

الجريمة الإلكترونية – قراءة سوسيو تاريخية في النشأة والآثار

Electronic crime: A Sociohistorical- Reading on its origin and impacts

عفاف بعون¹، نسيم أولاد سالم²¹ جامعة قاصدي مرباح ورقلة (الجزائر)، yasminenina05@gmail.com² جامعة قاصدي مرباح ورقلة (الجزائر)، nassimanoss3@gmail.com

تاريخ الاستلام : 2023/09/16 ؛ تاريخ القبول: 2023/10/05 ؛ تاريخ النشر : 2023/12/22

ملخص الدراسة:

أصبحت الجرائم الإلكترونية اليوم تطرح عدة إشكاليات خطيرة على الصعيدين الاقتصادي والقانوني وحتى الاجتماعي منها، فهي تشكل خطراً على كافة الأعمال الاقتصادية في قطاع المعلوماتية ليس هذا فحسب، بل باتت تهدد الحياة الشخصية للأفراد وأمنهم كذلك، حيث انتقلت من الجانب الاقتصادي إلى الجانب الاجتماعي، وبهذا فهي تشكل تحدياً خطيراً على الجانب الاقتصادي فتؤدي إلى خسائر مالية كبيرة للأفراد والمؤسسات والحكومات، وعلى المستوى القانوني فهي تشكل تحدياً للقوانين الدولية، حيث تتطلب مكافحتها تطوير التشريعات والسياسات الفعالة. تناولت هذه الدراسة الجريمة الإلكترونية من خلال قراءة سوسيو تاريخية في النشأة والآثار، وأظهرت النتائج أن الجريمة الإلكترونية ليست ظاهرة حديثة، فقد بدأت مع انتشار التكنولوجيا والانترنت في القرن العشرين. وتؤثر بشكل كبير على الحياة الخاصة للأفراد وحياتهم الاجتماعية والاقتصادية.

الكلمات المفتاحية: الجريمة الإلكترونية؛ الأسباب والدوافع؛ المجرم الإلكتروني؛ الآثار الاجتماعية.

Abstract:

Today, electronic crimes raise several serious issues on economic, legal, and even social levels. They pose a threat to all economic activities in the IT sector and endanger individuals' personal lives and security. These crimes have shifted from the economic to the social side, presenting a serious challenge to the economic side as they lead to significant financial losses for individuals, institutions, and governments. Legally, they challenge international laws, requiring the development of effective legislation and policies to combat them. This study approached electronic crime through a socio-historical reading of its emergence and effects. The results showed that electronic crime is not a new phenomenon, as it began with the spread of technology and the internet in the twentieth century. It significantly affects individuals' private lives and their social and economic life.

Keywords: Electronic crime; Causes and Motivation; Cybercriminal; Social effects

- مقدمة:

تعد الجريمة الإلكترونية من أهم المشكلات التي تواجه المجتمع الحديث، حيث تعددت أشكالها وأنواعها وتطورت مع التطور التكنولوجي الذي شهده العالم خلال العقود الماضية. فهي تعد نتيجة لتقدم التكنولوجيا واستخدام الأفراد للتقنية بصورة غير مشروعة أو غير قانونية. ومن بين الأسباب التي تؤدي إلى الجريمة الإلكترونية هي عدم وعي الأفراد بأخلاقيات الإنترنت والتكنولوجيا وسهولة الوصول إلى الأدوات والبرمجيات المستخدمة في الهجمات الإلكترونية. كما أن الجريمة الإلكترونية ترتبط أيضاً بالظروف الاقتصادية والاجتماعية للأفراد، حيث يقوم بعض الأفراد بارتكاب الجريمة الإلكترونية كوسيلة للحصول على المال أو لتحقيق غايات شخصية.

ومن آثار الجريمة الإلكترونية على المجتمع، تأثيرها على الاقتصاد العالمي والتأثير السلبي الذي يمكن أن تحدثه في الأمن الإلكتروني للدول والشركات. كما أنها قد تؤدي إلى فقدان الثقة بين الأفراد فيما بينهم وزيادة الانعزالية والتشكيك بالآخرين. وقد تؤدي أيضاً إلى تأثير سلبي على الصحة النفسية للأفراد المتضررين من الهجمات الإلكترونية.

ولحل مشكلة الجريمة الإلكترونية، يجب تحديد الأسباب التي تؤدي إليها وتطوير استراتيجية الأمن السيبراني. كون الجريمة الإلكترونية تشكل التحدي الأمني الحديث الذي يواجهه العالم في الوقت الحالي، فهي تمثل تهديدًا للأمن الرقمي وترزعزع الاستقرار الاجتماعي والاقتصادي. فكما تعرف الجريمة الإلكترونية فإنها عملية جنائية تتم باستخدام التكنولوجيا الحديثة، وتشمل العديد من الجرائم، مثل الاحتيال الإلكتروني والتجسس الإلكتروني والتشويش الإلكتروني والاعتداءات الإلكترونية والابتزاز الإلكتروني وغيرها.

لهذا تحتاج الجريمة الإلكترونية إلى دراسة وتحليل عميق من منظور سوسيولوجي، حيث يتم تحليلها وفقًا للظروف الاجتماعية والاقتصادية والثقافية التي تؤثر عليها. ومن هذا المنطلق، فإن منظور سوسيولوجي يساعد على فهم العوامل المؤثرة على زيادة الجرائم الإلكترونية وما يحفز الأفراد على ارتكابها، وما هي الثقافات والتقاليد التي تؤدي إلى زيادة مخاطر الجرائم الإلكترونية. كما تعتبر الجريمة الإلكترونية أيضًا عاملاً رئيسيًا في تغيير الأنظمة الاجتماعية والثقافية والاقتصادية في العالم. فهي تتطلب إعادة تفكير المفاهيم التقليدية للجريمة والعدالة والأمن، وتفعيل أدوات الحوكمة الرقمية للتصدي لها. ومن هذا المنطلق، فإن الجريمة الإلكترونية تمثل تحديًا كبيرًا للمجتمعات والحكومات في الوقت الراهن، وتحتاج إلى دراسة شاملة لفهم العوامل المؤثرة.

01. إشكالية الدراسة:

أصبحت الجرائم الإلكترونية اليوم تطرح عدة إشكاليات خطيرة على الصعيدين الاقتصادي والقانوني وحتى الاجتماعي منها، فهي تشكل خطراً على كافة الأعمال الاقتصادية في قطاع المعلوماتية ليس هذا فحسب، بل باتت تهدد الحياة الشخصية للأفراد وأمنهم كذلك، حيث انتقلت من الجانب الاقتصادي إلى الجانب الاجتماعي، فزيادة التقنيات العالية الدقة مكنت بعض الأشخاص من استغلالها في تخريب وابتزاز غيرهم بدوافع شخصية، معنوية، وحتى المادية منها.

لم تكن الجرائم المتعلقة بالإنترنت متطورة في بداية ظهورها، لكن التطور الذي عرفته نظم المعلوماتية والشبكة العنكبوتية ساعدت في تطوير تلك الجرائم، حتى أصبح تأثيرها واسع مس مختلف مؤسسات المجتمع. ومن هذا المنطلق ارتأينا طرح التساؤل الآتي: ما هي الجريمة الإلكترونية، وكيف ظهرت؟ وما هي آثارها على الأفراد والمجتمعات؟

02. أهداف الدراسة:

تسعى الدراسة الحالية إلى تحقيق جملة من الأهداف، ونهدف من خلال هذه الدراسة إلى:

- تحديد مفهوم الجريمة الإلكترونية في شكلها المعاصر.
- تحديد ورصد أهم التغيرات التي حدثت على مفهوم الجريمة من شكلها التقليدي إلى ما هي عليه الآن.
- الكشف عن الآثار الاجتماعية والنفسية التي يخلفها الجريمة الإلكترونية سواء على المستوى الفردي أو الأسري أو المجتمع.

03. أهمية الدراسة:

تكتسي معالجة هذا النوع من المواضيع أهمية بالغة، ذلك بالنظر إلى الآثار التي يخلفها على المستويين الفردي والمجتمعي، إضافة للإشكالات العلمية التي يطرحها على المستوى القانوني ذلك لتمييزها بمجموعة من الخصائص التي جعلتها تختلف عن غيرها من الجرائم. ولكونها انتشرت في المجتمع بصورة جلية خاصة في السنوات الأخيرة التي عرفت تطورا تكنولوجيا وقفزة تقنية متميزة وواسعة. كل هذا ساهم في تطوير مهارات بعض الأفراد مما سمح لهم بالولوج إلى عالم الجريمة السيبرانية واختراق أنظمة وبرامج كانت يشهد لها بالأمن ومحافظة على سرية وخصوصية الأفراد والمؤسسات وحتى الدول.

ومنه تحظى الجريمة الإلكترونية بأهمية كبيرة في الدراسات السوسيولوجية، حيث تعد تطورا مهما في مجالي الجريمة والعدالة الجنائية في العالم الرقمي الحديث، فهي تتسم بالتطور والتغير السريع، حيث تتغير الأساليب والتقنيات باستمرار وتتطور الجرائم الإلكترونية بسرعة. وبالتالي، فإن دراسة الجريمة الإلكترونية من منظور سوسيولوجي يمكن أن تساعد في فهم الأسباب والتأثيرات المتعلقة بالجريمة الإلكترونية وكيفية مواجهتها.

04. الدراسات السابقة:

هناك مجموعة من الدراسات والبحوث الأكاديمية التي ساعدتنا في تناول هذا الموضوع، وكانت بمثابة الدعامة الأولى للانطلاق في خوض غمار هذا البحث. ومن بين تلك الدراسات نجد:

دراسة "عبد الحليم بوقرين" و "صورية قلالي" الموسومة بـ: " أثر الجريمة الإلكترونية على الحياة الخاصة للأفراد" حيث تناول الباحثان إشكالية مفادها: ما مدى تأثير الجريمة الإلكترونية على الحق في الحياة الخاصة؟ تطرق الباحثان إلى تأثير الانتهاك الإلكتروني على الحياة الخاصة للأفراد، وخلصا إلى أن وسائل الاتصال والأنترنت كما لها إيجابيات فإنه أيضا لها سلبيات وأثر في انتهاك الخصوصية في التنصت على الأفراد واعتراض اتصالاتهم وتتبعها. وأصبحت تتزايد جريمة انتهاك الحياة الخاصة للأفراد، كما أن البيانات الشخصية الموجودة على شبكات التواصل الاجتماعي أصبحت عرضة لعدد من المخاطر.

دراسة "معاشي سميرة" الموسومة بـ " الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)"، هدفت الباحثة من خلال هذه الدراسة إلى معرفة الاتجاهات والتصنيفات المختلفة لمفهوم الجريمة المعلوماتية، وكذا إلى معرفة الخصائص المشتركة بينها وبين الجرائم الأخرى. وخلصت إلى عدم وجود مفهوم مشترك لماهية الجريمة المعلوماتية ولا تعريف قانوني دولي موحد لها. وأن التعريفات التي قدمت إلى هذا النوع من الجرائم إنما بني على معيار قد يرجع إلى طبيعة وسيلة ارتكاب الجريمة أو محل الجريمة أو ربما إلى دوافع ارتكابها.

