ISSN : 2543-3938 - EISSN : 2602-7771

إشكالية العوالم الافتراضية المظلمة على شبكة الأنترنيت: قراءة إعلامية نقدية للجرائم السيبرانية الفكرية والثقافية على شبكة الويب العالمية

Problematic dark virtual worlds on the Internet: Critical Media Reading of Intellectual and Cultural Cybercrime on the World Wide Web

مريم قويدر

جامعة الجزائر3 (الجزائر)

kouider.meryem@univ-alger3.dz

تاريخ الإستلام: 2024/01/09 تاريخ القبول: 2024/06/13 تاريخ النشر: 2024/06/21

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على العوالم الافتراضية المظلمة للشبكة العنكبوتية العالمية، والتي سنركز فيها على الجرائم السيبرانية المعلوماتية الفكرية والثقافية ، إضافة إلى البحث في الأسباب الفردية والمجتمعية والكونية الكامنة وراء ارتكاب هذه الجرائمعلى الواقع الافتراضيوأهم أنواع وتصنيفات الجرائم السيبرانية عليها، وأهم ما توصلت له الدراسة أن القوانين والتشريعات وحتى البحوث العلمية تعتبر عاملا أساسيا في مواجهة الجريمة المعلوماتية، بالإضافة إلى زيادة الخبرة لدى العاملين في قطاع أمن المعلومات والهوية الرقمية، وتفعيل الجهات الوصية من الجانب المدني والتعليمي في المؤسسات للقيام بالتوعية والوقاية لمثل هذه الجرائم الإلكترونية التي تمس بخصوصية وأمن الأفراد والمجتمعات والمنظمات على حد سواء.

كلمات مفتاحية: العوالم الافتراضية، شبكة الأنترنيت ، الجرائم الإلكترونية، الجرائم السيبرانية، الجرائم الفكرية، الجرائم الثقافية.

Abstract:

This study aims to highlight the dark virtual worlds of the global spider web in which we will focus on intellectual and cultural cybercrime, as well as research into the individual, societal and cosmological causes behind the commission of such crimes on virtual reality and the most important types and classifications of cybercrime on them. and, most importantly, that laws, legislation and even scientific research are an essential factor in the face of information crime, In addition to increasing expertise in the information security and digital identity sector and the activation of civil and educational guardians in institutions to raise awareness and prevent such cybercrime affecting the privacy and security of individuals, communities and organizations alike.

Keywords: *Virtual worlds, Internet, cybercrime, cybercrime, intellectual crime, cultural crime.*

1. مقدمة:

لقد أحدثت الطفرة النوعية للتقنية والسهولة النسبية لاستعمال التكنولوجيات الحديثة سهولة أكبر وأسرع في الحصول على الأنترنيت، وهذا يرجع بطبيعة الحال إلى الأسعار المعقولة لاشتراكات الأنترنيت وسهولة الحصول على أجهزة الحواسيب مع أجهزة المودم الفائقة السرعة، كل هذا سهل للأفراد التواصل وتكوين العلاقات والصداقات الجديدة ووسع التجارة والتسلية والتعليم ومكن من القيام بالعديد من صفقات والأشغال التجارية وتسديد الفواتير والمستحقات عبر شبكة الأنترنيت، حيث كونت شبكة ويب العالمية ما يدعى بالعالم الافتراضي أو الفضاء الإلكتروني والذي يعرف على أنه مكان غير محدد بآجال معينة وأماكن محددة يتفاعل فيه مجموعة من الأفراد والمجتمعات لتكوين فضاء خاص بهم، مما أتاح للعديد من الأفراد الانتقال من العالم الحقيقي الواقعي إلى العالم الافتراضي الخيالي.(الشربجي، جوان2019، صفحة244)

ومن هذا المنطق الافتراضي الغير ملموس برزت تصنيفات أخرى للجرائم كما ظهرت أساليب مستحدثة لتنفيذ جرائم لم تكن معروفة في السابق، وبهذا فقد ظهر ما يسمى بالجرائم المستحدثة أو الجرائم السيبرانية Cyber Crimes، وأصبحت هذه الظاهرة هاجسا يؤرق ويقلق معظم بلدان العالم نظرا لتسارع تطورها وانتشارها عبر كافة الدول وبشكل يدعو للقلق والريبة لما لها من آثار عكسية وخيمة على الأفراد والمجتمعات على حد سواء، ومن أهم هذه الجرائم المستحدثة جرائم الأنترنيت التي نذكر أهمها: سرقة محتويات الخوادم الرئيسية للشركات والمؤسسات والمنظمات، وسرقة حسابات البنوك عبر الأنترنيت، جرائم التهديد والابتزاز، جرائم القرصنة، الاختراقات الأمنية للشبكات، احتيال وسرقة البيانات، هجمات الفيروسات المتنوعة، جرائم تكنولوجيا المعلومات الأخرى.(المزاهرة،2014، صفحة373)

حيث يمكن القول إن الجريمة السيبرانية الإلكترونية نوعان الأول هو الجرائم التي تستهدف جهاز الحاسوب الإلكتروني أو أنظمة تقنية المعلومات والاتصالات الأخرى بقصد اتلافها أو تدميرها أو تعطيلها أو إحداث خلل فيها، والنوع الثاني الجرائم التي يكون فيه الحاسب الآلي أو الكمبيوتر وسيلة ارتكاب جرائم الاحتيال وسرقة الهويات وبطاقات الائتمان والأرصدة المالية والتزوير والاختلاس وسرقة حقوق الملكية الفكرية والأصول الفكرية والابتزاز والسلوك الانحرافي والاستغلال الجنسي للأطفال عن طريق الابتزاز والتهديد. (والدراسات، 2016، صفحة09)

أما النوع الثاني من هذه الجرائم الإلكترونية فهو الذي يعتبر محل تسليط الضوء في دراستنا هذه، بحيث سنتطرق بالدراسة والتفسير والتحليل والتعقيب إلى كل ما تعلق بالجرائم السيبرانية الفكرية والثقافية في العوالم الافتراضية المظلمة والغامضة على الشبكة العنكبوتية العالمية، والتي تخص كل ما تعلق بالأشخاص أو المنظمات ويشمل ذلك بث الأفكار الهدامة والمنحرفة وعرض المواد الإباحية الفاضحة والاحتيال والابتزاز والتزوير وانتهاك الحقوق الخاصةوالاستلاب الثقافي والتأثير على القيم الدينية والأخلاقية للمجتمع العربي الإسلامي، وهو ما يتسبب في مشاكل قانونية واجتماعيةواقتصادية وأمنية معقدة وأخلاقية وعقائدية مما يستدعي بالضرورة إصدار قوانين خاصة بالجريمة الإلكترونية تتماشى مع خصوصياتها الافتراضية وتضمن أمن المعلومات الإلكترونية داخل إدارة المنظمات وخارجها وحتى حقوق الأفراد والمجتمعات ككل، ومن هذا المنطق وتأسيسا على ما تقدم تكمن إشكالية دراستنا في تناول: ما هي إشكالية الجرائم السيبرانية الفكرية والثقافية في العوالم الافتراضية المظلمة على الشبكة العنكبوتية العالمية "الأنترنيت"؟

فرضيات الدراسة:

- الارتفاع الكبير والمتلاحق في أعداد مستخدمي الأنترنيت وازدياد المعدل القياسي لنقل المعلومات يؤدي إلى ارتفاع معدلات الجريمة الإلكترونية الافتراضية وتعدد أشكالها وأنماطه.
- عزز غياب القوانين والأنظمة الإلكترونية الخاصة بتسيير شبكة الأنترنيت عبر العالم إلى إضعاف جهاز المناعة الذاتية ضد الجرائم السيبرانية والمعتمد على تقوية مؤسسات التنشئة الاجتماعية.
- أدى تطور تكنولوجيا الاتصال والمعلومات إلى إنتاج سوق عالمية في مجال تكنولوجيا المعلومات والتي أصبح له دخل كبير ورأس مال يفوق أسواق الذهب والبترول، مما ساعد انتشار جرائم إلكترونية بدوافع مالية مادية محضة.
- يشكل واقع الوضع الاقتصادي والمالي والتجاري للدول العالم بيئة مغرية للجريمة الإلكترونية والأغراض غير المشروعة للاحتيال على شبكة الأنترنيت.
- تأكيد دور المراكز التقنية والآليات الأخرى الوطنية والإقليمية والدولية في إعداد البرامج التنفيذية وحماية الأمن السيبراني.
- يعتبر غياب الوازع الديني والأخلاق الدينية والعقائدية السبب الرئيسي في تفشي الجرائم السيبرانية في العالم الافتراضي وعدم وجود رادع داخلي إزاء هذه الأفعال الشنيعة التي تمس بتطور المجتمعات في عصرنا الحالي.

