حقيقة الجريمة المعلوماتية والأساليب التشريعية لمواجهتها

The Reality of cybercrimes and Legislative Ways to Counter It

جنادي عبد الحق*

مخبر الدراسات القانونية المقارنة

كلية الحقوق والعلوم السياسية، جامعة سعيدة د/ الطاهر مولاي، الجزائر

abdelhak.janadi@univ-saida.dz

هيشور أحمد

مخبر الدراسات القانونية المقارنة

كلية الحقوق و العلوم السياسية، جامعة سعيدة د/ الطاهر مولاي، الجزائر

ahmed.hichour@univ-saida.dz

تاريخ الاستلام: 01 / 12/ 2021 تاريخ القبول: 30 / 05/ 2022 تاريخ النشر: 06 / 06/ 2022

الملخص:

تطورت الجرائم التقليدية و اتخذت صورا حديثة، و هذا راجع لتطور صور و أساليب ارتكابها ، اذ نجد ان الجرائم الالكترونية أصبحت تتميز بخصوصية في طرق و وسائل ارتكابها، إضافة الى خصوصيات يتميز بها مرتكبيها، و هو ما نتج عنه صعوبة في عملية تقصي و اثبات هذه الجرائم، و كذا صعوبة معالجة هذا النوع من الجرائم من الناحية القانونية في شقها الموضوعي او الاجرائي، و هو الامر الذي دفع بالكثير من

* المؤلف المرسل

الدول الى الوقوف من اجل سن قوانين من شأنها الحد من ارتكاب هذه الجرائم و مواكبة التطور الذي تتميز به.

الكلمات المفتاحية: صعوبات التحقيق، الإثبات، الجرائم المعلوماتية، أساليب مواجهتها.

Abstract:

Traditional crimes have Evolved and reproduced modern ways, through the development of ways and methods to commit them. We find that cybercrimes, are characterized by the protection of privacy in the ways and means of committing them, as well, as by the particular characteristics of the perpetrators. It has therefore been difficult to investigate and establish these crimes, as well as to treat them legally in their substantive or procedural aspects.

المقدمة

ظهر نوع جديد من الجرائم يسمى بـ" الجرائم المعلوماتية" ، و التي تعتبر اكثر خطورة و فتكا من الجرائم التقليدية، بل أصبحت الجريمة المعلوماتية تشكل تهديدا حقيقيا سواء على الأفراد أو المجتمعات و الدول في كل المجالات، و ذلك راجع لكون الجناة على قدر كبير من المعرفة الفنية ببرامج الحاسب الآلي؛ حيث ترتكب هذه جرائم دون ترك آثار و الذي ينتج عنه صعوبة الحصول على دليل الجريمة، كما شغلت الجرائم المعلوماتية بال الحكومات العربية و الغربية لأن هذا النوع من الجرائم يصعب التحقيق فيه و إثباته ،رغم من ذلك بذلت العديد من الدول الغربية و الدول العربية ، جهودا كبيرة لمكافحة هذا النوع الخطير من الإجرام ،على هذا الأساس سنحاول التطرق

إلى الصعوبات التي تعترض عملية التحقيق و إثبات الجريمة المعلوماتية ، من خلال الوسائل القانونية المتاحة بالإضافة إلى أساليب التحقيق القانونية، و منه عرض بعض التجارب للدول الرائدة في هذا المجال مثل الولايات المتحدة الأمريكية و فرنسا، أما على صعيد الدول العربية سنحاول استعراض التجربة السعودية و الجزائرية في هذا المجال. و عليه فإن موضوع بحثنا هذا يطرح الإشكالية التالية :

ما المقصود بالجريمة الالكترونية و فيما تتمثل الخصوصية التي تتمتع بها، و ما هي الصعوبات المترتبة عنها فيما يخص الاثبات ، و كيف قامت التشريعات بمعالجة هذا النوع من الجرائم ؟

و عليه ارتأينا اتباع المنهج التحليلي في عملية دراستنا لهذه الإشكالية وفقا للخطة التالية:

تقسم الدراسة كالتالي:

تطرقنا في المبحث الأول الى خصوصية الجريمة الالكترونية، اما المبحث الثاني تمم تخصيصه لمعالجة الجريمة الالكترونية في بعض التشريعات الداخلية.

