عياش، راشد حسن. مجلة القدس للبحوث الأكاديمية
نسخة العلوم الإنسانية والاجتماعية 1 (3): 102 - 92، 2024.
DOI: https://doi.org/10.47874/2024pp:92-102

جريمة الاختراق وتأثيرها على الشبكة الإلكترونية في ظل القانون الفلسطيني

راشد حسن عياش

الملخص

تعدّ جريمة الاختراق من الجرائم الإلكترونية المستحدثة التي ظهرت مع التقدم والتطور التقني والتكنولوجي الهائل، والتي تتمّ بواسطة الحاسب الآلي وشبكة المعلومات، ويتمّ الوصول من خلالها للبيانات والمعلومات السرية الخاصة بكل من يتعامل معها. كما أن جريمة الاختراق يقوم بها المجرم المعلوماتي، وليس باستطاعة أي شخص أن يطلق على نفسه مخترقاً، فهو يتميّز بصفات تميّزه عن غيره من الخبراء كالكفاءة والمهارة التي تؤهله للتعامل مع الحاسوب ومكوناته. وتجدر الإشارة إلى أن هذه الجريمة تكون نافذة بمجرد دخول الجاني إلى النظام أو الشبكة حتى ولو لم يقم بأي عمل إجرامي. وقد توصلنا إلى أن الجرائم المعلوماتية لها خاصية معيّنة أهمها صعوبة اكتشافها، فمثل هذه الجرائم لا عنف فيها ولا تترك أي أثر مادي وهو ما يستدعينا إلى أن نطلق عليها مصطلح «الجرائم النظيفة»، بمعنى أنها جريمة غير وطنية حيث لا تحتاج إلى بذل أي عناء بالانتقال من دولة لأخرى أو من مكان لآخر.

ومن النتائج التي توصّل إليها الباحث أن هذه الجريمة لا تقوم إلا بتوفّر العلم لدى المستخدم بأن دخوله غير مشروع، فإذا علم بعد دخوله واستمر بالدخول، فتكون الجريمة من لحظة علمه بالدخول غير المشروع، شريطة استمراره بالبقاء في الشبكة أو النظام، أما إذا قام بالدخول وبعد ذلك علم بأن دخوله غير مشروع، وخرج من النظام فلا تقوم الجريمة عليه، وكذلك توصل الباحث فيما يخص المستخدم الذي يكون له تصريح وصلاحية الدخول والاطلاع على المعلومات، حيث إنه إذا تجاوز التصريح الخاص بالدخول والاطلاع على المعلومات أو استمر بالتواجد أكثر من المدة المحددة في التصريح الخاص له مع علمه بذلك، فالجريمة تكون قائمة، والهدف من ذلك أن المشرع أراد إيجاد حماية للشبكات والأنظمة المعلوماتية المخزنة عليها.

الكلمات المفتاحية :الاختراق، الجرائم الإلكترونية، الشبكة الإلكترونية.

The Crime of Hacking and its Impact on the Electronic Network under Palestinian Law

Abstract

Hacking is a modern cybercrime that has emerged with the rapid technological advancements. It involves unauthorized access to data and confidential information through computers and networks. It is carried out by skilled individuals known as cybercriminals. It›s important to note that hacking itself is considered a crime, regardless of whether any criminal activity is committed. Cybercrimes have the characteristic of being difficult to detect. Such crimes are non-violent and do not leave any physical evidence, which is why they are referred to as «clean crimes.» They are considered non-national crimes as they do not require any effort to move from one country or place to another. The researcher's findings indicate that the crime of unauthorized access requires the user›s knowledge of their unauthorized entry. If the user becomes aware of the unauthorized entry and continues to stay in the network or system, the crime occurs from the moment they become aware of the unauthorized entry, as long as they continue to stay. However, if the user enters and later becomes aware of the unauthorized entry and exits the system, the crime does not apply to them. The researcher also concluded that if a user has permission and authorization to access and view information, but exceeds the granted access or stays longer than the specified duration with knowledge of that, the crime is established. The purpose of this is to provide protection for networks and stored information systems.

Keywords: Penetration, Cybercrimes, Electronic Network.

راشد حسن عياش، موظف سابق في هيئة تسوية الاراضي والمياه، حاصل على الماجستير في القانون الجنائي من جامعة القدس، للمراسلة: rashedayyash21@gmail.com
هذا البحث مستل من رسالة الماجستير التي عنوانها «جريمة اختراق النظم والشبكات المعلوماتية» وقد نوقشت وأجيزت بتاريخ 2019/4/13 من جامعة القدس، فلسطين.

مقدمة

شَهِدَ عالمنا الحالي تطوراً كبيراً في مجالات الحياة كافّة، ومنها التطور السريع في المجال التكنولوجي على مختلف الأصعدة في مجالات الحياة كافّة، وهذا ما جعل العالم قرية صغيرة، وأصبحت كل القطاعات المختلفة تعتمد على الأنظمة الإلكترونية، لما يميزها من سرعة ودقة في تجميع المعلومات وتخزينها ومعالجتها ونقلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو مع عدّة دول.

وقد تميز التطور التكنولوجي في أنه أتاح المجال لجميع الفئات العمرية في استخدام الشبكة الإلكترونية، وهذا بدوره كان سبباً في فتح النوافذ المغلقة، وقرع أجراس الخطر لا سيما وأن هذه الشبكة في بداية نشأتها كانت بلا قيود وحماية، وهذا ما جعلها سبباً في ظهور جرائم جديدة ليست تقليدية وإنما جرائم مستحدثة على الإنسان وهي ما يطلق عليها البعض اسم الجرائم المعلوماتية أو الإلكترونية، وبالرغم من المزايا الهائلة التي وجدت بفعل هذا التطور، إلا أنه نتج عنها انعكاسات خطرة وسلبية جراء استخدام الشبكة الإلكترونية، وفي غمرة هذا التطور التكنولوجي السريع برزت جريمة الاختراق، إذ تعد جريمة إلكترونية تتمّ في الخفاء، ولها دوافع عدّة من بينها دوافع شخصية، أو انتقامية، أو سياسية أو بهدف كسب المال بطريقة غير مشروعة. إن شبكة الإنترنت بقيت دون حراسةٍ أو قيود أو حدود لردع الجرائم الإلكترونية، وعليه فإن التطور التكنولوجي كان سبباً لظهورها، والتي دقّت ناقوس الخطر، ولتنبّه مجتمعات العصر الحالي من حجم المخاطر وهول الخسائر الناجمة عنها.

فكما هو معروف أن الجهات المكلَّفة بالبحث والتحرّي عن الجريمة والمجرمين اعتادت التعامل مع الجريمة بصورتها التقليدية، حيث وإنه في مسرح الجريمة التقليدية يترك -غالباً- آثار مادية من بصمات، أو آثار أقدام، أو بقع دم، أو أداة الجريمة، فالمشكلات الإجرائية التي ستواجه هذه الجهات عند تعاملها مع الجريمة الإلكترونية، تبدأ من طبيعة البيئة الافتراضية التقنية التي ترتكب فيها، فجريمة الاختراق من الجرائم التي لا تخلف أي آثار مادية محسوسة، وهي جريمة تتمّ في الخفاء، وهي من العناصر الأساسية التي يلجأ إليها المجرم المعلوماتي لإخفاء نشاطه الإجرامي -الإلكتروني- من خلال تلاعبه بالبيانات، وغالبا ما يتحقق دون علم المَجني عليه، وتجدر الإشارة أيضاً إلى أن هناك جرائم إلكترونية لا تتمّ في الخفاء، وتترك آثاراً مادية كجرائم النشر الإلكتروني، والشتم والتحقير فهي تترك أثراً مادياً وهو ما يميزها عن جريمة الاختراق.

وعلى ضوء ذلك فإن الجريمة الإلكترونية أثارت العديد من المشكلات مع جهات الاختصاص في كيفية التعامل مع تلك الجرائم، وهو الأمر الذي كان سبباً لتدخّل المشرع الفلسطيني لهذا النوع من الجرائم، وذلك بموجب قرار بقانون خاص بالجرائم الإلكترونية الفلسطيني رقم (١٠) لعام (٢٠١٨)، حيث أوجد طرقاً إجرائية تتفق مع طبيعة الجريمة المعلوماتية، وجرّم وعاقب على الجرائم التي ترتكب من خلال الحاسوب، وكذلك الأمر في القرار الصادر عن مجلس الوزراء الفلسطيني رقم (١٦) لعام (٢٠١٥)، المتعلق بالنظام الداخلي لعمل الفريق الفلسطيني للاستجابة لطوارئ الحاسوب، حيث جاء في المادة الرابعة منه ما ينصّ على ضرورة خلق بيئة معلوماتية حاسوبية فلسطينية آمنة وموثوقة ضمن أحدث وسائل التكنولوجيا المستخدمة.

