المواجهة الامنية لجرائم الانترنت دوليا

م.د ســـــامـــــان سلمـــان رحمـــن

ا.م.د ليث الدين صلاح حبيب

كلية القلم الجامعة/ قسم القانون

جامعة الانبار / كلية القانون

المقدمة

الانترنت ما هي الا شـبكة عالمية تمتاز بأنها عابرة للحدود وبالتالي فإن الجرائم المتصـلة بها ذات طابع عالمي لان اثرها يمتد الى اكثر من دولة, ولبحث التحديات التي تفرضـــها جرائم الانترنت يقتضـي دراسـته من عدة جوانب, وما يهمنا في هذا البحث وســنصـــب تركيزنا عليه هو الجهود الدولية والاقليمية, اذ لم يظهر التعاون الدولي في بداية انتشـــار خدمة الانترنت وانما ظهر الى الوجود بعد ســوء اســتخدام هذه الخدمة وبروز ارتكاب الجرائم بواســطته, وان اطلاق شــرارة هذه الظاهرة الخطرة وتأثيرها على الدول ولد الحاجة الفعلية للشــروع في وســائل وقائية وعقابية نابعة من تصــور كل دولة حسـب مصـالحها, فقد ركزت الدول في البدء بتقييد او حصر انتشار هذه الخدمة ولكن سهولة الحصول عليه ورخصـه وتعدد وسائل الاتصـال قلل من اهمية تلك الوسائل.

هـذا وقـد برز دور الجهود الامنيـة الى جانب الجهود القضـائية للحد من جرائم الانترنت مما دفع بـالمجتمع الـدولي متمثلا بـالمنظمـات الـدوليـة والدول لإصـدار قرارات تحث الدول للتعاون في هذا المجال ولمكافحة هذه الجرائم على المسـتوى الدولي والمحلي, اذ تم عقد مؤتمرات واتفـاقيـات في هـذا الصدد, والتي سنسلط الضوء عليها في ثنايا البحث, الى جانب صـــور ووســـائل مكافحة جرائم الانترنت دوليا بواسطة الجهد الامني.

1- **أهمية الدراسة:** تكمن اهمية دراسة الجهود الامنية في مجال مكافحة الانترنت بوصفه وسيلة مهمة ووقائية مكملة للجهود القضائية والتعاون الدولي في هذا المجال.

2- **اشكالية الدراسة:** تكمن اشكالية الدراسة في عدم توحيد الاجراءات الامنية واختلاف الدول في الاعتماد على المعلومات الامنية الى جانب تنازع الدول في مسائل سياسية او عسكرية, والاهم من ذلك تفاوت كبير في امتلاك الدول للوسائل التكنولوجيا التي تستخدم لهذا الغرض.

3- **منهجية الدراسة:** اعتمدنا في كتابة هذه الدراسة على المنهج التحليلي والوصفي, وذلك من خلال تحليل نصوص الاتفاقيات الدولية المتعلقة بها الى جانب وصف وقائع واجراءات ذات صلة بالموضوع.

4- **هيكلية الدراسة:** يتضمن الدراسة مبحثين الاول منه لدراسة الجهود الامنية لمواجهة جرائم الانترنت دولياً اما المبحث الثاني لدراسة الاسس الاتفاقية لمواجهة جرائم الانترنت دوليا.

المبحث الاول

الجهود الامنية لمواجهة جرائم الانترنت دولياً

بفضـــل الثورة التكنلوجية ومع ظهور الانترنـت, بـات الفضـــاء الالكتروني واحـدة من العناصـر الرئيسـة التي تؤثر سلبا وايجاباً في النظام الـدولي بمـا يحملـه من ادوات تكنلوجيـة تلعـب دوراً بارزا في التعبئة والحشد عالمياً, فظلا عن تأثيرها في القيم والسلوك.

حيث اصـبح من السـهولة لمسـتخدمي الانترنت القيام بأفعال جرمية او الاشـــتراك فيها بدون تجاوز الحدود الدولية التقليدية وان يوقعوا خســائر \\ غيرها من الجرائم, لذا بات من الضـــروري بحث ســـبل مواجهة جرائم الانترنت سواء كان اجرائيا ام اداريا..

المطلب الاول

المواجهة الامنية واجراءاتها

اتساع المجال الدولي وتعدد صور وأشكال الجرائم الالكترونية وصعوبة حصرها في ظل الوسائل المتجددة جعلت من هذا النوع من الجرائم في تطور وتشظي مستمر ترهق الدول عند مواجهتها وتبذل جهود كبيرة سواء كانت مادية او بشرية للحد منها[1], لكن هذا لا يعني استحالة وصعوبة بالغة لمواجهتها وللحد منها, وذلك بفضل تعاون دولي بين الاجهزة الامنية والاستخبارية بين الدول سواء كانت بناء على اتفاقيات ثنائية او اتفاقيات اوسع تضم دول او منضمات دولية سواء كانت عالمية او اقليمية.

[1] – د. علاء الدين شحاتة, التعاون الدولي لمكافحة الجريمة, القاهرة, 2000, ص 18 وما بعدها.

على هـذا الاســـــاس فـإن فكرة الجهود الدولية(تعاون دولي) ينبع من النتيجة التي يصـــــل اليها القانون الدولي الجنائي باعتبارها وسيلة لتحقيق الانســـــجام والتوافق مع اهداف المجتمع الدولي في الحد ومنع الجريمة للوصـــــول الى مجتمع مســـــتقر ووقايته من المجرمين, وهذا التعاون الامني يقتضـــي خطط وبرامج وتنفيذ لجهود جماعية امنية قســـرية[2], وعلى هذا الاســاس ســنعرج على خصــائص جرائم الانترنت واسس المواجهة الامنية لها

الفرع الاول

خصائص جرائم الانترنت

أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية, او داخل نظام حاسوبي, والجريمة تلك تشمل من الناحية المبدئية, جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية3, فالفرق بين هذه الجريمة والجرائم التقليدية يكمن فيما يلي:

1. محل الجريمة يقع على مكون مادي للحاسب الالي.
2. وقوعها على المكونات غير المادية في الوقت ذاته(البرامج والتطبيقات).
3. اداة الجريمة هو حاسب آلي[4].

لذا فالجريمة الالكترونية تتميز بخصـــــائص خطيرة عجلت من انتشارها ومن هذه الخصائص ما يلي:

1. سرعة تنفيذ الجريمة الالكترونية, اذ يكفي ضغط رز واحد لارتكابه بدون فاصل زمني.
2. صعبة اثبات ارتكابها وحتى صعوبة وارهاق لاكتشافها[5].

---

[2] – د. محمود شريف بسيوني, المدخل لدراسة القانون الجنائي الدولي, مكتبة المعهد العالي للدراسات الجنائية, سيركوزا– ايطاليا, 1990, ص1.

