جـامعـــة النجاح الوطنية

كليـــة الدراســـات العليـــا

الحماية الجنائية لعمليات التحويل الإلكتروني للأموال في التشريعات السارية في فلسطين

إعداد

لميس تيسير محمود لحلوح

إشراف

د. فادي شديد

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجه الماجستير في القانون الجنائي، من كلية الدراسات العليا، في جامعة النجاح الوطنية، نابلس– فلسطين.

2024

الحماية الجنائية لعمليات التحويل الإلكتروني للأموال في التشريعات السارية في فلسطين

إعداد

لميس تيسير محمود لحلوح

نوقشت هذه الرسالة بتاريخ 2024/10/16 م، وأجيزت:

د. فادي شديد	التوقيع
المشرف الرئيسي	
د. غسان عليان	التوقيع
الممتحن الخارجي	
د. نور عدس	التوقيع
الممتحن الداخلي	

ب

الإهداء

إلى أمي وأبي وأخوتي اللذين كانوا سبباً في نجاحي ومصدر سعادتي وقوتي ومهما تكلمت لن أفي بحقهم إلا القليل

وإلى زوجي عبد الله الذي سندني ورعاني وقدم لي جميع وسائل الراحة والطمأنينة وهيّأ لي الجو المناسب طوال فترة الدراسة فجزاه الله عني خير جزاء

إلى خالتي المعلمة الفاضلة ابتهال التي كانت الدافع وراء دخولي للماجستير وقدمت لي كل الدعم المعنوي والمساندة خلال مسيرتي الدراسية إلى أن وصلت إلى هذه المرحلة

إلى صديقاتي الحبيبات وأخص بالذكر إيمان التي كانت تشجعني دائماً على الاستمرار والتقدم وعدم اليأس والإحباط فكانت بمثابة الداعم المعنوي والمشجع لي

إلى أسرة مكتب الأستاذ غسان دبابنة رحمه الله، حيث تدربت على يديه واكتسبتُ منهُ العلم والمعرفة ، وكان يقدم لي يد العون والمساعدة والعطاء فكان لا يبخل بإعطاء أي معلومة قانونية نحتاجها، فأسال الله أن يتغمده برحمته جزاءً لعطاءه الدائم لنا

أقدم عملي هذا.

الشكر

الحمدُ للهِ على نعمه ظاهرها وباطنها ما علمنا منها وما لم نعلم والحمد الله أن أرزاقنا بيده ونحمده ونشكره على تمام نعمته وعلى منَه عليَ أنّ أعانني على إنجاز هذا العمل المتواضع.

وأتوجه بخالص الشكر والامتنان إلى أساتذتي في جامعه النجاح ولكل من علمني حرفاً

وأتوجه بالشكر والتقدير للدكتور فادي شديد لإشرافه على رسالتي والذي كان المعين لي بعد الله في إتمام هذه الرسالة فله مني كل الاحترام والامتنان.

كما أشكر أعضاء لجنة المناقشة لموافقتهم المشاركة في عضوية لجنة المناقشة متطلعة لما سوف يقدمونه من النصح والإرشاد.

الإقرار

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل عنوان:

الحماية الجنائية لعمليات التحويل الإلكتروني للأموال في التشريعات السارية في فلسطين

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرسالة ككل أو أي جزء منها لم يقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب: ليث نصير محمود خلوع

التوقيع: _____

التاريخ: ١٠/١٦/ ٢٠٢٤

فهرس المحتويات

الحماية الجنائية لعمليات التحويل الإلكتروني للأموال في التشريعات السارية في فلسطين

إعداد

لميس تيسير محمود لحلوح

إشراف

د. فادي شديد

الملخص

لقد تحدثت في دراستي عن موضوع الحماية الجنائية لعمليات التحويل الإلكتروني للأموال في التشريعات السارية في فلسطين "دراسة وصفية تحليلية"، وقد احتوت على فصلين، حيث تناول الفصل الأول القواعد الجنائية الموضوعية لحماية عمليات التحويل الإلكتروني للأموال، من حيث ماهية هذه العمليات وصور الحماية الجنائية الموضوعية لعمليات التحويل الإلكتروني للأموال، أما بالنسبة للفصل الثاني فقد تم التطرق إلى القواعد الجنائية الإجرائية لحماية عمليات التحويل الإلكتروني للأموال، من خلال الحديث عن إجراءات التتبع والملاحقة الخاصة بالجرائم الواقعة على عمليات التحويل، والإجراءات الوقائية الخاصة بمكافحة هذه الجرائم الواقعة عليها.

وتكمن الأهمية العملية في هذه الدراسة أنها عالجت أمور حياتية نعيشها بشكل يومي، وفي كثير من الأحيان نضطر للقيام بأعمال التحويل الإلكتروني للأموال، فإذا لجأ إلى الطريقة التقليدية فقد يتعرض للسرقة أو للتزوير وغيرها من المخاطر، وبالتالي عمليات التحويل الإلكتروني للأموال سهلت هذه العملية، إلا أن هذه العمليات غير آمنة بشكل مطلق، فلذلك حرصت التشريعات على توفير الحماية الجنائية اللازمة لهذه العمليات وذلك من خلال وضع نصوص تنظم هذه العمليات وتُجرّم الاعتداء عليها.

أما بالنسبة لإشكالية هذه الدراسة فتمحورت في الإجابة على التساؤل الرئيسي ألا وهو كيف حمى المشرع الجنائي عمليات التحويل الإلكتروني من المخاطر التي قد تواجهها، ومن خلال بحثي هذا توصلت إلى

عدة نتائج وتوصيات، ومن أهم هذه النتائج التي توصلت لها هي أن التحويل الإلكتروني للأموال أصبح من أمور العصر الحديث، فمن الدول من قامت بسن تشريعات تنظم وتجرم الاعتداء على عمليات التحويل الإلكتروني للأموال وذلك انطلاقاً من الطبيعة الخاصة بتلك الجرائم، ومن الدول من لم يسن تشريع خاص ينظم ويُجرّم الاعتداء على هذه العمليات، وأن قانون التجارة الأردني والساري في فلسطين لم يضع نصوصاً خاصة تنظم عمليات التحويل الإلكتروني للأموال، وبالتالي اجتهد الفقهاء والقضاء في إيجاد نصوص بديلة لتنظيم هذه العملية، وذلك من خلال القرار بقانون بشأن المعاملات الإلكترونية والقرار بقانون بشأن الجرائم الإلكترونية وقانون المدفوعات الوطنية الفلسطيني، وبخصوص التوصيات التي توصلت لها هو ضرورة العمل على تدريب الكوادر البشرية الموجودة في فلسطين على طريقة كشف الجرائم التي تقع على عمليات التحويل الإلكتروني للأموال وطرق التعامل معها وجمع الأدلة الإلكترونية والمحافظة عليها، وطرق تحويل الدليل الإلكتروني لدليل مادي ملموس مثل تخزينه على قرص صلب حتى تتمكن النيابة من تقديمه للمحكمة والاستناد عليه للإدانة.

الكلمات المفتاحية: التحويل الإلكتروني للأموال، القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، الدليل الرقمي.

المقدمة

تعتبر عمليات التحويل الإلكتروني للأموال من الأمور التي أصبحت منتشرة في الوقت الحالي بشكل كبير؛ وذلك نتيجة التقدم التكنولوجي والتقني، حيث أصبح لدينا فضاء إلكتروني، وبالتالي أصبح التواصل مع دول العالم أمر سهل ليس كما كان قديماً، حيث أصبح ارتباط تقدم الدولة يقارن بما وصلت له من تقدم تكنولوجي، وبالتالي هذا ساهم بالقيام بعمليات تحويل ضخمة بين بالدول المختلفة، وخاصة تحويل الأموال الذي هو موضوع دراستنا، ففي السابق كان تحويل الأموال يتم بالطرق العادية، وما كان يرافق هذه العملية من مخاطر منها السرقة أو التزوير وغيرها من المخاطر، فجاءت عمليات التحويل الإلكتروني للأموال؛ لتوفير الوقت والجهد وإعطاء الأمان والراحة لأصحاب العلاقة، وبالتالي قل الاستخدام المادي للنقود، فأصبح هناك حاجة لوضع ضوابط لتنظيم عمليات التحويل الإلكتروني للأموال، في إطار قانوني يتناسب مع ظروف عمليات التحويل (فهمي، 2021).

تعتبر عمليات التحويل الإلكتروني للأموال من أهم العمليات وأكثرها انتشاراً في الوقت الحالي، ولكن قانون التجارة الأردني لم يضع نصوصاً خاصة تنظم عمليات التحويل الإلكتروني للأموال (عمر، 2007)، وبالتالي اجتهد الفقهاء والقضاء في إيجاد نصوص بديلة لتنظيم هذه العملية سواء القرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018، والقرار بقانون بشأن المعاملات الإلكترونية رقم 15 لسنة 2017، والقرار بقانون الخاص بغسل الأموال وتمويل الإرهاب رقم 39 لسنة 2022.

وبخصوص التطور التاريخي لعملية التحويل الإلكتروني للأموال، فقد ساهم التقدم العلمي والتكنولوجي في تطوير هذه العملية بشكل كبير، فأصبح هناك سهولة في عملية التحويل، وبالتالي اختصار الوقت والجهد ،ومع هذا التطور فإن دور البنوك قد ظهر وأصبح بارزاً، حيث وفرت خدمات بنكية إلكترونية عالية التقنية؛ وذلك نتيجة طبيعة عمل البنوك فهي مواكبة للتطورات الحديثة وخاصة في أعمال التحويل الإلكتروني للأموال، ولا بد من الإشارة إلى أن هذا التطور له إيجابيات وسلبيات، فالتكنولوجيا هي سلاح

ذو حدين، وبالتالي هذا الأمر فرض على المشرع وضع قواعد قانونية وضوابط لحماية أموال الأفراد، ووضع أيضاً ضوابط لتحديد المسؤولية القانونية لكل طرف في العلاقة (عديس، 2017).

أهمية الدراسة

الأهمية النظرية

تكمن الأهمية النظرية في ضرورة تنظيم عمليات التحويل الإلكتروني للأموال، حيث أن هناك وجهات نظر مختلفة بين التشريعات، فمن التشريعات من قامت بتنظيم عمليات التحويل الإلكتروني للأموال مثل الولايات المتحدة الأمريكية، حيث قامت بتنظيم عمليات التحويل الإلكتروني من خلال قانون التحويل الإلكتروني(EFT) لعام 1978، وهناك من التشريعات الأخرى لم تقم بتنظيم هذه العمليات ضمن قانون خاص بها، مثل المشرع الفلسطيني الذي نظم هذه العمليات ضمن عدة قوانين منها القرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية، والقرار بقانون رقم 41 لسنة 2022 بشأن المدفوعات الوطني الفلسطيني، وتعليمات سلطة النقد الفلسطينية حول تنظيم أعمال التحويل الإلكتروني للأموال.

الأهمية العملية

تكمن الأهمية العملية في أن العديد من التشريعات قد تنبهت لموضوع ضرورة توفير حماية جزائية في تشريعاتها لحماية عمليات التحويل الإلكتروني للأموال، ووضعت نصوص جرمت الاعتداء على هذه العمليات وكذلك وضعت عقوبات يمكن وصفها بأنها رادعة مثل التشريع السعودي والفرنسي والتشريع المغربي، حيث وضعت هذه الدول في القوانين والتشريعات الخاصة بها نصوص واضحة جرمت الاعتداء على عمليات التحويل الإلكتروني للأموال، ووضعت ضمن العقوبات غرامات مالية كبيرة لتحقيق الردع، وأما بالنسبة للمشرع الفلسطيني فقد وضع نصوص تشريعية جزائية لحماية هذه العمليات، إلا أن هناك نقص من ناحية كفاية هذه النصوص التشريعية وذلك لتوفير الحماية الجنائية لعمليات التحويل الإلكتروني للأموال.

إشكاليات الدراسة

سوف تعالج الباحثة من خلال هذه الدارسة إشكالية عامة تتمثل من خلال التساؤل الرئيس التالي وهو: **كيف حمى المشرع الجنائي عمليات التحويل الإلكتروني للأموال من المخاطر التي تواجهها ؟** وتتفرع عن هذه الاشكالية العديد من التساؤلات:

1. ماهية عمليات التحويل الإلكتروني للأموال ؟.
2. كيف يتم تنفيذ عمليات التحويل الإلكتروني للأموال وما هي شروطها ؟.
3. توضيح صور الحماية الجنائية الموضوعية لعمليات التحويل الإلكتروني الأموال في فلسطين ؟.
4. ما هي الجرائم التي يمكن أن يتم ارتكابها على عمليات التحويل الإلكتروني للأموال وصورها وأشكالها؟.
5. توضيح الإجراءات القانونية الخاصة بضبط وملاحقة الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال؟.

أهداف الدراسة

1. توضيح ماهية عمليات التحويل الإلكتروني للأموال.
2. بيان أنواع عمليات التحويل الإلكتروني للأموال التي يتم تنفيذها سواء داخل الدولة أو خارج إقليم الدولة والقوانين التي تغطيها داخلياً أو خارجياً.
3. توضيح كيفية تنفيذ عمليات التحويل الإلكتروني للأموال وشروط تنفيذها.
4. توضيح طبيعة الجرائم التي يمكن أن يتم ارتكابها على عمليات التحويل الإلكتروني للأموال.
5. بيان الجرائم التي يمكن أن يتم ارتكابها على عمليات التحويل الإلكتروني للأموال وصورها وأشكالها.

منهج الدراسة

استخدمت الباحثة المنهج الوصفي التحليلي، وذلك من خلال تحليل النصوص التي نظمت موضوع التحويلات الإلكترونية المالية، وجرمت القيام بالأعمال التي تشكل اعتداء عليها، وكذلك استرشدت الباحثة بالمنهج المقارن، وذلك من خلال الاطلاع على قوانين الدول الأخرى أينما لزم، المتعلقة بموضوع الحماية الجنائية والتنظيم القانوني لموضوع التحويل الإلكتروني للأموال.

حدود الدراسة

إن الحدود الموضوعية في هذه الدراسة تكمن في القرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018، وقانون التجارة رقم 12 لسنة 1966، والقرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية، والقرار بقانون رقم 41 لسنة 2022 بشأن المدفوعات الوطنية الفلسطيني.

الدراسات السابقة:

تمثلت أبرز الدراسات السابقة التي تناولت الموضوع بما يلي:

1. أ نور الدين زحوفي، أ عمر زمالة، التحويل المالي الإلكتروني والمخاطر في ظل عصرنة وسائل الدفع : جامعة الجيلالي بونعامة، الجزائر، مجلة الاقتصاد الدولي والعولمة، تحدثت هذه الدراسة عن تعريف وتوضيح وسائل الدفع الحديثة في التحويل الإلكتروني، وما أهمية التحويل الإلكتروني المالي كآلية لتفعيل العمليات المالية والمصرفية، ومن أهم النتائج التي وصلت لها هذه الدراسة أن التحويل الإلكتروني للأموال ساهم في سرعة دوران النقود، حيث أن هناك تسهيل وتسريع لهذه العمليات وذلك بسبب التطور التكنولوجي الحاصل، وبالرغم من وجود عدة ميزات إلا أنه لا زال هناك عوائق ومخاطر تضعف أداء التحويل الإلكتروني للأموال كالقرصنة والفيروسات التي تضعف نظام شبكة المعلومات وقد تقوم بتعطيله.

2. سميحة دغوش، النظام القانوني لجريمة التحويل الإلكتروني غير المشروع للأموال، جامعة أم البواقي، الجزائر، رسالة ماجستير 2018 تحدثت الرسالة عن ماهية التحويل الإلكتروني للأموال، وما هي أهميته، وما طبيعته القانونية، وكذلك صور التحويل الإلكتروني غير المشروع، مثل الاحتيال على النظام المعلوماتي، والاحتيال باستخدام بطاقات الدفع الإلكتروني، وجريمة خيانة الأمانة في النطاق المعلوماتي، ومن أهم النتائج التي وصلت لها في هذه الدراسة، أن شبكة الإنترنت هي سلاح ذو حدين وقد تعتبر أداة لارتكاب الجريمة في حال استخدامها بطريقة سلبية، فتكون المنفذ والطريقة لحصول الجاني على البيانات والمعلومات بصورة غير شرعية كما هو الحال في جرائم الاعتداء على الأموال بطريقة إلكترونية، وأيضاً أن السعي في التطور التكنولوجي وتحسين الخدمات المقدمة من قِبل البنوك والمؤسسات والشركات المالية أدى إلى حدوث العديد من الجرائم أهمها جريمة الاحتيال.

وقد تميزت الدراسة عن الدراسات السابقة في أنها تحدثت عن الجانب العملي في فلسطين، من جهة الحديث عن كيفية تنفيذ عمليات التحويل الإلكتروني للأموال، وأن المشرع قد أفرد حماية خاصة بالرغم أنه لا يوجد تشريع خاص بجرائم عمليات التحويل الإلكتروني للأموال، في حين أن الدراسات السابقة لم تتحدث عن الحماية الجنائية لعمليات التحويل الإلكتروني للأموال، وتميزت الدراسة أيضاً في جانب الإجراءات القانونية الخاصة بالتتبع وملاحقة الجرائم، حيث تحدثت عن الخصوصية في هذه الإجراءات حيث يوجد وحدة متخصصة ونيابة اقتصادية متخصصة بهذا النوع من الجرائم وهي التي تشرف على إحالة هذا النوع من الجرائم إلى المحكمة، بالإضافة إلى الحديث عن إجراءات التحقيق النهائي وصولاً إلى دور الدليل الإلكتروني في الإثبات وكيفية تكوين القاضي قناعته بناءً على هذا الدليل، وهذا ما سوف يميز هذه الدراسة حيث أن الدراسات السابقة لم تتحدث عن الواقع العملي والتطبيقي في حماية عمليات التحويل الإلكتروني للأموال وتمييزها عن غيرها من الجرائم .

مخطط الدراسة

سوف تقوم الباحثة بالإجابة عن الإشكالية العامة من خلال بيان القواعد الجنائية الموضوعية لحماية عمليات التحويل الإلكتروني للأموال في الفصل الأول، ومن ثم الحديث عن القواعد الجنائية الإجرائية لحماية عمليات التحويل الإلكتروني للأموال في الفصل الثاني.

الفصل الأول

القواعد الجنائية الموضوعية لحماية عمليات التحويل الإلكتروني للأموال.

تعرف عمليات التحويل الإلكتروني، على أنها مجموعة من الإجراءات التي تبدأ عن طريق البنك الآمر أو ما يسمى البنك الوسيط، الذي يصدر منه أمر التحويل إلى بنك آخر يسمى البنك المستفيد ، وتتم العملية بشكل نهائي عند قبول البنك المستفيد أمر التحويل، ويكون المبلغ مبين ومحدد في أمر التحويل، فمثلاً البنك العربي أجرى تحويلة لبنك فلسطين بقيمة مليون شيكل، هنا تتم عملية التحويل بقبول البنك الفلسطيني هذه الحوالة، ويسمى هنا البنك العربي المصدر، والبنك الفلسطيني المستفيد، وبعض الفقهاء قاموا بتسمية هذه العملية؛ بأنها عملية تجري بين دائن ومدين، ويترتب على هذه العملية نقل مبلغ من حساب أحد العملاء في البنك الأول، إلى حساب آخر في البنك الثاني، مع العلم أنه في الواقع الحالي تجرى التحويلات إلكترونياً (راشد، 2022)، ولكي نفهم موضوع الحماية الجزائية الموضوعية لعمليات التحويل الإلكتروني للأموال، سوف نتطرق لموضوع ماهية عمليات التحويل الإلكتروني للأموال في المبحث الأول، و صور الحماية الجنائية الموضوعية لعمليات التحويل الإلكتروني للأموال في المبحث الثاني.

المبحث الأول: ماهية عمليات التحويل الإلكتروني للأموال

يُعرف التحويل الإلكتروني للأموال على أنه القيام بعملية نقل واحدة أو أكثر لحساب مصرفي واحد أو أكثر من حساب العميل، باستخدام وسائل حديثة نتيجة التقدم التكنولوجي الحديث، مثل المصارف التي يتم التعامل معها عن طريق الإنترنت، أو أجهزة الصراف الآلي، أو عن طريق الهاتف المحمول، وبالتالي توفير الوقت والجهد الذي سوف يبذل لو أن هذه الطرق غير موجودة، مثل جهد السفر ونقل المال، بالإضافة للمخاطر التي يمكن أن يتعرض لها الشخص الذي سوف ينقل المال مثل السرقة أو ضياع المبلغ، وتتم إجراءات النقل المالي بشكل سريع وفوري، وذلك نتيجة إجراءات المقاصة السريعة والدفع الفوري (زخوفي ، 2018)، وسوف تدرس الباحثة في هذا المبحث مفهوم عمليات التحويل الإلكتروني

للأموال في المطلب الأول، وكيفية تنفيذ عمليات التحويل الإلكتروني للأموال في المطلب الثاني، وشروط عمليات التحويل الإلكتروني للأموال في المطلب الثالث.

المطلب الأول: مفهوم عمليات التحويل الإلكتروني للأموال.

وبالرجوع للنصوص المختلفة المتعلقة بتحويل الأموال إلكترونياً، سواء قانون التجارة الأردني رقم 12 لسنة 1966، والقرار بقانون بشأن المعاملات الإلكترونية رقم 5 لسنة 2017 الساري في فلسطين، نجد أن هذه القوانين لم تعرف مفهوم التحويلات الإلكترونية للأموال، إنما هي نظمت موضوع تحويل الأموال الإلكترونية، دون التطرق لموضوع تعريف التحويلات الإلكترونية، بخلاف القوانين الأجنبية منها القانون الأمريكي حيث عرف التحويل الإلكتروني للأموال ضمن قانون تحويل الأموال الإلكتروني الصادر في عام 1978 في الفقرة aمن المادة 6 على أن "مصطلح التحويل الإلكتروني للنقود يعني تحويل النقود وغيرها ويستثنى من ذلك صفقات نشأت عن طريق الصك أو الحوالة أو سند ورقي مشابه، والتي بدأت من خلال محطة إلكترونية، وسيلة هاتفية أو حاسوب أو شريط مغناطيسي، لكي يصدر أمر أو يفوض منشأة مالية بإجراء قيد دائن أو مدين بالحساب وهذا مصطلح يشمل لكن ليس على سبيل التحديد، التحويلات في نطاق البيع، مكائن الصراف الآلي، إيداع أو سحب النقود والتحويلات التي بدأت عن طريق الهاتف" (كلية القانون جامعة كربلاء).

ويمكن تعريف التحويل الإلكتروني على أنه عملية يقوم فيها البنك من الجانب الدائن إلى جانب المدين وبمقتضى هذه العملية يتم نقل مبلغ معين من المال من الجانب الأول وهو حساب الآمر إلى حساب آخر وذلك بموجب أمر كتابي، وقد قُربت هذه العملية إلى عملية الدّين، حيث تتم هذه العملية بحسابين، الأول يسمى الآمر والثاني يسمى حساب المستفيد، ويأخذ البنك عمولة مقابل هذه الحوالة، ولابد من الإشارة إلى أن عملية تحويل الأموال قد تتم بطريقتين الأولى الطريقة التقليدية والثانية الطريقة الإلكترونية الحديثة، فالطريقة الأكثر انتشاراً واستخداماً في الوقت الحالي هي الطريقة الإلكترونية، وذلك من أجل السرعة وتوفير الوقت والجهد وقلة التكلفة وتتم بوسائل تكنولوجية مثل الهاتف والحاسوب، ويرتب أثره القانوني دون

الحاجة إلى أن يكون طرفا العقد في مجلس واحد، فيمكن أن تتم العملية من خلال رسالة بريد إلكتروني من البنك المصدر (الآمر) إلى البنك المستفيد، يطلب بموجبها بقيد مبلغ إلى جهة المستفيد بعد الرد بقبول الحوالة من جهة المستفيد (غزوي، 2021).

وقد وفرت البنوك بطريقة الحوالات المالية عدة مميزات للمتعاملين معها، إلى جانب أن البنوك أصبحت من أهم المؤسسات في العصر الحالي، وخصوصاً فيما يتعلق بالحياة الاقتصادية، وبالتالي قيام البنوك بعمليات التحويلات الإلكترونية للأموال وفرت على الزبائن الوقت والجهد كبديل للوسائل التقليدية؛ نظراً لارتفاع تكلفة النقل التقليدي للأموال وطول المسافة، حيث كان قديماً لنقل الأموال من قارة لأخرى، يحتاج إلى وقت وجهد وطول المسافات بالإضافة إلى خطر السرقة، وبالتالي فإن التحويل الإلكتروني للأموال، وفر العديد من المميزات للمستخدمين في الوقت الحالي (الزبن، 2019).

ولعمليات التحويل الإلكتروني للأموال فوائد كثيرة، أهمها أنها تمكن أي مواطن في أي دولة من الاستفادة من خدمات بنك في دولة أخرى فهي تعتبر عابرة للحدود، وبالتالي أصبح التعاملات المصرفية منتشرة على الصعيد الدولي وهذه العمليات ساعدت بشكل كبير في موضوع التجارة الإلكترونية، ومن فوائدها أيضاً تقليل الأعمال الورقية، وهي عبارة عن وسيلة تساهم بشكل كبير بالوفاء بالالتزامات المالية، وبراءات الذمة دون تكليف الشخص بالحضور الفعلي للمكان (أوشن، 2022).

بالإضافة إلى أن التحويل الإلكتروني للأموال مكّن الأشخاص من تحويل أموالهم من دولة إلى أخرى بكل سهولة وسرعة، وبالتالي توفير جهد التوجه إلى البنك مباشرة، فأصبح بكبسة رز يتمكن من إجراء عملية التحويل، ويمكن إجراء عملية التحويل بأي وقت، بالتالي يمكن إجراء التحويل حتى بفترة عطلة نهاية الأسبوع الخاصة بالمصارف (ريد، 2017).

ويمكن أن يتم إجراء التحويلات الإلكترونية للأموال داخل الدولة نفسها بين المحافظات، أو داخل المحافظة نفسها بين فروع البنوك المختلفة، ويمكن أن يكون التحويل دولياً فقد تستغرق عدة أيام، وقد تصل إلى ثلاثة أيام وذلك في الماضي، بخلاف الحوالة التي تكون داخل البلد التي قد تستغرق بضعة ساعات، أما في الوقت الحاضر ومع التطور الحاصل فأصبح التحويل الخارجي والداخلي يأخذ بضع ساعات قليلة دون الفرق الشاسع بين التحويل الداخلي والخارجي، ومن مميزات الحوالات البنكية الدولية أنها في بعض البنوك يمكن لها إجراء الحوالة عن طريق بطاقات مسبقة الدفع، ولابد من الإشارة إلى أن لإجراء الحوالة البنكية مجموعة من الشروط أهمها، بلوغ سن 18 سواء للمُرسل أو المُستقبل، بالإضافة للهوية الشخصية، وامتلاك رقم الحوالة البنكية، واستقبال رسالة تفيد بنجاح عملية التحويل (موقع صناع الأمل، 2023).

إن التحويل الإلكتروني للأموال من العمليات المصرفية التي لا تتطلب وجود نقل مادي للأموال بل يمكن نقل أو تحريك النقود بين الحسابات المختلفة من خلال شبكة الإنترنت، إن عقد تحويل الأموال الإلكترونية ينعقد بمجرد تلاقي الإيجاب مع القبول دون اشتراط أن يكون الطرفين في مجلس واحد فيمكن أن يتم باستخدام وسائل حديثة تعبر عن إرادة الطرفين، إن عمليات التحويل الإلكتروني الأموال سهلت على الناس إنهاء معاملاتهم وتنفيذها مجرد وضع المبلغ في حساب الدائن تبرأ ذمة المدين، وهذا ما حرصت عليه الدول من أجل تشجيع عمليات التحويل الإلكتروني في معاملاتهم المالية حيث تعتبر عمليات التحويل الإلكتروني من أيسر العمليات وأقل تكلفة في الواقع العملي ولكونها عمليات سهلة فإن ذلك شجع المواطنين في استخدام التحويلات الإلكترونية للأموال من أجل تسوية معاملاتهم الخاصة (محمد، 2022).

ويقوم التحويل الإلكتروني للأموال على أساس القيام بنقل قيمة مالية من حساب مصرفي إلى حساب مصرفي آخر أو يمكن أن يتم على حسابات مصرفية متعددة من خلال الآليات الإلكترونية مختلفة التي تتم من خلال الإنترنت أو أجهزة الصراف الآلي أو من خلال استخدام الهاتف المحمول، ويقوم هذا النظام على استخدام إجراءات المقاصة الآلية التي تلغي عملية التسوية العادية، وفي ظل التطور التكنولوجي

ينعكس ذلك على التطور في عمليات التحويل الإلكتروني الأموال سواء بالسحب أو الدفع وهذا زاد من ثقة الأفراد في التعامل مع عملية التحويل الإلكتروني خاصة في ظل أن نسبة الخطأ والتزوير قد قلت ذلك من جهة، ومن جهة أخرى أنها تقوم بتخزين البيانات والمعلومات بطريقة آمنة (نور الدين و عمر، 2018).

وبالرغم من الإيجابيات الكثيرة للحوالات البنكية، إلا أنه يوجد لها بعض السلبيات، من أهمها أنها تعتبر ملغية في حال أن المستقبل لم يقم باستلامها أو السؤال عنها، وتحتسب المدة في الحوالات النقدية ثلاثة أشهر، والبنكية ستة أشهر من تاريخ التحويل، وبالإضافة إلى أنه في حال تم القيام بإعادة إرسالها، فإن البنك أو شركة الصرافة يقومون بأخذ عمولة جديدة، بالإضافة إلى العمولة التي تم سحبها بأول عملية تحويل، ويتم أيضاً خصم فروقات الأسعار، وهناك سلبية أخرى تتعلق في أنه إذا تم إرسال الحوالة إلى المُستقبِل، وكان العميل قد حدد البيانات الخاصة بالمُستقبِل، ولكن كان هناك خطأ بهذه البيانات فإن العميل هو الذي يتحمل هذا الخطأ، وبالتالي يتحمل الخسارة المالية، وكذلك في حالة أن العميل قام بإلغاء الحوالة أو غير المعاملة، فأنه يقوم بدفع العمولة المالية للبنك أو لشركة الصرافة، ومن السلبيات كذلك أنه على العميل توضيح جميع المعلومات التي يطلبها البنك أو شركات الصرافة، أي عليه تقديم معلومات عن مصدر هذه الأموال التي سوف يجري الحوالة بناءً عليها، أي أن يكون مصدر المال قانوني وموثوق، بالإضافة إلى أنه إذا رغب العميل بتقديم شكوى نتيجة خطأ أو خلل، فأنه يجب عليه تقديمها خلال 14 يوم من تاريخ إصدار المعاملة وغير ذلك لا يجوز تقديمها (العتوم، 2021).

