العنوان : آليات تفعيل الحماية الأمنية للتوقيع الإلكتروني .

الناشر : مجلة روح القوانين – كلية الحقوق – جامعة طنطا .

المؤلف : محمود سيد أحمد عبد القادر عامر .

المجلد : الثانى .

العدد : الثامن والثمانون .

محكمة : نعم .

التاريخ الميلادى : ٢٠١٩ .

الشهر : أكتوبر .

الصفحات : ٢ – ٤١ .

مواضيع : الحماية المدينة – التوقيع الإلكترونى .

تمهيـــــد

أن التحول الحضاري والتقدم الذي اجتاح العالم في العصر الحديث أحدث تغيراً ملموسا في نوعية الجرائم فبعد أن كانت الغلبة للجرائم القائمة على العنف أو القسوة أصبحت الغلبة للجرائم القائمة على المقدرة الذهنية والذكاء.

تعتبر تقنية المعلومات إحدى نتائج هذا التحول الحضاري والتقدم الذي اجتاح العالم في العصر الحديث فهي عالم ضخم ومتنوع عالم دخلت تقنية المعلومات جميع نواحيه بل وساهم في إنتاج وتطوير العديد من السلوكيات الإجرامية ذات الإثر البالغ على حياة الأفراد والمجتمع.

يعتبر موضوع البحث (**آليات الحماية الأمنية للتوقيع الإلكتروني**) من الموضوعات المهمة التي تثير جوانب جديده ترجع إلى اتصالها بتطور وسائل التعاملات بسبب انتشار استخدام الكمبيوتر وخاصة استعمال شبكة الإنترنت فالتعاملات بطريق الوسائل الإلكترونية أصبحت تشكل قمة التطور في التبادلات بين الأفراد والشركات والجهات المختلفة.

يمكن تعريف جرائم التوقيع الإلكتروني بأنها نشاط إجرامي يتم عبر استخدام الحاسب الألى وذلك خلال الاعتداء على المعلومات محفوظة في أجهزة الحاسب الألى عن طريق الدخول غير القانوني أما مباشراً لهذه الحواسيب أو من خلال التسلل غير المشروع عن طريق الشبكة العنكبوتية لشبكات داخلية أو مؤسسات مالية أو جهات حكومية ما يعرف بجريمة الاعتداء عن الشبكات.

مما لا شك فيه أن هذا الموضوع أصبح على جانب من الأهمية وذلك نظرً لشيوع استخدام أجهزة الحاسب الألى سواء على مستوى الأفراد أو الشركات او الجهات الحكومية وهو ما يعرف الحكومة الإلكترونية ولهذا ظهرت الحاجة الى إجراءات قانونية لتوثيق التعاملات القانونية عبر الإنترنت فعرف التوقيع الإلكتروني كبديل للتوقيع التقليدي عبر شبكة الإنترنت وأصبحت الحاجة ملحة للتدخل التشريعي لهذا الظاهرة المستحدثة.

في هذا البحث سوف نقوم بتحاليل ظاهرة التوقيع الإلكتروني من حيث ماهية التوقيع الإلكتروني وبيان المصلحة محل الحماية الأمنية وصور التجريم في مصر والحماية الأمنية للتوقيع الإلكتروني داعين المولى عز وجل أن يوفقنا في ذلك.

أهميــة البحث

يحتل موضوع الحماية الجنائية للتوقيع الإلكتروني موقعا هاماً في الدراسات القانونية الجنائية الحديثة فهو من موضوعات الحاضر والمستقبل وهذه الأهمية تتبلور أمامنا سواء من الناحية النظرية أو التطبيقية.

فمن الناحية النظرية يثير مفهوم الحماية الجنائية للتوقيع الإلكتروني والجرائم التي تمثل اعتداء علية وما يثيره من مشاكل قانونية جنائية متعلقة بفكرة العقود الإلكترونية والتجارة الإلكترونية للتحايل الذي يظهر من جانب العميل او التاجر او الغير وصور الاعتداء المتمثلة في الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع أو التزوير.

ومن ناحية العلمية التطبيقية يثير مشاكل اختراق نظم المعلومات وعدم الأمان في استخدام شبكة الإنترنت في المعاملات وممارسة قطاع البنوك لهذه النمطية من المعاملات الإلكترونية وأساليب الحماية الإلكترونية.

ومما يؤكد أهمية الموضوع ذلك القدر من التداخل بين التوقيع الإلكتروني والتجارة الإلكترونية فإذا كان قوام هذه التجارة هي تبادل السلع والخدمات فإن هذا التبادل لا يعدو أن يكون في حقيقة الأمر معقدا يستجمع كافة شروطه القانونية من إيجاب قبول ويقترن بتوقيع ينسب إلى صاحبه ويرتب أثارة القانونية.

ومن ثم فأن الاعتداء على التوقيع الإلكتروني من شأنه المساس بالثقة والأمان في المعاملات التي تكون التجارة الإلكترونية محلا لها.

وللتوقيع الإلكتروني صلة وثيقة بالحق في الإعلام ذلك أنه إذا كان هذا الحق الأخير يعنى أن للفرد الحق في أن يتلقى ويطلع وينتقل المعلومات فأن هذه المعلومات قد يتضمنها المستند الإلكتروني.

غير أن مدلول المستند الإلكتروني لا يتطابق دائما من دائرة المعلومات فقد تصاغ المعلومات في شكل مستند الإلكتروني او غيره من الصور ويعنى ذلك أن للمعلومات نطاقا أوسع من نطاق المستند الإلكتروني.

ومن ناحية أخرى فان الصلة الوثيقة بين التوقيع الإلكتروني والحكومة الإلكترونية تدفع الى القول بأن الحماية المقررة لأحدهما تنطوي بطريق اللزوم على حماية الأخر.

أهداف البحث

١- التعمق في موضوع جريمة الاعتداء على التوقيع الإلكتروني كمسألة قانونية حديثة بدراسة وافيه قدر الإمكان والمشاركة في إيجاد الملامح العامة لتشكيل الإطار القانوني الذي يعرف هذه الجرائم ويحكمها.
٢- العمل على إحاطة الناس وتوعيتهم بهذا النوع من الجرائم والذي ارتبط ارتباطا وثيقا بكثير من معاملاتهم اليومية التي تعتمد على الحاسب الألى في ظل هيمنة ثورة تقنية المعلومات وخطورة التعامل معها دون ضوابط وأحكام تعرفها وتحديدها بدقة.

صعوبات البحث

لقد اصطدمت بكثير من الصعوبات والعقبات عند إعدادي لهذا البحث:

اولا: حداثة الموضوع مما ترتب عليه محدودية المراجع المتخصصة باللغة العربية وندرة السوابق القضائية التي يمكن الرجوع إليها والاستدلال بها.

ثانيا: بحث الحماية الأمنية للتوقيع الإلكتروني يستلزم الوقوف على الطبيعة التقنية للتوقيع الإلكتروني وألية استخدامه وهو ما يتسم بالدقة ويستلزم قدراً من التخصص.

ثالثا: أن الحماية الأمنية للتوقيع الإلكتروني يجب إن توكبها حماية تقنية تحد من مخاطر الاعتداء وهو ما استلزم الوقوف على مدلول الحماية التقنية للتوقيع الإلكتروني ولا شك إن تناول تلك الجوانب التقنية يتسم بالدقة والصعوبة.

رابعا: قلة الإلمام بتقنيات الحاسب الألى المتطورة وكيفية استخدامها ومصطلحاتها.

خامسا: في الغالب الجرائم المعلوماتية تحدث في الخفاء مما يصعب اكتشافها وملاحقة أصحابها وبالتالي عدم الإحاطة بملابسات هذه الجرائم وإمكانية تكييفها وتصنيفها.

منهج البحث

اتبعنا في دراسة هذا الموضوع منهجاً تأصيليا مقارنا مبنى على التتابع والتسلسل المنطقي للبحث العلمي.

فهو اولاً منهج تأصيلي يرد النقاط التفصيلية الى أصولها النظرية فعندما نعالج جريمة من الجرائم التي تقع على التوقيع الإلكتروني نردها الى الأماكن العامة في التجريم وعندما نحلل نشرح كل جريمة وذلك بعرضها على القواعد العامة في القانون الجنائي والتعليق عليها ثم عرض المسالة ذاتها على القوانين والتشريعات الوطنية والدولية ثم إلقاء نظرة على أراء الفقه وانتهى الى المقارنة بين ذلك مع بيان رأيي عند الاقتضاء.

وينقسم البحث الى ثلاث مطالب:

المطلب الأول: تسليم المجرمين.

المطلب الثاني: التدريب واهميته في مجال مكافحة جرائم التوقيع الإلكتروني.

المطلب الثالث: طرق الوقاية من الاعتداءات على التوقيع الإلكتروني.

المطلب الأول

تسليم المجرمين

تمهيد:

تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها او تطبيق مبدأ المعاملة بالمثل بتبادل المعلومات بما أن يكفل تفادى ارتكاب جرائم تقنية المعلومات والمساعدة على التحقيق فيها وتتبع مرتكبيها وبالتالي يعد التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات وتسليم المجرمين من أهم سبل توحيد الصف لتفعيل الحماية الأمنية للتوقيع الإلكتروني [١] فتسليم المجرمين يقتضى منا بداية ماهيته في مطلب أول ثم معرفه شروطه وإجراءاته في مطلب ثاني.

ماهية نظام تسليم المجرمين

لقد افتقرت الأحكام والمعاهدات الدولية الإجراءات الواجب إتباعها بشأن تسليم المجرمين الفارين من العدالة الى الدولة الراغبة في محاكمة أو تنفيذ الأحكام الصادرة ضده أو تنفيذ حكم صادر عليه [٢] ولقد افتقرت الدول الى وجود معاهدة دولية ملزمة تلزم جميع أطرافها بضرورة تسليم المجرمين المحكوم عليهم بأحكام جنائية (مبدأ المعاملة بالمثل) ويظهر ذلك جليا في جرائم دولية معينة [٣].

وفى فتره ما بعد الحرب العالمية الثانية كانت الزيادة في عدد المعاهدات والاتفاقيات خاصة الثنائية منها لتنظيم إجراءات تسليم المجرمين خاصة عند دول القانون العام حيث تم استخدامها على نطاق واسع بالإضافة الى ما سبق ظهرت العديد من الاتفاقيات متعددة إلا طراف بشأن تسليم المجرمين فهناك اتفاقية.

البلدان الأمريكية [٤] لتسليم المجرمين ١٩٨١ في إطار منظمه الدول الأمريكية وكذلك اتفاقية جامعة الدول العربية لتسليم المجرمين ١٩٥٢ وهناك الاتفاقية الأوربية المتعلقة

---

[١] قانون رقم ١٧٥ لسنه ٢٠١٨ في شان مكافحة جرائم تقنية المعلومات.

[٢] M. Cherif bassoon international extradition – us law and practice .new York Oceana Publications I.N.C. third edition ١٩٩٦.p٣٢

[٣] M . Cherif bassoon the need for international accountability international criminal law vole fff٣ .١٩٩٩.p٣

[٤] الأمم المتحدة – مجموعه المعاهدات – المجلد ١٧٥٢ الرقم ٣٠٥٩٧.

بتسليم المجرمين ١٩٥٧ م وبروتوكولاتها الإضافة ١٩٧٥-١٩٧٨ وكذلك اتفاقيه المنظمة المشتركة لإفريقيا ومدغشقر ١٩٦١ ومعاهده تسليم المجرمين والمساعدات المتبادلة في المسائل الجنائية ١٩٦١ وخطة الكومنولث لتسليم المجرمين ١٩٦٦ م وهناك أيضا اتفاقية الرياض العربية للتعاون القضائي ١٩٨٣ م والاتفاقية الأمنية الخليجية ١٩٩٤م واتفاقية الجماعة الاقتصادية لدول غرب أفريقيا بشأن تسليم المجرمين ١٩٩٤م وهناك اتفاقيه تبسيط إجراءات تسليم المجرمين بين الدول الأعضاء في الاتحاد الأوربي واتفاقيه الأمم المتحدة لمكافحه الجريمة المنظمة عبر الوطنية ٢٠٠٠ [١].

تعريف تسليم المجرمين: يعنى قيام دوله ما (الدولة المطلوب منها التسليم) بتسليم شخص موجود في إقليمها إلى دوله أخرى (الدولة طالبه التسليم) بناء على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها او لتنفيذ حكم صادر ضده من محاكمها [٢]. بمعنى أخر تسليم دوله لدوله أخرى شخصياً منسوبا إليه اقتراف جريمة ما أو صدر ضده حكما بالعقاب كي تتولى محاكمته أو تنفيذ العقاب عليه.

