تأثير الجريمة الإلكترونية على الجريمة المنظمة

الدكتور: فرعون محمد

الرتبة العلمية: دكتوراه في العلوم

التخصص : قانون المنازعات/ كلية الحقوق والعلوم السياسية – جامعة سيدي بلعباس–

ملخص

كان من نتاج التطور التكنولوجي ظهور أدوات واختراعات وخدمات جديدة فى مختلف المجالات ولقد نتج عن الثورة التكنولوجية ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التي نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.

نتيجة للتوسع التجاري بين الدول وعولمة اقتصاديات الدول وما نتج عنها من عولمة الثقافة وكذلك الجريمة، هذا ما عجل بظهور منظمات خطيرة تعمل على مستوى دولي ومنظم متجاوزة الحدود الدولية ومخترقة لأكثر من دولة ومعتمدة استراتيجيات معينة وتحالفات بين المنظمات الإجرامية الوطنية والخارجية لفرض السيطرة على الدول خاصة في ظل تحالف المخصصين في مجال المعلوماتية مع العصابات الإجرامية المنظمة، مما جعلها من أكبر التحديات التي تواجه الدول بكافة أشكالها وبدون تمييز بين المتقدمة منها والمتخلفة.

الكلمات المفتاحية: جريمة إلكترونية، تحديات المجتمع الدولي، الجريمة المنظمة، حماية قانونية.

Abstract:

It was a product of the emergence of tools and technological inventions and new services in various areas and technological revolution has resulted in the emergence of a new type of transaction called electronic transactions differ from

traditional transactions that we know in terms of the environment where these transactions.

As a result of the expansion of trade between the States and the globalization of economies and the resulting globalization of culture and crime, that's what precipitated the emergence of serious organisations working on an international level and organized beyond international borders and infiltrated more than one State and supported specific strategies and alliances between national criminal organizations And exert control over foreign countries especially in light of ad litem in Informatics Alliance with organized criminal gangs. Making it one of the biggest challenges facing all countries without distinction between developed and underdeveloped.

Through the above problem arises: to what extent can online crime impact on organized crime?

keywords: electronic crime, organized crime, the international community challenges, legal protection.

مقدمة

إذا كان للتقدم التقني واستخدام الحاسوب الآلي والانترنت مزايا وإيجابيات ، فإن له كما هو شأن كل الاكتشافات والاختراعات الجديدة مشاكل وسلبيات، من بينها ظهور صور جديدة من الجرائم لم تكن معروفة في الماضي، إلى جانب ظهور مشاكل قانونية وفقهية منها فكرة المجرم المعلوماتي الذي بمقدوره استخدام الوسائل التقنية الحديثة ليتوصل إلى أنظمة الحاسب الآلي في أي مكان في العالم ، إلى جانب فكرة المال المعلوماتي (غير المادي) المتمثل في البرامج والمعلومات والبيانات أيا كان موضوعها، والخطر الأكبر أن هذه الجريمة أصبحت قاعدة خلفية لباقي الجرائم تعتمد عليها للوصول إلى أهدافها كما هو الشأن بالنسبة

للجريمة المنظمة التي أصبحت تعتمد على الوسائل التكنولوجية الحديثة في القيام بأعمالها فهي في تطور مستمر، كل ذلك أدى إلى تعدد الجهود المبذولة سواء على الصعيد الدولي أو المستوى الإقليمي لمجابهة هذا الخطر؛ فعلى الصعيد الدولي عقدت الأمم المتحدة العديد من المؤتمرات لمواجهة الجرائم الإلكترونية وإصدار الكثير من التوصيات، ففي المؤتمر السابع للأمم المتحدة الخاص بمكافحة الجريمة ومعاملة المجرمين أشار المؤتمر إلى جرائم الحاسوب الآلي والصعوبات المتعلقة بها باعتبارها من الجرائم المتعدية الحدود ذات الطابع الاقتصادي.

ومن خلال ما سبق تثار الإشكالية التالية:

إلى أي مدى يمكن للجريمة الإلكترونية التأثير على الجريمة المنظمة ؟

حيث تتفرع عن هذه الإشكالية عدة تساؤلات من بينها البحث عن العلاقة بين الجريمتين وإلى أي حد توصلت الجهود الدولية والوطنية لمجابهة هذه الجرائم.

المبحث الأول: ماهية الجريمة الإلكترونية

ترجع أهمية موضوع الجرائم الإلكترونية في الانتشار الواسع لهذا النوع من الجرائم والذي رافق الاستخدام الواسع للمعاملات الالكترونية على الصعيد الدولي والإقليمي والوطني هذا من جهة، ومن جهة أخرى فقد أصبحت الجريمة الالكترونية مُتلازمة مع التطور السريع والهائل في مجال تكنولوجيا الاتصالات والمعلومات.

المطلب الأول: مفهوم الجرائم الإلكترونية.

الجريمة الإلكترونية أو جرائم الحاسوب والإنترنت أو الجريمة السايْبِريّة أو مهمهما إختلفت تسميتها هي جرائم تتشابه معالجرائم التقليدية فى أطراف الجريمة من مجرم قام بارتكاب الجريمة و ضحية الذيقد يكون

شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة. وهنا يكمن الاختلافالحقيقي بين نوعي الجريمة ففي الجريمة الالكترونية الأداة ذات تقنية عالية وأيضامكان الجريمة الذي لا يتطلب انتقال الجاني إليه انتقالا حقيقيا ولكن في الكثير منتلك الجرائم فإن الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة[1].

