Journal Of the Iraqia University (73-7) May (2025)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

آليات الحد من جريمة الاحتيال الإلكتروني

م.م. أسراء حميد مجيد كلية العلوم السياحية
Mustansiriyah University
bezujax@gmail.com

المقدمة

احتياج العالم في العصر الحالي نوع جديد من الجرائم نتيجة للتقدم العملي، ولما صاحبه من نطور ونهضة ليس لها ما يشابه في جميع المجالات اليومية، والتي كان من أبرزها التقدم المُحدث في جريمة الاحتيال الالكتروني وبما يترتب عليه من إحداث ثورة تنموية بشرية على كافة المستويات، وعلى الصعيد المحلي والدولي؛ فقد استطاع الانسان رصد ومتابعة كل ما يحدث حوله في مختلف دول العالم منذ لحظة وقوعه.وكانت جريمة الاحتيال الالكتروني من الجرائم الخاصة بالأموال الماسة بالمجتمع من الجانب الاقتصادي، كون شيوعها يعمل على خلخلة الثقة بين الأفراد، كما يعمل على التشكيك في مصداقيتهم في التعامل خاصة في المجتمع العربي، لأنه يتصف بالمقومات الاجتماعية الطيبة التي يسهل من استخدامها لغرض الاحتيال عن طريق عدة من الوسائل الخاصة بالخداع والكذب، وهو ما يؤدي لوقوع الضحية المُحتال عليها.فلكون هذه الجريمة تؤثر على نمط الحياة فهو يحول دون استغلال الموارد المتاحة بشكل أمثل، نتيجة لزيادة نسبة جرائم الاحتيال داخل الوطن العربي بشكل عام، وبالمجتمع العراقي بشكل خاص، فكانت التشريعات العراقية من أولى التشريعات التي عرفت الجريمة الاحتيالية؛ فقد عرف العراق القديم ثلاث من الطوائف من القوانين القديمة المتمثلة في القوانين السومرية، والقوانين البابلية، والقوانين الآشورية، وبناءً على ما اقره مجلس النواب في العراق وطبقًا لأحكام البند (أولا) من المادة (٦١)، والبند (ثانيًا) من المادة (٧٣) من الدستور قرر رئيس الجمهورية بتاريخ (٣/ ٩/ ٢٠١٣م) بإصدار القانون رقم (٣١) لسنة ٢٠١٣م، بتصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

إشكالية البحث:

تتمثل إشكالية البحث في ان التطور التكنولوجي الخاص بأساليب ارتكاب الجريمة خاصة التي تتم من خلال الانترنت، ووسائل التواصل الاجتماعي، تكون في حاجة من قبل القانون على أن يتم التعامل مع هذه الجريمة والحد منها، فتكمن إشكالية البحث حول السؤال الرئيسي وهو كيف يتم الحد من جريمة الاحتيال الالكتروني؟

تساؤلات البحث:

يثير البحث عدة من التساؤلات التي تتمركز في:

-ماهية جريمة الاحتيال الإلكتروني؟

-ما هي الأسباب المتعلقة بإنشاء ضبطية جريمة الاحتيال الإلكتروني؟

-ما أهم الجهود الوطنية لمكافحة جريمة الاحتيال الإلكتروني؟

-ما أهم الحلول العملية الخاصة بمكافحة جريمة الاحتيال الإلكتروني؟

أهمية البحث:

الأهمية العلمية:

تكمن الأهمية العلمية للبحث في التعرف على ماهية جريمة الاحتيال الإلكترونية، وبيان الطبيعة القانونية لها من أجل تمييزها عن باقي الجرائم المتشابهة، وللتعرف على خصائصها، كما تكمن الأهمية في إيضاح الأسباب المتعلقة بضبطية جريمة الاحتيال الإلكتروني، وإيضاح أهم الحلول الخاصة بمكافحتها ليس فقط على المستوى المحلي بل والدولي أيضا.

-الأهمية العملية:

تكمن الأهمية العلمية لهذا البحث في إفادة أكبر قدر ممكن المجتمع، وإفادة الباحثين والدارسين كالرجوع إليه كأحد المراجع فيما يتعلق بآليات الحد من جريمة الاحتيال الإلكتروني، بالإضافة إلى وضع توصيات ومقترحات يمكن من خلالها إدراج المتغيرات المعاصرة التي تشدها الدولة العراقية.

أهداف البحث:

تتمثل أهداف البحث في:

- بيان ماهية الجريمة الإلكتروني، والطبيعة القانونية التي تتسم بها.التعرف على الأسباب الخاصة بإنشاء الضبطية لجريمة الاحتيال الإلكتروني.
- بيان الجهود التي قامت بها دولة العراق في مكافحة جريمة الاحتيال الإلكتروني.التعرف على الحلول العملية التي تحد من انتشار جريمة الاحتيال الإلكتروني.

منهجية البحث:

اعتمد الباحث على المنهج العلمي المتمثل في المنهج الوصفي عن طريق الرجوع للمصادر الأساسية للمعلومات، والقيام بجمع المعلومات والبيانات والوقائع الحقيقية المتعلقة بها، كما تم الاعتماد على المنهج التحليلي في تحليل النصوص القانونية تحليل قانوني دقيق.

الدراسات السابقة:

١. **قام (وائل محمد نصيرات)، بإجراء دراسة بعنوان (جريمة الاحتيال عبر شبكة المعلومات الدولية)، عام (٢٠١٨م)** [١]**اعتمدت الدراسة على المنهج** التحليلي وتفسير الانظمة والنصوص القانونية ذات الصلة بالموضوع، وبيان المبدأ القانوني الذي تقوم عليه.