وأخيراً يتضح لنا مما سبق أنه من الضروري لتطبيق فكرة التسليم ينبغي لنا وجود علاقة بين الدولتين **أولا:** أن تقوم الدولة الطالبة لتسليم بتقديم طلب للدولة الأخرى لتتخذ الإجراءات اللازمة لتنفيذ العقوبة. **ثانياً:** الاستجابة من الدولة الأخرى بعد توجيه طلب التسليم لتقرر بعد ذلك اما الموافقة عندما يكون هناك اتفاق و معاهدة تربط بين تلك الدول بضرورة التسليم او الرفض بعدم وجود اتفاقية او معاهدة تلزم الدولتين بالتسليم ومن جهة أخرى نجده يشمل طائفتين من الأشخاص: طائفة الأشخاص المتهمين الذين تسند إليهم ارتكاب جرائم إلا انه لم يصدر بحقهم أحكام بعد الفرض هنا أن شخصا ما اقترف جريمة ما في دولة معينه وقبل أن تلقى القبض عليه يفر هارباً الى دولة أخرى عندها تطلب الدولة المرتكب على إقليمها الفعل جريمة ما قد لوحق جنائيا من قبل قضاء الدولة التي أرتكب فيها الفعل الإجرامي وصدر بحقه حكماً قضائيا إلا إنه وقبل البدء في التنفيذ يفر هاربا إلى دوله أخرى فتطلب الدولة التي ارتكبت فيها الجريمة استلامه من الدولة التي فلا إليها والتسليم بمعناه السابق يختلف عن مفاهيم أخرى قد

---

[١] قرار الجمعية العامة للأمم المتحدة وثيقة ٢٥/so/ A /Res. بتاريخ ٢٠٠٠/١/٨م.
[٢] د/جميلا عبد الباقي الصغير الجوانب الإجرائية المرجعة السابقة ص٨٨

تختلف به فهو لا يعد من قبيل الإبعاد الذى يعد عملا إداريا تستقل باتخاذه الجهة الإدارية في حالات متعددة [١].

الإجرامي من الدولة التي فر المتهم هاربا إليها أن تسلمه لها لمحاكمته عما أرتكب من جرم وطائفه الأشخاص المحكوم عليهم الذين صدر بحقهم حكم بالإدانة إلا انه لم ينفذ بعد نتيجة لفرارهم إلى دوله أخرى والفرض هنا أن الشخص المتهم بارتكابها

ولا يعتبر كذلك من قبيل الطرد التي تمارس الدولة بما لها من سيادة على إقليمها متى ما رأت أن بقاء الشخص على إقليمها من شأن ان يؤثر على وجودها او أمنها [٢].

مقارنه التسليم بالإبعاد : تسليم المجرمين Extradition هذا التسليم عباره عن قيام الدولة بالتخلي عن الشخص المتهم بجريمة معينة (المراد تسليمة) أو محكوم علية جنائيا ومن حق الدولة طالبة التسليم من محاكمته وتوقيع العقاب عليه وهو يخالف الطرد او الإبعاد Expulsion وهو عمل إداري لا تنظر فيه الدولة لصالح دولة أخرى بل لا تراعى فيه الأمن القومي للدولة (الصالح الخاص) فتقوم الدولة بطرد الأجنبي التي تجد في وجوده خطرا على الأمن في إقليمها او أن بقاءه في ارضها يدعو الى عدم الطمأنينة فتقوم بأبعاده خارج البلاد دون تسليمة الى دولة أخرى حتى وان لم يكن مطلوب في جريمة أو محكوم عليه وإنما تقوم بطرده لأن من مصلحة الدولة عدم وجوده في إقليمها[٣].

---

[١] لواء – سراج الدين محمد الروبي – الإنتربول وملاحقه المجرمين مرجع سابق ص ٤٠
[٢] د/جميلا عبد الباقي الصغير – الجوانب الإجرائية المرجعة السابقة ص ٨٨
[٣] د/ محمد مصباح القاضي – التدابير الاحترازية في السياسة الجنابية الوضعية والشرعية – دار النهضة العربية ٢٠٠٨ ص ٤٥

الفرع الأول

أنواع نظم تسليم المجرمين

١ـ التسليم القضائي : تعتبر السلطة القضائية هي الجهة الوحيدة المختصة بإصدار قرار التسليم ولا شأن لجهة الإدارة بهذا الخصوص و يقوم هذا النظام على أساس احترام حقوق الأفراد وصيانه حرياتهم والدولة التي تأخذ بهذا الاتجاه تنتهج في التنفيذ أحد النهجين **: الأول** أن تكون المحكمة هي الجهة الوحيدة المختصة بإصدار قرار التسليم للدولة طالبة التسليم ولا دخل للنيابة العامة في إصدار هذا القرار وإنما يقتصر عملها أو دورها على تلقى طلب التسليم من الجهة المختصة وتعد أوراق الموضوع للعرض على المحكمة المختصة لتتولى الأخيرة عملية إصدار القرار النهائي حول هذا الطلب [١] .

تقوم الدولة المطلوب منها التسليم بإعطاء النائب العام إصدار القرار النهائي بالموافقة أو الرفض وإن ذلك النظام يسمح لشخص المطلوب تسليمة بالدفاع الكامل عن نفسه وتقديم كافة الأوراق والمستندات وله كافة الحرية باستخدام أوجه دفاعه إلا أنه يوجد بعض السلبيات التي تتطلب التوازن بين الخبرة القانونية الدولية والأبعاد السياسية بالإضافة الى ذلك طول الفترة التي تستغرقها إجراءات المحاكمة قد تدفع المحكمة الى الإفراج المؤقت عن الشخص المطلوب تسليمة لحين استكمال واستيفاء باقي الإجراءات الأمر الذى يفاجئ الدولة بهروب المتهم الى دولة أخرى .

٢ـ **التسليم الإداري**: تعتبر السلطة التنفيذية هي صاحبة اليد العليا وهي التي تمتلك الصالحية المطلقة في تقرير تسليم المجرم من عدمه فيعتبر تسليم المجرمين في هذا النظام دليل على أعمال السيادة التي يقوم أجهزة الإنتربول بالدولة طالبة التسليم بشأن المتهم المطلوب بمخاطبة الإنتربول في الدولة الأخرى وفقا لاعتبارات سياسية وأمنية ودولية.

ولذلك فيكون للتسليم الإداري سلبيات وإيجابيات ومن إيجابيات سرعه التسليم فهو يتم في حين تأكد أجهزة الشرطة المختصة بتجريم الفعل في تلك الدولتين بالإضافة الى التأكد من وجود اتفاقية ثنائية بين الدولتين فيجب أن ينص فيها صراحه على جواز التسليم وأن الفعل المجرم المطلوب التسليم لأجله من الجرائم المنصوص على جواز التسليم فيها في حاله الاتفاقية المقيدة بنوعية معينه من الجرائم وهذا بالطبع يتم بعد التأكد من وجود الشخص المطلوب تسليمة على أرض الدولة المطلوب منها التسليم وعدم مغادرته البلاد وأنه لا توجد أي موانع قد تعوق عملية التسليم وإتمامه [٢].

بالإضافة الى أن هذا النظام يتميز بالابتعاد عن التعقيد والروتين والسير في الإجراءات الطويلة التي تحمل الدولة النفقات الباهظة كما إنه يساعد على تحسين العلاقات الدولية

---

[١] د/هشام محمد فريد رستم الجرائم المعلوماتية اصول التحقيق الجنائي الفني مجله الأمن والقانون دبى كليه الشرطة العدد (٢) ١٩٩٩ – ص ٤٤٥

[٢] د/ جميل عبد القوى الصغير – الجوانب الإجرائية المرجع السابق ص ٩١

بين دول الأطراف وبالرغم من توافر العديم من الإيجابيات في هذا النظام الى إنه هناك بعض السلبيات التي تنسب له كعدم الوضع في الاعتبار حقوق الإفراد الدفاعية المجاملات الدولية التي تقوم بها الدول لصالح الدولة طالبة التسليم ويكون في هذه الإجراءات أضرار بالمتهم كأن يكون الشخص غير مطلوب جنائيا وإنما قد أتهم بهتانا على غير حقيقه بارتكاب عمل ما بقصد تسليم الدولة له بحيث عندما يعاد إلى دولته طالبة التسليم تتخذ ضده إجراءات عقابيه مختلفة كلياً وعن وقائع لا علاقه لها مطلقاً بالموضوع الذى ذكر أن ارتكبه ايضاً من السلبيات أن التسليم الإداري غالباً ما يتم عن طريق السلطة التنفيذية التي ربما قد لا تتوافر لها ملكه الفحص القانوني لعدم توافر الثقافة القانونية المؤهلة للصلاحية لاستصدار مثل هذا القرار ناهيك عن أي هذا النوع من التسليم يتم في إطار من التعتيم والكتمان مما يعنى بعده عن الأجهزة الرقابية القضائية والتشريعية.

٣ـ **التسليم المختلط**: يعتبر هذا النوع من التسليم من أفضل أنواع التسليم وذلك لأنه تقوم في السلطة القضائية بالحق في فحص طلب التسليم وتعطى الفرصة إلى الشخص المطلوب كافة الضمانات للدفاع عن نفسه مع وقوف الدولة على الحياد دون التأثير في فحص وقائع الدعوة فيما لا يخل بحق الدولة في طلب التسليم والرد على الفحص بالمستندات والوثائق وبالتالي يعد الأكثر انتشارا حيث يوازى بين مصلحة الدولتين المتعارضتين للتسليم.

الفرع الثاني

شروط وإجراءات تسليم المجرمين

هناك شروط لتسليم المجرمين لابد من وجودها وإجراءات معينه لا يتم التسليم بدونها وذلك على النحو التالي:

الشروط التسليم:

ينبغي توافر عدة شروط تمكن في كونها تفصل حدود العلاقة بين الدول الأطراف في عمليه التسليم وتضع الأحكام العامة التي على أساسها سيتم التسليم من عدمه وذلك متى توافرت هذه الشروط حال البت في قرار التسليم وتكاد تتفق هذه الشروط في جميع حالات التسليم من حيث العناصر أما من حيث الموضوع فهي محل خلاف بين الدول وذلك بحسب حاجتها للتسليم واعتبارات المصالح الدولية التي تراعيها كل دوله وهي كالتالي [١]:

١ – **التجريم المزدوج** : ينبغي أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولة طالبه التسليم وكذلك في تشريع الدولة المطلوب إليها التسليم حتى وأن اختلف التكيف القانوني في تشريعات الدول والمطلوب هنا أن يكون الفعل مجرماً أيا كانت الصورة التشريعية المعاقب عليها فلا عبرة للوصف او التكيف القانوني الذى يطلب على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه فمثلاً لو كان الفعل معاقبا عليه في تشريع الدولة الطالبة التسليم تحت مسمى جريمة توظيف الأموال بينما كان الفعل نفسه معاقبا عليه تحت مسمى جريمة النصب والاحتيال في الدولة المطلوب منها التسليم فإن ذلك لا يمنع من توافر شروط ثنائيه التجريم وازدواجيته [٢].

فينبغي أن يكون الفعل الذي تبتغى الدولة طالبة التسليم محاكمة الشخص من ارتكاب تلك السلوك إن يكون مجرماً فمن البديهي إن السلوك مجرم في تشريعها حيث إنه إذا لم يكن مجرما فلا يتصور وجود دعوى عموميه او ملاحقه جنائية ضد الشخص المتهم كما لا يتصور قيام حكم جنائي يقضى بعقوبة عليه هذا من ناحية ومن ناحية أخرى لا يجوز مطالبه الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الأساس غير مجرم وفقاً لقانونه.

فهناك العديد من الأمثلة والحالات التي قام الجاني بارتكاب جريمة معينة على إقليم دولة للأضرار بدولة أخرى ومن أشهر الحالات التي وقعت في التسعينيات الهجوم الذي شنه شاب روسي على مصرف سيتي بنك.

---

[١] د/ عبد الفتاح محمد سراج – النظرية العامة لتسليم المجرمين ص ٢٠٩.
[٢] د/هشام فريد محمد رستم الجرائم المعلوماتية مرجع سابق ص ٤٣٩-٤٤٠

فعن طريق استخدام حاسوبه الموجود في روسيا نجح المتهم في إن يخترق دون إذن وحدات خدمه حواسيب المسرب في الولايات المتحدة.

وقام بتجنيد عدد من المواطنين لفتح حسابات مصرفيه في شتى أنحاء العالم ثم أصدر تعليمات الى حاسوب سيتي بنك بتحويل أموال الى تلك الحسابات وعند اكتشاف المخطط وتحديد هوية المتهم صدر بحقه أمر اعتقال من محكمه اتحادية بالولايات المتحدة ولم تكن هناك معاهده لتسليم المجرمين في ذلك الوقت بين روسيا والولايات المتحدة لكن المتهم ارتكب خطأ بزيارته دول بريطانيا لحضور معرض للحواسيب وقد اضطرت السلطات البريطانية الى التعاون في تسليمه لمواجهة التهم الموجهة ضده في الولايات المتحدة فوفقاً لترتيبات تسليم المجرمين النافذة بين المملكة المتحدة والولايات المتحدة يمكن لسلطات المملكة المتحدة تقديم المساعدة ما دامت الجريمة موضع الاتهام لها ما يقابلها في قانونها الداخلي .