منهج الدراسة:

الدراسة التي بين أيدينا دراسة نظرية بحتة تستخدم المنهج الوصفي في تناول إشكالية تأثير العوالم الافتراضية المظلمة من جرائم إلكترونية سيبرانية في المجال الثقافي والجرائم الإلكترونية في المجال العلمي والمعرفي والجرائم الإلكترونية في مجال الفكري على الأفراد والمجتمعات والمنظمات، وذلك بوصف الظواهر الإجرامية السيبرانية على شبكة الأنترنيت وتأثيرها الكبير في الفساد الاجتماعي والاقتصادي والأخلاقي للمجتمعات.

أهداف الدراسة:

تتمثل أهداف الدراسة فيما يلي:

- توعية العامة والخاصة من المتعاملين مع عالم الأنترنيت وجمهور المستخدمين ومتفاعلين مع العوالم الافتراضية بالجوانب السلبية والخطيرة لشبكة الأنترنيت.
- تغطية معرفية شاملة لجرائم الأنترنيت الإلكترونية التي تخص الأفراد والمؤسسات والمنظمات.
- معرفة انعكاسات استخدام العوالم الافتراضية على الأفكار والمعتقدات والثقافة الرقمية والهوية الرقمية.
- تحديد الجرائم السيبرانية الثقافية والفكرية والبحثية التي تمس الأفراد والجماعات على حد سواء.
- انشاء أجيال أكثر نضجا وقدرة على التصدي للجوانب السلبية لعصر تكنولوجيا المعلومات والذكاء الاصطناعي.

2. التعريف الجـريمة الإلكترونيـة

تعرف الجريمة المعلوماتية أو الجريمة الإلكترونية أو الجريمة الرقمية على أنها كل نشاط سلبي غير قانوني يتعلق باستخدام تقنية الحوسبة أو الاستخدام التكنولوجيا الرقمية قصد تنفيذ الأعمال الإجرامية، أو ما تعلق بربط الاتصال بكيان معنوي أي الكمبيوتر دون وجه حق أو بنظام المعلومات العالمية (الأنترنيت)، أو الإبقاء عليه عند تحققه أو التأثير عليه بتعطيله أو إضعاف قدراته على آداء وظائفه بالنسخ أو التعديل بالإضافة أو الحذف الكلي أو الجزئي، أو بالمناقلة للخصائص الأساسية للبرامج أو مجرد النسخ أو الوصل إلى البرامج أو المعلومات المخزنة، أو الوصول إليها أثناء نقلها أو إرسالها أو الاتصال بها من غير وجه حق وبأي وسيلة إلكترونية كانت. (باسبعين، 2016، صفحة 71)

كما تعرف الجريمة بأنها أي سلوك أو تصرف سيئ متعمد يتسبب في إلحاق الضرر بالضحية أو يعرض الضحية إلى ضرر محتمل، أو ينتج عنه حصول الجاني أو محاولته الحصول على كسب (مادي، معنوي) أو فائدة لا يستحق الحصول عليها، فلكي نعرف جريمة نظم المعلومات يجب أن نضيف إلى هذا التعريف شرط أن تتضمن الجريمة إتلاف المعلومات وإساءة استخدامها، واشتراط أن يكون ذلك عن طريق استخدام نظم المعلومات، وبذلك يصبح تعريف جريمة نظم المعلومات على النحو التالي: "جريمة نظم المعلومات هي السلوك السيء المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها، مما يسبب أو يحاول التسبب إما بإلحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها". (المزاهرة، 2014، صفحة 374)

3. أسباب الجريمة الإلكترونية المعلوماتية في العالم الافتراضي

بما أن هذه الجرائم ما هي في حقيقتها إلا نبضات إلكترونية فإن هذا يشكل عقبة آداء أمام اكتشافها وأمام التعرف على مرتكبيها، ولكن هذا القول لا يمكن أن يؤخذ على اطلاقه أي أن هذا القول لا يعني أن بعض جرائم الحاسب الآلي لا يمكن أن يتم اكتشافها إذ بقدر ما تطورت وسائل الحاسب الآلي وأنظمته تطورت الوسائل التقنية لحمايته وحماية أنظمته من الاختراق والعبث بها ورصد الاعتداءات التي يتعرض وتتعرض لها أنظمة الحاسب الآلي.

وبصورة عامة فإن الأسباب التي تكمن وراء ذلك أي وراء كون جرائم الحاسب الآلي تعترض سبيل اكتشافها ثمة صعوبات تعود إلى جملة من الأسباب منها:(باسبعين، 2016، صفحة 71)

- قدرة الجاني على تدمير أدلة الإدانة الموجودة ضده.
- عدم تخلف الآثار المادية كما هو الأمر في الجرائم التقليدية.
- النشاط الإجرامي فيها لا يمكن رؤيته بالعين المجردة.
- قلة خبرات لدى السلطات المسؤولة عن ضبط الجرائم والتحقيق فيها.

ومما زاد من خطورة جرائم الحاسب الآلي هو أن هذه الجرائم أخذت طابعا دوليا حيث لم تعد مقتصرة على النطاق الوطني وذلك بسبب سهولة الاتصال بين دول العالم اليوم، حيث جعلت أنظمة المعلومات اليوم العالم قرية لا يعترف فيها بحدود لا طبيعية ولا سياسية، غير أن انسياب هذه المعلومات متجاوزة بذلك الحدود الدولية للدول تثير الكثير من المشاكل القانونية، فلا تقتصر ما يذهب البعض على مدى مشروعية هذه المعلومات وانسيابها ومنها ما يتعلق بشروط المعلومات التي يجوز بثها عن هذا الطريق، إن كان لا ينكر هذا الجانب بل أن لها مخاطر تتعلق بالمبادئ الراسخة في القانون الجنائي وعلى وجه الخصوص فيما يتعلق بمبدأ الإقليمية. (باسبعين، 2016، صفحة 72)

هناك عدد من الأسباب يمكن حصرها كأسباب للجريمة الإلكترونية على الفضاء الافتراضي لشبكة الأنترنيت منها ما يقع على المستوى الفردي أو الشخصي ومنها ما يقع على المستوى المجتمعي، كما أن أسباب الجريمة المعلوماتية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي، كوني)، فالجرائم التي يرتكبها الشاب أو الهاوي أو المراهق تختلف من حيث الأسباب عن جرائم الشخصيات المحترفة وذلك وفقا للهدف منها: سرقة معلومات أو التجارة بالمعلومات أو انتحال الشخصية.(البداينة، 2014، صفحة 9)

1.3 أسباب الجريمة الإلكترونية على المستوى الفردي

1.1.3 البحث عن التقدير Sake of Recognition

حيث نجد أن بعض الجرائم السيبرانية التي يفعلها بعض الشباب الطائش أو المراهقين بدافع المنافسة والتحدي وحب البروز أمام الآخرين واستعراض العضلات، والتي يتوقف عنها لاحقا بعد مرور سنوات العشرينات والدخول في مرحلة النضج، فيلجأ للبحث من خلالها عن كل من التقدير والمدح من قبل الآخرين، وذلك لاحترافيته في التحكم في الوسائط الرقمية على الشبكة وقدرته الكبيرة في الاستيلاء على حسابات الآخرين بكل سهولة وسرعة، مما يزيد من تقديره لذاته ورفع نسبة امتنانه لنفسه.