هذا وتشير مجلة لوس انجلوس تايمز فى عددها الصادر فى 22 مارس عام 2000 إلى أن خسارة الشركات الاميريكية وحدها من جراء الممارسات التي تتعرض لها والتي تندرج تحت بند الجريمة الالكترونية بحوالي 10 مليار دولار سنويا، وللتأكيدعلى جانب قد تغفله الكثير من مؤسسات الأعمال فان نسبة 62% من تلك الجرائم تحدث منخارج المؤسسة وعن طريق شبكة الانترنت بينما تشكل النسبة الباقية (38 %) من تلكالخسائر من ممارسات تحدث من داخل المؤسسات ذاتها.

ومن الجرائم الأخرى ذات التأثيرات المختلفة سرقة بيانات بطاقات الائتمان الشخصية والدخول علىالحسابات البنكية وتعديلها وسرقة الأسرار الشخصية والعملية الموجودة بصورة الكترونية وأيضا الدخول على المواقع وقواعد البيانات وتغيير أو سرقة محتوياتها وأيضا بث الأفكار الهدامة أو المضادة لجماعات أو حكومات بعينها وأيضا السب والقذف والتشهير بالشخصيات العادية والعامة ورموز الدين والسياسة وخلافه.

وبالنظر فينطاق القانون الجنائي، يعرف الأستاذ الدكتور محمود نجيب حسني الجريمة " بأنها فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيراً احترازياً"[2]. ويبدو أنه لا اتفاق بين الفقهاء حول مصطلح للدلالة على هذه الظاهرة المستحدثة ، باعتبار أن موضوع الجريمة الإلكترونية يختلف بحسب ما إذا كان الاعتداء موجَّهاً إلى أحد مكونات النظام المعلوماتي أو كان

وسيلة لتنفيذ جرائم معينة ، فالجريمة الإلكترونية كظاهرة إجرامية ذات طبيعة خاصة ، تقنية وعابرة للحدود تتعلق في الغالب بما يسمى القانون الجنائي المعلوماتي[3].

كما يتم تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية وتعريف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال[4].

وتعتمد تعاريف الجريمة الإلكتروني في الغالب على الغرض من استخدام هذا المصطلح وتشمل عددا محدداً من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة ويمثل جوهر الجريمة الإلكترونية أبعد من هذا الوصف ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر بما في ذلك أشكال الجرائم المتصلة بالهوية والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية. "

ورغم صعوبة وضع تعريف لظاهرة هذه الجريمة وحصرها في مجال ضيق، إلا أن مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسوب الآلي بأنها " الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي"

لقد عرف الدكتور عبد الفتاح مراد جرائم الانترنت على أنها :" جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسوب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسوب الآلي و نظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط عير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الالكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبيرية أو السيبرانية لتعلقها بالعالم الافتراضي[5].

وقد عرفتها الدكتورة هدى قشقوش بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[6].

ويعرفها خبراء منظمة التعاون الاقتصادي والتنمية " بأنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها. "

وقد اصطلح المشرع الجزائري على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 09-04 المؤرخ في 05 غشت 2009، على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية[7].

في عام 2000 أقرّت وزارة العدل الأمريكية تصنيفا لجرائم الحاسب الآلي تضمن: السطو على بيانات الحاسب، والاتجار بكلمة السر، وحقوق الطبع (البرامج – ألأفلام – التسجيل الصوتي) وعمليات القرصنة، وسرقة الأسرار التجارية باستخدام الحاسب، وتزوير الماركات التجارية باستخدام الحاسب، وتزوير العملة باستخدام الحاسب، والصور الفاضحة واستغلال الأطفال، والاحتيال بواسطة شبكة الإنترنت ، والإزعاج عن طريق شبكة الإنترنت، وتهديدات القنابل بواسطة شبكة الإنترنت، والاتجار بالمتفجرات أو الأسلحة النارية أو المخدرات، وغسيل الأموال عبر شبكة الإنترنت، وصنف مكتب التحقيقات الفيدرالي الجرائم المعلوماتية في أبريل 2000 إلى سبع جرائم هي: اقتحامات شبكة الهواتف العامة أو الخاصة بواسطة الحاسب، واقتحامات شبكة الحاسب الرئيسية لأي جهة، واقتحامات السرية المؤرخة على بعض المواقع بالإنترنت أو الجهات، وانتهاكات سلامة الشبكة المعلومانية، والتجسس الصناعي، وبرامج الحاسب المسروقة[8].

ورغم الفارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الإنترنت، فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب وبرامجه والمعلومات المخزنة به، فإن جرائم الإنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب عبر خطوط الهاتف أو الشبكات الفضائية، إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والاتصالات) وظهور مصطلح (Cybercrime) [9].

واشتملت الاتفاقية الأوروبية لجرائم الحاسب الآلي والإنترنت المسماة باتفاقية بودابست بشأن الإجرام الكوني (Cybercrime)، الموقعة في 11/23 /2001 على خمسة عناوين ، الأربعة الأول تناولت أربعة أنواع من الجرائم هي : الجرائم التي تمس سرية وأمن وسلامة وتوفير بيانات الحاسب ومنظوماته وهي تضم (الدخول غير المشروع – والإعراض غير المشروع – والتدخل في البيانات – والتدخل غير المشروع في المنظومة – وإساءة استخدام الأجهزة)، والجرائم المتصلة بالحاسب الآلي وتضم (جريمة التزوير المتعلقة بالحاسب – وجريمة التدليس المتعلقة بالحاسب)، والجرائم المتصلة بالمواد الإباحية للأطفال (الإنتاج أو النشر غير المشروع للمواد الإباحية وصور الأطفال الفاضحة)، والجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المرتبطة بها (الطبع والنشر)؛ والعنوان الخامس خصص للمسؤولية وللجزاءات، وهو يشتمل على بنود إضافية بشأن الشروع والاشتراك، وأيضا الجزاءات أو التدبير وذلك طبقا للاتفاقيات أو المعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية[10].

