اتجاهاتُ الشَّبابِ السُّعُوديِّ نحو الجرائمِ السَّيبرانيَّةِ وخُطُورتِها

دراسةٌ ميدانيةٌ

د/ عبد الرحمن بن سالم بن فهاد الطريف

أستاذ مساعد علم الاجتماع ــ قسم علم النفس

كلية العلوم والدراسات الإنسانية بشقراء ــ جامعة شقراء.

مُلخصُ الدِّراسة:

إنَّ الوعيَ بالجرائمِ السَّيبرانيةِ بينَ الشَّبابِ السُّعُوديِّ أمرٌ هامٌّ، خاصَّةً وأنَّ استخدامَ الإنترنتِ أصبحَ نمطَ حياةِ اليومِ. وبالتَّالي، يجبُ أن يكونَ الوعيُ بالجريمةِ السَّيبرانية جزءاً من ضرورةِ حياةِ المجتمعاتِ المعاصرةِ. ومن هُنا، حاولتْ الدِّراسةُ فهمَ مدى إدراكِ الشَّبابِ السُّعُوديِّ واتجاهاتِهم نحوَ خُطُورةِ الجرائمِ السَّيبرانيَّة، والتَّفاعُلاتِ عبرَ الفضاءِ السَّيبرانيّ، واعتمدتْ الدِّراسةُ في تحليلاتِها على عينةٍ غيرِ احتماليَّةٍ بلغَ حَجْمُهَا (٣٠٠) مفردةً تمَّ جمعُها من الشَّبابِ الجامعيِّ في الفئةِ العُمْريةِ ١٨-٢٤ سنةً التي تدرسُ الآنَ في المرحلةِ الجامعيَّة، من الذُّكُورِ بجامعةِ شقراء .

وخلصتْ الدِّراسةُ إلى أنَّ من أخطارِ الجرائمِ السَّيبرانيةِ من وجهةِ نظرِ عينةِ الدِّراسةِ تشويهَ السُّمعةِ والإضرارِ بها، وتَعرُّضَ أفرادِ المجتمعِ إلى الابتزازِ، والتي جاءت في المرتبةِ الأُولى بنسبةِ ٩٦٪ ومتوسطٍ حسابيٍّ ١.٩٢، وهو ما يعكسُ حجمَ الخطرِ الذي يحيطُ بأفرادِ المجتمعِ نتيجةَ انتشارِ الجرائمِ السَّيبرانيةِ وتزايدِ مُعدلاتِهَا، كما أوضحتْ نتائجُ الدِّراسةِ أنَّ الوسائلَ الأكثرَ تأثيراً في نشرِ الجريمةِ السَّيبرانيةِ من وجهةِ نظرِ عينةِ الدِّراسةِ كان الاستخدامَ المستمرَّ لمواقعِ التَّواصُلِ الاجتماعيِّ بنسبةِ ٩٩.٥٪ ومتوسطٍ حسابيّ بلغ ١.٩٧، وأنَّ الشَّبابَ هم الفئةُ الأُولى المُستهدَفَةُ من الجرائمِ السَّيبرانيةِ بنسبةِ ١٠٠٪ ومتوسطٍ حسابيٍّ] بلغ ٢.٠.

الكلماتُ المفتاحيَّةُ: الجرائمُ السَّيبرانيَّةُ ــ الإيذاءُ السَّيبرانيُّ ــ الجريمةُ الإلكترونيّةُ ــ جرائمُ الحاسُوبِ .

أولاً : مُقدمَةُ الدِّراسة :

ما نشهده اليوم من سباق تكنلوجي من خلال التقنيات والتطبيقات ووسائل التواصل الاجتماعي الذي أصبح وجودها جزءاً تكاملياُ من وجودنا البشري . فلا نستغني عن التكنلوجيا في جوانب حياتنا المختلفة . فلا يوجد بين الانسان والتقنية حدود مانعة يقف عندها ولا بين ماهو في الحقيقة أو العالم الافتراضي كذلك .

فالتَّمييزُ الزائفُ بينَ الفضاءِ الافتراضيِّ والحقيقيِّ يُعرِّضُ أفرادَ المجتمعِ إلى تهديداتٍ سَيبرانيةٍ عديدةٍ (Leukfeldt, Yar, 2016;2) فتطوُّرُ تكنولوجيا المعلوماتِ والاتصالاتِ قد أحدثَ تحولًا في العالمِ، وأَثَّر على مجالاتٍ عديدةٍ ومتنوعةٍ، بما في ذلك: المجالاتِ الاجتماعيةِ، والثَّقافيَّةِ، والاقتصاديَّةِ، والسِّياسيَّةِ، وهو ما أدَّى إلى انتشارِ الجريمةِ بينَ الشَّبابِ (ابن شفلوت، ٢٠١٨: ٩٦١).

وقد أوجدتْ هذه التَّطوراتُ التُّكنولوجيةُ أيضًا فُرصًا لا حصرَ لها للجُناةِ لارتكابِ مُختلَفِ أشكالِ الجريمةِ، ويكادُ يكونُ من المستحيلِ تقديرُ حجمِ الجرائمِ الإلكترونيةِ التي تحدثُ في معظمِ الدُّولِ في جميعِ أنحاءِ العالمِ؛ بسببِ الافتقارِ إلى تعريفاتٍ قانونيّةٍ مُوحَّدةٍ لهذه الجرائمِ، ونُدرةِ الإحصاءاتِ الرَّسميَّةِ الصَّالحةِ والموثُوقةِ. ومع ذلك، تُظْهِرُ الدِّراساتُ أنَّ معدلاتِ الجرائمِ السَّيبرانيةِ آخذةٌ في الازديادِ معَ استمرارِ انخفاضِ مُعدَّلاتِ العديدِ من أشكالِ الجرائمِ التَّقليديّةِ (Bossler & Berenblum, 2019;496) وهذا النَّوعُ من الجرائمِ المعاصرةِ، يثيرُ العديدَ من الإشكالاتِ المرتبطةِ باكتشافِ الجريمةِ وإثباتِها، خاصّةً مع تَعقُّدِ الأدواتِ الرَّقميّةِ وتِقنياتِها المُتعدِّدةِ، هذا فضلاً عن الفضاءِ السَّيبرانيِّ غيرِ المحدودِ في الزمانِ والمكانِ(الخنين، ٢٠٠٨: ٢٨٤).

إنَّنَا نعيشُ الآنَ في "مجتمعِ معلوماتٍ"، أو "عصرِ معلوماتٍ"، أو "مجتمعٍ افتراضيٍّ"، أو مجتمعٍ ما بعدَ الصِّناعةِ"، أو "مجتمعِ المعرفةِ"، أو "مجتمعِ الشَّبكةِ"، وتُوضِّحُ جميعُ هذه التَّسمياتِ التَّحولَ في القُوةِ التَّحويليةِ التي توفرُها تكنولوجيا المعلوماتِ والاتصالاتِ لإعادةِ تشكيلِ، وإعادةِ تنظيمِ العملِ البشريِّ والتَّفاعُلِ، ممَّا يَخلُقُ نظامًا اجتماعيًّا جديدًا يختلفُ اختلافًا ملحوظًا عن سابقيه. وفيما يتعلقُ بمسائلِ الجريمةِ والانحرافِ، بدأت تتظافَرُ جهودُ علماءِ الجريمةِ في الآونةِ الأخيرةِ في الاهتمامِ متضافرِ في الطُّرقِ التي يغيرُ بها عصرُ

المعلوماتِ طبيعةَ، وأنماطَ السُّلوكِ الذي يخرِقُ القانونَ، وكيف يتمُّ طرحُ تحديات جديدة، وغيرِ مسبوقةٍ لمنعِ الجريمةِ، ومكافحتِها؟ (Yar,2012;1) بل إنَّهُ يمكنُ القولُ أنَّ التَّطورَ التكنولوجيَّ المذهلَ ذاته قد خلقَ أشكالًا جديدةً من الجريمةِ، وعالماً جديداً من المجرمينَ بخصَالٍ وسماتٍ جديدةٍ، سماتِ المجتمعِ الرقميِّ(الألفي، ٢٠١٠: ٤٧) بل إنَّ هذه التِّقنيات شَجَّعَتْ من انخراطِ الكثيرِ من المجرمينَ، وأزَدَاتْ أعدادَهم، وحجمَ جرائمِهم السَّيبرانيةِ عبرَ الفضاءِ الإلكترونيِّ(الطحاوي، ٢٠٠٨: ٣٦٥). ويمكنُ القولُ أنَّ الجريمةَ السَّيبرانيةَ قد تَطوَّرَتْ ونَمَتْ بشكلٍ مُوازٍ لتطورِ ونُمُوِّ الشبكاتِ الإلكترونيةِ، والقواعدِ المعلوماتيةِ(التايب، ٢٠٠٨: ١٤٥).

لقد أصبحتْ الجرائمُ السَّيبرانيةُ من التَّحدياتِ، والتَّهديداتِ الأمنيةِ المُستجدَّة، والتي تنعكسُ بمخاطرَ أمنيةٍ عديدةٍ على النَّسقِ العالميِّ؛ نتيجةَ الاستخدامِ المفرطِ لتكنولوجيا الاتصالاتِ، والإنترنتِ فائقِ السُّرعةِ، وهو ما ينعكسُ كذلكَ على حالةِ الأمنِ الاجتماعيِّ (حيمد، ٢٠١٩: ٨٣) فالتطوراتُ التُّكنولوجيةُ الفائقةُ، والاستخدامُ المفرطُ لمواقعِ التَّواصلِ الاجتماعيِّ ساعدَ في تغييرِ شكلِ الجريمةِ، وأساليبِ ارتكابِها ووقتِ ارتكابِها، وسياقِ تنفيذِ الجريمةِ ذاتِها (محمود، ٢٠١٥: ٣٥) ويمكنُ تفسيرُ ظُهورِ الفضاءِ الإلكترونيِّ الذي يُمكنُ الوصولُ إليه في سلسلةٍ من التَّغييراتِ الهَامَّةِ في مُعدَّلِ انتشارِ الإنترنتِ، ومُستخدميه.

وتشملُ العناصرُ الرئيسيةُ التي تميزُ هذا الارتفاعَ الملحوظَ خفضَ رُسُومِ تصفُّحِ الإنترنت، وتطويرَ تكنولوجيا الإنترنتِ لتوسيعِ النِّطاقِ التَّردُّديِّ، وزيادةَ سرعةِ الإنترنتِ وموثُوقيته. ووفقًا للاتحادِ الدُّوليِّ للاتصالاتِ، فقد تغيَّرَ عددُ الأفرادِ الذين يستخدمونَ الإنترنتَ بشكلٍ كبيرٍ في جميعِ أنحاءِ العالَمِ في العُقُودِ الثلاثةِ الماضيةِ، ففي عامِ ١٩٩٠ م لم يستخدمْ الإنترنتَ سوى ٠.٠٤٩٪ من سُكانِ العالَمِ، وبحلولِ عامِ ٢٠١٦ م كان ٤٥.٨٪ من سكانِ العالمِ متصلينِ بالإنترنتِ.

في المُجمَلِ، يُشكِّلُ تطورُ الفضاءِ الإلكترونيِّ، واستخدامُ الحواسيبِ في الأنشطةِ الإجراميةِ تحدياتٍ كبيرةً أمامَ القانونِ الجنائيّ، وتبينُ الإحصاءاتُ المتعلقةُ بالإبلاغِ عن هذا النَّوعِ من الجرائمِ وملاحقته قضائيًّا أنَّ صُكُوكَ العدالةِ الجنائيةِ التَّقليديّةِ ليست أدواتٍ كافيةً لقمعِ الإجرامِ السَّيبرانيِّ على نحوٍ فَعَّالٍ. وعلى عكسِ الجرائمِ الجنائيةِ التَّقليديةِ

في(العَالَمِ المادي)، تَتَّسمُ الجرائمُ السَّيبرانيةُ بالإيذاءِ الجماعيِّ، والوُصُولِ العالَمِيِّ، والانفصالِ الإقليميِّ بينَ الفعلِ والعواقبِ، والأعمارِ الأصغرِ للمُجْرمينِ، والفَجواتِ في التَّشريعاتِ الجنائيةِ بسببِ التَّطوّرِ التُّكنولوجيِّ المُستمرِّ.

وتنعكسُ المشاكلُ الإجرائيةُ في نقصِ الإبلاغِ عن الجرائمِ السَّيبرانيةِ، والصُعُوباتِ في كشفِ الجُناةِ وجمعِ الأدلةِ الرَّقميةِ، والمُعضلاتِ القضائيةِ، والافتقارِ إلى المعرفةِ التِّقنيةِ من جانبِ الجهاتِ الفاعلةِ الإجرائيةِ، لذلك، فإنَّ جميعَ الجُهُودِ المبذولةِ لمكافحةِ الإجرامِ السَّيبراني لا يُمكنُ أنْ تحقِّقَ نتائجَ مُرضيَّةً طالما أنَّنا نستخدمُ أدواتٍ قديمةً في البيئةِ السَّيبرانيةِ الجديدةِ(Bajovic,2017;99) ومن هذا المنطلقِ، كانت هذه الدِّراسةُ التي اعتبرتْ الجريمةَ السَّيبرانيةَ هي التَّهديدُ الرَّئيسيُّ لمجتمعِنا اليومَ من جميعِ النَّواحيّ: الحياةِ الاجتماعيةِ، انتهاكِ الخُصُوصيةِ، وسَرقةِ الهَويّةِ، والجرائمِ الماليّةِ، والاحتيالِ، والتَّحرُّشِ، والبَلطجةِ، والقذفِ، وأمنِ المجتمعِ، والحربِ الإلكترونيَّةِ(Viano,2017;18).

ثانيًا: مشكلةُ الدِّراسةِ وتساؤلاتُها:

لقد أصبحتْ الجريمةُ السَّيبرانيةُ الآنَ واحدةً من أهمِّ التَّحدياتِ التي تُواجهُ مُجتمعاتِنَا المعاصرةَ؛ فالفضاءُ الإلكترونيُّ يتيحُ للشَّبابِ فرصَ التَّسلُّلِ، والتَّفاعُلِ عبرَ هذا الفضاءِ، ومن ثَمَّ تعرضُهُم للانخراطِ في النَّشاطِ الجنائيِّ السَّيبرانيّ، وذلك من خلالِ الاستفادةِ من المصادرِ المفتوحةِ، وغيرِ الخاضعةِ للرقابةِ، والتي تُوِّفُر المعلوماتِ، والأدواتِ حولَ كسرِ الشَّفرةِ، واختراقِ الشَّبكةِ، والقرصنةِ، وإجراءاتِ التَّصيُّدِ الاحتياليِّ (Aiken & Davidson,2016:5) والتَّجسُّسِ السَّيبرانيِّ من خلالِ توظيفِ البرمجياتِ الخبيثةِ في اختراقِ الهواتفِ الذَّكيةِ، والشَّبكاتِ الرَّقميَّةِ.

وفي الوقتِ الحاضرِ، تَتَزايدُ الجريمةُ السَّيبرانيةُ بسرعةِ يومٍ بعدَ يومٍ مع تطوُّرِ التُّكنولوجيا، حيثُ تَتَّخذُ خُطوةً نحوَ العَالَمِ الرَّقميَّ، ومعَ كُلِّ خُطْوةٍ، تنشأُ أيضًا تحدياتٌ ومسؤولياتٌ جديدةٌ يوميًّا. وتُعَدُّ شريحةُ الشَّبابِ والمُراهقونِ هم الفئةُ المُستهدَفةُ من الهُجُومِ السَّيبرانيِّ؛ لسببٍ يرتبطُ بأنَّهُم الشَّريحةُ الأكثرُ كثافةً في الاستخدامِ الرَّقميِّ والتَّفاعُلِ عبرَ الفضاءِ الإلكترونيِّ، ومن هُنَا تُشكِّلُ الجريمةُ السَّيبرانيةُ تهديدًا رئيسيًّا للمجتمعِ العَالَمِيِّ؛ فكُلُّ بلدٍ في العالمِ يُشجِّعُ ويُعزِّزُ التَّحوُّلَ الرَّقميَّ، والرَّقمنةَ للبقاءِ من أجلِ البقاءِ في هذا

العالمِ الرَّقميِّ(Meena et al,2020;177). والجريمةُ السَّيبرانيَّةُ هي مشكلةٌ عالميَّةٌ، وتُوجَدُ في كُلِّ بُلدانِ العالَمِ؛ حيثُ لا يُوجدُ بلدٌ مُحصَّنٌ منها، خاصَّةً وأنَّها مُرتبطةٌ بالفَضاءِ السَّيبرانيِّ المَفتوحِ، فَتَزايدُ الاتصالِ بالإنترنتِ في السَّنواتِ الأخيرةِ تَسبَّبَ في نُمُوِّ الأنشطةِ الإجراميةِ الإلكترونية، وبمُرورِ السَّنواتِ تَتَطوَّرُ الجرائمُ الإلكترونيةُ إلى جانبِ التَّطوُّرِ التِّقنيِّ، وبمُرورِ الوقتِ تنوَّعتْ الجريمةُ السَّيبرانيةُ وتَعقَّدَتْ، مثل: جرائمُ الاتصالاتِ السِّلكيةِ واللاسلكية، غَسيلُ الأَموالِ الإلكترونيِّ، قَضايا تزويرِ الهُويَّةِ عبرَ الإنترنت، الغشُّ في حَالةِ عدمِ وُجودِ بطاقةٍ، حَوَادثُ جَسَديةٍ ومُضايقات، حَالاتٌ مُتَعلِّقةٌ بجِنسِ الأَطفالِ..... إلخ(Kamruzzaman et al, 2016; 23).

هذا، وقد ازدادتْ البُحوثُ والدِّراساتُ حولَ الجريمةِ السَّيبرانية، ونَمتْ نُمُوًّا هائلاً على مدى العُقودِ القليلةِ الماضية؛ حيثُ ركَّزَ جزءٌ كبيرٌ من تلكَ البحوثِ في هذا المجالِ على استكشافِ كَيفيَّةِ اختلافِ طبيعةِ الجريمةِ السَّيبرانية، والفضاءِ الإلكترونيِّ عن الجريمةِ التَّقليديةِ، والفضاءِ الأرضيِّ. ومن التَّحدياتِ الكبيرةِ التي يواجهُهَا علماءُ الجرائمِ السَّيبرانيةِ ـــــــــ قديمًا وحديثًا ـــــــــ عدمُ وُجودِ إحصاءاتٍ رسميةٍ عن معظمِ أشكالِ الجرائمِ السَّيبرانية(Bossler & Berenblum, 2019;497) حيثُ تَتَدرَّجُ الجرائمُ السَّيبرانيةُ من الجرائمِ الأقلِّ خُطورةً، كالمضايقَاتِ، والمُلاحقةِ عبرَ البريدِ الإلكترونيِّ إلى الجرائمِ الأشدِّ خطرًا، كالاستدراجِ، والتَّشهيرِ، فضلاً عن صناعةِ الفيروساتِ الضَّارةِ ونشرِها، وُصولاً إلى الإرهابِ الإلكترونيِّ، ودعمِ الجماعاتِ التَّكفيريَّةِ (الفرجاني، ٢٠١٧: ٣٧) ومن ثَمَّ، تُعَدُّ الجرائمُ السَّيبرانيةُ أكثرَ خُطورةً من الجرائمِ التَّقليدية؛ نظراً لانتشارِها السَّريعِ والخفيِّ، واستهدافِها الفردَ، والمؤسساتِ، والمجتمعِ برُمَّتِه، ومن ثَمَّ، ترتفعُ الخسائرُ التي يَتَكَبَّدُهَا الفردُ والمجتمعُ في آنٍ واحدٍ(الصاعدي، ٢٠١٠: ٤) هذا، فضلاً عن تَعددِ أغراضِ الجرائمِ السَّيبرانية، وأشكالِها، وأدواتِها، كذلك تَعددِ مُرتكبِيها وتَنوُّعِهم، وهو ما يُصعبُ من التَّنبؤِ بها(سياب، ٢٠٠٩: ٢١٤).

أوضحتْ دراسةٌ (فوزي، ٢٠١٩) بأنَّ التَّكلفةَ الماديَّةَ التي سيتكبَّدُهَا العالمُ بسببِ انتشارِ الجرائمِ السَّيبرانيةِ في عام ٢٠٢١ ستُقَاربُ (٦) تريليون دولار، وهو ما يعني تضَاعُفَ هذا المبلغِ خلالَ خمسِ سنواتٍ، حيثُ بلغَ في عام ٢٠١٥ (٣) تريليون دولار،

وهو ما لا يَدعُ مجالاً للشَّكِّ حجمُ الخسائرِ الماديةِ الفادحةِ التي يَتَكبَّدُها الاقتصادُ العالميُّ بسببِ انتشارِ تلك الجرائمِ السَّيبرانيةِ في الفضاءِ الرَّقميِّ المفتوحِ، أما في فترةِ انتشارِ كوفيد ١٩ ، فالجريمةُ السَّيبرانيةُ تزايدت في عام ٢٠٢٠ في جميعِ أنحاءِ العالمِ، فضلاً عن حجمِ الآثارِ الاجتماعيةِ والنَّفسيةِ النَّاجمةِ عن انتشارِ تلك الجرائمِ المُتنوِّعةِ ذاتِ الطَّبيعةِ الصَّامتةِ والهادئةِ، حيثُ انتهاكِ الحُرمةِ الشَّخصيةِ، والحقوقِ الإنسانيةِ، ووُقُوعِ الكثيرِ من الضَّحايا لتلكَ الجرائمِ؛ نتيجةَ حداثةِ السِّنِّ، وانخفاضِ الخبْراتِ، والجهلِ بمُعطياتِ المجتمعِ الرَّقميِّ. كما أوضحتْ دراسةٌ (الصبان، ٢٠١٩) أنَّ الطُّلابَ والمُراهقينَ والأطفالَ هم أكثرُ الشَّرائحِ العُمريةِ استهدافاً في الجرائمِ السَّيبرانية، فهم الضَّحايا الحقيقيونَ لذلك النَّوعِ من الجرائمِ، خاصَّةً مع غيابِ الرِّقابةِ، والحمايةِ الأُسريةِ. كما أشارتْ دراسةٌ (Hutchins & Yiting, 2016) إلى أنَّ مُرتكبِي الجرائمِ السَّيبرانيةِ يَمتلكُونَ بعضَ القواسمِ المُشتركةِ، وأحدُ أبرزِ هذه العواملِ هو نوعُ الجنسِ، وغَالبيتُهم ذكورٌ، فضلاً عن إتقانِهم مهاراتِ استخدامِ النُّظمِ المعلوماتيةِ، ومواكبةِ التَّطوراتِ في البنيةِ التُّكنولوجيةِ (دريس، ٢٠١٧: ٢٩) فهم مُجرمونَ يمتلكونَ مَهاراتٍ، وقُدراتٍ خاصةٍّ، ويمتلكونَ معرفةً رقميةً مُميَّزةً، ويتمتَّعُونَ بذكاءٍ حادٍّ (سعيد، ٢٠١٩: ٣٣٨) وهُنا صَنَّفتْ بعضُ الدِّراساتِ الجرائمَ السَّيبرانيةَ إلى فئاتٍ مختلفةٍ، بما في ذلك التَّعدي الإلكترونيّ (على سبيلِ المثالِ، الوصولُ غيرُ المُصرَّحِ به للنِّظامِ)، والخداعِ الإلكترونيّ ، والسَّرقةِ (على سبيل المثال، سرقةُ الهُويةِ، والاحتيالُ عبرَ الإنترنتِ بالتَّغلغُلِ عبرَ المجالِ االافتراضيّ (أحمد، ٢٠٢٠: ١٠٩٨)، والقرصنةُ الرَّقميةُ والاستيلاءُ على البطاقاتِ الائتمانيةِ)(محمد، ٢٠٠١: ٧٠)، والإباحيةُ الإلكترونيةُ،ــ والفُحشُ (مثل، الاستغلالِ الجنسيّ للأطفالِ)(ايديو، ٢٠٢٠: ٣٤١)، والعُنفُ السَّيبراني (على سبيل المثالِ، المُطاردةُ الإلكترونيةُ، الإرهابُ السَّيبرانيِ)(Tcherni et al. 2016) حيثُ يَستهدفُ الإرهابُ السَّيبرانيُّ استغلالَ المجرمينَ لاختراقِ الأنظمةِ المدنيةِ والعسكريةِ، وهو ما يَنعكِسُ سلبيًّا على الأمنِ الوطنيِّ، والأمنِ العَالميِّ (كزبر، ٢٠١٨: ٢٩٥).