المبحث الأول: خصوصية الجريمة الالكترونية

سنتطرق في المطلب الأول الى مفهوم بالجريمة المعلوماتية، اما المطلب الثاني فسيتم التطرق فيه الى الصعوبات والتحديات التي تواجه نظم التحقيق و أدلة الإثبات في التشريعات الوطنية.

المطلب الأول: مفهوم بالجريمة المعلوماتية

لدراسة مفهوم الجريمة الالكترونية يتطلب منا تقسيم المبحث الى فرعين، حيث سيتم التطرق الى تعريف الجريمة المعلوماتية في الفرع الأول، و يخصص الفرع الثاني الى خصائص الجريمة المعلوماتية.

الفرع الاول: تعريف الجريمة المعلوماتية

استعمل مصطلح المعلوماتية لأول مرة من طرف (A.I. MIKLAILOV) مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفيتي سابقا، وبعدها ذاع استعمال المصطلح على نحو عالمي بشكل واسع حتى أحصى له البعض ثلاثين تعريفا مختلفا في الكتابات المتخصصة في علم المعلومات[1].

وصفها الدكتور محمد صالح العدلي، أستاذ القانون الجنائي بكلية الحقوق بمسقط وجامعة الأزهر بمصر بقوله: « الجريمة الإلكترونية هي الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة، ولا تستطيع العولمة أن تصرفه بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيا المعلومات.»[2].

تعرف الجريمة المعلوماتية من منظور منظمة التعاون الاقتصادي والتنمية بأنها: « كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عبر تدخل التقنية المعلوماتية». كما عرفها مكتب المحاسبة العام في الولايات المتحدة الأمريكية بأنها تلك الأفعال العمدية التي تسبب خسائر للحكومة أو مكاسب للأفراد، والمرتبطة بتصميم أو استخدام أو تشغيل النظام الذي تقع هذه الأفعال في نطاقه[3].

من الناحية القانونية تعرف الجريمة المعلوماتية بأنها: «كل عمل أو امتناع عن عمل أتاه الإنسان إضرارا بمكونات الحاسب الآلي المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي يحميها قانون العقوبات.» أما الأستاذ (MASS) فقد عرفها بأنها: «تلك الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بهدف تحقيق الربح» [4].

بالنسبة للمشرع الجزائري فقد نص في المادة 394 مكرر إلى 394 مكرر7 من قانون العقوبات الصادر عام 2006 على جريمة المساس بأنظمة المعالجة الآلية للمعطيات والبيانات وتتعلق بارتكاب أحد الأفعال التالية بعقوبات متفاوتة:

أولاً: الإدخال أو الإبقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة القيام بذاك.

ثانياً: تخريب نظم أشغال المنظومة.

ثالثاً: القيام عمدا وبطريق الغش بتصميم، أو بحث، أو تجميع، أو توفير، أو نشر، أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

رابعاً: حيازة، أو إفشاء، أو نشر، أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. و الملاحظ أن المشرع الجزائري قد أعطى وصف الجرائم المعلوماتية الجنحة وليس الجناية، غير أنه يعاقب على الشروع فيها بنص صريح ورد في المادة 394 مكرر 7.