دراسة "سمير شعبان" (2009) الموسومة بـ: "الجريمة الإلكترونية، مقارنة تحليلية لتحديد مفهوم الجريمة والجرم"، حاول الباحث من خلال بحثه هذا التطرق إلى تحديد مفهوم الجريمة الإلكترونية وذلك من خلال عرض تصنيفين للتعريفات، الأول تمثل في التعريفات القائمة على معيار واحد، وهي بدورها قسمت إلى: تعريفات قائمة على المعيار القانوني، وأخرى على معيار شخصي. أما التصنيف الثاني فتمثل في تعدد المعايير والتي تشمل التعريفات

التي تبرز موضوع الجريمة وأنماطها. كما تطرق الباحث إلى تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة ودور الكمبيوتر. وتعرض في بحثه إلى القائم بهذه الجرائم وخصائصه، وختم البحث بدوافع ارتكاب الجريمة الإلكترونية. استغلت هذه الدراسات في التحليل وكذا تفسير بعض جوانب البحث، كما تم الاستفادة منها في تحديد بعض أبعاد الجريمة الإلكترونية التي كانت تبدو غامضة نوعا ما بالنسبة لنا.

المحور الأول: المحددات التاريخية والمفاهيمية للجريمة الإلكترونية

1- النشأة ومراحل التطور التاريخي للجريمة الإلكترونية.

إن مفهوم الجريمة الإلكترونية مر بتطور تاريخي تبعا لتطور التقنيات واستحداثها وخاصة بعد أن أصبحت المجتمعات تعتمد على الحاسب الآلي بشكل رئيسي.

لقد مرت الجريمة الإلكترونية في تطورها بعدة مراحل منذ رصدها في الإحصائيات لأول مرة في الفترة (1971-1990) تضمنت أبرز الجرائم التي تم رصدها وضبطها على نطاق العالم وهي قليلة جدا ويتراوح عددها بين جريمة واحدة إلى ثلاثة في العالم وأشهرها في عام 1988م عندما استخدم الحاسب الآلي لسرقة 70 مليون دولار من بنك شيكاغو الوطني الأول، وفي ذات العام 1988 تم لأول مرة تكوين فريق طوارئ الحاسب الآلي (CERT) في معهد هندسة البرمجيات بجامعة "كارنيجي ميلون" الأمريكية لمواجهة الجريمة الإلكترونية بأشكالها المختلفة. وفي عام 1989 تبنت اللجنة الوزارية لمجلس أوروبا التوصية رقم 9 (89) الخاصة بمواجهة جرائم الحاسب الآلي.

وفي عقد التسعينات ارتفع معدل الجرائم الإلكترونية نسبيا وكان أشهرها عام 1994م عندما كان عدد مستخدمي الانترنت حول العالم 25.454.590 مليار اخترق طالب أمريكي عمره 16 سنة اسم الشهرة **data Stream** (نهر البيانات) أجهزة كمبيوتر في معهد أبحاث الطاقة كوري - وكالة ناسا ووكالات حكومية أمريكية أخرى وتم اعتقاله في إنجلترا. وفي عام 1995 تمكنت عصابة روسية محترفة من سرقة عشرة ملايين دولار من مصرف سيتي بنك باستخدام الكمبيوتر وتحويلها إلى حسابات في فنلندا وإسرائيل. وبدأت العمليات الإجرامية الإلكترونية في التزايد في مختلف دول العالم إلى يومنا هذا وبدأت الجهود الدولية والإقليمية بوضع استراتيجيات للوقوف في وجه هذه الجرائم المستحدثة. (مجمع البحوث والدراسات، 2016، ص ص 9-10)

وعليه فقد مرت الجريمة الإلكترونية بتطور تاريخي تبعا للتطورات التقنية والتكنولوجية، وكانت المراحل كالتالي: (حبايب، 2022، ص ص 25-28)

أ. مرحلة الخمسينيات من القرن الماضي

تعد بداية صناعة الحواسيب وانطلاق ثورة تكنولوجيا المعلومات الإلكترونية مستقلة عن وسائل الاتصال التي وقعت بأربعينيات القرن الماضي وعليه يعد تاريخ ظهور الجرائم الإلكترونية حديثا نسبيا، حيث ارتبط ظهورها التاريخي مع ظهور الكمبيوتر وانتشار استعماله والذي كان عام 1954 في الولايات المتحدة الأمريكية، حيث بدأ طرح أول جهاز كمبيوتر للشراء وبدأ الاستخدام التجاري للحواسيب في الخمسينيات ومنذ ذلك الوقت بدأت

ظاهرة جرائم الحاسوب في الظهور، ولكن كانت بدايتها تقتصر على إساءة استخدام الحاسوب على البعد الأخلاقي، حيث تم تسجيل أول جريمة إلكترونية في الولايات المتحدة الأمريكية عام 1957، وبعدها صدرت عدة تقارير تبين نسب ورصد حالات إساءة استخدام الحاسوب وصنفت هذه الجريمة إلى جرائم العبث والتخريب وسرقة المعلومات أو الاحتيال والاستخدام غير المصرح به، وفي هذا الوقت كان هناك عدم التمييز بين الجرائم التي تستهدف مادية الحاسوب أو التي تستهدف معطيات الحاسوب بسبب أن الأنشطة الإجرامية المتعلقة بالحاسوب تصاغ وفق مدلول أخلاقي أكثر منه قانوني، أما من حيث التكييف القانوني للجريمة الإلكترونية كانت تتعامل معها بذات الدلالة التي تتعامل معها مع الجرائم التقليدية.

ب. مرحلة الستينيات والسبعينيات من القرن الماضي

بهذه الفترة شاع استخدام الحاسوب وبرز مفهوم إساءة استخدامه والعبث في بياناته مطلع الستينيات، وبدأت الصحف لأول مرة تنشر مقالات بصددتها، وكانت هذه المقالات تناقش فكرة التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر.

ج. مرحلة الثمانينيات من القرن الماضي

في هذه المرحلة ظهر مفهوم جديد لجرائم الكمبيوتر والانترنت يرتبط بعمليات اقتحام نظم الكمبيوتر عن بعد كما ظهرت أنشطة الفيروسات الإلكترونية التي تقوم بتدمير الملفات والبرامج، وشاع مصطلح الهاكرز المعبر عن مقتحمي نظام الكمبيوتر.

د. مرحلة التسعينيات من القرن الماضي والقرن الحالي.

شهدت هذه المرحلة أنواعا فريدة من جرائم الكمبيوتر التي ظهرت بظهور الإنترنت منها الدخول غير المصرح به إلى نظام الكمبيوتر والعبث بمحتوياته وتدميرها والهجوم على مواقع معلوماتية وتدميرها، وشملت جرائم الكمبيوتر التجسس الصناعي والأمني والاستيلاء على بطاقات الائتمان البنكية واستخدامها بطريقة غير مشروعة وكذلك الإساءة إلى سمعة الأفراد وتحقيرهم عبر الرسائل الإلكترونية.

أما في الألفية الجديدة فإنها شهدت تزايدا في حجم الجرائم الإلكترونية ومن خلال ما سبق فإنه يتبين أن الجرائم الإلكترونية لها جذور تاريخية ترجع في ذلك إلى الأربعينيات والخمسينيات من القرن الماضي ولكنها لم تكن معروفة كما هي عليه الآن، حيث بدأت الآن الدول تتسابق في وضع التشريعات التي تعمل على الوقاية والمكافحة من هذه الجرائم الإلكترونية.

وبنتيجة هذا التطور في عالم المعلوماتية نشأت ونمت أنواع جديدة من الجرائم التي ما كانت لتبصر النور لولا ظهور الكمبيوتر حيث شهدت التسعينيات والقرن الحالي أنواعا فريدة من جرائم الكمبيوتر وترافق ذلك مع ظهور الإنترنت وبدأت أنشطة الهاكرز باختراق مواقع المعلومات ونظمه عبر الإنترنت"، والدخول دون تصريح أو تحويل إلى النظم والعبث بالبيانات والمعلومات المخزنة فيها أو تدميرها التي يتيحها الإنترنت بشكل كبير، وكذلك تعطيل الأنظمة والبرمجيات الخبيثة أو التدمير المادي لها أو استغلالها دون تصريح أو الهجوم عبر الإنترنت على مواقع

المعلوماتية لتعطيل عملها، وشملت جرائم الكمبيوتر أنشطة التجسس الصناعي والأمن والاستيلاء على البيانات ذات القيمة الاقتصادية أو الاستيلاء على أرقام بطاقات الائتمان واستخدامها بشكل غير مشروع للاستيلاء على الأموال، وكذلك الإساءة إلى سمعة الأفراد وتحقيرهم عبر الرسائل الإلكترونية أو استغلال مواقع انترنت لترويج محتوى غير قانوني. (يونس عرب، 2002، ص 306)

2- التأصيل المفاهيمي للجريمة الإلكترونية

الجريمة الإلكترونية:

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crimes) والإلكترونية cyber. يستخدم مصطلح الجريمة الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة ويقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت (مثل غرف الدردشة ،والبريد الإلكتروني، والموبايل). (البداينة، 2014، ص 3) وبناء على هذا تم التطرق لتعريف الجريمة لغة واصطلاحاً حتى تتمكن من ضبط مفهوم الجريمة الإلكترونية.

تعريف الجريمة لغة: من الفعل جرم بمعنى كسب وقطع، ولكن خصصت الجريمة عند العرب للدلالة على الكسب القبيح المخالف للحق والعدل. (الخمشي، 2013، ص 17) فيقول أهل اللغة أن الجريمة تأتي بمعنى الجناية وبمعنى الذنب، وجاء في لسان العرب " وجرم إليه وعليه جريمة وأجرم: جنى جناية.

