



المحاضرة الخامسة عالمية الجريمة السيبرانية ومراحل إرتكابها

• عناصر المحاضرة:

المحور الأول : عالمية الجريمة السيبرانية:

- أولا: مفهوم الجريمة العالمية بصفة عامة.
 - ثانيا : الجرائم السيبرانية هي جرائم عالمية.
 - ثالثا : علاقة الجريمة العابرة للحدود بالإنترنت.
 - رابعا: أسباب جعل الجريمة السيبرانية جريمة عالمية:
١. إنفتاح شبكة المعلوماتية.
 ٢. انعدام الحواجز الجغرافية.
 ٣. صعوبة الكشف عن هوية المستخدم.
 ٤. بساطة التعامل مع الإنترنت وزهد ثمنه.

المحور الثاني : مراحل إرتكاب الجرائم السيبرانية:

- أولا: مرحلة الإدخال.
- ثانيا: مرحلة المعالجة.
- ثالثا: مرحلة الإخراج.

المحور الأول

عالمية الجريمة السيبرانية

• تمهيد وتقسيم :

الجرائم السيبرانية لم تعد تقتصر علي النطاق الوطني فقط، بل بدأت تأخذ بعدا دوليا نتيجة لسهولة الاتصالات الإلكترونية السلوكية واللاسلكية التي أحاطت بالعالم وجعلت منه قرية صغيرة لا يعترف فيها بحدود طبيعة أو سياسية وإن من أهم السمات التي تميز الجريمة السيبرانية هي تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية للحدود، أو عالمية الجريمة السيبرانية.

ولكي نتعرف على عالمية الجريمة السيبرانية، يجب أن نتعرف على مفهوم الجريمة العالمية بصفة عامة وبصفة خاصة، وعلاقتها بالإنترنت والتعرف على الأسباب التي جعلتها جريمة عالمية وذلك علي النحو التالي:

أولا: مفهوم الجريمة العالمية بصفة عامة :

إذا كانت الجريمة الدولية مصدرها القانون الدولي الجنائي، فإن الجريمة العالمية مصدرها في الحقيقة هو القانون الجنائي الوطني، أو بالأحرى القوانين الجنائية الوطنية مجتمعة.

فالجريمة العالمية هي جريمة داخلية يعاقب عليها قانون العقوبات بالفعل في كل الأنظمة القانونية المتمدينة؛ لأنها تتمثل في التصرفات المنافية للأخلاق والمنطوية علي عدوان علي القيم البشرية الأساسية في العالم المتمدين ... كالحياة

وسلامة الجسم، ونضيف إلى ذلك مختلف الصور الإجرامية التي يعرفها قانون العقوبات المصري - علي سبيل المثال- من جرائم المخدرات، إلى تزيف العملة إلى الجرائم الأخلاقية الخ.

ويرجع سر تسمية هذه الجرائم بالجرائم العالمية - فضلاً عن الاعتبار المتقدم - إلى اعتبار آخر أصبحت له السيادة في الوقت الحالي وهو مزاوله هذه الأنشطة الإجرامية علي مستوي عالمي، وعبر الدول والحدود نتيجة للتقدم المذهل في وسائل الاتصالات والمواصلات ، وعن طريق عصابات دولية تتفنن في إضفاء صبغة مشروعة علي أنشطتها الإجرامية.

ثانيا : الجرائم السيبرانية هي جرائم عالمية:

إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية، والفضائيات، والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمراً شاسعاً، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان ولا بالزمان، بل أصبحت ساحتها العالم أجمع .

ففي مجتمع المعلومات تتلاشى الحدود الجغرافية للدول؛ لارتباط العالم بشبكة واحدة؛ حيث إن أغلب الجرائم المرتكبة عبر الإنترنت ، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى، وقد يكون الضرر المترتب عن الجريمة ليس واقعا علي المجني عليه داخل إقليم دولة الجاني.