المطلب الثاني: خصائص الجريمةالإلكترونية :

تتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن غيرها من الجرائم الأخرى ومن بين أهم هذه الخصائص ما يلي:

1-يتميز الجاني في الجريمة الإلكترونية بمهارات تقنية عالية في مجال أنظمة الحاسب الآلي تسهل له الولوج والحصول على المعلومات حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية حتى لا يمكن ملاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب[11].

2- تتعدد أنماط الجناة في الجريمة المعلوماتية ، فهناك الهاكارز " Hackers " أو المتسللون وهم عادةً مجرمون محترفون يستغلون خبراتهم وإمكانياتهم في مجال تقنية المعلومات للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به بقصد الانتقام أو الابتزاز.

وهناك الكراكرز" " Crackers " المخترقون" سواء كان من الهواة أو المحترفين وعادةً ما يستخدم مجرمو هذا النمط قدراتهم الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير شرعية كالحصول على معلومات سرية أو للقيام بأعمال تخريبية. إلخ وهناك العابثون بالشفرات ومؤلفو الفيروسات " Malecions hackerS " .

3-الجريمة الإلكترونية ذات بعد دولي أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية ، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

4-هي جريمة لا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، فالقيام بهذه الجريمة لا تحتاج إلا إلى لمسات أزرار تنفذ بسرعة.

5- هي جريمة صعبة الإثبات لعدم وجود الآثار المادية التقليدية وهذا ما جعل وسائل الإثبات التقليدية غير كافية، مما أدى إلى البحث عن أدلة فعالة لإثباتها، كاستخراج البصمات الصوتية أو استعمال شبكية العين ومضاهاتها باستخدام وسائل آلية سريعة[12].

6-نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أوسرقة البنوك أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات...الخ.

8-سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه حيث يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما إن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبيها،أمر في غاية الصعوبة [13].

المبحث الثاني: علاقة الجريمة المنظمة بالجريمة الإلكترونية

لقد أصبحت الهجمات الإلكترونية مصدر تهديد حقيقيا لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية، وذكر بعض الخبراء أن الأرباح الضخمة التي تحققها الجرائم الإلكترونية تجاوزت أرباح تجارة المخدرات مما جعلها تصبح من بين أهم موارد الجريمة المنظمة.

المطلب الأول: تعريف الجريمة المنظمة

وعرفها الدكتور مصطفى طاهر بقوله : " الجريمة المنظمة جريمة متنوعة و معقدة من الأنشطة الإجرامية والعمليات السريعة واسعة النطاق المتعلقة بالعديد من السلع والخدمات غير المشروعة تهيمن عليها

عصابات بالغة القوة والتنظيم، تضم آلاف المجرمين من مختلف الجنسيات، وتتم بقدر كبير من الاحتراف والاستمرارية وقوة البطش، وتستهدف تحقيق الربح المالي واكتساب القوة والنفوذ باستخدام أساليب عديدة ومختلفة[14].

كما حاولت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تحديد استخدام عبارة "جماعة إجرامية منظمة" بكونها " جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى[15].

ويمكن أن نستنتج من تعريف الأمم المتحدة المشار إليه أعلاه أن الجريمة المنظمة تتميز بالسمات التالية:

1 – أن الجريمة المنظمة هي جريمة خطيرة كثيرا ما تنطوي على استخدام العنف في سبيل تحقيق غاياتها، والمقصود بالخطورة هنا هو أن تكون هذه الأفعال يعاقب على ارتكابها بالحرمان من الحرية لمدة لا تقل عن أربع سنوات.

2 – إن هذه الجرائم ليست جرائم فردية، بل تقوم بها جماعات إجرامية منظمة بمعنى أن هذه الجماعات تتوفر على هيكل تنظيمي ويتسم تكوينها بنوع من الاستمرارية.

3 – يكون الهدف من القيام بالجريمة المنظمة في الأساس تحقيق منافع مالية أو الحصول على أية منافع مادية أخرى، فالجريمة المنظمة تقوم على حسابات عقلانية، فهي تتجه دوما حيث توجد الأموال، وحيث يوجد أقل قدر من المخاطر، لأنها مبنية على حسابات الربح والخسارة .

4 – تتسم الجريمة المنظمة بمرونتها الفائقة في قدرتها على تخطي حدود الدولة والعمل على تجنيد الفاعلين في دول عدة، وتنظيم شبكات إجرامية تعمل على المستوى الوطني أو القاري ومنها التي يطول نشاطها العالم أجمع [16].

ومن بين أهم المجالات التي تمارس فيها الجريمة المنظمة نشاطها:

1. غسل الأموال والرشوة والفساد الإداريوالمالي.
2. الأنشطة غير المشروعة بالمواد المخدرة.
3. الربح غير المشروع في سوق الأوراقالمالية.
4. انتهاك حقوق الملكية الفكرية وقرصنة المنتجات وسرقة العلامات التجارية.
5. الجرائم المعلوماتية المرتبطة بالفضاء السيبراني مثل تزوير البطاقات البنكية والائتمانية واقتحام وسرقة الحسابات البنكية والبرامج المعلوماتية إلى غير ذلك من الجرائم التي يفسح التطور التكنولوجي أمامها آفاقا واسعة .