ومن ثَمَّ، تزدادُ التَّهديداتُ في شبكاتِ تُكنولوجيا المعلوماتِ، والاتصالاتِ، وتَتَنوعُ ويَتَغيرُ طَابعُها، وهَيكلُها مع تطورِ التُّكنولوجيا، ومشاركةِ المجتمعِ العالميِّ على نطاقٍ

أوسعَ في شبكاتِ تُكنولوجيا المعلوماتِ والاتصالات؛ فقد تَزايدَ عددُ مرتكبي الجرائمِ السَّيبرانيةِ عبرَ الفضاءِ الإلكترونيِّ، وهو ما يُضاعفُ من أعباءِ النُّظمِ الأمنيةِ، وطُرُقِ مُواجهتِها. وتَتَوقَّعُ عددٌ من الدِّراساتِ أنَّه يُمكنُ وُقوعُ جرائمَ ذاتِ طابعٍ إرهابيٍّ في المستقبلِ، بل إنَّ الهجماتِ على نُظمِ الحاسوبِ ستكونُ أكثرَ شُيوعًا، وتَستهدفُ أساسًا الأبنيةَ الأساسيةَ للمجتمعاتِ المُعاصرةِ، وتَفترضُ تلك الدِّراساتُ أنَّ الفضاءَ الإلكترونيِّ سيكونُ قريبًا السَّاحةَ الرَّئيسيةَ للهجماتِ الإرهابيةِ، والحُروبِ السَّيبرانيةِ (الرفادي، ٢٠١٨: ١٠)، ومن المُتَوقَّعِ في السَّنواتِ المُقبلةِ أنْ تكونَ الهجماتُ على نُظمِ الحاسوبِ أكثرَ شُيوعًا على نحوٍ مُتزايدٍ (Amberg,2017;68) وفي ضَوءِ ما تَقَدَّمَ، تَتَحدَّدُ مشكلةُ الدِّراسةِ في التَّساؤليينِ الآتيينِ: ما طبيعةُ اتجاهاتِ الشَّبابِ السُّعُوديِّ نحوَ الجرائمِ السَّيبرانية؟ وكيف يَنخرِطُ الشَّبابُ في الجرائمِ السيبرانيةِ؟ ويتفرعُ عن مشكلةِ الدِّراسةِ عددٌ من التَّساؤُلاتِ الفرعيةِ على النَّحوِ التَّاليِّ:

١. كيف يَتعاملُ الشَّبابُ مع المنصَّاتِ الرَّقميةِ؟ وما عَلاقةُ تلك المنصَّاتِ بانتشارِ الجرائمِ السَّيبرانية؟

٢. ما مفهومُ الجرائمِ السَّيبرانيةِ السَّائدُ بينَ الشَّباب؟ وما طبيعةُ تصوراتِ الشَّبابِ عن تلك الجرائمِ؟

٣. ما مدى وعي الشَّبابِ بالجرائمِ السَّيبرانيةِ وخُطُورتِهَا؟

٤. كيف يرى الشَّبابُ السُّعوديُّ دوافعَ ارتكابِ الجرائمِ السَّيبرانية؟

٥. كيف يُحدِّدُ الشَّبابُ المخاطرَ السَّيبرانيةَ، ويَنْظُرونَ إليها ويُعَانُونَ منها؟

ثالثًا: أهميَّةُ الدِّراسة :

تَظهرُ أهميةُ الدِّراسةِ من خلالِ مُساهمتِها في إثراءِ الأدبياتِ السُّوسيُولوجيةِ حولَ الجرائمِ السَّيبرانيةِ، وخُطورتِها الاجتماعيةِ، ورصدِ اتجاهاتِ، وتصوراتِ الشَّبابِ السُّعوديِّ بشأنِ تلك الجرائمِ التي تَزايدَ عددُ مُرتكبيها، وضحاياها في الآونةِ الأخيرةِ بشكلٍ واضحٍ، واتَّسعَ نطاقُ تأثيراتِها، وخُطورتِها في المجتمعِ المعاصرِ، وتَتَحدَّدُ أهميةُ الدِّراسةِ في النِّقاطِ الآتيةِ:

- إنَّ دراسةَ الجرائمِ السَّيبرانيةِ: الجرائمِ التي تَنطوي على استخدامِ تُكنولوجياتٍ رقميةٍ، وتَعتمدُ عليها في تخطيطِها وتنفيذِها، هي الآنَ مجالُ حديثٍ للبُحُوثِ في مجالِ سُوسيولوجيا الانحرافِ؛ فالجريمةُ السَّيبرانيةُ، والانحرافُ الرَّقميُّ هو العملُ الذي يجمعُ بينَ رُؤى علمِ اجتماعِ الجريمةِ، وعُلومِ الكُمبيوترِ لاستكشافِ الجرائمِ السَّيبرانيةِ، مثل: القرصنةِ، والتَّصيدِ، والاحتيالِ، جنبًا إلى جنبٍ مع أشكالٍ من الانحرافِ الإلكترونيِّ، مثل: إدمانِ الموادِّ الإباحيةِ، والإيذاءِ السَّيبرانيِّ.
- إنَّ حجمَ الجرائمِ السَّيبرانيةِ، وتَكلفتَها يَتزايدُ بمعدلِ خطرٍ على مجتمعِنا، ومن هُنا، كانت هناك حاجةٌ ماسَّةٌ إلى إجراءِ المزيدِ من الأبحاثِ، والدَّراساتِ التي تُساهمُ في منعِ الجريمةِ السَّيبرانيةِ، وتُعزِّزُ الأمنَ السَّيبرانيَّ من خلالِ صياغةِ سياساتٍ أمنيةٍ، واجتماعيةٍ، وتثقيفيةٍ، وتُفيدُ نتائجُ هذه الدِّراسةِ في دعمِ تلك السِّياساتِ.
- إنَّ الشَّبابَ في الغالبِ هم أكثرُ الشَّرائحِ العُمريةِ تعرُضًا للخطرِ المعلوماتيِّ، فهم ضحايا الجرائمِ السَّيبرانيةِ؛ فالشَّبابُ في تلك المرحلةِ أكثرُ ديناميكيةً، وانفعالاً، وتَفاعُلاً مع المجتمعِ الرَّقميِّ، ولديه التَّطلُّعُ والرَّغبةُ في التَّغييرِ، والاستجابةُ لكلِّ ما هو جديدٌ، ومن هُنا، كان الشَّريحةَ المُستهدفةَ بالدِّراسةِ، والتَّحليلِ في هذه الدِّراسةِ.
- أصبحت إدارةُ أمنِ الفضاءِ الإلكترونيِّ عُنصرًا هامًّا في إدارةِ الأمنِ الوطنيِّ في جميعِ أنحاءِ العالمِ، وقد لا تأتي الاختراقاتُ المستقبليةُ التي تُهدِّدُ أمنَنا الوطنيَّ بالضَّرورةِ عبرَ الحُدودِ البريةِ، أو في الفضاءِ الجويِّ، أو عبرَ المياهِ البحريةِ، ولكنَّها تَحدثُ في الفضاءِ الإلكترونيِّ، وهو ما يَدفعُنا للبحثِ حولَ الجرائمِ السَّيبرانيةِ، وخُطورتِها على أمننا القوميِّ.

رابعاً: أهدافُ الدِّراسةِ :

١. الكشفُ عن ملامحِ تَعاملُ الشَّبابِ السُّعوديِّ مع المنصاتِ الرَّقميةِ.
٢. الكشفُ عن المفهومِ السَّائدِ بينَ الشَّبابِ السُّعوديِّ حولَ مفهومِ الجرائمِ السَّيبرانيةِ.
٣. الوقوفُ على تصوراتِ الشَّبابِ السُّعوديّ حولَ الخُطورةِ الاجتماعيةِ للجرائمِ السَّيبرانيةِ.
٤. التَّعرُّفُ على دوافعِ ارتكابِ الجرائمِ السَّيبرانيةِ، ومُعدَّلِ انتشارِها بينَ الشَّبابِ.

خامساً: مفاهيمُ الدِّراسةِ :

١. الجرائمُ السَّيبرانيةُ :

صِيغَ مصطلحُ "الجريمة السيبرانية" لأولِ مرةٍ من قِبَل وليام جيبسون William Gibson في عامِ ١٩٨٢، ومنذُ ذلك الحين، اتَّسعت الحُدودُ التي تُحددُ الجريمةَ السَّيبرانية، فخلال نشأةِ (الجريمةِ السَّيبرانية) كمجالٍ، فَضَّلت الأجيالُ الأولى من العلماءِ، والمُنظماتِ مصطلحَ (جرائم الكمبيوتر)، بالمعنى الأضيقِ للجريمةِ السَّيبرانيةِ القائمةِ على الكمبيوتر، على (الجريمة السَّيبرانية) بالمعنى الأوسعِ للكلمةِ. وابتداءً، فإنَّ المفهومَ اللُّغويَّ للجرائمِ السيبرانيةِ يُركزُ على العَلاقةِ بينَ الجرائمِ، والفضاءِ المعلوماتيِّ المُتَّسع (الراظمي، ٢٠١٩: ٢٥). وقد عَرَّفَ المركزُ الوطنيُّ لجرائمِ الياقاتِ البيضاءِ الجرائمَ السَّيبرانيةَ بأنَّها: انتهاكٌ للقانونِ المُتعلِّق بجهازِ الكمبيوتر، ومحتوى، وأنظمةِ التَّشغيلِ، والتي تَتَضمنُ عادةً: الوصولَ إلى أنظمةِ الكمبيوتر بدونِ إذن، وإتلافَ أنظمةِ الكمبيوتر، والحصولَ على معلوماتٍ مُخزَّنةٍ على أنظمةِ الكمبيوتر بدون تصريحٍ (Choi et al, 2020;32) فالجريمةُ السيبرانيةُ شرٌّ لابدَ من مكافحته (Pasculli,2020;49).

وتفهمُ عمومًا الجرائمَ السيبرانيةَ، والتي يُطلقُ عليها (جرائمُ الحاسوب)، و(الجريمةُ الرَّقميةُ)، وجرائمُ الإنترنت)، (والجريمةُ المتطورةُ)، والتي تشملُ طائفةً واسعةً من الأنشطةِ الإجراميةِ التي تَستخدمُ الحواسيبَ، والأجهزةَ الرَّقميةَ، والإنترنتَ. وعلى الرّغمِ من خُطورةِ، وتزايدِ الجريمةِ السَّيبرانية، إلا أنَّه لا يُوجدُ تعريفٌ مقبولٌ عالميًّا في الأدبياتِ للجريمةِ السَّيبرانية، حيثُ يُصنِّفُ معظمُ الباحثينَ الجرائمَ الإلكترونيةَ على أساسِ دورِ التُّكنولوجيا، وطريقةِ العملِ الإجرامية. جرائمُ الكمبيوتر (أو الجرائمُ السَّيبرانيةُ "الحقيقية")، مثل: القرصنةُ، والحرمانُ من الخدمة، وإنتاجُ البرمجياتِ الخبيثةِ التي تكونُ فيها أنظمةُ، وشبكاتُ الكمبيوترِ هدفًا للنَّشاطِ الإجراميِّ، و (الجرائمُ المتعلقةُ بالكمبيوتر، حيثُ تُستخدَمُ أجهزةُ الكمبيوترِ كأدواتٍ للجريمةِ غيرِ الرَّقمية، مثل: التَّزويرُ، أو الاحتيالُ، أو الاعتداءُ الجنسيُّ على الأطفالِ، أو انتهاكِ حُقوقِ الطَّبعِ والنَّشرِ (Aiken & Davidson,2016: 5). ولذلك يُمكنُ النَّظرُ إلى الجريمةِ السَّيبرانيةِ على أنَّها مصطلحٌ جامعٌ شاملٌ يشملُ الجريمةَ بمساعدةِ الحاسوبِ التي تُستخدَمُ فيها الحواسيبُ، والتُّكنولوجيا في دورٍ داعمٍ،

مثل: استخدامُ الحاسوبِ لإرسالِ رسائلَ مضايقةٍ. وفي الوقتِ نفسِه، يَشملُ مصطلحُ الجرائمِ السيبرانيةِ أيضًا الجرائمَ التي تُركِّزُ على الحاسوب، والتي هي نتيجةٌ مباشرةٌ لتكنولوجيا الحاسوبِ، وما كانت لِتُوجَدَ بدونِها، مثل: التَّعدي غيرُ المُصرَّحِ به على نظامِ الحاسوبِ (Bossler & Berenblum, 2019;496) ومن ثَمَّ، فالجريمةُ السيبرانيةُ تُعَدُّ سُلوكًا، وفعلاً غيرَ أخلاقيٍّ، وغيرَ قانونيٍّ في نفسِ الوقت، أي غيرُ مُصرَّحٍ به قانونًا (الحذيفي، ٢٠١٣: ١٣٣).

والجريمةُ السيبرانيةُ هي أيُّ جريمةٍ تُرتكَبُ من خلالِ الأجهزةِ الإلكترونية (مثل: الكمبيوتر، أو الهواتفُ الذَّكيةُ) باستخدامِ الإنترنت، وتَشملُ هذه الجرائمُ سَرقةَ البياناتِ، والمضايقاتِ، ونشرَ المعلوماتِ المُضلِّلةِ، وتضليلِ النَّاسِ، واختراقِ تفاصيلِ الحساباتِ، وقرصنَتِها، وما إلى ذلك(Kashif & UrRehman,2020;48) ومن ثَمَّ، فالجريمةُ السيبرانيةُ نشاطٌ إجراميٌّ مرتبطٌ مباشرةً باستخدامِ أجهزةِ الكمبيوتر، وتحديدًا التَّعدي غيرِ القانونيِّ على نظامِ الكمبيوتر، أو قواعدِ البياناتِ، والتَّلاعب، أو سَرقةِ البياناتِ المُخزَّنةِ على الإنترنت(Saini, Yerra, 2012;202). وتُعدُّ شبكاتُ الكمبيوتر أداةً، أو هدفًا، أو مكانًا للنَّشاطِ الإجراميّ، وقد تنطوي الجريمةُ السيبرانيةُ في سياقِ الأمنِ الوطنيِّ على النَّشاطِ، أو التَّجسسِ التَّقليديّ، أو حربِ المعلوماتِ، والأنشطةِ ذاتِ الصِّلةِ(Gandhi,2012;1) وهو ما يَستدعي معه تفعيلَ حوكمةٍ إلكترونيةٍ لكشفِ مجرمي الإنترنتِ، وآلياتِهم التي يُطورُونَها لتحقيقِ أهدافِهم، واختراقاتِهم الإلكترونيةِ بالسَّرقةِ، والاحتيالِ والتَّصيُّدِ (Lusthaus,2012;71).

وتعتمدُ الكثيرُ من الدَّراساتِ في تصنيفِ أشكالِ الجرائمِ الإلكترونية، والخطأُ السيبرانيِّ على تصنيفٍ طَوَّرَهُ ديفيد وول David Wall ، والذي قَسَّمَ الجرائمَ الإلكترونية إلى: التعدي على ممتلكاتِ الغيرِ، والخداعِ الإلكتروني، والعنفِ السَّيبرانيِّ، والتَّصويرِ السيبرانيِّ. وهذا التَّصنيفُ بسيطٌ بما فيه الكفايةُ لفَهمِ الجرائمِ الإلكترونية، ونظرًا لأنَّه يَستندُ إلى فئاتٍ قانونيةٍ من التَّعدي على ممتلكاتِ الغيرِ، والاحتيالِ، وجرائمِ العنفِ ضدَ الأشخاصِ، والتَّجاوزاتِ الأخلاقيةِ، فإنَّه يُوفِّرُ أساسًا جيدًا لدراسةٍ أعمقَ (Graham & Smith, 2019;5-6).

ومن ثَمَّ، فالجريمةُ السيبرانيةُ هي الجريمةُ التي يكونُ فيها الكمبيوترُ هدفًا لجريمةٍ، أو هو الوسيلةُ المعتمدةُ لارتكابِ جريمةٍ. ويبتكرُ المجرمونَ طرقًا مختلفةً للقيامِ بأنشطةٍ إجراميةٍ قياسيةٍ، مثل: الاحتيالُ، والسَّرقةُ، والابتزازُ، والتَّزويرُ، والاختلاسُ باستخدامِ الوسائلِ الرَّقميةِ الجديدةِ(Malar,2012;9) ومن أمثلةِ الجرائمِ السَّيبرانيةِ: المطاردةُ السيبرانيةُ، وهو استخدامُ الإنترنتِ، أو غيرِها من الوسائلِ الإلكترونيةِ لمطاردةِ شخصٍ ما. ويُستخدَمُ هذا المصطلحُ بالتَّبادلِ مع التَّحرشِ عبرَ الإنترنت، وإساءةِ الاستخدامِ عبرَ الإنترنت، فالتَّحرشُ الرَّقميُّ هو صورةٌ حديثةٌ لتوظيفِ التُّكنولوجيا الرَّقميةِ، واستغلالِ اختراقِها لكُلِّ البُيوتِ، حيثُ يَتعرضُ الغالبيةُ من أفرادِ المجتمعِ إلى هجماتٍ عبرَ صفحاتِ المواقعِ الإباحيةِ؛ بقصدِ نشرِ المحتوى الجنسيِّ بينَ شرائحِ المجتمعِ المختلفةِ (زيتون، ٢٠١٨: ٢٠٤-٢٠٥) وتنطوي المطاردةُ بشكلٍ عام على مضايقةٍ، أو تهديدِ الفردِ مراراً وتكراراً، مثل: ملاحقةُ شخصٍ ما، أو الظُّهورُ في منزلِ الشَّخصِ، أو مكانِ عملِه، أو إجراءُ مكالماتٍ هاتفيةٍ مضايقةٍ، أو تركُ رسائلَ، أو أشياءَ مكتوبةٍ، أو تخريبُ ممتلكاتِ الشَّخصِ وإفراغُ الحساباتِ المصرفيةِ. أما القرصنةُ فهي جريمةٌ سيبرانيةٌ تنطوي على اختراقِ النُّظمِ، والوصولِ غيرِ المُصرَّحِ به إلى البياناتِ المُخزَّنةِ فيها، والقرصنةُ هي أيُّ جهدٍ تقنيٍّ للتَّلاعبِ في السُّلوكِ الطَّبيعيِّ للاتصالاتِ، والأنظمةِ المُتَّصلةِ من خلالِ توظيفِ البرامجِ الخبيثةِ على شبكةِ الإنترنتِ، وغيرِها من الشَّبكات(Gandhi,2012;2) وتنقسمُ الجرائمُ السيبرانيةُ إلى ثلاثِ فئاتٍ: الجرائمِ التي يكونُ فيها الحاسوبُ هدفًا للجريمةِ، والجرائمِ التي يكونُ فيها الحاسوبُ أداةً للجريمةِ، والجرائمِ التي يكونُ فيها الحاسوبُ عرضيًّا في ارتكابِ الجريمةِ(Alil & Shahariar,2014; 10218).

إذا كانت الجريمةُ العالميةُ هي أيُّ جريمةٍ يتمُّ عولمةُ أسبابِها، ووسائلِها، وأشكالِ ارتكابِها، فإنَّ الجريمةَ السَّيبرانيةَ هي مظهرٌ نموذجيٌّ للجريمةِ العالميةِ، حيث إنَّ أسبابَهَا، ووسائلَها، وأشكالَ ارتكابِها، وآثارَها مُتجذِّرَةٌ بعمقٍ في تطوراتِ العولمةِ. وهناك فئتانِ رئيسيتانِ من أسبابِ الجريمةِ السيبرانيةِ، والعالميةِ: الأسبابُ المباشرةُ، والأسبابُ غيرُ المباشرةِ. الأسبابُ المباشرةُ: وهي مرتبطةٌ بالعواملِ الشَّخصيةِ، والتي تُؤثرُ مباشرةً على السُّلوكِ الفرديِّ، وتشملُ هذه الدوافعَ والفرصَ. فالدوافعُ هي التي تُحدِّدُ بعضَ الأهدافِ،

والأنشطة على أنَّها مرغوبةٌ، والفُرصُ المُتاحَةُ هي حالاتٌ، مثل: الوصولُ إلى أهداف مناسبة، أو توافرُ الوسائل، أو عدمُ وجودِ ضوابطَ فعالة، والتي تَجعلُ بعضَ السُّلوكيات مُمْكنةً، أو أكثرَ إغراءً. أما فيما يَتعلقُ بالأسبابِ غيرِ المباشرة، فهي الأسبابُ الأعمقُ، والتي تَرتبطُ بالأبعاد الثَّقافية، والاجتماعية، والنَّفسية، والاقتصادية، والتطورات السِّياسية، فهي مستقلةٌ إلى حدٍّ كبيرٍ عن الخياراتِ الفرديةِ التي تُحدِّدُ، أو تفاقمُ الدوافعَ الفرديةَ، والفرصَ المتاحة لارتكاب الجريمة. والفواصلُ بينَ الأسبابِ المباشرة، وغيرِ المباشرة ليست قَطْعِيَّةً، فَرُبَّما تَتطوَّرُ الأسبابُ غيرُ المباشرة في كثيرٍ من الأحيانِ إلى أسبابٍ مباشرة(Pasculli,2020;51-52).

إذن، يُستخدَمُ مصطلحُ الجريمة السيبرانية لوصف العديد من الأنشطة غير القانونية، وغير الأخلاقية في الفضاء الإلكتروني. ولا يُوجَدُ تعريفٌ عالميٌّ، وواسعُ النِّطاقِ للجريمة السَّيبرانية؛ وذلك تحديداً بسببِ الحقائقِ المذكورة أعلاه، والآراءِ المختلفة بشأنِ هذه المسألة(Ilievski & Bernik, 2016: 10) .

