دور الشرطة فى مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى
- دراسة مقارنة

دكتور/ سعد عاطف عبد المطلب حسنين
دكتور فى القانون الجنائي
ومفوض مكتب براءات الاختراع – جامعة المنوفية

مقدمة

يفرض التقدم المتواصل فى تكنولوجيا الحاسب الآلى والإنترنت على جهات إنفاذ القانون أن تسير فى خطوات متناسقة مع التطورات السريعة التى تشهدها هذه التقنيات، والإلمام بها حتى يمكن التصدى للأفعال الإجرامية التى صاحبت هذه التكنولوجيا ومواجهتها هذا من ناحية، ومن ناحية أخرى فإن إعمال القانون فى مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادىء المستقرة فى المدونة العقابية التقليدية[1]، لما تتسم به هذه الجرائم من حداثة فى الأسلوب وسرعة فى التنفيذ و سهولة فى إخفائها، و القدرة على محو آثارها حيث أثبتت الوقائع العملية أن هناك جرائم متعلقة بالحاسب الآلى والإنترنت قد ارتكبت على مرآى و مسمع من رجال الشرطة، بل قام بعض رجال الشرطة بتقديم المساعدة لمرتكبى هذه الجرائم دون قصد و عن جهل، على سبيل واجبات المهنة التى يلزمهم بها هذا القانون.

مثلما حدث عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلى لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة و نتيجة لذلك أتلف ما قد سلم من ملفات و برامج، و إتلاف الأدلة قد يقع عن خطأ مشترك بين الخبراء و بين الجهة المجنى عليها ممثلاً فى تحقيق إحدى الجرائم المعلوماتية والتى تدور وقائعها حول طلب أحد الأشخاص من إحدى الشركات رغم أنه وضع قنبلة منطقية بنظام حاسبها الآلى ، تبين أن الشركة و قبل إبلاغ السلطات المختصة كانت قد استدعت خبيرة للتحقيق من صحة ذلك وإبطال مفعول القنبلة إن وجدت ، وبالفعل نجح الخبير فى اكتشاف القنبلة وإزالتها من البرنامج الموضوع فيه، وعندما تولت الشرطة التحقيق إتضح بإزالة القنبلة أتلفت كل الأدلة على وجودها، وبالتالى فإن ظهور هذه الأنماط الجديدة من

[1]Cour de cassation Chambre criminelle Arrêt du 6 novembre 2013,Patrick X. / Ministère public…https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-6-novembre-2013/

الجرائم أصبح و هذا ما أثبته الواقع العملى يشكل عبئا ثقيلاً على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائى أو رجال التحقيق أو المحاكم على مختلف درجاتها و بخاصة أن متطلبات العدالة تقتضى أن تتحمل الأجهزة الأمنية كامل المسئولية تجاه اكتشاف كافة الجرائم المعلوماتية و ضبط الجناة منها و تحقيق العدالة فى حقهم[1].

لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة و المعرفة و القدرة على كشف غموض تلك الجرائم و التعرف على مرتكبيها بسرعة و دقة متناهية ، و هذا لن يتحقق إلا بالتدريب و التعليم المستمر، فكفاءة رجال العدالة لمواجهة هذة الظواهر المستحدثة و قدرتهم فى التصدى لها لابد وأن ترتكز على كيفية تطوير العملية التدريبية و الإرتقاء بها و النهوض بأساليب تحقيقها لأهدافها ، فمن هذا المنطلق كانت الدعوة إلى وجوب تأهيل القائمين على هذة الأجهزة ، فضلاً عن التعاون الدولى و التنسيق فى مجال تدريب رجال العدالة[2].

وإدراكاً من وزارة الداخلية لحقيقة وأهمية العلاقة بين الأمن والتقدم الاقتصادى للمجتمع وأثر الجهود الأمنية فى تحقيق الاستقرار الأمنى اللازم لجذب الاستثمارات وإنجاح خطط وسياسات التنمية الاقتصادية فقد حرصت الوزارة على التصدى لكافة صور الجرائم المعلوماتية تنفذاً لأحكام ومبادئ التشريعات القائمة فى ضوء التزامات مصر الدولية فى هذا الشأن [3].

وبرامج الحاسب الآلى تعتبر بمثابة العقل المفكر للحاسب ويطلق عليها القيم الفكرية وتحتاج إلى العناية الكافية لحمايتها من العبث بها لزيادة إنتاجها والاستثمار فيها للارتقاء بكفاءتها الاقتصادية والمحافظة على القدرات المادية والبشرية المستخدمة فيها[4].

---

(1) د/ أحمد يوسف محمد السولية، التدريب التخصصى على مواجهة الجرائم المعلوماتية ، بحث منشور بندوة المواجهة الأمنية للجريمة المعلوماتية، كلية الشرطة، أكاديمية الشرطة، أبريل، 2009، صـ 1 وما بعدها، أيضاً: د/ محمد أبو العلا عقيدة، التحقيق و جمع الأدلة فى مجال الجرائم المعلوماتية، صـ 24، متاح على: موقع الموسوعة الإلكترونية العربية www. Arablaw inf.com، أيضاً: د/ هشام فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائى الفنى، بحث منشور بمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، بالتعاون مع مركز الإمارات للدراسات و البحوث الاستراتيجية و مركز تقنية المعلومات بالجامعة فى الفترة من 1 – 3 مايو 2000، المجلد الأول، ط 3، 2004، صـ 439 وما بعدها.

(2) د / أحمد يوسف محمد السولية، مرجع سابق، صـ 1 وما بعدها، أيضاً: د/ محمد أبو العلا عقيدة، مرجع سابق، صـ 24، أيضاً: د/ هشام فريد رستم، مرجع سابق، صـ 439 وما بعدها.

(3) أ/ مجدى فؤاد، الجريمة المعلوماتية وحماية حقوق الملكية الفكرية، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، أبريل، 2009، صـ 22 وما بعدها.

(4) أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية (مع التطبيق على قطاع الأمن العام، رسالة مقدمة للحصول على درجة العضوية فى العلوم الإدارية، أكاديمية السادات للعلوم الإدارية، المعهد القومى للإدارة العليا، 2004، صـ 15.

مشكلة الدراسة: تتسم الجرائم المعلوماتية بمجموعة من الخصائص التى تؤدى إلى صعوبة التعامل معها وضبطها وهذه الصعاب قد تكون على المستوى الوطنى، وقد تكون على المستوى الدولى؛ مما يتطلب التغلب على هذه الصعوبات التى تعوق ضبط هذا الإجرام المستحدث وتقديمه لساحة العدالة لمحاكمته.

الفروض والتساؤلات التى تطرح نفسها على بساط البحث فى موضوع دراستنا ما يلي:

إلى أى مدى وصلت كفاءة وقدرة قوات الشرطة المصرية فى مكافحة الجرائم السيبرانية المستحدثة بالمقارنة بدول العالم المقارن مثل فرنسا وأمريكا؟ وما هى الصعوبات والعقبات الفنية والقانونية التى تواجها فى سبيل تحقيق الأمن المعلوماتى؟ فى ضوء المنظومة التشريعية الجنائية الوطنية والمقارنة؟وسبل التغلب عليها؟ وما هى مقترحات التطوير؟

أهمية البحث: ترجع أهمية البحث لأهمية دور الشرطة فى مجال مكافحة جرائم المعلوماتية لما فرضته المتغيرات على الساحة الدولية ومنها ما تفرضه التحديات التى تواجه مرحلة النمو الاقتصادى الرقمى التى تمر بها البلاد والتى تستلزم وجود مناخ اقتصادى مستقر يعتمد على المنافسة الشريفة وتكافؤ الفرص، فضلاً عن تطور أنماط الجريمة بمختلف أشكالها باستخدام الحاسب الآلى، سواء التى تنال من الأشخاص أو الأموال أو المصلحة العامة.

هدف البحث: النهوض بدور الشرطة فى مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى أسوةً بالتجارب الموجودة فى الدول المتقدمة.

منهج البحث: دراسة تحليلية مقارنة؛ فهى دراسة تحليلية تتناول دور الشرطة فى مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فما هو متاح من نصوص تشريعية ولوائح، ودراسة مقارنة حيث يتعرض الباحث لتجارب العديد من الدول للوقوف على مدى جاهزية المنظومة التشريعية المنظمة لدور الشرطة المصرية فى مكافحة هذ الإجرام المستحدث، ومن ثم تطويره.

خطة البحث بالتفصيل: وانطلاقاً من أهمية موضوع الدراسة محل البحث، ونظراً لما عرضه الباحث سابقاً، وكضرورة تقتضيها البحوث العلمية فقد رأينا أن نقدم لموضوع دراستنا من خلال أربعة مباحث، يتناول دور الشرطة الوقائي فى مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث أول، ثم يتناول دور الشرطة فى ملاحقة وتعقب مرتكبي الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث ثان، ثم يتناول دور جهاز الشرطة الدولية (الإنتربول) بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث ثالث، ثم

يتناول مقترحات تطوير الدور الأمنى لجهاز الشرطة بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث رابع، على النحو التالى:

المبحث الأول: دور الشرطة الوقائي فى مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى.

المبحث الثانى: دور الشرطة فى ملاحقة وتعقب مرتكبي الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى.

المبحث الثالث: دور جهاز الشرطة الدولية (الإنتربول) بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى.

المبحث الرابع: مقترحات تطوير الدور الأمنى لجهاز الشرطة بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى.

الخاتمة والنتائج والتوصيات

والله ولى التوفيق،،،

الباحث: د/ سعد عاطف حسنين

المبحث الأول
دور الشرطة الوقائي
فى مواجهة الجرائم السيبرانيةالمستحدثة
وتحقيق الأمن المعلوماتى

تمهيد:

لقد ترتب على التقدم العلمي لتقنية المعلومات والتقدم السريع والمتواصل لتطوير الأجهزة والبرامج المعلوماتية، واعتماد قطاعات كبيرة من المجتمع على التقنية المعلوماتية على المستوى الدولي والمحلي فى شتى المجالات والميادين الحربية والمالية والثقافية والاجتماعية والاقتصادية والسياسية، فقد إتسعت دائرة استخدام الحاسبات الإلكترونية خلال القرنين الماضيين باضطراد وتطور مستمر وبسرعة غير مسبوقة وأصبحت كافة الأجهزة العامة والخاصة تعتمد عليها فى تسيير شئونها، وتقل دور الأوعية الورقية، وإقترن ذلك بالاعتماد على أوعية أخرى غير ورقية فى البيئة المعلوماتية كالملفات والأشرطة والأسطوانات والأقراص الضوئية.

ونظراً لهذا التغيير الذي صاحب التقدم العلمي الهائل أصبح لزاماً على الدولة أن تحمي هذا الكيان الجديد وتوفر له وسائل تأمينية تتفق وطبيعة المعلوماتية، سيما وأن الأجهزة الإجرائية يقع على عاتقها دوراً هاماً لمواجهة الجريمة المعلوماتية، وهذه الجرائم لها طبيعة خاصة وأدلتها غير محسوسة وتحتاج إلى خبرة فنية وتقنية عالية حتى تتعامل مع هذه الخواص الجديدة وبيئة المعلوماتية والعاملين والمتعاملين فيها[1].

ولهذا فإن دور الشرطة ومأموري الضبط القضائي هام جداً، فى منع هذه الجريمة سيما وأن الأدلة الرئيسية لصيانة أمن المجتمع ووقايته من عوامل تفويضه بالإضافة لدوره القضائي فى ضبط الجرائم، ذلك أن له دوراً يهدف إلى منع ارتكاب الجرائم والحيلولة دون ارتكابها، وتقليل فرص اقترافها على أرواحهم وأموالهم، وذلك بمنع أو إتقاء كل خطر من شأنه أن يسبب ضرراً لهم. كما ويتعاظم دور الشرطة الوقائي يوماً بعد يوم بسبب تعاظم الوظيفة الوقائية للقانون الجنائي على المستوي المحلي والدولي[2].

وحين تمارس الشرطة هذه الوظيفة فإنه يطبق عليها – الضبطية الإدارية أو بوليس المنع، وهي سابقة على وظيفة الشرطة القضائية التى لا تباشرها سوى بعد وقوع الجريمة والتى يطلق عليها بوليس العقاب، وإن كان من الناحية العملية يصعب

---

(1) د/ عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص 231.

(2)Cour de cassation Chambre criminelle Arrêt du 22 octobre 2013,Mohamed X. / Ministère public…https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-22-octobre-2013/

التمييز بين سلطتي المنع والعقاب أو الدور الإداري والقضائي لجهاز الشرطة والذي يتحمل فى الغالب مهام الوظيفتين وذلك لتحقيق الفاعلية وتبسيط الإجراءات[1].

فرجال الضبط القضائي la police judiciaire تخلص وظيفتهم فى التحري عن الجرائم بعد وقوعها، أما رجال الضبط الإداري la police préventive فإن مهمتهم وقائية[2] وتتمثل فى اتخاذ التدابير الكفيلة بمنع الجرائم كالتحري عن المشتبه فى أمرهم ومراقبتهم وتنظيم الدوريات لمراقبة حالة الأمن ليلاً ونهاراً، وقد عهد القانون بمهمة الضبطية الإدارية لرجال الشرطة على اختلاف درجاتهم، ولكنه لم يضف صفة الضبطية القضائية إلا على بعضهم فقط، كما أنه منحها فى الوقت ذاته لفئات من الموظفين من غير رجال الشرطة.

وتنظم دور الشرطة الوقائي، التشريعات الوضعية بقوانين ولوائح فى مختلف الدول منها السودان والكويت والبحرين وقطر والسعودية والإمارات ومصر، حيث تأخذ نصوص قوانين هذه الدول بفكرة الخطورة الإجرامية[3] فى المجال الجنائي التى تسمح باتخاذ تدابير وقائية تمنع وقوع الجريمة، والغرض من ذلك حماية المجتمع ونظمه[4]. فالتبرير الحقيقى للتدابير الاحترازية هو سد مواضع الثغرات والقصور فى نظام العقوبات، ويأتى بعد ذلك الحرص على حماية الحريات العامة، مثال ذلك اعتقال المجرم المجنون والمجرم المعتاد على الإجرام[5]. أيضاً لمأمور الضبط القضائي لدى قيام خطر من أخطار جريمة الإرهاب ولضرورة تقتضيها مواجهة هذا الخطر الحق

---

(1) أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية، مرجع سابق، صـ 114.

(2) وفى ذلك قضت محكمة النقض بأنه: لما كانت المادتان 34، 35 من قانون الإجراءات الجنائية المعدلتان بالقانون رقم 73 لسنة 1972 المتعلق بضمان حريات المواطنين لا تجيزان لمأمور الضبط القضائي أن يقبض على المتهم الحاضر إلا فى أحوال التلبس بالجنايات والجنح المعاقب عليها بالحبس مدة تزيد على ثلاثة أشهر إذا وجدت دلائل كافية على اتهامه ، وقد خولته المادة 46 من القانون ذاته تفتيش المتهم فى الحالات التى يجوز فيها القبض عليه قانوناً ايًا كان سبب القبض أو الغرض منه ، وكان سند إباحة التفتيش الوقائي هو أنه إجراء تحفظى يسوغ لأى فرد من أفراد السلطة المنفذة لأمر القبض القيام به درءًا لما قد يحتمل من أن يلحق المتهم أذى بشخصه من شيء يكون معه أو أن يلحق مثل هذا الأذى بغيره ممن يباشر القبض عليه ، فإنه بغير قيام مسوغ القبض القانونى لا يجوز لمأمور الضبط القضائي القيام بالتفتيش كإجراء من إجراءات التحقيق أو كإجراء وقائى . (الطعن رقم 8981 لسنة 74 جلسة 2005/12/26 س 56 ص 837 ق 113)، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:
http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

(3) والخطورة الإجرامية هى احتمال ارتكاب المجرم جريمة تالية؛ والاحتمال يفترض التسليم بأن للجريمة أسبابها التى تفضى اليها، سواء أكانت أسباب داخلية تتعلق بالتكوين البدنى أو النفسى للمجرم، أم كانت أسباب خارجية ترجع الى بيئته الاجتماعية. والجريمة التالية تقوم إذا كان محتملاً إقدام المجرم على سلوك إجرامى أياً كان تقوم به جريمة من الجرائم، ومن ثم فهى بطبيعتها جريمة غير معينة. وموطن الخطورة هو شخص المجرم وليس واقعة مادية معينة.... د/ محمود نجيب حسنى، شرح قانون العقوبات، القسم العام، الطبعة السابعة، دار النهضة العربية، القاهرة، 2012، صـ 1047 وما بعدها.

(4). د/ عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، مرجع سابق، صـ 232 وما بعدها.

(5) د/ محمود نجيب حسنى، شرح قانون العقوبات، مرجع سابق، صـ 1044.

في جمع الاستدلالات عنها والبحث عن مرتكبها والتحفظ عليه لمدة لا تجاوز أربع وعشرين ساعة (المادة 40 من قانون مكافحة جرائم الإرهاب رقم 94 لسنة 2015)[1]، هذا ويخضع إجراء التحفظ فى مصر تحت رقابة القضاء، كما تحسب مدة التحفظ ضمن مدة الحبس الاحتياطي ويجب إيداع المتهم في أحد الأماكن المخصصة قانوناً (المادة 40 من قانون مكافحة الإرهاب المذكور).

وقد نصت المادة 62-2 من قانون الإجراءات الجنائية الفرنسى المعدل بالقانون رقم 392 فى 14 إبريل 2011 – ثلاثة شروط لمباشرة مأمور الضبط القضائى سلطته فى التحفظ على المشتبه فيه، هى أن تكون الجريمة المشتبه فى ارتكابها أو الشروع فى ارتكابها جناية أو جنحة معاقب عليها بالحبس، وأن تتوافر أسباب معقولة للاشتباه فى ارتكابها أو الشروع فى ارتكابها، وأن يهدف من وراء ذلك تحقيق ستة أهداف منها أن يضمن إتخاذ التدابير التى توقف وقوع الجناية أو الجنحة، كما ان الحد الأقصى للتحفظ بمعرفة مأمور الضبط القضائى فى جرائم الإرهاب 144 ساعة أى 6 أيام[2].

ويخضع إجراء التحفظ فى فرنسا لرقابة الهيئة القضائية، إذ يجب من بداية التحفظ أن يخطر مأمورى الضبط القضائى النيابة العامة (إذا تطلبته أعمال الاستدلالات أو عند وقوع الجريمة فى حالة التلبس) أو قاضى التحقيق (إذا تطلبه تنفيذ الندب للتحقيق، وقد استقر قضاء محكمة النقض الفرنسية على أن التأخير غير المبرر فى هذا الاخطار يترتب عليه بطلان التحفظ[3].

ويتناول الباحث فيما يلى: دور الشرطة فى منع جرائم الاعتداء السيبرانية، ثم ضرورة تأهيل رجال الشرطة فى مجال ضبط الجريمة المعلوماتية، ثم استراتيجية وزارة الداخلية المصرية بشأن مكافحة جرائم الاعتداء السيبرانية، ثم تفعيل الدور الأمني الوقائى لجهاز الشرطة فى مكافحة جرائم الاعتداء السيبرانية، واخيراً مدى جواز الاستعانة بمحام أثناء الاستدلالات على النحو التالى:

---

(1) قانون مكافحة جرائم الإرهاب رقم 94 لسنة 2015، الجريدة الرسمية، العدد 33 مكرر، 30 شوال 1436، 15 أغسطس 2015.

(2) د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، الكتاب الأول، دار النهضة العربية، القاهرة، ط10، 2016، ص 710.

(3) – Crim.10 mai.2001,Bull.n°114, 2 Fevr.2005,Bull.n°411

أولاً
دور الشرطة فى منع جرائم الاعتداء السيبرانية

يقصد باستراتيجية منع الجريمة؛ ذلك المنهج أو الإطار القائم على منع الجريمة وحصر معدلات ارتكابها وذلك من خلال العديد من الوسائل المتنوعة والكفيلة بتحقيق ذلك.

وتعتمد الاستراتيجية فى خطتها لمنع الجريمة على عدة مقومات أساسية تعتبر بمثابة ركائز أو دعائم يتعين توافرها ويمكن حصرها فى القيم الفكرية وسلامة التوجه، وكفاءة الأجهزة المنفذة، وفعالية القوانين العقابية.

والقيم الفكرية يقصد بها مجموعة المبادئ المستمدة من التراث الاجتماعى للمجتمع مثل حسن التنشئة الدينية وإسهام المواطن والأسرة فى حماية أنفسهم والمجتمع من الجريمة وتصديهم لمكافحتها وكذلك الموازنة العادلة بين اعتبارات الحرية الفردية ومقتضيات المصلحة العامة.

أما عن كفاءة الأجهزة المنفذة فلابد من تحديث أجهزة العدالة الجنائية وآلياتها التنفيذية من شرطة وإدعاء وقضاء ومؤسسات عقابية وإحلال المنهج العلمى كأسلوب لعملها بدلاً من الأساليب التقليدية.

وبالنسبة لفاعلية القوانين فمهما حفلت استراتيجية منع الجريمة بالقيم الفكرية القويمة أو سهرت على تنفذها أجهزة العدالة القادرة على حسن أداء مهامها فإن ذلك لا يكفى ولابد من توافر الوسيلة الفعالة التى تعتبر الأساس الجوهرى القادر على وضع تلك القيم موضوع التنفيذ وذلك من خلال قوانين عقابية فعالة.

وبجانب تلك المقومات التى ترتكز عليها استراتيجية منع الجريمة فإن وسائل تحقيق تلك الاستراتيجية للوصول من خلالها إلى الغاية المرجوة منها والمتمثلة فى منع الجريمة أو النزول بها إلى أدنى معدل ممكن تتمحور حول ضرورة إجهاض عنصر أو أكثر من العوامل المكونة لدورة السلوك الإجرامى دون إكتمال حلقاتها.

ولابد من إجراء الدراسات العميقة للإحاطة بكافة العوامل لمنع الجريمة ولابد من وضع الخطط الكفيلة بإجهاض دورة السلوك الإجرامى[1] والحيلولة دون اكتمال عناصرها وكذا الاهتمام برسالة الإعلام الأمنى والتركيز على دوره فى منع الجريمة.

---

[1] نظرًا للتغيرات السريعة في التقنية، أصبح سلوك مجرمي الإنترنت ديناميكيًا، مما يجعل من الضروري إعادة تصنيف النوع الذي يتم استخدامه حاليًا. وبشكل أساسي، يتطور سلوك مجرمي الإنترنت بمرور الوقت حيث يتعلمون من أفعالهم وتجارب الآخرين، ويعززون مهاراتهم. إن توقيع الجاني، وهو سلوك متكرر يعرضه مرتكبو الجرائم في كثير من الأحيان في مسرح الجريمة، يوفر لوكالات إنفاذ القانون أداة تعريف مناسبة ويقدم للمحققين فرصة فهم الدوافع التي ترتكب مثل هذه الجرائم. وقد ساعد هذا الباحثين على تصنيف نوع مرتكب الجريمة الذي يتم البحث عنه. إن قراءة وفهم سيكولوجية مجرمي الإنترنت، وفهم وتحليل دوافعهم والمنهجيات التي يعتمدونها. مع فهم هذه الدوافع ، يمكن للباحثين والحكومات والممارسين اتخاذ تدابير فعالة للتصدي للجرائم الإلكترونية والحد من أضرارها.....

Jahankhani, Hamid (Ed.), Cyber Criminology,2018,https://www.springer.com/gp/book/9783319971803

ولابد من تركيز استراتيجية المواجهة على خطط منع الجريمة للحيلولة إبتداء دون إتمامها ولأجهزة الإعلام دور كبير فى مواجهة الجريمة ومنع ارتكابها وذلك من خلال توظيف جانب مناسب من برامجها للغايات الأمنية ومتابعة الأحداث على الساحة الأمنية متابعة دقيقة وتطوير رسالتها الإعلامية على نحو مشوق وجذاب ومبتكر لتزيد من وعى الأفراد تجاه القضايا الأمنية المختلفة.

وتعد التكنولوجيا الحديثة أهم مظاهر حياتنا اليومية المعاصرة ولكن الاستخدام المتزايد للأنظمة المعلوماتية رغم ماله من فوائد جمة وعظيمة فى مجال الرقى والتقدم التكنولوجى والإنسانى يقابله وجه آخر مظلم حيث توجد آثاراً سلبية لهذا الاستخدام نتيجة لهذا الاستخدام نتيجة لهذا الاستخدام نتيجة الاستغلال المتعسف والسيئ لهذه التقنية مما أفرز نوعاً جديداً من الإجرام المعلوماتى وأصبح حقيقة اجتماعية أو ظاهرة إجرامية تستوعب النظر إليها ومعالجتها.

ونظراً لطبيعة الجرائم المعلوماتية الخاصة فإنه توجد صعوبة فى دور الشرطة الوقائى لمنع ارتكاب هذه الجرائم خصوصاً إذا كان محلها البيانات التى تحويها الملفات أو الأسطوانات أو بنوك المعلومات.

ونظراً لأن قلب النظام المعلوماتى أو البيئة المعلوماتية هو البرامج المعلوماتية فقد وضعت القوانين الحديثة بعض النصوص توفر الحماية الممكنة لهذه البرامج من السرقة أو النسخ الغير مشروع لها. وتقوم أجهزة الشرطة بدور هام فى الحفاظ على هذه البرامج من السرقة أو النسخ غير المشروع.

ولما كانت صناعة البرمجيات قد غدت من الصناعات الهامة التى تساهم فى زيادة الدخل القومى فأصبحت محل عناية واهتمام الدولة فوفرت لها الحماية القانونية كما أوكلت إلى الأجهزة الأمنية باتخاذ الإجراءات الكفيلة للحد من جرائم سرقتها أو نسخها أو التعدى عليها.

ونظراً لطبيعة هذه البرامج الغير محسوسة فى الواقع المادى والتى تتطلب حمايتها طبيعة خاصة ووسائل تأمينية ذات تقنية عالية توفر لمنتجيها والقائمين عليها والمتعاملين معها.

ودور الشرطة ينحصر فى نطاق ضيق حدده القانون بإلزام المتعاملين فى هذه البرامج والمتعاملين معها بالحصول على ترخيص للتعامل مع هذه الأجهزة وبرامجها ومنوط بجهاز الشرطة التأكد من التزام هذه الجهات بذلك الأمر كما توجد وحدات من الشرطة متخصصة بالعمل فى هذا المجال مزودة بالخبراء المدربين وتنظم دورات لهم فى هذا المجال لأحكام الرقابة على المحلات العامة وتوجد هذه الوحدات تحت

مسمى (شرطة المصنفات الفنية) يتبعها العديد من المخالفات كما حالت فى أحيان غير قليلة دون وقوع جرائم الغرض منها الاعتداء على برامج الحاسب[1].

وتبدو أهمية هذه الوظيفة فى شأن الحفاظ على النظام العام بالدولة، والذي قد تحل به التكنولوجيا الحديثة، فى هذه الحالة تتدخل سلطات الضبط الإداري لوضع الأمور فى نصابها سيما فى حالة إساءة استخدام الحاسب الآلى. فالكمبيوتر من معجزات القرن العشرين والحادي والعشرين حيث غزا مجالات الحياة وأنشطة الإنسان اليومية وأصبح لا غنى عنه كالماء والهواء تماماً.

ويذكر كذلك أن الاستخدام المتزايد للأنظمة المعلوماتية رغم ما له من فوائد جمة وعظيمة فى مجال الرقي والتقدم التكنولوجي والإنساني، يقابله وجه سلبي آخر حيث توجد آثار سلبية لهذا الاستخدام بسبب الاستغلال المتعسف والسيئ لهذه التقنية الأمر الذي أفرز عنها نوعاً جديداً من الإجرام يطلق عليه الإجرام المعلوماتي وقد أصبح حقيقة اجتماعية أو ظاهرة إجرامية تستوجب النظر إليها، ومعالجتها قانونياً: حتى تضع الضوابط التى من شأنها أن تحد من التعدي على برنامج الحاسب الآلى أو بياناته أو ملفاته، والتى تسبب الكثير من الخسائر الفادحة للمجتمع أو لأفراده القائمين على العمل فى هذه المجالات والتى تقدر بمليارات الجنيهات، وتشكل قطاعاً كبيراً من الدخل القومي لكثير من البلدان، وقد تهدد هذه الجرائم الكيان الاقتصادى والسياسي والأمني لدول كثيرة متى كانت هذه الجرائم محل اهتمام الدول على الصعيد المحلي والدولي[2].

وبالنظر إلى الطبيعة الخاصة للجريمة المعلوماتية، كذلك البيئة المعلوماتية غير المحسوسة تظهر صعوبة الدور الشرطي – أو الوقائي – فى منع ارتكاب هذه الجرائم، خصوصاً إذا كان محلها البيانات التى تحويها الملفات المعلوماتية أو بنوك المعلومات حيث لا يمكن للشرطة أن تقوم بدور إيجابي فى هذا المجال.

---

(1) أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية، مرجع سابق، صـ 114 وما بعدها.

(2) ووفقاً لبعض التقديرات، تقدر أن الخسائر الناجمة عن الجرائم السيبرانية، هي صناعة تريليون دولار أمريكي وتنمو بسرعة بانتشار الشركات العاملة في الأنشطة الإجرامية السيبرانية، للمزيد فى ذلك؛ لتوضيح الجوانب النوعية والكمية المختلفة في صناعة الجريمة السيبرانية العالمية.....

- Kshetri, Nir,The Global Cybercrime Industry,Economic, Institutional and Strategic,Perspectives,2010,https://www.springer.com/gp/book/9783642115219

- Smith, Russell G., Chak-Chung Cheung, Ray, Yiu-Chung Lau, Laurie (Eds) Cybercrime Risks and Responses,Eastern and Western Perspectives,2015,https://www.springer.com/gp/book/9781137474155#aboutBook

وبالنظر إلى قلب النظام المعلوماتي أو البيئة المعلوماتية هو البرامج المعلوماتية، فقد وضعت القوانين الحديثة بعض النصوص التى توفر الحماية الممكنة لهذه البرامج، ومن هذه القوانين: قانون التجارة الإلكترونية فى إمارة دبي رقم (2) لسنة 2002 الذي كفل حماية جنائية ومدنية للمعاملات الإلكترونية والتوقيع الإلكتروني فى إمارة دبي[1]، وكذلك قانون حماية حقوق المؤلف والحقوق المجاورة الإتحادي رقم (7) لسنة 2002 والذي تضمن حماية جنائية لبرامج الحاسب الآلى بوصفها من المصنفات المشمولة بالحماية فى نطاق هذا القانون، والمرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات فى دولة الإمارات العربية المتحدة[2].

وتقوم أجهزة الشرطة بدور هام فى الحفاظ على هذه البرامج من السرقة أو النسخ غير المشروع لها، ومن هذه التشريعات كذلك فى مصر: قانون حماية حقوق الملكية الفكرية رقم 182 لسنة 2002م[3]، وقانون التوقيع الإلكتروني رقم (15) لسنة 2004م[5]، وقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م[4].

وبرامج الحاسب الآلى تعد بمثابة العقل المفكر للحاسب الآلى، ويطلق عليها القيم المنطقية أو الكيانات المنطقية وتحتاج إلى العناية الكافية لحمايتها من العبث بها لزيادة إنتاجها والاستثمار فيها للارتقاء بكفاءتها الاقتصادية والمحافظة على القدرات المادية والبشرية المستخدمة فيها.

ولما كانت صناعة البرمجيات قد غدت من الصناعات الهامة التى تساهم فى زيادة الدخل القومي وتساهم فى كفاءة إنتاجية الأنظمة المعلوماتية فقد أصبحت محل عناية واهتمام الدولة، ووفرت لها الحماية القانونية، كما لو وكلت إلى الأجهزة الأمنية باتخاذ الإجراءات الكفيلة للحد من الجرائم الخاصة بسرقة البرامج أو نسخها أو التعدي عليها.

---

(1) قانون إمارة دبى رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية، صدر فى دبى بتاريخ 12 فبراير 2002م، الموافق 30 ذى القعدة 1422هـ .

(2) منشور بالجريدة الرسمية العدد 540 ملحق السنة الثانية والأربعون - بتاريخ 26-8-2012، متاح على:

- Available at:
http://rakpp.rak.ae/ar/Pages/%D9%85%D8%

(3) قانون حماية حقوق الملكية الفكرية المصرية رقم 82 لسنة 2002 – الجريدة الرسمية – العدد 22 مكرر -2 يونيه 2002.

(4) القانون رقم 15 لسنه 2004 بشأن تنظيم التوقيع الإلكترونى و بإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات فى أبريل سنة 2004- الجريدة الرسمية – العدد 17 تابع (د) فى 22 أبريل سنة 2004.

(5) القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر ج فى 14 أغسطس سنة 2018.

وبالنظر إلى طبيعة هذه البرامج غير المحسوسة فى الواقع المادي، والتى تتطلب حمايتها طبيعة خاصة ووسائل تأمينية ذات تقنية عالية توفر لمنتجها والقائمين علىها واستخداماتها والمعاملين معها. ذلك أن دور الشرطة ينحصر فى نطاق ضيق حدده القانون بالتزام المتعاملين فى هذه البرامج واستخدامات المتعاملين فىها بالحصول على ترخيص للتعامل مع هذه الأجهزة وبرامجها ومنوط بالشرطة التأكد من التزام هذه الجهات بذلك الأمر. وتوجد على سبيل المثال وحدات شرطة متخصصة لمكافحة الجريمة المعلوماتية منها فى مصر، مباحث جرائم الحاسب الآلى وشبكات المعلومات، مباحث المصنفات الفنية، ويتبعها الكثير من الخبراء وضباط البحث الجنائى فى القاهرة، وقد تسنى لها ضبط العديد من المخالفات فى مجال المعلوماتية[1]. كذلك فإن الشرطة فى مختلف إمارات دولة الإمارات العربية المتحدة مدربة تدريباً على مكافحة الجريمة المعلوماتية من خلال وحدات أو فرق خاصة جاهزة لمواجهة هذه الجريمة[2].

هذا ومن الأهمية بمكان إنشاء قاعدة بيانات عن جميع نوادى التكنولوجيا المستخدمة لشبكة الانترنت وكذلك جميع الشركات والمؤسسات لتيسير وتسهيل عملية الكشف عن مصدر سوء استخدام شبكة الانترنت وإجراء التحريات الفنية اللازمة فى هذا الشأن[3].

ثانياً

[1] وبشأن اساءة استخدام الحاسب الآلى والانترنت.... فقد قضت محكمة النقض على أنه: من المقرر أن التفتيش الذي يجريه رجال الشرطة فى منزل بغير إذن من النيابة العامة ولكن بإذن صاحب المنزل هو تفتيش صحيح قانونًا ، ويترتب عليه صحة الإجراءات المبنية عليه ، وإذ أذنت الطاعنة لضابط الواقعة بالتفتيش على اعتبار أنها صاحبة المنزل والحائزة له فى الفترة التي تم فيها التفتيش ، وكان الحكم المطعون فيه قد خلص فى استدلال سائغ إلى أن رضاء الطاعنة بالتفتيش كان حُرًّا حاصلًا فيما انتهى إليه من أن تفتيش مسكن الطاعنة تم صحيحًا قانونًا ، ومن ثم فإن النعي عليه فى هذا الخصوص لا يكون سديدًا . (الطعن رقم 9680 لسنة 86 جلسة 2018/3/21)، س69، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:
http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

[2] د/ عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 231 وما بعدها.

[3] د/ إيهاب عبدالسميع روبى محمد، الجريمة عبر الانترنت، صورها ومشاكل اثباتها، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2016، صـ 315.

ضرورة تأهيل رجال الشرطة في مجال ضبط الجريمة المعلوماتية

إن الملاحقة الجنائية فى جرائم الكمبيوتر تتطلب استراتيجية خاصة بخبرة رجال الشرطة وجهات الإدعاء والقضاء على نحو يساعدهم على مواجهة تقنيات الحاسب الآلى المتطورة وتقنيات التلاعب فيه حيث تتعقد التقنيات المرتبطة بوسائل ارتكاب الجرائم الخاصة بها[1]. لذلك فإنه يجب استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبيها، وكيفية ارتكابها مع الاستعانة بوسائل جديدة كذلك لضبط الجاني والحصول على أدلة إدانة.

ولهذا فمن المتصور أن يجد مأموري الضبط القضائي أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، ومما يزيد من صعوبة هذا الأمر افتقار أنظمة الحاسبات وشبكات المعلومات فى البدايات الأولى لاستخدامها، لأساليب الرقابة وضوابط التدقيق والمراجعة على العمليات والتطبيقات وعدم تزويدها بوسائل فنية لاكتشاف وتتبع مسار العمليات، فضلاً عن ما تصادفه هذه الجهات من صعوبات فى التحري عن جرائم الحاسب عابرة الحدود لاسيما بعد انتشار استخدام شبكة المعلومات العالمية.

وفى أحيان كثيرة تفشل أجهزة الشرطة فى تقدير أهمية الجريمة المعلوماتية نظراً لنقص الخبرة والتدريب، وللسبب ذاته كذلك قد تفشل جهات التحقيق فى جمع أدلة جرائم الحاسب الآلى مثل مخرجات الحاسب وقوائم التشغيل، بل إن المحقق كما هو الحال أحياناً فى بعض الجرائم الأخرى قد يدعو الدليل بمحوه الأسطوانة الصلبة لخطأ وقع منه، أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة أو بالتعامل المتسرع أو الخاطئ مع الأدلة.

وحين يستخدم الكمبيوتر كأداة لارتكاب الجريمة، تظهر معوقات لرجل الشرطة أو مأمور الضبط القضائي وتخلص فى الآتي:

- إما أنه يتجاهل هذا الدليل تماماً.
- وإما محاولة فحص هذا الدليل بدون أية مهارات فى مجال الكمبيوتر، وإما حمل المشتبه به على استعادة معلومات من الكمبيوتر ثم بعد ذلك تتم مصادرة الكمبيوتر، حيث أن الشهادة التى سيدلي بها تصبح حرجة فى ظل مواجهة المعلومات المستمدة من الكمبيوتر.
- وإما مصادرة جهاز الكمبيوتر بدون معرفة ما يوجد فيه من معلومات وبالتالى زيادة الفرصة فى فقد هذه المعلومات.

---

[1] Tribunal correctionnel de Nanterre Jugement du 10 novembre 2011,Greenpeace et autres / EDF et autres…https://www.legalis.net/jurisprudences/tribunal-correctionnel-de-nanterre-jugement-du-10-novembre-2011

ولذلك يرى جانب من الفقه الجنائي – كخطوة أولى – ضرورة منح صفة الضبطية القضائية لأولئك العاملين فى مجال المعلومات الأمنية سواء كانوا من أفراد الأمن أو فى القطاعات ذات العلاقة بجهاز الحاسب الآلى سواء كانوا فنيين أو خبراء، وذلك حتى يتمكنوا من ضبط الجرائم المعلوماتية فى نطاق عملهم[1]، سيما وأن المادة (23 أ.ج) من القانون المصري، والمادة (34) من قانون الإجراءات الجزائية الإماراتي، تسمح بذلك، إذ يحق لوزير العدل بالاتفاق مع الوزير المختص تخويل بعض الموظفين صفة الضبطية القضائية بالنسبة للجرائم التى تدخل فى دائرة اختصاصهم، وتكون متعلقة بأعمال وظائفهم.

وتحقيقاً لهذه الآمال صدر القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، وقد نص فى المادة الخامسة من على ذلك كما سنرى لاحقاً[2].

والحقيقة أن المشكلة ليست فى منح الموظفين ذوي العلاقة بجرائم الحاسب الآلى، صفة الضبطية القضائية، ذلك أن مأموري الضبط القضائي القائمين بضبط هذه الجرائم وسلطات التحقيق تنقصها الثقافة فى الجريمة المعلوماتية، وأن اكتشاف هذه الجرائم والتوصل إلى فاعليها وملاحقتهم قضائياً، لا يتطلب فقد الإلمام بأصول البحث الجنائي أو قواعد التحقيق القانونية، فذلك مفترض باعتبار أنه إعمال لقاعدة الشرعية التى تحكم الإجراءات الجنائية، لكن يجب الإلمام بأصول التحقيق الجنائي الفني فى الجرائم التقليدية، فضلاً عن مهارات خاصة تسمح باستيعاب تقنيات الحاسب الآلى من حيث برامجه وأنظمته، وطبيعة الجريمة الواقعة عليه ومفرداته من احتيال إلكتروني وقرصنة واختراق وحماية وكيفية كسر جدران هذه الحماية، وفيروسات الكمبيوتر، ونظم استعمال ومعلومات دولية وغيرها من مصطلحات يمكنه عن طريقها التعامل مع هذه الجريمة المتفردة فى خصوصيتها، وكذلك التعامل مع المجرم المعلوماتي وهو مجرم ذا طبيعة خاصة يتعين فهم كيفية التعامل معه.

ولهذا تبدو أهمية تبني استراتيجية واضحة فى مجال البحث عن أدلة إثبات الجريمة المعلوماتية من حيث إعداد مأموري الضبط القضائي والنيابة العامة وقضاء الحكم بصفة خاصة بالنسبة للبحث عن الأدلة لإثبات جرائم تقنية المعلومات.