هدفت الدراسة إلى: التعرف على جريمة الاحتيال التي تتم من خلال شبكة المعلومات الدولية، والملاعبة في البيانات والبرامج الالكترونية، ووسائل معالجتها، وللتطرق لمكافحة هذه الجريمة عبر شبكة المعلومات الدولية من خلال التشريعات الوطنية والدولية.

توصلت الدراسة إلى: ساعدت شبكة المعلومات الدولية الكثير من المجرمين على التخفي ورائها من أجل ممارسة افعالهم الجرمية، وهو ما يؤدي لصعوبة عمليات الملاحقة لهم، ولا يكفي القانون الجنائي التقليدي من حيث المبدأ لمواجهة هذا النوع من الإجرام المتمثل في الاحتيال عبر شبكة المعلومات الدولية.

٢. قام (حمد عبد الله حيي بو غانم السليطي)، بإجراء دراسة بعنوان (تجريم الاحتيال الالكتروني في القانون القطري)، عام (٢٠١٨م) [٢].

اعتمد الباحث على المنهج الاستقرائي التحليلي الذي يتم عن طريقه تحليل النصوص القانونية، كما اعتمد على المنهج المقارن في بعض القوانين، ودراسة الظواهر المتعلقة بالاحتيال الالكتروني كما هي موجودة على أرض الواقع، ووصفها وصف دقيق.

هدفت الدراسة إلى: إيضاح مفهوم جريمة الاحتيال الالكتروني، وبيان المسؤولية الواقعة على مرتكب هذا النوع من الجرائم الالكترونية، العمل على نشر الوعي لدى مختلف أفراد المجتمع.

توصلت الدراسة إلى: أن التطور الحادث للنظام المعلوماتي أدى لخلق نوع جديد من الجريمة الواقعة على حق الغير، كما تعد جريمة الاحتيال من الجرائم الواقعة على الأموال الماسة بحياة المجتمع.

التعليق الدراسات السابقة:

- **أوجه التشابه:** تتشابه الدراسة الحالية مع الدراسات السابقة في تطرق كلاهما إلى الإشكالية التي تسببها جريمة الاحتيال الالكتروني، والتأثير السلبي لها على أفراد المجتمع ليس فقط على الجانب المحلي، بل والدولي أيضا، كما أنهم متشابهون في استخدامهم للمنهج الوصفي التحليلي لوصف هذه الظاهرة وتحليل نصوصها القانونية تحليل دقيق.
- **أوجه الاختلاف:** تختلف الدراسة الحالية عن الدراسات السابقة في تطبيقها والاعتماد على نصوص القانون العراقي، فقد اعتمدت الدراسة الأولي على دراسة القانون المقارن بين السعودية والاردن، بينما اعتمدت الثانية على القانون القطري، كما تختلف الدراسة الحالية عنهم كونها لم تعتمد على المنهج المقارن على غير كلاهما.

خطة البحث:

المبحث الأول: ماهية جريمة الاحتيال الإلكتروني.

تُعد جريمة الاحتيال الإلكتروني جريمة يتم ارتكابها عبر شبكة المعلومات الدولية، وأنها تعد من أهم الجرائم المتطورة، والتي تختلق صورها تبعًا للتطور الاجتماعي والاقتصادي؛ حيث يتعتد مرتكب هذه الجريمة على مدى قابلية الناس للاقتناع تبعًا للظروف المحيطة بهم، وعليه يلجأ لعدة من الطرق والوسائل الاحتيالية التي توقع بهم في أخطاء مما يدفعهم لتسليم الأموال الخاصة بهم إلى الجاني طواعية واختيارًا دون أدنى مقاومة.

المطلب الأول: تعريف جريمة الاحتيال الإلكتروني وطبيعتها.

كثيرًا من الدول العربية لم تتناول تعريف لجريمة الاحتيال، سواء أن كان بالشكل التقليدي له، أو بالشكل الإلكتروني في القوانين العقابية، بل ترك الأمر للتقدير الفقهاء.

الفرع الأول: تعريف جريمة الاحتيال الإلكتروني.يوجد الكثير من التشريعات العربية التي لم تضع تعريف خاص بجريمة الاحتيال الالكتروني سوى بالشكل التقليدي له في القوانين العقابية وترك الامر للفقهاء، وهذا يوضح لنا أن صياغة التعريف لا تعد من المهام التي يقوم بها المنظم، بل انها من اختصاصات الفقهاء.فهناك مجموعة من الفقهاء الذين عرفوا الاحتيال المعلوماتي على أنه تلاعب عمدي بالبيانات وبالمعلومات التي تمثل قيمة مادية مختونة في النظام الحاسب الآلي، أو الإدخال الغير مصرح به لمعلومات وبيانات صحيحة، أو التلاعب في بعض الأوامر والتعليمات المتحكمة في عملية البرمجة، أو بأي وسيلة أخرى يمكن من شأنها التأثير على الحاسب الآلي من أجل القيام بعملياته على هذه الأوامر والبيانات، ولأجل الحصول على الربح الغير مشروع، ولإلحاق الضرر بالغير [٣].وذهب البعض الآخر لتعريفه على أنه استعمال ليس مصرح به للنظام الخاص بالحاسب الآلي بهدف الحصول على أي من الممتلكات، أو الخدمات من خلال الاحتيال.ويتبين من خلال التعريفات السابقة أنه قد يكون العمل المُرتكب ليس بمشروع قد يكون عن طريق استخدام وسائل احتيالية، أو بتغيير حقيقة البيانات، أو اختلاس البيانات وتخريبها، أو الدخول الغير مصرح به لموقع خاص، وهناك احتمالية حول هذا الفعل الغير مصرح به ضد نظام حاسب آلي أخر مثل تخريب البيانات الخاصة به، أو قد يكون متعلق بذات النظام للحاسب الآلي مثل استخدام وتقديم خدمة وهمية على سبيل المثال.