المطلب الثاني: علاقة الجريمة الالكترونية بالجريمة المنظمة

ما حدث في أواخر عام 2000 عندما استعمل نوع من الفيروس الذي عُرف باسم "بقة الحب" في محاولة للوصول إلى كلمات السر للحسابات في يونيون بنك أوف سويتزرلاند، وفي ما لا يقل عن مصرفين آخرين في الولايات المتحدة، ومع إن القصة لم تلق اهتماماً يذكر، ولم يعرف بالضبط من كانوا فاعلوها، فهي تعطي مصداقية أكبر للنظرية القائلة بان الجريمة المنظمة تطور علاقات مع معتدين صغار مهرة في تقنيات الكمبيوتر، والأمر الذي يمكن أن نتوقع حصوله هو ما يمكن تسميته تبديل مناطق "الصلاحيات القانونية". فلا شك أن الجرائم المتعلقة بالشبكات الإلكترونية – عندما ترتبط بالجريمة المنظمة – سوف تنطلق من

مناطق لا يوجد فيها إلا القليل إن وجد، من القوانين الموجهة لمحاربة الجرائم التي ترتكب عبر الشبكات الإلكترونية أو المناطق التي لا تملك قدرات تذكر على تطبيق القوانين المضادة للجرائم التي ترتكب عبر الشبكات الإلكترونية. حيث كان هذا أحد الدروس التي قدمها فيروس "بقة الحب". ومع أن الفيروس انتشر في العالم أجمع وكلف المؤسسات التجارية آلاف الملايين من الدولارات، فعندما تمكن مخبرو مكتب التحقيقات الفيدرالي من تحديد هوية مرتكب العمل، وكان طالباً في الفلبين، اكتشفوا أيضاً أنه ليس هناك من قانون يمكن من خلاله محاكمة المرتكب، بعد ذلك عمدت دولة الفلبين إلى إصدار قوانين تحرّم الجرائم التي تُرتكب عبر الشبكات الإلكترونية، وتبعتها في هذا السياق دول أخرى.

ومن وجهة نظر جماعات الجريمة المنظمة، توفر شبكة الإنترنت، كما يوفر نمو التجارة الإلكترونية، مجموعة جديدة من الأهداف للتغلغل وممارسة النفوذ، وهو احتمال يشير إلى وجوب أن تكون تكنولوجيا الإنترنت وشركات خدمات الإنترنت حذرة بصورة خاصة حول الشركاء المحتملين والداعمين الماليين لها . وخضوعها وملكيتها لرقابة حكومية.

كما هو الشأن في سبتمبر من سنة 2016، حيث كشفت شركة ياهوو (yahoo)عن أكبر عمليات قرصنة وسرقة لقاعدة بيانات مستخدميها، هذه العملية تُعتبر من أكبر عمليات القرصنة في التاريخ لشركة تقنية، حيث حصل القراصنة على بيانات أكثر 500 مليون مستخدم، و في ديسمبر من نفس السنة تعرضت الشركة نفسها، لصدمة أخرى حيث أعلنت بأن بيانات أكثر من مليار مستخدم قد تم الاستيلاء عليها وأصبحت معروضة للبيع ، منها كلمات السر وأسئلة الأمان وأرقام هواتف وتواريخ ميلاد، هذه الحوادث خفضت من أسهم الشركة الأمريكية اقتصاديا وإعلامياً بشكل ملحوظ[17].

كما كشف محققون عما يعتقدون أنه أكبر جريمة إلكترونية في التاريخ، سرق خلالها قراصنة روس من العديد من بنوك دول العالم (شملت مصارف في اليابان والصين والولايات المتحدة، مروراً بمصارف في الدول الأوروبية)، ما يصل إلى مليار دولار، وهي العملية التي وصفت بأنها "ثورة في عالم الجريمة الإلكترونية" ، وهذه السرقة تشكل علامة فارقة على بداية مرحلة جديدة في ثورة النشاط الإجرامي الإلكتروني، حيث يسرق المستخدمون الأموال مباشرة من البنوك ويتجنبون المستخدمين العاديين[18].

والمؤكد أن الترابط بين الجريمة المنظمة وشبكة الإنترنت ليس طبيعياً فقط، ولكنه ترابط من المرجح له أن يزدهر وان يتطور إلى حد أبعد في المستقبل.

وقد ساهمت التجارة الحرة ووسائل الاتصال السريعة في تسهيل القيام بأنشطة مالية معقدة وتبييض الأموال عبر الحدود الوطنية، بما يقدر بنحو مليار دولار من عوائد الجريمة يتم تحويلها إلكترونياً كل يوم من خلال الأسواق المالية العالمية، كما قدر الخبراء أنه يتم تبييض ما يتراوح بين 300 و500 مليار دولار من العوائد غير المشروعة من خلال الأسواق الدولية لرأس المال كل عام[19].

وإذا كان تبييض الأموال لا يعتبر في حد ذاته خطرا على الاقتصاد العالمي والأسواق المالية مباشرة، إلا أن مكمن الخطر فيه هو ما يمكن أن ينتج عنه من آثار وخيمة، حيث يعاد استثمار العوائد غير المشروعة في أعمال الفساد والتأثير السلبي على القطاعات الشرعية للمجتمع، وعلى نطاق أوسع؛ قد تتعرض معه شرعية النظم السياسية والاجتماعية للمخاطر من جراء ذلك، ومن هنا كانت أهمية دراستنا في ربط مواجهة الجريمة الإلكترونية مع الجريمة المنظمة ومكافحة تبييض الأموال، ذلك أن تلك المواجهة تمثل أحد أهم أدوات الإقلال من فعالية جماعات الجريمة المنظمة وإعطاء السلطات القائمة على تنفيذ القانون قدرة أكبر في مطاردتهم.

