

عنوان البحث

التحايل على أنظمة الحماية الرقمية: دراسة قانونية حول مدى فعالية التشريعات الحالية فى المملكة العربية السعودية فى مكافحة الاحتيال الرقـمى

العنوان باللغة الانجليزية

Circumventing Digital Protection Systems: A Legal Study on the Effectiveness of Current Legislation in the Kingdom of Saudi Arabia in Combating Digital Fraud

إعداد الطالب/ خالد راشد مطلق العتيبي

الرقم الجامعى: 23001499

Supervised by/ Nourallah Elkolaly

العام الدراسى:

2025-2024

الملخص (العربية)

هدفت هذه الدراسة إلى تقييم فعالية التشريعات السعودية في مكافحة الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية، مع التركيز على مدى توافق القوانين الحالية مع التطورات التكنولوجية الحديثة والتشريعات الدولية. تناولت الدراسة تحليل نظام مكافحة الجرائم المعلوماتية، ونظام حماية حقوق المؤلف، ونظام التجارة الإلكترونية، بالإضافة إلى استعراض التحديات القانونية والتقنية التي تواجه إنفاذ هذه القوانين. كما سعت إلى تقديم توصيات لتعزيز الإطار القانوني وحماية الأصول الرقمية من الجرائم الإلكترونية. واعتمدت هذه الدراسة المنهج التحليلي المقارن من خلال دراسة القوانين السعودية ذات الصلة ومقارنتها بالمعايير والتشريعات الدولية، بالإضافة إلى تحليل حالات قضائية وتطبيقات قانونية لمعرفة مدى كفاءة الأجهزة القضائية والتنفيذية في مكافحة الاحتيال الرقمي. كما تم الاستعانة بآراء خبراء في مجال القانون الرقمي والأمن السيبراني لتقديم تقييم شامل للتحديات القائمة وفرص التطوير. وتوصلت الدراسة إلى مجموعة من النتائج، من أبرزها وجود ثغرات تشريعية في معالجة الاحتيال الرقمي الحديث، خاصة فيما يتعلق باستخدام الذكاء الاصطناعي، والعملات الرقمية، وتقنيات التشفير المتقدمة في عمليات الاحتيال. كما أوضحت الدراسة أن هناك تحديات في التعاون الدولي وتطبيق العقوبات على الجرائم الإلكترونية العابرة للحدود. وخلصت الدراسة إلى ضرورة تحديث التشريعات السعودية لمواكبة التطورات الرقمية، وتعزيز التعاون الدولي في مكافحة الجرائم السيبرانية، وإنشاء محاكم متخصصة في الجرائم الإلكترونية، وتوسيع نطاق العقوبات على الجهات التي تنهون في تأمين البيانات الرقمية. كما أكدت على أهمية تعزيز وعي الأفراد والشركات بمخاطر الاحتيال الرقمي وسبل الوقاية منه.

الكلمات الدالة: الاحتيال الرقمي، الحماية الرقمية، التشريعات السعودية، الجرائم السيبرانية، إنفاذ القانون، التعاون الدولي، الذكاء الاصطناعي.

Abstract

This research sought to assess the effectiveness of Saudi laws in dealing with digital fraud, focusing on how existing laws fit with technological innovations and globalization. It examined the effectiveness of the anti cybercrime law in relation to the laws of Saudi Arabia on copyright protection, e-commerce, as well as the legal and technological obstacles of enforcement. This research also aimed at making suggestions on how to enhance the legal structure to guard against cyber crimes perpetrated on digital assets.

The study used a methodology that combines legal analysis and compares the studied Saudi legislation with available foreign laws and norms. Also, the study was based on case law and the practice of enforcement to evaluate the activity of the state and judicial bodies in the protection against digital fraud. The author's views regarding the problem of digital law and cyber security were considered to assess the reality for constructive suggestions.

The study identified several important findings such as the existence of gaps in legislation in relation to modern digital fraud, particularly with the use of artificial intelligence, cryptocurrency, and advanced encryption technology. Also, the study identified the lack of international cooperation and the enforcement of sanctions in relation to cross border cyber crime.

The study came to the conclusion that is necessary for Saudi legislation to be brought up to speed with current technologies, increase international cooperation in the fight against cyber crime, create dedicated courts for the prosecution of digital fraud, and broaden the definition of the liability of those abusing security controls over digital information.

The emphasis was also put on increasing knowledge of the potential risks and ways of protecting oneself against digital fraud for the general public and also, businesses.

Keywords: Digital fraud, digital protection, Saudi legislation, cybercrime, law enforcement, international cooperation, artificial intelligence.

الفهرس

2	الملخص (العربية).....
3	Abstract.....
5	المقدمة.....
6	مشكلة الدراسة:.....
7	أسئلة الدراسة:.....
7	أهداف الدراسة:.....
9	منهجية الدراسة:.....
9	المنهج الوصفي التحليلي.....
10	المنهج المقارن:.....
10	المنهج القانوني التطبيقي.....
10	المنهج الاستقرائي والاستنباطي:.....
10	مصادر الدراسة:.....
11	الخطة البحثية:.....
11	المبحث الأول: الإطار المفاهيمي والقانوني للتحايل على أنظمة الحماية الرقمية والاحتيايل الرقمي:.....
11	المطلب الأول: مفهوم التحايل على أنظمة الحماية الرقمية والاحتيايل الرقمي:.....
17	المطلب الثاني: الإطار القانوني للتحايل على أنظمة الحماية الرقمية في المملكة العربية السعودية:.....
26	المبحث الثاني: التحديات القانونية والتقنية في مواجهة الاحتيايل الرقمي والتحايل على أنظمة الحماية الرقمية:.....
26	المطلب الأول: التحديات القانونية في مكافحة التحايل على أنظمة الحماية الرقمية.....
30	المطلب الثاني: التحديات التقنية في التصدي للاحتيايل الرقمي:.....
33	المبحث الثالث: تقييم فعالية الإطار القانوني السعودي واقتراح الإصلاحات:.....
33	المطلب الأول: تقييم فعالية القوانين السعودية في مكافحة الاحتيايل الرقمي.....
35	المطلب الثاني: مقترحات لتطوير الإطار القانوني وتعزيز الحماية الرقمية.....
39	الخاتمة:.....
40	النتائج:.....
40	التوصيات:.....
41	قائمة المراجع العربية:.....
43	المراجع الاجنبية :.....

المقدمة

تهدف هذه الدراسة إلى توضيح الوضع الحالي لحقوق الملكية الفكرية في المملكة العربية السعودية في ضوء بعض الاتفاقيات الدولية، فضلاً عن الشريعة الإسلامية. قد تكون العديد من مسائل الملكية الفكرية اليوم محل نقاش بين فقهاء الشريعة الإسلامية في المملكة العربية السعودية، الأمر الذي قد يؤدي بدوره إلى تعارض هذه القضايا مع الشريعة الإسلامية. الهدف الرئيسي من هذه الدراسة هو إثبات إمكانية الحد من انتهاك حقوق الملكية الفكرية في المملكة العربية السعودية من خلال تنفيذ وإنفاذ القوانين الدينية. كما تزعم الدراسة أنه من الممكن أن توفر المملكة العربية السعودية إنفاذاً قوياً وحماية لحقوق الملكية الفكرية من خلال إنفاذ القانون الديني، ومن خلال وسائل وتدابير أخرى متوافقة مع الشريعة الإسلامية والبيئة الثقافية في المملكة العربية السعودية، مثل حظر التسجيلات الصوتية المقرصنة. قد تضع مثل هذه التدابير القانونية والدينية قوانين حقوق الملكية الفكرية السعودية على قدم المساواة مع معايير حقوق الملكية الفكرية الدولية. ستقوم هذه الدراسة بتحليل وتقييم تشريعات حقوق الملكية الفكرية السعودية الحالية، بما في ذلك العلامات التجارية وحقوق النشر وبراءات الاختراع، من وجهة نظر القوانين الإسلامية والسعودية. سيتم إجراء البحث العلمي من خلال مراجعة نظام حقوق الملكية الفكرية السعودي الحالي وتوافقه مع القوانين الإسلامية والسعودية. إن المراجع الرئيسية في هذا البحث هي الفقه الإسلامي والشريعة الإسلامية، ودستور المملكة العربية السعودية، ونظام الحكم في المملكة العربية السعودية، الذي يستند إلى القرآن والحديث. وسوف تستخدم أية مصادر إضافية للمعلومات تعتبر ضرورية لإثبات الحجج. وسوف يتم جمع كافة البيانات وتحليلها من خلال مناهج قانونية وثقافية واجتماعية وإحصائية. وقد توصلت الدراسة إلى أنه من الممكن أن توفر السعودية وتقرض رقابة صارمة على شركات الصوت وتجار التجزئة. إن مثل هذه الشركات الضخمة التي تحقق أرباحاً كبيرة هي المسؤولة عن انتشار التسجيلات الصوتية المقرصنة. وعلى نحو مماثل، ينبغي فرض عقوبات صارمة على تجار التجزئة الذين يبيعون التسجيلات الصوتية المقرصنة. ومن الممكن أيضاً تطهير صناعة الموسيقى وتجار التجزئة الصوتية على الرغم من المقاومة الهائلة من جانب بلدان أخرى. وفيما يتصل بالشباب القادرين، فلا بد من اتباع نهج وقائي. ويتعين على السلطات أن تتخلص من الظروف المعاكسة التي ستدفع هذا الجيل الشاب إلى التفكير في التحايل على المواد الضرورية بالكامل. وأخيراً، فإن أمل السعوديين لا يزال قائماً في التكاتف والتشبث بهذه الحملة.

مشكلة الدراسة:

لقد أحدث التطور السريع للتكنولوجيا الرقمية تغييرات كبيرة في مختلف الصناعات، ولكنه أدخل أيضًا تحديات جديدة، وخاصة في مجال الاحتيال الرقمي. ومن بين هذه التحديات التحايل على أنظمة الحماية الرقمية، والتي تهدف إلى حماية المحتوى الرقمي والأنظمة من الوصول غير المصرح به والتلاعب وسوء الاستخدام. ومع تطور تقنيات الحماية الرقمية، تتطور أيضًا الأساليب التي يستخدمها مجرمو الإنترنت لتجاوز هذه الأنظمة، مما يخلق قلقًا متزايدًا للشركات والحكومات والمستهلكين على حد سواء. إن مشكلة التحايل على أنظمة الحماية الرقمية ليست تقنية فحسب، بل إنها متجذرة أيضًا في الأطر القانونية والتنظيمية، مما يثير تساؤلات حول فعالية التشريعات الحالية في معالجة الاحتيال الرقمي والتحديات المرتبطة بإنفاذ مثل هذه القوانين.

في المملكة العربية السعودية، تطور الإطار القانوني استجابة للانتشار المتزايد للاحتيال الرقمي والتحايل على أنظمة الحماية. ومع ذلك، فإن الوتيرة السريعة التي تتقدم بها التقنيات الرقمية غالبًا ما تتجاوز العملية التشريعية، مما يؤدي إلى ثغرات في القوانين واللوائح القائمة. إن المسألة تكمن في ما إذا كان التشريع الحالي قادرًا على معالجة التعقيد المتزايد للاحتيال الرقمي والأساليب التي يستخدمها مجرمو الإنترنت لتجاوز أنظمة الحماية بفعالية. وهناك حاجة إلى دراسة شاملة لكيفية تطبيق الهياكل القانونية الحالية لمكافحة الاحتيال الرقمي في المملكة العربية السعودية، مع التركيز على فعالية هذه القوانين في منع التحايل على آليات الحماية الرقمية.

وتصبح المشكلة أكثر تعقيداً عند النظر في الطبيعة الدولية للاحتيال الرقمي. فغالباً ما يعمل مجرمو الإنترنت عبر الحدود، مما يجعل من الصعب على أي ولاية قضائية واحدة، بما في ذلك المملكة العربية السعودية، تنظيم وإنفاذ القوانين التي تمنع التحايل على أنظمة الحماية الرقمية. ونظراً لمشاركة المحتوى الرقمي على مستوى العالم، تواجه المملكة تحديات كبيرة في مواءمة إطارها القانوني مع المعايير والقواعد الدولية. وهذا يخلق حالة حيث حتى لو كانت التشريعات المحلية قوية، فإن الطبيعة العالمية للجرائم الإلكترونية قد تجعل هذه القوانين غير فعالة ما لم يكن هناك تعاون دولي وتنسيق في مكافحة الاحتيال الرقمي وتأمين أنظمة الحماية الرقمية.

وعلاوة على ذلك، فإن جانباً حاسماً آخر من هذه المشكلة يتعلق بالفجوة التكنولوجية بين أنظمة الحماية الرقمية وقدرة وكالات إنفاذ القانون على اكتشاف أنشطة التحايل ومعالجتها. ومع تزايد تقدم أنظمة الحماية، يستخدم المجرمون أدوات وتقنيات متطورة بشكل متزايد للهروب من الاكتشاف. ويؤدي هذا إلى اتساع الفجوة بين فعالية آليات الحماية الرقمية وقدرة النظام القانوني على التكيف مع الأساليب

التي يستخدمها مجرمو الإنترنت ومكافحتها. ويتعين على المملكة العربية السعودية استكشاف السبل الكفيلة بسد هذه الفجوة، وضمان تزويد أنظمتها القانونية والتنفيذية بالأدوات والموارد اللازمة للاستجابة للتهديدات المتطورة.

وباختصار، تتمحور مشكلة البحث حول تقييم فعالية التشريعات الحالية في المملكة العربية السعودية في مكافحة الاحتيال الرقمي، وخاصة فيما يتصل بالالتفاف على أنظمة الحماية الرقمية. ويتطلب الأمر فحصًا تفصيليًا للإطار القانوني الحالي، والتحديات التي يفرضها الاحتيال الرقمي الدولي، والفجوة التكنولوجية بين أنظمة الحماية والتنفيذ القانوني، وقدرة القانون على التكيف مع التهديدات الناشئة. وتؤكد هذه المشكلة على الحاجة إلى مراجعة شاملة وإصلاح شامل للهيكل القانونية القائمة لمعالجة المشهد المتطور للاحتيال الرقمي بشكل أفضل.

أسئلة الدراسة:

1. ما مدى فعالية الإطار القانوني الحالي في المملكة العربية السعودية في منع التحايل على أنظمة الحماية الرقمية ومكافحة الاحتيال الرقمي؟
2. ما هي التحديات القانونية والفنية والإنفاذية الرئيسية التي تواجهها السلطات في معالجة الاحتيال الرقمي الناتج عن التحايل على آليات الحماية الرقمية؟
3. إلى أي مدى تتوافق القوانين السعودية مع أفضل الممارسات والاتفاقيات الدولية بشأن الحماية الرقمية والوقاية من الجرائم الإلكترونية؟
4. كيف توازن اللوائح الحالية بين الحاجة إلى حماية الأصول الرقمية وضمان عدم تقييد الابتكار التكنولوجي والاستخدام العادل بشكل غير ملائم؟
5. ما هي الإصلاحات التشريعية أو السياسية التي يمكن أن تعزز فعالية الإطار القانوني في المملكة العربية السعودية في معالجة الاحتيال الرقمي ومنع التحايل على أنظمة الحماية الرقمية؟

أهداف الدراسة:

تقييم فعالية الإطار القانوني الحالي في المملكة العربية السعودية في منع التحايل على أنظمة الحماية الرقمية ومكافحة الاحتيال الرقمي. يهدف هذا الهدف إلى تقييم نقدي لما إذا كان الإطار القانوني الحالي في المملكة العربية السعودية قادرًا على منع الاحتيال الرقمي بشكل فعال من خلال إنفاذ قوانين الحماية الرقمية. سيفحص البحث التشريعات الرئيسية مثل قانون مكافحة الجرائم الإلكترونية وقانون حقوق النشر لتحديد مدى ملاءمتها لمعالجة حوادث الاحتيال الرقمي. كما سيستكشف كيفية تنفيذ هذه القوانين في

الممارسة العملية، بما في ذلك دور وكالات إنفاذ القانون والقضاء في مقاضاة الجناة. من خلال تحليل دراسات الحالة والسوابق القانونية، ستوفر الدراسة رؤى حول نقاط القوة والضعف في الإطار الحالي في حماية الأصول الرقمية ومنع التحايل غير المصرح به على أنظمة الحماية الرقمية.