الفرع الثاني: طبيعة جريمة الاحتيال الالكتروني.

لا تتوقف جريمة الاحتيال الواقعة على العمليات الالكتروني عن طريق استخدام الطرق الإلكترونية الحديثة، والخاصة بالأفعال التي المُحققة بهذه الجريمة، بل انها تكون ممتدة حتى تشمل البعد العالمي لهذا النوع من الجريمة، فأن كانت شبكة الاتصالات من بعد ذات نطاق عالمي غير مقيد بحدود محددة، وعليه تتميز الجرائم الواقعة عليه مما يمكن أي من الأشخاص في أي دولة من دول العالم الدخول لشبكة المعلومات الدولية، وأنه من الممكن لأي من الأشخاص ارتكاب نشاطه الإجرامي في دولة واحدة، أو عدة من الدول الاخرى.كما تتسم طبيعة هذه الجرائم بأن من يرتكبو مثل هذه الجرائم هم فئة محددة من المجرمين متميزين بعدة من الصفات الخاصة، فهم أفراد يتمتعون بالسلطة في التعامل مع المعلومات تلك التي يحتوي عليها نظام الحاسب الآلي، الأمر الذي يستوي إن كان هذا في مرحلة إدخال البيانات، أو إخراجها، أو التعامل معها بعد إتمام التخزين، ويمكنهم التلاعب بهذه البيانات وتحويلها لربح مادي غير مصرح به.هذا وبالإضافة إلى أنه تحتاج الجريمة الاحتيالية الواقعة على العمليات الالكترونية عن طريق استخدام الوسائل الالكترونية لتأهيل فني وعلمي خاص لا بد من تواجده في كافة الأفراد من تتصل أيديهم بتلك الجرائم بداية نم مرحلة التحري، وجمع الاستدلالات، مرورًا بمرحلة التحقيق الابتدائي، والانتهاء بمرحلة المحاكمة [٤].وعلى هذا فان هذا النوع من الجريمة يتسم بطبيعة فنية معقدة من الممكن ان يخلف ورآه آثار تكشف عنه، وانه يكون محتاج للكشف عنه ووصول مرتكبيه لخبرة معينة فكلًا من يتصلوا بهذه الجريمة كرجال الشرطة، والأشخاص أصحاب سلطة الادعاء، وقضاء الحكم.

المطلب الثاني: خصائص الجريمة الالكترونية.

تُعد جريمة الاحتيال الإلكتروني من الجرائم الإنترنت التي تتم من خلال الشبكة المعلوماتية، وباستخدام جهاز الحاسب الآلي، فهي تتسم بعدة من الخصائص التي يمكن حصرها في:

الفرع الأول: خصائص موضوعية تتعلق بموضوع الجريمة والطريقة المستخدمة.

١. **الأداة المستخدمة في الجريمة الاحتيالية متمثلة في الشبكة المعلوماتية، والحاسب الآلي.**يتمكن الجاني من خلال استخدام الشبكة المعلوماتية والحاسب الآلي ارتكاب مختلف الجرائم خاصة تلك الجرائم التي تتعلق بالاحتيال، فغالبًا ما تعد هي حجر الاساس في ارتكاب الجريمة، فهي جريمة فردية؛ حيث يتمكن الشخص من الدخول على الانترنت، وتسهيل القيام بتنفيذ هذه الجريمة [٥].

٢. **جريمة عابرة للحدود.**تُعد جريمة الاحتيال الالكتروني من الجرائم الدولية كونها عابرة للحدود؛ حيث أُلغت الشبكة المعلوماتية الحدود الجغرافية الفاصلة بين الدول، فكان من السهل التحدث المتبادل بين الأشخاص من مختلف الدول، فهي تتخطى حدود الدول المُرتكبة فيها لتنتج آثارها لمختلف البلاد على المستوى الدولي [٦].

٣. **الشبكة المعلوماتية حلقة الوصل للجريمة الالكترونية.**تُرتكب جريمة الاحتيال الالكتروني عبر استخدام شبكة الانترنت، فهي حلقة الوصل بين جميع الأهداف المحتمل حدوثها لهذه الجرائم مثل: البنوك والشركات الصناعية إلى غير ذلك من الأهداف المتمثلة في الغالب بالضحايا، وهو

ما جعل كثير من هؤلاء الضحايا اللجوء لوضع أنظمة امنية إلكترونية من أجل عدم اختراق مواقعهم، والحد من الخسائر الكبيرة الناتجة عن الاختراق وحدوث جريمة الاحتيال [٧].

الفرع الثاني: خصائص شخصية تتعلق بشخصية الجاني.

١. جريمة الاحتيال الالكتروني شأنها شأن الجريمة المعلوماتية.يُمكن أن يكون الجناة من قبل الأشخاص المسرح لهم باستخدام الحاسب الآلي والدخول لنظامه، فأنه كثير ما يكون الجناة مرتكبي جريمة الاحتيال الالكتروني، واختلاس الأموال العامة من داخل الجهات المجني عليها؛ حيث يوجد علاقة بين مرتكب الجريمة وبين الجاهات المجني عليها المن يباشرون في إطار الأعمال الاحتيالية لهم، بالإضافة لمونه يتسمون بعدم وجود أي من السوابق الإجرامية لكونهم يشغلون مناصب في المؤسسة الضحية، وهو ما يتطلب وجود الثقة والمسؤولية في أصحابها.

٢. **صغر سن مرتكب الاحتيال الالكتروني.**غالبًا ما يكون مرتكب جريمة الانترنت من فئة صغار السن من بعد سن (الثامنة عشر)، وتُعد النسب الأكبر للذكور من مرتكبي الجريمة الاحتيالية، وهو غالبًا ما يرجع بشكل أساسي للتفوق العددي لمن هم عاملين في هذا المجال.

