المحاضرة الثانية: المجرم الالكتروني والمجني عليه في الجريمة الالكترونية

ثانيا – خصائص وصفات المجرم الالكتروني: ليس هناك اتفاق على صفات مرتكبي الجرائم الالكترونية ومنفذيها، ولا يوجد قالب يتضمن الفئات والسمات التي يتسم لها مرتكب الجريمة المعلوماتية ، إلا أن هناك صفات ذات دلالة مشتركة يجمع المختصون بأنها توجد في كل الأشخاص الذين تم التحقق والقبض عليهم في جرائم من هذا النوع، حيث أوردت العديد من الدراسات العربية والأجنبية في هذا المجال بأن متوسط عمر مرتكبي هذه الجرائم بين 14– 34 سنة وهذا يدل بأن أغلب مرتكبي الجرائم الالكترونية من فئة الشباب ، ويتميز المجرم المعلوماتي بعدد من السمات والخصائص هي:

– المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء، حيث يمكنه التغلب على الكثير من العقبات التي تواجهه أثناء ارتكاب الجريمة.

– المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي، حيث أن المزايا التي يتمتع بها المجرم المعلوماتي تمكنه من ارتكاب جريمته، وقد تتمثل هذه السلطة مثلا في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي المجرم إمكانية فتح الملفات وقراءتها وكتابتها ومحو المعلومات.

– المجرم المعلوماتي شخص ذو مهارة فنية عالية متخصص في الاجرام المعلوماتي (الالكتروني)، قادر على استخدام خبراته في الاختراقات وتغيير المعلومات.

– المجرم المعلوماتي قادر على تقليد البرامج وتحويل الأموال، محترف في التعامل مع شبكات الحاسبات، وهو شخص غير عنيف لأن تلك الجريمة لا تلجأ إلى العنف لارتكابها. (قابوسة، 2019، صفحة 247)

– المجرم الالكتروني يميل الى تقليد غيره في المهارات والاحترافية.

– القيام بالتخطيط والتنظيم في عالم الشبكات الالكترونية.

– التطور في السلوك الاجرامي.

3–أنواع المجرمين الالكترونيين : توصلت الدراسات والأبحاث التي تناولت مجرمي المعلوماتية إلى تصنيف المجرمين الالكترونيين إلى أنماط ، لكن لابد من الإشارة إلى أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة

محددة دون غيرها من الفئات المذكورة ، بل يمكن ان يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة: نجد اشهرهم ما يلي :

أولا: فئة صغار مجرمي المعلوماتية: يسميهما البعض صغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها حيث يجب عدم التقليل من خطورة هؤلاء الأشخاص ، فهذه الفئة قد تتعدي مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في ارتكاب الجرائم المعلوماتية، وهي مرحلة الاحتراف لهذه الجرائم، كما أنه هناك مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للاستفادة من مهاراتهم وتطويرها، حيث أن هذه الفئة أكثر تقبلا لأي أفكار تعرض أو تفرض عليها خاصة إذا كانت تحمل المغامرة والاثارة والتحدي في طياتها.

ومن الأمثلة الشهيرة لجرائم الحاسوب التي ارتكبت من هذه الفئة العصابة الشهير التي أطلق عليها عصابة 414 والتي نسب إليها ارتكاب 60 فعلا تعدي في الولايات المتحدة الامريكية علي ذاكرات الحواسيب حيث نجم عنها أضرار كبيرة لحقت بالمنظمات العامة والخاصة.