2.1.3 الفرصة Opportunity

قد فتحت التكنولوجيا الحديثة وشبكة الإنترنت أفقًا واسعًا لانتشار الجريمة الإلكترونية بأشكال غير مسبوقة، تلعب البيئة الرقمية وترتيباتها دورًا حاسمًا في تشجيع الظواهر الإجرامية وانحراف الأفراد عن قواعد السلوك الاجتماعي، حيث يُشكل الانحراف عن قواعد الامتثال فرصًا مستمرة على مدار الساعة وفي أي مكان وزمان حيث أن غياب الرقابة يعزز هذه الفرص، كما تُعزز فرص ارتكاب الجريمة الإلكترونية بشكل إضافي بسبب سهولة الوصول إلى المعلومات، حيث يُعد استهداف المحتوى الرقمي هدفًا مثيرًا للاهتمام من طرف المجرمين بسبب تحقيقه للعوائد المادية السريعة، كما تُوفر هذه الجرائم فرصة للربح المادي مع مخاطر قليلة واحتمالات ضئيلة للاكتشاف، حيث تعمل تقنيات الاتصال والمعلومات الحديثة جنبًا إلى جنب مع الانتشار المتزايد للإنترنت، فقد خلقت بيئة مثالية للمجرمين وسهلت تزايد حدة الجريمة، مما يجعل من التحديات الإلكترونية في تزايد والوقاية من جرائم الإنترنيت أمرًا ضروريًا حتميا لمواكبة هذا التطور(البداينة، 2014، صفحة 10)

3.1.3 ضبط الذات المنخفض Low self-control

يمكن أن يكون لضبط الذات تأثير كبير على أداء الأشخاص في مجموعة متنوعة من المؤسسات المجتمعية كالمدرسة والعمل والحياة الزوجية، فالأفراد الذين يفتقرون إلى ضبط الذات بشكل جيد هم ليس فقط عرضة للسلوكيات الغير ملائمة إنما غالبًا ما يواجهون فشلًا في النجاح في مختلف جوانب حياتهم سواء في المدرسة أو العمل أو حتى في العلاقات الزوجية أو العلاقات الاجتماعية، كما تشير الدراسات أيضا إلى أن الأفراد الذين يفتقرون إلى ضبط الذات ويظهرون استعدادًا منخفضًا لتحمل المخاطر وقد يتجهون نحو تحقيق مكاسب قصيرة الآجال، وهذا التوجه يمكن أن يؤثر على سلوكياتهم بشكل سلبي خاصة في ظل الوسائط الإلكترونية والإنترنت، حيث يمكن أن يسهم التفاعل مع هذه الوسائط في تسهيل أو تعزيز

السلوكيات المنحرفة، بالإضافة إلى ذلك فهم يتعرضون في الإنترنيت إلى نماذج "التعلم الإجرامية" وإلى تأثير الأقران الذين قد يكونون أكثر ميلاً للانخراط في عالم الجريمة السيبرانية. (البداينة، 2014، صفحة 12)

4.1.3 الضغوط العامة General Strain

ترى نظرية الضغوط العامة أن "انحراف السلوك" و"انتهاك القانون" ينشأ بدافع تأثيرات البنية الاجتماعية أو استجاباتها النفسية من قبل الأفراد للأحداث والظروف المحيطة، حيث تُعَدّ هذه العوامل مصدرًا للضغوط والاضطرابات خاصةً عندما يكون من الصعب على الأفراد تحقيق أهدافهم المقبولة اجتماعيًا، كما أن تلك القوى الاجتماعية تشكل ضغوطًا تظهر لا سيما عندما يعجز الفرد عن تحقيق هدفه بسبب عراقيل مختلفة، يُفهم الضغط هنا ليس فقط كالإحباط الذي ينشأ عندما يواجه الفرد عقبات في سبيل تحقيق هدفه، بل يشمل أيضًا المشاعر السلبية التي تظهر في سياقات اجتماعية متنوعة، بالإضافة إلى ذلك يُمكن أن تلعب العوامل الاجتماعية والاقتصادية دورًا حيويًا في زيادة حدوث الجريمة السيبرانية الإلكترونية على الواقع الافتراضي الذي يعتبر نتاج للواقع الحقيقي.

5.1.3 النشاط الروتيني Routine Activity

يمكن فهم زيادة ضحايا الجريمة الإلكترونية من خلال التغيرات في أنشطة الحياة اليومية للأفراد، فمع ظهور شبكة الإنترنت تغيرت طرق تواصل الناس وتفاعلهم في العلاقات الشخصية والتسلية والتجارة، وقد أتاحت تلك التغيرات في الأنشطة الروتينية مثل استخدام الإنترنت والمشاركة في شبكات التواصل الاجتماعي مثل الفايسبوك والبريد الإلكتروني والمواقع الإلكترونية الأخرى فرصًا للجناة المتحمسين لاستغلال هذا الفضاء الافتراضي لتوفره على أهداف نافعة وبسيطة ومربحة بدون أي مراقبة فعّالة وناجعة وبدون أي مقابل مادي، كما يرى الفيلسوف "كوهين" أنه من المرجح أن تحدث الجريمة الإلكترونية عندما تتلاقى ثلاثة عوامل أساسية: الجاني المتحفز Motivated Offender والهدف المناسب Suitable Targets وغياب الحراسة Absence Of Capable Guardians، وأنه من الضروري بشكل حتمي تواجد هذه العوامل الثلاثة من أجل حدوث الجريمة وعدم تواجد عنصر من هذه العوامل هو كافي لمنع حدوث الجريمة(مرعي، أوت2016)

2.3 أسباب الجريمة الإلكترونية على المستوى المجتمعي

1.2.3 التحضر Urbanization

إن التحضر أو ما يسمى بالحداثة يشكل إحدى العوامل الرئيسية التي تساهم في زيادة حالات الجريمة الإلكترونية بشكل عام، يعزى هذا التزايد إلى التوجه الكبير للترحال من المناطق الريفية النائية إلى المدن والمناطق الحضرية الكبيرة، فعادةً ما يكون الشباب الذين يهاجرون غير قادرين على تحمل التكاليف الباهظة للحياة الحضرية والتي تتطلب مهارات عالية في بعض الأحيان، ونتيجة لذلك يجد العديد من المهاجرين أنفسهم عاجزين عن تلبية احتياجات الحياة الحضرية ومتطلباتها، مما يدفعهم للعيش في مناطق هامشية مثل المدن الصفيحية والأحياء الطرفية أو القصديرية.

يتسبب هذا التنافس الشديد في جعل الأفراد يجدون صعوبة في مجاراة التحديات الاقتصادية، مما يدفع بعضهم إلى النظر إلى الجريمة السيبرانية كوسيلة لتحقيق دخل إضافي، وبالإضافة إلى ذلك يُعزى استثمار البعض في الجريمة تقنية المعلومات إلى توفرها على ميزة التكلفة البسيطة جدا في الاعتداء الرقمي وهو ما يُعرف بـ "أولا الياهو"، وفقًا لـ"ميك" يعتبر التحضر سببًا رئيسيًا للجرائم الشبكية في نيجيريا، حيث يرى أن التمدن بدون جريمة يكاد يكون مستحيلاً، ونتيجة لهذا التوجه يجد الأفراد في الطبقة الاجتماعية الراقية أن الاستثمار في مجال الجريمة المعلوماتية يعد أمرا مربحًا.(البداينة، 2014، صفحة 14)

2.2.3 البطالة Unemployment

ترتبط جرائم المعلومات في الإنترنيت بشكل كبير بمشكلة البطالة والظروف الاقتصادية المزرية مما يجعلها مشابهة للجريمة التقليدية، حيث تظهر البطالة بشكل خاص بين شرائح كبيرة من الشّبان والفتيان، وكما يوضح "المثل النيجيري" في هذا السياق معرجا على أن "العقل الخالي من أي عمل هو عبارة عن ورشة لنشاط الشيطان"، لذلك يتجه الشباب الذين يمتلكون المعرفة المعلوماتية نحو استغلال تلك المهارات في العمل الإجرامي السيبراني عبر شبكة الويب(مرعي، أوت2016)

3.2.3 الضغوط العام Public Pressures

تعتبر الظروف العامة التي يواجهها المجتمع مثل الفقر والبطالة والأمية والتحديات الاقتصادية الصعبة، والعوامل المضغوطة على مستوى المجتمع بشكل عام مصدرًا رئيسيا لضغوط كبيرة داخل المجتمع خاصة لدى فئة الشباب، مما ينجم عن هذه الضغوط مشاعر سلبية سيئة اتجاه الظروف والمجتمع بشكل عام لدى شرائح واسعة من الناس، وتؤدي هذه المشاعر إلى تبني أساليب تأقلم ضارة مثل الانخراط في الجرائم المعلوماتية كالمتاجرة بالأشخاص و ترويج للجنس وسرقة المعلومات والجريمة الشبكات الإلكترونية بشكل عام، بالإضافة إلى التورط في تجارة المخدرات وأنشطة غير قانونية أخرى على مواقع الشبكة العنكبوتية العالمية. (البداينة، 2014، صفحة 15)

4.2.3 البحث عن الثراء Quest for Wealth

تقول نظرية "لجتفردسون وهيرشي" أن الفرد يتجه نحو البحث عن المتعة ويحاول تجنب الألم، فهو يسعى إلى تحقيق أهدافه الاجتماعية باستخدام وسائل قد تكون غير مقبولة على المستوى الاجتماعي، وفي هذا السياق ترى نظرية "الأنومي لميرتون" أن الرغبة في الثراء تواجه عراقيل كبيرة في التحقيق عبر الوسائل الاجتماعية والقانونية المقبولة، ومن هنا يتجه بعض الأفراد نحو الجرائم الرقمية على الشبكة، حيث يجدون فيها فرصة لتحقيق أهدافهم بشكل أسرع وأسهل مستهدفين بذلك مجتمعًا أوسع ومستفيدين من سرعة العائد وقلة المخاطر وغياب الرقابة وانعدام القوانين.