وطلب المتهم أن تنظر المحكمة في قانونيه توقيفه للطعن في تسليمه وساق حججاً منها أن أمر تحويل الأموال قد صدر في روسيا حيث توجد لوحه مفاتيح حاسوبه وليس في الولايات المتحدة وارتأت المحكمة أن الوجود المادي للمتهم في سان بطرسبرج هو أقل أهميه من كونه باشر عملياته على أقراص ممغنطة موجوده في الولايات المتحدة وفضلا عن ذلك فأن الأفعال الموجهة إلى المتهم لها مقابلها الواضح في قانون إساءه استعمال الحواسيب لعام ١٩٩٠ ولو مارس عملياته من المملكة المتحدة بدلا من روسيا لكان الاختصاص القضائي للمحاكم الإنجليزية وأخيراً تم تسليم المتهم الى الولايات المتحدة حيث أدين وسجن كذلك نجد العديد من الاتفاقيات والمعاهدة المتعلقة بتسليم المجرمين قد نصت وأكدت على هذا الشرط فهناك مثلا المادة الثانية من المعاهدة النموذجية للأمم المتحدة بشان تسليم المجرمين والمادة الثالثة من اتفاقية جامعه الدول العربية لتسليم المجرمين والمادة ٤٠ من اتفاقيه الرياض العربية للتعاون القضائي والمادة ٢٤ من الاتفاقية الأوربية للإجرام المعلوماتي.

٢ـ الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

عدم جواز تسليم الرعايا: تعتبر من أهم المبادئ والأعراف في المجتمع الدولي بتنفيذ مبدأ عدم جواز تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم [١].

عدم جواز تسليم ممنوحي حق اللجوء السياسي: لقد اكدت المبادئ السائدة في أغلب التشريعات والاتفاقيات الدولية والإقليمية والثنائية المتعلقة بتسليم المجرمين عدم جواز تسليم ممنوحي حق اللجوء السياسي.

عدم جواز تسليم من تمت محاكمتهم عن ذات الجريمة المطلوب تسليمهم لأجلها: فلا ينبغي معاقبة الشخص المطلوب تسليمة عن جريمة قد سبق محاكمته فيها من قبل فلا يجوز معاقبه الشخص مرتين عن جريمة واحده بل انه ايضا لا يجوز التسليم متى ما كان قيد التحقيق والمحاكمة عن ارتكابه فعلا ما هو ذاته المطلوب تسليمه لأجله ويعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمة ويهدف الى توفير أكبر قدر ممكن من الحماية القضائية للشخص المطلوب تسليمة في الدولة الطالبة.

٣ـ الشروط المتعلقة بالجريمة المطلوبة التسليم لأجلها.

الجرائم التي يجوز التسليم فيها وتلك التي لا يجوز التسليم فيها:

إنه لمن الضروري تحديد طبيعة الجريمة من كونها تخضع لنطاق التسليم أو لا تخضع وبالتالي يجوز تسليم المجرم إذا توافر في الجريمة عده شروط في ثلاثة اتجاهات: [٢]

اسلوب الحصر "نهج القائمة ": ينبغي حصر تلك القائمة على جميع الجرائم التي يتم التسليم لأجلها والا يؤدى ذلك الى إفلات بعض المجرمين من العقاب فيعتمد هذا الأسلوب على إدراج مجموعه من الجرائم على سبيل الحصر " قتل نصب سرقه غسل أموال إرهاب ....." في قائمه تضمن القانون أو تلحق بالاتفاقية لتكون هذه الجرائم دون غيرها من الجرائم الأخرى هي التي يتم التسليم لأجلها ويعتبر هذا الأسلوب من أقل الأساليب شيوعا وانتشارا بين الدول [٣].

أسلوب جسامة الجريمة أو الحد الأدنى للعقوبة: يجب على الدول تحديد الجرائم التي يجوز التسليم فيها وبالتالي يجب أن تحدد الدول في تشريعاتها الداخلية ومعاهداتها الثنائية العقوبة المقرر لتلك الجرائم فيعتبر هذا الأسلوب الأكثر شيوعا في تحديد الجرائم التي يجوز التسليم فيها.

النظام المختلط: وهو من الأساليب الشائعة أيضا في التحديد الجرائم التي يجوز التسليم فيها وهو يحقق فائدتين: فمن جهة يضمن درجه معينه من جسامة الجريمة المعاقبة عليها في البلدين ليتم التسليم وفقاً لها ومن وجه أخرى يضمن خضوع جرائم محدده

(١) Gilbert aspects of extradition law London – Kluwer academic ١٩٩١.P٩٥.

٠٢ د/عبد الفتاح محمد سراج – المرجع السابق ص ٣٥٨.

٠٣ د/ جميل عبد الباقي الصغير الجوانب المعلوماتية مرجع سابق ص٨٨.

تمثل خطراً على الدول الأطراف للتسليم دون النظر لدرجه جسامتها او لعقوبة المقررة لها.
ولقد اعتمدت العديد من الاتفاقيات بهذا النظام ولقد أخذت الاتفاقيات الأوروبية للجرائم المعلوماتية بهذا الأسلوب حيث نصت المادة ٢٤ منها على أنه تطبق هذه المادة على عمليه تسليم المجرمين فيما بين الدول الأطراف بالنسبة للجرائم المنصوصة عليها وفقاً للمواد من ٢-١١[١] بهذه الاتفاقية بشرط أن يعاقب عليه قانون بموجب القوانين بالدولتين المعنيتين طرفي الاتفاقية بالحرمان من الحرية لفترة لا تزيد عن سنة واحده على الأقل او بعقوبة أشد.

ومما تجدر الإشارة إليه في هذا المقام أنه يسود المجتمع الدولي اتجاه عام يقضى لعدم جواز التسليم في الجرائم السياسية [٢] وذلك راجع الى إن المجرم السياسي لا يعتبر مجرماً بالمعنى الذى يحمله هذا الاصطلاح في علم الإجرام او علم الاجتماع اذ غالبا ما يرتكبه السلوك بهدف تحقيق أغراض وأهداف قوميه قد تنطوي على أعمال بطوليه لتحرير الأرض واستقلال الوطن والدفاع عن مبادئ ساميه [٣] وهذا الاتجاه نجد تطبيقاً له في المادة الثالثة من معاهده الأمم المتحدة النموذجية بشأن تسليم المجرمين ١٩٩٠ م والمادة الرابعة من اتفاقيه جامعه الدول العربية لتسليم المجرمين ١٩٥٢ م.

عدم انقضاء الدعوى العمومية او العقوبة: يشترط لجواز التسليم أن لا تكون الدعوى العمومية أو الحكم القاضي بفرض عقوبة قد انقضى بأحد أسباب الانقضاء المحددة في التشريعات الوطنية للدولة طالبه التسليم والمطلوب إليها التسليم أو الدولة التي ارتكبت الجريمة على أرضها.

ثانيا: إجراءات التسليم: وهذه الإجراءات تتقاسمها الدولتان الطالبة والمطلوبة كما إنها ليست مطلقة بل مقيده ببعض الالتزامات الدولية ويقصد بمراحل وإجراءات التسليم تلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عمليه التسليم وفقاً لقوانينها الوطنية وتعهداتها لأجل إتمام عمليه التسليم بهدف التوفيق بين المحافظات على حقوق الإنسان وحريته وبين تأمين الصالح العام الناشئ عن ضرورة التعاون الدولي في مكافحه الجريمة بحيث لا يفلت أي مجرم من العقاب.

إجراءات الدولة الطالبة التسليم: لا يجوز أن يقدم هذا الطلب شفاهه غير مكتوب كان يرسل برقيا وتلغرافيا أو عن ايه طريق الاتصال الإلكتروني الا في حالات معينه تتميز بصفه الاستعجال وعلى سبيل الاستثناء ويعتبر طلب التسليم الأداة التي من خلالها

---

[١] هذه الجرائم هي الدخول غير مشروع م٢ والاعتراض غير مشروع م٣ التداخل في البيانات م٤ التداخل غير المشروع في المنظمة م ٦٥ اساءه استخدام م٦ جريمة التزوير المتعلقة بالكمبيوتر م٧ جريمة التدليس المتعلقة بالكمبيوتر م٨ الجرائم التعلق بالإعمال الإباحية وصور الأطفال الفاضحة م٩ الجرائم الخاصة.

[٢] يقصد بالجريمة السياسية: تلك الجريمة الموجه مباشره الى كيان السلطة السياسية في الدولة سواء من جهة الخارج والداخل.

[٣] HANS SCHULTZ the general framework of extradition and asylum bassoon and named treatise no ١,٢,٤,١١.p٤١٣-٣١٥.

تعبر الدولة الطالبة صراحة عن رغبتها في استلام الشخص المطلوب فبدونه لا يمكن إن ينشأ الحق في التسليم والأصل أن يكون كتابه حيث أنه.

الجهات المنوط بها إعداد طلب التسليم: يعتبر إعداد طلب التسليم من الأعمال التي تتسم بالنظام القضائي للدول فمثلا في مصر نجد أن المادة ١٧١٢ من التعليمات العامة للنيابة تقضى بأن تتولى النيابة العامة إعداد طلب التسليم من خلال مكتب المحامي العام الأول أما في الولايات المتحدة الأمريكية فأن إجراءات التسليم تبدأ من إدارة العدل مكتب الإعمال والخارجية حيث يقدم الطلب بصفه أساسيه من محاكم الولاية الطالبة التسليم.

أو من المحامي العام لهذه الولاية او النائب المحلى الخاص بها وفى فرنسا يتم إعداد طلب التسليم من وكيل النائب العام الذي يرسله الى النائب العام فيتولى هذا الأخير إرساله الى وزاره العدل حيث تقوم الأخيرة بأرسال ملف التسليم كاملاً الى وزارة الخارجية التي تتولى عبر القنوات الدبلوماسية إرسال الملف إلى سفارتها في الدولة المطلوب منها التسليم [١].

بالإضافة الى ما سبق فأنه يوجد نوع أخر من مظاهر التعاون الدولي في مجال تسليم المجرمين يتمثل في الاعتراف المتبادل بأوامر القبض أو الحبس أو التوقيف وبمقتضاه تصدر السلطة المختصة إحدى الدول أمراً بالقبض او الحبس او التوقيف وتعترف بصلاحيتها دوله أخرى ويتعين تنفيذه [٢].

---

[١] د/ عبد الفتاح محمد سراج المرجع السابق ٣٧٤ – ٣٧٦.

[٢] القرار الطارئ H.A/٥٨٥/٢٠٠٢ بشأن الأمر الأوروبي الخاص بالتوقيف واجراء التسليم بين الدول الأعضاء والذى يعد اول تدبير محدد في ميدان تنفيذ القانون الجنائي ينفذ مبدا الاعتراف المتبادل في القرارات القضائية التي تصدرها اجهزه العدالة الجنائية لدى الدول الأعضاء في الاتحاد ولقد اعتمد على اساس التوصيات الصادرة من مجلس الأوروبي في اجتماعه المنعقد في فنلندا يومي ١٥-١٦/١٠/١٩٩٠ ووفقا لهذا القرار ينبغي ان يصبح مبدا الاعتراف المتبدل هو حجر الإساس في التعاون القضائي في المسائل الجنائية داخل الاتحاد الأوروبي.

المطلب الثاني

التدريب واهميته في مكافحة جرائم الاعتداء على التوقيع الإلكتروني

يلعب التدريب دوراً هاماً في مكافحة جرائم الاعتداء على التوقيع الإلكتروني فلقد أكد القانون رقم ١٧٥لسنه ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات على أهمية التدريب للعاملين الفنيين والتقنيين العاملون في هذا المجال وتدريبهم وتوعيتهم بالقواعد والأحكام الخاصة لتنظيم الخبرة أمام جهات القضاء وتحديد التزاماتهم والأحكام الخاصة بالمساءلة الإدارية والتأديبية وبالتالي يظهر مدى أهمية التدريب وأهمية التعاون الدولي بين الدول[1].

وينقسم الى فرعين:

الفرع الأول: اهمية التدريب.

الفرع الثاني: مظاهر التعاون الدولي في مجال التدريب رجال العدالة الجنائية.

[1] القانون رقم ١٧٥ لسنه ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

الفرع الأول

أهمية التدريب

ينظر الى التدريب على إنه وسيله للاستثمار الذي تلجا إليه المنظمات الإدارية لتحقيق أهدافها باعتباره عنصراً حيويا لا بد منه لبناء الخبرات والمهارات المتجددة [١] والواقع ان التدريب أصبح يلعب دورا هاما في حياة الإنسان في عصرنا الحاضر حتى يمكننا القول بأننا نعيش اليوم عصر التدريب.

