

الأمن السيبراني وحماية خصوصية البيانات الرقمية في الإمارات في عصر التحول الرقمي والذكاء الاصطناعي
**"CYBERSECURITY AND THE PROTECTION OF DIGITAL DATA
PRIVACY IN THE UAE IN THE ERA OF DIGITAL TRANSFORMATION
AND ARTIFICIAL INTELLIGENCE"**

ميثاء مصباح سالم بن ضاوي الخاطري
Islamic Civilization Academy
maithaalkhateri226@gmail.com
musabahsalem@graduate.utm.my

ضياء الدين الزيتاوي
Islamic Civilization Academy
diaya@utm.my

الملخص

إن قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر - عصر الثورة الصناعية الرابعة حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات، لكن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، وتكمن المشكلة في عدم وضوح جاهزية دولة الإمارات وأنظمتها الدفاعية الإلكترونية، ويمكن استخلاص ذلك من الاستراتيجيات والآليات التي تنتهجها الدولة الإماراتية لتوفير الحماية لبنيتها المعلوماتية الأساسية. وتهدف دراستنا هذه إلى كشف واقع الأمن السيبراني وخصوصية البيانات الرقمية الموجودة على قواعد البيانات والمواقع الإلكترونية في الإمارات العربية المتحدة، و المكانة التي تعطيها لها الدولة الإماراتية ضمن منظومتها الأمنية، ويتحقق ذلك من خلال التعرف على أنواع التهديدات السيبرانية التي تواجهها الإمارات، وأهم التقنيات المستحدثة التي تستخدم في اختراق البيانات الرقمية وتنفيذ الهجمات والحروب السيبرانية، وأيضاً الوصول إلى التحديات والعقبات التي تقف أمام تنفيذ السياسة الأمنية الداخلية لدحض الجريمة الإلكترونية عموماً، ومن ثم معرفة الإجراءات الاحترازية وآليات التصدي للهجمات السيبرانية التي تعمل عليها الإمارات، ووسائل المعالجة في حالة وقوع الهجمات، وباعتبار أن الإمارات تسير نحو التحول إلى رقمته جميع القطاعات، مما ينعكس على تزايد التهديدات على أمنها الداخلي وبنيتها التحتية الحيوية - في ظل التطور غير المسبوق في تقنيات الذكاء الاصطناعي، توجب علينا دراسة هذا الموضوع لما له من أهمية بالغة على مستوى الأمن الداخلي وخصوصية البيانات الشخصية، ولتحقيق الكفاية البحثية والوصول إلى إجابات وافية حول الموضوع استخدمنا منهجية شاملة تشمل البحث المكتبي لجمع المعلومات والبيانات من الكتب، والمقالات العلمية، والتقارير الرسمية المتعلقة بالأمن السيبراني ودور الإمارات في هذا المجال. أظهرت الدراسة أن الأمن السيبراني يشمل حماية الأنظمة الإلكترونية والمعلومات الحساسة من الهجمات، وأكدت دور الإمارات في تعزيز هذا المجال من خلال تطوير استراتيجية وطنية وإنشاء هيئة تنظيم الاتصالات وسن قوانين مثل قانون مكافحة جرائم تقنية المعلومات، تبين أن الإمارات تمتلك جاهزية دفاعية إلكترونية قوية بفضل التعاون الحكومي والدولي، رغم التحديات المتزايدة مثل التهديدات المعقدة والتطور السريع للتكنولوجيا، تسلط الدراسة الضوء على أهمية التوعية السيبرانية والتعليم والتدريب المستمر لتعزيز الأمن السيبراني.

كلمات مفتاحية: الأمن السيبراني، خصوصية البيانات الرقمية، الجريمة السيبرانية (الإلكترونية)، التحول الرقمي، الذكاء الاصطناعي.

المقدمة:

مما لا شك فيه فالأمن المعلوماتي يعد مجموعة من الإجراءات والتدابير التي تتخذها المؤسسات والأفراد لحماية أنظمتهم الإلكترونية والمعلومات الحساسة والبيانات من التهديدات والهجمات الإلكترونية، كما يهدف إلى ضمان سلامة وسرية المعلومات والبيانات والحفاظ على توافر الخدمات الرقمية وحماية البنية التحتية الرقمية للمؤسسات والمنظمات، ومنه فالأمن الرقمي هو مفهوم يشبه إلى حد كبير مفهوم الأمن الإلكتروني أو الأمن السيبراني، بحيث يرتبط الأمن الرقمي بحماية الأنظمة الرقمية الحساسة والبيانات من التهديدات الإلكترونية والهجمات السيبرانية إلا أنه يركز بشكل أوسع على الجوانب الرقمية والإلكترونية للأمان، ويشمل أيضاً مجموعة من العمليات والسياسات والممارسات التي تهدف إلى ضمان الحفاظ على أمان العالم الرقمي. (المهيري، 2023) إن قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر - عصر الثورة الصناعية الرابعة حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات، لكن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها، وتختلف هجمات الهاكرز من جهة الأخرى ومن مكان لآخر ومن زمن إلى زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت، وهذا يؤكد على أهمية الأمن الإلكتروني وذلك للحفاظ على أمن وسلامة الوطن والمواطنين. (سالم، 2022) فمن الجوانب التي يتم التركيز عليها في أمن السيبراني بدولة الإمارات العربية المتحدة والتي تهدف إلى تحسين مستوى الأمن الرقمي وتعزيز استدامة التكنولوجيا الرقمية وتطور المجتمع، نجد استراتيجية الأمن السيبراني تم تطوير استراتيجية وطنية للأمن السيبراني تهدف إلى تحسين مستوى الأمان الإلكتروني وحماية المعلومات والبنية التحتية الرقمية للدولة. (الحميري، 2023)

وتتضمن هذه الاستراتيجية تحديد الأهداف والمبادئ التوجيهية لتعزيز الأمن السيبراني في جميع القطاعات وتتجلى في:

هيئة تنظيم الاتصالات بحيث تلعب هيئة تنظيم الاتصالات (TRA) دوراً رئيسياً في تعزيز الأمان السيبراني في الإمارات تتولى TRA تنظيم ومراقبة قطاع الاتصالات وتقنية المعلومات وتطوير اللوائح والسياسات المتعلقة بالأمن السيبراني، بالإضافة إلى قوانين ولوائح الأمان السيبراني بحيث يتم وضع مجموعة من القوانين واللوائح لتعزيز الأمن السيبراني في الإمارات. يشمل ذلك قانون الجرائم الإلكترونية والمعلوماتية وقانون حماية المعلومات الشخصية والعديد من اللوائح الأخرى التي تنظم مجال الأمان السيبراني.

