الجامعة العربية الأمريكية

كلية الدراسات العليا

قسم العلوم القانونية

برنامج الماجستير في العلوم الجنائية

جريمة انتحال الشخصية الإلكترونية وفقاً للقرار بقانون بشأن الجرائم الالكترونية الفلسطيني "دراسة تحليلية "

ثائر خضر احمد بني عوده

202020332

أسماء لجنة الإشراف:

د. عبد اللطيف ربايعة

د. عصام الأطرش

د. أحمد الاشقر

تم تقديم هذه الرسالة استكمالاً لمتطلبات درجة الماجستير في تخصص العلوم الجنائية

فلسطين، 12/ 2024

© الجامعة العربية الأمريكية، جميع حقوق الطبع محفوظة

الجامعة العربية الأمريكية

كلية الدراسات العليا

قسم العلوم القانونية

برنامج الماجستير في العلوم الجنائية

صفحة إجازة الرسالة

جريمة انتحال الشخصية الإلكترونية وفقاً للقرار بقانون بشأن الجرائم الالكترونية الفلسطيني "دراسة تحليلية "

ثائر خضر احمد بني عوده

202020332

نوقشت هذه الرسالة وأجيزت بتاريخ 28 / 12 / 2024 من لجنة المناقشة التالية أسمائهم وتواقيعهم:

الاسم		التوقيع
1. د. عبد اللطيف ربايعة	المشرف الرئيس	
2. د. عصام الاطرش	عضو لجنة الرسالة	
3. د. احمد الاشقر	عضو لجنة الرسالة	

فلسطين، 12 / 2024

الإقرار

أنا الموقع أدناه مقدم الرسالة الموسومة:

جريمة انتحال الشخصية الإلكترونية وفقاً للقرار بقانون بشأن الجرائم الالكترونية الفلسطيني "دراسة تحليلية "

أقر بأن ما اشتملت عليه الرسالة إنما هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وإن هذه الرسالة ككل، أو جزء منها لم يقدم من قبل لنيل درجة علمية أو بحث لدى أي مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: ثائر خضر أحمد بني عودة

الرقم الجامعي: 202020332

التوقيع: ثائر بني عودة

تاريخ تسليم النسخة النهائية من الرسالة: 29-6-2025

الإهداء

وجد الإنسان على وجه البسيطة، ولم يعش بمعزل عن باقي البشر

إلى من أُفضِلها على نفسي، ولِمَ لا؛ فلقد ضحَّت من أجلي

ولم تدَّخر جُهدًا في سبيل إسعادي على الدَّوام

(أُمِّي الحبيبة).

كم كنت تتمنى ان تمر هذه الايام وانت تشاهد وتتلمس هذا النجاح والسعادة الى روحك الطيبة أجمل اهداء (ابي الغالي)

وفي كل المراحل من الحياة، يُوجد أُناس يستحقُّون منَّا الشُّكر

وأولى الناس بالشُّكر هما الأبوان؛ لما لهما من الفضل ما يبلغ عنان السماء؛

فوجودهما سبب للنجاة والفلاح في الدينا والآخرة.

إلى زوجتي ورفيقة الكفاح في مسيرة الحياة

الى فلذات كبدي ابنائي وسندي في هذا الدهر القاصي

إلى أصدقائي الذين أشهد لهم بأنهم نعم الرُّفقاء في جميع الأمور..

أُهديكم جميعا بحثي المُتواضع.

ثائر خضر أحمد بني عودة

الشكر والتقدير

بعد رحله بحث وجهد واجتهاد تكللنا بإنجاز هذا البحث والرسالة، نحمد الله عز وجل على النعمة التي من بها علينا فهو العلي القدير، كما لا يسعنا الا ان نخص باسمي عبارات الشكر والتقدير للدكتور الغالي (عبد اللطيف ربايعة) لما قدمه لي من جهد ونصح ومعرفه طيلة انجاز هذا البحث فلولا الله ثم وجوده لما احسست بمتعه العمل وحلاوة البحث وليونه الجد والاجتهاد ولما وصلنا الى ما وصلنا اليه فله كل الشكر والتقدير.

كما لابد لنا ان نتقدم بأجمل عبارات الشكر والعرفان الى رئيس القسم الدكتور (احمد الأشقر) وبقيه الأساتذة ومن له منهم علينا حقا والى كادر الجامعة فردا فردا فلكم مني جميعا كل الشكر والتقدير.

جريمة انتحال الشخصية الإلكترونية وفقاً للقرار بقانون بشأن الجرائم الالكترونية الفلسطيني "دراسة تحليلية "

ثائر خضر احمد بني عوده

د. عبد اللطيف ربايعة

د. عصام الاطرش

د. أحمد الاشقر

ملخص

تناولت هذه الدراسة جريمة انتحال الشخصية الإلكترونية، من الناحية الموضوعية والناحية الإجرائية، وهدفت هذه الدراسة إلى بيان المقصود بتلك الجريمة، وتوضيح الأركان الواجب توافرها فيها، والتعرف على صورها، وبيان كيف قام المشرع الفلسطيني بتنظيم أحكامها وفرض عقوبات على مرتكبيها، وتوضيح الإجراءات المتبعة في ضبط الأدلة المستعملة في ارتكاب هذه الجريمة، وبيان إجراءات التحقيق والمحاكمة فيها.

واستخدم الباحث في هذه الدراسة المنهج الوصفي التحليلي ومنهج البحث المقارن، من خلال عرض المناهج التشريعية الناظمة لعقوبة انتحال الشخصية الالكترونية.

وقد توصل الباحث إلى عدد من النتائج، كان أبرزها أن جريمة انتحال الشخصية الإلكترونية تتمثل في ادعاء شخص ما بأنه شخص آخر وذلك من خلال ظهوره أمام الأخرين بشخصية منتحلة، وأن المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية نص على تجريم انتحال الشخصية الإلكترونية وفرض عقوبة على مرتكبيها، وساوى بين عقوبة مرتكب هذه الجريمة الأصلي، وبين عقوبة من يشترك معه في ارتكابها.

وقد خلص الباحث إلى عدد من التوصيات، منها ضرورة رفع وتشديد العقوبة المقررة على جريمة انتحال الشخصية الإلكترونية نظراً لخطورتها.

الكلمات المفتاحية: انتحال، الشخصية الالكترونية، الجرائم الإلكترونية، أركان الجريمة، عقوبة جريمة الانتحال

فهرس المحتويات

الإقرار ..... أ

الإهداء..... ب

الشكر والتقدير ..... ت

ملخص ..... ث

المقدمة 1

أهمية الدراسة..... 1

مشكلة الدراسة..... 2

أهداف الدراسة..... 3

منهجية الدراسة..... 3

خطة الدراسة..... 3

الفصل الأول: احكام القواعد الموضوعية لجريمة انتحال الشخصية الالكترونية. 4

المبحث الأول: ماهية جريمة انتحال الشخصية الالكترونية..... 4

المطلب الأول: مفهوم انتحال الشخصية الالكترونية..... 5

المطلب الثاني: خصائص جريمة انتحال الشخصية الالكترونية وتمييزها عن غيرها من الجرائم:
..... 9

المبحث الثاني: أركان جريمة انتحال الشخصية الالكترونية..... 21

المطلب الأول: الركن الشرعي 21

المطلب الثاني: الركن المادي..... 25

المطلب الثالث: الركن المعنوي..... 31

الفصل الثاني: القواعد الإجرائية لجريمة انتحال الشخصية الإلكترونية..... 34

المبحث الأول: إجراءات التحري والتحقيق في جريمة انتحال الشخصية الالكترونية. 35

المطلب الأول: إجراءات الاستدلال في جريمة انتحال الشخصية الالكترونية.....36
المطلب الثاني: إجراءات التحقيق في جريمة انتحال الشخصية الالكترونية. 50
المبحث الثاني: إجراءات المحاكمة والاثبات في جريمة انتحال الشخصية الالكترونية والعقوبة المقررة لها. 64
المطلب الأول: إجراءات المحاكمة في جريمة انتحال الشخصية الإلكترونية وعقوبتها المقررة. 65
المطلب الثاني: إجراءات الاثبات في جريمة انتحال الشخصية الإلكترونية.....71
الخاتمة 76
أولاً: النتائج: 76
ثانياً: التوصيات:.....77
المراجع 78
Abstract:.....86

المقدمة

يشهد الوقت الراهن ثورة تكنولوجية كبيرة، أثرت بشكل مباشر في حياة الإنسان شكلاً ومضموناً، وعملت على خلق بيئة اجتماعية جديدة، يطلق عليها البيئة الرقمية أو الالكترونية، وكان من نتائجها المباشرة أنها أصبحت أداة للكثير من العلاقات ولممارسة العديد من الأنشطة، وعلى الرغم من المزايا الكثيرة الناتجة عن التطور العلمي الهائل، إلا أنه ترتب عليها مخاطر عدة ناجمة عن إساءة استخدام شبكة المعلومات الدولية وتطويعها لصالح المجرمين لممارسة نشاطاتهم الجرمية، حيث أسهمت في ظهور طائفة جديدة من الجرائم المستحدثة، ومن بينها جريمة انتحال الشخصية الإلكترونية.

وتعد جريمة انتحال الشخصية الإلكترونية من أكثر الجرائم المعلوماتية التي تُرتكب على نطاق واسع في مختلف دول العالم، وتسبب خسائر اقتصادية فادحة، الأمر الذي يُشكل قلقاً متزايداً لدى المعنيين بالأمر، إذ إن هذه الجريمة تهدد ثقة الأفراد بالوسائل التقنية المستحدثة لنقل الأموال والمعلومات، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، من بيانات ومعلومات وبرامج بكافة أنواعها، فهي جريمة تقنية تنشأ في الخفاء، ويتميز مرتكبوها بالذكاء، ويمتلكون أدوات المعرفة التقنية ويقومون باستغلال هذه المعرفة من أجل الاعتداء على برامج الحاسوب، واحتيال شخصية وصفة الغير.

وقد تنبه المشرع الفلسطيني لخطورة المجال الافتراضي " العالم الإلكتروني" وعالج الكثير من المسائل التي تتعلق بالجرائم الإلكترونية في القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وتعديلاته، ومن ضمنها جريمة انتحال الشخصية الإلكترونية والتي تعتبر جريمة من بين أهم الجرائم لما تشكله من خطورة كبيرة تتمثل في الإساءة لصاحب الشخصية الإلكترونية وطمس للحقائق، مما دعا المشرع الفلسطيني لفرض عقوبات على مرتكب هذا النوع من الجرائم.

أهمية الدراسة

تكمن أهمية هذه الدراسة من خلال بيان ماهية جريمة انتحال الشخصية الإلكترونية ومعرفة وسائلها وأركانها، وبيان النصوص الجزائية لجريمة الانتحال بصورتها التقليدية ومدى انطباقها على جريمة الانتحال عبر شبكة المعلومات الدولية. كذلك تبرز الأهمية في مواكبة سرعة تطور الصور الجرمية المتمثلة في انتحال الشخصية الالكترونية وانتشارها، وخطورة الآثار والأضرار

الجرمية المترتبة عليها على الفرد والجماعة.

كما للبحث أهمية من الناحية العملية كون أن موضوعه يعد موضوع حيوي شديد الصلة بالواقع، فموضوع البحث يعالج موضوع انتشر بصورة كبيرة في المواقع الالكترونية ومواقع تواصل الاجتماعي، وهو استعمال انتحال الشخصية للنصب على الآخرين، والاستيلاء على أموالهم.

كما أن لهذه الدراسة اهمية كبيرة نظراً لقلة الدراسات الفقهية القانونية التي تناولت جرائم انتحال الشخصية الالكترونية، وعدم كفاية الدراسات السابقة في الإحاطة بدراسة كافة جوانبها.

مشكلة الدراسة

تكمن مشكلة الدراسة في بروز جريمة انتحال الشخصية الإلكترونية واستغلال جانب من الجناة للثورة التكنولوجية في مجال الاتصالات الالكترونية في ارتكاب هذه الجريمة، خصوصاً أن معظم مستخدمي الاتصالات الإلكترونية يجهلون التعامل السليم مع هذه التقنية فيقعون فريسة للمنتحلين الذي يقومون باستغلال الضحايا والنصب عليهم، علاوة على سهولة ارتكاب هذه الجريمة لأنها ترتكب عن بعد فهي متخطية للحدود الجغرافية ويمكن أن تُرتكب من أي مكان في العالم ، وكذلل بالوسائل التي يمكن إثبات الجريمة من خلالها إضافة الى العقوبات المفروضة عليها .

ويمكن طرح مشكلة الدراسة من خلال التساؤل الرئيسي التالي: " ما هي جريمة انتحال الشخصية الالكترونية في التشريع الفلسطيني، وما مدى كفاية النصوص القانونية في القرار بقانون بشأن الجرائم الإلكترونية لمواجهة ومكافحة انتحال الشخصية الالكترونية؟"

ويتفرع عن التساؤل الرئيسي التساؤلات الفرعية التالية:

1- ما المقصود بجريمة انتحال الشخصية الإلكترونية، وما الفرق بينها وبين الجرائم الشبيهة بها؟
2- ما هي الأركان الواجب توافرها لقيام جريمة انتحال الشخصية الإلكترونية؟
3- ما هي صور جريمة انتحال الشخصية الإلكترونية؟
4- كيف عالج المشرع الفلسطيني جريمة انتحال الشخصية الإلكترونية، وما هي العقوبة التي رتبها على ذلك؟

أهداف الدراسة

1- بيان مفهوم جريمة انتحال الشخصية الإلكترونية.

2- توضيح الفرق بين جريمة انتحال الشخصية الإلكترونية والجرائم الشبيهة بها.

3- شرح الأركان الواجب توافرها في جريمة انتحال الشخصية الالكترونية.

4- ذكر صور جريمة انتحال الشخصية الالكترونية.

5- بيان التنظيم القانوني لجريمة انتحال الشخصية الالكترونية، والعقوبة التي فرضها المشرع الفلسطيني عليها.

منهجية الدراسة

سنتبع في هذه الدراسة المنهج الوصفي التحليلي، من خلال عرض المناهج التشريعية الناظمة لعقوبة انتحال الشخصية الالكترونية وسيجنح الباحث حيث يلزم الى المنهج المقارن مع بعض القوانين.

خطة الدراسة

سوف نتناول في الفصل الأول من هذه الرسالة أحكام القواعد الموضوعية لجريمة انتحال الشخصية الالكترونية، من حيث بيان مفهوم تلك الجريمة وما يميزها عن غيرها من الجرائم وبيان أركانها وخصائصها.

أما الفصل الثاني سنتناول فيه القواعد الاجرائية لجريمة انتحال الشخصية الالكترونية، من حيث الية التحقيق حول هذه الجريمة وجمع الأدلة والتفتيش عليها، وكيفية إثبات تلك الجريمة أمام القضاء الجزائي.

الفصل الأول: أحكام القواعد الموضوعية لجريمة انتحال الشخصية الالكترونية.

تُعد جرائم انتحال الشخصية الإلكترونية من أكثر الجرائم التي يمكن أن تؤثر تأثيراً سلبياً على الأشخاص والبنية المؤسسية، وتهدد أمن وسلامة واستقرار الضحية سواء كانت شخصاً طبيعياً أو اعتبارياً، فرداً أو مؤسسة أو دولة؛ حيث أن الانتحال يجعل الجاني وكأنه الشخص أو المؤسسة ذاتها التي قام بالاستيلاء على اسمها، بكل ما يترتب على ذلك من تداعيات خطيرة تضر بمصالح الضحية والمتعاملين معها.

تتناول الدراسة في هذا الفصل بيان ماهية جريمة انتحال الشخصية الإلكترونية (المبحث الأول) وتتناول كذلك أركان تلك الجريمة (المبحث الثاني)

المبحث الأول: ماهية جريمة انتحال الشخصية الالكترونية.

تعد جرائم انتحال الشخصية الإلكترونية من الجرائم المستحدثة، وهي خلف وامتداد لجريمة الانتحال التقليدية والتي استفادت من التقنيات الحديثة في مجالات الاتصال والحوسبة لتلد هذه الصورة المعاصرة من جريمة الانتحال.

وتعد جريمة انتحال الشخصية الإلكترونية من الجرائم الإلكترونية التي تستهدف بيانات لأشخاص أو مؤسسات؛ وذلك بهدف جلب منافع مالية أو لانتحال الشخصية الإلكترونية، فهي تشمل أنشطة اقتحام أو الدخول أو تجاوز الحد المسموح به أو الاتصال غير المرخص به مع نظام إلكتروني أو الشبكة المعلوماتية وتخريب البيانات والنظم والممتلكات وخلق البرمجيات الخبيثة الضارة ونقلها عبر النظم والشبكات واستخدام العلامة التجارية أو اسم الغير دون ترخيص[1].

وقد وفر القانون الفلسطيني الحماية الجزائية على جريمة انتحال الشخصية الإلكترونية في القرار بقانون قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، وقد هدف المشرع من تجريم هذه الجريمة لمنع الجناة من استغلال أي بيانات إلكترونية تعود لشخص ما على الإنترنت، ومنع المحتالين من استخدام أسماء كاذبة ومن ثم استخدام تلك الأسماء والمعلومات في خداع المجني عليهم ووقوعهم كضحايا في شباك منتحل الشخصية.

[1] زيد بني خالد، التنظيم القانوني لجريمة انتحال الشخصية الإلكترونية وفقا لقانون الجرائم الإلكترونية الأردني، رسالة ماجستير، كلية الحقوق، جامعة جرش، 2021م

في هذا المبحث سيوضح الباحث مفهوم انتحال الشخصية الالكترونية (المطلب الأول) ثم يبين خصائص تلك الجريمة والفرق بينها وبين الجرائم المشابهة لها (المطلب الثاني)

المطلب الأول: مفهوم انتحال الشخصية الالكترونية.

في هذا المطلب سيوضح الباحث المقصود بانتحال الشخصية الإلكترونية في اللغة والاصطلاح، ومن ثم سيبين أهم الخصائص التي تتميز بها جريمة انتحال الشخصية الإلكترونية.

الفرع الأول: تعريف انتحال الشخصية الالكترونية لغة:

الانتحال في اللغة من قولهم انتحل الشيء إذا ادعاه لنفسه وهو لغيره[2].

وجاء في لسان العرب لابن منظور: نَحِل جسمه، ونَحَل، يَنحل، ويَنحُل نُحولاً، فهو ناحل: ذهب من مرض أو سفر والفتح أفصح. وانتحل فلان شعر فلان أو قول فلان إذا ادعاه أنه قائله، وتنحله: إذا ادعاه وهو لغيره، ونَحَله القول يَنحَله نَحلاً: نسبه إليه [3].

وجاء في معجم مقاييس اللغة لابن فارس: " نَحَلَ: النون والحاء واللام كلمات ثلاث: الأولى تدل على دِقة وهُزال والأخرى على عطاء والثالثة على ادعاء. الأولى نَحَل جسمه نُحولاً فهو ناحل، إذا دقّ، وأنحله الهم. والنواحل: السيوف التي رقت ظُباتُها من كثرة الضرب بها. والثانية: نَحلتُه كذا، أي أعطيته، والاسم النُّحل. والثالثة قولهم: انتحل كذا، إذا تعاطاه وادعاه. وقال قوم: انتحله إذا ادعاه مُحقاً، وتنحَّله إذا ادعاه مُبطلاً[4].

يتضح مما سبق أن الانتحال في اللغة يطلق على ادعاء الشيء للنفس وهو للغير، وعلى الإلزام، وعلى الهبة.

---

[2] محمد بن يعقوب الفيروزابادي، القاموس المحيط، تحقيق: مكتب تحقيق التراث في مؤسسة الرسالة، مؤسسة الرسالة، بيروت، الطبعة الثامنة، 2005م، ص 1061، مادة (نحل)

[3] محمد بن مكرم ابن منظور، لسان العرب، الجزء 11، المطبعة الأدبية ببولاق، مصر، الطبعة الأولى، 1888م، ص650.

[4] ابن فارس، معجم مقاييس اللغة، تحقيق عبد السلام هارون، دار الفكر للنشر والتوزيع، بيروت، 1979م، ص 402.

وأما الشخصية ففي اللغة هي صفات تميز الشخص عن غيره، وهي مشتقة من كلمة شخص، والشخص يعرف باللغة بأنه: جماعة شخص الانسان وغيره، والمراد باللفظ إثبات الذات فاستعير لها لفظ الشخص[5].

الفرع الثاني: تعريف انتحال الشخصية الالكترونية اصطلاحاً:

يعرف الانتحال بمفهومه العام بأنه: " أن يدعي المتهم لنفسه شخصية غيره[6]" كما عرفها البعض بأنها: " ادعاء شخص أو أكثر شيئاً ما بطريق خفي ليوهم الناس أنه الحقيقة المعهودة[7]" كما تعرف بأنها: "أن يقوم شخص بالاستيلاء على بعض البيانات الشخصية لشخص أخر، ثم يقوم باستخدام تلك المعلومات من أجل تقمص شخصية الشخص الآخر من أجل أغراض مالية أو غيرها [8]"

أما جريمة انتحال الشخصية الإلكترونية فيمكن تعريفها بأنها: " السلوك المحظور الذي يتم من خلاله تقمص شخصية الكترونية على دون الحقيقة والتي يعاقب عليها القانون[9] "

كما يمكن تعريف انتحال الشخصية الإلكترونية بأنها: " الظهور أمام الغير بمظهر الذي تم انتحال شخصيته وبالتالي يوهم المتعامل معه أو الناظر إليه على أنه نفس الشخص الذي تم انتحال شخصيته عبر الشبكة المعلوماتية[10] "

---

[5] ابن منظور، مرجع سابق، ص 650.

[6] أحمد عبد السلام علي، التعليق على جرائم التزييف والتزوير في قضاء العقوبات في ضوء الفقه والقضاء، دار الكتب القانونية، مصر، 2007م، ص121.

[7] ولاء البياري، انتحال الشخصية في الفقه الإسلامي، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2018م، ص11.

[8] عبد العزيز الشبل، الاعتداء الإلكتروني (دراسة فقهية) دار كنوز إشبيليا، الرياض، الطبعة الأولى، 2012م، ص 407

[9] دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، بحث مقدم للمؤتمر العلمي الرابع لكلية الحقوق جامعة طنطا تحت عنوان (القانون والإعلام) المنعقد في 23-24 إبريل 2017م، ص 16.

[10] زيد بني خالد، التنظيم القانوني لجريمة انتحال الشخصية الإلكترونية وفقا لقانون الجرائم الإلكترونية الأردني، رسالة ماجستير، كلية الحقوق، جامعة جرش، 2021م، ص15.

وبعد إطلاع الباحث على القوانين الجنائية المطبقة في فلسطين ولاسيما القرار بقانون قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، فإنه لم يجد تعريف صريح لجريمة الانتحال سواء بشكلها التقليدي أو بشكلها التقني، ونفس الأمر ينطبق على غالبية القوانين المقارنة التي لم تقم بتوضيح مفهوم جريمة الانتحال وتركت مهمة تعريفه للفقه.

فجريمة الانتحال هي ما يتعمد الفاعل القيام به دون وجه حق من استخدام هوية شخص أخر للإفادة من سمعته أو صلاحياته، وتتخذ جريمة انتحال الهوية عبر الانترنت أحد وجهين: انتحال هوية الفرد أو انتحال هوية المواقع، ووصفها المختصون بجريمة الألفية الجديدة نتيجة لسرعة تزايد وانتشار ارتكابها[11].

يتضح من التعريفات السابقة لانتحال الشخصية الإلكترونية أنه يمكن القيام بانتحال الشخصية من خلال الحصول على البيانات الشخصية لفرد ما؛ حيث عرفت المادة (4) من النظام العام الأوربي لحماية المعطيات الشخصية البيانات الشخصية بأنها: ".. أي معلومات تتعلق بشخص طبيعي معرف أو قابلاً لتعرف عليه، ويعتبر شخصاً قابلاً للتعرف كل شخص طبيعي يمكن معرفته بشكل مباشر أو غير مباشر، وعلى وجه الخصوص بالرجوع إلى عنصر معرف، مثل الاسم ورقم التعريف وبيانات الموقع ومعرف الاتصال عبر الانترنت أو لواحد أو أكثر من العناصر المميزة لهويته الفيزيولوجية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية[12] " فيقوم المنتحل بالاستيلاء على تلك البيانات الشخصية بهدف انتحال صفة ذلك الشخص والقيام بسلوكيات جرمية متعددة من خلال استخدام اسمه، إلى جانب المعلومات الأساسية مثل الاسم، رقم الهاتف، والعنوان الشخصي .

والجدير بالإشارة أن الشخصية الإلكترونية مرتبطة بشكل وثيق بما يعرف بالهوية الإلكترونية، حيث من المفترض أن يكون لكل شخص الكتروني هوية، وتعرف الهوية الإلكترونية بأنها : " اسم حقيقي أو مستعار، يفرد ويخصص على الإنترنت، ويسمح بتعيين صاحبه وتحديد مكانه الجغرافي أو المادي، ويتم تعين الهوية الإلكترونية باستخدام أداتين أولهما اسم المجال، وثانيهما

[11] زيد بني خالد، مرجع سابق، ص17.

