

الجريمة الإلكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية

غنية عباس *

أستاذة ، (كلية الحقوق)

جامعة لونيبي علي - البليدة 02.

تاريخ الارسال 10-03-2021 - تاريخ القبول 04-12-2021

الملخص:

مرت الجريمة الإلكترونية بعدة مراحل مختلفة فوصلت إلى درجة عالية من التطور وذلك بتطور التكنولوجيا، وبتطورها وتغيرها صعب على التشريعات إيجاد مفهوم متفق عليه، حيث تأرجحت تعاريفها بين التعريفات التي استندت إلى موضوع الجريمة وتعريفات استندت على وسيلة الجريمة ولكنها لم تتخلف عن التصدي لها ومحاربتها بأحدث الطرق، أما بالنسبة للمشرع الجزائري فقد تطرق إلى تعريف الجريمة الإلكترونية مسميا إياها بجريمة المساس بأنظمة المعالجة الآلية للمعطيات وتتمحور خصائص هذه الجريمة بالدرجة الأولى في أنها جرائم عابرة للحدود فمسرحة الجريمة لم يعد محليا بل أصبح عالميا بالإضافة إلى صعوبة اكتشاف وإثبات الجرائم الإلكترونية بحيث انها تتطلب وسائل خاصة في الحاسب الآلي وشبكة الانترنت، أضف إلى ذلك أنها جرائم تتطلب خبرة وتحكم في التكنولوجيا المعلوماتية عند متابعتها، أما آخر خاصية في أن هذه الجرائم تعد اقل عنف من الجرائم التقليدية. ولم تكتف التشريعات المقارنة والتشريع الجزائري بتجريم الجريمة الإلكترونية بما فيها الجريمة المنظمة من خلال قانون العقوبات وقانون الإجراءات المدنية والإدارية والقوانين الخاصة والمتعلقة بها، بل أقرت أجهزة خاصة لمتابعة هذه الجريمة كالمخابرات المركزية بالولايات المتحدة الأمريكية والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

بأحدث الطرق العلمية المتطورة وأخيرا ما يمكن قوله في هذا المقام أن الجريمة الالكترونية وطرق ارتكابها مهما تمت مكافحتها فهي متطورة بتطور وسائل التكنولوجيا.

الكلمات الدالة:

الجريمة المنظمة، المجرم المعلوماتي، الجريمة الإلكترونية، الثورة التكنولوجية

La cybercriminalité dans l'environnement numérique et son impact sur la criminalité organisée transnationale

Ghania abbas

Resume:

La cybercriminalité a traversé plusieurs étapes différentes, atteignant un niveau élevé de développement grâce aux avancées technologiques. Avec cette évolution et ces changements, il est devenu difficile pour les législations de parvenir à une définition consensuelle. Les définitions ont oscillé entre celles qui se basent sur le sujet de la criminalité et celles qui s'appuient sur les moyens utilisés pour la commettre. Cependant, les législations n'ont pas tardé à lutter contre ce phénomène en utilisant les méthodes les plus récentes. Quant au législateur algérien, il a abordé la question de la cybercriminalité en la qualifiant de crime portant atteinte aux systèmes de traitement automatisé des données. Les caractéristiques principales de cette criminalité résident dans le fait qu'il s'agit principalement de crimes transnationaux, car le lieu du crime n'est plus localisé mais devient mondial. De plus, il est difficile de détecter et de prouver les crimes électroniques, car cela nécessite des moyens spécifiques en informatique et en réseau internet. En outre, ces crimes nécessitent une expertise et une maîtrise des technologies de l'information lors de leur suivi. Enfin, une dernière caractéristique de ces crimes est qu'ils sont moins violents que les crimes traditionnels. Les législations comparées, ainsi que la législation algérienne, ne se contentent pas de criminaliser la cybercriminalité, y compris la criminalité organisée, à travers le Code pénal, le Code de procédure civile et administrative, et les lois spécifiques y afférentes, mais elles ont également mis en place des organismes spéciaux pour suivre ces crimes, tels que la CIA aux États-Unis et l'Autorité nationale de

prévention des crimes liés aux technologies de l'information et de la communication, utilisant les méthodes scientifiques les plus avancées. Enfin, il est important de souligner que la cybercriminalité et ses modes de commission, quelle que soit leur lutte, continuent de se développer avec les progrès des technologies.

Mots-clés : Criminalité organisée, criminel informatique, cybercriminalité, révolution technologique.

Cybercrime in the Digital Environment and Its Impact on Transnational Organized Crime.

Ghania Abbas

Summary :

Cybercrime has gone through various stages of development and reached a highly sophisticated degree due to technological progress. this evolution of technology and its changing nature have made it difficult for legislations to agree on a common definition of the concept; the definitions range from those focusing on the object of the crime to those having for focus its means, however, all stress the need to fight cybercrimes with the most sophisticated means. for the Algerian lawmaker, it is defined as " a crime of violating automatic information processing systems".

