايا الفنية الدقيقة التي من خلالها يتولد الدليل المتحصل عليه من الوسائل الالكترونية .

كذلك فان الكثير من العمليات الالية للبيانات التي يقوم بها الحاسب الالي بطريقة الية دون الحاجة الى عمليات الادخال كما هو الحال في احتساب الفائدة على الايداعات البنكية التي تقيد اليا بأرصدة حسابات العملاء على ضوء الشروط المتفق عليها مسبقا والمخزنة في برنامج الحاسب، قد يكون من السهل اختراقها وارتكاب جرائم تزوير واستيلاء تقع عليها عن طريق ادخال بيانات غير معتمدة في نظام الحاسب او اجراء تعديلات في برامجه او القيام بالتلاعبات في البيانات المخزنة .

وبالنظر الى ان هاته العمليات يصعب ان تخلف ورائها اثرا ماديا ملموسا يكشف عنها ، فان ذلك سيزيد من صعوبة عمل المحققين الذين يعملون على مثل هاته الجرائم التي تنتج عن هذه العمليات الالكترونية ، فقد يستعصي عليهم فهم الأدلة المتحصلة عن هذه الوسائل بسبب تعقيدها وصعوبة الوصول الى مرتكبي هاته الجرائم (الصغير،1998،ص 113) .

ثالثا : الصعوبات التي تكون بسبب الجهات المتضررة وصعوبة تحديد الجاني :

1/ الصعوبات التي تكون بسبب الجهات المتضررة: تعتبر الجهات المتضررة من الجرائم الالكترونية من الأسباب الرئيسية لعدم الوصول الى الأدلة التي تثبت الجريمة وذلك راجع للأسباب التالية :

- تتعمد اغلب الشركات والأشخاص الى التستر على الجريمة الالكترونية وعدم ابلاغ الجهات المختصة ، وهو ما يكون غالبا في جرائم الابتزاز الالكتروني ، وهدا يؤدي الى عدم التعاون مع السلطات المختصة لمكافحة هدا النوع من الجرائم .
- مجال الاستثمار في نظم المعلومات يؤدي الى تسابق الشركات مما يدفعها الى في مقابل تحقيق الربح الى تبسيط الإجراءات وتسهيل استخدام البرامج وملحقاها وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة مقابل اهمال الجانب الأمني ، حيث ان بعض الشركات لا تطلب من المشتركين هوايتهم عند الاشتراك مما يحول دون معرفة هواية المستخدم في البحث في حالة البحث والتحري .

- كثيرا من الجهات التي تتعرض أنظمتها المعلوماتية للاعتداء تعمد الى عدم الكشف والتبليغ عن ذلك لدة السلطات المختصة تجنبا للإضرار بسمعتها او خوفا من الكشف عن أسلوب ارتكاب الجريمة مما قد يؤدي الى تكرار وقوعها من طرف اخرين .

لاجل ذلك فقد طرحت العديد من الاقتراحات لحمل المجني عليهم في الجريمة الالكترونية على التبليغ والتعاون مع الجهات المختصة ، بان تفرض النصوص القانونية المتعلقة بجرائم الالكترونية التزاما على عاتق موظفي الجهات المتضررة بالإبلاغ عما يصلهم من اخبار عن وقوع تلك الجرائم ، مع تحديد المسؤولية الجنائية في حالة عدم الإبلاغ (احمد ، 2019 ، ص125).

2/ صعوبة تحديد الجاني : من اكثر الصعوبات التي توجهها السلطات المختصة في مكافحة الجريمة الالكترونية هو ان المجرم المعلوماتي يعمل بذكاء على إخفاء هويته للحيلولة دون تعقبه وكشف هويته وذلك حتى تظل أعمالهم الاجرامية بعيدة كل البعد عن السلطات المعنية بمكافحة هذا النوع من الجرائم .

نتائج الدراسة : من خلال ما تم عرضه حول هذا الموضوع توصلنا الى عدة نتائج أهمها :

أ/ ان الجريمة الالكترونية تعد من المواضيع المستحدثة التي فرضت نفسها في الآونة الخيرة بقوة على المستوى الوطني او الدولي، واجبرت الدول على دق ناقوس الخطر والتدخل من اجل مواجهتها.

ب/ ان الجريمة الالكترونية من الجرائم العابرة للقارات وهذا ما اثر سلبا على التحكم فيها وذلك ان الدول تستطيع اصدار التشريعات التي تحكم هذا النوع داخل حدودها، الا انها لا تستطيع ذلك خارج حدودها ،

ج/ استعمال الوسائل التقلدية في عملية التحقيق والكشف عن مثل هاته الجرائم المتطورة ، وكذلك غياب التكوين الفعال الذي يسمح لأصحاب الاختصاص بمواجهة مثل هاته الجرائم .

د/ ان الكثير من الأشخاص والمؤسسات التي تتعرض الى الهجمات الالكترونية لا تقوم بالتبليغ وهذا مايؤدي الى تفاقم هاته الجرائم ، واكتساب المجرمين ثقة كبيرة والتمادي في ممارسة نشاطهم الاجرامي .

هـ/ صعوبة الحصول على الأدلة في مثل هاته الجرائم مما يزيد من خطورتها ان هاته الأدلة سهلة التخلص منها عكس الجرائم التقليدية التي يكون فيها الدليل مرئيا ويسهل الحصول عليه .

