# علم الجريمة الرقمي ومداخله السوسيولوجية الحديثة المفسرة للجريمة في مجتمع الرقمنة

## نموذج نظرى

**Digital criminology and its modern sociological approaches that explain crime in the digitization society**

**Theoretical model**

**د/ خالد السيد شحاتة**

**مدرس علم الاجتماع – كلية الآداب – جامعة دمنهور**

khaled.shehata@art.dmu.edu.eg

## مقدمة

أدى التطور الهائل في مجال تقنيات الحاسب الآلي، والاقبال المتزايد على استخدام التكنولوجيا وشبكة الانترنت، إلى إحداث تغيير متسارع في وتيرة الحياة داخل المجتمعات. حيث يشهد مجتمعنا المعاصر تحولات عديدة، وتوصيفات عدة لملامح المجتمع الذي نعيشه، بأنه مجتمع الإشباع الرقمي عبر الوسائط التكنولوجية المتنوعة، والتطبيقات الإلكترونية، وعصر الميديا الرقمية، حيث الصورة، والصوت، والفيديو المتداول عبر شبكات التواصل الاجتماعي، والأقمار الصناعية. ومن هنا لم تجد الدول مفراً أمام هذه الثورة التكنولوجية، إلا الاتجاه نحو تعميم استخدام التكنولوجيا الحديثة في شتى مجالات الحياة؛ من أجل تحسين جودة الحياة، وتقديم الخدمات للمواطنين بشكل سهل وسريع، مما مهد بالفعل الاتجاه نحو الرقمنة، حيث أصبح العالم الرقمي جزءاً بارزًا من حياتنا اليومية، وتغلغل داخل العديد من المجالات كالتعليم، والاقتصاد، والأمن، والخدمات، والتواصل بين البشر .

وتزامن تبني الدول المختلفة لسياسات التنمية المستدامة، مع دخولها إلى عصر الرقمنة والتحول الرقمي، باعتماد إستراتيجيات وطنية للرقمنة، بهدف تحسين أداء المؤسسات، وكسب ثقة المواطنين في الخدمات المقدمة بوسائل الكترونية، وهو ما يُمكن من تعزيز قيم الشفافية والمحاسبة والمراقبة لكافة الأعمال، من خلال التفاعل مع كافة عناصر المجتمع الرقمي. وبدأت مصر بالفعل في تفعيل فكرة التحول الرقمي بداية من عام 2016 في إطار رؤية مصر 2030 ، والتي تعتمد في أغلب جوانبها على تنمية البنية التحتية التكنولوجية، واعتماد تكنولوجيا الاتصالات والمعلومات كوسيلة لإنجاز المهام الحكومية وغير الحكومية. وعلى الرغم من أن التحول الرقمي جلب فوائد ضخمة للعالم بأسره، إلا أنه صنع أيضًا أخطار هائلة، متمثلة في الجريمة الرقمية، والتي تعد واحدة من أسرع الأنشطة الإجرامية نموًا، حيث يقع أكثر من مليون شخص ضحايا لها في جميع أنحاء

العالم كل يوم، كما أنها تشكل قلقًا خاصًا وتهديدا للأمن الاجتماعي والاقتصادي للأفراد والمؤسسات والدول، لما تسببه من خسائر سنوية تقدر بالمليارات.

وبالرغم من هذا التقدم الرقمي الذى أصاب الجريمة، إلا أن النظريات العلمية المفسرة للجريمة لم تتطور بنفس الوتيرة التي تتيح لها تفسير انعكاس التكنولوجيا على السلوك الإجرامي، وارتكاب الجرائم الرقمية. وبالتالي ستصبح محدودة التأثير في التفسير، طالما لم يكن هناك اهتمام بتأثير الاستخدام السائد للتكنولوجيا. ومن هنا تأتى هذه الدراسة لمعالجة تلك الظاهرة، حيث جاء في محورها الأول تعريف الرقمنة، ونشأة المجتمع الرقمي، ومفهومه، ومقوماته، وواقعه الذي فُرض على حياتنا اليومية، ودور علم الاجتماع في دراسة ظاهرة الرقمنة، وبداية ظهور علم الاجتماع الرقمي وأهم مجالاته. ثم جاء في المحور الثاني للدراسة استعراض الجرائم الرقمية من حيث تطور الاهتمام بها وتعريفها، وبداية ظهور علم الجريمة الرقمي ومجالاته، وتناوله للجرائم في مجتمع الرقمنة. ثم يأتى المحور الثالث بعنوان النظريات المفسرة للجريمة في المجتمع الرقمي، وفيه يتم تناول الارهاصات الأولى للنظريات الاجرامية، ومن ثم عرض مجموعة من النظريات السوسيولوجية وما انبثق منها من مداخل، والتى تم اختبارهم امبريقيا فى تفسير الجرائم الرقمية، فى محاولة للخروج بنموذج نظري يشمل مجموعة من القضايا والفروض التى تصلح لتفسير تلك الأنواع من الجرائم. وأخيراً عرض لمجموعة التوصيات التى قد تساعد الباحثين فى فتح مجالات جديدة للبحث العلمى، وكذلك صناع القرار لمواجهة ومكافحة الجرائم الرقمية .

## أولا :الكلمات المفتاحية Key words

المجتمع الرقمى Digital Society – الرقمنة Digitization – علم الاجتماع الرقمى Digital sociology – علم الجريمة الرقمى Digital Criminology – الجريمة الرقمية Digital crime . وسوف يتم القاء الضوء على كل تعريف داخل إطار البحث .

## ثانيا : الدراسات السابقة

فرضت طبيعة الدراسة أهمية مسح التراث، بالتركيز على مجموعة من الدراسات السابقة، والتى أختبرت فروض النظريات الكلاسيكية والمعاصرة المفسرة للجريمة التقليدية، وتم تطبيقها على الجرائم الرقمية، فى محاولة لاستخلاص القضايا النظرية التى تسمح للباحث بوضعها فى نموذج نظرى مفسر للجرائم فى مجتمع الرقمنة، ومن أهم هذه الدراسات: دراسة "Sheena Lewis" بعنوان" رقمنة نظريات منع الجريمة: كيف تؤثر التكنولوجيا على الضحية وسلوك الجاني" والتى أجرتها عام ٢٠١١ . ودراسة أخرى بعنوان" التحول الرقمي للنظرية الاجتماعية: تحديث بحثي" للعالم " Wyatt Brown " والتى أجراها عام 2015. كذلك دراسة كل من "Powell and Stratton" فى عام ٢٠١٧ بعنوان " الجريمة والعدالة في المجتمع الرقمي: نحو "علم الجريمة الرقمي". ودراسة "Brian K. Payne " فى عام ٢٠١٨ بعنوان " استخدام نظرية التسمية كدليل لفحص الأنماط والخصائص والعقوبات المفروضة على جرائم الإنترنت. كذلك دراسة " Thomas E Dearden" فى عام ٢٠٢١ وعنوانها " نظرية الاغتراب المؤسسي والجرائم الالكترونية ." ودراسة أخرى بعنوان " التقييم التجريبي لنمط الحياة –

ونظريتي النشاط الروتيني والتعلم الاجتماعي على جرائم الإنترنت "والتى قام بها" Elizabeth Phillips " عام2021 . وأخيرا دراسة أجريت عام ٢٠٢٢ بعنوان " نحو الجريمة المنظمة الرقمية وعلم الاجتماع الرقمي للجريمة المنظمة " للعالم Andrea " Di Nicola. وسوف يتم تناول تلك الدراسات بالتحليل داخل محاور الدراسة.

## ثالثا: أهداف الدراسة وأهميتها

يتحدد الهدف الرئيسي للدراسة فى محاولة رقمنة نظريات الجريمة، ونعني بذلك إبراز تأثير استخدام التكنولوجيا على كل من الجريمة، والمجرمين، والضحايا. وإلقاء الضوء على أهمية إدماج عنصر التكنولوجيا فى نظريات الجريمة، لاستخدامها في توقع السلوك الإجرامي، وتفسيره، ومكافحته فى المجتمع الرقمى. وينبثق من هذا الهدف الرئيسي مجموعة من الأهداف الفرعية تتمثل فى: تقديم عرض تحليلى لمجموعة من النظريات الكلاسيكية والمعاصرة فى إطار سوسيولوجيا الجريمة، بقصد الوقوف على التطورات التى شهدتها هذه النظريات، وما طرأ عليها من تغييرات تواكب قدرتها على تفسير الجرائم الرقمية، لاسيما فى ظل مجتمع رقمى تكنولوجي متطور سريع التغيرات على كافة المستويات، واستعراض ما طرأ على الجريمة ذاتها من تغيرات فى ظل مجتمع الرقمنة، والذي يعترف بهذه التقنيات كجزء لا يتجزأ من الكيان الاجتماعي الأكبر، ويقر بإدماج التقنيات الرقمية والوسائط والشبكات في حياتنا اليومية، بما في ذلك ارتكاب الجريمة، والتى أصبح معظمها مرتبط ارتباطا وثيقا بالتكنولوجيا، سواء من حيث الإعداد للجريمة أو تنفيذها، ومن ثم القاء الضوء على فرع حديث من فروع العلم وهو "علم الجريمة الرقمي"، والذى من خلاله يحاول الباحث تقديم نموذج نظري مقترح لتفسير الجرائم الرقمية.

ومن هنا تتجلى أهمية هذه الدراسة فى مواكبتها لحالة التحول الرقمي التي بدأت بالفعل تؤتي ثمارها في العديد من المجالات، وبصفة خاصة بعد أزمة جائحة كورونا، وما خلفته من الاعتماد بشكل كبير على المعلوماتية والانترنت، وظهور دعوات واسعة النطاق إلى أن الاستثمار الأمثل يجب أن يكون في مجالات التقنية الحديثة والتكنولوجيا، وهو ما ترتب عليه لفت الانتباه لهذه المجالات الحيوية، ومن هنا تتحدد الأهمية النظرية والتطبيقية للدراسة على النحو التالي :

نظرياً: تقدم هذه الدراسة قراءة تحليلية متعمقة لمجموعة من الاتجاهات النظرية المعاصرة فى مجال سوسيولوجيا الجريمة، ومعرفة مدى تحديثها وكفاءتها النظرية والتطبيقية فى تفسير الجرائم الواقعة داخل إطار مجتمع الرقمنة، مما يترتب عليه محاولة وضع فرع علم اجتماع الجريمة والسلوك الانحرافى فى أطر نظرية أكثر حداثة وكفاءة، ومحاكاة لواقع المجتمع الرقمى. ومحاولة إضافة جانب معرفي ونظرى لتراث هذا الفرع من فروع علم الاجتماع، خاصة مع التطور الرقمى الذي حدث وغَيّر من نوع الجريمة وأطر تفسيرها.

تطبيقياً: تحاول الدراسة استخلاص مجموعة من النتائج والتوصيات والحلول ووضعها أمام كل من الباحثين وصانعي القرار، تفيد فى تفسير الجرائم الرقمية التى تحدث فى مجتمعاتنا المعاصرة، من خلال نموذج نظرى يعتبر محاولة لسد الفجوات المعرفية التى يعاني منها التنظير فى مجال الجريمة، ومحاولة لحث الباحثين على إجراء المزيد من الدراسات لاختبار فاعلية النظريات فى تفسير ومكافحة الجرائم الرقمية .

## رابعا: مشكلة الدراسة

لم تغير الثورة الرقمية جوانب متعددة من الحياة الاجتماعية فحسب، بل إنها أعادت تشكيل النظريات الاجتماعية والفروض الأساسية التي تقوم عليها، وهو ما استدعى من علم الاجتماع الرقمي تبني نهج انعكاسي نقدي، يكون علماء الاجتماع قادرين من خلاله على معالجة تداعيات الرقمنة على الممارسات الاجتماعية نفسها. كما أعطى المجتمع الرقمي دفعة كبيرة لعدد من الجرائم التقليدية، التي تم تضخيم نطاقها باستخدام أجهزة الكمبيوتر، وشبكات الانترنت، وتكنولوجيا المعلومات، والتى تم تسميتها بالجرائم الإلكترونية أو الرقمية، والتى تعتبر أحدث تطور في عالم الجريمة، وانعكاس للأنواع الجديدة من التكنولوجيا الرقمية، التي غيرت جميع أنواع السلوكيات التي يؤديها الأفراد في الواقع. تاريخياً، وعلى مدى العقود العديدة الماضية، ظهر الكثير من الكتب والمؤلفات والأبحاث العلمية فى العديد من العلوم المختلفة، التى تناولت نظريات الجريمة، وتفسيرها للتباين الفردى والمجتمعى لارتكاب الجرائم فى عالمنا الواقعي. إلا أنه ومع هذا التطور الرقمى لم تعد تلك النظريات بنفس كفاءتها فى تفسير الجرائم الرقمية، نظرا للاختلاف الكبير بينها وبين الجرائم التقليدية من حيث طبيعة الجناة والضحايا والوسط التى ترتكب فيه الجريمة، أو حتى من حيث الدوافع والأضرار وطرق المكافحة. وبالتالى تتحدد إشكالية الدراسة فى الوقوف على مدى فعالية تلك النظريات فى تفسير الجرائم الرقمية، ومدى احتياجها للاختبار التطبيقى ومن ثم تعديلها وتطويرها، ولاسيما مع التغيرات والتطورات التكنولوجية التى شهدتها المجتمعات الحديثة.

## خامسا: تساؤلات الدراسة

يتحدد مما سبق، عدد من التساؤلات التي تسعى الدراسة للإجابة عليها، فيتحدد التساؤل الرئيسي فى: ما مدى جودة نظريات الجريمة الحالية في تفسير جرائم العصر الرقمى ؟. وينبثق منه مجموعة من التساؤلات الفرعية تتمثل فى: ما مفهوم المجتمع الرقمى؟ وما أهم مقوماته؟ ما تعريف علم الاجتماع الرقمى وأهم مجالاته؟ كيف تتشكل ملامح الجريمة فى العصر الرقمى؟ ومن هم مرتكبيها ؟ وما هى دوافعهم؟ وكيف تطور مفهوم الجريمِة الرقمى ؟ وكيف غَيّرت الرقمنة من ملامح الجريمة؟ وهل هناك حاجة إلى نموذج نظري جديد لتفسير الجرائم الرقمية فى إطار علم الجريمة الرقمى ؟ .

## سادسا: التوجه النظرى والمنهجى للدراسة

تنطلق الدراسة من توجه نظرى يشمل مجموعة من نظريات الجريمة الكلاسيكية والمعاصرة التى تم تحليلها، واستخلص منها مجموعة من الفروض والقضايا النظرية، التى أثبتت علميا مدى ملاءمتها لتفسير الجرائم الرقمية، ووضعها فى إطار نظرى، يفيد فى تفسير وقراءة التغيرات التى وقعت على الجريمة فى مجتمعنا الرقمى، وتحليل الآليات التكنولوجية والتى شكلت الجرائم الرقمية، ووضعها فى صورة نموذج نظرى مقترح.

ومن هنا انتَهجت الدراسة الأسلوَب التحليلى التفكيكى في استعراِض لنظريات علم اجتماِع الجريمة، من خلال وصف وتحليل الجريمة والانحراف باعتبارهما ممارسات تكنولوجية اجتماعية متزايدة في المجتمع الرقمي. والذي يرصد الظاهرة ويحاول تحليلها، فيتطرق لماهية عملية التحول الرقمي في واقعنا المعاصر.