لذلك، يُمكنُنَا تقسيمَ الجرائمِ السيبرانية في معظمِها إلى أربعِ فئاتٍ رئيسية: الجرائمُ السيبرانيةُ ضدَ الأفراد، وتَضمُّ تلك الجرائمُ الموجَّهةُ في الأساسِ ضدَّ الأفرادِ بثَّ تصويرِ الأطفال، والإباحيةَ الإلكترونيةَ، وازعاجَ الفردِ عن طريقِ جهازِ كمبيوتر، مثل: البريدِ الإلكتروني، والاحتيالِ والتزوير. إنَّ نقلَ، ونشرَ الموادِّ المسيئة ذاتِ الموادِّ الإباحية، والتَّعرضِ غيرِ اللائقِ يؤسسُ لواحدةٍ من أهمِّ الجرائمِ الإلكترونية التي تمَّ تحديدُها في الوقتِ الحاضر: الجرائمُ السيبرانية ضدَّ الممتلكات، وتَضمُّ كافةَ الجرائمِ السيبرانيةِ المُوجَّهةِ ضدَّ جميعِ أشكالِ الأُصول، وتشملُ هذه الجرائمُ التَّخريبَ الحاسوبيَّ (طمس ممتلكات الآخرين)، وجرائمُ الملكيةِ الفكرية، والتَّخويف. ويهيمنُ هذا النَّوعُ من الجرائمِ عموماً على ارتكابِ الجرائمِ الماليةِ: الجريمةِ السيبرانيةِ ضدَّ الشركات، أو المنظمات، وهي واحدةٌ من أكثرِ الأشكالِ المعتادةِ للجريمةِ السيبرانيةِ في الوقتِ الرَّاهنِ عندما يتمُّ اختراقٌ للشَّركةِ عبرَ الإنترنت، أو أيٌّ من بضائعها، وكذلك موظفيها وشركائها، وعملائها.

الجريمةُ السيبرانيةُ ضدَّ الحكومة: كشفَ تطورُ الإنترنتِ أنَّ معيارَ الفضاءِ الإلكتروني يستخدمُه الأفرادُ والجماعاتث لترصُّدِ الحكوماتِ، وكذلك لتهديدِ شعوبِ الدَّولة. هذه

الجريمةُ تُثبِتُ نفسَها في العُنفِ عندما يخترقُ فردٌ موقعَ إدارةٍ، أو موقعَ عسكريٍّ محفوظ(Meena et al,2020;177).

٢. الشَّبابُ:

الشَّبابُ شريحةٌ عُمريةٌ، واجتماعيةٌ، لها محدداتٌ بيولوجيةٌ واضحةٌ، ومعاييرُ قانونيةٍ للعمرِ الذي تندرجُ تحته هذه الشَّريحةَ، غيرَ أنَّ التَّحديدَ القاطعَ لشريحةِ، ومفهومِ الشَّبابِ لا يزالُ يَشُوبُه قدرٌ من الصُّعوبةِ، ومن هنا، أوضحت منظمةُ اليُونسكو أنَّه لا يُوجد حدٌّ أدنى من التَّوافقِ الدُّوليِّ حولَ مفهومِ الشَّباب(رجب، ٢٠١٨: ٢١٦) ومن هنا، يمكنُ تقسيمُ التَّعريفاتِ السَّائدةِ للشَّبابِ في أدبياتِ العُلومِ الاجتماعيةِ إلى مجموعتينِ: تلك التي تُعرِّفُ الشَّبابَ بأنَّهم حالةٌ فرديةٌ من الوجودِ، تُحدَّدُ حسبَ العمرِ البيولوجي الزَّمني، في مقابلِ مجموعةٍ أخرى من التَّعريفاتِ، تُحددُ الشَّبابَ على أنَّها صفةٌ، أو طريقةٌ للدّلالةِ على نمطِ حياةٍ، أو سُلوكٍ، أو حالةٍ ذهنيةٍ، وجسميةٍ تُعبِّرُ عن الطَّاقةِ والمظهرِ، حيثُ الحديثِ حولَ تأثيرِ الشَّبابِ في نواحي الحياةِ المختلفةِ، والنَّظرِ إليهم باعتبارِهم شخصياتٍ مفكرةٍ، وليست متلقيةً، ومُستَلَبةَ الإرادةِ(الروسي، ٢٠٢٠:) وعلى الرَّغمِ من أنَّ المعيارَ الطَّاغيَّ في تعريفِ الشَّبابِ بيولوجيًّا في المقامِ الأولِ، فإنَّ المعانيَّ الاجتماعيةَ المرتبطةَ بحالةِ الشَّبابِ تَضَعُ الشَّبابَ ليس كمرحلةٍ عُمريةٍ في حدِّ ذاتِها، وإنَّما في أسلوبِ إدارةِ الحياةِ، وطريقةِ التَّفكيرِ، وصناعةِ النَّجاحِ. وهناك منظورٌ آخرُ في تعريفِ الشَّبابِ، يرتبطُ بالمنظورِ الاقتصاديّ، حيث يُعرِّفُ الشبابَ بأنَّهم الشريحةُ العُمريةُ التي تتراوحُ أعمارُهم بينَ ١٥ سنة باعتبارِهم عاملٍ اقتصاديٍّ، وذلك وفقًا لاتفاقيةِ منظمةِ العملِ الدُّوليةِ. أما التَّعريفاتُ الإحصائيةُ للشبابِ، فتتفاوتُ من مجتمعٍ إلى آخرَ، فقد اعتمدت بعضُ البُلدانِ تعريفَ الأممِ المتحدةِ للشَّباب (١٥ إلى ٢٤ سنة) في حين تَستخدمُ بلدانٌ أخرى تعريفَ الكومنولث (١٥ إلى ٢٩ سنة) والأغراضُ السياسةُ العامةُ يمكنُ أن تكونَ الفئةُ العمريةُ أوسعَ نطاقًا. وفي بعضِ البُلدانِ الأفريقية، مثل: غانا، وكينيا، وتنزانيا يتراوحُ تعريفُ الشبابِ المُستخدمِ لأغراضِ السياسةِ العامةِ بين ١٥ سنة و ٣٥ سنة. في نيجيريا، تتراوح بين ١٢ إلى ٣٠ سنة(Curtain,2001;3).

٣. الأمنُ السَّيبرانيُّ:

إنَّ التَّطرُّقَ إلى الأمنِ السيبرانيّ يدفعُنا إلى دراسةِ الدَّورِ الذي تلعبُه تكنولوجيا الاتصالاتِ في الحركاتِ الإرهابيةِ والمُتطرِّفةِ، وتحديدِ التَّدابيرِ القانونيةِ العديدةِ التي اُتخِذَت للتَّعاملِ مع استخدامِ الإنترنت من قِبلِ الجماعاتِ المتطرفةِ بما في ذلك إغلاقُ بعضِ المواقعِ الإلكترونية، ومكافحةُ أيديولوجيةِ الإرهابِ، الأمرُ الذي يَتطلَّبُ من السُّلطاتِ المسؤولةِ (مراعاةَ الحاجةِ إلى منعِ النَّاسِ من الانجرارِ إلى الإرهابِ")(Edwards,2017;25). فالجريمةُ السيبرانيةُ، والأمنُ السيبرانيُّ مرتبطانِ ببعضِهما البعض، ويؤثرُ كُلٌّ منهما في الآخرِ، فالجريمةُ السيبرانيةُ تتغيرُ وتتطورُ بسرعةٍ بمهاراتٍ، وتكنولوجياتٍ جديدة(Choi & Claire,2018;3) بل إنَّه يمكنُ القولُ أنَّ المُهدِّدَ الحقيقيَّ للأمنِ السيبراني هي الجرائمُ السَّيبرانية(بلحميتي، ٢٠١٧: ٦). ولا يزالُ الأمنُ السيبراني يُمثِّلُ تحدياً كبيراً في المجتمعِ المعاصرِ، خاصَّةً، وأنَّ المجتمعاتِ البشريةَ تعيشُ الآنَ في خضمِ ثورةٍ رقميةٍ، غيَّرت ثوابتِ المجتمعِ، مثل: الثَّورتينِ الصِّناعيتينِ اللتينِ سبقتاها، فإنَّ المشكلةَ الحقيقيةَ التي تواجه مجتمعاتنا المعاصرةَ العديدُ من المخاطرِ، والكيفيةِ التي نستطيعُ من خلالها حمايةَ تفاعلاتِنا عبرَ الفضاءِ الالكتروني . وهذا الوضعُ يتعلقُ بما نسميه الأمنَ السَّيبراني(Dupont,2019;19) ولاسيَّما مع غيابِ القوانينِ، والأُطرِ التَّشريعيةِ لمواجهةِ الجرائمِ السيبرانيةِ في ظلِّ وُقُوعِها في بيئةٍ سيبرانيةٍ عابرةٍ للحُدودِ(دبابنة، ٢٠١٥: ١٩)، ومجرمٍ سيبرانيٍّ يُتقِنُ الأسلوبَ الرَّقميَّ في الاختراقِ، والاحتيالِ(الردفاني، ٢٠١٤: ١٦٠-١٦٣).

ومن هذا المُنطلقِ، أنشئت المملكةُ العربيةُ السُّعُوديةُ الهيئةَ الوطنيةَ للأمنِ السَّيبراني(ابن داود، ٢٠٢٠: ١٥٤) وذلك تَزامنَ مع ما أكدت عليه رؤيةُ المملكةِ ٢٠٣٠ في التَّوسُّعِ في الاستخدامِ الرَّقميِّ لمُجملِ الأعمالِ الحكوميةِ، والخاصَّةِ في كافةِ المجالاتِ، وهو ما يدفعُ المملكةُ العربيةُ السُّعوديةُ لتحقيقِ الأمنِ السَّيبرانيِّ، خاصَّةً مع تعرضِها إلى هجماتٍ سيبرانيةٍ متكررةٍ، حيث أشارَ تقريرُ نورتونَ الأمريكيةِ إلى أنَّ ٨٥٪ من سكانِ المملكةِ العربيةِ السُّعوديةِ كانوا ضحايا الهجماتِ السَّيبرانيةِ في ٢٠١٦(أبو زيد، ٢٠١٩: ٥٧) ويتمُّ الهجومُ السَّيبرانيُّ من قِبلِ مجرمي الإنترنت، حيث يَستخدِمونَ أنظمةَ الكمبيوتر، أو

الشَّبكاتِ للتَّلاعبِ بالبياناتِ، أو سَرقتِها، أو الوُصولِ إليها دون إذنٍ. فالجريمةُ السيبرانيةُ هي تهديدٌ لأمنِ المعلوماتِ، والسَّطوِ على الأُصولِ الرَّقميةِ من قِبلِ مجرمي الإنترنت (Meena et al,2020;177) ومن هذا المُنطلقِ، فالأمنُ السَّيبرانيُّ هو مجموعةٌ من السِّياساتِ، والإجراءاتِ التي تَستهدِفُ وضعَ التَّدابيرِ الأمنيةِ لمواجهةِ الجرائمِ السَّيبرانيةِ(المقصودي، ٢٠١٧: ١٠٦). وعَرَّفَ الاتحادُ الدُّوليُّ للاتصالاتِ الأمنَ السَّيبرانيَّ على أنَّه إجراءاتٌ أمنيةٌ تَستهدِفُ إدارةَ المخاطرِ؛ بقصدِ توفيرِ الحمايةِ للأفرادِ، والمؤسساتِ، والدُّولِ في البيئةِ السَّيبرانية(فوزي، ٢٠١٩: ١٠٣).

وقد أتاحت تُكنولوجيا المعلوماتِ والاتصالاتِ فُرصًا كبيرةً للجماعاتِ الإرهابيةِ، والمنظماتِ المُتطرِّفةِ لتحقيقِ أهدافِها . فالطَّابعُ المُعقَّدُ، والمُتداخلُ لكُلٍّ من: الجريمةِ السَّيبرانيةِ، والإرهابِ يجعلُ من الصَّعبِ الفصلَ بوضوحٍ بين هاتينِ المسألتينِ، لاسيَّما في البيئاتِ الافتراضيةِ، بسببِ الطَّابعِ المجهولِ للاتصالاتِ الإلكترونيةِ، وهو ما يَدعُونا إلى تَكريسِ ثقافةٍ للأمنِ الرَّقميِّ(بشريف، ٢٠١٨: ٧١). وهناكَ بعضُ الأدلةِ على تَورُّطِ الدُّولِ القوميةِ، والأفرادِ في هجماتٍ قرصنةٍ واسعةِ النِّطاقِ ضدَّ أهدافٍ سياسيةٍ وعسكريةٍ. وبالمثلِ، استخدمت الجماعاتُ ذاتُ الدَّوافعِ السِّياسيةِ تِقنياتِ القرصنةِ للمشاركةِ في ضرباتٍ خطيرةٍ ضدَّ الحكوماتِ، والمنظماتِ السِّياسيةِ. وقد يَسَّرت تُكنولوجيا المعلوماتِ والاتصالاتِ إلى حدٍّ كبيرٍ التَّفاعلاتِ والتَّعاوُنِ، كذلك دمجَ الجريمةِ المُنظَّمَةِ، والجرائمَ الماليةَ، والاتجارَ والإرهابَ(Viano,2017;6).

سادساً ــ الإطارُ النَّظريُّ للدِّراسةِ :

في ظلِّ انتشارِ الجرائمِ السَّيبرانيةِ أصبحَ الباحثونَ مُهتَمِّينَ بشكلٍ خاصٍّ باختبارِ ما إذا كانت نظرياتُ الجريمةِ التَّقليديةِ، مثل: نظريةُ الأنشطةِ الرُّوتينيةِ، ونظريةُ التَّعلُّمِ الاجتماعيِّ، والنَّظريةُ العامةُ للجريمةِ، تنطبقُ على أشكالٍ مختلفةٍ من الجرائمِ السَّيبرانيةِ. وقد اُستخدِمَت نظريةُ النَّشاطِ الرُّوتينيِّ؛ لتفسيرِ الجرائمِ السَّيبرانيةِ على المستوى الفرديِّ، ولكنْ ليس على المستوى الوطنيِّ. وتُعَدُّ نظريةُ النَّشاطِ الرُّوتينيِّ من أبرزِ النَّظرياتِ التي كانت تُستخدَمُ سابقًا للتَّنبُّؤِ بمعدلاتِ الجريمةِ الإجماليةِ في الشَّوارعِ، ولكنَّها تَكيَّفَتْ منذُ ذلك الحينِ؛ لتُناسِبَ الجريمةَ السَّيبرانيةَ. وهناك بعضُ الأدلةِ التي تَدعَمُ تلك النَّظريةَ من حيثُ

التنبؤ بالجريمة السَّيبرانية. ومع ذلك، تمَّ استخدامُ نظرية النَّشاط الرُّوتيني فقطْ للتنبؤ بما إذا كان الفردُ سيكونُ متلقيًا للجرائم الإلكترونية، وسيشاركُ في الانحراف عبر الإنترنت(Kigerl,2012;470). وقد رَكَّزت الكثيرُ من البُحوث على البُلدان التي تَتَزايدُ فيها معدلاتُ الجرائم السيبرانية(Kigerl,2012;470). ونتيجةً لذلك، جَمعَ العلماءُ البيانات الأَوَّلية، وقَاسُوا المفاهيمَ الرَّئيسيةَ لنظريات الجريمة التَّقليدية، وتَحوَّلَ التَّركيزُ من تحليل أوجه التَّشابه والاختلاف في الجريمة السيبرانية بشكلٍ عامٍّ إلى دراسة ما إذا كانت نفسُ الأسباب النَّظرية، والارتباطات بين الجريمة التَّقليدية تنطبقُ بشكلٍ جيدٍ على الجريمة السَّيبرانية. وبالنَّظر إلى أنَّ هذه الدراسات كانت تَستندُ في كثيرٍ من الأحيان إلى عيناتٍ من الشَّباب، فَحَصَ العلماءُ أشكالاً أبسطَ من الجرائم السَّيبرانية، والخداع السَّيبرانيِّ، مثل: التَّحرش عبرَ الإنترنت، والقرصنة الرَّقمية، بدلاً من الأشكال الأكثر تعقيدًا للجرائم الإلكترونية التي تَتطلَّبُ مهارات تقنية(Bossler & Berenblum, 2019;497). فالجريمةُ السَّيبرانيةُ لديها القدرةُ على التَّأثير على الأنشطة اليومية للجميع، حيثُ يعتمدُ المجتمعُ بشكلٍ كبيرٍ على تُكنولوجيا الكمبيوتر لكُلِّ شيءٍ تقريبًا في الحياة، ويتراوحُ استخدامُ تُكنولوجيا الحاسوب بين مبيعات المُستهلكين الفردية، وتجهيز مليارات الدُّولارات في الصِّناعات المَصرفية والمالية. ويَستخدمُ مُجرمُو الكمبيوتر هذه التَّبعيةَ المُتزايدةَ كفرصةٍ كبيرةٍ؛ للانخراط في سُلوكياتٍ غيرِ مشروعةٍ، أو جَانحةٍ(Choi,2008;308).

وقد ابتدعت بعضُ النَّظريات طريقتانِ لقياس البلدان التي ترتفعُ فيها نسبةُ الجريمة السَّيبرانية، الأول: هو قياسُ المكانِ الذي يعيشُ فيه معظمُ مجرمي الإنترنت في الفضاءِ الماديِّ. ومن المُؤكَّد أنَّ بعضَ البلدانِ هي موطنٌ لمجرمي الإنترنت أكثرُ من غيرها. الوسيلةُ الثَّانيةُ لقياس البلدانِ ذاتِ الجرائم الإلكترونية العالية: هي تحديدُ الدُّول التي تأتي منها الهجماتُ الإلكترونيةُ، على سبيل المثال: البلدانِ التي تستضيفُ معظمَ خوادمِ التَّصيد الاحتياليِّ، والتي هي مصدرُ معظمِ رسائلِ البريدِ المزعجِ، ومن ثَمَّ، لا يقتصرُ نطاقُ الجريمة السَّيبرانية على الحُدود الوطنية(Kigerl,2012;473).

(١) نظريةُ الانتقالِ الفضائيِّ لجرائمِ الإنترنت Space Transition Theory :

منذُ أنْ بدأَ علمُ الجريمةِ ينظرُ إلى الفضاءِ السَّيبرانيِّ باعتباره مكانًا جديدًا للنَّشاطِ الإجراميِّ، وهناك حاجةٌ إلى نظريةٍ جديدةٍ؛ لشرحِ لماذا تحدثُ الجريمةُ السَّيبرانيةُ؟ ومن هذا المُنطلَقِ، تُقَدِّمُ نظريةُ الانتقالِ الفضائيِّ تفسيرًا للسُّلوكِ الإجراميِّ في الفضاءِ الإلكترونيِّ. ومن ثَمَّ، فقد جاءت نظريةُ الانتقالِ الفضائيِّ من أجلِ شرحِ سببِ الجرائمِ في الفضاءِ الإلكترونيِّ، خاصَّةً وأنَّ النَّظريةَ العامةَ في تفسيرِ السُّلوكِ الإجراميِ غيرُ كافيةٍ لتفسيرِ ظواهرِ الانحرافِ المرتبطةِ بالجرائمِ السَّيبرانيةِ، وتُفسِّرُ (نظريةُ الانتقالِ الفضائيِّ) سُلوكَ الأشخاصِ في الفضاءِ الإلكترونيِّ، وآلياتِ انتقالِ الأشخاصِ من فضاءٍ إلى آخرَ (مثلاً، من الفضاءِ الماديِّ إلى الفضاءِ الإلكترونيِّ، والعكس بالعكس). وتَفترِضُ النَّظريةُ بأنَّ النَّاسَ يتصرفون بشكلٍ مختلفٍ عندما ينتقلون من مساحةٍ إلى أخرى، وتَنهضُ تلك النَّظريةُ على عددٍ من الافتراضات(Jaishankar,2007;7):

١. الأشخاصُ الذين لديهم سلوكٌ إجراميٌّ مَكبُوتٌ (في الفضاء المادي) لديهم ميلٌ لارتكابِ جريمةٍ في الفضاءِ الإلكتروني، والتي لولا ذلك لما ارتكبُوها في الفضاءِ الماديِّ؛ بسببِ وضعِهم، ومَكانَتِهم.

٢. إنَّ مُرونةَ الهُويةِ، وعدمَ الكشفِ عن الهويةِ الشَّخصيةِ، وعدمَ وُجودِ عاملِ ردعٍ في الفضاءِ السَّيبرانيِّ تُتيحُ للمجرمينَ خيارَ ارتكابِ الجرائمِ السَّيبرانية.

٣. يُعَدُّ الفضاءُ الإلكترونيُّ للمجرمينَ فُرصةً للهُروبِ من الواقعِ المُعاشِ.

٤. ومن الأرجحِ أنْ يَرتَكبَ الأشخاصُ المنتمونَ إلى مجتمعٍ مُغلَقٍ جرائمَ في الفضاءِ الإلكتروني أكثرَ من الأشخاصِ المُنتمينَ إلى مجتمعٍ مفتُوحٍ.

٥. قد يؤدي تضاربُ معاييرَ، وقيمِ الفضاءِ الماديِّ مع معاييرَ، وقيمِ الفضاءِ الإلكترونيِّ إلى جرائمَ سَيبرانية.

