النظام الجزائي لجرائم المعلوماتية وأثره في حماية الأمن السيبراني في السعودية

The Penal System for Cybercrimes and Its Impact on Protecting Cyber security in Saudi Arabia

إعداد

الدكتور/ نواف بن نايف بن عبد الله اللغيصم الشمري

دكتوراه في القانون الإداري – كليات الخليج – حفر الباطن

البريد الإلكتروني: nawaf.079@hotmail.com

ملخص البحث

أدى التوسع في استخدام تكنولوجيا المعلومات والإنترنت إلى زيادة الجرائم الإلكترونية التي تهدد الأفراد والمؤسسات، أبرز هذه الجرائم تشمل الاحتيال الإلكتروني، سرقة الهوية، اختراق الحسابات البنكية، والنصب عبر الإنترنت. هذه الجرائم تؤدي إلى أضرار جسيمة مثل الخسائر المالية، تدمير السمعة، وانتهاك الخصوصية، وقد تؤثر بشكل كبير على الثقة في الخدمات الرقمية.

في المملكة العربية السعودية، تم اعتماد نظام جزائي يهدف إلى مكافحة هذه الجرائم وتعزيز الأمن السي براني، تتضمن الجرائم المعلوماتية في السعودية قرصنة الأنظمة، التصيد الإلكتروني، الفيروسات، الاحتيال عبر الإنترنت، واختراق الخصوصية. تم إنشاء قوانين صارمة لمكافحة هذه الجرائم، ويشمل ذلك استخدام تقنيات مثل تشفير البيانات وبرامج مكافحة الفيروسات، بالإضافة إلى تأسيس هيئات متخصصة للأمن السي براني. كما يتم التحقيق في الجرائم الرقمية وملاحقة الجناة عبر نظام قضائي يهدف إلى ردعهم وتحقيق العدالة.

وبرزت هناك تساؤلات حول مدى فعالية النظام الجزائي السعودي في مواجهة جرائم المعلوماتية، وخاصة فيما يتعلق بالثغرات التشريعية والتطبيقية بين القطاعات الحكومية والخاصة. كما يتطلب تعزيز الأمن السيبراني التوازن بين حماية الخصوصية وحقوق الأفراد وبين حماية المجتمع من الجرائم الإلكترونية.

البحث اعتمد منهجيه تعتمد على التحليل التأصيلي والمنهجي، مع مقارنة النظام السعودي بنظم أخرى لتحليل فعالية القوانين والتشريعات في مكافحة هذه الجرائم.

الكلمات المفتاحية: النظام الجزائي لجرائم المعلوماتية، الأمن السيبراني، الجرائم المعلوماتية .

Summary

The expansion of information technology and the internet has led to an increase in cybercrimes that threaten individuals and organizations. Among the most prominent of these crimes are electronic fraud, identity theft, hacking of bank accounts, and online scams. These crimes cause significant harm, including financial losses, damage to reputation, and violation of privacy, which can greatly affect trust in digital services.

In Saudi Arabia, a penal system has been adopted to combat these crimes and enhance cyber security. Cybercrimes in Saudi Arabia include hacking systems, phishing, viruses, online fraud, and privacy breaches. Strict laws have been established to combat these crimes, including the use of technologies such as data encryption and antivirus programs, as well as the establishment of specialized cyber security bodies. Digital crimes are investigated and offenders are pursued through a judicial system aimed at deterring them and ensuring justice.

There have been questions regarding the effectiveness of the Saudi penal system in addressing cybercrimes, particularly with respect to legislative and practical gaps between the public and private sectors. Additionally, strengthening cyber security

requires balancing privacy protection and individual rights with the need to protect society from cybercrimes.

The research relies on an analytical and foundational methodology, comparing the Saudi system with other systems to analyze the effectiveness of laws and regulations in combating these crimes.

key terms:(Penal System for Cybercrimes- Cyber security, - Cybercrimes).

مقدمه

انطلاقاً من قوله تعالى" ولا تجسسوا ولا يغتب بعضكم بعضا أَيُحِب أحَدُكُمْ أَن يَأْكل لحم أخيه ميتا فَكَرِهْتُمُوهُ" صدق الله العظيم

أدى الانتشار الواسع لتكنولوجيا المعلومات والإنترنت إلى زيادة فرص ارتكاب الجرائم الإلكترونية. توفر الشبكة العالمية مساحات غير محدودة للتفاعل والتبادل، مما جعلها ساحة خصبة للمجرمين لاختراق البيانات أو التلاعب بها. ومن أبرز هذه الجرائم: الاحتيال الإلكتروني، سرقة الهوية، اختراق الحسابات البنكية، والنصب عبر الإنترنت. تشمل نتائج جرائم المعلوماتية أضرارًا كبيرة على الأفراد والشركات. ففي حالة سرقة الهوية أو المعلومات الحساسة، قد يتعرض الأفراد لخسائر مالية فادحة أو سمعة مهنية مدمرة. كما أن الشركات تتعرض لتكبد خسائر ضخمة نتيجة تعطيل أنظمتها أو تسريب بيانات العملاء، مما يؤدي إلى فقدان الثقة من قبل المستخدمين. لمكافحة هذه الجرائم، وضعت الدول قوانين صارمة وتدابير أمان متقدمة، مثل تشفير البيانات، برامج مكافحة الفيروسات، وكلمات المرور المعقدة. كما تم تأسيس هيئات متخصصة في مكافحة الجرائم المعلوماتية، مثل وكالة الأمن السيبراني في بعض الدول، والتي تتعاون مع المنظمات الدولية لمكافحة الجريمة الرقمية فما **النظام الجزائي لجرائم المعلوماتية وأثره في حماية الأمن السيبراني في السعودية؟**

اولا : اهمية الموضوع

برزت أنواع من الجرائم المعلوماتية: القرصنة الإلكترونية (الهاكرز) اختراق الأنظمة والشبكات بغرض الحصول على معلومات سرية أو تدمير البيانات، التصدي الإلكتروني :(Phishing) خداع الأفراد للحصول على معلومات شخصية أو مالية مثل كلمات المرور وأرقام الحسابات البنكية، الفيروسات والبرمجيات الضارة :برامج تُصمم لإلحاق الضرر بأجهزة الكمبيوتر أو سرقة البيانات الشخصية، الاحتيال الإلكتروني :استخدام الإنترنت لارتكاب عمليات الاحتيال مثل المبيعات الوهمية أو تغيير بيانات الدفع، الجرائم المتعلقة بالخصوصية :مثل اختراق حسابات البريد الإلكتروني أو حسابات التواصل الاجتماعي بهدف التجسس أو سرقة الهوية، الابتزاز الإلكتروني :تهديد الأفراد أو المؤسسات بنشر معلومات حساسة أو ضارة إذا لم يتم دفع فدية وينتج عنها الأضرار المعلوماتية التالية ، المالية :سرقة الأموال أو البيانات المالية من الأفراد أو الشركات، الخصوصية :انتهاك الخصوصية الشخصية عبر التجسس أو سرقة المعلومات الحساسة، الأمن :تدمير أو اختراق الأنظمة الأمنية للمؤسسات. السمعة :تضرر سمعة الأفراد أو الكيانات نتيجة تسريب معلومات حساسة أو حملات تشويه. مما تتطلب مكافحة هذه الجرائم وجود تشريعات قانونية وأنظمه جزائية تحكم استخدام الإنترنت والأنظمة الإلكترونية، بالإضافة إلى تعاون بين الدول والمنظمات الدولية لتعزيز الأمن الإلكتروني، واستخدام تقنيات حديثة مثل أنظمة الحماية من الفيروسات، وتشفير البيانات.

ثانيا : إشكاليه البحث: من فرضية البحث تكون اشكاليه البحث وفق التساؤلات التالية:

١- ما مدى كفاية النظام الجزائي المعمول به في السعودية في مواجهة جرائم المعلوماتية وتأثيره على تعزيز الأمن السيبراني؟

٢- كيف يساهم الإطار الجزائي في ردع الجناة وتحسين نظم الأمن الرقمي، وهل تظهر فروقات في التطبيق بين القطاعات الحكومية والخصوصية؟

٣- ما هي الثغرات الواقعية والتشريعية في النظام الجزائي لجرائم المعلوماتية التي تعيق حماية الأمن السيبراني؟

٤- ما التوازن بين حماية الخصوصية وحق المجتمع في الأمن الرقمي ضمن الإطار الجزائي السعودي؟

٥- ما آليات التنفيذ والتطبيق القضائي (من التحقيق إلى المحاكمة والعقاب) لدلائل جرائم المعلوماتية، وما مدى فاعليتها في الردع؟

٦- كيف يقارن النظام الجزائي السعودي بالنظم المقارنة في المنطقة أو عالميًا من حيث الآثار على الأمن السيبراني؟

ثالثا: منهجية البحث

أسلوب البحث الذي سنسير عليه هو المنهج التأصيلي والتحليلي باعتباره المنهج الأكثر انسجاما مع طبيعة وأهداف هذا البحث لدراسة وتحليل النصوص التشريعية

وهو المنهج الأكثر ملائمة في دراسة **النظام الجزائي لجرائم المعلوماتية وأثره في حماية الأمن السيبراني** في المملكة العربية السعودية وبعض الدول المقارنة ، مستعيناً بالمنهج المقارن في حالة الاقتضاء، وفقا لحاجة البحث ولخدمته وأهدافه.

رابعاً: خطة البحث:

ارتئي الباحث ان يقسم موضوع بحثه **النظام الجزائي لجرائم المعلوماتية وأثره في حماية الأمن السي براني في السعودية على النحو التالي:**

المطلب التمهيدي :مفهوم جرائم المعلوماتية والأمن السيبراني

الفرع الأول :تعريف جرائم المعلوماتية

الفرع الثاني :مفهوم الأمن السيبراني وأهدافه

المطلب الأول :النظام الجزائي لجرائم المعلوماتية في السعودية

الفرع الأول :التشريعات والقوانين المتعلقة بجرائم المعلوماتية في السعودية

الفرع الثاني :آلية تطبيق النظام الجزائي على الجرائم المعلوماتية

المطلب الثاني :أثر النظام الجزائي على حماية الأمن السيبراني

الفرع الأول :فعالية النظام الجزائي في تعزيز الأمن السيبراني

الفرع الثاني :التحديات التي تواجه النظام الجزائي في حماية الأمن السي براني

الخاتمة:

- **النتائج**
- **التوصيات**

المطلب التمهيدي

مفهوم جرائم المعلوماتية والأمن السيبراني

تمهيد:

تعتبر جرائم المعلوماتية من أخطر الجرائم التي تواجه المجتمع في العصر الحديث، حيث تتعلق باستخدام التكنولوجيا والإنترنت في ارتكاب أفعال غير قانونية. هذه الجرائم تتنوع بين القرصنة الإلكترونية، سرقة البيانات، الاحتيال عبر الإنترنت، والتلاعب بالمعلومات. كما تشمل نشر الفيروسات والبرمجيات الخبيثة التي تهدف إلى تعطيل الأنظمة أو سرقة المعلومات الحساسة. يتزايد تأثير هذه الجرائم بسبب الاعتماد المتزايد على الإنترنت في جميع جوانب الحياة الشخصية والعملية.

أما الأمن السيبراني، فهو مجموعة من التدابير والعمليات المتخذة لحماية الأنظمة الإلكترونية والشبكات من الهجمات والاختراقات. يشمل الأمن السي براني حماية البيانات الشخصية والمالية، والحفاظ على خصوصية الأفراد والمؤسسات، وضمان استمرارية الأعمال عبر الإنترنت. يُعتبر الأمن السيبراني عنصرًا حيويًا لضمان سلامة المعلومات وحمايتها من تهديدات الجرائم المعلوماتية.

وتتعدد أساليب الأمن السيبراني مثل التشفير، والتحقق الثنائي، واستخدام برامج مكافحة الفيروسات، والأنظمة المتقدمة للكشف عن الهجمات. من الضروري أن تكون

المؤسسات والأفراد على دراية بأهمية الأمن الشيباني، حيث أن الهجمات الإلكترونية قد تؤدي إلى أضرار جسيمة تشمل خسارة البيانات، والتعرض لمشاكل قانونية، أو حتى تدمير السمعة.

في هذا السياق، تتعاون الحكومات والمؤسسات الدولية على وضع قوانين وتشريعات لمكافحة الجرائم المعلوماتية. ومع تزايد تهديدات الفضاء الإلكتروني، يصبح تعزيز الأمن السيبراني مسؤولية جماعية تحتاج إلى تنسيق بين الأفراد والهيئات الحكومية والشركات الخاصة.

تقسيم:

الفرع الأول :تعريف جرائم المعلوماتية

الفرع الثاني :مفهوم الأمن السي براني وأهدافه

الفرع الأول

تعريف جرائم المعلوماتية

تعتبر الجرائم المعلوماتية من أخطر التحديات التي تواجه العصر الرقمي، حيث يتزايد استخدامها في ارتكاب الأفعال الإجرامية عبر الإنترنت باستخدام التكنولوجيا الحديثة. تشمل هذه الجرائم مجموعة واسعة من الأنشطة مثل الاختراقات الإلكترونية، الاحتيال عبر الإنترنت، نشر الفيروسات، والتهديدات الإلكترونية التي تهدد الأفراد

والمؤسسات على حد سواء. ومع التطور المستمر في وسائل الاتصال والأنظمة الرقمية، أصبح من الضروري تطوير آليات قانونية وتقنية لمكافحة هذه الجرائم وحماية المعلومات الرقمية. تشكل الجرائم المعلوماتية تهديدًا خطيرًا للأمن السي براني، مما يستدعي تعزيز الوعي والتعاون الدولي لمكافحتها. وفيما يخص تعريف جرائم المعلوماتية من الناحية اللغوية والاصطلاحية:

من الناحية اللغوية:

كلمة "جريمة" في اللغة العربية تأتي من الجذر "جرم"، الذي يعني الفعل الخاطئ أو السيء الذي يؤدي إلى مخالفة القانون أو الأخلاق. أما "المعلومة"، فتعني البيانات أو الحقائق التي يتم جمعها وتخزينها لمعالجتها واستخدامها. وبالتالي، "جرائم المعلوماتية" تشير إلى الأفعال غير القانونية التي يتم تنفيذها عبر الوسائل التكنولوجية لسرقة أو تلاعب أو تدمير البيانات والمعلومات.[١]

من الناحية الاصطلاحية:

تم اعتبار الاصطلاحية[٢]، فقد تطور مفهوم "جرائم المعلوماتية" ليشير إلى الأفعال التي يتم فيها استخدام تكنولوجيا المعلومات والإنترنت لتنفيذ مخالفات قانونية. تشمل هذه الجرائم مجموعة من الأفعال مثل القرصنة الإلكترونية، التسلل إلى الأنظمة، الاحتيال الإلكتروني، وتوزيع البرمجيات الخبيثة. ويرتكب الجاني هذه الجرائم باستخدام

[١] د. العبد الله، مصطفى. "الجرائم الإلكترونية: التحديات والحلول". دار الفكر، ٢٠٠٩، ص ٣٥.

[٢] د. الحداد، فهد. "الجرائم المعلوماتية في التشريع العربي". دار الثقافة، ٢٠١٢، ص ١٠٢.

الكمبيوتر أو الشبكات لتحقيق أغراض غير قانونية، مثل سرقة المعلومات أو تعطيل الأنظمة.

من الناحية الفقهية، تشير "الجرائم المعلوماتية" إلى الأفعال غير المشروعة التي ترتكب باستخدام تكنولوجيا المعلومات والإنترنت، والتي تؤدي إلى انتهاك حقوق الأفراد أو المؤسسات أو تهديد الأمن المعلوماتي. في الفقه الإسلامي، يختلف الحكم على هذه الجرائم حسب الضرر الذي تسببه، ويُعَتَبرُ الفعل غير المشروع في هذا المجال جريمة إذا تضمن تلاعباً بالمعلومات أو اختراقاً لخصوصية الأفراد أو انتهاكاً للأمن العام.[١]

وقد تم اعتبار العديد من الأفعال المرتبطة بالجرائم المعلوماتية، مثل سرقة البيانات أو تدميرها أو تعديلها، بمثابة جريمة ضمن قواعد الشريعة الإسلامية التي تنص على أن أي تلاعب أو تخريب في المال أو الأعراض يُعد جريمة تستوجب العقاب. وفي هذا السياق، تتضمن الجرائم المعلوماتية سرقة المعلومات الشخصية، القرصنة على المواقع الإلكترونية، والاحتيال الإلكتروني[٢].

---

[١] د. عادل محمد النعيمي: الجرائم المعلوماتية في القانون الإسلامي: دراسة فقهية مقارنة"، اطروحة دكتوراه ، جامعة ام القرى ، ٢٠١٣، ص١٢٢

[٢] د. فاطمة سعيد البدري: أثر الجرائم المعلوماتية على النظام القانوني: دراسة مقارنة بين الشريعة والقانون الوضعي"، جامعة القاهرة ، ٢٠١٦، ص٨٩

وقد ذكر بعض[١] ،في الفقه الإسلامي، يُعتبر تدمير أو سرقة البيانات من جرائم الاعتداء على مال الغير، ويُعاقب عليها بالحدود أو التعزير حسب تقدير القاضي. تُعتبر هذه الجرائم من أخطر الجرائم في العصر الحديث نظرًا للتطور التكنولوجي السريع، والذي يتطلب مواكبة القوانين الفقهية لهذا التغيير في وسائل ارتكاب الجرائم.

مما تقدم يرى الباحث ، أن الجرائم المعلوماتية هي الأعمال غير القانونية التي تُرتكب باستخدام أجهزة الكمبيوتر أو الشبكة الإلكترونية (الإنترنت) كأداة لتنفيذ الجريمة. وتُعرف أيضًا بالجرائم الرقمية أو الإلكترونية. تشمل هذه الجرائم مجموعة واسعة من الأفعال التي تستهدف البيانات والمعلومات، سواء بتخزينها أو نقلها أو استخدامها بطرق غير قانونية، ولابد لنا من معرفة طابعها التقني.

- مفهوم جرائم المعلوماتية كجريمة ذات طابع تقني.

ان مفهوم **جرائم المعلوماتية** يُعتبر جزءًا من الجرائم ذات الطابع التقني التي تستهدف المعلومات الإلكترونية أو تُستخدم فيها التكنولوجيا الحديثة. هذه الجرائم تشمل الأنشطة غير القانونية التي ترتكب باستخدام الأجهزة الإلكترونية أو الشبكات المعلوماتية، مثل الاختراقات، الاحتيال الإلكتروني، القرصنة، سرقة البيانات، نشر الفيروسات، والابتزاز الرقمي[٢].

---

[١] د. خالد عبد الرحمن الفقي: الجرائم المعلوماتية وأثرها على حقوق الإنسان في العالم الإسلامي، جامعة الملك عبد العزيز، ٢٠١٨،ص٧٧

[2] M. L. Ray; Cybercrime: Law and Practice, Oxford University Press,2019, p102

يُعتبر مفهوماً **جرائم المعلوماتية** جزءًا من الجرائم ذات الطابع التقني التي تستهدف المعلومات الإلكترونية أو تُستخدم فيها التكنولوجيا الحديثة. هذه الجرائم تشمل الأنشطة غير القانونية التي ترتكب باستخدام الأجهزة الإلكترونية أو الشبكات المعلوماتية، مثل الاختراقات، الاحتيال الإلكتروني، القرصنة، سرقة البيانات، نشر الفيروسات، والابتزاز الرقمي، تناول Ray مفاهيم وأساليب مكافحة جرائم المعلوماتية من خلال فهم الطبيعة التقنية لهذه الجرائم، مع تسليط الضوء على الأدوات المستخدمة في تنفيذ هذه الجرائم وأثرها على الأفراد والمجتمعات. واشار Ray إلى أن جرائم المعلوماتية تتراوح بين التهديدات البسيطة مثل الرسائل الاحتيالية عبر البريد الإلكتروني، إلى الأفعال المعقدة مثل الهجمات الرقمية على البنية التحتية للدول.

ويرى البعض الآخر [١] ، ان مفهوم جرائم المعلوماتية كجريمة ذات طابع تقني في القانون الجنائي المصري يشير إلى الأنشطة الإجرامية التي ترتكب باستخدام التكنولوجيا أو المعلومات الرقمية. هذه الجرائم تشمل التصرفات غير القانونية التي تتم عبر الإنترنت أو باستخدام أجهزة الحاسوب، مثل الاختراقات الإلكترونية، سرقة البيانات، الاحتيال عبر الإنترنت، وتوزيع البرمجيات الخبيثة. كما أن **جرائم المعلوماتية** تشكل تحديًا كبيرًا أمام التشريعات التقليدية، حيث يصعب على الأنظمة القانونية مواكبة التغيرات السريعة في التقنيات الرقمية. وهو يصف هذه الجرائم بأنها **جرائم ذات طابع تقني**، حيث تعتمد على الأدوات الإلكترونية وتستغل الفضاء الإلكتروني كأداة لتنفيذ الجريمة. يرى الباحث أن القانون الجنائي المصري يواجه

[١] د. محمود مصطفى حسن: الجرائم الإلكترونية: دراسة في إطار القانون الجنائي المصري، دار النشر: دار النهضة العربية،٢٠١٨ ، ٥٦

صعوبة في توفير حماية قانونية فعالة ضد هذه الجرائم في ظل غياب تشريعات متكاملة تكفل الوقاية والملاحقة القضائية المتقدمة.

- تتنوع الجرائم المعلوماتية لتشمل العديد من الأفعال التي تُرتكب باستخدام التكنولوجيا الحديثة والشبكات الرقمية، مثل الاختراق، الاحتيال الإلكتروني، نشر الفيروسات، والتهديدات الإلكترونية. ومن أبرز هذه الأنواع[1]:

١- الاختراق :(Hacking) ويقصد به الدخول غير المصرح به إلى الأنظمة أو الشبكات الرقمية بهدف الوصول إلى المعلومات أو تدميرها.

٢- الاحتيال الإلكتروني :(Online Fraud) يتضمن استخدام الإنترنت لتنفيذ عمليات احتياليه مثل بيع منتجات وهمية أو الاحتيال على الأفراد للحصول على بياناتهم الشخصية أو المالية.

٣- نشر الفيروسات :(Virus Distribution) يشمل استخدام البرمجيات الخبيثة لإلحاق الضرر بأجهزة الحاسوب أو سرقة المعلومات الحساسة.

٤- التهديدات الإلكترونية :(Cyber Threats) يشير إلى التهديدات التي قد يتم توجيهها ضد الأفراد أو المؤسسات عبر الإنترنت باستخدام أساليب مثل الابتزاز الرقمي أو التشهير.

(1) Droit, J.-P. (2020). Les crimes informatiques: Entex et législation. Editions' Dalloz, p. 122

الفرع الثاني : مفهوم الامن السيب راني

ان مفهوم الأمن السيبراني يشير إلى مجموعة من السياسات والإجراءات التي تهدف إلى حماية الأنظمة الحاسوبية والشبكات الرقمية من الهجمات والتهديدات الإلكترونية، وذلك لضمان سرية البيانات وسلامتها وموثوقيتها. يتضمن الأمن السي براني الوقاية من التهديدات الإلكترونية مثل الفيروسات، والقرصنة، والهجمات المعقدة على الشبكات، وكذلك التعامل مع الهجمات التي قد تحدث بعد وقوعها.[١] وتتلخص أهدافه على النحو التالي[٢]:

١- حماية البيانات :الحفاظ على سرية المعلومات وحمايتها من الوصول غير المصرح به.

٢- حماية الشبكات :تأمين الأنظمة والشبكات من الهجمات التي قد تؤدي إلى تعطيل الخدمات أو تدمير البيانات.

٣- الحفاظ على الموثوقية :ضمان أن الأنظمة تعمل بشكل صحيح وآمن دون وجود تهديدات قد تضر بالعمليات أو الخدمات.

٤- الامتثال :التزام المؤسسات بالقوانين والسياسات المتعلقة بحماية البيانات والمعلومات.

---

(١) لفتاح: دور الأمن السي براني في حماية المعلومات في المؤسسات الحكومية (رسالة دكتوراه). جامعة القاهرة، ٢٠٢١ص. ٤٥.

(٢) العتيبي، مفاهيم وتقنيات الأمن السي براني في مؤسسات التعليم العالي السعودية (رسالة دكتوراه). جامعة الملك سعود، ٢٠٢٠.ص. ٧٨

اما مفهوم الأمن السي براني من منظور القانون الجنائي الفرنسي[١] ، فانه يركز على الحماية القانونية للأصول الرقمية ضد التهديدات الإلكترونية والهجمات التي قد تعطل الأنظمة الرقمية أو تؤدي إلى سرقة أو تدمير البيانات. ينطوي هذا المفهوم على الحفاظ على سرية وسلامة المعلومات عبر الشبكات الرقمية، وضمان أن الأفراد والشركات والمؤسسات محمية قانونيًا من الجرائم المرتكبة عبر الإنترنت.

ويوضح ميشيل فورتين[٢] ،أن القانون الجنائي الفرنسي يجب أن يعكس التطورات في التكنولوجيا لمواكبة الجرائم الإلكترونية، مؤكداً أن الأمن السي براني لا يتوقف عند منع الهجمات، بل يتضمن أيضًا وضع إطار قانوني للتعامل مع تداعيات تلك الهجمات.

- الأمن السيبراني كمفهوم أساسي لحماية المعلومات والأنظمة.

يُعتبر من المفاهيم الأساسية التي تضمن حماية المعلومات والأنظمة من الهجمات الإلكترونية والتسلل غير المشروع. يرتكز الأمن السي براني على مجموعة من السياسات، الإجراءات، والأدوات التقنية التي تهدف إلى الحفاظ على سرية البيانات وسلامتها وموثوقيتها. في العصر الرقمي، حيث تزداد التهديدات الإلكترونية،

(1) Frénol, J.-P. (2019). Droit pénal de l'internet. Edition’s L.G.D.J, p. 112

(2) Fortin, M. (2021). La Cybercriminalité et le Droit Pénal. edition’s Dalloz, p. 95

أصبح من الضروري أن تواكب التشريعات الوطنية والدولية التطور السريع في مجال التكنولوجيا لضمان الأمن الرقمي.[١]

وتبرز د. كيتلين روبرتسون[٢] ،أهمية الأمن السي براني في تأمين البنية التحتية الحيوية مثل أنظمة الطاقة والمياه، موضحة أن غياب التشريعات المناسبة قد يعرض هذه الأنظمة لهجمات تهدد الأمن القومي.

ويرى الباحث لابد من تطور القوانين الجنائية لمواكبة التهديدات المتزايدة في الفضاء السي براني. فكيف يمكن للقانون الجنائي أن يتعامل مع الجرائم الرقمية من خلال وضع عقوبات رادعة وآليات لحماية الأنظمة الرقمية دون مواكبة الجريمة المعلوماتية ومتغيراتها ؟، ويشدد الباحث على دور القانون في مكافحة الجرائم الإلكترونية بشكل فعال، مع التركيز على ضرورة تحديث التشريعات لتلبية احتياجات الأمان السيبراني.

(1) Wilkinson, S. (2018). Cyber security: Legal and Practical Approaches ,these Oxford University, , p92

(2) Caitlin Robertson; The Role of Cybersecurity in Protecting Critical Infrastructure, these, University of Cambridge ,p105

المطلب الاول

النظام الجزائي لجرائم المعلوماتية في السعودية

تمهيد:

النظام الجزائي لجرائم المعلوماتية في المملكة العربية السعودية، والمعروف بنظام مكافحة جرائم المعلوماتية[١]، يُعدّ من التشريعات الحديثة التي تهدف إلى حماية الأمن السي براني، وضمان سلامة المعلومات، ومكافحة الجرائم المرتكبة باستخدام تقنيات المعلومات. ويهدف إلى: تحقيق الأمن المعلوماتي، حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، حماية المصلحة العامة، والأخلاق، والآداب العامة، حماية الاقتصاد الوطني، وقد حدد النظام في مادته الثانية أهدافه بوضوح، مشيرًا إلى أهمية هذه الأهداف في تعزيز الأمن المعلوماتي وحماية المجتمع من الجرائم الإلكترونية.

عليه سنذهب في تقسيم المطلب اعلاه على النحو التالي:

الفرع الأول :التشريعات والقوانين المتعلقة بجرائم المعلوماتية في السعودية.

الفرع الثاني :آلية تطبيق النظام الجزائي على الجرائم المعلوماتية.

[١] نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (م/١٧) بتاريخ ٨ ربيع الأول ١٤٢٨هـ، الموافق ٢٦ مارس ٢٠٠٧م

الفرع الأول

التشريعات والقوانين المتعلقة بجرائم المعلوماتية في السعودية

في المملكة العربية السعودية صدر المرسوم الملكي[١] ، بشأن نظام مكافحة جرائم المعلوماتية ولم يكن هو الخطوة الأولى في مجال التشريع المعلوماتي، بل سبقه العديد من المراسيم الملكية التي تناولت تنظيم مجال التقنية المعلوماتية المرسوم الملكي[٢] ،بشأن الموافقة على نظام المطبوعات والنشر، وقرار مجلس الوزراء[٣]، بشأن الموافقة على تنظيم هيئة الإذاعة والتليفزيون، وقرار وزير الاعلام[٤]، بشأن اعتماد اللائحة التنفيذية لنظام المطبوعات والنشر، والمرسوم الملكي[٥] ،بشأن الموافقة على نظام المطبوعات والنشر ، واللائحة التنفيذية[٦] ،بشأن الموافقة على نظام الاعلام المرئي والمسموع، والتعميم الاداري[٧]، بشأن تطبيق قرار المجلس الأعلى لمجلس التعاون لدول الخليج العربي في دورته الثالثة والثلاثين التي عقدت بالبحرين في شأن الموافقة على القانون الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون. وقرار مجلس الوزراء[٨] ،بشأن السياسة الاعلامية في المملكة العربية السعودية، والتوقيع على الاتفاقية العربية لمكافحة الجرائم المعلوماتية لسنة ٢٠١٠م والتي تعد من أهم

---

(١) المادة / ١٧ بتاريخ ٨ / ٣ / ١٤٢٨ هـ

(٢) المادة/١٧ بتاريخ ١٣ / ٤ / ١٤٣٣هـ

(٣) المادة(٣٠٢) بتاريخ ١١ / ٩ / ١٤٣٣هـ

(٤) المادة / و / ٢٧٥٩ / ١ / م بتاريخ ١٦ / ٦ / ١٤٢٢هـ

(٥) المادة/ ٣٢ بتاريخ ٣ / ٩ / ١٤٢١هـ

(٦) صدرت بتاريخ ١٦ / ٦ / ١هـ والمعدلة بقرار وزير الاعلام رقم ٩١٥١٣ بتاريخ ٩ / ١١ / ١٤٣٩ هـ والمرسوم الملكي رقم م / ٣٣ بتاريخ ٢٥ / ٣/ ١٤٣٩هـ

(٧) الصادر من وزير العدل برقم (٣٥١) بتاريخ ٣ / ١١ / ١٤٣٤هـ

(٨) رقم ١٦٩ بتاريخ ٢٠ / ١٠ / ١٤٣٢هـ

الاتفاقيات في مكافحة الجرائم المعلوماتية من حيث التجريم والعقاب والتعاون الدولي والأمن القضائي .

وفي مصر صدر القانون رقم ١٧٥ لسنة ٢٠١٨ م[١] ، ولائحته التنفيذية رقم ١٦٩٩ لسنة ٢٠٢٠م[٢] ، بشأن مكافحة جرائم تقنية المعلومات وسبقه العديد من القوانين الخاصة المتعلقة بالمعلومات كقانون حماية الملكية الفكرية، وقانون التوقيع الالكتروني ، وقانون تنظيم الاتصالات وتكنولوجيا المعلومات.

يُعدُّ نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية من أبرز التشريعات الحديثة التي تهدف إلى حماية الأمن السي براني، وضمان سلامة المعلومات، ومكافحة الجرائم المرتكبة باستخدام تقنيات

المعلومات صدر نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (م/١٧) بتاريخ ٨ ربيع الأول ١٤٢٨هـ، الموافق ٢٦ مارس ٢٠٠٧م. ويهدف[٣] ،هذا النظام إلى:

١- تحقيق الأمن المعلوماتي.

٢- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

٣- حماية المصلحة العامة، والأخلاق، والآداب العامة.

---

[١] منشور بالجريدة الرسمية العدد ٣٢ مكرر (ج) بتاريخ ٢٠٢٨/٨/١٤

[٢] منشور بالجريدة الرسمية العدد ٣٥ تابع (ج) بتاريخ ٢٠٢٠/٨/٢٧.

[٣] المادة الثانية من نظام مكافحة جرائم المعلوماتية رقم ١٧

٤- حماية الاقتصاد الوطني.

نص النظام على عدة جرائم معلوماتية وعقوبات محددة لها[١]، منها:

[١] المادة الثالثة من نظام مكافحة جرائم المعلوماتية رقم ١٧

* يُعد نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية أحد أهم الأنظمة التي تُعنى بحماية الفضاء الإلكتروني من مختلف الجرائم التي قد تُهدد أمنه واستقراره.

صدر نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية بمرسوم ملكي رقم (م /17) بتاريخ8/3/1428 هـ عام2007 ، وتم تعديله في عام .2017 ويهدف إلى مكافحة الجرائم التي يتم ارتكابها باستخدام تقنية المعلومات، وحماية حقوق الأفراد والمجتمع من هذه الجرائم.

أهم ميزات نظام مكافحة جرائم المعلوماتية في السعودية

١- تعريف الجرائم المعلوماتية :يحدد النظام أنواع الجرائم المعلوماتية التي يُعاقب عليها، مثل الدخول غير المشروع إلى أنظمة المعلومات، واختراق المواقع الإلكترونية، وسرقة البيانات، والاحتيال الإلكتروني، ونشر المعلومات الكاذبة.

٢- العقوبات :يحدد النظام العقوبات المقررة لكل جريمة معلوماتية، والتي تشمل السجن والغرامة، بالإضافة إلى عقوبات تكميلية مثل مصادرة الأدوات المستخدمة في ارتكاب الجريمة.

٣- الإجراءات :يحدد النظام الإجراءات التي يجب اتباعها للتحقيق في جرائم المعلوماتية وملاحقة مرتكبيها.

٤- الوقاية :يهدف النظام إلى الوقاية من جرائم المعلوماتية من خلال نشر الوعي حول هذه الجرائم وطرق مكافحتها.

أمثلة على الجرائم المعلوماتية

١- الاختراق الإلكتروني.

٢- الابتزاز الإلكتروني.

٣- نشر المعلومات الكاذبة.

٤- التشهير الإلكتروني.

٥- السرقة الإلكترونية.

٦- العقوبات

١- التنصت أو اعتراض البيانات: يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين.

٢- الدخول غير المشروع: يشمل الدخول إلى موقع إلكتروني لتغيير تصاميمه أو إتلافه أو تعديله أو شغل عنوانه.

٣- المساس بالحياة الخاصة: مثل إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها.

٤- التشهير بالآخرين: عبر وسائل تقنيات المعلومات المختلفة.

وسنتناول في هذ المضمار من بحثنا فروع السياسة الجنائية المعلوماتية باعتبارها العمود الفقري للنظام الجزائي للجريمة المعلوماتية وتعالج السياسة الجنائية في اطار حماية المجتمع من مخاطر الظاهرة الاجرامية بصفة عامة والجريمة المعلوماتية بصفة خاصة عده موضوعات وهي التجريم والعقاب والمنع وسنتناول بإيجاز فروع السياسة الجنائية وهي :

١- سياسة التجريم:

وسياسة التجريم كفرع من فروع السياسة الجنائية هي مجموعة المبادئ التي من خلالها توجه المشرع الجنائي في مرحلة انشاء القاعدة القانونية الجنائية الى المصالح الاجتماعية والقيم التي يتعين عليه حمايتها، لاسيما أن الاصل في الاشياء الاباحة ما

يُحدد نظام مكافحة جرائم المعلوماتية العقوبات المُقررة لكل جريمة على حدة، وتتراوح هذه العقوبات بين السجن والغرامة، وقد تصل إلى السجن المؤبد. يمكن الرجوع الى
https://etqanlawfirm-sa.com
تارح الزيارة ٢٠٢٥/٩/٢٧ الساعة ١٢:٤٠

لم يتدخل المشرع بتجريم المباح وجعله محظورا وذلك حفاظا على المصالح الاجتماعية العامة وضماناً للسير الطبيعي لحركة المجتمع، ولذا فالمشرع يكفل الحماية بواسطة القوانين الجنائية وغيرها من القوانين الأخرى كالقانون الاداري والمدني[١]. مع الأخذ في الاعتبار أن السياسة الجنائية في مجال التجريم والعقاب والمنع تختلف من دولة إلى أخرى وفق التطورات الاقتصادية والسياسية والاجتماعية والثقافية من اجل الحفاظ على المصالح والقيم الاجتماعية التي تولدت اثر هذه التطورات ولا سيما وان النصوص القانونية سواء المتعلقة بالتجريم والعقاب والمنع والمتعلقة بموانع المسئولية والمبيحة جميعها ترتبط ارتباطا وثيقاً بالقيم والاخلاق الاجتماعية السائدة داخل المجتمع. [٢]

وخلاصة القول فسياسة التجريم تحتوي على ما يتعلق بالمصالح الجديرة بالحماية للمجتمع وذلك من خلال القيام بعملية تجريم كل الأفعال التي تمس بالمصالح الأساسية للدولة، فهذه السياسة تتضمن المصالح الاجتماعية بشقيها الفردي والجماعي من الاعتداء عليها[٣] . وعلى ذلك يمكن اعتبار سياسة التجريم من أهم الوسائل التي تحظى بها كل المجتمعات في التعبير عن اقصى درجات الحماية للقيم والمصالح التي تهمها. ٢- سياسة العقاب

---

(١) د احمد فتحي سرور، اصول السياسة الجنائية ، دار النهضة العربية ، ١٩٧٢ ، ص ١٥٢.

(٢) د. عادل يحيى – السياسة الجنائية في مواجهة الجريمة المعلوماتية ، دار النهضة العربية ، الطبعة الأولى، ٢٠١٤ ، ص٢٨

(٣) د. اسامة صلاح محمد بهاء الدين ، مكانه الاصلاح واعادة التأهيل في السياسة الجنائية المعاصرة، مجلة الدراسات العليا، جامعة النيلين ، العدد د س ، ص١٦

سياسة العقاب كفرع من فروع السياسة الجنائية ليست قاصرة على المشرع الجنائي فحسب بل تتعلق بالمشرع الجنائي والقاضي والسلطة التنفيذية فمن ناحية المشرع الجنائي وفق القاعدة الشرعية لا جريمة ولا عقوبة إلا بنص ، ولا جريمة بدون عقوبة أو تدبير ، ولذا يتدخل المشرع بتجريم الفعل وبموجبه يقوم القاضي بتوقيع العقوبة الواردة بالنص وفق مبدأ الشرعية الجنائية مع الآخذ في الاعتبار أن العقوبة ايلام مقصود يوضع من اجل الجريمة ويتناسب معها[١] وأن العقوبة مرتبطة ارتباطا وثيقا بالجريمة (١) وهذا الارتباط والتناسب بين ايلام العقوبة مع جسامة الجريمة الذي يبرز معنى الجزاء العادل في العقوبة[٢] والتدابير الاحترازية. ويتعين على القاضي توقيع العقوبة الواردة بالنص، إلا أنه يترك له سلطة تقديرية في اختيار العقوبة الملاءمة من بين العقوبات التي يحددها القانون تحقيقاً للردع العام والخاص والعدالة.

وأخيرا وبصدور حكم واجب التنفيذ يتعين على الدولة متمثلة في السلطة التنفيذية في الزام المحكوم عليه بتنفيذ الحكم في المؤسسات العقابية مرتكزة على مجموعة من المبادئ الاساسية في مجال التنفيذ العقابي، منها تحديد اساليب التنفيذ العقابي وفقا للقواعد العلمية والاصول الفنية من خلال فحص شخصية المحكوم عليه وتصنيفهم وتحديد اساليب الاصلاح والتأهيل وما يتعلق بالمؤسسات العقابية، مع ضرورة احترام حقوق المحكوم عليه بما يحفظ عليه كرامته وتمكينه من العمل والتريض والتعلم مع ربط المحكوم عليه بالمجتمع اثناء تنفيذ فترة العقوبة.

---

(١) د. نجاتي سيد احمد سند – علم الاجرام والعقاب، حقوق الزقازيق، ٢٠٠٢ ، ص ٣٥؛ د/ عادل يحيى –مبادئ علم العقاب – الطبعة الأولى، دار النهضة العربية، ٢٠٠٥ ، ص ٤٦

(٢) د .عبد التواب معوض الشوربجي، علم العقاب – حقوق الزقازيق، ٢٠١٧ ، ص ١٥.

٣- سياسة المنع

سياسة المنع كفرع من فروع السياسة الجنائية يقصد بها التدابير الفعالة التي تتخذ من اجل وقاية المجتمع من مخاطر الجريمة قبل وقوعها ، وذلك من خلال العوامل المتهيئة لارتكابها . [١]ومن اساليب منع ارتكاب الجريمة في القضاء على اسباب الظاهرة الاجرامية تختلف باختلاف طبيعة الجريمة ونحن بصدد الجريمة المعلوماتية يتمثل اساليب سياسة المنع في وضع برامج وأنظمة حماية وتأمين ضد الفيروسات وملاحقة المجرم المعلوماتي، مع تشفير البيانات وتتبع غسل الاموال عبر الانترنت الى غير ذلك من الوسائل التي تمثل عائقاً أمام ارتكاب الجرائم المعلوماتية.[٢]

- التشريعات المساعدة: مثل نظام حماية البيانات الشخصية وأي قوانين مرتبطة بحماية المعلومات.

في مصر والسعودية كانت هناك ايضا التشريعات المساعدة في مجال حماية المعلومات مع التركيز على نظام حماية البيانات الشخصية وبعض القوانين ذات الصلة، السعودية ومصر اعتمدتا مؤخرًا تشريعات متقدمة وحديثة لحماية البيانات الشخصية تتماشى مع المعايير العالمية (قريبة من اللائحة الأوروبية(GDPR) وهذه التشريعات مدعومة بقوانين مكافحة الجرائم

(١) د .عادل يحيى المرجع السابق، ص ٤٠.

(٢) د. هدى حامد قشقوش السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية ، ٢٠١٢ ، ص ١٠.

المعلوماتية والأمن السيبراني لضمان شمولية الحماية وهي تعزز الثقة في الاقتصاد الرقمي وتشجع على الاستثمارات التكنولوجية.[١]

ونظام حماية البيانات الشخصية السعودي تشريع متكامل في هذا المجال. أهم ما ينص عليه: الحصول على موافقة صاحب البيانات قبل جمعها أو معالجتها، تحديد الغرض من جمع البيانات واستخدامها فقط فيما جُمعت له، الحق في التعديل أو الحذف عند انتهاء الحاجة، قيود على نقل البيانات خارج المملكة إلا بضوابط محددة وتقع تحت اشراف الهيئة السعودية للبيانات.

اما في مصر، فقد صدر قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ وهو أول تشريع مصري شامل لحماية البيانات ومن أهم أحكامه هي:

١- موافقة مسبقة من صاحب البيانات لجمع أو استخدام معلوماته.

٢- إلزام الشركات بتعيين مسؤول حماية بيانات (Data Protection Officer).

٣- منع نقل البيانات إلى الخارج إلا بضوابط صارمة.

٤- حق الفرد في الاطلاع، التصحيح، والاعتراض على المعالجة.

---

[١] نظام حماية البيانات الشخصية السعودي صدر بموجب المرسوم الملكي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩هـ، ٢٠٢١ وفي مصر صدر قانون حماية البيانات الشخصية رقم ١٥١ | ٢٠٢٠ | صدر بموجب القانون رقم ١٥١ لسنة ٢٠٢٠ ب

وتقع تحت اشراف مركز حماية البيانات الشخصية التابع لوزارة الاتصالات وتكنولوجيا المعلومات كما صدر قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ والذي يجرم اختراق الأنظمة والشبكات.او الاعتداء على البيانات أو تعطيلها.او نشر أو إفشاء بيانات خاصة دون موافقة. وتشمل عقوبات تصل إلى السجن المشدد وغرامات بمئات الآلاف من الجنيهات. وهناك قوانين أخرى مساندة مثل قانون حماية المستهلك الذي يضمن سرية بيانات العملاء لدى الشركات. وقوانين الأمن القومي والتي تلزم بعض المؤسسات بتأمين بياناتها وربطها بالجهات الرقابية.

الفرع الثاني

آلية تطبيق النظام الجزائي على الجرائم المعلوماتية

يظهر النظام السعودي اهتمامًا بالغًا بمكافحة الجرائم المعلوماتية، من خلال تحديد الإجراءات القانونية الواضحة، وتحديد دور الجهات القضائية في التحقيق والمحاكمة، مما يسهم في تعزيز الأمن المعلوماتي وحماية حقوق الأفراد والمؤسسات. وفي إطار مكافحة الجرائم المعلوماتية، تتبنى المملكة العربية السعودية نظامًا قانونيًا متكاملًا يحدد الآليات والإجراءات المتبعة للتحقيق والمحاكمة، ويحدد دور الجهات القضائية في معاقبة مرتكبي هذه الجرائم[١]. والإجراءات المتبعة في السعودية للتحقيق في الجرائم الإلكترونية تكون تقديم البلاغات حيث يتيح النظام السعودي للأفراد تقديم

[١] مجلس الوزراء السعودي: نظام مكافحة جرائم المعلوماتية دار نشر مجلس الوزراء،2007 ، المادة ١

بلاغات عن الجرائم المعلوماتية من خلال عدة قنوات، أبرزها: تطبيق "كلنا أمن" الذي يتيح للمواطنين والمقيمين تقديم البلاغات بشكل مباشر وسريع. كذلك المراكز الأمنية المنتشرة في مختلف المناطق، حيث يمكن تقديم البلاغات بشكل تقليدي. ومن ثم إجراء لتحقيقات حيث تتولى النيابة العامة التحقيق في الجرائم المعلوماتية، حيث تشمل الإجراءات: جمع الأدلة الرقمية من الأجهزة الإلكترونية والمواقع الإلكترونية، استجواب المشتبه بهم والشهود، التعاون مع الخبراء الفنيين لتحليل الأدلة الرقمية ومن ثم تتولى الجهات القضائية حيث تتولى المحكمة الجزائية النظر في القضايا المتعلقة بالجرائم المعلوماتية، حيث تشمل اختصاصاتها: محاكمة المتهمين وتحديد العقوبات المناسبة، إصدار الأحكام المتعلقة بمصادرة الأجهزة المستخدمة في ارتكاب الجريمة، إغلاق المواقع الإلكترونية أو الحسابات المرتبطة بالجريمة[١].

[١] د. خالد عايض آل حمدان الغامدي: الاختصاص القضائي في الجرائم الإلكترونية وفقًا للنظام السعودي، مجلة الفقه والقانون

المطلب الثاني

أثر النظام الجزائي على حماية الأمن السي براني

الأمن السي براني[١]، هو مجموعة من الإجراءات، والسياسات، والتقنيات التي تهدف إلى حماية الأنظمة الرقمية والشبكات من الهجمات والتهديدات التي قد تضر بالبيانات أو النظام ذاته. في ظل التقدم التكنولوجي المستمر وازدياد استخدام الإنترنت، أصبح الأمن السي براني جزءًا لا يتجزأ من أي استراتيجية لحماية المعلومات وحفظ الأمن في العصر الحديث. وفي هذا السياق، يظهر دور النظام الجزائي كأداة قانونية هامة في مكافحة الجرائم الإلكترونية وحماية الأمن السي براني.

االنظام الجزائي: تعريف وأهمية النظام الجزائي يشير إلى القوانين التي تحدد المسؤوليات الجنائية والعقوبات المترتبة على الأفعال غير القانونية التي تمس الأفراد أو المجتمع. يهدف هذا النظام إلى ردع الجرائم وضمان العدالة، من خلال تطبيق العقوبات المناسبة على الأفعال التي تُعتبر جريمة في النظام القانوني. مع تزايد استخدام التقنيات الرقمية وتنوع الجرائم الإلكترونية، أصبح النظام الجزائي أكثر تعقيدًا وأهمية في تأمين الحماية اللازمة للأمن السي براني.

---

[١] صدر الأمر الملكي رقم (٥٥٧٧٥) بتاريخ ١/١٢/١٤٣٨ هـ القاضي بإنشاء هيئة باسم الهيئة الوطنية للأمن السي براني، وصدر الأمر الملكي رقم (٦٨٠١) بتاريخ ١١/٠٢/١٤٣٩ هـ القاضي بالموافقة على تنظيمها – المعدّل بالأمر الملكي رقم (٧٠٥٣) بتاريخ ٢/٢/١٤٤٣ هـ – لتكون الهيئة الوطنية للأمن السي براني الجهة المختصة بالأمن السي براني في المملكة والمرجع الوطني في شؤونه، وتتمتع بالشخصية الاعتبارية العامة والاستقلال المالي والإداري، وترتبط بالملك

ومع ازدياد عدد المستخدمين للإنترنت، ظهر العديد من التهديدات الإلكترونية التي تستهدف البيانات والمعلومات الحساسة. تتنوع هذه التهديدات من هجمات على مستوى الأفراد مثل سرقة الهوية الرقمية، إلى هجمات على مستوى المؤسسات الكبرى مثل اختراق الأنظمة، الابتزاز الإلكتروني، وتدمير البنية التحتية للأنظمة. هذه الجرائم تضر بالاقتصاد، وتزعزع الثقة في الأنظمة الرقمية، مما يهدد استقرار المجتمعات ويدفع الحاجة إلى وجود آليات قانونية وقائية فاعلة.

يتضمن هذا النظام[١] ،العديد من المواد التي تتعلق بحماية المعلومات الشخصية، التصدي للهجمات الإلكترونية، ضمان أمان الشبكات، وتعزيز التعاون بين الجهات المختلفة في المملكة لضمان استقرار الأمان السيبراني.

والنظام الجزائي له دور في حماية الأمن السيبراني، ومن أبرز الأدوار التي يلعبها النظام الجزائي هو رصد الجرائم الإلكترونية، مثل اختراق البيانات، هجمات البرمجيات الخبيثة، والتهديدات المرتبطة بالشبكات. من خلال فرض عقوبات صارمة على مرتكبي هذه الجرائم، يحقق النظام الجزائي ردعًا قويًا لكل من يفكر في استخدام التقنيات الرقمية لأغراض غير قانونية. وتساهم العقوبات القاسية في تحجيم الجرائم السيرانيه وتقليل فرص انتشارها. كما ان النظام الجزائي يسهم أيضًا في تنظيم الممارسات الرقمية. فعند تطبيق قوانين صارمة تحظر التصرفات غير الأخلاقية أو

[١] المرسوم الملكي رقم (م/٨٢) لعام ٢٠١٨ الخاص بـ "نظام الأمن السي براني"، الذي يهدف إلى تنظيم قطاع الأمن السي براني في المملكة ويدعم تطوير البنية التحتية الأمنية وحمايتها من المخاطر، كما صدرت اللائحة التنفيذية لنظام الأمن السي براني، التي تحدد الإجراءات التفصيلية لمتابعة تنفيذ النظام وتطبيق السياسات الأمنية المتعلقة بالأمن السي براني .

المخالفة للقانون عبر الإنترنت، مثل التجسس على البيانات أو التلاعب بالأنظمة، فإن هذا يعزز من ثقافة الاستخدام الآمن للتقنيات. كما أن النظام الجزائي يشجع الشركات والمؤسسات على الالتزام بالمعايير الأمنية لحماية بيانات العملاء والمستخدمين، ما يعزز من فعالية الأمن السي براني. وفي عالم متشابك تقنيًا، حيث تصبح الجرائم السيبرانية عابرة للحدود، يلعب النظام الجزائي دورًا في تشجيع التعاون بين الدول والمنظمات الدولية لمكافحة الجرائم الإلكترونية. قوانين مشتركة تساعد في تبادل المعلومات والتعاون في ملاحقة مرتكبي الجرائم الإلكترونية في مختلف البلدان. هذا التعاون يعزز من قدرة السلطات على محاربة الجريمة السي برانية بشكل أكثر فعالية والجدير بالذكر بالإضافة إلى حماية الأنظمة من الهجمات، يسهم النظام الجزائي في ضمان حماية حقوق الأفراد في الفضاء الرقمي. يتضمن ذلك حماية الخصوصية الرقمية، وضمان أمان البيانات الشخصية، ومنع الانتهاكات التي يمكن أن تحدث من خلال الوصول غير المصرح به أو الاستغلال غير القانوني للمعلومات.

رغم الدور الكبير الذي يلعبه النظام الجزائي في حماية الأمن السي براني، إلا أنه يواجه العديد من التحديات:

- التطور السريع للتقنيات: مع تطور تقنيات الهجوم والدفاع، تصبح الجرائم الإلكترونية أكثر تعقيدًا وتحديًا من الناحية القانونية. قد لا تكون القوانين الحالية كافية لمواكبة هذه التطورات، مما يستدعي تعديلات مستمرة في النظام الجزائي لمواكبة التغيرات السريعة.

- الاختلافات القانونية بين الدول: بما أن الجرائم الإلكترونية يمكن أن تكون عابرة للحدود، فإن اختلاف الأنظمة القانونية بين الدول يشكل عقبة في تطبيق العدالة. وهذا يتطلب تنسيقًا دوليًا فعالًا لتحديد مسؤولية الأفراد ومحاسبتهم.
- الوعي القانوني والتقني: كثير من الأفراد والشركات قد لا يكونون على دراية كافية بالقوانين المتعلقة بالجرائم الإلكترونية، مما يؤدي إلى ضعف الالتزام بالقوانين أو عدم معرفة الأضرار المحتملة من الجرائم السي برانية. لذلك، فأن تطوير حملات توعية قانونية وتقنية يصبح أمرًا أساسيًا

ختاما إن النظام الجزائي يلعب دورًا محوريًا في حماية الأمن السي براني من خلال فرض عقوبات رادعة، تنظيم الممارسات الرقمية، وتعزيز التعاون بين الدول وهذا ما سعت اليه السعودية[١]. ولكن لا بد من تكامل الجهود التشريعية والتقنية لتوفير بيئة رقمية آمنة ومستدامة. مع تطور التهديدات الرقمية وتعدد الجرائم الإلكترونية، تصبح الحاجة إلى تعديل وتطوير الأنظمة الجزائية أمرًا ضروريًا لمواكبة هذه التحديات وحماية المصالح الاقتصادية والاجتماعية للأفراد والمجتمعات.

(١) في النظام السعودي، تناولت عدة مواد قانونية موضوع الأمن السي براني، ومن أبرزها:
نظام مكافحة الجرائم المعلوماتية :وهو يشمل العديد من المواد التي تتعلق بالأمن السي براني وحماية المعلومات. على سبيل المثال:
المادة الأولى :تعرف الجريمة المعلوماتية وتحدد الأفعال التي تشكل تهديدًا للأمن السي براني.
المادة الثالثة :تتعلق بالتحقيق والملاحقة القانونية للأشخاص الذين يتورطون في الجرائم

الفرع الأول :فعالية النظام الجزائي في تعزيز الأمن السي براني

دور القوانين في تعزيز الأمان السي براني على مستوى المؤسسات الحكومية والشركات الخاصة.

إن التمييز بين الجرائم السي برانية والجرائم غير السي برانية يعتبر أمراً بالغ الأهمية، خاصة عند العودة إلى التشريعات المتعلقة بالجرائم السي برانية في الدول العربية التي تتعمد إضافة جرائم غير سيبرانني في جوهرها ضمن هذه القوانين. وهذا يترافق مع تشديد العقاب ومنح الأجهزة الأمنية سلطات واسعة للتحقيق، مثل اعتراض الاتصالات وحجز أنظمة المعلومات والأجهزة الإلكترونية، وغيرها من الصلاحيات التقنية التي من شأنها تهديد خصوصية الأفراد.

على الرغم من غياب توافق دولي حول تعريف الجرائم السي برانية، إلا أننا نلاحظ بأن كل التعريفات ترتكز على استعمال أنظمة المعلومات والاتصال لارتكاب الجريمة كعنصر جوهري في التعريف[١]. وعلى هذا الأساس، ظهرت عدة تصنيفات[٢] من

---

(١) يراجع في ذلك:

Kristy Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken, Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies, available online: https://www.mdpi.com/2673-6756/2/2/28

Rick Sarre, Laurie Yiu-Chung Lau & Lennon Y.C. Chang (2018) Responding to cybercrime: current trends, Police Practice and Research, available online: https://doi.org/10.1080/15614263.2018.1507888

(2) Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken, Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies, available online:

أهمها التصنيف بين الجرائم السي برانية الصرفة Cyber-enabled crimes والجرائم السي برانية بالتبعيةCyber-dependent crimes .

تعتبر الجرائم السي برانية بطبيعتها جرائم مستحدثة ظهرت نتيجة للتطور التكنولوجي الذي عرفه العالم في العقود الأخيرة والتي لا يمكن ارتكابها إلا عبر أنظمة المعلومات والاتصال، مثل تعطيل أنظمة المعلومات والاتصال أو النفاذ غير المشروع إليها. في المقابل، هناك جرائم سي برانية بالتبعية، التي أصبح بالإمكان ارتكابها داخل الفضاء السي براني إلى جانب الفضاء الحقيقي. ويشمل هذا التصنيف عدة جرائم مثل نشر المحتوى الذي يتضمن اعتداءات جنسية على القصر أو الاعتداء على الملكية الفكرية أو الاحتيال والابتزاز الرقميين، وغيرها من الجرائم التي يمكن أن تمارس خارج الفضاء السيبرانيه.

وعند العودة إلى التشريعات الموجودة في المنطقة العربية، نلاحظ أن المواد المتعلقة بالجرائم السيبرانيه بالتبعية أكثر من المواد المتعلقة بالجرائم السي برانية الصرفة. كما يوجد توجه مفرط نحو تجريم طائفة واسعة من المضامين وفقاً لعبارات فضفاضة، مثل تعطيل العمل بالدستور أو المساس برموز الدولة أو الترويج لمظاهرات دون ترخيص أو نشر الأخبار الزائفة والإساءة إلى الأفراد. وقد وصل الأمر في بعض الدول العربية إلى أن عدد جرائم المحتوى تجاوز الجرائم السي برانية

https://www.mdpi.com/2673-6756/2/2/28

الصرفة. مثل الاختراق السي براني وتدمير أنظمة الاتصال، وهي الجرائم التي كانت السبب الأصلي لتوجه الدول نحو سن مثل هذه التشريعات. "[١]

كما لاحظنا أيضاً ضعفاً في الضمانات القانونية حتى بالنسبة للجرائم السيبرانيه الصرفة، حيث تكتفي أغلب الدول العربية إما بتجريم النفاذ غير المشروع لأنظمة المعلومات والاتصال أو تشترط في أحسن الأحوال نية العمد، في حين أن عليها أن تشترط أيضاً أن يكون النفاذ غير المشروع لأنظمة المعلومات والاتصال بدون وجه حق.

كما لاحظنا أيضاً ضعفاً في الضمانات القانونية حتى بالنسبة للجرائم السي برانية الصرفة، حيث تكتفي أغلب الدول العربية إما بتجريم النفاذ غير المشروع لأنظمة المعلومات والاتصال أو تشترط في أحسن الأحوال نية العمد، في حين أن عليها أن تشترط أيضاً أن يكون النفاذ غير المشروع لأنظمة المعلومات والاتصال بدون وجه حق.

---

[١] د. ايمن الزغرودي: ورقة سياسات قوانين الجرائم السيبرانيه في المنطقة العربية: حماية للفضاء الرقمي ام قمع للحريات (مقالة) ayman @ccesnow.org تاريخ الزيارة ٢٠٢٥/١٠/٨ الساعة ٦:٣٠

* تدافع أكساس ناو (https://www.accessnow.org) عن الحقوق الرقمية للأشخاص المعرضين للخطر حول العالم.تاريخ الزيارة ٢٠٢٥/١٠/٨، الساعة ٦:٣٠
تكافح من أجل حقوق الإنسان في العصر الرقمي من خلال الجمع بين الدعم التقني المباشر والمشاركة الشاملة في مجال السياسات العامة والمناصرة الدولية وتقديم المنح للقواعد الشعبية وعقد المؤتمرات مثل الراي تسكون.

ومن شأن هذا الشرط الأخير (النفاذ بغير حق أن يحمي عدة ممارسات مشروعة يتعمد أصحابها النفاذ غير المشروع من أجل غايات سامية ونبيلة، مثل الأعمال التي تقوم بها الصحافة الاستقصائية للكشف عن انتهاكات حقوق الإنسان ومكامن الفساد أو أنشطة الباحثين في مجال السلامة المعلوماتية الذين يمكن أن تساهم أنشطتهم في كشف الثغرات التي تشكو منها بعض أنظمة المعلومات والاتصال وتطوير أدائها.

مما تقد نخلص ان مدى فعالية النظام الجزائي في ردع الجرائم المعلوماتية وحماية الأنظمة الإلكترونية، تنحصر في الاغلب في قمع الحريات وخاصة في الأنظمة العربية، اما تحقيق الردع الالكتروني فهذه تتحقق بنسبه ضئيلة.

الفرع الثاني

التحديات التي تواجه النظام الجزائي في حماية الأمن السي براني

ان دور القوانين في تعزيز الأمان السي براني على مستوى المؤسسات الحكومات والدول وعلى الرغم من المزايا العديدة التي خلفها التطور التكنولوجي الحديث ، افرز لنا الكثير من الجرائم التي تختلف في صفاتها واشكالها واثارها عن الجرائم التقليدية، واصبحت تمثل تهديدا مباشرا وواضحا للأمن والسلم المحلي والدولي نظراً لكونها جرائم تتميز بأنها معقدة للغاية لتنوعها وسهولة ارتكابها وقدرة الجناة على

التخفي والهرب ومحو دليل الادانة، مما يصعب معه اكتشافها واثبات ادلتها وضبط مرتكبيها[١].

وعن اسباب ظهور هذه الجرائم وانتشارها بصورة مرعبة ، التطورات العلمية، والتحولات الاجتماعية والاقتصادية والثقافية المحلية والعالمية والفراغ الاجتماعي الاسري وغياب القيم والمبادئ الاخلاقية والدينية لدى الابناء والبطالة مع عدم وجود التشريع المناسب والعقوبة الرادعة نظراً لحداثة هذه الطائفة من الجرائم والمجرمين ، واعتماد اغلب الدول على التشريعات التقليدية والتي لا تتناسب مع خطورة هذه الطائفة من الجرائم المعلوماتية ، مما دفع المجتمع الدولي الى البحث فيما اذا كانت القوانين المتعلقة بمكافحة الجريمة كافيه لمواجهة ظاهرة الاجرام المعلوماتي التقني والاستخدامات غير المشروعة لتكنولوجيا المعلومات، أم أنها بحاجة لتطوير قواعدها ونصوصها القانونية المعمول بها لمواجهة الجريمة والفكر الاجرامي التقني وسن تشريعات ونصوص عقابية جديدة.

ولا يجب التغافل ان هناك تحديات وقانونية والإجرائية: مثل صعوبة تتبع الجرائم عبر الإنترنت، وضرورة تحسين التعاون الدولي في مكافحة الجرائم الإلكترونية

---

(١) د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت – دار الكتب القانونية ٢٠٠٥ ، ص ٣٥ ، د/ هشام محمد فريد رستم الجرائم المعلوماتية ، اصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي ، بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنت –كلية الشريعة والقانون بدولة الامارات ٢٠٠٥، ص ٣٨.

الخاتمة

تناولنا في بحثنا الجرائم المعلوماتية والتي هي من أخطر الجرائم في العصر الحديث، وتشمل القرصنة الإلكترونية، سرقة البيانات، الاحتيال عبر الإنترنت، ونشر الفيروسات والبرمجيات الخبيثة. تتزايد بسبب الاعتماد على الإنترنت في الحياة اليومية. أما الأمن السيب راني فهو إجراءات لحماية الأنظمة والشبكات من الهجمات والاختراقات، ويهدف إلى حماية البيانات الشخصية والمالية وضمان استمرارية الأعمال عبر الإنترنت. وعرفنا الأمن السيبرانيه بانه: مجموعة من التدابير لحماية الأنظمة والشبكات من الهجمات، ويشمل حماية البيانات الشخصية والمالية وضمان استمرارية الأعمال. يتم استخدام أساليب مثل التشفير والتحقق الثنائي لمكافحة الهجمات الإلكترونية. الهجمات قد تؤدي إلى خسارة البيانات ومشاكل قانونية. تتعاون الحكومات والمؤسسات لوضع قوانين لمكافحة الجرائم المعلوماتية، وتعزيز الأمن السيب راني يتطلب تنسيقًا بين الأفراد والحكومات والشركات. وعرفناها من الناحية الاصطلاحية، فهي تشير "جرائم المعلوماتية" إلى الأفعال غير القانونية التي تتم باستخدام تكنولوجيا المعلومات والإنترنت، مثل القرصنة الإلكترونية، التسلل، الاحتيال، وتوزيع البرمجيات الخبيثة. تهدف هذه الجرائم إلى سرقة المعلومات أو تعطيل الأنظمة ومن الناحية الفقهية فهي تشير إلى الأفعال غير المشروعة التي تُرتكب باستخدام تكنولوجيا المعلومات، مما يهدد حقوق الأفراد والأمن المعلوماتي. في الفقه الإسلامي، اذ تُعد هذه الجرائم جريمة إذا تسببت في تلاعب بالمعلومات أو اختراق للخصوصية أو انتهاك للأمن. تدميراً أو سرقة البيانات يُعد من الجرائم التي تستوجب العقاب وفقاً لقواعد الشريعة الإسلامية. وتناولنا مفهوم جرائم المعلوماتية

كجريمة ذات طابع تقني وذكرنا ان تتنوع الجرائم المعلوماتية لتشمل العديد من الأفعال التي تُرتكب باستخدام التكنولوجيا الحديثة والشبكات الرقمية، مثل الاختراق، الاحتيال الإلكتروني، نشر الفيروسات، والتهديدات الإلكترونية. **وتوصلنا الى نتائج** ومنها:

- لابد من تطور القوانين الجنائية لمواكبة التهديدات المتزايدة في الفضاء السيبراني. فكيف يمكن للقانون الجنائي أن يتعامل مع الجرائم الرقمية من خلال وضع عقوبات رادعة وآليات لحماية الأنظمة الرقمية دون مواكبة الجريمة المعلوماتية ومتغيراتها ؟، ويشدد الباحث على دور القانون في مكافحة الجرائم الإلكترونية بشكل فعال، مع التركيز على ضرورة تحديث التشريعات لتلبية احتياجات الأمان السيب راني.

- ان النظام الجزائي يجب ان يكون متدرجا، سياسة تجريم، سياسة منع، سياسة عقاب

- والإجراءات المتبعة في السعودية للتحقيق في الجرائم الإلكترونية تكون تقديم البلاغات حيث يتيح النظام السعودي للأفراد تقديم بلاغات عن الجرائم المعلوماتية من خلال عدة قنوات، أبرزها: تطبيق "كلنا أمن" الذي يتيح للمواطنين والمقيمين تقديم البلاغات بشكل مباشر وسريع. كذلك المراكز الأمنية المنتشرة في مختلف المناطق، حيث يمكن تقديم البلاغات بشكل تقليدي.

- **وخرجنا بعدة توصيات متعلقة بالنظام الجزائي**، مبتغاها لابد ان يحقق في البداية العدالة ؛ويحافظ على قيم العدل؛ وان لا تمس الخصوصيات؛ الا اذا اقتضت الضرورة ذلك

- تعديل القوانين والأنظمة المتعلقة بكيفية التعامل مع المنصات الرقمية العالمية.

- التأكيد على حماية البيانات والأمن السيبراني.

المراجع

القران الكريم

- سورة الحجرات: الآية ١٢

اولا :المراجع العربي

١- احمد فتحي سرور، اصول السياسة الجنائية ، دار النهضة العربية ، ١٩٧٢ ، ص ١٥٢.

٢- اسامة صلاح محمد بهاء الدين ، مكانه الاصلاح واعادة التأهيل في السياسة الجنائية المعاصرة، مجلة الدراسات العليا، جامعة النيلين ، العدد د س ، ص١٦

٣- ايمن الزغرودي: ورقة سياسات قوانين الجرائم السيب رانيه في المنطقة العربية: حماية للفضاء الرقمي ام قمع للحريات (مقالة) ayman @ccesnow.org

٤- الحداد، فهد. "الجرائم المعلوماتية في التشريع العربي". دار الثقافة، ٢٠١٢، ص ١٠٢.

٥- خالد عبد الرحمن الفقي: الجرائم المعلوماتية وأثر المعلوماتية، في العالم الإسلامي، جامعة الملك عبد العزيز، ٢٠١٨، ص٧٧

٦- عادل محمد النعيمي: الجرائم المعلوماتية في القانون الإسلامي: دراسة فقهية مقارنة"، اطروحة دكتوراه ، جامعة ام القرى ، ٢٠١٣، ص١٢٢

٧- عادل يحيى – السياسة الجنائية في مواجهة الجريمة المعلوماتية ، دار النهضة العربية ، الطبعة الأولى، ٢٠١٤ ، ص٢٨

٨- عبد التواب معوض الشور بجي، علم العقاب – حقوق الزقازيق، ٢٠١٧ ، ص ١٥.

٩- عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت – دار الكتب القانونية ٢٠٠٥ ، ص ٣٥ ، د/ هشام محمد فريد رستم الجرائم المعلوماتية ، اصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي ، بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنت –كلية الشريعة والقانون بدولة الامارات ٢٠٠٥

١٠- العبد الله، مصطفى. "الجرائم الإلكترونية: التحديات والحلول". دار الفكر، ٢٠٠٩، ص ٣٥.

١١- فاطمة سعيد البدري: أثر الجرائم المعلوماتية على النظام القانوني: دراسة مقارنة بين الشريعة والقانون الوضعي"، جامعة القاهرة ، ٢٠١٦، ص٨٩

١٢- فهد لعتيبي، مفاهيم وتقنيات الأمن السيب راني في مؤسسات التعليم العالي السعودية (رسالة دكتوراه). جامعة الم، ٢٠١٨سعود، ٢٠٢٠.ص. ٧٨

١٣- محمود مصطفى حسن: الجرائم الإلكترونية: دراسة في إطار القانون الجنائي المصري، دار النشر: دار النهضة العربية،٢٠١٨ ، ٥٦

١٤- مصطفى عبد الفتاح: دور الأمن السيب راني في حماية المعلومات في المؤسسات الحكومية (رسالة دكتوراه). جامعة القاهرة، ٢٠٢١ص. ٤٥.

١٥- نجاتي سيد احمد سند – علم الاجرام والعقاب، حقوق الزقازيق، ٢٠٠٢ ، ص ٣٥؛ د/ عادل يحيى –مبادئ علم العقاب – الطبعة الأولى، دار النهضة العربية، ٢٠٠٥ ، ص ٤٦

١٦- هدى حامد قشقوش السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية ، ٢٠١٢م ، ص ١٠. خالد عايض آل حمدان الغامدي: الاختصاص القضائي في الجرائم الإلكترونية وفقًا للنظام السعودي، مجلة الفقه والقانون

ثانيا: المراجع الأجنبية

1- M. L. Ray; Cybercrime: Law and Practice, Oxford University Press, 2019,

2- Droit, J.-P. (2020). Les crimes informatiques: Enjeux et législation. Editions' Dalloz

3- Frénol, J.-P. (2019). Droit Pénal de l'Internet. Editions' L.G.D.J.

4- Fortin, M. (2021). La Cybercriminalité et le Droit Pénal. Editions' Dalloz

5- Wilkinson, S. (2018). Cyber security: Legal and Practical Approaches ,these Oxford University,

6- Caitlin Robertson; The Role of Cyber security in Protecting Critical Infrastructure, these, University of Cambridge

ثالثا : الأنظمة والقوانين

١- الأمر الملكي رقم (٥٥٧٧٥) بتاريخ ١/١٢/١٤٣٨ هـ القاضي بإنشاء هيئة باسم الهيئة الوطنية للأمن السيب راني، وصدر الأمر الملكي رقم (٦٨٠١) بتاريخ ١١/٠٢/١٤٣٩ هـ القاضي بالموافقة على تنظيمها – المعدّل بالأمر الملكي رقم (٧٠٥٣) بتاريخ ٢/٢/١٤٤٣ هـ – لتكون الهيئة الوطنية للأمن السيب راني الجهة المختصة بالأمن السيب راني في المملكة والمرجع الوطني في شؤونه، وتتمتع بالشخصية الاعتبارية العامة والاستقلال المالي والإداري، وترتبط بالملك

٢- قانون حماية البيانات الشخصية المصري رقم ١٥١ | ٢٠٢٠ | صدر بموجب القانون رقم ١٥١ لسنة ٢٠٢٠ ب

٣- المادة الثانية من نظام مكافحة جرائم المعلوماتية رقم ١٧

٤- المادة الثالثة من نظام مكافحة جرائم المعلوماتية رقم ١٧

٥- مجلس الوزراء السعودي: نظام مكافحة جرائم المعلوماتية نشر مجلس الوزراء، ٢٠٠٧، المادة ١

٦- المرسوم الملكي رقم (م/٨٢) لعام ٢٠١٨ الخاص بـ "نظام الأمن السيب راني"، الذي يهدف إلى تنظيم قطاع الأمن السيب راني في المملكة ويدعم تطوير البنية

التحتية الأمنية وحمايتها من المخاطر، كما صدرت اللائحة التنفيذية لنظام الأمن السيب راني، التي تحدد الإجراءات التفصيلية لمتابعة تنفيذ النظام وتطبيق السياسات الأمنية المتعلقة بالأمن السيب راني.

٧- نظام حماية البيانات الشخصية السعودي صدر بموجب المرسوم الملكي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩هـ، ٢٠٢١

٨- نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (م/١٧) بتاريخ ٨ ربيع الأول ١٤٢٨هـ، الموافق ٢٦ مارس ٢٠٠٧م

٩- نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية بمرسوم ملكي رقم (م/17)بتاريخ8/3/1428 هـ عام2007 ، وتم تعديله في عام2017.

رابعا: مواقع الكترونيه

1- https://www.mdpi.com/2673-6756/2/2/28

2- https://doi.org/10.1080/15614263.2018.1507888

3- https://www.mdpi.com/2673-6756/2/2/28

4- https://www.accessnow.org