لهذا أصبح التدريب يعد جزء من عمليه التنمية الإدارية وهو يهتم بالدرجة الأولى بالكفاءة والفعالية في إنجاز العمل من هنا فقد حرصت الكثير من المنظمات العامة والخاصة على العناية به باعتبار أحد الأدوات الأساسية لرفع مستوى الإداء وزياده الكفاية الإنتاجية وإعداد العاملين على اختلاف مستوياتهم للقيام بواجبات أعمالهم والمهام الموكلة إليهم على خير وجه إضافة الى تهيئتهم لتحمل المزيد من المسؤوليات من خلال زياده قدراتهم على مواجهة المهام المعقدة في الحاضر والمستقبل فقد زاد الاهتمام بالتدريب بمختلف جوانبه الفنية والتكتيكية فقد أضحى ضرورة للفرد المتدرب وللمنظمة التي ينتسب إليها في إن واحد سواء كانت منظمه مدنيه او عسكريه حكومية أو خاصه تعمل في قطاع العدالة أما في غيرها فهو أحد العناصر الأساسية لزيادة كفاءة العنصر البشرى ويرفع إنتاجيته ويحقق التنمية بمفهومها الشامل والهدف من عملية التدريب إدخال واحداث تعديلات جوهريه على سلوك المتدربين تبدو أثارها واضحه في سلوكهم لأداء الإعمال التي يكفلون بمهامها كل في مجال تخصصه بشكل أفضل بعد عمليه التدريب لا قبلها .

تبدوا أهمية التدريب وضرورته في أنه من ناحية يعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الأخرين من خلال أشخاص أكفاء مؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهله ميسرة كما انه يعد من ناحيه أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق الفعلي والتعرف على الإخطاء والسلبيات التي يمكن أن يكشف التطبيق العملي للقوانين

---

[١] مثال ذلك التوصية الصادرة من اللجنة الفنية المتخصصة بدراسة سبل مكافحه الجرائم الإلكترونية بدول مجلس التعاون الخليجي الاجتماع الأول المنعقد بالأمانة العامة للمجلس بالرياض بالمملكة العربية السعودية في الفترة ٤-٢٠٠٤/٤/٥.

والأنظمة واللوائح ووضع الحلول الكفيلة بتجنبها وتزداد أهمية التدريب في الوقت الحاضر نظراً للتطورالتكنولوجى الكبير الذى يشهده العالم اليوم [1].

لقد كان ضرورياً أن يفرض على الجهات القانونية أن تقوم بإجراءات متناسقة وخطوات سريعة تواكب التطورات السريعة التي تشهدها تقنيات التكنولوجيا الحاسب الألى والإنترنت فكان ضرورياً أن تتصدى للأفعال الإجرامية التي صاحبت التكنولوجيا ومواجهتها هذا من ناحيه ومن ناحيه أخرى فان أعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقر في المدونة العقابية والتقليدية لما تتسم به هذه الجرائم من حداثه في الأسلوب وسرعه في التنفيذ وسهوله في إخفائها والقدرة على محو أثارها حيث أثبتت الوقائع العملية أن هناك جرائم متعلقة بالحاسب الألى وشبكه الإنترنت قد ارتكبت على مرأي ومسمع من رجال الشرطة بل قام بعض رجال الشرطة بتقديم يد المساعدة لمرتكبي هذه الجرائم دون قصد وعن جهل أو على سبيل واجبات المهنة التي يلزمهم بها هذا القانون فيجب ان تتحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه اكتشاف كافه الجرائم المعلوماتية وضبط الجناة فيها وتحقيق العدالة في حقهم .

هذا ما أثبته الواقع العملي لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيره من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعه ودقه متناهيين وهذا لن يتحقق الا بالترتيب [2] فكفاءه رجال العدالة لمواجهة هذه الظواهر المستحدثة وقدرتهم في التصدي لها لا بد وان ترتكز على كيفية تطوير العملية التدريبية [3] والارتقاء بها والنهوض بأساليب تحقيقها.

ويظهر ذلك جاليا عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركه تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الألى لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة بنتيجة ذلك اتلف ما كان قد سلم من الملفات

---

[1] د/محمد السيد عرفه تدريب رجال العدالة وأثره في تحقيق العدالة جامعه نايف العربية للعلوم الأمنية الرياض ٢٠٠٥ ص٢.

[2] د/هشام فريد رستم الجرائم المعلوماتية مرجع سابق ص ٤٣٩-٤٤٠

[3] يعرف بالتدريب بانه : نشاط مستمر ومخطط يهدف الى سد الفجوة بين الإداء الحالي والإداء المتوقع لشاغل الوظيفة فهو يقوم على اساس تحديد المهارات والقدرات الواجب توافرها في شاغل الوظيفة من ثم احداث التغيرات في سلوك وقدرات الفرد او الجماعة المسئولة عن اداة هذه الوظيفة انظر د/صالح محمد النواجم تقوم كفاءة العملية التدريبية في معاهده التدريب الأمنية من جهة نظر

والبرامج وإتلاف الأدلة قد يقع ذلك عن خطأ مشترك بين الخبراء وبين الجهة المجنى عليها فمثلا في تحقيق إحدى الجرائم المعلوماتية والتي تدور وقائعها حول طلب أحد الأشخاص من أحد الشركات زعم أنه وضع قنبلة منطقيه بنظام حاسبها الألى تبين أن الشركة وقبل إبلاغ السلطات المختصة كانت قد استدعت خبيراً للتحقيق من صحه ذلك وإبطال مفعول القنبلة إن وجدت وبالفعل نجح الخبير في اكتشاف القنبلة وإزالتها من البرامج الموضوعية فيه عندما تولت الشرطة لتحقيق اتضح إنه بإزاله القنبلة اتلفت كل الأدلة على وجودها وبالتالي فأن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق جميع أجهزه العدالة الجنائية سواء رجال الضبط القضائي او رجال التحقيق او المحاكمة على مختلف درجاتها سيما وأن متطلبات العدالة

لأهدافها فيجب تأهيل القائمين على هذه الأجهزة لكي يتم الوصول الى نجاح الدول في مواجهة هذه الأنماط المستخدمة بمفردها دون تنسيق مع الدول الأخرى فكانت الدعوة الى ضرورة وجود تعاون دولي في مجال تدريب رجال العدالة الجنائية.

لقد كان من الضرورة أن تتوافر لدى العدالة الجنائية الخلفية القانونية والتدريب الغير تقليدي ومعرفة القائمين على ذلك بمفهوم أركان العمل الشرطي واكتسابهم الخبرة الفنية في مجال الجريمة المعلوماتية وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقى التدريب ويلاحظ هنا أنه من السهل تدريب.

متخصصين في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي الادعاء العام ويذهب بعض الخبراء إنه يجب أن تتوافر لدى المتدرب خبره لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الألى [1] وبالنسبة للمنهج التدريبي فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكه المعلومات وأجهزه الحاسب الألى مع ذكر مفاهيم معالجه البيانات وتحديد نوعيه وأنماط الجرائم المعلوماتية وبيان

[1] وتعريف العملية التدريبية بانها مجموعه الأنشطة او العمليات الفرعية التي توجه لعدد من المتدربين لتحقيق اهداف معينه في برنامج تدريبي معين وتحت الإثر او الإثار المطلوبة فيه انظر صالح محمد النواجم المرجع السابق ص٧.

لأهم الصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكاب الجرائم المعلوماتية وفيما يتعلق بمنهج التحقيق فأنه لا بد وان يشمل على: [1]

١- أساليب المواجهة والاستجواب

٢- أساليب المعمل الجنائي

٣- إجراءات التحقيق

٤- التخطيط للتحقيق

٥- تجميع المعلومات وتحليلها

يجب أن يشتمل على ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الألى كأداة للمراجعة والحصول على أدله الاتهام وما يخص الملاحقة الدولية والتعاون المشترك [2].

شبكات الحاسب الألى وما يرتبط بها من قواعد بيانات ومعلومات وقد يكون البرنامج التدريبي غير رسمي من خلال تكليف المتدرب بالعمل مع شخص لديه خبره في تحقيق الجرائم المعلوماتية أو تدريب باستخدام أسلوب الفريق والذي تقوم فلسفه على تدريب الفريق او مجموعه متخصصة في جرائم الحاسب الألى مره واحده بحيث يكون لكل فريق من الفرق مهمه محدده فضلا عن إلمامه بمهام زملائه الأخرين فطبقً لهذا الأسلوب يتم التركيز على تدريب مجموعة من المتخصصين في مجالات

معينه بحيث يلم كل منهم بتخصص الأخرين ويزداد في نفس الوقت فيهما لتخصصه الأصلي [3] ويتعين هنا على الفريق أن يخوض تجارب عمليه وحيث تعرض عليه عينه من الجرائم المعلوماتية التي تم التحقيق فيها على أن يرعى في هذه العينة التنويع لكى تؤدى دورها في اكتساب المشاركين في البرنامج التدريبي الخبرة المطلوبة وهذا الأمر يتطلب إن يعهد بالتدريب الى جهات متخصصه تعنى باختيار المدربين ممن تتوافر لديهم الصلاحية العملية والفنية والصفات الشخصية تتولى التدريب في هذا

---

[1] د/ هشام محمد فريد رستم الجرائم المعلوماتية اصول التحقيق الجنائي الفني بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت كليه الشرعية والقانون بجامعه الإمارات العربية المتحدة فترة ١-٢٠٠٠/٥/٣ الطابعة الثالثة ٢٠٠٤م ص ٤٩٦.

[2] د/هشام محمد فريد رستم الجرائم المعلوماتية اصول التحقيق الجنائي الفني المرجع السابق ص ٤٩٧

[3] يمكن تقسيم الفريق الى ثلاث مجموعات رئيسيه هي: مجموعه اولى مهمتها تنفيذ القانون - مجموعه ثانيه مهمتها التدفيق والمراجعة الحسابية - مجموعه ثالثه مهمتها معالجه البيانات الكترونيه.

المجال والذى من شأنه تحقيق نتائج طيبه في عمليه التدريب [1] والعملية التدريبية لابد أن تكون مستمرة ولا تتوقف عند حد معين ولاسيما وأن الجرائم المعلوماتية ومنها الجرائم المتعلقة بالإنترنت في تطور مستمر وبشكل سريع جدا .

بالإضافة الى ذلك ينبغي أن نوصى بأن تسعى الأجهزة الأمنية المعنية بالتحقيق الى استقطاب متخصصين والكفاءات في المجال المعلوماتي وضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم ومن أجل ذلك ينبغي على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات من الجامعين من خريجي كليات الحاسبات الألية لتخرجهم ضباطا مؤهلين قانونياً وتقنيا كذلك يتعين على الكليات المعنية بتدريس القانون أن تسعى جاهده الى تدريس الحاسبات الإليه وكل ما يتعلق به الى الطلبة وأن تكون ماده الحاسب الألى وتقنيه المعلومات وإحدى المواد الأساسية لأن من شأن ذلك أن تتكون لدى خريجي هذه الكليات ثقافه قانونية وثقافه حاسوبية .

خلاصة القول إن غَرس وتطوير الثقافة الحاسوبية وسط رجال القانون والشرطة وربطها بالثقافة القانونية والشرطية التقليدية يكفل للأجهزة الأمنية ولسلطات التحقيق النجاح الباهر في مواجهة الجرائم المعلوماتية.

[1] من الأمثلة على انماط التدريب والاهتمام به على المستوى العلمي.

الفرع الثاني

مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجنائية

وينقسم الى أمرين:

اولا: تجربه الولايات المتحدة الأمريكية في هذا المجال.

ثانيا: جهود المنظمة الدولية للشرطة الجنائية الإنتربول.

ترجع أهمية مظاهر التعاون الدولي في مجال العدالة الجنائية الى افتقار الدول النامية ولاسيما أجهزة العدالة فيها الى الجاهزية لمواجهة الجرائم المتعلقة بشبكه الإنترنت والجرائم المستحدثة ذات التطور المستمر لعده أسباب منها الافتقار الى الموارد الكافية ماديه كانت أو بشريه أو لأن سلطات التحقيق لديها محدودة او لأنه لديها قوانين ونظم سبقها الزمن أو قد تفتقر لأي قوانين لتتصدى بها لهذه النوعية من الجرائم. ويرجع ذلك لأنه من البديهي أن أي دوله يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق ما غيرها من الدول كانت الدعوة الى ضرورة وجود تعاون دولي ليس فقط في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين فحسب وإنما أيضا في مجال تدريب رجال العدالة [١].

في جمهورية مصر العربية نجد أن النيابة العامة تعقد الكثير من الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقدت داخل مصر أو خارجها بالإضافة انه يتم إرسال أعضاء النيابة من اختلاف الدرجات في برنامج خارجية وذلك بالتعاون مع أجهزه النيابة العامة في الدول الأخرى والهيئات الدولية بهدف الاطلاع على أحدث النظم المقارنة وذات الشيء نجد في سلطنه عمان وقد يتم من خلال عقد ندوات ومؤتمرات أو ورش العمل الجماعي [٢] متخصصه في مواجهة تلك الجرائم تعقد على المستوى الدولي أعلى المستوى الإقليمي حيث تقدم هذه الفعاليات العلمية من أبحاثها ودراستها موضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل مناقشه أبعادها بعقليه ناجحة مما يمكن المعنيين بالوقاية ومكافحه هذه الجرائم من التعرف على أساليب ارتكابها وإخطارها ووسائل الوقاية والمكافحة بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها .

فتدريب الكوادر البشرية القائمة على إنفاذ القانون ليس بذات المستوى في جميع الدول وإنما يختلف من دولة لأخرى فحسب تقدم الدولة ورقيها ولو أمنعنا النظر في بعض الصكوك الدولية والإقليمية لوجدنا أنها دعت وبصريح النص الى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها كما في الحال في المادة ٢٩ اتفاقيه الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ٢٠٠٠م والمادة ٩من مشروع الاتفاقية العربية لمكافحه الجريمة المنظمة عبر الحدود.

التعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكه الإنترنت قد يكون بين الدول وأجهزه العدالة الجزائية لديها فعلى الصعيد العربي نجد مثلا انه هناك اجتماعات تم عقدها في إطار التنسيق بين المعاهد الفضائية العربية لتوفير التدريب والتأهيل المناسبين لأعضاء.

الهيئات القضائية العربية وقد تمخضت الاجتماعات عن الاتفاق على إعداد مشروع اتفاقيه للتعاون بين المعاهد القضائية العربية تسمى اتفاقية عمان للتعاون العملي بين المعاهد القضائية العربية والتي وقعت في ٩ ابريل ١٩٩٧.

وقد يتحقق من عقد اللقاءات وحلقات المناقشة المصغرة بين مسؤولي الاتصال بالسفارات أو المكاتب الجغرافية الإقليمية للمنظمات والأجهزة المعنية مع جهات أو أطراف يقعون في دائرة عملهم او بالقرب منها بناء على رغبه الجهة التي يمثلونها يتم خلالها تبادل الآراء والخبرات بين المشاركين وتمثل كافة هذه اللقاءات وحلقات المناقشة وسيله طيبه للحوار والمناقشة والتشاور للتعارف وتبادل الرأي والخبرة وطرح الأفكار والتصورات وتدارس سبل تنميه وتشجيع التعاون فيما بين الأطراف.

وتعد هذه الصور أكثر تطوراً للتعاون الدولي الذى يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين في مكافحه الجرائم في الدول المختلفة من خلال تبادل الخبرة وطرح موضوعات ومشكلات للتدارس المشترك والتعرف على أحداث التطورات في مجال الجريمة المعلوماتية وأساليب مكافحة وغالبا ما يجرى تنظيم مثل هذا التدريب من خلال المنظمات او الدول او الأجهزة الكبرى التي تتميز بمستوى أكثر تقدما يمكن أن يشجع الأطراف الإجرائية على المشاركة في هذه البرامج التدريبية للاستفادة منها كما يمكنها تحمل نفقات و أعباء مثل هذه الدورات .

مثل هذه الدورات البرامج العادية من الفوائد الجهات المنظمة والمشاركين فيها والجهة المنظمة يمكنها من خلال عقد مثل هذه البرامج أن تطرح ما تريد من موضوعات حيوية كما أنها تعلم عن دورها الرائد لتزيد من ثقه الأطراف الأخرى في أدائها بما يشجع على إجراء المزيد من التعاون معها وبما يضعها في مكان خاص لدى المدربون والجهات التي يتبعونها وعلى الجانب الأخر فإن هذه البرامج يمكن أن تفيد متلقى التدريب عن طريق زياده مهاراته وخبراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى الأمر الذى ينعكس على الجهة التي ينتمى إليها بالفائدة.

أولاً: تجربه الولايات المتحدة الأمريكية في هذا المجال

تعد الولايات المتحدة الأمريكية من الدول المتقدمة تكنولوجيا والمتطورة في مجال مكافحه الجرائم المعلوماتية وجرائم الشبكات وعلى الرغم من ذلك فهي تعي وتعلم أنه ما من دوله وإن كانت متقدمة يمكنها التصدي لإخطار هذه الأنماط المستحدثة من الجرائم.

لذلك فأنه كان من الضروري على الولايات المتحدة الأمريكية الحرص على تشجيع المتدربين على رفع قدرات العدالة الجنائية للدول الأخرى والحكومات الأخرى ومساعدة ما لديها من أجهزة الشرطة والمسؤولين بالادعاء العام والقضاء أكثر فاعليه لمكافحة الجريمة فمثل هذه المساعدة لا تؤدى الى تيسير بناء إطار للتعاون الدولي في مجال تطبيق القانون وحسب ولكنها تعزز أيضاً قدره الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة المعلوماتية لديها قبل أن يمتد ليتجاوز حدود بلدانها فمكتب المساعدة والتدريب على تطوير أجهزه الادعاء العام في الخارج التابع لوزارة العدل الأمريكية مكلف تحديدا بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى وتعزيز إدارة القضاء في الخارج [1] .

بالإضافة إلى ذلك وإلى الدور الحيوي الذي يلعبه البرنامج الدولي المساعدة والتدريب من قيامه بتطوير أجهزه الادعاء العام في الخارج العامل داخل وزارة العدل بنفسها على توفير مساعدات لأجهزه الشرطة في البلدان النامية في مختلف أنحاء العالم وتهدف المساعدة التي يقدمها هذا البرنامج الأخير إلى تعزيز القدرات التحقيقية لدى أجهزة الشرطة في البلدان الناشئة.

كما أنه لوزارة العدل الأمريكية دور حيوي حيث تقدم وزارة العدل الأمريكية مساعدات لتطوير القطاع القضائي في عدد من البلدان في أفريقيا وأسيا وأوروبا الشرقية والوسطى وأمريكا اللاتينية ومنطقة حوض الكاريبي والدول المستقلة حديثاً بما ذلك روسيا والشرق الأوسط مستعينة في ذلك بخبرة الوحدات المتخصصة التابعة لها منها على سبيل المثال.

---

[1] تم الاستعانة ببحث منشور لنائب مساعد وزير العدل للقسم الجزائي بوزارة العدل الأمريكية بروس سواريز على موقه وزاره الخارجية الأمريكية الصفحة الإعلامية بتاريخ ٢٠٠٦/٨/٢٦.

وحدة مكافحة استغلال الأطفال وأعمال الفحش التابعة للقسم الجزائي بها قامت بالدور الأساسي في صياغة قانون نموذجي يهدف الى مكافحة استغلال الناس عن طريق الإتجار بالبشر.

ليس هذا فحسب فمن خلال مما سبق نجد أجهزة تطبيق القانون الأمريكية توفر أيضا تدريبا لنظيرتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهد خاصه بتدريب العاملين في أجهزة تطبيق القانون كما هو الحال في كل من المجر وبوتسوانا وكوستاريكا وتايلاند وهي هذه المعاهد يقوم خبراء أمريكيون في عمل أجهزه تطبيق القانون بالاطلاع.
المتدربين على أساليب وسبل مبتكره للتحقيق ويشجعون على تبادل الآراء مع نظرائهم في مختلف أنحاء العالم.
خلاصة القول إنه ما من دوله يمكنها تحقيق النجاح بمجابهة هذا التحدي في مواجهة هذه الأنماط المستحدثة من الجرائم ومنها الجرائم الناشئة عن استخدام شبكه الإنترنت بمفردها ولا مفر من مواصلة أجهزه التطبيق القانون في أنحاء العالم تطوير القدرة على التعاون الدولي في المجال التدريبي ولا مفر للدول المتقدمة من مساعدة الدول النامية لتعزيز مؤسساتها المتخصصة للتحري والتحقيق والمحاكمة من خلال توفير التدريب وسائر أنواع المعونة التقنية.

ثانياً: جهود المنظمة الدولية للشرطة الجنائية "الإنتربول "

يرجع تاريخ التعاون الدولي الشرطي إلى بداية القرن ال ١٩، عام ١٩٠٤ عندما تم إجرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض لتاريخ ١٩٠٤/٥/١٨ م والتي نصت في مادتها الأولى.

تتعهد كل الحكومات المتعاقدة بإنشاء او تعين سلطه لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج ولهذه السلطة الحق في أن تخاطب مباشره الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة.

كان نتيجة ذلك إلى زيادة العديد رغبة العديد من الدول الى إنشاء تلك الأجهزة والاستفادة من تبادل المعلومات والخبرات والبيانات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج مناجل القضاء على هذه الجريمة في إقليمها [١].

ثم تطور بعد ذلك التعاون الشرطي الدولي إلى مرحلة دولية ويصبح موثقا ويأخذ صوره المؤتمرات الدولية [٢] أولها وأسبقها تاريخيا كان مؤتمر موناكو ١٨-١٩١٤/٤/١٤ والذي ضم رجال الشرطة والقضاء والقانون من ١٤ دولة وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية خاصة ما يتعلق بمدى إمكانيه أنشأ مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عمليه تذكر.

بعد انتهاء الحرب العالمية الأولى وتحديدا عام ١٩١٩م حاول الكولونيل فغن هوتين أحد ضباط الشرطة الهولندية أحياء فكرة التعاون الدولي الشرطي وذلك بالدعوى لعقد مؤتمر دولي لمناقشه هذا الموضوع غير أنه لم يوفق في مسعاه.

وبنهاية عام ١٩٢٣م نجح الدكتور جوهان سويرا مدير شرطة فينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي لشرطة الجنائية وذلك في الفترة من ٣-١٩٢٣/٩/٧ م ضم مندوبي تسعه عشر دول وتمخضت عنه اللجنة الدولية لشرطة الجنائية International Criminal Police Commission (ICPO) يكون مقرها فينا وتعمل على تنسيق بين اجهزة الشرطة من أجل التعاون في مكافحه الجريمة.

غير أسمها ليصبح المنظمة [٣] الدولية للشرطة الجنائية International Criminal Police Organization وحتى كتابه هذه السطور في عضويتها ١٨٢ عضواً [٤] وتهدف هذه المنظمة الى تأكيد وتشجيع التعاون بين أجهزه الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في

---

[١٠] H. Fraud Eschlanilz la cooperation policiere international.R.I.D.P.١٩٧٤.P٤٧٧-٤٧٨

[٠٢] د/محمد منصور الصاوى احكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات دار المطبوعات الجامعية الإسكندرية ص ٦٤٨ وكذلك د/ علاء الدين شحاته التعاون الدولي لمكافحة الجريمة اجتراك للنشر والتوزيع القاهر ٢٠٠٠م ص١٧٤ -١٧٦.

[٠٣] تم وضع ميثاق هذه المنظمة في الفترة ٧-١٩٥٦/٦/١٣م واعتبر نافذا اعتبار من ١٩٥٦/٦/١٣م.

[٤] http//:www.interpol.com/public /Icon/ members /default abs

أقاليم الدول المنظمة إليها [١] وتتبادل فيما بينها بالإضافة الى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف [٢] ومدها بالمعلومات المتوفرة لديها على إقليمها والخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت ومن الأمثلة على دور الإنتربول في ما يتعلق الجرائم المتعلقة بالإنترنت ما حصل في الجمهورية البناية عندما تم إيقاف أحد الطلبة الجامعين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكه الإنترنت وذلك اثر تلقى النيابة البناية برقيه من الإنتربول في المانيا بهذا الخصوص.

للإنتربول دور حيوي حيث ينظم الإنتربول القيام ببعض العمليات الشرطية والأمنية المشتركة فتعقب مجرمي المعلوماتية عامة والتوقيع الإلكتروني خاصه بتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العائد للحدود لمكونات الحاسب الألى المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثاً عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية كلها أمور تستدعى القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة والتي ينظمها الإنتربول وهى شأنها صقل مهارات وخبرات القائمين على مكافحه تلك الجرائم وبالتالي وضع حد لها [٣].

على غرار هذه المنظمة انشأ المجلس الأوروبي في لكسمبورج عام ١٩٩١ م شرطة أوروبية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت [٤] اما على مستوى العربي نجد أن مجلس وزاره الداخلية العرب أنشأ لمكتب العربي للشرطة الجنائية [٥] بهدف تأمين وتنميه التعاون بين أجهزه الشرطة في الدول الأعضاء في مجال مكافحه الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة بالإضافة الى تقديم المعونة في مجال دعم وتطوير أجهزه الشرطة في الدول الأعضاء.

---

[١] International police cooperation "clarendon press oxford ١٩٨٩P١٦٨-١٨٥malcom Anderson: policing the world: Interpol the politics of

[٢] هذا يوكد ان هذه المنظمة ليست سلطه دوليه عليا فوق الدول الأعضاء فالتعاون الشرطي في إطار هذه المنظمة يحكمه مبدا احترام السيادة الوطنية للدول الأعضاء.

[٣] Malcolm Anderson policing the world Interpol the politic s of international police cooperation "clarendon press oxford ١٩٨٩P١٦٨-١٨٥

[٤] د/ جميلا عبد الباقي الصغير الجنوب الإجرائي المرجع السابق ص٧٩.

[٥] هذا المكتب هو احد المكاتب الخمسة التابعة للأمانة العامة لمجلس وزراء الداخلية العرب مقره دمشق بالجمهورية العربية السورية.

المطلب الثالث

طرق الوقاية من الاعتداءات على التوقيع الإلكتروني

الطريقة الأولي: حماية البرامج والمعلومات.