[3] – تعريف الجريمة الالكترونية وفقا لمؤتمر الامم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا عام 2000.

[4] – د. محمد سامي الشوا, ثورة المعلومات وانعكاساتها على قانون العقوبات, دار النهضة العربية, مصر, 1994, ص 11.

[5] – د. خالد حسن احمد لطفي, الارهاب الالكتروني آفة العصر الحديث والآليات القانونية للموجهة, ط1, دار الفكر الجامعي, الاسكندرية, 2018, ص 95.

3. تميزها بالتشويق والجاذبية, وقد تتعدى الى رغبة من الجاني لتحدي النظام التكنلوجي للحاسب الالي ومحاولة اختراقه عن طريق الوصول الى المعلومات او التلاعب لها[6], اذ تمثل الوسائل الالكترونية والتسويق لها ورخص اسعارها دافعا مغريا لاستعمالها, اذ يمكن لأي شخص من الحصول عليها حتى وان كانت ذا نوعية رديئة ولكن في النهاية تؤدي العمل ذاته, لذا فإن سهولة الاستخدام ورخص اسعارها معززا بالتشويق الذي يكتنف الفضاء الالكتروني وتحديدا التطبيقات ووسائل التواصل الاجتماعي التي كونت عالماً افتراضياً مبنياً على التشويق , لذا المجرم في الجريمة الالكترونية يبدأ فعله وينتهي منها وهو يعلم انه في عالم افتراضي شجعه وشوقه الوسائل الالكترونية.

4. تتخطى الحدود الدولية اي بمعنى ان اثارها تمتد حتى الى خارج الحدود لأن الانترنت وبالرغم من بعض التقييدات التي تفرضها بعض الدول[7] فإن الانترنت لا يزال تتميز خدماتها بأنها عابرة للحدود ويعد الجريمة الالكترونية (الانترنت) عالمية.

[6] – محمود احمد عبابنة, جرائم الحاسب الالي وأبعادها الدولية, ط1, دار الثقافة للنشر والتوزيع, الاردن, 2009, ص 25.

[7] – من الامثلة على ان هذه الجرائم عابرة للحدود, تمكن احد الهواة في اوروبا من حل شفرة احد مراكز المعلومات في البنتاجون (وزارة الدفاع الامريكية) ومن ثم اصبح المجال مفتوحا للعبث ببيانات هذا المركز : نقلا عن د. عمر الفاروق الحسيني, تأملات في بعض صور الحماية الجنائية لنظم الحاسوب الالي, الجوانب القانونية الناجمة عن استخدام الحاسب الالي في المصارف, اتحاد المصارف العربية, 1991.

الفرع الثاني

وسائل المواجهة الامنية

تتعدد الوسائل ولكن ما يهمنا في هذا البحث هي الوسائل الاكثر فاعلية لمواجهة هذه الجرائم ومنها:

اولا: الوسيلة الاعلامية: اجهزة الاعلام لها القدرة للتوعية ومكافحة الجريمة لما لها تأثير مباشر على المجتمع, وخصوصا الاجهزة الاعلامية التي تحظى بقبول واحترام المجتمع, وذلك من خلال برامجها الموجهة بهذا الصدد[8], فوسائل الاعلام باتت مندرجة في ميادين المعرفة واستمدت قوتها من التقدم التكنلوجي الهائل واصبحت لها شأنا بارزا في تكوين وتوجيه الفكر العالمي وتأثيرا على القيم وانماط السلوك والخلق, اذ تمتلك وسائل مرئية ومسموعة ومكتوبة تمكنها حرية الولوج الى حياة الفرد وتترك بصمتها على صياغة فكره وسلوكه[9].

لكن هذا الدور يجب ان يكون ممنهجا, وذلك عن طريق قيام اجهزة الامن بالتنسيق والاستعانة بوسائل الاعلام وخصوصا الاعلام الامني[10], او انشاء وسائل اعلام(ضل) بالرغم من خطورة الاجراء الاخير وخصوصا عندما تحيد اجهزة الامن عن اهدافها في هذا المجال وتستخدم هذه الوسيلة لتحقيق اهداف سياسية, ومع ذلك فالمهم على ان يعيوا إن فكرة الامن العام هي حاجة جماعية وفردية في آن وواحد وهي الهدف الذي يسعى له السلطة وينشد له المعارضة ايضاً.

ثانيا: الوسيلة الدينية: للوسائل الدينية تأثير على مكافحة الجريمة والتوعية بشأنها والتركيز على اضرارها والتحذير لمواجهة الافكار والآراء المنحرفة وذلك من خلال تنظيم وتوجيه الخطاب الديني في هذا المجال وذلك من خلال طبع ونشر مؤلفات دينية او نشر كتيبات و القاء خطب ووعظ والقيام بندوات او مؤتمرات , لأن رجل الدين ومن خلال ما يقوم به من دور تربوي رائد قائم على التبصير[11], وبدورنا نرى ان الوسائل الدينية مازالت تتميز

---

[8] – د. محمد محي الدين عوض, دراسات في القانون الجنائي الدولي, مجلة القانون والاقتصاد, القاهرة بدون عدد, 1993, ص 2.

[9] – د. احمد ضياء الدين خليل ود. عمر حسن عدس, ادارة الازمة المالية, دراسة تطبيقية لادارة الازمة المالية في موجهة الكوارث والارهاب, اكاديمية الشرطة , القاهرة, السنة الرابعة, 1997/1996, ص 93.

[10] – د. عبد الكريم الردايدة, الجرائم المستحدثة واستراتيجية مواجهتها, ط 1, دار ومكتبة الحامد للنشر والتوزيع, عمان, 2013, ص 194.

[11] – د. احمد الكبيسي, دور الشريعة في الوقاية من الجرائم, بحث تم تقديمه في ندوة الرباط, 25–28 تشرين الاول, 1982, ص 28.

بالحيوية في هذا المجال وخصوصا في الشرق الاوسط وافريقيا لأن مجتمعاتها لازالت تتأثر بالوسائل الدينية اكثر من المجتمعات الاخرى.

ثالثا: الوسائل الادارية: تتراوح هذه الوسائل باتخاذ قرارات ادارية او امنية وعلى سبيل المثال تستطيع الدول فرض رقابة الكترونية من خلال شركات توريد الانترنت للرقابة على الفعاليات الذي يقوم به المشترك في خدماتهم لمعرفة ما يقوم به هؤلاء من نشاطات مريبة من خلال برامج خاصة مثل تقنية (كارنيفور) العائدة لمكتب التحقيقات الفدرالية وغيرها من التقنيات[12], بالرغم من هذا الاجراء يعد انتهاك للحقوق الشخصية وخصوصية الفرد الذي يحميه اتفاقيات حقوق الانسان, لكن يمكن اعتماده كاستثناء من القاعدة العامة وفي حدود ضيقة كما فعل المشرع الامريكي وتشريعات اخرى[13].