مشكلة الدراسة:

تكمن إشكالية الدراسة في أن جريمة الإختراق تعدّ من الجرائم الإلكترونية التي ظهرت مع التطور التكنولوجي الكبير الذي شهده العالم، حيث إن التغيير الحاصل على مستوى النشاط الإجرامي بفعل اتصاله بتقنية المعلومات، وهذا ما صاحبه تحوّل كبير على المستوى القانوني بشكل عام، وعلى المستوى الإجرائي بشكل خاص، فظهرت آليات وإجراءات قانونية مستحدثة في مجال البحث والتحقيق، أساسها النصّ القانوني، و ميدانها الجرائم الإلكترونية، لكنّ هذا التطور لا يسري بنفس الوتيرة في المجالين، فالجرائم المعلوماتية تتطور بشكل سريع، بينما النصوص والإجراءات القانونية تسير ببطئ بالنسبة لواقع الجريمة المعلوماتية، وهذا ما يشكلُ فجوةً بين الجريمة والإجراءات الموضوعة لمتابعتها. وعليه يمكن طرح مشكلة البحث في التساؤل الرئيس الآتي:

ما مدى فاعلية النصوص القانونية الناظمة لجريمة الاختراق الإلكتروني في التشريع الفلسطيني في الحد من ارتكاب الجريمة؟

منهجية الدراسة:

اعتمد الباحث في هذه الدراسة على المنهج الوصفي التحليلي، إذ عمل الباحث على تحليل بعض النصوص القانونية الواردة في القرار بقانون بشأن الجرائم الإلكترونية رقم (١٠) لسنة (٢٠١٨)، ولبعض النصوص الواردة في القانون رقم (٣) لعام (١٩٩٦) والمتعلق بالاتصالات السلكية واللاسلكية التي لها صلة في موضوع الدراسة.

أهداف الدراسة:

تهدف هذه الدارسة إلى تحقيق الأهداف التالية بعد دراسة النصوص القانونية وتحليلها التي تعالج جريمة الاختراق، وتتلخّص في التعرف على جريمة الاختراق، وأثرها على الشبكة الإلكترونية ونظم المعلومات، ومعرفة أنه هل باستطاعة أي شخص أن يقوم بعملية الاختراق، وهل يمكن اعتبار جريمة الاختراق جريمة قائمة دوماً أم لا؟

أهمية الدراسة:

تعدّ الجريمة مظهراً سلبيّاً من مظاهر المجتمع، فهي تعكس السلوك السلبي الإنساني، وتأتي أهمية الدراسة فيما يأتي:

١. إنّ موضوع جريمة الاختراق يعدّ من الجرائم المستحدثة التي ظهرت مع التطور التكنولوجي في المجالات كافّة.

٢. توضّح كيفية تعامل المشرّع الفلسطيني مع هذا النوع من الجرائم الإلكترونية.

ستتناول الدراسة موضوع جريمة الاختراق من خلال مناقشة مفهوم جريمة الاختراق وأركانها وأشكال جريمة الاختراق، ثم ستتحدث عن جريمة الاختراق وطبيعتها القانونية من خلال دوافع جريمة الاختراق والطبيعة القانونية لجريمة الاختراق.

جريمة الاختراق- أركانها وأشكالها

إنّ سهولة التعامل مع شبكة الإنترنت مهّدت طريقاً ليس صعباً للمجرمين من أجل تحقيق مصالحهم والقيام بأعمالهم الإجرامية، وتعدّ جريمة الاختراق من الجرائم الإلكترونية التي ظهرت مع تطور شبكة الإنترنت، حيث أسهم تطورها إلى بروز جرائم إلكترونية لم تكن تعرفها البشرية من قبل، ومع بروز تلك الجرائم ونموها بشكل مستمر أصبح من الضروري إيجاد الحلول، وتوفير الحماية ضد تلك الهجمات الإلكترونية التي تكلّف الدول خسائر مالية فادحة، من خلال مواكبة التطور التكنولوجي، وتصميم البرامج التي تختصّ بحماية الحاسوب والشبكة الإلكترونية، وتقديم دورات توعية لمستخدمي الحاسوب والشبكة؛ من أجل حمايتها من المخاطر الناجمة عنها.

مفهوم جريمة الاختراق وأركانها:

يعدّ جهاز الحاسوب الأداة التي تستخدم في ارتكاب جريمة الاختراق ومن خلال شبكة الإنترنت. فيمكن اعتبار جريمة الاختراق على أنها ضمن عائلة الجرائم المعلوماتية التي يتم ارتكابها بوساطة النظام المعلوماتي، وهناك من يرى إلى أنها تنتمي للسلوك الإجرامي بجرائم الاعتداء على نظم المعالجة الآلية، أو بجرائم السلوك التي تتصل بنظام المعالجة الآلية للمعلومات (حجازي، ٢٠٠٢، ص. ٢٣٥) وسنتناول في ما يلي مفهوم جريمة الاختراق وأركانها.

أولاً: مفهوم جريمة الاختراق:

تُعرّف الجريمة على أنها انحراف الإنسان عن طبيعته الإيجابية، وانتقالها إلى طبيعة سلبية، ويكون ذلك ناجم عن عدة عوامل مختلفة منها: طبيعة البيئة التي يعيش فيها الإنسان، فيتأثر منها وبالتالي تكسبه السلوك السلبي، فالجريمة تعبّر عن السلوكيات السلبية للشخص، والإنسان بطبيعته يولدُ خالياً من أي شوائب، والجريمة التقليدية تختلف عن المستحدثة في أن الجريمة المستحدثة تكون الشبكة الإلكترونية مسرحها، والأدوات تكون برامج معينة، والنتيجة الجرمية تتحق بالدخول غير المشروع للبيانات والمعلومات، وتعطيل البرمجيات، وإتلاف البيانات الخاصة بالمجني عليه.

والاختراق لغةً: الخَرْق: الخُرقة، وجمعه خُروق؛ خَرَقه يَخْرِقُه خَرْقاً وخرَّقه واخْتَرَقه فتخَرَّق وانخرَق واخْرَوْرَق، يكون ذلك في الثوب وغيره التهذيب الخرق الشَّقُّ في الحائط والثوب ونحوه، يقال: في ثوبه خَرق وهو في الأَصل مصدر والخِرْقة: القِطعة من خِرَقِ الثوب، والخِرْقة المِزْقةُ منه وخَرَقْت الثوب إذا شَقَقْتَه ويقال للرجل المُتمزِّق الثياب: مُنْخَرِق السِّرْبال (ابن منظور، ١٩٩٠، ص. ٧٣).

والاختراق كما ورد في معجم مالية هو دخول غير مصرّح به إلى نظام إلكتروني لمعالجة البيانات (ب) الحصول على حصّة في السوق ويكون ذلك عادة من خلال تخفيض الأسعار، وتعني بالانجليزي (penetration) (موقع معجم المعاني: www.almaany.com) وقد ورد في قوله تعالى: {إِنَّكَ لَنْ تَخْرِقَ الْأَرْضَ} (سورة الإسراء، الآية ٣٧)، ويقصد بخرق الأرض يخرقها: قطعها حتى بلغ أقصاها، وخرقت الأرض أي جبته (ابن منظور، ١٩٩٠، ص. ٧٥). وقوله تعالى: {وَخَرَقُوا لَهُ بَنِينَ وَبَنَاتٍ بِغَيْرِ عِلْمٍ} (سورة الأنعام، الآية ١٠٠)، ويُقصد بالآية أنهم افتعلوا ذلك كذبا وكفراً (ابن منظور، ١٩٩٠، ص. ٧٥). من هما نرى أن الاختراق في اللغة قد ورد بمعانٍ عديدة تتحدث معظمها عن التجاوز بالحق وبغير الحق.

أمّا اصطلاحاً: أدركت دولة فلسطين الخطر الحقيقي للجرائم الإلكترونية، وتأثيره الكبير على مرافق الدولة العامة، وتوجهت إلى أنه ومن الضروري أن يكون هناك قانون يتعلق بالجرائم الإلكترونية ويعاقب عليها، فقد أصدر الرئيس الفلسطيني محمود عباس قراراً بقانون رقم (١٠) لسنة (٢٠١٨) والمتعلق بالجرائم الإلكترونية، حيث ورد تعريف الاختراق في المادة الأولى منه، فالاختراق: هو الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات، أو الشبكة الإلكترونية. (انظر إلى م(١) قرار بقانون بالجرائم الإلكترونية الفلسطيني رقم(١٠) لسنة (٢٠١٨)). وإذا أمعنا النظر في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة في القاهرة بمقر جامعة الدول العربية عام (٢٠١٠م)، نجد بأن المادة السادسة منها تحدثت عن جريمة الدخول غير المشروع، وهو ما يتفق مع مفهوم جريمة الاختراق، ولكن دون أن يشار إليها بمعنى مباشر، وقد نصت المادة السادسة على ما يأتي:

١- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

٢- تشدّد العقوبة إذا ترتّب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال، وإلحاق الضرر بالمستخدمين والمستفيدين.