[12] انظر: المادة (4) من النظام العام الأوربي لحماية المعطيات الشخصية.

العنوان الإلكتروني[13]" لكن مع انتشار الإنترنت وظهور المجتمعات الافتراضية، برزت مشكلات انتحال الشخصيات الافتراضية من حيث السن والأنوثة والذكورة والدور الاجتماعي وغير ذلك من المعلومات الشخصية لمستخدمي الإنترنت. وقد تعزز مفهوم الهوية الإلكترونية نتيجة للانتشار المتزايد للحكومات الإلكترونية والتي تتعامل بالبيانات الشخصية التي يتم من خلالها تحديد هوية الأشخاص المختلفة، إذ تطور استخدامها في التعاملات المالية سواء في الوزارات أو المؤسسات المختلفة إضافة إلى استخدامها في التصويت في الانتخابات. [14]"

يتبين مما سبق أن الأساس التي تقوم عليه جريمة انتحال الشخصية الإلكترونية هو ادعاء شخص ما بأنه شخص أخر وذلك عن طريق ظهوره أمام الغير بالشخصية المنتحلة، بحيث من يتعامل معه لن يراوده الشك بأنه لا يتعامل مع الشخص الحقيقي، وغايته من انتحال شخصيته تكون غالباً لتحقيق غايات ومكاسب شخصية أو بقصد الإضرار بمن انتحل شخصيته أو لخلل في شخصيته ورغبة في إشباع الشعور بالنقص.

وتجدر الإشارة إلى أن المشرع قد هدف من العقاب على جريمة انتحال الشخصية الإلكترونية المتمثل بالاسم الكاذب، والصفة غير الصحيحة كوسائل جرمية، أن مقتضيات حسن النية والسماحة في التعامل تقتضي ألا يطالب الناس بعضهم بالتحقق من شخصية وصفة من يتعاملون معه بإبراز ما يثبت صحة اسم الفرد أو صفته وفق معيار الشخص العادي، رغم أن البعض يأخذ منحنى متشدداً للاشتياق من اسم وصفة من يتعامل معه كشخص حريص، والأحكام القانونية الجزائية في أغلبها مبينة على معيار الشخص المعتاد لا بالغ الذكاء[15].

---

[13] صابر عبد العزيز سلامة، العقد الإلكتروني، دار النهضة العربية، القاهرة، الطبعة الثانية، 2007م، ص 27.

[14] صابر عبد العزيز سلامة، مرجع سابق، ص 27.

[15] خليل إعبية، القالب التشريعي لجرائم انتحال الصفة والشخصية الإلكتروني: دراسة مقارنة، مجلة العلوم الإنسانية والإدارية، جامعة المجمعة، العدد 22، 2021م، ص91.

المطلب الثاني: خصائص جريمة انتحال الشخصية الالكترونية وتمييزها عن غيرها من الجرائم:

في هذا المطلب سيستعرض الباحث أبرز الخصائص التي تتمتع بها جريمة انتحال الشخصية الإلكترونية، ومن ثم سيبين الفرق بينها وبين الجرائم المشابهة لها مثل جريمة التزوير والاحتيال وانتحال الصفة الإلكترونية.

الفرع الأول: خصائص جريمة انتحال الشخصية الالكترونية:

من خلال تعريفات جريمة انتحال الشخصية الإلكترونية يتبين أن لتلك الجريمة العديد من الخصائص التي قد تكون خصائص مشتركة لأغلب الجرائم المعلوماتية وهي كما يلي:

أولاً: جريمة انتحال الشخصية الالكترونية متعدية الحدود:

ففي جريمة انتحال الشخصية الالكترونية غالباً ما يكون الجاني في بلد والمجني عليه في بلد أخر، كما قد يكون الضرر المتحصل في بلد ثالث؛ وعليه فتعتبر تلك الجريمة شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الاقليمية أو القارية. وقد خلقت هذه الخاصية العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق بالإضافة الى اشكاليات تتعلق بإجراءات الملاحقة القضائية[16] .

ثانياً: صعوبة اكتشاف واثبات جريمة انتحال الشخصية الالكترونية:

لا تحتاج تلك الجريمة إلى أي عنف لارتكابها، وإنما فقط تحتاج إلى شخص يملك مهارات تكنولوجية عالية في عملية الانتحال، وفي العادة يكون المنتحل من أصحاب الخبرات والمهارات الفائقة في المجالات التقنية، فهو يقوم بعملية صعبة تتمثل بفك رموز وشيفرات معينة وتغيير ارقام وبيانات أو محيها تماماً من السجلات المخزونة في ذاكرة الحاسوب؛ وذلك بهدف الوصول

[16] نهلا المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، 2008م، ص 188.

إلى معلومات الموقع المراد انتحاله؛ وكون أن تلك الجريمة لا تترك أي أثر خارجي مرئي لها بعد أن يرتكبها الجاني فتكون صعبة الاكتشاف[17].

وبالتالي فإن هذه الجريمة وفي الغالب لا تترك أثراً لها بعد ارتكابها، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها[18].

ويرى الباحث أن ما يزيد من صعوبة اكتشاف جريمة انتحال الشخصية الإلكترونية هو أن تحديد هوية مستعمل معين على شبكات التواصل الاجتماعي هي من أكثر المسائل تعقيداً وصعوبة، وباتت تشغل اليوم العالم الحقوقي بامتياز. كما أنه من الصعب أيضاً اعتبار الإثبات الإلكتروني إثباتاً كاملاً، إذ يمكن تحوير حتى المواقع الإلكترونية التابعة للإدارات العامة، فالأدوات التكنولوجية تسمح للشخص الذي يمتلك معرفتها بالسيطرة على كل ما يريد من معلومات والتصرف بها كما يشاء.

ثالثاً: ترتكب جريمة انتحال الشخصية الالكترونية بأسلوب ناعم وبسهولة فائقة:

حيث تتميز جريمة انتحال الشخصية الإلكترونية بأسلوب ارتكابها الناعم، حيث لا تحتاج الى مجهود عضلي كجرائم القتل والسرقة وغيرها، بل كل ما تحتاجه الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسوب والاحاطة ببعض البرامج التشغيلية[19] .

فجريمة انتحال الشخصية الالكترونية تتميز بأنها جريمة هادئة بطبيعتها لا تحتاج إلى عنف؛ حيث أن كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في

---

[17] عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007م، ص 44.

[18] محمد رحموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، المجلد 17، العدد41، 2018م، ص 441.

[19] موفق عبيد، ماهية جريمة الاحتيال المعلوماتي، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد 5، العدد19، 2016م، ص 349

ارتكاب تلك الجريمة، وتحتاج كذلك إلى وجود مجرم يوظف خبرته أو قدرته على التعامل مع شبكة الإنترنت للقيام بتلك الجريمة[20].

فجريمة انتحال الشخصية الالكترونية تعد من الجرائم الخفية؛ لأن المجني عليه لا يلاحظها أو لا يدري حتى بوقوعها والامعان في حجم السلوك المكون لها إخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمر ليس في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسوب غالباً لدى مرتكب هذه الجريمة[21].

ويرتكب الجاني جريمة انتحال الشخصية الإلكترونية بسهولة نوعاً ما؛ وذلك بسبب ما تمنحه شبكة الإنترنت بشكل عام ومواقع التواصل الاجتماعي بشكل خاص من حيز واسع لمستخدميها من الحرية، بالمقارنة مع عالمنا الواقعي الذي يتسم بالتضييق على الأفراد في ممارسة حرياتهم؛ حيث تَمكن هذه المواقع روادها من انتحال شخصيات الغير بسهولة عن طريق إنشاء حسابات خاصة بأسماء وشخصيات الأخرين بناء على البيانات المتعلقة بهم، والتي من خلالها يمكنهم التواصل بسهولة مع الجمهور بأسماء الشخصيات التي تم انتحالها؛ وذلك راجع بالأساس إلى قدرة مستخدمي هذه المواقع على إخفاء هوياتهم الحقيقية الأمر الذي يُسقط بعض الأشخاص في براثيم الإجرام الإلكتروني إما عن علم وإرادة أو عن غير علم[22] .

حيث أصبح من السهل جداً خلق هوية افتراضية والقيام بأعمال إجرامية، دون إمكانية تحديد الهوية الحقيقية للفاعل، فانتحال الهوية والشخصية أصبح من الأمور الشائعة جداً في عصرنا الرقمي وبشكل اعتيادي ولغايات مختلفة، وتعتبر الهوية الوهمية عامل أساسي في ارتفاع نسبة

---

[20] عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007م، ص 52.

[21] موفق عبيد، مرجع سابق، ص 350.

[22] أمين الخنتوري، الهوية الشخصية على شبكات التواصل الاجتماعي بين اللاتنظيم وضرورة التنظيم، مجلة البوغاز للدراسات القانونية والقضائية، العدد 9، 2020م، ص 144.

الإجرام الإلكتروني على الانترنت في ظل صعوبة التحقق من الهوية الحقيقة لصاحب الهوية الوهمية[23].

رابعاً: خطورة مرتكب جريمة انتحال الشخصية الالكترونية وسرعة تنفيذها:

يتميز المجرم الذي يرتكب جريمة انتحال الشخصية الإلكترونية بصفات خاصة من الذكاء والمهارة لتنفيذ سلوكه الاجرامي بل إن هذا المجرم يكون لديه من الخبرة والمهارة التي يكتسبها في كثير من الأحيان من دراسته في مجال تكنولوجيا المعلومات، فهو غالباً مجرم محترف ولكن لا يعني ذلك أن كل مجرم إلكتروني يكون لديه المهارة والخبرة الكافية للقيام بجريمته، فالإجرام المعلوماتي هو إجرام يحتاج إلى الذكاء دون استخدام للعنف أو القوة وهو ما يقوم به الجاني في جريمة انتحال الشخصية الالكترونية[24].

كما تتميز تلك الجريمة بسرعة التنفيذ؛ إذ أنه بضغطة واحدة على لوحة المفاتيح يمكن للجاني أن ينتحل شخصية أخرى ويجري المعاملات باسم الشخصية التي تم انتحالها، وهذا لا يعني أن تلك الجريمة لا تتطلب الإعداد قبل التنفيذ او استخدام برامج معينة. كما لا تتطلب جريمة انتحال الشخصية الإلكترونية وجود الفاعل في مكان الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه[25]. وهو الذي يجعل من الصعوبة بمكان الوصول الى الفاعل بسهولة، وكذلك يجعل الجاني في مأمن الملاحقة الإدارية والعقابية، الا في الحدود التي تقتضيها قوانين الدولة التي يعيش فيها، ومدى تجاوبها مع القضايا التي يمثلها قانون الدولة التي وقعت الجريمة في إقليمها.

الفرع الثاني: تمييز جريمة انتحال الشخصية الالكترونية عن غيرها من الجرائم

---

[23] المرجع السابق، ص144

[24] غنام غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة، مصر، 2017م، ص 13.

[25] محمد الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2006م، ص 30.

تعد جريمة انتخال الشخصية الإلكترونية إحدى الجرائم المعلوماتية؛ لذلك فهي تتشابه بشكل كبير مع بعض الجرائم الإلكترونية الأخرى مثل جريمة التزوير الإلكتروني وجريمة الاحتيال الإلكتروني وجريمة انتحال الصفة الإلكترونية؛ الأمر الذي يُثير بعض اللبس والغموض في تمييز تلك الجريمة عن غيرها من أشكال الجرائم الإلكترونية الأخرى.

أولاً: تمييز جريمة انتحال الشخصية الإلكترونية عن جريمة الاحتيال الإلكتروني:

تُعرف جريمة الاحتيال بشكلها التقليدي بأنها: "الاستيلاء على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال[26] " كما تعرف بأنها: "استعمال وسيلة من وسائل التدليس التي نص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني مالا مملوكاً لغيره نتيجة الوقوع في الغلط [27]"

أما جريمة الاحتيال المعلوماتية فتعرف بأنها: "أي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي "كما عرفت بأنها: "التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الالي، أو الادخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أي وسيلة أخرى من شأنها التأثير على الحاسب الالي حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع والحاق الضرر بالغير[28]" وعرفها البعض بانها: "حث الحاسب الآلي على تغيير بعض الحقائق بأي وسيلة كانت تهدف إلى الحصول على ربح غير مشروع على حساب شخص أخر، فوظيفة الحاسب الالي مكنت الجاني من اتمام فعل الاحتيال [29]"

أما منظمة الامم المتحدة، فقد أقرت تعريف الاحتيال المعلوماتي بناء على توصية المجلس الاوربي رقم (R9/89) الذي جاء فيها: "انه الإدخال أو المحو أو التعديل أو كبت البيانات أو

---

[26] حسن المرصفاوي، قانون العقوبات الخاص، منشأة المعارف، الاسكندرية، 1975، ص 394.

[27] أحمد أبو خطوة، شرح قانون العقوبات القسم الخاص، جرائم الاعتداء على الأموال، دار النهضة العربية، القاهرة، 1994، ص196.

[28] نائلة قورة، جرائم الحاسب الالي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2005م، ص 425.

[29] علي الطوالبة، الجرائم الالكترونية، جامعة العلوم التطبيقية، الطبعة الأولى، 2008م، ص 181.

برامج الحاسوب، أو التدخل المؤثر في معاجلة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص أخر، بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص أخر[30]"

ويرى الباحث أن جريمة الاحتيال الإلكتروني هي: "الاستيلاء عن طريق الشبكة المعلوماتية أو جهاز الحاسوب أو ما في حكمها على مال ما أو معلومات أو برامج أو على سند يتضمن تعهداً أو ابراءً أو أي امتياز مالي أخر، وذلك عن طريق خداع المجني عليه، أو خداع الحاسوب أو الالة الخاضعة لسيطرة المجني عليه، وإلحاق الضرر به".

وتجدر الاشارة إلى أن القوانين قد اختلفت في تسمية جريمة الاحتيال، فسمتها بعض القوانين جريمة النصب كما هو الحال في قانون العقوبات المصري لسنة 1937[31]، وقانون العقوبات الجزائري لعام 1966م[32]، وقانون عقوبات البحرين لسنة 1968م[33]، ومشروع قانون العقوبات الفلسطيني[34] . في حين أن قوانين أخرى أطلقت عليها تسمية جريمة الاحتيال كما هو الحال في قانون العقوبات الأردني لسنة 1960م[35]، وقانون العقوبات اللبناني لسنة 1943م[36]، وقانون العقوبات السوي لسنة 1949م[37].

والجدير ذكره أن معظم التشريعيات جعلت جريمة الاحتيال الالكتروني خاضعة للقواعد العامة في جريمة الاحتيال الواردة في القسم الخاص من قانون العقوبات، ومن ثم اكتفت بما هو وارد فيها ولم تستحدث نصوصاً قانونية خاصة بها؛ فهذه التشريعات وسعت من تفسيرها لهذه النصوص وجعلتها تشمل جريمة الاحتيال الواقعة من خلال شبكة الانترنت. وعلى الجانب الأخر هناك من

---

[30] نهلا المومني، الجرائم المعلوماتية، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان، 2008م، ص 188.

[31] انظر: المادة (336) من قانون العقوبات المصري لسنة 1937م .

[32] انظر: المادة (372) من قانون العقوبات الجزائري لسنة 1966م.

[33] انظر: المادة (242) من قانون عقوبات البحرين لسنة 1967م.

[34] نصت المادة (353) من مشروع قانون العقوبات الفلسطيني لعام 2011م على تعريف جريمة النصب، فعرفته بأنه: " الحصول على مال مملوك للغير إما باستعمال طريقة احتيالية مدعمة بمظاهر خارجية من شانها خداع المجني عليه في واقعة تنتمي إلى الماضي أو الحاضر، وإما باتخاذ اسم كاذب أو صفة غير صحيحة بما يحمله على الاعتقاد بصدق ما يدعيه الجاني وتسليم المال نتيجة لذلك "

[35] انظر: المادة (417) من قانون العقوبات الأردني لسنة 1960م.

[36] انظر: المادة (655) من قانون العقوبات اللبناني لسنة 1943م.

[37] انظر: المادة (641) من قانون العقوبات السوري لسنة 1949م.

التشريعات الجزائية قد وضعت نصوصاً قانونية خاصة بهذا النوع من الجرائم المستحدثة كالقانون الاتحادي لمكافحة جرائم تقنية المعلومات الاماراتي.

ومن الملاحظ أن القانون الفلسطيني قد سار على نهج التشريعات التي شرعت نصوصاً قانونية تجرم وتعاقب مرتكبي جريمة الاحتيال الالكتروني، حيث نصت المادة (14) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: "كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. " ويمكن القول كذلك أن نص المادة (417) من قانون العقوبات الأردني لسنة 1960م يطبق كذلك على جريمة الاحتيال التقليدي وجريمة الاحتيال الالكتروني[38].

ويرى الباحث أنه على الرغم من وجود فوارق بين جريمة الاحتيال التقليدية وفق مفهومها الوارد في قانون العقوبات وبين الجريمة الالكترونية، إلا أن هذه الفوارق تنحصر في الأسلوب الإجرامي فقط، فبدلا من أن كانت تتم الجريمة بطريقة تقليدية أصبحت اليوم في ظل التطور التكنلوجي تأخذ أسلوبا آخر، إلا أن ذلك لا يمنع تطبيق نص المادة 417 من قانون العقوبات للتصدي لجرائم الاحتيال التي تتم من خلال شبكات الانترنت بالوسائل الالكترونية.

وعلى الرغم من التشابه الكبير بين الجريمتين إلا أنهما يختلفان في هدف كل واحدة منهما؛ حيث تهدف جريمة انتحال الشخصية الإلكترونية إلى الإضرار بسمعة ومصلحة الضحية؛ من خلال

---

[38] تنص المادة (417) من قانون العقوبات الأردني رقم (16) لسنة 1960م على أنه : " كل من حمل الغير على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراء فاستولى عليها احتيالاً: باستعمال طرق احتيالية من شأنها إيهام المجني عليه بوجود مشروع كاذب أو حادث أو أمر لا حقيقة له أو إحداث الأمل عند المجني عليه بحصول ربح وهمي أو بتسديد المبلغ الذي أخذ بطريق الاحتيال أو الإيهام بوجود سند دين غير صحيح أو سند مخالصة مزور، أو بالتصرف في مال منقول أو غير منقول وهو يعلم أن ليس له صفة للتصرف به، أو باتخاذ اسم كاذب أو صفة غير صحيحة، عوقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبالغرامة من خمسة دنانير إلى خمسين ديناراً

الوسائل التي يقوم بها الجاني بخداع الأخرين المتعاملين مع منتحل الشخصية، بحيث يتولد لدى الأخرين الاعتقاد بأنهم يتعاملون مع الشخصية الحقيقية. في حين أن جريمة الاحتيال الإلكتروني تهدف إلى الحصول على أموال الأخرين من خلال استخدام الجاني طرق تدليسية؛ ومن أشهر تلك الطرق إنشاء المحتالين لمواقع وهمية للبيع والشراء، وبمجرد ان يدخل مستخدم الانترنت، ويقوم بشراء ما يحتاجه عن طريق وضع أرقام بطاقته الائتمانية لخصم المبالغ النقدية المستحقة مقابل البضاعة حتى يقع في الشرك، ولا تصل أية بضاعة بعد أن فقد جزءاً من نقوده من خلال بطاقته الائتمانية ويكتشف أنه كان ضحية لجريمة الاحتيال الإلكتروني.

ثانياً: تمييز جريمة انتحال الشخصية الإلكترونية عن جريمة التزوير الإلكتروني:

يعد التزوير عملية مادية وصورة من صور الكذب التي يقوم بها شخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو سند رسمي بإحدى الطرق المحددة في القانون، وشأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الادعاء بالتزوير[39]. فالتزوير الإلكتروني يكون عن طريق تغيير الحقيقة الذي يرد على مخرجات الحاسوب سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطباعة، أو كانت مرسومة عن طريق الرسم، فجريمة التزوير الإلكتروني تشير إلى أي نشاط غير قانوني يتعلق بتلاعب أو تحايل على البيانات الإلكترونية مثل: البيانات الموجودة على الإنترنت، أو المعاملات المالية الإلكترونية، ويشمل ذلك استخدام معلومات كاذبة أو تزوير الهوية الرقمية، أو تعديل البيانات الرقمية بطرق غير قانونية؛ بهدف الاحتيال أو التلاعب[40].

وقد عرف قانون العقوبات رقم (16) لسنة 1960م التزوير بأنه: " تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد اثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي[41]"

---

[39] عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور، دار هومة، الجزائر، الطبعة الأولى، 2005م، ص14.

[40] عبد الفتاح بيومي، مرجع سابق، ص 170.

[41] انظر: المادة (260) من قانون العقوبات الأردني رقم (16) لسنة 1960م.

وقد جرم المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، صور جريمة التزوير الإلكترونية ووضع عقوبات مناسبة لها[42]، واعتبر المشرع الفلسطيني أن تغيير الحقيقة هو الأساس الذي تقوم عليه جريمة التزوير، وإذا انتفى ذلك العنصر فلا تقوم تلك الجريمة، كأن يقوم أحدهم بإثبات بيانات مطابقة للحقيقة، فلا تقوم جريمة التزوير حتى ولو كان ذلك الشخص يعتقد بعدم صحة هذه البيانات وحتى ولو ترتب على فعله ضرر في حق الغير[43].

ويتصور وقوع التزوير الإلكتروني عن طريق تغيير الحقيقة على شرائط أو المحررات التي تمثل مخرجات الحاسب الالي أي لا بد أن يحصل التغيير في البيانات الموجودة في جهاز، شرط حصول ضرر والذي يتمثل في اهتزاز الثقة المفترضة في المحررات الرسمية حال التزوير الإلكتروني في المحرر الرسمي أو يُلحق لأحد الأفراد وذلك حال التزوير الإلكتروني في المحرر العرفي؛ ومما تجدر الإشارة إليه أن التزوير الإلكتروني لا يتم من قبل مشغل الحاسب الآلي فقط، وإنما يمكن أن يقع من شخص عادي ليس له دراية بتشغيل الكمبيوتر ولا يتمتع بأي قدر من الكفاءات والمهارات الفنية والعلمية لتشغيل هذا الجهاز الإلكتروني ومع ذلك يرتكب التزوير الإلكتروني كما هو الحال بالنسبة للشخص الذي يعمد إلى فتح حساب جاري فيقوم باستعمال اسم شخص أخر أو الاتصاف بصفة ليست له، أو بتقرير وقائع كاذبة أو أي أمر من شأن المستند المبرمج إثباته [44].

يتضح لنا مما سبق أنه يوجد تشابه كبير بين جريمة التزوير وجريمة انتحال الشخصية الإلكترونية؛ فالعنصر الجوهري الذي يقوم عليه كلا الجريمتين هو تغيير الحقيقة، وهذا التغيير هو الذي يعد جوهر كلا الجريمتين، وهذا التغيير هو السلوك الذي يجرمه المشرع الجنائي بوصفه تزويراً إذا وقع في المحررات، فتغيير الحقيقة باستبدالها بما يخالفها يعد جريمة تزوير فإذا لم يحصل هذا التغيير فلا تتحقق جريمة التزوير، وكذلك الحال في جريمة انتحال الشخصية الإلكترونية فهي تقوم على تغيير الحقيقة كما سنوضح لاحقاً.

---

[42] انظر: المادة (12) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[43] عبد الستار فوزية، مرجع سابق، ص 245.

[44] عمر الجبوري، جريمة التزوير الإلكتروني في التشريع الأردني: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2017م، ص42.

وعلى الرغم من وجهة النظر القائلة بأن انتحال شخصية الغير تعد صورة من صور التزوير الإلكتروني وإحدى تطبيقاته، إلا أن الباحث يرى خلاف ذلك، حيث أن قانون العقوبات قد قام بتعريف جريمة التزوير وبيان طرقها، في حين لم يعرف المشرع جريمة انتحال الشخصية، وكذلك نلاحظ أن المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية قد عدد في المادة (12) صور وأشكال التزوير الإلكتروني التي يعاقب عليها القانون، ولم يورد ضمن تلك الصور ما يتعلق بانتحال الشخصية الإلكترونية وإنما أفرد لها نصاً خاصاً خارج إطار المادة التي تُجرم التزوير مما يعني بوجود فرق بين الجريمتين .

كما أن الخلاف يتضح بين الجريمتين في محل كل جريمة منهما، حيث أن الأصل أن محل الجريمتين هو معطيات الكمبيوتر بأي صورة تتخذها محلاً لتلك الجريمتين ، إلا أنه وفق المعنى الضيق للتزوير الإلكتروني، وباعتبار الكمبيوتر مجرد أداة لإرتكاب جريمة التزوير لا أكثر، يكون للتزوير صورة واحدة وهو التزوير المنصب على المستندات المعالجة آلياً، وهو ما يفترض أننا أمام مستندات موجودة في الأصل بصورة تقليدية أو كانت تتخذ شكلاً ورقياً في السابق ثم أدخلت إلى الكمبيوتر كنماذج إلكترونية في اطار معالجتها ألياً أو رقمياً، وهو التي تكون محلاً لجرم التزوير الذي يستهدف التغيير في مشتملاتها بالحذف والإضافة والتعديل . وفي المقابل فإننا نجد أن جريمة انتحال الشخصية الإلكترونية يختلف محلها بشكل واضح على النحو الذي ذكر حول جريمة التزوير؛ كون أن جريمة الانتحال ليس لها علاقة بالمستندات وإنما هي اعتداء على شخصية الغير وتغيير الحقيقة من خلال ادعاء المنتحل أنه شخص ما، ويقوم بمعاملات إلكترونية مع الغير بصفة واسم الشخص الذي تم انتحال شخصيته.