وهذه المهمة المتعلقة بالتدريب، تحتاج إلى الدراية التامة بطبيعة هذا النوع من الجرائم، ويتسم الكشف عنه وإثباته بصعوبات كبيرة فمن المعلوم أن جهات التحري والتحقيق بطرقها التقليدية لجمع عناصر الإثبات عن طريق التفتيش

---

(1) د/ عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، مرجع سابق، صـ 237 وما بعدها.

(2) القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14/ 8/ 2018.

والضبط[1]، أي تجميع الاستدلالات المادية، وذلك تمهيداً لتحقيق واستخلاص الأدلة والبراهين المادية، ولكن فى محيط الجريمة المعلوماتية القائمة على تقنية الاتصالات والتوصيلات والوسائط الإلكترونية، لا تستطيع سلطة الاستدلال أو التحقيق أو القضاء تطبيق إجراءات الإثبات التقليدية على غالبية جرائم تقنية المعلومات خاصة ما يتعلق بالأشياء المعنوية كمحل للجريمة، وعلى ذلك فإنه يجب تدريب وتأهيل مأموري الضبط وسلطة التحقيق والقضاء المختصين بجرائم تقنية المعلومات[2].

كما يتطلب الأمر زيادة العناية بأعمال الخبرة الفنية القضائية المتخصصة بالإثبات العلمي الفنى للجرائم الرقمية، فضلاً عن إقامة علاقات تبادل وتكامل فى هذا المجال مع الدول العربية من جانب، وبينها وبين غيرها من الدول المتقدمة من جانب آخر[3].

ثالثاً
استراتيجية وزارة الداخلية المصرية بشأن مكافحة الجرائم السيبرانيةالمستحدثة

لقد حدد دستور مصر الجديد لعام 2014، نطاق العمل الأمنى لجهاز الشرطة المصرية، حيث تنص المادة 206 من الدستور المصرى على أنه: "الشرطة هيئة مدنية نظامية، فى خدمة الشعب، وولاؤها له، وتكفل للمواطنين الطمأنينة والأمن، وتسهر على حفظ النظام العام، والآداب العامة، وتلتزم بما يفرضه علىها الدستور والقانون من واجبات، واحترام حقوق الإنسان وحرياته الأساسية، وتكفل الدولة أداء أعضاء هيئة الشرطة لواجباتهم، وينظم القانون الضمانات الكفيلة بذلك".

وقد حددت المادة 3 من القانون رقم 109 لسنة 1971 فى شأن هيئة الشرطة اختصاصات هيئة الشرطة بالمحافظة على النظام والأمن العام والآداب وبحماية الأرواح والأعراض والأموال وعلى الأخص منع الجرائم وضبطها كما تختص بكفالة الطمأنينة والأمن للمواطنين فى كافة المجالات وتنفيذ ما تفرضه عليها القوانين واللوائح من واجبات.

وقد صدر القرار الوزارى رقم 13507 لسنة 2002 فى شأن إنشاء إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق نص على "تنشأ بالإدارة العامة للمعلومات والتوثيق إدارة بحث بمسمى إدارة مكافحة جرائم

---

(1) الطعن رقم 9680 لسنة 86 جلسة 2018/3/21، س69، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:
http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

(2) د/ عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، مرجع سابق، صـ 237 وما بعدها.

(3) د/ أحمد يوسف أحمد حسين الطحاوى، الأدلة الالكترونية ودورها فى الاثبات الجنائى- دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2015، صـ 335.

الحاسبات وشبكات المعلومات تخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنياً مصلحة الأمن العام وتختص بما يلى:

* وضع خطة تأمين ووقاية نظم وشبكات المعلومات لأجهزة وزارة الداخلية لمنع وقوع أية جرائم عليها باستخدام الأساليب والتقنيات العلمية الحديثة وبحث مدى كفاية تلك الأساليب لتحقيق الأهداف المطلوبة وتنفذها بعد اعتمادها وذلك بالتنسيق مع الأجهزة المختصة بذلك سواء من داخل الوزارة أو خارجها ووفقاً للقوانين واللوائح والتعليمات المنظمة لذلك.

* مكافحة وضبط الجرائم التى تقع باستخدام الحاسبات على نظم شبكات المعلومات وقواعد البيانات كالتخريبات والفيروسات والاختراقات – واتخاذ الإجراءات القانونية حيالها وذلك بالاشتراك والتنسيق مع الأجهزة المعنية وفقاً للتعليمات المنظمة لذلك.

* إخطار الأجهزة النوعية الشرطية المختصة بأعمال المكافحة بالبيانات والمعلومات المتعلقة بالجرائم الأخرى والتى يمكن جمعها أو التوصل إليها من خلال شبكات المعلومات باستخدام أجهزة الحاسب الآلى والتنسيق معها لإجراء التحريات وأعمال الضبط فى تلك الجرائم وفقاً للقواعد واللوائح والتعليمات المنظمة لذلك[1].

* اعداد البحوث الفنية والقانونية فى مجال مكافحة جرائم الحاسبات وشبكات المعلومات بالتنسيق مع الأجهزة المختصة من داخل الوزارة أو خارجها وفقاً للتعليمات المنظمة لذلك.

---

[1] قضت محكمة النقض بأنه: لما كان الحكم المطعون فيه قد عرض للدفع ببطلان الإذن لابتنائه على تحريات غير جدية واطرحه فى قوله : " .... وحيث إنه عن الدفع ببطلان إذن النيابة العامة لابتنائه على تحريات غير جدية - منعدمة – فمردود بأن المحكمة تطمئن إلى التحريات التي أُجريت بمعرفة النقيب/ .... الضابط بالإدارة العامة لمكافحة المخدرات لأنها تحريات واضحة وصريحة تضمنت بيانات كافية عن المتهم ومن ثم تكون تحريات جدية ومسوغة لإصدار الإذن ويكون الدفع غير سديد وتطرحه المحكمة .... " . لما كان ذلك ، وكان من المقرر أن تقدير جدية التحريات وكفايتها لإصدار إذن التفتيش هو من المسائل الموضوعية التي يوكل الأمر فيها إلى سلطة التحقيق تحت إشراف محكمة الموضوع ، وكانت المحكمة قد اقتنعت بجدية الاستدلالات التي بُني عليها إذن التفتيش وكفايتها لتسويغ إصداره وأقرت النيابة على تصرفها فى هذا الشأن ؛ فإنه لا معقب عليها فيما ارتأته لتعلقه بالموضوع لا بالقانون ، ولما كانت المحكمة قد سوغت الأمر بالتفتيش وردت على الدفع ببطلانه لعدم جدية التحريات رداً كافياً وسائغاً ، وكان ضعف قوة إبصار الطاعن – إن صح قوله فى هذا الخصوص – لا يقدح بذاته فى جدية التحريات ؛ إذ ليس هناك ما يمنع من قيادته السيارة لمزاولة نشاطه الإجرامي مع وجود ضعف فى إبصاره ، وكان لا يعيب الإجراءات والتحريات أن تبقى شخصية المرشد غير معروفة وأن لا يفصح عنها رجل الضبط القضائي الذي اختاره لمعاونته فى مهنته ؛ فإن النعي على الحكم فى هذا الشأن لا يكون له محل. (الطعن رقم 43358 لسنة 85 جلسة 2018/1/17)، س 69، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

* إعداد أرشيف متكامل للمعلومات التى تخدم أعمال الإدارة فى مجال الحاسبات ونظم المعلومات وتحديثه أولاً بأول وفقاً للتعليمات المنظمة لذلك وبالتنسيق مع الأجهزة المختصة.

صدر القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات[1]، ونص فى المادة (5) منه على تحديد صفة مأمورى الضبط القضائى على النحو التالى: " يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلى الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم". وعليه فقد خول القانون صفة الضبطية القضائية للعاملين فى مجال الأمن المعلوماتى يصدر بهم قرار من وزير العدل بالاتفاق مع وزير الاتصالات والمعلومات. وحسناً فعل المشرع لسرعة ضبط الجريمة السيبرانية فى مهدها قبل اتمامها فى مرحلة الشروع أو محو أدلتها، فضلاً عن الجوانب الفنية المطلوبة.

وقد ارتكزت استراتيجية وزارة الداخلية فى مجال مكافحة جرائم الاعتداء على حقوق الملكية الفكرية منذ صدور القانون رقم (82) لسنة 2002 بحماية حقوق الملكية الفكرية على إتباع المنهج العلمى المدروس الذى اعتمد على عدة محاور تتوافق مع طبيعة الظروف الاقتصادية التى تمر بها البلاد والتى تتمثل فى تحرير التجارة والاتجاه نحو اقتصاديات السوق والمنافسة الحرة وخصخصة القطاع العام وأيضاً اتجاهات الحكومة نحو جذب استثمارات أجنبية وتشجيع القطاع الخاص وما يستتبع ذلك من حدة المنافسة بأشكالها المختلفة ومن أهم تلك المحاور ما يلى:

1- وجود إدارات أمنية متخصصة لمكافحة الجرائم المعلوماتية والاعتداء على حقوق الملكية الفكرية[2]، وهى:

---

[1] القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 2018/8/14.

[2] نظراً للأهمية البالغة لصناعة البرمجيات للاقتصاد القومى المصرى وضرورة الاهتمام بحمايتها، فقد إضطلعت وزارة الداخلية المصرية بدورها فى مجال حماية الملكية الفكرية بما لها من خبرات تواكب متطلبات العصر الحديث وذلك بالتنسيق مع باقى وزارات وهيئات الدولة المعنية بهذا الشأن فقامت بإنشاء جهاز شرطى متخصص لمكافحة جرائم التعدى على الملكية الفكرية تابعة لقطاع الأمن الاقتصادى. فقد أنشئ هذا الجهاز الشرطى المتخصص فى مكافحة جرائم المصنفات الفنية عام 1981 تنفيذاً لالتزامات مصر الدولية بحماية الملكية الفكرية ضمن إدارات الإدارة العامة لمباحث

التهرب من الضرائب والرسوم. وفى ظل اتفاقيات منظمة التجارة العالمية وتنامى الاهتمام الدولى بالملكية الفكرية تم رفعها لتصبح إدارة رئيسية مستقلة بمسمى إدارة مكافحة جرائم المصنفات الفنية والمطبوعات عام 1996. وتتويجاً لاهتمام الوزارة المتنامى بالملكية الفكرية تم رفعها إلى مستوى إدارة عامة عام 2005 بمسماها الحالى وزيادة اختصاصاتها لتشمل التنسيق لحماية الملكية الفكرية بكافة صورها. وتعمل الإدارة على حماية حق المؤلف والحقوق المجاورة داخل حدود جمهورية مصر العربية بمكافحة كافة صور التعدى عن طريق ضبطها والحد من ارتكابها وذلك فى ضوء القوانين المنظمة. كما تختص الإدارة بالتنسيق بين أجهزة وزارة الداخلية العاملة فى هذا المجال وباقى أجهزة الدولة الأخرى وكذا الأجهزة غير الحكومية. ومكافحة أى جريمة تعتمد على شقى المنع والضبط، و المنع ويقصد به منع ارتكاب الجريمة قبل وقوعها ويتنامى هنا دور منظمات المجتمع المدنى والأجهزة الإعلامية للتوعية بمخاطر القرصنة وآثارها السلبية على المجتمع وعلى الأفراد بحد سواء. و الضبط ويقصد به كشف جوانب الجريمة عقب ارتكابها وضبط مرتكبيها واتخاذ الإجراءات القانونية قبلهم ويعتمد فى هذا على الأجهزة الأمنية والأجهزة القضائية بمعاونة منظمات المجتمع المدنى.

و خطة الإدارة فى مجال المنع من خلال:

1- التوعية المستمرة بالآثار السلبية لانتشار القرصنة على حق المؤلف اجتماعياً واقتصادياً على الفرد والمجتمع ككل عن طريق المشاركة بالمؤتمرات والندوات للتعريف بخطورة انتشار النسخ والتقليد والعقوبات التى توقع على المخالف لتحقيق الردع.

2- تنشيط دور منظمات المجتمع المدنى فى التوعية العامة بخطورة القرصنة.

3- المرور اليومى على أماكن تداول المصنفات سواء التقليدية أو المستحدثة للتأكد من قانونيتها.

وخطة الإدارة فى مجال الضبط من خلال:

1- سرعة فحص الشكاوى والبلاغات التى ترد للإدارة من أصحاب الحقوق أو المواطنين واتخاذ الإجراءات القانونية اللازمة لتحقيق الحماية.

2- توفير مصادر المعلومات بين أوساط العاملين فى هذا المجال للوقوف على الأنشطة الغير المشروعة وضبطها.

3- تبادل المعلومات بين الإدارة وفروعها الجغرافية لسرعة تحديد الجناة.

4- متابعة أماكن تداول المصنفات سواء التقليدية أو عبر شبكة الإنترنت للوقوف على المخالف منها وضبطه.

القوانين التى تستند إلها الإدارة خلال قيامها بدورها:

1- القانون رقم 20 لسنة 1936 وتعديلاته – الخاص بالمطبوعات.

2- القانون رقم 430 لسنة 1955 المعدل بالقانون رقم 38 لسنة 1992 الخاص بأحكام الرقابة على المصنفات الفنية.

3- القانون رقم 102 لسنة 1985 الخاص بتنظيم طباعة المصحف الشريف والأحاديث النبوية.

4- القانون رقم 82 لسنة 2002 بشأن حماية حقوق الملكية الفكرية "الكتاب الثالث الخاص بحماية حق المؤلف والحقوق المجاورة".

5- بعض مواد قانون العقوبات المصرى.

6- بعض القوانين الخاصة ذات الصلة مثل قانون تنظيم التوقيع الإلكترونى، وقانون تنظيم الاتصالات، وقانون الطفل، وقانون المحاكم الاقتصادية.

7- القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

الجهات التى تتعامل معها الإدارة خلال قيامها بدورها:

أولاً: الجهات الشرطية:

1- الإدارة العامة لشرطة التموين والتجارة المختصة بحماية العلامات التجارية والنماذج الصناعية وبراءات الإختراع ونماذج المنفعة.

أ- الإدارة العامــة للمعلومــات والتوثيــق: (وتتبعهــا إدارة مكافحــة جـرائم الحاسـبات وشبكات المعلومات): سبق عرض اختصاصاتها.

ب- الإدارة العامــة للمصـنفات الفنيــة وحمايــة حقـوق الملكيــة الفكريــة: وتـنهض بالاختصاصات التالية:

* مكافحة الجرائم التى تستغل المصنفات الفنية أو المطبوعات بهدف التأثير فى الرأى العام وبناء اتجاهاته بما يمس الأمن القومى أو يخرج عن الإطار القانونى سواء من الناحية السياسية أو الجنائية وذلك وفقاً للقوانين واللوائح المنظمة لذلك.
* وضع خطة لحماية المصنفات بكافة صورها بما يحقق حماية حقوق الملكية الفكرية (حق المؤلف والحقوق المجاورة) ومتابعة تنفيذها بالتنسيق مع الجهات المعنية سواء داخل الوزارة أو خارجها وفقاً للقوانين واللوائح والقرارات المنظمة لذلك.
* وضع خطة للاتصال والتنسيق مع الجهات سواء داخل الوزارة أو خارجها لحماية كافة صور حقوق الملكية الفكرية وفقاً للقوانين واللوائح والقرارات المنظمة لذلك.
* تنفيذ الاتفاقيات الدولية التى تنضم إليها جمهورية مصر العربية فى مجال حماية المصنفات وحقوق الملكية الفكرية ومتابعة تنفيذ التعهدات الناشئة عنها بالتنسيق مع الأجهزة المعنية سواء داخل الوزارة أو خارجها.

2- الإدارة العامة لشرطة المسطحات المائية التي تختص بحماية الأصناف النباتية

3- الإدارة العامــة للمعلومـات والتوثيـق "إدارة مكافحــة جـرائم الحاسـبات وشـبكات المعلومـات" والمختصـة بمتابعـة تنفيذ القـانون رقم 82 لسنه 2002 والقـانون رقم 175 لسنة 2018وغيره من القوانين ذات الصلة والمتعلقة بجرائم الشبكة الدولية للمعلومات "الإنترنت".

4- الإدارة العامـة للمصـنفات الفنيـة وحمايـة حقـوق الملكيـة الفكريـة والمختصـة بمتابعـة تنفيذ القـانون رقـم 82 لسـنه 2002 بشـأن حمايـة حقـوق الملكيـة الفكريـة والقـانون رقـم 175 لسـنة 2018 بشـأن مكافحة جرائم تقنية المعلومات.

ثانيا: الجهات غير الشرطية:

* جهاز نقطة الاتصال لحقوق الملكية الفكرية
* مكتب حماية حق المؤلف بوزارة الثقافة
* مكتـب حمايـة حـق المؤلـف بالهيئـة العامـة لتنميـة صـناعة تكنولوجيـا المعلومـات التـابع لـوزارة الاتصالات.
* مكتب حماية حق المؤلف بإتحاد الإذاعة والتليفزيون التابع لوزارة الإعلام.
* الإدارة العامة للبحوث والترجمة بالأزهر الشريف.
* المجلس الأعلى للصحافة
* المجلس الأعلى للجامعات
* جهاز المطبوعات
* مصلحة العلامات التجارية
* مكتب براءات الإختراع المصرى بأكاديمية البحث العلمى- وزارة البحث العلمى.
* مركز حماية الأصناف النباتية بوزارة الزراعة
* مصلحة الجمارك .... للمزيد أ/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، أبريل 2009، صـ 180 وما بعدها.

* اتخاذ الإجراءات التى تحقق السيطرة على منافذ البلاد البحرية والجوية والبرية لمنع المصنفات أو المطبوعات التى تستغل فى مجالات الأنشطة الضارة سياسياً أو جنائياً من دخول البلاد وذلك وفقاً للقوانين والقرارات المنظمة لذلك وبالتنسيق مع الأجهزة الأمنية المعنية.
* تلقى الشكاوى التى يقدمها أصحاب المصلحة (ذوى الشأن) أو التى تحال إليها فى مجال حقوق الملكية الفكرية وإخطار أجهزة الوزارة المعنية بها – كل فيما يخصه – ومتابعة نتائج فحصها وما اتخذ بشأنها من إجراءات قانونية وإدارية.
* متابعة التطور العلمى والتكنولوجى فى مجال المصنفات خاصة الحاسبات والأقمار الصناعية لحماية الأمن القومى والنظام العام والآداب وحقوق الملكية الفكرية من إساءة استخداماتها.
* تنسيق جهود الأجهزة العاملة فى مجال المصنفات وحماية حقوق الملكية الفكرية التى تشرف عليها الإدارة العامة فنياً ومتابعتها وتوجيهها وتقديم الدعم الفنى اللازم لها بما يمكنها من النهوض باختصاصاتها فى عمل الإدارة العامة بالتنسيق مع الأجهزة المعنية.

2- المكافحة الميدانية:

مما لا شك فيه أن أهم عناصر مكافحة الجريمة بوجه عام هى المكافحة الميدانية المستمرة وذلك من خلال القضايا التى يتم ضبطها بصفة مستمرة[1]، وما يتخذ بشأنها بعد ذلك من إجراءات قانونية وقضائية وفى هذا المجال تقوم إدارات المكافحة بما يلى:
* تكثيف الحملات المستمرة التى غالباً ما تكون مفاجئة وتتسم بالسرية لتحقيق أفضل نتائج حيث يتم الإعداد الجيد والمسبق لها وكذلك تنظيم إدارة الحملات المشتركة المكبرة والتى تتم بالاشتراك مع الفروع الجغرافية التابعة للإدارة المعنية بالمحافظات.
* تلقى شكاوى وبلاغات المواطنين وأصحاب حقوق الملكية الفكرية التى تم الاعتداء عليها وفحصها واتخاذ الإجراءات القانونية حيالها على وجه السرعة بهدف توفير الحماية اللازمة لبرامج الحاسب الآلى والتى تتمتع بالحماية القانونية.

---

[1] وقد أسفرت الجهود المستمرة للإدارة عن ضبط الآتي:
* الآلاف من الأسطوانات المقلدة لبرامج إحدى شركات البرمجيات العالمية تقليداً يضاهي الأصلي وموضوع عليها العلامة التجارية بطريقة توهم متداوليها أنها أصليه وقدرت المضبوطات في تلك القضية بملايين الدولارات.
* العديد من قضايا التعدي على البرمجيات بمحلات السيبر كافية وكذا بيع الأسطوانات المنسوخة حيث يبلغ عدد القضايا فى الشهر الواحد حوالى 139 قضية.
* العديد من شركات الكمبيوتر لقيامها بتحميل الأجهزة المباعة لعملائها ببرامج منسوخة مقابل مبالغ مالية زهيدة منها ضبط فرعين لإحدى كبرى الشركات فى ذات التوقيت بالقاهرة والإسكندرية حيث تم ضبط عدد 15 جهاز كمبيوتر محمل ببرامج مقلدة ومنسوخة وعدد كبير من الأسطوانات المقلدة المعدة للبيع وكذا ضبط عدد كبير من الأسطوانات المقلدة تقليد جيد يجعلها تشبه الأسطوانات الأصلية وكذا أسطوانات تحوي برامج CRAC " لتنشيط البرامج المنسوخة وإعطائها صلاحية البرامج الأصلية دون موافقة الشركات المنتجة لها تم برمجته بمعرفة المتهم المضبوط وهو أول برنامج CRAC مصري يضبط حتي الآن وقد تم اتخاذ الإجراءات القانونية تجاه المتهمين والعرض على النيابة فى حينه وصدرت فيها أحكام قضائية رادعة.... للمزيد: أ/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، مرجع سابق، ص 180وما بعدها.

* رصد الأماكن المشهور عنها بيع وتداول البرامج المقلدة والتى تمثلت فى الآونة الأخيرة فى مناطق معينة أو شوارع تجارية هامة أو تجمع محلات (مولات الكمبيوتر) والتى تخصصت فى بيع نوع معين من السلع حيث ترتبط غالبية السلع المقلدة بتلك الأماكن وتعد أيضاً مكاناً لإلتقاء إرادتى الشراء والبيع لدى المواطنين[1].

آثار الجهود المصرية فى مكافحة الجرائم السيبرانية:

وقد ظهرت آثار جهود وزارة الداخلية فى مجال مكافحة جرائم القرصنة المعلوماتية، وتتمثل فيما يلى:

1. زيادة معدلات الاستثمار فى صناعة تكنولوجيا المعلومات لتصل إلى 1.17 مليار دولار فى عام 2007.

2. إنخفاض معدلات القرصنة على البرمجيات وفق دراسات مؤسسة IDC فى مصر لتصل إلى 60 بالمائة عام 2007 بعد أن كانت 80 بالمائة عام 2000 كما رفعت الحكومة الأمريكية مصر من قائمة الدولة الأولي بالمراقبة فى مجال القرصنة على البرمجيات.

3. زيادة معدلات التصدير للبرمجيات المصرية لتصل إلى 150 مليون دولار عام 2007 وفق دراسة أجرتها مؤسسة ICD[2].

4- كما تسعى غرفة الاتصالات وتكنولوجيا المعلومات باتحاد الصناعات بمصر خلال الخمس سنوات القادمة لزيادة حجم الصادرات المصرية من برامج السوفت وير إلى مليار دولار، وزيادة صادرات الـ IT المصرى خلال أربع سنوات إلى 500 مليون دولار[3].

رابعاً

تفعيل الدور الأمني الوقائى لجهاز الشرطة فى مكافحة الجرائم السيبرانية

إن تفعيل دور الدور الأمني الوقائى لجهاز الشرطة فى مكافحة الجريمة الإلكترونية، يتطلب ما يلى:

1- تجنيد المصادر من المتخصصين فى مجال الحاسب الآلى وآلات التقنية الحديثة، وذلك للوقوف على أحدث البرامج " Soft Ware " ومعرفة استخداماتها وكذا أحدث ماكينات التصوير بألوان وطابعات الليزر.

2- حصر مقاهي الإنترنت " Net Coffee " وإلزام أصحاب تلك المقاهي بعمل دفاتر تدون بها بيانات المترددين علىه من واقع إثبات الشخصية الرسمي.

---

(1) أ/ مجدى فؤاد، الجريمة المعلوماتية وحماية حقوق الملكية الفكرية، مرجع سابق، صـ 21 وما بعدها.

(2) أ/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، مرجع سابق، صـ 185وما بعدها.

(3) أ/ وليد جاد، رئيس غرفة الاتصالات وتكنولوجيا المعلومات باتحاد الصناعات، بوابة الأهرام، 2018/7/2، متاح على: gate.ahram.org.eg/news/1976109 -

3- مداومة المرور على مقاهي الإنترنت والعمل على تجنيد أصحابها ومناقشتهم عن الأشخاص الذين يترددون باستمرار لاستخدام الإنترنت وممن لهم ميول فى تصميم البرامج أكثر من تشغيلها، والمتابعة والملاحظة لكل ما يدور بتلك المقاهي ومعرفة من الذين يقومون بأعمال القرصنة على مواقع الإنترنت والبريد الإلكتروني، وحصرهم فى سرية .

4- مداومة المرور على شركات تقديم خدمات الإنترنت والعمل على تجنيد أحد المصادر بها للإبلاغ عن أي شئ غير عادي يحدث.

5- بالنسبة للشركات والمؤسسات والبنوك التى بها شبكات حاسب آلى، يجب العمل على الربط مع المديرين بها ومناقشتهم عن مدى متابعتهم للموظفين بهذه الشركات والبنوك، وعما إذا كانت هناك محاولات اختراق للشبكات فى هذه المؤسسات.

6- الاهتمام بالدراسات العلمية لرجال الأمن لعلوم الحاسب الآلى حتي يواكبوا بفكرهم التطورات السريعة فى هذا المجال مما يعطيهم ويمنحهم الثقة بالنفس ويدفعهم المزيد من طلب العلم فى هذا الحقل الخصيب[1].

7- تدريب وتأهيل مأموري الضبط وسلطة التحقيق والقضاء المختصين بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة فى ارتكاب الجريمة، وفيما يتعلق بطرق الكشف عنها، والقرائن والدلائل[2] والأدلة المستحدثة فى مجال إثباتها وكيفية معاينتها وفحصها فنياً، وتدريب القضاة كذلك على معالجة هذا النوع من القضايا التى تحتاج إلى خبرات فنية عالية لملاءمة قبول هذا النوع من الأدلة فى الإثبات وتقديرها حتي يتمكن من الفصل فى القضايا المتعلقة بهذا النوع من الجرائم. وهذا يقتضي تنمية استعدادهم الخاص وتكوين مهارات فنية خاصة حتي تكون لديهم درجة من المعرفة الفنية مع حجم المتغيرات والتطورات المتلاحقة فى مجال جرائم تقنية المعلومات، مع تطوير أساليب البحث عن الأدلة وتقديمها وتقديرها لتواكب هذه التطورات ولا تتخلف عنها[1].

---

(1) أ/ مروان عادل عبده، الدور الأمني فى مواجهة صور الجريمة المعلوماتية، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، أبريل 2009، صـ20.

(2) ويقصد بالدلائل الكافية "وجود شبهات أو مظاهر تفيد الاتهام ولا ترقى إلى مرتبة الأدلة". ولمأمور الضبط القضائى تقدير الدلائل الكافية تحت رقابة النيابة العامة ومحكمة الموضوع، فالبلاغ عن الجريمة لا يعتبر وحده من الدلائل الكافية. ويشترط أن تكون الدلائل الكافية غير معروفة لمأمورى الضبط القضائى سلفاً، فإذا كانت هذه الدلائل نتيجة تحريات مسبقة فعلي مأمور الضبط القضائى اتخاذ الطريق الطبيعى للقبض على المتهم، فيجب عليه عرض الأمر على النيابة العامة، وذلك لاستصدار أمر بالقبض عليه فإذا توافرت شروط هذه المادة جاز اتخاذ الاجراءات التحفظية المناسبة. ويقصد بالاجراءات التحفظية "تلك الإجراءات التى تحول دون هرب المتهم أو تمنعه من إتلاف آلة الاتهام"، ومثال على ذلك استيقاف المتهم أو اصطحابه إلى مركز الشرطه أو تجريده من السلاح الذى يحمله. ويجب على مأمور الضبط القضائى أن يطلب من النيابة العامة إصدار أمر بالقبض على المتهم الذى اتخذت ضده الإجراءات التحفظية.... د/ كمال عبدالرشيد، التحفظ على الاشخاص، رسالة دكتوراه، أكاديمية الشرطة، 1989، ص 224، د/ عمر السعيد رمضان، مبادىء قانون الإجراءات الجنائية، الجزء الأول، 1993، ص311، د/ محمود نجيب حسنى، الدستور والقانون الجنائى، دار النهضة العربية، 1992، ص 86.... مشار اليه لدى: د/ طلعت محمد الدسوقى الشهاوى، المسئولية الجنائية عن جرائم الاتصالات- دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2016، ص 298.

(1) د/ عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، مرجع سابق، صـ 238 وما بعدها.

8- استخدام تقنيات عالية لرصد العناصر الإجرامية التى تستخدم شبكة المعلوماتية للنصب على ضحاياها[2].

خامساً

مدى جواز الاستعانة بمحام أثناء الاستدلالات

يهدف الاستدلال إلى كشف الحقيقة، ولذلك فهو من مراحل إثبات الدعوى. وفى هذا الشأن يشترك الاستدلال مع التحقيق الابتدائى، ولكنهما يختلفان من حيث الموضوع فى الأمور التالية:

1- يهدف الاستدلال أساساً إلى جمع عناصر الإثبات اللازمة لتحضير التحقيق الابتدائى. نعم قد يقدم الاستدلال أدلة كافية فى مرحلته المبكرة مما يسمح للنيابة العامة برفع الدعوى الجنائية إلى المحكمة بناء على هذه الأدلة، ولكنه أساساً لا يهدف إلى جمع هذه الأدلة، فذلك متروك لسلطة التحقيق.

2- لا تنطوى إجراءات الاستدلال بصفة أصلية على أى مساس بالحرية، فذلك أمر قاصر على حالة التلبس فقط.هذا بخلاف الحال فى إجراءات التحقيق الابتدائى.

3- لا يخضع الاستدلال والتحقيق إلى القواعد نفسها فكل منها يخضع لقواعد تحكمه تختلف باختلاف طبيعته من حيث المساس بالحرية والهدف منها[1].

كما يتميز الاستدلال عادة بتغيب الدفاع، بحسب أن المشتبه فيه لم يتحدد اتهامه بعد. وقد انتقد هذا الوضع فى مصر وفرنسا. وقد نص قانون المحاماه المصرى على حق المحامين فى الحضور عن ذوى الشأن أمام دوائر الشرطة (المادة 3أ)، ونص على أنه يجب على دوائر الشرطة أن تقدم للمحام التسهيلات التى يقتضيها القيام بواجبه، ويمكن من الاطلاع على الأوراق والحصول على البيانات وحضور التحقيق مع موكله (المادة 52 من قانون المحاماه). كما نص القانون الإيطالى الصادر فى

---

[2] وقد نجحت وزارت الداخلية فى ضبط أخطر عصابة إلكترونية فى يوليو 2014، حيث احترفت تلك العصابة النصب على المواطنين فى مختلف دول العالم ولكن انتهى بهم الأمر إلى إلقاء القبض عليهم فى مصر بعد رصدهم بناء على البلاغ المقدم من أحد ضحاياهم، موضحاً أن الإدارة تلقت بلاغاً من مذيعة، بتلقيها رسائل إلكترونية على بريدها الشخصى من عناوين بريدية مختلفة من شخص مجهول، وأنه قام بالنصب عليها والإستيلاء على 50 ألف دولار أمريكى مقابل زواجها من ضابط بالجيش الأمريكى، وأكدت فى بلاغها أنها قامت بتحويل المبلغ على الحساب الخاص لذلك المجهول، حتى تلقت اتصالاً هاتفياً من شخص آخر زعم أنه صديقه وقام بتحديد موعد لمقابلتها ليتسلم منها مبلغ 50 ألف دولار أخرى لإنهاء إجراءات الزواج بالضابط الأمريكى، وهنا جاء دور إدارة مكافحة جرائم الحاسبات والشبكات "مباحث الإنترنت"، حيث قامت برصد البريد الإلكترونى المستخدم من قبل هؤلاء المحتالين وتمكنت من تحديد أماكنهم وضبطهم..... تصريحات أ/ محمد أبو زيد - مدير مباحث الإنترنت - حول رصد مرتكبى الجرائم الإلكترونية، جريدة الأهرام اليومى، يوليو 2014، متاح على:

- Available At: http://digital.ahram.org.eg/articles.aspx?serial=1642232=11472

[1] د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص 699.

ديسمبر سنة 1969 على حق كل شخص تستدعيه الشرطه لسماع أقواله فى الاستعانة بمحام[2].

وليس لمأمور الضبط القضائى استجواب المشتبه فيه، بل يستوضح الأمر منه بالسؤال لا الاستجواب، فلا يجوز توجيه الأسئلة التفصيلية التى تهدف إلى اثبات التهمة أو محاولة الايقاع به وإلا اعتبر استجواباً، وهو أمر محظور على مأمور الضبط القضائى ولو بطريق الإنتداب للتحقيق[3].

كما لا يوجب القانون أن يتولى مأمور الضبط القضائى بنفسه التحريات أو أن يكون على معرفة سابقة بالمتحرى عنه، بل له أن يستعين فيما يجريه من تحريات بمعاونيه من رجال السلطه العامة والمرشدين السريين ومن يتولون إبلاغه عما وقع بالفعل من جرائم ما دام أنه اقتنع شخصياً بصحة ما نقلوه إليه وبصدق ما تلقاه من معلومات[4]. ونظلراً لخطورة التحريات وتأثيرها فى تقدير سلطة التحقيق عند مباشرة إجراءاتها، فإنه إذا ثبت أن التحريات كانت غير صادقة فللنائب العام أن يطلب من الجهة المختصة النظر فى أمر كل من تقع منه مخالفة لواجب وظيفته أو تقصيره فى عمله، وله أن يطلب رفع الدعوى التأديبية عليه، وهذا كله لا يمنع من رفع الدعوى الجنائية (المادة 2/22 إجراءات)[5].

المبحث الثاني
دور الشرطة فى تعقب وملاحقة مرتكبي الجرائم السيبرانية المستحدثة
وتحقيق الأمن المعلوماتى

تمهيد:

انه يتوقف حسن أداء آليات العدالة الجنائية سواء فى مجال منع الجريمة بصفة عامة، أو فى مجال البحث عنها وضبط مرتكبيها على الدور الذى يقوم به مأمور الضبط فى مكافحة الجريمة والإجرام، ولكونه يعد أو هكذا افترض المشرع، خط الدفاع الأول ضد الجريمة، إذ أن رجال الضبط القضائى أول من ينتقلون إلى

(2) د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع السابق، ص 717.
(3) نقض 24 مارس 1974، مجموعة أحكام محكمة النقض، س 25، ق 69، ص 317.
(4) نقض 29 ديسمبر سنة 1969، مجموعة الاحكام، س 20، ص 1479. 8 إبريل سنة 1979، س 30، ق 96، ص 453.
(5) د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص 700 وما بعدها.

مسرح الجريمة[1]، وفيه يقومون بالتحفظ على الأدلة وجمع المعلومات لعرضها على سلطة التحقيق، وقد يستمعون إلى أقوال المتهم أو المجنى عليه وشهادة الشهود والتى قد لا تتيح الظروف سماعهم مرة أخرى نظراً لوفاة أحدهم أو غير ذلك، هذا مع ضرورة وجود رقابة قضائية على تلك الاجراءات السابقة واللاحقة صوناً للحريات الشخصية والخصوصية المعلوماتية للأفراد[2]، وخاصة فى الدعاوى الجنائية التى يتم تحريكها بناء على إجراءات جمع الاستدلالات كما هو الحال فى الجنح والمخالفات والتى لم يسبقها تحقيق ابتدائى[3].

كما قضت محكمة النقض بأحقية محكمة الموضوع فى الرقابة والإشراف على تقدير سلطة التحقيق فى إذن التفتيش والضبط[1].

---

(1) من المقرر أن الدفع بعدم معقولية تصوير الواقعة وتلفيق الاتهام وكيديته وبعدم الوجود على مسرح الجريمة لا يعدو أن يكون من أوجه الدفاع الموضوعية التي لا تستوجب رداً صريحاً ، بل الرد يستفاد من أدلة الثبوت التي أوردها الحكم ، فإن ما ينعاه الطاعن فى هذا الخصوص لا يكون مقبولاً . (الطعن رقم 10621 لسنة 82 جلسة 2014/5/14، س 65)، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

(2) قضت محكمة النقض بأنه: لما كان لا يعيب الحكم إغفال ما تضمنته التحريات من متهمين آخرين أو عن صدور إذن بتفتيشهم ، لأنه ما دام هذا الجزء من التحريات أو من الإذن لا علاقة له بموضوع الدعوى المطروحة فإنه ليس هناك داع يقتضي إثبات الحكم له فى مدوناته، إذ أن شمول التحريات لأكثر من شخص فى بلاد مختلفة وإجرًاء التفتيش أثناء حملة تفتيشية لا يكشف بذاته عن عدم جدية التحريات لأنه لا يمس ذاتيتهما، ومن ثم فإن النعي علي الحكم فى هذا الصدد لا يكون له محل . (الطعن رقم 8426 لسنة 87 جلسة 2017/11/4)، س68، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

(3) د/ محمد كمال عبد السميع شاهين، الجوانب الإجرائية للجريمة الالكترونية فى مرحلة التحقيق الابتدائى – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2015، صـ 151 وما بعدها.

(1) حيث قضت محكمة النقض بأنه من حيث أن البين من مدونات الحكم المطعون فيه أنه حصل على دفع الطاعن المبين بوجه النعى بقوله"ودفع الحاضر معه بعدم جدية التحريات وبطلان الإذن الذى بنى عليها لخلوها من وصف مسكن المتهم وبيان عمله لعدم ذكر رقم تسجيله بالمكتب أو أرقام القضايا السابق ضبطه فيها" ورد عليه فى قوله "وحيث أن الدفع بعدم جدية التحريات مردود عليه بأن السلطة القائمة على إصدار الإذن قد اطمأنت إليها فى حدود السلطة الممنوحة لها وأعطت إذنها بناءً على ذلك. وأن القانون لا يشترط شكلاً معيناً لإذن التفتيش فلا ينال من صحته خلوه من بيان اسم المأذون بتفتيشه كاملاً أو صفته أو صناعته أو محل إقامته أو الخطأ فى اسمه طالما أنه الشخص المقصود بالإذن". ومفاد ما تقدم أن المحكمة قد أسست رفضها للدفع ببطلان إذن التفتيش لعدم جدية التحريات التي بنى عليها مجرد اقتناع سلطة التحقيق بتوافر مسوغات إصدار هذا الأمر، لما كان ذلك، وكان الأصل فى القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة جناية أو جنحة" وترجحت نسبتها إلى متهم معين، وإن كان من الدلائل ما يكفى للتصدى لحرمة مسكنه أو لحريته الشخصية". وكان من المقرر أن تقدير جدية التحريات وكفايتها

تتميز الجرائم المعلوماتية بعدة صعاب تعوق أداء الأجهزة الشرطية مما جعل الأجهزة الشرطية تقوم بالتطوير فى أدائها وظائفها وهذه الصعاب تمثل حجر عثرة فى أداء العمل الشرطى مما استتبع ضرورة التعرض لها وكذلك لدور الأجهزة الشرطية ومدى التطور الذى ألحقته فى أداء عملها للتغلب على تلك الصعاب، وهذا ما يتضح من خلال السطور التالية:

وتتسم الجرائم المعلوماتية بمجموعة من الخصائص التى تؤدى إلى صعوبة التعامل معها وضبطها وهذه الصعاب قد تكون على المستوى الوطنى وقد تكون على المستوى الدولى وذلك وفقاً لما يلى:

1- الصعوبات على المستوى الوطنى:

تتعدد الصعوبات التى تواجه الدور الذى تقوم به الأجهزة الشرطية فى مكافحة الجرائم المعلوماتية على المستوى الوطنى، ومن أهم تلك الصعوبات ما يلى:

أ- عدم كفاية القوانين القائمة:

يقابل التطور فى المجال التكنولوجى سواء من ناحية الحياة العامة أو الخاصة واعتماد الجميع عليه فى سائر شئونهم وكذلك استغلال الجناة لتلك التقنية فى ارتكاب جرائمهم عدم التطور فى المجال التشريعى بذات الصورة التى تؤهل لإمكانية مكافحة تلك الصور الإجرامية المستحدثة مما يصيب الدور الشرطى بعدم المشروعية فى حالة مكافحة الكثير من تلك الجرائم. وبالتالى فإن القانون الجنائى بنصوصه الحالية لا يكفى لإمكانية مواجهة تلك الصور المستحدثة من الجرائم لتطلب غالبية النصوص الصفة المادية فى الشئ محل ارتكاب الجريمة مما يتنافى مع الطبيعة المعلوماتية وبالتالى تخرج تلك الصور من تحت طائلة العقاب.