وفي هذا الاطار استهدفت رؤية الإمارات العربية المتحدة التطوير الشامل للوطن واقتصاده وأمنه ورفاهية مواطنيه وعيشهم الكريم، ولقد كان من الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وحمايته إلكترونياً وتنمية البنية التحتية الرقمية؛ بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتمشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها وبما يهيئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة. (نصار، 2021)

يشكل موضوع الأمن السيبراني معضلة العصر باعتباره السلاح الاستراتيجي الحالي، نظراً لما يفرزه الواقع التكنولوجي الذي يفرض نفسه على المجتمعات ومتطلباته من تهديدات سيبرانية غير معروفة وهجمات غير متوقعة، تثير تخوف الجميع، وبما أن الإمارات تتجه بشكل متسارع نحو رقمنة قاطاعاتها وهياكلها الحساسة، فقد بات من الضروري مناقشة، اهتمامها بقضية تأمين منظومتها الإلكترونية، وبنيتها المعلوماتية التحتية، ومدى قدرتها على توفير الأمن المناسب والحماية الكافية لمستخدمي الفضاءات الإلكترونية، وتكمن المشكلة في أنه لا بد معرفة مدى جاهزية دولة الإمارات وأنظمتها الدفاعية الإلكترونية، ويمكن استخلاص ذلك من الاستراتيجيات والآليات التي تنتهجها الدولة الإماراتية لتوفير الحماية لبنيتها المعلوماتية الأساسية.

ومنه تبرز لنا أهمية الموضوع كون تطور الثورة التكنولوجية أدى إلى زيادة عدد الأجهزة المتصلة بشبكة الإنترنت؛ الأمر الذي وفر أرضية خصبة للجرائم الإلكترونية، ومما لا شك فالأمن الرقمي والسيبراني أمر ضروري لحماية الأمن القومي للدول؛ لما له من دور في حماية مختلف القطاعات الحيوية من الهجمات الإلكترونية، وبذلك فتعد دولة الإمارات من الدول التي خطت خطوات مهمة لتعزيز ممارساتها في مجال الأمن السيبراني، منها إقرار «الاستراتيجية الوطنية للأمن السيبراني، وكذلك إعلان دولة الإمارات إنشاء مجلس للأمن السيبراني جاء من أجل تعزيز الأمن السيبراني؛ ورفع جاهزية جميع القطاعات للاستجابة للتهديدات.

تهدف هذه الدراسة إلى تعريف مفهوم الأمن السيبراني وتوضيح أهميته في العصر الرقمي الحالي، بالإضافة إلى دراسة دور دولة الإمارات في هذا المجال من خلال تسليط الضوء على الجهود والمبادرات التي تقوم بها لتعزيز الأمن السيبراني، كما تسعى الدراسة إلى تحليل الاستراتيجيات والآليات الوطنية واللوائح والقوانين التي تم وضعها لتعزيز الأمان السيبراني في الإمارات، وتقييم مدى جاهزية الأنظمة الدفاعية الإلكترونية وقدرتها على التصدي للتهديدات السيبرانية. كذلك، تهدف إلى تسليط الضوء على التحديات التي تواجهها الإمارات في مجال الأمن السيبراني والفرص التي يمكن استغلالها لتحسين الوضع الأمني السيبراني.

لتحقيق أهداف هذه الدراسة، سيتم اتباع منهجية شاملة تشمل البحث المكتبي لجمع المعلومات والبيانات من الكتب والمقالات العلمية والتقارير الرسمية المتعلقة بالأمن السيبراني ودور الإمارات في هذا المجال.

مفهوم الأمن السيبراني:

إن لفظة سيبار (Cyber) هي كلمة يونانية، مشتقة من كلمة (Kybernets)، وتعني الشخص الذي يدير دفة السفينة، وهناك من يرجع أصل اللفظة إلى منتصف القرن 20، مع عالم الرياضيات الأمريكي "Narbert Wiener"، الذي استخدمها للتعبير عن التحكم الآلي، حيث عرف السيبرنيتيكية على أنها "التحكم والتواصل عند الحيوان والآلة"، كما ذكر في الكتاب ذاته أنها "علم نقل الرسائل بين الإنسان والآلة أو بين الآلة والآلة"، من هنا تبلورت السيبرانية وتم توظيفها للتعبير عن العمليات الآلية والعلاقات بين الأجهزة الإلكترونية والإنسان. (بن مرزوق، 2018)

أما الأمن السيبراني فهو ممارسة الدفاع عن أجهزة الكمبيوتر، والأجهزة المحمولة والأنظمة الإلكترونية، والشبكات، والبيانات، من الهجمات الخبيثة، كما يرد بمعنى أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالإنترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع الهجمات، أو على الأقل الحد من آثارها. (قنديل، 2023) وقد عرفته وزارة الدفاع الأمريكي Pentagon أنه: كافة الإجراءات التنظيمية التي تأمن الحماية الكافية للمعلومات بجميع أنواعها وأشكالها، سواء كانت الكترونية أو مادية، من مختلف المخاطر والهجمات والجرائم، وأفعال التخريب والتحسس والحوادث، بينما أدرج الإعلان الأوروبي، الأمن السيبراني بمعنى: "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات". (الشمري، 2020)

ومن بين من عرف الأمن السيبراني Edward Amors، الذي قدم الأمن السيبراني بأنه: الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، ومنها الوسائل المستخدمة في مواجهة القرصنة وكشف الفيروسات. (Amoroso, 2007) حيث جزم بالجدارة المطلقة لأجهزة الأمن السيبراني في ردع الجريمة المعلوماتية، إلا أن الوسائل المسخرة لحماية المعلوماتية والأمن السيبراني ليس بالضرورة أنها تقوم دائما بردع الجرائم الإلكترونية، وإنما قد تعمل على الحد منها والحماية من وقوعها.