ب- الحصول على معلومات حكومية سرية (انظر إلى م(٦) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية لعام (٢٠١٠م).

والاختراق يطلق عليه باللغة الإنجليزية مصطلح (hacking) وهو محاولة الدخول لجهاز المشترك في شبكة الإنترنت من قبل شخص آخر لا يحق له الدخول إلى ذلك الجهاز أو تلك الشبكة، وذلك بهدف الاطلاع على البيانات والمعلومات وتدميرها أو زرع فيروسات (عمار، ٢٠١١، ص. ١٨). ويمكن أن نطلق على الاختراق بأنه الدخول أو الولوج إلى النظام إما بقيام الجاني بالدخول إلى الحاسوب كله أو إلى جزء منه، وتكون عملية الاختراق غالباً في حال كان للجاني القدرة على الدخول للحاسب، ويشبه جانب من الفقه الجنائي الفرنسي عملية الدخول غير المشروع أو الاختراق إلى نظام الحاسوب أو الموقع الإلكتروني، كالدخول أو اختراق ذاكرة الإنسان (خلف، ٢٠١٠، ص. ١٨). **وبناءً** على ما سبق، يعرّف الباحث الاختراق على أنه قدرة، يستطيع من خلالها المخترق (المجرم) من الدخول إلى جهاز شخص ما (الضحية)، بحيث يقوم من خلال هذا الهجوم بتحقيق النتيجة (الغاية) وهو حدوث ضرر، وبصرف النظر عن قيمة الأضرار التي تحدث للضحية.

ثانياً: أركان جريمة الاختراق:

تقوم جريمة الاختراق كما الجرائم الأخرى على ركنين أساسيين: ركن مادي، وآخر معنوي، ويمكن أن نضيف أيضاً لها ركناً آخر وهو الركن القانوني. فالركن المادي يتمثل بالفعل أو النشاط الذي يقوم به الجاني، ويتمثل بالاعتداء على حقٍّ حماهُ القانون، والركن المعنوي يتمثل بعنصري العلم والإرادة وهو أن يكون الجاني عالماً بما يفعل ولديه علم بالنتيجة وغير مجبر أو مكره على ذلك، ويقصد بالإرادة وهي أن تتجه إرادة الجاني إلى حدوث النتيجة وإرادتها بغض النظر عن خطورة النتيجة التي حدثت أو ستحدث، والركن القانوني أي أن يكون هذا الفعل معاقباً عليه بالقانون وأن يكون المشرع قد ذكر تلك الجريمة في قانون العقوبات أو في قانون خاص «بالجرائم الالكترونية»، وسنتناول هنا بشرح تفصيلي للركن المادي والمعنوي والقانوني.

١- الركن القانوني: يسميه بعض الحقوقيين بالركن الشرعي، فكما هو معروف أنه «لا جريمة ولا عقوبة إلا بنصّ» ومعنى ذلك أن القواعد الجنائية هي التي تحدّد الأفعال التي تعتبر جريمة أم لا وهي التي تقرر العقوبة المناسبة لها، والجهة المختصة بإصدار تلك العقوبات، وتحديد تلك الجرائم هي السلطة التشريعية، لأنها هي من تقوم بإصدار القوانين، والسلطة القضائية تقوم بتطبيق تلك القوانين على المجرمين والجرائم التي ترتكب (نجم، ٢٠١٢، ص. ١٣٧). وهناك العديد من الدول التي وضعت قوانين خاصة للجرائم الإلكترونية، وتعدّ دولة السويد أول دولة تسنّ قوانين خاصة بالجرائم الإلكترونية، حيث أصدرت في عام (١٩٧٣) قانون البيانات، وسارت على هذا النهج الولايات المتحدة الأمريكية، حيث شرّعت قانوناً خاصاً بحماية أنظمة الحاسوب وذلك بين عامي (١٩٧٦-١٩٨٥)، وتبعتها بذلك فرنسا ففي عام (١٩٨٨) عملت على تطوير قوانينها الجنائية لتتوافق مع ما استحدث من جرائم (مقال بعنوان الجريمة الإلكترونية في فلسطين مباحة: www.cutt.us/Y2noU)، وفي فلسطين صدر قرار بقانون رقم (١) لسنة (٢٠١٨) بشأن الجرائم الإلكترونية محاولاً بذلك وضع العقوبات وتبيان خطورة الفعل المرتكب من الجرائم الإلكترونية، وقد خص القرار بقانون المواد (٦/٥/٤) والمتعلق بالجرائم الإلكترونية جريمة الدخول غير المشروع، وإتلاف البيانات، وتعطيلها، والعقوبة المترتبة عليها.

٢- الركن المادي: هو الوجه الخارجي للنشاط الإجرامي، ويقصد به الفعل أو النشاط الذي يقوم به الجاني من خلال الاعتداء على حقٍّ كفله القانون، والركن المادي في جريمة الاختراق يتمثّل في الدخول إلى نظام جهاز الحاسوب، وإتلاف برامج، وبيانات، أو الوصول إلى معلومات سرية هامة، وهو ما نصّت عليه المادة الرابعة الفقرة الأولى من القرار بالقانون الصادر عن رئيس دولة فلسطين محمود عباس والخاص بالجرائم الإلكترونية رقم (١) لعام (٢٠١٨) (انظر إلى م(١) قرار بقانون بالجرائم الإلكترونية الفلسطيني رقم(١) لسنة (٢٠١٨). ويقوم الركن المادي من سلوك إجرامي (فعل أو امتناع عن الفعل) والنتيجة علاقة سببية، وهو ما سنفصله هنا:

إن السلوك الإجرامي في جريمة الإختراق يتمثل في استخدام تقنية الحاسوب، ويتم ذلك من خلال استخدام شبكة الإنترنت أداةً لارتكاب جريمة الاختراق بطريقة غير مشروعة، وهذا من شأنه أن يلحق الضرر بالمجني عليه من خلال إتلاف البيانات والوصول لمعلومات هامة.

أ- الفعل: وهو النشاط أو السلوك الإجرامي للجاني، والسلوك قد يكون إيجابياً وقد يكون سلبياً؛ فالسلوك الإيجابي: عبارة عن حركة عضوية إرادية، نهى القانون عن القيام بها؛ لأنها ستسبّب وقوع النتيجة، ويشترط أن تكون الحركة إرادية أي صادرة عن إرادة الإنسان وأنه غير مكره على فعلها. بينما السلوك السلبي: هو عبارة عن الامتناع عن القيام بفعل أوجب القانون على القيام به رعاية لمصالح الأفراد وحقوقهم (نجم، ٢٠١٢، ص ص. ٢٠٩-٢١٠). والسلوك الإجرامي في الجرائم التقليدية هو ما يقوم به الشخص من فعل يؤدي إلى تحقق النتيجة التي يسعى إليها، فمثلاً في جريمة القتل نجد أن سلوك الجاني يهدف إلى إزهاق روح المجني عليه، وهذا بحد ذاته سلوك إجرامي، وهذا ما أكدته المادة (٣٢٦) من قانون العقوبات الأردني رقم (١٦) لعام (١٩٦٠) والمطبق في فلسطين والتي تتحدث عن القتل العَمد، وكذلك الأمر قد يكون السلوك الإجرامي في جريمة القتل بالامتناع عن القيام بالعمل المطلوب منه بهدف إزهاق روح المجني عليه، كامتناع الأم عن إرضاع طفلها بهدف التخلص منه. فالسؤال هنا ما هو طبيعة السلوك الإجرامي في جريمة الاختراق؟

فكما أشير سابقاً أن الجاني في الجريمة الإلكترونية يتمتع بمهارة وكفاءة تميّزه عن الجاني في الجريمة التقليدية، ففي جريمة الإختراق -محلّ البحث- يكون السلوك الإجرامي في إتلاف البيانات والمعلومات الخاصة بالمجني عليه، أو بإغلاق مواقع وتدميرها.