ب- إحجام الكثير من الجهات عن التبليغ عن تلك الجرائم:

ويكون هذا الإحجام بهدف عدم الإساءة لطبيعة عمل المنشأة وبيان عجزها عن تحقيق الأمان الكافى للمعلومات وبالتالى لأصول الأموال التى تتعامل معها وقد يكون لذلك مردوده السئ لدى العملاء عن طريق لجوء الكثير منهم لسحب أموالهم مما يؤدى إلى إفلاس المشروع.

ج- سهولة القيام بإخفاء معالم الجريمة:

ويتمثل ذلك فى عدم معرفة مصدر مرتكب الفعل بحيث إذا تم ارتكاب الفعل وظهرت نتيجته بعد فترة زمنية مثل قيام شخص ما بزرع برنامج فيروس وقد يكتشف وجوده بعد قيامه بتحقيق آثاره التدميرية للمعلومات.

لتسويغ إصدار الإذن بالتفتيش موكول ابتداءاً إلى سلطة التحقيق التى أصدرته إلا أن تقديرها يخضع لرقابة وإشراف محكمة الموضوع، ومن ثم لا يكفى لطرح الدفع ببطلان إذن التفتيش لعدم جدية التحريات التى بنى عليها القول – كما انتهى الحكم المطعون فيه – باقتناع سلطة التحقيق التى أصدرته بجدية التحريات وإنما يتعين على المحكمة – أن تبدى رأيها فى عناصر التحريات السابقة على الإذن وأن تقول كلمتها فى كفايتها أو عدم كفايتها لتسويغ إصدار الإذن من سلطة التحقيق، وبذلك يكون هذا الحكم فوق خطئه فى تفسير القانون مشوباً بالقصور فى التسبيب" ....حكم محكم النقض 4 نوفمبر سنة 1992، الطعن رقم 486 لسنة 61ق، س43، ص2، غير منشور.

د- عدم توافر القدرات الفنية لمواجهة تلك الجرائم:

وتتمثل تلك القدرات فى الفريق المدرب لمواجهة هذه الجرائم وفى الأسلوب الذى يتبع فى تعقب تلك الجرائم وضبط مرتكبيها وكذلك فى الوسائل الفنية اللازمة لتعقب تلك الجرائم مثل البرامج الحديثة التى يجب أن تتوافر بصفة الاستمرار لاكتشاف أى تدخل غير مشروع على أنظمة الحاسبات الآلية ولعل ذلك يكون نتيجة إرتفاع أسعار تلك البرامج.

ه- عدم وجود دليل مادى واضح:

لأن الدليل المادى الذى قد يتوفر يكون عبارة عن أوراق محصلة من الطابعة من خلال الجهاز كالعملات الورقية المزيفة للشخص القائم بعملية التزوير والدليل هنا هو الورقة المالية المحصلة من الطابعة وليس ما يحويه الجهاز فى حد ذاته.

و- صعوبة الوصول إلى الدليل فى بعض الأحيان:

لأن الدليل وهو عبارة عن معلومات قد تحاط بوسائل فنية لحمايتها وتلك الوسائل قد تكون عائق أمام عملية البحث والتحرى والاطلاع علىها من قبل فريق البحث لأن الدليل ليس بالضرورة أن يكون أوراق نقدية مزيفة محصلة من الطابعة[1].

ز- وجود كم كبير من المعلومات يتعين فحصها:

يتطلب البحث عن معلومات تفيد فى كشف أدلة جريمة معينة البحث فى كم كبير من الملفات والبرامج المخزنة والتى قد يكون لها ارتباط بمعلومات خاصة بارتكاب الجريمة.

وفى غير ذلك من الأحوال يكون تتبع المعلومات داخل الجهاز دليل تسعى الجهات الأمنية لملاحقته أمر يتميز بكثير من الصعوبات تتمثل إما فى طبيعة المعلومات أو فى نقص الخبرة الفنية من قبل رجال الأمن فى ملاحقته لتلك الأدلة والتى يتطلب معه البحث استغراق فترة زمنية كبيرة تؤثر بالسلب على طبيعة عمل المنشأة.

2- الصعوبات على المستوى الدولى:

تعتبر الجرائم المعلوماتية صور حديثة من الجرائم العابرة للحدود الوطنية فى عالم ذابت فيه الفواصل وتلاشت الحدود مما جعل من السهولة ارتكاب الجرائم المعلوماتية ليس فقط على المستوى الوطنى بل وعلى المستوى الدولى، مما يتطلب البحث فى الصعوبات التى تعترض مكافحة تلك الجرائم وهذه الصعوبات يمكن تفصيلها وفقاً لما يلى:

أ- ليس هناك مفهوم عام مشترك بين الدول حتى الآن حول نماذج النشاط المكون للجريمة المعلوماتية.

---

[1] أ/ محمد عبد اللطيف فرج، مشكلات ملاحقة وتحقيق الجرائم المعلوماتية، مجلة مركز البحوث بأكاديمية الشرطة، العدد العاشر، 2000، صـ 144.

ب- اختلاف مفاهيم الجريمة لاختلاف الأنظمة القانونية وفلسفة النظم القانونية المختلفة.
ج- ليس هناك مفهوم عام حول تعريف القانون للنشاط الإجرامى المتعلق بهذا النوع من الجرائم.
د- عدم التناسق بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحرى والتحقيق فى الجرائم المتعلقة بالكمبيوتر.
هـ- نقص الخبرة لدى الشرطة وجهات الإدعاء والقضاء فى هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع المعلومات والأدلة عنها.
و- تعقد المشاكل القانونية والفنية الخاصة بتنفيذ نظام معلوماتى خارج حدود الدولة أو ضبط معلومات مخزنة فيه أو الأمر بتسلمها.
ز- عدم وجود معاهدات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولى أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة بجرائم الكمبيوتر وديناميكية وسرعة التحريات فيها[1].

ويتناول الباحث فيما يلى دور الشرطة فى المعاينة، والتفتيش، والضبط، فى مجال جرائم المعلوماتية، ثم يوضح الباحث حدود الدور الفنى للأجهزة الأمنية فى ملاحقة الجرائم المعلوماتية، كما يتناول الباحث دور الشرطة الأمريكية فى مواجهة الجرائم المعلوماتية، ثم يعقد الباحث مقارنة بين أسلوب عمل أجهزتى الشرطة المصرية والأمريكية فى مواجهة الجرائم المعلوماتية، وذلك على التفصيل التالى:

أولاً
دور الشرطة فى معاينة مسرح الجرائم السيبرانية

المعاينة هي إثبات لحالة الأماكن والأشخاص وكل ما يفيد فى كشف الحقيقة كما يعرفها البعض بأنها: "رؤية بالعين لمكان أو شخص أو شئ لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"[1]. والمعاينة أياً كان التعريف الموضوع لها تتطلب أن ينتقل مأمور الضبط القضائى إلى مكان ما لمباشرتها وذلك لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد فى الجريمة محل الاجراء.

وفيما يتعلق بالجنايات غير المتلبس بها والجنح عموماً، فالانتقال للمعاينة متروك لتقدير النيابة العامة وفقاً لظروف التحقيق وما تراه ضرورياً لجمع الأدلة. وللمحكمة القيام بإجراء معاينة المكان الجريمة الذى وقعت فيه الجريمة، إذا ما رأت لأن معاينة سلطة التحقيق أو سلطة جمع الاستدلالات غير كافية لاستخلاص دليل

---

[1] د/ أيمن عبد الحفظ عبد الحميد سليمان، الدور الفنى لأجهزة الشرطة فى مواجهة الإجرام المعلوماتى، ندوة لمواجهة الجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، 7 أبريل 2009، صـ 4 وما بعدها.

[1] د/ محمد ذكى أبو عامر، الإجراءات الجنائية، منشأة دار المعارف، الإسكندرية، 1997، صـ 233.

سائغ لإثبات الجريمة[2]. وفى كل الأحوال فالأدلة من معاينة المكان الجريمة تخضع كسائر الأدلة الأخرى التى تطرح فى الجلسة – لتقدير قاضى الموضوع طبقاً لمبدأ حرية الإثبات، فإن اطمأن استند إليها فى حكمه، وإذا لم يطمئن يقوم بطرحها جانباً دون معقب أو رقابة عليه من محكمة النقض[3].

وتكمن أهمية المعاينة وفعاليتها فى التيسير على سلطة التحقيق فيما إذا تم المبادرة إلى إجراؤها كلما سنحت الفرصة لذلك على وجه السرعة, ذلك لأن من شأن المبادرة بالانتقال إلى مكان الجريمة لمعاينته هو ما قد يوجد به من أشخاص أو أشياء يساعد على جمع الأدلة المترتبة على ارتكاب الجاني لجريمته قبل أن تمتد إليها يد العبث أو قبل زوال معالمها, كما من شأن السرعة فى اتخاذ هذا الاجراء أن يمنح مأمور الضبط الفرصة لمشاهدة المسرح الذي وقعت فيه الجريمة بنفسه وبالتالى يتمكن من تقييم أقوال الشهود وغيرهم حول الجريمة وكيفية ارتكابها ومدى وضوح الرؤية وغيرها من الأمور الفنية المتطلبة فى التحقيق.

والمعاينة قد تتم فى مكان عام أو فى مكان خاص حيث لا تتطلب المعاينة فى الأماكن العامة إلى إذن أو ندب سلطة التحقيق بإجرائها طالما كان من حق مأموري الضبط دخولها أو التواجد فيها, أما إذا كان محل المعاينة مكان خاص كمنزل مثلاً فلا بد لصحتها أما رضا صاحب المكان أو وجود إذن مسبق من سلطة بإجرائها.

ويجب على مأموري الضبط أثناء قيامه بالمعاينة ضبط كل ما استعمل فى ارتكاب الجريمة أو نتج عنها كذلك وضع الأختام فى الأماكن التى أجريت فيها المعاينة متي وجد فيها آثار أو أشياء تفيد فى كشف الحقيقة ويجوز لهم تعيين حراس على هذه الأماكن مع ضرورة إخطار النيابة بهذه الإجراءات مع اعتبار هذه

---

(2) قضت محكمة النقض بأنه: خلو الأوراق من الأدلة سوى من الدليل المستمد من اجراء التفتيش الباطل وشهادة من أجراه، يتعين الحكم بالبراءة. (الطعن رقم 3367 لسنة 87 جلسة 2017/5/24)، س 68، دائرة جنائى،

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

(3) د/ مفتاح بوبكر المطردى، المستشار بالمحكمة العليا الليبية، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا فى الدول العربية بجمهورية السودان المنعقد فى الفترة من 23 – 25 /9/ 2012، صـ 11.

الإجراءات صحيحة قانوناً حتى ولو تمت فى غير حضور المتهم أو المشتبه فيه بالرغم من أن العمل قد جرى على منع المتهم من الحضور.

التعريف المعاصر لمسرح الجريمة:

من الطبيعي أن ترتكب الجريمة فى مكان معين, هذا المكان يحوي فى الواقع التصرفات التى تطرأ بداخلة أثناء ارتكاب العمل, وهذه التصرفات تمثل سلوكاً إيجابياً بالحركة الناتجة عن الفعل, والتى تتخلف عنها آثار, وتترك ملاحظات ذات أهمية فى كشف غموض الجريمة, وهذا المكان هو الذى يطلق عليه اصطلاح "مسرح الجريمة". فمن البديهي أن يكون لكل جريمة مكان قد وقعت فيه وهو بهذا المفهوم قد يكون مكان واحد أو عدة أماكن متصلة أو متباعدة تكون فى مجملها "مسرح الجريمة" فكل مكان يستدل منه على أثر مرتبط بالجريمة محل البحث يكون جزء من مسرحه. وقد أجمع الخبراء فى مجال البحث الجنائي بمختلف دول العالم على أن مسرح الجريمة أو مكان الجريمة هو مستودع سرها, لإحتوائه على الآثار المادية, والأدلة الجنائية التى تؤدي إلى كشف الحقيقة مما دفع البعض منهم إلى التوسع فى تحديد نطاق مكان ارتكاب الجريمة فامتد به إلى الأماكن المجاورة من طرقات وأماكن عامة للبحث عن الآثار المادية المتعلقة بالحادث[1].

[1] قضت محكمة النقض بأنه: لما كان ما أثاره كل من الطاعنتين الأولى والثالثة من عدم ضبطهما على مسرح الجريمة لا يعدو أن يكون من أوجه الدفاع الموضوعية التى لا تستوجب رداً صريحاً من الحكم بل الرد يستفاد من أدلة الثبوت التى أوردها الحكم ، فإن النعى على الحكم فى هذا الشأن يكون فى غير محله . (الطعن رقم 3225 لسنة 81 جلسة 2012/11/20، س 63 ص 742 ق 132)، دائرة جنائى.

- كما قضت محكمة النقض بأنه: لما كان الحكم قد عرض لدفاع الطاعنة القائم على عدم وجودها على مسرح الجريمة وطرحه فى قوله : "وحيث إنه عن قالة الدفاع بأن المتهمة لم تكن على مسرح الجريمة مردود عليه بأنه لايشترط فى جريمة القتل بالسم وجود المتهمة على مسرح الجريمة وقت تناول المجنى عليه السم بعد وضعه فى مشروب الشاى، وتعتبر المتهمة فاعلة أصلية فى الجريمة لأنها اشترت المادة السامة من إحدى صيدليات القرية حسبما اعترفت بالتحقيقات وأعطتها لابنتها ..... مستغلة صغر سنها فهى لم تتجاوز الخامسة عشر عاماً وقت الواقعة طالبة منها وضع محتوى الكيس البلاستيك الأبيض فى أى شىء يتناوله المجنى عليه بعد إفهامها بأن محتوى الكيس يؤدى إلى ربط المودة والمحبة بينها وبين والدها المجنى عليه فالمتهمة فاعلة أصلية ". وكان ما أورده الحكم كافياً وسائغاً لإطراح دفاع الطاعنة حيث بين دورها كفاعلة أصلية للجريمة خططت ودبرت لها ونفذت ما استقرت عليه بأن أعدت المادة السامة وجعلتها فى متناول المجنى عليه فتمت

مدى صلاحية مسرح جرائم الحاسب الآلى لمعاينته:

يجب التفرقة بين الجرائم الواقعة على المكونات المادية للحاسب والجرائم الواقعة على المكونات المعنوية أو بواسطتها.

الحالة الأولي : الجرائم الواقعة على المكونات المادية للحاسب:

وهذه الجرائم مثل جرائم الاعتداء على أشرطة الحاسب وكابلاته وشاشة العرض الخاصة به ومكونات الحاسب نفسه ولوحة المفاتيح والأقراص وغيرها من مكونات الحاسب ذات الطابع المادي الملموس، والأمر هنا لا يثير صعوبة للتقرير بصلاحية مسرح الجريمة الذي يحوي هذه المكونات لمعاينته من قبل مأموري الضبط والتحفظ على الأشياء التى تعد أدلة مادية تدل على ارتكاب الجريمة ونسبتها لشخص معين وكذا وضع الأختام فى الأماكن التى تمت فيها معاينة وضبط كل ما استعمل فى ارتكاب الجريمة وتحفظ عليها مع إخطار النيابة بذلك.

الحالة الثانية: الجرائم الواقعة على المكونات المعنوية أو بواسطتها:

ويأتي فى مقدمة هذه الجرائم تلك الواقعة على برامج الحاسب وبياناته أو بواسطتها[1]، وهنا تثور صعوبات عده تحول دون فاعلية المعاينة أو فائدتها ويمكن تلخيص هذه الصعوبات فى عاملين رئيسين هما:

الجريمة على نحو ما أرادت ، ومن ثم فإن الحكم يكون قد أصاب صحيح القانون . (الطعن رقم 2353 لسنة 68 جلسة 1998/6/3 س 49 ص813 ق 106)، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

[1] وقد رصدت وحدة متابعة الإنترنت بالإدارة العامة للمصنفات الفنية بعض المعاملات التجارية بين أحد الأشخاص وإحدى شركات الحاسب الآلى (رايت كليك) بولاية كاليفورنيا بالولايات المتحدة الأمريكية حيث طلب هذا الشخص شراء قطع من جهاز الكمبيوتر بما قيمته (600) دولار، وطلب تسليمها بعنوان حدده وطالب بخصم ثمنها على بطاقة ائتمانية خاصة بشخص آخر، وعند الاستعلام عن رقم الفيزا تبين أنها تخص أحد الأشخاص المقيمين بمحافظة أخرى، وبعمل تحريات سريعة عن الشخص الأخير تبين أنه لا يرتبط بأية صلة بالمشترى وأنه فوجيء بالخصم عند تسلمه كشف تعاملاته عن الشهر المنتهى. وعليه صدرت التعليمات بتتبع سير التعاملات على شبكة الإنترنت، وبعد عدة أيام تم رصده أثناء القيام بالاتصال بذات الشركة وطلب شراء بعض أجزاء من الكمبيوتر وخصم ثمنها على بطاقة فيزا تخص شخص آخر غير الشخص الأول ومستخدماً أسماء وهمية فى كل مرة ولذلك تم التأكد من قيام هذا الشخص باستخدام كروت فيزا تخص أشخاص آخرين وتم ضبط هذا الشخص أثناء تسلمه البضاعة فى الوقت والمكان المحدد والمتفق عليه وبمواجهة هذا الشخص اعترف بارتكابه للجريمة.... أ/ محمد يوسف محمد، التحديات التى تواجه التحقيقات فى الجرائم، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، 7أبريل 2009، هامش صـ 19.

(1) تكمن الصعوبة الأولي فى قله الآثار المادية التى تتخلف عن الجرائم التى تقع على برامج الحاسب وبياناته أو بواسطتها.

(2) الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التى غالباً ما تكون طويلة نسبياً وذلك ما بين اقتراف الجريمة والكشف عنها الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقي ظلالاً من الشك على الدليل المستقي من المعاينة[2].

توجد بعض التوصيات التى يجب إتباعها عند إجراء معاينة مسرح جريمة الجرائم المعلوماتية وتتمثل فى:

(1) القيام بتصوير الحاسب وما قد يتصل به من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد به بصفه عامة مع العناية بتصوير الأجزاء الخلفية وملحقاته الأخرى على أن يراعي أن يتم تسجيل زمان وتاريخ المكان الذي التقطت فيه كل صورة.

(2) ملاحظة طريقة إعداد نظام الحاسب بعناية فائقة.

(3) يجب أن يلاحظ وأن يتم إثبات الحالة التى يكون عليها توصيلات وكابلات الحاسب والتى تكون متصلة بمكونات النظام وذلك حتي يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة[1].

---

[2] لما كان التناقض بين معاينة الشرطة وتقرير مصلحة الأدلة الجنائية فى خصوص .... لا يعيب الحكم مادام قد استخلص الإدانة منهما استخلاصاً سائغاً لا تناقض فيه فإن ما يثيره الطاعن فى هذا المنحى لا يعدو أن يكون جدلاً موضوعياً فى تقدير الدليل وهو ما تستقل به محكمة الموضوع . (الطعن رقم 33078 لسنة 86 جلسة 2017/11/7)، س 68، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

[1] قضت محكمة النقض بأنه: لما كان الحكم قد عرض لطلب الطاعنين إجراء معاينة لمكان الحادث للوقوف على استحالة حدوث الواقعة كما صورها الشهود واطرحه فى قوله :- " وحيث إنه عن طلب إجراء معاينة لمكان الحادث فإنه يرمى إلى التشكيك فى صحة أقوال شاهدة الواقعة لعدم وجود أعمدة إنارة يمكنها معها الوقوف على كيفية ارتكاب الجريمة . لما كان ذلك ، وكانت الشاهدة المذكورة قد قررت بتحقيقات النيابة العامة أن الواقعة حدثت فى نحو الساعة السادسة مساء وأن المكان كان لم يزل مضيئا بنور الشمس ، التى لم تكن قد غربت بعد ، وكان من المقرر أن طلب المعاينة الذى لا يتجه إلى نفى الفعل المكون للجريمة ، ولا إلى استحالة حصول الواقعة كما رواها الشهود ، وإنما كان المقصود به إثارة الشبهة فى الدليل الذى اطمأنت إليه المحكمة ، يعد من قبيل الدفاع الموضوعى الذى لا تلتزم المحكمة بإجابته ، فمن ثم تعرض المحكمة عنه " . لما كان ذلك ، وكان من المقرر أنه ولئن كان القانون قد أوجب على محكمة الموضوع سماع ما يبديه المتهم من أوجه الدفاع وتحقيقه ، إلا أنه متى كانت الواقعة قد وضحت لديها ، أو كان الأمر المطلوب تحقيقه غير منتج فى الدعوى ، فلها أن تعرض عن ذلك مع بيان العلة ، وإذ كان ما أورده الحكم - فيما تقدم - كافياً وسائغاً ويستقيم به اطراح طلب إجراء المعاينة دون أن يوصم الحكم المطعون فيه بالقصور أو الإخلال بحق الدفاع ، فضلاً عن أن هذا الوجه من الدفاع لا يتجه إلى نفى الفعل المكون للجريمة ، ولا إلى استحالة حصول الواقعة كما رواها شهود الإثبات ، بل الهدف منه إثارة الشبهة فى الأدلة التى اطمأنت إليها المحكمة ، ويعتبر من أوجه الدفاع الموضوعية التى لا تلتزم المحكمة بإجابته ، ومن ثم فإن ما يثيره الطاعنان فى هذا الشأن يكون فى غير محله . (الطعن رقم 3559 لسنة 81 جلسة 2012/12/25 س 63 ص 878 ق 160)، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

(4) عدم التسرع فى نقل أي مادة معلوماتية من مكان وقوع الجريمة وذلك قبل إجراء الإختبارات اللازمة للتقنين من وجود أي مجالات مغناطيسية فى المحيط الخارجي حتي لا يحدث أي إتلاف للبيانات المخزنة.

(5) حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة وفحصها ورفع البصمات التى قد تكون لها صلة بالجريمة المرتكبة.

(6) القيام بحفظ المستندات الخاصة بالإدخال وكذا مخرجات الحاسب الورقية التى قد تكون ذات صلة بالجريمة وذلك من أجل رفع ومضاهاة البصمات التى قد تكون موجودة عليها.

(7) يجب أن تقتصر عملية المعاينة على مأموري الضبط سواء كانوا من الباحثين أو المحققين ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية فى مجال الحاسبات واسترجاع المعلومات ممن تلقوا التدريب الكافى لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة[2].

ثانياً
دور الشرطة فى التفتيش فى الجرائم السيبرانية

لم تشرع الإجراءات الجنائية للوصول إلى الإدانة أو العقاب، وإنما شرعت لتكون وسائل للوصول إلى محاكمة منصفة فى إطار يحافظ على جوهر الحريات تحت مظلة قضاء مستقل محايد يباشر ويشرف ويراقب من أجل تحقيق العدالة وانتقاء الظلم. ومن هنا وجب التدقيق فى تطبيق الإجراءات الجنائية، فكما يمكن أن تكون الإجراءات الجنائية وسيلة لمحاكمة القتلة والمجرمين واستيفاء الحقوق، ليس بعيداً أن تتحول تلك الإجراءات نفسها إلى اداة اغتيال أبرياء معنوياً وتحطيم كرامتهم واعتبارهم إذا أسيء استخدامها. لهذا كانت الإجراءات الجنائية دائماً فى قلب المناقشات الدستورية والقانونية، يتم وضعها تحت تأثير الوثائق الدولية لحقوق الإنسان، ويقتضى بحث الالتزام بالمتطلبات الأساسية للدولة الديمقراطية وأصول دولة القانون والخروج عن الثوب الفنى لتعميق الحق فى المحاكمة المنصفة[1].

---

[2] أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية، مرجع سابق، صـ 117 وما بعدها.

[1] د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص 5.

هذا ويؤكد الخبراء أن الجرائم الإلكترونية تزداد كلما توغل العالم فى استخدام الإنترنت، وأن أدلة إثبات الجريمة يصعب التوصل إليها[2]. ويعد التفتيش إجراء من إجراءات التحقيق التى يختص بها أصلاً سلطة التحقيق واستثناءاً مأموري الضبط القضائي من جهاز الشرطة، ولم يحدد المشرع المقصود بالتفتيش إلا أنه يمكن تعريفه بأنه " إجراء من إجراءات التحقيق يهدف إلى البحث عن دلائل أو أشياء موجودة فى مكان مغلق تفيد فى كشف الحقيقة عن الجريمة يباشره أحد مأمورى الضبط القضائى أو سلطة التحقيق أو المحكمة وفقاً للقانون". وهو ليس من إجراءات كشف الجرائم قبل وقوعها، بل هو إجراء من إجراءات تحقيقها بعد ارتكابها[3].

والتفتيش ليس غاية فى حد ذاته وإنما هو وسيلة تتمثل فيما يمكن الوصول من خلاله إلى أدله مادية تسهم فى بيان وظهور الحقيقة، وهو بذلك قد يكون محلة الفرد وقد يكون مسكنه وتوابعه مثل الحديقة والجراج أو أي مكان آخر مهما كانت طبيعته مثل المحال العامة ووسائل المواصلات.

مدي صلاحية جرائم الحاسب الآلى للتفتيش على أدلتها:

تلعب الشرطة دوراً رئيسياً فى القيام بإجراء التفتيش سواء كان ذلك عن طريق الندب من سلطة التحقيق أو عن طريق قيامها بذلك فى الأحوال الاستثنائية الأخرى التى تجيزها حالة التلبس بارتكاب جناية أو جنحة[1]؛ وهنا يجب أن نفرق بين حالتين:

الحالة الأولي: الجرائم الواقعة على المكونات المادية للحاسب:

حيث تقع هذه الجرائم فى معظم الأحيان على معدات الحاسب وكابلاته وشاشة العرض الخاصة به ومفاتيح تشغيله... إلخ وذلك فى حال سرقتها أو إتلافها أو

---

[2] بدون، الجريمة الإلكترونية فى الوطن العربى، متاح على:
- Available At: http:// eljaraimeliliktouniya.blogspot.com

[3] د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص 947.

[1] قضت محكمة النقض بأنه: لما كان الثابت من مدونات الحكم المطعون فيه، أن الضابط ... انتقل إلى كشك المتهم الأول لضبط الطاعن لتنفيذ حكم صادر ضده فى جريمة سرقة، وأنه عقب ضبطه له اقتاده إلى ديوان قسم الشرطة، وأنه قبل إيداعه بحجرة الحجز بالقسم قام بتفتيشه وقائياً فعثر معه على المخدر المضبوط ومطواة قرن غزال، وكان هذا الذى أورده الحكم فى مدوناته كافياً فى الرد على الدفع ببطلان القبض والتفتيش ويصادف صحيح القانون، ذلك أن التفتيش فى خصوصية هذه الدعوى أمر لازم لأنه من وسائل التوقى والتحوط من شر من قبض عليه إذا ما سولت له نفسه، التماساً للفرار، أن يتعدى على غيره بما قد يكون محرزاً له من سلاح أو نحوه، وكان الطاعن لا ينازع فى حق الضابط فى تفتيشه عند إدخاله سجن القسم، فإن منعاه على الحكم فى هذا الخصوص يكون على غير سند، و لاينال من سلامة الحكم فى هذا الشأن ما يثيره الطاعن من أن المحكمة لم تعن ببحث أمر الخصومة على ثبوت الواقعة المسندة إلى الطاعن والتى دانه بها. (الطعن رقم 5409 لسنة 62 جلسة 1994/2/16 س 45 ص 291 ق 42)، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:
http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

اختلاسها... فلا تثار أدني صعوبة إذا كان محل الجرائم الأشياء سالفة الذكر حيث ينطبق بصددها ذات القواعد التقليدية للتفتيش[2].

الحالة الثانية: الجرائم الواقعة على المكونات المعنوية أو بواسطتها:

إن الأمر هنا يختلف ويحتاج وقفة للتأمل قبل تقرير إمكانية التقرير بإمكانية تطبيق قواعد التفتيش التقليدية، وفيما يتعلق ببرامج الحاسب فإن الأمر لا يحتاج إلى تقرير قواعد جديدة للتفتيش عن أدلة الجرائم التى يكون محلها برامج الحاسب كالسرقة أو الإتلاف أو استعمال هذه البرامج كأداة فى ارتكاب بعض الجرائم كالتزوير أو التلاعب فى البيانات أو الإتلاف الفني للأنظمة المعلوماتية.

أما فيما يتعلق ببيانات الحاسب فإذا كانت هذه البيانات مخزنة بالأنظمة وهنا تتجرد من الكيان المادي الملموس، وعليه فإنه قد ثار جدل فقهى بين فقهاء القانون الجنائى، حول مدى إمكانية تفتيش وضبط البيانات المخزنة أو المعالجة إلكترونياً بصورها وأشكالها المختلفة كالأقراص والأشرطة الممغنطة بما فى ذلك ذاكرة جهاز الحاسب الآلى وانقسموا إلى اتجاهين:

الاتجاه الأول: ذهب أنصاره إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب الآلى باعتباره وسيلة للإثبات المادى، يهدف لضبط أدلة مادية تتعلق بالجريمة وتفيد فى كشف الحقيقة، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلى، ويمثل هذا الرأى جانب من الفقه الفرنسى الذى يرى أن النبضات أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المادية المحسوسة التى يمكن تفتيشها وضبطها[3].

الاتجاه الثانى: يرى أنصاره أن المعلومات التى لا تعد شيئاً مادياً وإنما ذات طبيعة معنوية، الأصل مجرد ذبذبات ونبضات إلكترونية أو إشارات أو موجات كهرومغناطيسية، إلا أنها قابلة لأن تخزن فى أوعية ووسائط مادية كالأقراص والأشرطة الممغنطة، وبالتالى فهى ليست شيئاً معنوياً كالحقوق والآراء والأفكار، بل هى أشياء مادية محسوسة لها وجود ملموس فى العالم الخارجى، ومن ثم يصح أن يرد عليها التفتيش والضبط[1].

بالإضافة إلى ما سبق توجد صعوبات إجرائية من شأنها إعاقة خضوع البيانات المخزنة آلياً لقواعد التفتيش التقليدية والتى يمكن بلورتها فيما يلي:

(1) حالة وجود النظام المعلوماتي داخل إحدى المساكن مع وجود النهاية الطرفية له فى مكان آخر، الأمر الذي يتطلب منح الشخص المخول له بالتفتيش السلطة الكاملة للتوصل إلى مكان النظام المعلوماتي وتسجيل ما يحويه من بيانات تعد أدلة على ارتكاب جريمة ما دون التقيد بالحصول على إذن القاضي بذلك كما هو مقرر قانوناً فى حال تفتيش منزل غير المتهم.

---

[2] أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية، مرجع سابق، صـ 121.

[3] Gassin(R) Le droit et linfromatique,D,1980.p.38 ، مشار اليه لدى: د/ عبد الفتاح بيومى حجازى، مبادىء الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، مرجع سابق، صـ 380.

[1] د/ هشام فريد رستم، الجوانب الإجرائية لجرائم المعلوماتية، مكتبة الآلاء الحديثة، 1994، صـ 66 وما بعدها.

(2) فمـا يتعلـق بـإذن التفتـيش تبـدو الصـعوبة فـى إشـتراط أن يكـون الإذن محـدد فيمـا يخص محله والأشياء التى يهدف التفتيش إلـى ضـبطها، ويقتضـي هذا الشرط أن يقوم مصـدر الإذن بتحديـد الأشـياء المـراد ضـبطها بطريقـة فنيـة الأمـر الـذي لا يكـون فـى مقدوره لأنه يتطلب نوع من المعرفة تتجاوز المعرفة العامة أو السطحية.

(3) يقتضـي التفتيش عن البيانات المخزنـة آلياً القيـام بعمليـة ولـوج للأنظمـة المعلوماتيـة التى تحويها لضبط ما يعد صالحاً من هذه البيانات كدليل أو قرينة لارتكاب جريمة مـا، وهذا الأمر يقتضـي سلفاً معرفة تامة من قبل الشخص القائم بالتفتيش بكيفية التعامل مـع برامج وملفات المخزنة وكذا كلمة السر والمرور اللازمين للدخول على النظام.

ويزداد الأمر تعقيداً إذا علمنـا أن كافـة التشريعات العقابيـة والإجرائيـة تقضـي بإعفاء المتهم من تقديم ما من شأنه إدانته بطريقة مباشرة، وبذلك لا يجوز إجبار المتهم علـى البـوح أو الإفصـاح لسـلطة التحقيـق بـالرقم الكـودي السـري للمـرور إلـى ملفـات البيانات أو أن يكشف عن كلمـة السر وطبـع البيانـات المخزنـة وغير ذلك من الأمور التى من شأنها إدانتـه. ولـذا بدت الحاجـة للتدخل التشريعي لتقرير الضـوابط القانونيـة الكفيلة للتغلب علـى الصـعوبات الإجرائيـة التـى تثـار عنـد تفتيش الأنظمـة المعلوماتيـة. والجدير بالذكر أنه صدر قرار وزاري عام 2002 بشـأن إنشـاء إدارة لمكافحـة جـرائم الحاسبات وشبكات المعلومات يكون من اختصاصها مكافحة وضبط الجرائم التـى تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانـات واتخـاذ الإجراءات القانونية حيالها[2].

ثالثاً

دور الشرطة فى ضبط أدلة الجرائم السيبرانية

إن الضبط فى معظم الأحوال يكون هو غرض التفتيش وإن لم يكن هو السبب الأوحد له، فقد يأتي الضبط لأسباب أخرى غير التفتيش مثل المعاينة وما يقدمه المتهم والشهود لمأموري الضبط القضائي[1]. وللقاضى أن يستعين فى اقتناعه بالقرائن التى تعزز الأدلة وتساندها، فللمحكمة أن تستعين فى تعزيز أدلة الثبوت باستعراف الكلب

---

[2] أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية، مرجع سابق، صـ 122 ومابعدها، أيضـاً د/ مفتـاح بـوبكر المطـردى، المستشـار بالمحكمـة العليـا الليبيـة، الجريمـة الإلكترونية والتغلب على تحدياتها، مرجع سابق، صـ 48.

[1] قضت محكمة النقض بأنـه: لمـا كـان مـا يثيره الطاعنـان من عدم إيراد الحكم لتفصيلات مـا جاء بمحضر المعاينة ، فإن الحكم المطعون فيه قد أورد منها ما يكفى لتبرير اقتناعه بالإدانـة ، ومـا دامت المحكمة قد اطمأنت إلى هذه المعاينة واعتمدت عليها فى تكوين عقيدتها ، فـإن إغفالهـا إيراد بعض تفصيلات معينة يعتبر اطراحاً منها لهذه التفصيلات ، فإن ما يثيره الطاعنـان فـى هذا الشـأن لا يكـون لـه محـل . (الطعـن رقـم 3559 لسـنة 81 جلسـة 2012/12/25 س 63 ص 878 ق 160)، دائـرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

البوليسى[2]. وفى ممارسة القاضى لتكوين حريته فى الاقتناع فإنه يتقيد بأن تكون عقيدته واقتناعه قد استمدا من أدلة طرحت بالجلسة، فلا يسوغ للقاضى أن يستند فى حكمه إلى دليل ليس له أصل ثابت بالأوراق ولم يحققه فى الجلسة طالما كان ذلك ممكناً، ومع ذلك يجوز للمحكمة الاستناد إلى ما ورد بالتحقيقات الأولية من أدلة بوشرت فى مواجهة المتهم أو اطلع عليها. أيضاً يجب أن يكون اقتناع القاضى مبنياً على دليل مستمد من إجراء صحيح. أيضاً يجب أن يكون اقتناع القاضى مبنياً على أدلة مستساغة عقلاً، وللقاضى فى استخلاصه للأدلة وتكوين اقتناعه يجوز له أن يبنى عقيدته على الثقافة العامة السائدة والتى يفترض علمها فى كل شخص يتواجد فى ذات الزمان والمكان ودون أن يكون ذلك قضاء بعلم القاضى الشخصى، أيضاً يجب أن يكون اقتناع القاضى مبنياً على اليقين، وعليه فإن الشك فى الاثبات أو فى مفهوم الأدلة يجب أن يفسر لمصلحة المتهم. أخيراً لا يجوز للقاضى أن يؤسس اقتناعه بناء على قرينة واحدة أو استدلال واحد، فلا يجوز مثلاً أن يستند فقط على شهادة صدرت من صغير وحدها، أو أن يستند فقط إلى شهادة شاهد سمعت أقواله بمحضر النيابة على سبيل الاستدلال دون حلف اليمين القانونية[3].

هذا ويجب ألا يفهم القاضى من مبدأ حرية الاقتناع أنه تحلل من مراعاة القواعد اللازمة لقبول أدلة الإثبات، فالقاضى حر فى أن يعتقد أو لا يعتقد فى صحة الأدلة المطروحة، ولكنه لا يملك التحكم فى هذا الاعتقاد، فاليقين المطلوب عند الاقتناع ليس هو

اليقين الشخصى للقاضى، وإنما هو اليقين القضائى، الذى يصل إليه القاضى بناء على العقل والمنطق[1].

---

[2] نقض 13 فبراير 1967، مجموعة أحكام النقض س18، رقم 38، نقض 4 ديسمبر 1967، س 18، رقم 255.

[3] د/ مأمون محمد سلامة، قانون الإجراءات الجنائية معلقاً عليها بالفقه وأحكام النقض طبقاً لأحدث التعديلات والأحكام ، ط3، دار طيبة للطباعة، الجيزة، 1430هـ – 2010م، ص 1259 وما بعدها.

[1] وضماناً للوصول إلى الاقتناع القضائى بالعقل والمنطق استقر قضاء محكمة النقض على المعايير التالية لضمان الوصول إلى اليقين القضائى البعيد عن التحكم: - لا يجوز الاعتماد فى الاثبات على الدلائل وحدها، بل يجب أن تكون هذه الدلائل مكملة للدليل. – لا يجوز للمحكمة أن تحل نفسها محل الخبير فى مسألة فنية بحتة، بل عليها ألا تشق طريقها لإبداء الرأى فيها دون الاستعانة بخبير يخضع رأيه لتقديره، كل ذلك دون إخلال بسلطة المحكمة فى تقدير رأى الخبير ووفقاً لاقتناعها. – الالتزام عند الإدانة بمبدأ الأدلة فى المواد الجنائية متساندة متكاملة يكمل بعضها بعضاً، ومنها مجتمعة فتكون عقيدة المحكمة، فلا ينظر إلى دليل معين لمناقشته فى معزل عن تأثير بقية الأدلة فى عقيدة المحكمة (نقض 7 مايو سنة 2002، مجموعة الأحكام، س53، ص721). مما مقتضاه أنه لا يشترط أن تكون الأدلة التى اعتمد عليها الحكم ينبىء كل دليل منها ويقطع بالإدانة بشرط أن تكون المحكمة قد استخلصت اقتناعها اليقينى من مجموع الأدلة.... د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص617 وما بعدها.

والضبط لا يخرج عن كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد فى كشف الحقيقة عنها وعن مرتكبيها سواء فى ذلك أن يكون هذا الشئ عقاراً أو منقولاً، والضبط أيضاً يكون للأشخاص.

مدى صلاحية جرائم الحاسب الآلى لضبط أدلتها:

نفرق هنا أيضاً بين حالتين:

الحالة الأولي: الجرائم الواقعة على المكونات المادية للحاسب:

فى هذه الحالة لا يثر الأمر أدني صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها بموجب قواعد التفتيش التقليدية، وذلك لوجود أشياء مادية محل الجرائم مثل معدات الحاسب وكابلاته وأسلاكه ومفاتيح التشغيل وشاشة العرض والدعامات المادية والأشرطة والأسطوانات وغيرها.

الحالة الثانية: الجرائم الواقعة على المكونات المعنوية للحاسب أو بواسطتها:

فما يخص برامج الحاسب: ليس من الصعوبة التقرير بإمكانية ضبط الجرائم وأدلتها والتى يكون محلها مثلاً سرقة الدعامة المادية للبرامج أو الوسائل المادية المستخدمة فى نسخة بصورة غير مشروعة أو إتلافه بوسائل تقليدية. أما فما يخص بيانات الحاسب: فتوجد ثمة عوائق أثناء القيام بعملية الضبط وذلك بغض النظر عن الخلاف القانونى الدائر حول طبيعتها حيث توجد صعوبات عملية تحول دون ضبط البيانات التى تعد دليلاً على ارتكاب جريمة ما فى بيئة المعالجة الإلكترونية. وتكمن هذه الصعوبات فما يلى:

(1) عدم وجود دليل مرئى يمكن فهمه بالقراءة.

(2) تتسم الجرائم التى يكون محلها بيانات الحاسب بعدم تركها لآية آثار يمكن الاستدلال بها علىها ويتجلى ذلك بصورة واضحة فى جرائم الاختلاس والتزوير التى يستخدم فىها الحاسب الآلى، وحتى البيانات التى يمكن التوصل إليها فإنه يمكن للجانى محوها أو تدميرها فى فترة زمنية قصيرة جداً لا تتعدى ثوان معدودة.

(4) تطلب قدر من المعرفة الفنية لتحديد البيانات التى تصلح كأدلة جنائية من عدمه، وفى حالة الأنظمة الكبيرة والمتصلة بنهاية طرفية أخرى فإن الأمر قد يؤدى إلى انتهاك سيادة دولة أخرى موجود بها هذه البيانات المطلوبة كأدلة من قبل سلطات التحقيق.