5.2.3 ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية lack of law enforcement and implementation

تعاني العديد من الدول من عدم تطوير تشريعاتها وأجهزة العدالة بما يتناسب مع التطور المستمر في مجال الجرائم الإلكترونية وأساليبها، حيث يظهر هذا النقص ليس فقط في ميدان التشريعات بل يتسع ليشمل أيضًا الشرطة وعمليات التحقيق والقضاء، بالإضافة إلى كيفية التعامل مع الأدلة الرقمية على الصعيدين الوطني

والدولي، يُعزى اشتعال جريمة سيبرانية إلى فقدان التشريعات الجنائية والجزائية الملائمة، فضلاً عن ضعف الممارسات العدلية والشرطية والقضائية في معالجة وتحقيق الجرائم الرقمية على الشبكة، وفي كثير من الأحيان يكون هناك نقص في تبني التقنيات الحديثة، ونقص في توفير خبراء قادرين على متابعة ورصد ومكافحة الجريمة الإلكترونية داخل المجتمع، سواء داخل حدود الدولة أو خارجها كالجرائم السيبرانية العابرة للقارات والتي تمس أمن الدول.(مرعي، أوت2016)

3.3 أسباب الجريمة الإلكترونية على المستوى الكوني

1.3.3 التحول للمجتمع الرقميTransformation for Digital Society

دخلنا عصر المعلومات الجديد أي ما يسمى بالفضاء السيبراني أو البيئة الرقمية التفاعلية أو العالم الرقمي ثلاثي الأبعاد، حيث يخصص الأفراد جزءًا من حياتهم اليومية للتفاعل في هذا الفضاء الافتراضي، فهم يقومون بإنشاء شبكات اجتماعية ومواقع شخصية ويستمتعون بتكوين علاقات اجتماعية جديدة، بذلك يبقون على اتصال مباشر بأحداث العالم الخارجي إضافة إلى قيامهم ببعض الأعمال والمهام من خلال هذا الفضاء السيبراني، إذن كل هذه الأنشطة أفضت أهمية قصوى لوجود جهاز الحاسوب ومودم واستيعاب معتدل للتقنيات الحديثة من أجل الولوج إلى الفضاء السيبراني أو العالم الافتراضي.

إذن وببساطة فإن شبكة الإنترنيت هي التي خلقت ما نعرفه اليوم باسم الفضاء الرقمي الإلكتروني، وهو فضاء يستدعي من الأفراد أن يكونوا على تواصل مستمر مع أحداث العالم مع توفير وبشكل مهم كلاً من السلامة والأمان والاستقرار داخل هذا العالم الجديد، فالمجتمع بأسره بحاجة إلى تأمين وضمان استمراريته ليس فقط في الواقع المادي لكن ينبغي أن يكون هناك أمان واستقرار للمجتمع حتى في العالم الافتراضي الغير حقيقي ليتحقق النظام وتدوم سيرورة المجتمع ككل(Leukfeldt, 2013, pp. 1-17)

2.3.3 العولمةGlobalization

يعد ظهور "العالم الافتراضي" فرصة لخلق حوادث جديدة تختلف تماما عن وجود أنظمة الحواسيب ذاتها إذ يُعطي هذا الفضاء فرصًا جديدة ومباشرة للجريمة، إذ يمكن رؤية التباين الكبير في التزام الأفراد بالقوانين والأنظمة وعدم الامتثال لها في هذا السياق الرقمي مقارنة بتصرفاتهم في العالم الحقيقي، فعلى سبيل المثال قد يلجأ بعض الأفراد إلى ارتكاب جرائم في الفضاء الإلكتروني دون أن يفعلوا ذلك في الواقع الحقيقي وذلك نتيجة لظروفهم وموقعهم ومكانتهم الاجتماعية، بالإضافة إلى ذلك يُشجع العالم الافتراضي على السلوك الإجرامي نظرا لتزييف الهويات والشخصيات الحقيقية وغياب سبل ناجعة للكشف عنها، فضلاً عن ضعف الردع المتاح في هذا السياق الافتراضي الذي أصبح أرض خصبة للجرائم السيبرانية بكل أشكالها وأنواعها. (البداينة، 2014، صفحة 17)

3.3.3 الترابط الكونيUniversal Interdependence

يمكن أن يشكل ظهور الترابط العالمي في سياق تغيرات الاقتصاد والديموغرافيا عاملاً مساهماً في زيادة مستويات الجريمة، فوفقًا لتقرير صادر عن المركز الوطني لجرائم الياقات البيضاء يُتوقع أن يتضاعف عدد سكان المدن إلى 6.2 مليار بحلول سنة2050، ممثلاً70 في المائة من إجمالي سكان العالم والمتوقع أن يصل إلى 8.9 مليار نسمة، وقد أظهر ذات التقرير أن الإنترنت قد فتحت أبواباً جديدة لفرص الجريمة السيبرانية،

بحيث يُمكن للمجرمين التواصل مع المتضررين بشكل فعّال دون الكشف عن هوياتهم الرقمية، مستفيدين في ذلك من سهولة استخدام الأنترنيت وعدم كشف الهوية الافتراضية في هذا الفضاء الرقمي.

بالإضافة إلى ما سبق توفر شبكة الأنترنيت للمجرمين طرق فعالة وناجعة لنقل كميات هائلة من المعلومات بقدرة استيعاب عالية وسرعة فائقة، سواءً عبر غرف الدردشة أو البريد الإلكتروني أو لوحات الرسائل أو حتى مواقع الأنترنيت، ونتيجة لذلك يمكن لجهاز حاسوب واحد أن يُوفر وسائل متعددة لارتكاب مجموعة متنوعة من الجرائم السيبرانية وتنفيذ العديد من المعاملات المالية التي تدخل في سياق النصب والاحتيال الإلكتروني على العديد من الأشخاص خاصة الذين تقل خبرتهم في هذا المجال.(مرعي، أوت2016)

4.3.3 انكشاف البنية التحتية المعلوماتية الكونية Exposing Cosmic Information Infrastructure

تتباين هياكل البنى التحتية المعلوماتية في درجة تعرضها للكوارث الطبيعية والإهمال البشري وسوء التصرف الإنساني، حيث أشار التقرير الرئاسي الأمريكي الخاص بحماية "البنية التحتية الحساسة" إلى خمسة قطاعات تتشارك في خصائص محددة، وهذه القطاعات تشمل: "قطاع الاتصالات والمعلومات" و"قطاع التوزيع المادي الفيزيائي" و"قطاع الطاقة" وقطاع المال والبنوك" و"قطاع الخدمات الإنسانية الحيوية". (البداينة، 2014، صفحة 18)

4. أنواع الجرائم الإلكترونية

نظرا لانتشار الجريمة الإلكترونية بشكل كبير وواسع فقد تعددت أنواع هذه الجرائم وأهمها ما يلي:

1.4 الجريمة المادية Financial Crime

وهي التي تسبب أضرار مالية على الضحية أو المستهدف من عملية النصب وتأخذ واحدة من الأشكال الثلاثة التالية:

أ-عملية السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك كتلك المنتشرة الآن في الكثير من الدول، وبها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية.
ب-إنشاء صفحة أنترنيت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها.
ج-الرسائل البريدية الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي.(المزاهرة،2014، صفحة374)

2.4 الجريمة الثقافية Cultural Crime

هي استيلاء المجرم على الحقوق الفكرية ونسبتها له من دون موافقة الضحية ومن الممكن أن تكون على إحدى الصور التالية:
أ-قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على أسطوانات وبيعها للناس بسعر أقل.