المطلب الثالث: الجهود الدولية والمحلية لمكافحة الجريمة المنظمة

لقد أثبت الواقع أن كل دولة منفردة لا تستطيع القضاء على الجريمة، يضاف إلى ذلك مسألة هروب المجرمين من الدولة التي ارتكبوا فيها أعمالهم الإجرامية إلى دولة أخرى بهدف التخلص من المتابعات القضائية، وهنا تظهر مسألة التعاون والتنسيق بين الدول لتعاقب المجرمين والقبض عليهم في أي بلد كانوا فيه.

الفرع الأول: الجهود الدولية

لقد بدأت دراسة الجريمة المنظمة في عام 1975 باعتبارها ظاهرة تدخل في نطاق مجموعة الجرائم التي ارتكبت في الولايات المتحدة والتي عرفت باسم (جرائم رجال الأعمال)، وبعد أن اكتسبت الجريمة المنظمة شيئاً فشيئاً خصائصها المتعلقة بالخطورة والعدوان وظهورها في كثير من الأوساط الاجتماعية والسياسية؛ أصبحت لها ذاتية خاصة، وتوجهت عندها الجهود الدولية لمواجهة مخاطرها، إلى أن عقد بمدينة بالميرو الإيطالية في 12 من ديسمبر من عام 2000 المؤتمر الدبلوماسي الخاص بالتوقيع على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الإقليمية، وأتبعت بها البروتوكولات الثلاثة المكملة للاتفاقية، والتي يختص الأول منها بمنع وقمع ومعاقبة الاتجار بالأشخاص وبخاصة النساء والأطفال؛ والثاني يتعلق بمكافحة تهريب المهاجرين عن طريق البر والبحر والجو؛ والثالث يتعلق بمكافحة صنع الأسلحة النارية وأجزائها ومكوّناتها والذخيرة والاتجار بها بصورة غير مشروعة، والتي صيغت في الفترة ما بين يناير 1999 وأكتوبر 2000 بواسطة اللجنة الخاصة التي شكلتها الجمعية العام للأمم المتحدة بالقرار رقم 111/53 الصادر في ديسمبر 1998.

لقد كان التوقيع على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة وليد جهود مضنية ومناقشات ودراسات للأجهزة المتخصصة في الأمم المتحدة، والتي هيأت إلى عقد المؤتمر الوزاري العالمي في عام 1994 حول الجريمة المنظمة العابرة للحدود الإقليمية، والذي اشترك فيه ممثلون سياسيون وخبراء دوليون من 142 دولة، وعقد اجتماع تحضيري في بالميرو–إيطاليا سبتمبر 1994، وصودق عليه من طرف الجمعية العامة لمنظمة الأمم المتحدة بتاريخ 15 نوفمبر سنة 2000[20].

وكان من أبرز ما تم التوصل إليه في المؤتمر وفي الاجتماع اللاحق للجمعية العام للأمم المتحدة الوثيقتان الخاصتان بالإعلان السياسي، وخطة العمل الدولية ضد الجريمة المنظمة العابرة للحدود الإقليمية، واللتان أظهرتا الحاجة والأهمية القصوى والعاجلة لكل محاولة دولية لمكافحة الجريمة المنظمة، تضع في اعتبارها الخصائص المتعلقة بالتنظيمات الإجرامية حتى يتسنّى تحقيق المكافحة الفاعلة لها[21].

وبخصوص المسؤولية الجنائية عن الإجرام المنظم؛ نصت الاتفاقية على أن تتخذ كل دولة الإجراءات الضرورية بالاتفاق مع المبادئ القانونية المعمول بها لتحديد مسؤولية الأشخاص الاعتبارية الذين يشتركون في الجرائم الجسيمة الصادرة عن جماعة الإجرام المنظم وفي الجرائم الأخرى التي تنص عليها المواد (5،6،8،23) من الاتفاقية، وقد تكون تلك المسؤولية جنائيةً أو مدنيةً أو إداريةً دون المساس بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم، وكذلك دون المساس بالمبادئ القانونية المعمول بها في الدولة الطرف في الاتفاقية.

كما تعتبر مواد الاتفاقية المتعلقة بأعمال البحث الجنائي المشترك والتشريعات الخاصة بالتحقيق من أهم الأحكام الخاصة بتفعيل جهود مكافحة الإجرام المنظم على المستويين الوطني والدولي، خاصة لأنها توفر للدول الأطراف فرصة عقد الاتفاقات أو التفاهم الثنائي أو متعدد الأطراف تجاه المسائل الخاصة

بالبحث الجنائي أو الإجراءات القضائية في دولة أو أكثر، وذلك بهدف إنشاء أجهزة مشتركة للتحقيق، على أن توضع في الاعتبار الاحترام التام والكامل لسيادة الدولة الطرف التي يتم التحقيق على أراضيها[22].

