

الجرائم الإلكترونية وأثرها على الأمن السيبراني في المملكة العربية السعودية
Cybercrimes and Their Impact on Cybersecurity in the Kingdom of Saudi Arabia

بحث مقدم ضمن متطلبات مقرر:
"RML002 دورة" أساليب البحث العلمي القانوني
Research Paper Submitted for the Course:
"Legal Scientific Research Methods (RML002)"

برنامج ماجستير القانون الرقمي – الفصل الدراسي الثاني ٢٠٢٥ م
Master's Program in Digital Law – Second Semester 2025

بدر عبدالله القحطاني: إعداد الطالب
Prepared by: Bader Abdullah Al-Qahtani

(Midocean University) جامعة ميدأوشن: الجامعة
كلية القانون الرقمي: الكلية
College of Digital Law – Midocean University

◆ الفصل الأول: الإطار العام للجريمة الإلكترونية والأمن السيبراني

Chapter One: The General Framework of Cybercrime and Cybersecurity

المبحث الأول: المفهوم القانوني للجريمة الإلكترونية وتمييزها عن الجرائم التقليدية

Section One: The Legal Concept of Cybercrime and Its Distinction from Traditional Crimes

تُعد الجريمة الإلكترونية من أبرز التحديات القانونية المستحدثة في القرن الحادي والعشرين، إذ تعتمد على التكنولوجيا كوسيلة وأداة لارتكاب الفعل الإجرامي. ويُقصد بها كل فعل غير مشروع يُرتكب باستخدام أنظمة الحاسب أو الشبكات أو المنصات الرقمية ويهدف إلى الإضرار بالبيانات أو الحصول غير المصرح به على المعلومات أو تعطيل الخدمات الإلكترونية.

Cybercrime is one of the most significant emerging legal challenges of the twenty-first century, as it relies on technology as both a medium and a tool for committing criminal acts. It is defined as any unlawful act committed through computer systems, networks, or digital platforms aimed at harming data, gaining unauthorized access to information, or disrupting electronic services.

وتتميز الجريمة الإلكترونية عن الجرائم التقليدية في أن مسرحها افتراضي، لا يرتبط بمكان محدد، وتُرتكب غالباً عن بُعد دون وجود مادي بين الجاني والمجني عليه. كما أن أدلتها رقمية تتطلب خبرة تقنية متقدمة لإثباتها أو تتبعها، مما يجعل إجراءات التحقيق والإثبات أكثر تعقيداً من الجرائم التقليدية.

Cybercrimes differ from traditional crimes in that their scene is virtual and not bound

by a specific geographic location. They are often committed remotely without any physical presence between the offender and the victim. The evidence in such crimes is digital and requires advanced technical expertise to identify and verify, making investigation and proof far more complex than in conventional crimes.

وقد حدد نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (م/١٧) لعام ١٤٢٨ هـ مجموعة من الأفعال التي تُعد جرائم معلوماتية، مثل الدخول غير المشروع إلى الأنظمة، أو التنصت على البيانات، أو إساءة استخدام الأجهزة التقنية، أو المساس بالحياة الخاصة عبر الشبكات.

The Saudi Anti-Cybercrime Law, issued by Royal Decree No. M/17 of 1428H, identifies a number of acts that constitute information crimes, such as unauthorized access to systems, interception of data, misuse of technical devices, or violating individuals' privacy through digital networks.

المبحث الثاني: مفهوم الأمن السيبراني وأهدافه في النظام السعودي

Section Two: The Concept of Cybersecurity and Its Objectives in the Saudi Legal System

يُعرف الأمن السيبراني بأنه مجموعة الإجراءات التقنية والتنظيمية والتشريعية الرامية إلى حماية الأنظمة الرقمية من الهجمات أو الاستخدامات غير المشروعة، وضمان سرية وسلامة وتوافر المعلومات. وقد أولت المملكة العربية السعودية اهتمامًا بالغًا بهذا المجال من خلال إنشاء الهيئة الوطنية للأمن السيبراني عام ٢٠١٧م لتكون الجهة المختصة بوضع السياسات الوطنية للأمن السيبراني.

Cybersecurity is defined as the set of technical, organizational, and legal measures aimed at protecting digital systems from attacks or unauthorized uses while ensuring the confidentiality, integrity, and availability of information. Saudi Arabia has given great attention to this field by establishing the National Cybersecurity Authority in 2017 as the body responsible for setting national cybersecurity policies.

