

مخاطر الذكاء الاصطناعي على المجال البنكي دراسة مقارنة بين التشريعين المغربي والعُماني

The risks of artificial intelligence to the banking sector: A comparative study between Moroccan and Omani legislation

الدكتورة جودية خليل

أستاذة التعليم العالي بكلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض بمراكش

الباحث عبد الحكيم خوماني

باحث بسلك الدكتوراه بكلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض بمراكش

ملخص:

أدت التطورات الرقمية المتسارعة إلى دفع مختلف التشريعات الدولية لمواكبتها لضمان انسيابية التحول الرقمي خصوصا في المجال البنكي، الذي يعد ركيزة أساسية للنمو الاقتصادي وتحسين الكفاءة وتحقيق التنمية المستدامة، لاسيما أن الاستعانة بالذكاء الاصطناعي في المعاملات المصرفية لا يخلو من مخاطر متعددة لعل أبرزها المساس بالمعطيات الشخصية والتجسس المعلوماتي للمصارف وغيرها من صور الأنشطة غير المشروعة فضلا عن تأثيرها على الحياة الخاصة للأفراد واستقرار النظم المعلوماتية للبنوك مما يطرح إشكالا جوهريا يتعلق بمسألة ضرورة سن ضوابط وأسس قانونية وأخلاقية في التشريعين المغربي والعُماني لمكافحة الاعتداء على الحقوق التي من شأنها أن تؤثر بالسير العادي للبنوك وتمس بثقة العملاء خاصة مع استخدام تقنيات الذكاء الاصطناعي في نطاق الأنشطة المصرفية.

الكلمات المفتاحية: الذكاء الاصطناعي - المسؤولية المدنية - المجال البنكي

Abstract

The rapid pace of digital developments has compelled various international legislations to adapt in order to ensure the smooth implementation of digital transformation, particularly in the banking sector, which constitutes a fundamental pillar for economic growth, enhanced efficiency, and the achievement of sustainable development. Nevertheless, the use of artificial intelligence in banking transactions is not devoid of multiple risks, most notably the violation of personal data, cyber espionage targeting banking institutions, and other forms of unlawful activities, in addition to their impact on individuals' privacy and the stability of banks' information systems. This raises a fundamental issue concerning the necessity of establishing legal and ethical rules and frameworks within both Moroccan and Omani legislation to combat infringements upon rights that may disrupt the normal functioning of banks and undermine customer confidence, especially with the increasing use of artificial intelligence technologies in banking activities.

Keywords: Artificial Intelligence – Civil Liability – Banking Sector

المقدمة:

يعرف العالم اليوم مجموعة من التحولات التكنولوجية، التي أصبحت تؤثر على جميع جوانب الحياة لاسيما المستويين الاقتصادي والمصرفي، بحكم أن البنوك تعتبر ركيزة أساسية تساهم في تحقيق التنمية والاستقرار داخل الدول، ما أدى إلى ظهور أنماط حديثة للتعامل نتيجة لتقديم الخدمات البنكية عن بعد عبر شبكة الإنترنت، وظهور مفهوم "البنك الإلكتروني" الذي يتيح إمكانية للعملاء لإبرام عقد الحساب البنكي بشكل افتراضي، وأداء الفواتير وغيرها من العمليات البنكية بدون تواصل مباشر مع مستخدم

البنوك، ومن هذا المنطلق برز الذكاء الاصطناعي كنظام ذكي لمحاكاة العنصر البشري في نطاق الخدمات المصرفية وأداء وظيفته التشغيلية للرفع من جودة الخدمات وتعزيز الثقة المطلوبة في المجال البنكي بوجه عام.⁽¹⁶¹⁾ إلا أنه على الرغم من كل الإيجابيات التي يوفرها الذكاء الاصطناعي⁽¹⁶²⁾، فإنه في مقابل ذلك لا يخلو من عدة مخاطر تؤثر على الحياة الخاصة للأفراد وعلى مكانة المصارف التنافسية داخل الأسواق.

وبناء على ذلك، تولي المجتمعات أهمية قصوى لحماية المعطيات الشخصية ولسرية المعلومات المصرفية بحيث يجب ألا تصل إلى أشخاص غير معينين بها، نظرا لأن الحفاظ على هذه المعلومات يؤثر بشكل مباشر على الجوانب الشخصية للأفراد، ومع ذلك ورغم اتخاذ كافة التدابير التقنية والقانونية أصبح من السهل السيطرة على الأنظمة المعلوماتية، على اعتبار أن المجرمين المعلوماتيون يستغلون ضعف النظم الرقمية للاستيلاء على الأموال والبيانات، والتي تحظى بكل تأكيد بحماية وطنية⁽¹⁶³⁾ ودولية على حد سواء.⁽¹⁶⁴⁾

وبالتالي تدخل كل من المشرعين المغربي والعماني لحماية الأسرار المهنية للأفراد وتنظيم القواعد المتعلقة بالمؤسسات البنكية، وذلك من خلال القانون رقم 103.12 المتعلق بمؤسسات الائتمان والهيئات الاعتبارية في حكمها، والمرسوم السلطاني رقم 2/ 2025 بإصدار القانون المصرفي فضلا عن تدخلهم في مجال حماية البيانات الشخصية عبر القانونين 09.08 المتعلق بحماية الأشخاص الذاتيين والمرسوم السلطاني رقم 6/ 2022 بإصدار قانون حماية البيانات الشخصية، وفي سياق متصل تم تنظيم مقتضيات الخاصة بمكافحة الجرائم المعلوماتية بسن القانون رقم 07.03 المتعلق بنظم المعالجة الآلية للمعطيات والمرسوم السلطاني رقم 12/ 2011 بإصدار قانون مكافحة جرائم تقنية المعلومات، ولتوفير حماية للفضاء الرقمي تم اعتماد القانون 05.20 المتعلق بالأمن السيبراني والقانون 43.20 المتعلق بخدمات الثقة الإلكترونية، وتهدف هذه الترسانة التشريعية إلى حماية الخدمات بما في ذلك المجال المصرفي.

رغم الجهود المبذولة لا يزال غياب تأطير خاص بالذكاء الاصطناعي في القطاع البنكي يمثل تحديًا قائمًا في ظل تصاعد الجريمة الإلكترونية، مما يستدعي ضرورة تطوير استراتيجيات قانونية وفنية فعالة لمكافحة هذه الظاهرة.

أهمية الموضوع:

ينفرد موضوع دراستنا بأهمية قصوى تتمثل في إبراز مخاطر الذكاء الاصطناعي على المجال البنكي، لدى سنعمل على توضيح هذه الأهمية على الشكل التالي:

(161) للمزيد حول استخدام الذكاء الاصطناعي في المجال المصرفي راجع عزام عبد البليل التحديات القانونية للخدمات المصرفية في ضوء الاصطناعي، دار النشر (غير مذكورة) طبعة سنة 2024 الصفحة: 1 وما بعدها

(162) هناك مجموعة من التعاريف الخاصة بالذكاء الاصطناعي يبقى من أهمها تعريف عالم برمجيات الأمريكي "Johan McCarthy" والذي وصفه بكونه " العلم الذي يتعلق بهندسة صناعة الآلات الذكية وبرمجتها على النحو الذي تتقارب فيه مع الذكاء البشري وأنماطه السلوكية والتي يمكن ملاحظتها من الناحية البيولوجية " للمزيد من الاطلاع راجع: JOHAN MaCarty , what is Artificial Ingelligence ? Computer Science Department , Stanford University November 12 2007 , page : 2 lien <https://www-formal.stanford.edu> vu 18/ 01/2025

(163) ينص الفصل 24 من الدستور على مايلي " لا تنتهك سرية الاتصالات الشخصية كيفما كان شكلها، ولا يمكن الترخيص بالاطلاع على مضمونها أو نشرها كلاً أو بعضاً أو باستعمالها ضد أي كان إلا بأمر قضائي ووفق الشروط التي ينص عليها قانون..." كما أكد الدستور العماني في المادة 30 على أنه "حرية المراسلات والبريدية والبرقية والمخاطبات الهاتفية وغيرها من وسائل الاتصال مصنونة وسريتها مكفولة، فلا يجوز مر اقبتها أو تفتيشها أو إفشاء سريتها..."

(164) نجد من بين المرجعيات الدولية الإعلان العالمي لحقوق الإنسان لسنة 1948 الذي جاء في مادته 12 مايلي " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون مثل هذا التدخل أو تلك الحملات" كما تم أيضا التأكيد على ذلك من خلال العهد الدولي لحقوق المدنية والسياسية لسنة 1966 في المادة 17 والتي جاء فيها " لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو أسرته أو بيئته أو مراسلاته ولا أي حملات غير قانونية تمس بشرفه أو سمعته، كما من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس".

الأهمية القانونية: تظهر الأهمية القانونية من خلال ضرورة المواكبة التشريعية للذكاء الاصطناعي في المجال البنكي من أجل توفير الحماية القانونية للبيانات الشخصية للعملاء وضمان السرية اللازمة للعمليات البنكية، بالإضافة إلى تقيد البنوك بالضوابط المهنية والمعايير الدولية وضمان التحكم في كل القرارات التي يتخذها الذكاء الاصطناعي، وإقرار المسؤولية البنكية عند إخلال البنك بالالتزامات القانونية.

الأهمية الاجتماعية: تبرز الأهمية الاجتماعية لموضوع الدراسة في حماية النشاط البنكي المخاطر التي تهدد الاستقرار المالي نتيجة لأخطاء الذكاء الاصطناعي، بالإضافة إلى خطر تسرب المعلومات الخاصة بالعملاء والبنوك، لذلك يتطلب الاستقرار الاجتماعي التصدي لأي ممارسات تمس الثقة في النظام البنكي.

الأهمية الاقتصادية: يساهم تقليل مخاطر الذكاء الاصطناعي في القطاع البنكي في زيادة الكفاءة والإنتاجية ويعزز من فرص الابتكار وتيسير الخدمات، كما يؤدي ذلك إلى تحسين تجربة العملاء من خلال تقديم خدمات أكثر دقة، ويعتبر الحد من المخاطر عاملاً حاسماً في بناء الثقة وتحفيز الاستثمار واستراتيجيات جديدة تدعم التنمية المستدامة.

المنهج المعتمد:

في سياق البحث، اعتمدنا مجموعة من المناهج البحثية للوصول إلى النتائج المرجوة من أبرزها المنهج التحليلي الذي عملنا من خلاله على تحليل كافة النصوص القانونية المنظمة للنشاط البنكي بهدف رصد المخاطر البنكية المرتبطة بالاعتماد على أنظمة الذكاء الاصطناعي مع العمل على بيان مظاهر الحماية القانونية والتقنية لعملاء البنوك، فضلاً عن ذلك قمنا بتوظيف المنهج الوصفي لوصف الجهود المبذولة على المستويين الدولي والوطني في مكافحة الجريمة المعلوماتية التي تستهدف المصارف، وذلك نتيجة لتسارع استخدام الذكاء الاصطناعي في محاولة للاستجابة الفعالة للتحديات الحديثة التي تطرأ على البنوك، بالإضافة إلى المنهج المقارن من خلال مقارنة التشريع المغربي والعماني بهدف تسليط الضوء على الآفاق التي يقدمها الذكاء الاصطناعي لتحسين الكفاءة الائتمانية، مع الأخذ بعين الاعتبار المخاطر المرتبطة بالاستقرار المعلوماتي للبنوك.

إشكالية البحث:

يترتب عن الاستخدام المتزايد للذكاء الاصطناعي من قبل البنوك، زيادة مخاطر اختراق الأنظمة المعلوماتية، وتسرب المعطيات الخاصة للأفراد الأمر الذي يثار معه إشكالا جوهريا يتعلق بوضع ضوابط قانونية وأخلاقية خاصة به في القطاع البنكي في كل من المغرب وعمان.