Cybercrime has its distinct characteristics. In the first place, it has a across-borders scope; its reach is no longer confined to a territorial area but has become global. Furthermore, detection and provision of evidence of cybercrimes proves also to be challenging because of the special computer and internet equipment that is required. In addition, monitoring and tracking cybercrimes necessitates special expertise in information technology. Lastly, these crimes are less violent than traditional crimes. And it should be noted that compared legislations and the Algerian legislation have not only criminalized cybercrimes including organized crime through criminal codes

and codes of civil procedures and related laws, but have also set up special agencies to monitor this kind of crimes such as the CIA in the USA and the National Agency for the Prevention of Information and Communication related Crimes and have endowed them with the most advanced technological means. To conclude, we may say that whatever efforts are made into fighting cybercrime, it will always evolve as technology evolves

Key Words:

Organize Crime, Technological Revolution, Informational Criminal, Electronic Crime

مقدمة:

تعد الثورة التكنولوجية وخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم حتى أصبح مثلما قال الباحث فرانسوا جين الإنسان: "اليوم يملك سعة إرسال واستقبال المعلومات والأصوات بشكل خيالي"⁽¹⁾.

إذ تعتبر ثورة الاصلاحات هي المحرك الأساسي في التطورات الحادثة في الوقت الحالي إلا أنها ليست المحرك الوحيد في هذا التطور، حيث أن التطور الكبير في تكنولوجيا الحاسبات قد أسهم بصورة كبيرة في تسارع معدلات التقدم في مجال الاتصالات والمعلومات . وقد كان من نتاج التطور في الجانبين ظهور أدوات واختراعات وخدمات جديدة في مختلف المجالات، نتج عن ثورة التكنولوجية تلك ظهور نوع جديد من المعاملات سمي بالمعاملات الالكترونية وهي تختلف عن المعاملات التقليدية التي نعرفها من حيث البيئة التي تتم فيها هذه المعاملات، ونقصد بالمعاملات الالكترونية التي تتم عبر تجهيزات الكترونية مثل الهاتف والفاكس، وأجهزة الحواسيب وشبكة الانترنت ومؤخرا عن طريق الهاتف المحمول، وتتكون هذه المعاملات من عدد المكونات

الأساسية والذي يهتما في هذه المقال طرح مكون أساسي فيها وهو الجزء الخاص لجرائم تلك المعاملات ونذكر بالأخص الجريمة المنظمة"أو بمعنى أدق القواعد القانونية الجنائية التي تحكم الأفعال التي تتم من خلال أجهزة الحواسب أو عبر شبكة الانترنت وبالتالي فجرائم الكمبيوتر والانترنت أو ما يسمى Cyber Crimes، هي ظواهر إجرامية تفرع أجراس الخطر لتوعية مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة الكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية مما يسبب خطر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية، فإذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أنه هناك دولا عربية كثيرة أضحت مهتمة بتلك الظواهر، ومفهومها القانوني وسمات المجرم المعلوماتي، ومدى تأثيرها على الجريمة المنظمة، وهو ما سوف نحاول أن نتعرض له بشيء من التفصيل في هذا المقال محاولين أن نضع ولو في حلة صغيرة تعريف الجريمة الالكترونية، مراحل تطورها، ومدى تأثيرها على الجريمة المنظمة.

فعلى أساس ما سبق ذكره نطرح الإشكالية التالية:

ما المقصود بالجريمة الالكترونية؟ وما مدى تأثيرها على الجريمة المنظمة؟

ومن تم تتفرع عنها مجموعة من التساؤلات كالاتي:

- ما تعريف الجريمة الالكترونية؟

- ما هي خصائص الجريمة الالكترونية؟

- ما موقف المشرع الجزائري من الجريمة الالكترونية؟ وفيما تتمثل المراحل التي مرت بها الجريمة

الالكترونية؟

وأخيرا ما مدى تأثير الجريمة الالكترونية على الجريمة المنظمة؟

ولقد إرتأينا إعتقاد المنهج الوصفي، والتحليل كأساس في البحث بالإضافة إلى الاستعانة بالمنهج المقارن كمنهج مساعد كلما اقتضت الضرورة ذلك.

وللإجابة على الإشكالية المطروحة وتماشيا مع العنوان المقترح، نتبع الخطة التالية لدراسة هذا الموضوع

حيث قسمناه إلى محورين:

I- مفهوم الجريمة الالكترونية

II- مدى تأثير الجريمة الالكترونية أو جرائم الانترنت على الجريمة المنظمة

I- مفهوم الجريمة الالكترونية

أصبحت الجريمة الالكترونية موضوعا واسعا، ورغم صعوبة إيجاد تعريف جامع مانع لها، إلا أن اجتهاد كل الفقهاء والباحثين أدى إلى عدة تعريفات لها وإن كانت قد تباينت تبعا لمحل إهتمام كل فئة، فمنهم من عرفها من الجانب التقني، والبعض الآخر من الجانب القانوني، ومن أجل مفهوم شامل للجريمة لا بد من تعريفها من كل الجوانب.

