ISSN: 1112-9212 / EISSN 2602-5043	2020 (01) 13	مجلة تطوير العلوم الاجتماعية (20،07)
تاريخ النشر: 2020/11/09	تاريخ القبول: 2020/11/01	تاريخ الاستلام: 2020/06/13

الجريمة الإلكترونية: الأسس والمفاهيم

Cyber crime: foundations and concepts

سليمة ذياب [1]* – بلال بوترعة[2]

1– طالبة دكتوراه، تخصص علم اجتماع التربية، جامعة الوادي (الجزائر)

2– أستاذ محاضر علم الاجتماع، رئيس قسم علم الاجتماع، جامعة الوادي (الجزائر).

ملخص: برزت الجريمة الإلكترونية كظاهرة اجتماعية بشكل محسوس خاصة بعد انتشار الخدمات الإلكترونية وخدمات الجيل الثالث، فبعدما كانت بالعشرات أصبحت الآن تتجاوز الآلاف أغلبها تلك المتعلقة بالحياة الشخصية، والمكاسب الأمنية للأفراد. نصب واحتيال قذف وتشهير وانتحال للشخصيات وابتزاز؛ جرائم كثيرة تدخل على المجتمع الجزائري بإسم التكنولوجيا، جرائم مستحدثة مسرحها افتراضي وخسائرها تلامس أرض الواقع إنها الجريمة الإلكترونية.

لذا ارتأينا في هذه الورقة أن توضيح مفهوم الجريمة الالكترونية، وتوضيح مفهوم الجريمة الالكترونية وموضوعها. ابراز أهم المراحل التي تحدث فيها إضافة الفاعل الاجتماعي في هذه الجريمة وتحديد دوافعه وكذا سماته، وهذا من أجل لفت أنظار المسؤولين نحو ظاهرة اجتماعية مستحدثة في مجال الجريمة، والكشف عن الخطر والخسائر والمخاطر التي تنجم عنها، وتوليد نوع من الوعي اتجاه هذا النوع من الجرائم داخل النسق المعلوماتي لأخذ الحيطة والحذر.

الكلمات المفتاحية: جريمة – حاسب الكتروني– انترنت– جريمة الكترونية.

Abstract:

Cybercrime has become a significant social phenomenon, especially after the spread of electronic and third generation services. After tens, it now exceeds thousands, most of which are linked to personal life and the security gains of individuals. Fraud, defamation, defamation, impersonation of characters and blackmail; Numerous crimes enter Algerian society in the name of technology, new crimes whose scene is hypothetical and whose losses touch the ground: this is the electronic crime.

This paper aims to clarify the concept of online crime, and explain the concept of online crime theme. Highlight the most important stages of adding social actor in this crime and to determine his motives and characteristics, and This is to bring to the attention of officials towards a new social phenomenon in crime, detect danger and losses and risks that result, generating the kind of awareness towards this type of crime in cyber theme to take caution

Keywords: the crime – Computer - Internet - Electronic crime.

* Corresponding author, e-mail: dhiab-salima@univ-eloued.dz

1- مقدمة

إن الدارس في علم الاجتماع ليس بعيدا عن الواقع البيئي المعاش و يعي مدى أهمية هذا النسق ووظيفته في المجتمع الكلي، فلقد وجد نفسه مجبرا وليس مخيرا للاهتمام والبحث في المشكلات المجتمعية الراهنة، لأجل الفهم ومحاولة إصلاح الخلل الذي وقع فيه البناء الاجتماعي من جراء تراكم الظواهر الجديدة بشكل متسارع.

فلقد شهد العالم في الآونة الأخيرة ثورة في عالم المعلومات والتي فرضت نفسها في شتى المجالات الحياتية حيث اصبح تقدم الدول يقاس بالرأس المال المعلوماتي، ولكن رغم الجوانب الايجابية المتعددة لاستخدام الإنترنت، برز نمط مستحدث من الجرائم، من بينها الجرائم الالكترونية والتي تعتمد في تخطيطها بصورة أساسية على شبكة المعلومات. برزت الجريمة الإلكترونية كظاهرة اجتماعية بشكل محسوس خاصة بعد انتشار الخدمات الإلكترونية وخدمات الجيل الثالث، فبعدما كانت بالعشرات أصبحت الآن تتجاوز الآلاف أغلبها تلك المتعلقة بالحياة الشخصية، والمكاسب الأمنية للأفراد. نصب واحتيال قذف وتشهير وانتحال للشخصيات وابتزاز؛ جرائم كثيرة تدخل على المجتمع الجزائري بإسم التكنولوجيا، جرائم مستحدثة مسرحها افتراضي وخسائرها تلامس أرض الواقع إنها الجريمة الإلكترونية.لهذا إرتاءينا في هذه الورقة البحثية تأصيل للجانب النظري لجريمة الإلكترونية إبرز بعض القضايا والمفاهيم المتعلقة بها.