٣. **الخبرة العلمية والعملية لمرتكب جريمة الاحتيال الالكتروني.**يتسم الكثير من مرتكب جريمة الاحتيال الالكتروني بالخبرة العلمية الفائقة في مجال الحاسب الآلي من أجل ارتكاب الجريمة عبر استخدام الانترنت، فلا بد من أن يكون مستخدم الحاسب الآلي على دراية كافية تمكنه بتنفيذ جريمته، والقيام على عدم اكتشافها، وعلى هذا كان كثيرًا من مرتكبي هذه الجريمة من الخبراء في مجال التقنية والحاسب الآلي؛ حيث تبحث الجهات الأمنية بشكل مستمر عن الخبراء في مجال الحاسب الآلي حالة وقوع جريمة إلكتروني [٨].

٤. **تحقيق الربح الغير مشروع.**يُعد الهدف من ارتكاب الجريمة الإلكترونية في أغلب الجرائم من أجل تحقيق ربح غير مشروع، أما لأجل الرغبة في إظهار المهارات الفنية، وهي تعد واحدة من البواعث على ارتكاب جريمة الاحتيال الإلكتروني، وبناًء عليه يكون لمرتكبي هذه الجرائم سلطة في التعامل مع المعلومات التي يحتوي عليها نظام الحاسب الآلي، الأمر الذي يستوي أن كان في مرحلة إدخال البيانات، أو إخراجها، أو التعامل معها بعد التخزين، وهو متمكنون في تحويل هذه البيانات والمعلومات لربح مادي غير مشروع.

المبحث الثاني: أسباب إنشاء ضبطية تتعلق بالجرائم الإلكترونية.

اعتاد أعضاء الضبطية القضائية البحث والتحقيق في الجرائم العادية التي تحدث في الواقع المادي، والانتقال إلى مسرح الجريمة، والبحث عن الأدلة، وتخمين مرتكب الجريمة، والاعتقال والتحقيق، حتى ظهور الجرائم الإلكترونية، وهي عملية تتطلب التحضير والمهارات البدنية في المقام الأول.وهي تختلف تماما عن الجرائم التقليدية من حيث كيفية حدوثها وعواقبها والوسائل المستخدمة لارتكابها، لذلك حدثت حالة طارئة في هيئات الإدارة القضائية والتحقيقية، وتم رفع الأصوات لإنشاء جهاز خاص للدراسة والتحقيق في مثل هذه الجرائم والتي لا تعتمد على التدريب البدني والفسيولوجي، بل على مستويات عملية وفكرية معينة ومهارات خاصة في مجال الاتصال والإنترنت، حتى يتمكن المحققون من التحقيق والتخمين في العالم الافتراضي ومطاردة المجرمين في البيئة الإلكترونية. [٩]

المطلب الأول: حداثة الجرائم الإلكترونية.

وبما أن معظم القوانين لم تنص على وجود سلطات قضائية مختصة بالتحقيق في الجرائم الإلكترونية والحكم عليها، فإن اختصاص النظر في هذه القضايا يعود إلى القضاء العادي للجانب الجنائي، لذلك يصعب الحكم على مثل هذه الجرائم بسبب الافتقار إلى الخبرة العلمية والتقنية والخبرة القضائية في هذا المجال، ولكن القانون يسمح للقضاة باستخدام خبراتهم لتحديد ملابسات القضية والوصول إلى الحقيقة ساهمت تجربة القاضي وإحاطته بوقائع القضية وبياناتها في كشف الحقيقة.**أعضاء ضبطية غير الجاهزين في مواجهة المجرمين:**يعود الاختصاص في البحث والتحري في الجرائم الإلكترونية إلى أعضاء الضبطية القضائية، المشار إليها في القانون، ونقص الخبرة في مجال عالم الكمبيوتر والإنترنت والمعاملات الإلكترونية، والأطراف الأخرى هي قراصنة احتيالية من ذوي المهارات العالية الذين يلحقون بكل ما هو جديد في عالم المعلوماتية والاتصالات. [١٠]بناءً على المثل القائل بأن فاقد الشيء لا يعطيه، يستحيل على ضابط شرطة عادي البحث عن الجرائم الإلكترونية والتحقيق فيها والتعامل مع الجناة، لذلك، لا مفر من السعي إلى وجود مؤسسات متخصصة لهذا النوع من الجرائم، أو العمل على تطوير خبرات ومهارات المخولين بالبحث عنها والتحقيق فيها، وكذلك تطوير مناهج تدريبية مدروسة جيدا للتحقيق وإثبات هذا النوع من الجرائم، مع مراعاة خصوصيات التطور التكنولوجي السريع في مجال الاتصالات، دون إهمال التعاون الدولي في مثل هذه الحالات.

وتكون موصفات المجرم الإلكتروني:

١. **مجرم متخصص**.غالبا ما يتبين أن العديد من المجرمين يرتكبون جرائم الكمبيوتر فقط، أي أنهم متخصصون في هذا النوع من الجرائم، لا علاقة لهم بأنواع أخرى من الجرائم التقليدية.

٢. **مجرم عائد إلى الإجرام**.يعود العديد من مجرمي المعلومات، بدافع الرغبة في سد الثغرات التي أدت إلى تحديد الهوية، يعودون إلى ارتكاب جرائم أخرى في مجال الكمبيوتر ويتم تقديمهم للمحاكمة آخر مرة، وهذا يؤدي إلى العودة إلى الجريمة ويمكن أيضا تقديمهم للمحاكمة في المرة القادمة.

