الجريمة المعلوماتية

د. عمارة فتيحة

جامعة سعيدة– الجزائر

مقدمة

الكثير منا يطلق على عصرنا هذا اسم عصر المعلومات أو ثورة المعلومات، وهي إحدى أهم الثورات في العالم، وتعد مكملة للثورة الزراعية والتجارية والصناعية حيث اكتسبت المعلومات فيها من أهمية فائقة، و تأثير هائل على البشر والحكومات فأصبحت المعلومة قوة لا يستهان بها في يد الفرد أو في يد الدولة[1].

بل أكثر من ذلك أصبحت مقياساً تقاس به قوة الشعوب، فمن يملك المعلومات في هذا العصر و لديه القدرة على حمايتها يستطيع أن يسيطر على العالم.

ومن الطبيعي أن يواكب هذا التطور السريع الموسوم بالثورة المعلوماتية الظاهرة الإجرامية الخاصة به، لذا كان لزاماً ونحن في مستهل دراستنا بالبحث في الظاهرة الإجرامية الخاصة بجرائم الاعتداء على المعلومات الالكترونية، تلك الظاهرة المستحدثة التي يملك بنواصيها فئة خاصة من المجرمين ذوي مهارات تختلف عن تلك التي يتمتع بها المجرمون التقليديون[2] مهما اتسم إجرامهم بالخطورة، فهم وبالاستناد إلى التطور التكنولوجي الذي عرفه العالم أواخر القرن العشرين استطاعوا أن يطوعوا التكنولوجيا لأغراضهم الإجرامية، وأهم ما ميز هذا النوع من الإجرام المستحدث إلى حد ما هو اعتماده وبصورة اساسية على نظام معلومات بالغ الدقة والتعقيد، فنجد أن مجرمي المعلوماتية على قدر لابأس به من الذكاء الذي يعكس في الوقت ذاته قدرتهم على التكيف الاجتماعي مع المجتمع، وتتنوع أنماط هؤلاء المجرمين وتتباين الأسباب التي تدفعهم إلى ارتكاب أعمال غير مشروعة.

هذا وقد أظهرت الدراسات والأبحاث التي أجريت في هذا الشأن أن المؤسسات المجني عليها يغلب عليها الطابع المالي، كالبنوك وشركات السمسرة وشركات التأمين أي المؤسسات المالية، ومن العجيب أن المؤسسات المجني عليها

تفضل التكتم والسرية حيال وقوع جريمة معلوماتية بها بحجة الحفاظ على سمعتها وثقة المتعاملين معها[3].

1: داود حسن طاهر، جرائم نظم المعلومات، الطبعة ال أولى، مركز الدراسات والابحاث ، الرياض، سنة 2000، ص 21

2: بحيث يظهر أن للمجرم المعلوماتي مزايا تجعله مختلف عن المجرم التقليدي فهو محب للمخاطرة و إضافة لتملكه خيالاً نشطاً وحب انتحال الشخصيات كما يملك مهارة تؤهله لوصول اجرامه لحدود غير متوقعة، انظر: ريم جعفر الشريمي، هوية المجرم المعلوماتي، مقال منشور على موقع المركز العربي لأبحاث الفضاء الالكتروني ، اكتوبر 2012،

.http://accronline.com/article_detail.aspx?id=4712

3 : عمر ابو الفتوح حمامي، الحماية الجنائية للمعلومات، دار النهضة العربية، القاهرة ، سنة 2010 ، ص 65

هذا الأمر أدى إلى – مع وجود أسباب أخرى– ظهور ما يعرف بالرقم الأسود لجرائم المعلوماتية، والذي يتم على قلة الجرائم المكتشفة أو المبلغ عنها، إذ أوجد صعوبة شديدة في تحديد حجم الخسائر الناشئة عن الجرائم المعلوماتية سواء في القانون المقارن أو القانون الجزائري.

وقد أصبح النظام المعلوماتي بالرغم من فوائده الجمة مصدر ازعاج وقلق للآخرين حيث أصبحت المعلومات الإلكترونية هدفاً للمحتالين، وأتاحت الفرصة لارتكاب جرائم تقليدية بطرق غير تقليدية[4]، كما لا يتوانى محترفو الإجرام المعلوماتي من ابتكار وسائل تقنية حديثة من أجل الاعتداء على هذه المعلومات.

ومن ثمة كان لزاماً التطرق أولا لماهية الإجرام المعلوماتي ثم الحديث عن طبيعة الشخص مرتكب هذا النمط من الإجرام، لنختم البحث بقراءة في دواعي الحماية الجنائية للمعلومات الإلكترونية.

وترتيباً لما تقدم سنقسم هذه الورقة البحثية إلى ثلاثة مباحث:

المبحث الأول: طبيعة الإجرام المعلوماتي

المبحث الثاني: المجرم المعلوماتي

المبحث الثالث: الحماية الجنائية للمعلومات الإلكترونية

4 : خالد بوكشير، الجريمة المعلوماتية، مذكرة نهاية التدريب، المنظمة الجهوية للمحاميين ناحية سطيف، 2005-2006،ص6

المبحث الأول

الإجرام المعلوماتي

إن المعلوماتية باعتبارها ظاهرة علمية اقتصادية اجتماعية، لا يمكن أن تتطور دون أن تتوافر لها القواعد القانونية التي تنظم استغلالها ونظرا لأنها لازالت في مرحلة التطور والتفاعل فإنها مثل كل تطور جديد تحمل في طياتها جانبا مظلما يتجسد في مجال القانون الجنائي في ظاهرة الإجرام المعلوماتي[5] ، وقد ارتبط هذا التطور بظهور ثورة الاتصال والمعلومات التي نجد فيها صراعاً مستمراً بين جانبي الخير والشر.

فنجد هذه الثورة من ناحية ساعدت على عولمة المعلومات وسهلت كثير من الخدمات والأعمال[6]، بحيث توصلت البشرية إلى السيطرة على المعلومات من خلال استخدام الحاسب الآلي لتخزين ومعالجة واسترجاع المعلومات، فضلا عن استخدامه في عمليات التصميم والتصنيع والتعليم والإدارة مقتحما بذلك شتى نواحي الحياة الانسانية.

إضافة إلى جعل المعلومات في متناول الجميع من خلال شبكات الانترنت، فأصبح العالم مزدخراً بكم هائل من المعلومات لا تعرف الحواجز الجغرافية، ولا المسافات بصورة يمكن معها القول أن العالم أصبح أشبه بمجتمع كبير تترابط فيه الحاسبات وشبكات المعلومات، لتعلن بزوغ فجر ثورة جديدة هي الثورة المعلوماتية la révolution informatique [7].

إن هذه الخدمات التي تقدمها ثورة المعلوماتية للبشرية جمعاء، تبقى عرضة للإساءة في الاستخدام، فإذا كانت الكثير من المؤسسات والبنوك تستخدم الحاسب الآلي فإنه من خلاله ترتكب الكثير من الجرائم مثل السحب الالكتروني من الرصيد بواسطة البطاقة الممغنطة إذا كان مزوراً أو من غير صاحب الصفة الشرعية كذلك يمكن تصور التجسس عن بعد وسرقة بيانات تتعلق بالأمن القومي، ومن الممكن أن يترتب عن الإصابة بالفيروس المعلوماتي تدمير برامج هامة علاوة على أنه من المتصور أن يحدث مساساً بحياة الأفراد الخاصة وانتهاكها من خلال استخدام الحاسب الآلي وشبكة الانترنت بصورة اجرامية

لذلك ولتحديد السمات العامة للإجرام المعلوماتي، وجب علينا دراسة بدايات ظهور هذا النوع من الإجرام علاوة على تحديد مفهوم أو تعريف لمصطلح الجريمة المعلوماتية قصد الوصول إلى أهم عناصر هذه الجريمة المستحدثة .

5 : علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، طبعة أولى، الدار الجامعية، بيروت، سنة 199، ص 07

6 : يوسف امير فرج، الجريمة الالكترونية والمعلوماتية والجهود الدولية لمكافحتها، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، سنة 2011، ص 155

7 : يوسف امير فرج، نفس المرجع، ص 155-156

المطلب الأول

ظاهرة الإجرام المعلوماتي وتطورها

ترجع البدايات الأولى لظاهرة الإجرام المعلوماتي إلى ستينات القرن الماضي عندما طرحت الصحف والكتب العلمية البيانات الأولية التي تتناول ما يطلق عليه بصفة عامة جرائم نظم المعلومات، وارتكز الحديث غالباً حول أعمال التخريب والتلاعب بالحاسب الآلي وتعطيله واستخدامه بطريقة غير مشروعة[8] ولما كانت الصحافة غير المتخصصة هي أول من سلط الضوء على هذه الظاهرة الإجرامية المستحدثة، أحدث ذلك نوعاً من الصعوبة في تحديد طبيعة هذه الظاهرة بالاعتراف بها كظاهرة واقعية حقيقية أو حصرها في زاوية الخيال الصحفي[9].