(5) تقاعس المجنى علىهم وخاصة فى قطاع الأعمال عن الإبلاغ عنها تحاشياً للأضرار المترتبة على العلانية خشية أن تهتز صورتها أمام العملاء.

(6) فى حالة عدم وجود مدربين مؤهلين ومدربين على التعامل مع البيانات التى تعد دليلاً لجريمة معلوماتية فإن هذا الأمر قد يؤدى إلى إغفال الدليل أو إهماله أو إتلافه أو إفساده.

وبغض النظر عن الجدل الدائر فى موقف الفقهاء والتشريعات والطبيعة القانونية لهذه البيانات المخزنة آلياً فهناك صعوبات يقابلها مأمورى الضبط عند تصديه لضبط هذه البيانات وتمييز ما يصلح منها كدليل من عدمه.

وهناك عدة مقترحات لمواجهة هذه الصعوبات:

- إنشاء أقسام متخصصة بأكاديمية الشرطة لدراسة هذه الصعوبات وتدريب الطلاب على كيفية التعامل معها بطريقة فنية صحيحة، فضلاً عن إنشاء شرطة متخصصة وتسليحها بالتقنيات الحديثة لمكافحة هذا النوع من الإجرام[1].

- تشجيع المجنى عليهم للإبلاغ عن هذه الجرائم ووضع نص قانونى يلزم العاملين على النظام المعلوماتى بالمعاونة الفعالة لضبط البيانات التى تعد أدلة جنائية. وحسناً فعل المشرع الجنائى المصرى حيث صدر القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات[2]، ونص فى المادة (6) منه على تحديد صفة مأمورى الضبط القضائى على النحو التالى: " لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي :1- ..... 2- ..... 3- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني" .

- ضرورة منح سلطة التحقيق الصلاحية القانونية والتدريب العملى اللازم لاختراق نظام الحاسب وضبط مايحويه من بيانات مخزنة وضرورة إتباع القواعد الفنية التى يوصى بها المتخصصون فى مجال تحريز البيانات المضبوطة وتأمينها من الإتلاف.

وقد نص المشرع الجنائى المصرى فى القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات على ذلك فى نص البند الثالث من الفقرة الأولى من المادة (6) على أنه: " لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي:...2- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط ."

---

[1]- Available At: متاح على:
http://digital.ahram.org.eg/articles.aspx?serial=26957&eid=1785

[2] القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018.

وبصفة عامة لابد من وجود أساليب تأمين مختلفة لمواجهة جرائم التكنولوجيا الحديثة يجب على جهاز الشرطة إتباعها[1].

رابعاً
حدود الدور الفنى للأجهزة الأمنية فى ملاحقة الجرائم المعلوماتية

أمام تلك العقبات السابقة يتبين محدودية الدور الفنى للأجهزة الأمنية فى ملاحقة تلك الجرائم وهذا ما يتبينه الباحث من خلال استعراض الدور الذى تقوم به الجهات والإدارات التالية:

1- الإدارة العامة لمباحث الأموال العامة:

تضطلع الإدارة العامة لمباحث الأموال العامة بمكافحة الجرائم الاقتصادية التقليدية بصفة عامة والمستحدثة بصفة خاصة اعتبارها إحدى الروافد الرئيسية لقطاع الأمن الاقتصادى.

وتعتبر جرائم تزييف العملات الورقية من أكثر الجرائم التى تضطلع الإدارة العامة لمباحث الأموال العامة لمكافحتها وتسهم أجهزة الحاسب الآلى بدور كبير فى ارتكابها وتقوم الإدارة بإتباع الخطوات التالية لمكافحة تلك الجريمة وذلك على النحو التالى:

- مرحلة جمع المعلومات: وتكون مرحلة جمع المعلومات إما قبل إتمام عملية التزييف أوبعد تمامها وطرح العملات للتداول، ولذلك فإن لكل مرحلة منها إجراءات معينة كما يلى:

أ- مرحلة جمع المعلومات قبل تمام عملية التزييف وتشتمل على الاتجاهين التاليين:

- يتمثل الاتجاه الأول: فى السعى الدائم خلف الجرائم فى جميع مراحلها سواء أكانت فى مرحلة الأعمال التحضيرية أو فى مرحلة التنفيذ الفعلى أثناء عملية التزييف ويكون ذلك عن طريق المصادر السرية للإدارة التى تقوم بجمع معلومات عن ارتكاب تلك الجرائم.

- أما الاتجاه الثانى: فيتم عن طريق تلقى البلاغات من أحد المواطنين أو من أحد المصادر السرية عن معلومات تفيد بقيام شخص بارتكاب تلك الجريمة واعتزامه طرحها للتداول.

ب- مرحلة جمع المعلومات بعد طرح العملات المزيفة للتداول:

وتبدأ مرحلة جمع المعلومات مع بداية عمليات الترويج وهى التى تتم على عدة مراحل وفى أماكن متفرقة وذلك على النحو التالى:

---

[1] أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية، مرجع سابق، صـ 123.

- فحص عينة من العملات الورقية المزيفة التى ظهرت فى التداول فنياً لمعرفة أسلوب وطريقة تزييفها والأدوات المستعملة فى تزييفها.
- يتم الكشف بعد ذلك عن طريق الأرشيف للبحث عن الأشخاص المسجلين الذين سبق ضبطهم فى قضايا إتبع فيها ذات الأسلوب والتحرى عن علاقتهم بتلك الجريمة.
- إخطار البنوك والمصارف بمواصفات تلك العملات الورقية المزيفة للإبلاغ عن أى عملات ورقية قد ترد إليهم من مرتكبيها حيث أن كثرة البلاغات تساعد على زيادة ووفرة المعلومات التى تفيد فى عملية ضبط مرتكب الفعل.
- الدفع بالمصادر السرية الموثوق فيها داخل أوساط المزيفين والمروجين وعرض شراء كميات من العملات المزيفة التى تم تداولها.
- فحص عمليات بيع وشراء ونقل ماكينات الطباعة والتصوير التى استعمل مثلها فى إتمام عملية التزييف والتحرى عن علاقة أصحابها بالعملات التى تم تداولها.
- وعند القيام بعملية الضبط يتم تكليف مجموعة الضباط المتخصصين من الناحية الفنية فى كيفية التعامل مع الأدوات والآلات التى تستخدم فى ارتكاب جريمة التزييف ولاسيما أجهزة الكمبيوتر لأن تعامل خاطئ قد يتسبب فى فقد دليل جوهرى على ارتكاب تلك الجريمة.

وبجانب ما سبق تكليف الإدارة العامة لمباحث الأموال العامة بمتابعة ما يرد إليها من جرائم أخرى تتعلق بطبيعة عملها وقد تكون من هذه الجرائم ما يتصل بالحاسبات الآلية.

2- الإدارة العامة للتوثيق والمعلومات:

تعتبر الإدارة العامة للتوثيق والمعلومات من أكثر الإدارات بوزارة الداخلية تعاملاً مع الجرائم المعلوماتية حيث إنها تختص بعمليات المتابعة الفنية لكثير من الجرائم المعلوماتية ويبدأ عمل الإدارة من خلال:

1- المتابعة الفنية والتحرى عن الجرائم التى تبلغ إلى الإدارة من الإدارات الأخرى وتتطلب تلك الجرائم المتابعة الفنية الدقيقة من خلال استخدام شبكة الإنترنت وتحديد شخص المتهم.

2- كذلك تقوم الإدارة بتحديد شخص المتهم من خلال عملية تتبع له عند اكتشافهم لارتكاب جريمة ترتكب باستخدام شبكة الإنترنت.

ويعتمد أسلوب عمل الإدارة فى معرفة شخص مرتكب الجريمة على استخدام البرامج الحديثة وذلك عن طريق الاعتماد أن لكل شخص يتعامل مع شبكة الإنترنت له رقم للدخول على الشبكة يعرف بـ (IP) بحيث يمكن من خلال تتبع هذا الرقم معرفة مكان الشخص ويتم ذلك باستخدام برامج على درجة عالية من الكفاءة ويلاحظ أن هذه البرامج فى تطور مستمر حتى لا يتم معرفتها واكتشافها وبالتالى يسهل اختراقها.

وتعتبر جرائم السرقة التى ترتكب باستخدام كارت الفيزا من أكثر الجرائم التى تسعى الإدارة العامة للمعلومات والتوثيق إلى ضبطها وذلك من خلال متابعة الشخص ومعرفة مكانه ومتابعة تنفيذ الجريمة ويتم ضبطه أثناء تسليمه البضائع التى يقوم بشرائها من خلال الكروت المسروقة.

3- الإدارة العامة للمصنفات الفنية وحماية حقوق الملكية الفكرية:

تعتبر جرائم النسخ والتقليد من أكثر الجرائم شيوعاً فى مجال المعلومات ويقع على عاتق إدارة مباحث المصنفات الفنية مسئولية متابعتها، ويبدأ عمل مباحث المصنفات الفنية من خلال ما يلى:

- تلقى الإخطار عن وقوع تلك الجرائم سواء بالإبلاغ أو عن طريق تلقى الشكاوى أو من أحد المصادر السرية.
- يبدأ فريق البحث القيام بعملية التحرى عن مكان مرتكب الفعل ومعرفة شخصيته والتأكد من ارتكابه الجريمة من خلال إجراء التحريات حول طبيعة نشاط المتهم.
- يتم تفتيش مقر عمل الشخص أو منزله إذا لزم الأمر وذلك بعد الحصول على إذن من النيابة العامة بالقيام بالتفتيش[1].
- يتم التحفظ على الوسائط المنسوخة وارسالها إلى المعمل الجنائى الخاص بالإدارة للتأكد من أن البرامج الموجودة بها ليست أصلية وإنما تم نسخها وكذلك يتم التحفظ على الأجهزة المستخدمة فى عملية النسخ وعمل محضر بذلك وارساله إلى النيابة العامة.

كذلك تقوم الإدارة العامة للمصنفات الفنية وحماية حقوق الملكية الفكرية بحملات تفتيشية كبيرة على جميع أنحاء الجمهورية لضبط تلك الجرائم. ولاشك أن هذا الدور الذى تضطلع به الإدارة العامة للمصنفات الفنية هو انعكاساً لما يطالب به المجتمع الآن من حماية للملكية الفكرية وحرية الإبداع والتعبير وذلك من خلال حماية البرامج من النسخ والتقليد[1].

التطور فى أسلوب عمل أجهزة الشرطة:

---

[1] الطعن رقم 9680 لسنة 86 جلسة 2018/3/21، س69، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:
http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

[1] د/ أيمن عبد الحفظ عبد الحميد سليمان، الدور الفنى لأجهزة الشرطة فى مواجهة الإجرام المعلوماتى، مرجع سابق، صـ 12 وما بعدها، أيضاً: أ/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، مرجع سابق، صـ 189 وما بعدها.

بدأت أجهزة الشرطة المصرية فى إنتاج سياسة التقدم العلمى والتكنولوجى ومواكبة التطور واللحاق بالمسيرة العلمية من خلال الاعتماد على التقنيات الحديثة لمواجهة الصور المستحدثة من الإجرام المعلوماتى وكان ثمرة هذا التطور إنشاء إدارة جديدة تختص بتلك الجرائم وهى:

إدارة مكافحة جرائم الحاسبات وشبكات المعلومات:

أنشئت تلك الإدارة الجديدة بالقرار رقم 13507 لسنة 2002 وهى تابعة للإدارة العامة للمعلومات والتوثيق وهى تخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنياً مصلحة الأمن العام وهى تختص بما يلى:

1- وضع خطة تأمين ووقاية نظم وشبكات المعلومات لأجهزة وزارة الداخلية لمنع وقوع أية جرائم علىها باستخدام الأساليب والتقنيات العلمية الحديثة وبحث مدى كفاية تلك الأساليب لتحقيق الأهداف المطلوبة وتنفيذها بعد اعتمادها وذلك بالتنسيق مع الأجهزة المختصة بذلك سواء من داخل الوزارة أو خارجها ووفقاً للقوانين واللوائح والتعليمات المنظمة لذلك.

2- مكافحة وضبط الجرائم التى تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات كالاختراقات واتخاذ الإجراءات القانونية حيالها وذلك بالاشتراك والتنسيق مع الأجهزة العنية وفقاً للتعليمات المنظمة لذلك.

3- إخطار الأجهزة النوعية الشرطية المختصة بأعمال المكافحة بالبيانات والمعلومات المتعلقة بالجرائم الأخرى والتى يمكن جمعها أو التوصل إلىها من خلال شبكات المعلومات باستخدام أجهزة الحاسب الآلى والتنسيق معها لإجراء التحريات وأعمال الضبط فى تلك الجرائم وفقاً للقواعد واللوائح والتعليمات المنظمة لذلك.

4- إعداد البحوث الفنية والقانونية فى مجال مكافحة جرائم الحاسبات وشبكات المعلومات بالتنسيق مع الأجهزة المختصة من داخل الوزارة أو خارجها وفقاً للتعليمات المنظمة لذلك.

5- إعداد أرشيف متكامل للمعلومات التى تخدم أعمال الإدارة فى مجال الحاسبات ونظم المعلومات وتحديثه أولاً بأول وفقاً للتعليمات المنظمة لذلك وبالتنسيق مع الأجهزة المختصة.

وتضم الإدارة الأجهزة التالية:

1- قسم العمليات: ويختص بما يلى:

أ- مكافحة الجرائم التى تقع باستخدام أجهزة الحاسب الآلى فى مجالات نظم المعلومات وشبكات وقواعد البيانات بالاشتراك مع الأجهزة المختصة بذلك سواء من داخل الوزارة أو خارجها وفقاً للتعليمات المنظمة لذلك.

ب- إخطار الأجهزة النوعية المختصة بأعمال المكافحة بالبيانات والمعلومات المتعلقة بالجريمة الجنائية التى يمكن التوصل إليها من خلال الاتصال بشبكات المعلومات

والتنسيق معها لإجراء التحريات وأعمال الضبط فى تلك الجرائم وفقاً للتعليمات المنظمة لذلك.
ج- إعداد قاعدة بيانات بجرائم المعلومات التى تدخل فى نطاق اختصاص الإدارة والأحكام الصادرة فيها وكذا مرتكبى تلك الجرائم.
د- إنشاء الملفات والسجلات والبطاقات اللازمة لذلك.

2- قسم التأمين: ويختص بما يلى:

أ- وضع الخطط والأساليب التى تستخدم فى مجال تأمين نظم المعلومات والشبكات الخاصة بأجهزة الوزارة وتنفيذها بعد اعتمادها بالتنسيق مع الأجهزة المختصة ووفقاً للتعليمات المنظمة لذلك.
ب- تقديم يد العون لكافة أجهزة الوزارة التى تطلب تأمين نظم معلوماتها وشبكاتها حماية للثروة المعلوماتية بها وذلك وفقاً للقواعد والتعليمات الصادرة فى هذا الشأن.
ج- متابعة التراخيص التى تصدر للشركات الخاصة فى مجال نظم وأجهزة وشبكات المعلومات وذلك بالتنسيق مع الجهات المعنية ووفقاً للتعليمات المنظمة لذلك[1].

3- قسم البحوث والمساعدات الفنية: ويختص بما يلى:

أ- القيام بإعداد البحوث الفنية والقانونية فى مجال تأمين نظم وشبكات المعلومات بالحاسبات الآلية ودراسة الظواهر الإجرامية بالنسبة للجرائم التى تقع فى هذا المجال – وما يستحدث منها – واستنباط النتائج للاستفادة منها فى أساليب المكافحة وذلك بالتنسيق مع الأجهزة المختصة سواء من داخل أو خارج الوزارة ووفقاً للتعليمات المنظمة لذلك.
ب- بحث مدى ملائمة التشريعات الجنائية لمواجهة جرائم المعلومات بالتنسيق مع الأجهزة المختصة بذلك.
ج- تقييم الدعم الفنى لجميع جهات الوزارة فى كافة القضايا والوقائع المرتبطة بمجال نظم وبرامج وأجهزة وشبكات المعلومات أو التى يستخدم الحاسب الآلى فى ارتكابها.
د- توفير كافة المساعدات الفنية وإبداء الرأى والمشورة للجهات سواء من داخل الوزارة أو خارجها للمعاونة فى عمليات ضبط الجرائم التى تتم باستخدام الحاسب الآلى وفقاً للقواعد والتعليمات المنظمة لذلك.

ويفوض مساعدى أول ومساعدى الوزير النوعيين والجغرافين (كل فى نطاق اختصاصه) بالاشتراك مع مدير الإدارة العامة للتنظيم والإدارة فى إنشاء

---

[1] د/ أيمن عبد الحفظ عبد الحميد سليمان، الدور الفنى لأجهزة الشرطة فى مواجهة الإجرام المعلوماتى، مرجع سابق، صـ 18 وما بعدها، أيضاً: مقدم/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، مرجع سابق، صـ 190 وما بعدها.

وحدات مكافحة جرائم الحاسبات وشبكات المعلومات (بعد استكمال مقوماتها البشرية والمادية) وذلك بالأجهزة التى تنهض بأعمال البحث تبعيتها والواقعة ضمن نطاقات إشرافهم النوعية أو الجغرافية. وتحديد تبعيتها واختصاصاتها التفصيلية على أن تخضع تلك الوحدات للإشراف الفنى التقنى لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق.

ويتبين من قانون إنشاء الإدارة العامة لمكافحة جرائم الحاسبات وشبكات المعلومات مدى حرص أجهزة الشرطة المصرية على مواكبة التطور الذى تنتهجه بلدان العالم المتطور من ضرورة الاهتمام بمكافحة ما يستجد من صور حديثة فى ارتكاب الجرائم بكل ما هو جديد فى عالم التكنولوجيا[1].

ورغم هذا وذاك، إلا أن الأمر يتطلب ضرورة إنشاء مركز قومى لأمان الحاسب الآلى والمعلومات[2]. فهل يمكن أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز القومي لتنظيم الاتصالات المنشأة بالقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات[1]– نواة لهذا المركز وهو ما يأمله الباحث. حيث نصت المادة (4) من القانون المذكور على أنه " تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها .على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن."

خامساً
دور الشرطة الأمريكية فى مواجهة الجرائم المعلوماتية

تأتى الولايات المتحدة الأمريكية فى مقدمة الدول التى واجهت الجرائم المعلوماتية وذلك بالنص على مواجهتها تشريعياً حتى يعطى للفعل وصف الجريمة ثم بإنشاء إدارة متخصصة لمتابعة الجرائم المعلوماتية بمكتب التحقيقات الفيدرالى

---

(1) د/ أيمن عبد الحفظ عبد الحميد سليمان، الدور الفنى لأجهزة الشرطة فى مواجهة الإجرام المعلوماتى، مرجع سابق، صـ 20، أيضاً: مقدم/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، مرجع سابق، ص 192 وما بعدها.

(2) بدون، جرائم الحاسبات والإنترنت، الجرائم المعلوماتية، تاريخ الإنترنت ونشأة العالم الافتراضى، متاح على:

- Available At:http://adel-amer.catsh.info/vb/showthread.php?p=3967

(1) القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018.

(FBI) يضم داخله مجموعة من الأفراد المدربين على كيفية متابعة تلك الجرائم والتحرى عنها وضبطها والحفاظ على ما يتم تحصيله من أدلة[2].

ويتم استعراض اختصاصات تلك الإدارة وما طرأ عليها من تطور بعد أحداث الحادى عشر من سبتمبر ثم المقارنة مع أسلوب عمل أجهزة الشرطة المصرية، وذلك من خلال ما يلى:

اختصاصات إدارة مكافحة الجرائم المعلوماتية بمكتب التحقيقات الفيدرالى (FBI):

تتحدد اختصاصات إدارة مكافحة الجرائم المعلوماتية بمكتب التحقيقات الفيدرالى وفقاً لما يلى:

1- عند تلقى الإخطار بوقوع الجريمة يتم الانتقال إلى مكان ارتكاب الجريمة ثم يقوموا بالحصول على كافة المعلومات عن أسلوب العمل والتى يمكن أن تفيد فى كشف الجريمة وتحديد شخص مرتكبيها.

2- يقوم الفريق المكلف بالبحث والتحرى بتنظيم العمل داخله من خلال الآتى:

أ- تنظيم عملية الاتصال بين الأعضاء المختلفون للفريق ولذلك تبدأ عملية الاتصال قبل بدء عملية البحث.

ب- يتم وضع خطة بحثية مكتوبة توضح بالتفصيل كافة الأنشطة البحثية المتوقعة ويحدد فيها دور كل فرد بالفريق وكيفية التنسيق فيما بينهم.

ج- يقوم الفريق بعملية البحث فى الأنواع المختلفة من السجلات والتسجيلات التى لها صلة بالقضية والتى تتضمن بعض المعلومات الهامة مثل توثيق نظام الكمبيوتر ومعلومات تشغيله.

3- يتم الاستعانة بعملية المراقبة لتحديد الشخص المشتبه فيه إذا كان هذا الشخص من داخل المؤسسة أو المنشأة وذلك عن طريق الاستعانة بمجموعة من البرامج عالية الكفاءة فى اكتشاف مرتكب الجريمة.

4- يتم تصوير الأرقام المسلسلة للأجهزة وأرقام النموذج ومخطط بيان التوصيلات.

5- يتم تسجيل كافة المعلومات التى يتم العثور عليها فى أى من الوسائط المتعددة أو فى وحدات التسجيل الداخلية عند بداية ونهاية التحريات لإثبات عدم التسبب فى حدوث أى تلف لأى من الأدلة.

6- يتم تصوير كافة ما تعرضه شاشات الكمبيوتر.

7- يتم التمييز بين كافة الأدلة بحيث يمكن إعادة تجميع كافة الكبلات والأجهزة الأخرى.

---

(2) State v. Castagnola, 2013-Ohio-1215,https://cases.justia.com/ohio/ninth-district-court-of-appeals/26185.pdf?ts=1396138498

8- يتم تدوين وتسجيل كافة الوسائط المتعددة التى يتم العثور عليها فى موقع ارتكاب الجريمة.
9- إذا وجد فى مسرح ارتكاب الجريمة أجهزة الاستدعاءات الآلية فنجب مراعاة الآتى:
أ- عدم فصل التليفون أو المستدعى آلياً عن مصدره لتحديد هوية الأشخاص الداخلين على أجهزة الحاسبات الآلية وذلك فى حالة الجرائم التى ترتكب من خارج المكان الذى ارتكبت فنه الجريمة باستخدام شبكات الكمبيوتر.
ب- يتم توصيل مسجل الرقم الذى تم الاتصال به تليفونياً أو باستخدام المستدعى آلياً ويتم وضع هذا الرقم المخزن أو كود الدخول من خلال الذاكرة الداخلية.
ج- عقب الحصول على تلك الأرقام والأكواد يتم فصل التليفون أو المستدعى آلياً ويحتفظ به كدليل.
د- يتم فحص جميع الملفات الموجودة داخل الحاسب الآلى والمتعلقة بالجريمة ولكن لا يتم بحث تلك الملفات بالنظام الخاص بالجهاز التى ارتكبت عن طريقه الجريمة لأن فى ذلك خطورة كبيرة على صلاحية الدليل لذلك يتم استخدام النظام الخاص بفريق البحث والتحرى.

القواعد التى يتم مراعاتها عند التعامل مع الجرائم المعلوماتية:

يقوم فريق البحث والتحرى بمراعاة عدة أمور عند قيامه بالبحث والتحرى فى الجرائم المعلوماتية ومن أهم هذه القواعد ما يلى:
1- عند الانتقال إلى مسرح الجريمة يراعى عدم فصل الطاقة عن أجهزة الحاسب الآلى لأن فصل الطاقة قد يؤدى إلى مسح البيانات الموجودة على شاشة الحاسبات الآلية إذا لم يتم حفظها.
2- عدم تغيير وضع الأجهزة بأى طريقة وإبقائها على وضعها فى المكان التى وجدت فيه.
3- عند التعامل مع أى من الوسائط المتعددة يراعى البعد نهائياً عن المجالات المغناطيسية.
4- يراعى إرتداء فريق البحث للقفازات لعدم حدوث أى تلوث لتلك الوسائط مما يعرضها للتلف.
5- عدم إهمال أى أوراق قد توجد فى المكان وبالأخص ما يوجد فى سلة المهملات.

التطور فى عمل الشرطة الأمريكية بعد أحداث الحادى عشر من سبتمبر لسنة 2001م:

بدأ مكتب التحقيقات الفيدرالى بعد أحداث الحادى عشر من سبتمبر عام 2001 فى فتح آفاق جديدة تمكنه من مراقبة الاتصالات الإلكترونية لذلك طلب مكتب

(FBI) من الشركات تغيير أنظمتها لزيادة الدقة فى عمليات التنصت[1] من قبل أجهزة (FBI)، وأيضاً لإعطاء مساحة واسعة من الحرية لمراقبة الاتصالات الصوتية المرسلة عبر شبكة الإنترنت، هذا مع تأكيد إدارة الشرطة الأمريكية بأنها سوف تحرص دائماً على أن تكون التدخلات عند حالة الطوارئ فقط ولمدة محددة وفقاً لما تقتضيه الظروف، كذلك سوف تكون التدخلات دقيقة جداً كى لا يشعر المستخدمون بأن اتصالاتهم مراقبة.

وعلى الرغم من هذا التأكيد إلا أن حالة الرعب الذى فرضته أحداث الحادى عشر من سبتمبر جعلت المراقبة شبه دائمة مما جعل الأمر أشبه بتطبيق قانون طوارئ دائم على شبكة الإنترنت من حيث التنصت على المكالمات والاطلاع على كافة الرسائل التى يجريها الأشخاص حتى ولو تم استخدام برامج لتشفير المعلومات لتأمين الاتصالات فيتم فك تلك الشفرات عن طريق برامج متقدمة والاطلاع على مضمونها من قبل سلطات التحرى والبحث بمكتب (FBI)[2].

سادساً
المقارنة بين أسلوب عمل أجهزتى الشرطة المصرية والأمريكية

تنعقد أوجه المقارنة بين أسلوب عمل أجهزة الشرطة المصرية والأمريكية من خلال أوجه التشابه والاختلاف وفقاً لما يلى:

1- أوجه التشابه:

يتشابه التطور فى عمل أجهزة الشرطة فى كلا البلدين من خلال إنشاء إدارة متخصصة فى مجال مكافحة الجرائم الناشئة عن استخدام الحاسب الآلى مما يعكس مدى الاهتمام والحرص على مواجهة الصور الإجرامية المستحدثة فى كلا البلدين.

2- أوجه الاختلاف:

يختلف أسلوب عمل أجهزة الشرطة فى البلدين وهذا مرجعه إلى عدة أمور هى:

أ- وجود تشريع يجرم كافة صور الاعتداءات فى مجال الحاسب الآلى فى التشريع الأمريكى بعكس التشريع المصرى الذى لم يتناول أغلب تلك الاعتداءات مما يسهل عملية المواجهة فى الولايات المتحدة الأمريكية وحصرها فى جرائم معينة دائم

- [1]U.S. Supreme Court,United States v. White, 401 U.S. 745 (1971),United States v. White,No. 13,Argued November 10, 1969,Reargued October 20, 1970,Decided April 5, 1971,401 U.S.745,https://supreme.justia.com/cases/federal/us/401/745

[2] د/ أيمن عبد الحفظ عبد الحميد سليمان، الدور الفنى لأجهزة الشرطة فى مواجهة الإجرام المعلوماتى، مرجع سابق، صـ 22 وما بعدها.

جمهورية مصر العربية طبقاً لمبدأ الشرعية. إلا أنه حسناً فعل المشرع الجنائى المصرى بإصداره القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات[1] كخطوة جادة تعقبها خطوات أخرى. والقانون رقم 15 لسنه 2004 بشأن تنظيم التوقيع الإلكترونى و بإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات فى إبريل سنة 2004[2].

ب- وجود فريق متخصص فى مجال مكافحة تلك الجرائم داخل أجهزة الشرطة الأمريكية يمتلك المهارة التقنية التى تؤهله لمواجهة كافة ما يستجد من تلك الصور والعمل على تدريب ذلك الفريق بصفة دورية للارتفاع بالمستوى المهارى لديه على عكس أجهزة الشرطة المصرية التى لا يوجد بها هذا الفريق نظراً لحداثة إنشاء تلك الإدارة المتخصصة فى مجال مكافحة تلك الجرائم.

وعليه فإنه يتضح مما سبق أن عنصر الخبرة من قبل فريق البحث والتحرى في مجال الجرائم المعلوماتية له أهمية كبيرة لأن أى خطأ ولو يسير قد يؤدى إلى فقد الأدلة المترتبة على عملية البحث والتحرى[3]، وهذا لا يتوافر بدوره إلا بتحقيق ما يلى:

1- وجود نصوص تشريعية تجرم الأفعال التى تعد جرائم وتعالج القصور التشريعى فى مواجهة تلك الجرائم. على غرار القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

2- وجود فريق متخصص فى التعامل مع هذه النوعية من الجرائم.

3- يتم تدريب هذا الفريق على كيفية التعامل مع هذه النوعية من الجرائم لاكتسابهم عنصر الخبرة.

4- العمل على نشر شبكة اتصال بين الشركات والجهات الكبرى التى تعتمد على الحاسبات الآلية بأجهزة الشرطة بحيث يتم المتابعة من قبل أجهزة الشرطة ورصد أى محاولات للدخول والاقتحام ويكون ذلك فى حالة حدوث أى تدخل خارجى غير مرغوب فيه حتى يمكن التعامل الفورى مع هذا الدخيل عن طريق رصده وتحديد موقعه وضبطه[1].

---

[1] القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018.

[2] القانون رقم 15 لسنه 2004 بشأن تنظيم التوقيع الإلكترونى و بإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات فى أبريل سنة 2004، الجريدة الرسمية – العدد 17 تابع (د) فى 22 أبريل سنة 2004.

[3] يقول د/ جولييه: " إن التكنولوجيا مورد قادر على خلق الثروة، وهى وسيلة تتيح لمالكيها ممارسة السيطرة الاجتماعية، وهى عامل يشكل مؤثر وفعال لأساليب صنع القرار، وتتيح التكنولوجيا – بوصفها المورد الفريد والأكثر أهمية بين كل الموارد، اللازم لخلق موارد أخرى، وإن الخبرة التكنولوجية تمثل جواز مرور لسلطة صنع القرار، وتميل التكنولوجيا الحديثة بقوة إلى مركز القرارات، وهى توصل فضلاً عن ذلك للميادين المتضمنة لعمليات اتخاذ القرارات - أفضلياتها القيمية الخاصة، أى أنماط معينة من العقلانية، الكفاءة، ومن تفكيك الواقع إلى أجزاء قابلة للتفسير"... د/ جولييه، نظام الدعم الدولى لتلبية الحاجات الأساسية، كتاب حاجات الإنسان الأساسية فى الوطن العربى، الجوانب البيئية والتكنولوجيا والسياسات، ترجمة د/ عبد السلام رضوان، ط1، المجلس الوطني للثقافة والفنون والآداب، مطبعة السياسة (موسوعة عالم المعرفة)، الكويت، 1990، صـ 426.

[1] د/ أيمن عبد الحفظ عبد الحميد سليمان، الدور الفنى لأجهزة الشرطة فى مواجهة الإجرام المعلوماتى، مرجع سابق،

صـ 26 وما بعدها، أيضاً: د/ مفتاح بوبكر المطردى، المستشار بالمحكمة العليا الليبية، الجريمة الإلكترونية والتغلب على تحدياتها، مرجع سابق، صـ 48.

5- مع ضرورة احترام الخصوصية وإتخاذ الاجراءات القانونية عند التتبع و الضبط والتفتيش[2].

المبحث الثالث
دور جهاز الشرطة الدولية (الإنتربول) بشأن مكافحةالجرائم السيبرانيةالمستحدثة وتحقيق الأمن المعلوماتى

تمهيد:

لما كانت جرائم الإنترنت ذات صفه عالمية يمكن أن تتعدى آثارها عدة دول، فإن ملاحقة مرتكبيها وتقديمهم للمحاكمة، وتوقيع العقاب عليهم، يتطلب ضرورة التعاون فما بين الدول للقبض على المتهمين أو لجمع الأدلة أو سماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم المعلومات التى يمكن أن تساهم فى تحقيق ذلك، وهذا ما نصت عليه الاتفاقية الأوروبية لجرائم الإنترنت وأكدت عليه، لكونه أصبح يمثل إحدى الضرورات اللازمة لمواجهة هذه الأنشطة الإجرامية المستحدثة على نحو يتكامل مع دور القوانين الوطنية. وتجدر الإشارة إلى أنه لم يعد ينظر إلى ذلك التعاون باعتباره أنه يخلق " سيادة فوق الدول " بقدر ما أصبح يعني التعاون بين " سيادات

[2]The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." It is beyond dispute that a vehicle is an "effect" as that term is used in the Amendment. United States v. Chadwick, 433 U. S. 1, 12 (1977) . We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search" -United States v. Jones, 565 U.S. 400 (2012),https://supreme.justia.com/cases/federal/us/565/400/

دول مختلفة "، ترمي – جميعها – إلى تشييد وتفعيل حلقات مكافحة الجريمة بوجه عام، والجريمة عبر الوطنية بوجه خاص.

بصدور القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات[1]، حيث أولى للتعاون القضائى والأمنى أهمية كبيرة فى مكافحة الاجرام السيبرانى المستحدث، فقد نص فى المادة (4) منه على أنه: " تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها. على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن.

من صور هذا التعاون؛ التعاون القضائي (La coopération judiciare)، والذي من أهم صوره: التعاون الشرطي الدولي والمساعدة القضائية فى المواد الجنائية فى مجال مكافحة الجرائم العابرة للحدود ومنها جرائم الإنترنت. ويعد التعاون الشرطي الدول، كما سبق ذكره، من أهم صور التعاون الدولي فى مكافحة الإجرام بصفة عامة، والإجرام العابر للحدود لاسيما إجرام الإنترنت بصفة خاصة، ذلك لكونه منظم للدخول إلى مراكز المصادر التى تقدم المساعدات اللازمة فى مجال تقريب والبحث وتبادل المعلومات بين سلطات التحقيق المختلفة للدول وكذا التى تقوم بالتنسيق فى أعمال السلطات القمعية الدولية وفى تسهيل مكافحة الجرائم والانحرافات عن طريق تقديم حصيلة خبراتها إلى سلطات التحقيق لاسيما فما يتعلق بجرائم ضد الإنسانية، والأعمال الإباحية والتى هي من اختصاصها النوعي.

هذا من جهة، ومن جهة أخرى فإن أجهزة هذا التعاون تقوم بتحقيق الأهداف التى لا يمكن للشرطة الإقليمية بمفردها تحقيقها فى مكافحتها لإجرام الإنترنت والتى منها: تسهيل الدخول إلى المحتويات غير المشروعة المتواجدة فى إقليم دولة أخرى بناء على قرار قضائي واجب النفاذ، وتحديد مالكها أو مستخدمها، وملاحقة المشتبه فيه.

ولهذا التعاون أجهزة تقوم به، فما هي هذه الأجهزة التى تقوم بمكافحة الإجرام بصفة عامة والإجرام المعلوماتى بصفة خاصة على المستوى الدولى، ثم على المستوى الأوروبى[1]، على النحو التالى:

المطلب الأول

---

[1] القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018.

[1] أ/ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2007، صـ 147وما بعدها.

الوحدات المتخصصة فى مكافحة جرائم المعلوماتية
على المستوى الدولي

من أهم أجهزة التعاون الشرطي المكلفة بمكافحة الإجرام بصفة عامة، وإجرام الإنترنت بصفة خاصة " المنظمة الدولية للشرطة الجنائية " الإنتربول – (OIPC) التى تتخذ من باريس مقراً لها. وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون المتبادل بين سلطات البوليس فى الدول الأطراف على نحو فعال يحقق مكافحة الجريمة، وإقامة وتنمية النظم التى من شأنها أن تسهم على نحو فعال فى منع ومكافحة جرائم القانون العام. وهي تباشر ذلك أو تحقق ذلك من خلال وظيفتين: الأولى: هي القيام بتجميع كافة البيانات والمعلومات المتعلقة بالجريمة والمجرم، من خلال المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة فى أقاليم الدول الأعضاء. أما الوظيفة الثانية: فتتمثل فى التعاون فى ضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدولة التى تطلب تسليمهم. وهي فى ذلك متخصصة بمكافحة الجرائم ذات الطابع الدولي، وخاصة تلك المتعلقة بالعنف ضد الأشخاص والجرائم الواقعة على الأموال، وهي كذلك تختص بمكافحة الإجرام المنظم العابر للحدود بجميع صوره، بما فى ذلك المرتبط بجرائم الإنترنت وخاصة ذلك المتعلق بالاستغلال الجنسي للأطفال.

وفى هذا السياق نجد دعوة سكرتيرها " Raymound Kendall " فى مؤتمر جرائم الإنترنت المنعقد فى لندن فى 2000/10/9 – على ضرورة إيجاد تعاون دولي لمكافحة هذا النوع المتميز من الإجرام، وعلى ضرورة تقرير ذلك التعاون. وكذا مديرها التنفيذي للخدمات الشرطية، السيد لوبوتان فى المؤتمر الدولي السادس بشأن الجرائم المعلوماتية الذي عقد فى القاهرة مصر فى الفترة ما بين 13 إلى 2005/4/15 وهذا ما أكدته (الانتربول) كذلك فى إحدي مؤتمراتها الدولية التى عقدتها فى كوريا الجنوبية. وذات الشأن بالنسبة للمدير العام لمركز بحوث الشرطة الأسترالية "ACPR- " Des Berwick، إذ نجده يدعو إلى ضرورة القيام بالتحقيق فى الإجرام المعلوماتي الذي تستخدم فيه الشبكات العالمية، بطريقة متزامنة فى العالم أجمع. وتحقيقاً لذلك، فقد أنشأت المنظمة الدولية للشرطة الجنائية (الإنتربول) وحدة لمكافحة جرائم التكنولوجيا. هذا من جهة، ومن جهة أخري فهي تقوم بوضع استراتيجيات محكمة لمواجهة هذا النوع المستحدث من الإجرام بالتعاون مع المجموعة الثمانية (G8)، وذلك من خلال:

1- إنشاء مركز اتصالات أمني عبر الشبكة يعمل 24 ساعة و7 أيام على 7 أيام، على مستوى مصالح البوليس فى الدول الأطراف.

2- استخدام وسائل حديثة فى تلك المكافحة، كاستخدام تلك القاعدة من البيانات المركزية للصور الإباحية الممولة من قبل الدول الأطراف، والتى تستخدم برنامج " Excalibur " للتحليل والمقارنة الأوتوماتيكية لتلك الصور.

وإضافة إلى ذلك تقوم المنظمة بتزويد شرطة الدول الأطراف بكتيبات إرشادية حول جرائم الإنترنت وكيفية التدريب على مكافحاتها والتحقيق فيها، مثل ذلك الذي قدمته للشرطة الأوروبية والذي تم مناقشته فى اجتماع فى Poitiers والمسمي بدليل جرائم الحاسب الآلى " (Computer crime manual).

ومن بين هذه الإنجازات التى حققتها تلك الأخيرة فى ظل مواجهتها لإجرام الإنترنت، تلك العملية التى قامت لها المباحث الفيدرالية الأمريكية بالاشتراك مع الإنتربول، والمتعلقة بملاحقة الشخص الذي قام بنشر دودة الحب (love bug) عبر الإنترنت فى الفلبين[1]، أضف إلى ذلك العملية التى قامت بها شرطة الإنتربول بالاشتراك مع المباحث الفيدرالية الأمريكية وكذا الشرطة الإنجليزية، والتى أحرزت فيها إنجازات كبيرة عام 1998، والمعروفة بعملية " Cathédral " إذ حققت من خلالها تفكيك موقع منشور عليه أكثر من 75000 صورة سلبية لدعارة الأطفال، وكذا القبض على 107 شخص فى 12 دولة، وكذا تلك العملية التى تم القبض فيها على شاب ألماني بتهمة توزيع أحد الفيروسات، من خلال تنسيق الإنتربول بين المباحث الفيدرالية الأمريكية والشرطة الألمانية، وحققت من خلالها نتائج مبهرة من خلال تفكيكها لموقع منشور فيه صور إباحية بالاشتراك مع الأوربول 2005/5/2، ولقد أطلق على تلك العملية اسم عملية callidus، ولكن وبالرغم من تلك الإنجازات التى تحققها الإنتربول، فإن هناك سلبيات تعاني منها: كتلك المتعلقة بالبلاغات والمعلومات المحولة من دولة لدولة عن طريق السكرتارية العامة، إذ أنها تتسم بالبطء فى تحويلها.