**سابعا: محاور الدراسة**

تنقسم الدراسة إلى ثلاثة محاور

## المحور الأول :المجتمع الرقمى والرقمنة....المفهوم والواقع والمقومات

تُستخدم التكنولوجيا الرقمية على نطاق واسع فى مجتمعاتنا الحديثة، متمثلة فى أجهزة الكمبيوتر التقليدية والمحمولة والهواتف الذكية وغيرها، والتى تهدف إلى حدوث اتصال سريع وسهل وبأقل تكلفة بين أفراد المجتمع. وقد أحدثت التقنيات الرقمية، ولاسيما وسائل التواصل الاجتماعي، تأثيرات كبيرة على حياتنا اليومية، حيث ساهمت وسائل التكنولوجيا الحديثة في إرساء العديد من التحولات المجتمعية، تحديداً على مستوى العلاقات الاجتماعية، كما أفرزت فاعلين جدد متميزين فى الاستعانة بوسائل التكنولوجيا الحديثة في أداء أدوارهم الاجتماعية والثقافية والأسرية في سياق التحول الرقمي الراهن. لهذا، فإن أى تحليل للظواهر الاجتماعية لا يكون مكتملاً أو علمياً إلا بالانفتاح على الفضاء الرقمي، وبشكل عام أحدثت الثورة الرقمية الكثير من التغيرات الاجتماعية والثقافية – إيجابية وسلبية – على البنى الاجتماعية.

### ١- نشأة المجتمع الرقمي

ظهر المجتمع الرقمي فى منتصف القرن العشرين، تزامناً مع التغييرات والتطورات العميقة في التحول من التقنيات الميكانيكية والتناظرية إلى التقنيات الرقمية التي شكّلت حياتنا اليومية. وبعد ذلك وتحديداً في أواخر الثمانينيات من القرن الماضي، بدأت الثورة الرقمية، حيث كان العامل المحفز لها هو ظهور الإنترنت وشبكة الويب العالمية عام ١٩٨٩. وفي السنوات الأولى من القرن الحالي، بدأ تبادل المراسلات الإلكترونية، وانتشرت المنتديات والمواقع الإلكترونية، والتجارة ومنصات البيع عبر الإنترنت، حيث يستخدم معظم أفراد المجتمع الآن الخدمات المصرفية الإلكترونية لإدارة حساباتهم ودفع مستلزماتهم[١]. ثم حدث التحول الأخير للرقمنة، في العقد الأول من هذا القرن، عندما ارتبطت أجهزة الكمبيوتر الشخصية الأصغر حجمًا والأكثر قوة ، بالإنترنت الأكثر سرعة، وأصبحت الهواتف المحمولة هى وسيلة الاتصال القادرة على الوصول إلى الإنترنت، وإدارة تطبيقات البرامج المعقدة ووسائل التواصل الاجتماعي، والتي تمكنت في غضون سنوات قليلة من ربط العديد من الهويات الحقيقية والرقمية في جميع أنحاء العالم. نتيجة لذلك، أصبح المليارات من الأشخاص والمؤسسات حول العالم متصلين بالإنترنت، يقرأون ويتعلمون ويتخذون القرارات، ويقومون بتسجيل وجمع المعلومات، وأصبح الخط الفاصل بين العالم الواقعي والافتراضي غير واضح[٢].

وتأكيدا لوجودنا فى العصر رقمي، بلغ عدد مستخدمي الإنترنت في العالم عام ٢٠٢٠ حوالى ٥,٠٥ مليار، مما يعني أن ٦٤٪ من سكان العالم كانوا متصلين بالإنترنت. وهناك ٣,٨ مليار مستخدم لوسائل التواصل الاجتماعي في جميع أنحاء العالم في نفس العام. كما بلغ عدد مستخدمي الإنترنت في العالم ٦ مليار شخص وذلك وفقاً لإحصائيات عام ٢٠٢٢، وهذا الرقم يعادل تقريباً ٦٨% من إجمالي سكان العالم، ويبلغ عدد مستخدمي الشبكات الاجتماعية ٤,٦٥ مليار مستخدم، ومتوسط الوقت الذي يقضيه المستخدمين على الإنترنت هو ٦ ساعات و٥٣ دقيقة[٣].

محليًا، في عام٢٠٢١، كان هناك ٥٩,١٩ مليون مستخدم للإنترنت في مصر، وارتفع عدد مستخدمي الإنترنت في مصر بمقدار ٤,٥ مليون (+٨,١٪) عن عام ٢٠٢٠. وفى عام ٢٠٢٢ ارتفع عدد مستخدمي الإنترنت في مصر إلى ٦٨,٥ مليون مستخدم في شهر يونيو ٢٠٢٢. ووفقًا لتقرير صادر عن مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري (IDSC)، وصل عدد مستخدمي مواقع التواصل الاجتماعي في مصر في يناير ٢٠٢٢ لأكثر من ٥١ مليون مستخدم بزيادة ٥٪ مقارنة بعام ٢٠٢١. علاوة على ذلك، أشار الجهاز القومي لتنظيم الاتصالات، إلى أن متوسط الأنشطة اليومية هو ٣,٥ مليون ساعة يوميًا من مقاطع الفيديو الترفيهية القصيرة المنشورة، و١٨١ مليون زيارة تسوق عبر الإنترنت(٤). ومن هنا تؤكد هذه البيانات على حقيقة مؤداها أن معظم سكان العالم يعيشون فى العالم الرقمى.

## ٢- تعريف المجتمع الرقمي ومقوماته

يعرف كل من "فرنسوا لسلي" و"نقولا ماكاريز" العصر الرقمي بأنه: "زمن كل شيء عددي، أين بإمكان المرتكزات الإلكترونية اليوم أن تخزن، تعالج وتتبادل المعلومات، وتمزج الصوت والمعطيات والصور الثابتة أو المتحركة، مع مستويات من الأمان والدقة، تعادل المستويات المتعلقة بالمعطيات وحدها(٥). أما الرقمنة Digitization فيمكن تعريفها اجرائيا باعتبارها " نظام الكترونى يسمح بتحويل المواد التقليدية كالكتب والسجلات والبيانات، إلى شكل رقمى؛ لسهولة معالجتها بواسطة الحاسب الآلى. ونتيجة للرقمنة، نشأ مجتمع جديد هو المجتمع الرقمي، الذي يعيش ويتفاعل أفراده مع بعضهم البعض في الواقع الافتراضي، بشكل يختلف تماما عما يجري في العالم الواقعي، ويمكن تعريفه بأنه: "ذلك المجتمع الذي يتميز بالتسارع في النمو- والتنمية- وبالانفجار المعرفي وبالاعتماد على التقنية المتقدمة(٦) . ويمكن تعريف "Digital Society" اجرائيا كمفهوم يعترف بالتقنيات الرقمية كجزء لا يتجزأ من الكيان الاجتماعي الأكبر، ويقر بإدماج هذه التقنيات والوسائط والشبكات في حياتنا اليومية، حيث تحولت العلاقات بشكل مفاجئ إلى التواصل والتفاعل داخل العالم الرقمي. ويمكن تحديد أبرز مقومات المجتمع الرقمي، فى المعلوماتية والرقمنة اللتان أفرزتا واقعا جديدا، قائم على الإنترنت(٧)، وسقطت معه الحواجز الصماء التي كانت تفصل بين البشر، كالبعد الجغرافي واختلاف اللغات والافتقار المزمن للمعلومات، فالمجتمع الرقمي هو مجتمع مكون من أفراد غير قادرين على التفكير لأنفسهم فيما يتصل بالعالم الحقيقي(٨).

## ٣- علم الاجتماع الرقمى

لم يترك علم الاجتماع أزمته تستمر بفعل العولمة، وإنما حاول أن يتكيف معها، بل ويعمل على إعادة بناء ذاته، وذلك من خلال إعادة النظر فى موضوع إهتمامه، وميدان إختصاصه، ومن خلال بلورته تيارات نظرية جديدة، وإستراتيجيات منهجية مغايرة، واستطاع معها أن يسهم فى علاج مشاكل الحياة اليومية، وهو ما ترتب عليه ظهور فرع جديد لعلم الاجتماع، هو علم الاجتماع الرقمىDigital Sociology(٩)، والذي برز موضوعه فى غضون عام 2002 عندما نشر العالم "جوناثان وين" مقالاً حول علم الاجتماع الرقمى، حاول فيه تقديم خبرته البحثية الخاصة بالعلاقة الحتمية بين التكنولوجيا وعلم الاجتماع، مقترحاً أن التفكير بطريقة تأملية حول استخدام التكنولوجيا، قد يعزز من قدرات علماء الاجتماع عندما يقومون بأبحاثهم أو عندما يقومون بتدريس ذلك العلم. ويعود زيادة الاهتمام بذلك التخصص إلى المملكة المتحدة، ورابطة علم الاجتماع البريطانية، التى أقامت

مؤتمر لعلم الاجتماع الرقمى، أوضحت فيه المبادئ الموجهة لإجراء البحوث الرقمية. كما بدأت ارهاصات علم الاجتماع الرقمي تظهر في أعمال" ديبورا لوبتون "عام ٢٠١٥ وكانت بعنوان "الحياة الرقمية"، حيث أشار إلى أننا نعيش في مجتمع رقمي، حيث غيرت التكنولوجيا العالم الذي نعيش فيه، وأصبحت التقنيات الرقمية جزءًا لا يتجزأ من الحياة اليومية للعديد من الأشخاص، وتتشكل الحياة الاجتماعية الآن من خلالها، وبذلك يساعدنا مفهوم المجتمع الرقمي على فهم كيفية قيام التقنيات الرقمية بإعادة تشكيل المجتمع الحديث(١٠).

ومن هنا يُعّد علم الاجتماع الرقمى أحد الفروع الحديثة لعلم الاجتماع، والذى يمثل تحدياً فى التعامل مع الأساليب الرقمية، والممارسات المعلوماتية، والاستخدام المجتمعى للبيانات، فهو يهتم بتوضيح وتحليل كيفية جعل البيانات الرقمية مولدة ومنتجة، لمعرفة جوهر المشكلات الاجتماعية المعاصرة، كما أنه دليل مثالي على تطور المناقشات التى تتم حول السلوك الاجتماعي بصورة رقمية. ويركز ذلك الفرع على أربعة نقاط رئيسية؛ الأولى: استخدام وسائل الإعلام الرقمية من قِبَل علماء الاجتماع. والثانية: البحوث الاجتماعية حول استخدام التكنولوجيا الرقمية. والثالثة: استخدام البيانات التى تم إنشاؤها رقمياً. وأخيراً: التحليلات النقدية لوسائل الإعلام الرقمية فى المجتمع(١١). كما لا يقتصر اهتمام علم الاجتماع الرقمي على المجالات التقليدية لعلم الاجتماع كالثقافة، والعمل، والتعليم، والعرق، والطبقة، والمساواة بين الجنسين، لكنه يغطى مجموعة واسعة من الموضوعات الاجتماعية المعاصرة، كالمواطنة الرقمية، والتنظيمات الرقمية، ومناهج علم الاجتماع الرقمية، والثقافة الرقمية، والعلاقات الرقمية، والبحوث الرقمية، والفضاءات الرقمية، والممارسات الرقمية، والمستقبل الرقمي، والمدينة الرقمية، والمساواة وعدم المساواة الرقمية، والجريمة الرقمية(١٢) والتى سوف يتم تناولها فى المحور القادم.

## المحور الثانى : جرائم المجتمع الرقمى (الجرائم الرقمية)

يجب علينا أن نعترف بأن التقنيات الرقمية الحديثة هي مكون رئيسي لمعظم – إن لم يكن كل – الجرائم المرتكبة. فبحسب الخبراء، تتراوح حجم الخسائر السنوية للجرائم الرقمية من ٥٥ مليون دولار إلى ١٣ مليار دولار أمريكي سنويًا. في الوقت نفسه، من المستحيل عمليًا تقييم الحجم الحقيقي للعواقب الاجتماعية للجريمة الرقمية، حيث لا يدرك جميع الأفراد غالباً أنهم أصبحوا ضحايا لمثل هذه الجرائم، تمامًا كما يستحيل تحديد العدد الحقيقي للضحايا في حالة هجمات التصيد الاحتيالي والقرصنة. ووفقًا لمنظمات الأمن السيبراني"McAfee" و "Oracle" وصل الضرر الناجم عن الجرائم الإلكترونية فى عام ٢٠٢١ إلى ٦ تريليونات دولار، وهو ما يتجاوز أرباح التجارة العالمية من المخدرات والأدوية بأنواعها، مما جعل هذا الموضوع فى صدارة اهتمامات مؤتمر "العدالة في أوروبا في مواجهة التحديات الرقمية"، الذي عقد في ١٥ أكتوبر ٢٠١٩، في ستراسبورغ بفرنسا . مما يؤكد أن الجريمة الرقمية تثير قلقًا، خاصة مع الاعتراف بأن طرق مكافحتها غير كافية، ولايزال الإطار القانوني الحالي لمواجهتها فى معظم دول العالم قيد التطوير(١٣).

١– تطور الاهتمام العالمى بالجرائم الرقمية وتعريفها

استغرق مناقشة الجرائم الرقمية والحاجة إلى تعريفها أكثر من ٤٠ عامًا، ويرجع ذلك إلى صعوبة وضع تعريف محدد أو متفق عليه، نتيجة أن هذا المصطلح يختلف من دولة إلى أخرى، وبين العلم والآخر. في الواقع، يمكن رسم التطورات التكنولوجية

وانعكاساتها على الجريمة عبر ثلاث فترات واسعة، الأولى هى حقبة "ما قبل الويب" وتشمل الفترة من الثمانينيات إلى أوائل التسعينيات، والثانية هي عصر "الويب العالمي" وتمتد من التسعينيات إلى أوائل القرن الحادي والعشرين، والأخيرة هى عصر "الويب الاجتماعي" والممتدة من العقد الأول من القرن الحادي والعشرين حتى يومنا هذا. حيث تجلب كل فترة معها تطورات فريدة في التكنولوجيا لها انعكاساتها المختلفة على الجريمة، ويمكن ربطها على نطاق واسع مع التحولات المصاحبة في التفكير والبحث الإجرامي(١٤).

فى البداية، استخدم مصطلح "جرائم الكمبيوتر" لأول مرة في أحد تقارير معهد ستانفورد للأبحاث. لاحقًا قامت الأمم المتحدة باستعراض مختلف الجوانب المتعلقة باستخدام أجهزة الكمبيوتر في المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين، الذي عقد في عام ١٩٩٠ . من بعدها تم تعريف الجريمة الإلكترونية عام ٢٠٠٠ في مؤتمر الأمم المتحدة العاشر لمنع الجريمة والعدالة الجنائية، حيث تم الاعتراف بأن جرائم الكمبيوتر تتعلق بأي عمل إجرامي " قد يرتكب باستخدام، أو داخل، أو ضد، نظام أو شبكة كمبيوتر، من حيث المبدأ، فإنه يغطي أي شكل من أشكال الجرائم التي قد تُرتكب في بيئة إلكترونية. ولكن في وقت مبكر من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية عام ٢٠٠٥، تم اقتراح صياغة هذا المفهوم بطريقة أخرى، باعتبار الجرائم المتعلقة بالكمبيوتر سلوكًا محظورًا، بموجب أن يكون الفعل موجه في مجال الكمبيوتر وتكنولوجيا الاتصالات، أو يشمل استخدام التكنولوجيا الرقمية في ارتكاب جريمة، أو يتضمن استخدام الكمبيوتر كأداة في عملية ارتكاب جرائم أخرى. وفى مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية في كيوتو عام ٢٠٢٠، أقيمت ورشة عمل بعنوان "الاتجاهات الحديثة في الجريمة والتغييرات الأخيرة والحلول الجديدة. ويتضح مما سبق، أن مفهوم "الجريمة الرقمية" غائب عمليًا في الأعمال الدولية، حيث تستخدم معظم تلك الأعمال مصطلح "جريمة الكمبيوتر" كبديل، والذي يُفهم على أنه أي إجراء تكون فيه أجهزة الكمبيوتر وشبكات الكمبيوتر، وكذلك التقنيات الرقمية هي الأداة أو الهدف أو مكان الأعمال الإجرامية(١٥).

