مجلة الباحث في العلوم الإنسانية والاجتماعية
ISSN 2170-0370/E-ISSN 8127-2710
المجلد16/العدد01 – السنة 2025 ،ص08 ص28

الجريمة السيبرانية وتأثيراتها على الفرد والمجتمع في عصر التكنولوجيا

Cybercrime and Its Impacts on Individuals and Society in the Age of Technology

أ.عبد الحميد بوديار[1]*، أ.د/رشيد طبال[2]

[1] جامعة 20 أوت 1955 سكيكدة (الجزائر)،(a.boudiar@univ-skikda.dz)

[2] جامعة 20 أوت 1955 سكيكدة (الجزائر)،(r.tobal@univ-skikda.dz)

تاريخ الاستلام : 2024/10/26 ؛ تاريخ القبول : 2025/01/27 ؛ تاريخ النشر : 2025/01/31

الملخص

تتناول هذه الدراسة "الجريمة الإلكترونية وانعكاساتها على الفرد والمجتمع في الجزائر" التأثيرات المتزايدة للجريمة الإلكترونية على مختلف جوانب الحياة، وسنحاول التعرض لأنواع الجرائم الإلكترونية مثل الاحتيال المالي، وسرقة الهوية، والتجسس الإلكتروني، بالإضافة إلى الجرائم المرتبطة بالتطبيقات الاجتماعية مثل **تيك توك**، ومن أهداف دراستنا إلى تحليل آثار هذه الجرائم على الأفراد من حيث فقدان الخصوصية والأمان الشخصي، وتأثيراتها على المجتمع من حيث تآكل الثقة بين المواطنين والمؤسسات، ومن بين الأمثلة التي سنتطرق لها حادثة "فيجر" التي توضح كيفية استخدام الجرائم الإلكترونية كأداة للتجسس وتأثيرها على الأمن القومي، من خلال استعراض المعطيات والبيانات المتاحة.

وفي خلاصة هذه المداخلة نقدم توصيات لتعزيز الأمن السيبراني ورفع الوعي المجتمعي حول المخاطر المرتبطة بالجريمة الإلكترونية.

الكلمات المفتاحية :الجريمة الإلكترونية، الاحتيال المالي، سرقة الهوية، الأمن السيبراني، تيك توك، التأثيرات الاجتماعية.

***المؤلف المراسل.**

Abstract

This study, titled "Cybercrime and Its Impact on Individuals and Society in Algeria," addresses the increasing effects of cybercrime on various aspects of life. We will explore types of cybercrimes such as financial fraud, identity theft, and cyber espionage, in addition to crimes related to social media applications like TikTok. One of the main objectives of our study is to analyze the effects of these crimes on individuals, particularly in terms of loss of privacy and personal security, as well as their impact on society through the erosion of trust between citizens and institutions. Among the examples we will discuss is the "Veger" incident, which demonstrates how cybercrimes can be used as tools for espionage and their impact on national security, using available data and information.

In the conclusion of this presentation, we offer recommendations for strengthening cybersecurity and raising public awareness of the risks associated with cybercrime.

Keywords: Cybercrime, financial fraud, identity theft, cybersecurity, TikTok, social impacts.

. **المقدمة:**

تعتبر الجريمة السيبرانية من أبرز التحديات التي تواجه المجتمعات الحديثة، مع التطور التكنولوجي السريع وزيادة استخدام الإنترنت، باتت هذه الجرائم تهدد الأفراد والمؤسسات على حد سواء، تتنوع أشكال الجريمة السيبرانية لتشمل الاحتيال الإلكتروني، وسرقة الهوية، والابتزاز الإلكتروني، مما يسبب آثارًا سلبية على الأفراد والمجتمع.

على سبيل المثال، وفقًا لتقرير مكتب التحقيقات الفيدرالي الأمريكي (FBI) لعام 2020، تم الإبلاغ عن خسائر مالية تجاوزت 4.2 مليار دولار نتيجة لجرائم الاحتيال الإلكتروني فقط في الولايات المتحدة .Federal Bureau of Investigation, 2020, p (3)، يعكس هذا الرقم حجم المخاطر التي يتعرض لها الأفراد والشركات في ظل تنامي هذه الجرائم، في الجزائر، أظهرت دراسة حديثة أن 34% من الشركات تعرضت لهجمات إلكترونية خلال السنوات الأخيرة، مما يؤكد الحاجة الملحة لتحسين استراتيجيات الأمن السيبراني في البلاد (جيماوي، 2021، ص 140) .

إن تأثير الجريمة السيبرانية لا يقتصر على الأبعاد الاقتصادية فقط، بل يمتد إلى الجوانب النفسية والاجتماعية، فقد أشارت الدراسات إلى أن الأفراد الذين تعرضوا لجرائم إلكترونية يعانون من زيادة في مستويات القلق والاكتئاب، مما يؤثر على جودة حياتهم (أون، 2020، ص68) .

تتطلب مواجهة هذه الظاهرة فهمًا عميقًا لتأثيراتها المتعددة على الأفراد والمجتمعات، فضلاً عن استكشاف الآليات الفعالة للحد من هذه الجرائم وحماية الأمن الشخصي والاجتماعي.

2.الإشكالية :

تشهد الجزائر تزايدًا ملحوظًا في الجرائم الإلكترونية التي تمثل تهديدًا مباشرًا للأفراد والمجتمع، وتشمل هذه الجرائم سرقة الهوية، الاحتيال المالي، التلاعب بالبيانات، والتجسس الإلكتروني، الذي يعد الأخطر لتأثيره على الأمن القومي والاجتماعي، ومع الاعتماد المتزايد

على التكنولوجيا الرقمية في الحياة اليومية، أصبحت هذه الجرائم أكثر تعقيدًا وانتشارًا، مما يجعل الأفراد والمؤسسات عرضة للاختراق.

يُعد مثال حادثة اختراق أنظمة حزب الله عبر أجهزة "فيجر" من قبل المخابرات الإسرائيلية تجسيدًا لخطورة هذه الجرائم، حيث أدى هذا الاختراق إلى كشف معلومات حساسة وأضعف قدرة التنظيم على اتخاذ قرارات فورية، إذا تعرضت الجزائر لاختراق مماثل لأنظمتها الاتصالية أو الرقمية، فقد يهدد ذلك أمنها القومي والاجتماعي.