ب- النتيجة: وهي ما يترتب من أضرار على النشاط الإجرامي الذي قام به الجاني، فالنتيجة في الجريمة التقليدية هي ما يترتب على الفعل الذي قام به الجاني، فليس المهم أن يقوم الجاني بنشاطه الإجرامي، بل يجب أن ينتج عن هذا الفعل تحقق النتيجة الجرمية، ففي جريمة السرقة يجب أن ينتج عن النشاط الذي قام به الجاني انتقال المال من المجني عليه إلى الجاني، وإذا لم تتحقق النتيجة فنكون هنا أم جريمة شروع بالسرقة، ويكون عدم تحققها لعدة أسباب، فقد يكون لعدم رغبة المجني عليه في تحقق النتيجة، أو لسبب خارج عن إرادته، كأن يتمّ اعتقاله قبل الشروع في الجريمة. والنتيجة الجرمية في جريمة الاختراق تتحقق بمجرد الدخول غير المشروع، وإذا ترتّب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزّنة أو إتلاف، أو أعاق الوصول إليها فهنا النتيجة الجرمية تكون قد تحققت، وهو ما أشارت إليه المادّتان الرابعة والخامسة من القرار بقانون رقم (١٠) لعام (٢٠١٨) بشأن الجريمة الإلكترونية.

ت- العلاقة السببية: وهي أن يكون هناك علاقة أو رابطة سببية بين الفعل والنتيجة، حيث يكون السلوك هو السبب الطبيعي لحدوث النتيجة، والنتيجة تكون هي الأثر المترتب عن السلوك الإجرامي الذي قام به الجاني. ففي جريمة الاختراق تتمثل العلاقة بين الفعل والنتيجة بالدخول غير المشروع إلى الجهاز أو بإلغاء البيانات أو المعلومات الإلكترونية المخزنة أو بإتلافها، والجدير بالذكر أنه في الجرائم الإلكترونية بشكل عام لا يستوجب على الجاني القيام بأي عنف أو بذل أيّ جهد (قشقوش، ١٩٩٢، ص ص.٦١-٦٢). وللتوسع أكثر في العلاقة السببية فقد ظهرت نظريات متعددة لتحديد معيار العلاقة السببية، منها نظرية السبب المباشر، ونظرية السبب الملائم، ونظرية تعادل الأسباب. ونظرية السبب المباشر تقوم على أساس وجود اتصال مباشر وقوي بين النتيجة والسلوك الإجرامي، فلا يُسأل الجاني عن جريمة الاختراق دون أن يكون هناك اتصال مباشر بين السلوك الإجرامي والنتيجة الجرمية، وبهذا المعيار أخذ القضاء الفرنسي (مصطفى, ١٩٦٩, ص٢٧١). ونظرية السبب الملائم هي التي تنصّ على أنّ العلاقة السببية ما بين السلوك الإجرامي والنتيجة الجرمية، تكون متوافرة متى ثبت أن مساهمة السلوك الإجرامي في إحداث النتيجة الجرمية يمثل قدراً معيناً من الأهمية، والعلاقة السببية في هذه النظرية تنقطع بين السلوك الإجرامي والنتيجة الجرمية بمجرد دخول عوامل أخرى غير متوقعة، فتقف هنا مسؤولية الجاني في جريمة الاختراق بقدر الفعل الذي قام فيه فقط، ولا يسأل عن النتيجة التي تلت دخول شخص آخر واستمراره في الاختراق وإتلاف البيانات (سرور, ٢٠٢٢, ص٤٨٤). أما نظرية تعادل الأسباب ففيها يتم اعتبار جميع العوامل والظروف التي ساهمت في حدوث النتيجة الجرمية متساوية ومتعادلة، بمعنى آخر أن العلاقة السببية تكون متوافرة بين الفعل والنتيجة الجرمية، متى ثبت أن السلوك الإجرامي كان أحد العوامل التي ساهمت في حدوثها.

٣- الركن المعنوي: ويعدّ الركن المعنوي في هذه الجريمة من الأركان المهمة لقيام المسؤولية الجزائية، فهذه الجريمة لا تقوم إلا عمدية، وتتطلب القصد الجنائي العام، والذي يمكن أن نقسمه إلى قسمين هما: العلم والإرادة، والمقصود بالعلم: هو العلم بالقانون وهو أمر افتراضي، والعلم بالوقائع. أما الإرادة فهي أن تتّجه إرادة الجاني إلى إحداث الفعل الإجرامي والإصرار على تحقق النتيجة الجرمية، وبالتالي فإن جريمة الاختراق بصورتها البسيطة لا تتطلب قصداً جنائياً خاصاً، بل يكفي توفر القصد الجنائي العام المتمثل في اتجاه إرادة الفاعل إلى الدخول عمداً دون وجه حقّ بأيّة وسيلة موقعاً إلكترونياً، أو نظاماً، أو شبكة إلكترونية، أو تجاوز الدخول المصرح به، أو الاستمرار في التواجد بها بعد علمه بذلك. ويرى جانب من الفقه إلى أن الدخول إلى النظام يكون مشروعاً إذا كان دخوله نتيجة الصدفة أو الخطأ، فإذا دخل الشخص لمكان فجأةً فعليه الخروج وهو ما يطلق عليه اسم مصطلح «حسن النية»، وإذا بقي في داخل النظام فيكون توافر بحقه القصد الجنائي العام الذي تقوم عليه الجريمة وهو ما نطلق عليه اسم مصطلح «سيء النية» (رمضان، ٢٠٠١،، ص. ٥٢).

أشكال جريمة الاختراق:

تحدّث الباحث سابقاً عن جريمة الاختراق وبيّن أنها عملية دخول غير مشروعة لأجهزة الحاسوب ولشبكات الإنترنت المختلفة، بهدف إحداث ضرر في جهاز الضحية، أو في الموقع الخاص بالمجني عليه، ووضّح دوافعها، واستنتج في نهاية المطاف بأن هذه الجريمة لها دوافع كما الجريمة التقليدية، وتختلف الدوافع من مجرم لآخر، وذكر الباحث أيضاً أنّه ليس باستطاعة أيّ شخص أن يكون مخترقاً، فالمخترق هو إنسان طبيعي ولكن عقلية الإنسان وذكاءه يختلف من إنسان لآخر، فالمخترق يتمتّع بذكاء عالٍ، ولديه الدراية الكاملة في برامج الحاسوب. ولجريمة الاختراق أشكال عديدة سوف نتحدث عنها على النحو الآتي:

١- اختراق البريد الإلكتروني: يعدّ البريد الإلكتروني وسيلة من وسائل الاتصال والتواصل بين الشركات والأفراد، وتعود بدايات ظهور البريد الإلكتروني إلى فترة تطوّر شبكة (ARPANET) وظهورها، وكان لسهولة استخدامه السبب في الإقبال الكبير من قبل المجتمع والشركات التجارية والمؤسسات الحكومية، وقد أصبح وسيلة لحفظ المعلومات والبيانات وتبادلها فيما بينهم، وهذا ما جعله عرضةً لأن يتم اختراقه، وهدفهم بذلك هو الحصول على تلك البيانات والمعلومات السرية الخاصة بمستخدم البريد الإلكتروني، وعند حصولهم على تلك المعلومات والبيانات يقومون إما بتهديد صاحبها، أو (ابتزازه) بنشر تلك المعلومات إن لم يقم بدفع مبلغ معين من المال،

أو أن يقوموا بنشرها على الإنترنت؛ من أجل فضح صاحب تلك المعلومات. أذكر مثالاً على ذلك ما حدث مع الرئيس السوري بشار الأسد عندما قام مجموعة مخترقين باختراق بريده الشخصي وتسريب رسائل خاصة به (الغفيلي، ٢٠١٣، ص. ٤). وكان أول حكم قضائي لجرائم الإنترنت في الوطن العربي بتاريخ (٨\١٢\٢٠١٣) حيث أصدرت محكمة الإحساء شمال شرق السعودية حكماً يقضي بسجن شاب سعودي وجلده وتغريمه بعد أن تبين أنه قام باختراق بريد إلكتروني يعود لفتاة سعودية، حيث قام بسحب صورها وابتزازها بتلك الصور (فتحية، ٢٠١٢، ص. ١٨٣).

٢- اختراق الهاتف: كان للتطور العلمي الكبير، ونتيجة لانتشار الهواتف الذكية بشكل كبير جداً في مختلف أنحاء العالم، ونتيجة لاتصال تلك الهواتف بشبكة الإنترنت، فقد أصبحت الهواتف عُرضة للاختراق من قبل المجرمين، بدءاً من التجسّس على مكالماته ومحادثاته، مروراً بسرقة الصور، أو الفيديوهات، أو المراسلات، أو حتى تعطيله عن العمل وضربه بالفايروسات، وقد يتم اختراق الهاتف من خلال إرسال رسائل تكون ملغمة بفايروسات ويكون لها القدرة على تدمير الهاتف بالكامل.

٣- اختراق الحواسيب الشخصية: تعدّ هذه الجريمة الأكثر انتشاراً على مستوى العالم، وذلك لأسباب عديدة منها: سهولة اختراق الحاسوب بسبب ضعف استخدام المستخدم للحاسوب، أو بسبب تصفحه لمواقع غير آمنة، أو لسهولة اختراق الحاسوب، إذ إنّ مستخدم الحاسوب قد يستخدم كلمة مرور ضعيفة، كذلك عدم وجود أنظمة حماية ضد برامج الاختراق وضد الفيروسات، هذا كله يجعل الحاسوب عرضة للاختراق بشكل قوي.