ثانيا : المخترقون والمتطفلون(فئة القراصنة) :

وهم عادة من أصحاب الخبرة يدخلون إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها، وكسر الحواجز الأمنية المحيطة بهذه الأنظمة ، يتحدد في هذا الاطار نوعين من المجرمين هما :

أ-القراصنة الهواة العابثون أو الهاكرز :وهم المتطفلون والمتسللون يتحدون إجراءات أمن الشبكات لكن لا تتوفر لديهم في الغالب دوافع التحدي واثبات الذات ،وهذه الفئة أغلبها من التلاميذ وطلبة الثانويات والشباب العاطل عن العمل. (قابوسة، 2019، صفحة 248)

والهاكرز هو الشخص الذي يقوم بإنشاء او تعديل البرمجيات والعتاد الحاسوبي، حيث يقوم الهاكرز بتثبيت ملف يعرف

Patch- trojan على الحاسوب المراد اختراقه.

ويقصد به الشباب البالغ المقترن بالمعلوماتية والحاسب الالية وقد يطلق على صغار نوابغ المعلوماتية. واغلبهم طلبة لهم معرفة في المجال. ويكون الباعث عادة للهاكرز هو الاستمتاع باللعب والمزاح لإثبات قدراتهم.

ب-القراصنة المحترفون أو ما يعرف بـ الكراكرز: وهو المقتحم، وهو الشخص الذي يقوم بالتسلل إلى نظام الحاسوب للاطلاع على المعلومات المخزنة فيه أو الالحاق الضرر أو العبث بها أو سرقتها. ويتراوح اجمالي الخسائر الناجمة عن القرصنة الالكترونية بين 375 و575 مليار دولار سنويا. (قابوسة، 2019، صفحة 248)

ثالثا: فئة الموظفون العاملون في مجال الأنظمة المعلوماتية: وهذه الفئة من المجرمين يشكل النظام المعلوماتي مجال عملهم الأساسي، ولهذا فهم يقترفون جرائم تمكنهم من تحقيق أهدافهم الشخصية، هؤلاء يعودون إلى مقر عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو سرقته، وقد يجد الموظف نفسه أحيانا مرتكب لجريمة الكترونية صدفة ودون تخطيط مسبق لها.

رابعا : الحاقدون: هذه الفئة يغلب عليها عدم توفر أهداف وأغراض الجريمة المتوفرة لدى الفئات الأخرى، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية ، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم، أو لتصرف المنظمة المعنية معهم عندما لا يكونوا موظفين فيها. ولهذا فإنهم ينقسمون إما إلى مستخدمين للنظام بوصفهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء تتوفر لديهم أسباب الانتقام من المنظمة المستهدفة في نشاطهم.

خامسا: فئة مجرمو المعلومات أصحاب الآراء المتطرفة: وتتكون هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات أو أفكار اجتماعية أو سياسية أو دينية، ويرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الاجرامي.

سادسا: فئة مجرمو المعلوماتية في إطار الجريمة المنظمة: الجريمة المنظمة هي تعبر عن مجتمع إجرامي يعمل خارج الشعب والحكومة، ويضم في طياته الآلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المنظمات تطورا وتقدما ، كما يخضع أفرادها إلى إحكام قانونية سنوها بأنفسهم، وتفرض عليهم أحكاما بالغة القسوة على من يخرج عن الجماعة ، ويلتزمون في أداء أنشطتهم الاجرامية التخطيط الدقيق والمدروس، حيث يجنون من وراءه الأموال الطائلة، ومن أمثلة هذه الجرائم ، عصابات سرقة السيارات الذين يحددون بواسطة شبكة الانترنت الأماكن التي ترتفع بها أسعار قطع غيار السيارات ومن ثم يبيعون القطع المسروقة في تلك الأماكن ليضمونا أكبر ربح ممكن. (قابوسة، 2019، صفحة 248)

4-المجرم والمجني عليه في الجريمة الالكترونية:

أصبح الحاسب الآلي على مدى العشرين عاما الماضية ركيزة أساسية بسبب التطور في كل مجالات الحياة والمتضمن كافة الأنشطة المختلفة سواء اقتصادية أو عملية أو اجتماعية أو صناعية أو زراعية.