على الصعيد الفردي، تسبب الجرائم الإلكترونية فقدان الخصوصية والأمان، مما يعزز مشاعر الخوف والقلق، كما أن سرقة البيانات أو الاحتيال المالي يمكن أن يؤدي إلى خسائر مادية ونفسية كبيرة، ويضعف ثقة الأفراد في الأنظمة الرقمية، أما على المستوى المجتمعي، فإن هذه الجرائم تعمق الفجوة بين من يمتلكون المهارات التقنية ومن يفتقرون إليها، وتؤدي إلى تراجع الثقة بين المواطنين والمؤسسات.

إذا طالت الجرائم الإلكترونية البنية التحتية للقطاعات الحيوية مثل البنوك والتعليم والصحة، فقد يؤدي ذلك إلى تعطيل الخدمات الأساسية ويؤثر سلبًا على حياة المواطنين واستقرار المجتمع، كما يمكن أن تهدد الهجمات على المؤسسات الأمنية بتسريب معلومات حساسة، مما يعرض الأمن الوطني للخطر.

تتضح الإشكالية في قدرة الدولة على مواجهة هذه التحديات، وتُطرح تساؤلات حول الخطوات التي يجب اتخاذها لحماية الأفراد والبنية التحتية الرقمية من هذه الجرائم المتزايدة، وضمان الاستقرار الوطني والأمن الاجتماعي.

3.الأهداف :

❖ تحليل تأثير الجريمة السيبرانية على الأفراد والمجتمعات :تسعى هذه الدراسة إلى كيفية تأثير الجرائم السيبرانية على الأفراد من حيث الأمان الشخصي والصحة النفسية، وكذلك تأثيرها على المجتمعات من حيث الاستقرار الاجتماعي والاقتصادي.

❖ تحديد أنواع الجرائم السيبرانية الشائعة :تهدف كذلك إلى تصنيف الجرائم السيبرانية التي تتزايد في العالم وفي الجزائر، بما في ذلك الاحتيال المالي، وسرقة الهوية، والابتزاز الإلكتروني، لفهم مدى انتشارها وتأثيراتها.

❖ تقييم تأثير الجرائم السيبرانية على الأمن الاجتماعي والاقتصادي : دراسة الآثار السلبية لهذه الجرائم على الأمن الاجتماعي، مثل فقدان الثقة في المؤسسات، وتأثيرها على الاقتصاد الوطني من خلال تقليل الاستثمارات وزيادة التكاليف المرتبطة بالأمن.

❖ استكشاف السبل الممكنة لمواجهة الجريمة السيبرانية : تقديم توصيات حول استراتيجيات فعالة للحد من تأثيرات الجرائم السيبرانية، بما في ذلك تعزيز التشريعات، وزيادة الوعي المجتمعي، وتحسين تكنولوجيا الحماية.

❖ تحليل الأطر القانونية والتشريعية المتعلقة بالأمن السيبراني : مراجعة القوانين والسياسات المعمول بها في الجزائر والعالم لمواجهة الجريمة السيبرانية، وتقديم مقترحات لتطويرها بما يتماشى مع التحديات الحالية.

❖ تعزيز التعاون المحلي والدولي في مكافحة الجريمة السيبرانية : تسليط الضوء على أهمية التعاون بين مختلف الجهات الفاعلة، بما في ذلك الحكومات، والقطاع الخاص، ومنظمات المجتمع المدني، لمواجهة الجريمة السيبرانية بشكل أكثر فعالية.

4.مفاهيم ومصطلحات الدراسة:

3.1. **الجريمة السيبرانية** :تُعرف الجريمة السيبرانية بأنها أي نشاط إجرامي يُرتكب باستخدام تقنيات المعلومات أو الإنترنت، والذي يُستهدف فيه الأفراد أو المؤسسات، تتضمن هذه الجرائم مجموعة واسعة من الأفعال مثل الاحتيال الإلكتروني، وسرقة الهوية، والقرصنة، والابتزاز الإلكتروني، وتعتبر الجريمة السيبرانية تهديدًا متزايدًا للأمن الشخصي والاقتصادي في جميع أنحاء العالم (McGuire & Dowling, 2013, p. 9) .

4.2.الأمن السيبراني :يشير الأمن السيبراني إلى مجموعة من التدابير التقنية والتنظيمية التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات السيبرانية، يشمل ذلك

استخدام برامج الحماية، تشفير البيانات، وتطبيق السياسات الأمنية المناسبة لضمان سرية وسلامة المعلومات (Bertino & Sandhu, 2010, p. 42) .

4.3.سرقة الهوية :تُعرّف سرقة الهوية بأنها عملية الاحتيال التي يتم فيها استخدام المعلومات الشخصية لشخص آخر، مثل الاسم، ورقم الضمان الاجتماعي، أو معلومات بطاقة الائتمان، بدون إذن، تعتبر سرقة الهوية من أخطر أشكال الجريمة السيبرانية حيث يمكن أن تؤدي إلى خسائر مالية كبيرة وأضرار دائمة لسمعة الضحايا(Smith, 2019, p. 205) .

4.4.الابتزاز الإلكتروني :يشير الابتزاز الإلكتروني إلى استخدام التهديدات أو الضغط للحصول على أموال أو معلومات حساسة من الأفراد أو الشركات، غالبًا ما يتضمن ذلك تهديد الضحية بنشر معلومات خاصة أو حساسة ما لم يتم دفع فدية (Cheng, Liu, & Yao, 2017, p. 130).

4.5.الاحتيال المالي عبر الإنترنت :يُعتبر الاحتيال المالي عبر الإنترنت من أكثر الجرائم السيبرانية شيوعًا، حيث يتم استغلال الثغرات في الأنظمة الرقمية لتحقيق مكاسب مالية غير قانونية، قد يشمل ذلك تقديم عروض وهمية، إنشاء مواقع احتيالية، أو إرسال رسائل بريد إلكتروني مزيفة لاستدراج الضحايا(Aoun, 2020, p. 75) .

4.6.الهندسة الاجتماعية :تُعرف الهندسة الاجتماعية بأنها مجموعة من الأساليب المستخدمة لخداع الأفراد للحصول على معلومات حساسة، مثل كلمات المرور أو البيانات الشخصية، يعتمد المهاجمون على الحيل النفسية، مثل الاحتيال عبر البريد الإلكتروني، للتلاعب بالضحايا وإقناعهم بالكشف عن معلوماتهم (Kumar & Somani, 2018, p. 82) .