٤- اختراق الشبكات: تعدّ الشبكات وسيلة من وسائل نقل البيانات والمعلومات؛ لذلك فمن الواجب أن يتمّ ضمان أمنها من الاختراق لكي تصل المعلومات والبيانات بسلامة ودون أي اعتراض، والشبكات لها أنواع عديدة: فقد تكون شبكة محلية «منزلية»، وهي شبكة تربط عدة حاسبات داخل منطقة معينة، ويتم اختراقها من أجل تحقيق أهداف خاصة، وقد تكون شبكة تخص عمل مؤسسة حكومية أو شركة، بحيث يكون الهدف من ذلك الاختراق هو تعطيل عمل المؤسسة، أو من أجل الوصول إلى البيانات الخاصة بها من أجل ابتزاز تلك الشركة، إما بنشر بياناتها، أو بدفع مبلغ مالي معين مقابل عدم نشر تلك البيانات والمعلومات. أذكر مثالاً على ذلك لقائد قيادة الإنترنت في البنتاغون الأمريكي الجنرال كيث ألكسندر، حيث أنه حذر من هجوم إلكتروني يشلّ واشنطن، وقال إنه تقدّم بطلب إلى الرئيس الأمريكي السابق باراك أوباما؛ لمنحه سلطات إدارة شبكات الإنترنت في واشنطن، وذلك تخوفاً من وقوع هجوم إلكتروني، ومن أجل ضمان حماية أنظمة الحاسوب في كلّ الولايات الأمريكية (جريدة الشرق الأوسط «قائد قيادة الإنترنت في البنتاغون...»).

٥- اختراق مواقع الإنترنت: لقد ساهم تطور الإنترنت وانتشاره بشكل كبير إلى انتشار مواقع الإنترنت، وقد أدى ذلك التطور إلى ظهور ثغرات أمنية، وهذه الثغرات تشكل تهديداً على إدارة الموقع ليس وحدهم فقط، وإنما تهدد أيضاً مستخدمي تلك المواقع كافّة، ويعدّ اختراق مواقع الإنترنت من الاختراقات التي تحدث بشكل كبير جداً في الوقت الحالي، لسهولة اختراق تلك المواقع والسبب في ذلك هو أن مواقع الإنترنت قد تكون الحماية فيها ليست قوية وهو ما يسهّل عملية الاختراق، وقد أسهم اختراق مواقع الإنترنت إلى تدمير المواقع وإتلاف بياناتها، وإلى حدوث خسائر مالية لأصحاب المواقع (العنزي، «اختراق المواقع الإلكترونية والتأمين...»).

دوافع جريمة الاختراق وطبيعتها القانونية:

إن فئات مرتكبي الجرائم التقليدية تختلف عن فئات مرتكبي الجرائم الإلكترونية، فكما هو معروف فإن لكل جريمة شكلها الخاص وخصائصها الخاصة بها، ومن الطبيعي أن نرى بأن دوافع الجرائم الإلكترونية تختلف عن دوافع الجرائم التقليدية. وفي هذا المطلب سوف يتحدث الباحث عن دوافع جريمة الاختراق وطبيعتها القانونية.

دوافع جريمة الاختراق:

مما لا شك فيه أن الجريمة هي ظاهرة اجتماعية، ولا يوجد مجتمع على وجه الأرض يخلو من الجريمة مهما بلغ من التطور والتقدم والرقي، ولإختلاف المصالح أثر كبير في ظهور الجريمة وارتكابها، وبالتالي مخالفة القانون والإضرار بالمصالح التي حماها القانون وتحقيق الأهداف بطريقة غير مشروعة. وإذا قارنا ما بين الجريمة التقليدية والجريمة الإلكترونية، سنجد بأنّ المجرم في كلتا الجريمتين يكون له دوافع وغايات يسعى لتحقيقها من خلال ارتكابه للجريمة سواء أكانت تقليدية أم إلكترونية، وهذا ما سنتحدث عنه في هذا المطلب.

الباعث(الدافع): بالرجوع إلى المادة (٦٧) من قانون العقوبات الأردني رقم (١٦) لسنة (١٩٦٠) والمطبّق في فلسطين حتى يومنا هذا، فقد عرفت الفقرة الأولى منها الدافع على أنه: العلّة التي تحمّل الفاعل على الفعل، أو الغاية القصوى التي يتوخّاها. ويعدّ الدافع أو «الباعث» كمحرك المركبة الذي يجعلها تعمل بناءً على حركة إرادية صادرة عن سائق المركبة، فالدافع في الجريمة هو محرك لإرادة المجرم، فهو الذي يوجّه السلوك الإجرامي إلى القيام بارتكاب الجريمة بناءً على حركة عضوية إرادية.

إن لمعرفة الدافع أو الباعث على ارتكاب الجريمة أثراً كبيراً في دراسة شخصية المجرم وتحليلها، وبالتالي معرفة الأسباب الكامنة وراء قيامه بارتكاب الجريمة، ومن خلالها الوصول إلى إيقاع العقوبة المناسبة للمجرم بما يتوافق مع الجريمة المرتكبة، وهذا يسهم بشكل

رئيس في تحقيق العدالة والحفاظ على مصالح الأفراد والمجتمع؛ فالدافع في الجرائم المعلوماتية لا يختلف عن الدافع في الجريمة التقليدية، وقد يكون دافع ارتكاب الجريمة شخصياً، وقد يكون دافعاً خارجياً كل مصدر هذه الدوافع هو الرغبة الإجرامية، ما هو معروف أن الحاجات تسبق عادةً الدوافع، فحاجة الإنسان المجرم تنشأ نتيجة شعوره بنقص ما، أو شعوره بأنه محروم من شيء كفله القانون للفرد، وهذا بحد ذاته يؤدي إلى التأثير بشكل كبير على نفسيته الداخلية، وبالتالي يتشكل لديه دافع قوي لأن يقوم بممارسة عمل إجرامي نهى عنه القانون، وذلك من أجل إشباع حاجته ولكي يسد الفراغ أو النقص الذي يشعر به من خلال حالة الرضاء النفسي لديه، إن دوافع القيام بارتكاب الجريمة الإلكترونية هو مختلف باختلاف منفذيها، وتبعاً لخبرته في مجال المعلومات والإنترنت، حيث يمكن تصنيف هذه الدوافع إلى صنفين: دوافع شخصية، ودوافع خارجية، وهو ما سنتحدث عنه بشكل تفصيلي.

أولاً- الدوافع الشخصية: يمكن إجمال الدوافع الشخصية لدى مرتكب الجريمة المعلوماتية إلى دوافع مالية، وأخرى دوافع ذهنية.

١- الدوافع المالية (تحقيق الربح والكسب المالي): تعدّ الدوافع المالية من أكثر الدوافع تحفيزاً للمجرم لكي يقوم بارتكاب جريمته، حيث يشعر أنه ومن خلال ارتكابه للجريمة سوف يحصل على مال كثير، وربح كبير وهذا يشجع المجرم المعلوماتي على مواكبة التطور والتقدم التكنولوجي في مجال الحاسوب والإنترنت؛ لكي يكون باستطاعته إيجاد الثغرات كافة من أجل الاستفادة منها لكي يحصل على المال. ويكون تحقيق الدافع المالي عن طريق اختلاس المعلومات ثم المساومة عليها، أو استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية (سندالي، ٢٠٠٧). وقد أشارت مجلة الأمن المعلوماتي (Securite informatique)أن (٤٣٪) من حالات الغشّ المعلن عنها قد تمت من أجل اختلاس أموال، و(٢٣٪) من أجل سرقة معلومات، و(١٩٪) أفعال إتلاف و(١٥٪) الاستعمال غير المشروع للحاسوب؛ لأجل تحقيق منافع شخصية (المومني، ٢٠١٠، ص. ٩)، إذن نفهم بأن الإنسان لديه حب كبير للمال، وهذا ما أكده الله سبحانه وتعالى في كتابه العزيز: {وَتُحِبُّونَ الْمَالَ حُبًّا جَمًّا} (سورة الفجر، الآية ٢٠). فحبّ المجرم للمال هو ما يشجعه على ارتكاب الجرائم بمختلف أنواعها.

نخلص للقول: أنه في حال نجاح المجرم المعلوماتي في ارتكاب جريمته المعلوماتية فإن ذلك سيدرّ عليه أرباحاً كبيرة وفي زمن قياسي (سعيداني، ٢٠١٣، ص. ٦١). وفي الجرائم الإلكترونية كل شخص يستخدم الحاسوب والإنترنت هو معرض للاختراق في أي لحظة (ياسمينة، ٢٠١٥، ص. ١١).