ومثال عملي لاستغلال حسابات البنوك لسرقة واختلاس الأموال الموجودة فيها، وفي حكم لمحكمة النقد الفلسطينية المنعقدة في رام الله رقم 33 لسنة 2018 الذي فصل بتاريخ 15 فبراير 2021، حيث كان الطعن المقدم من شركة بنك القاهرة عمان المساهمة العامة المحدودة رام الله والمطعون ضدهم شركة المهندس أبو هاشم للمقاولات وتعهدات العامة العادية، وكان موضوع الدعوى المطالبة بمبلغ 26555598، وكانت المدعى عليها حصلت على التسهيلات وبكفالة المدعى عليه الثاني، حيث قامت

المدعى عليها بفتح اعتماد مالي عام بالشيكل وكفالات مصرفية متعددة، ونتيجة استغلالها لهذه التسهيلات ترصد في ذمتها المبلغ المذكور أعلاه، وردَت المدعى عليها باللائحة الجوابية أنها لم تستغل التسهيلات المصرفية لوقوع عملية السرقة أو الاختلاس وأن هذه التسهيلات تمت بالبنك من قبل المدير، وجاء قرار المحكمة لصالح المدعي حيث قررت إلزام وتضمين المدعى عليها المبلغ المذكور أعلاه وورثة المدعى عليه الثاني والثالث والرابع بالتضامن بدفع هذا المبلغ، وقامت المدعية بتقديم استئناف على الحكم لكن محكمة الاستئناف ردت الطعن وأيّدت حكم محكمة الموضوع وبعد ذلك توجهت المدعى عليها لمحكمة النقض وجاء في قرار محكمة النقض التأكيد على إلزام المدعى عليها بكامل المبلغ بالإضافة إلى الرسوم والمصاريف وأتعاب المحاماة (مقام، 2018).

أما بالنسبة لرأي الباحثة فترى أن قرار المحكمة قد وافق الصواب وأن المدعى عليها قد استغلت التسهيلات المقدمة من قبل البنك، وأنها قامت بخداع البنك فقامت المحكمة بإصدار قرار بإعادة المبلغ وتضمينها الرسوم والمصاريف.

ولتحديد طبيعة عقد الحوالة، قام الفقهاء بتقريب هذا العقد إلى عدة عقود اختلفوا فيها، فمنهم قرب الحوالة لعقد النقل، ودافعوا عن فكرتهم بناءً على أن عقد الحوالة والنقل كلاهما يرتب التزام بنقل الشيء محل العقد وكلاهما بمقابل، ولكن ما يناقض هذه الفكرة أن العميل يتوجه للبنك أو شركة الصرافة لإجراء عملية النقل، أما الفقهاء الفرنسين اعتبروا عقد الحوالة عقد مركب، وأسسوا فكرتهم على أساس أن الحوالة تتم بثلاثة مراحل، أولها توجه العميل للبنك لإيداع المبلغ الذي سوف تتم الحوالة لأجله، والمرحلة الثانية قيام البنك بتحويل المبلغ للمستفيد، والمرحلة الأخيرة قبول المستفيد هذا المبلغ، ولكن الانتقاد الذي وجه لهذه العملية أنه من الصعب تجزئة عملية التحويل؛ لأن حق المستفيد ينشأ بمجرد قيد المبلغ في حسابه، أما النظرية الثالثة والتي أخذ فيها القضاء العربي، هي أن الحوالة المالية تعتبر حوالة قيد أموال؛ وذلك لأنها تعتبر نقود قيديه، ولا تختلف عن النقود العادية التي يتم تداولها بالحوالات المالية عن طريق الحسابات، وهذا ما أكدت

عليه محكمة النقض المصرية، حيث أكدت المحكمة أن تحويل العملاء للأموال عن طريق البنوك لا تعتبر عقود، بل هي عمليات تحويل مصرفية تجري داخل جدران المصارف، وهي لا تعتبر عمليات رضائية بالمعنى البحت وبالتالي هي عمليات مصرفية، والانتقاد الذي وجه إلى هذه النظرية، أنها لم تراعي أن أصل هذه العملية، هي عقد ناشئ بين الآمر والبنك، وكذلك أن هذه النظرية اعتبرت أن إرادة المستفيد تدور وجوداً وعدماً مع إرادة الآمر والبنك، وهذا الأمر مخالف لطبيعة العقد القانونية، وأن هذا العقد لا يرتب التزام قانوني على المستفيد تجاه الآمر والبنك (فهمي، 2021).

المطلب الثاني: كيفية تنفيذ عمليات التحويل الإلكتروني للأموال

وانطلاقاً من عنوان الدراسة (التحويل الإلكتروني للأموال)، فله عدة أنواع منها التحويل المصرفي، وسوف توضح الباحثة هذا النوع في هذا المطلب، ثم التحدث عن باقي أنواعه مثل ويستر يونيو أو باي بال أو المحفظة المالية أو التحويل عبر الإنترنت، وذلك بالتسلسل موضحة لكل نوع مميزاته وعيوبه خلال الدراسة.

الطريقة الأولى: التحويل المصرفي

فتجري عملية التحويل المصرفي، عن طريق أمر صادر عن أحد العملاء ينقل بموجبه مبلغ معين من المال من حسابه إلى حساب آخر لنفس العميل أو عميل آخر، وتتم هذه العملية بطريقة سريعة بخلاف الحوالة العادية، ويتم على أثر هذه العملية نقل مبلغ من المال، من حساب العميل إلى المستفيد، مع الإشارة إلى أن نوع العملة غير مهم، سواء كانت عملة أجنبية أو وطنية، ويمكن أن تتم عملية التحويل لحسابين لنفس الشخص أو حسابين لعميلين مختلفين، وقد يكون التحويل لنفس المصرف أو مصارف مختلفة وقد يتم التحويل لشخصين من نفس الجنسية أو جنسيات متعددة، وقد تتم بين أشخاص يسري عليهم القانون الخاص، أو أشخاص يخضعون للقانون العام، وقد يكون التحويل من أجل عمل مدني أو عمل تجاري، سواء كان داخلي أو خارجي (التكروري، 2020).

وفيما يتعلق بأحكام التحويلات المالية الإلكترونية هناك قرار لمحكمة استئناف رام الله رقم 551 لسنة 2017 حيث جاء بحيثيات القرار أن المدعي أقام دعوى مطالبة مالية ناتجة عن عدم قيام الجهة المدعى عليها (المصرف) بإجراء الحوالة المصرفية، وهي عبارة عن أتعاب عمالية ل 27 عامل في غزة، وفي التدقيق تجد محكمة الاستئناف أنه كان على محكمة الدرجة الأولى تكيف العلاقة بين المدعي والمدعى عليهم، بأنها حوالة مصرفية حتى وإن لم يكن هناك اتفاق مسبق على ذلك ، وأن على المدعى عليهم (العمال) فتح حسابات بنكية لاستقبال هذه الحوالات، وقد أشارت محكمة الاستئناف في قرارها، أن الأمر بتحويل أو ما يسمى (الحوالة المصرفية) لا يكون إلا من تاريخ تنفيذها، وقيد قيمتها في حساب المستفيد، وعدم إجراء الحوالة يرتب حق للمستفيد للقيام بالمطالبة بالتعويض عن الضرر، وأيضاً قد أشارت المحكمة أن على البنك أن ينفذ أمر الحوالة دون تأخير معني لذلك، وبالتالي لا يجوز عليه التأخير دون مبرر، وإلا يكون مسؤولاً عن تعويض المتضرر عن الضرر الذي لحق به نتيجة التأخير، وفي هذه الدعوى نرى أن البنك لم يقدم أي بينة يثبت فيها أنه كان لديه مبرر للتأخير؛ ونتيجة تأخيره قام العملاء بسحب مبالغ الحوالات، بالتالي لا يستطيع البنك هنا القيام بتحويل المبالغ للمستفيدين، ولحل المشكلة قام البنك بأرسال إخطارات عدلية للعملاء بإيداع المبالغ المطلوبة إلا أنهم لم يستجيبوا لهذه الاخطارات، وبقرار المحكمة لجبر الضرر قررت الحكم للمدعي بقيمة ما فاته من مبالغ مالية وإجراء الحوالة للعمال (قرار محكمة استئناف رام الله رقم 551 لسنة 2017).

ويتم تنفيذ الحوالة عن طريق التوجه لأي فرع من فروع البنك، وتزويد البنك بالمبلغ المراد تحويله، ومن ثم الموظف يقوم بتحديد العمولة التي يجب اقتطاعها من المبلغ، وذلك من خلال نظام البنك الذي يعمل فيه، ويحدد المرسل اسم الشخص المراد إجراء الحوالة إليه، ويرسل رقم سري يسمى MTCN ، ومن ثم يقوم المستقبل باستلام رقم الحوالة MTCN من المرسل سواء عن طريق الهاتف أو البريد الإلكتروني أو أي وسيلة تواصل، ومن ثم يتوجه المستفيد لأي فرع من فروع البنك الذي تم إجراء الحوالة إليه، ومن ثم يقدم المستفيد رقم الحوالة و الهوية الشخصية أو جواز السفر لإثبات الهوية، وعلى إثر ذلك يتم سحب الحوالة

وتسليمها للمستفيد ويقوم بالتوقيع على الاستلام، مع العلم أنه يمكن للمرسل التراجع عن الحوالة إذا لم يقم المستفيد باستلامها بعد (موقع البنك الإسلامي العربي، 2023).

وبالنسبة لأنواع الحوالات المالية فتقسم إلى قسمين، الأول الحوالة الداخلية والقسم الثاني الحوالة الخارجية؛ أما الحوالة الداخلية فلها أنواع النوع الأول منها، الحوالات الداخلية التي يبيعها المصرف وهي الحوالة التقليدية التي يقوم بها العميل بتحويل مبلغ من المال لحساب آخر عن طريق البريد أو الهاتف أو أي طريقة أخرى، أما النوع الثاني فهي الحوالة التي يشتريها المصرف، ومثال عليها الشيكات حيث يتم تقديمها إلى البنك لغاية صرفها مقابل عمولة بسيطة، والنوع الثالث هو الحوالات المالية المسحوبة على البنك، حيث يتم إصدار هذه الحوالة من قبل البنك، وتسحب من أي فرع من فروعه داخل الدولة، وقد تكون بموجب صك مالي أو أمر دفع أو برقية مالية أو حوالة مالية مسحوبة على الفروع من خلال الهاتف، والنوع الرابع هو الحوالات الداخلية التي تكون برسم التحصيل، ومثال عليها الكمبيالة أو السفتجة أو الصكوك المالية والخطابات المتعددة وغيرها من المستندات المالية التي يمكن تقديمها للبنوك وتحصيل قيمتها المالية (العتوم، 2021)، والقسم الثاني من الحوالات هو الحوالات الخارجية، ويمكن تعريفها بأنها أمر دفع يتخذه العميل لتحويل مبلغ معين من مصرف معَين(الجهة المحولة)، أو قد يتم التحويل عبر موقع معتمد أو عن طريق الإنترنت وغيرها من طرق تحويل الأموال إلكترونياً، وبناءً على هذا الأمر يتم دفع مبلغ إلى المستفيد في الجهة المقابلة، وقد تكون هذه الحوالة صادرة أي يتم إرسال هذه الحوالة للخارج، أو واردة أي يتم إرسالها إلى الداخل، ويكون العميل هو الجهة المستفيدة، وقد يتم استلامه نقداً أو يتم إيداع المبلغ في حساب العميل نفسه (اسماعيل، وآخرون، 2022).

الطريقة الثانية: أولاً التحويل عبر شبكات التحويل المعتمدة ويسترن يونون:

وهي عبارة عن شركة أمريكية، متخصصة بالتحويلات المالية بين دول العالم المختلفة، وتحظى هذه الشركة بشهرة واسعة جدا على مستوى العالم، حيث تتميز بسهولة التحويل والأمان الذي توفره على

المستوى الدولي، ويعتمد عليها الكثير من الأفراد سواء من خلال تحويل الأشخاص لأموالهم لعائلاتهم أو للأمور التجارية، مثل شركات التسويق والإعلانات وغيرها، وقد وفرت الشركة فروع لها في جميع أنحاء العالم، فلديها 550000 فرع، وعميل في 200 دولة، وأكثر من 130 عملة مختلفة، ولهذه الشركة مميزات عديدة سوف تقوم الباحثة بذكر أهمها:

1) "يمكن تتبع الحوالة بسهولة كذلك السرعة الكبيرة باستلام النقود أي بعد دقائق من تحويلها.
2) لكثرة فروعها ولكونها لها فروع في أغلب دول العالم، بالتالي سهولة تحويل واستلام الأموال من أي مكان في العالم، ويمكن استخدام وسترن يونيون لتحويل الأموال لحسابات بنكية.
3) وقد وفرت الشركة تطبيق ع الهاتف، وبالتالي يمكن إجراء الحوالة عن طريق الهاتف المحمول بأسهل الطرق وأسرعها.
4) يمكن سحب المال بالعملة التي تم إرسالها مثل اليورو أو الدولار.
5) من المميزات أيضاً، أنه يكفي لإجراء التحويل أو الاستلام بطاقة الهوية، كذلك المستلم لا يدفع أي رسم على الاستلام.
6) يمكن تحويل الأموال عبر بطاقة الائتمان" (داردونا، 2015).

يعتبر موقع ويسترن يونيون خيار مثالي لتحويل الأموال، خاصة أنه يتعامل مع العملات الصعبة مثل الدولار واليورو والجنيه الإسترليني، وهناك عدة طرق يستخدمها ويسترن يونيون لتحويل الأموال، منها wire transfer وهذه الطريقة الأكثر انتشاراً كونها لا تحتاج لحساب بنكي، حيث يتم استلام الأموال بشكل شخصي، ويتم سحب العملة التي جرى تحويلها، فمثلاُ قام المرسل بتحويل مبالغ بعملة اليورو يتم استقبالها بعملة اليورو، مع العلم أنه يمكن استخدام الحساب البنكي للتحويل، وذلك في حال كان التحويل لحساب بنكي آخر، ويمكن أن يتم التحويل من خلال الهاتف المحمول، وذلك عن طريق تحديد المبلغ المراد تحويله في البداية، والبلد المستقبلة للحوالة، وتحديد المبلغ المراد تحويله، واسم الشخص الرباعي

المراد التحويل لحسابه، مع العلم أن عملية الاستلام تكون خلال فترة قصيرة، إما بنفس اللحظة أو حد أقصى ثلاثة أيام، مع العلم أنه عند استلام الحوالة لا يتم سحب أي رسم عليها، إلا في حال تحويل البنك يتم فرض الرسم من قبل البنك (صناع المال، 2023).

وثانياً: التحويل عبر شبكات التحويل المعتمدة هي باي بال:

حيث تتميز هذه الطريقة بأنها توفر الأمن والحماية وسهولة الاستخدام، حيث تعتمد على وجود بريد إلكتروني فقط وليس حساب بنكي أو غيره، ومن مميزاته أيضاً أنه يمكن استخدام هذا الموقع لشراء المقتنيات المنتشرة عبر الإنترنت، ولكن يوجد لها بعض السلبيات منها أن الكثير من الدول العربية غير داعمة لهذا الموقع، وكذلك لا يمكن ربط هذا الموقع مع مواقع أخرى كثيرة، وكذلك من عيوب هذا الموقع أيضاً أنه يفرض شروط جديدة من فترة لأخرى، وبالتالي لابد من مراجعة البيانات باستمرار وتحدثها، وبالإضافة إلى أن تحويل الأموال قد يستغرق بعض الوقت أحياناً (يوسف، 2021).

الطريقة الثالثة: التحويل عبر التطبيقات والبرامج الإلكترونية التي توفر لك المحفظة المالية

هي عبارة عن وسيلة دفع إلكترونية أو رقمية تمكن من تنفيذ دفعات وتحويل أموال، وهذه الطريقة موجودة منذ سنوات، ولكنها تطورت في الآونة الأخيرة بشكل كبير، وأبسط تعريف لها أنها وسيلة دفع مقابل شراء أشياء معينة، ويمكن استخدامها عن طريق الهاتف المحمول وتسمى بالمحفظة كونها تشبه إلى حد كبير المحفظة العادية، حيث تخزن العديد من الأشياء مثل رخصة القيادة وتعتبر أكثر أماناً من التقليدية، ومن مميزاتها أنها يمكن استخدامها عن طريق جهاز الهاتف ويمكن عن طريق جهاز الحاسوب، وهذا التطبيق أصبح أكثر شيوعاً، ويتم استخدامه عن طريق تثبيت تطبيق المحفظة على جهاز الهاتف أو الحاسوب، وعند القيام بعملية الشراء لابد من التأكد مسبقاً أن هذا الموقع المراد الشراء منه يتعامل بالمحفظة الإلكترونية، وتتميز المحفظة الرقمية بالعديد من المميزات أهمها:"1) الراحة، حيث يمكن ببساطة التجول فيها بدلاً من حمل المحفظة التقليدية التي تحتوي على الأوراق والأموال، 2) تعتبر طريقة منظمة وآمنة،

كون المحفظة التقليدية تسهل عملية سرقتها، وبالتالي يمكن تفادي هذه الأمور بالمحفظة الإلكترونية، فإذا سرق الهاتف فإن السارق يحتاج إلى معرفة كلمة المرور لدخول الهاتف المحمول وكذلك كلمة المرور الخاصة بالمحفظة الإلكترونية، وذلك على عكس المحفظة التقليدية 3) توفر المحفظة مكافئات إضافية، مثل الحصول على مشتريات أكثر مقابل الأموال المدفوعة بالمقارنة بالطريقة التقليدية 4) تعتبر أكثر أماناً بدلاً من حمل مستندات مالية وأوراق مالية والتنقل فيها من مكان لآخر، وما يجعلها أكثر أماناً أنها تعمل على تشفير البيانات الخاصة بالمستخدمين وخصوصاً البيانات المالية" (جريس، 2018).

وما يميز هذه الطريقة أيضاً أنه يمكن إيداع الأموال في المحفظة مباشرة دون أي عملات أو رسوم إضافية كذلك يمكن استقبال الأموال من أي حساب بنكي للمحفظة الإلكترونية، كذلك يمكن تحويل العملات المرسلة إلى المحفظة حسب عملة البلد المستقبلية (السيد، 2022).

وحتى يتم إجراء عملية التحويل للمحفظة يتم اختيار الأموال التي أريد إرسالها إلى محفظة الهاتف المحمول وتحدد البلد والعملة والمبلغ الذي أريد إرساله وأختار طريقة الدفع وإدخال اسم ورقم الهاتف المستفيد الخاص بي ومن ثم أؤكد المبلغ وأرسله (أفضل 4 خدمات تحويل الأموال عبر الإنترنت في 2023، 2023).

الطريقة الرابعة: التحويل عبر الإنترنت من خلال بعض المواقع الإلكترونية والمرخصة والمعتمدة

تهدف هذه العملية إلى تسهيل عملية تحويل الأموال، وخاصة في خدمة فئات المهاجرين الذين يحتاجون هذه الطريقة من أجل تحويل الأموال إلى أهليهم في بلدهم الأصلي، وتقليل تكلفة عملية التحويل عليهم مقارنة بتكلفتها عند توجههم للمصارف، وذلك انطلاقاً من غاية تحسين ظروفهم الاقتصادية ووصول المبلغ كامل للمُستقبِل دون خصم منه عمولات بنكية، ويتم عرض هذه الخدمات في حوالي 40 بنك، وصندوق توفير وشركات تحويل، ويتم إخبار المُرسل المدة التي سوف تستغرقها الحوالة للوصول للمستقبل، وكثير من الشركات عملت على تخفيض أسعارها، منها الموقع البريطاني sendmonyhome الذي خفض مصاريف التحويل من بريطانيا إلى الهند، وبالتالي توفير مصادر دخل ناتجة عن الحوالات للبلدان الفقيرة،

حيث أن البنك الدولي قدر الحوالات بقيمة 310 مليار دولار أمريكي، وبالتالي أكثر بكثير من المساعدات التنموية التي تم تقديمها للدول النامية في سنة 2006 والتي قدرت بحوالي 104 مليار دولار أمريكي، وهذا يعمل بشكل كبير على تقليل نسبة الفقر في الدول التي تتلقى هذه الحوالات وبالتالي المساعدة في زيادة النمو الاقتصادي (فيله، 2007).

ويمكن أن نقوم بطرح تساؤل: كيف حمى المشرع عمليات التحويل الإلكتروني للأموال من الجرائم التي قد تقع عليها؟

فيمكن الإجابة على هذا التساؤل بأن المشرع حمى هذه العمليات من خلال إصدار تشريعات خاصة تكفل الحماية الجنائية لمستخدميها، لا سيما أن الأمر يتعلق بأموال المستخدمين، والذي يفرض على الدولة ضمان حمايتها وذلك لاستقرار المجتمع (شبول، 2023)، وأيضاً من أجل الحد من انتشار الجريمة وذلك بإتباع إجراءات احترازية، ووضع عقوبات صارمة تحقق الردع العام داخل المجتمع، ولأن المسؤولية الجنائية تخضع لمبدأ الشرعية فأي سلوك خاطئ يرتكب يحتاج إلى نص يجرمه وربط الفعل بالنتيجة الجرمية ووجود علاقة سببية بينهم (دهشان، 2023)، فاشترط المشرع حتى تستطيع المؤسسات المالية القيام بعمليات التحويل أن تحصل أولاً على الترخيص، فهذا يعتبر بمثابة حماية وحرص على أموال المواطنين، وذلك من أجل تجنب الخداع من أي جهة تدعي بأنها جهة مسموح لها القيام بهذه الإعمال، وعلى مستوى البنوك فهناك اجراءات احتياطية تتبعها البنوك، وذلك كالمصادقة على أوامر الدفع المتمثلة في الإجراءات الاحتياطية، مثل توفير حماية عالية وتشفير عالي حتى تكون الحوالات في مأمن من الغش والاعتراض، وهذا ما يزيد الثقة في البنوك، ويرجع الفقه أساس مسؤولية البنك التعاقدية إلى نوعين، أولها الأدوات المستخدمة في البنك لإتمام عملية التحويل مثل الأجهزة وبرامج النظام المالي التابع للبنك، وثانياً مسؤولية البنك بالالتزام بالسلامة استناداً لفكرة العدالة، وهو شرط أضافه القضاء، فإذا حصلت مشكلة وكان السبب الضرر يعود للأجهزة والبرامج التي يستخدمها البنك فإن المسؤولية هنا مسؤولية تقصيرية

وليست مسؤولية عقدية، وهناك رأيي فقهي آخر يقول أن البرامج والأجهزة غير مستقلة عمن يستخدمها فالضرر الذي يحصل لا يخرج البنك من دائرة المسؤولية العقدية، وهناك بنوك قامت بتغيير شروط طبيعة الالتزام لجعلها التزام ببذل عناية وليس تحقيق نتيجة، وذلك لإعفائها من المسؤولية عن الأضرار التي قد تحدث، فيقع على عاتق البنك مسؤولية مدنية وهي بالتعويض عن الضرر الذي لحق العميل، مثل عدم إتمام أمر الدفع أو حصول خطأ في أمر الدفع، كأن يقوم بالتحويل لشخص آخر غير الشخص المطلوب، فيكون هناك التزام على البنك يتضمن بموجبه برد مبلغ التحويل في هذه الحالة (المري، 2019)، وهناك مسؤولية جنائية تقع على المصرف وذلك في حالة إخلاله بقواعد الالتزام، كأن يقدم معلومات يحميها السر المصرفي دون إذن صاحبها كأن يعطي معلومات عن الحوالات المالية التي يقوم بها العميل دون إذنه، وهذا ما ذهب به المشرع الفرنسي في المادة 13/226 من قانون العقوبات وذلك أن البنك يعتبر مؤتمن على أسرار عملائه، فعكس ذلك يعرضه للمسؤولية الجزائية، وأيضاً نص المشرع العراقي في قانون العقوبات العراقي رقم 111 لسنة 1969 في المادة 123 على وقف الشخص المعنوي إذا ارتكبت جريمة جناية أو جنحة من أحد ممثليه، وإذا تكررت فيجوز للمحكمة أن تأمر بحل الشخص المعنوي، ويستنتج من هذا النص أن جرائم الاعتداء على الأموال الخاصة بالعملاء بأي وسيلة كانت كأن يكون بإفشاء سر خاص يتعلق بأموال العملاء، سواء كان يتعلق بأمر تحويل أو غيره فيعاقب على هذا الفعل، وإذا تكرر ذلك الفعل الذي يشكل جنحة أو جناية من أحد ممثلي هذا الشخص المعنوي، فإن للمحكمة أن تأمر بحل الشخص المعنوي (مسؤولية المصرف عن تقديم معلومات الإئتمان المالي، 2023)، ونرى أن هناك من التشريعات الأجنبية من قامت بتنظيم عمليات التحويل الإلكتروني للأموال مثل الولايات المتحدة من خلال قانون للتحويل الإلكتروني (EFT) لعام1978 ، وأيضاً نجد أن قانون النموذجي وضع أعباء على عاتق البنوك، فألزمها بالفحص المستمر لأوامر الدفع التي تستلمها لإثبات أنها لا تحتوي على أي شبهات أو أخطاء، والتأكد من أي أمر دفع جرى استلامه لا يتضمن المعلومات الكافية، وهناك إجراء أمني تطلبته المادة A 4 من ذات القانون وهو ما يطلق عليه بالمصادقة "فهو إجراء تتبناه البنوك للحد من احتمال أن

يكون أمر الدفع الذي تسلمته البنوك جرى إرساله من قِبل الشخص المعّين، كما يعد مثل هذا الإجراء وسيلة للتأكد من صحة أمر الدفع" (المري، 2019)، بإضافة إلى أمر المصادقة **ترى الباحثة** أن هناك نقطة يجب الانتباه إليها، وذلك إذا كان هناك اتفاق بين البنك و العميل على إتباع إجراء أمني معين، فعلى البنك الالتزام بهذا الإجراء، وإذا لم يقم البنك بهذا الالتزام فيكون البنك مسؤولاً عن أضرار التي سوف تحصل بسبب الإهمال في الالتزام الواقع عليه.

وفي المملكة السعودية هناك لجنة تسمى لجنة المنازعات المصرفية وفي قرار لها رقم (177/1424) جاء "أن أموال العملاء أمانة لدى البنك ويجب الحفاظ عليها وحمايتها فإذا أخل البنك بالتزامه بالمحافظة عليها فيتحمل مسؤولية ذلك، فإذا تمت عملية مالية دون توقيع العميل أو من يُنيبه فالبنك ملزم بإعادة المبالغ المسحوبة من الحساب، وهذا داخل في باب إهمال الموظف من التأكد من صحة توقيع العميل" (العيسى، 2021).

وأيضاً شدد المشرع السعودي على القيام بجرائم الاستيلاء على الأموال والتي ترتكب بطريقة إلكترونية، فلم يكتفي بالعقاب على الفعل المجرم إنما عاقب على الشروع أيضاً، وذلك بنصف العقوبة للجريمة الأصلية كحد أعلى، وذلك لتحقيق أقصى درجات الحماية (عطاالله، 2024) .

وأيضا قام المشرع الفلسطيني بتوفير الحماية القانونية سواء بطرق مباشرة أو غير مباشرة، مثل تجريم الاعتداءات على عمليات التحويل الإلكتروني للأموال، وذلك وفقا لنصوص المواد التي جرمت أي جريمة تقع على عملية التحويل الإلكتروني للأموال، كتجريم الاحتيال الإلكتروني وتشمل إدخال البيانات غير صحيحة أو تعليمات غير المشروع التصريح بها، أو استعمال بيانات وعمليات غير مصرح للوصول إليها بغية السرقة من قبل الموظفين فاسدين في الشركات المؤسسات المالية حذف أو تعديل المعلومات المحفوظة أو إساءة استعمال أدوات الأنظمة المتوفرة وخرق البرامج (الاستخبارات العكسرية الفلسطينية، 2022).

فإذا حصلت جريمة سرقة بطريقة إلكترونية، فنجد ان قانون العقوبات رقم 16 لسنة 1960 لم يسعفنا في تكييف نوع التهمة، وذلك بأن قانون العقوبات صنف أنواع السرقة وشدد بعضها إلا أننا نجد أن الدعاوى المنظورة أمام محاكم الفلسطينية حول جريمة السرقة التي تتم بوسائل إلكترونيه، يتم تكييفها تارة بأحكام السرقة وفقا لنص المادة 399، وتارةً أخرى يتم تكييفها على أنها جريمة احتيال وفقا لنص المادة 417 على اعتبار أن ما حصل هو خداع أوقع المجني عليه على تسليم المال، فنرى أن المشرع قد قصر بعدم وضع نص خاص يتناسب مع جريمتي السرقة والاحتيال التي تتم بطريقة إلكترونية، وذلك لعدم تناسب جسامة الفعل مع العقوبة المخصصة للجرائم التقليدية.

المطلب الثالث : شروط عمليات التحويل الإلكتروني للأموال.

