



الآليات الاتفاقية والتشريعية لمكافحة الجريمة الالكترونية على الصعيدين الاقليمي والدولي

Conventional and legislative mechanisms for combating cybercrime at the regional and international levels

زينب سالم¹

جامعة محمد لمين دباغين سطيف 02-الجزائر

z.salem@univ-setif2.dz

تاريخ القبول للنشر: 2025-05-26

تاريخ الاستلام: 2024-10-12

ملخص:

تصدت الدول للجرائم الالكترونية باتخاذ العديد من الإجراءات المشتركة من بينها إبرام الاتفاقيات ووضع التشريعات، وذلك لما لهذه الجرائم من آثار بالغة الخطورة في مختلف المجالات الاقتصادية والاجتماعية والثقافية، فما مضمون هذه الاتفاقيات والتشريعات وما مدى نجاعتها في الحد من تداعيات الجرائم الالكترونية؟ عرضت هذه الدراسة مختلف الجهود الاتفاقية والتشريعية على المستويين الاقليمي والدولي، وخلصت الى ضرورة تكثيف التعاون الاتفاقي بين الدول من خلال ابرام اتفاقيات جديدة والحث على الانضمام لاتفاقيات قائمة، وكذلك توحيد القوانين الموضوعية لتحقيق الامن الالكتروني.

الكلمات المفتاحية: اتفاقيات، تنسيق تشريعي، الجريمة الكترونية، الامن الالكتروني، التعاون الدولي.

Abstract:

Countries have confronted cybercrimes by taking numerous joint measures, including signing agreements and enacting legislation, due to the severe impacts of these crimes in various economic, social, and cultural fields. What is the content of these agreements and legislations, and how effective are they in mitigating the repercussions of cybercrimes? This study presented various regional and international efforts in agreements and legislation and concluded the necessity of

¹ زينب سالم



intensifying cooperative agreements between countries by signing new agreements and encouraging adherence to existing ones, as well as unifying the laws enacted to achieve cybersecurity.

Keywords: Conventions, legislative coordination, cybercrime, electronic security, international cooperation

المقدمة:

شهد العالم سلسلة من التطورات التكنولوجية أثرت في أسلوب حياة الانسان ومعيشته ومتطلباته الضرورية، وظهرت قمة هذا التطور عند المزاوجة بين تقنيات الحواسيب وشبكات الاتصال أدت الى ظهور نظم المعلومات وشبكات المعلومات، حيث أحدثت تقنية المعلومات تغيرات مستمرة ومضطردة في أساليب العمل كافة، إذ أصبحت عملية نقل المعلومات عبر الشبكات المحلية والدولية المفتوحة وأجهزة الحاسوب من الأمور الروتينية والاعتيادية في العصر الحالي، واحدى سماته التي لا يمكن الاستغناء عنها لدورها الواضح والفعال في تسهيل متطلبات الحياة، من خلال تقليل حجم الاعمال وتطوير أساليب خزن وتوفير المعلومات.

فقد أصبح عصرنا الحالي يسمى بعصر المعلومات أو عصر المعلوماتية، فالمعلومات أصبحت في ظل هذا التطور التكنولوجي الأداة التي تقاس بها قوة الشعوب فمن يملك القوة وفي ظل تنامي أهمية وقيمة المعلومات والوسائل التقنية التي تعالجها والبيئة التي تستخدم هذه المعلومات والاشخاص الذين لهم الدور في اعدادها وتفعيلها.

هذا التطور التكنولوجي المشرق كان له وجه مظلم وجوانب سلبية ومخاطر عدة على الأشخاص وعلى حياتهم الخاصة، وكذا على أمن تعاملاتهم وسرية وسلامة بياناتهم سواء المتداولة أو المخزنة عبر أنظمة المعالجة الآلية للبيانات وحتى سلامة النظام المعلوماتي من جانبه التقني في حد ذاته.

ولم تتوقف تلك المخاطر على الأشخاص العاديين بل تعدى ذلك إلى المساس بأمن وسلامة أنظمة ومعلومات المؤسسات والإدارات والحكومات والمنظمات في ظل ما شهدته الحكومات في أغلب دول العالم من تحولات نحو الحكومات الالكترونية عملاً بمبدأ العصرية والتوجه نحو التكنولوجيا، وتعدى تأثيرها المجال الاجتماعي إلى

المجال السياسي والاقتصادي، ولم تعد القضية قضية أشخاص عاديين بل امتدت إلى المسائل الوطنية والقومية وأمن الدول والمنظمات الدولية. فأصبح من الممكن استغلال هذه التكنولوجيا لاختراق أي نظام معلوماتي واستخدامه في التجسس وتهديد أو النيل من أمن الدول وسلامة البنية التحتية المعلوماتية التي تعتمد عليها الحكومات، خاصة وأن الحكومات باتت تعتمد على تقنيات المعلومات الحديثة، وتقديم الخدمات العامة عبر نظم المعلومات الالكترونية التي شكلت نظم الادارة الحديثة في التعامل مع المواطنين، وكذا تهديد السلامة العامة وترويع المواطنين باستهداف تلك النظم مما يزعزع الثقة في هذه التعاملات.

وهكذا وجد العالم نفسه أمام ظواهر متغيرة وغير محدودة ويصعب التحكم فيها هي ظواهر إجرامية نمت وازدهرت بنماء وتطور التقنية الرقمية، لتجد كل الدول نفسها أمام تحدي كبير أمل عليها ضرورة التعاون وإيجاد طرق ووسائل لمكافحة الجرائم الالكترونية، ومن بينها الاتفاقيات والتشريعات الاقليمية والدولية .

وتأسيسا على ذلك تكمن أهمية هذه الدراسة في أنها تمثل أحد المجالات الحيوية في العلوم القانونية والدولية المعاصرة من ناحية، والتحديات المتزايدة التي تواجهها دول العالم في عصر الرقمنة من ناحية أخرى .

