الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد الشريف مساعدية

سوق أهراس

كلية العلوم الإنسانية والاجتماعية

**المؤتمر العلمي الافتراضي الأول: الجريمة الإلكترونية (الواقع والتداعيات)**

**عنوان المداخلة:** **الإجرام الإلكتروني، كفاءات ضائعة في عالم التقنية!**

الباحثة: شفيقة خنيفر

الهيئة المستخدمة: جامعة محمد الشريف مساعدية –سوق أهراس-

**مقدمة:**

**الحديث عن التطورات المتسارغعة للتكنلوجيا وكيف تتضمن من حيث الاستخدام أمورا مقبولة وأخرى غير مقبولة**

**1/ العالم قبل ظهور الجريمة الإلكترونية:**

قبل ظهور الانترنت وجرائمه، كانت توجد الأفعال الإجرامية وكانت هذه الأفعال تشمل القتل والسرقة والنصب والتزوير وغيرها من الجرائم، فالشر قائم، بيد أن الانترنت ساعد على سهولة ارتكاب هذه الجرائم، ففضاء المعلومات ليس له مبادئ أخلاقية عامة، فحدود السلوك المقبول أو حتى السلوك الأخلاقي في فضاء المعلومات ليست واضحة، فوجود الانترنت أدى إلى تطور الجرائم التقليدية واستحداث جرائم جديدة[[1]](#footnote-2). (غادة نصار، 2017، صفحة 09)

2/ **نشأة الجريمة الإلكترونية:**

مرت الجرائم الإلكترونية بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ولهذا يمكننا القول بأن تلك الجرائم مرت بثلاث مراحل يمكن إيجازها على النحو التالي:

* **المرحلة الأولى:** تتمثل في شيوع استخدام الحواسيب في الستينيات والسبعينيات، ومع تزايد استخدام الحواسيب الشخصية في السبعينيات ظهر عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر، وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.
* **المرحلة الثانية:** في الثمانينيات طفا على السطح مفهوم جديد للجرائم الإلكترونية ارتبط بعمليات اقتحام نظام الكمبيتر عن بعد، وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات والبرامج.
* **المرحلة الثالثة:** وتتمثل في فترة التسعينيات حيث شهدت تناميا هائلا في حقل الجرائم الإلكترونية، وتغييرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعملية دخول الأنظمة واقتحام شبكة المعلومات.[[2]](#footnote-3) (هشام بشير، 2012، الصفحات 06-07)

وقد ظهرت الجرائم الإلكترونية لأول مرة بشكل مكثف في المجتمعات الغربية كأمريكا وما جاورها، وذلك لأن هذه التقنية وجدت في الأساس لديهم في معامل وزارة الدفاع الأمريكية، وكان من الطبيعي وجود تجاوزات ومخالفات جسيمة من قبل مستخدمي الانترنت لدى هذه الوزارات الحكومية من الفنيين والمهندسين والمؤتمنين على أجهزة الحاسب، ومما ساعد على انتشار هذا النوع من الجرائم واستفحال خطرها أول الأمر، عدم وجود القوانين التي تجرم الاعتداء على المعلومات والبيانات، وحتى لو فرض وجود هذه القوانين، فإن صعوبة الكشف عن هذه الجرائم وصعوبة ملاحقة فاعليها، أغرى الكثيرين بخوض غمار هذا الفن من فنون الإجرام.[[3]](#footnote-4) (حمود بن محسن الدعجاني، صفحة 557).

**3/ حول مفهوم الجريمة الإلكترونية:**

إن الجريمة المعلوماتية تكاد تستعصي على التعريف، ذلك أن الأبحاث والدراسات التي تتعلق بها قد أوردت لها تعريفات مختلفة ومتنوعة، بحيث اتفقت جميعها على أن لا تتفق على تعريف محدد لهذه الجريمة، وتكشف النماذج المعروضة لتعريفات هذه الجريمة تعدد المصطلحات المستخدمة للدلالة عليها وتحديد مفهومها، فهناك من يطلق عليها اسم جرائم الحاسبات، أو إساءة استخدام الحاسب، أو الجرائم المرتبطة أو المتعلقة بالحاسبات، أو جرائم المعالجة الآلية للبيانات أو جرائم التكنولوجيا الحديثة أو جرائم المعلوماتية[[4]](#footnote-5). (خالد حسن أحمد لطفي، 2019، صفحة 25)

