السياسة الجنائية لمواجهة الجرائم المعلوماتية

إعداد

محمد جمال دياب

باحث دكتوراة في القانون الجنائي

كلية الحقوق جامعة القاهرة

مقدمـــة

يشهدُ العالمُ اليومَ عصرًا جديدًا أطلِقُ عليه المفكرُ الأمريكىُّ ألفين توفلر Alven Tovilr[1] "العصرَ المعلوماتىّ" أو عصرَ المعلوماتِ.

حيثُ شَهِدَت البشريةُ فى **الآونةِ** الأخيرةِ مرحلةً جديدةً تضافُ إلى ما سبقتها من مراحل التطور الفكرىّ والمعرفىّ الهائلِ غيرِ المسبوق[2].

وقد اتسع نطاقُ هذا التطور ليشملَ كلَّ مناحى الحياة المعاصرة، وذلك بفضلِ الثورةِ العلمية التكنولوجية فى مجال الاتصالات والمعلومات، والتى **غَـــدَت** تتربع على ذروة **سِنَام** هذه المرحلة من مراحل التطور التكنولوجى الهائل.

وصَاحَبَ التطور الذى عرفهَ المجتمعُ الدولى فى مجال تكنولوجيا الاتصالات[3] تطوراً كبيراً فى مجال شبكات الاتصال، حيث أصبحت هذه الشبكات من بين أهم الوسائل التى تتم بها المعاملات على المستوى الدولى، ولعل من أهم الشبكات الاتصالية– التى تأخذ حيزًا كبيرًا فى الحياة اليومية لمعاملات الأفراد والدول على حد سواء– **شبكة الإنترنت.**

وقد أدى هذا التطور الهائل، إلى حدوث ثورة معلوماتية أدت إلى ربط العالم كله وأصبح قرية صغيرة، وقد نشأت هذه الثورة من جماع طفرتين، هما طفرة الاتصالات وطفرة تقنية المعلومات؛ فأصبح الإنسان يستطيع أن يتحدث عبر الآخر من الكرة الأرضية بالصوت والصورة فى لحظة قيام الحدث، وأصبحت عملية تبادل المعلومات سهلة وميسرة، وأدى ذلك إلى تدفق هائل فى المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية يعجز الإنسان بقدرته العادية عن متابعتها والإلمام بها فى عمره القصير [4].

---

(1) المفكر الأمريكى ألفين توفلر هو أحد رواد علم المستقبل الحديث ويقصد به ذلك العلـــم الـــذى يحـــاول استنزاف السنوات القائمة فى دولة معينة أو مجموعة الدولة استنزاف علميًّا ومنهجيًا من أجل تطويرهـــا على الصورة المبتغاة أو المطلوبة.

راجع، ألفين توفلر (الموجة الثالثة): ترجمة فادى عصون، دار الروح، بيروت، لبنان، سنة 1985م، وأيضًـــا ألفين توفلر وعود المستقبل: ترجمة فادى عصون، دار الروح، بيروت، لبنان، سنة 1989م .

(2) د/ عادل يحيى، السياسة الجنائية فى مواجهة الجريمة المعلوماتية، دار النهضة العربية، الطبعة الأولـــى، 2014م، ص 7 .

(3) د/ عطا عبد العاطى محمد السنباطى، موقف الشريعة الإسلامية من الإجرام الدولى "جرائم الحاسب الآلى والانترنت"، مؤتمر الوقاية من الجريمة فى عصر العولمة، كلية الشريعة والقانون، جامعـــة الامـــارات العربية المتحدة، 6 – 8 مايو 2001م، ص 287 .

(4) د/ هلالى عبد اللاه أحمد، حجية المخرجات الكمبيوترية فى المواد الجنائية، دار النهضة العربيـــة، ســـنة 1988 م، ص 5 .

وبالرغم من مزايا التقنية المعلوماتية فى شتى مجالات الحياة، إلا أنه كما هو شأن كل اكتشاف أو اختراع جديد، أدى إلى ظهور مشاكل قانونية، دعت الدول إلى البحث عما إذا كانت القوانين القائمة تكفى لمواجهة بعض الاستخدامات غير المأمونة بل الضارة للإنترنت، أم إنه يتعين مواجهة هذه الأعمال بنصوص قانونية وإجرائية تجريمية جديدة [5].

ففى عام 2011 م كان هناك 2,3 مليار شخص على الأقل لهم القدرة على الوصول إلى شبكة الانترنت[6] أى ما يعادل أكثر من ثلث إجمالى سكان العالم فى ذلك الوقت.

كما تشير التقديرات إلى أن قبل عام 2017م كانت اشتراكات المتنقل تقترب من 70% من إجمالى عدد سكان العالم, وبحلول عام 2020م عدد الأجهزة التى تدخل على الإنترنت يفوق عدد الناس بمعدل 6 إلى 1، محولين بهذه المفاهيم الحالية للإنترنت فى عالم الغد إلى عالم الشبكات فائق السرعة [7].

وعبر أطراف هذه الشبكة الضخمة المتداخلة والمزدحمة من الحاسبات وشبكات المعلومات الكثيفة المحيطة بها وفى أوصالها تسرى المعلومات وتتدفق فى اتجاهات مختلفة وعند كل طرف من أطرافها يجرى التعامل معها بصورة مختلفة، فقد يجرى عند طرف اتصال المعلومات وعند طرف ثان تخزينها وعند طرف ثالث معالجتها وعند طرف آخر يتطلب استرجاعها وعند طرف خامس يتم تعديلها.. . إلخ وهكذا تذخر هذه الشبكة بكم هائل من المعلومات **والآلاف** من البرامج التى لا يمكن حصره من الأطراف والنهايات [8].

ومع زيادة عدد مستخدمي الشبكة المعلوماتية "**الإنترنت**"، وزيادة تدخلها فى كافة مناحى حياة الإنسان السياسية، الاقتصادية، الاجتماعية، الثقافية، ظهر نوع من الإجرام المستحدث وهو الجرائم المعلوماتية وهى أنشطة إجرامية تتم عبر هذه الشبكة أو عن طريقها, حيث أساء البعض استخدام الإمكانيات التى تقدمها شبكة **الإنترنت** فى ارتكاب الأنشطة الإجرامية.

---

(5) د/ هدى حامد قشقوش، "جرائم الحاسب الإلكترونى فى التشريع المقارن"، دار النهضة العربية، سنة 1992م، ص 5.

(6) راجع د/ أسامة أبو الحسن مجاهد، خصوصية التعاون عبر الانترنت، دار النهضة العربية، سنة 2000م، ص 10.

(7) د/ محمد السعيد رشدى، الانترنت والجوانب القانونية لنظم المعلومات – بحث منشور مجموعة أبحاث المؤتمر العلمى الثانى، كلية الحقوق جامعة حلوان تحت عنوان الإعلام والقانون فى الفترة من 14 – 15 مارس سنة 1999م، ص 11 وما بعدها .

(8) د/ كمال كاشف : "فيروس الكمبيوتر ومخاطر العدوى"، مجلة الكمبيوتر، دار المعارف، القاهرة، عام 1989م، ع 30، ص 23 .

وأستغل أسوء استغلال هذه الإنجازات العلمية من قبل النظم الإلكترونية الأمر الذي أدى إلى ظهور أنماط جديدة من الجرائم وبـــروز أشخاص لم تعهدهم المجتمعات الحديثة من قبل يتمتعون بالخبرة التى تمكنهم من تطويع تقنية الحاسب الآلى– للقيام بأفعال إجرامية لم تكن معروفة من قبل، وحولت الجريمة من نمطها التقليدى وأبعادها المحدودة إلى أنماط مستحدثة باعتماد التقنية الحديثة، والتى أطلق عليها **الجريمة الإلكترونية أو المعلوماتية** (9).

ولقد تطورت الجريمة الإلكترونية أو المعلوماتية بشكل رهيب فى المدة الأخيرة وذلك نظرًا إلى التطور المستمر والمتسارع لشبكة الإنترنت مما جعل هذه الشبكة وسيلة مثالية لتنفيذ العديد من الجرائم بعيدًا عن أعين الجهات الأمنية، حيث مكنت الإنترنت العديد من المجرمين والجهات الإجرامية من القيام بعدة أفعال غير مشروعة مستغلين مختلف التسهيلات التى تقدمها هذه الشبكة، وذلك بدون أدنى مجهود وبدون الخوف من العقاب، وهو ما دفع العديد من الدول والهيئات والمنظمات الدولية إلى التحذير من خطورة هذه الظاهرة التى تهدد كل مستخدمى الانترنت، حيث أصبحت من أسهل الوسائل التى يعتمد عليها **مرتكبو** الجريمة، وسعت الدول إلى مواجهة هذا الإجرام المستحدث والتصدى للجرائم المعلوماتية عن طريق الدراسة والتحليل من أجل وضعها فى إطار قانونى يمكن من خلاله وضع الطرق السلمية لمكافحتها برسم سياسة جنائية جديدة اتجاهـــا.

ومن ثم أصبحت الجريمة المعلوماتية مشكلة معقدة تؤرق الدول والأفراد، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشرى لا تفرق بين الدول المتقدمة والنامية، فالإجرامُ واحد وإن اختلفت صوره أو تعددت وسائله بل إن الأمر تعدى أنماط الجرائم إلى ظهور أنماط جديدة، على وجه الخصوص فى مجالات الإرهاب وتجارة المخدرات والاتجار بالسلاح والدعارة المنظمة باستخدام **الإنترنت**، والحروب الإلكترونية (10).

لذلك قد ذهبت كل دولة إلى التصدى لهذا الإجرام المعلوماتى كلًا وفقًا لسياستها الجنائية وتحقيق التعاون الدولى فى مواجهتها حيث إنها جريمة من الجرائم العابرة للحدود.

---

(9) بيل جيتس، المعلوماتية بعد الانترنت، طريق المستقبل، ترجمة عبد السلام رضوان، سلسلة كتب المجلس الوطنى للثقافة والفنون والأدب، الكويت، مارس 1998 م، ص 151.

(10) ومن هذه الظواهر على سبيل المثال لا الحصر نشر الأفكار المتطرفة، إساءة العلاقات السياســية بــين الدول، تهديد الأمن العسكرى والقومى للدول، إتلاف أجهزة الحاسب الإلكترونى، التجسس الصــناعى – وسرقة الأسرار الخاصة، عرض الشذوذ الجنسى، تشويه سمعة الشرفاء، سرقة المعلومات السرية مــن مستخدمى الشبكات الدولية، نشر الرسائل الإلكترونية المزعجة، هجمات البريد الإلكترونــى، الاحتيــال والتجسس والإرهاب الإلكترونى . متاح على موقع الأهرام – www.ahram.org

إلا أنه توجد العديد من الصعوبات التي تقف امام مواجهة الجرائم المعلوماتية في السياسات الجنائية للدول داخليا وعلي المستوي الدولي من الناحية التشريعية الموضوعية والإجرائية من التجريم والعقاب وضبط مرتكبيها فهي من الجرائم العابرة للحدود

السياسة الجنائية بصورة عامة يرجع تعريفها إلى الفقيه الألمانى " قوبرباج " والذى يعد أول من استعمل هذا التعبير فى بداية القرن التاسع عشر وكان يقصد بها " مجموعة الوسائل التى يمكن اتخاذها فى وقت معين وفى بلد ما من أجل مكافحة الإجرام " [11].

فلكى يرسم المشرع سياسة جنائية سليمة تكفل مواجهة الجريمة والحد من انتشارها يجب معرفة العوامل المؤدية إلى الجريمة باعتبارها ظاهرة اجتماعية [12].

فهى تشمل الوقاية من الجريمة قبل وقوعها، ورد فعل الدولة ضد الجريمة بعد وقوعها أيضاً وفقاً لما استقر عليه غالبية الفقهاء.

وتوجد العديد من الصعوبات التي تتعلق بمواجهة الجريمة المعلوماتية على المستوى الداخلى والدولى وفى سبيل القضاء على هذه الصعوبات لمكافحة الجريمة المعلوماتية والحد من انتشارها، يجب بناء سياسة جنائية لمواجهة الجريمة المعلوماتية داخليًّا ودوليًّا وعليه سنتناول هذا البحث من خلال مطلبين :-

المطلب الأول: السياسة الجنائية لمواجهة الجرائم المعلوماتية داخليًّا

المطلب الثانى: السياسة الجنائية لمواجهة الجرائم المعلوماتية دوليًّا

(11) د/ أحمد فتحى سرور، أصول السياسة الجنائية الجنائية، دار النهضة العربية، عام 1972، ص 13.

(12) د/ عبد الرحمن توفيق أحمد، دروس فى علم الإجرام، " نشأة علم الإجرام وعوامل الإجـــرام الداخليـــة والخارجية مقروناً بإحصاءات جنائية "، دار وائل للنشر، الطبعة الأولي، الأردن، عام 2006، ص 26 .

المطلب الأول

السياسة الجنائية لمواجهة الجرائم المعلوماتية داخليًّا

وسنتناول هذا المطلب فى فرعين :-

- الفرع الأول: الآليات الجنائية الواجب اتخاذها على المستوى التشريعى
- الفرع الثانى: استخدام التكنولوجيا الأمنية فى مكافحة الجريمة المعلوماتية

الفرع الأول

الآليات الجنائية الواجب إتخاذها على المستوى التشريعى

وصولًا إلى مكافحة الجريمة المعلوماتية لمكافحتها والحد منها يجب على كل دولة أن تقوم بإصدار تشريعات جنائية خاصة للجريمة المعلوماتية, لتجريم كافة الأفعال المستحدثة التى لا يتناولها التشريع العقابى التقليدى، وكذلك القواعد الإجرائية بها لاكتشافها وإثباتها والاعتراف بالأدلة الرقمية كدليل للجريمة المعلوماتية، **وهذا ما سيتناوله الباحث**

اولا التدابير الموضوعية

إن أولى خطوات مكافحة الجرائم المعلوماتية العابرة للحدود هو إصدار تشريع جنائى يجرم هذه الأفعال، ويكون مستقل عن قانون العقوبات التقليدى – الذى يتناول الجرائم التقليدية العادية – فلا يكفى أن تقوم الدولة بتعديل أو إضافة بعض الجرائم المعلوماتية إلى قانون العقوبات التقليدى إنما يجب أن تنظم لهذه الجرائم قانون خاص بها لمواجهتها والحد من آثارها.

فبلغت عدد الدول فى العالم التى سنت تشريعات لمكافحة [13] الجرائم المعلوماتية حوالى 138 دولة تقريبًا سواء بنصوص خاصة أو بتعديل فى قانون العقوبات أو بالإضافة منها 13 دولة عربية أقدمت على سن تشريعات مختلفة لمواجهة الجرائم المعلوماتية، فيما طبقت البقية قواعد عامة على هذه الجرائم المستحدثة.

---

(13) متاح على الموقع الإلكتروني :-
https://arij.net/news
تم الإطلاع فى 2020/7/7م .

فبالنسبة للدول الأجنبية، نجد دولة السويد من أوائل الدول التى سنت تشريعات خاصة بجرائم الحاسب الآلى والإنترنت.

وتأتى فرنسا بعد ذلك حيث سن المشرع الفرنسى القانون رقم 19–88 عام 1988م الخاص ببعض جرائم المعلوماتية وضمنه قانون العقوبات الفرنسى فى المادة " 462" والمادة " 2/462 " وخضع هذا القانون لتعديلات عام 1993م يشمل بعض الجرائم المعلوماتية [14] ثم أصدرت قانون المعالجة الإلكترونية للبيانات رقم 7 لسنة 1978م، ووضعت عدة قوانين رُوعِيَ فيها التطور التكنولوجى فى عالم الاتصالات والكمبيوتر منها قانون 1980م – المتعلق بإثبات التصرفات القانونية ذات المعالجة الإلكترونية وقانون 1982م و 1986م وقانون العقوبات الجديد لعام 1992م والمعمول به منذ عام 1994م وبعدها قانون 1998م.

وسن المشرع البريطانى قانون إساءة إستخدام الحاسوب الكمبيوتر وتناول فيه المسئولية الجنائية عن الجرائم المعلوماتية عام 1990م.

وفى الولايات المتحدة شرعت قانوناً خاصة بحماية أنظمة الحاسب الآلى " 1976م – 1985م "وفى عام 1986م صدر قانوناً تشريعيًّا يحمل الرقم" 1213" عرف فيه جميع المتطلبات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت المتطلبات الدستورية اللازمة لتطبيقه وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم المعلوماتية ،حيث عدلت فى عام "1985م" قانونها الجنائى بحيث شمل قوانين خاصة بجرائم الحاسب الآلى والإنترنت وفى اليابان هناك قوانين خاصة بجرائم الحاسب الآلى والإنترنت " الجرائم المعلوماتية [15]

كذلك أصدرت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلى والإنترنت والتى شملت فى فقراتها العقوبات المحددة لجرائم الحاسب الآلى كالدخول غير المشروع إلى الحاسب الآلى، أو التزوير أو أى كسب غير مشروع سواء للجانى أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلى كإتلافها أو تغييرها أو الاستفادة منها.

---

(14) مركز هاردو لدعم التعبير الرقمى، التنظيم القانونى والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، بدون سنة نشر، بدون ناشر، ص 21 .

ومتاح على موقع البحث Google .

https://hardoegypt.org

تم الإطلاع فى 2020/7/7م .

(15) متاح على الموقع الإلكترونى ؛ صوت الأمة.

http://www.soutalomma.com/Article1870700.

كما توجد فى هولندا والمجر وبولندا قوانين خاصة بجرائم الحاسب والإنترنت [16] توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها.

وفى النرويج عدل المشرع قانون العقوبات عام 1985م، وجود الوصول غير المصرح به عن طريق تخطى الحماية إلى البيانات المخزنة أو المنقولة بالوسائل الإلكترونية أو الفنية الأخرى، وجرَّمَ إتلاف وتعطيل البيانات والاستخدام غير المصرح به لوقت وخدمات الحاسوب.

وفى سويسرا تضمن القانون السويسرى بشأن جرائم المعلوماتية نصوصًا تعاقب على الحصول دون تصريح على بيانات مخزنة إلكترونيًا أو على البرامج.. . إلخ [17].

وفى البرتغال صدر قانون المعلوماتية الجنائى فى عام 1991م وتضمن فى القسم الأول المادة السابقة المتعلقة بالجرائم المعلوماتية.

وفى إيرلندا صدر تشريع الإتلاف الجنائى عام 1991م وتناول بعض جرائم المعلوماتية.. .. وغيرها من الدول الأجنبية.