الجريمة اصطلاحاً: يرى كثير من الباحثين أن مفهوم الجريمة يعبر عن الانتهاكات التي يقوم بها الكبار. (القاسمي، 2013، ص 62) الجريمة هي أي فعل أو تجاوز يمكن للدولة تطبيق العقوبات عليه. وهذا هو التعريف الأكثر استخداماً للجريمة. (William, Joseph, 2012, p136)

يشير "جاك روسو" إلى أن الجريمة هي كل فعل أو عمل يسهم في تفكيك روابط العقد الاجتماعي، والجريمة باعتبارها مشكلة اجتماعية وجدت في المجتمعات البشرية بغض النظر عن حجم المجتمع أو بساطته أو تعقيده. (اسماعيل الزبيد، 2010، ص 171) أما "راد كليف براون" فيعرفها بأنها: سلوك من خلاله يقوم المجرم بخرق العادات والقيم والقواعد السائدة في المجتمع مما يتطلب تطبيق العقوبات الجنائية. (هرزاني، 2005، ص 27)

بداية قبل تعريف الجريمة الإلكترونية، لابد من الإشارة بأن هناك تعدد في التعريفات التي تناولت الجريمة الإلكترونية ويرجع ذلك إلى الخلاف الذي أثير بشأن تعريف هذه الجريمة، فالجرائم الإلكترونية هي صنف جديد من الجرائم ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقل بالجريمة من صورتها التقليدية إلى أخرى معاصرة قد يصعب التعامل معها. (الديري، اسماعيل، 2012، ص 40)

تعد الجريمة الإلكترونية ظاهرة إجرامية جديدة يقتربها مجرمون أذكاء يمتلكون أدوات المعرفة التقنية، وتطال اعتداءاتها المعلومات المخزنة والمنقولة عبر نظم وشبكات المعلومات، وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي

والسيادة الوطنية، وأيضا تشجيع فقدان الثقة بالتقنية وتهدر إبداع العقل البشري. (محمد سعيد، 2006، ص 13) وهي مخالفة ترتكب ضد الأفراد أو جماعات بدافع جرمي ويقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية سواء كان ذلك بطريقة مباشرة أو غير مباشرة باستخدام شبكات الاتصالات مثل الانترنت (مثل غرف الدردشة، المجموعات، والبريد الإلكتروني، والموبايل... وغيرها. (شفيق، 2015، ص 16) وهي كل فعل من شأنه القضاء على استخدام التكنولوجيا الحديثة عبر الوسائط الإلكترونية. (عبد الصبور عبد القوي، 2012، ص 92) وعرفها القانون الأمريكي لولاية تكساس رقم 1213 لعام 1986 الخاص بمواجهة جرائم الكمبيوتر بأنها: الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملف البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أم ملف البيانات. (سليبي، 2021، ص 28)

هناك عدة اصطلاحات تستخدم للدلالة على الجرائم الإلكترونية مثل الجريمة المعلوماتية وجرائم التقنية العالية وجرائم الكمبيوتر والانترنت وكلها تستلزم معرفة التقنيات الحديثة والشبكات الإلكترونية والشفرات وأنظمة التحويل المالي. (محمد سعيد، 2006، ص 14)

وتمثل شبكة الإنترنت وجه المجتمع المعلوماتي الجديد بما تنشره من قيم وعادات وتقاليد وثقافة خاصة وكذلك بما تقدمه من قوة كبيرة للنخبة التي تدير هذه الشبكة، والدليل على مدى قوة الإنترنت تقريرا ستار حول "فضيحة كلينتون" على سبيل المثال والذي يعد علامة فاصلة في تاريخ استخدام الإنترنت سياسيا. وتتيح الإنترنت أيضا المعلومات من مصادر متعددة ومتنوعة ومن جهات ذات توجهات مختلفة مما يساعد على مضاهاة مقارنة المعلومات وتقييمها وهي لا تجعل المعلومة حكرا على أحد فالكل يعرفها والكل قادر على الوصول إليها وهي لا تتجاوز مستوى التغطية السطحية للأحداث السياسية. (محمد سعيد، 2006، ص 20)

إن الجريمة الإلكترونية التي اجتاحت العالم بفضل التطور التكنولوجي العالمي أوجدت نوعا من الصعوبة في تحديد مفهوم الجرائم الإلكترونية كظاهرة مستحدثة ويرجع السبب في ذلك كونها نمطا إجراميا من الأنماط المستحدثة التي رافقت التطور التكنولوجي الحديث وكونها كذلك تتميز عن الجرائم التقليدية بمفهومها وأدواتها ارتكابها وخصائصها وصورها والطبيعة الخاصة لمرتكب هذه الجريمة. كل هذا ساهم في ظهور عدة مسميات للجريمة الإلكترونية.

3- مسميات الجريمة الإلكترونية (حسنين شفيق، 2015، ص 17)

- جرائم الحاسوب والانترنت.
- جرائم التقنية العالية.
- الجريمة السيبرانية.
- جرائم المعلوماتية.

4- العلاقة بين الجريمة الإلكترونية والجريمة التقليدية

تشابه الجريمة الإلكترونية مع الجريمة التقليدية من جانب أركان الجريمة من مجرم لدافع لارتكاب الجريمة، والضحية والذي يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة. ففي الجريمة الإلكترونية تكون أداة الجريمة من مخرجات التقنية، وكذلك مكان الجريمة الذي لا يرهق الجاني في الوصول إليه، مما يسهل عملية الجريمة الإلكترونية في العديد من هذه الجرائم فإن الجريمة تتم عن بعد باستخدام الخطوط وشبكات الاتصال بين الجاني وموقع الجريمة. (موسى يعقوب، 2014، ص 201)

5- الاتجاهات النظرية المفسرة للجريمة الإلكترونية

حدد العلماء ثلاثة اتجاهات لتفسير الجريمة الإلكترونية وهي الاتجاه الفردي وينصب على عوامل تختص بالشخص نفسه وما يمتلكه من خصائص وسمات قد تكون ذات طابع ثابت لا يقبل التحوير أو التبديل، وقد تكون مكتسبة في بعض جوانبها تقسم إلى عدة اتجاهات، تتمثل في:

اتجاه فردي بيولوجي: ويحاول هذا اتجاه تفسير السلوك الإجرامي بإعادته إلى خصائص البيولوجية يمتلك الفرد المجرم.

اتجاه فردي نفسي: وفي هذا الاتجاه يفسر علماء السلوك في ضوء الخصائص النفسية أو الدوافع المحركة للسلوك الإنساني وهذه الحركات مرتبطة بعدة عوامل منها الدوافع الغريزية ومكونات الجهاز النفسي والتخلف العقلي الاتجاه الاجتماعي لتفسير الجريمة بصفة عامة. حيث يحاول علماء الإجرام بعوامل خارجة عن الفرد ومكوناته الذاتية غير بدونها بعوامل خارجية تحيط بالفرد وتعمل على تكوين السلوك الإجرامي ومن أمثله هذه العوامل الاقتصادية.

الاتجاه التكاملي: هو اتجاه يأخذ من جميع العوامل ويبحث في كل ما يتصل بحياة الفرد من النواحي العضوية والنفسية والاجتماعية، وينظر لها أنها متفاعلة معا في إبراز الجريمة وأن أي عامل من العوامل له أهميته الخاصة بهذا الشأن. (الزبود، 2010، ص ص 172-173)

6- التفسيرات السوسولوجية للجريمة الإلكترونية

يعزو التفسير الاجتماعي للجريمة الإلكترونية إلى الأسباب التي تكمن وراء السلوك الإجرامي إلى عوامل تتعلق بالمجتمع ككل وإلى الظروف البيئية الاجتماعية المباشرة التي يعيش في ظلها الفرد، ويتأثر بها بطريق مباشر أو غير مباشر، وقد اختلف العلماء في تحديد أهمية هذه العوامل في تأثيرها على سلوك الأفراد والجماعات.

1- النظرية اللامعيارية - الأنومي -

آراء دوركايم في سبب حدوث الجريمة الإلكترونية:

إن الجريمة ظاهرة اعتيادية في أي مجتمع يصعب القضاء عليها لأنها ظاهرة تتصل ببناء المجتمع وبطبيعة حياته الاجتماعية، لذا فهي جزء من وظائفه. الجريمة ظاهرة ينتجها المجتمع نفسه وذلك بانتقاده لبعض قواعد السلوك التي يرى أنها طرق شاذة وخارجة على عاداته وتقاليده ويعتبرها جريمة. وفي النهاية يعتبر من يسلك هذا السلوك مجرماً. وعندما يقوم أي مجتمع بالقضاء على ظاهرة الجريمة نهائياً فإن المعيار الذي يفصل بين العمل الممنوع والعمل

المشروع ينعدم، أي أن الضبط الاجتماعي ينعدم ، وهذا لا يحدث إلا في مجتمعات مثالية غير موجودة. إن الجريمة ظاهرة سليمة ومفيدة لسلامة المجتمع لارتباطها بمقومات الحياة الاجتماعية الأساسية، فهي كالألم يحس به الفرد لتنبيهه بوجود خلل.

إن حاجات ومتطلبات الفرد لا تقف عند حد معين، لذا يجب أن يحدد التنظيم الاجتماعي أهداف الفرد، وأن يحدد الطرق الاجتماعية التي تضمن للفرد تحقيق هدفه ومتطلباته. فاختلاف التنظيم الاجتماعي يؤدي إلى اضطرابات في تأدية عملية الضبط مما يؤدي في النهاية إلى تجاوز الأفراد حدود متطلباتهم وأهدافهم مما يعرض المجتمع إلى حالة فوضوية تدعى حالة "الأنومي" ويتبع الشخص شهواته ورغباته دون الاهتمام بالضوابط الاجتماعية ومن ثم يقوم بارتكاب أية جريمة. مثل ذلك الانتحار الذي يحدث إما نتيجة لأزمات اقتصادية شديدة أو بسبب الرخاء المفاجئ أو بسبب التقدم الصناعي وعدم استطاعة الفرد استيعاب هذا التطور خلافا لتصوره لقدرته على السيطرة.

(الحمشي، 2013، ص 46)

عموما يمكن تطبيق هذه النظرية على الجريمة الإلكترونية حيث يشير البعض إلى أن تزايد استخدام التكنولوجيا يؤدي إلى تشتت الانتباه وتفكك العلاقات الاجتماعية، وبالتالي يمكن أن يزيد من احتمالية حدوث الجريمة الإلكترونية.

على سبيل المثال، يمكن للأفراد الذين يشعرون بالعزلة والتبعية في الحياة الواقعية أن يلجؤوا إلى الإنترنت ووسائل التواصل الاجتماعي للبحث عن التفاعل الاجتماعي، ويمكن لهذا السلوك الدفع ببعضهم للاحتيال عبر الإنترنت وغيرها من أنواع الجرائم الإلكترونية. علاوة على ذلك، يمكن أن يؤدي التعرض المستمر للمحتوى الإلكتروني ذو الطبيعة العنيفة أو الإباحية إلى تقليل الحس الأخلاقي لدى الأفراد، مما يمكن أن يؤدي إلى زيادة احتمالية ارتكاب جرائم إلكترونية.