وتهدف هذه الدراسة الى بيان الاستراتيجيات المشتركة الاقليمية منها والدولية لمكافحة الجرائم الإلكترونية ، والوقوف على مدى فعاليتها في الحد من تداعيات هذه الجرائم.

فما مدى فعالية الاتفاقيات والتشريعات الاقليمية والدولية التي وضعت في اطار التعاون لمواجهة الجرائم الالكترونية؟

اعتمدنا في هذه الدراسة المنهجين الوصفي و التحليلي من خلال عرض ماتم ابرامه من اتفاقيات ووضعه من تشريعات على الصعيدين الاقليمي والدولي، وتحليل آثارها في تحقيق الأمن الإلكتروني، والعدالة العابرة للحدود في مكافحة الجرائم الالكترونية.



قسمنا هذه الدراسة الى ثلاث مباحث، تناولنا في المبحث الأول مفهوم الجريمة الالكترونية ، وفي المبحث الثاني بينا الجهود الاتفاقية والتشريعية على المستوى الإقليمي، وفي المبحث الثالث عرضنا الجهود الاتفاقية والتشريعية على المستوى الدولي.

المبحث الأول: مفهوم الجريمة الالكترونية

رغم صعوبة إيجاد تعريف جامع مانع للجريمة الالكترونية إلا أن اجتهاد كل من الفقهاء والباحثين أدى إلى وضع عدة تعريفات لها وإن كانت قد تباينت تبعاً لمحل اهتمام كل فئة، منهم، هذه التعريفات مكنتنا من الوقوف على خصائصها، ولذلك سنعرض في هذا المبحث تعريف الجرائم الإلكترونية، وخصائصها من خلال المطالبين الآتين:

المطلب الأول: تعريف الجريمة الالكترونية

تعددت مسميات الجريمة الالكترونية حيث سميت بجرائم الحاسوب أو الانترنت، أو جرائم التقنية العالية أو جرائم الياقات البيضاء، أو الجرائم المعلوماتية، وقد تم تعريفها من ناحيتين فقهية وقانونية نعرضهما على النحو الآتي:

الفرع الأول: التعريف الفقهي

عرف جانب من الفقه القانوني المصري الجريمة الالكترونية بأنها "كل نشاط إجرامي يستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود". (الفتاح، 2007، صفحة 20) وعرفها جانب آخر "بأنها تلك الأفعال الإجرامية الناتجة من خلال أو بواسطة استخدام المعلوماتية والتقنية الحديثة المتمثلة في الكمبيوتر أو أي من الوسائل الالكترونية" (الشوا، 1994، صفحة 5).

كما عرفت بأنها "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية أو شبكة الأنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها" (مراد، بدون سنة نشر، صفحة 40).

وعرفت أيضا بأنها: "هي عمل أو امتناع عن عمل يأتيه الانسان اضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض للاعتداء عليها عقابا" (هلالي، 2000، الصفحات 105-106)

وعرفها جانب من الفقه القانوني الأردني بأنها: "هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل" (الشوابكة، 2004، الصفحات 8-9)

أما بالنسبة للفقه القانوني الجزائري عرفها بأنها "كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة اليكترونية" (شهرزاد و مخلوفي، 2019، صفحة 19)

الفرع الثاني: التعريف القانوني

جرت العادة عند القانونيين أن التعاريف من اختصاص الفقه والقضاء ، وبالتالي عادة ما يتجنب المشرع الخوض في التعاريف، غير أن المشرع الجزائري مستعملا مصطلح الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات عرف الجريمة الالكترونية في 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."

كما عرفها المشرع الجزائري في المادة 211 مكرر 22 من الأمر 21-11 المؤرخ في 25 أوت، 2021 المتضمن قانون الإجراءات الجزائية مستعملا مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها : "كل جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال."

وتجدر الاشارة الى أن المشرع الجزائري تبني انشاء منظومة وطنية لامن الانظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20/01/2020 والمتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية.

المطلب الثاني: خصائص الجريمة الالكترونية

تتميز الجريمة الالكترونية عن غيرها من الجرائم التقليدية بالعديد من المميزات والخصائص تجعلها تختلف من حيث مرتكبيها والآثار المترتبة على ارتكابها والوسيلة المستعملة لهذا الغرض، وتتمثل مميزاتها في :

الفرع الأول: خطورة الجريمة الالكترونية

تنطوي الجريمة الالكترونية على قدر كبير من الخطورة، لما لها من آثار على النشاط الاقتصادي، وأمن البلاد الوطني، مع ما في ذلك من خطر المساس بالمعلومات والأسرار السياسية والعسكرية والاقتصادية، وفي جانب آخر فإنها جرائم تنتهك حرمة الحياة الخاصة، فالاطلاع على خصوصيات الأفراد يظل جريمة يعاقب عمليا القانون، كونها تنتهك حقا أساسيا للأفراد في حماية خصوصياتهم، وهو حق كفله مختلف التشريعات.

إن الاختراقات المتكررة التي تتم لأنظمة الحواسيب في الهيئات الرسمية لعدد الدول، أثبتت كيف أنه مهما بلغ تقدم الدول فإنها تبقى معرضة لتلك الاختراقات.

الفرع الثاني: الجريمة الالكترونية جريمة منظمة عابرة للحدود الوطنية

من أهم الخصائص التي تتسم بها الجريمة الالكترونية أنها جريمة عابرة للحدود الجغرافية للدول وذلك لتعلقها بتقنية المعلومات، التي سهلت التواصل بين مختلف الدول و الأفراد في العالم بشكل سريع، ما جعل الاتصالات والمعلوماتية تتخطى حدود الدولة ، وبالتالي أصبح من السهل ارتكاب جريمة في دولة ما بينما يتواجد مرتكبه وتقع آثارها في دولة أخرى، وهذا ما خلق تحديات قانونية وادارية وفنية بل وسياسية لمواجهتها لا سيما ما يتعلق بإجراءات الملاحقة الجنائية (عفيفي، 2013، صفحة 13).