(٢) نظريةُ الأنوميِّ Global Anomie Theory :

إنَّ نظريةَ الأنوميِّ العالميِّ، والجريمةَ السَّيبرانيةَ هي إحدى أقوى الأُطُرِ النَّظريةِ لتفسيرِ الجريمةِ. الأنوميُّ (اضطراب المعايير) وهو الوضعُ الذي يَفشلُ فيه المجتمعُ في تنظيمِ الرَّغباتِ الطَّبيعيةِ غيرِ المحدودةِ للأفرادِ، ووفقًا لدوركايم، هذه الحالةُ هي نموذجيةٌ

لفترات التَّغييرِ الكبيرِ، عندما لا يُمكنُ للمجتمعِ على الفورِ ضبطُ السُّلوكياتِ الفرديةِ إلى الأفضلِ، وقد أصبحت حالةُ الأنوميِّ مزمنةً في مجالِ الأعمالِ التِّجاريةِ مع التَّنميةِ الصِّناعيةِ، والامتدادِ "اللا محدود" للسُّوقِ. إنَّ التزامَ كُلِّ دولةٍ، بغضِّ النَّظرِ عن النُّموذجِ الاقتصاديِّ المُتَّبعِ بالازدهارِ الصِّناعيِّ، وما يترتبُ على ذلك من إخضاعِ الدَّولةِ للحياةِ الاقتصاديةِ قد أدت إلى تحريرِ الإنسانِ من أيِّ تنظيمٍ، وعَزَّزت من نزواتِه ومطامعِه. وقد أوضح ميرتونث بأنَّ الأهدافَ غيرَ الواقعيةِ ليست بالضَّرورةِ بيولوجيةً، ولكنَّها يمكنُ أنْ تكونَ نتيجةً لضغوطٍ اجتماعيةٍ، وثقافيةٍ، ويحدثُ هذا عندما يكونُ هناك عدمُ توازنٍ بين الأهدافِ التي يسعى على تحقيقِها الفردُ النَّاجمةِ عن الثَّقافةِ، والوسائلِ المُتاحةِ لتحقيقِها. وعندما يكونُ هناك تعظيمٌ من ثقافةِ المجتمعِ المحليِّ على أهميةِ الثَّروةِ، والسُّلطةِ، وما إلى ذلك، في مقابلِ عدمِ توفرِ الوسائلِ المشروعةِ، والفعَّالةِ لتحقيقِها، قد يلجأُ الأفرادُ إلى وسائلَ محظورةٍ، ولكنَّها فعالةٌ في تحقيقِ أهدافِه، وبالتَّالي، فإنَّ السُّلوكَ المعادي للمجتمعِ ناجمٌ عن البناءِ الطَّبقيِّ الذي يمنعُ المساواةَ في الوصولِ إلى الفرصِ القانونيةِ؛ لتحقيقِ الأهدافِ الثَّقافيةِ التَّقليديةِ، وعليه، فَسَّرَ ميرتون الجرائمَ السَّيبرانيةَ في ضوءِ الأبنيةِ الاجتماعيةِ، والاقتصاديةِ لأفرادِ المجتمعِ المحليِّ، والتي تَنعكسُ بشكلٍ، أو بآخرَ على انتشارِ الجرائمِ السَّيبرانية(الفالح، ٢٠٠٨: ١٤٧-١٤٨).

وهنا يُشيرُ أنومي دوركايم إلى انعدامِ المعاييرِ في الأهدافِ، في حين، يشيرُ أنومي ميرتون إلى انعدامِ المعاييرِ في الوسائلِ، فقد أشارَ "ميسنر وروزنفيلد" إلى أنَّ إزالةَ العقباتِ الهيكليةِ أمامَ الفُرصِ المشروعةِ لا تكفي لخفضِ معدلاتِ الجريمةِ عندما تَدْعُمُ جميعُ المؤسساتِ الاجتماعيةِ الرئيسيةِ في المقامِ الأولِ السَّعيَ؛ لتحقيقِ النَّجاحِ الماديِّ، وتَفشَلُ في تعزيزِ تعاريفَ بديلةٍ للكفاءةِ الذَّاتيةِ والإنجازِ، وبعبارةٍ أخرى، يجبُ أنْ تكونَ الأهدافُ الثَّقافيةُ موضعَ تَساؤُلٍ، جنباً إلى جنبٍ مع كفايةِ الوسائل(Pasculli,2020;52).

ونَظريةُ الأنومي تَتَوسعُ تدريجيًّا إلى ما هو أبعدُ من تركيزِها الاجتماعيِّ الأصليِّ. وقد نقل روبرت أغنيو Robert Agnew التَّحليلَ من المستوى الكليِّ للنِّظام الاجتماعيِّ إلى المستوى الاجتماعيِّ، والنَّفسيِّ للفردِ، وبيئتهم المباشرةِ، حيثُ توسيعِ رُؤيةِ ميرتونِ، والاعتمادِ على أعمالِ ألبرت كوهين وكلوارد وأوهلين، حيث تُفسرُ الجريمةَ السيبرانيةَ هنا

ليس نتيجةَ الفشلِ فقط في تحقيقِ أهدافٍ ذاتِ قيمةٍ إيجابيةٍ، ولكنْ من عدمِ القُدرةِ على الهُروبِ بشكلٍ قانونيٍّ من المواقفِ المؤلمةِ أيضاً ، ومن ثَم، تُستخدَمُ حديثًا، نظريةُ الأنومي؛ لشرحِ الأشكالِ النُّموذجيةِ للجريمةِ المُعولَمَة، مثل: الجرائمِ الماليةِ العابرةِ للحُدودِ الوطنيةِ، وجرائمِ الشَّركاتِ، والإرهابِ، وإجرامِ اللاجئين، والقرصنةِ عبرَ الإنترنت، حيث لاحظَ باساس Passas أنَّ الجرائمَ السَّيبرانيةَ التي تُشكِّلُها حالةُ الأنومي تتَزايدُ في جميعِ أنحاءِ العالمِ من خلالِ العولمةِ، واللِّيبراليةِ الجديدة؛ حيثُ فشلت اللِّيبراليةُ العالميةُ الجديدةُ في الوفاءِ بوعُودِها، وتحقيقِ التَّرابُطِ العالميِّ. فاللِّيبراليةُ الجديدةُ للنُّمُوِّ الاقتصاديِّ، والأسواقِ الحُرَّةِ ساهمت في تعزيزِ الفرديةِ، والنَّزعةِ الاستهلاكيةِ والخصخصةِ، ومن ثَم، خَلْقُ احتياجاتٍ جديدةٍ، ومن ثَم، تأجيجٌ للرَّغباتِ والغرائزِ، ممَّا يَدفعُ الأفرادَ الذين يشعرون بالإحباطِ، والحرمانِ؛ نتيجةَ عدمِ القُدرةِ على تحقيقِ الأهدافِ، وإشباعِ الاحتياجاتِ إلى الانحراف(Pasculli,2020;53).

إنَّ الاعترافَ بعدمِ المُساواةِ، وعدمِ كفايةِ الوسائلِ لتحقيقِ الأهدافِ ذاتِ القيمةِ الثَّقافيةِ كسببٍ لأشكالِ الإجرامِ المُعولَمَةِ لا يعني ضمناً أنَّ الفقرَ ـــــــــــ في حدِّ ذاتِهِ ـــــــــــ هو سببٌ للجريمةِ العالمية. والواقعِ أنَّ المجتمعاتِ الفقيرةَ التي تَتّسمُ ببنيةٍ اجتماعيةٍ شديدةِ الصَّلابةِ، وأهدافٍ ماديةٍ أقلَّ هي أكثرُ مناعةً ضدَّ الآثارِ الإجراميةِ النَّاجمةِ عن الاضطرابِ المعياريَّ. ويوضح دوركايم بوضوحٍ شديدٍ أنَّ الفقرَ هو قيدٌ في حدِّ ذاتِهِ؛ لأنَّ الرَّغباتِ تعتمدُ على الواردِ (كلما قلت مواردُ الفردِ، قلت مُيُولُهُ إلى توسيعِ نطاقِ احتياجاتِهِ إلى أجلٍ غيرِ مُسمَّى) . فالأفرادُ الذين لديهم إمكانيةُ الوُصولِ إلى الفُرصِ الماديةِ هم الذين يتمُّ الضَّغطُ عليهم بسهولةٍ؛ لتحقيقِ المزيدِ والمزيد. إنَّ التَّوسعَ في الفُرصِ الاقتصاديةِ يُعزِّزُ التَّأكيدَ على أهدافِ النَّجاحِ الماديِّ، ويُوفِّرُ وسائلَ جديدةً لتحقيقِها بصُورةٍ غيرِ مشروعةٍ. والجرائمُ السَّيبرانيةُ مثالٌ نُموذجيٌّ على ذلك، فنادراً ما يكونُ مجرمو الإنترنت فُقراءَ، وغيرَ متعلمينَ؛ لأنَّ الجرائمَ السَّيبرانيةَ تَتَطلبُ الوُصولَ إلى تُكنولوجيا المعلوماتِ والاتصالات، وامتلاكَ المهاراتِ المُتقدِّمة، وعلاوةً على ذلك، فإنَّ الوُصُولَ إلى الإنترنت يَزيدُ من التَّعرُّضِ للضُّغوطِ الثَّقافيةِ التي لا هَوادةَ فيها من النَّزعةِ الاستهلاكيةِ، والمنافسةِ، والفرديةِ. وعلى الرُّغم من أنَّ العديدَ من الجرائمِ الإلكترونية يتمُّ تحريكُها من

خلال الدافعِ الماديِّ الذي يتمثلُ في تحقيقِ الربِّحِ الماليِّ، أو الفوائدِ التِّجاريةِ، فإنَّ الأبحاثَ التَّجريبيةَ تُشيرُ إلى أنَّ الدَّافعَ الثَّاني الأكثرَ شُيوعًا لجرائمِ الكمبيوتر هو الانتقام (Pasculli,2020;54).

(٣) نظريةُ مجتمعِ المخاطرِ:

جاءت نظريةُ مجتمعِ المخاطرِ؛ لتُشخِّصُ حالةَ الفوضى، والمخاطرَ العديدةَ التي تُحيطُ بالفردِ في مجتمعٍ ما بعد الحداثةِ: المجتمعِ الرَّقميِّ الجديدِ، مجتمعِ التِّقنيةِ العالية، المجتمعِ المعلوماتيِّ المُعولَمِ الجديدِ العابرِ للحُدودِ والأزمنة، وهو ما سَاعدَ بشكل كبيرٍ في تَعرُّضِ الفردِ لمُهَدَّدَاتٍ، ومخاطرَ محتملةٍ عديدةٍ؛ نتيجةَ تفاعُلِه عبرَ الفضاءِ السَّيبرانيِّ، فقد أعادت العولمةُ تشكيلَ حياتنا من جديد(فوزي، ٢٠١٩: ١٠٥-١٠٦). فمجتمعُ المخاطرِ هو مجتمعٌ يحتوي على أخطارٍ عدةٍ تتجاوزُ حدودَ الدَّولةِ، وسيادتِها، حيثُ التَّدفُّقِ المعلوماتيِّ، والسُّيولةِ في حركةِ المجتمعِ عبرَ الفضاءِ الإلكتروني(نظمي، ٢٠١٩: ٢٠٠-٢٠١). ومن هذا المنطلقِ، دارت نظريةُ مجتمعِ المخاطرِ حولَ فرضياتٍ ثلاثةٍ: فرضيةِ العولمةِ، حيث إنَّ العولمةَ تَرتَّبَ عليها كوارثُ، ومخاطرُ عدَّةٌ: سياسيةٌ، واقتصاديةٌ، واجتماعيةٌ، وتُكنولوجيةٌ، وفرضيةُ الصَّراعِ التي تَتَشكلُ بفعلِ الصراعاتِ الطَّبقية التي تَتَشكلُ في ضَوءِ النِّزعاتِ الاستهلاكيةِ للرَّأسماليةِ، وفرضيةُ الفردانيةِ، حيث إنَّ العولمةَ عَمَّمَت ثقافةَ الفرديةِ، وتفكيكَ الرَّوابطِ التَّقليديةِ، وشُيوعَ القيمِ التَّقليدية(السيد، ٢٠١٩: ٢٠).

سابعاًـ الدَّراساتُ السَّابقةُ :

المحورُ الأولُ: الجرائمُ السَّيبرانيةُ : طبيعتُها، ومستخدميها، وضحاياها:

دراسةُ (قيسي، ٢٠١٠) حولَ: الجرائمِ الإلكترونيةِ المُوجَّهةِ ضدَّ مستخدمي الإنترنتِ بالمملكةِ العربيةِ السَّعُوديةِ، والتي حاولت رصدَ أبرزِ جرائمِ الإنترنت شُيُوعًا بينَ مُستخدمي الإنترنتِ في المملكةِ، ولاسيَّمَا الجرائمُ الجنسيةُ، وجرائمُ الاختراقاتِ، وجرائمُ الإرهابِ الإلكتروني. واعتمدت الدَّراسةُ على المسحِ الاجتماعيِّ بالعينةِ، وبلغت عينةُ الدِّراسةِ ١٠٥٥ مفردةً سُحبت من (١٥) موقعًا بالمملكةِ العربيةِ السُّعودية. وخلصت الدراسةُ إلى أنَّ جرائمَ الاختراقِ التي تَعرَّضَت لها عينةُ الدِّراسةِ كانت تُعَرِّضُ البريدَ الشَّخصيَّ للاختراقِ، وتُعَرِّضُ هاتفَهم للاستيلاءِ، وأجهزتَهم الشَّخصيةَ للاختراق. ودراسة

(Aransiola & Asindemade,2010) حول: مرتكبي الجرائمِ الإلكترونيةِ، والاستراتيجياتِ التي يستخدمُونها في نيجيريا، والتي انطلقت من دراسة بياناتٍ من (٤٠) حالةً من مرتكبي الجرائمِ الإلكترونيةِ الذين تمَّ اختيارُهم بطريقةِ كرةِ الثَّلجِ، وكشفت النَّتائجُ أنَّ معظمَ مرتكبي الجرائمِ الإلكترونيةِ في نيجيريا تتراوحُ أعمارُهُم بين ٢٢ و٢٩ عامًا، وكانوا طُلابًا جامعيينَ، ولديهم أنماطُ حياةٍ مميزةٍ، حيث إنَّ معظمَ مرتكبي الجرائمِ السَّيبرانية مُتورِّطُونَ في الإنترنت، والشراءِ، والبيعِ بهويةٍ مُزَيَّفَة. ودراسةُ (Susheel & Durgesh,2011) حولَ: الجرائمِ السَّيبرانيةِ في الهندِ، والتي سلَّطت الضَّوءَ على الجرائمِ السيبرانية في الهندِ استنادًا على تحليلِ مضمونٍ لبياناتٍ من الصُّحُف، ومواقعِ الإنترنت، ووسائلِ الإعلامِ، وخلصت الدِّراسةُ إلى أنَّ الجرائمَ السيبرانيةَ تُعتَبرُ أهمَّ خطرٍ يُهدِّدُ المجتمعاتِ في الوقتِ الرَّاهنِ. ودراسةُ (Boateng & Olumide,2011) حولَ: الجريمةِ السَّيبرانية في غانا، والتي بحثت في انتشارِ الجرائمِ السَّيبرانيةِ في غانا، وأشكالِها، وآثارِها من خلالِ استخدامِ منهجٍ نوعيٍّ؛ لاستكشافِ الجُهودِ التي تَبذُلُها المنظماتُ، والوكالاتُ الحكوميةِ في غانا؛ للحدِّ من الجرائمِ السَّيبرانيةِ من حيثُ الاعتقالِ، والملاحقةِ القضائيةِ، والإبلاغِ، وإنفاذِ القانونِ. وأظهرت النَّتائجُ أنَّه على الرُّغم من أنَّ الوعيَ بالجرائمِ السيبرانيةِ في ازديادٍ، إلا أنَّ الجرائمَ لا يتمُّ الإبلاغُ عنها في الغالبِ. ودراسة (Alil & Shahariar,2014) حولَ: أنشطةِ الجريمةِ السَّيبرانيةِ بينَ طُلابِ الثَّانويِّ في مدينةِ دكا ببنجلاديش، والتي حاولت الكشفَ عن مدى انتشارِ أنشطةِ الجريمةِ السَّيبرانيةِ بينَ طلابِ المرحلةِ الثَّانويةِ (الذين تتراوحُ أعمارُهم بين ١٣ و١٩ عامًا)، وإلى أيِّ مدًى هناك وعيٌ بينَ عينةِ الدِّراسةِ بهذه الأنشطةِ الإجراميةِ؟ حيثُ يتمُّ استخدامُ الكمبيوتر: إمَّا كأداةٍ، أو هدفٍ، أو كليهما.

وخلصت الدِّراسةُ إلى انتشارِ عددٍ من الجرائمِ السيبرانيةِ بينَ طلابِ المدارسِ الثانويةِ في مدينةِ دكا: القرصنةِ، والاحتيالِ على بطاقاتِ الائتمانِ، وقرصنةِ البرمجياتِ، وسرقةِ الهُويةِ السيبرانيةِ، والتَّصيدِ الاحتياليِّ. دراسةُ (Olayemi, 2014) حولَ: تحليلٍ اجتماعيٍّ تُكنولوجيٍّ للجرائمِ السيبرانيةِ في نيجيريا، والتي هدفت إلى دراسةِ العواملِ الاجتماعيةِ، والتُّكنولوجيةِ التي تُؤثرُ على الجريمةِ الإلكترونيةِ في نيجيريا، وتناولت

الدِّراسةُ الجرائمَ السيبرانيةَ من وجهةِ نظرٍ نظريةٍ، واستقصائيةٍ، كما أُجرت مُقابلاتٍ مُنظَّمَةً مع وكالاتِ إنفاذِ القانونِ، والمؤسسةِ الحكوميةِ للأمنِ السَّيبرانيّ، واعتمدت الدِّراسةُ على نظريةِ النَّشاطِ الرُّوتينيِّ، وأوضحت الدِّراسةُ أنَّه لا تُوجَدُ قوانينُ حاليةٌ في نيجيريا، تتعاملُ بشكلٍ مباشرٍ مع الجرائمِ الإلكترونية. دراسة (Nasi& Oksanen, 2015) حولَ: الإيذاءِ في الجرائمِ السيبرانيةِ بين الشَّبابِ، وبحثت الدِّراسةُ في الخصائصِ المشتركةِ لهذه الجرائمِ، وبعضِ التَّوقعاتِ العامةِ للإيذاءِ في الجرائمِ السيبرانيةِ بين المراهقين والشَّبابِ، وتَمَّ بناءُ عينةٍ من أربعةِ بلدانٍ مُجتَمِعةٍ: (فنلندا، والولايات المتحدة، وألمانيا، والمملكة المتحدة) وتراوحت أعمارُ عينةِ الدِّراسةِ بين (١٥ و ٣٠) سنةً، ووفقًا لنتائجِ الدِّراسةِ، فإنَّ القذفَ، والتَّهديدَ بالعُنفِ هما أكثرُ أشكالِ الإيذاءِ، والتَّحرشِ الجنسيِّ شُيُوعًا. ودراسة (إبراهيم، ٢٠١٥) حولَ: جرائمِ الإنترنت في المجتمعِ المصريِّ، والتي استهدفت الكشفَ عن جرائمِ الإنترنت، وخصائصها، ووسائلِ مواجهتِها، واعتمدت في تحليلاتِها على نظرياتٍ تقليديةٍ كنظريةِ المخالطةِ الفاصلةِ، ونظرياتٍ معاصرةٍ كنظرياتِ الانتقالِ الفضائيِّ لجرائمِ الإنترنت، واعتمدت على الأساليبِ الكَميةِ، والكَيفيةِ، وقامت الدِّراسة بفحصِ (٦١) محضرًا لجرائمِ الإنترنت ذاتِ الطَّابعِ الاقتصاديِّ، وخلصت الدِّراسةُ إلى تَنوُّعِ جرائمِ الإنترنت، وكان أبرزُها جريمةَ سبٍّ، وقذفٍ، وتشهيرٍ، ثُم جريمةَ تمريرِ المكالماتِ الدُّوليةِ، ثُم جرائمَ الانتحالِ. كذلك دراسةُ (Goldsmith & Wall,2019) حولَ: إغراءاتِ الجريمةِ السيبرانيةِ، والتي بحثت في الآثارِ المترتبةِ على (الانجرافِ الرَّقميِّ) للمراهقين خلالَ تفاعلاتِهم على منصَّاتِ الإنترنت المختلفةِ : (وسائلِ التواصلِ الاجتماعيِّ، والألعابِ، وعملياتِ البحثِ على شبكةِ الإنترنت)، وتنظرُ هذه الدِّراسةُ إلى الشَّبابِ كضحايا للجريمةِ السيبرانية، حيثُ حوَّلَ الإنترنتُ المراهقينَ الذين تتراوحُ أعمارُهُم بينَ (١٢ و١٩) عامًا نحو الإساءةِ، والانجرافِ الرَّقميِّ. وفَسَّرَت الدِّراسةُ ارتكابَ المراهقينَ لهذه الجرائمِ في ضَوءِ ما أَسمَتهُ بـــ (اللاوعي التُّكنولوجيِّ) كما أوضحت الدِّراسةُ أنَّ المُتسلِّلينَ كانوا من المراهقينَ الذُّكورِ الصِّغارِ. ودِراسةُ (الصبان، ٢٠١٩) حولَ: إدمانِ الطُّلابِ على استخدامِ مواقعِ التَّواصلِ الاجتماعيِّ، والتَّورطِ في الجرائمِ السَّيبرانية التي حاولت استكشافَ العَلاقةِ بينَ إدمانِ الطُّلابِ لمواقعِ التَّواصلِ الاجتماعيِّ، وتورطِهم في

الجريمةِ السيبرانية، وبلغت عينةُ الدِّراسةِ (٢٥٢) طالبًا بجامعةِ طيبةَ، واعتمدت الدِّراسةُ على المنهجِ الارتباطيِّ التَّحليليِّ، وخلصت الدِّراسةُ إلى أنَّ استخدامَ الطُّلابِ الكثيفِ لمواقعِ التَّواصلِ الاجتماعيِّ كان له عَلاقةٌ مُباشِرَةٌ بتورطِهم في الجرائمِ السَّيبرانيةِ.

المحورُ الثَّاني: اتجاهاتُ ورُؤَى الشَّبابِ للجرائمِ السَّيبرانيَّةِ :

دِراسةُ (غزال، ٢٠١١) حولَ: جرائمِ الإنترنتِ في المجتمعِ المصريِّ : دِراسةٌ مَيْدانيةٌ على عينةٍ من الشَّبابِ الجَامعيِّ، والتي استهدفت الكشفَ عن أنواعِ الجرائمِ المنتشرةِ بين الشَّبابِ نتيجةَ التَّفاعلِ على شبكةِ الإنترنت، وتمَّ سَحبُ العينةِ من محافظةِ الإسكندرية، وبلغَ قِوامُها (٣٠٠). وخلصت الدِّراسةُ إلى أنَّ أبرزَ الجرائمِ السَّيبرانيةِ المنتشرةِ بينَ الشَّبابِ هي على التَّوالي: جرائمِ القرصنةِ، الجرائمِ الجنسيةِ، الجرائمِ الماليةِ، وجرائمِ الاختراقِ. دراسةُ (خميس، ٢٠١١) حولَ: رُؤَى الشَّبابِ نحوَ الجرائمِ المعلوماتيةِ في المجتمعِ المصريِّ، والتي حاولت التَّعرفَ على رُؤَى الشَّبابِ تِجاهَ الجرائمِ المعلوماتيةِ، هذا، وعَرَّفت الدِّراسةُ الجرائمَ المعلوماتيةَ بأنَّها تَلاعبُ في البياناتِ؛ بهدفِ الدُّخُولِ غيرِ المشروعِ على بياناتِ الحاسبِ الآليِّ، واستخدمت الدِّراسةُ المنحى الوصفيَّ؛ للتَّعرفِ على اتجاهاتِ الشَّبابِ اعتمادًا على عينةٍ بلغَ عددُها (٣٠٠) مفردةً، وأظهرت الدراسةُ أنَّ الذُّكورَ أكثرُ معرفةً بالجرائمِ السَّيبرانيةِ مقارنةً بالإناثِ، وظهرت الجرائمُ المعلوماتيةُ بالنِّسبةِ للشَّبابِ في تنفيذِ أنشطةٍ غيرِ مشروعةٍ عن طريقِ استخدامِ الحاسبِ الآليِّ.