خطة البحث:

يقتضي كل مشروع بحثي سلوك خطة مضبوطة حتى يتأتى مقارنته من كافة الجوانب وقد حاولنا معالجة الإطار القانوني الخاص بالقوانين الرقمية التي لها علاقة بالذكاء الاصطناعي في المعاملات البنكية، وسبل توفير حماية تقنية تنسجم وخصوصيات الذكاء الاصطناعي خاصة مع تسارع الاختراقات وأساليب الاحتيال المالي، وسنعمل على تقسيم موضوع الدراسة إلى مبحثين، سنخصص الأول لدراسة مخاطر الذكاء الاصطناعي على القطاع البنكي، وسنتطرق في المبحث الثاني لمبحث المسؤولية القانونية للذكاء الاصطناعي.

المبحث الأول: مخاطر الذكاء الاصطناعي على المعاملات البنكية

يفتح التقدم التكنولوجي آفاقا واسعة لتطور البشرية، حيث يسهل الحصول على المعلومات وتبادلها عبر شبكة الإنترنت، غير أنه في المقابل تأثرت المؤسسات البنكية بمخاطر متعددة يمكن أن نجعلها في: انتهاك الخصوصية المصرفية، إذ يسعى العديد من الأفراد من خارج المؤسسات البنكية إلى المساس بالنظام المعلوماتي للمصارف، مما يشكل تهديدا حقيقيا لأمان البيانات، ويعود السبب أساسا إلى القدرات المتطورة للذكاء الاصطناعي في معالجة المعطيات البنكية والتي يمكن أن تؤدي في بعض الحالات إلى تحيز

وعدم المساواة في اتخاذ القرارات المالية، وبذلك يتوجب على المؤسسات البنكية اتخاذ تدابير فعالة لحماية الأمن الإلكتروني وضمان العدالة في الخدمات.

لذلك سنحاول معالجة هذا المبحث من خلال مطلبين الأول سنخصصه لمخاطر الاختراق البنكي وتأثيره على المعطيات الشخصية (المطلب الأول) بينما نخصص الثاني لدراسة لوسائل الحماية من مخاطر الذكاء الاصطناعي في المجال المصرفي (المطلب الثاني).

المطلب الأول: مخاطر الاختراق البنكي وتأثيره على المعطيات الشخصية

شكلت الجرائم الرقمية هاجسا إضافيا بالنسبة للمجتمعات في ظل الانفتاح الاقتصادي الأمر الذي برز معه، معطى انتقال المعلومات بسرعة دون رقابة وتحكم بل أكثر من ذلك، تضاعفت عمليات النصب والاحتيال الإلكتروني، وكذا التنصت على المؤسسات المصرفية، الوضع الذي صعب من حصر المخاطر التي تهدد النظام المعلوماتي للمصارف نظرا لتعدد صور الأنشطة غير المشروعة التي يكون دافعها؛ السيطرة على أموال الأفراد والشركات، في خضم وجود الذكاء الاصطناعي وقدرته على التجسس المعلوماتي للبنوك والتدخل في المعطيات الشخصية.

ومن تم سنعمل على تقسيم هذا المطلب الأول إلى فرعين سنخصص الأول لتحديد نطاق مخاطر الاختراق المعلوماتي للبنوك باستعمال الذكاء الاصطناعي (الفرع الأول) في حين نخصص الثاني لأوجه حماية القانونية للمعطيات الشخصية للبنوك (الفرع الثاني).

الفرع الأول: مخاطر الاختراق المعلوماتي للبنوك باستعمال الذكاء الاصطناعي

عرفت المهنة البنكية تطورا، واسعا بفعل اعتماد الذكاء الاصطناعي والوسائل الإلكترونية لتسهيل ابرام العمليات البنكية كالأداء الإلكتروني؛ وأداء الخدمات المرتبطة بشؤون العملاء بكل مرونة، لكن يجب الأخذ بالحسبان، وأنه بالرغم من الفعالية التي يوفرها الذكاء الاصطناعي يبقى هاجس اختراق النظم المعلوماتية للبنك مفتوحا؛ وذلك نتيجة قيام بعض الأشخاص، باستغلال الثغرات الأمنية المرتبطة بهذا الذكاء لتفادي الكشف عن هويتهم، وبناء عليه يشكل هذا النمط الإجرامي انتهاكا خطيرا تكون له آثار وخيمة على الحقوق الفردية والجماعية للإنسان ويتجسد هذا الواقع في القطاع البنكي، بالاطلاع على المعلومات البنكية للأشخاص، سواء كانوا أشخاص اعتباريين أو ذاتيين والتعرف على أسرارهم. (165)

لكن لم يعمل المشرع المغربي والقانون المقارن العماني على وضع إطار قانوني خاص بالذكاء الاصطناعي في نطاق المعاملات البنكية بحيث يثار التساؤل حول متطلبات المواكبة التشريعية للذكاء الاصطناعي؟

نرى على أن تدخل كل من المشرع المغربي والمشرع العماني وكل التشريعات لوضع ضوابط للذكاء الاصطناعي لنشاط البنوك ومناخ الأعمال لم يعد خيارا بل توجه استراتيجي؛ لمسايرة مخاطر الأمن الاقتصادي، وما يؤكد هذا القول هو توجه بنك المغرب باعتباره المشرف على السياسة النقدية وتشديده على حتمية التكيف مع التحولات التي فرضتها الثورة الرقمية على مستوى القطاع البنكي والاستفادة من التقنيات الحديثة وتعزيز القدرة على معالجة وتحليل الحجم المتزايد للبيانات الواردة في البيئة المهنية، خاصة من خلال استعمال الذكاء الاصطناعي في تسهيل قدرة البنك على استغلال البيانات بشكل لا يتعارض مع الأمن المعلوماتي. (166)

أولا: مخاطر التجسس المعلوماتي وخداع الذكاء الاصطناعي

يبرز معطى التجسس المعلوماتي كتحدٍ واقعي يؤثر على السير العادي للبنوك، ويهدد بشكل مباشر الأنظمة المعلوماتية للبنوك، وتماسكها لأن المجرمين المعلوماتيين؛ يعتمدون على نشر مجموعة من التطبيقات الذكية بغرض اختراق الحسابات والمعطيات

(165) اميمة باجابر، السر المني البنكي في المادة البنكية مقال إلكتروني منشور في موقع الجامعة القانونية المغربية الافتراضية تم الاطلاع عليه يوم 2025/22/11 على الساعة 11:01 عبر الرابط الاتي: www.aljami3a.com

(166) انظر المخطط الاستراتيجي لبنك المغرب لسنة 2019-2023 حول الشمول المالي الصفحة: 34

المصرفية ونقلها والحفاظ عليها، ومن ثم فإن الذكاء الاصطناعي يضاعف من خطر انتهاك سرية البيانات البنكية وكل ما له علاقة بالأجهزة الإلكترونية للبنوك والتي لا ينبغي الاطلاع عليها إلا بحكم القانون.⁽¹⁶⁷⁾

تأسيسا على ما سبق ومن أجل تلافي نسخ المعطيات البنكية والاعتداء عليها تدخلا كل من المشرعين المغربي والعماني انسجاما مع التوجيهات الإقليمية⁽¹⁶⁸⁾ والدولية⁽¹⁶⁹⁾ في هذا الباب لتوفير الحماية التقنية ضد كل أشكال الاعتداء على النظم الآلية للمعطيات من خلال إضافة القانون 07.03 لتميم مجموعة القانون الجنائي فيما يتعلق بالنظم الآلية للمعطيات التي تمس النظم المعلوماتية⁽¹⁷⁰⁾ والمرسوم السلطاني رقم 2011/12 المتعلق بمكافحة جرائم تقنية المعلومات.

من جانب آخر يثار التساؤل حول إمكانية تطبيق القواعد الجزية الحالية، عند تنفيذ التجسس المعلوماتي باستعمال الذكاء الاصطناعي خاصة في ظل عدم وجود تأطير قانوني نعتقد على أن الفصلين 607 - 3 من مجموعة القانون الجنائي المغربي والمادة 3 من المرسوم السلطاني رقم 12 / 2011 المتعلق بقانون مكافحة جرائم تقنية المعلومات يشكلان الأساس القانوني، لمكافحة التجسس المعلوماتي للبنوك وذلك لعدة مبررات:

المبرر الأول: إمكانية التجسس بواسطة أنظمة الذكاء الاصطناعي على النظم الآلية للبنوك باختراق الأجهزة الداخلية لشبكة الإنترنت؛

المبرر الثاني: يستخدم الذكاء الاصطناعي بشكل مستقل أو من قبل أفراد يسعون للحصول على الأموال بطرق غير مشروعة مما يؤثر سلبا على النظام العام البنكي، ومع تزايد الجرائم الإلكترونية الخارجية في الآونة الأخيرة الناتجة عن عمليات الاحتيال في الاتصالات، أكد بنك المغرب على ضرورة عدم تبادل أي معلومات سرية تتعلق بالعملاء عبر التطبيقات الحديثة حرصا منه على أهمية اليقظة البنكية في حماية الأمن الإلكتروني للبنوك.⁽¹⁷¹⁾

المبرر الثالث: تضاعف البنوك الجهود لمجابهة مخاطر الذكاء الاصطناعي عبر الوسائل التقنية لتلافي إمكانية فقدان مكانتها التجارية وتحملها المسؤولية القانونية عن أخطاء الذكاء الاصطناعي؛

ثانيا: خداع الذكاء الاصطناعي والدخول غير المشروع للنظام المصرفي

أصبح الذكاء الاصطناعي في الوقت الحالي وسيلة لخداع مستخدمي المصارف، في ظل اللجوء إلى تقنية الدردشة المباشرة THE IA CHAT BOT لتقديم كافة الخدمات البنكية دون الحاجة للعنصر البشري ومع ذلك على الرغم من كل أساليب التواصل الحديثة التي تراعي السرعة والشفافية يبقى الذكاء الاصطناعي وسيلة مساعدة في التخفي من خلال إجراء تعديلات على الصور الحقيقية

(167) توجد العديد من الطرق والوسائل التي تستعمل من أجل التجسس المعلوماتي والمساس بالنظم المعلوماتية لكن نجد من أهمها:

الطريقة الأولى: تتعلق بإرسال الشخص الذي يريد التجسس ملف إلى المجني عليه بغرض إخباره بأن الرسالة تتعلق بأموره الخاصة لكن في الحقيقة يكون ذلك الملف هو مفتاح اختراق النظام المعلوماتي وتحقق النتيجة الاجرامية.

الطريقة الثانية: إرسال رسالة إلكترونية إلى المجني عليه فيقوم بفتحها فإذا بها تحتوي على ملفات ملحقه تحمل ملف التجسس الأول.

الطريقة الثالثة: تكون عن الشخص أو الجهة المجني عليها لمواقع مجهولة وتقوم بإغراء الزائرين بتزليل بعض البرامج والملفات المجانية ومنها ملفات التجسس

للمزيد حول الموضوع أنظر: نهلا عبد القار المومني، " الجرائم المعلوماتية" النشر دار الثقافة للنشر والتوزيع عمان الطبعة الأولى سنة 2008 الصفحة: 219 وما يليها.

(168) نجد من أهم التوجيهات الإقليمية: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بتاريخ 2010/12/21 بمدينة القاهرة بمصر والتي نصت المادة الأولى منها على أنه: تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

(169) على المستوى الدولي نجد الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية بودابست تم الاطلاع على أحكام هذه الاتفاقية على الموقع الخاص بالمجلس الأوروبي على الموقع الاتي: www.coe.int/budapest 2025/23/11 على الساعة 15:30

(170) ظهير شريف رقم 1.03.197 صادر في رمضان 1424 (11 نونبر 2003) بتنفيذ القانون رقم 03.07 بتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، منشور بالجريدة الرسمية عدد 5171 - 1424 شوال الصادر بتاريخ 22 دجنبر 2003 الصفحة: 4284.