ونجد اتجاهات الدول الأجنبية لمكافحة الجرائم بتعديل قانون العقوبات التقليدى وإضافة الجرائم إليه عند بداية مواجهة الجريمة المعلوماتية لها وقلة منها اتجهت إلى إفراد قوانين خاصة لها

وإذا انتقلنا إلى الوضع فى الدول العربية، نجد أن أولى الدول العربية فى إصدار قانون خاص بالجريمة المعلوماتية هى دولة السودان بإصدارها قانون جرائم المعلوماتية عام 2007م والمملكة العربية السعودية عام 2007م ثم تبعتهما العديد من الدول العربية على النحو التالى :-

- دولة الجزائر بالقانون رقم " 4 – 9 " لعام 2009م المتضمن قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال [18].
- سلطنة عمان بقانون مكافحة جرائم تقنية المعلومات رقم 12 لسنة 2011م [19]

---

(16) أنظر: بتاريخ 2019/5/5م
د/عبد الرحمن عبد العزيز الشنقيطى، أمن المعلومات وجرائم الحاسب الألى، ط1، الرياض، ص 110،
د/ أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الألى، دار النهضة العربية، ط1، بدون سنة نشر، ص 200 .

(17) مراجع مركز هاردو لدعم التعبير الرقمى، مرجع سابق، ص 22 .

(18) متاح عبر الوقع الإلكتروني :
https://www.arpce.dz/ar/dac/reg/loi/loi-og-04.pdf

- دولة سوريا بالمرسوم التشريعى رقم 17 لسنة 2012م المتعلق بتطبيق أحكام قـــانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية [20].
- دولة الإمارات العربية المتحدة بالقانون رقم 2 لسنة 2006م والمعدل بالقانون رقم 5 لسنة 2012م.
- البحرين قانون رقم " 60 " لسنة 2014م بشأن جرائم تقنية المعلومات [21].
- قطر بقانون رقم 14 لسنة 2014م بشأن قانون مكافحة الجرائم الالكترونية.
- الكويت، قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015[22].
- الأردن، بقانون الجرائم الالكترونية رقم 27 لسنة 2015[23].
- مصر، بقانون رقم 175 لسنة 2018م، الخاص بمكافحة جرائم تكنولوجيا المعلومات [24].

وتجدر الإشارة هنا إلى مشروع الأسكوا [25] وهو المشروع التى أطلق لتنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة فى المنطقة العربية " , والذى بدأ تنفيذه عام 2009م وأنتهى بنهاية عام 2012م [26].

وقد هدف المشروع إلى تعزيز وتنسيق التشريعات السيبرانية فى المنطقة العربية بغية بناء قطاع متين ومستدام لتكنولوجيا المعلومات والاتصالات عبر وضع الأطر التشريعية والقانونية الملائمة، وقد تخلل عن هذا المشروع تنفيذ عدد من الأنشطة المتنوعة التى صدر عنها مخرجات مختلفة أبرزها " إرشادات الإسكو للتشريعات السيبرانية " والتى صممت لتساعد البلدان العربية فى تطوير قوانين سيبرانية وطنية، وتطوين البنية الأساسية للتكامل الإقليمى بين البلدان العربية عبر تنسيق التشريعات السيبرانية فيما بينها محاور أساسية لتنظيم

---

(19) متاح على الموقع الإلكتروني :
https"//www.ita.gov.com/iTAportal-AR/mediacenter/Document-detail.aspx?NID=64
(20) http://www.parliament.gov.sy/arabic/lidex.php?node=201&nid=4337&ref=tree
(21) متاح على الموقع الإلكتروني :
http://www.acees.gov.bh/cyber-crime/anti-cyber-crime-law-in-the-kingdom-ofbahrain
(22) متوفر على الموقع الالكترونى :-
https://www.e.gov.kw/sites/kgoenglish/froms/ACiTlawNo.63of2015oncombatingInformation technology crimes. pdf
(23) متوفر على الموقع الإلكتروني :-
http://moict.gpv.jo/uploads/policies-and-strategies-Directorate/legistiation/laws/Electron-ic-crime-law.pdf
(24) متوفر على موقع البحث Google .
(25) وهى احدى الهيئات التابعة لمنظمة الأمم المتحدة مقرها فى لبنان والخاص بالمنطقة العربية .
(26) Legislation/projects/ tabid/161 language / en-us /Defautl . aspx.

الفضاء السيبرانى، والتى يمكن استخدامها إما كقانونين منفصلة بحسب المحور أو كقانون واحد وشامل، والمحاور الستة هى: الاتصالات الإلكترونية، المعاملات الإلكترونية، التوقيعات الإلكترونية، التجارة الإلكترونية وحماية المستهلك، معالجة البيانات ذات الطابع الشخصى، والجرائم السيبرانية، والملكية الفكرية فى المجال المعلوماتى [27] وذلك كله لتتضمن حجم الفجوة القانونية السيبرانية بين المنطقة العربية ودول العالم ولا سيما دول الإتحاد الأوروبي.

ثانيا التدابير الإجرائية الجنائية

عند تناولنا المواجهة الإجرائية للجريمة المعلوماتية على المستوى الداخلى وجدنا عدة صعوبات تعترض اكتشاف وإثبات الجرائم المعلوماتية، وإن الإجراءات الجنائية التقليدية لا تصلح فى أغلب الأحوال لإثباتها وإقامة الدليل على مرتكبيها وفى سبيل مكافحة هذه الجرائم المستحدثة يجب اعتماد إجراءات تتناسب مع طبيعتها وذلك علي النحو التالي

1استخدام آليات لإكتشاف الجرائم المعلوماتية

أ اكتشاف الجريمة المعلوماتية بطريق المراقبة

المراقبة – بصفة عامة – تعنى وضع شخص أو مكان أو أى شىء معين تحت ملاحظة رجل البحث الجنائى وتسجيل كل ما يحدث من تصرفات فى جو من السرية والحذر على النحو الذى لا يمكن معه الإحساس بوجود مراقبة[28].

ولا تختلف مفهوم المراقبة الإلكترونية عن ذلك، إلا أنها تتميز بأنها تتم باستخدام الأجهزة والوسائل الإلكترونية أو عبر شبكة الإنترنت لتحقيق غرض محدد، وإفراغ النتيجة فى ملف إلكترونى، وتحرير تقارير بهذه النتيجة , ففى جرائم الحاسوب والإنترنت " الجرائم المعلوماتية " قد يرغب رجال الضبط القضائى فى مراقبة أحد الهاكرز ممن قام باختراق الحاسوب الخاص بالمجنى عليه، أو قام بإعداد صندوق بريد إلكترونى مُستنسخ لمراقبة المشتبه فيه عند إرساله أو استقباله لصورة داعرة للأطفال على الإنترنت [29].

---

(27) أنظر فى ذلك ؛ د/ نضال أدلبى، بحث بعنوان تطوير وتنسيق التشريعات السيبرانية فى المنطقة العربية ومواجهة الجرائم السيبرانية، الأمم المتحدة، الاسكو، نقل بتصرف، ص 4 وما بعدها .

(28) د/ عماد عوض عدس، التحريات كإجراء من إجراءات البحث عن الحقيقة، دار النهضة العربية، القاهرة، عام 1428هـ / 2007م، ص 95 .

(29) د/ عمر محمد أأو بكر يونس، الإجراءات الجنائية عبر الإنترنت فى القانون الأمريكي، المرشد الفيدرالى الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني فى التحقيقات الجنائية، مترجم، بدون ناشر، عام 2006، ص 245 .

ولذلك يجب على رجال البحث الجنائى – مواكبة هذه التطورات باستخدام التكنولوجيا فى تحقيق أهدافها, لكشف الحوادث المخالفة للقانون والتوصل لمرتكبيها وضبطهم وإقامة الدليل عليهم , وتهدف المراقبة أساسًا إلى جمع المعلومات، فالمراقبة هى اللبنة الأولى لتأكيد المعلومات التى تصل إلى رجال هيئة الشرطة، وتصبح لها مجالات لها قبل التروى فيها تحريضًا واتفاقًا ومساعدة – ومنها الجرائم المعلوماتية – فهى وسيلة لمنع وقوع الجرائم وضبط مرتكبيها قبل تنفيذها وتحقيق نتائجها – بمجرد الشروع فى ارتكابها [30].

فهى وسيلة لاكتشاف الجريمة المعلوماتية قبل وقوعها – أى فى مرحلة البدء فى التنفيذ – للحد من أخطارها وتتم باستخدام الوسائل الإلكترونية الحديثة عن طريق أشخاص ذو خبرة عالية فى مجال تقنية المعلومات ممن لهم صفة الضبطية القضائية، وتتم فى إطار من المشروعية بغرض الوقاية من ارتكاب الجرائم المعلوماتية على شبكة الإنترنت أو أى نظام معلوماتى آخر, وافتراض أن تتم فى إطار من الشرعية, لأنها تفرض نوعًا من التدخل فى الحريات الشخصية للأفراد، فيجب أن يتم ذلك فى حدود القانون فيجب أن تكون هناك شبهة جنائية لارتكاب جريمة معلوماتية على شبكة الإنترنت، ويجب تحديد مواقع الأشخاص والأماكن والأشياء حتى يتم منع وقوع الجريمة وقبل الشروع فيها وتحقيق أضرارها أى أن تتوافر جدية لأسباب المراقبة، والتقيد بالكشف عن النشاط الإجرامى، والتقيد بالغرض المقصود من المراقبة ومشروعية الوسيلة المستحدثة فى المراقبة.

فهى " عملية رقابة وملاحظة سرية لابد أن تكون مشروعة تتم بشأن شخص أو مكان أو اتصالات أو أحاديث معينة بصورة سرية، ويجب أن يتم إجراؤها فى إطار من الشرعية، لأنها تفرض نوعًا من التدخل فى الحريات الشخصية للأفراد "

- **وعناصر المراقبة الإلكترونية [31] :-**

القائم بالمراقبة: "المراقب" قد يكون أحد مأمورى الضبط القضائى ذاته، إذا توافرت فيه الخبرة الكافية لاستخدام التقنيات التكنولوجية التى يعتمد عليها فى عملية المراقبة بدرجة عالية من الدقة والكفاءة او الاستعانة بأحد الخبراء للقيام بهذه المهمة، وحتى يتمكن القائم بالمراقبة الإلكترونية من أداء مهام عمله فإنه يجب أن يتوافر فيه صفات عدة نذكر منها :-

---

(30) د/ قدرى عبد الفتاح الشهاوى، مناط التحريات، " الإستدلالات والإستخبارات، دار المعارف، الإسكندرية، عام 1998م، ص 195 .

(31) للمزيد من المعلومات أنظر ؛ د/ إنشراح محمد الدسوقى، بحث ميدانى عن التحصيل الدراسى وعلاقته بكل من مفهوم الذات والتوافق النفسى، دراسة مقارنة، نشر بمجلة علم النفس، الهيئة المصرية العامة للكتاب، ع 20، س5، أكتوبر 1991م، ص 63 .

1- الخبرة والمهارة الإلكترونية.

2- الثقة بالنفس إلكترونيًّا.

3- الذكاء الإلكتروني الرقمى.

محل المراقبة: وهو ذلك الهدف الذى تتم مراقبته وتتبع تحركاته وتصرفاته وفى نطاق المراقبة الإلكترونية الرقمية، فإن محل المراقبة هو الحاسوب الرقمى أو موقع ما عبر شبكة الإنترنت أو البريد الإلكتروني بما يحويه من مراسلات إلكترونية وحلقات نقاش أو عزف للدردشة أو يكون محلها الهاتف النقال المتصل بالإنترنت.

فالمشتبه به محل المراقبة الإلكترونية حينما تجد الجهات الأمنية ضرورة لمراقبته لقيامه بمخالفة القانون أو لأى سبب أخر, فإنها تقوم بعملية المراقبة الإلكترونية بحقه , ولكى يتم المراقبة للبريد الكترونى أو موقع معين على شبكة الإنترنت يجب استئذان النيابة العامة، وفى الولايات المتحدة الأمريكية يمكن اخضاع البريد الإلكتروني أو أى موقع من مواقع شبكة الإنترنت للمراقبة، وأيا كانت جنسيته مادام يشكل خطرًا ويمثل ضررًا للمصلحة العامة للبلاد والأفراد [32].

وسائل وأدوات المراقبة الإلكترونية [33]: كى تتحقق النتائج المرجوة من عملية المراقبة الإلكترونية فلابد من استخدام وسائل وأدوات تواكب وتلائم تلك الوسائل التى يستخدمها المجرمين الرقميون فى انتهاكهم وارتكابهم للجرائم المعلوماتية، ولما كان هؤلاء المجرمين هم فئة خاصة ومميزة عن المجرمين، حيث تنصب أفعالهم المخالفة على استخدامات الحاسوب وشبكة الإنترنت والبريد الإلكترونى أو إحدى تطبيقات التكنولوجيا فى مجال المعلومات، وبصورة تشكل انتهاك للقوانين ومخالفتها.

فكان لزامًا على القائمين بعملية المراقبة الإلكترونية استخدام ذات وسائل وأدوات وأساليب هؤلاء المجرمين حتى تؤتى المراقبة فوائدها وتحقق هدفها وتوصل إلى المجرمين، بل أن الأمر يذهب إلى أبعد من ذلك فقد لجأت العديد من الدول إلى استخدام بعض مجرمى الإنترنت أنفسهم كقراصنة للحد من بعض الظواهر الإجرامية.

---

(32) جريدة الجمهورية، مقال بعنوان " مكافحة الإرهاب، مكتب التحقيقات الفيدرالى يتجسس على الأمريكيين منشور فى تاريخ 2002/6/1، ص 4 .

(33) متاح على الموقع الإلكتروني :-

وعلى ذلك فإن الوسائل التى تستخدم فى المراقبة الإلكترونية هى أجهزة الحواسيب الألية وشبكات الإنترنت وما يتعلق بها من تطبيقات كالبريد الإلكتروني والبرامج المصممة بهدف التنصت والتسجيل وتقصى وتتبع المجرمين والبرمجيات المخصصة لذلك.

فهناك عدة تقنيات وبرمجيات لتتبع المجرمين والمشتبه بهم من مراقبة البريد الإلكتروني وتعقب واقتحام المواقع الإباحية التى تساعد فى المراقبة فى نطاق شبكة الإنترنت (34).

ب: اكتشاف الجريمة المعلوماتية عن طريق الإبلاغ

إن الجرائم المعلوماتية هى جرائم مستترة ما لم يتم الإبلاغ عنها، ومن صعوبات مواجهة الجريمة المعلوماتية على المستوى الوطنى كما تناول الباحث سابقًا هى إحجام المجنى عليه عن الإبلاغ عنها، ومن ثم لا يتم عمل الاستدلالات أو تحريك الدعوى الجنائية، وفى سبيل مواجهة الجريمة المعلوماتية والقضاء عليها يتعين على الأفراد والجهات المجنى عليها الإبلاغ عنها وكذلك الغير, وذلك نظرًا لخطورتها وجسامتها حتى يتم كشفها والوصول إلى الجانى ومحاكمته وتوقيع العقاب عليه.

ولا شك أن الجرائم المعلوماتية تتفق مع الجرائم التقليدية فى كونها أفعالًا مخالفة للقانون فكليهما جرائم – ويجوز الإبلاغ عن الجرائم بصفة عامة – بأى طريقة تيسر على المبلغ الإبلاغ بها حيث لم يشترط القانون شكلًا أو أسلوبًا محددًا بذاته للإبلاغ، إلا أن الإبلاغ عن الجرائم المعلوماتية يختلف عن الإبلاغ عن الجرائم التقليدية وذلك بسبب طبيعتها الخاصة.

لكن ما هى الطريقة التى يتم بها الإبلاغ عن جرائم المعلوماتية؟

يمكن الإبلاغ عن الجرائم المعلوماتية بالطرق التقليدية، إلا أنه من المناسب للإبلاغ عن جرائم الإنترنت " الجرائم المعلوماتية، أن يكون عن طريق الإنترنت ذاته، وهو ما يسمى بالبلاغ الرقمى ويكون ذلك عن طريق مواقع متخصصة فى تلقى البلاغات والشكاوى الخاصة بجرائم عبر هذه المواقع.

---

(34) للمزيد من المعلومات حول هذا الموضوع – التقنيات والبرمجيات المستخدمة فى المراقبة الإلكترونية – أنظر المواقع الاليكترونية:

http://www.arabips.com/foroms/index.php?showtopic=8010.
http://www.Tartoos.com
http://www.e-msjed.com/msjed/site/details-asp?topicid=748.

تم الإطلاع بتاريخ 2020/6/23م.

ويستطيع المواطنون في مصر – كمثال – تقديم البلاغات بجرائم الإنترنت بالمكان المخصص لتقديم البلاغات في وحدة تلقى بلاغات المنطقة المركزية بميدان العباسية فضلًا عن تقديم البلاغات بكافة مديريات الأمن على مستوى الجمهورية. كذلك يمكنهم التواصل مع مباحث الإنترنت عن طريق أرقام تليفونية يمكن الاتصال عليها [35].

وأيضًا فى دولة الإمارات العربية المتحدة، نجد أن التبليغ يتم عن طريق اللجوء إلى قسم الجرائم الإلكترونية " دبى " فى الجهات الاتحادية أو المحلية المسئولة عن الأمن الإلكتروني فى الدولة، وهم الإدارة العامة للتحريات والمباحث الجنائية، إدارة المباحث الإلكترونية، مراكز الشرطة فى إدارة دبى، كذلك تحديد أرقام تليفونية للإبلاغ عنها[36] , وكذلك استحداث وسيلة جديدة للإبلاغ عن طريق تطبيق ذكى يتيح للأفراد الإبلاغ عن أى جريمة او اشتباه يقع من خلال مواقع التواصل الاجتماعى يسمى " مجتمعى أمن " ويتلقى من خلاله مكتب التحقيقات الاتحادى التابع للمكتب النائب العام للدولة كافة الشكاوى ويمكن التصالح أون لاين بين الخصوم عبر منصة إلكترونية ذكية أُنشئت لتسهيل إجراءات التحقيق دون عناء[37].

وفى السعودية يمكن الإبلاغ عن الجرائم الإلكترونية من خلال الاتصال على أرقام حددتها المملكة، وكذلك عن طريق تطبيق " كلنا آمن " أو من خلال وزارة الداخلية [38] , وفى مصر فقد تم إنشاء موقع خاص لإدارة مكافحة جرائم الحواسيب وشبكات المعلومات " http://ccd.gov.eg" وذلك لتلقى البلاغات والشكاوى عن جرائم الانترنت.