ولا بد أن نشير إلى أن خاصية عالمية الحدود للجريمة الالكترونية يترتب عليها عدة آثار قانونية أهمها القانون الواجب التطبيق عليها والقضاء المختص بالفصل فيها، هل هو قانون الدولة التي وقع فيها النشاط الاجرامي أم قانون الدولة التي يقيم فيها الجاني أو قانون الدولة التي أضرت هذه الجريمة بمصالحها.

الفرع الثالث: الجريمة الالكترونية يتطلب ارتكابها وجود حاسب آلي ومعرفة تقنية

ترتكب الجريمة الالكترونية في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية، وأجهزة ومعدات وتجهيزات الحاسب الآلي، بمعنى تتم بواسطة المكونات المادية للحاسوب ومكوناته البرمجيات.

كما يرتكبها مجرم ذو طبيعة خاصة وإمكانات خاصة علمية معلوماتية مستخدما موارد معرفية تقنية واساليب إحترافية.

الفرع الرابع: الجريمة الالكترونية صعبة الاكتشاف والاثبات

تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، ويعود ذلك لعدم وجود الآثار التقليدية للجريمة، حيث يسهل في الجريمة الالكترونية محو الدليل 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 هذه الجريمة وتحديد مرتكبها أمر في غاية الصعوبة (ارحومة، 2009، صفحة 03).

كما أن معظم الجرائم الإلكترونية يتم اكتشافها بمحض الصدفة، وبعد مرور وقت طويل، إضافة إلى أنه لا يتم في الغالب الإبلاغ عن الجرائم الإلكترونية، إما لعدم اكتشافها من طرف الضحية أو خوفا من التشهير به (بوحليط، 2019، صفحة 82)، كما في حالة الشركات والمؤسسات، لتجنب الإساءة للسمعة والرغبة في عدم زعزعة ثقة العملاء، ففي إحدى الوقائع تعرض بنك "marchant bank city" في بريطانيا لسرقة ثمانية مليون جنية إسترليني من إحدى أرصده إلى رقم في سويسرا، وتم ضبط الفاعل متلبسا يسحب المبلغ المسروق وبدلا من محاكمته، قام



البنك بدفع مليون جنية له ، بشرط التزام الفاعل بعدم الإعلام عن جريمته، وإعلام البنك عن الألية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي.

الفرع الخامس: الجريمة الالكترونية هادئة

ان الجريمة الالكترونية تختلف عن الجرائم التقليدية كونها جرائم لا تحتاج الى جهد عضلي مثل جريمة الخطف والقتل، بل تعتمد على الذكاء التقني القائم على معرفة تقنية الكمبيوتر، كونها عبارة عن معطيات وبيانات تتغير او تعدل او تمحى من السجلات المخزنة في ذاكرة الحاسوب (رحموني، 2018، صفحة 442)

المبحث الثاني: الجهود الاتفاقية والتشريعية على المستوى الإقليمي

بذلت العديد من الجهود لإرساء سبل التعاون القانوني على المستوى الاقليمي لمواجهة الجرائم الالكترونية، وسنركز على الجهود المبذولة على المستوى الاوربي (المطلب الاول)، والجهود المبذولة على المستوى العربي (المطلب الثاني).

المطلب الاول: الجهود المبذولة على الصعيد الاوربي

تمثلت أولى جهود المجلس الأوروبي في مجال مكافحة الجرائم الالكترونية في توقيع دول الاتحاد في 1981/10/28 اتفاقية رقم 108 تتعلق بحرية تنقل البيانات الشخصية المعالجة الكترونيا وحمايتها من أشكال التعدي (Myriam, Mai 2010, p. 174)

ثم في عام 1985 قام المجلس بوضع قواعد ارشادية خاصة بتحديد انماط جرائم الحاسب ونبه من خلالها المشرع الدول الاعضاء الى ضرورة حصر الانشطة غير المشروعة المرتبطة باستخدام الحاسب الآلي، على أن تراعي في ذلك التوازن بين الحاجة للحماية الجنائية ضد هذه الانشطة من ناحية، و الحق في حماية المعلومات وحريات الافراد المدنية من ناحية أخرى (Nidal, 2003, p. 312).

وعلى نفس المسلك أصدر المجلس الاوربي توصية رقم 13/95 صدرت في 1995/09/11 في شأن مشاكل الاجراءات الجنائية المتعلقة بتكنولوجيا المعلومات

لحث الدول الاعضاء على مراجعة قوانين الاجراءات الجنائية الوطنية لتتلاءم مع التطور الحاصل في هذا المجال وأهم ما ورد بتوصية المجلس الاوربي ما يلي: (فضل، صفحة 433).

-الاعتراف للجهات المختصة بالتفتيش اذا دعت الضرورة بمد عملية التفتيش الى انظمة الحاسب الآلي الأخرى المتصلة بالنظام محل التفتيش داخل دائرة اختصاصهم وضبط ما بها من معلومات وبيانات.

-السماح بتطبيق اجراءات المراقبة والتسجيل لأغراض التحقيق الجنائي على تقنية المعلومات كلما دعت الضرورة لذلك، وفي حالة جمع المعلومات بطريق المراقبة والتسجيل يجب مراعاة معايير احترام الخصوصية وسرية المعلومات والحصانات المقررة لذلك.

-الزام المتعاملين بخدمات الاتصال الحكومية والخاصة بالتعاون مع سلطات التحقيق وتقديم يد المساعدة لهم بخصوص التحقيق.

-تطبيق النصوص الاجرائية الخاصة بالأدلة التقليدية (جمع الادلة، المحافظة عليها، تقديمها، حجيتها) على الأدلة الالكترونية، والسعي الى تطوير وتوحيد انظمة التعامل مع الادلة الالكترونية حتى يتم الاعتراف بها بين كل الدول الأعضاء.