1- الإطار المفاهيمي:

1.1- الجريمة:

لقد اختلف الباحثين في تعريف الجريمة ، فجاءت متنوعة فهناك من يتناول التعريف من الناحية التقنية ومنهم من يتناوله من الناحية القانونية، وبينما تناوله اهل الفقه من جانب اخر؛ إلا أننا اختارنا أن ندرج تعريف لعلماء الاجتماع. فعلماء الاجتماع يتفقون على أن (الجريمة) هي ظاهرة اجتماعية لا يخلو منها أي مجتمع إنساني، رغم أنها تتناقض مع الحاجات الأساسية والمصالح الرئيسية للمجتمع وتمثل خطرا عليه (أكرم المشهداني: 2005، ص 41). حيث توزعت تعاريف علماء الاجتماع لمفهوم الجريمة إلى ثلاث اتجاهات.

- **الجريمة من ناحية القانون:**

فالجريمة من الناحية القانونية: هي كل عمل مخالف لأحكام قانون العقوبات، فهي عمل لا أخلاقي تنفر منه النفوس. (عريم: 1970، ص 16)، وبالتالي فإن الجريمة هي كل فعل يعاقب عليه القانون.

- **الجريمة الاجتماعية**

وهي الفئة التي تربط بين الجريمة وبين الأفعال التي تسبب أذى للمجتمع، وقد تبنى هذا الإتجاه عدد من علماء الاجتماع والأنثروبولوجيا، من بينهم مثلا (سلين) Sillin الذي يعرف الجريمة بأنها انتهاك للمعايير الاجتماعية، ويعرفها كل من هيربت Herbart وسميث Smith بأنها شكل من أشكال السلوك الإنحرافي يهدف إلى فساد النظام الاجتماعي القائم، أما غاروفالو فيعرف الجريمة بأنها فعل غير اجتماعي، أو كل فعل ترى الاتجاهات والآراء السائدة في المجتمع أنه ضار، أو كل فعل يتعارض مع الأفكار والمبادئ السائدة في المجتمع، أو كل فعل يتضمن اعتداء على حق أو مخالفة لواجب، أو كل فعل يتعارض مع الناموس الطبيعي للأخلاق. (أكرم المشهداني: 2005، ص43)

- **الفئة الثالثة: الجمع بين المفهومين الاجتماعي والقانوني**

ويركز أصحاب هذا الاتجاه على أن الجريمة هي انحراف عن المعايير الاجتماعية، وفي نفس الوقت فإنها انتهاك للقانون. فقد عرفها مارشال كلينارد Clinard بأنها سلوك مؤذي وضار اجتماعيا ويتعرض صاحبه للعقاب من السلطة أو الدولة، ويعرفها علد الجبار عريم بأنها انتهاك للقيم الاجتماعية التي حددها الغالبية العظمى من الهيئة التي وضعت القانون الذي يجسد هذه القيم.(أكرم المشهداني: 2005، ص 44)

والجريمة اصطلاح شائع يطلق على عدد من الأفعال التي تخالف قواعد القانون أو المجتمع أو الأخلاق أو الدين.(العمرابي، صالح ،55،2006)، وفي الشريعة الإسلامية فإن الجريمة ارتكاب محظور شرعا إما بفعل نهي أو بترك مأمور به ويقصد بالمحظور شرعا ما ورد فيه نص شرعي على خطره والعقاب عليه.(العمرابي، صالح ، نفس المرجع، ص 58).