٢- الدوافع الذهنية: في الواقع إن المجرم المعلوماتي يقوم عادة بارتكاب الجريمة الإلكترونية، وذلك من باب إحساسه وشعوره بأنه له القدرة على القيام بذلك الفعل، ومن باب أيضا إثباتهم للذات، ووضع بصماتهم ومن أجل مواجهة التطور والتقدم التقني في الحاسوب والإنترنت، ولكي يظهروا قدراتهم بالتفوق على ذاك التقدم، ولا يكون لديهم أي ميول سلبية تجاه تلك الأفعال، وإنما من أجل إثبات قدرتهم على الاختراق والدخول للنظام في أي لحظة يشاؤون، فهم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه في حال ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف في قهر النظام أكثر من شهوة تحقق النتيجة، فيحاولون جاهدين لإيجاد الوسيلة التي يستطيعون من خلالها تحطيمها والتفوق عليها (غايب، ٢٠١١، ص. ١٠٥). نخلص للقول: إن مجرمي الجرائم الإلكترونية لديهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية، ففي بعض الأحيان نجد أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي (فتحية، ٢٠١٢، ص. ٦٦). وقد بلغت نسبة ارتكاب الجريمة الإلكترونية بسبب الحب بالرغبة في إثبات الذات إلى (٣٠٪) موزعة كالآتي: (٣١,٠٪) للذكور في مقابل (٢٩,٠٪) للإناث (نصار، ٢٠١٧، ص. ١٦٢).

ثانياً- الدوافع الخارجية: قد يتأثر المجرم المعلوماتي ببعض المواقف التي تكون سبباً في القيام بالفعل الإجرامي، فهو بتلك الأسباب لا يكون جاهداً لحصوله على المال ولا يقوم بهذا الفعل الإجرامي من باب التسلية، ولا من باب إثبات قدرته على خرق كل تطور يظهر على التقنيات، وإنما يقوم بذلك الفعل من باب دوافع خارجية؛ كالانتقام من شخص ما، أو من مؤسسة ما، وقد يكون دافعاً سياسياً. وكما هو معروف فإن المجرم يتأثر بالعوامل الاجتماعية المحيطة به والتي تكون سبباً في حدوث الجريمة وارتكابها (عبدالله، ٢٠١١، ص. ١٣٢).

١- الانتقام: يعدّ دافع الانتقام من أخطر الدوافع التي تجبر المجرم على القيام بعمله الإجرامي، فقد يكون دافع الانتقام من باب الثأر -لا سيّما- عندما يتعرّض موظف ما في شركة أو مؤسسة إلى الفصل التعسفي من وظيفته، مع العلم أن لديه الخبرة والكفاءة العالية بالعمل؛ فيقوم ذاك الموظف بالرد على الفصل التعسفي بقيامه بالانتقام من تلك الشركة أو المؤسسة من خلال اختراق موقعها وتدمير ملفاتها وتعطيلها، بحيث تتكبّد الشركة أو المؤسسة خسائر مالية فادحة، حيث يشعر حينها ذاك الموظف الذي فصل من علمه بالرضاء على العمل الذي قام به، وأضع مثالاً في هذا الصدد، حيث قام موظف يعمل لدى إحدى شركات التأمين بعد أن فصل منها بحجز وحدة التخزين المركزية الخاصة بالشركة كرهينة ووسيلة لكي يقوم رئيسه بإرجاعه للعمل، حيث قام بتدمير البيانات الخاصة بحسابات شركة التأمين وهو ما حصل بالفعل بعد رحيله من العمل بعدة أشهر (مزغيش، ٢٠١٤، ص. ١١).

٢- دافع سياسي: يعدّ الدافع السياسي من أهم الدوافع الخارجية التي تحفّز المجرم على ارتكاب الجرائم الإلكترونية، فالخلافات السياسية بين الدول أو بين المعارضة والدولة نفسها أو بين الأحزاب نفسها يؤدي إلى انتهاك القانون وارتكاب الجرائم في ظل غياب الوعي وعدم تقبل وإدراك معنى الديمقراطية كوسيلة من وسائل التطور والتقدم. الباحث مثالاً على قيام بعض القراصنة الموجودين

على الأراضي الروسية باختراق نظام الحاسبات الإلكترونية الحكومية في الولايات المتحدة الأمريكية لمدة سنة كاملة، فقاموا بسرقة معلومات غير سرية من أجهزة الحواسيب الخاصة بالعسكرية (فتحية، ٢٠١٢، ص ص. ٦٧-٦٨). كذلك الأمر ما قام به مجموعة مخترقين من اختراقهم لوكالة الأنباء القطرية بتاريخ ٢٤\٥\٢٠١٧م، حيث اتهمت قطر الإمارات بأن المخترقين ينتمون لها، وأشارت الحكومة القطرية بأن المخترقين قاموا بنشر أخبار مفبركة عن أمير قطر الشيخ تميم ابن حمد آل ثاني في الموقع الرئيسي لوكالة «قنا» وحسابات مواقع التواصل الخاصة بها، كما نشر فيديو ملفق على اليوتيوب، وقاموا أيضاً باختراق الحسابات الخاصة بوكالة قنا وسرقة كل حساباتها، وأشار المسؤول القطري إلى أنّ جريمة اختراق وكالة الأنباء القطرية تنقسم إلى ثلاثة أقسام: أولاً- جريمة اختراق الوكالة والسيطرة على الشبكة، وزرع الفايروسات الخبيثة، وثانياً- قيام المخترقين بنشر الأخبار المفبركة لأمير قطر، وثالثاً- الجهة المستفيدة من الاختراق والأخبار المفبركة هو من كان ينتظر نشر تلك الأخبار المفبركة (اختراق وكالة الأنباء القطرية).

٣- دوافع دينية (طائفية): يعدّ الدافع الديني (الطائفي) أحد الدوافع التي ظهرت مؤخراً وبشكل كبير في العالم العربي، والسبب في ذلك هو غياب الديمقراطية، وانتشار الظلم، وعدم وجود القوانين التي تكفل احترام المواطن وتحقيق مصالحه، فقد ظهرت الحركات التكفيرية التي تدعم العنصرية الطائفية. وهذا ما دفع كثير من الشباب والمراهقين للجوء إلى العنف للتعبير عن آرائهم وأفكارهم (اسماعيل، دوافع الجريمة في المجتمع الفلسطيني).

٤- دافع لفت الانتباه: وهذا الدافع قد يستخدمه بعض المخترقين من أجل توجيه الأنظار عليهم ولفت الانتباه، فمرتكبو الجرائم الإلكترونية لديهم شعور بالبحث عن القوة، ولديهم الحب في إظهار التفوق على التطورات التي تحدث على تقنيات التكنولوجيا والحاسوب. يذكر الباحث مثالاً للفت الانتباه وهو ما قام به شاب إيراني يُدْعى (فرهد)، حيث قام باختراق صفحة المغنية اللبنانية نانسي عجرم وقد كتب اسمه على صفحتها بأنه هو من قام باختراقها، وأضاف إلى أنه معجب كثيراً بها هو وعدد كبير من الجمهور الإيراني مطالباً منها بأن تقوم بإنتاج أغنية لإيران كما فعلت للكويت ولمصر (الغفيلي، ٢٠١٣، ص. ٥).

الطبيعة القانونية لجريمة الاختراق:

وهنا سنتطرّق إلى الحديث عن الجرائم الإلكترونية بشكل خاص والتي تدخل ضمن نطاق دراسة التشريعات الجزائية الخاصة بتلك الجرائم، فهذه التشريعات تكون مختصة بدراسة وتفصيل كل جريمة، ومتناولاً عناصرها الأساسية والعقوبة المقررة لها. إن دراسة الطبيعة القانونية للجرائم الإلكترونية، ومدى إمكانية اعتبارها من ضمن أنماط الجرائم التقليدية بحيث يتم بسط نصوص جريمة الدخول غير المشروع، والتي ذكرت في قانون العقوبات الأردني (١٦) لعام (١٩٦٠) والمطبّق في فلسطين والتي يمكن اعتبارها على أنها جريمة اختراق، وذلك من خلال الأخذ بالنموذج القانوني لمحل الجريمة، مع الإدراك أن جريمة اختراق المعلومات والبيانات المخزّنة في جهاز الحاسوب والإضرار بها وإتلافها هي من أكثر الجرائم المنتشرة في العصر الحديث.