ثالثاً: تمييز جريمة انتحال الشخصية الإلكترونية عن جريمة انتحال الصفة الإلكترونية:

تعرف جريمة انتحال الصفة بشكل عام بأنها: " قيام شخص ما بتقمص صفة موظف عام، وممارسة عمل من أعمال هذه الصفة، بشكل متعمد من دون صفة رسمية أو تخويل من جهة

مختصة بذلك[45]" وهناك من يعرفها بأنها:" إساءة استخدام المعرفات الشخصية من أجل الحصول على أشياء ذات قيمة أو لغرض تسهيل نشاط إجرامي معين[46]"

وتعد جريمة انتحال الصفة الإلكترونية إحدى الجرائم الجنائية الإلكترونية التي برزت بالآونة الأخيرة، والتي يرتكبها بعض الجناة لغرض تحقيق غاياتهم الإجرامية بطرق ملتوية وغير مشروعة مستغلي ثقة الناس بهذه الصفات، من حيث إن رابطة الثقة هذه هي التي غالباً ما يتم كسرها من قبل المجرمين، بالإضافة إلى صعوبة التمييز التي قد تواجه الأفراد ما بين الصفة الرسمية والصفة الوهمية؛ فيقوم مرتكبي جريمة انتحال الصفة الإلكترونية بإنشاء صفحات وهمية على مواقع التواصل الاجتماعي والاحتيال على المواطنين الذين سُرعان ما يقعون ضحية لهؤلاء الأشخاص الذين ينتحلون صفة تُمثل جهة رسمية بهدف تحقيق مكاسب مالية أو منافع شخصية[47].

ومن الأمثلة على جريمة انتحال الصفة الإلكترونية قيام بعض المجرمين بانتحال الصفات القانونية بطرق ووسائل غير مشروعة، ولا سيما عبر إنشاء الصفحات الوهمية في برامج التواصل الاجتماعي، بالشكل الذي يوهم الناس بأنهم قضاة أو محامون، مستغلين حاجة الناس لهذه المهن التي تتطلب خبرة ومعرفة أكاديمية لممارستها وفق القوانين، وبما أن نسبة الجريمة أخذت بالازدياد مما يتطلب إلى المزيد من نسب المحامين والقضاة لإنجاز الوظائف القضائية، ولهذا يُحاول منتحلي الصفة الإلكترونية إلى إظهار أنفسهم بأنهم محامين أو قضاة عن طريق تزوير الشهادات الجامعية أو الهويات النقابية واستخدامها بشكل غير مشروع لممارسة هذه المهمة، ويقومون بنشر البطاقات الخاصة بهم عبر الإنترنت لخداع الناس ولا سيما الطبقات الفقيرة والساذجة ممن لديهم حاجات أو استفسارات قانونية، ومن المؤكد يكون ذلك مقابل مبالغ مالية محددة من قبل منتحل الصفة، وهذا على الأغلب قد يكون الهدف الذي يسعى له المنتحل

---

[45] قيس التميمي، شرح قانون العقوبات العراقي، العاتك للطباعة، بيروت، 2019م، ص 2179.

[46] اقبال أمين، انتحال الوظيفة العامة ونطاق مسؤوليتها، مجلة الحقوق، العدد41، الجامعة المستنصرية، 2021م، ص 409.

[47] محمد سهيل، انتحال الصفة في المجتمع العراقي: الأنماط والمخاطر، مجلة الدراسات المستدامة، الجمعية العلمية للدراسات التربوية المستدامة، المجلد 6، 2024م، ص1711

لتحقيقه بصورة غير مشروعة، مستغلاً للثقة المجتمعية التي تُمنح لهذه الشريحة لمزاولة المهمة[48].

ومن تطبيقات جريمة انتحال الصفة الإلكترونية، أن يقوم أحد الأشخاص بانتحال صفة مدير عمل المستخدم أو محاسب في الشركة التي يعمل بها المستخدم ويرسل رسالة لهذا الشخص عبر البريد الإلكتروني الخاص به بناءا على هذا الأساس ويطلب من المستخدم إرسال بيانات معينة أو كلمة مرور أو غير ذلك. أو أن يقوم أحدهم بانتحال صفة مسوق الكتروني أو بائع الكتروني يتمم صفقات تجارية ويطلب من الراغبين بالشراء ارسال بياناتهم أو أرقام بطاقات الائتمان الخاصة بهم لخصم سعر المنتج من البطاقة، أو بالإعلان عن جائزة كبيرة لمن يساهم في دفع مبلغ رمزي لصالح جهة خيرية وهذا المبلغ تم من خلال كتابة رقم البطاقة[49].

ويشير الباحث إلى أن قانون العقوبات رقم (16) لسنة 1960م، قد نص على جريمة انتحال الصفة بموجب المادتين (201،202) حيث فصلت المادة (201) فيما يتعلق بانتحال الصفات، وفصلت المادة (202) فيما يتعلق بانتحال الوظائف والتي تعد احدى صور انتحال الصفات.

وتتشابه جريمة انتحال الشخصية الإلكترونية مع جريمة انتحال الصفة الإلكترونية في أن كلا الجريمتين تعتمد على التضليل مع من يتعامل مع الشخصية أو على الصفة الإلكترونية على أنه يتعامل مع الشخص أو الصفة المطلوبة، كما تتشابه كلا الجريمتين بأنهما تهدفا إلى تحقيق مكاسب شخصية وغايات تتمثل بالإضرار بالأخرين[50].

وعلى الرغم من التشابه الكبير بين الجريمتين، إلا أنهما يختلفان؛ حيث أن الشخصية الإلكترونية يمثلها اسم الفرد، سواء أكان اسماً حقيقياً وفق قيود الأحوال المدنية أم اسم شهرة أو كنية ينادى بها ويعرف بها بين الناس، ويمكن أن يقع الانتحال على الاسم واللقب معاً أو على واحد منهما دون الأخر. أما الصفة فلا تقع تحت حصر، إذ هي كل مركز أو رتبة أو وظيفة أو مهنة يحتلها

---

[48] محمد سهيل، مرجع سابق، ص 1719.

[49] فتحي كبور، جرائم انتحال الوظائف والألقاب وإساءة استعمالها في التشريع الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، الجزائر، 2019م، ص 20.

[50] زيد بني خالد، مرجع سابق، ص210

الفرد ويشغلها؛ مما يعطيه اعتباراً أو احتراماً معيناً[51]؛ وعليه فإذا ما قام المجرم بانتحال اسم أو كنية شخص ما فنكون أمام جريمة انتحال الشخصية الإلكترونية، أما إذا ما قام المجرم بانتحال صفة شخص ما مثل من يدعي صفة البنوة أو الأبوة أو الأخوة لشخص أخر، أو يدعي كونه محامياً أو طبيباً أو مهندساً، أو يدعي رتبة علمية أو وظيفية؛ ففي هذه الحالة نكون أمام جريمة انتحال الصفة الإلكترونية.

المبحث الثاني: أركان جريمة انتحال الشخصية الالكترونية.

من المعلوم أن لكل جريمة ثلاثة أركان هي: " الركن الشرعي، والركن المادي، والركن المعنوي" وبدون هذه الأركان تنتفي الجريمة، وهذا هو الحال بالنسبة للجرائم الإلكترونية، فلقيام جريمة انتحال الشخصية الإلكترونية لا بد أن يتوفر فيها أركان الجريمة، ويتمثل الركن الشرعي في مبدأ " لا جريمة ولا عقوبة إلا بنص" بحيث يستوجب أن ينص القانون بشكل مسبق على تجريم السلوك ورصد عقوبة له. أما الركن المادي فيتكون من السلوك الإجرامي، والنتيجة الإجرامية، ووجوب توفر علاقة السببية بينهم. أما الركن المعنوي فهو الذي يعالج مسألة الإرادة والعلم والقصد الجنائي.

ولما كانت الجريمة الإلكترونية جريمة جزائية يتم تنظيم أحكامها وفق القرار بقانون قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، حيث تعد جريمة انتحال الشخصية الإلكترونية ضمن الجرائم التي نظمها القرار بقانون وفرض عقوبات جزائية لمن يرتكبها.

في هذا المبحث سيناقش الباحث أركان جريمة انتحال الشخصية الالكترونية وذلك من خلال المطالب التالية:

المطلب الأول: الركن الشرعي

[51] خليل إعبية، مرجع سابق، ص92

يقصد بمبدأ الشرعية الجزائية أنه " لا جريمة ولا عقوبة إلا بنص في القانون" وأن المشرع هو الذي يحدد الأفعال التي تعد جرائم ويبين مضمونها من أركان وعناصر بدقة ووضوح لا يكتنفها اللبس والغموض، وهو الذي يحدد العقوبات المقررة لها نوعاً وكماً ومقداراً، فهذا المبدأ يضع حداً فاصلاً بين ما للشارع وبين ما للقاضي من اختصاص ويقع على عاتق سلطات الدولة مراعاته.

وقد نص القانون الأساسي الفلسطيني على هذا المبدأ، حيث جاء فيه: "العقوبة شخصية، وتمنع العقوبات الجماعية، ولا جريمة ولا عقوبة إلا بنص قانوني[52] " وهو ما أخذت به المادة الثالثة من قانون العقوبات رقم (16) لسنة 1960م والتي جاء فيها: " لا يقضى بأية عقوبة لم ينص القانون عليها حين اقتراف الجريمة .... "

وبناء على ما سبق فلا يمكن للقاضي أن يعاقب على أي فعل غير معاقب عليه قانوناً، وبالتالي يثور هنا التساؤل حول ما هو النص القانوني الذي يعاقب على ارتكاب جريمة انتحال الشخصية الإلكترونية؟ وهذا ما سيجيب عليه الباحث في هذا المطلب من خلال بيان النصوص القانونية المجرمة لتلك الجريمة سواء في القانون الفلسطيني أو القوانين المقارنة.

الفرع الأول: القانون الواجب التطبيق على جريمة انتحال الشخصية الإلكترونية:

قبل نشر القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية بتاريخ 2017/7/9م كانت ملاحقة مرتكبي الجرائم الالكترونية تتم بتطبيق النصوص التقليدية من قانون العقوبات الأردني رقم 16 لسنة 1960م على الجرائم الالكترونية، والقانون رقم 3 لسنة 1996م بشأن الاتصالات السلكية واللاسلكية، بالإضافة إلى القرار بقانون رقم (15) لسنة 2009م بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات، وقانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 وتعديلاته.

حيث كان المتبع قبل إقرار القرار بقانون بشأن الجرائم الإلكترونية ملاحقة مرتكبي جريمة انتحال الشخصية الإلكترونية عن طريق إسقاط نصوص قوانين العقوبات السارية في فلسطين لاسيما قانون العقوبات رقم (16) لسنة 1960م، خاصة المواد رقم (201،202) بحيث يتم تطبيق هذه النصوص عندما ترتكب هذه الجرائم بواسطة الكمبيوتر أو شبكة الانترنت ، وغني عن البيان بأن هذه النصوص تعتبر قاصرة عن الوفاء بالغرض وبالتالي تدق الحاجة إلى التجريم الالكتروني

[52] انظر: المادة (15) من القانون الأساسي الفلسطيني.

الخاص بهذه الجرائم ، ذلك أن نصوص هذه الجرائم تنطبق عندما يكون الكمبيوتر وسيلة لارتكاب السلوك وفي بعض الأحيان عندما تقع على الكمبيوتر ذاته إلا أن المجرم في كثير من الأحيان يفلت من العقاب بسبب عدم وجود النص التشريعي المناسب للتجريم[53].

ومما لا شك به أن القرار بقانون بشأن الجرائم الالكترونية يعد حاجة أساسية وضرورية للمجتمع الفلسطيني في ظل التغيرات التكنولوجية وتطورها، ونتيجة للالتزامات المترتبة على دولة فلسطين بعد انضمامها إلى الاتفاقات الدولية والاقليمية حول الجرائم المعلوماتية التي حثت الدول الأعضاء على اتخاذ تدابير تشريعية لإصدار قانون الجرائم الالكترونية، حيث صادق رئيس دولة فلسطين على قرار بقانون بشأن الجرائم الالكترونية رقم 16 لسنة 2017م بتاريخ 2017/6/24م وأصبح هذا القرار ساري المفعول بتاريخ نشره 2017/7/9م. وبسبب الانتقادات التي وجهت إلى القرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة 2017، أجرى المشرع الفلسطيني تعديلات جوهرية على القرار بقانون لسنة 2017م، وأصدر لاحقاً القرار بقانون رقم (10) لسنة 2018م بشان الجرائم الإلكترونية الصادر بتاريخ 2018/4/29 والمنشور في العدد الممتاز رقم 16 من الوقائع الفلسطينية بتاريخ 2018/5/3م ، وهو القانون الساري المفعول حتى الان في الضفة المحتلة . وفي تاريخ 2021/12/23م أصدر الرئيس الفلسطيني قرار بقانون رقم (38) لسنة 2021م بتعديل قرار بقانون رقم (10) لسنة 2018م، بشأن الجرائم الإلكترونية وتعديلاته. وقد عدل هذا القرار بقانون اسم القانون الأصلي ليصبح " قرار بقانون بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات".

الفرع الثاني: النصوص القانونية المنظمة لجريمة انتحال الشخصية الإلكترونية في التشريع الفلسطيني والقوانين المقارنة:

نص المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، على تجريم انتحال الشخصية الإلكترونية، حيث نصت المادة (14) منه على أنه : " كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء

[53] عبد اللطيف ربايعة، الجرائم الإلكترونية، بحث مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، جامعة النجاح، 2016م.ص 11.

توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل وعن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.[54]"

كما نصت المادة (4) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه : " 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 تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.[55]"

يلاحظ مما سبق أن المشرع الفلسطيني قد جرم الدخول إلى الموقع لانتحال صفته أو انتحال شخصية مالكه، وعاقب على ذلك بالحبس والغرامة معاً، كما جرم كل من استخدم برنامجاً أو نظاماً معلوماتياً لانتحال صفة الموقع أو شخصية المالك. ويتبين من المواد السابقة أن المشرع الفلسطيني قد جعل السلوك الجرمي المتمثل في انتحال الشخصية الإلكترونية غاية من غايات الولوج المجرم لنظام المعلومات، إذ جعله ظرفاً مشدداً للعقوبة، فنرى أن المشرع الفلسطيني قد جرم الولوج المجرد للنظام الإلكتروني، ثم جرم فعل الجاني الذي لا يكتفي بمجرد الاطلاع الشخصي على البيانات والمعلومات الإلكترونية، بل يبتغي غرضاً أخر، وغلظ عليه العقوبة

أما فيما يتعلق بالقوانين المقارنة فنجد أن المشرع الأردني قد سار على نفس النهج الذي سار عليه المشرع الفلسطيني[56]، ونجد أن بعض التشريعات لم تُجرم الانتحال كفعل مثل ما انتهج المشرع الفلسطيني والأردني، وإنما جرم الأفعال المترتبة على الانتحال وهذا ما اتبعه المشرع

---

[54] انظر: المادة (14) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[55] انظر: المادة (4) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[56] انظر: المادة (3/ج) والمادة (4) من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015م.

الإماراتي والذي نص على أنه : " " يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات [57]" كما أن المشرع الإماراتي فرض عقوبة شديدة الغلظة تصل إلى مليوني درهم لكل من استغل عنواناً عائداً للغير بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها [58].

والملاحظ أن بعض التشريعات قد جرمت انتحال الشخصية الإلكترونية في نطاق ضيق؛ حيث ربطت الانتحال بالاستيلاء على المال أو السند أو التوقيع، مثل ما فعل المشرع السوداني والذي نص على أنه: " كل من يتواصل عن طريق شبكة المعلومات عن طريق الانتحال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة بغرض الاستيلاء على مال أو سند أو توقيع للسند يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً[59]"

وخلاصة ما سبق أن المشرع الفلسطيني قد كان موقفه أفضل من التشريعات الأخرى كون أنه جرم فعل الانتحال كسلوك، ووضع عقوبة عليه، ولم يضيق من نطاق تجريمه كما فعلت التشريعات الأخرى.

المطلب الثاني: الركن المادي

يعد الركن المادي أحد أهم الأركان القانونية الواجب توافره في أي جريمة جنائية، ويتمثل الركن المادي في جريمة انتحال الشخصية الإلكترونية في مجموعة السلوكيات التي يقوم بها المنتحل لانتحال شخصية الاخرين، فلا يكفي مجرد أن يكون قد تعمد انتحال شخصية لأحد أخر بل يجب أن يقوم بأفعال وسلوكيات لازمة لذلك.

---

[57] انظر: المادة (9) من القانون الاتحادي رقم 12 لسنة 2016م.

[58] انظر: المادة (1) من القانون الاتحادي رقم 12 لسنة 2016م.

[59] انظر: المادة (11) من قانون جرائم المعلوماتية السوداني.

ويتكون الركن المادي لجريمة انتحال الشخصية الإلكترونية من عناصر ثلاث هي: السلوك الإجرامي، والنتيجة الإجرامية، وعلاقة السببية بينهما. وهذه العناصر هي ما سيناقشها الباحث في هذا المطلب، من خلال الفروع التالية:

الفرع الأول: السلوك الإجرامي:

ينقسم السلوك الإجرامي، إلى سلوك إيجابي وسلوك سلبي، فالسلوك الإيجابي هو نشاط إرادي ينفذه الجاني في العالم الخارجي تحقيقاً لغاية معينة مخالفاً بذلك نهياً تفرضه قاعدة جنائية، وقد يكون ذلك السلوك من فعل واحد أو جملة أفعال متتابعة، تجمعها وحدة الهدف. أما السلوك السلبي فيتمثل في احجام الشخص ارادياً عن اتيان سلوك إيجابي معين، كان من الواجب عليه قانوناً أن يأتيه في ظروف معينة، ويطلق عليه الامتناع الاجرامي او الترك الاجرامي [60].

وقد يأتي السلوك الإجرامي بصورة بسيطة، وقد يتضمن عملية معقدة تحتوي سلسلة سلوكيات لازمة مثل الانتحال، إذ لا بد في جرائم الانتحال من الخداع والكذب ثم تدعيم هذا الكذب بمظاهر خارجية. كما يعد السلوك المادي عبر الانترنت محلاً لجملة من التساؤلات لاسيما فيما يتعلق ببدايته أو الشروع في ارتكابها وهو يختلف عما هو الحال في العالم المادي ذلك لأن ارتكاب الجريمة عبر الانترنت تحتاج بالضرورة إلى منطق تقني أي أنها تتم عبر الانترنت أو باستخدام المعالجة الالية للبيانات كما أنها تحتاج إلى ممارسة نشاط تقني محدد يتمثل في استخدام الحاسوب والانترنت أو باستخدام المعالجة الالية للبيانات كما أنها تحتاج إلى ممارسة نشاط تقني محدد يتمثل في استخدام الحاسوب والانترنت[61] .

ويتمثل السلوك الإجرامي في جريمة انتحال الشخصية الإلكترونية في مجموعة من الطرق والوسائل التقنية التي يستخدمها المنتحل، فيتطلب تحقق السلوك الاجرامي قيام الجاني بصورة إيجابية كأن يقوم باستخدام الحاسب الآلي في عملية الانتحال واستخدام قدراته العقلية[62].

---

[60] عبد القادر جرادة، القضاء الجنائي الدولي والحرب على غزة، المجلد الأول: الجريمة الدولية، مكتبة أفاق، غزة، الطبعة الثانية، 2010م، ص369.

[61] محمد الشموط، الإثبات في الجرائم الالكترونية: دراسة مقارنة، رسالة دكتوراة، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية، الأردن،2015م، ص42.

[62] زيد بني خالد، مردع سابق، ص 36.

والملاحظ أن القرار بقانون بشأن الجرائم الإلكترونية الفلسطيني قد أورد صورتين من صور انتحال الشخصية الإلكترونية هما:

أولاً: انتحال شخصية المواقع بعد دخولها بطريق غير مشروع:

ذكر المشرع الفلسطيني هذه الصورة في المادة (4) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، حيث أنه حتى يشق المحتال طريقة السلوك الجرمي في جريمة انتحال الشخصية كان لا بد من الجاني الدخول بطريق غير مشروعة إلى الموقع الإلكتروني[63]، وبالتالي تكون جريمة الدخول غير المشروع للموقع الالكتروني عنصراً أساسياً في تكوين السلوك الجرمي لجريمة انتحال الشخصية الإلكترونية، حيث يلجأ الجاني في جريمة الدخول غير المشروع إلى استخدام تقنية نظم المعلومات الإلكترونية للدخول إلى نظام إلكتروني[64] لمعالجة أو حفظ البيانات والمعلومات، والذي يخص أحد الأشخاص بعد اختراقه سواء أكان شخصاً معروفاً لديه أم مجهولاً. كما يعد السلوك جرمياً كذلك إذا كان الجاني مأذوناً له بالدخول إلى النظام الإلكتروني فتجاوز حدود الإذن، كما يستوي في التجريم زمن بقاء الجاني داخل النظام الالكتروني طال أم قصر، طالما تجاوز حد الترخيص أو الإذن[65].

وبعد أن يقوم الجاني بالولوج بطريقة غير مشروعة إلى النظام الإلكتروني أو الموقع الإلكتروني الخاص بشخص ما، فيقوم بانتحال شخصية وصفة صاحب هذا الموقع أو النظام الإلكتروني دون إظهار ما يدل على حقيقة هوية المالك الأصلي، كما أن جريمة انتحال الشخصية الإلكترونية قد تتم باستخدام هوية شخص طبيعي أو موقع معروف قد يستخدمها الجاني للتحدث باسمه والإضرار به في نفسه أو ماله عن طريق إرسال معلومات أو تصريحات خاطئة، وقد يكون بهدف إخفاء شخصية الجاني لتسهيل ارتكاب جرائم أخرى[66].

---

[63] يعرف الموقع الالكتروني بأنه: " مجموعة من صفحات الويب التي يتم تجميعها معًا وعادة ما تكون متصلة بطرق مختلفة."

[64] الأنظمة الإلكترونية هي: "منظومة إلكترونية متكاملة تهدف تحويل العمل المالي أو الإداري العادي من إدارة يدوية الي إدارة باستخدام الحاسب الآلي وذلك بالاعتماد على نظم معلوماتية قوية"

[65] محمد الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دراسة مقارنة، دار الفكر والقانون، المنصورة، الطبعة الأولى، ص 26.

[66] خليل اعبية، مرجع سابق، ص93.

ونجد أن المادة (4) من القرار بقانون بشأن الجرائم الإلكترونية قد جرمت انتحال شخصية المواقع، والتي تتمثل بانتحال الجاني لشخصية صاحب موقع معين، فيظهر بشخصيته ويتفاعل ويتعامل باسم وهوية المالك الأصلي، ومثال هذه الصورة : حالة قيام الجاني بانتحال شخصية مالك النظام أو مستخدمه الأصلي أو يقنع المجني عليه بأنه خادم هذا الموقع ويطلب إليه إعادة إدخال اسم المستخدم وكلمة السر فيستغلها الجاني لتحقيق الجريمة، كما قد يقوم الجاني بشن هجوم على الموقع المستهدف بهدف فرض سيطرته عليه وتحويله إلى موقع وسيط، أو يخترق موقعاً مشهوراً لتقديم الخدمة ويركب برنامجه الإلكتروني عليه، ليتولى توجيه من يطلب اسم موقع الخدمة المشهور المغتصب إلى موقع الجاني الزائف، وهو ما يمكن أن يتم مع أكثر نظم الاتصال أماناً لإمكانية اختراق الحواجز الأمنية بهذه الطريقة التي يصعب اكتشافها[67].

ثانياً: انتحال الشخصية الإلكترونية بهدف الاحتيال الإلكتروني:

إن كل ما يؤدي إلى الخداع يمكن أن يعد طريقة احتيالية، ومن ثم فإن الكذب المجرد مهما كان منمقاً مرتباً يوحي بتصديقه لا يكفي وحده لتحقق الطريقة الاحتيالية، ما لم يكن مصاحباً بمظاهر خارجية أو أعمال مادية يعتمد النصاب أو المحتال حبكها، تحمل المجني عليه على تصديقه والاعتقاد بصحته؛ فكل ما من شانه إيهام المجني عليه وخداعة وإيقاعه في دائرة النصب والاحتيال يعد طريقة احتيال، مثال ذلك: القدرة على شفاء الناس من المرض، والإعلان عن مشروع استثماري عقاري وهو في الحقيقة مشروع وهمي [68].