لابد من توفير شروط عامة تتعلق بتحويل الأموال عن بعد والتي سوف تقوم الباحثة بعرضها، فهي عقد صالح يعبر عن إرادة صريحة، ففي البداية لابد من بلوغ المرسل سن 18 سنة أي سن الأهلية القانونية، وأن تكون عملية تحويل الأموال لأغراض مشروعة، مثلا إجراء عملية التحويل للأصدقاء أو العائلات لأغراض قانونية؛ وذلك لتجنب الأعمال غير المشروعة مثل غسيل الأموال أو الاحتيال أو تمويل الإرهاب، ولابد للعميل من تحديد هويته أي إضافة بعض البيانات الشخصية الخاصة به، وكذلك البيانات الشخصية الخاصة بمُستقبِل الحوالة مثل الاسم وعنوان البريد الإلكتروني وبعض المعلومات المالية (انترناشيونال، 2023).

كذلك يتم التحقق من هوية العميل، وفي بعض الأحيان يتم أخذ رقم الهاتف الخاص بالعميل، وإعطاؤه رقم سري خاص به، ويمكن للعميل تغير الرقم السري بالوقت الذي يريد، ولابد من أن يلتزم العميل بالتعليمات الخاصة بسلطة النقد الفلسطينية، ولابد من التأكد من التزام العميل بالقوانين والأحكام الفلسطينية المنظمة لهذه المواضيع، ويكون استخدام هذه الخدمات للعميل نفسه، وليس له أن يطلع أي شخص عليها أو يمكّنه من استخدامها، ويجب على العميل الحفاظ على سرية البيانات وأي تغير أو إفشاء للسرية يتحمل العميل المسؤولية، ويتعهد العميل بأنه هو المستفيد الحقيقي من تحويلات الأموال، وليس شخص آخر يقوم

بتوجيهه أو يعمل تحت سلطته، وتخضع عمليات التحويل للقوانين الفلسطينية والقرارات بقانون السارية فيها، وفي حال تغير أي بيان من بيانات العميل، فأنه يلتزم بإخطار الجهة المتعامل معها بهذه البيانات، وإلا يتحمل المسؤولية (موقع البنك الاستثمار الفلسطيني، 2023).

ومن أهم الشروط الخاصة بعملية التحويل الإلكتروني أن يكون أمر التحويل الإلكتروني مكتوباً فقد اشترطت بعض التشريعات القانونية على وجوب أن يكون أمر التحويل الإلكتروني الصادر من العميل الآمر للبنك مكتوباً، فقد نصت المادة 2/329 من قانون التجارة المصري رقم 17 لسنة 1999 على ذلك بشكل ضمني، فبيّنت أنه: "ينظم الاتفاق بين البنك والآمر بالنقل شروط إصدار الأمر، ومع ذلك لا يجوز أن يكون أمر النقل لحامله" (قانون التجارة المصري رقم 17 لسنة 1999)، وكذلك الأمر بالنسبة للتشريع الإماراتي، فقد نصت المادة 380 من قانون المعاملات التجارية الإماراتي رقم 18 لسنة 1993 على أمر الكتابة بشكل صريح، فجاء في المادة: "التحويل المصرفي عملية يقيد المصرف بمقتضاها مبلغاً معيناً في الجانب المدين من حساب الآمر بالتحويل ويقيد ذات المبلغ في الجانب الدائن من حساب آخر وذلك بناء على طلب كتابي من العميل الآمر بالتحويل" (قانون المعاملات التجارية الإماراتي رقم 18 لسنة 1993) ، و نصت المادة (1/6) من قانون التجارة الأردني رقم 12 لسنة 1966 والساري في الضفة الغربية على أنه: " تعد الأعمال التالية بحكم ماهيتها الذاتية أعمالاً تجارية برية: د–أعمال الصرافة والمبادلة المالية ومعاملات المصارف العامة والخاصة" (قانون التجارة الأردني رقم 12 لسنة 1966)، فبما أنّ المشرّع قد اعتبر أعمال الصرافة والمبادلة وأعمال المصارف أعمالاً تجارية بريّة، فبالتالي يُمكن إثباتها بكافة طرق الإثبات، فلا يوجد نص في قانون التجارة الأردني يوجب على أن يكون أمر التحويل مكتوباً ولكن جرت العادة على الكتابة في إصدار أي أمر تحويل إلكتروني (ذوابة، 2006).

أما بالنسبة للشرط الثاني ألا وهو أن يقع التحويل على مبلغ من المال فيُعَدُّ هذا الشرط شرطاً بديهيّاً ومنطقيّاً، فالأصل أنه حتى تتم عمليّة التحويل الإلكتروني للأموال بشكل صحيح من حِساب الآمر إلى

حساب المستفيد، أو من أحد حسابات الآمر إلى حسابه الآخر؛ أنْ يكون المبلغ المطلوب تحويله موجوداً في حساب الآمر بالتحويل إذا كان عن طريق إحدى الطرق التي تلزم بوجود رصيد سابق مثل المصرف والمحفظة الإلكترونية، وأما إذا كان التحويل الإلكتروني عن طريق خدمة Western union مثلا فإن المبلغ يجب إحضاره عند القيام بعملية التحويل، فلذلك فلا يُتَصوّر أن تنفّذ عمليّة التحويل في حال عدم وجود هذا المبلغ، ففي حال أن حساب الآمر كان بالتحويل فارغاً، أو كان فيه ما لا يساوي قيمة المبلغ المطلوب تحويله، فلا يُمكن للبنك أو أي مؤسسة مالية تمارس أعمال التحويل الإلكتروني للأموال أن تقوم بتنفيذ العملية، وبحيث تنتظر المؤسسات المذكورة سابقاً توافر المبلغ عندئذٍ لإتمام عملية التحويل. (الغانمي، 2016).

وأما الشرط الثالث أن يتم انعقاد العقد أو تنفيذه بوسائل إلكترونية، حيث يشترط لإطلاق وصف وسيلة (إلكترونية) على التحويل أن يتم تنفيذه كله أو بعضاً منه باستخدام طريقة أو وسيلة إلكترونية، ويعتبر هذا المعيار الذي يميز التحويل العادي عن التحويل الإلكتروني، وهو طريق لتعبير طرفي العقد عن إرادتهم المنشأة للعقد حيث لا يشترط وجود طرفي العقد في مجلس واحد كما هو في التحويل العادي، فيتم التعبير عن الإرادة في التحويل وذلك باستخدام وسيلة إلكترونية ويتم من خلالها إيجاب والقبول لطرف التعاقد (ذوابة، 2006)، ونصت المادة 1 من القرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية أن "العقد الإلكتروني: الاتفاق بين شخصين أو أكثر بوسائل أو وسائط إلكترونية، الوسيلة الإلكترونية: الوسيلة المستخدمة في تبادل المعلومات وتخزينها وتتصل بالتقنية الحديثة وذات قدرات كهربائية، أو رقمية، أو مغناطيسية، أو لاسلكية، أو بصرية، أو كهرومغناطيسية، أو ضوئية، أو أية قدرات مماثلة. السجل الإلكتروني: مجموعة المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية والتي تشكل بمجملها وصفاً لحالة شخص أو شيء ما" (قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية).

والشرط الرابع جاء بأنه يجب أن يكون التحويل إسمياً أي أن يكون التحويل الإلكتروني لشخص معروف ومعين بالذات، ولكن المشرع الفلسطيني لم يشر في قانون المعاملات الإلكترونية إلى كون التحويل الإلكتروني إسمي وكذلك المشرع الأردني لم يشر إلى ذلك، واعتبر بعض الفقهاء وجرى العرف على أن التحويل الإلكتروني إسمي وليس لحامله وذلك للحفاظ على الحقوق ومنع السرقة والضياع (الغانمي، 2016).

المبحث الثاني: صور الحماية الجنائية الموضوعية لعمليات التحويل الإلكتروني للأموال

تتنوّع صُوَر الحماية الجنائية لعمليّات التحويل الإلكتروني للأموال، إذ أنّ هناك العديد من الصور الخاصة بهذه العملية والتي تتحدّد بحسب الجهة الخاصة بها والأطراف المتعلقة بها، سواء على مستوى البنوك أو شركات الصرافة أو المؤسسات المالية، فقامت الباحثة بتقسم الدراسة إلى مطلبين، جاء في المطلب الأول الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال ، والمطلب الثاني سوف تتحدث فيه عن قيام المسؤولية الجنائية في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

المطلب الأول: الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال

لقد أدت الثورة المعلوماتية والتكنولوجيا إلى تطور عمليات التحويل الإلكتروني للأموال والتي انتشرت بشكل سريع وهائل، ورافق هذا التطور الكبير تطور بالشق الجنائي، أي تطور الجرائم التي يمكن ارتكابها على هذه العمليات، ومن هنا جاءت الحاجة إلى توفير حماية جنائية لها، واستناداً لمبدأ الشرعية (لا جريمة ولا عقوبة إلا بنص) فلا يمكن تجريم أفعال لا ينص عليها القانون، فما كان من الفقه والقضاء في بداية الأمر إلا أن حاولوا تطبيق النصوص القانونية التقليدية المتعلقة بالجرائم العادية عليها، إلا أنه في بعض الدول تدخل المشرع وقام بسن نصوص تشريعية تتماشى مع جرائم عمليات التحويل الإلكتروني للأموال، وفي الجانب المقابل لم تقم بعض الدول بسن تشريعات جديدة لجرائم التحويل الإلكتروني للأموال؛ وإنما قاموا بتعديل النصوص التقليدية لكي تتماشى مع جرائم عمليات التحويل الإلكتروني للأموال (شنين، 2013).

ولقيام المسؤولية الجنائية في جرائم الواقعة على عمليات التحويل الإلكتروني للأموال، لابد من ارتكاب جريمة من جرائم الاعتداء على عمليات التحويل الإلكتروني للأموال، ويترتب على قيام الجريمة إسقاط النص القانوني المناسب لأركانها، وبالتالي إيقاع العقوبة المرتبطة بالنص الجرمي المرتبط بها، والتي تتعلق بعمليات التحويل الإلكتروني للأموال، ولذلك حتى تقوم المسؤولية الجنائية لابد من ارتكاب جريمة، ولفهم طبيعة هذه الجرائم سوف تقوم الباحثة في هذا المطلب ببيان بعض الجرائم الواقعة على عملية التحويل الإلكتروني للأموال.

ونتيجة أن المجتمع الفلسطيني في الفترة الأخيرة أصبح مُجاري إلى حد ما لما يحدث في الخارج، وما ينتج من تطورات في وسائل التحويل الإلكتروني للأموال، فأدى ذلك إلى ظهور جرائم مستحدثة تتمثل في أعمال نصب واحتيال للأموال التي تجري عليها عملية التحويل الإلكتروني للأموال، وقد تتم هذه الطرق عن طريق شركات وهمية توحي للعملاء بتقديم الخدمات أو السلع، ومن ثم يقوم العميل بتحويل هذه الأموال ولكن لا يحصل على شيء، وغيرها من وسائل التسويق الإلكتروني التي تهدف للوصول إلى جيوب الأفراد ودفعهم للقيام بعمليات تحويل إلكتروني، ومن ثم لا يحصلوا على شيء، وقد تتم عملية الاستيلاء على الأموال المحولة، عن طريق أسلوب احتيالي يقوم على إقناع العملاء بأن يقوم بإيداع وتحويل مبالغ مالية بهدف استثمارها وتحويلها ومن ثم تعود للعميل بمبالغ أكبر ومن ثم لا يحصل على شيء مما سبق، وهنا يثور تساؤل هل نجح المشرع الفلسطيني في ضبط جميع الجرائم التي تقع على عمليات التحويل الإلكتروني للأموال؟ وذلك لأن الأصل في التجريم أنه لا جريمة ولا عقوبة إلا بنص ، وحتى لا نكون أمام فجوة تشريعية يستطيع الجناة من خلالها الهروب من الجريمة نتيجة عدم وجود نص قانوني يجرم الفعل، فإن الحل والمخرج القانوني الذي يعتمد عليه القضاء الفلسطيني في تجريم الأفعال التي يتم ارتكابها على عمليات التحويل الإلكتروني للأموال، انطلاقاً من قانون العقوبات الساري في فلسطين رقم 16 لسنة 1960، والقرار بقانون رقم10 لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته 38 لسنة 2021.

أولاً: استغلال وسائل الدفع الإلكتروني لتبييض الأموال

إن استخدام تقنيات الدفع الإلكتروني في الواقع العملي أثبت أنه بقدر ما سهلت عمليات تحويل الأموال، وبالمقابل أصبح المجرمين قادرين على ابتكار تقنيات حديثة من أجل الاستيلاء على الأموال المحولة وتحصيلها، حيث أصبحت من أخطر الوسائل التي يستخدمها الجناة لتبييض أموالهم؛ وذلك لما توفره الوسائل التكنولوجية من سرعة، وبالتالي تمويل المصدر بأموال غير مشروعة ناتجة عن اتجار مخدرات أو غيرها، وذلك عن طريق إيداع مبالغ كبيرة ناتجة عن مصادر غير مشروعة لدى البنوك الخاصة، وثم تحويلها لصالح المستفيد، دون الكشف عن المصدر غير المشروع لهذه الأموال، وبالتالي إخفاء مصدر هذه الأموال عن البنوك، لكونها لن تبحث في كيفية كسب هذه الأموال، وخاصة أن عملية التحويل تتم بطريق سريعة ومعقدة في نفس الوقت؛ ولأن عملية التحويل الإلكتروني تقوم بنقل الأموال وليس معلومات عن مصدر هذه الأموال انطلاقاً من هذه النقطة التي يستغلها الجناة لتبييض الأموال بالطرق الإلكترونية، وجريمة تبييض الأموال التي تتم عن طريق التحويل الإلكتروني للأموال هي جريمة يمكن وصفها وصف مزدوج، فهي ذات شق يتعلق بتبييض الأموال، وهي جريمة متفق عليها في جميع دول العالم، والشق الثاني يتعلق بالوسيلة الحديثة التي تتعلق بالتقنية المتطورة التي استغلتها عن طريق التحويل الإلكتروني للأموال (ليندا، 2017). أغلب التشريعات ومنها التشريع الفلسطيني اعتبر تبييض الأموال يتم بطريقة التحويل الإلكتروني بعدة طرق وفقاً لنص المادة الخامسة من القرار بقانون رقم 39 لسنة 2022 بشأن غسيل الأموال و تمويل الإرهاب والتي نصت على "1 يعد مرتكباً لجريمة غسل الأموال كل من قام بأي فعل من الأفعال الآتية: أ- استبدال أو تحويل أو نقل الأموال من قبل أي شخص وهو يعلم بأن هذه الأموال تشكل متحصلات الجريمة لغرض إخفاء أو تمويه الأصل غير المشروع لهذه الأموال، أو لمساعدة شخص متورط في ارتكاب الجريمة الأصلية على الإفلات من التبعات القانونية المترتبة عليه....2. يستخلص العلم أو النية أو الهدف باعتبارهم عناصر أساسية للجريمة من الظروف الواقعية والموضوعية وعند إثبات أن الأموال هي متحصلات الجريمة فلا يشترط الحصول على إدانة الشخص في الجريمة الأصلية" (القرار

بقانون رقم 39 لسنة 2022 بشأن مكافحة غسيل الأموال وتمويل الإرهاب)، فهذه المادة تحدث عن الركن المادي وذلك بتوظيف الأموال غير المشروعة والتي تمت عليها عمليات التحويل الإلكتروني، وتوظيفها في أعمال مشروعة داخل الدولة أو خارجها، مثل مشاريع اقتصادية عن طريق المصارف والبنوك والشركات مع العلم أن الركن المادي لهذه الجريمة لا توقفه حدود جغرافية، ويتم بطريقة هادئة وسريعة (توريه، 2020) ويتم ذلك عن طريق القيام بعملية استبدال أو بعملية تحويل أو نقل الأموال من قبل أي شخص وهو يعلم أن هذه الأموال متصلة من جريمة معينة وقام بعملية التحويل بهدف إخفاء أو مساعدة شخص متلبس في جريمة معينة على الإفلات من العقاب، وبالتالي يرتكز الركن المادي في هذه الجريمة على فعل التحويل أو الاستبدال أو القيام بعملية النقل للأموال غير المشروعة، وبالتالي فإن هذه الجريمة يتصور وقوعها من خلال عمليات التحويل الإلكتروني للأموال وذلك من خلال قيام أحد الجناة بعد تحصيله مبلغ معين من المال (مبلغ متحصل من جريمة سرقة مثلاً) من أجل إخفاء مصدر هذه الاموال أو تهريبهاً بعيداً عن أعين السلطات يقوم بعملية تحويلها عبر البنوك وبذلك تتم الجريمة من خلال عمليات التحويل الإلكتروني، أما الركن المعنوي فيتمثل بالعلم والارادة (القصد العام) بحيث يكون لديه علم بأن مصدر هذه الأموال غير مشروع ومع ذلك اتجهت إرادته لتحويل هذه الأموال من خلال عمليات التحويل الإلكتروني للأموال .

وبتحليل نص هذه المادة أيضاً نجد أن المشرع الفلسطيني قد عالج موضوع تبييض الأموال بطريقة إلكترونية كون أن المشرع لم يحدد الوسيلة المستخدمة لتحويل هذه الأموال، فيعتبر الأمر واسع وغير مقيد (فالمطلق يؤخذ على إطلاقه مالم يحدده المشرع).

وفي قرار لمحكمة النقض الفلسطينية رقم 676 لسنة 2019 الصادر بتاريخ 28– يونيو، 2020 أن جريمة غسيل الأموال جريمة قائمة بذاتها ومستقلة وتقوم بشكل أساسي على التحصيل على أموال من مصادر

غير مشروعة دون الكشف عن هذه المصادر، ويمكن أن تتم بالطرق العادية أو من خلال وسائل حديثة مثل وسائل التحويل الإلكتروني للأموال (موقع مقام، 2019).

وفي قرار محكمة استئناف الجنايات رام الله رقم 419 لسنة 2016 الصادر بتاريخ 26 ديسمبر 2016 حيث جاء في مضمون القرار أن جريمة غسيل الأموال تكون مبنية على أموال متحصلة من جرائم عدة منها التهريب، وهذا ما أكدت عليه المادة الثالثة من القرار بقانون رقم 20 لسنة 2015 بشأن مكافحة غسل الأموال وتمويل الإرهاب ومن ضمن هذه الجرائم جريمة التهريب وفي البند العاشر التزوير والتزييف وقرصنة المنتجات أو البضائع وأكدت المحكمة أن تقرير الاشتباه مقدم مدير الوحدة المالية أن هناك جريمة تهريب حصلت وكذلك جريمة تزوير في الأوراق الرسمية ووضحت المحكمة في قرارها أيضاً أنه في حال تم إدخال أموال غير مشروعة لحسابات المشتبه به يصعب فصل هذه الأموال تقسيمها إلى مشروعة وغير مشروعة وكذلك وضحت المحكمة أن تقرير الاشتباه المقدم من مدير المالية له يصلح بما فيه ولرئيس الوحدة المالية صفة الضبط القضائي (موقع مقام ، 2016).

وفي قرار لمحكمة النقض الفلسطينية، طعن جزائي رقم 256 لسنة 2016 الصادر بتاريخ 2 إبريل 2017 وقد جاء في قرار محكمة النقض أن محكمة الدرجة الأولى أخطأت حين أدانت الطاعن بتهمة غسيل الأموال، لأنها بنت حكمها على بينة وهمية لا وجود لها من ناحية القانون، لأن شرط قيام جريمة غسيل الأموال هو أن يكون مصدر هذه الأموال مصدر غير مشروع، والنيابة بنت الاتهام على الشك وقد حددت المحكمة أيضاً أنه يجب أن يكون الركن المعنوي الذي يتمثل في علم الجاني أن مصدر هذه الأموال غير مشروع، علم مؤكد وليس على سبيل التخمين (موقع مقام، 2016).

وفي قرار آخر لابد من الإشارة إلى مبدأ قضائي استقرت عليه محكمة استئناف القدس رقم 2018/150، الصادر بتاريخ 27 سبتمبر 2018 جاء في مضمونه إجراء الحجز التحفظي على جميع أموال المستأنفين ورفع السرية وأكدت المحكمة في قرارها على نص المادة 33 من القرار بقانون رقم 20 لسنة 2015 بشأن

مكافحة غسيل الأموال وتمويل الإرهاب، على مراقبة الحسابات المصرفية وكذلك الوصول لشبكة الحاسوب وإخضاعها للمراقبة وتعقب الاتصالات، وكذلك يحق للمحكمة إلقاء الحجز التحفظي على جميع الأموال المرتبطة بجريمة غسيل الأموال أو تمويل الإرهاب دون تجزئة هذه الأموال إلى أموال مشروعة أو غير مشروعة (موقع مقام، 2018).

أما بالنسبة للتشريع الجزائري فقد اعتبر أن تبيض الأموال يتم بطريقة التحويل الإلكتروني وفقاً لنص المادة 2 من القانون الخاص بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال الجزائري والتي نصت على "أ) تحويل الأموال أو نقلها إلكترونياً، مع علم الفاعل أن مصدرها غير شرعي وبغرض إخفاء أو تمويل المصدر غير المشروع لها، أو بهدف مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تحصلت منها الأموال والإفلات من العقاب ب) إخفاء أو تمويل مصدر هذه الأموال أو مكانها أو طريقة التصرف فيها أو نقلها أو الالتزامات والحقوق المتعلقة فيها"، وبتحليل هذه المادة نجد أن القانون الجزائري كان متنبهاً لجرائم عمليات التحويل الإلكتروني للأموال، فقام بسن تشريعات حديثة تتناسب مع هذه الجرائم، وإضافة نص تشريعي خاص لجرائم الاعتداء على عملية التحويل الإلكتروني يتناسب مع طبيعتها ولم يسقطها على النص التقليدي، حيث أقر بجريمة تبييض الأموال التي تتم من خلال التحويل الإلكتروني، حيث اعتبر جريمة تبيض الأموال عبارة عن أفعال يكون الهدف منها إخفاء المصدر الأصلي للأموال التي يكون مصدرها غير مشروع أو إعطاء تبرير غير صحيح لهذه المصادر، بغض النظر عن الوسيلة المستخدمة أياً كانت، سواء من خلال استخدام تحويل الأموال أو استبدالها لغرض إخفاء أو تمويه مصدرها أو القيام بتلك الأموال غير مشروعة أو حيازتها أو استخدامها أو توظيفها لشراء أموال منقولة أو غير منقولة أو القيام بعمليات مالية، وبذلك نرى أن المشرع الجزائري قد أدخل جريمة تبييض الأموال التي تتم من خلال عملية التحويل الإلكترونية ضمن النص قانوني، وقد حدد الركن المعنوي لجريمة تبييض الأموال واعتبرها جريمة عمدية يلزم لقيامها تحقق القصد العام، ولابد لتحقق الركن المعنوي أن يكون الجاني لديه علم بأصل المال غير المشروع (دريس، 2016).

ثانياً: جريمة الاحتيال الإلكتروني

ويعرف الاحتيال الإلكتروني على أنه الاستيلاء غير المشروع للأموال دون وجه حق ويتم بطريق الخداع أو التحريف، وذلك من أجل الحصول على ربح غير مشروع وترتكب عن طريق نظام الحاسب الآلي، وذلك بإدخال معطيات للحاسب الآلي كمعلومات وهمية أو تعديل البرامج وذلك لتحويل مبالغ غير شرعية للجاني، ومن وسائل الاحتيال، التلاعب بالمعلومات والبيانات التي يتم إدخالها وإخراجها إلى أنظمة الحاسوب، وذلك من خلال تغيير البيانات سواء بحذف أو زيادة أو التلاعب البيانات التي يتم تحويلها عن بعد عن طريق النهايات الطرفية ،فيكفي أن يكون الجهاز الآلي متصل بوحده التشغيل المركزية عن طريق وصلات حتى يستطيع الدخول إلى المؤسسة وتحويل أموالها بطريقة غير مشروعة، ويشترط أن تؤدي هذه الأفعال إلى إيهام الجاني وإيقاعه بالغلط، أي تحقق النتيجة التي هي تسليم المال بسبب الفعل الذي قام به وذلك لكي لا تنقطع العلاقة السببية بينهما.

فيختلف الاحتيال بصورته التقليدية عن الاحتيال الإلكتروني في الأداة المستخدمة بارتكاب الجريمة ألا وهي الأجهزة الإلكترونية، ومحل السلوك الإجرامي من جهة أخرى، فالاحتيال الإلكتروني قد يرتكب من قبل أشخاص مصرح لهم بالدخول إلى النظام أي من داخل المؤسسة نفسها، حيث يكون هناك أشخاص لديهم السلطة للتعامل مع هذه المعلومات التي توجد في نظام الحاسوب يقوم بالتلاعب بهذه المعلومات وبياناتها وتحويلها إلى ربح غير مشروع، والاحتيال التقليدي يكون التسليم بطريقة مباشرة بين الجاني والمجني عليه ،وذلك بعكس الاحتيال الإلكتروني الذي يكون بطريقة غير مباشرة كالتسليم المادي وغير المادي، فالتسليم المادي يكون باستخدام البطاقات الائتمانية من قبل الجاني والاستيلاء على مال الغير، أما التسليم غير المادي يكون عن طريق التلاعب البيانات وتكنولوجيا المعلومات والأنظمة الخاصة به (المعايطة، 2012).

يتمثل الاحتيال الإلكتروني بتحويل أموال الغير من حساب إلى حساب آخر عن طريق التلاعب بالمدخلات والبيانات وتنصرف إرادته رغم علمه بأنها أفعال تدليسية ، فالتلاعب في نظم التحويل الإلكتروني للأموال يتم بعدة طرق أولاً التلاعب بالمكونات المادية وخطوط الاتصالات وتدمير البيانات، وثانياً استخدام برامج خاصة لتحويل أموال غير مشروعة، ثالثاً التلاعب في البيانات بغرض تنفيذ تحويل غير مشروع للأموال (الجبوري، 2014).

وحتى يتحقق الركن المادي يجب توافر ثلاث عناصر ألا وهي قيام الفعل المادي وحدوث النتيجة ووجود علاقة سببية التي تربط بينهما، فالفعل يكمن جوهرة في الغش والخداع والكذب؛ وذلك من أجل خداع المجني عليه من خلال استغلال الأجهزة الإلكترونية، فمجرد الكذب لا يكفي لتحقيق الركن المادي إنما لابد من وجود أفعال مادية حملت المجني عليه على تصديقه كأن يقوم بتصميم موقع إلكتروني وهمي وإظهار أنه شركة حقيقية والقيام بأنشطة ونشر صور؛ وذلك لدعم أكاذيبه وزرع الثقة في نفس الغير ثم يقوم بالاحتيال عليهم، أما بالنسبة للركن المعنوي في جريمة الاحتيال الإلكتروني فيشترط توافر القصد العام أي علم الجاني أنه يرتكب فعل من شأنه إيقاع المجني عليه في الفخ وذلك لتسليمه المال. (نصيرات، وآخرون، 2018)

وهناك نصوص خاصة تجرم هذا النوع من الجرائم ألا وهو الاحتيال الإلكتروني في التشريع الفلسطيني فجاء في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية في المادة 14 من هذا القرار على أن "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 اتخاذ 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 عن ثلاثة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانونياً، أو بكلتا العقوبتين"

(موقع مقام، 2018)، فاعتبرت هذه المادة أن الاحتيال قد يتم بطريقة إلكترونية كما قد يتم بطريقة تقليدية وذلك عن طريق اتخاذ الاسم الكاذب أو الصفة غير الصحيحة وذلك لتحويل الأموال إلكترونياً.

ونرى أن المشرع لم يغفل عن وضع نصوص تتلاءم مع تطور تكنولوجيا المعلومات والجرائم التي تنشأ عن استخدام الحاسب الآلي وتطبيقاته، إلا أنه قصر من ناحية تشديد العقوبة فجريمة الاحتيال التقليدية تكون العقوبة بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 5 إلى خمسين دينار، إلا أن العقوبة في الاحتيال الإلكتروني لا تقل عن سنة أو غرامة لا تزيد عن 3000 دينار أردني، وهذا العقوبة تعتبر غير رادعة بنظر الباحثة إذ يجب التشديد لمثل هذا النوع من الجرائم كما فعلت الدول الأخرى كالتشريع الإماراتي.

وجاء في قرار آخر لمحكمة النقض الفلسطينية في قرارها رقم 2021/418 حيث جاء في قرارها أن إيهام المجني عليه ودفعه لشراء أرض مقابل أن يتم دفع ثمن هذه الأرض وبعد تحويل المبلغ إلى الأردن لشراء هذه الأرض من أشخاص على صلة قرابة تفاجئ المجني عليه بوضع اسم آخر غير أسمه في الوكالة الدورية وبعد ذلك طلب المجني عليه من الجاني التنازل عن العقار إلا أنه كان يماطل في الأمر، وبناءً على ذلك حكمت المحكمة بلائحة إتهام حسب نص المادة 417 من قانون العقوبات التي تحدثت عن الاحتيال (موقع مقام، 2022).

جاء في التشريع الإماراتي التفريق بين الاحتيال الإلكتروني والاحتيال التقليدي، وذلك بموجب نص المادة 40 من قانون مكافحة الشائعات والجرائم الإلكترونية رقم 34 لسنة 2021 حيث نصت المادة على أنه "يعاقب بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن (250,000) مائتين وخمسين ألف درهم ولا تزيد عن(1000,000) مليون درهم، أو بإحدى هاتين العقوبتين، كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريق من الطرق الاحتيالية أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات" فكل من استولى على أموال الغير عن طريق الخداع وذلك

باستخدام وسيلة إلكترونية، فيتم إدراجه تحت مسمى جريمة الاحتيال الإلكتروني، أما النص التقليدي الذي تحدث عن الاحتيال بصورته التقليدية فنص في المادة 399 من قانون العقوبات الإماراتي رقم3 لسنة 1987 على أنه "يعاقب بالحبس أو بالغرامة كل من توصل إلى الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع هذا السند أو إلى إلغائه أو إتلافه أو تعديله، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ الاسم كاذب أو صفة غير صحيحة متى كان من شأن ذلك خداع المجني عليه وحمله على التسليم.....، ويعاقب على الشروع بالحبس مدة لا تجاوز سنتين أو بالغرامة التي لا تزيد على عشرين ألف درهم ويجوز عند الحكم على العائد بالحبس مدة سنة فأكثر وأن يحكم بالمراقبة مدة لا تزيد على سنتين ولا تجاوز مدة العقوبة المحكوم بها" (شبول، 2023).