ويري الفقهاء أن الجرائم المتصلة بنظم المعالجة الآلية للمعلومات هي جرائم عالمية لأنها باعتبارها ابتكارات علمية وتقنية جديدة تهدف كل دولة إلى حماية ما وصلت إليه فيها، مما شجع الدول علي التعاون في مجال مكافحة الإجرام السيبراني علي المستويين العالمي والإقليمي ولعله بات واضحاً من بيان ما سبق أن الجريمة

العالمية هي جريمة داخلية في حقيقتها، وأن أركان تلك الجريمة هي أركان الجريمة الداخلية ذاتها، ومضافاً إليها البعد الدولي الذي أشرنا إليه وهو ارتكاب الجريمة عبر عدة دول.

• ملحوظة هامة:

ولكن البعد الدولي في الجريمة العالمية لا يصح أن يختلط بالركن الدولي في الجريمة الدولية، فبينما الركن الدولي في الجريمة الدولية يتصل بسلوك دولة بشكل أو بآخر فإن البعد الدولي في الجريمة العالمية يعبر عن مشكلة تتعلق بالاختصاص المكاني، أو بقواعد سريان قانون العقوبات الوطني من حيث المكان.

ولبيان الصورة بشكل أوضح يعرف بعض الفقهاء الجريمة الدولية بأنها هي كل سلوك - فعلاً كان أو إمتناعاً - إنساني يصدر عن فرد باسم الدولة أو برضاء منها صادر عن إرادة إجرامية يترتب عليه المساس بمصلحة دولية مشمولة بحماية القانون الدولي عن طريق الجزاء الجنائي، ونجد أنه لا يوجد إلى الآن تعريف موحد للجريمة الدولية علي الصعيدين الفقهي والإتفاقي، فعلي الصعيد الفقهي هناك إختلاف بين الفقهاء علي تعريف الجريمة الدولية، وأما علي الصعيد الإتفاقي فإن المواثيق الدولية ذات الصلة من معاهدات وقرارات صادرة عن منظمات دولية لا تعرف الجرائم الدولية بل تكتفي بتعداد الجرائم التي تنطبق عليها القواعد القانونية الواردة فيها.

ومن أمثلة الجرائم الدولية، الجرائم ضد أمن وسلام البشرية، وجرائم الحرب، وجرائم ضد الإنسانية.

ولا يقصد بمبدأ العالمية أن لقانون العقوبات الوطني سلطاناً علي العالم بأسره، وإنما يعني ذلك المبدأ أن يطبق قانون العقوبات الوطني علي كل مجرم

يقبض عليه في إقليم الدولة، التي ارتكب فيها جريمته، ويعبر أحيانا عن هذا المبدأ بـ "عالمية" القاعدة الجنائية .

ثالثا : علاقة الجريمة العابرة للحدود بالإنترنت :

استنادا لما سبق نلاحظ أن المنظمات الإجرامية فطنت لإيجابيات الوسيلة التكنولوجية لتوظيفها في أغراض شريرة تعود عليها بالربح، لكن كيف يمكن للفضاء الرقمي أن يتحول إلى دعامة في خدمة كل ما هو مناف للقوانين، والأخلاق والأعمال غير المشروعة؟

لا يخفى على أحد أن الإنترنت سوق كبيرة للمعاملات بكل أنواعها، سواء كانت إنسانية، أو مالية، أو تجارية، وذلك بأقل النفقات، الأمر الذي شد انتباه المجرمين الذين وجدوا في هذا الفضاء ضالتهم لممارسة أنشطتهم الخبيثة، وتم تكريسها من خلال ما يعرف بالجرائم السيبرانية والتي هي موضوع دراستنا والتي لا يقتصر عملها على انتهاك النفس (نشر المواد الإباحية، بغاء الأطفال...) والأموال النصب والاحتيال، وسرقة المعلومات، والبيانات، وبطاقات الائتمان...)، بل تتعدى المنظمات الإجرامية التي اكتسحت الإنترنت الخطوط الحمراء بالاعتداء على حرمة الحياة الخاصة، تلك هي مساوئ هذه التكنولوجيا.