الفرع الثاني: خصائص الجريمة المعلوماتية

تمتاز الجريمة المنظمة بميزات وخصائص تميزها عن غيرها من الجرائم التقليدية، وتتمثل خصائص الجريمة المعلوماتية فيما يلي:

أولاً: خطورة الجريمة المعلوماتية: حيث تمس الحياة الخاصة للإنسان، كما أنها تمس أمن ولاسيما منها المؤسسات العامة والخاصة منها البنوك والمصارف التي أصبحت مستهدفة معلوماتيا كما أنها تستهدف أمن الدول وتمس باقتصادها، وقد يصل الأمر إلى التأثير على الجانب السياسي فيها، وذلك عندما يتم تسريب البيانات والمعلومات الخاصة بها ونشرها أو تخريب أنظمة تشغيل المعلومات الخاصة بها.

ثانياً: عالمية الجريمة المعلوماتية "جرائم عابرة للحدود الوطنية" : لم تعد الجريمة المعلوماتية جريمة وطنية، بل تعدت الأوطان للتجاوز حتى القارات، ويعود السبب في هذا إلى انتشار شبكة الاتصالات العالمية " الانترنت "، بحيث أصبحت الحواسيب في كل أرجاء العالم مربوطة بهذه الشبكة، وبالتالي يمكن للجاني أن يكون من جنسية دولة ما، ويرتكب جريمة إلكترونية باستعمال حاسب آلي في دولة أخرى قصد إحداث ضرر في دولة ثالثة، وبهذا تقع الجرائم في أغلب الأحيان عبر حدود دولية[5].

ثالثاً: صعوبة إثباتها: على عكس الجرائم التقليدية التي يترك فيها الجاني دليل للوصول إليه أو عن طريق التحقيق والتحري يمكن الوصول إلى حل لغز الجريمة، والوصول والقبض على مرتكبيها فالجريمة الإلكترونية صعبة الإثبات لأنها لا تترك دليلا

خارجيا، حيث أن هذه الجرائم ما هي في حقيقتها إلا نبضات إلكترونية، فإن هذا الشكل عقبة كأداة أمام اكتشافها، وأمام التعرف على مرتكبيها، ولاسيما أن هناك صعوبة في تعقب آثار تلك الجرائم وتعقب مرتكبيها[8]، كما ترجع صعوبة إثباتها لأسباب أخرى نذكر منها:

- أنها جريمة لا تترك أثرا بعد ارتكابها.
- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- أنها تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.
- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
- أنها تعتمد على قمة الذكاء في ارتكابها، فالمجرم على قدر كبير من المعرفة الفنية ومن الذكاء[6].

رابعاً: جرائم لا تعتمد على العنف: على عكس الجريمة التقليدية التي تحتاج إلى جهد بدني في ارتكابها مثل السرقة والاغتصاب، فإن الجرائم المعلوماتية توصف بالجرائم الناعمة، أو جرائم الذكاء، بحيث أنها تقوم على الدراسة الذهنية والتفكير العلمي المدروس القائم على دراية ومعرفة كبيرة بالحاسب الآلي كما أن أغلب المجرمين ذوي مستوى تعليمي عالي[7].

خامساً: جرائم تعتمد على وجود الحاسب الآلي وعلى معرفة جيدة بأنظمة التشغيل وتقنيات المعلومات، كما أن الأشخاص مرتكبيها فهم أشخاص من ذوي الخبرة والذكاء في هذا المجال.

المطلب الثاني: الصعوبات و التحديات التي تواجه نظم التحقيق و أدلة الإثبات في التشريعات الوطنية

للقيام بعملية دراسة هذا المطلب فقد تم تخصيص الفرع الأول من هذا المطلب الى مشكلة عدم ظهور الدليل المادي، اما الفرع الثاني فسيتم التطرق فيه الى نقص الخبرة في عملية تتبع الجريمة وتحديد طرق ووسائل وزمان ارتكابها.

الفرع الأول: عدم ظهور الدليل المادي

يعتبر عالم الشبكة العنكبوتية عالم افتراضي، وبالتالي فيمكن بضغطة زر تغيير الكثير من المعلومات في وقت قصير، فيصعب استخلاص الدليل المادي لهذه الجريمة، لأنه بكل بساطة في عالم غير واقعي.