-ضرورة تشكيل وحدات أمن خاصة لمكافحة الجرائم الالكترونية، واعداد برامج تدريبية خاصة، لتأهيل العاملين في العدالة الجنائية وتطوير معارفهم وخبراتهم في مجال التقنية المعلوماتية.

-اعتماد سياسة واضحة وفعالة حول التعاون المتبادل والمساعدة القضائية والفنية بين الدول في مجال مكافحة الجريمة الالكترونية من خلال تبني اجراءات التحقيق والمتابعة الجزائية سريعة ومناسبة، وخلق قنوات اتصال ثنائية أو متعددة الاطراف تسمح للسلطات القائمة على التحقيق الاتصال بسهولة بممثلتها الاجنبية والتنسيق معها، أو التدخل السريع للتحقيق في اقليم دولة أجنبية دون ان يشكل ذلك مساسا بسيادة هذه الدولة.



وفي فيفري 1997 كلف المجلس لجنة خبراء بإجراء دراسة معمقة حول الجريمة الالكترونية واعداد مشروع اتفاقية عامة ملزمة حول ذلك (الشهري، 2010، صفحة 41)، انتهت بوضع اتفاقية أوروبية لمكافحة الجرائم الالكترونية بالتعاون مع الولايات المتحدة الأمريكية، كندا، اليابان، جنوب افريقيا، عرضت للتوقيع في العاصمة الجرية بودابست في عام 2001 بمناسبة المؤتمر الدولي حول الاجرام الالكتروني ودخلت حيز التنفيذ في عام 2004.

وجاءت هذه الاتفاقية لتعالج اشكالية دولية الجريمة الالكترونية، وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبها والمساعدة على الاستدلال عليهم وضبطهم كما تحدد أفضل الطرق الواجب اتباعها في التحقيق في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق من أجل محاربتها.

والهدف من هذه الاتفاقية توحيد التدابير التشريعية بين الدول الاطراف والتأكيد على أهمية التنسيق والتعاون الاقليمي والدولي في ميدان مكافحة الاجرام الالكترونية، وكذا تحقيق التوازن بين حقوق الانسان والاجراءات المتخذة لمواجهة هذا النوع من الجرائم (سكولمان، 2007، صفحة 62).

وقد احتوت هذه الاتفاقية 48 مادة في مضمونها ثلاث اقسام هي:
القسم الاول:تضمن مجموعة الجرائم الالكترونية التي حددت في اربعة طوائف رئيسية نتناولها على النحو الآتي:

-الطائفة الاولى: تتضمن الجرائم التي تستهدف عناصر أمن المعلومات وهي الجرائم ضد السرية والسلامة واتاحة البيانات ونظم الحاسب وتشمل جريمة غير المشروع، جريمة الاتلاف غير المشروع للنظم أو البرامج أو بيانات الحاسب، جريمة المراقبة أو الاعتراض غير المشروع.

-الطائفة الثانية: تضم جريمة الغش المعلوماتي وجريمة التزوير المعلوماتي.
-الطائفة الثالثة: تتعلق بالجرائم المرتبطة بالمحتوى وهي جريمة الانتاج أو النشر غير المشروع للمواد الاباحية الطفولية.

-الطائفة الرابعة: تتضمن جرائم الاعتداء على الملكية الفكرية و الحقوق المجاورة. القسم الثاني:تضمن القواعد الاجرائية المناسبة لمواجهة الجرائم الالكترونية عبر مختلف مراحل المتابعة الجزائية، خاصة مرحلة التحري والاستدلال، ومن ثمة التحقيق، بحيث تتصل هذه القواعد بتنظيم عملية جمع الادلة الالكترونية، تدابير الحماية الوقائية للنظم المعلوماتية، وتسليم معطياته المخزنة واجراءات حفظها، والقواعد المتعين اتخاذها بشأن تفتيش وضبط وجمع المعطيات الالكترونية، واعتراض المعلومات، واصدار الأوامر بتسليمها أو انتاجها أو اتلافها.

القسم الثالث: تناول موضوع التعاون الدولي بين الأعضاء الموقعة على الاتفاقية لمواجهة الجرائم المعلوماتية العابرة للحدود وقد قسم الى فصلين، خصص الفصل الاول للتعاون القضائي بين الدول اطراف في تطبيق اصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية، الاتفاقيات المعتمدة على التشريعات المماثلة أو النضيرة والقوانين المحلية، وهذا التعاون يشمل ثلاثة محاور هي تدابير تسليم المجرمين، والمبادئ العامة التي تحكم الالتزام بالمساعدة القضائية المتبادلة، وكذا اجراءات طلب المساعدة القضائية المتبادلة في ظل غياب اتفاقيات دولية مطبقة، وجود قيود متعلقة بسرية وتحديد الاستخدام.

أما الفصل الثاني فخصص للتعاون الامني المتبادل بين سلطات انفاذ القانون التابعة للدول الأطراف، وتضمن ثلاث محاور هي محور المساعدة المتبادلة في مجال الاجراءات الوقتية العاجلة، كتلك المتعلقة بالتحفظ العاجل على بيانات معلوماتية مخزنة في نظام معلوماتي متواجد داخل اقليم طرف آخر، و بالإفشاء العاجل لسرية بيانات المرور المتحفظ عليها في اقليم دولة أخرى. ومحور المساعدة الفنية المتبادلة في مجال اجراءات التحقيق كالمساعدة المتبادلة الخاصة بالوصول أو الولوج الى البيانات المعلوماتية المخزنة في الخارج، والمساعدة الخاصة بالتجميع في الوقت الفعلي لبيانات المرور واعتراض بيانات المحتوى في الخارج. والمحور الثالث يخص انشاء شبكة طوارئ دائمة لتفعيل المساعدة الامنية المتبادلة، وهي شبكة



اتصال تعمل على مدار 24 ساعة وبمعدل سبعة ايام في الاسبوع بغرض توفير المساعدة الفورية لإجراءات التحقيق المتعلقة بالجرائم الالكترونية. ولا تعتبر اتفاقية بودابست هي المجهود الوحيد الذي بذله المجلس الاوربي في هذا المجال، بل هناك جهود أخرى عديدة اهمها اتفاقية التعاون المتبادل في مجال قانون العقوبات بين الدول الاعضاء في الاتحاد الاوربي، التي سعت من خلالها هذه الدول الى توحيد تشريعاتها العقابية الوطنية أو على الأقل تقريب بعضها بعض (هنروت، 2007، صفحة 107).