وقد عُرفت هذه الجرائم بشكل واضح بزيادة مروعة لها في البنوك الامريكية، حيث قام موظفو البنك غير الأمناء باستبدال قسائم إيداع النقدية في حسابات العملاء بقسائم إيداع في حساب الموظف وبذلك يتم إيداع النقدية في حسابه بدلاً من حساب العميل، وانتشر ذلك الأسلوب في الاختلاس حين بدأت البنوك في استخدام ترميز الشيكات بالحبر الممغنط، ولم يكن هناك وقتها أساليب رقابية على هذا الاستخدام[10].

وفي منتصف السبعينات دخلت ظاهرة الإجرام المعلوماتي نطاق بعض الأبحاث المتعلقة بعلم الإجرام، وخلال هذه الفترة استطاع الباحثون تحديد بعض الافعال التي يمكن ادراجها ضمن هذا النوع من الإجرام.

لقد بدأ مفهوم الإجرام المعلوماتي بالتغير والتطور بحلول الثمانينات فلم يعد نشاطه قاصراً على المجال الاقتصادي، وإنما أصبح ماسا بمجالات أخرى كالاعتداء على حرمة الحياة الخاصة للأفراد.[11]

ومنذ عام 1987 بدأت جرائم الفيروسات باعتبارها إحدى صور الجريمة المعلوماتية تلوح في الأفق بشدة، فهي تعتبر من أخطر صور الاعتداء على المعلومات، إذ أن عملها قد يؤدي إلى جعل النظام المعلوماتي بأكمله والعدم سواء.

8 : عمر عبد الفتوح الحمامي، مرجع سابق، ص 52

9 : جدير بالذكر أن ظاهرة الاجرام المعلوماتي شهدت ميلادها عالميا في أواخر الستينات القرن الماضي بالولايات المتحدة الامريكية باعتبارها مهد المعالجة الآلية للمعلومات ، ثم غزت بعد ذلك أوروبا، وأجريت في هذا الشأن العديد من الأبحاث والدراسات نذكر منها على وجه الخصوص تلك الدراسة التي قام بها الأستاذ parker تحت اشراف معهد stand ford reseache بالولايات المتحدة، كما أجريت أيضا العديد من الدراسات في أوروبا، منها تلك التي قام بها معهد علم الإجرام للقانون الجنائي بجامعة فريقوري بألمانيا كما شهدت فرنسا العديد من الندوات والمؤتمرات في هذا المجال.

10 : عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، الطبعة الأولى ، دار المستقبل للنشر والتوزيع، الأردن، سنة 2009، ص 112.

11 : عمر عبد الفتوح الحمامي، مرجع سابق، ص 53

المطلب الثاني

تعريف الجريمة المعلوماتية

تتشابه الجريمة المعلوماتية أو جريمة تقنية المعلومات مع الجريمة التقليدية في أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة، وضحية والذي يكون شخصاً طبيعياً أو شخصاً معنوياً، أداة و حين وجود مكان الجريمة، وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة، ففي جريمة تقنية المعلومات فالأداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجاني إليه ، ولكن في الكثير من تلك الجرائم فإن الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة [12].

ولقد ارتبطت الجريمة محل الدراسة ولايزال يرتبط مفهومها بظهور التكنولوجيا الحديثة وتطوراتها المستخدمة في تشغيل ونقل وتخزين المعلومات في شكل الكتروني.

ولما كان مصطلح الجريمة المعلوماتية أو جريمة تقنية المعلومات الأكثر اتساعاً لامتداد دلالته التقنية لدلالته القانونية لتشمل جميع الاعتداءات التي تقع في البيئة الرقمية[13] حيث يشمل مضمونها في هذا الإطار كل جرائم الاعتداء على المعلومات بمختلف أنواعها ، أنظمة الحاسبات، أنظمة الاتصالات.

كما يتسع ليشمل جميع الابتكارات الالكترونية في مجال تكنولوجيا المعلومات فضلا عن الجرائم التي تستخدم فيها هذه النظم كوسيلة لارتكاب جرائم أخرى.[14]

ويظهر جلياً ترادف مصطلح جرائم المعلوماتية أو تقنية المعلومات ومصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. والذي آثار المشرع الجزائري استخدامه وحسنا فعل في القانون رقم 09-04 لسنة 2009 المتضمن الوقاية من هذه الجرائم ومكافحتها

كان هذا عن المصطلح القانوني الدال على الجرائم الناشئة عن البيئة الرقمية أما مسألة تعريفها فإنه من بين أكثر المشاكل الشائكة إذ لم يتفق الفقه على تحديد تعريف جامع مانع يوضح من خلاله ماهية وعناصر الإجرام المعلوماتي.

فقد عرفها الفقيه تيدمان [15] بأنها " كل جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات" وعرفها البعض[16] الآخر بأنها " تلك الجرائم التي تكون قد حدث في مراحل ارتكابها بعض العليات الفعلية داخل الحاسب " وبمعنى آخر " هي التي يكون فيها للحاسب دوراً ايجابياً أكثر منه سلبياً ".

12 : جمال فؤاد، بحث حول الجرائم المعلوماتية ،منشور على الموقع:
http://www.shaimaaatalla.com/vb/showthread.php?t=3160

13 : رشيدة بوكر، المرجع السابق، ص 37

14:عمر عبد الفتوح الحمامي، مرجع سابق، ص 52

15 : مثل الفقيه الالماني تيدمان أنظر: عمر عبد الفتوح الحمامي ، مرجع سابق، ص 55

بينما أعطى الخبير Hparker مفهوماً واسعاً للجريمة المعلوماتية والذي أحاط من خلالها بكل أشكال التعسف في مجال استخدام نظم المعلومات، فهي من وجهة نظره " كل فعل إجرامي عمدي يتصل بالمعلوماتية، ويتسبب عنه خسارة تلحق بالمجني عليه أو كسب يجنيه الفاعل".[17]

كذلك يعرفها الاستاذ rosemblatt على انها " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول إليها أو التي تحول عن طريقه"[18].

ما يلاحظ على هذا التعريف أنه يضيق من مفهوم الجريمة المعلوماتية، اذ يخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسب كأداة لارتكابها .

ويعرف الاستاذان vivant et le stanc الغش المعلوماتي على أنه " مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب" [19].

أما خبراء منظمة التعاون الاقتصادي والتنمية المعروفة اختصارا بـ OECD عام 1983 فقد عرفوها على أنها " كل سلوك غير مشروع أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها" [20]. وقد عرفها البعض الآخر[21] بأنها " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب".

ولقد حاول البعض من جهته تحديد المقصود بجرائم الانترنت حيث عرفها بأنها " تلك الجرائم التي لا تعرف حدوداً جغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي، عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة بها"[22].

كما تبنى مؤتمر الامم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين[23]، التعريف الاتي " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية ".

ولعل التقارب يظهر جليًا فيما تبناه المشرع الجزائري حديثا في تعريفه لجريمة تقنية المعلومات وذلك بموجب المادة الثانية من الفصل الأول من قانون 09-04 الصادر بتاريخ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حين عرفتها بأنها " جرائم المساس بأنظمة المعالجة

16 : مثل كل من الفقيه richard totty و anathony hardcastle أنظر: محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، مصر ، سنة 2003، ص 06

17 : نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع ، عمان، 2008، ص 48

18: نهلا عبد القادر المومني، نفس المرجع، نفس الصفحة.

19 : حيث يفضل الاستاذان vivant et le stanc مصطلح الغش المعلوماتي لإطلاقه على هذا النوع من الجرائم، انظر عمر عبد الفتوح الحمامي ، مرجع سابق، ص 55

20 : مشار إليه لدى : رشيدة بوكر، مرجع سابق، ص 39

21 : david thomson, current trends in cumputer crime, computer control quarterly, vol 9 n°1, 1991, p 2

22: منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، سنة 1994، ص 13

23: اعقد في فينا في الفترة ما بين 10-17 أبريل عام 2000 مشار له من نهلا المومني عبد القادر، مرجع سابق، ص 50

الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية".

