



الحماية القانونية للعمليات المصرفية الإلكترونية
في ضوء تحديات الأمن السيبراني
"دراسة مقارنة"

مخطط بحث لاستكمال متطلبات الحصول على درجة الماجستير في القانون الخاص

إعداد الطالبة: حصه عبدالواحد نجم

الرقم الأكاديمي: 20125356

إشراف الدكتور: سامر محمد الزعبي

أستاذ القانون التجاري المساعد

جامعة البحرين

مملكة البحرين

2024م.

المخلص

أكد المشرع البحريني على ضرورة توفير الحماية القانونية للمعاملات التي تجري بواسطة أحد وسائل تقنية المعلومات، فالتطور التكنولوجي يحتاج إلى مظلة تشريعية قادرة على توفير الحماية القانونية لمستخدمي شبكة الانترنت، لذلك سعت مملكة البحرين إلى تطوير التشريعات التي من شأنها توفير وتعزيز الحماية القانونية للعمليات التي تحدث من خلال الفضاء السيبراني.

ومن أهم التشريعات التي سنّها المشرع البحريني؛ القانون البحريني رقم (54) لسنة 2018م بشأن الخطابات والمعاملات الإلكترونية وقانون رقم (30) لسنة 2018 بإصدار قانون حماية البيانات الشخصية إذ تعد هذه التشريعات إطاراً حامياً للمعاملات التي تجري من خلال أحد وسائل تقنية المعلومات.

ستتناول هذه الدراسة مفهوم العمليات المصرفية الإلكترونية والمخاطر السيبرانية التي تتعرض لها من خلال توضيح التوجه الحاصل لرقمنة هذه العمليات من أجل تعزيز القطاع المصرفي مما ينعكس ايجاباً في تشجيع الاستثمار في مملكة البحرين.

إذ تشكل العمليات المصرفية الإلكترونية الآن الخيار الأسهل لعملاء المصارف حيث تسعى المؤسسات المصرفية لتوفير المرونة والجودة اللازمين عند ممارسة العمليات المصرفية والتي من شأنها تحقيق رضا العميل المصرفي، وعلى الرغم من أن المرونة والجودة غالباً ما تكون من جانب تقني باعتبار أن العمليات المصرفية تقام في إطار إلكتروني إلا إنه لا بد من تحقق أمن هذه العمليات وفق أسس وقواعد منظمة قادرة على حماية العميل أثناء ممارسة الخدمة المصرفية الإلكترونية.

حيث إن العمليات المصرفية الإلكترونية لاقت معارضة وتخوف من ممارسة العمليات المصرفية في بادئ الأمر إلا إنه وحتى هذا اليوم فإنه لا يمكن إغفال العدد الكبير من المعاملات المصرفية التي تحدث يومياً في العالم إلكترونياً، إذ إن القطاع المصرفي والعمليات المصرفية بحد ذاتها ذاتها مجال يحوز على أهمية كبيرة إذ سهل عمل العديد من العمليات التجارية والاستثمارية ونماها لعديد من الأسباب أهمها الانسيابية في إتمام التحويلات المصرفية، والدفع الإلكتروني في مجال التجارة الإلكترونية على سبيل المثال، إلا إنه على الرغم من ذلك فإن هذه المرونة والانسيابية لازمتها مخاطر وخسائر جسيمة بسبب تعرضها لانتهاكات من قبل أشخاص غايتهم الاستيلاء على أموال الغير بطرق غير مشروعة أو معلومات سرية غير متاحة إلا لجهات معينة.

ولذلك فإن كثرة الهجمات الإلكترونية على العمليات المصرفية الإلكترونية أوجب تحركا دوليا من أجل حماية القطاع المصرفي من خلال سن تشريعات تضمن أمن وحماية القطاع المصرفي فضلا عن جهود دولية بإبرام اتفاقات دولية تضمن سير القطاع المالي بصورة منتظمة وديناميكية تحت إطار قانوني واضح وسليم قادر على أن يوفر الحماية القانونية اللازمة للعمليات المصرفية.

الحمد لله عانقت اليوم مجداً عظيماً، كان درباً طويلاً قاسياً، ولكنني وصلت بفضل الله وكرمه بعد أيام التشوق والعناء، اليوم أختتم أطروحة الماجستير في القانون الخاص، بكل ما لدي من همّة، فالحمد لله من قبل ومن بعد..

أهدي هذه الأطروحة :

إلى العزيز الذي حملت اسمه فخراً، إلى من فارقتني بجسده وروحه ومازال حاضراً في قلبي، إلى الروح الطاهرة (والدي العزيز) رحمه الله..

إلى من كانت الداعمة الأولى والأبدية، من كان وجودها يمدني بالسعي دون ملل، من كافحت لأجل وصولي، أهديك هذا الإنجاز الذي لولاك لم يكن، كنت لي الأم والأب منذ طفولتي ياخير عوض ويا أعظم سند (والدتي العزيزة) ..

إلى خيرة أيامي وصفوتها إلى من مدت لي أياديهم وقت ضعفي وآمنوا بقدرتي وراهنوا على نجاحي،(أخواتي، إخواني، عمران) ..

إلى الذين يبهجهم نجاحي، ومن كان عوناً وسنداً في هذا الطريق منذ البداية (أصدقاء ورفقاء السنين) ..

إلى مشرف رسالتي، الذي لطالمها وجهني وساعدني لإتمام الأطروحة بهذا الشكل (د. سامر محمد الزعبي) ..

أهدي هذا النجاح لنفسِي، التي ترقبت حلماً طال انتظاره وتحقق بفضل من الله وأصبح واقعاً افتخر به ..

الشكر والتقدير

الحمد لله حباً وشكراً وامتناناً، الحمد لله بفضلته أدركت أسمى الغايات ..

فلله الفضل وله الحمد، ماكنت لأختم مسيرتي هذه لولا فضله فالحمد لله عند البدء والختام،
الحمد لله مانتهى درب، ولا ختم جهد، ولا تم سعي إلا بفضلته، الحمد لله على التمام والكمال
وعلى لذة الإنجاز ..

أتقدم بالشكر الجزيل لجامعة البحرين وأساتذتي في كلية الحقوق على دعمهم الدائم
وتوجيهاتهم البناءة والقيمة لإتمام الإطروحة..

كل الشكر والتقدير والامتنان لكل شخص كان له الفضل في مسيرتي وقدم لي المساعدة
والتوجيه ..

لكم خالص احترامي وتقديري..

الفهرس

أ-ب	الملخص باللغة العربية
ج	الإهداء
د	الشكر والتقدير
10-1	المقدمة
11	الفصل الأول: مفهوم العمليات المصرفية الإلكترونية في ظل المخاطر السيبرانية
12	1) المبحث الأول: مفهوم العمليات المصرفية الإلكترونية وأبرز أنواعها
13	أ- المطلب الأول: ماهية العمليات المصرفية الإلكترونية
14	<u>-الفرع الأول: المفهوم العام للعمليات المصرفية (الإلكترونية والتقليدية)</u>
14-16	- أولاً: تعريف العمليات المصرفية التقليدية والإلكترونية
19-16	- ثانياً: المفهوم العام للبنك
19	<u>-الفرع الثاني: المفهوم السائد للعمليات المصرفية الإلكترونية والتجارة الإلكترونية</u>
19-21	- أولاً: مفهوم التجارة الإلكترونية
21-23	- ثانياً: ارتباط العمليات المصرفية الإلكترونية بالتجارة الإلكترونية:
24	ب-المطلب الثاني: أهم أنواع العمليات المصرفية الإلكترونية وخصائصها(الدفع الإلكتروني نموذج)
25	<u>-الفرع الأول: عملية الدفع الإلكتروني</u>
28 -25	- أولاً: مفهوم الدفع الإلكتروني
32 -28	- ثانياً: خصائص الدفع الإلكتروني
32	<u>-الفرع الثاني: مخاطر استعمال عمليات الدفع الإلكتروني</u>
35-33	- أولاً: مخاطر الاستعمال
35	- ثانياً: المخاطر المرتبطة بالأمان والسرية
37-36	- ثالثاً: المخاطر التقنية والتشغيلية
38	ج-المطلب الثالث: مزايا وعيوب العمليات المصرفية الإلكترونية
39	<u>-الفرع الأول: مزايا العمليات المصرفية الإلكترونية</u>
40-39	- أولاً: زيادة الراحة وتوفير الوقت
40	- ثانياً: توفير في التكاليف ورفع الكفاءة
40	- ثالثاً: الانتشار والقدرة على الوصول إلى قاعدة أوسع من العملاء

41	- رابعاً: الأمان والموثوقية
41	- الفرع الثاني: عيوب العمليات المصرفية الإلكترونية
41	- أولاً: التعرض للهجمات الإلكترونية
42	- ثانياً: عدم الإلمام الإلكتروني
42	- ثالثاً: زيادة التكلفة الناتجة عن استخدام التقنيات الإلكترونية
42	- رابعاً: الأخطاء التقنية والفنية
43-42	- خامساً: صعوبة الوصول إلى المجرم المعلوماتي
44	(2) المبحث الثاني: ماهية المخاطر السيبرانية في القطاع المصرفي
45	المطلب الأول: المخاطر السيبرانية بين المفهوم والتنظيم القانوني
48-46	- الفرع الأول: مفهوم المخاطر السيبرانية
48	- أولاً: المخاطر التقليدية
49-48	- ثانياً: المخاطر السيبرانية
51-49	- الفرع الثاني: التنظيم القانوني للمخاطر السيبرانية
52-51	- أولاً: مخاطر التشغيل
52	- ثانياً: مخاطر السمعة
53-52	- ثالثاً: المخاطر القانونية
54	المطلب الثاني: دور الأمن السيبراني في القطاع المصرفي
57-55	- الفرع الأول: أهمية الأمن السيبراني في القطاع المصرفي
57	- الفرع الثاني: الجهود الدولية المتبعة للحد من المخاطر السيبرانية على القطاع المصرفي
60-58	- أولاً: من حيث التعاون الدولي
64-61	- ثانياً: من حيث الإطار التشريعي
65	المطلب الثالث: معوقات تعزيز الأمن السيبراني في القطاع المصرفي
66	- الفرع الأول: معوقات تعزيز الأمن السيبراني
66	- أولاً: عدم وجود استراتيجيات شاملة للأمن السيبراني
66	- ثانياً: التدابير التفاعلية بدلاً من التدابير الاستباقية
67	- ثالثاً: تخصيص الموارد غير الكافية
67	- رابعاً: قلة الوعي والتدريب

68	-الفرع الثاني: طرق لتعزيز الأمن السيبراني المصرفي
68	- أولاً: الشراكة بين القطاع العام والقطاع الخاص
68	- ثانياً: تعزيز البحث والابتكار في مجال الأمن السيبراني
68	- ثالثاً: تطوير البنية التحتية (التقنية والبشرية)
69	- رابعاً: وضع استراتيجية لتعزيز الأمن السيبراني
70-69	- خامساً: استخدام تقنيات مبتكرة كالذكاء الاصطناعي
71	الفصل الثاني: طرق الحماية القانونية للعمليات المصرفية الإلكترونية وآثارها على الاقتصاد الوطني
72	1) المبحث الأول: الآليات القانونية المتبعة لحماية العمليات المصرفية الإلكترونية
73	المطلب الأول: الرقابة على العمليات المصرفية الإلكترونية وآليات الحماية المتبعة
74	-الفرع الأول: مفهوم الرقابة على العمليات المصرفية الإلكترونية
75-74	- أولاً: تعريف الرقابة على العمليات المصرفية الإلكترونية
77-75	- ثانياً: أنواع الرقابة على العمليات المصرفية الإلكترونية:
77	-الفرع الثاني: أشكال الرقابة على العمليات المصرفية الإلكترونية
79-77	- أولاً: الرقابة القانونية
80-79	- ثانياً: الرقابة التشغيلية
81	المطلب الثاني: دور الحفاظ على سرية البيانات الشخصية (سرية المعلومات) في تعزيز الحماية
82	-الفرع الأول: جوانب الحفاظ على سرية المعلومات في العمليات المصرفية الإلكترونية
84-82	- أولاً: أمن المعلومات بين الخصوصية والتوافر
86-84	- ثانياً: مفهوم البيانات الشخصية في نطاق الخدمات المصرفية الإلكترونية
88-86	-الفرع الثاني: النطاق القانوني لحماية البيانات الشخصية
89	المطلب الثالث: الطبيعة القانونية لمسئولية المصارف أثناء ممارسة العمليات المصرفية الإلكترونية
90	-الفرع الأول: مسؤولية المصرف العقدية
92-90	- أولاً: الخطأ الإلكتروني كركن لقيام المسؤولية العقدية

94-92	- ثانياً: الضرر كركن لقيام المسؤولية العقدية
95-94	- ثالثاً: العلاقة السببية كركن لقيام المسؤولية العقدية
95	- <u>الفرع الثاني: مسؤولية المصرف التقصيرية</u>
98-95	- أولاً: أساس مسؤولية المصرف التقصيرية
100-98	- ثانياً: جوانب الاختلاف بين المسؤولية التقصيرية والمسؤولية العقدية
101	(2) المبحث الثاني: آثار حماية العمليات المصرفية الإلكترونية
102	المطلب الأول: الأثر المباشر لحماية العمليات المصرفية الإلكترونية
105-103	- <u>الفرع الأول: أثر حماية العمليات المصرفية الإلكترونية على المصرف</u>
108-106	- <u>الفرع الثاني: أثر حماية العمليات المصرفية الإلكترونية على العميل</u>
109	المطلب الثاني: الأثر غير المباشر لحماية العمليات المصرفية الإلكترونية
112-110	- <u>الفرع الأول: أثر حماية العمليات المصرفية الإلكترونية على الدولة</u>
112	- <u>الفرع الثاني: انعكاس أثر الحماية على جذب الاستثمارات الأجنبية</u>
114-113	- أولاً: أهمية الاستثمار الأجنبي على التنمية الاقتصادية
117-114	- ثانياً: مساعي قانونية لجذب الاستثمارات الأجنبية
125-118	المطلب الثالث: تطبيقات عملية لقضايا انتهاك عمليات مصرفية إلكترونية
127-126	الخاتمة (النتائج والتوصيات)
146-128	قائمة المراجع
147	الملخص باللغة الإنجليزية

المقدمة

يحوز المجال الاقتصادي وبالأخص القطاع المالي على اهتمام كبير من قبل الدول، نظراً لما له من دور في رفع الاقتصاد، وتحقيق النمو في الناتج المحلي، لذلك تتوجه أنظار الدولة إلى تحقيق الاستقرار المالي، وخصوصاً استقرار المؤسسات المالية فيها، إذ تلعب هذه المؤسسات دوراً هاماً في تعزيز المؤشرات الاقتصادية للدولة، حيث ثبت في بيان المؤشرات الاقتصادية المنشور عن مصرف البحرين المركزي للعام 2023م، إذ يساهم القطاع المصرفي في الناتج المحلي الإجمالي لمملكة البحرين بمقدار 17.8%، وبالتالي فإن التركيز على تطوير القطاع المصرفي أمر لا بد منه، خصوصاً أن مملكة البحرين أصبحت مركزاً مالياً مهماً له تأثير مباشر على السوق المالي في دول مجلس التعاون والشرق الأوسط، إذ يبلغ العدد الإجمالي للبنوك في مملكة البحرين حتى أبريل 2024م عدد 84 بنكاً، من بينها بنوك أجنبية وبنوك محلية¹، وعليه فإنه هذا الكم من البنوك التي تؤثر بشكل كبير على القطاع الاقتصادي في مملكة البحرين، يجب أن يصاحبه بنية تحتية تبين عمل هذه المؤسسات وفق إطار قانوني سليم، بحيث تتحقق معها الأهداف المرجوة.

أحدث التطور التكنولوجي قفزة نوعية في مجالات الاستثمار والعمل في القطاع المصرفي، فبدخول التكنولوجيا المالية والتوسع الكبير في القطاع المصرفي، أصبحت المصارف تتعرض لهجمات من خلال الفضاء السيبراني، ومن الصعب عليها صدها كمرحلة أولية، أو تجاوزها في المرحلة التالية على الهجمة؛ لذلك فإن المستثمرين في المصارف يزيحون النظر عن الدول التي لا توفر لهم الحماية القانونية لصد الهجمات السيبرانية، والتي تؤثر بشكل كبير على مواردها المالية.

تتفاوت قدرة الدول في التصدي إلى الهجمات السيبرانية على حسب مواردها، وبسبب الارتباط بين القطاع المالي والتكنولوجيا في الوقت الحالي، فإن أي هجمة سيبرانية ناجحة على مؤسسات مالية كبرى أو خدمات مالية يقدمها المصرف، يمكن أن ينتشر أثرها سريعاً في النظام المالي، مما يؤدي بدوره إلى اضطراب وعدم استقرار في القطاع المالي، وزعزعة الثقة بين الأفراد والمصارف، ومن جانب آخر فإن ذلك يؤدي إلى عدم ثقة المستثمرين من المؤسسات المصرفية وقدرة الدولة على توفير الحماية اللازمة لصد هذه الهجمات.

هناك عدداً من الحالات التي تم طرحها في مختلف الدول للاختراقات التي حدثت في القطاع المصرفي، والتي أدت إلى تحمل المصرف مسؤولية تعويض العملاء عن الخسائر الناجمة

¹ بيان عن القطاع المالي | مصرف البحرين المركزي (cbb.gov.bh).

جراء انتهاك البيانات والحسابات المصرفية، كالانتهاك الحاصل في مملكة البحرين واختراق 174 بطاقة صراف آلي وائتمان لبعض العملاء في عام 2014م²، مما حدا بالبنوك إلى تعويض العملاء عن هذه الانتهاكات، وحالة الاختراق التي حصلت في مصرف عملاء مصرف "كابيتال وان" الأمريكي، حيث تمت سرقة معلومات وبيانات شخصية لعملاء أمريكيين وكنديين للمصرف، من قبل مهندسة معلوماتية وتم القبض عليها في العام 2019م³. ولا يخفى أن هناك عدداً كبيراً من حالات القرصنة التي تستهدف المصارف من خلال الخدمات الإلكترونية التي يقدمها المصرف، كالدفع الإلكتروني وما يدخل في مجال التجارة الإلكترونية.

ولكي نوفّر جداراً متيناً قادراً على التصدي للهجمات التي تتعرض لها المصارف لابد من توفير بيئة تقنية محكمة وإطار قانوني واضح وسليم قادر على أن يتماشى مع التطور التكنولوجي، وعليه سنت مملكة البحرين سلسلة من التشريعات التي تنظم العمليات الإلكترونية، لذلك فإنه لا بد من طرح المفهوم القانوني للعمليات المصرفية الإلكترونية، والمخاطر التي تواجهها، وارتكازاً على ما يمكن أن يتعرض له الاقتصاد من مخاطر نتيجة الوصول إلى معلومات حساسة تتعلق بالبيانات الشخصية للمستهلكين، فإن فكرة هذه الدراسة تتبلور في توضيح الجوانب القانونية للعمليات المصرفية الإلكترونية، والجهود المبذولة من قبل الأطراف ذات العلاقة لتوفير الحماية القانونية اللازمة، فضلاً عن أثر أمن العمليات المصرفية الإلكترونية على جذب الاستثمارات في القطاع المصرفي.

أولاً : أسباب اختيار موضوع البحث:

نسعى من خلال هذه الدراسة إلى بيان الإطار التشريعي في الحفاظ على أمن العمليات المصرفية الإلكترونية، وتوضيح المخاطر التي تحيط بهذه العمليات، إلى جانب الأثر الممتد إلى المستهلكين من عملاء المصارف، حيث قد تطالهم أضراراً لا يمكن تداركها، ومن الصعب إيجاد حل لها إن وقعت.

فضلاً أن الطفرة التكنولوجية التي دخلت في الخدمات المالية، توجب علينا النظر في التشريعات المنظمة للهجمات السيبرانية التي تطال المصارف، والتي تؤثر بدورها بشكل مباشر

² خالد موسى، البنوك عوّضت المتضررين من حادثة اختراق البطاقات البنكية، صحيفة الأيام البحرينية، العدد 9337، مملكة البحرين، 2014م. [البنوك عوّضت المتضررين من حادثة اختراق البطاقات البنكية - صحيفة الأيام البحرينية \(alayam.com\)](http://alayam.com)
³ Capital One to pay \$80 million fine for 2019 hack that exposed 100 million accounts - CBS News.

على عدم استقرار القطاع المالي، وزعزعة ثقة الأفراد في قدرة المصارف على حماية أموال العملاء أثناء إجراء أي من العمليات المصرفية الإلكترونية.

كما سيبين الباحث دور التشريعات الوطنية في حماية العمليات المصرفية، وإسهام المنظمات الدولية والموقف الدولي في تعزيز وحث الدول على سن تشريعات تنظم الخدمات المالية التي تقدمها المصارف من خلال الفضاء السيبراني.

ثانياً: أهمية البحث:

تكمن أهمية البحث في التحديات التي تواجه المؤسسات المالية، ومسئوليتها تجاه العملاء في ضمان معاملات مالية ميسرة ومؤتمنة، دون خوف من التعرض لضياح هذه الأموال، والتي زادت وتيرتها مؤخراً بسبب القيود والاحتياطات التي نشأت جراء انتشار فيروس كوفيد-19، إذ حثت الحكومات على التحول الرقمي في أغلب العمليات إلكترونياً، دون الحاجة إلى حضور شخصي من قبل العميل، فضلاً عن المعوقات التي تواجه الدولة للحفاظ على الاستقرار في القطاع المالي، والحيلولة دون وقوع هذه الهجمات، إذ يشكل القطاع المالي الركيزة الأساسية لجذب العديد من الاستثمارات، يحتم على الدولة بذل جهودٍ مدروسةٍ بحيث توفر البنية التقنية اللازمة لبناء جدارٍ واقٍ لصد الهجمات السيبرانية، إلى جانب توافر التشريعات والقواعد القانونية التي تلزم المؤسسات التي تتعرض لهذه الهجمات بالإفصاح عنها للجهات المنوط بها مراقبتها.

ندرة البحوث التي تتعلق بالعمليات المصرفية الإلكترونية في ظل توجهات الحفاظ على البيئة السيبرانية في المجتمع البحريني والمجتمعات المجاورة تحتم علينا بيان العمليات المصرفية الإلكترونية، ودور المؤسسات المصرفية في إطار تعزيز الأمن السيبراني في القطاع المصرفي بداية كمفهوم، وإظهار التحديات والمعوقات التي تواجه المؤسسات المالية والدولة، إلى جانب توضيح دور التشريعات المحلية وتجارب الدول، في توفير الحماية القانونية للمؤسسات المالية وعملاء المصارف، فضلاً عن دور أمن العمليات المصرفية في جذب الاستثمارات إلى مملكة البحرين.

ثالثاً: الدراسات السابقة:

من خلال البحث في موضوع العمليات المصرفية الإلكترونية من الجانب القانوني وجدنا أن في غالب الدراسات يتم التركيز عليها وفق القانون العام والنظر فيها من الناحية الاقتصادية دون التطرق للقانون الخاص كما تبحث في العمليات المصرفية الإلكترونية دون المخاطر والمسئولية التي تتعرض لها، ومن أهم الدراسات التي كان لها علاقة مباشرة بموضوع الدراسة هي:

1- إيلاف فاخر كاظم، مخاطر العمليات المصرفية الإلكترونية، المركز العربي للنشر والتوزيع، مصر، 2019م. إذ تطرقت الباحثة إلى بشكل عام إلى مفهوم العمليات المصرفية الإلكترونية والمخاطر التي تواجهها، فضلاً عن الإثبات وسرية المعلومات والمسئولية القانونية.

2- حنان بوعكوش، شادية زايدي، حماية العمليات المصرفية في ظل تطور الصيرفة الإلكترونية، جامعة العربي التبسي، رسالة ماجستير، الجزائر، 2019م. حيث تناولت الباحثة العمليات المصرفية الإلكترونية من حيث المفهوم والحماية من مخاطرها من الجانب الاقتصادي.

3- النظام القانوني للبنوك الإلكترونية، رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، الجزائر، 2018. حيث تناولت الباحثة بشكل أكبر مفهوم البنوك الإلكترونية فضلاً عن الإشكاليات القانونية التي تتعرض لها البنوك الإلكترونية بما فيها من مسؤولية مدنية وجنائية والمخاطر التي تتعرض لها المصارف في طور التقدم التكنولوجي.

وعليه، بعد مطالعة الدراسات المتعلقة بموضوع البحث نرى أن الدراسات السابقة تركز على المفهوم إما من ناحية اقتصادية أو ناحية قانونية دون الجمع فيما بينهم لذلك في هذه الدراسة سيتم الاعتماد على موضوعات لم يتم التطرق إليها بشكل تفصيلي والتركيز على جوانب اقتصادية وقانونية والربط فيما بينهما لارتباطهما الوثيق الذي يؤدي إلى تحسين مستوى العمليات المصرفية الإلكترونية، وذلك من خلال مناقشة المخاطر السيبرانية التي تواجه العمليات المصرفية الإلكترونية وتبسيط الضوء على المسؤولية المدنية، إلى جانب أثر الحماية القانونية وأثرها على نمو الاقتصاد في مملكة البحرين.

رابعاً: منهج البحث:

يعد موضوع الدراسة من المواضيع الحديثة، التي تتطلب شرحاً دقيقاً ومتعمقاً، بدءاً ببيان الجوانب القانونية الخاصة بالعمليات المصرفية الإلكترونية، وعليه ستتبع الدراسة المنهج الوصفي التحليلي، وذلك لتحديد مفهوم العمليات المصرفية، وذكر أبرز أنواع العمليات المصرفية تعرضاً للتعدي من قبل المجرم المعلوماتي، وتحليل المخاطر المرتبطة بالفضاء السيبراني، وتحديد كيفية إدارتها، وبيان مدى أثر أمن العمليات المصرفية على جذب الاستثمارات الأجنبية، فضلاً عن محاولة إيجاد حلول للمشكلات، وسدّ للثغرات القانونية إن وجدت، وذلك لتحقيق الأهداف المرجوة من سنّ هذه التشريعات، عن طريق مقارنتها بالتشريعات الأخرى محل الدراسة.

خامساً: مشكلة البحث:

تتلخص مشكلة البحث في الانتشار السريع الذي اتسمت به الجرائم السيبرانية، والتي طالت المعاملات المالية التي يقوم بها الأفراد، عن طريق وسيلة من وسائل تقنية المعلومات، سواءً عن طريق الهاتف أو شبكة الحاسوب أو غيرها، فضلاً عن الأثر الذي تواجهه الدولة جراء الاعتداءات التي تقع على المصارف، لذلك فإن الدراسة تتطلب معرفة كفاءة التشريعات التي تنظم العمليات المصرفية في شقها الإلكتروني، وماهية المعوقات التي تواجه المصارف أثناء وقوع الجريمة السيبرانية؟ وهل التشريعات الصادرة في مملكة البحرين قادرة على حماية المصرف من هذه الهجمات أو تداركها؟ وما مدى رقابة مصرف البحرين المركزي على المعاملات المصرفية الإلكترونية؟ وهل الآليات التي سنتها القوانين المنظمة للعملية الإلكترونية قادرة على توفير الحماية للمعاملة المصرفية؟ وما مدى ارتباط أمن العمليات المصرفية بتحقيق أهداف التنمية وخلق بيئة استثمارية جاذبة للمصارف الأجنبية؟.

سادساً: تساؤلات البحث:

1. ما المقصود بالعمليات المصرفية الإلكترونية؟ وماهي المخاطر السيبرانية التي تواجه القطاع المصرفي؟
2. دور المصرف المركزي في ضمان الأمن السيبراني للعمليات المصرفية الإلكترونية؟
3. مدى مسؤولية المصرف والعميل في حالة حدوث الاختراق السيبراني؟
4. ما الآليات القانونية التي أوجدتها التشريعات للمحافظة على أمن القطاع المصرفي؟
5. هل القوانين والتشريعات الحالية قادرة على حماية المصارف من الاختراقات السيبرانية ؟

سابعاً: أهداف البحث:

تهدف هذه الدراسة إلى بيان إمكانية التشريعات التي تنظم العمليات المصرفية الإلكترونية من ردع الجرائم السيبرانية الواقعة على المصارف إلى جانب نشر الوعي في مجال الخدمات المالية الإلكترونية بالإضافة إلى الوصول لحلول للمعوقات والمشكلات التي تواجه المصارف عند حدوث الجريمة السيبرانية في إطار القانون البحريني والتشريعات المقارنة، والتعرف على الآليات القانونية التي أوجدتها التشريعات للمحافظة على الأمن السيبراني في القطاع المصرفي، فضلاً عن التعرف على الالتزامات الملقاة على عاتق كل من العملاء والمصارف للمحافظة على الأمن في القطاع المصرفي، وطبيعة المسؤولية القانونية على كل من المصرف والعميل، أثناء ممارسة العملية المصرفية الإلكترونية.

ثامناً: نطاق البحث:

يسعى الباحث إلى بيان مفهوم العمليات المصرفية الإلكترونية: والتحديات التي تواجه المصارف في الحفاظ على أمن العمليات المصرفية، وأثر الإجراءات والآليات القانونية التي حددها المشرع البحريني لفرض الحماية للعمليات المصرفية، والتي بدورها تحفز الاستثمارات الأجنبية إلى الدخول للقطاع المصرفي في مملكة البحرين، وعلى هذا فإننا سنتناول في هذا البحث مرسوم بقانون رقم (7) لسنة 1987م بإصدار قانون التجارة، والقانون البحريني رقم (54) لسنة 2018م بشأن الخطابات والمعاملات الإلكترونية، والقانون رقم 30 لسنة 2018م لحماية البيانات الشخصية، والقانون الإماراتي الاتحادي رقم (34) لسنة 2021م بشأن مكافحة الشائعات والجرائم الإلكترونية، والقانون الإماراتي الاتحادي رقم (1) لسنة 2006م بشأن المعاملات والتجارة الإلكترونية.

تاسعاً: تقسيم البحث:

الفصل الأول: مفهوم العمليات المصرفية الإلكترونية في ظل المخاطر السيبرانية.

المبحث الأول: مفهوم العمليات المصرفية الإلكترونية وأبرز أنواعها.

المطلب الأول: ماهية العمليات المصرفية الإلكترونية.

الفرع الأول: المفهوم العام للعمليات المصرفية (الإلكترونية والتقليدية).

أولاً: تعريف العمليات المصرفية التقليدية والإلكترونية.

ثانياً: المفهوم العام للبنك.

الفرع الثاني: المفهوم السائد للعمليات المصرفية الإلكترونية والتجارة الإلكترونية.

أولاً: مفهوم التجارة الإلكترونية.

ثانياً: ارتباط العمليات المصرفية الإلكترونية بالتجارة الإلكترونية.

المطلب الثاني: أنواع العمليات المصرفية الإلكترونية وخصائصها.

الفرع الأول: عملية الدفع الإلكتروني.

أولاً: مفهوم الدفع الإلكتروني.

ثانياً: خصائص الدفع الإلكتروني.

الفرع الثاني: مخاطر استعمال عمليات الدفع الإلكتروني.

أولاً: مخاطر الاستعمال.

ثانياً: المخاطر المرتبطة بالأمان والسرية.

ثالثاً: المخاطر التقنية والتشغيلية.

المطلب الثالث: مزايا وعيوب العمليات المصرفية الإلكترونية.

الفرع الأول: مزايا العمليات المصرفية الإلكترونية.

أولاً: زيادة الراحة وتوفير الوقت.

ثانياً: توفير في التكاليف ورفع الكفاءة.

ثالثاً: الانتشار والقدرة على الوصول إلى قاعدة أوسع من العملاء.

رابعاً: الأمان والموثوقية.

الفرع الثاني: عيوب العمليات المصرفية الإلكترونية.

أولاً: التعرض للهجمات الإلكترونية.

ثانياً: عدم الإلمام الإلكتروني.

ثالثاً: زيادة التكلفة الناتجة عن استخدام التقنيات الإلكترونية.

رابعاً: الأخطاء التقنية والفنية.

خامساً: صعوبة الوصول إلى المجرم المعلوماتي:

المبحث الثاني: ماهية المخاطر السيبرانية في القطاع المصرفي.

المطلب الأول: المخاطر السيبرانية بين المفهوم والتنظيم القانوني.

الفرع الأول: مفهوم المخاطر السيبرانية.

أولاً: المخاطر التقليدية.

ثانياً: المخاطر السيبرانية.

الفرع الثاني: التنظيم القانوني للمخاطر السيبرانية.

أولاً: مخاطر التشغيل.

ثانياً: مخاطر السمعة.

ثالثاً: المخاطر القانونية.

المطلب الثاني: دور الأمن السيبراني في القطاع المصرفي.

الفرع الأول: أهمية الأمن السيبراني في القطاع المصرفي.

الفرع الثاني: الجهود الدولية المتبعة للحد من المخاطر السيبرانية على القطاع المصرفي.

أولاً: من حيث التعاون الدولي.

ثانياً: من حيث الإطار التشريعي.

المطلب الثالث: معوقات تعزيز الأمن السيبراني في القطاع المصرفي.

الفرع الأول: معوقات تعزيز الأمن السيبراني المصرفي.

أولاً: عدم وجود استراتيجيات شاملة للأمن السيبراني.

ثانياً: التدابير التفاعلية بدلاً من التدابير الاستباقية.

ثالثاً: تخصيص الموارد غير الكافية.

رابعاً: قلة الوعي والتدريب.

الفرع الثاني: طرق لتعزيز الأمن السيبراني المصرفي.

أولاً: الشراكة بين القطاع العام والقطاع الخاص.

ثانياً: تعزيز البحث والابتكار في مجال الأمن السيبراني.

ثالثاً: تطوير البنية التحتية "التقنية والبشرية".

رابعاً: وضع استراتيجية لتعزيز الأمن السيبراني.

خامساً: استخدام تقنيات مبتكرة كالذكاء الاصطناعي.

الفصل الثاني: طرق الحماية القانونية للعمليات المصرفية الإلكترونية وآثارها على الاقتصاد

الوطني.

المبحث الأول: الآليات القانونية المتبعة لحماية العمليات المصرفية الإلكترونية.

المطلب الأول: الرقابة على العمليات المصرفية الإلكترونية وآليات الحماية المتبعة.

الفرع الأول: مفهوم الرقابة على العمليات المصرفية الإلكترونية.

أولاً: تعريف الرقابة على العمليات المصرفية الإلكترونية.

ثانياً: أنواع الرقابة على العمليات المصرفية الإلكترونية.

الفرع الثاني: أنواع الرقابة على العمليات المصرفية الإلكترونية.

أولاً: الرقابة القانونية.

ثانياً: الرقابة التشغيلية.

المطلب الثاني: دور الحفاظ على سرية البيانات الشخصية (سرية المعلومات) في تعزيز الحماية.

الفرع الأول: جوانب الحفاظ على سرية المعلومات في العمليات المصرفية الإلكترونية.

أولاً: أمن المعلومات بين الخصوصية والتوافر.

ثانياً: مفهوم البيانات الشخصية في نطاق الخدمات المصرفية الإلكترونية.

الفرع الثاني: النطاق القانوني لحماية البيانات الشخصية.

المطلب الثالث: الطبيعة القانونية لمسئولية المصارف أثناء ممارسة العمليات المصرفية الإلكترونية.

الفرع الأول: مسئولية المصرف العقدية.

أولاً: الخطأ الإلكتروني كركن لقيام المسئولية العقدية.

ثانياً: الضرر كركن لقيام المسئولية العقدية.

ثالثاً: العلاقة السببية كركن لقيام المسئولية العقدية.

الفرع الثاني: مسئولية المصرف التقصيرية.

أولاً: أساس مسئولية المصرف التقصيرية.

ثانياً: جوانب الاختلاف بين المسئولية التقصيرية والمسئولية العقدية.

المبحث الثاني: آثار حماية العمليات المصرفية الإلكترونية.

المطلب الأول: الأثر المباشر لحماية العمليات المصرفية الإلكترونية.

الفرع الأول: أثر حماية العمليات المصرفية الإلكترونية على المصرف.

الفرع الثاني: أثر حماية العمليات المصرفية الإلكترونية على العميل.

المطلب الثاني: الأثر غير المباشر لحماية العمليات المصرفية الإلكترونية.

الفرع الأول: أثر حماية العمليات المصرفية الإلكترونية على الدولة.

الفرع الثاني: انعكاس أثر الحماية على جذب الاستثمارات الأجنبية.

أولاً: أهمية الاستثمار الأجنبي على التنمية الاقتصادية.

ثانياً: مساعي قانونية لجذب الاستثمارات الأجنبية.

المطلب الثالث: تطبيقات عملية لقضايا انتهاك عمليات مصرفية إلكترونية

الكلمات الدالة للبحث: العمليات المصرفية، العمليات المصرفية الإلكترونية، سائل الدفع الإلكتروني، الأمن السيراني، السيرانية، القطاع المصرفي، مسئولية المصارف، المعاملات الإلكترونية، حماية البيانات الشخصية.

الفصل الأول

مفهوم العمليات المصرفية الإلكترونية في ظل المخاطر السيبرانية

يشهد العالم اليوم تطوراً كبيراً في المجال الرقمي، إذ إن جميع القطاعات العامة والخاصة أصبحت تتنافس من أجل تحويل المعاملات والخدمات التقليدية التي تتطلب حضور الفرد شخصياً إلى عملية إلكترونية تتطلب الدخول إلى موقع مرتبط بالجهة المختصة، حيث يقدم فيها الأول المستندات المطلوبة منه وفق شروط معينة ملزمة على إثرها يتم تقديم الخدمة دون الحاجة إلى حضور شخصي من قبل العميل، وعليه فإن الطرفين يكسبان وقتاً وجهداً لإتمام عمليات قد يطول فيها الانتظار عند الحضور للموقع⁴.

لم يكن القطاع المصرفي بعيداً عن هذا التحول الرقمي؛ بل وإنه مع ارتباطه بالاستثمار في المجالات الرقمية والتزايد النسبي في معاملات التجارة الإلكترونية، أضحت البنوك مواكبة التقدم التكنولوجي الذي تولّد عن هذا التطور السريع، إذ إن هذا النوع من التحول الرقمي يحتاج إلى أنماط غير تقليدية لا تقتيد بالمكان والزمان لإتمام العمليات المصرفية، لذلك ظهرت العمليات المصرفية الإلكترونية بالتزامن مع بدء التطور التكنولوجي⁵، ولأهمية التي تحوزها العمليات المصرفية الإلكترونية اليوم، سيتناول الباحث في المبحث الأول العمليات المصرفية الإلكترونية أما المبحث الثاني فيلخص المخاطر السيبرانية التي تواجه المؤسسة المصرفية والعمل أثناء ممارسة العملية المصرفية الإلكترونية.

⁴ كمال محمد حامد الفكي، دور التسويق في انتشار خدمات الصيرفة الإلكترونية بالمملكة العربية السعودية دراسة تطبيقية على مصارف محافظة الأفلاج، مجلة الدراسات التجارية المعاصرة جامعة الأمير سطام بن عبدالعزيز، المملكة العربية السعودية، العدد الثاني، 2016م، ص8.

⁵ يتوجي سامية، الصيرفة الإلكترونية في سياق القانون رقم 5-18 المتعلق بالتجارة الإلكترونية، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد12، عدد خاص 22، 2020م، ص77.

المبحث الأول

مفهوم العمليات المصرفية الإلكترونية وأبرز أنواعها

المؤسسات المصرفية من أوائل المؤسسات التي سعت إلى تجديد وتطوير خدماتها من أجل مواكبة التكنولوجيا، حيث تنبّهت إلى حدوث الطفرة التكنولوجية مع ظهور الانترنت⁶، ووجهت مصادرها إلى تحسين الخدمات المصرفية والمالية مما أسهم في تعزيز العملية المصرفية وممارستها من قبل العملاء والمصرف نفسه لمجاراة التطور التكنولوجي، ودخول التكنولوجيا المالية في القطاع المصرفي حتم على البنوك استحداث عمليات مصرفية إلكترونية جديدة أو تحويل شكل العمليات التقليدية الموجودة إلى شكل إلكتروني للوصول إلى شريحة أكبر من العملاء، خصوصاً إن البيئة الرقمية فريدة من نوعها توجب استحداث أساليب متنوعة غير مألوفة، لذلك ظهر ما يعرف بالبنوك الإلكترونية⁷، والتي أدت إلى نتوج عمليات وخدمات مصرفية تقدمها المؤسسة المصرفية بصورة إلكترونية⁸ وعليه في هذا المبحث سنبين مفاهيم العمليات المصرفية التقليدية والإلكترونية، ومن ثم ذكر أبرز أنواع العمليات المصرفية الإلكترونية والخصائص التي تتميز بها فيما يلي:

⁶ صليح بونفيلة، النظام القانوني للعمليات المصرفية الإلكترونية، أطروحة دكتوراة، جامعة 8 ماي 1945، الجزائر، 2019-2020م، ص5.

⁷ زعباب سهام، النظام القانوني للبنوك الإلكترونية، رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، الجزائر، 2018م، ص7، يقصد بالبنك الإلكتروني بأنه بنك له وجود كامل على شبكة الإنترنت ويحتوي موقعه على كافة البرمجيات اللازمة للأعمال المصرفية، حيث يتيح هذا البنك للعميل القيام بكافة الأعمال الخاصة بالبنك عن طريق أي مكان موجود به، وذلك بواسطة خط يوفره البنك يسمح له بإنجاز كافة معاملاته دون أن يضطر إلى الذهاب بنفسه إلى مقر البنك.

⁸ زعباب سهام، المرجع نفسه، ص6.

المطلب الأول

ماهية العمليات المصرفية الإلكترونية

نتج عن التحول الرقمي في القطاع المصرفي ما يسمى المصارف الإلكترونية أو البنوك الإلكترونية، والتي يتم استخدامها للتعبير عن العمليات المصرفية التي تمارس عن طريق وسيلة إلكترونية، عادة ما يستخدم تعبير المصارف الإلكترونية كتعبير شامل، يقصد به قيام العميل بممارسة عمليات مصرفية من خلال نظام إلكتروني عبر شبكة المعلومات التي يوفره المصرف لعملائه وفقاً لشروط وضوابط معينة وقد يستخدم العميل هاتفه المحمول، أو موقع الويب الخاص بالمصرف، أو غيره من الوسائل التقنية⁹.

ولبيان ماهية العمليات المصرفية الإلكترونية سيتناول الباحث من خلال الفروع التالية:

- الفرع الأول: المفهوم العام للعمليات المصرفية (الإلكترونية والتقليدية).
- الفرع الثاني: المفهوم السائد للعمليات المصرفية الإلكترونية والتجارة الإلكترونية.

⁹ فريدة قلقول، أهمية أنظمة الدفع الإلكتروني في المصارف دراسة حالة في بنك الفلاحة والتنمية الريفية، رسالة ماجستير، جامعة العربي بن مهيدي، الجزائر، 2012-2013م، ص3.

الفرع الأول

المفهوم العام للعمليات المصرفية (الإلكترونية والتقليدية)

يدور مفهوم العمليات المصرفية حول العمليات التي تقوم بها البنوك وفقاً للقانون المنظم لها، ونرى إن المشرع البحريني أوكل تنظيم المؤسسات المصرفية إلى قانون رقم 64 لسنة 2006م بإصدار قانون مصرف البحرين المركزي والمؤسسات المالية وتعديلاته¹⁰، إذ يُعنى هذا القانون بالعديد من المسائل التي تنظم النقد في مملكة البحرين وإعطاء التراخيص لمزاولة نشاطاتٍ مختلفة على سبيل المثال لا الحصر، كالتأمين والصيرفة والأحكام الفنية المتعلقة بهما، فضلاً أن العمليات المصرفية تعد أحد صور الأعمال التجارية لذلك تطبق عليها أحكام قانون التجارة في كثير من البلدان ومنها مملكة البحرين.

وعليه فسيبين الباحث موقف التشريعات من تعريف العمليات المصرفية والجهة المخولة بممارسة العمليات المصرفية تبعاً:

أولاً: تعريف العمليات المصرفية التقليدية والإلكترونية:

العمليات المصرفية عادة ما يتم ممارستها من قبل جهة معتمدة من قبل المصرف المركزي، ولكن هذا لا يمنع أن تتم ممارستها من قبل أفراد لا يتخذون الشكل القانوني للمصارف وفقاً للتشريع المنظم للمصارف في الدولة، مع العلم إن قيام المصرف بمهمة إجراء العمليات المصرفية يوفر الضمانات اللازمة لممارسة عمليات مصرفية آمنة رجوعاً لشعور الطرف الآخر بالأمان، باعتبار أن المصرف مجازاً قانوناً بإجرائها وفقاً للقانون، فالمصرف يمارس العمليات أيّاً كان نوعها على وجه الاحتراف مع الطرف الآخر سواء كان تاجراً أو لا، وتعتبر هذه من أهم الضمانات الضمنية التي يستشفها العميل أثناء إجراء أي من العمليات المصرفية، والتي حري بها أن تكون عملياتٍ مضمونةٍ لأنها قد أجريت عبر جهة معتمدة ومصرحة قانوناً¹¹.

إن المشرع البحريني نص في المادة رقم (5-8) من المرسوم بقانون رقم (7) لسنة 1987م بإصدار قانون التجارة والذي ينص على اعتبار عمليات المصارف من قبيل الأعمال التجارية متى ما كانت مزاولتها على وجه الاحتراف، إلا أن القانون لم يتضمن تعريفاً للعمليات المصرفية إنما ذكر تعداداً يبين فيه أنواع العمليات المصرفية التي يمارسها المصرف على وجه الاحتراف مع

¹⁰ قانون رقم 64 لسنة 2006 بإصدار قانون مصرف البحرين المركزي والمؤسسات المالية، الجريدة الرسمية، العدد 2755، مملكة البحرين، 2006م.

¹¹ علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية دراسة للقضاء المصري والمقارن وتشريعات البلاد العربية، المكتبة القانونية، مصر، 1993م، ص24.

الطرف الآخر سواء كانوا تجاراً أم غير تجارٍ وأياً كانت طبيعة هذه العمليات¹²، وهذا هو مسلك غالب التشريعات كالقانون المصري والقانون الإماراتي إذ اتخذت موقفاً مشتركاً في عدم تعريف العمليات المصرفية بشكل محدد¹³، إذ إن تعريف العمليات المصرفية سيحد من نطاقها، خصوصاً في خضم تطورها المستمر، وعادة ما يتطلب من المصرف توفير وسائل متجددة أو ابتكار عملياتٍ مصرفيةٍ جديدة، وبالتالي وجود تعريف محدد يحد من توفير الحماية القانونية لها، بحيث إن تغير الوسائل من الممكن أن يؤثر في طبيعة العملية، ونتيجة لذلك تتبين لنا الحكمة في ذكر أنواع العمليات المصرفية دون التعريف لتواكب بدورها الأعمال التجارية التي تتسم بتطورها المستمر.

ولم يغفل الفقه القانوني عن إيراد تعريف للعمليات المصرفية الإلكترونية، فهناك جانب منه تناول تعريف العمليات المصرفية الإلكترونية على الرغم من اختلافهم في المصطلح المستخدم، فيعبر عنها البعض بالبنوك الإلكترونية، أو بنوك الإنترنت، أو البنك على الخط وغيرها، إلا أن المقصد منها واحد يشير إلى استخدام تكنولوجيا المعلومات في إطار عمل المصارف، حيث تُعرف العمليات المصرفية الإلكترونية بأنها: "عبارة عن تقديم الخدمات المصرفية الجديدة والتقليدية بصورة مباشرة للعملاء من خلال قنوات التسليم الإلكترونية التفاعلية وذلك على نحو يُمكن العملاء سواء كانوا أفراداً أم شركاتٍ من دخول الحساب والحصول على معلوماتٍ خاصة بالخدمات التي يقدمها البنك عبر الشبكات الخاصة أو العامة، بما في ذلك شبكة الإنترنت"¹⁴، كما تعرف العمليات المصرفية الإلكترونية بتقديم البنوك الخدمات المصرفية التقليدية أو المبتكرة من خلال شبكات اتصال إلكترونية، وتقتصر صلاحية الدخول إليها على المشاركين فيها وفقاً لشروط العضوية التي يحددها البنك¹⁵ سيما عرفت مؤسسه النقد العربي السعودي، العمليات المصرفية الإلكترونية بأنها "الخدمات المصرفية التي تقدمها عن بعد مصارف مصرحة أو ممثلوها عبر أجهزة تعمل تحت رقابة وإدارة مباشرة من المصرف أو بموجب اتفاقية إسناد هذه المهمة لجهة أخرى¹⁶. وبالنظر إلى

¹² المادة 274، مرسوم بقانون رقم (7) لسنة 1987 بإصدار قانون التجارة، الجريدة الرسمية، العدد 1739، مملكة البحرين، 1987م.
¹³ فنرى أن المشرع المصري أيضاً ضمن العمليات المصرفية من قبيل الأعمال التجارية في قانون رقم 17 لسنة 1999 بإصدار قانون التجارة، إذ ذكر في المادة رقم (5) الفقرة (و) على أن عمليات البنوك والصيرفة تعد أعمالاً تجارية تُطبق عليها أحكام قانون التجارة ولم يختلف مسلك المشرع الإماراتي أيضاً في قانون المعاملات التجارية، القانون الاتحادي رقم (18) لسنة 1993 إذ نصت المادة رقم (5) على أن "تعد الأعمال التالية أعمالاً تجارية بحكم ماهيتها ... البند (4): عمليات المصارف والصيرفة وسوق البورصة..."، العايب عصام، الرقابة على عمليات البنوك في التشريع الجزائري، أطروحة دكتوراة، جامعة باتنة-الحاج لخضر، الجزائر، 2019-2020م، ص31.
¹⁴ طيبي جلال، الصيرفة الإلكترونية في سياق القانون رقم 05-18 المتعلق بالتجارة الإلكترونية، رسالة ماجستير، جامعة محمد خيضر بسكرة، الجزائر، 2021م، ص12.

¹⁵ محمود أحمد إبراهيم الشراوي، مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص17.
¹⁶ صليح بونفلة، المرجع السابق، ص31.

التعاريف السابقة الذكر فإن هناك عنصراً واحداً مشتركاً، وهو إجراء العملية المصرفية إلكترونياً بشرط أن يكون هناك تصريحاً من قبل البنك أو الجهة الرقابية يسمح بممارسة العملية.

وعليه، عند الإشارة للعمليات المصرفية في التشريعات كأصل عام يتم اعتبار البنوك وحدها كليا صاحبة الصلاحية في تنفيذ هذه العمليات باستخدام وسائل تقدمها لعملائها المشاركين، ومع ذلك نرى أن هناك تشريعات في بعض الأحيان تمنح صلاحيات لأطراف أخرى، بموجبها يستطيع أن يمارس فيها العمليات المصرفية وفقاً لشروط وحالات محددة يحددها القانون نفسه، لهذا سيبين الباحث فيما يلي المفهوم العام للبنوك، ومدى صلاحية ممارسة العمليات المصرفية من قبل جهات أخرى فيما يلي:

ثانياً: المفهوم العام للبنك:

أغلب التشريعات عربية وأجنبية لم تتطرق إلى تعريف البنك تعريفاً محدداً ودقيقاً، إنما اكتفت ببيان معايير محددة تحدد الأعمال التي إذا ما قامت المؤسسة بممارستها على وجه الاحتراف تعتبر بنكاً¹⁷، ولا يمكن التسليم بأن ممارسة هذه الأعمال دون الإلتزام بالإطار التنظيمي من قبل الدولة يعني التمسك بصيرورة المؤسسة بنكاً، إذ يتوجب أن يمر البنك بمرحلة فنية وقانونية تنظم شكله القانوني والأعمال التي بإمكانه ممارستها وفقاً لنظام قانوني تحدده الدولة.

إلا إن الفقه القانوني لم يترك هذا المجال فارغاً، فنجد أن هناك محاولات عديدة لتعريف البنك ووضع الخطوط العريضة التي يتبين معها من هي المؤسسات التي يمكن أن يطلق عليها وصف البنك، وبالتالي يتم تطبيق أحكام المصارف المركزية عليها. فعرف جانب من الفقه البنك بأنه: "المنشأة أو الشركة المالية التي تقبل الودائع من الأفراد والهيئات (الأشخاص المعنوية) تحت الطلب أو لأجل، ثم تستخدم هذه الودائع في فتح الحسابات والقروض"¹⁸.