والسبب الرئيسي لظهور ما يعرف بالإجرام المعلوماتي هو الاستخدام المطرد للمعلوماتية سواء كان في شكل أموال معلوماتية أو أساليب مستحدثة وهذه هي الخلاصة والنتيجة القطيعة لأي تقدم علمي وتقني مستحدث.

فالحاسب الآلي وما قام به من خدمات عائلة من اجل زيادة الاستثمار كأداة للإدارة فانه أيضا قد استخدم في الضرر والشر من اجل إخفاء الغش ويمكن أن يكون محلا للمعارضة الايديلوجية.

وبسبب ما تم ذكره فيما سبق اصبحت القوانين العقابية التقليدية تقف اليوم مكتوفة الايدي بل عاجزة عن احتواء هذه الظاهرة الاجرامية المستحدثة والتي ظهرت حديثا.

وقد ذكر الأستاذ هايت ان الجرائم التقليدية المعمول بها والتي تم صياغتها بعد تأمل في الثروات المادية أو في المستندات المعرضة للتلف المادي تضمن صعوبة حماية هذه القيم المعنوية الناشئة عن المعلوماتية. (عياد، 2006، صفحة 46، 47)

وسوف نتناول المجرم المعلوماتي والمجني عليه في الجريمة المعلوماتية:

أولا- المجرم المعلوماتي: عملية المعالجة الآلية للمعلومات محفوفة بالمخاطر فقد المعلومات والافشاء غير المسموح والاعتداء على سلامة النظام المعلومات لأن هذه العملية محصلة تعاون وعمل مجموعة مدعما في كل لحظة أفكار مستحدثة وابداع.

فالمعلوماتية دائما لها دور يذكر وان مصدر التدعي عليها وضعفها هو الانسان ذاته فجوهر يرتبط إذا بالإنسان وشخصيته ودوافعه، وهذا ما اشارت اليه شركة للحاسبات الآلية عن طريق الإعلانات في الجرائد الامريكية ذات الشهرة الواسعة من ان الحاسبات الآلية ليس بإمكانها ان ترتكب بذاتها الجرائم ولكن يمكن ان تستخدم كوسيلة في ارتكابها.

GBM (عياد، 2006، صفحة 47)

**** السمات المميزة لشخصية المجرم المعلوماتي: الملاحظ ان أي عقوبة جنائية يتم توقيعها على المجرم لا يمكن ان تحقق أهدافها سواء في مجال الردع العام أو الخاص ما لم نضع نصب اعيننا ونأخذ في الاعتبار الشخصية المميزة للمجرم والذي يتطلب من المختصين إعادة تأهيله اجتماعيا. حتى يعود انسانا صالحا يتلائم مع ظروف المجتمع.

أ- المجرم المعلوماتي كانسان ذكي: الاجرام التقليدي يتسم بالعنف وهو الوسيلة الوحيدة الاقتراف جريمته بعكس الاجرام المعلوماتي فهو اجرام الاذكياء.

ولكن قد يتصور الاجرام العنيف الموجه ضد النظام المعلوماتي ويتجسم هذا في اتلاف الحاسب الآلي أو الدعائم الممغنطة ويحدث هذا في اطار الأفعال الإرهابية ولكن يجب الا يتصور أو يستنتج ان الاتلاف المعلوماتي دائمة بحاجة إلى سلوك عنيف فهو من الممكن ان ينشأ من تقنيات التدمير الناعمة، مثل التلاعب بالمعلومات أو الكيانات المنطقية أو البيانات ويحدث هذا في عدة طرق أولهما ما يعرف بالتلاعب عن طريق "" القنابل المنطقية "" وتتم عن طريق زرع تعليمات في برنامج مزود بعداد وعندما يصل إلى بادية كعينة تنطلق هذه التعليمات لكي تمحو البرامج أو البطاقات ،والذين يستخدمون هذه الوسيلة دائما هم غالبا من قبل العاملين في المنشآت المعلوماتية لحماية انفسهم ضد خطر الفصل.