كما افتتح موقع وزارة الداخلية المصرية قسمًا خاصًا بتلقى البلاغات عن جرائم النصب والاحتيال التى تقع عبر شبكة الإنترنت أو الواقعة عبر الهواتف النقالة، وجرائم الفيزا

---

(35) متاح على موقع اليوم السابع :-
http://m.youn7.com/story/201912/19/%D8... خطوات البلاغ لجرائم الإنترنت
منشور بتاريخ 2019/2/19م .
تم الاطلاع بتاريخ 2020/6/25م .
(36) متاح على الموقع الإلكتروني :-
" مای بیوت "
https"//www.bayut.com/mybayut/ar. تم الإطلاع بتاريخ 2020/6/27م.
(37) متاح على الموقع الإلكتروني :-
https://www.emaratalyoum.com/local-section/accidents/2018-07-02-1.11138882.
تم الاطلاع بتاريخ 2020/6/27م "الإمارات العربية "
(38) متاح على الموقع الإلكتروني :-
https://www.mohamah.net/law
منشور بتاريخ 2019/11/28، تم الإطلاع بتاريخ 2020/6/27م .

كارد، وكذلك جرائم الخدمات المزيفة او الإيميلات الوهمية، أو باستخدام أى طريقة أخرى عبر شبكة الإنترنت ذاتها – البلاغ الرقمى – من خلال رسائل البريد الإلكتروني، ويتم ذلك عن طريق إرسال بريد الكترونى إلى عنوان البريد الإلكتروني الخاص بجهات التحقيق والتحرى؛ بقصد إبلاغها بوجود مواقع أو صفحات غير مشروعة وخادعة أو بوجود موقع يحوى صورة داعرة أعدت للاستغلال الجنسى للأطفال.

وعلى سبيل المثال فإن فى فرنسا يمكن إرسال رسالة البريد الإلكتروني الخاص بالدرك الوطنى الفرنسى [39].

ولقد أنشئ بالولايات المتحدة الأمريكية مركز الشكاوى الخاصة بجرائم الإنترنت وأطلق عليه "Ic3 " وهو كناية عن نظام تبليغ وإحالة الشكاوى الناس فى الولايات المتحدة الامريكية والعالم أجمع ضد جرائم الإنترنت.

ويخدم هذا المركز "IC3 " الجمهور ووكالات فرض تطبيق القانون الأمريكي والدولى التى تختص بجرائم الإنترنت كشفًا وتحقيقًا وإثباتًا بواسطة استمارة الشكاوى مرسلة على الإنترنت وبواسطة فريق من الموظفين والمختصين والمحللين.

وقد تم تأسيس أول مكتب لمركز الشكاوى الخاصة بجرائم الانترنت عام 1999م فى " موجانتاون " بولاية " ويست فيرجينا " وسمى مركز شكاوى الاحتيال على الإنترنت ،وكان المكتب عبارة عن شراكة بين مكاتب أجهزة تطبيق القانون على صعيد الولاية والصعيد المحلى، ويهدف إلى إكتشاف جرائم الإنترنت.

وفى عام 2002م، وبغية توضيح نطاق جرائم الانترنت أعيدت تسمية المركز، مركز الشكاوى الخاصة بالإنترنت.. ودعا مكتب التحقيقات الفيدرالى ووكالات فيدرالية أخرى، هى مكتب التفتيش البريدى والتجارة الفيدرالية والشرطة السرية وغيرها للمساعدة فى تزويد المركز بالموظفين وللمساهمة فى العمل ضد جرائم الإنترنت.

وقد أصبح بمركز الشكاوى حوالى اربعين محللًا من القطاع الأكاديمى وقطاع صناعة الكمبيوتر وخدمات الإنترنت وستة موظفين فيدراليين يتلقون الشكاوى المتعلقة بجرائم الإنترنت من الجمهور، ثم يقومون بالبحث عن تلك الشكاوى وتجهيز ملفها وإحالتها إلى وكالات تطبيق القانون, وبإمكان الناس فى كافة أنحاء العالم تقديم شكوى تتعلق بجريمة ما من جرائم الإنترنت بواسطة موقع مركز الشكاوى الخاص بجرائم الإنترنت

(39) د/ عمر محمد ابو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، مرجع سابق، ص 831 .

التالى"http://www.ic3.gov"، ويقوم الموقع بطلب اسم الشخص وعنوانه البريدى ورقم هاتفه وإضافة اسم وعنوان ورقم تليفون والعنوان البريدى إذا كانت تلك المعلومات او البيانات متوفرة عن الشخص أو المنظمة المشتبه بقيامها بنشاط إجرامى، وعلاوة على تفاصيل تتعلق بمعلومات عن الجريمة، مثل كيفية وقوعها حسب اعتقاد الشخص مقدم الشكوى وسبب اعتقاده بوقوعها بالإضافة إلى اى معلومات أخرى تدعم الشكوى [40]

ويرى الباحث أنه يتعين على كل دولة أن تنشئ لها موقعًا خاصًا بتلقى البلاغات والشكاوى عن جرائم الحاسوب والإنترنت " الجرائم المعلوماتية " حتى يتسنى للمواطنين لديها سرعة الإبلاغ عن هذه الجرائم، وذلك عند الشروع فيها وسرعة ضبط مرتكبيها عند ارتكابها ويعهد لإدارة الموقع لأشخاص ذو خبرة عالية فى تلقى البلاغات وتحليلها واثباتها، وإنشاء وحدة تحقيق فى هذه البلاغات على وجه السرعة.

ج : اكتشاف الجرائم المعلوماتية عن طريق تطوير أجهزة وسلطات الضبط القضائى

فى سبيل كشف الجرائم المعلوماتية، يجب أن تتطور أجهزة وسلطات الضبط القضائى بما يتلائم مع هذا الإجرام المستحدث، وذلك حتى يتسنى لهذه الأجهزة الأمنية تحقيق العدالة وكشف هذه الجرائم مثل ارتكابها أو ضبط الجناة بعد ارتكابها، ولاسيما أن أغلب الجهات المجنى عليها قد تمتنع عن الإبلاغ عنها حتى لا يضر ذلك بمصالحها، والاهتمام بما يستجد من تقنيات وأدوات وأجهزة وبرامج والتى تنجز الكثير من الأعمال فى المجال الأمنى وتوفر الجهد والوقت والمال من تقنيات الحاسوب والإنترنت وتواكب التطور المستمر فى آليات ارتكاب تلك الجرائم والتعامل معها ومجابهتها [41].

ومن أجل السيطرة على الجرائم المعلوماتية، فإنه يجب تطوير الأساليب والوسائل والآليات المناسبة فى الوقاية من الجريمة ومكافحتها، ولذلك فلابد أن تكون برامج التدريب لرجال الضبط القضائى مستمرة ومواكبة التدريب لكل ما يحدث من تغييرات وتطورات فى شتى مجالات الحياة حتى يتم السيطرة على الجريمة والتفوق على العناصر الإجرامية واتباع أساليب التدريب الأمنى المتطورة[42].

---

(40) متاح على الموقع الإلكتروني :-

http://www.moheet.com

تم الإطلاع بتاريخ 2020/6/26م .

(41) د/ محمد السيد عرفه، تدريب رجال العدالة وأثره فى تحقيق العدالة، جامعة نايف، الرياض، عام 2005م، مرجع سبق ذكره، ص 8 .

(42) للمزيد من المعلومات عن هذا الموضوع أنظر :

لذلك **يقترح الباحث** – فى إطار تطوير سلطات الضبط القضائى أنه يجب على كل دولة أن تنشىء مركز متخصص فى كشف ومواجهة الجرائم المعلوماتية، وأن يشتمل هذا المركز على نوعين أو قسمين :-

الأول: قسم متخصص فى تدريب وتأهيل رجال العدالة " رجال الشرطة، القضاة، والمحققين وغيرهم " وأجهزة العدالة عامة واعدادهم الإعداد المناسب والكافى فى كشف والتحقيق والمحاكمة للجرائم المعلوماتية.

الثانى: قسم متخصص فى رصد الجرائم المعلوماتية وتقصى أثر المجرمين وتتبعهم بما يوصل إلى ضبطهم والقبض عليهم، وهو ما يسمى بشرطة الإنترنت – التى نفذت فى العديد من الدول – يتألف من الأفراد ذو القدرات والكفاءات التقنية العالية الذين يم تدريبهم على أعلى مستوى للتعامل مع هذه الجرائم.

ثانيا الاعتراف بالدليل الرقمى فى الإثبات الجنائى

إن من العقبات التى تقف أمام إثبات الجريمة المعلوماتية، وتعتبر من أهم الصعوبات التى يجب القضاء عليها عدم الاعتراف بالدليل الرقمى كوسيلة من وسائل الإثبات للجرائم بصفة عامة والجرائم المعلوماتية والإنترنت بصفة خاصة، ورأينا فيما سبق عند تناول الباحث أنظمة الإثبات الجنائى والدليل الرقمى **– أن هناك ثلاثة أنظمة للإثبات الجنائى أدلة يتقيد بها القاضى الجنائى ينص عليها المشرع على سبيل الحصر وتتقيد سلطة القاضى فى الحكم بناء عليها** "نظام الإثبات المقيد"، ونظام إعطاء سلطة واسعة للقاضى فى الحكم فى الدعوى بناء على أى دليل يمكن أن يكون اقتناعه " نظام الإثبات الحر "، ونظام الإثبات المختلط الذى يجمع بين النظامين السابقين فيحدد المشرع الأدلة المقبولة ويعطى سلطة تقديرية للقاضى للحكم بناء عليها، وهناك نظام رابع هو نظام الإثبات بالأدلة العلمية الذى ظهر حديثًا ويعطى الدور الرئيسى فى الإثبات للخبير.

وحيث أن الجرائم المعلوماتية ترتكب فى بيئة إلكترونية، ومن ثم فإن الأدلة التى يمكن الحصول عليها هى أدلة رقمية وليست كالأدلة التقليدية التى توجد فى مسرح الجريمة

د/ سالم مرزوق المطرفى، نموذج مقترح لإنشاء مركز تدريب عن بعد بالمديرية العامة للدفاع المدنى بالمملكة العربية السعودية، رسالة ماجستير، جامعة نايف، الرياض، السعودية، عام 2005م، ص 11 .

د/ صالح العساف، المدخل إلى البحث فى العلوم السلوكية، مكتبة العبيكان، عام 1995م، السعودية، ص 33.

د / محمد محمود درويش، التدريب الأمنى ورقة عمل قدمت للحلقة العلمية حول تطوير التدريب الأمنى، المنعقدة بجامعة نايف خلال الفترة 10 – 14 /2003/5، الرياض، السعودية، د/ على سالم " نحو تأهيل خصائص التدريب الأمنى وركائزه " مجلة بحوث الشرطة، العدد 18 عام 2000م .

التقليدى، ولذلك يتعين الاعتراف بالأدلة الرقمية كأهم وسائل إثبات الجريمة المعلوماتية من حيث قبول هذه الأدلة والاقتناع بها والحكم بناء عليها، وذلك بالنص عليها ضمن وسائل الإثبات فى نظام الإثبات المقيد، وإعطاء سلطة تقديرية للقاضى كبيرة فى نظام الإثبات الحر للحكم بناء عليها، وكذلك فى النظام المختلط طالما توافرت فيها اليقينية وخضعت للسلامة فى الحصول عليها وتتسم بالمشروعية.

لكن السؤال هنا ما الذى يؤدى إلى عدم الاعتراف بالدليل الرقمى كوسيلة للإثبات فى الجرائم المعلوماتية سواء فى نظام الإثبات المقيد أو الحر أو غيره ؟

إن السلطة التقديرية للقاضى لا يمكن أن تمتد لتشمل الأدلة العلمية حيث أن الأدلة العلمية تكاد تكون يقينية فى غالبية الحالات ومنها الدليل الرقمى، كما أن القاضى لا يمكن أن يدرك الحقيقة المتعلقة بالدليل الرقمى إلا بواسطة خبير فى غالبية الحالات،، فإن عدم الاعتراف بالدليل الرقمى ليس من ناحية تدليه على الحقائق التى يعبر عنه ولكن الإشكالية تثير من حيث صحة الإجراءات المتبعة للحصول عليه وسلامته من العبث، فإذا توافرت فيه ذلك الأمرين يمكن الاعتراف به كدليل إثبات أو نفى، أى أن الشك فى الدليل الرقمى لا تتعلق بمضمونه كدليل ولكن بعوامل مستقلة عنه ولكنها تؤثر فى مصداقيته، وبالتالى يمكن الاعتراف به والتعويل عليه إذا توافرت فيه هذه العوامل.

ويتم تقييم الدليل الرقمى من حيث سلامته من العبث، ومن حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالى :-

أ- يمكن تقييم الدليل الرقمى من حيث سلامته من العبث بعدة طرق منها :

1- يلعب علم الكمبيوتر دورًا مهمًا فى تقديم المعلومات الفنية التى تساهم فى فهم مضمون وهيئة الدليل الرقمى، وهذه العلوم يستعان بها فى الكشف عن مدى التلاعب بمضمون هذا الدليل.

2- فى حالة عدم الحصول على النسخة الأصلية للدليل الرقمى أو فى حالة أن العبث قد دفع على النسخة الأصلية، ففى الإمكان التأكد من سلامة الدليل الرقمى من التبديل أو العبث من خلال إستخدام عمليات حسابية خاصة تسمى بالخوارزميات.

3- هناك نوع من الأدلة الرقمية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم فى التأكد من مدى سلامة الدليل الرقمى المقصود من حيث عدم حصول تعديل أو تغيير فى النظام الكمبيوترى.

فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل الرقمى ومطابقته للواقع.

ب- تقييم الدليل الرقمى من حيث السلامة الفنية للإجراءات المستخدمة فى الحصول على الدليل الرقمى ويتم ذلك من خلال وسيلتين:

1- إخضاع الأدلة المستخدمة لعدة تجارب للتأكد من دقتها فى إعطاء النتائج المبتغاة وذلك باتباع اختبارين رئيسين هما:

- **اختبار السلبيات الزائفة** ومفاد هذا الإختبار أن تخضع الأدلة المستخدمة فى الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمى، وأنه لا يتم إغفال بيانات مهمة عنه.
- **اختبار الإيجابيات الزائفة،** ومفاد ذلك أن تخضع الأدلة المستخدمة فى الحصول على الدليل الرقمى لإختبار فنى يمكن التأكد من أن هذه الأداة لا تفرض بيانات إضافية جديدة.

ويتم من خلال هذين الاختبارين التأكد من أن الأدلة المستخدمة حصرت كل البيانات المتعلقة بالدليل الرقمى، وفى ذلك الوقت لم تضف إليها أى بيان جديد، وهذا يعطى للنتائج المقدمة عن طريق تلك الألة المصداقية فى التدليل على الواقع.

2- الاعتماد على الأدوات التى أثبتت البحوث العلمية كفاءتها فى تقييم نتائج أفضل :

حيث تدل البحوث المنشورة فى مجال تقنية المعلومات على الطرق السليمة التى يجب اتباعها فى الحصول على الدليل الرقمى، وفى المقابل تثبت تلك الدراسات الأدوات المشكوك فى كفاءتها، وهذا يساعد فى تحديد مصداقية المخرجات المستمدة من تلك الأدوات.

ومن خلال ما تقدم يمكن الوقوف على سلامة الدليل الرقمى والتعويل عليه كوسيلة للإثبات الجنائى للجرائم المعلوماتية[43].

فالخلاصة يرى الباحث: أنه لا توجد ثمة مشكلة فى الإعتراف بالدليل الرقمى فى إثبات الجرائم المعلوماتية من جهة المشرع فى نظام الإثبات المقيد وتطبيقه من جهة القضاء، وكذلك

---

(43) مركز هاردو لدهم التعبير الرقمى فى الجريمة الإلكترونية وحجية الدليل الرقمى فى الإثبات، القاهرة، عام 2014م، مرجع سابق
متاح على الموقع الإلكتروني :-
" كتيب "

فى نظام الإثبات الحر والمختلط طالما توافرت فيه شروط صحة الدليل ومن حيث سلامته من العبث وسلامة الإجراءات المتبعة فى الحصول عليه، وأنه من غير المقبول أن يعيد القاضـــى تقييم الدليل وطرحه من جديد على بساط البحث حيث أن دلالته قاطعة بشأن الواقعة المستشهد به فيها لأنه من الأدلة العلمية يقينة الثبوت ويعتبر من أهم وسائل الإثبات الجنائى فى الجرائم المعلوماتية الذى يفرض نفسه على مسرح الجريمة المعلوماتية ولا يمكن إغفاله فى إثبـــات أو نفى الواقعة المرتكبة فى هذا المسرح الإفتراضى، فيجب على كل دولة الأخذ به كوسيلة مـــن وسائل الإثبات الجنائى فى الجرائم المعلوماتية أيّا كان نظام الإثبات الخاص بها، وذلك بالنص عليه في قوانين الدول التي تأخذ بنظام الإثبات المقيد أو تطبيقه من جانب القضاء في الـــدول التي تأخذ بنظام الإثبات الحر أو المختلط.

الفرع الثاني

استخدام التكنولوجيا الأمنية فى مكافحة الجرائم المعلوماتية

إذا كان من مقتضيات الحكمة أن " الوقاية خير من العلاج " فيجب استخدام الوسائل الفنية التقنية الكفيلة بمنع ارتكاب الجريمة، أو على أقل تقدير التقليل من آثارها وأضرارها، وذلك خيرًا من الانتظار لوقوع الجريمة ثم محاكمة مرتكبيها.

ولا يقصد بالطبع بهذا القول المنع بمفهومه المطلق لاستحالة تحقيق ذلك علميًّا وواقعيًا وذلك لأن الجريمة ناموس من نواميس الطبيعة، وإنما المقصود هو الحد من معدلات وقوع الجرائم، ولا يتحقق ذلك غالبًا بالإجراءات الشرطية وحدها والمتمثلة فى الرقابة على شبكة الإنترنت وتأمينها، إنما يستلزم ذلك الاستعانة بوسائل التكنولوجيا المتطورة والمتاحة فى هذا المجال بهدف تحقيق أقصى درجات الأمان.

وتتمثل استخدام التكنولوجيا الأمنية فى مكافحة الجريمة المعلوماتية فى استخدام تكنولوجيا المعلومات فى العمل الأمنى، واستخدام التدابير التكنولوجية الأمنية فى حماية المعلومات فى النظام المعلوماتى.