2.1- تعريف الحاسب الالكتروني والإنترنت:

- **تعريف الحاسب الالكتروني:**

الحاسوب هو عبارة عن آلة إلكترونية مصممة بطريقة تسمح باستقبال البيانات واختزالها ومعالجتها بحيث يمكن إجراء جميع العمليات البسيطة والمعقدة بسرعة، وبدقة، ويتم الحصول على نتائج هذه العمليات بطريقة آلية، حيث تحول البيانات إلى لغة يتعامل معها جهاز الحاسوب، وإذا نظرنا للحاسوب نظرة شاملة نجد أنه يقوم ليس فقط باستقبال البيانات ومن ثم معالجتها حسب رغبتنا وإخراج نتائج عملية المعالجة وتخزينها، بل يمكنه أيضاً نقلها إلى جهاز حاسب آخر، أي تبادل المعلومات بين الحاسبات وبعضها أي تكوين ما يسمى بالشبكات. (نسرين حسونة: شبكة الألوكة)

- **تعريف الإنترنت (شبكة المعلومات العالمية):**

وهو عبارة عن دائرة معارف عملاقة، يمكن للمشتركين فيها الحصول على المعلومات حول أي موضوع معين في شكل نص مكتوب أو مرسوم أو خرائط أو التراسل عن طريق البريد الإلكتروني، لأنها تضم ملايين من أجهزة الحاسوب تتبادل المعلومات فيما بينها. (نجلاء عبد الفتاح: 2015، ص 77)

وتعد شبكة (الانترنت) أكبر مزود للمعلومات في الوقت الحاضر، بل إنها أم الشبكات أو شبكة الشبكات، لأنها تضم عددا كبيرا من شبكات المعلومات المحسوبة المحلية أو الواسعة الموزعة على مستويات محلية ولإقليمية عالمية وفي مختلف بقاع العالم وتسمح شبكة الإنترنت هذه لأي حاسوب مزود بمعدات مناسبة سهلة الاستخدام بالاتصال بأي حاسوب وفي أي مكان في العالم، وتبادل المعلومات المتوافرة معه أو المشاركة فيها، مهما كان حجم معلوماته التي يمتلكها أو موقعه أو برمجياته أو طريقة ارتباطه. (فاضل عباس: 2007، ص323).

3.1- الجريمة الإلكترونية:

تعددت تعريفات الجريمة الإلكترونية نذكر منها:

"الجرائم التي تلعب فيها بيانات الكمبيوتر والرامج المعلوماتية دورا هاما، أو هي فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية".(حنان ريحان مبارك: 2014، ص 25)

وجاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقدة في فيينا سنة 2000 تعريف الجريم الإلكترونية كما يلي " يقصد بالجريم الإلكترونية أي جريمة يمكن

ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبيه ، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية. (يوسف جفال: 2016-2017،ص 11)

وهناك تعريف شامل نعتقد أنه للجريمة الإلكترونية " جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات".(عبد الفتاح بيومي: 2006، ص 33).

فالجريمة الإلكترونية هي جريمة تقع على الأفراد أو المؤسسات الذين يستخدمون جهاز الحاسب الآلي أو الهواتف الذكية، لذا تعتبر فعل لا أخلاقي وغير مصرح به ويرفضه المجتمع والقانون ويعاقب عليه ويدينه الشرع. وبالنظر لتوسع أدوات الاتصال الحديثة بالإضافة إلى مجموعة البرامج والتقنيات المعدة سهلت عملية الجريمة الإلكترونية.

2- الإطار النظري والدراسات السابقة:

1.2- الدراسات السابقة:

- أجرى رعد فجر فتيح (2017)، دراسة بعنوان" **إثبات الجريمة الإلكترونية بالدليل العلمي**"، في ضوء طبيعة وخصوصية الجريمة الالكترونية وكيفية مواجهتها وإثباتها، تمحورت هذه الدراسة حول ما أذا كان بالإمكان الاكتفاء بقواعد الإثبات العادية لإثبات الجريمة الالكترونية وتطبيق النصوص التي تتعلق بجرائم الأموال في صورتها التقليدية مثل السرقة، والنصب، وخيانة الأمانة، والإتلاف، أم أن الأمر يتطلب وضع نصوص وقواعد أثبات خاصة بها تنسجم مع طبيعتها وخصوصيتها.

- أجرى عصام ومحمد (2019)، دراسة بعنوان "**معوقات مكافحة الجرائم المعلوماتية في الضفة** الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية"، هدفت هذه الدراسة التعرف على معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية والمتعلقة بكل من) الجريمة المعلوماتية ذاتها، والمجني عليه، والتحقيق الجنائي) من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية، ولتحقيق ذلك أجريت الدراسة على العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية حيث تكونت العينة من(125) شخص تم اختيارهم بطريقة العينة المتيسرة من مجتمع الدراسة، وقام الباحثان باستخدام أداة الاستبانة لجمع المعلومات حيث تكونت الاستبانة من (26) فقرة، وقد توصلت الدراسة إلى النتائج التالية: أن معوقات مكافحة الجرائم