5.مفهوم الجريمة الإلكترونية :

5.1.لغة: تتكون كلمة "الجريمة" من الجذر العربي "ج، ر، م"، والذي يعني ارتكاب فعل غير قانوني أو إلحاق الضرر بالآخرين، يُستخدم مصطلح "الإلكترونية" للإشارة إلى كل ما يتعلق

بالتكنولوجيا الحديثة والأنظمة الرقمية. لذا، فإن "الجريمة الإلكترونية" تعني أي فعل غير قانوني يُمارس باستخدام الوسائل الإلكترونية أو الإنترنت.

2.5. اصطلاحا: تُعرَّف الجريمة الإلكترونية بأنها أي نشاط إجرامي يُرتكب باستخدام نظام معلوماتي أو في سياق نظام معلوماتي، سواء كان ذلك من خلال شبكات الكمبيوتر أو على الإنترنت (OSCE, 2006, p. 5) ، وتشمل هذه الجرائم مجموعة واسعة من الأفعال مثل الاحتيال الإلكتروني، وسرقة الهوية، والابتزاز الإلكتروني، مما يجعلها تهديدًا متزايدًا للأمن الشخصي والاجتماعي.

يُعرَّف مكتب التحقيقات الفيدرالي الأمريكي الجريمة السيبرانية بأنها أي جريمة يتم ارتكابها باستخدام أجهزة الكمبيوتر أو الشبكات، بما في ذلك الجرائم التي تستهدف الأنظمة الرقمية (Federal Bureau of Investigation, 2020, p. 3)، ويشير هذا التعريف إلى أن الجريمة الإلكترونية تشمل أي فعل غير قانوني يمكن أن يؤثر على الأفراد أو المؤسسات من خلال استخدام التكنولوجيا الحديثة.

يمكن تعريف الجريمة الإلكترونية أيضًا بأنها أي عمل غير قانوني يتم تنفيذه عبر الإنترنت، حيث يتم استغلال التقنيات الرقمية لتحقيق مكاسب شخصية أو اقتصادية، هذا التعريف يسلط الضوء على الأبعاد الاقتصادية والاجتماعية لهذه الجرائم، مما يعكس الحاجة الملحة لتعزيز الوعي والمواجهة(Honour & Tiessen, 2008, p. 12) .

يمكن تعريف الجريمة الإلكترونية إجرائيًا بأنها أي فعل غير قانوني يتم تنفيذه كليًا أو جزئيًا باستخدام أجهزة الكمبيوتر أو الشبكات، والذي يؤثر على المعلومات أو البيانات أو الأصول الرقمية، ويؤدي إلى إلحاق الضرر بالأفراد أو المؤسسات. يشمل ذلك أفعال مثل الاحتيال المالي عبر الإنترنت، وسرقة الهوية، والقرصنة، والابتزاز الإلكتروني، مما يتطلب استراتيجيات قانونية وتقنية خاصة لضمان الحماية من هذه التهديدات (محمد ، 2020 , p. 75) .

6. خصائص الجريمة الإلكترونية:

6.1.الخفاء والسرية :تتميز الجريمة الإلكترونية بأنها غالبًا ما تُرتكب بسرية وخفاء، مما يجعل من الصعب اكتشافها أو تتبع الجاني، فالأدوات التكنولوجية التي تُستخدم في تنفيذ الجرائم، مثل برامج التشفير والشبكات الافتراضية الخاصة(VPN) ، تُساعد المجرمين على إخفاء هويتهم وأماكنهم(McGuire & Dowling, 2013, p. 15) .

6.2.السرعة :تُنفذ الجرائم الإلكترونية بسرعة فائقة، حيث يمكن للمجرم القيام بعملية احتيال أو سرقة بيانات في ثوانٍ معدودة، هذه السرعة تعني أن الضحايا قد لا يكون لديهم الوقت الكافي لاتخاذ إجراءات لحماية أنفسهم قبل وقوع الجريمة (Aoun, 2020, p. 78) .

5.3.التوسع والانتشار العالمي :نظرًا لأن الإنترنت يُستخدم في جميع أنحاء العالم، فإن الجرائم الإلكترونية ليست محصورة في منطقة جغرافية معينة، يمكن للمجرمين استهداف ضحاياهم في دول مختلفة دون الحاجة إلى الانتقال من مكانهم (Kumar & Somani, 2018, p. 85) .

5.4.الاعتماد على التكنولوجيا :تعتمد الجريمة الإلكترونية بشكل كبير على تقنيات المعلومات والاتصالات، فهي تتطلب معرفة فنية قوية في كيفية عمل الأنظمة الرقمية، مما يجعلها أكثر تعقيدًا مقارنة بالجرائم التقليدية(Cheng, Liu, & Yao, 2017, p. 135) .

5.5.استهداف البيانات :تركز الجرائم الإلكترونية على استهداف البيانات والمعلومات الحساسة، سواء كانت معلومات مالية أو شخصية، مما يجعلها تهديدًا كبيرًا للأمان الشخصي والاجتماعي(Smith, 2019, p. 210) .

7.أسباب الجريمة الالكترونية :

7.1.**الدوافع المالية** :تعتبر الدوافع المالية من الأسباب الرئيسية وراء الجرائم الإلكترونية، على سبيل المثال، في عام 2021، تعرضت **شركة** Colonial Pipeline لهجوم بفيروس الفدية أدى إلى دفع فدية مقدارها 4.4 مليون دولار لاستعادة البيانات، مما يبرز أهمية المكاسب المالية كمحفز للمجرمين(McMillan, 2021) .

كما أفاد تقرير Cybercrime Magazine أن خسائر الاحتيال الإلكتروني قد تصل إلى حوالي 6 تريليونات دولار سنويًا بحلول عام 2021، مما يعكس أن الربح المالي هو هدف رئيسي لمجرمي الإنترنت(Cybercrime Magazine, 2021) .

7.2. **قلة الوعي الأمني** :يعاني الكثير من الأفراد والشركات من نقص الوعي بتهديدات الأمن السيبراني، وفقًا لتقرير Verizon Data Breach Investigations Report لعام 2021، كان حوالي **85%** من خروقات البيانات ناتجة عن عوامل بشرية، مثل استخدام كلمات مرور ضعيفة أو استجابة سريعة للهجمات(Verizon, 2021) .