وتحقيقا لهذه الغاية، يتم استخدام مصطلح "جرائم الإنترنت أو الالكترونية" و"جرائم الكمبيوتر" بشكل متكرر ومترادف تقريبًا لتحديد ماهية هذه الجرائم، على الرغم من أنهما يشيران من الناحية الفنية إلى سلوكيات مختلفة. فيشير المصطلح الأول إلى الجرائم "التي يستخدم فيها المجرم معرفة خاصة بالفضاء السيبراني"، في حين يشير المصطلح الثانى إلى الجرائم "التى يستخدم فيها المجرم معرفة خاصة حول تكنولوجيا الكمبيوتر. ومع ذلك، يستخدم مصطلح "الجرائم الإلكترونية" بشكل أعم نظرًا للعدد الكبير من الجرائم التي يمكن أن تحدث في بيئات الإنترنت والعدد الهائل من أجهزة الكمبيوتر المتصلة به. ومن هنا تعتبر الجريمة الرقمية ظاهرة اجتماعية غير قانونية، تتضمن مجموعة من الجرائم المرتكبة في مجال التقنيات الرقمية أو باستخدامها، وعادة ما يتم استبدال مفهوم الجريمة الرقمية digital crime بمصطلحات أخرى مثل جرائم الكمبيوتر computer crime ، والجرائم الإلكترونية cyber crime، والجرائم الاونلاينOnline crime. إلا أن الجريمة الرقمية تُعد أكثر شمولا ولها ميزاتها الفريدة، فهى ليس لها حدود جغرافية، ويمكن ارتكابها من أي مكان، وضد أي مستخدم موجود في أي مكان في العالم. كما أن العالم الرقمي يثير الإحساس بعدم الكشف عن هوية المرتكب، وسهولة الإفلات من العقاب عند ارتكاب جريمة باستخدام التقنيات الرقمية، كما يمكن تغيير الدليل الرقمي للجريمة أو إتلافه بسهولة، حيث لا يترك المجرمون عادة أثرًا رقميًا.

وقد حددت اتفاقية الاتحاد الأوروبي الموقعة في ٢٣ نوفمبر ٢٠٠١، جميع أنواع الجرائم في مجال نظم المعلومات والاتصالات، مثل الوصول غير المصرح به إلى البيانات الرقمية، والاعتراض غير القانوني للمعلومات، والتأثير على أنظمة الكمبيوتر، والضرر الجنائي المتعمد بالحذف، والتغيير أو الحظر للبيانات الرقمية. كما تشمل القائمة أيضًا الاستخدام غير المصرح به لأجهزة تقنية خاصة لارتكاب جريمة التزوير والاحتيال، وتوزيع المواد الإباحية للأطفال، أو المعلومات التي تروج للعنصرية والكراهية، والتحريض على العنف ضد الأقليات، والاحتيال المالي، وسرقة البيانات، وكشف خصوصية المعلومات، وجرائم الهوية، والأضرار الشخصية مثل الاستغلال الجنسي للأطفال والنساء عبر الإنترنت(١٦). واخيراً يمكن تعريف الجريمة الرقمية digital crime اجرائياً باعتبارها "سلوك أو فعل يعاقب عليه القانون، يرتكب ضد الأفراد والمجموعات والشركات، بهدف الإيذاء وإلحاق الضرر المادي أو المعنوي، من خلال استخدام الحاسب الآلى أو جهاز الكترونى متصل بشبكة الإنترنت، لتحقيق مكاسب مادية أو معنوية".

ظهر لنا مع انتشار شبكة الويب الاجتماعية، ما يسمى "الويب المظلم" أو "الويب العميق"، وهو اختصار للمحتوى الموجود على الإنترنت غير المفهرس، وغير القابل للبحث بواسطة محركات البحث التقليدية، ويتم حمايته بواسطة التشفير وآليات الأمان الأخرى. لذلك، فإن مثل هذه الشبكات السرية توفر البيئة المثالية للمحتوى الإجرامي لشبكات الإرهاب والجريمة المنظمة(١٧). ويشير النشاط الإجرامي المنظم إلى الأنشطة الإجرامية الخطيرة التي يتم تنفيذها بأشكال التنظيم الإجرامي المهني والمتخصص من قبل جماعات الجريمة المنظمة، التي تعمل معًا عبر الإنترنت أو خارجها على مدار فترة زمنية طويلة وممتدة، وباستخدام تقنيات الاتصالات والمعلومات. وتركز الأدبيات حول الجرائم المنظمة على أنشطة الاتجار بالأدوية المزيفة، وتهريب المهاجرين، والاتجار بغرض الاستغلال الجنسي. وبالتالي، سعى التركيز المتزايد لبحوث الجريمة الإلكترونية إلى تحديد وفهم طبيعة وأنماط شبكات التواصل الاجتماعي الإجرامية عبر الإنترنت.

٢- نحو علم اجتماع رقمي للجريمة (علم الجريمة الرقمي)

مما سبق يتضح عمق التأثير القوي والمباشر للمجتمع الرقمي على عالم الجريمة، فتغير الجرائم من حيث الأنماط وأساليب العمل، أستتبعه أيضًا جرائم جديدة، وطرق حديثة لمكافحة الجريمة. فليس من المستغرب، أنه كلما أصبح العالم أكثر اعتمادًا على التكنولوجيا، تتزايد الجرائم الإلكترونية. حيث توفر شبكة الإنترنت مكانًا للأفراد الذين ينخرطون في الجريمة والانحراف للتواصل وتبادل المعلومات، بشكل آمن عن العالم الحقيقي. نتيجة لذلك، من الضروري أن نبدأ في فهم كيفية حدوث هذه التغييرات، وما يعنيه هذا للجريمة في القرن الحادي والعشرين.

يعتبر تصور الجريمة والانحراف باعتبارهما ممارسات تكنولوجية اجتماعية متزايدة في المجتمع الرقمي، إحدى الطرق التي يمكن أن يفسر بها علم الجريمة الرقمى التأثيرات الواسعة للتكنولوجيا. حيث غيّر الإنترنت وتطبيقاته المتعددة الطريقة التي يقوم بها الأفراد بالعديد من الأنشطة الروتينية، مثل الذهاب إلى العمل، أو المدرسة، أو التواصل الاجتماعي. وتعد مواقع التواصل الاجتماعي مثل Facebook إعدادات مثالية للتفاعل مع الآخرين، ولكنها أيضًا بيئة مثالية لارتكاب الجرائم الإلكترونية .على سبيل المثال، ينشر العديد من الأشخاص بشكل روتيني المعلومات والصور الشخصية عبر الإنترنت، مما يزيد من احتمالية

تعرضهم لجرائم مثل المطاردة أو سرقة الهوية؛ نتيجة السهولة التي يمكن للمجرمين من خلالها الوصول إلى تلك المعلومات عبر الإنترنت، حيث يمكن للجاني الوصول إلى الضحية في أي وقت ومن أي مكان. بالإضافة إلى ذلك، يظل الجاني مجهول الهوية، لأنه يعمل بشكل خفى، ويمكن أن يظهر مجددًا لارتكاب الجرائم مثل الابتزاز الجنسي، والتهديد عبر الإنترنت، والمضايقات، والمطاردة. ومع استمرارية المعلومات والمحتوى للضحايا عبر الإنترنت يظل الشعور بديمومة الجريمة مستمر(١٨).

ومن هنا، ظهر مؤخرًا علم الجريمة الرقمي Digital Criminology من التقاء علم الجريمة والرقمنة بتغيراتها الاجتماعية العميقة، والذي يمكن تعريفه على أنه " مجال دراسي سريع التطور يطبق علم الجريمة، والنظرية الاجتماعية، والأساليب الثقافية والتقنية لدراسة الجريمة والانحراف والعدالة في مجتمعنا الرقمي"، ويشمل مجال علم الجريمة الرقمي الآثار الأوسع للأنظمة التكنولوجية على المجتمع، والثقافة والطرق التي تشكل بها العوامل الاجتماعية والسياسية والثقافية(١٩). ومن خلال وجود علم اجتماع رقمي للجريمة sociology of digital crime يتم التركيز على الجريمة الرقمية ومرتكبيها وضحاياها؛ وردود الفعل الاجتماعية للجريمة الرقمية، والبحث الاجتماعي الذي يستخدم التكنولوجيا كمصدر للمعلومات حول الجريمة الرقمية. كما يعني علم الاجتماع الرقمي للجريمة بدراسة الفرص والمخاطر الرقمية في مجال العدالة ومكافحة الجريمة الرقمية، ويدرس أيضاً الآثار السلبية المحتملة التي قد يخلفها المجتمع الرقمي والمخاوف المرتبطة بها. فعلم الجريمة الرقمي ليس هو علم الجريمة السيبراني والمهتم بالجرائم الإلكترونية فقط، ولكنه إطار أوسع وأشمل، حيث لا يقتصر اهتمام علم الاجتماع الجريمة الرقمية على دراسة الجريمة الإلكترونية فحسب، بل أيضًا دراسة تأثير المجتمع الرقمي على الجريمة، وعلى الاستجابات الرقمية الرسمية وغير الرسمية للجريمة الرقمية، مثل استخدام الذكاء الاصطناعي والروبوتات(٢٠)، والتعرف على طبيعة ما يسمى بالوسط الرقمي وهو الوسط الذي ترتكب فيه الجريمة الرقمية؛ وهو وسط حديث غير معروف، يصعب على العامة فهمه والتعامل مع خباياه. كما يُطلَق على المجرم الرقمي إسم المخترق Hacker، وهو الذي يمارس جريمته السيبرانيّة من خلال أجهزة الكومبيوتر بهدف القرصنة والتصيّد الإحتيالي، والإضرار بالأشخاص أو الشركات، وبالتالي الوصول الى معلومات شخصية أو تجارية يتمّ بيعها واستثمارها من خلال التهديد وقبول الرشوة. كما يتمثل جناة الوسط الرقمي فى :القراصنة، وصغار السن، والمهنيون. ونجد لديهم مجموعة من الدوافع تتمثل فى الدوافع الشخصية الداخلية مثل دافع الكسب المادي، والدافع الذهني، ودافع التعلم. أو قد تكون الدوافع خارجية مثل دافع الانتقام، أو التسلية والدعابة، أو دافع التواطؤ، أو الدافع السياسي(٢١).

وأخيرا، وعلى الرغم من الزيادة الهائلة في الجرائم الرقمية، إلا أن ذلك لم يقابله إلا محاولات قليلة لتطوير وتطبيق نظريات الجريمة على الجريمة الرقمية لتفسيرها. ففي مراجعة حديثة للوضع الحالي لعلم الجريمة السيبراني، يصف "هولت وبوسلر " السنوات العشرين الماضية من البحث فى مجال الجريمة، بأنه اقتصر على دراسة تأثير التكنولوجيا على ممارسات المجرمين، والعوامل التي تؤثر على خطر الإيذاء، وإمكانية تطبيق النظريات التقليدية للجريمة على الجرائم الافتراضية(٢٢). ولذلك سيحتاج علم اجتماع الجريمة الرقمي إلى محاولة تطوير مفاهيم جديدة، ونماذج نظرية إجرامية حديثة حول الجريمة الرقمية والاستجابة الاجتماعية لها. كما سيحتاج إلى اختبار النظريات الإجرامية الكلاسيكية حول الجريمة في المجالات الرقمية، وتطوير واختبار تفسيرات جديدة لها. إن الفشل في تكييف النظرية الإجرامية مع البيئات الرقمية سيؤثر بشكل كبير على جودة المساهمة التي

يمكن أن يقدمها علم الجريمة في تفسير الجريمة والعدالة في العصر الرقمي وعصر البيانات الضخمة[٢٣]. ولذا هناك حاجة ماسة إلى تعاون جديد لسد الفجوات المعرفية والمنهجية الحالية، وهو ما ستحاول الدراسة تقديمه فى المحور الثالث.

## المحور الثالث: النظريات المفسرة للجريمة فى المجتمع الرقمى

يعتبر الإنترنت الاختراع التكنولوجي الأكثر تأثيرًا في الحياة اليومية لكل شخص على وجه الأرض تقريبًا، حيث يتصل الملايين من الأشخاص بالفضاء الإلكتروني يوميا، مما أحدث ثورة في طريقة التفاعل والحياة. ومع استمرار ازدهار تقنيات الإنترنت والكمبيوتر؛ وجد المجرمون طرقًا لاستخدام هذه التقنيات كأداة لأفعالهم المنحرفة، بارتكاب نوعًا جديدًا من الجرائم تُرتكب باستخدام أجهزة الكمبيوتر أو الهواتف المحمولة المرتبطة بالانترنت؛ أطلق عليها حديثا الجريمة الرقمية، والتى تُرتكب من خلال وسيط إلكتروني، مما يجعل من الصعب تعقب المجرمين وتحديد هويتهم، وتشمل عدة أنواع منها الاحتيال الإلكتروني، والتشهير والقرصنة، والتصيد الاحتيالي. في مجال سوسيولوجيا الجريمة، يوجد مجموعة من النظريات التي تحاول تفسير سبب انخراط بعض الأشخاص في السلوك المنحرف أو الإجرامى، بينما يمتنع الآخرون عن فعله. وبالرغم من أن هذه النظريات كانت تهدف في الأساس إلى شرح الجرائم المرتكبة في العالم الحقيقي أو الواقعى، إلا أنه لا يزال من الممكن تطبيقها على الجرائم الإلكترونية، خاصة أن هذا أمر بالغ الأهمية لأن المجتمع أصبح أكثر اعتمادًا على التكنولوجيا، ويقضي أفراده وقتًا أطول في المشاركة في البيئة الرقمية، خاصة بعد حدوث جائحة كورونا عام ٢٠٢٠، والتى تسببت في "جائحة جريمة رقمية"، خاصة بعد عمليات الإغلاق العامة، والقيود شبه المطلقة على السفر في العديد من البلدان، اتجه المجرمون والمنظمات الاجرامية إلى الانتقال للواقع الافتراضي لارتكاب جرائمهم، بدلا من الواقع المادى. لذا يعتبر الوباء هو السبب الرئيسي فى زيادة التحول الرقمى للجريمة.