دِراسةُ (Yu,2014) حولَ: الخوفِ من الجرائمِ السيبرانيةِ بين طُلابِ الجامعةِ، في الولاياتِ المتحدةِ، والتي اهتمت باستعراضِ أدبياتٍ بشأنِ الخوفِ من الجريمةِ في ضَوءِ خُطُورةِ الجريمةِ المُتصوَّرةِ، والخطرِ المتصورِ للإيذاءِ، وتجربةِ الإيذاءِ، باعتبارِها العواملَ الرئيسيةَ الثَّلاثةَ للتَّنبُّؤِ بالخوفِ من الجريمةِ. في هذه الدِّراسةِ اُختُبِرَت هذه العواملُ المتعلِّقةُ بالجرائمِ السَّيبرانيةِ، حيث إنَّ تلك العَلاقةَ لم تُدرسْ بشكلٍ كبيرٍ في الأدبياتِ، واختارت الدِّراسةُ أربعَ جرائمَ إلكترونيةٍ، بما في ذلك الاحتيالُ عبرَ الإنترنت، والبلطجةُ عبرَ الإنترنت، والقرصنةُ الرَّقميةُ، وفيروساتُ الكمبيوتر. وتُشيرُ النَّتائجُ إلى أنَّ استخدامَ الإنترنت يَلعبُ دَورًا في الخوفِ من الجريمةِ السَّيبرانيةِ. ودراسةُ (Solak & Topaloglu, 2015) حولَ: تحليلٍ تَصوُّرِيٍّ للجرائمِ السَّيبرانيةِ من وِجهةِ نظرِ طُلابِ

عُلومِ الحاسبِ، حيثُ تَوقَّفَت الدِّراسةُ عندَ الاختلافاتِ بينَ تصوراتِ الجريمةِ السيبرانيةِ بينَ الطُّلابِ الجامعيينَ في جامعةِ تراكيا من خلالِ تطبيقِ استبيانٍ، تمَّ توزيعُهُ على الطُّلابِ في جامعةِ تراكيا، وكانَ مُصمَّماً لقياسِ، وتقييمِ مستوياتِ الاهتمامِ بالتُّكنولوجيا، وشدةِ الجرائمِ السَّيبرانيةِ، وخلصت الدِّراسةُ إلى أنَّ ٨٠٪ من الشَّبابِ الجامعيِّ أجمعَ على أنَّ استخدامَ المعلوماتِ الشَّخصيةِ، وتسريبِها يُعدُّ جريمةً سَيبرانيةً. دراسةُ (الشهراني، ٢٠١٩) حولَ: تَصورٍ مُقترَحٍ؛ لوقايةِ الشَّبابِ الجامعيِّ من مخاطرِ جرائمِ الإرهابِ السَّيبرانيِّ، والتي استهدفت تقديمَ تصورٍ مُقترَحٍ؛ لحمايةِ الشَّبابِ الجامعيِّ من تهديداتِ، ومخاطرِ جرائمِ الإرهابِ السَّيبرانيِّ، واعتمدت على عينةٍ عشوائيةٍ بلغت (٢١٣) من طلبةِ جامعةِ الملكِ سُعودٍ، والإمامِ محمدِ بن سعودٍ الإسلاميةِ، واعتمدت الدِّراسةُ على المنهجِ الوصفيِّ التَّحليليِّ، وخلصت الدراسةُ إلى أنَّ جهلَ الشَّبابِ باستخدامِ المواقعِ السَّيبرانيةِ تَسبَّبَ في وُقوعِهم في شَبكاتٍ مُضلِّلَةٍ، حيثُ الانحرافِ الفكريِّ والدِّينيِّ، والتَّشجيعِ على تجارةِ المُخدِراتِ. ودراسةُ كُلٍّ من : (Volodymyr& Olexandr,2020) حولَ: موقفِ الشَّبابِ من مشكلةِ الإجرامِ في مجتمعٍ ما بعدَ الحداثةِ الأوكرانيِ، والتي احتوت على النَّتائجِ الرَّئيسيةِ؛ لمسحِ الرَّصدِ العشوائيِّ للطُّلابِ الأوكرانيين الذي يُغطِّي الفترةَ (٢٠٠٢-٢٠١٧) حيثُ تمَّ استكشافُ موقفِ الشبابِ من مشاكلِ الجريمةِ، وأنشطةِ الشُّرطةِ الهادفةِ إلى مُواجهتِها في مدينةِ (كييف) حيثُ سَمَحَ تحليلُ نتائجِ المسحِ بتحديدِ مستوى خوفِ الطُّلابِ من أنْ يصبحوا ضحايا لأنواعٍ معينةٍ من الجرائمِ، ودرجةِ تَعرُّضِهِم للإيذاءِ بشكلٍ عامٍ، وخوفِهِم من المُعاناةِ من جرائمَ معينةٍ، وتقييمِهم لطبيعةِ دِينَامِيَاتِ الجريمةِ في أنشطةِ المدينةِ والشُّرطةِ؛ لمعرفةِ الآراءِ حولَ الوضعِ مع الأمنِ الشَّخصيِّ في وقتٍ معينٍ؛ وفي المستقبلِ.

ومن بينِ الاتِّجاهاتِ التي تمَّ تحديدُها في سياقِ البحثِ مستوىً عالٍ من خوفِ المُستجيبينَ من أنْ يصبحوا ضحيةً للعنفِ، والجرائمِ البسيطةِ الأكثرِ انتشاراً، ارتفاعُ مستوى إيذائِهم الذي انخفضَ بشكلٍ واضحٍ في السَّنواتِ الأخيرةِ، التقييماتُ السَّلبيةُ السَّائدةُ لديناميَاتِ الجريمةِ، وتقييمُ أنشطةِ الشرطةِ، والثِّقةِ بها على أنَّها غيرُ مرضيةٍ بغضِّ النَّظرِ عن التَّحسيناتِ في هذه المؤشراتِ في السَّنواتِ الثَّلاثِ الأخيرةِ، والتَّقييمُ السَّلبيُّ السَّائدُ

للوضعِ مع الأمنِ الشَّخصيِّ، والتَّوقعاتُ الإيجابيةُ فيما يَتعلَّقُ بالتَّغييراتِ في المستقبل. دراسةُ (البشري، ٢٠٢٠) حولَ: الجرائمِ الإلكترونيةِ، وكيفيةِ التَّعاملِ معها من وجهةِ نظرِ الشَّبابِ الجامعيِّ، والتي استهدفت التَّعرُّفَ على أنماطِ الجرائمِ الإلكترونيةِ، والوقوفَ على مخاطرِها، والكشفَ عن دورِ الجهاتِ التَّنظيميةِ؛ لمكافحةِ تلك الجرائمِ من وجهةِ نظرِ الشَّبابِ الجامعيِّ، واعتمدت الدِّراسةُ على منهجِ المسحِ الاجتماعيِّ بالعينةِ، وقد بلغت عينةُ الدِّراسةِ (٢٢٦) طالبًا، وتَوصَّلَت الدِّراسةُ إلى أنَّ أبرزَ الجرائمِ الإلكترونيةِ خُطورةً من وجهةِ نظرِ عينةِ الدِّراسةِ جرائمُ اختراقِ الحسابِ الشَّخصيِّ، وجرائمُ إنشاءِ مواقعَ معاديةٍ للمجتمعِ، وجرائمُ إنشاءِ مواقعَ متطرفةٍ.

ثامنًا- منهجُ الدِّراسةِ، وأُسلُوبُ التَّحليلِ:

هذه الدِّراسةُ وصفيةٌ كميةٌ بطبيعتِها، حيثُ تَستندُ التَّحليلاتُ السُّوسيولوجيةُ، والإحصائيةُ على البياناتِ الأَوَّليةِ التي تمَّ جمعُها من الشَّبابِ الجامعيِّ بجامعةِ شقراءَ، من خلالِ تطبيقِ الاستبيانِ، فجميعُ طلابِ المرحلةِ الجامعيةِ في جامعةِ شقراءَ هم مجتمعُ هذه الدِّراسةِ، ولتحقيقِ أغراضِ هذه الدِّراسةِ تمَّ سحبُ عينةٍ غيرِ احتماليةٍ من الفئةِ العُمريةِ (١٨-٢٤) سنةً التي تَدرسُ الآنَ في المرحلةِ الجامعيةِ من الذُّكورِ، وتمَّ سحبُ عينةٍ غيرِ احتماليةٍ من الشَّبابِ الجامعيِّ بجامعةِ شقراءَ بلغَ حجمُها (٣٠٠) مفردةً. هذا، وتمَّ اختبارُ صدقِ أداةِ الدراسةِ من خلالِ عرضِ محتواها على خبراءَ، وأساتذةٍ متخصصينَ في علمِ الاجتماعِ من جامعةِ تبوكَ، وجامعةِ الإمامِ مُحمدِ بن سُعودٍ، وجامعةِ نايفِ العربيةِ للعُلُومِ الأمنيةِ ، كما تمَّ اختبارُ ثباتِ أداةِ الدِّراسةِ من خلالِ عينةٍ تجريبيةٍ، شملت (٥٪) من العينةِ، وبلغَ مُعاملُ الثَّباتِ ألفا كرونباخ (٨٨٪) .

تاسعًا- خصائصُ عينةِ الدِّراسةِ :

جدول رقم (١) متوسطُ أعمارِ عينةِ الدِّراسةِ

متوسطُ الأعمار	العددُ	النِّسبةُ
١٨-٢٠	١٠٥	٣٥
٢٠-٢٢	٩٩	٣٣
٢٢-٢٤	٩٦	٣٢
الإجمالي	٣٠٠	١٠٠٪

تُظهِرُ بياناتُ الجدولِ رقم (١) متوسطَ أعمارِ عينةِ الدِّراسةِ من الشبابِ من جامعةِ شقراءَ، حيث يَتَبينُ أنَّ متوسطاتِ الأعمارِ متقاربةٌ بينَ عينةِ الدراسة، ومُقسَّمَةٌ إلى ثلاثِ شرائحَ، تَرتبطُ بشكلٍ أساسيٍّ بطبيعةِ المرحلةِ الجامعية، حيث نجدُ أنَّ (٣٥٪) من أفرادِ العينةِ متوسطُ أعمارِهم ما بين (٢٠-١٨) سنة، وهي الشَّريحةُ الأصغرُ عمراً من الشبابِ من عينةِ الدراسة. أما الشَّريحةُ العُمريةُ الثَّانيةُ فبلغت (٣٣٪) متوسطُ أعمارها ما بين (٢٠-٢٢) سنة، ثُمَّ الشَّريحةُ العمريةُ الأكبرُ عمراً، والتي بلغت (٣٢٪) وتتراوحُ أعمارُهُم ما بين (٢٤-٢٢) سنة.

جدول رقم (٢) المستوياتُ الجامعيةُ لعينةِ الدِّراسة

المستوياتُ الجامعية	العددُ	النِّسبة
المستوى الأول والثاني	٥٠	١٦,٦
المستوى الثالث والرابع	٥٥	١٨,٤
المستوى الخامس والسادس	٩٨	٣٢,٦
المستوى السابع والثامن	٩٧	٣٢,٤
الإجمالي	٣٠٠	١٠٠٪

تُوضِّحُ بياناتُ الجدولِ رقم (٢) المستوياتِ الجامعيةَ لعينةِ الدراسة، والتي ترتبطُ بشكلٍ أساسيٍّ بمتوسطِ أعمارِ الشَّبابِ في عينةِ الدِّراسة، حيث يُلاحَظُ أنَّ هناك توزيعاً مُتقارباً لعينةِ الدراسةِ على كافةِ المستوياتِ الدراسية؛ حتى يكونَ هناك تمثيلٌ جيدٌ لكُلِّ الأعمارِ، ولكافةِ المستوياتِ الدراسية، وهو ما يعني خِبراتٍ معرفيةً مختلفةً، حيث نجدُ أنَّ (٣٢.٦٪) من أفرادِ العينةِ في المستوى الخامسِ والسَّادسِ، يليهم (٣٢.٤٪) من أفرادِ العينةِ في المستوى السَّابعِ والثَّامنِ، في المقابلِ، نجدُ المستوى الثَّالثَ، والرَّابعَ بلغ (١٨.٤٪) ثم (١٦.٦٪) في المستوى الأولِ والثَّاني.

جدول رقم (٣) التَّقديراتُ الجامعيةُ لعينةِ الدِّراسة

التَّقديراتُ الجامعية	العددُ	النِّسبة
مقبول	٥٢	١٧,٣
جيد	١٣٢	٤٤
جيد جدا	٧٦	٢٥,٣
ممتاز	٤٠	١٣,٤
الإجمالي	٣٠٠	١٠٠٪

تُوضِّحُ بياناتُ الجدولِ رقم (٣) التَّقديراتِ الجامعيةَ لعينةِ الدِّراسةِ، والتي لم تكنْ بطبيعتِها نِهائيةٌ، وإنَّمَا تُؤشِّرُ للحالةِ التَّعليميةِ، والدراسيةِ لعينةِ الدراسةِ خلالَ المرحلةِ الجامعيةِ، حيثُ يُلاحَظُ من بياناتِ الجدولِ أنَّ النِّسبةَ الأكبرَ من عينةِ الدِّراسةِ (٤٤٪) تقديراتُهُم الجامعيةُ جيدٌ (B) و(٢٥.٣٪) تقديراتُهُم الجامعيةُ جيدٌ جدًا (+B)، ثم (١٣.٤٪) كانت تقديراتُهُم ممتازٌ (A)، وأخيرًا (١٧.٣٪) من عينةِ الدِّراسةِ تقديراتُهُم مقبولٌ .

جدول رقم (٤)

متوسطُ الدَّخلِ الشَّهريِّ لأُسَرِ عينةِ الدِّراسةِ

الدَّخلُ الشَّهريُّ	العددُ	النِّسبةُ
أقل من ٤٠٠٠ ريال	١٨	٦
٤٠٠٠-٧٠٠٠	١٧٤	٥٨
٧٠٠٠-١٠٠٠٠	٥٥	١٨,٣
أكثر من ١٠٠٠٠ ريال	٥٣	١٧,٧
الإجمالي	٣٠٠	١٠٠٪

تُظهِرُ بياناتُ الجدولِ رقم (٤) متوسطَ الدَّخلِ الشَّهريِّ لأسرةِ عينةِ الدراسةِ من الشبابِ، حيثُ يتبينُ أنَّ (٥٨٪) من أُسرِ عينةِ الدراسةِ تتراوحُ دُخولُهم ما بين (٤٠٠٠ إلى ٧٠٠٠ ريال) سُعودي، وهي النِّسبةُ الأكبرُ، والأكثرُ شُيوعًا بين عينةِ الدراسةِ، وأنَّ (١٨.٣٪) من أسرِ عينةِ الدراسةِ متوسطُ دخولِهم الشَّهريةِ تتراوحُ ما بين (٧٠٠٠ إلى ١٠٠٠٠ ريال) سعودي، يليها (١٧.٧٪) من أسرِ عينةِ الدِّراسةِ دُخولُهم الشهريةُ أكثرُ من (١٠٠٠٠ ريال) سعودي، بينما أقلُّ نسبةٍ جاءت (٦٪) للأسرِ التي تَنخفِضُ دُخولُهُم عن (٤٠٠٠ ريال) سعودي.

جدول رقم (٥)

نَوعُ الكليةِ بين عينةِ الدِّراسةِ

نوعُ الكليةِ	العددُ	النِّسبةُ
كلية نظرية	١٥٠	٥٠
كلية علمية	١٥٠	٥٠
الإجمالي	٣٠٠	١٠٠٪

تُوضِّحُ بياناتُ الجدولِ رقم (٥) نوعيةَ الكليةِ بين عينةِ الدراسةِ من الشِّبابِ بجامعةِ شقراءَ ، حيثث راعى البَاحثُ أنءِ يكونَ هناك تمثيلٌ مُتساوٍ في سحبِ العينةِ غيرِ

الاحتماليةِ من الشَّبابِ الجامعيِّ بين الكلياتِ النَّظريةِ، والكلياتِ العمليةِ بجامعةِ شقراءَ ، والتي بلغت (٥٠ %) للكليةِ النَّظريةِ، وللكليةِ العمليةِ بجامعةِ شقراءَ .

جدول رقم (٦)

مدةُ ساعاتِ استخدامِ الإنترنتِ، وتطبيقاتُهُ بينِ عينةِ الدراسةِ يوميًّا

السَّاعاتُ	العددُ	النِّسبةُ
أقل من ٣ ساعات	٤٤	١٤,٧
٣- ٦ ساعات	١٦٤	٥٤,٦
٦-٩ ساعات	٦٨	٢٢,٧
أكثر من ٩ ساعات	٢٤	٨
الإجمالي	٣٠٠	٪١٠٠

تُوضِّحُ بياناتُ الجدول رقم (٦) مدةَ ساعات استخدام الإنترنت، وتطبيقاته بين عينة الدراسة يوميًّا، حيثُ يُلاحَظُ أنَّ (٥٤.٦٪) من أفراد العينة متوسطُ استخدام للإنترنت يوميًّا يتراوحُ ما بين (٦-٣) ساعات يوميًّا، ولاشكَّ أنَّ هذا متوسطٌ ليس بالقليل، وتجاوزَ (٥٠٪) من أفراد العينة يقضونَ هذا الوقتَ الطَّويلَ على الإنترنت، ممَّا يعرِّضُهُم بشكل أكبر للتَّعرضِ إلى الهجمات الإلكترونية، والجرائم السَّيبرانية، كذلك الحالُ، نجدُ أنَّ (٢٢.٧) يستخدمُونَ الإنترنتَ لعدد ساعات تتراوحُ ما بينَ (٩-٦) ساعات، وهو عددُ ساعات كبير للغاية، كذلك كانَ هناك (٨٪) يستخدمُونَ الإنترنتَ لأكثرَ من (٩) ساعات يوميًّا في مقابل نسبة قليلة بلغت (١٤.٧٪) يستخدمُونَ الإنترنتَ أقلَّ من (٣) ساعات .

جدول رقم (٧)

استخداماتُ الإنترنت بينَ عينة الدَّراسة

استخداماتُ الإنترنتِ	العددُ	النِّسبةُ
التَّحصيلُ العلميُّ والدراسةُ	١٠٢	٣٤
التَّرفيهُ وشغلُ الأوقاتِ	٢٨	٩,٣
متابعةُ الأخبارِ المحليةِ والعالميةِ	١٧	٥,٧
الألعابُ	٤٤	١٤,٦
التَّواصلُ الاجتماعيُّ وتكوينُ الصَّداقاتِ	١٠٩	٣٦,٤
الإجمالي	٣٠٠	٪١٠٠

تُوضِّحُ بياناتُ الجدول رقم (٦) استخدامات الشباب من عينة الدراسة للإنترنت، حيث يَتبينُ أنَّ هناك تفاوتًا في استخداماتِ الإنترنتِ بينَ الشَّبابِ من عينةِ الدَّراسةِ، غيرَ أنَّ

النِّسبةَ الأكبرَ من استخدامِ الإنترنت بينَ الشباب نسبةُ (٣٦.٤٪) اتَّجهت نحوَ التَّواصل الاجتماعيِّ، وتكوين الصَّداقات عبرَ مواقع التَّواصل الاجتماعيِّ المختلفة، وهي نسبةٌ مرتفعةٌ، واستخدامٌ كثيفٌ للإنترنتَ؛ بقصدش التَّواصلِ الاجتماعي، وهو ما يُوضحُ سببَ ارتفاع متوسط عدد ساعات استخدام الإنترنت، أمَّا النِّسبةُ الأُخرى الموازيةُ لاستخدامات الإنترنت بينَ عينة الدِّراسة فكانت بقصد الدراسة، والتَّحصيل العلميِّ بنسبة (٣٤٪) وهو استخدامٌ أغلبُهُ أصبحَ الآنَ إجباريًّا من خلال الدُّخول على منصات الجامعات والتَّعليم عن بُعد لاسيَّما في فترة انتشار فَيروسٍ كورونا. يليهم نسبةُ (١٤.٦٪) تَستخدمُ الإنترنتَ؛ بهدف اللَّعبِ عبرَ الفضاءِ الإلكترونيِّ مع الأصدقاء سواءً في العالم الحقيقيِّ، وفي الفضاء الافتراضيِّ، وهو ما يُعَدُّ مدخلًا ملائمًا للاختراق، وسَرقة البيانات... إلخ.

جدول رقم (٨)

تَعرُّضُ عينةُ الدراسة للجرائم السَّيبرانية

التَّعرضُ	العددُ	النِّسبة
نعم	١٨٩	٦٣
لا	١١١	٣٧
الإجمالي	٣٠٠	١٠٠٪

تُظهرُ بياناتُ الجدول رقم (٨) تَعرُّضَ عينة الدراسة للجرائم السَّيبرانية، وذلك في ضَوءِ الاستخدام المرتفعِ لعينة الدِّراسة للإنترنت، وعددَ السَّاعات الطَّويلة التي يَقضُونَها عبرَ الفضاءِ الإلكتروني، حيث تُظهرُ بياناتُ الجدول أنَّ (٦٣٪) من أفراد العينة من الشَّباب تَعرَّضُوا لخبرة الجرائمِ السَّيبرانية، في مقابل (٣٧٪) لم يتعرضُوا لخبرة الجرائم السَّيبرانية عبرَ الفضاء الرَّقميِّ .