(171) تواصل بنك المغرب يوم 14 / 11 / 2025 بشكل مباشر مع كافة المواطنين عبر التطبيقات الذكية وذلك بإرساله رسالة نصية جاء في نصها ما يلي " كونوا يقظين! لا تفصحوا أبدا عن رمز التأكيد السري الذي تتوصلون به عبر رسائل القصيرة ولا عن معلوماتكم المتعلقة بوسائل الدفع الخاصة بكم أي رسالة أو مكالمة تطلب منكم هذه المعلومات في احتيالية.

للعلماء، الأمر الذي يسمح بالتلاعب بالخوارزميات وتجنب التعرف على الوجه الحقيقي على اعتبار أن كل هذه التعديلات تروم إلى خداع نظام المراقبة الداخلية للمصارف. (172) الأمر الذي يسهل عملية الدخول غير المشروع للحاسب الآلي وذلك بأي شكل من الأشكال لاختراق النظام المعلوماتي من خلال؛ استعمال برنامج فيروس - قرصنة برامج أو رموز التشفير- تجاوز نظام الحماية.... (173)

وبذلك عمل المشرع العماني على حماية التعدي على سلامة وسرية توافر البيانات والمعلومات الالكترونية والنظم المعلوماتية إذ؛ منع كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر فيها بعد علمه وطراً إلغاء أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر البيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية أو إلحاق ضرر بالمستخدمين أو المستفيدين وقرر عقوبة زجرية تتمثل في السجن لمدة لا تقل عن ستة أشهر ولا تزيد عن سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد عن ألف ريال عماني أو بإحدى هاتين العقوبتين. (174)

ويلاحظ على أن القانونين المغربي والعماني عملا على وضع ضوابط لحماية المعلومات المخزنة داخل النظام وتلافي التجسس أو الاختراق بدون موجب قانوني أو أخلاقي على اعتبار أن التجسس والخداع الرقمي بوجه عام، وغيرها باستخدام الذكاء الاصطناعي يكشف عن نتائج سلبية:

- خطر المساس بالثقة الرقمية على مستوى الخدمات البنكية وغياب الشعور بالأمن الرقمي.
- تنامي ظاهرة الاحتيال الإلكتروني المصري.

الفرع الثاني: حماية المعطيات الشخصية المصرفية في قانونين المغربي والعماني

عمد المشرع المغربي من خلال القانون رقم 09.08 المتعلق بحماية المعطيات ذات طابع الشخصي على إيجاد فضاء رقمي ملائم لمتطلبات الأفراد، بمن فهم عملاء المؤسسات البنكية على اعتبار وأن المستهلك أصبح يبرم العديد من العقود الالكترونية عن بعد إما لأغراضه الشخصية أو المهنية (175) لدى كان من المؤكد حماية كل البيانات ومعالجتها بشكل لا يتعارض مع الخصوصية، فالمصرف يتعرف أثناء نشاطه على الأسرار المختلفة لطالبي الاعتمادات وهو ما يفرض الاطلاع على كافة العناصر التي تساعد على التعرف على العملاء (176) وتبحث في نظير ذلك على كل السبل التقنية لحمايتها من كل المخاطر الرقمية.

كما ينبغي على البنوك أن تخضع المعطيات الشخصية للمعالجة الإلكترونية وتحويلها إلى بيانات رقمية لتفادي كشف سريتها أو الاعتداء عليها، لأن معظم المواقع التجارية تعتمد في سياستها التسويقية على البيانات الشخصية كوسيلة من وسائل التسويق المباشر. (177)

وفي ذات السياق عمل القانون العماني على إصدار المرسوم السلطاني رقم 20 22 / 7 المتعلق بحماية البيانات الشخصية، حيث عرف البيانات الواجب حمايتها وهي كل البيانات؛ التي تجعل شخصا طبيعيا معرّفا أو قابلا للتعريف بطريقة مباشرة أو غير مباشرة وذلك بالرجوع إلى معرف أو أكثر كالأسم أو الرقم المدني أو بيانات المعرفات الإلكترونية أو البيانات المكانية أو بالرجوع إلى عامل أو

(172) Mohit Kumar "and others The Impact Of Artificial Intelligence On The Banking Sector" An article published in the magazine Afr. J. Biomed. Res. Vol. 275s December 2024; 95-100 Research Article page : 97

(173) عبد الكريم عباد " الجريمة المعلوماتية " مقال منشور في المجلة الوطنية للعلوم القانونية والقضائية، العدد الأول مطبعة الأمنية - الرباط سنة 2020 الصفحة: 75.

(174) المادة 3 المرسوم السلطاني رقم 12 / 2011 لسلطنة عمان بإصدار قانون مكافحة جرائم تقنية المعلومات الصادر في الجريدة الرسمية تحت عدد: 929.

(175) يمكن تعريف المستهلك الرقمي كل شخص ذاتي أو اعتباري يقوم بإبرام خدماته الشخصية باستخدام الوسائط الإلكترونية عن بعد.

(176) أنطوان جورج سركيس "السرية المصرفية في ظل العولمة" دار النشر منشورات الحلبي الحقوقية الطبعة الأولى سنة 2008 مرجع سابق الصفحة: 290

(177) نسمة الخلفي "الحماية الجنائية والتقنية للبيانات البنكية" رسالة لنيل دبلوم الماستر في القانون الخاص جامعة القاضي عياض كلية العلوم القانونية والاقتصادية والاجتماعية بمراكش السنة الجامعية 2019 - 2018 : الصفحة 55

أكثر للهوية الجينية أو الجسدية أو العقلية أو النفسية أو الاجتماعية أو الثقافية والاقتصادية، بينما تظل المعطيات والخدمات المصرفية من أهم البيانات التي يجب حمايتها من كل صور الاعتداء الرقمي.⁽¹⁷⁸⁾

تأسيسا على ذلك يجب؛ معالجتها بشكل مستمر وعلى نحو ينسجم مع ضوابط المعالجة وضبط المتحكم بها، بحكم أن كل المعلومات المصرفية، يجب أن تعالج بناء على تحديد المخاطر التي قد تقع على صاحب البيانات الشخصية في عملية المعالجة وكذا ضمان التدابير التقنية لضمان تنفيذها بشكل سليم.⁽¹⁷⁹⁾

أولا: سبل التقليل من مخاطر الذكاء الاصطناعي على المعطيات الشخصية المصرفية

سعت دول العالم⁽¹⁸⁰⁾ إلى تسخير كل مقدراتها الوطنية في دعم البنوك من أجل استفادتها من الوسائل الإلكترونية لتحديث الخدمات البنكية وتوفير السرعة واقتصاد النفقات بعيدا عن التفاعل المباشر مع العاملين مع البنك.⁽¹⁸¹⁾

وحرصا منها على التخلي عن الآليات التقليدية، انفتحت البنوك على الذكاء الاصطناعي نظرا للكمية الهائلة من المعلومات الشخصية التي تخزن وتعالج من قبل البنك، لدى أضحت الحاجة للتقليل من المخاطر المحتملة الناجمة عن استخدامه هذه التقنيات ووضع حدود للأخطاء المرتكبة من قبله.⁽¹⁸²⁾

وبناء عليه يشكل تخزين البيانات الرقمية بواسطة الذكاء الاصطناعي، خطرا يمس بالحياة الشخصية للفرد، مثل الأرقام السرية للبطاقة البنكية والمبالغ أو القروض، التي تحصل عليها من البنك المانح للائتمان.⁽¹⁸³⁾

وعليه تختلف أبعاد الذكاء الاصطناعي بحسب الحالات، فهو من جهة يسعى إلى تحقيق أعلى مستوى من الحماية للأنشطة المصرفية، وفي المقابل قد يؤثر سلبا على النظام المعلوماتي للبنك ككل.⁽¹⁸⁴⁾

نتيجة لذلك عندما يستعمل الذكاء الاصطناعي؛ كمعالج للبيانات المرتبطة بتحسين الأداء، فإن السيطرة على الأسماء والعناوين، بالإضافة إلى الأرقام السرية والملفات الحساسة للعملاء تصبح أسهل، الأمر الذي يفرض ضمان حماية قانونية لتفادي الاستغلال غير المشروع لهذه المعلومات الرقمية.⁽¹⁸⁵⁾

ثانيا: معالجة المعطيات الشخصية في المصارف المغربية والعمانية

(178) المرسوم السلطاني لسلطنة عمان رقم 2022/7 المتعلق بحماية البيانات الشخصية المنشور بالجريدة الرسمية عدد: 1429.

(179) المادة 13 من مرسوم السلطاني لسلطنة عمان المتعلق بحماية البيانات الشخصية.

(180) أصبح الذكاء الاصطناعي جزءا لا يتجزأ من أنظمة المصارف الحديثة من أنظمة المصارف الحديثة مما يتيح اتخاذ القرارات المعتمدة على البيانات والعمليات، وهو الأمر الذي بدأت تعتمد الدول لتحقيق الفعالية، وفي هذا النطاق عملت البنوك في المملكة المتحدة على استخدام واسع للأنظمة الذكية لتفاعل مع العملاء وتحليل المخاطر، وتخفيف الاحتيال والامتثال الوظيفي، كما تحتل المملكة المتحدة مكانة رائدة على المستوى العالمي بفعل استعمال تطبيقات NLP وrap المالية للتقنيات الناشئة بسبب نظامها المالي الذي يتماشى مع نشر تقنيات والمصادقة البيومترية لتحقيق الشفافية والتقييد بقواعد بازل الخاصة بالرقابة الاحترازية.

Iyanu Emmanuel Olatunbosun and Abosede Rebecca Olatunbosun Artificial Intelligence and Risk Management in Financial Institutions: Evidence from the UK Banking Sector published in the magazine EthAlca, page: 6

(181) علاء التميمي، التنظيم القانوني للبنك الإلكتروني على شبكة الإنترنت دار النشر الجامعة الجديدة الإسكندرية دون ذكر الطبعة سنة 2012 الصفحة: 19 وما يليها.

(182) مروان الدلكي "حماية المعطيات ذات طابع الشخصي في عصر الذكاء الاصطناعي" رسالة لنيل دبلوم الماستر في القانون الخاص، جامعة القاضي عياض كلية العلوم القانونية والاقتصادية والاجتماعية بمراكش، الموسم الجامعي 2025 - 2026 الصفحة: 32.

(183) عرف مفهوم الحق في الحياة الخاصة تطورات ملحوظة إذ لم يعد يرتبط فقط بالجوانب المالية الاقتصادية للأفراد بل أضحت يتسم بطابعه المعنوي نتيجة لشعور استخدام الحاسوب في جميع المجالات.

للمزيد حول هذا الموضوع راجع جودية خليل "المعلومة بين الإفصاح وقيد الإبقاء طي الكتمان" مقال منشور في مجلة أطروحة للدراسات والأبحاث في العلوم القانونية عدد خاص سنة 2024 الصفحة: 43

(184) المادة 13 من المرسوم السلطاني لسلطنة عمان المتعلق بحماية البيانات الشخصية.

(185) محمد حمداوي "تأثير الذكاء الاصطناعي على الخدمات البنكية بين تحسين الجودة وحماية الخصوصية" مقال منشور في مجلة الإلكترونية للأبحاث القانونية العدد 15 سنة 2025، الصفحة: 85.