خصوصية البيانات الرقمية:

يعود الفضل في صياغة مفهوم خصوصية المعلومات الإلكترونية أو البيانات الرقمية، كمفهوم مستقل عن باقي مفاهيم الخصوصية إلى المؤلفين الأمريكيين milar و westin alan في مؤلفهما الخصوصية والحرية، وفي كتاب الاعتداء على الخصوصية، ويمكن القول أن مفهومي الخصوصية و الخصوصية المعلوماتية أو الرقمية مترادفان وما يفرقهما هو فقط أن الخصوصية المعلوماتية برزت في ظل ظهور الانترنت وتقنيات الاتصال الحديثة والفضاءات الرقمية، بينما الخصوصية عامة موجودة منذ القدم، انطلاقا من ضبط الحياة والسلوكيات الفردية في إطار الجماعة، وأحقية الآخرين عليه في احترام خصوصياتهم ولا يجوز لأي شخص التعدي عليها بأي شكل من الأشكال. ومن هنا فالخصوصية المعلوماتية (الرقمية) هي حق الفرد في أن يضبط عملية جمع المعلومات الشخصية

عنه، وعملية معاملتها آليا وحفظها وتوزيعها واستخدامها في صنع القرار الخاص بالمؤثر فيه. (أبو حسين، 2021)

الجريمة السيبرانية:

الجريمة السيبرانية بمفهومها التقني؛ تعني الجريمة المعلوماتية تقنيا؛ ذلك النوع من النشاط الإجرامي الذي تستخدم فيه تقنيات الحاسوب الآلي، بطريقة مباشرة أو غير مباشرة، والهدف من ذلك النشاط الإجرامي تنفيذ الفعل الإجرامي المقصود. (نور الهدى، 2023)

بينما يتناولها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بمعنى: "الجرائم التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دورا رئيسيا" (إحليل، 2023)، وقد ركز هذا الطرح على نوع الوسيلة التي ارتكبت بها الجريمة في تحديده لمفهومها.

ومن جهتها، عرفت رابطة كبار ضباط الشرطة الجريمة الالكترونية بأنها: تتضمن في ارتكابها، أو تسهيل ارتكابها، استخدام الكمبيوتر أو الانترنت وشبكات التكنولوجيا، ويبدو أن هذا التعريف قد ركز على وسيلة ارتكاب الجريمة، بينما فصل في أنواع الوسائل التي تدخل ضمن ممارسة الجريمة السيبرانية فقط، ومن جهته يرى المعهد الاستراتيجي لعلم الإجرام، أن الجريمة الالكترونية هي تسمية عامة تطلق على ذلك النوع من الجرائم التي ترتكب باستخدام البيانات الالكترونية، أو أجهزة الاتصالات. (عبد الجواد، 2023) ومن هنا فالجريمة الالكترونية لا تعني الجرائم التي تستهدف البيانات الموجودة على أنظمة الحاسوب فقط، وإنما كل الأنشطة الإجرامية التي يستخدم فيها الحاسوب والانترنت ومختلف التقنيات المتطورة، بما في ذلك أنظمة الذكاء الاصطناعي التي توظف في حروب الجيل الخامس G5.

التحول الرقمي:

ويعني التغيير الثقافي، والتنظيمي، والتشغيلي لمؤسسة، أو صناعة، أو نظام إيكولوجي، من خلال التكامل الذكي للتقنيات، والعمليات، والكفاءات الرقمية عبر جميع المستويات والوظائف بطريقة مرحلية وإستراتيجية. (i-scoop) فهو عملية تحويل المعلومات التناظرية إلى شكل رقمي، باستخدام محول تناظري إلى رقمي، كما هو الحال في الماسح الضوئي للصور أو للتسجيلات الصوتية الرقمية، ومع تزايد استخدام الإنترنت منذ التسعينيات، زاد استخدام الرقمنة أيضاً، ومع ذلك، فإن التحول الرقمي أوسع من مجرد رقمنة العمليات الحالية (الشامسي، 2023). ويستلزم النظر في كيفية تغيير المنتجات والعمليات والمؤسسات، من خلال استخدام التقنيات الرقمية الجديدة. ويعني أيضا الاعتماد الاستراتيجي للتقنيات الرقمية، يتم استخدامه لتحسين العمليات الإنتاجية، وتقديم تجارب أفضل للعملاء والموظفين، وإدارة مخاطر الأعمال، والتحكم في التكاليف. (عيف وخولوفي، 2022)

الذكاء الاصطناعي:

يعرف الذكاء الاصطناعي بأنه: "نظام كومبيوتر له القدرة على تقليد السلوك البشري، والذكاء والأداء والمهام." (توفيق، 2023)، ويرى البعض أن الذكاء الاصطناعي يشير إلى الآلات والأجهزة التي تقوم بمهام تتطلب نوعاً من الذكاء، لفهم العمليات المعرفية، مثل تمثيل المعرفة والتخطيط والتعلم وحل المشكلات والتكيف والتفاعل. من الناحية الرياضية، الذي بدوره سيؤدي إلى تفعيل هذه العمليات في نظام كومبيوتر، كما يمكن أن يشير إلى الأساليب المطلوبة لتحقيق ذلك، أي الخوارزميات والهياكل الحاسوبية. (توفيق، 2023).