تتمثل أهم أهداف الأمن السيبراني في المملكة في بناء بيئة رقمية آمنة تسهم في تحقيق التنمية الاقتصادية والاجتماعية، وتعزيز ثقة الأفراد والمؤسسات في الخدمات الإلكترونية الحكومية والخاصة، وتطوير القدرات الوطنية في مواجهة التهديدات السيبرانية.

The main objectives of cybersecurity in the Kingdom include building a secure digital environment that contributes to economic and social development, enhancing individuals' and institutions' trust in governmental and private electronic services, and developing national capabilities to confront cyber threats.

كما أصدرت الهيئة الاستراتيجية الوطنية للأمن السيبراني التي حددت خمسة محاور رئيسية: الحوكمة، والجاهزية، والمرونة، والتعاون، وتنمية القدرات. ويمثل ذلك نموذجًا متكاملًا لتفعيل الأمن السيبراني على المستويين الوطني والمؤسسي.

The Authority also issued the National Cybersecurity Strategy, which defines five main pillars: governance, preparedness, resilience, cooperation, and capacity building. This represents an integrated model for implementing cybersecurity at both national and institutional levels.

◆ الفصل الثاني: الإطار النظامي والمؤسسي للأمن السيبراني في المملكة العربية السعودية

Chapter Two: The Legal and Institutional Framework of Cybersecurity in the Kingdom of Saudi Arabia

المبحث الأول: نظام مكافحة جرائم المعلوماتية وتحليل نصوصه

Section One: The Anti-Cybercrime Law and Analysis of Its Provisions

صدر نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (م/١٧) وتاريخ ١٤٢٨/٣/٨هـ، ليكون الإطار التشريعي الأساسي لمكافحة الجرائم الإلكترونية في المملكة العربية السعودية. ويهدف النظام إلى تحقيق العدالة والأمن والمصلحة العامة من خلال تحديد الأفعال المجرّمة والعقوبات المقررة لكل منها.

The Anti-Cybercrime Law was issued under Royal Decree No. M/17 dated 8/3/1428H, serving as the primary legislative framework for combating cybercrimes in the Kingdom of Saudi Arabia. The law aims to promote justice, security, and public interest by defining criminalized acts and prescribing penalties for each.

من أبرز الجرائم التي تناولها النظام: الدخول غير المشروع إلى الأجهزة أو الشبكات، وإتلاف البيانات أو تعطيلها، والتجسس المعلوماتي، وانتهاك الخصوصية عبر إساءة استخدام الهواتف النقالة المزوّدة بالكاميرا، ونشر المواد الإباحية، أو التهديد والابتزاز الإلكتروني.

Among the main offenses covered by the law are unauthorized access to devices or networks, destruction or alteration of data, information espionage, privacy violations through the misuse of mobile phones with cameras, dissemination of pornographic materials, and online threats or blackmail.

وتتراوح العقوبات المقررة بين السجن من سنة إلى عشر سنوات، والغرامة التي تصل إلى خمسة ملايين ريال سعودي، بحسب جسامة الفعل الإجرامي. كما منح النظام للمحاكم سلطة تقديرية في تحديد العقوبة المناسبة.

The penalties range from one to ten years of imprisonment and fines of up to five million Saudi Riyals, depending on the severity of the criminal act. The law also grants courts discretionary power in determining appropriate penalties.

وقد أسهم هذا النظام في الحد من الجرائم الإلكترونية ورفع مستوى الوعي القانوني لدى المجتمع، لكنه ما يزال بحاجة إلى تطوير مستمر يتناسب مع تسارع التطورات التقنية وتنوع أساليب الهجمات السيبرانية.

This law has contributed to reducing cybercrimes and increasing legal awareness in society, yet it still requires continuous updates to keep pace with rapid technological advancements and evolving methods of cyberattacks.

المبحث الثاني: الهيئة الوطنية للأمن السيبراني ودورها التنظيمي والرقابي

Section Two: The National Cybersecurity Authority and Its Regulatory and Supervisory Role

تُعد الهيئة الوطنية للأمن السيبراني الجهة المختصة بوضع وتنفيذ السياسات والإستراتيجيات الوطنية للأمن السيبراني، وقد أنشئت بالأمر الملكي رقم (٦٨٠١) في ١١/٢/١٤٣٩ هـ، وترتبط مباشرة بخادم الحرمين الشريفين، مما يعكس أهمية الدور الذي تضطلع به.