تخضع معالجة المعطيات الشخصية للأبنك لقواعد رقابة صارمة، بهدف الحيلولة دون وصول البيانات البنكية المسلمة من قبل العملاء إلى الأغيار، وكتماها على نحو يحافظ على سريتها، الأمر الذي أكدته المشرع المغربي من خلال الفرع الثالث الخاص بالقانون رقم 09.08 الخاص بحماية المعطيات الشخصية والمعنون بالالتزام بسرية وسلامة السر المهني⁽¹⁸⁶⁾. وفي هذا الصدد فإن كافة العمليات البنكية مع الطفرة التكنولوجية أصبحت تمر بمرحلة المعالجة المشروعة والتي لا مناص وأنها يتعين ألا تؤثر على شؤون العملاء.

ولا ريب أن إدماج الذكاء الاصطناعي في المنظومة البنكية، سيؤدي إلى خلق نوع من الصعوبة في معالجة سليمة للمعطيات البنكية مع تضاعف مساهمة هذا الذكاء في الجرائم المعلوماتية التي تلحق بالنظام البنكي، ومن المهم الإشارة إلى مسألة غياب نص صريح يعالج حماية المعطيات الشخصية من قبل الذكاء الاصطناعي سواء في القانون البنكي المغربي في إطار القسم السابع الخاص بعلاقة المؤسسات البنكية بعملائها، وكذلك القانون العماني، لكن يمكن الاستناد على المادتين 180(187) و 24 (188) من القانونين المغربي والعماني اللتان توفران حماية لسرية المعطيات، من وجهة نظرنا نرى أنها تنطبق حتى على خوارزميات الذكاء الاصطناعي وتقيدته بضوابط عدم تسريب أي معلومات خاصة بالمصرف، مادام أن النص العام يرد على عموم مالم يرد خاص يخصه، ويمنع تطبيق هذه المقتضيات التي تؤسس للأمن المعلوماتي البنكي.

وتماشيا مع ما سبق ذكره، أوصت اللجنة الوطنية لحماية المعطيات الشخصية بمسألة ضبط معالجات الذكاء الاصطناعي وفقا لأحكام القانون 09.08 الخاص بحماية المعطيات الشخصية، تكريسا لمبادئ الثقة والشفافية المطلوبة في المجتمع⁽¹⁸⁹⁾. وبناء على الاختصاصات المخولة أيضا لوزارة النقل والاتصالات وتقنية المعلومات، وفقا للفقرة الثانية من المرسوم السلطاني العماني الخاص بحماية البيانات الشخصية، فإن الوزارة تعمل على تطوير التكنولوجيا الحديثة لغاية تعزيز الأمن الرقمي بشكل يحافظ على معالجة المعطيات البنكية وفقا للضوابط القانونية والأخلاقية التي يجب أن تؤثر عمل البنوك في السلطنة. وعليه يعد إدخال أنظمة الذكاء الاصطناعي في المجال المصرفي مدخلا هاما لتبسيط الخدمات وتحسين بيئة الأعمال عبر الخدمات الرقمية الأساسية التي، تتوافق مع السياسة الوطنية العمانية للذكاء الاصطناعي لسنة 2025 المرتكزة على تبني شامل لتقنيات الذكاء الاصطناعي بشكل آمن في القطاعات الاقتصادية، وتحفيز الاستثمار والارتقاء بالمكانة العالمية للسلطنة في مجال رؤية عمان 2040 في مجال الذكاء الاصطناعي⁽¹⁹⁰⁾.

(186) عاقب المشرع المغربي في المادة 54 من القانون 07.03 المتعلق بالمعالجة الآلية للمعطيات كل من قام بخرق بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة بالجيب من 3 أشهر إلى سنة وبغرامة 20.000 درهم إلى 200.000 أو بإحدى هاتين العقوبتين فقط، لكن لا يفوتنا أن نوه أن مسألة معالجة هذه المعطيات ذات طابع شخصي لا تتم إلا بعض تصريح مسبق طبقا لأحكام المادة 52 من نفس القانون من قبل العملاء في المجال البنكي حيث أن هذه البيانات تعد من صميم الحياة الخاصة للعميل، الأمر الذي يتطلب موافقة هذا الأخير من أجل معالجتها بشكل لا يؤدي إلى تفشي أسرار العميل.

(187) تنص المادة 180 من القانون رقم 103.12 المتعلق بمؤسسات الائتمان وهيئات الاعتبارية في حكمها على أنه "يلزم بكتمان السرا المهني جميع الأشخاص الذين يشاركون في إدارة أو تسيير أو تدبير مؤسسة ائتمان أو هيئة معتبرة في حكمها أو يكونون مستخدمين لديها أو أعضاء المجلس الوطني للائتمان ولجنة تنسيق والرقابة على المخاطر الشمولية ومجلس الإدارة ومستخدمي الشركة المسيرة والأشخاص المكلفون بالمؤسسات وبنك المغرب".

مع مراعاة المادة 181 من نفس القانون التي تقضي بعدم الاحتجاج بالسر المهني على بنك المغرب وعلى السلطة القضائية العاملة في إطار قانون المسطرة الجنائية وعلى أي سلطة تابعة لدول أبرمت اتفاقية ثنائية مع المملكة المغربية تنص على تبادل المعلومات في المجال الضريبي.

(188) مرسوم سلطاني لسلطنة عمان 2025/2 بإصدار القانون المصرفي والذي شهد تعديلات والذي جاء في مادته 98 ما يلي " لا يجوز للمصرف المرخص أو عضو في المجلس إدارته أو مسؤول أو عامل فيه حالي أو سابق أو الغير الذي أسند إليه أحد الأنشطة الخاضعة لأحكام هذا القانون أو أي من الاعمال المرتبطة بتلك الأنشطة أو أي شخص آخر أن يفصح عن أي معلومات تتعلق بأي إجراء يتعلق بحساب مصرفي أو ودعية ائتمانية أو استئمانية أوي أي معلومات مصرفية إلا في الأحوال التالية:

1- بناء على إذن صريح أو تعليمات من البنك المركزي

2- بناء على موافقة كتابية صريحة من العميل

3- بناء على أمر أو حكم قضائي صادر عن محكمة مختصة في سلطنة عمان...

(189) انظر الموقع الرسمي للجنة الوطنية لمراقبة حماية المعطيات ذات طابع شخصي اطلع عليه عبر الرابط التالي:

<https://www.cndp.ma.ar> يوم 2025/12/21 الساعة 2025/12/21.

(190) انظر الموقع الرسمي لوزارة النقل والاتصالات والمعلومات لسلطنة عمان اطلع عليه عبر رابط التالي: <https://mtcit.gov.oma> اطلع عليه يوم 2025/12/21 على الساعة 15:05

المطلب الثاني: وسائل الحماية من مخاطر الذكاء الاصطناعي في المجال المصرفي

تفاديا لأي خطأ أو إهمال من قبل المصارف تعد صيانة، وكذا تحديث الوسائل الرقمية أمراً جوهرياً للرفع من جودة الخدمات المقدمة للعملاء، ويتعين على المصارف اتخاذ كافة التدابير التقنية اللازمة لتعزيز أمن أنظمتها المعلوماتية، بالإضافة إلى تنفيذ برامج توعوية لمستخدميها تركز على واجبات الحيطة والحذر، والعمل بشكل دوري للحد من المخاطر المرتبطة بالجرائم السيبرانية. فمن الضروري توفير التدريب؛ المتخصص للمستخدمين لضمان استجابة تجاه هذه التهديدات المحتملة، مما يساعد في الحفاظ على سلامة المعلومات المالية، ولذلك يتعين تعريف تقنية التشفير ودورها في حماية البنوك من المخاطر الإلكترونية (الفرع الأول) وبعد ذلك سيتم في مرحلة ثانية العمل على توضيح أهمية تقنية البلوك تشين (الفرع الثاني).

الفرع الأول: تقنية التشفير

تصاعدت وتيرة ظاهرة الاختراق الإلكتروني للنظام المعلوماتي البنكي من قبل قراصنة يستخدمون شتى الوسائل الاحتيالية، للتلاعب بالمعطيات البنكية، والاستحواذ على أموال العملاء بطرق مخالفة للقانون والنظام العام، وهذا بدوره يسبب انعدام الثقة ويضعف من مخاوف العملاء من استخدام الوسائط الرقمية لإجراء العديد من الخدمات البنكية المتعلقة بحياتهم اليومية. ولما كان الذكاء الاصطناعي من أبرز التحديات التي تطرح في مجال العمل المصرفي، فإنه أضحى وسيلة مثلى لكل الأشخاص الذين تكون غايتهم الاعتداء على النظام البنكي، لدى يجب على البنوك إيجاد أمن رقمي مستدام من خلال اتخاذ كافة التدابير التقنية المناسبة. (191)

وبالتالي نجد العديد من الوسائل التقنية لحماية البيانات البنكية من أهمها، التشفير وتقنية البلوك تشين "فالتشفير"؛ يعتبر من الوسائل الرقمية الضرورية التي تساعد في إخفاء المعطيات الحقيقية للعمليات البنكية وتحويلها إلى رموز غير معروفة إلا للبنك وعميله، كما تعتبر تقنية "البلوك تشين" كوسيلة لتخزين المعلومات بشكل أكثر أماناً فعالية.

وتعد تقنية التشفير؛ أداة للحماية التقنية في العالم الرقمي بحيث، عرفها قانون الأونسترال بشأن التوقيعات الرقمية باعتبارها فرع من الرياضيات التطبيقية الذي يعنى بتحويل رسائل إلى أشكال تبدو غير مفهومة تم إعادتها إلى أصنافها الطبيعية. (192) وفي المقابل لم يعرف المشرع المغربي هذه التقنية، لكن من زاوية أخرى عمد على تحديد الوسائل الخاصة بها في نطاق أحكام المادة 45 من القانون 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية وهي كافة؛ المعدات أو البرمجيات المصممة أو المعدلة من أجل تحويل معطيات إلكترونية سواء كانت عبارة عن معلومات أو إشارات أو رموز استناداً إلى اتفاقيات سرية أو من أجل إنجاز العملية العكسية بموجب اتفاقية سرية أو بدونها، وتهدف هذه الوسائل إلى ضمان سلامة تبادل المعطيات بطريقة إلكترونية أو تخزينها بكيفية تمكن من ضمان سريتها والتيقن منها ومراقبتها. (193)

وعلى خلاف ذلك عرف المشرع العماني التشفير في مقتضيات المادة الأولى من المرسوم السلطاني رقم 39 / 2025 على أنها "عملية تحويل المعلومات أو البيانات الإلكترونية إلى نص غير معروف أو مقروء بما يمكن فقط الأشخاص الذين يحملون مفتاح التشفير أو فك التشفير من الوصول إلى النص الأصلي". (194)

ونستشف من تعريف التشفير، ووسائله على أن هذه التقنية بمثابة برنامج يقوم على إخفاء المعلومات الخاصة بعملاء البنوك من الأسماء والودائع والأرقام إلى رموز غامضة تكون معروفة حصراً بين البنك وعملائه، إلا أنه وعلى الرغم من ذلك يساعد الذكاء

(191) هناك مجموعة من الوسائل التقنية الأخرى التي تساهم في توفير الحماية التقنية من المخاطر البنكية منظمة في قانونين العماني والمغربي، حيث نظما التوقيع الإلكتروني سواء كان المؤهل أو المتقدم أو مؤهلاً والخاتم الإلكتروني للمزيد حول هذا الموضوع راجع مصطفى مالك "النظام القانوني لمقدمي خدمات الثقة بشأن المعاملات الإلكترونية" دار النشر، دار السلام للطباعة والنشر والتوزيع – الرباط الطبعة الأولى سنة 2023.

(192) للاطلاع على التعريف وباقي أحكام التوقيعات الإلكترونية انظر قانون الأونسترال بشأن التوقيعات الإلكترونية مع دليل الاشتراع 2001، منشور بالموقع الرسمي الخاص بالأونسترال في الموقع الآتي: www.uncitral.un.org تم الاطلاع 2024/27/11 على الساعة 22:23.