وبدورنا نرى بان قرار المراقبة الالكترونية يجب ان تحقق توازن بين انتهاك الخصوصية والمصلحة العامة (مشروعة) التي تهدف المراقبة لتحقيقها, بالرغم من ان هذا التوازن قد يعتريها تفاوت لكن لا يجب ان لا يهمل او يصرف النظر عنها لان من طبيعة الادارة ان تغلو في سلطتها وتسيء استخدامها, مع تأكيدنا على ان رقابة المجازة من قبل القضاء في هذا المجال هو الحل الامثل سواء كانت سابقة او معاصرة او لاحقة للمراقبة.

المطلب الثاني

اسس وصور المواجهة الامنية

تترابط هذه صور والوسائل التي تستخدمها الدول والمنظمات المتخصصة في مكافحة جرائم الانترنت, وهذه الصور تطبق واقعياً في اقاليم الدول من خلال اجهزتها الامنية, وتتمم تنسيقيا على المستوى الدولي, وهذه الاسس هي بعضها اجرائية وبعضها ادارية.

الفرع الأول

الاسس الاجرائية

اولا: التحري وجمع المعلومات:

ان هذا الاجراء يعد من احد المصادر الرئيسية الممهدة لتبادل المعلومات

[12] - محمد عبد الكريم حسين, المسؤولية الجنائية لمورد خدمة الانترنت, ط1, منشورات الحلبي الحقوقية, 2017, ص 103.

[13] - د. طوني ميشال عيسى, التنظيم القانوني لشبكة الإنترنت دراسة مقارنة في ضوء القوانين الوضعية والاتفاقات الدولية, ط1, المنشورات الحقوقية /صادر, 2001, ص175.

والتعاون بين الدول في هذا المجال, اذ يقتضي وخطورة الجرائم المعلوماتية, التحري عن الفاعل او اي دليل او قرينة تدل على الفاعل, اذ بدون توافر معلومات موثوقة ومصنفة في التوقيت الملائم, يرهق عمل الاجهزة الامنية ويجعل جهودهم غير مجدية ويولد نتائج سلبية ومتأخرة في كثير من الاحيان.

فالمعلومات يجب ان تمحص وتبنى على اساس استخباري وان تمر بمراحلها المعروفة كالجمع والتصنيف والتحليل والتوجيه والحفظ من قبل مراكز متخصصة في الاجهزة الامنية والشرطية او الاستخبارية, وعلى سبيل المثال نجد في العراق تعدد لهذه الاجهزة كجهاز الامن الوطني او المخابرات(الامن السيبراني) و مركز الامن السيبراني في وزارة الداخلية[14]و مديرية الامن السيبراني والمعلوماتي في جهاز الآسايش في كوردستان العراق[15], فهذه الاجهزة على قدر كاف من التخصص والموارد البشرية يجعل منها مؤهلة للتعاون مع الاجهزة الموازية لها في الدول الاخرى لتبادل المعلومات حول جرائم الانترنت او السيبرانية في اطار اتفاقيات وتفاهمات سيادية دولية في هذا الشأن.

في الاطار ذاته نجد ان هناك اتفاقيات اقليمية ودولية تشجع التعاون الدولي وعلى سبيل المثال الاتفاقية العربية لمكافحة الارهاب لعام (1998)[16], التي اوجبت التعاون في مجال الجرائم الارهابية وفقا للتشريعات الداخلية ويمكن قياس خطورة جرائم الانترنت بالجرائم الارهابية نظرا لخطورتها وتأثيرها واستخدامها من قبل المجرمين ومن قبل الجماعات الارهابية ايضاً.

لذا يعد التحري من الوسائل الوقائية لهذه الجرائم ويسهل من مهام الاجهزة الامنية والشرطية داخل الدول من معرفة الفاعل وحيثيات الجريمة اولا ويوفر خزين معلوماتي للتعاون الدولي ثانيا17, مما يجعل الدول الراغبة لتوقيع اتفاقيات مع هذه الدول التي تمتلك اجهزة امنية وشرطية مدربة ومتخصصة

[14] – تم استحداث هذا المركز مطلع عام 2023 في وزارة الداخلية العراقية , لموجهة التحديات المتزايدة في عالم الانترنت والتكنولوجيا , ويرتبط بهذا المركز شعب الامن السيبراني في مديريات الشرطة في جميع المحافظات, نقلا عن مجلة الداخلية, ع 81, السنة الثانية عشر, ص 30, 2024.

[15] – هي مؤسسة امنية تعنى بالامن الداخلي في اقليم كوردستان العراق, يرأسها مدير بدرجة وزير, لها مديريات عامة تختص بمكافحة المخدرات والجرائم الالكترونية ومكافحة الارهاب والجريمة المنظمة, تم تأسيس هذا الجهاز بموجب قانون وتم تعديل قانونه بتشريع رقم (5) لعام 2011.

[16] – المادة 1/4 من الاتفاقية العربية لمكافحة الارهاب لعام 1998.

[17] – د. سناء خليل, الجريمة المنظمة والعبر الوطنية, الجهود الدولية ومشكلات الملاحقة القضائية, مجلة العدالة الجنائية القومية, ع2, مج39, 1996, ص100.

وتمتلك معلومات وقادرة للوصـــول الى المعلومة في الوقت المناسب, كل هذا يشكل حافزا للدول الاخرى ويجعل منها متلهفة للتعاون في هذا المجال ومن الممكن ان تستغل الدولة ذات الاجهزة الامنية الكفؤة مميزاتها للحصول على مكاسب امنية او عسكرية او اقتصادية لدولتها.

ثانيا: التدريب والخبرة الفنية:

تدريب الافراد في الاجهزة الامنية الشرطية هو اهم اسباب نجاح أي جهد امني للحد من الجرائم الالكترونية والعابرة للحدود, اذ بدون تدريب يجعل الاجهزة الشـــرطية غير فعالة, لذا يقتضـــي تعاون ثنائي اذا كانت هنالك اتفاقية امنية ثنائية مع دولة اخرى او تعاون جماعي سـواء كانت اتفاقية شـارعة او عامة وعلى ســبيل الذكر فإن منظمة الشـــرطة الجنائية الدولية(الانتربول) تقدم الدعم لأفراد أجهزة إنفاذ القانون في البلدان الأعضاء ليكتسبوا المعارف والكفاءات وأفضــل الممارســات التي يحتاجون إليها للتصـــدي للتحديات الراهنة بهدف مواكبة عالم الجريمة ســـريع التغير، وعلى أجهزة الشـــرطة أن تنهض بكفاءاتها باسـتمرار، وأن تتمكن من تسـخير الأدوات والنظم التقنية المتطورة التي توفرها لها، وأن تحرص على أن تكون أحدث البيانـات دائمـا في متناولها[18].