فمن يستخدم مصطلح الجريمة المعلوماتية أراد التعبير عن الجريمة التي يكون فيها موضوع الحق المعتدى عليه المعلومة، أما من يستخدم مصطلح جرائم الانترنت فهو استخدام ضيق لأنه سيقصر هذه الجرائم على سلوكيات غير مشروعة ترتكب عن طريق الولوج إلى شبكة الانترنت دون الجرائم التي يمكن أن نتصور إمكانية ارتكابها عن طريق جهاز الكمبيوتر دون الحاجة إلى استخدام الانترنت، أما من يستخدم مصطلح الجريمة الإلكترونية فيقصد بها الجرائم المرتكبة عن طريق الكمبيوتر وغيره من وسائل الاتصال الحديث[[5]](#footnote-6). (المرجع السابق، صفحة 27)

وقد تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلى الخلاف الذي أثير بشأن تعريف هذه الجريمة ومن قبلها تعريف المعلومة ذاتها، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية، قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريفها الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها...وذهب البعض إلى ترجيح عدم وضع هذا التعريف بحجة أن هذا النوع من الإجرام ماهو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني.[[6]](#footnote-7) (عبد العال الديربي، محمد صادق إسماعيل، 2012، صفحة 41)

**4/ مفهوم الجريمة الإلكترونية:**

تتكون الجريمة الإلكترونية أو الافتراضية (CYBER CRIMES) من مقطعين هما الجريمة (CRIME) و الإلكترونية (CYBER) ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة الإلكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة، وبقصد إيذاء سمعة الضحية أذى مادي أو عقلي، مباشر أو غير مباشر، باستخدام شبكات الاتصال مثل الانترنت (مثل غرف الدردشة والبريد الإلكتروني والموبايل) (ذياب موسى البداينة، صفحة 03).[[7]](#footnote-8)

ويمكن تعريف جرائم الانترنت بأنها "مجمل الجرائم المرتكبة باستعمال المعلوماتية أو الشبكات المعلوماتية، وتكون هذه الجرائم ذات طبيعة متعددة، ويمكن أن تأخذ شكل الإجرام التقليدي باستعمال الوسائل التقنية للشبكات". (مي العبد الله، 2014، صفحة 139)[[8]](#footnote-9)

ومن التعريفات كذلك نذكر: "أنها كل فعل ضار بالآخرين عبر الوسائط الإلكترونية مثل الحواسيب، أجهزة الموبايل، شبكات الاتصال الهاتفية، شبكة نقل المعلومات، شبكة الانترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموما"

كما تعرف بأنها: "مجموعة من الأفعال والأنشطة المعاقب عليها قانونا، والتي تربط بين الفعل الإجرامي والثورة التكنولوجية"[[9]](#footnote-10) (محمود مدين)

وتعرف بأنها: "فعل غير مشروع يعتمد الدراية والمعرفة الفنية بتقنية المعلومات، يتم بأي أداة من أدوات الاتصال الذكي والبرمجي، ويكون فيه الفضاء الإلكتروني محلا ومسرحا لها"[[10]](#footnote-11) (ابراهيم محمد بن محمود الزنداني، 2018)

5/ **النشاط الإجرامي في فضاء الانترنت**

إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالانترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه، ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة، فيقوم بتحميله ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها، وليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والانترنت.[[11]](#footnote-12) (عبد الحليم موسى يعقوب، 2014، الصفحات 215-216)

**6/ أهدافها**

1. الوصول إلى المعلومات بشكل غير قانوني، كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق الهدف الإجرامي.
2. الوصول إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو تخريبها، وعادة ما تتم هذه العملية على مواقع الانترنت.
3. الحصول على معلومات، تغيير عناوين مواقع الانترنت بهدف التخريب على المؤسسات العامة وابتزازها.
4. الوصول إلى الأشخاص أو الجهات المستخدمة للتكنولوجيا، بغرض التهديد أو الابتزاز، كالبنوك أو الدوائر الحكومية والأجهزة الرسمية والشركات بكافة أشكالها.
5. الاستفادة من تقنية المعلومات من أجل كسب مادي أو معنوي أو سياسي غير مشروع لعمليات تزوير بطاقات الائتمان وعمليات اختراق مواقع إلكترونية على الشبكة العنكبوتية..الخ
6. استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة، أو نشر الأفكار التي يمكن أن تؤسس إلى فكر تكفيري.[[12]](#footnote-13)