ويعد الانترنت وسيلة لارتكاب جريمة الاحتيال الالكتروني، ويعد عنصراً أساسياً في الركن المادي لجريمة الاحتيال الالكتروني؛ حيث يستخدم في ارتكاب جميع أنواع الجرائم الالكترونية المختلفة، كسرقة بطاقات الائتمان وغيرها من الجرائم الأخرى التي تكون شبكة الانترنت هي الوسيلة المستخدمة في ارتكابها؛ وعليه فإنه يتوجب على الجاني المحتال، حتى يستطيع ممارسة أعماله

---

[67] خليل اعبية، مرجع سابق، ص94.

[68] علي الفيل، جريمة الاحتيال عبر البريد الالكتروني: دراسة مقارنة، مجلة الحقوق، جامعة الكويت، المجلد 36، العدد2، 2012م، ص 581.

الاحتيالية بصورة الكترونية، أن يكون قادراً على الإلمام ولو بالحد الأدنى بتقنية أجهزة الحاسب الالي، وكيفية استخدامه، وتسخيره للوصول إلى مبتغاه الاحتيالي الجرمي[69].

وفي هذه الصورة التي نصت عليها المادة (14) من القرار بقانون بشأن الجرائم الإلكترونية يكون السلوك المكون للركن المادي عبارة عن اتخاذ اسم كاذب يؤدي إلى الاستيلاء على مال الغير بطريق الحيلة والخداع بنية تملك هذا المال وحرمان صاحبه منه نهائياً، ويتمثل هذا المال في بيانات ومعلومات إلكترونية مالية أو متصلة بحقوق مالية؛ حيث يتوصل المحتال للمال برضاء المجني عليه تحت تأثير الاحتيال والتدليس الجنائي المتمثل في اتخاذ اسم كاذب أو انتحال صفة غير حقيقية[70].

وبناء على ما سبق نجد أن المشرع جرم انتحال الشخصية بهدف الاحتيال، والتي يقوم بها المنتحل باستخدام اسم كاذب بهدف الاستيلاء على ممتلكات الغير وهذا ما يعد احتيال.

والجدير بالإشارة أن السلوك المادي في جريمة انتحال الشخصية الإلكترونية يأخذ الصورة الإيجابية فقط أي القيام بفعل ما، أما الصورة السلبية (الامتناع عن القيام بفعل) فهي غير متصورة في هذه الجريمة التي تستلزم قيام المنتحل باستخدام قدراته العقلية واستخدام الحاسب الآلي للقيام بعملية الانتحال[71].

الفرع الثاني: النتيجة الإجرامية

تُعرف النتيجة الإجرامية بأنها: "كل نتيجة تحدث في العالم الخارجي تكون أثر لارتكاب السلوك الإجرامي، وتعتبر النتيجة الإجرامية من اهم العناصر في الركن المادي للجريمة ولها مدلول مادي يتمثل في الأثر ومدلول قانوني يتمثل في العدوان الذي ينطبق على السلوك الاجرامي بالنسبة للحق.[72]".

---

[69] حمزة المعايطة، جريمة الاحتيال الإلكتروني: دراسة تحليلية مقارنة، رسالة ماجستير، جامعة مؤتة، الأردن، 2012م، ص 47.

[70] خليل اعبية، مرجع سابق، ص 103.

[71] زيد بني خالد، مرجع سابق، ص 36.

[72] عبد القادر جرادة، مرجع سابق، ص 372

وتقسم الجرائم حسب النتيجة الإجرامية من حيث المعيار المادي، بالنظر إلى مدى تطلب حدوث نتيجة ما من عدمه، إلى جرائم شكلية وجرائم مادية، وتقسم حسب المعيار القانوني إلى جرائم الخطر، وجرائم الضرر، حيث أن الأولى لا يشترط لظهورها واستحقاق فاعلها العقاب تحقق نتيجة جرمية معينة، بل إن مجرد الإقدام على السلوك المجرم يوجب المسؤولية، وأكثر ظهور هذا النوع من الجرائم يكون في السلوكيات السلبية التي يحظرها المشرع، من ذلك الامتناع عن أداء الشهادة، في حين يكون من مستلزمات ظهور الجريمة في النوع الثاني تحقق نتيجة جرمية ضارة تلحق بالمصلحة العامة، أو المصلحة الخاصة، أو بكليهما، وإن كانت النتيجة الجرمية الضارة التي أصابت مصلحة يحميها القانون هي علة العقاب في جرائم الضرر، فإن الخطورة الجرمية الكامنة في نفس الفاعل في جرائم السياسة الجنائية التي ينتهجها المشرع الجزائي[73].

ويثور النقاش بشأن النتيجة الاجرامية في الجرائم الالكترونية فيما إذا كانت نتيجة الفعل الجرمي في العالم الافتراضي أم في العالم الحقيقي، وفي الحقيقة فإن الفرضيتان محتملات الحدوث في الجرائم الإلكترونية، فمن الممكن حدوثها بالعالم الحقيقي، مثل إزهاق روح إنسان كانت حياته مستمرة عن طريق جهاز كمبيوتر، فباختراق هذا الكمبيوتر (جريمة الكترونية) فإن نتيجتها تكون بالعالم الحقيقي بقتل هذا الإنسان[74].

ويجب ان تؤدي الوسائل التي يستخدمها الفاعل في الانتحال، إلى ايهام المجني عليه، وإيقاعه بالغلط الذي يحمله إلى تسليم المال للجاني مثلاً لكي تكتمل الجريمة، فتتحقق النتيجة الإجرامية في جريمة انتحال الشخصية الإلكترونية في استيلاء الجاني لنفسه أو لغيره على مال أو منفعة أو مستند أو توقيع على مستند، حيث يعد الاستيلاء على تلك الأمور هو النتيجة الإجرامية للسلوك المادي، فالجاني لا يكفي منه فقط أن يقوم بالأفعال مستخدماً وسائل انتحاليه، بدون

---

[73] أحمد مصطفى، جرائم الحاسبات الالية في التشريع المصري، دار النهضة العربية، 2010م، الطبعة الأولى، ص109.

[74] نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت، دار الفكر الجامعي، 2007 م، الطبعة الأولى، ص45.

تحقق نتيجة جرمية، وفي حال لم يتحقق التسليم نكون بصدد الشروع في ارتكاب جريمة انتحال الشخصية الإلكترونية؛ وذلك لعدم تحقق النتيجة الإجرامية بسبب خارج عن إرادة الجاني[75].

الفرع الثالث: علاقة السببية:

يقصد بعلاقة السببية الصلة التي تربط السلوك بالنتيجة، فهي تسند النتيجة إلى الفعل فتقرر بذلك توافر شرط أساسي من شروط المسؤولية الجنائية، وقد ثار حول علاقة السببية جدل كبير بين الفقهاء أثمر نظريات عديدة أهمها: نظرية تعادل الأسباب، ونظرية السبب الأقوى، ونظرية السبب الملائم [76].

ولتحقيق علاقة السببية في جريمة انتحال الشخصية الإلكترونية فلا بد من قيام الرابطة السببية بين طريقة الانتحال التي استخدمها الجاني في خداع المجني عليه والنتيجة المتمثلة في تسلم المال أو المستندات أو أي شيء أخر يكون محل الجرمية؛ أي أن تسلم الأمر الذي هدف إليه المنتحل كان نتيجة منطقية ثابتة للخدعة التي وقع بها المجني عليه. فعلاقة السببية في جريمة الانتحال تفيد أن ما قام به الجاني من أفعال وسلوكيات كانت هي السبب الذي حمل المجني عليه على تسليم المال أو نقل حيازته، أي أن يكون الاستيلاء ثمرة لما استخدمه الجاني من اتخاذ اسم كاذب او انتحال صفة غير صحيحة[77].

المطلب الثالث: الركن المعنوي

الركن المعنوي كقاعدة عامة هو السلوك غير المشروع للإدراك وللإرادة تجاه الواقعة الاجرامية ويبحث في توافر عنصر الارادة في الجريمة، وهو الذي يؤثر في تكوين صور الركن المعنوي والتي تأخذ منحى إما العمد، واما الخطأ. ولقيام المسئولية الجنائية يجب أن يكون الفعل غير المشروع مصحوب بعنصر العلم من خلال توافر ارادة اتجهت لارتكاب الفعل وهو عنصر الإرادة في الجريمة.

---

[75] محمد العجمي، جريمة انتحال الشخصية في مواقع التواصل الاجتماعي: دراسة فقهية مقارنة بالقانون الكويتي، مجلة الشريعة والدراسات الإسلامية، جامعة الكويت، المجلد 37، العدد 130، 2022م، ص195.

[76] عبد القادر جرادة، مرجع سابق، ص 375.

[77] علي الفيل، مرجع سابق، ص 590.

في هذا المطلب سيناقش الباحث الركن المعنوي لجريمة انتحال الشخصية الإلكترونية من خلال الفروع التالية:

الفرع الأول: القصد الجنائي العام:

يقوم القصد الجنائي العام على عنصرين، أولهما العلم، وثانيهما الإرادة، وهذا ما نص عليه قانون العقوبات رقم (16) لسنة 1960م والذي جاء فيه: "لا يحكم على أحد بعقوبة ما لم يكن قد أقدم على الفعل عن وعي وإرادة[78] " والوعي هو: " الإدراك والقدرة العقلية على التمييز وفهم عواقب سلوك الفرد فيختار العمل أو الامتناع " إلا أن الوعي لا ينعدم بالجهل بالقانون؛ لأن العلم بالقانون الجزائي أمر مفترض، ولا يعتبر جهل القانون عذراً لارتكاب الجريمة. أما الإرادة في المتطلب الأخر لقيام المسؤولية الجزائية وتعني:" القوة النفسية التي تحرك سلوك الجاني لتحقيق نتيجة جرمية عن رضا واختيار "

وبناء على ما سبق فلا تقوم جريمة انتحال الشخصية الإلكترونية ولا يُسأل الجاني جزائياً عنها إذا انعدمت فيه الأهلية الجنائية بتخلف التمييز أو حرية الاختيار، فالمجنون أو المصاب بعاهة عقلية أو نفسية إذا قام بجريمة انتحال الشخصية الالكترونية معتقداً على خلاف الحقيقة أنه صاحب الشخصية تمتنع مسؤوليته الجزائية، وكذلك الحال في باقي حالات موانع المسؤولية كصغر السن والسكر وغيرها[79].

ويتمثل القصد الجنائي العام في جريمة انتحال الشخصية الإلكترونية إذا توافر لدى المنتحل الوعي والإدراك والقصد الجرمي، فلا تقوم هذه الجريمة بطريق الخطأ[80].

ويتحقق القصد الجرمي بتوافر عنصريه العلم والإرادة، فيجب أن يكون الجاني المنتحل على علم بأن الأفعال التي يقترفها ويأتيها يعدها القانون انتحال، كما يجب أن يحيط الجاني علماً بماديات الواقعة الإجرامية، وهو هنا علم الجاني بأنه يستولي باستخدام انتحال الشخصية على المواقع الالكترونية على مال الغير أو منفعة أو مستند أو توقيع على نفسه، لنفسه أو لغيره، دون وجه

---

[78] انظر: المادة (74) من قانون العقوبات الأردني رقم 16 لسنة 1960.

[79] محمد صبحي نجم، قانون العقوبات، القسم العام، دار الثقافة، عمان، الطبعة السادسة، ص 230.

[80] خليل اعبية، مرجع سابق، ص96.

حق؛ مسبباً بذلك ضرراً للغير. كما يجب أن يكون على علم بأن هذا النوع من السلوكيات من شأنه خداع المجني عليه والنصب عليه وحمله على تسليم ما يريده المنتحل طواعية[81].

كما يشترط أن تتوجه إرادة المنتحل إلى ارتكاب السلوك الالكتروني المتمثل بانتحال شخصية الغير، والقصد هنا مسألة نفسية يضمرها الجاني ولا يستدل عليها إلا من ظروف القضية وملابساتها ووقائعها، وهي من المسائل الموضوعية التي تختص بها محكمة الموضوع دون معقب عليها، ولا تملك النيابة العامة البت في توافر القصد الجرمي من عدمه[82] .

ولا يُشترط علم المتهم بأن انتحال الشخصية الإلكترونية التي استعملها في النصب هي إحدى الوسائل التي نص عليها المشرع، فذلك علم بقانون الجزاء يُفترض توافره[83].

الفرع الثاني: القصد الجنائي الخاص

الملاحظ من النصوص القانونية التي تُعاقب على جريمة انتحال الشخصية الإلكترونية في التشريع الفلسطيني أن المشرع الفلسطيني تطلب توافر القصد الجنائي الخاص وهذا بدلالة نصوص المواد التي أشرنا إليها سابقاً أثناء الحديث عن الركن الشرعي.

ويتمثل القصد الجنائي الخاص في جريمة انتحال الشخصية الالكتروني في انصراف نية الجاني المحتال إلى الاستحواذ والاستيلاء على اسم الغير أو صفته؛ بحيث لا يستطيع المجني عليه مباشرة أي تصرف قانوني أو مادي عليه، ومن ثم فإذا لم تنصرف نية الجاني إلى الاستيلاء على اسم أو صفة الغير واستخدامه لخداع الاخرين، فعندئذ يعد القصد الجنائي الخاص منتفياً[84].

---

[81] علي الفيل، مرجع سابق، ص 591.

[82] خليل اعبية، مرجع سابق، ص 96.

[83] محمد العجمي، مرجع سابق، ص196.

[84] جلال ثروت، النظرية العامة لقانون العقوبات، مؤسسة الثقافة الجامعية، الاسكندرية، الطبعة الأولى، ص 209.

الفصل الثاني: القواعد الإجرائية لجريمة انتحال الشخصية الإلكترونية

لا شك أن حداثة بعض الجرائم ومن ضمنها جريمة انتحال الشخصية الالكترونية، والبحث في جمع أدلتها ووسائل ارتكابها والتوصل إلى مرتكبها، ووضع السبل الناجعة في مكافحتها، يواجه العديد من الصعوبات من الناحية الإجرائية؛ نظراً لحداثة وسائل ارتكاب تلك الجريمة التي تعتمد على تقنيات حديثة.

وتتطلب معالجة جريمة انتحال الشخصية الالكترونية والحد منها تحقيقاً فعالاً وقدرة عالية على جمع الأدلة والإثبات الجنائي، وهذا النهج يتطلب الاستجابة للصعوبات القانونية التي تعيق تنفيذ القانون وصولاً للتحقيق والمحاكمة في جريمة انتحال الشخصية الإلكترونية.

وقد حرصت كافة التشريعات الحديثة في مختلف الدول ومن بينها التشريع الفلسطيني على تنظيم قواعد إجرائية خاصة بالجرائم الإلكترونية؛ حيث احتوى القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على مجموعة من القواعد الإجرائية التي تساعد في التحقيق بالجرائم الإلكترونية إضافة إلى القواعد العامة الواردة في قانون الإجراءات الجزائية.

وبهدف ضمان وسلامة تطبيق القواعد الإجرائية في جريمة انتحال الشخصية الإلكترونية، من حيث القواعد المتعلقة بالتحري والتحقيق والمحاكمة، فقد أنشأت السلطة الوطنية الفلسطينية قسماً خاصاً بالتحقيق في الجرائم الالكترونية وجمع الأدلة الرقمية يتبع الشرطة الفلسطينية، وذلك لإدراكهم أهمية تكنولوجيا المعلومات كمفتاح لتحسين أداء الإدارة والأمن على السواء.

في هذا الفصل سيناقش الباحث القواعد الاجرائية لجريمة انتحال الشخصية الالكترونية، وذلك من خلال المباحث التالية.

المبحث الأول: إجراءات التحري والتحقيق في جريمة انتحال الشخصية الالكترونية.

المبحث الثاني: إجراءات المحاكمة والاثبات في جريمة انتحال الشخصية الالكترونية والعقوبة المقررة لها.

المبحث الأول: إجراءات التحري والتحقيق في جريمة انتحال الشخصية الالكترونية.

من المعلوم أن جريمة انتحال الشخصية الإلكترونية تندرج ضمن الجرائم المعلوماتية والتي تحتاج الى أدلة وبيانات ذات طبيعة معلوماتية وفنية، الأمر الذي يتطلب من رجال الضبط القضائي، أن يكونوا على قدر ودراية جيدة في الإلمام بطبيعة عمل الحاسب الالي ونظم المعلومات ليتمكنوا من مباشرة إجراءات جمع الاستدلات. ويمكن القول بان التحري الالكتروني إنما يتم عبر الحواسيب ونظم المعلومات وشبكة الانترنت وهو عمل أمنى وقانوني يقوم به مأموري الضبط القضائي بواسطة التقنيات الالكترونية والرقمية للحصول على المعلومات عن الأشخاص أو الأماكن أو الأشياء وذلك للحد من تلك الجريمة أو ضبطها.

وللتحقيق أهمية كبيرة في إثبات وقوع جريمة انتحال الشخصية الالكترونية وإقامة الدليل على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو يدل عليه استجلاء الحقيقة لغرض الوصول إلى ملاحقة المشتكى عليه من عدمه بعد جمع الأدلة القائمة على الجرائم الإلكترونية.

في هذا المبحث سيتطرق الباحث إلى إجراءات التحري والتحقيق في جريمة انتحال الشخصية الالكترونية، وذلك من خلال المطالب التالية.

المطلب الأول: إجراءات الاستدلال في جريمة انتحال الشخصية الالكترونية.

يعرف الاستدلال بأنه: "جمع المعلومات والبيانات الخاصة بالجريمة، عن طريق التحري عنها والبحث عن فاعليها بشتى الطرق والوسائل القانونية وبالتالي إعداد العناصر اللازمة للبدء في التحقيق في الجريمة، ويعبر البعض عن الاستدلال بالتحريات[85]"

جريمة انتحال الشخصية الإلكترونية مثل أنواع الجرائم الأخرى، تمر بذات مرحلة الاستدلال والتحري المتكامل، وما يترتب على ذلك من إجراءات قانونية وفنية وشكلية، إلا أن الطبيعة الخاصة التي تتميز بها جريمة انتحال الشخصية الإلكترونية ينتج عنها صعوبات تتعلق بالاستدلال والتحري، ويرجع ذلك إلى كون مسرح الجريمة في هذه الجريمة يختلف بشكل تام عن مسرح الجريمة في الجرائم التقليدية.

في هذا المطلب سيوضح الباحث إجراءات الاستدلال المتبعة في ملاحقة جريمة انتحال الشخصية الإلكترونية وذلك من خلال الفروع التالية.

الفرع الأول: معاينة مسرح جريمة انتحال الشخصية الإلكترونية

يتم بدء التحري والاستدلال في جريمة انتحال الشخصية الإلكترونية بناء على الشكوى المحالة من قبل النيابة العامة، ويباشر التحقيق الفني الاستدلالي بعد توجيه كتاب من قبل وكيل النيابة إلى وحدة الجرائم الإلكترونية؛ حيث يقوم الضابط المعني ومن وقت وصول كتابة النيابة العامة، بسماع افادة المشتكى عليه، وهي هنا ليست استجواباً وإنما إفادة بالواقعة التي حصلت مع الشاكي وخاصة الوسائط الإلكترونية ذات الصلة بالجريمة محل التحقيق، وفي ضوء أقوال

[85] رؤوف عبيد، مبادئ الإجراءات، مكتبة النهضة، مصر، 1956م، ص 208.

صاحب الشكوى وما يسلمه لوحدة الجرائم الإلكترونية من أوراق أو تطبيقات أو أجهزة، يشرع الضابط المسؤول بجمع الأدلة الاستدلالية من مسرح الجريمة[86].

وبعد تلقي البلاغ عن جريمة انتحال الشخصية الإلكترونية، تأتي الخطوة التالية، وهي الانتقال لمعاينة مسرح الجريمة والتي غالباً ما يقوم بها رجال الضبط القضائي للكشف على مكان وقوع الجريمة وفحصه والتحفظ على أي آثار أو مخلفات أو متعلقات مادية تمت بصلة إلى الجريمة ومرتكبيها، وكذلك تصوير الموقع ووضع السيناريوهات المقترحة لكيفية حدوثها وزمن ارتكابها والملابسات المحيطة بها وإثباتها على مرتكبها[87].

ويعد مسرح جريمة انتحال الشخصية الإلكترونية هو المفتاح الأول لحل لغز هذه الجريمة، ولذلك أطلق عليه البعض الشاهد الصامت، وبذلك يعتبر مسرح الجريمة اللبنة الاولى والهامة لبداية التعامل مع جريمة انتحال الشخصية الإلكترونية، فانطلاقاً من القاعدة الفقهية التي تقول ما بني على باطل فهو باطل والعكس صحيح فإذا صلحت الإجراءات المتخذة التي يقوم بها فريق مسرح الجريمة صلح التحقيق في القضية بأكملها.

ويمكن تعريف مسرح الجريمة بشكل عام بأنه: " المكان الذي تقع فيه الحادثة الجنائية أو المكان الذي تنقل إليه بعض ظواهر الجريمة مثل العثور على جثة المجني عليه، أو العثور على أدلة الجريمة به[88]" كما يعرف بأنه: "المكان الذي تنبثق منه كافة الأدلة، فهو الذي يزود ضابط التحقيق بنقطة البدء في بحثه عن الفاعل، ويكشف عن معلومات هامة لمن يفد بعد ذلك من الأخصائيين[89]".

أما مسرح الجريمة في الجرائم الالكترونية فإنه يختلف عن مفهوم مسرح الجريمة بمعناه التقليدي؛ كون أنه لا وجود لمسرح جريمة بشكل مادي في الجرائم الالكترونية، وإنما يكون المسرح هو افتراضي مكانه الخوادم والمواصلات وأجهزة التخزين المربوطة بالشبكة العنكبوتية، لا سيما تلك

---

[86] مصطفى الرواشدة، جريمة الابتزاز الإلكتروني في القانون الأردني، رسالة ماجستير، عمادة الدراسات العليا، جامعة آل البيت، 2019م، ص41.

[87] عبد الفتاح مراد، مرجع سابق، ص 247.

[88] سعد سلامة، معاينة مسرح الجريمة والاثبات الجنائي، أكاديمية الشرطة، كلية الشرطة، مصر، ص 18.

[89] محمد عنب، معاينة مسرح الجريمة، رسالة دكتوراة، كلية الدراسات العليا، أكاديمية الشرطة، مصر، 1988م، ص 105.

التي تحاط بتأمين مثل البنوك وغيرها. كما أن عملية الانتقال والمعاينة في الجرائم الإلكترونية تواجه العديد من الإشكالات الإجرائية أثناء سير إجراءات التحقيق، ونجد أن عملية الانتقال والمعاينة في الجرائم الالكترونية تتطلب شروطاً خاصة لا بد أن تتوفر في مجريها، مثل الخبرة في مجال الأمن المعلوماتي وغيره من المجالات المتصلة بالبيئة الرقمية، فتختلف هنا المعاينة للجرائم التقليدية عن المعاينة في الجرائم الالكترونية؛ كون أن البيئة في المجال التقني مختلفة تماماً عن البيئة في أرض الواقع، وكون أن الجريمة الإلكترونية هي جريمة مستمرة الأثر تقبع في عالم افتراضي، بخلاف الجرائم الاعتيادية والتي حدثت وانتهت في الماضي وأحدثت آثارها بشكل مادي في أرض الواقع[90].

ويتكون مسرح جريمة انتحال الشخصية الإلكترونية من قسمان هما[91]:

أ. مسرح تقليدي: يقع خارج بيئة الحاسوب والانترنت، ويتكون بشكل أساسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، قد يترك فيه الجاني عدة آثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

ب. مسرح افتراضي: ويقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الإنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله، فإذا كانت عملية الانتقال إلى المسرح التقليدي تتم بطريقة مادية، فالأمر يختلف بالنسبة إلى المسرح الافتراضي، فلا يكون الانتقال بالضرورة عبر العالم المادي، وإنما يتم الانتقال عبر العالم الافتراضي، حيث يستطيع عضو سلطة التحقيق أو مأمور الضبط القضائي أن يقوم بهذه المعاينة وهو جالس في مكتبه من خلال الحاسوب الموضوع في المحكمة، كما يمكنه أن يلجأ إلى مقر مزود الإنترنت الذي يعد أفضل مكان يمكن من خلاله إجراء معاينة مسرح الجريمة الإلكترونية.

---

[90] عبد اللطيف ربايعة، مرجع سابق، ص 10.

[91] عادل عثمان، ضبط الأدلة في مجال الجريمة المعلوماتية، رابطة الأدب الحديث، مجلة فكرة وإبداع، المجلد 113، 2017م، ص 192.

وكما نعلم بأن أول مهمة لرجال الضبط القضائي بمجرد علمهم بوقوع جريمة الانتقال إلى مسرح جريمة انتحال الشخصية الإلكترونية ومعاينته، حيث يقصد بالمعاينة في الجرائم الإلكترونية: "معاينة الآثار التي يتركها مستخدم الشبكة الإلكترونية أو الإنترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها، وكل الاتصالات التي تمت من خلال الحاسوب الآلي والشبكة الإلكترونية[92]"

ووفقاً لنص المادة 27 من قانون الإجراءات الجزائية الفلسطيني فيجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فورا إلى مكان الجريمة، ويعاين الآثار المادية لها ويتحفظ عليها، ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة ويسمع أقوال من كان حاضرا أو من يمكن منه الحصول على إيضاحات في شأن الجريمة ومرتكبيها، ويجب عليه أن يخطر النيابة العامة فورا بانتقاله، ويجب على عضو النيابة المختص بمجرد إخطاره بجناية متلبس بها الانتقال فورا إلى مكان الجريمة[93].