The National Cybersecurity Authority (NCA) is the competent body responsible for formulating and implementing national cybersecurity policies and strategies. It was established by Royal Order No. (6801) dated 11/2/1439H and reports directly to the Custodian of the Two Holy Mosques, reflecting the high importance of its role.

تهدف الهيئة إلى حماية المصالح الحيوية للمملكة من الهجمات السيبرانية، وضمان استمرارية الخدمات الحكومية والاقتصادية الحساسة، وبناء قدرات وطنية متخصصة في مجال الأمن السيبراني.

The Authority aims to protect the Kingdom's vital interests from cyberattacks, ensure the continuity of critical governmental and economic services, and develop specialized national capabilities in the field of cybersecurity.

كما أطلقت الهيئة الإستراتيجية الوطنية للأمن السيبراني التي تضمنت محاور رئيسية مثل تعزيز الحوكمة، والتعاون، والاستجابة الفعالة للحوادث، والتدريب وبناء القدرات البشرية، وإصدار اللوائح التنفيذية التي تنظم أمن المعلومات في الجهات الحكومية والقطاع الخاص.

The NCA launched the National Cybersecurity Strategy, which includes key pillars such as strengthening governance, promoting cooperation, ensuring effective incident response, developing human capacity, and issuing executive regulations governing information security across public and private sectors.

يُضاف إلى ذلك دورها في تقييم جاهزية الجهات الحكومية عبر مبادرة “التصنيف الوطني للأمن السيبراني”، التي تهدف إلى رفع كفاءة المنظومات التقنية وتحفيز الالتزام بالمعايير الوطنية.

Additionally, the Authority plays a role in assessing governmental entities' readiness through the “National Cybersecurity Classification” initiative, which aims to improve technical systems' efficiency and promote adherence to national standards.

الفصل الثالث: التحديات والاتجاهات المستقبلية للأمن السيبراني في المملكة

Chapter Three: Challenges and Future Trends of Cybersecurity in the Kingdom

المبحث الأول: التحديات القانونية والتقنية التي تواجه الأمن السيبراني

Section One: Legal and Technical Challenges Facing Cybersecurity

من أبرز التحديات القانونية التي تواجه المملكة في هذا المجال هو سرعة تطور الجريمة الإلكترونية مقارنة بوتيرة تحديث التشريعات، إذ تظهر أنماط جديدة من الهجمات تتطلب نصوصاً قانونية مرنة تستجيب للتحوّل

التقني المستمر.

One of the main legal challenges facing the Kingdom in this field is the rapid evolution of cybercrime compared to the pace of legislative updates, as new forms of attacks emerge that require flexible legal provisions capable of adapting to ongoing technological transformations.

كذلك تواجه الجهات المختصة تحديات في توظيف الكوادر المتخصصة في الأمن السيبراني، ورفع مستوى الوعي المجتمعي حول مخاطر الجرائم الإلكترونية، إضافة إلى صعوبة التعاون الدولي في تتبع الجرائم التي تتجاوز الحدود الوطنية.

Authorities also face challenges in recruiting specialized cybersecurity personnel, raising public awareness of cybercrime risks, and achieving effective international cooperation in tracking crimes that transcend national borders.

أما على الصعيد التقني، فإن التطور المتسارع في مجالات الذكاء الاصطناعي، والحوسبة السحابية، وإنترنت الأشياء، يُنتج مخاطر جديدة تتطلب تحديث البنية التحتية الرقمية باستمرار وتطوير أنظمة الحماية.

On the technical side, rapid developments in artificial intelligence, cloud computing, and the Internet of Things create new risks that require continuous updates to digital infrastructure and the enhancement of protection systems.

المبحث الثاني: مقترحات تطوير الإطار القانوني والتقني

Section Two: Proposals for Developing the Legal and Technical Framework

أولاً، ضرورة تحديث نظام مكافحة جرائم المعلوماتية بحيث يشمل الجرائم الناشئة مثل الاختراقات المعتمدة على الذكاء الاصطناعي، والتزوير الإلكتروني في العملات الرقمية.

First, it is essential to update the Anti-Cybercrime Law to encompass emerging crimes such as AI-based hacking and digital currency fraud.

ثانياً، إنشاء منصة وطنية موحدة تجمع بين المشرعين والخبراء التقنيين لتطوير تشريعات مرنة تتكيف مع المتغيرات التقنية.