وسنتناول ذلك علي النحو التالي

اولا استخدام تكنولوجيا المعلومات فى العمل الأمني

يعد الاتجاه نحو الاعتماد على تكنولوجيا المعلومات فى العمل الأمنى أمرًا منطقيًّا فى ظل الثورات العلمية، وتزايد الحاجة إلى أدوات وأجهزة متطورة تخدم قطاع الأمن فى في علاقته بالمجتمع على المستويين الوطنى والدولى [44].

بل أنه يمكن القول بأن تطور النظام الاجتماعى وما يفرضه من ضروريات بتطور مستوى الأداء الأمنى، يفرض على المسئولين فى العمل الأمنى سرعة الاستجابة لمتطلبات التطورات المعاصرة للاستعانة بالتقنيات التكنولوجية والمعلوماتية.

حيث أن الاعتماد على تكنولوجيا المعلومات فى العمل الأمنى بصفة عامة ومواجهة الجرائم المعلوماتية والإنترنت والتصدى لها بصفة خاصة مزايا عديدة وأهم تلك المزايا :-

1- الفعالية [45]

---

(44) Thamas Kuhn the structure of scinentific Revolutions.
" توماس كون، بيئة الثورات العلمية "، ترجمة : شوقي جلال، عالم المعرفة، الكويت، ص 142 .

والفعالية فى ذلك وجهان :-

الوجه الأول: يتعلق بغنى النظم الاتصالية وشمولها على كم كبير، وهائل من البيانات سهلة التداول، كاملة المضمون، ووفقاً لهذا الاتجاه يعتبر الاتصال الحاسوبى فعالاً للأبد.

الوجه الثانى: خاص بالتفاعل بين البيانات والمرسل والمستقبل لتلك البيانات وهو ما يحقق قدر كبير من فعالية نظم الحاسوب وتتحقق تلك الفعالية عن طريق :-

أ- قابلية تكرار المعلومات وترسيخها.

ب- تعدد الوسائط والحواس.

ج- تفرق الاتصال.

وهذا يؤدى إلى إمكانية الربط بين مختلف خيوط الجريمة والتمكن من اكتشافها قبل ارتكابها والتوصل لمرتكبيها بعد الارتكاب.

2- كفاءة الأداء للأفراد داخل المؤسسة الأمنية (46)

ويتضح ذلك فى :-

أ- توفير طباعة المواد على المؤسسات الأمنية.

ب- تحقيق أعلى درجة من كفاءة الاتصال وذلك بسبب استخدام تكنولوجيا الاتصال بواسطة الحاسب وعبر شبكة الإنترنت.

3- المرونة (47)

حيث أن استخدام الحواسيب وشبكات المعلومات والاعتماد عليها تحقق درجة عالية من المرونة، والتى يمكن التكيف بشكل كبير مع التطورات والتغيرات البيئية والواقع ويتضح مرونة النظم التكنولوجية المعلوماتية من خلال :-

أ- قابلية استبدال الملفات " صور – نصوص – عروض الفيديو – صوت " بشكل سريع لا يتعدى توان محددة.

---

(45) د/ يوسف شمس الدين شاسبوغ، التحريات الشبكية، ورقة عمل مقدمة الى مؤتمر الأمن والتكنولوجيا / 2006م، مركز بحوث شرطة الشارقة، ص 232 .

(46) د/ عبد الرحمن توفيق، التدريب، الأصول والمبادئ، موسوعة التدريب والتنمية البشرية، الإصدار الأول، مركز الخبرات المهنية للإدارة، القاهرة، بدون سنة نشر، ص 257 وما بعدها .

(47) د/ يوسف شمس الدين، المرجع السابق، ص 226 وما بعدها .

ب- إن إلغاء أو تعديل أى مواد غير حاسوبية يتطلب مخصصات تستغرق وقت وجهد يحد من مرونة التعديل عند الطلب، غير أن الحاسوب وشبكات المعلومات لا تتطلب مثل هذه الكلفة.

4- نظام رصد شديد التطور والفعالية وقاعدة بيانات متطورة (48)

تعتبر تكنولوجيا المعلومات عنصرًا هامًا فى مواجهة الجريمة المعلوماتية، وذلك عن طريق جعل قاعدة بيانات ومعلومات لكل شخص أو مواطن يمكن الرجوع إليها لمعرفة شخصه وكافة المعلومات عنه فى حالة إرتكابه أى جريمة معلوماتية.

كما أنها يمكن أن تكون نظام رصد يمكن من خلالها التوصل إلى كل من تسول له نفسه ارتكاب أو الشروع فى ارتكاب الجريمة المعلوماتية، وذلك من خلال البرمجيات والأدوات الحديثة المتطورة التى تستخدم فى حماية المعلوماتية.

والخلاصة أنه لابد من استخدام تكنولوجيا المعلومات فى مواجهة الجرائم فى العمل الأمنى الشرطى، حتى يمكن منع وقوع هذه الجرائم أو ضبط الجناة عند الشروع فى ارتكابها أو القبض عليهم بعد ارتكابها بسهولة ويسر دون عناء فى البحث عنهم ومعرفة هويتهم وتدريب وإعداد وتسليح أفراد الشرطة على ذلك وسد الثغرات الأمنية فى نظم المعلومات.

ويمكن استخدام تكنولوجيا المعلومات عن طريق إنشاء شبكة معلوماتية داخل الدولة مرتبطة ببعضها البعض على مستوى الإقاليم تختص برصد كافة الأنشطة الإجرامية المعلوماتية التى تتم على شبكة الإنترنت وتتضمن قاعدة بيانات بأسماء معتادى الإجرام المعلوماتى، يتم من خلالها الإبلاغ بسرعة عن أى نشاط إجرامي يقع على الشبكة دون الحاجة إلى الإبلاغ من جانب المواطنين، ويمكن أن ترتبط هذه الشبكة المعلوماتية الشرطية بشبكات فى دول أخرى وفقًا لإتفاقيات ثنائية، جماعية، دولية بينهما يتم من خلالها تبادل المعلومات الأمنية بين أجهزة الشرطة، ومتابعة الإجرام المعلوماتى والتعاون بين رجال الشرطة فى تحقيق أعلى قدر من التدريب على ذلك – فهذا الأمر من البديهيات المسلم بها فى مكافحة جرائم المعلوماتية والإنترنت التى ترتكب فى عالم افتراضي يجب أن يكون هناك سرعة فى منع وقوع هذه الجرائم أو القبض على مرتكبيها وتقديمهم للمحاكمة بعد وقوعها من قبل رجال الأمن المدربين على ذلك.

باستخدام تكنولوجيا المعلومات فى العمل الأمنى متمثلة فى كافة البرامج والبرمجيات والأبحاث فى الرصد، المراقبة لمعتادي الإجرام، التتبع، المعاينة، وغير ذلك من الإجراءات

(48) المرجع السابق، ص 229، 230 .

الشرطية يعد ضرورة لابد منها فى مكافحة الجرائم المعلوماتية من جانب رجال الأمن متمثلًا فى جهاز الشرطة وكافة البرمجيات والتقنيات التى يمكن أن تكشف عنها التكنولوجيا الحديثـــة فى المستقبل فى مجال تقنية المعلومات والإتصالات.

ثانيا: استخدام التدابير التكنولوجية الأمنية

أ: تعريف التدابير التكنولوجية

هى تلك الوسائل التى تسعى إلى الحفاظ على أمن المعلومات من خلال تحديد شخص المستخدم ومدى مشروعية دخوله على النظام، والتحكم فى دخوله على الشبكة، وتحقيق سرية المعلومات وتكاملها وتتمثل فى :-

1- وسائل الأمن المتعلقة بالتعريف بشخص المستخدم ومشروعيته.

2- وسائل التحكم فى الدخول والنفاذ إلى الشبكة.

3- وسائل تهدف إلى تحقيق سرية المعلومات.

4- وسائل حماية البيانات وسلامتها.

5- وسائل مراقبة وتتبع الإستخدام وسجلات النفاذ أو الأداء.

وهذه هى الوسائل أو الطرق التى يتحقق بها أمن المعلومات وتشمل كافة أنواع البرمجيات والتقنيات المستخدمة كلاً حسب الغرض المخصوص لأجله البرنامج لتأمين النظام المعلوماتى[49].

فالأمن فى مجال عمل الحاسوب والإنترنت منظورين :-

المنظـــور الأول: أمن الوثائق والمعلومات بما يضمن عدم تسريب ما يتم إرساله وتبادله منها إلى جهات لا يجوز لها الإطلاع عليها وعدم تمكنهم من الاستيلاء أو التسلل إليها وسرقتها أو نسخها.

المنظور الثانى: عدم وصول المتطفلين إلى الأنظمة الحاسوبية، وعدم تمكينهم من الإضرار بالنظم البرمجية سواء من خلال برامج الفيروسات أو الدخول المباشر[50].

---

(49) د/ شريف فتحى الشافعى، تخطيط وتصميم وتركيب شبكات الحاسب الآلى، القاهرة، دار الكتب العلمية للنشر والتوزيع، عام 2002م، ص 174 .

(50) د/ يوسف شمس الدين، المرجع السابق، ص 432 .

ويُعرف أمن المعلومات من المنظور القانونى أنه " محل دراسات وتدابير حماية سرية وسلامة محتوى وتوافر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها فى ارتكاب الجريمة [51] ".

فالتدابير التكنولوجية هى وسائل أمن المعلومات وهى " مجموعة الآليات والإجراءات والأدوات التى تستخدم للوقاية من المخاطر، أو تقليل الخسائر بعد وقوع التعدى على المعلومات وأنظمتها، وتتعدد وسائل الحماية أو الوسائل التأمينية التى يمكن أن تتبعها للوقاية من القرصنة الإلكترونية ومكافحة الفيروسات والمحافظة على المعلومات والبيانات من التسرب ".

ب : أنواع التدابير التكنولوجية " وسائل أمن المعلومات "

1- برمجيات كشف ومقاومة الفيروسات

هى تلك البرامج التى تقوم بحماية الأجهزة من هجمات الفيروسات وتعمل على مكافحة الفيروسات المصممة خصيصًا للإضرار بنظام الحاسب الآلى، وتشكل تهديدًا أو خطرًا على البيانات، ويمكن رصد هذه البرامج فى القرص الصلب والأقراص المدمجة والرسائل الإلكترونية، وتسميتها بمضادات الفيروسات وهو اصطلاح يطلق على هذا النوع من البرمجيات، وتستطيع هذه البرامج مسح أو تعطيل عمل البرامج المهددة لسلامة الجهاز، وملفات البرامج الموجودة على جهاز الحاسب الآلى ويتكون البرنامج المضاد للفيروسات من جزأين مختلفين :-

1- التشغيل المباشر عند الدخول وهذا الجزء يعمل تلقائيًا عند تشغيل الدخول إلى البرامج أو تنزيل الملفات من الإنترنت، وهو ما يعرف " on Access Element ".
2- التشغيل عند الطلب وهذا الجزء يعمل عندما تطلب أنت منه ذلك وهو متخصص بالكشف عن الفيروسات وأحضة طروادة[52]

وقد تطورت برامج الفيروسات من الجيل الأول الماسحات البسيطة ثم الجيل الثانى الماسحات الموجهة إلى الجيل الثالث والرابع ويشمل الحماية المتكاملة.

---

(51) د/ خضر مصباح، أساسيات أمن المعلومات والحاسوب، الطبعة الأولي، عمان، دار الجامعة للنشر، عام 2010م، ص 43 .

(52) Chuck Easttom , Jeff Taylor : " Computer crime , Investigation , and the law " , course Technology , C 2010 , 2010 , p 145.

وهذه البرامج تحمى فقط من الفيروسات والديدان وتستطيع التعرف عليها وإكتشافها والقضاء عليها لكن لا تستطيع أو غير مصممة لحماية النظام المعلوماتى أو الحاسب من الإختراق إلا أنه بعض البرمجيات الحديثة لها خواص الجدار النارى لحماية الجهاز من الإختراق – كما سنرى.

لكن ليس هناك برنامج مضاد للفيروسات قادر على حماية كاملة لجهاز الحاسب الآلى، بالرغم من القيام بالتحديث المستمر لبرنامج مكافحة الفيروسات بصفة مستمرة [53].

2- الجدار النارى

الجدار النارى هو نظام يوفر حماية للشبكة عبر ترشيح البيانات المرسلة أو المستقبلة عبر الشبكة بناء على قواعد حددها المستخدم عموماً، والهدف من الجدار النارى هو تقليل أو إزالة وجود الاتصالات الشبكية غير المرغوب فيها، والسماح فى الوقت نفسه للاتصالات الشرعية أن تنقل بحرية، توفر الجدر النارية طبقة أساسية من الحماية – التى تدمج مع غيرها – تمنع المهاجمين من الوصول لخادمك بطرق خبيثة [54].

فهى عبارة عن أجهزة " Hard ware "، أو برامج " Soft ware "، وتعمل على فلترة أو تصفية حركة البيانات الواردة والصادرة من وإلى الشبكة إعتماداً على قوانين ومعاملات بسيطة، وتتمثل أهم وظائف الجدران النارية فيما يلى :-

1- التحقق من هوية المستخدمين
2- مراقبة الإستخدام وتتبع سجلات الدخول والخروج للشبكة
3- مراقبة المحتوى الوارد إلى الشبكة للبحث عن الفيروسات والبرمجيات الضارة، ومراقبة عناوين الإنترنت وهناك ما يسمى "بالحماية الداخلية لجدار الحماية" وهى حماية الحاسوب عن طريق عملية منع الهجمات من الوصول إليه عبر شبكة الإنترنت، كما أنه يوجد ما يسمى بـ "الحماية الخارجية لجدار الحماية" وهى حماية جدار الحماية للحاسوب عن طريق منع الاتصالات من مغادرة الحاسوب والانتقال خارجيًّا[55].

---

(53) لواء دكتور / أشرف السعيد أحمد، القرصنة الالكترونية، القاهرة، عام 2011م، ص 105 .

(54) متاح على الموقع الإلكتروني :

https://academy.hsoub.com

تم الإطلاع بتاريخ 2020/7/5م .

(55) متاح على الموقع الإلكتروني :

https://www.euro.dell.com

تم الإطلاع بتاريخ 2020/7/6م .

وهناك ثلاثة أنواع أساسية للجدر النارية للشبكة :-

- ترشيح الرزم " packet filtering "
- أو عديمة الحالة "stateless "
- ذات الحالة " Stateful "
- طبقة التطبيقات "application layer "

- ترشيح الرزم أو عديمة الحالة، تعمل عبر تصفح كل الرزم الشبكية على حدة وبالتالى ستكون غير مدركة لحالة الاتصال، ويمكنها فقط أن تسمح أو تمنع مرور الرزم بناء على كل ورقة بشكل منفرد.
- الجدر ذات الحالة، قادرة على تحديد حالة الاتصال للرزم، مما يجعل تلك الجدر أكثر مرونة من الجدر عديمة الحالة، وإنها تعمل عبر جمع الرزم الشبكية المترابطة إلى أن تستطيع تحديد حالة الاتصال قبل أن تطبق أية قواعد للجدار النارى على بيانات التراسل الشبكى.
- صور التطبيقات، تذهب خطوة إضافية إلى الأرقام عبر تحليل البيانات التى قد أرسلت، مما يسمح بمطابقة بيانات التراسل الشبكى على قواعد الجدار النارى التى تكون مخصصة لخدمات أو تطبيقات معينة وتسمى هذه الجدر أيضًا "الجدر النارية البسيطة"(56).

أ- استخدام كلمات المرور

الإنجليزية passord، هى عبارة عن آلية أمان أساسية وتتكون من عبارة مكونة من أحرف أبجدية أو رقمية أو كلاهما معًا، ورمزية، أو جميعها معًا، وعادة ما يتم استخدامها المستخدم للوصول إلى نظام أو تطبيق، أو خدمة خاصة به ويتم استخدامه فى معظم الحالات مع اسم مستخدم " user name "، وتعتبر كلمة المرور من أكثر الإجراءات المستخدمة فى جميع الأجهزة الرقمية والمحوسبة للتحكم فى الوصول، وعادة ما يتم إنشاء كلمة المرور من قبل المستخدم نفسه فى معظم التطبيقات والخدمات، وتكون منفصلة ومختلفة لكل نظام أو خدمة (57).

---

(56) متاح على الموقع الإلكتروني السابق :-

www.academy.shoub.com

تم الإطلاع فى 2020/7/15م .

(57) متاح على الموقع الإلكتروني :-

Pass word " , www.techapedia.com

منشور بتاريخ 2018/6/21م .

ويوجد نوعان لكلمة المرور يمكن إنشاؤها وهى [58] :

- كلمة مرور قوية: وهى كلمة فعالة، ويصعب اختراقها وغالبًا ما تحوى على ستة أو عشرة أحرف، وأرقام ورموز، وتكون الأحرف كبيرة وصغيرة.
- كلمة مرور ضعيفة: وهى كلمة مرور غير فعالة، بسبب سهولة تذكرها وعادة ما تكون تحتوى على الأسماء، تاريخ الميلاد، أرقام الهواتف، كلمات يسهل تخمينها.

ولكن يجب أن تكون كلمة المرور قوية حتى لا يتم اختراق الحساب أو الموقع أو النظام المعلومتى فيجب [59].

1- أن تحتوى كلمة المرور على ثمانية حروف على الأقل أو رموز أو أرقام وست عشر حرفاً أو رمزاً أو رقم إلى 64 حرفاً.

2- تضمين أحرف كبيرة وصغيرة

3- استخدام رقم واحد على الأقل

4- استخدام حرف خاص واحد على الأقل

4- التشفير

عبارة عن دراسة التقنيات الرياضية المتعلقة بعدد من مظاهر أمنية المعلومات مثل الموثوقية " Confidentication " تكامل البيانات " Data Integrity "، إثبات شخصية الكينونة "Entity Authentication"، إثبات شخصية مصدر البيانات " Data origin Authentication" وان التشفير ليس عبارة عن وسيلة لتزوير أمنية المعلومات إنما عبارة عن مجموعة من التقنيات.

فكرة نظام التشفير " cipher system "، وهى إخفاء المعلومات الموثوقة بطريقة معينة بحيث يكون معناها غير معروف للشخص غير المخول له فإن أى شخص يعترض

---

(58) متاح على الموقع الإلكتروني :-

http://www.computerhope.com

منشور بتاريخ 2017/4/26 م .

تم الإطلاع فى 2020/7/17م .

(59) متاح على الموقع الإلكتروني :-

http://www.serchsecurity.techtarget.com

تم الإطلاع فى 2020/7/17م .

عبارة معينة " أى يحصل عليها " مرسلة من المشفر " cryptograpjer " " إلـــى مســـتقبل العبارة يسمى المعترض " Intercepto ".

فهدف التشفير هو الزيادة " Maximize " الى الحد الأقصى لعدم الترتيب لغـــرض إخفـــاء المعلومات، لذلك فإن تقليص عدد الاختصاصات الممكنة، وذلك بمراقبة النماذج الثنائية الغير مقبولة تميل إلى امتلاك نوع من الترتيب.

ويمكن أن يعرف التشفير أيضًا أنه علم الكتابة السرية وعدم فتح شفرة هـــذه الكنيـــة السرية من قبل غير المخولين [60].

فهى إحدى وسائل الحفاظ على سرية البيانات والمعلومات باستخدام برامج لها القدرة على تحويل ترجمة تلك البيانات والمعلومات إلى رموز، بحيث إذا ما تم الوصول إليها مـــن قبل أشخاص غير مخول لهم بذلك لا يمكنهم فهم أى شيء، لأن ما سيظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة، وتنطوى عملية التشفير على تحويـــل النصـــوص العادية إلى نصوص مشفرة على اختلاف أنواع وأشكال البرامج المتخصصة فى هذا المجال، إلا أنها جميعًا تتشارك فى القاعدة أو الأساس، وهى مبنية على مفهوم بســـيط، حيـــث يقـــوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس ويجعلها التشـــفير فـــى مرحلة نقلها عبر الشبكات غير قابلة للقراءة من قبل أى شخص يستطيع أن يتسلل خلسة إلـــى الجهاز دون إذنه [61].

ويتم التشفير من خلال مرحلتين رئيسيتين :

المرحلة الأولى: تتمثل فى تشفير النص على نحو رموز غير مفهومه، أو رموز مقروءة بلغة مفهومة.

والمرحلة الثانية: تتم عقب استلام الرسالة وتتمثل فى فك الترميز، بإعادة النص المشفر إلـــى وضعه الأصلى كنص مفهوم ومقروء، وهذه المسألة تقوم بها برمجيات التشفير التى تختلـــف أنواعها ووظائفها [62].

---

(60) د/ على محمد دهب، التشفير وأمن المعلومات، دولة السودان، كلية دراسات الحاسوب والإحصاء، بدون ناشر، بدون سنة نشر، ص 7 .

(61) أنظر :-

Kiarl Del , eeuw, J. A . Bergstra
The History of Information Security :
A Comprehensive Hand book , Elsevier , c 2007 p . 164 .

(62) أنظر :-

وللتشفير عدة أنواع :-

التشفير المتماثل " Symmetric Encryption "

فى التشفير المتماثل يتم استخدام كل من المرسل والمستقبل للمفتاح السرى ذاته فـــى تشفير الرسالة، وفك تشفيرها، ويتفق الطرفان فى البداية على عبارة المرور Key التى ســيتم استخدامها (63).

التشفير غير المتماثل "Unsymmetric Encryption "

يستخدم التشفير غير المتماثل مفتاحين اثنين تربط بينهما علاقة، يدعى هذا المفتاحان بالمفتاح العام والمفتاح الخاص، وهو يتلاشىء عيوب التشفير المتماثل بوجود علاقــة تــربط المفتاح العام بالمفتاح الخاص (64).

المفتاح العام " public key "، يكون معرفًا لدى أكثر من شخص أو جهة، وهو الرقم الذى يتم تداوله ونشره بين المستخدمين لتشفير البيانات أو المعلومات أو الرسائل الإلكترونية، ويستطيع المفتاح العام فك شفرة الرسالة التى شفرها المفتاح الخاص، ويمكــن اســتخدامه – أيضًا لتشفير رسائل مالك المفتاح الخاص، ولكن ليس بإمكان أحد استخدام المفتاح العام لفــك شفرى رسالة شفرها هذا المفتاح العام، إذ أن مالك المفتاح الخاص هو الوحيد الذى يســتطيع فك شفرة الرسائل التى شفرها المفتاح العام.

المفتاح الخاص " private key " ويعد المفتاح الخاص النصف الآخر المكمل للمفتاح العام للوصول إلى الرقم الأساسي واعادة المعلومات المشفرة إلى وضعها الحقيقى أو الطبيعى قبل التشفير، وهو معروف لدى جهة أو شخص واحد فقط، وهو المرسل ويســتخدم لتشــفير الرسالة وفك شفرتها، وهو الذى يميز كل شخص عن غيره من المستخدمين (65).

هــ- المعلومات الضرورية لإدارة حقول المعلومات

Paulus R . Wayleith : Data Security : laws and safeguards , Nova Science pulishers, Incorporated , 2008 , p . 94 .

(63) أنظر :- د/ محمد القحطانى، خالد الخثبر، أمن المعلومات بلغة ميسرة، المملكة العربيــة الســعودية، الرياض، مركز البحوث، معهد الإدارة العامة، عام 2000م، ص 76 .

(64) لواء دكتور/ أشرف السعيد أحمد، تكنولوجيا المعلومات فى المجال الأمنى، القاهرة، عام 2013م، ص 85 .

(65) أنظر :

John R . Vacca , Computer and information security hand book , Second edition , Amsterdam Elsevier , Morgan Kaufmeunn , 2013 c . p . 124 .

" Rights Management Information "

إدارة حقول المعلومات تتم عن طريق إما التدرج الهرمى، وإما بواسطة التقابل بين الأشخاص والموضوعات:

فبالنسبة للتدرج الهرمى: يتم تحديد حقول الدخول إلى المعلومات فى ظل تدرج هرمى أساسه الأهمية الإستراتيجية للمعلومات، فتبدأ قاعدة الهرم بأقل المعلومات أهمية ثم يبدأ تقييد حق الدخول إلى ما يلى ذلك من معلومات حسب أهميتها، فنكون أمام معلومات خاصة أو سرية أو غاية في السرية.

وأما بالنسبة للاعتماد على المقابلة بين الأشخاص والموضوعات، إذا كان الأسلوب الهرمى يأخذ فى الحسبان مدى أهمية المعلومات كأساس لتنظيم حقوق الوصول إليها.

فإن أسلوب الاعتماد على المقابلة بين الأشخاص والموضوعات بهدف إلى الوصول إلى ذات الهدف حيث يحاول الإجابة عن السؤال الآتى: من يستطيع الوصول ؟ وإلى ماذا ؟

على سبيل المثال فإن مدير إحدى الإدارات يستطيع الوصول إلى كل المعلومات المتعلقة بشئون إدارته والتعديل فيها بالإضافة أو الحذف ولكن من دون المدير لا يستطيعون الوصول إلى جزء من هذه المعلومات فقط.

ومن أمثلة المعلومات التأمينية الضرورية لإدارة حقول المعلومات العلامات المائية الرقمية، وهذه الوسيلة لا تمنع الإعتداء ولكن تتيح إمكان تتبع النسخ الغبر المشروعة [66].

و- ملقم البروكسى

البروكسى هو رابط الاتصال بين المستخدم " USER "، وبين مزود خدمات الإنترنت "ISP" الذى يزود المستخدم بالاتصال لدخول شبكة الإنترنت عبر ضوابط خاصة حسبما تحدده الشركة المزودة، فعندما يقوم المستخدم مثلًا بطلب صفحة ما فى الإنترنت، فإن البروكسى الذى لديه يمر عبر خوادم الشركة، ومن حيث إمكانية دخوله للموقع تقوم هى بدورها بنقله لشبكة المعلومات، وتستخدم الشركة البروكسى فى تجهيزات كثيرة من حيث الأمان والجدار النارى وغير ذلك.

حيث يعتبر البروكسى وكيلًا للمستخدم المتصل بالإنترنت للدخول إلى مواقع الويب مع إخفاء عنوانIP الخاص بجهاز المستخدم عند زيارته بهذه المواقع، وتتشابه بشكل كبير مع

(66) د/ حسام الدين الصغير، قضايا عالمية جديدة فى مجال الملكية الفكرية، ورقة عمل مقدمة فى الإجتماع المشترك بين المنظمة العالمية للملكية الفكرية " الويبو " وجامعة الدول العربية، حول الملكية الفكرية لممثلى الصحافة والإعلام، القاهرة، 23 – 24 مايو 2005م، ص 3 .

محركات البحث من حيث الاستخدام وليس مبدأ العمل ويمكن اعتبارها طاقية إخفاء سحرية لعنوان IP الخاص بالمستخدم، فعلى سبيل المثال عند استعراض المستخدم لصفحة ويب باستخدام Proxy، سيصعب على الموقع الإلكتروني رصد IP الخاص بالمستخدم نظرًا لإتمام الوصول بين الجهاز وخادم الويب بواسطة الخادم الوكيل، وباختصار فإنه وسيط للوصول إلى الموقع الإلكتروني عوضًا عن المستخدم ذاته لتأمين جهاز الأخير [67].

ويوفر البروكسى أعلى درجات الحفاظ على الخصوصية فى سياق عمليات البحث عبر الإنترنت وتوفير أفضل خدمات للعملاء، ومنها جدران الحماية وفلترة البيانات وإخضاع عنوان URL الخاص بالمستخدم للفحص والتحقق من الأمان، وصعوبة تحديد الموقع الجغرافى للمستخدم فيصعب الوصول إليه وبالتالى درجة أمان عالية من الاختراق لجهاز المستخدم والوصول إليه.

ويري الباحث أن هناك عدة إرشادات عامة لحماية النظام المعلوماتى من الجرائم المعلوماتية نعرض أهمها على النحو الآتى :-

1- يجب على كل دولة أن تراجع تشريعاتها الوطنية باستمرار فى تجريم الجرائم المعلوماتية الحالية وما يكشف عنه المستقبل من جديد، وكذلك قوانين إجراءاتها الجنائية وأن تتواءم هذه الإجراءات مع طبيعة هذه الجرائم.

2- عدم الاتصال الدائم بشبكة الإنترنت والحذر من تحميل الملفات المجهولة من الإنترنت.

3- تشفير البيانات واستخدام كلمات المرور القوية باستخدام الأدوات اللازمة والحصول على جدار نارى قبل الدخول للإنترنت والإبقاء عليه.

4- تجنب الدخول إلى المواقع المشكوك فيها وتحميل برنامج مكافحة الفيروسات الغير محدث والعمل على تحديثه كل فترة.

---

(67) متاح على الموقع الإلكتروني:

http://www.lifewire.com
Jerricollins,whatis aweb proxy

منشور بتاريخ 2019/1/29م.
تم الإطلاع فى 2020/7/20م .

5- الحذر من النوافذ المنبثقة على الإنترنت والبرامج الدعائية التى تعمل دون أخـــذ إذن المستخدم والتى تُستخدم للاختراق والتجسس أو تدمير البيانات والحذر عند إقفال هذه النوافذ.

6- عمل نسخ احتياطية من ملفاتك المهمة- التى يخشى إصابتها بالفيروسات أو فقدها - على أقراص خارجية.

7- وأخيراً وليس آخراً تجريم التحايل على التدابير التكنولوجية الأمنية، مـــن كلمـــات المرور والسر والتشفير.. ... وغيرها من وسائل حماية النظام المعلوماتى.

المطلب الثاني

السياسة الجنائية لمواجهة الجرائم المعلوماتية دولياً

هناك العديد من العقبات أمام المواجهة الدولية للجريمة المعلوماتية سواء على المستوى التشريعى "الموضوعى والإجرائى" أو على مستوى التدريب الدولي وفى إطار بناء سياسة جنائية لمكافحة الجرائم المعلوماتية فإنه يجب القضاء على هذه العقبات، فلا يكفى بناء سياسة جنائية داخلية لكل دولة فى سبيل مواجهة هذه الجرائم المستحدثة، بل يجب توحيد هذه السياسات الداخلية للدول فى سياسة دولية واحدة للحد من الجرائم المعلوماتية دوليًّا، وذلك عن طريق عقد المزيد من المعاهدات والاتفاقيات الدولية، ومن خلال القضاء على إشكاليات التعاون الدولى القضائى، والقضاء علي العقبات التي تعترض مجال التدريب لرجال العدالة، وتحسين التعاون الشرطى الدولى بين الدول وتحقيق التعاون الدولى على المستوى التشريعى والمستوى الإجرائي أيضًا فى مكافحتها **وهذا ما سيتناوله الباحث فى هذا المطلب وذلك فى فرعين :-**

الفرع الأول: عقد والانضمام للإتفاقيات والمعاهدات الدولية

الفرع الثانى: تعزيز التعاون الدولى فى مواجهة الجريمة المعلوماتية

الفرع الاول

عقد الاتفاقيات والمعاهدات الدولية والانضمام إليها

إن أولى الخطوات لمواجهة الجريمة المعلوماتية على المستوى الدولى هى عقد الاتفاقيات والمعاهدات الثنائية والجماعية والدولية والانضمام إليها، وأن تتناول هذه المعاهدات تجريم الجرائم المعلوماتية على مختلف أنواعها، وأن تتناول الجوانب الإجرائية فيها وتنظيمها، أى الاتفاق على تجريم الأفعال التى تعد جرائم معلوماتية، وكذلك عقد الاتفاقيات والمعاهدات الخاصة بتسليم المجرمين حتى لا يستطيع المجرم المعلوماتى الهروب إلى أى دولة والإفلات من العقاب، وتوحيد الإجراءات الجنائية على المستوى الشرطى والمساعدة القضائية المتبادلة فالاتفاقيات والمعاهدات الدولية هى التشريع الدولى الذى تعتمد عليه الدول فى مكافحة أى من الجرائم العابرة للحدود، ومنها الجرائم المعلوماتية.

أنه كان هناك العديد من الجهود الإقليمية والدولية فى هذا الشأن. وكذلك إبرام المزيد من المعاهدات والاتفاقيات الدولية لتحقيق التعاون الدولى بصفة عامة والتعاون الدولى فى مكافحة الجرائم المعلوماتية بصفة خاصة.

حيث أن القانون السائد فى بلد ما يصلح لأن يطبق فى حدود جغرافية هذه البلد، إلا أن الأمر مختلف فى الجرائم المعلوماتية التى ترتكب فى بيئة الإنترنت حيث لا حدود بين الدول فى هذا العالم الافتراضى.

كما أنه ما يعتبر فى بلد معين قد يكون فعل مشروع فى بلد آخر طبقًا لقانون هذه الأخيرة، والأمر يجد صعوبة أكبر فى مجال الجرائم المعلوماتية المستحدثة، فمثلًا الولايات المتحدة الأمريكية تحظر قوانين العديد من الولايات ممارسة القمار عبر الإنترنت، ومع ذلك تقف عاجزة أمام انتشار هذه الظاهرة فى بلدان مجاورة على مواقع شبكة الإنترنت والمواطنون يشاهدون العديد من هذه المواقع على الشبكة.

كذلك من الناحية الإجرائية سواء مرحلة قبل المحاكمة " التحقيقات " أو مرحلة المحاكمة أو بعدها، من التفتيش، الضبط، الخبرة.. .. وغيرها من وسائل جمع الأدلة التى تصطدم بفكرة السيادة لكل دولة وطلب المساعدة القضائية " الإنابة القضائية، نقل الإجراءات " كل هذه الإجراءات لابد أن تخضع لضوابط يتم الاتفاق عليها من خلال معاهدات واتفاقيات تتناول هذه الإجراءات التى لا تستطيع دولة بمفردها تنفيذها على إقليم دولة أخرى دون وجود اتفاق مسبق، وكذلك مسألة الاختصاص القضائى بالمحاكمة، وتسليم المجرمين.. . إلخ.

فكل هذه الإجراءات وغيرها يجب أن يكون هناك اتفاق مسبق بين الدول ينظمها، تتمثل فى الاتفاقيات والمعاهدات الثنائية والجماعية والدولية ؛فهى الوسيلة الوحيدة للتغلب على القصور التشريعى فى مواجهة الجرائم المعلوماتية فى توحيد النظم القانونية المتعلقة بها، وبيان الأنشطة الإجرامية التى تشكل جرائم معلوماتية، والاتحاد والتعاون فى مجال الإجراءات الجنائية.

بحيث تكون مهمة هذه الاتفاقيات والمعاهدات تحقيق التناغم والارتباط بين الدول فى مكافحة كافة أنماط الجرائم المعلوماتية الحالية وما يستجد منها فى المستقبل من الناحية الموضوعية والإجرائية.

ولتحقيق التعاون الدولى فى هذا المجال بالإضافة لما سبق ولتفعيل التعاون الدولى لابد من التركيز على العناصر الرئيسية التالية [68] :-

1- الانضمام للمعاهدات الدولية التى تعمل على زيادة التعاون والتنسيق بين الجهود التى تبذلها الدول فى مكافحة الجرائم المعلوماتية.

2- إدخال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلى.

ومن أمثلة الإتفاقيات والمعاهدات الدولية التى ساهمت فى مكافحة الجرائم المعلوماتية من الناحية **الموضوعية** :-

1- اتفاقية حماية الأفراد فى مجال المعالجة الآلية للبيانات الشخصية عام 1981م.
2- الاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والإنترنت عام 1999م.
3- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وتم التوقيع عليها فى مدينة باليرمو عام 2000م.
4- الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتى " بودابست " عام 2001م.
5- اتفاقية الأمم المتحدة لمكافحة الفساد عام 2003م من " الناحية الإجرائية ".
6- اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية فى العقود الدولية " نيويورك 2005م وكذلك يوجد العديد من الاتفاقيات الثنائية والجماعية والدولية للتعاون الدولى فى مكافحة الجرائم العابرة للحدود ومنها الجريمة المعلوماتية التي لامجال لذكرها تفصيلًا.

وكذلك إبرام الاتفاقيات والمعاهدات الدولية للتغلب على شيوع واختلاف النظم القانونية الإجرائية لكى تواكب المتغيرات والتطورات المطردة فى جرائم تقنية المعلومات والتعديلات المتلاحقة فى نصوص قانون العقوبات فى شأنها، وتفعيل الإجراءات الجنائية وخاصة إجراءات الإثبات فى مجال تقنية المعلومات.

وتمثل الإصلاحات الإجرائية الحديثة فى دمج كافة الإبتكارات والتطبيقات الناتجة عن تقنية المعلومات فى مجال الإجراءات الجنائية وبصفة خاصة إثبات جرائم تقنية المعلومات، وتستجيب النصوص المستحدثة لإحتياجات الشرطة القضائية وإستغلالها بالنسبة للتحقيقات فى هذا المجال [69].

---

(68) د/ وليد الزيدى، القرصنة على الإنترنت والحاسوب، التشريعات القانونية، الطبعة الأولى، دار أسامة، عمان، الأردن، عام 2003م، ص 128 .

(69) للمزيد من المعلومات أنظر؛

وقد أبرمت العديد من الاتفاقيات الدولية فى مجالات التعاون الدولى من أجل مواجهة الجرائم المعلوماتية من الناحية الإجرائية، من تفويض الإجراءات الجنائية، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطني لعام2000م، والاتفاقية الأوروبية للإجرام المعلوماتى لعام 2001م، واتفاقية الأمم المتحدة لمكافحة الفساد عام 2003[70] وسبق الإشارة إليهم – حيث ركزت هذه الإتفاقيات على الجوانب الإجرائية فى مواجهة الجريمة المعلوماتية هذا بالإضافة إلى الأحكام الموضوعية لها.

وبالنسبة للجهود العربية المبذولة للتغلب على القصور التشريعى فى مكافحة الجرائم المعلوماتية نجد – القانون الجزائرى العربى الموحد – الصادر بموجب القرار رقم 229، لسنة 1996م [71].

ومن الناحية الإجرائية نجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م قد تناولت الجوانب الإجرائية لجرائم تقنية المعلومات، بالإضافة إلى الأحكام الموضوعية وتجريم كافة الأفعال التى تعد جرائم معلوماتية تناولت التجريم فى الفصل الثانى، والأحكام الإجرائية فى الفصل الثالث منها، والاتفاقية العربية لمكافحة الجريمة المنظمة عبر الوطنية عام 2010م وتناولت بعض الأحكام الإجرائية التى يمكن تطبيقها على الجريمة المعلوماتية عابرة الحدود، وكذلك أحكام موضوعية لبعض الجرائم عابرة الحدود التى يمكن أن تتم أو يشرع فى تنفيذ بعضها باستخدام شبكة المعلومات الدولية " الإنترنت ".

والخلاصة يري الباحث أنه يجب على كل دولة فى سبيل مواجهتها للإجرام المعلوماتى للحد منه، بالإضافة إلى سن تشريعات داخلية لمكافحتها من الناحية الموضوعية والإجرائية، وأن تعقد الاتفاقيات والمعاهدات الثنائية والجماعية، فلا تكفى المواجهة الداخلية فقط لهذه الجرائم عابرة الحدود , إنما يجب أن يكون هناك تعاون دولى فعال فى القضاء على القصور التشريعى الموضوعي وتنوع واختلاف النظم القانونية الإجرائية القائمة، فعلى كافة الدول أن

د/ سعيد عبد اللطيف حسين، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، " الجرائم الواقعة فى مجال تكنولوجيا المعلومات "، الطبعة الأولى، دار النهضة العربية، عام 1999م، ص 59.

(70) للمزيد من التفاصيل أنظر؛

د/ مدحت محمد رمضان، جرائم الإعتداء على الأشخاص والإنترنت، مرجع سبق ذكره، ص 80 وما بعدها .

د/ عمرو زكى عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة لمؤتمر الجوانب القانونية للتجارة القانونية، مقر جامعة الدول العربية، يناير عام 2001م، ص 60 .

(71) للمزيد من المعلومات أنظر؛

د/ على جبار الحسيناوى، جرائم الحاسوب والإنترنت، دار البازورى العملية للنشر والتوزيع، الأردن، عام 2009م، ص 158 .

تواجه هذه الجرائم دوليّا فلا تستطيع أى دولة مهما كانت قوتها السياسية أو الاقتصادية أو الاجتماعية.. .إلخ أن تواجه هذا الإجرام المستحدث بمفردها دون عقد معاهدات واتفاقيات للتعاون بينها، لأن الجرائم المعلوماتية تتسم بسرعة ارتكابها وانتشارها وسهولة محو أدلتها والتخلص منها، وإنها من الجرائم عابرة الحدود ويمكن أن تتعدى آثارها إلى أكثر من دولة , وتثير إشكاليات عدة من الناحية الموضوعية، ومن الناحية الإجراءات الجنائية والاختصاص القضائى وتسليم المجرمين.. . إلخ والتى سبق ذكرها.

الفرع الثاني
تعزيز التعاون الدولى لمواجهة الجرائم المعلوماتية

حتى يتم الحد من الجرائم المعلوماتية دوليًّا فإنه يجب تحقيق أقصى تعاون دولى، وأن يكون هذا التعاون فعالًا – وحتى يكون هذا التعاون الدولى فعالًا ومحققًا ثماره – فإنه يجب القضاء على كافة الصعوبات التى تعترضه، وقد سبق أن **تناول الباحث** الإشكاليات التي تعترض التعاون الدولى من الناحية القضائية وعلى مستوى التدريب لرجال العدالة الجنائية وفى المجال الشرطى ***وسيتناول*** **كيفية القضاء على إشكاليات التعاون الدولى علي النحو التالى :-**

اولا القضاء على إشكاليات التعاون القضائى الدولى

توجد عدة صعوبات تتعلق بالتعاون القضائى الدولى فى مواجهة الجريمة المعلوماتية سواء فى مرحلة قبل المحاكمة " مرحلة التحقيق " أو مرحلة المحاكمة وتسليم المجرمين، وفى سبيل تحقيق وتسهيل التعاون القضائى بين الدول يجب القضاء على هذه الإشكاليات سواء إشكاليات الإنابة القضائية أو الاختصاص القضائى أو إشكاليات تسليم المجرمين على النحو التالى :-

آلية التغلب على إشكاليات الإنابة القضائية

1: إشكالية السيادة

أولى الإشكاليات التى تعترض التعاون الدولى القضائى متمثلًا فى الإنابة القضائية هى إشكالية سيادة الدولة على إقليمها، والسيادة هى السند القانونى الذى تستند إليه الدولة لمباشرة

صلاحياتها الداخلية والخارجية ولا تقبل أى دولة بوضع أى قيود على سيادتها، ولكن إزاء تحقيق مصلحة المجتمع الدولى فى مكافحة الجرائم والقبض على المجرمين الهاربين إلى دول أجنبية قبلت الدول بوضع قيود على سيادتها.

ولكن فى سبيل الحفاظ على فكرة السيادة المخولة لكل دولة وعدم أحقية أى دولة فى التدخل فى شئونها قامت الدول بإبرام المعاهدات والاتفاقيات الدولية سواء الثنائية أو الجماعية, وذلك باعتبارها الوسيلة الدولية لتحقيق الإنابة القضائية – فأصبحت هى الوسيلة الدولية الوحيدة للحفاظ على فكرة السيادة والقضاء على إشكالية السيادة أيضًا التى تعترض تحقيق التعاون الدولى القضائى الذى يتمثل فى المساعدة القضائية أو الإنابة القضائية.

فالإنابة لا تعنى سيادة فوق الدول بل تعنى تعاونًا بين سيادات الدول عن طريق المعاهدات، وهذا لا يصطدم بفكرة السيادة بل تؤكدها وتقويها فى سبيل مواجهة الإجرام العابر للحدود ومنه الجرائم المعلوماتية وتحقيق مصالح المجتمع الدولى والتغلب على الصعوبات المادية والقانونية التى تعترض الإنابة القضائية.

2: إشكالية البطء في الإجراءات

يمكن التغلب على إشكالية البطء فى الإجراءات بالنسبة لطلب الإنابة القضائية بوسيلتين:

أ- الإتصال المباشر بين السلطات القضائية للدول

مما لا شك فيه أن مرور إجراءات التعاون القضائى بالطريق الدبلوماسى يجعلها تتسم بالبطء وكثرة الشكليات، وهو ما يتعارض مع طبيعة الجرائم المعلوماتية التى تتميز بسرعة عبور وتبادل المعلومات من خلال شبكتها، لذلك فإن مكافحة الجرائم المتعلقة بالإنترنت تقتضى ردود سريعة، خشية التلاعب فى البيانات التى قد تشكل دليلًا ضد المتهم [72] والذى سبق شرحه.

والاتصال المباشر بين السلطات القضائية للدول فى طلب الإنابة القضائية يعد أحد الآليات للتغلب على البطء فى الإجراءات, حيث بمقتضى هذه الوسيلة يتم الإتصال مباشرة بين السلطات القضائية، السلطة القضائية الطالبة والسلطة القضائية المطلوب إليها، ويُعَدُّ هذا الطريق أكثر اختصارًا وبالتالى أكثر سرعة ومرونة، وهو بالتالى يتلاءم مع أحوال الضرورة والاستعجال التى تتطلب سرعة اتخاذ إجراء من إجراءات التحقيق, خشية من استحالة اتخاذ

(72) أنظر؛ د/ محمد فتحى أنور، تفتيش شبكة الإنترنت لضبط جرائم الإعتداء على الآداب العامة والشرف والإعتبار التى تقع بواسطتها، مرجع سبق ذكره، ص 547 .

الإجراء بفوات الوقت، لهذا فقد نصت غالبية التشريعات الوطنية والاتفاقيات الدولية المعنية بتنظيم الإنابة القضائية الخارجية على جواز اتباع هذا الطريق فى أحوال الاستعجال [73].

واتبعت ذات الطريقة كل من اتفاقية التعاون القضائى فى المواد الجنائية فى مصر وفرنسا، والاتفاقية العربية لمكافحة الإرهاب والإتفاقية الأوروبية للمساعدة القضائية فى المسائل الجنائية عام 2000م [74].

واتفاقية لاهاى عام 1954م وتعديلاتها عام 1970م وتعتبر من أهم الاتفاقيات الدولية المعقودة فى هذا الشأن على مستوى الصعيد الدولى.

ووضعت اتفاقية بودابست حلّا للبطء فى إجراءات التعاون القضائى الدولى، ومنها طلب الإنابة القضائية فى المادة 3/25 وهى – الاتصال السريع بين الدول الأطراف – وبالتالى يمكن أن يتم ذلك بين السلطات القضائية للدول [75].

ب– التنفيذ الإلكتروني للإنابة القضائية

ويمكن أن يتحقق ذلك عن طريق :–

1 التحقيق عن بعد: يمكن للتحقيق عن بعد أن يتغلب على مساوئ فاعلية الإنابة القضائية الدولية ومنها البطء فى الإجراءات المادية والفنية لتنفيذ هذه الإجراءات فدورها مادى لا يمتد إلى القيام بأعمال قضائية والدولة الطالبة هى التى تباشر إجراءات التحقيق بهذه التقنية.

ولا شك أن ذلك يوفر الكثير من الوقت والجهد والمال والبطء فى إجراءات الإنابة القضائية الدولية وتجنب نقل المتهمين ذوى الخطورة.. ..إلخ [76]، وكذلك اختلاف النظام الإجرائى بين الدولة الطالبة والمنفذة.

وقد اتجهت إلى الأخذ به بعض التشريعات الجنائية الحديثة وبعض الإتفاقيات الدولية المنظمة للتعاون الدولى، فقد أخذ بالتقنية التشريع الإيطالي بموجب المرسوم رقم 306 لعام 1992م , وكذلك الولايات المتحدة سواء فى مجال التحقيق على المستوى الداخلى أو فى مجال

---

(73) د/ أمين عبد الرحمن محمود، الإنابة القضائية، رسالة دكتوراة، حقوق الإسكندرية، عام 2011م، ص 298 .

(74) متاح على :

http://conventions.coe-int/treaty/fr/reports/html/0300/htm.

(75) د/ هلالى عبد اللاه أحمد، إتفاقية بودابست، مرجع سبق ذكره، ص 323 .

(76) للمزيد من المعلومات أنظر ؛

د/ عمر سالم، الإنابة القضائية الدولية، فى المسائل الجنائية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، عام 2001م، مرجع سبق ذكره، ص 180 وما بعدها .

المساعدة القضائية فى المسائل الجنائية حال وجود إتفاقية دولية تقضى بذلك , كما أقرت بهذه التقنية **الاتفاقية الأوروبية الجديدة للمساعدة القضائية المتبادلة بين دول الاتحاد الأوروبي فى المسائل الجنائية لعام 2000م**[77].

2- التقاضى الإلكتروني: وهو عملية نقل مستندات التقاضى الإلكتروني إلى المحكمة عبر البريد الإلكتروني إذ يتم فحص هذه المستندات بواسطة الموظف المختص وإصدار قرار بشأنها بالقبول أو الرفض وإرسال إشعار إلى المتقاضى يفيده علماً ما تم بشأن هذه المستندات [78].

ويشمل مفهومها المحاكم المعلوماتية والإلكترونية والبحث فى وسائل ونظم جديرة لتسجيل الدعاوى وحضور الأطراف والتمثيل القانونى وتقديم البيانات الخطية والشخصية والترافع وتقديم لوائح الطعن ومتابعتها والحصول على قرار الحكم وتنفيذه وتدوين الإجراءات ومباشرة المحاكمات بصورة عامة بوسائل غير تقليدية تتميز بالحداثة والسرعة العالية والدقة فى المواعيد والحضور الإلكتروني دون داع للمجيء شخصاً إلى المحاكم [79].

وقد إستطاعت دول عديدة تحويل المحاكم التقليدية إلى محاكم إلكترونية عن طريق إدخال وسائل رقمية متقدمة بنشر المعلومات والقرارات القضائية للجميع والاطلاع على الوثائق والمستندات عبر شبكة الإنترنت من خلال بوابات إلكترونية تفاعلية ومن هذه الدول، الولايات المتحدة وهولندا وأستراليا وسنغافورة والنمسا [80].

ويمكن إستخدام التقاضى الإلكترونى والإستفادة منه فى الجريمة المعلوماتية بالقدر الذي يسمح بذلك إلا انه يوجد أنواع منها لا يمكن إستخدامه وتلجأ الدول إلى تسليم المجرمين فى حالة وجود إتفاقية دولية بينها تسمح بذلك.

---

(77) للمزيد من المعلومات أنظر :
د/ عادل يحيى، التحقيق والمحاكم الجنائية عن بعد، دراسة تحليلية تأصيلية لتقنين الفيديو video فى المجال الجنائى، دار النهضة العربية، القاهرة، الطبعة الأولى، عام 2006م، ص 16 وما بعدها .

(78) د/ خالد ممدوح إبراهيم، التقاضي الإلكتروني، الدعوى الإلكترونية وإجراءاتها أمام المحاكم، دار الفكر الجامعى عام 2008م، ص1، بحث منشور على شبكة الإنترنت على الموقع الإلكتروني :-
http://www.kenananonline.net

(79) القاضى حازم محمد الشرعة، التقاضي الإلكتروني والمحاكم الالكترونية، الطبعة الأولي، دار الثقافة للنشر والتوزيع، عمان، عام 2010م، ص 55 .

(80) الكاتب أحمد عامر عبد الله، القضاء الإلكتروني هو الحل، مقال منشور فى مجلة الأهرام الرقمى، منشور على شبكة الإنترنت على موقع : Htto://www.digital.ahram.org
متاح على موقع البحث Google .
تم الإطلاع فى 2020/7/24م .

ثانيا آلية التغلب على إشكالية تنازع الإختصاص القضائى الدولى

إن لقواعد الإختصاص القضائي أربعة مبادئ وهم مبدأ الإختصاص الإقليمي، مبدأ الإختصاص الشخصى، مبدأ الإختصاص العينى، مبدأ الإختصاص العالمي، وأقرب المبادئ للتطبيق على الجريمة المعلوماتية العابرة للحدود هو مبدأ الاختصاص العالمى ووفقاً لهذا المبدأ يطبق القانون الجنائي على أى جريمة يقبض على مرتكبيها فى اقليم الدولة أى كان مكان إرتكابها وجنسية الفاعل أو الجانى[81].

وبالتالى فإن حل إشكالية تنازع الإختصاص القضائى الدولى، يكون من خلال إعتبار الجرائم المعلوماتية من الجرائم الدولية وبالتالى يعطى الحق لأى دولة يوجد على أراضيها مرتكب الجريمة بملاحقته والقبض عليه ومحاكمته دون أى إعتبار لجنسية مرتكب الجريمة المعلوماتية أو المكان الذى أُرتكبت فيه , أى يحق لأى دولة أن تحاكم مرتكبها الموجود داخل الأراضى الوطنية عليها، طالما ينص عليها قانونها العقابى [82].

وعلى ذلك فإن القانون الدولى هو الذى يحكم أو يمكن أن يستوعب الأحكام الخاصة بتلك النوعية من الجرائم المستحدثة، وليس القانون الوطنى وذلك بتحقيق العدالة الجنائية فى مكافحة الجرائم المعلوماتية فى إطار من الشرعية القانونية والإجرائية، وأهمية إفراز سياسة موحدة فى مجال تناول المعلومات وتطوير وسائل الملاحقة القضائية لضمان مكافحة مرتكبى الجرائم المعلوماتية، ولتفادي مساوىء مبدأ الإقليمية التى ظهرت جلياً نتيجة تطور وسائل الإتصال المعلوماتية العابرة للحدود المكانية للدول [83].

ويتم ذلك عن طريق عقد المعاهدات والإتفاقيات الدولية بخصوص مكافحة الجرائم المعلوماتية والنص على هذه الجرائم ضمن الجرائم الدولية فى المعاهدات الدولية المتعقودة بالفعل وذلك للسماح بتطبيق هذا المبدأ على الجرائم المعلوماتية العابرة للحدود وإعتبارها من الجرائم الدولية التى تتيح لكل الدول محاكمة مرتكبى هذه الجرائم إذا وجد على إقليمها أى

---

(81) د/ محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، دار النهضة العربية، عام 2002م، مرجع سبق ذكره، ص 723 .

(82) للمزيد من المعلومات أنظر ؛

د/ أحمد فتحى سرور، الوسيط فى قانون العقوبات، القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، عام 1996م، ص 229 .

د/ مأمون سلامة، قانون العقوبات القسم العام، مطبعة جامعة القاهرة والكتاب الجامعى، عام 1991م، د/ عمر السعيد رمضان، شرح قانون العقوبات، القسم العام، طبعة 1994م، ص 112 .

(83) د/ محمد سامى عبد الحميد، أصول القانون الدولى العام، الطبعة الخامسة، دار الجامعة، الإسكندرية، عام 1996م، ص 32 وما بعدها .

إعتبار الجريمة المعلوماتية من الجرائم الدولية وإدراجها فى الإتفاقيات الدولية التى تواجه هذه الجرائم والنص عليه أيضاً فى الإتفاقيات الخاصة بمكافحة الجرائم المعلوماتية وقد أخذ بهذا المبدأ المشرع المصرى فى قانون مكافحة جرائم تقنية المعلومات فى المادة (3) من الباب الأول " الأحكام العامة ".

المادة "(3)" نطاق تطبيق القانون من حيث المكان، حيث نص فى الفقرة الرابعة " إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة تمارس أنشطة إجرامية فى أكثر من دولة من بينها جمهورية مصر العربية.

والفقرة " 5 " إذا كان من شأن الجريمة إلحاق بأي من مواطنى جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأي من مصالحها فى الداخل أو الخارج.

والفقرة "6" إذا وجد مرتكب الجريمة فى جمهورية مصر العربية بعد إرتكابها ولم يتم تسليمه " وكذلك العديد من قوانين مكافحة الجرائم المعلوماتية العربية.

وقد نصت على هذا المبدأ العديد من الإتفاقيات الدولية وعولت عليه فى ذلك خصوصاً إتفاقية بودابست عام 2001م.

والخلاصة يري الباحث أنه يجب على جميع الدول التعويل على هذا المبدأ فى مكافحتها للجريمة المعلوماتية وذلك عن طريق النص عليه في قوانينها الداخلية وفى المعاهدات الدولية الخاصة بمكافحة الجريمة المعلوماتية وذلك بسبب أهمية هذا المبدأ وملائمته للجريمة المعلوماتية وذلك لخطورتها وذلك فى كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية الإجرامية بين أكثر من دولة وفى فترات زمنية قصيرة جداً ولسهولة تنصل الجاني من المحاكمة أو توقيع العقاب على المجرم الموجود على إقليم دولة أخرى نظراً لإختلاف قوانين العقوبات والإجراءات الجنائية للدول.. .. إلخ.

ثالثا آلية التغلب على إشكاليات التسليم

أ : آلية التغلب على إشكالية إزدواجية التجريم

لأجل التغلب على إشكالية التجريم المزدوج ركزت الإتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط وذلك بإدراج أحكام عامة فى المعاهدات والإتفاقيات الدولية المعنية بتسليم المجرمين، وذلك إما بسرد الأفعال التى

تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضى قوانين الدولتين معاً أو بمجرد السماح بالتسليم لأى سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة فى كل دولة [84].

وبالتالى يمكن ان ينص فى الاتفاقيات التى تعقد بين الدول فى مجال التسليم على الجرائم المعلوماتية التى يجوز فيها التسليم أو الأفعال التى تشكل هذه الجرائم، إلا أنه مع تطور الجرائم المعلوماتية وتعقد أساليب إرتكابها فإنه يجب أن يكون هناك تنسيق أو توحيد بين التشريعات المختلفة فيما تتعلق بتعريف الجريمة المعلوماتية، وعدم إشتراط إزدواج التجريم كشرط للتسليم فى المعاهدات الدولية، خصوصاً بالنسبة للدول التى لم تجرم بعد الجرائم المعلوماتية، وتوجد بعض الإتفاقيات التى لم تنص على شرط إزدواجية التجريم كشرط للتسليم ومنها الجرائم المعلوماتية مثل الإتفاقية الثنائية المتعلقة بالمساعدة القانونية المتبادلة بين أمريكا وكندا والتى لم تتطلب إزدواجية التجريم، وتدخل الجرائم المعلوماتية فى إطار هذه الإتفاقية [85].

واتفاقية جامعة الدول العربية التى أجازت التحلل من شرط إزدواجية التجريم، إذا كان الشخص المطلوب من رعايا الدولة طالبة التسليم أو من رعايا دولة أخرى تقرر نفس العقوبة , ولكن الأفضل استثناء هذا الشرط بالنسبة للجريمة المعلوماتية.

بـً: آلية التغلب على إشكالية التزاحم فى طلبات التسليم

لم تستقر الإتجاهات الدولية فى تحديد أولويات التسليم فى حالة تزاحم الطلبات حيث تلاحظ إختلافات جذرية فى تحديد وترتيب هذه الأولويات بين الدول، كما نلاحظ ذات الإختلاف فى الدولة الواحدة فى كل إتفاقية على حدة، ولا شك أن ذلك يرجع إلى إختلاف مصالح وأولويات الدول بصفة أساسية.

فإذا نظرنا إلى الإتفاقية الأوروبية للتسليم نجد أنها أشارت إلى حالة تزاحم الطلبات فى المادة "(17) " حيث رتبت أولويات التسليم حيث أوصت أن تأخذ الدولة المطالبة كل الإعتبارات عند تحديد الدولة التى بها أولويات التسليم، مع الوضع فى الإعتبار كل الظروف وبصفة خاصة خطورة الجريمة، مكان إرتكابها وتواريخ الطلبات المقدمة وجنسية الشخص المطلوب.. ..إلخ، اما الإتفاقية النموذجية للتسليم فقد جاءت صياغتها بلا فائدة تذكر حيث

---

(84) د/ حسين بن سعيد الغافرى، السياسة الجنائية فى مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص 558 وما بعدها .

(85) للمزيد من المعلومات أنظر؛

د/ جميل عبد الباقى الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، عام 2002م، مرجع سبق ذكره، ص 91 .

قضت المادة " (16) " منها بأنه إذا تلقى أحد الطرفين طلب تسليم الشخص ذاته من الطـــرف الآخر ومن دولة ثالثة فإنه يحدد تبعاً لما يراه مناسباً إلى أى من هاتين الدولتين ينبغى أن يسلم الشخص [86].

وإذا ذهبنا إلى إتفاقية جامعة الدول العربية نجد ؟أن المادة "(13)" منها حددت أولويات التسليم حيث نصت على أنه " إذا تقدمت للدولة المطلوب إليها عدة طلبات مـــن دول مختلفـــة بشأن تسليم متهم بذاته من أجل نفس الجريمة فتكون الأولوية للتسليم للدولـــة التـــى أضـــرت الجريمة بمصالحها، ثم للدولة التى إرتكبت الجريمة على أرضها ثم إلى الدولة التـــى ينتمـــى إليها المطلوب تسليمه أما إذا كانت طلبات التسليم خاصة بجرائم مختلفة فتكون الأولوية للدولة التى طلبت التسليم قبل غيرها [87].

وقد عالجت جميع الإتفاقيات المصرية مشكلة تزاحم الطلبات بوضع معايير كاتبـــه إذا كانت مصر الدولة المطلوب منها التسليم مثل نص المادة " (34) " من الإتفاقيـــة المصـــرية الفرنسية التى نصت على أن " إذا قدمت للدولة المطلوب إليها عدة طلبات تســـليم مـــن دول مختلفة أما عن ذات الأفعال أو أفعال متعددة فيكون لهذه الدول أن تفصل فى هـــذه الطلبـــات بمطلق حريتها، على أن تراعى فى ذلك كافة الظروف وعلى الأخص إمكان التسليم اللاحـــق فيما بين الدول، وتاريخ وصول الطلبات ودرجة خطورة الجرائم والمكان الذى أُرتكبت فيـــه [88].

أما إذا كان الشخص المطلوب تسليمه لإرتكابه إحدى الجرائم المعلوماتيـــة المضـــرة بالدولة الطالبة والذى تتزاحم عليه طلبات التسليم موجهاً إليه إتهام أو صادر ضده حكـــم فـــى الدولة المطلوب إليها لإرتكابه إحدى الجرائم الماسة بها وكانت الجريمة الثانية أشد خطـــورة من الجريمة المعلوماتية المطلوب التسليم من أجلها، فإن فى الحقيقة لم ترد نصوص فـــى أى إتفاقيات دولية أو تشريعات وطنية تعالج هذه المشكلة.

---

(86) للمزيد من المعلومات حول هذا الموضوع أنظر ؛

د/ أحمد محمد السيد عبد الله، التعاون الدولى فى الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراة، حقوق المنصورة، عام 2009م، ص 394 وما بعدها .

(87) إتفاقية تسليم المجرمين المعقودة بين دول الجامعة العربية والموقع عليها فى 9 يونيه سنة 1953م متاح على الموقع الإلكتروني :-

http://www.laweg.net/Default.aspx?action=viewActivepages&itemid=21002&type=6

تم الإطلاع بتاريخ 2020/7/17م .

(88) أنظر فى ذلك الإتفاقية الفرنسية لتسليم المجرمين متاح على موقع البحث Google .

ويرى البعض أن الأولى – **يذهب معه الباحث** – تطبيق مبـــدأ الإقليميـــة ومحاكمـــة الشخص المطلوب عن الجريمة التى وقعت منه فى الدولة المطلوب إليها وتوقيع العقاب عليه أولاً وعلى الدولة المطلوب إليها أن تخطر الدولة الطالبة بذلك والدولة الطالبة عليها أن تقـــدم طلب التسليم بعد إستيفاء العقوبة للشخص المطلوب تسليمه، ويتم بحثه من جديد والبت فيه – ويكون ذلك إذا كانت الجريمة التى يحاكم عليها المطلوب تسليمه على درجـــة كبيـــرة مـــن الخطورة من الجريمة المعلوماتية المطلوب تسليمه لأجلها ,أما إذا كانـــت بســـيطة أو تافهـــة وكانت بهدف عرقلة إجراءات التسليم تعين على الدولة المطلوب إليها التسليم تسليم الشـــخص إلى الدولة الطالبة [89].

أما فى حالة تعدد جنسية المطلوب تسليمه، فى حالة ما إذا كان الشـــخص المطلـــوب يتمتع بجنسية الدولة الطالبة إلى جانب أخرى فإن هذه الدولة بالتأكيد ستتمسك بالقواعد العامة التى تطبقها فى هذا الخصوص، فقد ترفض تسليمه للدولة الثانية حتى ولو كان يحمل جنسيتها ،وقد توافق على التسليم إنطلاقاً من الضوابط والمعايير التى تحددها من حقوقه كمواطن.

أما إذا لم يكن يحمل جنسية الدولة المطلوب إليها، وبالتالى يخضع الأمر كلـــه هنـــا للعلاقات الدبلوماسية ويمكن أن يخضع لمبدأ المعاملة بالمثل وقواعد المجاملات الدولية التـــى تحددها طبيعة العلاقة بين الدول الأطراف فى التسليم [90].

والخلاصة يرى الباحث بخصوص شرط إزدواجية التجريم فى التسليم عدم النص عليه فـــى الإتفاقيات والمعاهدات الدولية الخاصة بتسليم المجرمين والجريمة المعلوماتية وخصوصاً وأن الجريمة المعلوماتية من الجرائم المستحدثة التى يمكن أن توجد بعض الدول التي لم تجرمهـــا فى تشريعاتها كما أنها فى حالة تطور مستمر ودائم الأمر الذي يصعب وضعها فـــي قالـــب يحتوي علي كافة أشكالها المتنوعة – ولا تستطيع معه التشريعات الجنائية الإلمام بما يســـتجد منها وحصرها بالإضافة إلى آثارها المدمرة التى تتعدى حدود الدول.

وبالنسبة لإشكالية التزاحم فى طلبات التسليم – فإنه من الأولى [91] عقد إتفاقية دولية تتضمن وضع ضوابط موضوعية وآليات محددة يتبعها المجتمع الدولى، على أن يتم وضـــع

---

(89) د/ أحمد محمد السيد، المرجع السابق، ص 400 .

(90) د/ أحمد عبد الكريم سلامة، المبسوط فى شرح نظام الجنسية، الطبعة الأولى، دار النهضة العربية، عام 1993م، ص 574 .

(91) للمزيد من المعلومات أنظر ؛

د/ عبد الغنى عبد الحميد محمود، تسليم المجرمين على أساس المعاملة بالمثل , مجلة كلية الشريعة والقـــانون بالقاهرة، العدد 16، عام 1997 / 1998م، ص 161 .

هذه الضوابط وتلك الآليات بصفة موضوعية مجردة وبعيدة عن مصالح دولة بعينها ويقدم فيها مصالح الجماعة الدولية بأسرارها بصفة عامة فتكون الأولوية للتسليم لأكثر دولة أضرت الجريمة على أرضها ثم إلى الدولة التى تنتمى إليها المطلوب تسليمه وفى حالة تعدد الجنسيات نتناول كيفية علاج ذلك وإذا تساوت الجريمة فى الخطورة تكون الأولوية للدولة التى قدمت طلبها أولاً.

أو على الأقل تحديد هذه الضوابط وتلك الآليات فى المعاهدات والإتفاقيات الدولية لتسليم المجرمين الثنائية أو الجماعية والإتفاق عليها وكذلك النص عليها فى التشريعات الداخلية للدول.

ثانيا تدعيم التعاون الدولى فى مجال التدريب

لا شك أن التدريب على مواجهة الجرائم المعلوماتية هى إحدى أهم الوسائل اللازمة لمكافحتها والحد منها على المستويين الداخلى والدولى، حيث أنها تتسم بالتقنية العالية فى ارتكابها وسرعة تطورها وصعوبة ملاحقة التقدم التكنولوجى فى أساليب ارتكابها وبناء على ذلك فلابد أن تقوم كل دولة بتدريب كل شخص يتصل بمكافحتها، سواء كان رجال الأمن أو النيابة العامة أو القضاء أو الخبراء ورفع مستواهم المهنى فى الإلمام بكافة جوانبها من اكتشافها وإثباتها وتحقيقها حتى إصدار حكم فيها بالأمانة أو البراءة – وقد تناولنا ذلك سابقًا ونحيل إليه منعًا للتكرار [92].

فلا يكفى أن يكون هناك تدريب لرجال العدالة على المستوى الداخلى بل لابد أن يكون هناك تعاون دولى فعال فى مجال التدريب على كيفية التعامل مع هذه الجرائم عابرة الحدود ومكافحتها والحد منها , وذلك للكوادر البشرية القائمة على تنفيذ القانون وتطبيقه والاستعانة بالخبرات والتكنولوجية الحديثة فى كل دولة وخاصة فى الدول المتقدمة كما تناولنا سابقًا.

وقد رأينا فيما سبق – أمثلة لتحقيق التعاون الدولى فى التدريب وصعوبات تعترض التعاون الدولى فى هذا المجال منها ما يتعلق بالقيادات الإدارية ومنها ما يتعلق بالملامح العامة للبيئة التدريبية ومنها ما يتعلق بالفوارق الفردية للمتدرب ونظرة المدرب للتدريب ذاته، وفى سبيل نجاح التعاون الدولى فى التدريب على مكافحة الجريمة المعلوماتية يجب القضاء على هذه الصعوبات الداخلية بالإضافة إلى عقد المزيد من المعاهدات والاتفاقيات الدولية فى مجال

(92) أنظر ؛ الباب الثانى، الفصل الثانى، المبحث الثانى ،المطلب الأول، ماهية التدريب .

التدريب، وعقد الندوات وورش العمل والدورات التدريبية الدولية – أى بـذل الجهـد علـى المستوى الدولى.

فبالنسبة للإشكاليات الداخلية, فإنه يجب على كل دولة أن تحفز على التدريب للقيادات الإدارية بها وعدم الإقتصار على ما تعلمه المتدربون فى الدورات التدريبية الداخلية وذلك لان الجرائم المعلوماتية فى حالة تجدد وتطور مستمر وأن تعتمد ميزانية للتدريب فى الخارج وأن تبرم البروتوكولات اللازمة مع الدول خاصة الدول المتقدمة فى هذا المجال.

أما بخصوص البيئة التدريبية, لابد أن تتناول الجرائم المعلوماتية الحقيقية التى إرتكبت بالفعل وتحليل كيفية إرتكابها وأساليبها وكيفية إنتقالها إلى عدة دول فى وقت قصير جـداً أى يجب أن تكون البيئة التدريبية متطابقة مع الواقع العملى للجرائم المعلوماتية.

وبالنسبة للمدرب والمتدربين, فإنه يجب على كل دولة أن تقوم بتدريب المدربين بصفة دورية ومستمرة وأن تعمل علي تطوير قدراتهم وتحديثها والإلمام بكل ما هو يستجد فى عالم المعلوماتية والاتصالات حتى يمكن تحقيق العملية التدريبية على المستوى الدولى بكفاءة وعدم الاكتفاء بما حصل عليه المدرب فى مجال دراسته من مؤهلات أو شهادات ،حتي ولو تطلـب الأمر الاستعانة بالهاكرز أو محترفى الجرائم المعلوماتية الذين قضوا عقوبـاتهم فـى تنميـة مهاراتهم والتدريب.

وبالنسبة للمتدربين فعلى الدول أن تقضى على الفوارق الفرديـة للمتـدربين، وذلـك بتبسيط منهج التدريب كى يصل إلى كل الأشخاص أو الشخص ذو القدرات المحدودة فى الفهم حتى يتم فهم واكتساب وإتقان العملية التدريبية؛ حتى يكونوا على قدر كبير من المهارة لتحقيق التعاون الدولى فى مجال التدريب مع الدول الأخري بعد ذلك.

وبعد القضاء على الإشكاليات الداخلية التى تعترض التعاون الدولى فى مجال التدريب والتي تقف عائق دون تحقيقه، لابد أن تقوم كل دولة بعد ذلك بعقد والانضمام إلى المعاهدات والاتفاقيات الثنائية والجماعية والدولية, لتدريب رجال العدالة لديها على الجرائم المعلوماتيـة سواء كانوا من مأمورى الضبط القضائى أو النيابة العامة أو القضاة أو الخبراء، وكـل مـا يتصل بمكافحة الجريمة المعلوماتية لتدريبهم ورفع قدراتهم والإلمام بكـل مـا هـو جديـد ومستحدث طرأ عليها ودراسة الحالات المختلفة والتقنيـات المسـتخدمة فيهـا وموضـوعها ومحاورها وتحليلها والوصول إلي وسائل الوقاية والمكافحة.

ويكون ذلك عن طريق عقد البرتوكولات بين الجهات الداخلية لكل دولة ونظائرها فى الدول الأخرى مثل وزارة الداخلية المصـرية ووزارة الداخليـة الفرنسـية ووزارة العـدل

ونظيرتها فى دولة أخرى.

كذلك عقد المؤتمرات والندوات وورش العمل على المستوى الدولى وتنظيم الدورات التدريبية وذلك من خلال المنظمات الإقليمية والدولية.

فلابد أن تسعى كافة دول العالم فى مواكبة التطورات وأن تتعاون فيما بينها وخاصة الدول النامية ينبغي عليها أن تتعاون مع الدول المتقدمة فى مجال تقنية المعلومات للتدريب على مواجهة الجرائم المعلوماتية ونقل الخبرات والمعلومات والمهارات التقنية لرجال العدالة لديها.

ويمكن أن تتم العملية التدريبية على المستوى الدولى عن طريق تدريب رجال العدالة عن بعد، ويقصد به نظام أو أسلوب تدريبى يستطيع المتدرب أو المرشح أيا كان موقع عمله أن يلتحق بدورة أو برنامج تدريبى أو يحضر مؤتمر أو ندوة أو حلقة علمية بشكل متزامن أو غير متزامن دون الحاجة إلى الحضور الشخصى لمكان إنعقادها أو التقيد بعدد المتدربين أو الوقت بطريقة مرنة وذلك عبر وسائل إتصال تقنية حديثة ووسائط أخرى [93] كشبكة الإنترنت.

ولا شك أن هذا النظام يوفر الوقت والجهد والمال، ويتيح لكافة الدول تحقيق التعاون بينها فى مجال تدريب رجال العدالة بكل سهولة، والوصول إلى العديد من مصادر المعرفة التكنولوجية والتدريب.

كذلك اعتماد وتبادل البحث العلمى لتطوير خطط وبرامج التدريب بين الدول حيث سيساهم ذلك فى نقل النتائج والتوصيات التى يتوصل إليها الباحثون وستزيد من الإثراء الفكرى لرجال العدالة ورفع الأداء المهنى لديهم.

فالخلاصة يري الباحث – أنه يجب على كل دولة أن تتعاون مع الدول الأخرى فى مكافحة الجرائم المعلوماتية للحد منها وذلك في مجال التدريب – فلا يكفى تحقيق التعاون التشريعي والقضائى فقط – ويتم ذلك عن طريق القضاء على كافة الصعوبات التى تعترضها داخلياً فى مجال التدريب وعقد والإنضمام للمعاهدات والإتفاقيات الدولية لتحقيق التعاون الدولى بصفة عامة والتعاون الدولى فى مجال التدريب لرجال العدالة على هذه الجرائم المستحدثة بصفة خاصة وعقد المزيد والمزيد من الندوات والمؤتمرات والدورات التدريبية

(93) د/ محمد قطب، الظواهر الإجرامية المستحدثة وطرق مواجهتها، دراسة مقارنة بين القانون الوضعى والشريعة الإسلامية، بحث غير منشور، الأكاديمية الملكية للشرطة، البحرين، عام 2010م، ص 173 .

وورش العمل وتطبيق أسلوب التدريب عن بعد لتفادى مساوى التدريب ولتوفير الوقت والجهد والمال والإستعانة بالخبرات من كافة دول العالم عن طريق تبادل البحث العلمى.

ثالثا تحسين التعاون الشرطى الدولى

يمثل التعاون الشرطى الدولى بين أجهزة الشرطة الجنائية فى الدول إحدى الوسائل الهامة التى يمكن من خلالها منع الجرائم المعلوماتية أو الإقلال منها وتؤكد التحقيقات فى الجرائم – عامة – والمعلوماتية بصفة خاصة على أهمية التعاون الشرطى الدولى، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الأمن فى هذه الدولة أو غيرها لا يمكنه تعقب المجرمين أو ملاحقتهم إلا فى حدود الدولة التابع لها، فملاحقة مرتكبى هذه الجرائم وتقديمهم للعدالة لتوقيع العقاب يستلزم إجراء التحريات خارج حدود الدولة حيث إرتكبت الجريمة أو جزء منها، ومن هذه الإجراءات معاينة مواقع الإنترنت فى الخارج أو ضبط الأقراص الصلبة، أو تفتيش نظم الحاسب الآلي.. ... إلخ [94].

و دور الإنتربول الدولى" منظمة الشرطة الجنائية الدولية " البارز فى تحقيق التعاون الشرطى الدولى [95].

إلا أنه ينبغى تحسين التعاون الشرطى الدولى فى مواجهة الجريمة المعلوماتية بصفة خاصة وذلك عن طريق عقد المزيد من المعاهدات والإتفاقيات الدولية الخاصة بالجريمة المعلوماتية وبيان كل ما يتعلق بالتعاون الشرطى الدولى من لحظة إرتكاب الجريمة حتى ضبط المتهم فيها أو محاكمته أو تسليمه والسماح لأجهزة الشرطة فى كل دولة من الدولتين إذا كانت هناك إتفاقيات ثنائية أو بين الدول إذا كانت معاهدة جماعية بالإتصال المباشر بينها على مدار 24 ساعة طوال أيام الأسبوع وذلك لملاحقة المجرمين وضبطهم دون اللجوء إلى الطرق الدبلوماسية المعقدة التى تتطلب مزيد من الوقت مما يسمح للمجرمين بالهرب ويمكن أن يتم ذلك عن طريق شبكة معلومات دولية بين أجهزة الشرطة للدول مما يفتح المجال لها بالإتصال المباشر وتحقيق التعاون الشرطى الدولى والتضييق على المجرمين وضبطهم ومحاكمتهم أو تسليمهم " وهذا ما قام به الانتربول الدولى ".

وكذلك عقد المؤتمرات والنقاشات والندوات وورش العمل لرجال الشرطة على المستوى الدولى بين الدول وذلك لتقريب الأفكار بينهم والوصول إلى أعلى مستوى من

---

(94) د/ فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية رسالة دكتوراة، حقوق عين شمس، عام 2012م، ص 514 .

(95) أنظر ؛ الباب الثانى، الفصل الأول، المبحث الأول، المطلب الاول، جهود المنظمات الدولية ويحيل الباحث إليه منعاً للتكرار .

التنسيق والإتصال بينهم فى تعقب المجرمين وضبطهم ويمكن أن يتم ذلك عن طريق شـــبكة المعلومات الدولية دون الحضور الشخصى لهم على مستوى العالم وذلك وفقاً لبروتوكـــولات تعاون بين الدول.

وإنشاء جهاز أو قسم فى وزارة الداخلية فى كل بلد يكون مخـــتص دون غيـــره فـــى التعامل مع الجرائم المعلوماتية وتلقى الشكاوى والبلاغات وإجراء المعاينات وضبط المتهمين وتسليمهم بالإضافة لذلك تحقيق التعاون الدولى فى تبادل المعلومـــات وأفضـــل الممارســـات الشرطية فى مكافحة الجرائم المعلوماتية دون اللجوء إلى الطرق الدبلوماسية المعقدة وتحقيـــق التعاون مع الانتربول الدولى.

كل ذلك سيساعد فى الحد من الإجرام المعلوماتى تدريجياً وعدم تحقيق آثاره المدمرة التى تنال أكثر من دولة.

ومن أمثلة ذلك فى جمهورية مصر العربية نجد الجهاز المختص بتلقـــى البلاغـــات والشكاوى عن الجرائم المعلوماتية والانترنت.

الخاتمـــة:

تناول الباحث السياسة الجنائية المقترحة لمواجهة الجرائم المعلوماتية داخلياً ودولياً وتناول على المستوى الداخلى فى المطلب الأول مبيناً الأليات الجنائية الواجب إتخاذها على المستوى التشريعى من تدابير موضوعية وإجرائية أى التجريم والعقاب وضبط مرتكبيها وتناول إستخدام التكنولوجيا الأمنية فى المكافحة أى إتباع أسلوب الوقاية من الجرائم يسن التشريعات وإستخدام التقنية فى الحد منها فى العمل الأمنى والتدابير والتكنولوجية الأمنية.

وعلى المستوى الدولى تناوله فى المطلب الثانى من الناحية التشريعية ضرورة عقد والإنضمام للإتفاقيات والمعاهدات الدولية التى تخص تجريم الأعمال التى تشكل جرائم معلوماتيه وكذلك الخاصة بالتعاون الدولى فى مواجهتها ومن الناحية الإجرائية تعزيز التعاون الدولى فى مواجهة الجرائم المعلوماتية وذلك للقضاء على إشكاليات التعاون القضائى الدولى من إشكاليات الأنابة القضائيه وتنازع الأختصاص القضائى الدولى وإشكاليات تسليم المجرمين.

وتدعيم التعاون الدولى فى مجال تدريب رجال العدالة، وتحسين التعاون الشرطى الدولى.

كل ذلك سيساعد فى الحد من الإجرام المعلوماتى تدريجياً وعدم تحقيق آثاره المدمرة التى تنال أكثر من دولة نظراً لعالمية هذه الجرائم فهى من الجرائم عابرة الحدود فيجب مواجهتها ليس على المستوى الوطنى فقط إنما بناء سياسة جنائية موحدة على المستويين الداخلى والدولى من الناحية التشريعية، القضائية، التنفيذية.

المراجـــع

أولاً: المراجـــع العامـــة:

- أحمد عبد الكريم سلامة، المبسوط فى شرح قانون الجنسية، الطبعة الأولى، دار النهضة العربية، عام1993.
- أحمد فتحى سرور، الوسيط فى قانون العقوبات، القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، عام 1996م.
- أحمد محمد السيد عبدالله، التعاون الدولى فى الإجراءات الجنائية، دراسة مقارنة بالنظام الإسلامى، رسالة دكتوراة حقوق، المنصورة، عام 2009.
- حماد عوض عباس، التحريات كإجراء من إجراءات البحث عن الحقيقة، دار النهضة العربية، القاهرة، عام 2007/1428.
- عادل يحيى، التحقيق والمحاكم الجنائية عن بعد، دارسة تحليلية تأصيليةلتحقيق الفيديو Video فى المجال الجنائى، دار النهضة العربية، القاهرة، الطبعة الأولى، عام 2006م.
- عبدالرحمن توفيق أحمد درويش: فى علم الإجرام نشأة علم الإجرام وعوامل الإجرام الداخلية والخارجية مقروناً بإحصاءات جنائية، دار وائل للنشر، ط1، الأردن، عام 2006.
- عبدالرحمن توفيق، التدريب، الأصول والمبادئ، موسوعة التدريب والتنمية، الإصدار الأول، مركز الخبرات المهنية للإدارة، القاهرة، بدون سنة نشر.
- عمر السعيد رمضان، شرح قانون العقوبات، القسم العام، ط 1994.
- عمر سالم، الإنابة القضائية الدولية فى المسائل الجنائية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، عام 2001.
- قدرى عبدالفتاح الشهاوى، مناط التحريات، " الإستدلالات الاستخبارات، دار المعارف، الإسكندرية، عام 1998م.
- مأمون سلامة، قانون العقوبات القسم العام، مطبعة جامعة القاهرة والكتاب الجامعى، عام 1991م.

- محمد السيد عرفة، تدريب رجال العداله وأثره فى تحقيق العدالة، جامعة نايف، الرياض، عام 2005م.
- محمد سامى عبد الحميد، أصول القانون الدولى العام، الطبعة الخامسة، دار الجامعة، الإسكندرية، عام 1996م.
- محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، دار النهضة العربي، عام 2002م.
- المدخل إلى البحث فى العلوم السلوكية، صالح العساف، مكتبة العبيكان، عام 1995، السعودية.

{1} **المراجـــع الخاصـــة**:

1. أحمد حسام طه تمام، الجرائم الناشئة عند إستخدام الحاسب الآلى، دار النهضة العربية، الطبعة الأولى، بدون سنة نشر.
2. أحمد فتحى سرور، أصول السياسة الجنائية، دار النهضة العربية، عام 1972.
3. خالد ممدوح إبراهيم، القاضى الإلكترونى، الدعوى الإلكترونية وإجراءاتها إمام المحاكم، دار الفكر الجامعى عام 2008م، بحث منشور على شبكة الإنترنت.
4. خضر مصباح، اساسيات أمن المعلومات والحاسوب، ط1، عمان، دار الجامعة للنشر، عام 2010م.
5. د/ محمد قطب الظواهر الإجرامية المستحدثة وطرق مواجهتها، دراسة مقارنة فى القانون الوضعى والشريعة الإسلامية، بحث غير منشور والأكاديمية الملكية للشرطة، البحرين عام 2010.
6. سعيد عبد اللطيف حسين: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، " الجرائم الواقعة فى مجال تكنولوجيا المعلومات"، الطبعة الأولى، دار النهضة العربية، عام 1999م.
7. شريف فتحى الشافعى، تخطيط وتصميم وتركيب شبكات الحاسب الآلى، القاهرة، دار الكتب العلمية للنشر والتوزيع، عام 2002م.
8. عبد الرحمن عبدالعزيز الشنقيطى: أمن المعلومات وجرائم الحاسب الآلى، ط1، الرياض.

9. على جبار الحسيناوى، جرائم الحاسوب والإنترنت، دار البازورى للنشر والتوزيع، الأردن، عام 2009م.
10. على محمد دهب، التشفير وأمن المعلومات، دولة السودان، كلية دراسات الحاسوب والإحصائى، بدون ناشر، بدون سنة نشر.
11. عمر محمد أبو بكر يونس، الإجراءات الجنائيه عبر الإنترنت فى القانون الأمريكي، المرشد الفيدرالى الأمريكى لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكترونى فى التحقيقات الجنائية، مترجم، بدون ناشر، عام 2006م.
12. القاضى حازم محمد الشرعة، التقاضى الإلكترونى والمحاكم الإلكترونية، ط1، دار الثقافة والنشر والتوزيع، عمان، عام 2010م.
13. لواء دكتور أشرف السعيد أحمد، تكنولوجيا المعلومات فى المجال الأمنى، القاهرة، عام 2013م.
14. محمد فتحى أنور، تفتيش شبكة الإنترنت لضبط جرائم الإعتداء على الآداب العامة والشرف والإعتبار التى تقع بواسطتها.
15. مدحت محمد رمضان، جرائم الإعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، عام 2000م.
16. مواد د/ أشرف السعيد أحمد، القرصنة الإلكترونية، القاهرة، عام 2011م.
17. نضال أدلبى، بحث بعنوان تطوير وتنسيق التشريعات السيبرانية فى المنطقة العربية ومواجهة الجرائم السيبرانية، الأمم المتحدة، الأسكو، نقل بتصرف.
18. هلالى عبداللاه أحمد، إتفاقية بودابست، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء إتفاقية بودابست الموقعة فى 2001/11/23، دار النهضة العربية، الطبعة الأولى، عام 2006م.
19. وليد الزيدى، الفرضة على الإنترنت والحاسوب، التشريعات القانونية، الطبعة الأولى، دار أسامة، عمان، الأردن، عام 2003.

{2} رسائـــل الماجستيـــر والدكتـــوراه:

1. أمين عبدالرحمن محمود، الأنابة القضائية، رسالة دكتوراة، حقوق الإسكندرية، عام

2011م.

2. حسين بن سعيد الغامزى، السياسة الجنائية فى مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، عام 2009م، رسالة دكتوراة، جامعة عين شمس.
3. سالم مرزوق المطرفى، نموذج مقترح لإنشاء مركز تدريب عن بعد بالمديرية العامة للدفاع المدنى بالمملكة العربية السعودية، رسالة ماجستير، جامعة نايف، الرياض، السعودية، عام 2005م.
4. فهد عيد الله العبيد، الإجراءات الجنائية المعلوماتية، رسالة دكتوراة، حقوق، عين شمس، عام 2012.

{3} **الجرائـــد والمجـــلات**:

1. إنشراح محمد الدسوقى، بحث ميدانى عن التحصيل الدراسى وعلاقته بكل من مفهوم الذات والتوافق النفسى، دراسة مقارنة، نشر بمجلة علم النفس، الهيئة المصرية العامة للكتاب، عام 20 أكتوبر 1991م.
2. جريدة الجمهورية، مقال بعنوان مكافحة الإرهاب، مكتب التحقيقات الفيدرالى يتجسس على الأمريكيين.
3. حلمى سالم، نحو تأهيل خصائص التدريب الأمنى وركائزه، مجلة بحوث الشرطة، العدد 18، عام 2000.
4. عبد الغنى عبد الحميد محمود، تسليم المجرمين على أساس المعاملة بالمثل، مجلة كلية الشريعة والقانون، القاهرة، العدد16، عام 1998/1997.

{4} **المؤتمـــرات والنـــدوات**:

1. حسام الدين الصغير، قضايا عالميه جديدة فى مجال الملكية الفكرية، ورقة عمل مقدمة فى الإجتماع المشترك بين المنظمة العالمية للملكية الفكرية "الويبو"، وجامعة الدول العربية، حول الملكية الفكرية لمملكتى الصحافة والإعلام، القاهرة، 23-24 مايو 2005م.
2. عمرو زكى عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة لمؤتمر الجوانب القانونية للتجارة القانونية، مقر جامعة الدول العربية، يناير عام 2001م.
3. محمد محمود درويش، التدريب الأمنى، ورقة عمل قدمت للحلقة العلمية حول تطوير التدريب الأمنى المنعقده بجامعة نايف خلال الفترة 10-2003/5/14، الرياض، السعودية.
4. يوسف شمس الدين شاسبوغ، التحريات الشبكيه ورقة عمل مقدمة إلى مؤتمر الأمن والتكنولوجيا عام 2006، مركز بحوث شرطة الشارقة.

{5} **المواقـــع**:

- http:conventions.coe-int/treaty/fr/reports/html/10300/htm
- https://arij.net/news
- https://hardoegypt.org
- https://www.soutalomma.com/Arcle1870700
- https:www.ita.gov.com/itAportal.Ar/mediacenter/Document.detail.aspx?NId=64
- https://www.parliament.gov.sy/arabic/lidex.php?node=2012nid=4337&ref=tree
- https://www.acees.gov.bh/cyber-crime/anti-cyber-crimw-law-in-The-kingdom-ofbahrain
- https://www.e.gov.kw/sites/kgoenglish/froms/AcitlowNo.63of2015oncombanglnformationtechnologycrimes
- https://mdct.gov.jo/uploads/policies-and-strategiess

Directorate/legistation/lows/Electron-ic-crime-low-pdf

- http://www.moheet.com
- www.arabips.com/foroms/index.php
- https://m.youm7.com
- https://www.bayut.com/mybuyut/ar
- https://www.mohamah.net.law
- https://academy.hosoub.com
- www.academy.shoun.com
- www.techapedia.com
- www.computererhopp.com
- www.serchsecurity.techtarget.com
- www.lifewire.com
- www.digital.ohram.org
- www.laweg.net/default.aspxacon=viewACvepages&itemid=21002&type=6

- د/ محمد الفحطانى، خالد الخثبر، أمن المعلومات بلغة ميسرة، الرياض، مركز البحوث، معهد الإدارة العامة، عام 2000.