بالرجوع إلى دراسة نصوص قانون العقوبات الأردني، والمطبّق في فلسطين، نجد أنه لم ينص في أي من مواده على تعريف للجرائم الإلكترونية، وهذا ما يظهر لنا أن المشرّع لما يواكب التطور التكنولوجي وما نتج عنه من جرائم حديثة، وهذا ما يشكل مشكلة في النظر بالجرائم الإلكترونية، وإيقاع العقوبات وفقاً للقانون المذكور أعلاه. وسنتطرق إلى قرار بقانون رقم (١٠) لعام (٢٠١٨) والمتعلق بالجرائم الإلكترونية، وإلى قانون رقم (٣) لعام (١٩٩٦) والمتعلق بالاتصالات السلكية واللاسلكية لذكر نصوص المواد التي تحدثت عن جريمة الاختراق أو الدخول غير المشروع والتي غالباً ما تؤدي إلى إتلاف البيانات والإضرار بها وبيان العقوبة المقررة لها.

ووفقاً للمادة (١٢٤) من قانون العقوبات الأدرني رقم (١٦) لعام (١٩٦٠) والمطبّق بفلسطين والتي تتحدث عن عقوبة الدخول إلى مكان محظور بقصد الحصول على وثائق مكتومة حيث نصّت على أنه: «من دخل أو حاول الدخول إلى مكان محظور قصد الحصول على أشياء أو وثائق أو معلومات، يجب أن تبقى مكتومة حرصاً على سلامة الدولة عوقب بالأشغال الشاقة المؤقتة، وإذا حصلت هذه لمنفعة دولة أجنبية، عوقب بالأشغال الشاقة المؤبدة. والمادة (١٢٦) من نفس القانون والتي تتحدث عن عقوبة إفشاء الوثائق والمعلومات المكتوبة دون سبب مشروع : «فأبلغها أو أفشاها دون سبب مشروع عوقب بالأشغال المؤقتة مدة لا تقل عن عشر سنوات، ويعاقب بالأشغال الشاقة المؤبدة إذا أبلغ ذلك لمنفعة دولة أجنبية. وإذا أردنا تطبيق تلك المادتين على جريمة الاختراق، فإنّ تلك المادتين تنظران فقط في الأماكن المحظورة من قبل الدولة، والأماكن من الوهلة الأولى تشمل العالم الحقيقي، ولا تشمل العالم الافتراضي، وجريمة الاختراق تتمثل في الدخول غير المشروع إلى المواقع الإلكترونية دون إذن صاحبها وما يترتب عليها من إضرار وإتلاف بالمعلومات والبيانات أو الإفشاء بها دون سبب مشروع، وقد يتمثل في الدخول غير المشروع مع عدم الإخلال بشيء ولكن مجرد الدخول والبقاء فيه يعتبر غير مشروع وبحد ذاته يعتبر جريمة اختراق، وإذا أردنا إيقاع العقوبة على مرتكب جريمة الاختراق وتطبيق تلك المادتين عليه فالعقوبة المقررة لها لا تتوافق على جسامة الخطورة الإجرامية لجريمة الاختراق.

وبالرجوع للقوانين الخاصة الفلسطينية، نجد أن القانون رقم (٣) لعام (١٩٩٦) والمتعلق بالاتصالات السلكية واللاسلكية، قد تحدّث ببعض نصوصه عن جريمة الاعتداء على مراسلات الآخرين عبر الوسائل الإلكترونية، ونصّت المادة (٩٢): «كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات، أو شجع غيره على القيام بهذا العمل، يعاقب بالحبس مدة لا تقل على شهر، ولا تزيد على ستة أشهر، أو بغرامة لا تقل عن ٥٠ ديناراً، ولا تزيد على (٢٠٠) دينار أو بكلتا العقوبتين».

وجريمة العبث بالبيانات المتعلقة بالمشتركين، حيث نصّت المادة (٩٣) من نفس القانون على أنه: «كلّ من أقدم على كتم رسالة عليه نقلها بواسطة شبكات الاتصال إلى شخص آخر، أو رفض نقل رسائل طلب منه نقلها سواء من قبل المرخص له أو الوزارة أو نسخ أو أفشى رسالة أو عبث بالبيانات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غير المعلنة والرسائل المرسلة أو المستقبلة، يعاقب بالحبس بمدة لا تزيد على ستة أشهر، أو بغرامة لا تزيد على (١٠٠٠) دينار أو بكلتا العقوبتين».

وخلاصة القول: إنّ هذا القانون يعالج الجرائم الواقعة على الاتصالات، ولا يعالج أي نوع من الجرائم الإلكترونية، كما أنّ القانون بحاجة الى إجراء تعديلات، لمواكبة التطور التقني والتقدم التكنولوجي في مجالات الاتصالات والتواصل، وبالتالي لا يمكن إسقاط مواد هذا القانون على الجرائم الإلكترونية بمختلف أنواعها لأنها تتعلّق بالاتصالات فقط.

وبالإطلاع على قرار بقانون رقم (١٠) لعام(٢٠١٨) والمتعلق بالجرائم الإلكترونية، فكما تم الإشارة إليه سابقاً أنّ المشرع عرّف الاختراق بأنه الدخول غير المشروع وما يترتب عليه من أضرار وإتلاف للبيانات والمعلومات، وسنستعرض في هذا القرار ببعض نصوص موادّه التي تحدث عن الاختراق. حيث نصت المادة (٤) على أنّه:

١- كلّ من دخل عمْداً دون وجه حقّ بأيّ وسيلة موقعاً إلكترونياً، أو نظاماً، أو شبكة إلكترونية، أو وسيلة تكنولوجيا معلومات، أو جزءاً منها، أو تجاوز الدخول المصرح به، أو استمرّ في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

٢- إذا ارتكب الفعل المذكور في الفقرة (١) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

٣- إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو حذفها، أو إضافتها، أو إفشاؤها، أو إتلافها، أو تغييرها، أو نقلها، أو التقاطها، أو نسخها، أو نشرها، أو إعادة نشرها، أو ألحق ضرراً بالمستخدمين، أو المستفيدين، أو تغيير الموقع الإلكتروني، أو إلغاؤه، أو تعديل محتوياته، أو شغل عنوانه، أو تصميماته، أو طريقة استخدامه، أو انتحال شخصية مالكه، أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقلّ عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

٤- إذا ارتكب الفعل المذكور في الفقرة (٣) من هذه المادة على البيانات الحكومية، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

من الملاحظ في الفقرة الأولى من هذه المادة أن المشرع الفلسطيني جرّم الفعل بمجرد الدخول أو الاطلاع على البيانات، وقد توسّع المشرع في مفهوم الفعل والوسيلة والنشاط، حيث قال بأن يتم الدخول بأيّ وسيلة كانت، وهذا يعني أن المشرع لم يحدد وسيلة معينة للدخول، وكذلك الأمر في الفقرة الأولى منه أيضاً أشار المشرع إلى «إذا استمر في الدخول بعد علمه...» أنه اشترط لكي يكون الفعل مجرّماً بأن يكون على علم بأنّ بقاءه في النظام أو الشبكة الإلكترونية هو غير مشروع.

ونصّت **المادة (٥)** منه على أنه: «كلّ من أعاق، أو عطل الوصول إلى الخدمة، أو الدخول إلى الأجهزة، أو البرامج، أو مصادر البيانات، أو المعلومات بأيّ وسيلة كانت عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

و**المادة (٦)** منه وضّحت على أنّ: «كلّ من أنتج، أو أدخل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل، أو تعطيلها، أو إتلاف البرامج، أو حذفها أو تعديلها، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

فيما نصّت **المادة (٤٧)** على أنّ: «كلّ من أقدم على العبث بأدلة قضائية معلوماتية، أو أقدم على إتلافها، أو إخفائها، أو التعديل فيها، أو محوها، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

وبالتدقيق في الجرائم التي ذكرها القرار بقانون والمتعلق بالجرائم الإلكترونية، نرى أن المشرع الفلسطيني لم يتطرق لذكر الجرائم الإلكترونية جميعها، وهذا ما يطرح تساؤلاً فيما إذا كان المشرع قد تطرق إلى الجرائم الأكثر شيوعاً؟ أم لكون المشرع ليس على دراية بمواكبة التطورات التكنولوجية المستمرة؟ وما ينجم عنها من جرائم إلكترونية جديدة.

في الحقيقة نجد أنّ المشرع الفلسطيني لم يتطرق إلى ذكر نوع معين من الجرائم الإلكترونية، وقد ذكر بعضها من باب التعريف فقط دون التوسع فيها مع بيان خطورة كل جريمة إلكترونية، ودون مواكبة للتطور التكنولوجي وما يترتب عليه ظهور نوع جديد من الجرائم الإلكترونية، وهذا ما يؤدي إلى إفلات بعض مرتكبي الجرائم الإلكترونية من العقاب، لكن المشرع الفلسطيني ذكر جريمة الاختراق بوجه صريح، وحدّد محلها على أنها تشمل المواقع والبيانات الشخصية أو الحكومية، كما تناول المشرع جريمة الاختراق بتعريف واضح وصريح.