ويرد بمعنى بسيط: هو تقليد لسلوكيات الناس بطريقة ذكية، باستخدام الروبوتات، أو الآلات مع نظام مدمج من التفكير، بالطريقة المعرفية نفسها، التي يقوم بها البشر، وأداء مهام مثل حل المشكلات واتخاذ القرارات والتعرف على الكلام والترجمة. وغيرها. (nasrallah, 2021) بحيث تصبح تقنياتها قادرة على التعلم والتعامل مع كميات ضخمة من البيانات، وتحويلها إلى أدوات فعالة، كما يمكنها توقع واتخاذ قرارات بدلاً عن البشر، بعد جمع ومعالجة وتحليل كميات هائلة من البيانات، بسرعة تفوق سرعة البشر بكثير. (بوعبا، 2021) ويمكن الاستدلال على ذلك من خلال؛ التقدم الذي بلغته أنظمة الذكاء الاصطناعي، الذي وصل حد التعلم الآلي (ML) والتعلم العميق (DL)، ويمرزان إلى طريقة تعلم الخوارزميات التي يعمل بها الكومبيوتر لكيفية القيام بالأشياء، مثل تصنيف البيانات والتنبؤ بالقيم، ويتحقق ذلك عن طريق تحليل ومعالجة البيانات الضخمة.

دور دولة الإمارات العربية في مجال الأمن السيبراني والرقمي:

تعد دولة الإمارات العربية المتحدة من الدول التي تبنت خطوات مهمة لتعزيز ممارساتها في مجال الأمن الإلكتروني، منها إقرار "الاستراتيجية الوطنية للأمن السيبراني"، التي تهدف إلى إيجاد بيئة سيبرانية آمنة وصلبة، تساعد على تمكين الأفراد من تحقيق طموحاتهم، وتمكن الشركات من التطور والنمو في بيئة آمنة ومزدهرة. وتدعم معايير الأمن الإلكتروني في الدولة عبر آليات ومحاور مختلفة، وأقرت دولة الإمارات وفعلت قوانين وأنظمة متطورة لمكافحة الجرائم الإلكترونية، منها قانون مكافحة جرائم تقنية المعلومات الجديد لسنة 2021.

وفي هذا السياق جاء إعلان إنشاء مجلس للأمن السيبراني؛ بهدف إعداد سياسات وتشريعات لتعزيز الأمن السيبراني في الدولة، ورفع جاهزية جميع القطاعات للاستجابة للتهديدات السيبرانية. وقد وقع المجلس في مارس 2022 مذكرة تفاهم مع شركة "ديلويت"، إحدى كبريات شركات الخدمات المهنية في العالم؛ لتنظيم أطر التعاون بين الطرفين، وبناء القدرات ليس داخل دولة الإمارات فقط؛ بل في المنطقة والعالم أيضاً؛ ما سيمكن المجلس من الإسهام بفاعلية في الجهود الدولية لمحاربة التهديدات السيبرانية والتصدي لها.

تدخل الدولة لسن تشريعات حماية لتحقيق الأمن الرقمي:

يعد تدخل الدولة في جل الميادين ما هو إلا فرض لسيادتها، ولعل التدخلات التشريعية التي تهم المجال الأمني ما هو إلا لبسط الحماية وفرض تطبيقها من أجل استتبابه ومنه فالتدخل التشريعي لدولة الإمارات العربية المتحدة في الميدان الإلكتروني إنما تسعى من خلاله للحماية من الاختراقات والشائعات والتصدي لها بما يضمن الأمن

الإلكتروني السليم، وقد عملت دولة الإمارات العربية على غرار دول العالم إلى إصدار ترسانة قانونية تنظم هذا الميدان. (رجب، 2022)

1. مضمون قانون مكافحة جرائم تقنية المعلومات الإماراتية

بموجب هذا القانون الصادر لسنة 2016 تتم معاقبة كل من يقوم بالتحايل على العنوان البروتوكولي للشبكة المعلوماتية، أو يقوم باستخدام العنوان الوهمي، أو العناوين العائدة للغير أو بأي الوسائل الأخرى، وذلك بقصد ارتكاب جريمة، أو التحايل لعدم اكتشافها.

كما يعمل هذا القانون على توفير الحماية القانونية والخصوصية لما يتم تداوله أو نشره من بيانات ومعلومات على شبكة المعلومات من خلال العديد من المواد التي يتناولها لتوفير تلك الحماية، كما يتضمن القانون معاقبة كل من قام باستخدام الشبكة المعلوماتية أو إحدى وسائلها في الاعتداء على الخصوصية لشخص إما عن طريق استراق السمع، أو الاعتراض، أو التسجيل، أو البث، أو إفشاء المحادثات أو اتصالات أو المواد صوتية أو المرئية، أو التقاط الصور للغير، أو إعداد صور الكترونية، أو نقلها أو كشفها، أو نسخها أو الاحتفاظ بها، أو نشر أخبار أو صور إلكترونية، أو صور فوتوغرافية أو بيانات أو معلومات ولو كانت صحيحة وحقيقة. (الحميري، 2023)

بالإضافة إلى ذلك فإنه يعاقب القانون كل من قام بابتزاز أو هدد شخص آخر وأجبره على القيام بفعل، أو الامتناع عن فعل شيء، وذلك باستخدام الشبكة المعلوماتية، أو وسيلة تقنية المعلومات. وفي هذا الصدد تم تأسيس مركز الاستجابة لطوارئ الحاسب الألي لتحسين المعايير والممارسات أمن المعلومات، ولحماية البنية التحتية لقطاع الاتصالات وتقنية المعلومات من المخاطر والاختراقات عبر الإنترنت، ويعتبر الهدف من المركز هو تعزيز قانون مكافحة الجرائم التقنية للمعلومات، وكذلك مساعدة استحداث القوانين الجديدة حول أمن المعلومات على مستوى دولة الامارات، وبناء العديد من الخبرات الوطنية والخاصة بمجال أمن المعلومات والعمل على إدارة الطوارئ بالإضافة الى إنشاء مراكز اتصال موثوقة للإبلاغ عن جرائم تقنية المعلومات ومركز وطني لجمع المعلومات عن جرائم تقنية المعلومات (مرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات). (رجب، 2022)

ومما لا شك فيه فقد دأب هذا القانون لتعزيز الأمن الإلكتروني الرقمي للمواطنين والمقيمين داخل دولة الإمارات، من خلال خدمة الدخول الذكي وبطاقات الهوية الصادرة من دولة الإمارات، فبخصوص الخدمة المتعلقة ببطاقات الهوية فقد تم تسجيل جميع سكان دولة الامارات من قبل الهيئة الاتحادية، للهوية والجنسية بالإمارات في مشروع السجل السكاني وبطاقات الهوية، كما تم الاعتماد على البيانات البيومترية للأشخاص، والتي تعتبر من الصفات الفريدة والتي لا يمكن نقلها للآخرين، مثل هندسة كف اليد وبصمة الأصابع وشبكية العين وبعض ملامح وخصائص الوجه.