2- نظرية روبرت ميرتون:

هناك بعض الجرائم ترتبط بالمكانة الاجتماعية، فالسرقة مثلا عندما تصدر من أفراد الطبقة الدنيا المحرومة اقتصاديا يظهر دعاة القانون والمحافظون على السلم والأمن الاجتماعيين ويطالبون بإنزال أشد العقوبات عليهم حتى يكونوا عبرة لغيرهم، أما أبناء الطبقة العليا والوسطى فلا يعاقبون. أما فيما يتعلق بجرائم "ذوي الياقات البيضاء" الذين يرتكبون جرائم كالنصب والاحتيال والتزوير وغيرها... إلخ فإن النظرة تختلف وتخف نبرة المطالبة بإنزال أشد العقوبات عليهم، وقد يغض الطرف عن السرقة عموما، وفي أحسن الأحوال يفرض على السارق أخف العقوبات أو بفرض غرامة مالية للإفراج عنه، ومن جهة ثالثة تختلف أساليب وطرق وحجم السرقات عند الطبقتين (العليا والدنيا) فأبناء الطبقات المحرومة تكون سرقاتهم عادة لإشباع حاجاتهم الضرورية، وهي جرائم خفيفة وصغيرة، أما جرائم ذوي الياقات البيضاء هي جرائم واختلاسات كبيرة تضر بالمصلحة العامة، تسعى لتحقيق الثراء والغنى الفاحش. (أبو عليان، 2016، ص 53)

بالنسبة للجريمة الإلكترونية، يمكن تطبيق نظرية ميرتون على دراسة دوافع وسلوك المجرمين الإلكترونيين. فعلى سبيل المثال، يمكن أن تكون دوافع المجرمين الإلكترونيين هي الحصول على المال بسرعة وسهولة، أو الحصول على المعلومات السرية للمنافسين أو الأفراد الآخرين. وتركز النظرية على أن الجريمة تحدث بسبب عدم تحقيق الأهداف المرجوة بالطرق القانونية والاجتماعية المقبولة، وهذا ينطبق على الجرائم الإلكترونية حيث يتم ارتكابها بالطرق غير القانونية والغير مقبولة اجتماعيًا.

ويمكن أيضًا تطبيق نظرية ميرتون على تفسير الأثر الاجتماعي للجرائم الإلكترونية، حيث تؤثر هذه الجرائم على الفرد والمجتمع على المستويين الاقتصادي والنفسي. فعلى سبيل المثال، يمكن أن تؤدي الجرائم الإلكترونية إلى فقدان الثقة بين الأفراد والمؤسسات، وتأثير سلبي على الاقتصاد والأمن الوطني، مما يؤثر على المجتمع بشكل عام.

3- نظرية الاختلاط التفاضلي:

تعتبر هذه النظرية من أبرز الاتجاهات السوسيولوجية المفسرة للجريمة والانحراف حيث ترى هذه النظرية أن السلوك المنحرف إنما هو عبارة عن سلوك متعلم حيث يتطلب ارتكاب الجريمة من الجاني فهم وتعلم وسائل إجرامية معينة تكون بمثابة الدافع الرئيس لارتكابها، يتم تعلم هذه الوسائل عن طريق مجموعة من الاتصالات والعلاقات الشخصية داخل جماعات تتميز بالتقارب والألفة بين أفرادها والتأثر بتوجيههم نحو تصرف معين في مواقف معينة، فإذا كانت هذه المواقف مواقف سلبية نحو الجريمة فلن يقع الفرد في السلوك الإجرامي أما إذا كانت مواقف إيجابية نحوها أي تحبذ ارتكاب الجريمة فإنها تدفع الفرد إلى الانخراط في ممارسة السلوك المنحرف. ولذا فإن محور نظرية الاختلاط التفاضلي يدور حول أن الفارق الأساسي بين سلوكيات الأفراد يعتمد بالدرجة الأولى على نوعية الأفراد الذين يختلطون بهم وإن كل شخص ينطبع بالطابع الثقافي والاجتماعي المحيط به. (الخمشي، 2013، ص50)

عموماً فإن هذه النظرية تعد إحدى النظريات الاجتماعية التي تركز على دراسة كيفية تفاعل الأفراد المختلفين في المجتمع، وكيفية تأثير الاختلافات الاجتماعية والثقافية والاقتصادية في هذه العلاقات. ومنه فإنها تشير إلى أن الجرائم الإلكترونية يمكن أن تنشأ نتيجة للاختلاط بين أفراد مختلفين اجتماعيًا في المساحات الافتراضية على الإنترنت، وأن هذا الاختلاط يؤدي إلى تكوين ثقافات ومجتمعات افتراضية تختلف عن المجتمعات الحقيقية في العالم الواقع.

ومثلما فسرت النظرية الجريمة التقليدية فإنها تفسر الجريمة الإلكترونية أيضاً، وبما أن الجريمة سلوك مكتسب وليست سلوكاً موروثاً، فإن الجريمة الإلكترونية يتم تعلمها وتعلم آلياتها، فمثلاً عدم مراقبة الآباء للأبناء أثناء انشغالهم بتصفح مواقع الأنترنت من شأنه أن يزيد للمنظمات المتطرفة والهاكرز فرصة استدراج الأبناء، ثم إن عدم مراقبة الأبناء ومتابعة صفحاتهم والمجموعات المنضمين لها أيضاً يساعد الجماعات المتطرفة على سحب البعض منهم إلى دوائر الجريمة الإلكترونية والجريمة المنظمة أيضاً. فالاختلاط غير المراقب يؤدي إلى البعض إلى السقوط في عالم الجريمة دون قصد.

ومنه فإنه يمكن تطبيق نظرية الاختلاط التفاضلي على دراسة الجريمة الإلكترونية، حيث يتم ارتكاب هذه الجرائم عبر الإنترنت ويتفاعل الأفراد في العالم الافتراضي بطريقة مختلفة عن العالم الحقيقي. فعلى سبيل المثال، يمكن أن يكون لدى مجموعات معينة من الأفراد في العالم الافتراضي ثقافات وأنشطة وأهداف مختلفة، وقد يؤدي هذا الاختلاف إلى تفاعلات مختلفة فيما يتعلق بالجرائم الإلكترونية. على سبيل المثال، يمكن أن تؤدي الاختلافات الثقافية إلى تفاوت في التعامل مع المعلومات الحساسة على الإنترنت، مما يؤدي إلى زيادة أو نقصان الجرائم الإلكترونية في بعض المجتمعات.

4- نظرية التفكك الاجتماعي

يعتبر عالم الاجتماع الأمريكي "ثورستن سيلين" من رواد النظرية، إذ يعتبر التفكك الاجتماعي يساهم بشكل كبير في زيادة الجريمة في المجتمع. ويعتبر التكافل الاجتماعي أقوى حاجز للتحصن من الجريمة. (أبو عليان، 2016، ص 58) كما اعتبر أن التفكك الاجتماعي يحدث شيئاً فشيئاً في المجتمعات المدنية المتحضرة حيث تضعف الروابط الاجتماعية فيكون المجتمع المتحضر فيه تنافر وصراع فيحدث خلل في السلوكيات فتحدث الجريمة. بمعنى أنه عندما تتباعد الروابط وتطغى الأنانية والفردية وينتشر الطمع والجشع بين الأفراد فيتصرف فيها الأفراد بتصرفات مختلفة ومنها التصرفات المنحرفة حتى تقع الجريمة. (آمنة الكتبي، 2010، ص 56)

تنظر نظرية التفكك الاجتماعي إلى الجريمة الإلكترونية على أنها واحدة من العوامل التي تساهم في تفكك البنية الاجتماعية، ففي هذه النظرية يتم النظر إلى المجتمع كنظام متكامل من المؤسسات والقيم والتوجهات الثقافية، وتؤثر الجريمة الإلكترونية على هذا النظام بطرق عدة، فعلى سبيل المثال يمكن أن تؤدي الجريمة الإلكترونية إلى زيادة الشك والقلق بين الأفراد في المجتمع، والتي بدورها تساهم في إضعاف الثقة بين الأفراد وتقليل مستوى الاتصال الاجتماعي، وهذه العوامل بدورها تؤدي إلى تفكك البنية الاجتماعية وزيادة العزلة والانعزال بين الأفراد.

ومن الجانب الآخر يمكن أن تؤدي الجريمة الإلكترونية إلى تفكك المؤسسات والهياكل الاجتماعية، مثل الحكومات والشركات والمؤسسات المالية، فعلى سبيل المثال يمكن أن يتم اختراق أنظمة الحكومة أو الشركات وسرقة البيانات الحساسة، مما يؤدي إلى فساد المؤسسة وتفككها.

5- نظرية الضبط الاجتماعي

من أنصار هذه النظرية "هرتن وزلي" و "تراقز هيرزخ"، وهم ينظرون للجريمة والإجرام بصفة عامة على أنه نتاج حالة التحرر النسبي من الارتباط بالقيم والمعتقدات الأخلاقية التي تحكم السلوك والعلاقات أثناء التفاعل الاجتماعي بالمجتمع، حيث تؤكد هذه النظرية على أن ضعف رابطة الفرد بالمجتمع أو تصدع علاقات الأفراد بالمجتمع تنتج الأفعال الإجرامية. (آمنة الكتبي، 2010، ص 63)

ومن أهم فرضيات هذه النظرية أن الجريمة ناجمة عن فشل الضوابط الشخصية الداخلية والاجتماعية الخارجية في إيجاد الاتساق بين السلوك و بين المعايير الاجتماعية ويعني الضبط الشخصي الداخلي ، قدرة الفرد

على الامتناع من أن يقابل حاجاته بطرق يخالف بها المعايير في جماعته ، كما يعني الضبط الاجتماعي الخارجي ، قدرة الجماعة أو النظم الاجتماعية على أن تجعل لمعاييرها الاجتماعية الأثر الفعال على أعضائها.

(الخمشي، 2013، ص57)

تنص نظرية الضبط الاجتماعي على أن السلوك الإنساني يتم ضبطه بواسطة مجموعة من العوامل الاجتماعية والثقافية، مثل القيم والمعايير الاجتماعية والمؤسسات الاجتماعية. وتشير النظرية إلى أن هذه العوامل تؤثر على سلوك الأفراد وتساهم في تقليل السلوكيات السلبية، بما في ذلك الجريمة.

يمكن تطبيق نظرية الضبط الاجتماعي على دراسة الجريمة الإلكترونية، حيث يمكن للعوامل الاجتماعية والثقافية المؤثرة على الضبط الاجتماعي أن تلعب دورًا في تقليل الجرائم الإلكترونية. فعلى سبيل المثال، قد تؤدي القيم والمعايير الاجتماعية التي تحترم خصوصية الآخرين وتحث على الاحترام المتبادل على تقليل الجرائم الإلكترونية التي تنتهك خصوصية الآخرين، مثل القرصنة الإلكترونية. وبما أن بعض الجرائم الإلكترونية تعتمد على النصب والاحتيال، ويمكن للضبط الاجتماعي أن يقلل من حدوث هذه الجرائم عن طريق توعية الناس بأساليب النصب والاحتيال وكيفية تفاديها، كما يمكن للضبط الاجتماعي تعزيز الوعي بأهمية تحمي أنظمة الكمبيوتر والبرمجيات الأمنية لتقليل فرصة التعرض للهجمات الإلكترونية.