الطريقة الثانية: حماية الملفات على مواقع الشبكات العالمية.

الطريقة الثالثة: الجدران النارية.

الطريقة الرابعة: البرامج الكاشفة.

الطريقة الخامسة: المراقبة التقنية.

الطريقة الأولي: حماية البرامج والمعلومات.

لقد ظهرت الكثير من الاعتداءات في تقنية المعلومات التي تعتبر من أبرز العوائق عن طريق الانتشار السريع وتطور تقنية المعلومات وظهر ذلك بشكل واضح ومع ظهور الضرر الواقع على المتعاملين في هذا المجال. وسعت الدول الى مقاومه هذه الاعتداءات فكانت المقاومة لهذه الجرائم والاعتداءات على نوعين: النوع الأول: المقاومة الفنية والنوع الثاني: المقاومة الأمنية.

صناعه القنبلة النووية والعقاقير المخدرة وسرقه البطاقات الائتمانية والاعتداء على حقوق الملكية الفكرية بكافة أنواعها فضلا عن الممارسات غير الأخلاقية حتى أوصلت بعض الإحصائيات تجاره الممنوع عبر الشبكة الى ١٠ % من مجموع التجارة عبر الإنترنت [١].

للمؤسسات الأمنية دور حيوي في الوقاية ومكافحة الاعتداءات وجرائم الإنترنت والكمبيوتر وقد أظهر تقرير لمراكز الإمام المتحدة للتطوير الاجتماعي والشئون الإنسانية إن الوقاية من الاعتداءات وجرائم الكمبيوتر تعتمد على المؤسسات الأمنية في إجراءات معالجه المعلومات والبيانات الإلكترونية وتعاون ضحايا جرائم الكمبيوتر مع رجال الأمن إلى جانب الحاجة الى التعاون الدولي المتبادل للبحث الجنائي

[١] د/احمد عبد الكريم سلامه: الإنترنت والقانون الدولي الخاص مؤتمر القانون والكمبيوتر والإنترنت المجلد الأول سابق الإشارة اليه الطبعة الثالثة ٢٠٠٤ م ص٤٣.

والنظامي في مجال مكافحة جرائم الكمبيوتر. هناك العديد من المشكلات القانونية في استخدام بيانات الكمبيوتر التي قدمت لجنة جرائم الكمبيوتر توصيات في هذا النوع من الجرائم الكمبيوتر وهي عدم الارتباط بالحدود الجغرافية وأيضا كون التقنية المستخدمة في هذه الجرائم متطورة جداً فالأموال التي يتم الحصول عليها من المخدرات لعصابة في طوكيو يمكن تحويلها في ثانيه واحدة الى أحد البنوك في نيويورك دون إمكانيه ضبطها [١].

تحتاج أجهزة الأمن الى التدريب والتطوير من قدراتها للتعامل مع إجراءات الكشف عن جريمة على مسرح الأحداث ومكافحة جرائم الكمبيوتر وتطوير العمل في هذا المجال وأن يكون رجل التحقيق قادراً على تشغيل جهاز الحاسب الألى ومعرفة المعدات الإضافية فيه معرفة البرمجيات اللازمة للتشغيل حيث يتمكن من تقديم الدليل المقبول للجهات القضائية وايضاً يلزم إيجاد الأنظمة اللازمة لحمايه الملكية الفكرية المتعلقة بتقنيه المعلومات ونشر الوعى العام بجرائم الكمبيوتر والعقوبات مترتبة عليها واستحدث الأجهزة الأمنية المختصة القادرة على التحقيق في جرائم الكمبيوتر والتعاون مع الدولة الأخرى في الحماية والوقاية من هذه الجرائم فقد تم بعض الدول [٢] إنشاء وحده لجرائم الكمبيوتر لتقديم مهام التدريب والمساعدة والخبراء للجهات القضائية والمشاركة في تبادل المعلومات مع الجهات ذات العلاقة.

أنه لمن الصعب على العديد من الدول القدرة على السيطرة على التحكم على الشبكة العنكبوتية وأن العديد من الجرائم الإلكترونية تكون متوافره الأمر الذى لا تمنعه الأنظمة في معظم الدول مما يعطى الفرصة للمتعدي أن يستغل هذه البرامج في فتح جهاز معين واستغلاله الاستخدام السيئ لأن هناك استخدامات مفيدة لهذا البرامج فمثلا هناك عدة برامج لسكر كلمه السر لدخول الأجهزة المحمية كلمه مرور وهما يطلق عليه CRACKING وهذه البرامج تكون مفيدة لمن نسى كلمه السر لدخول على الجهاز او الدخول على أحد الملفات المحمية وفى نفس الوقت يمكن للمعتدى أن يستغل هذه البرامج في فتح جهاز معين بعد معرفه كلمه السر والدخول على الإنترنت واستغلاله في الاستخدام السيء اذن أدوات القرصنة والإجرام متوافر لكن الإجرام يكون في الاستغلال السيء لهذه الأدوات ويوجد لدى معظم الدول الكبرى أدوات تعقب لمعرفه مصادر مطلق الفيروس مثلا أو الهجوم على بريد الإلكتروني وموقع رسمي لإحدى هذه الدول لذلك يحرض هؤلاء المعتدون على أن يتم هذا العمل الإجرامي عن طريق أجهزه الأخرين وهذا يبين أهميه أن يحمى كل واحد جهازه أن يحرص على رقمه السرى حتى لا يستغل من قبل الأخرين وينطبق هذا ايضاً على أصحاب الشبكات

---

[١] جريدة الشرق الأوسط العدد ٨١٩٦ يوم الإثنين ٢٠٠١/٥/٧ ص ٥١.

[٢] تم في الولايات المتحدة إنشاء وحده لجرائم الكمبيوتر تابعه لقسم العدالة الجنائية وتقوم بتبادل المعلومات حول جرائم الكمبيوتر مع مكتب التحقيقات الفيدرالي انظر/احمد عبد الكريم سلامه الإنترنت والقانون الدولي الخاص المرجع السابق ص٥٩.

كالجامعات والمعاهد التي توفر الإنترنت لمنسوبيها فقد يستغلها بعضهم لإطلاق الفيروسات أو غيرها من الاعتداءات الإلكترونية.

تحرص الهيئات والمنظمات على المحافظة على المعلومات إذا يمكن تعويض فقدان الأجهزة والبرامج ولكن تعويض فقدان البيانات والمعلومات والتلاعب بها يعد من الأمور الصعبة والمكلفة فالمعلومات والبيانات تعد من اهم ممتلكات أي منظمه لذا يتم السعي للمحافظة على البيانات والمعلومات قدر الإمكان حتى لا يصل إليها أشخاص غير مصرح لهم ويتم اتباع مجموعه من الإجراءات التي تضمن سلامة هذه المعلومات منها ما يلي:

١- يجب تمزيق المخرجات بواسطة الآلات خاصه قبل إلقائها وعدم إلقاء مخرجات الحاسب الألى او شريط حبر طابعه لا مثل هذه المخرجات قد تحتوي على معلومات مهمه تصل الى أشخاص غير مصرح لهم الاطلاع عليها.
٢- يجب تغير كلمة السر للدخول الى الحاسب الألى كل فتره بحيث تعتمد كل الفترة على أهمية البيانات بالنسبة للمنظمة كما ان بعض أنظمه التشغيل لا تسمح باستخدام كلمة السر نفسها مره أخرى وتجبرك على تغيرها بعد فتره معينه من قبل المشرف على نظام التشغيل.
٣- عمل طرق تحكم داخل النظام تساعد على منع محاولات الدخول النظامية مثال ذلك عمل ملف يتم فيه تسجيل جميع الأشخاص الذين وصلوا او حاولوا الوصول الى أي جزء من البيانات يحوي رقم المستخدم ووقت المحاولة وتاريخها ونوع العملية التي قام بها وغير ذلك من المعلومات المهمة.
٤- فحص ملف المتابعة للتعرف على الأشخاص الذين وصلوا الى البيانات او حاولوا الوصول اليها وتوظيف اشخاص تكون مهمتهم المتابعة المستمرة لمخرجات برامج الحاسب الألى للتأكد من انها تعمل بشكل صحيح خاصة البرامج المالية التي غالبا ما يكون التلاعب بها من قبل المبرمجين او المستخدمين وذلك عن طريق اخذ عينات عشوائية لمخرجات البرنامج في فترات مختلفة.
٥- تشفير البيانات المهمة المنقولة عبر وسائل الاتصالات كالأقمار الصناعية او عبر الألياف البصرية بحيث يتم تشفير البيانات ثم إعادتها الى موضعها السابق عند وصولها إلى الطرف المستقبل ويتم اللجوء الى تشفير البيانات والمعلومات إذا كانت مهمه لأن عمليه الشفير مكلفة.
٦- عمل نسخ احتياطيه من البيانات تخزن خارج مبنى المنظمة.

الطريقة الثانية: حماية الملفات على مواقع الشبكة العالمية

تقوم العديد من المنظمات بإخفاء المعلومات السرية المتاحة للجميع نظراً لأن الإنترنت نظام مفتوح يستطيع أي شخص الوصول من خلاله الى ملفات الأخرين ومعلوماتهم وقد يسمح الاتصال بالإنترنت لأشخاص بالوصول الى المعلومات السرية بطريقه معينه كما يستطيع بعض المتطفلين إرسال برامج سيئة كالفيروسات وغيرها تؤثر في نظام الشبكة.

من أبرز الخدمات التي تقدمها الإنترنت خدمة تنقل الملفات FTP حيث تستخدم هذه الخدمة بكثره خلال عمليه استعراض الملفات أو صفحات الإنترنت وهذه الخدمة تجعل عمليه نقل الملفات من جهاز الى أخر سهلة جدا ولتشغيل هذه الخدمة يجب أن تحصل على تصريح للدخول على ملفات جهاز معين أو على جميع أجهزه الشبكة ولذلك لابد من الانتباه الى حمايه الملفات التي يجب عدم الاطلاع عليها من قبل الأخرين الذى يتولى حماية الملفات وتحديد الملف الذى يمكن الاطلاع عليه من عدمه وهو مدير الشبكة الذى يتولى إعطاء التصاريح للدخول على الملفات حسب الأهمية والحاجه ومنها كملفات مشاعه يمكن الدخول إليها بدون كلمه سر ولا تصريح.

ينبغي قصر حق تعديل الملفات على أقل عدد ممكن من المستفيدين [١] ومن الطرق المفيدة في حماية الملفات حصر الصلاحيات اذ يمكن عن طريق حصر الصلاحيات ان تنشئ خطأ دفاعيا مبدئياً في مواجهة اختراق الملفات او الاطلاع عليها.

الطريقة الثالثة: الجدران النارية

لقد أصبحت شبكة الإنترنت شبكه تجارية ولقد زاد عدد الشبكات المتصلة بالإنترنت بشكل سريع لتبادل الخدمات والمعلومات منذ عام ١٩٩٠ م لكن الشبكات الخاصة تشتكي من عدم وجود بيئة أمنيه بسبب وصول المفتوح بين المحطات في الإنترنت ونظام الإنترنت المفتوح. [٢]

هناك العديد من الشبكات الخاصة التي ترفض الربط مع الإنترنت وبالفعل تحتاج الشبكات الخاصة الى خطه أمنيه تمنع الوصول غير المسموح به للمعلومات السرية وتمنع وصول الرسائل الضارة كالمحملة بالفيروسات وتأثير على نظام وغير ذلك تعطير الجدران النارية FIRE WALLمن الحلول الناجحة لهذه المشاكل وأن المعلومات السرية في الإنترنت مثل كلمات السر والمعلومات السرية بين المتعاملين والمصرح لهم يمكن اختراقها عن طريق الأخرين بواسطة شبكه الإنترنت.

---

[١] د/ هشام محمد فريد رستم الجوانب الإجرائية للجريمة المعلوماتية مرجع سابق ص ١١٢.

[٢] د/ فائزة يونس الباشا – الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية مرجع سابق ص ٨٩.

يعتبر فكرة الجدار الناري من الأفكار التاريخية ويرجع تاريخها حينما قام البعض بحفر خندق حول قلعه لمنع أي شخص من الدخول أو الخروج من القلعة ويمكن تفتيش من قبل الحراس على القلعة الجدار الناري هو مجموعة أنظمه توفر سياسات الأمنية بين الإنترنت وشبكات الخاصة لتصبح جميع عمليات العبور الى شبكه او الخروج منها تمر من خلال الجدار الناري الذى يصد المستعملين غير المرغوب فيهم فالجدار الناري يقوم بالتحقق من صلاحيه المستعمل المحلى والمستعمل الخارجي ونظام الدخول والخروج وتشفير المعلومات وإجراءات الحماية من الفيروسات .

ومن مزايا الجدار الناري:

١- توفير الحماية الأزمة للشبكة والمعلومات.
٢- توفير الخدمات التشفير في تكنولوجيا الجدار الناري.
٣- تخزين العمليات والمعلومات التي تمر عن طريق الجدار الناري.
٤- متابعه المستخدمين للشبكة ومن يحاول العبث بها من الخارج أو يطلب منك الموافقة عندما تريد الاتصال او الدخول الى موقع من المواقع.