وفي بيئة الإنترنت، تتدفق المعلومات والاتصالات عبر الحدود دون أي اعتبار للجغرافيا والسيادة والأفراد يعطون معلوماتهم لجهات داخلية وخارجية، وربما جهات ليس لها مكان معروف، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوافر فيها مستويات الحماية القانونية للبيانات الشخصية، وقد لا تخدم القوانين الوطنية كثيرا في هذا الفرض ، كما أن تضمينها نصوصا بشأن السيطرة على نقل البيانات قد لا يكون فاعلا في ظل غياب التنسيق الدولي، وضمان أن يكون نقل البيانات محكوما باتفاقات تكفل حمايتها أو تضمن توافر حماية مماثلة في الدولة المنقول لها البيانات.

وتعدو المخاطر بخطي متسارعة مع نشوء ملاجئ آمنة لا تقيد عمليات المعالجة بأي قيد ولا تتوافر عندها قيود منعية على جمع ومعالجة البيانات، وهي ملاجئ تهرب إليها مؤسسات الأعمال في بيئة الإنترنت للإفلات من القيود القانونية، تماماً كما في حالات البحث عن ملاجئ لا تفرض فيها الضرائب، أو تتيح تبادل الأموال دون رقابة، وهذه تمثل تحدياً عالمياً وليس مجرد تحدٍ وطني، ولعلها الأساس الذي يدفع نحو إبرام اتفاقيات ثنائية وعالمية في حقل حماية البيانات الشخصية عبر الحدود، وهو نفس الأساس الذي أوجب إيجاد الأدوات العقدية التي تفرض على الجهة متلقيّة البيانات أو الوسيطة في تلقيها لإرسالها لطرف ثالث التزامات قانونية معينة تدور في مجموعها حول هدف حماية الخصوصية، ومنع إساءة استخدام بيانات الأفراد الخاصة، إلى جانب منع الأنشطة الاحتيالية والمساس بالمستهلك في بيئة الإنترنت.

وفي الواقع إن كافة الدول مرتبطة بينها بنظم معلومات تقنية عبر الأقمار الصناعية وشبكات الاتصال العالمية، الأمر الذي سهل على منظمات الإجرام استغلال هذه الوسيلة لأغراض مشبوهة غير مشروعة.

ومن الجدير بالذكر أن العصابات بالنظر لقوتها المالية، إضافة إلى استعمالها لوسائل القوة و التهديد وتوظف الأشخاص ذوي الكفاءة العلمية والتقنية العالية وذوي الاحترافية الكبرى والخبرة في مجال عالم المعلوماتية بغية اختراق نظم الإعلام الآلي والتسلل لمواقع الدول، والشركات الاقتصادية والمؤسسات الكبرى بهدف الاطلاع على أسرارها لابتزازها وسلب أموالها من ثم تخريبها.

وتظهر هذه المشكلة بصفة خاصة في مجال البنوك، حيث أدى التوسع الكبير في إجراء المعاملات الدولية إلى إعطاء بعد دولي لجرائم الاحتيال المعلوماتية بصفة خاصة. فربط وسائل الاتصالات بالحاسبات ضاعف المعاملات المالية الدولية التي تتم بوسائل إلكترونية وبصفة خاصة من خلال التحويل الإلكتروني للأموال

والتبادل الإلكتروني للمعلومات، ولا يقتصر الأمر على المعلومات المالية فقط ، بل إن الطبيعة الدولية للجريمة السيبرانية تظهر في أنماط أخرى من السلوك، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسوب الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصاً آخر موجود في بلد ثالث.

وكذلك فيما يتعلق بالإتلاف المعلوماتي، فإعداد أحد البرامج الخبيثة (الفيروسات) يمكن أن يحدث في دولة ما، من ثم يتم نسخ هذا البرنامج آلاف المرات ويرسل إلى دول متفرقة، و تزداد خطورة الوضع في الدول التي تتحكم فيها وتديرها الوسائل التكنولوجية إذ بمجرد الضغط علي زر حاسوب يمكن استهداف ما لا يخطر على بال أحد، بشن حرب دون سلاح و تنفيذ هجوم مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو شل محطات إمداد الطاقة والماء، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية ، فالحرب إذن قائمة بطرق مستحدثة دون عناء أو تكاليف وكذلك تزداد الخطورة عندما يتم التدخل في حرمة الحياة الخاصة التي كفلتها كل الأديان السماوية.