في الجزائر، أظهرت دراسات أن **70%** من المستخدمين ليس لديهم معرفة كافية بأساسيات الأمن السيبراني، مما يجعلهم عرضة للاختراقات.

7.3.**تطور التكنولوجيا** :مع تقدم التكنولوجيا، يزداد عدد الأدوات المستخدمة لارتكاب الجرائم الإلكترونية، في عام 2020، تم الإبلاغ عن زيادة بنسبة **400%** في هجمات الفدية على مستوى العالم بسبب سهولة الوصول إلى أدوات البرمجة والتشفير (Cybersecurity Ventures, 2020).

في الجزائر، ازدادت نسبة استخدام البرمجيات الخبيثة، مما أدى إلى زيادة الجرائم الإلكترونية، وفقًا لتقرير من مركز الأمن السيبراني، ارتفعت نسبة الهجمات الإلكترونية بمعدل **50%** في عام 2021 مقارنة بالعام السابق.

7.4.**الإحباط الاجتماعي** :يُعزى الإحباط الاجتماعي والاقتصادي إلى زيادة الجرائم الإلكترونية، وفقًا لدراسة أُجريت في عام 2020، اعتبر **32%** من الشباب في الجزائر أن استخدام التكنولوجيا لارتكاب الجرائم هو وسيلة للتعبير عن استيائهم من الظروف الاقتصادية (جيماوي، 2021).

7.5.سهولة التنفيذ :تتيح الجريمة الإلكترونية للمجرمين تنفيذ جرائمهم بسهولة، على سبيل المثال، يُشير تقرير Europol إلى أن **94%** من الهجمات الإلكترونية يتم تنفيذها عبر

الإنترنت، مما يعني أن المجرمين لا يحتاجون إلى التواجد فعليًا في مكان الجريمة (Europol, 2021).

في الجزائر، أدت زيادة الوصول إلى الإنترنت وتوافر أدوات تكنولوجيا المعلومات إلى ارتفاع معدل الجرائم الإلكترونية، حيث أفاد **75%** من المستخدمين أنهم قد تعرضوا لمحاولات اختراق.

8. العوامل المؤدية للجريمة الالكترونية :

8.1. **العوامل الأسرية** :تلعب الأسرة دورًا كبيرًا في تشكيل سلوك الأفراد. يمكن أن يؤدي التفكك الأسري أو نقص الدعم النفسي إلى انخراط الأفراد في أنشطة إجرامية، بما في ذلك الجرائم الإلكترونية، وفقًا لدراسة أُجريت في الجزائر، يُظهر **40%** من الشباب الذين ارتكبوا جرائم إلكترونية أنهم عانوا من مشاكل أسرية (جيماوي، 2021).

8.2. **المدرسة** :تسهم المدارس في توجيه سلوك التلاميذ وتوعيتهم بمخاطر الإنترنت، تشير دراسة من **المنظمة الدولية للشرطة الجنائية (Interpol)** إلى أن **60%** من الطلاب في دول متعددة لم يتلقوا أي تدريب أو توعية بشأن الأمن السيبراني في المدارس، مما يزيد من تعرضهم للاختراقات(Interpol, 2020) .

8.3. **المؤسسات الجامعية** :تُعد المؤسسات التعليمية مكانًا رئيسيًا لاكتساب العلم و المعرفة، ولكنها أيضًا قد تُصبح بيئة مناسبة لارتكاب الجرائم الإلكترونية، في الجزائر، أظهرت دراسة أن **30%** من طلاب الجامعات تعرضوا لمحاولات اختراق حساباتهم الجامعية بسبب قلة الوعي الأمني (محمد ، 2020).

8.4. **جماعة الأقران** :تؤثر جماعة الأقران بشكل كبير على سلوك الأفراد، حيث يمكن أن تشجعهم على الانخراط في أنشطة غير قانونية، تشير إحصائيات إلى أن الشباب الذين ينتمون إلى جماعات غير قانونية هم أكثر عرضة بنسبة **25%** لممارسة الجرائم الإلكترونية مقارنة بأقرانهم (Kumar & Somani, 2018, p. 85) .

8.5.**البيئة السكنية** :تلعب البيئة السكنية دورًا مهمًا في تشكيل سلوك الأفراد، الأحياء ذات مستوى التعليم المنخفض أو ارتفاع معدلات البطالة تُعزز من احتمالية انخراط الأفراد في أنشطة إجرامية، في الجزائر، أظهرت التقارير أن المناطق التي تعاني من الفقر والبطالة شهدت زيادة في الجرائم الإلكترونية بنسبة **35%** (جيماوي، 2021) .

8.6.**قلة الوعي الأمني** :تعتبر قلة الوعي بالتهديدات الأمنية من العوامل الرئيسية المؤدية للجريمة الإلكترونية، وفقًا لتقرير **Verizon**، كان حوالي **85%** من خروقات البيانات ناتجة عن أخطاء بشرية، مثل استخدام كلمات مرور ضعيفة أو الاستجابة السريعة للهجمات (Verizon, 2021).

8.7.**سهولة التنفيذ** :تتيح الجريمة الإلكترونية للمجرمين تنفيذ جرائمهم من أي مكان في العالم، مما يقلل من خطر القبض عليهم، يُشير تقرير **Europol** إلى أن **94%** من الهجمات الإلكترونية تتم عبر الإنترنت، مما يعني أن المجرمين لا يحتاجون إلى التواجد فعليًا في مكان الجريمة (Europol, 2021) .

8.8.**الإحباط الاجتماعي** :يُعزى الإحباط الاجتماعي والاقتصادي إلى زيادة الجرائم الإلكترونية، دراسة أُجريت في الجزائر أظهرت أن **32%** من الشباب يعتبرون أن استخدام التكنولوجيا لارتكاب الجرائم هو وسيلة للتعبير عن الاستياء من الظروف الاقتصادية (جيماوي، 2021) .

8.و.تطور التكنولوجيا :مع تقدم التكنولوجيا، يزداد عدد الأدوات المستخدمة لارتكاب الجرائم الإلكترونية، على سبيل المثال، تم الإبلاغ عن زيادة بنسبة **400%** في هجمات الفدية على مستوى العالم في عام 2020(Cybersecurity Ventures, 2020) .