ويلاحظ من المادة السابقة أن مسرح الجريمة في الجرائم العادية واضح المعالم وكل ما يتطلبه من مأمور الضبط القضائي ووكيل النيابة المحقق معاينته وتحديد أوصافه وضبط ما فيه من أدوات جرمية، بينما مسرح الجريمة الالكترونية حتما ليس بوضوح مسرح الجريمة العادية، فالبحث فيه سيتم باستخدام الأجهزة الالكترونية، والأجهزة أو الأدلة الالكترونية لها أشكال مختلفة، فقد تكون كمبيوتر وقد تكون هاتف خلوي، وطريقة ضبط الأجهزة الالكترونية ليس بالأمر البسيط، فقد تكون جهاز كمبيوتر واحد وقد تكون عدة أجهزة، وقد يكون الجهاز في حالة تشغيل[94].

وتعد معاينة مسرح جريمة انتحال الشخصية الإلكترونية صعبة للغاية، ويرجع ذلك لسببين هما[95]:

---

[92] سعيد المزروعي، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقا للتشريع الإماراتي، مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث غزة، المجلد 2، العدد 13، 2018م، ص 117.

[93] انظر: المادة (27) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[94] علاء شريم، أدلة مسرح الجريمة وحجيتها في الإثبات الجنائي: دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2021م، ص15.

[95] سعيد المزروعي، مرجع سابق، ص 119.

أ. أن جريمة انتحال الشخصية الإلكترونية لا تخلف في الغالب آثاراً مادية يمكن فحصها أو معاينتها، خلافاً للجرائم التقليدية التي غالباً ما تخلف وراءها أثاراً مادية ملموسة، كالشعر والدماء وبصمات الأصابع وغيرها، أما جريمة انتحال الشخصية الإلكترونية، فهي جريمة مستترة لا تخلف وراءها في الغالب أية آثار مادية، وكل ما يمكن أن تخلفه هو عبارة عن بيانات الكترونية، يصعب جداً إجراء أية معاينة عليها أو ضبطها.

ب. كثرة الأشخاص الذين يترددون على مسرح الجريمة خلال الفترة من وقت وقوع الجريمة وحتى وقت اكتشافها والتحقيق بها.

ومن المعلوم أنه حتى تكون معاينة مسرح الجريمة ذات فائدة للمحقق، فلا بد من الإسراع في إجرائها قبل أن يحدث أي تغيير على مسرح الجريمة، وهذا الأمر يصعب تصوره في جريمة انتحال الشخصية الإلكترونية بالنظر إلى صعوبة اكتشاف هذه الجريمة، الأمر الذي يعطي الفرصة للجاني أو للأخرين بأن يتلفوا أو يعبثوا بالآثار التي قد تخلفها الجريمة، وهو الأمر الذي سيكون له تأثير على قيمة الأدلة المتحصلة من معاينة مسرح الجريمة.

وتحتاج معاينة مسرح جريمة انتحال الشخصية الإلكترونية إلى مهارات فنية خاصة وإلى كوادر مدربة حتى تكون قادرة على معاينة مسرح تلك الجريمة الذي لا حدود لها، فهو منتشر على شبكة الإنترنت العالمية في جميع دول العالم، ولذلك فقد نصت المادة (3) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: "1. تنشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية"، وتتولى النيابة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه. 2. تتولى المحاكم النظامية والنيابة العامة، وفقاً لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية.[96]"

والجدير ذكره أن المشرع الفلسطيني في قانون الإجراءات الجزائية رقم 3 لسنة 2001 لم يشترط إجراء المعاينة في زمن محدد، إلا أن مضمون النصوص تشير إلى وجوب إجراءها عقب ارتكاب الجريمة وبمجرد علم السلطات بها ولا يقصد من ذلك أن يبدأ المحقق إجراءات التحقيق بالمعاينة

[96] انظر: المادة (3) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

وترك الحرية لفريق مسرح الجريمة في التقدير إلى الانتقال لإجراء المعاينة من عدمه وتحديد اختيار الوقت أيضاً للانتقال[97].

وعلى الرغم من تضاؤل أهمية المعاينة في جريمة انتحال الشخصية الإلكترونية، إلا أنه وفي حالة العلم بوقوع تلك الجريمة، فيجب التحرك بسرعة إلى مسرح الجريمة لإجراء المعاينة، وقد يكون انتقال المحقق انتقالاً مادياً لمسرح الجريمة، وقد ينتقل إلى مسرح الجريمة في العالم الافتراضي عن طريق الحاسوب الموجود في مكتبه، او من حاسوب آخر، كما قد يكون الانتقال إلى المكان الذي تحقق فيه الجريمة الالكترونية، سواء كان مصرفاً أو مؤسسة مالية، أو مشروعاً صناعياً أو كان مسرح الجريمة حاسوب أحد الأشخاص، او ينتقل المحقق إلى مقر مزود الخدمة الذي يعد أفضل الأماكن لإجراء المعاينة[98].

وفي كافة الأحوال يحب على المحقق إتباع عدة قواعد فنية، تضمن له الحصول على الأدلة عند معاينة مسرح جريمة انتحال الشخصية الإلكترونية، ومن تلك القواعد ما يلي:

أ. قصر إجراء المعاينة على الأشخاص ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسوب وتقنية المعلومات، ممن تلقوا تدريبات في مجال الحاسب الآلي، وكيفية التعامل مع الجرائم الالكترونية وجمع أدلتها، فإن لم يوجد ممن تتوافر فيهم هذه الشروط، فيجب على المحقق الاستعانة بأهل الخبرة[99].

ب. تأمين جهاز الحاسب الآلي، وعدم السماح للمتهم أو أي شخص أخر له علاقة بالجريمة استعمال الحاسب محل الجريمة أو أي حاسب آخر متصل بالشبكة[100].

ت. تحديد نوع الجهاز – أو الأجهزة – محل المعاينة، وما إذا كانت متصلة بالشبكة أو كانت أجهزة معزولة، وإذا كان الجهاز متصلاً بالشبكة فيجب معرفة أنواع أجهزة الاتصال، وإحصاء الطرفيات وتحديد طبيعة الروابط الموجودة بينها، لمعرفة الطريقة

---

[97] علاء شريم، مرجع سابق،.ص 16

[98] حسن طاهر داوود، جرائم نظم المعلومات، أكاديمية نايف للعلوم الأمنية، الرياض، السعودية، الطبعة الأولى، 2000م، ص 122.

[99] حسن طاهر داوود، مرجع سابق، ص 62.

[100] المرجع السابق

التي تتم بها عملية نقل البيانات من موقع لآخر وإن كان ثمة أجهزة أخرى متصلة بجهاز الحاسب خارج المنطقة[101].

ث. حماية البيانات المخزنة على جهاز الحاسب من محاولة العبث بها أو تدميرها، لهذا يجب التعامل بحرفية مع تلك البيانات، فمثلاً إن كان الجهاز يعمل فيجب تركه يعمل، وإن كان مطفئاً فيجب عدم تشغيله إلا بعد التأكد من خلوه من أية برامج قد تدمر البيانات المخزنة على قرصه الصلب عند التشغيل أو عند إيقاف تشغيل الجهاز، كما يجب تأمين عدم انقطاع التيار الكهربائي عن الجهاز، لتجنب إتلاف وتدمير البيانات نتيجة لذلك الانقطاع[102].

ج. قبل القيام بتفحص أو نقل جهاز الحاسب أو أي من ملحقاته يجب القيام بتصوير فوتوغرافي للحاسب الآلي وما يتصل به من أجهزة طرفية، وخصوصاً الأجزاء الخلفية للجهاز، كما يجب حفظ ما يظهر على شاشة العرض باستخدام برمجية تجميد الشاشة، وكذلك حفظ الموقع الالكترونية باستخدام خاصية الحفظ المتوفرة في نظام التشغيل[103].

ح. جمع الدليل، فيجب الاهتمام بجمع كل البيانات الموجودة في مسرح الجريمة والتي تشكل أدلة تفيد التحقيق، لذا يجب على المحقق الاهتمام بتفحص جهاز الحاسب وعلى الأخص الرسائل الواردة عبر البريد الالكتروني وذلك لمعرفة عنوان بريد المرسل، وعنوان الحاسوب المستخدم، كما على المحقق أن يقوم بتفحص البرامج المثبتة داخل جهاز الحاسب الآلي وإن كان ثمة برنامج مخبأ، كما يجب التعرف على نوع الفيروس الذي هاجم النظام لأن ذلك قد يساعد في التعرف على الشخص الذي استعمله[104] .

---

[101] عبد الفتاح حجازي، مرجع سابق، ص 190.

[102] عبد الفتاح حجازي، مرجع سابق، ص 190.

[103] عبد الفتاح حجازي، مرجع سابق، ص 190.

[104] وليد دقديقة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية، رسالة ماجستير، كلية القانون، جامعة طرابلس، ليبيا، 2015م، ص 52 .

خ. الحرص على حماية أي مادة معلوماتية أو وسائط تخزين تم ضبطها من التعرض لعوامل قد تفسد البيانات المخزنة عليها، وذلك كالحرارة أو الرطوبة أو الغبار أو أي مجالات مغناطيسية قد تدمر تلك البيانات[105].

الفرع الثاني: وسائل البحث عن الأدلة في جريمة انتحال الشخصية الإلكترونية

تعد الأدلة التقليدية عاجزة على تأدية دورها في عملية إثبات جريمة انتحال الشخصية الإلكترونية، ولذلك ظهر ما يعرف بالدليل الإلكتروني، الذي يتم الحصول عليه من خلال عملية جمع المعلومات في مسرح الجريمة الإلكترونية سواء كان في حاسوب الجاني أو المجني عليه، أو في غرف المحادثة، أو في المواقع الإلكترونية التي سبق وزار أي منهما، فالأدلة الإلكترونية التي تنتج عن هذا البحث والتحري التقني تبقى هي الاساس الأول والحدث المهم الذي يمكن به التوصل إلى دليل قاطع يثبت الجريمة الإلكترونية[106].

وقد تعددت تعريفات الدليل الالكتروني واختلف الفقه فيها، فاتجه البعض منه نحو التوسع في تعريف الدليل الالكتروني، والبعض الاخر نحو تضييقه وحصره في نواح معينة، وذلك بحسب الزاوية والمجال الذي ينظرون اليه، فعرف البعض الدليل الالكتروني بأنه: " دليل مأخوذ من أجهزة الحاسوب ويكون في شكل مجالات أو نبضات مغناطيسية أو كهرومغناطيسية، يمكن تجميعها وتحليلها باستخدام البرامج والتطبيقات والتكنولوجيا الخاصة، ويتم تقديمها في شكل أدلة معتبرة أمام القضاء[107]"

كما يعرف الدليل الالكتروني على أنه: " دليل يتم الحصول عليه بواسطة تقنية فنية الكترونية من معطيات الحاسوب وشبكة الانترنت والأجهزة الالكترونية الملحقة والتي تتصل به وشبكات

---

[105] وليد دقديقة، مرجع سابق، ص 53.

[106] مسعود المعمري، مرجع سابق، ص 198.

[107] هلال امنة، الاثبات الجنائي بالدليل الإلكتروني، رسالة ماجستير، جامعة محمد خيضر، بسكرة، الجزائر،2015م،ص7.

الاتصال من خلال الاجراءات القانونية لتقدم للقضاء كأحد الأدلة الالكترونية الجنائية التي تصلح لإثبات الجريمة [108]"

وعرفه بعض الفقهاء بأنه : " دليل مأخوذ من أجهزة الحاسوب ويكون في شكل مجالات أو نبضات مغناطيسية أو كهرومغناطيسية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل نصوص مكتوبة أو صور أو أصوات وأشكال ورسوم وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة انفاذ وتطبيق القانون[109]" كما يعرف على أنه : " الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الالي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية؛ لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات؛ لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها[110] "

وقد عرف البعض الدليل الالكتروني بالمفهوم الواسع، فذكروا أنه: "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية، بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الالي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه[111] "

وقد عرف المشرع الأردني الدليل الالكتروني في قانون المعاملات الالكترونية رقم (15) لعام 2015 في المادة الثانية تحت عنوان المعلومات الالكترونية بأنها: "البيانات أو النصوص أو

---

[108] منصور، المعايطة، الأدلة الجنائية والتحقيق الجنائي، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2007م، ص 18.

[109] أحمد، الحديثي، قيمة الدليل الإلكتروني في الإثبات الجنائي: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة عمان الاهلية، الأردن، 2019م، ص33.

[110] عبد الناصر فرغلي، ومحمد المسماري، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، مقدم في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الامنية، الرياض، 2007م، ص 13 .

[111] ميسون الحمداني، مشروعية الادلة الالكترونية في الاثبات الجنائي، بحث منشور، كلية الحقوق، جامعة النهرين، بغداد، 2007م،ص196.

الصور أو الرسومات أو الأشكال أو الأصوات أو الرموز أو قواعد البيانات وما شابه ذلك " أما بالنسبة للمشرع الفلسطيني، فلم يورد تعريف صريح للدليل الالكتروني كما فعل المشرع الأردني، إلا أنه أورد العديد من المصطلحات المشابهة للدليل الالكتروني فنص القرار بقانون رقم (15) لسنة 2017م بشأن المعاملات الإلكترونية على العديد من المصطلحات، حيث عرف البيانات الإلكترونية بأنها: "بيانات ممثلة أو مرمزة إلكترونيا سواء على شكل نص أو رمز أو صوت أو صور أو غيرها. " كما عرف السجل الإلكتروني بأنه: " مجموعة المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية والتي تشكل بمجملها وصفاً لحالة شخص أو شيء ما.[112]"

وبناء على التعريفات السابقة فإن الباحث يرى بأن الدليل الإلكتروني هو: "مجموعة المجالات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية "

ويوجد للدليل الالكتروني العديد من الصور والاشكال، حيث قسمها البعض إلى الأقسام التالية:

أ. أدلة رقيمة خاصة بأدلة الحاسب الالي وشبكاتها: وهي سلوك بشري يشكل فعل غير مشروع على أجهزة الحاسوب، سواء كان هذا الامر واقع على المكونات المادية له أو المكونات المعنوية، أو قواعد البيانات الرئيسية، مثل تخريب مكونات الحاسوب كالطابعة[113] .

ب. الأدلة الالكترونية المتعلقة بالشبكة العالمية للمعلومات: وهي سلوك بشري شكل فعلاً غير مشروع قانوناً يقع على أي وثيقة أو نص موجود بالشبكة مثل قرصنة المعلومات وسرقة أرقام بطاقات الائتمان، وانتهاك الملكية الفكرية للبرامج وغيرها، فهذا النوع من البرامج يتطلب اتصالاً بالإنترنت. كما إن هذا السلوك البشري غير المشروع يقع على الية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات، مثل جرائم الدخول غير المشروع لمواقع يمنع الدخول غليها، واستخدام عناوين (ip) غير حقيقة للولوج إلى الشبكة العالمية للمعلومات وغيرها.

---

[112] انظر: المادة (1) من القرار بقانون رقم (15) لسنة 2017م بشأن المعاملات الإلكترونية.

[113] امنة هلال، مرجع سابق، ص 9.

ت. الأدلة الالكترونية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات: وهي متعلقة بالجرائم التي ترتكب باستخدام الكمبيوتر، بحيث لا يعتبر استخدام الكمبيوتر أو الشبكة العالمية للمعلومات أو الانترنت في هذه الجرائم من طبيعة الفعل الجرمي، بل تستخدم كوسيلة مساعدة لارتكاب الجريمة مثل غسيل الأموال أو نقل المخدرات من مكان لأخر، وجهاز الكمبيوتر في هذه الحالة يحتفظ بآثار الكترونية يمكن أن تستخدم للإرشاد عن الفاعل[114].

والجدير ذكره أنه يمكن أيضاً تقسيم الدليل الالكتروني إلى نوعين رئيسيين، هما[115]:

أ. أدلة اعدت لتكون وسيلة إثبات: ويمكن اجمال هذا النوع من الأدلة الالكترونية يمكن فيما يلي:

1- السجلات التي تم انشاؤها بواسطة الألة تلقائياً، وتعتبر هذه السجلات من مخرجات الالة التي لم يساهم الانسان في انشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.

2- السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الالة، ومن أمثلة ذلك البيانات التي تم إدخالها الى الألة وتتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

ب. أدلة لم تعد لتكون وسيلة اثبات: إن هذا النوع من الأدلة الالكترونية نشأ دون ارادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الالكترونية، وهي ما يمكن تسميته أيضاً بالأثار المعلوماتية الالكترونية، وهي تتجسد في الاثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الالة أو شبكة المعلومات العالمية، والواقع أن هذا النوع من الادلة لم يعد أساساً للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من انشائها، فالاتصالات التي تجري عبر الانترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها، جميعها يمكن ضبطها بواسطة تقنية خاصة بذلك .

---

[114] نبيل جاد، جرائم الحاسب الالي، مطبعة بن دسمال، الطبعة الأولى، دبي، 2014م، ص 128.

[115] خالد ابراهيم، التقاضي الالكتروني، القاهرة، دار الفكر الجامعي، 2008، ص 97-98.

ويتخذ الدليل الإلكتروني ثلاثة أشكال رئيسية هي[116]:

أ. الصور الرقمية: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة إما في شكل ورقي او في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطوراً ولكنها ليست بالصورة أفضل من الصورة التقليدية.

ب. التسجيلات الصوتية: وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الالة الرقمية، وتشمل المحادثات الصوتية على الإنترنت والهاتف وغيرها.

ت. النصوص المكتوبة: وتشمل النصوص التي يتم كتابتها بواسطة الالة الرقمية، ومنها الرسائل عبر البريد الالكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي، ووسائل التواصل الاجتماعي المعروفة في وقتنا الحالي مثل " واتساب "

ويجد محققو الشرطة والاجهزة المعنية بجمع الادلة أنفسهم في مواجهة مع تحديات تقنية المعلومات، ويضطرون إلى التعامل مع أجهزة الكمبيوتر والاتصالات ومع البرامج وقواعد البيانات متى ما اتصلت بجريمة انتحال الشخصية الإلكترونية، وبالتالي فإن ما يتعين على المحقق عمله في بيئة الحاسب الالي والانترنت يتطلب ابتداء المعرفة الكافية والتدريب العلمي فيما يتعلق بالحصول على الأدلة، وحفظها لتقديمها إلى المحكمة؛ لان الادلة وإجراءات التحري والتحقيق في بيئة جرائم الكمبيوتر لا يكفيها المعرفة العامة، بل تحتاج تدريباً متواصلا يتوازن مع التحديات الجديدة في عالم التقنية .

ويجب على سلطات الاستدلال أثناء قيامها بالمعاينة التحفظ على جميع أدوات ارتكاب جريمة الاحتيال الالكتروني أو ما ينتج عنها، لذلك ينبغي على القائمين على معاينة مسرح الجريمة مراعاة ما يلي[117]:

أ. التحفظ على الاجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الأشياء التي يعتقد أن لها صلة بالجريمة.

---

[116] عائشة مصطفى، مرجع سابق، ص 72.

[117] مسعود المعمري، الدليل الالكتروني لإثبات الجريمة الالكترونية، مجلة كلية القانون الكويتية العالمية، العدد 3، 2018م، ص195.

ب. إثبات الطريقة التي تم بواسطتها إعداد النظام والعمليات الإلكترونية، وخاصة ما تحتويه السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام.

ت. إثبات حالة التوصيلات والكيبلات المتصلة بمكونات النظام كله، وذلك لإجراء المقارنة اللازمة عند عرض الأمر على القضاء.

ث. عدم نقل أية مادة متحفظ عليها من مسرح الجريمة قبل التأكد من خلو المحيط الخارجي بموقع الحاسب الالي من أية مجالات لقوة مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة عليها.

ويمكن لمأمور الضبط القضائي الحصول على الدليل الإلكتروني على جريمة انتحال الشخصية الإلكترونية، من خلال الدخول إلى العالم الافتراضي، بهدف البحث عن جريمة الانتحال وكشف مرتكبها لتقديمهم للمحاكم المختصة، كما يمكن أن يقوم مأمور الضبط القضائي بالبحث والتحري بنفسه عن مرتكب جريمة انتحال الشخصية الإلكترونية من خلال الحصول على إذن رسمي لمباشرة مهامه في البحث والتحري عن تلك الجريمة ومرتكبها، ويجب أن يتضمن الإذن على رقم الحاسوب وصلاحيته للعمل وخلوه من العوائق التكنولوجية واحتواءه على برمجيات أصلية وليست منسوخة، ثم يجلس بعد ذلك أمام حاسوب متصل بالشبكة الإلكترونية للقيام بعمله بالتحري، وذلك من خلال دخوله في نقاشات مع الغير باستخدام أسماء مستعارة لأشخاص أو لهيئات مختلفة عبر قاعات الدردشة وحلقات النقاش[118].

كما يمكن لمأمور الضبط القضائي الحصول على الأدلة الإلكترونية لإثبات جريمة انتحال الشخصية الإلكترونية من خلال تتبع مرتكب تلك الجريمة إلكترونياً، ويكون ذلك عن طريق تحديد الجهاز المستخدم في ارتكاب الجريمة وتحديد موقعه، حيث لكل كمبيوتر متصل بالإنترنت

[118] نبيلة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2013م، ص 195.

عنوان خاص به، وهذا العنوان يتكون من جزئين، الأول يشمل أرقام الشبكة والثاني يشمل أرقام مقدم الخدمة[119] ، وهناك جانبان رئيسيان للتتبع الإلكتروني هما:

أولاً: الرجوع على مزودي الخدمة:

تكون جميع معلومات المشتركين مرتبطة بالحساب الخاص بهم لدى مزودي الخدمة باسم الحساب الشخصي الخاص بهم، وحالة الاشتراك ومعلومات الفواتير، إضافة إلى هوية الهواتف الخاصة بهم وبرتوكولات الإنترنت التي قاموا بزيارتها في الوقت والتاريخ المحددان، وقد ألزمت المادة (1/51) من القرار بقانون بشأن الجرائم الالكترونية لعام 2018م مزود الخدمة بتزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناء على طلب النيابة أو المحكمة المختصة[120].

فعند وجود شكوى حول ارتكاب جريمة انتحال الشخصية الإلكترونية، فهنا يتم فحص جهاز الحاسوب للمشتبه به، ومعرفة عنوان الانترنت الخاص به، ومن ثم يتم مخاطبة الشركة التي يتبعها رقم العنوان للحصول على بيانات المستخدم الذي انتحل اسم شخص ما وقام بإرسال بيانات أو بريد الكتروني باسمه، حيث ألزم القرار بقانون بشأن الجرائم الإلكترونية لعام 2018م على مزودي الخدمة أن يحتفظوا بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات[121].

ثانياً: مراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها:

تستخدم هذه الطريقة في تتبع المشتبه به في ارتكاب جريمة انتحال الشخصية الإلكترونية، حيث يتم مراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها ومراقبة الاتصالات السلكية واللاسلكية التي يجريها المشتبه به من هاتفه، وقد نظم قانون الإجراءات الجزائية الفلسطيني قبل صدور القرار بقانون بشأن الجرائم الإلكترونية تلك العملية، حيث نصت المادة (51) على أنه: "يجوز للنائب العام أو أحد مساعديه مراقبة المحادثات السلكية واللاسلكية، وإجراء تسجيلات لأحاديث في مكان خاص بناء على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في

---

[119] إيهاب التاج، التحقيق وجمع الأدلة في الجرائم المعلوماتية، مجلة العدل، وزارة العدل، المملكة العربية السعودية، المجلد 11، العدد 26، 2009م، ص404.

[120] انظر: المادة (1/51) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[121] انظر: المادة (51/2) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة[122]" كما نظم تلك العملية القرار بقانون بشأن الجرائم الإلكترونية لعام 2018م حيث نصت المادة (54) منه على أنه: "لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها ..[123] "

المطلب الثاني: إجراءات التحقيق في جريمة انتحال الشخصية الالكترونية.

بعد الانتهاء من مرحلة جمع الاستدلالات يتم الانتقال إلى مرحلة التحقيق الابتدائي في جريمة انتحال الشخصية الإلكترونية، وفي مرحلة التحقيق يأتي دور النيابة العامة في التحقيق والاستجواب، والقبض والضبط والتفتيش، وهي المرحلة الأهم ومنها نبدأ في تحريك الدعوى الجزائية ضد المتهم في جريمة انتحال الشخصية الإلكترونية.