1- تعريف الجريمة الالكترونية

لقد عرف فقهاء القانون الجريمة الالكترونية من جوانب عدة كالآتي:

أ- تعريف الجريمة الالكترونية

- من الجانب التقني الفني

الجريمة الالكترونية عبارة عن نشاط إجرامي يستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كوسيلة أو هدف لتنفيذ الفعل الإجرامي، كما يعرفها البعض الآخر بأنها: "تعرف عبر مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها"⁽²⁾.

فقد انقسم أنصار تعريف الجريمة من الجانب التقني والفني، فالبعض استند إلى موضوع الجريمة والبعض الآخر إلى وسيلة الجريمة⁽³⁾.

– أهم التعريفات التي استندت على موضوع الجريمة

أنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"⁽⁴⁾.

كما عرفت بأنها: "كل سلوك غير مشروع أو غير مسموح به يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"⁽⁵⁾.

أو هي: " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"⁽⁶⁾.

أو هي: "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية، مثل تعديل الكمبيوتر أو اعتداء على المعلومات المخزنة في الحاسب الآلي بعد استغلالها لأمر شتى، بخلاف الهدف الذي جمعت لأجله"⁽⁷⁾.

– أهم التعريفات التي استندت على وسيلة الجريمة

إن أنصار هذا الاتجاه ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة، وبالتالي تعرف على أنها: "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"⁽⁸⁾.

كما تعرف بأنها: "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"⁽⁹⁾.

كما أطلق فقهاء القانون الجنائي على الجريمة الالكترونية "المجرم المعلوماتي وهو شخص الذي لديه مهارات تقنية ودراية بالتكتيك المستخدم في نظام الحاسب الآلي الالكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري، لتغيير المعلومات، أو لتقليد البرامج، أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه"⁽¹⁰⁾.

وأنها: "كل فعل أو إمتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"⁽¹¹⁾.

يعتبر هذا التعريف الرأي الراجح لتبنيه من قبل العديد من الباحثين والدارسين نظرا لشموليته، بحيث يعبر عن الطابع التقني، أو المميز الذي ينطوي تحته أبرصور الجريمة الالكترونية.

ب- من الجانب القانوني

تعرف بأنها: "مجموعة الأفعال والأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الاجرامي والثورة التكنولوجية"⁽¹²⁾.

وتعرف كذلك على أنها: "نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي"⁽¹³⁾.

كما أن هناك من عرفها كالأتي: "الجريمة التي يتم إرتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني"⁽¹⁴⁾.

أو هي: " الجرائم التي لا يلجأ مرتكبيها إلى العنف بتاتا في تنفيذ جرائمهم، وذلك بأنه ينتمي إلى إجرام -الحيلة-، فهو لا يلجأ إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدر من العناء للقيام به"⁽¹⁵⁾.

كما عرفها الفقيه: " الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"⁽¹⁶⁾

وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال.

كما عرفت بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية، والتي يمكن أن تكون جديرة بالعقاب" أما بالنسبة لبعض الفقه المصري، فهي تنشأ عن الاستخدام غير المشروع لتقنية المعلومات وتهدف إلى الاعتداء على الأموال، أو الأشياء المعنوية، وهناك فريق آخر يرى أن الجريمة المعلوماتية "هي عمل أو امتناع يأتي إضراراً بمكونات الحاسب، وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض له عقاباً".

كما عرفها آخرون بأنها "كل فعل إيجابي أو سلبي عمدي يؤدي إلى الاعتداء على تقنية المعلومات أي كان غرض الجاني"⁽¹⁷⁾

أما بالنسبة للتعريف الدولي للجريمة الالكترونية فتعتمد تعريفات الجريمة الالكترونية في الغالب على الغرض من استخدام هذا المصطلح، إذ هناك عدد محدود من الأفعال السرية والنزاهة وتوافر بيانات الكمبيوتر، أو أنظمتها تمثل جوهر الجريمة الالكترونية أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية، أو مال أو ضرر لما في ذلك أشكال الأفعال المتصلة بجريمة الهوية وجرائم محتويات الكمبيوتر.

فقد جاءت توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين المنعقد في فيينا سنة 2000.

تعريف الجريمة الالكترونية بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوبي والجريمة تلك تشتمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"⁽¹⁸⁾.

وعلى أساس ما سبق ذكره يصح القول: بالرغم من المجهودات المبذولة من طرف الفقهاء والباحثين إلا أنه ليس بالسهولة الوصول إلى التعاريف القانونية للمصطلح الكلي.