7.10.**الدوافع المالية** :تعتبر الدوافع المالية من الأسباب الرئيسية وراء الجرائم الإلكترونية، وفقًا لتقرير Cybercrime Magazine، يُتوقع أن تصل خسائر الاحتيال الإلكتروني إلى حوالي 6 تريليونات دولار سنويًا بحلول عام 2021 (Cybercrime Magazine, 2021) .

9. صور الجريمة الإلكترونية مع إحصائيات وأمثلة:

9.1.الاحتيال عبر البريد الإلكتروني :يعاني الكثير من الأفراد في الجزائر من عمليات الاحتيال عبر البريد الإلكتروني، في عام 2021، تم الإبلاغ عن 2000 حالة احتيال عبر البريد الإلكتروني، حيث تم استغلال رسائل من مؤسسات حكومية أو بنوك للحصول على معلومات شخصية، من بين هذه الحالات، تعرض بعض الضحايا لخسائر تتجاوز 500,000 دينار جزائري (حوالي 3,600 دولار أمريكي) (المركز الوطني للأمن السيبراني، 2021، ص. 12).

9.2.سرقة الهوية :تعتبر سرقة الهوية من الجرائم الشائعة. وفقًا لتقارير المركز الوطني للأمن السيبراني، تم الإبلاغ عن حوالي 1500 حالة لسرقة الهوية في الجزائر في عام 2020 (وزارة البريد والمواصلات السلكية واللاسلكية، 2022، ص. 8)، يمكن أن تؤدي هذه الجريمة إلى فقدان الأموال وتدمير السمعة الشخصية.

9.3.استخدام برمجيات الفدية :في عام 2021، شهدت الجزائر زيادة ملحوظة في هجمات برمجيات الفدية، تم الإبلاغ عن **ثلاث** هجمات رئيسية استهدفت شركات محلية، حيث تم تشفير بيانات هذه الشركات وطُلبت فدية تبلغ 2 مليون دينار جزائري (حوالي 14,500 دولار أمريكي) لاستعادة الوصول إلى المعلومات (أحمد، 2021، ص. 45) .

9.4.الهندسة الاجتماعية : تشير إلى مجموعة من الأساليب التي تهدف إلى خداع الأفراد أو التلاعب بهم للحصول على معلومات حساسة أو الوصول إلى أنظمة أو بيانات غير مصرح بها. تُستخدم الهندسة الاجتماعية غالبًا في سياق الأمن السيبراني، حيث يقوم المخترقون بتوظيف تقنيات نفسية لتضليل الضحايا وجعلهم يكشفون عن معلومات شخصية مثل كلمات المرور أو بيانات بطاقة الائتمان، تشير التقارير إلى أن **35%** من الأفراد الذين تعرضوا للاحتيال الإلكتروني أُخدعوا من خلال تقنيات الهندسة الاجتماعية، في عام 2021، تم توثيق 1500 حالة في الجزائر حيث تم استخدام هذه الأساليب لخداع المواطنين للحصول على معلومات حساسة (المركز الوطني للأمن السيبراني، 2021، ص. 22) .

9.4.قرصنة الحسابات على وسائل التواصل الاجتماعي : في عام 2021، تم الإبلاغ عن أكثر من **500 حالة** لقرصنة حسابات وسائل التواصل الاجتماعي، استخدم المهاجمون هذه الحسابات للاحتيال على الأصدقاء أو نشر معلومات مضللة (وزارة الداخلية والجماعات المحلية، 2022، ص. 10).

9.5.النصب في التجارة الإلكترونية :ارتفعت حالات النصب في التجارة الإلكترونية بنسبة **30%** في الجزائر خلال عام 2021، حيث تعرض الكثير من الأفراد لعمليات احتيال خلال التسوق عبر الإنترنت، مما أدى إلى خسائر تقدّر بحوالي 1.5 مليار دينار جزائري (حوالي 11 مليون دولار أمريكي) (المركز الوطني للأمن السيبراني، 2021، ص. 30) .

10. أثر الجريمة الإلكترونية على الأمن الاجتماعي الجزائري مع أمثلة واقعية:

10.1.تآكل الثقة بين الأفراد والمؤسسات :في عام 2021، أظهرت تقارير من المركز الوطني للأمن السيبراني أن نسبة **70%** من المواطنين يشعرون بأن المؤسسات الحكومية لم تكن قادرة على حماية بياناتهم، هذا الأمر يتجلى في عدة حوادث، مثل الاختراق الذي تعرضت له بعض الوزارات، مما أدى إلى فقدان بيانات حساسة للموظفين والمواطنين، مثل هذه الأحداث جعلت المواطنين أكثر حذرًا في التعامل مع الخدمات الحكومية الإلكترونية (المركز الوطني للأمن السيبراني، 2021، ص. 22).

10.2.زيادة الجرائم التقليدية :تشير التقارير إلى أن بعض ضحايا الجرائم الإلكترونية، مثل الاحتيال المالي، قد يلجئون إلى الانتقام بطرق غير قانونية، على سبيل المثال، تم الإبلاغ عن حالات في الجزائر حيث قام بعض الأفراد باستهداف المحتالين بالتحقيق الشخصي، مما أدى إلى تفشي العنف في بعض المناطق، ووفقًا لإحدى الدراسات، أظهرت **20%** من الضحايا أنهم اتخذوا إجراءات انتقامية ضد المجرمين (الجزائر 24، 2021، ص. 12).

9.3.تعزيز الفجوة الاجتماعية :في الجزائر، أظهرت دراسة أن **30%** من الشباب الذين يفتقرون إلى المعرفة بالأمن السيبراني كانوا عرضة للاختراقات، على سبيل المثال، تعرض عدد

من الطلاب في الجامعات لهجمات احتيالية بسبب عدم وعيهم بأساليب الحماية على الإنترنت، هذا الأمر يؤدي إلى تهميشهم وزيادة الفقر بين هؤلاء الشباب، حيث يجدون أنفسهم معرضين للخطر بشكل أكبر (وزارة التعليم العالي والبحث العلمي، 2022، ص. 30).