بشكل عام، تسمح لنا النظريات الإجرامية بتنظيم ما نعرفه عن الجريمة، بحيث يمكن فهمها وتفسيرها. على سبيل المثال، تتناول النظريات قضايا مثل كيفية تعلم الجناة تقنيات ارتكاب الجريمة، وارتباطهم بالجناة الآخرين، ومواقفهم تجاه الجريمة وضحاياها، ودوافعهم لارتكابها، وتصوراتهم عن الضبط والعقاب. خلال القرن العشرين كانت التفسيرات النفسية غير الطبيعية شائعة، إلى جانب النظريات الاجتماعية عن الاغتراب، والحرمان النسبي، ونظريات الثقافة الفرعية والتسمية. في هذا المحور، تجرى محاولة وضع إطار تفسيري تكنولوجى لنظريات الجريمة التي يتم استخدامها للمساعدة في الفهم وتفسير، وتوقع السلوك الإجرامي، وبيان التعديلات التى أضيفت على كل إطار لزيادة فعاليته في التنبؤ بالسلوك الإجرامي. كما يهدف هذا المحور إلى وضع نموذج نظرى مقترح لتفسير الجرائم الرقمية، من خلال فروض النظريات الكلاسيكية والحديثة التى تم اختبارها فعليا وأثبتت فعاليتها فى تفسير تلك الجرائم.

### أولا: الارهاصات المعاصرة لنظريات الجريمة

نلاحظ عند التحليل الدقيق للتراث النظري فى سوسيولوجيا الجريمة والانحراف، أن هناك الكثير من الاتجاهات والمدارس التى اهتمت بتفسير الظواهر الاجرامية فى مجتمعنا المعاصر، وتمثلت فى الاتجاه البيولوجي وأعمال العالم" لمبروزو"، والاتجاه

النفسي للعالم "فرويد"، والمدخل الجغرافى، والفلسفى، والاجتماعى وتحديدا أعمال كل من "دوركايم وميرتون" وتحليلهم للبناء الاجتماعى، كذلك المدخل الثقافى واللامعيارى، والايكولوجى. كما ظهر الاتجاه التقليدى المحافظ المرتبط بالاستقرار والتوازن داخل المجتمع، والذي يؤكد على تحليل البعد الثقافى والاجتماعى المرتبط بالجريمة وتفسيرها، كما ظهرت مجموعة من الاتجاهات الاجتماعية المعاصرة والحديثة في سوسيولوجيا الجريمة منها الاتجاه الثقافى، وتفسيره للجريمة فى ظل مجتمع الانترنت، وهو اتجاه يركز على المضمون الثقافى لتفسير الجريمة من خلال الوقوف على السمات المميزة للجماعات والطبقات والثقافات الفرعية الموجودة فى المجتمع. ومع الزيادة الكبيرة في استخدام التكنولوجيا، بدأ الباحثون الأكاديميون في تطبيق نظريات الجريمة لتفسير الجرائم الرقمية، واعتمدت الأعمال التي نفذت مثل هذا التطوير المفاهيمي في الغالب على عدد قليل من النظريات مثل "الاختيار العقلاني" ونظريات الثقافية الفرعية للجريمة. لذا، ستحلل هذه الدراسة جوانب من النظريات، وتطبيقها في سياق الأنشطة الإلكترونية والجرائم الرقمية .

كان بداية التوجه نحو نظريات جديدة لتفسير الجرائم الرقمية، في مقالة رائدة ظهرت في ميدان علم الجريمة، للباحثة "شيلا براون" عام ٢٠٠٦ بعنوان "نحو نظريات التكنولوجيا الاجتماعية" والتى سعت من خلالها إلى تطوير وترجمة الأطر القانونية والنظرية "القديمة" لفهم الجرائم "الجديدة" في الفضاء الإلكتروني. وبعد عشر سنوات من مقالة براون، وعلى الرغم من الأدبيات المزدهرة حول الكمبيوتر والإنترنت وتأثيرهم على الجريمة، لم يتبنى الكثير من علماء الجريمة هذا التوجه المفاهيمي المهم، باستثناء أعمال علماء الجريمة الثقافية، الذين سعوا لاستكشاف كيف يمكن لشبكة الانترنت أن تغير الطبيعة المبنية ثقافيًا، والممارسات الاجتماعية للجريمة والانحراف(٢٤). على سبيل المثال، قام عالم الجريمة" مجيد يار" بدراسة للنظر في تأثير تقنيات الاتصالات، ووسائل الإعلام الجديدة على أنها بحد ذاتها حافز للإجرام(٢٥). وهناك مثال آخر وثيق الصلة يكمن في مقالة" كيث هاوارد "عام 2012 التي أشار فيها بالمثل إلى التأثير المحدود للنظريات المفسرة للجرائم الإلكترونية، ودعا إلى مزيد من الانخراط في الدمج بين نظريات علم الجريمة مع التكنولوجيا، بدلاً من التركيز على الجريمة الإلكترونية وعلى التكنولوجيا كأداة للنشر، والتي زادت من فرص الشبكات الإجرامية فى تنفيذ جرائمها، ويقترح "طريقة أفضل للتفكير في الأنشطة الرقمية عبر الإنترنت باعتبارها ظواهر إجرامية، متداخلة مع ظواهر تقنية وتكنولوجية أخرى(٢٦).ومن هنا سنحاول فى الجزء القادم عرض مجموعة من النظريات التى تم اختبارها بالفعل فى تفسير الجرائم التقليدية، ومن ثم الجرائم الرقمية واقتراح نموذج نظرى جديد.

## ثانيا: نظريات الجريمة

### ١- نظرية الاختيار العقلاني Rational Choice Theory ونظرية النشاط الروتيني Routine Activity Theory

تعتبر نظرية الاختيار العقلاني "Rational Choice Theory" لكلارك وكورنيش" نهج يستخدمه علماء الاجتماع لفهم السلوك البشري، وكيف يتخذ أفراد المجتمع قرارًا بارتكاب أو عدم ارتكاب جريمة، بناءً على تحليل بسيط للتكلفة والعائد. ويشير هنا مصطلح "العقلانية" إلى تصرف الفرد كما لو كان يوازن بين التكاليف والفوائد؛ للتوصل إلى إجراء يزيد من المنفعة الشخصية مثل "المال أو الجنس أو الإثارة". كما تقر النظرية بأن تصورات الجناة للتكاليف والفوائد، يحكمها عدة عوامل مثل الوقت،

والقدرات المعرفية للجاني، وتوافر المعلومات ذات الصلة عن مكان الجريمة، وأدواتها، والضحية، وبالتالي يزن الجناة نوع ومقدار المنفعة المحتملة، مقابل المخاطر المتصورة للاكتشاف والعقاب. فيما يتعلق بالجرائم الرقمية على سبيل المثال، يمكن للآليات الإلكترونية مثل معرف المستخدم(كلمات السر)، وأنظمة التحكم في الوصول الآلي، وكاميرات المراقبة، أن تكون بمثابة الرادع، لأنها تزيد من نسبة اكتشاف المجرم الرقمي. لذلك، لمنع الجريمة، يجب التركيز بشكل أكبر على العقوبة كرادع[٢٧].

تم إجراء (٦) دراسات لاختبار فروض نظرية الاختيار العقلاني نُشرت بين عامي ١٩٨٩ و ٢٠٠٥. ركزت الدراسة التي أجراها "باتيرنوستر"عام ١٩٨٩، على جنوح الأحداث، وتناول القاصرين للخمر، وتعاطى المارجوانا، والسرقات الصغيرة والتخريب، تم تحديد مجموعة متغيرات لقياس المهارات المطلوبة لارتكاب السلوكيات الاجرامية السابقة، وذلك لأن النظرية تنص على أن المهارات اللازمة لارتكاب الجريمة تؤخذ في الاعتبار عند التفكير في تكاليف وفوائد الفعل. وفى دراسة أخرى أجراها كل من "باتيرنوستر وسيمبسون"عام ١٩٩٦ حول جرائم الشركات، سُئل المستجيبون حول الفوائد المتمثلة فى المكاسب المالية المحتملة، فى مقابل الاحتمالية المتصورة للاكتشاف والعقاب، مثل الكشف من قبل الشرطة، واحتمال إبلاغ الضحية بالحادثة، واحتمال عرض الأمر على المحاكم والهيئات العقابية الأخرى. وتضمنت مقاييس العقوبة الجنائية، السجن، والفصل من الجامعة أو المدرسة أو العمل، والعقاب من الأسرة والأصدقاء. أخيرا، في دراسة أجرتها "McQuade" لفحص تصورات الطلاب عن القبض عليهم بسبب مجموعة متنوعة من الجرائم التي ترتكب بواسطة التكنولوجيا، وُجِد أن المستجيبين يعتقدون أن احتمالية القبض عليهم منخفضة، وأن العقوبة لن تكن شديدة[٢٨].

ظهرت حديثا نظرية النشاط الروتيني Routine Activity Theory (RAT) وهي نظرية إجرامية انبثقت من نظرية الاختيار العقلاني، طرحها كل من "كوهين وفيلسون" عام ١٩٧٩، وتفترض النظرية أنه من أجل ارتكاب جريمة، يجب أن يكون هناك مجموعة عوامل متواجدة ومتوافرة بشكل متزامن وهم: (هدف مناسب ومتاح: مثل شخص أو شيء أو مكان)، (عدم وجود وصي مناسب لمنع وقوع الجريمة: مثل دوريات الشرطة وحراس الأمن والأصدقاء والجيران وأنظمة الدوائر التلفزيونية المغلقة)، (وجود الجاني والدافع). في حالة غياب واحد أو أكثر من هذه العناصر الثلاثة الضرورية، تقل فرصة وقوع الجريمة . تم تأكيد فاعلية نظرية النشاط الروتيني فى تفسير الجريمة الإلكترونية من قبل كل من " بوسلر وهولت"، فى منشورهما عام ٢٠٠٩ بعنوان "الأنشطة عبر الإنترنت، الوصاية، وعدوى البرامج الضارة: فحص نظرية الأنشطة الروتينية"، والذى تم إضافة مناهج بديلة لتوسيع إطارها النظري، واستخدامه لدراسة الإيذاء الإجرامي تم تسميته Lifestyle and Routine Activity Theory (LRAT)، وتؤكد LRAT على فكرة أن تعرض الأفراد لأحداث إجرامية يعتمد بشكل أساسي على نوع الأماكن التي يقضي فيها الفرد وقته، ومع من يقضيه، ونوع الأنشطة التي ينخرط فيها خلال هذه الأوقات. وفقًا لـ LRAT ، فإن الأنشطة والسلوكيات الروتينية لنمط حياة الفرد هي ما تجعل الفرد هدفا مناسبًا، وتشمل القضايا الرئيسية لهذه للنظرية فى (١) القرب من الجريمة، (2)التعرض للمجرمين المحتملين، (3) جاذبية الهدف، (٤) الوصاية. وبذلك فإن الإيذاء هو نتيجة لأنشطة وسلوكيات روتينية معينة يقوم بها الفرد[٢٩].

وجد الباحثون مع الاستخدام المتزايد للإنترنت، بعض الدعم لتطبيق مبادئ نظرية النشاط الروتيني على الجرائم الرقمية، حيث وجد المجرمون فرصًا جديدة لتحقيق أهدافهم على منصة جديدة تمامًا، كما توصلت الأبحاث إلى أن مقدار الوقت الذي يقضيه

الافراد على الإنترنت، وزيادة استخدام الخدمات المصرفية والمشتريات، والسلوك المحفوف بالمخاطر الممارس عبر الإنترنت، ونقص برامج الحماية من الفيروسات وأمن الشبكات، تجعلهم أهدافا سهلة للمجرمين(٣٠). على سبيل المثال، قام العالم "Choi" عام 2008 بتطبيق نظرية LRAT على الإيذاء الفردي من خلال جرائم الكمبيوتر، وخاصة جريمة القرصنة. ووجد أن أحد المبادئ الثلاثة، المتمثل فى غياب الوصاية، هو المساهم الأكبر فى زيادة جرائم الكمبيوتر، وذلك لأن سهولة الوصول إلى الإنترنت، تجعل إمكانية وجود مجرمين متحمسين وأهداف مناسبة لا حدود لها، حيث تُقاس الوصاية من خلال مستويات مختلفة من تفعيل اجراءات الأمان عبر الإنترنت، مثل إعدادات الخصوصية على مواقع الشبكات الشخصية، وتثبيت برامج الفيروسات وجدار الحماية. كما تم إجراء دراسة أخرى بواسطة كل من Reyns " و Fisher و" Hensonعام ٢٠١١ وجدت نتائج مماثلة فى دراستهم "نظرية الأنشطة الروتينية لنمط الحياة السيبراني والإيذاء للجرائم الإلكترونية"، والتى أهتمت بجريمة المطاردة عبر الإنترنت. وجد المؤلفون أن أهم مؤشر على وقوع ضحايا للمطاردة عبر الإنترنت هو التحدث بشكل متكرر إلى شخص ما بطريقة عنيفة، أو التهديد بإيذائه جسديًا عبر الإنترنت، ومحاولة اختراق مواقع التواصل الاجتماعي لشخص، وإرسال صور جنسية إلى شخص ما من خلال الرسائل النصية عبر الإنترنت. الأهم من ذلك، تظهر النتائج دعمًا لهذه النظرية ليتم تطبيقها على بيئات الإنترنت وأبحاث الجرائم الإلكترونية(٣١). وأخيرا، تم استخدام نظريتى الاختيار العقلاني والأنشطة الروتينية لتفسير أسباب الجريمة الرقمية بمفهومها الذي ينص على أن كل شخص يشارك في نشاط إجرامي بعد اختيار عقلاني للقيام به، يتداول مثل هذا الشخص أولاً فوائد ومخاطر الانخراط في مثل هذه السلوكيات ويفعل ذلك فقط إذا تجاوزت المكاسب المخاطر.

## ٢- نظرية الارتباط التفاضلي Theory of differential association ونظرية التعلم الاجتماعي Social Learning Theory

تنطلق نظرية الارتباط التفاضلي" لساذرلاند "من أن السلوك الإجرامي وتقنيات ارتكاب الجريمة هما سلوك طبيعي يتم تعلمه من خلال التفاعل مع الآخرين، واكتساب مجموعة الدوافع العقلانية والمواقف سواء كانت مؤيدة أو معارضة لارتكاب الجريمة، فتُرتكب الجريمة عندما تتجاوز تلك التعاريف المؤيدة لارتكاب الجريمة تلك التعاريف المعارضة لارتكابها. ومن ثم فهناك نوعان من العناصر الأساسية للرابطة التفاضلية: الأول هو العنصر المعرفي، أو محتوى ما يتم تعلمه، مثل تقنيات ارتكاب الجرائم، والدوافع العقلانية، والمواقف المناسبة المؤيدة لانتهاك القانون، ولم يحدد "ساذرلاند" آليات التعلم، وأكد أن عملية تعلم السلوك الإجرامي مثلها مثل أي تعلم آخر. العنصر الثاني من الارتباط التفاضلي هو الارتباط مع أشخاص آخرين في مجموعات شخصية حيث يتم التعلم، وفسّر سبب قيام الأشخاص المختلفين الذين يتعرضون لنفس الظروف الاجتماعية بسلوك إجرامي وآخرون لا، بأن المعاني التي يعطونها لهذه الظروف التي يواجهونها هي التي تحدد ما إذا كانوا ينتهكون القانون أم لا، وتختلف هذه المعاني باختلاف "التكرار والمدة والأولوية والشدة". قام العالم "والكلي" عام ٢٠٠٥ بتطبيق نظرية الارتباط التفاضلي على جرائم الكمبيوتر، وتحديدا جريمتى القرصنة والاحتيال عبر الإنترنت، تم التركيز على ما إذا كان الجناة يتفاعلون أو يعملون بمعزل عن الآخرين، وماهية التفاعل الذي يترتب عليه ارتكاب الجريمة. وعلى الرغم من الإشارة إلى أن المتسللين

يتواصلون عبر الإنترنت باستخدام البريد الإلكتروني، وغرف الدردشة، وعن طريق الهاتف، خلص "والكلى" إلى أنه لا يمكن تطبيق الارتباط التفاضلي على جميع أشكال الجرائم الرقمية، لأن بعض من المجرمين يعملون بشكل منفرد(٣٢).