وتجدر الإشارة إلى منظومة اتصالات الأنتربول العالمية والتي ظهرت الحاجة لها مع الضعف المتزايد لمعنى الحدود الوطنية بالنسبة للمجرمين حيث تزايدت أهمية الاتصالات الشرطية الفعالة عبر الحدود أكثر من أي وقت مضى و تتمثل إحدى مهام الأنتربول الأساسية في تمكين أجهزة الشرطة في العالم من تبادل المعلومات بشكل آمن و فعال، وقد طور الأنتربول منظومة الاتصالات الشرطية العالمية " 24/7 " i– لوصل أجهزة إنفاذ القانون في البلدان الأعضاء، الأمر الذي يتيح للمستخدمين المرخص لهم تبادل البيانات الشرطية الهامة فيما بينهم والوصول إلى قواعد بيانات المنظمة وخدماتها على مدار الساعة[23].

فالمنظومة تتيح للمحققين الربط بين معلومات تبدو للوهلة الأولى غير متصلة فيما بينها لكنها تؤدي إلى تيسير التحقيقات و المساعدة في حل الجرائم . و بالتالي فهذه المنظومة تتضمن معلومات عن المجرمين ووثائق السفر والمركبات المسروقة والبصمات والأعمال الفنية المسروقة ...الخ. وقد أصبحت كندا بتاريخ 20 جانفي 2003 أول بلد يتم وصله بهذه المنظومة ، والى حد الآن تم وصل جميع البلدان الأعضاء، وبالرغم من أن المنظومة تنصب أساسا في المكاتب المركزية الوطنية ، إلا أن العديد من البلدان قررت وضعها أيضا في المواقع الإستراتيجية كمراكز الحدود والمطارات وأجهزة الجمارك ..الخ

الفرع الثاني: جهود الجزائر في مكافحة الجريمة المنظمة والإلكترونية

إن الجزائر كغيرها من الدول، تعاني من أخطار الجريمة المنظمة والتي استفحلت بسبب الوضع الأمني الذي مرت به خلال العشرية السوداء، وما صاحبها من إختلالات أمنية واقتصادية واجتماعية، مما جعل الجزائر بلدا خصباً تنمو فيه مثل هذه الجرائم التي تتأقلم والظروف غير المستقرة للبلدان.

ومما يدل على استشراء ظاهرة الجريمة المنظمة في الجزائر، هو تسجيل مصالح الأمن الوطني لإحصائية 1300 ملفاً سنوياً في قضايا الجريمة المنظمة[15]. والدولة مهتمة بشكل كبير بهذه الظاهرة، فبعد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية التي صودق عليها من طرف الجمعية العامة في 15 نوفمبر 2000، صادقت الجزائر مع التحفظات على تلك الاتفاقية في فبراير 2002، لتؤكد بأن المسؤولين في البلد مؤمنون بمدى أهمّية التعاون الدولي لمكافحة الجريمة المنظمة، والتي تعرف هي الأخرى تطوراً في الأساليب والأنماط باطّراد مع التقدم التكنولوجي الحاصل في شتى الميادين، وخاصة في المجالين الاقتصادي والمالي. ولقد صادقت الجزائر في هذا الإطار دائماً على اتفاقيات شبيهة تهدف إلى تقويض أنشطة الإجرام المنظم بشتى أنماطه وبخاصة تجارة المخدرات وظاهرة الإرهاب التي عانت كثيراً من ويلاتها، ومن بين تلك الاتفاقيات نذكر اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروعة بالمخدرات والمؤثرات العقلية في ديسمبر 1988 وصودق عليها في يناير 1995، وكذا الاتفاقية العربية لمكافحة الإرهاب بالقاهرة في أبريل 1998 والمصادق عليها في ديسمبر 1998، وأيضاً اتفاقية منظمة الوحدة الإفريقية للوقاية ومكافحة الإرهاب بالجزائر في يوليو 1999 والمصادق عليها في أبريل 2000، وكذلك الاتفاقية الدولية لقمع تمويل الإرهاب في ديسمبر 1999 والتي صودق عليها من طرف الجزائر في ديسمبر 2000([24]).

إن المشرع الجزائري في تعديله للمادتين **176** و **177** من قانون العقوبات بمقتضى القانون رقم **04-15** المؤرخ في **2004/11/10** ، فإنه وسع مجال جمعية الأشرار إلى الجنح، وكذا ما نصت عليه المادة **177** مكرر **01** بمسؤولية الشخص المعنوية جنائيا و هذا ما لم يكون موجودا في التشريع الجزائري، ويعتبر هذا تلميحا أو تصريحا معنويا بالجريمة المنظمة.

وعلما بخطورة هذه الجريمة على المجتمع الدولي الذي تعتبر الجزائر جزاءا منه فإن المشرع الجزائري قام إجراء بتعديلات في بعض القوانين وكذا سن قوانين وذلك لمحاصرة شبح الجريمة المنظمة وقد تمثل ذلك في الآتي:

بمصادقة الجزائر على اتفاقية الأمم المتحدة الخاصة بالجريمة المنظمة ليوم **2000/11/15** وذلك بناءا على المرسوم رقم **02-55** المؤرخ في **2002/02/05** المتضمن التصديق بتحفظ على محتوى الاتفاقية، وبعد المصادقة بسنتين تجسدت اهتمامات المشرع الجزائري بخطورة هذه الظاهرة الإجرامية – الجريمة المنظمة– حيث نص عليها صراحة في التعديل الذي مس قانون الإجراءات الجزائية ،قانون رقم **04-14** الموافق ل:**2004/11/10** وذلك في المواد **المادة 08 مكرر، المادة37، المادة40**، حيث مس التعديل النقاط التالية:

- تمديد اختصاص وكيل الجمهورية **م37** ق.إ.ج
- تمديد اختصاص قاضي التحقيق **م40** ق.إ.ج
- تمديد اختصاص المحاكم و الجهات القضائية م**40** مكرر
- عدم انقضاء الدعوى العمومية بالتقادم **م8** مكرر
- عدم انقضاء الدعوى المدنية للمطالبة بالتعويض عن الضرر الناجم م**8**مكرر الفقرة
- المتابعة الجزائية للشخص المعنوي م **65مكرر م65/ مكرر 14-2-3-4.**

وبعد التعديلات الأتي أجراها المشرع الجزائري على قانون الإجراءات الجزائية وكذا قانون العقوبات في المواد 176 .177 .389 .394[25]، بخصوص هذه الجريمة الخطيرة التي تمتد و تتشعب فإنه تم إجراء تعديل قانون الإجراءات الجزائية مرة أخرى تحت **رقم06/ 22** المؤرخ في **20** ديسمبر **2006 حيث مس**

المواد 16. 44 .45. 47. 51 .65. وذلك تماشيا مع توجهه في القضاء على الجريمة المنظمة أو الحد منها على أقل تقدير.

كما نجد أن الجزائر ركزت في التصدي لظاهرة الإجرام الإلكتروني على تخصيص القسم السابع مكرر من قانون العقوبات رقم 04-15 تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات " جملة من القواعد حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات، وتأخذ هذه الأفعال إما وصف الإعتداء على نظم المعالجة الآلية أو وصف الإعتداء على معطيات نظام المعالجة الآلية.

وذلك في المواد 394 مكرر فيما تعلق بالدخول غير المرخص إلى منظومة المعالجة الآلية للمعطيات والمادة 394 مكرر1 فيما تعلق بإدخال معطيات بطريق الغش إلى نظام المعالجة الآلية للمعطيات.

كما قام المشرع باستحداث مجموعة من التدابير الإجرائية في القانون 06-22 المتضمن تعديل قانون الإجرءات الجزائية تدابير تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في تسجيل الإتصالات الإلكترونية ومراقبتها بالإضافة لعملية التسرب في المواد 45 .47 و المادة 65 مكرر 5 وما بعدها.

إلى جانب وضع المشرع الجزائري حماية خاصة لبرنامج الحاسب الآلي من خلال إدخالها ضمن حقوق المؤلف والحقوق المجاورة في الأمر 03-5 المتضمن حقوق المؤلف والحقوق المجاورة بوصف المصنف المحمي لمصنفات الإعلام الآلي[26].

الخاتمة

بالرغم من الجهود المبذولة في مجال مكافحة الجريمة المنظمة من خلال التصدي لجرائم المعلوماتية وتجفيف منابع التمويل للتضيق والقضاء على الجماعات الإجرامية ، إلا أن المشوار أمام هذه المواجهة يبقى

طويلا يتسم بالاستمرارية وعدم الانقطاع أو التراخي، فعصابات الجريمة المنظمة تقوم بتطوير أساليبها وتنويع أنماط جرائمها بشكل سريع سرعة التقدم التكنولوجي والعلمي، مما يستدعي اليقظة الدائمة والبحث المستمر لتعزيز ذلك الجهد المبذول إلى حد الآن، وتجدر الإشارة هنا إلى العلاقة بين التواصل بين الجريمة المنظمة وباقي الجرائم مثل عمليات تبييض الأموال التي تعتبر من الوسائل الجديدة ، والتي يستغلها الإجرام المنظم لتقوية نفسه واستمرار نشاطه، بهدف تعزيز مواقعه وتسهيل تسلله إلى مراكز النفوذ والسلطة في المجتمع، والسعي إلى اكتساب زعمائه المكانة الاجتماعية المرموقة بصفتهم من كبار رجال الأعمال ، إضافة إلى حماية أموال العصابة من المصادرة .

الهوامش:

[1]– إسراء جبريل رشاد مرعي ،الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها" المركز الديمقراطي العربي.،ص3.

[2] – إسراء جبريل رشاد مرعي، المرجع السابق،ص5

[3] – د / عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية مصر 2006 ، ص3.

[4] – هشام محمد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999.ص29.

[5] – أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية ، الإسكندرية ، 2009 ، ص 106.

[6] – د هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة ، 1992 ، ص6

[7] – القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47.

[8] – د.المستشار عبد الفتاح بيومي حجازى ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، مصر ، المجلة الكبرى ، دار الكتب القانونية ، 2007 ، ص7-8.

[9] – د. سالم محمد الأوجلي ، التحقيق في جرائم الكمبيوتر والإنترنت، منشور علي الموقع http://afaitouri.maktoobblog.com/1624946/، ص 5.تاريخ الإطلاع 2018/05/20.

[10] – د. هلالي عبد اللاه أحمد ، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها) ، دار النهضة العربية، الطبعة الأولى، القاهرة ، 2007 ، ص47 وما بعده.

[11] – مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بالسودان المنعقد في 23-2012/9/25، ص 16.

[12] عبد العال الديربي، الجريمة المعلوماتية.تعريفها..أسبابها..خصائصها، دوريات مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، مقال منشور بتاريخ 2013/01/13 على الرابط : http://accronline.com/article_detail.aspx?id=7509 تاريخ الاطلاع 2018/05/20.

[13] – موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص3.

[14] – الأستاذ غربي أسامة ، جامعة المدية ، القيت المداخلة في الملتقى الوطني للجريمة المنظمة بجامعة عمار ثليجي بالاغواط.ص3.