أما فيما يتعلق خدمة الدخول الذكي (الدبابسة) باعتباره يتيح الوصول إلى الخدمات الإلكترونية كافة، ولجميع الجهات الحكومية في دولة الإمارات، كما تجعل من السهل إجراء جميع المعاملات عبر شبكة الإنترنت باستخدام الحساب الموحد، وكلمات المرور الموحدة، فلا يحتاج المتعامل مع الخدمة إنشاء عدة حسابات مختلفة وكلمات مرور مختلفة للحصول على الخدمات من مختلف الجهات الحكومية، حيث تعمل الخدمة على توفير الكثير من الوقت والجهد فيما يختص بتعريف المتعاملين وتمكنها من التعرف على صاحب المعاملة بالطريقة الذكية للحصول على البيانات الأساسية له بدون الحاجة إلى سؤاله عنها كل مرة، بالإضافة إلى تجنب نسيان المتعامل اسم المستخدم وكلمات المرور لكل موقع إلكتروني حكومي في الدولة.

كما أنه باستطاعة المستخدم الدخول مرة واحدة، باستخدام ملف المستخدم الواحد، وعند استخدام الدخول الذكي يستلزم أولاً للمتعامل بتسجيل الدخول، فيمكن للمقيمين أو المواطنين في دولة الإمارات التسجيل باستخدام بطاقة الهوية الخاصة بهم والصادرة من دولة الإمارات.

2. قانون مكافحة الشائعات والجرائم الإلكترونية:

في ظل وجود الخطر الإرهابي ووجود الجرائم الإرهابية في الكثير من مناطق العالم لا بد من القول بأن هناك البات وجهود حثيثة ومستمرة لمكافحة هذه المخاطر بدولة الإمارات العربية المتحدة وهذا ما يتضح في جميع مراحل التاريخ وعلى كافة المستويات الدولية والوطنية وفي كافة المجالات والإجراءات والتدابير اللازمة بالنسبة لجميع صور الإرهاب ومن هذا المنطلق أيضاً لا بد من التقرير بأن مكافحة الإرهاب بحد ذاتها تواجه كثير من الصعوبات وهذا الأمر بالنسبة للإرهاب التقليدي فكيف يكون الأمر عندما يتعلق الأمر بالفضاء السيبراني حيث الانتشار الواسع على الشبكة وسهولة التخفي وسهولة ارتكاب الجرائم وتدمير آثارها وما إلى ذلك من خصائص تدور حول الجريمة السيبرانية وبالتالي فإن مزيد من الجهود يجب أن تبذل في هذا المجال مع عدم إغفال وانكار دور الوسائل التقليدية في مواجهة تلك التهديدات إذ يمكن القول في أن إطار مكافحة التهديدات السيبرانية من تطبيق ذات الوسائل والإجراءات المستخدمة في علاج الإرهاب الإلكتروني والإرهاب التقليدي في مكافحتهم مع فارق الخصوصية الذي يتمتع بها الفضاء السيبراني، وفي هذا الصدد فالتحديث التشريعي الجديد من خلال صدور مرسوم القانون بشأن مكافحة الشائعات والجرائم الإلكترونية. (الزعابي، 2021)

ويهدف مضمون هذا القانون إلى توفير إطار عمل قانوني شامل لتعزيز حماية المجتمع من الجرائم الإلكترونية المرتكبة من خلال شبكات وتقنيات الإنترنت. كما يسعى إلى حماية المواقع الإلكترونية وقواعد البيانات الحكومية في دولة الإمارات، ومكافحة انتشار الشائعات والأخبار المزيفة، الاحتيال الإلكتروني، والحفاظ على الخصوصية والحقوق الشخصية. (فضل الله، 2020)

إذ يوضح بشكل جلي الجرائم والعقوبات ضد أي شخص قد ينشئ أو يستخدم موقعًا إلكترونيًا أو أي وسيلة تقنية معلومات لاختراق نظم المعلومات والبيانات الحكومية أو مهاجمتها أو العبث بها، أو نشر معلومات كاذبة، أو معلومات تضر بمصالح وأمن دولة الإمارات. يتناول القانون جرائم إلكترونية أخرى تشمل إنشاء أو تعديل روبوتات إلكترونية لنقل بيانات زائفة في الدولة، وتزوير المستندات الإلكترونية، والاعتداء على البيانات والمعلومات الشخصية، والتلاعب بالبيانات الطبية والحسابات المصرفية والأكواد السرية، والتسول الإلكتروني، ونشر بيانات أو معلومات لا تتوافق مع معايير المحتوى الإعلامي، وإتاحة محتوى غير قانوني والامتناع عن إزالته، وإنشاء أو إدارة موقع إلكتروني للاتجار بالبشر، التحريض على الفجور، ونشر مواد، وإباحية والمساس بالآداب العامة، وتحويل أو حيازة أو استخدام أو اكتساب أموال غير مشروعة، والاحتيايل الإلكتروني، والابتزاز والتهديد الإلكتروني، والسب والقذف، وإجراء المسوحات الإحصائية أو الدراسات الاستطلاعية دون ترخيص، والإعلان أو الترويج المضلل للمستهلك، والترويج لمنتجات طبية دون ترخيص، والدعوة والترويج لمظاهرات دون ترخيص، والتحريض على عدم الانقياد للتشريعات، الإساءة لدولة أجنبية، والاتجار والترويج للأسلحة النارية أو الذخائر أو المتفجرات، والإعلان أو الترويج المضلل للمستهلك. (الحافظ، 2023)