إلا أنه بشكل عام، يتم تعلم الجرائم الرقمية مثل عمليات الاحتيال عبر الإنترنت، وقرصنة البرامج عن طريق التقليد، والذي يحدث عندما يتعلم الشخص الأنشطة من خلال المشاهدة ويقوم بتنفيذها. كما تتطلب هذه الجرائم نطاقًا معينًا من المهارات والخبرات، في هذا الصدد، يعزز المجرمون الرقميون الشبكات التي تربطهم بالآخرين وتعلمهم هذه المهارات، على سبيل المثال، توفر عصابات الجرائم الإلكترونية بيئة مناسبة من مواقع وغرف دردشة وغيرها لتعليم الشباب المهارات اللازمة للانخراط في الجرائم المتعلقة بالكمبيوتر. وبالتالي تعتبر نظرية الارتباط التفاضلي ذات صلة في توضيح ظهور الجريمة الرقمية، لأن المجرم الرقمي يتعلم مثل هذه السلوكيات المنحرفة من خلال علاقاته المتبادلة مع الآخرين(٣٣).

تُعتبر نظرية التعلم الاجتماعي Social Learning Theory (SLT) ل"بورجيس وأكرز"، إعادة صياغة لنظرية الرابطة التفاضلية "لإدوين ساذرلاند". فوفقًا لنظرية التعلم الاجتماعي، يتم تعلم السلوك الإجرامي من خلال التفاعل مع الآخرين، وتزداد احتمالية أن ينخرط الأشخاص في أنشطة منحرفة عندما يرتبطون بشكل مختلف مع آخرين يفضلون السلوك الإجرامي، ويتعرضون لنماذج إجرامية أو منحرفة، ويقرون أنها مرغوبة أو مبررة، ويتوقعون أو يتلقون مكافأة أكبر من العقاب المتوقع على هذا السلوك(٣٤)، ويتم تعلم المعلومات والسلوكيات الجديدة من خلال عمليتي المشاهدة والملاحظة. تحتوى SLT على أربعة مفاهيم نظرية، الأول: وهو الارتباط التفاضلي Differential association، ويشير إلى الأشخاص الذين يرتبط بهم الفرد، ويتفاعل معهم كالعائلة والأصدقاء، الذين ينخرطون في نوع معين من السلوك، يمكن أن يؤثر على أنماط المعايير والقيم للفرد. المفهوم الرئيسي الثاني هو التعريفات Definitions أو المواقف والمعاني التي يطلقها المرء على سلوكيات معينة، وتحدد هذه التعريفات ما إذا كان الفرد يعتبر الفعل صواب أو خطأ، أو مبررًا أو غير مبرر. وبالتالي، إذا كان لدى الفرد تعريفات مواتية لارتكاب الجريمة، فمن المرجح أن ينخرط في سلوك منحرف. المفهوم الثالث للنظرية هو التعزيز التفاضلي Differential reinforcement، ويشير إلى العلاقة بين المكافآت المتوقعة والفعلية والعقوبات التي تتبع السلوك، وما إذا كان الفرد ارتكب أفعالًا منحرفة بشكل متكرر ولم يتم القبض عليه، أو تمت مكافأته ماليًا وعاطفيًا، فمن المرجح أن يستمر في الفعل. ويشير المفهوم الأخير، وهو التقليد أو النمذجة Imitation or modeling ، إلى مراقبة السلوك الذي يقوم به الآخرون، ثم الانخراط في هذا السلوك. ويمكن توسيع نظرية التعلم الاجتماعي للنظر في الجرائم المرتكبة في العالم المادي وكذلك الجرائم الإلكترونية، كما يمكن تطبيق عنصر الارتباط التفاضلي على مسألة كيفية تأثير "الأصدقاء" على الفرد عبر الإنترنت ودفعه للمشاركة في نشاط اجرامى الكترونى(٣٥).

وفى دراسة حديثة أجراها "Ricketts" عام 2014 حول الجريمة الإلكترونية، وتحديداً سلوكيات المطاردة عبر الإنترنت بين المراهقين، من خلال تطبيق نظرية التعلم الاجتماعي على البيانات التي تم جمعها من طلاب المدارس الثانوية في مقاطعة ريفية في ولاية كارولينا الشمالية الأمريكية، وجدت الدراسة أن المستويات الأعلى من الارتباط بالأقران المنحرفين ساهمت فى زيادة جريمة المطاردة الإلكترونية بين المراهقين، وكان المستجيبون الذين ارتبطوا بأقران منحرفين أكثر عرضة لإختراق البريد الإلكتروني لشخص آخر. ويؤكد الباحثون أن الجناة المحتملين تعلموا التقنيات المعقدة لهذه الجريمة الإلكترونية من خلال

ارتباطهم بأقرانهم المنحرفين عبر الإنترنت(٣٦). كما أجرى كل من "هولت وبوروس وبوسلر "عام ٢٠١٠ أيضًا دراسة تطبق نظرية التعلم الاجتماعي على جرائم الإنترنت، وتحديدا على قرصنة البرامج والوسائط، والمواد الإباحية. ودعمت نتائج هذه الدراسة، الأبحاث السابقة المتعلقة بالعلاقات بين مكونات التعلم الاجتماعي والجرائم الإلكترونية، فى أن الارتباط التفاضلي مع الأقران المنحرفين والتعريفات المؤيدة لانتهاك القانون ترتبط ارتباطًا وثيقًا بزيادة جرائم الإنترنت. حيث وجدت الأبحاث أن نظرية التعلم الاجتماعي، لا تفسر قرصنة البرامج فقط، بل يمكن أن تفسر جرائم إلكترونية أخرى، على سبيل المثال، في أي جريمة، يجب تعلم المبررات والمهارات وتعزيز السلوك من خلال الارتباط بالآخرين ومراقبتهم. وبالتالي، فإن الفكرة الرئيسية وراء نظرية التعلم الاجتماعي هي أننا نصبح ما نحن عليه بناءً على محيطنا، ومن ثم يمكن استخدام هذا التفسير لشرح الجرائم الإلكترونية **المختلفة**(٣٧).

## ٣- نظرية الضغط البنيوي Structural strain theory ونظرية الضغوط والجرائم الإلكترونية Strain and Cybercrimes Theory

تركز هذه النظرية على البنية الاجتماعية، والتحليل على مستوى الوحدات الكبرى macro ، فتنص نظرية الضغوط ل"ميرتون"، والتي تُعرف أيضًا باسم نظرية الفرص المحظورة Blocked Opportunity Theory على عدم المساواة بين الأهداف المحددة ثقافيًا (المقاسة بالقيمة النقدية) والوسائل المشروعة (المقاسة من خلال العمل والتعليم) لتحقيق هذه الأهداف. لكن ليس كل شخص تتاح له الوسائل المشروعة لتحقيق أهدافه، لذلك يتم خلق إجهاد أو ضغط على أفراد الطبقة الدنيا، الذين من المرجح أن يلجأوا إلى الوسائل غير المشروعة (الجريمة) لتحقيق الهدف(٣٨). قام "ميرتون "بتحديد خمسة أنماط للتكيف مع الضغوط هم: التوافق، والطقوس، والابتكار، والتراجع، والتمرد. فالشخص المتوافق يقبل الأهداف الثقافية ويقبل الوسائل المؤسسية للحصول عليها، لذا فمن غير المرجح أن يرتكب أعمال إجرامية. ويرفض رجل الطقوس الأهداف الثقافية، لكنه يقبل الوسائل المؤسسية، كما أنه من غير المحتمل أن يرتكب الجرائم. ويقبل المبتكرون الأهداف، لكن ليس بالطريقة العادية لتحقيقها، وقد يلجأ المبتكرون إلى الجريمة لتحقيق أهدافهم. كما يرفض المتراجعون كلاً من الأهداف والوسائل، كما إنهم لا يطمحون إلى أن يكونوا ناجحين، ولا يهتمون بأهداف المجتمع التقليدية، لذلك قد يصبح المتراجعون مجرمون. وأخيراً، يرفض المتمردون الأهداف والوسائل الثقافية ويستبدلونها بأهداف ووسائل جديدة، غالبًا ما تكون هذه الأهداف الجديدة إجرامية(٣٩).

تكمن أهمية نظرية الضغوط "لأجنيو" فى تركيزها على العوامل المجتمعية، وليس الفردية. وتعتبر تحديث لنظرية "ميرتون"، فى النظر إلى الجريمة والجنوح كرد فعل لقائمة أوسع من الضغوطات أو مصادر التوتر. يحدد" أجنيو "ثلاثة أنواع من الضغوط التي قد تؤدي إلى الانحراف والجريمة: أولهم الفشل في تحقيق أهداف الفرد، ثانيا إزالة المحفزات ذات القيمة الإيجابية من الفرد، وثالثا مواجهة الفرد بالمحفزات السلبية، مما ينتج عنه الانحراف الناتج عن ضغوط. وتتمثل إزالة المحفزات ذات القيمة الإيجابية من الحياة الفردية للشخص، بخسارة أو وفاة أو مرض أحد المقربين، أو ترك المدرسة أو العمل. كما تؤدي المواجهة مع المحفزات السلبية أيضًا إلى إنتاج ضغوطات مختلفة، كأحداث الحياة التي تنطوي على مواجهة الأفعال السلبية من قبل الآخرين، كرد فعل لذلك، قد يلجأ الأفراد إلى السلوك المنحرف كطريقة للتغلب على التوتر، والسعي للانتقام من المصدر

المتصور للتوتر أو الاتجاه إلى السلوكيات مثل تعاطي المخدرات(٤٠). ويؤكد" أجنيو" أن التوتر يجعل الناس يشعرون بالغضب، والإحباط، والاكتئاب، واستجابة لهذا الضغط، يلجأ الأشخاص إلى الجرائم الرقمية مثل التنمر الإلكتروني، للتخفيف من المشاعر السيئة لديهم. توفر نظرية الإجهاد العام وفرضية الإحباط فهمًا لكيفية استجابة الأفراد، وخاصة الشباب، للتعامل مع الضغط السلبي، سواء كان ذلك بالتنمر على الآخرين، أو أن يلجأوا إلى عمليات الاحتيال على الكمبيوتر وغيرها من الأنشطة التي قد تؤدي إلى مكاسب مالية؛ لتخفيف الضغط(٤١).

قام العالم "والكلي" عام ٢٠٠٥ بتحليل نظرية الإجهاد البنيوي؛ لتحديد قوتها التفسيرية فيما يتعلق بالقرصنة والاحتيال عبر الإنترنت، مع التركيز فقط على أساليب التكيف الابتكارية والتمرد، وأكد "والكلي" أن مرتكبي جرائم الكمبيوتر الذين سعوا لتحقيق مكاسب مالية كانوا مبتكرين، على الرغم من عدم وجود دليل يشير إلى أنهم تعرضوا لضغوط. كما قام أيضًا بتوضيح العلاقة بين التمرد والموظفين الساخطين الذين يسرقون أو يتلفون معلومات صاحب العمل السابق، وأثبت من خلال دراسته فاعلية تطبيق نظرية الضغوط على الجرائم الإلكترونية(٤٢).

## ٤- نظرية التسمية Labeling theory

تنطلق نظرية التسمية ووضع العلامات للعالم "بيكر" من مكونين هامين: الأول، يبحث في السلوكيات التي يتم تسميتها على أنها إجرامية، وأن الجماعات هى التي تتخذ هذه القرارات وتطلق تلك المسميات، وفقًا "لبيكر" تعتبر الجريمة من صنع المجتمع، نظرًا لأن الجماعات الاجتماعية تضع القواعد وتطبقها، وتسمي أولئك الذين يخالفون القواعد بأنهم منحرفون، لذلك فإن أولئك الذين تبين أنهم خالفوا القانون يشاركون "تسمية وخبرة وصفهم بأنهم غرباء"، وبالتالي يجب أن تركز تفسيرات الجريمة على العملية التي يتم من خلالها تصنيف وتسمية الأفراد باعتبارهم مجرمين. المكون الثاني لنظرية بيكر، مستمد من "المدخل التفاعلي الرمزي"، والذى يفحص معاني الجريمة للفرد والمجتمع، حيث ذكر بيكر أن المجرمين، اعتمادًا على خطورة الجريمة، يمكن اعتبارهم من قبل الآخرين "غرباء"، لأنهم انتهكوا قاعدة اجتماعية، تؤدي هذه التسمية إلى أن تبنى الأفراد هويات إجرامية ويعيدون ارتكاب الجريمة لاحقًا. كما أن عملية وضع العلامات يقوم بها العديد من الأشخاص والمؤسسات، بما في ذلك، على سبيل المثال، الآباء والأصدقاء والمعلمين والمحاكم وضباط الشرطة وحراس السجون والأقران المنحرفين(٤٣). وبالتالى هي إحدى النظريات التي يمكن استخدامها لفهم ديناميكيات الجرائم الإلكترونية، خاصة لوصف الاستجابة المجتمعية للسلوك. فمن ناحية أخرى، تم تطبيق النظرية في هذا السياق على الجرائم الإلكترونية، خاصة بين متسللي" القبعة البيضاء "و"قراصنة القبعة السوداء. حيث يشير المصطلح الأول إلى المتسللين الذين ينخرطون في سلوكيات القرصنة كاستراتيجية لمساعدة الشركات على حماية شبكتها. أما قراصنة القبعة السوداء، بدورهم، هم الهاكرز الأكثر إجراماً والذين ينخرطون في السلوكيات الإجرامية، ما يؤكد على إعطاء مسميات وعلامة جنائية لمرتكبي الجرائم الإلكترونية، تساهم فى زيادة هذا النوع من الجرائم(٤٤).

## ٥- نظرية الانتقال في الفضاء Space Transition Theory

ظهرت الحاجة إلى نظرية جديدة منفصلة للجرائم الرقمية؛ لشرح أسباب الجرائم في الفضاء الإلكتروني، لأن التفسيرات النظرية العامة كانت غير كافية للتفسير. ومن هنا، ظهرت "نظرية الانتقال الفضائي" في كتاب بعنوان "جرائم الإنترنت" للعالم "فرانك شماليجر" و"مايكل بيتارو"، وهي تركز على شرح طبيعة سلوك الأشخاص الذين يظهرون في الفضاء المادي والإلكتروني، ويقصد بالانتقال الفضائي هنا، عملية حركة الأشخاص من الفضاء المادي "الواقع"، إلى الفضاء السيبراني "الانترنت" والعكس، وتصرفهم بشكل مختلف. وللنظرية مجموعة فروض تتمثل فى، أولا: يميل الأشخاص أصحاب السلوك الإجرامي المكبوت (في الفضاء المادي) إلى ارتكاب الجريمة في الفضاء السيبراني، لصعوبة ارتكابها في الفضاء المادي، بسبب وضعهم الاجتماعي أو الوظيفي. ثانيا: توفر مرونة وسرية الهوية، وغياب عامل الردع فى الفضاء السيبرانى للجناة، يمثل دافع قوى لارتكاب الجريمة الرقمية. ثالثا: من المرجح أن يتم جلب الدافع للسلوك الإجرامي للمجرمين من الفضاء السيبراني إلى الفضاء المادي والعكس أيضًا. رابعا: الطبيعة الديناميكية الزمانية والمكانية للفضاء السيبراني تتيح فرص للهروب والإختفاء اكثر من الواقع المادى(٤٥).