كذلك قرار JAI 222/2005 حول الاعتداءات التي تشن على نظم المعلومات الصادرة عن المجلس الاوربي بتاريخ 2005/01/17 (JAI/222/2005) الذي ألزم المجلس الدول الاعضاء بتوحيد نصوصها الجنائية التي تجرم وتعاقب على أفعال الاعتداء التي تمس الانظمة المعلوماتية، كأفعال القرصنة، كسر كلمة السر، كشف كلمات المرور، والهجمات بواسطة الفيروسات الالكترونية...الخ. كما وضع المجلس الاوربي في الفترة الممتدة ما بين 2010 و 2014 مخطط عمل شامل مشترك يحدد الاستراتيجية التشريعية والامنية التي يجب على جميع الدول الاعضاء اتباعها سواء على المستوى الوطني أو على المستوى الاوربي للتصدي لظاهرة الاجرام الالكترونية (Myriam, Mai 2010, p. 231)، وقد ساهم هذا الخطط بشكل كبير في توحيد السياسة الجنائية التشريعية بين دول الاتحاد الاوربية في مواجهة تحديات الجرائم الالكترونية، وخلق مناخ للتعاون المشترك فيما بينها في هذا الشأن.

المطلب الثاني: الجهود المبذولة على الصعيد العربي

تتمثل أهم محاولات العربية لتحقيق التوافق والتنسيق بين النصوص العقابية والاجرائية الوطنية التي تعنى بالجرائم الالكترونية القرار رقم 495 المتضمن القانون العربي النموذجي لمكافحة الجريمة الالكترونية الذي اعتمدته جامعة الدول العربية عبر مجلس وزراء العدل العرب في دورته التاسعة عشر المنعقدة بتاريخ 2003/10/08، وقد تضمن هذا القانون 27 مادة موزعة على أربعة ابواب ونص

الباب الاول على الجرائم الالكترونية والعقوبات المقررة لها في المواد من 3 الى 22 وتمثل في ما يلي :

- جريمة الولوج غير المشروع الى موقع أو نظام معلوماتي والتلاعب في بياناته.
 - جريمة تزوير المستندات المعالجة في نظام معلوماتي واستعمالها.
 - جريمة الادخال المؤدي الى ايقاف أو تعطيل نشاط الشبكة المعلوماتية أو اتلاف البرامج أو البيانات. -جريمة التصنت واعتراض المراسلات عبر الشبكة المعلوماتية.
 - الجرائم المخلة بالآداب العامة والنظام العام وأمن الدولة عبر الشبكة المعلوماتية.
- أما الباب الثاني تناول التجارة والمعاملات الالكترونية، وتناول الباب الثالث تدابري حماية حقوق الملكية الفكرية عبر الوسائل الالكترونية، في حين نص الباب الرابع الجوانب الاجرائية المتعلقة بالجرائم الالكترونية (فضل، صفحة 437).

وعلى الرغم من أن هذا القانون مثل القواعد الأساسية الارشادية البتي يمكن أن يستعين بها المشرع في الدول العربية فيما يخص الجرائم الالكترونية، إلا أنه يؤخذ عليه تركيزه على الجانب الموضوعي لهذه الجرائم واهماله للأحكام الاجرائية الضرورية للملاحقة مرتكبي هذه الجرائم، فهو لم يتعرض لمسألة اختصاص القضائي بشكل واضح، ولم يشر إلى اخضاع البيانات والمعلومات لإجراءات التحقيق، ولم يتعرض كذلك للدليل الالكتروني وضوابط قبوله وحجيته (جمال، 2018، صفحة 289).

ولتدارك الفراغ القانوني في القانون العربي النموذجي لمكافحة الجريمة الالكترونية في الجانب الاجرائي أبرمت جامعة الدول العربية بتاريخ 2010/12/21 اتفاقية العربية لمكافحة جرائم التقنية المعلوماتية.

وقد أكدت الاتفاقية في ديباجتها على الحاجة الملحة الى تبني اتفاقية اقليمية ملزمة تأسس لسياسة جنائية مشتركة بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وتعزيز التعاون وتدعيمه فيما بينها لدرء أخطار هذه الجرائم حفاظا على أمنها ومصالحها وسلامة مجتمعاتها وأفرادها.