جهود دولة الإمارات في تعزيز الأمن السيبراني:

تولي دولة الإمارات العربية المتحدة أهمية كبيرة لتعزيز الأمن السيبراني وحماية البنية التحتية الرقمية للدولة والمؤسسات والمواطنين، بحيث هناك عدة جهود قامت بها الإمارات في هذا المجال وتتجلى في: (العيسوي، 2017) إنشاء هيئة تنظيم الاتصالات بحيث أسست الإمارات هيئة تنظيم الاتصالات (TRA) لتنظيم ومراقبة قطاع الاتصالات وتقنية المعلومات وضمان توافر بيئة آمنة ومأمونة للاتصالات والانترنت، بالإضافة إلى استراتيجية الأمن السيبراني الوطنية بحيث أطلقت الإمارات استراتيجية الأمن السيبراني الوطنية لتحسين أمان البنية التحتية الرقمية وحماية البيانات الحيوية والحيوية للدولة، علاوة على ذلك تطوير القوانين واللوائح بحيث نُشرت قوانين ولوائح جديدة تتعلق بالأمان السيبراني وحماية المعلومات الحساسة، مثل قانون الجرائم الإلكترونية والمعلوماتية وقانون حماية المعلومات الشخصية (عامري، 2021).

كما نجد أيضا التعاون الدولي كون الإمارات شاركت في جهود التعاون الدولي لتبادل المعلومات والممارسات الجيدة في مجال الأمن السيبراني، وكذلك التعاون في مكافحة الجرائم الإلكترونية عبر مختلف المنتديات الدولية، وتحسين التعليم والتدريب بحيث ركزت الإمارات على تطوير المهارات اللازمة لمواجهة التهديدات السيبرانية من خلال توفير التعليم والتدريب المتخصص للموظفين والطلاب والجمهور (الحيدري، 2019).

ومما لا شك أن دولة الإمارات العربية المتحدة تعمل جاهدة وفق منظومتها التشريعية على سن سبل لتعزيز أمنها الإلكتروني بما يواكب مخاطر التحديات العالمية عبر تعزيز كل المباني والبن التحتية لمواجهة هذه الهجمات

1. سبل تعزيز الأمن السيبراني بدولة الإمارات العربية المتحدة

لقد أدت الثورة المعلوماتية لفتح باب لحدوث تغيرات كبيره في الحضارة الانسانية إذ امتدت هذه التغيرات لتشمل مختلف جوانب الحياة الاقتصادية والاجتماعية والسياسية والثقافية، كما ان تميم الحدود المكانية وسيادة الفضاء المفتوح، مع غياب المركزية وعدم وجود مركزية تمسك زمام السلطة داخل كيان الفضاء السيبراني جعل المجتمع أكثر عرضة للتهديدات الرقمية، يضاف الى ذلك وجود ثغرات امن معلوماتي نتيجة لتنامي الخبراء لدى مستخدمين وتقدم التكنولوجيا الرقمية بسرعة كبيرة تساهم بتعميق المخاطر المحتملة أو الهجمات السيبرانية، لذا أضحت عملية الدخول الى المنظمات الرقمية، او مجاميع العمل بحاجة الى تحويل رقمي ، واستخدام كلمات مرور وانشاء جدران نار محكمة للحفاظ على مقومات امن سليمة، لذلك فقد اصبح توفر الامن السيبراني في الإمارات العربية المتحدة ضرورة لحماية الدولة ضد الاعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصالات والمعلومات، خاصة بعد استخدام الجماعات الارهابية للفضاء السيبراني للتجسس وتجنيد الاعضاء مما فرض تحديات جديدة يواجهها الامن الوطني دعت الحاجة الى التنسيق والتعاون بين المؤسسات الامنية من اجل المحافظة على الامن السيبراني. (عبد الرضا والمعموري، 2020)

ومن الوسائل التقنية الإلكترونية لتحقيق الأمن السيبراني ضمان سرية المعلومات ومحتواها وتوافرها عند الحاجة اليها مجموعه من الاليات والوسائل التقنية التي تستخدم للوقاية من خطر التهديدات الإلكترونية او التخفيف من حجم الخسائر والأضرار الناجم في حاله حدوثها وتعدد وسائل الحماية بحسب طبيعتها والغرض من استعمالها اذ يتم ذلك من خلال مجموعه من الوسائل الإجرائية التي يقصد بها تقوية اجهزه التحريات والمعلومات من قبل الأجهزة المعنية والتي تؤدي الى ضبط مرتكبي الجرائم والمساهمة في ردعهم عن ارتكاب الجرائم والمساهمة في الاجهاض المبكر للعمليات الإرهابية وكشف المخططات الإجرامية للإرهابيين والهجوم عليهم وضرهم بالطريقة الاستباقية وذلك بعد جمع المعلومات اللازمة والدقيقة عنهم وعن مخططاتهم لذلك تتخذ الوسائل التقنية الجانب الأهم في مجال تحقيق الأمن السيبراني الإماراتي ومواجهه التهديدات الإلكترونية وذلك مع عدم تقليل شان التدابير غير التقنية وبالتالي فان اللجوء الى هذه التدابير من قبل الأجهزة الأمنية يساعد اجهزه الحاسب الالي على مقاومه الاعتداءات الموجهة اليها او تعطيلها. (الحميري، 2023)

إن وجود مركز يعنى بأمن المعلومات وإدارة الحوادث ومعالجتها والسيطرة على جرائم المعلوماتية أمر مهم جداً وضروري في ظل ما يتعرض له الدول من هجمات إرهابية متمثلة بتنظيمات متطرفة تعتمد اعتماداً رئيساً على تناقل المعلومات والبيانات عبر الشبكات وعبر الفضاء السيبراني، بحيث إن سيطرة الحكومة عبر إنشاء مركز لأمن المعلومات سيقبل من الجرائم الإرهابية بنسبة كبيرة جداً تصل إلى أكثر من 70٪ ويساهم بتقليل نفقات الجهود العسكرية والخسائر البشرية نتيجة المواجهة المباشرة مع القراصنة، وأن هذا المركز. مرتبط بجهة محددة ومستقلة غير خاضعة للضغوطات لغرض ضمان انسيابية العمل، ويكون ذلك من خلال تشريع قانون يتضمن الجوانب التنظيمية والفنية والإدارية والمالية كافة لإنشاء هذا المركز. (الشمري، 2022)