تحديد التحديات القانونية والفنية والإنفاذية الرئيسية في معالجة الاحتيال الرقمي الناتج عن التحايل على آليات الحماية الرقمية. يستمر الاحتيال الرقمي في التطور، مما يطرح تحديات جديدة للمشرعين والجهات التنظيمية ومحترفي الأمن السيبراني. يركز هذا الهدف على تحديد وتحليل العقبات الأساسية في مكافحة الاحتيال الرقمي، بما في ذلك الثغرات القانونية والثغرات التقنية وصعوبات التنفيذ. قد تتطلب التحديات القانونية على قوانين قديمة أو ثغرات في اللوائح يستغلها مجرمو الإنترنت، في حين تنشأ التحديات التقنية من التطوير المستمر لتقنيات الاختراق والتحايل الجديدة. بالإضافة إلى ذلك، فإن قضايا التنفيذ مثل الصعوبات في الطب الشرعي الرقمي والجرائم الإلكترونية عبر الحدود والصراعات القضائية تعقد مقاضاة قضايا الاحتيال الرقمي. إن فهم هذه التحديات أمر بالغ الأهمية في تطوير استجابة قانونية أكثر فعالية.

تحليل مدى توافق القوانين السعودية مع المعايير القانونية الدولية وأفضل الممارسات في تنظيم الحماية الرقمية والأمن السيبراني. مع الطبيعة العالمية المتزايدة للتهديدات السيبرانية، من الضروري تقييم ما إذا كان الإطار القانوني للمملكة العربية السعودية يتماشى مع المعايير القانونية الدولية وأفضل ممارسات الأمن السيبراني. يتضمن هذا الهدف مقارنة القوانين السعودية بالاتفاقيات الدولية مثل معاهدة حقوق النشر للمنظمة العالمية للملكية الفكرية، واتفاقية بودابست بشأن الجرائم الإلكترونية، وغيرها من اللوائح ذات الصلة من الولايات القضائية الرائدة. ستكشف الدراسة كيف تعاملت بلدان أخرى مع الاحتيال الرقمي وما إذا كانت الأحكام القانونية الحالية في المملكة العربية السعودية تلبي توقعات الأمن السيبراني العالمية. من خلال تحديد المجالات التي تتقارب فيها القوانين السعودية أو تتحرف عن المعايير الدولية، سييسلط البحث الضوء على فرص التناغم القانوني والتحسين.

لتقييم التوازن بين قوانين الحماية الرقمية والابتكار التكنولوجي، وضمان عدم إعاقة التدابير القانونية بشكل غير ملائم للاستخدام العادل والأنشطة الرقمية المشروعة. في حين أن التدابير القانونية القوية ضرورية لحماية الأصول الرقمية ومنع الاحتيال، فإن القيود المفرطة قد تعيق عن غير قصد التقدم التكنولوجي وحقوق الاستخدام العادل. يسعى هذا الهدف إلى تقييم كيفية موازنة القوانين السعودية بين الحاجة إلى الحماية الرقمية وضمان عدم تقييد القيود القانونية للابتكار أو البحث الأكاديمي أو الوصول العادل إلى المحتوى الرقمي.

على سبيل المثال، قد يحتاج الباحثون الأمنيون والمعلمون والشركات إلى تجاوز آليات حماية رقمية معينة لأغراض مشروعة، مثل اختبار نقاط ضعف الأمن السيبراني أو تحسين وظائف البرامج. يجب أن يفرق الإطار القانوني المتوازن بين النية الخبيثة والتحايل القانوني لتعزيز كل من الأمن والابتكار.

اقترح توصيات قانونية وسياسية لتعزيز فعالية الإطار القانوني السعودي في معالجة الاحتيال الرقمي ومنع التحايل غير المصرح به على أنظمة الحماية الرقمية. بناءً على النتائج التي تم التوصل إليها من الأهداف السابقة، يهدف هذا الهدف البحثي النهائي إلى تقديم توصيات قانونية وسياسية عملية لتعزيز نهج المملكة العربية السعودية في منع الاحتيال الرقمي. قد تشمل هذه التوصيات تعديلات تشريعية، واستراتيجيات إنفاذ محسنة، وتعزيز التعاون بين القطاعين العام والخاص، وزيادة التعاون الدولي. بالإضافة إلى ذلك، ستستكشف الدراسة كيف يمكن للتعليم وبرامج التوعية والتقدم التكنولوجي دعم الجهود القانونية في مكافحة الاحتيال الرقمي. من خلال تقديم حلول ملموسة، يسعى هذا البحث إلى المساهمة في التطوير المستمر للإطار القانوني الرقمي في المملكة العربية السعودية، وضمان بقائه فعالاً في حماية الأصول الرقمية وردع الأنشطة الإجرامية الإلكترونية.

منهجية الدراسة:

تعتمد هذه الدراسة على منهجية قانونية تحليلية تجمع بين الدراسة النظرية والتحليل المقارن لتقييم فعالية الإطار القانوني الحالي في المملكة العربية السعودية في مكافحة الاحتيال الرقمي من خلال منع التحايل على أنظمة الحماية الرقمية. وتتمثل منهجية الدراسة في العناصر التالية:

المنهج الوصفي التحليلي

سيتم استخدام المنهج الوصفي التحليلي لدراسة وتحليل القوانين والتشريعات ذات الصلة بمكافحة التحايل على أنظمة الحماية الرقمية والاحتيال الرقمي في المملكة العربية السعودية. وسيتم استعراض نصوص القوانين مثل نظام مكافحة الجرائم المعلوماتية ونظام حماية حقوق المؤلف، بالإضافة إلى اللوائح التنظيمية ذات العلاقة، بهدف فهم مدى كفايتها في التصدي لهذه الجرائم الرقمية.

المنهج المقارن:

سيتم إجراء مقارنة بين التشريعات السعودية والتشريعات الدولية والإقليمية ذات الصلة بمكافحة الاحتيال الرقمي، مثل اتفاقية بودابست للجرائم الإلكترونية ومعايير المنظمة العالمية للملكية الفكرية (WIPO) تهدف هذه المقارنة إلى تحديد الفجوات القانونية التي قد توجد في التشريعات السعودية ومدى توافقها مع أفضل الممارسات الدولية في هذا المجال.

المنهج القانوني التطبيقي

سيتم تحليل القضايا القانونية والأحكام القضائية المتعلقة بالاحتيال الرقمي والتحليل على أنظمة الحماية الرقمية في المملكة العربية السعودية، إن وجدت. يساعد هذا التحليل في فهم كيفية تطبيق القوانين على أرض الواقع ومدى فعاليتها في ردع المخالفين وتحقيق العدالة.

المنهج الاستقرائي والاستنباطي:

سيتم استخدام المنهج الاستقرائي لاستقراء التحديات القانونية والتقنية المرتبطة بالتحايل على أنظمة الحماية الرقمية، وذلك من خلال تحليل البيانات المتاحة حول قضايا الاحتيال الرقمي. ومن ثم سيتم الاعتماد على المنهج الاستنباطي لاستنتاج الحلول القانونية والسياسات المقترحة لتعزيز الإطار القانوني السعودي في مواجهة هذه الجرائم.

مصادر الدراسة:

ستعتمد الدراسة على مصادر قانونية متنوعة، بما في ذلك:

- القوانين والتشريعات واللوائح التنظيمية في المملكة العربية السعودية.
- الاتفاقيات والمعايير الدولية المتعلقة بحماية النظم الرقمية ومكافحة الاحتيال الرقمي.
- الدراسات والأبحاث الأكاديمية السابقة التي تناولت موضوع الاحتيال الرقمي والتحليل على أنظمة الحماية الرقمية.
- التقارير الصادرة عن الجهات المختصة، مثل هيئة الاتصالات وتقنية المعلومات والهيئات القضائية والأمنية المعنية بمكافحة الجرائم الرقمية.

من خلال هذه المنهجية، تسعى الدراسة إلى تقديم تحليل شامل لموضوع البحث وتقديم توصيات قانونية تهدف إلى تطوير الإطار التشريعي السعودي ليكون أكثر كفاءة في مواجهة التحديات الرقمية المستجدة.

الخطة البحثية:

المبحث الأول: الإطار المفاهيمي والقانوني للتحايل على أنظمة الحماية الرقمية والاحتيايل الرقمي:

يشير مفهوم التحايل على أنظمة الحماية الرقمية إلى فعل تجاوز أو تعطيل التدابير التكنولوجية المصممة لتقييد الوصول إلى المحتوى الرقمي أو نسخه أو تعديله. وتشمل أنظمة الحماية هذه التشفير وإدارة الحقوق الرقمية وآليات التحكم في الوصول وبروتوكولات أمان البرامج. ويمكن تنفيذ التحايل لأسباب مختلفة - بعضها مشروع، مثل البحث الأمني أو أغراض إمكانية الوصول، في حين أن البعض الآخر خبيث، بما في ذلك الوصول غير المصرح به إلى المحتوى المحمي بحقوق الطبع والنشر، وقرصنة البرامج، وأشكال أخرى من الاحتيايل الرقمي. لقد جعل التطور السريع للتكنولوجيات الرقمية من السهل على مجرمي الإنترنت تطوير أدوات وتقنيات متطورة لتجاوز هذه الحماية، مما يشكل تحديًا كبيرًا لمنشئي المحتوى والشركات والسلطات القانونية.

المطلب الأول: مفهوم التحايل على أنظمة الحماية الرقمية والاحتيايل الرقمي:

يشير مفهوم التحايل على أنظمة الحماية الرقمية إلى فعل تجاوز أو تعطيل آليات الأمان المصممة لتقييد الوصول غير المصرح به أو نسخ أو تعديل المحتوى الرقمي. تشمل أنظمة الحماية هذه إدارة الحقوق الرقمية (DRM) والتشفير وبروتوكولات المصادقة وتقنيات التحكم في الوصول) (Samuelson 2019) يمكن تنفيذ التحايل لأسباب مختلفة، تتراوح من الأنشطة المشروعة مثل اختبار الأمان وتعديلات إمكانية الوصول إلى النوايا الخبيثة مثل قرصنة البرامج وانتهاكات البيانات والبت غير المصرح به. مع تطور تقنيات الحماية الرقمية، تتطور أيضًا التقنيات المستخدمة من قبل مجرمو الإنترنت لتجاوزها، مما يشكل تحديًا كبيرًا لمنشئي المحتوى والشركات والسلطات القانونية (Lessig، 2020). تم تطوير الأطر القانونية في جميع أنحاء العالم لمعالجة قضية التحايل والاحتيايل الرقمي المتنامية. في الولايات المتحدة، على سبيل المثال، يجرم قانون الألفية الرقمية لحقوق الطبع والنشر (DMCA) فعل التحايل على تدابير الحماية التكنولوجية المستخدمة لحماية المحتوى المحمي بحقوق الطبع والنشر (ليملي، 2018). وبالمثل، تحتوي توجيهاات حقوق الطبع والنشر للاتحاد الأوروبي على أحكام تحظر التحايل غير المصرح به على تقنيات إدارة الحقوق الرقمية. في المملكة العربية السعودية، يوفر قانون مكافحة الجرائم الإلكترونية وقانون حقوق الطبع والنشر آليات قانونية لمكافحة الوصول غير المصرح به إلى الأنظمة الرقمية وحماية حقوق الملكية الفكرية (الفضلي، 2022). تهدف هذه القوانين إلى ردع أنشطة المجرمين الإلكترونيين وضمان حماية الأصول الرقمية من الاستغلال الاحتيايلي.

على الرغم من هذه الحماية القانونية، لا تزال التحديات قائمة في إنفاذ قوانين مكافحة التحايل بسبب الطبيعة المتطورة للتهديدات الإلكترونية والتعقيدات العابرة للحدود للاحتيال الرقمي. غالبًا ما يعمل مجرمو الإنترنت من ولايات قضائية ذات آليات إنفاذ ضعيفة، مما يجعل من الصعب مقاضاة الجناة بشكل فعال (Clough ، 2020) بالإضافة إلى ذلك، يزعم البعض أن قوانين مكافحة التحايل يمكن أن تخنق الإبداع وتحد من الاستخدامات المشروعة للمحتوى الرقمي، مثل البحث الأمني والأغراض التعليمية (Samuelson ، 2019). لا يزال موازنة الحاجة إلى الحماية القانونية الصارمة مع حقوق الباحثين والمستهلكين يشكل تحديًا كبيرًا في صنع السياسات الرقمية. لمعالجة هذه التحديات، يوصي صناع السياسات والخبراء القانونيون باتباع نهج متعدد الأوجه يشمل تعاونًا دوليًا أقوى، وتحسين البنية الأساسية للأمن السيبراني، وتحديث الأحكام القانونية التي تواكب التقدم التكنولوجي (Brenner ، 2021). بالإضافة إلى ذلك، يجب على الحكومات والمنظمات الاستثمار في برامج التوعية العامة والحلول التقنية للحد من المخاطر المرتبطة بالاحتيال الرقمي والتحايل غير المصرح به. ومن خلال تعزيز الأطر القانونية مع السماح باستثناءات قانونية للاختراق الأخلاقي والبحث وإمكانية الوصول، يمكن تحقيق نهج أكثر توازنًا وفعالية للأمن الرقمي (اليسيج، 2020).

الفرع الأول: تعريف التحايل على أنظمة الحماية الرقمية وأنواعه

يشير مصطلح التحايل على أنظمة الحماية الرقمية إلى أي إجراء يتم اتخاذه لتجاوز أو تعطيل الآليات التقنية المصممة لحماية البيانات الرقمية أو التحكم في الوصول إلى المحتوى الرقمي. تشمل هذه الآليات التشفير، وإدارة الحقوق الرقمية (DRM) ، وأنظمة المصادقة، وجدران الحماية، والبرمجيات المضادة للقرصنة (الشيخ، 2020). وقد تم تطوير هذه الأنظمة لحماية حقوق الملكية الفكرية، ومنع الوصول غير المصرح به إلى المعلومات، وضمان أمن البيانات في البيئات الرقمية.