إن الجدران النارية تمنع محاولات الدخول الغير مصرح به كما يحمى الموقع كل شبكه الإنترنت أو على شبكه خاصه من محاوله الدخول العشوائية كما يمكن باستخدام بعض الوسائل المساعدة تتبع محاولات الدخول الى النظام ومعرفه مرتكبيها ومعلومات الكاملة عن هذا الاختراق من جهة الوقت والمكان.

ويمكن عن طريق الجدار الناري التحكم في طريقه الاستفادة من موقعك على الشبكة حيث يسمح لمستخدمي الشبكة العالمية بالاطلاع على الموقع ولا يسمح بنقل الملفات من والى الشبكة الخاصة ويمكن أن يسمح بنسخ الملفات من الموقع ولا يسمح بنسخ الملفات الى الموقع.

أن جدران الحماية والجزء المرئي من الشبكة الخاصة او الحاسب الألى الشخصي ولذلك تعتبر من أكثر الأهداف المعرضة للهجوم فالأفضل عدم الاعتماد على جدار ناري وحيد وايضا فأن قدره الجدار الناري على مقاومه محاولات الاختراق ليست مطلقه ولذلك يعتمد مصممو هذه البرامج الإبقاء على أن تكون الجدران النارية الصغيرة وبسيطة ما أمكن لضمان انه في حاله واختراقها لا يجد المخترق فيها أي أدوات تساعده على مواصلة الاختراق.

الطريقة الرابعة: البرامج الكاشفة

لا شك أن الحاسب الألى يتكون من أجزاء مادية وبرامج ولا يقوم الحاسب الألى بإنتاج المطلوب منه بالأجهزة وحدها والا ستكون عديمة الفائدة بدون برامج وبدون صوت الحاسب الألى تستهدف الجزء البرمجي وهجوم فيروسات الحاسب الألى على الأنظمة كثيره الحدوث خصوصا في عصر انتشار شبكات الحاسب الألى وتطور وسائل تبادل المعلومات أذا أن الجهاز المصاب قد ينقل العدوى الى مئات بل ألاف الأجهزة المتصلة به على مستوى الدولة أو على مستوى العالم لقد أعلن المعهد GALLUP للبحوث عام ١٩٩١ م أن ٥٤٪ من اكبر ٥٠٠ شركه في بريطانيا قد أصيبت بهجوم من فيروسات الحاسب الألى فالحسابات الضخمة ليست بمنأى عن هجوم الفيروسات كالفيروس الذى هاجم شبكه ARPANETفي الولايات المتحدة وتسبب في ايقاف ٦٠٠٠ حاسب وكلف ٥٠٠٠٠ ساعه عمل من المبرمجين لا عاده الشبكة للعمل [١].

فلقد كان الاهتمام كبير بالوقاية من الفيروسات والكشف إنها فقد أنشأت بيوت برمجيات تحوى على عدد من الموظفين من إداريين ومحللي نظم ومبرمجين لتصميم وإعداد وكتابه برامج الكشف عن الفيروسات ANTI –VIRUSE تكون لها القدرة على اكتشاف فيرس ومن ثم تدميرها قبل أن يبدأ عمله في النظام .

مع كل البرامج الكاشفة عن الفيروسات والمضادة لها وأن أغلب برامج الكشف على الفيروسات هناك بعض ملفات التجسس قد لا تستطيع برامج مكافحة الفيروسات اكتشافها لذا لا بد من أخذ الحيطة الكافية لمنع ملفات التجسس من اختراق الموقع أو الحاسب الألى.

مكافحتها تستطيع التعرف على ملفات التجسس وتقوم بإزالتها من الجهاز وإن الجهاز لازال غير أمن ولهذا لابد من تجنب وضع قوائم بكلمات السر أو الاستخدام على الجهاز بخصوص أرقام الحسابات البنكية وبطاقه الائتمان مع التقليل من الدخول على الحسابات البنكية عبر الإنترنت وعدم الاحتفاظ بتقارير سريه تحتوي منظومه إنشاء توقيع الإلكتروني او أرقام مهمه على القرص الصلب فإن المخترقين يعملون بجد لاختراق كل الأنظمة والبرامج.

---

[١] Managing computer viruses Enliven and N.Ouffy “new you're: oxford university. press١٩٩٢.

لقد قام بعض مجرمين جرائم الإنترنت بإنشاء وتوزيع الفيروسات وإرسالها على شكل رسائل غرامية او تحذيرات أمنية و نشر مؤخرا عن صدور حكم في بريطانيا بالسجن لمده عامين ضد أحد قراصنة الإنترنت الذى قام بإنتاج وتوزيع أخطر أنواع فيروسات الحاسب في العالم والتي كان يرسلها على شكل رسائل غراميه او تحذيرات أمنيه احيانا وتعد الفيروسات الأكثر انتشار في العالم وقد وصلت التقديرات الخاصة بتكلفه تنظيف الأجهزة المصابة بهذه الفيروسات إلى ملايين الدولارات وقد القى القبض على المخرب فالورد الذى يعتبر من أكبر مصممي شبكات المعلومات في العالم وهو يتفاخر بهذه الإعمال عبر غرف الدردشة على شبكه المعلومات العالمية.

الطريقة الخامسة: المراقبة التقنية

لقد زادت وتنوعت وتعددت أساليب المراقبة التقنية بسبب تهديد البالغ للأمن القومي للدول ويظهر ذلك منذ أول حالة لجريمه موثقه ارتكبت عام ١٩٥٨م في الولايات المتحدة الأمريكي بواسطة الحاسب وخصوصا تلك التي ترتكز مصالحها الحيوية على المعلومات وتعتمد عليه في تيسير شئونها فقد تحولت هذه الجرائم من مجرد انتهاكات فرديه لأمن النظم المعلومات الى ظاهرة تقنيه عامة ينخرط فيها الكثير ممن تتوافر لديها القدرات في مجال الحاسب الألى والاتصال بشبكات المعلومات.

وتتم المراقبة التقنية بعده وسائل منها:

١- تشفير البيانات المهمة المنقولة عبر الإنترنت
٢- إيجاد نظام أمنى متكامل يقوم بحمايه البيانات والمعلومات
٣- توفير برامج الكشف عن الفيروسات والمقاومة لها لحماية الحاسب الألى والبيانات والمعلومات من الإضرار بها.
٤- عدم استخدام شبكات الحاسب الألى المفتوحة لتداول المعلومات الأمنية مع عمل وسائل التحكم في الدخول الى المعلومات والمحافظة على سريتها
٥- توزيع مهام العمل بين العاملين فلا يعطى المبرمج مثلا وظيفة تشغيل الحاسب الألى اضافه الى عمله ففي هذه الحالة سوف يكون قادراً على كتابه برامج قد تكون غير سليمه ومن ثم تنفيذها على البيانات الحقيقة كما يتم توزيع مهام البرنامج الواحد على مجموعه من المبرمجين مما يجعل كتابه برامج ضاره امراً صعباً.

الخاتمة

بعد أن استعرضنا أليات تفعيل الحماية الأمنية للتوقيع الإلكتروني من خلال إيضاح نظام تسليم المجرمين ومدى أهمية التعاون الدولي في مكافحة جرائم تقنية المعلومات وأهمية التدريب ومواكبة التطورات في المجال التكنولوجي وشروط وإجراءات تسليم المجرمين ومدى أهمية التدريب في مجال مكافحة جرائم التوقيع الإلكتروني ومظاهر التعاون الدولي في مجال تدريب رجال العدالة الجنائية و طرق الوقاية من الاعتداءات على التوقيع الإلكتروني وإيضاح مدى جهود المنظمة الدولية الشرطة الجنائية (الإنتربول) للحد من الاعتداءات على التوقيع الإلكتروني وحماية الملفات على الشبكة العالمية.

النتائج

١- آليات الحماية الأمنية للتوقيع الإلكتروني من الموضوعات المهمة التي تثير جوانب جديده ترجع الى تطور وسائل التعاملات في الإنترنت ومدى التغير السريع في الوسائل الإلكترونية فأصبح التدريب من أهم آليات الحماية الأمنية لتوقيع الإلكتروني.

٢- التداخل بين التوقيع الإلكتروني والتجارة الإلكترونية يقوم على تبادل السلع والخدمات فأن هذا التبادل أصبح معقداً يستجمع كافة شروطه القانونية من إيجاب وقبول ويقترأ بتوقيع ينسب إلى صاحبة ويرتب أثاره القانونية ومن ثم فأن الاعتداء على التوقيع الإلكتروني من شأنه المساس بالثقة والأمان في المعاملات التي تكون التجارة الإلكترونية محلا لها.

٣- العمل على تدريب الأشخاص وتوعيتهم على تفعيل الحماية الأمنية للتوقيع الإلكتروني والذي ارتبط ارتبطا وثيقا بكثير من المعاملات اليومية وطبقا للتطور السريع للجريمة الإلكترونية كان حكميا من مواكبة الجريمة المعلوماتية في ظل هيمنة ثورة تقنية المعلومات وخطورة التعامل معها دون ضوابط.

٤- افتقرت الأحكام والمعاهدات الدولية الإجراءات الواجب إتباعها بشأن تسليم المجرمين الفارين من العدالة الى الدولة الراغبة في محاكمة أو تنفيذ الأحكام الصادرة ضده وبالتالي وجود معاهده دولية ملزمة لجميع الأطراف بضرورة تسليم المجرمين.

٥- أصبح التدريب يعد جزء من عملية التنمية الإدارية فهو يهتم بالكفاءة والفاعلية بإنجاز العمل وزيادة الكفاية الإنتاجية وإعداد العاملين بالقيام بواجباتهم على اختلاف مستوياتهم على أجمل وجه.

٦- تقوم الولايات المتحدة الأمريكية بتشجيع المتدربين على رفع قدرات العدالة الجنائية للدول الأخرى ومساعده المسؤولين على مكافحة الجريمة وتيسير بناء إطار للتعاون الدولي في مجال مكافحة جرائم الإنترنت وتفعيل الحماية الأمنية للتوقيع الإلكتروني.

التوصيات

وفى ضوء نتائج الدراسة سالفة البيان فإنني أخلص لبعض التوصيات التي تفتضيها الضرورة التشريعية الجنائية املاً أن اكون قد أسهمت بذلك الجهد المتواضع في إيجاد حلول لمكافحة الجرائم الناشئة عن الاعتداء على التوقيع الإلكتروني وتتمثل هذه التوصيات في:

١- نوصى المشرع المصري بمواكبة التطورات المتلاحقة من خلال سن تشريعات جديدة أو تعديل أخرى مع إمكانيه الانضمام لاتفاقية بودابست بتاريخ ٢٣ نوفمبر ٢٠٠١ بشأن الإجرام المعلوماتي بعد تطوير البنية التكنولوجية والأمنية والقضائية حتى يمكن تطبيق بنود هذه الاتفاقية الدولية.

٢- نوصى بإدخال نصوص خاصة لحماية النظام ولحماية المعلومات المتواجدة داخل النظام بسبب قصور القواعد العامة في توفير الحماية المناسبة في هذا المجال من النصوص الخاصة التي تحمى النظام: تجريم الدخول بدون وجه حق او البقاء في النظام بدون وجه حق وتجريم الإخلال بسير النظام ومن النصوص الخاصة التي تحمى البيانات داخل النظام تجريم إتلاف البيانات او العبث بها وتجريم انتهاك سرية المراسلات الإلكترونية.

٣- نوصى أن يوضع نص تشريعي يعاقب على حيازة او استعمال برامج اختراق أنظمة الحاسب الألى او الإتجار فيها أو في كلمات المرور نظراً لخطورتها والتي تقوم بعض الجهات بنشر إعلانات عنها مفادها أنهم يمكنهم أن يخترقوا أي نظام نظير دفع مبلغ معين ومن الضروري توفير حماية لكلمات السر من محاولة المقتحمين التعرف عليها أو الإتجار فيها وهو ما يصيب الإفراد والشركات التجارية بأضرار كبيرة.

٤- نوصى بتعديل نص المادة ٢٤ من قانون التوقيع الإلكتروني المصري رقم لسنة ٢٠٠٤ فيما تضمنته من اشتراط أن يكون فعل الممثل القانوني للشخص المعنوي قد أسهم في وقوع الجريمة من علمة بذلك كشرط للمعاقبة على مخالفة أحكام القانون ومن ثم فأن مخالفه الشخص المعنوي للالتزامات المنصوص عليها في قانون التوقيع كام يلزم محلا للتجريم ولو لم يترتب عليها ارتكاب جريمة بالفعل متى كان ارتكابها نتيجة لمخالفة أحكام القانون مع اعتبار أن علمة بالجريمة التي ارتكبت بالفعل متى كان ارتكابها نتيجة لمخالفة أحكام القانون يكون ظرف مشدد يؤدى الى تغليظ العقوبة.