ج-موقف المشرع الجزائري من تعريف الجريمة الإلكترونية

لم يعرف المشرع الجزائري الجريمة الإلكترونية، وإنما تبنى للدلالة على الجريمة مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات"، معتبرا أن النظام المعلوماتي في حد ذاته وما تحتويه من مكونات غير مادية محلا للجريمة، ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحقيقه حتى يمكن توفر أركان الجريمة استنادا إلى قانون العقوبات الجزائري المعدل والمتمم، فلم يعرف المشرع الجزائري جرائم الانترنت بل اكتفى بالعقاب على بعض الأفعال، تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية بالمعطيات". (19)

د-خصائص الجريمة الإلكترونية

يمكن إجمال خصائص الجريمة الإلكترونية ضمن العناصر التالية:

- جريمة عالمية

بمعنى أنها تتعدى الحدود الجغرافية للدول فتعتبر الجرائم العابرة للقارات، لأنه مع انتشار شبكة الاتصالات العالمية والانترنت أمكننا ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر. (20)

-جرائم صعبة الإثبات

صعوبة متابعتها واكتشافها، بحيث لا تترك أثر، فهي مجرد أرقام تتغير في السجلات ومعظم الجرائم الإلكترونية تم اكتشافها بالصدفة، وبعد وقت طويل من ارتكابها ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها أساسا لأنها تقتصر إلى الدليل المادي التقليدي كالبصمات، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، هذا ما جعل مكتب التحقيقات الفيدرالي الأمريكي يطلق

عليها وصف الوباء EPIDÉMIE. (21)

كما يحتاج الكشف عن الجريمة الإلكترونية لخبرة فنية خاصة يتعذر على المحقق التقليدي التعامل معها، لأنها تعتمد غالباً على قمة الذكاء المصحوب بالخداع والتضليل بدس برامج أو وضع كلمات سرية ورموز مرتكبيها لتشفير المعلومات لمنع إيجاد أي دليل يدينه. (22)

- جرائم ناعمة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي لارتكابها كالقتل، السرقة وغيرها فالجرائم الإلكترونية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم والتفكير العلمي المدروس القائم على معرفة تقنية ممتازة بالحاسب الآلي والتعامل السليم بالشبكة على أساس أن الجاني في الجرائم الإلكترونية هو إنسان متوافق مع المجتمع ولكنه يقترب هذا النوع من الجرائم بدافع اللهو، أو لمجرد إظهار تفوقه على آلة الكمبيوتر، أو على البرامج التي يشتغل بها، وأكد لتحقيق مصلحة ما. (23)

- عدم التبليغ

عند وقوع الجريمة بواسطة الانترنت نجد أن المجني عليهم يمتنعون على إبلاغ السلطات المختصة خشية على السمعة والمكانة، وعدم اهتزاز الثقة في كفاءته خاصة إذا كان كياناً أو هيئة معنية، وقد اقترح في الولايات المتحدة الأمريكية بأن تفرض النصوص المتعلقة بجرائم الحاسوب التزاماً على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يقع عليها من جرائم متى وصل إلى علمهم، ذلك مع تقرير جزاء في حالة إخلالهم بهذا الالتزام. (24)

ومن ثمة فإن عملية الاعتراف نابعة من وجود العديد من المشكلات والصعوبات العملية والإجرائية التي تظهر عند ارتكاب أحد ما جريمة ما من جرائم تكنولوجيا المعلومات. (25)

2-مراحل تطور الجريمة الالكترونية وموقف المشرع الجزائري

أ- مراحل تطور الجريمة الالكترونية

أصبحت الجريمة الالكترونية تشكل هاجسا أمنيا واقتصاديا وسياسيا بل ومجتمعيًا، وذلك بفضل التطور اللافت والمتسارع لشبكة الانترنت، حيث يعد ذلك السبب الرئيسي في اتخاذها ووسيلة لتنفيذ العديد من الجرائم بعيدا عن أعين الجهات الأمنية ودون أدنى مجهود أو خوف من العقاب. وبالتالي مر تطور الجريمة المعلوماتية (الالكترونية) في ثلاث مراحل تبعا لتطور التقنية واستخدامات الحاسوب .

- المرحلة الأولى

بظهور واستخدام الكمبيوتر وروابط الشبكة في الستينيات إلى السبعينات، ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكلت موضوع للتساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أو ظاهرة مستجدة؟ وهل هي جرائم بالمعنى القانوني ام مجرد سلوكيات غير أخلاقية في مجال المعلوماتية فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني ومع توسيع الدراسات تدريجيا وخلال التسعينات بدا الحديث عنها كظاهرة إجرامية جديدة.⁽²⁶⁾

- المرحلة الثانية:

في بداية الثمانينات تأكد مفهوم جديد لجرائم الكمبيوتر والانترنت، حيث ارتبطت هذه الأخيرة بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدمير كلي للملفات أو البرامج وشاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم، وكذا المجرم المعلوماتي المتفوق⁽²⁷⁾.