المعلوماتية؛(المتعلقة بالجريمة المعلوماتية ذاتها كانت بدرجة كبيرة حيث بلغ الوسط الحسابي) 3.51 في حين جاءت درجة المعوقات المتعلقة بالمجني عليه بدرجة متوسطة حيث بلغ الوسط الحسابي(3.39)، أما درجة المعوقات المتعلق بالتحقيق الجنائي كانت كبيرة حيث بلغ الوسط الحسابي (3.55)؛ وفي ضوء نتائج الدراسة أوصى الباحثان بعدد من التوصيات أبرزها ضرورة تدريب وتأهيل العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية، وضرورة التنسيق بين الأجهزة الأمنية لمكافحة تلك الجرائم، وتشجيع المواطنين عن الإبلاغ عن الجرائم المعلوماتية، وزيادة وعي المواطنين بمخاطر تلك الجرائم.

– وقد أجرى العنزي سليمان بن مهجع (2003)، دراسة بعنوان: " **وسائل التحقيق في جرائم نظم المعلومات**" ماجستير، هدفت هذه الدراسة إلى تحديد وسائل التحقيق في الجرائم المعلوماتية وذلك بالكشف عن الجوانب المختلفة المحيطة بجريمة نظم المعلومات بتجديد أنماطها ودوافعها وإبراز أضرارها، وحصر الأساليب والأدوات المستخدمة من قبل المجرمين نظم المعلومات.

وقد تميزت الدراسة الحالية عن الدراسات السابقة في النواحي الآتية: أنها جاءت كدراسة تأصيلية نظرية لأسس والمفاهيم حول الجريمة الإلكترونية، وفقا للمنهج الوصفي.

2.2- لإطار النظري:

1.2.2- موضوع الجريمة الالكترونية:

إن الجريمة المعلوماتية إما أن تقع على جهاز الحاسب ذاته بمكوناته المادية Hardwareأو المنطقيةSoftware، وإما أن تقع بواسطة الحاسب وبالتالي يكون الحاسب مجرد وسيلة لاقترافها ، وبالتالي سنميز بين حالات ثلاث فيما يأتي : (طاهر جمال الدين كرابيج: 2010-2011)

- **الحالة الأولى: وقوع الجريمة على المكونات المادية للحاسب:**

وتتحقق هذه الحالة إذا كانت أجهزة الحاسب ومكوناته المادية من أجهزة ومعدات وكابلات وشبكات ربط وآلات طباعة وشرائط خام من التي يُسجل عليها البرامج والمعطيات هي محلاً أو موضوعاً لهذه الجريمة.

- **الحالة الثانية: وقوع الجريمة على المكونات المنطقية(الغير مادية) للحاسب:**

وتتحقق هذه الحالة عندما تكون مكونات الحاسب المعلوماتية الغير مادية مثل البرامج المستخدمة والبيانات والمعطيات المخزنة في ذاكرة الحاسب ، محلاً أو موضوعاً للجريمة حيث من المتصور عملاً أن يقوم أحد الأشخاص بالاعتداء على برنامج الحاسب أو أن يدعي ملكيته أو يقوم بسرقته أو

يقلده أو يتلفه أو يعطله أو يقوم بإفشاء محتوياته، أما البيانات أو بنك معلوماته فيستطيع العبث بها، كتحريفها أو تزويرها أو نسخها.

- **الحالة الثالثة: حالة استخدام الحاسب كأداة لارتكاب الجريمة:**

في هذه الحالة لا يكون الحاسب محل أو موضوع الجريمة، وبالتالي لا يكون محلاً للحماية الجنائية ولكن تقع الجريمة في هذه الحالة بواسطته أي أنه يستخدم كأداة لارتكابها ... ومن الناحية النظرية، يمكن أن تقع بعض الجرائم بواسطة الحاسب مثل الجرائم التي تقع على الذمة المالية من سرقة ونصب وخيانة الأمانة والتزوير في عمليات السحب على الجوائز وانتهاك حرمة الحياة الخاصة، بل وتستخدم في القتل وذلك عن طريق برمجة جهاز تفجير يتم التحكم فيه آلياً أو جهاز لإطلاق الأشعة القاتلة ومرتكب هذه الجرائم هو المستخدم أو المتلاعب في الحاسب ونظامه الأخير ما هو إلا وسيلة أو أداة لتنفيذ الجريمة ومحلها يختلف بحسب الشيء الذي ينصب عليه سلوك الفاعل والذي يُشكل محل الحق أو المصلحة المحمية.