(193) المادة 45 من القانون 43.20 المتعلق بخدمات الثقة الإلكترونية بشأن المعاملات الإلكترونية.

(194) المادة الأولى من المرسوم السلطاني لسلطنة عمان رقم 2025/39 بإصدار قانون المعاملات الإلكترونية الصادر بالجريدة الرسمية عدد: 1591

الاصطناعي على التعرف على المعطيات، رغم تحويلها إلى إشارات، ومن تم يبقى هاجس حماية الأمن الرقمي، وكذا حماية المستهلك والبيانات ذات الطابع الشخصي من المخاطر المتعددة التي أصبحت تشكل مصدر قلق كبير ليس فقط على المستوى الوطني ولكن أيضا على المستوى الدولي.⁽¹⁹⁵⁾

من زاوية أخرى يمكن أن يؤثر الذكاء الاصطناعي على تقنية التشفير وذلك عن طريق نسخ الصوت الذي يعود للعميل الأصلي بشكل مزيف مما يؤدي إلى تسرب معلومات حساسة تتعلق بالخدمات البنكية.

الفرع الثاني: تقنية البلوك تشين في القانون البنكي

أصبح التحول الرقمي من الخيارات الضرورية للمصارف، التي تسعى لتطوير خدماتها، ومن هنا تظهر أهمية تقنية "البلوك تشين" أو سلسلة الكتل؛ كبرنامج له علاقة بالمؤسسة وأسلوب عملها داخليا وخارجيا، وأيضا بتقديم الخدمات للعملاء وجعلها أكثر سرعة الشيء الذي يساعد في تعديل أنماط واستراتيجيات التواصل مع العملاء وإرساء الشفافية.⁽¹⁹⁶⁾

وهكذا يتبين دور هذه التقنية في دعم الخصوصية الرقمية؛ كنظام يخزن المعلومات بطريقة تقلل من وقوع الاحتيال الرقمي؛ باستخدام أدوات الذكاء الاصطناعي، فضلا عن تقييم دائم للمخاطر وإدارتها بما في ذلك مكافحة غسل الأموال ومساءلة كشف هوية العملاء والتحقق منها الأمر الذي يسهل استخدامه بشكل فعال دون مخاطر تذكر.⁽¹⁹⁷⁾

وتعرف هذه التقنية على أنها وسيلة لتسجيل البيانات بشكل متواصل في كتل مترابطة زمنيا، وبوجه عام تستخدم في كافة العمليات السيبرانية، حيث تعمل كسجل آمن لجميع المجالات، لدى أضحت في الوقت الراهن آلية فعالة تستخدم من قبل البنوك لضبط النظام المعلوماتي وتحويل كافة البيانات إلى خوارزميات معقدة تخضع فيه كل المعاملات المسجلة فيه لرقابة جماعية من طرف كافة المستخدمين.⁽¹⁹⁸⁾

علاوة على ذلك ولتأمين القطاع البنكي من كل المخاطر الناجمة عن سوء استخدام خوارزميات الذكاء الاصطناعي وتحيزها في القرارات المتعلقة بالائتمان والخدمات البنكية، يتعين ضمان حيادها الأخلاقي، لإرساء الأمن وعدم الوصول إليها بشكل غير مصرح به.⁽¹⁹⁹⁾ بذلت جهود كبيرة في المغرب وعمان من أجل الاستفادة من هذه التقنية الذكية لتحسين النظام البنكي.⁽²⁰⁰⁾

المبحث الثاني: المسؤولية القانونية عن استخدام الذكاء الاصطناعي في المجال البنكي

إن القواعد التقليدية للمسؤولية القانونية بشكل عام بدأت تعرف عجزا، في مسيرة التحولات الحاصلة خصوصا في مجال اثبات الأخطاء البنكية التي يكون سببها المباشر أنظمة الذكاء الاصطناعي، بالإضافة إلى الأخطاء التقنية التي يتم ارتكابها عند صيانة الآلات الذكية، وأمام هذا الوضع بدأت الحاجة ملحة لإقرار قواعد خاصة للمسؤولية المدنية في شقيها التقصيري والعقدي تنظم العمل البنكي ومتطلباته، وكذا المسؤولية الجنائية عن الأخطاء المرتكبة؛ على اعتبار أن الفقه والقضاء أكدوا على أهمية مساءلة البنوك عن الأخطاء المعلوماتية على أساس مواكبة متطلبات المجتمع والنظر للصفة المهنية التي تحتلها البنوك ومن تم كان لزاما وضع

(195) كلمة السيد والي بنك المغرب في الجلسة الافتتاحية للمؤتمر الإقليمي والشرق الأوسط الذي ينظمه بنك المغرب بشراكة مع صندوق النقد الدولي حول التحول الرقمي وتنفيذ برنامج بالي للتكنولوجيا المالية منشور في الموقع الرسمي للبنك: www.bkam.ma تاريخ الاطلاع 2024 / 2711 على الساعة 23:36.

(196) روان ثائر عيسى القيسي "أثر استخدام تقنية سلسلة الكتل blockchain على القوائم المالية في البنوك التجارية الأردنية" رسالة للحصول على درجة الماجستير في المحاسبة بجامعة الأوسط تشرين ثاني 2021 الصفحة: 36 وما يليها.

(197) Paolo Capuano corporate governance and artificial intelligence in the banking industry: challenges, risks and opportunities an article published international online conference june 5, 2025 "corporate governance: international outlook page : 31

(198) عبد الرزاق ابن يعيش "حكمة الأمن السيبراني نحو بناء منظومة قانونية فعالة لحماية البيانات الرقمية" رسالة لنيل دبلوم الماستر في قانون الخاص، جامعة عبد المالك السعدي كلية العلوم القانونية والاقتصادية والاجتماعية تطوان الموسم الجامعي 2024-2025 الصفحة: 161 وما يليها.

(199) وليد الشريبي "تأثير الذكاء الاصطناعي في إدارة المخاطر الائتمانية بالمصارف المالية" مقال إلكتروني منشور في الموقع التالي: <https://masrafeyoun.ebi.gov.eg> اطلع عليه يوم 2025/12/25.

(200) تم استعمال تقنية بلوك تشين بسلطنة عمان من قبل مصرف ظفار بتعاون مع شركة ريبيل بالتعاون مع جمعية المصارف العمانية كخطوة هامة في لتعزيز الحوكمة الالكترونية وتأمين المعاملات البنكية بشكل يقلل من مخاطر استخدام التقنيات الرقمية للمزيد راجع في هذا الإطار:

Raqiya Ahmed Al Hilali and Hothefa Shaker Published article on journal International Journal of Computing and Digital Systems may 2021 page: 719.

الآليات التشريعية لحفظ حق العملاء في التعويض وتحمل البنك المسؤولية عن كل المخاطر وتبني نظرية تحمل التبعة والمخاطر والذي عمل القضاء في المغرب وعمان على تطبيقها تكريسا للأمن السيبراني، ومن ثم سنعمل على تحديد نطاق المسؤولية المدنية للبنوك في مجال المعاملات الإلكترونية (المطلب الأول) فضلا عن التطرق إلى دور القضاء في حماية المجال البنكي وانخراطه في الجهود الدولية للحد من الجرائم الاقتصادية (المطلب الثاني).

المطلب الأول: المسؤولية المدنية للبنوك في نطاق المعاملات الإلكترونية

تعتبر العناية المصرفية مدخلا أساسيا لتنمية الثقة وضمان حماية المعاملات البنكية، فالمساس بالودائع البنكية ورؤوس الأموال يؤثر بشكل سلبي على علاقة مؤسسات الائتمان بعملائها، فمن الواجب والضروري التدخل لإقرار المسؤولية عن الاخلال بالضوابط والأعراف المهنية المنظمة للعمل البنكي بحكم وأنه لا ينبغي، التعرف على الذمة المالية والمعنوية للعملاء، نظرا لطابعها السلبي على المعاملات داخل المجتمع، لكن يتوجب بداية معالجة المسؤولية الرقمية للبنوك الفرع الأول تم بعد ذلك نعمل على تبيان المسؤولية الجنائية والتقنية للذكاء الاصطناعي في نطاق الخدمات البنكية (الفرع الثاني).

الفرع الأول: تكريس المسؤولية المدنية الرقمية للبنوك

تساهم أنظمة الذكاء الاصطناعي في تحسين اليات الكشف عن الاحتيال المالي وتقييم القروض باستخدام نماذج خوارزمية، لكن تبقى مخاطر استنساخ البيانات وغياب معايير مفتوحة لتقاسم المعلومات، وعدم فرض قيود على ولوج الشركات الناشئة في مجال التكنولوجيا المالية هاجسا يهدد الاستقرار البنكي.

وعليه فإن التزليل التدريجي للنظام البنكي المفتوح يعتبر من الأولويات التي، تتطلب اعتماد الآليات مفتوحة، وكذا قابلية نقل البيانات وإشراف خوارزمي. (201) فالخوارزميات تستعمل لاختراق الحسابات البنكية وتفشي أسرارهم الأمر الذي انعكس على مؤشر الثقة للأفراد، بشكل أصبح معه الحذر مطروحا عن أي عملية يريد العملاء القيام بها. (202)

فالذكاء الاصطناعي يركز على تطوير تقنيات وخوارزميات وأنظمة تعمل على تحليل البيانات والتعلم منها ومحاكاة بعض القدرات الإدراكية مثل الرؤية وفهم اللغة وحل المشكلات واتخاذ القرارات كما يمكن لهذه الأنظمة استنساخ حلول من البيانات المتاحة. (203)

ومن ثم فكل هذه المخاطر تبقى محتملة في المجال المصرفي، فيمكن اتخاذ قرارات مثل تحويل أموال من خلال استنساخ صوت أحد العملاء، مع العلم أن معظم المجرمين المعلوماتيون يعتمدون على استخدام تطبيقات مزيفة يكون غرضها هو السيطرة على المعلومات البنكية وتهديد استقرار النظام البنكي. (204)

بيد أن غياب نصوص خاصة في القانونين المغربي والعماني تطبق على أخطاء الذكاء الاصطناعي في المجال البنكي يطرح السؤال حول مساهمة القواعد العامة في ضبط أخطاء هذا الذكاء نرى أن المسؤولية تتخذ صورتين:

(201) المناظرة الوطنية حول "الذكاء الاصطناعي استراتيجيات فعالة وأخلاقية للذكاء الاصطناعي في خدمة مجتمعنا"، والذي انعقد يوم الرباط 2-1-2025 تم الاطلاع عليها بالموقع الرسمي لوزارة الانتقال الرقمي وإصلاح الإدارة عبر رابط التالي: <https://www.mmsp.gov.ma> يوم 12/28 / 2025 على الساعة 13:41.

(202) Marine Julien La confiance numérique dans le domaine bancaire THESE soutenue le 12 mai 2020 droit privé Université de la Rochelle page :35.