لقد حاول هذا التعريف أن يشمل قدر الإمكان جميع الصور الإجرامية لجريمة تقنية المعلومات سواء التي تقع على النظام المعلوماتي في حد ذاته وما يحويه من مكونات غير مادية، كما لو كان الهدف الاساسي من ارتكابها هو الحصول على المعلومات أو تشويهها أو تخريبها والتي اما تكون مخزنة في النظام أو منقولة منه أو إليه عبر شبكات المعلومات[24] كما استطاع هذا التعريف أن يحيط بجميع الجرائم الممكن حدوثها في البيئة الالكترونية، عاملا على تجنب حصرها بشكل يسمح بإفلات العديد من صورها من دائرة التجريم.

المبحث الثاني

المجرم المعلوماتي

تتعرض المعلومات الإلكترونية والمخزنة داخل الحاسب الآلي لعدة مخاطر من شأنها الاعتداء عليها بأية صورة، كفقد المعلومات أو إذاعتها أو إفشائها على نحو غير مسموح به، أو تهديد النظام المعلوماتي بأكمله لخطر الاعتداء عليه(25)، ومؤدى هذه المخاطر عدة أسباب منها أسباب طبيعية، تتمثل في الحرائق والزلازل أو أي إرتفاع مفاجئ في مستوى التيار الكهربائي، وقد تعزى هذه المخاطر للإنسان ذاته سواء كان عن خطأً من إنسان حسن النية ، أو يكون عن إنسان سيء النية أي يعتدي على المعلومات عن عمد وسوء نية.

فالمعلوماتية يمكن القول بأنها أداة حياد وأن مصدر انتهاكها والاعتداء عليها هو الإنسان ذاته، فالمسألة مرتبطة به في المقام الأول وبشخصه ودوافعه.

لذلك فإنه من الضروري ونحن بصدد إلقاء الضوء على جرائم الاعتداء على المعلومات الإلكترونية ككل، ألا نغفل شخصية مرتكبها، وألا نكون بمعزل عنه.

وترتيباً على ما تقدم سوف يتم التطرق إلى خصائص شخصية المجرم المعلوماتي في مطلب أول، أما المطلب الثاني فسيكون الحديث فيه عن الفئات المختلفة للمجرم المعلوماتي.

المطلب الأول

صفات شخصية المجرم المعلوماتي

حتى تحقق العقوبة أهدافها سواء في مجال الردع العام أو الردع الخاص يجب أن نضع في الاعتبار شخصية المجرم، وذلك لإعادة تأهيله اجتماعياً حتى يعود مواطناً صالحاً مرة أخرى، وإن انطبق هذا القول على

24 : رشيدة بوكر، المرجع السابق، ص 44

25: محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، مصر ، سنة 2003، ص 23.

المجرم التقليدي فإنه كذلك ينطبق على المجرم المعلوماتي، هذا الأخير الذي تقترب سماته من سمات المجرمين ذوي الياقات البيضاء[26] فهو مجرم يتمتع بقدر لا يستهان به من المهارة والمعرفة بالوسائل الالكترونية المستخدمة في التحكم في المعلومات بما في ذلك الحاسوب والانترنت، فهو انسان ذكي (الفرع الأول) واجتماعي بطبعه(الفرع الرابع) .

الفرع الأول: المجرم المعلوماتي كإنسان ذكي

يتميز غالباً بالذكاء حيث أن هذا النوع من الجرائم تتطلب مقدرة عقلية وذهنية عميقة، خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة ، فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجأ إلى استخدام العنف أو الاتلاف المادي بل يحاول تحقيق أهدافه بهدوء[27].

وعلى هذا الأساس يقال أن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة مع الإجرام التقليدي الذي يصل إلى العنف، في حين أن مرتكبي الإجرام المعلوماتي من الأفراد ذوي المهارات الفنية وينتمون إلى التخصصات المرتبطة بالحاسب الآلي.

غير أن بعض الفقه[28] تحفظ حيال رسم صورة عامة للمجرم المعلوماتي متسمة بالذكاء، وذلك على سند من القول أن بعض أنماط الجريمة المعلوماتية مثل اتلاف الحاسب الآلي أو تدميره كلياً أو جزئياً أو سرقة المعلومات المخزنة داخله لا تحتاج من مرتكبها أن يكون على قدر من الذكاء.

والواقع أنه لا يمكن وصف كل جريمة تتصل بالحاسب بأنها نمط من أنماط الجريمة المعلوماتية حيث أن المقصود بالإجرام المعلوماتي بالمعنى الدقيق هو الإجرام الذي ينشأ عن تقنيات التدمير الناعمة التي تتمثل في التلاعب بالمعلومات أو الكيانات غير مادية.

الفرع الثاني: المجرم المعلوماتي مجرم عائد للإجرام

يتميز المجرم المعلوماتي بأنه عائد للجريمة دائما، فهو يوظف مهارته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات[29]، فهو بذلك لا يحقق جريمة الاختراق بهدف الإيذاء في أغلب الحالات وإنما نتيجة شعوره ومهارته في الاختراق.

26: مصطلح المجرمين ذوي الياقات البيضاء ، مصطلح حديث نسبيا و أول من أطلقه عالم الاجتماع suther land حيث وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية ذوي المناصب الادارية الكبيرة وتشمل أنواعا مختلفة من الجرائم كغسيل الاموال وتجارة الرقيق الابيض وتزوير العلامات التجارية وغير ذلك من الجرائم التي يقومون بإرتكابها وهم جالسون في مكاتبهم الفخمة. انظر المخاطر الامنية للانترنت مقال منشور على موقع: http://www.minshawi.com/node/58

27 : نهلا المومني عبد القادر، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع ، عمان، 2008، ص 77

28 :حيث يقرر الاستاذ michel kabag أنه لا يوجد حتى الان نظام أو شبكة كومبيوتر سواء فيما يتعلق بالاتصالات أو بشبكة الحاسبات الآلية لايمكن اختراقها حيث تبدو هذه النوعية من القراصنة ولسوء الحظ مستمرة البقاء. مشار إليه عمر ابو الفتوح الحمامي، المرجع السابق ص 78

29 : يوسف أمير فرج، الجريمة الالكترونية والمعلوماتية والجهود الدولية لمكافحتها، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، سنة 2011، ص 120

ومن جهة أخرى قد يعود مجرمي المعلومات إلى ارتكاب جرائم أخرى انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة، فيؤدي ذلك إلى العودة إلى الإجرام[30].

الفرع الثالث: المجرم المعلوماتي يبرر ارتكاب جريمته

حيث يعتبر مرتكب الجرائم المعلوماتية، أن الفعل الذي أتى به لا يمكن أن يدخل في عداد الجرائم أو بمعنى أخر لا يصنف على أنه فعل غير أخلاقي خاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله [31].

ولعل التباعد في العلاقة الثنائية بين الفاعل والمجني عليه، يسهل المرور إلى الفعل الغير مشروع، ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل، كما أن مرتكبي هذه الجرائم يضعون تفرقة بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها تحمل نتائج تلاعبهم.

وهناك واقعة حدثت أمام القضاء الألماني فيها دهشة وغرابة نابعة من اعترافات متهم يبلغ العمر 16 سنة تحقق وبصورة جلية التصور الذي يتبناه مجرمو المعلوماتية على اعتبار أن سلوكهم لا يعد بأي شكل من الأشكال عملاً اجرامياً[32].

الفرع الرابع: المجرم المعلوماتي انسان اجتماعي

إذ أن المجرم المعلوماتي وفي الغالب لا يظهر أية ميول عدائية تجاه المجتمع الذي يعيش فيه، وليس هذا فحسب ولكنه متكيف مع هذا المجتمع ويمكن ربط هذه القدرة على التكيف باعتباره انسانا ذكيا والذكاء في نظر الكثيرين ليس سوى القدرة على التكيف [33] فمن خلال الجرائم التي تم اكتشافها، يلاحظ أن المجرم المعلوماتي غالبا ما تكون له علاقات مع المؤسسات المجني عليها، ويزداد ذلك بالثقة التي يوليها أصحاب المنشأة المجني عليها له.

غير أن ذلك لا يقلل من الخطورة الإجرامية لديه، بل إن هذه الاخيرة قد تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية عنده [34].

30:غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، طبعة 2010، ص 14

31: نهلا المومني عبد القادر، المرجع السابق، ص 78

32: حيث نسب اليه ولوجه المقترن بالغش في نظام الفيديوتكس الخاص بـ bundes post والمعروف بمصطلح BTX ودافع المتهم عن نفسه قائلا " تملكني احساس قوي بأن أكون مفيدا في كشف عيوب نظام btx ولذا أرسلت في الحال إلى مجموعة عمل btx كل العناصر التي اكتشفتها بالصدفة، والتي أظهرت تشككها فيما يخص حماية البيانات لا سيما وأن غالبية ملاحظاتي لم تكن معروفة بعد لدى هؤلاء، مما أتاح الأمر إلى تلاشي هذه العيوب، ومن جهة أخرى إذا كنت مولعا بنظام btx وأكرس له نفسي صباحاً مساءاً ولكني لست شريراً على الاطلاق، كبعض القائمين على نظام btx ولا يملكون أية كفاءة" أنظر: عمر ابو الفتوح الحمامي ، مرجع سابق، ص 81-82

33 : أنظر عمر ابو الفتوح الحمامي ، مرجع سابق، ص 80

34 : غنام محمد غنام، المرجع السابق، ص 15

المطلب الثاني

الفئات المختلفة للمجرم المعلوماتي

تختلف الأفعال في الجريمة المعلوماتية على نحو يسير في مضمونها وتنفيذها ومحو أثرها عن تلك الافعال الخاصة بالإجرام التقليدي، ولقد ساهم التسارع الرهيب في مجال التقنيات الرقمية الحديثة بدوره بتغيير وتطوير أنواع الجرائم، فضلاً عن تقدم جدوى وسائل الاعتداء.

وأمام هذا التطور والتغير السريع في أصناف الجريمة المعلوماتية وصورها فقد يكون من الصعب وضع تصنيف ثابت لطوائف مجرمي التقنية.

غير أنه يمكن لنا ووفقاً لما توصلت له الدراسات والأبحاث التي تناولت ذلك، أن نبين بعض الانماط لهؤلاء المجرمين[35].

الفرع الأول: صغار مجرمي المعلوماتية

ويقصد بهم الشباب الذين استهوتهم المعلوماتية والحاسبات الآلية حيث لفتوا الانظار عقب أفعال الانتهاك غير المسموح بها في العديد من ذاكرات الحاسبات الآلية، وقد تعددت أوصافهم في الدراسات الاستطلاعية والمسحية.

وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح المتلعثمين الدال حسب تعبير توم فورسستر على "الصغار المتحمسين للحاسوب بشعور من البهجة، دفعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب "،[36] ويسميهم البعض كذلك بمجانين المعدلات والمعدلات العكسية، بالاستناد إلى كثرة استخدامهم لتقنية المعدل والمعدل العكسي المورديم الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم.

ويذهب بعض الفقه[37] إلى أنه غالباً ما يكون أفراد هذه الطائفة من ذوي النوايا الحسنة، فغالباً ما يكون الباعث من وراء هذه الانتهاكات إثبات المهارة في التعامل مع الحاسبات الآلية، وإبراز مواطن الضعف في الأنظمة المعلوماتية، دون قصد إلحاق ضرر بالغير.

لكن نستطيع أن نقرر أنه إذا كان لا يوجد خوف من أفعال هذه الطائفة إلا أن الخطر مؤكد يتجلى في الآتي: [38]

35: نهلا المومني عبد القادر، مرجع سابق، ص 81

36 : Tom foreste, high tech society, third printing, 1990, combridge ; p141

37: محمد سامي الشوا ، مرجع سابق، ص 40

38 : الحمامي عمر عبد الفتوح ، مرجع سابق، ص 85-86

أن هذا النمط من أفعال الغش ولئن كان مرتكبوه ليسوا في الغالب الأعم من ذوي النوايا السيئة، إلا أنه يرتبط ومن ناحية أخرى بمشكلة أكثر تعقيدًا تتمثل في المخاطر التي تطارد الأسرار والمعلومات المسجلة والمخزنة بالذاكرات الصناعية للحاسبات الآلية، وتلك التي تنتقل من خلال الشبكات .

الفرق بين التدخل الحقيقي لمحترفي أفعال الغش المعلوماتي و ماهري قرصنة المعلومات حيث أنهم أكثر خبرة ودراية بالمعلوماتية من هؤلاء الشباب.

الخوف من انزلاق أفراد هذه الطائفة من مجرد هواة، إلى مصاف محترفي السلب pirate professionnel والخطر الأعظم يتجلى في احتضان منظمات وأفراد خارجين عن القانون لهؤلاء الشباب.

الفرع الثاني: المخترقون أو القراصنة

أهم ما يميز أفراد هذه الطائفة أنهم أصحاب التخصصات العالية ولهم الهيمنة الكاملة على تقنية الإلكترونيات، وعلى قدر كبير من الذكاء ويمكن تقسيم هذه الفئة إلى ما يلي:

القراصنة الهواة العابثون أو الهاكرز: وهم المتطفلون الذين يتحدَون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، فهذه الطائفة غالباً ما تكون من هواة الحاسوب، فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع[39].

إذ يدفعهم في ذلك الفضول وحب المعرفة والتعمق في عمل الانظمة المعلوماتية، ومجرمو المعلوماتية من هذا الصنف هم عادة أشخاص عاديون يشغلون مناصب محل ثقة[40] ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات الإلكترونية.[41]

وتتميز هذه الفئة عن غيرها، بوجود نوع من العلاقة فيما بين القراصنة المصنفين ضمنها من حيث تبادل المعلومات وبالأخص التشارك في وسائل الاختراق وآليات نجاحها في مواطن ضعف نظم الحاسوب والشبكات، ولقد ساهم هؤلاء القراصنة الهواة في الكشف عن الفجوات الأمنية للأنظمة المعلوماتية في المؤسسات المالية وغيرها، وحسبنا فهو الأمر الذي ساعد في تطوير نظم الأمن ضد الاختراقات الأمنية.

القراصنة المحترفون: وهم أشخاص يقومون بالتسلل في نظم المعالجة الآلية للإطلاع على المعلومات المخزنة فيها لإلحاق الضرر أو العبث بها أو سرقتها وذلك بدافع التحدي الإبداعي.

39 : نهلا المومني عبد القادر، مرجع سابق، ص82

40 : خرق استشاريو تقنية المعلومات أحد الانظمة الامنية لشبكة الانترنت البريطانية لمجرد كشف الفجوات الامنية بها وقد نجح في الحصول على اسماء لأكثر من 24 الف شخص وعناوينهم وكلمات السر ومعلومات البطاقات الائتمانية من بينهم خبراء عسكريون وموظفون حكوميون وكبار مديري الشركات . أنظر نهلا المومني عبد القادر، نفس المرجع، ص 83

41: نهلا المومني عبد القادر، نفس المرجع، ص 84

وقد أجريت دراسة قام بها معهد stand ford reseache الامريكي، أن محترفي الجرائم المعلوماتية هم من الجيل الحديث من الشباب الذين تتراوح اعمارهم من 25–45 سنة، وهي المرحلة الزمنية التي تتناسب مع تعميم تقنية المعلومات[42].

وجاءت نتائج الإحصاءات التي اجريت في هذا الصدد بعدة ملاحظات تتمثل في الآتي[43]:

25% من أفعال الغش المعلوماتي يرتكبها المحلل .

18% من هذه الافعال يرتكبها المبرمج.

17% من هذه الافعال يرتكبها المستخدم الذي لديه أفكار خاصة بنظم المعلومات.

16% من هذه الافعال يرتكبها الصراف.

12% من هذه الافعال يرتكبها شخص غريب عن المنشأة المجني عليها.

11% من هذه الفئة يرتكبها المشغل operateur.

وتعكس اعتداءات هذه الفئة ميولات إجرامية خطرة تنبئ عن رغبتها في احداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يلحقون أضراراً كبيرة بمستعملي الاجهزة [44].

الفرع الثالث: المتطرفون الفكريون:

وهم طائفة من الناس نزلت بهم عقولهم إلى سوء التفكير، متطرفون لأفكارهم وآرائهم ومتجاوزون بذلك كل الحدود المعقولة والمقبولة للحوار والنقاش، وهم في سبيل تحقيق ما يعتقدونه صحيحاً على استعداد لارتكاب أنشطة إجرامية مخلفة وراءها أضرار جسيمة سواء بأفراد المجتمع أو بقطاعات كاملة منه [45]، هادفين من ذلك إلى تحول المجتمع إلى الأفضل من وجهة نظرهم.

وتتألف هذه الفئة من الجماعات الإرهابية أو المتطرفة التي لديها أفكاراً ومعتقدات اجتماعية أو سياسية أو دينية نشاطها الأساسي فرض هذه الافكار أو المعتقدات بأي وسيلة كانت [46].