وثانيهما ما يعرف "" الفيروسات "" المعلوماتية وهي عبارة عن برنامج من الحجم الصغير يصعب اكتشافه ويتم وضعه في أسطوانة ثم يقوم بنسخ نفسه في نظام تشغيل الحاسبات الآلية، وبعد ذلك ينشر في كل الدعائم الممغنطة والمستخدمة في هذه الأجهزة، وخلال فترة زمنية وجيزة يستطيع الفيروس ان يحطم جميع البطاقات ودائما نجد ان شخصية المجرم المعلوماتي تتسم بالنشاط والمخاطرة والذهن المتقد الذي يسعى إلى خداع الآلة. (عياد، 2006، صفحة 49، 50)

ب- المجرم المعلوماتي كانسان اجتماعي:

باستثناء سرقة تقنيات المعلوماتية واستخدامها من قبل اللصوص نجد ان هناك عوامل متحدثة يلجأ اليها العديد منهم الى ارتكاب هذه الجرائم بدافع اللهو أو لمجرد اظهار تفوقهم على الآلة أو على البرامج المخصصة لأمن النظم المعلوماتية، وقد لا يحصلوا على اية منافع مالية من جرائمهم ويكن ذلك بدافع الالتحاق بالفريق المعلوماتي المكلف بضمان امن النظام المعلوماتي في المنشأة.

ولكن لا يجب ان نستخلص من ذلك انعدام أي خطر اجتماعي للإجرام المعلوماتي، وليس السبب في ذلك عدم وجود نوايا ولكن أيضا للسلوك غير الواعي الذي يمكن ان يتسبب في اضرار جسيمة ولو لم يكشف عن أي عداء للمجتمع. (عياد، 2006، صفحة 50، 51)

ج-الأنماط المختلفة للمجرم المعلوماتي: الجريمة المعلوماتية لا تستلزم جهدا شاقا حيث يكفي نصاب المعلوماتية بلمس لوحة مفاتيح الحاسب الآلي والتي تقوم بعمليات الحاسب والتحليل واسقاط حواجز وأساليب الحماية الأكثر خداعا مما يوضح ان أفعال الغش هذه تتمايز قليلا في مضمونها وتنفيذها ومحو أثارها عن الأفعال الخاصة بالإجرام التقليدي.

وعليه يتعين على الفاعل ان يحوز عناصر ثلاثة أثناء تدخله غير المشروع في ذاكرة الحاسب الآلي لالتقاط المعلومات المختزنة بها او تعديلها او لإتلافها وهذه العناصر هي:

- ان يحوز بنفسه حاسبا آليا مصغرا او نهاية طرفية وهي عبارة عن محطة للتراسل بين المستعمل والحاسب الآلي، أو يكون لديه على الأقل الشفرة.

- ان يكون مزودا بمودم وهي أداة لترجمة تعليمات مكتوبة بلغة الحاسب الآلي الى رموز رقمية أو العكس.

- ان يكون لديه قدر لا بأس به من الحيل والكفاءة والمواظبة.

وسوف نلقي نظرة عابرة على مجموعة خصائص خاصة من المخادعين وهو صغار نوابغ المعلوماتية، قبل الدخول في أفعال الغش المرتكب بواسطة المحنكين.

- صغار نوابغ المعلوماتية: وهم الشباب البلغ المفتون بالمعلوماتية والحاسبات الآلية وتتمثل افعالهم في الانتهاكات غير المسموح به في ذاكرات الحاسبات الآلية وان كانت وسائل الاعلام المرئية تحاول التضخم من هذه الظاهرة لتسويق وسائلهم لان هؤلاء الشباب مفتونين بهذه الأنشطة الاجرامية المبتكرة والمستحدثة ومثال على ذلك:

***** العصابة التي يطلق عليها 414 والتي تقطن بالولايات المتحدة الامريكية وقد نسب اليها ارتكاب ستين فعلا تعد على ذاكرات الحاسبات الآلية بما نجم عنها اضرار لحقت بالمنشآت العامة والخاصة.