وترى الباحثة أن قانون مكافحة الشائعات والجرائم الإلكترونية رقم 34 لسنة 2021 قد وضح جريمة الاحتيال المرتكبة بطريقة إلكترونية وشدد بالعقوبة، حيث نص على عقوبة أشد من حيث الحبس والغرامة لجريمة الاحتيال الإلكتروني، وكنا نتمنى على المشرع الفلسطيني وضع عقوبات مشددة تتلاءم مع طبيعة الجريمة المرتكبة، وذلك لمحاربة جريمة الاحتيال الإلكتروني، وأن يجعل ارتكابها بطريقة إلكترونية ظرفاً مشدداً للعقوبة لكي تتناسب مع السلوك الإجرامي، وذلك لتحقيق فكرة الردع في ارتكاب مثل هذا النوع من الجرائم، ويجب أن تكون الحماية الجنائية كافية لتستوعب الأفعال التي ترتكب في إطار الجرائم الإلكترونية.

ومن الأمثلة على الاحتيال الإلكتروني هو انتحال مواقع إلكترونية مطابقة للمؤسسة المالية التي يتعامل مع العميل، وتقوم هذه المؤسسة بإرسال رسائل إلى العميل على أنها المؤسسة المالية التي يتعامل معها، وذلك باتباع تعليمات الرسالة الموجهة له منها، وقد ينتحل الجاني اسم البنك أو شركات ومواقع التحويل ويرسل رابط معين للعميل لتعبئته وبمجرد فتحه يقوم بالإستلاء على الأموال، مثال ذلك أن هناك شخص يدعى ويليام جاكسون استلم رسالة على أنها من شركة PayPal وطلب منه في الرسالة تعبئة بياناته وإلا سوف

يتم إغلاق حسابه وأدخل جاكسون البيانات وانتهى الأمر به بسرقة أمواله، وهذه الطريقة تعتبر من صور الاحتيال، فيكون تسليم المال بناءً على الخداع الذي مارسه الجاني في حق المجني عليه.

فلو قام الجاني بالاحتيال على المجني عليه وإيهامه بطريقة معينة أنه بنك أو جهة رسمية ليرسل له الرقم السري أو الدخول إلى رابط معين للاستيلاء على أمواله فالمشرع السعودي اعتبر ذلك جريمة يعاقب عليها حتى لو لم تتم هذه الجريمة، حيث جاء في نص المادة 4 من قانون الجرائم المعلوماتية على أنه :"يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال ، أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :1. استيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند ، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة2. الوصول – دون مسوغ نظامي صحيح – إلى بيانات بنكية ، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات ، أو معلومات، أو أموال، أو ما تتيحه من خدمات"، لم يعرف المشرع السعودي الاحتيال الإلكتروني إنما اكتفى ببيان وسائله، فيتعرض للعقوبة كل من قام بالوصول لمعلومات أو بيانات بنكية دون مسوغ قانوني، وأيضاً عاقب على الشروع فمحاولة الاستيلاء على الأموال وفشلها لأي سبب كان يوقع على الجاني العقوبة، وذلك وفقاً لنص المادة 10 من ذات القانون حيث ينص على "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة" (عطاالله، 2024).

فنرى أن المشرع السعودي قد تنبه لنقطة مهمة ألا وهي الاستيلاء غير المشروع للأموال عن طريق الاحتيال الإلكتروني أو الوصول غير المصرح به للبيانات أو المعلومات فهذا يمثل جريمة الاحتيال الإلكتروني وفرض عليها عقوبة، فلم يكتفي بتجريم الفعل فقط بل امتد ليصل إلى الشروع بهذه الجرائم، وهذا في نظر الباحثة يعتبر تعمق في النصوص بطريقة ذكية لكي لا يسمح للجاني بالهروب من العقاب

سواء قام بإتمام فعله والحصول على الأموال، أم لم يستطع إتمام فعله لأي سبب من الأسباب، وهذا يعتبر مواكبة للتقدم التكنولوجي ولعدم تهرب الجاني بصورة أو بأخرى من العقاب.

وجاء المشرع العُماني بنص واضح وصريح على أن التلاعب في البيانات والمعلومات بهدف الاحتيال هو يمثل جريمة توجب العقاب، فنصت المادة 13 من قانون مكافحة جرائم تقنية المعلومات رقم 12 لسنة 2011 على أنه "يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من أدخل أو عدل أو غير أو أتلف أو شوه أو ألغي بيانات أو معلومات إلكترونية في نظام معلوماتي إلكتروني أو حجبها عنه أو تدخل في وظائفه أو أنظمة تشغيله أو عطل وسائل تقنية المعلومات أو البرامج أو المواقع الإلكترونية عمداً ودون وجه حق بقصد التحايل والتسبب في إلحاق الضرر بالمستفيدين أو المستخدمين لتحقيق مصلحة أو الحصول على منفعة لنفسه أو لغيره بطريقة غير مشروعة، فإذا كان النظام المعلوماتي خاصاً بجهة حكومية أو مصرف أو مؤسسة مالية تكون العقوبة السجن المؤقت مدة لا تقل عن ثلاث سنوات ولا تزيد على خمس عشرة سنة وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرين ألف ريال عماني"، فجرم المشرع العمُاني في هذه المادة التلاعب في البيانات سواء بإتلاف أو تعديل أو تعطيل البرامج والمواقع، وتتحقق الجريمة عن طريق رغبة الجاني لتحقيق ربح مادي بطريقة غير مشروعة، وبالتالي تحقيق خسارة مادية للمجني عليه، وتتم الجريمة عن طريق الدخول للحاسوب الآلي نفسه أو للبرامج الموجودة عليه، ومن ثم تقديم بيانات أو تنفيذ مشاريع لتحويل الأموال إلكترونياً، أو بهدف تحطيم برامج حاسب آلي أو يعد أو يمحو بعض هذه البيانات المخزنة على الحاسب الآلي من أجل الحصول على مال والقيام بتحويله لحساب الجاني، وتتم هذه الجريمة بعدة وسائل منها التلاعب بالبيانات الموجودة على الحاسب الآلي، مما يؤدي إلى القيام بعمليات تحويل للأموال من غير إرادة صاحبها أو قد يقوم الجاني بإعاقة وإفشال عملية تحويل للأموال، وذلك بهدف الدخول من قبل الجاني نفسه وتحويل هذه الأموال له، فإذا كان الاعتداء على بيانات حكومية أو مصرف أو مؤسسة مالية أي المؤسسات

المتخصصة بالتحويل الإلكتروني للأموال فهذا يعتبر ظرف مشدد للعقوبة المرتكبة (البلوشية، 2018)، أما بالنسبة للمشرع الفلسطيني فإذا حدث تلاعب في البيانات يتم تطبيق نص المادة 4 من القرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018 الذي نص على"1. كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا ارتكب الفعل المذكور في الفقرة (1) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3. 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. 4. إذا ارتكب الفعل المذكور في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً". (قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية)، فجاء في نص هذه المادة تجريم الدخول المتعمد بوسيلة إلكترونية إلى بيانات أو نظام إلكتروني وقد ترتكب من قبل أشخاص لديهم السلطة للتعامل مع هذه المعلومات التي توجد في نظام الحاسوب يقوم بالتلاعب بهذه المعلومات وبياناتها إلا أنهم تجاوزوا الصلاحية المعطاة لهم،_عن طريق حذف أو إضافة أو التعديل على البيانات، وتلاحظ الباحثة أن مشرعنا الفلسطيني لم يحدد الهدف من

الدخول التلاعب بالبيانات إنما اكتفى بتجريم الفعل الحاصل، فلابد من وجود تنظيم قانوني يغطي كافة صور الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال، حتى لا نكون أمام فجوة وقصور تشريعي يسمح لمرتكبي الجرائم بالإفلات من العقاب، فيعتبر أن هناك نقص من ناحية كافية الأحكام القانونية ذات الصلة، وذلك في تأمين الحماية اللازمة لوسائل التحويل الإلكتروني للأموال.

رابعاً: جريمة إساءة استخدام البطاقة خلال فترة انتهاء صلاحيتها.

يقوم الركن المادي في هذه الجريمة على قيام الجاني صاحب البطاقة بشراء ودفع ثمن سلع وخدمات إلكترونية رغم عدم توفر رصيد فيها أو انتهائه وتقع أيضاً بطريقة أخرى عن طريق قيامه بإجراء تحويل إلكتروني من رصيد شخص آخر لرصيده حتى يتمكن من دفع ثمن هذه السلع والخدمات التي أقدم على شرائها وقد اختلف الفقهاء في تكيف هذه الجريمة فالبعض كيفها على أنها:

أ. "جريمة سرقة والبعض الآخر كيفها على أنها جريمة نصب، ويقوم الركن المعنوي في هذه الجريمة على علم الشخص بأن رصيده في البطاقة قد انتهى واتجاه إرادته نحو الفعل وتحقيق النتيجة الجرمية التي تتمثل في دفع ثمن السلع والخدمات التي أقدم على شراءها حتى لو من حساب آخر.

ب. إساءة استخدام البطاقة بعد فترة صلاحيتها أو إلغاؤها وتقوم هذه الجريمة على الاستخدام الغير مشروع للبطاقة التي تم إلغاؤها من قبل البنك: يقوم الركن المادي في هذه الجريمة في حال قام البنك بإلغاء البطاقة وأخطر العميل بذلك فإنه عليه إعادة البطاقة للبنك فإذا قام العميل بسحب مبلغ من البطاقة يكون قد ارتكب جريمة خيانة الأمانة.

ج. الاستخدام غير المشروع للبطاقة المنتهية الصلاحية: يقع الركن المادي أيضاً لهذه الجريمة في حال انتهت صلاحية بطاقة الائتمان ولم يقوم صاحبها بإعادتها للبنك بل استمر في استخدامها وتحويل الأموال للتجار الذين تعامل معهم أو اشترى منهم السلع والخدمات ولكن هنا يقع التزام على التاجر

بالتأكد من مدة صلاحية البطاقة قبل استخدامها أما الركن المعنوي فيها فيقوم على العلم والارادة (غانم، 2019)."

نلاحظ أن أغلب التشريعات لم تأتي بنصوص خاصة لتجريم مثل هذه الأفعال، إنما إذا وقعت تطبق عليها النصوص التقليدية، إلا أننا نجد أن هناك من الدول من قامت بوضع نصوص خاصة بهذا النوع من الجرائم كسلطنة عُمان وذلك في قانون جرائم الحاسب الآلي، حيث جاء في نص المادة 276 مكرر أربعة أنه "يعاقب مدة لا تزيد عن ثلاث سنوات وغرامة لا تتجاوز 500 ريال كل من:"1. يستخدم البطاقة كوسيلة لوفاء مع علمه بعدم وجود رصيد لها 2. استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك" (حميد وآخرون، 2010)، أما بالنسبة لموقف مشرعنا العقابي نرى أنه لم يتطرق إلى هذا النوع من الجرائم إنما يطبق عليها النصوص التقليدية، ونتمنى على المشرع أن يأتي بنص يجرم مثل هذا النوع من الأفعال دون التوسعة في النص التقليدي أو أن يأتي بقانون يتناول به كل الأفعال التي ممكن أن تقع على عمليات التحويل الإلكتروني وهذا هو الأكمل والأفضل.

المطلب الثاني: قيام المسؤولية الجنائية في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

من أجل تطبيق أحكام قيام المسؤولية الجزائية على عمليات التحويل الإلكتروني للأموال لابد من تحقق جميع أركان الجريمة التي تتعلق بجرائم عمليات التحويل الإلكتروني للأموال، بحيث يتم ارتكاب الجريمة التي تحدث عنها القانون ضمن نصوص المواد الخاصة بعمليات التحويل الإلكتروني للأموال.

إن جرائم الاعتداء على عمليات التحويل الإلكتروني للأموال، مثلها مثل باقي الجرائم لابد من تحقق الأركان أساسية فيها وهي الركن المادي والمعنوي والركن الشرعي الذي يتمثل بالنص القانوني، وحتى يكون لدينا جريمة يجب أن يكون هناك لدينا فعل جرمي جرمه القانون ونص قانوني يجرم هذا الفعل، ففي البداية الركن المادي في جرائم الاعتداء على عمليات التحويل الإلكتروني للأموال يتمثل في الجانب المادي الظاهر الذي يشكل عمل تنفيذه لإيقاع الجريمة، وإخراج النوايا إلى الواقع العملي، والركن المادي

في جرائم عملية التحويل الإلكتروني يتمثل بالسلوك المادي الذي يهدف إلى الاستيلاء على الأموال ومن صور السلوك المادي لجرائم عملية التحويل الإلكتروني، اختراق مواقع مخصصة لعمليات التحويل الإلكتروني للأموال وتحويلها إلى الجاني وجاء في نص المادة 13 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية أن "1.كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن أو غرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بكلتا العقوبتين"، ومن صور الركن المادي أيضاً قيام الموظفين بتحويل مبالغ مالية لحساباتهم الخاصة من خلال الاستيلاء عليها من قبل حسابات العملاء، ويمكن أن يقوم الجانب المادي في ارتكاب هذه الجرائم من خلال وسائل مشروعة مثل أن يكون موظف يعمل لدى البنك، ويقوم بالاعتداء على هذه عمليات التحويل الإلكتروني الأموال وقد يستخدم وسائل غير مشروعة مثل استخدام برامج الاختراق لمواقع تابعة للشركات مالية أو بنوك وإجراء عملية تحويل لحساب الجاني، ويمكن أن يرتكب الجاني جريمة داخل بلد معين، فيقوم بتحويل الأموال الموجودة من حساب المجني عليه لحساب خاص به داخل المدينة نفسها أو داخل الدولة نفسها، ويمكن أن يقوم بإجراء هذه التحويلات لدولة أخرى مثل بريطانيا أو غيرها من الدول حتى يتمكن من السفر إلى هذه الدولة وسحب هذه الأموال وذلك من أجل إتمام الجريمة بعيداً عن ملاحقة السلطات (أمجد، 2017) ، ونصت المادة 27 من ذات القانون "كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار مستغلاً صلاحياته وسلطاته أثناء تأديته 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 القرار بقانون أثناء تأديته عمله أو بسببه أو سهل ذلك لغيره تزيد العقوبة بمقدار الثلثين" (موقع مقام، 2018)، أما بخصوص الركن المعنوي الذي يجب توفره حتى تقع جريمة الاعتداء على عمليات التحويل الإلكتروني للأموال فهو القصد العام، ولا يتصور وقوع هذه الجرائم عن طريق الخطأ أو الإهمال، فيكفي توفر القصد العام الذي يتمثل بالعلم والإرادة حيث يكون لديه علم أنه يرتكب جريمة اعتداء على عمليات التحويل الإلكتروني، وبالتالي هي جرائم عامة لا يتصور وقوعها عن

طريق الخطأ أو الإهمال، فيكون الجاني لديه القصد العام الذي يتمثل بالعلم والإرادة حيث يكون لديه علم أنه يرتكب جريمة اعتداء على عملية التحويل الإلكتروني الأموال، كذلك لابد أن يكون لديه الإرادة وتتجه إرادته نحو الاستيلاء على هذه الأموال، وهذه الجرائم لا تتطلب قصد خاص إنما يكفي لقيامها وجود الركن المادي والمعنوي ووجود العلاقة السببية والنتيجة الجرمية حتى يتم محاسبة الشخص على قيام هذه الجريمة.

إن قيام المسؤولية الجزائية في جرائم عمليات التحويل الإلكتروني للأموال لم تعد تقتصر على الأشخاص طبيعيين بل أصبح يمتد ويشمل الأشخاص المعنويين، وذلك تكريس لمبدأ المسؤولية الجزائية عن فعل الغير وخاصة أن هذه الجريمة لا تقل الخطورة عن الجرائم الواقعة على الأشخاص مثل جريمة القتل وغيرها وخاصة أن سلبياتها تمتد لتشمل المجتمع ككل، ومما يجب الإشارة إليه أن الركن المعنوي يضعف في جرائم عمليات التحويل الإلكتروني للأموال، وتقوم المسؤولية الجنائية في جرائم عمليات التحويل الإلكتروني للأموال على أساس تصرفات مجرمة مخالفة للقوانين التي تتعلق بتنظيم الجانب المالي في الدولة، فتقوم على مخالفة واضحة للقوانين المالية التي شرعتها الدولة من أجل تنظيم عمليات التحويل الإلكتروني للأموال سواء القوانين الخاصة بالبنوك أو عمليات التحويل الخاصة بالصرافة أو أي طريقة من طرق التحويل المعتمدة دولياً وقانونياً (ناصر، 2010).

ويمكن أن تقع المسؤولية الجنائية على الأشخاص المعنويين، كحالة إخلال المصرف بقواعد الالتزام بتقديم المعلومات، كأن يقدم معلومات يحميها السر المصرفي دون إذن صاحبها كأن يعطي معلومات عن الحوالات المالية التي يقوم بها العميل دون إذنه، وذهب المشرع الفرنسي في المادة 13/226 من قانون العقوبات "كشف معلومات لها صفة سرية بواسطة شخص يحوزها بحكم مركزه أو مهنته أو بسبب وظيفته أو مهمة مؤقته يعاقب الحبس لمدة سنة وبغرامة15,000 يورو"، وذلك لأن البنك يعتبر مؤتمن على أسرار عملائه، فعكس ذلك يعرضه للمسؤولية الجزائية، ونص قانون العقوبات العراقي رقم (111) لسنة1969

المعدل في المادة 123 "وقف الشخص المعنوي إذا ما ارتكب أحد ممثليه جناية أو جنحة، إذا ما ارتكب الجناية والجنحة أكثر من مرة فللمحكمة أن تأمر بحل الشخص المعنوي" ويستنتج من هذا النص أن جرائم الاعتداء على الأموال الخاصة بالعملاء بأي وسيلة كانت كأن يكون بإفشاء سر خاص يتعلق بأموال العملاء، سواء كان يتعلق بأمر تحويل أو غيره، فيعاقب على هذا الفعل وإذا تكرر ذلك الفعل الذي يشكل جنحة أو جناية من أحد ممثلي هذا الشخص المعنوي، فإن للمحكمة عن تأمر بحل الشخص المعنوي، أيضاً نصت في المادة 340 من ذات القانون "يعاقب بالسجن مدة لا تزيد على سبع سنوات كل موظف أو مكلف بخدمة عامة أحدث عمداً ضرراً بأموال الجهة التي يعمل فيها ويتصل فيها بحكم وظيفته أو بأموال الأشخاص المعهودة إليه" وإضافة إلى ذلك يعاقب الموظف الذي تعمد إحداث الضرر، فحدد المشرع العراقي هنا أنه يشترط لقيام المسؤولية أن يكون هناك قصد، فإذا تحقق القصد وقام بإحداث ضرر بأموال المؤسسة التي يعمل بها أو أموال عملائها تحت المسمى الوظيفي، فتقع عليه المسؤولية الجنائية (مسؤولية المصرف عن تقديم معلومات الإئتمان المالي، 2023).

وكان توجه المشرع المصري في جرائم عمليات التحويل الإلكتروني للأموال برفع العقوبة إذا كانت الجهة المجني عليها هي جهة من جهات الشخصية الاعتبارية العامة، ففرض عقوبة السجن بالإضافة إلى عقوبة الغرامة من 100 إلى 300 ألف جنيه، فيقوم الركن المادي في هذه الجريمة من خلال إنشاء موقع أو بريد إلكتروني أو حسابات وهمية ونسبُها إلى أشخاص سواء كانوا طبيعيين أو اعتبارين، بغض النظر عن الهدف أو الغاية من الإنشاء، (ياسر، 2021).

قرار محكمة التميز الأردنية رقم 1999/200 وقد صدر بتاريخ 1999/9/30الذي جاء في قرار المحكمة عن الضرر المعنوي الذي يلحق بالعميل جراء الخطأ في عملية التحويل الإلكتروني للأموال عبر المصارف، حيث يوجب الخطأ التعويض عن الضرر، ومثال ذلك قيام البنك بتنفيذ تعليمات لعملاء من

حساب لحساب مستفيدين آخرين دون علمه، ونتيجة لذلك ترتب خطأ مادي ومعنوي يتمثل في انتشار اسمه على الحوالات وهو لا يرغب بذلك (شقيرات، 2005)

وهناك مسؤولية تقع على الجهات المصدرة لشهادة التوثيق، وذلك إذا تم التحويل الإلكتروني وحصل هناك تزوير للتوقيع الإلكتروني، فيتم العودة للجهات التي قامت إصدار شهادة التوثيق، ويقصد بشهادة التوثيق حسب نص المادة ٢من قانون المعاملات الإلكترونية الأردني هي "الشهادة التي تصدر عن جهة مختصة مرخصة أو معتمدة لإثبات نسبة توقيع إلكتروني إلى شخص معين استناداً إلى إجراءات توثيق معتمدة" فإذا قامت هذه الجهات بإصدار شهادة توثيق دون التحقق من هوية الشخص مقدم الطلب، من أنه هو ذاته الذي سيتم إصدار شهادة باسمه، فيترتب على هذا التقصير إجراء عملية تحويل إلكتروني مزورة بناءً على شهادة التوثيق، ويستطيع البنك تعويض الضرر الذي لحق بالغير حسن نية، ثم الرجوع إلى الجهات التي قامت بإصدار مثل هذه الشهادة، ولا تقف المسؤولية هنا على المسؤولية المدنية إنما تمتد لتصبح مسؤولية جزائية فقد تتوافر في فعل مصدر أمر التحويل المصرفي الإلكتروني المزور وصف السرقة أو الاحتيال إذا استجمع الفعل أركان هذه الجريمة وهذا ما نصت عليه المادة 38 من قانون معاملات الإلكترونية الأردني على "أن ارتكاب أي فعل يشكل جريمة موجب التشريعات النافذة يعتبر مُجرّماً إن تم تنفيذه باستخدام وسيلة إلكترونية" وهذا يشمل السرقة أو الاحتيال الواقع على التحويل الإلكتروني المزور (ذوابة، 2006).

فيستنتج من الحديث السابق أن لقيام المسؤولية يشترط وقوع الفعل المجرم ووقوع النتيجة الجرمية ، ولكن المشرع السعودي جاء بنص يحاسب على الشروع في الجريمة أيضاً، فإذا قام الجاني بالاحتيال على المجني عليه وإيهامه بطريقة معينة أنه جهة رسمية أو بنك، وذلك ليرسل له الرقم السري الخاص به أو إدخاله على رابط بهدف الاستيلاء على أمواله، فالمشرع السعودي اعتبر هذه جريمة توجب العقوبة بناء على نص المادة 4 من قانون الجرائم المعلوماتية فنصت على :"يعاقب بالسجن مدة لا تزيد عن ثلاث

سنوات وبغرامة لا تزيد عن مليوني ريال ، أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :1. استيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند ، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة2. الوصول – دون مسوغ نظامي صحيح – إلى بيانات بنكية ، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات ، أو معلومات، أو أموال، أو ما تتيحه من خدمات"، وأيضاً عاقب على الشروع فمحاولة الاستيلاء على الأموال وفشلها لأي سبب كان يوقع على الجاني بالعقوبة وذلك وفقاً لنص المادة 10 من ذات القانون حيث ينص على "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة" (عطاالله، 2024).

الفصل الثاني

القواعد الإجرائية لحماية عمليات التحويل الإلكتروني للأموال.

تعتبر عمليات التحويل الإلكتروني للأموال من أفضل طرق تمويل التجارة الخارجية، وإتمام البيوع الإلكترونية ودفع ثمنها عن طريق آلية التحويل الإلكتروني للأموال، ومع استغلال الجناة لهذه الوسائل تنبهت الدول، لاتخاذ إجراءات ضرورية لمكافحة استغلال هذه الوسائل في ارتكاب الجرائم، فقد قامت بعض الدول بسن قوانين خاصة بالتحويل الإلكتروني للأموال كالولايات المتحدة الأمريكية، وهناك من الدول من لم تقم بسن قوانين خاصة إنما اعتمدت على القواعد العامة سواء قانون العقوبات أو قانون الإجراءات الجزائية أو قانون الجرائم الإلكترونية كما فعل المشرع لدينا (ليندة، 2017).

وقد تنشأ عن عمليات التحويل الإلكتروني للأموال، سواء عن طريق البنوك أو عن طريق شركات معتمدة لهذا المجال أو عن طريق بطاقات الائتمان وغيرها من الطرق التي ذكرتهم الباحثة في بداية الدراسة، بعض من الجرائم والمنازعات، وبالتالي لحل هذه المنازعات وإيقاف المجرمين من استغلال هذه المجالات سوف نكون بحاجة للتوجه للقضاء، ولذلك لابد من تحديد القضاء المختص في هذا المجال.

ولتحديد المحكمة المختصة بنظر الجرائم التي تقع على عمليات التحويل الإلكتروني للأموال، فإنه ينظر إلى طبيعة هذه الجريمة، ولأنه لا يوجد قانون خاص يتم تقريبها للنصوص التجريمية السارية في فلسطين، سواء كانت أقرب لجريمة نصب واحتيال حسب قانون العقوبات الساري في فلسطين رقم 16 لسنة 1960 أو السرقة ويمكن تقريبها أيضاً إلى النصوص التجريمية في قانون الجرائم الإلكترونية رقم 10 لسنة 2018 وتعديلاته، وبالتالي يتم تحديد المحكمة المختصة حسب كل جريمة (شقيرات، 2005).

أما في حال كانت الجريمة متعددة الأطراف، أي تتعلق بأكثر من طرف متعدد الجنسية، وخاصة أن هذه الجرائم في أغلب الأحيان يدخل فيها طرف أجنبي، ومثال ذلك أن يتم الجاني جريمته بتحويل المبالغ المالية لخارج البلاد، أو قيام الجاني وهو يعمل لدى فرع بنك معين بإجراء عملية تحويل بنكي لفرع آخر

خارج البلاد، ومن ثم يدخل طرف أجنبي لاستلام المبلغ، فهنا تثور مشكلة تنازع الاختصاص القضائي، وفي هذه الحالة يكون محل الجاني والمجني عليه ومكان ارتكاب الجريمة محل اختصاص، ولكن الدولة التي تبدأ بإجراءات المحاكمة هي تكون صاحبة الاختصاص في نظر الدعوى وإكمال اجراءاتها، وفي هذا الدراسة لن تتطرق الباحثة للاختصاص الدولي لهذه الجرائم لأنه ليس موضوع الرسالة، بل سوف تبحث في الاختصاص القضائي داخل الدولة نفسها، وما هي الحماية الإجرائية لعمليات التحويل الإلكتروني للأموال (عرب، 2021).

وسوف تقوم الباحثة في هذا الفصل بالحديث عن إجراءات التتبع والملاحقة الخاصة بالجرائم الواقعة على عمليات التحويل الإلكتروني للأموال وذلك في المبحث الأول، ثم التطرق إلى الإجراءات الوقائية الخاصة بمكافحة الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال في المبحث الثاني.

المبحث الأول: إجراءات التتبع والملاحقة الخاصة بالجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

باعتبار جرائم عمليات التحويل الإلكتروني للأموال أصبحت ترتكب بطرق حديثة إلكترونية، فإن ملاحقتها وجمع الاستدلال فيها يختلف عن الجرائم التقليدية، فهي أصعب إلى حدٍ ما من إجراءات جمع الأدلة التي تتعلق بالجرائم التقليدية؛ وذلك نتيجة الطبيعة الخاصة التي ترتكب فيها جرائم عمليات التحويل الإلكتروني للأموال، فهذا يزيد العبء على الدولة من أجل توفير حماية خاصة للأفراد من أي اعتداء عليها، ومن جهة أخرى يجب على الدولة توفير أجهزة مختصة لديها القدرة على كشف الجريمة، وملاحقتها وإحراز الدليل من أجل إثبات الجريمة أمام القضاء، وبعدها إيقاع العقوبة المناسبة على الجاني، وباعتبار أن الدراسة ركزت على الوضع في فلسطين، وكيفية ملاحقة جرائم عمليات التحويل الإلكتروني للأموال، وعليه قامت الباحثة بتقسيم هذا المبحث إلى مطلبين، تناول المطلب الأول إجراءات الضبط وجمع الاستدلالات الخاصة في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال، أما المطلب الثاني تحدث عن إجراءات التحقيق النهائي الخاصة في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

المطلب الأول: إجراءات الضبط وجمع الاستدلالات الخاصة في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

إن التحقيق في جرائم الإلكترونية وكيفية الضبط الإلكتروني واختلافها عن ما هو معتاد، يعتبر واجهة جديدة ومستحدثة، ويعتبر أيضاً من المواضيع القانونية المهمة؛ وذلك بسبب التطور الحاصل في ارتكاب الجريمة، فهناك اختلاف عن الإجراءات المعتادة، لأن الجرائم أصبحت ترتكب بطريقة إلكترونية فأصبح الضبط الملاحقة والتفتيش وجمع الاستدلالات يختلف عن ما هو معتاد (السوفي، 2017).

ولبيان ذلك وتوضيحه قامت الباحثة بتقسيم المطلب إلى ثلاثة فروع وفق الآتي:-

الفرع الأول: إجراءات الضبط وجمع الاستدلالات في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

الفرع الثاني: إجراءات التفتيش في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

الفرع الثالث: إجراءات التحقيق في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

الفرع الأول: إجراءات الضبط وجمع الاستدلالات في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

الأجهزة المختصة بالضبط القضائي:-يتولى مأموري الضبط القضائي الاستقصاء والبحث والتفتيش وجمع الاستدلالات التي يستلزم جمعها لضرورة التحقيق، وبخصوص الضبط في عمليات التحويل الإلكتروني فهناك وحدة خاصة متخصصة في الجرائم الإلكترونية، وهي وحدة الجرائم الإلكترونية والتي تم إنشاؤها في سنة 2013 وهي وحدة تابعة للمباحث العامة، وتم إنشاءها من أجل مواجهة التحديات التي تواجه السلطة في الجرائم التي يتم ارتكابها بوسائل إلكترونية، مثل جرائم عمليات التحويل الإلكتروني للأموال، وتأتي دور هذه الوحدة للكشف عن هذه الجرائم وتقديم الجناة للقضاء، وتسعى هذه الوحدة أيضاً إلى توفير الأدلة الازمة لإثبات الجرائم الإلكترونية من أجل استخدامها لإدانة الجناة وإعداد محضر الاستدلال على مستوى

الضبط القضائي، وهذه الوحدة لديها كادر فنيين متخصصين في هذا المجال للتعامل مع الأدلة الرقمية وفحصها وإعدادها كدليل يصلح تقديمه في الإدانة، وفي واقع الحال نرى أن هذه الوحدة حققت نجاح كبير على الأراضي الفلسطينية، بدليل أن في تاريخ 2015 تم تحويل 502 قضية أُنجز منها 223 و 248 قيد المتابعة و31 تعطلت (ربايعة، 2016).