حيث تغطي فعاليات التدريب وكذلك بنـاء القـدرات جميع منـاطق العـالم وفي كـل مجـالات الإجرام، بـدءا من توفير الخبرات المتخصصـة وأدوات الإنتربول وخدماته ووصـولا إلى تعزيز العمـل المحترف والمســـاواة بين الجنسـين والاسـتدامة, تتمحور أنشـطة التدريب على مبادرتين رئيســيتين تســتندان إلى معايير الجودة[19]:

1. أكاديمية الإنتربول الافتراضية: وهي المنصة الرقمية للتعليم.
2. أكاديمية الإنتربول العالمية: وهي شبكة شريكة مع الانترنيت
3. قبول من الشركاء الإقليميين في التدريب.

ثالثاً: تبادل المعلومات وانشاء مراكز استجابة للطوارئ الالكترونية:

[18] – د. قزران مصطفى ود. زرقين عبد القادر, الاليات الدولية لمكافحة الجريمة الالكترونية, مجلة صوت الحق, مج 8, ع2, ص1226, 2022.

[19] – الموقع الرسمي للشرطة الجنائية الدولية(الانتربول): https://www.interpol.int/ar/2/6

يتم تبادل المعلومات بالوسائل التقليدية بواسطة المخاطبات الرسمية او بالوسائل المستحدثة كالبريد الالكتروني او انشاء قاعدة بيانات تشارك في ادارتها الدول المتعاقدة, حيث يتم اشباع هذه القاعدة بالمعلومات بصورة مستمرة بالإضافة الى امتيازها بخاصية تتبع الطلبات بشأن المتهمين في الجرائم الالكترونية, لذلك تحتاج الاتصالات الشرطية والامنية الى هذه الوسائل لتتمكن من التواصل فيما بينها[20].

هذا ويعد الانتربول[21] نموذج حي عن التعاون الدولي في تبادل وتعقب المجرمين, حيث تستهدف هذه المنظمة تأكيد وتشجيع الدول للتعاون من خلال اجهزتها الشرطية[22] من خلال جمع المعلومات وضبط المجرمين الصادر بحقهم قرارات قضائية واحضارهم للمثول امام المحاكم وتقديم الدعم في مجال الادلة الجنائية وغيرها من الاجراءات الشرطية الخاصة في هذا المجال[23].

بالإضافة الى منظمات اخرى كمنظمة الدولية لضباط الجرائم المالية التي تختص بجمع المعلومات الاستخبارية في مجال جرائم الاموال, وكذلك منظمة(يوروبول) التي تعنى بمحاربة الجريمة المنظمة والعابرة للحدود، ويتألف من وحدات أمنية تُساهم بها الدول الأعضاء في الاتحاد الاوروبي[24].

لكن هذا لا يعني ان تبادل المعلومات يمر بيسر وانما هنالك معضلة أساسية في مجال الاستخبارات, وهي تردد الدول في تبادل المعلومات الاستخبارية المهمة لأن ادارة المعلومات المتعلقة بالأمن كانت ولازلت لدى بعض الدول تعد جزءاً أساسياً من السيادة الوطنية, ولكن وفي الوقت ذاته نجد ان هذه الدول لديهم مصلحة قوية بشكل متزايد

[20] – في هذا المضمار, فقد نصت اتفاقية الامم المتحدة لمكافحة الفساد. المادة 48/ اولا على: تتعاون الدول الاطراف فيما بينها تعاونا وثيقا بما يتوافق مع نظمها القانونية والادارية الداخلية, كي تعزز فاعلية تدابير إنفاذ القانون من اجل مكافحة الجرائم المشمولة بهذه الاتفاقية, وتتخذ الدول الاطراف على وجه الخصوص تدابير فعالو لأجل: أ- تعزيز قنوات الاتصال بين سلطاتها واجهزتها ودوائرها المعنية, وانشاء تلك القنوات عند الضرورة, من اجل تيسير تبادل المعلومات بطريقة آمنة وسريعة عن كل جوانب الجرائم ...

[21] – ينظر الموقع الرسمي لمنظمة الشرطة الجنائية الدولية : https://www.interpol.int/ar

[22] – بعد انضمام جمهورية العراق لعضوية المنظمة الدولية للشرطة الجنائية في دورة انعقاد الجمعية العمومية رقم (36) المنعقدة في اليابان عام 1997, فقد تم استحداث مديرية للشرطة العربية والدولية في وزارة الداخلية ويكون ارتباطه بوزير الداخلية, الى جانب فتح مكاتب خاصة لها في جميع المحافظات للتنسيق وتبادل المعلومات الامنية والجنائية وملاحقة وتنفيذ مذكرات القبض مع نظيراتها في البلدان الاخرى وكذلك مع منظمة

[23] – د. سليمان احمد فضل, المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية(الانترنت), دار النهضة العربية, 2013, ص415.

[24] – اليوروبول اختصار للتسمية التي تطلق على "المكتب الأوروبي للشرطة"، وهو جهاز أمني مهمته تنسيق الجهد الأوروبي لمحاربة الجريمة المنظمة والعابرة للحدود، ويتألف من وحدات أمنية تُساهم بها الدول الأعضاء في الاتحاد الاوروبي, تأسست في عام 1999 بهدف محاربة "الإرهاب" والجريمة المنظمة، ومواجهة التحديات التي تواجه الأمن الأوروبي عموما، ولا سيما في ضوءِ مبدأ حرية التنقل داخل الفضاء الأوروبي كما حددته اتفاقيات, تقع مقرها في مدينة لا لاهاي الهولندية, للمزيد ينظر الموقع الرسمي: https://www.europol.europa.eu

في تبادل المعلومات الاســـتخباراتية نظراً لمخاوفهم الأمنية المماثلة.

لـذا لا يمكن الركون واليـأس في هـذا المجـال وخصـوصـا اذا اتفقت مجموعة من الدول على تبادل المعلومات وتفعيل الاجهزة الامنية المشـــتركة, ففي هذا المجـال فقد اتفقت دول الاتحـاد الاوروبي على اســـتراتيجيـــة امنيـــة للأعوام(202-2025) في أعقاب اسـتراتيجية الاتحاد الأمني المعتمدة في يوليو 2020، حيث تم قبول تعزيز ولاية (اليوروبول) من أجل الســـماح للوكالة بدعم ســـلطات إنفاذ القانون الوطنية بشـكل أفضـل بالمعلومات والتحليل والخبرة, واعتمد مقترح آخر وهو تمكين اليوروبول من إصدار إنذارات في نظام معلومات (شـــنغن) على أســـاس معلومات من مصادر دولية ثالثة[25].