جدول رقم (٩)

نوعيةُ الجرائمِ السَّيبرانيةِ التي تَعرَّضت لها عينةُ الدِّراسةِ

نوعيةُ الجرائمِ	العددُ	النِّسبةُ
سَرقةُ بياناتِ الهاتفِ من صُورٍ وفِيديوهاتٍ	٩٨	٥١,٩
التَّصيُّدُ والاحتيالُ الإلكترونيُّ	٧	٣,٧
الابتزازُ عبرَ الإنترنتِ	٤	٢,٢
فَيروساتٌ لأجهزةِ الهاتفِ والحاسبِ الآليِّ	٢٦	١٣,٧
تَحرُّشٌ ومُضايَقَاتٌ ونشرُ الإباحيةِ	١٣	٦,٨
التَّهكيرُ واختراقُ الحساباتِ الشَّخصيةِ	٣٩	٢٠,٦
التَّزويرُ	٢	١,١
الإجمالي	١٨٩	٪١٠٠

تَعكسُ بياناتُ الجدولِ رقم (٩) الجرائمَ السَّيبرانيةَ التي وَقَعَ الشَّبابُ من عينةِ الدِّراسةَ ضَحَايَاها، حيثُ يتبينُ أنَّ أكثرَ من نصفِ عينةِ الدَّراسةِ (٥١.٩٪) من أفرادِ العينةِ من الشَّبابِ تَعرضُوا لسَرقةِ بياناتِ الهاتفِ من صُورٍ، وفيديوهاتٍ، ممَّا عَرَّضَهم للعديدِ من المشكلاتِ سواءً ارتبطت بالابتزازِ، والاستنزافِ الماديِّ؛ خوفًا من نشرِ الصُّورِ، والفيديوهاتِ الخاصةِ، وبلغت نسبةُ تَعرضِ أفرادِ العينةِ للابتزازِ عبرَ الإنترنتِ (٢.٢٪) ولا شكَّ أنَّ هذه السَّرقةَ لصورٍ، وفيديوهاتِ الهاتفِ تحدثُ نتيجةَ جهلِ بعضِ الشَّبابِ بكيفيةِ الحفاظِ على الخُصوصيةِ، وتأمينِ البياناتِ الخاصةِ، كما تَعرَّضَ (٢٠.٦٪) من أفرادِ عينةِ الدراسةِ من الشبابِ لجرائمِ التَّهكيرِ، واختراقِ الحساباتِ الشَّخصيةِ، ولاسيَّما البريدُ الإلكترونيُّ، وحساباتِ مواقعِ التَّواصلِ الاجتماعيِّ: كتويتر، أو انستجرام، أو فيس بوك، وهو ما يُؤدِي إلى سَرقةِ بياناتٍ، وصُورٍ شخصيةٍ، وكذلك الحالُ استغلالُ تلك المواقعِ، والحساباتِ الشخصيةِ في نشرِ الإباحيةِ بين أفرادَ المجتمعِ، وبين الأصدقاءِ، والمعارفِ، وهو ما يُعرِّضُ الشَّخصَ للكثيرِ من الإحراجِ.، كما وَاجهَ (١٣.٧٪) من أفرادِ العينةِ لفَيروساتٍ خبيثةٍ أَضرَّت بأجهزتِهم الشَّخصيةِ، وهواتفِهم الذَّكيةِ، ممَّا يُؤدِي إلى سُهُولةِ الاختراقِ، ونقلِ بياناتٍ، والاطِّلاعِ عليها، كما أوضحَ (٦.٨٪) من أفرادِ العينةِ من الشَّبابِ لتَعرُّضِهم للتَّحرشِ، والمضايقاتِ، ونشرِ الإباحيةِ عن طريقِ الرَّسائلِ المتكررةِ التي يَتَلَقَّونَها عبرَ الشَّبكةِ. وفي المجملِ، فإنَّ حجمَ تَعرُّضِ الشبابِ من عينةِ الدراسةِ، ووقوعِهم كضحايا للجرائمِ السَّيبرانيةِ يُنذرُ بالكثيرِ من المخاطرِ، والتَّهديداتِ التي تُواجِهُ

الشبابَ؛ نتيجةَ تفاعلاتِهم، واستخدامِهم الكثيفِ للإنترنت، حيثُ تَتَفاوتُ الجرائمُ السَّيبرانيةُ التي يَتعرَّضُونَ إليها ما بينَ الأقلِّ خُطورةً: كالمُضايَقاتِ، والملاحقةِ عبرَ البريدِ الإلكترونيِّ إلى الجرائمِ الأشدِّ خطراً: كالاستدراجِ، والاحتيالِ، وسَرقةِ البياناتِ، والتَّشهيرِ، والابتزازِ.

عاشراً ــ الدَّراسةُ المَيدانيةُ، والتَّحليلُ السُّوسيولوجيُّ لقضايا الدَّراسةِ :

(١) مفهومُ الجرائمِ السَّيبرانيةِ لدى عينةِ الدِّراسةِ :

تُوصَفُ الجريمةُ السَّيبرانيةُ عموماً بأنَّها أنشطةٌ إجراميةٌ تَستخدِمُ تُكنولوجيا المعلوماتِ الحديثةِ، مثل: تكنولوجيا الحاسوبِ، وتكنولوجيا الشَّبكاتِ، وما إلى ذلك. وهناك أنواعٌ عديدةٌ للجرائمِ السَّيبرانيةِ، بما في ذلك الوصولُ غيرُ القانونيِّ، مثل: (القرصنةِ)، الاعتراضِ غيرِ القانونيِّ، تدخُّلِ البياناتِ، تدخُّلِ الأنظمةِ، إساءةِ استخدامِ الأجهزةِ، التَّزويرِ (سَرقةِ الهُويةِ)، الاحتيالِ الإلكترونيِّ، وما إلى ذلك.

جدول رقم (١٠)

المفهومُ السَّائدُ للجريمةِ السَّيبرانيةِ بينَ عينةِ الدِّراسةِ

م	المفهومُ السَّائدُ للجريمةِ السَّيبرانيةِ	متوسطٌ حسابيٌّ	انحرافٌ معياريٌّ	النِّسبةُ المئويةُ	اتجاهُ العينةِ
١	اختراقاتٌ غيرُ مشروعةٍ لأجهزةِ الحاسبِ الآليِّ	١,٨٠	٠,٤٠	٩٠	موافق
٢	أنشطةٌ إجراميةٌ تَضرُّ بمستخدمي الإنترنتِ، وحساباتِهم الشَّخصيةِ	١,٩٠	٠,٣٠	٩٥	موافق
٣	سَرقةٌ، وابتزازٌ، وتصيدٌ احتياليٌّ لضحايا الإنترنتِ	١,٩٣	٠,٢٥	٩٦,٥	موافق
٤	إساءةُ استخدامِ الإنترنتِ، وتطبيقاته ومواقع التواصل الاجتماعي	١,٦٠	٠,٤٩	٨٠	موافق
٥	مطارداتٌ، ومُضايَقاتٌ إلكترونيةٌ يترتَّبُ عليها خسائرُ للفردِ	١,٩٧	٠,١٨	٩٨,٥	موافق
	الاتِّجاهُ العام	١,٨٤	٠,٣٧	٩٢	موافق

تُوضِّحُ بياناتُ الجدولِ رقم (١٠) المفهومَ السَّائدَ بين عينةِ الدراسةِ من الشبابِ الجامعيِّ للجرائمِ السَّيبرانيةِ، ويُلاحَظُ من بياناتِ الجدولِ أنَّ الاتِّجاه العام بين عينةِ الدراسةِ، والذي بلغَ

(٩٢٪) يُظهِرُ اتجاهاً إيجابيًّا بينَ عينةِ الدراسةِ، وفَهماً جيداً، وإدراكًا لمعنى الجرائمِ السَّيبرانيةِ، حيثُ وافقَ الغالبيةُ من العينةِ على المضمونِ الواردِ بالجدولِ، والذي يُلخِّصُ مضمونَ، ومفهومَ الجرائمِ السيبرانيةِ، ويتبينُ من بياناتِ الجدولِ أنَّ هناك تقارباً في

مضمونِ الجرائمِ السَّيبرانيةِ، غيرَ أنَّ المفهومَ الأكثرَ شُيوعًا، وقَبُولاً بين عينةِ الدراسةِ للجرائمِ السيبرانيةِ هو مطارداتٌ، ومُضايَقاتٌ إلكترونيةٌ يترتبُ عليها خسائرُ للفردِ بنسبةِ (٩٨.٥٪) وبمتوسطٍ حسابيٍّ (١.٩٧) وهو ما يُلخِّصُ الحالةَ التي يَعيشُها أفرادُ العينةِ، ويَتعرَّضُونَ إليها من مضايقاتٍ إلكترونيةٍ، ومطارداتٌ مُستمرةٌ عبرَ الفضاءِ الإلكترونيِّ، أما المفهومُ الثاني الأكثرُ شُيوعًا، وقَبُولاً بينَ عينةِ الدِّراسةِ لمفهومِ الجرائمِ السَّيرانيةِ فهو سَرقةٌ، وابتزازٌ، وتصيدٌ احتياليٌّ لضحايا الإنترنتِ بنسبة (٩٦.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٣) وهو ما يَعكِسُ حجمَ الخُطورةِ التي يُدركُها الشَّبابُ من أفرادِ العينةِ من الشَّباب، والتي تُوضِّحُ أنَّ الجرائمَ السيبرانيةَ من ضمنِ معانيها، ومستهدفاتِها السَّرقةُ، والابتزازُ، عبرَ الشبكاتِ الافتراضيةِ، أما المعنى، والمَضمونُ الثالثُ فهو أنشطةٌ إجراميةٌ، تضرُّ بمستخدمي الإنترنتِ، وحساباتِهم الشَّخصيةِ بنسبة (٩٥٪) ومتوسطٍ حسابيٍّ (١.٩٠) ثُم اختراقاتٌ غيرُ مشروعةٍ لأجهزةِ الحاسبِ الآليِّ بنسبة (٩٠٪) ومتوسطٍ حسابيٍّ بلغ (١.٨٠) ثُمَّ إساءةُ استخدامِ الإنترنتِ، وتطبيقاتِه، ومواقعِ التّواصلِ الاجتماعيِّ بنسبة (٨٠٪) ومتوسطٍ حسابيٍّ بلغ (١.٦٠) . وفي هذا الصَّدد، أشارت دراسةُ (الصبان، ٢٠١٩) إلى أنَّ أكثرَ الجرائمِ الرَّقميةِ انتشاراً هي جرائمُ الاحتيالِ العاطفيِّ، والإباحيةُ، كما أنَّ من أبرزِ العواملِ التي ساعدت على انتشارِ الجرائمِ السَّيبرانيةِ هي العواملُ المرتبطةُ بشخصيةِ المجرمِ .

(٢) دوافعُ ومخاطرُ الجرائمِ السَّيبرانيةِ على الشَّبابِ :

جدول رقم (١١)

دوافعُ الجريمةِ السَّيبرانيةِ من وِجهةِ نظرِ عينةِ الدِّراسةِ

م	دوافعُ الجريمةِ السَّيبرانية	متوسطٌ حسابيٌّ	انحرافٌ معياريٌّ	النِّسبةُ المِئويةُ	اتجاهُ العينةِ
١	إثباتُ الذَّاتِ، وتطويعِ تِقنيةِ الاتصالاتِ لرغباتِ مرتكبيها	١,٩٧	٠,١٨	٩٨,٥	موافق
٢	تحقيقُ أهدافٍ ماديةٍ باستغلالِ مهاراتِ التعاملِ مع النتِ، والبحثِ عن الثَّراءِ	١,٩٧	٠,١٦	٩٨,٥	موافق
٣	الانتقامُ من أشخاصٍ، والإساءةُ لهم، والتَّشهيرُ بهم	١,٤٣	٠,٥٠	٧١,٥	غير موافق
٤	الحصولُ على معلوماتٍ، وبياناتٍ سريةٍ، واستغلالِها	١,٥٧	٠,٥٠	٧٨,٥	موافق
٥	التَّسليةُ، والتَّرفيهُ، والتُّلاعبِ بالآخرينَ	١,٩٣	٠,٢٥	٩٦,٥	موافق
	الاتِّجاهُ العام	١,٧٧	٠,٤٢	٨٨,٥	موافق

تَتَنوَّعُ دوافعُ ارتكاب الجريمة السَّيبرانية ما بينَ: دوافعَ ذهنية لإثبات الذَّات، ودوافعَ للتَّسلية، وثالثة: خاصةٌ بالانتقام، ورابعة: دوافعَ مادية، هذا فضلاً عن الدَّوافع السِّياسية المرتبطة باختراقات الشبكات الدُّولية، وتحقيق أهداف سياسية وأمنية، وتختلفُ دوافعُ ارتكاب جرائم الجريمة السَّيبرانية ما بينَ المكاسب المالية، والانتقام، ونشر الأفكار، والأيديولوجيا، والتَّجسس، وتشويه السُّمعة، وما إلى ذلك. وعلى الرُّغم من حقيقة أنَّ دوافعَ مرتكبي الجرائم السيبرانية آخذةٌ في التَّغير تاريخيًّا، بالنَّظر إلى الأضرار النَّاجمة، والفوائد المالية لحالات الجرائم السَّيبرانية، فإنَّ الدافعَ الماديَّ لا يزالُ هو الدافعُ الرَّئيسيُّ، ويُعزِّزُ مجرمو الجرائم الإلكترونية الجُدُدُ إمكانيات الثَّراء الماليِّ، ويعملُ كُلُّ مخترق، أو مُطوِّر برمجيات خبيثةً؛ من أجل المال، وليس فقطْ من أجل الشُّهرة (Ilievski & Bernik, 2016;11). وفي هذا الإطار تُوضحُ بياناتُ الجدول رقم (١١) دوافعَ الجريمة السَّيبرانية من وجهة نظر عينة الدراسة، حيثُ يَتَكشَّفُ أنَّ الاتِّجاهَ العام بينَ عينة الدِّراسة بالموافقة على الدوافع المذكورة بالجدول، وبلغت نسبةُ الموافقة (٨٨.٥٪) ومتوسط حسابيٍّ بلغ (١.٧٧) . ويتبينُ من بيانات الجدول أنَّ إثباتَ الذَّات، وتطويعَ تقنية الاتصالات لرغبات مرتكبيها، والتي بلغت نسبةَ (٩٨.٥٪) ومتوسطًا حسابيًّا بلغَ (١.٩٧٪) كانت في المرتبة الأولى بالتَّوازي مع تحقيق أهداف مادية باستغلال مهارات التَّعامل مع النتِّ، والبحث عن الثَّراء بنسبة (٩٨.٥٪) ومتوسط حسابيٍّ بلغ (١.٩٧) وهو ما يعني أنَّ الدافعَ الماديَّ المرتبطَ بتحقيق الثَّراء الماليِّ السَّريع يُعدُّ من الأسباب الجوهرية لانتشار الجرائم السَّيبرانيةِ مع الدَّافعِ المرتبطِ بإثباتِ الذَّاتِ عبرَ الفضاءِ الإلكترونيِّ من خلالِ السَّيطرةِ

على تحركات الأفراد، وتفاعلاتهم السَّيبرانية، أما الدَّافعُ الثالثُ لارتكاب الجرائم السَّيبرانية من وجهة نظر عينة الدِّراسة فكانَ التَّسليةَ، والتَّرفيهَ، والتَّلاعُب بالآخرينَ بنسبة (٩٦.٥٪) ومتوسط حسابيٍّ بلغ (١.٩٣) وهو دافعٌ يرتبطُ بسمات شخصية مرتكب تلك الجرائم، وحداثة السِّنِّ، ثُم الحصولُ على معلومات، وبيانات سرية، واستغلالها في المرتبة الرَّابعة بنسبة (٧٨.٥٪) ومتوسط حسابيٍّ بلغ (١.٤٣) وهو ما يعني أنَّ دافعَ الحصول على معلومات، وبيانات هو هدفٌ وسيطٌ مرتبطٌ بتحقيق هدف أكبرَ، وهو توظيفُ تلك البيانات في الابتزاز، أو استغلال الأفراد، وترهيبهم.

وأخيراً، جاء رفضُ عينة الدِّراسة على الدَّافع المرتبط بالانتقام من أشخاص، والإساءة لهم، وذلك بنسبة منخفضة بلغت (٧١.٥٪) ومتوسط حسابيٍّ بلغ (١.٤٣) وهو ما يعني أنَّ الدَّوافعَ الماديةَ، وإثباتَ الذَّات هي الأهدافُ، والدوافعُ الأهمُّ في ارتكاب الجرائم السَّيبرانية .

جدول رقم (١٢)

مخاطرُ الجريمة السَّيبرانية من وجهة نظر عينة الدِّراسة

م	مخاطرُ الجريمةِ السَّيبرانيةِ	متوسطٌ حسابيٌّ	انحرافٌ معياريٌّ	النِّسبةُ المئويةُ	اتجاهُ العينةِ
١	تشويهُ السُّمعةِ، والإضرارُ بها، والابتزازُ لأفرادِ المجتمع	١,٩٢	٠,٢٨	٩٦	موافق
٢	التَّحرشُ الجنسيُّ، ونشرُ الإباحيةِ	١,٦٦	٠,٤٧	٨٣	موافق
٣	سَرقةُ البياناتِ، والصُّور، والفِيديوهاتِ	١,٧٠	٠,٤٦	٨٥	موافق
٤	وُقوعُ ضحايا من فئاتٍ مختلفةٍ في المجتمع بفعلِ الابتزاز	١,٧٤	٠,٤٤	٨٧	موافق
٥	خسائرُ ماديةٌ، والاحتيالُ الماليُّ	١,٦٠	٠,٤٩	٨٠	موافق
٦	انتهاكُ الخُصوصيةِ، وتَزييفُ المعلوماتِ	١,٥٩	٠,٤٩	٧٩,٥	موافق
٧	انتشارُ الإرهابِ الإلكترونيِّ، وتهديدُ الأمن السَّيبرانيِّ	١,٥٣	٠,٥٠	٧٦,٥	موافق
	الاتِّجاهُ العام	١,٦٨	٠,٤٧	٨٤	موافق

إنَّ ارتكابَ الجرائمِ السَّيبرانيةِ هو فعلٌ إجراميٌّ غيرُ قانونيٍّ يترتبُ عليه جُملةٌ من الآثارِ، والمخاطرِ الاجتماعيةِ، والاقتصاديةِ، والأمنيةِ العديدةِ، حيثُ تَستهدِفُ أمنَ الأفرادِ الشَّخصيِّ، وتُخترَقُ حساباتُهُم، وبياناتُهُم الشَّخصيةُ؛ بهدفِ ابتزازِهِم، والرِّبحِ من ورائهم.

ويَتَّضحُ من بياناتِ الجدولِ رقم (١٢) مخاطرُ الجرائمِ السَّيبرانيةِ من وِجهةِ نظرِ عينةِ الدِّراسةِ، حيثُ يَتبينُ من الجدولِ أنَّ الاتِّجاهَ العام السَّائدَ بينَ عينةِ الدِّراسةِ بالموافقةِ على مخاطرِ الجريمةِ السَّيبرانيةِ بلغت (٨٤٪) وبمتوسطٍ حسابيٍّ (١.٦٨) وهو ما يعني إدراكَ، ووعيَ عينةِ الدراسةِ من الشَّبابِ الجامعيِّ بالمخاطرِ العديدةِ لانتشارِ الجرائمِ السيبرانيةِ، وهو ما يدفعُهُم أخذُ الحَيطةِ، والحذرِ في تعاملاتِهم عبرَ الفضاءِ السَّيبرانيِّ الذي تَحملُ تِقنياتُهُ، وتطبيقاتُهُ ملامحَ الخُطورةِ الاجتماعيةِ. كذلك أوضحت بياناتُ الجدولِ ترتيبَ ملامحِ الخُطورةِ للجرائمِ السيبرانيةِ من وِجهةِ نظرِ عينةِ الدراسةِ، حيثُ يتبينُ أنَّ تشويهَ السُّمعةِ، والإضرارَ بها، والابتزازَ لأفرادِ المجتمعِ جاءت في المرتبةِ الأولى بنسبةِ (٩٦٪) ومتوسطٍ حسابيٍّ (١.٩٢) وهو ما يَعكسُ حجمَ الخطرِ الذي يُحيطُ بأفرادِ المجتمعِ؛ نتيجةَ انتشارِ الجرائمِ السَّيبرانيةِ، وتَزايُدِ معدلاتِها، ومن ثَم، كان أكبرُ خطرٍ من وِجهةِ نظرِ العينةِ تشويهَ السُّمعةِ، والابتزازَ، وما يَتبَعُهُ من آثارٍ اجتماعيةٍ عديدةٍ، والنَّاجمُ عن اختراقاتٍ، وسَرقةِ بياناتٍ، وتفاعلاتٍ بدونِ وعيٍ على الفضاءِ الرَّقميِّ. أما المرتبةُ الثَّانيةُ، فكانت وُقوعَ ضحايا من فئاتٍ مختلفةٍ في المجتمعِ بفعلِ الابتزازِ بنسبةِ (٨٧٪) ومتوسطٍ حسابيٍّ بلغ (١.٧٤) وهو نتيجةٌ طبيعيةٌ للابتزازِ الذي أصبح متكرراً، وشائعاً مع ارتكابِ الكثيرِ من الجرائمِ السَّيبرانيةِ، فوقوعُ ضحايا من فئاتٍ عُمريةٍ مختلفةٍ أمرٌ شائعٌ ومتكررٌ ، في مقدمتِها الشَّرائحُ العُمريةُ الأصغرُ: الشَّبابُ والمراهقون. أما المرتبةُ الثَّالثةُ، فكانت سَرقةَ البياناتِ، والصُّورِ، والفيديوهاتِ، واختراقَ الخصوصياتِ بنسبةِ (٨٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٧٠) وهو ما يَترتبُ عليه جملةٌ من المشكلاتِ الاجتماعيةِ، والأمنيةِ التي تُواجِهُ أفرادَ المجتمعِ الذين تَعرَّضُوا للاختراقِ، وتمَّ انتهاكُ خُصوصيَّتِهم. وفي هذا الصَّددِ أشارت دراسةُ (الجفناوي، ٢٠١٦، الجراحي، ٢٠١٥) إلى المخاطرِ العديدةِ للجرائمِ السَّيبرانيةِ، ولاسيَّما مع الاختراقاتِ التي تَتمُّ أثناءَ نقلِ الصُّورِ، والفيديوهاتِ الشَّخصيةِ، وهو ما يُوقِعُ الضحايا في فَخِّ الابتزازِ، كذلك وقوعُ الشَّبابِ ضحايا المواقعِ المعلوماتيةِ المشبوهةِ، وهو ما يَدفَعُ إلى ضرورةِ سَنِّ القوانينِ التي تَحُدُّ من انتشارِ الجرائمِ السَّيبرانيةِ، بينما جاء في المرتبةِ الرَّابعةِ، التَّحرشُ الجنسيُّ، ونشرُ الإباحيةِ بنسبةِ (٨٣٪) ومتوسطٍ حسابيٍّ بلغ (١.٦٦) ورغمَ أنَّ هذه الخطورةَ تأتي في المرتبةِ الرَّابعةِ إلا أنَّ نسبَتَها

مرتفعةٌ، وتَعكِسُ خطراً حقيقيًّا، يُحيطُ بالأفرادِ في الفضاءِ السَّيبرانيِّ، غيرَ أنَّ الإبلاغَ عن تلك النَّوعيةِ من الجرائمِ يُحيطُهُ قدرٌ من السِّريةِ؛ لطبيعةِ مُجتمَعِنا المحافظِ، أما المرتبةُ الخامسةُ، فكانت خسائرَ ماديةً، والاعتداءَ على أموالِ البعضِ من أفرادِ المجتمعِ، والاحتيالَ الماليَّ بنسبةِ (٨٠٪) ومتوسطٍ حسابيٍّ بلغ (١.٦٠) وهذه نتيجةٌ طبيعيةٌ للانخراطِ في المجتمعِ الرَّقميِّ، والوقوعِ ضحيةً للجرائمِ السَّيبرانيةِ، بينما جاءت المرتبةُ السَّادسةُ، انتهاكُ الخصوصيةِ، وتزييفُ المعلوماتِ بنسبةِ (٧٩.٥٪) بمتوسطٍ حسابيٍّ بلغ (١.٥٩) وهو ما يَترتبُ عليه خسائرُ عديدةٌ للأفرادِ والمجتمعاتِ، وأخيراً، في المرتبةِ السَّابعةِ، انتشارُ الإرهابِ الإلكترونيِّ، وتهديدُ الأمنِ السَّيبرانيِّ بنسبةِ (٧٦.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٥٣) وربَّما تكونُ تلك الخطورةُ في المرتبةِ الأخيرةِ، ليس من مُنطلَقِ أنَّها الأقلُّ خطورةً، ولكنْ الأقلُّ بالنِّسبةِ لأفرادٍ، وإدراكِ عينةِ الدراسةِ بالخطورةِ المباشرةِ، والتي تَنعكِسُ بشكلٍ مباشرٍ على حياتِهم.