ولقد تعددت التعريفات حول مفهوم التحقيق في الجرائم الالكترونية، حيث يعرف بأنه: " عمل قانوني يقوم به المختصون في ضبط الجرائم المعلوماتية من فاعل ودليل إلكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذا النوع من الجرائم لإقامة العدل[124]"

ويمكن القول إنه لا يوجد أي اختلاف بين التحقيق الجنائي في الجرائم الالكترونية عن غيرها من الجرائم الأخرى، فهو يحتاج إلى إجراءات تتشابه في عمومها، وتعد وسيلتي التفتيش الإلكتروني وضبط الأدلة من أهم الأساليب المتبعة في الكشف عن جريمة انتحال الشخصية الإلكترونية، وسيناقش الباحث ما يتعلق بهاتين الوسيلتين من خلال الفروع التالية.

الفرع الأول: التفتيش الإلكتروني في جريمة انتحال الشخصية الإلكترونية.

الفرع الثاني: ضبط الأدلة الناجمة عن التفتيش في جريمة انتحال الشخصية الإلكترونية.

---

[122] انظر: المادة (51) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[123] انظر: المادة (54) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[124] مصطفى موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، الطبعة الأولى، القاهرة، ص 166.

الفرع الأول: التفتيش الإلكتروني في جريمة انتحال الشخصية الإلكترونية.

عرف المشرع الفلسطيني التفتيش التقليدي بأنه: "إجراء من إجراءات التحقيق الابتدائي الذي لا يتم إلا بمذكرة من النيابة العامة أو في حضورها، بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة "

أما فيما يتعلق بالتفتيش الإلكتروني فيمكن تعريفه بأنه: "إجراء تحقيقي تقوم به الضابطة القضائية بموجب مذكرة قضائية، أو بدون مذكرة في احوال استثنائية؛ للبحث عن أدلة الجريمة الرقمية في جهاز كمبيوتر أو أي من أجهزة الاتصال الذكية[125]."

ويعد التفتيش أحد إجراءات التحقيق، الذي يهدف إلى البحث عن الأشياء المتعلقة بالجريمة، يقوم به موظف مختص طبقاً لإجراءات مقررة قانوناً في مكان يتمتع بمكانة خاصة من أجل الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثباتها أو نسبتها لفاعلها، وقد نظم القانون قواعد التفتيش ودخول المنازل والانتقال إلى مسرح الجريمة وإجراء الكشف والمعاينة، فقد نص القانون الاساسي الفلسطيني في المادة 2/11 منه على عدم جواز تفتيش الشخص أو حبسه او الاعتداء على حريته إلا بأمر قضائي وفق أحكام القانون، وكذلك نص قانون الاجراءات الجزائية الفلسطيني على اجراءات الكشف والمعاينة والانتقال الى مسرح الجريمة وأقر كذلك قواعد دخول وتفيش المساكن واقر لها حرمة خاصة بحيث لا يجوز دخولها او تفتيشها إلا بأمة من جهات الاختصاص [126].

وقد نصت المادة (32) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: "1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين

---

[125] أمير يوسف، الاثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، مكتبة الوفاء القانونية، الطبعة الاولى، الإسكندرية، 2016م، ص 290.

[126]– وقد جاء ذلك في المواد (21، 27، 39) من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م.

على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية."

يتضح من المادة السابقة أن القرار بقانون بشأن الجرائم الإلكترونية قد منح الصلاحية للنيابة العامة في تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة، شريطة أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة، وفي حال أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. كما يلاحظ أن المادة السابقة قد جاءت متوافقة مع ما ورد في قانون الإجراءات الجزائية الفلسطيني حول جواز انتداب النيابة العامة لأحد مأموري الضبط القضائي للقيام بعملية التفتيش، والجدير بالإشارة أنه في جرائم انتحال الشخصية الإلكترونية يجب على النيابة العامة عند انتدابها لمأمور ضبط قضائي للقيام بالتفتيش مراعاة أن يكون مأمور الضبط القضائي المناب ذو خبرة ودراية فنية في تفتيش نظم الحاسوب والانترنت؛ وذلك حتى يستطيع أن يتعامل عملياً وبصورة سليمة وصحيحة مع مخرجات الحاسوب والانترنت؛ وذلك من أجل الحفاظ على سلامة الأدلة المتحصلة والمتعلقة بجريمة انتحال الشخصية الإلكترونية[127]. وقد اعتبر القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية موظفو الوزارة المعينون من قبل الوزير من مأموري الضابطة القضائية المختصة بالتفتيش عن الجرائم الإلكترونية، حيث نص في المادة (54) على أنه : " تتولى الوزارة وفقاً لاختصاصها تقديم الدعم والمساندة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون " إلا أن

[127] مهدي رضوان، إجراءات الضبط والتفتيش في الجرائم الالكترونية في النظام الفلسطيني، رسالة ماجستير، كلية الدراسات العليا، جامعة بيرزيت، فلسطين، 2023م، ص78.

هذه المادة قد تم إلغائها لاحقاً بموجب القرار بقانون رقم (38) لسنة 2021م المعدل للقرار بقانون رقم (10) لسنة 2018م[128].

ونظراً للطبيعة الخاصة التي تتميز بها جريمة انتحال الشخصية الإلكترونية فإننا نجد أن التفتيش لا يتوقف على جهاز الحاسب الآلي وتفتيش وضبط المكونات المادية والمعنوية لهذا الجهاز، وإنما يمتد ليشمل مختلف أجزاء النظام الإلكتروني ليشمل المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، وأي أدوات دفع إلكترونية أو أي أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف[129]. ونجد في هذا الإطار أن القرار بقانون بشأن الجرائم الإلكترونية لسنة 2018م قد أجازت نصوصه أن يمتد التفتيش إلى البيانات والمعلومات الموجودة على حاسوب آلي في موقع أخر، فعند الرجوع إلى نص المادة (53/2) من القرار بقانون بشأن الجرائم الإلكترونية نرى أنه قد نص على أن "للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة[130]"

ومن خلال نص المادة (32) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، يتبين أنه يوجد العديد من القواعد القانونية الشكلية والموضوعية التي تستند عليها عملية التفتيش في الأنظمة الإلكترونية:

أولاً: القواعد الشكلية للتفتيش في جريمة انتحال الشخصية الإلكترونية:

قد حدد المشرع الفلسطيني مجموعة من الشروط الشكلية للتفتيش تستهدف إقامة سياج قانوني يحمي الحريات الفردية على أساس أن التفتيش بحث في مستودع أسرار الناس التي يحرصون على الاحتفاظ بها لأنفسهم، ومن هذه الشروط ما يلي:

أ. التفتيش في جريمة انتحال الشخصية الإلكترونية بناء على مذكرة:

---

[128] انظر: المادة (26) من القرار بقانون رقم (38) لسنة 2021م، بتعديل قرار بقانون رقم (10) لسمة 2018م بشأن الجرائم الإلكترونية وتعديلاته.

[129] زيد بني خالد، مرجع سابق، 51.

[130] انظر: المادة (53/2) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

اشترط المشرع الفلسطيني في قانون الاجراءات الجزائية رقم (3) لسنة 2001، إصدار النيابة العامة لمذكرة تفتيش قبل القيام بالتفتيش، حيث نصت المادة (39/1) على أنه: " دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها ... [131]" كما نص القرار بقانون بشأن الجرائم الإلكترونية على أنه: " للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة[132]"

يتبين من النصوص السابقة أن التفتيش يتطلب إذن يجيز تفتيش أنظمة الحاسوب، كون أن التفتيش دون إذن أو الحصول على بيانات من جهات ليست محلاً للاشتباه لتعلقها بالمشتبه به، فإنها مسألة تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد وتوجب مشروعية الدليل وسلامة مصدره[133].

ولم يحدد المشرع صيغة معينة لمذكرة التفتيش متى ثبت صدورها من النيابة العامة، كما لم يشترط عبارات خاصة تصاغ بها، وإنما اشترط أن تكون مكتوبة ومؤرخة وموقعاً عليها ممن أصدرها مشتملة بياناتها، وأن تكون صريحة في الدلالة على التفويض. ويجب ان يعين أمر التفويض بالتفتيش اسم ووظيفة وتوقيع من أصدره واسم وظيفة مأمور الضبط المصرح له بمباشرته، واسم صاحب المنزل المراد تفتيشه وشهرته، والتهمة المسندة إليه، والغرض من التفتيش وعنوان منزل المراد تفتيشه، والمدة التي تسري خلالها مذكرة التفتيش[134].

وقد اشترط المشرع الفلسطيني ضرورة تسبيب مذكرة التفتيش وفقاً لنص المادة (2/39) من قانون الإجراءات الجزائية، ويقصد بالتسبيب بيان العناصر التي استخلص منها عضو النيابة توافر الدلائل والقرائن الكافية المبررة للتفتيش، والتي أصدر أمره بناء عليها؛ حتى يتاح للمحكمة أن تراقب تقديره لجدية تلك الدلائل وكفايتها، وأنه استهدف الغاية التي حددها المشرع لمباشرة

---

[131] انظر: المادة (39/1) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[132] انظر: المادة (52/1) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[133] أحمد براك، الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية تأصيلية مقارنة، الطبعة الأولى، دار الشروق، رام الله، 2019م، ص 105.

[134] انظر: المادة (40) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001.

التفتيش، وتقدير بطلانه إذا ثبت أنه استهدف غاية غير ما حدد التشريع[135]. كما يجب أن يكون أمر التفتيش محدد، ويقصد هنا بتحديد أمر التفتيش في ظل جريمة انتحال الشخصية الإلكترونية، عندما يكون المحقق يعلم ابتداء عن وجود الأدلة المتصلة بتلك الجريمة ضمن أحد أنظمة الحاسب الألي أو الشبكات، فإن مذكرة التفتيش يتعين أن تكون واضحة في تحديد النظام محل التفتيش، أما إذا كان النظام أو مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش، فيتعين أن تجئ عبارات مذكرة التفتيش عامة ما أمكن حتى لا يكون نصها قيداً على نطاق التفتيش والضبط، والعمومية هنا لا تعني عدم وجوب بيان السبب ومبرر التفتيش ولا تعني تجاوز الاجراء بذاته للقواعد القانونية المقررة لحماية الأفراد[136].

ب. حضور بعض الأشخاص أثناء التفتيش:

يتضمن التفتيش تقييداً لقاعدة علانية التحقيق بالنسبة للخصوم، إذ يُقصر الحضور على المتهم والقائم بالتنفيذ وذوي الشأن، والعلة أن التفتيش إطلاع على أسرار الغير التي يحرم المشرع الاطلاع عليها لغير الضرورة، وهذه الضرورة يجب أن تقدر بقدرها، فلا يتم التوسع في إعطاء الخصوم الحق في الاطلاع، وبالتالي لا يسمح للمجني عليه أو المدعي بالحق المدني أو المسئول عنها بحضور التفتيش[137].

وضماناً لزيادة الثقة في نتائج التفتيش وسلامة الأدلة المتحصلة منه وإتاحة الفرص للمتهم لمواجهة الدليل المستمد منه، فقد أوجب المشرع إجراء التفتيش بحضور المتهم أو حائز المنزل، وإذا تعذر وجود أي منهما فإن التفتيش يجري بحضور شاهدين من أقاربه أو جيرانه[138] .

ويرى الباحث أنه ينبغي على المشرع أن يبين أوصاف الشهود الحاضرين للتفتيش، فهو لم يذكر إذا كان يتوجب ان يكونوا من القاطنين مع المتهم، وهل يشترط فيهم بلوغ سن معينة، وأن عموم النص كما هو عليه قد يفهمه القائم بالتفتيش أن استدعاء ولدين قاصرين لحضور التفتيش فيه تطبيق لنص المادة (43) من قانون الاجراءات الجزائية، إضافة إلى أن يجب ان يتم النص على

---

[135] محمود نجيب حسني، مرجع سابق، ص 662

[136] أحمد براك، مرجع سابق، ص 388.

[137] عبد القادر جرادة، مرجع سابق، ص 493.

[138] انظر: المادة (43) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

كيفية إجراء التفتيش الحاصل في مسكن غير المتهم وهو أمر لم يتطرق له قانون الاجراءات الجزائية الفلسطيني كما فعل المشرع المصري.

ت. تحرير محضر التفتيش:

أوجب المشرع الفلسطيني على القائم بالتفتيش تحرير محضر يذكر فيه الأشياء التي تم ضبطها، ويذكر كذلك حالة عدم عثوره على شيء من هذا القبيل، ولم يتطلب المشرع شكلاً معيناً للمحضر المهم في ذلك محتوياته، والتي تشمل إجراءاته ووقته[139].

وإذا كان القائم بالتفتيش عضو النيابة، فإنه يلزم بتحرير محضر التفتيش، وأن يتم تدوينه بمعرفة كاتب التحقيق، أما إن كان التفتيش يجري بمعرفة مأمور الضبط القضائي، فلم يشترط القانون وجود الكاتب، ومؤدى ذلك أنه هو المسؤول وحده عن صحة ما يدون بالمحضر ما دام موقع منه إقراراً منه بصحته، فلا يهم بعد ذلك إن كان قد حرر بيده أو استعان في تحريره بغيره[140] .

وفي حالة وجود نقص في المحضر أو بطلانه أو عدم وجوده أصلاً، لا يترتب على ذلك بطلان التفتيش؛ إذ لكل منهما شروطه الخاصة، حيث يعتبر المحضر الصورة المكتوبة التي يتجسد فيها التفتيش ذاته، وبما أن التفتيش إجراء لا يمكن إعادته في التحقيق النهائي أثناء مرحلة المحاكمة بنفس الصورة التي تم بها في التحقيق الابتدائي، فإنه في هذه الحالة يكون للمحضر قيمته الفعلية على الرغم من أنها محدودة؛ وذلك لأنه إذا توفرت شروط صحة التفتيش، فهو صحيح ولا تأثير لبطلان المحضر عليه متى كان هذا البطلان بسبب شكلي يتعلق بتحريره فقط؛ لأنه في هذه الحالة يمكن إثبات التفتيش بوسائل أخرى مثل شهادة الشهود[141] .

ث. أن يتم التفتيش بأسلوب آلي الكتروني:

لا بد أن يتم التفتيش في جريمة انتحال الشخصية الإلكترونية بأسلوب آلي يتناسب مع طبيعة هذه الجريمة من قبل القائم بالتفتيش؛ وذلك لأن هذا التفتيش لا بد أن يتم بسرعة ودقة عند القيام به لسهولة التخلص من الدليل في مثل هذه الجريمة بالإتلاف أو الشطب أو التعديل أو المسح،

---

[139] انظر: المادة (4/50) من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[140] عبد القادر جرادة، مرجع سابق، ص 492.

[141] أمال عبد الله، مرجع سابق، ص 215.

فمن الأفضل أن يتم إبعاد المشتبه به في هذه الجريمة عن محل التفتيش ومنعه من استخدام الأجهزة الالكترونية خلال التفتيش كالمفكرة الالكترونية أو الهاتف النقال أو أي جهاز أخر يمكن الولوج من خلاله إلى نظام الحاسوب محل التفتيش؛ وذلك لأن المفتش في هذه الجريمة يتعامل مع محترف في اقتحام أنظمة الحاسوب وبرامجه مما يترتب على استخدامه هذه الأجهزة إمكانية الولوج إلى النظام الرئيسي للحاسوب محل التفتيش وزرع فيروس قادر على تدمير النظام بأكمله أو إتلاف الملفات الموجودة بالجهاز أو تشفيرها بحيث تتلف بشكل تلقائي.

ثانياً: القواعد الموضوعية للتفتيش في جريمة انتحال الشخصية الإلكترونية:

أحاط المشرع اجراء التفتيش بالعديد من الشروط الموضوعية والتي تتمثل فيما يلي:

أ. سبب التفتيش:

يقصد بسبب التفتيش أي ما يبرر اجراؤه، فوقوع العمل الاجرامي المعاقب عليه قانوناً هو الذي يفسح المجال للنيابة العامة لإقامة الدعوى الجنائية ضد المتهم، فلا يجوز مباشرة التفتيش إلا بعد وقوع الجريمة، ويشترط لصحته أن تكون الجريمة من نوع الجناية أو الجنحة أياً ما كانت جسامتها أو طبيعتها، وقد أخرج المشرع الفلسطيني الجرائم من نوع المخالفات من جواز التفتيش[142].

ولا يصح القيام بالتفتيش لضبط جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل. إلا أن وقوع الجريمة ذاتها لا يكفي لتنفيذ التفتيش وإنما يتعين إلى جوار ذلك اتهام شخص ما بارتكاب جريمة، وأن يكون الهدف من التفتيش ضبط أشياء تتعلق بالجريمة[143].

وفيما يتعلق بجريمة انتحال الشخصية الإلكترونية فإن سبب التفتيش فيها يجب أن يستند على ثلاثة شروط، ومنها وقوع الجريمة وفق الأفعال التي يحددها المشرع في هذا المجال، بالإضافة إلى اتهام أحد الأشخاص بارتكاب تلك الجريمة أو الاشتراك بها، ويكون ذلك بناء على أدلة كافية تشير بأن المتهم هو من قام بارتكاب الجريمة، وأما الشرط الثالث فهو ضرورة توافر أدلة أو

---

[142] انظر: المادة (39) من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[143] عبد القادر جرادة، مرجع سابق، ص 484.

قرائن جدية لدى سلطات التحقيق على وجود بيانات أو معلومات أو معدات بحوزة المتهم أو غيره تفيد في إظهار الحقيقة[144].

ب. محل التفتيش:

يقصد بمحل التفتيش عموماً بأنه المستودع الذي يحتفظ فيه الشخص بأشيائه المادية التي تتضمن أسراره، والسر الذي يوفر القانون له الحماية هو المكان الذي يتوافر به حرمة خاصة من الاعتداء عليها، كالمسكن والمكالمات والرسائل الشخصية والشخص نفسه، ومحل التفتيش في جريمة انتحال الشخصية الإلكترونية هو الجهاز الإلكتروني والشبكات المرتبطة به وما يرتبط بهما من ملحقات مادية وتقنية[145].

والمحل في جريمة انتحال الشخصية الالكترونية لا يكون قائماً بذاته بل مقترناً إما بمكان معين كمسكن المشتكى عليه أو بشخص معين بصفته مالك أو حائز مثلما هو الشأن في الحاسب المحمول أو الهاتف النقال، لذلك فإنه يتعين قبل مباشرة إجراء التفتيش مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الالكترونية المراد تفتيشها وكذا الضمانات القانونية المحاطة به، لأن حكم تفتيش هذه الوسائل يتوقف غالباً على طبيعة المكان الذي تتواجد فيه[146].

والتفتيش الواقع على الكيانات المادية لجهاز الحاسوب في الجرائم الإلكترونية يخضع لذات الإجراءات القانونية والقواعد العامة للتفتيش، أي أن حكم تفتيش المكونات المادية متوقف على طبيعة المكان الذي توجد فيه تلك الكيانات، فإذا كانت موجودة بحوزة أحد الأشخاص في مكان عام وسواء أكان عام بطبيعته كالطرق العامة والحدائق والمتنزهات أو كان المكان عام بالخصوص كمقاهي الانترنت ووسائل النقل العامة، فإنها تخضع للحالات التي يجوز فيها تفتيش الأشخاص، أما إذا كانت موجودة في مكان خاص كمنزل الجاني أو أحد ملحقاته فإنها تخضع للحالات التي يجوز فيها تفتيش المساكن مع ضرورة الانتباه فيما إذا كانت تلك الكيانات منفصلة

---

[144] سامي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2011م، ص 117-126.

[145] أشرف قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015م، ص149.

[146] أشرف قنديل، مرجع سابق، ص 150.

أو متصلة بجهاز حاسوب اخر موجود في مكان غير منزل المتهم، فإذا كانت متصلة فيتعين تفتيش تلك الكيانات الأخيرة ولكن ضمن الحالات التي يجوز فيها تفتيش تلك الأماكن[147].

وعلى الرغم من أن تفتيش المكونات المادية للحاسب الآلي تخضع لنفس قواعد التفتيش في الجرائم التقليدية إلا أن المشكلة تثور فيما يتعلق بتفتيش المكونات المعنويات للحاسب الآلي والتي يقصد بها: " مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات [148]" حيث ثار جدل فقهي واسع حول مدى جواز تفتيش تلك المكونات المعنوية لضبط الأدلة منها، وهل يمكن تطبيق قواعد التفتيش التقليدية عليها؟ وبغض النظر عن ذلك الخلاف الفقهي إلا أن المشرع الفلسطيني لم يمنع تفتيش المكونات المعنوية، ولكن على الرغم من جواز ذلك إلا أن الباحث يرى بأن القواعد الواردة في القرار بقانون بشأن الجرائم الإلكترونية وفي قانون الإجراءات الجزائية لا تصلح للتطبيق على تلك المكونات المعنوية لجهاز الحاسب الآلي؛ لذلك فإن الباحث يوصي المشرع الفلسطيني بضرورة وضع قانون خاص يتعلق بإجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية.

الفرع الثاني: ضبط الأدلة الناجمة عن التفتيش في جريمة انتحال الشخصية الإلكترونية.

يقصد بضبط الأدلة أي: " وضع اليد على شيء متعلق بجريمة انتحال الشخصية الإلكترونية ويفيد في الكشف عن كافة الحقائق عنها وعن مرتكبيها سواء كان هذا الشيء عقاراً أو منقولاً، وقد يرد الضبط على الأشخاص وهو ما يصطلح على تسميته بالقبض[149] "

والاصل أن التفتيش يهدف لضبط الأدلة التي تفيد في كشف الحقيقة في الواقعة التي يتم التحقيق بشأنها، ومع ذلك يرد عليه استثنائيين: الأول: يتمثل في إجازة ضبط الأشياء التي تظهر عرضاً أثناء التفتيش إذا كانت حيازتها تعد في ذاتها جريمة أو تفيد في كشف الحقيقة في جريمة

---

[147] علي الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004م، ص 82.

[148] كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي القانونية، دمشق، 2007م، ص 61.

[149] عبد الفتاح حجازي، الجوانب الإجرائية لأعمال التحقيق، دار النهضة العربية، القاهرة، الطبعة الأولى، ص 274.

أخرى[150]. والثاني: أنه لا يجوز أن يضبط لدى محامي المتهم الأوراق والمستندات التي سلمها له أيهما لأداء المهمة التي عهد بها له أو المراسلات المتبادلة بينهما في القضية إذا سلمت فعلاً للمحامي وتعلقت بأداء مهمته في الدفاع عن المتهم[151].

فالضبط هو إجراء يتبع التفتيش، فالهدف الذي تسعى إليه سلطة التحقيق من التفتيش هو ضبط الأدلة والوثائق والأشياء التي تفيد في كشف الجريمة وإماطة اللثام عن غموضها، وتحقيق العدالة، ولذلك يجب التقيد بالقواعد الإجرائية التي تحدد الأماكن التي يجوز تفتيشها أو الأشخاص الذين يجري تفتيشهم[152].

والأصل أن الضبط يرد على الأشياء المادية فقط، وبالتالي هناك صعوبة في ضبط الأدلة في جريمة انتحال الشخصية الإلكترونية؛ وتكمن الصعوبة هنا في ضبط الوسائل الفنية المستخدمة في تدمير الأدلة المتعلقة بتلك الجريمة وفي ضبط بيانات الحاسوب.

وقد عالج المشرع الفلسطيني موضوع ضبط الأدلة الإلكترونية في المادة (33) من القرار بقانون بشأن الجرائم الإلكترونية لعام 2018م والتي نصت على أنه: "1. للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعمليها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية. 2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة. 3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. 4. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات. 5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما

---

[150] انظر: المادة (1/50) من قانون الاجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[151] انظر: المادة (211) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

[152] عبد الله حسين محمود، إجراءات جمع الأدلة في مجال الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003م، ص 623.

في ذلك الوسائل الفنية لحماية محتواها. 6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.[153]"

ويلاحظ الباحث من خلال استقراء المادة السابقة، أنها لم تتناول على أي إجراءات أو قواعد خاصة تتعلق بحفظ المضبوطات في الجرائم الإلكترونية، رغم ضرورة وجود مثل هذه القواعد للحفاظ على المضبوطات الإلكترونية من الإتلاف أو التدمير، مما يوجب فرض إجراءات خاصة للحفاظ عليها وصيانتها من العبث والتلف، بحيث يجب على المحقق على سبيل المثال ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخ منها، كما يجب عدم ثني الأقراص الصلبة المخزن عليها البيانات؛ لأن ذلك يؤدي إلى تلفها وفقدان البيانات، وعدم تعريض الأقراص والأشرطة الممغنطة لدرجات حرارة عالية، وعدم كتابة بيانات على الأقراص الصلبة من الخارج لأن ذلك يفسدها، وغيرها من القواعد الأخرى التي يجب اتباعها لحفظ المضبوطات في جريمة انتحال الشخصية الإلكترونية .

وهناك العديد من الطرق للتحفظ على الأنظمة المعلوماتية، فيمكن التحفظ على هذه المعلومات عن طريق ابقائها داخل النظام أو الحاسوب نفسه وتتم عن طريق حجز الحاسوب الذي يتواجد الدليل الرقمي فيه، أما الطريقة الثانية فيتم التحفظ على البيانات والمعلومات خارج الحاسب الآلي وذلك عن طريق استخدام فلاش ميموري أو عن طريق استخدام أقراص صلبة خارجية[154]. وقد أجاز القرار بقانون عملية نسخ البيانات والمعلومات إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه[155].

