

الموضوع الرابع

المجرم المعلوماتي

السؤال الذي يطرح هنا هو: من هو المجرم المعلوماتي؟ ما هي خصائصه ومميزاته؟
وما هي دوافعه؟

أولاً: تعريف المجرم المعلوماتي

المجرم المعلوماتي هو كل مجرم ارتكب الجريمة المعلوماتية، هذا المفهوم البسيط يقتضي منا تعريف المجرم ثم تعريف الجريمة المعلوماتية، باعتبار المصطلح مركبا إضافيا.

-**تعريف المجرم:** يعرف المجرم بالمفهوم القانوني كل من أتى سلوكا منصوصا عليه في قانون العقوبات وحكم عليه بالعقوبة المقررة بحكم بات، بما يعني ثبوت نسبة السلوك الإجرامي إليه.

-تعريف الجريمة المعلوماتية:

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة المتصلة بتكنولوجيات الإعلام والاتصال، فهناك من يطلق على تسميتها الجرائم الإلكترونية وهناك من يطلق عليها تسمية الجرائم المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، جرائم الكمبيوتر والأنترنت، الجرائم المستحدثة، الجريمة الناعمة، جرائم التقنية العالية، إجرام ذوي الياقات البيضاء، في حين ذهب المشرع الجزائري إلى تسميتها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

وتجدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الأنترنت، فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات المخزنة به، فإن جرائم الأنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة

الحاسب الآلي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والاتصالات) وظهر مصطلح cybercrim.

وقد انقسم الفقهاء إلى اتجاهين، منهم من ينظر إلى الجريمة الإلكترونية بمفهوم ضيق، ومنهم من ينظر إليها بمفهوم واسع.

01-تعريفها من الجانب التقني الفني

تعرف الجريمة الالكترونية بأنها "عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة او غير مباشرة كوسيلة أو هدف لتنفيذ العمل الإجرامي"، كما يعرفها البعض الآخر بأنها "تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها".

لقد انقسم أنصار تعريف الجريمة من الجانب الفني والتقني إلى اتجاهين؛ اتجاه استند إلى موضوع الجريمة والبعض الآخر إلى وسيلة الجريمة.

*أهم التعريفات التي استندت إلى موضوع الجريمة

منها "أنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو المحولة عن طريقه"، "كل سلوك غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات".

*أهم التعريفات التي استندت إلى وسيلة الجريمة

أنصار هذا الاتجاه ينطلقون في تعريفاتهم من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة، منها "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"، "كل فعل أو امتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".

وربما يعتبر هذا التعريف الأخير هو الراجح لتبنيه من قبل الكثير من الباحثين والدارسين نظرا لشموله، بحيث يعبر عن الطابع التقني أو المميز الذي تتطوي تحته أبرز صور الجريمة الالكترونية.

02-تعريفها من الجانب القانوني

تعرف على أنها "مجموعة الأفعال والأنشطة المعاقب عليها قانونا، والتي تربط بين الفعل الإجرامي والثورة التكنولوجية"، كما تعرف على أنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"، وحسب هذا التعريف فإنها من جرائم الأموال.

"عمل أو امتناع يأتيه الفاعل إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا". "كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على تقنية المعلوماتية أيا كان غرض الجاني".

*تعريفها في القانون الجزائري

أما بالنسبة لتعريفها في القانون الجزائري، فقد عرفها بموجب أحكام المادة 02 من القانون رقم 04-09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية".

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394

مكرر 7، وترك المجال واسعا لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عددا كبيرا من الجرائم. ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر، تسريب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري "حمزة بن دلاج" بقرصنة حسابات بنكية عالمية الذي ألقى عليه القبض من طرف الشرطة الفيدرالية الأمريكية.

مما سبق يمكن القول أن المجرم المعلوماتي هو كل من أتى سلوكا أو امتنع عن واجب إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات أو القوانين الخاصة ويفرض له عقابا، وحكم عليه بالعقوبة المقررة بحكم بات.

كما يعرف المجرم المعلوماتي بأنه المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليا أو دوليا.

ثانيا: خصائص الجريمة المعلوماتية

01- جريمة عالمية: بمعنى أنها تتعدى الحدود الجغرافية للدول، جرائم عابرة للقارات، لأنه مع انتشار شبكة الاتصالات العالمية والانترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يكون الجاني في بلد والمجني عليه في بلد آخر.

02- جرائم صعبة الإثبات: صعوبة متابعتها واكتشافها، لأنها لا تترك أثرا ماديا، فهي مجرد أرقام تتغير في السجلات فمعظم الجرائم الإلكترونية تم اكتشافها بالصدفة وبعد وقت طويل،

ويلاحظ أن الجرائم التي لم تكشف أكثر بكثير من الجرائم التي كشف عنها على أساس أنها تقتصر إلى الدليل المادي التقليدي كالبصمات، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها، لأنها تعتمد على قمة الذكاء والمصحوب بالخداع، والتضليل بدس برامج أو وضع كلمات سرية ورموز تعيق الوصول إلى الدليل وقد يلجأ مرتكبيها لتفسير التعليمات لمنع إيجاد أي دليل يدينه.