وبالإضافة إلى هذا فيعمل المجرم على التخطيط الجيد من أجل عدم ترك دليل مادي حتى وإن تركه، فإنه بإمكانه العودة مرة ثانية ومحوه قبل وصول يد القضاء إليه[8].

الفرع الثاني: نقص الخبرة في تتبع الجريمة وتحديد طرق ووسائل وزمان ارتكابها

إن وتيرة ارتكاب الجريمة المعلوماتية سريعة جدا، كما أن المجرمين على قدر كبير من الذكاء والمعرفة الفنية بالحاسب الآلي، الأمر الذي لا يتوافر لدى المحققين، مما يضعنا أمام أجهزة غير متكافئة[9]، وقد وصل ببعض مجرمي المعلوماتية الإطلاق على أنفسهم اسم النخبة، أما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء.

في دراسة أجريت في إنجلترا عام 1986، والتي شملت 195 حالة من حالات الاحتيال لاختلاس المال عن طريق الحاسب الآلي، 15 % منه قد تم اكتشافها مصادفة، في حين أن 15 % منها قد تم اكتشافه نتيجة يقظة المدققين، والمراجعين الداخلين والخارجين حيال قيامهم بأعمال التدقيق الروتينية 16 % منها اكتشفت بفضل دقة عمل الإدارة، 10 % منها على شكوى المجني عليه، 7 % على أثر تغيرات في القيادة الإدارية، و3 % لأسباب تتعلق بتغير نمط حياة الجاني[10].

المبحث الثاني: معالجة الجريمة الالكترونية في بعض التشريعات الداخلية

سيتم عرض وتقدير تجارب بعض الدول الغربية في معالجة الجريمة الالكترونية في المطلب الاول، اما المطلب الثاني نتطرق فيه الى تجارب بعض الدول العربية.

المطلب الأول: عرض وتقدير تجارب بعض الدول الغربية

اتجهت كافة الدول المتقدمة الى صياغة نصوص قانونية جديدة قادرة على التعامل ومواجهة هذا النوع من الجرائم المتطورة تكنولوجيا[11].و عليه سنتطرق في الفرع الأول الى تجربة الولايات المتحدة الأمريكية، و كذا التجربة الفرنسية في الفرع الثاني.

الفرع الاول: تجربة الولايات المتحدة الأمريكية

شرعت الولايات المتحدة الأمريكية في إصدار قوانين خاصة تجرم الجرائم الإلكترونية، حيث شرعت قانون خاص لحماية

أنظمة الحاسب الآلي الفيدرالي، بعدما تبلور جهد لجنة الكونجرس بإصدارهم مشروع القانون، وأطلق عليه قانون الاحتيال وإساءة استخدام الحاسب الآلي (The computer Fraud and abuse Act)، وقد تم تعديل هذا القانون عام 1986 و1994، وفي عام 1986 صدر قانونا يحمل الرقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، ووضعت المتطلبات اللازمة لتطبيقه[12].

في فيفري 1996 قام الرئيس الأمريكي "بيل كلنتون" بالتوقيع على قانون الاتصالات، والذي استهدف تقييد حرية القصر في الاطلاع على الصور و المواد المخلة بالآداب، إلا أن هذا القانون تم إلغاءه من المحكمة الدستورية الفيدرالية [13].

في ديسمبر عام 1997 وقع الرئيس كلينتون على قانون السرقة غير الإلكترونية (The No Electronic Theft) بالقرار (H.R 2265)، وجاء قانون "النيت" من أجل تعزيز حماية حقوق الطبع والعلامات التجارية، ومن أجل تعديل النصوص الواردة في القانون الفيدرالي رقم 18 والقانون رقم 17[14].