كما تضمنت الاتفاقية خمسة فصول، خصص الفصل الاول لتعريف بعض المصطلحات، وتحديد نطاق تطبيق أحكام الاتفاقية، وكذا موقفها اتجاه سيادة دول الاطراف، في حين خصص الفصل الثاني لحصر الافعال التي من قبيل الجرائم الإلكترونية. أما الفصل الثالث تضمن أهم اجراءات التحقيق والاثبات الجنائي في جرائم تقنية المعلومات، كإجراءات التفتيش عن بعد في البيئة المعلوماتية، اجراءات ضبط وتأمين بيانات تقنية المعلومات، اجراءات اعتراض ومراقبة المرسلات الالكترونية، الجمع والتسجيل الفوري لبيانات المحتوى وبيانات المرور المتعلقة بالاتصالات عبر وسائل تقنية المعلومات. بينما تناول الفصل الرابع أحكام التعاون القانوني والقضائي بين الدول الأطراف لمواجهة تقنية المعلومات، وقد اشتمل عدة صور للتعاون ابرزها تمديد الاختصاص، إذ من خلالها يجوز لأية دولة طرف في الاتفاقية مد اختصاصها القضائي في الجرائم المنصوص عليها في هذه الاتفاقية إلى أقاليم الدول الأطراف الأخرى، والتعاون في تسليم وتبادل المجرمين المعلوماتيين بين الدول الأطراف، سواء في اطار معاهدات التبادل أو خارجها، المساعدة الفنية المتبادلة لأغراض التحقيق وجمع الأدلة في الجرائم المعلوماتية، كالمساعدات المتبادلة بين دول الاطراف في مجال البحث أو ضبط أو تأمين أو كشف أو الحفظ العاجل أو الجمع الفوري لبيانات مخزنة في أنظمة معلوماتية تقع خارج الاقليم الوطني، أو المساعدات المتبادلة المتعلقة بالوصول عن بعد إلى معلومات الكترونية مخزنة في نظم معلوماتية متواجدة خارج الاقليم الوطني. وفي ختام الفصل الرابع ألزمت الاتفاقية الدول الاطراف بأن تنشئ على اقليمها جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية والمشورة المتبادلة فيما بينها لأغراض التحقيق أو نقل الاجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الادلة بشكلها الالكتروني فيها، أما الفصل الخامس والأخير فتناول الاحكام الختامية.

وتجدر الاشارة إلى أنه اذا كانت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تشكل نموذجا موفقا يمكن للدول الأطراف الاعتماد عليه لتوحيد تشريعاتها

الجزائية الوطنية في مجال الجرائم الالكترونية أو على الأقل لتحقيق التقارب فيما بين هذه التشريعات إلا أنها وللأسف الشديد بقيت حبر على ورق ولم تدخل حيز التنفيذ إلى يومنا هذا بسبب عدم بلوغها النصاب القانوني المقرر لذلك، والمتمثل في التصديق عليها من طرف سبع دول عربية على الأقل.

المبحث الثالث: الجهود الاتفاقية والتشريعية على المستوى الدولي
ابرز الجهود التي بذلت على الصعيد الدولي لمواجهة الجرائم الالكترونية تمثلت في جهود الامم المتحدة (المطلب الاول)، ومنظمة التعاون والتنمية الاقتصادية (المطلب الثاني).

المطلب الاول: جهود منظمة الامم المتحدة
حظيت الجريمة الالكترونية باهتمام منظمة الامم المتحدة منذ مؤتمرها السابع الخاص بمنع الجريمة ومعاملة المجرمين المنعقد بمدينة ميلانو الايطالية في 1985، حيث كلفت لجنة الخبراء العشرين بدراسة موضوع حماية المعالجة الآلية والاعتداء على الحاسب الآلي (البشري ومحسن، 1998، صفحة 19).
وقد عرض تقرير هذه اللجنة على المؤتمر الثامن الذي عقد بهافانا في عام 1990، وتمت الموافقة عليها ثم أصدرتها منظمة الأمم المتحدة على شكل مجموعة من التوصيات بخصوص الجريمة الالكترونية، أكدت فيها بأن مواجهة هذا النوع الجديد من الاجرام يتطلب من الدول الأعضاء اعتماد عدة تدابير أهمها (الحن، 2011، صفحة 118)

- ضرورة تحديث القوانين الموضوعية والاجرائية التي تتناول هذا النوع الجديد من الجرائم والعمل على تحسين أمن المعلومات والوقاية المتعلقة بالحسابات الآلية وشبكات الانترنت المتصلة بها.
- وضع التدابير الوقائية والأمنية لمنع الجريمة مع مراعاة خصوصية الأفراد واحترام حقوق الانسان.

-توعية الجماهير بخطورة الجريمة الالكترونية و أهمية مكافحتها.



تنظيم دورات تدريب مكثفة لرجال القضاء والأمن حول تقنيات وفنيات التصدي مثل هذه الجرائم.

-التعاون مع المنظمات المهتمة بهذا الموضوع، وادراج ابجديات الاعلام الآلي واستخدام الحواسيب ضمن المناهج المدرسية.

واعتمدت لجنة الامم المتحدة في عام 1996 قانون الانسيترال النموذجي بشأن التجارة الإلكترونية، الذي يعتبر مرجعا مهما للدول في مواجهة جرائم الانترنت في مجال التجارة الالكترونية، وقد كان الهدف الرئيسي من وضع هذا القانون هو تعزيز تنسيق وتوحيد القانون التجاري الدولي بغية ازالة أية عقبات لا لزوم لها أمام التجارة الدولية تنتج عن أوجه القصور والاختلاف في القانون المتعلق بالتبادل التجاري، وأن يكون نموذجا تهتدي به البلدان يتعلق بتقييم وتحديث جوانب معينة من قوانينها وممارستها في ميدان العلاقات التجارية، ومساعدة جميع الدول على تحسين تشريعاتها وتدارك المساوئ الناجمة عن قصور التشريعات على الصعيد الوطني مع تقديمه للمشرعين الوطنيين كمجموعة من القواعد المقبولة دوليا في هذا المجال. واستمرارا في هذا المسار أصدرت اللجنة ذاتها القانون النموذجي بشأن التوقيعات الالكترونية في عام 2001 باعتباره صكا قانونيا جديدا مستمد من القانون الانسيترال النموذجي بشأن التجارة الالكترونية ومتسقا مع أحكامه وبشكل مفصل (محسن، 2007، صفحة 54).

و عقدت منظمة الامم المتحدة مؤتمرا في بودابست عام 2000 أسفر عن ابرام الاتفاقية الخاصة بمكافحة اساءة التكنولوجيا لأغراض اجرامية رقم 55/63 في 18 و 19 ديسمبر 2000.