تستلزم طرقا خاصة مستحدثة للإثبات، قوامها التعليم و التدريب المتخصص المستمر لعلوم الحاسب الآلي، لذا فإنها تقتضي وجود رجل شرطة إلكتروني، ومحقق إلكتروني، وقاضي إلكتروني، فضلا عن الخبير الإلكتروني حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، وعليه فإن الاستعانة بالخبراء تصبح حتمية لكشف وتحليل وتفسير الدليل الجنائي، الذي يثبت البراءة أو الإدانة.

03-جرائم ناعمة: فهي لا تحتاج إلى مجهود عضلي بل تعتمد على المجهود الذهني والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة على أساس أن الجاني الإلكتروني متوافق مع المجتمع ولكنه يرتكب هذا النوع من الجرائم إما بدافع اللهو أو إظهار تفوقه على الكمبيوتر أو على البرامج التي يشتغلها، وقد تكون هناك مصلحة ما في ذلك.

04-عدم التبليغ عنها: تدني نسبة الإبلاغ عن الجريمة من طرف المجني عليه خاصة في حالة شركات ومؤسسات، لتجنب الإساءة للسمعة و الرغبة في عدم زعزعة ثقة العملاء، ففي إحدى الوقائع تعرض أحد البنوك، وهو بنك "marchant bank city" " في بريطانيا لسرقة ثمانية مليون جنية إسترليني من إحدى أرصده إلى رقم في سويسرا، وتم ضبط الفاعل متلبسا يسحب المبلغ المسروق وبدلا من محاكمته، قام البنك بدفع مليون جنية له، بشرط التزام الفاعل

بعدم الإعلام عن جريمته، وإعلام البنك عن الألية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي.

- غالبا ما تكون الخسائر الناجمة عنها فادحة للمجني عليه

ثالثا: مميزات المجرم المعلوماتي

- يتميز المجرم الإلكتروني بالمعرفة والمهارة والذكاء حيث أن نسبة 94 بالمائة من العينة المدروسة يتصفون بالذكاء والمهارة في التعامل مع تقنية المعلوماتية، لذلك فهو يتميز بالقدرة على اختراق النظم المعلوماتية (حواسيب أو شبكة الاتصال) والتلاعب بأنظمتها الأمنية، يبتكر أساليب جديدة ومتطورة لارتكاب أفعاله، لديه قدرة فائقة على المعالجة الإلكترونية للنصوص والكلمات والتعامل مع البرامج، فهو يتصور جريمته قبل ارتكابها، وتظهر عبقريته أكثر في الجرائم المالية التي تحقق أرباحا مادية، وتلحق خسارة بالمجني عليه.

- المجرم الإلكتروني يبرر ارتكاب جريمته، إذ يوجد شعور لدى كل مرتكب فعل إجرامي أن ما يقوم به لا يدخل في قائمة الجرائم، خاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.

- المجرم الإلكتروني يتصف بالخوف من كشف جريمته، فهو شخصية حذرة جدا، وبالرغم من أن هذه الخشية تصاحب المجرم على اختلاف أنماطه، إلا أنها تميز المجرم الإلكتروني بصفة خاصة، لما يترتب على كشف أمره من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان، كما أن طبيعة الأنظمة المعلوماتية نفسها تساعد الجاني على الحفاظ على سرية أفعاله.

-المجرم الإلكتروني يميل إلى التقليد، ويظهر ذلك من خلال محاولة الفرد تقليد غيره بالمهارات الفنية، مما يؤدي به الأمر إلى ارتكاب الجريمة.

-القيام بالتخطيط والتنظيم، ففي عالم الشبكات الإلكترونية، كما هو الحال في العالم الحقيقي، يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة حيث ترتكب أغلب الجرائم من مجموعة متكونة من عدة أشخاص يحدد لكل شخص دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة.

-التكيف الاجتماعي، فالمجرم الإلكتروني يقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية دون أي عائق في حياته اليومية.

-التطور في السلوك الإجرامي، حيث يساهم وجود المجرم الإلكتروني في جماعة إجرامية إلى سرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة، إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة.

رابعا: تصنيف المجرم المعلوماتي: يصنف الجرم المعلوماتي إلى عدة أصناف، مع أن هذا التصنيف يتغير بتطور الجريمة في كل مرة.

01-الهاكرز: ويطلق هذا الاسم على القراصنة الذين يتخذون من الجريمة الإلكترونية هوية والقرصنة هوية أو فضولي ليس أكثر وغرضها تخريبيا ليس هادفا لغايات، وتكون غالبا من الفئة الشبابية التي تهوى التعمق بالمعلومات الإلكترونية والحاسوب.

02-الكرakers: وهم القراصنة المحترفون ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية أو متخصصين في العلوم الإلكترونية

03-الطائفة الحاقدة: وتستهدف هذه الفئة المنظمات والمنشآت وأرباب العمل ويكون الهدف من ارتكابها للجريمة بحق هذه الأطراف عادة الحقد والحصول على المنفعة المادية والسياسية. وقد يكون تطرف أو جاسوس أو مخترق الأنظمة.

خامسا: دوافع ارتكاب الجريمة المعلوماتية

قد تكون دوافع مادية سعيًا لإشباع الرغبة في الثراء، أو دوافع شخصية، التعلم، الانتقام، التسلية السياسية.