2.2.2- سمات المجرم المعلوماتي:

هو إنسان اجتماعي بطبعه يمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى، ويمكن حصر السمات الأساسية لمجرم المعلوماتية في ما يلي: (شريفة، صليحة، 2017، ص ص 49-50)

- **مجرم متخصص:** له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفرات، ويسبح في عالم الشبكات ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات.

- **مجرم يعود للإجرام:** يتميز المجرم المعلوماتي بأنه يعود للجريمة دائما، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات. فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته في الاختراق.

- **مجرم محترف:** له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.

- **مجرم ذكي:** حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب.

3.2.2- تصنيف مرتكبي الجرائم الالكترونية:

ويمكن تصنيف المجرم الإلكتروني في أربع مجموعات رئيسية وهي: (شروق سامي: 2014، ص ص 47-48)

- **المجموعة الأولى:** الموظفون العاملون بمراكز الكمبيوتر وهم يمثلون الغالبية العظمى من مرتكبي الجرائم الإلكترونية وذلك بحكم سهولة اتصالهم بالحاسب ومعرفتهم بتفاصيله الفنية.

- **المجموعة الثانية:** الموظفون الساخطون على مؤسساتهم أو شركاتهم والذين يستغلون معرفتهم بأنظمة الحاسب الآلي في شركاتهم وسيلة لإيقاع الضرر بهم عبر نشر البيانات أو استعمالها أو مسحها.

- **المجموعة الثالثة:** فئة العابثين مثل الهاكرز (HACKERS) أو الكراكرز (CRACKERS) وهم الذين يستغلون الكمبيوتر من أجل التسلية في أمور غير قانونية وليس غرض التخريب.

- **المجموعة الرابعة:** الأفراد الذين يعملون في مجال الجريمة المنظمة عبر استخدام الكمبيوتر.(شبكة الارهاب- الجوسسة...الخ).

4.2.2- دوافع مرتكبي الجريمة الالكترونية:

وتتمثل هذه الدوافع في نقاط أساسية كما يلي:

أ- **السعي إلى تحقيق الكسب المالي:** تعد الرغبة في تحقيق الثراء من العوامل الرئيسية للارتكاب الجريمة عبر الانترنت، وهو من أهم الدوافع وأكثرها تحريكا للمجرم. (صالح، انيسة: 2014-2015، ص30)

فقد تدفع الحاجة البعض إلى تحقيق الثراء السريع او البحث عن حلول لأزمته المادية لارتكاب مثل هذه الجريمة؛ وذلك بالتلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات ثم بيع المعلومات المتحصل عليها بأسعار باهضه، او تحويل الأموال لحساباتهم الشخصية.

ب- **دافع الانتقام:** يعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى إرتكاب الجريمة لأنه غالبا ما يصدر من شخص يملك معلومات كبيرة عن مؤسسة أو الشركة التي يعمل بها، ويقوم بدافع الانتقام إما نتيجة فصله من العمل أو تخطيه في الحوافز أو الترقية، او زرع فيروسات في أجهزة العمل أو سرقة صور شخصية بنية التحرش أو التهديد.

ت- **دوافع ذهنية ونمطية:** الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنت غالبا هي صورة البطل و الذكي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فغالبا ما يكون الدافع لدى مرتكبي جرائم المعلومات هي الرغبة في إثبات الذات وتحقيق انتصار على تقنية المعلومات (صالح، انيسة: المرجع نفسه، ص 31)، وهم فئة غير خطيرة لان دافعهم هو الفضول بالدرجة الأولى وليس الربح ولا يملكون أية نوايا سيئة.

ث- **دوافع سياسية:** وتتمثل في الرغبة في الدفاع عن الآراء والأيدولوجيات مما ينتج عنه نشاط ارهابي الكتروني وافعال اجرامية ضد المعارضين.

ج- **دافع التهديد والمنافسة:** ينتشر هذا الدفع نتيجة الوقوع تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة. (صالح، انيسة: المرجع نفسه، ص 33) لمحاولة اكتشاف أسرار المنافسين.

5.2.2- مراحل حدوث الجريمة الالكترونية:

عادة ما تحدث الجريمة الإلكترونية في إحدى المراحل التالية: (شروق سامي: المرجع السابق، ص ص 48-49)

- **المرحلة الأولى:** وتتمثل في مرحلة إدخال البيانات. فعلى سبيل المثال قيام المجرم الإلكتروني بتغيير أو تزوير البيانات مثل: فاتورة الهاتف، كشف النقاط...الخ.