-المرحلة الثالثة

حيث شهدت فترة التسعينيات تنامياً هائلاً في حقل الجرائم الإلكترونية، وتغيراً في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيلات لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة وخطيرة في ذات الوقت بحيث تطورت الانترنت بشكل مذهل خلال هذه الفترة، بعدما كانت مجرد شبكة أكاديمية صغيرة ثم تحولت إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان اهتمام ببناء الشبكة وتوسيع نشاطها دون مراعاة لتحديات أمن المعلومات فالاهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة، وهذه الثغرة التي شجعت من تنامي الجريمة الالكترونية وتسببت في أضرار بالغة، هو ما أدى إلى لفت النظر إلى حاجة شبكة الانترنت إلى توفير معايير من الأمن، وبدأ التفكير مالياً للثغرات ونقاط الضعف وعليه قد يكون الكمبيوتر هدف للجريمة وغايتها المعلومات المخزنة والسيطرة على النظام دون تصريح والسرقه واعتداء على الملكية الفكرية.....إلخ، كما قد يكون الكمبيوتر للاستيلاء على أملاك الغير لإجراء تحويلات غير شرعية، كما أن الكمبيوتر قد يعد أداة للجريمة كحالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر مواد غير قانونية. (28)

ب- موقف المشرع الجزائري من الجريمة الالكترونية

رغم صعوبة ضبط ومكافحة جرائم الانترنت على الصعيد الوطني، إلا أن هناك جهوداً معتبرة قام بها المشرع الجزائري في محاربة قرصنة الأنترنت وإحالتهم قانونياً على المحاكم متأثراً بجل الدول العربية التي وضعت قوانين لمكافحة جريمة الانترنت، فعلى امتداد الوطن العربي من المحيط إلى الخليج نجد ترسانة قانونية تنظم جرائم الانترنت، وبدأت هذه الحركة في الظهور والانتشار منذ بداية الألفية الثالثة وعلى الأخص منذ منتصف العشرية الأولى منها، ومن أهم الأمور التي أولاهها المشرع

الجزائري أهمية قصوى: أمن الدولة والحفاظ على النظام العام، كما أنه ركز كل اهتماماته على حماية الدولة وجعلها من أسمى أهدافه.

حاول المشرع الجزائري إصدار قوانين عامة وخاصة، هياكل وأجهزة للتصدي للجريمة الالكترونية ويعود أسباب الاهتمام بتنظيم جرائم الانترنت من جهة تطور تكنولوجيا الإعلام فأدى إلى اتساع نطاق الجريمة الالكترونية، حيث أصبحت لا تقتصر على جريمة واحدة وإنما اتسعت إلى عدت جرائم ترتكب عن طريق الهاتف وعن طريق الكمبيوتر، ولا ترتكب هذه الجريمة من طرف شخص طبيعي فقط بل تعدت إلى الشخص المعنوي، ومن جهة أخرى يكون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الالكترونية الحديثة، أضف إلى ذلك المحافظة على مبدأ الشرعية الجنائية متكلا على تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها، ومن بين هذه القوانين العامة الموضوعية المنظمة للجريمة الالكترونية ينص الدستور الجزائري لسنة 1996،⁽²⁹⁾ المعدل سنة 2016 في المواد 40،44،38،46 وغيرها. أضف إلى ذلك قانون العقوبات بموجب قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156،⁽³⁰⁾ المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 07. وفي عام 2006 أدخل المشرع الجزائري تعديلا آخر على قانون العقوبات بموجب قانون 06-23 المؤرخ في 20 ديسمبر 2006، حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع

ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة لتنشيط وسائل التكنولوجيا المعلومات وانتشار الانترنت كوسيلة لنقل المعلومات.

II - مدى تأثير جرائم الإنترنت على الجريمة المنظمة

خلال السنوات العشر الأخيرة نشط وتنامى حجم الجرائم الاليكترونية بشكل مذهل، وتحولت الشبكة العنكبوتية التي تظم تحتها ملايين المستخدمين من وسيلة تحصيل المعلومات، أو وسيلة بحث أكاديمي إلى بيئة متكاملة لاستثمار والعمل والإنتاج والحصول على المعلومات بل أداة وبيئة خصبة لذلك النوع من الجرائم ونذكر بالأخص الجرائم المنظمة

1- جرائم تقع بواسطة لانتريت

أي أن الشبكة تكون أداة إيجابية لارتكاب الجريمة فتسهل للمجرم المعلوماتي تحقيق غايته ونلاحظ أن أغلب صورها في هذه الحالة تشكل الجرائم الواقعة على الأشخاص.

أ- الجرائم المنظمة

الجرائم المنظمة هي عنف منظم قصد الحصول على مكاسب مالية بطرق وأساليب غير مشروعة وتمارس الجريمة المنظمة على شكل نصب واحتيال وتزوير وسطو وخطف من أجل الابتزاز والقتل... الخ إلا أنها تختلف عن الجرائم المعروفة كونها تنفذ بعد تدبير وتنظيم، لذا سميت "بالجريمة المنظمة" ويشير مصطلح الجريمة المنظمة إلى جماعات ترتكب أفعالاً تخرق بها القانون للحصول على مساعدات مادية كما تهتم بالابتزاز والخداع والإنتاج والتوزيع غير القانوني لإدمان المخدرات، والتعامل مع السلع الممنوعة مثل الأسلحة غير القانونية. (31)

من خلال التعريف يتبين أن الجريمة المنظمة تمتاز بخاصيتين أساسيتين أولهما التنظيم وثانيهما الكسب المادي.