[15] – اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنيةاعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 نوفمبر 2000.

[16] – محمود شريف بسيوني، الجريمة المنظمة عبر الوطنية، دار الشروق، لبنان، 2004، ط1، ص13.

[17] – مدثر النور أحمد، أكبر حوادث الاختراق حجمًا وتأثيرًا في العالم للعام 2016!، مقال منشور:2016/12/25، على موقع http://www.arageek.com/tech/2016/12/25/2016-hacking-operations.html:، تاريخ الاطلاع 2018/05/22

[18] – أكبر سرقة بالتاريخ.. متسللون سرقوا مليار دولار، مقال منشور على موقع » عربية« NEWS SKY ، بتاريخ 2015/02/16 على الرابط http://www.skynewsarabia.com/web/article/724420 تاريخ: الاطلاع:2018/05/23.

[19] – محمود شريف بسيوني، الجريمة المنظمة عبر الوطنية، مرجع سابق، ص26.

[20] – صادقت عليه الجزائر بتحفظ بموجب مرسوم رئاسي رقم 02-55 بتاريخ 05 فبراير 2002 الجريدة الرسمية العدد 09 بتاريخ 10 فبراير 2002 – ص61.

[21] – سمير شعبان، مقال حول مكافحة الجريمة المنظمة من خلال التصدي لعمليات تبييض الأموال، كلية الحقوق – جامعة الحاج لخضر باتنة.ص7

[22] – نسرين عبد الحميد نبيه, الجريمة المنظمة عبر الوطنية, دار الفكر الجامعي, الإسكندرية, دط, 2007.ص78

[23] – الأستاذ غربي أسامة ، جامعة المدية ، ألقيت المداخلة في الملتقى الوطني للجريمة المنظمة بجامعة عمار ثليجي بالاغواط. ص16

[24] – سمير شعبان، المرجع السابق ،ص 9.

[25] – تم هذا التعديل بمقتضى قانون رقم **04– 15** الموافق **10** نوفمبر 2004.المتضمن قانون العقوبات .جريدة رسمية عدد71 الصادرة بتاريخ 2004/11/10.

[26] – الأمر 03–5 المتضمن حقوق المؤلف والحقوق المجاورة المؤرخ في 2003/07/19.جريدة رسمية عدد 44 الصادر بتاريخ 2003/07/23.

قائمة المراجع

1/ الكتب:

1. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2009
2. عبد الفتاح بيومي حجازى ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مصر، المجلة الكبرى، دار الكتب القانونية ، 2007 .
3. عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية مصر 2006 .
4. محمود شريف بسيوني، الجريمة المنظمة عبر الوطنية، دار الشروق، لبنان، 2004، ط1.

نسرين عبد الحميد نبيه, الجريمة المنظمة عبر الوطنية، دار الفكر الجامعي، الإسكندرية، دط، 2007.

5. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992
6. هشام محمد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999.
7. هلالي عبد اللاه أحمد ، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها) ، دار النهضة العربية، الطبعة الأولى ، القاهرة ، 2007 .

2/ مقالات ومؤتمرات:

1. إسراء جبريل رشاد مرعي ،الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها" المركز الديمقراطي العربي.

2. سمير شعبان، مقال حول مكافحة الجريمة المنظمة من خلال التصدي لعمليات تبييض الأموال، كلية الحقوق – جامعة الحاج لخضر باتنة.

3. غربي أسامة، جامعة المدية، ألقيت المداخلة في الملتقى الوطني للجريمة المنظمة بجامعة عمار ثليجي بالاغواط.

4. مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بالسودان المنعقد في 23-2012/9/25.

5. موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009.

3/ القوانين:

1. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنيةاعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 نوفمبر 2000.

2. قانون رقم **04- 15** الموافق **10** نوفمبر 2004.المتضمن قانون العقوبات .جريدة رسمية عدد71 الصادرة بتاريخ 2004/11/10.

3. القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47.

4. الأمر 03-5 المتضمن حقوق المؤلف والحقوق المجاورة المؤرخ في 2003/07/19.جريدة رسمية عدد 44 الصادر بتاريخ 2003/07/23.

5. المواقع مرسوم رئاسي رقم 02-55 بتاريخ 05 فبراير 2002 الجريدة الرسمية العدد 09 بتاريخ 10 فبراير 2002.

4/ المواقع الإلكترونية:

1. د. سالم محمد الأوجلي ، التحقيق في جرائم الكمبيوتر و الإنترنت .

2. عبد العال الديربي، الجريمة المعلوماتية.تعريفها..أسبابها، خصائصها، دوريات مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، مقال منشور بتاريخ 2013/01/13 على الرابط : http://accronline.com/article_detail.aspx?id=7509 تاريخ الاطلاع 2018/05/20.

3. مدثر النور أحمد، أكبر حوادث الاختراق حجمًا وتأثيرًا في العالم للعام 2016!، مقال منشور :2016/12/25،على موقع-http://www.arageek.com/tech/2016/12/25/2016-hacking operations.html، تاريخ الاطلاع 2018/05/22

4. مقال بعنوان أكبر سرقة بالتاريخ.. متسللون سرقوا مليار دولار، مقال منشور على موقع » عربية NEWS SKY «، بتاريخ 2015/02/16 على الرابط

5. http://www.skynewsarabia.com/web/article/724420 : تاريخ الاطلاع:2018/05/23.

6. منشور علي الموقع http://afaitouri.maktoobblog.com/1624946/ ، ص 5. تاريخ الإطلاع 2018/05/20.