42 : محمد سامي الشوا ، مرجع سابق، ص 42

43 : محمد سامي الشوا ، مرجع سابق، ص 43

عمر عبد الفتوح الحمامي ، مرجع سابق، ص 88

44 : نهلا المومني عبد القادر، مرجع سابق، ص 84

45: ظهر بوضوح في القرن السابع عشر التطرف الفكري ضد الثورة التكنولوجية وذلك حينما قامت مجموعة من المتظاهرين في عام 1811 بتحطيم الآت النسيج الخاصة بمصانع nottinggam مناهضين لفكرة إحلال الألة محل الإنسان وتخفيف أجورهم. أنظر عمر عبد الفتوح الحمامي ، مرجع سابق، ص 19

46: نهلا المومني عبد القادر، المرجع السابق، ص 86

وبدأ اهتمام هذه الجماعات وخاصة تلك التي تتمتع بدرجة عالية من التنظيم بالنشاط الإجرامي المعلوماتي، وعلى ذلك اختلف المجرم المعلوماتي العادي عن المجرم المعلوماتي المتطرف، فالأول لا يبغي سوى تحقيق منفعته الشخصية ، أما الثاني فتحركه بواعث أخرى سبق الإشارة لها.

ويتجسد هذا التطرف الفكري اليوم في ما يعرف بصراع الحضارات، حيث أطلق بعض المتطرفين والمتشددين الخلاف إلى الوراء بالزج بالدين إلى حلبة الصراع، فقد ادعى بعضهم بأفضلية أحد الأديان عن الأديان الأخرى من حيث المساهمة في التقدم الحضاري الذي وصلت إليه البشرية ومن الطبيعي أن يكون لهذه الادعاءات صدى لدى اتباع هذه الديانة الذي قد ينعكس سلباً لدى اتباع الدين المفترى عليه [47].

وتوجد جماعة دينية متطرفة تسمى blak hebrew والتي إرتكبت مجموعة من أعمال النصب بواسطة بطاقة الائتمان كما مارست عمليات أخرى مشبوهة في مجال الكومبيوتر.

ويمكن أن نشير أيضا إلى منظمة الألوية الحمراء الإيطالية [48] les brigades rouges التي استهدفت نظم المعلومات في الكثير من الهيئات، ومن ذلك اعتدائها على مكتب المرور الرئيسي في إيطاليا منذ بضعة سنوات مما أدى إلى أضرار جسيمة دمرت معظم المعلومات الخاصة باللوحات المعدنية ورخص القيادة بما فيها النسخ الاحتياطية، وظل الإيطاليون لمدة عامين متتاليين لم يكن لديهم أي مستند يثبت ملكيتهم لسيارتهم، كما تعرضت وزارات وجامعات ومؤسسات مالية لهجمات الألوية الحمراء، وكذلك الشركات المتعددة الجنسية، باعتبارها تجسيداً للإمبريالية في العالم، فكانت الجريمة المعلوماتية بصفة عامة تعبر عن فكر هذه المنظمة تجاه صراع الطبقات.

وقد أصدرت منظمة الألوية الحمراء في فبراير عام 1998 منشورا شرحت فيه استراتجيتها وأهدافها في الهجوم على النظم المعلوماتية، وهذا المنشور له أهمية خاصة لكل القائمين على أمن نظم المعلومات.

ولقد أظهر أفراد هذه الفئة من المجرمين أن لديهم اتجاه إجرامي خطير وذو نية بالغة السوء، وذلك لأنهم لا يبالون بالأضرار الجسيمة التي أصابت الأفراد أو المجتمع أو بعض قطاعاته.

الفرع الرابع: مجرمو المعلوماتية في إطار الجريمة المنظمة

رغم عدم دخول الجريمة المنظمة [49] عالم الإجرام المعلوماتي بشكل كبير عن الآن إلا أنه من المتوقع دخولها هذا المجال على نحو واسع وذلك لارتفاع عائد الجريمة المعلوماتية، ورغبة منها في اقتصار نشاطها على

47: عمر عبد الفتوح الحمامي ، مرجع سابق، ص 9

48: منظمة الألوية الحمراء هي جماعة ارهابية من أنصار الثورة اليسارية في ايطاليا والتي تعتقد أن إدخال نظام المعالجة الآلية للمعلومات هي عبارة عن خطة من الغرب يستطيع من خلالها متخصصين التغلغل في المؤسسات الاساسية في الدولة،

49: الجريمة المنظمة هي تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويفسر بين طياته آلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظام التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها لأحـــــكام قانونية =بنوها لأنفسهم وتفرض أحكاما بالغة القسوة على من يخرج عن قاموس الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من وراءها الأموال الطائلة. انظر في ذلك نهلا عبد القادر المومني ، مرجع سابق، ص 87

الجرائم التقليدية مثل المخدرات والسطو وغيرها، ويطلق على هذا الإجرام المنظم الحديث أحيانا إجرام ذوي الياقات البيضاء الذي يعبر عن حالة الطمع والجشع لدى مرتكبي هذه الأفعال.

سعى هذه المنظمات إلى الاستفادة من أجهزة التقنية الحديثة الممثلة في جهاز الحاسوب وشبكة الانترنت لتسوية اعمالها وتسهيل تنفيذها، فهي تعمل على تجنيد الكفاءات في هذا المجال أو تدريب عناصرها على احتراف التعامل مع التكنولوجيا الحديثة وتطويعها لأجل تحقيق مآربها.

ونستطيع القول بأن هناك عدة أهداف مقصودة من هذا الإجرام منها تحقيق كسب معين للجاني قد يكون كسب مالي كاختلاس أموال وقد يكون الهدف إلحاق خسائر بالمجني عليه وهذه الخسائر هي في ذات الوقت تعني كسب للمجرم المعلوماتي في هذه الفئة، كالحصول على حصة معينة في إحدى الصفقات أو الوصول إلى ملفات الزبائن أو إلى عروض تجارية وأسرار أخرى من أي طبيعة كانت تعود في النهاية بنفع على المجني عليه [50].

وفي الغالب فإن ضحايا الإجرام المعلوماتي هي الهيئات والمؤسسات الحائزة للأموال كالبنوك وشركات التأمين وغيرها من المؤسسات المالية، وفي هذا إشارة إلى أن الجريمة المنظمة ستأخذ أهمية أكبر في إطار الإجرام المعلوماتي، طالما أن اختلاس الاموال بطريقة الكترونية يعتبر أقل خطورة من السطو على البنوك .

المبحث الثالث

الحماية الجنائية للمعلومات الالكترونية

لقد أصبحت الحاجة ملحة لحماية المعلومات الالكترونية من كل اشكال الإجرام التي قد تلحقها، مرجعين ذلك للتطور غير المسبوق في مجالات الاعلام والاتصال وتوغل وسائل التكنولوجيا والابتكارات المستحدثة في الانشطة المعلوماتية ودخولها في جميع نواحي الحياة ، الأمر الذي جعل العالم يلجأ إلى ضرورة تطبيق الحكومة الالكترونية[51] والذي قد يكون الوسيلة الأفضل للاستخدام التكاملي الفعال بجميع تقنيات المعلومات والاتصالات لتسهيل وتسريع التعاملات بدقة عالية داخل الجهات الحكومية [52].

وعلى غرار دول العالم تعمل الحكومات العربية على تعزيز هذه التقنية لمواجهة الخطر الأكبر والذي يتمثل في استهداف الجرائم محل الدراسة، الأمن القومي، كما أن لجوء الاقتصاد الحديث لما يعرف بالاقتصاد الرقمي جعله أكثر عرضة لهذه الجرائم، عن طريق الاعتداء على الاموال إلكترونيا والمتداولة في التجارة الالكترونية أو غيرها.

50 : عمر عبد الفتوح الحمامي ، مرجع سابق، ص 103

51 : الحقوق الإلكترونية هي النسخة الافتراضية عن الحكومة الحقيقية، مع بيان أن الحكومة الالكترونية تعيش محفوظة في الخوادم(السيرفر) الخاصة بمراكز حفظ البيانات data center للشبكة العالمية للانترنت وتحاكي أعمال الحكومة التقليدية والتي تتواجد بشكل حقيقي ومادي في أجهزة الدولة : انظر الحكومة الالكترونية، مقال منشور على الموقع :/http://ar.wikipedia.org

52 : رشيدة بوكر، المرجع السابق، ص 136

ولهذا فإن قصور التشريعات العقابية التقليدية في توفير الحماية من جرائم الاعتداء على المعلومات الالكترونية، تدعو بصورة جدية إلى وجود قوانين جديدة قادرة على التكيف مع طبيعة هذه الجرائم، ولعل أبرزها التوجه نحو الحكومة الالكترونية المطلب الأول.