(203) المديرية العامة للسياسيات والحوكمة وزارة النقل والاتصالات وتقنية المعلومات، "السياسة العامة للاستخدام الآمن والأخلاقي لأنظمة الذكاء الاصطناعي سلطنة عمان" النسخة الأولى أبريل 2025 الصفحة: 7

(204) Patnaik, S. 2023, June 29. How advanced AI threatens banking security systems. Récupéré sur CENTRAL BANKING

<https://www.centralbanking.com>

الصورة الأولى: تتعلق باستخدام الذكاء الاصطناعي في المصارف المغربية والعمانية كوسيلة لأداء المعاملات البنكية واختصار الوقت من خلال استعماله في تحليل البيانات وضبط الخدمات فإنه تتحقق "المسؤولية عن حارس الشيء"؛ لأن البنك يتعين عليه اتخاذ جل الاحتياطات للتحكم في قرارات الذكاء الاصطناعي على نحو لا يضر بالعملاء. (205)

الصورة الثانية: تتصل بمسألة محاكاة الذكاء الاصطناعي للعنصر البشري وتصرف الروبوتات باستقلال عن العنصر البشري فإن المصرف يكون مسؤولاً في إطار "المسؤولية عن فعل الغير" نتيجة تسبب هذا الذكاء في أخطاء تمس بالمعطيات الشخصية والاستقرار المطلوب داخل القطاع المالي. (206)

الفرع الثاني: المسؤولية الجنائية والتقنية للبنوك في ظل استخدام الذكاء الاصطناعي

تعتبر التكنولوجيا المالية للمصارف ورشا استراتيجية لتحسين التمويل وتسريع عمليات الإقراض وإرساء الشفافية المطلوبة على اعتبار هذه التكنولوجيا تعتمد على الاتصالات، الأمر الذي قد يستغل في الهجمات الإلكترونية وقرصنة المعطيات الخاصة، ومن ثم يتعين تشديد الرقابة على الأجهزة الداخلية للبنوك وإقرار المسؤولية الجنائية والتقنية للأشخاص المخالفين وذلك تفادياً للأضرار بالنظام العام البنكي.

1- المسؤولية التقنية لأنظمة الذكاء الاصطناعي

عرفت المسؤولية القانونية للبنوك تغييراً عن الأنماط الكلاسيكية نتيجة انعكاس، الواقع الرقمي على المؤسسات المصرفية ومحاولتها مواكبة التطورات المتسارعة الناجمة عن استخدام التقنيات التكنولوجية لتسهيل الخدمات البنكية. (207) في حين تتضاعف مخاطر الأمن المعلوماتي المرتبط بمسألة الجانب التقني للبنوك فتخزين المعلومات يثير أكرهات الاختراق من الخارج والأخطاء التقنية من قبل مستخدمي البنوك بسبب ذلك ظهرت المسؤولية التقصيرية عن الأخطاء التقنية، وظهر تحدي بالنسبة للمسؤولية البنكية عن إدماج الذكاء الاصطناعي في تصريف الخدمات البنكية. (208)

2- المسؤولية الجنائية لأنظمة الذكاء الاصطناعي

تساهم أنظمة الذكاء الاصطناعي في مجموعة من الجرائم التقنية بما فيها المرتبطة بالمجال البنكي ومن ثم فإن المسؤولية الجنائية تعتبر أساسية لتحقيق الاستقرار البنكي غير أن التساؤل يطرح حول إمكانية تطبيق قواعد المسؤولية على هذا النوع من الأنظمة، في هذا الإطار يمكن مساءلة الروبوت كنظام ذكي انطلاقاً من الشخصية المفترضة وخاصة الإدراك والأتممة، الأمر الذي سيؤدي إلى تحميل الذكاء الاصطناعي المسؤولية الجنائية شخصياً في حالة ارتكابه جريمة معينة ينص القانون على عقوباتها.

(205) انظر الفصل 88 من ظهير الالتزامات والعقود المغربي والذي يقابله في القانون العماني المادة 199 من المرسوم السلطاني رقم 20/13/29 المتعلق بقانون المعاملات المدنية العماني.

(206) تميز في مجال قواعد المسؤولية التقصيرية لعمل البنوك بين مجرد فعل بسيط يرقى إلى مرتبة خطأ إذ عادة ما تلجأ المحاكم إلى تقدير هذا الخطأ بنوع من الشدة لعدة اعتبارات مرتبطة بالمركز الذي تحظى به البنوك:

يفترض في المؤسسة البنكية كطرف مهني أن تقوم بكافة الاحتياطات اللازمة من أجل تلافي كل ما يمكن أن يسبب للعميل ضرراً، فالمؤسسة البنكية يجب عليها نهج سياسة استباقية للحفاظ على سرية المعلومات وتقديم كافة الخدمات وفقاً للمبادئ الثقة والشفافية.

تشكل المصارف أساس الاقتصاد القومي لأي دولة وبالتالي فإنها ملزمة بالحرص على الحفاظ مكانتها داخل الأسواق الوطنية والدولية، فالإضرار بالعملاء وعدم تقديم خدمات بشكل أم قد يؤدي إلى المساس بالنظام الاقتصادي ككل وهو الأمر الذي تم تنظيمه ف ينص الفصل 77 من ظهير الالتزامات والعقود المغربي والمادة 187 من المرسوم السلطاني رقم 20/13/29 بإصدار قانون المعاملات المدنية العماني.

2. المسؤولية العقدية عن الخطأ البنكي

إلى جانب المسؤولية في شقها التقصيري، يمكن أن يسأل البنك عن المسؤولية في شقها العقدي في حالة إبرام عقد مستوفي لأركانه وشروط صحته، فكل تجاوز لبنود العقد يعتبر خرقاً يوجب إقرار المسؤولية البنكية العقدية وهو ما تم تكريسه في الفصلين 264 و339 من ظهير الالتزامات والعقود المغربي وقانون المعاملات المدنية العماني للمزيد حول موضوع المسؤولية البنكية راجع محمد جنكل "المسؤولية البنكية دراسة مقارنة بين التشريع المغربي والعمل القضائي" الحديث الطبعة الأولى سنة 2015 الصفحة: 16 وما بعدها.

-فصل 85 من ظهير الالتزامات والعقود المغربي والمادة 196 من القانون العماني المتعلق بالمعاملات المدنية.

(1) المادة 3 من منشور والي بنك المغرب.

(2) الفصل 85 من ظهير الالتزامات والعقود المغربي والمادة 196 من القانون العماني المتعلق بالمعاملات المدنية.

ومن تم يمكن أن يسأل الروبوت عن جرائم الاختراق وتفشي المعطيات الشخصية للعملاء وكذا جرائم غسل الأموال وبوجه عام كل الجرائم الاقتصادية التي لها صلة بالقطاع الائتماني.(209)

فطبيعة النشاط المصرفي تفرض بالإضافة إلى إقرار المسؤوليات القانونية إرساء ضوابط للحوكمة الرقمية بما يحقق التوازن بين الابتكار المالي وحماية المستهلكين وما يعزز هذا القول هو إطلاق بنك الإمارات دبي الوطني لمنصة الخدمات المصرفية غير الورقية عبر الأجهزة الإلكترونية والتي تتوافق مع الهوية الرقمية الإماراتية (UAE PASS) حيث أتاحت هذه المنصة المصادقة الفورية ومعالجة طلبات العملاء بالاستناد على تقنيات الذكاء الاصطناعي من خلال خدمات التفاعلية "إيفا" وأوليفيا "(210) وهي تجربة تؤكد قيادة الإمارات العربية المتحدة في مجال التكنولوجيا المتطورة والتي تعطي تجربة مبتكرة للعملاء. (211)

المطلب الثاني: المنازعات القضائية في حماية الأمن المعلوماتي للبنوك في التشريع المغربي والعُماني

تعمل جل التشريعات على تعزيز الحماية للخدمات البنكية، لكن فضلا عن ذلك يظهر دور القضاء في حماية النشاط الاقتصادي والمالي، وبالتالي يظهر الانخراط الإيجابي للقضاء، في تعزيز ثقة العملاء خاصة في ظل الطفرة الرقمية التي تعرفها المنظومة البنكية، جراء استعمال الذكاء الاصطناعي وسهولة الوصول إلى كافة المعلومات داخل الأجهزة البنكية وبالتالي فإن القضاء يحرص؛ على إعادة التوازن بين البنوك وعملائها وإرساء الشفافية في المعاملات.

وهذا إن دل على شيء إنما يدل على أن القضاء يتدخل من خلال القرارات القضائية لإقرار المسؤولية البنكية الرقمية، فارتباطا بمخاطر الذكاء الاصطناعي على القطاع المصرفي نجد أن محكمة النقض المغربية أقرت مسؤولية البنك عن عدم التوفر على نظم معلوماتية مؤمنة ضد جرائم الاختراق وقرصنة القن السري وعدم إمكانية تطبيق الفصلين 286 و269 من ظهير الالتزامات والعقود.(212)

وفي ذات السياق تم تأكيد في سلطنة عمان على ضرورة التكامل بين النظامين القضائي والمصرفي باعتباره ركيزة محورية، لتحقيق العدالة الناجزة وصون الحقوق المالية في بيئة اقتصادية، متطورة في إشارة إلى القضايا المصرفية، التي تعد من الأمور التي تتسم بالدقة والحساسية، وذلك لما تتضمنه من تفاصيل فنية ومحابسية معقدة تتطلب خبرات متخصصة ومعرفة دقيقة بطبيعة العمل المصرفي، واستعراض مسألة التحديات التي تواجه البنوك أمام المحاكم، وأهمية هذا التنسيق الذي يساعد على تنمية ودعم الاستقرار الاقتصادي في سلطنة عمان، ويواكب الاكراهات الناجمة عن استخدام تطبيقات الذكاء الاصطناعي والأدوات الرقمية في الأنشطة المصرفية، انسجاما مع رؤية عمان 2040.(213) سنقوم بداية بتبيان مسألة صعوبة اثبات الجرائم المصرفية بسبب تقنيات الذكاء الاصطناعي (الفرع الأول) ونخصص بعد ذلك شق خاص بصعوبة جمع الأدلة (الفرع الثاني).

الفرع الأول: صعوبة اثبات الجرائم المصرفية عند استخدام الذكاء الاصطناعي في المجال المصرفي

(209) سعادية مجيدي وآخرون، "التأصيل التشريعي للقانون الرقمي والعمل القضائي" مؤلف جماعي، دار النشر مطبعة الأمانة – الرباط دون ذكر الطبعة سنة 2022 الصفحة: 78 وما يليها.

(210) Eva هو أول مساعد افتراضي صوتي ذكي للخدمات المصرفية في منطقة الشرق الأوسط وشمال أفريقيا أطلقه بنك الإمارات دبي الوطني في نوفمبر 2016 حيث يتيح إمكانية التفاعل مع المساعد الافتراضي باللغة الطبيعية أو لغة المحادثة، ويقدم خدمات أكثر سرعة وبساطة تناسب احتياجات كل عميل بأسلوب تفاعلي ذكي

أما liv فهي منصة رقمية للخدمات المصرفية تابعة لبنك الإمارات دبي الوطني وهو برنامج فريد من نوعه للبطاقات الائتمانية وهي تجربة تناسب طموحات وتطلعات العملاء للمزيد حول هذه التقنيات الذكية راجع الموقع الرسمي لبنك الإمارات دبي الوطني تم الاطلاع عليه يوم 2026/02/27 على الساعة 23:15 عبر الرابط التالي:

<https://www.emiratesnbd.com/ar/media-center/liv-launches-uaes-most-flexible-credit-card>

(211) وليد عبد الله محمود " المخاطر القانونية للذكاء الاصطناعي في الخدمات المصرفية دراسة تحليلية مقارنة " مقال منشور في مجلة اداب الفراهيدي جامعة تكريت العدد 2663- 811 سنة 2025 الصفحة: 113

(212) قرار صادر عن محكمة النقض عدد 372/1 الصادر بتاريخ 27/07/2017 في الملف التجاري عدد

1365/1/3/2016، منشور على دفاتر محكمة النقض، العدد 31 سنة 2020 الصفحة: 61.