Second, a unified national platform should be established to bring together legislators and technical experts to develop adaptable legislation responsive to technological change.

ثالثاً، إدراج مقررات متخصصة في القانون السيبراني ضمن برامج التعليم العالي والقضائي لتأهيل كوادر قادرة على فهم التداخل بين التقنية والتشريع.

Third, specialized courses in cyber law should be integrated into higher education and judicial training programs to prepare professionals capable of understanding the intersection of technology and legislation.

رابعاً، تعزيز التعاون الدولي في مجال تبادل المعلومات وملاحقة الجرائم الإلكترونية العابرة للحدود، خاصة عبر الانضمام إلى الاتفاقيات الدولية كاتفاقية بودابست للأمن السيبراني.

Fourth, international cooperation should be strengthened in the exchange of information and the pursuit of transnational cybercrimes, particularly through participation in global agreements such as the Budapest Convention on Cybersecurity.

الخاتمة والنتائج والتوصيات

Conclusion, Findings, and Recommendations

خلصت الدراسة إلى أن المملكة العربية السعودية حققت إنجازات كبيرة في بناء إطار قانوني ومؤسسي للأمن السيبراني، إلا أن التحديات التقنية المتسارعة تستلزم تطوير تشريعات أكثر مرونة واستباقية. كما بينت أن التكامل بين القانون والتقنية هو المفتاح لتحقيق بيئة رقمية آمنة ومستدامة.

The study concludes that Saudi Arabia has achieved significant progress in establishing a legal and institutional framework for cybersecurity; however, the fast-paced technological developments necessitate more flexible and proactive legislation. It also revealed that the integration between law and technology is the key to achieving a secure and sustainable digital environment.

أهم النتائج:

- فعالية نظام مكافحة جرائم المعلوماتية في الحد من الجرائم الإلكترونية.
- دور الهيئة الوطنية للأمن السيبراني في تعزيز الحماية الرقمية.
- الحاجة إلى تطوير تشريعات جديدة لمواكبة الذكاء الاصطناعي.
- قصور التعاون الدولي في تتبع الجرائم العابرة للحدود.

Key Findings:

- The effectiveness of the Anti-Cybercrime Law in limiting cyber offenses.
- The significant role of the National Cybersecurity Authority in enhancing digital protection.
- The need for new legislation to address AI-driven crimes.
- Insufficient international cooperation in tracking cross-border crimes.

أبرز التوصيات:

- تطوير نظام مكافحة الجرائم المعلوماتية وتحديث لوائح التنفيذ.
- إدراج التعليم السيبراني ضمن المناهج القانونية والأمنية.
- إنشاء مجلس وطني مشترك بين الجهات القانونية والتقنية.
- تبني معايير دولية موحدة للأمن السيبراني.

Main Recommendations:

- Update the Anti-Cybercrime Law and its executive regulations.
- Incorporate cybersecurity education into legal and security curricula.
- Establish a national joint council between legal and technical authorities.
- Adopt unified international cybersecurity standards.

◆ قائمة المراجع | References

المراجع العربية:

- نظام مكافحة جرائم المعلوماتية، المرسوم الملكي رقم (م/١٧)، ١٤٢٨ هـ.
- نظام حماية البيانات الشخصية، ١٤٤٣ هـ.
- تنظيم الهيئة الوطنية للأمن السيبراني، ٢٠١٧ م.
- دار النشر القانونية، ٢٠٢١ م. الجرائم المعلوماتية في النظام السعودي. السيف، محمد.
- جامعة الملك سعود، التحول الرقمي والأمن السيبراني في المملكة العربية السعودية. الحربي، فهد. ٢٠٢٣ م.
- مجلة الدراسات. الأمن السيبراني في المملكة العربية السعودية: دراسة تحليلية. الجهني، أحمد. ٢٠٢٢ م.

English References:

- Saudi Anti-Cybercrime Law, Royal Decree No. M/17 (2007).
- National Cybersecurity Authority (2017). National Cybersecurity Strategy.
- Al-Seif, M. (2021). *Cybercrimes in the Saudi Legal System*. Legal Publishing House.
- Al-Harbi, F. (2023). *Digital Transformation and Cybersecurity in Saudi Arabia*. King Saud University.
- Al-Juhani, A. (2022). *Cybersecurity in the Kingdom of Saudi Arabia: An Analytical Study*. Journal of Legal Studies.