6- نظرية الوصم الاجتماعي - الإلصاق-

ترى نظرية الوصم الاجتماعي أن الجريمة أو السلوك الانحرافي ناتج عن نجاح مجموعة من الأفراد بالإشارة إلى أفراد آخرين أنهم مجرمين أو منحرفين، على سبيل المثال إذا ألصقت المجتمعات الغربية فكرة التخلف بدول العالم الثالث وكرروها في إعلامهم وخطابهم السياسي، تصبح جميع الدول العالم الثالث متخلفة في نظر الغربيين، وإن كان الواقع يخالف ذلك. (أبو عليان، 2016، ص 64)

ويرى تانينبوم أن ما يؤدي إلى خلق المجرم إنما هو الكيفية التي يعامله بها الآخرون حيث ذكر أن عملية صنع المجرم تتصف بأنها عملية تحوي عناصر تشمل وضع علامات وألقاب وتعريفات تقوم الجماعة بالإصاقها بالشخص، والهدف من عملية الوصم هذه خدمة الجماعة وتحقيق بعض أهدافها فعن طريقها تتم بلورة نقمة الجماعة ضد الشخص المخالف ، ونقمة المخالف على نفسه عن طريق هز معنوياته وتشويه قيمه وأخلاقه.

(الخمشي، 2013، ص53)

تنظر نظرية الوصم الاجتماعي إلى الجريمة الإلكترونية على أنها ظاهرة ترتبط بشكل وثيق بعمليات التسميم والوصم الاجتماعي، حيث يتم تسميم وصقل سمعة الأفراد الذين يرتكبون الجرائم الإلكترونية، وتصبح العقوبة التي تلحق بهم أكثر صرامة وقسوة من غيرهم، ويتم عزلهم عن المجتمع. وتشير النظرية إلى أن الجرائم الإلكترونية قد تؤدي إلى تسليط الضوء على فئات معينة من المجتمع تم وصمها سلفًا، مما يؤدي إلى تفاقم الوصم الاجتماعي لهم. ويعتبر الانحراف الإلكتروني أحد أشكال الانحراف الاجتماعي والذي يؤدي إلى تمييز الفئات المجتمعية وتمثيلها على أنها مجموعة معينة تستحق الوصم والتمييز.

وعند تطبيق نظرية الوصم الاجتماعي على الجريمة الإلكترونية، يمكن أن تكون لها آثار سلبية على المجتمع بأكمله، حيث يتم إقصاء المتورطين في الجرائم الإلكترونية من المجتمع، وقد يؤدي ذلك إلى تحويلهم إلى مجموعات معادية للمجتمع. ولذلك، يعتبر العمل على منع الجريمة الإلكترونية ومكافحتها وتقليل انتشارها، أمراً ضرورياً من أجل الحفاظ على استقرار المجتمع وتحقيق العدالة الاجتماعية.

7- نظرية التقليد والمحاكاة:

تنطلق نظرية التقليد من فرض: أن الفرد مقلد لسلوك من يتفاعل معهم، وعليه فإن السلوك الإجرامي سلوك مكتسب مثل أنماط السلوك الأخرى، إلا أنه غير سوي. وتنتظر للفرد المحرم أنه مثل أي فرد في المجتمع من حيث السمات الشخصية والجسمية والعرقية، وما إجرامه إلا نتيجة تفاعله مع أفراد مجرمين. (أبو عليان، 2016، ص 66) يعد "غابريال تارد" منشئ نظرية المحاكاة حيث يعزو السلوك الخارج عن القانون إلى عامل نفسي اجتماعي رئيسي وهو المحاكاة والتي يقصد بها تكرار نموذج سلوكي. حيث يعتبر أن الفرد لا يولد مجرماً ولا يعتبر مجرماً بالفطرة وإنما يتم ذلك من خلال البيئة الاجتماعية التي يعيش فيها ومن خلال التنشئة الاجتماعية ومعتقداته الثقافية وبمحاكاة الآخرين. (آمنة الكتبي، 2010، ص 68)

ومنه، فإن نظرية التقليد والمحاكاة تنص على أن الأفراد يتعلمون من خلال مشاهدة وتقليد سلوكيات الآخرين، سواء كانت إيجابية أو سلبية. وبالتالي، فإن الأفراد يتعلمون سلوكياتهم من النماذج الأخرى التي يرونها، وينقلون هذه السلوكيات إلى سلوكياتهم الخاصة.

يمكن تطبيق نظرية التقليد والمحاكاة على الدراسة والتحليل للجرائم الإلكترونية، حيث يمكن للأفراد تعلم السلوكيات الإلكترونية السلبية من المجرمين الإلكترونيين الذين يرتكبون الجرائم الإلكترونية، ويقومون بمحاكاة هذه السلوكيات فيما بعد. ويمكن أن تتضمن هذه السلوكيات الجرائم الإلكترونية مثل الاحتيال الإلكتروني، والقرصنة الإلكترونية، والتهديد عبر الإنترنت، والتنمر الإلكتروني، وغيرها. وبما أن الجريمة الإلكترونية يمكن أن تتم من خلال الإنترنت، فإن الأفراد قد يشاهدون ويتعلمون السلوكيات السلبية من الجرائم الإلكترونية على الإنترنت، سواء كانت على شبكات التواصل الاجتماعي أو من خلال المنتديات الإلكترونية أو الألعاب الإلكترونية، ويمكن لهذه الأفراد تحاكي هذه السلوكيات فيما بعد. (موسى يعقوب، 2014، ص 201)

المحور الثاني: الجريمة الإلكترونية - الأهداف والخصائص والأنواع-

1- أهداف الجريمة الإلكترونية

1. الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق الهدف الإجرام.
2. الوصول إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو تخريبها وعادة ما تتم هذه العملية على مواقع الإنترنت.
3. الحصول على المعلومات تغيير عناوين مواقع من الإنترنت بهدف التخريب على المؤسسات العامة وابتزازها.

4. الوصول إلى الأشخاص أو الجهات المستخدمة للتكنولوجيا بغرض التهديد أو الابتزاز كالبانوك والدوائر الحكومية والأجهزة الرسمية والشركات بكافة أشكالها.
5. الاستفادة من التقنية المعلومات من أجل كسب المادي أو معنوي أو سياسي غير مشروع كعمليات تزوير بطاقات الائتمان وعمليات اختراق مواقع الكترونية على الشبكة العنكبوتية.
6. استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة أو نشر الأفكار التي يمكن أن تؤسس إلى فكر تكفيري. (موسى يعقوب، 2014، ص ص 213-214)

2- سمات الجريمة الإلكترونية

تتمحور خصائص الجريمة الإلكترونية في المحاور التالية: (الهاشمي، 2019، ص 50)

- الدافع للارتكاب.
- موضوعها من مراحل تشغيل نظام معالجة البيانات.
- التواطؤ والتعاون على الإضرار.
- دور المخالطة الفارقة.
- إغراض النخبة.
- صعوبة الاكتشاف.

3- أسباب الجرائم الإلكترونية

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية ، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي ، كما أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي، كوني) فجرائم الشباب والهواة والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة معلومات أو تجارة بالمعلومات أو شخصية الخ...

أسباب الجريمة على المستوى الفردي:

- البحث عن التقدير: هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار السن، وذلك من باب التحدي وحب الظهور في الإعلام. وغالبا ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.
- الفرصة: أن تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للإنترنت قد خلق فرص جديدة للمجرمين وسهلت نمو الجريمة، وأن جرائم الإنترنت تمثل شكلا جديدا ومميزا للجريمة وقد خلقت تحديات لتوقع التطورات والوقاية منها. (إسراء جبريل، 2018، ص 432)
- ضبط الذات المنخفض: احتمالية انخراط الأفراد في فعل إجرامي يحدث بسبب وجود الفرصة مع توفير سمة شخصية من سمات الضبط الذاتي المنخفض. إن توفير صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب

السلوك الطائش يعدان عاملان مؤثرين في ارتكاب السلوك الطائش، فتأثير هذين العاملين يكون نتيجة لاتحادهما، والتفاعل بينهما هو المؤدي للسلوك الطائش.

- **الضغوط العامة:** ترجع نظرية الضغوط العامة للانحراف وخرق القانون إلى دافع ناجم عن قوى البناء الاجتماعي أو استجاباته النفس اجتماعية للحوادث والظروف والتي تعمل كضغوطات أو مقلقات خاصة عندما لا تتاح للأفراد الفرصة لتحقيق أهدافهم المقبولة اجتماعيا وأن مصادر الضغوط لا تتوقف على الإحباط الذي يخبره الفرد عندما تسد الطرق لتحقيق هدف ما، وإنما يشمل المشاعر السلبية التي تحدث في المواقف الاجتماعية المتنوعة كما قد تلعب العوامل الاجتماعية والاقتصادية أيضا دورا هاما في زيادة الجريمة الالكترونية.

- (البداينة، 2014، ص ص 11-12)

- **النشاط الروتيني:** ويمكن تفسير زيادة ضحايا الجريمة الالكترونية من خلال التغيرات في أنشطة الناس الروتينية في الحياة اليومية. فمع ظهور شبكة الانترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية، والترفيه والتجارة... الخ. إن التغيرات في أنشطة الناس الروتينية مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيسبوك، والإيميل والمواقع وغيرها قد خلقت فرصا للجنة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة. (صفاء محمد، 2018، ص ص 60-61)

أسباب الجريمة على المستوى المجتمعي

- **التحضر:** يعد أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة. وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهظة التكاليف، والتي تتطلب مهارات عالية أحيانا. مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية وكنيجة يجد الناس أنفسهم في تنافس غير قادرين على مجاراته، مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب رأسمال كبير. (إسراء جبريل، 2018، ص 435)

- **البطالة:** ترتبط الجريمة الالكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة. وتتركز البطالة بين قطاعات كبيرة من الشباب. لذا فإن الشباب الذين يملكون المعرفة والمهارة يستثمرون ذلك في النشاط الإجرامي الإلكتروني.