- **المرحلة الثانية:** وتتمثل في مرحلة تشغيل البيانات، مثل قيام المجرم الإلكتروني بتغيير أو تعديل البرامج الجاهزة (soft wear)التي تقوم بتشغيل البيانات للوصول إلى نتائج محددة أو مقصودة بطريق غير شرعي من قبل الجاني، مثل: تجميع الفروق بين الأرقام المقربة والأرقام الفعلية وإضافتها لحساب سري آخر لنفس العميل...وقد تبدو هذه الفروق بسيطة ولكنها ستكون كبيرة إذا تمت إضافتها خلال عدة سنوات.

- **المرحلة الثالثة:** مرحلة إخراج البيانات، ومثل ذلك سرقة بعض البيانات الإلكترونية أو المعلومات الآلية المتعلقة بمراقبة مخزون إحدى الشركات.

6.2.2- صعوبة مكافحة الجريمة الإلكترونية:

من أهم صعوبات مكافحة الجرائم الإلكترونية: (سعيد وآخرون: 2016، ص41)

- عدم كفاية القوانين ومواكبتها للتطورات التقنية في كثير من الدول.

- احجام الكثير من الجهات التبليغ عن تلك الجرائم.
- سهولة إخفاء معالم الجريمة.
- عدم وجود دليل مادي واضح.
- صعوبة الوصول إلى الدليل في بعض الأحيان.
- وجود كم هائل من المعلومات بتعيين فحصها.

3- آلية التحقيق في الجرائم الإلكترونية:

يمر التحقيق في الجرائم الإلكترونية بمرحلتين رئيستين: المرحلة الأولى تمثل الإجراءات التي يتم تنفيذها في مسرح الجريمة، وتشمل إغلاق أو تجميد مسرح الجريمة لمنع فقدان أو تلف أو تلوث الأدلة والحفاظ على مسرح الجريمة وتأمينه ومنع العبث به؛ والمرحلة الثانية تشتمل على الإجراءات التالية التي ينبغي على فريق مسرح الجريمة من مأموري الضبط القضائي، ذوي الاختصاص، القيام بها، وهي:

توثيق حالة مسرح الجريمة، أي تسجيل كافة التفاصيل المتعلقة بحالة الكمبيوتر، مثل تحديد ما إذا كان في وضع التشغيل (مفتوحا) وقت ضبطه أم لا، وما إذا كان موصولاً بالإنترنت أم لا؛ تحديد هوية وتوثيق جهاز الكمبيوتر والأجهزة الملحقة به التي يعثر عليها في مسرح الجريمة، حيث أن رمز بروتوكول الإنترنت يلعب دورا كبيرفي تحديد موقع ومكان المشتبه به؛ (IP) التي يعثر عليها في مسرح الجريمة؛ (DVDs و CDs تحديد هوية وتوثيق أجهزة التخزين (مثل تصوير مسرح الجريمة؛ حفظ الأدلة والمواد الرقمية؛6 حفظ الوثائق المطبوعة؛ حفظ الأجهزة؛ إجراء استرجاع للوثائق العالقة، من قبيل طباعة الأوراق العالقة في ماكنة الطباعة؛ إجراء استرجاع للوثائق الملغاة أو التي تم مسحها؛ نقل الأدلة التي يتم ضبطها. (مصطفى:2018، ص 286).

4- معدلات الجريمة الالكترونية على المستوى العالمي:

القضية كبيرة وأكبر مما نتصور، ففي بريطانيا وفي عام 2007 هناك جريمة الكترونية تقع كل 10 ثواني (3 مليون جريمة بالسنة، أو 8 آلاف جريمة باليوم). وأكبر نسبة فيها تعود لجرائم التحرش الجنسي (850 ألف حالة) ، بينما هناك 92 ألف حالة لسرقة الهوية أي الحصول على معلومات شخصية حول مستخدمي الانترنت، و 145 ألف حالة لاختراق الحواسيب بهدف سرقة المعلومات أو التخريب، و 207 ألف حالة للحصول على الأموال من خلال الاحتيال للسطو على أرقام البطاقات الائتمانية. وتقول إحصائيات شركات التأمين أن 70% من هذه الجرائم تستهدف الأفراد.(سمير وآخرون: 2011، ص 49)