كما عرفت بأنها: "مؤسسات مالية تقوم بتلقي إيداعات نقدية وتفتح حسابات لمعاملات مختلفة وتنشئ اعتمادات لمصلحة زبائنها تحت أشكال مختلفة مثل تسليف دراهم وفتح اعتمادات، وخطابات اعتماد ودفع سندات تجارية، والمساهمة في العمليات المالية العائدة للشركات والمجموعات، وتتلقى إيداع سندات من زبائنها وتضع لمصلحتهم خدمات خاصة"¹⁹.

ويترتب على ماسبق أن الفقه القانوني واجه صعوبة أيضاً في تحديد مفهوم البنك بل فضل كثير من الفقه على عدم تحديد تعريف للبنك واكتفى بعرض عام للعملية المصرفية التي تتم من

¹⁷ عبدالرحمن السيد قرمان، عمليات البنوك وفقاً لقانون التجارة الجديد، الطبعة الثانية، دار النهضة العربية، مصر، 2000م، ص3.

¹⁸ العايب عصام، المرجع السابق، ص13.

¹⁹ سهام ملياط، النظام القانوني للمؤسسات المصرفية في الجزائر، رسالة ماجستير، جامعة أم البواقي، الجزائر، 2013-2014م، ص6.

خلال الكيان المصرفي²⁰، والجدير بالذكر أن تحديد مفهوم البنك بشكل جامع من الناحية القانونية يحد من صلاحيات البنوك في ممارسة أعمالهم خصوصاً أن البنوك تقوم بوظائف متنوعة منها الوظائف التجارية، الوظائف الاستثمارية، الوظائف الاقتصادية والسياسية أحياناً²¹، لذلك يحتاج البنك مرونةً دائمةً ليواكب بها العمل المصرفي الذي يتسم بالسرعة والتجديد على أثر التطورات المستحدثة في العالم وعلى جميع الأصعدة.

تسند مهمة تنظيم المصارف إلى المصرف المركزي، والتي تعود ملكيته إلى الدولة باعتباره مؤسسة عامة²²؛ وحيث إن المشرع الإماراتي والمصري أوكل هذه المهمة إلى المصرف المركزي التابع للدولة²³، ولم يختلف المشرع البحريني عن موقف المشرعين في دولة الإمارات العربية المتحدة، وجمهورية مصر العربية في اعتبار المصرف المركزي ذو شخصية مستقلة تعود ملكيته للدولة²⁴، وينظم مصرف البحرين المركزي الناحية الفنية والقانونية للبنوك والمؤسسات المصرفية بحيث يقوم بالدور الإشرافي والرقابي على الجهاز المصرفي في مملكة البحرين، إذ أوكل القانون المهمة النقدية والإشرافية على المصارف والائتمان إلى المصرف المركزي، باعتباره رأس الهرم المسئول عن أداء الجهاز المصرفي والذي بدوره يضمن ممارسة البنوك أعمالها بما يتناسب مع نجاح الخطة التي تسهم في تحقيق التنمية الاقتصادية والاستقرار المالي في مملكة البحرين.

استناداً لقانون المصرف المركزي في البحرين، نرى أن المشرع البحريني حدد مفهوم البنك من خلال 3 فئات في نص المادة رقم (1) من نفس القانون والتي تنص على أن البنك هو:

"1- أي شخص اعتباري مرخص له بموجب أحكام هذا القانون بقبول الودائع وتقديم القروض وإدارة استثمار الأموال، سواء مع تقديم الخدمات الأخرى ذات العلاقة أو بدونها.

²⁰ علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية، المكتبة القانونية، مصر، 1993م، ص8.

²¹ منى بن لطرش، احتكار البنوك والمؤسسات المالية للعمليات المصرفية، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمن ميرة، الجزائر، المجلد 14، العدد 1، ص117.

²² سهام ملياط، المرجع السابق، ص8.

²³ إذ إن التشريع الإماراتي نص على أنه: "يعتبر المصرف المركزي مؤسسة اتحادية عامة ذات شخصية اعتبارية عامة، المادة 2، المرسوم بقانون اتحادي رقم 14 صادر بتاريخ 23-9-2018 في شأن المصرف المركزي وتنظيم المنشآت والأنشطة المالية، الإمارات العربية المتحدة. كما نص القانون المصري على أن "البنك المركزي جهازاً رقابياً مستقلاً، له شخصية اعتبارية عامة يتبع رئيس الجمهورية، ويتمتع بالاستقلال الفني والمالي والإداري. المادة رقم 2، القانون المصري رقم 194 لسنة 2020 بإصدار قانون البنك المركزي والجهاز المصرفي.

²⁴ مادة 2، قانون رقم 64 لسنة 2006 بإصدار قانون مصرف البحرين المركزي والمؤسسات المالية، ملحق العدد 2755، الجريدة الرسمية، مملكة البحرين.

2- أي شخصٍ اعتباري مرخص له بموجب أحكام هذا القانون بقبول الودائع وإدارتها واستثمارها طبقاً لأحكام الشريعة الإسلامية، سواءً مع تقديم الخدمات الأخرى ذات العلاقة أو بدونها.

3- أية فئةٍ أو فئاتٍ أخرى من المرخص لهم يصدر بتحديدٍها قرارٌ من المصرف المركزي²⁵.

بالإشارة إلى المادة المذكورة أعلاه فإنه يتبين من نص المادة إنه هناك شكلين عامين أساسيين مرخصين من قبل المصرف المركزي وشكلٌ ثالثٌ آخر ثانوي تمارس من خلالهما عمليات البنوك فالشكلين الأوليين تم تقسيمهما وفقاً للشريعة الإسلامية وهما البنوك التقليدية والبنوك الخاضعة لأحكام الشريعة الإسلامية، أما الشكل الثالث هو أي فئة من الفئات التي يرخص لها المصرف بممارسة العمل المصرفي²⁶. يتبين لنا أن البند الأخير من هذه المادة يوسع من نطاق أشكال البنوك بحيث يعطي الصلاحية للمصرف المركزي بإعطاء الترخيص لفئةٍ ما بممارسة العمل البنكي وفقاً لقرارٍ صادرٍ منها مطبقةً عليه أحكام البنوك حتى لو لم يتخذ شكل البنك التقليدي الربوي أو البنك الإسلامي.

نرى أن هذا التوسع في التشريع البحريني يصب في مصلحة كلٍ من المنظومة المصرفية من الجانب الاستثماري من جهة سواءً كان هذا الاستثمار أجنبياً أم محلياً، ومصلحة الطرف الثاني عندما يتعامل مع الطرف الأول الذي يقدم عملاً مصرفياً يوجب بدوره تطبيق الأحكام المتعلقة بالبنوك وفقاً للقانون، والغرض من ذلك هو توفير الضمانة اللازمة للعميل باعتبار أن هذه العلاقة أحد العلاقات التجارية التي يستوجب فيها تطبيق أحكام قانون التجارة.

استناداً إلى نصوص قانون التجارة البحريني، إن العمليات المصرفية تعد من قبيل الأعمال التجارية وعليه وفقاً للمادة 5 من قانون التجارة فإن العمليات التي يقوم بها البنك إذا تمت مزاولتها على سبيل الاحتراف تُعد عملياتٍ مصرفيةٍ توجب الالتزام بالقواعد المنظمة للبنوك والعمليات البنكية.

وهذا دليل على أن المشرع البحريني أيد موقف الفقه الذي أخذ بأنه إذا كانت العملية المصرفية قد صدرت من شخصٍ لا يعد بنكاً وفقاً للقانون أو لم تصدر من قبل بنكٍ مرٍّ بمراحل

²⁵ المادة 1، قانون رقم 64 لسنة 2006 بإصدار قانون مصرف البحرين المركزي والمؤسسات المالية، المرجع السابق.

²⁶ يختلف تقسيم البنوك على حسب عوامل قانونية، اقتصادية أو تصنيفية فالتقسيم الأول يكون وفقاً للوضع القانوني للمصرف: فإما تكون مصارف عامة وهي المصارف التي مصارف خاصة، ومصارف المختلطة. التقسيم الثاني من حيث طبيعة الأعمال التي تزاولها المصارف: مصارف تجارية، مصارف صناعية، مصارف زراعية، مصارف عقارية. التقسيم الثالث: من حيث مصادر الأموال: مصارف مركزية، مصارف الودائع "المصرف التجاري التقسيم الرابع: وفقاً للشريعة الإسلامية: مصارف تقليدية ربوية، مصارف إسلامية، هيثم حسن مبارك بوعمار، العمليات المصرفية دراسة مقارنة بين التشريع الوضعي والشريعة الإسلامية، المجلة القانونية، هيئة التشريع والإفتاء القانوني، مملكة البحرين، العدد الخامس، 2016م، ص 62.

نشوء البنك وفقاً للقواعد القانونية التي وضعها المصرف المركزي فلا يمكن الاعتداد بها كعملية مصرفية، وبالتالي لا تعد العمليات التي يقوم بها شخص عادي من قبيل عمليات البنوك، ويجب أن تصدر من قبل جهازٍ محترفٍ في المجال المصرفي، وأساس هذا الرأي يعود إلى التنظيم المهني الذي يحدده المصرف المركزي²⁷ كسلطةٍ تنظيميةٍ لممارسة الأعمال المصرفية في الدولة.

وعليه، فإن غالبية التشريعات أسندت العمليات المصرفية إلى المؤسسة المصرفية وحددت الجهة المنوط بها مراقبتها وذلك لضمان الممارسة السليمة للعمليات المصرفية بصورتها التقليدية والإلكترونية، ولانتشار التجارة الإلكترونية التي أدت إلى كسر الحدود الجغرافية بحيث يتم التعامل من قبل أطرافها في أماكن تبعد آلاف الكيلومترات أدى إلى إقبال التجار والأفراد من أجل ممارسة مدفوعاتهم أو عملياتهم عن طريق البنك²⁸، ولذلك سنبين فيما يلي بالتفصيل كيف أن مفهوم العمليات المصرفية الإلكترونية مرتبطٌ بالتجارة الإلكترونية ومدى هذا الارتباط فيما بينهما.

الفرع الثاني

المفهوم السائد للعمليات المصرفية الإلكترونية والتجارة الإلكترونية

ترتبط العمليات المصرفية الإلكترونية بالعديد من المجالات، وإن من أهم المجالات ارتباطاً هو مجال التجارة الإلكترونية، حيث غالباً ما نرى أن التجارة الإلكترونية تعتمد على العمليات المصرفية الإلكترونية في دفع المبالغ أو تحويلها، وعليه لابد من التطرق إلى مفهوم التجارة الإلكترونية من أجل تحديد وبيان ارتباطها بالعمليات المصرفية الإلكترونية وذلك على النحو الآتي:

أولاً: مفهوم التجارة الإلكترونية:

إن دخول الانترنت وتطور الأساليب والوسائل الإلكترونية توجه اهتمام التجار في عرض أعمالهم ومنتجاتهم من خلال الفضاء الرقمي ولأقوى هذا الأمر إقبالاً من قبل الأفراد على اقتناء مايلبي احتياجاتهم بكل يسرٍ وسهولة دون الحاجة إلى بذل مجهود يذكر مقارنة بالذهاب إلى الأسواق والتمسك بالطرق التقليدية لقضاء حوائجهم²⁹.

²⁷ عبدالرحمن السيد قرمان، المرجع السابق، ص14.

²⁸ وليد أحمد سعيد مصباح، دور المصرفية الإلكترونية في دعم التجارة الإلكترونية، رسالة ماجستير، جامعة المنصورة، مصر، 2020م، ص21.

²⁹ ضويحي بن عبدالله الضويحي، القواعد الفقهية الحاكمة للعقود ومدى تناولها للعقود الإلكترونية من حيث الانعقاد والإثبات، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص 2356.

ازدياد التعامل في مجال التجارة الإلكترونية جعل من العالم يتوجه إلى تنظيم أحكام المعاملات الإلكترونية التي تنشأ عبر الفضاء الرقمي، مما حدا إلى صدور قانون "الأونسيترال" بشأن التجارة الإلكترونية في عام 1996 والذي ييسر استخدام التجارة الإلكترونية من جهة، كما أمن المعاملات التجارية الإلكترونية وفق حدود وأطر قانونية سليمة من جهة أخرى، حيث كانت الغاية من إصدار قواعد "الأونسيترال" إيجاد حلول لمشاكل التعاقد الإلكتروني الذي يتم عبر الإنترنت والإثبات في القوانين الوطنية، ولأقت هذه القواعد قبولاً من قبل الدول بغية الاندماج في مجالات التجارة الإلكترونية ساعية لتحقيق أكبر قدر من التطور التكنولوجي في ظل مظلة تشريعية منظمة تحقق التوازن بين المعاملات التجارية التقليدية والمعاملات التجارية الإلكترونية، إذ عالج القانون العديد من الموضوعات المتعلقة بالمصارف بوصفها حلقة الوصل للدفع بين التاجر والمستهلك كمسائل الحفاظ على البيانات الشخصية وأنشطة التحويل النقدي ومسائل التوقيع الإلكتروني³⁰، على الرغم من أن قانون "الأونسيترال" النموذجي يعنى بالتجارة الإلكترونية إلا إنه لم يعرف التجارة الإلكترونية كمفهوم واكتفى بتعريف التبادل الإلكتروني للبيانات في المادة الثانية-ب: "نقل المعلومات إلكترونياً من حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لتكوين المعلومات"³¹، وهذا الأمر لا يعيب قانون الأونسيترال إلا من ناحية إطلاقه فالتجارة الإلكترونية أوسع من التبادل الإلكتروني الذي يحد بنقل المعلومات في التعريف الآنف الذكر، فالتجارة الإلكترونية تشمل بيع أو شراء أو تبادل سلع وخدمات بالإضافة إلى العديد من الأنشطة والمعاملات التجارية الإلكترونية.

بعد صدور هذا القانون قامت العديد من الدول بتحديث قوانينها لكي تواكب التطور التكنولوجي في مجال التجارة، خصوصاً إنه لا يمكن إغفال أثر التجارة الإلكترونية على صعيد التنمية الاقتصادية للدول، إذ تسهم التجارة الإلكترونية في ازدهار التبادل التجاري الدولي الذي يعتمد في أساسه على المعاملات المصرفية الإلكترونية كالتحويلات المالية الدولية³²، أما منظمة التجارة العالمية فقد عرفت التجارة الإلكترونية على أنها "مجموعة متكاملة من عمليات الصفقات وتأسيس الروابط وتوزيع وتسويق وبيع المنتجات والخدمات بوسائل إلكترونية"³³، وهذا التعريف

³⁰ نسرين عبدالحميد نبيه، الجانب الإلكتروني للقانون التجاري، منشأة المعارف، مصر، 2008م، ص166.

³¹ المادة 2 ب، قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، الأمم المتحدة، 1996م.

³² محمود سمير الشرقاوي، التحكيم في المعاملات المصرفية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص2324.

³³ بريس عبدالقادر، زيدان محمد، دور البنوك الإلكترونية في تطوير التجارة الإلكترونية، بحث منشور، ص2. انظر إلى الرابط التالي: <http://ketabpedia.com/pdf> تحميل كتاب دور البنوك الإلكترونية في تطوير التجارة الإلكترونية ل. بريس عبدالقادر. زيدان محمد

يحقق معنى التجارة الإلكترونية ويوسع من آفاقها، مما يحقق المرونة التي تتطلبها المشاريع التجارية الإلكترونية.

وبشكلٍ عام نجد مفهوم التجارة الإلكترونية في الفقه يدور حول عمليات بيع وشراء أو تبادل منتجات وخدمات ومعلومات من خلال شبكة الإنترنت، فتعرف التجارة الإلكترونية بأنها "نظامٌ يتيح عبر الإنترنت حركات بيع وشراء السلع والخدمات والمعلومات، كما يتيح أيضاً الحركات الإلكترونية التي تدعم توليد العوائد"³⁴، كما عرفت المؤسسة العربية لضمان الاستثمار بأنها "التجارة التي تتم باستخدام التقنيات التي وفرتها ثورة المعلومات والاتصالات وشبكة الإنترنت عبر التبادل الإلكتروني لبيانات متجاوزة الزمان والمكان وتغطي قطاعاتٍ عديدة، وتضع قواعد جديدة لعمليات البيع والتسجيل والتسليم"³⁵.

وفي الختام انقسم الفقهاء بين مضيّق في تعريف التجارة الإلكترونية وموسّع، إلا إنه نستخلص مما سبق بأن التجارة الإلكترونية تشمل مختلف الأنشطة التجارية مثل إنتاج، بيع، شراء وتسويق السلع والخدمات في علاقةٍ يتكون أطرافها من بائعٍ ومشتريٍّ تتم من خلال وسيلةٍ إلكترونية.

ثانياً: ارتباط العمليات المصرفية الإلكترونية بالتجارة الإلكترونية:

ارتبطت التجارة الإلكترونية بالعمليات المصرفية الإلكترونية ارتباطاً وثيقاً إذ كان اللجوء إلى المعاملات المصرفية الإلكترونية الخيار الأمثل للتجار خصوصاً بعد أن قامت البنوك بتوفير خدمات بنكية شاملة تُصاحب الدفع الإلكتروني بوقتٍ زمني قصيرٍ ومنجزٍ يواكب السرعة التي يطلبها المستهلك جراء التسوق الإلكتروني وطلب الخدمة الإلكترونية، وهناك دراسة أجرتها شركة DELUX³⁶ تُبين لجوء عددٍ كبيرٍ من الأفراد إلى إتمام عملياتهم المصرفية الإلكترونية وفتح حسابات مصرفية إلكترونية مقارنة بالأعداد التي رَفُضت، إذ كانت نسبة المؤيدين لفتح حسابات عبر الإنترنت 365 من أصل 400 شخص على الرغم من توجيه بعض الانتقادات حول التعقيد التي كانت به البنوك الإلكترونية آنذاك والخوف الذي كان يسود حول إتمام العمليات وإنشاء

³⁴ نسرين عبدالحميد نبيه، المرجع السابق، ص134.

³⁵ بريش عبدالقادر، المرجع السابق، ص2.

³⁶ تعد شركة Deluxe من الشركات الرائدة في مجال المدفوعات والتسويق القائم على البيانات بحيث تعمل على مساعدة الشركات الكبيرة والصغيرة على الازدهار من خلال ابتكار طرق اتصال الدافعين والمستفيدين والعملاء. من خلال الجمع بين تقنيات الأعمال المتقدمة والاستراتيجيات من مصادر البيانات ولديها خبرة أكثر من 100 عام في مجال التمويل، لتساعد الشركات على التوسع بفعالية والنمو بشكل أسرع وتطوير علاقات مربحة مع العملاء سواء كان الأمر يتعلق بإدارة المعاملات ذات الحجم الكبير، أو دمج مصادر دفع متعددة بسلاسة أو الانتقال إلى الاقتصاد الرقمي، انظر إلى الرابط التالي [History of Our Company | Deluxe](#), 13, January, 2024.

الحسابات عبر الإنترنت³⁷، إلا إنه ومع تطور التكنولوجيا وزيادة الوعي المالي والإلكتروني أصبح الأفراد والتجار عامة يفضلون اللجوء إلى المعاملات المصرفية الإلكترونية في مجال التجارة الإلكترونية لسهولة مروتها فضلاً عن إخبار الوقت والجهد من الذهاب إلى البنك من أجل إجراء عمليات مصرفية تحصل في وقتنا الحالي بضغطة زر³⁸.

العديد من العمليات المصرفية الإلكترونية تخدم التجارة الإلكترونية، وأكثر العمليات المصرفية الإلكترونية مصاحبة بها هي عملية الدفع الإلكتروني وعمليات التحويل المالي للنقود، فالكثير من الأعمال التجارية تتجه إلى تحصيل أموالها من العملاء عن طريق الدفع الإلكتروني، مما يفتح للطرفين آفاقاً جديدةً من توفير خدمات ووسائل إلكترونية تخدم احتياجات التاجر الإلكتروني، ومثالاً على هذه الأعمال شركات الطيران والفنادق³⁹.

انتشار التجارة الإلكترونية أدى إلى توسع في المعاملات المصرفية الإلكترونية، التي أدت بدورها إلى جهد إضافي من قبل المصارف من أجل تعزيز الثقة والأمان أثناء ممارسة العملية المصرفية على شبكة الإنترنت⁴⁰، فضلاً عن التوجه التشريعي في الدول المتقدمة لتحقيق بيئة قانونية وأسس فنية سليمة وتوفير الضمانات اللازمة لتحقيق أسمى غايات الأمن أثناء ممارسة المراحل الإلكترونية على الصعيدين المصرفي والتجاري، ولهذا دعت لجنة الأمم المتحدة إلى إصدار تشريعات تتعلق بالمعاملات الإلكترونية وحل النزاعات التي تنتج عنها، مثل إصدار قوانين تعترف بالكتابة الإلكترونية، والتوقيعات الإلكترونية في شأن الإثبات سنة 2001م، كما أصدر مجلس الاتحاد الأوروبي حزمة من التشريعات المتعلقة بالتجارة الإلكترونية والأعمال التجارية التي تُعد الأعمال المصرفية، من ضمنها التوجيه الأوروبي رقم 65/2002 المتعلق بالتسويق عن بعد للخدمات المالية للمستهلكين، والتوجيه الأوروبي رقم 65/2008 المتعلق بالوساطة في المواد المدنية والتجارية، بحيث يُمكن الأفراد من حل نزاعاتهم الناشئة بالطرق البديلة عن القضاء العادي⁴¹، وهذه الجهود كانت اعترافاً من الدول المتقدمة بتوسع مجال التجارة الإلكترونية وميدان التعامل في القطاع المصرفي، باعتباره أحد أهم أضلع التجارة الإلكترونية في غالبية الشركات التي تمارس العديد من أعمالها إلكترونياً، والتي تتطلب توفير خدمات وعمليات مصرفية إلكترونية مستحدثة

³⁷ إبراهيم سيد أحمد، الاقتصاد الإلكتروني، المكتبة العصرية، مصر، 2010م، ص109.

³⁸ وليد أحمد سعيد مصباح، المرجع السابق، ص 24.

³⁹ زعباب سهام، المرجع السابق، ص10.

⁴⁰ حازم نعيم الصمادي، المسؤولية المدنية للمصرف عن الأضرار الناجمة عن استعمال الوسائل الإلكترونية في العمليات المصرفية، رسالة ماجستير، جامعة آل البيت، الأردن، 2002م، ص10.

⁴¹ صليح بونفيلة، المرجع السابق، ص9،10.

مما قد ينشأ عن ممارستها مخاطر غير مألوفة عن تلك المخاطر الناشئة عند ممارسة العمليات المصرفية التقليدية.

وتحقيقاً لغاية الدول العربية في الاندماج مع الأسواق العالمية فهناك تحركات عربية عديدة في مجال التجارة الإلكترونية من ضمنها القطاع المصرفي والمالي والملكية الفكرية الرقمية، ومن أهم هذه التحركات إصدار مجلس وزراء العدل العرب في العام 2009 الدليل الاسترشادي للمعاملات والتجارة الإلكترونية، والذي يهدف إلى تنظيم التجارة الإلكترونية ومن ضمنها العمليات المصرفية الإلكترونية⁴².

استجاب القانون البحريني لهذه التحركات التشريعية إيماناً منه على أثر الرقمية في جميع المجالات، كما وقّعت مملكة البحرين على العديد من الاتفاقيات التي تنظم التجارة الإلكترونية والملكية الفكرية الرقمية، بل انضمت مملكة البحرين إلى منظمة الملكية الفكرية في عام 1996م، وأصدرت قوانين تتماشى مع قوانين الدول المتقدمة والدول المجاورة، والتي من شأنها أن تعود نفعاً على مملكة البحرين واقتصادها، مثالاً على هذه القوانين: المرسوم بقانون مرسوم بقانون رقم (54) لسنة 2018م بإصدار قانون الخطابات والمعاملات الإلكترونية⁴³، والقانون رقم (6) لسنة 1420هـ بالموافقة على قانون (نظام) العلامات التجارية لدول مجلس التعاون لدول الخليج العربية⁴⁴.

حاجة السوق التجاري في السنوات المقبلة تتزايد نحو استعداد تقني وقانوني في مجال المصارف الإلكترونية⁴⁵ لمواكبة زخم التطور التكنولوجي، لذلك على الحكومات أن تسعى إلى تقنين التجارة الإلكترونية، ووضع مبادئ قانونية واضحة توازن بين حرية الأسواق التجارية الإلكترونية، والتي تتسم بالانفتاح وبين مرونة وقانونية العمليات المصرفية الإلكترونية والتي تؤثر بشكل كبير على الاقتصاد المحلي من جوانب عديدة وأهمها جذب الاستثمار الأجنبي إليها.

⁴² صليح بونفيلة، المرجع السابق، ص9.

⁴³ مرسوم بقانون رقم (54) لسنة 2018م بإصدار قانون الخطابات والمعاملات الإلكترونية، الجريدة الرسمية، العدد 3395، مملكة البحرين، 2018م.

⁴⁴ قانون رقم 6 لسنة 2014م بالموافقة على قانون نظام العلامات التجارية لدول مجلس التعاون لدول الخليج العربية، الجريدة الرسمية، العدد 3145، مملكة البحرين، 2014م.

⁴⁵ صلاح زين الدين، دراسة اقتصادية لبعض مشكلات وسائل الدفع الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص306.

المطلب الثاني

أهم أنواع العمليات المصرفية الإلكترونية وخصائصها

(الدفع الإلكتروني نموذج)

كل يوم يتجه المزيد من المصارف وعملاء المصارف إلى التغلغل في استخدام التكنولوجيا، من أجل توفير واستخدام العمليات والخدمات المصرفية، خصوصاً بعد وسائل الأمان التي يوفرها القطاع المصرفي للحفاظ على أمن الحسابات المصرفية أثناء ممارسة العمليات المصرفية الإلكترونية على مدار 24 ساعة في اليوم، لذلك أصبح التوجه إلى اختيار أداء العمليات المصرفية الإلكترونية محبباً لدى البنوك وعملاء وأصبح خياراً ذو قيمة لدى الطرفين، وازدادت شعبيتها لما تنطوي عليه من مميزات تُمكن كلا منهما الحفاظ على الوقت والجهد فضلاً عن تقليل التكاليف المترتبة على الاستعمال الإلكتروني للصيرفة⁴⁶.

تقدم الصناعة المصرفية في مجال التكنولوجيا أدى إلى تطور العمليات المصرفية وكان من أهم هذه التطورات ظهور وسائل دفع إلكترونية متنوعة، مثل بطاقات الائتمان والخصم، المحافظ الرقمية، والنقود الإلكترونية مما يرسخ الرقمنة في هذه العمليات وبينما تزداد شعبيتها فإنها تمر بمرحلة انتقالية نحو مستقبل واعد مع التركيز على التحديات التكنولوجية العملية والتطبيقية وكيفية التغلب عليها إذ تشمل هذه التحديات قضايا قانونية وتنظيمية كحماية البائع والمشتري في التجارة الإلكترونية، أيضاً تتضمن قدرات مقدمي خدمات الدفع الإلكتروني بالإضافة إلى العلاقات التجارية واسعة الآفاق فضلاً عن الاعتبارات الأمنية مثل التحقق والمصادقة كل ذلك،⁴⁷ وعليه سيتناول هذا المطلب من خلال فرعين:

- الفرع الأول: عملية الدفع الإلكتروني.
- الفرع الثاني: مخاطر استعمال العمليات المصرفية الإلكترونية.

⁴⁶ K. Böhle, M. Krueger, C. Herrmann, G. Carat, I. Maghiros, Electronic Payment Systems, Institute for Prospective Technological Studies, Background Paper No. 1,2000,page127.

⁴⁷ K. Böhle, M. Krueger, C. Herrmann, G. Carat, I. Maghiros, Ibid page,127.

الفرع الأول

عملية الدفع الإلكتروني

تعد عملية الدفع الإلكتروني أحد العمليات المصرفية الإلكترونية الأكثر شيوعاً نظراً للتطور الحاصل في البيئة التجارية في العالم اليوم، والتي بدورها تتطلب وسائل دفع تختلف عن وسائل الدفع التقليدية التي اعتادها الناس في السابق، ولا يمكن إنكار أثر نمو التجارة الإلكترونية والعمليات الرقمية على استحداث أنظمة دفع إلكترونية لتتماشى مع الطبيعة الجديدة التي تتسم بها العمليات التجارية في ظل الاقتصاد الرقمي، لذلك في هذا الفرع سيتناول الباحث مفهوم عملية الدفع الإلكتروني من خلال البحث في ماهيتها، ومن ثم التطرق إلى الخصائص التي يتميز بها عن عملية الدفع التقليدية⁴⁸.

أولاً: مفهوم الدفع الإلكتروني:

التحول الناشئ عن تطور التكنولوجيا والتوجه إلى تطوير عمليات البنوك لتتوافق مع معايير التقدم الإلكتروني من أجل الدخول ضمن الاقتصاد الرقمي العالمي أصبح مصيراً حتمياً للبقاء في السوق التجارية والمنافسة، ووفقاً لمتطلبات هذا التحول الإلكتروني فإن نجاح البنوك الآن وزيادة ربحيتها مرتبط بتحولها الإلكتروني، وتقديم خدمات إلكترونية ميسرة لعملائها على المستويين الداخلي والخارجي⁴⁹.

ونظراً لارتباط العمليات المصرفية الإلكترونية بالتجارة الإلكترونية، فالعديد من أصحاب الأعمال يسعون إلى توفير خدمات دفع ميسرة إلى عملائهم، ونتيجة هذا التيسير في عمليات الدفع ينعكس إيجاباً على نمو التجارة الإلكترونية من جهة، وزيادة ولاء عملاء البنوك وثقتهم بأمن العمليات المصرفية الإلكترونية لدى البنك الوسيط من جهة أخرى⁵⁰.

كما أن العمليات المصرفية الإلكترونية بشكل عام، والدفع الإلكتروني على وجه الخصوص يستعمل في العديد من العمليات الحكومية، إذ اتجهت الدول إلى الدفع الإلكتروني في تحصيل الرسوم في عديد من الوزارات، فتعدد الأطراف التي تستعمل الدفع الإلكتروني له أثر إيجابي يمتد إلى منظومة واسعة من الجهات الخاصة والعامة، وعلى الرغم من هذا الأثر الإيجابي الذي لازم

⁴⁸ مروة لعلوي، دليلة طبري، النظام القانوني لوسائل الدفع الإلكتروني، جامعة محمد البشير الإبراهيمي، رسالة ماجستير، الجزائر، 2023م، ص8.

⁴⁹ هداية بوعزة، النظام القانوني للدفع الإلكتروني دراسة مقارنة، رسالة ماجستير، جامعة أبي بكر بلقايد، الجزائر، 2018-2019، ص20.

⁵⁰ فارح عائشة، التنظيم القانوني لوسائل الدفع الإلكترونية: حتمية أساسية لتفعيل التجارة الإلكترونية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، الجزائر، المجلد 10، العدد 3، 2021م، ص226.

التحول الرقمي في مجال الدفع الإلكتروني⁵¹؛ إلا أن هناك جانباً آخر سلبياً ظهر مع ازدياد التعامل الإلكتروني وتطور وسائل الدفع مما خلق تحدّ على البنوك وهو الحفاظ على أمن وسلامة عملية الدفع الإلكتروني، مما أوجب خلق تعاون بين المؤسسات المصرفية والمؤسسات التشريعية حيث كان نتاجه سن تشريعاتٍ تقتضي حماية البنك والعميل من أي هجمة إلكترونية بحيث يتم تشكيل بناءً قانوني قادرٌ على حل المشكلات التي تظهر مع ممارسة عمليات الدفع الإلكتروني⁵² سواءً في مجال التجارة الإلكترونية أو مجال الخدمات التي تقدمها الحكومة وتستلزم دفع رسومٍ أو مبالغ عن طريق الدفع الإلكتروني.

نظراً للإقبال الكبير على الدفع الإلكتروني من قبل الجمهور فنرى أن هناك زخماً كبيراً في توجيه الاهتمام إلى الحفاظ على أمن الدفع الإلكتروني من خلال توفير البيئة التقنية والقانونية التي توائم التطور المصاحب للممارسات الإلكترونية⁵³، ولمدى أهمية عملية الدفع الإلكتروني المنعكسة على أطرافها سنبين فيما يلي مفهوم الدفع الإلكتروني وخصائصه العامة ومدى حمايتها في القانون البحريني والقانون المقارن على النحو الآتي:

ماهية الدفع الإلكتروني

أدى التطور الاقتصادي والتكنولوجي إلى ظهور عملياتٍ مصرفيةٍ مستحدثةٍ كعملية الدفع الإلكتروني وهذه العملية ماهي إلا الصورة المطورة الحديثة لعملية الدفع التقليدي التي اعتدنا على وجودها كوسيلة للوفاء بالمبالغ المستحقة⁵⁴، لفهم مفهوم الدفع الإلكتروني لابد من تحليل هذه العملية إلى قسمين أساسيين أولهما مصطلح الدفع ومن ثم مفهوم مصطلح إلكتروني، لاشك أن مفهوم الدفع لا يختلف فيه العديد من الفقهاء إذ يقصد بالدفع " سداد دينٍ أو تسوية التزام⁵⁵"، وهذا هو المختصر للمفهوم العام للدفع ويرادفه في القانون المدني مفهوم الوفاء، ويُعد الوفاء من أهم صور تنفيذ الالتزام وحدث أن يكون سبباً في انقضاء الالتزام المترتب على الطرف المدين ويقصد به أداء الدين المستحق المتعلق في ذمة المدين⁵⁶.

⁵¹ Mark Fajfar, Role and Security of Payment Systems in an Electronic Age, IMF Institute Seminar, 2004, page3.

⁵² إبراهيم سيد أحمد، المرجع السابق، ص401.

⁵³ هداية بوعزة، المرجع السابق، ص22.

⁵⁴ هداية بوعزة، المرجع نفسه، ص20.

⁵⁵ جودي نبيل، دور أنظمة الدفع الإلكترونية في تحسين المعاملات المصرفية -دراسة حالة- بنك السلا فرع ورقلة، جامعة قاصدي مرياح، رسالة ماجستير، الجزائر، 2022م، ص4.

⁵⁶ أنور العمروسي، صور انقضاء الالتزام في القانون المدني، دار الفكر الجامعي، مصر، الطبعة الأولى، 2004م، ص50.

نظم المشرع البحريني أحكام الوفاء بالدين في القانون المدني، بذكر أحكامه العامة فيما يتعلق بانقضاء الدين، ويرى الباحث إن ربط الوفاء بالدفع يكون من خلال الصورة العامة لانقضاء الالتزام واتحاد النتيجة فيهما، والتي تتمثل بإبراء الذمة المالية للمدين بعد السداد، لذلك وانطلاقاً من المبدأ العام لنظرية الالتزام والتي ترتب على كل من أطرافها؛ الالتزام بأداء الثمن يمكن القول أن الوفاء هو الصورة المقابلة للدفع.

أما القسم الثاني للدفع الإلكتروني هو المصطلح الإلكتروني، إذ تضمنت التشريعات القانونية هذا المصطلح في طيات القوانين المنظمة للمعاملات الإلكترونية، على الرغم من أن هذه القوانين قد جاءت متأخرة في الدول العربية إلا إن هناك وضوحاً فيما يتعلق بتعريف الإلكتروني، فنرى المشرع البحريني عرفها في قانون الخطابات والمعاملات المصطلح الإلكتروني بـ: "تقنية استعمال وسائل كهربائية أو مغناطيسية أو كهرومغناطيسية أو بصرية أو بايومترية أو فوتونية أو أي شكل آخر من وسائل التقنية المشابهة"، كما عرف المشرع الإماراتي مصطلح إلكتروني في المادة الأولى من مرسوم بقانون اتحادي لسنة 46 لسنة 21 شأن المعاملات الإلكترونية وخدمات الثقة بـ: "كهرومغناطيسي أو كهروضوئي أو رقمي أو ضوئي أو مشابه ذلك"، وعليه فإن مانلاحظه في القانونين الأنفي الذكر لتعريف المصطلح كان شاملاً لأشكال التكنولوجيا إما كهرومغناطيسية أو ضوئية أو رقمية أو غيرها.

بناءً على ما سبق فإنه يمكننا القول الدفع الإلكتروني ما هو إلا الصورة الإلكترونية لصورة الدفع التقليدي إلا إنه قد تتعدد وسائله نظراً لتطور التكنولوجيا المصاحبة له، إذ ظهرت العديد من الصور المقابلة لوسائل الدفع التقليدي بشكل إلكتروني، ومثالاً على ذلك الشيك الإلكتروني الذي يُعد الصورة الافتراضية للشيك التقليدي ولا يختلف من ناحية المعلومات التي يحتوي عليها الأخير إنما ينشأ بواسطة وسيلة إلكترونية كجهاز الحاسب الآلي وعادة ما يتم استخدامه في الديون عالية القيمة⁵⁷، أما من وسائل الدفع المستحدثة للدفع الإلكتروني هو ظهور النقود الإلكترونية والتي تُعد البديل الافتراضي للنقود المعدنية أو الورقية⁵⁸، والجدير بالذكر أنه من الواجب التفرقة بين النقود الإلكترونية والدفع الإلكتروني إذ قد يحدث لبس أحياناً فيما إذا كان يقصد بالنقود الإلكترونية كتعريف للدفع الإلكتروني، وعليه فإنه يمكن أن نفرق بينهما باعتبار أن الدفع الإلكتروني هو

⁵⁷ نبيل صلاح محمود العربي، الشيك الإلكتروني والنقود الرقمية دراسة مقارنة، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص 67.

⁵⁸ عدنان إبراهيم سرحان، الوفاء (الدفع) الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص 267.

المظلة الأكبر التي تتفرع من خلالها أفرع وأشكال متنوعة كالتحويلات المصرفية، الشيكات الإلكترونية، والنقود الإلكترونية باعتبارها أحد وسائل الدفع الإلكتروني⁵⁹.

تقبل العالم الانفتاح الإلكتروني والانتشار السريع للإنترنت مع تطور التكنولوجيا واستحداث وسائل عدة أدى إلى تعزيز وتسهيل استخدام الشبكة من أجل غايات عديدة أثرت على نمو الممارسات الإلكترونية بشكل غير متوقع في السنوات الماضية، ولاشك أن نمو التجارة الإلكترونية التي أصبحت تصل إلى عشرات الملايين من الناس عبر القارات جعل من الدفع الإلكتروني وسيلة محببة للتجار والمستهلكين تواكب السرعة التي تمتاز بها العملية، فضلاً أن تطوير نظام آمن من قبل البنوك وتوفير وسائل دفع إلكترونية مختلفة تمكن الأفراد والحكومات من استخدامها كان له دور فعال في الانتشار الذي يحظى به اليوم⁶⁰، وتتعدد وسائل الدفع الإلكتروني وتستحدث مع استحداث الظروف والعمليات التجارية حول العالم، ومثالاً على هذه الوسائل البطاقات البنكية الإلكترونية على الرغم من أنواعها واختلاف أحكام كل منها إلا إن صورتها الأساسية واحدة ويقصد بها منح العميل القدرة على استخدام البطاقة في نقاط البيع بحيث يتم تعبئتها بالمبلغ المطلوب من قبل العميل في البنك، وتتم عملية الخصم من البطاقة في نقاط البيع وفقاً لمدفوعات العميل حتى استنفاد المبلغ بالكامل وتقوم البنوك بالتواصل مع البنك عن طريق أنظمة إلكترونية للتأكد من صحة العملية وإمكانية سحب المبلغ إلى جانب التحقق من فاعلية البطاقة المستخدمة⁶¹.

تتميز عملية الدفع الإلكتروني بوصفها أحد العمليات المصرفية الإلكترونية بمجموعة من الخصائص وعليه سيبينها الباحث فيما يلي:

ثانياً: خصائص الدفع الإلكتروني:

الدفع الإلكتروني كما ذكرنا ما هو إلا انعكاس مستحدث عن الدفع التقليدي، إذ يُعد الدفع الإلكتروني تحويل لطرق الدفع التقليدية الموجودة إلى صيغة إلكترونية، بحيث تتناسب مع المعاملات المصرفية الإلكترونية، إلى جانب ذلك ظهرت وسائل مستحدثة لم تكن موجودة منذ البداية، وظهرت وليدة للتطور التكنولوجي الحاصل في شتى المجالات⁶² إلا أن هناك سماتاً

⁵⁹ نسرين عبدالحميد نبيه، المرجع السابق، ص 12.

⁶⁰ فريدة قلقول، المرجع السابق، ص 67.

⁶¹ حنان بوعكوش، شادية زايدي، حماية العمليات المصرفية في ظل تطور الصيرفة الإلكترونية، جامعة العربي التبسي، رسالة ماجستير، الجزائر، 2019م، ص 17.

⁶² شادي سلامة الحولي، إدارة مخاطر العمليات المصرفية الإلكترونية وفق مقررات لجنة بازل دراسة تطبيقية على البنوك المحلية العاملة في فلسطين، رسالة ماجستير، الجامعة الإسلامية، فلسطين، 2015م، ص 27.

وخصائص مشتركة تندرج تحت جميع وسائل الدفع الإلكتروني، وإن اختلفت في نسبتها وسنذكر هذه الخصائص على النحو التالي:

1- عملية الدفع الإلكتروني متعددة الأطراف:

تعد عملية الدفع الإلكتروني أياً كان شكلها عملية تتم ممارستها من قبل ثلاثة أطراف، تجمعهم روابط قانونية وتسمى العلاقة الثلاثية، يكون أحد الأطراف العامل المشترك بين العقود الثلاث⁶³ وهم المستهلك، المستفيد (التاجر، هيئة عامة أو خاصة)، والبنك، إذ تبرز هذه الخاصية على عدة مراحل، المرحلة الأولى وهي مرحلة العلاقة الأولية بين البنك والعميل على إثرها يقوم بإنشاء علاقة تعاقدية مع البنك تنتج عنها استصدار وسيلة ما من وسائل الدفع الإلكتروني كالبطاقة الائتمانية، أما المرحلة الثانية هي مرحلة استعمال العميل سلطته القانونية في التصرف بهذه الوسيلة أي وسيلة الدفع الإلكتروني، ومثال عليها قيام المستهلك بشراء سلعة ما من التاجر تستوجب دفع ثمنها، أما المرحلة الأخيرة هي الاستقطاع الذي يتم من قبل البنك من حساب العميل وتحويل المبلغ إلى التاجر⁶⁴، وعادة ما ترتبط هذه العلاقات بأطرافها وجوداً وعدماً، وهذا يعود إلى خاصية الأمان التي تسعى إليها أنظمة الدفع الإلكتروني؛ حيث أن وجود البنك كطرف في هذه العلاقة يوفر الأمان لكل من العميل والتاجر، إذ إن صلاحية وسيلة الدفع الإلكتروني التي يمتلكها العميل جاءت نتيجة لتوافر شروط معينة من قبل البنك كان أساسها راجعاً لقواعد قانونية سليمة، وبالتالي يمكن أن يبعث ذلك رسالة اطمئنان للتاجر بصلاحية عملية الدفع الإلكتروني ومثال على ذلك عندما يقدم العميل شيكاً إلكترونياً للتاجر فيلتزم البنك في هذه الحالة بضمان قبول الشيك الإلكتروني والتزامه بالتحقق من وجود رصيدا يقابل المبلغ المستحق وبالتالي فإن وجود البنك كطرف في عملية الدفع الإلكتروني يكون عاملاً مساعداً لتجنب المخاطر التي تتبع استصدار الشيكات التي لا يقابلها رصيد كافٍ⁶⁵.

2- سهولة استخدام الدفع الإلكتروني:

تحوز أنظمة الدفع الإلكتروني على مقدار من التقبل من قبل الأفراد (تجاراً أو غير تجار)، الحكومة سواء كانت (هيئات عامة أو خاصة) وذلك استناداً على أن هناك العديد من الجهات تستخدم وسائل دفع إلكترونية مختلفة من خلال موقع يربط بين العميل وبين الجهة المستفيدة وهذا يعد دليلاً على اعتراف هذه الجهات بأنظمة الدفع الإلكترونية وتُعد بطاقات الخصم وبطاقات

⁶³ حوالف عبدالصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة دكتوراة، جامعة أبوبكر بلقايد، الجزائر 2015م، ص 178.

⁶⁴ شما جاسم السليطي، الجوانب القانونية لوسائل الدفع الإلكترونية في ضوء القانون القطري، رسالة ماجستير، جامعة قطر، قطر، 2021م، ص 18.

⁶⁵ ذكرى عبدالرزاق محمد، النظام القانوني للبنوك الإلكترونية، دار الجامعة الجديدة، مصر، 2010م، ص 40.

الائتمان من أهم وسائل الدفع الإلكتروني التي تتميز بمستوى عالٍ من الثقة من قبل مستخدميها⁶⁶، والجدير بالذكر أن سهولة استخدام الدفع الإلكتروني هو ما جعله محبباً وقابلاً للانتشار بشكل كبير؛ حيث إن لجوء الأطراف المستفيدة من الدفع الإلكتروني نابع من فكرة سهولته وسرعته، وذلك بضمان المؤسسة التي قامت بإصدار وسيلة الدفع لذلك كان حرياً على مقدمي خدمة الدفع الإلكتروني مراعاة السهولة والبساطة في استخدام الوسائل لكي تكون متوافقة مع الغرض منها⁶⁷.

3- السرعة في إتمام عمليات الدفع الإلكتروني:

عمليات الدفع الإلكتروني التي تمارسها الهيئات الحكومية والخاصة والأفراد تجاراً أو مستهلكين يطغى عليها عنصر السرعة، إذ أن غالباً ما تكون الأطراف في عمليات الدفع الإلكتروني يتطلعون لسهولة إنجاز المعاملة، فعلى سبيل المثال عندما يقوم المستهلك بالتسوق عبر الإنترنت من مكانه في المنزل، فإنه يتوقع أن عملية الدفع الإلكتروني لن تأخذ منه وقتاً طويلاً بل يستطيع أن يدفع ثمن السلعة في ثوانٍ معدودة بعد إدخال معلومات الدفع الخاصة به لتسديد ثمن السلعة أو الخدمة المتلقاة، كما أن أهمية خاصية السرعة في إنجاز معاملات الدفع الإلكتروني برزت بشكل أكبر بعد انتشار التجارة عبر الإنترنت خصوصاً أن المستهلك أصبح يستطيع إتمام عمليات الدفع الإلكتروني دون الحاجة إلى زيارة البنك من أجل إتمام التحويل المصرفي والانتظار إلى حين استلام التحويل من قبل الطرف الآخر⁶⁸، ناهيك عن إتمام عمليات الدفع الإلكتروني التي لا ترتبط بوقت وأيام عمل معينين إذ يمكن إتمام عمليات الدفع الإلكتروني ولو كان في يوم عطلة رسمية، وهذه من أهم مزايا الدفع الإلكتروني التي أدت إلى تسريع عمليات الدفع الإلكتروني وقبولها ومن ثم السرعة في إنجازها وتسليم محل الاتفاق في أسرع وقت ممكن.

4- الأمان والخصوصية:

خاصتي الأمان والخصوصية تعد أهم خصائص الدفع الإلكتروني على الرغم من أنهما حدا سيف مزدوج، ففي الحد الأول فإن عمليات الدفع الإلكتروني تحظى باهتمام كبير من قبل الهيئات المختصة لحماية هذه العمليات من أي اعتداء إلكتروني، إلا أن هناك دراسات تؤكد أن نسبة الاعتداء والتعرض مرتفعة جداً، كما أن نقص آليات التنظيم والانتصاف الفعالة وكل ذلك يؤدي إلى فرص الوقوع في فخ المهاجمين السيبرانيين والخسائر المالية في نهاية المطاف على الرغم من التوعية المستمرة والجهود المبذولة في تحقيق أمان العمليات المالية الإلكترونية إلا أنه

Dr. Atul Kumar, A Study of Significant Characteristics of E-payment Regime in India, MERC Global's ⁶⁶

International Journal of Management, Volume 7, Special Issue 1, May 2019, page111.

⁶⁷ حوالف عبدالصمد، المرجع السابق، ص46.

⁶⁸ شما جاسم السليطي، المرجع السابق، ص20.

لازال مجرمو الإنترنت يجدون وسيلة جديدة من أجل سرقة الأموال من الأفراد مما يزعزع ثقة المستهلكين في أمان عمليات الدفع الإلكتروني⁶⁹، أما الحدّ الآخر هو أن عمليات الدفع الإلكتروني تتسم بالأمان والخصوصية خصوصاً إن أنظمة الدفع الإلكتروني توفر لمستخدميها توثيقاً واضحاً يبين فيه حقيقة وجود الطرف الآخر، فضلاً على أن عملية الدفع أساساً تقوم على آلية تشفير البيانات والرموز السرية⁷⁰ لضمان المعلومات البنكية عند إتمام المعاملة وهذا مايعزز أمان إجراء عملية الدفع الإلكتروني عبر البنك فعادةً مايرسل البنك رمزاً سرياً لمرة واحدة على رقم الهاتف المتصل بالمعلومات البنكية بوسيلة الدفع الإلكتروني (OTP) تأكيداً على ممارسة العملية من قبل صاحبها، لا شك أن عملية الدفع الإلكتروني لا بد أن تكون مصحوبةً بوسائل فنية توفراً لأمان لضمان تحديد هوية المستخدم والمستفيد وتتجدد هذه الوسائل لدرة مستجدات الوسائل المستخدمة للقرصنة عبر الإنترنت⁷¹.

كما أنه من أهم مظاهر الخصوصية في الدفع الإلكتروني هو مبدأ الخصوصية وسرية البيانات في العمليات البنكية، إذ إن عملية الدفع الإلكتروني تتضمن رموزاً وتشفيراً لا يمكن ظهورها عبر شبكة الويب⁷²، فأنظمة الدفع الإلكتروني تقوم في أساسها على أنظمة التشفير والرموز حفاظاً على خصوصية وسرية البيانات المتعلقة بالمعاملة البنكية التي تمت من قبل العميل والمستفيد، والسبب في ذلك هو الحفاظ على أمن المعلومات البنكية التي ستمر عبر شبكة الإنترنت والتي ستكون عرضة لخطر اعتراض الغير من أجل الحصول عليها لأغراض غير مشروعة⁷³ وفقاً لهذه الأنظمة المشفرة لا ينبغي لأحد أن يكون قادراً على إنتاج الرموز الإلكترونية بمفرده⁷⁴، إلا أن تجدد وسائل التعرض وقرصنة الإنترنت والعمل على تصميم برامج لخرق الرموز والتشفيرات يصعب من مهمة الأمان والحفاظ على خصوصية المعلومات ونتيجة لهذا التجدد السريع والمستمر فإن المنظمات المالية والتشريعات المتعلقة بالعمليات المالية الإلكترونية تسعى إلى توفير بيئة فنية وقانونية قادرة على صد هذه الهجمات وإنشاء جدارٍ حامٍ لهذه العمليات الإلكترونية.

5- عملية الدفع الإلكتروني تتسم بالتفاعل عن بعد:

أهم انعكاسٍ لعملية الدفع الإلكتروني هي أنها عمليةً تتطلب التفاعل عن بعد، إذ ليس بالضرورة أن يكون الطرفان في مجلسٍ واحدٍ لإتمام العملية، ومثالاً على ذلك نظام المرور في مملكة البحرين

⁶⁹ Jevish Sharma, Suhasini Verma, Mounting Cases of Cyber-Attacks and Digital Payment, page 60.

⁷⁰ عدنان ابراهيم سرحان، المرجع السابق، ص294.

⁷¹ Jevish Sharma, Suhasini Verma, Ibid, page 66.

⁷² وافت يوسف، النظام القانوني للدفع الإلكتروني، جامعة مولود معمري تيزي، رسالة ماجستير، الجزائر، 2011م، ص24.

⁷³ عدنان ابراهيم سرحان، المرجع السابق، ص294.

⁷⁴ Dr. Atul Kumar, A Study of Significant Characteristics of E-payment Regime in India, Ibid, page 111.