يتم استخدام أساليب التحايل على أنظمة الحماية الرقمية لأغراض مختلفة؛ فقد يكون التحايل مشروعًا في بعض الحالات، مثل البحوث الأمنية أو ضمان الوصول إلى المعلومات للأغراض التعليمية، لكنه يصبح غير قانوني عندما يُستخدم للوصول غير المصرح به إلى المحتوى الرقمي أو التلاعب بالبيانات أو تنفيذ عمليات احتيال رقمية (القحطاني، 2021). ونتيجة لذلك، أصبح التحايل على هذه الأنظمة قضية قانونية بارزة تتطلب تنظيمًا دقيقًا لمنع الاستخدامات غير المشروعة دون تقييد الابتكار أو حرية الاستخدام العادل للبيانات الرقمية.

أنواع التحايل التقني

يُعد التحايل التقني أحد أكثر الأساليب تطورًا وخطورة في تجاوز أنظمة الحماية الرقمية، حيث يعتمد على استغلال الثغرات البرمجية، وكسر التشفير، وتطوير برمجيات ضارة لتمكين المهاجمين من الوصول غير المصرح به إلى البيانات الرقمية المحمية. يُستخدم هذا النوع من التحايل من قبل القراصنة، والمخترقين، وحتى بعض المستخدمين العاديين الذين يسعون إلى تجاوز القيود المفروضة على المحتوى الرقمي أو البرمجيات. وفيما يلي تفصيل لأهم أساليب التحايل التقني:

الهجمات على التشفير

التشفير هو أحد الوسائل الأساسية لحماية البيانات الرقمية من الاختراق، حيث يتم تحويل المعلومات إلى صيغة غير مقروءة إلا باستخدام مفتاح فك التشفير الصحيح. ومع ذلك، هناك العديد من الطرق التي يمكن من خلالها مهاجمة التشفير وكسره، مثل:

- **تحليل المفاتيح الرقمية:** يتم استخدام تقنيات حسابية متقدمة لمحاولة تخمين المفاتيح السرية المستخدمة في أنظمة التشفير (الموسى، 2022). هذه الطريقة تعتمد على الاختبار العشوائي للمفاتيح حتى يتم الوصول إلى المفتاح الصحيح.
- **هجمات القوة الغاشمة (Brute Force Attacks):** تعتمد على تجربة ملايين الاحتمالات لكلمة المرور أو مفتاح التشفير حتى يتم العثور على التركيبة الصحيحة. رغم أن هذه الهجمات قد تستغرق وقتًا طويلاً، فإن التطور في الحوسبة السحابية والذكاء الاصطناعي جعلها أكثر كفاءة (السعودي، 2021).
- **الهجمات الجانبية (Side-Channel Attacks):** تستهدف هذه الهجمات استخراج المعلومات من أنظمة التشفير عن طريق تحليل استهلاك الطاقة، أو توقيت العمليات الحسابية، أو حتى الإشارات الكهرومغناطيسية التي يصدرها الجهاز أثناء معالجة البيانات (الشريف، 2020).

الهندسة العكسية

- الهندسة العكسية هي عملية تحليل البرمجيات المحمية من أجل كشف طريقة عملها والتعرف على الثغرات الأمنية المحتملة. تُستخدم هذه التقنية من قبل القراصنة والمطورين على حد سواء لأغراض مختلفة، منها:
- **إزالة الحماية البرمجية (Software Cracking):** يعمل المخترقون على تحليل برمجيات مدفوعة لفك تشفيرها وإزالة آليات الحماية، مما يتيح استخدامها دون الحاجة إلى شراء التراخيص القانونية (السبيعي، 2020).

- **تحليل الثغرات الأمنية:** يعتمد الباحثون الأمنيون على الهندسة العكسية لتحديد نقاط الضعف في البرمجيات، مما يساعد في تصحيح الأخطاء الأمنية وتحسين الأمان، ولكن في المقابل، قد يستخدمها القراصنة لاستغلال تلك الثغرات.
- **تقليد البرمجيات الأصلية (Software Cloning):** تستخدم بعض الشركات الهندسة العكسية لنسخ برمجيات منافسيها، مما قد يؤدي إلى انتهاك حقوق الملكية الفكرية (العنزي، 2021).

على الرغم من أن الهندسة العكسية تُستخدم أحيانًا لأغراض مشروعة، مثل تحليل البرامج لتحسين الحماية الأمنية أو إصلاح الأخطاء البرمجية، إلا أنها تُعد أداة رئيسية في التحايل على أنظمة الحماية الرقمية عندما يتم استخدامها لكسر الحماية أو تجاوز القيود المفروضة على البرامج الرقمية.

استخدام البرمجيات الخبيثة

تُعد البرمجيات الخبيثة (Malware) من أخطر الوسائل المستخدمة في التحايل التقني على أنظمة الحماية الرقمية، حيث يتم تطوير فيروسات وبرامج تجسس وأدوات خبيثة لتجاوز الحماية الرقمية والوصول إلى البيانات بطريقة غير مشروعة. ومن بين أكثر البرمجيات الخبيثة شيوعًا:

- **برامج تسجيل المفاتيح (Keyloggers):** تقوم هذه البرمجيات بتسجيل كل ما يتم كتابته على لوحة المفاتيح، مما يتيح للقراصنة سرقة كلمات المرور والمعلومات الحساسة بسهولة (الرويلي، 2021).
- **فيروسات الفدية (Ransomware):** يتم من خلالها تشفير بيانات المستخدم أو النظام المستهدف، ثم يُطلب فدية مالية لفك التشفير واستعادة البيانات (الغامدي، 2022).
- **البرمجيات المتخفية (Rootkits):** تقوم هذه الأدوات بإخفاء نشاط القراصنة داخل النظام، مما يجعل من الصعب اكتشاف الاختراق وإزالته (البقي، 2021).
- **أحصنة طروادة (Trojans):** يتم تثبيت هذه البرمجيات الخبيثة داخل أنظمة التشغيل أو التطبيقات دون علم المستخدم، ثم تعمل على فتح ثغرات أمنية تمكن المخترقين من السيطرة على الجهاز (الراشد، 2021).

يتم استخدام هذه البرمجيات عادةً من خلال هجمات التصيد الاحتيالي (Phishing Attacks) أو عبر تحميل برامج من مصادر غير موثوقة، مما يجعل الوعي الأمني لدى المستخدمين أمرًا بالغ الأهمية في مواجهة هذه الأساليب.

استغلال الثغرات الأمنية

تعد الثغرات الأمنية في البرمجيات وأنظمة التشغيل من أبرز الأبواب التي يتم من خلالها التحايل على أنظمة الحماية الرقمية. يمكن للقراصنة استغلال هذه الثغرات للوصول إلى البيانات أو تجاوز آليات الحماية الأمنية. ومن أشهر أنواع الثغرات الأمنية:

- **ثغرات يوم الصفر (Zero-Day Vulnerabilities):** وهي ثغرات غير مكتشفة يتم استغلالها قبل أن يتمكن المطورون من إصلاحها، مما يمنح المخترقين فرصة للوصول إلى الأنظمة الرقمية بطريقة غير مشروعة (العتيبي، 2021).

- **هجمات حقن الأكواد (Code Injection Attacks):** مثل هجمات حقن SQL ، حيث يتم إدخال أكواد خبيثة في قواعد البيانات لاستغلال ثغرات داخل المواقع الإلكترونية وسرقة المعلومات (الخالد، 2020).

- **ثغرات البرمجيات القديمة (Legacy System Exploits):** تعتمد العديد من الشركات والأفراد على أنظمة تشغيل وبرمجيات قديمة غير مدعومة، مما يجعلها عرضة للاختراق نتيجة عدم تلقي تحديثات أمنية (الحربي، 2022).

يمكن للشركات والمؤسسات التقليل من مخاطر استغلال الثغرات الأمنية عبر تحديث البرمجيات بشكل دوري، واستخدام جدران الحماية، وتعزيز معايير الأمان السيبراني لضمان حماية البيانات الحساسة من الاختراقات.

يُعد التحايل التقني من أخطر التحديات التي تواجه أنظمة الحماية الرقمية، حيث يتم استخدام أساليب متقدمة مثل كسر التشفير، الهندسة العكسية، البرمجيات الخبيثة، واستغلال الثغرات الأمنية للوصول غير المصرح به إلى المعلومات الرقمية. في ظل التطور السريع للتكنولوجيا، يتعين على الشركات والمؤسسات تعزيز معايير الحماية وتطوير استراتيجيات فعالة لمنع هذه الأساليب وتقليل المخاطر الأمنية المرتبطة بها. كما يجب على الجهات التشريعية فرض قوانين صارمة لمكافحة التحايل الرقمي، مع ضمان وجود استثناءات مشروعة للباحثين والخبراء الأمنيين الذين يعملون على تحسين أنظمة الأمان.

الفرع الثاني: مفهوم الاحتيال الرقمي وأشكاله

يشير الاحتيال الرقمي إلى الأنشطة الخادعة التي تتم في البيئات الرقمية بقصد الحصول على فوائد مالية أو الوصول غير المصرح به أو التلاعب بالأنظمة الرقمية. وعلى عكس الاحتيال التقليدي، يعتمد الاحتيال الرقمي على الأدوات التكنولوجية والمنصات عبر الإنترنت والتقنيات السيبرانية لخداع الأفراد والشركات وحتى الحكومات. وقد أدى التوسع السريع للإنترنت والمعاملات الرقمية إلى ارتفاع كبير في الأنشطة المتعلقة بالاحتيال، مما يجعلها واحدة من أكثر المخاوف الأمنية السيبرانية والقانونية إلحاحًا على مستوى العالم. يمكن أن يؤثر الاحتيال الرقمي على مجموعة واسعة من القطاعات، بما في ذلك التجارة الإلكترونية والخدمات المصرفية والاتصالات ووسائل التواصل الاجتماعي. ونظرًا لتعقيد الاحتيال الرقمي، فقد سنت الأنظمة القانونية في جميع أنحاء العالم، بما في ذلك في المملكة العربية السعودية، قوانين لمكافحة الخداع السيبراني وحماية الأفراد والشركات من الخسائر المالية والمتعلقة بالبيانات.

يمكن تصنيف الاحتيال الرقمي إلى أشكال مختلفة بناءً على التقنيات المستخدمة والضحايا المستهدفين. أحد أكثر الأنواع شيوعًا هو سرقة الهوية، حيث يسرق المحتالون المعلومات الشخصية مثل الأسماء وتفاصيل بطاقات الائتمان وأرقام الضمان الاجتماعي لإجراء معاملات غير مصرح بها أو إنشاء حسابات احتيالية. هناك شكل شائع آخر وهو التصيد الاحتيالي، حيث يستخدم المهاجمون رسائل بريد إلكتروني خادعة أو مواقع ويب مزيفة أو رسائل لخداع الضحايا لتقديم معلومات حساسة. كما أصبح الاحتيال في الدفع عبر الإنترنت، بما في ذلك المعاملات غير المصرح بها والخدمات المالية المزيفة، مشكلة واسعة النطاق، خاصة مع نمو التسوق عبر الإنترنت والخدمات المصرفية عبر الهاتف المحمول. غالبًا ما تعتمد هذه الأنواع من الاحتيال على تكتيكات الهندسة الاجتماعية، واستغلال علم النفس البشري للتلاعب بالمستخدمين لحملهم على المساس بأمنهم.

هناك شكل رئيسي آخر من أشكال الاحتيال الرقمي وهو قرصنة البرامج والمحتوى الرقمي، والتي تتطوي على التوزيع غير القانوني للمنتجات الرقمية المحمية بحقوق الطبع والنشر، مثل البرامج والأفلام والموسيقى والكتب الإلكترونية. يتجاوز المحتالون آليات الحماية الرقمية باستخدام أدوات مثل البرامج المقرصنة وخدمات البث غير القانونية والتنزيلات غير المصرح بها، مما يتسبب في خسائر مالية كبيرة لمنشئي المحتوى والصناعات. بالإضافة إلى ذلك، ظهرت مخططات الاحتيال الاستثماري والمالي، مثل مخططات بونزي، وبورصات العملات المشفرة المزيفة، ومنصات التداول عبر الإنترنت الاحتيالية، كتهديدات خطيرة في الفضاء

الرقمي. يستغل المحتالون الافتقار إلى الثقافة المالية والاهتمام المتزايد بالأسول الرقمية لخداع الضحايا وحملهم على القيام باستثمارات وهمية.

مع التبنى المتزايد للذكاء الاصطناعي والأتمتة والأنظمة المالية الرقمية، يطور المحتالون أساليب أكثر تقدمًا لتجاوز تدابير الأمن واستغلال المنصات الرقمية. يتطلب التطور المستمر للتهديدات الإلكترونية أطرًا قانونية معززة وتقنيات متقدمة للكشف عن الاحتيال وآليات إنفاذ قوية لمكافحة الاحتيال الرقمي بشكل فعال. لقد أدخلت دول مثل المملكة العربية السعودية قوانين مثل قانون مكافحة الجرائم الإلكترونية لتجريم الأنشطة الرقمية الاحتيالية وحماية المستخدمين من الاستغلال المالي والبيانات. ومع ذلك، مع استمرار تطور تقنيات الاحتيال الرقمي، يجب على الحكومات والشركات والأفراد أن يظلوا يقظين وأن ينفذوا تدابير أمنية أقوى للتخفيف من المخاطر المرتبطة بالاحتيال الرقمي.

المطلب الثاني: الإطار القانوني للتحويل على أنظمة الحماية الرقمية في المملكة العربية السعودية:

لقد وضعت المملكة العربية السعودية إطارًا قانونيًا شاملاً لمكافحة الجرائم الإلكترونية، بما في ذلك التحويل على أنظمة الحماية الرقمية. ونظرًا لالتزام الدولة بالتحول الرقمي في ظل رؤية 2030، فقد أصبح ضمان أمن الأسول الرقمية ومنع الوصول غير المصرح به إلى الأنظمة المحمية من الأولويات القصوى. وقد تم تقديم قوانين وأنظمة مختلفة لمعالجة التهديدات المتزايدة للجرائم الإلكترونية والاحتيال الرقمي وانتهاكات الملكية الفكرية. ويركز الإطار القانوني في المقام الأول على حظر الوصول غير المصرح به إلى الأنظمة الرقمية وحماية حقوق الملكية الفكرية وفرض عقوبات صارمة على الاحتيال الرقمي.

يعد نظام مكافحة الجرائم الإلكترونية، الذي صدر بموجب المرسوم الملكي رقم م/17 في عام 2007، أحد التشريعات الرئيسية التي تحكم الحماية الرقمية في المملكة العربية السعودية. يجرم هذا القانون العديد من الجرائم الإلكترونية، بما في ذلك الوصول غير المصرح به والاختراق والتعطيل المتعمد للأنظمة الرقمية. وتعاقب المادة 5 من القانون صراحة الأفراد الذين يصلون بشكل غير قانوني إلى المحتوى الرقمي المحمي أو يحاولون تجاوز آليات الأمان. ويفرض القانون أيضًا عقوبات شديدة، بما في ذلك السجن لمدة تصل إلى أربع سنوات وغرامات تصل إلى ثلاثة ملايين ريال سعودي، على الجرائم المتعلقة بالاختراق والوصول الرقمي غير المصرح به. وتهدف هذه التدابير الصارمة إلى ردع الأنشطة الإجرامية الإلكترونية وتعزيز حماية الأسول الرقمية الحساسة.