وحيث أن الضبط يكون محله في مجال جريمة انتحال الشخصية الإلكترونية، البيانات المعالجة إلكترونياً، فقد ثار تساؤل حول مدى صلاحية هذا النوع من البيانات لأن يكون محلاً للضبط؟

---

[153] انظر: المادة (33) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[154] توفيق خشاشنة، مسرح الجريمة ومعاينته عبر شبكة المعلومات الدولية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2020م، عمان، ص343.

[155] انظر: المادة (53/3) من القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018م وتعديلاته.

حيث يوجد هناك اتجاهان فقهيان، فيرى الاتجاه الأول أن بيانات الكمبيوتر لا تصلح لأن تكون محلاً للضبط؛ لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادي، ويستند هذا الاتجاه إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملوسة. أما الاتجاه الثاني فيرى أن البيانات المعالجة إلكترونياً ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره[156]. وفي تقدير الباحث فإن الاتجاه الثاني هو الأدق باعتبار أن المشرع الفلسطيني نص على صلاحية ضبط الأدلة الإلكترونية بشكل صريح، إضافة إلى كون الأدلة الإلكترونية يمكن الاحتفاظ بها ويكون لها دلالة مادية في الإثبات لاسيما بعد أن يصار إلى تفريغ محتواها، وبالتالي جواز التعويل عليها في الإدانة وبشكل منفصل.

ويمكن حصر الأشياء التي يتم ضبطها في مجال الإثبات الإلكتروني بما يلي[157]:

أ. ضبط النظام الإلكتروني، وملحقاته من سجلات تم إنشاؤها عن طريق النظم الإلكترونية بشكل تلقائي وتتمثل في السجلات وفي المخرجات الإلكترونية التي لم يكن لأي شخص أي يد في إنشائها وإعدادها مثل الهواتف النقالة، البطاقات البنكية، والفواتير.

ب. ضبط المعدات والأجهزة المستعملة في الشبكة الإلكترونية، وأهمها المودم وهي الوسيلة التي تمكن الأجهزة الإلكترونية من الاتصال ببعضها البعض عبر خطوط الهاتف النقال.

ت. ضبط وسائط التخزين المتحركة كالأقراص المدمجة، والأقراص المرنة، والأشرطة المغناطيسية وغيرها.

ث. ضبط البرمجيات الإلكترونية، فإذا كان الدليل الإلكتروني ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بتنصيب هذا البرنامج أمر مهم عند فحص الدليل الإلكتروني.

---

[156] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية،2009م، ص 225.

[157] عبد الفتاح حجازي، مرجع سابق، ص 201-206.

ج. ضبط البريد الإلكتروني والذي قد يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية.

ويحق لعضو التحقيق ضبط وتحريز دليل تم العثور عليه عن طريق الصدفة، أي أن مأمور الضبط القضائي مخول بضبط الدليل الذي يعثر عليه دون أن يكون هذا الدليل مستهدفاً للبحث خلال البحث والتفتيش، فمثلاً لو صدرت مذكرة تفتيش وبحث عن جريمة نشر فايروسات وأثناء التفتيش في حاسوب المتهم وجد بالصدفة أدلة تفيد أن صاحب هذا الجهاز قام بجريمة انتحال لشخصية ما، فإن ضبط مأمور الضبط القضائي لتلك الأدلة يعتبر صحيحاً رغم أن التهمة الموجهة له كانت نشر فايروسات وليس انتحال شخصية الكترونية[158].

والجدير بالذكر أن ضبط الأدلة في جريمة انتحال الشخصية الإلكترونية يواجه العديد من الصعوبات والمشاكل، أبرزها أن المنتحل يصل إلى مراده باستخدام شيفرات وأساليب احتيالية وبالتالي يرتكب جريمته بشكل مخفي ولا يترك دليل خلفه، وإذا قام الجاني الذي ينتمي لدولة معينة بانتحال شخصية المجني عليه الذي ينتمي لدولة أخرى فإن ذلك يشكل صعوبة قانونية بالغة تتمثل في عدم القدرة في الوصول إلى الجاني في تلك الدولة. كما أنه من الصعوبات التي تواجه عمليه ضبط الأدلة في جريمة انتحال الشخصية الإلكترونية أن إجراءات الضبط في هذه الجريمة تختلف عن الإجراءات المتبعة في الجرائم التقليدية، فإذا كان من السهل القيام بالمشاهدة والتتبع والمساعدة في الجرائم التقليدية فإن ذلك غير ممكن في جريمة انتحال الشخصية الإلكترونية؛ فالمنتحل في هذه الجريمة عادة ما يتخذ كلمات سر وشيفرات معينة تزيد من صعوبة ضبط الأدلة، إضافة إلى وجود صعوبة من حيث الحصول على الدليل الإلكتروني، عندما يكون الحاسب الآلي مرتبط بحواسيب أخرى خارج فلسطين[159].

وللتغلب على الصعوبات السابق ذكرها في عملية ضبط الأدلة في جريمة انتحال الشخصية الإلكترونية، يجب على المحقق أن يستعين بالخبراء والفنيين؛ كون أن الخبراء الفنيين هم القادرين على كشف غموض جريمة انتحال الشخصية الإلكترونية والتعامل مع الجوانب التقنية والتكنولوجية في كشف هذه الجريمة، وقد وفق المشرع الفلسطيني بقانون الجرائم الإلكترونية عند

---

[158] مصطفى عبد الباقي، مرجع سابق، ص 291.

[159] زيد بني خالد، مرجع سابق، ص 61.

نصه على الخبرة كطريق من طرق إثبات الجرائم الإلكترونية، حيث نصت المادة (4/32) على أنه : " لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات[160] "

والجدير بالإشارة أن المشرع الفلسطيني ومن أجل تسهيل عملية ضبط الأدلة في الجرائم الإلكترونية، فقد أجاز الاعتراض الفوري لمحتوي الاتصالات، حيث نصت المادة (36) من القرار بقانون بشأن الجرائم الإلكترونية لعام 2018م على أنه: "1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له، ومدته. 2. تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط. 3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.[161]"

يتضح من المادة السابقة أن أهم الشروط التي يجب أن تتوفر في اعتراض محتوى المكالمات وتسجيلها، هي ضرورة صدور أمر بالمراقبة من السلطة المختصة، وقد قرر القضاء الفلسطيني أن أي تجيل يتم بواسطة أي جهاز لا يجوز الاعتماد عليه إلا إذا كان بناء على إذن من قاضي الصلح، وقد حكمت محكمة النقض ببطلان الدليل وعدم مشروعيته[162].

المبحث الثاني: إجراءات المحاكمة والاثبات في جريمة انتحال الشخصية الالكترونية والعقوبة المقررة لها.

بعد أن تنتهي النيابة العامة من الإجراءات المقررة قانوناً تجاه المشتكى عليه، وبعد تحرير الضبوط وتكييفه للفعل على أنه جريمة تستلزم المحاكمة، تنتقل الدعوى إلى المرحلة التالية

---

[160] انظر: المادة (32/4) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[161] انظر: المادة (36) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[162] حكم محكمة النقض الفلسطينية رقم 607 لسنة 2019م، منشور عبر المقتفي.

بتحويل المشتكى عليه إلى المحكمة، وهنا تبدأ المحاكمة التي تخضع أيضاً لقواعد أصولية خاصة نص عليها قانون الإجراءات الجزائية الفلسطيني. وبالتالي إذا كان ما تمخضت عنه الشكوى التي قدمها المشتكي عن صدقية في ادعاءاته من كونه تعرض لانتحال يمس اسمه أو مركزه أو شخصيته من خلال أي وسيلة إلكترونية، وقامت السلطات بجمع الأدلة، والتأكد من الشكوى وتحويلها للنيابة العامة، وعند عرض الشكوى والاستدلالات على وكيل النيابة العامة؛ فإذا تيقن بأن هناك فعلاً يشكل جريمة بحسب نصوص القانون، يقوم حينها بإحالة ملف الدعوى إلى المحكمة المختصة.

والحديث عن مرحلة المحاكمة يرتبط بشكل كبير بالحديث عن نظرية الإثبات، على اعتبار أن القاضي في مرحلة المحاكمة يبني حكمه بالدعوى المنظورة من قبل بناء على ما تتمخض عنه المراحل السابقة من أدلة وإثباتات وبراهين.

في هذا المبحث سيتطرق الباحث إلى إجراءات المحاكمة والاثبات في جريمة انتحال الشخصية الالكترونية والعقوبة المقررة لها، وذلك من خلال المطالب التالية:

المطلب الأول: إجراءات المحاكمة في جريمة انتحال الشخصية الإلكترونية وعقوبتها المقررة.

المطلب الثاني: إجراءات الاثبات في جريمة انتحال الشخصية الإلكترونية.

المطلب الأول: إجراءات المحاكمة في جريمة انتحال الشخصية الإلكترونية وعقوبتها المقررة.

تختص السلطة القضائية بصلاحية الفصل في المنازعات التي تنشأ بين الأفراد، وقد منح القانون هذه السلطة الاستقلالية التامة[163]، فهي تصدر أحكامها في الوقائع التي تنظر فيها دون تدخل من أي سلطة أخرى، وأكد على ذلك نص المادة (1) من قانون السلطة القضائية رقم 1 لسنة 2002م، حيث نصت على أنه: "السلطة القضائية مستقلة ويحظر التدخل في القضاء أو في شؤون العدالة[164] "

ولا تختلف إجراءات المحاكمة في جريمة انتحال الشخصية الإلكترونية عن إجراءات المحاكمة في الجرائم التقليدية، إلا أنه يستحسن أن تخصص هيئة قضائية متخصصة في المحاكم

[163] نصت المادة رقم (98) من القانون الأساسي الفلسطيني المعدل لسنة 2003م على أنه : " القضاة مستقلون، لا سلطان عليهم في قضائهم لغير القانون، ولا يجوز لأية سلطة التدخل في القضاء أو في شؤون العدالة "

[164] انظر: المادة (1) من قانون السلطة القضائية رقم 1 لسنة 2002م.

الفلسطينية لمحاكمة المتهمين بالجرائم الإلكترونية؛ كون أنه من الضروري أن يكون القاضي مدرباً على فهم أساليب التقنيات الحديثة حتى يتمكن من أداء رسالته في محاكمة المجرمين بارتكاب هذا النوع المتخصص من الجرائم.

الفرع الأول: الاختصاص القضائي لجريمة انتحال الشخصية الإلكترونية

من المعروف أن قواعد القانون الجنائي تخضع في تطبيقها من حيث المكان لمبدأ معروف وهو مبدأ الإقليمية، الذي يعني خضوع الجرائم التي تقع في إقليم دولة معيمة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي.

والأصل أن عناصر الركن المادي للجريمة تكتمل في مكان واحد، أو بالأحرى في نطاق إقليم دولة واحدة، حيث يقع السلوك الإجرامي وتترتب عليه أثاره الضارة في إقليم دولة واحدة، ومن ثم تعتبر الجريمة مرتكبة في هذا المكان، وعلى ضوء ذلك يتحدد القانون الواجب التطبيق، وبالتبعية المحكمة المختصة بنظر الدعوى[165].

وقد بينا سابقاً أن من خصائص جريمة انتحال الشخصية الإلكترونية أنها متعدية الحدود، بمعنى أنها غالباً ما يتجاوز مداها حدود الدولة، بحيث يتوزع ركنها المادي على أكثر من مكان، فيمكن وقوع سلوك الانتحال في مكان، وليكن إقليم دولة (س)، في حين تتحقق نتيجة الانتحال في نطاق إقليم دولة (ص)، وهذا يقودنا إلى التساؤل عن مكان وقوع الجريمة في هذه الحالة، هل هو مكان وقوع السلوك الإجرامي أم المكان الذي تحققت فيه النتيجة الإجرامية؟

لقد حاول الفقه الإجابة على السؤال السابق منذ وقت مبكر، من أجل حل مشكلة تنازع القوانين من حيث المكان بصدد هذه الفروض المثارة، وانقسم الرأي إلى ثلاث اتجاهات، فذهب الاتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه السلوك بغض النظر عن المكان الذي تحققت فيه النتيجة، أو من المفترض تحققها فيه. وفي المقابل ذهب اتجاه أخر إلى أن مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة أو كان من المفترض تحققها

---

[165] محمد الخوالدة، جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني: دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، الجامعة الأردنية، الأردن،2012م، ص 114

فيه، وبين الاتجاهين ظهر اتجاه ثالث يرى بأن العبرة في ذلك تكون بمكان حصول أي منهما (السلوك أو النتيجة)[166].

وبعيداً عن اختلافات الفقهاء حول مسألة الاختصاص في الجرائم الإلكترونية عبر الحدود، فقد حسم المشرع الفلسطيني الاختصاص القضائي وما يمكن أن يثيره من إشكاليات، عندما نص على ذلك في القرار بقانون بشأن الجرائم الإلكترونية لعام 2018، حيث جاء فيه: "1. تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرضاً أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين، مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ. 2. يجوز ملاحقة كل من يرتكب خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات الآتية: أ. إذا ارتكبت من مواطن فلسطيني. ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية. ج. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية.[167]"

يتضح من المادة السابقة أن أي شخص يرتكب جريمة انتحال الشخصية الإلكترونية خارج فلسطين كنوع من التحايل على القانون أو للإفلات من العقاب، فإن هذه المادة تحول دون ذلك؛ كون أنها منعت اللجوء من قبل المنتحل إلى اختصاصات قضائية أخرى لارتكاب تلك الجريمة.

ويرى الباحث أنه نظراً لكون جريمة انتحال الشخصية الإلكترونية من الجرائم الحديثة، والقوانين التي تتداخل في الجرائم الإلكترونية بشكل عام عديدة؛ نظراً لوقوع أثارها في غالب الأحيان في أكثر من دولة وتتنازع القوانين الخاصة بنظر الدعوى على ذلك الاختصاص، مما يثير مسألة تنازع الاختصاص القضائي في حال تصدت لها المحاكم الفلسطينية، وهنا نتمنى على المشرع الفلسطيني أن يضع معياراً أوضح للاختصاص سواء من حيث مكان وقوع الفعل أو مكان

---

[166] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، مصر، الطبعة الأولى، ص 43.

[167] انظر: المادة (2) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

الاستضافة أو مكان الاطلاع على نتائج هذا الفعل أو مكان ترتب أثاره، وقد تجتمع كلها في أحد هذه الجرائم في معظم دول العالم ويكون أثر هذه الجريمة في فلسطين هو أثر ثانوي جداً لا يبرر جعل الاختصاص للمحاكم الفلسطينية، فيستغل الأخرون هذا النص ويباشروا قضية جزائية في فلسطين بين أطراف غير فلسطينيين بحجة أن أثرها قد تحقق في فلسطين، وتتنازع الدول في هذا الموضوع وتحاول كل دولة ونظراً لوجود عنصر أجنبي في هذه المعادلة أن تجعل الاختصاص لها.

الفرع الثاني: العقوبة المقررة لجريمة انتحال الشخصية الإلكترونية

من خلال استقراء نصوص القرار بقانون بشأن الجرائم الإلكترونية نجد أن المشرع الفلسطيني قد نص على عقوبتي الحبس والغرامة لمنتحل الشخصية الإلكترونية بموجب المادتين (4، 14) من القرار بقانون بشأن الجرائم الإلكترونية لعام 2018م، حيث أنه في المادة الرابعة نص على أنه: "إذا ترتب على الدخول .... أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.[168]" أما في المادة (14) فقد نص على أنه: " كل من استولى عن طريق الشبكة الإلكترونية ... وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين[169]"

يلاحظ من المواد السابقة أن المشرع الفلسطيني قد وحد عقوبة الحبس والغرامة بين صورتي انتحال الشخصية الالكترونية، فيعاقب المنتحل بعقوبة الحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار ولا تزيد عن ثلاثة ألاف دينار، أو بكلتا العقوبتين، سواء قام بجريمة انتحال الشخصية الإلكترونية المرتبطة بجريمة الدخول غير المشروع أو قام بانتحال الشخصية الإلكترونية المرتبطة بالاستيلاء على أموال أو تواقيع الغير. وعليه فإن محكمة الصلح هي من

[168] انظر: المادة (4/3) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية..
[169] انظر: المادة (14) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

تختص في نظر جريمة انتحال الشخصية الإلكترونية، حيث أن عقوبة جريمة الانتحال هي من قبيل الجنح.

وقد شدد المشرع الفلسطيني من عقوبة انتحال الشخصية الإلكترونية المرتبطة بالدخول غير المشروع في حال كان الانتحال بهدف الدخول إلى البيانات الحكومية، فغلظ من العقوبة لتصل إلى الحبس مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة ألاف دينار أردني، ولا تزيد على خمسة ألاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً[170].

أما من حيث عقوبة الشروع فقد نص القرار بقانون بشأن الجرائم الإلكترونية لعام 2018م في المادة (27) منه، على عقوبة الشروع في الجرائم المنصوص عليها في ذات القرار بقانون، على أن يعاقب من شرع بالقيام بجريمة انتحال الشخصية الإلكترونية بنصف العقوبة المقررة لها[171].

كما جرم المشرع الفلسطيني إخفاء الأدلة الجنائية المتعلقة بجريمة انتحال الشخصية الإلكترونية، بحيث يعاقب كل من أقدم على العبث بأدلة قضائية معلوماتية أو قام بإتلافها أو إخفائها أو التعديل فيها أو محوها بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار ولا تزيد على ثلاثة ألاف دينار أو ما يعادلها بالعملة المتداولة قانوناً[172].

وقد ساوى المشرع الفلسطيني بين عقوبة مرتكب جريمة انتحال الشخصية الإلكترونية الأصلي، وبين عقوبة من يشترك معه في تلك الجريمة، حيث نصت المادة (48) من القرار بقانون بشأن الجرائم الالكترونية لعام 2018م على أنه: "يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة أو التدخل في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب بنصف العقوبة[173]"

---

[170] انظر: المادة (4/4) من القرار القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[171] نصت المادة (27) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه : " يعد مرتكباً جريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها "

[172] انظر: المادة (47) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

[173] انظر: المادة (48) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

وقد نص القرار بقانون بشأن الجرائم الإلكترونية لعام 2018م على مجموعة من الظروف المشددة للعقاب في حال وجدت أثناء ارتكاب جريمة انتحال الشخصية الإلكترونية ومن هذه الظروف التي تشدد من العقوبة ما يلي:

أ. إذا وقعت جريمة انتحال الشخصية الإلكترونية على موقع أو نظام تكنولوجي أو بيانات معلوماتية تكنولوجيا إلكترونية لها صلة بالدولة أو بأحد مؤسساتها[174].

ب. إذا وقعت جريمة انتحال الشخصية الإلكترونية من خلال عصابة منظمة[175].

ت. إذا وقعت الجريمة على طفل لم يتم (18) عام من عمره[176].

ث. إذا قام أحد الموظفين أو مزودين الخدمة بارتكاب جريمة انتحال الشخصية الإلكترونية[177].

ج. في حال قام المنتحل بتكرار الجريمة مرة أخرى[178].

---

[174] تنص المادة (52/1) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: " تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية: 1. إذا وقعت الجريمة على موقع أو نظام معلوماتي أو بيانات أو أرقام أو حروف أو شفرات أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها، بما في ذلك الهيئات المحلية. "

[175] تنص المادة (52/2) القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: " تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية: ،،،، 2. ارتكاب الجاني الجريمة من خلال عصابة منظمة "

[176] تنص المادة (52/3) القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: " تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية: 3. التغرير أو استغلال من لم يكمل الثامنة عشر سنة ميلادية."

[177] تنص المادة (27) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: " كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون، مستغلاً صلاحياته وسلطاته أثناء تأدية عمله، أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلث. 2. كل من ارتكب، من موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون، أثناء تأدية عمله أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلثين. "

[178] تنص المادة (51) القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه : " تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أياً من الجرائم المنصوص عليها فيه، سواء ارتكبت في فلسطين أو خارجها، وتعتبر الأحكام الأجنبية سابقة في التكرار بحق الجاني. "

والملاحظ أن القرار بقانون بشأن الجرائم الإلكترونية لم ينص على أي عقوبات تكميلية واكتفى فقط بفرض عقوبات أصلية على مرتكب جريمة انتحال الشخصية الإلكترونية مثل الحبس والغرامة، ويرى الباحث أن هذا غير كاف لمكافحة تلك الجريمة الخطيرة، والأحرى على المشرع الفلسطيني أن ينص في القرار بقانون بشأن الجرائم الإلكترونية على بعض العقوبات التكميلية التي تساهم في مكافحة تلك الجريمة مثل عقوبة مصادرة الموقع الالكتروني لمنتحل الشخصية الالكترونية أو إتلافه.

المطلب الثاني: إجراءات الاثبات في جريمة انتحال الشخصية الإلكترونية.

يعد الإثبات بالدليل الإلكتروني أحد مظاهر التطور في مكافحة الجريمة، وملائمة للتطور التكنولوجي والتقني في العصر الحاضر، وتكمن أهمية الدليل الإلكتروني في إثبات الدعوى الجزائية، خصوصاً في مرحلة المحاكمة، والإثبات بصفة عامة هو تأكيد وجود أو صحة أمر معين بأي دليل أو برهان، ويعد الاثبات الجزائي من أهم الموضوعات الإجرائية الجزائية، كون أن جميع الإجراءات هدفها بالأساس هو كيفية إثبات الحقيقة التي وقعت، إذ بموجب الاثبات الجزائي تتحقق براءة المشتبه به في ارتكاب جريمة انتحال الشخصية الإلكترونية أو معاقبته.

في هذا المطلب سيتطرق الباحث إلى إجراءات الاثبات في جريمة انتحال الشخصية الإلكترونية، وذلك من خلال الفروع التالية:

الفرع الأول: حجية الدليل الرقمي في إثبات جريمة انتحال الشخصية الإلكترونية

تستند إدانة المتهم في جريمة انتحال الشخصية الإلكترونية إلى أدلة تم الحصول عليها من مصادر مشروعة ووفقاً لقواعد النزاهة واحترام الضوابط والإجراءات المنصوص عليها في القانون، أما إذا تم الحصول على هذا الدليل من الوسائل الإلكترونية بوسائل وطرق غير مشروعة أصبح الدليل باطلاً، ويحق للمحكمة المختصة القضاء ببطلانه من تلقاء نفسها، إذا تعلق البطلان بالنظام العام كما أن الدليل الباطل بطلاناً مطلقاً لا يصلح للمحكمة أن تبني عليه قرار الإدانة بحق المتهم[179].

[179] خالد الجسمي، الإثبات الجنائي بالأدلة الرقمية، مجلة القانون المغربي، دار السلام للطباعة والنشر، المغرب، العدد34، 2017م، ص 33.

وبناء على ما سبق فإن للقاضي، وحسب قناعته الوجدانية، اعتماد أي وسيلة طرحت أمامه واقتنع بها في حكمه، طالما كانت طريقة الحصول عليها مشروعة، وحتى نكون أمام دليل إلكتروني مقبول ومعتمد أمام القضاء، فلا بد توافر مجموعة من الشروط في الدليل الالكتروني وهي:

أولاً: مشروعية الدليل الإلكتروني:

يقصد بمشروعية الأدلة الإلكترونية ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر، فقاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب مراعاة إعلانات حقوق الإنسان والمواثيق الدولية، وكذلك قواعد النظام العام وحسن الآداب السائدة في المجتمع، والمبادئ التي استقرت عليها محكمة النقض[180].

إن إجراءات الحصول على الأدلة الجنائية المتعلقة بجريمة انتحال الشخصية الإلكترونية يجب أن تندرج تحت الإطار العام الذي نص عليه القانون الأساسي الفلسطيني وقانون الإجراءات الجزائية الفلسطينية، ويقع باطلاً كل دليل مستمد بطريقة غير مشروعة ويكون بذلك مخالف للنظام العام.

ومن الأمثلة على الطرق غير المشروعة التي يمكن استخدامها في الحصول على الأدلة الجنائية استخدام التعذيب أو الإكراه المادي والمعنوي، والاستجواب المنهك للمتهم، والتجسس المعلوماتي، والاستخدام غير المصرح به للحاسب، والتنصت، واستخدام العش، والتزوير المعلوماتي[181].

ثانياً: مناقشة الأدلة الإلكترونية:

الأصل الذي يحكم إجراءات المحاكمة هو حضورية وشفوية جميع إجراءات التحقيق النهائي الذي تُجريه المحكمة، وتشمل كافة الطلبات والدفوع والمرافعات ومناقشة الأدلة في حضور كافة

[180] أحمد هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2008م، ص 118.

[181] أحمد هلالي، مرجع سابق، ص 122.

الخصوم، وعلى ذلك دلت أحكام قانون الإجراءات الجزائية من أطراف الدعوى وتلاوة التهمة على المتهم، وسؤاله ومناقشته، وإفهام المحكوم عليه وتلاوة الحكم وعلانية الجلسات[182].