ب-التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الأنترنيت من خلال تقنية Soft Cop.
ج-جريمة نسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية المستحدثة.

3.4 الجريمة السياسية والاقتصادية Political and Economic Crime

أ-تستخدم المجموعات الإرهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية، وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتحويل بعض الأموال في سبيل تحقيق أهدافهم، ففي الولايات المتحدة الأمريكية يقوم الإرهابيون باستخدام الأنترنيت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية.
ب-الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات، وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجانا.
ج-نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنا لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى.

4.4 الجريمة الجنسية Sexual Crime

هذا النوع من الجريمة يمكن أن يتمثل بإحدى الصور التالية:
أ-الابتزاز: من أشهر حوادث الابتزاز عندما يقوم أحد الشباب باختراق جهاز إحدى الفتيات أو الاستيلاء عليه وبه مجموعة من صورها، وإجبارها على الخروج معه وإلا سيفضحها بما يملكه من صور. (المزاهرة،2014، صفحة 375)
ب-التغرير والاستدراج: في العادة تتواجد هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات عبر الشات أو برامج المحادثة، ويكون علاقة معها ثم يستدرجها بالكلام المعسول ويوهمها بالزواج لكي تثق به، ومن ثم يقوم بتهديدها وفضحها بما يملكه من صور أو تسجيلات لصوتها إن لم تستجب لطلباته.(المزاهرة،2014، صفحة 376)

5. تصنيف جرائم تكنولوجيا المعلومات

يمكن تصنيف جرائم تكنولوجيا المعلومات إلى جرائم إلكترونية تستهدف النظام المعلوماتي وجرائم إلكترونية باستخدام النظام المعلوماتي وجرائم منفذة في بيئة النظام المعلوماتي وجرائم تمس بحقوق الملكية الفكرية، لكننا سنركز على جرائم تكنولوجيا المعلومات وأنظمة المعلومات التي تمس الجانب الفكري والثقافي والعلمي والمعلوماتي للأفراد والمؤسسات والأنظمة، مما يساعد على فهم سليم لتأثير الجرائم الإلكترونية على البيئة الرقمية والافتراضية في الحقل العلمي والثقافي والفكري، وبذلك يسهل علينا التحكم في المشكل أو الظاهرة المستحدثة في عالم الأنترنيت المظلم، ومن أهم هذه الجرائم الإلكترونية المعلوماتية في هذا السياق ما يلي:

1.5 صناعة ونشر الفيروسات

تعد الفيروسات من أخطر الجرائم الرقمية من حيث انتشارها وتأثيرها ولا يمكن إلقاء اللوم على الإنترنت كوحيدة المسبب، فقد كان لفكرة الفيروسات في عالم الحوسبة أصول تمتد إلى منتصف الأربعينات الميلادية مع فهم العالم الرياضي "فون نيومن"، لقد كانت الإنترنت تستخدم بشكل مختلف في الماضي ولكن في

السنوات الأخيرة أصبحت وسيلة فعالة لنشر الفيروسات وبرامج التدمير، يظهر ذلك بسرعة انتشار ما يعرف بـ "الدودة الحمراء" حيث تمكنت من اختراق ما يقرب من ربع مليون جهاز في غضون تسع ساعات فقط في 19 يونيو 2001،حيث يكمن هدف هذه الفيروسات في التلاعب بالمعلومات المخزنة على الأجهزة المصابة سواءً من خلال تغييرها أو حذفها أو حتى سرقتها ونقلها إلى أجهزة أخرى،إذ تتنوع أصناف الفيروسات التي تستهدف المعلومات بما في ذلك حصان طروادة وفيروس الدودة والقنبلة الموقوتة(الشرع، 2012، صفحة 333)

2.5 تخريب المعلومات وإساءة استخدامها

تتضمن جرائم نظم المعلومات جريمة تخريب المعلومات ويقصد بذلك الأذى الذي يقع على المعلومات مثل إتلافها أو تحويرها أو جعلها غير ذات فائدة (كتشفيرها باستخدام مفتاح مجهول مثلا)، كما تتضمن جرائم نظم المعلومات كذلك جريمة إساءة استخدام المعلومات، والمقصود بها الأذى الذي يتم تحقيقه باستخدام هذه المعلومات مثل عدم تمكين المستفيد من الوصول إليها أو كشفها أو استغلالها في إلحاق الضرر بمصالح صاحب المعلومات، وإلى جانب الضرر المباشر الذي تسببه هاتان الجريمتان، فهنالك أيضا الضرر غير المباشر الذي يلحق بالأشخاص أو الممتلكات أو حتى الخدمات التي تقدمها المؤسسات التي تقتني هذه المعلومات التي وقعت عليها الجريمة، ومهمة أمن المعلومات هنا هي منع الأضرار المباشرة وغير المباشرة معا، فنحن لا نعرف مسبقا بالضبط ماذا سيكون هدف المجرم فالحل هو الحماية ضد كل أنواع الضرر التي يمكن أن تلحق بالمعلومات.

وتعبر جريمة تخريب المعلومات من جرائم نظم المعلومات الخطيرة وتكمن خطورتها في آثارها البالغة السوء على الجهات التي تتعرض لها، فالتخريب يمكن أن يتم بمحو الملفات أو تدمير الوسائط التي تحتويها، ونود هنا أن نشير إلى وسيلة خطيرة لتخريب المعلومات وهي أن يقوم المجرم بتشفير هذه المعلومات والاحتفاظ بمفتاح الشفرة وعدم الكشف عنه، وتزداد فرصة حدوث هذه الجريمة كلما قل الانضباط بين الموظفين في الشركات والمؤسسات ولكما تراخت الرقابة على الموظفين الذين لديهم صلاحية التشفير، ويمكن أن تؤدي هذه الجريمة إلى أضرار هائلة للشركات. (المزاهرة،2014، صفحة 376)

3.5 سرقة المعلومات

تعد سرقة المعلومات أو البيانات النقل غير القانوني لمعلومات شخصية أو سرقة أو مالية يمكن لهذه المعلومات أن تشمل كلمات مرور أو كود برنامج أو خوارزميات أو عمليات أو تقنيات خاضعة لحقوق الملكية، حيث تعتبر سرقة البيانات انتهاكا كبيرا للأمان والخصوصية مع احتمالية وقوع عواقب وخيمة بالنسبة لكل من الأفراد والشركات، ففي عام 1992 ضبط لصوص المعلومات Information Thieves وهم يخترقون ملفات إدارة الأمن الاجتماعي Social Security Administration ويسرقون سجلات شخصية مهمة للغاية، ثم يقومون ببيع المعلومات التي يحصلون عليها، كما قام اللصوص أيضا بالتسلل إلى أجهزة الكمبيوتر لمكاتب الائتمان الرئيسية Credit Bureaus وقاموا بسرقة معلومات ائتمانية ثم استخدموا المعلومات ليدفعوا مقابل بعض المشتريات أو يقوموا بإعادة بيعها إلى أشخاص آخرين، وفي حرم بعض الجامعات استطاع اللصوص التطفل للاطلاع على درجات الطلاب أو سرقة هذه المعلومات الخاصة وبيعها للطلاب.(اللبان، 2012، الصفحات 119-120)

4.5 اختراق الأنظمة والحواسيب

تتمثل المشكلة في الوصول غير المصرح به إلى أجهزة الحاسوب أو شبكات الكمبيوتر، حيث يتم تنفيذ عمليات اختراق أو محاولات للاختراق باستخدام برامج متاحة على الإنترنت، حيث يمكن للأفراد ذوي الخبرة التقنية المتواضعة اللجوء إلى هذه البرامج لتنفيذ هجماتهم على أجهزة الآخرين وهنا يكمن مصدر الخطورة.