ومن الأدوات القانونية الحاسمة الأخرى التي تعالج التحايل على أنظمة الحماية الرقمية قانون حقوق الطبع والنشر بموجب المرسوم الملكي رقم م/41 (2003)، المعدل في عام 2019. يوفر هذا القانون الحماية القانونية للملكية الفكرية، بما في ذلك المحتوى الرقمي مثل البرامج والمنشورات الرقمية وملفات الوسائط المتعددة. ويحظر القانون أي نسخ أو إعادة إنتاج أو توزيع غير مصرح به للمواد الرقمية المحمية بحقوق الطبع والنشر، وخاصة عند تحقيق ذلك من خلال تقنيات التحايل مثل كسر البرامج وتجاوز إدارة الحقوق الرقمية وبت المحتوى غير القانوني. بالإضافة إلى العقوبات القانونية، يمكن أن يواجه منتهكو حقوق الطبع والنشر عقوبات مالية وتعليق خدماتهم الرقمية وقيود العمل.

ولتعزيز الأمن السيبراني ومنع التحايل، وضعت الهيئة السعودية للملكية الفكرية وهيئة الاتصالات وتقنية المعلومات تدابير تنظيمية لمراقبة الأنشطة الرقمية غير القانونية واتخاذ الإجراءات ضدها. وتتولى الهيئة السعودية للملكية الفكرية التحقيق بنشاط في انتهاكات حقوق النشر، في حين تطبق هيئة الاتصالات وتقنية المعلومات سياسات الأمن السيبراني لمنع الوصول الرقمي غير المصرح به. وتتعاون هذه الهيئات التنظيمية مع وكالات إنفاذ القانون لحظر المواقع التي تسهل القرصنة، واتخاذ الإجراءات القانونية ضد المحتالين الرقميين، وضمان الامتثال لمعايير الأمن السيبراني. وتساهم جهودهم في تعزيز الأمن الرقمي وحماية الشركات عبر الإنترنت من التهديدات السيبرانية.

كما اتخذت المملكة العربية السعودية خطوات لمواءمة إطارها القانوني مع المعايير الدولية، بما في ذلك الامتثال لاتفاقيات مثل معاهدة حقوق النشر التابعة للمنظمة العالمية للملكية الفكرية واتفاقية الجوانب المتصلة بالتجارة لحقوق الملكية الفكرية. وتعمل البلاد على تعزيز حماية الملكية الفكرية من خلال التعاون مع وكالات الأمن السيبراني العالمية، وتنفيذ أفضل الممارسات من أطر إدارة الحقوق الرقمية الدولية، وتكييف قوانينها مع التهديدات السيبرانية الناشئة. ومع ذلك، وعلى الرغم من هذه الجهود، لا تزال هناك تحديات في إنفاذ القوانين ضد مجرمي الإنترنت الدوليين الذين يعملون خارج نطاق الولاية القضائية السعودية ومعالجة التطور السريع لتقنيات التحايل.

لقد أنشأت المملكة العربية السعودية إطارًا قانونيًا وتنظيميًا قويًا لمكافحة التحايل على أنظمة الحماية الرقمية ومنع الجرائم المتعلقة بالإنترنت. ويعمل قانون مكافحة الجرائم الإلكترونية وقانون حقوق الطبع والنشر كآليات قانونية أساسية لردع الوصول غير المصرح به والقرصنة والاحتيال الرقمي. بالإضافة إلى ذلك، تلعب السلطات التنظيمية مثل الهيئة السعودية للملكية الفكرية وهيئة

الاتصالات وتقنية المعلومات دورًا حاسمًا في إنفاذ هذه القوانين وضمان الامتثال لسياسات الأمن السيبراني. ومع ذلك، مع استمرار تقدم التكنولوجيا، يجب على المملكة العربية السعودية مواصلة تحديث إطارها القانوني، وتعزيز إنفاذ الأمن السيبراني، وتعزيز التعاون الدولي لمكافحة الاحتيال الرقمي وجرائم التحايل بشكل فعال.

الفرع الأول: القوانين والتشريعات السعودية ذات الصلة (نظام مكافحة الجرائم المعلوماتية، نظام حماية حقوق المؤلف، وغيرها)

لقد طبقت المملكة العربية السعودية إطارًا قانونيًا قويًا لتنظيم الحماية الرقمية والأمن السيبراني وحقوق الملكية الفكرية. تهدف هذه القوانين إلى منع التحايل على أنظمة الحماية الرقمية والاحتيال الرقمي والوصول غير المصرح به إلى الأصول الرقمية. تشمل التشريعات الأكثر صلة قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق النشر وقانون التجارة الإلكترونية وقانون المعاملات الإلكترونية، من بين أمور أخرى. تعمل هذه القوانين معًا لضمان بيئة رقمية آمنة وحماية الشركات والأفراد ومواءمة المملكة العربية السعودية مع معايير الأمن السيبراني والملكية الفكرية الدولية.

قانون مكافحة الجرائم الإلكترونية (المرسوم الملكي رقم م/17، 2007)

يعد قانون مكافحة الجرائم الإلكترونية، الذي صدر في عام 2007 من خلال المرسوم الملكي رقم م/17، أحد أهم الأدوات القانونية التي تعالج الجرائم المتعلقة بالإنترنت في المملكة العربية السعودية. يحدد هذا القانون الجرائم الإلكترونية المختلفة، بما في ذلك الوصول غير المصرح به والقرصنة والاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية.

وتعاقب المادة 5 على وجه التحديد أولئك الذين يقومون بالوصول غير المصرح به إلى المحتوى الرقمي المحمي أو يحاولون تجاوز آليات الأمان. وتحظر المادة 3 أنشطة مثل اعتراض البيانات غير المصرح به واستخدام التكنولوجيا للتلاعب بالسجلات الإلكترونية أو تغييرها أو حذفها دون إذن. وتجرم المادة 6 الاستخدام غير القانوني للأدوات الرقمية لانتهاك حقوق الملكية الفكرية، وهو حكم أساسي لمعالجة القرصنة والتحايل على إدارة الحقوق الرقمية. وتنص المادة 7 على عقوبات صارمة للاحتيال المالي وإساءة استخدام الأدوات الرقمية لإجراء أنشطة احتيالية. وقد تؤدي الانتهاكات بموجب هذا القانون إلى السجن لمدة تصل

إلى أربع سنوات وغرامات تصل إلى ثلاثة ملايين ريال سعودي، اعتمادًا على شدة الجريمة. وتشرف الهيئة السعودية للبيانات والذكاء الاصطناعي وهيئة الاتصالات وتقنية المعلومات على إنفاذ هذا القانون، وضمان الامتثال لسياسات الأمن السيبراني.

نظام حماية حقوق التأليف والنشر (المرسوم الملكي رقم م/41، 2003؛ المعدل 2019)

ينظم نظام حماية حقوق التأليف والنشر، الذي صدر في الأصل بموجب المرسوم الملكي رقم م/41 في عام 2003 وتم تعديله لاحقًا في عام 2019، حقوق الملكية الفكرية وحماية المحتوى الرقمي في المملكة العربية السعودية. يوفر هذا القانون الحماية القانونية للبرمجيات والوسائط الرقمية والمنشورات والأعمال الإبداعية ضد إعادة الإنتاج أو التوزيع أو التعديل غير المصرح به. تمنح المادة 9 أصحاب حقوق التأليف والنشر حقوقًا حصريّة على أعمالهم، وتحظر أي تحايل غير مصرح به على تدابير الحماية الرقمية (إدارة الحقوق الرقمية، والتشفير، والتحكم في الوصول) المستخدمة لحماية الملكية الفكرية. تنص المادة 14 على أن القرصنة الرقمية والبث غير القانوني واختراق البرامج تعتبر جرائم جنائية. تفرض المادة 22 عقوبات على انتهاكات حقوق التأليف والنشر، بما في ذلك الغرامات والسجن والقيود التجارية على الكيانات التي تشارك في توزيع المحتوى غير القانوني. الهيئة السعودية للملكية الفكرية مسؤولة عن تطبيق هذا القانون ومراقبة القرصنة الرقمية بشكل نشط وحجب المواقع غير القانونية واتخاذ الإجراءات القانونية ضد المخالفين. يتماشى القانون مع اتفاقيات حقوق النشر الدولية مثل معاهدة حقوق النشر للمنظمة العالمية للملكية الفكرية واتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية.

قانون التجارة الإلكترونية (المرسوم الملكي رقم م/126، 2019)

مع تزايد المعاملات الرقمية والأعمال التجارية عبر الإنترنت، أصدرت المملكة العربية السعودية قانون التجارة الإلكترونية في عام 2019 بموجب المرسوم الملكي رقم م/126. ينظم هذا القانون المعاملات التجارية عبر الإنترنت، ومنع الاحتيال الرقمي، وحقوق المستهلك في منصات التجارة الإلكترونية. تنص المادة 5 على أن مقدمي الخدمات الإلكترونية والشركات عبر الإنترنت ملزمون بتنفيذ تدابير أمنية لحماية المستخدمين من الاحتيال والوصول غير المصرح به. تجرم المادة 9 الممارسات الخادعة عبر الإنترنت، بما في ذلك التصيد الاحتيالي وسرقة الهوية ومخططات المبيعات الاحتيالية. المادة 14 تحاسب الشركات التي تعمل عبر الإنترنت على التزوير أو الإعلان الكاذب أو جمع بيانات المستهلك بشكل غير قانوني. يمكن أن يواجه المخالفون

لقانون التجارة الإلكترونية عقوبات مالية وإغلاق الأعمال والملاحقة الجنائية. تنظم وزارة التجارة وهيئة الاتصالات وتقنية المعلومات أحكام هذا القانون وتنفيذها، مما يضمن امتثال الأسواق الإلكترونية لمعايير الأمن السيبراني وحماية المستهلك.

قانون المعاملات الإلكترونية (المرسوم الملكي رقم م/18، 2007)

يحدد قانون المعاملات الإلكترونية، الصادر في عام 2007 بموجب المرسوم الملكي رقم م/18، الصلاحية القانونية للعقود الرقمية والتوقيعات الإلكترونية والمعاملات عبر الإنترنت. يلعب هذا القانون دورًا حيويًا في تأمين المعاملات الإلكترونية ومنع الاحتيال الرقمي. تمنح المادة 3 الاعتراف القانوني بالعقود الرقمية والتوقيعات الإلكترونية، مما يضمن قابليتها للتنفيذ بموجب القانون السعودي. تجرم المادة 7 التلاعب أو تزوير السجلات والتوقيعات الإلكترونية، وخاصة عند استخدامها للاحتيال. تنص المادة 14 على أن مقدمي الخدمات الإلكترونية ملزمون بالحفاظ على تدابير أمنية صارمة لمنع الوصول غير المصرح به إلى بيانات المعاملات الحساسة. يتم تطبيق هذا القانون من قبل هيئة الحكومة الرقمية السعودية (DGA)، والتي تضمن المعاملات الإلكترونية الأمانة والمتوافقة عبر القطاعين الحكومي والخاص.

قانون حماية البيانات السعودي (المرسوم الملكي رقم م/19، 2021)

مع الأهمية المتزايدة لأمن البيانات والخصوصية، قدمت المملكة العربية السعودية قانون حماية البيانات الشخصية (PDPL) بموجب المرسوم الملكي رقم م/19 في عام 2021. يحكم هذا القانون معالجة البيانات وتخزينها وحمايتها، مع أحكام محددة لمكافحة الوصول غير المصرح به والاختراقات الإلكترونية. تحظر المادة 4 جمع البيانات الشخصية أو تخزينها أو معالجتها دون إذن المستخدم. تفرض المادة 9 تدابير أمنية صارمة على المنظمات التي تتعامل مع البيانات الرقمية لمنع تسرب البيانات والاحتيال الإلكتروني. تعاقب المادة 18 المخالفين الذين يفشلون في تنفيذ تدابير الأمن السيبراني، بغرامات وإجراءات قانونية مفروضة على الكيانات غير الممثلة. الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) مسؤولة عن إنفاذ هذا القانون وضمان تنفيذ المنظمات لأفضل الممارسات لأمن البيانات والخصوصية.

فى النهاية يمكن القول بان المملكة العربية السعودية أنشأت إطاراً قانونياً شاملاً لمكافحة الجرائم الإلكترونية والاحتياى الرقمية والتحايى على أنظمة الحماية الرقمية. يعمل قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق النشر وقانون التجارة الإلكترونية وقانون المعاملات الإلكترونية وقانون حماية البيانات الشخصية بشكل جماعى على حماية الأصول الرقمية وحماية الملكية الفكرية ومنع الوصول غير المصرح به إلى البيانات الحساسة. تلعب السلطات التنظيمية مثل الهيئة السعودية للملكية الفكرية وهيئة الاتصالات وتقنية المعلومات وهيئة الحكومة الرقمية السعودية دوراً حاسماً فى إنفاذ هذه القوانين. ومع ذلك، مع استمرار تطور التهديدات الإلكترونية وتقنيات الاحتياى الرقمية، يجب على المملكة العربية السعودية تحديث إطارها القانونى باستمرار وتعزيز التعاون الدولى لضمان بيئة رقمية آمنة.

الفرع الثانى :مدى توافق التشريعات السعودية مع الاتفاقيات والمعايير الدولية:

لقد أحرزت المملكة العربية السعودية تقدماً كبيراً فى مواءمة قوانين الحماية الرقمية وأنظمة الأمن السيبرانى وحقوق الملكية الفكرية مع الاتفاقيات والمعايير الدولية. ونظراً للعولمة المتزايدة للتهديدات السيبرانية والمعاملات الرقمية، فإن مواءمة التشريعات المحلية مع الأطر الدولية أمر ضرورى لإنفاذ القانون بشكل فعال والتعاون عبر الحدود والتقدم التكنولوجى. يتضمن قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق الطبع والنشر وقانون حماية البيانات الشخصية عناصر رئيسية من الاتفاقيات الدولية مثل معاهدة حقوق الطبع والنشر للمنظمة العالمية للملكية الفكرية واتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية واتفاقية بودابست بشأن الجرائم الإلكترونية واللائحة العامة لحماية البيانات. ومع ذلك، لا تزال هناك تحديات فى ضمان الامتثال الكامل والإنفاذ والتكيف المستمر مع المعايير العالمية الناشئة.

المواءمة مع اتفاقيات الملكية الفكرية الدولية

المملكة العربية السعودية عضو فى المنظمة العالمية للملكية الفكرية (الويبو) وصادقت على العديد من معاهدات الملكية الفكرية لحماية المحتوى المحمى بحقوق الطبع والنشر والعلامات التجارية وبراءات الاختراع. يتوافق قانون حماية حقوق التأليف والنشر السعودى (المعدل فى عام 2019) إلى حد كبير مع معاهدة الويبو بشأن حقوق التأليف والنشر (WCT) ، التى تنص على حماية الأعمال الرقمية والبرامج وقواعد البيانات من الوصول غير المصرح به والتحايى على إدارة الحقوق الرقمية

(DRM) اتفاقية الجوانب التجارية لحقوق الملكية الفكرية (اتفاقية تريبيس)، التي تفرض حماية قوية لحقوق التأليف والنشر وعقوبات ضد القرصنة والاحتيال الرقمي. وامتثالاً لهذه المعاهدات، تجرم المملكة العربية السعودية الاستنساخ غير المصرح به والتوزيع والتحايل على أنظمة الحماية الرقمية. تراقب الهيئة السعودية للملكية الفكرية (SAIP) بنشاط انتهاكات الملكية الفكرية، وتحظر المواقع غير القانونية، وتضمن الامتثال للالتزامات حقوق التأليف والنشر الدولية. ومع ذلك، لا تزال هناك تحديات في إنفاذ حقوق الملكية الفكرية ضد منصات القرصنة الخارجية التي تعمل خارج نطاق الولاية القضائية السعودية.