المطلب الأول

التوجه نحو الحكومة الالكترونية

إن مفهوم الحكومة الالكترونية وما ستحققه من تيسير للإجراءات الرسمية وتذليل الصعوبات التي يواجهها المواطن، هي وبلا شك الهدف الاساسي من تطبيق هذا المفهوم والاعتماد على تقنيات الحاسوب وشبكات الاتصال، إذ هي الوسيلة الأنجع لتقديم الخدمات بشكل أكثر تطورا بعيدا عن البيروقراطية والإجراءات الروتينية، وقد كانت مصر بإنشائها مركز المعلومات واتخاذ القرار عام 1985 والإمارات العربية المتحدة سنة 2001 بإطلاق اول الخدمات الالكترونية والأردن من أوائل الدول التي بعثت الشرارة الأولى في سبيل إنشاء حكومة الكترونية تعتمد على التقنيات المعلوماتية [53] ، ولم تكن الجزائر بمنأى عن هذا التطور الحاصل في البيئة العربية، فقد عملت على تبني مشروع يدعم هذا الطرح والمتمثل في برنامج الجزائر الالكترونية 2013.

الفرع الأول : مفهوم الحكومة الالكترونية:

أصبحت الحكومة الالكترونية تتواجد في كثير من الدول، وإن لم تكتمل صورتها النهائية بعد، نظراً لحاجتها لجهود مضنية، وأجهزة متطورة، وأنظمة ذكية بصفة مستمرة.

ويقصد بالحكومة الالكترونية استخدام تكنولوجيا المعلومات الرقمية في إنجاز المعاملات الإدارية وتقديم الخدمات المرفقية، والتواصل مع المواطنين بمزيد من الديمقراطية، ويطلق عليها احيانا حكومة عصر المعلومات أو الادارة بغير أوراق أو الادارة الالكترونية، وهذا هو التعبير الادق [54].

كما عرفتها الامم المتحدة على انها " استخدام الانترنت والشبكة العالمية العريضة لتقديم معلومات وخدمات الحكومة للمواطنين" وعرفتها منظمة التعاون الاقتصادي والتنمية عام 2001 على أنها " استخدام تكنولوجيا المعلومات والاتصالات وخصوصا الانترنت للوصول إلى حكومات أفضل" [55].

53 : نهلا عبد القادر المومني ، مرجع سابق، ص 60

54 : ماجد راغب الحلو: الحكومة الالكترونية والمرافق العامة، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، مركز البحوث والدراسات، العدد 4، تاريخ الانعقاد 26 أبريل 2003، دبي، الامارات .

55 : الحكومة الالكترونية، مقال منشور على الموقع : http://ar.wikipedia.org والذي أوردته : نهلا عبد القادر المومني ، مرجع سابق، ص 13

وقيل أيضا في تعريف الحكومة الالكترونية " أنها البيئة التي تتحقق فيها خدمات المواطنين واستعلاماتهم، وتحقق فيها الانشطة الحكومية للدائرة المعنية من دوائر الحكومة ذاتها أو فيما بين الدوائر المختلفة باستخدام شبكات المعلومات والاتصال عن بعد" [56].

يبنى على ما سبق أن نظام الحكومة الالكترونية يقوم على عدة أهداف تتمثل أساساً في رفع كفاءة الأداء بالجهاز الحكومي عن طريق توفير أحدث وأشمل المعلومات المطلوبة، مع تيسير الحصول على أي منها بعد تصنيفها الكترونيا، وكذلك تسهيل تبادل المعلومات وسبل الاتصالات الالكترونية بين الادارات المعنية[57].

كما انها تستهدف أداء الخدمات المرفقية للجمهور وللمستثمرين عن طريق شبكة المعلومات، دون الحاجة إلى التوجه إلى الإدارة المعنية، وتخدم بشكل فعال دور المواطن في ممارسة الديمقراطية الالكترونية في عملية اتخاذ القرار وتوجيه العمل العام عن طريق استعمال وسائل اتصال الكترونية كالبريد الالكتروني.

الفرع الثاني : مراحل الحكومة الالكترونية

يعتبر التطبيق الفوري للحكومة الالكترونية امراً عسيراً نوعاً ما، لحاجته إلى موارد مالية كبيرة، ووجود موارد بشرية ذات تأهيل عالي المستوى، وهذه العناصر تعد من مستلزمات بنية الحكومة الالكترونية لتشييد مجتمع معلوماتي تهتم بتحقيقه وإرساء أسسه جميع دول العالم.

ولقد كان التدرج في أسلوب تنفيذ هذا المشروع الرائد الوسيلة الأنجع، لضمان استمراريته على أرض الواقع، وتأديتها لوظائفها على أكمل وجه، وكذلك توعية المواطنين على هذه الفكرة بصورة تدريجية لتقبلها.

وأسلوب التنفيذ التدريجي يتم وفق اربع مراحل يبدأ بالتواجد[58] ، ثم التفاعل [59] ، ثم تنفيذ التعاملات الكترونيا وأخيراً مرحلة التحول النهائي. [60]

وتبقى الجزائر إلى حد الساعة تخط الخطى الأولى في تعزيز فكرة الانتقال إلى الحكومة الالكترونية، الأمر الذي اكده وزير البريد وتكنولوجيات الاتصال على هامش توقيع اتفاقية تعاون لتطبيق هذا المشروع في الجزائر عام 2013ما بين كل من شركة) ام بي سوفت (لخدمات الكومبيوتر والبرمجيات، ومؤسسة) هيومن بيرد (الكندية العاملة في حقل نشر وتطوير البرامج الالكترونية . [61]

56: مشار اليه : نهلا عبد القادر المومني ، مرجع سابق، ص 61

57 ماجد راغب الحلو، مرجع سابق.

58: تقوم الحكومة في هذه المرحلة باستخدام الحكومة الالكترونية لتوفير المعلومات والبيانات للمستخدمين من المواقع المختلفة للوزارات والوحدات الحكومية دون الحاجة إلى الذهاب الفعلي لتلك الوزارات والوحدات : أنظر المومني نهلا عبد القادر، المرجع السابق، ص 63

59 : يستطيع المواطن أو رجل الأعمال الاتصال المباشر عن طريق البريد الالكتروني : أنظر المومني نهلا عبد القادر، المرجع السابق، ص64

60: من أكثر مراحل الحكومة الالكترونية تعقيداً، حيث اتمام المعاملات المختلفة مع الوحدات الحكومية مباشرة من خلال المواقع الالكترونية للحكومة ووحداتها، بما في ذلك السداد الالكتروني للرسوم والمدفوعات المتنوعة: أنظر المومني نهلا عبد القادر، المرجع السابق، ص 64

61 : وهي آخر مراحل تنفيذ الحكومة الالكترونية إذ يصبح استخدام تقنية المعلومات والاتصالات في المعاملات ممارسة يومية عادية ومتوفرة في المناطق كلها.

ولعل أبرز المشاكل التي تواجه تحقيق هذا المشروع تظهر وبصورة جلية في مرحلة تنفيذ المعاملات الكترونيا الأمر الذي يتطلب تدخلاً تشريعياً جزائياً [62] لبسط الحماية على الأفراد والحكومة.

الفرع الثالث :متطلبات الحكومة الالكترونية

إن تطبيق نظام الحكومة الالكترونية الذي يتيح لطالب الخدمة أن يتعامل مع الانترنت بدلاً من الموظف الحكومي التقليدي، وهذا يستلزم إحداث تغيرات كثيرة وواسعة تشمل نوعية العاملين، والأجهزة المستخدمة وطرق الأداء، وذلك لأن إدارة الخدمات التي تقدمها الحكومة الالكترونية عبر الانترنت لها خصوصياتها ومقوماتها التي تختلف عن الإدارة التقليدية وتكمن أهم مستلزمات الحكومة الالكترونية في المعطيات البشرية والإدارية.

ولعل أهمها وأخطرها هي المتطلبات التشريعية التي تعتبر محل الاهتمام كونها تشكل الإطار التنظيمي الوقائي الرادع الذي يحيط بكل متعلقات الحكومة الالكترونية .ويشكل غيابها خطورة بالغة تكمن في جعل الباب مفتوحاً للمتطفلين والقراصنة ومجرمي المعلوماتية بكل أطيافهم.