رابعاً: عمليات ميدانية مشتركة:

تتضـــمن هذه الوســـيلة عمليات ميدانية ســـواء كانت مشـتركة من اجهزة الامن والشـرطة في اطراف التعاون الامني الدولي او من خلال تنفيذ مباشر من اجهزة لدولة ما بإشراف اجهزة الدولة صاحبة السيادة, وهـذه العمليـات لتعقـب المتهمين او تعقـب وجمع الادلة وضبطها[26], فالعامل المشترك في هذه الوسيلة او سـابقاتها, هو ان المتهمين في الجرائم المعلوماتي (الالكترونية- الانترنت) قد يكونون خلف الحدود او يرتكبون الفعـل المـادي للجريمـة في دلو وتتحقق النتائج في دول اخرى.

الفرع الثاني

الاسس الادارية والقضائية

اولاً: تسليم المجرمين:

من المعروف بـأن تســـليم المجرمين هو احدى اشـــكال التعاون القضـــائي الدولي لمكافحة الجريمة, ونتيجة لتشـــظي جرائم الانترنت, بات من الضروري وجود تعاون دولي في هذا المجال ويشترط لهذا الاجراء تجريم الفعل المطلوب التسليم بشأنه هو ان يكون الفعل جريمة في كلتا الدوليتين المتعاونتين وان تقوم الدولة طالبة التســـليم بمحاكمته ولا يكون الجريمة ذا باعث سياسـي ولا يكون المتهم من رعايا الدولة المطلوب منها التســـليم, مع اخذ بـالاعتبار الاجراءات القـانونيـة من مخـاطبـات رســـميـة وفق القنوات الرسـمية للطلب والتسـلم, ولكن هذا الاجراء التقليـدي قـد لا يفي بـالغرض في مجـال جرائم

[25] – المركز الاوروبي لدراسة مكافحة الارهاب والاستخبارات, مكافحة الإرهاب في أوروبا . أهمية تبادل المعلومات, 21ابريل 2023, على الموقع الالكتروني:
https://www.europarabct.com/?p=87886

[26] – د. عادل عبد العال ابراهيم خراشي, اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها, دار الجامعة الجديدة, 2015, ص 24.

الانترنت وذلك لسرعة ارتكاب الجريمة واختفاء الادلة والمتهم لذا كان لزاما البحث عن وسيلة ادارية (تسليم اداري) [27]عوضا عن التسليم القضائي او القانوني بحيث يكون في اطار امني وبوصفه عملا من اعمال السيادة او تدبير من تدابير السلطة التنفيذية لتقرر تسليم المجرمين من عدمه استنادا الى معاهدة دولية او اتفاقية ثنائية وفقا لاعتبارات خاصة كأن تكون سياسية او امنية.

لذا لا يخفى بأن هذا النوع من التسليم له ايجابيات وهي السرعة في التنفيذ وعدم التعقيد في الاجراءات, اما سلبياتها فتتلخص في هدر حق المتهم في الدفاع عن نفسه لدى الدولة المطلوب منها التسليم, كذلك امكانية محاكمة المتهم بتهم اخرى غير التي سلم من اجلها, كذلك تعد هذه الطريقة في التسليم يحومه السرية والكتمان لذا قد يستغل لأغراض سياسية غير قضائية او قانونية ولا يخض للرقابة.

ثانيا: موائمة تشريعية:

تتمثل بوضع الدول لتشريعات خاصة للجرائم الالكترونية مثل قوانين حماية البيانات وقوانين الجرائم المعلوماتية, بالإضافة الى تسهيل الاجراءات القضائية للإنابة او تسليم المجرمين.

المطلب الثاني

الأساس الاتفاقي لمواجهة جرائم الانترنت دوليا

الاساس الاتفاقي يعتمد على اتفاقيات ومعاهدات عامة بهدف تنسيق الجهود ما بين الدول لمكافحة الجرائم الانترنت عبر الحدود, ونظرا لطبيعة الانترنت العالمية فإن التعاون الدولي ضرورة لمواجهة هذه التحديات.

لكل ما اشرنا اليه فقد اضحت ضرورة ملحة, تعاون دولي في مجال مكافحة جرائم الانترنت والوقاية منها وذلك لعجز الدول فرادا من السيطرة عليها وعلى اثارها الممتدة, ولكن هذا التعاون قد لا يكون هيناً بل يواجه عقبات اجرائية وقانونية وسياسية, غير ان هذه العقبات لا تنفي وجود جهود امنية دولية مبذولة في هذا الشأن , وهذا ما سنعرج عليه تباعاً:

المطلب الاول

الاساس الاتفاقي على مستوى الدول

[27] - امير فرج يوسف, الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت, ط1, مكتبة الوفاء القانونية, مصر- الاسكندرية, 2011, ص 450.

خطورة جرائم الانترنت عجل على الدول جهودها لوضع اطار اتفاقي سواء كان هذا الاطار عاما كالمعاهدات العامة او خاصا كالاتفاقيات الخاصة سواء كانت ثنائية او اكثر, ولنوضح هذه الاسس سنعرج على بعض هذه المعاهدات والاتفاقيات تالياً:

الفرع الاول

المؤتمرات والاتفاقية العامة

اولاً: الاتفاقية الخاصة بحماية الافراد من اساءة استخدام البيانات المعالجة الكترونيا لعام (1981) التي تعنى مبادئها [28] بـ :

- توفير الحد الادنى من الاحتياطات الواجب توافرها في القوانين الداخلية لأطراف المعاهدة لحماية الفرد من اساءة استخدام الحاسب وبياناتها.
- النص على مراعاة المشروعية من حيث مصدر الحصول على البيانات الشخصية.
- اتباع الوسائل والطرق الفنية السليمة في استخدام البيانات الشخصية.

بالرغم من اهمية هذه الاتفاقية لاحتوائها على اطر واسس مهمة للتعاون الدولي وسيما الامني منها لموجهة جرائم الانترنت, إلا ان البعض يشكك في فاعليتها مقارنة بالاتفاقيات الخاصة بالجرائم التقليدية ويعزون السبب الى ان الاتفاقية اعلاه لم تحوي على مبادئ عامة تحكم وتنظم الفضاء الالكتروني فظلا عن عدم الاتفاق

[28] – اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية لعام 1981.

بين الدول على اليات محددة لتطبيق بنود الاتفاقية29, وبدورنا نرى بأن الاتفاقية كانت مهمة في حينها لأنها كانت قد بحثت جرائم مستحدثة الا وهي جرائم الانترنت مقارنة ببوادر وبداية انتشار تقنية الانترنت في العالم بصورة واسعة, وقد ازدادت اهمية الاتفاقية تباعا وتصاعديا مع بروز خطورة سوء استخدام تقنية الانترنت وتشظي استخداماتها سيما وان هذه الاتفاقية تعد استكمال للمعاهدات الخاصة بتسليم المجرمين والمساعدة المتبادلة بين الدول في المسائل الجنائية.