جدول رقم (١٣)

الوسائلُ الأكثرُ تأثيراً في نشرِ الجريمةِ السَّيبرانيةِ من وجهةِ نظرِ عينةِ الدِّراسةِ

م	الوسائلُ والأدواتُ	متوسطٌ حسابيٌّ	انحرافٌ معياريٌّ	النِّسبةُ المئويةُ	اتِّجاهُ العينةِ
١	التَّسوقُ الإلكترونيُّ	١,٩٧	٠,١٦	٩٨,٥	موافق
٢	استخدامُ مواقعِ التَّواصلِ الاجتماعيِّ	١,٩٩	٠,١٠	٩٩,٥	موافق
٣	استخدامُ البريدِ الإلكترونيِّ	١,٧٣	٠,٤٤	٨٦,٥	موافق
٤	استخدامُ البطاقاتِ الإئتمانيةِ	١,٧٨	٠,٤١	٨٩	موافق
٥	المعاملاتُ الإلكترونيةُ عبرَ الهاتفِ الذَّكيِّ	١,٩٦	٠,٢٠	٩٨	موافق
٦	التَّعاملُ مع التَّطبيقاتِ الحديثةِ في الهاتفِ الذَّكيِّ	١,٩٨	٠,١٣	٩٩	موافق
	الاتِّجاهُ العام	١,٩٠	٠,٢٩	٩٥	موافق

يَتضحُ من بياناتِ الجدولِ رقم (١٣) اتجاهاتُ عينةِ الدِّراسةِ نحوَ الوسائلِ الأكثرِ تأثيراً في نشرِ الجريمةِ السَّيبرانيةِ من وجهةِ نظرِ عينةِ الدراسةِ، حيثُ يَتبيَّنُ أنَّ الاتِّجاهَ العامَّ السَّائدَ بين عينةِ الدراسةِ مرتفعٌ بنسبةِ (٩٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٠) وهو ما يعني أنَّ هناك وعياً، وإدراكاً من عينةِ الدراسةِ بشأنِ الوسائلِ الأكثرِ تأثيراً في نشرَ

الجريمةِ السَّيبرانيةِ، وهذا الإدراكُ يُفيدُ بشكلٍ، أو بآخرَ عينةَ الدراسةِ في تفاعلاتِهم، وتعاملاتِهم الرَّقميةِ عبرَ الفضاءِ الرَّقميِّ. وجاءت في المرتبةِ الأولى من حيثُ الوسائلِ الأكثرِ تأثيراً في نشرِ الجريمةِ السَّيبرانيةِ من وجهةِ نظرِ عينةِ الدراسةِ استخدامُ مواقعِ التواصلِ الاجتماعيِّ بنسبة (٩٩.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٧) وهو ما يَعكسُ حجمَ الخطرِ الذي يَتَأَتَّى من خلالِ استخدامِ مواقعِ التواصلِ الاجتماعيِّ بكثرةٍ، وعددَ السَّاعاتِ التي يقضيها الشَّبابُ عبرَ مواقعِ التواصلِ الاجتماعيِّ المختلفةِ، حيثُ يَعتبِرُها الشَّبابُ من عينةِ الدراسةِ أنَّها الوسيلةُ الأكثرُ تأثيراً في نشرِ الجرائمِ السَّيبرانيةِ، حيثُ يَستطيعُ مرتكبو تلك الجرائمِ النَّفاذَ إلى الصُّورِ، والبياناتِ الشَّخصيةِ للضَّحايا، ومحاولةَ ابتزازِهم، والتَّلاعبِ بهم، وهو ما يتطابقُ إلى حدٍّ كبيرٍ مع ما أشارت إليه دراسةُ (المعايطة، ٢٠١٥) والتي أوضحت تَعرُّضَ الشَّبابِ لوسائلِ الإعلامِ الإلكترونيِّ الذي ساعد على نشرِ الفكرِ المُتطرِّفِ بينَ الشَّبابِ، وهو ما يَدفعُ هؤلاء الشبابَ نحوَ نشرِ الأفكارِ المُتطرِّفةِ عبرَ مواقعِ التَّواصلِ الاجتماعيِّ.

(٣) اتجاهاتُ الشَّبابِ نحوَ مخاطرِ الجرائمِ السَّيبرانيةِ :

جدول رقم (١٤)

اتجاهاتُ الشَّبابِ نحوَ الجرائمِ السَّيبرانيةِ

م	الاتجاهاتُ	متوسطٌ	انحرافٌ	النِّسبةُ	اتجاهُ

		حسابيٌّ	معياريٌّ	المِئويةُ	العينةِ
١	تؤدي الجرائمُ السَّيبرانيةُ إلى هدمِ قيمِ المجتمعِ، ونشرِ الفَوضى	١,٩٨	٠,١٤	٩٩	موافق
٢	تزايدُ أعدادِ مرتكبي الجرائمِ السَّيبرانيةِ وضحاياه من مُختَلَفِ فئاتِ المجتمعِ	١,٩٩	٠,٠٨	٩٩,٥	موافق
٣	تَتزايَدُ الجرائمُ السَّيبرانيةُ في الوقتِ الرَّاهنَ بسببِ تكنولوجيا الاتصالاتِ وانتشارِ فَيروس كورونا	٢,٠	٠,٠٦	١٠٠	موافق
٤	جهلُ الضَّحايا بِتِقنياتِ الإنترنتِ سببُ انتشارِ الجرائمِ السَّيبرانيةِ	١,٩٢	٠,٢٧	٩٦	موافق
٥	الشَّبابُ هم الفئةُ الأولى المُستهدَفةُ من الجرائمِ السَّيبرانية	٢,٠	٠,٠	١٠٠	موافق
٦	يَتعرَّضُ الفردُ لتهديداتِ الجرائمِ السَّيبرانية بشكلٍ يوميٍّ	١,٩٧	٠,١٧	٩٨,٥	موافق
٧	يَرتبطُ انتشارُ الجرائمِ السَّيبرانيةِ بمجرمينَ محترفينَ يَمتلِكُون قدراتٍ تِقنيةٍ فائقةٍ	١,٩٦	٠,٢٠	٩٨	موافق
٨	يُتيحُ الفضاءُ الإلكترونيُّ للشَّبابِ فرصَ التَّسلُّل والتَّفاعلِ عبرَ هذا الفضاءِ	١,٩٧	٠,١٨	٩٨,٥	موافق
٩	تَعتمِدُ أساليبُ مكافحةِ الجرائمِ السَّيبرانيةِ على الأسرةِ والرِّقابةِ الأسريةِ	١,٨٥	٠,٣٦	٩٢,٥	موافق
	الاتِّجاهُ العامَّ	١,٩٦	٠,٢	٩٨	موافق

تُوضِّحُ بياناتُ الجدولِ رقم (١٤) اتجاهاتِ الشَّبابِ من عينةِ الدِّراسةِ نحوض الجرائمِ السَّيبرانيةِ، وخطورتِها، وآثارِها الاجتماعيةِ، وحجمِ انتشارِها في مجتمعِنا العربيِّ، وعددِ مرتكبيها، والتِّقنياتِ التي يَستخدِمُها مرتكبو تلك الجرائمِ، ويَتضحُ من بياناتِ الجدولِ أنَّ الاتِّجاهَ العامَّ لاتجاهاتِ الشَّبابِ من عينةِ الدراسةِ على جميعِ فقراتِ الاستبانةِ في هذا المحورِ بلغ (٩٨٪) ومتوسطٍ حسابيٍّ (١.٩٦) وهو ما يَعكِسُ حجمَ الاتجاهِ الإيجابيِّ بينَ عينةِ الدراسةِ فيما يَتعلَّقُ بإدراكِهم لحجمِ المخاطرِ، وتَزايُدِ حجمِ الجرائمِ السَّيبرانيةِ في مجتمعِنا العربيِّ المعاصرِ، وجاء في المرتبةِ الأولى، أنَّ الشَّبابَ هم الفئةُ الأولى المُستهدَفةُ من الجرائمِ السَّيبرانية بنسبةِ (١٠٠٪) ومتوسطٍ حسابيٍّ بلغ (٢.٠) وهو ما يعني بشكلٍ قاطعٍ الإيمانَ المُطلَقَ من عينةِ الدراسةِ بأنَّ الشَّبابَ هم المُستهدَفُونَ من قِبلِ مرتكبي تلك الجرائمِ، خاصَّةً أنَّهم الفئةُ الأكثرُ تواجداً عبرَ الفضاءِ الرَّقميِّ، واستخدامِهم اليوميِّ لمواقعِ التَّواصلِ الاجتماعيِّ، وهو ما يَجعلُهُم أكثرَ تَعرُّضاً للهجماتِ الإلكترونيةِ، أما المرتبةُ

الثَّانيةُ فتَحدَّدت في تَزايُدِ الجرائمِ السَّيبرانيةِ في الوقتِ الرَّاهنِ؛ بسببِ تكنولوجيا الاتصالاتِ، وانتشارِ فَيروس كورونا بنسبةِ (١٠٠٪) ومتوسطٍ حسابيٍّ بلغ (٢.٠) وهو ما يعني كذلك فهمَ الشَّبابِ من عينةِ الدِّراسةِ بأنَّ التُّكنولوجيا تَسبَّبت في نشرِ الجرائمِ السَّيبرانيةِ، وكذلك الحالُ سَاهَمَ كوفيد ١٩ في حاجةِ البشرِ للتَّفاعُلاتِ الرَّقميةِ، وهو ما سَاهمَ في نشرِ الجرائمِ السَّيبرانيةِ، ووقوعِ ضحايا جُدُدٍ. أوضحت نتائجُ دراسةِ (حيمد، ٢٠١٩) أنَّ العَولمةَ ــ ولاسيَّما الرَّقميةُ ــ سَاهمت في إتاحةِ بيئةٍ مناسبةٍ، وآلياتٍ رقميةٍ؛ للارتباطِ والتَّواصلِ بينَ الجماعاتِ الإرهابيةِ المتطرفةِ، وهو ما يُساعِدُهم في تحقيقِ أهدافِهم في التَّجنيدِ الإلكترونيِّ لعناصرَ شبابيةٍ جديدةٍ . أمَّا المرتبةُ الثَّالثةُ لاتجاهاتِ الشَّبابِ نحوَ الجرائمِ السَّيبرانيةِ فتَحدَّدَت في تزايدِ أعدادِ مرتكبي الجرائمِ السَّيبرانيةِ وضحاياهُ من مختلفِ فئاتِ المجتمعِ بنسبةِ (٩٩.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٩) وهو ما يَدُلُّ على وعيِ عينةش الدِّراسةِ بوقوعِ ضحايا كُثُرٍ؛ للهُجومِ السَّيبرانيِّ، والجرائمِ السَّيبرانيةِ، وأوضحت عينةُ الدراسةِ أنَّ تلك الجرائمَ يترتبُ عليها آثارٌ عِدَّةٌ على المجتمعِ، حيث جاءت في المرتبةِ الرَّابعةِ لاتجاهاتِ الشَّبابِ نحوَ الجرائمِ السيبرانيةِ تؤدي الجرائمُ السَّيبرانيةث إلى هدمِ قيمِ المجتمعِ، ونشرِ الفوضى بنسبةِ ٩٩٠٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٨) أما المرتبةُ الخامسةُ لاتجاهاتِ الشَّبابِ نحوَ الجرائمِ السَّيبرانيةِ، فتَحدَّدت في تَعرُّضِ الفردِ لتهديداتِ الجرائمِ السيبرانيةِ بشكلٍ يوميٍّ بنسبةِ (٩٨.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٧) وهو ما يَعكِسُ حجمَ الخطرِ من الجرائمِ السَّيبرانيةِ لدرجةٍ تصلُ إلى الهُجومِ السَّيبرانيِّ المتكررِ بشكلٍ يوميٍّ، حيث يرتبطُ بشكلٍ كبيرٍ باستخدامِ الإنترنتِ، وتطبيقاتِه بشكلٍ يوميٍّ ولَحظِيٍّ، حيث أصبح التَّفاعلُ السَّيبرانيُّ نمطًا للحياةِ . وكذلك أظهرت إحدى الدِّراساتِ الحديثةِ أنَّ جريمةً إلكترونيةً جديدةً تُرتَكَبُ كلَّ (١٠ ثواني) حتى أنَّ بعضَ الجرائمِ السَّيبرانيةِ تجاوزت مَثيلاتَها من الجرائمِ التَّقليديةِ في العالَمِ الماديِّ، ويُقدِّرُ الخبراءُ أنَّ حوالي (٩٠٪) من الجرائمِ السَّيبرانيةِ لا يتمُّ الإبلاغُ عنها. أما المرتبةُ السَّادسةُ لاتجاهاتِ الشَّبابِ نحوَ الجرائمِ السَّيبرانيةِ فتَحدَّدت، يُتيحُ الفضاءُ الإلكترونيُّ للشَّبابِ فرصَ التَّسللِ، والتفاعلِ عبرَ هذا الفضاءِ بنسبةِ (٩٨.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٧) حيثُ استثمارِ تِقنياتٍ، وتطبيقاتٍ تُكنولوجيةٍ في تحقيقِ أهدافِ مرتكبي تلك الجرائمِ، أما المرتبةُ

السَّابعةُ فتَحدَّدت في ارتباطِ انتشارِ الجرائمِ السَّيبرانيةِ بمجرمينَ محترفينَ يَمتلكُونَ قُدراتِ تِقنيةٍ فائقةٍ بنسبةِ (٩٨٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٦) وهو يَعكِسُ وعيَ الشَّبابِ من عينةِ الدِّراسةِ باقترانِ الجرائمِ السَّيبرانيةِ بسماتِ خِصالِ مرتكبي تلك الجرائمِ التي تَتطلَّبُ مهاراتِ تِقنيةٍ عاليةٍ. وجاءت في المرتبةِ الثَّامنةِ جهلُ الضَّحايا بتِقنياتِ الإنترنت سببُ انتشارِ الجرائمِ السَّيبرانيةِ بنسبةِ (٩٦٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٢) وهو ما يَتسبَّبُ في نشرِ الجرائمِ السَّيبرانيةِ، ووُقُوعِ الكثيرِ من الضَّحايا لاسيَّما في ظِلِّ عدمِ معرفةِ تفاصيلِ مجتمعِ المعلوماتِ، وتطبيقاتِه المختلفةِ. وأخيراً، جاءت في المرتبةِ التَّاسعةِ اعتمادُ أساليبِ مكافحةِ الجرائمِ السَّيبرانيةِ على الأُسرةِ، والرِّقابةِ الأُسريةِ بنسبةِ (٩٢.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٨٥) وهو ما يَعكِسُ أهميةَ الرِّقابةِ الأسريةِ في مكافحةِ الجرائمِ السَّيبرانيةِ، وغيرَ أنَّ هذه الفقرةَ جاءت في مرتبةٍ أقلَّ من الفقراتِ السَّابقةِ لاتجاهاتِ عينةِ الدِّراسةِ، فإنَّ هذا يعني أنَّ انتشارَ الجرائمِ السَّيبرانيةِ يَرتبِطُ بشكلٍ أكبرَ بسماتِ الشَّخصِ الذي يَتفاعَلُ عبرَ الفضاءِ الرَّقميِّ من جانبٍ، وسماتِ، وخصالِ مرتكبِ تلك الجريمةِ الذي يَترصَّدُ لحظاتِ التَّفاعُلِ المتكررِ عبرَ الشَّبكةِ، وكذلك تُشيرُ بعضُ الدِّراساتِ إلى أنَّه لا يمكنُ أنْ تَختفِيَ الجرائمُ بشكلٍ نهائيٍّ، ولكنْ يُمكنُ التَّقليلُ منها إلى أدنى حدٍّ من خلالِ تفعيلِ الأنظمةِ، والقوانينِ، والتَّشريعاتِ، وما إلى ذلك. وكذلك، ترى تلك الدِّراساتُ أنَّ الجرائمَ السَّيبرانيةَ لا يُمكنُ تجنُبُها، وينبغي معاقبتُها باللَّوائحِ، والقوانينِ، وما إلى ذلك، ومع ذلك، ففي العالَمِ الرَّقميِّ، لم تَنْضجْ بعدُ القوانينُ ذاتُ الصِّلةِ، ولا تُوجَدُ حتى الآنَ قوانينُ سليمةٌ لحمايةِ المستخدمين من الجرائمِ السَّيبرانيةِ؛ بسببِ التَّاريخِ القصيرِ نسبيًّا لتكنولوجيا المعلوماتِ، وفَهمِ النَّاسِ المحدودِ لمثلِ هذه الجرائمِ، ولذلك، من الصُّعوبةِ بمكانٍ اكتشافُ مرتكبي الجرائمِ السَّيبرانيةِ بسهولةٍ، والقبضُ عليهم، ومعاقبتُهم. ففي العالَمِ الرَّقميِّ، يتمُّ إلحاقُ الأضرارِ دائمًا عن بعدٍ، ولا يُمكنُ ملاحظتُها إلاَّ بعدَ وقتٍ طويلٍ، ويختلفُ هذا النَّوعُ من الضَّررِ اختلافًا كبيرًا عن الأضرارِ الواضحةِ داخلَ المجتمعِ المَعيشِ، مثل: الإصاباتِ الشَّخصيةِ، أو فقدانِ الممتلكاتِ؛ فالهجماتُ في العالَمِ الرَّقميِّ لا يُمكنُ اكتشافُها بسهولةٍ، على سبيلِ المثالِ، العديدُ من المستخدمينَ، أو المسؤولينَ لا يُدرِكُونَ أنَّ أجهزةَ الكمبيوتر، والشَّبكاتِ الخاصَّةَ بهم قد تَعرضَت للاختراقِ، أو الهُجُومِ.

وعلى المدى الطَّويلِ، فإنَّ أفضلَ الاستراتيجياتِ لمواجهةِ الجرائمِ السَّيبرانيةِ هي تثقيفُ أفرادِ المجتمعِ بخُطورةِ تلك الجرائمِ، ومن ثَم، منعُهم من الوُقوعِ فريسةً، وضحايا الاحتيالِ، والخداعِ(Sarre, Chung, 2018;518) وأشارت بعضُ الدِّراساتِ إلى أنَّ الوُقوعَ ضحيةٌ لجرائمَ سيبرانيةٍ يرتبطُ بشكلٍ أساسيٍّ بمدى الإلمامِ بتقنياتٍ، ومهاراتٍ، وفنياتِ استخدامِ الشَّبكةِ العنكبوتيةِ، وتطبيقاتِها المُتعدِّدَةِ، هذا فضلاً عن اتِّخاذِ الحيطةِ، والحذرِ عبرَ التَّفاعلِ الشَّبكيِّ(شريف، ٢٠١٢: ٥٤) واتخاذِ الاجراءاتِ الوِقائيةِ من الافرادِ، والجهاتِ المَعنيةِ .

الحادي عشرــ نتائجُ الدِّراسةِ :

١. إنَّ (٣٥٪) من أفرادِ العينةِ متوسطُ أعمارِهم ما بين (٢٠-١٨) سنة، أما الشَّريحةُ العُمرية الثَّانيةُ فبلغت (٣٣٪) متوسطُ أعمارِها ما بين (٢٢-٢٠) سنة، ثُم الشَّريحةُ العُمرية الأكبرُ عمرًا، والتي بلغت (٣٢٪) وتراوحت أعمارُهم ما بين (٢٤-٢٢) سنة.

٢. إنَّ (٣٢.٦٪) من أفرادِ العينةِ في المستوى الخامسِ والسَّادسِ، يليهم (٣٢.٤٪) من أفرادِ العينةِ في المستوى السَّابعِ والثَّامنِ.

٣. إنَّ (٤٤٪) من أفرادِ العينةِ تقديراتُهُم الجامعيةُ(B) و(٢٥.٣٪) تقديراتُهم الجامعيةُ (+B)، ثُم (١٣.٤٪) كانت تقديراتُهُم(A).

٤. إنَّ (٥٨٪) من أُسرِ عينةِ الدِّراسةِ تتراوحُ دُخولُهم ما بين (٤٠٠٠ إلى ٧٠٠٠) ريال سعودي، و(١٨.٣٪) من أُسرِ عينةِ الدِّراسة متوسطُ دُخولِهم الشَّهريةِ تتراوحُ ما بين (٧٠٠٠ إلى ١٠٠٠٠) ريال سعودي، يليها (١٧.٧٪) من أُسرِ عينةِ الدِّراسة دُخُولُهم الشَّهريةُ أكثرُ من (١٠٠٠) ريال سعودي.

٥. إنَّ (٥٤.٦٪) من أفرادِ العينةِ متوسطُ استخدامِهم للإنترنتِ يوميًّا يتراوحُ ما بين (٣-٦) ساعاتٍ يوميًّا، و(٢٢.٧) يستخدمون الإنترنتَ لعددِ ساعاتٍ تتراوحُ ما بين (٦-٩) ساعات، و(٨٪) يستخدمون الإنترنتَ لأكثر من (٩) ساعاتٍ يوميًّا.

٦. إنَّ هناك تفاوتاً في استخدامات الإنترنت بين الشَّباب من عينة الدراسة، غيرَ أنَّ النِّسبةَ الأكبرَ من استخدامِ الإنترنتِ بين الشَّبابِ نسبةُ (٣٦.٤٪) اتجهت نحوَ التَّواصلِ الاجتماعيَّ، وتكوينِ الصَّداقاتِ عبرَ مواقعِ التواصلِ الاجتماعيِّ المختلفة.

٧. إنَّ (٦٣٪) من أفرادِ العينةِ من الشَّبابِ تَعرَّضُوا للتَّهديداتِ، والجرائمِ السَّيبرانية.

٨. إنَّ أكثرَ من نصفِ عينةِ الدراسةِ (٥١.٩٪) من أفرادِ العينةِ من الشَّباب تعرضُوا لسَرقةِ بياناتِ الهاتفِ من صُورٍ، وفيديوهاتٍ، كما تَعرَّضَ (٢٠.٦٪) من أفرادِ عينةِ الدِّراسةِ من الشَّبابِ لجرائمِ التَّهكيرِ، واختراقِ الحساباتِ الشَّخصيةِ، ولاسيَّما البريدُ الإلكترونيُّ، وحساباتُ مواقعِ التَّواصلِ الاجتماعيِّ، كما واجه (١٣.٧٪) من أفرادِ العينةِ فَيروساتٍ خبيثةً أضرت بأجهزتِهم الشَّخصيةِ، وهواتفهم الذَّكيةِ، مما يؤدي إلى سُهولةِ الاختراقِ، ونقلِ بياناتٍ، والاطِّلاعِ عليها.