(213) فعاليات وزارة العدل والشؤون القانونية "ندوة التكامل بين النظامين القضائي والمصرفي في معالجة القضايا المالية والمصرفية رؤية مشتركة"، والمنشورة على الموقع الرسمي لوزارة العدل والشؤون القانونية العمانية اطلع عليه على الساعة 12:45 يوم 2026/01/04 <https://www.mjla.gov.oma>

أدى التقدم الإلكتروني إلى تضاعف صور الغش في التسوق ونقل الأموال بالوسائل الإلكترونية وعائدات الجريمة ونقلها وإخفاء الأرباح المشبوهة، عبر الأداء بالبطاقات البنكية مباشرة لكن يبقى الاعتراض واختراق البنوك وسرقة الأرصدة وتحويلها إلى حسابات أخرى هاجس يضع جل التشريعات أمام ضرورة الضبط البنكي، خاصة في ظل الانفتاح، واستعمال الذكاء الاصطناعي الذي يمكن أن يستغل في نقل المعطيات المصرفية للأغيار غير المصرح لهم بشكل قانوني بالوصول إليها، إذ يمكن للذكاء الاصطناعي الوصول إلى المعلومات السرية بسهولة وبدون رقابة نتيجة للعولمة والتقدم الهائل الذي يعرفه العالم، في ظل وجود مشكل اثبات هذا النوع من الجرائم المرتكبة في الفضاء الرقمي.⁽²¹⁴⁾

1- الجهود الوطنية والدولية لمكافحة الاجرام المعلوماتي على النظم المصرفية.

في مستهل الحديث عن الجهود الوطنية والدولية في مكافحة الاجرام المعلوماتي بما فيه النشاط المصرفي، يلزم تعزيز التعاون بين دول العالم للتغلب على الاحتيال باستخدام الأنظمة الذكية وتدمير البيانات أو الوصول إلى البرامج بدون تصريح، ويمكن القيام بكل هذه الأعمال غير المشروعة بالاستناد على الذكاء الاصطناعي، فإن هذا المعطى يستدعي تكثيف التكامل بما يحافظ على الاستقرار النقدي للدول ويحافظ على السيادة الرقمية.⁽²¹⁵⁾

وفي ضوء هذه التطورات اتجه المجتمع الدولي نحو إصدار العديد من الاتفاقيات الدولية والعربية من أبرزها اتفاقيتي بودابست⁽²¹⁶⁾ وهانوي⁽²¹⁷⁾ بشأن منع الجريمة السيبرانية، وفي نفس السياق عملت الدول العربية على تنسيق الجهود من أجل تلافي الأضرار المتعلقة بالجرائم التقنية والتي بطبيعة الحال؛ تهدد أمنها ومصالحها وسلامة مجتمعاتها بحيث جرمت مسألة تدمير أو محو أو إعاقة أو تعديل أو حجب البيانات دون مقتضى قانوني، وفي هذا النطاق فإن جل هذه الأحكام تنطبق على المصارف العربية لما تحمله الجرائم الإلكترونية من تأثير سلبي على الشق الاستثماري والائتماني، وانعكاسه على ثقة العملاء في نطاق العمليات البنكية وهو ما دفع المشرعين العماني والمغربي للمصادقة على أحكام هذه الاتفاقية.⁽²¹⁸⁾

الفرع الثاني: صعوبة جمع الأدلة في الجريمة المعلوماتية البنكية بسبب إخفاء البيانات

تختلف صور الجرائم العادية عن الجرائم المعلوماتية التي تقع على الحسابات أو بواسطتها والتي تكون في الغالب الأعم بشكل خفي لا يلاحظها المجني عليه أو يدري حتى بوقوعها، على اعتبار أن التلاعب في المنظومة الإلكترونية البنكية؛ يهدد الحاسب الآلي ويتم

(214) سيف بن عبد الله بن سعيد، عملة الجريمة الاقتصادية ومواجهتها في التشريع المغربي والعماني أطروحة لنيل شهادة دكتوراه في قانون خاص بكلية العلوم القانونية والاقتصادية جامعة محمد الأول بو جدة الموسم الجامعي 2017/2016 الصفحة: 15 وما يليها.

(215) ادريس النوازي "جريمة النصب المعلوماتي والتعاون الدولي" مقال منشور في المجلة المغربية للقانون التجاري والأعمال العدد 3 / 2015 الصفحة: 31.

(216) الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية بودابست والتي نصت في المادة 3 منها على ضرورة:

1- أن تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني إذا ما ارتكبت عمدا: إتلاف بيانات حاسوبية أو حذفها، إفسادها أو تعديلها أو تدميرها.

2- يجوز لدولة طرف أن تحتفظ بحققها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة -

الأولى من ضرر جسيم تم الاطلاع عليه عبر الموقع الرسمي لمجلس أوروبا <https://rm.coe.int/budapest> يوم 2026/01/04 الساعة 14:00

(217) جاء في أحكام المادة الأولى من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية والتي انعقدت يوم 31 كانون سنة 2025 بالعاصمة الفيتنامية هانوي ما يلي "أ تشجيع وتعزيز التدابير الرامية إلى منع ومكافحة الجريمة السيبرانية على نحو أكثر كفاءة وفعالية؛

ب تشجيع وتيسير وتعزيز التعاون الدولي في مجال ومنع ومكافحة الجريمة السيبرانية؛

ج تشجيع وتيسير ودعم وتوفير المساعدة التقنية وبناء القدرات من أجل منع ومكافحة الجريمة السيبرانية وخصوصا لصالح دول النامية؛

للاطلاع على أحكام هذه الاتفاقية راجع الموقع الرسمي للأمم المتحدة عبر الرابط التالي <https://www.unodc.org> تمت مراجعته يوم 2026/01/04 الساعة 13:48

(218) للمزيد انظر الاتفاقية العربية لمكافحة الجرائم التقنية والموقعة يوم 2010/ 10/21 بالعاصمة المصرية القاهرة والتي صادق عليها كل من المشرع المغربي بموجب ظهير شريف رقم 46.1.13 صادر في فاتح جمادى الأولى 1434 الصادر 13 مارس 2013 بتنفيذ القانون رقم 75.12 الموافق بموجبه على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة 21 ديسمبر 2010. والمنشور على الموقع الرسمي للمجلس الأعلى للسلطة القضائية عبر رابط التالي: <https://www.cspj.ma> تم الاطلاع عليه عبر رابط 206/01/04 على الساعة 14:30

وكذلك صادق عليه المشرع العماني في الجريدة الرسمية عدد 1093 بشأن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إخفائه، عبر التجسس على ملفات البيانات المخزنة في البنوك واستنساخها، ومن تم من الطبيعي أن يقلل الذكاء الاصطناعي من فرص المؤسسات البنكية في التنبؤ بالمخاطر أو كشفها.⁽²¹⁹⁾

1 - غياب الدليل المادي في الجرائم المعلوماتية البنكية

نظرا للطبيعة التقنية للمنظومة المعلوماتية واستهداف البيانات غير المرئية يصعب الكشف عن هوية مرتكبها، الفعل الذي يصعب على المستخدمين داخل المصارف من التدقيق في هوية المجرمين المعلوماتيين خاصة، عند استخدام تقنيات الذكاء الاصطناعي إذ تصبح عملية الوصول إلى دليل مادي ضد استهداف النظام الألي البنكي ومعرفة الشخص الذي يقف وراء عملية معالجة الخدمات البنكية بشكل غير مصرح به صعبة.⁽²²⁰⁾

2 - سهولة تغيير ومحو الدليل الرقمي لاختراق النظام المعلوماتي

يساهم الذكاء الاصطناعي في محو الدليل وتعديله داخل حيز زمني قصير، مما ينتج عنه وجود عوائق تقنية تساعد المجرم المعلوماتي على التخفي لاسيما وأن حجم البيانات التي تتم معالجتها على مستوى الجهاز البنكي في تزايد، إلا أن هذا ليس هو السبب الوحيد، الذي يطرح صعوبة الإثبات بل هناك عامل آخر يضاعف من صعوبة الكشف عن الجرائم المعلوماتية في نطاق الاعتداء على أسرار العملاء وهو الإحجام الكبير في التبليغ عن الجرح من قبل المؤسسات البنكية، فعادة ما تفضل عدم الكشف عن ما تعرضت له من اختراق حتى في مواجهة المستخدمين، والباعث وراء ذلك هو تفادي الإضرار بسمعتها التجارية.⁽²²¹⁾

3 - جهود الشرطة القضائية في البحث والتحري عن هذا الصنف من الجرائم

تقوم الشرطة القضائية بدور طلائعي في التصدي للجريمة الرقمية البنكية، ومنع كل الاختراقات التي من شأنها المساس بالحقوق والحريات داخل المجتمع، في هذا الصدد بدل المغرب جهود، وذلك بتكوين مجموعة من المحققين المتخصصين في ميدان الجريمة الإلكترونية وتم إلحاقهم بالمصالح الولائية والجهوية للأمن الوطني، كما تم إنشاء خلية مكافحة الجرائم المعلوماتية ووحدة خاصة على مستوى الفرقة الوطنية للشرطة القضائية، فضلا عن معالجة الجرائم التقنية وتوفير الدعم للمصالح الخارجية للشرطة القضائية في إطار البحث والتحري بشأن هذا النوع من الجرائم.⁽²²²⁾

أما على المستوى القانوني فإن المشرع المغربي أعطى صلاحيات واسعة لضباط الشرطة القضائية بمقتضى المادة 57 من قانون المسطرة الجنائية الجديد في الشق المتعلق بتقنيات البحث والتحري عن الجرائم الرقمية حيث يتولى ضباط الشرطة القضائية بحث الآثار والمعالم المتخلفة من الجريمة ويقوم برفعها باعتماد الوسائل التقنية والفنية التي يستلزمها هذا الإجراء، كما يقوم برفع الآثار وحجز التسجيلات السمعية البصرية من مكان ارتكاب الجريمة.⁽²²³⁾

في مقابل ذلك أيضا أعطى المشرع العماني صلاحيات واسعة في المادة 30 من المرسوم السلطاني 79 / 2022 حيث خول لمأموري الضبط القضائي البحث عن الجرائم وجمع الاستدلالات وأن يتخذوا جميع الوسائل اللازمة للمحافظة على أدلة الجريمة.⁽²²⁴⁾

(219) محمد كمال نور الدين طوطح " الجريمة المعلوماتية في المجال البنكي " دراسة مقارنة رسالة لنيل دبلوم الماستر في قانون الخاص بكلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض بمراكش السنة الجامعية 2014/2015 الصفحة: 78.

(220) هشام محمد فريد رستم "الجوانب الإجرائية للجرائم المعلوماتية" دار النشر، مكتبة الآلات الحديثة بأسبوط سنة 1994 الصفحة: 16.

(221) (مراد العلمي " السرية المصرفية بين متطلبات العمل البنكي وتحديات الأموال غير النظيفة" أطروحة لنيل دكتوراه في قانون الخاص جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط أكدال الموسم الجامعي 2011 -2012: 333 وما بعدها

(222) محمد كمال نور الدين طوطح " الجريمة المعلوماتية في المجال البنكي " مرجع سابق الصفحة: 92 وما يليها

(223) الظهير الشريف رقم 1.25.5 الصادر في 19 من صفر 1447 13 أغسطس 2025 بتنفيذ القانون رقم 03.23 بتغيير وتنظيم القانون رقم 22.01 المتعلق بالمسطرة الجنائية، منشور بالجريدة الرسمية عدد 7437 ربيع الأول 1447 (8 سبتمبر 2025) الصفحة: 6976.

(224) المرسوم السلطاني 79 / 2022 الصادر بالجريدة الرسمية عدد: 1473.