تختلف الأهداف المباشرة للاختراقات فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة، وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترق بعمليته بقصد إبراز قدراته الاختراقية أو لإثبات وجود ثغرات في الجهاز المخترق، ومن أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الأنترنيت، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع Defacing، إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة، وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة.(الشرع،2012، صفحة334)

وإذا كان الخواص من الأشخاص العاديين يتعرضون يوميا وبسهولة فائقة لهجومات ما أصبح يسمى بالهكرةHackers الذين لا يهمهم انتهاك خصوصية مستخدم الأنترنيت، فيتجولون في ملفاته ويفحصون قرصه الصلب لمجرد التطفل والمتعة وقضاء أوقات الفراغ، فإن أجهزة الأشخاص المهمين علميا، ثقافيا، اقتصاديا، سياسيا، وكذا أجهزة المؤسسات الحكومية والخاصة المدنية والعسكرية تخترق للتجسس عليها وكشف أسرارها وسرقة معلوماتها أو تعطيل عملها وتخريب ملفاتها أو حتى لمجرد رفع تحدي حمايتها معلوماتيا، ومن جهة أخرى فقد أوحت فاعلية هذه الاختراق إلى بعض شركات البرمجيات ومواقع الأنترنيت باتخاذ إجراءات هجومية ضد من يستخدم برامجها المقرصنة، ومن أهم هذه الشركات "شركة مايكروسوفت" و"شركة ياهو" اللتين هددتا بفحص القرص الصلب لزوار مواقع الأنترنيت بدون علمهم، وذلك بإضافة نصوص برمجية إلى مواقعها تفحص القرص الصلب لواحد من كل مائة زائر لهذه المواقع بحثا عن برامج مقرصنة، لكن الظاهر أن رد الفعل القوي لمنظمات حماية الخصوصية عبر شبكة الأنترنيت ضد هذه الإجراءات أدى إلى تراجع هذه الشركات عن استخدام أحد أسلحة أعدائها غير القانونية.(دليو، 2015، صفحة64)

5.5 النصب والاحتيال على المواقع الإلكترونية

أصبحت الإنترنت مجالًا شاسعًا للأفراد الذين يمتلكون سلعًا أو خدمات تجارية أو ثقافية أو فكرية ويرغبون في تقديمها أو نشرها بطرق غير مسبوقة، مثل استخدام البريد الإلكتروني أو عرضها على مواقع الويب أو من خلال منتديات الحوار، ومع ذلك من الطبيعي أن يتسبب هذا التفاعل الواسع في استغلال الوسائل الإلكترونية في عمليات احتيال ونصب على المستخدمين، كما قد يجد القارئ نفسه متعرضًا لرسائل بريد إلكتروني تحمل محتوى مشبوه حيث يتعرض الأفراد لأشكال متعددة من الاحتيال عبر الإنترنت، مثل بيع سلع وخدمات وهمية أو المشاركة في مشروعات استثمارية وهمية أو حتى سرقة معلومات بطاقات الائتمان واستخدامها بشكل غير قانوني، وتظهر عمليات النصب والاحتيال على شبكة الإنترنت بشكل واضح في المزادات العامة للسلع حيث يتميز هذا النوع من الاحتيال عبر الإنترنت بسرعة القرصنة والتمويه، وهي سمة تميزها عن الاحتيال في الحياة اليومية.

إنه من المهم أن نلاحظ أن أبرز الأسباب التي أدت إلى انتشار قضايا اختراق البرمجيات كما أشير إليها من قِبَل الشيخ والراشد والضراب وترافقان وتريفيث، تتمثل في التكلفة الباهظة لاقتناء البرامج أو الحصول على

نسخ مرخصة، يأتي ذلك في سياق تطور الإنترنت وشبكات الحواسيب بشكل هائل وتوفر مسجلات الأقراص المدمجة في أجهزة الحواسيب الشخصية، مما يُيسر عمليات نسخ وتوزيع البرمجيات بشكل مبسط ويسهل الحصول على نسخ بأسعار مخفضة، ويرجع سبب نجاح هذه الظاهرة إلى صعوبة اكتشاف مرتكبي هذه الجرائم ومقاضاتهم، حيث يكون في معظم الحالات غياب شاهد على الجريمة ونقص في الأدلة التي يمكن استخدامها لتحديد الجاني، كما تُعزى سلامة هذه الأسباب أيضًا إلى عدم وجود أنظمة وقوانين فعّالة للردع وضعف الوعي بأخطار هذه الجريمة وطرق ارتكابها وكيفية الحماية منها، وقد أكد "هيندوجا" أن توفير سهولة الوصول والاستخدام السريع للإنترنت في الجامعات كان له دور أساسي في تسارع انتشار هذه الظاهرة.(الشرع، 2012، صفحة 336)

6.5 القرصنة عبر شبكة الأنترنيت

هي الحصول على معلومات مخزنة في ذاكرة الكمبيوتر دون وجه حق قصد الاستعمال المباشر أو غير المباشر كالمحاكاة مثلا وهي تعتبر من أكثر الجرائم المعلوماتية انتشارا وتنوعا، مما أدى إلى نشوء عدد كبير من المنظمات المتخصصة في محاربة المحاكاة والقرصنة والتجسس بأنواعها بغية الدفاع عن حقوق التأليف والنشر الفكريين، لقد انتقلت المعركة بين الطرفين من مجال المطبوع السمعي البصري التقليدي إلى المجال المعلوماتي الحديث.

فبالرغم من الحواجز العديدة التي تضعها كبرى شركات البرمجيات كالمايكروسوفت ولوتس أمام قراصنة الكمبيوتر مما جعل نسبة قرصنة برمجيات الأعمال في العالم، مثلا يهبط إلى ما دون خط الأربعين في المائة فإن الأساليب الجديدة التي طورها قراصنة البرمجيات لتجاوز هذه الحواجز ستؤدي حتما إلى ازدياد معدلات القرصنة من جديد، وتنتشر الآن في الأنترنيت العشرات من مواقع القرصنة والتجسس والتي يصطلح على تسميتها في المجتمع الموازي للأنترنيت بمواقع Warez وهي تتضمن مختلف الأنواع من البرامج "الألعاب، نظم التشغيل، البرامج الخدمية، إلى غير ذلك والتي تجلب مجانا أو بأثمان بخسة بينما قد يقدر ثمنها في السوق بعشرات الآلاف من الدولارات.(دليو، 2015، الصفحات 57-58)

7.5 زعزعة عقيدة المسلمين وتشويه الدين

قامت إحدى المنظمات المشبوهة في سنوات التسعينات من خلال شبكة الأنترنيت بمحاولة لتشويه القرآن الكريم، حيث طالبت هذه المنظمة من زوار موقعها على الأنترنيت بتأليف سور تحاكي السور القرآنية الكريمة في محاولة منها لإقناع جمهور الشبكة العالمية بأن القرآن ليس معجزة إلهية من عند الله بل هو من صنع البشر، وبعد كم الاحتجاجات الهائلة من قبل المسلمين المستخدمين للشبكة العالمية على استضافة الشبكة لهذه المنظمة مع ما تثبته من أفكار هدامة وتسيء للإسلام، أعلنت شركة أمريكا أون لين America On Line التي تدير الأنترنيت رفضها بث أفكار هذه المنظمة، ورغم ما تثيره هذه المحاولة للنيل من عقيدة الإسلام من غضب واستياء في نفوس المسلمين إلا أنها تمثل إنذارا مباشرا ينبهنا إلى أننا نحتاج إلى الداعية الإسلامي المناسب للتعامل مع تقنيات القرن القادم، والذي يتمتع بفهم جيد للإسلام ويتحدث لغة أجنبية بطلاقة ويستطيع استخدام تكنولوجيا الحاسبات الرقمية، ويمكن له أن ينفذ إلى مثل هذه المواقع على الشبكة العالمية ويعد الرد المناسب على تبثه من أكاذيب ودعاوى مضللة، (اللبان، 2012، صفحة 126)فهذه المحاولات الهدامة للدين الإسلامي ليست الأولى من نوعها فهناك العديد من محاولات تشويه للدين والإسلام عبر شبكة

الأنترنيت ومواقع الألعاب الإلكترونية والمواقع الإباحية، وهذ كله لضرب العقيدة وتأثير على الفكر والثقافة الإسلامية والعقيدة المحمدية بإفساد الأخلاق بشتى السبل والمحاولات والطرق المباشرة والغير المباشرة مستغلة في ذلك تعلق الشباب العربي بشبكة الأنترنيت ومواقع التواصل الاجتماعي والألعاب الإلكترونية وإدمانهم على المواقع الإباحية الإلكترونية على الشبكة العنكبوتية العالمية.