٣. **مجرم محترف**.يتمتع المجرم الإلكتروني باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

٤. **مجرم غير عنيف**.مجرمو الإنترنت هم مجرمون لا يلجؤون إلى العنف في ارتكاب الجرائم، لأنه ينتمي إلى جريمة خدعة، وهذا النوع من الجرائم لا يتطلب أي جهد للقيام به.بالإضافة إلى ما سبق، فإن مجرمي الإنترنت هم مجرمون أذكياء ويتمتعون بالتكيف الاجتماعي، ولديهم المهارات والمعرفة وغالبا ما تكون ثقافة متقدمة.

المطلب الثاني: جرائم معقدة ولا حدود لمسرح الجريمة.

الجرائم الإلكترونية متميزة عن الجرائم العادية:

من أهم العوامل التي تدعو إلى إنشاء مؤسسات متخصصة للجرائم الإلكترونية الطبيعة المميزة لهذه الجرائم، لأنها جرائم تحدث في بيئة افتراضية ولا تترك أي آثار مادية، كما في حالة الجرائم العادية، من بين الميزات والميزات.

١. **الجريمة الإلكترونية جريمة عابرة للحدود**:هائلة على نقل كميات كبيرة من المعلومات وتبادلها بين الأنظمة على بعد آلاف الأميال، مما يؤدي إلى استنتاج أن مواقع متعددة في بلدان مختلفة يمكن أن تتأثر بالجريمة السيبرانية في وقت واحد، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود. [١١]بعد ظهور شبكات المعلومات، لا توجد قيود واضحة أو محددة على نقل المعلومات بين البلدان المختلفة، أدت قدرة أجهزة الكمبيوتر وشبكاتها على نقل كميات كبيرة من المعلومات وتبادلها بين الأنظمة على بعد آلاف الأميال إلى استنتاج مفاده أن مواقع متعددة في بلدان مختلفة يمكن أن تتأثر في وقت واحد بجرائم الإنترنت، تتيح لك سهولة نقل المعلومات بواسطة الأنظمة التكنولوجية الحديثة ارتكاب جريمة من خلال جهاز كمبيوتر موجود في بلد ما، بينما يتم تحقيق عمل إجرامي في بلد آخر.تثير طبيعة الجريمة السيبرانية، التي تتميز بأنها جريمة عابرة الحدود، العديد من القضايا فيما يتعلق بتحديد البلد الذي له ولاية قضائية على هذه الجريمة، وتحديد القانون الواجب التطبيق، والقضايا المتعلقة بإجراءات المقاضاة، وغيرها من النقاط التي تثيرها الجريمة عبر الوطنية بشكل عام.كان الحادث، الذي أطلق عليه اسم نقص المناعة المكتسب (الإيدز)، أحد الحوادث التي لفتت الانتباه إلى الجانب الدولي للجرائم الإلكترونية، وحقيقة هذا الحادث، الذي حدث لمدة عام، تتلخص في حقيقة أن شخصا واحدا وزع نسخا عديدة من برنامج إطلاق النار يهدف إلى تقديم المشورة بشأن نقص المناعة المكتسب. [١٢]ومع ذلك، احتوى البرنامج بالفعل على فيروس طروادة، أدى تشغيله إلى إيقاف تشغيل الكمبيوتر، وظهرت عبارة على الشاشة تطلب مبلغ المال الذي يمكن للممثل إرساله إلى عنوان معين، حتى يتمكن الضحية من الحصول على مضاد للفيروسات، وف الثالث من فبراير تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستر بسبب حالته العقلية ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:

أولا: إنها المرة الأولى التي يتم فيها تسليم شخص مهم لارتكابه جريمة معلومات.

ثانيا: هذه هي المرة الأولى التي يتم فيها محاكمة شخص لإعداد برنامج ضار.

٢. **صعوبة إثبات الجريمة الإلكترونية**.من الصعوبات العملية التي تواجه المحققين أن الجريمة الإلكترونية لا تترك أي آثار واضحة وأن الخبراء أو الخبراء فقط هم من يمكنهم اكتشافها وتتبعها وإثباتها، والسبب في صعوبة إثبات هذه الجرائم هو أن الجاني يوقظ آثارها والآثار التي وجدها K فاكتشاف الجريمة المعلوماتية أمر ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب. [١٣]فالجرائم الإلكترونية تحدث في بيئات غير تقليدية تقع خارج إطار الواقع المادي الملموس لجعل أركانها في بيئات الكمبيوتر والإنترنت، مما يجعل الأمور أكثر تعقيدا للسلطات الأمنية ووكالات التحقيق والادعاء، في هذه البيئة، وتكون البيانات والمعلومات عبارة

عن نبضات إلكترونية غير مرئية تتدفق عبر نظام المعلومات، مما يجعل من السهل جدا محو الأدلة ومحوها تماما من قبل الممثل.ففي إحدى الحالات التي شهدتها ألمانيا أدخل أحد الجناة في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا تم اختراقه من قبل الغير.

المبحث الثالث: مواجهة الأضرار الناتجة عن جريمة الاحتيال الإلكترونية.

سوف نتناول في هذا المبحث اهم الحلول العملية والعلمية فيما هو متعلق ببعض من الاجراءات الخاصة بالضبط والتفتيش والآليات التي من خلالها تحد من جريمة الاحتيال الالكتروني على النحو التالي:

المطلب الأول: الحلول العلمية في مكافحة جريمة الاحتيال الإلكتروني.

هناك مجموعة من الحلول العملية فيما هو متعلق ببعض من الاجراءات المتعلقة بمكافحة جريمة الاحتيال الالكتروني فيطرح الفقه مجموعة من الحلول العملية لمكافحة التحديات والاشكاليات المتعلقة بالجريمة الالكترونية وهي:

١. يلزم اتخاذ عدة من وسائل الحيطة والحذر في مجال التعامل مع البنوط بالأنشطة المصرفية تلك التي تتم من خلال استعمال الانترنت، والسبب في ذلك كون تركيز غاسلي الأموال يتم على هذه البنوك، ويكون بهذه الطرق كونها مرتعًا خصب لتجارتهم خاصة إن كانت هناك عجز في النظام الرقابي العام للدول التي ترعى هذه البنوك [١٤].