لا تفسر هذه النظرية الجريمة التقليدية ولكنها تركز على الجريمة الإلكترونية، الناتجة عن الأشخاص الذين لديهم سلوك إجرامي مكبوت في الفضاء المادي، والتي لن يرتكبون الجريمة فيه، ويصبح لديهم ميل لارتكاب تلك الجريمة في الفضاء الإلكتروني، لأن السلوك الفردي المكبوت في الفضاء المادي، لا يتم قمعه في الفضاء الإلكتروني. في هذا السياق، فإن نفس هؤلاء الأشخاص المهتمين بوضعهم الاجتماعي في العالم المادي ليسوا منزعجين من وضعهم في الفضاء السيبراني، لأنه لا يوجد من يراقبهم ويوصمهم. حيث يمكن استخدام ميزة عدم الكشف عن الهوية للتعبير عن المشاعر السلبية، عن طريق الإساءة إلى أشخاص آخرين، والتى لا يمكن فعلها في لقاء وجهاً لوجه، فالفضاء السيبراني من ناحية أخرى يغير الوضع ويفسح المجال لعدم وجود عامل ردع، نظرًا للطبيعة الديناميكية التى يتميز بها، فهناك صعوبة كبيرة في تحديد موقع المجرمين على الإنترنت. ومن المرجح أن يتحد الغرباء معًا في الفضاء الإلكتروني لارتكاب جريمة في الفضاء المادي، كذلك من الممكن أن يتحد شركاء الفضاء المادي لارتكاب جريمة في الفضاء الإلكتروني(٤٦).

## ٦- نظرية تقنيات التحييد Techniques of neutralization theory

تعرّف تقنيات التحييد بأنها "سلسلة من الأساليب التي يقوم بها أولئك الذين يرتكبون أفعالًا غير مشروعة، عن طريق إبطال مؤقت لبعض القيم داخل أنفسهم، والتي من شأنها أن تمنعهم عادةً من تنفيذ مثل هذه الأفعال، مثل الأخلاق، والالتزام بالقانون، وما إلى ذلك". بمعنى آخر، هى طريقة يستخدمها الأفراد لإيقاف "الاحتجاجات الداخلية" عندما يفعلون أو على وشك القيام بفعل يعتبرونه خطأ. وتنص فرضية" ماتزا وسايكس" أصحاب هذا الإتجاه، على أن الناس يدركون دائمًا أهمية أن يلتزموا بالقانون، وأن عليهم نفس الالتزام الأخلاقي داخل أنفسهم لتجنب الأعمال غير المشروعة. وهكذا، فأنه عندما يرتكب شخص ما أعمالًا غير مشروعة، يجب عليه استخدام نوع من الآلية لإسكات الرغبة في اتباع هذه الالتزامات الأخلاقية. كما ترفض هذه الفرضية، رؤية النظريات الأخرى التي اقترحت أن المجموعات التي تحتوي على المجرمين، قد أنشأت قانونًا أخلاقيًا دائمًا

خاصًا بهم يحل تمامًا محل الالتزامات الأخلاقية. وهكذا، كان" ماتزا وسايكس" قادرين على شرح كيف أن الجناة "ينجرفون" مرارًا وتكرارًا من أنماط الحياة غير الشرعية إلى أنماط الحياة المشروعة، لأنهم يحتفظون بالقانون الأخلاقي بدلاً من مسحه، واستبداله بآخر غير شرعي كما اقترحت نظريات أخرى.

ابتكر" ماتزا وسايكس" مجموعة من الأساليب التي اعتقدوا أن المجرمين يبررون بها أفعالهم غير المشروعة تتضح فى، أولا: إنكار المسؤولية، حيث يؤكد الجناة أنهم كانوا ضحايا للظروف أو أُجبروا على أوضاع وأفعال خارجة عن إرادتهم. ثانيا: إنكار الضرر، وفيها يصر المجرم على أن أفعاله لم تسبب أي ضرر أو إيذاء لأحد. ثالثا: استحقاق الضحية، ويعتقد المجرم أن الضحية تستحق أي فعل ارتكب ضدها. رابعا: إدانة الأفعال، ويؤكد الجناة أن أولئك الذين يدينون جرمهم من أفراد المجتمع، يفعلون ذلك بدافع تصنع المثالية أو تحقيق الشهرة على حسابهم. خامسا: جذب الولاءات الأعلى، ويبرر من خلالها الجاني أن جريمته كانت من أجل الصالح العام أو لنصرة فئة مقهورة أو لرفع الظلم عن شخص أو طبقة(٤٧).

نُشرت (٩) دراسات بين عامي ١٩٨٠ و٢٠٠٩ اختبرت نظرية تقنيات التحييد، وكان هناك اختلاف كبير في منهجيات البحث. ففى الدراسات الثلاث الأولى، التي أجريت بين عامي ١٩٨٠ و ١٩٩٤، تم استخدام اجراءات البحث الكمي، من خلال تصميم مقياس لاختبار عدد من تقنيات التحييد المحتملة. وبالمقارنة، استخدمت الدراسات الست المنشورة بين عامي ٢٠٠٣ و ٢٠٠٩ أساليب كيفية، بما في ذلك المقابلات المفتوحة، والملاحظات، وتحليل مدونات الإنترنت، لتحديد وتحليل تقنيات التحييد(٤٨). وثبتت الدراسات السابقة كلها استخدام تقنيات التحييد فى الجرائم الالكترونية بدرجات مختلفة، وهو ما أكده العالم "McQuade"، حيث أن عدم المواجهة الجسدية مع الضحية تسمح للمجرم إنكار الضرر، خاصة أن الضحايا، بالنسبة للمجرم تصبح كيانات مجهولة الهوية، أو أنظمة كمبيوتر، أو ربما شركات، بدلاً من أشخاص حقيقيين تتعرض سبل عيشهم ورفاهيتهم للخطر. كما يؤكد العالم "yar" أيضًا على أن دوافع المتسللين للإساءة، تتمثل فى "الفضول الفكري، والرغبة في توسيع حدود المعرفة، ومقاومة استبداد وهيمنة الشركات، وتحسين أمن الكمبيوتر من خلال كشف التراخي وعدم كفاءة أولئك المكلفين بحماية البيانات الحساسة اجتماعيًا، قد تكون أشكالًا من أشكال التحييد التي تهدف إلى التغلب على الاحساس بالذنب. واقترح " يار" أشكال إضافية للتحييد، مثل إلقاء اللوم على الضحية على أنها تستحق، أو أن الضحايا من الشركات مثل Microsoft يمكن أن يتحملوا الخسائر. واشتملت الدراسة التي أجراها"Turgeman" عام ٢٠٠٩ على مقابلات متعمقة مع من ارتكبوا جرائم قرصنة البرامج، والتجسس على الهاتف، لتحديد ما إذا كانوا قد قاموا بتحييد سلوكهم المسيء أم لا، خلصت نتائج الدراسة إلى أن هؤلاء الجناة، ينكرون الضرر على الضحايا بالفعل، بالادعاء بأن "تنزيل المعلومات هو نسخ وليس سرقة"؛ وتبرير أفعالهم على أنها انتقامية، وخلص أيضا إلى أن هناك دعمًا قويًا لتقنيات التحييد بعد تنفيذ الجرائم الرقمية(٤٩).

## ثالثا: نظريات مكافحة الجريمة:

ركزت نظريات منع ومكافحة الجريمة في الثلاثين عامًا الماضية على تفسير سلوك الضحايا المحتملين ودوافع المجرمين، من خلال نظريتان بارزتان تم استخدامهما لمكافحة السلوك الإجرامي هما :١) منظور الإيذاء victimization perspective ، الذي يركز على التفاعلات بين الضحية والمجرم والبيئة؛ لإنتاج الجريمة، ٢) منظور الضبط الاجتماعي social control

perspective والذى يركز على الدور الذي يلعبه أفراد المجتمع والأسرة في التأثير غير الرسمي على القيم الأخلاقية للمجرمين المحتملين. وعلى الرغم من أهمية المنظورين في تطوير علم الجريمة والوقاية منها، إلا أن هذه النظريات لم تأخذ في الحسبان الزيادة الهائلة في استخدام تكنولوجيا المعلومات والاتصالات، وكيف يؤثر استخدام التكنولوجيا على الجريمة، ولم تتطور من أجل ذلك. وبدون النظر إلى تأثير الاستخدام السائد للتكنولوجيا، فإن نظريات منع الجريمة التقليدية سنصبح محدودة، بسبب الافتراضات المتأصلة التي يتخذها كلا النهجين حول اقتصار تواصل أفراد المجتمع مع بعضهم البعض على أن التفاعل وجهاً لوجه وبشكل مادى مباشر، هو المؤثر الوحيد على السلوك الاجتماعي. ومن هنا تأتى محاولة" رقمنة "نظريات مكافحة الجريمة التقليدية، لتصبح أكثر تنبؤية من خلال الاعتراف بأن التكنولوجيا تغير كيفية تلقينا للمعلومات والتواصل، مما يؤثر بالتالي على سلوك الضحية والمجرم، وكذلك التفاعلات بينهما. وستصبح تلك النظريات أكثر قدرة على تحديد العوامل الاجتماعية والاقتصادية التى تتحكم فى قدرة الفرد على الوصول إلى المعلومات، والتي يمكن أن تؤثر في النهاية على احتمالية تعرضه للإيذاء، حيث يتمتع أولئك الحاصلون على مستويات أعلى من التعليم والمهارات، بفرصة أفضل للوصول إلى المعلومات الواردة وتفسيرها، وهذا يمكن أن يقلل من خطر وقوعهم كضحية، أى أن التكنولوجيا يمكن أن تجعل البعض أقل أو أكثر عرضة للوقوع كضحية(٥٠).

## ١- منظور الإيذاء victimization perspective

يركز منظور الإيذاء على تفسير الجريمة على أنها أحداث تقع بين الضحية المحتملة والجاني والبيئة، وتم استخدام هذا المنظور لتطوير تقنيات وقائية تقلل من فرص الإيذاء، من خلال اعتبار الضحايا والجناة المحتملين كفاعلين يلعبون دورًا في البيئة (أي المكان والزمان). لذلك، حاولت تقنيات منع الجريمة تعديل سلوك الضحايا المحتملين (على سبيل المثال، تشجيعهم على عدم المشي في الشوارع المظلمة) والجناة (على سبيل المثال، معالجة دوافعهم مثل نقص الوظائف، وزيادة معرفتهم بالعقوبات). كما يلعب الزمان والمكان دورًا رئيسيًا في تحديد احتمالية وقوع السلوك الإجرامي وأيضًا فهم العلاقة – سواء كان القرب المادي أو الوضع الاجتماعي – للضحايا والجناة المحتملين. من خلال منظور الإيذاء، تُستخدم البيئة والعلاقة بين الضحايا والجناة المحتملين لتوجيه استراتيجيات منع الجريمة. يركز منظور الإيذاء التقليدي على الضحايا والجناة الذين يستوعبون المعلومات التقليدية المتاحة ومعالجتها (على سبيل المثال، الشوارع الفارغة المظلمة تمثل خطرا أكبر على الضحية، وفرص أعلى للمجرم لارتكاب جريمته)، إلا أنها لا تأخذ في الحسبان، المعلومات التي توفرها التكنولوجيا، مثل الرسائل النصية التى تحذر من السير في طريق معين، أو وجود الهاتف المزود بكاميرا يمكن أن يساهم فى القبض على الجاني. فالتكنولوجيا تسبب تغييرا في المعالجة المعرفية، لأنها تعدل العلاقة بين الضحية والجاني والبيئة، وتجعل الناس يقومون بتقييم خطر التعرض للإيذاء أو الوقوع كضحية. على الرغم من أن التكنولوجيا تجعل هذا النوع من المعلومات متاحًا بسهولة، إلا أن منظور الإيذاء التقليدى يأخذ في الاعتبار المعلومات المتعلقة بالضحية، والجاني، والبيئة، التي تتم معالجتها معرفيًا فقط، ولا يأخذ في الاعتبار المعلومات المستمدة من التكنولوجيا. لذلك، يجب أن يعترف منظور الإيذاء بالتكنولوجيا، وكيفية الوصول إلى المعلومات، لمنع الوقوع كضحية بشكل أفضل(٥١).

## ٢- منظور الضبط الاجتماعي

يركز منظور الضبط الاجتماعي للعالم "هيرشى" على نقل القيم وتنظيم السلوك من خلال التفاعلات. وبشكل أكثر تحديدًا، يقترح علماء هذا المنظور أن البالغين يشكلون أخلاق المراهقين وسلوكهم، عن طريق وضع المعايير وتنفيذها، من خلال التفاعلات المباشرة وجهاً لوجه. هذا يشير إلى أن هناك العديد من مصادر الرقابة الاجتماعية في المجتمع، فالتأثير الذي ينتج عن العلاقة بين الأطفال والآباء وغيرهم من البالغين، يعطى الطفل الدافع للالتزام أو رفض أخلاق ومعايير المجتمع. ومع ذلك، ماذا يحدث عندما يتم اكتساب المعايير والقيم من خلال التفاعلات التي تحدث على الإنترنت؟. لقد غيَّر الإنترنت إلى حد كبير إجراءات التواصل والتفاعل، وبالتالي أثَّر على السلوك الاجتماعي، خاصة بين الشباب، لأن أنظمة القيم الخاصة بهم لا تزال تتطور. حيث تتيح التكنولوجيا التواصل مع مجموعة أكبر من الأشخاص، وتسمح بالتعرض لمجموعة أكبر من المعايير المستمدة من الفضاء السيبرانى.

ويقترح علماء المنظور أنه مع زيادة مقدار الوقت الذي يقضيه الشباب في التكنولوجيا، قد يكون هناك بالتأكيد تأثير أكبر على أنظمة قيم الشباب التي تكون نتيجة مباشرة لزيادة استخدامها. يشير هذا المنظور المعدل إلى أن التعرض للأفكار والمعتقدات والقيم التي قد تتعارض مع كيفية تأثير المجتمع على الأخلاق، وأن استيعاب مثل هذه الأخلاق يمكن أن يؤثر بشكل مباشر على دوافع المجرمين المحتملين، فهناك مستويات مختلفة من التأثير وربما التفاعلات وجهاً لوجه هي أقوى تأثير على الأعراف الاجتماعية، نظرًا لأن الناس يقضون المزيد من الوقت والطاقة في التواصل عبر الإنترنت مع أولئك الذين يعيشون ولا يعيشون في مجتمعاتهم المحلية. يجب أن تراعي نظريات منع الجريمة كيف يشكل الاتصال عبر الإنترنت أنظمة القيم، وعلى الرغم من أن التواصل وجهاً لوجه قد يكون وسيلة لبناء العلاقات داخل المجتمع، فإن العلاقات التي تنتج بسبب التعديلات التكنولوجية في إجراءات التواصل تؤثر على الضحية والسلوك الإجرامي. سيكون منظرو الضبط الاجتماعي أكثر دقة في توقع الجريمة إذا أدركوا التأثير الهائل للتكنولوجيا – وخاصة وسائل التواصل الاجتماعي – على العلاقات[٥٢].