2. تعزيز البنى التحتية الحساسة ضد الهجمات الالكترونية السيبرانية

مع أن آثار هجمات الحرمان من الخدمة قد تبدو ضئيلة نسبياً من الناحية التقنية فإنها قد تكون مدمرة على الصعيد الوطني، ولا يجوز إطلاقاً الاستهانة بالخسائر الاقتصادية المحتملة التي قد يتكبدها البلد خلال أسبوع من الشلل الذي قد يصيبه جراء انقطاع خدمات الإنترنت عنه. وفي البلدان التي تتمتع بأنظمة عسكرية متطورة تعتمد على تقنيات الشبكة، بإمكان هذه الهجمات أن تقلل من جاهزية تلك الأنظمة وفعاليتها، وغالباً ما تقتصر آثار هذه الهجمات على الفضاء الإلكتروني، إلا أنه في ظل تزايد استخدام أنظمة التحكم الصناعي للإنترنت من أجل تشخيص الأنظمة وإعادة ضبطها وتنفيذ الوظائف الإدارية الأخرى، أصبح بإمكان العابثين والأوغاد الإلكترونيين السيطرة والتحكم عن بعد بوظائف أنابيب الغاز ومرافق إنتاج الوقود والمصانع الكيماوية والمحطات الكهربائية، وفي أي من هذه الحالات قد ينتج عن التلاعب بالبرمجيات المتحكممة في هذه الأنظمة ضرر وإرباك حقيقي على مستوى العالم.

وقد أجرى مختبر أيداهو الوطني التابع للحكومة الأمريكية عام 2006 تجربة أظهرت كيفية تدمير مولد في شركة خدمات عن طريق شن هجوم عبر الإنترنت، وقد تم توصيل المولد إلى نظام مخبري بطريقة تحاكي الأسلوب الواقعي المتبع لدى شركات الكهرباء في توصيل الأنظمة، ثم تم الدخول عن بعد إلى نظام المولد وإعطائه أوامر أحدثت فيه فرقة وارتجاجاً ثم انفجر من تلقاء نفسه، والجدير بالذكر أن هذه المولدات تحتاج ستة أشهر لتصنيعها ويتم إنتاجها حسب الحاجة فقط. (الحافظ، 2023)

الخاتمة:

تشكل السلامة السيبرانية والرقمية حماية العالم الرقمي والمعلومات الحساسة والبيانات من التهديدات والهجمات الإلكترونية، بحيث تعد السلامة السيبرانية والرقمية أمراً حيوياً في عصرنا الحالي، حيث أصبحت التكنولوجيا جزءاً أساسياً من حياتنا اليومية ونظم الأعمال والحكومات.

ويتجلى هذا الدور في حماية الأنظمة والشبكات بحيث يتضمن ذلك اتخاذ التدابير اللازمة لحماية الأنظمة الحاسوبية والشبكات الإلكترونية من الاختراق والوصول غير المصرح به واستغلال الثغرات الأمنية، وتأمين البيانات بحيث يتضمن حماية البيانات الحساسة والمعلومات الشخصية من التسرب والوصول غير المصرح به عن طريق تطبيق سياسات الوصول المناسبة واستخدام تقنيات التشفير والحماية، بالإضافة للتصدي للهجمات السيبرانية بحيث يشمل ذلك التحقق من الهجمات السيبرانية ومكافحتها والاستجابة لها بسرعة للحد من الأضرار واستعادة النظام إلى حالته الطبيعية. والتوعية السيبرانية عبر توعية الموظفين والمستخدمين بأهمية الأمان السيبراني وتوجيههم حول الممارسات الآمنة والوقاية من التهديدات السيبرانية.

نتائج الدراسة:

فهم مفهوم الأمن السيبراني: أظهرت الدراسة أن الأمن السيبراني يشمل مجموعة واسعة من التدابير والإجراءات التي تهدف إلى حماية الأنظمة الإلكترونية والمعلومات الحساسة من الهجمات السيبرانية، وهو مفهوم يشمل حماية الأجهزة، والشبكات، والبيانات من التهديدات المختلفة.

دور الإمارات في تعزيز الأمن السيبراني: توصلت الدراسة إلى أن دولة الإمارات العربية المتحدة قد اتخذت خطوات مهمة لتعزيز الأمن السيبراني، بما في ذلك تطوير استراتيجية وطنية للأمن السيبراني، وإنشاء هيئة تنظيم الاتصالات (TRA)، وسن قوانين ولوائح لتعزيز الحماية السيبرانية مثل قانون مكافحة جرائم تقنية المعلومات وقانون حماية المعلومات الشخصية.

تحليل الاستراتيجيات والآليات: أظهرت الدراسة أن الإمارات قد وضعت استراتيجيات واضحة لتعزيز الأمن السيبراني تشمل تحسين البنية التحتية الرقمية، وتطوير التشريعات اللازمة، والتعاون الدولي، وتحسين التعليم والتدريب في مجال الأمن السيبراني.

تقييم الجاهزية الدفاعية الإلكترونية: أظهرت الدراسة أن الإمارات تمتلك جاهزية دفاعية إلكترونية قوية وقادرة على التصدي للتهديدات السيبرانية، مدعومة بجهود منسقة بين مختلف الجهات الحكومية والتعاون مع شركات دولية لتحسين القدرات السيبرانية.

التحديات والفرص: تم تحديد التحديات التي تواجه الإمارات في مجال الأمن السيبراني، بما في ذلك التهديدات المتزايدة والمعقدة والتطور السريع للتكنولوجيا. من ناحية أخرى، توفر التحولات الرقمية والابتكار التكنولوجي فرصاً لتحسين الأمن السيبراني وتعزيز الحماية الإلكترونية.