الأطفال هم من أكثر ضحايا الجريمة الالكترونية على الانترنت الإحصائيات العالمية تقول أن 80 % من الأطفال الذين يستخدمون البريد الإلكتروني يستقبلون رسائل بريد إلكتروني دعائية كل يوم وبخاصة خلال فترات العطلة حيث يقضي الأطفال الكثير من الوقت في تصفح الإنترنت. وبعض تلك الرسائل تتضمن محتوى لا ينبغي عليهم أن يطلعوا عليه في أي حال من الأحوال. والمشكلة تكمن في أن معظم الأطفال لا يتجاهلون الرسائل الطفيلية ويفتحونها مدفوعين بالفضول الذي تحركه لديهم العناوين الرنانة لتلك الرسائل، وغالبًا يفتح الطفل الرسالة. الكثير من هؤلاء الأطفال بالطبع ينزعجون من تلك الرسائل ولا يناقشون الموضوع مع أهاليهم، بعضهم الرسائل تثير فضولهم ويطلعون عليها، وحتى عندما يطلعون على محتوى تلك الرسائل فإن الكثير منهم لا يطلعون أهاليهم على ذلك.. ويتم استدراج الأطفال عن طريق غرف الدردشة أو عن طريق طلب صورهم والعبث فيها ونشرها فوق أجسام عارية وخاصة في حالة صور الفتيات. .(سمير وآخرون: 2011، ص 49)

5- توصيات لتحدي الجريمة الإلكترونية:

ينبغي على كل متعامل مع الشبكة الإلكترونية أن يحتاط مسبقا لكي لا يقع ضحية هذا النوع من الجرائم ويكون ذلك من خلال تتبع النقاط التالية:

- توعية الناس بمفهوم الجريمة الإلكترونية وأنه الخطر القادم ويجب مواجهته والحرص على ألا يقعوا ضحية له.
- ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية كبطاقة ائتمانية أو حساب البنكي.
- عدم الافصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمات سر غير مألوفة.
- عدم حفظ الصور الشخصية في الكمبيوتر.
- عدم تنزيل أي ملف أو برنامج من مصادر غير معروفة.
- عدم إيقاف برامج مكافحة الفيروسات والجدار الناري.
- الحرص على تحديث أنظمة الحماية.
- تكوين منظمة لمكافحة الجريمة الإلكترونية.
- إبلاغ الجهات المختصة في حال التعرض لجريمة إلكترونية.

– وضع أنظمة تشريعية متطورة لتنظيم البيئة القانونية والتنظيمية والتي تخدم أمن تقنيات ونظم المعلومات.

– تتبع تطورات الجريمة الإلكترونية وتطوير الوسائل والأجهزة والتشريعات لمكافحته.

– تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية وبرمجيات الفيروسات وبرامج التجسس.

– تعزيز الحوار بين أفراد الأسرة وطلب الاستشارة.

– رفع مستوى الوعي عند الأفراد بعدم استعمال معلوماتهم الشخصية.

– اشراف الكبار على الأطفال والفتيات الصغيرات والمراهقات، وربما حتى المتزوجات.

وتبقى أهم خطوة في مكافحة جرائم الانترنت هي تحديد هذه الجرائم بداية ، ومن ثم تحديد الجهة التي يجب أن تتعامل مع هذه الجرائم والعمل على تأهيل القائمين على النظر فيها بما يتناسب وطبيعة هذه الجرائم المستجدة، ويأتي بعد ذلك وضع تعليمات مكافحتها والتعامل معها

6- الخلاصة:

مما سبق يمكننا تحديد مفهوم للجريمة الالكترونية جريمة وهو تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات موضوعها وقوع الجريمة على المكونات المادية للحاسب، وقوع الجريمة على المكونات المنطقية(الغير مادية) للحاسب حالة استخدام الحاسب كأداة لارتكاب الجريمة. كما تطرقنا لأهم سمات المجرم المعلوماتي فهو مجرم متخصص، مجرم يعود للإجرام محترف و ذكي.

وكذا يمكننا تصنيف مرتكبي الجرائم الالكترونية إلى أربع فئات الموظفون العاملون بمراكز الكمبيوتر وهم يمثلون الغالبية العظمى من مرتكبي الجرائم الإلكترونية، والموظفون الساخطون على مؤسساتهم أو شركاتهم، وفئة العابثين مثل الهاكرز (HACKERS) أو الكراكرز (CRACKERS) وأخيرا الأفراد الذين يعملون في مجال الجريمة المنظمة. وقد تم تحديد دوافع مرتكبي الجريمة الالكترونية في بعض النقاط منها السعي إلى تحقيق الكسب المالي، الأسباب الشخصية، الانبهار بالتقنية المعلوماتية والدوافع سياسية وتجارية. تحدث الجريمة الالكترونية خلال مراحل وهي مرحلة إدخال البيانات، مرحلة تشغيل البيانات، مرحلة إخراج البيانات. وفي الاخير تم توضيح أهم صعوبة مكافحة الجريمة الإلكترونية وكذا طرق الوقائية للتصدي للجريمة الإلكترونية.