والذي يقدم خدمات إلكترونية عبر منصات إلكترونية متعددة مثل موقع الحكومة الإلكترونية في مملكة البحرين أو عن طريق تطبيق ⁷⁵ E-Traffic، وتتمثل هذا الصورة في قيام الفرد بدفع مخالفة مرورية وهو في منزله للهيئة المنوط بها بتحصيل الغرامات المالية التابعة لوزارة الداخلية عن طريق وسيلة إلكترونية مصرحة، وهنا نرى أن الطرفين لم يكونوا متقابلين في مجلس واحد وهناك أولاً إيجاباً مقدم من قبل العميل وفقاً لقاعدة بيانات ظهرت عند إدخال المعلومات الشخصية وثانياً ظهور قبول من قبل هيئة المرور على عملية الدفع وبالتالي تتم عملية الدفع عن طريق إحدى وسائل الدفع الإلكتروني على الرغم من هذا البعد، إلا أن هذا التفاعل عن بعد هو السمة الجوهرية التي تشكل خطراً على العملية البنكية الإلكترونية بحيث قد تتعرض عملية الدفع الإلكترونية لإضطرابات أو قرصنة أو ولوج غير مشروع لمعلومات شخصية للعميل أو المستفيد ⁷⁶.

يعد فهم المخاطر التي تتعرض لها عمليات الدفع الإلكترونية أمراً بالغ الأهمية، فالبنى التحتية التكنولوجية والأساس القانوني الذي ينطوي عليه تقييم المخاطر المرتبطة بعمليات الدفع الإلكتروني بدءاً من ضمان الامتثال للوائح حماية البيانات والخصوصية يؤكد أن الاعتبارات القانونية تلعب دوراً محورياً في تسهيل العمليات المصرفية الإلكترونية إلى جانب توفير الأمان اللازم وتخفيف العواقب الناتجة عند استخدام استراتيجيات التخفيف المعتمدة ⁷⁷، وعليه سيتطرق الباحث للمخاطر التي تتعرض لها عمليات الدفع الإلكتروني وذلك فيما يلي.

الفرع الثاني

مخاطر استعمال عمليات الدفع الإلكتروني

عملية الدفع الإلكتروني تحظى بأهمية تتعلق بتنفيذ الالتزامات المستحقة على عاتق المدينين نحو دائنيهم، ولا شك أن تحقق هذا الالتزام ينطوي عليه إبراء ذمة المدين من الدين والدفع الإلكتروني سهل إتمام هذه العملية بسرعة ومرونة تواكب البيئة الإلكترونية الخصبة التي تحقق نماءً مستمراً وازدهاراً في الاستثمار وبناء العلاقات في القطاع المصرفي ⁷⁸، إلا أن هذه الأهمية تواجه مشاكل ومخاطر معقدة تواجه كل الأطراف الثلاثة عند ممارسة عملية الدفع الإلكتروني مما يشكل ضغطاً كبيراً على فاعليتها مقارنة بالدفع النقدي وعليه فإننا سنتناول في هذا الفرع بعض المخاطر التي تواجه الأطراف عند ممارسة الدفع الإلكتروني والمشاكل القانونية التي ظهرت عند

⁷⁵ خدمات الإدارة العامة للمرور (bahrain.bh)، مملكة البحرين.

⁷⁶ Mark Fajfar, Ibid, page 10.

⁷⁷ زلاسي بلقاسم، غريب الحاج علي، الحماية القانوني لوسائل الدفع الإلكتروني في التشريع الجزائري، رسالة ماجستير، جامعة الشهيد حمة لخضر، الجزائر، 2021م، ص7.

⁷⁸ بن برونو مصطفى، دور وسائل الدفع الإلكترونية وانعكاساتها على البنوك، جامعة عبد الحميد بن باديس، رسالة ماجستير، الجزائر، 2018م، ص30.

استعمال عمليات الدفع الإلكتروني بأي وسيلة من وسائل الدفع الإلكتروني وسنحاول إبراز الحلول لهذه المخاطر إن أمكن ذلك فيما يلي:

أولاً: مخاطر الاستعمال:

ممارسة العمليات المصرفية الإلكترونية بشتى أنواعها أفضت إلى إبراز دور العميل في التحكم في حساباته البنكية بشكل فردي دون اللجوء إلى المصرف من أجل إتمام أي من تلك العمليات وهذا ما جعل العمليات المصرفية الإلكترونية محببة لدى العملاء، إذ يعزز هذا النشاط الشعور بالتحكم الذاتي وإدارة الأموال والطمأنينة بحيث يرى عملية سير أمواله منذ بدئها حتى انتهائها⁷⁹.

إلا أنه على الرغم من هذا التحكم الناشئ عن الاستخدام الفردي، فإنه قد يصاحبه إهمال من قبل العميل عند ممارسة العمليات المصرفية الإلكترونية بشكل عام، والدفع الإلكتروني بشكل خاص، إذ يمارس العميل عملية الدفع الإلكتروني دون أخذ الحيطة والحذر عند استعماله هذه الوسيلة لإجراء معاملة ما، مما يجعله عرضة للهجوم الإلكتروني والاستيلاء على أمواله الخاصة، والجدير بالذكر أن الاستيلاء على أموال العميل يتم عن طريق استخدامه لوسيلة إلكترونية يوازي خطر الاستيلاء على الأموال بالصورة التقليدية وأحياناً يفوقه، فصورة الاستيلاء الإلكتروني تنتشعب لتطال الأموال والبيانات بحيث يمتهن قراصنة الإنترنت هذه العملية إذ يكتسب من خلال ممارستها مهارات عالية تشجعه على ابتكار طرق جديدة يصعب معها الوصول إليهم فضلاً عن المردود المالي الكبير الناتج عن السرقة⁸⁰.

لاسيما أن دخول العميل إلى مواقع غير مرخصة أو غير موثوقة وعند ضياع أمواله فإنه يقوم بالاتصال بالبنك ويطلب باسترجاع الأموال مما يؤدي إلى النظر في مدى مسؤولية العميل والبنك في حالة حدوث هذا النوع من الاختراق كما نجد أحياناً حالات يتواطأ فيها العميل مع آخر من أجل سحب وتزوير التوقيع ومخاطبة البنك بعدم قيامه بالعملية ومن ثم استرجاع المبلغ بعد الطعن بصحة التوقيع⁸¹ وتتحقق هنا أهم التحديات التي تواجه المصارف في معرفة صدق العميل

⁷⁹ علي محبوب، علي سنوسي، واقع الصيرفة الإلكترونية في البنوك التجارية، مجلة شعاع للدراسة الاقتصادية، الجزائر، المجلد الرابع، العدد 2، 2020م، ص13.

⁸⁰ شما جاسم السليطي، المرجع السابق، ص47.

⁸¹ عبدالرحيم وهيبة، تقييم وسائل الدفع الإلكترونية ومستقبل وسائل الدفع التقليدية في ظل وجودها، مجلة الاقتصاد الجديدة الجزائر، العدد 2، 2010م، ص201.

من عدمه خصوصاً أن المبدأ المستند عليه هو فرض حسن نية العميل وعلى المصرف إثبات التواطؤ وسوء نية العميل.

كما أن من أهم صور مخاطر الاستعمال هو الإهمال الصادر من قبل العميل والذي ينتج عن أثره سرقة أمواله كضياع البطاقة البنكية وقيام الغير باستعمالها دون قيامه بالتبليغ، أو قيام العميل بإعطاء الرمز السري المرسل له عبر الهاتف للغير عندما يغيره بفوزه بجائزة أو تحديث بيانات من قبل شركات الاتصالات⁸² وكثيراً ما نرى ذلك في الواقع العملي.

تعد المخاطر المرتبطة بالعمل من أهم التحديات التي تواجه القطاع المصرفي، وبالتالي نرى تكافؤاً من الجهات المختصة بالدولة والمؤسسات المصرفية على نشر الوعي القانوني بالسيبرانية والحذر عند ممارسة العمليات المصرفية الإلكترونية، ومن أقرب الحملات التوعوية في هذا المجال في مملكة البحرين لدراسة وتطوير التعاون مع الجهات المعنية من المؤسسات المصرفية، وزارة الداخلية ومعهد الدراسات المصرفية والذي سلط الضوء على الاحتيال الإلكتروني وكيفية التصدي للتحديات الناتجة عن الممارسة المصرفية الإلكترونية⁸³، سيما يمكن للمصارف أن تستفيد من تجارب المصارف في الدول المختلفة حول وضع خطط وقائية تواجه الأعطال الإلكترونية التي قد توجه نظم الصيرفة الإلكترونية بحيث يتم التنسيق مع الجهات العليا في المصرف وتحت رقابة المصرف المركزي للحيلولة دون حدوث الضرر أو احتوائه⁸⁴، كما أنه من أبرز السبل في الحد من مخاطر العمليات المصرفية الإلكترونية وبالأخص استخدام البطاقات باعتبارها أحد وسائل الدفع الإلكتروني قيام City Bank في الولايات المتحدة الأمريكية بوضع الصورة الشخصية لصاحب البطاقة على الرغم من أن هذه الوسيلة لم تقم بالقضاء على الاحتيال وسرقة البطاقات إلا إنه ثبت أن هذه الطريقة كانت فعالة في مواجهة نسب الاحتيال⁸⁵.

علاوة على ذلك في إطار توفير وسائل الحماية اللازمة للحد من المخاطر الناتجة عن الاستعمال عادة ماتقوم المصارف باستعمال تقنية التشفير من أجل الحفاظ على المعلومات والبيانات التي تم الحصول عليها أثناء ممارسة عملية الدفع الإلكتروني بما في ذلك اتباع وتنفيذ تدابير

⁸² لعماري وليد، لوحيدية عبدالناصر، الضمانات القانونية ضد مخاطر استخدام وسائل الدفع الإلكتروني، بحث منشور لمداخلة في الملتقى الوطني المنظم بقسم الحقوق لكلية الحقوق والعلوم السياسية جامعة باتنة، 2019م، ص5.

⁸³ جريدة أخبار الخليج تعاون مشترك بين النيابة والمؤسسات المصرفية لمكافحة الاحتيال الإلكتروني (akhbar-alkhaleej.com)، مملكة البحرين، العدد 16958، 2023م.

⁸⁴ فريدي مشري، أمانة قاجة، الحماية القانونية لوسائل الدفع الإلكتروني، المركز الجامعي عبدالحفيظ بو الصوف، الجزائر، 2018م، ص9.

⁸⁵ عبدالرحيم وهيبة، المرجع السابق، ص11.

احترافية تتعلق بالوصول المصرح للمعلومات المشفرة من خلال أعداد محدودة من الموظفين وتصنيفها لأقسام متخصصة وتوزيعها لكل قسم القدر الذي يحتاجه لإتمام العمل⁸⁶.

ثانياً: المخاطر المرتبطة بالأمان والسرية:

أعمق التحديات وأشدّها تعقيداً وتداخلاً في ممارسة العمليات المصرفية عبر الإنترنت، هي الحفاظ على أمان عملية الدفع الإلكتروني واحترام الحق في الخصوصية وسرية المعلومات الواردة في عملية الدفع، وعليه، فعملية الدفع الإلكتروني عملية واسعة لانتقيد بنطاق جغرافي معين ومن الممكن أن تعيقها هجمات إلكترونية من الصعب تفاديها أو إيقافها وتختلف هذه المخاطر على حسب وسيلة الدفع المستخدمة⁸⁷.

وتتجلى أهمية الحد من المخاطر المتعلقة بالأمان في سلامة العمليات المصرفية الإلكترونية بشكل عام وعملية الدفع الإلكتروني باعتبارها أحد العمليات المصرفية الإلكترونية بشكل خاص في تحقيق الاستقرار المالي والاقتصادي للقطاع المالي، إذ أن انتهاك الشبكات والتجسس تفضي إلى مشكلات أمنية تصل إلى زعزعة الاستقرار السياسي لذلك تسعى المؤسسات المعنية والحكومات إلى تضمين التشريعات المنظمة للمصارف بنوداً تتعلق بأمان العمليات والشبكات الداخلية والخارجية وذلك فيه حماية للعمليات المصرفية الإلكترونية من مخاطر غسيل الأموال⁸⁸ وانتهاك البيانات الخاصة والسرية ومثالاً على أحد وسائل تحقيق أمن العمليات هو استعمال أنظمة التشفير⁸⁹ على الرغم من أن هذه الأنظمة تتطلب تدخلاً تقنياً إلا أنه تم تنظيمها في القوانين وفرض جزاءات جنائية على من ينتهك الخصوصية باستعمال وسيلة إلكترونية لفك التشفير، كما نظم المشرع البحريني التشفير وعرفه في قانون رقم (60) لسنة 2014 بشأن جرائم تقنية المعلومات على أنه: "عملية تحويل المعلومات أو نظم أو وسائل تقنية المعلومات أو الاتصالات إلى رموز غير مفهومة أو مبعثرة بحيث يصعب قراءتها أو معرفتها دون إعادتها إلى هيئتها الأصلية باستخدام كلمة سرية معينة أو أداة التشفير المستخدمة"⁹⁰، إذ تضمن القانون العقوبات المترتبة على الجرائم المرتكبة بوسائل تقنية المعلومات والغرض منه الحد من هذه الجرائم والقضاء عليها كلما أمكن ذلك.

⁸⁶ نصيرة شوب، الإدارة البنكية الإلكترونية في الجزائر، رسالة ماجستير، جامعة الجزائر، الجزائر، 2013م، ص87.

⁸⁷ أيمن عبدالله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2014م، ص777.

⁸⁸ عبدالرحيم وهيب، المرجع السابق، ص9.

⁸⁹ سعيد عبدالله الحامز، العمليات المصرفية الإلكترونية والإطار الإشرافي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص2398.

⁹⁰ مادة 1، قانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات، الجريدة الرسمية، العدد 3178، مملكة البحرين، 2014م.

ثالثاً: المخاطر التقنية والتشغيلية:

تواجه عملية الدفع الإلكتروني باعتبارها أحد العمليات المصرفية الإلكترونية مخاطر لا يكون لأطرافها يد فيها بتاتاً في بعض الأحيان أو أن تكون لأحدهم علاقة غير مباشرة في حدوث خلل تقني يمنع إتمام عملية الدفع الإلكتروني وبالتالي قد يتحصل من وراء هذا الخلل أضرار مرتبطة بأطراف عملية الدفع مثل نقل الأموال إلى طرف آخر غير مقصود⁹¹ فعدم كفاءة الأنظمة التي يمارس من خلالها عمليات الدفع الإلكتروني ممكن أن تتعرض لأعطال تؤدي إلى إخفاقها ومن ثم عدم تحقيق الغاية أو الهدف من إبرام الصفقة الأولى من بين الدائن والمدين في علاقة الدفع⁹²، ومن الضروري أن يكون لدى البنوك سياسات وإجراءات يتم العمل بها من أجل مواجهة المخاطر الكامنة في العمليات المصرفية الإلكترونية خصوصاً التقنية منها والتي تتطلب على وجه التحديد أدوات وخبرات تقنية إضافية للحفاظ على سلامة وأمن هذه العمليات⁹³.

لذلك هناك عديد من المحاولات في القطاعات المالية بشأن توحيد الأنظمة ورفع مستوى الكفاءة في العمليات المصرفية الإلكترونية عامة وعمليات الدفع الإلكتروني خاصة ومن هذه التحركات هي بروتوكول الصفقات المالية الآمنة⁹⁴ SET transaction Electronic Secure، إذ ظهر هذا النظام في العام 1996 بالتعاون مع أكبر شركات الدفع الإلكتروني ماستر كارد وفيزا وأمريكان اكسپريس، والغاية من هذا البروتوكول هي الحفاظ على أمن البيانات المرسلة مع مراعاة الخصوصية والتأكد من استلام الأمر إلى الجهة المراد الإرسال إليها بحيث يتم استخدام برمجيات المحفظة الإلكترونية والتي يدور مفهومها حول أن التاجر له شهادة رقمية معتمدة الإصدار من بنك ما، والعميل حامل البطاقة له شهادة رقمية تابعة للبطاقة بحيث يتيح لكل منهما التحقق من هوية الآخر دون أن يكون للتاجر الحق في الإطلاع على رقم البطاقة الائتمانية إذ تتم العملية بطريقة مشفرة وترسل إلى الرقم المرتبط بمصدر البطاقة للموافقة على العملية المالية⁹⁵.

⁹¹ هداية بوعزة، المرجع السابق، ص319.

⁹² علي عبدالله شاهين، نظم الدفع الكترونية ومخاطرها ووسائل الرقابة عليها دراسة تطبيقية على بنك فلسطين، مجلة جامعة الأزهر، فلسطين، سلسلة العلوم الإنسانية، المجلد 12، العدد 1، 2010م، ص14.

⁹³ Scott Sargent, Esq, Baker Donelson; Electronic banking: Risks and requirements; Thomson Reuters 2018, page 2.

⁹⁴ يقوم نظام الحركات المالية الآمنة بضمان أمن وسلامة المعاملات الإلكترونية التي تتم باستخدام بطاقات الائتمان حيث تم تطويره من قبل فيزا وماستر كارد حيث تم تصميمه لحماية معاملات بطاقات الائتمان والخصم ويجب التنويه بأنه ليس نظاماً يتيح الدفع إنما هو بروتوكول أمان يطبق على المدفوعات ويستخدم تقنيات تشفير وتجزئة مختلفة لتأمينها عبر الإنترنت ويوفر هذا النظام السرية، الثقة والخصوصية، بحث منشور ل Rahul Awati، على الرابط التالي: What is Secure Electronic Transaction (SET)? (techtargt.com).

⁹⁵ وافتد يوسف، المرجع السابق، ص167.

وعليه، يمكننا القول بأنه لاشك إن المخاطر التي تواجه عملية الدفع الإلكتروني عديدة ولا يمكن حصرها، ويعود ذلك لحجم العمليات التي يتم إبرامها في اليوم الواحد، "وطبقاً للإحصائيات بلغت الخسائر الناجمة عن جرائم الكمبيوتر 100 مليون دولار أمريكي في عام 1999 في الولايات المتحدة الأمريكية وحدها"⁹⁶ ولنفس على السنة الحالية مقارنة بالتطور الموهول في التقنيات والتكنولوجيا فبالأكيد، هذه الخسائر إن لم تواجه بشكل صحيح فإن ذلك يعود سلباً على الاقتصاد العالمي وليس اقتصاد الدولة وحدها، وبالتالي فإن هذه المخاطر توجب على الجهات المسؤولة أن توفر التأمين اللازم للحد من هذه المخاطر من أجل الحفاظ على سلامة وأمن العمليات ولا يمكن الحد من المخاطر دون تحليل شامل وتفصيلي للمعطيات التي تواجه العمليات المصرفية الإلكترونية بشكل عام ومن ثم النظر في مخاطر عملية الدفع الإلكتروني بشكل خاص للوصول إلى حلول تتماشى مع طبيعة المخاطر التي تواجهها.

⁹⁶ محمود أحمد الشراوي، مفهوم العمليات المصرفية الإلكترونية وأهم تطبيقاتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م، ص52.

المطلب الثالث

مزايا وعيوب العمليات المصرفية الإلكترونية

تلعب العمليات المصرفية الإلكترونية دوراً بارزاً في الحياة اليومية للأشخاص أفراداً وتجاراً مما يحتم على البنوك مواكبة التطورات العالمية في ما يتعلق بتحسين وابتكار وسائل تمكن البنك نفسه والعملاء من إجراء عمليات مصرفية إلكترونية آمنة وسليمة⁹⁷.

ولما للعمليات المصرفية الإلكترونية من أهمية فإننا في هذا المطلب سنطرح أبرز المزايا التي نتجت عن التحول من العمليات المصرفية التقليدية إلى العمليات المصرفية الإلكترونية ومن ثم بيان المشكلات والعيوب التي نشأت إثر هذا التحول الإلكتروني من خلال تقسيمه إلى فرعين:

- الفرع الأول: مزايا العمليات المصرفية الإلكترونية.
- الفرع الثاني: عيوب العمليات المصرفية الإلكترونية.

⁹⁷ شيرين سلطان، التنظيم القانوني للمعاملات المصرفية الإلكترونية في ضوء السياسة النقدية للدولة، دار الجامعة الجديدة للنشر، مصر، 2020م، ص 296.

الفرع الأول

مزايا العمليات المصرفية الإلكترونية

تعتبر العمليات المصرفية الإلكترونية من أهم التطورات التي شهدتها قطاع المصارف في العقود الأخيرة، حيث تمثل هذه العمليات الطرق الحديثة لإجراء العمليات المصرفية والتعاملات المالية بشكل أسرع وأكثر أماناً وفعالية.

تتميز العمليات المصرفية الإلكترونية بالعديد من المزايا والفوائد التي أدت إلى نمو القطاع المصرفي بشكل كبير فضلاً عن التأثير في ازدهار التجارة الإلكترونية وانتشارها، لذلك فيما يلي سنذكر أهم المزايا الناتجة عن وجود العمليات المصرفية الإلكترونية:

أولاً: زيادة الراحة وتوفير الوقت:

استخدام العمليات المصرفية الإلكترونية أفضت إلى الحد من زيارات العميل من أجل إتمام معاملاته المصرفية إلى مقر البنك، وبالتالي عادةً ما يرتبط في مواعيد عمل البنوك، مما يؤدي في بعض الأحيان إلى ضياع الهدف من إجراء العملية المصرفية، لذلك من أهم الفوائد المرتبطة بالوقت هو أن العميل قادرٌ على إتمام عملياته في أي وقت على مدى 24 ساعة خصوصاً أن الأعمال التجارية بطبيعتها تتسم بالسرعة والمرونة وبالتالي يحفز التجار إنجاز معاملاتهم بشكلٍ سريعٍ ومثمرٍ مما يخلق فرصة لدى البنك على التركيز والاستثمار في بعض القطاعات المستهدفة التي تفضل العمل مع بنوك تستخدم الوسائل الإلكترونية من أجل الوصول للغاية المطلوبة في أقل وقت ممكن⁹⁸.

كما أن توفير الوقت لا يصب فقط في مصلحة العميل، بل أن أتمتة العمليات المصرفية الإلكترونية قللت من الوقت الذي يستغله موظف البنك في إتمام العمليات المصرفية بالشكل التقليدي والتي يحسب فيها وقت انتظار العميل، النظر في الموضوع طباعة الأوراق، وجميع الإجراءات المتصلة في إتمام العملية وبالتالي يكتسب البنك وقتاً إضافياً يُمكن الموظف من إتمام العمليات المصرفية التي لازالت تحتاج إلى حضورٍ شخصيٍّ من قبل العميل نفسه.

أيضاً من المزايا التي تعود على الفرد عند إجراء العمليات المصرفية الإلكترونية يستطيع العميل أن يقوم بأداء المدفوعات الإلكترونية، إصدار بطاقاتٍ بنكيةٍ، أو إنشاء حسابات بنكية

A.Anish Kumar, S.Ariharan, D. Asir Immanuvel, Internet Banking – benefits and challenges,⁹⁸ International Conference on "Innovative Management Practices" Organize by SVCET, Virudhunagar, Vol-1 Issue-1 2016 , page 149.

بضغطه زرٍ حتى دون الحاجة إلى الخروج من المنزل أو مغادرة المكان وذلك تسهيلً من الصعب أن يتغاضى عنه⁹⁹.

ثانياً: التوفير في التكاليف ورفع الكفاءة:

تقدم العمليات المصرفية الإلكترونية كفاءة وسرعة أكثر من العمليات المصرفية التقليدية، ويمكن أن تؤدي إلى توفير التكلفة عن طريق استخدامها، فالاستعانة بالوسائل الإلكترونية من أجل إتمام العملية المصرفية يقلل التكاليف المرتبطة بالعناصر المادية فيها مثل تكاليف بناء الفروع البنكية، تكاليف الطباعة، الشحن، التخزين والتدقيق اليدوي من قبل الموظف، بالإضافة إلى ذلك يتحقق التوفير في التكلفة من خلال تحسين كفاءة العمل وتقليل الحاجة إلى الموظفين¹⁰⁰.

كما أن استخدام التكنولوجيا المتقدمة من شأنه رفع كفاءة وجودة العملية المصرفية الإلكترونية، وتحسين العمليات، وتقليل الأخطاء الناتجة، ويمكن استخدام التقنيات المتطورة من أجل تحليل البيانات وتحسين العمليات الإلكترونية والتواصل الدوري مع العملاء، وبشكل عام يمكن تقليل التكلفة من خلال استخدام العمليات المصرفية الإلكترونية بدل العمليات المصرفية التقليدية كلما أمكن ذلك لتحسين كفاءة العمل المصرفي¹⁰¹.

ثالثاً: الانتشار والقدرة على الوصول إلى قاعدة أوسع من العملاء:

مايميز العمليات المصرفية الإلكترونية أنها عابرة للحدود غير مرتبطة بمكان وزمان معينين وبالتالي فإنه كنتيجة ومزية بديهية للبنك هو الانتشار والوصول إلى قواعد عريضة من العملاء دون التقيد بوقت أو مكان ما¹⁰²، وعليه فإن هذا الانتشار يؤدي إلى زيادة عدد العملاء مما يصب في مصلحة البنك، على الرغم من أن هذا الانتشار سلاح ذو حدين، فالحد الإيجابي هو مايتعلق بالربح والانتشار أما الحد السلبي هو العالمية ومايترب عليها من مخاطر قانونية أو فنية وما إلى ذلك.

⁹⁹ Hajera Fatima Khan, "E-Banking: Benefits and Related Issues". American Research Journal of Business and Management; Vol3, Issue1, page5.

¹⁰⁰ خالد عبد المنعم عبدالفتاح، هاني محمد السيد على، أثر المخاطر الإلكترونية على البنوك الإلكترونية، مجلة حقوق دمياط للدراسات القانونية والاقتصادية، العدد السادس، مصر، 2022م، ص82.

¹⁰¹ Hajera Fatima Khan, Ibid, Page5.

¹⁰² Abdul-Hussein Jasim Mohammed, Munaf Abdulkadhim Mohammed, Ahmed Hussein Ahmed, Impact of Banking Riskson the Electronic Banking Services: A Comparative Study, TEM Journal. Volume 10, Issue 2, Page667.

رابعاً: الأمان والموثوقية:

من أهم المخاوف التي تواجه العملاء عن أداء العمليات المصرفية الإلكترونية هي أمانها وموثوقيتها، لذلك توفر البنوك آليات ووسائل تقنية متجددة ومتطورة من أجل حماية ممارسة العمليات المصرفية الإلكترونية من أي هجوم خارجي أو داخلي وبالتالي تحافظ على عملائها بزيادة استعمال الخدمات المصرفية التي تقدمها¹⁰³. ومثالاً على هذه التقنيات هي تقنية التشفير.

تعد العمليات المصرفية الإلكترونية البديل المثالي للعمليات المصرفية التقليدية مما يجعلها الخيار الأمثل للعملاء، ولكن على الرغم من هذه المزايا فإن هناك عيوباً صاحبت التحول الإلكتروني تم حل بعضها ولكن لا يمكن إغفال العيوب الناتجة عن استعمال العمليات المصرفية الإلكترونية، وعليه فإن الباحث سيبين في الفرع التالي عدداً من عيوب العمليات المصرفية الإلكترونية وذلك فيما يلي.

الفرع الثاني

عيوب العمليات المصرفية الإلكترونية

على الرغم من العديد من المزايا التي تصاحب ممارسة العمليات المصرفية الإلكترونية إلا أن هناك عيوباً تؤثر على القطاع المصرفي والقطاع الاقتصادي فضلاً عن التأثير المباشر على الأفراد من ممارسي العملية المصرفية الإلكترونية بشكل عام، وبالتالي من الممكن أن يغض الأفراد النظر عن ممارسة العمليات المصرفية الإلكترونية والبقاء على الصورة التقليدية وعليه، فإننا سنبين أهم العيوب التي تواجه أطراف العملية المصرفية الإلكترونية تباعاً:

أولاً: التعرض للهجمات الإلكترونية:

ربما يكون التحدي الأكبر الذي يواجه خدمات الإنترنت هو مسألة سلامة العمليات التي يجريها العملاء وأمن معلوماتهم الخاصة. إذ أثبتت الشبكة أنها معرضة بشكل مكثف للاحتيال وسرقة الهوية حيث يتم سرقة معلومات خاصة حساسة حول الأعمال التجارية والأفراد من قبل أشخاص غير مصرح لهم، واستخدامها لدفع فواتير بطاقة ائتمان كبيرة أو لتدمير سمعة الضحايا¹⁰⁴.

¹⁰³ Bojan Daniela, Mutu Simona, Pun Drago, Electronic Banking – Advantages for financial services delivery, Cluj-Napoca University, Article published on : [106 \(steconomiceuoradea.ro\)](http://106.steconomiceuoradea.ro), 2010, page 674.

¹⁰⁴ Machogu AM, Okiko E-banking Complexities and the Perpetual Effect on Customer Satisfaction in Rwandan Commercial Banking Industry: Gender as a Moderating Factor. J Internet Bank E-banking Complexities and the Perpetual Effect on Commer,(Article published), 2015, page 5.

ثانياً: عدم الإلمام الإلكتروني:

أداء العمليات المصرفية الإلكترونية عن بعد يحتاج إلى مزيد من الجهود التي تقع على عاتق القطاع المصرفي في نشر الوعي المتعلق باستخدام العمليات المصرفية الإلكترونية دون الحاجة إلى اللجوء إلى البنوك من أجل إتمام هذه العمليات، ولكن تزال هناك فئة من العملاء لا تحبذ استعمال الخدمات المصرفية الإلكترونية، وذلك قد يرجع لصعوبة الاستعمال أو اللغة أو الخوف من الهجمات الإلكترونية التي ستؤدي إلى خسارة أموالهم¹⁰⁵.

ثالثاً: زيادة التكلفة الناتجة عن استخدام التقنيات الإلكترونية:

يمكن أن يتحمل البنوك والعملاء تكاليف إضافية لاستخدام العمليات المصرفية الإلكترونية أو حمايتها وتطوير البرامج التي من شأنها الحفاظ على أمان العمليات واستمراريتها، ومن هذه التكاليف استخدام شبكات الإنترنت، التواصل، شراء برمجيات تقنية للحفاظ على الأمان¹⁰⁶.

رابعاً: الأخطاء التقنية والفنية:

قد يواجه العملاء والبنوك أعطالاً فنية عند ممارسة العمليات المصرفية الإلكترونية مما يفوّت الغرض من إتمام العملية الإلكترونية فضلاً عن ضياع الأموال، كما أن التحدي الأكبر هو عند تحقق هذا الخلل يسهّل اللوج إلى قواعد بيانات البنك من أجل الحصول على معلومات تتعلق بالبنك والعملاء وبالتالي يمكن أن تحدث الجريمة المعلوماتية¹⁰⁷.

خامساً: صعوبة الوصول إلى المجرم المعلوماتي:

العمليات المصرفية الإلكترونية تتميز باللاجغرافية، فحدودها غير معلومة ودائماً مايلقى المجرم المعلوماتي طريقة من أجل الحصول على أموال ومعلومات¹⁰⁸ عن طريق العمليات الناشئة عبر الفضاء الرقمي فيكون من الصعب على الجهة المعنية أن تصل إلى المجرم المعلوماتي¹⁰⁹

[Customer Satisfaction in Rwandan Commercial Banking Industry: Gender as a Moderating Factor | Open Access Journals \(icommercecentral.com\)](https://www.icommercecentral.com/Customer-Satisfaction-in-Rwandan-Commercial-Banking-Industry-Gender-as-a-Moderating-Factor)

¹⁰⁵ أديب قاسم شندي، الصيرفة الإلكترونية أنماطها وخيارات القبول والرفض، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 27، 2011م، ص15.

¹⁰⁶ أديب قاسم شندي، المرجع نفسه، ص15.

¹⁰⁷ زعباب سهام، المرجع السابق، ص26.

¹⁰⁸ Hajera Fatima Khan, Ibid, page 6.

¹⁰⁹ "المجرم المعلوماتي هو الذي لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محلياً ودولياً"، سهام خليلي، خصوصية المجرم الإلكتروني، مجلة المفكر، جامعة محمد خيضر بسكرة، العدد 14، 2017م، ص405.

بطريقة سهلة، على الرغم من وجود جهود دولية لوضع التشريعات التي تحد من الهجمات الإلكترونية إلا إنها لاتزال موجودة وشائعة.

ختاماً، العمليات المصرفية الإلكترونية تتمتع بالعديد من المزايا كالراحة والسهولة والسرعة وزيادة الكفاءة، إلا أنه تقابلها أيضاً عيوب لا يمكن إنكارها، ولكن من الممكن تقاؤها أو التقليل من حجمها كلما أمكن ذلك، فأثر التحول إلى العمليات المصرفية الإلكترونية كبير جداً وواضح على جميع الأصعدة، خصوصاً فيما يتعلق بتحسين الكفاءة، الدقة، زيادة الأرباح ورضا العميل من خلال تحسين تجربته والتقليل من الزحام في الفروع المصرفية، ومع ذلك فإنه يجب توخي الحذر من استخدام العمليات المصرفية الإلكترونية، حيث ثبت أن المنظمات التي تبنت بنجاح الخدمات المصرفية الإلكترونية كانت قادرة على أن تدمج بين التركيز على العملاء وعملية التخطيط الاستراتيجي فضلاً عن قياس الأداء والكفاءة التقنية وتجسين جودة المنتجات ومرونتها في إطار تشريعي متكامل قادر على الاستجابة لتغيرات السوق وطلب العملاء¹¹⁰.

¹¹⁰ Bojan Daniela, Mutu Simona, Pun Drago, Ibid, page 667.

المبحث الثاني

ماهية المخاطر السيبرانية في القطاع المصرفي

شهدت الصناعة المالية تحولاً كبيراً في مجال العمليات المصرفية الإلكترونية التي تشمل مجموعة واسعة من الخدمات والعمليات المالية التي تتم من خلال القنوات الرقمية، مثل الإنترنت وتطبيقات الهاتف المحمول وأنظمة الدفع الإلكترونية. تتضمن العمليات المصرفية الإلكترونية مجموعة واسعة من الأنشطة المالية التي تتم من خلال الوسائل الإلكترونية، تشمل هذه الأنشطة، على سبيل المثال لا الحصر، تحويل الأموال عبر الإنترنت وإدارة الحسابات ودفع الفواتير ومعاملات الأموال الإلكترونية والخدمات المصرفية عبر الهاتف المحمول، أحدثت الخدمات المصرفية الإلكترونية ثورةً في طريقة تفاعل العملاء مع مؤسساتهم المالية¹¹¹.

أدى تطوير التكنولوجيا المالية إلى تحسين الخدمات التي تقدمها البنوك بشكل كبير من خلال قنوات جديدة ومبتكرة، لقد غير هذا التحول الطريقة التي يعمل بها القطاع المصرفي وسمح بتوفير الوقت والمال والجهد ومع ذلك، مع الفرص التي أوجدتها التكنولوجيا تواجه البنوك مخاطر جديدة، مثل الهجمات الإلكترونية، والتي يمكن أن تعطل الخدمات المالية وتقوض الأمن والاستقرار، كما أظهرت التقارير أن قطاع الخدمات المالية معرضٌ بشكل خاصٍ للهجمات الإلكترونية أكثر من أي قطاع آخر¹¹².

وعليه سيتناول هذا المبحث المخاطر السيبرانية التي تواجه العمليات المصرفية الإلكترونية من خلال عرض مفهوم المخاطر السيبرانية والتنظيم القانوني، كما سيتم مناقشة أهمية الأمن السيبراني في القطاع المصرفي وتسلط الضوء على الحاجة الماسة لاتخاذ تدابير وقائية تقلص من المخاطر التي تتعرض لها العمليات المصرفية الإلكترونية وذلك فيما يلي.

¹¹¹ سيماء محسن علاوي، آفاق تطبيق الصيرفة الإلكترونية في الاقتصاد الإماراتي، مجلة كلية المأمون، العراق، العدد الرابع والثلاثون، 2019م، ص 141، 142.

¹¹² Aquiles A. Almansi, Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision, World Bank Group, Washington, 2018, page 1.

المطلب الأول

المخاطر السيبرانية بين المفهوم والتنظيم القانوني

أدى الاعتماد المتزايد على الأنظمة الرقمية إلى زيادة المخاطر الإلكترونية، وقد يسميها آخرون المخاطر السيبرانية، والتي تعتبر الآن أكبر خطرٍ على الشركات على مستوى العالم، حيث تواجه الشركات هجمات إلكترونية معقدة وموجهة، مثل برامج الفدية والقرصنة عبر البريد الإلكتروني للأعمال، والتي غالبًا ما تكون مصحوبةً بمطالب ابتزازٍ كبيرة، كما تضيف الاختلافات السياسية بين البلدان أيضًا تعقيدًا إلى التهديدات السيبرانية¹¹³. في هذا المطلب سيبين الباحث بشكل أوضح المخاطر السيبرانية من خلال تمييزها عن المخاطر التقليدية من ناحية مفهومها، والخصائص التي تتمتع بها، كما سيوضح الباحث التنظيم القانوني للمخاطر السيبرانية وصولاً إلى أهم المخاطر التي تواجه البنوك وكيفية التصدي لها فيما يلي من خلال الفرعين التاليين:

- الفرع الأول: مفهوم المخاطر السيبرانية.
- الفرع الثاني: التنظيم القانوني للمخاطر السيبرانية.

¹¹³ زيدك الطاهر، محمد ورنقي، استراتيجية مكافحة الإرهاب الإلكتروني في المجال الاقتصادي، المركز العربي الديمقراطي، مجلة الدراسات الأفريقية وحوض النيل، المجلد الثاني، العدد الخامس، 2019م، ص 271.

الفرع الأول

مفهوم المخاطر السيبرانية

يدور مفهوم المخاطر السيبرانية حول احتمالية وقوع حادثة إلكترونية، يترتب عليها آثار تطل الأصول أو السمعة لمؤسسة ما¹¹⁴، هنالك العديد من التعريفات للمخاطر السيبرانية وإجمالاً يمكن الإشارة لها بأنها أي خطر ينشأ عن استخدام تكنولوجيا المعلومات والاتصالات، والذي يضر بسرية البيانات أو الخدمات أو توفرها أو سلامتها أو إمكانية تتبعها. يمكن أن تؤدي هذه المخاطر إلى نقاط ضعف في التكنولوجيا التشغيلية، وتعطل الأعمال، وفشل البنية التحتية، والأضرار المادية للأفراد والممتلكات وقد يتعدى الخطر نطاق جغرافي معين "محلي" والانتشار بشكل أكبر على نطاق عالمي مثلاً¹¹⁵، فضلاً عن احتمال حدوث ضررٍ مادي ناتج عن حوادث الأمن السيبراني أو إساءة استخدام البيانات.

تنتج المخاطر السيبرانية عن حدث إلكتروني في نظام المعلومات، يمكن أن يتشكل الحدث الإلكتروني بصورة سلبية كحقن البرامج الضارة والتصيد، فيمكن ملاحظته داخل نظام معلومات مما يسبب انتهاكاً للسياسات الأمنية للأنظمة واختراق المعلومات، ويمكن أن تعمل الأحداث الإلكترونية بصورة إيجابية كمؤشرات للحوادث الإلكترونية المحتملة مستقبلاً، قد تتضمن هذه الحوادث تهديدات للأمن السيبراني لنظام المعلومات أو انتهاكات لسياسات أو إجراءات الأمان أو سياسات الاستخدام المقبولة، بغض النظر عما إذا كانت ناتجة عن نشاطٍ ضارٍ¹¹⁶.

يساهم عددٌ من العوامل في المخاطر السيبرانية في المؤسسات المالية، بما في ذلك الاتجاه المتزايد نحو العولمة، والاعتماد على التكنولوجيا المبتكرة سريعة التطور داخل كلٍ من النظام المالي والبنية التحتية لتكنولوجيا المعلومات، على الوعي بالمخاطر المرتبطة بالحوادث السيبرانية من خلال المشرفين والهيئات التنظيمية في جميع أنحاء العالم، مما أجبرهم على اتخاذ خطواتٍ تهدف إلى التخفيف من المخاطر السيبرانية في المؤسسات المالية، بما في ذلك تعزيز قدرات المرونة

¹¹⁴ دلم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون، المعهد العربي للتخطيط، الكويت، العدد 63، 2019م، ص 12.

¹¹⁵ Van Eeten, M.J.G., De Bruijn, H., Kars, M., Van der Voort, H. and van Till, J, 'The governance of cybersecurity: a framework for policy', Int. J. Critical Infrastructures, Vol. x, No. x, 2006, page 361.

¹¹⁶ European Insurance and Occupational Pension Authority cyber risk of insurers challenges and opportunity, Publication of the European union, Luxembourg, 2019, Page 9.

وتتخذ خططاً للاستجابة الفعالة للهجمات السيبرانية والتعافي منها¹¹⁷، وطبيعة المخاطر السيبرانية أنها دائماً متجددة، وتختلف مقاييس التصدي لها من مؤسسة إلى أخرى، ولذلك حاول أصحاب المصلحة من هيئات دولية ومنظمات مختصة بالقطاع المالي إيجاد معايير أساسية مشتركة، من أجل الحد من انتشار المخاطر السيبرانية وتقليل أثرها على القطاع، على سبيل المثال: ألزمت هيئة المصارف الأوروبية تحديد مخاطر تكنولوجيا المعلومات وفق 5 فئات وهي:¹¹⁸

- 1- **مخاطر التوفر والاستمرارية:** وهي مخاطر تأثر أداء وتوافر الأنظمة والبيانات سلباً، بما في ذلك عدم القدرة على التعافي في الوقت المناسب، بسبب فشل الأجهزة أو البرامج، أو نقاط الضعف الإدارية، أو أي حدث آخر.
- 2- **مخاطر سلامة البيانات:** وهي خطر أن تكون البيانات المخزنة والمعالجة غير كاملة أو غير دقيقة، أو غير متسقة عبر الأنظمة المختلفة.
- 3- **مخاطر التغيير:** وهي المخاطر الناشئة عن عدم قدرة المؤسسة على إدارة تغييرات النظام في الوقت المناسب، وبطريقة خاضعة للرقابة.
- 4- **مخاطر الاستعانة بمصادر خارجية:** وهي إشراك طرف ثالث، أو كيان آخر في المجموعة (الاستعانة بمصادر خارجية داخل المجموعة)، لتوفير الأنظمة أو الخدمات ذات الصلة، مما يؤثر سلباً على أداء المؤسسة وإدارة المخاطر.
- 5- **المخاطر الأمنية:** وهي خطر الوصول غير المصرح به إلى الأنظمة، من داخل المؤسسة أو خارجها.

إيجاد لغة مشتركة بين المصارف لتحديد المخاطر، يعد من أهم الخطوات نحو التصدي لها، إذ التعاون والتنسيق بين المصارف لتبادل المعلومات يؤدي للحد من انتشار الأحداث الإلكترونية لعدد أكبر من المؤسسات، مما يسهم في تعزيز أمن القطاع المالي.

التمييز بين المخاطر السيبرانية والمخاطر التقليدية في العمليات المصرفية:

يعد التمييز بين المخاطر الإلكترونية والمخاطر التقليدية أمراً أساسياً في فهم التحديات الفريدة التي يفرضها المشهد الرقمي، لا سيما في سياق العمليات المصرفية الإلكترونية، في حين

¹¹⁷ Filippo Curti, Jeffrey Gerlach, Sophia Kazinnik, Michael Lee and Atanas Mihov, Cyber Risk Definition and Classification for Financial Risk Management, published online paper on : [Cyber Risk Definition and Classification for Financial Risk Management \(richmondfed.org\)](http://CyberRiskDefinition.org), 2019, page 2.

¹¹⁸ Aquiles A. Almansi, Ibid, page 8.

أن المخاطر التقليدية كانت لفترة طويلة مصدر قلقٍ للقطاع المالي، فإن ظهور المخاطر السيبرانية يقدم بعداً جديداً من نقاط الضعف والعواقب المحتملة¹¹⁹.

أولاً: المخاطر التقليدية:

تدور المخاطر التقليدية في القطاع المصرفي بشكل أساسي حول تقلبات السوق، ومخاطر الائتمان، ومخاطر أسعار الفائدة، والمخاطر التشغيلية الناشئة عن العمليات الداخلية والأخطاء البشرية. تمت إدارة هذه المخاطر تاريخياً من خلال ممارسات وأنظمة إدارة المخاطر الراسخة¹²⁰.

ثانياً: المخاطر السيبرانية:

من ناحية أخرى، تنشأ المخاطر السيبرانية من رقمنة العمليات المالية والاعتماد المتزايد على العمليات التي تحركها التكنولوجيا. تتضمن هذه المخاطر انتهاكات متعددة أو عرضية للأنظمة والبيانات الرقمية من قبل مجرمي الإنترنت أو المتسللين أو حتى المتصفحين، وتتمتع المخاطر الإلكترونية بخصائص مميزة:

1. **الطبيعة الرقمية:** تكمن جذور المخاطر السيبرانية في المجال الرقمي، حيث يستغل المهاجمون نقاط الضعف في البرامج والشبكات والمنصات الرقمية للحصول على وصول غير مصرح به أو التسبب في اضطراب¹²¹.
2. **عدم الكشف عن الهوية والوصول:** يمكن تنفيذ الهجمات الإلكترونية عن بُعد، ودون الكشف عن الهوية، مما يسمح للجناة باستهداف المؤسسات عبر الحدود دون وجود مادي مباشر¹²².
3. **التطور السريع:** يتطور مشهد المخاطر الإلكترونية بسرعة، حيث يتكيف المهاجمون مع الإجراءات الأمنية، مما يستلزم اليقظة والقدرة على التكيف بشكل مستمر.

¹¹⁹ محمد الكويتي، الاتجاهات المتباعدة للأمن السيبراني: مبادرة النبض السيبراني.. دراسة حالة، أوراق محاضرات (3)، أبوظبي: مركز تريندز للبحوث والاستشارات، الإمارات العربية المتحدة، 2022م.

¹²⁰ Joel Burleson-Davis, "Cybersecurity: Trends From 2022 and Predictions For 2023", info security magazine, 14 Dec. 2022, <https://bit.ly/3WSMFed>

¹²¹ بلال عبدالمطلب بدوي، البنوك الإلكترونية ماهيتها معاملاتها والمشاكل التي تثيرها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003، ص 1952.

¹²² ناظم محمد الشمري، د. عبدالفتاح زهير العبدلات، الصيرفة الإلكترونية "الأدوات والتطبيقات ومعوقات التوسع"، دار وائل للنشر، الأردن، 2008م، ص 245.

4. **النطاق والسرعة:** يمكن أن تؤثر الهجمات الإلكترونية على عدد كبير من الأفراد والمؤسسات في وقت واحد، وتنتشر بسرعة من خلال الشبكات المترابطة¹²³.

5. **التهديدات غير المرئية:** على عكس المخاطر التقليدية، فإن المخاطر الإلكترونية غير ملموسة وقد لا تظهر إلا بعد وقوع هجوم، مما يجعل الوقاية والتخفيف من آثارها أكثر صعوبة¹²⁴.

الفرع الثاني

التنظيم القانوني للمخاطر السيبرانية

نشأت الصعوبات في تحديد المسؤولية الإلكترونية عن المخاطر الإلكترونية، من عدم وجود تعريف واضح. تصبح هذه المشكلة أكثر تعقيداً عند محاولة توحيد مصطلحات "الأمن السيبراني، والهجمات الإلكترونية على المستوى العالمي، إذ واجه المتخصصون تحديات في التوفيق بين هذين المصطلحين لمعالجة هذا الأمر، يمكن أن نستند إلى تعريف الاتحاد الدولي للاتصالات¹²⁵ في التقرير الصادر بعنوان: "اتجاهات الإصلاح في الاتصالات لعام 2010-2011 الأمن السيبراني على أنه: "مجموعة من المهمات، مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريب وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين¹²⁶"، أما الهجمات الإلكترونية، فهناك العديد من التعريفات التي تبين مفهومها، حيث عرّفها جانب من الفقه بأنها "فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام."¹²⁷ وبالإشارة إلى تعريف الهجمات الإلكترونية الآنفة الذكر، فيتبين للباحث أنه عرّف الهجمات الإلكترونية وحدها بغرضين فقط، ولذلك فالأخذ بهذا التعريف يمكن أن يولد التساؤل ماذا لو كان الغرض شخصي، هل هذا يعني إن المهاجم يفر من المسؤولية؟ أو هل ذلك لا يعد من المخاطر الإلكترونية التي تواجه الأفراد عند حدوثها؟

¹²³ بغدادي شامي، تامين الخطر السيبراني، مجلة هيردوت للعلوم الإنسانية والاجتماعية، الجزائر، المجلد 7، العدد 25، ص 241.

¹²⁴ بغدادي شامي، المرجع نفسه، ص 241.

¹²⁵ الاتحاد الدولي للاتصالات هو وكالة الأمم المتحدة في مسائل تكنولوجيا المعلومات والاتصالات تأسس عام 1865 حيث يتولى وضع المعايير التقنية لضمان توصيل سلس بين الشبكات والتكنولوجيا لتسهيل تواصل الشبكات هدف الاتحاد من أجل تعزيز الوصول إلى تكنولوجيا المعلومات والاتصالات عالمياً، ويواجه التحديات العالمية الحديثة، للمزيد انظر إلى [الاتحاد الدولي للاتصالات \(itu.int\)](http://itu.int).

¹²⁶ حنين جميل أبوحسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2021م، ص 20.

¹²⁷ منى عبدالله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، 2020م، ص 11.

أما المشرع الإماراتي قد أوضح تعريف الهجمات السيبرانية وشمل كلاً من المصطلح "سيبراني"، و "الهجمات السيبرانية" في المرسوم بقانون الاتحادي رقم (34) لسنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية، في المادة 1 حيث عرفها:

- **السيبراني:** كل ما يتعلق بالشبكات المعلوماتية الحاسوبية، وشبكة الإنترنت، والبرامج المعلوماتية المختلفة وكل الخدمات التي تقوم بتنفيذها.

- **الهجمات الإلكترونية:** كل استهدافٍ متعمدٍ ومخططٍ للأنظمة المعلوماتية، أو البنية التحتية، أو الشبكات الإلكترونية، أو وسائل تقنية المعلومات يقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمها¹²⁸.

ويمكن أن نعول على تعريف المشرع الإماراتي المذكور أعلاه، حيث شمل العديد من الجوانب المتعلقة بالهجمات الإلكترونية، وبالتالي فإنه تقادى القصور في التعريف الأول، إذ وسع من دائرة الأغراض المتنوعة للهجمات، كالأغراض الشخصية مثل السرقة أو التجسس، أو لأغراض اعتراضية كالتسلل والتجسس وغيرها، فضلاً عن بيانه الاستهداف المتعمد والمخطط التي قد يواجه أحد الأشكال الإلكترونية كالأنظمة المعلوماتية أو البنية التحتية ويؤثر عليها سلباً كتوقف الخدمات أو تعطيلها. لذلك فإن هذه النقاط تمثل جوانب مهمة في تعريف الهجمات الإلكترونية، وتسلط الضوء على تأثيرها السلبي على الأنظمة والمعلومات الحيوية بشكل عام.

من المهم تحديد ومراقبة مخاطر المسؤولية المدنية المرتبطة بمثل هذه الهجمات بموجب القانون الوطني، بحيث يمكن وضع حدودٍ للمسؤولية لتحفيز تدابير الأمن السيبراني، دون التسبب في آثارٍ جانبيةٍ مقيدةٍ لا داعي لها، أو إعاقة الوصول إلى الابتكارات والاختراعات الجديدة في العديد من البلدان، لذلك وجب على الشركات ضمان أمن المعلومات والبيانات الشخصية من حيث اتخاذ التدابير التقنية والقانونية اللازمة للحفاظ على وجودها واستمراريتها في السوق، إذ وضعت العديد من البلدان قوانين تتعلق بحماية المعاملات الإلكترونية في شتى المجالات، إلا أن طبيعة هذه المعاملات الإلكترونية اللامحدودة والغير مرتبطة بحدودٍ جغرافيةٍ معينة، يحتاج إلى تعاونٍ إقليميٍ ودوليٍ من خلال إبرام اتفاقياتٍ تعاونيةٍ من شأنها الكشف عن بيانات الهجمات السيبرانية، وتعقب أثرها عن طريق قاعدة بياناتٍ مركزيةٍ يتم التتبع من خلالها، وإعلام الجهات المسؤولة في الدول الموقعة للحد من الأضرار الناتجة عن الهجمات السيبرانية وردع مرتكبها، الجدير بالذكر أن

¹²⁸ المادة 1، مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية ، الإمارات العربية المتحدة.

الاتحاد الأوروبي يسعى إلى إستحداث تشريع إقليمي، من شأنه الحفاظ على أمن المعاملات الإلكترونية في الاتحاد، وتسهيل عملية الكشف عن الجرائم السيبرانية¹²⁹.