- **الضغوط العامة:** تعد هذه الضغوط التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف: كالاتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية وغيرها. (البداينة، 2014، ص ص 14-15)

- **البحث عن الثراء:** يسعى الفرد إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لـ "جيفرودسون" و"هيرشي" ويسعى الناس إلى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية

الأنومي لميرتون. فالرغبة في الشراء يواجهها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعيا وقانونيا، ولذا يلجأ بعض الناس إلى الجرائم الإلكترونية حيث المستهدف أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة. (صفاء محمد، 2018، ص 61)

ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية: هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها كي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها. وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء، كيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحال على المستوى الدولي. فمما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية. وغالبا ما تجد في دول كثيرة تواضع التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة هذه الجريمة داخل المجتمع والعبارة منها للحدود. (إسراء جبريل، 2018، ص 436)

أسباب الجريمة على المستوى الكوني:

- **التحول للمجتمع الرقمي:** لقد دخلنا عصر المعلوماتية الجديدة (أي الفضاء الإلكتروني أو العالم الافتراضي). فالناس يقضون جزءا من حياتهم اليومية في الفضاء الإلكتروني، ينشؤون الشبكات والمواقع ويتمتعون بأنواع جديدة من العلاقات الاجتماعية ، وهم على تواصل مع ما يجري في العالم الخارجي، والقيام ببعض الأعمال . كل هذه الأنشطة قد جعلت من الممكن للجميع وبوجود جهاز كمبيوتر أو مودوم مع معرفة التقنية القليلة. وبعبارة أخرى، فإن شبكة الإنترنت هي من خلقت ما يعرف الآن باسم الفضاء الإلكتروني أو العالم الافتراضي. يحتاج المجتمع لكي يقوم بوظائفه إلى أن يعم الأمن والأمان وان يتحقق النظام والاستمرارية ولا يتوقف توفر الأمن والأمان في الواقع المادي للمجتمع بل أنتقل ليشمل العالم الافتراضي. (البداية، 2014، ص 15)

- **العولمة:** أن ظهور (الفضاء الإلكتروني) يخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر أنفسها، والفرص المباشرة للجريمة والتي وفرتها أجهزة الكمبيوتر الآن. ضمن الفضاء الإلكتروني قد يظهر الأشخاص الفروق في امتثالهم الخاص (القانوني) وعدم الامتثال (غير القانوني) مقارنة مع السلوك سلوكهم في العالم المادي. فالأفراد، على سبيل المثال، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم. بالإضافة إلى ذلك فمرونة الهوية، وعدم ظهور الهوية وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي (صفاء محمد، 2018، ص ص 62-63)

- **انكشاف البنية التحتية المعلوماتية الكونية:** تتفاوت البنى التحتية المعلوماتية بدرجة انكشاف إلى الكوارث الطبيعية ، والإهمال البشري، وسوء التصرف الإنساني. حدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة خمس قطاعات بناء على الخصائص المشتركة لها، وهذه القطاعات هي:

✓ قطاع الاتصالات والمعلومات، وتشمل شبكات الاتصالات العامة والإنترنت والحاسبات في المنازل والاستخدام الأكاديمي والحكومي والتجاري.

- ✓ قطاع التوزيع المادي (الفيزيقي) ويشمل الطرق السريعة للمواصلات وخطوط السكك الحديدية والموانئ وخطوط المياه، والمطارات، وشركات النقل، وخدمات الشحن التي تسهل انتقال الأفراد والبضائع.
- ✓ قطاع الطاقة وتشمل الصناعات التي تنتج الطاقة وتوزع الطاقة الكهربائية والبتول والغاز الطبيعي.
- ✓ قطاع المال والبنوك وتشمل البنوك، وشركات الخدمات المالية من غير البنوك ونظم الرواتب ونظم الرواتب وشركات الاستثمار والقروض المتبادلة والتبادلات الأمنية والمادية.
- ✓ قطاع الخدمات الإنسانية الحيوية وتشمل نظم التزويد بالمياه، وخدمات الطوارئ والخدمات الحكومية (البطالة والضمان الاجتماعي وتعويض الإعاقات وإدارة سجلات المواليد... الخ

(إسراء جبريل، 2018، ص ص 438-439)

4-أنواع الجرائم الإلكترونية

أقرت وزارة العدل الأمريكية سنة 2009 إحدى عشرة نوع من الجرائم الإلكترونية وهي كما يلي: (الهاشمي،

2019، ص52)

- السطو على بيانات الكمبيوتر.
- الاحتيال عبر الانترنت.
- الاتجار بكلمة السر.
- عمليات الهاكرز القرصنة.
- سرقة أسرار التجارية باستخدام الكمبيوتر.
- تزوير العملة باستخدام الكمبيوتر.
- الاتجار بالمتفجرات والأسلحة النارية أو المخدرات وغسل الأموال عبر شبكة الانترنت.
- الصور الجنسية باستغلال الأطفال.
- الإزعاج عن طريق شبكة الانترنت.
- تهديدات القنابل بواسطة الانترنت.
- تزوير الماركات التجارية.

وهناك من صنفها إلى الأنواع التالية: (لينا جمال، 2016، ص102)

أولا: جرائم الاعتداء على الحياة الخاصة للأفراد

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة. (لينا جمال، 2016، ص 102) أما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الآونة الأخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية. (عبد الصبور، ومنال عبد اللاه، 2012،

ص 130)

ثانيا جرائم الاعتداء على الأموال

إذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن أن يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرع شكل السلوك

الإجرامي لها، يمكن أن يتم بأي فعل يؤدي إلى حرمان المجني عليه من المال المنقول وإدخاله في حيازة الجاني، كذلك الحال بالنسب لجريمة النصب حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية، فهل ينطبق ذلك على جرائم السرقة و الاحتيال التي ترتكب عن طريق التقنية المعلوماتية ؟

(لينا جمال، 2016، ص 105)

وتشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة، المخدرات، غسيل الأموال، ولعل جرائم هذا القسم أوضح من ناحية معرفة كونها مجرمة حيث لا تختلف في نتيجتها عن الجرائم التقليدية. (عبد الصبور، ومنال عبد اللاه، 2012، ص 134)

ثالثا: جرائم الإضرار بالبيانات

يعتبر هذا الفرع من الجرائم الالكترونية من أشدها خطورة و تأثيرا وأكثرها حدوثا وتحقيقا للخسائر للأفراد والمؤسسات. ويشمل كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة الكترونية على الحواسيب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها. (موسى يعقوب، 2014، ص 218)

أبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها. ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون ذوى القبعات البيضاء **White Hat Hackers** الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الانترنت مستغلين بعض الثغرات في تلك النظم مخترقين بذلك كل سياسات وإجراءات أمن المعلومات التي يقوم بها مديري تلك الأنظمة والشبكات (System And Network Administrators). (لينا جمال، 2016، ص 110)

رابعا: جرائم الاعتداء على الأفراد

المقصود بالاعتداء هنا هو السب والقذف والتشهير وبث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بالشخص أو الجهة المقصودة. (لينا جمال، 2016، ص 111)

تنقسم هذه الجرائم التي تستهدف الاعتداء على الأفراد وحياتهم الخاصة، إلى عدة أقسام منها:

- **جرائم القذف والسب والتشهير الإلكتروني:** تبرز هنا من منطلق ابتزازي، حيث يتم التقاط صور للفرد في أوضاع غير مقبولة اجتماعيا، ويتم بعد ذلك بثها على شبكة الانترنت، بعدة طرق أسهلها عن طريق موقع اليوتيوب. ومن ثم تكون الصورة متاحة لكل مرتادي هذا الموقع. (موسى يعقوب، 2014، ص 222)
- **جرائم الاعتداء على حرمة الحياة الخاصة:** هذا النوع من الجرائم تم التطرق له سابقا، وهو أيضا يعد نوعا من الجرائم التي تدخل في إطار الجرائم الممارسة على الأفراد. حيث باتت حياة الكثيرين أسيرة لهواجس انتهاك خصوصياتهم، وهنا المقصود بهذا النوع كل الأفعال التي تدخل ضمن إطار الاطلاع على أفعال الآخرين دون علمهم أو إذن منهم ولو لم تكن أسراراً. (الزنداني، 2018، ص 96)

• **جرائم الابتزاز والتهديد:** بظهور العالم الافتراضي والشبكة العالمية زادت وتيرة السلوك الإجرامي الإلكتروني وتعتبر من أهم الأسباب استخدام التكنولوجيا الحديثة أدوات لتنفيذ الفعل غير المشروع التي سرعت تحقيق النتيجة الإجرامية بخلاف الجرائم التقليدية التي تحتاج لشروط وظروف معينة لتكتمل عناصر الجريمة. يضاف إلى ذلك الخداع والتضليل الذي يمارسه هؤلاء المجرمين المحترفين مستغلين الطبيعة الخاصة في تقنية المعلومات. ومن أمثلة هذه الجرائم التهديد والابتزاز وانتحال الشخصية عبر الشبكة المعلوماتية. (الزندان، 2018، ص 100)

خامسا: جرائم تطوير ونشر الفيروسات

كانت البداية لتطوير فيروسات الحاسب في منتصف الثمانينات من القرن الماضي في باكستان على أيدي اثنين من الإخوة العاملين في مجال الحواسيب الآلية. استمرت الفيروسات في التطور و الانتشار حتى بات يظهر ما يقارب المئتين فيروس جديد شهريا. والتي تعددت خصائصها وأضرارها فالبعض ينشط في تاريخ معين والبعض الآخر يأتي ملتصقا بملفات عادية وعند تشغيلها فإن الفيروس ينشط ويبدأ في العمل الذي يختلف من فيروس لآخر بين أن يقوم بإتلاف الملفات الموجودة على القرص الصلب أو إتلاف القرص الصلب ذاته أو إرسال الملفات الهامة بالبريد الإلكتروني ونشرها عبر شبكة الانترنت. (لينا جمال، 2016، ص 112) يحاول المجرمون الاستفادة من كل إفرازات التقدم التكنولوجي، لذلك من الطبيعي أن تظهر صورا جديدة من الجرائم لم تكن معروفة من قبل، وهذا ليس بسبب التقدم التكنولوجي فحسب، بل لأن المجرمون والجريمة في تغير مستمر، فمجرم الأمس ليس كمجرم اليوم، وبالتالي فجريمة الأمس ليست كجريمة اليوم. (أبو عليان، 2016، ص 169)

5- تصنيف الجرائم الإلكترونية

جدول يمثل تصنيف الجرائم الإلكترونية

م	جرائم عامة	جرائم مادية	جرائم اقتصادية	جرائم ضد الأفراد
1	أخطاء الأداء المتعمد	السرقه	النصب الاحتيال	القذف والتشهير
2	إغفال الواجب	التدمير والإتلاف	الاختلاس	تسهيل الدعارة
3	التجاهل	تزييف المستندات	الرشوة	انتهاك الخصوصية
4	التهور والطيش	السطو الليلي	الابتزاز	الإهانة
5	التآمر والنواطؤ	التهريب	التهديد	التحرش الجنسي
6	-	انتحال شخصية	انتهاك الأسرار الاقتصادية	الخطف
7	-	قرصنة البرامج	التزييف والتزوير	القتل
8	-	التجسس العسكري	-	الانتحار
9	-	التجسس الصناعي	-	-
10	-	التجسس الاقتصادي	-	-

المصدر: (نصار، 2017، ص 13)

6- فئات الجناة في الجرائم الإلكترونية:

• **المستخدمون للكمبيوتر في منازلهم:** نظرا لسهولة اتصالهم بأجهزة الكمبيوتر دون التقيد بوقت أو نظام محدد يقيد استخدامهم للكمبيوتر.