التشريعات والمبادرات: أظهرت الدراسة أن الإمارات قد أصدرت ترسانة قانونية متقدمة لمكافحة الجرائم الإلكترونية وحماية البيانات الحساسة، وركزت على تطوير مهارات القوى العاملة في مجال الأمن السيبراني من خلال التعليم والتدريب المستمر.

أهمية التوعية السيبرانية: تم التأكيد على أهمية التوعية السيبرانية بين الموظفين والمستخدمين كجزء أساسي من استراتيجية الأمن السيبراني، لتعزيز الممارسات الآمنة والوقاية من التهديدات السيبرانية.

في المجمل، تعزز نتائج هذه الدراسة الفهم الشامل للأمن السيبراني وتسلط الضوء على الجهود المبذولة من قبل دولة الإمارات العربية المتحدة لحماية بنيتها التحتية الرقمية وتعزيز الأمن السيبراني في مواجهة التهديدات المتزايدة.

المراجع:

- عفيف، هناء، و خولوفي، وهيبه. (2022). الاتجاه نحو التحول الرقمي: حتمية أو خيار. مجلة اقتصاديات المال والأعمال، مج6، ع1، 276 - 291.
- الشامسي، مريم. (2023). التحول الرقمي في التعليم: دولة الإمارات العربية المتحدة أنموذجاً. مجلة ريادة الأعمال الإسلامية، مج8، ع1، 11 - 21.
- عبد الرضا، أسعد طارش، والمعموري، علي إبراهيم، (2020)، الأمن السيبراني ودوره في انتشار ظاهرة الارهاب في العراق بعد العام 2003، مجلة دراسات دولية، العدد 80
- سالم، ماجد صدام. (2022). الأمن السيبراني العراقي وأثره في قوة الدولة. مجلة العلوم التربوية والإنسانية، ع18، 69 - 84،
- الشمري، صلاح مهدي هادي، (2020) الأمن السيبراني كمرتكز جديد في الاستراتيجية العرقية. قضايا سياسية، 12 (62)، 273-296.
- بارة، سمير، الأمن السيبراني في الجزائر: السياسات والمؤسسات: المجلة الجزائرية للأمن الإنساني، (2).
- بوعباية، نصيرة، الوافي شهرزاد، (2021)، تحليل البيانات الضخمة باستخدام تقنيات الذكاء الاصطناعي في مهنة التدقيق، مجلة التكامل الاقتصادي 9 (3) (9).
- الحميري، سهيل علي ناصر، (2023)، دور السلامة السيبرانية والأمن الرقمي في دولة الإمارات العربية المتحدة، مجلة الباحث للدراسات القانونية والقضائية، (58)، 517-538.
- مرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات
- العامري، محمد سعيد، (2021)، الأمن السيبراني والتحقيقات الرقمية، مطبعة الاتحاد النشر والتوزيع - أبوظبي.
- الحيدري، زينب، (2019)، الأمن السيبراني - المخاطر. التحديات. المواجهة-، دار الشرق للطباعة النشر والتوزيع.
- عبد الصادق، عادل، (2019)، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية.
- مرسوم القانون الاتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية في 2 يناير 2022.
- قنديل، اشرف عبدالقادر. (2023). آليات تحقيق الأمن المعلوماتي في دولة الإمارات العربية المتحدة. الفكر الشرطي، مج32، ع126، 185 - 229
- المهيدي، عبدالرحمن أحمد. (2023). دور دولة الإمارات العربية المتحدة في تحقيق الأمن الإلكتروني. مجلة قراءات علمية في الأبحاث والدراسات القانونية والإدارية، ع20، 441 - 471.

- الحافظ، محمد باسل، (2023)، قانون مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة، سلسلة دار الحافظ لدولة الإمارات العربية المتحدة.
- نصار، ولاء محمد الطاهر عبد الخالق. (2021). آليات مركز دبي للأمن الإلكتروني للتوعية بالاستراتيجيات الوطنية للأمن السيبراني للحكومات الذكية عبر منصات التواصل الاجتماعي: استجرام نموذجاً. مجلة اتحاد الجامعات العربية لبحوث الإعلام وتكنولوجيا الاتصال، ع6، 46 – 108
- رجب، ياسر محمد عبد السلام. (2022). التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي دراسة مقارنة. المجلة العربية للمعلوماتية وأمن المعلومات، ع6، 115 – 152
- أبو حسين، حنين جميل. (2021). الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمان.
- توفيق، صلاح الدين محمد، (2023)، الذكاء الاصطناعي: مدخل لتعزيز التميز الأكاديمي في الجامعات المصرية: دراسة استشرافية، مجلة العلوم التربوية، مج31، ع1.
- نور الهدى، قادري، (2023)، الجريمة السيبرانية وآليات مكافحتها: مواجهة تحديات الأمن السيبراني، المجلة الجزائرية للحقوق والعلوم السياسية، مج8، ع1.
- الزعاوي، سلطان علي سلطان، (2021)، آليات مكافحة الجريمة الإلكترونية بالإمارات العربية المتحدة، مجلة القانون المغربي، ع46.
- فضل الله، فضل الله محمد الحسن، (2020)، جريمة انتهاك حرمة الحياة الخاصة في التشريع الإماراتي: دراسة تحليلية، مجلة جيل الأبحاث القانونية المعمقة، ع44.
- إحليحل، كريم، (2023)، الجريمة السيبرانية والجهود الدولية في مواجهتها، المجلة الإلكترونية الدولية لنشر الأبحاث القانونية، مج1، ع3.
- عبد الجواد، نجوان أحمد عاصم، (2023)، الجريمة السيبرانية وتأثيرها على الأمن القومي المصري: دراسة سوسيو تحليلية، مجلة كلية الآداب، مج15، ع1.
- nasrallah, N. M, (2021), Using Artificial Intelligence (AI), in Banking Services, introductory Booklet series, (24).