## النتائج

### أولا : النتائج العلمية

#### ١- أهمية بناء نموذج نظري جديد للجرائم الرقمية :

كان الهدف الأخير من أهداف الدراسة هو محاولة اقتراح مدخل نظري يساهم في فهم وتفسير الجرائم الرقمية. ويتجلى أهمية هذا الهدف فى ما توصلت إليه هذه الدراسة، من أن كل النظريات التى تم عرضها ساهمت بجزء ضئيل جدا فى تفسير الجرائم الرقمية، بالإضافة إلى أن الكثير من فروض تلك النظريات تحتاج الكثير من التدقيق العلمي، سواء على المستوى النظري أو الامبريقى فى تفسيرها لتلك الأنواع من الجرائم. حيث قدمت النظريات التي تم عرضها في هذا البحث رؤى حديثة ومختلفة للجرائم الرقمية، ولكن لم تقدم أي منها تفسيراً كاملاً لسبب حدوث تلك الجرائم مثل القرصنة والاحتيال المالي عبر الانترنت، بل قدمت تلك النظريات تفسيرات جزئية لكيفية بدء الجناة في سلوكهم، وارتكابهم جريمتهم، ورؤيتهم للعقاب.

ومن هنا كان لابد من التوجه إلى محاولة بناء نموذج نظري، أكثر شمولاً يتضمن دمج الجوانب المتوافقة من النظريات؛ لتحقيق جانب من التكامل النظري، والذى قد يشكل إطارا نظريا لوصف وتحليل وتفسير أكثر دقة وتحديدا للجرائم الرقمية، ويمكن اختباره تجريبيًا لاحقًا، أو إضافة منظمة لقضايا وفروض جديدة، حتى يتحول إلى نظرية شاملة، ويكون هذا النموذج بمثابة خطوة أولى فى طريق تطوير طرق مكافحة الجريمة الرقمية، واثراء نظرى لمجال سوسيولوجيا الجريمة الرقمية .

أ- بناء النموذج

تعتمد فكرة النموذج على بنية فكرية تصورية، يتم تجريدها من كمٍّ هائل من العلاقات والتفاصيل، فيتم اختيار بعضها ثم يعاد ترتيبها وتنسيقها ترتيبًا خاصًّا، بحيث تصبح مترابطة ترابطًا يتميَّز بالاتساق والاعتماد المتبادل. فالنموذج كما عرفه "ميرتون" بأنه عبارة عن تشخيصات مؤقتة لماهية النسق، قد تفترض علاقات معينة بين المتغيرات من أجل إجراء البحث الامبريقى، ويصاغ النموذج فى حالة غياب النظرية أو فى حالة عدم توافرها فيما يتعلق بنطاق امبريقى معين، وتعتبر النماذج عوامل اساسية فى عملية التحليل، ويتكون النموذج من مجموعة قضايا نظرية متشابكة ومتفاعلة، وهى بمثابة مقدمات نظرية قابلة للاختبار الامبريقى، وتتيح له القدرة على تفسير اتجاهات يمكن تعميمها، وعلاقات متبادلة تسود في العالم الواقعي، ومن هنا يبدأ النموذج بجمع المفاهيم المرتبطة ذات الأهمية في الموقف المراد بحثه، وينتهي عندما ينتج قضايا نظرية تساهم فى تفسير الجرائم الرقمية، ويتمثل الأمر الأكثر أهمية للنماذج بأنها تمدنا بالتقديرات المبدئية التى يمكن أن نختبرها، والتى منها يمكن أن نصوغ النظريات ذات القيمة التفسيرية الأخرى.

ب- صياغة المفهوم:

وهى عملية يكون الغرض منها صياغة أسم أو مفهوم للظاهرة محل الدراسة فى النموذج، وأن يكون معبرا بصورة واقعية وتجريدية عن تلك الظاهرة، وقد استخدم الباحث مجموعة من المفاهيم الرئيسية داخل هذه الدراسة وتم تعريفها اجرائيا، وهى

تشكل أحد الأسس الهامة لهذا النموذج النظرى مثل مفهوم ( الرقمنة Digitization – المجتمع الرقمى Digital Society – علم الجريمة الرقمى Digital Criminology – الجريمة الرقمية Digital crime ). وهو ما دفع الباحث إلى اختيار " نموذج الجرائم الرقمية" ليرمز إلى الأفكار والقضايا النظرية محل الدراسة. ويتمتع هذا النموذج بالمرونة والقابلية للتطور والاتساع، بما يعنى إمكانية إضافة قضايا نظرية جديدة تكون قابلة للاختبار الامبريقى.

ثانيا: مستويات التحليل

يجمع هذا المقترح النظرى بين مستويين من التحليل مستمدين من النظريات التى تم استعراضها داخل هذه الدراسة، حيث انقسمت إلى: نظريات تعتمد على التوجه البنائي الوظيفي، والذى أعتمد على التحليل الكلّي والمرتبط بالوحدات الكبرى (ماكرو)، وأشهر منظّريها: " ميرتون " و " أجينيو ." النوع الثاني من النظريات تلك التى تعتمد على التوجه التفاعلي الرمزي والذي يعتبر أن المجتمع هو نتاج التفاعل اليومي بين الأفراد، والواقع المشترك الذي يبنيه الناس بأنفسهم عندما يتفاعلون مع بعضهم البعض. ويعتمد هذا المدخل على أسلوب التحليل المصغّر المتمثل فى الوحدات الصغرى (ميكرو)، وأشهر منظّريها جورج هربرت ميد، وإرفينغ غوفمان، كلارك وكورنيش. ومن هنا جمع هذا المقترح النظرى بين التحليل على مستوى الماكروسوسيولوجي و الميكروسوسيولوجي، وهو ما يعطى قوة ومرونة فى تحليل وتفسير الجرائم الرقمية، سواء من حيث ربطها بالبناء الاجتماعى، أو تفسيرها من خلال روتين وأنشطة وتفاعل الأفراد فى حياتهم اليومية.

ثالثا : القضايا النظرية

تم بناء هذا النموذج المقترح بعد عرض مجموعة من النظريات الكلاسيكية والمعاصرة، والتى تم تعديل إطارها النظرى ،واختبار فروضها النظرية من قبل مجموعة من العلماء المعاصرين – وهذا سبب اختيار هذه النظريات دون غيرها – ليكونا أكثر قدرة على تفسير الجرائم الرقمية. واشتملت هذه النظريات على نظرية (الاختيار العقلاني – النشاط الروتيني – الارتباط التفاضلى – التعلم الاجتماعى – الضغط البنيوى– التسمية ووضع العلامات – الانتقال فى الفضاء – تقنيات التحييد – منظور الايذاء – الضبط الاجتماعى). ويمكن استخلاص مجموعة من القضايا النظرية والتى يمكن أن تشكل إطارا تفسيريا لأسباب وقوع الجرائم الرقمية :

١. تسمح طبيعة الإنترنت بضمان إخفاء هوية الجناة، والوصول إلى مجموعة كبيرة من الأهداف المحتملة، لتحقيق مكاسب كبيرة للغاية. فزيادة التكلفة والعائد من تلك الجرائم، تكون أكثر من العواقب والخسائر، والتى تكون تكلفتها بسيطة إن حدثت. فالعائد المحتمل من الكسب المادى أو الانتقام والقصاص، أو اختبار المهارات الرقمية، وممارسة القوة على الآخرين، والإشباع الجنسي، يكون أكبر من احتمالية كشف المجرم وعقوبته بعقوبة ضعيفة. مما يؤكد أن طبيعة الانترنت والفضاء السيبرانى والادوات التكنولوجية، تمثل بيئة خصبة لارتكاب الجرائم الرقمية.

٢. يعود زيادة ارتكاب الجرائم الرقمية إلى حدوث أنشطة وسلوكيات روتينية لنمط حياة الفرد، تجعله ضحية لجريمة رقمية، مثل التواجد فى مكان يسمح بارتكاب الجريمة ضده، أو أن يصبح هدفا مناسبا ومتاحا، من خلال نشر بياناته

الشخصية أو المالية، كذلك عدم وجود وصي مناسب لمنع ارتكاب الجريمة، مثل أنظمة الحماية من الفيروسات، وضعف كلمات المرور، ومحدودية الرقابة الاسرية، وأخيرا وجود المجرم ذو الخلفية التقنية متزامنا مع دافع الثراء أو الانتقام أو اثبات الذات والقدرات.

٣. يرجع أسباب انتشار تلك الجرائم، إلى سهولة تعلم تكتيكات الاجرام الرقمى بالتعلم، والمشاهدة، والملاحظة، والتقليد عبر مواقع الانترنت، والمجموعات التى يتم انشائها على مواقع التواصل الاجتماعى لنشر ثقافة الجريمة الرقمية. كذلك يمكن تعلم طرق ارتكاب الجريمة الرقمية من خلال الارتباط أو مخالطة فرد، أو مجموعة ينخرطون فى ذلك السلوك المنحرف، سواء كان ذلك فى الفضاء المادى أو السيبرانى، مثل المنتديات المخصصة لاهتمامات التكنولوجيا أو الألعاب عبر الإنترنت؛ مما يكسب الشخص قيم ومعايير مؤيدة ومواتية للسلوك الإجرامي، كذلك يتعلم الشخص الموازنة بين المكافآت المتوقعة والخطورة المحتملة والعقوبات.

٤. يساهم الضغط الذي يمارسه البناء الاجتماعي على أفراده، من خلال عدم القدرة على تحقيق الأهداف المحددة ثقافيا مثل الثروة، بالوسائل المتاحة والمشروعة لتحقيق هذه الأهداف مثل التعليم والعمل، وإزالة المحفزات الايجابية من الفرد، وتعرضه لمجموعة من المحفزات السلبية، مما ينتج عنه ضغوط قد تدفع به إلى الجريمة الرقمية تحديدا لما يعتقد توفيرها للسرية فى إخفاء الهوية، وصعوبة تحديد المجرم، ومن ثم معاقبته .

٥. تعتبر الجريمة الرقمية من صنع المجتمع، نظرا للمسميات الاجرامية التى يطلقها أفراده على مجرمي الانترنت، والتى تمثل وصمة لهم، أو فى بعض الأحيان تصبح مصدر للتباهي والفخر، ودليل على الذكاء والمهارة الالكترونية، مثل مصطلح " الهاكرز"، فاولئك الذين يتم تصنيفهم على أنهم مجرمون يتبنون هذه التسمية، وبالتالي يسيئون التصرف وفقًا لكيفية فهمهم .

٦. سَهّل الفضاء السيبراني من ارتكاب الجرائم الرقمية، وتحديدا للأشخاص الذين لديهم سلوك إجرامى مكبوت داخل العالم الواقعى، ويمنعهم وضعهم الاجتماعي والاقتصادي والثقافي من ارتكاب جرائم تقليدية خوفاً من اكتشاف أمرهم، أو خوفا من العقوبة والردع .

٧. توفّر تقنيات التحييد والخاصة بتبرير السلوك الإجرامي الرقمى الفرصة لزيادة معدلات ارتكاب تلك الجرائم، فارتكاب الأشخاص لجرائم رقمية وعودتهم سريعا إلى إطارهم الاخلاقى المزين باحترام القانون، نابع من سهولة استخدامهم لتقنيات التحييد والتبرير، والمتمثلة فى إنكار المسئولية والضغوط الخارجية، كذلك إنكار الضرر بالضحية، أو أن الضحية تستحق ما ارتكب ضدها، أو أن جريمتهم ارتكبت من أجل الصالح العام، أو لمناصرة فئة أو لرفع الظلم طبقة بعينها .

٨. تحدث الجريمة الرقمية عندما يتم تخفيف الرقابة المجتمعية بسبب ضعف الروابط الاجتماعية، حيث يفتقر معظم مجرمو الانترنت إلى الروابط التقليدية فى المجتمع الواقعى، ويتم استبدالها بروابط اجتماعية افتراضية مستمدة من مواقع التواصل والشبكات الاجتماعية، والتى غالبا ما تضم أقران منحرفين.

رابعا: اشتقاق الفروض

تعد هذه العملية من أهم الخطوات الضرورية عند بناء أى نموذج نظرى، حيث يكون الهدف منها إعادة صياغة القضايا النظرية التى اشتمل عليها النموذج فى هيئة فروض جديدة، تحتاج مستقبلا إلى إثبات صدقها الامبريقى. ويشتمل " نموذج الجرائم الرقمية" على عدد من الفروض نذكر منها:

- لا توجد نظرية كلاسيكية أو معاصرة فى علم الاجتماع الجريمة قادرة على تفسير ظاهرة الجرائم الرقمية بشكل متكامل.
- يعتبر المجرم الرقمى أن العائد المحتمل من الجريمة الرقمية أكثر من خطورتها واحتمايه عقوبته.
- هناك العديد من الأنشطة الروتينية اليومية على شبكة الانترنت التى يمارسها أفراد المجتمع تجعلهم عرضة لأن يصبحوا ضحايا للجرائم الرقمية.
- من السهل تعلم طرق وتكتيكات ارتكاب الجريمة الرقمية من خلال مواقع أو مدونات شبكة الانترنت.
- يعتبر مخالطة الفرد للمجرم الرقمى سببا فى زيادة نسبة الجرائم الرقمية.
- يمارس البناء الاجتماعى ضغوطا بأشكال مختلفة على أفراد المجتمع، قد تتسبب فى سلوكهم طريق الجريمة الرقمية.
- تعتبر تسمية " الهاكرز" من المسميات الدالة على المجرم الرقمى والتى تدفع الاشخاص لتنمية مهاراتهم بشكل أكثر لارتكاب تلك النوع من الجرائم.
- لا توجد جريمة رقمية تحدث فى الفضاء السيبرانى إلا باستخدام مجرميها لتقنييات التحييد لتبرير سلوكهم.

## ثانيا: النتائج المجتمعية

١- كشفت الدراسة عن قصور النظريات التقليدية والمعاصرة فى مواكبة التقدم الحادث داخل المجتمعات، وتحديدا فى كشف خبايا المجتمع الرقمى وما يحدث به من جرائم مستحدثة، مع وجود ندرة فى الدراسات العربية والأبحاث العلمية التى تسعى لمعالجة مثل هذه الظاهرة الرقمية.

٢- يمثل نشر المعلومات الشخصية، وتنزيل الألعاب، ومقاطع الفيديو من مواقع الويب غير المعروفة، وتكوين صداقات مع الغرباء على صفحات مواقع التواصل الاجتماعي، من الأنشطة المحفوفة بالمخاطر عبر الإنترنت، والتى تعرض فاعلها إلى أن يصبح ضحية للجرائم الرقمية.

٣- يشكل الارتباط بأقران منحرفين، والذين يحملون تعريفات مواتية لارتكاب الجريمة، احتمالاً لارتكاب الجرائم الإلكترونية المتمثلة في المضايقات الإلكترونية والمطاردة وانتحال الهوية وإرسال الرسائل الجنسية .