ي/ عدم وجود وحدات مختصة في البحث والتحري عن الجرائم الالكترونية ، وان وجدت فانها تفتقر الى الخبرة والوسائل في الكشف عن مثل هاته الجرائم .

خاتمة:

من خلال ما سبق التطرق اليه سابقا نجد ان التطور الذي نعيشه في هذا العصر خاصة فيما يتعلق بالثورة المعلوماتية نتج عنه العديد من المشكلات والاخطار التي تكون مصاحبة بشكل عفوي لكل تطور حضاري، فدخول الانترنت عالمنا وانتشارها انتشارا كبيرا لدى مختلف أطياف المجتمع أدى الى ظهور الجريمة الالكترونية التي أصبحت تشكل خطرا على كل مستخدمي هاته التقنية وهذا بسبب غياب الرقابة على مستخدمي الشبكات المعلوماتية ، خاصة مع ظهور محترفين في هاته الجرائم يسرقون وينهبون ويخربون مما أدى بالدول الى دق ناقوس الخطر واخذ موقف صارم تجاههم ومحاولة إيجاد الحلول اللازمة للحد من انتشار هاته الافة وانطلاقا مما تم التعرض اليه تم التوصل الى جملة من المقترحات جاءت كالاتي :

1/ ضرورة تعديل القوانين واستحداث قوانين جديدة لتواكب التطور السريع في مجال الجرائم الالكترونية .

2/ ضرورة عقد دورات تدريبية لرجال القضاء والمحققين في مجال تقنية المعلومات حتى يتسنى لهم مواجهة الجرائم الالكترونية .

3/ ضرورة الاهتمام بالبحوث والدراسات القانونية والاجتماعية التي تهتم بالجريمة الالكترونية والاخذ بالتوصيات التي توصل اليها الباحثين في هذا المجال .

4/ يجب ان يتم تفعيل الاتفاقيات الدولية التي تعنى بمواجهة الجرائم الالكترونية وان تأخذ على محمل الجد ، كذلك يجب استحداث اتفاقيات جديدة تتماشى مع الجرائم الالكترونية المستحدثة وتفعيلها على ارض الواقع .

5/ انشاء مراكز خاصة ومختصة في معالجة الجرائم الالكترونية مع الاستعانة بالخبراء في هذا المجال.

6/ رفع نسبة الوعي لدى مستخدمي وسائل التكنولوجيا الحديثة وذلك من خلال عقد المؤتمرات والملتقيات للتحسيس من مخاطر سوء استخدام هاته الوسائل الحديثة.

الإحالات و المراجع :

1- ضياء مصطفى عثمان، السرقة الالكترونية، دار النفائس، عمان، الطبعة الاولى،2011

2- مختارية بوزيدي، ماهية الجريمة الالكترونية، الملتقى الوطني "اليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، بتاريخ 29 مارس 2017

3- محمد امنية الشوايكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، 2009

4- عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وازمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، جامعة الكوفة "كلية القانون" العدد السابع، 2008

5- بوضياف اسمهان، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، العدد الحادي عشر،9 سبتمبر 2018

6- ابراهيم رمضان ابراهيم عطايا، الجريمة الالكترونية وسبل مواجهتها في الشريعة الاسلامية والانظمة الدولية، مجلة كلية الشريعة والقانون، طنطا، الجزء الثاني، العدد 30

7- علي عبد القادر القهواجي. (1985). علم الإجرام وعلم العقاب. بيروت: الدار الجامعية للطباعة والنشر

8- محمد محمد نصر. (2012). علم الاجرام. عمان: دار الراية للنشر والتوزيع.

9- طارق السيد. (2008). الإحراف الإجتماعي الأسباب والمعالجة. الإسكندرية: مؤسسة شباب الجامعة للنشر والتوزيع.

10- عبد الله سلمان ، 1998 ، شرح قانون العقوبات الجزائري القسم العام ، ديوان المطبوعات الجامعية .

11- بن شيخ لحسن ، 2002، مبادى القانون الجزائي العام ، دار هومة .

12- محمد بن بكر ابن منظور ، 1997، لسان العرب ، دار بيروت للطباعة والنشر ، المجلد الثاني عشر .

13- مصطفى محمد موسى ، التحقيق في الجرائم الالكترونية ، مطابع الشرطة ، ط1 .

14- غنام محمد غنام ، 2003، الحماية الجنائية لبطاقات الائتمان الممغنطة ، مؤتمر الجوانب القانونية للعمليات الالكترونية .

15- خالد ممدوح إبراهيم، 2009، الجرائم المعلوماتية ، دار الفكر الجامعي ،ط1 .

16- نائلة عادل محمد فريدة،2005، جرائم الحاب الالي الاقتصادية ، منشورات الحلب .

17- رشيد أبو بكر ، 2002، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائي والمقارن ، منشورات الحلبي.

18- عطا الله فشار، بحث حول مواجهة الجريمة المعلوماتية في التشريع الجزائري ، كلية الحقوق والعلوم السياسية ، جامعة الجلفة.

19- محمد طارق عبد الرؤوف الحن، 2011، جريمة الاحتيال عبر الانترنت ،الاحكام الموضوعية والاحكام الإجرائية، منشورات الحلبي الحقوقية.

20- خالد عياد الحلبي،2011، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، دار الثقافة للنشر والتوزيع .