الخاتمة

لقد تطرّق الباحث في هذا البحث إلى إحدى الجرائم الإلكترونية الخطرة، وهي جريمة الاختراق، حيث إنّ هذه الجريمة تنشأ في بيئة إلكترونية، وترتبط ارتباطاً وثيقاً بالتطور والتقدم التكنولوجي، وتجدر الإشارة إلى أنّ المشرع الفلسطيني جرّم جريمة الدخول غير المشروع أو غير المصرح به، وهو ما يتّفق مع تعريف جريمة الاختراق وبالتالي يمكن القول: إنّه تفرّد بجريمة الاختراق وبين العقوبة المقررة لها في مع بيان الحالة التي تتم فيها عملية الاختراق ومن يقوم بها.

وتوصل الباحث من خلال بحثه إلى جملة من النتائج والتوصيات ومن أهمها:

١. إنّ الجرائم الإلكترونية ظهرت وانتشرت بشكل سريع مع التقدم والتطور التكنولوجي المتسارع.

٢. إنّ جريمة الاختراق، جريمة صامتة تتم بالخفاء، ولا تترك أي أثر مادي، فهي تمتاز بذوبانها السريع، واختفائها العجيب، مما شكل صعوبة بالغة في محاولة كشفها.

٣. يعدّ جهاز الحاسوب -في الجريمة الإلكترونية- هو الأداة، وشبكة الإنترنت مسرح الجريمة، بينما في الجريمة التقليدية قد تكون سلاحاً أبيضَ كالسكين، وقد تكون سلاحاً نارياً، ومسرح الجريمة في الجريمة التقليدية قد يكون مكاناً عامّاً، وقد يكون داخل شقة في عمارة، وقد يكون داخل إحدى غرف المنزل.

٤. تعدّ جريمة الاختراق جريمة قائمة بحد ذاتها، فبمجرد الدخول والبقاء غير المشروع، حتى ولو لم يقم بأيّ عمل تخريبي، كتعطيل نظام الحاسب الآلي، أو تدمير البيانات، أو إتلافها.

٥. إنّ المستخدم الذي يكون له تصريح وصلاحية الدخول والإطلاع على المعلومات، حيث إنّه إذا تجاوز التصريح الخاص بالدخول والإطلاع على المعلومات، أو استمرّ بالتواجد أكثر من المدة المحددة في التصريح الخاص له مع علمه بذلك، فالجريمة تكون قائمة، والهدف من ذلك أن المشرع أراد إيجاد حماية للشبكات والأنظمة المعلوماتية المخزنة عليها.

ويوصي الباحث بما يأتي:

١. إن القرار بقانون بشأن الجرائم الإلكترونية رقم (١٠) لسنة (٢٠١٨). بيّن الجرائم الإلكترونية، وأوقع العقوبة لكل جريمة.

٢. إيجاد أجهزة مختصّة لملاحقة مرتكبي الجرائم الإلكترونية.

٣. إقامة الدورات التدريبية لرجال الشرطة وأعضاء النيابة العامة والقضاء، وللأجهزة المختصة، وعقد الندوات العلمية المختصة بالجرائم الإلكترونية، وإعداد ورش عمل مستمرة، لمحاربة هذه الجريمة، من أجل الحد من مخاطرها المترتبة عليها.

٤. تعزيز التعاون على المستويين الوطني والدولي في مجال مكافحة الجرائم الإلكترونية.

قائمة المراجع

- ابن منظور، محمد بن مكرم. (١٩٩٠): (ت٧١١هـ\١٣١١م)، معجم لسان العرب، مج١٢، ط ٣، دار صادر للنشر والتوزيع، بيروت، لبنان.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية لعام (٢٠١٠).
- إسماعيل، أيمن،خبر بعنوان دوافع الجريمة في المجتمع الفلسطيني، موقع دنيا الوطن، تاريخ النشر(٢٧\٣\٢٠١٢م).
- جامعة الدول العربية، المركز العربي للبحوث القانونية (٢٠١٢)،الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات المنعقد في(٥-٧/٣/٢٠١٢) بيروت، الجمهورية اللبنانية، ص٦-٧، متاح على الرابط التالي https://carjj.org/node/1242.
- الجريمة الالكترونية في فلسطين مباحة، مقال منشور على https://cutt.us/Y2noU، تاريخ الدخول (٣/٥/٢٠١٩).
- حجازي، عبد الفتاح، (٢٠٠٢). الدليل الجنائي والتزوير في جرائم الكمبيوتر، ط1، دار الفكر الجامعي، الأسكندرية، مصر.
- خبر منشور على جريدة الشرق الأوسط تحت عنوان «قائد قيادة الإنترنت في البنتاغون يحذر من هجوم إلكتروني يشل واشنطن، تاريخ النشر (٢٥/٩/٢٠١٠).
- خبر نشر على موقع الجزيرة، اختراق وكالة الأنباء القطرية تم من الإمارات، http://www.aljazeera.net/portal.
- خلف، سامية، (٢٠١٠). بحث بعنوان «جريمة اختراق أنظمة المعلومات دراسة مقارنة»، مجلة العلوم القانونية، جامعة بغداد.
- الدنف، أيمن، (٢٠١٣). واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، رسالة ماجستير غير منشورة، الجامعة الإسلامية، كلية التجارة ، غزة، فلسطين.

رسائل الماجستير

- رمضان، مدحت، (٢٠٠١). الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، مصر.
- سرور، أحمد، (٢٠٢٢). الوسيط في قانون العقوبات، القسم العام، ج١، دار الاهرام للنشر والتوزيع، مصر، القاهرة.
- سعيداني، نعيم، (٢٠١٣). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر غير منشورة، جامعة الحاج لخضر باتنة، الجزائر.
- سندالي، عبد الرازق، مداخلة بعنوان «التشريع المغربي في مجال الجرائم المعلوماتية»، قدمت لندوة تحت عنوان الجرائم المتصلة بالكمبيوتر، المملكة المغربية، تاريخ الإنعقاد (١٩\٦\٢٠٠٧).
- عبدالله، نوري، (٢٠١١). بحث منشور بعنوان «العوامل الإجتماعية المؤثرة في ارتكاب الجريمة»، مجلة الأنبار للعلوم الإنسانية، ع١.
- عمار، زكريا، (٢٠١١). حماية الشبكات الرئيسية من الاختراق والبرامج الضارة، رسالة ماجستير غير منشورة، جامعة النيلين، كلية الدراسات العليا، السودان.
- العنزي، فهد، مقال بعنوان» اختراق المواقع الإلكترونية والتأمين»، الاقتصادية جريدة العرب الاقتصادية الدولية، https://www.aleqt.com/2011/08/08/article_567334.html, تاريخ النشر(٨/٨/٢٠١١).
- غايب، محروس، (٢٠١١). الجريمة المعلوماتية، بحث منشور في مجلة التقني، هيئة التعليم التقني، مج٢٤، ع٩، الأنبار، العراق.
- الغفيلي، فهد، دورة تدريبة حول توظيف التقنيات الحديثة في العمل الأمني، مداخلة بعنوان «استخدام الحاسب الآلي في الوقاية من الجريمة (جرائم الاختراق نموذجاً)»، جامعة نايف العربية للعلوم الأمنية، تاريخ الانعقاد(٦-١٣\٣\٢٠١٢).
- فتحية، رصاع، (٢٠١٢). الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماستر غير منشورة، جامعة أبي بكر بلقايد، تلمسان، الجزائر.
- قرار بقانون بشأن الجرائم الالكترونية، رقم (١٠) لسنة (٢٠١٨).
- القرآن الكريم.
- مزغيش، سمية، (٢٠١٤). جرائم المساس بالأنظمة المعلوماتية، مذكرة ماستر غير منشورة، جامعة محمد خيضر بسكرة.
- مصطفى، محمود، (١٩٦٩). قانون العقوبات، القسم العام، ط٨، دار النهضة العربية، القاهرة، مصر.
- موقع معجم المعاني، https://www.almaany.com.
- المومني، نهلا، (٢٠١٠). الجرائم المعلوماتية، ط٢، دار الثقافة للنشر والتوزيع، عمان ، الأردن.
- نجم، محمد، (٢٠١٢). قانون العقوبات القسم العام النظرية العامة للجريمة، ط٤، دار الثقافة للنشر والتوزيع، عمان، الأردن.
- نصار، غادة، (٢٠١٧). الإرهاب والجريمة الالكترونية، دار العربي للنشر والتوزيع، القاهرة، مصر.
- ياسمينة، بونغارة، (٢٠١٥). الجريمة الالكترونية، مذكرة ماستر منشورة، جامعة الأمير عبد القادرة للعلوم الإسلامية، الجزائر.