٢. أن يتم إصدار مجموعة من القواعد القانونية الصارمة التي تلزم كافة البنوك بوضع خطوات عملية ضرورية من اجل منع غسيل الأموال خصوصًا الأموال التي يتم التعامل بها من خلال الانترنت.

٣. ضرورة قيام المصارف باتخاذ تدابير عملية يكون من شأنها الكشف عن أي من المحاولات التي تتم بها عملية غسيل الأموال، ومراقبة كافة التعاملات الالكترونية.

٤. أن تقوم البنوك بإنشاء أجهزة وإدارات خاصة تتولى مهمة مراقبة ومتابعة البلاغات تلك التي تصلها عن أي من العمليات، أو الأنشطة المشبوهة مما يترتب عليه الابلاغ عنها للجهة المختصة في الدولة، خاصة وان كانت هذه العمليات المصرفية متعلقة بالأنشطة التي تتم من خلال الانترنت.

٥. لا بد من ضرورة تدريب العاملين في المباحث الجنائية في القيام بتفحص الادلة الالكترونية.

٦. ضرورة تدريب المحققين للقيام بالكشف عما تحتوى عليه أجهزة الحواسب الالية من برامج وبيانات مخزنة عند الحاجة، وهو ما يساهم في تيسير عمليات التفتيش تلك التي تتم على الحاسب الآلي للمتهم.

٧. الاستعانة بالخبراء في الحاسب الآلي، وفي الشبكات العالمية (الانترنت) خلال عمليات التقصي، والتحقيق في الجرائم الالكترونية [١٥].

المطلب الثاني: الحلول العملية في مكافحة جريمة الاحتيال الإلكتروني.

الحلول العلمية فيما يتعلق بضبط وتفتيش الأليات التي تنفذ من خلال الجريمة الإلكترونية.حيث سعاد الانتشار الكبير للإنترنت الحياة العملية الحاجة إلى الحلول العلمية للمشاكل التي تنتج عن استخدام الأنترنت في ضوء القواعد العامة للقانون، أيضا بالنظر إلى توجه المشرع للتدخل لوضع قواعد خاصة لتنظيم استخدام الأنترنت وذلك في بعض المجالات الحيوية، واستخلاص القواعد الرئيسية في هذا المجال، والتي تساعد المشرع إذا ما أراد يوما تنظيم مجال أو أكثر من مجالات استخدام الإنترنت بقواعد خاصة كالإثبات وبيان الأحكام القانونية لاستخدام الإنترنت في العديد من المجالات.ويوضح أيضا أن شركة مكافئ والتي تختص في تقنيات حماية الأنظمة الخاصة بالمعلومات أعلنت النتائج التي توصلت إليها، أخر الأبحاث، والتي أثبتت أن الجريمة الإلكترونية تعمل على إغواء الجيل الجديد من مستخدمي الكمبيوتر لتنفيذ الجرائم الشبكية المدهشة، وذلك باستخدام تكتيكات تشبه تكتيكات الكي جي بي، المخابرات الروسية لتجنيد العملاء وذلك خلال الحرب الباردة.حيث أظهر تقرير مكافئ السنوي حول الأنترنت والجريمة، والذي يعتمد على النتائج التي توصلت إليها أهم وحدات مكافحة الجرائم التقننية الرفيعة، حيث أصبحت عصابات الجريمة المنظمة تستهدف أوائل طلبة المعاهد الأكاديمية لكي يحصلوا على المهارات التي تسمح لهم بتنفيذ جرائمهم الجديدة ذات التقنية الرفيعة.كما أوضحت الدراسة أيضا أن المراهقين الماهرين في استخدام الإنترنت والتي تتجاوز أعمارهم الرابعة عشرة حيث صاروا ينجذبون إلى الجرائم الخاصة بالشبكة العالمية وذلك نتيجة الصيت الواسع الذي يحصل عليه مجرمو التقننية الرفيعة، وأيضا إمكانية اكتساب بعض المال وذلك دون التعرض لمخاطر الجرائم التقليدية.ويوضح التقرير أيضا أن مجرمي الشبكة العالمية بدأوا يغادرون أماكنهم الخاصة إلى الأماكن العامة، كمقاهي المزودة بشبكات الواي فاي ومن النتائج الأخرى التي توصل إليها تقرير مكافحي حول الجريمة في العالم الافتراضي.

١. الأساليب الجديدة لتطوير البرامج الضارة حيث أصبحت جماعات الجريمة المنظمة تلجأ إلى أساليب تشبه أساليب الكي جي بي، لاستقطاب الأجيال الجديدة لكتابة البرامج الضارة.

٢. جرائم داخلية، من خلال استغلال ضعف الإجراءات الأمنية في الشركات، أصبح الموظفون الحاليون والمتعاملون مع الشركة من أكثر ما ينظم عمليات الهجوم على شبكات الشركة والتسلل إليها. [١٦]بل أصبح مجرمو الشبكة العالمية يتوجهون إلى الخريجين الجدد وتجنيدهم لكي يستفيدوا من المعرفة الداخلية بشبكات الشركات التي سيعملون بها، كما يوضح التقرير أيضا إمكانات التسلل وإخفاء الهوية التي يمكن أن تقديمها بيئة الشبكة العالمية، وكيف أن أصبح كشف هويات المجرمين أمرا في غاية الصعوبة على هيئات تطبيق القانون، كما دجاء في التقرير القائمة الأتية والتي تشمل علي أخطر التهديدات والأدوات التي تستكشفها عصابات الجريمة المنظمة وهي كالاتي:

– الألعاب الذهنية: وفيها يزداد توجه مجرمو الشبكة العالمية إلى أساليب الحرب النفسية للوصول إلى مساعيهم، كما أرتفع حجم رسائل سرقة المعلومات الشخصية، وذلك بنسبة ٢٥٪ خلال العام الماضي، ومع مرور الوقت يكون من الصعب كشفها ويزيد أعداد الأشخاص الذين تنجح في خدعاهم، وذلك من خلال اللجوء إلى قصص واقعية بدلا من الوعود الخلابة التي لا يصدقها أي شخص، كالفوز بملايين الدولارات.