هذا من جهة، ومن جهة أخرى تجدر الإشارة إلى أن نطاق اختصاصه المكاني محدد فى الدول التى لا تنتمي إلى الإتحاد الأوربي وذلك لانعقاد الاختصاص فيه لوحدات أخرى كالإنتربول وقنوات شنجن. وهكذا يتولى الإنتربول، إقامة العلاقات بين الدول المنضمة وتبادل المعلومات بين سلطات التحقيق فيها يتعلق بالجرائم

---

[1] ذلك أنه لا يجوز لسلطات التحقيق فى الدولة التى ارتكبت الجريمة على إقليمها، أو أضرت بأحد رعاياها أو بمصالحها الأساسية أن تباشر التفتيش أو غيره من إجراءات التحقيق خارج حدودها الإقليمية، وفى هذا الشأن قضت إحدى المحاكم الألمانية فى جريمة غش ارتكبت فى ألمانيا بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة فى سويسرا لا يتحقق إلا بطلب الحصول المساعدة من الحكومة السويسرية، وفى واقعة نشر فيروس (Love blog) عام 2000 الذى تسبب فى إتلاف المعلومات فى أجهزة الحاسب الآلى، فعندما اكتشف الخبراء الأمريكيون بأن هذا الفيروس أرسل من الفلبين فإن تفتيش منزل المشتبه فيه تقتضى تعاون السلطات الفلبينية والحصول على إذن من قاضى التحقيق بالفلبين.... د/ مفتاح بوبكر المطردى، المستشار بالمحكمة العليا الليبية، الجريمة الإلكترونية والتغلب على تحدياتها، مرجع سابق، صـ 39.

المتشعبة فى عدة دول كتلك المرتبطة بجرائم الإنترنت، ولاسيما تلك المتعلقة بالاستغلال الجنسي للأطفال[1].

من أهم وظائف ومهام الإنتربول:

أ- دور الإنتربول ودعمه لمنع المخاطر الإجرامية ومكافحتها:

قام الإنتربول بالسعي نحو منع المخاطر الإجرامية ومكافحتها، وهذا يتضح فيما يلي: بالإنتربول عدد 181 مكتب مركزي. استحدث الإنتربول تلك المنظومة الجديدة والتى يرمز إليها بـ 24/ 7-1 والتى من شأنها أنها تؤدي إلى اتساع نطاق الإمكانيات إزاء سرعة نقل المعلومات وبالتالى سهولة الاستخدام بالدخول المباشر عليها بالإنتربول للوقوف على ما تحويه من بيانات تتزايد والتى لعل أهمها توافر ما يلي: 66 ألف مجرم بالصورة وكذلك البصمة الخاصة بهم. 222 هارب مطلوب اعتقالهم فى 35 بلد فى عام 2004. أكثر من 6 مليون وثيقة سفر مسروقة. عدد 33000 ناقلات مسروقة بنسبة زيادة 25% أكثر من عام 2001. فى عام 2004 تم تزويد الشبكة بالـ DNA الدنا – البصمات الوراثية. هذا ولاختلاف التشريعات بين الدول ووسائل حماية الحياة الخاصة أدخل أكثر من 17 بلد النظام الناشئ بغية تجريبة. وجود 40 ألف من الوسائل التى تحمل البصمات للحكم وتحديد المجرم والتحقق من جنسيته.

ب- التعامل بين قواعد البيانات:

الواقع أن وجود مثل هذا التكامل بين قواعد البيانات التى تستتبع إمكانية الحكم على شخصية المجرم وبصفة عامة تبادل المعلومات وإدارة الأزمات, ودفع مجموعات العمل الميدانية التى تعتمد على سرعة الانتقال وممارسة الأعمال فى مواقع الأحداث, أن يضحى فى الإمكان تقديم المعلومات المطلوبة فى الوقت المناسب لإدارة الأزمة، وإزاء هذا التكامل إن أمكن مكافحة الإرهاب والمخدرات والبحث عن المجرمين فى جرائم شبكة الإنترنت عن طريق مركز التحكم والتنسيق، ولا مراء أن هذا سوف يساعد على سهولة الاتصال وتبادل الخبرات فى العمليات الواسعة التى تتضمن خدمات شرطية بين بلدان متعددة وبالتالى مباشرة القيام بوظائف إدارة الأزمات فى حالة وقوعها.

ج- التدريب :

* هناك برامج لتدريب الضباط لتلقينهم كيفية وسبل الاتصال، وأسلوب التعامل، بين المجرمين وكيفية السعي نحو معرفة وحصر المجرمين الجدد، لا سيما أن المجموعات التى تعمل ببرنامج التدريب، تسعى بالطبع دائماً نحو تجديد البرامج الخاصة بتحديد

[1] أ/ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات، مرجع سابق، صـ 147وما بعدها.

من يستخدم شبكة الإنترنت فى هذه التجارة للتعامل معه، على اعتبار أن المجرمين على شبكة الإنترنت لديهم الأساليب واللغة الخاصة بصدد التعامل فيما بينهم.
* هذا وتعمل تلك البرامج التدريبية على حصر عدد الأشخاص الذين يتعاملون أو حتي يساعدون على نشر هذه التجارة وقد أمكن تحديد عدد من يتعامل بها بل وتحديد مكانه، فضلاً عن تحديد هويته وعدد مرات ارتكابه للجريمة على حسب نوعها .... الإتجار بالمخدرات أو بالأطفال[1] أو الأسلحة، ومن أمثلة ذلك: ما تم بشأن استقطاب أحد تجار المخدرات من أحد غرف المحادثة العامة الـ Chat حيث قام أحد الضباط بالتعامل معه داخل غرفة محادثة خاصة لعدة مرات حيث تبين له من اللقاء الأول أن المجرم يقوم بتعاطي المخدرات وكذا الاتجار والتصنيع فأظهر الأخير رغبته فى شراء كمية كبيرة من مخدر Scazy الذي يقوم المجرم بتصنيعه وبالاتفاق على موعد ومكان التسليم تم ضبط المذكور ومعه شبكة كبيرة تعمل معه فى التصنيع والاتجار.
* هذا ويوجد أكثر من توقيع إلكتروني للكثير من المجرمين وذلك يمثل سجل إجرامي لهؤلاء المجرمين حيث يمكن عن طريقه ضبط المجرمين بمواقعهم أو إرسال عدد من الرسائل التحذيرية لهم للحد من نشاطهم الإجرامي[2].
وإلى جانب الإنتربول، توجد منظمات أخرى لها دور فعال فى معالجة إشكاليات مواجهة هذه الأنواع من الجرائم على المستوى الدولي، كمنظمة التعاون الاقتصادى والتنمية (OECD) ومجموعة الثمانية الاقتصادية التى قامت بإعداد ملتقى دولي مع منظمات دولية وبعض الدول (كمصر والصين) فى نهاية نوفمبر 2000 فى طوكيو، لتكوين قوة دولية تسمي " The digital opportunity task force " تتمثل مهامها فى تحقيق أمن تكنولوجيا المعلومات والإنترنت. ويجب التنويه فى هذه النقطة (مكافحة جرائم الإنترنت)، أنه وباستثناء المباحث الفيدرالية فإن منظمات الضبط القضائي حول العالم حتى الآن لا تتحرك إلا فى نطاقها الإقليمي. وعلى نمط الإنتربول، يوجد على المستوى الأوربي، مكاتب متخصصة لمواجهة الإجرام المنظم، والإجرام عبر الإنترنت خاصةً[1]، وسيتم تناولها على النحو التالى:

المطلب الثاني
الوحدات المتخصصة فى مكافحة جرائم المعلوماتية على المستوى الأوروبي

أولاً: الأوربول أو مركز الشرطة الأوربية:

[1] State v. Stefan, https://cases.justia.com/ohio/eighth-district-court-of-appeals/2018-104979.pdf?ts=1516907492
[2] د/ قدرى عبد الفتاح الشهاوى، قانون التوقيع الإلكتروني ولائحته التنفذية والتجارة الإلكترونية فى التشريع المصري والعربي والأجنبي، دار النهضة العربية، القاهرة، 2006، صـ 492 وما بعدها.
[1] أ/ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات، مرجع سابق، صـ 149وما بعدها.

الأوربول هو أحد الأجهزة المتواجدة على المستوى الأوربي، والتى تتخذ من لاهاي- هولندا مقراً لها وهي مكلفة بمكافحة الإجرام عن طريق: معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الإتحاد الأوربي، ودعم وتشجيع سلطات التحقيق وذلك بتكميل وسائلهم وتحديثاتها من أجل مكافحة جميع أنواع الإجرام المنظم الدولي الخطير[2]، وكذا بتسهيل تبادل تلك المعلومات عن طريق تزويد المحققين بتحاليل عملية واستراتيجية، ودعمهم بخبراته ومدهم بمساعداته التقنية.

وللأوربول دور فعال فى مكافحة جرائم الإنترنت، إذ نجده يقوم بتسهيل التحقيقات المرتبطة بوقائع بث أو امتلاك محتويات إباحية عبر الإنترنت بين الدول الأوربية. وتجدر الإشارة إلى أن ملفات التحليل الثرية بالمعلومات المبلغة من قبل سلطات التحقيق التابعة للدول الأطراف فى الإتحاد الأوربي تمثل وسيلة هامة فى عمل هؤلاء المحققين وفى مكافحتهم للشبكات الإجرامية، ومن أمثلتها: ملف تحليل الدعارة عبر الإنترنت. ولقد تم فى ذات السياق اجتماعات لمكافحة هذا النوع من الإجرام فى جوان 2001 فى لاهاي إلى جانب اجتماعات أخرى بمشاركة السلطات القمعية الألمانية، تحت عنوان: مكافحة الاستغلال الجنسي للأطفال.

ثانياً: الأورجست:

وإلى جانب الأوربول، يتواجد على المستوى الأوربي الأورجست، كجهاز يساعد على التعاون القضائي والشرطي فى مواجهة ومكافحة جميع أنواع الجرائم الخطيرة. وتنعقد اختصاصاته عندما يمس ذلك الإجرام دولتين على الأقل من أعضاء الإتحاد الأووربي أو دولة عضو مع دولة من دول العالم الثالث أو دولة عضو مع الرابطة الأوربية (Communate Europeene) وهي فى ذلك غير مقتصرة على الأشخاص فقط وإنما تشمل كذلك المؤسسات.

---

(2) هذا وفى كل الأحوال يفترض أن لا يكون الأمر بالتفتيش أمراً عاماً، وإنما يكون الهدف منه تحديداً دقيقاً وأن يتم وصف الأشياء المطلوب ضبطها بصورة تفصيلية، بحيث لا يترك ذلك للسلطة التقديرية لرجل الشرطة الذى سيقوم بتنفيذ الأمر، وأن لا يكون الأمر بالتفتيش لضبط الأشياء المتعلقة بالحياة الخاصة أو بالتعبير عن الرأى، ومنها أجهزة الحاسب الآلى – التى تحتوى بيانات شخصية أو بيانات تتعلق بالجريمة – فهذه الأجهزة يجب أن تكون موصوفة فى أمر التفتيش بصورة دقيقة فلا يصدر أمر بالتفتيش مثلاً لمجرد ظنون أو معتقدات توافرت لدى أحد رجال الشرطة بوجود صور فاضحة على الأسطوانات الصلبة لأحد أجهزة الحاسب الآلى، وهذا ما اقتضى أن يكون عضو جهة التحقيق ملماً ببعض الجوانب الفنية بالحاسب الآلى واستخداماته حتى لا تكون القرارات القضائية وسيلة لاصطناع الأدلة أو التسلط والاستبداد فى يد البعض، حيث أنه لا توجد وسيلة للتأكد من أن البيانات الموجودة على الأجهزة هى تلك التى تم ضبطها، إذا يمكن عن طريق الوسائل العلمية والتقنية الحديثة العبث بالبيانات الموجودة على الحاسب ومحوها. ففى الولايات المتحدة الأمريكية أصدر القضاء حكماً بتعويض شركة ستيف جاكسون التى تقوم بأعمال النشر، وكانت تصدر جريدة إلكترونية وتخضع للحماية المقررة بموجب قانون حماية الخصوصية وقانون حماية الاتصالات الإلكترونية، اللذان لا يجيزان القبض والتفتيش فى حق الناشرين ما لم يتوافر سبب آخر يرجح ارتكاب الشخص للجريمة، وتتلخص الواقعة فى أنه خلال شهر مارس عام 1990 قام البوليس السرى الأمريكى بتفتيش الشركة وضبط أجهزة للحاسب الآلى وملحقاتها ومجموعة من البرامج وطابعات الليزر وكمية من الأسطوانات وملفات خاصة بجريدة إلكترونية، وكذلك آلة حاسبة شخصية، ووضعت الأختام على المضبوطات فترتب على هذا الإجراء تعرض الشركة لأزمة مالية كبيرة فى الوقت الذى لم توجه أية إتهامات لصاحب الشركة أو لأى من العاملين معه، بل فى النهاية تبين أن التفتيش لم يكن متعلقاً به أو بعمله، وأن أحد العاملين بالشركة – والذى لم توجه له تهمة – كان الهدف من الاجراء، وكانت المعلومات المطلوب ضبطها موجودة بمنزله .... د/ مفتاح بوبكر المطردى، المستشار بالمحكمة العليا الليبية، الجريمة الإلكترونية والتغلب على تحدياتها، مرجع سابق، صـ 39 وما بعدها.

وتجدر الإشارة إلى أن الأورجست يمثل دعامة فى فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية، وخصوصاً فيما يتعلق بالأنشطة المرتبطة بجرائم الإنترنت. وهو فى ذلك على علاقة وثيقة مع الأوربول إذ يمدها بالتحليلات اللازمة للقيام بالتحقيقات فى الجرائم المنظمة. وهو يتكون من نواب عامين، ومستشارين ومأموري ضبط قضائي للدول الأعضاء فى الإتحاد الأوروبي ذوي الاختصاص والمندوبين من قبل كل دولة عضو فى الإتحاد وفقاً لنظامها القانوني.

وتتلخص نشاطاته فى: تحسين التنسيق والتعاون بين السلطات القضائية المختصة للدول الأطراف. تبادل المعطيات بين دول أعضاء الإتحاد الأوربي وكذا التحفظ عنها. كما يمكنه أن يطلب من الوكلاء العامين ذوي الاختصاص الوطني إجراء تحقيقات أو إجراء ملاحقات أو التبليغ عن الجرائم إلى السلطات المختصة للدول الأطراف.

ثالثاً: شنجن:

وإلى جانب الأورجست والأوربول، لقد تم إنشاء فضاء جماعي من غير حدود (espace communautaire sans frontière) سمي بشنجن (schengen) فى 1985/6/14 وعلى اتفاقية تطبيق تلك المعاهدة فى 1990/6/19[1]. وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوروبي لمواجهة التحديات الأمنية التى تفرضها الظروف الجديدة، ومنها جرائم الإنترنت، وتتمثل هاتان الوسيلتان فى مراقبة المشتبه فيهم عبر الحدود، وملاحقة المجرمين.

*** حق المراقبة عبر الحدود:**

وفقاً للمادة 40 من الاتفاقية السابقة، على رجل الشرطة فى إحدى دول schengen أن يستمر فى مراقبة شخص مشتبه فيه موجود على إقليم دولة أخرى طرف فى الاتفاقية وذلك فى إطار أعمال الاستدلال التى بدأ القيام بها كمأمور ضبط قضائي، للكشف عن تلك الجريمة.

ويخضع استعمال هذا الحق لعدة شروط، تختلف تبعاً لما إذا كانت المراقبة تتم فى الأحوال العادية أم أن هناك حالة ضرورة، إذ يشترط فى الحالة الأولى:

1- الحصول على إذن مسبق من الدولة المطلوب إليها السماح باستمرار مراقبة المشتبه فيه على أراضيها.

---

[1] أ/ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات، مرجع سابق، صـ 158 وما بعدها.

2- أن تكون الجريمة التى وقعت ويحتمل نسبتها إلى المشتبه فيه من الجرائم التى يجوز فيها تسليم المتهمين.

أما فى حالة الضرورة فالعكس: إذ يجوز لرجل الشرطة أن يتجاوز الحدود الإقليمية لدولته ويدخل إقليم دولة أخرى بدون إذن تلك الأخيرة، وتجدر الإشارة إلى أن ذلك لا يطبق إلا فى جرائم محددة على سبيل الحصر. ومن الإجراءات التى يجوز لمأمور الضبط القضائي القيام بها على إقليم دولة أخرى خلال عملية المراقبة: إجراء المعاينة اللازمة، وإقتفاء أثر المشتبه فيه، وأخذ صور شمسية وسماع الشهود إختياراً.

*** الحق فى ملاحقة المجرمين خارج الحدود الوطنية:**

قصرت المادة 41 من اتفاقية تطبيق معاهدة "Schengen " مجال تطبيقها على حالتين فقط، نظراً لما تمثله من قيد واضح على مبدأ السيادة الوطنية، وتتمثل هاتان الحالتان فى: حالة التلبس بإحدى الجرائم الجسيمة المحددة فى هذه المادة على سبيل الحصر، وفى حالة هروب شخص محبوس، فتجيز الاتفاقية فى الحالتين، لرجل الشرطة أن يتجاوز حدود دولته لملاحقة المجرم على إقليم دولة أخرى طرف فى الاتفاقية دون تصريح مسبق منها. مع الإشارة إلى أن بعض الدول الأطراف كألمانيا تعطي لرجال الشرطة هذه الحالة سلطة استجواب الشخص الملاحق والقبض عليه على غرار دول أخرى كفرنسا.

هذا من جهة، ومن جهة أخرى فقد نصت الاتفاقية على نظام لتسجيل المعلومات يسمي نظام معلومات شنجن " Le systeme d'information schengen " وهو يمثل قاعدة تكنولوجيا المعلومات المتعلقة بالأشخاص المطلوبين والأموال والأسلحة... التى يتم البحث عنها، كما يساهم ذلك النظام فى ملاحقة ومنع بث الصور الإباحية فى الدول الأطراف عبر الإنترنت. وتجدر الإشارة إلى أنه لتسهيل مهام هذا النظام، تم إبرام اتفاقية تعاونية بين الشرطة القضائية والجمارك فى فرنساوسويسرا فى مارس 1998.

يستخلص مما سبق تفصيله، أن استخدام الإنترنت على نطاق واسع فى تبادل المعلومات المالية وكذا التحويلات المصرفية، وما يتطلبه ذلك من الحفاظ على سرية

المعلومات الشخصية والبيانات تقتضي إنشاء شعبة بوليس للإنترنت سواء على المستوى الوطني أو الدولي، مهمتها تحديد ما يباح وما لا يباح عمله عبرها لمستخدم هذه الشبكة[1].

وفيما يلى التوصيات التى انتهى إليها المؤتمر الدولى السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة من 13 – 15 إبريل 2005م:

نظراً للتهديدات الموجهة ضد البنية التحتية الوطنية الحيوية من خلال إساءة استخدام التقنية الحديثة، فضلاً عن التهديد المتزايد الموجه للأنظمة المالية من خلال إساءة استخدام التقنية الحديثة من قبل جماعات الإجرام المنظم، أيضاً التهديد المتزايد الذى يفرضه الإرهاب المعلوماتى نتيجة استخدام الجماعات الإرهابية التقنية الحديثة فى الاتصال والدعاية والقيام بهجماتهم. يضاف إلى ذلك الحاجة الملحة لنشر الوعى بين الشرطة والجماهير والإدارة والصناعات الخاصة مع الحاجة للموارد المتاحة، فضلاً عن الحاجة للتبادل السريع للمعلومات ذات الصلة بإساءة استخدام المجرمين للتقنية الحديثة، أيضاً حاجة العالم للتدريب ووضع معايير قانونية وإجرائية قياسية.

فقد أوصى المؤتمر الدولى السادس للجرائم المعلوماتية بما يلى:

1- اعتبار اتفاقية المجلس الأوروبى بشأن الجرائم المعلوماتية بمثابة نموذج استرشادى لوضع معايير دولية قانونية وإجرائية لمكافحة الجرائم المعلوماتية، وأن يتم توزيع الاتفاقية على سائر الدول الأعضاء بالإنتربول باللغات الرسمية الأربعة بالمنظمة وتشجيع الدول للإنضمام للاتفاقية.

2- أن يقوم الإنتربول بتعزيز الجهود التى بذلها فى إطار مبادرة تعظيم معايير التدريب والتشغيل من أجل توفير المعايير الدولية اللازمة فى مجالات التفتيش عن الدليل الإلكترونى وضبطه والتحرى بشأنه.

---

[1] أ/ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات، مرجع سابق، صـ 162 وما بعدها.

3- يجب أن يظل التدريب والمساعدة الفنية من الأولويات الدولية لتعزيز الجهود المبذولة ضد الجرائم المعلوماتية بما فى ذلك إقامة دورات تدريبية ملائمة، بل وإقامة شبكة دولية بين معاهد التدريب والمتدربين بلغة تحقيق الاستخدام الأمثل للأدوات والبرامج المتاحة، مثل فصول الإنتربول المتنقلة ونماذج التعليم الإلكتروني، وذلك كله شريطة أن تتضمن مبادرات التدريب والمساعدة الفنية قطاعات متعددة وتشتمل على الشراكة بين القطاعين العام والخاص.

4- العمل على بدء تطوير وتعاون واتصال حيوي بين المؤسسات الدولية والكيانات الوطنية العامة فى مجال مكافحة الجريمة المعلوماتية.

5- تجميع المعلومات ذات الصلة بقضايا الجرائم المعلوماتية فى قاعدة بيانات منظمة الإنتربول على أن يتم نشرها فى صورة نواتج محللة من أجل مساعدة الدول الأعضاء على إنتاج استراتيجيات المنع المناسب.

6- تكوين مجموعات عمل لمنظمة الإنتربول تعني بجرائم تكنولوجيا المعلومات فى سائر الأقاليم التى لا توجد بها فى الوقت الحالى مثل هذه المجموعات، مع ضرورة الاستفادة من الخبرات المتوافرة لدى المجموعات القائمة حالياً من أجل دعم إنشاء مثل هذه المجموعات الجديدة[1].

المبحث الرابع
مقترحات تطوير الدور الأمنى لجهاز الشرطة بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى

تمهيد:

يقصد بالقرصنة على البرمجيات التعدي على الحقوق الفكرية الواقعة على برامج الكمبيوتر وقواعد البيانات سواء الأدبية مثل عدم نسبتها لمبرمجها أو المادية باستغلالها دون الحصول على تصريح من مالكها[1].

---

[1] د/ قدرى عبد الفتاح الشهاوى، قانون التوقيع الإلكتروني ولائحته التنفيذية والتجارة الإلكترونية فى التشريع المصري والعربي والأجنبي، مرجع سابق، صـ 499 وما بعدها.

[1] وقد أسفرت حملات وزارة الداخلية فى محافظات مصر عن الآتى: فى محافظات القاهرة أسفرت تلك الحملات التى أجرتها بالفنادق الكبرى عن ضبط فرعين لأحد الفنادق المعروفة لاستخدامها برامج كمبيوتر منسوخة، وفى محافظة الجيزة، أسفرت الحملة عن ضبط شركة كبيرة تتعامل فى مجال تداول الأوراق المالية ولديها ستة عشر جهاز حاسب آلى محملة بالبرامج المنسوخة وفى محافظة البحر الأحمر وفى مدينة الغردقة أسفرت الحملة عن تحرير الكثير من المحاضر لفنادق وقرى سياحية تستخدم البرامج المنسوخة، وفى مدينة مرسى مطروح أسفرت الحملة عن تحرير محضر لشركة

وللقرصنة المعلوماتية أشكال وصور عديدة منها: نسخ البرامج الأصلية الخاصة بالمؤسسات: ويقصد بذلك شراء برامج أصلية وتحميلها على عدد من الأجهزة أكبر من المصرح باستخدامه أو زيادة عدد مستخدمي الأجهزة الخادمة عن العدد المصرح به. كما من أشكال القرصنة المعلوماتية تحميل الأجهزة ببرامج منسوخة أثناء تجميعها: ويقصد بذلك تجميع أجهزة الكمبيوتر وتحميلها ببرامج مقلدة ومنسوخة وبيعها دون تسليم التراخيص الدالة على أصالتها. أيضاً من صور القرصنة المعلوماتية الاستغلال غير المشروع للإصدارات الخاصة من البرامج الأصلية: حيث أدت فكرة المواءمة بين مصلحة منتج البرمجيات وحق المجتمع فى استخدام التكنولوجيا إلى ظهور إصدارات من البرامج تخصص لفئة معينة مراعاة لظروف خاصة بتلك الفئة سواء اجتماعية أو جغرافية وغالباً ما تكون بأسعار رمزية رخيصة مثل الإصدارات المخصصة للطلبة أو تلك المخصصة للاستخدام المنزلي ويعتبر بيع تلك الإصدارات للاستخدام التجاري مخالفة لشروط التعاقد.

ومن صور القرضنة المعلوماتية: نسخ البرامج على أسطوانات وبيعها: وهو عبارة عن طريقتين: أولاً: نسخ المحتوى البرمجي فقط، ويقصد به تحميل البرنامج على أسطوانة والاكتفاء بكتابة اسم البرنامج عليها فقط وهو تقليد مفضوح للمشترى. ثانياً: نسخ المحتوى وتقليد الشكل الخارجى ووضع العلامة التجارية للشركة المنتجة وتكمن خطورته فى كون المشترى يعتقد أنه يتعامل فى برمجيات أصلية.

ومن صور القرصنة المعلوماتية إتاحة البرامج للتداول عبر شبكة الإنترنت دون موافقة أصحاب الحقوق عليها: وذلك بتعطيل التقنية التى يضعها المنتج لحمايتها بإتاحة البرمجيات التى تقوم بتوليف مفاتيح الإنزال "key generator" أو ملفات التنشيط المعروفة "crack tools" ووضعها على المواقع وإتاحتها للكافة بمقابل مادى أو بدون.

ومن صور القرصنة المعلوماتية استخدام البرمجيات المقرصنة فى التعدى على القنوات الفضائية المشفرة عبر شبكة الإنترنت "الشيرنج" بقيام القرصان باستخدام برمجيات خاصة لإتاحة مفاتيح فك شفرة القنوات الفضائية المشفرة ومنحها لزبائنه مقابل تحصيل مبالغ مالية منهم[1].

هذا ويتمثل الدور الأمنى فى مجال حماية برامج الحاسب الآلى فى مكافحة تقليد أو نسخ البرامج واستعمال البرامج المقلدة أو المنسوخة وهو ما يطلق عليه مكافحة قرصنة البرمجيات Software Piracy وتتخذ مجموعة من الإجراءات الأمنية فى هذا الصدد والموضحة فى ثلاث صور: أولاً: الإجراءات السابقة على

للمقاولات والرسومات الهندسية تستخدم برامج "أوتوكاد" منسوخة فى مباشرة أعمالها... أ/ محمد يوسف محمد، التحديات التى تواجه التحقيقات فى الجرائم، مرجع سابق، هامش صـ 20.

[1] أ/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، مرجع سابق، ص180.

تدخل السلطة القضائية وهى الإجراءات التى تقوم بها الأجهزة الأمنية المختصة بهدف ضبط البرامج المقلدة والمنسوخة وتعد محاضر جمع الاستدلالات التى تحررها هذه الأجهزة بناء على ما تجريه من تحريات وكذا المحاضر التى يحررها المتضررون من أهم صور الحماية فى هذه المرحلة. ثانياً: الإجراءات الأمنية المعاصرة لعمل السلطة القضائية وتتمثل فى ضبط البرامج المقلدة أو المنسوخة تنفيذاً لأمر وقتى صادر من المحكمة والتحفظ عليها لحين الحكم فى الدعوى الموضوعية. ثالثاً: الإجراءات الأمنية التالية لعمل السلطة القضائية وتتمثل فى التصرف فى هذه البرامج تنفيذاً لحكم المحكمة وذلك بالمصادرة [2] أو الإتلاف[3].ويتناول الباحث فيما يلى: معوقات الدور الأمنى فى مواجهة جرائم المعلوماتية فى مطلب أول، ثم التحديات التى تواجه مكافحة الإجرام المعلوماتي على الصعيدين الوطني والدولي فى مطلب ثان، ثم مقترحات مواجهة التحديات الأمنية فى مواجهة جرائم المعلوماتية فى مطلب ثالث، على النحو التالى:

المطلب الأول
معوقات الدور الأمنى فى مواجهة جرائم المعلوماتية

بدايةً لن يتهيأ للنصوص التشريعية أن تحقق وحدها الأهداف المرجوة منها مهما بلغت قوة الحماية المستمدة منها دون بذل الجهد لتنفيذها، ومن ثم يتمثل الدور المنوط بأجهزة الأمن فى هذا الصدد فى التصدى لقراصنة البرامج بهدف القضاء على التجارة غير المشروعة لبرامج الحاسب المقلدة أو المنسوخة بما تمثله من مخاطر على بيئة الأعمال فى الدولة[1].

بالإضافة إلى ذلك فإنه يتطلب الأمر توحيد الجهة المسئولة عن تطبيق ومتابعة الأمن المعلوماتى الحكومى، لتكون عبر الحكومة الإلكترونية، فضلاً عن ضرورة حصول الأجهزة الحكومية على الشهادة الدولية (الآيزو) (ISO/ IEC

---

[2] المصادرة هى نزع ملكية المال على مالكه وإضافته إلى ملك الدولة بغير مقابل. ومناطها أن تكون الأشياء مضبوطة وقت الحكم بالمصادرة، ويستوى فى ذلك أن تكون الأشياء المضبوطة تحت يد المحكمة أو النيابة العامة أو الشرطة، وتشمل الأشياء التى تجوز مصادرتها: الأشياء التى تحصلت من الجريمة كحصيلة ألعاب القمار، وحصيلة ترويج النقود المزيفة، كما تشمل الأشياء التى استعملت فى ارتكاب الجريمة كالأسلحة والآلات، أيضاً الأشياء التى من شأنها أن تستعمل فى الجريمة، وهى تلك الأشياء التى أعدها الجانى لاستعمالها فى الجريمة ثم وقف فعله عند حد الشروع. وكل ما يشترط فى هذه الأشياء جميعها أن تكون قد ضبطت بالفعل، ومتى كان الشيء مضبوطاً فلا يمنع من المصادرة أن يكون الشيء قد بيع بواسطة النيابة العامة عند ضبطه طبقاً للمادة 109 إجراءات، وفى هذه الحالة ترد المصادرة على ثمنه. ويشترط أن تقتصر المصادرة على الأشياء المضبوطة التى تكون محلاً للجريمة فى الأحوال التى تقتصر فيها المصادرة على ذلك، ولا تكون الأشياء خارج دائرة التعامل. والمصادرة جائزة فى الجنايات والجنح فقط، وبدون الحاجة إلى نص خاص اكتفاء بالنص العام المبين فى المادة 30 عقوبات، أما المخالفات فلا يجوز فيها المصادرة إلا حين ينص القانون صراحة على ذلك .... د/ أحمد فتحى سرور، قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، ط6، 2015، ص 1004 وما بعدها.

[3] د/ فؤاد جمال الدين، التطور التشريعي لحماية البرمجيات مع إشارة خاصة لمصر، ندوة المواجهة الأمنية للجريمة المعلوماتية, مركز بحوث الشرطة، أكاديمية الشرطة، أبريل، 2009, صـ 7.

[1] د/ فؤاد جمال الدين، المرجع سابق, صـ 8 وما بعدها.

27001) فى ذلك المجال، مع إنشاء مركز للتميز فى الأمن المعلوماتى كالموجود بالمملكة العربية السعودية، وقد حصلت بعض المنظمات السعودية الخاصة على الشهادة الدولية لهذا المعيار، إلا أنه ما زالت المنظمات الحكومية فى مجال الأمن المعلوماتى للمواقع الإلكترونية تسير ببطء فى حصولها على شهادة الآيزو[2]، وكانت وزارة العدل السعودية أول قطاع حكومى يحصل على الآيزو العالمية لإصدار 2013 (ISO/ IEC 27001:2013) فى أمن المعلومات، وذلك فى 10يناير 2015 [3]، كما حصل مركز المعلومات الوطنى السعودى كثانى قطاع حكومى على شهادة الآيزو لإصدار 2013 (ISO 27001:2013) فى أمن المعلومات [4].

ويصطدم الدور التنفيذى لأجهزة الأمن فى شأن حماية برامج الحاسب الآلى ببعض المعوقات التى نستعرضها فيما يلى مشيرين إلى تجارب الدول الأخرى فى هذا المجال بما يساعد على تقديم اقتراحات فعالة للتغلب على هذه المعوقات، على النحو التالى:

1- ضعف الوعى بقضية حماية حقوق الملكية الفكرية بوجه عام وحماية برامج الحاسب الآلى بوجه خاص:

مما لا شك فيه أن ما يطلق عليه ثقافة الملكية الفكرية من الأمور المغيبة فى مصر شأنها فى ذلك شأن سائر الدول النامية وإذا كان هذا هو الشأن فى تلك القضية بوجه عام فإنها أكثر وضوحاً فيما يتعلق ببرامج الحاسب الآلى نظراً لحداثتها من ناحية ولعجز كثيرين – ليس من العامة فحسب بل من المتخصصين أيضاً – عن الاقتناع بأن برنامج الحاسب يعد من قبيل المصنفات الأدبية من ناحية أخرى.

ومازال الكثيرون يتساءلون حتى الآن عن العلاقة بين برنامج الحاسب والكتاب أو قطعة الموسيقى ولماذا لا تتم معاملة البرنامج باعتباره اختراعاً تتم حمايته بنظام براءات الاختراع؟ حقيقة أن هذا الأمر قد تم حسمه باتفاقية "التريبس" والتزام الدول الموقعة عليها – ومنها مصر – بتعديل تشريعاتها للتوافق مع نص المادة العاشرة من الاتفاقية التى أسبغت على برامج الحاسب الحماية المقررة للمصنفات الأدبية ولكن تبقى العقبة الأساسية فى كيفية إقناع الأشخاص الذين يتعاملون مع هذه البرامج بتلك الحقيقة.

---

[2] وقد قامت المنظمة الدولية للمعايير (ISO) بتبنى معيار موحد لرسم وتحديد السياسات الأمنية للمعلومات (BS 9977)، والذى ظهر بعده عدة معايير كان آخرها (ISO 27001) ... د/ عمر بن محمد العتيبى، الأمن المعلوماتى فى المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة مقدمة استكمالاً لمتطلبات الحصول على درجة دكتوراه الفلسفة فى العلوم الأمنية، قسم العلوم الإدارية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 1431 هـ، 2010م، صـ 1 وما بعدها.

[3] بدون، متاح على: - www.al-madina.com/node/582132

[4] بدون، متاح على: - www.moi.gov.sa

ومن ثم فمن المناسب أن نشير هنا إلى تجربة إحدى الدول المتقدمة فى مجال التكنولوجيا وهى اليابان ففى التقرير السنوى لإتحاد منتجى برامج الكمبيوتر (BSA) Business Software Alliance عام 1995 قدرت خسائر اليابان من جراء قرصنة البرامج بـ 101 بليون دولار.

ومن هنا ثار التساؤل عن كيفية تطبيق قوانين حماية الملكية الفكرية والتعاون بين الأجهزة الحكومية والمؤسسات الصناعية فى هذا الخصوص والحقيقة أنه يمكن أن يطلق على التجربة اليابانية فى هذا الخصوص تجربة "إنشاء وعى شعبى مضاد لعمليات القرصنة" حيث قامت أجهزة الإعلام بدور فعال فى إيضاح الصورة لدى الناس وما يؤدى إليه استخدام البرامج المنسوخة أو المقلدة من أضرار بالاقتصاد اليابانى مما ترتب عليه تقليص الخسائر فى السنوات التالية ولقد كان دور التوعية واقعياً حيث فرق بين قيام شركات أو مجموعات بنسخ وتزوير البرامج وبين الأفراد الذين يقومون بعملية نسخ لإهدائها لأصدقائهم أو لاستخدامهم الشخصى. وقد قام مركز المعلومات ودعم اتخاذ القرار بدور فعال بخصوص نشر الوعى الخاص بمكافحة قرصنة البرمجيات من خلال التعاون مع الجهات المعنية وممثليها فى مصر لتنظيم مؤتمرات وندوات فى هذا الموضوع.

2- ارتفاع أسعار البرامج الأصلية:

من أهم المعوقات فى طريق مكافحة قرصنة البرمجيات إرتفاع أسعار البرامج الأصلية فإن نشر الوعى الخاص بحماية الملكية الفكرية فى هذا الخصوص لن يجدى نفعاً مع عدم قدرة الكثيرين على استخدام البرامج الأصلية بسبب إرتفاع أسعارها. وحلا لهذه المشكلة فقد حدث مؤخراً اتفاق بين الحكومة المصرية وعدة شركات عالمية منتجة للبرمجيات سيكون له تأثير إيجابي على الحد من ظاهرة القرصنة فى مجال برامج الحاسب الآلى إذ تسمح هذه الاتفاقية لجميع المؤسسات والهيئات الحكومية بالحصول على ترخيص استخدام برامج هذه الشركات بتكلفة مخفضة مما يؤدي إلى ترسيخ استخدام البرامج الأصلية كسلوك حضاري.

3- عدم كفاية الإجراءات التنفيذية المساندة للدور الأمني فى محاربة القرصنة:

مما لا شك فيه أن النقص فى الإجراءات التنفيذية الخاصة بمكافحة قرصنة البرمجيات يشكل معوقاً أساسياً أمام الدور الأمني فى هذا الخصوص، وسوف نعرض فى إيجاز لتجارب بعض الدول بهذا الشأن مما ساعد على خفض نسبة الخسائر الناتجة عن القرصنة إلى حد كبير:

الاتحاد الأوروبي: وافق الاتحاد الأوروبي فى مايو 2000 على تقرير يتضمن إجراءات مباشرة ضد السرقات المنتشرة بشكل واسع فى دول الاتحاد للأعمال التى

تحتوي على ابتكار ومنها برامج الحاسب الآلى[1]، وقد عهد بتنفيذ هذه الإجراءات إلى لجنه خاصة لمكافحة التزييف والقرصنة على هذه الأعمال وأعطيت اللجنة صلاحيات واسعة لاتخاذ ما تراه مناسباً من إجراءات رادعة وفقاً للظروف.

الولايات المتحدة الأمريكية: عزز الموسم الرئاسي لمقاومة السرقات الإلكترونية وتعزيز حماية حق المؤلف Digital Theft Deterrence and copyright Damages Improvement Act من التعويضات المدنية المقررة على انتهاك حقوق المؤلف بالنسبة للأعمال ذات الصبغة الابتكارية ومنها برامج الحاسب، مثال ذلك زيادة الحد الأقصى للتعويض عن العمل الذي انتهك فى الدعاوى المدنية من 10.2 مليون دولار إلى 15.3 مليون دولار.

وفى ولاية كولورادو الأمريكية: صدر أمر تنفذي فى مارس 2000 (EO) Executive Order بخصوص القرصنة على برامج الحاسب ويطبق هذا الأمر ليس فقط على جميع الأجهزة الحكومية فى الولاية وإنما أيضاً على الأطراف الأخرى Third Parties التى تقوم بالعمل فى إطار أو بالتعاون مع الأجهزة الحكومية، ويلزم هذا القرار جميع تلك الجهات باستخدام النسخ الأصلية والمرخصة من البرامج كشرط للتعامل مع الجهات الأخرى.

اليابان: أكد مشروع القانون الياباني لحماية حقوق المؤلف على ضرورة قمع القرصنة المنظمة. وهناك اتجاه إلى تعديل قانون الإجراءات المدنية Civil Proceeding Act لمنع المحاكم الحق فى إلزام المشتبه فى قيامهم بأعمال اعتداء على حقوق المؤلف بتقديم سجلات خاصة لغرض حساب الأضرار الناشئة عن هذه الاعتداءات ولتمحيص إدعاءات القرصنة.

الصين: فى إبريل عام 1992 خططت الصين خطوة هامة نحو مواجهة قرصنه البرامج وذلك بإصدار مرسوم يعكس رغبة الحكومة فى إيقاف هذه القرصنة المنتشرة بشكل واسع فى المجتمع الصيني، وذلك بإلزام الأجهزة الحكومية بألا تستخدم سوى البرامج الأصلية المرخصة.

من بين الدول العربية: تم حذف كل من الأردن والإمارات العربية المتحدة من لائحة الدول الخاضعة للمراقبة التى تضمنها الدائرة التجارية الأمريكية USTR، وقد نشر هذا الخبر فى التقرير السنوي التابع للبند الخاص Special 301 الذي أصدرته دائرة USTR فى شهر فبراير 2001 وذلك لإحرازها تقدما ملموساً فى مجال الحد من قرصنه البرامج، وورد بالتقرير أن الدولتان ركزتا جهودهما على البنية التحتية وإقامة

---

[1]Dommages-intérêts à payer par les membres mineurs du forum Utopi-Board, JEUDI 10 JANVIER 2019, https://www.legalis.net/actualite/dommages-interets-a-payer-par-les-membres-mineurs-du-forum-utopi-board/

بيئة تشجع القطاع المعلوماتي، بينما بقيت العديد من دول الشرق الأوسط بما فيها مصر وتركيا مدرجتان فى التقرير التابع للدائرة[1].