تزايد الاعتماد على العمليات المصرفية الإلكترونية في العالم، أدى إلى تعرض القطاع المصرفي إلى مخاطر مرتبطة بالفضاء السيبراني التي تتم من خلاله، لذلك كان لزاماً على الجهات المعنية بتوفير الأسس والمعايير التي يتم فيها الحفاظ على أمن وسلامة العملية المصرفية الإلكترونية، وبذلك تحد من الأضرار الناتجة عن التعامل السيبراني المصرفي، وكانت لجنة "بازل" التي نشأت في عام 1974م¹³⁰ أولى الخطوات نحو تحقيق التوازن وسلامة العمليات المصرفية، حيث اهتمت اللجنة بإدارة المخاطر المصرفية، وسلامة عمليات البنوك المالية والرقابة عليه¹³¹، ومن أهم السياسات التي حددتها في سبيل قياس ورقابة المخاطر التي تتعرض لها كان سياسة تحديد المخاطر التي تواجه البنوك، وسببين الباحث أهم أنواع المخاطر التي تواجه العمليات المصرفية الإلكترونية وفق لجنة "بازل" على النحو الآتي:

أولاً: مخاطر التشغيل:

تعد مخاطر التشغيل من أهم المخاطر التي تواجه البنوك وأكثرها تعقيداً وارتباطاً بالمخاطر الأخرى، إذ تعنى هذه المخاطر بتلك المخاطر التي تنشأ نتيجة لخلل ما في التكنولوجيا المرتبطة بالنظم العاملة في البنك¹³²، وقد تحدث نتيجة أسباب عديدة منها إخفاق برامج التغذية والصيانة للأنظمة المستخدمة، أو عدم كفاية النفقات التابعة لها أو التغاضي عنها، كما تسهم الأخطاء المصاحبة لممارسة العملية المصرفية الإلكترونية في حدوث المخاطر والاختراق من غير المرخص لهم، سواء كان الخطأ من قبل موظفي البنك أو العملاء، ويمكن تلخيص هذه المخاطر في ثلاث عناوين رئيسية:¹³³

¹²⁹ اللجنة الاقتصادية والاجتماعية لغربي آسيا، بناء الثقة بالخدمات الإلكترونية بمنطقة الإسكوا، الأمم المتحدة، 2009م، ص5.

[/https://www.unescwa.org](https://www.unescwa.org)

¹³⁰ لجنة بازل للرقابة المصرفية هي لجنة استشارية فنية ال تستند إلى أية اتفاقية دولية، ولكنها استطاعت أن تساهم بقدر كبير في إعطاء إطار دولي للرقابة المصرفية وإيجاد فكر مشترك بين البنوك المركزية في دول العالم المختلفة، يقوم على التنسيق بين مختلف السلطات الرقابية والتفكير في إيجاد آليات لمواجهة المخاطر التي تتعرض لها البنوك، بوراس أحمد، عياش زبير، المعايير الدولية للرقابة المصرفية وتطبيقاتها على الأنظمة المصرفية للدول النامية، مجلة العلوم الإنسانية، الجزائر، العدد 27، 2007م ص 164.

¹³¹ عمار عريس، مجوب بحوصي، تعديلات مقررات لجنة بازل وتحقيق الإستقرار المصرفي، مجلة البشائر الاقتصادية، المجلد الثالث، العدد 1، 2017م، ص100.

¹³² زعباب سهام، المرجع السابق، ص28.

¹³³ غريب جبر جبر، تهديدات الأمن السيبراني للمصارف الإلكترونية وآلية مواجهاتها، المجلة الأكاديمية للعلوم الاجتماعية، الجزائر، المجلد 1 العدد 1، 2023م، ص61.

1- **عدم التأمين الكافي المنظم:** إذ يتم اختراق حسابات البنك بغرض الحصول على معلومات حساسة خاصة بالعملاء أو بالبنك، واستغلالها في أهداف غير مشروعة.

2- **عدم الصيانة أو عدم ملاءمة تصميم النظم:** ويحدث عند إخفاق الأنظمة في تلبية متطلبات العملاء من ناحية الكفاءة، أو عدم قيام الجهة المعنية بأداء الصيانة الضرورية بسرعة تخدم سدّ الثغرات التي يستهدفها المقرصن الإلكتروني.

3- **إساءة الاستخدام من قبل العملاء:** وذلك يحدث نتيجة لضعف الوعي لدى العملاء أو عدم إحاطتهم بالتدابير الوقائية، مثل أن يقوم العميل بالدخول إلى برنامج غير محمي أو غير موثوق، ومشاركة رقم بطاقته أو السماح للغير بالحصول على معلوماته الشخصية.

ومن ثم إدارة هذه المخاطر وفق إطار عمل مناسب واتخاذ الإجراءات الوقائية اللازمة يحد من حدوثها أو التصدي لها، لذلك يجب على البنوك الاهتمام بهذا النوع من المخاطر، لما له من أثر كبير على العمليات المصرفية الإلكترونية، والعمل على إعداد الخطط والممارسات المناسبة لضمان الاستجابة للهجمات الإلكترونية التي تتعرض لها الأنظمة أثناء ممارسة العمليات المصرفية الإلكترونية.

ثانياً: مخاطر السمعة:

لا شك أن المؤسسات المصرفية تؤسس أعمالها وتسعى دائماً إلى تطويرها من أجل كسب ثقة عملائها وجذب عملاء جدد، ويحدث ذلك من خلال بناء سمعة جيدة نتيجة للقدرة والكفاءة التي يتمتع بها المصرف على التصدي للمخاطر بشتى أنواعها، وفي الجانب الآخر فإن المصرف قد يتضرر من سوء الأنظمة المستخدمة، وعدم أمان الشبكة التي تشكل دعماً لإتمام العمليات المصرفية الإلكترونية في البنك¹³⁴، مما يجعل معلومات وثقة العملاء فريسة سهلة للقراصنة، وبالتالي إحجام العملاء عن التعامل معه، وبالتالي تأثر القيمة السوقية للبنك واستقراره¹³⁵.

ثالثاً: المخاطر القانونية:¹³⁶

وتقع هذه المخاطر عندما يتعلق الأمر بعدم احترام الأنظمة القانونية والتشريعات المنظمة للعمليات المصرفية، خصوصاً عند عدم وضوح الحقوق والواجبات المرتبطة بممارسة العمليات المصرفية الإلكترونية، ومن أهم هذه التحديات المتعلقة بطبيعة العمليات المصرفية الإلكترونية في كل بلد والقوانين الواجبة التطبيق، حجية التوقيعات الإلكترونية وأنظمة الدفع، غسيل الأموال وغيرها.

¹³⁴ سعيد عبالله الحامز، المرجع السابق، ص 2400.

¹³⁵ حنان بوعكوش، المرجع السابق، ص 22.

¹³⁶ مروة فتحي السيد، اقتصاديات الأمن السيبراني، مجلة البحوث القانونية والاقتصادية، مصر، العدد 76، 2021م، ص 1479.

المخاطر التي تتعرض لها العمليات المصرفية الإلكترونية تتطور وتزداد أو تنقص وفقاً للمعطيات والأسباب التي تسهل من حدوث هذه المخاطر لدى كل مؤسسة على حدة، والملاحظ أن ثقة العملاء هي المعيار الأساسي الذي يجب على البنوك وضعه في عين الاعتبار واتخاذ جميع الإجراءات والاحتياطات التي من شأنها الحد من هذه المخاطر أو التحكم بها، مثل المراقبة المستمرة والصيانة الدورية وتعزيز الوعي القانوني والتقني لدى موظفي البنك وعملائه، لإنشاء جدارٍ حاميٍّ ضد الهجمات الإلكترونية.

المطلب الثاني

دور الأمن السيبراني في القطاع المصرفي

أصبحت دراسة الأمن السيبراني ضرورة في التطور التكنولوجي في العالم، حيث إنها تنص على التهديدات التي تشكلها التطورات الرقمية، إذ يهدف الأمن السيبراني إلى حماية البيانات والشبكات والأنظمة الإلكترونية من الانتهاكات التي قد تعرض استقرارها للخطر¹³⁷. يعد تهديد الأمن السيبراني المصرفي أحد أنواع الإرهاب المالي¹³⁸، مع العلم أن كلمة إرهاب تشتمل مفهوماً واسعاً وقد تفتح آفاقاً ومعايير شديدة الخطورة، إلا إنه يمكن بالفعل اعتبار الخطر الذي يطال الخدمات المصرفية الإلكترونية إرهاباً، خصوصاً إنه بالإمكان الوصول إلى بيانات ومعلومات حساسة وسرقة أموال وجرائم ابتزاز وغيرها.

ولبيان دور الأمن السيبراني في القطاع المصرفي، سنتطرق في الفرع الأول إلى أهمية الأمن السيبراني في الحفاظ على سلامة العمليات المصرفية الإلكترونية، ومن ثم الجهود الدولية المتبعة في الحد من مخاطر الهجمات الإلكترونية على القطاع المالي¹³⁹. وعليه سنتناول هذا المطلب من خلال الفرعين التاليين:

- الفرع الأول: أهمية الأمن السيبراني في القطاع المصرفي.
- الفرع الثاني: الجهود الدولية المتبعة للحد من المخاطر السيبرانية على القطاع المصرفي.

¹³⁷ محمد الكويتي، حالة الأمن السيبراني بالقطاع المصرفي، مركز الإمارات للدراسات والبحوث الاستراتيجية، مقال

<https://mufakirualemarat.ecssr.ae/publications/edaat/detail/603>

¹³⁸ Diptiben Ghelani, Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking.

American Journal of Computer Science and Technology. Vol. x, 2022, page 1.

¹³⁹ قامت العديد من الدول بإنشاء هيئات ومراكز لضمان الأمن السيبراني، فنرى على الصعيد العربي قامت مملكة البحرين بإنشاء المركز الوطني للأمن السيبراني في العام 2020م، حيث بينت الدراسات التابعة له باعتبار الخدمات المالية من أهم القطاعات الحيوية التي يترتب على انتهاكها تحقق آثار اقتصادية واجتماعية واسعة النطاق، كما واكبت جمهورية مصر العربية الجهود في الحفاظ على الأمن السيبراني، وأنشأت أول مركز قطاعي في الدولة للاستجابة لطوارئ الحاسب الآلي للقطاع المالي في 2009م، إذ يسهم هذا المركز بإصدار الإنذارات المبكرة لدى البنوك لتواجه بها التهديدات الإلكترونية بالتعاون مع البنك المركزي المصري، إنشاء مركز متخصص ومتكامل للأمن السيبراني ليصبح أول المراكز القطاعية من نوعها في مصر، مجلة اتحاد المصارف العربية، العدد 491، 2021م.

الفرع الأول

أهمية الأمن السيبراني في القطاع المصرفي

خاض القطاع المصرفي تطوراً هائلاً فيما يتعلق بتوظيف التكنولوجيا في إطار الخدمات الإلكترونية التي يقدمها، ومن أجل المساهمة والبقاء في الأسواق العالمية، كان لزاماً على البنوك تطوير العمليات والخدمات المصرفية الإلكترونية، إذ ترمي أهداف شركات التكنولوجيا والبنوك إلى توفير بيئة مالية مناسبة لمواجهة الظروف والتحديات العالمية، وأن كان هذا التحول آتٍ لا محالة، إلا أنه كان على وتيرة متفاوتة بين بطيئة إلى متوسطة السرعة في الدول بشكل عام، وتجدر الإشارة إلى أن حدوث جائحة كوفيد-19 تعتبر من أهم الأسباب التي أدت إلى طفرة وتحول رقمي سريع نظراً للظروف التي واجهت المجالين التكنولوجي والمصرفي، والتي جعلت جميع القطاعات ملزمة بالتحول الإلكتروني المفاجئ، وبالتالي اتخاذ إجراءات وتدابير غير مسبقة¹⁴⁰.

توالت التهديدات السيبرانية على مهاجمة القطاع المصرفي من خلال استخدام وسائل إلكترونية، أو ثغرات في الأنظمة المستعملة في البنوك، وكان من أهم السرقات في تاريخ البنوك حادثة نيويورك في عام 2013م، حيث عبرت عنها الأخبار في ذلك الوقت بـ "بدلاً من الأسلحة والأقنعة استعانت منظمة إجرامية باللابتوب والإنترنت لسرقة ملايين الدولارات في ساعاتٍ محدودة"¹⁴¹ تتلخص هذه الحادثة بأنه تمت سرقة أكثر من 45 مليون دولار خلال ساعاتٍ معدودة من خلال آلات الصراف الآلي، وباستخدام بيانات بطاقات مصرفية مسروقة من بعض البنوك في دول الخليج العربي والهند، حيث تم اختراق أجهزة الصراف الآلي، واستخدمت فيها بطاقات ائتمان تابعة لشركة ماستر كارد¹⁴². بهذه الطريقة ينتشر أثر السرقة في العمليات المصرفية الإلكترونية، حيث لا حدود للجغرافيا في عالم اليوم المترابط رقمياً.

كما نما دور الأمن السيبراني في القطاع المصرفي بشكل كبير وأصبح عاملاً حاسماً في الحفاظ على استقرار العمليات المالية ومصادقيتها ونزاهتها، نظراً لأن المؤسسات المالية تعتمد بشكل متزايد على التكنولوجيا في أنشطتها اليومية، فضلاً عن دخول الأموال الإلكترونية وضرورة موثوقية وأمان تحرك الأموال، فإن فعالية تدابير الأمن السيبراني تؤثر بشكل مباشر على قدرتها

¹⁴⁰ تيم مورر وآرثر نيلسون، التهديد السيبراني العالمي، مجلة التمويل والتنمية، عدد مارس، 2021م، ص 25. [التهديد السيبراني العالمي](#)

(imf.org)

¹⁴¹ Marc Santora, in housemen thieves took \$45 million in the A.T.M. Scheme, the new York times , article.

¹⁴² عبدالقادر ورسمه غالب، الهجمات الإلكترونية على الشركات والبنوك، مجلة اتحاد المصارف العربية، لبنان، العدد 399، 2014م.

[الهجمات الإلكترونية على الشركات والبنوك \(uabonline.org\) - Union of Arab Banks](#)

على تقديم خدماتٍ آمنةٍ وموثوقةٍ للعملاء¹⁴³. نجد أن بعض البنوك المركزية كالبنك المركزي الأردني في نص المادة 6 أب من التعليمات الصادرة عنه ألزم البنوك بتوعية عملائها بالطبيعة التي تحوزها العمليات المصرفية المبرمة بوسائل إلكترونية، وبيان مخاطرها وما يترتب عليها من التزامات¹⁴⁴، في حين أن المشرع البحريني قد أشار إلى حماية عملاء المؤسسات المالية كأحد أهداف المصرف المركزي في المادة الثالثة والرابعة من قانون مصرف البحرين المركزي¹⁴⁵ وبالتالي فإنه ألزم المصرف المركزي ككيان دون المؤسسات المالية الأخرى الخاضعة لرقابته ولم نجد في التشريع البحريني ما يلزم المصارف بتوعية العملاء كما هو معمول في الأردن، لذلك نرى أنه من الأفضل أن يلزم المشرع البحريني المصارف بنشر التوعية كأحد سبل تعزيز التعاون في خلق بيئة مصرفية إلكترونية آمنة، إذ يسهم الوعي الإلكتروني في الحد من الخسائر الناجمة عن الانتهاكات التي قد تطال العمليات المصرفية الإلكترونية.

حيث أن التركيز على حماية العمليات المصرفية الإلكترونية من خلال تعزيز الوعي السيبراني يشكل عاملاً مهماً يعود بالنفع على أطراف العملية الإلكترونية، يمكن أن نجل أهمية الحفاظ على الأمن السيبراني في القطاع المصرفي من خلال عرض المزايا التي تبرز عندما يباشر البنك العمليات المصرفية الإلكترونية ضمن بيئة تحظى بمستوى عالٍ من الأمن في البيئة السيبرانية:

1- ضمان ثقة العملاء:

يلعب الأمن السيبراني دوراً محورياً في الحفاظ على ثقة العملاء داخل القطاع المصرفي، حيث يعهد الأفراد والشركات إلى البنوك بمعلوماتهم المالية الحساسة، ويتوقعون أن تظل بياناتهم سريةً ومحميةً، ويمكن أن يؤدي أي خرق لهذه الثقة إلى استياء العملاء، وفقدان العملاء، والإضرار بسمعة المؤسسة المالية، لذلك يعد ضمان أمان وخصوصية بيانات العميل أمراً بالغ الأهمية¹⁴⁶.

2 - منع الخسائر المالية:

المؤسسات المالية تتعامل مع كمياتٍ كبيرةٍ من المعاملات والأصول النقدية، ويمكن أن تؤدي الهجمات الإلكترونية إلى خسائر ماليةٍ مباشرةٍ من خلال السرقة أو المعاملات الاحتيالية أو

¹⁴³ منى الأشقر، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، لبنان، 2016م، ص 30.

¹⁴⁴ محمود محمد أبو فورة، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2012م، ص 34.

¹⁴⁵ المادة 4، 3، قانون رقم 64 لسنة 2006 بإصدار قانون مصرف البحرين المركزي والمؤسسات المالية، المرجع السابق.

¹⁴⁶ مصطفى إبراهيم سلمان الشمري، "الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، جامعة ديالى، العراق، مقال، المجلد العاشر، العدد 1، 2021م، ص 158.

حتى طلبات الفدية¹⁴⁷. بالإضافة إلى ذلك، يمكن أن تكون التكاليف المرتبطة بالتعافي من حادث إلكتروني مثل الإصلاح والإجراءات القانونية والغرامات التنظيمية كبيرة. حيث تساعد إجراءات الأمن الإلكتروني الفعالة في منع هذه الخسائر المالية، وتقليل تأثير الحوادث السيبرانية.

3- استقرار النظام المالي:

يعد الأمن السيبراني أمراً ضرورياً للحفاظ على استقرار ومرونة النظام المالي، ويحدث الاستقرار من خلال منع الحوادث السيبرانية من التسبب في فوضى واسعة النطاق، لذا التعاون الدولي مطلوب من أجل اتخاذ إجراءات وتدابير تحد من المخاطر السيبرانية على القطاعات بشكل كبير ومن بينهم القطاع المالي، بحيث إن الترابط بين الأنظمة المالية أمر لا بد منه، فتهجؤ إلكتروني على مؤسسة واحدة يمكن أن يعطل النظام البيئي المالي بأكمله، مما يسهم في حدوث اضطرابات تطل المركز المالي للمصارف والعملاء، يؤدي إلى خلق الذعر على المستوى المحلي، وفقدان ثقة المستثمرين الأجانب على المستوى العالمي، وصولاً إلى التأثير على الاقتصاد¹⁴⁸.

الفرع الثاني

الجهود الدولية المتبعة للحد من المخاطر السيبرانية على القطاع المصرفي

كان القطاع المصرفي ولا زال حتى اليوم، من أبرز القطاعات التي تتال أهمية كبيرة من قبل الحكومات، إيماناً بأهمية نمو القطاع المالي والمصرفي في تعزيز التنمية الاقتصادية والاجتماعية والسياسية، ويشهد القطاع المصرفي تنافساً بين البنوك المحلية والدولية، إذ تسعى البنوك للانتشار والاستقرار وتحقيق الأرباح، وقد أصبحت تقنية المعلومات أحد أهم العوامل المؤثرة في الأنشطة التي تمارس من قبل المصارف بل شكلت عاملاً مسانداً لتعزيز العمليات المصرفية الإلكترونية منذ القرن الماضي ومازالت مستمرة¹⁴⁹.

لذلك كان لزاماً على الدول أن تسعى من أجل توفير بيئة مالية مستقرة في ظل التحديات السيبرانية التي تواجهها، وعليه فسيبين الباحث فيما بعد الآليات المتبعة للحد من التهديدات السيبرانية في القطاع المصرفي، وعرض التطبيقات العملية التي تعرضت لها البنوك إثر الهجمات الإلكترونية على النحو الآتي:

¹⁴⁷ بلعل بنت نبي ياسمين، عمروش الحسين، التهديدات الإلكترونية والأمن السيبراني في الوطن العربي، مجلة نوميروس الأكاديمية،

المجلد الثاني، العدد الثاني، 2021م، ص171.

¹⁴⁸ تيم مورر وأرثر نيلسون، المرجع السابق، ص26.

¹⁴⁹ ناظم محمد الشمري، د. عبدالفتاح زهير العبدلات، المرجع السابق، ص24-25.

أولاً: من حيث التعاون الدولي:

تعتبر الجهود الدولية لتعزيز الأمن السيبراني في القطاع المصرفي أمراً مهماً جداً في ظل التحديات المتزايدة التي تواجهها البنوك والمؤسسات المالية، إذ تتضافر جهود المنظمات الدولية من أجل تطوير إطارات ومعايير لضمان الأمن السيبراني في هذا القطاع من خلال عقد اتفاقيات دولية ذات الصلة بالعمليات المصرفية الإلكترونية، ومن أهم هذه الاتفاقيات "اتفاقية بودابست لمكافحة الجرائم السيبرانية الصادرة عن مجلس أوروبا في عام 2001م¹⁵⁰، والتشريعين الأوروبيين لحماية البيانات والخصوصية الصادرين في عامي 1995 و2002م، وقانون الأونسيتال النموذجي الصادر في عام 1996م، وقانون الأونسيتال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع الصادر في عام 2001م¹⁵¹"، فضلاً عن مبادئ بازل التي تم إقرارها لأول مرة من قبل لجنة بازل في عام 1997م، إذ أسفرت هذه الاتفاقيات والمبادئ الدولية إلى رسم الخطوط العريضة لإرشاد الدول من أجل التصدي للخطر السيبراني في عديد من القطاعات، وكان من أهم النتائج التي أثمرتها الجهود الدولية هي سن التشريعات التي تعنى بالعمليات التي تتم ممارستها بواسطة وسيلة من وسائل تقنية المعلومات، والحث على وضع استراتيجية وطنية للأمن السيبراني، حيث يتم من خلالها الاستعداد والتأهب لمواجهة التهديدات السيبرانية والصمود ضدها، وعملت بعض الجهات المعنية وأصحاب المصلحة الوطنية على إعداد دليلٍ إرشاديٍّ لاستراتيجية وطنية للأمن السيبراني، وهم الاتحاد الدولي للاتصالات، والبنك الدولي، وأمانة الكومنولث، ومركز التميز التعاوني للدفاع السيبراني التابع لمنظمة حلف الشمال الأطلسي¹⁵²، بحيث توضع هذه الاستراتيجية بناءً على الدليل، لتسهيل عمل القيادات والدول للحفاظ على الأمن السيبراني، إذ تضع كل دولة استراتيجيتها بناءً على أهدافها وأولوياتها في إطار المبادئ الشاملة المذكورة فيه، على سبيل المثال الازدهار الاقتصادي والاجتماعي، الشمولية وحقوق الإنسان.

¹⁵⁰ تعد اتفاقية بودابست أول معاهدة دولية ملزمة نظمت جرائم تقنية المعلومات وجرائم الإنترنت حيث تم تطوير الاتفاقية في الفترة الزمنية بين 1997 إلى 2001 حيث انضمت 30 دولة في بادئ الأمر، إذ تضمنت هذه الاتفاقية موضوعات جرائم الإنترنت وضرورة اتخاذ التدابير التشريعية اللازمة من أجل توفير بيئة إنترنت ملائمة مع الطبيعة التي تحوزها الجرائم الإلكترونية كما تضمنت أحكاماً مختلفة تتعلق بالملكية الفكرية والإنتاج والنشر، وتحديد الجرائم التي تطل الشبكة المعلوماتية وبيان العقوبات على مرتكبيها، للمزيد انظر إلى، قطاف سليمان، بوقرين عبدالحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، الجزائر، المجلد السادس، العدد الأول، 2022م، ص 337-340.

¹⁵¹ اللجنة الاقتصادية والاجتماعية لغربي آسيا، المرجع السابق، ص 23.

¹⁵² الاتحاد الدولي للاتصالات والبنك الدولي وأمانة الكومنولث ومركز التميز التعاوني للدفاع السيبراني التابع لمنظمة حلف الشمال الأطلسي، دليل لوضع استراتيجية وطنية للأمن السيبراني "التزام استراتيجي للأمن السيبراني، ص 1.

ومن أهم محتويات هذه المبادئ ولا يعني أن الأخرى أقل أهمية، إلا أنه من وجهة نظر الباحث يستحسن التركيز على هاتين المسألتين، من منطلق فكرة التدابير الوقائية الاستباقية كمرحلة أولى، ومن ثم التدابير العلاجية كمرحلة ثانية لتحقيق أقل نسبة من الخسائر، وسببها الباحث بشكل موجز فيما يلي:

1- الحوكمة:

تتضمن الحوكمة إنشاء إطار عمل للسياسات والإجراءات وعمليات صنع القرار التي توجه جهود الأمن السيبراني للمنشآت، ويشمل تحديد الأدوار والمسؤوليات، ووضع خطوط اتصال واضحة، وضمان الإشراف التنفيذي على مبادرات الأمن السيبراني، ومن الضروري وجود استراتيجية أمنية للأمن السيبراني خاصة للمؤسسات المالية، ولكل مؤسسة أن تطور استراتيجيتها الخاصة لإدارة المخاطر الإلكترونية، على حسب طبيعة المشكلة والتحديات التي تواجهها¹⁵³، كما أن المفهوم الخاص المتعلق بالحوكمة لا يعني التدخل في عمل المؤسسات، إلا أنه يحدد الأطر التي يتوجب على المؤسسات اتباعها لضمان تحقيق أهداف الدولة في الحفاظ على أمان العمليات التي تنشأ من خلال وسائل إلكترونية، ولاشك أن في قياس المخاطر من ناحية تقييمها وتحديدتها تحت الإطارات المركزية الموحدة، من شأنه تطبيق معايير ذات فعالية تحقق استعمالاً أفضل لإدارة المخاطر، وخير برهان ما توصلت إليه البنوك البريطانية مقارنة بالبنوك الأمريكية، في أن الأولى قد أنفقت مبالغ أعلى للحفاظ على أمان الصرافات الآلية، إلا أن البنوك الأمريكية تتعامل بشكل أفضل يسمح لها بإدارة المخاطر فيما يتعلق بمسؤولية البنك عن الأضرار الناشئة، مالم يتم إثبات إهمال العميل، وذلك يوصلنا إلى أن إدارة المخاطر وفق سياسة مركزية تتبع فيها التداعيات والاحتمالات والعواقب، وكيفية إدارتها يساعد على الحد من الأضرار الناتجة عن حدوثها¹⁵⁴.

2- إدارة المخاطر:

تعد عملية إدارة المخاطر من أهم العمليات التي تتبعها المصارف من أجل الحفاظ على الاستقرار المالي للكيان المصرفي، ويدور مفهومها حول تحديد الإجراءات التي تتبعها المصارف من أجل الحد من حدوث المخاطر أو تجنبها، حيث عرّفت الجمعية الدولية حوكمة تكنولوجيا المعلومات على أنها "عملية تحديد نقاط الضعف والتهديدات لموارد المعلومات التي تستخدمها أي

¹⁵³ محمد الكويتي، قمة الحوكمة والمخاطر والامتثال 2023 تسلط الضوء على الحوكمة للمستقبل الرقمي للإمارات، صحيفة مباشر نيوز، مقال [قمة الحوكمة والمخاطر والامتثال 2023 تسلط الضوء على الحوكمة للمستقبل الرقمي للإمارات - صحيفة مباشر نيوز](https://mubasher.news/) (mubasher.news)

¹⁵⁴ van Eeten, M.J.G., de Bruijn, H., Kars, M., van der Voort, H. and van Till, J. 'The governance of cybersecurity: a framework for policy', Int. J. Critical Infrastructures, Vol. x, No. x, 2006, page 374.

جهة أو مؤسسة في تحقيق أهدافها وتحديد الإجراءات المضادة التي يجب اتخاذها للحد من المخاطر إلى مستوى مقبول، بناءً على قيمة موارد المعلومات للمؤسسة¹⁵⁵، يرى البعض أن مفهوم إدارة المخاطر يتحدد على حسب التمييز بين أنواع المخاطر من حيث طبيعتها، سواء كانت مالية أو غير مالية، فتصنيف مخاطر رأس المال على سبيل المثال تتعين بمخاطر الائتمان، مخاطر انخفاض السوق، ومخاطر التشغيل حيث يعد النوعين الأوليين من المخاطر المالية، أما الأخيرة فهي من المخاطر غير المالية¹⁵⁶.

تقوم البنوك بوضع السياسات اللازمة التي تمكنها من إدارة المخاطر الناتجة عن ممارسة العملية المصرفية الإلكترونية¹⁵⁷، بحيث تقوم بإجراءات الفحص والمراقبة من قبل البنوك بشكلٍ دوريٍّ تمكنهم من التقليل من حدوث الخطأ أو تداركه أو حتى تجنبه في أفضل الأحوال، فضلاً عن التدقيق¹⁵⁸، وتجدر الإشارة بأن إدارة المخاطر تقوم على أسسٍ ومعايير يتم فيها تقييم حجم الخطر الذي تعرض له البنك أو قد يتعرض له في المستقبل، مع دراسةٍ شاملةٍ لقدرة البنك في تحمل الأضرار الناتجة عنه، وكيف له أن يتحملها والصمود ضدها،¹⁵⁹ كما تشمل إعداد خططٍ للطوارئ، فضلاً عن الرقابة المستمرة وإجراء التأمين اللازم ومتابعة الخطر، وعليه فأنها تقوم على سلسلةٍ من المراحل تبدأ أولها في تحديد المخاطر، ومن ثم قياس المخاطر، مروراً نحو اتخاذ الإجراءات اللازمة إما للحد منها والقضاء عليها وفي النهاية أو رصدها ورصد القرارات السابقة وهكذا¹⁶⁰.

في الختام، يعد مبدأ الرقابة على المخاطر وإدارتها أولى المبادئ التي أقرتها لجنة بازل، والتي تلزم الإدارة العليا بالتأكد من إدماج نهج إدارة المخاطر المتعلقة بالعمليات المصرفية الإلكترونية في نهج الإدارة الشاملة للبنك، ليتأكد البنك من قدرته على تغطية المخاطر الجديدة الناشئة عن ممارسة الأنشطة المصرفية الإلكترونية¹⁶¹.

¹⁵⁵ معهد الدراسات المصرفية، مستقبل المخاطر في العصر الرقمي، معهد الدراسات المصرفية، الكويت، العدد 2، السلسلة 15، 2022م، ص4.

¹⁵⁶ زينب قاسم، عبدالرحمن رشوان، أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، المؤتمر العلمي الدولي الأول، جامعة عمان العربية، الأردن، 2022م، ص12.

¹⁵⁷ مروة فتحي السيد، المرجع السابق، ص1477.

¹⁵⁸ حنان بوعكوش، شادية زايدي، المرجع السابق، ص31.

¹⁵⁹ بن شريف مريم، الأعمال المصرفية الإلكترونية الرهانات والتحديات - إشكالية الإشراف والرقابة المصرفية، مجلة الاقتصاد الجديد، العدد 2، 2010م، ص160.

¹⁶⁰ الأكاديمية المالية، أساسيات إدارة المخاطر في الخدمات المالية، الأكاديمية المالية أساسيات إدارة المخاطر في الخدمات المالية، مكتبة الملك فهد الوطنية، المملكة العربية السعودية، 1442هـ، ص13.

¹⁶¹ Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, bis.org, July 2003, page9.

ثانياً: من حيث الإطار التشريعي:

المجال القانوني يلعب دوراً بارزاً في تحقيق الأمن بشكل عام، والتطور المستمر الذي يشهده العالم في دخول التكنولوجيا إلى ممارستنا اليومية في شتى القطاعات يحتم على الدول اتخاذ مواقف جدية وتشريعات تنظم هذه العمليات الإلكترونية، كما تنبغي الإشارة إلى أن القطاع المالي يعتبر أحد أهم جوانب اهتمام الدول، مما يدفعها لوضع تشريعات لضمان تنظيمه وتطويره ليتماشى مع التطور التكنولوجي المستمر، وقد أرسى هذا التطور في القطاع المالي العالمي بمرور الوقت مبادئ أساسية تهدف إلى الحفاظ على حماية البيانات المالية وتنظيم العمليات المصرفية الإلكترونية من خلال تحديد المتطلبات التقنية اللازمة وفرض العقوبات المناسبة، بالإضافة إلى وضع قواعد للتعاون الدولي وضمان سرية البيانات والخصوصية، وحيث من الثابت أن إرساء هذه القوانين الصارمة يعزز من الحماية الرقمية والثقة في النظام المالي الإلكتروني للدولة، مما يسهم في تعزيز النمو الاقتصادي والتكنولوجي في المجتمعات الحديثة¹⁶².

على صعيد القوانين المقارنة في البحث فسيبين الباحث جهود الدول في الحفاظ على الأمن السيبراني من خلال طرح القوانين ذات الصلة بالعمليات المصرفية الإلكترونية فيما يلي:

الإطار القانوني للتشريعات ذات الصلة بالعمليات المصرفية الإلكترونية: بالمقارنة بين المشرع البحريني، الإماراتي، المصري

1- المشرع البحريني: قانون رقم 54 لسنة 2018م بشأن الخطابات والمعاملات الإلكترونية:

أدرك المشرع البحريني أهمية العمليات الإلكترونية بشكل عام، والعمليات المصرفية الإلكترونية بشكل خاص، باعتبارها أحد العمليات الإلكترونية التي تستوجب الحماية في كافة المجالات، حيث تحتل مملكة البحرين مركزاً مالياً متقدماً في الشرق الأوسط، كما حازت مملكة البحرين على لقب العاصمة المالية لدول مجلس التعاون¹⁶³، لذلك كان على المشرع أن يواكب التقنيات التي تفرضها الأنشطة المصرفية الإلكترونية، وكان من أهم الخطوات التي اتخذها نحو هذا الاتجاه هو سن القانون البحريني رقم 54 لسنة 2018م، والمتعلق بالخطابات والمعاملات الإلكترونية، والذي ركز على العديد من المحاور التي تخدم القطاع المصرفي، مثل الاعتراف القانوني بالخطابات والوثائق والمعاملات الإلكترونية، كما اعترف بالتوقيعات الإلكترونية ومنحها الصلاحية القانونية كوسيلة لتوثيق المستندات والمعاملات الإلكترونية، وفي ذلك ضمان لمصادقية العمليات المصرفية الإلكترونية ولعدم الاتصال منها، كما أكد على أهمية ضمان سلامة وأمن

¹⁶² مروة فتحي السيد، المرجع السابق، ص1499.

¹⁶³ قطاع الخدمات المالية - مجلس التنمية الاقتصادية البحرين (bahrainedb.com).

البيانات والمعاملات الإلكترونية، مع الحاجة إلى حماية المعلومات المالية الحساسة ومنع الوصول غير المصرح به، ولم يغفل المشرع البحريني عن حماية حق المستهلك في المعاملات الإلكترونية، ووضع آليات لمعالجة النزاعات والأخطاء والأنشطة الاحتيالية، إذ تعد هذه الحماية ضرورية من أجل بناء ثقة العملاء في العمليات المصرفية الإلكترونية.

2- **المشرع الإماراتي:** القانون الاتحادي لدولة الإمارات العربية المتحدة رقم (34) لسنة 2021م في شأن مكافحة الشائعات والجرائم الإلكترونية¹⁶⁴ ومرسوم بقانون اتحادي رقم 46 لسنة 2021م بشأن المعاملات الإلكترونية وخدمات الثقة:

القانونان السابقان يمثلان إطاراً قانونياً شاملاً مصمماً لمواجهة الآثار السلبية للجرائم الإلكترونية وانتشار المعلومات الكاذبة عبر القنوات الرقمية، في عصر تعتبر فيه العمليات المصرفية الإلكترونية ضرورية للأنظمة المالية، إذ يلعب كل منهما دوراً حاسماً في ضمان سلامة وأمن المعاملات المالية التي تتم من خلال الوسائل الإلكترونية، إذ شمل المشرع الإماراتي تدابير الأمن السيبراني والتي تنال أهمية عالية، وتحتوي على تدابير تهدف إلى تحقيقه وحماية البنية التحتية الرقمية إذ تعد الأحكام والإجراءات ضرورية لحماية العمليات المصرفية الإلكترونية وبيانات العملاء، كما رفع قوة التوقيع الرقمي الذي يعزز من ثقة الأفراد والمؤسسات في العمليات الإلكترونية¹⁶⁵.

3- **المشرع المصري:** قانون رقم 175 لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات، القانون المصري لتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم (15) لسنة 2004م:

ينظم القانونان مسألة المعاملات الإلكترونية بشكل عام، ويبين كلاً من الضوابط والأحكام التي توجب تطبيقها عليها، إذ يواجه القانونان التحديات التي تفرضها استخدام تقنية المعلومات بما في ذلك التي تؤثر على العمليات المصرفية الإلكترونية، حيث تطرق إلى حماية البيانات والمعلومات المالية، كما عزز تدابير التعاون الدولي بشأن مكافحة جرائم تقنية المعلومات، وحماية البنية التحتية الرقمية، ومنع الهجمات الإلكترونية التي تقع على البنوك وأنظمة الدفع الإلكتروني.

من وجهة نظر الباحث يعد المشرع الإماراتي والمشرع المصري أكثر شمولاً وتحديثاً بخصوص تدابير الأمن السيبراني، مما يعزز من الحماية القانونية للعمليات المصرفية الإلكترونية في العديد من الأوجه، على عكس نظيرهما المشرع البحريني الذي لم يتطرق للتدابير السيبرانية

¹⁶⁴ القانون الاتحادي لدولة الإمارات العربية المتحدة رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، الإمارات العربية المتحدة، 2021م.

¹⁶⁵ مرسوم بقانون اتحادي رقم 46 لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة، الإمارات العربية المتحدة.

والإجراءات ذات الصلة بالعمليات المصرفية الإلكترونية بشكل تفصيلي، لذلك نرى إنه بالإمكان الاستفادة من القانون الإماراتي الذي وضع الخطوط العريضة التي تساعد في الحفاظ على أمن العمليات الإلكترونية في ظل التطور السيراني الذي نعيشه الآن في العالم، كما يتوجب على المشرع البحريني أن يبين التعاون الدولي وتنسيق الإجراءات التي من شأنها الحد من الهجمات الإلكترونية وتسهيل الوصول إلى مرتكبيها.

أهم التطبيقات التي قامت بها الدول العربية في إطار الحفاظ على الأمن السيراني هو إنشاء مراكز استجابة وطنية من شأنها الوصول إلى أهداف تخدم الأمن السيراني، على سبيل المثال لا الحصر التنبؤ بالهجمات الإلكترونية وتعزيز الوعي السيراني في المجتمع، وتعد هذه المراكز حديثة، وبدأ ظهورها أول مرة في الولايات المتحدة الأمريكية في جامعة كرنجي إذ ظهرت الديدان (worms) في إحدى شبكات شركة (IBM)، ونتيجة لذلك تنبّهت الولايات المتحدة الأمريكية لضرورة حماية شبكات الحاسوب والحفاظ على أمانها ودعمت إنشاء أول هذه المراكز في الجامعة وحثت إلى إنشاء مزيد من المراكز لأهداف مشابهة في الولايات الأخرى¹⁶⁶.

• الجمهورية التونسية

أما في الدول العربية كانت الجمهورية التونسية من الدول الرائدة في مجال حماية الفضاء السيراني، وتعد أول دولة عربية تنشئ هذا النوع من المراكز في عام 2003م¹⁶⁷. منذ نهاية العام 1999 أطلقت تونس العديد من القوانين المعنية بأمن وحماية تكنولوجيا المعلومات كقانون مكافحة الجرائم السيرانية، والقوانين ذات الصلة بالتوقيع الإلكتروني وحماية الخصوصية كما ألزمت المؤسسات الصغيرة والكبيرة على مراقبة أمن تكنولوجيا المعلومات وحمايتها بشكل دوري كما أوجبتها على إعلام مركز الاستجابة الوطني عن أي خطر تتعرض له الشبكات السيرانية ذات العلاقة بعملياتهم بحيث يقوم فريق المركز بالاستجابة لهذا الإنذار وإدارة الخطر ومعالجتها بالتعاون مع المؤسسة مع الحفاظ على السرية والخصوصية، كما وفرت خطأً ساخناً للتبليغ عن أي خطر أو هجمة إلكترونية على مدار أيام الأسبوع، وكان من أهم المبادرات التي عرضها مركز الاستجابة الوطني في تونس هو نظام (ساهر)، إذ تتمحور مهمة هذا النظام على توقع الأخطار المحيطة بشبكات الاتصال والبنية الأساسية للفضاء السيراني في تونس¹⁶⁸.

¹⁶⁶ اللجنة الاقتصادية والاجتماعية لغربي آسيا، المرجع السابق، ص26.

¹⁶⁷ المنتدى الإقليمي للاتحاد بشأن الأمن السيراني لإفريقيا والدول العربية، في تونس، تقرير منشور، 2009م، ص 8. [Meeting Report : ITU Regional Cybersecurity Forum for Africa and Arab States held in Tunis, Tunisia \(4-5 June 2009\)](#)

¹⁶⁸ اللجنة الاقتصادية والاجتماعية لغربي آسيا، المرجع السابق، ص27،28.

على الرغم من تقدم تونس وإنشائها مركز الاستجابة إلا إن مملكة البحرين كانت متأخرة نسبياً في إنشاء هذا المركز مع العلم من أهميته وقدرته على التصدي إلى العديد من الهجمات التي تتعرض لها المؤسسات قبل إنشاء المركز، إذ إنشأت مملكة البحرين المركز الوطني للأمن السيبراني استناداً للمرسوم بقانون رقم 65 لسنة 2020¹⁶⁹، إذ يوفر المركز حماية البنية التقنية على المستوى المحلي والحفاظ على فضاء إلكتروني آمن، ويقوم المركز بالعديد من المهام منها على سبيل المثال لا الحصر، وضع خطة استراتيجية للأمن السيبراني والرقابة على تنفيذها فضلاً عن نشر الوعي السيبراني وإدارة منصة وطنية موحدة من شأنها رصد وتحديد الهجمات السيبرانية في القطاعات الحيوية وإشعار الجهات المعنية بالمخاطر والتهديدات السيبرانية¹⁷⁰.

في الختام يوصي الباحث أن تكون هناك أداة قانونية تلزم المؤسسات الحكومية والخاصة بما يشمل المصرفية منها بضرورة إبلاغ المركز الوطني للأمن السيبراني عند حدوث أي هجوم إلكتروني، وعند ثبوت إهمال الجهة المتعرضة للخطر تتعرض لجزاءات إثر هذا الإهمال الذي قد يكبد القطاع المالي أضراراً من الصعب تداركها، وتشكل تهديداً لاستقرار القطاع المالي على المستوى المحلي أو المستوى العالمي.

¹⁶⁹ المادة 1 بند 18 رقم أولاً، مرسوم بقانون رقم 65 لسنة 2020 بتعديل بعض أحكام المرسوم رقم 69 لسنة 2004 بإعادة تنظيم وزارة الداخلية، الجريدة الرسمية، العدد 3494، مملكة البحرين.

¹⁷⁰ المركز الوطني للأمن السيبراني، مملكة البحرين، من نحن (ncsc.gov.bh)

المطلب الثالث

معوقات تعزيز الأمن السيبراني في القطاع المصرفي

أصبحت دراسة الأمن السيبراني أمراً مهماً لانعكاسات السيبرانية على القطاعات المختلفة في الحياة اليومية، ولكن هناك أيضاً جانبٌ مظلمٌ للتقدم الرقمي، حيث يمكن أن يشكل تهديداً للبلدان والمؤسسات كذلك، تعد دراسة الأمن السيبراني أمراً بالغ الأهمية لحماية البيانات والأنظمة الإلكترونية. ظهر مصطلح الأمن السيبراني كمفهومٍ أوسع يشمل حماية البلدان والمنازل من التهديدات، على غرار بناء جيشٍ قويٍ للدفاع، في هذا المطلب سوف يتم التعرف على أهم معوقات تعزيز الأمن السيبراني في القطاع المصرفي تحديداً¹⁷¹ من خلال الفروع الآتية فيما يلي:

- الفرع الأول: معوقات تعزيز الأمن السيبراني.
- الفرع الثاني: طرق لتعزيز الأمن السيبراني المصرفي.

¹⁷¹ مروة فتحي السيد، المرجع السابق، ص 1487.

الفرع الأول

معوقات تعزيز الأمن السيبراني المصرفي

تتطلب معالجة التحديات التي تفرضها التهديدات الإلكترونية وضمان الأمن السيبراني القوي في قطاع الخدمات المصرفية الإلكترونية فهماً شاملاً للعقبات التي تواجهها خصوصاً مع زيادة تدخل التكنولوجيا واستخدام الإنترنت فيها إذ تعجز أحياناً البنوك عن التعامل مع التهديدات السيبرانية نظراً لسرعة التطور في التقنيات المستخدمة، ويمكننا بيان هذه المعوقات على سبيل المثال لا التحديد باعتبار أن المجال السيبراني سريع التطور ومرن، يمكن أن تتخلله معوقاتٌ تتطور بتطور التقنيات التي تهدده وعليه، فيمكن إيجاز المعوقات التي تعرقل تعزيز الأمن السيبراني في القطاع المصرفي على النحو الآتي:

أولاً: عدم وجود استراتيجياتٍ شاملةٍ للأمن السيبراني:

في مجال العمليات المصرفية الإلكترونية، هناك عقبة أمام تعزيز الأمن السيبراني في جميع أنحاء العالم وهي الافتقار المستمر لاستراتيجيات الأمن السيبراني الشاملة داخل المؤسسات المالية، هذا النقص يجعل القطاع المصرفي عرضةً للتهديدات السيبرانية المتطورة ويعيق قدرته على التصدي بشكلٍ استباقيٍّ للهجمات المحتملة. حيث يتطور مشهد التهديدات الإلكترونية باستمرار، إذ يستخدم مجرمو الإنترنت تقنياتٍ متطورةٍ بشكلٍ متزايدٍ لاختراق أنظمة الأمن بدون استراتيجية شاملة تحقق الأمن السيبراني، فتكون البنوك غير مجهزة لمواجهة هذه التهديدات، مما يجعل عملياتها المصرفية الإلكترونية عرضةً للانتهاكات والوصول غير المصرح به¹⁷².

ثانياً: التدابير التفاعلية بدلاً من التدابير الاستباقية:

إن عدم وجود إستراتيجية واضحة المعالم للأمن السيبراني يحيل المؤسسات المالية إلى موقف رد الفعل، بدلاً من تنفيذ تدابير استباقية لمنع الحوادث الإلكترونية، قد تجد البنوك نفسها تستجيب للانتهاكات بعد وقوعها بالفعل، يمكن أن يؤدي هذا النهج التفاعلي إلى خسائر مالية أكبر وانعدام ثقة العملاء وإلحاق الضرر بالسمعة، يرى المختصون في الأمن السيبراني إمكانية الاستفادة من الذكاء الاصطناعي في تحديد التحركات المشتبهة والأنماط للخوارزميات التي تشكل اختلافاً

¹⁷² خورخي فلوريس كايخاس، وعائشة عفيفي، ونيكوالي لوزينسكي، الأمن السيبراني في مؤسسات منظومة الأمم المتحدة، تقرير منشور مترجم، 2021، ص 24. على الرابط التالي: (61) الأمن السيبراني: المفهوم والتداعيات في السياسة العالمية – Iman Alaa ElDeen |

Academia.edu

على النمط المعمول به في الأنظمة، مما يجعلها تطلق إنذاراً قبل حدوث الهجمة وبالتالي صدها في أسرع وقت¹⁷³.

ثالثاً: تخصيص الموارد غير الكافية:

تتطلب استراتيجيات الأمن السيبراني الشاملة موارد مخصصة، سواءً من حيث الموارد المالية أو الموظفين، قد يؤدي عدم وجود استراتيجية واضحة إلى تخصيص موارد غير كافية لجهود الأمن السيبراني، وبالتالي إضعاف قدرة البنك على مواجهة التهديدات بشكلٍ فعالٍ وتنفيذ التدابير الأمنية اللازمة¹⁷⁴.

رابعاً: قلة الوعي والتدريب:

لا تتضمن إستراتيجية الأمن السيبراني الشاملة الحلول التكنولوجية فحسب، بل تتضمن أيضاً زيادة الوعي وتدريب الموظفين للتعرف على التهديدات المحتملة والاستجابة لها بدون وجود إستراتيجية محددة، قد تتجاهل البنوك أهمية تثقيف الموظفين حول المخاطر الإلكترونية وتنفيذ بروتوكولات أمنية فعالة، خصوصاً كما تم ذكره سابقاً إن أحد المخاطر التي تواجه العمليات المصرفية الإلكترونية هي المخاطر التشغيلية، والتي تتضمن إساءة الاستعمال من قبل العملاء أو الموظف الراجع لقلة الوعي أو التدريب¹⁷⁵.

¹⁷³ الأمن السيبراني أساسي لتطوير قطاع التكنولوجيا المالية في البحرين، مقال منشور في جريدة الوطن، 8 يونيو-2023، على الرابط التالي: الأمن السيبراني أساسي لتطوير قطاع التكنولوجيا المالية في البحرين - صحيفة الوطن (alwatannews.net)

¹⁷⁴ تيم مورر وآرثر نيلسون، المرجع السابق، ص27.

¹⁷⁵ علم الدين بانقا، المرجع السابق، ص32.

الفرع الثاني

طرق لتعزيز الأمن السيبراني المصرفي

يعد تعزيز الأمن السيبراني في القطاع المصرفي أمرً حيويًا لحماية بيانات العملاء والمعاملات المالية وضمان استقرار النظام المصرفي، وتبعاً لما سبق بيانه في الفرع الأول بشأن المعوقات التي تواجه البنوك في تعزيز الأمن السيبراني، لابد من بيان الطرق التي تمكن البنك من التغلب على هذه المعوقات من خلال توضيح التدابير والإجراءات المتكاملة التي تتطلب جهوداً مستمرة وتحديثاتٍ دوريةً لمواكبة التطورات التكنولوجية والتهديدات الجديدة كلما أمكن، وهنا بعض الطرق المهمة لتعزيز الأمن السيبراني في القطاع المصرفي:

أولاً: الشراكة بين القطاع العام والقطاع الخاص:

يمكن القول بأن الحفاظ على الأمن السيبراني في القطاع المالي هدفٌ تسعى إليه المؤسسات المصرفية متمثلةً بالبنوك والحكومة بشتى دوائرها، ولتحقيق هذا الأمان لابد من التعاون بين هذين القطاعين للحد من الهجمات السيبرانية التي تتعرض لها الأنظمة، والتي تؤثر في تدهورها فضلاً عن التعاون الدولي والاستفادة من التجارب الإقليمية والدولية في المجال، مما يسهم في تحسين أمان القطاع والقدرة على التصدي للتهديدات السيبرانية، والحفاظ على سمعته في السوق المالي العالمي¹⁷⁶.

ثانياً: تعزيز البحث والابتكار في مجال الأمن السيبراني:

يعتبر الاستثمار في مجال البحث والابتكار وسيلة للحفاظ على الأمن السيبراني بشكل عام وأمن القطاع المصرفي السيبراني بشكل خاص، إذ يجب أن يتم تخصيص المزيد من الجهود والموارد لدعم البحث العلمي وتطوير التقنيات الحديثة في مجال الأمن السيبراني، من تعزيز البحث والابتكار فضلاً عن تحسين استجابة الأنظمة الأمنية¹⁷⁷.

ثالثاً: تطوير البنية التحتية "التقنية والبشرية":

من المهم جداً تحسين البنية التحتية التكنولوجية للمؤسسات المالية، بما في ذلك تحديث الأجهزة وتوفير أنظمة حماية متطورة، وتطبيق إجراءات أمان قوية، بالإضافة إلى ذلك يجب تدريب

¹⁷⁶ حنان بوعكوش، شادية زايدي، المرجع السابق، ص 11.

¹⁷⁷ الاتحاد الدولي للاتصالات والبنك الدولي وأمانه الكومنولث ومركز التميز التعاوني للدفاع السيبراني التابع لمنظمة حلف الشمال الأطلسي، المرجع السابق، ص 45.