٤- تمثل الدراسة الحالية أهمية للباحثين وصانعي السياسات لتحقيق مزيد من الفهم لنمط الحياة، والضغوط التى يمارسها البناء الاجتماعى على أفراده، والتى قد تساهم في ارتكاب الجرائم الرقمية، ومحاولة تغييره أو تجنبه؛ للحد من مخاطر هذه الجرائم، ومحاولة جعل بيئة الإنترنت مكانًا أكثر أمانًا للأفراد للمشاركة في أنشطتهم الروتينية اليومية، مثل الشبكات الاجتماعية والتواصل مع الآخرين والتعليم والعمل .

## التوصيات

- تؤثر الثورة الرقمية بشكل مباشر على حياة كل أفراد المجتمع، لذا يجب إجراء حوار مجتمعى، يشمل العلماء من جميع المجالات، وصناع القرار، وأيضًا المواطنين، حول التوعية بخطورة الجريمة الرقمية، خاصة مع تفشي الأمية التكنولوجية. مما يستوجب إجراء المزيد من الاستثمارات في مجال التعليم الرقمى، ونشر دورات التثقيف التكنولوجى، وتطوير مساحة مفتوحة للمناقشات حول التقنيات الرقمية، من أجل تحقيق الأمن المجتمعى والأمان الرقمى.

- ضرورة دراسة الفضاء السيبرانى وإنعكاساته على الشباب، لفهم ثقافتهم وقيمهم الجديدة المستمدة من ذلك العالم الرقمى، حيث بات جيل الشباب اليوم يطلق عليه " الجيل الرقمي"، نظرا إلى اعتماده الكبير على التكنولوجيا فى جميع أموره الحياتية، مع ضرورة توفير فرص عمل مشروعة تتيح للشباب أصحاب المهارات العالية فى استخدام التكنولوجيا، من عرض قدراتهم والاعتراف بها بطريقة توفر لهم فرص حياة أفضل، بدلاً من التحاقهم بمهن إجرامية؛ للحصول على الفوائد والمكاسب غير المشروعة.

- أهمية وجود إستراتيجية طويلة المدى ودمجها في المناهج المتعلقة بعلوم الكمبيوتر داخل المدارس والجامعات؛ تساعد في تعزيز ثقافة المسؤولية لسلوكيات الفرد على الإنترنت، وخاصة فى مواقع التواصل الاجتماعى ومجتمعات الألعاب عبر الفضاء الالكترونى، على غرار حملة (Stop.Think.Connect) التي قدمتها وزارة الدفاع الأمريكية، والتى تعتبر من أكثر الأساليب الواعدة للتثقيف في مجال مكافحة الجرائم الرقمية والوقاية منها. وتمثل الهدف منها إلى زيادة فهم التهديدات الإلكترونية وتمكين أفراد المجتمع ليكونوا أكثر أمانًا عبر الإنترنت. يشمل الجمهور المستهدف طلاب المدارس والجامعات وأولياء الأمور والمعلمين والمهنيين الشباب والشركات الصغيرة والمتخصصين في الصناعة والحكومة ورجال القانون وكبار السن. وتقدم الحملة خمس نصائح تتمثل فى: ١) حماية جميع الأجهزة المتصلة بالإنترنت، بما في ذلك أجهزة الكمبيوتر والهواتف الذكية وأنظمة الألعاب والأجهزة الأخرى التي تدعم الويب. ٢) الحفاظ على خصوصية أرقام الضمان الاجتماعي وأرقام الحسابات وكلمات المرور

والمعلومات الشخصية الأخرى. ٣) تعيين إعدادات الخصوصية الأمنية على مواقع الشبكات الاجتماعية. ٤) التحقق للتأكد من تمكين أمان الموقع باستخدام قبل استخدامه، وعند إجراء المعاملات المصرفية أو التسوق عبر الإنترنت. ٥) التفكير قبل التصرف أو كتابة أى منشور شخصى أو إرسال رسالة لشخص أو جهة ما، كذلك الحذر من الرسائل التي تطلب معلومات شخصية أو مالية.

– لا يوجد أمان كامل فى الفضاء السيبرانى، سواء للأفراد أو المؤسسات، والتي قد لا تمتلك المعرفة والمهارات اللازمة لتأمين أنظمتها بشكل مناسب. لذلك، يجب إمداد الشركات بالضوابط والاجراءات التي يمكنها تنفيذها، لتقليل الفرص الإجرامية وضمان اكتشاف الأنشطة الاحتيالية. من الهام أيضًا أن يكون هناك مزيد من التثقيف للضحايا المحتملين، لاسيما الأطفال وكبار السن الذين قد يتحولون إلى التكنولوجيا لأول مرة، وأولئك الأقل مهارة من الناحية التقنية. وذلك عن طريق حملات توعية مستمرة باستخدام مجموعة متنوعة من الوسائط الرقمية، للتأكد من أن الأفراد على دراية بكيفية استخدام بياناتهم، وتحذيرهم من أى نشاط الكترونى قد يعرضهم للخطر، وكيف يمكنهم حماية أنفسهم عبر الإنترنت.

– يجب على الباحثين والمتخصصين فى علم الاجتماع بفروعه المختلفه، اجراء المزيد من البحوث والدراسات حول النظريات الاجتماعية، للارتقاء بها وتحديث أطرها النظرية، وتوسيع نطاقها الامبريقى؛ من أجل مواكبة التطورات التى حدثت على مجتمعاتنا، والاتجاه بسرعة كبيرة نحو مزيد من الرقمنة.

– يجب أن تخضع نظريات الجريمة بشكل مستمر إلى التدقيق العلمى والتحديث، من خلال تطبيقها على الجرائم التي تحدث في الفضاء السيبراني وليس الواقعى فقط. بالإضافة إلى أهمية وجود إطار نظري حديث يأخذ في الاعتبار انسيابية وسرعة المجتمع الرقمي، والتغييرات التى تحدثها التقنيات التكنولوجية على كل من تنظيم الجريمة والمجرمين والضحايا. فضلاً عن الابتكارات التي يجلبها المجتمع الرقمي إلى العناصر الذاتية والموضوعية للجريمة .

– أهمية التجديد النظرى والمنهجى فى مجال سوسيولوجيا الجريمة، بما يتناسب مع طبيعة التحولات التى يعيشها مجتمعنا المعاصر، من التحول نحو الرقمنة، والاستخدام المكثف للانترنت، مع ضرورة إجراء مزيد من الدراسات والأبحاث حول الجرائم الرقمية، لتدعيم فرع علم الجريمة الرقمى؛ ليصبح أكثر تكاملا فى تفسير ومكافحة تلك الجرائم التى ترتكب فى نطاق المجتمع الرقمى.

**المراجع**


1. Andrea Di Nicola1, Towards digital organized crime and digital sociology of organized crime , Published 26 May 2022, https://doi.org/10.1007/s12117-022-09457-y

2. Carlo Ghezzi, Should We Rethink How We Do Research? Perspectives on Digital Humanism, Springer, Cham. 2022, https://doi.org/10.1007/978-3-030-86144-5_44

٣. موقع الاتحاد الدولي للاتصالات التابع للأمم المتحدة
https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use/

٤. https://mcit.gov.eg/ar/Digital_Government
موقع وزارة الاتصالات وتكنولوجيا المعلومات المصرية

٥. فرنسوا لسلي، نقولا ماكاريز، وسائل الاتصال المتعددة "ملتيميديا"، ترجمة : فؤاد شاهين، ط١، بيروت :عويدات للنشر والطباعة، ٢٠٠١، ص ٩ .

٦. ياس خضر البياتي، الإعلام الجديد (الدولة الافتراضية الجديدة)، ط١، عمان: دار البداية، ٢٠١٤، ص ١٠٠ .

٧. _____، الاتصال الرقمي: أمم صاعدة وأمم مندهشة، ط١، عمان: دار البداية، ٢٠١٤، ص ٣٥١.

٨. ريتشارد واطسون، عقول المستقبل (كيف يغير العصر الرقمي عقولنا، ولماذا نكترث، وما الذي في وسعنا)، ط١، ترجمة: عبد الحميد نحمد دابوه، القاهرة: المركز القومي للترجمة، ٢٠١٦، ص ١٥.

٩. على عبد الرازق جلبي، هانى خميس أحمد، العولمة والحياة اليومية، القاهرة، مكتبة الأنجلو المصرية،٢٠١١ ، ص ٤١.

10. Andrea Di Nicola1, Towards digital organized crime and digital sociology of organized crime ,op.cit.,p: ٢.

11. Greyson, Devon, et.al, Digital sociology and information science research, proceedings of the Association for Information Science and Technology, Vol 53, Issue 1, 27 December 2016, p.1–3. http://onlinelibrary.wiley.com/doi/10.1002/pra2.2016.14505301002/full .

12. Noortje Marres, Digital Sociology: The Reinvention of Social Research 1st Edition, Polity, 28May 2017. P 81.

13. Rakhmanova and, Pinkevich, Digital Crime Concept, Advances in Economics, Business and Management Research, 2nd International Scientific and Practical Conference “Modern

Management Trends . and the Digital Economy: from Regional Development to Global Economic Growth" . volume 138, MTDE 2020.

14. Stratton G, Powell A and Cameron R, Crime and Justice in Digital Society: Towards a 'Digital Criminology'? International Journal for Crime, Justice and Social Democracy 6(2). RMIT, Australia. 2017. p20.

15. Rakhmanova and, Pinkevich, Digital Crime Concept, Advances in Economics, Business and Management Research,op.cit.,p: 5

16. Kirwan G. Can, Theories of Crime be applied to Cybercriminal Acts? the Psychology of Cyber Crime: Concepts and Principles, Information Science Reference. 2012 .P 39.

17. Jildau Borwell, Jurjen Jansen and Wouter Stol , Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions, journal of digital social research, vol. 3, no. 3, 2021. P 67.

18. Elizabeth Phillips, Empirical Assessment of Lifestyle-Routine Activity and Social Learning theory on Cybercrime Offending. Bridgewater State University, In BSU Master's Theses and Projects. Item 25. 2015. Available at http://vc.bridgew.edu/theses/25

19. Bedford and others, A post-capitalocentric critique of digital technology and environmental harm: new directions at the intersection of digital and green criminology. International Journal for Crime, Justice and Social Democracy, 11(1). 2022. p 171.

20. Andrea Di Nicola1, Towards digital organized crime and digital sociology of organized crime ,op.cit.,p 4.

21. Jaishankar K. Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology,no 1, 2007. P 7.

22. Holt TJ and Bossler, Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses. New York: Routledge. 2015. P 21 .

23. Gavin J. D. Smith, Lyria Bennett Moses, Janet Chan, The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach, The British Journal of Criminology, Volume 57, Issue 2, 1 March 2017, P 259. https://doi.org/10.1093/bjc/azw096

24. Stratton G, Powell A and Cameron R, Crime and Justice in Digital Society: Towards a 'Digital Criminology' ,op.cit.,p: 25.

25. M. Yar, Crime, media and the will- to- representation: Reconsidering relationships in the new media age. Crime, Media, Culture 8(3). 2012. p 252.

26. Hayward KJ , Five spaces of cultural criminology. British Journal of Criminology 52(3). 2012. P 455.

27. Friday Wada and others, Action speaks louder than words – understanding cyber criminal behavior using criminological theories, journal of internet banking and commerce, https://www-icommercecentral-com. /action-speaks-louder-than-words-understanding-cyber-criminal-behavior-using-criminological-theories.php?aid=38083&_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=op,sc.

28. Hutchings, Alice, Theory and Crime: Does it Compute? School of Criminology and Criminal Justice, Griffith University, 2013. https://doi.org/10.25904/1912/2800

29. Bossler Adam M., Holt Thomas J., Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory, International Journal of Cyber Criminology (IJCC) , January-June Vol 3 (1), 2009. P 410.

30. Applying Criminological Theories to Cyber Crime, UKEssays.. Applying Criminological Theories to Cyber Crime. (November 2018) . Retrieved from https://www.ukessays.com/essays/criminology/explaining-cybercrime-using.php?vref=1

31. Elizabeth Phillips , Empirical Assessment of Lifestyle-Routine Activity and Social Learning theory on Cybercrime Offending. ,op.cit.

32. Hutchings, Alice, Theory and Crime: Does it Compute? ,op.cit.

33. Digital Crime Causes and Theories. Research Paper. Exclusively available on IvyPanda.Updated: Sep 21st, 2020.https://ivypanda-com.translate.goog/essays/digital-crime-causes-and-theories/?_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=op,sc

34. Thomas E. Dearden & Katalin Parti , Cybercrime, Differential Association, and Self-Control: Knowledge Transmission Through Online Social Learning, American Journal of Criminal Justice volume 46, p935.(2021)Cite this article: https://doi.org/10.1007/s12103-021-09655-4.

35. Robert G.Morris,'George E.Higgins, Criminological theory in the digital age: The case of social learning theory and digital piracy, Journal of Criminal Justice, Volume 38, Issue 4, July–August 2010, P 477.

36. Marcum, C.D., and others, (). Hacking in high school: Cybercrime perpetration by juveniles. Deviant Behavior, 35(7). 2014. P581. https://doi.org/10.1080/01639625.2013.867721

37. Thomas E. Dearden & Katalin Parti , Cybercrime, Differential Association, and Self-Control: Knowledge Transmission Through Online Social Learning, ,op.cit.

38. Brown Wyatt, "An Intersectional Approach to Criminological theory: Incorporating the Intersectionality of Race and Gender into Agnew's General Strain theory," Ralph Bunche Journal of Public Affairs: Vol. 4: Iss. 1, Article 6, 2015. p 233 Available at: http://digitalscholarship.tsu.edu/rbjpa/vol4/iss1/6

39. Sarah Lowman, Criminology of Computer Crime. May 2010 . https://silo.tips/download/criminology-of-computer-crime

40. Brown Wyatt, "An Intersectional Approach to Criminological theory: Incorporating the Intersectionality of Race and Gender into Agnew's General Strain theory,op.cit.,p: 240.

41. Applying Criminological Theories to Cyber Crime, UKEssays. (November 2018). Applying Criminological Theories to Cyber Crime. Retrieved from https://www.ukessays.com/essays/criminology/explaining-cybercrime-using.php?vref=1

42. Thomas E. Dearden, Katalin Parti, and James Hawdon, Institutional Anomie Theory and Cybercrime—Cybercrime and the American Dream, Journal of Contemporary Criminal Justice.2021. p 36.

43. Hutchings, Alice, Theory and Crime: Does it Compute? ,op.cit.,.

44. Brian K. Payne & Brittany Hawkins & Chunsheng Xin, Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes, American Journal of Criminal Justice, 4 October 2018, https://doi.org/10.1007/s12103-018-9457-3

45. K. Jaishankar, Establishing a Theory of Cyber Crimes,op.cit.,p: 29.

46. Thomas E. Dearden & Katalin Parti , Cybercrime, Differential Association, and Self-Control: Knowledge Transmission Through Online Social Learning,op.cit.,p: 41.

47. Volkan Topalli, The Seductive Nature of Autotelic Crime: How Neutralization Theory Serves as a Boundary Condition for Understanding Hardcore Street Offending, Sociological InquiryVolume 76, Issue 4Nov 2006.p 503.

48. Hutchings, Alice, Theory and Crime: Does it Compute? ,op.cit.p 9.

49. Ibid, p: 10.

50. Sheena Lewisa, and Dan A Lewis, Digitalizing Crime Prevention Theories: How Technology Affects Victim andOffender Behavior, International Journal of Criminology and Sociological Theory, Vol. 4, No. 2, December 2011, p 760.

51. Ibid, p 762.

52. ibid, p 765.