**7/ خصائص الجريمة الإلكترونية**

تتشابه الجريمة الإلكترونية مع الجريمة التقليدية من جانب أركان الجريمة، من مجرم ذي دافع لارتكاب الجريمة، وضحية، والذي قد يكون شخصا طبيعيا أو شخصا اعتباريا، وأداة الجريمة، ففي الجريمة الإلكترونية تكون أداة الجريمة من مخرجات التقنية، وكذلك مكان الجريمة الذي لا يرهق الجاني في الوصول إليه، مما سهل عملية الجريمة الإلكترونية، وفي العديد من هذه الجرائم فإن الجريمة تتم عن بعد، باستخدام خطوط وشبكات الاتصال بين الجاني وموقع الجريمة"[[13]](#footnote-14)

ومن خصائص الجريمة الإلكترونية:

**أولا: جريمة عابرة للقارات:**

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم، أدى إلى انعكاس على طبيعة الأعمال الإجرامية، التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا.

**ثانيا: جرائم ناعمة ومغرية للمجرمين:**

إذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى مجهود عضلي كجرائم القتل والاغتصاب، فإن الجريمة الإلكترونية على العكس لا تحتاج إلى أدنى مجهود عضلي، بل تعتمد على الدراية الذهنية والتفكير المدروس، القائم على المعرفة بتقنيات الحاسب الآلي، فهي لا تحتاج إلى أي درجة من القرب أو التلامس المادي بين الجاني والضحية، لذا تتسم بأنها أقل عنفا وخشونة من التقليدية.[[14]](#footnote-15) (أدهم باسم نمر بغدادي، 2018، الصفحات 11-12)

**8/ أطراف الجريمة الإلكترونية:**

لكل جريمة جاني ومجني عليه وآثار تترتب على تنفيذ الجريمة.[[15]](#footnote-16)

1. **الجاني في الجريمة الإلكترونية**

في العالم الإلكتروني صغير المجرمين كالكبير منهم، والمازح من بينهم كالحاقد، وضمان أمن المعلومات وضمان عدم التعرض للمسؤوليات يوجب التعامل مع الكل على أنهم مصدر للخطر، وليس المسألة اهدارا لفكرة حسن النية أو الثقة بالآخرين، إنها الضمان الوحيد للحماية من مصادر بالغة الخطر تؤدي إلى مسؤوليات وخسائر لا يمكن تقديرها أو تجاوزها.[[16]](#footnote-17) (أيمن عبد الله فكري، 2014، صفحة 120)

وتعتبر أغلب الدراسات والتشريعات أن الجاني في الجرائم الإلكترونية شخص طبيعي يعمل لحسابه، ويهدف إلى تحقيق مصلحة خاصة به من وراء الجريمة التي يرتكبها، حيث يتم تصنيف معظم من يرتكب جرائم الحاسب الآلي إلى الجيل الحديث من الشباب، أو هم قد يكونون محترفين عاملين بمجال الحاسب الآلي أو قد يكونون هواة أو عابثين صغار، بيد أن الواقع العملي أثبت خلاف ذلك، فإلى جانب الشخص الطبيعي قد يوجد مشتركون يمدونه بما يحتاجه من أدوات وبرامج ومعدات، أو على الأقل يبيعونه تلك المنتجات والبرامج، التي بدونها فإنه لن يكون هنالك جريمة من الأساس، كما قد يكون الجاني مجموعة من الأشخاص أو مؤسسات أو أشخاص معنوية، وقد يصل الأمر إلى الجرائم الإلكترونية التي يكون فيها الجاني أنظمة سياسية ودولا.[[17]](#footnote-18)

و خطورة هذه الجرائم تكمن بصفة أساسية في المجرم الذي يقوم بتنفيذ الجريمة، حيث أنه يمتاز بالذكاء والدراية في التعامل في مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية.[[18]](#footnote-19)

1. **الصفات الشخصية للمجرم الإلكتروني:**

تنوعت الدراسات التي تحدد الصفات الشخصية للمجرم المعلوماتي، والتي توصلت إلى أنه لا يمكن أن يكون هناك نموذج محدد له، وإنما هناك سمات مشتركة بين هؤلاء المجرمين يمكن إجمالها في الآتي:

* مجرم يتمتع بقدرة فائقة من الذكاء، وهذا ما يؤهله أن يقوم بتعديل وتطوير في الأنظمة الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات، أو داخل أجهزة الحواسيب.
* مجرم متخصص، الذي له القدرة الفائقة في المهارة التقنية، ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفرات.
* مجرم دائما عائد للإجرام، يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في الدخول غير المصرح به مرات ومرات.
* مجرم ينتمي إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية.[[19]](#footnote-20)

1. **الصفات السيكولوجية للمجرم الإلكتروني**

من خلال الدراسات النفسية للمجرم المعلوماتي، ثبت أنه ليس لديه أي شعور بعدم مشروعية الأفعال التي يقترفونها، وعدم استحقاقهم للعقاب من هذه الأفعال، فحدود الشر والخير متداخلة لدى هذه الفئة، وتغيب في دواخلهم مشاعر الإحساس بالذنب، وهذا يأتي من خلال عدم وجود احتكاك مباشر بين الجاني والمجني عليه.[[20]](#footnote-21)

1. **أصناف المجرم الإلكتروني:**

**أولا: القراصنة:** يمكن تصنيفهم إلى صنفين:

1. **الهاكرز**: هي طائفة من المتطفلين يتحدون إجراءات أمن النظام والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، فاصطلاح الهاكرز مرادف في الغالب لهجمات التحدي.[[21]](#footnote-22)

كما يعرف الهاكرز بأنهم الأشخاص الذين يخترقون جهازك، فيستطيعون مشاهدة ما به من ملفات، أو سرقتها أو تدمير جهازك أو التلصص أو مشاهدة ما تفعله على شبكة الانترنت.[[22]](#footnote-23)

فمن خلال الدخول إلى أنظمة الحاسبات الآلية، غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، ويكون هدف هذا الصنف الشاب الخبرة، أو يكون المحرك الأساسي لهم هو الفضول أو إثبات الذات.[[23]](#footnote-24)

1. **الكراكرز:** اصطلاح الكراكرز مرادف للهجمات الحاقدة والمؤذية،[[24]](#footnote-25) وهم الأشخاص الذين يقومون بالتسلل إلى أنظمة المعالجة الآلية للإطلاع على المعلومات المخزنة بها، لإلحاق الضرر أو العبث بها أو سرقتها.[[25]](#footnote-26)

وطبعا هذا التمييز لا يؤثر على مسؤولية مرتكبي الأنشطة من كلا الطائفتين، ومساءلتهم عما يلحقونه من أضرار بالمواقع المستهدفة باعتداءاتهم.[[26]](#footnote-27)

**ثانيا: الحاقدون:**

يحرك أنشطة هذه الفئة الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم، عندما لا يكونون موظفين فيها، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات زراعة الفيروسات و البرامج الضارة وتخريب النظام.[[27]](#footnote-28)

فالعاملون في قطاع التقنية أو المستخدمون لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل، والمشكلات المالية وعن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور قد تمثل في حالات كثيرة قوة محركة لبعض العاملين لارتكاب جرائم معلوماتية باعثها الانتقام من المنشأة أو رب العمل، ومثال ذلك فقد دفع الانتقام بمحاسب إلى التلاعب بالبرامج المعلوماتية، بحيث جعل هذه البرامج تعمل على إخفاء تلك البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله ب 6 أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.[[28]](#footnote-29)

**ثالثا: الهواة:**

من يرتكبون هذه الجرائم بغرض التسلية، دون أن تكون لديهم نية إحداث أي أضرار بالمجني عليهم، وتتميز هذه الفئة بصغر سنهم ونبوغهم في علوم الحاسب، إلا أن خطورتهم تكمن في أنهم قد يكونون نواة جيدة للتحول إلى قرصان محترف.[[29]](#footnote-30)

1. **المجني عليه في الجريمة الإلكترونية:**

من الصعب تحديد ضحايا الجرائم الإلكترونية تحديدا دقيقا، لأنهم غالبا لا يعلمون عن هذه الجرائم إلا بعد أن تقع بالفعل، وكما الجاني فإن المجني عليه أيضا قد يكون شخصا طبيعيا أو أشخاصا معنوية أو مجتمعات أو دول.[[30]](#footnote-31)

**9/ أشكال الجرائم الإلكترونية**

1. **الجرائم الجنسية والإباحية وغير الأخلاقية:**

توجد مواقع على شبكة الانترنت تحرض على ممارسة الجنس، سواء على الكبار أو الأطفال، وتقوم هذه المواقع بنشر صور جنسية أكثر تخصصية، فمنها ما هو متخصص في أفلام الفيديو، ومنها ما هو متخصص في الصور، وكثير منها متخصص في برامج المحادثة...و قد تم حصر المواقع الإباحية العربية دون الأجنبية على شبكة الانترنت فوجد أنها تصل إلى 71 موقعا.