وتكون الأدلة الإلكترونية على اختلاف أشكالها محلاً للمناقشة أثناء جلسات المحاكمة، ولا يتم ذلك من خلال أعمال التحقيق الابتدائي، بل في مجلس القضاء مباشرة، لأن حيدة القاضي الجنائي توجب عليه ألا يقيم قضائه أو يقرر حكمه إلا على ما كان في مجلسه، ولا يكون ذلك حكراً على الأدلة الإلكترونية التي تأخذ شكل المعلومات الرقمية أو غيرها من الأدلة المتولدة على الحاسب الآلي، بل يشمل كافة الأدلة المرتبطة بجريمة انتحال الشخصية الإلكترونية كالشهود ومحاضر الضبط القضائي[183].

ثالثاً: يقينية الأدلة الإلكترونية:

وهذا يوجب على القاضي الجنائي تحري الحقيقة، واستثناء الأدلة التي تحوطها الشكوك والظنون، أو التي يقدح في صحتها الإثبات العلمي، وعلى كل الأحوال ففي حال توفرت الشروط السابقة في الدليل الالكتروني؛ فإنه يتمتع من حيث قوته الإثباتية بقيمة قد تصل إلى درجة اليقين في إثبات جريمة انتحال الشخصية الإلكترونية، شانه في هذا شأن الادلة العلمية مثل البصمات، ويكون الدليل الالكتروني بينة قانونية مقبولة يجوز لمحكمة الموضوع الاستناد إليها في إدانة مرتكب تلك الجريمة.

الفرع الثاني: مدى قناعة القاضي الجزائي بالدليل الإلكتروني لإثبات جريمة الاحتيال الالكتروني.

لقد انتهج المشرع الفلسطيني في مجال الإثبات الجنائي مبدأ الإثبات الحر، فقد نص قانون الإجراءات الجزائية الفلسطيني على جواز الإثبات في الدعاوى بجميع طرق الإثبات القانونية وان

---

[182] أحمد شهاب، ونور بن مارني، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة الندوة للدراسات القانونية، العدد23، 2019م، ص12.

[183] أحمد شهاب، ونور بن مارني، مرجع سابق، ص 13.

الحكم الجزائي يخضع لمبدأ الاقتناع الذاتي للقاضي[184]. وهذا ما أكدته أحكام محكمة النقض الفلسطينية[185] .

وقد اقر المشرع الفلسطيني بعض الوسائل الحديثة في الإثبات والتي تدخل في إطار الدليل الالكتروني حيث نص في قانون 1البينات رقم 4 لسنة 2001م في المادة (19) من على أنه "1- تكون للرسائل الموقع عليها قيمة السند العرفي من حيث الإثبات ما لم يثبت موقعها أنه لم يرسلها، ولم يكلف أحداً بإرسالها. 2- تكون للبرقيات ومكاتبات التلكس والفاكس والبريد الإلكتروني هذه القوة أيضاً إذا كان أصلها المودع في مكتب التصدير موقعاً عليها من مرسلها، وتعتبر البرقيات مطابقة لأصلها حتى يقوم الدليل على عكس ذلك."

وقد نص قانون الإجراءات الجزائية على أن تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات إلا إذا نص القانون على طريقة معينة للإثبات. وهذا يعني أن الإثبات بالوثائق الإلكترونية جائز في الدعاوى الجزائية طالما لم ينص القانون على طريقة معينة للإثبات، وطالما اقتنع القاضي

---

[184] نص قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م في المادة (206) منه على انه "1- تقام البينة في الدعاوى الجزائية بجميع طرق الاثبات إلا إذا نص القانون على طريقة معينة للإثبات.2- إذا لم تقم البينة على المتهم قضت المحكمة ببراءته. " وكذلك نص في المادة (208) على انه " للمحكمة بناءً على طلب الخصوم، أو من تلقاء نفسها أثناء سير الدعوى أن تأمر بتقديم أي دليل تراه لازماً لظهور الحقيقة، ولها أن تسمع شهادة من يحضر من تلقاء نفسه لإبداء معلوماته في الدعوى." وفي تأكيد لهذا النهج ما ذهب اليه حكم لمحكمة النقض الفلسطينية المنعقدة في عزة في الدعوى الجزائية رقم (205) لسنة 2003م " من المقرر قانونا في المواد الجزائية جواز اثباتها بكافة طرق الاثبات ما لم ينص القانون على خلاف ذلك ... وإن من ضمن هذه الطرق حسبما نصت عليه المواد (108،106، 109) من قانون البيانات رقم 4 لسنة 2001م القرائن القضائية ، كما ان ما استقر عليه قضاء هذه المحكمة ان البينة الظرفية كافية لإثبات التهمة قبل فاعلها " ، وكلك نصت الفقرة الاولى من المادة (273) على انه " 1- تحكم المحكمة في الدعوى حسب قناعتها التي تكونت لديها بكامل حريتها ولا يجوز لها أن تبني حكمها على أي دليل لم يطرح أمامها في الجلسة أو تم التوصل إليه بطريق غير مشروع."

[185]وفي تأكيد لهذا النهج ما ذهب اليه حكم لمحكمة النقض الفلسطينية المنعقدة في عزة في الدعوى الجزائية رقم (205) لسنة 2003م " من المقرر قانونا في المواد الجزائية جواز اثباتها بكافة طرق الاثبات ما لم ينص القانون على خلاف ذلك ... وإن من ضمن هذه الطرق حسبما نصت عليه المواد (108،106، 109) من قانون البيانات رقم 4 لسنة 2001م القرائن القضائية، كما ان ما استقر عليه قضاء هذه المحكمة ان البينة الظرفية كافية لإثبات التهمة قبل فاعلها "

بالدليل. وعلى الرغم من ذلك، فإن معظم القضاة وأعضاء النيابة العامة يجهلون المعلومات الأساسية الضرورية المتعلقة بالجرائم الإلكترونية وكيفية التحقيق بها وإثباتها وينقصهم التدريب الكافي، وبالتالي يترددون في الأخذ في الأدلة الرقمية لإثبات الجرائم الإلكترونية.

وقد نصت المادة (37) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية على أنه: "يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات. "

وقد نص قانون المعاملات الإلكترونية الفلسطيني صراحة على أن يكون للمعاملات والتوقيعات الإلكترونية أثرها القانوني وتعتبر صحيحة وقابلة للتنفيذ شأنها في ذلك شأن الوثائق والمستندات الخطية بموجب أحكام التشريعات النافذة من حيث إلزامها لأطرافها أو صلاحيتها في الإثبات. كما نص على اعتبار الصورة المنسوخة على الورق من رسالة البيانات الإلكترونية الرسمية حجة على الكافة بالقدر الذي تكون فيه مطابقة لأصل هذه الرسالة. ويلاحظ على هذه النصوص أنها ركزت على العقود والتوقيعات الإلكترونية. ويحق لنا التساؤل حول البيانات الإلكترونية الأخرى من قبيل ملفات السجل وبيانات التعريف وغيرها ما إذا كانت مشمولة بذلك أم لا؟

ومن المعلوم أن وكيل النيابة هو من يتولى تقديم الدليل الالكتروني أمام المحكمة، وعليه تبيان الألية والكيفية التي تم التوصل بها إلى ذلك الدليل، وكيف تم استخراجه. كما يجب على وكيل النيابة تقديم الدليل الى المحكمة بصورة مفهومة نظرياً، وكذلك عليه أن يوضح وبمساعدة الخبير علاقة الدليل الإلكتروني المنوي تقديمه بجريمة انتحال الشخصية الإلكترونية المرتكبة، وكذلك توضيح الامور التقنية والجوانب العلمية التي استند إليها الخبير[186].

وتجدر الاشارة إلى أن تقديم الدليل الالكتروني لإثبات جريمة انتحال الشخصية الإلكترونية يعطي للمحكمة الصلاحية المطلقة في تقدير هذا الدليل، ويدخل ذلك ضمن الصلاحية التقديرية لقاضي الموضوع، مع التأكيد انه لا يسوغ للقاضي استبعاد الدليل الالكتروني إلا بواسطة دليل فني او الكتروني أخر يولد قناعة لدى القاضي بعدم صحة الدليل الالكتروني المقدم لإثبات جريمة انتحال الشخصية الإلكترونية.

[186] مصطفى عبد الباقي، مرجع سابق، ص 55.

الخاتمة

في ختام هذه الدراسة يستعرض الباحث مجموعة من النتائج والتوصيات:

أولاً: النتائج:

1- تكمن جريمة انتحال الشخصية الإلكترونية في ادعاء شخص ما بأنه شخص آخر وذلك من خلال ظهوره أمام الأخرين بشخصية منتحلة، وتكون الغاية من انتحال الشخصية غالباً تحقيق غايات ومكاسب شخصية أو بقصد الإضرار بمن انتحلت شخصيته أو لخلل في شخصية المنتحل ورغبة في إشباع الشعور بالنقص.
2- تعد جريمة انتحال الشخصية الالكترونية من الجرائم الخفية؛ كون أن المجني عليه لا يستطيع ملاحظتها ولا يعلم غالبا حتى بوقوعها والامعان في حجم السلوك المكون لها، فالمنتحل يستطيع إخفاء انتحاله بحكم توافر المعرفة والخبرة في مجال الحاسوب غالباً لدى مرتكب هذه الجريمة.
3- نص المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، على تجريم انتحال الشخصية الإلكترونية، حيث جرم الدخول إلى الموقع لانتحال صفته أو انتحال شخصية مالكه، وعاقب على ذلك بالحبس والغرامة معاً، كما جرم كل من استخدم برنامجاً أو نظاماً معلوماتياً لانتحال صفة الموقع أو شخصية المالك.
4- السلوك المادي في جريمة انتحال الشخصية الإلكترونية يأخذ الصورة الإيجابية فقط أي القيام بفعل ما، أما الصورة السلبية (الامتناع عن القيام بفعل) فهي غير متصورة في هذه الجريمة التي تستلزم قيام المنتحل باستخدام قدراته العقلية واستخدام الحاسب الآلي للقيام بعملية الانتحال.
5- لا تقوم جريمة انتحال الشخصية الإلكترونية عن طريق الخطأ، ويجب أن يتوفر لدى المنتحل القصد الجرمي.
6- لا تخلف جريمة انتحال الشخصية الالكترونية في الغالب آثاراً مادية يمكن فحصها أو معاينتها، خلافاً للجرائم التقليدية التي غالباً ما تخلف وراءها أثاراً مادية ملموسة، كالشعر والدماء وبصمات الأصابع وغيرها، أما جريمة انتحال الشخصية الإلكترونية، فهي

جريمة مستترة لا تخلف وراءها في الغالب أية آثار مادية، وكل ما يمكن أن تخلفه هو عبارة عن بيانات الكترونية، يصعب جداً إجراء أية معاينة عليها أو ضبطها.

7- يجب على المحقق للكشف عن ملابسات جريمة انتحال الشخصية الإلكترونية أن يستعين بالخبراء والفنيين؛ كون أنهم هم القادرين على كشف غموض تلك الجريمة والتعامل مع الجوانب التقنية والتكنولوجية في كشفها، وقد وفق المشرع الفلسطيني بقانون الجرائم الإلكترونية عند نصه على الخبرة كطريق من طرق إثبات الجرائم الإلكترونية.

8- وحد المشرع الفلسطيني عقوبة الحبس والغرامة بين صورتي انتحال الشخصية الالكترونية، فيعاقب المنتحل بعقوبة الحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار ولا تزيد عن ثلاثة آلاف دينار، أو بكلتا العقوبتين، سواء قام بجريمة انتحال الشخصية الإلكترونية المرتبطة بجريمة الدخول غير المشروع أو قام بانتحال الشخصية الإلكترونية المرتبطة بالاستيلاء على أموال أو تواقيع الغير.

9- ساوى المشرع الفلسطيني بين عقوبة مرتكب جريمة انتحال الشخصية الإلكترونية الأصلي، وبين عقوبة من يشترك معه في تلك الجريمة.

ثانياً: التوصيات:

1- أوصي المشرع الفلسطيني برفع وتشديد العقوبة المقررة على جريمة انتحال الشخصية الإلكترونية نظراً لخطورتها.

2- ضرورة تنظيم العقوبات التبعية لجريمة انتحال الشخصية الإلكترونية، بحيث ينص المشرع الفلسطيني على عقوبة مصادرة الموقع الالكتروني لمنتحل الشخصية الإلكترونية أو إتلافه.

3- ضرورة تفعيل دور أنظمة الحماية الإلكترونية في المؤسسات الحكومية والخاصة، وتزويد هذه المؤسسات ببرامج ووسائل متطورة لمكافحة هذه الجريمة.

4- ضرورة النص صراحه في التشريعات الجنائية على الأدلة الإلكترونية كأدلة إثبات في المجال الجنائي والاعتراف لها بحجيه قاطعه.

المراجع

أولاً: المصادر:

قانون العقوبات الأردني رقم 16 لسنة 1960م، الساري في الضفة الغربية في فلسطين.

القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

القرار بقانون رقم (38) لسنة 2021م، بتعديل قرار بقانون رقم (10) لسمة 2018م بشأن الجرائم الإلكترونية وتعديلاته.

القرار بقانون رقم (15) لسنة 2017م بشأن المعاملات الإلكترونية.

القانون الأساسي الفلسطيني المعدل لسنة 2003م.

قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م.

مشروع قانون العقوبات الفلسطيني لسنة 2011م.

قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015م.

قانون العقوبات المصري رقم 58 لسنة 1937م.

قانون العقوبات الجزائري أمر رقم 66-156 لسنة 1966م.

قانون العقوبات اللبناني رقم 340 لسنة 1943م.

قانون العقوبات السوري رقم 148 لسنة 1949م.

قانون عقوبات البحرين لسنة 1967م.

ثانياً: المراجع

أ. الكتب:

ابن فارس، معجم مقاييس اللغة، تحقيق عبد السلام هارون، دار الفكر للنشر والتوزيع، بيروت، 1979م.

أحمد عبد السلام علي، التعليق على جرائم التزييف والتزوير في قضاء العقوبات في ضوء الفقه والقضاء، دار الكتب القانونية، مصر، 2007م.

أحمد براك، الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية تأصيلية مقارنة، الطبعة الأولى، دار الشروق، رام الله، 2019م

أحمد مصطفى، جرائم الحاسبات الالية في التشريع المصري، دار النهضة العربية، الطبعة الأولى، 2010م.

أحمد أبو خطوة، شرح قانون العقوبات القسم الخاص، جرائم الاعتداء على الأموال، دار النهضة العربية، القاهرة، 1994م.

أحمد هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2008م.

أمير يوسف، الاثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، مكتبة الوفاء القانونية، الطبعة الاولى، الاسكندرية، 2016م.

أشرف قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015م.

توفيق خشاشنة، مسرح الجريمة ومعاينته عبر شبكة المعلومات الدولية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2020م.

جلال ثروت، النظرية العامة لقانون العقوبات، مؤسسة الثقافة الجامعية، الاسكندرية، الطبعة الأولى.

جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، مصر، الطبعة الأولى.

حسن المرصفاوي، قانون العقوبات الخاص، منشأة المعارف، الاسكندرية، 1975م.

حسن طاهر داوود، جرائم نظم المعلومات، أكاديمية نايف للعلوم الأمنية، الرياض، السعودية، الطبعة الأولى، 2000م.

خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية،2009م.

خالد ابراهيم، التقاضي الالكتروني، القاهرة، دار الفكر الجامعي، 2008.

رؤوف عبيد، مبادئ الإجراءات، مكتبة النهضة، مصر، 1956م.

سعد سلامة، معاينة مسرح الجريمة والاثبات الجنائي، أكاديمية الشرطة، كلية الشرطة، مصر.

سامي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2011م.

صابر عبد العزيز سلامة، العقد الإلكتروني، دار النهضة العربية، القاهرة، الطبعة الثانية، 2007م.

عبد العزيز الشبل، الاعتداء الإلكتروني (دراسة فقهية) دار كنوز إشبيليا، الرياض، الطبعة الأولى، 2012م.

عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007م.

عبد الفتاح حجازي، الجوانب الإجرائية لأعمال التحقيق، دار النهضة العربية، القاهرة، الطبعة الأولى.

علي الطوالبة، الجرائم الالكترونية، جامعة العلوم التطبيقية، الطبعة الأولى، 2008م.

علي الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004م.

عبد الستار فوزية، شرح قانون العقوبات (القسم الخاص) دار النهضة العربية، الطبعة الأولى، القاهرة، 1988م.

عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور، دار هومة، الجزائر، الطبعة الأولى، 2005م.

عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007م.

عبد القادر جرادة، القضاء الجنائي الدولي والحرب على غزة، المجلد الأول: الجريمة الدولية، مكتبة أفاق، غزة، الطبعة الثانية، 2010م.

غنام غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة، مصر، 2017م.

قيس التميمي، شرح قانون العقوبات العراقي، العاتك للطباعة، بيروت، 2019م.

كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي القانونية، دمشق، 2007م.

محمد بن يعقوب الفيروزبادي، القاموس المحيط، تحقيق: مكتب تحقيق التراث في مؤسسة الرسالة، مؤسسة الرسالة، بيروت، الطبعة الثامنة، 2005م.

محمد صبحي نجم، قانون العقوبات، القسم العام، دار الثقافة، عمان، الطبعة السادسة.

محمد الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دراسة مقارنة، دار الفكر والقانون، المنصورة، الطبعة الأولى.

محمد الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2006م.

محمد بن مكرم ابن منظور، لسان العرب، الجزء 11، المطبعة الأدبية ببولاق، مصر، الطبعة الأولى، 1888م.

منصور، المعايطة، الأدلة الجنائية والتحقيق الجنائي، دار الثقافة للنشر والتوزيع، الطبعة الاولى، عمان، 2007م.

مصطفى موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، الطبعة الأولى، القاهرة.

نهلا المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، 2008م.

نائلة قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2005م.

نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت، دار الفكر الجامعي، الطبعة الأولى، 2007م.

نبيل جاد، جرائم الحاسب الآلي، مطبعة بن دسمال، الطبعة الأولى، دبي، 2014م.

ب. الرسائل العلمية:

أحمد، الحديثي، قيمة الدليل الإلكتروني في الإثبات الجنائي: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة عمان الاهلية، الأردن، 2019م.

حمزة المعايطة، جريمة الاحتيال الإلكتروني: دراسة تحليلية مقارنة، رسالة ماجستير، جامعة مؤتة، الأردن، 2012م

زيد بني خالد، التنظيم القانوني لجريمة انتحال الشخصية الإلكترونية وفقا لقانون الجرائم الإلكترونية الأردني، رسالة ماجستير، كلية الحقوق، جامعة جرش، 2021م.

عمر الجبوري، جريمة التزوير الإلكتروني في التشريع الأردني: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2017م.

علاء شريم، أدلة مسرح الجريمة وحجيتها في الإثبات الجنائي: دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2021م.

فتحي كبور، جرائم انتحال الوظائف والألقاب وإساءة استعمالها في التشريع الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، الجزائر، 2019م.

محمد الشموط، الإثبات في الجرائم الالكترونية: دراسة مقارنة، رسالة دكتوراة، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية، الأردن،2015م.

محمد عنب، معاينة مسرح الجريمة، رسالة دكتوراة، كلية الدراسات العليا، أكاديمية الشرطة، مصر، 1988م.

محمد الخوالدة، جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني: دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، الجامعة الأردنية، الأردن،2012م.

مبارك البنيان، المسؤولية الجزائية عن اتلاف البيانات والمعلومات الإلكترونية، رسالة ماجستير، كلية القانون، جامعة اليرموك، الأردن، 2021م.

مصطفى الرواشدة، جريمة الابتزاز الإلكتروني في القانون الأردني، رسالة ماجستير، عمادة الدراسات العليا، جامعة آل البيت، 2019م.

مهدي رضوان، إجراءات الضبط والتفتيش في الجرائم الالكترونية في النظام الفلسطيني، رسالة ماجستير، كلية الدراسات العليا، جامعة بيرزيت، فلسطين، 2023م.

هلال امنة، الاثبات الجنائي بالدليل الإلكتروني، رسالة ماجستير، جامعة محمد خيضر، بسكرة، الجزائر،2015م.

ولاء البياري، انتحال الشخصية في الفقه الإسلامي، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2018م.

وليد دقديقة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية، رسالة ماجستير، كلية القانون، جامعة طرابلس، ليبيا، 2015م.

ت. الأبحاث والمجلات العلمية:

أمين الخنتوري، الهوية الشخصية على شبكات التواصل الاجتماعي بين اللاتنظيم وضرورة التنظيم، مجلة البوغاز للدراسات القانونية والقضائية، العدد 9، 2020م.

أحمد شهاب، ونور بن مارني، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة الندوة للدراسات القانونية، العدد23، 2019م.

اقبال أمين، انتحال الوظيفة العامة ونطاق مسؤوليتها، مجلة الحقوق، العدد41، الجامعة المستنصرية، 2021م.

إيهاب التاج، التحقيق وجمع الأدلة في الجرائم المعلوماتية، مجلة العدل، وزارة العدل، المملكة العربية السعودية، المجلد 11، العدد 26، 2009م.

خليل إعبية، القالب التشريعي لجرائم انتحال الصفة والشخصية الإلكتروني: دراسة مقارنة، مجلة العلوم الإنسانية والإدارية، جامعة المجمعة، العدد 22، 2021م.

خالد الجسمي، الإثبات الجنائي بالأدلة الرقمية، مجلة القانون المغربي، دار السلام للطباعة والنشر، المغرب، العدد34، 2017م.

دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، بحث مقدم للمؤتمر العلمي الرابع لكلية الحقوق جامعة طنطا تحت عنوان (القانون والإعلام) المنعقد في 23-24 إبريل 2017م.

سعيد المزروعي، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقا للتشريع الإماراتي، مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث غزة، المجلد 2، العدد 13، 2018م.

عبد اللطيف ربايعة، الجرائم الإلكترونية، بحث مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، جامعة النجاح، 2016م.

علي الفيل، جريمة الاحتيال عبر البريد الالكتروني: دراسة مقارنة، مجلة الحقوق، جامعة الكويت، المجلد 36، العدد2، 2012م.

عادل عثمان، ضبط الأدلة في مجال الجريمة المعلوماتية، رابطة الأدب الحديث، مجلة فكرة وإبداع، المجلد 113، 2017م.

عبد الناصر فرغلي، ومحمد المسماري، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، مقدم في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الامنية، الرياض، 2007م.

عبد الله حسين محمود، إجراءات جمع الأدلة في مجال الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003م.

محمد رحموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، المجلد 17، العدد41، 2018م.

محمد العجمي، جريمة انتحال الشخصية في مواقع التواصل الاجتماعي: دراسة فقهية مقارنة بالقانون الكويتي، مجلة الشريعة والدراسات الإسلامية، جامعة الكويت، المجلد 37، العدد 130، 2022م.

محمد سهيل، انتحال الصفة في المجتمع العراقي: الأنماط والمخاطر، مجلة الدراسات المستدامة، الجمعية العلمية للدراسات التربوية المستدامة، المجلد 6، 2024م.

موفق عبيد، ماهية جريمة الاحتيال المعلوماتي، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد 5، العدد19، 2016م.

ميسون الحمداني، مشروعية الادلة الالكترونية في الاثبات الجنائي، بحث منشور، كلية الحقوق، جامعة النهرين، بغداد، 2007م.

مسعود المعمري، الدليل الالكتروني لإثبات الجريمة الالكترونية، مجلة كلية القانون الكويتية العالمية، العدد 3، 2018م.

The Crime of Electronic Identity Impersonation According to the Palestinian Cybercrime Law: An Analytical Study

Thaer Khader Ahmad Bani Odeh
Dr. Abdul Latif Rabaia
Dr. Issam Al-Atrash
Dr. Ahmad Al-Ashqar

Abstract

This study addresses the crime of electronic identity impersonation from both substantive and procedural aspects. The aim of this study is to clarify the meaning of this crime, explain the elements that must be present, identify its various forms, and demonstrate how the Palestinian legislator has regulated its provisions and imposed penalties on perpetrators. Additionally, the study outlines the procedures for collecting evidence used in committing this crime and the investigation and trial processes involved.

The researcher employed the descriptive-analytical method and the comparative legal approach by presenting the legislative frameworks that govern the punishment of electronic identity impersonation.

The study reached several findings, the most significant of which is that the crime of electronic identity impersonation involves a person claiming to be someone else by presenting themselves under a false identity. The Palestinian legislator, through Decree-Law No. (10) of 2018 on Cybercrimes, explicitly criminalized electronic impersonation and imposed penalties on its perpetrators, treating both the main perpetrator and any accomplice equally in terms of punishment.

The researcher concluded with several recommendations, most notably the necessity of increasing and tightening the penalty prescribed for the crime of electronic identity impersonation due to its seriousness.

Keywords: Impersonation, Electronic Identity, Cybercrimes, Elements of Crime, Penalty for Impersonation Crime