صدرت احكام على القضاء الأمريكي فيما يتعلق باختصاص بالنظر والفصل فيها في حالة تنازع الاختصاص المكاني مع قضاء دولة أخرى، حتى ولوم ترتكب الجريمة على أقاليمها تطبيقا لمبدأ الشخصية هذا الأخير بالنظر في الجرائم الإلكترونية أو المعلوماتية وقد أشارت التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء المذكور إلى جريمة وقعت في الخارج أن تكون آثارها قد مست مصالح أمريكية أو عرضتها للخطر، تأسيساً على مبدأ الاختصاص الشخصي، و طبق المبدأ في قضية

مؤداها قيام إحدى الشركات بولاية" بنسلفانيا" بالادعاء على أحد مزوّدي الإنترنت في ولاية كاليفورنيا بدعوى الاعتداء على علامة مسجلة في الولاية الأولى، وقد أسست المحكمة حكمها على أن قضاء "بنسلفانيا" ينعقد له الاختصاص الشخصي على اعتبار أن مزود خدمة الإنترنت له مشتركون في الولاية[15].

بذلك نستخلص أن القانون الأمريكي يتسع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية، ففي الولايات المتحدة الأمريكية يجيز القانون اعتراض الاتصالات الإلكترونية بصفة عامة بما في ذلك شبكات الحاسب الآلي ، وذلك متى تم بإذن من المحكمة.

اما بشأن التفتيش عن الجرائم المعلوماتية فإن في الولايات المتحدة الأمريكية تجيز وفقا للمادة 41 من قانون الإجراءات الجنائية الفيدرالي الأمريكي لقاضي التحقيق إصدار إذن تفتيش ملكية داخل منطقة أو خارجها، متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة، ولكن يخشى أو يتوقع تحركها خارج المنطقة قبل تنفيذ الإذن، وربما المشكلة التي تواجه رجال الضبط عند تنفيذهم التفتيش أنه لا يكون باستطاعتهم التحقق من أن البيانات المضبوطة جرى تخزينها داخل المنطقة أم خارجها[16].

الفرع الثاني: تجربة فرنسا

تعتبر فرنسا من الدول المتقدمة في مجال استخدام المعلومات في أوروبا، وقد سعت فرنسا إلى تطوير منظومتها القانونية لمواجهة الجرائم الإلكترونية، حيث صدر قانون خاص عام 1988 يعدل قانون العقوبات الفرنسي، وأضاف جرائم جديدة

الحاسب الآلي والعقوبات المقررة لها، حيث تم تجريم غش الحاسب الآلي، وفي عام 1994 تم مرة ثانية تعديل قانون العقوبات ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية، حيث خصص الفصل الثالث من الكتاب الثالث منه بجرائم الاعتداء على نظم المعالجة الآلية للبيانات[17].

كما أقر المشرع الفرنسي حماية جنائية خاصة لبطاقات الائتمان بموجب القانون رقم 91/1383 المؤرخ في 1991/12/30 حيث تم النص على ثلاث جرائم تتعلق بالبطاقات الائتمانية وهي تقليد أو تزوير بطاقة وفاء وسحب، استعمال، أو محاولة استعمال لبطاقة وفاء أو سحب مقلدة، أو مزورة مع العلم بذلك، وكذلك وجوب مصادرة وتدمير البطاقات المقلدة ومصادرة الأدوات التي استخدمت أو المعدة للاستخدام في التزوير أو التقليد، إلا إذا استخدمت بدون علم مالكها.

اما بشأن التفتيش عن الجرائم الإلكترونية فقد سمح بامتداد التفتيش إلى الحواسيب الموجودة خارج إقليم الدولة، لتسهيل عمل سلطات الضبط والتحقيق، وهذا الاتجاه أخذ به القانون الفرنسي من خلال المادة (17) من قانون الأمن الداخلي الفرنسي[18].

المطلب الثاني: عرض و تقدير تجارب بعض الدول العربية

في هذا السياق سنتطرق إلى كل من تجربة المملكة العربية السعودية في الفرع الأول، كما سنخصص الفرع الثاني للتطرق الى التجربة الجزائرية.