وتطرح الجريمة العابرة للحدود التي تستعمل الوسائل التكنولوجية الجديدة تحديات تكمن في صعوبة تصنيف الأنشطة الإجرامية ضمن الجرائم التقليدية المنصوص عليها في التشريعات الجنائية الوطنية، و كذلك في ضعف وسائل الملاحقة القضائية الوطنية التي تعترضها مسائل التسليم والمحاكمة.

رابعاً: أسباب جعل الجريمة السيبرانية جريمة عالمية:

والجدير بالذكر أن الذي ساهم في جعل الجريمة السيبرانية عابرة للحدود وبالتالي هي جريمة عالمية كما سبق أن بينا الآتي:

١ . انفتاح شبكة المعلوماتية:

ذكرنا سابقا أن عالم المعلوماتية ، فضاء مفتوح على مصراعيه لا يخضع للرقابة أو الملكية، الأمر الذي سهل عمليات التسلل إليه و اختراقه. وبالرغم من حقيقة أن الصراع يحتدم على السيطرة على الإنترنت ، من خلال السعي للسيطرة على أسماء البطاقات وعناوين المواقع ، والتنافس للسيطرة على سوق استضافة المواقع عبر الخوادم التقنية والتوجه أحيانا للتحكم بالمعلومات وطرق تبادلها عبر التحكم بالحلول التقنية واحتكارها لتكون وسيلة التحكم بمصائر المستخدمين وأداة السيطرة الفعلية، بالرغم من يرافقه من نشاط مضاد لجهة منع الاحتكار المعلوماتي.

كل ذلك، ومع وتباين المصالح بين أمريكا وأوروبا وشرق آسيا في هذا الشأن، فإن الإنترنت يتصف باللامركزية وغياب السلطة التحكيمية، وليس دعوات إنشاء حكومة الإنترنت أو بوليس الإنترنت أو معايير الاستخدام الموحد، أو سياسات التنظيم الذاتي للالتزامات إلا وسائل افتراضية شأنها شأن البيئة التي نشأت فيها ، ومن هنا يكون لبعض مسائل التعاون الدولي أهمية بالغة، أبرزها الاتفاق في حقل الاختصاص القضائي والقانون الواجب التطبيق في بيئة منازعات الإنترنت.

ومع وجود توجهات للتعاون والتنظيم الدولي، وجهود مميزة لدى منظمة التعاون الاقتصادي والتنمية والاتحاد الأوروبي، وجهات تقنية، وهيئات وقطاعات عاملة في بيئة الانترنت كما سوف نري، فإن كافة هذه الجهود حتى الآن لم تقدم حولا لحل مشكلات عدم وجود تنظيم مقبول يحكم الإنترنت في كل مسائله، ولعل طبيعة الإنترنت واتجاهات تطور طريق المعلومات السريع يعطي انطباعا أن

الإنترنت سيبقى خارج أمنيات الحكومات في إيجاد تنظيم قانوني يحكمه أو يسيطر على شئونه.

٢. انعدام الحواجز الجغرافية:

إن التداول والنقل الدولي للمعلومات، بل وأيضا للبيانات يلغي فكرة الزمان والمكان، ولهذا السبب فإنه من الخطورة بمكان، أن تنأى هذه المعلومات عن أي تنظيم ، فأهم ما يميز الإنترنت عالميته وكونه يربط بين دول لا تحدها حدود الطبيعة أو حدود السياسة، وتسمح لمستخدميها بالتنقل المعنوي أو الافتراضي بين الدول والقارات بدون تعقيدات أو صعوبات أو عوائق فهو عالم ضخم متنوع متجدد خال من الحدود والعوائق.