المراجع:

1. أكرم عبد الرزاق المشهداني (2005)، **واقع الجريمة واتجاهاتها في الوطن العربي، دراسة تحليلية لجرائم السرقات والقتل العمد والمخدرات**، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.
2. بن غذفة شريفة، القص صليحة، **الجريمة الإلكترونية ضد المرأة على صفحات الانترنت وطرق محاربتها**، أعمال الملتقى: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائي، الجزائر.
3. بن منصور، كوش آنيسة، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة ماستر في الحقوق، تخصص قانون خاص والعلوم الجنائية، جامعة عبد الحمان ميرة–بجاية– كلية الحقوق والعلوم السياسية، قسم القانون الخاص.
4. حنان ريحان مبارك المضحاكي(2014)، **الجرائم المعلوماتية**، بيروت: منشورات الحلبي الحقوقية.
5. سعيد بن سالم البادي، زايد بن حمد الجنيبي، يوسف الشيخ يوسف حمزة، محمود أحمد العطاء (2016)، **الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها**، سلطنة عمان: مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة نزوي.
6. سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن (2011)، **الجريمة الإلكترونية عبر الانترنيت أثرها وسبل مواجهتها**، مجلة التقني، المجلد: 24، جامعةFoundation of technical education.
7. شروق سامي فوزي (2014)، **تكنولوجيا الإعلام الحديث**، القاهرة: مؤسسة طيبة للنشر والتوزيع.
8. طاهر جمال الدين كرابيج (2010–2011)، **الجريمة المعلوماتية**، الصحيفة القانونية الالكترونية، عن طريق الموقع: http://jle.gov.sy/index.php اطلع عليه بتاريخ:19–02–2019، الساعة: 10:54.
9. عبد الجبار عريم(1970)، **نظريات علم الإجرام**، بغداد: دار المعارف.
10. عبد الفتاح بيومي حجازي (2006)، **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي نموذجي**، الإسكندرية، القاهرة: دار الفكر الجامعي.
11. عصام حسني الأطرش، محمد محي الدين عساف يونيو(2019)، **معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية**، مجلة جامعة الشارقة للعلوم القانونية، المجلد16،العدد01، الشارقة.

12. العمرابي، صالح التوم (2006)، الجرائم المعاقب عليها بالقتل في الشريعة والقانون، الخرطوم: دار عزة للنشر والتوزيع.
13. العنزي سليمان بن مهجع (2003)، **وسائل التحقيق في جرائم نظم المعلومات**، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، السعودية.
14. فاضل عباس خليل (آيار 2007)، **تطور الشبكة الدولية للمعلومات ودورها كوسيلة إعلامية متقدمة**، مقال في مجلة جامعة تكريت للعلوم الانسانية، بالكويت، المجلد 14، العدد5.
15. فاطمة الزهرة خبازي (29 مارس 2017)، **جرائم الدفع الإلكتروني وسبل مكافحتها**، أعمال الملتقى: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائي، الجزائر.
16. مصطفى عبد الباقي (2018)، **التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة**، دراسات، علوم الشريعة والقانون، المجلد45، عدد4، ملحق2،الأردن.
17. نجلاء عبد الفتاح طه (2015)، **دور الاعلام في حل القضايا المعاصرة (الإرهاب- جرائم- قضايا العولمة)**، الاسكندرية: دار التعليم الجامعي.
18. نسرين حسونة 2015/2/28 ميلادي - 1436/5/11 هجري. **تكنولوجيا الحاسب الإلكتروني**، مقال على شبكة الألوكة. تم الاطلاع على المقال:2019/03/16.على الساعة: 01:00.
19. يوسف جفال(2016-2017)، **التحقيق في الجريمة الإلكترونية**، رسالة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف- المسيلة.

كيفية الاستشهاد بهذا المقال حسب أسلوب APA:

ذياب سليمة، بوترعة بلال، (2020) **الجريمة الإلكترونية: الأسس والمفاهيم**، مجلة تطوير العلوم الاجتماعية، المجلد 13 (العدد 01)، الجزائر: جامعة زيان عاشور الجلفة، ص.ص07-20.