– الحيل الاجتماعية: مجرمي الشبكات العالمية تجذبهم التجمعات الكبيرة في الشبكات الاجتماعية، فيملون هوياتهم وصفحاتهم المزيفة بالبرامج الإعلامية حتى تصبح مؤلفو البرامج الضارة يقبضون ثمن شعبيتهم، وأيضا جمع المعلومات الشخصية عبر الإنترنت ليخلقوا لأنفسهم هوية ثانية مزيفة يستخدمونها في الأغراض السيئة.

– تسرب البيانات: حيث أن كثيرا من البيانات تكون مكشوفة ولا يتطلب الاستلاء عليها أساليب معقدة، فانتشار استخدام كلمات السر في مواقع الشراء قد جعل من التخمين كافيا ليفتح الباب الموصد، وفيما يتعلق بأجهزة تخزين البيانات الغير محمية كأصبح اليو أس بي، فهي التي تفتح الباب أمام نقل المعلومات بسهولة ويسر، وأدي أيضا تقارب التقنيات إلى مضاعفة التهديدات وجعل أنظمة الحماية لا تقوم بمهمتها.

– المستقبل: حيث ركز التقرير على التهديدات التي من خلالها يمكن أن تنتشر خلال السنة القادمة، حيث جعلت الهواتف الذكية والكمبيوترات المحمولة سبب من السباب الأساسية في الحياة العصرية، ومن المتوقع أن تزيد جهود مجرمي الشبكات العالمية، وذلك للاستخلاص المعلومات ذات القيمة الثمينة خلال الأشهر المقبلة.أما ما يتعلق بالانتشار المتواصل لتقنيات البلوتوث والاتصالات الهاتفية، سوف يؤدي إلى ظاهرة جديدة من التسلل إلى الشبكات الهاتفية. [١٧]لكن هذه الحلول العلمية في نطاق التفتيش تتناقض مع القواعد التي يقررها القانون، في ظل ضمانات احترام حقوق الإنسان والحريات الفردية، فمثل هذه الإجراءات من الممكن أن تؤدي إلي كشف البيانات الشخصية أو كشف الأسرار الخاصة بالعمل أو أن تصل إلى ملفات يكون أصحابها حرصين كل الحرص على سريتها أو أن يتيح لهم القانون ذلك.وتصبح المسألة أكثر خطورة عندما يمتد التفتيش إلي نظم مرتبطة بالنظام الخاص بموضوع الاشتباه، فتطال ملفات وبيانات الجهات التي لا علاقة لها بالجريمة والتي من الممكن أن تكون خاضعة لسرية المهنة أو قواعد حماية سرية بيانات العملاء.كما في حالات نظم الكمبيوتر الخاصة بمزودي الخدمات أو نظم كمبيوترات البنوك أو الشركات التي تتعاطي البيع عن طريق الإنترنت.وبعد العرض السابق يري الباحث أن الوقاية من إشكاليات الجرائم الإلكترونية خير من العلاج لذلك يكون من الأفضل لمستخدمي الوسائل الإلكترونية بجميع أشكالها أن يحصنوا أجهزتهم ضد هذه الجرائم، وأقترح عدد من الطرق لذلك وهي:

١. على المستخدم أن يجتنب إرسال الصور الخاصة به للغرباء لتجنب حوادث سوء استخدام هذه الصور.

٢. الامتناع عن كشف المعلومات الشخصية للغرباء مثل رقم الهوية ورقم الضمان الاجتماعي ورقم الحساب البنكي.

٣. استخدام أحدث البرامج المضادة للفيروسات.

٤. الامتناع عن إرسال الرقم الخاص ببطاقة الائتمان على أي موقع غير مضمون.

٥. الاحتفاظ بنسخة احتياطية للبيانات الموجودة في الجهاز لحفظه من الفقدان نتجه لتعرض هجومي عليه.

٦. على أصحاب المواقع مراقبة مواقعهم باستمرار والتحقق من المخالفات وتثبيت برامج تكشف الحركات الغير طبيعية للموقع.

٧. متابعة الأطفال عند استخدامهم شبكة الإنترنت لمنع أي نوع من التحرشات أو المضايقات. [١٨]

الخاتمة

ومن خلال ما تم تناوله يتضح لنا أن الجريمة الالكترونية كان يعد الجانب السلبي للتطور العلمي والتقني المستمر وهو ما أدى لزيادة خطورة مثل هذا النوع من الجرائم على المجتمع، كما قد توصلنا لعدة من النتائج والمقترحات على النحو التالي:

النتائج:

- أنه للقضاء على جريمة الاحتيال الالكتروني يتطلب تكاتف الجهود من أجل العمل على مكافحة هذا النوع من الجرائم من اجل القضاء عليها والحد منها.
- تمثل هذه الجريمة انتهاك واضح لحقوق الأفراد وخصوصياتهم، وكذلك الحقوق السياسية والاجتماعية والاقتصادية والامنية للدولة، بالإضافة لكونها تتعدى على كافة المعاملات التي تتم من خلال شبكة الانترنت خاصة التحويلات التجارية.
- وفقًا لحداثة جريمة الاحتيال الالكترونية فأن هناك تقصير من ناحية الاطار التشريعي، كما أن هناك ندرة فيما يتعلق بالأحكام القضائية الخاصة بهذا النوع من الجرائم.