ثانياً: المؤتمر الدولي للجمعية الدولية لقانون العقوبات عام (1984) في البرازيل وقد تمخض عن المؤتمر العديد من الاسس الواجب مراعاتها لمكافحة جرائم المعلوماتية ومنها30:

1. تحديد السلطة المختصة بالتفتيش في مجال تكنلوجيا المعلوماتية.
2. اعطاء المشروعية للسلطات العامة بالولوج الى نظام الحاسب الالي واعتراض الاتصالات وذلك لغرض تقديمه كدليل امام المحاكم المختصة.
3. لدى اتخاذ الاجراءات الامنية يجب مراعاة الجدوى الاقتصادية وخصوصية مستخدم نظام الحاسبة قبل اجراء تفتيش وولوج الى نظام حاسبة.
4. موائمة قواعد الاثبات التشريعية مع قواعد الاثبات الالكتروني مع التركيز على مصداقية الاخيرة طبقا للقواعد العامة للإثبات.

[29] – نقلا عن اياد خلف محمد, المنازعات الدولية ذات الطابع الالكتروني, رسالة ماجستير, جامعة كركوك, كلية القانون والعلوم السياسية, 2019, ص 78.

[30] – نقلا عن د. محمود رجب فتح الله, الوسيط في الجرائم المعلوماتية, دار الجامعة الجديدة, 2019, ص223.

ثالثاً: اتفاقية مجلس اوروبا للجريمة الالكترونية بودابست لمكافحة جرائم المعلوماتية لعام 2001[31]:

تعد هذه الاتفاقية اســـتجابة جماعية لخطورة الجرائم الالكترونيــة , دخلــت حيز النفــاذ عــام 2004حيث تهدف هذه الاتفاقية الى[32]:

1. سعي وحث الدول على توحيد تشريعاتها للوقاية من جرائم المعلوماتية.
2. اهمية التعاون الدولي في مجال المكافحة.
3. مراعاة حقوق الانسان الاساسية وحرية الرأي وخصوصية مستخدم الحاسب الالي.

الفرع الثاني

الاسس الادارية الحكومية

من القرارات الحكومية في هذا الصدد, فقد مجلس وزراء داخلية العرب اصدر جملة توصيات وهي[33]:

1. تتولى الدول تشكيل هيئة او لجنة داخل دولها من اجهزتها المختصة, مهمتها وضع التدابير لضمان سلامة استخدام الحاسوب ورسم الخطط الكفيلة لمكافحة الجرائم التي ترتكب بواسطة الحاسوب والانترنت.
2. تشريع قواعد قانونية لتجريم الجرائم الالكترونية, وتحديد العقوبات الرادعة لها.

31 - اتفاقية مجلس اوروبا للجريمة الالكترونية المعروفة باتفاقية بودابست لعام 2001 والتقرير التفسيري الملحق بها.

32 – للمزيد يرجى مراجعة الموقع الرسمي لمجلس اوروبا: http://www.coe.int/t/e/legal-affairs/legal-co-operation

33 – مؤتمر مجلس وزراء الداخلية العرب رقم 288, المنعقد في دولة المقر/ تونس بتاريخ 1998/1/5.

3. حث الدول للتعاون لتشكيل هيئة او لجنة مهمتها التنسيق بين الدول لمكافحة وتتبع الجرائم الالكترونية.
4. انشاء لجنة في الامانة العامة لمجلس وزراء الداخلية العرب تتألف من اعضاء تمثل عدد من الدول مهمتها مراقبة ومتابعة وتوحيد التشريعات العربية بهذا الشأن, حيث تجتمع كلما دعت الحاجة لذلك[34].

ولا ننسى جهود مجموعة الدول الثماني(G8) من خلال اجتماعات وزرائها الداخلية والاتفاق على مبادئ عامة في مجال مكافحة جرائم الانترنت مثل(عدم توفير ملاذ لمجرمي الانترنت والتنسيق الدولي بشأنها وتدريب الموظفين لتتبع وملاحقة وتوفير المستلزمات المادية من اجهزة وبرامج) والاتفاق بشأن خطط عمل في هذا المجال, من خلال بيان نظم حماية المعلومات عام 2002[35].

ولا ننسى جهود الاتحاد الدولي للاتصالات, حيث شرعت بوضع برامج للامن الالكتروني العالمي من خلال استراتيجية لتطوير التشريعات السيبرانية قابلة للتطبيق محليا وعالميا.

المطلب الثاني

الاسس على مستوى المنظمات الدولية

عقب انشاء منظمة الامم المتحدة عام 1945 اتخذت خطوات عملية من خلال المجلس الاقتصادي والاجتماعي التابع لها في رسم سياسة لمنع الجريمة وتحقيق العدالة على المستوى الدولي وقد توالت هذه الجهود حتى تم انعقاد مؤتمرات الامم المتحدة لمنع الجريمة ومعاملة المجرمين

[34] – مؤتمر وزراء الداخلية العرب رقم 416 المنعقد في دولة المقر/تونس بتاريخ 2004/1/30

[35] - د. عادل مشموشي, جرائم المعلوماتية, ط1, المؤسسة الحديثة للكتاب, طرابلس, 2019, ص446.

عام1970 في اليابان ثم عام 1985 في ايطاليا ومؤتمر هافانا عام 1990 حيث تخصصت مبادئها حول تحديث القوانين الجنائية وتحسين امن الحاسب الالي وتدابير المنع والتدريب على مكافحة بجرائم الحاسب وضرورة تعاون الدول في هذا المجال وعلى هذا النمط فقد عقد مؤتمر القاهرة عام 1995 ثم مؤتمر بودابست بشأن معاملة المجرمين والتي نوقشت فيها جرائم الحاسب الالي واكدت فيها وجوب العمل على الحد منها36.

الفرع الاول

قرارات المنظمات الدولية

في مجال تكنلوجيا المعلومات والوسائل السلكية واللاسلكية, فقد بحث الجمعية العامة للأمم المتحدة في دوراتها (53 و54 و55-64) والتي تركز على التطور في مجال المعلومات وتأثيرها على الامن الدولي ودعت الدول الى التعاون لمواجهة التي تجتاح ميدان الامن المعلوماتي 37 , فيما اصدر المجلس الاوروبي عام (1995) في مجال مشاكل الاجراءات الجنائية المتعلقة بتكنلوجيا المعلومات, اذ اوصت الدول بالعديد من التوصيات ومن اهمها[38]:

[36] – د.عبود السراج, مكافحة الجرائم الاقتصادية والظواهر الإنحرافية, اكاديمية نايف العربية للعلوم الامنية, الرياض, 1998, ص109.