الفرع الأول: تجربة المملكة العربية السعودية

وافق مجلس الوزراء في المملكة عام 2007 على نظامي مكافحة جرائم المعلوماتية والتعاملات الإلكترونية، وذلك من أجل وضع حد من وقوع الجرائم المعلوماتية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقررة لكل جريمة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات على مجرمي المعلوماتية.

كما يهدف هذا القانون إلى تأمين استخدام أجهزة الكمبيوتر وشبكة الانترنيت من عبث الأفراد و المنظمات الإجرامية وغيرها، والذي يتمثل في ارتكاب جرائم الأموال وجرائم الآداب وجرائم الإرهاب وجرائم السب والقذف وجرائم غسيل الأموال[19].

كما جاء في نص المادة 13 من نظام مكافحة الجرائم المعلوماتية السعودي: « مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها، كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقًا نهائيًّا أو مؤقّتًا متى كان مَصدرًا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتُكِبَت بعلم مالكه.»، وفي هاتين المادتين إشارة إلى صعوبة إثبات مثل هذه الجرائم، وهذا واقع الأمر ولذلك عبّر المقنّن بقوله: "وكانت الجريمة قد ارتُكِبَت بعلم مالكه" ففيه إشارة إلى جهالة الفاعل الأصلي وصعوبة تعيينه، ثم إذا تُوصِّل إليه بطرق الإثبات العامة المتقدِّم ذكرها، فإنَّه بعينه يقع تحت طائلة هذه المواد العقابيّة.

الفرع الثاني: التجربة الجزائرية

عام 2009 صادق البرلمان الجزائري على مشروع القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد تضمن هذا القانون 19 مادة موزعة على 6 فصول تم إعداده من نخبة من رجال القانون وبمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها، إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها، وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، أو حالة توفر معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام، وينص القانون أيضا على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال، ومكافحته تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المعلوماتية، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفّل اللجنة أيضا بتبادل المعلومات مع نظيراتها في الخارج، علما أن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل[20].

فيما يتعلق بقانون الجرائم المعلوماتية، فقد نص المشرع الجزائري في المادة 394 مكرر إلى 394 مكرر إلى مكرر 7 من قانون العقوبات لعام 2006 على جريمة المساس بأنظمة المعالجة الآلية للمعطيات والبيانات، وقرر لها عقوبات متفاوتة[21].

الخاتمـــة

في ختام هذه الورقة العلمية، نشير إلى ما قاله الأمريكي (Eric Holder) الانترنيت والحاسبات الآلية جلبت منافع جمة للمجتمع، متضمنة حرية عظمى للتعبير وللنمو الاقتصادي، ولكن يجب أن ندرك أنه ونتيجة لتزايد اعتماد مجتمعاتنا على التكنولوجيا فإن جهات التحقيق والمدعين والعاملين يواجهون على كافة المستويات (دولية - فيدرالية - محلية) تحديات فريدة. كما يشير (James Robinnso) إلى هذه التحديات وهي ثلاث تحديات :

- تحديات تقنية: وتتمثل في صعوبة تحديد مصدر اعتداء مرتكبي جرائم الحاسب الآلي لأن المجرم الإلكتروني عادة يحاول ترك أمر تتبعه مستحيلا، ومع تزايد التطور التكنولوجي ظهرت تقنيات جديدة لإخفاء الأثر، إضافة إلى أن شبكة الانترنيت تزيد الأمر تعقيدا، لأن المجرمين بواسطتها يتمكنون من إخفاء هويتهم ويستطيعون ارتكاب جرائمهم من أماكن بعيدة وبمعاونة شركاء لهم من بلدان أخرى وبإجراء اتصالات مختلفة لتضليل لجان التحقيق[22].