وتأهيل العاملين في القطاع المصرفي على مهارات الأمن السيبراني، وذلك من خلال توفير برامج تدريبية وورش عمل متخصصة.¹⁷⁸

رابعاً: وضع استراتيجية لتعزيز الأمن السيبراني:

لاشك أن من أهم آليات تعزيز الأمن السيبراني هو وضع استراتيجية وطنية تحت الجهات المعرضة للمخاطر السيبرانية على اتخاذ التدابير التقنية والقانونية التي من شأنها رفع مستوى الأمان والتحصين الرقمي، حيث تحدد هذه الاستراتيجية الأولويات ورفع الوعي السيبراني وتبادل المعلومات والخبرات والتنسيق بين القطاعات من أجل مكافحة التهديدات السيبرانية¹⁷⁹.

خامساً: استخدام تقنيات مبتكرة كالذكاء الاصطناعي:

يشكل الذكاء الاصطناعي ثورة في العالم اليوم، إذ تعتمد العديد من المؤسسات على هذه التقنية من أجل ممارسة أعمالها، ويمكن الاستفادة منها في إطار أمن العمليات المصرفية الإلكترونية، وذلك من خلال تحليل المعلومات والبيانات لكشف التهديدات السيبرانية والتحذير منها، كما يمكن تحليل وتقييم الخطر الناتج وتقديم تقييمات تلقائية، وتحديد أولويات اتخاذ إجراءات مناسبة لمواجهة التهديدات¹⁸⁰.

تلخيصاً لما سبق ناقشته في هذا المبحث فإن الأمن السيبراني يلعب دوراً بارزاً في القطاع المصرفي، حيث ناقش الباحث التحديات التي تواجه جمهورية مصر ومملكة البحرين والإمارات العربية المتحدة في تحسين الأمن السيبراني في الخدمات المصرفية الإلكترونية، والمخاطر التي تواجهها البنوك وكيفية التغلب عليها، كما تم عرض أهم النماذج الناجحة في إنشاء مراكز وطنية للاستجابة لطوارئ الأمن السيبراني. يعتبر القطاع المصرفي عرضةً للتهديدات السيبرانية سريعة التطور، ومن المهم وجود استراتيجيات تقنية للأمن السيبراني لحماية العمليات وثقة العملاء. كما أن العوامل البشرية أحد أهم ركائز الحفاظ على أمن السيبرانية المصرفية إذ يجب تدريب الموظفين وتوعيتهم بالمخاطر السيبرانية، ولتقليل نقاط الضعف تقدم التطورات التكنولوجية في الخدمات المصرفية فرصاً ولكنها توفر أيضاً نقاط الضعف التي يستغلها مجرمو الإنترنت مما ينشأ تحديات تنظيمية في مواكبة التهديدات السيبرانية المتطورة، والتعاون الدولي أمر

¹⁷⁸ محمد تقروت، متطلبات تنشيط العمل المصرفي الإلكتروني في الدول العربية، مجلة الإقتصاد الجديد، العدد 7، 2012م، ص294.

¹⁷⁹ ميليسا هاثواي، المرجع السابق، ص5.

¹⁸⁰ محمد الكويتي، الأمن السيبراني في 2023: تحولات وتحديات عصر الذكاء الاصطناعي، تريندز للبحوث والاستشارات، مقال على

الرابط التالي:

ضروري لمكافحة الجريمة السيبرانية. في نهاية الأمر يعد تحقيق التوازن بين الأمان والابتكار أمراً مهماً لقطاع مصرفي مستدام عبر الإنترنت على الحكومات أن تسعى إلى تحقيقه كلما أمكن ذلك.

الفصل الثاني

طرق الحماية القانونية للعمليات المصرفية الإلكترونية وآثارها على الاقتصاد الوطني

تتضمن طرق الحماية القانونية للعمليات المصرفية الإلكترونية مجموعةً من القوانين والضوابط التي تهدف فيها إلى حماية أطراف المعاملات المصرفية المباشرين (البنك والعميل) وغير المباشرين (الدولة والمستثمرين)؛ حيث أن تطبيق قوانين الحماية الإلكترونية تؤدي إلى تعزيز الثقة في النظام المصرفي الإلكتروني، مما يسهم في تشجيع المزيد من الأفراد والشركات على استخدام هذه الخدمات المؤثرة على الاقتصاد الوطني والاستقرار المالي، وتحسين كفاءة العمليات المالية إلى جانب تقليل التكاليف الإدارية والمصرفية مما يؤثر بشكل إيجابي على الارتقاء بالنمو الاقتصادي ويعطي دفعةً للتنمية الوطنية¹⁸¹.

سيتم تقسيم هذا الفصل إلى مبحثين، حيث يتناول الباحث في المبحث الأول الآليات القانونية المتبعة لحماية العمليات المصرفية الإلكترونية، مروراً بدور الرقابة على المصارف أثناء ممارسة العمليات المصرفية الإلكترونية وجوانب الحفاظ على سرية البيانات وسط التطور التكنولوجي الحاصل، كما سيتطرق إلى طبيعة مسئولية المصارف أثناء ممارسة العمليات المصرفية الإلكترونية، أما في المبحث الثاني سيبين أثر حماية العمليات المصرفية الإلكترونية على المجالات المختلفة، مع تسليط الضوء على أثرها في زيادة نمو الاقتصاد الوطني وجذب الاستثمارات الأجنبية وذلك فيما يلي.

¹⁸¹ اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية، نيويورك، الأمم المتحدة، العدد 18، 2012م، ص7.

المبحث الأول

الآليات القانونية المتبعة لحماية العمليات المصرفية الإلكترونية

لطبيعة شبكات الإنترنت التي تتم من خلالها العمليات المصرفية الإلكترونية، تحتم على الجهات ذات الصلة اتخاذ إجراءات وتدابير مستحدثة للحفاظ على أمنها وموثوقيتها، لذلك تم سن تشريعات تتلائم مع الطبيعة الإلكترونية التي تتسم بها،¹⁸² حيث ركزت على إسباغ الحماية والرقابة على العمليات المصرفية الإلكترونية، بالإضافة إلى الحفاظ على سرية البيانات إثر الممارسة الإلكترونية.

في طور الحفاظ على الأمان والسرية، نشأت التزامات وحقوق ترتب على أثرها مسؤولية قانونية على أطراف العمليات المصرفية الإلكترونية، لذلك في هذا السياق سيتم تقسيم هذا المبحث إلى ثلاثة مطالبات، نتناول فيها آليات الحماية ومراحل الرقابة، ومن ثم سيبين أثر حق الخصوصية والتعارض الذي قد ينشأ مع طبيعة العمليات المصرفية الإلكترونية، وختاماً المسؤولية القانونية المترتبة على المصارف أثناء ممارسة العمليات المصرفية الإلكترونية.

¹⁸² رهان لطيفي، البنوك الإلكترونية، المجلة الإلكترونية للأبحاث القانونية، العدد 8، 2021م، ص81.

المطلب الأول

الرقابة على العمليات المصرفية الإلكترونية وآليات الحماية المتبعة

تلعب البنوك دوراً حاسماً في اقتصاد أي بلد، فهي بمثابة القوة الأساسية والدافع لها، وتلعب دوراً مهماً في المدخرات المالية وتوفير التمويل للاقتصاد، ويجب على القطاع المصرفي أن يتكيف ويتطور ليواكب متطلبات الأفراد للخدمات المصرفية المختلفة كما يعد الإشراف المصرفي ضرورياً لحماية النظام المصرفي من المخاطر وضمان ثقة المستثمرين، وهذا يتطلب وضع قوانين وأنظمة وتعليمات مصرفية، بما في ذلك إطاراً للرقابة المصرفية¹⁸³.

في الآونة الأخيرة، توسعت الرقابة إلى ما هو أبعد من دورها التقليدي في الإشراف على المؤسسات المالية. ويشمل الآن أيضاً تدخل الجهات الحكومية لضمان شرعية المعاملات المالية والكشف عن أي انتهاكات للوائح المالية وخلق بيئة لضمان حماية حقوق المودعين والمستثمرين ودعم تنفيذ سياسات نقدية فعالة وبيئة تشريعية،¹⁸⁴ مما تؤدي إلى استقرار واستمرارية البنوك في السوق، ويساعد على تجنب المخاطر المحتملة مع الحفاظ على مستوى عالٍ من الأداء والسلامة العامة للنظام المصرفي¹⁸⁵ لذلك سيتم تقسيم هذا المطلب إلى فرعين على النحو الآتي:

- الفرع الأول: مفهوم الرقابة على العمليات المصرفية الإلكترونية
- الفرع الثاني: أنواع الرقابة على العمليات المصرفية الإلكترونية

¹⁸³ عثمان خالدي، دور الرقابة المصرفية الداخلية والخارجية في تحسين الأداء داخل البنوك التجارية (دراسة حالة عينة من البنوك التجارية)، رسالة الماجستير، جامعة المسيلة، الجزائر، 2014\2015م، ص 2.

¹⁸⁴ سهام سوادى طعمه، الرقابة الداخلية للمصارف على العمليات المصرفية الإلكترونية، المؤتمر العلمي الدولي الأول، تحت عنوان "العلوم الإنسانية والصرفة رؤية نحو التربية والتعليم المعاصر، جامعة دهوك، العراق، 2019م، ص 53.

¹⁸⁵ ماجدة احمد شلبي، الرقابة المصرفية في ظل التحولات الاقتصادية العالمية، المكتبة القانونية العربية، المغرب، ص 2.

(bibliotdroit.com).

الفرع الأول

مفهوم الرقابة على العمليات المصرفية الإلكترونية

تشكل الرقابة على العمليات المصرفية الإلكترونية تحدياً على الجهات الرقابية والإشرافية، كون أن الطبيعة التي تتسم بها العمليات المصرفية الإلكترونية تختلف عن طبيعة العمليات المصرفية التقليدية، حيث تحاول هذه الجهات الحد من المخاطر الناتجة عن ممارسة العمليات المصرفية عن طريق إحدى وسائل تقنية المعلومات، وفي هذا الإطار تقوم الجهات الرقابية على المؤسسة المصرفية بوضع السياسات، وإنشاء الإطار القانوني والتنظيمي اللازم من أجل ممارسة مصرفية آمنة تتفق مع المعايير الأمنية المطلوبة دون زعزعة الاستقرار المالي¹⁸⁶.

أولاً: تعريف الرقابة على العمليات المصرفية الإلكترونية:

عرف البعض الرقابة المصرفية بأنها: "عملية إدارية تهدف بالدرجة الأولى إلى التأكد من أن العمليات التي تقوم بها البنوك والمؤسسات المالية، تحترم الأحكام التشريعية والتنظيمية السارية المفعول، القواعد المحاسبية والوقائية، والتحقق من أن العمليات التي تقوم بها البنوك تحترم القواعد والمعايير المحددة، إضافة إلى التعرف على مواطن الخطأ والإهمال لتصحيحها"¹⁸⁷. كما عرفها آخرون وفقاً للجهة المسؤولة عن الرقابة على البنوك بأنها: "مجموعة من الوسائل والإجراءات التي تتفرد السلطات النقدية والمالية وبشكل خاص البنك المركزي بممارستها، بهدف تجنب المصارف مغبة الانزلاق في مخاطر ائتمانية أو تصرفات تأتي بنتائج سلبية على النشاط الاقتصادي والتجاري، إضافة إلى هدف آخر يكمن في المحافظة على مصالح أصحاب الودائع من الجمهور والمؤسسات والدائنين الآخرين"¹⁸⁸. بالتعقيب على التعريفين آنفي الذكر فنجد التعريف الأول هو الأرجح لعدة أوجه:

الوجه الأول: من ناحية تحديد الجهة المسؤولة على الرقابة: أن مفهوم الرقابة المصرفية لابد أن يكون شاملاً دون تحديد جهة واحدة بحد ذاتها في الرقابة والتحقق من سلامة الإجراءات والأنظمة التي تمارسها المؤسسات المصرفية، وإن كان البنك المركزي هو رأس الهرم في الرقابة

¹⁸⁶ مروة فتحي السيد، المرجع السابق، ص 1491.

¹⁸⁷ لعماري وليد، بولحيس سامية، دور اللجنة المصرفية في الرقابة على العمليات المصرفية، مجلة الباحث للدراسات الأكاديمية، المجلد 5، العدد 3، 2018م، ص 412.

¹⁸⁸ نور الهدى عبدالكاظم راضي، أساليب الرقابة المصرفية، مجلة بحوث الشرق الأوسط، جامعة عين شمس، مركز بحوث الشرق الأوسط والدراسات المستقبلية، مصر، العدد 52، 2019م، ص 421.

على القطاع المالي بشكل عام، إلا أن هذا لا يعني أن المؤسسة نفسها لا تقوم بالرقابة على السياسات والإجراءات المتخذة أثناء ممارسة العمل المصرفي.

الوجه الثاني: من ناحية الرقابة الشاملة: تضمن مفهوم الرقابة جميع المعايير التي من شأنها الحفاظ على سلامة الإجراءات سواء كانت احترام القوانين والإجراءات والتدابير التقنية المحاسبية والوقائية، دون تحديد خطر معين مثل ما تم ذكره في التعريف الثاني (بالمخاطر الائتمانية).

الوجه الثالث: من ناحية التركيز على الرقابة الوقائية: يجب أن يبين التعريف مدى أهمية الرقابة الوقائية للتعرف على مواطن الخطأ لتجنب المخاطر الناتجة عنها واتخاذ مايلزم من تدابير، وهذا ما يبينه التعريف الأول وغفل عنه التعريف الثاني.

ثانياً: أنواع الرقابة على العمليات المصرفية الإلكترونية:

لاشك أن الرقابة على الأعمال التي تقوم بها المصارف مهمة للحفاظ على الاستقرار المالي للمصرف وحماية العملاء من التهديدات، لذلك تلعب الرقابة دوراً حيوياً لضمان أمن وسلامة المعاملات المالية سواء كانت إلكترونية أو تقليدية، ويختلف الفقه في تحديد أنواع الرقابة، فمنهم من قسمها على حسب الجهة المنوط بالإشراف والرقابة، ومنهم من قسمها على حسب توقيتها، وآخرون على حسب المعايير والأهداف وسيبين الباحث هذه الأنواع فيما يلي:

1- الرقابة على حسب الجهة المنوط بها الإشراف:

أ- **الرقابة الداخلية:** يقصد بمفهوم الرقابة الداخلية للعمليات المصرفية، الخطة التنظيمية التي تضعها المؤسسة المصرفية (البنك) من أجل حماية الأصول والتحقق من مصداقية البيانات والمعلومات الحسابية المذكورة في التقارير الدورية¹⁸⁹، وقد تتناسب الرقابة الداخلية من بنك إلى آخر وفقاً للأهداف التي يصبو إلى تحقيقها، ولكن عادة ما يكون جهاز الرقابة الداخلي للبنك يهدف من خلال إشرافه على العمليات الممارسة بالتأكد من أنها لا تخالف اللوائح والقوانين التي وضعتها الأجهزة الرقابية العليا كالبنك المركزي، كما يعنى الجهاز الرقابي بالتأكد من احترام البنك للضوابط والإجراءات المنصوص عليها لتقييم المخاطر، والحفاظ على أمن المعلومات والمستندات والوثائق الخاصة بالعمليات المصرفية الممارسة من قبله¹⁹⁰.

¹⁸⁹ جلايلة عبد الجليل، آليات تفعيل الرقابة المصرفية على الصيرفة الإلكترونية دراسة حالة الجزائر، أطروحة دكتوراه، جامعة أحمد دراية أدرار، الجزائر، 2018\2019م، ص36.

¹⁹⁰ شيخ محمد زكرياء، دور الرقابة الداخلية للبنوك في حماية العمليات المصرفية، مجلة حقوق الإنسان والحريات العامة، المجلد 7، العدد 1، 2022م، ص263، 262.

ب- **الرقابة الخارجية:** تعد الرقابة الخارجية هي الرقابة المكمل للرقابة الداخلية، وعادة ماتقوم بها أجهزة مستقلة يتم التعاقد معها من أجل التأكد من المعلومات الحسابية والإجرائية وفقاً للنتائج والتقارير التي حققها البنك، وكفاءة أدائه في الحفاظ على أمواله وتسيير أعماله¹⁹¹.

ج- **رقابة البنك المركزي:** إذ يخول القانون البنك المركزي بالرقابة على أعمال البنوك بشكل عام، للتأكد من مطابقتها الأحكام والقواعد المنصوص عليها في القوانين واللوائح التي حددها المشرع، لضمان استقرار القطاع المصرفي والحيلولة دون تعرضه لتهديدات تؤثر على القطاع المالي بشكل عام، بحيث يحق للبنك المركزي القيام بجولات تفتيشية على البنوك للتأكد من سلامة مستنداتها وإجراءاتها¹⁹².

2- الرقابة على حسب التوقيت:

أ- **الرقابة السابقة:** وتسمى بالرقابة الوقائية، ويقصد بها تلك الرقابة التي تمارسها الجهة الرقابية من أجل الحد من المخاطر التي تتعرض لها البنوك، واتخاذ اللازم من التدابير التي تُجنب الأنظمة من التعرض للتهديدات وقد يدخل من ضمنها التراخيص، سلامة الأداء، وكفاءة البرمجيات والنظم للتصدي للهجمات الإلكترونية والتحقق من مطابقة الإجراءات للقوانين واللوائح¹⁹³.

ب- **الرقابة أثناء التنفيذ:** وتعني بالرقابة التي يقوم البنك أثناء ممارسة العمليات المصرفية واكتشاف الأخطاء والتهديدات فور حدوثها، واتخاذ مايلزم من تدابير وإجراءات للحد من المخاطر الناتجة والعمل على القضاء عليها كلما أمكن ذلك لاحتواء الخسارة الناجمة¹⁹⁴.

ج- **الرقابة اللاحقة:** وتعني ممارسة الأجهزة الرقابية المراجعات وفحص المستندات والعمليات المصرفية التي تمت ممارستها خلال فترة معينة من الزمن، والتحقق من أنها قد لاقت النتائج والأهداف المرجوة، فضلاً عن سلامتها وموافاتها للأنظمة والتشريعات التي حددتها الجهة الرقابية¹⁹⁵.

¹⁹¹ العايب عصام، المرجع السابق، ص52.

¹⁹² جلاله عبد الجليل، المرجع السابق، ص37.

¹⁹³ مبارك بن الطيبي، الرقابة المصرفية على البنوك التجارية في التشريع الجزائري، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو/ الأغواط، العدد 5، 2020م، ص109.

¹⁹⁴ عامر العتوم، نجيب بوخرس، وآخرون، دور الهيئات الرقابية في إدارة مخاطر الخدمات المصرفية الإلكترونية في المصارف الإسلامية، المجلة الأردنية في الدراسات الإسلامية، الأردن، مجلد16، العدد3، 2020م، ص123.

¹⁹⁵ مبارك بن الطيبي، المرجع السابق، ص109.

3- الرقابة على حسب المعايير¹⁹⁶:

أ- الرقابة على أساس الإجراءات: يقوم هذا النوع من الرقابة على التحقق من أن جميع الإجراءات التي مارسها المصرف في إطار العمليات المصرفية المبرمة توافق القواعد والقوانين دون النظر إلى النتائج التي تم تحقيقها، أي أنها تراقب العملية الإجرائية وسلامتها دون النظر إلى النتيجة المحققة.

ب- الرقابة على أساس النتائج: تتمثل هذه الرقابة في التركيز على قياس النتائج الفعلية التي تحقّقها المنظمات المراقبة، بدون أخذ بالاعتبار مدى التزام المنظمة بالإجراءات المطلوبة لتحقيق تلك النتائج، وذلك بغض النظر عن الأهداف المحددة مسبقاً.

الفرع الثاني

أشكال الرقابة على العمليات المصرفية الإلكترونية

يحوز القطاع المصرفي أهمية كبيرة في العديد من الجوانب، إذ يؤثر بشكل كبير على الاقتصاد العام المحلي والدولي، وعادةً ما تسعى الدولة إلى فرض الرقابة على العمليات المصرفية بشكلها (إلكتروني، تقليدي) للحفاظ على أمانها واستقرار القطاع المالي، بحيث تكون هذه الرقابة تحقق غاية البنوك في الربح وأيضاً غاية الدول في الاستقرار المالي، الذي بدوره يجذب الاستثمارات المحلية والأجنبية دون المساس أو التعدي على حقوق العملاء، لذلك سنبين فيما يلي مراحل وأوجه الرقابة التي تضعها الجهات المعنية لضمان سلامة العمليات المصرفية الإلكترونية¹⁹⁷.

أولاً: الرقابة القانونية:

هي الرقابة التي يحددها القانون على المؤسسة المصرفية والعمليات التي تمارس من خلالها، حيث تحدد السلطة التشريعية في كل دولة جهة رقابية على المؤسسات المالية من أجل التحقق من سلامة الممارسات المالية للحفاظ على الاستقرار المالي للقطاع المالي بشكل عام، وعادةً ما يكون البنك المركزي هو السلطة الرقابية على المؤسسات المالية باعتباره الجهة العليا، وينظم قانون كل دولة صلاحيات البنك المركزي وفقاً لرؤية الدولة وأهدافها¹⁹⁸، وأحد أهم المهام التي يقوم بها البنك المركزي هي الحفاظ على الاستقرار المالي للقطاع المصرفي، من خلال إرساء

¹⁹⁶ العايب عصام، المرجع السابق، ص51.

¹⁹⁷ عائشة بوثلجة، الصيرفة الإلكترونية، جامعة الشلف حسيبة بن بوعلي، الجزائر، بحث منشور، 2021م، ص26.

¹⁹⁸ صلاح الدين محمد أمين الإمام، صادق راشد الشمري، تفعيل أنظمة الرقابة المصرفية وتطويرها وفق المعايير الدولية، مجلة الإدارة والاقتصاد، السنة الرابعة والثلاثون، العدد 90، العراق، 2011م، ص358.

قواعد عامة يتوجب على المؤسسات المالية العمل من خلالها والتقيّد بها¹⁹⁹. وتتمثل أهمية مرحلة التشريع والرقابة القانونية بتوفير إطار قانوني ينظم العمليات المصرفية بشكلها التقليدي والإلكتروني، كما يحمي حقوق العملاء والبنوك، فضلاً عن تعزيز الثقة في العمليات المصرفية وزيادة معدلات استخدامها، فضلاً عن الحد من المخاطر المرتبطة بالعمليات المصرفية الإلكترونية²⁰⁰.

ويقصد بالرقابة القانونية في مجال الصيرفة الإلكترونية، هي أن يكون هناك إطار قانوني منظم للعمليات المصرفية الإلكترونية يضمن أمنها وسلامتها، ولاشك أن تشعب المواضيع التي نتجت إثر ارتباط تكنولوجيا المعلومات بالقطاع المصرفي، أدت إلى ظهور حركة تشريعية من أجل الحفاظ على الحقوق المشتقة من ممارسة هذه العمليات من خلال شبكة الإنترنت²⁰¹، ومثال عليها كما ذكر الباحث سابقاً إصدار قانون يُعنى بجرائم تقنية المعلومات، وقانون يحدد أحكام المعاملات الإلكترونية، وقانون البيانات الشخصية، فضلاً عن حزمة متكاملة من القوانين المتعلقة بأمن المعلومات والتكنولوجيا في المجال المصرفي.

تشكل الرقابة القانونية دوراً مهماً في الحفاظ على أمن وسلامة القطاع المصرفي، وتحدد الدولة جهات معينة للتأكد من سلامة تطبيق القوانين المنظمة بالإضافة إلى رقابة البنك المركزي، فنجد أن مملكة البحرين قد مهدت الأساس القانوني المطلوب للتعامل الإلكتروني ونظمت أحكامه من خلال إصدار قانون الخطابات والمعاملات الإلكترونية الصادر بالمرسوم رقم (54) لسنة 2018م، وعينت هيئة تنظيم الاتصالات الجهة الإدارية المختصة بالقانون الآن في المرسوم بقانون رقم (45) لسنة 2021م²⁰².

أما دولة الإمارات العربية المتحدة فنجد أن المرسوم بقانون اتحادي رقم (46) لسنة 2021م بشأن المعاملات الإلكترونية وخدمات الثقة، يهدف إلى تعزيز الثقة في المعاملات الإلكترونية كافة، كما يرفع القيمة القانونية للتوقيع الرقمي ليكون مدعوماً بتقنيات حديثة وآمنة، وحجية قانونية كاملة، بما يُغني عن الحضور الشخصي لإتمام المعاملات في المؤسسات سواء من داخل الدولة أو من خارجها، وتعد الهيئة العامة لتنظيم قطاع الاتصالات والحكومة الرقمية المعنية بتحديد الإجراءات والضوابط المتعلقة بالتعامل الإلكتروني، على سبيل المثال التحقق من

¹⁹⁹ سهام ملياط، المرجع السابق، ص54.

²⁰⁰ صلاح الدين محمد أمين الإمام، وصادق راشد الشمري، المرجع السابق، ص360.

²⁰¹ عبدالرزاق خليل، عادل نقموش، السلطات الإشرافية والعمليات المصرفية الإلكترونية، مجلة الإقتصاد الجديد، العدد 00، 2009م، ص36.

²⁰² المادة 1، المرسوم بقانون رقم (45) لسنة 2021، مملكة البحرين، الجريدة الرسمية، العدد 3521.

صحة التوافق الإلكترونية والإشراف والرقابة على المنشآت المالية بالتنسيق مع مصرف الإمارات العربية المتحدة المركزي²⁰³.

ثانياً: الرقابة التشغيلية:

تعد الرقابة التشغيلية من أهم أنواع الرقابة على العمليات المصرفية الإلكترونية، حيث تتمثل في مراقبة العمليات المصرفية الإلكترونية من قبل البنوك نفسها، للتأكد من أنها تتم بشكل آمن وموثوق، ويقصد بالرقابة التشغيلية الإشراف على المخاطر التشغيلية التي تؤدي إلى إحداث خلل ما في الأنظمة التشغيلية للبنك عند ممارسة العمليات المصرفية، على سبيل المثال يمكن أن تؤدي الضوابط غير الكافية في النظم التشغيلية إلى هجوم ناجح من قبل قرصنة الإنترنت، مما يمكنهم للوصول إلى معلومات سرية وبيانات خاصة بالعملاء²⁰⁴.

ويكون الهدف من الرقابة التشغيلية في إطار العمليات المصرفية الإلكترونية في تقييم مدى كفاءتها وفعاليتها فضلاً عن تحديد المخاطر المحتملة واتخاذ الإجراءات اللازمة لضمان سلامتها وأمان ممارستها، إذ تستخدم البنوك آليات مختلفة لتحقيق الأمان وفرض الرقابة على المخاطر التشغيلية التي قد تواجهها الممارسات الإلكترونية، فعلى سبيل المثال تقنية تشفير البيانات من خلال استخدام أنظمة وخوارزميات معقدة لحماية المعلومات الحساسة الغير مصرح بها، بحيث لا يمكن اختراقها، كما تعد آلية حماية تسجيل الدخول من أهم صور الرقابة التشغيلية التي تمارسها البنوك، وذلك بإعطاء مهلة للجلسة في حالة وجود صفحة ويب خاملة لم يتم استخدامها لدقائق، أو تعطيل عمليات تسجيل الدخول المتعددة في نفس الوقت²⁰⁵.

تتم إجراءات الرقابة التشغيلية حيث يتم قياس المخاطر التشغيلية ومايتخللها من تقييم للمخاطر، من خلال مراجعات مستمرة واتخاذ إجراءات وتدابير وقائية²⁰⁶ كتعزيز الكادر الملم بمستجدات الأمن السيبراني للتصدي للهجمات الإلكترونية التي تتعرض لها البنوك والمعاملات المصرفية الإلكترونية²⁰⁷، وذلك من خلال المواقع أو التطبيقات المقدمة للخدمات المصرفية التابعة

²⁰³ المادة 4، المرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة، الإمارات العربية المتحدة.

²⁰⁴ Risk management for electronic banking and electronic money activities ,electronic money, page5

[\(bis.org\) Risk management for electronic banking and electronic money activities \(March 1998\)](http://bis.org/Risk%20management%20for%20electronic%20banking%20and%20electronic%20money%20activities%20(March%201998))

²⁰⁵ [Top 10 technology trends in Digital Banking Security Solution | IDFC FIRST Bank](http://idfcfirstbank.com/Top%2010%20technology%20trends%20in%20Digital%20Banking%20Security%20Solution)

²⁰⁶ Risk management for electronic banking and electronic money activities, Ibid, page 15.

²⁰⁷ بناء أفضل للمستقبل تقرير صندوق النقد الدولي بشأن الخدمات المالية الإلكترونية، واشنطن، 2021، ص37. [International](http://www.imf.org/International)

[Monetary Fund \(IMF\)](http://www.imf.org/Monetary%20Fund)

للمصرف بحيث يستطيع بهم الكشف عن التسلل ومراقبة الأنظمة والأنشطة غير المتوقعة، وتجنب الأخطاء التي من شأنها خرق النظام²⁰⁸.

ختاماً فإن الرقابة التشغيلية من أصعب أنواع الرقابة التي تمارسها الجهات المختصة، نظراً للوتيرة السريعة التي يتميز بها التطور التكنولوجي، ولذلك من وجهة نظر الباحث ستحتاج البنوك إلى فهم المتطلبات القانونية الوطنية المختلفة، واختلاف توقعات العملاء عند ممارسة العمليات المصرفية الإلكترونية، وبالتالي لابد من ضرورة وجود اجتماعات تنسيقية دورية بين الجهات الداخلة في الاختصاص، من بينها السلطتين التشريعية والتنفيذية، البنك المركزي، المؤسسات المصرفية، الهيئة المختصة بالأمن السيبراني، للبحث في أهم التطورات الطارئة على موضوعات القطاع المصرفي الإلكتروني ويمكن الاستفادة من الذكاء الاصطناعي في تحسس وتيرة الأنشطة غير الاعتيادية في البرامج الخادمة مما يسهل التصدي للهجمات.

²⁰⁸ R. D.Tanase , R. serbu, operational risk and E-banking, vol 3(52), series V, 2010, page332.

المطلب الثاني

دور الحفاظ على سرية البيانات الشخصية (سرية المعلومات) في تعزيز الحماية

الحفاظ على سرية المعلومات في العمليات المصرفية الإلكترونية يلعب دوراً حاسماً في ثقة العملاء أثناء التعامل مع البنوك في إجراء عملياتهم اليومية²⁰⁹، ولبيان دور سرية المعلومات في الحفاظ على حقوق العملاء من الاختراق والتعدي وأثرها على تعزيز الحماية، سيتناول الباحث مفهوم السرية في ظل العمليات المصرفية، وكيف يمكن تحقيق التوازن بين الطبيعة الخاصة لسرية المعلومات الشخصية، وبين الانفتاح والتدفق الإلكتروني إثر التعامل الإلكتروني من خلال الفرعين التاليين.

- الفرع الأول: جوانب الحفاظ على سرية المعلومات في العمليات المصرفية الإلكترونية.
- الفرع الثاني: الفرع الثاني النطاق القانوني لحماية البيانات الشخصية.

²⁰⁹ Kassim Mukuuma, Mwase Ali, Benard Engotoit, Examining the influence of E-banking security on customer satisfaction in Uganda – a case study of Ugandan commercial banks, ICTACT journal on management studies, Vol.06 Issue 02, page 1227.

الفرع الأول

جوانب الحفاظ على سرية المعلومات في العمليات المصرفية الإلكترونية

تشكل سرية المعلومات هاجساً لدى البنوك والحكومة والعملاء، حيث تشكل قضايا أمن المعلومات مخاوفاً لدى كلٍ منهم،²¹⁰ فتكون مصلحة الحكومة هي الحفاظ على الاستقرار المالي وتكوين بيئة أعمال خصبة قادرة على جذب الاستثمارات الأجنبية، سيما أن تكون مصلحة المؤسسات المصرفية في استقطاب عدد أكبر من العملاء والبقاء في السوق والمنافسة، أما مصلحة العملاء تكمن في ممارسة عملياتهم المصرفية بكل يسر وسهولة وأمان²¹¹.

أولاً: أمن المعلومات بين الخصوصية والتوافر:

إن مبدأ السرية والثقة يعدان ضماناً جوهرياً للبنوك بأن المعلومات المتوفرة لديهم تحظى بحماية فائقة، مما ينعكس على جودة العمليات المتاحة عبر الشبكة التي بدورها تؤثر على استقطاب عدد أكبر من العملاء²¹²، إذ إن أمن المعلومات يشكل اللبنة الأساسية لدى البنوك، حيث يجد البنك الناجح الذي يقدم خدمات إلكترونية مؤشرات نجاحه عندما يحقق أعلى مدى من الأمان في المعاملات الإلكترونية التي تتم من خلال أحد وسائل تقنية المعلومات، وفي سبيل تحقيقه لا بد من توجيه الإهتمام نحو متانة البنى التحتية التشغيلية والأنظمة القانونية المساندة، التي توفر الحماية من الاختراق أو الإلتلاف أو المخاطر التابعة الأخرى²¹³.

إن مصطلح الخصوصية واسع ويطال العديد من الجوانب حيث قسمها الباحث Steven Devis إلى أربع فئات، خصوصية المعلومات، الخصوصية الجسدية، خصوصية الاتصالات وأخيراً الخصوصية الإقليمية حيث يشمل Steven الخصوصية المرتبطة بالإنترنت بخصوصية المعلومات وأمنها، خصوصاً أن قدرة الفرد تكون محدودة في التحكم بالمعلومات الخاصة به عندما يمارس أعماله عبر الشبكة وينتظر عادة أن تقوم الحكومة والشركات الخاصة بتوفير تقنيات متطورة من أجل حمايته كمستهلك²¹⁴.

يعتبر الحق في الخصوصية حقاً محمياً في التشريعات والداستير بشكل عام، ويمكن أن نستشف الحق في خصوصية المعلومات التي تدار عبر شبكة الإنترنت من نص المادة 26 من

²¹⁰ Zachary B. Omariba, Nelson B. Masese, Dr. G. Wanyembi, Security and privacy of electronic banking, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, page 435.

²¹¹ إيلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية، المركز العربي للنشر والتوزيع، مصر، 2019م، ص 25.

²¹² دلندة دوايدي، زهرة بن حود، أمن المعلومات المصرفية، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر، 2019-2020م، ص 20.

²¹³ دلندة دوايدي، زهرة بن حود، المرجع نفسه، ص 27.

²¹⁴ Zachary B. Omariba, Nelson B. Masese, Dr. G. Wanyembi, Ibid, page 438.

دستور مملكة البحرين، التي نصت على: "حرية المراسلة البريدية والبرقية والهاتفية والإلكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقاً للإجراءات والضمانات المنصوص عليها فيها"²¹⁵، إذ كفل الدستور الحق في خصوصية المراسلات بمختلف أشكالها ولايجوز انتهاك سريتها، ومع ذلك فإن التقنيات الحديثة المستخدمة في مجال تكنولوجيا المعلومات والاتصالات تتطور بشكل هائل ولايمكن توقع إمكانيتها بمعزل عن تطور التكنولوجيا²¹⁶، وبالتالي أصبح من السهل انتهاك الخصوصية خاصة مع زيادة التعاملات التجارية أو الحكومية أو غيرها من المعاملات التي تتم عبر أحد وسائل تقنية المعلومات. تختلف دواعي انتهاك الحق في الخصوصية بحسب كل فرد، ويمكن أن تتجلى الجوانب القانونية لهذا الانتهاك في عدد من الجرائم والأعمال غير الشرعية التي يمارسها الأفراد، من بين هذه الجرائم: انتحال الهوية، الابتزاز، اختراق أنظمة المعلومات، والوصول إلى الأسرار المهنية والتجارية²¹⁷.

الهدف الرئيسي الذي يوجه العميل المصرفي إلى استخدام الجانب الإلكتروني من العمليات المصرفية هو التوافر، بحيث إن تكون الخدمة المصرفية الإلكترونية متوفرة في جميع الأوقات، لذلك يجب على البنك أن يعمل بشكل منظم ودقيق للوصول إلى الأمن، السرية وإمكانية الوصول، وعليه لتحقيق خاصية التوافر إلى جانب أمن المعلومات، لابد من إدراك أهمية المقاييس الثلاثة الأساسية وهم التحكم بالوصول، إثبات الصلاحيات والتدقيق، للحفاظ على أعلى مستوى من الأمن²¹⁸ وأخيراً ضمان الوصول إلى البيانات والمعلومات للمستخدمين المصرح لهم في أي وقت²¹⁹. إذ إنه في ظل السماح والتوافر يُخلق أماناً أمراً حساساً ودقيقاً يتعلق بالحفاظ على الخصوصية وحماية البيانات الشخصية لدى ممارسي العمليات الإلكترونية، إذ لابد أن تتمتع البيانات الشخصية بحماية وضمانات تحول عن الوصول غير المصرح به بتقنيات ومعالجات آمنة وفقاً لمعايير الأمان المعترف بها عالمياً، كاستخدام تقنية التشفير والتي تعد أهم التقنيات وأكثرها استخداماً في صدد

²¹⁵ المادة 26، دستور مملكة البحرين، الجريدة الرسمية، مملكة البحرين، العدد 2571، 2002م.

²¹⁶ منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، بغداد، 2013م، ص323.

²¹⁷ منى الأشقر جبور، المرجع السابق، ص122.

²¹⁸ نزيه محمد علي، دور التشريعات والقوانين الوطنية والدولية الحاكمه لحماية امن المعلومات، المجلة المصرية لبحوث الإعلام، الجزء الثاني، العدد 8، 2022م، ص 1306.

²¹⁹ Daniela popescul, The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security,

Proceedings ofThe16thInternational Business Information Management Association Conference,2011,

page2. <https://www.researchgate.net/publication/257985911>

تأمين العمليات المصرفية الإلكترونية من خطر الاعتداءات،²²⁰ فضلاً عن استخدام تقنية جدران الحماية والتي تعمل على فصل الشبكة الداخلية للبنك عن الشبكة العامة في الإنترنت، فلا تسمح بالدخول إلى الطلبات الموثوقة وتسمح بمرورها²²¹، مع ذلك لابد من تحقيق توازن مهم بين أمن المعلومات وإمكانية الوصول إليها، خصوصاً في القطاع المصرفي، ولا يعني أنه يقل أهمية في باقي القطاعات، إلا أننا نركز على محور الدراسة، فالتطور التكنولوجي السريع وانتشار العمليات المصرفية الإلكترونية جعل من البيانات الشخصية للأفراد عرضة للتهديدات الأمنية.

فإذا رأينا مفهوم إمكانية الوصول من ناحية إيجابية فإنه يسهل من التبادل، التعاون والإبتكار، أما الناحية السلبية فهي سهولة الوصول إلى بيانات حساسة تؤدي إلى الإضرار بالأفراد المستخدمين. لذلك لابد من خلق توازن بين الحق في الخصوصية وبين إمكانية الوصول، وذلك من خلال فرض حماية صارمة تنظم جمع واستخدام البيانات الشخصية، بالإضافة إلى زيادة الوعي والتثقيف بشأن حق الأفراد في الخصوصية، وأهمية حماية البيانات الشخصية بتعاون من القطاعين العام والخاص لتحقيق أعلى مستويات الأمان والحماية.

ثانياً: مفهوم البيانات الشخصية في نطاق الخدمات المصرفية الإلكترونية:

ظهرت البيانات الشخصية لأول مرة بشكل ورقي، بحيث يصل إليها أفراد معينون ذوو تصريح مسبق لإجراء عملية معينة، ولهذا يمكننا القول بأنها محدودة إلى حد ما، ويرجع مفهوم البيانات الشخصية لفكرة الحق الشخصي للأفراد في الحفاظ على حرمة حياتهم الخاصة بما فيها من معلومات شخصية وخاصة ينفرد فيها عن الغير تتعلق به، إذ تكون هذه المعلومات ملتصقة به تحديداً قابلة للتعرف عليه سواءً بطريقة مباشرة أو غير مباشرة²²².

في ظل التطور التكنولوجي، أصبحت هناك وسائل تقنية متقدمة لجمع ومعالجة البيانات الشخصية قد تشمل وسائل الاتصال الإلكتروني كمواقع الويب، التطبيقات الذكية وتقنيات الذكاء الاصطناعي، وبالنظر إلى هذا التطور أصبح من الضروري تدخل التشريع لتحديد مفهوم البيانات الشخصية بشكل واضح ودقيق، سيما بيان الحقوق والالتزامات المتعلقة بها، فضلاً عن بيان العقوبات المترتبة على انتهاكها وحمايتها من الوصول الغير مصرح به²²³.

²²⁰ صليح بونفلة، المرجع السابق، ص117.

²²¹ Mohammad Al Animat, Legislation of Legal Protection for Electronic Banking Operations and Challenges in Jordan, International Journal of Economics, Business and Management Research Vol. 6, No.11, 2022,page217.

²²² إكرام سليمان قجم، الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن، رسالة ماجستير، جامعة قطر، قطر، 2021م، ص10.

²²³ دلندة دوايدي، زهرة بن حود، المرجع السابق، ص27.

اهتم الجانب التشريعي بتعريف البيانات الشخصية لما له من آثار مرتبطة بحقوق الإنسان التي تتسم بالطابع الشخصي وترتبط بالحق في الخصوصية بشكل خاص، فيرى البعض أن البيانات الشخصية ماهي إلا عنصر من عناصر الحق في الخصوصية وجزء لا يتجزأ منها،²²⁴ ولذلك نجد أن المشرع البحريني عرّف البيانات الشخصية من خلال تقسيمها إلى بيانات شخصية وبيانات شخصية حساسة، إذ عرّف النوع الأول من البيانات وأطلق عليها البيانات الشخصية التي تعني بأية معلومات في أية صورة تخص فرداً مُعرّفاً، أو قابلاً بطريق مباشر أو غير مباشر لأن يُعرّف، وذلك بوجه خاص من خلال رقم هويته الشخصية، أو صفة أو أكثر من صفاته الشكلية، أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية. وعرّف البيانات الشخصية الحساسة بأنها: أية معلومات شخصية تكشف على نحو مباشر أو غير مباشر عن أصل الفرد العرقي أو الإثني أو آرائه السياسية أو الفلسفية أو معتقداته الدينية أو انتمائه النقابي أو سجل السوابق الجنائية الخاص به أو أية بيانات تتعلق بصحته أو حالته الجنسية²²⁵.

سعى المشرع البحريني لفرض الحماية اللازمة للبيانات الشخصية، حيث تناول مفهومها بشكل عام مع تسليط الضوء على أهم العناصر التي إن وجدت كان حرياً أن تحظى بالحماية المقررة وفقاً للقانون، حيث ميّز المشرع البيانات الشخصية عن البيانات الشخصية الحساسة، وذكر لها أمثلة حيث يعد رقم الهوية الشخصية من البيانات الشخصية، أما سجل السوابق الجنائية تعد من البيانات الشخصية الحساسة. ونرى أن التعميم ووضع النقاط الأساسية في التعريف يسهم في إلحاق العديد من البيانات من ضمن الحماية القانونية، فعلى سبيل المثال اعتبار أية معلومات تصل بشكل مباشر أو غير مباشر لمعلومات الفرد خاضعة للحماية القانونية، باعتبارها بيانات شخصية، أي لم يحد الوصول للمعلومات المباشرة فقط، بل حتى تلك المعلومات التي قد توصل الغير لبيانات شخصية لشخص ما ولو كانت بوسيلة غير مباشرة.

تحليلاً لتعريف المشرع البحريني للبيانات الشخصية نجد أن هناك ثغرة قانونية قد يستفيد منها البعض للفرار من المسؤولية، وهي الجملة التالية: " أية معلومات في أية صورة تخص فرداً مُعرّفاً"²²⁶، فمصطلح فرداً يعود على الشخص الطبيعي دون الشخص المعنوي وهذا ما ذكره في القانون نفسه المذكور أعلاه في المادة الأولى، فعلى سبيل التوضيح انتهاك نظام مؤسسة للحصول على معلومات وبيانات حساسة تعطي تصريحاً بإجراء عمليات تؤدي إلى أضرار وخسائر مادية أو معنوية، بحيث يكون هذا الانتهاك غير خاضع للحماية وفقاً لقانون حماية البيانات الشخصية،

²²⁴ طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية، مجلة القانون والاقتصاد، مصر، ملحق خاص، العدد الثاني والتسعون، 2019م، ص209.

²²⁵ المادة 1، قانون رقم 30 لسنة 2018 بإصدار البيانات الشخصية، الجريدة الرسمية، العدد 3375، مملكة البحرين.

²²⁶ المادة 1، قانون رقم 30 لسنة 2018 بإصدار البيانات الشخصية المرجع السابق.

باعتبار أن البيانات الشخصية تعود لشخصٍ معنويٍّ وليس شخصاً طبيعياً. لذلك يمكننا صياغة تعريف البيانات الشخصية على النحو الآتي:

"أية معلوماتٍ في أية صورة تخصُّ شخصاً طبيعياً أو معنوياً مُعرِّفاً، أو قابلاً بطريق مباشر أو غير مباشر لأن يُعرَّف، وذلك بوجه خاص من خلال رقم هويته الشخصية أو صفةٍ أو أكثر من صفاته الشكلية أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية".

أخيراً إن البيانات الشخصية للأفراد والمعلومات الخاصة التابعة لهم محط حمايةٍ وخصوصيةٍ، لا يجوز المسُّ بها أو نشرها، مع العلم أن معالجتها وحفظها وتخزينها أصبح شائعاً لأغراضٍ متنوعة إلا أنه لا بد من حمايتها من قبل المسئول وإتخاذ جميع الإجراءات والتدابير اللازمة لحمايتها ومنع انتشارها أو الوصول إليها أو استخدامها خارج الأغراض المقصودة، وعدم الكشف عنها إلا وفقاً لما ينص عليه القانون²²⁷.

الفرع الثاني: النطاق القانوني لحماية البيانات الشخصية:

التطورات الحديثة التي يشهدها العالم في استخدام الانترنت وانتشاره في جميع المجتمعات أوجد حاجة ملحة لتحديث القوانين الحالية، إذ تتزايد الحاجة إلى حماية البيانات التي يتم مشاركتها في مواقع الويب، فضلاً عن البيانات التي يتم مشاركتها في مواقع التواصل الاجتماعي، على الرغم من وجود بعض القوانين واللوائح التي تنظم قضايا الخصوصية إلا أنها لا تستطيع التكيف بشكل كاف مع تحديات العالم الرقمي الحالي، فمنذ فترة طويلة دافعت الشركات الكبرى التي تجمع بيانات الأشخاص عن تنظيم الخصوصية وحماية البيانات، ومع ذلك يجب على الشركات أن تعمل بالتعاون مع الهيئات التنظيمية الحكومية، ومشاركة الخبرات لتحديث القوانين والإطار القانوني الملزم لتتناسب مع التطورات التكنولوجية، وتوفر مزيداً من المرونة في حماية البيانات وضمان الخصوصية للمستخدمين²²⁸، ولذلك سيعرض الباحث أولاً الحماية القانونية للبيانات الشخصية التي وضعتها القواعد القانونية في التشريعات العامة، ومن ثم سيبينها في التشريعات الخاصة بحماية البيانات الشخصية، مع ربط أثرها على العمليات المصرفية الإلكترونية، خصوصاً أن الأمن المصرفي الإلكتروني غاية تسعى إليها البنوك للحفاظ على العلاقة مع عملائها²²⁹ فيما يلي:

²²⁷ محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، مصر، 2007 م، ص312.

²²⁸ رويدا حسن الجعافر، قانون حماية البيانات الشخصية في الأردن، المجلة العربية للنشر العلمي، الأردن، الإصدار الخامس، العدد خمسون، 2022م، ص1083.

²²⁹ Kassim Mukuuma, Mwase Ali, Benard Engotoit, Examining the influence of E-banking security on customer satisfaction in Uganda – a case study of Ugandan commercial bank, Ibid, page 1226.

1- الحماية في التشريعات العامة:

• الحماية الدستورية:

عادةً ما يسعى التنظيم القانوني في الدول إلى وضع الخطوط العريضة التي تضمن الحقوق الأساسية للأفراد في المجتمع، سواءً كانت هذه الحقوق يعود أثرها عليهم مباشرة أو على الدولة، وبما أن الحق في الخصوصية من أهم الحقوق للصيقة بالفرد وينبثق منه العديد من الحقوق يعد تضمينه في الدستور غايةً لا بد منها لبيان أهميته وخطر التعدي عليه، لذلك نجده من ضمن القواعد التي تتعلق بالحرية الشخصية والحياة الخاصة للأفراد²³⁰.

يمكن أن نستخلص من الدستور البحريني حماية البيانات الشخصية، من خلال استقراء النصوص التي تناولها المشرع في هذا الباب، خصوصاً فيما يتعلق بسرية المراسلات والاتصالات التي ذكرها في المادة 26 منه، إذ يمكن اعتبار عمومية نص المادة في الحفاظ على سرية المراسلات وإنزاله على البيانات الشخصية التي تكون عرضة للانتهاك عندما يتم إدخالها لإجراء عملية ما، كما حدّ القانون من صلاحية الجهات في إفشاء سريتها إلا في الحالات التي يحددها القانون وذلك حفاظاً على المعلومات المتبادلة وخصوصيتها²³¹.

• الحماية المدنية:

وتتعلق الحماية المدنية للبيانات الشخصية من المبدأ العام في القانون المدني، الذي يعنى بمسؤولية الفرد بالتعويض عن الأعمال غير المشروعة التي تسبب بها، وأدت إلى إضرار الغير عن طريق جبر الضرر الناتج، وقد يصل التعويض إلى جبر الأضرار المادية والمعنوية جراء الانتهاك الحاصل على البيانات الشخصية²³².

2- الحماية في التشريعات الخاصة:

• قانون جرائم تقنية المعلومات رقم (60) لسنة 2014م:

تجدر الإشارة أن القانون المنظم لجرائم تقنية المعلومات في التشريعات الخاصة في مملكة البحرين هو قانون رقم (60) لسنة 2014م، والذي يهدف إلى حماية المجتمع البحريني من الجرائم التي ترتكب باستخدام تقنية المعلومات. ويتضمن القانون تعريفات للمصطلحات المتعلقة بجرائم تقنية المعلومات، وعقوبات على مرتكبي هذه الجرائم. إذ جرّم القانون اختراق أنظمة

Bandita Das, Jayanta Boruah, Right to privacy and data protection under Indian legal regime, ²³⁰ published online on : <https://ssrn.com/abstract=3827766>, page9.

²³¹ المادة 26، دستور مملكة البحرين، مملكة البحرين، الجريدة الرسمية، العدد 2571، 2002م.

²³² مادة 158، 162، مرسوم بقانون رقم 19 لسنة 2001 بإصدار القانون المدني، مملكة البحرين، الجريدة الرسمية، العدد 2476، 2001م.

المعلومات والاطلاع على البيانات الشخصية بدون تصريح قانوني في العديد من نصوصه، ومن أمثلة هذه الجرائم²³³:

- الدخول غير المشروع إلى نظام تقنية المعلومات أو جزء منه.

- إدخال بيانات غير صحيحة إلى نظام تقنية المعلومات أو جزء منه.

• قانون حماية البيانات الشخصية رقم 30 لسنة 2018م، مملكة البحرين²³⁴:

قانون حماية البيانات الشخصية رقم 30 لسنة 2018م في البحرين، يُعنى بحماية البيانات الشخصية، وعرفها كما ذكرنا آنفاً فوفر الحماية اللازمة لها من خلال بيان طريقة الحفظ والتخزين والمعالجة والجهات المخولة بها، كما حظر القانون على أي شخص معالجة البيانات الشخصية دون موافقة صاحبها، ما لم يكن ذلك ضرورياً لتنفيذ عقد أو اتخاذ خطوات بناءً على طلب صاحب البيانات أو تنفيذ التزام يرتبه القانون، كما أنشأ قانون حماية البيانات الشخصية هيئة وطنية لحماية البيانات الشخصية، تتولى وضع الضوابط والإشراف على تطبيق القانون²³⁵.

• قانون حماية المستهلك رقم (35) لسنة 2012م، مملكة البحرين²³⁶:

يُعد قانون حماية المستهلك رقم (35) لسنة 2012م من أهم التشريعات الخاصة في مملكة البحرين والتي تحمي حقوق المستهلك، يهدف القانون إلى حماية المستهلك من أي ممارسات تجارية غير عادلة أو احتيالية، وضمان حقه في الحصول على المنتجات والخدمات التي تلبي احتياجاته ورغباته. يشمل قانون حماية المستهلك مجموعة من الحقوق الأساسية للمستهلك، كحق الحصول على المعلومات الصحيحة للمنتج، وحق الضمان، كما ألزم التجار بعدم استخدام بيانات المستهلكين إلا للأغراض المتفق عليها²³⁷.