كما عقدت في الفترة بين 12 و 15 ديسمبر 2000 مؤتمرا دوليا يضم الشخصيات السياسية للحكومات المصادقة على اتفاقية الامم المتحدة الخاصة بالجريمة عبر الوطنية، بعنوان تحديات الجريمة السيبرانية العابرة للحدود، ومن أهم المسائل التي تمت مناقشتها في هذا المؤتمر هي ضرورة حصر واحصاء كل الافعال المجرمة

التي تعد من قبيل الجرائم العابرة للحدود واعدادها في قائمة تضع في متناول علم جميع الاعضاء حتى يتم ادراجها في نصوصها الداخلية.

وعلى نفس المسار عقدت منظمة الامم المتحدة بالبرازيل في الفترة الممتدة من 12 الى 19 افريل 2010 مؤتمرها الثاني عشر حول منع الجريمة والعدالة الجنائية الذي دارت فيه مناقشات عميقة بخصوص حصيلة تطورات استخدام العلم والتكنولوجيا من جانب المجرمين بالمقارنة مع المجهودات المبذولة من طرف السلطات المختصة في مكافحة الجريمة الحديثة بما فيها الجريمة الالكترونية.

وقد دعت لجنة منع الجريمة والعدالة الجنائية الى عقد اجتماع دولي لفريق من خبراء حكوميين مفتوح العضوية في الفترة الممتدة من 17 الى 21 جانفي 2011 اين تولى الفريق بإجراء دراسة مفصلة لظاهرة الجريمة الالكترونية، بداية من تحليل هذه جمع المعلومات والاحصائيات المتعلقة بها تحدياتها، ثم عرج الى ابراز مدى مواكب التشريعات الوطنية خاصة المتعلقة بإجراءات التحقيق وجمع الأدلة الالكترونية، مسئولية مزودي خدمات الانترنت لظاهرة الاجرام الالكتروني، ومكانة التدابير الوقائية والتعاون الدولي والمساعدة التقنية الدولية في مواجهة هذه الجرائم، وكذا دور القطاع الخاص في الحد منها، وخلصت الدراسة بتقديم حلول مناسبة للمشكلات التي تعيق المواجهة الفعالة للجريمة الإلكترونية. وقد دونت نتائج هذه الدراسة في تقرير مفصل قدم الى أمانة منظمة الامم المتحدة التي وضعت تحت تصرف جميع الدول الاعضاء لتستفيد منه كمرجع في التصدي للإجرام الالكتروني (جمال، 2018، صفحة 273)

وبالإضافة الى جهود منظمة الامم المتحدة من خلال مؤتمراتها التي تعنى بخلق تقارب وتواءم بين التشريعات العقابية للدول الاعضاء من خلال ايجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة بصفة عامة والجريمة الالكترونية بصفة خاصة تبذل الوكالات والمنظمات العالمية تحت لواء الامم المتحدة مجهودات لا يستهان بها في هذا المجال، نذكر منها المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المتعقد في ريو دي جانيرو عام 1994،

والذي خرج بالعديد من التوصيات في مجال القانون الجنائي الموضوعي، منها ما يتعلق بضرورة وضع قائمة بالحد الأدنى للأفعال المعتبرة من قبيل الجرائم الالكترونية، ووجوب تحديد الجهات التي تتولى التفتيش والضبط فيها، مع ضرورة وضع القواعد المتعلقة بالإثبات الالكترونية حجية ومصداقية الادلة الإلكترونية امام القضاء (الحن، 2011، صفحة 188).

كذلك مجهودات لجنة حقوق الطفل التابعة لمنظمة الامم المتحدة التي أبرمت اتفاقية حول حقوق الطفل والوقاية من الجرائم الالكترونية التي ترتكب في حق الطفولة كاستغلالهم في المواد الاباحية عبر الانترنت.

المطلب الثاني: جهود منظمة التعاون والتنمية الاقتصادية

في عام 1980 وضعت منظمة التعاون و التنمية الاقتصادية دليل تشريعي يتضمن مجموعة من قواعد ارشادية لحماية الخصوصية ونقل البيانات عبر وسائل الاتصال الالكترونية وأوصت الدول الاعضاء ادراجها ضمن تشريعاتها الداخلية والالتزام بها، ومن بين هذه القواعد (Mohamed, 2009, p. 308):

-ضمان أمن وحماية المعلومات الخاصة للأفراد ضد كل اختراق، ضياع، اتلاف، أو تعديل دون ترخيص.

-الحق في الخصوصية مضمون ولا يجوز الاطلاع على المعلومات الخاصة للأفراد أو افشائها إلا في اطار القانون بعد علمهم وموافقتهم على ذلك.

-عدم جواز استعمال المعلومات الخاصة للأفراد لأغراض أخرى غير تلك التي تم الحصول عليها من اجلها.

وفي عام 1986 اصدر مجلس المنظمة تقريراً حول الغش الالكتروني تم من خلاله تشخيص وضع السياسة التشريعية الجنائية القائمة لدى عدد من الدول الاعضاء في هذا المجال، واقترح قائمة تتضمن الحد الأدنى لأفعال سوء استخدام الحاسب الآلي التي يجب على الدول الأعضاء أن تجرمها وتفرض عليها عقوبات في قوانينها الداخلية، من أهمها الاستخدام أو الولوج غير المصرح به الى نظام الحاسب والمعلومات المخزنة داخله، الافشاء غير المرخص به للمعلومات المعالجة آلياً ونسخ

أو تعديل أو إتلاف أو تخريب ما تحتويه من بيانات، الاعاقة غير المشروعة للوصول الى مصادر الحاسب كمنع أو تعطيل استخدام الحاسب أو برامج أو البيانات المخزنة فيه.

وفي عام 1992 اصدرت منظمة التعاون والتنمية الاقتصادية توصية ارشادية تتضمن جملة من التدابير الفعالة لمواجهة الجرائم المرتكبة عبر الانترنت و التي أوصت الدول الاعضاء بضرورة ادراجها ضمن قوانينها العقابية الوطنية وهي كالتالي: -تجريم التلاعب في البيانات المعالجة ومحوها.

-منع التجسس المعلوماتي ويندرج تحته جمع أو اقتناء أو استعمال الغير المشروع للمعطيات الالكترونية.