[37] – الوثيقة A/RES/54/49 صادرة عن الجمعية العامة للأمم المتحدة, دورة 45, البند 71, في 1999/12/1 متاح على الموقع الالكتروني: https://www.undocs.org/ar/A/RES/54/49

[38] – التوجيه رقم EC 46/95/الصادر عن البرلمان الأوروبي والمجلس بتاريخ 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرية حركة تلك البيانات، الاتحاد الأوروبي .

1. تشريع قواعد لتفتيش اجهزة الحاسب الالي.
2. ان تسمح التشريع المؤمل اقراره للسطات المختصة بضبط برامج معلومات الحاسب الالي.
3. ان يقتصر التفتيش على الاجهزة المرتبطة بالجريمة الالكترونية وان يكون ذلك ضروريا.
4. مراعاة السرعة والسرية والخصوصية لدى اجراء التفتيش.
5. تطوير وسائل التحقيق ليلائم الادلة الالكترونية.
6. تشكيل وحدات وتطوير الموارد البشرية في مجال جرائم الكومبيوتر.

هذا ويركز الاستراتيجية التعاون العربي والدولي لمواجهة جرائم الانترنت على محاور عديدة, اهما:

– التعاون الامني داخل الدولة الواحدة اي تعاون الاجهزة الامنية المتعددة الى جانب وجود تعاون بين مواطني تلك الدول مع اجهزة الامن.

– تعاون اجهزة الامن على المستوى الاقليمي على مستوى الدول العربية, من خلال لقاءات وندوات ودورات ومذكرات تعاون في هذا المجال.

– تعاون اجهزة الامن على المستوى الاقليمي مع اجهزة الامن على المستوى الدولي .

على سبيل المثال نورد عدد من قرارات الامم المتحدة بشان جرائم الانترنت وضرورة التعاون الدولي بشأنها: كقرار رقم(159) التي اصدرته الدورة التاسعة والاربعون للجمعية العامة للأمم المتحدة وسميت بإعلان نابولي الساسي لمكافحة الجريمة عبر الوطنية وقرار رقم (70) التي اصدرته الدورة الثالثة والخمسون للجمعية العامة للأمم المتحدة بشأن الاتصالات السلكية واللاسلكية وتأثيرها على الامن الدولي و قرار رقم (53) التي اصدرته الدورة السابعة والخمسون للجمعية العامة للأمم المتحدة بشأن الاتصالات

السلكية واللاسلكية وتأثيرها على الامن الدولي قرار رقم (63) التي اصدرته الدورة الخامسة والخمسون للجمعية العامة للأمم المتحدة بشأن مكافحة اساءة استخدام التكنلوجيا لأغراض اجرامية وقرار رقم (121) التي اصدرته الدورة السادسة والخمسون للجمعية العامة للأمم المتحدة بشأن تدفق المعلومات والثغرات التي قد تعتريها وتستخدم لأغراض اجرامية وقرار رقم (239) التي اصدرته الدورة السابعة والخمسون للجمعية العامة للأمم المتحدة بشأن نشر ثقافة امنية على مستوى العالم حول شبكة الحاسوب, وقرارات اخرى لا مجال للتعمق بشأنها.

الفرع الثاني

قرارات المنظمات الاقليمية

اصـــدرت منظمة الاتحاد الاوروبي توجيه بشـأن الهجمات السـيبرانية عام(2013) الذي شـمل تعريفا للجرائم الالكترونية وتحديد العقوبات بشـــأنها, فظلا عن اصدار لائحة النظام العام لحماية البيانات التي تهدف الى حماية الخصـوصـية للمسـتخدمين وتضمن فرض عقوبات على منتهكي البيانات.

المنظمة الدولية للمعايير (ISO): تطورت معـايير مثـل(ISO/IEC27001) لتعزيز الامن السـيبراني للمؤسـسـات وتحسـين سـياسـاتها الامنية وتطوير نظم ادارة امن المعلومات.

لذا نرى بأن الاتفاقيات الدولية والمعاهدات بهذا الشأن قد لا يكون كافيا نظرا لتعدد مجالات استخدام الانترنت وسوء استخدامها كأداة للجرائم, اذ لابد من تحـالفـات امنيـة سـيبرانيـة تتمم مـا بـدأتـه منظمـة الانتربول, وهذا البنيان لابد من توفير الوسائل التقنية والبشـــرية لتنفيذه على ارض الواقع, لتتيح للدول معا التصـــدي بفعالية للجرائم الالكترونية التي تتخطى حدودها وتعزيز الامن السيبراني العالمي.

الخـاتمـة

توصـــلنا من خلال البحث بـأن جرائم الانترنـت لازالـت تمثـل خطورة ملحـة وفي تتطور مستمر ويقابله وسائل وجهود متفاوتة من الدول للحد من هذه الجرائم وتتبع مرتكبيها وخصوصا في الشرق الاوســط وافريقيا نظرا لضـــعف الامكانيات المادية والتكنولوجيا في هذا المجال, الى جانب هذا فقد برز لدينا ســبب رئيســي لضــعف التعاون الامني في مواجهة ومكافحة جرائم الانترنت يعود الى اســباب ســياســية من جهة تتعلق بمصــالح الدول دائمة العضـــوية في مجلس الامن وعدم تبلور ارادة دولية في هذا الصـــدد وتحديدا الولايات المتحدة الامريكية وروسـيا وتعارض مصـالحهما للوصـول الى اتفاقية دولية شـاملة للحد من الهجمات والجرائم السـيبرانية

بالرغم من توصـــلهما لاتفاقية ثنائية عام (2013) لتجنب اية ازمة ســـيبرانية لكن نظرا لفقدان الثقة بينهما لم نرى اثار هذه الاتفاقية على المســـتوى الدولي, فجرائم الانترنت لابد وان تتم مكافحتها من النقطة التي تبدأ به وهي وجود الجاني داخل حدود دولة ما وبفعله يرتكب جريمة قد تتخطى حدود اكثر من دولة وتترك اثار في دولة اخرى, اذ نقطة البداية هي التي تبدء عندها التعاون الدولي وتحديدا الامني منها في مواجهة جرائم الانترنت, بالإضـــافة الى اســـباب قانونية تتمثل باختلاف وفوارق في الانظمة العقابية والاجرائية للدول.

ففي هـذا المجـال نقترح تكـاثف الـدول وســيما الدول الاقليمية ســواء كان على المســتوى القاري او القومي لعقد اتفاقات جماعية او ثنائية لتتبع ومكافحة جرائم الانترنت وتشـــكيل وحدات من الاجهزة الامنيـة والعســـكريـة لتنفيذ برامج وقـائيـة ولمكـافحـة هذه الجرائم, الى جـانـب تظـافر الـدول للضـــغط من خلال الجمعية العامة للأمم المتحدة على مجلس الامن والطلـب منهـا لحـث الـدول الاعضاء في المجلس على بلورة رأي يتسم بالعمومية لإصـــدار قرارات توجيهية للدول في مجال مكافحة جرائم الانترنت ورعاية اتفاقيات شارعة عامة في هذا المجال.