10.4.فقدان الخصوصية والأمان الشخصي :في إحدى الحوادث، تم اختراق بيانات 1,500 عميل في أحد البنوك الجزائرية، مما أدى إلى تسريب معلوماتهم الشخصية، هذا الاختراق جعل الضحايا يشعرون بالخوف من استخدام الخدمات البنكية عبر الإنترنت، حيث أصبحوا يترددون في التعامل مع أي منصة رقمية قد تعرض معلوماتهم للخطر (وزارة البريد والمواصلات السلكية واللاسلكية، 2022، ص. 15).

1.5.التأثير على الأسرة :هناك العديد من الحالات التي شهدت فيها الأسر مشكلات داخلية نتيجة للضغوط المالية الناتجة عن الجرائم الإلكترونية، على سبيل المثال، تعرض أحد أفراد الأسرة للاحتيال المالي عبر الإنترنت، مما أدى إلى فقدان مدخرات الأسرة، وأدى ذلك إلى توتر وخلافات عائلية، العديد من الأسر أبلغت عن مشكلات نفسية نتيجة لهذه الضغوط.

10.6.التأثير على الصحة النفسية :وفقًا لدراسة أُجريت في الجزائر، فإن **40%** من ضحايا الجرائم الإلكترونية يعانون من اضطرابات نفسية مثل القلق والاكتئاب، تم الإبلاغ عن حالات تعرض فيها الأفراد لنوبات قلق شديدة بعد فقدان بياناتهم الشخصية أو تعرضهم للاحتيال، مما أثر على حياتهم اليومية وعلاقاتهم الاجتماعية (المنظمة العربية للتنمية الإدارية، 2022، ص. 50).

11- انعكاسات الجريمة الالكترونية على الفرد والمجتمع في الجزائر:

11.1.الانعكاسات على الفرد الجزائري:

❖ الخسائر المالية :تُعتبر الخسائر المالية من الانعكاسات الأكثر وضوحًا للجريمة السيبرانية على الأفراد، على سبيل المثال، في عام 2021، تعرض أحد المواطنين لعملية احتيال إلكتروني عبر بطاقة ائتمان، حيث تم سرقة 300,000 دينار جزائري (حوالي 2,200 دولار أمريكي) من حسابه، هذه الخسارة كانت لها تأثيرات سلبية على مستوى معيشته،

حيث اضطر إلى تقليص نفقاته اليومية والبحث عن مصادر دخل إضافية (المركز الوطني للأمن السيبراني، 2021، ص. 30) .

❖ التأثير النفسي :تشير الدراسات إلى أن الأفراد الذين يتعرضون لجرائم إلكترونية يعانون من مشاعر القلق والاكتئاب، وفقًا لدراسة أُجريت في الجزائر، وجد أن **40%** من الضحايا أبلغوا عن صعوبات نفسية مستمرة مثل الأرق والقلق الشديد بعد تعرضهم للسرقة الإلكترونية، مثل هذه التجارب قد تؤدي إلى تدهور الصحة النفسية والاعتماد على المساعدة الطبية (المنظمة العربية للتنمية الإدارية، 2022، ص. 50).

❖ فقدان الخصوصية :سرقة البيانات الشخصية تؤدي إلى فقدان الخصوصية، مما يشعر الأفراد بعدم الأمان، على سبيل المثال، في إحدى حالات الاختراق، تم تسريب بيانات 1,500 عميل في بنك جزائري، مما أدى إلى تعرض هؤلاء الأفراد لمخاطر كبيرة تتمثل في استخدام معلوماتهم في أنشطة احتيالية (وزارة البريد والمواصلات السلكية واللاسلكية، 2022، ص. 15).

❖ القلق المستمر :مع تزايد الجرائم السيبرانية، يشعر الأفراد بقلق دائم بشأن أمان معلوماتهم الشخصية، وفقًا لاستطلاع أُجري في الجزائر، أظهر أن **55%** من المواطنين لا يثقون في أمان المعلومات المقدمة عبر الإنترنت، العديد منهم بدأوا في تجنب التعاملات الإلكترونية أو استخدام الإنترنت بشكل أقل (جيماوي، 2021، ص. 140).

❖ تأثيرات اجتماعية :الجرائم السيبرانية قد تؤدي إلى العزلة الاجتماعية، العديد من الضحايا قد يتجنبون استخدام وسائل التواصل الاجتماعي أو الإنترنت، مما يؤدي إلى فقدان الروابط الاجتماعية والشبكات التي تعتبر ضرورية في العصر الرقمي.

11.2.الانعكاسات على المجتمع الجزائري:

❖ تآكل الثقة في المؤسسات :تعزز الجرائم السيبرانية من فقدان الثقة في المؤسسات الحكومية والخاصة، وفقًا لتقرير المركز الوطني للأمن السيبراني، يشعر **70%** من المواطنين بأن المؤسسات لم تكن قادرة على حماية بياناتهم، مما يجعلهم مترددين في الاعتماد على الخدمات الإلكترونية (المركز الوطني للأمن السيبراني، 2021، ص. 22).

❖ التأثير على النمو الاقتصادي :تؤثر الجرائم السيبرانية سلبًا على الاقتصاد الوطني، في الجزائر، تكبدت الشركات خسائر تُقدر بحوالي 500 مليون دينار جزائري بسبب الجرائم السيبرانية في عام 2021 (المركز الوطني للأمن السيبراني، 2021، ص. 25)، يؤدي ذلك إلى تأثيرات غير مباشرة على الاستثمار الأجنبي والقدرة التنافسية للاقتصاد الوطني.

❖ تعزيز الفجوة الرقمية :تُظهر الدراسات أن **30%** من الشباب الذين يفتقرون إلى المعرفة بالأمن السيبراني كانوا عرضة للاختراقات، هذا يعكس كيف تعزز الجرائم السيبرانية الفجوة الرقمية بين الأفراد الذين يمتلكون المهارات التقنية والذين لا يمتلكونها، مما يؤدي إلى زيادة الفقر والعزلة الاجتماعية (وزارة التعليم العالي والبحث العلمي، 2022، ص. 30).

❖ زيادة التكاليف الأمنية :نتيجة لتزايد الجرائم الإلكترونية، يتعين على المؤسسات الحكومية والخاصة استثمار موارد كبيرة في تحسين الأمن السيبراني. تشير التقارير إلى أن التكاليف الأمنية زادت بنسبة **40%** في عام 2021 مقارنة بالعام السابق، مما يؤثر على الميزانية العامة ويشتت الموارد (الجزائر 24، 2021، ص. 10).