1. **قرصنة البرامج عبر شبكة الانترنت**

وهي من الجرائم التي ارتبطت بنشأة الحاسبات الآلية بصفة عامة، إلا أن ظهور شبكات المعلومات قد ساعد على نحو كبير في زيادة حجم هذه الجريمة، لما وفرته هذه الشبكات من مجال خصب لارتكابها، نظرا لطبيعتها المفتوحة وارتفاع قيمة هذه البرامج وسهولة نسخها في ثوان معدودة، وما توفره الشبكات من مجال خصب لتسويق هذه البرامج المنسوخة، أغرى قراصنة البرامج لممارسة أعمالهم داخل الشبكة.

1. **إتلاف المعلومات**

عن طريق ضرب وحدات تشغيل المعلومات بأدوات ثقيلة واستعمال الحريق بها، أو تفجيرها بشحنات ناسفة، أو باستخدام قنبلة غاز قارض أو مواد ملتهبة بمفاتيح التشغيل، كذلك عن طريق محو بطاقة التعريف بماهية المعلومات المختزنة أو بمسح البرنامج أو إخفاء بعض البطاقات..أو يمكن إفساد المعلومات مغناطيسيا بإخضاعها لقوى مغناطيسية متلفة.

1. **إساءة استخدام البطاقات البنكية**

وهي من الجرائم المتعلقة خصوصا في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور والحداثة، وتمنح فيها البطاقات البنكية، وكذلك تستخدم بأقل قدر من الإجراءات، ومن صورها:

* استخدام البطاقات المسروقة أو منتهية الصلاحية، تزوير البطاقات، قيام صاحب البطاقة نفسه بسحب مبالغ نقذية أكبر من المبالغ المسموح له عن طريق آلة التوزيع الآلي للنقوذ، مستغلا بعض الثغرات التي تعاني منها الآلات...كذلك قيام بعض الأشخاص بإبلاغ البنك بضياع بطاقاتهم البنكية دون أن يكون ذلك صحيحا، ثم يقومون على الفور بسحب النقوذ قبل أن يقوم البنك بالتحفظ على أموالهم وحمايتها، بحيث يعطون انطباعا بأن سارق البطاقة أو من وجدها هو الذي قام بسحب النقوذ.[[31]](#footnote-32)

1. **سرقة البيانات الشخصية:**

وهي الاستيلاء على المعلومات المقدمة للجهاز (برامج أو بيانات المعالجة) سواء أكانت هذه البيانات في أسطوانات أو على شريط ممغنط أو على ورق.

1. **التلاعب في برامج الأشخاص**

للبرامج أهمية عظمى في مجال استخدام الحاسب الآلي، لأن هذا البرنامج هو الذي يعطي الروح للحاسب فيجعله قادرا على القيام بما يناط به من أعمال، ومن هذه البرامج: تغيير برنامج نظام التشغيل، خلق برنامج جديد (وهمي) من أجل ارتكاب الجريمة.

1. **جرائم القذف والتشهير:**

من خلال التعرض للحياة الخاصة والتلصص على مواقع الأشخاص على الشبكة والتسلل إليها وأخذ ما فيها من صور خاصة وأخبار، والعمل على نشر هذه الصور التي قد تمس الشرف.[[32]](#footnote-33)

كما تبرز هذه الجريمة من منطق ابتزازي، حيث يتم التقاط صور للشخص 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.[[33]](#footnote-34)

1. **جرائم المقامرة**

وتشمل تملك وإدارة مشروع مقامرة على الانترنت، وتسهيل ذلك وتشجيعه، واستخدام الانترنت لترويج الكحول ومواد الإدمان للقصر.