8.5 تزوير العلامات التجارية

تشكو بعض الشركات المنتجة لشرائح المعالجات المركزية مثل شركة "إنتل" من ظاهرة خطيرة تضر بمصالح هذه الشركات، كما تضر بمصلحة المستفيد وهي تزوير العلامات التجارية والاعتداء على العلامة التجارية بإنشاء شرائح ذات الأداء المنخفض، وبيعها على أنها شرائح ذات أداء أعلى بأسعار أكثر ارتفاعا، ويلجأ بعض موزعي هذه الشرائح وبعض منتجي أجهزة الحاسب الشخصي إلى ارتكاب هذه الجريمة سعيا وراء المزيد من الربح وهذا يدخل من سرقة حقوق الملكية الفكرية للعلامة التجارية والفكرة التي سعت من أجل توسيعها، وذلك بحثا عن التفوق في المنافسة والربح السريع فضلا عما يسببه ذلك من أضرار مؤكدة للمستفيدين وللشركات المنتجة التي يتم تزوير علامتها، فإن ذلك يفقد المستفيدين الثقة فيما يحصلون عليه في الأسواق وتفقد الشركة الأم مصداقيتها في جودة السلع والخدمات مما يهدم السوق الموازية للشركة أو المؤسسة المنتجة. (المزاهرة،2014، صفحة382)

9.5 التزييف والتزوير باستخدام الحاسوب

نظرا للتطور التقني الهائل في أجهزة الكمبيوتر والطابعات الملونة وأجهزة المسح الضوئي دخل الحاسوب وبتوسع في مجال التزييف والتزوير، حيث يمكن من خلاله نقل توقيع شخص ما على شيك أو إيصال أمانة أو عقد أرض أو شقة، كم يمكن استخدام الكمبيوتر في عملية تزييف العملات الورقية العربية والأجنبية، والمشكلة أن العملات المزيفة تكاد تتطابق تماما مع النقود السليمة ولا يمكن التعرف عليه إلا من خلال خبرة فنية ومهارية عالية، وقد ظهر حديثا "جريمة المعلومات" حيث أن البطاقة الشخصية صادرة عن نظام معلومات وقاعدة بيانات، وفي كل بطاقة جزء في ظهرها يسمى "البركوت" ثنائي الأبعاد يخزن كل المعلومات الخاصة بصاحب البطاقة، كما يمكن الإشارة إلى أن هذه البطاقة مشفرة وإذا أدخلناها في جهاز قارئ تظهر المعلومات نفس الشيء بالنسبة لجواز السفر، ومن هنا فمن الممكن أن يتم اختراق هذه المعلومات لتزييفها وانتحال الشخصية. (اللبان، 2012، صفحة133)

10.5 انتهاك الخصوصية على الشبكة

الخصوصية الفردية هي حق الإنسان في حجب معلوماته الشخصية عن الآخرين، فالتطفل على مكتب شخص آخر أو منزله أو جهاز الحاسب الشخصي الخاص به أو حتى أفكاره يعتبر انتهاكا لهذه الخصوصية، بالتطفل لا نعني تدمير المعلومات أو تحويلها بل إن مجرد فتح الحاسب الشخصي الخاص بشخص ما والاطلاع فقط على ما به من بيانات هو انتهاك للخصوصية الفردية للإنسان، فهل أدى انتشار استخدام الحاسب الشخصي إلى زيادة تعرض الخصوصية الفردية للإنسان لخطر الانتهاك أم أنه قلل من ذلك؟ هذه قضية يثور

حولها الجدل فبعض الناس يرون أن إخراج بياناتك من الأدراج والملفات وجمعها كلها في مكان واحد هو الكمبيوتر يزيد من خطر تعرضها للانتهاك، ويرون كذلك أن عدم تعود الناس على أساليب تأمين المعلومات وعدم إلمامهم بهذا الفن يزيد أيضا من خطر تعرض معلوماتهم للانتهاك، كما يلمحون إلى الانتشار الحالي الذي يحظى به استخدام شبكات المعلومات، ما يعني أن معلوماتك الآن تسري في الهواء بعد أن كانت حبيسة غرفتك أو خزانتك.

وعلى الجانب الآخر يرى فريق آخر أن وجود المعلومات في حيز ضيق محدود (في حاسوب) واتباع الأساليب الصحيحة لتأمين البيانات من تشفير ووضع كلمات مرور وغيرها، يجعل معلوماتك أكثر أمنا مما كانت عليه في ملفاتك أو أدراج مكتبك، حيث يمكن أن يطلع عليها خلسة السكرتير أو عامل النظافة، كما أنه لا خطر في حالة الحاسب من أن تنسى مفاتيحك مرة فيتم نسخها، بل من الحاسب تستطيع تغيير كلمة المرور كلما شئت ذلك، بل إن بعض نظم أمن المعلومات تفرض استخدام كلمة مرور جديدة في كل مرة تدخل فيها على الحاسب. (المزاهرة،2014، صفحة 383)

11.5 نسخ البرامج والأفلام والإعلانات

من بين أكبر الجرائم الإلكترونية المعلوماتية على شبكة الأنترنيت سرقة ونسخ البرامج وتقليدها وإعادة بيعها لربح المال وزيادة الثروة، حيث يفترض أن تتم حماية كل من الكتب والبرمجيات والتسجيلات الصوتية والأفلام والخرائط والإعلانات وغيرها من المواد التي تدخل المعلومات في تكوينها بنسبة كبيرة بواسطة قوانين حقوق الملكية الفكرية التي تخص الأفراد والمؤسسات والمنظمات، والقانون يحمي حقوق استخدام هذه الأعمال في مختلف صورها وعلى مختلف الوسائط التي قد تنقل إليها، ولكن هذه الحماية موقوتة بفترة زمنية محددة وقد تم منذ فترة قريبة تعديل القانون الأمريكي ليتضمن النص على حماية برامج الكمبيوتر سواء في صورتها الأصيلة أو المترجمة، ومثلما يلجأ منتجو الخرائط إلى إضافة بعض العلامات السرية أو المائية الخاصة في خرائطهم لتمكنهم من كشف التزييف، فالمبرمجون أيضا يقومون بالشيء نفسه لحماية برامجهم، وتقوم شركات البرمجة باستخدام علامات سرية ضمن العلامة التجارية للشركة Logo كما تستخدم وسائل حديثة لإضافة العلامات المائية الرقمية لإثبات حقوق الملكية، وعند نسخ البرنامج بصورة غير قانونية يتسبب وجود العلامة المائية في إزاحة بعض الكلمات المعينة أو بعض السطور في النص بمقدار أجزاء من المليمتر بحيث يمكن تمييز الوثيقة الأصلية من المنسوخة، وكذلك على شاشة الحاسب تتم إزاحة بعض الكلمات بمقدار بيكسل واحد فقط، ولكنه يكون كافيا لكشف التزوير دون أن تلحظه عين غير خبيرة. (المزاهرة، 2014، صفحة 387)

12.5 انتحال الشخصية عبر الذكاء الاصطناعي

على الرغم مما يروج له عمالقة التكنولوجيا من فوائد ومزايا الذكاء الاصطناعي في جميع الميادين دون استثناء إلا أن المخاوف تزداد بشأن الجانب المظلم للخوارزميات التي أصبح القراصنة يستخدمونها في طرق الاحتيال والانتحال والابتزاز المالي الذي تضرر منه أشخاص ومؤسسات مالية، وقد تم استغلال تقنيات الذكاء الاصطناعي في التزييف العميق للصور أو مقاطع الفيديو والتي يمكن أن تظهر شخصا ما يفعل شيئا لم يفعله مما يؤدي إلى تنفيذ مؤامرات ابتزاز، ويمكن تركيب وجه في مقطع مزيف بما في ذلك القدرة على وضع وجه جديد على موقع إباحي أو حتى استغلال ذلك في قضايا الانتحال والاحتيال والسرقات المادية وتشويه السمعة، وقال البروفيسور "لويس غريفين" أحد مؤلفي ورقة بحثية نشرها مركز "داوس" للجريمة المستقبلية بجامعة

"يونيفيرسيتي كوليدج" لندن عام2020، والتي صنفت الاستخدامات غير القانونية المحتملة للذكاء الاصطناعي "إنه أمر مزعج للغاية".(ترجمات، أوت2023)