❖ الانعكاسات الاجتماعية :هناك زيادة في السلوكيات الإجرامية نتيجة للجرائم الإلكترونية، تم الإبلاغ عن أن **20%** من ضحايا الجرائم الإلكترونية اتخذوا إجراءات انتقامية ضد المجرمين، مما يساهم في تفشي العنف في المجتمع (الجزائر 24، 2021، ص. 12).

12. سبل الوقاية والعلاج:

☒ التوعية والتثقيف:

- تدريب الأفراد :يجب تنظيم ورش عمل ودورات تدريبية لتعليم الأفراد كيفية حماية أنفسهم على الإنترنت، يشمل ذلك كيفية استخدام كلمات مرور قوية، وتجنب النقر على الروابط المشبوهة، والتمييز بين الرسائل الحقيقية والمزيفة.

- برامج التوعية في المدارس :ينبغي إدخال مناهج دراسية تشمل الأمن السيبراني في المدارس، حيث يتم تعليم الطلاب المخاطر المرتبطة باستخدام الإنترنت وكيفية حماية بياناتهم الشخصية.

☒ **تعزيز الأمن الشخصي:**

- استخدام برمجيات الحماية :يُنصح الأفراد بتحميل وتحديث برمجيات الحماية من الفيروسات والبرمجيات الخبيثة بشكل دوري.

- تفعيل المصادقة الثنائية :يساعد تفعيل خاصية المصادقة الثنائية على توفير طبقة إضافية من الأمان عند الدخول إلى الحسابات الإلكترونية.

☒ **تأمين المؤسسات:**

- تحديث الأنظمة :يتعين على المؤسسات تحديث أنظمتها وبرامجها بشكل دوري لسد الثغرات الأمنية، يُعتبر استخدام برامج أمان متقدمة مثل جدران الحماية ضروريًا لحماية البيانات.

- التدقيق الأمني :ينبغي إجراء عمليات تدقيق أمني دورية لاكتشاف أي ثغرات أو نقاط ضعف في الأنظمة وتقييم مدى فعاليتها.

☒ **الشراكة بين القطاعين العام والخاص:**

- التعاون بين الحكومة والشركات :يجب تعزيز التعاون بين الحكومة والشركات الخاصة لتطوير استراتيجيات شاملة لمواجهة الجريمة الإلكترونية، يمكن أن تشمل هذه الاستراتيجيات تبادل المعلومات حول التهديدات السيبرانية وتطبيق أفضل الممارسات.

☒ **الإطار القانوني:**

- تطوير القوانين :يتعين على الحكومة تطوير قوانين تتعلق بالجريمة الإلكترونية وتطبيق عقوبات رادعة ضد مرتكبيها، ينبغي أن تشمل هذه القوانين أيضًا حماية بيانات الأفراد.

- تحسين آليات التحقيق :يجب تحسين قدرات الشرطة ومراكز الأمن السيبراني على التحقيق في الجرائم الإلكترونية، يتطلب ذلك التدريب على تقنيات التحقيق المتقدمة واستخدام أدوات تحليل البيانات.

☒ **الدعم النفسي للضحايا:**

- توفير خدمات الدعم النفسي :من المهم أن توفر المؤسسات الحكومية والمراكز الاجتماعية الدعم النفسي للضحايا، لمساعدتهم في التغلب على آثار الجرائم السيبرانية.

- خطوط مساعدة :ينبغي إنشاء خطوط مساعدة لمساعدة الأفراد الذين تعرضوا للاختراق أو الاحتيال، حيث يمكنهم الإبلاغ عن الجرائم وتلقي الدعم.

☒ تعزيز ثقافة الأمان في المجتمع:

- إقامة حملات توعية مجتمعية :يمكن تنظيم حملات توعية مجتمعية لنشر الوعي حول مخاطر الجريمة الإلكترونية وسبل الحماية، تشمل هذه الحملات توزيع مواد تعليمية عبر وسائل الإعلام المحلية والمواقع الإلكترونية.

13. توصيات الدراسة :

1) تعزيز الوعي والتثقيف:

- تطوير برامج تعليمية :ينبغي تطوير برامج تعليمية متخصصة حول الأمن السيبراني في المدارس والجامعات لتعريف الطلاب بالمخاطر المرتبطة باستخدام الإنترنت وسبل الحماية المناسبة.

- حملات توعية مجتمعية :تنفيذ حملات توعية مستمرة في المجتمع لرفع مستوى الوعي حول الجرائم الإلكترونية، وكيفية التعرف على الأساليب الاحتيالية وطرق الوقاية.

2) تفعيل التعاون بين الجهات الحكومية والخاصة:

- شراكات استراتيجية :تعزيز الشراكات بين الحكومة والقطاع الخاص لتبادل المعلومات حول التهديدات السيبرانية وتطوير استراتيجيات مشتركة لمكافحة الجرائم الإلكترونية.

- إنشاء منصة معلوماتية :إنشاء منصة معلوماتية وطنية تتضمن معلومات حول الجرائم السيبرانية، بما في ذلك أنماط الهجمات الجديدة وتوجيهات للوقاية.

3) تطوير الإطار القانوني:

- تحديث القوانين :مراجعة وتحديث القوانين المتعلقة بالأمن السيبراني لتتوافق مع التغيرات السريعة في تكنولوجيا المعلومات وجرائم الإنترنت.

- تطبيق العقوبات الرادعة :تعزيز تطبيق العقوبات الرادعة ضد مرتكبي الجرائم الإلكترونية لضمان حماية البيانات والمعلومات الشخصية.

4) تعزيز الأمن السيبراني في المؤسسات:

- تحديث الأنظمة :يتعين على المؤسسات تحديث أنظمتها وبرامجها الأمنية بشكل دوري، وتطبيق بروتوكولات الأمان المتقدمة لحماية البيانات.

- تدريب الموظفين :إجراء تدريبات دورية للموظفين حول كيفية التعرف على التهديدات السيبرانية وكيفية التصرف في حالة حدوث اختراق.

5) دعم الضحايا:

- توفير خدمات الدعم النفسي :يجب توفير الدعم النفسي للضحايا الذين تعرضوا للجريمة الإلكترونية، لمساعدتهم في التغلب على الآثار النفسية السلبية.