1. **الاحتيال الإلكتروني:**

ويقصد به أي سلوك أو تصرف يحدث من فرد أو العديد من الأفراد يرهق أو يتسبب في أعباء إضافية على أية أطراف أخرى، نتيجة استخدام ممارسات غير أخلاقية للحصول على ميزة غير عادلة أو غير قانونية.[[34]](#footnote-35)

10/ **مكافحة الجرائم الإلكترونية**

يمكن أن نلخص أساليب مكافحة الجرائم الإلكترونية في الآتي:

* رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الانترنت، إذ يستلزم التدخل الحكومي والدولي نظرا للخطورة الجسيمة للأمر.
* الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكبيها والاستدلال عليهم بأقل وقت ممكن.
* توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وما يترتب عليها من مخاطر.
* الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية والبطاقات الائتمانية وغيرها.
* عدم الكشف عن كلمة السر نهائيا وتغييرها بشكل مستمر واختيار كلمات سر صعبة.
* تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.
* تجنب تحميل أي برنامج مجهول المصدر.
* استمرارية تحديث برامج الحماية الخاصة بالحاسوب.
* تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.
* المسارعة بإبلاغ الجهات الأمنية فور التعرض لجريمة إلكترونية.
* مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.
* استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.
* فصل اتصال جهاز الحاسوب بشبكة الانترنت في حال عدم الاستخدام.
* أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.[[35]](#footnote-36) (لامية طالة، كهينة سلام، مج 06، عدد 02 2020)

**الخلاصة**

**المراجع**

**1**-ابراهيم محمد بن محمود الزنداني. (2018). *الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني ماجستير في قسم الدراسات الإسلامية.* تايلند: جامعة فطاني.

**2**- أدهم باسم نمر بغدادي. (2018). *وسائل البحث والتحري عن الجرائم الإلكترونية، ماجستير في القانون العام.* نابلس، فلسطين: كلية الدراسات العليا، جامعة النجاح.

**3**- أيمن عبد الله فكري. (2014). *الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية.* الرياض: مكتبة القانون والاقتصاد.

**4**- حمود بن محسن الدعجاني. (بلا تاريخ). *ملحق العدد 173 ج16 مجلة الجامعة الإسلامية* .

**5**- خالد حسن أحمد لطفي. (2019). *الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية.* الاسكندرية: دار الفكر الجامعي.

**6**- ذياب موسى البداينة. *الجرائم الإلكترونية المفهوم والأسباب.* عمان، المملكة الهاشمية الأردنية: الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية.

**7**- عبد الحليم موسى يعقوب. (2014). *الإعلام الجديد والجريمة الإلكترونية.* الدار العالمية للنشر والتوزيع.

**8**- عبد العال الديربي، محمد صادق إسماعيل. (2012). *الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت.* القاهرة: المركز القومي للإصدارات القانونية.

**9**- غادة نصار. (2017). *الإرهاب والجريمة الإلكترونية.* القاهرة: ط1 العربي للنشر والتوزيع.

**10**- لامية طالة، كهينة سلام. (مج 06، عدد 02 2020). الجريمة الإلكترونية، بعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي. *مجلة الرواق للدراسات الاجتماعية والانسانية* ، الصفحات 86-88.

**11**- محمود مدين. *الجريمة الإلكترونيةوتحديات الأمن القومي دكتوراه في القانون الدولي العام.* المصرية للنشر والتوزيع.

**12**- مي العبد الله. (2014). *المعجم في المفاهيم الحديثة للإعلام والاتصال، المشروع العربي لتوحيد المصطلحات.* بيروت، لبنان: ط1 دار النهضة العربية.

13- هشام بشير. (2012). *الآليات الدولية لمكافحة الجريمة الإلكترونية.* المركز الدولي للدراسات المستقبلية والاستراتيجية.

استمارة المشاركة  
 الاسم و اللقب: شفيقة خنيفر  
الرتبة العلمية: أستاذ محاضر -ب-   
المؤسسة المستخدمة.: جامعة محمد الشريف مساعدية -سوق أهراس-  
البلد: الجزائر.

التخصص: الإعلام والاتصال.  
البريد الالكتروني:

رقم الهاتف: 04/55/36/0664.  
محورالمداخلة: المحور المفاهيمي

عنوان المداخلة:الإجرام الإلكتروني، كفاءات ضائعة في عالم التقنية!   
المكلمات المفتاحية: الإجرام الإلكتروني- التقنية.  
الملخص:..................................................................................................................................