هذا وقد طالب المؤتمر الأول لأمن المعلومات الإلكترونية الذى أقيم فى مسقط 2005 [2] بإصدار دليل موحد للمعايير المتعلقة بأمن المعلومات فى برامج الحكومة الإلكترونية ودعا الدول العربية لبناء أنظمة إنذار مبكر لمواجهة كل أشكال الجريمة المعلوماتية ذات التأثير على المستوى الوطنى، على أن يقوم مجلسا وزراء الداخلية والعدل العرب بتسهيل تبادل المعلومات المتعلقة بجرائم الإنترنت والشبكات من خلال تنظيم ورش عمل متخصصة فى هذا الإطار، كما طالب المؤتمر بناء على سياسة أمن معلومات قابلة للتحديث بشكل دورى لملاحقة التطورات العلمية فى هذا الإطار للحفاظ على الاستثمار فى قطاع تكنولوجيا المعلومات[3].

4- نقص الكفاءات المتخصصة فى محاربة هذا النوع من القرصنة:

إن مكافحة قرصنة البرمجيات تحتاج إلى مهارات خاصة نظراً لحداثتها ولارتباطها بالنواحي الفنية حيث يستلزم الأمر التعامل مع قراصنة على أعلى مستوى من المهارة التقنية فلا يكفى الإجراءات التقليدية التى تقوم بها إدارة المصنفات الفنية لضبط النسخ الواضحة التقليد والغير مرخصة وإنما لا بد بالإضافة إلى ذلك من تنمية المهارات القائمين بهذا العمل[1].

ومن هنا تأتى أهمية دور الخبراء فى الاستعانة بهم وكفاءاتهم بشأن مكافحة الجرائم السيبرانية[2]، وحسناً فعل المشرع الجنائى المصرى حيث ضمن القانون رقم

---

[1] د/ فؤاد جمال الدين، التطور التشريعي لحماية البرمجيات مع إشارة خاصة لمصر، مرجع سابق, صـ 8 وما بعدها.

[2] المؤتمر الدولي لأمن المعلومات الذي نظمته بلدية مسقط بالتعاون مع المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية، 2005/12/22، متاح على:
http://www.albayan.ae/economy/2005-12-22

[3] وقد قامت المنظمة الدولية للمعايير (ISO) بتبنى معيار موحد لرسم وتحديد السياسات الأمنية للمعلومات (BS 9977)، والذى ظهر بعده عدة معايير كان آخرها (ISO 27001) ... د/ عمر بن محمد العتيبى، الأمن المعلوماتى فى المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، مرجع سابق، صـ 3 وما بعدها.

[1] د/ فؤاد جمال الدين، التطور التشريعي لحماية البرمجيات مع إشارة خاصة لمصر، مرجع سابق, صـ 8 ومابعدها.

[2] هذا ويعد الطب الشرعي الرقمي أحد الكفاءات الرئيسية في مواجهة المخاطر المتزايدة للجريمة السيبرانية، بالإضافة إلى التحقيق الجنائي. بالنظر إلى تكنولوجيا المعلومات الحديثة - وطرق التكنولوجيا الحديثة - يتم جلبها عبر الإنترنت، حيث يواجه الباحثون والممارسون بانتظام تحديات تقنية جديدة، مما يجبرهم على تطوير مهاراتهم في التحريات بشكل مستمر....
DR.ANDRÉ ÅRNES, Digital forensics,Publisher: Wiley; 1 edition (July 24, 2017)
https://www.amazon.com/Digital-Forensics-Andr-eacute-Aring/dp/1119262380/

175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات[3]، نص خاص بالخبراء؛ حيث ورد فى المادة (10) منه على أنه : "ينشأ بالجهاز سجلان لقيد الخبراء، يقيد بأولهما الفنيون والتقنيون العاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به . وتطبق على الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء . واستثناء من تلك القواعد، تسري على الخبراء المقيدين بالسجل الثاني القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وجد . وتحدد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد في كل من السجلين."

هذا وتأتى أهمية الخبرة أنها تبدو ضرورية عند استخدام وسائل فنية فى ارتكاب الجريمة مثل الكمبيوتر، كما ينحصر مجال الخبرة فى المسائل الفنية أو العلمية، فلا يجوز للخبراء أن يتطرقوا إلى المجالين القضائى أو القانونى[4].

وقضت محكمة النقض بأن إدانة محكمة الموضوع للطاعن دون التعرض إلى تقرير الخبير الذى ندبته المحكمة تحقيقاً لدفاعه أو الإشارة فى مدونات الحكم إلى أسباب عدولها عن تحقيق دفاع رأت جديته يكون حكماً معيباً[5]. وقضت محكمة النقض أيضاً بأن عدم إيراد نص تقرير الخبير بكامل أجزائه لا يعيبه[6]. كما قضت بأن تقدير آراء الخبراء، والمفاضلة بين تقاريرهم موضوعى للمحكمة الأخذ بالتقرير الذى تطمئن اليه والالتفات عما عداه[1]. وقضت أيضاً بأن الجدل الموضوعى في تقدير الدليل، غير جائز أمام محكمة النقض[2].

وقد تثور الصعوبة حول الحدود الفاصلة بين المسائل القانونية التى تختص المحكمة بالفصل فيها والمسائل الفنية التى يختص بها الخبراء، وقد قضت محكمة النقض الفرنسية أن الاستعانة بأستاذ فى القانون البحرى فى تحليل مختلف العقود والاتفاقيات بين الأطراف واستخلاص وظائف مختلف العاملين من أجل تمكين القاضى من تقدير طبيعتها ونطاق المسئوليات المترتبة على غرق السفينة يعد تكليفاً بمهمة فنية مما يدخل فى أعمال الخبرة[3].

المطلب الثانى
التحديات التى تواجه مكافحة الإجرام المعلوماتي
على الصعيدين الوطني والدولي

---

(3) القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر ج فى 14 أغسطس سنة 2018.

(4) د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص 557 وما بعدها.

(5) الطعن رقم 4301 لسنة 71ق، جلسة 2007/3/28، س 58، غير منشور.

(6) الطعن رقم 1381 لسنة 67ق، جلسة 1999/1/4، مجموعة القواعد، س50، ق2، ص16

(1) الطعن رقم 19675 لسنة 67ق، جلسة 1999/10/5، مجموعة القواعد، س50، ق116، ص514

(2) الطعن رقم 6048 لسنة 64ق، جلسة 1996/2/18، مجموعة القواعد، س47، ق37، ص222

(3) Crim 9 juill 2003, Bull, n° 137 -

إن التحديات التى أضحت تواجه الدول بل والعالم بأسره من أجل مكافحة الإجرام المعلوماتي قد أجبر الدول عامة على ضرورة السعي نحو تعاظم بدايات التعاون فيما بينها للتصدي لمثل هذا الإجرام المنظم والمتزايد، والذي يواكب التطور التكنولوجي، فضلاً عن إعداد أنظمة ضبطية وقضائية مؤهلة للتعامل مع الجرائم المعلوماتية[4]، حيث عكفت الدول على تأكيد وتعظيم هذا السعي لاسيما بعد إنهيار عصر الحرب الباردة فى سباق التسلح، وقد كان من ثمار ذلك أن أصدر السيد وزير الداخلية فى جمهورية مصر العربية قراراً بإنشاء إدارة متخصصة لمكافحة جرائم الحاسبات وشبكات المعلومات وذلك بتاريخ 2002/7/7، ولا مراء أن هذا القرار ينطوي على حس أمني مستقبلي واعد لمواكبة ازدياد تطور وتزايد استخدام شبكة الإنترنت حيث تم وضع خطة عمل كان من أهم بنودها:

1- السعي نحو ضبط ومكافحة الجرائم المعلوماتية بشتي صورها وأنماطها.

2- العمل على تقديم المساعدات الفنية والأدلة المادية فى محاولة متعاظمة لضبط الجرائم المتعلقة بشبكة الإنترنت وذلك لكافة الأجهزة الشرطية النوعية الأخرى والنيابة العامة.

3- استمرارية متابعة ما يجري على شبكة الإنترنت من جرائم لا سيما تلك التى انتشرت محافظات مصر المختلفة.

4- التأكيد على تأمين جميع الشبكات الخاصة بوزارة الداخلية.

5- وإزاء تكاتف تلك الجهود استطاعت إدارة مكافحة جرائم الحاسبات بجمهورية مصر العربية بضبط عدد 62 قضية من بينهم عدد ثمانية قضايا كان للشرطة الدولية دور متعاظم فيها[1].

وهذا ومن بين التحديات سواء المحلية أو الدولية التى تؤدي إلى التردي فى مثل تلك الجرائم ما يلي:

أولاً : التحديات المحلية

وتتلخص التحديات المحلية فى ثلاث تحديات:

التحدي الأول:

أ- ومرجعه تزايد وانتشار مقاهي الإنترنت: ولا مراء أن هذا التواجد ييسر – لأي فرد – التعامل مع شبكة الإنترنت دون ضابط معين بل ويستقطب الشباب للتعامل مع شبكة الإنترنت بسهولة، لاسيما هؤلاء غير القادرين على تحمل نفقات شراء جهاز حاسب

---

[4] د/ عمر بن محمد العتيبى، الأمن المعلوماتى فى المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، مرجع سابق، صـ 191 وما بعدها. أيضاً: د/ مفتاح بوبكر المطردى، المستشار بالمحكمة العليا الليبية، الجريمة الإلكترونية والتغلب على تحدياتها، مرجع سابق، صـ 38 وما بعدها.

[1] د/ قدرى عبد الفتاح الشهاوى، قانون التوقيع الإلكتروني ولائحته التنفذية والتجارة الإلكترونية فى التشريع المصري والعربي والأجنبي، مرجع سابق، صـ 495 وما بعددها.

آلى مما يستتبع إمكانية اطلاعهم وتواصلهم مع ما هو جديد على شبكة الإنترنت بصفه دائمة.

ب- رغم تلك التوجهات، فإن تزايد انتشار تلك المقاهي أدى إلى سعي البعض نحو استخدام حاسوب تلك المقاهي من أجل تنفيذ جرائمهم مما أدي إلى صعوبة التعرف على مرتكبي تلك الجرائم المعلوماتية، لاسيما حال: كون المقهى قد تناسى الالتزام بشروط التراخيص اللازمة لتسجيل الدخول على شبكة الإنترنت – خاصة إذا إتبع الجاني أسلوب التنقل بين أكثر من مقهي خلال اليوم الواحد، الأمر الذي يؤدي إلى صعوبة إمكانية التوصل لأدلة الإثبات فى مواجهة تلك المقاهي لاسيما حال إعادة تشغيل أجهزة الحاسوب لديها بصورة دورية.

التحدي الثاني:

انتشار تكنولوجيا الـ ADSL: وتلك التكنولوجيا تعرف بإسم الإنترنت فائق السرعة إذ يتميز بالدخول السريع على شبكة الإنترنت وبالتالى التعامل مع الصفحات الإلكترونية بسرعة عالية مما يوفر وقت مستخدم الشبكة بالإضافة لسرعة تحميل البرامج من على الشبكة إلى المستقبل مما يتيح تحميل أو إنزال كميات من البرامج دفعة واحدة، لاسيما أن تلك التكنولوجيا تتميز بالتكلفة الرخيصة إذ تتم من خلال اشتراك شهري ثابت مقارنة بتكلفة الاتصال عن طريق خطوط التليفون أو ما يعرف باسم الـfree Net. والواقع أن تلك التكنولوجيا الـ ADSL ورغم ما اتصفت به من مكنات فائقة قد مكنت بعض الأشخاص من استغلالها الاستغلال السئ، وذلك عن طريق اشتراك أكثر من شخص فى جهاز واحد عن طريق موزع خطوط، حيث يكون الجاني هو أحد الأشخاص المتصلين بنظام المشاركة مما يؤدي إلى صعوبة الوصول إليه فى حالة ارتكابه جريمة معلوماتيه على اعتبار أن عمليات الفحص الفني، قد تثبت أن شخصاً آخر هو مستخدم النظام (المتعاقد على الاشتراك بخدمة الـ ADSL فى النهاية).

التحدي الثالث:

أ- التطور التكنولوجي فى ظهور الإنترنت اللاسلكي: وهذا التطور التكنولوجي يتيح سرعة الاتصال مع شبكة الإنترنت من خلال كروت اتصال لاسلكية مزودة بأجهزة الحاسبات المحمولة Laptop، وهي مزيج من نظام الـ ADSL والنظام اللاسلكي حيث يتم استقبال خدمة الإنترنت من مقدمي الخدمة ويتم توزيعها لاسلكياً على منافذ توصيل تسمى Access Point وتتميز هذه الخدمة بإمكانية الدخول السريع لشبكة الإنترنت، من أى مكان يقدم هذه الخدمة (المطارات – الفنادق – المراكز التجارية ....) فهى لا تتطلب كابلات للتوصيل إذ يكفى فى شأنها أن يكون مستخدم الخدمة بالقرب من منفذ التوصيل ومن خلال كارت الشبكة اللاسلكى المزود بجهازه المحمول حيث يتمكن من الدخول على الشبكة.

ب- وعلى الرغم من كون هذه الخدمة تعد من أكثر التطورات الحديثة فى التعامل مع شبكة الإنترنت إلا أن بعض الأشخاص قد أساءوا استخدمها حيث يقوم مرتكب الجريمة المعلوماتية باستخدام تلك التكنولوجيا تبعاً لسهولة وسرعة اتصاله بالإنترنت من أى مكان يقدم تلك الخدمة، وذلك باستخدام جهازه الشخصى الأمر الذى يسمح له بالتنقل بين أكثر من مكان فى اليوم الواحد – خاصة إذا كانت الجهة التى تقدم تلك الخدمة لا تقوم بتسجيل دخولة على الشبكة[1].

ثانياً: التحديات الدولية

وتتلخص التحديات الدولية فيما يلى:

التحدى الأول:

يتجلى ذلك التحدى فى صورة بعض عمليات التخفى (Proxy) أثناء التجوال على شبكة الإنترنت حيث تؤمنها بعض المواقع على الشبكة وبالتالى تسمح لمستخدمها بالانطلاق منها إلى أى موقع على شبكة الإنترنت بدون أن يكتشف ذلك الموقع شخصية الزائر، وعلى الرغم من أهمية الـ Proxys (البوروكسيات) وتزايد الهدف التى صممت من أجله لتأمين الشبكات والمواقع ضد عمليات الاختراق، إلا أنها استغلت الاستغلال السيء من قبل قراصنة الإنترنت، حيث أن مرتكب الجريمة المعلوماتية الذى يستخدم هذه المواقع يصعب الوصول إليه، كما أن الأمر لم يقف عند هذا الحد بل قام مصممى الفيروسات المدمرة من خلال استخدامهم لتلك المواقع إلى إطلاق فيروساتهم المدمرة على العالم، الأمر الذى بات يشكل ظاهرة خطيرة فى المجتمعات الدولية لصعوبة التوصل لشخصية مرتكب الفعل.

التحدى الثانى:

ويتمثل هذا التحدى فى غياب مفهوم عام متفق عليه بين الدول حول نماذج النشاط المكون للجريمة المعلوماتية بل والتعريف القانونى للنشاط الإجرامى المتعلق بهذا النوع من الإجرام، مما جعل الجريمة المعلوماتية العابرة للحدود من التحديات الكبيرة التى خصص لها وحدات شرطية فنية لمكافحتها، مما يتطلب تفعيل التعاون الدولى ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة[1]. وذلك بالقدر الذى لا يتعارض مع القانون المحلى للدول المطلوب منها التعاون، على أن

---

[1] د/ قدرى عبد الفتاح الشهاوى، قانون التوقيع الإلكتروني ولائحته التنفذية والتجارة الإلكترونية فى التشريع المصري والعربي والأجنبي، مرجع سابق، صـ 496 وما بعدها.

[1] د/ قدرى عبد الفتاح الشهاوى، قانون التوقيع الإلكتروني ولائحته التنفذية والتجارة الإلكترونية فى التشريع المصري والعربي والأجنبي، مرجع سابق، صـ 497 وما بعدها، أيضاً: د/ مفتاح بوبكر المطردى، المستشار بالمحكمة العليا الليبية، الجريمة الإلكترونية والتغلب على تحدياتها، مرجع سابق، صـ 39 وما بعدها.

تكفل الدول بعضها الأخر فى دعم قدراتها الإدارية والتنظيمية المكلفة بإنفاذ القانون فى مجال التعاون وتبادل المعلومات على الصعيد الدولى[2].

ذلك إن الجريمة والأمن عبر الحدود الوطنية هما طريقتان أساسيتان للحكم في عالم يتحول إلى العولمة. في جميع أنحاء العالم ، هناك ميل إلى التعامل مع كل مصدر ضرر يمكن تخيله كمصدر محتمل لانعدام الأمن ، وبالتالي كجريمة. في ظل نظام عالمي مضطرب بمخاطر أمنية. ومع انتشار هذه المنطق، يتم اللجوء إلى الإجراءات الأمنية في محاولة للسيطرة على مصادر الضرر المتوقعة، والنتائج ليست دائمًا واضحة المعالم. وعلاوة على ذلك ، فإن مصطلحات الجريمة عبر الوطنية والتهديد والمخاطر والأمن تكون محصورة من الناحية الفنية، مما يزيد من الصعوبات النظرية والعملية، خاصة مع السير في اتجاه نحو الحوكمة العالمية والحوكمة على مستوى العالم[3].

المطلب الثالث
مقترحات مواجهة التحديات الأمنية فى مواجهة جرائم المعلوماتية

إذا كان القرن الذي نعيشه كان له أثر بارز فى بزوغ أنواع جديدة من الجرائم والتى بدورها ألقت عبء شديد فوق عبء جهاز الأمن فمن المتوقع زيادة ذلك العبء باستمرار مع الزيادة الشديدة فى التقدم العلمي وثورة التكنولوجيا والاتصالات – وإذا كانت جمهورية مصر العربية وهي دولة منفتحة على العالم، وهو ما أبرزه مؤتمر دعم وتنمية الاقتصاد المصرى المنعقد فى الفترة من 13- 15 مارس 2015، من خلال طرح المشاريع الاقتصادية العالمية الواعدة القاهرة 2030، وعلى رأسها تدشين مشروع إنشاء العاصمة الإدارية الجديدة لجمهورية مصر العربية وهى مدينة القاهرة الجديدة، فضلاً عن مشاريع إنتاج الكهرباء من خلال الطاقة الجديدة والمتجددة، فضلاً عن الدخول فى منظومة المفاعلات النووية السلمية لإنتاج الكهرباء، يضاف إلى ذلك المدن التجارية الحرة، والمركز العالمى اللوجيستى لتجارة وتداول الحبوب والغلال

---

[2] من الصعوبات التى تثار فى وجه التعاون الدولى الدفع بأن الجريمة سياسية، والدفع بأن الجريمة ضريبية، والدفع بعدم ازدواج التجريم، وتطبيق الدولة المطلوب منها التعاون لقانونها الداخلى والإجرائى ... وقد نصت الاتفاقية الأوروبية بشأن مكافحة غسل الأموال على أن تكون طلبات التعاون الدولى بالقدر الذى لا يتعارض مع القانون المحلى للدول المطلوب منها التعاون (المادة 9)، وأجازت هذه الاتفاقية للدول المطلوب منها التعاون أن ترفض اتخاذ تدابير قسرية لجمع الأدلة أو اتخاذ تدابير مؤقتة إذا كان قانونها الداخلى لا يسمح بذلك (المادة 18 -2). كما نصت اتفاقية فيينا لمكافحة غسل الأموال على المبدأ ذاته (المادة 7-15). ونصت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة (المادة 7). واتفاقية الأمم المتحدة لمكافحة الفساد (المادة 14) على أن تكفل الدول الأعضاء قدرة السلطات الإدارية والتنظيمية والمكلفة بإنفاذ القوانين وغيرها من السلطات على التعاون وتبادل المعلومات على الصعيد الدولى.... د/ أحمد فتحى سرور، قانون العقوبات، القسم الخاص، الكتاب الأول، دار النهضة العربية، القاهرة، ط6، 2016، ص 1064 وما بعدها.

[3] (Series Editors: Sheptycki, James, Tsoukala, Anastassia,Transnational Crime, Crime Control and Security,https://www.springer.com/series/14398

بدمياط على شاطىء البحر الأبيض المتوسط، مراكز صناعة وصيانة السفن والناقلات البحرية، يضاف إلى ذلك المناطق الصناعية واللوجستية الجديدة والمتنوعة، صناعات البتروكيماويات، وصناعة الإلكترونيات والاتصالات، والصناعات الدوائية، أيضاً المدن السياحية ذات الميزة الإضافية كمدينة العلمين الجديدة، ومدينة الجلالة العالمية، فلابد وأن تكون على أتم الاستعداد وصاحب نظرة ثاقبة ورؤية مستقبلية لقمع ومنع أي عمل من شأنه الإضرار بالأمن الداخلي لمصر الحبيبة لتشجيع وجذب وحماية الاستثمارات الوطنية والأجنبية على أراضى الدولة، مما يتطلب ما يلى:

1- تطوير كفاءة جهاز الشرطة وتدعيمه بالقدرات المختلفة والكفاءات العلمية والفنية ووسائل التقنية[1] لمواجهة تحديات هذا القرن.

2- تشجيع سيادة التخطيط المدروس من حيث الاهتمام بالبحث العلمي والتقني فى مجال علوم الشرطة وعمل على رفع شأن الجهاز الشرطي عن طريق إمداده وتزويده بالكثير من القدرات العلمية لمواجهة الجرائم الموجهة ضد الأمن.

3- أن تعمل وزارة الداخلية على نشر الوعي الإعلامي الأمني لمواجهة ظاهرة العولمة الأمنية، من حيث القيام بنشر مفاهيم الأمن الوقائي بين أفراد الجمهور، وقيام الإدارة العامة للإعلام والعلاقات بالوزارة بهذا الدور الذي من شأنه تبصير المواطنين بتطوير الجريمة وأساليب مواجهتها فى عصر العولمة [2].

4- تنمية الوعي بقضية حماية حقوق المؤلف فما يتعلق ببرامج الحاسب الآلى وقواعد البيانات، ذلك مع ربط هذه القضية بالنتائج التى يمكن أن تحققها للاقتصاد المصري. ويكون ذلك بالتعاون بين أجهزة الأمن والجهات العاملة فى هذا المجال ومنها مركز دراسات الملكية الفكرية واتحاد منتجي البرامج التجارية وسائر وسائل الإعلام.

5- التوسع فى إنفاذ برامج متطورة لتدريب وتنمية مهارات رجال الأمن العاملين فى مجال محاربة قرصنة البرمجيات، والتنسيق فى ذلك مع الجهات المعنية والمؤهلة للإشراف على عملية التدريب فى الناحية الفنية والتقنية الخاصة بضبط جرائم القرصنة والتعامل السليم مع المضبوطات.

6- إتباع سياسة التعليم المستمر بتنظيم الندوات والمؤتمرات التى تناقش موضوع الملكية الفكرية بوجه عام وحماية برامج الحاسب بوجه خاص وذلك للتعرف باستمرار على الاتجاهات الدولية الحديثة في هذا الخصوص بغرض الاستفادة منها[1].

7- ضرورة إنشاء مركز قومى لأمان الحاسب الآلى والمعلومات[2].

---

[1] (Clovis Police now have a new app that allows you to submit evidence of a crime that you captured on surveillance video. Here's the link: https://cityofclovis.com/police/general-information/clovis-pd-app....https://kmph.com/news/local/clovis-police-hit-the-jackpot-with-3-identity-theft-arrests

[2] أ/ حسام رأفت، العولمة وآثارها على الاستقرار الأمني، مجلة الأمن العام، المجلة العربية لعلوم الشرطة، العدد 302، 1429هـ، أكتوبر 2008، صـ 39 وما بعدها.

[1] د/ فؤاد جمال الدين، التطور التشريعي لحماية البرمجيات مع إشارة خاصة لمصر، مرجع سابق, صـ 8 وما بعدها.

8- إنشاء جهاز إلكتروني لمكافحة الجريمة المعلوماتية، ويتناولها الباحث بشئ من التفصيل عبر السطور القادمة.

المطلب الرابع
ضرورة إنشاء جهاز إلكتروني لمكافحة الجريمة المعلوماتية

لقد أضحى من الأهمية بمكان ولحماية المال والنفس والمصلحة العامة ممثلة فى الدولة بأركانها الثلاث: الهيئة الحاكمة والشعب والإقليم, فى ظل ثورة الأقمار الصناعية والاتصالات التى لا يعرف مدى الاستفادة منها, أو ما هي عيوبها البعيدة خاصة لسكان الدول التى لم تتأثر بهذه التكنولوجيا والجماعات العرقية والدينية المنعزلة أو الدول الأقل نمواً كما لا يعرف إلى أي درجة تؤثر هذه العيوب وهل هي جانبية أو خارجية وستزيد التقنية من درجة التهديد من الدول والجماعات ذات التقنيات المنخفضة ولكن من المؤكد أن هذا التعاقب غير مستمر بالإضافة إلى أن الشعوب سيكون لديها قصور فى الوعي الإلكتروني الرقمي لتكنولوجيا (تقنية) المستقبل وآثارها الاقتصادية والأخلاقية والثقافية والبيئية والقانونية مع الاستمرار المحتمل للبحث والتطوير, مما سيعرض التقدم العلمي تحديات الأمن الوطني لخصائص ومعايير عدم التأكد وسيزيد التقدم فى العلوم والتكنولوجيا درجة الاعتماد على شبكات الكمبيوتر (الحاسب الآلى) مما يجعل البنية الأساسية فى الدولة هدفاً أكثر إغراء فعمليات تشغيل شبكة الحاسب الآلى تقدم احتمالات جديدة للهجوم على الشبكة من داخلها ومن المحتمل أن يتم ذلك بصورة غير معروفة، كما أفادت الدراسة أن عمليات تبييض الأموال حوالى ألف مليار دولار سنوياً من بينها 300و 500 مليار تأتي من تهريب المخدرات وقد بلغت التكلفة الإجمالية لاستهلاك المخدرات فى 1995 فى الولايات المتحدة 110 مليار دولار. وجاء فى الدراسة أن الإجرام الدولي سينضم إلى الإرهاب كأحد التهديدات الأكثر خطورة للعالم فى القرن الحادي والعشرين من دون أن تستبعد ظهور دول" إجرامية" فى العالم فى السنوات العشر القادمة. كما أضافت الدراسة أن الكلفة الباهظة للجريمة سترتفع أكثر عندما تمتلك المجموعات أو الأفراد المدافعون عنها القدرات المعلوماتية الضرورية للتلاعب بالأسواق وتعزيز نفوذها لدى حكومات"اللصوص" ولن يكتفى هؤلاء بتقديم "ملاجئ " للمجرمين بل يدعمون نشاطاتهم عبر السماح لهم بالعمل دون عقاب.

فالمطلوب على وجه السرعة إنشاء جهاز إلكتروني لمكافحة الجريمة خاصة وأن ملامح الجهاز العصبي الرقمي على مستوى الناس بدأ يتبلور مرحلياً وبالتالى

---

(2) بدون، جرائم الحاسبات والإنترنت، الجرائم المعلوماتية، تاريخ الإنترنت ونشأة العالم الإفتراضى، متاح على:
- Available At:http://adel-amer.catsh.info/vb/showthread.php?p=3967

بدأت الجريمة الإلكترونية فى ازدياد مما يتطلب جهاز أمن وإدعاء وقضاء إلكتروني وأيضاً قوانين إلكترونية للحد من تلك الجرائم وضبطها. ومن أهم أسباب استمرار هذا الجهاز تحقيق أهداف أفراده وذلك من خلال تحقيق أهدافه, وحتي يستمر الجهاز يجب أن تكون لدى أفراده مهارات إلكترونية معينة متمثلة فى توازنهم الإلكتروني معنوياً وفكرياً وجسمانياً واجتماعياً واقتصادياً ويمكن تحقيق ذلك تعيين أفراد تتوفر فيهم هذه التوازنات من أجل تحقيق أهدافهم وأهداف الجهاز. لذلك يتطلب الأمر تعيين خريجي الكليات المتخصصة فى مجال التكنولوجيا الرقمية فى جهاز الشرطة والإدعاء والقضاء بعد تأهيلهم نظامياً وقانونياً للإنخراط فى مجال المكافحة مع منحهم الأجر المتميز والمجزي حتي يعطوا وقتهم وجهدهم ومهاراتهم كلها من أجل الحد من هذه الجريمة وإقامة العدل فى حالة الضبط.

الأسلوب الأمريكي فى سد العجز فى الإمكانات البشرية الإلكترونية:

يتمثل هذا الأسلوب فى دعوة مخترقي الكمبيوتر فى الإلتحاق للعمل فى مكافحة هذا النوع من الجرائم خاصة تلك التى تعتبرها تهديدات حرب المعلومات والتى تتراوح ما بين حوادث تخريب مواقع الإنترنت ومخاوف فيروسات الكمبيوتر وبين تهديدات ترعاها دول أجنبية غير محددة ضد أمنها القومي. وفى هذا الصدد قال أرت ماني مساعد وزير الدفاع الأمريكي وكبير ضباط معلومات البنتاغون لشئون القيادة والسيطرة والاتصالات والمخابرات أمام مؤتمر لمخترقي الكمبيوتر الذي عقد بتاريخ 2000/7/28 وحضره حوالى 5000 شخص "أدعوكم للإنضمام للحكومة أو القطاع الخاص من أجل الأمر ولكن عليكم أن تكونوا فى جانب الدفاع " وأضاف " إذا كنتم تفكرون فيما تودون عمله بقية حياتكم فربما ترغبون فى العمل معنا". ووبخ ماني الحاضرين لمحاولات الاختراق الطائشة وأشار إلى واحدة منها حدثت منذ عامين فى مستشفى عسكري ولم تلق انتباهاً يذكر فى وسائل الإعلام وقال أن ذلك الاختراق عبث ببيانات إمدادات الدم فى المستشفى وعرض حياة المرضى للخطر قبل أن يتم اكتشافه. ولقد تضمنت كلمات زملاء ماني فى البنتاغون وسلاح الجو وأجهزة الشرطة الاتحادية التى ألقوها أمام المؤتمر بين التودد والترغيب وبين التهديد[1].

---

[1] د/ مصطفى محمد موسى, الجهاز الإلكتروني لمكافحة الجريمة, ط1, سلسلة اللواء الأمنية فى مكافحة الجريمة الإلكترونية, 2001, صـ 175 وما بعدها.
أيضاً:
-hiva V.N. Parasram, Digital Forensics with Kali Linux: Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools Paperback – December 19, 2017,Packt Publishing - ebooks Account (December 19, 2017),https://www.amazon.com/dp/1788625005/ref=sspa_dk_detail_2?psc=1

ونظراً لزيادة ظاهرة الإجرام عبر الإنترنت بالمجتمع الأمريكى، وتتضاعف فيها الخسائر الناتجة عن تلك الظاهرة والتى تلحق بالقطاعات العامة أو الخاصة, فقد تم وضع عدة أقسام ووحدات للشرطة لمواجهة هذا الإجرام والحد من خسائره، ومنها:

- قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية والذي تم إنشاؤه سنة 1991, والذي يختص بالكشف عن جرائم الحاسب الآلى وحقوق الملكية الفكرية وعن ملاحقة مرتكبيها.
- معهد أمن الحواسيب.
- وحدة جرائم الإنترنت: وهي وحدة تختص بالتحقيق فى جرائم حقوق الملكية الفكرية, وفى الجرائم المرتبطة بالتقنية العالية ويترأسها مدير مساعد لمكتب التحقيقات الفيدرالى, ولها ذات مرتبة وحدة التفتيش الجنائي.
- مكتب رئيس التكنولوجيا: وهو مكتب مفوض مباشر من مكتب مدير التحقيقات الفيدرالية الأمريكي, لتسيير مختلف المشروعات التكنولوجية وملاحقة مرتكبي الجرائم الواقعة فى ذلك المجال, كالملاحقة الشهيرة المسماة بكارنيفور وأيضاً تلك المسماة بالمصباح العجيب.
- كما تم إنشاء المركز الوطني لحماية البنية التحتية التابع للمباحث الفيدرالية الأمريكية فى 1998/2/28, والذي يتقاسم مهامه مع وزارة الدفاع, وهو يتكون من فريق سري يصل عدد أعضائه إلى 125 رجل حكومي, وتجدر الإشارة إلى أن نشأة هذا الفريق تعود إلى تقارير جمعية العمل حول جرائم الإنترنت, والمقدم إلى الرئيس الأمريكي السابق " بيل كلينتون" (bill Clinton), والذي حددت من خلاله البنية التحتية التى تعتبر هدفاً للهجومات والاعتداءات عبر الإنترنت. والمتمثلة فى: الاتصالات, الكهرباء, والغاز, والبترول, وسائل النقل, البنوك والمؤسسات الاقتصادية, المياه النقية, المصالح الإدارية والاجتماعية.

وإلى جانب الوحدات السابقة فقد تم تأسيس مركز تلقي الاحتيال عبر الإنترنت من طرف مكتب التحقيقات الفيدرالية بالاشتراك مع المركز الوطني لجرائم اللياقات البيضاء (NW3C). كما تم إنشاء وكالة تابعة لمكتب التحقيقات الفيدرالية إلى جانب المركز الوطني لحماية البنيات التحتية, مهمتها التنسيق فى مكافحة القرصنة المعلوماتية. وإلى جانب تلك الأقسام والمراكز, هناك وحدة متخصصة تابعة لقسم العدالة الأمريكي, مكلفة بمكافحة الإجرام المعلوماتي, تتكون من خبراء فى تقنيات الحوسبة والإنترنت ومن مستشارين قانونيين. ويجب التنويه إلى أن مكتب التحقيقات الفيدرالي يعتبر فى حد ذاته الجهاز القيادي لمواجهة الإرهاب عبر الإنترنت[1].

الأسلوب الفرنسى فى مكافحة جرائم المعلوماتية:

[1] أ/ نبيلة هبه هروال، الجوانب الاجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات (دراسة مقارنة)، مرجع سابق، صـ 111 وما بعدها.

أما فى فرنسا[2]: كغيرها من دول العالم, لم تبق مكتوفة الأيدي, بل سخرت كل قواتها لمكافحة هذا الهاجس الذي يعيشه العالم سواء على المستوى الوطني أو الأوروبي أو الدولي، على النحو التالى:

أ- خطة وزير الداخلية الفرنسي فى مكافحته لجرائم المعلوماتية:

لقد قرر وزير الداخلية الفرنسي السابق دومنيك دو فلبان (Dominique de villepin) بعد اطلاعه على التقرير المقدم له من قبل وزير المالية والاقتصاد تيري برتون (Thierry Breton) – والذي فيه تضاعف كم جرائم المعلوماتية بمختلف أشكالها – وضع حد لهذه الآفة التى تعاني منها دول العالم عامة وفرنسا خاصة, وذلك من خلال اقتراح مشروع قانون يهدف إلى دعم الأمن الداخلي عن طريق مكافحة الإجرام المرتكب عبر تلك الشبكة, وتوفير الأمن المعلوماتي عبرها لمستخدميها الفرنسيين والمؤسسات الفرنسية بالإضافة إلى جوانب أمنية أخرى، وشملت ذلك جميع أشكال الجرائم التي تنقلها أو تسهلها الشبكات الرقمية، فضلاً عن تجريم الهجمات على هذه الشبكات. حيث حدد وزير الداخلية أربعة اتجاهات تشمل؛ تطوير تدريب المحققين المتخصصة، وتنظيم المواقع لرصد الإرهابى[1]، وجرائم الاستغلال الجنسي للأطفال[2]، جرائم العنصرية أو المعاد

---

[2]-L'ACTUALITÉ DU DROIT DES NOUVELLES TECHNOLOGIES, MARDI 18 SEPTEMBRE 2001,Recherche surLEGALIS,https://www.legalis.net/recherche/?recherche.

- Le droit de l'Internet est né avec une décision de justice, l'ordonnance de référé rendue dans l'affaire Brel par le premier vice-président du TGI Paris de l'époque, Jean-Jacques Gomez, voici près de 20 ans. Les tribunaux ont été les pionniers de cette matière qui s'étend désormais à tous les domaines du droit…. Les textes sont regroupés en sept grands thèmes du contentieux de l'Internet : responsabilité des acteurs, droit d'auteur et bases de données, marques, contenus illicites, vie privée et données personnelles, commerce électronique et droit social …....Les 50 décisions clés du droit de l'Internet Broché – 1 juin 2015 de Collectif (Auteur) Editeur : Celog; Édition : Edition 2015 (1 juin 2015),https://www.amazon.fr/Les-d%C3%A9cisions-cl%C3%A9s-droit-lInternet/dp/2955292400

[1] ورغبة من المشرع الجنائى الفرنسى فى مكافحة جرائم الإرهاب حيث نص فى قانون الإجراءات الجنائية الفرنسية على جواز ندب مأمورى الضبط القضائى فى الاشتراك فى محادثات الكترونية غير مشروعة بهدف اثبات الجريمة التى تقع وسيلة اتصالات الكترونية وضبط مرتكبيها، بشرط ألا ينطوى ذلك على التحريض على ارتكاب الجريمة (المادة 706 – 25- 2 إجراءات فرنسى طبقاً للقانون رقم 267 الصادر فى 14 مارس سنة 2011). كما اجاز القانون الفرنسى اتخاذ هذا الإجراء فى الجرائم التى تقع بالألعاب التى تعتمد على الخط (القانون رقم 476 الصادر فى 12 مايو سنة 2010). ويجوز وفقاً للمادتين 95، 206 من قانون الإجراءات الجنائية المصرى اتخاذ هذا الإجراء بناء على ما سمح به القانون فى هذين النصين بالأمر بمراقبة المحادثات السلكية واللاسلكية .... د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، مرجع سابق، ص 1012.

للسامية، وإنشاء شبكة مشتركة تشمل خبراء من الشرطة والدرك لتبادل المهارات بشكل أفضل. الهدف هو "decompartmentalise المعرفة" لتحسين مراقبة التكنولوجيا فضلاً عن تطوير التعاون الدولي في هذا المجال[3].

وفى هذا يرى " دوفلبان " أنه يجب إتباع مخطط محكم لتحقيق تلك الأهداف, يتضمن كخطوط عريضة ما يلي:

1- دعم قوات الشرطة والدرك المتخصصين فى هذه المكافحة, وذلك عن طريق زيادة عددهم:

قرر وزير الداخلية الفرنسي السابق, فى إطار مكافحته لجرائم الإنترنت, زيادة عدد أفراد الشرطة والدرك المتخصصين فى البحث والتحقيق فى هذا النوع من الجرائم[4], ليصل عددهم سنه 2008 إلى 600 شرطي ودرك، إلى جانب حسن تنظيم أشغالهم وتقوية قدراتهم القانونية فى التحقيق وفى مراقبة كافة أشكال العدوان الإلكتروني التى يمكن أن ترتكب أو تكون تلك محلاً لها, كالإرهاب والقرصنة المعلوماتية والعنصرية والسامية وإرهاب الأجانب (Xénaphobie). وفى هذا الإطار نجد وزير الداخلية الفرنسي السابق يقترح: "خلق وسائل خاصة للتحقيق تمكن من اكتشاف الجرائم الخطيرة فى الوقت المناسب" فمثلاً يمكن للمحققين أن يشاركوا تحت اسم مستعار فى المحادثات الإلكترونية, بدون أن يكونوا مسئولين جنائياً". وإلى جانب ذلك نجد وزير الاقتصاد والمالية " Thierry

---

أيضاً ما نصت عليه المادة 46 من قانون مكافحة الإرهاب رقم 94 لسنة 2015 : من أنه للنيابة العامة أو سلطة التحقيق المختصة بحسب الأحوال في جريمة إرهابية أن تأذن بأمر مسبب لمدة لا تزيد على ثلاثين يوما بمراقبة وتسجيل المحادثات والرسائل التي ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة وتسجيل وتصوير ما يجرى في الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية وما يدون فيها وضبط المكاتبات والرسائل العادية أو الإلكترونية والمطبوعات والطرود والبرقيات بجميع أنواعها. ويجوز تجديد الأمر المشار إليه في الفقرة الأولى من هذه المادة مدة أو مددا أخرى مماثلة. (قانون مكافحة الإرهاب المصرى رقم 94 لسنة 2015، الجريدة الرسمية، العدد 33 مكرر، 30 شوال 1436، 15 أغسطس 2015).

(2)Cour d'appel de rennes 5ème chambre Prud'homale Arrêt du 12 décembre 2006

Accel Informatique / Sébastien L. M.

https://www.legalis.net/jurisprudences/cour-dappel-de-rennes-5eme-chambre-prudhomale-arret-du-12-decembre-2006/

(3) https://www.legalis.net/actualite/dominique-de-villepin-confie-le-chantier-cybercriminalite-a-thierry-breton/

(4)D. de Villepin double le nombre des policiers et gendarmes liés à la cybercriminalité, MARDI 07 SEPTEMBRE 2004, https://www.legalis.net/actualite/d-de-villepin-double-le-nombre-des-policiers-et-gendarmes-lies-a-la-cybercriminalite

Breton" فى تقريره المقدم إلى وزير الداخلية السابق, يقترح إضافة مادة فى مشروع قانون الرقابة من الانحراف, لتسهيل التحقيق وإجراءاته فى جرائم الإنترنت, وذلك كما يلي: " يمكن لرجال أو مأموري الضبط القضائي المختصين فى البحث عن الجرائم المشار إليها فى 227-18 إلى 227-24 من قانون العقوبات, إذا ما ارتكبت بواسطة اتصال عامة على المباشر, دون أن ترتب عليهم مسئولية جنائية, القيام بالأعمال التالية:

- المشاركة تحت اسم مستعار فى المحادثات الإلكترونية.
- الاتصال باستخدام تلك الوسيلة بالأشخاص المشتبه فى ارتكابهم لهذه الجرائم.
- التحفظ على المحتويات غير المشروعة وفقاً للشروط المحددة فى مرسوم.