- إنشاء خطوط مساعدة :إنشاء خطوط مساعدة وطنية لتقديم الدعم والإرشاد للضحايا، مما يمكنهم من الإبلاغ عن الجرائم وتلقي المساعدة اللازمة.

6) تعزيز التعاون الدولي:

- المشاركة في الاتفاقيات الدولية :الانضمام إلى الاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإلكترونية وتبادل المعلومات والخبرات مع الدول الأخرى في هذا المجال.

- تنظيم مؤتمرات وندوات :تنظيم مؤتمرات وندوات دولية لمناقشة التحديات والتهديدات المتعلقة بالأمن السيبراني، وتبادل المعرفة والخبرات.

14.خاتمة :

تعد الجريمة السيبرانية من أخطر التحديات التي تواجه الأمن الاجتماعي والاقتصادي في العصر الحديث، حيث تتجاوز آثارها الخسائر المالية لتشمل أضرارًا نفسية واجتماعية، ومع تطور التكنولوجيا، أصبحت هذه الجرائم أكثر تعقيدًا، كما يتضح في حادثة "فيجر" التي كشفت عن تهديدات خطيرة للأمن القومي من خلال التجسس الإلكتروني، يعاني الأفراد في الجزائر من فقدان الثقة بالتكنولوجيا خوفًا من اختراق خصوصياتهم، ما يؤثر على استخدامهم الآمن للخدمات الرقمية ويحدّ من مشاركتهم في المجتمع الرقمي.

تخلق هذه الجرائم إحساسًا مستمرًا بالقلق والتوتر، مما يؤثر سلبًا على حياة الأفراد الشخصية والمهنية، كما أن تعرض الأسر للاحتيال الإلكتروني يؤدي إلى توترات داخلية بسبب الضغوط النفسية والمالية، مما ينعكس سلبًا على العلاقات الأسرية، وتساهم الجريمة السيبرانية في توسيع الفجوة الرقمية، حيث يتمتع الأفراد الذين لديهم خبرة في الأمن السيبراني بحماية أكبر، بينما تزداد معاناة الفئات الأقل معرفة، ما يؤدي إلى تهميش اجتماعي واقتصادي.

تؤثر هذه الجرائم أيضًا على الثقة بين المواطنين والمؤسسات، حيث يتردد كثيرون في استخدام الخدمات الإلكترونية الحكومية أو البنكية خوفًا من الاختراق، مما يضعف من فعالية الدولة في تقديم خدماتها، وقد يدفع هذا الوضع بعض الضحايا إلى البحث عن الانتقام بطرق غير قانونية، مما يعزز من حالة الانفلات الاجتماعي.

لذلك، يتطلب التصدي لهذه الجرائم استجابة شاملة من جميع الأطراف المعنية، من خلال تعزيز الوعي المجتمعي وتحسين الأطر القانونية والتقنية لضمان حماية الأفراد والمؤسسات من تهديدات الجريمة السيبرانية المتزايدة.

14.قائمة المراجع:

1. Federal Bureau of Investigation. (2020). 2020 Internet Crime Complaint Center (IC3) Report. Récupéré de https://www.ic3.gov ,p. 3.

2. جيماوي، نتيجة. (2021). الجريمة الإلكترونية وأثرها على الأمن الاجتماعي. مجلة دفاتر المخبر، (16)، 130-140. ص. 140.

3. أون، عائشة. (2020). الأمن السيبراني وتأثيراته على المجتمع. مجلة الأمن السيبراني. ص. 68.

4. McGuire, M. & Dowling, S. (2013). Cyber Crime: A Review of the Evidence. London: Home Office, p. 9.

5. Bertino, E. & Sandhu, R. (2010). Cybersecurity: Concepts, Challenges, and Opportunities. Computer, 43(10), 42-49. p. 42.

6. Smith, R. (2019). Understanding Identity Theft: The Impacts and the Solutions. Cybersecurity Review, 15(3), 200-210. p. 205.

7. Cheng, L. Liu, Y. & Yao, Y. (2017). A Survey on Cybersecurity. Journal of Computer Science and Technology, 32(1), 121-134. p. 130.

8. Kumar, A. & Somani, A. (2018). Cyber Crime: Its Types, Causes, and Prevention. International Journal of Cyber Criminology, 12(1), 80-90. p. 82.

9. OSCE. (2006). The OSCE Strategy to Address Threats to Security and Stability in the Twenty-First Century. p. 5.

10. Cybercrime Magazine. (2021). Cybercrime to Cost the World $6 Trillion Annually by 2021. Retrieved from Cybercrime Magazine.

11. Kumar, A. & Somani, A. (2018). Cyber Crime: Its Types, Causes, and Prevention. International Journal of Cyber Criminology, 12(1), 80-90. p. 85.

12. المركز الوطني للأمن السيبراني. (2021). تقرير الأمن السيبراني في الجزائر. ص. 12.

13. وزارة البريد والمواصلات السلكية واللاسلكية. (2022). تقرير حول الأمن السيبراني في الجزائر. ص. 8.

14. أحمد، بوشمال. (2021). الجرائم السيبرانية: الواقع والتحديات في الجزائر. مجلة الدراسات القانونية، 5(3)، 45-60. ص. 45.

15. المركز الوطني للأمن السيبراني. (2021). تقرير الأمن السيبراني في الجزائر. ص. 30

16. وزارة الداخلية والجماعات المحلية. (2022). تقرير حول الجرائم الإلكترونية. ص. 10.

17. المنظمة العربية للتنمية الإدارية. (2022). تأثير الجرائم الإلكترونية على الأفراد والمجتمعات العربية. تقرير إحصائي. ص. 50.

18. وزارة التعليم العالي والبحث العلمي. (2022). تقرير حول التعليم والأمن السيبراني في الجزائر. ص. 30.
19. Cybersecurity Ventures.(2020). Retrieved from Cybersecurity Ventures.
20. جيماوي، نتيجة. (2021). الجريمة الإلكترونية وأثرها على الأمن الاجتماعي. مجلة دفاتر المخبر. ص. 140.
21. المركز الوطني للأمن السيبراني. (2021). تقرير الأمن السيبراني في الجزائر. ص. 30.
22. المركز الوطني للأمن السيبراني. (2021). تقرير الأمن السيبراني في الجزائر. ص. 22.
23. المركز الوطني للأمن السيبراني، 2021، ص. 25.