- الموظفون الساخطون على منظماتهم التي يعملون بها: يعودون إلى مقر عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو سرقة.
- المتسللون: منهم الهواة أو العابثون بقصد التسلية، والمحترفين اللذين يتسللون إلى أجهزة مختارة ويعبثون أو يتلفون أو يسرقون محتوياتها، وتقع أغلب جرائم الأنترنت تحت هذه الفئة.
- العاملون في الجريمة المنظمة: مثل عصابات سرقة السيارات حيث يحددون بواسطة الأنترنت أسعار قطع الغيار ومن ثم يبيعونها في دول أو مناطق أخرى بسعر أعلى. (أبو عليان، 2016، ص 175)

7- خصائص الجناة في الجرائم الإلكترونية:

- أ. يتمتع الجاني في الجرائم الإلكترونية بالذكاء: يعتبر الذكاء من أهم صفات مرتكبي الجرائم الإلكترونية؛ لأن ذلك يتطلب منهم المعرفة التقنية الكافية والاحترافية لكيفية الدخول إلى أنظمة الحاسب الآلي، والقدرة على التعديل والتغيير في البرامج بطريقة تمكنهم من ارتكاب جرائم السرقة والنصب وغيرها من الجرائم بطريقة أسهل وأكثر أماناً.
- ب. الجاني في الجرائم الإلكترونية كإنسان اجتماعي: هو إنسان متوافق مع المجتمع حيث أنه إنسان شديد الذكاء يساعده على عملية التكيف مع هذا المجتمع، ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيلها. (علي عبد الصبور، 2012، ص 52)

ت. المعرفة والمهارة والخبرة: في كثير من الأحيان تجد المجرم الإلكتروني يمتلك قدراً كبيراً من المعرفة والمهارة في استخدام التقنية المعلوماتية، ويعود ذلك لامتلاكه الخبرة في البرمجة ومعالجة الشبكات والقدرة على اتخاذ الإجراءات التقنية المناسبة لتخطي الحواجز الموضوعية لحماية الشبكات، كما يقوم بتنمية تلك القدرة الفنية بالممارسة الطويلة في فهم لغات البرمجة وأنظمة التشغيل، أما الخبرة فيكتسبها من خلال الدراسة أو التكوين في هذا المجال، أو من خلال الاحتكاك بالآخرين، وما أصبحت توفره مختلف البرامج المتواجدة على الوسائط الإلكترونية الكثيرة أو حتى عبر شبكة الأنترنت مباشرة.

ث. المجرم الإلكتروني مجرم عائد للإجرام: يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم للمحاكمة في المرة السابقة، ويؤدي ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم للمحاكمة. (شنتير، 2021، ص 33)

8- خصائص الجريمة الإلكترونية: (حباية، 2022، ص 41-48)

تتميز الجريمة الإلكترونية عن الجرائم التقليدية بمجموعة من الخصائص أبرزها:

- **عابرة للدول والقارات:** هي شكل من أشكال الجرائم العابرة للحدود حيث إن الجريمة لم تعد ترتكب محليا بل أصبحت إمكانية ارتكابها دوليا وأصبح الجاني يقوم بالجريمة عن طريق الدخول إلى ذاكرة الحاسوب الموجود في بلد آخر وفقا للمجتمع الإلكتروني لا يوجد هنالك اعتراف بالحدود الجغرافية للدول.

- **سهولة الارتكاب:** لا تتطلب الجريمة الإلكترونية عنفا أو مجهودا كبيرا في ارتكابها، حيث إنها تتطلب نوعا من الدراية الذهنية والتفكير المدروس القائم على معرفة بتقنية الحاسب الآلي وشبكة الإنترنت على عكس الجريمة التقليدية التي تحتاج إلى مجهود عضلي قد يكون في صورة ممارسة العنف الإيذاء كما هو الحال في جريمة القتل أو الاختطاف.

- **ترتكب من خلال الوسائل التقنية:** نظرا للطبيعة الخاصة لهذه الجريمة فإنها ترتكب في بيئة إلكترونية يستلزم التعامل معها استعمال الجاني لوسائل وأجهزة التقنية كالحاسب الآلي وكما أنها ترتكب عبر شبكة الإنترنت التي تعتبر أساسية لارتكاب الجريمة. (حبابية، 2022، ص 41-43)

- **جريمة يصعب اكتشافها:** فهي لا تترك أثرا لمتابعتها وملاحظتها بل وقد يستخدم الجاني برامج تقنية من خلالها تعرق الوصول إليه أو معرفة التقنية للجريمة المرتكبة أيا كان نوعها كما أن المجني عليه لا يكشفها مباشرة ولا يشعر بها أما لضعف قدرته الفنية على ذلك بالمقارنة بالمرتكب الجريمة أو للمهارات الفنان التي استخدمها الجاني عند ارتكابه للجريمة.

- **جريمة يصعب إثباتها:** تقع في بيئة إلكترونية والأدلة التي تخلفها تكون أدلة إلكترونية حيث يستطيع المجرم الإلكتروني التخلص من الآثار المادية لجريمته بفعل التقنيات المعلوماتية وإخفاء الدليل الرقمي الإلكتروني، حيث يستخدم المجرم تقنية لارتكاب الجريمة ويستخدم تقنية أخرى لإخفاء العمليات التقنية التي تم استخدامها لارتكاب الجريمة، وهذا يجعل التحري عن الدليل الرقمي الإلكتروني للجريمة من قبل المختبر الجنائي الإلكتروني والخبراء المختصين صعبا للغاية.

- **عدم وجود تعريف موحد للجريمة الإلكترونية على الصعيد الدولي:** من خلال البحث فإنه لا يوجد تعريف موحد للجريمة الإلكترونية وأنه يوجد عدة تسميات: جريمة الحاسب الآلي، الجريمة المعلوماتية، الجريمة الإلكترونية، جرائم الإنترنت، وتعود هذه التسميات إلى المعايير والأسس التي استند عليها الفقهاء والخبراء القانونيون مما جعل قراصنة التكنولوجيا المعلومات يستغلون هذا الاختلاف واعتباره أرضية خصبة للاستمرار بارتكاب الجريمة الإلكترونية واعتدائهم غير المشروع. (حبابية، 2022، ص 45-46)

- **جريمة تسبق الخبرة التقنية لدى الجهات القضائية والخبراء الأمنيين لدى الأجهزة الأمنية في الدولة:** تتميز بأنها تسبق الخبرة لدى الجهات المختصة بملاحقتها ومتابعتها ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلب أسلوبا خاصا في التحقيق والتعامل الأمر الذي لم يتحقق في جهات الأمن والقضائية، حيث إن هناك فروقات معرفية بين مرتكب الجريمة الفاعل وبين الخبراء الجنائيين والسلطة القضائية بفرعها القضاء النيابة.

- **جريمة قليلة المخاطر:** تتميز بأنها قليلة المخاطر نظرا لعدم وجود مواجهة مباشرة مع المجني عليه أو غيره ولا خطر لمواجهة الشرطة كما في الجرائم التقليدية.

- **جريمة مكلفة للضحايا:** تشير الدراسات إلى أن الأضرار التي تسببها هذه الجريمة بالغه للمجني عليه وتنفوق التي تنتج عن الجرائم التقليدية. (حبابية، 2022، ص 47-48)

المحور الثالث: الآثار الاجتماعية للجريمة الإلكترونية:

ما يمكن إدراكه أن الجريمة الإلكترونية عموما لها تأثيراتها على الأفراد والأسرة والمجتمع أيضا خاصة في مجال القيم والعادات والسلوك. فقد أضحت الجريمة الإلكترونية في يومنا هذا قوة لها أبعادها الاجتماعية بمقدار ما لها من قوة سياسية واقتصادية.

أصبحت الجريمة الإلكترونية واقعا له تداعياته السلبية على الاقتصاد العالمي وتسبب خسائر ضخمة للمجتمعات وعلاقة طردية ما بين التقدم العلمي في مجال الحاسب والنمو المتزايد في معدل الجريمة الإلكترونية فهذا النوع من الجرائم الحديثة والمستحدثة تتنوع وتتضاعف يوما بعد يوم. (حسين شفيق، 2015، ص 16)

ومن الآثار التي تترتب عن سلوك جرائم الأنترنت والحاسوب بصفة عامة، هناك بعض الآثار الوخيمة على الجانب الاجتماعي والنفسي والصحي على ضحايا هذه الجرائم، ومن أهمها: (عبد الرحمن البقلي، 2010، ص

ص 71-72)

- ✓ اختلال نظام الأسرة وانتهاكها نفسيا.
 - ✓ اختلال نظام العلاقات الاجتماعية وانحياز المجتمع تدريجيا.
 - ✓ الإحباط والاكتئاب النفسي.
 - ✓ اضطراب النوم والقلق والتوتر الدائم.
 - ✓ العزلة الاجتماعية ورفض الاختلاط بالآخرين.
 - ✓ الانحراف الجنسي للشباب والشابات واللجوء إلى الجنس المسلي.
 - ✓ ازدياد معدل الجريمة الجنسية بالإحجام عن الإبلاغ خشية افتضاح الأمر.
 - ✓ إصابة الأطفال بالمرض السيكوباتي.
 - ✓ اختلاف نظرة المجتمع إلى المجني عليها وشكوكه في سلوكها وإحجام الشباب عن الزواج منها.
 - ✓ انتشار جرائم القتل والإيذاء للأخذ بالتأثر من الجاني.
 - ✓ تفشي ظاهرة ارتياد المواقع الجنسية.
 - ✓ تدمير الأخلاق ونشر الرذائل.
 - ✓ انخيار الحياة الأسرية.
 - ✓ التجسس على الأسرار الشخصية باختراق البريد الشخصي.
- عموما، تؤثر الجريمة الإلكترونية بشكل كبير على المستوى الفردي والمجتمعي، ومن الآثار الناجمة عنها:

على المستوى الفردي:

- 1- **الأثر النفسي:** قد يشعر الضحايا بالانتهاك الخصوصية وفقدان السيطرة على بياناتهم الشخصية، وقد يؤدي ذلك إلى الشعور بالخوف والاضطراب النفسي.
- 2- **الأثر المادي:** يمكن أن تتسبب الجرائم الإلكترونية في خسائر مالية كبيرة للأفراد والشركات والحكومات، ويمكن أن تؤدي إلى تدهور الاقتصاد وزيادة البطالة.
- 3- **الأثر الاجتماعي:** قد يؤدي الانتشار الواسع للجرائم الإلكترونية إلى انخفاض مستوى الثقة في التكنولوجيا والإنترنت، وقد يؤدي إلى زيادة التحفظ والحذر في استخدام الإنترنت ووسائل التواصل الاجتماعي.