" كما لا تترتب أي مسؤولية جنائية على مصالح التحقيق عندما تبحث فى موقع يتضمن معلومات غير مشروعة تمثل إحدى الجرائم المشار إليها فى الفترة الأولي". من ناحية أخري, نجد الوزير "de villepin" يقترح فى ذات السياق النص على " جريمة خاصة تتعلق بالاقتراحات الجنسية المرسلة عبر الإنترنت أو عن طريق الرسائل المبعوثة عبر الهواتف النقالة (SMS)".

2- تكوين شبكة خبراء من الشرطة والدرك:

كما قرر وزير الداخلية تطوير تكوين رجال الشرطة والدرك المتخصصين فى التحقيق فى هذا الإجرام, تماشياً مع سرعة التطور التكنولوجي الذي يشهده العالم, وفى هذا يعلن وزير الداخلية الفرنسي السابق: " أن الشرطة والدرك سيستفيدون من ذلك التكوين مع هذا النوع من الإجرام عن طريق عقد مؤتمر للإنترنت (Forum d'internet) مشترك ومؤمن, يبدأ قبل نهاية يونيو 2005, حتي يتمكنوا من اقتسام المعلومات التقنية والقانونية". ويهدف ذلك التكوين إلى فهم طريقة تفكير المنحرفين عبر الإنترنت, وبالتالى تسهيل عملية الكشف عن جرائمهم والقبض عليهم. ولتجسيد ذلك على أرض الواقع, قام وزير الداخلية الفرنسي السابق بالإعلان عن إنشاء شبكة للخبراء تضم رجالاً من الشرطة والدرك, تتقاسم فيما بينها اختصاص المكافحة, بالإضافة إلى توفير رقابة تكنولوجية خاصة تستخدم فيها طرق حديثة للتنقيب والتحقيق تتماشى مع التطور الذي تشهده وسائل المعلوماتية. كما يتم عقد ندوة سنوية مشتركة بالتنسيق بين رجال الشرطة القضائية ورجال الدرك الوطني, تضم كل سنة مجموعة من المحققين المتخصصين فى مكافحة جرائم الإنترنت, من أجل مناقشة الإجرام المعلوماتي ووضع حلول له سواء من الناحية النظرية أو التطبيقية, وإلى جانب ذلك, تنظم أيام دراسية ذات مستوى عال لهؤلاء المحققين من قبل المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات (oclctic), الشرطة القضائية (CNFPG), ومعهد البحوث الجنائية التابع للدرك الوطني (IRCGN), يتم فيها مناقشة مواضيع ذات أهمية: كمشاكل الاتصال اللاسلكي,

التعريفات القانونية للاتصال الإلكترونية ... إلخ. وإضافة إلى كل ذلك وفى إطار تطوير تكوين رجال الضبطية القضائية فقد تم مدهم بوسائل تقنية مشتركة لتسهيل التحقيقات. هذا ويكون المكتب المركزي مسؤولاً عن العديد من الوظائف الأساسية؛ المشاركة في التحقيقات المتعلقة بجرائم تكنولوجيا المعلومات والاتصالات. تنوع انتهاكات أنظمة معالجة البيانات الآلية بجميع أشكالها، من البرامج المزيفة إلى برامج التجارة الإلكترونية المزورة إلى الاحتيال في الاتصالات والهواتف المحمولة وبطاقات الهاتف. المشاركة في التحقيقات الفنية التي تجرى أثناء التحقيقات القضائية. إجراء عمليات بحث على الكمبيوتر مع ملفات تعريف الارتباط ، وسيدخل أيضًا في أنظمة كبيرة، وفي النهاية، في سياق الإجراءات القضائية، سيجري شبكات مراقبة إلكترونية أو يقدم اعتراضًا للانترنت[1]. وإنشاء قاعدة البيانات مع توفير الدراسات القانونية والتقنية والاحصاءات السنوية عن الجريمة ذات التقنية العالية. المشاركة في التعاون الدولي. وينبغي أن ينظم عمليات تبادل المعلومات الدولية المتعلقة بالجريمة وأن يصبح نقطة الاتصال الوطنية الرفيعة المستوى للإنتربول. مهمة المجلس هي تدريب مختلف المحققين وضباط الشرطة وأصحاب المصلحة، وتثقيف المهنيين، بما في ذلك من خلال تنظيم المؤتمرات، على أنشطة إنفاذ القانون الفرنسي في مكافحة جرائم الكمبيوتر. وأخيراً ، وبفضل الروابط المهنية المتخصصة، لا سيما مع شركات الكمبيوتر وناشري البرمجيات والنفاذ إلى الإنترنت ومقدمي الخدمات، يقوم المكتب بإجراء بحوث جديدة في هذا المجال[2].

3- زيادة الرقابة على المواقع أو تعزيز الرقابة التكنولوجية:

قرر وزير الداخلية إلى جانب الاقتراحات السابقة أن تقتسم مهمة رقابة مواقع شبكة الشبكات بين رجال الشرطة والدرك: فخص الجهاز الأول منهما, بمراقبة المواقع التى تبث فيها الجرائم التالية: الأعمال العنصرية, الإرهاب, القرصنة المعلوماتية. أما جهاز الدرك فخصه برقابة المواقع التى تحوي صوراً إباحية. إلى جانب الاقتراحات السابقة, يضيف الوزير السابق ضرورة تطوير التعاون مع مراكز البحوث المتواجدة فى الجامعات والمؤسسات الكبيرة, بغرض تسهيل مسايرتهم للتطورات التكنولوجية, أضف إلى ذلك, فإنه من الأجدر أن يتم وضع شهادة مواطن مسندة إلى مزودي الخدمات أو الدخول إلى الإنترنت.

---

[1]Cour de cassation Chambre criminelle Arrêt du 22 octobre 2013,Mohamed X. / Ministère public,https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-22-octobre-2013/

[2]Sommet mondial sur la Cybercriminalité : rencontre du G8, MARDI 16 MAI 2000,https://www.legalis.net/actualite/sommet-mondial-sur-la-cybercriminalite-rencontre-du-g8/

ب- الأجهزة المختصة بمكافحة جرائم المعلوماتية فى فرنسا:

ولقد أنشئت عدة وحدات ومراكز متخصصة وغير متخصصة ضمن الشرطة والدرك الوطني فى فرنسا, لمكافحة هذا الإجرام المستحدث بجميع صوره. وهذا ما أشارت إليه الاتفاقية الأوروبية لمكافحة جرائم الإنترنت والتى وقعت وانضمت إليها فرنسا وصادقت على سريانها على أرضها, وكذلك وزير الداخلية الفرنسي من خلال مخططه فى مكافحة هذه النوعية من الإجرام, أبرز هذه الوحدات:

1- على مستوى مصالح الشرطة:

أ- المراكز المتخصصة: ونجد على هذا المستوى حوالى 50 محققاً ومتحرياً متخصصاً فى البحث والتحري عن الإجرام المعلوماتي وذلك كما يلي:

أولاً: القسم الوطني لقمع جرائم المساس بالأموال والأشخاص: D.N.R.A.P.B:

ويتكون هذا القسم فى مجموعة من ستة محققين ومتحرين, متخصصين فى التحقيق فى بيئة الإنترنت (العالم الافتراضي)، ولقد بدأ هذا القسم فى مهامه عام1997, وهو يشهد منذ ذلك التاريخ ارتفاعاً هائلاً فى عدد البلاغات التى تصل إليه من جراء الجرائم التى تقع فى تلك البيئة، إذا وصل عام 2004 إلى 3000 بلاغ. ويقوم أفراد هذا القسم بمعالجة حوالى 10% من الجرائم المبلغ عنها, مع إحالة القضايا الأخرى التى يكون المشتبه فيها معروفاً إلى الجهات القضائية المختصة. وتجد الإشارة إلى أن البلاغات التى تصل إلى القسم D.N.R.A.P.B تكون نتيجة للحجز على عناوين الـ IP (adresse IP), وأرقام بطاقات الإئتمان, من قبل السلطات الأجنبية التى تحيلها بدورها إلى السلطات الوطنية عن طريق قنوات القضاء الدولي.

ثانياً: المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات: o.c.l.c.t.i.c

يعتبر هذا المكتب سلاح الدولة الفرنسية فى مكافحة جرائم الإنترنت أساساً, إلى جانب وحدات أخرى, ولقد تم إنشاؤه بموجب مرسوم وزاري رقم 2000/405 المؤرخ فى 2000/5/15, على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية. يساعده فى نشاطه كل من وزارة الدفاع (المديرية العامة للدرك الوطني) ووزارة الاقتصاد والمالية والصناعة (المديرية العامة للجمارك والحقوق المباشرة والمديرية العامة للمنافسة والاستهلاك وقمع الاحتيال). وهو يتمتع كغيرة من المكاتب المتخصصة, باختصاص وطني يتحدد نطاقه فى الجرائم الخاصة والمرتبطة بتكنولوجيا المعلومات والاتصالات (سواء

أكانت تلك التكنولوجيا محلاً للاعتداء أو وسيلة لارتكاب وتسهيل ذلك الاعتداء). وهو مكلف وفقاً للمادة الثالثة من المرسوم بالمهام التالية:

على المستوى الوطني:

1- تنشيط وتنسيق عمليات ملاحقة مرتكبي (فاعلين أصليين أو شركاء) الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات.
2- مشاركة مصالح التحقيق التابعة للشرطة القضائية فى إجراءات التحقيق فى تلك الجرائم.
3- تقديم يد المساعدة لمصالح الشرطة الوطنية والدرك الوطني وللمديرية العامة للجمارك والحقوق غير المباشرة, والمديرية العامة للمنافسة والاستهلاك وقمع الإحتلال, وغيرها من المصالح فى حالة وقوع مثل تلك الجرائم, ومن بين هذه المساعدات, تلك التى تقدمها فى إجراءات الضبط وفحص وحدات الحاسب الآلى كالأقراص الصلبة مثلاً أو البيانات المتحصل عنها من الاتصال عبر الإنترنت (données de connéxion).
4- تحليل الشكاوى والبلاغات المقدمة له من قبل مستخدمي الإنترنت, نتيجة وجود مواقع غير شرعية ثبت فيه صوراً إباحية للأطفال, على موقعه الرسمي: http://www.internet-mineurs.gouv.fr.

وإضافة إلى المهام السابقة, يقوم هذا المكتب بتحليل وإبلاغ كل من مصالح الشرطة والدرك الوطني والمديرية العامة للجمارك والحقوق المباشرة والمديرية العامة للمنافسة والاستهلاك وقمع الاحتيال وغيرها من الإدارات والمصالح العامة, بجميع المعلومات المتعلقة بالجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات, وله إقامة جميع الروابط اللازمة بين منظمات القطاع الخاص المعنية (المادة 4 من المرسوم السابق). كما له وفى ذات السياق, تقديم كل من المعلومات اللازمة للتعرف أو البحث عن مرتكبي تلك الجرائم المميزة, كلما طلب منه ذلك من قبل المصالح السابقة (المادة 6 من ذات المرسوم). وتجدرالإشارة إلى أن المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات, يمثل لفرنسا نقطة الاتصال المركزية فى التبادلات الدولية, فهو من جهة يشارك على المستوى الوطني, فى تحريك وتنسيق الأعمال التحضيرية اللازمة. ومن جهة أخرى, فهو يشارك فى نشاطات المنظمات الدولية، كما أنه يحافظ على الروابط العلمية بين المصالح المتخصصة فى البلدان الأخرى ومع المنظمات الدولية – وذلك مع مراعاة الاتفاقات الدولية – فى بحثها على المعلومات المرتبطة بتلك الجرائم المميزة وكذا المتعلقة بالتعرف وتحديد مرتكبيها.(المادة 7 من نفس المرسوم).

ويستعين المكتب المركزي لمكافحة هذه الجرائم المستحدثة لتحقيق مهامه السابقة بثلاث بنيات:

الأولي: وحدة العمليات: وتتكون من أربع فرق, تختص إحداها بجرائم الاحتيال الواقعة على وسائل الدفع, أما البقية فتختص بمعالجة الجرائم الواقعة على شبكات الاتصال.

الثانية: وحدة المساعدات التقنية: وهي بنية مجهزة خصيصاً بوسائل أو برامج ذات مستوى تكنولوجي عال لتأمين المساعدة لمصالح التحري والبحث, ولتكوين محققين متخصصين فى التحقيق فى الإجرام المعلوماتي, ولتوفي الرقابة التكنولوجية وتسهيل التدخلات القضائية فى شبكة الإنترنت, وكذا لدراسة البلاغات الموجهة إلى ذلك المكتب بسبب وجود مواقع غير مشروعة تبث أو تمتلك صوراً إباحية.

الثالثة: وحدة التحليل والتوثيق العملي: وتتمثل مهام هذه الوحدة فى معالجة المعلومات المتحصلة من النشاطات القضائية للمصالح التى لها نفس اختصاص المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال سواء على المستوى الوطني أو الدولي.

ويتكون المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات من 32 شرطيا و 3 من الدرك. وتجدر الإشارة إلى أن هذا العدد, وفقاً لمخطط وزير الداخلية فى مكافحة إجرام الإنترنت, يتم مضاعفته, مع مشاركة فعالة للدرك إلى جانب الشرطة, ليصل إلى 75 مأمور ضبط قضائي، كما أنه وفى إطار تلك المكافحة سيتم إنشاء على مستواه, قطب وحيد لتلقي البلاغات والشكاوى عن المواقع غير المشروعة، يتكون من عدد متساو من رجال الشرطة والدرك. وإلى جانب المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات توجد هناك مراكز أخرى متخصصة فى البحث والتنقيب والتحقيق فى جرائم الإنترنت, كالمديرية المركزية لأمن النظام المعلوماتي، والتى هي عبارة عن مصلحة بيوزارية, تهتم بالمراقبة والسهر على أمن النظام المعلوماتي من أي اختراقات[1].

ب- المراكز غير المتخصصة فى مكافحة جرائم المعلوماتية فى فرنسا:

هذا من جهة, ومن جهة أخرى فإنه وإلى جانب تلك المراكز المتخصصة فى مكافحة جرائم الإنترنت, توجد فى فرنسا, وحدات شرطية أخرى, وبالرغم من عدم تخصصها فى تلك المكافحة إلا أنها تساهم فيها بقدر لا يمكن إنكاره، منها:

*** الإدارات الإقليمية للشرطة القضائية:**

[1]Tribunal correctionnel de Nanterre Jugement du 10 novembre 2011,Greenpeace et autres / EDF et autres,https://www.legalis.net/jurisprudences/tribunal-correctionnel-de-nanterre-jugement-du-10-novembre-2011

وهي إدارات تابعة للمديريات الجهوية (المناطق الإقليمية) للشرطة القضائية, وهي تساهم فى التحقيق فى جرائم الإنترنت وفى ملاحقة مرتكبيها والقبض عليهم، إما بناء على إذن من النيابة العامة أو بناء على سلطاتها, بشرط انعقاد اختصاصها الإقليمي. وكذلك الحال بالنسبة لفريق حماية الأحداث الذي أنشأ عام 2003 والتابع للمديرية الجهوية للشرطة القضائية (B.R.P.J) لباريس، والذي هو الآخر يساهم بقدر كبير فى مكافحة تلك الجرائم المستحدثة وخاصة تلك التى يكون محلها أو هدفها الأحداث، وهو فى ذلك يتكون من ستة محققين متخصصين فى تلك المكافحة. وتجدر الإشارة إلى أن هذا الفريق يتمتع باختصاص إقليمى واسع جداً يغطى المنطقة الأكثر اتصالاً بشبكة الإنترنت فى فرنسا، والمتمركز فيها مزودو خدمات الإنترنت الرئيسيين. هذا من جهة, ومن جهة أخري نجده قد عالج فى غضون السنة الأولى من نشأته حوالى 96 قضية تتعلق ببث أو امتلاك صور إباحية على الإنترنت من المتوقع ارتفاع عدد هذه القضايا سنة 2004 إلى 300 قضية. كما أن الشرطة المحلية دوراً فعالاً فى المساهمة فى مكافحة هذا الإجرام المستحدث، وذلك إما بناء على إذن من النيابة العامة أو بناء على سلطاتها, بشرط أن يكون ذلك ضمن اختصاصها الإقليمي[1]. وكما هو معروف فى فرنسا, فإنه يوجد إلى جانب الشرطة الوطنية, رجال الدرك الوطني, فما دور هذه الفئة فى مكافحة جرائم الإنترنت؟

2- على مستوى مصالح الدرك الوطني:

لقد سخرت الحكومة الوطنية الفرنسية, كما سيق ذكره, لمواجهة جرائم التكنولوجيا وخاصة تلك المتعلقة بالإنترنت قوات من مأموري الضبط القضائي منها: رجال الشرطة الوطنية ورجال الدرك الوطني. ولقد أقر ذلك من خلال خطاب وزير الداخلية الفرنسي المتضمن خطته لمكافحة هذا التميز من الإجرام, إذا تم تحديد اختصاص كل جهاز من تلك الأجهزة فى الرقابة على المحتوى غير المشروع الذي يبث عبر الإنترنت. وذلك كما يلي: يختص رجال الدرك الوطني برقابة المواقع غير المشروعة التى تبث أو تمتلك صوراً إباحية, ويختص رجال الشرطة فى مقابل ذلك, وكما سبق تحليله, برقابة المواقع غير المشروعة التى تحتوي على أعمال عنصرية سامية, وخصوصاً تلك المتعلقة بالتعصب العنصري والإرهاب والقرصنة المعلوماتية[2]. وتجدر الإشارة إلى أنه قد تم تسمية رجال

[1]Cour de cassation Chambre criminelle Arrêt du 6 novembre 2013,Patrick X. / Ministère public,
https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-6-novembre-2013/

[2]Dommages-intérêts à payer par les membres mineurs du forum Utopi-Board, JEUDI 10 JANVIER 2019,

الدرك الوطني المتخصصين بمكافحة ذلك الإجرام بـ"رجال درك الإنترنت" (Cyber Gendarme).

وينعقد اختصاص رجال درك الإنترنت فى مكافحة النوع من الإجرام على مستويين:

أ- **على مستوى الاختصاص الوطني المركزي:** ونجد على هذا المستوى وحدات الدرك الوطني التالية:

1- **قسم الإنترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية: (STRJD):**

ويعتبر هذا القسم إحدى الوحدات الرئيسية فى فرنسا, القائمة على ملاحقة مرتكبي جرائم الإنترنت وتم إنشاؤه سنه 1998 فى قلعة sous- Bois – Rosney، ومنذ ذلك العام وهو فى ملاحقة يومية ومستمرة لتلك الفئة من المجرمين، ويتكون من فريق من 13 دركياً. وهو بصورة عامة, يختص بجمع الأدلة الرقمية (preuves numériques), ويجعل المعلومات الممكن استخلاصها من تلك الأخيرة سهلة البلوغ للمحققين والقضاة وذلك عن طريق:

- **نشاطات الخبرة أو التقنية:** معالجة المعلومات, الشبكات والاتصالات, الإلكترونيات[1].

- **مساندة الوحدات على أرض الميدان:** وخاصة فى حالات التفتيش المعقدة.

- **التكوين:** والذي يستفيد منه كل من المحققين والقضاة إضافة إلى عملاء الاتصالات, والمؤسسات التى تعاني من مشاكل الأمن المعلوماتي.

- **البحث والتطوير:** من أجل فهم الوسائل الجديدة من قبل القسم أومن قبل المتدخل الأول على أرض الميدان. ويصل عدد أفراد هذا القسم إلى 14 شخص فيهم 8 مهندسين و 6 تقنيين وهم تحت قيادة الرائد (Eric freyssinet). وتجدر الإشارة إلى أن هذا العدد سيتم مضاعفته سنه 2007 من خلال مخطط مكافحة جرائم الإنترنت لوزير الداخلية الفرنسي. وإلى جانب وحدات الدرك السابقة, فقد تم منذ سنة 2001 تكوين محققين من الدرك متخصصين فى مكافحة هذا الإجرام المستحدث, تكويناً يتماشى مع التقدم والتطور التكنولوجي الذي تشهده تلك التقنية (الإنترنت)، ولقد أطلق علىهم إسم "N-tech" ويصل عددهم إلى 70 محققاً. وتجدر الإشارة إلى أن تكوين هذه الفرق يتم على مستوى " مركز التكوين الوطني للشرطة القضائية "

---

https://www.legalis.net/actualite/dommages-interets-a-payer-par-les-membres-mineurs-du-forum-utopi-board/

(1) Tribunal correctionnel de Nanterre Jugement du 10 novembre 2011,Greenpeace et autres / EDF et autres, https://www.legalis.net/jurisprudences/tribunal-correctionnel-de-nanterre-jugement-du-10-novembre-2011

(C.N.F.P.J) المتواجد فى Fontaine bleu. هذا من جهة, ومن جهة أخرى فإنه وبعد انتهائهم من ذلك التكوين, فإنهم يزودون بوسائل مادية متخصصة ومتميزة تسمى "بمجموعة المحقق"(Lot enquêteur). ومن جهة ثالثة, فإنه يترقب أن يصل عدد هؤلاء المحققين إلى 170 محققاً متخصصاً سنة 2007, موزعين على الوحدات المختصة وفقاً للتسلسل الإقليمي.

ويختص هذا الفريق بالمهام التالية: تأمين الرقابة على شبكة الإنترنت, وذلك عن طريق البحث والتنقيب عن الجرائم الماسة بالبروتوكولات الأساسية للإنترنت. وهو يقوم بذلك إما من تلقاء نفسه أو بناء على معلومات مقدمة إليه, إما من قبل رجال الدرك أو من الغير عن طريق بلاغ موجه إلى عنوان بريده الإلكتروني الرئيسي التالى: Sitepj@gendarmerie.défense.gouv.fr.

2- المركز الوطني لتحليل الصور الإباحية CNAIP

ولقد تم إنشاء هذا المركز بالقرب من قسم الإنترنت, فى Rosney – sous - Bois – فى أكتوبر 2003, وهو مركز مختص بجمع وترتيب جميع الصور المضبوطة أثناء التحقيق القضائي فى قاعدة البيانات، كما يقوم بالمشاركة فى التحقيقات وإجراءات الضبط الهامة. وتجدر الإشارة إلى أنه يستعين للقيام بأعماله تلك " ببرنامج صور "seeker (Logiciel image seeker), المصمم من الشركة الفرنسية LTU التكنولوجية.

3- القسم المعلوماتي الإلكتروني التابع لمعهد البحوث الجنائية للدرك الوطني: (IRCGN)

لقد تم إنشاء هذا القسم سنة 1992, على مستوى البحوث الجنائية للدرك الوطني (IRCGN), وكان هدفه الأول هو تحليل البيانات المدمجة بالأعمال الحواسيب الآلية فى إطار التحقيقات القضائية, والمتعلقة بالأعمال الاقتصادية والمالية, خاصة تلك المرتبطة بأرصدة المؤسسات وكذا أعمال قرصنة البرامج أي النسخ غير المشروع (Cople illicite). وهو يقوم بتقديم المساعدة التقنية (خبرة, رقابة, إعتراض) لمختلف مصالح الدرك.

ب- على المستوى الإقليمي:

ويتواجد على هذا المستوى:

1- الوحدات الإقليمية ووحدات البحوث:

تساهم الوحدات الإقليمية ووحدات البحوث إلى جانب الوحدات المركزية السابقة, فى مكافحة جرائم الإنترنت على المستوى الإقليمي، إذ يقوم محققوها بتلك المكافحة بالمساهمة مع المحققين المتواجدين في وحدات البحوث المتخصصة فى البحث والتنقيب عن ذلك النوع من الإجرام, فمثلاً نجد أنه على مستوى فرق البحث, تهتم فرق التحقيق "N-tech" بالجانب التقني للتحقيقات القضائية، أما بالنسبة لأقسام البحوث, فتقوم بمعالجة الجرائم الخاصة المتعلقة بالمساس بالنظام المعلوماتي, كما أنها

تمارس رقابة مشددة على مواقع الإنترنت وذلك بمشاركة قسم الإنترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية.

2- وحدات أقسام الاستعلامات والتحقيقات القضائية : B.D.R.I.J :

تقوم هذه الوحدات بدور هام, على مستوى الدرك الوطني, إذ تتركز أعمالها على تبادل الخبرات التقنية وتبادل الاختصاصات بين رجال الدرك. وتجدر الإشارة وكخلاصة عامة عن مهمة الدرك الوطني فى مكافحة جرائم الإنترنت, بأنها تتلخص فى ثلاث نقاط: الخبرة, معالجة المعلومات, التخصص فى المواقع والاتصالات الإلكترونية. هذا من جهة, ومن جهة أخرى فإنه ووفقاً للرائد "فرايسنت" (Freyssinet) يصل مجموع الضبطية القضائية المكلفة بمكافحة هذا النوع من الإجرام إلى 160 شرطياً ودركياً. ومن جهة ثالثة ومن أجل تدعيم عمل الدرك فى تلك المكافحة فقد تم تزويده بشبكة دولية تجمع معلومات عن الجرائم الجنسية الواقعة على الأحداث عبر شبكة الإنترنت عبر العالم. وتوجد إلى جانب وحدات الشرطة والدرك المختصة بمكافحة جرائم الإنترنت "خلية إستقبال وتحليل الانترنت", والتى تم إنشاؤه سنه 1998 من قبل المديرية العامة للجمارك والحقوق غير المباشرة التابعة لوزارة الاقتصاد والمالية والصناعة, وهي تختص بتأمين الرقابة على الإنترنت وتحليل المخاطر الناجمة عن استخدامها, والبحث عن أعمال الاحتيال فى ميدان التجارة الإلكترونية كما أنها تختص بمكافحة جرائم غسل الأموال عبر الإنترنت وكذا تجارة الممنوعات عبر تلك الشبكة. ويوجد فى مقابل ذلك, وفى ذات المستوى, المديرية العامة للمنافسة والاستهلاك وقمع الاحتيال, والتى وضعت بنية مماثلة لسابقتها تختص بحماية المستهلكين من المواقع المخالفة للخدمة الوطنية والأوروبية وكذا مكافحة الاحتيالات وقمعها عبر المواقع الإلكترونية[1].

هذا ولا يخفى الدور الملموس الذى تقوم به فرنسا شرطة وقضاء فى مكافحة الاجرام السيبرانى وتحقيق الأمن المعلوماتى، وحماية العلوم الانسانية عبر الانترنت، سواء كانوا مقترفيها أحداث أو بالغين، مثلما حدث فى وقائع وأحداث قضية المنتدى الالكترونى لتبادل الملفات غير المشروعة " Le forum utopi-board " والتى وترجع الوقائع بين عامي 2005 و 2006 ، أتاح منتدى Utopi Board لمستخدمي الإنترنت، دون إذن من أصحاب الحقوق، أكثر من 36000 ملف أو ألبومات موسيقية، 3500 فيلم، بعضها قبل أدائها في المسارح، و 750 برنامج. كشفت

[1] أ/ نبيلة هبه هروال، الجوانب الاجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات (دراسة مقارنة)، مرجع سابق، صـ 114 وما بعدها.

التحقيقات عن تحديد 27 عضواً نشطاً بالمنتدى، بما في ذلك مالك الكمبيوتر المصادر الذي كان في الواقع مؤسس المنتدى ومديره[2].

[2]Plus de 13 ans après les faits et 4 ans après le premier jugement pénal du 27 mai 2014 qui avait condamné les personnes majeures ayant pris part activement à un important forum d'échanges de fichiers illicites, le tribunal pour enfants de Béthune a finalement répondu aux demandes indemnitaires des parties civiles contre les prévenus mineurs. Par un jugement du 17 mai 2018 que le greffe a fait parvenir très tardivement, les prévenus ont été condamnés à verser plus de 160 000 € de dommages intérêts aux parties civiles : Microsoft, la Sacem, la SDRM, le SCPP et l'APP.

Entre 2005 et 2006, le forum Utopi-Board avait permis de mettre à la disposition des internautes, sans autorisation des ayants droit, plus de 36 000 fichiers ou albums de musique, 3 500 films, dont certains avant leur sortie en salle, et 750 logiciels. Les investigations ont révélé un forum très hiérarchisé avec des administrateurs, des modérateurs et des super modérateurs, avec trois zones d'accès aux fichiers (libre et gratuite, privée et super privée), plus ou moins payantes et plus ou moins riches en contenus illicites suivant les paliers. 27 membres actifs avaient été identifiés, dont le propriétaire de l'ordinateur saisi qui était en fait le fondateur et administrateur du forum.

Par un jugement du 27 mai 2014 du TGI de Béthune, une douzaine de personnes majeures ont été condamnées à des peines de prison, avec sursis, pour contrefaçon d'œuvres de l'esprit (films, musiques, jeux vidéos, logiciels) et de marques mais aussi pour fraude informatique. Et par un jugement du 5 février 2015, le TGI de Béthune s'est prononcé sur les intérêts civils. Les prévenus ont été condamnés à verser des dommages-intérêts importants, notamment 40 000 € respectivement à la SCPP, la Sacem et la SDRM.

Puis, par un jugement du 27 avril 2017, le tribunal pour enfants de Béthune a condamné à une peine d'admonestation les autres membres actifs du réseau, mineurs au moment des faits, reconnus coupables notamment de contrefaçon et d'accès frauduleux dans un système d'information. L'admonestation constitue la plus faible des sanctions pénales que peut prononcer le juge des enfants. Le 17 mai 2018, le même tribunal s'est prononcé sur les sanctions civiles.

En ce qui concerne l'Agence pour la protection des programmes (APP), le tribunal a reconnu qu'elle avait qualité à obtenir des dommages-intérêts lorsque les intérêts collectifs de la profession sont bafoués, ce qu'il admet être le cas en l'espèce. Pour le tribunal, les agissements des prévenus ont contribué à dévaloriser les éléments (jeux et logiciels) téléchargés et ainsi à limiter la rémunération de leurs créateurs et auteurs. Les prévenus concernés doivent lui verser 1 500 € de dommages-intérêts. S'agissant des demandes

بعد أكثر من 13 عامًا من الأحداث وبعد 4 سنوات من صدور الحكم الجنائي الأول في 27 مايو 2014 ، والذي حكم على البالغين الذين شاركوا في منتدى مهم لتبادل الملفات غير المشروعة، استجابت محكمة بيتون للأطفال " le tribunal pour enfants de Béthune " في النهاية مطالبات التعويض من أطراف مدنية ضد المدعى عليهم الصغار. في الحكم الصادر في 17 مايو 2018 ، حكم على المدعى عليهم بدفع أكثر من 160000 يورو (مائة وستين ألف يورو) كتعويض للأطراف المدنية: Microsoft، Sacem، SDRM، SCPP و APP.

وفى السويد "Se" :

أنشئ أول مركز شرطة على الإنترنت فى العالم لبلدية كرامفورس الريفية بالسويد ويمكن للأهالى التعامل مع هذا الموقع برفع الشكاوي وتسديد الغرامات عن طريق موقع إلكتروني على الشبكة تم تزويده بالصوت والصورة ليستطيع متلقي البلاغ عن مشاهدة المبلغ مما يتيح قدراً أكبر من المصداقية كما يحد من البلاغات الكاذبة أو الكيدية. لأن الاتصال عبر الفديو يشكل مساندة للشرطة لأن حركات ونظرات وأسلوب تصرف أي شخص يعبر عن مصادرة المهمة للمعلومات. ويعتبر هذا المركز الوهمي مقدمة لشبكة مراكز وهمية ستنتشر فى السويد وتتيح للمواطنين إمكانية الاتصال برجال الشرطة فى حالة الضرورة لتقديم المعلومات عن حوادث السرقة, أو رؤية السيارات المشبوهة وبناء على هذه المعلومات يتم تحديد موديل السيارة وعرض صورها على الموقع بما يساعد على سرعة إيقافها والقبض على المجرمين, وسيساعد هذا المركز على تخفيف الضغط على مراكز الشرطة التقليدية وتوفير وقت جميع الأطراف وتساهم فى حل إختناقات المرور. وقد احتاج إنشاء هذا المركز إلى مصمم أمني للموقع على الإنترنت وهو الشخص الذي يحدد الشكل الذي

---

de la Sacem et de la SDRM pour les fichiers musicaux, le tribunal a estimé que le téléchargement et la diffusion illégale des œuvres de leur répertoire ont généré un manque à gagner dont le préjudice à réparer est évalué à 40 000 €. La Société civile des producteurs de phonogrammes obtient également 40 000 €, pour la reproduction et la communication au public de leurs enregistrements.

Microsoft est indemnisé pour les contrefaçons par reproduction établies par l'enquête, pour le préjudice tiré de l'atteinte à ses droits extra-patrimoniaux en qualité d'éditeur des logiciels qu'il distribue en France et de l'atteinte à la marque Microsoft. Le tribunal fixe l'indemnité unitaire pour un système d'exploitation à 35 €, pour un logiciel applicatif à 15 € et pour un logiciel encyclopédique ou de jeux à 10 €, soit un total de plus de 160 000

https://www.legalis.net/actualite/dommages-interets-a-payer-par-les-membres-mineurs-du-forum-utopi-board/

ستظهر عليه صفحات الموقع وكيف ترتبط بهذه الصفحات بعضها البعض بما يتيح للمستخدم الإطلاع على المعلومات الموجودة فى هذا الموقع بسهولة وكذلك الانتقال بيسر من صفحة إلى أخرى, كما أن من مهام وظيفته أيضاً تناول الجانب الفني والإداري للموقع. إن الشخص الذي يشغل هذه الوظيفة عليه أن يجمع بين معرفته بالحاسب الآلى الرقمي واللغات المستخدمة فى تصميم الصفحات كلغة الجافا ولغة Html وبين الموهبة الفنية للتصميم الجمالى للصفحات كما يجب عليه دراسة شبكات الحاسبات الآلية الرقمية وكيفية ربط مواقع الإنترنت بهذه الشبكات. ويضاف إلى ذلك إلمامه بالنظم الأمنية للمعلومات سواء كانت للمرور أو وثائق السفر أو الأحوال المدنية أو غير ذلك من الأعمال الأمنية.

ويحتاج الجهاز الإلكتروني لمكافحة الجريمة إلى هذه الوظيفة لأنها من وظائف الأمن فى الحاضر والمستقبل.

وفى سنغافورة " sg" :

بدأ فى سنغافورة تطبيق نظام جديد يعرف بشبكة القانون وبموجب النظام الجديد يمكن للقاضي والمدعي العام والدفاع عن المتهم تبادل الآراء والمعلومات وتداول القضايا عن طريق الإنترنت، وتضم شبكة القانون جميع القوانين الخاصة بسنغافورة بحيث يصبح الرجوع إليها أمراً سهلاً، ووفق هذا النظام يمكن ما يلى: للمحامين إعداد دفاعهم وإرسال وثائقهم للقضاة. للقضاة الإطلاع على الدفاع عن طريق الشبكة. للدفاع والقضاة التحاور فى أية بيانات تخص القضايا. لمستخدمي الشبكة الحصول على أية أحكام صادرة سواء فى المحكمة الإبتدائية أم العليا وذلك دون الذهاب إلى المحاكم. وسيرفع نظام الشبكة كفاءة وفعالية أجهزة القضاء من جهة وتسهيل العمل على المحامين لأن هذا النظام لن يلغي الدور التقليدي للمحاكم.

وفى الصين "Cn" :

أسست شرطة إقليم إنهوي الجنوبي الشرقي وحدة شرطة متخصصة لمراقبة استخدام شبكة الإنترنت وتخطط 20 مدينة ومقاطعة أخري لإقامة وحدات مماثلة. وسبب تأسيس هذه الوحدة والتخطيط لإنشاء غيرها يرجع إلى أن 16.9 مليون صيني يستخدمون الإنترنت ويقضون فى المتوسط حوالى 16.5 ساعة أسبوعياً أمام الشبكة كما يوجد أكثر من 27.000 موقع صيني على الإنترنت وذلك وفق تقرير نشر فى 2000/7/27م.

ولقد تصدت هذه الوحدة لعمليات احتيال واختلاس ممتلكات وعرض أفلام إباحية على الشبكة كما ساعدت البنوك المحلية فى تحسين الوضع الأمن لديها كما تقوم الوحدة أيضاً بتدريب حراس أمن إلكتروني متطوعين وتتعاون مع أجهزة الإعلام المحلية فى نشر معلومات عن فيروسات الكمبيوتر وتعمل مع معاهد البحوث لتطوير برامج وقائية ضد الفيروسات. وفى هذا الصدد طرحت وزارة الأمن العام الصينية برنامجاً مصمماً لإبعاد المعتقدات والجنس والعنف عن الإنترنت فى الصين أطلق

عليه "شرطة الإنترنت" 110" لمنع المستخدمين من تلقي معلومات ضارة من مواقع أجنبية ومحلية ولقد سمي برقم هاتف شرطة الطوارئ الصينية، والبرنامج من ثلاث نسخ للمنازل ومقاهي الإنترنت والمدارس ويمكنه إلغاء أو منع الرسائل من المصادر التى تعد مشينه.

ولقد أصدرت الصين التى تستخدم الإنترنت كأداة للتجارة والتعليم مجموعة من الإجراءات عام 2000م لتنظيم الأنباء ومحتوى مواقع الإنترنت والبريد الإلكتروني والحوار عبر الإنترنت. وأصدرت فى أكتوبر 2000م لوائح جديدة لشركات الإنترنت للحد من الاستثمارات والمحتويات الأجنبية ولفرض رقابة مشددة على المحتوى المناهض للحكومة. وفى هذا الصدد أصدرت اللجنة الدائمة لمؤتمر الشعب الوطني قرار اعتبر من ضمن الجرائم التى تقع تحت طائلة القانون استخدام شبكة الإنترنت فى: التشهير بالأفراد والشركات على الإنترنت. نشر فيروسات الكومبيوتر واقتحام شبكات الدفاع الوطني. التلاعب بالمواقع الشخصية على البريد الإلكتروني. التحريض على الإطاحة بسلطة الدولة, أو الإطاحة بالنظام الاشتراكي, أو تدمير الوحدة الوطنية, أو الاتصال بأعضاء الطوائف. تصميم مواقع وصفحات مخلة بالآداب, أو تسهيل الاتصال بالمواقع الإباحية. الترويج لاستقلال تايوان وتشكيل الطوائف. إطلاق لشائعات التلاعب بأسعار البورصة. وتعد مواد القرار صدي للقوانين القائمة بالفعل والمستخدمة فى سجن المنشقين والإنفصاليين العرقيين وأعضاء طائفة فالون جونج إلا أنها تطبق بشكل خاص وللمرة الأولي على الإنترنت[1].

الخلاصة:

ومما سبق ذكره أنفاً, فإنه ولما كانت جرائم الإنترنت من الجرائم المستحدثة والعابرة للحدود, فإن معظم الدول سواء المتقدمة أو النامية, العربية أو الأجنبية أصبحت تخشاها وتعاني منها، ولذلك كان من الواجب إيجاد جهاز لمكافحتها والحد من خطورتها عن طريق زيادة الرقابة عليها (على تلك الشبكة)، ومن بين الدول العربية التى طبقت ما يعرف بنظام الرقيب (proxy) دولة الإمارات العربية, وذلك من أجل إحكام الرقابة على تلك الشبكة, عن طريق القيام بمراجعة نوعية الخدمات المقدمة عبر تلك الأخيرة لمنع ظهور أي من تلك الخدمات المحظورة.

إلى جانب الإمارات العربية, نجد جمهورية مصر العربية والتى كلفت جهات وإدارات معينة بتلك المكافحة منها:

* الإدارة العامة لمباحث الأموال العامة: والتى تضطلع بمكافحة الجرائم الاقتصادية التقليدية بصفة عامة والمستحدثة بصفة خاصة باعتبارها إحدي الروافد الرئيسية

---

[1] د/ مصطفى محمد موسي, الجهاز الإلكتروني لمكافحة الجريمة, مرجع سابق, صـ 171 وما بعدها.

لقطاع الأمن الاقتصادى، ومن أكثر تلك الجرائم المكافحة جرائم تزوير العملات الورقية التى يكون الحاسب الآلى أداة لارتكابها.

* الإدارة العامة للتوثيق والمعلومات: تعتبر هذه الإدارة من أكبر الإدارات بوزارة الداخلية تعاملاً مع الجرائم المعلوماتية، وهي فى ذلك تختص بعمليات المتابعة الفنية لكثير من الجرائم، ويبدأ عملها من خلال المتابعة الفنية والتحري عن الجرائم المبلغ عنها من الإيرادات الأخرى وذلك من خلال استخدام شبكة الإنترنت وتحديد شخص المتهم. هذا من جهة، ومن جهة أخرى فهي تقوم بتحديد ذلك المتهم من خلال عملية التتبع، ويعتمد أسلوب عمل هذه الإدارة فى معرفة شخص مرتكب الجريمة على استخدام البرامج الحديثة، وذلك عن طريق الاعتماد على رقم (IP) الذي يتعامل من خلاله الشخص مع شبكة الإنترنت. وتعد جرائم السرقة التى ترتكب باستخدام كارت الفيزا من أكثر الجرائم التى تسعى الإدارة العامة للمعلومات والتوثيق إلى ضبطها.