²³³ المادة 4، المادة 8، قانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات، مملكة البحرين، الجريدة الرسمية، العدد 3178، 2014م.

²³⁴ قانون رقم 30 لسنة 2018 لحماية البيانات الشخصية، مملكة البحرين، الجريدة الرسمية، العدد 3375، 2018م.

²³⁵ المادة 27، المرجع نفسه.

²³⁶ قانون رقم 35 لسنة 2012 بشأن حماية المستهلك، مملكة البحرين، الجريدة الرسمية، العدد 3063، 2012م.

²³⁷ المادة 2، قانون رقم 35 لسنة 2012 بشأن حماية المستهلك، المرجع السابق.

المطلب الثالث

الطبيعة القانونية لمسئولية المصارف أثناء ممارسة العمليات المصرفية الإلكترونية

أدى ظهور الخدمات المصرفية الإلكترونية إلى توجه الأفراد إلى إجراء معاملاتهم البنكية عن طريق الوسائل الإلكترونية التي تقدمها البنوك، ويرجع ذلك إلى المزايا التي تقدمها مقارنة بالخدمات المصرفية التقليدية، مثل الأمان والسرعة، إلا أن الخدمات المصرفية الإلكترونية لا تخلو من التحديات، إذ غالباً ما تحدث اضطرابات ونزاعات تشكل عبئاً على المصرف، كما تُزعزع استقرار مركزه المالي وسمعته، إذ تزداد الأنشطة الاحتيالية مع تزايد شعبية طرق الدفع الإلكترونية، فقد تسببت هذه الجرائم في أضرار جسيمة للأفراد والمؤسسات المالية والاقتصادات، كما أدى ظهور الخدمات المصرفية الإلكترونية إلى ظهور المنازعات المصرفية، ولذلك فإن حماية حقوق العملاء من مسؤولية البنوك أثناء ممارسة العمليات المصرفية الإلكترونية أمر مهم لضمان استقرار النظام المصرفي، وتعزيز الثقة بين العملاء والبنوك²³⁸.

بدأت الحاجة إلى الكشف عن قواعد المسؤولية المدنية في إطار التعامل الإلكتروني نظراً للطبيعة الخاصة التي تحوزها المعاملات الإلكترونية بأنواعها، لذلك كان لازماً بيان أحكام المسؤولية المدنية وكيفية مواجهة المخاطر الإلكترونية للحفاظ على أمن الأفراد والمؤسسات، ومواجهة الخطر الذي يدهم ممارسة العمليات المصرفية الإلكترونية ويهدد الاستقرار المالي²³⁹. وعليه سيتناول الباحث في هذا المطلب الطبيعة القانونية للمسؤولية المدنية التي تواجه المصارف من خلال الفرعين التاليين:

- الفرع الأول: مسؤولية المصرف العقدية.
- الفرع الثاني: مسؤولية المصرف التقصيرية.

²³⁸ حسني زايدي، أهمية البنوك الإلكترونية في تحسين العمليات المصرفية، رسالة ماجستير، جامعة العربي بن مهيدي، الجزائر، 2018م، ص15.

²³⁹ محمد حسين منصور، المرجع السابق، ص6.

الفرع الأول

مسئولية المصرف العقدية

تعد المسؤولية العقدية أولى أشكال المسؤولية المدنية، وتنشأ عند إخلال أحد الأطراف بالتزاماته العقدية أو عند امتناعه عن تنفيذها، أو قصد أن ينفذها بصورة غير موافقة لطبيعة العمل، أو قد يتخلف عن تنفيذ جزء معين، مما يسبب إحداث ضرر للطرف الآخر، ونتيجة لحدوث الضرر فيوجب على محدثه تعويض الطرف المتضرر وفقاً للمبادئ العامة في القانون المدني²⁴⁰.

تتحقق مسؤولية المصارف العقدية عن الأخطاء الإلكترونية والانتهاكات للبرامج الخاصة بها التي تؤدي إلى حدوث أضرار للعميل المصرفي، على سبيل المثال حدوث انتهاك لصفحة الموقع الخاصة بالبنك، أو أخطاء تقنية تتسبب في فقدان العميل لأمواله أو سرقة معلومات خاصة وحساسة، إلا أنه لا بد أن يثبت الخطأ قد صدر من جانب المصرف وأدى بدوره إلى حدوث الضرر مع ثبوت ارتباط العلاقة السببية بينهما²⁴¹، كما أن تحديد المسؤولية العقدية للمصرف والتعويض المناسب يستند إلى عوامل عديدة كشروط العقد والبنود الخاصة بتحديد المسؤولية والتعويض فضلاً عن القوانين ذات الصلة، لاشك أن وضع أحكام المسؤولية العقدية تحت إشراف السلطات القانونية يقود إلى تعزيز ثقة الأفراد في أمان الخدمات المصرفية الإلكترونية.

حيث تقوم المسؤولية العقدية للمصرف إذا تحققت أركانها جميعاً، ولا يمكن أن تقوم المسؤولية إذا تحقق أحدها دون الآخر، وتتمثل أركان المسؤولية العقدية بالخطأ، الضرر، والعلاقة السببية، مع مراعاة الطبيعة الإلكترونية الخاصة التي تنسم بها عمليات المصرف الإلكترونية والتي يترتب عليها قيام مسؤولية المصرف عند الإخلال بأي من التزاماته كالأمان والسرية وغيرها، وسيبين الباحث فيما يلي هذه الأركان على النحو الآتي:

أولاً: الخطأ الإلكتروني كركن لقيام المسؤولية العقدية:

يعرف الخطأ بالمفهوم العام بأنه "تقصير في مسلك الإنسان لا يقع من شخص يقظ وجد في الظروف الخارجية نفسها التي أحاطت بالمخطئ"²⁴²، أما الخطأ الإلكتروني فعرفه جانب من الفقه بأنه: "عبارة عن فعل غير مشروع قام به شخص يتعامل وفقاً للوسائل الإلكترونية، سبب على

²⁴⁰ مصطفى العوجي، القانون المدني - المسؤولية المدنية، مؤسسة بحسون، لبنان، الجزء الثاني، الطبعة الأولى، 1996م، ص15.

²⁴¹ إيلاف فاخر كاظم علي، المرجع السابق، ص133.

²⁴² إيلاف فاخر كاظم، المرجع السابق، ص135.

أثره ضرراً للغير، والخطأ يكون عقدي مصدره فعل يقوم به الشخص المتعامل ويسبب بذلك ضرراً لغيره يستوجب التعويض²⁴³.

يمكننا أن نستنتج مفهوم الخطأ من القواعد العامة للمسؤولية في القانون المدني، مع العلم أن الباحث لم يجد في نصوص القانون المدني تعريفاً واضحاً لتعريف للخطأ، إنما يمكن استخلاصه في إلزام المخطئ بتعويض المتضرر، سواء كان الفعل صدر منه شخصياً أو عن طريق الغير الذي يقع تحت رقابته، وذلك وفقاً لشروط حددها القانون. والخطأ في المسؤولية العقدية يكون ناتجاً عن الإخلال بالتزامات عقدية بين البنك والعميل، مالم يتذرّع المسئول عن الخطأ باستحالة التنفيذ،²⁴⁴ لتحقيق أحد أسباب الاستحالة القانونية كالقوة القاهرة. ويمكن للبنك أن يتحرر من مسؤوليته في حالة حدوث الخطأ من قبل العميل استناداً بأنه لا يحق للمتضرر الذي تسبب بخطأه في عدم تنفيذ الالتزام الموجب للبنك والمطالبة بالتعويض عند عدم القدرة على التنفيذ²⁴⁵.

ويقوم الخطأ على عنصرين أساسيين العنصر المادي، ويقصد به إخلال الطرف الملزم بتنفيذ التزامه كلياً أو جزئياً اتجاه الطرف الآخر أما العنصر الثاني هو العنصر المعنوي، ويقصد به الإدراك أو التمييز، يرى البعض أنه لا يشترط لتحقيق الخطأ تحقق ركنيه المادي والمعنوي في إطار عمل المصرف، باعتبار أن المصرف شخص معنوي لا يتحقق معه الإدراك أو التمييز، فلن يصدر الخطأ من قبل الشخص المعنوي بنفسه لاختلافه عن الشخص الطبيعي،²⁴⁶ وبالتالي فإن تحقق العنصر المادي كافٍ لقيام الخطأ باعتباره أحد أركان المسؤولية العقدية.

حيث إن قيام الخطأ الذي يترتب المسؤولية العقدية يوجب قيام شرطين أساسيين هو وجود العقد بين الطرفين البنك والعميل، أما الشرط الثاني هو تحقق الضرر للطرف الآخر، ومثال على هذه الأضرار هو "التأخر في تحويل الأموال بوسيلة إلكترونية وحصول تأخير في إتمام التحويل المالي مما تسبب بالإضرار بمصلحة العميل وعند حدوث انتهاك أو تعدي على العمليات المصرفية الإلكترونية لخطأ يعود إلى البنك سواء كان الخطأ صادر من البنك نفسه أو من بفعل أحد تابعيه²⁴⁷، حيث "أخذت محكمة النقض المصرية بهذا المبدأ في الطعن رقم 732 لسنة 1976 جلسة 2-3-41 تأكيداً على مسؤولية المتبوع في حالة صدور الخطأ من قبل تابعه، إذ جاء في الحكم الصادر" من المقرر في قضاء هذه المحكمة أن القانون المدني إذ نص في المادة 174 على أن يكون

²⁴³ زعباب سهام، المرجع السابق، ص 55.

²⁴⁴ مصطفى العوجي، المرجع السابق، ص 32.

²⁴⁵ مصطفى العوجي، المرجع نفسه، ص 107.

²⁴⁶ صفا علي حسين، المسؤولية المدنية للمصرف عن الإخلال بقواعد الاستعلام المصرفي، مجلة العلوم القانونية، جامعة بغداد، العراق،

العدد الخاص الثالث، الجزء الأول، 2017م، ص 392.

²⁴⁷ إيلاف فاخر كاظم، المرجع السابق، ص 137، 136.

المتبوع مسئولاً عن الضرر الذي يحدثه تابعه بعمله غير المشروع متى كان واقعاً منه في حال تأدية وظيفته أو بسببها، فقد أقام هذه المسؤولية على خطأ مفترض في جانب المتبوع فرضاً لا يقبل إثبات العكس، مرجعه سوء اختياره وتقصيره في رقابته²⁴⁸.

لذا فإن المصرف ملزمٌ بتحمل المسؤولية القانونية والعقدية إثر الإخلال بأحد التزاماته العقدية بحماية عملائه، وضمان أمان العمليات التي تمارس عبر الإنترنت، ففي حالة حدوث خطأ يجب على البنك أن يتحمل المسؤولية واتخاذ الإجراءات اللازمة لتصحيح الوضع وتعويض العميل المتضرر تعويضاً جابراً للضرر، وذلك وفقاً لقواعد المسؤولية في القانون المدني.²⁴⁹

ثانياً: الضرر كركن لقيام المسؤولية العقدية:

يعد الضرر ثاني أركان المسؤولية المدنية، حيث يعتبر الضرر من الأركان الجوهرية في تحقق المسؤولية المدنية، إذ يعد محلاً للالتزام بالتعويض لجبر الأضرار المرتبطة بالخطأ الصادر، ويقصد بالضرر بأنه الأذى الذي يصيب المدين في ماله أو شخصه أو غيره الذي يستحق التعويض وفقاً للقانون الواجب التطبيق،²⁵⁰ ولم يعرف المشرع البحريني الضرر إلا أنه نص على أحكامه في القانون المدني البحريني، في حين أن الفقه لم يترك المجال فارغاً، وعرف العديد من الفقهاء والباحثين الضرر، إذ يعرف الأستاذ بلحاج العربي الضرر بأنه: هو الأذى الذي يصيب الشخص في حق من حقوقه أو في مصلحة مشروعة له سواء كان ذلك الحق أو تلك المصلحة ذا قيمة مالية أو لم يكن²⁵¹.

يقسم الضرر إلى نوعين، فالنوع الأول ضررٌ ماديٌّ يصيب أحد حقوق المضرور وبشكل قيمة مالية تتحقق معها خسارة أو فوات كسب ما، أما النوع الثاني هو الضرر المعنوي ويقصد به الضرر الذي يصيب الفرد في نفسه من ألمٍ أو حزنٍ أي ليس له قيمة مالية، إلا أن تحققه يعطي المتضرر الحق في المطالبة بالتعويض وفقاً للقانون المدني،²⁵² ويمكن تصور الضرر المحقق لمسؤولية البنك جراء ممارسة العمليات المصرفية الإلكترونية في صورة انتهاك البرامج التي يطرحها البنك لإجراء عمليات مصرفية إلكترونية عبرها، أو انتهاك سرية المعلومات والبيانات الشخصية واستخدامها في أغراض مختلفة.²⁵³

²⁴⁸ سعيد أحمد شعلة، قضاء النقص المدني في المسؤولية والتعويض، مجموعة القواعد القانونية التي قررت محكمة النقض المصرفي خلال اثنتين وسبعين عاماً 1931-2005، المركز القومي للإصدارات القانونية، مصر، 2007م، ص20.

²⁴⁹ صفا علي حسين، المرجع السابق، ص391.

²⁵⁰ حمد حسين منصور، المرجع السابق، ص332.

²⁵¹ عميري مليسة، مطراف أنيس، الضرر في المسؤولية العقدية، رسالة ماجستير، جامعة مولود معمري، الجزائر، 2019م، ص6.

²⁵² مصطفى العوجي، المرجع السابق، ص 165، 166.

²⁵³ محمد حسين منصور، المرجع السابق، ص334.

الجدير بالذكر أن للبنك الحق التحرر من التعويض عن الضرر الناشئ عن المسؤولية العقدية في حالة حدوث الضرر غير المتوقع، إذ إن المبدأ العام في المسؤولية العقدية هو شمول الضرر المتوقع، إلا في حالتي الغش والخطأ الجسيم يمكن الاستناد إلى الضرر غير المتوقع في حالة حدوثه،²⁵⁴ وأكد الطعن رقم 92 لسنة 34 ق جلسة 24-4-2978 هذا المبدأ²⁵⁵.

مما تقدم فإن البنك يتحرر من المسؤولية في حالة حدوث الضرر غير المتوقع، إلا فيما يقع من ضمن الخطأ الجسيم والغش والذي يشمل الضرر سواء كان متوقعاً أو غير متوقع، وبالتالي يمكن أن يستفيد البنك في هذه الحالة بالتحرر من مسؤوليته لو حدث انتهاك لعملية مصرفية مورست عبر الإنترنت وتحقق معها ضرر للمدين، إلا أن البنك لم يكن بإمكانه توقع حدوثه، "ويعود تقدير الضرر والتعويض المناسب إلى السلطة التقديرية للمحكمة"²⁵⁶.

يُعتبر العميل الطرف الأضعف في العلاقة المصرفية، ومع ذلك هو الموجب قانوناً بإثبات هذا الضرر مشتملاً على شروط تحققه بأن يكون الضرر محققاً، حالاً، مباشراً، متوقعاً كأصل أو غير متوقع استثناءً في حالتي الخطأ الجسيم أو الغش²⁵⁷، فعند ممارسة العملية المصرفية الإلكترونية من الصعب أن يثبت الضرر غير المتوقع الحاصل، خصوصاً إذا كان الضرر ناتجاً لخطأ جسيم أو غش من قبل البنك أو تابعيه، وبالتالي قد لا يستطيع العميل إثبات المسؤولية المدنية للبنك، والجدير بالذكر، أن الاختراق قد يحدث في أي لحظة ولا يكون متوقعاً في غالب الأحيان، وعليه من وجهة نظر الباحث، عدم الأخذ بهذا المبدأ في مجال الصيرفة الإلكترونية خصوصاً أن الزيادة المطردة في عمليات الانتهاك التي تطال العمليات المصرفية الإلكترونية تتفاقم وتتطور مع تطور التكنولوجيا، والأخذ به على إطلاقه يُفقد المدين الحماية اللازمة، ومن الممكن أن تُفقد الثقة في العمليات المصرفية الإلكترونية مع مرور الزمن، ويرجح الباحث الأخذ بأن الضرر بحالتيه سواء كان متوقعاً أو غير متوقع، مع ضرورة تحقق بقية الأركان دون خطأ من قبل العميل أو مانع من موانع المسؤولية، لا بد من أن يكون البنك هو المسؤول الأول، وذلك استناداً للطبيعة الخاصة التي

²⁵⁴ محمد حسين منصور، المرجع السابق، ص 333.

²⁵⁵ إذ صدر عن محكمة النقض في قضية منظورة أمامها الآتي: "المدين في المسؤولية العقدية لا يلزم في غير حالتي الغش والخطأ الجسيم إلا بتعويض الضرر الذي يمكن توقعه عادةً وقت التعاقد، وذلك عملاً بالمادة 1\221 من القانون المدني، والضرر المتوقع يقاس بمعيّار موضوعي لا بمعيّار شخصي، بمعنى أنه هو ذلك الضرر الذي يتوقعه الشخص المعتاد في مثل هذه الظروف الخارجية التي وجد فيها المدين، لا الضرر الذي يتوقعه هذا المدين بالذات" سعيد أحمد شعله، المرجع السابق، ص 35.

²⁵⁶ مجبر حنان، مهدي صارة، المسؤولية المدنية المترتبة عن العقد الإلكتروني في التشريع الجزائري، رسالة ماجستير، جامعة د.مولاي الطاهر، الجزائر، 2021م، ص 32.

²⁵⁷ سليمان ضيف الله الزين، التحويل الإلكتروني للأموال ومسؤولية البنوك القانونية، دار الثقافة للنشر والتوزيع، مصر، الطبعة الأولى، 2012م، ص 153.

تتمتع بها العمليات المصرفية الإلكترونية والتي يتطلب معها أخذ جميع التدابير اللازمة لمنع حدوث الأضرار وقيام المسؤولية تبعاً لذلك.

ثالثاً: العلاقة السببية كركن لقيام المسؤولية العقدية:

لوجوب تحقق المسؤولية العقدية لا يكفي تحقق الخطأ والضرر، إنما يجب أن تتحقق معهما العلاقة السببية التي تربط فيما بينهما، وبالتالي فإن تحقق ضرر للعميل دون أن يكون للبنك سبباً مباشراً أدى بدوره حدوث الضرر ينفي مسؤولية البنك²⁵⁸، وبالتالي فإن وجود الرابطة السببية بين الخطأ المرتكب والضرر الناتج يعد نتيجة منطقية لقيام المسؤولية المدنية، فلا يُعقل أن يُسأل المصرف عن ضرر لم يكن نتيجة فعل قام به أو تابعيه²⁵⁹.

وحيث تنقطع العلاقة السببية بين الخطأ والضرر الحاصل في صورة أمرين، أما الأمر الأول فهو حدوث السبب الأجنبي كالحادث الفجائي والقوة القاهرة، كأن يحدث انقطاع في الكهرباء مما يتسبب في عدم قدرة البنك على التصدي للضرر الحاصل على المدين أثناء ممارسة العملية المصرفية الإلكترونية، والأمر الثاني هو حدوث الخطأ من قبل العميل أي لا يكون للمصرف علاقة في حدوث الانتهاك أو التعدي، كعدم قيام العميل باتخاذ التدابير اللازمة أو في حالة تقديم معلومات غير صحيحة أدت إلى الإضرار بمصلحة العميل²⁶⁰. وتجدر الإشارة أن انتفاء العلاقة السببية في حالة الخطأ التام من قبل العميل، بينما إذا كان الخطأ مشتركاً بين المصرف والعميل فإن ذلك يؤدي إلى انتقاص التعويض على حسب نسبة خطأ المسئول في وقوع الضرر²⁶¹.

كما ذكرنا آنفاً، قد يواجه العميل صعوبة عملية تتعلق بإثبات الخطأ الحاصل من قبل المصرف وتتعقد عملية الإثبات أكثر، عندما يتحتم على العميل إثبات أن الخطأ الصادر هو السبب الذي أدى إلى إحداث الضرر، أي أن تكون هناك رابطة سببية بين الخطأ والضرر، وفي كل الأحوال يستطيع المصرف أن يتحلل من مسؤوليته العقدية في حالة إثبات السبب الأجنبي الذي أدى إلى الاختراق، ب؛ حيث إنه اتخذ جميع التدابير اللازمة، ولكن عجزت هذه التدابير أن تدفع الضرر الحاصل²⁶².

²⁵⁸ صفا علي حسين، المرجع السابق، ص 398.

²⁵⁹ سليمان ضيف الله الزين، المرجع السابق، ص 158.

²⁶⁰ حسام عبد اللطيف حمي مخيس، الحماية القانونية للمعاملات المصرفية الإلكترونية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 11، العدد 43، 2022م، ص 429.

²⁶¹ محمد حسين منصور، المرجع السابق، ص 335.

²⁶² JACQUES DE WERRA, EVELYNE STUDER, REGULATING CYBERSECURITY What civil liability in case of cyber-attacks ?, EXPERT FOCUS, Droit, 2017, page 8.

أخيراً إن تقدير توافر العلاقة السببية يرجع للسلطة التقديرية للمحكمة، وذلك ما أخذت به محكمة النقض المصرية والذي بيّن انفراد قاضي الموضوع بتقدير واستخلاص توافر العلاقة السببية بين الخطأ والضرر دون أن يكون لمحكمة النقض الرقابة عليه إلا في حالة الاستخلاص غير السائب²⁶³.

الفرع الثاني

مسئولية المصرف التقصيرية

تتشابه المسؤولية التقصيرية في أركانها بالمسئولية العقدية، من خطأ يحدث في حالة الإخلال بواجب قانوني عام مقترن بإدراج المخل بهذا الواجب وضرر وعلاقة سببية، إلا أن الأولى تُعد أشمل من الأخيرة، إذ يمكن للمضرور أن يطالب بالأضرار المتوقعة وغير المتوقعة، ويكون أثر الحكم بالمسئولية التقصيرية جبر الضرر الذي أصاب المضرور سواء كان الضرر أدبياً أو مادياً، وقد تنتفي المسؤولية بنفس أسباب انتفاء المسؤولية العقدية كتحقق القوة القاهرة، أو خطأ المضرور وخطأ الغير²⁶⁴، ومنعاً لتكرار المضمون سيبين الباحث في هذا الفرع الأساس القانوني الذي تقوم عليه المسؤولية التقصيرية، ومن ثم سيبين بعض الفروقات بين المسؤولية التقصيرية والمسئولية العقدية فيما يلي:

أولاً: أساس مسؤولية المصرف التقصيرية:

تعتبر المسؤولية التقصيرية الوسيلة الأخرى التي يحتج بها العميل للحفاظ على حقه حتى لو لم يكن هناك التزام عقدي بينه وبين المصرف، بحيث يكون مصدر الالتزام القانوني على المصرف الإمتناع عن الإضرار بالغير، ومثال على ذلك كأن يقوم المصرف بنشر معلومات تتعلق بالعميل دون موافقته أو بدون تصريح قانوني²⁶⁵، وقسم الفقه أساس المسؤولية التقصيرية للبنك عن المخاطر الإلكترونية إلى عديد من النظريات، وقد أخذ بها العديد من المشرعين في النصوص القانونية المنظمة للعمليات المصرفية سواء التقليدية أم الإلكترونية، وسيبين الباحث أهم النظريات التي حددت الأساس التي قد تقوم عليه المسؤولية التقصيرية للمصرف وفق المحاور التالية:

²⁶³ السيد عبدالوهاب عرفة، المسؤولية المدنية في ضوء الفقه وقضاء النقض، المكتب الفني للموسوعات القانونية، مصر، المجلد الثاني،

لا توجد سنة نشر، ص 212.

²⁶⁴ السيد عبدالوهاب عرفة، المرجع نفسه، ص 15.

²⁶⁵ سليمان ضيف الله الزين، المرجع السابق، ص 176.

أ- مسؤولية المصرف التقصيرية وفق النظرية الشخصية:

تقوم هذه النظرية على أساس أن المصرف هو المسئول عن الأضرار التي تنتج عن حدوث المخاطر الإلكترونية، استناداً إلى أن المصرف عندما يقدم الخدمة الإلكترونية للعميل فإنه يمارسها بشكل مهني، وبالتالي فإن من العدل أنه عندما يحدث خطأ تسبب بإضرار العميل دون خطأ منه أن يتحمل المصرف تبعه ذلك، حيث تتأسس هذه النظرية وفقاً لقيام مسؤولية المصرف عن أعمال تابعيه على أساس الخطأ الشخصي²⁶⁶.

اتفق المشرع البحريني والإماراتي على قيام مسؤولية الأشياء التي تتطلب عناية خاصة من آلات وأجهزة إلكترونية، حيث تعد الأجهزة الإلكترونية العائدة للمصرف أو الآلات أو البطاقات وما في حكمها تابعة للمصرف نفسه، وعليه فإنه كان حرياً أن يكون هو المسئول عن الأضرار الناجمة عنها لكونها تخضع لرقابته وعنايته وفق هذا المبدأ²⁶⁷.

حيث نص المشرع البحريني على المسؤولية الناجمة عن ضرر الأشياء في المادة 175\أ من القانون المدني والتي نصت على أنه " كل من يتولى حراسة شيء مما يتطلب عناية خاصة لمنع وقوع الضرر منه يلزم بتعويض الضرر الذي يحدثه هذا الشيء، ما لم يثبت أن هذا الضرر قد وقع بسبب أجنبي من قوة قاهرة أو حادث فجائي أو فعل المضرور أو فعل الغير"²⁶⁸.

ومن أهم تطبيقات هذا النظرية هي نظرية "الخطأ المفترض" والذي يتمحور حول أن أساس المسؤولية التقصيرية يقوم على الخطأ ومن ارتكب خطأ أدى إلى إضرار الغير يُلزم بتعويضه، وبالتالي يكون المصرف مسئولاً عن الضرر الصادر على فرض إن الخدمة الإلكترونية المقدمة قد تطلها الإعتداءات نظراً لطبيعتها، "فلا يكون العميل ملزماً بإثبات حدوث الخطأ إنما يكون ملزماً بإثبات الشروط التي تتحقق بها مسؤولية الأشياء"²⁶⁹.

ب- مسؤولية المصرف التقصيرية وفق نظرية تحمل التبعة:

وجدت هذه النظرية لتلافي الانتقادات التي طالت فكرة النظرية الشخصية، إذ يمكن أن يتحمل المصرف من مسئوليته عندما يثبت حدوث السبب الأجنبي الذي حال دون حدوث الضرر، إذ يرى الجانب المؤيد لهذه النظرية أنه لا يحتاج العميل أن يثبت شروط مسؤولية الأشياء المحدثة

²⁶⁶ إيلاف فاخر كاظم علي، المرجع السابق، ص 164.

²⁶⁷ زينة غانم يونس العبيدي، مسؤولية المصرف عن أخطاء الكمبيوتر في النقل الإلكتروني للنقد، مجلة الراافدين للحقوق، المجلد 11، العدد 39، 2009م، ص 14.

²⁶⁸ المادة 175\أ، مرسوم بقانون رقم 19 لسنة 2001 بإصدار القانون المدني، مملكة البحرين، الجريدة الرسمية، العدد 2476، 2001م.

²⁶⁹ إيلاف فاخر كاظم علي، المرجع السابق، ص 162.

للضرر كما ذكرنا سابقاً، بل حتى أنه تخطى عن اعتبار الخطأ أساساً لقيام المسؤولية التقصيرية وتحقق الضرر والعلاقة السببية كافٍ لقيام مسؤولية المصرف وتعويض العميل²⁷⁰.

يستند أنصار هذه النظرية رجحان فعاليتها لحماية العمليات المصرفية الإلكترونية، فأرأوا بأن المصرف عندما يمارس النشاط الإلكتروني ويقوم بتوفير هذه الخدمة للعميل فإنه من الطبيعي أن يتحمل المخاطر التابعة لهذه الممارسة، خصوصاً أن التطور التكنولوجي الذي يطال الصناعة المصرفية يصعب من إيجاد الشخص المخطئ الذي تسبب بالضرر، كما استند مؤيدو هذه النظرية إلى أن المصرف بوصفه كيان احترافي يمارس عمله باحترافية، وتوصف نشاطاته بأنها عالية الخطورة يجب أن يتحمل مزايا الخوض في هذا العمل وعيوبه، فإن حدث ضررٌ لابد أن يُلزم بتعويض المتضرر على أثره،²⁷¹ فضلاً أن هذه النظرية توفر الحماية القانونية التي تقوم على العدل والمنطق، لكون العميل الطرف الضعيف في العلاقة وبالتالي من الصعب أن يثبت العميل الخطأ²⁷².

يمكن استخلاص موقف المشرع الإماراتي في الأخذ بنظرية تحمل المخاطر للمصرف من الحكم الصادر محكمة تمييز دبي، إذ يكون المصرف مسؤولاً حتى لو لم يكن مخطئاً إلا في حالة إذا ما ثبت الخطأ من العميل أو خطأ قد استغرق خطأ البنك، حيث استخلصت المحكمة بأن تحمل البنك المسحوب عليه هذه التبعة مشروطٌ بعدم وقوع خطأ أو إهمال من جانب العميل الوارد إسمه في الصك، وإلا تحمل العميل تبعة خطأه، ويعتبر الساحب مخطئاً على وجه الخصوص إذا لم يبذل في المحافظة على دفتر الشيكات المسلم إليه العناية الواجبة، ويعتبر تقصيره في ذلك هو السبب المباشر في استيلاء الغير عليه والعبث به²⁷³، وعليه فإن القضاء الإماراتي جعل انتفاء مسؤولية المصرف محددةً في حالتين هما خطأ العميل و خطأ المصرف.

وفي إطار تحليل المصرف من المسؤولية الناتجة لخطأ العميل أثناء ممارسة العملية المصرفية الإلكترونية فإن ذلك يعتبر موقفاً منطقياً، فمن البديهي أن تبرأ ذمة المصرف من المسؤولية عندما يكون الضرر الناتج سببه العميل، ولا يمكن أن يحتج العميل بنظرية تحمل المخاطر، فالقصد من إقرار هذه النظرية هي الحفاظ على حقوق العميل خصوصاً مع صعوبة تحديد الخطأ في الممارسات الإلكترونية، إلا أن هذا لا يعني أنه يستفيد من إهماله ويتضرر المصرف فقط لكونه مهني، وهذا ما أكدته محكمة التمييز البحرينية عندما قضت "بعدم مسؤولية

²⁷⁰ رياض السيد حسين أبو سعيدة، ضمان ضرر العميل في التعامل المصرفي الإلكتروني، مجلة الكوفة، العدد 12، 2011م، ص 30.

²⁷¹ سليمان ضيف الله الزين، المرجع السابق، ص 184.

²⁷² سليمان ضيف الله الزين، المرجع نفسه، ص 187.

²⁷³ جاسم علي سالم الشامسي، المرجع السابق، ص 1795.

البنك عن تعويض كامل الضرر المتمثل بدفع قيمة كامل الشيك للعميل بعد أن ثبت أن هذا العميل يتحمل جزءاً من الخطأ الذي أدى إلى تزوير توقيعه على الشيك²⁷⁴.

ثانياً: جوانب الاختلاف بين المسؤولية التقصيرية والمسؤولية العقدية:

1- من حيث أساس المسؤولية²⁷⁵:

- أ- يعد أساس قيام المسؤولية العقدية وجود عقد بين طرفين على أن يلتزم الطرفين كلاهما أو أحدهما بأداء عمل ما أو امتناع عن عمل، وبالتالي إخلال الملتزم بالتزامه يؤدي إلى قيام المسؤولية العقدية التي يترتب عليها آثارٌ يحددها إما العقد أو القانون.
- ب- أما أساس المسؤولية التقصيرية هو الإخلال بواجب قانوني وارتكاب عملٍ غير مشروع يترتب على أثره تعويضٌ للشخص المتضرر.

2- من حيث التضامن²⁷⁶:

- أ- لا تضامن في المسؤولية العقدية إلا في حالة وجود نصٍ اتفاقي في العقد أو نص قانوني يوجب التضامن، وهذا مانصت عليه مادة 263 من القانون المدني البحريني²⁷⁷.
- ب- أما في المسؤولية التقصيرية يكون المسؤولون عن إحداث الضرر مسئولون عن الضرر إذا تعدد، وذلك وفق القانون حيث نصت المادة 160 من القانون المدني البحريني على أنه "إذا تعدد المسؤولون عن عمل ضارٍ كانوا متضامنين في التزامهم بتعويض الضرر، وتكون المسؤولية بينهم بالتساوي، إلا إذا عيّن القاضي نصيب كلٍ منهم في التعويض²⁷⁸".

3- من حيث الإغفاء من المسؤولية:

- أ- كأصلٍ عامٍ يجوز الاتفاق على الإغفاء من المسؤولية العقدية في حالة الإخلال بالتزام عقدي، ولا مانع أن يتفق الطرفان على إعفاء الطرف المخل بالتزامه من المسؤولية في حالة قيام الخطأ العقدي أو التخفيف منها، وبالتالي على أثر هذا الاتفاق يتحلل الطرف الذي تسبب بالضرر من تعويض المضرور²⁷⁹.
- ب- أما في المسؤولية التقصيرية فلا يجوز الاتفاق على الإغفاء من المسؤولية، وقد نصت محكمة النقض المصرية على هذا المبدأ، والذي أبدته في الطعن على النحو الآتي: "إذا

²⁷⁴ سليمان ضيف الله الزين، المرجع السابق، ص 190.

²⁷⁵ شريف أحمد الطباخ، المسؤولية المدنية التقصيرية والعقدية، دار الفكر والقانون، مصر، الطبعة الأولى، الجزء الأول، 2009م، ص 53.

²⁷⁶ السيد عبدالوهاب عرفة، المرجع السابق، ص 10.

²⁷⁷ مادة 263، مرسوم بقانون رقم 19 لسنة 2001 بإصدار القانون المدني، مملكة البحرين، الجريدة الرسمية، العدد 2476، 2001م.

²⁷⁸ مادة 160، مرسوم بقانون رقم 19 لسنة 2001 بإصدار القانون المدني، مملكة البحرين، الجريدة الرسمية، العدد 2476، 2001م.

²⁷⁹ مصطفى العوجي، المرجع السابق، ص 125.

كان الحكم المطعون فيه قد انتهى بحق إلى أن مسؤولية الشركة المؤجرة مسئولية تقصيرية وكانت الفقرة الأخيرة من المادة 217 من القانون المدني صريحة في بطلان كل شرط يقضى بالإعفاء من هذه المسؤولية فإن دفاع الشركة المؤسس على إعفائها يكون مرفوضاً حتماً، وبالتالي فهو دفاعٌ جوهريٌّ لا يتغير به وجه الرأي في الدعوى، ومن ثم فإن إغفال الحكم الرد عليه لا يبطله²⁸⁰.

كما أيد المشرع البحريني موقف القضاء المصري في مسألة الإعفاء من المسؤولية، ونص الفقرة الأخيرة من المادة 217 من القانون المدني البحريني صراحةً على بطلان كل شرط يقضى بالإعفاء من هذه المسؤولية²⁸¹.

4- من حيث الإثبات:

أ- يشترط على العميل في المسؤولية العقدية إثبات إخلال البنك بالتزامه العقدي، فيكون الدائن العميل ملزماً بإثبات وجود عقدٍ بينه وبين البنك، على أن يلتزم البنك المدين بإثبات التزامه بما ورد في العقد²⁸².

ب- طبقاً لقواعد المسؤولية التقصيرية يكون العميل ملزماً بإثبات تحقق العمل غير المشروع متضمناً الخطأ والضرر، أي يكون عبء الإثبات مسنداً إليه بشكلٍ كامل.

ختاماً، نستخلص مما سبق إن المسؤولية المدنية للمصرف قد تختلف على حسب الأساس القانوني التي تستند عليه، فقد تكون مسئولية عقدية أم تقصيرية، يشترط في كلاهما وجود أركان المسؤولية والتي تتمحور بالخطأ، الضرر والعلاقة السببية، مع العلم أن هناك نظريات حاولت أن تحافظ على حقوق العميل مع التطور الحاصل في القطاع المصرفي بقدر الإمكان، بين مضيّق وموسّع في شروط قيام المسؤولية المدنية، فمنهم من اشترط وجود الأركان الثلاثة وغياب أحدها يعني انتفاء المسؤولية، ومنهم من عوّل على وجود الخطأ أو الضرر كلاً على حدةٍ كافٍ لقيامها، كما أن تحقق السبب الأجنبي يحلّل المصرف من المسؤولية إذا أثبت الأخير حدوثها، وكان من

²⁸⁰ أحمد سليم فريز نصر، الشرط المعدل للمسؤولية العقدية في القانون المدني المصري، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، 2006م، ص 29.

²⁸¹ المادة 217، مرسوم بقانون رقم 19 لسنة 2001 بإصدار القانون المدني، مملكة البحرين، الجريدة الرسمية، العدد 2476، 2001م

²⁸² انظر إلى د. جاسم علي سالم الشامي، تطبيقات المسؤولية المدنية المصرفية في قضاء المحكمة الاتحادية العليا ومحكمة تمييز دبي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الرابع، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003، ص 1787.

واللذي بين أن "المحكمة الاتحادية العليا في الطعن رقم 401 و 456 لسنة 20 قضائية جلسة الأحد الموافق 30 إبريل سنة 2000 والتي أخذت رأياً مخالفاً لما أخذه موقف الفقه المذكور أعلاه في عبء الإثبات للمسؤولية العقدية إذ ألزمت المصارف بتحمل تبعه الأضرار التي تصيب عملائها نتيجة ما يقدمونه لهم من خدمات مصرفية حتى لو لم يثبت خطأ البنك نفسه استناداً لفكرة التبعة التي تقوم على أساسها فكرة مخاطر المهنة ولا يعفى البنك من هذه التبعة إلا في حالة خطأ العميل أو إهماله".

غير الممكن أن يدفع التعدي أو الإنتهاك أو الخطأ الذي أدى إلى حدوث الضرر، أما من وجهة نظر الباحث فيما يتعلق بقيام المسؤولية التقصيرية فتتفق مع نظرية تحمل المخاطر استناداً للآتي:

1- يعد العميل الطرف الضعيف في العلاقة المصرفية ومن الصعب عليه إثبات خطأ البنك المحدث للضرر.

2- المشرع البحريني أوكل مزاولة العمل المصرفي إلى جهات احترافية مرخصة، وبالتالي فإن العمل الذي تقوم به يجب أن يكون قادراً على التصدي لأي نوع من الإعتداءات، وتعد مسؤوليته قائمة على مخاطر المهنة.

3- إذا أخذنا بنظرية السبب الأجنبي، يمكن أن يتحلل المصرف من مسؤوليته عن الأضرار الناجمة، وبالتالي على المشرع أن يحد من صور التحلل من المسؤولية دون شمول فعل الغير، لأن ذلك لا يتماشى مع طبيعة العمليات المصرفية الإلكترونية؛ حيث إن التعدي عادةً سيكون من فعل الغير كالمقرصن، وبالتالي فإن استبعاد المسؤولية قد تؤثر في نزوح العملاء وعدم التعامل مع المصرف لكونه غير قادرٍ على حفظ حقوق العميل المالية والتصدي لهذه الإعتداءات، فضلاً عن عدم تعويضه لجبر الأضرار الناتجة عن الإعتداء.

المبحث الثاني

آثار حماية العمليات المصرفية الإلكترونية

تُعد العمليات المصرفية الإلكترونية الركيزة الأساسية للقطاع المصرفي الناجح في العصر الرقمي اليوم، إذ تزايد التوجه نحو استعمال الصيرفة الإلكترونية لما تحتوي عليه من مزايا استطاعت بها تكوين قاعدة كبيرة ومحبة من قبل المستخدمين، إلا إنه مع الإقبال الكبير نحوها، واجه القطاع المصرفي تحديات واسعة تتعلق بالطبيعة الرقمية التي تحوزها العمليات المصرفية الإلكترونية والمخاطر المصاحبة لها، وتتمثل أهم هذه التحديات في القدرة على المحافظة على أمن وسرية العمليات المصرفية الإلكترونية والتصدي إلى التهديدات الإلكترونية، إذ تستمر معدلات الهجمات الإلكترونية بالارتفاع مع تطور التكنولوجيا يوماً بعد يوم، مما يحتم على الأطراف المعنية باتخاذ ما يلزم من إجراءات وتدابير تمكن العملاء من ممارسة سليمة قادرة على حماية أموالهم وحقوقهم ضد هذه الهجمات²⁸³.

ففي ظل هذا التداخل بين رغبة الأفراد في الحصول على خدمات ميسرة وسهلة، وبين الانفتاح وضخ البيانات اللامتناهية الحاصل في الفضاء السيبراني، أدى إلى نتوج آثار تعود إيجاباً وسلباً على المصارف والدول، ناهيك عن الأثر المباشر على العملاء أنفسهم، فبالنظرة في هذا المبحث سيقسم الباحث آثار العمليات المصرفية الإلكترونية إلى ثلاثة مطالب، ففي المطلب الأول سيتم بيان الأثر المباشر للعمليات المصرفية الإلكترونية من خلال توضيح مدى انعكاس الحماية على المصرف وتأثر ثقة العميل بالتدابير التي يتخذها المصرف من أجل الحفاظ على ولائه، ومن ثم سيتم التطرق إلى الأثر غير المباشر لحماية العمليات المصرفية الإلكترونية على نمو وتعزيز الاقتصاد الوطني وجذب الاستثمارات الأجنبية،²⁸⁴ أما في المطلب الثالث والأخير سيتم استعراض نماذج تطبيقية لحالات انتهاك فعلية ومأمدة تقبل المؤسسات المالية للخسائر الناتجة عنها، وطرق التسوية التي اتبعتها لجبر الأضرار الناتجة وذلك تبعاً:

²⁸³ شريف عبدالرحمن سيف النصر، السيبرانية (المفهوم، الخصائص، الفرض والإشكاليات)، مركز الحضارة للدراسات والبحوث، العدد الحادي والعشرون، 2021م، ص6.

²⁸⁴ حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الإلكترونية، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2003م، ص 22.

المطلب الأول

الأثر المباشر لحماية العمليات المصرفية الإلكترونية

تصاعد وتيرة الاعتداءات الإلكترونية على جميع الأصعدة يستدعي تكاتف المجتمعات الدولية من حكومات ومؤسسات خاصة لتوفير المناخ اللازم لاستمرار الاستقرار المالي وثباته بقدر الإمكان²⁸⁵. لذلك يهدف هذا المطلب إبراز الأثر المباشر لحماية العمليات المصرفية الإلكترونية، خصوصاً بعد انتشار الإنترنت وسهولة الوصول إلى الوسائل المتاحة لممارسة العمليات المصرفية الإلكترونية المقدمة من قبل المصارف، مع الاعتراف بالمخاطر التي تواجه الأطراف المتعاملين وأثرها سواءً كان إيجابياً أو سلبياً. وعليه سيقسم هذا المطلب إلى فرعين.

- الفرع الأول: أثر حماية العمليات المصرفية الإلكترونية على المصرف.
- الفرع الثاني: أثر حماية العمليات المصرفية الإلكترونية على العميل.

²⁸⁵ منى الأشقر، المرجع السابق، ص58.

الفرع الأول

أثر حماية العمليات المصرفية الإلكترونية على المصرف

أفضى التطور التقني إلى وجوب خلق حالة من التطور والابتكار في عديد من الكيانات المصرفية، فضلاً عن تطبيق تدابير أمان فعالة لحماية العمليات المصرفية الإلكترونية²⁸⁶، ففي ظل الثورة الرقمية المتسارعة واعتماد المزيد من الأفراد والشركات على الخدمات المصرفية الإلكترونية لتحقيق غاياتهم، أصبح جديراً على المصارف التركيز على الاستفادة من الموارد الموجودة وتحفيز الابتكار والتطوير من أجل توفير خدمات إلكترونية بمزايا جديدة ومستحدثة، سيما طمأنة العملاء وتشجيعهم على تبني الحلول الرقمية، وتمكين المصارف من استغلال التقنيات الحديثة في تقديم خدمات متميزة تنافسية يصب في مصلحة المصرف من خلال زيادة العملاء، الأرباح أو القوة المالية²⁸⁷.

تغيرت العوامل التي كانت تؤثر في نجاح المصرف اليوم عنها في السابق، إذ إن دخول العولمة والتكنولوجيا المالية ومدى استعمال المصارف التكنولوجيا صار يؤثر بشكل كبير على قوة المصرف محلياً وعالمياً، لذلك توالى جهود المصارف إلى تقديم خدمات مصرفية إلكترونية تنتم بالجودة والتي تساعد على المنافسة عالمياً في المجال المصرفي، حيث يُعد من أهم الأهداف التي تسعى لتحقيقها الوصول إلى قاعدة أكبر من العملاء، فضلاً عن استقطاب الاستثمارات ورؤوس الأموال الأجنبية، وعليه يجد المصرف نفسه في خضم منافسة من أجل مواكبة التحديات في السوق العالمية والتطورات التكنولوجية في القطاع المصرفي، فالإدارة المصرفية الناجحة تحقق متطلبات التغيرات المناخية الاقتصادية من خلال ابتكار تطبيقات مصرفية وخدمات إلكترونية مستحدثة تتميز بالسرعة، الكفاءة والأمان بحيث تتبع أساليب تطويرية دائمة مثل استحداث خدمة جديدة، أو إعادة تصميم خدمات موجودة لتحسين كفاءتها وأدائها²⁸⁸.

وعلى الرغم من أن الابتكار يعمل بطريقة مزدوجة، فالمصرف يبتكر سبل حماية أولاً، ومن ثم يبتكر ليوفر خدمات جديدة، إذ يُعد الابتكار أهم العوامل المساعدة على المنافسة والتميز، إلا أن ضعف المهارات وغياب الاهتمام بالبحث العلمي وتنمية الابتكارات والاعتماد على النسخ خصوصاً

²⁸⁶ شريف عبدالرحمن سيف النصر، المرجع السابق، ص6.

²⁸⁷ Mishra, A., Awal, A., Elijah, J., & Rabi, I. (2017). An Assessment of the Level of Information

Security Awareness among Online Banking Users in Nigeria. International Journal of Computer Science and Mobile Computing Volume and Issue: Vol. 6, Issue 5, page374.

²⁸⁸ نور الدين كروش، ليلي أولاد إبراهيم، جمال دقيش، أثر استخدام تكنولوجيا المعلومات على تحسين جودة الخدمة المصرفية، مجلة البحوث والدراسات العلمية، الجزائر، المجلد 14، العدد 1، 2020م، ص 171.

في الدول النامية لا يقوي من مركز البنك في الأسواق العالمية²⁸⁹، وقد يجد المصرف نفسه نتيجة الاحتدام الناشئ عن المنافسة في الأسواق المصرفية غير قادر على الاستمرار، أو تخلخل وضعه المالي، أو في بعض الأحيان غير موافق لمعدلات النمو مما يفضي في الأخير إلى تغير القيمة السوقية للمصرف. والجدير بالذكر أن القيمة السوقية للمصرف تتأثر بناءً على عناصر عديدة، وتعد مواكبة التطورات التكنولوجية المالية وجذب الجمهور من العملاء من أهمها، لذلك إما تتغير هذه القيمة بشكل إيجابي أو سلبي بالتبعية، وتأكيداً لذلك هناك دراسات مصرفية أثبتت أن الانخفاض في معدلات النمو بأي بنك يعني فقدان جزء من حصته السوقية لصالح البنوك المنافسة، ونتيجة لذلك سيأثر سلباً على صافي أرباحه²⁹⁰.

نظراً لأهمية دخول الصناعة المصرفية إلى عالم تكنولوجيا المعلومات، تحظى حماية العمليات المصرفية الإلكترونية بأهمية تتعاضد على مر السنوات، ويعود أثر الحماية على المصارف بعوائد كثيرة ومن بين هذه العوائد:²⁹¹

- 1- تكوين علاقات مباشرة بين المصرف والعملاء والأطراف الأخرى ذات العلاقة.
- 2- الإسهام في تسهيل سير التعامل من خلال المصرف.
- 3- الطابع التلقائي التي تتميز به العمليات المصرفية الإلكترونية مما يتيح إجراء حركات تجارية جديدة دون الحاجة لوجود علاقة مسبقة.
- 4- التقليل من القيود الجغرافية وقد يتحلل المصرف من العوائق التقليدية التي توجد في العمليات التقليدية.
- 5- سيما إن إدخال الإنترنت وفي العمليات المصرفية يشكل واجهة إعلامية تعزز من الشفافية بين المصرف والعميل، بحيث يمكنها أن تروج لأعمالها وخدماتها، وتوضح مدى متانة القدرة التي تتمتع بها لحماية العمليات المبرمة من خلال المواقع الإلكترونية أو الأجهزة أو أي وسيلة أخرى يوفرها المصرف نفسه.

²⁸⁹ Abdul-Hussein Jasim Mohammed 1 , Munaf Abdulkadhim Mohammed , Ahmed Hussein Ahmed,

Ibid, page667.

²⁹⁰ شيرين سلطان، التنظيم القانوني للمعاملات المصرفية الإلكترونية في ضوء السياسة النقدية للدولة، دار الجامعة الجديدة للنشر، مصر، 2020م، ص115.

²⁹¹ طواهر رضا، تأثير الخدمات المصرفية الإلكترونية على ربحية البنوك التجارية دراسة حالة بنك الخليج الجزائر AGB خلال الفترة 2011-2016، رسالة ماجستير، جامعة قاصدي مرباح- ورقلة، الجزائر، 2018م، ص10.

وكل ذلك يخدم مصلحة المصرف من خلال تنويع مصادر الدخل والاستثمار للاستفادة من التقنيات الحديثة بشكل يؤدي إلى تسهيل العملية المصرفية على العميل، مما يحقق غايات تعود بالنفع على المؤسسة المصرفية²⁹².

إلى جانب العديد من الآثار الإيجابية التي تصاحب حماية العمليات المصرفية الإلكترونية والعائدة على مصلحة المصرف، هل هناك آثارٌ سلبيةٌ تنتج عن حمايتها؟ وللإجابة على هذا التساؤل، لابد من تحليل وربط ماسبق ذكره في الفصل الأول بما يتعلق بالمخاطر التي تتعرض لها المصارف، إلى جانب العيوب الناتجة إثر استخدام العمليات المصرفية الإلكترونية.

إن ارتباط العمليات المصرفية الإلكترونية بالمجالات المختلفة كالتجارة الإلكترونية، رتب التزاماتٍ جديدةٍ تقع على عاتق المصارف لم تكن موجودة أثناء استعمال العمليات المصرفية التقليدية، وعليه شكلت هذا الالتزامات عبئاً على المصارف في توفير الحماية اللازمة، والتي من شأنها صد التهديدات الإلكترونية والحيلولة دون حصول أضرارٍ تؤثر على أطراف العملية المبرمة، فإن تعرض المصرف للمخاطر التشغيلية على سبيل المثال يشكل أعباءً جديدةً على عاتق المصرف:²⁹³

1- فعندما تحل الآلة محل الكادر البشري، واستعمال الشبكات الإلكترونية لتنفيذ عمليات مصرفية إلكترونية، يؤدي إلى خسائر تشغيلية يتحملها المصرف لكي يواكب التطور الحاصل في القطاع المصرفي والمنافسة.

2- كما يجب عليه أن يكون جاهزاً لكل مستجد في العالم المصرفي الرقمي من نظمٍ وتطويع كواحد وغيرها.

3- سيما أن المصرف قد يتحمل أضراراً كفقْدان الثقة، أو أعباءً ماليةً نتيجة عدم وعي العملاء أو الموظفين للمخاطر الرقمية، فالعميل يمكن أن يتعرض لانتهاكاتٍ عن طريق مواقع غير موثوقة، ومن ثم يجد المجرم المعلوماتي ثغرةً للوصول إلى بيانات العميل نفسه.

4- إضافة إلى ذلك أن موظفي البنك أيضاً قد يساهمون بقصد أو غير قصد إلى حدوث الانتهاكات الرقمية والوصول إلى قاعدة بيانات عريضة لدى البنك، مما يؤدي إلى تحقق أضرارٍ ماديةٍ ومعنويةٍ.

²⁹² حنان بوعكوش، شادية زايدي، المرجع السابق، ص14.

²⁹³ حنان بوعكوش، شادية زايدي، المرجع السابق، ص21.