٩. إنَّ المفهومَ الأكثرَ شُيوعاً، وقَبولاً بين عينةِ الدِّراسة للجرائمِ السَّيبرانيةِ هو مطارداتٌ، ومُضايَقاتٌ إلكترونيةٌ يترتبُ عليها خسائرُ للفردِ بنسبة (٩٨.٥٪) وبمتوسطٍ حسابيٍّ (١.٩٧).

١٠. تَتَنوَّعُ دوافعُ ارتكابِ الجريمةِ السَّيبرانيةِ ما بين دوافعَ ذهنيةٍ لإثباتِ الذَّات، ودوافعَ للتَّسليةِ، وثالثةٍ خاصَّةً بالانتقامِ، ورابعةٍ دوافعَ ماديةٍ، وأوضحت نتائجُ الدراسةِ أنَّ إثباتَ الذَّاتِ، وتطويعَ تِقنيةِ الاتصالاتِ لرغباتِ مرتكبيها، والتي بلغت نسبة (٩٨.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٧٪) كانت في المرتبةِ الأولى بالتَّوازي مع تحقيقِ أهدافٍ ماديةٍ باستغلالِ مهاراتِ التَّعاملِ مع النتِّ، والبحثِ عن الثَّراءِ بنسبةِ (٩٨.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٧) الدوافع الأكبر في ارتكابِ الجرائمِ السَّيبرانية.

١١. إنَّ تشويهَ السُّمعةِ، والإضرارِ بها، والابتزازِ لأفرادِ المجتمعِ أبرزُ المخاطرِ التي يُواجِهُها الفردُ في المجتمعِ الرَّقميِّ، حيثُ جاءت في المرتبةِ الأولى بنسبةِ (٩٦٪) ومتوسطٍ حسابيٍّ (١.٩٢) وهو ما يَعكسُ حجمَ الخطرِ الذي يُحيطُ بأفرادِ المجتمعِ نتيجةَ انتشارِ الجرائمِ السَّيبرانيةِ، وتَزايُدِ معدلاتِها، ومن ثَم، كان أكبرُ خطرٍ من وجهةِ

نظرِ العينةِ تشويهَ السُّمعةِ، والابتزازَ، وما يتبعُهُ من آثارٍ اجتماعيةٍ عديدةٍ، والنَّاجمِ عن اختراقاتٍ، وسَرقةِ بياناتٍ، وتفاعلاتٍ دونَ وعيٍ عن الفضاءِ الرَّقميِّ.

١٢. أمَّا الخطرُ الثَّاني للجرائمِ السَّيبرانيةِ، فكان وُقوعَ ضحايا من فئاتٍ مختلفةٍ في المجتمعِ؛ بفعلِ الابتزازِ بنسبةِ (٨٧٪) ومتوسطٍ حسابيٍّ بلغ (١٠٧٤) .

١٣. أوضحت نتائجُ الدِّراسةِ أنَّ الوسائلَ الأكثرَ تأثيرًا في نشرِ الجريمةِ السَّيبرانيةِ من وجهةِ نظرِ عينةِ الدِّراسةِ كانَ الاستخدامُ المستمرُ لمواقعِ التَّواصلِ الاجتماعيِّ بنسبةِ (٩٩.٥٪) ومتوسطٍ حسابيٍّ بلغ (١.٩٧).

١٤. أوضحت نتائجُ الدِّراسةِ أنَّ الشَّبابَ هم الفئةُ الأولى المُستهدَفةُ من الجرائمِ السَّيبرانيةِ بنسبةِ (١٠٠٪) ومتوسطٍ حسابيٍّ بلغ (٢.٠).

١٥. كما أوضحت نتائجُ الدِّراسةِ تَزايُدَ الجرائمِ السَّيبرانيةِ في الوقتِ الرَّاهنِ؛ بسببِ تُكنولوجيا الاتصالاتِ، وانتشارِ فَيروس كورونا بنسبةِ (١٠٠٪) ومتوسطٍ حسابيٍّ بلغ (٢.٠).

المراجعُ والهوامشُ:

١. إبراهيم، رانيا حاكم كامل محمد (٢٠١٥) جرائم الإنترنت في المجتمع المصري: دراسة ميدانية بمدينة القاهرة، مجلة البحث العلمي في الآداب، المجلد ١، العدد ١٦، ٢٩١-٣٢٦.

٢. ابن داود، عبد العزيز بن فهد بن محمد (٢٠٢٠) الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، مجلد ٩، العدد ٣، ١٤٤-١٦٦.

٣. ابن شفلوت، جعفر (٢٠١٨) دور الجامعات السعودية في مكافحة الجرائم الإلكترونية من وجهة نظر طلبة الجامعات: دراسة حالة جامعة نايف العربية للعلوم الأمنية، مجلة كلية الآداب، العدد ١٢، يوليو، ٩٥٥-٩٩٥.

٤. أبو زيد، عبد الرحمن عاطف (٢٠١٩) الأمن السيبراني الوطن العربي: دراسة حالة المملكة العربية السعودية، آفاق سياسية، العدد ٤٨، أكتوبر، ٥٥-٦١.

٥. التايب، عائشة (٢٠٠٨) الثورة الرقمية المضادة: مقاربة سوسيولوجية لجرائم الفضاء الإلكتروني، المجلة العربية لعلم الاجتماع – إضافات، العدد الأول، ١٤٢-١٧٢.

٦. أحمد، علي محمود إبراهيم (٢٠٢٠) الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية: دراسة فقهية مقارنة، مجلة كلية الشريعة والقانون بأسيوط، المجلد ٤، العدد ٣٢، ١٠٧٠-١٢١٢.
٧. البشري، هنيدي بن عطية بن عبد المعطي (٢٠٢٠) الجرائم الإلكترونية وكيفية التعامل معها من وجهة نظر الشباب الجامعي، مجلة كلية الآداب، العدد ٣٨، ٦٣٣-٦٦٤.
٨. الجراحي، منى (٢٠١٥) دور الجامعات السعودية في تنمية وعي الشباب بخطورة الجرائم المعلوماتية لدعم قضايا مكافحة الإرهاب، مؤتمر الإرهاب الإلكتروني، جامعة الإمام محمد بن سعود، الرياض.
٩. الجفناوي، خالد مخلف (٢٠١٦) الجرائم الإلكترونية وطرق معالجتها من وجهة نظر أعضاء هيئة التدريس في أكاديمية سعد العبد الله للعلوم الأمنية، مجلة الخدمة الاجتماعية، مجلد ٢، العدد ٥٦، ٣٧١-٣٩٩.
١٠. الحذيفي، أمين أحمد (٢٠١٣) جرائم الكمبيوتر والإنترنت، مجلة العدل، السنة ١٥، العدد ٤٠، ديسمبر، ١١٥-١٧٤.
١١. الخنين، حمد بن عبد الله (٢٠٠٨) الجرائم المعلوماتية وقضايا المستجدة، مجلد ١٠، العدد ٣٨، ٢٧٦-٢٩٦.
١٢. الراظمي، سيدي محمد الأمين (٢٠١٩) الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي والدولي، مجلة القانون والأعمال، العدد ٤٧، ٢٤-٣٤.
١٣. الردفاني، محمد قاسم أسعد (٢٠١٤) تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية، مجلد ٣٠، العدد ٦١، ديسمبر، ١٥٧-١٩٢.
١٤. الرفادي، بسمة يونس محمد (٢٠١٨) الحروب السيبرانية وأثرها في التنظيم الدولي، مجلة العلوم والدراسات الإنسانية، العدد ٤٩، فبراير، ١-١٤.
١٥. الروسي، محمد الحافظ (٢٠٢٠) الشباب والتطرف: مداخل تمنيعية، مجلة إيقاظ، العدد الأول، إبريل، ٥٢-٥٥.

١٦. السيد، نهي محمد أحمد (٢٠١٩) سوسيولوجيا المخاطر التي يتعرض لها الشباب في ظل العولمة: رؤية أولريش بيك، مجلة كلية الآداب والعلوم الإنسانية، العدد ٣١، ديسمبر، ١١-٦٠.

١٧. الشهراني، معلوي بن عبد الله حسين (٢٠١٩) تصور مقترح لوقاية الشباب الجامعي من مخاطر جرائم الإرهاب السيبراني، مجلد ٦، العدد الثاني، ٤٨٣-٥٢٧.

١٨. الصاعدي، محمد (٢٠١٠) جرائم الإنترنت وجهود المملكة العربية السعودية في مكافحتها، أعمال ندوة مكافحة الجريمة عبر الإنترنت، المنظمة العربية للتنمية الإدارية، القاهرة.

١٩. الصبان، عبير محمد (٢٠١٩) إدمان الطلاب على استخدام مواقع التواصل الاجتماعي وعلاقته بالأمن النفسي والتورط في الجرائم السيبرانية، المجلة الدولية للدراسات التربوية والنفسية، مجلد ٩، العدد الثاني، أكتوبر، ٢٦٧-٢٩٣.

٢٠. الطحاوي، ملك محمد (٢٠٠٨) الجرائم المعلوماتية: أسبابها ومستقبلها: تحليل سوسيولوجي، المجلة العلمية لكلية الآداب، العدد ٢٨، أكتوبر، ٢٦٣-٤١١.

٢١. الفالح، سليمان بن قاسم (٢٠٠٨) جرائم الاحتيال في المجتمع السعودي: العوامل والأخطار والتوقعات المستقبلية، المجلة العربية للدراسات الأمنية، مجلد ٢٣، العدد ٤٥، ١٣٧-١٧٨.

٢٢. الفرجاني، صلاح الدين محمد علي (٢٠١٧) الجرائم الإلكترونية باستخدام شبكة الإنترنت والبريد الإلكتروني، المال والاقتصاد، العدد ٨١، فبراير، ٣٦-٣٩.

٢٣. الألفي، محمد محمد (٢٠١٠) الجريمة والمجرم عبر الإنترنت، أعمال ندوة مكافحة الجريمة عبر الإنترنت، المنظمة العربية للتنمية الإدارية، القاهرة.

٢٤. المعايطة، حمزة عبد المطلب كريم (٢٠١٥) نوعية وحماية الشباب من ظاهرة الانحراف الفكري المتطرف عبر مواقع التواصل الاجتماعي، عالم التربية، السنة ١٦، العدد ٥٢، أكتوبر، ١-٣٥.

٢٥. المقصودي، محمد بن أحمد بن علي (٢٠١٧) الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات، الأمن والحياة، مجلد ٣٧، العدد ٤٢٧، ١٠٢-١٠٧.

٢٦. ايديو، ليلى (٢٠٢٠) دور مؤسسات التنشئة في الوقاية من مخاطر الجريمة الواقعة على الأشخاص عبر شبكات المعلومات "الإنترنت"، مجلة الباحث في العلوم الإنسانية والاجتماعية، مجلد ١٢، العدد الثالث، ٣٤١-٣٥٦.
٢٧. بشريف، وهيبة (٢٠١٨) أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي، المجلد ٨، العدد ١، ديسمبر، ٦٢-٧٣.
٢٨. بلحميتي، آمال (٢٠١٧) جرائم المجال السيبراني في الجزائر بين الواقع والقراءة القانونية، مجلة الرواق، العدد ٧، ٥-٢١.
٢٩. حيمد، محمد مسعد (٢٠١٩) رؤية استراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة، المجلة العربية الدولية للمعلوماتية، المجلد ٧، العدد ١٢، ٨٣-١٠٠.
٣٠. خميس، هاني (٢٠١١) رؤى الشباب نحو الجرائم المعلوماتية في المجتمع المصري: دراسة سوسيولوجية على عينة من طلاب جامعة الإسكندرية، مجلد ٥٤، العدد ٢، يوليو، ٨٥-١٣٢.
٣١. دبابنة، شيرين (٢٠١٥) الجرائم الإلكترونية: القرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، مجلد ٢٣، العدد الأول، ١٩-٢٢.
٣٢. دريس، نبيل (٢٠١٧) الجريمة السيبرانية بين المفاهيم والنصوص التشريعية: الجزائر أنموذجاً، العدد ١٠، ديسمبر، ٢٠-٤٠.
٣٣. رجب، سها عيد (٢٠١٨) اتجاهات الشباب الجامعي نحو ثقافة الثراء السريع: دراسة ميدانية على عينة من طلاب جامعة القاهرة، مجلة الخدمة الاجتماعية، مجلد ٥، العدد ٥٩، يناير، ٢٠٦-٢٥٧.
٣٤. زيتون، أيمن أحمد (٢٠١٨) التحرش عبر الإنترنت: الإشكاليات والمواجهة، مجلة القراءة والمعرفة، العدد ٢٠٦، ديسمبر، ٢٠١-٢٢٠.
٣٥. سعيد، أميمة دسوقي محمد (٢٠١٩) الوعي المجتمعي بالجرائم المعلوماتية لدى الطالبة الجامعية: دراسة من منظور تنظيم المجتمع في الخدمة الاجتماعية، مجلد ٣، العدد ٦١، ٣٣٥-٣٧٥.

٣٦. سياب، حكيم (٢٠٠٩) السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات وأبحاث، العدد الأول، ٢١٢-٢٤٠.
٣٧. شريف، إيمان (٢٠١٢) الخصال النفسية المميزة لضحايا جرائم الكمبيوتر والإنترنت، المجلة الجنائية القومية، مجلد ٥٥، العدد ٢، يوليو، ١-٥٨.
٣٨. غزال، إيناس محمد فتحي (٢٠١١) جرائم الإنترنت في المجتمع المصري: دراسة ميدانية على عينة من الشباب الجامعي في مدينة الإسكندرية، مجلة شؤون اجتماعية، مجلد ٢٨، العدد ١١٠، ٩-٤٦.
٣٩. فوزي، إسلام (٢٠١٩) الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي، المجلة الاجتماعية القومية، مجلد ٥٦، العدد الثاني، ٩٩-١٣٩.
٤٠. قيسي، نوال بنت علي بن محمد (٢٠١٠) الجرائم الإلكترونية الموجهة ضد مستخدمي الإنترنت: دراسة مسحية لبعض مستخدمي الإنترنت بالمملكة العربية السعودية، رسالة ماجستير، جامعة الإمام محمد بن سعود الإسلامية.
٤١. كزبر، صباح (٢٠١٨) الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي: دراسة تحليلية، مجلة التراث، العدد ٢٨، ٢٩٣ -٣١٠.
٤٢. محمد، عادل عبد الجواد (٢٠٠١) إجرام الإنترنت، مجلد ٢٠، العدد ٢٢١، ٧٠-٧٣.
٤٣. محمود، رعد سعدون (٢٠١٥) الجرائم الإلكترونية، مجلة الدراسات المالية والمصرفية، مجلد ٢٣، العدد الثالث، ٣٥-٤٠.
٤٤. نظمي، كرستينا لطيف (٢٠١٩) أنماط الجرائم الإلكترونية المرتكبة ضد الإناث: دراسة تحليلية، مجلة الاستواء، العدد ١٤، ١٤١-٢٠٧.
45. Aiken, Mary & Davidson, Julia. (2016) Youth Pathways into Cybercrime, Paladin Capital Group, Middlesex Unversity.
46. AliI, Md. Ramjan & Shahariar, Rezvi. (2014) Nature of the Cyber Crime Activities among the Secondary Student in Dhaka City of Bangladesh: A Baseline Study, European Acaemic Research, Vol. II, Issue 8, November, pp. 10216- 10232.
47. Aransiola ,Joshua Oyeniyi & Asindemade, Suraj Olalekan. (2010) Understanding Cybercrime Perpetrators and the Strategies They Employ in

Nigeria, Cyberpsychology, Behavior, and Social NetworkingVol. 14, No. 12, pp.1-20.
48. Amberg, Magorzata Skórzewska (2017) Global Threats But National Legislations— How to Adapt to the New Cyberspace Society, In; Cybercrime, Organized Crime, and Societal Responses International Approaches, Editor Emilio C. Viano, © Springer International Publishing Switzerland.
49. Bajovic, Vanja. (2017) Criminal Proceedings in Cyberspace: The Challenge of Digital Era ,In; Cybercrime, Organized Crime, and Societal Responses International Approaches, Editor Emilio C. Viano, © Springer International Publishing Switzerland.
50. Boateng, Richard & Olumide, Longe. (2011) Sakawa - Cybercrime and Criminality in Ghana, Journal of Information Technology Impact, Vol. 11, No. 2, pp. 85-100.
51. Bossler, Adam M & Berenblum, Tamar (2019) Introduction: new directions in cybercrime research, Journal of Crime and Justice, Volume 42, Issue 5, pp. 495- 499.
52. Choi, Kyung-shick and Lee, Claire Seungeun (2018) The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity, International Journal of Cybersecurity Intelligence & Cybercrime,Volume.1, Issue(1) pp, 1-4.
53. Choi, Kyung-shick. (2008) Computer Crime Victimization and Integrated Theory: An Empirical Assessment, An Empirical Assessment of an Integrated Theory of Computer Crime Victimization, Vol 2, (1),PP. 308–333.
54. Curtain, Richard. (2001) Youth and Employment: a Public Policy Perspective, Development Bulletin, No 55, August, pp7-11.
55. Dupont, Benoît. (2019) The ecology of cybercrime, In; The Human Factor of Cybercrime, 1st Edition, Routledge, London.
56. Edwards, Susan S.M.(2017) Cyber-Grooming Young Women for Terrorist Activity: Dominant and Subjugated Explanatory Narratives, In; Cybercrime, Organized Crime, and Societal Responses International Approaches, Editor Emilio C. Viano, © Springer International Publishing Switzerland.
57. Gandhi, V.Karamchand. (2012) An Overview Study on Cyber crimes in Internet, Journal of Information Engineering and Applications, Vol 2, No.1, pp.1-5.
58. Graham, Roderick S. & Smith, ‘Shawn K. (2019) Cybercrime and Digital Deviance, 1st Edition, Routledge, New York.

59. Goldsmith, Andrew & Wall, David S. (2019) The seductions of cybercrime: Adolescence and the thrills of digital transgression, European Journal of Criminology, December ,9, pp.1-20.
60. Hutchins, Lice & Yiting chua. (2016) Gendering cybercrime,im; Cybercrime Through an Interdisciplinary Lens 1st Edition, Routledge, London.
61. Jaishankar, K. (2007) Establishing a Theory of Cyber Crimes, International Journal of Cyber Criminology, Vol. 1, Issue 2, July,pp.7-9.
62. Kamruzzaman & Islam, Ashraful et al (2016) Plight of Youth Perception on Cyber Crime in South Asia, American Journal of Information Science and Computer Engineering, Vol. 2, No. 4, pp. 22-28.
63. Kashif, Muhammad & UrRehman, Aziz. (2020) A Surge in Cyber-Crime during COVID-19, Idonesian Journal of Social and Environmental Issues (IJSEI), Volume 1, Issue 2, August,pp.48-52.
64. Kigerl, Alex. (2012) Routine Activity Theory and the Determinants of High Cybercrime Countries, Social Science Computer Review, 30,(4),PP. 470-486
65. Leukfeldt, Eric Rutger & Yar, Majid. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, Deviant Behavior, Volume 37, Issue 3, pp.263-280.
66. Ilievski, Aleksandar & Bernik, Igor. (2016) Social-Economic Aspects of Cybercrime, Innovative Issues and Approaches in Social Sciences, Vol. 9, No. 3, pp.8-22.
67. Lusthaus ,Jonathan. (2012) Trust in the world of cybercrime, Global Crime, Volume 13, 2012 - Issue 2, pp.71-94.
68. Malar, M. Neela. (2012) Impact of Cyber Crimes on Social Networking Pattern of Girls, International Journal of Internet of Things, 1(1),pp. 9-15.
69. Meena, Yogesh & Sankhla, Mahipal Singh and Mohril, Shriyash. (2020) Cybercrime: youth awareness survey in Delhi NCR, India, Forensic Research & Criminology International Journal, Volume 8 Issue 5, pp. 177-180.
70. Nasi, Matti & Oksanen, Atte. (2015) Cybercrime victimization among young people: a multi-nation study, Journal of Scandinavian Studies in Criminology and Crime Prevention, Volume 16, Issue 2,pp. 203-210.
71. Olayemi, Odumesi John. (2014) A socio-technological analysis of cybercrime and cyber security in Nigeria, Academic Journal, Vol.6(3), March, pp. 116-125.

72. Pasculli, Lorenzo. (2020) The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory, Journal of Ethics and Legal Technologies, Volume 2,(1), April,pp.48-74.
73. Sarre ,Rick & Chung Lau, Laurie Yiu, Chang & Lennon Y.C. (2018), An International Journal, Volume 19, Issue 6,pp. 515-518.
74. Saini, Hemraj, Rao, Yerra Shankar. (2012) Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research, Vol. 2, Issue 2,Mar-Apr, pp.202-209.
75. Solak,Duygu & Topaloglu, Murat. (2015) The Perception Analysis of Cyber Crimes In View of Computer Science Students, Procedia - Social and Behavioral Sciences, Volume 182, May,pp. 590-595.
76. Susheel, Bhatt & Durgesh Chandra. (2011) Cyber Crime in India, International Journal of Advanced Research in Computer Science,Sep, Vol. 2, Issue 5, pp.153-156.
77. Tcherni, M., A. & Davies, G. Lopes, and A. Lizotte. (2016) "The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?" Justice Quarterly 33,pp.890–911.
78. Viano, Emilio C.(2017) Cybercrime: Definition, Typology, and Criminalization, In; Cybercrime, Organized Crime, and Societal Responses International Approaches, Editor Emilio C. Viano, © Springer International Publishing Switzerland.
79. Volodymyr, Kryvolapchuk & Olexandr Kulyk. (2020) Attitude of Young People to the Criminality Problem in Ukrainian Postmodern Society, Postmodern Openings / Deschideri Postmoderne,Supplement, Vol. 11, pp.93-115.
80. Yu, Szde. (2014) Fear of Cyber Crime among College Students in the United States: An Exploratory Study, International Journal of Cyber Criminology (IJCC), Vol 8, (1), June,pp. 36–46.
81. Yar, Majid. (2012) Sociological and Criminological Theories in the Information Era, W. Stol & R. Leukfeldt (eds) Cyber-Safety: An Introduction, Utrecht: Eleven International Publishing.

Abstarct;

Awareness of cybercrime among Young Saudis is important, especially as internet use has become a lifestyle today. Awareness of cybercrime must therefore be part of the necessity of the lives of contemporary societies. The study tried to understand the extent to which Saudi youth are aware of the seriousness of cybercrime and cyber-interactions. The study based its analyses on a non-probability sample of 300 single groups collected from university youth in the 18-24 age group now studying at university, male at Shaqra University. The study concluded that from the point of view of the sample of the study, one of the dangers of cybercrime is defamation and harm, and the exposure of members of the community to extortion, which came in first place with a median account of 1.92, which reflects the magnitude of the risk surrounding members of society as a result of the spread and increasing rates of cybercrime, and the results of the study showed that the most influential means of spreading cybercrime from the point of view of the sample study was the continuous use of social networking sites by 99.5% and the average account reached 1.97, young people are the first target group of cybercrime with 100% and an average account of 2.0.

82. **Keywords**: Cybercrime - abuse cybercrime – Electronic Crime - computer crimes