* وإلى جانب الإدارة السابقة توجد الإدارة العامة للمصنفات الفنية والتى تهتم بحماية الملكية الفكرية وحرية الإبداع والتعبير من أي أعمال غير مشروعة، كالنسخ والتقليد. وهي تقوم بذلك انطلاقاً من تلقيها إخطار (بلاغ أو شكوي) عن وقوع مثل ذلك الجرائم، لتبدأ فى التحري والتفتيش والتحفظ على ما تحصلت عليه من وسائط منسوخة وكذا الأجهزة المستخدمة فى عملية النسخ. وتجدر الإشارة إلى أن الإدارة العامة للمصنفات الفنية تقوم بمحلات تفتيشية كبيرة فى جميع أنحاء الجمهورية لضبط تلك الجرائم[1].

وحرصاً على مواكبة أجهزة الشرطة المصرية التطور الذي تنتجه بلدان العالم المتقدم من ضرورة الاهتمام بمكافحة ما يستجد من صور حديثة فى ارتكاب الجرائم بكل ما هو جديد فى عالم التكنولوجيا، فقد تم إنشاء الإدارة العامة لمكافحة جرائم الحاسبات وشبكات المعلومات بمقتضي القرار رقم (13507) لسنة 2002، وهي تابعة للإدارة العامة للمعلومات والتوثيق. وتعد هذه الإدارة إدارة جديدة فى تكوينها ونوعيتها تختص بمكافحة مثل تلك الجرائم، وتتكون من أجل ذلك من ضباط

---

[1] وتعد القضية التى ضبطتها إدارة مباحث المصنفات الفنية عن قيام شاب تمكن من استخدام جهاز كمبيوتر وطابعة وجهاز ماسح ضوئى ووحدة للقراءة والكتابة على الأقراص المدمجة من نسخ عدد كبير من الأفلام سواء من خلال القنوات الفضائيةأو من شرائط فيديو أخرى حيث يقوم بنقل صور الأغلفة والأفشات من على الشرائط الأصلية ويطبعها بالألوان عن طريق جهاز الإسكانر، كما استطاع تزوير العلامات المائية "اللوجو هليوم جرام" الخاصة بالحماية حيث يتم التزوير على أعلى مستوى من الجودة وقد قام هذا الشخص بتزويد جهاز الكمبيوتر بكارت فيديو (TV) لإمكانية الدخول على القنوات الفضائية وتسجيل الأفلام الفاضحة ومنها إعادة نسخها وبيعها، وكان هذا الشخص يبيع الشريط بمبلغ يتراوح ما بين مائة وخمسون جنيهاً ومائتين جنيه، وقد حقق هذا الشخص مبالغ طائلة من وراء ذلك، بعد أن تسبب فى إحداث عدة مشكلات بين شركات الإنتاج."المصدر: احصائيات الإدارة العامة لمباحث المصنفات الفنية، 2001....أ/ محمد يوسف محمد، التحديات التى تواجه التحقيقات فى الجرائم، مرجع سابق، هامش صـ 20.

على أعلى درجة من التخصص والحرفية فى تكنولوجيا الحاسبات وشبكة الإنترنت، مقسمين على أجهزتها المختصة وتشمل:

1- **قسم العمليات:** وهو قسم يختص بالاشتراك مع الأجهزة المختصة بمكافحة الجرائم التى تكون أجهزة الحاسب الآلى أداة لارتكابها فى مجالات نظم المعلومات وشبكات وقواعد البيانات، سواء من داخل الوزارة أو من خارجها وفقاً للتعليمات المنظمة لذلك، كما يقوم بإخطار الأجهزة النوعية المختصة بأعمال المكافحة بالبيانات والمعلومات المتعلقة بالجريمة الجنائية، والتنسيق معها لإجراء التحريات وأعمال الضبط فى تلك الجرائم وفقاً للتعليمات المنظمة لذلك[1]، كما تقوم بإعداد قاعدة بيانات تضم جرائم المعلومات والأحكام الصادرة فيها وكذا مرتكبيها التى تدخل فى نطاق اختصاص الإدارة، أضف إلى ذلك فهي تقوم بإنشاء الملفات والسجلات والبطاقات اللازمة لذلك.

2- **قسم التأمين**: ويختص بوضع الخطط والأساليب المستخدمة فى مجال تأمين نظم المعلومات والشبكات الخاصة بأجهزة الوزارة، وتنفيذها بعد اعتمادها بالتنسيق مع الأجهزة المختصة، وتقديم يد المساعدة لكافة أجهزة الوزارة التى تطلب تأمين نظم المعلومات وشبكاتها وكذا متابعة التراخيص الصادرة للشركات الخاصة فى مجال تلك النظم.

3- **قسم البحوث والمساعدات الفنية**: ويقوم هذا القسم كسابقيه بالقيام بإعداد البحوث الفنية والقانونية فى مجال تأمين نظم وشبكات المعلومات والحاسبات الآلية وبدراسة الظواهر الإجرامية المتعلقة بجرائم الحاسبات والإنترنت واستنباط النتائج للاستفادة منها فى أساليب المكافحة، وهذا بالتنسيق مع الأجهزة المختصة، كما يقوم ببحث مدى ملائمة التشريعات الجنائية لمواجهة مثل هذه الجرائم، أضف إلى ذلك فهو يقوم بتقديم الدعم الفني وتوفير المساعدات الفنية وإبداء الرأي والمشورة فى كافة القضايا والوقائع المرتبطة بهذا النوع المستحدث من الإجرام للجهات المختصة[1].

هذا ونتيجة للتطور التكنولوجى لتقنية المعلومات والتقدم السريع والمتواصل لتطوير الأجهزة والبرامج المعلوماتية، واعتماد قطاع كبير من المجتمع على تقنية المعلومات فى شتى المجالات فقد اتسعت دائرة استخدام الحاسبات الآلية فى الفترة الأخيرة بشكل متسارع وأصبحت كافة أجهزة الدولة والمؤسسات العامة والخاصة

---

(1) قضت محكمة النقض بأنه: تقدير جدية التحريات وكفايتها لإصدار إذن الضبط والتفتيش . موضوعي . اطراح الحكم المطعون فيه الدفع ببطلان إذن النيابة العامة بالضبط والتفتيش لابتنائه على تحريات غير جدية ومنعدمة وتجهيل مصدرها بأدلة منتجة لها أصل بالأوراق . صحيح (الطعن رقم 32611 لسنة 86 جلسة 2017/9/16)، س 68، دائرة جنائى، متاح على الموقع الرسمى لمحكمة النقض:

http://www.cc.gov.eg/courts/cassation_court/all/cassation_court_all_cases.aspx

(1) أ/ نبيلة هبه هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات (دراسة مقارنة)، مرجع سابق، صـ 141 وما بعدها.

تستخدمها فى إدارة شئونها لذا فقد أصبح لزاماً على الدولة أن تحمى هذا الكيان الجديد وتوفر له وسائل تأمينية تتفق وطبيعته والناحية القانونية وفى سبيل تحقيق ذلك، تقوم إدارة البحث الجنائى بمواجهةالجرائم التقليدية بالإضافة لجرائم المعلومات عبر شبكة الإنترنت كالقذف والسب والتشهير والإبتزاز والسرقة والاحتيال وإتلاف وتدمير برامج الكمبيوتر وقواعد البيانات أو نسخها واستغلالها بدون إذن صاحبها أو من آلت إليه حقوقه، عن طريق اختراقها وانتهاك حقوق الملكية الفكرية[2] بالتنسيق مع جهات الوزارات المتخصصة فى هذا المجال وذلك باستخدام تقنيات أمنية فائقة التطور للتوصل لمرتكبى هذه الجرائم، إذ أن عملية التوصل للجناة فى جرائم المعلوماتية هى عملية ذات مزيج من أعمال البحث الجنائى التقليدية من جمع تحريات وأدلة بالإضافة إلى الجوانب الفنية أوالتقنية[1].

إن جرائم تقنية المعلومات من الأهمية بمكان لتحظى بالاهتمام من كافة المؤسسات، وعلى رأسها المؤسسة التشريعية، والمؤسسة القضائية، فضلاً عن المؤسسة التنفيذية وجهاز الشرطة، وإدراجها ضمن التشريعات الوطنية المختلفة، كما إدراك أن جرائم الإنترنت ذات بعد دولى تتطلب الانخراط فى اتفاقيات دولية، والاهتمام بالتعاون الدولى فى مجال المكافحة. كما أن مبدأ الوقاية فى جرائم الإنترنت خير من العلاج وبشكل خاص فما يخص التشريعات، والتدريب، تعديل بعض التشريعات الحالية بما يتلائم مع طبيعة جرائم الإنترنت، والتقنية، وتثقيف العاملين فى الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح، مع إيضاح الحكم الشرعى الإسلامى تجاه جرائم الحاسبات والإنترنت، ونشرها ضمن برامج التوعية العامة. وفى مجال الإجراءات الفنية والإدارية مساعدة شركات التقنية والإنترنت

---

[2]Tribunal de Grande Instance de Paris 17ème chambre, chambre de la presse Jugement du 2 novembre 2000,Françoise V., Marc F. et Hans H. / ministère public,.
Arrêt du 17 décembre 2001 de la Cour de Paris, Jurisprudence.

[1] وفى إحدى الوقائع، قامت إدارت البحث الجنائى بمحافظة الغربية بتحقيق وضبط العديد من القضايا ومرتكبى جرائم المعلوماتية، ومن أمثلة ذلك: واقعة المحضر 61 ح قسم المصنفات الفنية فى ديسمبر 2009(تشهير وسب وقذف) بشأن إنشاء صفحة على موقع فيس بوك للمجنى عليها، ونشر صور لها تسىء إلى سمعتها وتشهر بها وسط أقرانها وإرسال دعوات لقائمة مراسلاتها لمشاهدة تلك الصور والتعليقات التى أسفلها التى تسىء لسمعتها ووضع رقم تليفونها المحمول مما تسبب فى اتصالات كثيرة أساءت لسمعة المجنى عليها وسببت لها إيذاءاً نفسياً شديداً. أسفر الفحص الفنى عن تحديد اسم وعنوان مالك الحاسب الذى تم إنشاء صفحة الفيس بوك محل الشكوى منه ورقم الخط التليفونى المستخدم فى ذلك، وتحرر بذلك محضر رسمى بمعرفة خبير، أرفق بملف القضية، بإجراء التحريات السرية التقليدية حول مستخدم الجهاز المذكور توصلت إلى تحديد شخصه وعقب تقنين الإجراءات تم ضبط الجانى وتقديمه للمحاكمة.... بدون، دور أجهزة البحث الجنائى فى مكافحة جرائم المعلومات، متاح على: Available At:http://Kenanaonline.com/users/hossapo/downloads/53393.

العربية فى اتخاذ إجراءات أمنية مناسبة سواء من حيث سلامة المنشآت، أو ما يختص بقواعد حماية الأجهزة والبرامج. أيضاً مساعدة شركات إنتاج البرامج العربية فى مجال تطوير أنظمة تشغيل، وبرامج تطبيقات عربية، وكذلك برامج حماية عربية للتخفيف من الاعتماد على الصادرات فى هذا المجال مع ما تحمله من مخاطر أمنية محتملة. ووضع سياسات عمل، وإجراءات إدارية وفنية واضحة فيما يختص بأمن المعلومات، والحرص على أن يطلع عليها العاملون فى الإدارة، وتحدث بشكل دورى. مع أهمية المرونة المالية فى شراء العتاد، والبرمجيات التى تكفل بناء، وصيانة أنظمة وشبكات المعلومات تتوافر لها الحماية فى جميع الأوقات. وعقد اجتماعات دورية للمسئولين عن تقنية المعلومات لتبادل الخبرات والمعلومات فيما يختص بأمن الحاسبات وجرائم الحاسب. فضلاً عن إعادة رسم الأولويات الوطنية مع التأكيد على أن المعلومات فى عصر المعلومات ثروة وطنية تستحق كل الجهود والموارد المالية والبشرية للمحافظة عليها وصيانتها. والتنسيق لإنشاء مركز معلومات أرشيف عربى مشترك يهتم برصد جرائم الحاسبات يضم معلومات مكتملة عن الجرائم لأى واقعة ومعلومات عن المجرمين والمشتبه بهم ، فضلاً عن التعاون وتبادل المعلومات مع جهاز الشرطة الدولية (الإنتربول) فى هذا المجال، حيث أن جريمة الإنترنت لا تحدها حدود وطنية أو قومية[1]. مع تفعيل والتحفيز بشأن الحصول على شهادة الآيزو فى مجال الأمن المعلوماتى على مستوى القطاعات الحكومية والخاصة[2].

---

[1] أ/ وليد الكشباطى، جرائم اختراق الأنظمة المعلوماتية، الجمعة 12 حزيران (يونيو) 2009، متاح على:

- Available At:http://www.chawkitabib.info/spip.php?article477

[2] الآيزو (ISO) هى المنظمة الدولية للمعايير International Organization For Standardization، وهى اتحاد عالمى ومنظمة غير ربحية مقرها فى جنيف، أنشئت عام 1946، وبدأت فعلياً عام 1947م، وتضم فى عضويتها ممثلين عن أكثر من 561 هيئة تقييس وطنية، وكلمة (ISO) هى ليست مختصراً للاسم السابق وإنما أخذت من كلمة يونانية الأصل يطلق عليها (ISOS)، وهى تعنى التساوى، وتتمثل جهودها بعمل مواصفات ومقاييس موحدة ومقبولة من كل الأطراف والدول لتقييم جودة المنتجات والخدمات المتبادلة تحت ضوابط ومقاييس تحقق الجودة فى ظل تحرير التجارة الدولية فى شتى المجالات، ومن أهمها إدارة الجودة والبيئة والسلامة والمختبرات وسلامة الغذاء وأمن المعلومات وغيرها من المجالات، وذلك اعتماداً واستفادة من المواصفات المتوافرة سواءً العسكرية منها والمدنية كالمواصفات الأمريكية والبريطانية. والمعيار الدولى (ISO/IEC27001) هو مواصفة دولية تعد أحد أحدث إصدارات المنظمة فى مجال إدارة الأمن المعلوماتى بعد تحديث النسخة الأولى، والتى يطلق عليها (ISO17799)، ويأتى هذا المعيار كمقابل للمعيار البريطانى (BS7799). ويعمل المعيار (ISO/IEC27001) على تقييم إجراءات الأمن المتبعة فى بيئات تكنولوجيا المعلومات، ويولى اهتماماً خاصاً بإجراءات العمل ذات العلاقة بتحديد التدابير ذات الأولوية، كما أنه يحدد الاشتراطات والالتزامات لتأسيس وتطبيق وتشغيل وصيانة محتوى وثيقة المعيار فى إطار المنظمة بحيث يأخذ فى الاعتبار جميع الأخطار المحتملة التى قد تتعرض لها المنظمة سواءً كانت هذه المنظمة حكومية أو منشأة تجارية أو خيرية. أيضاً يحدد هذا المعيار الشروط اللازمة لتطبيق نقاط التحكم الأمنية التى تلبى احتياجات كل منظمة على

الخاتمة

تتسم الجرائم السيبرانية من حداثة فى الأسلوب وسرعة فى التنفيذ و سهولة فى إخفائها، و القدرة على محو آثارها حيث أثبتت الوقائع العملية أن هناك جرائم متعلقة بالحاسب الآلى والإنترنت قد ارتكبت على مرآى و مسمع من رجال الشرطة، بل قام بعض رجال الشرطة بتقديم المساعدة لمرتكبى هذه الجرائم دون قصد و عن جهل، على سبيل واجبات المهنة التى يلزمهم بها هذا القانون. ونظراً لطبيعة الجرائم المعلوماتية الخاصة فإنه توجد صعوبة فى دور الشرطة الوقائى لمنع ارتكاب هذه الجرائم خصوصاً إذا كان محلها البيانات التى تحويها الملفات أو الأسطوانات أو بنوك المعلومات. كما أن الملاحقة الجنائية فى جرائم الكمبيوتر تتطلب استراتيجية خاصة بخبرة رجال الشرطة وجهات الإدعاء والقضاء على نحو يساعدهم على مواجهة تقنيات الحاسب الآلى المتطورة وتقنيات التلاعب فيه حيث تتعقد التقنيات المرتبطة بوسائل ارتكاب الجرائم الخاصة بها. لذلك فإنه يجب استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبيها، وكيفية ارتكابها مع الاستعانة بوسائل جديدة كذلك لضبط الجاني والحصول على أدلة إدانة.

ويخلص الباحث فى بحثه بعدة نتائج مقدماً عدة توصيات، يشرف بأن يودعها أمانة المؤتمر الدولى المنعقد، آملاً من الله سبحانه وتعالى أن تضىء شمعة فى سماء مكافحة الاجرام السيبرانى وتحقيق الأمن المعلوماتى وما ينعكس أثرة على تطور العلوم الانسانية فى مصر ودول العالم، على النحو التالى:

النتائج

- يفرض التقدم المتواصل فى تكنولوجيا الحاسب الآلى والإنترنت على جهات إنفاذ القانون أن تسير فى خطوات متناسقة مع التطورات السريعة التى تشهدها هذه التقنيات، والإلمام بها حتى يمكن التصدى للأفعال الإجرامية التى صاحبت هذه التكنولوجيا ومواجهتها.
- إن إعمال القانون فى مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادىء المستقرة فى المدونة العقابية التقليدية.
- ظهرت آثار جهود وزارة الداخلية فى مجال مكافحة جرائم القرصنة المعلوماتية، وتتمثل فى زيادة معدلات الاستثمار فى صناعة تكنولوجيا المعلومات وانخفاض معدلات القرصنة على البرمجيات.

حدة أو أى فرع من تلك المنظمة، وقد حظى هذا المعيار باهتمام عالمى متزايد، حيث يذكر أنه "على رأس معايير آيزو التى يبلغ عددها 15 ألفاً يأتى هذا المعيار مع معايير الإدارة الشهيرة (آيزو 9000) ضمن أعلى عشرة معايير والتى يسأل معظم المستخدمين عنها .... للمزيد: د/ عمر بن محمد العتيبى، الأمن المعلوماتى فى المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، مرجع سابق، صـ 24 وما بعدها.

- عدم التناسق بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحرى والتحقيق فى الجرائم المتعلقة بالكمبيوتر.
- تأتى الولايات المتحدة الأمريكية وفرنسا فى مقدمة الدول التى واجهت الجرائم المعلوماتية، وذلك بالنص على مواجهتها تشريعياً، وأمنياً.
- من حق المتهم الاستعانة بمحام فى حضور التحقيق مع موكله أمام دوائر الشرطة وفقاً لنص المادة 52 من قانون المحاماه.

التوصيات

- التدريب والتعليم المستمر بشأن تقنيات الحاسب الآلى، مع تطوير العملية التدريبية والإرتقاء بها و النهوض بأساليب تحقيقها لأهدافها، مما يتطلب وجوب تأهيل القائمين على هذه الأجهزة.
- وضع الخطط الكفيلة والبدائل بإجهاض دورة السلوك الإجرامى والحيلولة دون اكتمال عناصرها وكذا الاهتمام برسالة الإعلام الأمنى والتركيز على دوره فى منع الجريمة.
- تفعيل دور الدور الأمني الوقائى لجهاز الشرطة (شرطة مكافحة جرائم الحاسب وشبكات المعلومات) فى مكافحة الجريمة الإلكترونية.
- استخدام تقنيات عالية لرصد العناصر الإجرامية التى تستخدم شبكة المعلوماتية للنصب على ضحاياها.
- مداومة المرور على شركات تقديم خدمات الإنترنت والعمل على تجنيد أحد المصادر بها للإبلاغ عن أي شئ غير عادي يحدث.
- تفعيل التعاون الدولى و التنسيق فى مجال تدريب رجال الضبطية الإدارية والقضائية.
- زيادة العناية بأعمال الخبرة الفنية القضائية المتخصصة بالإثبات العلمي الفنى للجرائم الرقمية، فضلاً عن إقامة علاقات تبادل وتكامل فى هذا المجال مع الدول العربية من جانب، وبينها وبين غيرها من الدول المتقدمة من جانب آخر.
- الأخذ بمبدأ تعدد الخبراء فى جرائم التقنية المعلوماتية.
- إنشاء قاعدة بيانات عن جميع نوادى التكنولوجيا المستخدمة لشبكة الانترنت وكذلك جميع الشركات والمؤسسات.

- توفير أساليب تأمين مختلفة لمواجهة جرائم التكنولوجيا الحديثة يجب على جهاز الشرطة اتباعها.
- العمل على نشر شبكة اتصال بين الشركات والجهات الكبرى التى تعتمد على الحاسبات الآلية بأجهزة الشرطة بحيث يتم المتابعة من قبل أجهزة الشرطة ورصد أى محاولات للدخول والاقتحام، ومن ثم التعامل معها.
- ضرورة إنشاء مركز قومى لأمان الحاسب الآلى والمعلومات، مع امكانية الاستفادة بأن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز القومي لتنظيم الاتصالات المنشأة بالقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات– نواة لهذا المركز وهو ما يأمله الباحث، على أن يعمل على تطويره.
- الاستفادة من تجربة دولة المملكة العربية السعودية فى إنشاء مركز للتميز فى الأمن المعلوماتى.
- الاستفادة من تجربة دولة السويد فى إنشاء مركز شرطة على الإنترنت لتلقى البلاغات والشكاوى (صوت وصورة) وتسديد الغرامات.
- الاستفادة من تجربة دولة الصين والامارات فى الرقابة على الانترنت.
- تنمية الوعى القانونى بالتزام مقدمى الخدمة مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات الصادر بالقانون رقم 10 لسنة 2003، بحفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوما متصلة، وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي : (أ) البيانات التي تمكن من التعرف على مستخدم الخدمة . (ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة . (ج) البيانات المتعلقة بحركة الاتصال . (د) البيانات المتعلقة بالأجهزة الطرفية للاتصال . (هـ) أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز . (مادة 2 من القانون رقم 175 لسنة 2018).
- تنمية الوعى القانونى بالتزام مقدمى الخدمة بالمحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها . فضلاً عن تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها .
- تنمية الوعى القانونى بالتزام مقدمى الخدمة مع عدم الإخلال بأحكام قانون حماية المستهلك، بأن يوفر لمستخدمي خدماته ولأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية : 1- اسم مقدم الخدمة وعنوانه -2 .معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني -3 .بيانات الترخيص لتحديد هوية مقدم

الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها -4 .أي معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمي الخدمة، ويصدر بتحديدها قرار من الوزير المختص .
- تنمية الوعى القانونى بالتزام مقدمى الخدمة مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي ووفقا لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون .
- تنمية الوعى القانونى بالتزام مقدمى الخدمة ووكلائهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غيرهم القيام بذلك.

قائمة المصادر والمراجع

الكتب القانونية العامة

- د/ أحمد فتحى سرور، قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، ط6، 2015.
- د/ أحمد فتحى سرور، قانون العقوبات، القسم الخاص، الكتاب الأول، دار النهضة العربية، القاهرة، ط6، 2016.
- د/ أحمد فتحى سرور، الوسيط فى قانون الإجراءات الجنائية، الكتاب الأول، دار النهضة العربية، القاهرة، ط10، 2016.
- د/ مأمون محمد سلامة، قانون الإجراءات الجنائية معلقاً عليها بالفقه وأحكام النقض طبقاً لأحدث التعديلات والأحكام ، ط3، دار طيبة للطباعة، الجيزة، 1430هـ – 2010م.
- د/ محمد ذكى أبو عامر، الإجراءات الجنائية، منشأة دار المعارف، الإسكندرية، 1997.
- د/ محمود نجيب حسني، شرح قانون العقوبات، القسم العام، الطبعة السابعة، دار النهضة العربية، القاهرة، 2012.

الكتب القانونية المتخصصة

- د/ عبد الفتاح بيومي حجازى، مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006.
- د/ قدرى عبد الفتاح الشهاوى، قانون التوقيع الإلكتروني ولائحته التنفذية والتجارة الإلكترونية فى التشريع المصري والعربي والأجنبي، دار النهضة العربية، القاهرة، 2006.
- أ/ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2007.

- د/ مصطفى محمد موسى, الجهاز الإلكتروني لمكافحة الجريمة, ط1, سلسلة اللواء الأمنية فى مكافحة الجريمة الإلكترونية, 2001.
- د/ جولييه، نظام الدعم الدولى لتلبية الحاجات الأساسية، كتاب حاجات الإنسان الأساسية فى الوطن العربى، الجوانب البيئية والتكنولوجيا والسياسات، ترجمة د/ عبد السلام رضوان، ط1، المجلس الوطني للثقافة والفنون والآداب، مطبعة السياسة (موسوعة عالم المعرفة)، الكويت، 1990.

الرسائل:

- د/ إيهاب عبدالسميع روبى محمد، الجريمة عبر الانترنت، صورها ومشاكل اثباتها، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2016.
- د/ أحمد يوسف أحمد حسين الطحاوى، الأدلة الالكترونية ودورها فى الاثبات الجنائى- دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2015.
- د/ طلعت محمد الدسوقى الشهاوى، المسئولية الجنائية عن جرائم الاتصالات- دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2016.
- د/ عمر بن محمد العتيبى، الأمن المعلوماتى فى المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة مقدمة استكمالاً لمتطلبات الحصول على درجة دكتوراه الفلسفة فى العلوم الأمنية، قسم العلوم الإدارية، كلية الدراسات العلما، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 1431 هـ، 2010م.
- د/ محمد كمال عبد السميع شاهين، الجوانب الإجرائية للجريمة الالكترونية فى مرحلة التحقيق الابتدائى – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، 2015.
- أ/ محمد مصطفى حامد سعيد، تحليل وتعميم تأثير تطبيق تكنولوجيا المعلومات على التخطيط للأعمال الشرطية (مع التطبيق على قطاع الأمن العام، رسالة مقدمة للحصول على درجة العضوية فى العلوم الإدارية، أكاديمية السادات للعلوم الإدارية، المعهد القومى للإدارة العليا، 2004.

الأبحاث والمقالات:

- د/ أحمد يوسف محمد السولية، التدريب التخصصى على مواجهة الجرائم المعلوماتية ، بحث منشور بندوة المواجهة الأمنية للجريمة المعلوماتية، كلية الشرطة، أكاديمية الشرطة، إبريل، 2009.
- د/ هشام فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائى الفنى، بحث منشور بمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، بالتعاون مع مركز الإمارات للدراسات و البحوث الاستراتيجية و مركز تقنية المعلومات بالجامعة فى الفترة من 1 – 3 مايو 2000، المجلد الأول، ط 3، 2004.

- أ/ مجدى فؤاد، الجريمة المعلوماتية وحماية حقوق الملكية الفكرية، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، إبريل، 2009.
- أ/ عاصم الشريف، القرصنة على البرمجيات وجهود وزارة الداخلية فى مواجهتها، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، إبريل 2009.
- أ/ مروان عادل عبده، الدور الأمني فى مواجهة صور الجريمة المعلوماتية، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، إبريل 2009.
- أ/ محمد عبد اللطيف فرج، مشكلات ملاحقة وتحقيق الجرائم المعلوماتية، مجلة مركز البحوث بأكاديمية الشرطة، العدد العاشر، 2000.
- د/ أيمن عبد الحفظ عبد الحميد سليمان، الدور الفنى لأجهزة الشرطة فى مواجهة الإجرام المعلوماتى، ندوة لمواجهة الجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، 7 إبريل 2009.
- أ/ وليد جاد، رئيس غرفة الاتصالات وتكنولوجيا المعلومات باتحاد الصناعات، بوابة الأهرام، 2018/7/2، متاح على: - gate.ahram.org.eg/news/1976109
- أ/ محمد أبو زيد - مدير مباحث الإنترنت - حول رصد مرتكبى الجرائم الإلكترونية، جريدة الأهرام اليومى، يوليو 2014، متاح على: http://digital.ahram.org.eg/articles.aspx?serial=1642232=11472
- د/ فؤاد جمال الدين، التطور التشريعي لحماية البرمجيات مع إشارة خاصة لمصر، ندوة المواجهة الأمنية للجريمة المعلوماتية, مركز بحوث الشرطة، أكاديمية الشرطة، إبريل، 2009.
- المؤتمر الدولي لأمن المعلومات الذي نظمته بلدية مسقط بالتعاون مع المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية، 2005/12/22، متاح على: http://www.albayan.ae/economy/2005-12-22
- أ/ حسام رأفت، العولمة وآثارها على الاستقرار الأمني، مجلة الأمن العام، المجلة العربية لعلوم الشرطة، العدد 302، 1429ه، أكتوبر 2008.
- بدون، جرائم الحاسبات والإنترنت، الجرائم المعلوماتية، تاريخ الإنترنت ونشأة العالم الإفتراضى، متاح على: -Available At:http://adel- amer.catsh.info/vb/showthread.php?p=3967
- أ/ وليد الكشباطى، جرائم اختراق الأنظمة المعلوماتية، الجمعة 12 حزيران (يونيو) 2009، متاح على:
- Available At:http://www.chawkitabib.info/spip.php?article477

- د/ محمد أبو العلا عقيدة، التحقيق و جمع الأدلة فى مجال الجرائم المعلوماتية، متاح على: موقع الموسوعة الإلكترونية العربية www. Arablaw inf.com
- د/ مفتاح بوبكر المطردى، المستشار بالمحكمة العليا الليبية، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا فى الدول العربية بجمهورية السودان المنعقد فى الفترة من 23 – 25 /9/ 2012.
- أ/ محمد يوسف محمد، التحديات التى تواجه التحقيقات فى الجرائم، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، 7إبريل 2009.
- بدون، الجريمة الإلكترونية فى الوطن العربى، متاح على:
- Available At: http:// eljaraimeliliktouniya.blogspot.com

- بدون، جرائم الحاسبات والإنترنت، الجرائم المعلوماتية، تاريخ الإنترنت ونشأة العالم الافتراضى، متاح على:
- Available At:http://adel-amer.catsh.info/vb/showthread.php?p=3967

الأحكام القضائية:
- مجموعة القواعد القانونية التى قررتها محكمة النقض.
- مجموعة أحكام محكمة النقض التى يصدرها المكتب الفنى لمحكمة النقض.

التشريعات والاتفاقيات:
- قانون العقوبات والإجراءات الجنائية وتعديلاتهما.
- قانون حماية حقوق الملكية الفكرية المصرية رقم 82 لسنة 2002 – الجريدة الرسمية – العدد 22 مكرر -2 يونيه 2002.
- القانون رقم 15 لسنه 2004 بشأن تنظيم التوقيع الإلكترونى و بإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات فى إبريل سنة 2004- الجريدة الرسمية – العدد 17 تابع (د) فى 22 إبريل سنة 2004.
- قانون مكافحة الإرهاب المصرى رقم 94 لسنة 2015، الجريدة الرسمية، العدد 33 مكرر، 30 شوال 1436، 15 أغسطس 2015.
- القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر ج فى 14 أغسطس سنة 2018.
- قانون إمارة دبى رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية، صدر فى دبى بتاريخ 12 فبراير 2002م، الموافق 30 ذى القعدة 1422هـ .
- قانون حماية حقوق المؤلف والحقوق المجاورة الإتحادي الاماراتى رقم (7) لسنة 2002

-المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات فى دولة الإمارات العربية المتحدة، منشور بالجريدة الرسمية العدد 540 ملحق السنة الثانية والأربعون - بتاريخ 26-8-2012، متاح على:
http://rakpp.rak.ae/ar/Pages/%D9%85%D8%

المراجع الأجنبية (Références):

المراجع الأجنبية باللغة الفرنسية (Les Ouvrage , Les Recherché et Les Articl,):

-L'ACTUALITÉ DU DROIT DES NOUVELLES TECHNOLOGIES, MARDI 18 SEPTEMBRE 2001,Recherche surLEGALIS,https://www.legalis.net/recherche/?recherche.
- Les 50 décisions clés du droit de l'Internet Broché – 1 juin 2015 de Collectif (Auteur) Editeur : Celog; Édition : Edition 2015 (1 juin 2015),https://www.amazon.fr/Les-d%C3%A9cisions-cl%C3%A9s-droit-lInternet/dp/2955292400
-D. de Villepin double le nombre des policiers et gendarmes liés à la cybercriminalité, MARDI 07 SEPTEMBRE 2004, https://www.legalis.net/actualite/d-de-villepin-double-le-nombre-des-policiers-et-gendarmes-lies-a-la-cybercriminalite
- Sommet mondial sur la Cybercriminalité : rencontre du G8, MARDI 16 MAI 2000,https://www.legalis.net/actualite/sommet-mondial-sur-la-cybercriminalite-rencontre-du-g8/
-https://www.legalis.net/actualite/dominique-de-villepin-confie-le-chantier-cybercriminalite-a-thierry-breton/

الأحكام القضائية الأجنبية باللغة الفرنسية (les Arrêts):

- Cour de cassation Chambre criminelle Arrêt du 6 novembre 2013,Patrick X. / Ministère public,https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-6-novembre-2013/

- Cour de cassation Chambre criminelle Arrêt du 22 octobre 2013,Mohamed X. / Ministère public,https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-22-octobre-2013
- Tribunal correctionnel de Nanterre Jugement du 10 novembre 2011,Greenpeace et autres / EDF et autres,https://www.legalis.net/jurisprudences/tribunal-correctionnel-de-nanterre-jugement-du-10-novembre-2011
- Cour d'appel de rennes 5ème chambre Prud'homale Arrêt du 12 décembre 2006Accel Informatique / Sébastien L. M. https://www.legalis.net/jurisprudences/cour-dappel-de-rennes-5eme-chambre-prudhomale-arret-du-12-decembre-2006
-Tribunal de Grande Instance de Paris 17ème chambre, chambre de la presse Jugement du 2 novembre 2000,Françoise V., Marc F. et Hans H. / ministère public,Arrêt du 17 décembre 2001 de la Cour de Paris, Jurisprudence
- Dommages-intérêts à payer par les membres mineurs du forum Utopi-Board, JEUDI 10 JANVIER 2019, https://www.legalis.net/actualite/dommages-interets-a-payer-par-les-membres-mineurs-du-forum-utopi-board/
- Crim 9 juill 2003, Bull, n° 137
– Crim.10 mai.2001,Bull.n°114, 2 Fevr.2005,Bull.n°411

المراجع الأجنبية باللغة الانجليزية (The Books, The Research & articles):

- Jahankhani, Hamid (Ed.), Cyber Criminology,2018,https://www.springer.com/gp/book/9783319971803
- Kshetri, Nir,The Global Cybercrime Industry,Economic, Institutional and Strategic,Perspectives,2010,https://www.springer.com/gp/book/9783642115219
- Smith, Russell G., Chak-Chung Cheung, Ray, Yiu-Chung Lau, Laurie (Eds) Cybercrime Risks and Responses,Eastern and Western

Perspectives,2015,https://www.springer.com/gp/book/9781137474155#aboutBook
- DR.ANDRÉ ÅRNES, Digital forensics,Publisher: Wiley; 1 edition (July 24, 2017),https://www.amazon.com/Digital-Forensics-Andr-eacute-Aring/dp/1119262380/
-Series Editors: Sheptycki, James, Tsoukala, Anastassia,Transnational Crime, Crime Control and Security,https://www.springer.com/series/14398
-hiva V.N. Parasram, Digital Forensics with Kali Linux: Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools Paperback – December 19, 2017,Packt Publishing - ebooks Account (December 19, 2017),https://www.amazon.com/dp/1788625005/ref=sspa_dk_detail_2?psc=1
- https://kmph.com/news/local/clovis-police-hit-the-jackpot-with-3-identity-theft-arrests

الأحكام القضائية الأجنبية باللغة الانجليزية

:(Jurisprudence/ Judicial decisions)

-State v. Castagnola, 2013-Ohio-1215,https://cases.justia.com/ohio/ninth-district-court-of-appeals/26185.pdf?ts=1396138498
--U.S. Supreme Court,United States v. White, 401 U.S. 745 (1971),United States v. White,No. 13,Argued November 10, 1969,Reargued October 20, 1970,Decided April 5, 1971,401 U.S.745,https://supreme.justia.com/cases/federal/us/401/745
-United States v. Jones, 565 U.S. 400 (2012),https://supreme.justia.com/cases/federal/us/565/400/
-State v. Stefan, https://cases.justia.com/ohio/eighth-district-court-of-appeals/2018-104979.pdf?ts=1516907492

المواقع الإلكترونية على شبكة الإنترنت (WEB Sites):

- http://Kenanaonline.com/users/hossapo/downloads/53393.
- www.al-madina.com/node/582132
- www.moi.gov.sa
-http://rakpp.rak.ae/ar/Pages/%D9%85%D8%-
-http://digital.ahram.org.eg/articles.aspx
- http://www.cc.gov.eg/courts/cassation_court/

-https://www.legalis.net
-https://cases.justia.com
-https://supreme.justia.com
-https://www.springer.com
-https://www.amazon.com

ملخص بحث عن
دور الشرطة فى مكافحة الجرائم السيبرانية
المستحدثة وتحقيق الأمن المعلوماتى- دراسة مقارنة

ترجع أهمية الدراسة محل البحث لأهمية دور الشرطة فى مجال مكافحة جرائم المعلوماتية لما فرضته المتغيرات على الساحة الدولية ومنها ما تفرضه التحديات التى تواجه مرحلة النمو الاقتصادى الرقمى التى تمر بها البلاد والتى تستلزم وجود مناخ اقتصادى مستقر يعتمد على المنافسة الشريفة وتكافؤ الفرص، فضلاً عن تطور أنماط الجريمة بمختلف أشكالها باستخدام الحاسب الآلى، سواء التى تنال من الأشخاص أو الأموال أو المصلحة العامة.

لقد هدفت الدراسة محل البحث إلى: النهوض بدور الشرطة فى مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى أسوةً بالتجارب الموجودة فى الدول المتقدمة؛ من خلال دراسة تحليلية مقارنة.

وانطلاقاً من أهمية موضوع الدراسة محل البحث، ونظراً لما عرضه الباحث سابقاً، وكضرورة تقتضيها البحوث العلمية فقد رأينا أن نقدم لموضوع دراستنا فى أربعة مباحث؛ يتناول دور الشرطة الوقائي فى مواجهة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث أول، ثم يتناول دور الشرطة فى ملاحقة وتعقب مرتكبي الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث ثان، ثم يتناول دور جهاز الشرطة الدولية (الإنتربول) بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث ثالث، ثم يتناول مقترحات تطوير الدور الأمنى لجهاز الشرطة بشأن مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتى فى مبحث رابع.

وفى نهاية المطاف؛ انتهى الباحث الى مجموعة من النتائج مقدماً عدة توصيات بشأن النهوض بدور الشرطة فى مكافحة الجرائم السيبرانية المستحدثة ومن ثم تحقيق الأمن المعلوماتى وما ينعكس أثره على العلوم الإنسانية ومن ثم اثرائها.

الكلمات الدالة:
الشرطة- الجرائم السيبرانية- الأمن المعلوماتى – الجرائم الإلكترونية – الانتربول – الأوربول- الأورجست – تطوير

Research Summary
The role of the police in facing the new cybercrimes and the attainment of the cybersecurity - Comparative Study

The importance of the role of the police in the field of facing cybercrime is attributed to the changes imposed on the international scene, such as the challenges facing the country's digital economic growth stage, which necessitates a stable economic environment based on honest competition and equal opportunity. As well as the evolution of crime types in various forms using the computer, whether they affect persons, property or public interest.

The aim of the study in question is to: Promote the role of the police in facing the new cybercrimes and the attainment of the cybersecurity like developed countries experiences, through a comparative analytical study.

In view of the importance of the subject of the study in question, and in view of what was previously presented by the researcher, and the necessity of scientific research, we decided to present the subject of our study in four sections. The preventive role of the police in facing the new cybercrimes and the attainment of the cybersecurity in the first section. The role of the police in tracking the perpetrators of the new cybercrimes and the attainment of the cybersecurity in the second section. The role of the International Police Organization (INTERPOL) in facing the new cybercrimes and the attainment of the cybersecurity in a third section. Then, the proposals to develop the security role of the police in facing the new cybercrimes and the attainment of the cybersecurity in the fourth section.

Finally, the researcher ended up with a number of recommendations. He made several recommendations on enhancing the role of the police in facing the new cybercrimes in order to achieve

the cybersecurity and the impact of this on human sciences and its enrichment.

Key words :
Police - Cybercrime - Information Security - Cybersecurity - Electronic Crimes - Interpol - Europol - Eurojust - Development

Research
"The role of the police in facing the new cybercrimes and the attainment of the cybersecurity"
" Comparative Study"

Preparation
DR / Saad Attef Abdul Muttalib Hassanien
Doctorate in criminal law
And the agent
of the Patent Office - Menoufia University

2019 A.D / 1440 A.H