- تحديات قانونية: تختلف التشريعات في معالجتها للجرائم الإلكترونية، فنجد بعض الدول وإن وضعت منظومة تشريعية لمواجهة الجريمة المعلوماتية إلا أن الواقع أثبت قصورها في العديد من المرات بسبب التطور السريع للجريمة المعلوماتية، إضافة إلى هذا عدم تجريم الدول للجرائم المعلوماتية يجعل من الصعب و المستحيل تتبع المجرمين وضبطهم.

تحديات فنية: في أغلب الحالات يتفوق المجرم المعلوماتي عن رجال التحقيق ورجال القضاء، وهذا مرده إلى المعرفة الكبيرة

بتقنية المعلومات بالنسبة للمجرم المعلوماتي، بينما بالمقابل نجد أن رجال التحقيق ورجال القضاء يفتقرون على الخبرة والمعرفة الفنية في هذا النوع من الإجرام، الأمر الذي يزيد من صعوبة التحقيق وإثبات الجرائم.

تذليلا لهذه التحديات هناك ما يمكن القيام به على المستوى الوطني، كوضع منظومة تشريعية كفيلة بمحاربة الجريمة المعلوماتية، بالإضافة إلى وضع استراتيجية وطنية شاملة لحماية أمن المعلومات ومواجهة الهجمات الإلكترونية، بالإضافة إلى تكوين الكادر المؤهل في كل التخصصات للتعامل مع هذا النوع من الجرائم، و في الأخير فإن هذه الجهود لن تتكل بالنجاح إن لم تتحد الجهود على المستوى الدولي لمواجهة هذه الظاهرة.

كما توصلنا من خلال هذا البحث إلى النتائج والمقترحات التالية:

1- عدم قيام بعض الدول العربية بسن قوانين خاصة بالجرائم المعلوماتية، بالرغم من تزيد انتشارها في السنوات الأخيرة، لذلك على هذه الدول تدارك هذا النقص حتى يمكنها متابعة ومعاقبة مرتكبي هذه الجرائم استنادا إلى مبدأ الشرعية الجنائية ومواكبة التطور الحاصل في هذا المجال.

2- على الدول العربية توسيع اختصاصها القضائي في مجال الجرائم الإلكترونية استنادا إلى مبدأ الشخصية والعينية وعدم اقتصارها على مبدأ الإقليمية المعروف في النظم والقوانين الجنائية الداخلية، والاستفادة من تجربة الولايات المتحدة الأمريكية وبريطانيا وفرنسا في هذا الشأن.

3- إبرام اتفاقيات عربية وإقليمية لمكافحة الجرائم المعلوماتية، وتوثيق أواصر التعاون فيما بينها في هذا المجال.

4- التفكير في إنشاء شرطة جنائية عربية على غرار الشرطة الجنائية الدولية " الأنتربول"، والشرطة الجنائية الأوروبية " الإيربول " مكونة من خبراء عرب في المجال الشرطي والقانوني والمعلوماتي وغيرهم، وتكليفها بالبحث ومتابعة والتحقيق في الجرائم المعلوماتية التي تحدث في البلدان العربية أو تصيب مصالحها بضرر.

5- قيام الدول بتدريب قضاتها، وخاصة قضاة التحقيق والنيابة العامة على تكنولوجيا المعلومات والاتصالات بغية تسهيل مهامها في مجال البحث والتحقيق في الجرائم الإلكترونية وإثباتها.

6- الاعتداد بوسائل الإثبات الجنائي الحديثة وفي مجال الكشف عن الجرائم المعلوماتية ومرتكبيها بالمستندات الإلكترونية، البريد الإلكتروني و غيرها و النص عليها في نصوص قانوني واضحة وصريحة.

7- إنشاء معاهد وفتح تخصصات في الجامعات تعنى بالأمن المعلوماتي، والتدريب فيه، ومواكبة كل التطورات الحاصلة هذا المجال.

الهوامش

1- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنيت، دار الفكر العربي، الإسكندرية،2007، ص35.

2- عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنيت، دار الكتب والوثائق المصرية، ص43-45.

3- سامي علي حامد عياد، المرجع السابق، ص42.