وقد أدركت بعض الدول أهمية الحكومة الالكترونية فأصدرت تشريعات متعددة لتحقيقها وجعلت التحول إليها أمراً اجبارياً لا اختياريا، وكان تطبيق ذلك في الولايات المتحدة الامريكية و أوروبا متزامنا مع حملة لتعديل التشريعات القانونية القائمة خاصة الجنائية منها في خطوة الهدف منها الحماية القانونية الشاملة لها وتخطى الثغرات التي قد يستفيد منها العابثون بأمن المعلومات وأنظمتها [63] بل أكثر من ذلك حين يصل الأمر إلى درجة التلاعب في الأرقام والبيانات خاصة في الجانب الاقتصادي والمالي كما هو الحال في حالات الدفع الالكتروني عبر بوابة الحكومة الالكترونية دون وجود امكانية لمعاقبتهم لعدم وجود نصوص قانونية تسمح بذلك.[64]

أما بالنسبة للجزائر فتشكل الحكومة الالكترونية أحد الأهداف الرئيسية لبرنامج الجزائر الالكترونية2013 ، إذ برغم تضاعف حجم خدمات المعلومات تبقى الوضعية الراهنة متميزة بتطور بسيط جدا للخدمات التفاعلية لاسيما من حيث الإجراءات الالكترونية لفائدة المواطنين والمؤسسات.

ولقد عملت الجزائر على إعداد مجموعة من القوانين ومشاريع القوانين الهامة لإرساء أسس البناء السليم لمشروع الحكومة الالكترونية لتحقيق التوافق بين المنظومة القانونية وهذه التحولات، ومن مظاهر ذلك إفراد القسم السابع من قانون العقوبات لجرائم الاعتداء على نظم المعالجة الآلية بموجب القانون رقم 15-04 المؤرخ في 10

63:الجرائم الالكترونية قد تنطلق من مناطق لا يوجد بها قوانين لمحاربة هذا النوع من الإجرام كان هذا أحد الدروس التي قدمها فيروس(بقة الحب) فبالرغم ان الفيروس انتشر في العالم أجمع وألحق بالمؤسسات خسائر تقدر بملايين الدولارات ، إلا أن مخبري مكتب التحقيقات الفيديرالية وبعد ان تمكنوا من تحديد هوية مرتكب الفعل وكان طالباً من الفلبين وجدوا أن ليس هناك قانون يحاكم من خلاله.

64 : نهلا عبد القادر المومني ، مرجع سابق، ص66

نوفمبر 2004 المعدل والمتمم لقانون العقوبات، والذي تم تعزيزه بموجب القانون رقم 04-09 سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

وفي الواقع فإن الحماية المتكاملة للمعلومات ونظم معالجتها من الجرائم التي تستهدفها تتطلب تشريعات [65] متناسقة يكمل بعضها بعضاً، وتشمل جوانب الحياة الالكترونية كلها[66] والتي أصبحت تغزو مجتمعنا، ولعل تحقيق مشروع الحكومة الالكترونية على أرض الواقع يستدعي التحضير العام والشامل من خلال التهيئة النفسية والاجتماعية والبنية التحتية للاتصالات وخلق فضاء يضم كل الشركاء من خاص وعام، للوصول إلى تحقيق مجتمع معلوماتي سليم الأسس ومضمون الحماية.

المطلب الثاني

القطاعات المستهدفة في مجال جرائم المعلوماتية

ساعدت سهولة استخدام البرمجيات وتطور الشبكات على تدفق المعلومات، وأتاحت فرصاً أكبر لدخول المستخدمين إلى أكبر قدر من المواقع والملفات ومصادر المعلومات في شتى بقاع العالم، وإن كان هذا من مميزات عصر تقنية المعلومات ، لما يتضمن من معلومات متنوعة ووسائل متعددة، فالإتاحة الحرة للمعلومات فتحت الأبواب أمام الجميع، ولم تفرق بين المستخدمين، مما جعلها لقمة سائغة للعدوان عليها.[67]

ورغم اختلاف المجالات والأنشطة والقطاعات التي تستخدم الحاسب الآلي وتعددها، فهي ليست بمنأى عن ظاهرة الإجرام المعلوماتي على وجه عام وعلى وجه الخصوص المؤسسات المالية وبخاصة قطاع البنوك[68] ويظهر ذلك بصورة أكثر وضوح خلال تحقيق أجرته مجلة ressources informatiques تبين فيه الاتي:

19% من أفعال الإجرام المعلوماتي تستهدف البنوك.

16% للإدارة.

10% للإنتاج الصناعي.

10% للمعلومات.

ثم يلي ذلك شركات التأمين والشركات الخاصة.[69]

65: - قانون جرائم تقنيات المعلومات في مصر لسنة 2018.
- القانون الاردني رقم 27 لسنة 2015 المتعلق بالجرائم الالكترونية.

66: رشيدة بوكر، المرجع السابق، ص 143

67: علي بن ضبيان الرشيدي، العدوان على البيئة المعلوماتية خطورته ومواجهته، مقال منشور على موقع :
http://www.pmi.pna.ps/wpmi/

68: يذكر بأنه في عام 1973 قام صراف بنك dine singar بنيورك باختلاس اكثر من 2 مليون دولار بواسطة حاسب الكتروني، وفي عام 1978 كلفت عملية احتيال إلكتروني لبنك security Pacific national 10.2 مليون دولار، وفي عام 1981 وقع بنك wells fauga ضحية احتيال معلوماتي قيمته 21.35 مليون دولار. أنظر: عمر ابو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 141.

ولقد أبرزت المؤشرات ازدياد الإجرام المعلوماتي خاصة في الدول التي تعتمد بشكل كبير على نظم تقنية المعلوماتية الأمر الذي يشكل تحديا كبير لمواجهة هكذا جرائم ومكافحتها، غير أن وضع رقم ثابت ومحدد لحجم الخسائر يعد من الصعوبة بما كان وهو ما يعبر عنه بالرقم الأسو د[70].

هذه العوامل ساعدت على نمو السوق السوداء للمعلومات بالتوازي مع السوق الشرعية للمعلومات، ذلك السوق الذي تتم فيه مقايضة وبيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقين والشرعيين، وعلى ذلك يرتبط هذا النوع من الجرائم بالجزء الأعظم للأنشطة الاقتصادية والاجتماعية للمجتمع [71] ويمكن تصوره بالنسبة للمعلومات الآتية:

المعلومات المالية والتجارية: حيث تمس هذه الظاهرة المركز الحسابي والإداري وتنقلات الأموال والاستثمارات، سواء في المنشآت العامة أو الخاصة، إضافة إلى استهدافها لمشروعات التصنيع والإنتاج والتجارة والتوزيع ومراكز البيع والقطاع الصناعي للإنتاج [72].

المعلومات الشخصية: والمقصود بها تلك المختزنة في ذاكرات الحاسبات الآلية وشركات التأمين ولدى المحاميين والمستشفيات وأقسام الشرطة والأحزاب والنقابات، وتهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية النقابية أو السياسية وغيرها[73].

المعلومات العسكرية: وتتمثل في أسرار الدولة والمشروعات النووية والتصنيع الحديث للأسلحة [74] ويبدوا أن هذه المعلومات الأخيرة هي الاكثر رواجاً في سوق المعلومات السوداء.

ولقد قدرت اضرار جرائم المعلوماتية في الولايات المتحدة الامريكية بحوالي 5 مليارات سنويا ، كما قدرت المباحث الفيدرالية الامريكية (FBI) أن تكلفة جرائم الاعتداء على المعلومات الالكترونية حوالي 600 الف دولار، كما سجل المكتب أن 5000 من الهياكل الأساسية للبنية التحتية أصيبت بهذا الإجرام

---

69 : في واقعة نصب قام بها بعض العاملين في احدى شركات التأمين الامريكية سببت خسائر للشركة بلغت مليون دولار والملفت للنظر في هذه الواقعة أن عملية نصب واحدة نتجت عنها هذه الخسائر الكبيرة. أنظر : نهلا عبد القادر المومني، مرجع سابق ، ص67.

70 : مدلول الرقم الأسود: يشير إلى عدم التبليغ عن جرائم المعلوماتية الأمر الذي من شأنه أن يخفي الرقم الحقيقي لها ويقلل الشعور بمخاطرها وهذا يؤدي بدوره إلى وجود نسبة كبيرة من هذه الجرائم لا يتحقق العلم بوجودها. انظر: نهلا عبد القادر المومني، مرجع سابق ، ص 69.

71 : عمر ابو الفتوح الحمامي، مرجع سابق ، ص 144.