وباستخدام هذه التقنية الحديثة يمكن للمحتالين أن يستغلوا تقنية تركيب الأصوات لانتحال هوية شخص آخر لاستخدامها في عمليات خطف وهمية، وعلى سبيل المثال قد يستغل المجرمون تركيب بصمة الصوت لشخص ما للاتصال بذويه وإبلاغهم بأنه مخطوف مطالبا بدفع مبلغ معين كفدية لإطلاق سراحه، وأشار "غريفين" إلى أن انتحال الهوية الصوتية أو المرئية لشخص زادت بشكل أسرع بكثير مما كان متوقعا، وفي عام 2019 قام الرئيس التنفيذي لشركة طاقة مقرها المملكة المتحدة بتحويل220 ألف يورو أي 241.2 ألف دولار أمريكي إلى محتالين يستخدمون الذكاء الاصطناعي لانتحال شخصية رئيسه وفقا للتقارير، وقال غريفين ن مثل هذه الحيل يمكن أن تكون أكثر فاعلية إذا تم دعمها بالفيديو، ويمكن استخدام التكنلوجيا للتجسس على الشركات مع ظهور موظف مخادع في اجتماع عبر "زوم" للحصول على معلومات دون الحاجة إلى قول الكثير، وأضاف أن عمليات الاحتيال هذه يمكن أن تزداد على نطاق واسع مع احتمال أن تكون الروبوتات التي تستخدم لهجة محلية أكثر فاعلية في خداع الناس من المحتالين الذين يديرون حاليا المؤسسات الإجرامية التي تعمل من دول آسيوية. (ترجمات، أوت2023)

13.5 السرقة العلمية في الفضاء الرقمي

أدت العولمة والثورة الاتصالية إلى تفشي ظاهرة السرقات العلمية بصورة سهلت الحصول على المعلومات والأفكار فقط بضغطة زر، هذا ما سمح للباحث بالاعتماد على مختلف طرق النسخ واللصق والنقل لكن دون أن يتناسى أن هناك في الآونة الأخيرة رقابة وبرامج إلكترونية تسهل هي الأخرى محاولة في الحد من هذه الظاهرة، فالتدفق الحر للمعلومات في عصر العولمة لن ينه عصر الرقابة على المعلومات، ومن جهته اعتبر الباحث "سالم بن محمد سالم" سرقة المعلومات جريمة من أكثر الجرائم الفكرية خطورة ويقصد بالسرقة العلمية السطو على أفكار الآخرين المنشورة على شبكة الأنترنيت من بحوث ومقالات ودراسات ذات قيمة علمية، مما ذلك الانتحال والغش والقرصنة والسطو على المادة العلمية بمختلف اتجاهاتها الأدبية والفكرية، فهي سرقة الإنتاج العلمي للآخرين ونشرها دون الإشارة إلى المصدر الأصلي، وهذا حق غير مشروع ويختلف عن النقل والاقتباس الذي يعد حقا مشروعا للجميع.(بوزيفي، 2018، صفحة202)

أما فيما يتعلق بأنواع السرقات العلمية المنتشرة في الفضاء الرقمي فهي لا تختلف عن تلك السرقات التقليدية حيث تأخذ الأشكال التالية:

1. النسخ واللصق وعدم الإشارة إلى مصادر المعلومات وتوثيقها.
2. كتابة أو إعادة صياغة أفكار أو معلومات دون ذكر مصدرها وينسبها إلى نفسه.
3. شراء عمل أو بحث أو كتاب جاهز من شخص آخر وينسبها إلى نفسه أو دفع أموال لأشخاص آخرين من أجل الكتابة بالنيابة عنه. (بوزيفي، 2018، صفحة 206)
4. سرقة الفكرة أو الأسلوب أي استخدام مفهوم أو رأي مماثل لا يدخل في إطار المعارف العامة.
5. الانتحال الفني كإعادة تمثيل عمل شخص آخر باستخدام وسائط أخرى.
6. الانتحال بالترجمة أي ترجمة المحتوى للغات أخرى واستخدامه دون الإشارة إلى العمل الأصلي. (بوزيفي، 2018، صفحة207)

6. خاتمة:

لقد سهل التطور التكنولوجي والتقدم التقني لتكنولوجيات المعلومات العديد من الأمور في حياتنا اليومية، وساهم بشكل كبير في إحداث طفرة نوعية في جميع المجالات بشكل يفوق تصور العقل البشري بآلاف سنين، لكنه من جهة أخرى سبب الكثير من المخاطر والأضرار المرتبطة بالحواسيب الآلية والشبكة العنكبوتية العالمية، ما أحدث حالة طوارئ ورهاب اجتماعي لدى الكثير من الدول والمجتمعات دون استثناء، فمنها من سعت إلى إحداث ونشر الوعي المجتمعي فيما يخص الجرائم السيبرانية على الصعيدين الدولي والمحلي، كتبيان السبل والطرق المساعدة للحد والتقليل من هذه المخاطر الإلكترونية وكيفية تفاديها والتخلص منها، ومنها من لجأت في النصوص والأنظمة القانونية للحد من هذه الجرائم الشبكية وكبح تزايدها المستمر بين أوساط أفراد المجتمع.

إلا أن هذه القوانين والتشريعات الشبكية لم تكبح بشكل كامل هذه التجاوزات التي أودت باقتصاد الكثير من البلدان، وهذا راجع إلى تساهل رجال العدالة الذين لم يتعودوا على مثل هذه القضايا أو أن هذه المراسيم القانونية لا تشمل كافة الجرائم السيبرانية، مما يطيح بنا في فجوة رقمية معلوماتية ساهم الفراغ القانوني الرهيب في زيادة فجوتها، أو ربما أن هذه الجريمة كونها تقنية محضة فإن تجاوزها أصبح تقنيا حتى بدون أي دليل فيزيقي يدينها، وفي الختام نذكرك أنه في حالة ما تعرضت للمضايقة أو التهديد والابتزاز من طرف أشخاص آخرين فلا تتردد لحظة واحدة في الاتصال بخدمة الأمن المعلوماتي على الشبكة.

7. توصيات:

- حث الجامعات والمراكز البحثية العربية للبحث والدراسة في الجرائم المعلوماتية والجرائم عبر الانترنت ومحاولة إنشاء ديبلومات متخصصة في المجالات التقنية والقانونية المتعلقة بمكافحة تلك الجرائم
- العمل على تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية.
- إنشاء مجموعات عمل عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم المعلوماتية على العالم الافتراضي.
- حث جامعات الدول العربية على إصدار قانون نموذجي موحد لمكافحة الجرائم المعلوماتية على المستوى العربي.

8. قائمة المراجع:

- المزاهرة، منال هلال (2014)، تكنولوجيا الاتصال والمعلومات، دار المسيرة للنشر والتوزيع، عمان، الأردن.
- اللبان، شريف درويش (2014)، تكنولوجيا الاتصال، المخاطر والتحديات والتأثيرات الاجتماعية، الطبعة الثالثة، الدار المصرية اللبنانية، القاهرة، جمهورية مصر العربية.
- باسبعين، وسام صالح (2016)، ثورة تقنيات الاتصال الحديثة وتحدياتها، الطبعة الأولى، عالم الكتب الحديث للنشر والتوزيع، العبدلي، المملكة الأردنية الهاشمية.
- دليو، فضيل (2015)، تكنولوجيا الإعلام والاتصال الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر العاصمة، الجزائر.
- مرعي، إسراء جبريل رشاد (2016)، الجرائم الإلكترونية: الأهداف، الأسباب، طرق الجريمة ومعالجتها، المركز الديموقراطي العربي للدراسات الاستراتيجية والاقتصادية والسياسية، مجلة الدراسات الاستراتيجية.

- المايل، عبد السلام محمد، الشربجي، عادل محمد (2019)، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة آفاق للبحوث والدراسات، المركز الجامعي إيليزي، الجزائر.
- حسينات، محمد محسن، الصامدي، أحمد محمد الهزاع، الشرع، عبد الهادي ضيف الله (2012)، جرائم الحاسوب والأنترنيت، مجلة جامعة فلسطين للأبحاث والدراسات، العدد الثاني.
- بوزيفي، وهيبة (2018)، النشر الإلكتروني والسرقات العلمية، مجلة الآداب واللغات.
- البداينة، ذياب موسى (2014)، الجرائم الإلكترونية: المفهوم والأسباب، الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية.
- دبي ترجمات (2023)، كيف جعل الذكاء الاصطناعي عالم الجريمة "أكثر خطرا وقربا" من الناس؟، موقع قناة الحرة، دبي، الإمارات المتحدة، على الموقع:https://www.alhurra.com/tech
- مجمع البحوث والدراسات (2016)، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى، سلطنة عمان.
- Leukfeldt, R. a. (2013, January – June). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology (IJCC), Vol 7 (1).