٥- اننا نقترح ان يتضمن النص التجريم وضع المتهم تحت المراقبة الإلكترونية فتره زمنية محدده في محاولة لتجنب خطورته الإجرامية وحتى يطمئن المجتمع الى تحقيق العقوبة لمقصدها في مواجهته او من الناحية أخرى اننا نرى ضرورة النص على تغليظ عقوبة الغرامة فيما يتعلق بالعقوبة التي رصدها المشرع جزاءاك لجرائم الاعتداء على التوقيع الإلكتروني لما لهذه الجريمة من أثار اقتصادية تتجاوز ملايين الجنيهات فيجب أن تكون عقوبة الغرامة متناسبة من جسامة الجرم.

٦- اننا لا نتفق مع سياسة المشرع في رصيد عقوبة واحده لجميع جرائم الاعتداء على التوقيع الإلكتروني خاصة ان المصالح محل الحماية في التوقيع الإلكتروني متعددة ولا تقتصر فقط على حماية حرية ممارسة وتداول السلع والخدمات عبر الإنترنت وانما تتمثل المصالح المحمية في شرعية البيانات وسرية البيانات وخصوصيتها وبالتبعية تعدد أنماط التجريم وفقاً للمصلحة القانونية محل الاعتداء ولذا كان يجب على المشرع وهو ما نوصى به أن افرد العقوبة بحسب جسامة كل جريمة فيجب تشديد العقوبة على جرائم الاعتداء على التوقيع الإلكتروني المنسوب لمؤسسات الدولة والواقع على المستندات والوثائق والعقود الرسمية لما لهذه الجرائم من خطورة شديدة على انتظام العمل بمرافق الدولة.

٧- التوصية بإنشاء معمل جنائي رقمي يكون تابعا لوزارة العدل تختص بفحص الأدلة الرقمية والتحفظ عليها وبيان ما إذا كان تم التلاعب في مكوناتها من عدمه و يكون العاملون فيه خبراء وزارة العدل الذين تتوفر فيهم المهارات والخبرة الفنية والأمانة والحيدة مع مراعاة حفظ الأدلة الجنائية التي تتعلق بجرائم الاعتداء على التوقيع الإلكتروني بالطرق المناسبة لكل حالة وذلك بالطرق المناسبة لكل حالة وذلك حتى يتم تقديمها للمحكمة وهى على حالتها التي ضبطت إذ أي تأثير او تعديل للأدلة قد ينهى القضية لصالح المتهم الذى يفسر الشك لصالحة كقاعدة عامة .

٨- نوصى بتفعيل التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات وتسليم المجرمين الهاربين من الأحكام والتأكيد على أهمية تبادل المجرمين في مكافحة الجرائم الإلكترونية وتفعيل الحماية الأمنية للتوقيع الإلكتروني وأهمية تدريب العاملين على مكافحة الجرائم الإلكترونية ومواكبة تطورات الجريمة المعلوماتية.

المراجع

مراجع باللغة العربية:

١- المراجـــع العـــامـــة:

١- د/ احمد عوض بلال الجرائم المادية والمسئولية الجنائية بدون خطا دراسة مقارنه دار النهضة العربية عام ١٩٩٣ م.
٢- د/ ايمن عبد الحفيظ استخدام استراتيجية مكافحة جرائم الحاسب الألى دار النهضة العربية الطبعة الأولى ٢٠٠٣.
٣- د/ امال عبد الرحيم عثمان الإثبات الجنائي ووسائل التحقيق العلمية دار النهضة العربية عام ١٩٧٥م.
٤- د/ احمد فتحي سرور الوسيط في القانون العقوبات / القسم العام الطبعة الخامسة دار النهضة العربية عام ١٩٨٩م.
٥- د/ حسنين ابراهيم عبيد الجريمة الدولية دراسة تحليلية تطبيقية دار النهضة العربية الطبعة الأولى ١٩٨٩م.
٦- د/ سراج الروبي الإنتربول وملاحقة المجرمين الدار المصرية اللبنانية ٢٠٠٦.
٧- د/ محمد فهمي طلبة الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني القاهرة ١٩٩١م.
٨- د/ محمد محمد مصباح القاضي قانون العقوبات القسم الخاص في الجرائم المضرة بالمصلحة العامة وجرائم الاعتداء على الأشخاص دار النهضة العربية ٢٠١٤.

٢- المراجع المتخصصة:

١- د/ أشرف توفيق شمس الدين الحماية الجنائية للمستند الإلكتروني دراسة مقارنه دار النهضة العربية الطبعة الأولى ٢٠٠٦ م.
٢- د/ ايمن سعد سليم التوقيع الإلكتروني دراسة النهضة العربية ٢٠٠٤.
٣- د/احمد شرف الدين عقود التجارة الإلكترونية تكوين العقد وثباته كلية الحقوق جامعه عين شمس ٢٠٠٢م.
٤- د/ ايمن عبد الله فكرى جرائم نظم المعلومات دار النهضة الجديدة ٢٠٠٧م.
٥- د/ ايمان مأمون سليمان ابرام العقد الإلكتروني واثباته دار الجامعة الجديدة الإسكندرية ٢٠٠٨.
٦- د/ ثروت عبد الحميد التوقيع الإلكتروني ماهيته مخاطرة دار الجامعة الجديدة القاهرة ٢٠٠٧م.
٧- د/ جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجيا الحديثة الجرائم الناشئة عن استخدام الألى الكتاب الأول دار النهضة العربية ١٩٩٢.
٨- د/ سعيد عبد اللطيف حسن اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت دار النهضة العربية ١٩٩٩م.
٩- د/ سامح عبد الواحد التهامي التعاقد عبر الإنترنت دار الكتب القانونية الطبعة الأولى ٢٠٠٨ م.
١٠- د/ طارق سرور ذاتية جرائم الإعلام الإلكتروني دراسة مقارنة دار النهضة العربية ٢٠٠١م.
١١- د/عمرو احمد حسبوا حماية الحريات في مواجهة نظم المعلومات دار النهضة العربية ٢٠٠٠م.

٣- الرسائل:

١- د/ حسام طه تمام الجرائم الناشئة عن الحاسب الألى رسالة دكتوراه كلية الحقوق جامعه طنطا ٢٠٠٠

٢- د/ حسين محمد ابراهيم النظرية العامة للأثبات العلمي في قانون الإجراءات الجنائية رسالة دكتوراه كلية الحقوق جامعه القاهرة ١٩٨١.

٣- د/شيماء عبد الغنى محمد عطاء الله الحماية الجنائية للتعاملات الإلكترونية رسالة دكتوراه كلية الحقوق جامعه المنصورة ٢٠٠٥.

٤- د/عبد الله حسين على محمود سرقة المعلومات المخزنة في الحاسب الألى رسالة دكتوراه كلية الحقوق جامعه عين شمس ٢٠٠٢م.

٥- د/ صلاح عبد الحكيم المصري متطلبات استخدام التوقيع الإلكتروني في ادارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة رسالة مقدمة للحصول على الماجستير من كليه التجارة "قسم ادارة اعمال " بالجامعة الإسلامية بغزة ٢٠٠٨.

٤- المقالات والدوريات:

١- د/ ابراهيم الدسوقي ابو الليل توثيق التعاملات الإلكترونية ومسئولية جهات التوثيق تجاه الغير المتضرر بحث مقدم الى مؤتمر الإعمال المصرفية الإلكترونية بيع التشريع والقانون الذي نظمته كلية والقانون بجامعه الإمارات بدبي في الفترة من ١٠-١٢ مايو ٢٠٠٣ المجلد الخامس.

٢- د/ ابراهيم الدسوقي ابو الليل الإنترنت والقانون الدولي الخاص فراق ام تلاق المؤتمر الذي عقدته كلية الشريعة والقانون بجامعه الإمارات العربية المتحدة في موضوع القانون والكمبيوتر والإنترنت بمدينة العين في الفترة من ١-٣ مايو سنة٢٠٠٠ بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة المجلد الأول الطبعة الثالث ٢٠٠٤ م.

٣- د/ احمد شرف الدين التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية ورقة عمل مقدمة الى مؤتمر التجارة المنعقد في جامعه الدول العربية ٢٠٠٠م.

٤- د/ على ابو مارية التوقيع الإلكتروني ومدى قوته في الإثبات دراسة مقارنه مجلة جامعه الخليل للبحوث المجلد "٥" العدد ٢ ص ١١٥ , ٢٠١٠.

٥- د/ غنام محمد غنام عدم ملائمة قواعد قانون العقوبات لمكافحة جرائم الكمبيوتر دراسة مقدمة الى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعه الإمارات العربية المتحدة في موضوع القانون والكمبيوتر والإنترنت وذلك بفندق هيلتون العين في الفترة من ١-٣ مايو سنه ٢٠٠٠.

٦- د/محمود محى الدين عوض مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ورقة عمل مقدمة الى مؤتمر المؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة ١٩٩٣.

٧- د/ محمود ثابت محمود حجية التوقيع الإلكتروني في الإثبات مجلة المحاماة عدد٢ سنه ٢٠٠٢.

مراجع باللغة الإنجليزية:

١- M. C. Bassouni international criminal law: a draft international criminal code Netherlands ١٩٨٠ p ١١٦.

٢- Draft of a law on the framework conditions for electronic signatures and to amend other regulations. (in the version decided by the cabinet on ١٦ august ٢٠٠٠)

٣- Guide to electronic commerce regulation ٢٠٠٢ op – cit.

٤- Ian a: Rambarran. I accept but do they? : The need for electronic signature legislation on mainland china ١٥ transmit `law ٤٠٥ k ٤١٧ – ١٨-(٢٠٠٢).

٥- Council of Europe activates related to information technology data protection and computer crime esonka peter information and communication technology law vol.٥ ١٩٩٦. Issue ٣. p١٧٧.

٦- Alain bensoussan internet aspects jurisdiction Hermes ١٩٩٦p١٠٩.

٧- Philip Stanly computer crime investigation and investigators computer security north Holland ١٩٩٨ p٣١٠ -٣١١.

٨- Convention surf la cyber criminality Budapest ٢٣xl ٢٠٠١ article no. ٥.

٩- Legislative and legal frameworks for combating cybercrime Jonathan J. Ruschs conference of electronic signatures towards judicial strategies for the application of e-signature law Cairo Egypt march ٨-٩ .٢٠٠٩.

١٠- Electronic signatures in global and national commerce act. ١٥ U.S.C.FF٧٠٠١ (٢٠٠٠) .

١١- James Richards "transnational criminal organizations cybercrime. CRC press. New York Washington D.C ١٩٩٩.p٦٩.

١٢- David r. johnson – dues process and cyber jurisdiction p .٧ cyber space law institute. www.masseuse.org / ice /vow/issue/١٢/due.htm١.

مراجع باللغة الفرنسية:

١- Jean- francois henrotte : l`importance de la collaboration internationale et l`experience beigedans leeching d`informations polici`eres et de cooperation judiciare projet pour la modernization des ministers publics "conference regional surf la cyber criminality's Casablanca roamed du marc ١٩-٢٠ join ٢٠٠٧ p٩٩.

٢- Cristina Shulman : standards internationaux relatifs `a la cyberciminalit`e conseil de l`Europe nations unies et union Europe`enne conf`erence r`erence regionally surf la cyberciminalite Casablanca roamed du marc ١٣-٢٠juin p ٤٩.

٣- Lamy alain bensoussan la proble`matique francaise: cplloque du ١٣ mai: commerce electronique lamy no٥٤٠,١٩٩٨.

٤- Alexander seger l`etat actuel des lois dans les paps pilotes concern's par le project "presentation des experiences" conference r`egionaele surf la cyberciminalit`e Casablanca roamed du marc ١٣-٢٠juin p ٤.

مواقع الإنترنت:

- **قانون الإونيسترال النموذجي بشأن التوقيعات الإلكترونية الصادر بتاريخ ٢٠٠١/١/١٠.**

انظر موقع المنظمة عبر الإنترنت

http://www.uncitral.org/uncitral/ar.index.htm١

١- Computer crime& intellectual property section united states department of http://www.cybercreime.gov/reporting.htm.

٢- A.s.a.p. department of justice central district of California Debra Wong young United States Arttomey Thom morsel public affairs officer. http://www.cybercreime.gov/reporting.htm.

٣- David R. Joson due process and cyber jurisdiction p. ٧ cyberspace law institute. wwwascusw.org /imp/vow/issue /١٢/due.htm١

٤- Patrick s-an- automatic system for collecting crime on the internet ٣١ October ٢٠٠٠ journals of information law and technology available on line at http://worwick.ac.uk/jilt/٠٠,٣/chem.html.

٥- William l.la fuses Valerie k Fredric aggressive enforcement of rights involving internet abuses computer law review technology journal spring:http://www.smu.edu/csr/articles.htm١.

٦- Erman"sahit" les crimes informatiques et daughters' crime dams le domain de la technology informatique en torque .r.l.d.p.١٩٩٣p.٧٧.

٧- Ea. capriole & r.sorieui le commerce international e`lectronique: vers I

٨- 'emergence de regales juridiques transnational's client ١٩٩٧ p.٣٢٣.