وهؤلاء الشباب لا يقدرون مطلقا النتائج المحتملة التي يمكن ان تؤدي اليها افعالهم غير المشروعة بالنسبة لنشاط منشأة او شركة تجارية لان لديهم ميل للمغامرة والتحدي والرغبة في الاكتشاف وذلك عكس المجرم في جرائم السرقة فقد

يكون فردا أو موظفا عاما او مكلفا بخدمة عام – ثم ان الجاني في جرائم النصب كثيرا ما يستعين بشخص آخر لتأييد ادعاءاته الكاذبة مظهرا جديا يحمل المجني عليه على تصديقها.

وقد بدأت الولايات المتحدة وأحيانا في أوروبا في التحقق من المجرمين مرتكبي أفعال الغش المعلوماتي ومصادرة أجهزة الحاسبات الآلية الخاصة بهم وهي أداة الفعل الاجرامي وما يرتكبه هؤلاء الشباب من أفعال الغش لا خوف منه على الاطلاق.

وإذا كان بإمكان هؤلاء الشباب انتهاك الأنظمة إلا انه يخشى من التدخل الحقيقي لمحترفي أفعال الغش والتجسس او من ماهري قرصنة المعلومات.

ولكن الخطر الذي يواجه هذه الطائفة هو احتمال الانزلاق الذي من الممكن ان يحدث من مجرد هاوي صغير للأفعال غير المشروعة، الى محترفي لأعمال السلب والخطر والاهم هو اختصاص منظمات او افراد غير شرفاء لهؤلاء الشباب. (عياد، 2006، صفحة 52، 53)

– محترفوا الجرائم المعلوماتية: مرتكبي هذه الأفعال غير المشروعة يكون متعسفا وذات خطورة خاصة بسبب تقنيات العالية من جهة وغموض شخصية مرتكبيها(ويتشابه مرتكبو هذه الأفعال الآثمة مع المجرمين ذوي الياقات البيضاء من حيث كونهم من أصحاب التخصصات العالية ولهم الهيمنة الكاملة مع تقنية الالكترونيات، وعلى قدر من الذكاء) ، من جهة أخرى وتؤكد الدراسات والدعاوي التي تم تحريكها في هذا الشأن سواء في أمريكا او أوروبا ان الجيل الحديث هم الأكثر لمرتكبي افعال الغش المعلوماتي وتتراوح أعمارهم من 25 إلى 45 سنة هذه الفترة هي المرحلة الزمنية والتي مع تعميم تقنية المعلوماتية ومحترفي أفعال الغش المعلوماتي هم المحلل والمبرمج والمستخدم والصراف والشخص الأجنبي عن المنشأة و المشغل.

وعندما قام فريق من علماء النفس بدراسة عدد من شخصيات مرتكبي أفعال الغش المعلوماتي ولا حظوا ان هؤلاء المخادعين لا يدركون ان سلوكهم يستحق العقاب، ولكن الأبحاث اثبتت ان بعض مرتكبي أفعال الغش المعلوماتي لديه اتجاه اجرامي خطير ونية سيئة جلية مثال اعمال التجسس.

وأثبتت ان الغالبية العظمى نتيجة للأبحاث التي تمت من الحالات المكتشفة لأفعال الغش المعلوماتي قد ارتكبت بواسطة مستخدم من المنشأة التي تدار بنظام المعلوماتية او عن طريق الاشتراك فيها.

أ-**الفاعل في جريمة الغش المعلوماتي:** غالبا ما ترتكب أفعال الغش المعلوماتي بواسطة العاملون في المنشأة والتي تستهدف الحاسبات الآلية وعندما يقومون بهذه الاعمال فيكون ذلك إما لحسابهم أو لحساب اشخاص أجانب مقابل مبلغ من المال ولكن تبين ان هناك حالات ارتكبت فيها فعل الغش المعلوماتي بواسطة مستخدمي المنشأة ولحسابها أيضا وبموافقة واشتراك إدراتها.