1. غادة العربي نصار: الإرهاب والجريمة الإلكترونية، ط1، العربي للنشر والتوزيع، القاهرة 2017، ص: 09 [↑](#footnote-ref-2)
2. هشام بشير: الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية والاسترتيجية، 2012، ص: 06-07. [↑](#footnote-ref-3)
3. حمود بن محسن الدعجاني، ملحق العدد 173، ج16 مجلة الجامعة الإسلامية، جامعة شقراء، السعودية، ص: 557. [↑](#footnote-ref-4)
4. خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي الاسكندرية، 2019، ص: 25. [↑](#footnote-ref-5)
5. المرجع نفسه، ص: 27. [↑](#footnote-ref-6)
6. عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، ط1: المركز القومي للإصدارات القانونية، القاهرة، 2012، ص: 41 [↑](#footnote-ref-7)
7. ذياب موسى البداينة، ورقة علمية بعنوان: الجرائم الإلكترونية المفهوم والأسباب، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، المملكة الأردنية الهاشمية، ص: 03. [↑](#footnote-ref-8)
8. مي العبد الله، المعجم في المفاهيم الحديثة للإعلام والاتصال، المشروع العربي لتوحيد المصطلحات، ط1، دار النهضة العربية، بيروت، لبنان، 2014، ص: 139. [↑](#footnote-ref-9)
9. محمود مدين: الجريمة الإلكترونية وتحديات الأمن القومي، دكتوراه في القانون الدولي العام، ط2، المصرية للنشر والتوزيع. [↑](#footnote-ref-10)
10. ابراهيم محمد بن محمود الزنداني: الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني، ماجستير في قسم الدراسات الإسلامية، جامعة فطاني، تايلند 2018، ص: 27. [↑](#footnote-ref-11)
11. عبد الحليم موسى يعقوب: الإعلام الجديد والجريمة الإلكترونية، ط1: الدار العالمية للنشر والتوزيع، 2014، ص: 215-216. [↑](#footnote-ref-12)
12. المرجع السابق، ص: 213-214. [↑](#footnote-ref-13)
13. المرجع نفسه، ص: 201. [↑](#footnote-ref-14)
14. أدهم باسم نمر بغدادي: وسائل البحث والتحري عن الجرائم الإلكترونية، ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص:11-12. [↑](#footnote-ref-15)
15. خالد حسن أحمد لطفي –مرجع سابق-ص: 35. [↑](#footnote-ref-16)
16. أيمن عبد الله فكري: الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، ط1 مكتبة القانون والاقتصاد، الرياض، 2014، ص: 120. [↑](#footnote-ref-17)
17. ابراهيم بن محمد الزنداني-مرجع سابق- ص: 36. [↑](#footnote-ref-18)
18. خالد حسن أحمد لطفي: مرجع سابق، ص: 35 [↑](#footnote-ref-19)
19. المرجع السابق، ص: 36. [↑](#footnote-ref-20)
20. المرجع نفسه، ص: 37. [↑](#footnote-ref-21)
21. أيمن عبد الله فكري: مرجع سابق، ص: 123. [↑](#footnote-ref-22)
22. عبد الحليم موسى يعقوب، مرجع سابق، ص: 201. [↑](#footnote-ref-23)
23. خالد حسن أحمد لطفي، مرجع سابق، ص: 38. [↑](#footnote-ref-24)
24. أيمن عبد الله فكري، المرجع السابق، ص: 123. [↑](#footnote-ref-25)
25. خالد حسن أحمد لطفي، المرجع السابق، ص: 38. [↑](#footnote-ref-26)
26. أيمن عبد الله فكري، المرجع السابق، ص: 123. [↑](#footnote-ref-27)
27. المرجع نفسه، ص: 123. [↑](#footnote-ref-28)
28. خالد حسن أحمد لطفي، المرجع سابق، ص: 39. [↑](#footnote-ref-29)
29. المرجع نفسه، ص: 38. [↑](#footnote-ref-30)
30. ابراهيم محمد بن محمود الزنداني، مرجع سابق، ص: 37. [↑](#footnote-ref-31)
31. غادة نصار: مرجع سابق، ص ص: 15-19. [↑](#footnote-ref-32)
32. المرجع السابق، ص: 19-22 [↑](#footnote-ref-33)
33. عبد الحليم موسى يعقوب، مرجع سابق، ص: 222. [↑](#footnote-ref-34)
34. المرجع السابق، ص: 23. [↑](#footnote-ref-35)
35. لامية طالة، كهينة سلام: الجريمة الإلكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، المجلد06، العدد 02 مجلة الرواق للدراسات الاجتماعية والإنسانية، 2020، ص86-88. [↑](#footnote-ref-36)