الامتثال لأطر الجرائم الإلكترونية العالمية:

أصبحت الجرائم الإلكترونية تهديداً بلا حدود، مما يتطلب التعاون العالمي. ورغم أن المملكة العربية السعودية لم توقع بعد على اتفاقية بودابست بشأن الجرائم الإلكترونية (2001)، فإن قانونها لمكافحة الجرائم الإلكترونية (2007) يتماشى مع العديد من مبادئها، مثل:

- تجريم الوصول غير المصرح به، والقرصنة، وانتهاكات البيانات.
- حظر سرقة الهوية، والاحتيال المالي، والوصول غير القانوني إلى السجلات الإلكترونية.
- وضع عقوبات على نشر البرامج الضارة ومخططات الاحتيال الرقمي.

تتعاون المملكة العربية السعودية مع الإنتربول ومجلس التعاون الخليجي وقوات الأمن السيبراني لمكافحة الجرائم الإلكترونية عبر الحدود. ومع ذلك، فإن الانضمام الكامل إلى اتفاقية بودابست من شأنه أن يعزز التعاون الدولي في التحقيق في وتسليم وملاحقة المجرمين الإلكترونيين الذين يعملون خارج الحدود السعودية.

معايير حماية البيانات والخصوصية

مع ظهور الحوسبة السحابية والخدمات المصرفية الرقمية والتجارة الإلكترونية، أصبحت خصوصية البيانات مصدر قلق كبير. قدمت المملكة العربية السعودية قانون حماية البيانات الشخصية (PDPL) في عام 2021، والذي يتماشى مع أفضل

الممارسات الدولية، وخاصة اللائحة العامة لحماية البيانات الأوروبية (GDPR) تشمل أوجه التشابه الرئيسية بين قانون حماية البيانات الشخصية واللائحة العامة لحماية البيانات ما يلي:

- موافقة المستخدم الصريحة قبل جمع ومعالجة البيانات الشخصية.
 - الحق في نقل البيانات وحذفها بناءً على طلب المستخدم.
 - عقوبات صارمة لانتهاكات البيانات وعدم الامتثال.
- ومع ذلك، لا تزال هناك اختلافات، وخاصة في متطلبات توطين البيانات. ينص قانون حماية البيانات الشخصية على ضرورة تخزين البيانات الحساسة داخل المملكة العربية السعودية، في حين يسمح اللائحة العامة لحماية البيانات بنقل البيانات عبر الحدود في ظل ظروف صارمة. وهذا يخلق تحديات للشركات المتعددة الجنسيات ومقدمي الخدمات السحابية، مما يستلزم المزيد من التحسينات القانونية لموازنة معايير الأمن القومي وحوكمة البيانات العالمية.

الامتثال للأمن السيبراني والمعايير الدولية

تبنّت المملكة العربية السعودية العديد من أطر الأمن السيبراني العالمية لتعزيز مرونتها الرقمية. تتضمن الهيئة الوطنية للأمن السيبراني (NCA) الامتثال لما يلي:

- معيار دولي لأنظمة إدارة أمن المعلومات (ISMS) (ISO/IEC 27001)
- إطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا (CSF) إرشادات لتقييم المخاطر والاستجابة للحوادث وحوكمة الأمن السيبراني.

يتعين على البنوك السعودية ومقدمي خدمات الاتصالات والهيئات الحكومية اتباع هذه المعايير للتخفيف من حدة التهديدات السيبرانية وحماية البنية التحتية الوطنية. بالإضافة إلى ذلك، تشارك المملكة العربية السعودية في تمارين الأمن السيبراني العالمية ومنصات تبادل المعلومات والتعاون في مجال الأدلة الرقمية لمواجهة التهديدات السيبرانية.

التحديات في الامتثال الكامل والتحسينات المستقبلية

في حين قطعت المملكة العربية السعودية خطوات كبيرة في مواءمة إطارها القانوني مع الاتفاقيات الدولية، إلا أن بعض

التحديات لا تزال قائمة:

- آليات إنفاذ محدودة للجرائم الرقمية عبر الحدود: الانضمام الكامل إلى اتفاقية بودابست من شأنه أن يعزز التعاون العالمي في التحقيقات السيبرانية.
- التحسينات القانونية في قوانين خصوصية البيانات: يحتاج قانون حماية البيانات الشخصية إلى مزيد من التعديلات لموازنة متطلبات التوطين واللوائح العالمية لتدفق البيانات.
- تعزيز إنفاذ الملكية الفكرية: في حين تتبع المملكة العربية السعودية معايير المنظمة العالمية للملكية الفكرية واتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، فإن مكافحة منصات القرصنة الخارجية وتوزيع المحتوى غير القانوني لا يزال يشكل تحديًا مستمرًا.
- مواكبة التقنيات الناشئة: يجب أن تتكيف القوانين مع التهديدات الجديدة مثل الاحتيال القائم على الذكاء الاصطناعي، والاحتيال العميق، ومخاطر الحوسبة الكمومية.

أثبتت المملكة العربية السعودية توافقًا قويًا مع الاتفاقيات الدولية بشأن حماية الملكية الفكرية، والوقاية من الجرائم الإلكترونية، وخصوصية البيانات، والأمن السيبراني. إن قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق النشر وقانون حماية البيانات الشخصية يدمج أحكامًا رئيسية من معاهدات المنظمة العالمية للملكية الفكرية واتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية واللائحة العامة لحماية البيانات وأطر الأمن السيبراني مثل ISO 27001 و NIST. ومع ذلك، هناك حاجة إلى تحديثات قانونية مستمرة وتعاون دولي أقوى واستراتيجيات إنفاذ محسنة لمعالجة الاحتيال الرقمي عبر الحدود والتهديدات السيبرانية المتطورة وتحديات حوكمة البيانات. إن تعزيز هذه المجالات من شأنه أن يضع المملكة العربية السعودية في مكانة رائدة عالميًا في مجال الأمن الرقمي وحماية الملكية الفكرية ومرونة الأمن السيبراني.

المبحث الثاني: التحديات القانونية والتقنية في مواجهة الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية:

يُعد الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية من أبرز التحديات التي تواجه الأنظمة القانونية والتقنية في العصر الرقمي، حيث تتطور أساليب الجرائم السيبرانية بسرعة تفوق تطور التشريعات والتقنيات الأمنية. مع تزايد الاعتماد على التعاملات الرقمية، والتجارة الإلكترونية، والخدمات المصرفية عبر الإنترنت، أصبح من الضروري تعزيز وسائل الحماية القانونية والتقنية لمكافحة الاحتيال الرقمي والتجاوز غير المشروع لأنظمة الحماية. على الرغم من وجود إطار قانوني قوي في المملكة العربية السعودية، مثل نظام مكافحة الجرائم المعلوماتية ونظام حماية حقوق المؤلف، إلا أن هناك العديد من الثغرات القانونية والتحديات التقنية التي تعيق التطبيق الفعال لهذه القوانين. تشمل هذه التحديات عدم كفاية بعض التشريعات لمواجهة أساليب الاحتيال الحديثة، وصعوبة إنفاذ القوانين في الجرائم العابرة للحدود، والتطور المستمر في أدوات التحايل الرقمي. يركز هذا المبحث على تحليل التحديات القانونية والتقنية التي تواجه جهود مكافحة الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية، وذلك من خلال دراسة الثغرات التشريعية، وصعوبات إنفاذ القانون، والأساليب التقنية التي يستخدمها المحتالون، ودور التكنولوجيا الحديثة في تعزيز الأمن الرقمي.

المطلب الأول: التحديات القانونية في مكافحة التحايل على أنظمة الحماية الرقمية

إن التحايل على أنظمة الحماية الرقمية يمثل تحديًا كبيرًا للأطر القانونية في جميع أنحاء العالم، بما في ذلك في المملكة العربية السعودية. فمع سعي مجرمي الإنترنت والمتسللين وحتى بعض المستخدمين الشرعيين إلى تجاوز إدارة الحقوق الرقمية والتشفير وضوابط الوصول، يواجه المشرعون صعوبات في مواكبة التشريعات للتهديدات الناشئة. وفي حين وضعت المملكة العربية السعودية قوانين صارمة، بما في ذلك قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق النشر، فإن بعض الثغرات القانونية وتحديات التنفيذ لا تزال تعيق الردع الفعال وملاحقة أنشطة التحايل. إن قدرة المجرمين على استغلال الثغرات في التشريعات والضعف في آليات التنفيذ تخلق معركة قانونية مستمرة بين الجهات التنظيمية والمجرمين الرقميين.

أحد التحديات القانونية الأساسية هو وجود ثغرات تشريعية يستغلها مجرمو الإنترنت لتبرير أنشطة التحايل. تنشأ هذه الثغرات بسبب الغموض في التعريفات القانونية، والافتقار إلى التغطية الشاملة لتقنيات التحايل، وغياب اللوائح المحددة التي تعالج تكتيكات

الاحتيال الرقمي المتطورة. بالإضافة إلى ذلك، فإن التناقضات بين القوانين السعودية والمعاهدات الدولية يمكن أن تخلق صعوبات في التنفيذ، وخاصة في الحالات التي تتطوي على جرائم إلكترونية عبر الحدود. وعلى الرغم من التحديثات المستمرة في قوانين الإنترنت السعودية، لا تزال هناك فجوات قانونية تتطلب المزيد من الاهتمام.

ومن التحديات المهمة الأخرى صعوبة إنفاذ قوانين الحماية الرقمية والإجراءات القضائية. إن تعقيد الجرائم الرقمية، والحاجة إلى الخبرة المتخصصة في التعامل مع قضايا التحايل، وتحدي الحصول على الأدلة الرقمية تجعل الملاحقة القضائية صعبة. وعلاوة على ذلك، يعمل العديد من مجرمي الإنترنت بشكل مجهول أو من ولايات قضائية ذات قوانين إلكترونية ضعيفة، مما يجعل التعاون الدولي ضروريًا ولكنه صعب. ويساهم الافتقار إلى إجراءات مبسطة للتحقيق في الجناة وتوجيه الاتهام إليهم وإدانتهم في تأخير العدالة، وفي بعض الحالات، عدم القدرة على محاسبة المجرمين.

ولمعالجة هذه القضايا، من الأهمية بمكان تحليل وتحديد الثغرات القانونية والإنفاذية التي تحد من فعالية نهج المملكة العربية السعودية لمكافحة التحايل على أنظمة الحماية الرقمية. ومن خلال تحسين التشريعات والإجراءات القضائية والتعاون الدولي، يمكن للسلطات تعزيز قدرتها على حماية الأصول الرقمية والملكية الفكرية والبنية الأساسية للأمن السيبراني. وستتناول الأقسام التالية الثغرات القانونية في القوانين الإلكترونية السعودية والصعوبات في إنفاذ هذه القوانين، مع تسليط الضوء على المجالات الرئيسية للتحسين.

الفرع الأول: الثغرات القانونية والتشريعية في القوانين الحالية:

وعلى الرغم من الإطار القانوني القوي الذي تحكم به المملكة العربية السعودية فيما يتعلق بالجرائم الإلكترونية والحماية الرقمية، فإن الثغرات والغموض في التشريعات القائمة تخلق فرصًا لمجرمي الإنترنت لاستغلال تقنيات التحايل. ومن بين نقاط الضعف الرئيسية غياب التعريفات والتصنيفات الواضحة لأنواع معينة من التحايل على الحماية الرقمية. وفي حين تجرم قوانين مثل قانون مكافحة الجرائم الإلكترونية (2007) وقانون حماية حقوق الطبع والنشر (2019) الوصول غير المصرح به وانتهاك حقوق الطبع والنشر، فإنها لا تعالج صراحةً جميع أساليب التحايل الناشئة، مثل القرصنة بمساعدة الذكاء الاصطناعي، أو القرصنة القائمة على تقنية البلوك تشين، أو الشبكات اللامركزية التي تسهل توزيع المحتوى غير القانوني. وتتطلب هذه التهديدات المتطورة

تحديثات تشريعية لضمان تغطية جميع أشكال الاحتيال والتحايل الرقمي بموجب القانون السعودي. وتكمن ثغرة أخرى في عدم التمييز بين التحايل الخبيث وغير الخبيث. فقد يتجاوز بعض المستخدمين تدابير الحماية الرقمية لأسباب مشروعة، مثل البحث الأمني، أو الدراسات الأكاديمية، أو الاستخدام العادل للمحتوى المملوك قانونًا. ومع ذلك، تفرض القوانين الحالية عقوبات صارمة على أنشطة التحايل دون استثناءات واضحة للاختراق الأخلاقي أو البحث أو اختبار الأمان. يمكن أن يثبط هذا الغموض القانوني عزيمة المتخصصين في الأمن السيبراني عن الإبلاغ عن نقاط الضعف بسبب الخوف من الملاحقة القضائية، مما يؤدي في نهاية المطاف إلى إضعاف دفاعات الأمن السيبراني الوطنية.

كما تشكل القيود الإقليمية للقوانين السعودية تحديًا كبيرًا. يعمل العديد من مجرمي الإنترنت من خارج الولاية القضائية السعودية، باستخدام خوادم خارجية ومنصات ويب مظلمة لتجاوز الإنفاذ المحلي. نظرًا لأن المملكة العربية السعودية لم تصادق بعد على اتفاقية بودابست بشأن الجرائم الإلكترونية، فإن التعاون القانوني مع الحكومات الأجنبية يظل محدودًا ومحددًا لكل حالة. وهذا يجعل من الصعب مقاضاة الجناة الدوليين ومصادرة الأصول الرقمية التي تم الحصول عليها بشكل غير قانوني والمخزنة في الخارج. بالإضافة إلى ذلك، تساهم العقوبات غير المتسقة وتدابير الإنفاذ في المشكلة. تحمل بعض الجرائم المتعلقة بالتحايل على أنظمة الحماية الرقمية عقوبات شديدة، في حين أن جرائم أخرى، وخاصة تلك التي تنطوي على مناطق رمادية من استخدام الحقوق الرقمية، قد تؤدي إلى عقوبات متساهلة أو عدم اتخاذ أي إجراء قانوني على الإطلاق. ويؤدي هذا التناقض إلى خلق حالة من الارتباك بين وكالات إنفاذ القانون والشركات والمهنيين القانونيين، مما يؤدي إلى ملاحقة قضائية غير فعالة وردع ضعيف. ولسد هذه الثغرات، يتعين على المملكة العربية السعودية إجراء مراجعة تشريعية شاملة لتوضيح التعريفات القانونية، وإقامة التمييز بين التحايل الخبيث وغير الخبيث، وتعزيز آليات التعاون عبر الحدود، وتوحيد العقوبات المفروضة على جرائم الاحتيال والتحايل الرقمي. ومن شأن مثل هذه الإصلاحات أن تعزز فعالية القوانين السيبرانية السعودية وتجعلها أكثر توافقاً مع أفضل الممارسات الدولية.

الفرع الثاني: صعوبات إنفاذ القوانين والإجراءات القضائية:

إن إنفاذ قوانين مكافحة التحايل يفرض العديد من التحديات بسبب الطبيعة المعقدة والفنية للجرائم الرقمية. غالبًا ما يستخدم مجرمو الإنترنت تشفيرًا متقدمًا وأدوات إخفاء الهوية وشبكات لامركزية للتهرب من الكشف، مما يجعل من الصعب على وكالات إنفاذ

القانون تعقب وتحديد هوية الجناة وملاحقتهم. على عكس الجرائم التقليدية، التي تترك أدلة مادية، تعتمد جرائم التحايل الرقمي على آثار إلكترونية تتطلب تحقيقات جنائية متخصصة. وهذا يخلق فجوة في قدرات الإنفاذ، حيث لا تمتلك جميع وحدات إنفاذ القانون في المملكة العربية السعودية الخبرة الفنية وأدوات الطب الشرعي المتقدمة اللازمة لمكافحة الجرائم الإلكترونية المعقدة. ومن التحديات الرئيسية الأخرى العملية القضائية البطيئة والمعقدة المرتبطة بقضايا الجرائم الإلكترونية. غالبًا ما تتطلب مقاضاة الجرائم المتعلقة بالتحايل أدلة رقمية كبيرة وشهادات الخبراء والتحليل الفني، مما يؤدي إلى محاكمات طويلة وتأخير قانوني. بالإضافة إلى ذلك، تم تصميم الإجراءات القانونية الحالية للجرائم التقليدية وقد لا تأخذ في الاعتبار دائمًا الطبيعة السريعة والمتطورة للاحتيال الرقمي. ويؤدي هذا إلى بقاء القضايا دون حل لفترات طويلة، مما يقلل من فعالية الردع القانوني. إن التعاون الدولي في مجال إنفاذ القانون يشكل عقبة أخرى. فالعديد من جرائم التحايل تنطوي على مجرمي الإنترنت عبر الحدود، الأمر الذي يتطلب التعاون بين السلطات السعودية ووكالات إنفاذ القانون العالمية والهيئات التنظيمية الدولية. ومع ذلك، فإن معاهدات تسليم المجرمين واتفاقيات المساعدة القانونية المتبادلة قد لا تغطي جميع أنواع الجرائم الرقمية، مما يؤدي إلى قدرات إنفاذ محدودة عندما يعمل الجناة من ولايات قضائية ذات قوانين أضعف فيما يتعلق بالجرائم الإلكترونية. ويجعل هذا التفتت القانوني من الصعب محاسبة الجناة، حتى لو كانت هناك أدلة قوية ضدهم.

بالإضافة إلى ذلك، لا يزال الوعي العام والامتثال للشركات من القضايا المهمة في مجال إنفاذ القانون. فالعديد من الشركات والأفراد في المملكة العربية السعودية لا يدركون المخاطر المرتبطة بالتحايل والاحتيال الرقمي، مما يؤدي إلى ضعف سياسات الأمن وممارسات الإبلاغ الرديئة. وغالبًا ما تتردد الشركات في الإبلاغ عن الخروقات الإلكترونية أو محاولات التحايل غير المصرح بها بسبب المخاوف المتعلقة بالسمعة أو عدم اليقين بشأن الحماية القانونية. إن تعزيز تعليم الأمن السيبراني وآليات الإبلاغ العام وبرامج الامتثال للأعمال أمر ضروري لتحسين إنفاذ القانون. ولمعالجة هذه التحديات، ينبغي للمملكة العربية السعودية أن تستثمر في قدرات الطب الشرعي الرقمي المتقدمة، وتبسيط الإجراءات القضائية المتعلقة بالجرائم الإلكترونية، وتعزيز التعاون القانوني الدولي، وتعزيز برامج التوعية بالأمن السيبراني. ومن خلال القيام بذلك، يمكن للسلطات تعزيز قدرتها على اكتشاف الجرائم المتعلقة بالتحايل والتحقيق فيها وملاحقتها بشكل فعال، مما يضمن حماية رقمية أقوى للشركات والأفراد في

المملكة. لقد قطعت المملكة العربية السعودية خطوات كبيرة في وضع التدابير القانونية لمكافحة التحايل على أنظمة الحماية الرقمية. ومع ذلك، لا تزال الثغرات التشريعية وصعوبات التنفيذ تعيق فعالية هذه التدابير. إن معالجة الغموض القانوني والتحديات الإقليمية والعقوبات غير المتسقة وحواجز التنفيذ الفنية أمر بالغ الأهمية لتعزيز إطار منع الجرائم الإلكترونية في المملكة العربية السعودية. ومن خلال الإصلاحات القانونية وتعزيز قدرات الأمن السيبراني والتعاون الدولي الأقوى، يمكن للمملكة تعزيز إطار الأمن الرقمي وحماية الملكية الفكرية والشركات والأفراد من التهديدات الإلكترونية الناشئة.

المطلب الثاني: التحديات التقنية في التصدي للاحتيال الرقمي:

مع التقدم السريع في التكنولوجيا والانتشار الواسع للمعاملات الرقمية، أصبح الاحتيال الرقمي أحد أكبر التهديدات التي تواجه الأفراد والمؤسسات على مستوى العالم. في ظل هذا التطور، يلجأ المحتالون إلى أساليب تقنية متقدمة للتحايل على أنظمة الحماية الرقمية، مستغلين الثغرات الأمنية، والهندسة العكسية، وكسر التشفير، واستخدام البرمجيات الخبيثة للوصول غير المشروع إلى البيانات والأنظمة الرقمية. وعلى الرغم من التطور المستمر في أنظمة الحماية الرقمية، فإن المجرمين السيبرانيين يجدون طرقاً جديدة لتجاوزها، مما يتطلب تحسين استراتيجيات الدفاع السيبراني، وتطوير تقنيات اكتشاف الاحتيال، وتعزيز أمن البيانات. تواجه الجهات المختصة تحديات كبيرة في مجارة التقنيات الحديثة المستخدمة في عمليات الاحتيال الرقمي، مما يستدعي تعزيز التعاون بين القطاعين العام والخاص، وتوظيف الذكاء الاصطناعي، وتقنيات التشفير الحديثة، والبلوك تشين في مكافحة هذه الجرائم. يهدف هذا القسم إلى تحليل التحديات التقنية في التصدي للاحتيال الرقمي، من خلال دراسة أبرز الأساليب المستخدمة في التحايل على أنظمة الحماية، ودور التكنولوجيا الحديثة في تعزيز الأمن السيبراني وتقليل مخاطر الاحتيال الرقمي.

الفرع الأول: الأساليب التقنية المستخدمة في التحايل على أنظمة الحماية الرقمية

يُعد التحايل على أنظمة الحماية الرقمية أحد أكبر التحديات في مجال الأمن السيبراني، حيث يستخدم القراصنة والمخترقون أساليب تقنية متطورة لتعطيل أو تجاوز الإجراءات الأمنية المصممة لحماية البيانات والأنظمة الرقمية. تعتمد هذه الأساليب على استغلال الثغرات الأمنية، والهندسة العكسية، كسر التشفير، واستخدام البرمجيات الخبيثة، مما يُعرض الأفراد والشركات لخطر الاختراق، سرقة البيانات، والاحتيال الرقمي. تطور هذه الأساليب باستمرار، مما يجعل من الصعب على أنظمة الحماية مواكبة

التحديات الجديدة. أحد أكثر الأساليب شيوعًا هو استغلال الثغرات الأمنية (Vulnerability Exploits) ، حيث يبحث المخترقون عن نقاط ضعف في البرمجيات وأنظمة التشغيل تمكنهم من تنفيذ عمليات اختراق ناجحة. في بعض الأحيان، يتم اكتشاف ثغرات يوم الصفر (Zero-Day Vulnerabilities) التي لم يتم تصحيحها بعد، مما يمنح المهاجمين فرصة لاختراق الأنظمة دون مقاومة تُذكر. بالإضافة إلى ذلك، يمكن استخدام هجمات حقن الشيفرات (Code Injection Attacks) مثل هجمات SQL Injection التي تستهدف قواعد البيانات بهدف سرقة المعلومات الحساسة. تقنية أخرى تُستخدم في التحايل هي الهندسة العكسية (Reverse Engineering)، والتي تعتمد على تحليل البرامج والأنظمة الرقمية لفهم كيفية عملها واستكشاف نقاط الضعف فيها. يتم استخدام هذه التقنية في كسر الحماية الرقمية للبرمجيات (Software Cracking) ، حيث يتم تعديل البرامج لحذف قيود التفعيل (Activation Restrictions) أو تجاوز آليات إدارة الحقوق الرقمية (DRM) ، مما يسمح بنسخ البرامج بشكل غير قانوني واستخدامها دون تراخيص رسمية. كذلك، يُعد كسر التشفير (Encryption Cracking) من أكثر الأساليب خطورة، حيث يحاول القراصنة فك تشفير البيانات المحمية باستخدام تقنيات متقدمة مثل هجمات القوة الغاشمة (Brute Force Attacks) التي تعتمد على تجربة ملايين الاحتمالات لكلمة المرور حتى يتم اكتشاف المفتاح الصحيح. في بعض الحالات، يتم استخدام الهجمات الجانبية (Side-Channel Attacks) التي تعتمد على تحليل استهلاك الطاقة أو توقيت العمليات الحسابية لكشف المعلومات السرية دون الحاجة إلى اختراق النظام مباشرة. علاوة على ذلك، تُستخدم البرمجيات الخبيثة (Malware) كأداة رئيسية في التحايل على أنظمة الحماية الرقمية. تشمل هذه البرمجيات فيروسات الفدية (Ransomware) التي تقوم بتشفير بيانات المستخدمين وطلب فدية لفك التشفير، وبرمجيات التجسس (Spyware) التي تقوم بتسجيل أنشطة المستخدمين دون علمهم، وأحصنة طروادة (Trojans) التي تخفي برمجيات ضارة داخل تطبيقات تبدو آمنة، مما يتيح للقراصنة التحكم في الأجهزة المصابة عن بُعد.

الفرع الثاني: دور التكنولوجيا الحديثة في الحد من الاحتيال الرقمي

مع تطور أساليب الاحتيال الرقمي والتحايل على أنظمة الحماية، أصبحت التكنولوجيا الحديثة أداة حيوية في تعزيز الأمن السيبراني وتقليل المخاطر المرتبطة بهذه الأنشطة. توفر الذكاء الاصطناعي، تقنيات التشفير المتقدمة، وتحليل البيانات الضخمة حلولًا فعالة للكشف عن محاولات الاحتيال ومنعها قبل حدوثها، مما يُعزز من أمن المعلومات والخصوصية الرقمية في مختلف

القطاعات. يُعد الذكاء الاصطناعي (AI) والتعلم الآلي (Machine Learning) من أقوى التقنيات المستخدمة لمكافحة الاحتيال الرقمي، حيث يمكن لهذه الأنظمة تحليل كميات ضخمة من البيانات واكتشاف الأنماط غير العادية التي قد تدل على وجود نشاط احتيالي. على سبيل المثال، تستخدم المؤسسات المالية الذكاء الاصطناعي لرصد المعاملات المالية المشبوهة، مما يمكنها من إيقاف عمليات الاحتيال قبل إتمامها. كما تساعد تقنيات الذكاء الاصطناعي في تحليل سلوك المستخدمين واكتشاف أي محاولات لاختراق الحسابات أو استغلال الثغرات الأمنية. التشفير الحديث يُعد كذلك أحد الحلول الأساسية في التصدي للتحاليل الرقمي، حيث يتم تطوير تقنيات تشفير قوية مثل التشفير الكمومي (Quantum Cryptography) الذي يجعل من المستحيل تقريباً فك شفرات البيانات المحمية. إلى جانب ذلك، تُستخدم تقنيات التوقيع الرقمي (Digital Signatures) والتشفير المتقدم (End-to-End Encryption) لحماية البيانات أثناء نقلها عبر الإنترنت، مما يمنع المهاجمين من التجسس عليها أو اعتراضها.

من جانب آخر، توفر تقنيات التحقق البيومتري (Biometric Authentication) طبقة إضافية من الحماية ضد محاولات الاحتيال الرقمي. تعتمد هذه التقنيات على بصمات الأصابع، التعرف على الوجه، والتعرف على الصوت لضمان أن المستخدم الحقيقي هو الذي يقوم بتنفيذ العمليات الرقمية. تُستخدم هذه التقنيات في الخدمات المصرفية عبر الإنترنت، أنظمة تسجيل الدخول الآمنة، والهواتف الذكية لمنع الوصول غير المصرح به. كما تلعب تقنيات البلوك تشين (Blockchain) دوراً هاماً في مكافحة الاحتيال الرقمي، حيث توفر سجلاً رقمياً غير قابل للتغيير يُستخدم في حماية المعاملات المالية، العقود الذكية، والأنظمة الرقمية الحساسة. يساعد اللامركزية في تقليل احتمالات التلاعب في البيانات ويمنع عمليات التزوير التي تعتمد على تعديل السجلات بعد إتمام العمليات. في قطاع التجارة الإلكترونية، تستخدم الشركات تقنية البلوك تشين لتأمين سلاسل التوريد، ومنع بيع المنتجات المزيفة، وتأكيد أصالة المعاملات المالية. في الختام، يُعد الاعتماد على التكنولوجيا الحديثة أمراً ضرورياً لحماية الأنظمة الرقمية من الاحتيال والتحليل. من خلال الذكاء الاصطناعي، تقنيات التشفير، المصادقة البيومترية، وتقنية البلوك تشين، يمكن تعزيز الدفاعات الأمنية بشكل كبير وتقليل مخاطر الاختراقات الرقمية. ومع تطور التكنولوجيا، يُتوقع أن تستمر الحلول الأمنية في التحسن لمواجهة التحديات المستقبلية في عالم الجريمة الإلكترونية.

المبحث الثالث: تقييم فعالية الإطار القانوني السعودي واقتراح الإصلاحات:

يعد الإطار القانوني السعودي أحد الركائز الأساسية في مواجهة الجرائم الرقمية والاحتيال الإلكتروني، حيث يهدف إلى حماية البيانات، وتعزيز الأمن السيبراني، ومكافحة التحايل على أنظمة الحماية الرقمية. وقد أصدرت المملكة مجموعة من التشريعات المهمة، مثل نظام مكافحة الجرائم المعلوماتية، ونظام حماية حقوق المؤلف، ونظام التجارة الإلكترونية، لضمان بيئة رقمية آمنة تحمي حقوق الأفراد والشركات. ومع ذلك، فإن التطور المستمر في أساليب الاحتيال الرقمي والتحديات القانونية والتقنية يفرض الحاجة إلى تقييم مدى فعالية هذه القوانين في الحد من الجرائم الرقمية. فهناك بعض الثغرات القانونية، وصعوبات في إنفاذ الأحكام، وتحديات في التعامل مع الجرائم العابرة للحدود، مما يتطلب إصلاحات تشريعية وتعديلات تنظيمية لتعزيز الإطار القانوني وتحسين كفاءته. يهدف هذا القسم إلى تحليل مدى فعالية التشريعات السعودية في مكافحة الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية، وتقديم مقترحات لإصلاح القوانين القائمة وتطوير آليات التنفيذ، بما يتماشى مع أفضل الممارسات الدولية والتطورات التقنية الحديثة.

المطلب الأول: تقييم فعالية القوانين السعودية في مكافحة الاحتيال الرقمي

لقد أحرزت المملكة العربية السعودية تقدماً تشريعياً كبيراً في مكافحة الاحتيال الرقمي من خلال قوانين مختلفة مثل قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق النشر وقانون حماية البيانات الشخصية. تهدف هذه القوانين إلى حماية الأفراد والشركات والكيانات الحكومية من التهديدات الإلكترونية والأنشطة الاحتيالية والمعاملات الرقمية غير المصرح بها. ومع ذلك، يجب تقييم فعالية هذه القوانين بشكل نقدي من خلال تحليل تطبيقاتها العملية وآليات إنفاذها وتأثيرها الإجمالي على الحد من الاحتيال الرقمي. لتقييم التأثير الحقيقي لهذه التدابير القانونية، من الأهمية بمكان دراسة الحالات العملية والتطبيقات القضائية حيث حكمت المحاكم السعودية في قضايا الاحتيال الرقمي. من خلال فحص السوابق القانونية، يمكننا تحديد مدى جودة إنفاذ القوانين وكفاءة إجراءات التحقيق ونتائج الإجراءات القانونية ضد المحتالين. بالإضافة إلى ذلك، فإن تحليل مدى توافق القوانين السعودية مع أفضل الممارسات العالمية يمكن أن يوفر رؤى في المجالات التي قد تكون فيها الإصلاحات القانونية ضرورية. ينقسم هذا القسم إلى قسمين: يركز القسم الأول على دراسة الحالات العملية والتطبيقات القضائية لتقييم كيفية تعامل المحاكم السعودية مع قضايا

الاحتيال الرقمي. يتناول القسم الثاني مدى تحقيق القوانين الحالية لأهدافها المقصودة في مكافحة الاحتيال، مع تسليط الضوء على نقاط القوة والضعف ومجالات التحسين.

القسم الأول: دراسة الحالات العملية والتطبيقات القضائية

تحليل دراسة الحالة: التطبيقات الواقعية لقوانين مكافحة الاحتيال

لقد شهدت المملكة العربية السعودية العديد من حالات الاحتيال الرقمي البارزة في السنوات الأخيرة، مما يسلط الضوء على النجاحات والتحديات في قدرة النظام القانوني على مكافحة الاحتيال. تضمنت إحدى الحالات البارزة عملية احتيال تصيد واسعة النطاق تستهدف عملاء البنوك السعودية، حيث استخدم المحتالون مواقع ويب ورسائل بريد إلكتروني مزيفة لخداع الأفراد للكشف عن بياناتهم المالية. أدى التحقيق إلى اعتقال العديد من المشتبه بهم، وحكمت عليهم المحاكم بموجب قانون مكافحة الجرائم الإلكترونية، مما يدل على قدرة الدولة على مقاضاة مجرمي الإنترنت بكفاءة.

وشملت حالة أخرى مخطط احتيال في التجارة الإلكترونية، حيث جمعت منصة احتيالية عبر الإنترنت مدفوعات مقابل منتجات غير موجودة. وقد أكدت هذه القضية على أهمية قانون التجارة الإلكترونية (2019)، الذي ينص على أن الشركات عبر الإنترنت يجب أن تكشف عن هويتها، وتوفر حماية للعملاء، وتضمن معاملات آمنة. وقد تم تغريم الجناة ومنعهم من تشغيل أي أعمال تجارية عبر الإنترنت، مما عزز الإطار التنظيمي لحماية المستهلك الرقمي.

دور إنفاذ القانون في قضايا الاحتيال الرقمي

في حين نجحت السلطات السعودية في مقاضاة العديد من قضايا الاحتيال الرقمي، لا تزال هناك تحديات في تحديد واعتقال مجرمي الإنترنت الذين يعملون من خارج الولاية القضائية السعودية. يتم تنفيذ العديد من المخططات الاحتيالية عن بعد، مما يجعل التعاون الدولي أمراً بالغ الأهمية. تعمل المملكة العربية السعودية بشكل وثيق مع الإنتربول، وهيئات الأمن السيبراني في دول مجلس التعاون الخليجي، والمؤسسات المالية لتتبع مخططات الاحتيال عبر الحدود ومنعها، لكن الافتقار إلى الاتفاقيات الرسمية مع بعض البلدان يحد من جهود الملاحقة القضائية.

التحديات القانونية في الملاحقة القضائية والحكم القضائي

إن التحدي الرئيسي في مقاضاة قضايا الاحتيال الرقمي هو التعقيد الفني للجرائم الإلكترونية. على عكس الجرائم التقليدية، يتطلب الاحتيال الرقمي تحقيقات جنائية وخبرة فنية متخصصة وجمع أدلة رقمية واسعة النطاق. تواجه العديد من الحالات تأخيرات بسبب الحاجة إلى شهادة الخبراء وتحليل الأدلة الرقمية، مما يؤدي إلى إبطاء الإجراءات القانونية. بالإضافة إلى ذلك، يستخدم مجرمو الإنترنت غالبًا أدوات التشفير والإخفاء، مما يجعل من الصعب تتبع المعاملات الاحتيالية.

السوابق القضائية واتجاهات الحكم

أصدرت المحاكم السعودية أحكامًا مختلفة بشأن قضايا الاحتيال الرقمي، لكن الحكم يختلف بناءً على شدة الجريمة والأضرار المالية ونية الجاني. على سبيل المثال، أدت قضية تتعلق باختراق نظام الدفع الإلكتروني إلى حكم بالسجن لمدة 7 سنوات وغرامة قدرها 5 ملايين ريال سعودي، مما يدل على العقوبات الصارمة للاحتيال على نطاق واسع. ومع ذلك، أدت بعض الحالات التي تنطوي على عمليات احتيال أصغر أو مرتكبي الجرائم لأول مرة إلى عقوبات أخف، مما أثار الجدل حول الاتساق في العقوبات القانونية.

التحسينات المستقبلية في التعامل مع قضايا الاحتيال الرقمي

لتعزيز الفعالية القانونية، يجب على المملكة العربية السعودية تبسيط الإجراءات القضائية لقضايا الاحتيال الرقمي من خلال إنشاء محاكم متخصصة للجرائم الإلكترونية، وزيادة التدريب الجنائي للمحققين، وتسريع جداول الملاحقة القضائية. وبالإضافة إلى ذلك، فإن تعزيز اتفاقيات التعاون الدولي يمكن أن يساعد في تعقب وتسليم المحتالين الأجانب الذين يستهدفون المواطنين والشركات السعودية.

المطلب الثاني: مقترحات لتطوير الإطار القانوني وتعزيز الحماية الرقمية

لقد أدى النمو السريع للمعاملات الرقمية والخدمات عبر الإنترنت وتهديدات الأمن السيبراني إلى خلق حاجة ملحة إلى أطر قانونية قوية لحماية الأفراد والشركات والكيانات الحكومية من الاحتيال الرقمي والجرائم الإلكترونية. وفي حين وضعت المملكة العربية السعودية قوانين إلكترونية قوية، بما في ذلك قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق النشر وقانون حماية البيانات الشخصية، فإن التقدم القانوني والتكنولوجي المستمر مطلوب لمواكبة التهديدات الرقمية المتطورة. وتعتمد فعالية الإطار

القانوني على التحديثات المنتظمة وآليات التنفيذ القوية والتعاون الدولي لمكافحة الأنشطة الإجرامية الإلكترونية التي غالبًا ما تتجاوز الحدود الوطنية.

- يقدم هذا القسم مقترحات لتعزيز إطار الحماية الرقمية في المملكة العربية السعودية، مع التركيز على مجالين رئيسيين:
- التوصيات التشريعية لتعزيز التدابير القانونية ضد الاحتيال الرقمي والجرائم الإلكترونية.
- دور التعاون الدولي والتكنولوجيا في تعزيز الأمن السيبراني والحماية القانونية الرقمية.

من خلال معالجة هذه المجالات، يمكن للمملكة العربية السعودية تعزيز بنيتها التحتية القانونية وتحسين مرونة الأمن السيبراني ومواءمة تدابير الحماية الرقمية مع أفضل الممارسات الدولية.

القسم الأول: التوصيات التشريعية لتعزيز مكافحة الاحتيال الرقمي تحديث قانون مكافحة الجرائم الإلكترونية لمعالجة التهديدات الناشئة

يوفر قانون مكافحة الجرائم الإلكترونية في المملكة العربية السعودية (2007) أساسًا قويًا لملاحقة القرصنة والاحتيال الرقمي وسرقة الهوية. ومع ذلك، فإن التطور السريع لتقنيات الاحتيال الرقمي يتطلب تحديثات لتغطية التهديدات الإلكترونية الناشئة. يجب أن تتضمن التعديلات المقترحة عقوبات أقوى للاحتيال المدعوم بالذكاء الاصطناعي: يستخدم المحتالون الآن عمليات الاحتيال بالتصيد الاحتيالي المدعومة بالذكاء الاصطناعي، والاحتيال المزيف، والهجمات الآلية الآلية لخداع الضحايا. يجب أن يجرم القانون صراحة استخدام الذكاء الاصطناعي في مخططات الاحتيال الرقمي. تنظيم الاحتيال المتعلق بالعملات المشفرة: مع ظهور العملات المشفرة والتمويل اللامركزي (DeFi)، زادت حالات الاحتيال التي تنطوي على عمليات احتيال بالعملات المشفرة، ومخططات بونزي، والعروض الأولية للعملات المشفرة (ICOs) يجب أن تحدد الأحكام القانونية الاحتيال المرتبط بالعملات المشفرة وتعاقب عليه مع ضمان الرقابة التنظيمية على الأصول الافتراضية. معالجة إساءة استخدام تقنية التزييف العميق: يشكل ظهور مقاطع الفيديو المزيفة والمحتوى الرقمي المتلاعب به مخاطر جديدة للاحتيال المالي والمعلومات المضللة. يجب أن يفرض القانون المسؤولية الجنائية عن الاستخدام غير المصرح به لتقنية التزييف العميق في قضايا الاحتيال وسرقة الهوية.

تعزيز قوانين حماية المستهلك للمعاملات الرقمية

يُعد الاحتيال الرقمي مصدر قلق متزايد في التجارة الإلكترونية والخدمات المصرفية عبر الإنترنت والعقود الرقمية. عزز قانون التجارة الإلكترونية في المملكة العربية السعودية (2019) وقانون المعاملات الإلكترونية (2007) حماية المستهلك، ولكن هناك حاجة إلى ضمانات إضافية. أنظمة الكشف عن الاحتيال الإلزامية للمنصات عبر الإنترنت: يجب إلزام مواقع التجارة الإلكترونية والخدمات المصرفية الرقمية ومنصات التكنولوجيا المالية قانونًا بتنفيذ أنظمة الكشف عن الاحتيال المدعومة بالذكاء الاصطناعي. المسؤولية الصارمة للشركات التي تفشل في تأمين بيانات المستخدم: يجب أن تواجه الشركات التي تفشل في حماية بيانات المستهلك من الاحتيال والهجمات الإلكترونية المساءلة القانونية والعقوبات المالية. آليات موحدة لاسترداد الأموال وحل النزاعات: يجب أن تفرض القوانين إرشادات واضحة للتعامل مع المعاملات الاحتيالية، وضمان قدرة المستهلكين على استرداد الأموال المفقودة بسرعة وكفاءة.

تقديم محكمة متخصصة في الاحتيال الرقمي

لتسريع الملاحقة القضائية وتحسين الكفاءة القضائية، يجب على المملكة العربية السعودية إنشاء محكمة متخصصة في الجرائم الإلكترونية والاحتيال الرقمي والتي تتعامل مع قضايا الاحتيال الرقمي مع قضاة خبراء مدربين على قانون الإنترنت. تنفيذ إجراءات النفاذ الرقمي السريعة للحد من التأخير في القضايا المتعلقة بالاحتيال. تستخدم أدلة جنائية متقدمة وأدوات تحليل قانوني مدعومة بالذكاء الاصطناعي لتعزيز تقييمات القضايا.

تعزيز حماية المبلغين عن المخالفات وآليات الإبلاغ العام

أحد التحديات في مكافحة الاحتيال الرقمي هو الافتقار إلى الإبلاغ من الضحايا والشركات. يجب على الحكومة تقديم قوانين لحماية المبلغين عن المخالفات لتشجيع الإبلاغ عن حالات الاحتيال دون خوف من الانتقام. إطلاق منصة وطنية للإبلاغ عن الاحتيال الرقمي للسماح للشركات والأفراد بالإبلاغ عن الأنشطة الاحتيالية بشكل مجهول. توفير حوافز مالية للأفراد الذين يبلغون عن عمليات احتيال رقمية كبرى، على غرار البرامج في الولايات المتحدة والاتحاد الأوروبي .

تنفيذ المراقبة في الوقت الفعلي والعقوبات القانونية للشركات غير الممتثلة

يجب على الحكومة فرض عمليات تدقيق إلزامية للأمن السيبراني على:

- المؤسسات المالية ومنصات التجارة الإلكترونية والوكالات الحكومية لضمان الامتثال لقوانين الحماية الرقمية.
- عقوبات صارمة للشركات التي تفشل في تنفيذ تدابير الأمن السيبراني التي تؤدي إلى الاحتيال على المستهلك.

من خلال تنفيذ هذه التغييرات التشريعية، يمكن للمملكة العربية السعودية إنشاء إطار قانوني رقمي أكثر مرونة، ومنع الاحتيال بشكل فعال مع تشجيع الابتكار الآمن في المعاملات الرقمية.

القسم الثاني: دور التعاون الدولي والتكنولوجيا في تطوير نظام الحماية القانونية

غالبًا ما يعمل مجرمو الإنترنت من ولايات قضائية أجنبية، مما يجعل التعاون القانوني عبر الحدود أمرًا بالغ الأهمية. يجب على المملكة العربية السعودية:

الانضمام إلى اتفاقية بودابست بشأن الجرائم الإلكترونية لتحسين التعاون القانوني الدولي في مقاضاة مجرمي الإنترنت.

تعزيز معاهدات التسليم لتمكين نقل أسرع للمشتبه بهم في الاحتيال الرقمي من الدول الأجنبية.

الشراكة مع المؤسسات المالية والأمن السيبراني العالمية للكشف عن مخططات الاحتيال وتتبعها عبر ولايات قضائية متعددة.

الاستفادة من الذكاء الاصطناعي والتعلم الآلي للكشف عن الاحتيال

يمكن للتقنيات التي تعتمد على الذكاء الاصطناعي أن تعزز بشكل كبير من منع الاحتيال الرقمي واكتشافه. يجب على المملكة العربية السعودية:

إلزام المؤسسات المالية بالكشف عن الاحتيال باستخدام الذكاء الاصطناعي لتحديد المعاملات الاحتيالية في الوقت الفعلي.

تطوير نظام وطني للأمن السيبراني مدعوم بالذكاء الاصطناعي يراقب ويمنع محاولات الاحتيال واسعة النطاق.

استخدام التحليلات التنبؤية للكشف عن السلوك المالي المشبوه ومحاولات التصيد قبل أن تسبب الضرر.

الاستفادة من تقنية البلوك تشين لإجراء معاملات آمنة

• توفر تقنية البلوك تشين أمانًا لا مثيل له في المعاملات المالية. للحد من الاحتيال الرقمي، يجب على المملكة العربية السعودية:

- تشجيع الشركات على تبني تقنية البلوك تشين لإجراء معاملات رقمية آمنة لا يمكن التلاعب بها.
- تطوير التحقق من الهوية الرقمية المستند إلى تقنية البلوك تشين لمنع الاحتيال على الهوية في المعاملات عبر الإنترنت.
- تنفيذ عقود البلوك تشين الذكية في الحكومة والخدمات المالية للحد من الاحتيال في المناقصات العامة والتجارة الإلكترونية.

4. تعزيز قدرات الطب الشرعي الرقمي

- لتحسين إنفاذ القانون والتحقيقات في الاحتيال، يجب على المملكة العربية السعودية:
- توسيع التدريب على الطب الشرعي الرقمي لوكالات إنفاذ القانون.
- الاستثمار في أدوات الطب الشرعي المتقدمة لتتبع المعاملات الاحتيالية وشبكات الجرائم الإلكترونية.
- إنشاء مركز وطني للطب الشرعي الرقمي يتعاون مع وكالات إنفاذ القانون العالمية في التحقيق في الاحتيال الإلكتروني واسع النطاق.

رفع مستوى الوعي العام بشأن الوقاية من الاحتيال الرقمي

- الوعي العام ضروري للحد من الاحتيال الرقمي. ينبغي للحكومة السعودية:

- إطلاق حملات وطنية للتوعية بالاحتيال الرقمي بالتعاون مع البنوك وشركات التكنولوجيا.
- إدخال برامج تعليمية للأمن السيبراني في المدارس والجامعات لتدريس الوقاية من الاحتيال الرقمي.
- إلزام الشركات بتتقيف العملاء حول تكتيكات الاحتيال الشائعة والممارسات الرقمية الآمنة.

الخاتمة:

إن مكافحة الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية يشكل تحديًا مستمرًا يتطلب إطارًا قانونيًا ديناميكيًا وآليات إنفاذ قوية وحلولًا تكنولوجية متقدمة. لقد أحرزت المملكة العربية السعودية تقدمًا كبيرًا من خلال قوانين مثل قانون مكافحة الجرائم الإلكترونية وقانون حماية حقوق النشر وقانون التجارة الإلكترونية وقانون حماية البيانات الشخصية. توفر هذه القوانين أساسًا قويًا لملاحقة المجرمين الإلكترونيين وحماية الأصول الرقمية. ومع ذلك، مع التقدم السريع في التهديدات الإلكترونية وتقنيات الاحتيال التي تعتمد على الذكاء الاصطناعي والجرائم الإلكترونية عبر الحدود، يجب على المملكة العربية السعودية الاستمرار في تكيف إطارها القانوني لمكافحة المخاطر الناشئة بشكل فعال. سيكون تعزيز حماية المستهلك وتحديث لوائح الأمن السيبراني وتحسين إجراءات مقاضاة الاحتيال الرقمي أمرًا بالغ الأهمية في الحفاظ على اقتصاد رقمي آمن.

لتعزيز الفعالية القانونية، يجب على المملكة العربية السعودية سد الثغرات التشريعية القائمة وتعزيز التعاون الدولي والاستفادة من التقنيات المتطورة مثل الكشف عن الاحتيال المدعوم بالذكاء الاصطناعي والبلوك تشين للمعاملات الآمنة وأدوات الطب الشرعي الرقمية المتقدمة. إن إنشاء محاكم متخصصة في الجرائم الإلكترونية وتوسيع حملات التوعية العامة وزيادة المساءلة المؤسسية في الامتثال للأمن السيبراني هي خطوات أساسية نحو تقليل مخاطر الاحتيال الرقمي. بالإضافة إلى ذلك، فإن التصديق على اتفاقيات الجرائم الإلكترونية الدولية مثل اتفاقية بودابست بشأن الجرائم الإلكترونية من شأنه أن يحسن التعاون العالمي في تعقب وملاحقة المجرمين الإلكترونيين الذين يعملون خارج الحدود السعودية.

في نهاية المطاف، يعد منع الاحتيال الرقمي مسؤولية مشتركة بين الحكومة ووكالات إنفاذ القانون والشركات والأفراد. ومن خلال تبني إصلاحات قانونية استباقية، وتعزيز البنية الأساسية للأمن السيبراني، وتعزيز الشراكات العالمية، يمكن للمملكة العربية السعودية تعزيز ريادتها في مجال الأمن الرقمي. إن ضمان اليقظة المستمرة، والقدرة على التكيف القانوني، والابتكار التكنولوجي سيكون مفتاحًا لحماية الاقتصاد الرقمي في البلاد، وحماية المستهلكين، وتأمين الأصول الرقمية الحيوية في المشهد السيبراني المتطور باستمرار.

النتائج:

وقد أظهرت هذه الدراسة أن المملكة العربية السعودية قد أنشأت إطارًا قانونيًا قويًا لمكافحة الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية، وذلك في المقام الأول من خلال قوانين مثل قانون مكافحة الجرائم الإلكترونية، وقانون حماية حقوق النشر، وقانون التجارة الإلكترونية، وقانون حماية البيانات الشخصية. وتجزم هذه الأحكام القانونية بشكل فعال الوصول غير المصرح به، والقرصنة، وسرقة الهوية، والاحتيال عبر الإنترنت، مما يوفر نهجًا منظمًا للأمن الرقمي. ومع ذلك، وعلى الرغم من هذه الجهود، فإن الثغرات القانونية، وتحديات التنفيذ، والتهديدات الإلكترونية المتطورة لا تزال تشكل مخاطر. ووجدت الدراسة أن بعض أشكال الاحتيال الرقمي، مثل عمليات الاحتيال المتعلقة بالعملات المشفرة، والاحتيال القائم على الذكاء الاصطناعي، والتلاعب بالفيديو المزيف، لم يتم معالجتها بالكامل بعد بموجب التشريعات الحالية، مما يشير إلى الحاجة إلى تحديثات دورية لقوانين الإنترنت.

وكشفت الدراسة أيضًا أن صعوبات التنفيذ تعيق فعالية قوانين الإنترنت السعودية. وتحد التحديات مثل الأنشطة الإجرامية الإلكترونية عبر الحدود، والتأخير في الإجراءات القضائية، والحاجة إلى قدرات الطب الشرعي المتقدمة من قدرة وكالات إنفاذ القانون على تعقب وملاحقة وإدانة مجرمي الإنترنت بكفاءة. إن الافتقار إلى اتفاقيات التعاون القانوني العالمية، مثل الانضمام الرسمي إلى اتفاقية بودابست بشأن الجرائم الإلكترونية، يزيد من تعقيد الجهود الرامية إلى مكافحة عمليات الاحتيال الإلكتروني الدولية. بالإضافة إلى ذلك، تؤثر العقوبات غير المتسقة والافتقار إلى المحاكم المتخصصة في الجرائم الإلكترونية على التطبيق الموحد للقوانين، مما يخلق تباينًا في نتائج الحكم والملاحقة القضائية.

وأخيرًا، وجدت الدراسة أن الاستفادة من التكنولوجيا وتعزيز التعاون الدولي أمران ضروريان لتعزيز الإطار القانوني والأمني الرقمي في المملكة العربية السعودية. إن تنفيذ أنظمة الكشف عن الاحتيال المدعومة بالذكاء الاصطناعي، والبلوك تشين للمعاملات الآمنة، والتقدم في الطب الشرعي الرقمي من شأنه أن يحسن بشكل كبير جهود منع الاحتيال. وعلاوة على ذلك، فإن زيادة الوعي العام، وتعزيز لوائح الامتثال للشركات، وتعزيز شراكات الأمن السيبراني الدولية الأقوى ستلعب دورًا حاسمًا في تقليل مخاطر الاحتيال الرقمي. وتخلص الدراسة إلى أن التكيف القانوني المستمر، والاستثمار في البنية التحتية للأمن السيبراني، وتعزيز التعاون العالمي ضروري لضمان بقاء المملكة العربية السعودية في طليعة منع الاحتيال الرقمي وإنفاذ الجرائم الإلكترونية.

التوصيات:

وبناءً على نتائج هذه الدراسة، يوصى بأن تواصل المملكة العربية السعودية تحديث إطارها القانوني لمعالجة التهديدات الناشئة في الاحتيال الرقمي والتحايل على أنظمة الحماية الرقمية. ويشمل ذلك مراجعة قانون مكافحة الجرائم الإلكترونية لتضمين أحكام تتعلق بالاحتيال باستخدام الذكاء الاصطناعي، والاحتيال باستخدام تقنيات التزييف العميق، والاحتيال المتعلق بالعملات المشفرة، والجرائم المالية اللامركزية. بالإضافة إلى ذلك، ينبغي تعزيز القوانين التي تحكم حماية المستهلك في المعاملات الرقمية من خلال إلزام المنصات الإلكترونية والمؤسسات المالية بتنفيذ آليات إلزامية للكشف عن الاحتيال والوقاية منه. كما أن إرساء التمييز

القانوني الواضح بين البحث الأخلاقي في مجال الأمن السيبراني والقرصنة الخبيثة ضروري أيضًا لدعم المتخصصين في الأمن السيبراني مع الحفاظ على عقوبات صارمة على مجرمي الإنترنت.

لتعزيز قدرات الإنفاذ، ينبغي للمملكة العربية السعودية إنشاء محاكم متخصصة في الجرائم الإلكترونية بإجراءات سريعة وقضاة مدربين وخبراء في الطب الشرعي الرقمي للتعامل مع قضايا الاحتيال المعقدة بكفاءة. ويجب تزويد وكالات إنفاذ القانون بأدوات الطب الشرعي المتقدمة وتزويدها بتدريب مستمر في مجال الأمن السيبراني لتحسين قدرتها على الكشف عن قضايا الاحتيال الرقمي والتحقيق فيها وملاحقتها. إن تعزيز التعاون القانوني الدولي من خلال الانضمام الرسمي إلى اتفاقية بودابست بشأن الجرائم الإلكترونية وإبرام اتفاقيات ثنائية مع دول أخرى من شأنه أن يسهل التحقيقات في الاحتيال عبر الحدود وتسليم المجرمين الإلكترونيين.

وعلاوة على ذلك، من الضروري زيادة الوعي العام والمساءلة المؤسسية في الامتثال للأمن السيبراني. وينبغي للحكومة أن تطلق حملات وطنية للتوعية بالأمن السيبراني، وإلزام الشركات بإجراء عمليات تدقيق أمنية منتظمة، وفرض عقوبات مالية على الشركات التي تفشل في تنفيذ تدابير كافية لمنع الاحتيال. إن تشجيع تبني التقنيات الناشئة مثل الكشف عن الاحتيال بواسطة الذكاء الاصطناعي، وحلول الأمن القائمة على تقنية البلوك تشين، وأنظمة المصادقة البيومترية من شأنه أن يعزز جهود الحماية الرقمية. ومن خلال تنفيذ هذه التوصيات، يمكن للمملكة العربية السعودية تعزيز بنيتها التحتية للأمن السيبراني، والحد من مخاطر الاحتيال الرقمي، وضمان بيئة رقمية أكثر أمانًا للأفراد والشركات والكيانات الحكومية.

قائمة المراجع العربية:

البقمي، و. (2021). تحليل البرمجيات الخبيثة وتأثيرها على الأمن السيبراني. دار النشر الرقمي.

الحربي، ن. (2022). أمن المعلومات في العصر الرقمي. المجلة السعودية للأمن السيبراني.

الراشد، ف. (2021). أدوات القرصنة والاختراق: دراسة قانونية وتقنية. مركز الأبحاث الأمنية.

الرويلي، ع. (2021). الهجمات السيبرانية وأساليب الحماية الرقمية. جامعة الملك سعود.

السيبيعي، خ. (2020). الهندسة العكسية ودورها في تطوير البرمجيات. دار الفكر التقني.

الشيخ، م. (2020). الأمن الرقمي وحماية المعلومات في العصر الرقمي. دار النشر العربي.

القحطاني، ع. (2021). التحايل الرقمي والجريمة السيبرانية: دراسة قانونية وتقنية. مجلة القانون الرقمي.

- الموسى، ف. (2022). تطورات أمن المعلومات والتشفير. مركز البحوث الأمنية.
- السبيعي، أ. (2020). الهندسة العكسية وبرمجيات الحماية. دار النشر التكنولوجي.
- الرويلي، ن. (2021). الجرائم السيبرانية واختراق الأنظمة الرقمية. المجلة السعودية للأمن السيبراني.
- الراشد، خ. (2020). الثغرات الأمنية في أنظمة التشغيل وتأثيرها على الأمن الرقمي. مركز الدراسات التقنية.
- الحربي، س. (2021). حقوق الملكية الفكرية في العصر الرقمي. مجلة القانون والتقنية.
- العنزي، م. (2022). الهندسة الاجتماعية وأساليب الخداع الرقمي. دار الفكر القانوني.
- الغامدي، ف. (2020). مشاركة الحسابات الرقمية: التأثيرات القانونية والاقتصادية. مركز الدراسات الإعلامية.
- الزهراني، و. (2021). الشبكات الافتراضية الخاصة وتأثيرها على أمن المعلومات. المجلة الدولية لأمن المعلومات.
- العتيبي، م. (2021). ثغرات يوم الصفر وتأثيرها على الأمن السيبراني. دار النشر الأكاديمي.
- السعودي، ف. (2021). تطور الهجمات الإلكترونية وتأثيرها على البنية التحتية الرقمية. مجلة الأمن السيبراني العربي.
- المطيري، خ. (2022). التشريعات السعودية في مواجهة الجرائم المعلوماتية: تقييم وتحليل. دار القانون الرقمي.
- الخالد، ع. (2020). حماية البيانات الشخصية في المملكة العربية السعودية: دراسة مقارنة مع النظام الأوروبي لحماية البيانات (GDPR). المركز العربي للدراسات القانونية.
- العنبر، ح. (2021). التحديات القانونية لإنفاذ قوانين مكافحة الاحتيال الرقمي في السعودية. مجلة الدراسات القانونية والتشريعات الحديثة.

المراجع الأجنبية :

- Al-Fadhli, M. (2022). *Cybercrime and Intellectual Property Protection in Saudi Arabia: Legal Challenges and Solutions*. Riyadh: Legal Studies Journal.
- Brenner, S. (2021). *Cybercrime and Digital Law Enforcement: Strategies for a Secure Future*. Oxford University Press.
- Clough, J. (2020). *Principles of Cybercrime Law: A Comparative Analysis*. Cambridge University Press.
- Goodman, M., & Brenner, S. (2021). *The Impact of Digital Fraud on Global Security*. Harvard Law Review.
- Lemley, M. A. (2018). *Intellectual Property in the Digital Age: The Role of Law and Technology*. Stanford University Press.
- Lessig, L. (2020). *Code and Other Laws of Cyberspace*. Basic Books.
- Samuelson, P. (2019). *Digital Protection and Circumvention: Legal and Ethical Perspectives*. MIT Press.
- Wall, D. (2017). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

إعداد الطالب/ خالد راشد مطلق العتيبي

الرقم الجامعي: 23001499

Supervised by/ Nourallah Elkolaly