ب- أبعاد الجريمة الإلكترونية في التأثير على الجرائم المنظمة.

لقد أضافت الجريمة المنظمة عبر الحدود الوطنية بعدا سلبيا للعولمة مع غيرها من السلبيات الاقتصادية التي كانت أثارها سلبية على الدول النامية، فلقد أصبح الفساد أداة من الأدوات المفضلة للجريمة المنظمة بل جزءا لا يتجزأ من إستراتيجيتها، وذلك باعتبار أن المال الفاسد نوع من الاستثمار الناجح للجماعات الإجرامية المنظمة حيث يزيد من فرص نجاح جرائمهم ويقلل من ملاحقتهم والقبض عليهم ومحاكمتهم. (32)

ومن المعروف أن الحالة الراهنة لإنقاذ القانون يجب أن تخضع لتغيرات كبيرة للتعامل مع خطر الجريمة الإلكترونية، فكثير من العلماء والممارسون يحاولون إقامة نجاحات جديدة في التعامل مع الجريمة، نشير إلى أكبر تحدي للقانون الدولي فهو بتقيد الجريمة الإلكترونية العابرة للوطنية "فكر عالميا، وأعمل محليا". (33)

2- الجهود التي قامت بها الجزائر في مكافحة الجريمة المنظمة وضرورة التعاون الدولي.**أ- الجهود التي قامت بها الجزائر في مكافحة الجريمة المنظمة**

التصديق على المعاهدات والاتفاقيات والبروتوكولات الخاصة بقمع الجريمة المنظمة والتي كانت على النحو التالي:

- التصديق على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بموجب المرسوم الرئاسي رقم 55-22 المؤرخ في 05/02/2002 المنشور بالجريدة الرسمية العدد 09 سنة 2002 الصادر بتاريخ 10/02/2002.

- التصديق على البرتوكول الخاص بمكافحة تهريب المهاجرين عن طريق البر والبحر والجو بموجب المرسوم الرئاسي 06-2003 الصادر في 12/11/2003.

ب- إدماج القواعد الخاصة بالجريمة المنظمة في القانون الداخلي:

- القانون رقم 05/01 المؤرخ في 06/02/2005 المتعلق بتبييض الأموال وتمويل الإرهاب ومكافحتهما.
- لقد ربط هذا القانون بين تبييض الأموال العائدة من أفعال إجرامية والأفعال الإرهابية وأوجد آليات للرقابة على حركة الأموال ووضع عقوبات بموجب المواد 31-34 لقمع هذه الجريمة ووضع آليات للتعاون الدولي في هذا الشأن.
- القانون رقم 05/17 المؤرخ في 23/07/2005 المتعلق بمكافحة التهريب واهم ما جاء فيه تجريم تهريب الأسلحة (المادة 14 منه).
- تجريم التهريب مع حمل السلاح ناري (المادة 13).
- تجريم الشخص المعنوي الذي يقوم بأفعال التهريب (المادة 24).
- توجد آلية تسمى التعاون العابر للحدود بقصد تعاون الدول المجاورة لقمع هذه الجريمة.
- القانون رقم 06/01 المؤرخ في 20/02/2006 المتعلق بالوقاية من الفساد ومكافحته.
- وقد تضمن 23 جريمة كلها تصب في مصب الجرائم العابرة.
- بالإضافة إلى استحداث آليات دولية لمكافحة الفساد.
- تجريم الشخص المعنوي القائم بعملية الفساد.
- التعديلات التي أدخلت على قانون الاجراءات الجزائية:
- التعديلات التي جاءت في القانون 14 (04 المادة 29) (تمديد الإختصاص لوكيل الجمهورية بخصوص الجرائم...الجريمة العابرة).
- المادة 40 تمديد الاختصاص لقاضي التحقيق بخصوص الجريمة نفسها.
- المواد 65 مكرر 65 الى مكرر 04 (المتابعة الجزائية للشخص المعنوي).

- التعديلات التي جاءت في القانون 06/22
- تمديد اختصاص ضباط الشرطة القضائية في الجرائم المذكورة إلى كامل التراب الوطني (المادة 16).

- جواز التفتيش ليلا ونهارا بخصوص هذه الجرائم (المادة 47).
- آجال التوقيف للنظر 48 ساعة يجوز تمديدها 3مرات
- جواز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.
- تبني نظام التسرب

ج-التعديلات الواردة في قانون العقوبات:

- التعديلات الواردة في قانون العقوبات 04/15 أهمها:
- المسؤولية الجزائية للشخص المعنوي (المادة 51 مكرر).
- العقوبات المنطبقة على الشخص المعنوي (المادة 27).
- تعديل المواد (176-182) والمتعلقة بتكوين جمعيات الأشرار ومساعدة المجرمين.
- تجريم المساس بأنظمة المعالجة الآلية للمعطيات رقم 394-394 مكرر 7
- التعديلات الواردة في القانون 06/23 التنصيص على تحريم تبييض الأموال (المادة 389 مكرر الى 389 مكرر 02).⁽³⁴⁾