فالمحللين أنفسهم هم الذين يعتبرون العوبة هؤلاء القائمين على تشغيل ومراقبة نظام المعلوماتية لأنهم يملكون المعرفة اللازمة والتثنية الكافية للتلاعب بالحاسبات الآلية.

ب-الشريك في جريمة الغش المعلوماتي: الاشتراك، المساعدة غالبا ما تكون ضرورية من اجل الاقتراف المحدق لأفعال الغش المعلوماتي فجريمة الغش المعلوماتي نظرا لأن الأمر يستلزم دقة متناهية في ارتكابها، فإن الامر يتطلب مشاركة او مساعدة اشخاص آخرين او يكون سلبيا مثل الصمت وتكرهم يفعلون ما يحلو لهم او يكون إيجابيا مثل المساعدة الفنية او المادية.

(عياد، 2006، صفحة 54، 55)

ثانيا-المجني عليه في الجريمة المعلوماتية : وفقا لتقديرات خبراء الصندوق الدولي للبنوك أف بي جي من المستحيل ان يتم على نحو دقيق نطاق الجرائم المعلوماتية وقد لا يعلم ضحايا هذه الجرائم شيئا عنها، إلا عندما تكون انظمتهم المعلوماتية هدفا لفعل الغش وفي حالة علمهم بذلك فانهم يفضلون عدم افشاء الفعل لأنه لا يوجد من يريد الاعتراف بانتهاك نظامه المعلوماتي وبلغت خسائر أوروبا الغربية وحدها من ظاهرة الغش المعلوماتي حوالي 54مليون فرنك فرنسي في عام 1977 وخسائر الاقتصاد الأمريكي الناشئة عن هذه الظاهرة أيضا حوالي 400 مليون دولار.

(عياد، 2006، صفحة 60)

تشير الإحصاءات الى ان جميع الأنشطة التي تستخدم الحاسب الآلي تكون عرضة لخطر ظاهرة الغش المعلوماتي.

ويلاحظ دائما ان الاتجاه الأساسي للغش المعلوماتي يستهدف البنوك في حدود 19 بالمائة ويستهدف خاصة المنشآت المالية او التي تهيمن على الأقل على القيم الرأسمالية ثم تأتي بعد ذلك النقود وهناك سوق سوداء للمعلومات بجانب السوق الشرعي للمعلومات، والتي تتم بمقتضاه مقايضة وريع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين والشرعيين.

ويلاحظ ان هذا النوع من الاجرام يرتبط بالجزء الأعظم للأنشطة الاقتصادية والاجتماعية للمجتمع ويمكن تصوره بالنسبة للمعلومات الآتية:

-المعلومات المالية: ويستهدف المركز الحسابي والإداري وتنقلات الأموال والاستثمارات وفي المنشآت العامة والخاصة.

-المعلومات التجارية والصناعية: وتستهدف الدراسات الخاصة بالأسواق ومشروعات الاستثمار والتصنيع والإنتاج والتجارة والوزيع والاسعار ومراكز البيع والقطاع الصناعي للإنتاج.

-المعلومات الشخصية: وهي تلك المختزنة في ذاكرات الحاسبات الآلية للبنوك وشركات التأمين ولدى المحامين والمستشفيات واقسام الشرطة والأحزاب والنقابات.

-المعلومات العسكرية: تتمثل في اسرار الدولة والمشروعات النووية والتصنيع الحديث للأسلحة ويبدوا ان هذه المعلومات الأخيرة هي الأكثر رواجا في سوق المعلومات السوداء هذه الطائفة يحرك انشطتهم الرغبة في الانتقام من صاحب العمل او التصرف لمنشاة معنية لهم.

. (عياد، 2006، صفحة 61، 62)