المصـــادر

المصادر العربية:

1. د. احمد الكبيسي, دور الشريعة في الوقاية من الجرائم, بحث تم تقديمه في ندوة الرباط, 25–28 تشرين الاول, 1982.
2. د. احمد ضياء الدين خليل ود. عمر حسن عدس, ادارة الازمة المالية, دراسة تطبيقية لادارة الازمة المالية في موجهة الكوارث والارهاب, اكاديمية الشرطة , القاهرة, السنة الرابعة, 1997/1996.
3. امير فرج يوسف, الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت, ط1, مكتبة الوفاء القانونية, مصر – الاسكندرية, 2011.
4. اياد خلف محمد, المنازعات الدولية ذات الطابع الالكتروني, رسالة ماجستير, جامعة كركوك, كلية القانون والعلوم السياسية, 2019.
5. د. خالد حسن احمد لطفي, الارهاب الالكتروني آفة العصر الحديث والآليات القانونية للموجهة, ط1, دار الفكر الجامعي, الاسكندرية, 2018.
6. د. محمود رجب فتح الله, الوسيط في الجرائم المعلوماتية, دار الجامعة الجديدة, 2019.
7. د. سليمان احمد فضل, المواجهة التشريعية والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية(الانترنت), دار النهضة العربية, 2013.
8. د. سناء خليل, الجريمة المنظمة والعبر الوطنية, الجهود الدولية ومشكلات الملاحقة القضائية, مجلة العدالة الجنائية القومية, ع2, مج39, 1996.
9. د. طوني ميشال عيسى, التنظيم القانوني لشبكة الإنترنت دراسة مقارنة في ضوء القوانين الوضعية والاتفاقات الدولية, ط1, المنشورات الحقوقية /صادر, 2001.
10. د. عادل عبد العال ابراهيم خراشي, اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها, دار الجامعة الجديدة, 2015.
11. د. عادل مشموشي, جرائم المعلوماتية, ط1, المؤسسة الحديثة للكتاب, طرابلس, 2019.

12.د. عبد الكريم الردايدة, الجرائم المستحدثة واستراتيجية مواجهتها, ط 1, دار ومكتبة الحامد للنشر والتوزيع, عمان, 2013.

13.د. عبود السراج, مكافحة الجرائم الاقتصادية والظواهر الإنحرافية, اكاديمية نايف العربية للعلوم الامنية, الرياض, 1998.

14. د. علاء الدين شحاتة, التعاون الدولي لمكافحة الجريمة, القاهرة, 2000.

15.د. عمر الفاروق الحسيني, تأملات في بعض صور الحماية الجنائية لنظم الحاسوب الالي, الجوانب القانونية الناجمة عن استخدام الحاسب الالي في المصارف, اتحاد المصارف العربية, 1991.

16. د. قزران مصطفى ود. زرقين عبد القادر, الاليات الدولية لمكافحة الجريمة الالكترونية, مجلة صوت الحق, مج 8, ع2, 2022.

17. د. محمد سامي الشوا, ثورة المعلومات وانعكاساتها على قانون العقوبات, دار النهضة العربية, مصر, 1994.

18.محمد عبد الكريم حسين, المسؤولية الجنائية لمورد خدمة الانترنت, ط1, منشورات الحلبي الحقوقية, 2017.

19. د. محمد محي الدين عوض, دراسات في القانون الجنائي الدولي, مجلة القانون والاقتصاد, القاهرة بدون عدد, 1993.

20.محمود احمد عبابنة, جرائم الحاسب الالي وأبعادها الدولية, ط1, دار الثقافة للنشر والتوزيع, الاردن, 2009.

21. د.محمود شريف بسيوني, المدخل لدراسة القانون الجنائي الدولي, مكتبة المعهد العالي للدراسات الجنائية, سيركوزا– ايطاليا, 1990.

الاتفاقيات الدولية:

1. اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية لعام 1981.
2. اتفاقية مجلس اوروبا للجريمة الالكترونية المعروفة باتفاقية بودابست لعام 2001 والتقرير التفسيري الملحق بها.

المصادر الالكترونية:

1. المركز الاوروبي لدراسة مكافحة الارهاب والاستخبارات, مكافحة الإرهاب في أوروبا . أهمية تبادل المعلومات, 21ابريل 2023, على الموقع الالكتروني:https://www.europarabct.com/?p=87886
2. الموقع الرسمي للشرطة الجنائية الدولية(الانتربول): https://www.interpol.int/ar/2/6
3. الموقع الرسمي للجمعية العامة للامم المتحدة, دورة 45, البند 71, في 1999/12/1 متاح على الموقع الالكتروني: https://www.undocs.org/ar/A/RES/54/49 .
4. موقع الرسمي لليروبول : https://www.europol.europa.eu

الموقع الرسمي لمنظمة الشرطة الجنائية الدولية : https://www.interpol.int/ar

Abstract

This study aims to identify international security efforts in the field of combating cybercrime and show their cross-border characteristics. In order to combat these crimes and their important impact, on the economic, military and security aspects, we touched on some collective and private international efforts in this field, in addition to some local efforts.

The countries of the world whether developed or developing, have expanded their common procedures to reduce these crimes, based on a set of treaties and conventions to confront and combat these crimes, including the Budapest convention on combating cybercrimes, which is one of the main international means in this regard, but other international efforts are necessary because of the unlimited specificity of these crimes and their link to technology, which has become constantly developing.

المستخلص

تهدف هذه الدارســـة الى التعرف على الجهود الامنيـة الـدوليـة في مجـال مكـافحـة جرائم الانترنت وبيان خصـائصـها العابرة للحدود, ومن اجل مكـافحـة هـذه الجرائم وتـأثيرهـا المهم على الجوانـب الاقتصـادية والعسكرية والامنية, اذ تطرقنا الى بعض الجهود الدولية الجماعية والخاصـــة في هذا المجال الى جانب الجهود المحلية

هذا فقد وسعت دول العالم سواء المتقدمة او النامية منها اجراءاتها مشـتركة للحد من هذه الجرائم مســـتندا الى مجموعة من المعاهدات والاتفاقيات لمواجهة ومكافحة هذه الجرائم, وبما في ذلك اتفاقية بودابست لمكافحة جرائم المعلوماتية والتي تعد احدى الوسائل الدولية الاساسية في هذه الصدد, ولكن لابد من جهود دولية اخرى لما تتســم به هذه الجرائم من خصـوصـية غير محدودة وارتباطها بالتكنولوجيا التي اضحت تتطور باستمرار.