د-ضرورة التعاون الدولي:

بناء على ما سبق ذكره لا بد من ان يكون تعاون دولي يتفق مع طبيعة هذه الجرائم، والتي تتميز بطابع خاص، يقتضي أن تكون هناك إجراءات تحقيقية سريعة، وسيسمح هذا التعاون الدولي بسهولة الاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجريمة المتعلقة بالإنترنت والحاسوب وتعميمها⁽³⁵⁾، والدولة بمفردها

لا تستطيع القضاء على هذه الجرائم لأنها عابرة للحدود الوطنية، لذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل فيما بينها لضبط المجرمين، ومكافحة هذه الجرائم، وقد تبلور هذا النوع من التعاون الدولي في إنشاء المنظمة الدولية للشرطة الجنائية (Interpol).⁽³⁶⁾ وتتولى المنظمة الدولية للشرطة الجنائية (Interpol) إقامة العلاقات بين الدول المنظمة وتبادل المعلومات بي سلطات التحقق فيما يتعلق بجرائم المعلوماتية وخاصة بالنسبة للجرائم المتشعبة في عدة دول، ومنها جرائم الانترنت وقد أنشأ المجلس الأوروبي في عام 1991 شرطة أوروبية يختص بملاحظة الجرائم العابرة للحدود.⁽³⁷⁾

الخاتمة:

إن الجرائم الالكترونية ظاهرة بالغة الخطورة وإن احتمال تعرض الأشخاص أو المؤسسات لجريمة إلكترونية صارت مرتفعة جدا، ذلك أن حجم الجريمة الإلكترونية في تزايد مستمر، وعمق تأثيرها السلبي على المجتمع في تزايد مستمر هو الآخر. ولقد أثارت هذه الجرائم تساؤلات كثيرة، نظرا لجسامتها وأخطارها وخسائرها الفادحة وسرعة انتشارها، حيث أصبح التعامل مع صور هذه الجرائم موضع اهتمام الجميع، والإحساس بأن الكل معني بشكل أو بآخر بأخطار وعواقب الجرائم الالكترونية، ورغم وجود هذه النصوص القانونية، فإنها لم تضع حد للأفعال المجرمة، لأسباب ترجع تارة أن رجال العدالة لم يتعودوا بعد على تطبيق مثل هذه النصوص، وأن النصوص القانونية في حد ذاتها لا تلم بجميع الجرائم الالكترونية بالإضافة إلى ندرة القضايا المعروضة قضائيا في هذا المجال سواء بسبب استغلال الفراغ القانوني في هذا المجال، أو بما أن الجريمة هي تقنية محضة، فيمكن تجاوزها تقنيا أيضا بدون ترك دليل مادي يثبتها. فجرائم الحاسوب والانترنت هي جرائم عابرة للحدود، وقد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة واحدة يقع ضحيتها عدد من الأفراد يقيمون في دول مختلفة، فتظهر مشكلة التعارض والاختلاف بين التشريعات الإجرائية في دول العالم، ومنها اختلاف الجهات المختصة بالتفتيش والشروط الإجراءات ومكافحة جرائم المعلوماتية تتقضي إذن توحيد التشريعات الإجرائية من ناحية، وأن تكون نظام الإثبات بالدليل الالكتروني واحدا بين الدول التي تقع فيها هذه الجرائم، وهذا

أمر مستحيل تحقيقه، وعليه فصدور قوانين خاصة بالجرائم الإلكترونية والردع القانوني هو من أهم الحلول لمواجهة الظاهرة ذلك أنه ما تم خلقه تقنيا يمكن تجاوزه تقنيا أيضا، فيبقى الجزاء القانوني هو الحل الوحيد للقضاء على هذه الظاهرة التي استغللت بشكل ملحوظ.

بعض الاقتراحات:

- ضرورة تدريب وتأهيل أفراد الضبطية القضائية من العاملين من الإدعاء العام (النيابة) والقضاء على كيفية التعامل مع هذا النوع من الإجرام وتحقيق التعاون مع التقنيين من أصحاب الخبرة، وذلك بعقد دورات تدريبية بشكل دوري ودائم للاستفادة من خبراتهم وإرشاداتهم ابتداءً من مرحلة الاستدلال وجمع الأدلة وانتهاء بقرارات المحاكم.
- التطور المستمر للتشريعات القائمة بما يحقق مرونتها ومواكبتها بالتطورات المتسارعة في مجال تكنولوجيا المعلومات
- تفعيل دورة الأسرة في متابعة الأبناء لوقايتهم من الآثار السلبية والمخاطر المترتبة عن الاستخدام الغير الآمن لشبكات الأنترنت.
- ضرورة التعاون الدولي لمواجهة الإجرام في البيئة الرقمية الإلكترونية وذلك من خلال الدخول في إتفاقيات ومعاهدات تجرم صورة هذه الجرائم وتبين كذلك الاختصاص المحلي في حالة وقوعها، كما يمكن أن تنص هذه الإتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بالجرائم الإلكترونية، وهذا ما يجب أن يحدث بالنسبة للجزائر، وضرورة إنضمامها لاتفاقية بودا بست 2001 لمكافحة الجريمة المعلوماتية.