التوصيات:

- تشجيع البحث العلمي على دراسة جريمة الاحتيال الالكتروني؛ كونه يملك القدرة على المساهمة في إنشاء قاعدة من البيانات الصالحة حتى تكون الأساس لانطلاق البرامج الوقائية.
- دعم قدرات الاجهزة "القضائية والأمنية" عن طريق التوسع في المعرفة بهذا النوع من الجرائم، وبطريقة التحقيق فيها وجمع المعلومات الكافية عنها ومكافحتها.
- ضرورة نشر الوعي بين المواطنين فيما يتعلق بخطورة هذا النوع من الجرائم، وبطرق الوقاية منها، والعمل على تفعيل دور المؤسسات المحلية والدولية.

قائمة المصادر والمراجع

-وائل محمد نصيرات، جريمة الاحتيال عبر شبكة المعلومات الدولية، ع ١٩، مجلة دفاتر السياسة والقانون، المملكة العربية السعودية، ٢٠١٨م.

-سامر سليمان عبد الجبوري، جريمة الاحتيال الإلكتروني، كلية الحقوق، جامعة البحرين، البحرين، ٢٠١٤م.

-حمد عبد الله حيي بو غانم السليطي، تجريم الاحتيال الإلكتروني في القانون القطري والمقارن، كلية الحقوق، جامعة قطر، قطر، ٢٠١٨م.

-منير محمد الجنبية، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٥م.

-هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت، دار النهضة العربية، القاهرة، مصر، ٢٠٠٠م.

-جميل عبد الباقي الصغير، أدلة الأثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار، الحاسب الآلي، البصمة الوراثية)، دار النهضة العربية، القاهرة، مصر، ٢٠٠١م.

-محمد الألفي، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الأنترنت، المكتب المصري الحديث، القاهرة، مصر، ٢٠٠٥م.

-عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، جامعة الشرق الأوسط، كلية الحقوق، الأردن، ٢٠١٤م.

-عبد الله عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠١١م.

-هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر، ٢٠٠٠م.

-عمر عبد العزيز موسي عبد العزيز، أليات تفعيل الحماية والوقاية من الجرائم الإلكترونية: إنشاء ضبطية خاصة بالجرائم الإلكترونية، مركز جيل البحث العلمي وجامعة تلمسان، ٢٠١٧م.

-محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠١م.

-مريم أحمد مسعود أليات مكافحة جرائم تكنولوجيات الإعلام والاتصال، كلية الحقوق، جامعة ورقلة، ٢٠١٣م.

هوامش البحث

(١) وائل محمد نصيرات، جريمة الاحتيال عبر شبكة المعلومات الدولية، ع ١٩، مجلة دفاتر السياسة والقانون، المملكة العربية السعودية، ٢٠١٨م.

(٢) حمد عبد الله حيي بو غانم السليطي، تجريم الاحتيال الالكتروني في القانون القطري والمقارن، كلية الحقوق، رسالة ماجستير، جامعة قطر، قطر، ٢٠١٨م.

(٣) سامر سليمان عبد الجبوري، جريمة الاحتيال الالكتروني، كلية الحقوق، جامعة البحرين، البحرين، ٢٠١٤م، ص ٦.

(٤) وائل محمد نصيرات، جريمة الاحتيال عبر شبكة المعلومات الدولية، دراسة مقارنة، ع ١٩، مجلة دفاتر السياسة والقانون، المملكة العربية السعودية، ٢٠١٨م، ص ٩٨.

(٥) حمد عبد الله حيي بو غانم السليطي، تجريم الاحتيال الالكتروني في القانون القطري والمقارن، كلية الحقوق، جامعة قطر، قطر، ٢٠١٨م، ص ٢٤.

(٦) منير محمد الجنبي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، مصر، ٢٠٠٥م، ص ١٣٦.

(٧) هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، مصر، ٢٠٠٠م، ص ٤٨.

(٨) جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار، الحاسب الآلي، البصمة الوراثية)، دار النهضة العربية، القاهرة، مصر، ٢٠٠١م، ص ١١٧.

(٩) هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر، ٢٠٠٠، ص ٤٥.

(١٠) عمر عبد العزيز موسي عبد العزيز، أليات تفعيل الحماية والوقاية من الجرائم الإلكترونية: إنشاء ضبطية خاصة بالجرائم الإلكترونية، مركز جيل البحث العلمي وجامعة تلمسان، ٢٠١٧، ص ٢١٨.

(١١) محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الألي، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠١، ص ٩٤.

(١٢) عمر عبد العزيز موسي عبد العزيز دبور، أليات تفعيل الحماية والوقاية من الجرائم الإلكترونية، مرجع سابق، ص ٢٢١.

(١٣) أحمد مسعود مريم، أليات مكافحة جرائم تكنولوجيات الإعلام والاتصال، كلية الحقوق، جامعة ورقلة، ٢٠١٣، ص ١٢.

(١٤) محمد الألفي، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت، المكتب المصري الحديث، القاهرة، مصر، ٢٠٠٥م، ص ٢٠٣.

(١٥) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية (دراسة مقارنة)، جامعة الشرق الأوسط، كلية الحقوق، الاردن، ٢٠١٤م، ص ١١١.

(١٦) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، مرجع سابق، ص ١١٣.

(١٧) عبد الله عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠١١، ص ٦٠.

(١٨) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، مرجع سابق، ص ١١٨.