على المستوى المجتمعي:

- 1- **التهديد للأمن القومي:** يمكن أن تستخدم الجرائم الإلكترونية كأداة للتجسس والهجوم على المؤسسات الحيوية مثل البنوك والشركات والمؤسسات الحكومية، ويمكن أن تؤدي إلى تعطيل الخدمات الحيوية وزيادة التوتر بين الدول.
- 2- **الأثر الاقتصادي:** يمكن أن تؤدي الجرائم الإلكترونية إلى خسائر مالية كبيرة على المستوى الاقتصادي وتؤثر على الاستثمارات والتجارة الدولية.
- 3- **الأثر الثقافي:** قد يؤدي الانتشار الواسع للجرائم الإلكترونية إلى زيادة التحفظ والحذر في استخدام التكنولوجيا والإنترنت.

- خاتمة

بعد دراسة الجريمة الإلكترونية من منظور سوسيوتاريخي، يمكن القول إنها تمثل ظاهرة حديثة تدرج ضمن ثورة الاتصالات والتكنولوجيا التي شهدتها العالم في العقود الأخيرة. ومن خلال هذه الثورة، ازدادت قوة وتعقيد الأنظمة الإلكترونية، مما جعلها أكثر عرضة للاختراق والاستغلال. بشكل عام، فإن دراسة الجريمة الإلكترونية من منظور سوسيولوجي يمكن أن تساعد في تحديد العوامل التي تؤدي إلى حدوثها وتحديد السياسات العامة الفعالة لمواجهتها. كما يمكن أن تساعد في فهم كيفية التأثير على الأفراد والمجتمعات، وكيفية التعامل معها.

وعلى الرغم من أن الجريمة الإلكترونية قد تكون ظاهرة حديثة، إلا أنها تتسم بأثر كبير على المجتمعات والمؤسسات، حيث تسبب خسائر مالية كبيرة وتؤدي إلى تقليل الثقة بين الناس وتفكك الهياكل الاجتماعية. ولذلك، فإن الحاجة إلى مكافحة الجريمة الإلكترونية تتطلب تنسيق الجهود بين المؤسسات والحكومات والقطاع الخاص والأفراد، وذلك من خلال توفير الحماية اللازمة للأنظمة الإلكترونية وتعزيز الوعي الأمني وتعزيز التعاون الدولي لمواجهة هذه الظاهرة. ومن الجانب الاجتماعي، يمكن أن يؤدي العمل على مكافحة الجريمة الإلكترونية إلى تحسين الثقة بين الأفراد والمؤسسات، وتعزيز التعاون والتكامل الاجتماعي. وهذا يعزز بدوره استقرار المجتمع وتطوره الاقتصادي والاجتماعي.

وفي النهاية، يمكن القول إن مواجهة الجريمة الإلكترونية تحتاج إلى جهود مشتركة من جميع الأطراف المعنية، وإلى الاستفادة من التكنولوجيا والابتكار والتعاون الدولي للحفاظ على الأمن الإلكتروني. إن السيطرة على الجريمة الإلكترونية تتطلب أيضاً إيجاد الحلول الفعالة لمعالجة الأسباب الجذرية التي تؤدي إلى الارتفاع المستمر في عدد الجرائم الإلكترونية. ويجب أن يتم التعامل مع هذه الأسباب من خلال إجراءات وسياسات اجتماعية واقتصادية وقانونية فعالة. يجب أن يعمل المجتمع الدولي على إنشاء بيئة رقمية آمنة وتطوير القوانين والتشريعات الدولية لمكافحة الجريمة الإلكترونية، بالإضافة إلى تعزيز التعاون الدولي في هذا المجال. ومن المهم أن تأخذ الدول المسؤولية في تبني السياسات العامة وتطوير قوانين صارمة لمعاقبة الجريمة الإلكترونية، مع توفير الدعم والموارد اللازمة لإنفاذ هذه القوانين. بالإضافة إلى ذلك، يجب على الجميع أن يكون لديهم الوعي اللازم بالأمان الإلكتروني وتعزيز الثقافة الأمنية، وذلك من خلال توفير التدريب والتوعية للأفراد والمؤسسات، وتشجيع الأبحاث والتطوير في مجال الأمن الإلكتروني.

وفي النهاية، يجب أن يتعاون الجميع في العمل على مواجهة الجريمة الإلكترونية، لأنها تمثل تهديداً كبيراً للأمن الإلكتروني والاستقرار الاجتماعي والاقتصادي. وإذا تم العمل على تطبيق الإجراءات والسياسات اللازمة، فإنه يمكن الحد من هذه الظاهرة والحفاظ على الأمن الإلكتروني في المستقبل.

توصيات ومقترحات

يمكن تقديم بعض المقترحات والتوصيات للحد من الجريمة الإلكترونية، وتشمل:

1. تعزيز التوعية والتثقيف الإعلامي: ينبغي توفير المزيد من التوعية والتثقيف الإعلامي للجمهور حول أنواع الجرائم الإلكترونية وطرق الوقاية منها والإبلاغ عنها.
2. تشديد العقوبات وتطوير القوانين: ينبغي تطوير القوانين والتشديد على العقوبات المفروضة على الجرائم الإلكترونية، بما يواكب التطورات السريعة في هذا المجال ويحد من ارتكاب هذه الجرائم.
3. تعزيز الأمن الإلكتروني: يجب على المؤسسات والحكومات والأفراد تعزيز أمنهم الإلكتروني وتحسين نظم الحماية المستخدمة في الشبكات الإلكترونية.
4. تطوير التقنيات الأمنية: ينبغي تطوير التقنيات الأمنية المستخدمة في الحماية من الجرائم الإلكترونية، مثل تقنيات التشفير.
5. التعاون الدولي: يجب تعزيز التعاون الدولي والتبادل المعلوماتي بين الدول لمكافحة الجرائم الإلكترونية، وذلك من خلال إبرام اتفاقيات وتشكيل فرق عمل مشتركة.
6. التوجيه الأخلاقي والقيمي: يجب تعزيز التوجيه الأخلاقي والقيمي للأفراد والمجتمعات، والتأكيد على مسؤولية استخدام التكنولوجيا والإنترنت بشكل إيجابي وضمن إطار القوانين والأخلاقيات الإنسانية.

قائمة المراجع

-أبو عليان، بسام محمد: (2016)، الانحراف الاجتماعي والجريمة، ط3، فلسطين، دار الكتب للنشر والتوزيع.

- إسراء جبريل رشاد مراعي: (2018)، الجرائم الإلكترونية الأهداف، والأسباب وطرق الجريمة ومعالجتها، مجلة الدراسات الإعلامية، العدد 1، المركز الديمقراطي العربي.
- اسماعيل محمد الزبيد: (2010)، علم الاجتماع، عمان، دار كنوز المعرفة للنشر والتوزيع.
- البداينة، ذياب موسى: (2014)، الجرائم الإلكترونية -المفهوم والأسباب، ورقة بحث مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان.
- البقلي، هيثم عبد الرحمن: (2010)، الجرائم الإلكترونية الواقعة على العرض بين الشريعة والقانون، القاهرة، دار العلوم للنشر والتوزيع.
- حسنين شفيق: (2015)، الإعلام الجديد والجرائم الإلكترونية (التسريبات، التجسس، الإرهاب الإلكتروني)، مصر، دار فكر وفن للطباعة والنشر والتوزيع.
- الخمشي، سارة صالح عيادة: (2013)، الخدمة الاجتماعية في مجال الجريمة والإصلاح، المملكة العربية السعودية، مكتبة الملك فهد.
- الديري، عبد العال واسماعيل محمد صادق: (2012)، الجرائم الإلكترونية، القاهرة، المركز القومي للإصدارات القانونية.
- الزنداني، إبراهيم محمد بن حمود: (2018)، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: دراسة مقارنة. رسالة ماجستير في قسم الدراسات الإسلامية، جامعة فطاني.
- سمير، شعبان: (2009)، الجريمة الإلكترونية-مقاربة تحليلية-، العدد 1، مجلة دراسات وأبحاث، الجلفة.
- سليبي، زهراء عادل، (2021)، جريمة الابتزاز الإلكتروني، شركة دار الأكاديميون للنشر والتوزيع.
- شنتير، خضرة: (2021)، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أدرار.
- صفاء محمد نور عيد أحمد: (2018)، التغير الاجتماعي وعلاقته بتطور الجرائم الإلكترونية، رسالة ماجستير في علم الاجتماع، جامعة النيلين.
- صورية، قلالي، وعبد الحليم، بوقرين: (2019)، أثر الجريمة على الحياة الخاصة للأفراد، المجلد الثالث، العدد 2، المجلة الأكاديمية للبحوث القانونية والسياسية.
- عبد الصبور عبد القوي علي مصري، ومنال عبد الاله عبد الرحمن: (2012)، المحكمة الرقمية والجريمة المعلوماتية: دراسة مقارنة، الرياض، مكتبة القانون والاقتصاد.
- عبد الصبور عبد القوي، علي مصري: (2012)، التنظيم القانوني للتجارة الإلكترونية، الرياض، مكتبة القانون والاقتصاد.
- القاسمي، مهرة سالم: (2013)، انحراف الأحداث مشكلة تؤرق المجتمع العربي، القاهرة، مكتبة جزيرة الورد.
- الكتبي، آمنة جمعة: (2010)، الشباب والجريمة، الشارقة، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة.

- لينا، جمال: (2016)، الجرائم الإلكترونية-ماهيها وطرق مكافحتها- عمان، دار خالد اللحياني للنشر والتوزيع.
- مجمع البحوث والدراسات: (2016)، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، سلطة عمان، مجلس التعاون لدول الخليج العربية.
- محمد سعيد عبد المجيد، (2006)، المعلوماتية والجريمة، تحليل مضمون لبعض الجرائم الإلكترونية، مصر، دار ومكتبة الإسراء للطبع والنشر والتوزيع.
- مرفت محمد حبابية: (2022)، مكافحة الجريمة الإلكترونية، ط1، عمان، دار اليازوري العلمية للنشر والتوزيع.
- معاشي، سميرة: (2018)، الجريمة المعلوماتية- دراسة تحليلية لمفهوم الجريمة الإلكترونية، العدد 17، مجلة المفكر.
- موسى يعقوب عبد الحليم: (2014)، الإعلام الجديد والجريمة الإلكترونية، الهرم، الدار العالمية للنشر والتوزيع.
- نصار، غادة: (2017): الإرهاب والجريمة الإلكترونية، القاهرة، دار العربي للنشر والتوزيع.
- الهاشمي، رفد عيادة: (2019)، الإرهاب الإلكتروني القانوني، دار أمجد للنشر والتوزيع.
- هرزاني، نوري ياسين: (2005)، الإعلام والجريمة، كردستان، منتدى اقرأ الثقافي.
- يونس عرب: (2002)، موسوعة القانون وتقنية المعلومات (دليل أمن المعلومات والخصوصية)، الجزء الأول، منشورات اتحاد المصارف العربية.
- William Kornblum, Joseph Julian: Social problems, Pearson. Inc, 14th edition, 2012