قائمة الهوامش و المراجع

- (1) محمد لعقاب، المواطن الرقمي، كيف ساعدت تكنولوجيا المعلومات الثورات العربية، الطبعة الأولى، دار هومة، الجزائر، 2011، ص 32.
- (2) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر 2006، ص ص 01 - 02.
- (3) المرجع نفسه، ص ص 01 - 02.
- (4) هشام محمد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994، ص 31.
- (5) هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص 20.
- (6) هشام محمد رستم، مرجع سابق، ص 31.

(7) محمود أحمد عابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009، ص 72.

(8) TOM FORESTER. ESSENTIAL PROBLEMS TO HIGH-TECH SOCIETY FIRST MIT PRES, EDITION 3 CAMBRIDGE MASSACHUSETTS (7) 1989 P 104

(9) هشام محمد رستم، مرجع سابق، ص ص 29-30.

(10) هدى حامد قشقوش، مرجع سابق، ص 22.

(11) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، (دون دار النشر) القاهرة، 2009، ص 143.

(12) فضيلة عاقل، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب مؤتمر الجرائم الالكترونية المنعقد في طرابلس/ لبنان ليومي 24-25/03/2017، تاريخ النشر 2017/04/10.

(13) عبد الفتاح بيومي حجازي، مرجع سابق، ص 66.

(14) محمد عادل ريان، جرائم الحاسب الآلي (أمن البيانات)، (د.د.ن) بيروت، 2003، ص 03.

(15) أيمن رسلان، جرائم المعلوماتية والإنترنت بين العالم الافتراضي والواقع بالتطبيق على مصر والوطن العربي، (د.د.ن)، القاهرة، 2012، ص 46-47.

(16) محمد عادل ريان، مرجع سابق، ص 18.

(17) أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية 2009، ص 106.

(18) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2011، ص 30.

(19) قانون رقم 15/04 المؤرخ في 2014/11/10 يتضمن قانون العقوبات.

(20) عبد الفتاح مراد، التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، مصر 2006، ص 42. مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد 21، جوان 2012، ص 16.

(21) مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد 21، جوان 2012، ص 16.

(22) هشام محمد رستم، الجرائم المعلوماتية وأصول التحقيق الجنائي الفني، مجلة الأمن والقانون، العدد 2، دبي، 1999، ص 24.

(23) عبد الفتاح مراد، مرجع سابق، ص 46.

(24) منى الأشقر، القانون والإنترنت تحدي التكيف والضبط، بيروت، الناشر ش.م.م، 2008، ص 70 وما بعدها.

(25) جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البداية للنشر والتوزيع، عمان، 2007، ص 220.

01-02. ص عبد الفتاح بيومي حجازي، مرجع سابق، ص (26)

(27) فضيلة عاقل، مرجع سابق.

(28) منى الأشقر، مرجع سابق، ص 70.

(29) المرسوم الرئاسي رقم 96-438 المؤرخ في 7 ديسمبر سنة 1996، والذي يتعلق بإصدار نص تعديل الدستور

المصادق عليه في استفتاء 28 نوفمبر سنة 1996. في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية (ج)، ر 76

ل8 ديسمبر 1996) المعدل والمتمم بالقانون رقم 16-01 المؤرخ في 6 مارس سنة 2016 (ج، ر 14 ل 07 مارس 2016) المعدل والمتمم.

(³⁰) الأمر رقم 66-156 مؤرخ في 8 يونيو 1996 (ج، ر 49 مؤرخة في (11_06_1996)، معدل ومتمم بالقانون رقم 09-01 مؤرخ في 29 صفر عام 1430، الموافق ل 25 فبراير سنة 2009 (ج، ر 15 مؤرخة في 08_03_2009) المعدل والمتمم.

(³¹) نصيرة تامي، الإعلام الفضائي والإرهاب، الطبعة الأولى، دار أسامة للنشر والتوزيع، الأردن، عمان، 2015، ص 87.

(³²) السيد عوض، التطور التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون: قضايا السكان والتنمية من 19_22 ديسمبر 2004م، المركز الديمغرافي بالقاهرة، ص10.

(³³) (Chris E. Marshall et des autres:hand book of:transnational crime a justice computer crime in a brave New World ،sage publication, 2005, p11)

(³⁴) أمل المرشدي، الجريمة المنظمة العابرة للحدود الوطنية يوم 23 أكتوبر 2016 من الموقع استشارات قانونية [HTTPS://WWW.MOHAMAH.NET](https://www.mohamah.net)

(³⁵) عبد الفتاح بيومي حجازي، مرجع سابق، ص 102 وما بعدها.

(³⁶) علي حسن الطالبة، التعاون القضائي الدولي في مجال مكافحة الجرائم الإلكترونية، مركز الإعلام الأمني.

(³⁷) جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2006، ص ص 87_79.