4- محمد أمين الشوابكة، جرائم الحاسوب والانترنيت، دار الثقافة عمان الأردن، الطبعة الأولى، ص09.
5- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري بتيزي وزو، الجزائر، 2013، ص16.
6- رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، العدد الثاني، سنة 1999، ص16.
7- صغير يوسف، المرجع السابق، ص16.
8- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية، 2002، ص46.
9- صغير يوسف، المرجع السابق، ص19-20.
10- محمد حماد مرهج الهيتي، المرجع السابق، ص218.
11- علي جبار الحسيناوي، جرائم الحاسوب و الانترنيت، دار اليازوري العلمية للنشر والتوزيع، عمان الأردن، الطبعة الأولى، 2009، ص163.
12- د علي جبار الحسيناوي، المرجع السابق، ص164.
13- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، 2009، ص145.
14- الموقع الإلكتروني:
http :www.usdoj.gov/criminal/cybercrime/iplaws.html:.page 3 - 5
15- موسى مسعود أرحومة، مقال بعنوان الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، طرابلس، 2009، ص19.
16- المرجع نفسه، ص11.
17- محمود أحمد عبابنة، المرجع السابق، ص151.
18- موسى مسعود أرحومة، المرجع السابق، ص11.
19- محمد عبد الله المنشاوي، المرجع نفسه.
20- الموقع الإلكتروني التالي: http://www.essalamonline.com
21- راجع صغير يوسف، المرجع السابق، ص108-112.
http://www.djazairess.com
22- محمود أحمد عبابنة، المرجع السابق، ص146.

قائمة المصادر و المراجع المعتمد عليها

الكتب:

1- أسامة أبو الحجاج، دليلك الشخصي إلى الانترنيت، نهضة مصر، القاهرة، طبعة 1998.
2- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنيت، دار الفكر العربي الإسكندرية، طبعة 2007.
3- عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية، طبعة 2002.
4- عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنيت، دار الكتب والوثائق المصرية.

5- علي جبار الحسيناوي، جرائم الحاسوب والانترنيت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2009.
محمد أمين الشوابكة، جرائم الحاسوب والانترنيت، دار الثقافة عمان الأردن، الطبعة الأولى .
6- محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، عمان الأردن، الطبعة الأولى، 2006.
7- محمد عبد الله المنشاوي، جرائم الانترنيت من منظور شرعي وقانوني، مكة المكرمة.
8- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، طبعة 2009.

المقالات:

1- رستم هشام ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني، مجلة الأمن و القانون دبي ، العدد الثاني، سنة 1999.
2- رئيس اللجنة الاستشارية لحقوق الإنسان في الجزائر، بعنوان تطبيق العقوبات في قضايا الجريمة الإلكترونية صعب في الجزائر و160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الإنترنت، منشور بتاريخ 24 - 01 – 2014.
3- عبد الإله مجيد، الجريمة الالكترونية تكلف العالم 400 مليار دولار سنويًا، مقال منشور بتاريخ 10/06/ 2014.
4- المديرية العامة للأمن الوطني الجزائري، مقال بعنوان الجريمة الالكترونية: المديرية العامة للأمن الوطني تعالج أكثر من 380 قضية خلال السداسي الأول، 2013.
5- منى شاكر فراج العسبلي، تأثير الجريمة الإلكترونية على النواحي الاقتصادية.
6- موسى مسعود أرحومة، مقال بعنوان الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، طرابلس، 2009.

الرسائل الجامعية:

1- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري بتيزي وزو، الجزائر، 2013.

المواقع الالكترونية:

01- http://www.usdoj.gov
02- http://albosala.com
03- http://droit7.blogspot.com
04- http://elaph.com
05- http://www.aldaawah.com
06- http://www.djazairess.com
07- http://www.essalamonline.com
08- mohamed@minshawi.com
09- www.coeia.edu.sa
10- www.ennaharonline.com