-حظر التخريب المعلوماتي بما فيه الاستعمال غير المشروع للحاسب الآلي اتلافه ومكوناته المادية والمنطقية وسرقة وقت الحاسب.

-تجريم الولوج والبقاء غير المرخص داخل برامج الحاسب، واعتراض استخدام المعطيات أو نقلها.

-تجريم القرصنة.

الخاتمة

إن الجرائم الالكترونية ذات طبيعة خاصة يصعب التصدي لأنها من الجرائم العابرة للحدود من جهة، ولأنها تنتشر وتتنوع بسبب التطور التكنولوجي والرقمي من جهة أخرى، فلا تستطيع كل دولة منفردة مواجهة هذه الجرائم، فلا يتأتى ذلك الا بتظافر جهود كل الدول، وقد تناولت هذه الدراسة مختلف الآليات الاتفاقية والتشريعية على الصعيد الاقليمي من خلال المجلس الاوربي وجامعة الدول العربية أو على الصعيد الدولي من خلال منظمة الامم المتحدة ومنظمة التعاون والتنمية الاقتصادية.

وقد توصلنا من خلالها الى مجموعة من النتائج نوردها على النحو الاتي:



- ساهمت الاتفاقيات الدولية مثل اتفاقية بودابست لمكافحة الجريمة الإلكترونية (2001) في توحيد المفاهيم القانونية وتعزيز التعاون بين الدول، كما عملت التشريعات الإقليمية، كتلك الصادرة عن الاتحاد الأوروبي أو جامعة الدول العربية، على ملء الفراغ التشريعي في العديد من البلدان.

- قلة الاتفاقيات المتعلقة بمكافحة الجريمة الإلكترونية، مما يجعل التعاون الاتفاقي دون المستوى المطلوب.

- الاتفاقيات المبرمة في مجال مكافحة الجرائم الإلكترونية قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب الآلي وشبكة الانترنت، ومن ثم تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك سلطات امن الدول.

كما توصلنا من خلال هذه الدراسة الى مجموعة من الاقتراحات هي:

- ضرورة تكثيف إبرام اتفاقيات دولية وإقليمية ثنائية ومتعددة الاطراف في مجال مكافحة الجرائم الإلكترونية، وحث على الانضمام إلى الاتفاقيات المبرمة في هذا الخصوص، مع مراعاة المصلحة الوطنية ومبدأ السيادة.

- وضع إطار قانوني موحد وفعال يمكن من خلاله محاسبة المتورطين في الجرائم الإلكترونية عبر كل الدول، لتحقيق الاستقرار والامن الدولي.

- مواءمة التشريعات الوطنية المنظمة للجرائم الإلكترونية مع أحكام الاتفاقيات الدولية ذات الصلة، لضمان تحقيق الانسجام التشريعي وتعزيز التعاون الدولي في مكافحة هذه الجرائم.

قائمة المصادر والمراجع:

المؤلفات:

- البشري، محمد الأمين؛ محسن، محسن عبد الحميد، معايير الامم المتحدة في مجال العدالة ومنع الجريمة، اكااديمية نايف للعلوم القانونية، الرياض، السعودية، 1998.

- بوحليط يزيد (2019)، جرائم الإلكترونية والوقاية منها في القانون الجزائري، في ضوء الاتفاقيات العربية لمكافحة الجرائم التقنية، دار الجامعة الجديدة، الاسكندرية، مصر.

- الحن طارق عبد الرؤوف محمد ، جريمة الاحتيال عبر الانترنت (الاحكام الموضوعية والاحكام الاجرائية)، منشورات الحلبي الحقوقية، بيروت، لبنان، 2011.
- الشوا محمد سامي ، (1994) ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، مصر.
- الشوابكة أمين أحمد محمد (2004)، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان الاردن.
- عبد الفتاح حجازي بيومي (2007) ، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي : دراسة قانونية معمقة في القانون المعلوماتي، دار الكتب القانونية، القاهرة، مصر.
- مراد عبد الفتاح ، شرح جرائم الكمبيوتر والانترنت، بدون دار النشر، 2005.
- هلال عبد الله أحمد (2000)، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة) ، دار النهضة العربية، القاهرة، مصر.
- Mohamed Chawki(2009), Combattre la cybercriminalité, Edition Saint-Amans, France .

المقالات:

- بولحية شهرزاد، مخلوفي رشيد، تحديات الجريمة الالكترونية في الجزائر، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 02، العدد 4، 2019.
- حسين بن محمد الشهري ، قانون دولي موحد لمكافحة الجرائم الالكترونية، المجلة العربية للدراسات الامنية والتدريب، مجلد 27، عدد 53، 2010.
- محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018.
- Myriam, QUEMENER(Mai 2010), conseil de l'Europe et lutte contre la cybercriminalité , Revue Expertises des système de l'information, Paris.

الملتقيات:

- أرحومة موسى مسعود ، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28-29 أكتوبر 2009.
- سكولمان كريستينا، المعايير الدولية المتعلقة بجرائم الانترنت (مجلس اوروبا) ، الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 2007.



-محسن سينا عبد الله (2007)، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 2007.

-هنروت جان فرنسوا ، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 20-19 جوان 2007.

-رسائل واطروحات جامعية:

-ابراهيم جمال ، التحقيق الجنائي في الجرائم الالكترونية، اطروحة دكتوراه، جامعة تيزي وزو، الجزائر، 2018.

-عفيفي يوسف خليل يوسف ، الجرائم الالكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة، رسالة ماجستير كلية الشريعة والقانون "الجامعة الاسلامية"، غزة ، فلسطين، 2013.

-فضل سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات، أطروحة دكتوراه، كلية الدراسات العليا، 2007.

-Nidal, ELCHAER (2003), la criminalité informatique devant la justice pénale, thèse de doctorat en droit, faculté de droit de l'université Poitiers, Paris