ومن هذه الإجراءات التي يقوم بها مأموري الضبط القضائي حيث نصت المادة 22 من قانون الإجراءات الجزائية على أن مهام مأموري الضبط القضائي "1.قبول البلاغات والشكاوي التي ترد إليهم بشأن الجرائم وعرضها دون تأخير على النيابة العامة2.إجراء الكشف والمعاينة والحصول على إيضاحات اللازمة لتسهيل التحقيق والاستعانة بالخبراء المختصين والشهود دون حلف يمين3. اتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة 4. إثبات جميع الإجراءات التي يقومون بها في محاضر رسمية بعد توقيعها منهم ومن المعنيين بها" أنه في مرحلة جمع الاستدلال يقوم مأموري الضبط القضائي بقبول الشكاوي والبلاغات التي تأتي إليهم بخصوص هذه الجرائم وعرضها على النيابة العامة، ولابد أيضاً من الذهاب لمسرح الجريمة وذلك من أجل الحفاظ على الأدلة ومنع العبث بها وتوثيق وكتابة كافة التفاصيل المتعلقة بجهاز الحاسوب، مثال ما إذا كان مفتوحاً أم مغلق أو كان متصل بالإنترنت أو غير متصل به، وتحديد هوية جهاز الحاسوب والأجهزة الأخرى المتصلة به التي عثر عليها في مسرح الجريمة، وتحديد نوع أجهزة التخزين الموجودة في مسرح الجريمة، ولابد أيضاً من تصوير مسرح الجريمة، وحفظ الوثائق المطبوعة والأدلة الرقمية الموجودة في المسرح والأجهزة كذلك، والعمل على استرجاع جميع الوثائق التي تم مسحها ومن ثم نقل الأدلة التي تم ضبطها، وهذه الأعمال جميعها تحتاج إلى خبراء في هذا المجال، فيمكن الاستعانة بالخبراء والشهود دون تحليف اليمين (الباقي، 2018).

ويتم جمع الاستدلالات في الجرائم الإلكترونية عن طريق أجهزة الحاسوب والإنترنت وذلك من أجل الحصول على المعلومات اللازمة فتعتبر هذه المرحلة هي مرحلة لجمع البيانات والمعلومات الخاصة بهذه

الجرائم، أيضاً، ومن الإجراءات التي تتعلق بالجرائم التقليدية أيضاً، أنه لابد من تثبيت الإجراءات التي يقومون بها في محضر رسمي بعد توقيعه، وفي حال كانت الجريمة إلكترونية فأنه في هذه الحال يتم اتخاذ إجراءات جمع الاستدلال التي تخص الجريمة الإلكترونية وخصوصيتها، فيمكن لرجال الشرطة التوجه للخبراء المختصين إلكترونياً في هذا المجال والاستعانة بهم من أجل المحافظة على الدليل ومن أجل الاستفادة من خبراتهم في كشف الجريمة ومعرفة الحقيقة وعدم ضياع الأدلة وذلك لمعرفته في مجال تقنية المعلومات فجاء في قانون الإجراءات الجزائية رقم 3 لسنة 2001 في المادة 64 على جواز الاستعانة بالخبراء فنصت على "يستعين وكيل النيابة بالطبيب المختص وغيره من الخبراء لإثبات حالة الجريمة المرتكبة ويقوم الطبيب المنتدب لذلك وغيره من الخبراء باتخاذ الإجراءات اللازمة تحت إشراف الجهة المختصة بالتحقيق وللمحقق الحضور أثناء مباشرة أعمال الخبراء إذا قدَر أن مصلحة التحقيق تقتضي ذلك" فأجاز القانون الاستعانة بالخبراء من قبل وكيل النيابة العامة إذا اقتضت المصلحة ذلك، فمراحل جمع الاستدلال في الجرائم الإلكترونية تتم عبر الإنترنت وأجهزة الحاسوب لضبط جميع الجرائم التي تم ارتكابها بواسطة الكمبيوتر أو الأجهزة الإلكترونية الحديثة، وهنا لابد من الإشارة إلى أنه على الدولة تدريب كوادرها ليستطيعوا التعامل مع الجرائم الإلكترونية، وإلا سوف نخسر عنصر مهم في إثبات الدعوى وهو الدليل الإلكتروني، فيلزم الاستعانة برجال من الشرطة، يكونوا ذات اختصاص ليستطيعوا التعامل مع الجريمة الإلكترونية، والاحتفاظ بالأدلة بطريقة معينة خاصة بالوحدة الإلكترونية حتى لا يضيع الدليل وذلك لدقته (جامعة النجاح الوطنية، 2017).

ويقصد بالضبط الإلكتروني: هو وضع اليد على المكونات المادية المخزن بها البيانات الإلكترونية، والتي تتصل بالجريمة وتفيد في كشف الحقيقة (نجيب، 2018).

ونظم المشرع الفلسطيني في قانون الجرائم الإلكترونية في المادة 3/23 موضوع ضبط الأدلة، حيث جاء أنه "إذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري

الضبط القضائي تنظيم محضر المضبوطات وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها"، حيث جاء في هذا النص إذا عثر مأموري الضبط القضائي أثناء التفتيش على أدوات وأجهزة لها علاقة بالجريمة أن يقوم بإعداد محضر في هذه المضبوطات وعرضها على النيابة، وأن الضبط يقع على الأجهزة والأدوات المتصلة بالجريمة ، وهي تعتبر من الأدلة المادية ويتم ارتكابها بواسطة الحاسوب أو الأجهزة الإلكترونية، ويطبق عليها قواعد الضبط العامة كما في الجرائم التقليدية وذلك لأن الضبط يكون على شيء حسي، أما ضبط الأدلة غير المادية وهي الأدلة الرقمية أي المعلومات المخزنة في أجهزة الحاسوب وتختلف عن الضبط في الجرائم التقليدية ، حيث أن الضبط يكون على معلومات موجودة في الجهاز الآلي، أما الثانية يكون محل الضبط الأداة المستخدمة في الجريمة كما في السلاح في جريمة القتل (بغدادي، 2018).

ولا بد من الإشارة إلى أنه يتم جمع الدليل الإلكتروني المتحصل من جرائم عمليات التحويل الإلكتروني للأموال من خلال مأموري الضبط المتخصصين، وهناك عدة طرق ومراحل لابد أن يتبعها مأمور الضبط القضائي والتي تبدأ بمرحلة توثيق الدليل الإلكتروني وتأمينه، وهي مرحلة دقيقة ومهمة، ومن هذه الطرق هي استخدام برامج من أجل التوثيق، وممكن أن يتم استخدام التصوير أو تسجيل الفيديو في توثيق الدليل، وفي بعض الأحيان لابد من أن يكون هناك شهود على عملية التوثيق، ولا بد من عدم إهمال أي عنصر من عناصر الدليل ، وعلى مأمور الضبط أن يبين البرامج التي استخدمها في جمع الأدلة مثلا كود وخوارزمية معينة والتي تنتج من الدليل الرقمي وتدوين ذلك في المحضر أو التقرير الفني الذي قام بإعداده، وفي حال كان الدليل يتعلق بخصوصية أفراد معينين لابد من مراعاة القوانين التي تتعلق بحفظ خصوصية الأفراد (حمادي، 2021).

ونصت المادة 33 من ذات القانون على أن "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 الحقيقة3. 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 المعلومات4. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها"، ضبط الدليل في هذه الجرائم يحتاج إلى أجهزة وشبكات خاصة من أجل جمع الأدلة التي تكون عبارة عن نبضات كهربائية ومغناطيسية، بحيث يتم استخراج هذه الأدلة من خلال الحاسب الآلي، وكذلك يتم البحث عن هذه الأدلة من خلال شبكات الاتصال، أيضاً وفي هذه الجرائم التي تعتمد بشكل كبير على الوسائل الإلكترونية في عمليات التحويل يستخدم المختصين بجمع الأدلة المتحصلة من هذه الجرائم أجهزة تعمل على تحويل هذه الأدلة من أدلة لا ترى بالعين المجردة إلى أدلة يمكن رؤيتها وتقديمها كدليل للإدانة، وذلك بتحويل النبضات والكهرباء أو النبضات المغناطيسية إلى معلومات وبيانات تتعلق بالجريمة أي يتم كشف أوامر التحويل التي أجراها الجناة لإجراء عمليات تحويل إلكتروني تتعلق بالجرائم التي ارتكبوها (ماهر،، 2022)، ومن الأمور المهمة التي يجب الانتباه إليها بموضوع الأدلة الجنائية الإلكترونية أن النسخة الأصلية للدليل الإلكتروني لا يتم فحصها بل يتم عمل نسخة طبق الأصل عنها، ويجري الفحص على النسخة وليس على الأصل، فيختلف الضبط هنا عن الضبط التقليدي، حيث يتم التعامل مع هذا الدليل من خلال استخراجه من القطع الصلبة والتي يتكون منها الحاسب الآلي، وفي جرائم عمليات التحويل الإلكتروني للأموال يكون هناك صعوبة باستخراج الدليل في هذه الجرائم بسبب التطور بشكل كبير، حيث يتم التعامل مع بيانات إلكترونية يتم تداولها بصورة إلكترونية وقد يكون ثابت أو متحرك مثل أن يكون على شكل صورة وقد يكون تسجيل سمعي أو قد يكون الدليل مخزن على البريد الإلكتروني، وبالتالي لابد من توفير أجهزة خاصة وكذلك لابد من توفير أنظمة برمجية حاسوبية خاصة لهذه الأدلة (لميزا، 2023)، وإذا كان هناك استحالة من إجراء الضبط أو التحفظ يتم استخدام برامج وأدوات خاصة لحفظ الدليل من الوصول له والنفاذ إلى البيانات المخزنة به، ونصت الفقرة 33/5 "تتخذ الاحتياطات

الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها" الدليل الرقمي هو في العادة عبارة عن ملف يوجد بداخله بيانات رقمية تعطي مظهر معلوماتي محدد غير قابل للتحويل إلى مظهر آخر إلا عن طريق إجراء تعديلات رقمية في البيانات المذكورة، فالتحفظ على الدليل قد يكون داخل الحاسب الآلي، أو خارج الحاسب الآلي علىCD أما حفظها خارج الحاسب الآلي، فلابد من التنبه لموضوع آلية الحفظ والتخزين، وذلك لعدم ضياع الأدلة وفقدانها، حيث وجد العالم فيكتور كاردينيس أن هناك نوع من الفطريات يتغذى على الإسطوانات المدمجة وأنه يجب حفظ هذه الاسطوانات بمكان بارد وجاف لتثبيط قدرة الفطريات على النمو فيجب إدراك هذا الأمر والأخذ به حتى لا يتم خسارة الأدلة (إبراهيم، 2018).

ونصت الفقرة 6/33 "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"، ونظم المشرع طرق حفظ الدليل وذلك عن طريق إعداد قائمة المضبوطات وذلك بحضور المتهم إذا أمكن، ويجب حفظه حسب الحالة في ظرف أو مغلف مختوم، ويتم كتابة تاريخ وساعة التحفظ وعدد محاضر القضية.

وترى الباحثة أنه يجب تأمين الدليل وذلك لأن الأدلة حساسة فقد تكون عرضة للأتلاف، فيجب حفظها بطريقة معينة وفي أماكن خاصة لحفظ هذا النوع من الأدلة، كونها تختلف عن الأدلة المادية في الجرائم التقليدية، ونظراً لغياب الخبرة الكافية في حفظ الأدلة، فنرى ضرورة الاستعانة بخبراء خاصين في حفظ الأدلة وذلك لعدم ضياع الدليل.

وبعد إجراء مقابلة مع موظفي النيابة العامة وسؤالهم عن كيفية الضبط وجمع الاستدلالات في هذا الموضوع وجدت الباحثة أنه في الواقع العملي الفلسطيني يتم جمع المعلومات في هذه الجرائم إلكترونياً، وذلك عن طريق مخاطبة شركة الاتصالات الفلسطينية وشركة جوال وشركة أوريدو، وذلك عن طريق القسم

المتخصص بالشرطة أو النيابة بالعامة، وذلك لتزويد الجهة الطالبة بكافة المعلومات المتعلقة به (IB) أو التطبيق الإلكتروني أو وسيلة التواصل الإلكترونية لمعرفة صاحب (IB) أو صاحب رقم الهاتف الذي ارتكب الفعل المجرم، وبعد معرفة اسم الفاعل وتوثيق ذلك بتقارير فنية من شركة الاتصالات أو شركة جوال أو شركة أوريدو، يتم إحالة الملف مرفق بشكوى المشتكي من قسم جمع الاستدلالات وهو قسم الجرائم الإلكترونية في الشرطة وهو الذي يتابع ويعد محاضر الاستدلال بالتنسيق مع دائرة الاستدلالات القانونية بالشرطة، ويتم تحويل الملف إلى النيابة العامة وإذا رأت النيابة العامة ضرورة استيفاء بعض المعلومات لغايات تعزيز البيانات في الملف أو التوسع في التحقيقات، فإنه يتم مخاطبة نيابة مكافحة الجرائم الإلكترونية لغايات استكمال أو الحصول على معلومات المطلوبة في التحقيق مثل ضبط الهاتف الخلوي أو إرسال هذا الهاتف إلى وحدة الجرائم الإلكترونية لغاية النفاذ إلى الهاتف الخلوي واستخراج المعلومات المطلوبة منه سواء كانت على تطبيق Messenger أو Facebook وهذا ينطبق أيضا على أي جهاز إلكتروني، وذلك بناءً على قرار من وكيل النيابة المختص، وفي بعض الجرائم قد يكون هناك تقاطع بين عمل نيابة مكافحة الجرائم الاقتصادية ونيابة مكافحة الجرائم الإلكترونية فعندما يكون هناك تقاطع بين هاتين النيابتين، فيتم التعاون بينها، مثال ذلك وقوع جريمة مثل استخدام الشبكة الإلكترونية لترويج بضاعة معينة غير مرخصة وهذه تعتبر جريمة اقتصادية إلكترونية، فيتم التعاون فيها بين وكيل نيابة الجرائم الاقتصادية ونيابة مكافحة الجرائم الإلكترونية، ثم تعود إلى نيابة مكافحة الجرائم الاقتصادية لاستكمال الإجراءات القانونية، وأيضاً بالنسبة لخصوصية هذا النوع من الجرائم، حيث تعتبر هذه الجريمة من الجرائم المتطورة وذلك بفعل تطور التكنولوجيا المستمر، حيث أن المجرمون دائماً ما يتبعون وسائل جديدة لارتكاب الجريمة وذلك للإفلات من العقاب، ولذلك يقتضي على الجهات التشريعية في الدولة دائماً مواكبة هذه التطورات في الجريمة الإلكترونية عن طريق تحديث التشريعات المتعلقة بهذا الخصوص، والإثبات في هذه الجرائم صعب نوعا ما "1. لأنها تعتمد بالأساس على البيانات الكتابية وليس البيانات الشفوية 2. صعوبة الحصول على المعلومات الخاصة إذا كان المتهم يستخدم شبكة اتصالات غير

فلسطينية مثل الشبكات "الإسرائيلية" وذلك على الصعيد المحلي، فيصبح هناك نوع من التقاطع مع شركات أوريدو وشركة جوال وشركة الاتصالات لمعرفة رقم السيلكوم وصاحبه الذي قام بارتكاب الفعل، ما إذا كان اتصل بأحد المشتركين بهذه الشركات، فيتم استدعاء الأشخاص لسماع شهاداتهم لمعرفة من صاحب رقم السيلكوم الذي اتصل عليه الشخص المطلوب، أما على الصعيد الدولي يتم عن طريق نيابة قضائية دولية وهذا يخضع لمبدأ التعاون بالمثل بين الدول وما إذا كان هناك اتفاقيات ثنائية دولية بهذا الخصوص (شاهين، 2024).

الفرع الثاني: إجراءات التفتيش في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

يعد التفتيش أحد أهم الإجراءات الخاصة بالتحقيق الجنائي، والتي تهدف إلى ضبط الأدلة وكشف الحقيقة، وقد ينطوي على المساس بحقوق المتهم في سرية حياته الخاصة ولهذا السبب أحاطه المشرع بعدة ضمانات. (خلف، 2017)

إن التفتيش في الجرائم الإلكترونية يختلف عن التفتيش العادي، فالتفتيش الإلكتروني يكون لضبط وسائل تكنولوجيا المعلومات التي استخدمت لارتكاب الجريمة، فيجب الحصول على إذن خاص من النيابة للنفاذ المباشر لوسائل تكنولوجيا المعلومات وذلك للحصول على المعلومات المطلوبة، وهذا ما نص عليه قانون الجرائم الإلكترونية رقم 10 لسنة 2018 في المادة 32/ 4 "لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينوا بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا معلومات وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات" ، وعليه فإنه يجب أن يكون الإذن واضح وصريح وذلك بتحديد الوسيلة الإلكترونية المراد تفتيشها وهذا نصت عليه المادة 2/32"يجب أن يكون أمر التفتيش مسبباً ومحدداً ويجوز تجديده ما دامت مبررات هذا الإجراء قائمة"، فيعتبر تحديد محل التفتيش من أول الأعمال التحضيرية الخاصة بالتفتيش، وذلك بتحديد وسائل الإلكترونية المرتكبة في الجريمة وتحديد مكانها هذا يعتبر من أهم المعلومات اللازمة لإجراء التفتيش (عموري، 2018)، وفي الواقع العملي الفلسطيني يتم جمع المعلومات في هذه الجرائم إلكترونياً، وذلك عن طريق مخاطبة شركة الاتصالات

الفلسطينية أو شركة جوال أو شركة أوريدو، وذلك عن طريق قسم المتخصص بالشرطة أو النيابة العامة ، وذلك لتزويد الجهة الطالبة بكافة المعلومات المتعلقة ب (IB)، أو التطبيق الإلكتروني أو وسيلة التواصل الإلكتروني لمعرفة صاحب ال (IB)، أو صاحب رقم الهاتف الذي ارتكب الفعل المجرم، وذلك بمعرفة اسم الفاعل وتوثيق ذلك بتقارير فنية من شركة الاتصالات أو شركة جوال أو شركة أوريدو، حيث عرف قانون الجرائم الإلكترونية في المادة الأولى معلومات المشترك بأنها "أي معلومات موجودة لدى مزود الخدمة المتعلقة بمشتركين الخدمات حول نوع خدمة الاتصالات المستخدمة وهوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه أو معلومات الدفع المتوفرة بناء على اتفاق، أو تركيب الخدمة أو أي معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة"، ونصت المادة 31 من ذات القانون على أن "يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي : "1 تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة ، بناءً على طلب النيابة أو المحكمة المختصة .....3. الاحتفاظ بمعلومات المشترك مدة لا تقل عن ثلاث سنوات 4. التعاون ومساعدة الجهات المختصة...." وعليه يعتبر المشرع قد ألزم مقدمي هذه الخدمات بتقديم المعلومات اللازمة والمطلوبة للجهات المختصة ومساعدتهم والتعاون معهم في جمع المعلومات المطلوبة ، وألزم المشرع أيضاً مزودي الخدمة بحفظ المعلومات الخاصة بالمشترك مدة لا تقل عن 3 سنوات (شاهين، 2024).

ونصت المادة 1/50من قانون الإجراءات الجزائية الفلسطيني "لا يجوز التفتيش إلا عن الأشياء الخاصة بالجريمة الجاري التحقيق بشأنها..."، ونصت المادة 1/32من القرار بقانون بشأن الجرائم الإلكترونية رقم 10 لسنة 2018على أن "للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة"، وعليه فيجوز التفتيش بكل ما هو متعلق بالجريمة، فكلمة (وسائل تكنولوجيا المعلومات) تعطي معنى واسع لتستوعب المكونات المادية والمعنوية الخاصة بالوسائل الإلكترونية المستخدمة في ارتكاب الجريمة، إذاً فيشترط في التفتيش عن الأدلة أن يكون خاص بالأدلة المتعلقة بالجريمة وهو السبب والغاية من التفتيش، فجاء في كلمة (ذات صلة في الجريمة)

أنه لا يجوز تجاوز التفتيش إلى ما دون ذلك (2018)، فالتفتيش قد يقع على مكونات مادية أو غير مادية، فالمكونات المادية هي عبارة عن مواد حسية والتي لها صلة في الجريمة وتوجد بمكان الحدث، وهي كشاشة الكمبيوتر والأسلاك المتصلة بها ووحدة التخزين الكيبورد وغيرها من المواد الحسية، أما بالنسبة للمكونات الغير المادية فهي عبارة عن أنظمة التشغيل وبرامج التشغيل لغات البرمجة والتي يطلق عليها أيضاً اسم المكونات المعنوية (علي، 2018)، وترى الباحثة أنه لا يوجد أي إشكالية في تفتيش هذه المكونات سواء كانت مادية أو معنوية إذا تمت وفق إجراءات قانونية صحيحة، وذلك لأن الغاية من التفتيش هو كشف الحقيقة.

الفرع الثالث: إجراءات التحقيق الابتدائي الخاصة في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

ويقصد بالتحقيق الابتدائي هو التمحيص عن الأدلة الرقمية التي جمعت في مرحلة جمع الاستدلالات، وذلك من أجل تقديمها إلى سلطة التحقيق التي تقوم بدورها بإحالة ملف القضية للمحكمة أو عدم إحالته والتحفظ عليه، وتختص نيابة مكافحة الجرائم الاقتصادية في التحقيق في الجرائم دون غيرها (القهيوي، 2023).

نصت المادة 1 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 على أنه "تختص النيابة العامة دون غيرها بإقامة الدعوة الجزائية مباشرتها ولا تقام من غيرها إلا في الأحوال المبينة في القانون"، فبعد الانتهاء من مرحلة جمع الاستدلال تقوم النيابة بتقييم محضر جمع الاستدلالات، وتحديد مدى إمكانية إقامة الدعوى بناءً على المحضر الموجود لديها أم حفظ الدعوة وعدم إحالتها (قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة2001).

ونصت المادة 55 في الفقرة الأولى والثانية من ذات القانون على أنه "تختص النيابة دون غيرها بالتحقيق في الجرائم والتصرف فيها.2 للنائب العام أو وكيل النيابة العامة المختص تفويض أحد أعضاء الضبط

القضائي المختص بالقيام بأي عمل من عمل التحقيق في دعوى محددة وذلك عدا استجواب المتهم في مواد الجنايات"، أن معظم الأنظمة القانونية قد منحت سلطة التحقيق الابتدائي لجهة قضائية، حيث يتولاها قاض يطلق عليه قاضي التحقيق، كما فعل المشرعان اللبناني والفرنسي، أو تتولاها النيابة العامة كسلطة إضافية على عملها كسلطة اتهام وتمارسها بصفتها سلطة قضائية، حيث ذهب معظم الفقه إلى إصباغ الصفة القضائية على النيابة العامة كما فعل المشرع الأردني والمصري والفلسطيني ومعظم التشريعات العربية (صالح، 2006).

ففي مرحلة التحقيق يقوم عضو النيابة بمناقشة واستجواب المتهم بصورة تفصيلية عن الأفعال والشبهات الموجهة إليه، ولخصوصية هذه الجرائم الواقعة على عملية التحويل الإلكتروني للأموال يجب أن يكون هناك تطور لمفاهيم أساليب التحقيق وإجراءاته بصورة تتلاءم مع الخصوصية الخاصة به، فيجب تدريب الكوادر التي تباشر التحقيقات التحريات، وذلك في حالة عدم وجود الخبرة والكفاءة اللازمة سيؤدي ذلك إلى وقوع أخطاء جسيمة وأضرار في الأجهزة والملفات والأدلة الخاصة بالإثبات (البغدادي، 2018).

وفي ظل تطور تكنولوجيا المعلومات بشكل الملحوظ وذلك في الآونة الأخيرة، أصبح هناك عدة تحديات تقع على عاتق جهات التحقيق منها خصوصية الأفراد في الجرائم الإلكترونية، فلا يمكن الإغفال والتغاضي عن خصوصية المتهم في حقه في سرية معلوماته الشخصية الموجودة على الأجهزة الخاصة به حيث قد تكون هناك بيانات خاصة مخزنة على جهاز الحاسوب لا تتعلق بالجريمة، وتعتبر هذه من الصعوبات التي تواجهها سلطة التحقيق، وذلك لتحقيق الالتزام بالنصوص القانونية الخاصة في احترام الحق في الخصوصية (غنام، 2023).

فعلى المحقق في جرائم الاعتداء على عمليات التحويل الإلكتروني للأموال أن يكون لديه المعرفة اللازمة في مبادئ الاتصال والأنظمة التشغيلية لأجهزة الحاسوب، وكيفية الانتقال في هذه البيانات، وذلك لفهم وتصَور كيفية ارتكاب الفعل الإجرامي، من تلاعب في البيانات واختراق للشبكات وغيرها من الأمور التي

يقوم بها المجرمون، فإن المعرفة في هذه الأمور تعتبر ضرورية نظراً لأن هذه الجرائم ترتكب بطريقة إلكترونية، وذلك لكي يكون لدى المحقق الصورة الكافية عما حدث في هذه الجريمة، ويجوز للمحقق الاستعانة بالخبير المختص، وذلك لمعرفة بعض الأمور التقنية والإلكترونية التي تحتاج إلى ذوي اختصاص للأخذ برأيهم، فعلى المحقق أن يكون لديه القدر الكافي من المعرفة اللازمة وذلك لضرورة مناقشة الشهود واستجواب المتهمين، ولكي يستطيع طرح الأسئلة التي تتصل بالسلوك الإجرامي وطريقة ارتكابه، وذلك لأن كلام المجرم أثناء استجوابه يكون عبارة مفاهيم خاصة بالبرامج والشيفرات المستخدمة في الجريمة وآليات معينة للدخول، والمعرفة في الأمور التكنولوجية أمر لازم حتى يفهم المحقق كلام المجرم ويعلم مدى حقيقة صدق كلامه، ويجوز للمحقق إنهاء التحقيق إلى حين ندب من يأنس فيه الكفاءة والخبرة الفنية والتقنية اللازمة للاستعانة بخبرته، تظهر أهمية الاستعانة بخبير فني عند عجز الشرطة عن كشف الغموض الحاصل في الجريمة أو عجزها عن جمع الأدلة (الفيل، 2010).

فأجاز القانون الاستعانة بالخبرة من قبل وكيل النيابة إذا اقتضت مصلحة التحقيق ذلك، فإذا كان الخبير ليس من ضمن جدول الخبراء المعتمدين قانونياً يتم تحليفه اليمين على أداء مهمته بأمانة، ويترتب البطلان بحالة إغفال حلف اليمين، أن الخبرة تساهم وتعاون جهة التحقيق في البحث عن الحقيقة فقد تحتاج جهات التحقيق والشرطة إلى من يعاونها في الكشف عن الغموض الحاصل في الدليل الرقمي، وذلك بالاستعانة بالخبير لإعطاء رأيه في هذا الأمر، وينحصر دوره في المهام التي تم تكليفه بها، فعند ارتكاب الجريمة الإلكترونية يتم ترك بصمات رقمية في تعتبر غير مرئية، وهذه البصمات لها عدت أشكال منها الملفات المؤرشفة وهي ملفات يمكن الوصول لها بكل سهولة ولا تحتاج إلى خبرة لاستخراجها، ومنها البيانات الممسوحة فهذه تحتاج إلى خبراء خاصين لاستخراجها، وذلك لأن أي إجراء خاطئ من قبل الجهات المختصة يؤدي إلى فقدان الدليل وتلفها ويجعلها غير مقبولة أمام المحكمة، وتستخدم هذه الأدلة الرقمية في التحقيق وتكون المعلومات التي تسبق وتلي الجريمة مصدراً مهماً، مثل ذلك إذا قام المجرم باستخدام برامج معينة على شبكة الإنترنت وقام بالتواصل مع أحد فيتم تعقب أثر المعلومات الإلكترونية من قبل

الجهات المختصة، فمحاولة الجاني محو الدليل الرقمي يعتبر دليل ضده فهو يظن أن قيامه بمثل هذا الفعل لا يتم كشفه، إلا أن هناك سجل في ذاكرة الآلة يدون جميع الحركات والمعلومات، فالخبير الفني لديه الخبرة الكافية وذلك لمعرفة إذا ما تم العبث بالأدلة أو تحريفها أم لا (الباقي، 2018).

ويتميز التحقيق في إجراء عمليات التحويل الإلكتروني الأموال بتطور المفاهيم المستخدمة فيه، كونه يتم عبر بيئة افتراضية وتقنية تباشر فيها إجراءات التحقيق، فهناك عدة أهداف للتحقيق الإلكتروني بخصوص جمع الأدلة، تتمثل في معرفة الأدوات التي تم استخدامها لتثبت الاختراق وما هي نقاط الضعف الذي اتسم بها النظام الذي جرى اختراقه، والآثار التي رتبها الاختراق من حجم خسائر وتحديد من هو الذي قام بالاختراق، والعمل بأقصى جهد ممكن من أجل المحافظة على الدليل الإلكتروني في مسرح الجريمة (الشعار، 2022).

وبعد الانتهاء من هذه الإجراءات يتم إحالة الملف إلى المحكمة المختصة مشتمل على التحقيقات والمضبوطات التي عثر عليها أثناء التحري والتحقيق من قبل الضابطة القضائية.

المطلب الثاني: إجراءات التحقيق النهائي الخاصة في الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

يعتبر التحقيق النهائي مرحلة لاحقة للتحقيق الابتدائي يتم فيها جمع الأدلة والمعلومات النهائية لأثبات أو نفي التهمة التي سوف يتم إدانة المتهم فيها، ويتم استجواب المشتبه فيه أيضاً وتجميع جميع الأدلة من أجل تقديمها للمحكمة المختصة (موقع وكالة عمون الاخبارية، 2023).

ويقصد بالتحقيق النهائي تحويل القضية الجنائية إلى المحكمة المختصة، وتشمل جميع الإجراءات التي تبدأ منذ دخول الدعوى الجزائية للمحكمة المختصة، إلى حين صدور حكم نهائي سواء كانت المحكمة المختصة هي صلح أو بداية (موقع النيابة العامة الاتحادية ، 2020).

وفي مرحلة التحقيق النهائي التي تشرف عليها المحكمة المختصة في نظر الدعوى، تكون هذه التحقيقات علنية ومدونة وفق مبدأ علنية الجلسات، مالم يطلب الخصمان جعلها سرية إذا كانت تمس بالنظام العام والآداب العامة، وحتى لو كانت الجلسات سرية فإن النطق بالحكم يكون علني، فالقضاء الجنائي مبني على الحرية في الإقناع، فيكون للقاضي الحرية في الأخذ بالدليل أو طرحه جانباً وعدم الالتفات له (موسى، 2023).

وفي حال وقوع جريمة نص عليها التشريع الجنائي في الدولة، فإن هناك إجراءات رسمها القانون ويجب إتباعها من أجل الحفاظ على النظام في الدولة، وحماية الحقوق العامة للمواطنين، وللدعوى الجزائية مراحل عديدة سوف يتم التركيز في هذا المطلب على مرحلة المحاكمة، ففي بعض القضايا تنتهي مرحلة المحاكمة بسرعة بسبب إقرار المتهم بالتهمة المسندة إليه، وبالتالي السرعة في صدور الحكم بخلاف القضايا التي تتطلب مناقشة شهود وجلب خبراء فنين خاصة في جرائم عمليات التحويل الإلكتروني للأموال، والتي تتطلب خبراء فنين في هذا المجال، وفي بعض القضايا قد يقوم القاضي باحتجاز بعض الاشخاص المتهمين بالجريمة، وإجراءات التحقيق النهائي للجرائم تبدأ بمثول المتهم أمام المحكمة المختصة، وتكون النيابة العامة حاضرة وتوجه التهمة للمتهم الحاضر، ويتم سؤاله إذا كان مذنب أو غير مذنب، وتجري بعدها إجراءات المحاكمة، وبعد ذلك تجري عملية تقديم الأدلة التي يمكن من خلالها إدانة الشخص المتهم أو إعلان براءته، ويمكن خلال إجراء المحاكمة أن تقوم النيابة العامة بتقديم دليل حصلت عليه بطريقة غير مشروعة، وذلك قد يكون عن طريق انتهاك الخصوصية مثل تسجيلات صوت أو مكالمة أو غيرها، وهنا يأتي دور المتهم بتقديم طلب لقمع الدليل الذي تم الحصول عليه بشكل ينتهك الخصوصية أو يقوم بالاعتراض على الدليل قبل الشروع في تقديمه لأنه تحصل عليه بطريقة غير مشروعة منتهكة لخصوصيته، وفي حال سمحت المحكمة للنيابة العامة بتقديم هذا الدليل يستطيع محامي المتهم مناقشتها بهذا الدليل لأقناع المحكمة بالاستغناء عن هذا الدليل، وبعد تقديم النيابة العامة أدلة

الإدانة يقوم المتهم بتقديم أدلة البراءة الخاصة به، ويبدأ بمناقشتها لأقناع المحكمة ببراءته وبعد ذلك يصدر الحكم إما بالبراءة أو الإدانة (سمير، 2021).

ولابد من الإشارة إلى نقطة مهمة تتعلق بالمحاكمة قبل تحويل أي دعوى جزائية للمحكمة، تقوم النيابة من التأكد من أن الأدلة المتوفرة كافية لمحاكمة المتهم وفقاً لنصوص القانونية والعقابية التي نص عليها القانون، وتكون دور المحكمة هي إظهار الحقيقة بعد انتهاء المحاكمة سواء بإدانة المتهم أو إعلان براءته، فمن جهة تطلب النيابة العامة الإدانة، ومن جهة أخرى يطلب المتهم إعلان البراءة، وهنا يأتي دور المحكمة في وزن البينة لتكوين عقيدتها من حيث إعلان البراءة أو الادانة، ولابد من الإشارة إلى أن خلال فترة المحاكمة تدرس المحكمة الحالات التي قد تؤدي إلى سقوط الدعوى الجزائية فتتمثل هذه الحالات أ) وفاة المتهم، ففي حال كانت إجراءات المحاكمة سارية، وفي أي مرحلة تمر فيها الدعوى الجزائية ثم توفى المتهم، فهنا الدعوى الجزائية لا تورث بل تسقط، مع العلم أن أثر سقوطها لا يؤدي إلى سقوط الدعوى المدنية، بل تنتقل الدعوى المدنية إلى ورثة المتهم، والحالة الثانية التي تؤثر على سير الدعوى الجزائية هي ب) صدور عفو عن الجريمة، والمقصود به صدور نص قانوني يجعل الفعل المرتكب، من فعل مجّرم إلى فعل مباح، وبالتالي ذلك يوقف تحريك الدعوى الجزائية أو قد يصدر عفو خاص، ويرتب أيضاً نفس الأثر على الدعوى الجزائية ولكن يتميز عن العفو العام، أنه يصدر بحق شخص معين وموجه لجريمة محددة يعفي صاحبها من العقاب، ومن الحالات أيضاً التي تؤثر على الدعوى الجزائية وسيرها هي ج) التقادم، فتسقط الدعوى الجنائية بمرور عشرة سنوات على آخر إجراء تم فيها، وفي الجنح بمرور ثلاثة سنوات على آخر إجراء تم فيها، والمخالفات مرور سنة على آخر إجراء تم فيها (السلام، 2021).

ويجب معرفة أن تقديم الأدلة خلال إجراءات المحاكمة التي تتعلق بالجرائم الواقعة على عمليات التحويل الإلكتروني للأموال تختلف عن الجرائم التقليدية، وخاصة أن الأدلة لها طبيعة خاصة تتمثل بالحواسيب وأنظمة المعلومات وشبكات الإنترنت، وبالتالي تتمثل الأدلة في هذا النوع من الجرائم بتقنيات إلكترونية

ورقمية للحصول على معلومات تتعلق بالجاني ومكان ارتكابه للجريمة، وخاصة أنه في هذا النوع من الجرائم يتم الاستعانة بالخبراء الفنيين بشكل كبير؛ من أجل ضبط الدليل الإلكتروني والحفاظ عليه وعدم خسارته من أجل إدانة المتهم، ولابد في بعض الأحيان من الحفاظ على الدليل المخزن على الحاسوب وتجميده على شكل مادي ملموس من أجل تقديمه كدليل خلال إجراءات المحاكمة، ولابد من الانتباه لموضوع الحصول على الدليل بطريقة مشروعة، وضمن الإجراءات التي رسمها القانون، لأنه إذا لم تكن ضمن الإجراءات التي رسمها القانون نكون أمام خيار بطلان الإجراءات، وقد انتهج المشرع الفلسطيني في الإثبات الجنائي مبدأ الحرية في الإثبات فيجوز الإثبات بجميع طرق الإثبات والدليل يخضع لاقتناع القاضي (ربايعة،، 2016).

وهنا يمكن طرح تساؤل كيف يُكوَن القاضي الجزائي قناعته في جرائم التحويل الإلكتروني للأموال؟

من أبرز المبادئ التي يقوم عليها الإثبات الجنائي "أن يتوفر للقاضي الجزائي من الأدلة المطروحة أمامه، ما يكفي لتسبيب ما اعتقده بثبوت الوقائع أو نفيها كما أوردها في حكمه ونسبها للمتهم"، فاقتناع القاضي يُبنى على مدى قبوله للأدلة وتقدير قيمتها فله الحرية في ذلك إذا حقق ثقة لدى القاضي الذي ينظر الدعوى، وليس كل دليل قابل للتقدير، بحيث لا يقبل الدليل إذا كان غير دقيق أو غير سليم أو تم وفق إجراءات قانونية غير مشروعة، بالتالي يستبعد الدليل الناتج عنه، فيجب التأكد من مشروعية الدليل قبل إجراء عملية التقدير (الحجار، 2021).

فتعتبر حرية القاضي غير مطلقة، فليس له أن يدخل تخميناته وتصوراته الشخصية، بل يجب أن تكون قناعته بنيت بالعقل ووفق منطق سليم وأَسس ومبادئ علمية للتقدير (بشير، 2021)، ويتم مناقشة الدليل أمام المحكمة وذلك لتكوين القناعة الكافية لدى القاضي، ويجوز للمحكمة الاستعانة بالخبراء لمناقشة الدليل الرقمي كغيره من أدلة الإثبات التي تخضع للمناقشة ، فالقاضي الجزائي له أن يأخذ بهذا الدليل أو يطرحه جانباً ، ويجب على المحكمة عند النطق بالحكم تسبيبه (جامعة سعدة، 2018).

ويتم تكوين قناعة القاضي في هذه الجرائم بناءً على الأدلة المقدمة لديه، وفي قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 في المادة 206 نصت على"1–تقام البينة في الدعاوي الجزائية بجميع طرق الإثبات إلا إذا نص القانون على طريقة معينة للإثبات"، وترى الباحثة_بناءً على أن المطلق يؤخذ على إطلاقه، وبالتالي في جرائم عمليات التحويل الإلكتروني للأموال يكون الإثبات بكافة طرق الإثبات، ما لم ينص القانون على طريقة معينة، وبالتالي لابد أن يكون الدليل شكّل قناعة لدى القاضي من أجل اعتماده في الدعوى.

ومن الأدلة التي تبنى عليها قناعة القاضي هي الأدلة الرقيمة، والمقصود بها هو الدليل المأخوذ من أجهزة الكمبيوتر ويكون عبارة عن نبضات مغناطيسية أو كهربائية ويحتاج إلى معالج رقمي لقراءة محتواه وإلى مختصين تقنين، فإذا تم استخدام الأداة الرقمية في الجريمة فيكون الدليل الإلكتروني أو الرقمي محل لإثباتها (رجاء، 2018)، وقد تكلم عن حجية الدليل الإلكتروني في القرار بقانون الخاص بالجرائم الإلكترونية رقم 10 لسنة 2018 والذي عالج هذه المسألة بمادة قانونية صريحة، في المادة 37 منه التي أكدت على أن "تعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة معلومات أو شبكات المعلومات أو مواقع إلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات" ونص أيضاً في المادة 38 من ذات القانون على أنه "يعتبر الأدلة المتحصل عليها بمعرفة الأجهزة المختصة أو جهات التحقيق الدول من دول أخرى، من أدلة الإثبات طالما أن الحصول عليها قد تم وفق الإجراءات القانونية والقضائية للتعاون الدولي" ويستنتج من هذين النصين أن الدليل الرقمي يعتبر من أدلة الإثبات التي نص عليها القانون صراحةً إذا تم استخراجها بطريقة مشروعة عن طريق الأجهزة المختصة (قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001).

فالدليل الرقمي المتحصل من جرائم عمليات التحويل الإلكتروني للأموال يعتبر من أدلة الإثبات، ويعتبر أيضاً قضائياً دليل أصلي في الدعوى، ويتمتع بحجة قانونية في المحكمة، ولا يتم مناقشة هذا النوع من

الأدلة إلا بآلية معينة حددها القانون، أما دور القاضي فيتحقق من صحة الدليل أولاً لقبوله في المحكمة وتقع على المحكمة مهمة تقدير حجيته، وتستطيع الاستعانة بالخبراء لتقديم رأيه في الدليل المطروح، ويستطيع الخصم أيضاً المقدم الدليل ضده الاستعانة بالخبراء لطعن بالدليل وطرحه بعيداً، وبعد الاطلاع على القانون السعودي فإنه سمح للمحكمة في حال عدم قدرتها على معرفة مدى صحة الدليل أن تقدر قيمته حسب ما يظهر لها من ظروف الدعوى وبما أن الأدلة التي تنتج عن جرائم عمليات التحويل الإلكتروني في تتطور مستمر فإنه على الخبير المختص الذي توكله المحكمة بالاطلاع على الدليل أن يكون لديه خبرة في هذا المجال ولديه إلمام بجميع البرامج المستحدثة التي تستخدم لفصح هذه الادلة (العزيز، 2022).

وقد يتم الاستعانة بخبير فني وتقني للمساعدة في البحث عن الحقيقة ، إذا كانت المحكمة لا تستطيع في مثل هذا النوع من الجرائم تقدير قيمة الدليل الرقمي في جرائم التحويل الإلكتروني للأموال، وأن رأيه يخضع لتقدير المحكمة، إلا إذا كانت الخبرة متعلقة بمسائل فنية بحتة، فهنا لا يجوز للمحكمة تفنيدها إلا بأساليب فنية، فيعتبر الاستعانة بخبير من الأمور المهمة، وينحصر دوره في المهام التي تم تكليفه بها، فليس له صلاحيات إلا في حدود التي تسمح بها المحكمة التي تنظر الدعوى، وللخبير الفني والتقني جمع واستخراج الأدلة الرقمية المتعلقة بالجريمة باستخدام تقنيات حديثة ومع بيان هذه التقنيات التي قام باستخدامها من برامج وأجهزة ومعدات (مسار، 2012).

وتعد الشهادة أيضاً من أدلة الإثبات ويعد الإثبات بها أمراً لا غنى عنه، لأنها تنصب على حوادث عابرة قد تصبح أساساً في الدعوى، والشهادة كغيرها من وسائل الإثبات تخضع لتقدير القاضي للشهادة، فإذا كان هناك أدلة الأخرى تدعم هذه الشهادة فيكمن للأخذ بها، وقد تكون الشهادة من الأشخاص العاملين في الشركات، التي تقوم بجريمة من جرائم التحويل الإلكتروني للأموال كجريمة الاحتيال الإلكتروني، ويقوم العاملين بهذه الشركة، بإدخال البيانات التي تم تكليفهم بها، وذلك لإرسال رسائل إلكترونية إلى الزبائن

لخداعهم والاستيلاء على أموالهم دون علم العاملين، فيتم الأخذ بالشهادة كدليل من أدلة الإثبات في حال اقتناع القاضي واطمئنانه لها (الشديدي، 2016).

وقد تتكون قناعة القاضي بناءً على اعتراف المتهم بالجريمة الموجهة إليه، فيجب أن يكون اعترافه صريح لا غموض فيه، وأن لا يكون المتهم مكره على الاعتراف فيجب أن يكون حر الإرادة أثناء اعترافه، وأن يصدر اعترافه أمام مجلس القضاء وأن يكون مطابقاً للحقيقة وللبينات المقدمة في الدعوى، فإذا حصلت جريمة من الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال، وقام الشخص المرتكب لهذه الجريمة بالاعتراف بها مع موافقتها مع شروط الاعتراف فيجوز للمحكمة الأخذ بها، ويجوز للمحكمة الأخذ بالاعتراف حتى وإن لم يكن متطابق مع الدليل الإلكتروني إذا كان هذا الدليل يشوبه الغموض ولا يجزم ارتكاب المتهم لهذه الجريمة، فيكون اعتراف المتهم في تلك الحالة كافٍ (محمود، 2021).

وبالرجوع للمادة ٢٠٧ من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 "لا يبنى الحكم إلا على الأدلة التي قدمت أثناء المحاكمة والتي تمت مناقشتها في الجلسة بصورة علنية، أمام الخصوم" وكذلك المادة ٢٧٣ "لا يجوز أن يبنى الحكم على دليل لم يطرح في الجلسة" من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 وبالتالي فإن الدليل الذي يتم التحصيل عليه من قبل نيابة مكافحة الجرائم الاقتصادية في جرائم عمليات التحويل الإلكتروني للأموال، يتم مناقشته من قبل القاضي خلال الجلسة ويقوم القاضي باستبعاد الدليل الذي يكون محل شك في طياته، ويمكن للمشرع الفلسطيني الاستفادة من تجربة بعض الدول مثل السعودية التي تعاملت بطريقة خاصة في موضوع تقديم الدليل الرقمي المتحصل من جرائم عمليات التحويل الإلكتروني للأموال، حيث وضعت نصوص تشريعية خاصة بينت فيها أن مأمور الضبط في هذا الجرائم يجب أن تكون مختص في هذا المجال، كذلك نظم نصوص خاصة في آلية تقديم الدليل للمحكمة حيث أعطى المجال في حال لم تكن متأكدة من صحة مصدر الدليل أن تقوم بتقدير قيمته القانونية (شهاب، احمد عبد الكريم عبدالرحمن، 2018).

وكما ذكرنا فإن جرائم عمليات التحويل الإلكتروني للأموال لها خصوصية تختلف عن الجرائم التقليدية، وخاصة في المراحل التي تمر فيها الدعوى الجزائية، وهنا سوف تتحدث الباحثة أيضاً عن قواعد الاختصاص القضائي لجرائم عمليات التحويل الإلكتروني للأموال، والمقصود بها السلطة التي أعطاها القانون للقضاء للنظر في الدعوى، فالقاضي في هذه الجرائم يتحقق من الاختصاص الدولي أي البحث إذا كان القضاء الوطني مختص أم لا، وخاصة أن في جرائم عمليات التحويل الإلكتروني للأموال قد يشترك في الجريمة أكثر من طرف أجنبي، فقد تتم عملية التحويل من فلسطين إلى سوريا مثلاً، وبالتالي يبحث القاضي في هذه النقطة، وأيضاً يبحث في نقطة ثانية تتمثل في الاختصاص الداخلي، بعد التأكد أن القضاء الفلسطيني هو المختص، ولابد من تحديد المحكمة المختصة بالفصل في الدعوى، وبالنظر للمحاكم الفلسطينية نجد أنها لم تنشأ محاكم خاصة بجرائم عمليات التحويل الإلكتروني للأموال، وبالتالي تخضع الجرائم للاختصاص القضائي العام، وفق طبيعة كل جريمة والعقوبة المخصصة لها، ويبحث القاضي بالاختصاص الإقليمي، الذي يتمثل في أن الاختصاص الوطني يصبح صاحب ولاية في حال وقعت جريمة التحويل الإلكتروني للأموال على أرض الدولة، أو كان أحد عناصره قد تم على هذه الدولة، وهذا ما أكدت عليه المادة الثانية من القرار بقانون بشأن الجرائم الإلكترونية حيث جاء فيها أن هذا القرار يطبق في حال ارتكبت الجريمة كلياً أو جزئياً داخل فلسطين أو خارجها، وبخصوص الاختصاص الشخصي فأنه يتمثل في ملاحقة الجاني حامل الجنسية في حال ارتكابه لجريمة خارج البلاد، وقد استغلوا الجناة نقطة أن الدولة في العادة لا تقوم بتسليم رعاياها، ونلاحظ أن في جرائم عمليات التحويل الإلكتروني للأموال عادة ما يستخدم الجناة الكلمات المشفرة والألغاز المعقدة؛ وذلك من أجل إتمام جرائمهم وعدم الكشف عن جنسياتهم، والفرع الثالث يتمثل بالاختصاص العيني، ويقصد به تطبيق القانون الجنائي الوطني بغض النظر عن الجنسيات المختلفة التي شاركت في جريمة التحويل الإلكتروني للأموال، ويأتي منطقها من أن جرائم عمليات التحويل الإلكتروني للأموال تمس أمن الدولة الاقتصادي، وبالتالي تهدد كيان الدولة ونظامها، وخاصة إذا كانت جرائم عمليات الاحتيال المالي التي تمت عن طريق التحويل الإلكتروني

للأموال تؤثر على سيادة الدولة وكيانها، مثل القيام بتحويل أموال خاصة في الدول لمصارف أجنبية ومن ثم سرقتها باعتبارها جرائم عابرة للقارات، الاختصاص العالمي وخاصة في ظل انتشار شبكات الإنترنت التي ليس لها مقر معين في دولة معينة، وهي بالتالي صعوبة إخضاع جميع عمليات التحويل الإلكتروني للأموال للرقابة المشددة أو السيطرة الكاملة، وخاصة أنه لا يوجد قانون جنائي محدد يربطها، وبالتالي في هذا النوع من الجرائم نضطر للخروج عن مبدأ الإقليمية، حتى لو لم يكن الجاني من الدولة، يكفي أن تقع مخلفات الجريمة داخل إقليمها لتصبح مختصة (المصري، 2017).

وفي مرحلة التحقيق النهائي الذي تمارسه المحكمة في جرائم عمليات التحويل الإلكتروني للأموال يختلف عن الجرائم التقليدية في عدة أمور لامستها الباحثة سوف تقوم بعرضها:" أ) يتم استخدام في المحكمة مصطلحات جديدة، خاصة بالأدلة الإلكترونية التي سوف تقدم كبينة في المحكمة ضمن عالم التقنيات، ومثال ذلك استخدام مصطلح النسخ بدل الضبط ب) التحقيق في جرائم عمليات التحويل الإلكتروني للأموال في طبيعته يختلف عن الجرائم التقليدية، ونتاج ذلك أن البيئة في جرائم عمليات التحويل الإلكتروني للأموال تختلف عن الجرائم التقليدية، فبيئة الأولى هي شبكات الإنترنت وقواعد البيانات والبريد الإلكتروني ووسائل الدفع الإلكترونية بالإضافة إلى الأسهم والسندات وغيرها ج) مسرح الجريمة في جرائم عمليات التحويل الإلكتروني للأموال يختلف اختلاف كامل عن الجريمة التقليدية، فترتكب في الغالب هذه الجرائم باستخدام الحاسوب وفي الخفاء بعيداً عن أعين الناس، وبالتالي يجب على المحقق أن يتحلى بمهارات فنية، يختلف ويتميز فيها عن المحقق العادي د) من الصعوبات التي تواجه الدليل الذي تم أخذه في جرائم عمليات التحويل الإلكتروني للأموال، أنه يصعب في بعض الأحيان الشرح للمحكمة وخاصة إذا كان القاضي لديه صعوبة في إدراك المفاهيم وخاصة أنه لا يوجد محاكم مختصة في هذا المجال، وبالتالي على نيابة مكافحة الجرائم الاقتصادية خلال إجراءات المحاكمة أن يكون لديها فطنة وقوة ملاحظة، وأن يكون لديها القدرة على متابعة هذه الأدلة وتتبعها من أجل تقديمها للمحكمة هـ) المتهم خلال محاكمته في جرائم عمليات التحويل الإلكتروني للأموال، يتميز بعدة صفات منها الذكاء والخداع والقدرة الفنية العالية في

استخدام الحاسوب ووسائل الدفع الإلكترونية، ويختلف عن الجرائم التقليدية وهذا ما أدى إلى ظهور جرائم حديثة ومبتكرة بخصوص عمليات التحويل الإلكتروني للأموال، وهنا نقع في مشكلة ألا وهي مبدأ الشرعية من خلال النقص فيها وعدم قدرتها على تغطية الجرائم الحديثة التي ترتكب في هذا المجال، وهناك مشكلة أخرى تتمثل في الأجهزة المستخدمة في تتبع هذه الجرائم من أجل الحصول على الأدلة الجنائية لتقديمها للمحكمة تحتاج لإمكانيات مادية باهضه ومن المشكلات العملية التي تواجهنا في مكافحة جرائم عمليات التحويل الإلكتروني للأموال، هي عدم وجود تعاون بين الدول لتسليم المجرمين وغياب الإطار التشريعي الموحد بين الدول، بالإضافة الى ضعف التعاون الأمني مما أدى إلى انتشار جرائم غسيل الأموال، بحيث تخطت هذه الجرائم المساحات الجغرافية للبلدان وبنفس الوقت إخفاء هوياتهم" (الشعار، 2022).

وبخصوص التشريعات المقارنة فبعد الاطلاع على قوانين الأوروبية التي تتعلق بجرائم عملية التحويل الإلكتروني للأموال، نجد أن الدول الأطراف في مجلس أوروبا يعتبروا ملزمين في نصوصهم القانونية المتعلقة بالإجراءات بجمع الأدلة، حيث يجب عليهم الالتزام بالضمانات المتعلقة بحقوق الإنسان والحريات الخاصة أي منع اختراق ما يسمى بالخصوصية، كذلك الالتزام من قبل الأشخاص المخولين بضبط الأدلة والمعلومات الرقمية الحفاظ على سلامة هذه الأدلة لوقت كافي من الزمن، والولايات المتحدة الأمريكية كذلك أكدت على احترام خصوصية المواطن وضعت معايير من أجل ضبط هذا الموضوع حيث أن دور الرقابة والتحقيق لابد أن يتم ضمن قواعد تقوم على أساس احترام الخصوصية (التحقيق في الجرائم الالكترونية واثباتها في فلسطين دراسة مقارنة ، 2016).

وبناءً على ما تم ذكره في هذا المطلب ترى الباحثة أن هناك حاجة لتطوير النظام القضائي وذلك بسبب التقدم التكنولوجي والانفتاح على العالم الرقمي، وحتى يكون هناك قضاة ذوي اختصاص معمق في هذا النوع من الجرائم، لأنها تمتاز بالدقة والتعقيد وتحتاج إلى فهم أساليب وتقنيات إلكترونية، حتى لو أن في المحاكم العادية تقوم بالاستعانة بخبير لتقدير الأدلة، إلا أنه من الأجدر والأفضل أن يكون القاضي على

إطلاع وعلم كافي بهذه التقنيات، فوجود كادر قضائي متخصص يعمل على تحسين الأحكام وضمان وتحقيق العدالة متخصصة وينمي قدرة القضاء على مكافحة الجرائم المالية التي ترتكب بطريقة إلكترونية.

وأنه لا يوجد محاكم متخصصة في هذا المجال، ونرى أن السبب يعود إلى عدم انتشار هذه الجرائم، وعدم وجود كم كبير من هذه القضايا، وبالتالي يتم العودة للقواعد العامة الخاصة بالاختصاص فيتم تحديد الجريمة إذا كانت جنحة أو مخالفة أو جناية حسب العقوبة المفروضة لها، وذلك من خلال العودة لقانون العقوبات رقم 16 لسنة 1960 في المادة 14 منه نصت على "العقوبات الجنائية هي "1 . الإعدام 2. الأشغال الشاقة المؤبدة 3. الاعتقال المؤبد 4. الأشغال الشاقة المؤقتة 5. الاعتقال المؤقت" فإن المحكمة المختصة هي محكمة الجنايات، أما في حال كانت العقوبة حسب نص المادة 15 "العقوبات الجنحية هي 1. الحبس 2. الغرامة 3. الربط بكفالة"، فتكون من اختصاص محكمة الصلح ، وإذا كانت العقوبة جنحة أو مخالفة فإن المحكمة المختصة هي محكمة الصلح وهذا ما يتم تطبيقه لدين"ا (قانون العقوبات رقم 16لسنة 1996 المادة 14)، وأما عن الدول الأخرى فهناك دول وضعت محاكم مختصة للنظر في مثل هذه القضايا مثل دولة البحرين، حيث أصدر رئيس مجلس القضاء الأعلى فيها، قرار بتخصيص محكمة متخصصة تنظر في غسيل الأموال، ويخضع ضمن اختصاصها الجرائم المالية الواردة في قانون العقوبات وقانون غسيل الأموال وصنفها معالي المستشار على أنها من الجرائم المالية التي تضر بالاقتصاد، أيضاً دولة تركيا قامت بإنشاء محاكم متخصصة بالجرائم الإلكترونية والمالية (الله، 2008).

المبحث الثاني: الإجراءات الوقائية الخاصة بمكافحة الجرائم الواقعة على عمليات التحويل الإلكتروني للأموال.

هناك عدة تدابير يمكن اتخاذها من أجل حماية الأموال الخاصة بالمواطنين من جرائم عمليات التحويل الإلكتروني للأموال، وخاصة جريمة غسيل الأموال، وحماية المصارف خاصة أنه مكان لتخزين الأفراد لأموالهم الخاصة واستثماراتهم المالية، وبالتالي لابد من وجود أنظمة داخل الدولة لمكافحة هذه الجرائم، حيث لابد من أن يتم مراقبة المنتجات والخدمات التي تقدم للعملاء من أجل تجنب استخدام هذه السلع

كوسيلة لإخفاء عمليات غسيل الأموال، كذلك الأمر لابد من مراقبة قنوات النشر والتوزيع التي تهدف لتسويق منتجاتها، ويمكن أن تستخدم الإنترنت أو البريد الإلكتروني أو الهاتف لتسويق المنتجات، وتمم عملية البيع دون التواجد الفعلي للعميل، وهذه الطريقة ترفع من مستوى الخطورة في استغلال هذه القنوات في جرائم غسيل الأموال، وهناك طرق للحماية من جرائم عمليات التحويل الإلكتروني للأموال يمكن أن يتم اتباعها من قبل المصارف لحماية الأفراد من جرائم عمليات التحويل الإلكتروني للأموال، عن طريق معرفة من هو العميل وما مصدر دخله ومصدر الأموال المراد إيداعها، ولابد من توخي الحذر من العملاء الاعتبارين الذين يكون لديهم شركات دون الإفصاح عن المالك الرئيسي، والحذر كذلك من المؤسسات والشركات التي لا يمكن التأكد من شخصية مالكها الرئيسي، وبالتالي لابد للمصرف الحذر من النشاطات التي تمارسها هذه الشركات، وإمكانية تحويل هذه الأنشطة لجرائم تقع على عمليات التحويل الإلكتروني للأموال (الفلسطينية، 2017).

وهناك عدة مؤشرات قد تدل على أن هناك جريمة قد تحدث عن طريق عمليات التحويل الإلكتروني للأموال: "أ) رغبة العميل بالمشاركة في صفقات تكون غير واضحة سواء من غرضها أو الغاية منها قانوني أو اقتصادي ب) قيام العميل بتزويد الجهة التي يتعامل معها سواء مصرف أو جمعية مالية بمعلومات غير صحيحة أو مضللة ج) علم الجمعية أو الجهة المالية التي يتعامل معها العميل بتورطه بأنشطة غسيل أموال أو أي جريمة من جرائم عمليات التحويل الإلكتروني للأموال د) وجود شبهات أن العميل وكيل عن موكل مجهول الهوية وعدم إعطاءه معلومات عن الشخص الأصلي في العلاقة هـ) عدم قيام العميل بتقديم معلومات دقيقة عن طبيعة العمل أو الأنشطة التي يقوم بها و) اكتشاف أن هناك اختلاف في طبيعة الأنشطة التي يقوم بها العميل ويمارسها فعلاً، عن الأنشطة التي يدعي القيام بها ي) قيام العميل بتحويل مبالغ كبيرة إلى جهات معينة، دون تقديم أي معلومات عن هذه الجهة والغاية من تحويل هذه الأموال ع) قيام العميل بتكرار تحويل تبرعات بمبالغ ضخمة واكتشاف أن هذه المبالغ لا تتناسب مع دخله الاقتصادي أو نمط حياته وسلوكه ز) انتماء العميل لمنظمة غير معروفة أو اكتشاف أن

هذه المنظمة لها نشاطات محظورة ح) ظهور علامات بذخ على العميل، من خلال حياة الرفاهية والسفر والتنقل بين البلدان، ويكون ذلك بشكل مبالغ فيه ولا يتناسب مع الوضع المالي الذي كان يعيشه" (جمعية عرق الخيرية، 2019).

وهناك وحدة أخرى تختص بالأمور المالية والتي تحدث عنها القرار بقانون رقم 39 لسنة2022 بشأن مكافحة غسل الأموال وتمويل الإرهاب في المادة 34 حيث نصت على "تنشأ بموجب أحكام هذا القرار وحدة مستقلة مركزية وطنية لمكافحة غسل الأموال والجرائم الأصلية المرتبطة وتمويل الإرهاب تسمى وحدة المتابعة المالية ومقرها سلطة النقد الفلسطينية..." وهذه الوحدة من أحد مهامها متابعة التحويلات المالية الداخلية والخارجية ويقع على المؤسسات المالية مثل البنوك وغيرها إبلاغ وحدة المتابعة المالية عن الشبهات المحتملة في التحويلات المالية، وهذه الوحدة تقوم بإجراء تحقيق مالي موازي وأعداد محضر استدلال في الشبهات المالية، وتقوم بإحالتها إلى النائب العام والتي يحيلها بدوره إلى نيابة الاختصاص لمباشرة التحقيقات فيها حسب الأصول للتأكد إذا ما كان هناك جريمة من عدمه، وبذلك يكون المشرع قد قام بالتصدي لمثل هذه الجرائم بإنشاء هذه الوحدة التي تقوم بتتبع الجرائم المالية وبالتالي توفر حماية فعالة ضد هذا النوع من الجرائم (شاهين، 2024).

ومثال على الدول العربية التي أنشأت وحدة المتابعة المالية هي مصر ، وذلك بهدف التصدي للجرائم المالية منها جرائم عمليات التحويل الإلكتروني للأموال، حيث أنشأت هذه الوحدة بموجب قانون مكافحة غسل الأموال رقم 80 لسنة 2002، حيث وضعت مجموعة من التعليمات الخاصة التي يجب على البنوك و المؤسسات المالية أيضاً الالتزام بها من أجل الكشف عن مصدر الأموال المراد تحويلها، وذلك للكشف عن أي محاولة لتمويل عمليات إرهابية أو غسيل أموال، وهذه الوحدة مختصة في هذه الأمور حيث جرى تقديم الإخطارات لها في حال اشتباه بإيداع مبالغ ضخمة لأحد البنوك من قبل أشخاص لا يتمتعون بمستوى عالي من الدخل، بالتالي أذا أصبح هناك شك قوي لدى هذه الوحدة تقوم بتزويد مأموري الضبط

المختصين بتتبع هذه الجرائم وإحالتها إلى النيابة المختصة ، ومثال على ذلك قيام أحد المشتبه بهم بفتح حساب لدى أحد البنوك وأجرى عمليات تحويل الإلكتروني من خلال هذا الحساب الذي تم فتحه بعد فترة اكتشفت الوحدة أن والد الشخص الذي قام بفتح الحساب هو المالك الحقيقي له، وكانت تعاملات الحساب تختلف تماماً عن طبيعة عمله، بالتالي وبعد عملية البحث والتحري من قبل الوحدة تم اكتشاف أن الوالد هو منتمي لجماعات ارهابية. (ابراهيم، 2020)

وفي هذا المبحث سيتم الحديث في المطلب الأول عن الوسائل التي يمكن من خلالها الوقاية من جرائم عمليات التحويل الإلكتروني للأموال، أما المطلب الثاني سيتم الحديث عن إجراءات الحماية الخاصة بأنظمة وبرامج التحويل الإلكتروني للأموال.

المطلب الأول: الوسائل التي يمكن من خلالها الوقاية من جرائم عمليات التحويل الإلكتروني للأموال.

ولحماية أموالنا من الاحتيال عليها عبر الجرائم الإلكترونية التي تنصب على الأموال هناك عدة طرق يمكن أن نستخدمها منها : "1) تجنب نشر البيانات الخاصة على منصات ومواقع ليست محل للثقة 2) تجنب الضغط على أي رابط يصل للشخص من الغير، عبر رسالة أو بريد إلكتروني 3) تجنب القيام بتحميل تطبيقات أو برامج من مصادر مجهولة 4) في حال كان الشخص يملك جهاز هاتف حديث فعليه القيام بتحديث نظام التشغيل الخاص به، وتتبع التنبيهات الأمنية التي قد يصدرها الهاتف 5) هناك عدة علامات تنبه الشخص لوقوع اختراق لنظام المالي الخاص به، مثلاً إذا كان هاتفه مرتبط بالتحويلات المالية، وذلك في حال وقع اختراق فإنه سوف يلاحظ أن بطارية هاتفه تنفذ بشكل كبير، ويكون جهاز الحاسوب أو الهاتف يعمل ببطء، أو قيام الجهاز بإرسال رسائل أو تحميل ملفات دون أمر صاحبها لهذه الأوامر، وهناك علامة أخرى تتمثل بارتفاع درجة حرارة الجهاز بشكل ملحوظ دون أن يقوم صاحبه بممارسة أي نشاط عليه" (السلامة السيبرانية والأمن السيبراني).

وهناك عدة طرق يمكن اتباعها لحماية أموالنا في عصر التقدم التكنولوجي والتقدم الرقمي، ومن أجل تجنب ما يسمى الاحتيال المالي، وتبيض الأموال، واختلاس الأموال، والقرصنة والتزوير وغير من الجرائم التي تقع على عمليات التحويل الإلكتروني للأموال، والتي تهدد النظام المالي للدولة وخاصة المصارف، كون ارتكابها يؤدي خسائر كبيرة وفادحة في البنوك والعملاء، وكذلك في حال ارتكابها بشكل متكرر هذا قد يؤدي إلى انعدام الثقة في النظام الأمني التابع للمؤسسة المالية، سواء مصرف أو وزارة مالية تابعة لدولة، ومن سبل حماية أموالنا في العصر الحديث: "1) الحفاظ على الهوية الشخصية من السرقة؛ لأن سرقتها هي جريمة دارجة في العصر الحالي؛ لأن سرقة الهوية تفتح للمجرمين وسائل وسبل كثيرة لسرقة بيانات شخصية، مثل الاسم والعنوان وأرقام الضمان الاجتماعي مما يمكن المجرم من القيام بعمليات احتيالية، مثل فتح حساب بنكي والقيام بعمليات شرائية بالأسماء المسروقة 2) استخدام أنظمة إلكترونية تهدف إلى تعزيز الأمن السيبراني ولها قدرة أمنية على حماية أمن المعلومات والتحويلات المالية الحساسة، ومتابعة جميع برامج التحديث المتعلقة فيها وإجراءات الوقاية من الاختراق 3) هناك طريقة عملية يمكن اتباعها من أجل تعزيز الحماية التي يمكن أن تقع على عمليات التحويل الإلكتروني للأموال، تتمثل بتوعية الموظفين والعملاء من خلال التدريب المكثف، الذي يعمل على تعريفهم على التهديدات الإلكترونية التي تمس الأموال المحفوظة، وكذلك الأمر يمكن تقديم إرشادات ونصائح للعملاء نفسهم حول كيفية الحفاظ على أموالهم المحفوظة بالبنوك 4) العمل على تعزيز التعاون الدولي لمكافحة الجرائم المالية، والسعي لتحقيق ذلك من خلال تبادل الخبرات والمعلومات من أجل إجراء التحقيقات اللازمة، من أجل تعقب المجرمين عبر الحدود و القبض على الجناة وبعدها تقديمهم للعدالة والقضاء 5) العمل على إجراء مراجعات داخلية ودولية والتأكد من الالتزام بالإجراءات القانونية الخاصة بعمليات التحويل الإلكتروني للأموال والتحقيق ورصد الأنشطة الغير عادية أو المشبوهة 6) لابد من أن تكون الدولة على دراية في الجرائم التي تقع على عمليات التحويل الإلكتروني للأموال، وبالتالي تضع عقوبات رادعة للمجرمين ومن أجل تحقيق ذلك، فلابد من أن يكون هناك تعاون ما بين النظام القضائي والتشريعي والمؤسسات المالية وذلك من أجل تحقيق

أكبر قدر ممكن من العدالة" (الجرائم البنكية: أشكالها وسبل حماية الأموال في عصر الرقمية والتكنولوجيا،، 2023).

ومن طرق حماية النقود الإلكترونية وعمليات التحويل الإلكتروني للأموال من أي اعتداء قد يقع عليها، هي تأمين البيانات ويقصد بها العمل على تشفير المعلومات التي تنتقل عبر الإنترنت، بحيث يعتمد هذا النظام على التأكد أن العميل هو الشخص الحقيقي الذي يتعامل مع الموقع، وهذا بدوره يضمن سرية المعاملات التجارية وأمان الصفقات التي يجريها العميل، بحيث يعتمد هذا النظام على استخدام مفاتيح سرية وطرق حسابية معقدة يحول فيها الرسائل من رسائل مقروءة إلى رسائل يصعب قراءتها ما لم يتم فك الشيفرة الخاصة بها، وهناك مفتاح للتشفير يتم تزويد المستخدم والعميل به، وبالتالي لا يمكن قراءة الرسالة المشفرة إلا بعد فك شيفرتها عن طريق المفتاح العام الخاص بها، وفي حال رغب أي شخص بالدخول للنظام والمعلومات الخاصة به فلابد من إدخال الرقم السري المخصص له (خضير، 2014).

المطلب الثاني: إجراءات الحماية الخاصة بأنظمة وبرامج التحويل الإلكتروني للأموال.

الفرع الأول: الحماية ضد الفيروسات.

لحماية المصارف والمؤسسات المالية من الاختراق أو الاستيلاء على الاموال الموجودة فيها، نظراً لما تسببه من أضرار فادحة وخاصة في ظل تنوع هذه الفيروسات وانتشارها، وما لها من تأثير كبير سواء على سرعة النظام من خلال العمل على إبطاؤه وتقليل سرعته، وما تلحقه أيضاً من أضرار جسيمة على أجهزة الحاسب الآلي من خلال تعطيلها وتدمير ما هو موجود عليها وإبطال عمل جهاز الحاسب الآلي، فهناك بعض من الإجراءات الوقائية التي يمكن إتباعها لحماية البنوك والمؤسسات المالية من جرائم عمليات التحويل الإلكتروني للأموال منها "1) السعي دائماً لشراء البرامج الأصلية وعدم التعامل مع برامج غير معلومة المصدر 2) تجنب القيام بأي عملية نسخ لأي برنامج على جهاز الحاسب الآلي إلا بعد التأكد من أن هذه البرنامج بحالة جيدة 3) العمل دائماً على استخدام برامج تعمل على مسح الفيروسات 4) عدم

التعامل مع أي رابط مجهول الهوية أو مجهول المصدر 5) استخدام برامج لحماية جهاز الحاسب الآلي من جميع أنواع الفيروسات6) إغلاق الجهاز فوراً في حال اكتشاف وجود فايروس أو أن الأمر ليس على ما يرام" (الخشروم، 2005).

إبقاء البرامج ونظام التشغيل دائماً محدثين واستخدام برامج لأمان الإنترنت مثل kaspersky total حيث تعمل مكافحة الفيروسات وحماية النظام من الهجمات أياً كانت، وكذلك فحص التهديدات قبل أن تدخل وتؤثر على النظام والقيام بإزالتها، وبالتالي توفير الحماية لجهاز الكمبيوتر والبيانات الموجودة عليه، بالإضافة إلى استخدام كلمة مرور قوية لا يمكن تخمينها بسهولة، وأيضاً عند وضع كلمة المرور يجب استخدام نظام لإنشائها كي يضع كلمة مرور قوية لحماية البنك أو المؤسسة المالية، وتجنب فتح الرسائل العشوائية حتى لا يدخل على النظام فيروسات ضارة، كذلك الأمر بالنسبة للروابط فلابد من تجنب فتحها، حتى لا نقع محل لجريمة احتيال مالي، وهناك نقطة مهمة تتمثل بتجنب تقديم أي بيانات شخصية تتمثل في الدخل الاقتصادي أو الرأي السياسي أو مكان السكن وغيرها لأي جهة مجهولة المصدر، وفي حال تلقى الشخص مكالمة هاتفية من مصرف أو مؤسسة مالية معينة، وكان هناك شك أن هذا الاتصال لم يكن من المصرف أو البنك أي أن الجاني انتحل شخصية المصرف لابد من قيام الشخص بالاتصال فوراً بالمؤسسة المالية أو المصرف لتأكد من مصدر الاتصال ومن طرق الحماية، أيضاً التأكد من بياناتك المصرفية وسؤال المصرف عن أي معاملات غير مألوفة لتحقق ما إذا كان هناك احتيال أم لا (موقع كاسبرسكي لاب، 2023).

الفرع الثاني: إجراءات تأمين المخاطر التي تحيط بعملية التحويل الإلكتروني للأموال .

بدايةً لابد من المحافظة على السرية التامة في عمليات البنوك والتحول الإلكتروني للأموال، أي المحافظة على السرية التامة لحسابات العملاء ولا يجوز إعطاء أي معلومة سواء بصورة مباشرة أو غير مباشرة عن أحد العملاء أو ما يتوفر من في حسابه من أموال إلا بإذن خطي من صاحب الشأن، وقامت البنوك بوضع قواعد أمان للعمليات المصرفية، وتتمثل هذه القواعد في القيام بالتشفير حيث لا يستطيع أي شخص

غير مصرح له بالدخول بقراءة محتوى الرسالة، بحيث أن المستفيد أو ما يسمى بالمستقبل يقوم باستقبال هذه الرسالة وقراءتها فقط، بالتالي إتمام عملية التحويل الإلكتروني للأموال بطريقة آمنة، وهناك طريقة جديدة للحماية وتسمى بالجدار الناري، وتأتي وظيفته في حماية وحدات التحكم والإرسال في الإنترنت، ويقوم نظام عمله على إجبار جميع عمليات التحويل الإلكتروني للأموال للعبور من خلال هذا الجدار الناري، وبالتالي يقوم بصد الأشخاص والمواقع الغير مرغوب فيها بالدخول، كون الجناة قد يستخدموا طرق متعددة للتجسس على المعاملات التي تنتقل بين العميل والبنك، وهناك عدة أنظمة تتعلق بحماية عمليات التحويل الإلكتروني للأموال، يتمثل النظام الأول بنظام الفيد وير، وهذا النظام معروف لأنه معتمد لدى المصرف الاحتياطي الاتحادي في أمريكا، إذ يقوم بإجراء الاتصالات الهاتفية ويستخدم شيفرة خاصة لمقياس المال وإدخال الرسائل في الجهاز الإلكتروني لمعالجتها وإرسالها إلى الجهة المستلمة، وجميع عمليات التحويل الإلكتروني للأموال تتم عن طريق هذا النظام، وما يميزه أيضاً أنه يجري مكالمات هاتفية، ودولة الأردن تستخدم مثل هذا النظام، أما النظام الثاني وهو نظام التشيب وهو غرفة مقاصة يتم القيام بها في نهاية اليوم وموجودة في جمعية نيويورك لبيوت المقاصة، وأيضاً تستخدمه البنوك الأردنية فهو نظام آمن يقوم على تسهيل وتسريع عمليات التحويل الإلكتروني للأموال من خلال خدمات مدفوعة التجزئة (حمودة، 2021).

الفرع الثالث: الحماية الجنائية في التشريعات الأجنبية لمواقع التحويل المالي الإلكتروني ووسائل الدفع المختلفة.

لا يوجد ما يمنع من الاستعانة بالتشريعات الأجنبية من أجل سن نصوص قانونية أو تعديل النصوص القديمة بما يوفر حماية كافية لعمليات التحويل الإلكتروني للأموال، وخاصة أن ما أحدثته الثورة المعلوماتية من تطور غيّر في المفاهيم القانونية وخاصة في القانون الجنائي، وقد نجحت كثير من الدول في سن تشريعات تواكب هذا التطور في هذا المجال، وقد برزت دول الاتحاد الأوروبي وأمريكا وفرنسا في هذا المجال أولاً: الحماية الجنائية التي وفرها الاتحاد الأوروبي فقام بتأسيس لجنة أوروبية وخصصت قسم

خاص للخبراء في هذه المجال، وقد أعلن المجلس الأوروبي مشروع هذه الاتفاقية بتاريخ 27 إبريل 2000 وتكلم عن الاعتداءات التي تقع على عمليات التحويل الإلكتروني للأموال مثل موقع أمازون، وقد نبهت الاتفاقية المجتمع الدولي كذلك لجرائم عمليات التحويل الإلكتروني للأموال، وكذلك الأمر في أمريكا بسنة 2001 وقعت الولايات المتحدة الأمريكية وتسعة وعشرون دولة على الاتفاقية الصادرة عن المجلس الأوروبي بخصوص جرائم عمليات التحويل الإلكتروني، وقد ركزت الاتفاقية على عدة أمور أهمها مواجهة النشاطات الإجرامية الناتجة عن اختراق الأنظمة بطريقة غير مشروعة، وقد ركزت أيضاً على بذل عناية من قبل الدول المتعاقدة من خلال تجريم الأفعال التي تمس سرية البيانات والأنظمة التي تحميها، وأكدت في النصوص القانونية الخاصة بالاتفاقية على ضرورة تحقيق تعاون دولي للحد من هذه الجرائم العابرة للقارات (خليفة، 2011) .

الفرع الرابع: الحلول الواقعية التي وضعتها البنوك والقطاع المالي مثل المؤسسات المالية لتجنب الاحتيال الإلكتروني أو الاستيلاء على الأموال المخزنة في البنوك.

"1) توفير ما يسمى بالأمن السيبراني ضمن نطاق الخدمات البنكية الإلكترونية والعمل على تحديث ما يسمى بجدران الحماية بشكل دوري ومستمر 2) العمل على استخدام التوقيع الإلكتروني وذلك ضمن أحدث الوسائل، مثل بصمة العين أو البصمة البيومترية؛ وذلك من أجل تجنب التزوير أو انتحال الهوية 3) تجنب الاعتماد على رقم الهوية المدني لوحدها بل جعل الاعتماد بشكل أكبر على التوقيع الإلكتروني المصدق؛ وذلك من خلال اختيار الشخص للتوقيع إلكتروني وبعدها يتم مصادقة هذا التوقيع على بيانات التوقيع الإلكتروني المسجل 3) استخدام الدفع بالطريقة الإلكترونية دون وضع رقم للحساب أو البطاقة من أجل إجراء التحويلات المالية باستخدام التوقيع الإلكتروني المصدق من أجل تحويل الأموال من حساب الشخص إلى حساب بنكي آخر" (الجدران، 2022) .

الفرع الخامس: نصائح عملية مقدمة للعميل لتجنب جرائم عمليات التحويل الإلكتروني للأموال.

"1) تجنب الرد على الاتصالات المختلفة أو وسائل التطبيقات، سواء تلقيت هذه الرسائل عن طريق البريد الإلكتروني أو عن طريق الهاتف ويتمثل محتواها بالربح بمسابقات دولية أو جوائز، حيث يقوموا المجرمين بتزويدهم ببيانات خاصة بالمجني عليه مثل رقم الحساب المصرفي؛ من أجل تحويل الأموال من حسابك لحسابات أخرى من أجل خداع المجني عليه بخدعة استكمال الرسوم، ومن ثم استلام الجوائز والأموال المحولة ففي هذه الحالة يتوجب على العميل إبلاغ البنك مباشرة وعدم التعامل مع هذه الاتصالات 2) المحافظة على السرية وأمن المعلومات حيث تعد هذه المهمة من أولويات البنوك حيث تسعى دائماً للاطلاع على آخر المستجدات؛ من أجل توفير أقصى حماية من الفيروسات، وكذلك التأكد من هوية الشخص قبل السماح له بالدخول، والعمل كذلك على تشفير عمليات التحويل الإلكتروني للأموال، وتطبيق نظام الجدران النارية وأجهزة الحماية الخاصة بالأمن 3) استخدام كلمة مرور من ٨ خانات، وجعلها قوية تحتوي على حروف وأرقام ورموز مثل #@$؛ من أجل عدم تمكن الجاني من اختراقها بسهولة وعدم الإفصاح عنها لأي أحد، حتى ولو كان قريباً أو استخدامها وتركها على جهاز يستخدمه العامة، والعمل على تغيرها بشكل دوري، وعند وضعها لابد من أن تكون صعبة التخمين ولابد من أن لا يتم التكرار فيها، في بعض المواقع تقدم خدمة تذكير لكلمة المرور في حال نسيانها، فبالتالي لابد من الحذر من اختيار خانت تذكير كلمة المرور بحيث لا يمكن تخمينها، وعند استخدام كلمة مرور وكان هناك كلمة جديدة لابد أن تختلف عن القديمة، وفي حال وجود أشخاص آخرون يقفون في نفس المكان تجنب إدخالها حتى لا يتمكنوا من سرقة هذه الكلمة" (موقع بنك الاسكان، 2023).

الخاتمة

تعتبر جرائم عمليات التحويل الإلكتروني للأموال هي جرائم العصر، وعلى الرغم من صعوبة الموضوع؛ وذلك لأن القليل من الدول من تنبهت لخطورة هذا الموضوع من خلال سن تشريعات تكفل الحماية لعمليات التحويل الإلكتروني للأموال، إلا أن الباحثة حاولت بكل مجهودها طرح الموضوع بطريقة سلسة يفهما القارئ ووضع حلول فنية وتشريعية للحد من هذه الجرائم، وقد ظهر خلال الدراسة أن دول الاتحاد الأوروبي هي كانت السباقة لحل هذه المشكلة من خلال قوانين كفيلة بتوفير الحماية، وبالتالي لا مانع من استعانة الدول ومنها فلسطين بهذه التشريعات لتحسين تشريعاتها الداخلية بما يلائم التطورات التكنولوجية، ولإنقاذ وحماية عملية التحويل الإلكتروني للأموال سواء على المستوى الوطني أو الدولي.

النتائج:

1) إن التحويل الإلكتروني للأموال أصبح من أمور العصر الحديث، حيث أن كثرة استخدامه خاصة في الوقت الحالي نبه العديد من الدول لسن تشريعات تنظم وتجرم الاعتداء على عمليات التحويل الإلكتروني للأموال ونتيجة لذلك انقسمت الدول إلى قسمين، القسم الأول سن تشريعاً خاصاً للجرائم التي تقع على عمليات التحويل الإلكتروني للأموال وذلك انطلاقاً من الطبيعة الخاصة بتلك الجرائم، والقسم الثاني لم يسن تشريع خاص للجرائم التي تقع على عمليات التحويل الإلكتروني للأموال.

2) تعتبر عمليات التحويل الإلكتروني للأموال من أهم العمليات وأكثرها انتشاراً في الوقت الحالي، ولكن قانون التجارة الأردني والساري في فلسطين لم يضع نصوصاً خاصة تنظم عمليات التحويل الإلكتروني للأموال، وبالتالي اجتهد الفقهاء والقضاء في إيجاد نصوص بديلة لتنظيم هذه العملية سواء بالقرار بقانون بشأن الجرائم الإلكترونية والقرار بقانون بشأن المعاملات الإلكترونية والقرار بقانون الخاص بغسل الأموال وتمويل الارهاب.

3) حمى التشريع الفلسطيني عمليات التحويل الإلكترونية للأموال عن طريق وضع شروط خاصة على القائمين بأعمال التحويل من المؤسسات المالية، فكان من أهم الشروط هو الحصول على الترخيص وذلك من أجل حماية المواطنين من الخداع والحرص على أموالهم، أما على مستوى البنوك فهناك اجراءات احتياطية تتبعها البنوك، وذلك كالمصادقة على أوامر الدفع المتمثلة في الإجراءات الاحتياطية، مثل توفير حماية عالية وتشفير عالي حتى تكون الحوالات في مأمن من الغش والاعتراض

4) قام التشريع الفلسطيني بتوفير الحماية القانونية سواء بطرق مباشرة أو غير مباشرة، مثل تجريم الاعتداءات على عمليات التحويل الإلكتروني للأموال، وذلك وفقاً لنصوص المواد التي جرمت ارتكاب الأفعال التي تشكل جرماً على عمليات التحويل الإلكتروني للأموال، كتجريم الاحتيال الإلكتروني وتشمل إدخال البيانات غير صحيحة أو تعليمات غير المشروع التصريح بها، أو استعمال بيانات وعمليات غير مصرح للوصول إليها بغية السرقة وخرق البرامج.

5) إن عمليات التحويل الإلكتروني للأموال بالرغم من الإيجابيات التي حققتها إلا أنها سلاح ذو حدين، فمن جهة تعتبر طريقة آمنة وسريعة وسهلة الاستخدام، ومن جهة أخرى وفرت أدوات تكنولوجية لارتكاب جرائم على هذه العمليات.

6) إن الدليل الرقمي مهم في معرفة كيفية ارتكاب الجريمة وإثباتها، وأنه يتم الاستعانة بالخبراء المختصين في المجال الرقمي لاستخراجه، ويتميز عن الدليل المادي للجرائم التقليدية أنه لا يمكن التخلص منه بسهولة ويمكن إعادة البيانات باستخدام برامج خاصة.

التوصيات:

1) وضع قضاة ذوي اختصاص معمق في هذا النوع من الجرائم، لأنها تمتاز بالدقة والتعقيد وتحتاج إلى فهم أساليب وتقنيات إلكترونية، حتى لو تم الاستعانة بخبير لتقدير الأدلة، إلا أنه من الأجدر والأفضل أن يكون القاضي على إطلاع وعلم كافي بهذه التقنيات، فوجود كادر قضائي متخصص يعمل على تحسين الأحكام وضمان وتحقيق العدالة

2) تفعيل دور نظام التبادل الإلكتروني للبيانات المالية، ويقصد به عدم قصر عمليات التحويل الإلكتروني للأموال على النقود المالية فقط، بل تمتد أيضاً على المعلومات التي تتعلق بمصدر هذا المال أي من أين تم تحصيل هذه المبالغ.

3) توعية أفراد المجتمع من المخاطر التي قد تواجههم جراء التعامل مع أي روابط أو أي أحد يقوم بطلب الكلمات السرية الخاصة بهم أو أي رسالة قد تصل لهواتفهم، فهذه من الطرق الاحتيال الإلكتروني المنتشرة في الوقت الحالي بشكل كبير، حيث يحاول الكثير من المحتالين التلاعب والكذب وخداع المواطنين وذلك للحصول على الأموال بأي طريقة كانت، فعلى الدولة عمل دورات تثقيفية لأفراد المجتمع منها المدارس والجامعات والمعاهد وذلك لتجنب وقوعهم في مثل هذه المصيدة.

4) فرض عقوبات مالية كبيرة على الجناة الذين يرتكبون جرائم على عمليات التحويل الإلكتروني، بالإضافة لعقوبة الحبس وجعلها ظرف مشدد والمصادرة أيضاً، وذلك من أجل تحقيق الإيلام للجاني وإخضاعه لعقوبة رادعة من خلال تطبيق مبدأ الجزاء من جنس العمل، كونه استولى على مبالغ مالية من تنفيذ جريمته بالتالي عقوبته من نفس ما أجنى.

5) العمل على تدريب الكوادر البشرية الموجودة في فلسطين على طريقة كشف الجرائم التي تقع على عمليات التحويل الإلكتروني للأموال وطرق التعامل معها وجمع الأدلة الإلكترونية والمحافظة عليها،

وطرق تحويل الدليل الإلكتروني لدليل مادي ملموس مثل تخزينه على قرص صلب حتى تتمكن النيابة من تقديمه للمحكمة والاستناد عليه للإدانة.

المراجع العلمية

ابراهيم، قاسم. (21 مارس، 2020). 7 إجراءات لتتبع الأموال القذرة. *مجلة اليوم السابع*.

ابراهيم، محمد فوزي. (اغسطس، 2018). دور مأمور الضبط القضائي في الحصول على الدليل الرقمي. *مجلة البحوث القانونية والاقتصادية*، صفحة 110.

الاستخبارات العسكرية الفلسطينية. (2022). *من أنواع الجرائم الإلكترونية التي يعاقب عليها القانون* . تم الاسترداد من الإستخبارات العسكرية الفلسطينية:

https://www.pmi.pna.ps/pmia/pmia/%D9%85%D9%86-%D8%A7%D9%86%D9%88%D8%A7%D8%B9-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-/%D8%A7%D9%84%D8%AA%D9%8A-%D9%8A%D8%B9%D8%A7

إسكندر، ماهر. (5 يناير، 2022). *حجية الدليل الرقمي في الأثبات الجنائي* . تم الاسترداد من

https://eg.andersen.com/%D8%AD%D8%AC%D9%8A%D8%A9-%D8%A7%D9%84%D8%AF%D9%84%D9%8A%D9%84-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A-%D9%81%D9%89-%D8%A7%D9%84%D8%A7%D8%AB%D8%A8%D8%A7%D8%AA-%D8%A7%D9%84%D8%AC%D9%86%D8%A7%D8%A6%D9%89/

الأغا، أمجد نعيم. (2023). التجريم التشريعي للاحتيال والنصب المستحدث.

أفضل 4 خدمات تحويل الأموال عبر الإنترنت في 2023. (2023). تم الاسترداد من موقع سلة، المملكة العربية السعودية:

https://salla.com/%D8%AA%D8%AD%D9%88%D9%8A%D9%84-%D8%A7%D9%84%D8%A3%D9%85%D9%88%D8%A7%D9%84-%D8%B9%D8%A8%D8%B1-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA/

انترناشيونال، كادو ريم. 2023 *شروط عامة لخدمات تحويل الأموال عن بُعد*. موريتانيا.

البداينة، ذياب. (2014). الجرائم الالكترونية: المفهوم والأسباب. عمان الاردن: كلية العلوم الاستراتيجية.

بشير، فايز خضر. الحجار، عدنان إبراهيم. (تشرين الأول، 2021). الأدلة الرقمية وإثبات الجرائم السبرانية ما بين الاصيل والتأويل. *مجلة جامعة الإستقلال للأبحاث*.

البغدادي، أدهم باسم. (2018). *وسائل البحث والتحري عن الجرائم الإلكترونية*. فلسطين: دار المنظومة.

البلوشية، احلام بنت محمد بن علي. (2018). *المواجهة الجزائية للاحتيال المعلوماتي*. عمان: المنظومة.

بن غانم، اسامة. (2019). *الاتجاهات الحديثة في تجريم الاحتيال المعلوماتي*.

بوعديس، سارة. (2017). *لمسؤولة القانونية للبنوك في عملية التحويل الالكتروني للأموال*.

البوعين، المستشار عبد الله. (2008). *قرات بتخصيص محكمتين جنائيتين لنظر في جرائم الاتجار بالاشخاص والجرائم المالية وغسيل الأموال*،. تم الاسترداد من https://www.sjc.bh/page_016.php?pID=708

بوقادي، هديل ، أوشن، شيماء. (2022). *التحويل الالكتروني للاموال في العمليات المصرفية*،. جامعة العربي بن مهيدي،.

بيرم، غزل. (2021). جريمة الاحتيال الالكتروني.

التحقيق في الجرائم الالكترونية واثباتها في فلسطين دراسة مقارنة . جامعة المجهر الوطني (2016)..

تقرير التطبيقات حول غسيل الاموال عبر الوسائل الالكترونية. (ديسمبر، 2017). تاريخ الاسترداد 2023، من https://www.menafatf.org/sites/default/files/Newsletter/MLE-AR.pdf

تقرير التطبيقات حول غسيل الاموال عبر الوسائل الالكترونية. (ديسمبر، 2017). تاريخ الاسترداد 2023، من https://www.menafatf.org/sites/default/files/Newsletter/MLE-AR.pdf

التكروري، عثمان. (2020). *لتحويل المصرفي*.

توريه، ديش. (2020). *جريمة تبيض الاموال عبر الانترنت وانعكاسها على الاقتصاد المحلي والعالمي*.

توفيق، على ابراهيم. (22 1، 2023). *دور المحقق في الجرائم الالكترونية* . تم الاسترداد من موقع جمهورية العراق مجلس القضاء الأعلى: https://sjc.iq/view.70533/

جامعة النجاح الوطنية . (2016). *حكم محكمة استئناف رام الله رقم 419 لسنة 2016*. تاريخ الاسترداد 2023، من موقع جامعة النجاح الوطنية : https://maqam.najah.edu/judgments/3344/

جامعة النجاح الوطنية. (2017). *الاشكاليات الموضوعية والاجرائية في النظام القانوني الفلسطيني في الجرائم الالكترونية*. نابلس.

جامعة النجاح الوطنية. (2019). *موقع جامعة النجاح الوطنية* . تاريخ الاسترداد 2023، من https://maqam.najah.edu/judgments/7258/

الجدران، يحيى. (29 اغسطس، 2022). *الاحتيال الالكتروني.. وقطاعات البنوك، الشرق الأوسط*. تاريخ الاسترداد 2023، من

https://www.alarabiya.net/aswaq/opinions/2022/08/29/%D8%A7%D9%84%D8%A7%D8%AD%D8%AA%D9%8A%D8%A7%D9%84-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%88%D9%82%D8%B7%D8%A7%D8%B9-%D8%A7%D9%84%D8%A8%D9%86%D9%88%D9%83

الجرائم البنكية: أشكالها وسبل حماية الأموال في عصر الرقمية والتكنولوجيا. (5 يوليو، 2023). تم الاسترداد من موقع ودق القانونية:

https://wadaq.info/%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A8%D9%86%D9%83%D9%8A%D8%A9-%D8%A3%D8%B4%D9%83%D8%A7%D9%84%D9%87%D8%A7-%D9%88%D8%B3%D8%A8%D9%84-/%D8%AD%D9%85%D8%A7%D9%8A%D8%A9

جريس، حسام. (بلا تاريخ). *المحفظة الرقمية أو الالكترونية، مجلة التربية المالية- من الكلية الأكاديمية أونو*.

جمعية عرق الخيرية. (2019). *سياسة الوقاية من عمليات غسيل الأموال وجرائم الإرهاب*. تم الاسترداد من وزارة العمل والتنمية الاجتماعية:

https://irqahorg.sa/%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9-%D8%A7%D9%84%D9%88%D9%82%D8%A7%D9%8A%D8%A9-%D9%85%D9%86-%D8%B9%D9%85%D9%84%D9%8A%D8%A7%D8%AA-%D8%BA%D8%B3%D9%8A%D9%84-%D8%A7%D9%84%D8%A3%D9%85%D9%88%D8%A7%D9%84-/%D9%88

الحجار، عدنان. و بشير، دفايز. (2021). الأدلة الرقمية واثبات الجرائم السيبرانية ما بين التأصيل والتأويل. جامعة الاستقلال.

حمادي، رفعت. (22 اكتوبر، 2021). *حماة الحق*. تم الاسترداد من الضبط في الجرائم الإلكترونية: https://jordan-lawyer.com/2021/10/22/seizure-in-cybercrime/

حمود، أحمد وآخرون. (2015). *الأدلة الالكترونية*.

حمودة، خالد جبر. (2021). المسؤولية الالكترونية للبنك عن التحويلات المالية. الاردن.

حميد، جاسم خريبط خلف حسن حماد. 2010، *جريمة إساءة استخدام بطاقات الائتمان الإلكترونية الملغاة*. تم الاسترداد من مجلة جامعة بابل: مجلد 18 عدد2 .

حميد، رافع عبد الله. (2022). جريمة سرقة النقود الالكترونية.

الخشروم، عبدالله. (2005) أثر قانون المعاملات الالكترونية الاردني على عمليات البنوك.

خلف، مازن. (2017). *الإجراءات الخاصة بالضبط والتفتيش*. جامعة المستنصرية.

خليفة، مريم. (2011). الحماية الجنائية لمواقع التجارة الالكترونية عبر الانترنت، كلية الحقوق والعلوم السياسية. الجزائر: مجلة العلوم القانونية جامعة بشار..

الخليلي، أحمد. (2006). *غسيل الاموال عبر الانترنت: دراسة مقارنة(الاردن، مصر، الامارات)*.

دهشان، يحيى ابراهيم. (سبتمبر، 2023). الحماية الجناية للبيانات في ظل التحول الرقمي. *مجلة الدراسات القانونية والإقتصادية*.

ذوابة، محمد عمر. (2006). *عقد التحويل المصرفي الإلكتروني (دراسة قانونية مقارنة)* (المجلد ط1). عمان: دار الثقافة للنشر والتوزيع.

راشد، عايض. (2022). *التحويل الالكتروني للأموال دراسة مقارنة.* الكويت: مجلة كلية القانون الكويتية العالمية.

ربايعة، عبد اللطيف محمود. (2016). *الجرائم الالكترونية(التجريم والملاحقة والاثبات).* نابلس.

رجاء، رجاء. (2018). مفهوم الدليل الرقمي. *الملتقى الدولي حول أدلة الإثبات الجنائية الحديثة في التشريعات المقارنة.* الجزائر.

ريد، كايتلن. (2017). أضرار التحويلات المالية.

زخوفي، نور الدين عمر زمالة. (2018). مجلة الاقتصاد الدولي والعولمة .

الزين، سليمان ضيف الله. (2019). *التحويل الالكتروني للأموال ومسؤولية البنوك القانونية،.* الاردن.

سعدة، جامعة. (2018). الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية . تأليف عيدة بلعابد.

السلامة السيبرانية والأمن السيبراني. (بلا تاريخ). تاريخ الاسترداد 2023، من قانون مكافحة الشائعات والجرائم الإلكترونية: https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

سلطة النقد الفلسطينية. (2017). *دليل إجراءات مكافحة غسيل الاموال وتمويل الارهاب الخاص بالمصارف.* تم الاسترداد من سلطة النقد الفلسطينية: https://www.pma.ps/Portals/0/Users/002/02/2/Anti%20Money%20Launde

ring/Arabic/AML-CFT%20Manual%20for%20Banks.pdf?ver=2017-05-timestamp=1660216396348&25-141854-313

سمير، مينا. (5 مايو، 2021). *مراحل سير الدعوى الجزائية*. تم الاسترداد من https://www.almrsal.com/post/1074540.

السوفي، نور الهدى. (2017). *التحقيق في الجريمة المعلوماتية*. ورقلة: دار المنظومة.

السيد، هبة. (2022). مستخدمي المحفظة الإلكترونية للمحمول خمس طرق لتحويل واستقبال الأموال. *صحيفة اليوم السابع*.

شاهين، وكيل نيابة مكافحة الجرائم الإقتصادية عامر. (14 5، 2024). التحويل الإلكتروني للأموال. (التصدي لجرائم التحويل الإلكتروني للأموال والقصور التشريعي، المحاور) جنين.

شبول، شاكر. (2023). الحماية الجنائية لوسائل الدفع الإلكتروني دراسة مقارنة. *مجلة جرش للبحوث والدراسات*.

شديد، مراد تيم فادي. *الجزاءات غير الجزائية في الجرائم الاقتصادية*. 2017.

الشديدي،، يحيى. (2016). الشهادة في الجريمة الإلكترونية. *مجلة جامعة البعث*، صفحة 52.

الشعار، خالد. (2022). *التحقيق الجنائي في الجرائم الإلكترونية*. بحث مقدم للحصول على درجة الدكتوراه في الحقوق في جامعة المنصورة.

شقيرات، طارق. (2005). *مسؤولية البنوك في التحويل الإلكتروني للأموال دراسة مقارنة في التشريع الأردني*.

شنين، صالح. (2013). الحماية الجنائية للتجارة الالكترونية،.

شهاب، احمد عبد الكريم عبد الرحمن. (2018) شروط قبول الدعوى الجزائية امام القضاء الجنائي الفلسطيني.

صالح، نبيه. (2006). *شرح مبادئ قانون الإجراءات الجزائية الفلسطيني*. القدس: مكتبة دار الفكر.

طارق شقيرات. (2005). *مسؤولية البنوك في التحويل الالكتروني للاموال دراسة في التشريع الاردني*. الاردن .

الطريف، غادة عبد الرحمن. نصيرات، وائل محمد. (2018). *جريمة الاحتيال عبر شبكة المعلومات الدولية دراسة مقارنة النظام السعودي والقانون الأردني*. السعودية: دفاتر السياسة والقانون.

طعن جزائي رقم 256 لسنة 2016 .

عبد الجبوري، سامر سلمان. (2014). *جريمة الاحتيال الإلكتروني (دراسة مقارنة)*. بغداد: جامعة النهرين.

عبد الحميد، محمد. (7 سبتمبر، 2022). *المسؤولية الجزائية للشخص المعنوي على المال العام*. تم الاسترداد من حماة الحق، محامي الاردن: https://jordan-lawyer.com/2022/09/07/%D8%A7%D9%84%D9%85%D8%B3%D8%A6%D9%88%D9%84%D9%8A%D8%A9-%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D9%8A%D8%A9-%D9%84%D9%84%D8%B4%D8%AE%D8%B5-%D8%A7%D9%84%D9%85%D8%B9%D9%86%D9%88%D9%8A-%D8%B9%D9%84%D9%89/

عبد الرحيم، صباح ، عبد الرحيم، هبة. (2017). جرائم التجارة الالكترونية، .

عبد السلام، أحمد. (12 اغسطس، 2021). *مراحل الدعوى الجزائية في القانون الاردني*. تم الاسترداد من https://jordan-lawyer.com/2021/08/12/criminal-case-stages-in-jordan-law/.

عبدالباقي، مصطفى. (2018). *التحقيق في الجرائم الالكترونية واثباتها في فلسطين: دراسة مقارنة*. بيرزيت.

عبدالله، ليندة. (2017). *تبيض الأموال عن طريق الاعتماد المستندي الالكتروني*. طرابلس.

العتوم، حنين. (2021). *ما هي أنواع الحوالات وتقسيماتها؟*

العتوم، حنين. (2021). *ماهي سلبيات الحوالة البنكية؟*

العجمي، عبد الله. (2014). *المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة*.

عرب، لامية. (2021). *أحكام منازعات التحويل الدولي للأموال*،.

العربيد، نضال، وآخرون. (2022). *المحاسبة المصرفية*.

العزي، خالد. (2017). الجرائم المالية الالكترونية الجرائم المصرفية،.

عطا الله، .شيماء عبد الغني. (2024). *بحث قانوني ودراسة واسعة عن مكافحة جرائم المعلوماتية في المملكة السعودية*. جامعة الملك سعود، كلية الحقوق والعلوم ال'نسانية ، السعودية.

علي، علاء أحمد. (9 اغسطس، 2018). *مكونات الحاسب الآلي المادية والمعنوية*. تم الاسترداد من موضوع:

https://mawdoo3.com/%D9%85%D9%83%D9%88%D9%86%D8%A7%D8%AA_%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D8%A8_%D8%A7%D9%84%D8%A2%D9%84%D9%8A_%D8%A7%D9%84%D9

%85%D8%A7%D8%AF%D9%8A%D8%A9_%D9%88%D8%A7%D9%
84%D9%85%D8%B9%D9%86%D9%88%D9%8A%D8%A9

علي، محمد محرم محمد. (2003). جريمة النصب والتجارة الالكترونية.

عموري، أشرف أحمد مصطفى.(2018). *التفتيش في الجرائم الإلكترونية*. القدس: جامعة القدس.

العيسى، عاصم. (11 أبريل، 2021). اختراق الحسابات والبطاقات النكية مسؤولية من؟ *صحيفة مال*.

الغانمي، خضير مخيف فارس. (2016). *النظام القانوني للتحويل الإلكتروني للنقود دراسة مقارنة* (المجلد ط1). القاهرة: المركز القومي للإصدارات القانونية.

غزوي، محمد فهمي. (2021). *ماهية عقد التحويل الالكتروني للأموال وآثاره بواسطة البنوك التجارية الاردنية*. الاردن: جامعة الزيتونة الاردنية، ص 285.

غنام، محمد جواد محمد. (2023). *اجراءات التحقيق الابتدائي في الجريمة الإلكترونية*. جنين: دار المنظومة.

فاروق، ياسر الأمير. (24 اغسطس، 2021). *الجريمة السيبرانة وحماية اموال العملاء*. تم الاسترداد من https://www.youm7.com/story/2021/8/24/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%88%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A3%D9%85%D9%88%D8%A7%D9%84-%D8%A7%D9%84%D8%B9%D9%85%D9%84%D8%A7%D8%A1-%D

فوزي، عبد الكريم. (2005) *أثر قانون المعاملات الالكترونية الاردني على عمليات البنوك*.

الفيل، علي عدنان. (ديسمبر، 2010). إجراءات التحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة. *مجلة البحوث والدراسات العربية*.

فيله، فيله. (2007). *بوابة انترنت جديدة لتسهيل عملية تحويل الأموال من ألمانيا*. ألمانيا.

قابوسة، علي. (2017). الجريمة الالكترونية في الفضاء الالكتروني،. ليبا.

قانون 27 جوان 2005 المتعلق بالتحويل الإلكتروني للأموال التونسي، المادة 17 .

قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة2001.

قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة2001.

قانون التجارة الأردني رقم 12 لسنة 1966.

قانون التجارة الأردني رقم 12 لسنة 1966.

قانون التجارة المصري رقم 17 لسنة 1999.

قانون التجارة المصري رقم 17 لسنة 1999.

قانون العقوبات رقم 16لسنة 1996 المادة 14 .

قانون العقوبات رقم 16لسنة 1996 المادة 14 .

قانون المعاملات التجارية الإماراتي رقم 18 لسنة 1993.

قانون المعاملات التجارية الإماراتي رقم 18 لسنة 1993.

قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 مادة 24.

قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 مادة 24.

القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية.

القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية.

قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الالكترونية (الفصل الخامس والسادس).

قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الالكترونية (الفصل الخامس والسادس).

قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية (الفصل الخامس والسادس).

القرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية .

القرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية .

قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية.

قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية.

القرار بقانون رقم 39 لسنة 2022 بشأن مكافحة غسيل الأموال وتمويل الإرهاب.

القرار بقانون رقم 39 لسنة 2022 بشأن مكافحة غسيل الأموال وتمويل الإرهاب.

قرار بقانون رقم 41 لسنة2022 بشأن المدفوعات الوطني.

قرار بقانون رقم 41لسنة2022 بشأن المدفوعات الوطني.

قرار رقم 1106379 الصادر بتاريخ 2022/6/9 عن المحكمة العليا في الجزائر، .تم الاسترداد من https://www.coursupreme.dz/%D9%85%D9%84%D9%81-%D8%B1%D9%82%D9%85-1106379-%D9%82%D8%B1%D8%A7%D8%B1-%D8%A8%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE-09-06-2022/%D8%A7%D9%84%D8%BA%D8%B1%D9%81-

%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D9%8A%
D8%A9/%D9%85%D9%86-%D9%82%D8%B1%D8%

قرار لمحكمة النقض رقم 676 لسنة 2019 الصادر بتاريخ 28- يونيو، 2020 . تم الاسترداد من
/https://maqam.najah.edu/judgments/7258

قرار لمحكمة النقض رقم 676 لسنة 2019 الصادر بتاريخ 28- يونيو، 2020 . تم الاسترداد من
/https://maqam.najah.edu/judgments/7258

قرار محكمة استئناف رام الله رقم 551 لسنة 2017.

قرار محكمة النقض رقم 17 لسنة 2022 الصادر بتاريخ 30 يناير 2022 (بلا تاريخ). تم الاسترداد من
https://l.facebook.com/l.php?u=https%3A%2F%2Fmaqam.najah.edu%2Fj
udgments%2F8221%2F%3Ffbclid%3DIwAR3B9Y_7hJQFennYLTeCrY
h=AT01rH2-&ytCYZwW97sjHRbG5mq9xbAc3gem1J1-1yP9LY
BeQTUJ_gRi3Ecip9r7zJ3A3PhmgAND0jESRDXYKuSdJyvOpNGtzSo5
OLS3mhewGaeob0My4rer4xiXb4EEtmaBbpe

القهيوي، عمر محمود حمدان. (2023). *اجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية.* عمان: جامعة شرق الأوسط.

كيف يستغل مبيضو الأموال التكنولوجيا الحديثة لتنفيذ جرائمهم؟ (2021). تم الاسترداد من موقع الجزيرة:
https://www.aljazeera.net/ebusiness/2021/5/7/%D9%83%D9%8A%D9%8
1-%D9%8A%D8%B3%D8%AA%D8%BA%D9%84-
%D9%85%D8%A8%D9%8A%D8%B6%D9%88-
%D8%A7%D9%84%D8%A3%D9%85%D9%88%D8%A7%D9%84-
%D8%A7%D9%84%D8%AA%D9%83%D9%86%D9%88%D9%84%D9
%88%D8%AC%D9%8A%D8%A7

لميزا، امينة. 2023 الدليل الرقمي كالية لاثبات الجرائم المعلوماتية، . الجزائر: جامعة محمد بوقرة بومرداس.

لنقرش، أمجد. البنيان القانوني لجريمة غسيل الاموال،. جامعة العلوم التطبيقية في مملكة البحرين .

المادة 18 من القانون 27 جوان 2005 المتعلق بالتحويل الإلكتروني للأموال .

المادة 18 من القانون 27 جوان 2005 المتعلق بالتحويل الإلكتروني للأموال .

مانع، سلمى. (2011). *التفتيش كاجراء للتحقيق في الجرائم المعلوماتية*. جامعة محمد خيضر.

محمد عمر، عمر، ذوابة، . 2006 *عقد التحويل المصرفي الالكتروني*،.

محمد، سمية عبد العاطي. (2022). *التحويل الإلكتروني دراسة فقهية مقارنة*. الإسكندرية، مصر.

محمود، أكرم محمد. (5 نوفمبر، 2021). *حجية الاعتراف في الجرائم الإلكترونية*. تم الاسترداد من حُماة الحق للمحاماة: https://jordan-lawyer.com/2021/11/05/admission-in-cybercrime/

المرجان، عبد الرزاق بن عبد العزيز. (6 يناير ، 2022) *نظام الاثبات يحول الدليل الرقمي الى دليل اصلي*.

المركز الديمقراطي العربي. (9 اغسطس، 2016). *الجرائم الالكترونية "الأهداف–الأسباب–طرق الجريمة ومعالجتها"* . تم الاسترداد من https://democraticac.de/?p=35426

المري، عايض راشد. (15 اوكتوبر، 2019). التحويل الإلكتروني للأموال دراسة مقارنة. *مجلة كلية القانون الكويتية العالمية*.

مسار. (11 يناير، 2012). *أعمال الخبرة الفنية في ضوء قانون الجريمة الإلكترونية*. تم الاسترداد من مسار: https://masaar.net/ar/%D8%A3%D8%B9%D9%85%D8%A7%D9%84-

%D8%A7%D9%84%D8%AE%D8%A8%D8%B1%D8%A9-
%D8%A7%D9%84%D9%81%D9%86%D9%8A%D8%A9-
%D9%81%D9%8A-%D8%B6%D9%88%D8%A1-
%D9%82%D8%A7%D9%86%D9%88%D9%86-
/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A

مسؤولية المصرف عن تقديم معلومات الائتمان المالي. (12 ابريل، 2023). تم الاسترداد من mrlatalib.com: https://mrlatalib.com/89

المصري، نداء. (2017). خصوصية الجرائم المعلوماتية.

المعايطة، حمزة عاطف. (2012). *جريمة الاحتيال الإلكتروني*. عمان: جامعة مؤته.

الموسوي، نهى خالد ، خضير، اسراء. (2014). النظام القانوني لنقود الالكترونية. بابل: جامعة بابل.

موسى، ايثار. (24 مايو، 2023). *مراحل سير الدعوى الجزائية* . تم الاسترداد من https://www.mohamah.net/law/%D9%85%D8%B1%D8%A7%D8%AD%
D9%84-%D8%B3%D9%8A%D8%B1-
%D8%A7%D9%84%D8%AF%D8%B9%D9%88%D9%89-
%D8%A7%D9%84%D8%AC%D9%86%D8%A7%D8%A6%D9%8A%
./D8%A9

موقع البنك الاستثمار الفلسطيني. (2023). *الشروط والأحكام لتطبيق المحفظة الالكترونية من بنك الاستثمار الفلسطينيpin*.

موقع البنك الاسلامي العربي. 2023 *لحوالات السريعة ويستر يونون، شروط تحويل الأموال عبر ويستر يونيون*.

موقع *النيابة العامة الاتحادية* . (2020). تاريخ الاسترداد 2023، من https://www.pp.gov.ae/webcenter/portal/PublicProsecutionPortal/pages_aboutprosecution/crimecase.

موقع بنك الاسكان. 2023 *نصائح خاصة بأمن المعلومات.* تم الاسترداد من موقع بنك الاسكان : https://hbtf.ps/ar/information-security-tips

موقع جامعة النجاح. (2018). حكم *محكمة النقض رقن 33 لسنة 2018.* تاريخ الاسترداد 2023، من https://maqam.najah.edu/judgments/7927/

موقع سايبر ون. (4 12، 2021). *أسباب الجريمة الالكترونية*. تاريخ الاسترداد 2023، من سنايبر ون: https://cyberone.co/%D8%A7%D8%B3%D8%A8%D8%A7%D8%A8-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9/

موقع صناع المال. (2023). *كيفية التحويل عن طريق ويسترن يونيون.*

موقع كاسبرسكي لاب. 2023 *ما هي الجريمة الالكترونية؟ كيف تحمي نفسك من الجرائم الالكترونية* . تاريخ الاسترداد 2023، من https://me.kaspersky.com/resource-center/threats/what-is-cybercrime

موقع مقام . (26 ديسمبر، 2016). *القضية رقم 2016/419 المنعقدة في محكمة استئناف رام الله*. تاريخ الاسترداد 10، 2023، من موقع مقام: https://maqam.najah.edu/judgments/3344/

موقع مقام . (3 مايو ، 2021). *القضية رقم 2021/53 المنعقدة في محكمة النقض*. تاريخ الاسترداد 2023، من موقع مقام : https://maqam.najah.edu/judgments/7852/

موقع مقام. (27 سبتمبر، 2018). *أحكام قضائية*. تاريخ الاسترداد 2023، من مقام: https://maqam.najah.edu/judgments/3/

موقع مقام. (7 فبراير، 2022). *أحكام قضائية*. تاريخ الاسترداد 2023، من موقع مقام:

موقع وكالة عمون الاخبارية. (6، 2023). *الفرق بين التحقيق الابتدائي والتحقيق النهائي*. تم الاسترداد من https://www.ammonnews.net/article/738022

ناصر، رامي يوسف محمد. (2010). *المسؤولية الجزائية للشخص المعنوي عن الجرائم الإقتصادية*.

نجيب، هند. (نوفمبر، 2018). ضبط الأدلة في الجرائم الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة. *المجلة الجنائية القومية*.

النص الكامل لمشروع قانون الجرائم الالكترونية الأردني الجديد. (27 يوليو، 2023). تاريخ الاسترداد 16 2، 2024، من موقع البابور: https://albaboor.com/ar/archives/69494

النص الكامل لمشروع قانون الجرائم الالكترونية الأردني الجديد. (27 يوليو، 2023). تاريخ الاسترداد 16 2، 2024، من موقع البابور: https://albaboor.com/ar/archives/69494

نور الدين، زمالة عمر زخرف. (2018). التحويل المالي الإلكتروني :آليات التعامل والمحاطر في ظل عصرنة وسائل الدفع. *مجلة الإقتصاد الدولي والعولمة*، صفحة 249.

الوصيفي، اية. (2023). قراءة في جريمة التحويل الالكتروني غير المشروع للاموال.

وقع كدوريم،. 2023 *شروط عامة لخدمات تحويل الأموال عن بُعد*. مورتانيا .

وكيل النيابة الإقتصادية عامر شاهين. (14 5، 2024). التحويل الإلكتروني للأموال. (ضبط وجمع الإستلادلات في جرائم التحويل الإلكتروني للأموال، المحاور) جنين.

ياخور، دريس. 2016). أحكام مكافحة جريمة الطبي الأموال في التشريع الجزائري. جامعة إدرار، العدد 6.

يوسف، معاذ. (2021). *الحوالات البنكية أم باي بال : أيهما أفضل لسحب أرباحك من مستقل؟*.

Kaspersky *ما مدى أمان تحويل الأموال الكترونياً؟*(2023) .

An-Najah National University

Faculty of Graduate Studies

CRIMINAL PROTECTION FOR ELECTRONIC MONEY TRANSFER OPERATIONS IN CURRENT PALESTINIAN LEGISLATION

By

Lamis Tayseer Mahmoud Lahlouh

Supervisor

Dr. Fadi Shadeed

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Criminal Law, Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine.

2024

CRIMINAL PROTECTION FOR ELECTRONIC MONEY TRANSFER OPERATIONS IN CURRENT PALESTINIAN LEGISLATION

by
Lamis Lahlouh

Supervisor
Dr. Fadi Shadeed

Abstract

In my study, I examined the topic of criminal protection for electronic money transfer operations within the current legislation in Palestine, employing a descriptive and analytical approach. The study is structured into two chapters. The first chapter focuses on the objective criminal rules designed to protect electronic money transfer operations, addressing the nature of these operations and the various forms of objective criminal protection available. The second chapter discusses the procedural criminal rules pertinent to the protection of electronic money transfer operations, including the tracking and prosecution procedures for crimes committed against these operations, as well as preventive measures aimed at combating such crimes. The practical significance of this study lies in its exploration of issues that are relevant to our daily lives, particularly as individuals often find themselves compelled to engage in electronic money transfer operations. Traditional methods of transferring money may expose individuals to risks such as theft and forgery. Consequently, electronic money transfer operations have emerged as a more secure alternative; however, they are not entirely devoid of risk. Therefore, legislation has sought to provide the necessary criminal protection for these operations by establishing legal provisions that regulate them and criminalize any assaults against them. The central problem addressed in this study revolves around the question of how the criminal legislator has safeguarded electronic transfer operations from potential risks. Through this research, I arrived at several findings and recommendations. Notably, I concluded that electronic money transfer has become a hallmark of the modern era. Some countries have enacted specific legislation to regulate and criminalize attacks on electronic money transfer operations, reflecting the unique nature of these crimes. Conversely, other countries have yet to establish such specialized legislation. In Palestine, the Jordanian Commercial Law, which is currently in effect, lacks specific provisions governing electronic money transfer operations. As a

result, legal scholars and the judiciary have endeavored to identify alternative legal texts to regulate this process, utilizing the decision-law on electronic transactions, the decision-law on electronic crimes, and the Palestinian National Payments Law. Among the recommendations I propose is the necessity of training personnel in Palestine on the detection of crimes related to electronic money transfer operations, as well as on the appropriate methods for addressing these crimes. This includes the collection and preservation of electronic evidence and the conversion of such evidence into tangible material evidence, such as storing it on a hard disk, so that it can be presented in court and utilized for prosecution purposes.

Keywords: Electronic money transfer, criminal protection, electronic crimes, Palestinian legislation, electronic evidence, cybersecurity in financial transactions.