ونجد أن المعلومات تنتقل عبر الإنترنت من دولة لدولة ومن منظمة لمنظمة، ومن جهة عمل إلى أخرى، ومن فرد إلى مؤسسة، دون قيود وبكل اللغات، وتسافر المعلومة عبر الشبكات المحلية ثم الدولية، وتوجه من نقطة لأخرى في الفضاء، وفي رحلتها هذه تحط وتزور العديد من مناطق الاختصاص القضائي ومناطق السيادة، ومناطق قد لا تكون بينها تعاون أو حتى روابط ، ففي مثل هذه البيئة ثمة حاجة لجهد استثنائي على النطاق الدولي أهم ما يتعين أن يتصف به الخروج من الأطر والمفاهيم التقليدية للسيطرة ، فلم تعد إرادة القوي هي حجر الزاوية، فربما يكون لفرد ما القدرة في أن يتحدى أعظم القوى في هذه البيئة، ولهذا فإن ما نسميه ديمقراطية الإنترنت وعدالة التعامل مع المعرفة، وعدم التمييز وانتهاء عهد الاحتكار والسيطرة، هي الأسس التي يتعين يتم التفكير فيها في كل نشاط يهدف إلى تنظيم ضروري لمسائل الإنترنت.

فإن العديد من المنظمات الدولية والحكومية تعمل جاهدة من أجل إقامة تنظيم علي المستوى الدولي خاص بمسألة تدفق البيانات و المعلومات عبر

الحدود، والأهم أن يكون تنظيماً يراعي هذه السمات التقنية وهذه الخصائص وميزات التفاعلية اللامتناهية.

٣. صعوبة الكشف عن هوية المستخدم :

إن الحق في التخلي يعد من الحقوق الإلكترونية الكاملة دون منازع، لكنه يمارس عبر الإنترنت بسهولة ويسر. ومثل هذا الحق اعترف به التوجه الأوروبي، وبحيث يمكن لعضو الإنترنت أن يكون متخفياً عبر الإنترنت، كما يمكن له أن يكون كذلك في العالم المادي.

وبناء على ما سبق يمكن لأي شخص انتحال شخصية، أو التخلي وراء إنسان وهمي، والمذهل أنه تتم هذه العملية بأمان وهدوء بعيداً عن أعين المراقبة الأمنية؛ لأن في الحقيقة المجرم يتوارى وراء شاشته مستعملاً السلاح الرقمي و هو في مقهى، أو حديقة، أو أي مكان عام أو خاص، من أي قارة، لإلحاق الضرر بالغير دون أدنى تأثير عليه، مستفيداً مما تقدمه له التكنولوجيا من منافع.

والعكس صحيح أيضاً عندما يستخدم الأفراد مواقع الإنترنت، فإنهم قد يتوقعون قدرًا من الخفية في نشاطهم أكثر مما يتوقعون في العالم المادي الواقعي، ففي الأخير يمكن ملاحظة وجودهم ومراقبتهم من قبل الآخرين، وما لم يكشف الشخص عن بيانات تخصه، فإنه يعتقد أن أحداً لن يعرف من هو أو ماذا يفعل، لكن الإنترنت عبر نظم الخوادم ونظم إدارة الشبكات تصنع قدراً كبيراً من المعلومات عند كل وقفة في فضاء الشبكة. وهذه البيانات قد يتم اصطياها ومعرفتها عن طريق موظفي منشأة ما - مثلاً - من قبل صاحب العمل عند استخدامه للشبكة أو لاشتراكاتهم المربوطة عليها، وقد تجمع من قبل المواقع التي تمت زيارتها وكما قلنا فإن جمع شتات معلومات وسلوكيات معينة قد يقدم أوضح صورة عن شخص لم يرد كشف أي من تفاصيل ما تضمنته.

٤. بساطة التعامل مع الإنترنت وزهد ثمنه:

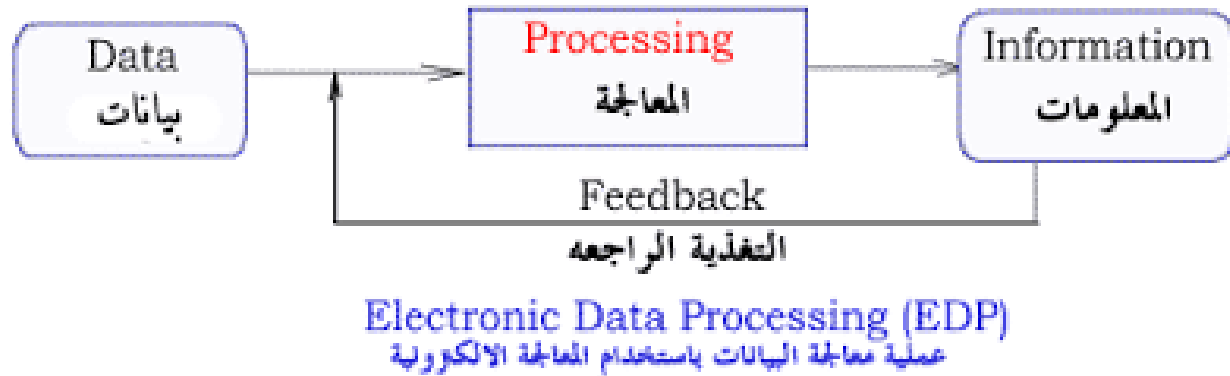
وخلاصة القول فإن هذه العناصر من جملة الأسباب التي تساعد الجماعات الإجرامية على المضي قدما في أنشطتها دون خوف و بكل آمان و تعتمد في ذلك على شن هجوم على المواقع الشخصية والعامة، الرسمية وغير الحكومية باختراقها والتسلل إليها للسيطرة عليها وتدمير أو سرقة بياناتها وحقن جرعات من الفيروسات مما يسبب لأصحابها أضرارا جسيمة مادية ومعنوية.

المحور الثاني

مراحل ارتكاب الجرائم السيبرانية

من خصائص الجريمة السيبرانية أنها تقع أثناء عملية المعالجة الآلية للبيانات أو المعطيات الخاصة بالكمبيوتر ، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة السيبرانية الخاصة بالتعدي علي نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة السيبرانية.

وعلي الرغم من إمكانية ارتكابها أثناء أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات (الإدخال - المعالجة - الإخراج) فإن لكل مرحلة منها نوعية خاصة من البرامج ، لا يمكن بالنظر إلي طبيعتها ارتكاب الجريمة السيبرانية إلا في وقت محدد يعتبر هو الأمثل بالنسبة لمراحل التشغيل.



أولاً: مرحلة الإدخال :

في مرحلة الإدخال حيث تترجم البيانات إلى لغة مفهومة من قبل الآلة، يكون من السهل إدخال معلومات غير صحيحة .

فقبل أن يصبح الأمن معيار التصميم ذا الأهمية كان الهدف غالباً هو تزويد قدرة الحوسبة لأكبر عدد من مجتمع المستخدمين. وحين تم تقييد اهتمامات الدخول علي منطقة غرفة الحاسوب فإنه كان يجب توسيع محطات عن بعد ودوائر تراسل، مما ترتب عليه أن يكون هناك شكلان من العدوان يؤديان إلي الدخول عن بعد وهما: استعمال تعريف كاذب وشفرات الدخول للحصول علي إمكانية استخدام النظامو الثاني هو الاستعمال غير المصرح به للمحطة بالدخول إليها من قبل شخص غير مصرح له، وهذه المرحلة هي التي يتم فيها الجانب الأكبر من الجرائم السيبرانية.

ثانيا : مرحلة المعالجة:

في مرحلة المعالجة يمكن إدخال أي تعديلات علي البرنامج تحقق الهدف الإجرامي، عن طريق التلاعب في برنامج النظام المعلوماتي، فيتم دس معلومات غير مصرح بها، أو يتم تشغيل برامج جديدة تلغي جزئيا أو كليا عمل البرامج الأصلية.

والجرائم المرتكبة في هذه المرحلة تتطلب توافر معرفة فنية عميقة لدي الفاعل بتلك التقنية كما وأن اكتشافها يكون صعبا للغاية وغالبا ما تقف الصدفه وراء اكتشافه .

فالأقراص المحفورة والذاكرة المجنبة يمكن كلها أن تحتوي علي بيانات متبقية، ويمكن أن تحتاج إلي مزيد من العناية. ولما كان هناك فقدان في الهيئة والمصادقية فإنه لن يكون هناك ضمانات لهذه البنود حتى ولو كانت هناك حماية لتلك المعلومات في مكان آخر من النظام. فالتساهل مع مثل هذه المصادر للمعلومات التي من السهل استعمالها قد ينتج عنه العديد من الانتهاكات.