فمخاطر الاحتيال الالكتروني في ارتفاع مستمر بحيث بلغ نسبته في سلطنة عمان 50% خلال النصف الأول من عام 2025 مقارنة بالفترة نفسها العام الماضي؛ في خضم الانتشار الواسع في الوسائل التقنية وأنظمة الدفع الإلكتروني واستعمال المنصات الرقمية.(225)

بالإضافة إلى ذلك يؤدي توسع استعمال الذكاء الاصطناعي في تحليل سلوكيات المستهلكين ضمن المعاملات المصرفية الرقمية لمخاطر واحتمال نشر المعطيات الشخصية عبر الانترنت أو شبكات التواصل الاجتماعي أو إساءة استخدامها للتأثير على قرارات العملاء دون علمهم، الأمر الذي يضع ثقتهم في الوسائط المالية الرقمية على المحك.(226) ولتوضيح حجم مخاطر الذكاء الاصطناعي وتأثيره على الاستقرار البنكي على سنعمل على تبيان بعض صور الهجمات الإلكترونية التي تستهدف النظام المعلوماتي للبنوك وفقا للجدول التالي:(227)

الاحصائيات "على مستوى الدولي"	
ارتفاع "حوادث" الذكاء الاصطناعي المرتبطة بالأمن والخصوصية سنة 2024 على مستوى الدولي	تم تسجيل نسبة 56.4 % بشأن الجرائم المرتبطة بالذكاء الاصطناعي
مخاطر الامتثال الوظيفي عن سوء استخدام الذكاء الاصطناعي	تم تسجيل غرامات تصل إلى 35 مليون يورو بنسبة 7% من رقم المعاملات العالمية
على المستوى المقارنة بين "التشريع المغربي والعُماني"	
على مستوى التشريع المغربي	على مستوى التشريع العماني
تعرف جرائم المس بالنظم الالية للمعالجة المعطيات نسب مئوية مرتفعة تصل إلى 59% حسب تقرير رئاسة النيابة العامة لسنة 2024	ارتفعت مخاطر الاحتيال الالكتروني في ارتفاع مستمر بحيث بلغ نسبته في سلطنة عمان 50 % خلال النصف الأول من عام 2025 حسب المدير العام لتحريات والبحث الجنائي

خاتمة

صفوة القول، يعد تطبيق الذكاء الاصطناعي في المجال المصرفي مدخلا أساسيا لتجويد العمليات وضمان التنافسية البنكية وتحسين مناخ الأعمال، ومن تم تساهم أنظمة الذكاء الاصطناعي في إرساء الشفافية والكفاءة والسرعة والامتثال التنظيمي للبنوك، لكن ومع ذلك لا تزال هناك تحديات تتعلق بتوفير حماية للبيانات وضمان عدم تحيز الخوارزمي في القرارات الائتمانية وعدم تمييز العملاء، بناء عليه ينبغي مواجهة المخاطر بشكل فعال ومستدام ينعكس بشكل إيجابي على مؤشر الثقة البنكية في القانونين المغربي والعُماني.

(225) أكد المدير العام لتحريات والبحث الجنائي بشرطة عمان السلطانية وأن سبب ارتفاع هذا النوع من الجرائم راجع إلى وتيرة التطور والتكنولوجيا وأنظمة الدفع الإلكتروني التي سهلت الحياة اليومية على الأفراد والمجتمعات، لكن في مقابل ذلك رافق ذلك زيادة في الأساليب الجرمية التي يبتكرها المحتالون بشكل متواصل، للإيقاع بضحاياهم عبر تقنيات متطورة، وعلى وجه الخصوص أساليب تستند إلى الذكاء الاصطناعي AI والتزييف العميق، تأكيداً على المجرمين الإلكترونيين باتوا أكثر براعة في التنكر بثوب الحقيقة والتلاعب بمشاعر وثقة الضحايا بهدف الاستيلاء على أموالهم وسرقة معطياتهم الخاصة.

الموقع الرسمي للوكالة الأنباء العمانية " ارتفاع جرائم الاحتيال الرقعي في سلطنة عمان تم الاطلاع عليه يوم 2026/01/10 عبر رابط تالي:

<https://omannews.gov.om/topics/ar/3/show/457578> على الساعة 22:00

(226) وليد عبد الله محمود " المخاطر القانونية الذكاء الاصطناعي في الخدمات المصرفية دراسة تحليلية مقارنة " مرجع سابق الصفحة: 121

Artificial Intelligence Index Report 2025 <https://hai.stanford.edu/> Le 30/01/2025 à l'heur 19 : 30

EU AI ACT "publication dans le site <https://ai-act-service-desk.ec.europa> Le 30/01/2025 à l'heur 20 : 00

وفقا للتقرير السنوي لسنة 2024 الذي أصدرته النيابة العامة تم الاطلاع عليه في الموقع الرسمي عبر رابط التالي: يوم 2026/01/30 على الساعة 20:30

<https://www.pmp.ma/bibliotheque>

بناء على هذه الدراسة خالصنا إلى مجموعة من النتائج والمقترحات نجملها على الشكل التالي:

1- النتائج

- ارتفاع عدد الهجمات الإلكترونية على البنوك بسبب استخدام الذكاء الاصطناعي في عملية المعالجة الخاصة بالمعلومات والبيانات الخاصة للعملاء.
- أصبح الذكاء الاصطناعي ضرورة هامة لتحقيق السرعة والفعالية في الخدمات البنكية.
- جل الدول والمنظمات الدولية تعمل على مضاعفة الجهود لتخفيف من تأثير مخاطر الذكاء الاصطناعي على المنظومة المالية والاقتصادية على اعتبار أن استعمال الذكاء الاصطناعي في المجال البنكي سي طرح تحديات أخرى على مستوى صعوبة التحري على الإجماع المعلوماتي.
- أهمية مسايرة للمسؤولية القانونية سواء في الشقين المدني أو الجنائي لتدخل من أجل حماية المصارف وتعويض العملاء على الأضرار المالية والمعنوية على حد سواء.
- عمل المغرب وعمان على توفير بيئة قانونية هامة في مجال حماية القطاع البنكي والمعطيات الشخصية فضلا عن الحماية التقنية للبيانات، وهناك خطوات جديدة نحو وضع إطار قانوني لمواجهة مخاطر الذكاء الاصطناعي.

2- المقترحات

- وضع قانون خاص بالذكاء الاصطناعي في كل من المغرب وعمان لتحديد الضوابط القانونية والأخلاقية للعمل به داخل المجال البنكي.
- وضع اليات لمراقبة الذكاء الاصطناعي للحد من مشكل التجسس والاحتيال المالي.
- تكوين موارد بشرية متخصصة في الذكاء الاصطناعي لمسايرة الزخم المتسارع لاستعماله في الأنشطة البنكية
- وضع استراتيجية خاصة بالذكاء الاصطناعي في المجال المصرفي.
- استخدام أنظمة الذكاء الاصطناعي وتقنية الروبوتات لتوفير الجهد والشفافية مع الأخذ بعين الاعتبار زيادة حجم الاجرام التقني للبنوك والذي يتطلب أساسا وجود اليات للتحري عن هذه الجرائم وفقا لخصوصية هذا الصنف من الجرائم المعقدة.
- توعية العملاء بأهمية الذكاء الاصطناعي في المجال المصرفي.
- مواكبة العولمة الاقتصادية لتأهيل البنوك اقتصاديا وجعلها قادرة على المنافسة.

❖ لائحة المصادر المعتمدة:

الكتب المتخصصة:

- أنطوان جورج سرقيس "السرية المصرفية في ظل العولمة" دار النشر منشورات الحلبي الحقوقية الطبعة الأولى سنة 2008
- عبد البليل "التحديات القانونية للخدمات المصرفية في ضوء الذكاء الاصطناعي" (دار النشر غير مذكورة)، طبعة سنة 2024.
- علاء التميمي "التنظيم القانوني للبنك الإلكتروني على شبكة الإنترنت" دار النشر الجامعة الجديدة الإسكندرية دون ذكر الطبعة سنة 2012
- الكتب العامة:
- محمد جنكل "المسؤولية البنكية دراسة مقارنة بين التشريع المغربي والعمل القضائي" "الحديث الطبعة الأولى سنة 2015

• مصطفى مالك "النظام القانوني لمقدمي خدمات الثقة بشأن المعاملات الإلكترونية" دار النشر، دار السلام للطباعة والنشر والتوزيع – الرباط الطبعة الأولى سنة 2023

• نهلا عبد القار المومني "الجرائم المعلوماتية" دار النشر دار الثقافة للنشر والتوزيع عمان الطبعة الأولى سنة 2008
لائحة الأطاريح والرسائل

• محمد كمال نور الدين طوطح "الجريمة المعلوماتية في المجال البنكي دراسة مقارنة" رسالة لنيل دبلوم الماستر في قانون الخاص بكلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض بمراكش الموسم الجامعي 2014/2015.

• مراد العلمي "السرية المصرفية بين متطلبات العمل البنكي وتحديات الأموال غير النظيفة" أطروحة لنيل دكتوراه في قانون الخاص جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط أكمال الموسم الجامعي 2011-2012
الرسائل:

• مروان الدلكي "حماية المعطيات ذات طابع الشخصي في عصر الذكاء الاصطناعي" رسالة لنيل دبلوم الماستر في القانون الخاص جامعة القاضي عياض كلية العلوم القانونية والاقتصادية والاجتماعية بمراكش الموسم الجامعي 2025 - 2026.

• نسمة الخلفي "الحماية الجنائية والتقنية للبيانات البنكية" رسالة لنيل دبلوم الماستر في القانون الخاص جامعة القاضي عياض كلية العلوم القانونية والاقتصادية والاجتماعية بمراكش الموسم الجامعي 2018-2019

• روان ثائر عيسى القيسي "أثر استخدام تقنية سلسلة الكتل blockchain على القوائم المالية في البنوك التجارية الأردنية" رسالة للحصول على درجة الماجستير في المحاسبة بجامعة الأوسط تشرين ثاني سنة 2021

• عبد الرزاق ابن يعيش "حكمة الأمن السيبراني نحو بناء منظومة قانونية فعالة لحماية البيانات الرقمية" رسالة لنيل دبلوم الماستر في قانون الخاص، جامعة عبد المالك السعدي كلية العلوم القانونية والاقتصادية والاجتماعية تطوان الموسم الجامعي 2024-2025
المقالات:

• عبد الكريم عباد "الجريمة المعلوماتية" مقال منشور في المجلة الوطنية للعلوم القانونية والقضائية، العدد الأول مطبعة الأمنية – الرباط سنة 2020.

• محمد حمداوي "تأثير الذكاء الاصطناعي على الخدمات البنكية بين تحسين الجودة وحماية الخصوصية" مقال منشور بمجلة الالكترونية للأبحاث القانونية العدد 15 سنة 2025.

• وليد عبد الله محمود "المخاطر القانونية للذكاء الاصطناعي في الخدمات المصرفية دراسة تحليلية مقارنة" مقال منشور في مجلة اداب الفراهيدي جامعة تكريت العدد 2663- 811 سنة 2025

• جودية خليل "المعلومة بين الإفصاح وقيد الإبقاء طي الكتان" مقال منشور في مجلة أطروحة للدراسات والأبحاث في العلوم القانونية عدد خاص سنة 2024
المواقع الإلكترونية:

• الموقع الخاص بالمجلس الأوروبي: www.coe.int/budapest-convention-in-arabic

• الموقع الرسمي لبنك المغرب: <https://www.bkam.ma>

• الموقع الرسمي لوزارة النقل والاتصالات والمعلومات لسلطنة عمان: <https://mtcit.gov.oma>

• الموقع الرسمي لرئاسة النيابة العامة: <https://www.pmp.ma/bibliotheque>

• الموقع الرسمي لوزارة الانتقال الرقمي وإصلاح الإدارة: <https://www.mmsp.gov.ma>

• الموقع الرسمي لوزارة العدل والشؤون القانونية العمانية: <https://www.mjla.gov.oma>

• الموقع الرسمي للمجلس الأعلى للسلطة القضائية عبر رابط التالي: <https://www.cspj.ma>