72 : في دراسة اجراها المركز الامريكي لجرائم الحاسب الآلي تبين أن المشروعات التجارية تمثل المستهدف الأول للإجرام المعلوماتي بنسبة 37% ويعتبر الكسب المالي هو الباعث على الإجرام في نصف هذه الحالات . أنظر : عمر ابو الفتوح الحمامي، مرجع سابق ، ص 150

73: ومثال ذلك ما أعلنته شبكة الاخبار cnn تحت عنوان طالب يسطو على المعهد الذي يدرس به، جاء فيه أن سلطات ولاية تكساس تحقق مع طالب يدعى (فليب أوستن) قد سطا الكترونيا على المعهد الذي يدرس فيه حيث سرقة بيانات خاصة بالضمان الاجتماعي وكذلك بيانات شخصية ومعلومات خاصة عن حوالي 55 ألف طالب وعضو هيئة التدريس بالمعهد، وقد قرر الطالب أنه لم تكن لديه أية نوايا اجرامية وانه لم يكن يخطط في استخدام تلك البيانات في انشطة اجرامية. انظر: منير محمد الجنبهي ، ممدوح محمد الجنبهي ، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي ، الاسكندرية، سنة 2005، ص 18

74: يوسف المصري، مرجع سابق، ص 21

أما في فرنسا، فقد نشرت الجمعية الفرنسية لأمن المعلومات عام 1991 تقريراً تقدر من خلاله حجم الخسائر من جرائم الإجرام المعلوماتي، والذي وصل إلى 10.4 مليار فرنك فرنسي، وقد أرجعت حوالي 57% من هذه الخسائر إلى أفعال إجرامية وخاصة اتلاف المعلومات وإفشائها والاحتيال المعلوماتي [75].

والدول العربية لم تكن بمنأى عن جرائم الاعتداء على المعلومات الالكترونية والخسائر الاقتصادية التي تسببها و إن كانت خسائرها ليست بمقدار ما تتكبده الدول الغربية في هذا المجال. [76]

أما في الجزائر وباعتبار هذه الأخيرة هي بدورها تحتل جزءاً من الفضاء الالكتروني فهي كذلك معرضة لخطورة جرائم الاعتداء على المعلومات الالكترونية خاصة فيما يتعلق بالمؤسسات المالية والبنوك بالاستيلاء على الأرصدة والاطلاع عليها وتحويل الاموال ورغم ذلك فإن مؤشرات الإجرام المعلوماتي في الجزائر لا تزال غامضة لعدم وجود عمل جدي لإحصاء رسمي يحدد ولو بقدر ما نسبة هذه الجرائم وبالتالي تقدير خطورتها وإرساء مفاهيم محددة لها من اجل خلق الوعي بها لدى المجتمع المحلي، ولعل مرد ذلك يرجع إلى حداثة الثورة التقنية بالجزائر والتي لا تزال بعد في بداياتها.

خاتمة

استتبعت المعلوماتية كظاهرة تكنولوجية حديثة ، ظهور مجرمين يختلفون عن نظرائهم مرتكبي الجرائم العادية، أطلق عليهم الفقه مجرمي المعلوماتية ،الذين يرتكبون جرائمهم باستخدام الأساليب التكنولوجية التي استحدثتها المعلوماتية، ولا يميلون للعنف المادي في ارتكاب جرائمهم، بل يستخدمون ما يطلق عليه تقنيات التدمير الناعمة، ويلاحظ في هؤلاء المجرمين أنهم يتمتعون بقسط وافر من الذكاء الذي يعكس في الوقت ذاته قدرتهم على التكيف الاجتماعي مع المجتمع، وهو ما يعكس في بعض الأحوال خطورة كامنة في نفوس هؤلاء المجرمون ذو أنماط متعددة، منهم صغار نوابغ المعلوماتية، ومنهم محترفو الجرائم المعلوماتية، ومنهم المخربون المعلوماتيون، ونصوص نظم المعلومات ، والمتطرفون الفكريون، والجريمة المنظمة ،بل وحتى منهم الحكومات الأجنبية ، وإذا كان هناك اختلاف في الأساليب المستخدمة في ارتكاب الجرائم المعلوماتية عن أساليب ارتكاب الجرائم العادية، فمن المنطقي أن تتباين الأسباب الدافعة لارتكاب الجرائم المعلوماتية، فقد يكون السعي لتحقيق الثراء ، أو الشغف بالإلكترونيات، أو مجرد إظهار دافع التفوق على الآلة ، وقد نعزي الأسباب إلى دوافع شخصية ومؤثرات خارجية ، وقد تكون دوافع شخصية ومؤثرات خارجية، وقد تكون الدوافع وراء ارتكاب الجريمة أسباب نابعة من المنشآت المجني عليها.

75 : رشيدة بوكر، مرجع سابق، ص 142

76 : تم اعتقال شخص بريطاني يبلغ من العمر 32 عاما يعمل مهندسا في إحدى شركات المقاولة في دبي بعد اتهامه أنه أحد أعضاء جماعة كانت وراء محاولة تخريب شبكة الانترنت الاماراتية وقدرت خسائر الفترة التخريبية والتي استمرت حوالي اسبوعين بملايين الدراهم وشلت قدرة الاف المستخدمين على البقاء في الشبكة. أنظر : نهلا عبد القادر المومني، مرجع سابق ، ص 71

إن المستهدف الأول للجريمة المعلوماتية هو المؤسسات المالية من بنوك وشركات تأمين وخلافه، ثم يأتي بعدها المعلومات، ومن العجيب أن المؤسسات المجني عليها تفضل التكتم والسرية عندما يقع بها أو عليها الجرم، بحجة الحفاظ على هيبتها وسمعتها المالية والتجارية، الأمر الذي زاد من معدل هذه الجرائم وبالتالي زادت حجم الخسائر الناشئة عنها ، بمبالغ تجاوزت ألاف الملايين من الدولارات في الدول التكنولوجية الكبرى أمثال الولايات المتحدة و انجلترا و فرنسا، وكذلك يمكن القول بأن معدل الجرائم المعلوماتية في الجزائر قد زاد وبالتبعية زادت الخسائر الناشئة عنها ، وحتى في حالة التبليغ من جانب المجني عليهم عن الجرائم المعلوماتية، فإن المشكلة تتأتى في هذا المقام من صعوبة إثبات الجريمة المعلوماتية، لأنها ليس لها آثار خارجية مادية ، كما أن الأساليب المستخدمة في ارتكابها وإخفاء أثرها أيضا على درجة عالية من التطور.

قائمة المراجع

الكتب العامة والمتخصصة

1- داود حسن طاهر، جرائم نظم المعلومات، الطبعة الأولى، مركز الدراسات والابحاث ، الرياض، سنة 2000.

2- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، الطبعة الأولى، دار المستقبل للنشر والتوزيع، عمان، سنة 2009.

3- عمر ابو الفتوح حمامي، الحماية الجنائية للمعلومات، دار النهضة العربية، القاهرة، سنة 2010

4- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، طبعة 2010.

5- القهوجي علي عبد القادر، الحماية الجنائية لبرامج الحاسب الآلي، طبعة أولى، الدار الجامعية، بيروت، سنة 1999.

6- ريم جعفر الشريمي، هوية المجرم المعلوماتي، مقال منشور على موقع مركز التميز لامن المعلومات.

7- نهلا عبد القادر المومني ، الجرائم المعلوماتية، الطبعة الأولى، دار القافة للنشر والتوزيع ، عمان، 2008

8- منير محمد الجنبهي ، ممدوح محمد الجنبهي ، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي ،الطبعة الثانية، الاسكندرية، سنة 2005.

9- يوسف أمير فرج، الجريمة الالكترونية والمعلوماتية والجهود الدولية لمكافحتها، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، سنة 2011

مراجع أجنبية

.Tom foreste, high tech society, third printing, combridge, 1990

david thomson, current trends in cumputer crime, computer control quarterly, vol 9 n°1,

الرسائل والمذكرات

1- خالد بوكشير، الجريمة المعلوماتية، مذكرة نهاية التدريب، المنظمة الجهوية للمحاميين ناحية سطيف، 2006-2005

الدوريات والمجلات

1- جمال فؤاد، بحث حول الجرائم المعلوماتية ،منشور على الموقع:
http://www.shaimaaatalla.com/vb/showthread.php?t=3160

2- علي بن ضبيان الرشدي، العدوان على البيئة المعلوماتية خطورته ومواجهته، مقال منشور على موقع :
http://www.pmi.pna.ps/wpmi

النصوص القانونية

1- قانون العقوبات الجزائري لسنة 2016

2- القانون رقم 09-04 سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها