مجلة الشرق الأوسط
للدراسات القانونية والفقهية
MESR
منار الشرق للدراسات والأبحاث
Manar Elsharq for Studies & Research

الحماية الجنائية للحسابات البنكية

م. د مكي محمد عبدالرحمن
جامعة كركوك–كلية القانون والعلوم السياسية
Dr.makkealrhman@uokirkuk.edu.iq

استلام البحث: 05/06/2026	مراجعة البحث: 06/07/2026	قبول البحث:04/08/2026

الملخص:

تهتم هذه الدراسة بمقارنة الحماية الجنائية لحسابات البنوك، وكذلك معالجة كلٍ من القانون العراقي وما تم التقاطه من التشريعات الأردنية والمصرية، ومن الاتجاهات الأوروبية، بما يشير إلى وجود بعض الاختلافات. تنبع أهمية الموضوع من مدى التعامل الواسع عبر حسابات البنوك وخدمات المصارف الإلكترونية، وبالتالي تنوع صور الاعتداء على المال والبيانات والمعاملات المصرفية. تتضمن الدراسة مقدمة، ومفهوم حساب البنك وموضوع الحماية الجنائية، تليها دراسة تحليلية للإطار القانوني الذي يحمي حسابات البنوك من خلال نصوص قانون العقوبات العراقي المتعلقة بجرائم البنوك، تبحث الدراسة الأسس القانونية لحماية هذا النوع من الجرائم بموجب العقوبات المنصوص عليها في كلٍ من القانون رقم 94 لسنة 164 (و307) من قانون 314 المتعلق بالاقتصاد. كما تتناول الأشكال التقليدية للاعتداء (السرقة، الاحتيال، خيانة الأمانة، التزوير، إساءة استخدام البطاقات) والاعتداء بصيغته الإلكترونية (الاختراق أو الاعتداءات من نمط التصيّد، سرقة بيانات تسجيل الدخول، انتحال الشخصية). خلصت الدراسة إلى أن الحماية العراقية ترتكز على نصوص متفرقة متداخلة بين التجريم العام للحماية، والتنظيم المصرفي والوقاية الإشرافية، لكنها ما زالت بحاجة إلى تشريعات متخصصة في مجال الجرائم الإلكترونية، والتواصل في مجال الدليل الرقمي، والتعاون الدولي. في المقابل، تمتلك الأردن ومصر نصوصًا أكثر صرامة في عدد من الجرائم التقنية؛ كما يبرز الاتحاد الأوروبي توسيع هياكله من أجل تعاظم التحقق الصارم، وحماية مستخدمي خدمات الدفع، وتعزيز الاستمرارية التشغيلية. وتوصي الدراسة بثلاثة أمور: اعتماد تشريعات متخصصة في العراق، وإلزام البنوك ومقدمي خدمات الدفع بواجبات محددة، ورفع القدرة على إنشاء وحدات تحقيق رقمية مرتبطة بالسلطة القضائية، وتحقيق توازن بين سرية العمل المصرفي ومتطلبات مكافحة الجريمة.

الكلمات المفتاحية: الحماية الجنائية، الحسابات البنكية، الجرائم المصرفية، الجرائم الإلكترونية، القانون العراقي.

Abstract

This study addresses the issue of criminal safeguarding for bank accounts, in a comparative approach based chiefly on Iraqi law but by also pointing out key differences with the laws of Jordan and Egypt as well as some European laws. The topic is important because, as bank accounts and electronic banking services are increasingly used for transactions, attacks against banks funds, data and transactions are growing. This study addresses the law of criminal protection concept and its subject matter, then examines this type of protection and its legislative basis in light of Iraqi Penal Code, Banking Law, Anti-money Laundering and Counter-Terrorist Financing Law rules and regulations related to banks. It covers both classical forms of infringement as theft, fraud, breach of trust, forgery and illegal use of bank cards, and cyberattacks such are hacking, phishing, login credentials and identity theft. The study concludes that Iraqi protection is based on geographically-dispersed provisions combining general purposes, banking regulation and supervisory prevention however that brought to deserve legislation with more specialized views for cybercrime, digital evidence, and international cooperation. The subsequent comparative analysis reveals that Jordan and Egypt have more specific provisions regarding some specific technology-oriented offences, while the EU includes advanced models with regard to strong customer authentication, payment-service-user-protections and digital operational resilience. The study recommends two categories of measures: legislation to be developed in Iraq, regional measures urging the obligations of banks and payment-service providers, and supporting capabilities for digital-investigation work while considering a balance between banking secrecy and the requirements of crime prevention.

Keywords: Criminal protection_ bank accounts_ banking crimes_ cybercrimes_ Iraqi law.

المقدمة

إن طبيعة المخاطر المرتبطة بكون الأنظمة المالية والمصرفية تتعرّض لتحوّل جذري في العصر الرقمي تتزايد بشكل كبير بسبب ظهور الجرائم الإلكترونية، وجرائم غسل الأموال، والجرائم المالية القائمة على التكنولوجيا الرقمية بوصفها أبرز التهديدات الأسرع نمواً لأمننا القومي واستقرارنا المالي، بما يؤثر على خصوصية الأفراد وحقوق الإنسان. وتشتمل هذه الساحة العديد من الأنظمة القانونية المتنافسة, القوانين المنظمة للبنوك وغيرها من المؤسسات المالية، وأحكام مكافحة غسل الأموال أو تشريعات قوية لمكافحة عائدات الجريمة من خلال الغسل، والقانون الجنائي، فضلاً عن توجيهات وتعليمات البنك المركزي أو السلطة النقدية، والقواعد الصادرة عن أنظمة تنظيم دولية أو إقليمية. إضافةً إلى ذلك، قد تكون هناك حاجة متزايدة إلى نهج تشريعي شامل وعالي التقنية لمعالجة قضايا الخصوصية الرقمية، وقضايا الهوية الرقمية، ومرونة التشغيل لدى البنوك والمؤسسات المالية. إن موقف العراق إزاء هذه التحديات يُعدّ موضع تساؤل من الناحية المنهجية والقانونية والتقنية، بمعنى أنه يرتبط ارتباطاً وثيقاً بحالة من التشتت التشريعي ضمن المعايير المتصلة بأحكام القطاع المصرفي، والقوانين الجنائية التي تستهدف الجرائم الرقمية، وقواعد الوقاية من غسل الأموال، في ظل غياب إطار تشريعي متكامل ومنسق لجرائم الفضاء السيبراني الذي يأخذ بجدية في الحسبان التنوعات المفضية إلى نزع حقوق الخصوصية عن مسارها بعد وقوع الجريمة بدل توجيهها نحو الالتزامات التنظيمية (مسؤولية المراقبة) فيما يتعلق بالبنوك أو غيرها من مقدمي جميع أنواع الخدمات الرقمية.

أولاً– أهمية الموضوع:

على الرغم من محدودية نطاق هذا البحث، فإن أهميته ترتبط بسد فجوة معرفية رئيسية وفجوة عملية, وكذلك (قانونية): تتمثل في تقييم مدى مواءمة القانون العراقي الوطني القائم مع المخاطر التي تفرضها ممارسات الخدمات المصرفية الإلكترونية في العراق، مع الاستفادة من المعايير المقارنة عبر رصد أوجه القصور المحددة مقابل تجارب إقليمية بعينها تم اختيارها للتحليل المقارن. إضافةً إلى ذلك، تشمل المعايير المتعلقة بالأردن ومصر كالمعايير المعروضة في القضايا ذات الصلة ضمن لوائح/توجيهات الاتحاد الأوروبي بموجب هذه اللوائح ذات الصلة (PSD2DORA) ايضا، والاتفاقيات والمعايير الدولية، مثل: اتفاقية بودابست وإرشادات مجموعة العمل المالي (FATF), ومبادئ بازل الأساسية والاتحاد الأوروبي . حيث يتمثل هدف هذا البحث ليس فقط في تحديد نصوص تشريعية بعينها، بل في تحديد عناصر قانونية أو أطر ذات صلة قابلة التكييف ضمن السياق العراقي القائم، بما يمكن من تيسير الامتثال لمعايير مكافحة غسل الأموال بما يدعم الاستقرار المالي والقدرة على الصمود التشغيلي في خدمات المصرفية الرقمية.

ثانياً– إشكالية البحث:

تبدأ مشكلة البحث بالسؤال الرئيسي الذي ينص على: إلى أي مدى يوفر القانون المحلي والإطار التنظيمي في العراق وقايةً وعقوبةً رادعةً في الوقت المناسب فيما يتعلق بالتحقيق والإنزال بالعقوبة لجرائم الخدمات المصرفية الإلكترونية، ومخاطر غسل الأموال عبر الوسائل الإلكترونية، والتهديدات الرقمية العملياتية؟ وما الذي قد يختلف عند مقارنته بحجم

المعرفة في الأردن ومصر والاتحاد الأوروبي، إلى أقصى الحدود، من المتطلبات والمعايير الدولية؟ المشتق: هل توجد تغطية كافية بموجب أحكام قانون المصارف العراقي، وقانون مكافحة غسل الأموال والتمويل للإرهاب، وقانون العقوبات (الذي يتضمن معالجة الخصوصية ضمن تشريعات الأصول الرقمية)، وذلك وفقًا للتعليمات الصادرة عن البنك المركزي فيما يخص كلًا من المدفوعات الإلكترونية وتوجيهات المرونة التشغيلية؟ ما التغيير التشريعي والتنظيمي المطلوب لسد الفجوات؟ يُلاحظ هنا أنه لا يوجد قانون عراقي لجرائم الفضاء السيبراني، ما يعني أن التعامل بهذه الطريقة وبصورة غير مباشرة من خلال الأحكام اليومية العامة المتفرقة في تجريم جرائم الفضاء السيبراني (والتي نادرًا ما تُرى) يؤدي إلى نهج محدود يعتريه قصورٌ عملي.

ثالثاً– اهداف الدراسة:

تهدف الدراسة التي قمت بأعدادها الى مايلي:

1. تشخيص واقع التشريعات والقواعد المطبقة في العراق فيما يتعلق بجرائم التمويل الإلكتروني، وغسل الأموال الناشئ عن الخدمات الرقمية, وتوفيرها تغطية للجرائم والخدمات المصرفية الالكترونية.
2. المقارنة بين الواقع القانوني والبيئات القانونية في العديد من الدول, وتحديد أوجه القصور الحرجة في النصوص العراقية مقارنة بالقوانين في بعض الدول العربية.
3. وضع إطار للمبادئ التشريعية والتنظيمية لتعزيز المشهد المصرفي الرقمي في العراق بما يعزز الوقاية والرصد والإنفاذ حول مكافحة غسل الأموال، مع تحقيق توازن بين المرونة التشغيلية وحماية المستهلك.
4. كيف يمكن إعداد المشرعين والجهات التنظيمية والبنوك في العراق قانونيًا، وكذلك عمليًا، من أجل حل التحديات الرقمية؟
5. اعداد التوصيات التشريعية والتنظيمية التي يمكن اقتراحها لصياغة اطار متماسك لمعالجة جرائم الخدمات المصرفية والالكترونية في العراق.

رابعا– منهجية البحث:

تم استخدام منهجية بحثية وصفية–تحليلية مقارِنة، وتضمنت مسارات عديده منها:

1. مراجعة النصوص التشريعية والتنظيمية المعمول بها حاليًا في العراق (قانون المصارف، وقانون مكافحة غسل الأموال، وقانون العقوبات، إضافةً إلى التعليمات الصادرة عن البنك المركزي) من خلال عدسات عملية–قانونية–تقنية–قضائية.

2. وضع مقارنات مع تشريعات الأردن ومصر، ونماذج تنظيمية مقارِنة بما يتوافق مع الاتفاقيات الدولية المتعلقة بالهوية الرقمية (مثل اتفاقية بودابست، وإرشادات مجموعة العمل المالي FATF حول الهوية الرقمية) ومبادئ بازل من أجل تعزيز مرونة التنظيم.

خامسا- خطة البحث:

اعتمدت في دراستي الخطة البحثية الآتية:

المبحث الأول: الإطار المفاهيمي والقانوني للحماية الجنائية للحسابات البنكية.

المبحث الثاني: صور الاعتداء على الحسابات البنكية وآليات الحماية الجنائية.

المبحث الأول

الإطار المفاهيمي والقانوني للحماية الجنائية للحسابات البنكية

تعمل حسابات البنوك كنقطة محورية في غاية الأهمية يتم من خلالها تفاعل الأفراد والمؤسسات، كلٌ بطريقته الخاصة في العمل، مع القطاع المصرفي المعني. فهي تمثل أصلًا يُحتفظ به، ووسيطًا للتبادل، وكذلك مؤشرًا ودلالةً على الثقة ضمن الإطار النقدي والاقتصادي الكامل. ومع ازدياد أنشطة البنوك تقدمًا من الناحية التكنولوجية وتطوير خدمات رقمية، وظهرت أيضًا مخاطر جديدة تتعلق بالنشاط الإجرامي، مما يحدّ من سلامة هذه الحسابات ومصداقية معاملاتها. وقد تطلّب الأمر استجابة تشريعية وتنظيمية وجنائية وإدارية، إلى جانب إجراءات وقائية. في هذا المبحث سأعرض أولاً مفهوم الحساب البنكي وأهميته القانونية والاقتصادية، ثم نبيّن محل الحماية الجنائية (المصالح–المصادر المحمية)، وبعدها أقدم إطاراً تحليلياً للقواعد القانونية العراقية المنوطة بحماية الحسابات البنكية جنائياً مع تعليق تحليلي على قانون المصارف العراقي وقوانين العقوبات ومكافحة غسل الأموال وضوابط البنك المركزي، وختاماً سأجري مقارنة مقصورة بالأردن ومصر والاتحاد الأوروبي[1].

المطلب الأول

مفهوم الحسابات البنكية وأهميتها القانونية والاقتصادية

يقصد بالحساب البنكي العلاقة القانونية التي تنشأ بين المصرف والعميل، والتي يتم بموجبها إيداع الأموال أو إدارتها أو سحبها وتحويلها وفقًا للقواعد المصرفية النافذة. ويُعد الحساب البنكي وسيلة أساسية لحفظ الأموال وإجراء المعاملات المالية بطريقة منظمة وآمنة. كما يكتسب أهمية قانونية لأنه يحدد حقوق العميل والتزامات المصرف، ويثبت العمليات المالية التي تتم بين الطرفين. وتبرز أهميته الاقتصادية في تسهيل حركة الأموال، وتشجيع الادخار، ودعم النشاط التجاري والاستثماري. كما تسهم الحسابات البنكية في تعزيز الشمول المالي وتقليل التعامل النقدي المباشر. وقد ازدادت

1. قانون المصارف العراقي رقم 94 لسنة 2004، الممارسات التنظيمية للبنك المركزي العراقي المتعلقة بحوكمة البنوك.

أهمية الحسابات مع انتشار الخدمات المصرفية الإلكترونية، الأمر الذي جعلها عرضةً لمخاطر السرقة والاحتيال والاختراق. ولذلك أصبحت حمايتها ضرورة قانونية واقتصادية لضمان ثقة الجمهور واستقرار النظام المصرفي[1].

والمفهوم القانوني للحساب البنكي هو ترتيب قانوني بين المصرف والعميل يقيم التزامات حقوقية متبادلة؛ من جهة يودع العميل مالا لدى المصرف، ومن جهة أخرى يلتزم المصرف بحفظ ذلك المال وإعادته عند الطلب أو وفق شروط محددة، كما يلتزم بتنفيذ أوامر الدفع والتحويل نيابة عن العميل. وطبيعته القانونية هجينة: تجمع بين عناصر التملك المؤقت (deposit) والعلاقة التعاقدية والخدمة المصرفية، وبعض النظم تعتبر الرصيد المدون في الحساب التزاماً للمصرف تجاه العميل، وهو ما ينعكس في معالجة الحماية القانونية لاحقاً.

اما الأهمية الاقتصادية للحسابات البنكية فهي تعد وسيط ائتمان ومدخرات حيث تعمل الحسابات كمخزن سيولة، مما يتيح للبنوك استخدام جزء منها لإنشاء الائتمان , حيث ترتبط حماية الحسابات بضمان رصيد كافٍ في القطاع المصرفي – النظام المالي. وكذلك وسائل تنفيذ وتشغيل الأنشطة التجارية التي تعد الحسابات شريان حياة للنشاط الاقتصادي من خلال البنوك التي تستخدمها كأدوات لتحويل الأموال أو الشيكات أو لإجراء خدمات دفع مختلفة. كما انها أداة للسياسة النقدية والرقابة فهي تساعد المعلومات التي تحصل عليها البنوك بشأن الودائع والتدفقات التجارية للسلطات الاقتصادية في تنفيذ سياستها.

فضلا عن تمكين الشمول المالي والابتكار, فالحسابات الرقمية وخدمات الدفع ترتبط بتوسيع الوصول المالي والابتكار المصرفي.

اما فيما يتعلق بالأهمية القانونية فتتمثل بحماية الملكية والحقوق المدنية فهذه الحسابات تحوي أموالاً شخصية أو مهنية، ومن ثم تدخل في باب الحماية المدنية والجنائية ضد الاعتداء عليها. وكذلك الامتثال التنظيمي والمالي فيما يخص قواعد الإفصاح، والتعرف على العملاء (KYC)، والتقارير الضريبية تربط حسابات العملاء بالالتزامات القانونية. فضلا عن الأمن العام والاقتصادي فان الاعتداءات المنظمة على الحسابات قد تؤثر في الثقة بالنظام المصرفي والاقتصاد الوطني، ما يبرر حماية جنائية وإجرائية[2]

المطلب الثاني

محل الحماية الجنائية في الحسابات البنكية

لغرض التعرف على محل الحماية الجنائية يجب اولا التعرف على مواقع وقيم المحل المحمي عند تحديد المحل المحمي جنائياً، وينبغي التفريق بين عدة مستويات سأتطرق لها على النحو الاتي:-

1. قانون المصارف العراقي رقم (94) لسنة 2004، المادة (1)، التي عرّفت العمل المصرفي والوديعة، والمادة (2) المتعلقة بالحفاظ على الثقة بالنظام المصرفي وحماية المودعين والحد من الجرائم المالية، منشور عبر بوابة الاستثمار العراقية، على الرابط: https://investpromo.gov.iq/ar/policies-and-laws/banking-law
2. قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 39 لسنة 2015 .

أ. المال المحسوب في الرصيد: المصلحة المباشرة هي حماية الملكية (أموال العميل أو الطرف الثالث) الموجودة في الحساب من السرقة، الاختلاس، الاحتيال أو التحايل.

ب. سلامة المعاملات والآليات: حماية نظم الدفع والتحويل، بما في ذلك الرسائل والتعليمات، من التدخل والعبث (interference) والتزوير.

ج. سرية البيانات والمعلومات المصرفية: حماية خصوصية العميل ومعلومات الحساب من الكشف غير المشروع أو استخدام البيانات لأغراض احتيالية.

د. سلامة النظام المصرفي والتنظيمي: حماية المصلحة العامة في استقرار القطاع المصرفي ومناعته أمام عمليات غسل الأموال والتمويل الإرهابي[1].

ونرى ان الإطار الجنائي للمحركات الإجرامية الأساسية والجرائم التي ترد بهذا الشان وهي من جرائم التعدي على الأموال اي سرقة الأموال من الحساب، وتحويلات غير مصرح بها، كلاختلاس من قبل موظفي مصرف أو متعاقدين. وجرائم الاحتيال الإلكتروني والمالي باستخدام وسائل تقنية لتزوير تعليمات الدفع أو المصادقة. وجرائم اختراق الأنظمة والتدخل في الخدمات المصرفية إلكترونياً عبر الوصول غير المشروع إلى نظم المعلومات البنكية وإحداث تغييرات لتعطيل الخدمة أو الاستيلاء على الأموال. وجرائم غسل الأموال وتمويل الإرهاب باستخدام الحسابات البنكيه لاستيعاب أو إخفاء مكاسب أو نقل أموال مشبوهة لتعزيز النشاط الإجرامي. وان العناصر المشتركة في وجوب العقاب وحماية المصالح يقرالاجماع العلمي بوجود عناصر متداخلة (العنصر المادي) الفعل–الامتناع المادي, (العنصر المعنوي)النية–التصرف الاحتيالي، ومصلحة الحماية (المصلحة الأصلية أو العامة)، ,بالتالي تقنين حماية الحسابات يستهدف أفعالاً ذات تأثير مادي مباشر على الأموال أو تأثير حمائي على سلامة التشغيل والثقة بالنظام المالي.

المطلب الثالث

الأساس القانوني للحماية الجنائية للحسابات البنكية

في العراق تتوزع مظلة الحماية القانونية للحسابات البنكية بين تشريعات مصرفية وإجرائية (تنظيمية) وتشريعات جنائية ووقائية مالية. لا يوجد إلى حد التاريخ المعاصر نص تشريعي واحد يجمع كل جوانب الحماية الجنائية المتصلة بالجرائم الإلكترونية المصرفية؛ بمعنى أنه لا يوجد قانون عراقي شامل ومتكامل مخصَّص للجرائم الإلكترونية يوازي إلى حد كبير تشريعات متقدمة في بعض الدول أو آليات الاتحاد الأوروبي. هذا الفراغ يفرض الاعتماد على تكييف أحكام عامة موجودة في القانون الجنائي، وقواعد خاصة في قانون المصارف وتعليمات البنك المركزي، وقانون مكافحة غسل الأموال وتمويل الإرهاب، مع توجهات دولية وإقليمية تساعد على سد الفجوات التشغيلية والقانونية.

ففي الإطار المصرفي وفي قانون المصارف العراقي رقم 94 لسنة 2004 وضوابط البنك المركزييتناول ثلاثة عناصر، وهي: يضع بصورة عامة آلية لطبيعة العمل الذي يجب أن تعمل بموجبه المصارف، ويحدد متطلبات الترخيص بما في ذلك التفرد لبعض الأنشطة (أي: لا يجوز للمصارف إجراء معاملات التأمين)، ويُنشئ أساسًا قانونيًا يمكن من خلاله

1. قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023.

إجراء الرقابة والتفتيش على تلك المؤسسات. ويُمنح البنك المركزي الصلاحية لتنظيم أسواق المصارف وتمكينه من وضع الأسس لتنفيذ الأحكام. كما تعكس تعليمات وضوابط البنك المركزي الجانب العملي المتمثل في تطبيق متطلبات حماية الحسابات، إذ تتضمن إجراءات التعرف على العملاء، وقواعد السرية المصرفية، فضلاً عن معايير الأمان التقنية للمصارف (بما في ذلك متطلبات قد تكون متعلقة بتدابير مكافحة الاحتيال الإلكتروني والتعامل مع الحوادث التشغيلية)، وإجراءات الإفصاح والتعاون مع جهات الضبط[1].

وفي مجال قوة الضوابط الإجرائية فان ضوابط البنك المركزي تمثل أداتين: أولهما وقائي تنظيمي للتقليل من المخاطر التشغيلية, والثاني احترازي لفرض التزام امتثالي على المصارف. ومع ذلك، كونها تعليمات تنفيذية يجعل من تطبيقها يتوقف على قدرة البنك المركزي على الرقابة والالتزام من جانب المصارف، مما يبرز أهمية آليات إنفاذ فعالة.
وان غياب النص الجنائي الخاص في قانون المصارف يهدف أساساً إلى تنظيم العمل المصرفي وإجراءات الرقابة، وليس إلى خلق جرائم وعقوبات جنائية خاصة بالحماية من الاعتداء على الحسابات. لذلك تصبح الحاجة إلى رابط بين الضوابط التنظيمية والعقاب الجنائي ضرورية، وتعتمد على مواد قانون العقوبات والتشريعات الجنائية الأخرى.
اما في الإطار الجنائي فأن قانون العقوبات العراقي رقم 111 لسنة 1969 يشمل جرائم تقليدية مثل السرقة والاختلاس والاحتيال والجرائم التي تُعدُّ اعتداءً على الملكية أو السلامة العامة. وهذه الأحكام تُطبق — بوصفها نصوصاً عامة — على الاعتداءات المتعلقة بالحسابات البنكية، سواء من خلال وسائل تقليدية أو بواسطة وسائل إلكترونية مادامت العناصر التقليدية للجرائم متوافرة (مثل التصرّف في مال غيره بنية الإضرار)[2] وان أهمية التطبيق العملي تعتمد على قدرات التفتيش والالتزام والتطبيق، وكذلك على وضوح الصلاحيات والمسارات القضائية والتعاون مع الأجهزة الأمنية والجهات القضائية. وهناك ثغرات محتمل تتمثل في عدم وجود قانون إلكتروني شامل يستجيب لمخاطر الجرائم التقنية ويترك عبئ إثبات وملاحقة الجرائم التقنية لدى الأجهزة القضائية، ويتطلب دوراً أكبر للضوابط التقنية والتنظيمية في منع الحوادث أو الحد من آثارها.

وفيما يخص الفراغ التشريعي في مجال الجرائم الإلكترونية الشاملة, فانه لا يوجد في النظام العراقي تشريع شامل للجرائم الإلكترونية ومتكامل يضم التعريفات الجنائية الخاصة بالجرائم المعلوماتية، والمسؤوليات الجنائية للمستخدمين والجهات وتدابير الحقائب الإجرائية الخاصة بالأدلة الرقمية والإجراءات التخطيطية لمواجهة الجرائم الإلكترونية المصرفية. وأن هذا النقص يجعل الاعتماد على نصوصٍ قديمة أو عامة أمراً عملياً لكنه غير كافٍ لمواجهة خصوصيات الجرائم المصرفية الرقمية.

وعن آليات التعاون والتحقيق والأدلة الرقمية فان تطبيع ممارسات جمع الأدلة الرقمية وتحليلها وتبادل المعلومات بين المصارف والسلطات القضائية والأمنية ضرورة لتطبيق النصوص القائمة، لكن غياب إطار تشريعي خاص بالأدلة

1. قانون المصارف العراقي رقم 94 لسنة 2004.
2. قانون العقوبات العراقي رقم 111 لسنة 1969.

الرقمية وتقنين إجراءات الحجز والنسخ والاحتفاظ يخلق تحديات في قبول الأدلة أمام المحاكم وفي حماية حقوق الخصوصية وحرية الاستخدام.

والجزاءات الجنائية النافذة في العراق تعتمد على التصنيف العام للجرائم (سرقة، اختلاس، تزوير، غسل أموال)، وبناءً عليه يتم تطبيق عقوبات السجن والغرامات وإجراءات المصادرة . إلا أن غياب نصوص متخصصة للجرائم الإلكترونية المصرفية قد يفضي إلى تطبيق عقوبات لا تتناسب مع الطابع التقني للضرر أو لا تعالج عناصر المسؤولية المؤسسية.

وعند اجراء مقارنة تحليلية بين قوانين الدولة المقارنة والاتحاد الاوربي نجد انه اعتمدت المملكة الأردنية قانون الجرائم الإلكترونية رقم 17 لسنة (2023) في نسخة مُعدَّلة، يتناول الجرائم الإلكترونية بشكل صريح ويشتمل على العديد من الآليات الخاصة بإجراءات التحقيق الرقمي، إلى جانب آلية حماية الأدلة، والتعامل مع أنواع مختلفة مثل بيان الوصول غير المصرّح به، والرسالة والإرسال والاستقبال باستخدام أجهزة أو معدات نقل البيانات دون موافقة، كما يشتمل على نقل البيانات المنسوخة والاحتيال المصرفي. علاوة على ذلك، فقد وضع قانون البنوك رقم 28 لسنة 2000 وتعديلاته أطرًا تنظيمية واضحة لالتزامات البنوك فيما يتعلق بالسرية، وكذلك الإفصاح والتعاون مع السلطات التنظيمية[1].

ومن ذلك يتضح في مجال سد الفجوات يوجود قانون إلكتروني خاص في الأردن يجعل الملاحقة الجنائية للحوادث المصرفية الإلكترونية أسهل من الناحية الإجرائية والتقنية، مقارنة بالعراق الذي يُعتمد على أحكام عامة. وكذلك التنسيق التشريعي الذي يعني الربط بين قانون الجرائم الإلكترونية وقانون البنوك وقوانين مكافحة غسل الأموال مؤشر على درجة متقدمة من الاتساق التشريعي تزيد من فاعلية الرد.

اما في مصر فان قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ولائحته يحدد مجموعة واسعة من الجرائم المعلوماتية، وينص على إجراءات التحقيق الرقمي وحماية الأدلة وطرق التعاون الدولي[2]، كما أن قانون البنك المركزي والجهاز المصرفي المصري رقم 194 لسنة 2020 يوفر إطاراً تنظيمياً متطوراً للرقابة على البنوك والإجراءات التشغيلية[3].

المبحث الثاني

صور الاعتداء على الحسابات البنكية وآليات الحماية الجنائية

لقد أصبح الاعتداء على الحسابات البنكية ظاهرة جنائية واقتصادية تقنية متعددة الأشكال والآثار، تتقاطع فيها قواعد القانون الجنائي والبنكي والأنظمة التنظيمية لمواجهة مخاطر الاحتيال، الاختلاس، غسل الأموال، والجرائم الإلكترونية. يهدف هذا المبحث الثاني إلى تقديم دراسة مقارنة دقيقة تركز على العراق كنظام رئيس، مع إشارات محدودة إلى الأردن

1. قانون البنوك الأردني رقم 28 لسنة 2000 وتعديلاته، لإيضاح الإطار المصرفي الأردني.
2. قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ولائحته التنفيذية، القاهرة، تشريع رسمي، 2020/2018، المواد 1 و2 و6 و23 و30.
3. قانون البنك المركزي والجهاز المصرفي المصري رقم 194 لسنة 2020، القاهرة، تشريع رسمي، 2020، مواد سرية حسابات العملاء وحماية نظم الدفع.

ومصر والاتحاد الأوروبي (خصوصاً PSD2 وDORA/النماذج الأوروبية)، وأيضاً إلى المعايير الدولية ذات الصلة مثل اتفاقية بودابست وإرشادات مجموعة العمل المالي (FATF) ومبادئ بازل للمرونة التشغيلية. سأعرض في ثلاثة مطالب: الاول نتناول جرائم الأموال والمعاملات البنكية التقليدية ومكانها في النظام العراقي؛ وفي الثالث نتعرض الى الجرائم الإلكترونية الماصة بالحسابات البنكية وتحليل أركانها وخصوصيات الإثبات؛ وفي الثالث نتطرق الى وسائل المكافحة الجنائية والمدنية والتنظيمية وحدود الحماية، مع بحث مسؤولية العميل، المصرف، الموظف، ومقدمي خدمات الدفع. في مقدمة كل مطلب سأبرز النصوص النافذة والمقارنة، وأذكر صراحة حالات غياب تشريع عراقي شامل للجرائم الإلكترونية حيث تنطبق[1]

المطلب الأول

الجرائم الواقعة على الأموال والمعاملات البنكية

في الإطار التشريعي العراقي ذي الصلة فان القواعد الرئيسية النافذة في العراق التي تنظم الممارسات البنكية ومسؤوليات المصارف تشمل قانون المصارف رقم 94 لسنة 2004، الذي يحدد الإطار القانوني لعمل المصارف والترخيص والسرية والواجبات التنظيمية العامة للمصرف والمودع ، ففي الجانب الجنائي تُطبّق أحكام قانون العقوبات العراقي رقم 111 لسنة 1969 على الجرائم التقليدية المرتبطة بالأموال مثل السرقة والاختلاس والاحتيال والجرائم ضد المال العام والخاص، إلى جانب أحكام خاصة في حالات تزوير المستندات والخيانة أو استغلال الوظيفة.

– أما في مجال مكافحة التمويل غير المشروع وغسل الأموال فتفرض أحكام قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 39 لسنة 2015 التزامات الإبلاغ عن المعاملات المشبوهة وإجراءات العناية الواجبة على المؤسسات المالية، وتفويض صلاحيات رقابية وسلطات عقابية إدارية وجنائية معينة للسلطات المختصة.

وعلى المستوى التنظيمي تكمل تعليمات وضوابط البنك المركزي العراقي الأحكام التشريعية بتوجيهات تشغيلية تتعلق بمعايير العناية الواجبة، حفظ السجلات، التبليغ، وإجراءات أمنية وإدارية واجبة التطبيق على المصارف.

اما عن تصنيف الجرائم البنكية التقليدية وأركانها الجنائية, فان جرائم السَرقة والاختلاس والاحتيال والاستيلاء على أموال الغير من حيث الطابع الجنائي تندرج ضمن الاعتداءات المادية على الأموال داخل الحسابات المصرفية, وأحيانًا تحت مرتبة اختلاس (em-b-ez-zle-ment) حين تكون الجريمة من فعل موظف مصرفي أو متولي أمانة، وتندرج تحت سرقة أو احتيال عندما يكون الفاعل طرفًا خارجيًا استولى على أموال بصفتها ملكًا للغير بوسائل احتيالية [2] . وان الأركان العامة لهذه الجرائم (الموضوعية/المادية): وجود مال مملوك لغير الفاعل، واقعة عليه انتزاع أو تحويل أو

1. د.عدنان خلف محيي، جريمة إفشاء سر المهنة في القانون العراقي، رسالة ماجستير، كلية القانون، جامعة بغداد، 1998، ص 60.
2. د. عادل يوسف عبد النبي الشكري، المسؤولية الجنائية الناشئة عن الإهمال، رسالة ماجستير، كلية القانون، جامعة بابل، 2005، ص 77.

إتلاف وأدى إلى حرمان المالك من المال أو التحكم به, وهنا يبرز عنصر السبيل الإجرائي (استعمال القوة أو الخداع أو استغلال الوظيفة). (ذهنية/معنوية): نية الاستيلاء أو الإضرار أو القصد الاحتيالي (قصد تملك دائم أو نية إضرار). ينبغي في كل حالة إثبات أن الفاعل اتخذ سلوكًا متعمّدًا يهدف إلى التمكين من المنفعة المالية.

اما الجرائم ذات الطابع المصرفي الخاص كخيانة الأمانة المصرفية، كما في حالة التزوير في دفاتر أو مستندات مصرفية أو إصدار شيكات مزورة أو أوامر تحويل موقعة زورًا يُعد جرائم مستقلة، أركانها تتطلب إظهار أن المستند زُور بقصد إحداث نتائج قانونية واقتصادية متعلقة بحسابات المصرف.

وجرائم غسل الأموال التي تتمثل في أعمال الإخفاء أو التحويل للأموال الناتجة عن أعمال إجرامية تدخل في تعريف غسل الأموال، وتتطلب نصوصًا على عنصر الأصل الإجرامي للأموال وإجراءات تلميعها أو إدخالها إلى النظام المالي بغية إضفاء صفة المشروعية[1]. وقانون مكافحة غسل الأموال العراقي يفرض التزامات إجرائية على المصارف ويجعل بعض أشكال السلوك جنائية ومدنية تجاه إدخال أموال ذات أصل إجرامي في النظام البنكي. وان آثار الضوابط التنظيمية البنكية على التجريم والوقاية فان تعليمات البنك المركزي العراقي تفرض معايير لحفظ السجلات (العناية الواجبة) والاحتفاظ بسجلات العمليات مما يعزز قدرات الإثبات لدى الجهات الرقابية والنيابية والمتضررين المدنيين، كما أنها تحدد واجبات الإفصاح والتبليغ التي تتحول لاحقًا إلى قواعد إثبات تنظيمية وإدارية. وان عدم التزام المصارف بتلك الضوابط قد يؤدي إلى مسؤولية تأديبية وإدارية وربما إلى إثبات إهمال جنائي إذا أدى التقصير إلى وقوع جريمة مالية[2].

المطلب الثاني

الجرائم الإلكترونية الماسة بالحسابات البنكية

في حالة عدم عدم وجود تشريع سيبراني شامل وصريح في العراق فان من المهم التأكيد صراحة على أن العراق لا يمتلك حتى تاريخ البحث تشريعًا جنائيًا مستقلاً أو موحدًا وشاملاً للجرائم الإلكترونية يوازي نصوصًا مثل قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 او القانون المصري لمكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018, وحالات الاعتداء الإلكتروني على الحسابات في العراق تُعالج حالياً بمحاور متفرقة: كأحكام قانون العقوبات التقليدي، وأحكام التجريم في قانون غسل الأموال عند الاقتضاء، وتعليمات البنك المركزي، هذه الحالة تثير مشكلات تفسيرية وإجرائية في تحديد عناصر الجرائم الإلكترونية وإجراءات التحري والادعاء والاعتقال والرقابة القضائية على ممارسات جمع الأدلة الرقمية. وبالمقارنة، أقر بالأردن في سنة 2023 تشريعًا مخصصًا للجرائم الإلكترونية يتناول جرائم الدخول

1. د. علي فوزي إبراهيم، الموازنة بين الالتزام بحفظ السر المصرفي وظاهرة غسيل الأموال، مجلة دراسات قانونية، بيت الحكمة، بغداد، العدد 24، 2009، ص 25.
2. لمى وهّاب إبراهيم، التزامات المرخّص له في مكافحة غسل الأموال وتمويل الإرهاب، مجلة جامعة بابل للعلوم الإنسانية، جامعة بابل، المجلد 27، العدد 3، 2019، ص 159–170.

غير المشروع، الاحتيال الإلكتروني، سرقة الهوية الرقمية، والجرائم المتعلقة بالخدمات الإلكترونية والحسابات المصرفية، مما يوفر إطارًا جزائيًا وإجرائيًا أكثر تفصيلاً لملاحقة مرتكبي الجرائم الرقمية[1]. كذلك مصر لديها قانون متكامل رقم 175 لسنة 2018 بشأن جرائم تقنية المعلومات ينص على جرائم دخول الأجهزة والشبكات دون تصريح، التشويش على البيانات والابتزاز الإلكتروني[2].

اما تصنيفات الجرائم الإلكترونية الماسة بالحسابات البنكية هي:-

أ. الدخول غير المشروع إلى الأنظمة والحسابات (unauthorized access)

ان الدخول غير المشروع الى الأنظمة والحسابات يعد اختراق حسابات بنكية عبر خروقات تقنية (اختراق نظم المصارف، التفريط في بيانات الاعتماد، استغلال ثغرات تطبيقات الدفع). وعناصر هذه الجريمة: هي فعل مادي يتعلق بالدخول/الوصول إلى نظام محمي بدون ترخيص, وأدلة على الاستخدام غير المصرح به. في نظم تقنين متقدّمة يظهر عنصر القصد الجنائي (معرفة أن الدخول غير مصرح به) ضرورة جنائية.

و اثباتها عن طريق سجلات الدخول (logs)، عناوين IP، سجلات الخوادم، شهادات الخبراء الجنائيين الرقميين، واستعلامات مزودي الخدمات. والتحدّي هنا يتمثل في سلسلة الحيازة على الدليل (chain of custody) وصياغة تقرير فني مقبول قضائياً[3].

ب. الاحتيال الإلكتروني وتنبيهات التحويل (electronic fraud)

ان الاحتيال الالكتروني هيو خداع الضحية لتحويل أموال من حسابه أو إجراء معاملات غير مرخصة بواسطة رسائل تصيّد (phishing)، برامج خبيثة، أو تقنيات هندسة اجتماعية , واركانه تتمثل في وجود فعل خداعي أدى إلى نقل ملكية أو تفويض انتقال أموال, ونيات احتيال/غش لدى الفاعل.

واثباتها عن طريق رسائل البريد أو تطبيقات الدردشة، او سجلات المعاملات المصرفية، او تقارير الطب الشرعي الرقمي، وتحقيقات سلاسل الاتصال بين المهاجم والضحية. في العراق قد تواجه التحقيقات عراقيل عملية لندرة وحدات الطب الشرعي الرقمي المتطورة وغياب نص قانوني محدد للجرائم السيبرانية يجعل إجراءات الحجز والتحري أقل وضوحًا من منظور الإجراءات الجنائية.

ج. سرقة الهوية الرقمية وفتح حسابات مزيفة أو التلاعب ببيانات الحساب

1. البنك المركزي العراقي، ضوابط مكافحة غسل الأموال وتمويل الإرهاب لمقدمي خدمات الدفع الإلكتروني، بغداد، 2025، إصدار رسمي، فقرات إدارة مخاطر الدفع الإلكتروني.
2. قانون الجرائم الإلكترونية الاردني رقم 17 لسنة 2023، عمان، تشريع رسمي، 2023، المواد المتعلقة بالدخول غير المشروع والاعتراض والاحتيال والبيانات.
3. د. محمود نجيب حسني، شرح قانون العقوبات؛ القسم العام، دار النهضة العربية، القاهرة، 1989، الطبعة الخامسة، ص 287.

سرقة الهوية الرقمية هي الاستحواذ على بيانات المصادقة أو الهوية لفتح حسابات مصرفية أو لإجراء معاملات باسم الغير. وأركان هذه الجرائم تتضمن وقوع الحصول على بيانات شخصية أو تزوير وثائق رقمية بغرض الاستفادة المالية[1].

– واثباتها يكون بواسطة سجلات التسجيل، صور الوثائق، نشاطات المصادقة، شهود من جهات التحقق، وخبراء تحقق من تزوير المستندات الرقمية.

د. استغلال الثغرات الداخلية/الدخلاء (insider threats)

استغلال الثغرات الداخلية هي قيام موظف مصرفي أو مزود خدمة بالاستفادة من صلاحياته لتحويل أموال أو الكشف عن بيانات حساسة. وأركانها تجمع بين الاستغلال الوظيفي ونيات الاستيلاء أو المساهمة في جريمة أخرى[2].

واثباتها يكون عن طريق سجلات الصلاحيات، وتتبع العمليات داخل النظام، وشهادات الموظفين، وتحليل سجلات الوصول. وهنا تتقاطع القواعد التأديبية الإدارية مع المسؤولية الجنائية.

هـ. جرائم متقدمة: برامج الفدية (ransomware) والتلاعب بترحيلات المدفوعات (manipulation of payment flows)

هي تعطيل أنظمة المصرف أو تشفير بيانات العملاء بهدف الابتزاز أو التعطيل المالي، وأركان هذه الجرائم توضح النية في ابتزاز وضمان القدرة على التأثير في نظام الدفع[3].

واثباتها يتم بواسطة، ملفات التشفير، ورسائل المطالبة بالفدية، وسجلات النظام قبل وبعد الهجوم، ونماذج التواصل مع المهاجم.

اماخصوصيات الإثبات الرقمي ومسائلها الإجرائية في العراق فهي تتطلب الدليل الرقمي وأساليب تقنية فريدة مثل (حفظ السجلات، واستخراج بيانات الخوادم، وتقارير من مختصين في الطب الشرعي الرقمي) مع الحفاظ على سلسلة الحيازة لضمان عدم حدوث أي تعديل من خلال العبث بالملفات الإلكترونية.

وإن غياب قانون شامل للأمن السيبراني في العراق يؤدي أيضًا إلى تباينات بين إجراءات التحقيق, وعلى سبيل المثال، اشتراط الحصول على أوامر قضائية عند التعامل مع مزودي خدمات الإنترنت أو الخوادم الخارجية، فضلًا عن التعقيدات المحيطة بتبنّي التحليلات الدولية.

1. د. ميادة صلاح الدين تاج الدين، السرية المصرفية: آثارها وجوانبها التشريعية/ دراسة مقارنة، مجلة تنمية الرافدين، جامعة الموصل، كلية الإدارة والاقتصاد، المجلد 31، العدد 95، 2009، ص 1–20.

2. د. محمود نجيب حسني، مصدرسابق , شرح قانون العقوبات, القسم العام، دار النهضة العربية، القاهرة، 1989، الطبعة الخامسة، ص 318.

3. د. علي فوزي إبراهيم، الموازنة بين الالتزام بحفظ السر المصرفي وظاهرة غسل الأموال، مجلة دراسات قانونية، بيت الحكمة، بغداد، العدد 24، 2009، ص 25.

فعلى سبيل المثال، يسهل قانون الجرائم الإلكترونية في الأردن وقانون مصر رقم 175 إجراءات البحث والتحقيق—كما يضعان الأساس لتقنيات الطب الشرعي الرقمي التي تعمل على تبسيط التحقيقات مع المخالفين[1].

المطلب الثالث:

وسائل مكافحة الاعتداء على الحسابات البنكية وحدود الحماية الجنائية

ان دور البنك المركزي والضوابط التنظيمية والمصرفية من خلال أدوات المكافحة الجنائية والإدارية في العراق

يطلب ايقاع العقاب على جرائم الاعتراض على الحسابات البنكية وفقا للقواعد الجنائية التقليدية ووفقا لقانون العقوبات، مع إمكانية تطبيق أحكام غسل الأموال في حال إدخال الأموال المكتسبة من أنشطة إلكترونية إلى النظام المالي، والعقوبات الإدارية والمالية تفرضها الهيئة الرقابية ومصرف العراق المركزي على المصارف المخالفة لالتزامات العناية الواجبة والإبلاغ[2].

وكذلك الضبط والتعاون والتحقيق فان تعليمات البنك المركزي وحدودها تمكن جهات التحقيق من الحصول على سجلات بنكية وإدراج تقارير عن التعاملات المشبوهة ضمن التحقيقات، إلا أن قلة نصوص خاصة بالجرائم الإلكترونية تُضعف الإطار القانوني لطلب أوتوماتيكي للبيانات من موفري خدمات الاتصالات أو مزودي خدمات الدفع الإلكتروني[3]. وبذلك تتجلى أهمية التعاون الدولي والإقليمي في قضايا تتضمن خوادم أو نشاطًا عابراً للحدود بغياب بنية تشريعية صلبة أو اتفاقات تعاون ثنائية, وهنا تظهر أهمية اتفاقية بودابست كإطار للتعاون الجنائي الدولي في الجرائم الإلكترونية[4].

اما الواجبات التنظيمية والتقنية على المصارف ومقدمي خدمات الدفع هي :-

أ. التزامات العناية الواجبة ومكافحة غسل الأموال: تفرض أحكام قانون مكافحة غسل الأموال والضوابط المصرفية واجب التعرف على العميل (CDD)، مراقبة المعاملات، والإبلاغ عن المعاملات المشبوهة، وهذه أدوات مهمة لكشف عمليات الاحتيال عبر الحسابات وتجنب استغلال النظام المصرفي لغسل عائد الجرائم[5]، و تطبيق إرشادات FATF بشأن الهوية الرقمية (Digital ID) يعزّز القدرة على التحقق من العملاء في البيئة الرقمية ويقلل مخاطر فتح حسابات مزورة.

ب. معايير الأمن السيبراني والمرونة التشغيلية: على المصارف ومقدمي خدمات الدفع توفير بنى تقنية لإدارة مخاطر تكنولوجيا المعلومات، وسياسات استمرارية الأعمال وخطط استجابة للحوادث، وفق مبادئ مثل مبادئ بازل للمرونة

1. د. بدر تراك سليمان الشمري، الجوانب القانونية المتعلقة بسر المهنة المصرفية/ دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، الجامعة الأردنية، 2007، ص67.
2. د. إياد خلف محمد، المسؤولية الجزائية عن إفشاء السرية المصرفية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 23، 2010، ص 22.
3. عادل محمد السيوي، التعاون الدولي في مكافحة غسل الاموال وتمويل الارهاب، ط١، سنة 2010، ص 27.
4. د. جمال إبراهيم الحيدري، أحكام المسؤولية الجزائية، منشورات زين الحقوقية، بيروت، 2010، الطبعة الأولى، ص 130.
5. د. وسام كاظم زغير، إفشاء الأسرار وأثره في المسؤولية الجزائية، رسالة ماجستير، كلية القانون، الجامعة المستنصرية، 2013، ص72.

التشغيلية (Operational Resilience) ومعايير جديدة مثل DORA على مستوى الاتحاد الأوروبي لمزودي الخدمات المالية، وفي إطار الاتحاد الأوروبي، تحدد PSD2 مسؤوليات مقدمي خدمات الدفع (مثل مقدمي خدمات الوصول إلى الحساب AIS/PIS ومقدمي خدمات الدفع) والتزامات تقنية مثل المصادقة القوية للعميل (SCA) التي تقلّل من الاحتيال الإلكتروني[1].

وان حدود الحماية القانونية والعملية في العراق تحتوي على ثغرات تشريعية وإجرائية بسبب غياب قانون جرائم إلكترونية موحد وهذا مايؤدي إلى صعوبات تتعلق بتحديد العقوبات الخاصة بالأفعال السيبرانية، وحصر سلطة الضبط القضائي للوصول إلى الأدلة الإلكترونية، وإجراءات التعاون الدولي. كما أن ضعف البنية الفنية لوحدات الطب الشرعي الرقمي في العراق يعوق سرعة وجودة الأدلة.

اما حدود إثبات القصد وشروط إثباته في الجرائم الرقمية فان الاجتماعات التقنية في إثبات نية الاحتيال أو التواطؤ قد تكون معقدة, وهل كانت عملية الدخول غير مصرح بها نتيجة تقصير الضحية (تسليم كلمات المرور)؟ أم نتيجة هجوم خارجي؟ هذا ينعكس في تحديد المسؤولية المدنية والجنائية تجاه الضحية والمصرف[2].

والمسؤوليات الجزائية والمدنية المحتملة للعميل، والمصرف، والموظف، ومقدم خدمة الدفع، فان مسؤولية العميل تنبع من واجباته في حفظ بيانات الاعتماد وعدم إفشائها، والإبلاغ فوراً عن عمليات غير مصرح بها، والتعاون مع المصرف والجهات الأمنية. وفي حال ثبت أن العميل ساهم بتصرف فاحش بالإهمال (مثل مشاركة كلمات المرور بصورة واضحة)، فقد يترتب عليه قصور إثباتي أو مسؤولية تقصيرية مدنية تقلل أو تلغي حق التعويض، لكن القانون المصرفي يحمّل المصارف مسؤولية تأمين أنظمة المصادقة وتطبيق معايير الأمان، ولا يجوز تحميل العميل وحده مسؤولية الخسائر إن كان المصرف قد أخفق في إقامة إجراءات أمنية معقولة[3].

اما عن مايخص مسؤولية المصرف فان المصارف تتحمل مسؤولية تنظيمية وقانونية عن سلامة الأنظمة واتباع تعليمات البنك المركزي وقانون غسل الأموال، ومدى التزام المصرف بمعايير العناية الواجبة والضوابط التقنية. وان عدم الامتثال قد يفضي إلى مسؤولية إدارية او غرامات أو مسؤولية مدنية تقتضي التعويض إن ثبت التقصير، وعند وقوع هجمات إلكترونية ناجمة عن قصور في الأمن أو إهمال إداري في تحديث النظم، قد تُعارض المصارف مطالبة العملاء بالتعويض ما لم يثبت أن الخسائر نتجت عن خطأ جسيم من العميل[4].

ومسؤولية الموظف (الداخل) الذي يستخدم صلاحياته للاستيلاء على أموال العملاء أو تسهيل عمليات الاحتيال يواجه تهمًا جنائية بمقتضى قانون العقوبات في حالة (الاختلاس، وخيانة الأمانة، والتزوير) ويمكن أن تُفرض عليه عقوبات

1. د. سعيد عبد اللطيف حسن، الحماية الجنائية للسرية المصرفية؛ دراسة مقارنة، دار النهضة العربية، القاهرة، 2004، الطبعة الأولى، ص 73.

2. د. خليل يوسف الجندي، المسؤولية الجزائية الناشئة عن الاعتداء على سرية الحسابات المصرفية، رسالة ماجستير، كلية القانون، جامعة الموصل، 2002، فصل الحماية الجزائية للسر المصرفي، ص 35.

3. د. سامر سعدون العامري، وكوثر عبد الرزاق عبد الله، جريمة إفشاء السرية المصرفية وآثارها الجزائية، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، المجلد 33، العدد 6، 2019، ص 448.

4. د. علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية، الجزء الثاني، دار النهضة العربية، القاهرة، 1989، الطبعة الأولى، ص 15.

جنائية ومدنية وتعسيرية (فصل، غرامات)، إضافة إلى احتمال تطبيق أحكام غسل الأموال إن اتضح تحويل الأموال بشكل مُشَوَّه[1].

كما ان مسؤولية مقدم خدمة الدفع (مبادئ مقارنة وفق PSD2 وDORA) فان نظم الدفع المفتوحة تحت PSD2 تتحمل مخاطر تقنية وتشغيلية لمقدمي خدمات الدفع فيما يتعلق بالأمان والمصادقة والإخطار، ويوجد ترتيب مسؤوليات واضح بين مقدم الخدمة والمصرف المشارك.DORA تفرض على موفري الخدمات المالية ومقدمي خدمات الطرف الثالث التزامات قوية في مجال إدارة مخاطر تكنولوجيا المعلومات والاتصالات والقدرة على التعايش أثناء الحوادث، ما قد يؤثر في تقييم المسؤولية المدنية تجاه الزبائن في حال وقوع اختراق نتيجة إهمال مورد تقني.

وبالمقارنة في العراق قد لا توجد آليات تنظيمية تفصيلية على مستوى مقدمي خدمات الدفع لا بالمستوى القانوني المتفق عليه في PSD2/DORA، مما يتطلب تحديث الأطر التنظيمية المحلية لاحتواء مخاطر مقدمي الطرف الثالث[2].

وان إثبات المسؤولية الجنائية والمدنية عن طريق عناصر الإثبات الجنائي لثبوت المسؤولية الجنائية يجب تجميع أدلة تقنية وتقليدية توضح الفعل والنتيجة والنية: كسجلات المعاملات، وسجلات الدخول، وشواهد خبير، وإفادات الشهود، ووثائق تقنية لخوادم الطرف الثالث. كقضايا غسل الأموال التي تتطلب إثبات أصول الأموال والعلاقة بالمخالفة المسبقة[3].

ونرى ان آليات استرجاع الأموال وتعويض المتضررين فالإجراءات المدنية والتعويضات المالية تعتمد على إثبات المسؤولية التقصيرية للمصرف أو الموظف أو مقدّم الخدمة، وعلى قدرة السلطة القضائية على إصدار أحكام منفذة واستعادة الأموال عبر إجراءات تحفظية أو تنفيذية. وفي حالات عبور الحدود تتطلب التعاون القضائي الدولي وفق اتفاقيات دولية مثل بودابست.

الخاتمة

يبدو أن النظام التشريعي والتنظيمي العراقي المتعلق بالجرائم السيبرانية وأمن الخدمات المصرفية الرقمية مجزّأ، إذ يعتمد في الغالب على الأحكام العامة في قانون العقوبات، فضلاً عن قوانين خاصة بقطاع الإيداع (مثل قانون المصارف) أو التعليمات الصادرة عن البنك المركزي العراقي، مثل ما يتعلق بكبح غسل الأموال وتمويل الإرهاب مع إلزام المصارف بالحكم الذاتي, ثم تجري مزيداً من التحققات هناك بالفعل, أذ لا توجد قوانين عراقية متكاملة ومحددة بشأن الجرائم السيبرانية التي تندرج ضمن العلوم الحديثة للجرائم اللازمة لحماية نظام البنوك، لأن أفضل الممارسات من الناحية التجريبية تُعنى بالنظام الاجتماعي أو السياسي، لكن نقص تقنية القانون المقيد إنفاذه للوقائع المتعلقة بالوقائع الرقمية المرنة , وهو ما أدى إلى فراغ قانوني وتفسيري يسبب مشاكل إضافية في الملاحقة القضائية والتعاون الدولي، ويستلزم

1. د. فخري عبد الرزاق صلبي الحديثي، شرح قانون العقوبات؛ القسم العام، بغداد، ساعدت جامعة بغداد على طبعه، 2010، الطبعة الثانية، ص 215.
2. د. إبراهيم حامد الطنطاوي، الحماية الجنائية لسرية معلومات البنوك عن عملائها؛ دراسة مقارنة، دار النهضة العربية، القاهرة، 2005، الطبعة الأولى، ص89.
3. د. علي عبد القادر القهوجي، شرح قانون العقوبات؛ القسم العام، منشورات الحلبي الحقوقية، بيروت، 2008، الطبعة الأولى، ص226.

من المؤسسات المالية اعتماد إجراءات معيارية لإدارة المخاطر في الفضاء السيبراني. حيث ان الإبلاغ عن الحوادث يستلزم فعلياً أخذ نمط هجوم أو اختراق لإدارة المخاطر الناشئة عن مقدمي خدمات من خارج المؤسسة, ويوفر ذلك نموذجاً مرجعياً لتطبيقه في السياق العراقي مع اختلافات المؤسسات والتقنيات، بما يفتح أعمالاً تشريعية وتنظيمية على ضوء التجارب المقارنة.

النتائج والتوصيات

أولاً: النتائج :

1. من خلال الإطار الجزائي والجنائي في العراق لم نجد نص تشريعي شامل ومحدَّث للجرائم الإلكترونية يغطي الجرائم المرتكبة عبر الشبكات الرقمية بشكل مستقل, بل يعتمد الملاحق الجزائية على أحكام عامة في قانون العقوبات رقم 111 لسنة 1969 وبعض نصوص متفرقة في تشريعات أخرى، ما يضع قيداً على مواكبة الطبيعة التقنية والسرعة في تطور الأدلة الرقمية وطرق ارتكاب الجرائم.
2. الحوكمة المصرفية الرقمية, قانون المصارف العراقي رقم 94 لسنة 2004 , وتعليمات البنك المركزي تمنح سلطة تنظيمية للقطاع المصرفي لكنها تفتقر إلى نظم مُفصَّلة للمرونة التشغيلية الرقمية وإدارة مخاطر مقدمّي الخدمات الخارجية واشتراطات أمن المعلومات بالمستوى المطلوب لمواجهة مخاطر الاعتماد الرقمي والربط بين البنوك والمنصات الرقمية.
3. ان قانون مكافحة غسل الأموال وتمويل الإرهاب (AML/CFT), العراقي رقم 39 لسنة 2015 يوفر قاعدة إلزامية لإجراءات معرفة العميل والإبلاغ عن العمليات المشبوهة, والتي أصبحت تتقاطع مع المخاطر الرقمية، غير أن استجابة الإطار الرقابي تجاه التحديات الخاصة بالهوية الرقمية والمحافظ الإلكترونية والأصول الافتراضية غير مكتملة تنظيمياً.
4. ضعف التكييف والتعاون القضائي, ان غياب تشريع إلكتروني شامل يعرّف الأدلة الرقمية ويحدد إجراءات حفظها واستردادها يحدّ من قدرة القضاة والمحققين على التكييف القانوني والإجرائي في التحقيقات السيبرانية ويصعّب عملية التعاون عبر الحدود، لا سيما في غياب انضمام العراق لأطر دولية محددة في هذا المجال.
5. قدرات الجهات الرقابية والفنية توجد مهارات وإرشادات داخل البنك المركزي وتعليماته، لكن ثغرات في التكوين التقني للكوادر بنية الإبلاغ عن الحوادث السيبرانية, وإطار اختبار الاستجابة للحوادث (incident response) تعوق تنفيذ سياسة وطنية موحدة للمرونة التشغيلية.

ثانياً: التوصيات:

1. نوصي بتأسيس وحدات تقنية رقابية قضائية وتجهيز وحدات فنية متخصصة داخل مراكز التحقيق الجزائي والنيابات العامة مزودة بخبراء تقنية معلومات وقواعد للتعامل مع الأدلة الرقمية وإجراءات السلاسة في سلسلة الحفظ (chain of custody) وإمكانية التعاون مع جهات فنية مركزية.

2. نوصي بتدريب القضاة والمدعين العامين على برامج تدريب منهجية على أحكام القانون الإلكتروني، ومبادئ التحليل الجنائي الرقمي، لتقييم الأدلة الرقمية وقبولها أثناء المحاكمة.

3. ندعوا للعمل على إبرام اتفاقيات دولية للتمكن من تبادل الأدلة إلالكترونية والتعاون في التحقيقات مع دول ذات خبرة وعضوّيات إقليمية ودولية، والاستفادة من آليات هذه الاتفاقيات لتسهيل استرداد الأدلة وإجراءات المساعدة القضائية.

4. نوصي بتطوير وتعزيز الأمن والمناعة في النظام المصرفي العراقي لمواجهة الجرائم السيبرانية والرقمية. وذلك بإصدار قانون شامل للجرائم السيبرانية، وتعزيز متطلبات المرونة من البنك المركزي، ودعم القدرات التقنية القضائية والمصرفية مدعومة باستراتيجية وطنية للهوية الرقمية , وينبغي أن يكون ضمن أعلى الأولويات. ويوفر ذلك مرونة لكل من بُعد الأمن، وفي الوقت نفسه يعزز ثقة المستهلك في نظم المصارف، ويقود إلى تحول رقمي آمن للنظام المالي.

5. نوصي بأعتماد المعايير القضائية لقبول الأدلة الرقمية, وكذلك وضع معايير قضائية وطنية لقبول نتائج التحليل الفني (forensic reports) من مختبرات معتمدة، ومتطلبات للشهادة الخبيرة في القضايا السيبرانية.

المصادر

اولا: الكتب

1. إبراهيم حامد الطنطاوي، الحماية الجنائية لسرية معلومات البنوك عن عملائها: دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2005.
2. جمال إبراهيم الحيدري، أحكام المسؤولية الجزائية، منشورات زين الحقوقية، بيروت، 2010.
3. سعيد عبد اللطيف حسن، الحماية الجنائية للسرية المصرفية: دراسة مقارنة، دار النهضة العربية، القاهرة، 2004.
4. عادل محمد السيوي، التعاون الدولي في مكافحة غسل الأموال وتمويل الإرهاب، الطبعة الأولى، 2010.
5. علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية، الجزء الثاني، الطبعة الأولى، دار النهضة العربية، القاهرة، 1989.
6. علي عبد القادر القهوجي، شرح قانون العقوبات: القسم العام، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008.
7. فخري عبد الرزاق صلبي الحديثي، شرح قانون العقوبات: القسم العام، الطبعة الثانية، بغداد، ساعدت جامعة بغداد على طبعه، 2010.
8. محمود نجيب حسني، شرح قانون العقوبات: القسم العام، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1989.

ثانياً: الرسائل الجامعية

1. بدر تراك سليمان الشمري، الجوانب القانونية المتعلقة بسر المهنة المصرفية: دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا، الجامعة الأردنية.
2. خليل يوسف الجندي، المسؤولية الجزائية الناشئة عن الاعتداء على سرية الحسابات المصرفية، رسالة ماجستير، كلية القانون، جامعة الموصل، 2002.
3. عادل يوسف عبد النبي الشكري، المسؤولية الجنائية الناشئة عن الإهمال، رسالة ماجستير، كلية القانون، جامعة بابل، 2005.
4. عدنان خلف محيي، جريمة إفشاء سر المهنة في القانون العراقي، رسالة ماجستير، كلية القانون، جامعة بغداد، 1998.
5. وسام كاظم زغير، إفشاء الأسرار وأثره في المسؤولية الجزائية، رسالة ماجستير، كلية القانون، الجامعة المستنصرية، 2013.

ثالثاً: المجلات العلمية

1. إياد خلف محمد، المسؤولية الجزائية عن إفشاء السرية المصرفية، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 23، 2010.
2. سامر سعدون العامري، وكوثر عبد الرزاق عبد الله، جريمة إفشاء السرية المصرفية وآثارها الجزائية، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، المجلد 33، العدد 6، 2019، ص 448–478.
3. علي فوزي إبراهيم، الموازنة بين الالتزام بحفظ السر المصرفي وظاهرة غسيل الأموال، مجلة دراسات قانونية، بيت الحكمة، بغداد، العدد 24، 2009.
4. لمى وهّاب إبراهيم، التزامات المرخّص له في مكافحة غسل الأموال وتمويل الإرهاب، مجلة جامعة بابل للعلوم الإنسانية، جامعة بابل، المجلد 27، العدد 3، 2019.
5. ميادة صلاح الدين تاج الدين، السرية المصرفية: آثارها وجوانبها التشريعية: دراسة مقارنة، مجلة تنمية الرافدين، جامعة الموصل، كلية الإدارة والاقتصاد، المجلد 31، العدد 95، 2009.

رابعاً: القوانين والضوابط:–

أ– العراقية

1– البنك المركزي العراقي، ضوابط مكافحة غسل الأموال وتمويل الإرهاب لمقدمي خدمات الدفع الإلكتروني، بغداد، 2025، إصدار رسمي، فقرات إدارة مخاطر الدفع الإلكتروني.
2– قانون العقوبات العراقي رقم 111 لسنة 1969.
3– قانون المصارف العراقي رقم 94 لسنة 2004، والممارسات التنظيمية للبنك المركزي العراقي المتعلقة بحوكمة البنوك.
4– قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 39 لسنة 2015 .

ب- المصرية

1- قانون البنك المركزي والجهاز المصرفي المصري رقم 194 لسنة 2020، القاهرة، تشريع رسمي، 2020، مواد سرية حسابات العملاء وحماية نظم الدفع.

2- قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ولائحته التنفيذية، القاهرة، تشريع رسمي، 2020/2018.

ج- الاردنية

1- قانون البنوك الأردني رقم 28 لسنة 2000 وتعديلاته، لإيضاح الإطار المصرفي الأردني.

2- قانون الجرائم الإلكترونية الاردني رقم 17 لسنة 2023، عمان، تشريع رسمي، 2023، المواد المتعلقة بالدخول غير المشروع والاعتراض والاحتيال والبيانات.