ثالثا: مرحلة الإخراج:

وهي المرحلة الأخيرة المتعلقة بالمخرجات وفيها يقع التلاعب في النتائج التي يخرجها النظام المعلوماتي بشأن بيانات غير صحيحة أدخلت فيها معالجة بطريقة صحيحة.

ونلاحظ في هذه المراحل أن المستخدمين يشكلون أكبر تهديد في مجال الجرائم السيبرانية. ذلك أنه أمر عادي أن يجد المشتغلون، و فنيو القطع الصلبة والأعضاء الآخرون أنفسهم في وضعية ممتازة ذات علاقة بأسس النظام و أصول المؤسسة

التي يعملون بها. ويزداد الأمر سوءاً في حالة التساهل من جانب الإدارة بتقرير مراقبة أقل صرامة علي المعالجة الآلية للبيانات.

المراجع

• الكتب:

١. د. أحمد خليفة الملط ، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي / الأسكندرية، سنة ٢٠٠٥.
٢. د. خالد ممدوح إبراهيم، (أمن الجريمة الإلكترونية) - الناشر الدار الجامعية - الطبعة الأولى - ٢٠١٠ م.
٣. د. محمد سامي الشوا : [ثورة المعلومات وانعكاسها علي قانون العقوبات] - دار النهضة العربية - الطبعة الأولى - سنة ١٩٩٤ م.

• الرسائل:

٤. د. أسماء رويحي : [الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية]، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة ، سنة ٢٠١٣ م.
٥. د. عمر محمد أبو بكر بن يونس، (الجرائم الناشئة عن إستخدام الإنترنت - الأحكام الموضوعية والجوانب الإجرائية) - رسالة دكتوراة - كلية الحقوق - جامعة عين شمس - ٢٠٠٤ م.
٦. د. نائلة عادل محمد فريد قورة : [جرائم الحاسب الإقتصادية] - رسالة دكتوراة - جامعة القاهرة - ٢٠٠٣ م.

• الدوريات والمؤتمرات:

٧. أخام بن عودة زواوي مليكة: (تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية) - ورقة عمل مقدمة للمؤتمر المغربي الأول حول المعلوماتية والقانون - تاريخ الإنعقاد : من ٢٧ إلي ٣٠ أكتوبر ٢٠٠٩ م.
٨. د. ذياب البداينة: { أمن المعلومات } - مجلة دراسات مستقبلية - السنة السادسة - العدد الثامن يوليو ٢٠٠٣ م.
- [الجرائم الإلكترونية : المفهوم والأسباب] - ورقة علمية مقدمة في الملتقى العلمي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحويلات الإقليمية و الدولية خلال الفترة من ٢ - ٩ / ٢٠١٤ م - عمان - الأردن.
٩. عمر الفاروق الحسيني، البعد الدولي للجرائم المتصلة بالحاسب الآلي وآلية مواجهته في التشريع المصري والتشريع الكويتي - مجلة المحامي - السنة السابعة عشر - أعداد أكتوبر

ونوفمبر و ديسمبر ١٩٩٣م، وهو بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد بالقاهرة في الفترة من ٢٥ - ٢٨ أكتوبر ١٩٩٣م.

١٠. د. يونس عرب، (دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي)، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات، نادي المعلومات العربي، في الفترة من ١٦ - ١٧ أكتوبر ٢٠٠٢م - عمان - الأردن.

• موقع إلكتروني:

١١. د. عادل عمر، جرائم الإنترنت، بحث منشور علي موقع :

www.Adelamer.com

• مرجع مترجم:

١٢. ملخص الترجمة العربية لمرشد الأمم المتحدة لعام ١٩٩٩م، (التحكم في جرائم الحاسوب وردعها - المراقبة الدولية للسياسة الجنائية) ، ترجمة وعرض د. عمر محمد بن يونس - دار النهضة العربية - الطبعة الأولى - سنة ٢٠٠٥م.

تم بحمد الله

الإنهاء من شرح المحاضرة الخامسة

مع تمنياتي بالتوفيق د. أسماء رويحي