الفرع الثاني

أثر حماية العمليات المصرفية الإلكترونية على العميل

أصبحت قضايا الأمان وحماية المعلومات الشخصية ذات أهمية بالغة، ويتساءل العديد من العملاء عن مدى أمان معاملاتهم المصرفية عبر الإنترنت، وما إذا كانت معلوماتهم الحساسة تحظى بالحماية الكافية، حيث يتطلب تحقيق الأمان في العمليات المصرفية الإلكترونية تبني تدابير أمانٍ فعّالةٍ لحماية البيانات والحسابات الشخصية، خصوصاً أن تفكير العميل أفراداً كان أم شركاتٍ قد تغير نحو الحصول على كافة الخدمات المالية التي يحتاجها أينما كان وكيفما شاء، والمصرف القادر على توفير الحزمة المتكاملة من خدماتٍ ماليةٍ ميسرةٍ ومحميةٍ هو الذي سيشكل قاعدةً تسهم في ولاء العملاء له²⁹⁴. يأخذ هذا الجزء من الدراسة مسألة تأثير حماية العمليات المصرفية الإلكترونية على العميل كمحورٍ رئيسيٍّ، مستكشفاً كيف يؤثر التوجيه نحو الأمان والحماية على تجربة العملاء، وثقتهم في استخدام الخدمات المصرفية عبر الإنترنت²⁹⁵، إذ عادةً ما يشكل التعامل في طور الجانب المالي للعملاء مصدر قلقٍ وفجوةٍ الثقة بين العميل والمصرف العامل الرئيسي نحو تخلي العميل عن إجراء العمليات المصرفية عبر الشبكة،²⁹⁶ بغض النظر عما توفره من راحةٍ وسرعةٍ.

تأثير حماية العمليات المصرفية الإلكترونية يظهر بوضوح في مستوى راحة العملاء وثقتهم في استخدام الخدمات المصرفية عبر الإنترنت، عندما يتمتع العميل بشعور بالأمان يكون أكثر استعداداً للمشاركة في عمليات مالية أكثر تعقيداً ويظهر اهتماماً أكبر باستكشاف المزيد من الخدمات والمميزات المصرفية المبتكرة مما ينعكس في النهاية إيجاباً على المصرف نفسه وتكمن أهمية حماية وأمن العمليات المصرفية الإلكترونية بالنسبة للعميل في ضمان سرية بياناته الشخصية ومعاملاته المالية، وحماية أمواله من أي اختراقات أو عمليات احتيال، بالإضافة إلى تعزيز ثقته العامة في تبني التقنيات والخدمات المصرفية الحديثة²⁹⁷.

إن أمن العمليات المصرفية الإلكترونية هو ببساطة ما يتحقق به حماية مصالح الأفراد المالية، فكل فردٍ يريد أن يحمي أمواله الخاصة من أي اعتداء، ويرى الأفراد المصارف ملجأً آمناً

²⁹⁴ عبدالمطلب عبدالحاميد، اقتصاديات تكنولوجيا الخدمات المصرفية، الشركة العربية المتجدة للتسويق، مصر، 2010م، ص194.

²⁹⁵ بناء الثقة بالخدمات الإلكترونية بمنظومة الإسكوا، المرجع السابق، ص4.

²⁹⁶ Marinela Vrincianu* and Liana Anica Popa, CONSIDERATIONS REGARDING THE SECURITY AND PROTECTION OF E-BANKING SERVICES CONSUMERS' INTERESTS, Amfiteatru Economic, Romania, page390.

²⁹⁷ خولة بلحسن، دور الصيرفة الإلكترونية في تحسين جودة الخدمات المصرفية دراسة مقارنة بين بنك القرض الشعبي الجزائري - وكالة بسكرة - وبنك السلام - وكالة بسكرة -، رسالة ماجستير، جامعة محمد خيضر، الجزائر، 2019-2020م، ص72.

لحفظ الأموال، وبالتالي يلجأ إلى المصرف باعتباره محل ثقة، حيث استمدت هذه الثقة من ثقة الفرد في الدولة التي أعطت الجهاز المصرفي تصريحاً بممارسة العمل المصرفي، وبالتالي فإن دور الحكومة يمتد ليحقق نزاهة النظام المالي بأكمله وتحقيق الثقة في ممارسة العمليات المصرفية الإلكترونية، أسوةً بالثقة الموجودة للنقد الورقي في الوقت الحالي²⁹⁸.

تعد جودة الخدمة المصرفية عبر الإنترنت غايةً يسعى المصرف تحقيقها لرضا العميل، وعادةً ما يبحث العميل على ممارسةٍ مرنةٍ وذات جودة، وكما تعرف جودة الخدمات المصرفية بأنها "القدرة على الإنتاج أو تقديم خدماتٍ مصرفيةٍ تكون قادرة على الوفاء بحاجات المستهلكين والعملاء، والقدرة على تحقيق رغبات المستهلك بالشكل الذي يتطابق مع توقعاته ويحقق رضاه التام عن السلعة أو الخدمة المصرفية التي تقدم له"²⁹⁹، وعليه فإن الراحة والمرونة في إجراء العمليات سواءً بين البنك وعملائه من الأفراد أو العمليات بين البنك والبنك التاجر الآخر هي عبارة عن تلاقي بين طموحات العميل وبين قدرة البنك على توفير خدمات مصرفية تتسم بالجودة المطلوبة، ومع ذلك فإن مفهوم الجودة مفهومٌ واسع جداً وينطوي على أبعادٍ عديدةٍ، على الرغم من أن السهولة والمرونة تعد أهم الأبعاد التي تتسم بها جودة العمليات المصرفية الإلكترونية، إلا أنه في الواقع اليومي تحتوي تلك العمليات على مخاطر ذات طابعٍ جديدٍ يشكل تحدياً أمام ممارسي الخدمات المصرفية والخبراء في هذا المجال³⁰⁰، وفي خضم التحول الرقمي، يعتبر أمان العمليات المصرفية الإلكترونية أمراً لا غنى عنه لضمان راحة وثقة العملاء، من خلال توفير جودةٍ توافق المعايير المتبعة في الدولة، فتأثير هذا الأمان يتجلى في صورٍ عدةٍ مثل: تحسين تجربة المستخدم، تعزيز التفاعل، وتشجيع العملاء على استكشاف خدماتٍ متقدمةٍ، لذلك ينبغي على المصارف ومقدمي الخدمات المالية أن يولوا اهتماماً كبيراً لتحقيق توازنٍ فعالٍ بين الأمان وتوفير تجربة مستخدم رائعة، مما يضمن استدامة وازدهار الخدمات المصرفية عبر الإنترنت في المستقبل³⁰¹.

لاشك أن أثر حماية العمليات المصرفية الإلكترونية يتطلب جهداً متقارباً من العميل والمصرف نفسه، فعلى العميل أن لا يكون عرضةً للتصيد الإلكتروني ومحاولة الارتقاء بوعيه الرقمي بحيث يستطيع أن يساعد المصرف في الحفاظ على أموال من الانتهاك، كما يجب عليه

²⁹⁸ Zachary B. Omariba, Nelson B. Masese, Dr. G. Wanyambi, Ibid, page 439.

²⁹⁹ نور الدين كروش د. ليلي أوالد إبراهيم د. جمال دقيش، المرجع السابق، ص 165.

³⁰⁰ Azharuddin, LEGAL PROTECTION FOR USERS OF INTERNET BANKING CUSTOMERS FOLLOWING CHANGES IN INFORMATION AND ELECTRONIC TRANSACTIONS LAW, Jurnal Pembaharuan Hukum ,Vol VI, No.1, 2019, page 55.

³⁰¹ طلال عبد الكريم القرعان، أثر الخدمات المصرفية الإلكترونية في تعزيز ولاء العملاء للقطاع المصرفي الأردني، مجلة المتقال للعلوم الاقتصادية والإدارية وتكنولوجيا المعلومات، المجلد الثامن، العدد 1، الأردن، 2022م، ص 24.

أن يتبع الإجراءات التي وضعتها الدولة عندما يشك في أي نشاط غير عادي في حسابه لكي يستطيع المصرف والجهات المعنية اتخاذ مايلزم وتقليص الخسائر والأضرار كلما أمكن³⁰².

ونرى أن حاجة الحماية للعمليات المصرفية الإلكترونية تعد ضرورة حتمية وذات أثر مزدوج ومتقابل، قد يتعرض المصرف إلى انتهاك رقمي للأنظمة المشغلة مما يترتب عليها انتهاكا للبيانات الشخصية أو ضياع الفرص التجارية أو الاستثمارية على العميل، وهنا نجد أهمية وجوب بيان مسؤولية العميل والمصرف في الحالات المختلفة التي تتعرض الأنظمة الإلكترونية أثناء ممارسة العمليات المصرفية الإلكترونية، كما يتعين على النظام القانوني في الدولة تحقيق التوازن في حماية حق العميل في الحصول على تجربة مصرفية إلكترونية تمكنه من تحقيق غايته في اللجوء إلى إبرام معاملات إلكترونية وبين حق المصرف في عدم تحمل المسؤولية الناتجة عن خطأ العميل.

خلاصة القول، إن الأثر المباشر لحماية العمليات المصرفية الإلكترونية يدور بصفة أساسية حول المصرف والعميل، بحيث تسهم الحماية إلى دفع عجلة الابتكار والتحول الرقمي داخل القطاع المصرفي، بحيث تسعى المصارف إلى تعزيز قدرة الكادر البشري على فهم واستخدام التقنيات الحديثة لتوفير الحماية اللازمة للخدمات المصرفية التي تقدمها مما يعزز ثقة العملاء ورضاهم وذلك عند ضمان مزيد من الأمان والخصوصية لبياناتهم وحساباتهم³⁰³.

³⁰² شريف عبدالرحمن سيف النصر، المرجع السابق، ص10.

³⁰³ أحمد مصفى مندور، الأمن السيبراني للخدمات المالية والمصرفية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، ألمانيا، لاتوجد سنة نشر، ص8.

المطلب الثاني

الأثر غير المباشر لحماية العمليات المصرفية الإلكترونية

بعد بيان الأثر المباشر الناتج عن حماية العمليات المصرفية الإلكترونية على المصرف والعميل، يتابع الباحث في هذا المطلب بيان أثر الحماية غير المباشر على الدولة من خلال تسليط الضوء على النظام القانوني ومدى انعكاسه على حماية الحقوق الناشئة عن التعامل الرقمي في ظل النمو الاقتصادي في مملكة البحرين، كما سيبين مدى جدوى الحماية القانونية التي يوفرها النظام عبر بيان المؤشرات التي تثبت تطور القطاع المصرفي الإلكتروني واتساقه مع الخطة التنموية التي وضعتها مملكة البحرين، وفي هذا المطلب يوضح الباحث الأثر غير المباشر على الدولة من خلال فرعين.

- الفرع الأول: أثر حماية العمليات المصرفية الإلكترونية على الدولة.
- الفرع الثاني: انعكاس أثر الحماية على جذب الاستثمارات الأجنبية.

الفرع الأول

أثر حماية العمليات المصرفية الإلكترونية على الدولة

تؤثر حماية العمليات المصرفية الإلكترونية بشكل كبير على الدولة وعملية التنمية فيها، فعندما يكون القطاع المصرفي محمياً بشكل جيد تتحقق معه العديد من الفوائد، منها تعزيز التنمية الاقتصادية والاجتماعية، حيث تُحسن الأنظمة المالية ذات التطور العالي القدرة على الابتكار والنجاح فيه مما يؤدي إلى دفع عجلة النمو الاقتصادي بشكل ملحوظ وأسرع من الأنظمة التي لا تستخدم فيها أدوات الابتكار، علاوة على ذلك فإن ما يسبب تدهور هذه الأنظمة يقلل تبعاً من معدل النمو الاقتصادي، وبالتالي فإن الأنظمة المالية المبتكرة تنعكس على الإنتاجية والتنمية الاقتصادية³⁰⁴.

سيما أن أثر حماية العمليات المصرفية الإلكترونية يعود نفعاً بشكل غير مباشر على التنمية الاجتماعية للدولة، بحيث يتم تنمية الكوادر البشرية وخلق فرص العمل في مجالات عدة مثل الأمن السيبراني، وتطوير التكنولوجيا، والخدمات المالية، مما يساهم في مستويات التوظيف الإجمالية وتبين "مبادرة التنمية الرقمية التي أطلقها الاتحاد الأوروبي في عام 2017م تركيزها على أولويات أربع من ضمنها تعزيز المعرفة والمهارات الرقمية وخلق فرص العمل،³⁰⁵ وهذا يعد دليلاً واضحاً على جدوى تعزيز الأمن والحماية في تحقيق غايات الدولة.

نجد أن عديداً من الدول ركزت على بناء وتعزيز القدرات البشرية في مجال تقنية المعلومات وتوظيفها في القطاعات المختلفة من أجل الابتكار والمنافسة، بحيث يتم تبني الكوادر البشرية من خلال رفع قدرتها على التصدي للهجمات الإلكترونية التي تتعرض لها القطاعات ومن ضمنها القطاع المصرفي، كما تطور من مهاراتها من خلال الدورات التدريبية تحت إشراف جهات دولية مختصة، مع العلم يعد مجال تطوير الكوادر البشرية، ووضع السياسات والضوابط، وكذلك النظم التقنية الحديثة مكلف جداً ويستدعي ميزانية عالية تُخصص لهذه الأغراض، إلا أنه مقارنةً بالفوائد التي تعود على الدولة حين تشارك في الأسواق المفتوحة، وأخذ مكانة مالية مرموقة يرفع من قوتها المالية والاقتصادية على مستوى المنطقة والعالم، لاشك سيعيد في الأخير التكاليف مع أرباح إضافية على جميع الأصعدة³⁰⁶.

³⁰⁴ محمد صالح محمد غريب الكردي، تطور الخدمات المصرفية الإلكترونية ودورها في تنشيط التجارة المصرية، المجلة العلمية للدراسات والبحوث المالية والتجارية، جامعة دمياط، مصر، المجلد الرابع، العدد 1، الجزء الرابع، 2023م، ص8.

³⁰⁵ الأمم المتحدة، إدارة الشؤون الاقتصادية والاجتماعية، تقرير الأمم المتحدة مسح الحكومة الإلكترونية 2020 منشور على الرابط التالي: [Final Copy \(un.org\)](https://www.un.org/development/desa/dest/2020/) ص 77.

³⁰⁶ محمد اسماعيل، الأمن السيبراني في القطاع المصرفي، صندوق النقد العربي، موجز سياسات، العدد الرابع، 2019م، ص8.

وعليه، تحليلاً لما سبق فإن حماية العمليات المصرفية الإلكترونية قد يؤثر على المدى البعيد فيما يتعلق بالإنفاق الحكومي أي من ناحية توفير تكاليف تتحملها الحكومة في مواجهة الإلكترونية، مما يؤدي إلى التخفيف من مخاطر الجرائم المالية والهجمات الإلكترونية عن طريق تقليل الحاجة من الموارد واسعة النطاق لمعالجة حوادث الانتهاكات أو التعافي منها.

إن احتضان التقدم التكنولوجي وتعزيز الابتكار أمرٌ ضروريّ لنمو القطاع المصرفي، ونرى أن تركيز مملكة البحرين على الابتكار التكنولوجي واعتماد التقنيات المالية (fintech) يساهم في تعزيز القدرة التنافسية للقطاع وكفاءته³⁰⁷، وتسهم حماية العمليات المصرفية الإلكترونية في تحفيز اعتماد الخدمات المصرفية الرقمية، مما يعزز النمو الملحوظ في هذا القطاع والتزايد في الاستخدام والتفضيل للخدمات الإلكترونية على نظيرتها التقليدية، ولاشك أن البنوك الوطنية بدورها تساهم في إجمالي الدخل المحلي، فضلاً عن الزيادة المطّردة في العمليات المصرفية الإلكترونية والتي تؤدي إلى زيادة كفاءة إنتاجية البنوك مما ينعكس بشكل إيجابي على الأداء الاقتصادي العام³⁰⁸.

الجدير بالذكر أن العديد من القوانين المالية التي تخدم القطاع المصرفي الإلكتروني بشكل خاص تبين مدى اهتمام مملكة البحرين في التحول الرقمي، بما في ذلك ما يخدم قوانين الملكية الفكرية، التي قد تجد لها محلاً في حماية القطاع المصرفي بطريقة أو بأخرى ومثال على ذلك، ابتكار برامج وتطبيقات حاسوبية تخدم المصرفية الرقمية يتطلب قوانين حماية الملكية الفكرية لصاحب الابتكار.

إذ تحتل مملكة البحرين مراتب عالية في جاهزية الدولة للتحول الرقمي، وذلك استناداً لمؤشر تنمية الحكومة الإلكترونية الذي أطلقته الولايات المتحدة الأمريكية بشكل طارئ قبل عام 2030م، والمعني بتحقيق أهداف خطط التنمية المستدامة للدول وذلك نظراً لتقسي فايروس كوفيد-19 الذي أوجب على المجتمعات بذل مزيدٍ من الجهود لحماية الخصوصية والبيانات والتصدي للتحديات الناتجة عن المخاطر الرقمية، حيث احتلت مملكة البحرين المرتبة الثانية على مستوى دول الخليج العربي بعد دولة الإمارات العربية المتحدة في تصنيف مؤشر تنمية الحكومة الإلكترونية لعام 2020م لمجموع المؤشر المرتفع جداً³⁰⁹، كما أثبت التقرير الاقتصادي الفصلي للربع الأخير لمملكة البحرين الصادر عن وزارة المالية والاقتصاد الوطني في 2023م مساهمة القطاع المالي في الناتج المحلي، والذي حدد ارتفاعاً في نسبة التحويلات الإلكترونية بمعدل 15.6 عن الربع

³⁰⁷ مصطفى سالم عبد الرضا، حيدر محمد كرمي، «سنان عبدالله حرجان، التكنولوجيا المالية ودورها في تحقيق التنمية المستدامة، مجلة جامعة جيبها، العراق، المجلد الرابع، العدد 2، 2020م، ص134.

³⁰⁸ خولة بلحسن، المرجع السابق، ص29.

³⁰⁹ الأمم المتحدة إدارة الشؤون الاقتصادية والاجتماعية، تقرير الأمم المتحدة مسح الحكومة الإلكترونية، المرجع السابق، ص55.

الثاني، إذ قُدرت نسبة التحويلات الإلكترونية بمعدل 12.6³¹⁰، وهذا دليل واضح على توجه العملاء نحو الصيرفة الإلكترونية، وقدرة مملكة البحرين على توفير بيئة مصرفية رقمية قادرة على حفظ الحقوق المالية للأفراد فيها بقدر الإمكان.

يمكن القول إن استمرار تطوير التكنولوجيا وتوسع استخدام العمليات المصرفية الإلكترونية تؤثر بشكل غير مباشر على الدولة بشكل إيجابي، إذ إن رفع الحماية يؤدي إلى ثقة الأفراد في النظام المصرفي والتشجيع على زيادة استخدامها مما يؤدي في النهاية إلى زيادة الثقة في النظام المصرفي وتعزيز الاستقرار المالي للدولة، كما تُسهم الحماية في تقليل التكاليف وتحسين الكفاءة الاقتصادية من خلال توفير الوقت والجهد مما يدعم نمو الاقتصاد والتنمية، وأخيراً فإنه وبفضل النظم المصرفية الإلكترونية الآمنة يمكن للأفراد والمشاريع الحصول على خدمات إلكترونية بكفاءة أكبر مما يتيح فرصاً تنموية أعلى منعكسة على الابتكار والريادة في الأعمال التجارية.

الفرع الثاني

انعكاس أثر الحماية على جذب الاستثمارات الأجنبية

تشير الاستثمارات الأجنبية إلى توجيه رؤوس الأموال والموارد الاقتصادية من قبل مستثمرين أجانب نحو بلد معين، سواء كانت هذه الاستثمارات تتم في القطاع العام أو القطاع الخاص، ويعتبر جذب الاستثمارات الأجنبية أمراً هاماً للدول، حيث يمكن أن يُسهم في تعزيز النمو الاقتصادي وخلق فرص العمل بالإضافة إلى تنويع مصادر الدخل ونقل المعرفة والخبرة³¹¹، وفي إطار البحث عن الآثار الناتجة عن حماية العمليات المصرفية الإلكترونية، يثور التساؤل حول العلاقة بين الاستثمار الأجنبي والقطاع المصرفي المحمي قانوناً؟ وكيف يمكن للحماية القانونية أن تنعكس على جذب الاستثمارات الأجنبية سواء كانت مباشرة أو غير مباشرة؟

للإجابة على هذا التساؤل، سيقسم الباحث الموضوع إلى نقطتين أساسيتين، الأولى سيستعرض فيها أهمية الاستثمار الأجنبي على التنمية الاقتصادية للدولة المضيفة، ومن ثم كيفية استطاعة النظام القانوني البحريني جذب الاستثمار الأجنبي في ظل التطور التكنولوجي الحاصل على العمليات المصرفية واتساع الحدود الجغرافية والمنافسة الكبيرة في الأسواق المجاورة والعالمية.

³¹⁰ وزارة المالية والاقتصاد الوطني، التقرير الاقتصادي الفصلي لمملكة البحرين، الربع الثالث 2023م، مملكة البحرين، ص 11، التقرير منشور على الرابط التالي: [beq32023ar_v15_final.pdf \(mofne.gov.bh\)](https://www.mofne.gov.bh/beq32023ar_v15_final.pdf)،

³¹¹ Hussien Alasrag, Foreign Direct Investment Development Policies in the Arab Countries, Munich

Personal RePEc Archive, No.2230, 2005, page 6.

أولاً: أهمية الاستثمار الأجنبي على التنمية الاقتصادية:

الاستثمارات الأجنبية لها دور في تطوير النمو وتحقيق التنمية للدولة، حيث توجه المجتمع الدولي إلى استقطاب رؤوس الأموال الأجنبية من أجل تحقيق غايات اقتصادية، سياسية، اجتماعية وتنموية، لذلك نرى أن دولاً عدة اتجهت إلى تضمين خططها التنموية معايير قياسية من أجل توفير بيئة جاذبة للاستثمارات الأجنبية، التي بدورها تعزز من النمو الاقتصادي وخلق فرص العمل، بالإضافة إلى الإسهام في نقل التكنولوجيا للدولة المضيفة وتحسين البنية الاقتصادية المحلية³¹²، لذا فإن توفير بيئة استثمارية آمنة وجاذبة يعد دوراً محورياً يقع على عاتق الدولة لاستقطاب الاستثمارات الأجنبية. وتركيزاً على محور الدراسة فإن المجال المصرفي والمالي يتسم بالحساسية والمنافسة الدائمة فيه، لذلك عادةً ما تقدم الدول ضمانات وحوافز للمستثمرين الأجانب، تحت مظلة ما يسمى السياسة المتبعة للانفتاح الاقتصادي كي تجذب الاستثمار الأجنبي وتوجهه نحوها من خلال التسويق للقطاعات المختلفة بمزايا جديدة أو مختلفة عن نظيراتها من الدول، ومن هذه المزايا المقدمة: عدم وجود قيود على الاستثمار أو درجة من التقييد التي لا تمنع من حركات التبادل التجاري وحسن توفير الكفاءة الاقتصادية³¹³، مع العلم أن المصلحة المراد تحقيقها تكون مزدوجة، فالمستثمر الأجنبي على سبيل المثال يبحث عن أسواق في الدول النامية لتحقيق مزيد من الأرباح والتوسع التجاري، والدولة من الجانب الآخر تسعى لتحقيق أهداف متعددة إثر دخول الاستثمار في المنطقة، مما يسهم في رفع قوتها الاقتصادية³¹⁴.

تجد الدولة مزايا عديدة في دخول المستثمر الأجنبي إلى أسواقها منها³¹⁵:

- 1- عند إسهام المستثمر الأجنبي إما بشكل مباشر أو غير مباشر في تطوير القطاعات المختلفة، فعندما يمول المستثمر الأجنبي قطاعاً معيناً فإنه يعد أحد رؤوس الأموال التي تخدم هذا القطاع، وبالتالي ينعكس نمو القطاع وازدهاره على الدولة إيجاباً.
- 2- أضف إلى ذلك أن نجاح تجربة الاستثمار الأجنبي فيه يشكل سمعة جيدة تجذب استثمارات أخرى للدولة.

³¹² لحلال شهباز، أيت عيسى وسام، دور البنوك في التنمية الاقتصادية، رسالة ماجستير، جامعة عبدالرحمن ميرة، الجزائر، 2016م، ص47.

³¹³ فريد أحمد قبلان، الاستثمار الأجنبي المباشر في الدول العربية الواقع والتحديات، دار النهضة العربية، مصر، 2008م، ص23.

³¹⁴ إسمهان خاطر، دور التكامل الاقتصادي في تفعيل الاستثمار الأجنبي المباشر، رسالة ماجستير، جامعة محمد مخيضر، الجزائر، 2012-2013م، ص61.

³¹⁵ منصورية زعفران، فاطمة لعلي، دور الاستثمار الأجنبي المباشر في تحقيق التنمية الاقتصادية في الدول النامية، جامعة عبد الحميد بن باديس مستغان، الجزائر، 2018م، ص11، 12. بحث منشور على الرابط التالي [f16.pdf\(univ-mosta.dz\)](http://f16.pdf(univ-mosta.dz))

3- فضلاً عن النقلة التكنولوجية التي تسهم فيها الاستثمارات الأجنبية، مما يحسن تطوير المهارات واستخدام الآلات، وتعزيز انتاج المنتجات الموجودة والسعي نحو ابتكار منتجاتٍ جديدةٍ.

4- سيما أن جذب الاستثمارات الأجنبية نحو الدول قادرٌ على أن يساعد في الحد من البطالة وتغير في أرقام عدد العاطلين عن العمل في الدولة، إذ عندما يقوم المستثمر الأجنبي بفتح شركته في الدولة المستضيفة، تستطيع الدولة أن تقدم له من الحوافز في حالة توظيف العمالة الوطنية.

5- إن جذب الاستثمار الأجنبي نحو الدولة مع تقديم التسهيلات المناسبة يؤدي إلى تحقيق التكامل الاقتصادي، بحيث يمكن توجيه الاستثمارات والعائد منها نحو تطوير المرافق في البنية التحتية للدولة³¹⁶.

هنالك العديد من الإيجابيات نحو جذب الاستثمارات الأجنبية إلى الدولة غير المذكورة أعلاه، وتختلف من دولةٍ إلى أخرى على حسب محدداتها وتقارب الأهداف التي تصبو إليها كلاً من الدولة والمستثمر الأجنبي، ولكن في جميع الأحوال إن من أهم المحددات الجاذبة للمستثمر الأجنبي للخوض في الاستثمار خارج الدولة الأم وضوح النظام القانوني الذي يحميه من المخاطر المتعلقة بمشروعه، ففي مجال القطاع المصرفي الإلكتروني سيبحث عن الضمانات التي تكفل له إجراءات سهلة ومرنة لإبرام عمليات مصرفية إلكترونية ووسائل محمية بنظم قانونية واضحة بالإضافة إلى الوسائل الحديثة في حل النزاعات القانونية والأخذ بحجية المعاملات والتوقيعات الإلكترونية³¹⁷، ولذلك سنبين فيما يلي المساعي التي تتخذها الدولة من أجل جذب الاستثمارات الأجنبية نحوها كسوق جاذب بالتركيز على مملكة البحرين.

ثانياً: مساعي قانونية لجذب الاستثمارات الأجنبية:

يرتبط نجاح القطاعات المختلفة في الدولة بمتانة النظام القانوني فيها؛ حيث إن يكون المتطلب الرئيسي والعنصر الثابت الجدار القانوني الحامي لحقوق الأفراد والشركات في الدولة، فلا يمكن أن ينجح قطاعٌ معينٌ بمعزلٍ عن نجاح نظامه القانوني، وشهدت الدول تطوراً ملحوظاً في نسبة التحول نحو الاقتصاد الرقمي والاستفادة من العولمة في مجالات عديدة وربط الإنترنت في المعاملات اليومية في القطاعين الخاص والعام، إن توجه المستثمرين نحو الدولة المضيفة يستند إلى معايير وأسباب عديدة أهمها الاستفادة من الحوافز التي تقدمها الدولة المضيفة، وتجنب تقليل

³¹⁶ خالد عبدالله براك الحافي، تنظيم الاستثمار المصرفي في الفقه الإسلامي والقانون الوضعي، دار الفكر الجامعي، مصر، 2010م، ص 619.

³¹⁷ إسمهان خاطر، المرجع السابق، ص 90.

خطر المنافسة في الدولة الأم، والدخول في أسواق يكون فيها مقدار التكلفة أقل منها في الدولة الأم، وكل ذلك يكون وفق خطط مدروسة حول السوق المراد تقديم الخدمات المصرفية فيه، بما فيها مدى الحماية القانونية التي تحددها الدولة فلا يمكن أن يضع المستثمر الأجنبي أمواله وتكون عرضةً للانتهاك خاصة في ظل التطور التكنولوجي الحاصل، فيقف في مقدمة متطلبات النجاح في جذب الاستثمارات الأجنبية نحو القطاع المصرفي اليوم بناءً بُنية قانونية تحمي المجال التقني، من خلال وضع استراتيجيات تحدد أولويات تطوير السوق المصرفي الإلكتروني بحيث يواءم الدخول في الأسواق المحلية والعالمية والمنافسة مع وضوح الالتزامات والحقوق وانطباق معايير أمن وسلامة العمليات المصرفية الإلكترونية مع التوجهات الدولية المهمة بحماية مجال المصرفية الإلكترونية من خلال ربط الإجراءات التقنية بفعالية الوثائق القانونية ومدى حجيتها³¹⁸. إن توفير البنية التحتية الرقمية بما يواكب رؤية الدولة في تحقيق التنمية يجب أن يخطو نحو استراتيجيات مدروسة تسعى إلى مواكبة التحول الرقمي في تقديم الخدمات الإلكترونية، وهذا ماتسعى إليه الدول في طور التحول.

تُعد مملكة البحرين إحدى الدول الجاذبة للاستثمارات الأجنبية في العديد من القطاعات، إذ نرى نموذجاً من استقبال مملكة البحرين للبنوك الدولية منذ القرن الماضي، إذ يُعد بنك ستاندرد تشارترد أول بنك دولي مملكة البحرين في عام 1920م، حيث قدم خدماته المالية من استقبال وحفظ الأموال وتحويلها للأفراد والتجار، وتوالى دخول البنوك الأجنبية في المملكة عاماً بعد عام، إذ كانت مملكة البحرين من الدول السبّاقة في تطور القطاع المصرفي وتسعى دائماً إلى تطوير الجانب القانوني المتعلق بتوفير الخدمات المالية وملائمته للمتغيرات السوقية الدائمة في القطاع المصرفي العالمي من أجل حفظ حقوق الأفراد وحمايتهم من أي انتهاك يهدد استقرار مراكزهم المالية أو القانونية³¹⁹.

إن إرساء قواعد حماية صارمة للاستثمارات بكافة أنواعها، يُعد عنصراً محورياً من عناصر الجاذبية الاستثمارية للدول، وقد وضعت مملكة البحرين نموذجاً متميزاً في هذا المجال، ساهم في استقطاب العديد من البنوك والمستثمرين الأجانب على مر الأعوام، وبهدف جذب الاستثمارات الأجنبية إلى مملكة البحرين قدمت البحرين حزمة متكاملة من الضمانات والتسهيلات للمستثمرين الأجانب كالسماح بملكية المشروع بنسبة 100% للأجانب في العديد من المجالات كمجال خدمات

³¹⁸ عبدالمطلب عبدالحמיד، المرجع السابق، ص 313-315.

³¹⁹ يوسف صلاح الدين، لمحات من تاريخ العمل المصرفي في مملكة البحرين، جريدة أخبار الخليج، مملكة البحرين، العدد 16712، مارس 2023م.

تكنولوجيا المعلومات والسياحة وتملك الأراضي والعقارات³²⁰، ومن أبرز المساعي التي قامت بها مملكة البحرين لجذب الاستثمارات الأجنبية في جميع القطاعات هو توقيع الاتفاقيات الاستثمارية الثنائية التي بدورها تعزز من دور الاستثمار الأجنبي وخلق علاقات دولية سياسية واقتصادية، ومن أولى هذه الاتفاقيات كانت اتفاقية تشجيع الاستثمار بين الولايات المتحدة الأمريكية ومملكة البحرين، التي تمت المصادقة عليها في العام 1999م بحيث تعطي المستثمرين في مملكة البحرين من التسهيلات والمزايا لفتح مشاريعهم الاستثمارية في المملكة، والمعاملة الوطنية³²¹، كما قدمت مملكة البحرين مؤخراً ما يسمى الرخصة الذهبية في إبريل 2023م، كوسيلة لجذب المستثمرين الأجانب بتوفير الأولوية لمن يحمل الرخصة الذهبية والدعم من خلال تسهيل تراخيص البناء³²².

كما بينت أيضاً تقارير وزارة المالية والاقتصاد الوطني في مملكة البحرين نمواً في تدفق الاستثمارات الأجنبية المباشرة في مختلف القطاعات بمعدل 13.9 في الربع الثاني من العام 2023م بما يعادل 14.7 مليار دينار بحريني مقارنةً بعام 2022م، الذي بلغ فيه معدل الاستثمارات الأجنبية المباشرة 13 مليار دينار بحريني،³²³ وتوالى ارتفاع مؤشر جذب الاستثمارات الأجنبية في الربع الأخير من نفس العام إلى ما يعادل 15.9 مليار دينار بحريني وما يقارب زيادة سنويةً بمقدار 19.4، كما أحرزت مملكة البحرين مراتب عالميةً من ضمن تصنيف التنافسية الرقمية العالمية للعام 2023م الصادر عن المعهد الدولي للتنمية الإدارية، والمعني بمدة تبني الدول للتكنولوجيا الرقمية الحديثة، حيث حصلت مملكة البحرين على المرتبة 38 عالمياً من 64 دولة، كما جاءت مملكة البحرين في المراكز العشرة الأولى في عددٍ من المؤشرات الفرعية، كالمركز الثالث عالمياً ضمن مؤشر مهارات التكنولوجيا الرقمية، والمركز الخامس عالمياً ضمن مؤشر الأمن السيبراني³²⁴.

أما فيما يتعلق بمساعي الدول نحو جذب الاستثمارات الأجنبية، أطلقت دولة الإمارات العربية المتحدة مبادرةً عالميةً لجذب أفضل الكفاءات والشبكات الرقمية في العالم في إطار رؤيتها في الخمسين عام المقبلة بأن تكون الإمارات أفضل دولة في العالم، إذ تقوم فكرة هذه المبادرة على جذب الاستثمارات الأجنبية من خلال توفير حوافز وضمانات للمستثمرين الأجانب مع توفير

³²⁰ فريد أحمد قبيلان، المرجع السابق، ص 308.

³²¹ مرسوم بقانون رقم (37) لسنة 1999 بالتصديق على اتفاقية تشجيع الاستثمار وتوفير الحماية المتبادلة له بين حكومة دولة البحرين وحكومة الولايات المتحدة الأمريكية، مملكة البحرين.

³²² [Bahrain – Introduces a new "golden licence" to promote FDI | Investment Policy Monitor | UNCTAD](#)

[Investment Policy Hub](#)

³²³ وزارة المالية والاقتصاد الوطني، التقرير الاقتصادي الفصلي لمملكة البحرين، الربع الثاني 2023م، المرجع السابق، ص 21.

³²⁴ وزارة المالية والاقتصاد الوطني، التقرير الاقتصادي الفصلي لمملكة البحرين، الربع الثالث 2023م، المرجع السابق، ص 33.

الحماية اللازمة والسبل الميسرة لبدأ وتسيير مباشرة الأعمال ؛حيث إن نجاح دولة الإمارات العربية المتحدة كمركزٍ ماليٍّ مستقرٍ قادرٍ على جذب الاستثمارات الأجنبية في جميع القطاعات ومن بينها القطاع المصرفي، والذي سيصب في الأخير في مصلحة الدولة نحو تحقيق أهدافها الاقتصادية³²⁵.

³²⁵ مقال بعنوان مبادرة عالمية لجذب أفضل الكفاءات والشركات الرقمية في العالم، وزارة الاقتصاد، المركز الإعلامي، الامارات العربية المتحدة، 6 يوليو 2022م.

المطلب الثالث

تطبيقات عملية لقضايا انتهاك عمليات مصرفية إلكترونية

تُعد قضايا انتهاك العمليات المصرفية الإلكترونية من التحديات الرئيسية التي تواجه المؤسسات المالية والمستهلكين على حد سواء، وقد شهد القطاع المصرفي العديد من الحوادث البارزة التي أدت إلى خسائر مالية وأضرار بالسمعة للمؤسسات بشكل مباشر، لذلك في هذا المطلب سيتم تسليط الضوء على حالتين واقعتين لانتهاكات حدثت للعمليات المصرفية الإلكترونية والأجهزة المصرفية، من خلال تحليل كيفية وقوع الجرائم والآثار المترتبة عليها وردود الفعل التنظيمية، حيث سنطرح بداية قضية خرق بيانات شركة Target عام 2013م، ومن ثم سناقش قضية خرق بيانات وكالة الائتمان Equifax عام 2017م وذلك فيما يلي:

1- القضية الأولى شركة Target Corporation

تعتبر إحدى الحالات المحورية التي تنطوي على انتهاك للعمليات المصرفية الإلكترونية هي خرق البيانات المستهدفة لعام 2013م. وتعد هذه الحادثة واحدة من أهم حالات الاحتيال عبر الإنترنت وسرقة بيانات بطاقة الائتمان وأكثرها شهرة:³²⁶

وصف الجريمة وكيفية تنفيذها:

في نوفمبر وديسمبر من عام 2013م، تمكن مجرمو الإنترنت من الوصول غير المصرح به إلى شبكة الكمبيوتر الخاصة بشركة Target.

قام المهاجمون ب تثبيت برامج ضارة على أنظمة نقاط البيع (POS) الخاصة بشركة Target، والتي تم تصميمها لجمع ونقل بيانات بطاقة الدفع، استهدفت البرامج الضارة على وجه التحديد الشريط المغناطيسي لبطاقات الائتمان والخصم التي يستخدمها العملاء أثناء المعاملات.

الأضرار التي لحقت بالعملاء والشركة:

تم اختراق المعلومات الشخصية، بما في ذلك الأسماء والعناوين وأرقام الهواتف وعناوين البريد الإلكتروني، لما يقرب من 40 مليون عميل مستهدف.

Krebs, Brian. "Target Hackers Broke in Via HVAC Company." Krebs on Security, 14 Feb. 2014, ³²⁶

<https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>

تمت سرقة معلومات بطاقات الائتمان والخصم، بما في ذلك أرقام البطاقات ورموز CVV، لنحو 70 مليون عميل، وكانت الخسائر المالية لكل من العملاء المتأثرين والبنوك المصدرة كبيرة بسبب المعاملات الاحتيالية وتكلفة إعادة إصدار البطاقات.

الإجراءات المتخذة:

- 1- استجابت شركة Target عن طريق إخطار وكالات إنفاذ القانون على الفور وتعيين فريق أدلة جنائية رائد من طرف ثالث للتحقيق في الانتهاك.
- 2- تم تحديد أنظمة نقاط البيع المخترقة وإزالتها من شبكة Target.
- 3- تم تقديم خدمات مجانية لمراقبة الائتمان للعملاء المتأثرين، وعملت شركة Target على تعزيز إجراءاتها الأمنية بما فيها إعادة تعيين كلمات مرور 445000 موظف ومقاول.

العواقب القانونية:

واجهت شركة Target العديد من الدعاوى القضائية من العملاء والمؤسسات المالية والمساهمين المتأثرين.

في عام 2017م، وافقت شركة Target على تسوية مطالبات المستهلكين عن طريق دفع 18.5 مليون دولار في صندوق للمستهلكين المتضررين، بالإضافة إلى ذلك، قامت شركة Target بالتسوية مع Visa مقابل 67 مليون دولار لتعويض البنوك عن التكاليف المتعلقة بالانتهاك، وأدى الحادث إلى زيادة الوعي بقضايا الأمن السيبراني ودفع الشركات الأخرى إلى تعزيز تدابيرها الأمنية.

العواقب التنظيمية:

يُعد خرق البيانات المستهدفة بمثابة مثال صارخ على التأثير الكبير والعواقب واسعة النطاق التي يمكن أن تتجم عن انتهاك العمليات المصرفية الإلكترونية. وشدد على أهمية تدابير الأمن السيبراني القوية ودفع إلى زيادة الجهود لحماية بيانات المستهلك في العصر الرقمي.

لم تكن الاستجابة الأولية لصد الهجوم هي الأفضل من قبل الشركة، فقد تجاهلت التحذيرات المبكرة ثم انتظرت بضعة أيام لإبلاغ الجمهور، وجاءت هذه الخسائر في المقام الأول بسبب التوقيت السيئ، وحيث بدأ الاختراق في أواخر شهر نوفمبر ولم يتم حله حتى منتصف شهر ديسمبر، وهذه الفترة من السنة هي قلب موسم التسوق في العطلات، ولم تتمكن شركة Target من توجيه اهتمامها الكامل نحوها وأدى تأخر الاحتواء والتنبيه إلى جعل Target يبدو غير جدير

بالثقة وأثار غضب العديد من العملاء وسط موسم التسوق في العطلات، وكان من الممكن احتواء الحادث بأكمله من خلال الرد على التهديد أو التحقق منه على الفور.

كما أن الشركة كانت تستخدم أسلوب التدفق في خوادم أساسية، مما صعب من مهمة الشركة على احتواء الهجوم وفصل الأجهزة، وكان من أهم التغييرات التي تبعت هذا الهجوم هو اختيار الأسلوب المعماري للشبكات الكبيرة إلى تقسيمها لشبكات فرعية منفصلة بما يساعد في تدفق البيانات بشكل أفضل وعزل المشكلات قبل أن يتمكن المهاجمون من الإضرار بالنظام بأكمله، كما نبه التغيير مخاطر السماح للأطراف الثالثة الدخول إلى شبكات الشركة والوصول إلى البيانات الخاصة بالعملاء³²⁷.

2- القضية الثانية خرق بيانات Equifax (2017)

شهد عام 2017م إحدى أكبر حوادث خرق البيانات في التاريخ، عندما تعرضت وكالة الائتمان الأمريكية Equifax لاختراق هائل أسفر عن تسريب بيانات شخصية حساسة لما يقرب من 147 مليون مستهلك، وكان لهذه الحادثة انعكاسات واسعة النطاق على الأفراد والمؤسسات المالية، فضلاً عن دفع المشرعين نحو سن قوانين أكثر صرامة لحماية البيانات:³²⁸

وصف الجريمة وكيفية تنفيذها:

في عام 2017م، عانت Equifax، إحدى أكبر وكالات إعداد التقارير الائتمانية، من اختراق هائل للبيانات أدى إلى كشف معلومات شخصية حساسة لحوالي 147 مليون مستهلك إذ حدث الاختراق بسبب ثغرة أمنية في إطار عمل تطبيق الويب Apache Struts، والتي فشلت شركة Equifax في تصحيحها في الوقت المناسب.

استغل مجرمو الإنترنت هذه الثغرة الأمنية للوصول غير المصرح به إلى قاعدة بيانات Equifax، حيث قاموا باستخراج الأسماء وأرقام الضمان الاجتماعي وتواريخ الميلاد والعناوين، وفي بعض الحالات، أرقام رخص القيادة ومعلومات بطاقة الائتمان.

³²⁷ David Lukic , Target Data Breach, How Target Almost Lost Everything, 2020, article published

on: [Target Data Breach: How Was Target Hacked? – IDStrong](https://www.idstrong.com/target-data-breach-how-was-target-hacked/)

³²⁸ Federal Trade Commission. "Equifax to Pay \$700 Million for 2017 Data Breach." FTC, 22 July

2019, <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-700-million-2017-data-breach>

الأضرار التي لحقت بالضحايا:

- 1- أدى الانتهاك إلى إلحاق أضرارٍ ماليةٍ جسيمةٍ وأضرارٍ بسمعة كل من Equifax والعملاء المتضررين.
- 2- واجه الأفراد مخاطر متزايدة لسرقة الهوية، وتطبيقات بطاقات الائتمان الاحتيالية، وغيرها من أشكال الاحتيال المالي.
- 3- كما عانت المؤسسات المالية التي اعتمدت على تقارير Equifax الائتمانية من خسائر حيث اضطرت إلى التعامل مع زيادة في الأنشطة الاحتيالية.

الإجراءات المتخذة:

- 1- اتخذت شركة Equifax خطوات لاحتواء الاختراق، وكلفت شركة للأمن السيبراني للتحقيق في مدى الاختراق.
- 2- قدمت الشركة خدمات مجانية لمراقبة الائتمان وحماية سرقة الهوية للأفراد المتضررين.
- 3- كان على المؤسسات المالية والبنوك التي تعتمد على Equifax لإعداد التقارير الائتمانية تعزيز إجراءات الكشف عن الاحتيال ومنعه.

العواقب القانونية:

واجهت Equifax العديد من الدعاوى القضائية من المستهلكين والمؤسسات المالية والجهات التنظيمية المتضررة، في يوليو 2019م، توصلت Equifax إلى تسوية مع لجنة التجارة الفيدرالية (FTC)، ومكتب الحماية المالية للمستهلك (CFPB)، و 50 ولاية وإقليمًا أمريكيًا. وتضمنت التسوية صندوقًا بقيمة 300 مليون دولار لتعويض المستهلكين ومراقبة الائتمان، بالإضافة إلى تغييرات كبيرة في ممارسات أمان البيانات في Equifax كما واجهت الشركة أيضًا إجراءات قانونية وتنظيمية في بلدان أخرى تأثر فيها الأفراد.

العواقب التنظيمية³²⁹:

أدى خرق Equifax إلى زيادة التدقيق والدعوات، وإلى وضع لوائح أقوى لحماية البيانات، كما أفضى ذلك إلى مناقشات حول الحاجة إلى معايير أكثر صرامة للأمن السيبراني لوكالات إعداد التقارير الائتمانية والكيانات الأخرى التي تتعامل مع معلومات المستهلك الحساسة.

³²⁹ Josh Fruhlinger, Equifax data breach FAQ: What happened, who was affected, what was the impact?, 2023, article published on: [Equifax data breach FAQ: What happened, who was affected, what was the impact? | CSO Online](#)

لم تنجح الشركة في الاستجابة السريعة لصد الهجوم على الأنظمة وخرق البيانات خصوصاً أن الإعلان عن كشف الاختراق استغرق شهراً منذ حدوث الحادثة، وكان المهاجمون نشطاء لما يقارب من 76 يوماً دون أن يتم اكتشافهم.

إهمال الموظفين المسؤولين في الشركة عن تصحيح الثغرات الأمنية من أجل الحفاظ على الأنظمة من الاختراق الإلكتروني والعمل على تجديد الاشتراكات الأمنية، التي تبين فيما بعد أن عديداً من الهجمات التالية التي وصلت إلى قاعدة البيانات كان بسبب ضعف أمن نظام التشفير الإلكتروني الذي يجب تجديده سنوياً من قبل أطراف ثالثة والذي كان منتهياً منذ عشرة شهور قبل الحادثة.

سلط خرق بيانات Equifax الضوء على الأهمية الحاسمة للتصحيح الأمني في الوقت المناسب وممارسات الأمن السيبراني القوية، خاصةً بالنسبة للمؤسسات التي تتعامل مع كميات هائلة من المعلومات الشخصية الحساسة. كما شدد على الحاجة إلى لوائح أقوى لحماية خصوصية الأفراد ومحاسبة الشركات على حماية البيانات الحساسة.

تكثر القضايا التي يتم فيها انتهاك بيانات الأفراد وحساباتهم، وقد تطل أموالهم، وتختلف أغراض الانتهاك من قضية إلى أخرى، إذ يكون الانتهاك في بعض الأحيان لأغراض عامة سياسية مثلاً، أو شخصية تعود لأهداف المنتهك نفسه، كسرقة الأموال أو بيع البيانات واستخدامها لأغراض غير مشروعة، وبالتالي على الجهات التي تتعامل إلكترونياً أن تستعين بالتدابير اللازمة لحماية نفسها وحماية العملاء والحفاظ على الأموال والبيانات من أي اختراق محتمل، ويمكن معالجة قضايا انتهاك عمليات المصرفية الإلكترونية والتي تعد قضايا هامة تشكل تحدياً للأفراد والمؤسسات، معظم الناس اليوم تتعامل مع خدمات مصرفية عبر الإنترنت في حياتهم اليومية، ولذلك يمكن أن تظهر قضايا مثل الاحتيال الإلكتروني وسرقة الهوية، وعليه فيما يلي بعض التطبيقات العملية لمعالجة قضايا انتهاك عمليات المصرفية الإلكترونية³³⁰:

1- نظم الحماية من الاحتيال:

تطوير وتحسين نظم الكشف عن الاحتيال لمراقبة وتحليل نماذج السلوك والتحقق من المعاملات غير المعتادة، كما يتم استخدام التحقق الثنائي لتعزيز الأمان، مثل رموز التحقق الثنائي (OTP) والبصمة الرقمية.

³³⁰ Bank for International Settlements, Basel Committee on Banking Supervision, 2000, "Electronic Banking Group Initiatives and White Papers," October (Basel); <http://www.bis.org/publ/bcbs76.htm>

2- التوعية والتدريب:

يتم إعداد خططٍ تساعد على توعية العملاء بشكل مستمرٍ ودوريٍ حول كيفية تحديد وتجنب الاحتيال الإلكتروني، إلى جانب تنظيم الورش من أجل تدريب الموظفين على أجدد طرق الانتهاكات وكيفية التصدي لها واحتوائها وكيفية التعامل معها³³¹.

3- تكنولوجيا الذكاء الاصطناعي: (AI)

استخدام تقنيات الذكاء الاصطناعي للكشف المتقدم عن أنماط السلوك غير الطبيعية والاحتمالات العالية للاحتيال، فضلاً عن تحليل البيانات بشكلٍ فوريٍ للكشف عن أنشطة غير معتادة³³².

4- التشريعات والتنظيم:

تطوير وتنفيذ تشريعاتٍ قويةٍ لحماية المستهلكين والشركات من جرائم الاحتيال الإلكتروني، وتشديد الرقابة وتوفير إطارٍ تنظيميٍ للمؤسسات المالية لضمان أمان البيانات المصرفية³³³.

5- تقنيات التشفير:

استخدام تقنيات التشفير القوية لحماية بيانات العملاء والمعاملات المالية عبر الإنترنت، وتطبيق تقنيات التشفير للاتصالات بين العملاء والبنوك.

6- الإبلاغ والتحقيق:

إنشاء آلياتٍ فعالةٍ للإبلاغ عن أي انتهاكات ومشكلات في العمليات المصرفية الإلكترونية، وتكوين فرق تحقيقٍ متخصصةٍ لمعالجة حالات الاحتيال وتعقب المتورطين³³⁴.

7- التحديث الدوري:

تحديث وترقية الأنظمة بشكل دوري لمواكبة أحدث التقنيات وتحسين الحماية.

³³¹ أحلام بلجودي، متطلبات الأمن القانوني في مجال الخدمات المصرفية الإلكترونية، كتاب جماعي بعنوان أثر التطور التكنولوجي على القانون معهد جامعة فلسطين لأهلية، فلسطين، لا توجد سنة نشر، ص44.

³³² خير الدين بوزرب، هبة سحنون،، الذكاء الاصطناعي وتطبيقاته في القطاع المصرفي، كتاب جماعي بعنوان: تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، لا توجد سنة نشر، ص157.

³³³ العمليات المصرفية الإلكترونية والإطراف الإشرافي، صندوق النقد العربي، تقرير منشور، 2019م ص68.

³³⁴ [العمليات المصرفية الإلكترونية | صندوق النقد العربي \(amf.org.ae\)](http://amf.org.ae)

³³⁴ بغداد شامبي، المرجع السابق، ص244.

تحليلاً لما سبق، فإنه في القضيتين الأنفتي الذكر، يتبين أن المخاطر السيبرانية التي قد تتعرض لها الجهات العامة أو الخاصة ترتبط في عاملٍ مشتركٍ واحدٍ وهو ضعف الأمن الإلكتروني للنظم المستخدمة، ويختلف ضعف الأمن باختلاف العوامل المسببة، فأحياناً يكون السبب الفعلي هو إهمال الموظف المختص، أو يكون بسبب العميل نفسه الذي تصفح مواقع مشبوهة أدت إلى سرقة أمواله أو بياناته، وكما تم ذكره سابقاً، فإن المسؤولية القانونية تختلف على حسب النظام القانوني الذي يحكم المسألة المنظورة، إذ أخذت بعض الدول بمسؤولية البنك المهنية والتي تحتم عليه تعويض الأضرار الناتجة عن الانتهاك الرقمي، في حين أن البعض الآخر ضيق من قيام مسؤولية البنك إلا في حالة خطأ العميل أو السبب الأجنبي³³⁵.

نرى أن العامل المؤثر في القضيتين السابقتين، هو فشل الجهتين بالتنبؤ بحدوث الانتهاك الرقمي من جهة أولى، وعدم قدرتهم على احتواء الأضرار بشكل أسرع لتقليل الخسارة بقدر الإمكان من جهة ثانية، ولذلك من خلال دراسة موضوع البحث وبالأخص بعد النظر في القضيتين السابقتين، توصل الباحث إلى وسيلةٍ تستطيع فيها الجهة المتعرضة للانتهاك الرقمي العمل بها للحد من الخسارة أو تلافيها، وسيتم طرحها فيما يلي:

لكي يستطيع المصرف أو الجهة المعنية تفادي الانتهاك وتوفير الحماية اللازمة كجهة وللعامل على حدٍ سواء، عليها أولاً أن تعتمد فكرة التنبؤ بالمخاطر، وهي وسيلةً استباقيةً تُسهم في الحد من الأضرار الناتجة عن المخاطر التي تتعرض لها المؤسسة، وهذه الفكرة يتم استخدامها في عديدٍ من المجالات التي تمتاز بحجم المخاطر فيها، وأثبتت نجاحها في عديدٍ من الحالات، فمثلاً نجد في مجال تنظيم الإفلاس في فرنسا، أعطى القانون الفرنسي الحق لمراقب الحسابات في الشركة أن يتقدم بطلب أمام المحكمة بإعادة التنظيم نتيجة لطبيعة عمله، وذلك عندما يتبين له بوادر صعوبات نتيجة لطبيعة عمله التي تمكنه استخلاص الصعوبات الاقتصادية والمالية، بحيث إن هذه الصعوبات تتضح بالتدقيق في الأمور المالية التابعة لعمل الشركة³³⁶، ويمكننا إسقاط هذه الفكرة لخدمة موضوع الدراسة على النحو الآتي:

1- تكوين فرق عملٍ مختصةٍ بالأمن السيبراني لفحص وقياس المؤشرات غير الطبيعية في الممارسات الإلكترونية في العمليات التي تتم من قبل العملاء والموظفين، ويمكن استخدام تطبيقات الذكاء الاصطناعي للتحسس.

³³⁵ إيلاف فاخر كاظم، المرجع السابق، ص 134-136.

³³⁶ عبدالعزيز بوخرص، التوجهات الجديدة في قوانين الإفلاس الحديثة: رؤية اقتصادية بإفكار قانونية جديدة، مجلة كلية القانون الكويتية العالمية، الكويت، 2019م، العدد 4 ملحق خاص، ص 441.

2- عند اكتشاف الانتهاك يتم إبلاغ الجهات المعنية فوراً وإيقاف الجهاز المنتهك للحد من الأضرار.

3- العمل بشكلٍ دوريٍّ على تحديث النظم التقنية وتصليح الخلل التقني.

4- فصل الأجهزة الفرعية عن الأجهزة الرئيسية لمنع وصول الانتهاك في حالة حدوثه.

5- تعاون الجهات المختصة في تقديم المعلومات الخاصة بالمنتهاك لتسهيل الوصول إليه ومحاسبته (قيام المصرف بإعلام المصرف المركزي فوراً بالانتهاك وتعاون فريق الأمن السيبراني في البحرين على توفير المساعدة اللازم للوصول إلى المعلومات المتعلقة بالمنتهاك ومن ثم جمع العمليات النمطية لمنع ارتكاب انتهاكٍ آخر على مصارف أخرى).

في الختام يُبرز هذا المطلب أهمية تطبيق تدابير أمنية فعالة ومراقبة مستمرة للتهديدات من أجل حماية سرية وسلامة العمليات المصرفية الإلكترونية، كما يسلط الضوء على ضرورة وضع أطر تنظيمية أكثر صرامة لضمان المساءلة وتعزيز الشفافية. تُظهر الحالات المذكورة الآثار واسعة النطاق التي يمكن أن تتجم عن عدم كفاية تدابير الأمان، مما يدل على الحاجة إلى نهج شاملٍ واستباقيٍّ لإدارة مخاطر الجرائم الإلكترونية، وبيان أهمية هذه التطبيقات إلى حدٍ ما في تحسين أمان العمليات المصرفية الإلكترونية، والحد من تأثير الاحتيال والانتهاكات التي تطال العمليات المصرفية الإلكترونية، بقصد خلق بيئةٍ آمنةٍ إلكترونياً، خصوصاً أن غالبية الأعمال المصرفية اليوم تنفذ إلكترونياً، فلا بد من حماية العمليات المصرفية الإلكترونية بكافة الطرق التقنية والقانونية ومحاسبة من ينتهك خصوصية هذه العمليات وسرقة الأموال أو البيانات التي تحتويها.

الخاتمة:

باختتام الدراسة، يُظهر البحث أن العمليات المصرفية الإلكترونية تُعد جزءاً حيوياً من النظام المالي الحديث، ورغم مزاياها العديدة فإنها تواجه تحديات أمنية سيبرانية كبيرة، وقد أظهرت القوانين والآليات القانونية المتبعة في مملكة البحرين ودولة الإمارات العربية المتحدة جهوداً كبيرة في تعزيز الأمان وحماية العمليات المصرفية الإلكترونية، ولهذا سنتناول أبرز النتائج والتوصيات:

أولاً: النتائج:

1. إن الأثر المباشر لحماية العمليات المصرفية الإلكترونية يدور بصفة أساسية حول المصرف والعميل بحيث تسهم الحماية إلى دفع عجلة الابتكار والتحول الرقمي داخل القطاع المصرفي بحيث تسعى المصارف إلى تعزيز قدرة الكادر البشري على فهم واستخدام التقنيات الحديثة لتوفير الحماية اللازمة للخدمات المصرفية التي تقدمها مما يعزز ثقة العملاء ورضاهم وذلك عند ضمان مزيداً من الأمان والخصوصية لبياناتهم وحساباتهم.
2. إن أمن العمليات المصرفية الإلكترونية هو ببساطة ما يتحقق به حماية مصالح الأفراد المالية، فكل فرد يريد أن يحمي أمواله الخاصة من أي اعتداء ويرى الأفراد المصارف ملجأً آمناً لحفظ الأموال وبالتالي يلجأ إلى المصرف باعتباره محل ثقة، حيث استمدت هذه الثقة من ثقة الفرد في الدولة التي أعطت الجهاز المصرفي تصريحاً بممارسة العمل المصرفي، وبالتالي فإن دور الحكومة يمتد ليحقق نزاهة النظام المالي بأكمله وتحقيق الثقة في ممارسة العمليات المصرفية الإلكترونية أسوة بالثقة الموجودة للنقد الورقي في الوقت الحالي.
3. يرتبط مفهوم الوفاء في القانون المدني بالدفع في القانون التجاري، وذلك لاتحاد نتيجتي الوفاء والدفع ألا وهي إبراء الذمة المالية للمدين بعد السداد .
4. يُعد المشرع الإماراتي والمشرع المصري أكثر شمولاً وتحديثاً بخصوص تدابير الأمن السيبراني، مما يعزز من الحماية القانونية للعمليات المصرفية الإلكترونية في العديد من الأوجه، على عكس نظيرهما المشرع البحريني الذي لم يتطرق للتدابير السيبرانية والإجراءات ذات الصلة بالعمليات المصرفية الإلكترونية بشكل تفصيلي.
5. إن تنامي تطور وأتمتة العمليات المصرفية وترباطها مع المجالات المختلفة كالتجارة الإلكترونية رتب على المصارف التزامات جديدة لم تكن موجودة أثناء استعمال العمليات المصرفية التقليدية ناتجة من المخاطر التي تتعرض لها العمليات جراء التعامل الرقمي.

ثانياً: التوصيات:

1. من الضروري أن تكون هناك أداة قانونية تلزم المؤسسات الحكومية والخاصة بما يشمل المؤسسات المصرفية بضرورة إبلاغ المركز الوطني للأمن السيبراني عند حدوث أي هجوم إلكتروني، وعند ثبوت إهمال الجهة المتعرضة للخطر تتعرض لجزاءات إثر هذا الإهمال الذي قد يكبد القطاع المالي أضراراً من الصعب تداركها، وتشكل تهديداً لاستقرار القطاع المالي على المستوى المحلي أو المستوى العالمي.
2. على المشرع البحريني أن يحذو حذو المشرع الأردني في إلزام المصارف بنشر التوعية لعملائها كأحد سبل تعزيز التعاون في خلق بيئة مصرفية إلكترونية آمنة، إذ يسهم الوعي الإلكتروني في الحد من الخسائر الناجمة عن الانتهاكات التي قد تطال العمليات المصرفية الإلكترونية.
3. إنشاء هيئة مستقلة تُعنى بالرقابة على الأعمال التي تتخذ شكل العمليات المصرفية بين الأفراد تجاراً أو غير تجارٍ، وإن تمت ممارستها من جهة لا تباشر عمل المصارف بدورها على وجه الاحتراف وعندها سيتحقق معها الحماية القانونية المطلوبة لاستقرار المراكز القانونية.
4. ضرورة وجود اجتماعات تنسيقية دورية بين الجهات الداخلة في الاختصاص من بينها السلطتين التشريعية والتنفيذية، البنك المركزي، المؤسسات المصرفية، الهيئة المختصة بالأمن السيبراني للبحث في أهم التطورات الطارئة على موضوعات القطاع المصرفي الإلكتروني بما يخدم رؤية الحكومة ويمكن الاستفادة من الذكاء الاصطناعي في تحسس وتيرة الأنشطة غير الاعتيادية في البرامج الخادمة مما يسهل التصدي.
5. ضرورة وجود هيئة تسعى إلى سن تشريع ينظم السيبرانية في القطاع المصرفي في قانون منفصل على أن يحتوي التشريع على عناوين رئيسية تضم أهم مواضيع العمليات المصرفية الإلكترونية مثل، التعريفات الخاصة بالأمن السيبراني، المخاطر السيبرانية، سبل الحماية للعمليات المصرفية الإلكترونية، حقوق والتزامات الأطراف، المسؤولية القانونية.

قائمة المراجع

أولاً: المراجع باللغة العربية

الكتب:

- 1- إبراهيم سيد أحمد، الاقتصاد الإلكتروني، المكتبة العصرية، مصر، 2010م.
- 2- أحلام بلجودي، متطلبات الأمن القانوني في مجال الخدمات المصرفية الإلكترونية، كتاب جماعي بعنوان أثر التطور التكنولوجي على القانون معهد جامعة فلسطين الأهلية، فلسطين، لا توجد سنة نشر.
- 3- الأكاديمية المالية، أساسيات إدارة المخاطر في الخدمات المالية، الأكاديمية المالية أساسيات إدارة المخاطر في الخدمات المالية، مكتبة الملك فهد الوطنية، المملكة العربية السعودية، 1442هـ،
- 4- أنور العمروسي، صور انقضاء الالتزام في القانون المدني، دار الفكر الجامعي، مصر، الطبعة الأولى، 2004م.
- 5- إيلاف فاخر كاظم علي، مخاطر العمليات المصرفية الإلكترونية، المركز العربي للنشر والتوزيع، مصر، 2019م.
- 6- أيمن عبدالله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2014م.
- 7- بلال عبدالمطلب بدوي، البنوك الإلكترونية ماهيتها معاملاتها والمشاكل التي تثيرها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003، ص1952.
- 8- جاسم علي سالم الشامسي، تطبيقات المسؤولية المدنية المصرفية في قضاء المحكمة الاتحادية العليا ومحكمة تمييز دبي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الرابع، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م.
- 9- حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الإلكترونية، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2003م.
- 10- خالد عبدالله براك الحافي، تنظيم الاستثمار المصرفي في الفقه الإسلامي والقانون الوضعي، دار الفكر الجامعي، مصر، 2010م.
- 11- خير الدين بوزرب، هبة سحنون، الذكاء الاصطناعي وتطبيقاته في القطاع المصرفي، كتاب جماعي بعنوان: تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات

- الأعمال المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين،
لاتوجد سنة نشر.
- 12- نكري عبدالرزاق محمد، النظام القانوني للبنوك الإلكترونية، دار الجامعة الجديدة، مصر،
2010م.
- 13- سعيد أحمد شعله، قضاء النقص المدني في المسؤولية والتعويض، مجموعة القواعد القانونية
التي قررتها محكمة النقص خلال اثنين وسبعين عاما 1931-2005، المركز القومي
للإصدارات القانونية، مصر، 2007م.
- 14- سعيد عبدالله الحامز، العمليات المصرفية الإلكترونية والإطار الإشرافي، مؤتمر الأعمال
المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة
تجارة وصناعة دبي، 2003م.
- 15- سليمان ضيف الله الزين، التحويل الإلكتروني للأموال ومسئولية البنوك القانونية، دار
الثقافة للنشر والتوزيع، مصر، الطبعة الأولى، 2012م.
- 16- السيد عبدالوهاب عرفة، المسؤولية المدنية في ضوء الفقه وقضاء النقص، المكتب الفني
للموسوعات القانونية، مصر، المجلد الثاني، لاتوجد سنة نشر.
- 17- شريف أحمد الطباخ، المسؤولية المدنية التقصيرية والعقدية، دار الفكر والقانون، مصر،
الطبعة الأولى، الجزء الأول، 2009م.
- 18- شيرين سلطان، التنظيم القانوني للمعاملات المصرفية الإلكترونية في ضوء السياسة النقدية
للدولة، دار الجامعة الجديدة للنشر، مصر، 2020م.
- 19- شيرين سلطان، التنظيم القانوني للمعاملات المصرفية الإلكترونية في ضوء السياسة النقدية
للدولة، دار الجامعة الجديدة للنشر، مصر، 2020م.
- 20- صلاح الدين حسن السيسي، القطاع المصرفي والاقتصاد الوطني، عالم الكتب، مصر،
2003م.
- 21- صلاح زين الدين، دراسة اقتصادية لبعض مشكلات وسائل الدفع الإلكتروني، مؤتمر
الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة،
غرفة تجارة وصناعة دبي، 2003م.
- 22- عبدالرحمن السيد قرمان، عمليات البنوك وفقا لقانون التجارة الجديد، الطبعة الثانية، دار
النهضة العربية، مصر، 2000م.
- 23- عبدالمطلب عبدالحميد، اقتصاديات تكنولوجيا الخدمات المصرفية، الشركة العربية المتجددة
للتسويق، مصر، 2010م.

- 24- علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية دراسة للقضاء المصري والمقارن وتشريعات البلاد العربية، المكتبة القانونية، مصر، 1993م.
- 25- علي جمال الدين عوض، عمليات البنوك من الوجهة القانونية، المكتبة القانونية، مصر، 1993م.
- 26- فريد أحمد قبلان، الاستثمار الأجنبي المباشر في الدول العربية الواقع والتحديات، دار النهضة العربية، مصر، 2008م.
- 27- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، مصر، 2007م.
- 28- محمود أحمد ابراهيم الشرقاوي، مفهوم الأعمال المصرفية الإلكترونية وأهم تطبيقاتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م.
- 29- محمود أحمد الشرقاوي، مفهوم العمليات المصرفية الإلكترونية وأهم تطبيقاتها، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م.
- 30- محمود محمد أبو فرة، الخدمات البنكية الإلكترونية عبر الإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2012م.
- 31- مصطفى العوجي، القانون المدني - المسؤولية المدنية، مؤسسة بحسون، لبنان، الجزء الثاني، الطبعة الأولى، 1996م.
- 32- ناظم محمد الشمري، د. عبدالفتاح زهير العبدلات، الصيرفة الإلكترونية الأدوات والتطبيقات ومعيقات التوسع، دار وائل للنشر، الأردن، 2008م.
- 33- نسرين عبدالحميد نبيه، الجانب الإلكتروني للقانون التجاري، منشأة المعارف، مصر، 2008م.

الرسائل العلمية:

- 34- أحمد سليم فريز نصر، الشرط المعدل للمسؤولية العقدية في القانون المدني المصري، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، 2006م.
- 35- إسمهان خاطر، دور التكامل الاقتصادي في تفعيل الاستثمار الأجنبي المباشر، رسالة ماجستير، جامعة محمد مخيضر، الجزائر، 2012-2013م.
- 36- إكرام سليمان قجم، الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن، رسالة ماجستير، جامعة قطر، قطر، 2021م.

- 37- بن برنو مصطفى، دور وسائل الدفع الإلكترونية وانعكاساتها على البنوك، جامعة عبد الحميد بن باديس، رسالة ماجستير، الجزائر، 2018م.
- 38- جلايلة عبد الجليل، آليات تفعيل الرقابة المصرفية على الصيرفة الإلكترونية دراسة حالة الجزائر، أطروحة دكتوراة، جامعة أحمد دراية أدرار، الجزائر، 2018\2019م.
- 39- جودي نبيل، دور أنظمة الدفع الإلكترونية في تحسين المعاملات المصرفية -دراسة حالة- بنك السلا فرع ورقلة، جامعة قاصدي مرباح، رسالة ماجستير، الجزائر، 2022م.
- 40- حازم نعيم الصمادي، المسؤولية المدنية للمصرف عن الأضرار الناجمة عن استعمال الوسائل الإلكترونية في العمليات المصرفية، رسالة ماجستير، جامعة آل البيت، الأردن، 2002م.
- 41- حسني زايدي، أهمية البنوك الإلكترونية في تحسين العمليات المصرفية، رسالة ماجستير، جامعة العربي بن مهيدي، الجزائر، 2018م.
- 42- لحال شهيناز، أيت عيسى وسام، دور البنوك في التنمية الاقتصادية، رسالة ماجستير، جامعة عبدالرحمن ميرة، الجزائر، 2016م.
- 43- حنان بوعكوش، شادية زايدي، حماية العمليات المصرفية في ظل تطور الصيرفة الإلكترونية، جامعة العربي التبسي، رسالة ماجستير، الجزائر، 2019م.
- 44- حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2021م.
- 45- حواف عبد الصمد، النظام القانوني لوسائل الدفع الإلكتروني، أطروحة دكتوراة، جامعة أبوبكر بلقايد، الجزائر، 2015م.
- 46- خولة بلحسن، دور الصيرفة الإلكترونية في تحسين جودة الخدمات المصرفية دراسة مقارنة بين بنك القرض الشعبي الجزائري -وكالة بسكرة - وبنك السلام -وكالة بسكرة-، رسالة ماجستير، جامعة محمد خيضر، الجزائر، 2019-2020م.
- 47- دلندة دوايدي، زهرة بن حود، أمن المعلومات المصرفية، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر، 2019-2020م.
- 48- زعباب سهام، النظام القانوني للبنوك الإلكترونية، رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، الجزائر، 2018م.
- 49- زلاسي بلقاسم، غريب الحاج علي، الحماية القانونية لوسائل الدفع الإلكتروني في التشريع الجزائري، رسالة ماجستير، جامعة الشهيد حمة لخضر، الجزائر، 2021م.
- 50- سهام ملياط، النظام القانوني للمؤسسات المصرفية في الجزائر، رسالة ماجستير، جامعة أم البواقي، الجزائر، 2013-2014م.

- 51- شادي سلامة الحولي، إدارة مخاطر العمليات المصرفية الإلكترونية وفق مقررات لجنة بازل دراسة تطبيقية على البنوك المحلية العاملة في فلسطين، رسالة ماجستير، الجامعة الإسلامية، فلسطين، 2015م.
- 52- شما جاسم السليطي، الجوانب القانونية لوسائل الدفع الإلكترونية في ضوء القانون القطري، رسالة ماجستير، جامعة قطر، قطر، 2021م.
- 53- صليح بونفيلة، النظام القانوني للعمليات المصرفية الإلكترونية، أطروحة دكتوراة، جامعة 8 ماي 1945، الجزائر، 2019-2020م.
- 54- طواهر رضا، تأثير الخدمات المصرفية الإلكترونية على ربحية البنوك التجارية دراسة حالة بنك الخليج الجزائر AGB خلال الفترة 2011-2016، رسالة ماجستير، جامعة قاصدي مرباح- ورقلة، الجزائر، 2018م.
- 55- طيبي جلال، الصيرفة الإلكترونية في سياق القانون رقم 05-18 المتعلق بالتجارة الإلكترونية، رسالة ماجستير، جامعة محمد خيضر بسكرة، الجزائر، 2021م.
- 56- العايب عصام، الرقابة على عمليات البنوك في التشريع الجزائري، أطروحة دكتوراة، جامعة باتنة-الحاج لخضر، الجزائر، 2019-2020م.
- 57- عثمان خالدي، دور الرقابة المصرفية الداخلية والخارجية في تحسين الأداء داخل البنوك التجارية (دراسة حالة عينة من البنوك التجارية)، رسالة ماجستير، جامعة المسيلة، الجزائر، 2014\2015م.
- 58- عميري مليسة، مطراف أنيس، الضرر في المسؤولية العقدية، رسالة ماجستير، جامعة مولود معمري، الجزائر، 2019م.
- 59- فريدة قلقول، أهمية أنظمة الدفع الإلكتروني في المصارف دراسة حالة في بنك الفلاحة والتنمية الريفية، رسالة ماجستير، جامعة العربي بن مهيدي، الجزائر، 2012-2013م.
- 60- مجبر حنان، مهدي صارة، المسؤولية المدنية المترتبة عن العقد الإلكتروني في التشريع الجزائري، رسالة ماجستير، جامعة د.مولاي الطاهر، الجزائر، 2021م.
- 61- مروة لعلاوي، دليلة طيري، النظام القانوني لوسائل الدفع الإلكتروني، جامعة محمد البشير الإبراهيمي، رسالة ماجستير، الجزائر، 2023م.
- 62- نصيرة شبوب، الإدارة البنكية الإلكترونية في الجزائر، رسالة ماجستير، جامعة الجزائر، الجزائر، 2013م.
- 63- هداية بوعزة، النظام القانوني للدفع الإلكتروني دراسة مقارنة، رسالة ماجستير، جامعة أبي بكر بلقايد، الجزائر، 2018-2019م.

64- وافد يوسف، النظام القانوني للدفع الإلكتروني، جامعة مولود معمري تيزي، رسالة ماجستير، الجزائر، 2011م.

65- وليد أحمد سعيد مصباح، دور المصرفية الإلكترونية في دعم التجارة الإلكترونية، رسالة ماجستير، جامعة المنصورة، مصر، 2020م.

البحوث العلمية المنشورة:

72- كمال محمد حامد الفكي، دور التسويق في انتشار خدمات الصيرفة الإلكترونية بالمملكة العربية السعودية دراسة تطبيقية على مصارف محافظة الأفلاج، مجلة الدراسات التجارية المعاصرة جامعة الأمير سطام بن عبدالعزيز، المملكة العربية السعودية، العدد الثاني، 2016م.

73- محمود سمير الشراقوي، التحكيم في المعاملات المصرفية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م.

74- عدنان ابراهيم سرحان، الوفاء (الدفع) الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م.

75- منى الأشقر، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، لبنان، 2016م.

76- نبيل صلاح محمود العربي، الشيك الإلكتروني والنقود الرقمية دراسة مقارنة، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م.

77- ضويحي بن عبدالله الضويحي، القواعد الفقهية الحاكمة للعقود ومدى تناولها للعقود الإلكترونية من حيث الانعقاد والإثبات، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003.

78- منى بن لطرش، احتكار البنوك والمؤسسات المالية للعمليات المصرفية، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة، الجزائر، المجلد 14، العدد 1.

79- هيثم حسن مبارك بوغمار، العمليات المصرفية دراسة مقارنة بين التشريع الوضعي والشريعة الإسلامية، المجلة القانونية، هيئة التشريع والإفتاء القانوني، مملكة البحرين، العدد الخامس، 2016م.

- 80- صالح محمد حسني محمد الحملاوي، دراسة تحليلية لدور النقود الإلكترونية في التجارة الإلكترونية والعمليات المصرفية الإلكترونية، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، 2003م.
- 81- بريش عبدالقادر، زيدان محمد، دور البنوك الإلكترونية في تطوير التجارة الإلكترونية، بحث منشور، لا يوجد سنة نشر.
- 82- فارح عائشة، التنظيم القانوني لوسائل الدفع الإلكترونية: حتمية أساسية لتفعيل التجارة الإلكترونية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، الجزائر، المجلد 10، العدد 3، 2021م.
- 83- علي محبوب، علي سنوسي، واقع الصيرفة الإلكترونية في البنوك التجارية، مجلة شعاع للدراسة الاقتصادية، الجزائر، المجلد الرابع، العدد 2، 2020م.
- 84- عبدالرحيم وهيب، تقييم وسائل الدفع الإلكترونية ومستقبل وسائل الدفع التقليدية في ظل وجودها، مجلة الاقتصاد الجديدة الجزائر، العدد 2، 2010م.
- 85- طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية، مجلة القانون والاقتصاد، مصر ملحق خاص، العدد الثاني والتسعون، 2019م.
- 86- لعماري وليد، لوحادية عبدالناصر، الضمانات القانونية ضد مخاطر استخدام وسائل الدفع الإلكتروني، بحث منشور لمداخلة في الملتقى الوطني المنظم بقسم الحقوق لكلية الحقوق والعلوم السياسية - جامعة باتنة، 2019م.
- 87- فريدي مشري، آمنة قاجة، الحماية القانونية لوسائل الدفع الإلكتروني، المركز الجامعي عبدالحفيظ بو الصوف، الجزائر، 2018م.
- 88- علي عبدالله شاهين، نظم الدفع الكترونية ومخاطرها ووسائل الرقابة عليها دراسة تطبيقية على بنك فلسطين، مجلة جامعة الأزهر، فلسطين، سلسلة العلوم الإنسانية، المجلد 12، العدد 1، 2010م.
- 89- خالد عيد عبدالمنعم عبدالفتاح، هاني محمد السيد علي، أثر المخاطر الإلكترونية على البنوك الإلكترونية، مجلة حقوق دمياط للدراسات القانونية والاقتصادية، العدد السادس، مصر، 2022م.
- 90- أديب قاسم شندي، الصيرفة الإلكترونية انماطها وخيارات القبول والرفض، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد 27، 2011م.
- 91- سيماء محسن علاوي، آفاق تطبيق الصيرفة الإلكترونية في الاقتصاد الإماراتي، مجلة كلية المأمون، العراق، العدد الرابع والثلاثون، 2019م.

- 92- زيدك الطاهر، محمد ورنقي، استراتيجية مكافحة الإرهاب الإلكتروني في المجال الاقتصادي، المركز العربي الديمقراطي، مجلة الدراسات الأفريقية و حوض النيل، المجلد الثاني، العدد الخامس، 2019م.
- 93- دلم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون، المعهد العربي للتخطيط، الكويت، العدد 63، 2019م.
- 94- محمد الكويتي، الاتجاهات المتباينة للأمن السيبراني: مبادرة النبض السيبراني.. دراسة حالة، أوراق محاضرات (3)، أبوظبي: مركز تريندز للبحوث والاستشارات، الإمارات العربية المتحدة، 2022م.
- 95- بغدادي شامبي، تامين الخطر السيبراني، مجلة هيردوت للعلوم الإنسانية والاجتماعية، الجزائر، المجلد 7 العدد 25.
- 96- منى عبدالله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد، 2020م.
- 97- اللجنة الاقتصادية والاجتماعية لغربي آسيا، بناء الثقة بالخدمات الإلكترونية بمنطقة الإسكوا، الأمم المتحدة، 2009م.
- 98- بوراس أحمد، عياش زبير، المعايير الدولية للرقابة المصرفية وتطبيقاتها على الأنظمة المصرفية للدول النامية، مجلة العلوم الإنسانية، الجزائر، العدد 27، 2007م.
- 99- عمار عريس، مجوب بحوصي، تعديلات مقررات لجنة بازل وتحقيق الاستقرار المصرفي، مجلة البشائر الاقتصادية، المجلد الثالث، العدد 1، 2017م.
- 100- غريب جبر جبر، تهديدات الأمن السيبراني للمصارف الإلكترونية وآلية مواجهاتها، المجلة الأكاديمية للعلوم الاجتماعية، الجزائر، المجلد 1 العدد 1، 2023م.
- 101- مروة فتحي السيد، اقتصاديات الأمن السيبراني، مجلة البحوث القانونية والاقتصادية، مصر، العدد 76، 2021م.
- 102- تيم مورر وآرثر نيلسون، التهديد السيبراني العالمي، مجلة التمويل والتنمية، عدد مارس، 2021م.
- 103- عبدالقادر ورسمه غالب، الهجمات الإلكترونية على الشركات والبنوك، مجلة اتحاد المصارف العربية، لبنان، العدد 399، 2014م.
- 104- مصطفى إبراهيم سلمان الشمري، "الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، جامعة ديالي، العراق، المجلد العاشر، العدد 1، 2021م.

- 105- بلعسل بنت نبي ياسمين، عمروش الحسين، التهديدات الإلكترونية والأمن السيبراني في الوطن العربي، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الثاني، 2021م.
- 106- قطاف سليمان، بوقرين عبدالحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، الجزائر، المجلد السادس، العدد الأول، 2022م.
- 107- الاتحاد الدولي للاتصالات والبنك الدولي وأمانه الكومنولث ومركز التميز التعاوني للدفاع السيبراني التابع لمنظمة حلف الشمال الأطلسي، دليل لوضع استراتيجية وطنية للأمن السيبراني "التزام استراتيجي للأمن السيبراني، 2018م.
- 108- معهد الدراسات المصرفية، مستقبل المخاطر في العصر الرقمي، معهد الدراسات المصرفية، الكويت، العدد 2 السلسلة 15، 2022م.
- 109- زينب قاسم، عبدالوحمين رشوان، أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، المؤتمر العلمي الدولي الأول، جامعة عمان العربية، الأردن، 2022م.
- 110- بن شريف مريم، الأعمال المصرفية الإلكترونية الرهانات والتحديات - إشكالية الإشراف والرقابة المصرفية، مجلة الاقتصاد الجديد، العدد 2، 2010م.
- 111- ميليسا هاثواي، إدارة الخطر السيبراني الوطني، بحث منشور ومترجم ، لا يوجد سنة نشر.
- 112- خورخي فلوريس كايخاس، وعائشة عفيفي، ونيكوالي لوزينسكي، الأمن السيبراني في مؤسسات منظومة الأمم المتحدة، تقرير منشور مترجم، 2021م.
- 113- محمد تقروت، متطلبات تنشيط العمل المصرفي الإلكتروني في الدول العربية، مجلة الإقتصاد الجديد، العدد 7، 2012م.
- 114- اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية، نيويورك، الأمم المتحدة، العدد 18، 2012م.
- 115- صابر محمد محمود المزعل، التوثيق الإلكتروني في مجال الأعمال المصرفية الإلكترونية، المجلة القانونية، جامعة القاهرة، مصر، العدد 2537، 2017م.
- 116- رهان لطيفي، البنوك الإلكترونية، المجلة الإلكترونية للأبحاث القانونية، العدد 8، 2021م.

- 117- سهام سواي طعمه، الرقابة الداخلية للمصارف على العمليات المصرفية الإلكترونية، المؤتمر العلمي الدولي الأول، تحت عنوان "العلوم الإنسانية والصرفة رؤية نحو التربية والتعليم المعاصر، جامعة دهوك، العراق، 2019م،
- 118- ماجدة احمد شلبي، الرقابة المصرفية في ظل التحولات الاقتصادية العالمية، المكتبة القانونية العربية، المغرب.
- 119- لعماري وليد، بولحيس سامية، دور اللجنة المصرفية في الرقابة على العمليات المصرفية، مجلة الباحث للدراسات الأكاديمية، المجلد 5، العدد 3، 2018م.
- 120- نور الهدى عبدالكاظم راضي، أساليب الرقابة المصرفية، مجلة بحوث الشرق الأوسط، جامعة عين شمس، مركز بحوث الشرق الأوسط والدراسات المستقبلية، مصر، العدد 52، 2019م.
- 121- شيخ محمد زكرياء، دور الرقابة الداخلية للبنوك في حماية العمليات المصرفية، مجلة حقوق الإنسان والحريات العامة، المجلد 7، العدد 1، 2022م.
- 122- مبارك بن الطيبي، الرقابة المصرفية على البنوك التجارية في التشريع الجزائري، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو/ الأغواط، العدد 5، 2020م.
- 123- عامر العتوم، نجيب بوخرس، وآخرون، دور الهيئات الرقابية في إدارة مخاطر الخدمات المصرفية الإلكترونية في المصارف الإسلامية، المجلة الأردنية في الدراسات الإسلامية، الأردن، مجلد 16، العدد 3، 2020م.
- 124- عائشة بو ثلجة، الصيرفة الإلكترونية، جامعة الشلف حسيبة بن بوعلي، الجزائر، بحث منشور، 2021م.
- 125- صلاح الدين محمد أمين الإمام، صادق راشد الشمري، تفعيل أنظمة الرقابة المصرفية وتطويرها وفق المعايير الدولية، مجلة الإدارة والاقتصاد، السنة الرابعة والثلاثون، العدد 90، العراق، 2011م.
- 126- عبدالرزاق خليل، عادل نقموش، السلطات الإشرافية والعمليات المصرفية الإلكترونية، مجلة الاقتصاد الجديد، العدد 00، 2009م.
- 127- طيبة ماجد، السرية المصرفية، كلية بغداد للعلوم الاقتصادية الجامعة، بحث منشور، 2021م.
- 128- منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، بغداد، 2013م.

- 129- نزيه محمد علي، دور التشريعات والقوانين الوطنية والدولية الحاكمه لحماية امن المعلومات، المجلة المصرية لبحوث الإعلام، الجزء الثاني، العدد 8، 2022م.
- 130- رويدا حسن الجعافر، قانون حماية البيانات الشخصية في الأردن، المجلة العربية للنشر العلمي، الأردن، الإصدار الخامس، العدد خمسون، 2022م.
- 131- صفا علي حسين، المسؤولية المدنية للمصرف عن الإخلال بقواعد الاستعلام المصرفي، مجلة العلوم القانونية، جامعة بغداد، العراق، العدد الخاص الثالث، الجزء الأول، 2017م.
- 132- حسام عبد اللطيف حمي مخيس، الحماية القانونية للمعاملات المصرفية الإلكترونية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 11، العدد 43، 2022م.
- 133- زينة غانم يونس العبيدي، مسؤولية المصرف عن أخطاء الكمبيوتر في النقل الالكتروني للنقود، مجلة الرافدين للحقوق، المجلد 11، العدد 39، 2009م.
- 134- رياض السيد حسين أبو سعيدة، ضمان ضرر العميل في التعامل المصرفي الإلكتروني، مجلة الكوفة، العدد 12، 2011م.
- 135- شريف عبدالرحمن سيف النصر، السيبرانية (المفهوم ، الخصائص، الفرض والإشكاليات)، مركز الحضارة للدراسات والبحوث، العدد الحادي والعشرون، 2021م.
- 136- نور الدين كروش، ليلي أوالد ابراهيم ، جمال دقيش، أثر استخدام تكنولوجيا المعلومات على تحسين جودة الخدمة المصرفية، مجلة البحوث والدراسات العلمية، الجزائر، المجلد 14 ، العدد 1، 2020م.
- 137- طلال عبدالكريم القرعان، أثر الخدمات المصرفية الإلكترونية في تعزيز ولاء العملاء للقطاع المصرفي الأردني، مجلة المتقال للعلوم الاقتصادية والإدارية وتكنولوجيا المعلومات، المجلد الثامن، العدد 1، الأردن، 2022م.
- 138- أحمد مصفى مندور، الأمن السيبراني للخدمات المالية والمصرفية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، ألمانيا، لا توجد سنة نشر.
- 139- محمد صالح محمد غريب الكردي، تطور الخدمات المصرفية الإلكترونية ودورها في تنشيط التجارة المصرية، المجلة العلمية للدراسات والبحوث المالية والتجارية، جامعة دمياط، مصر، المجلد الرابع، العدد 1، الجزء الرابع، 2023م.
- 140- محمد اسماعيل، الأمن السيبراني في القطاع المصرفي، صندوق النقد العربي، موجز سياسات، العدد الرابع، 2019م.

- 141- مصطفى سالم عبد الرضا، حيدر محمد كرمي، سنان عبدالله حرجان، التكنولوجيا المالية ودورها في تحقيق التنمية المستدامة، مجلة جامعة جيبها، العراق، المجلد الرابع، العدد 2، 2020م.
- 142- منصورية زعفران، فاطمة لعلمي، دور الاستثمار الأجنبي المباشر في تحقيق التنمية الاقتصادية في الدول النامية، جامعة عبد الحميد بن باديس مستغان، الجزائر، 2018م.
- 143- عبدالعزيز بوخرص، التوجهات الجديدة في قوانين الإفلاس الحديثة: رؤية اقتصادية بإفكار قانونية جديدة، مجلة كلية القانون الكويتية العالمية، الكويت، العدد 4، ملحق خاص، 2019م.
- 144- يتوجي سامية، الصيرفة الإلكترونية في سياق القانون رقم 5-18 المتعلق بالتجارة الإلكترونية، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، الجزائر، المجلد 12، عدد خاص 22، 2020م.

القوانين

أ- الجريدة الرسمية

الجريدة الرسمية

- 139- دستور مملكة البحرين، الجريدة الرسمية، مملكة البحرين، العدد 2571، 2002م.
- 140- قانون رقم 30 لسنة 2018 بإصدار البيانات الشخصية، الجريدة الرسمية، العدد 3375، مملكة البحرين.
- 141- قانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات، الجريدة الرسمية، العدد 3178، مملكة البحرين، 2014م.
- 142- قانون رقم 64 لسنة 2006 بإصدار قانون مصرف البحرين المركزي والمؤسسات المالية، الجريدة الرسمية، العدد 2755، مملكة البحرين، 2006م.
- 143- مرسوم بقانون رقم (7) لسنة 1987 بإصدار قانون التجارة، الجريدة الرسمية، العدد 1739، مملكة البحرين، 1987م.
- 144- مرسوم بقانون رقم (54) لسنة 2018 بإصدار قانون الخطابات والمعاملات الإلكترونية، الجريدة الرسمية، العدد 3395، مملكة البحرين، 2018م.

- 145- قانون رقم 6 لسنة 2014 بالموافقة على قانون نظام العلامات التجارية لدول مجلس التعاون لدول الخليج العربية، الجريدة الرسمية، العدد 3145، مملكة البحرين، 2014م.
- 146- مكافحة الشائعات والجرائم الإلكترونية، الإمارات العربية المتحدة، 2021م.
- 147- مرسوم بقانون رقم 65 لسنة 2020 بتعديل بعض أحكام المرسوم رقم 69 لسنة 2004 بإعادة تنظيم وزارة الداخلية، الجريدة الرسمية، العدد 3494، مملكة البحرين.
- 148- مرسوم بقانون رقم 19 لسنة 2001 بإصدار القانون المدني، مملكة البحرين، الجريدة الرسمية، العدد 2476، 2001م.
- 149- قانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات، مملكة البحرين، الجريدة الرسمية، العدد 3178، 2014م.
- 150- قانون رقم 30 لسنة 2018 لحماية البيانات الشخصية، مملكة البحرين، الجريدة الرسمية، العدد 3375، 2018م.
- 151- قانون رقم 35 لسنة 2012 بشأن حماية المستهلك ، مملكة البحرين، الجريدة الرسمية، العدد 3063، 2012م.
- 152- مرسوم بقانون رقم 19 لسنة 2001 بإصدار القانون المدني، مملكة البحرين، الجريدة الرسمية، العدد 2476، 2001م.
- 153- مرسوم بقانون رقم (37) لسنة 1999 بالتصديق على اتفاقية تشجيع الاستثمار وتوفير الحماية المتبادلة له بين حكومة دولة البحرين وحكومة الولايات المتحدة الأمريكية، مملكة البحرين.

ب- القوانين المقارنة

- 154- القانون المصري رقم 194 لسنة 2020 بإصدار قانون البنك المركزي والجهاز المصرفي.
- 155- قانون الاونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، الأمم المتحدة، 1996م.
- 156- المرسوم بقانون اتحادي رقم 14 صادر بتاريخ 23-9-2018 في شأن المصرف المركزي وتنظيم المنشآت والأنشطة المالية، الإمارات العربية المتحدة.
- 157- المرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة، الإمارات العربية المتحدة.

158- مرسوم بقانون اتحادي رقم 46 لسنة 2021 بشأن المعاملات الإلكترونية وخدمات الثقة، الإمارات العربية المتحدة.

159- مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، الإمارات العربية المتحدة.

المواقع الإلكترونية

- 160- History of Our Company | Deluxe
- 161- المركز الوطني للأمن السيبراني، مملكة البحرين، من نحن (ncsc.gov.bh)
- 162- بيان عن القطاع المالي | مصرف البحرين المركزي (cbb.gov.bh) .
- 163- What is Secure Electronic Transaction (SET)? (techtargget.com)
- 164- الاتحاد الدولي للاتصالات (itu.int) .
- 165- قطاع الخدمات المالية - مجلس التنمية الاقتصادية البحرين (bahrainedb.com)
- 166- Bahrain – Introduces a new "golden licence" to promote FDI Monitor | UNCTAD Investment Policy Hub | Investment Policy
- 167- Capital One to pay \$80 million fine for 2019 hack that exposed 100 million accounts - CBS News

المقالات

- 167- "الوطن" تحاور رئيسة نيابة الجرائم الإلكترونية.. المعلا: الاحتيال المالي أكثر أنواع الجرائم الإلكترونية ويمكن تتبعها محلياً ودولياً - صحيفة الوطن (alwatannews.net)
- 168- أخبار الخليج | تعاون مشترك بين النيابة والمؤسسات المصرفية لمكافحة الاحتيال الإلكتروني (akhbar-alkhaleej.com)
- 169- خالد موسى، البنوك عوضت المتضررين من حادثة اختراق البطاقات البنكية، جريدة الأيام، العدد 9337، مملكة البحرين، 2014م.
- 170- إنشاء مركز متخصص ومتكامل للأمن السيبراني ليصبح أول المراكز القطاعية من نوعها في مصر، مجلة اتحاد المصارف العربية، العدد 491، 2021م.

171- محمد الكويتي، حالة الأمن السيبراني بالقطاع المصرفي، مركز الإمارات للدراسات والبحوث الاستراتيجية، مقال

<https://mufakirualemarat.ecssr.ae/publications/edaat/detail/603>

172- محمد الكويتي، قمة الحوكمة والمخاطر والامتثال 2023 تسلط الضوء على الحوكمة للمستقبل الرقمي للإمارات، صحيفة مباشر نيوز، مقال قمة الحوكمة والمخاطر والامتثال 2023 تسلط الضوء على الحوكمة للمستقبل الرقمي للإمارات - صحيفة مباشر نيوز (mubasher.news)

173- مقال بعنوان مبادرة عالمية لجذب أفضل الكفاءات والشركات الرقمية في العالم، وزارة الاقتصاد، المركز الإعلامي، الامارات العربية المتحدة، 6 يوليو 2022م.

174- يوسف صلاح الدين، لمحات من تاريخ العمل المصرفي في مملكة البحرين، جريدة أخبار الخليج، مملكة البحرين، العدد 16712، مارس 2023م.

التقارير

174- الأمم المتحدة، إدارة الشؤون الاقتصادية والاجتماعية، تقرير الأمم المتحدة مسح الحكومة الإلكترونية، 2020م.

175- الأمن السيبراني أساسي لتطوير قطاع التكنولوجيا المالية في البحرين، مقال منشور في جريدة الوطن، 8 يونيو-2023.

176- بناء أفضل للمستقبل تقرير صندوق النقد الدولي بشأن الخدمات المالية الإلكترونية، واشنطن، 2021م.

177- العمليات المصرفية الإلكترونية والإطراف الإشرافي، صندوق النقد العربي، تقرير منشور، 2019م.

178- محمد الكويتي، الأمن السيبراني في 2023: تحولات وتحديات عصر الذكاء الاصطناعي، تريندز للبحوث والاستشارات.

179- المنتدى الإقليمي للاتحاد بشأن الأمن السيبراني لإفريقيا والدول العربية، في تونس، تقرير منشور، 2009م.

180- وزارة المالية والاقتصاد الوطني، التقرير الاقتصادي الفصلي لمملكة البحرين، الربع الثالث 2023م، مملكة البحرين.

ثانيا: المراجع باللغة الإنجليزية

- A.Anish Kumar, S.Ariharan, D. Asir Immanuvel, INTERNET –181
BANKING BENEFITS AND CHALLENGES, International
Conference on "Innovative Management Practices" Organized by
SVCET, Virudhunagar, Vol-1 Issue1 2016.
- Abdul-Hussein Jasim Mohammed 1 , Munaf Abdulkadhim –182
Mohammed 2, Ahmed Hussein Ahmed, Impact of Banking Riskson
the Electronic Banking Services: A Comparative Study,
TEM Journal. Volume 10, Issue 2.
- Aquiles A. Almansi, Cybersecurity, Cyber Risk and Financial –183
Sector Regulation and Supervision, World Bank Group,
.Washington, 2018.
- Azharuddin, LEGAL PROTECTION FOR USERS OF –184
INTERNET BANKING CUSTOMERS FOLLOWING CHANGES IN
INFORMATION AND ELECTRONIC TRANSACTIONS LAW, Jurnal
Pembaharuan Hukum ,Vol VI,No.1,2019.
- Bandita Das, Jayanta Boruah, Right to privacy and data –185
protection under Indian legal regime.
- Bank for International Settlements, Basel Committee on –186
Banking Supervision, "Electronic Banking Group Initiatives and
White Papers,2000.
- Bojan Daniela, Mutu Simona, Pun Drago, Electronic Banking –187
– Advantage for financial services delivery, Cluj-Napoca
University,2010.
- Daniela popescul, The Confidentiality – Integrity – –188
Accessibility Triad into the Knowledge Security, Proceedings of the
16th International Business Information Management Association
Conference, 2011.

- David Lukic , Target Data Breach, How Target Almost Lost Everything,2020. –189
- Diptiben Ghelani, Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. American Journal of Computer Science and Technology. Vol. x, 2022 –190
- Dr. Atul Kumar, A Study of Significant Characteristics of E-payment Regime in India, MERC Global's International Journal of Management, Volume 7, Special Issue 1, May 2019. –191
- Dr. Kavita, ANALYSIS OF INTERNET BANKING ALONG WITH LEGAL ASPECTS IN INDIA, Kurukshetra Law Journal,Vol XI,2021. –192
- European Insurance and Occupational Pension Authority cyber risk of insurers challenges and opportunity, Publication of the European union, Luxembourg, 2019. –193
- Federal Trade Commission. "Equifax to Pay \$700 Million for 2017 Data Breach." FTC, 22 July 2019. –194
- Filippo Curti, Jeffrey Gerlach, Sophia Kazinnik, Michael Lee and Atanas Mihov, Cyber Risk Definition and Classification for Financial Risk Management, 2019 –195
- Hajera Fatima Khan, "E-Banking: Benefits and Related Issues". American Research Journal of Business and Management; Vol3, Issue1. –196
- Hussien Alasrag, Foreign Direct Investment Development Policies in the Arab Countries, Munich Personal RePEc Archive,No.2230,2005. –197
- JACQUES DE WERRA, EVELYNE STUDER, REGULATING CYBERSECURITY What civil liability in case of cyber-attacks ?, EXPERT FOCUS,Droit,2017 –198
- Joel Burleson-Davis, "Cybersecurity: Trends From 2022 and Predictions For info **security-magazine**, 14 Dec. 2022. –199

- Josh Fruhlinger, Equifax data breach FAQ: What happened, who was affected, what was the impact?,2023. -200
- Jvish Sharma, Suhasini Verma, Mounting Cases of Cyber- Attacks and Digital Payment. -201
- K. Böhle, M. Krueger, C. Herrmann, G. Carat, I. Maghiros, Electronic Payment Systems, Institute for Prospective Technological Studies, Background Paper No. 1,2000. -202
- Kassim Mukuuma, Mwase Ali, Benard Engotoit, Examining the influence of E-banking security on customer satisfaction in Uganda – a case study of Ugandan commercial banks, ICTACT journal on management studies, Vol.06 Issue 02. -203
- Krebs, Brian. "Target Hackers Broke in Via HVAC Company." Krebs on Security, 14 Feb. 2014. -204
- Machogu AM, Okiko E-banking Complexities and the Perpetual Effect on Customer Satisfaction in Rwandan Commercial Banking Industry: Gender as a Moderating Factor. J Internet Bank Commer,(Article published), 2015. -205
- Marc Santora, in housemen thieves took \$45 million in the A.T.M. Scheme,the new York times , article. -206
- Marinela Vrîncianu^{1*} and Liana Anica Popa, CONSIDERATIONS REGARDING THE SECURITY AND PROTECTION OF E-BANKING SERVICES CONSUMERS' INTERESTS, Amfiteatru Economic,Romania. -207
- Mark Fajfar, Role and Security of Payment Systems in an .Electronic Age, IMF Institute Seminar, 2004. -208
- Mishra, A., Awal, A., Elijah, J., & Rabi, I.(2017). An Assessment of the Level of Information Security Awareness among Online Banking Users in Nigeria. International Journal of Computer Science and Mobile Computing Volume and Issue: Vol. 6, Issue 5. -209

- Mohammad Al Animat, Legislation of Legal Protection for Electronic Banking Operations and Challenges in Jordan, International Journal of Economics, Business and Management Research Vol. 6, No.11, 2022. -210
- R. D.Tanase , R. serbu, operational risk and E-banking, vol 3(52), series V 2010. -211
- Risk management for electronic banking and electronic money activities ,electronic money, 1998. -212
- Scott Sargent, Esq., Baker Donelson; Electronic banking Risks and requirements; Thomson Reuters,2018. -213
- Van Eeten, M.J.G., De Bruijn, H., Kars, M., Van der Voort, H. and van Till, J,The governance of cybersecurity: a framework for policy’, Int. J. Critical Infrastructures, Vol. x, No. x,2006 -214
- van Eeten, M.J.G., de Bruijn, H., Kars, M., van der Voort, H. and van Till, J. ‘The governance of cybersecurity: a framework for policy’, Int. J. Critical Infrastructures, Vol. x, No. x,2006,Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision,2003. -215
- Zachary B. Omariba, Nelson B. Masese, Dr. G. Wanyembi, Security and privacy of electronic banking ,IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3. -216

Abstract

Bahrain's legislature stressed the need to provide legal protection for transactions carried out by an IT means. Technological development requires a legislative umbrella capable of providing legal protection to Internet users. The Kingdom of Bahrain has therefore endeavoured to develop legislation that would provide and strengthen legal protection for operations occurring through cyberspace.

One of the most important laws enacted by Bahraini legislation; Bahrain's Law No. 54 of 2018 on Electronic Communications and Transactions and Law No. 30 of 2018 promulgate the Law on Protection of Personal Data. This legislation is a protective framework for transactions conducted through an IT tool.

This study will discuss the concept of electronic banking operations by explaining these operations in order to strengthen the banking sector, which is positively reflects on investment in the Kingdom of Bahrain.

Electronic banking operations are now the easiest option for bank customers. Banking institutions seek to provide the flexibility and quality necessary in the practice of banking operations that will achieve the customer's banking satisfaction. Although flexibility and quality are often technical in view of the fact that banking operations take place in an electronic frame, the security of such transactions must be achieved according to the rules which will be capable to protect the customer during the practice of electronic banking.

Since electronic banking operations were initially opposed and fearful of banking operations, to date the large number of banking transactions occurring daily in the world cannot be overlooked electronically. The banking sector and banking operations in themselves are a very important area, facilitating the operation and growth of many business and investment processes, for example, for many reasons, the most important of which is the streamlining of bank transfers and electronic payment in the field of e-commerce. However, this flexibility and streamlining has been accompanied by serious risks and losses due to violations by persons for the purpose of illegally seizing funds or confidential information that is available only to certain parties.

The cyberattacks on electronic banking operations has therefore necessitated international action to protect the banking sector by enacting legislation to ensure the security and protection of the banking sector, as well as international efforts to conclude international agreements to ensure the financial sector's regular and dynamic functioning under a clear legal framework capable of providing the necessary legal protection for banking operations.