

Cybersecurity and Legal Liability of Digital Service Providers

قسم القانون الرقمي، كلية العلوم الإنسانية، جامعة ميدأوشن

الباحث المعتمد للمراسلة: ماجد اياد راشد الشبلي

ملخص

هدفت هذه الدراسة إلى تحليل الجوانب القانونية للأمن السيبراني وتأثيرها على مقدمي الخدمات الرقمية. نظراً للتطور السريع في التكنولوجيا واعتماد الأفراد والشركات على الخدمات الرقمية، أصبح الأمن السيبراني ضرورة حتمية لحماية البيانات والمعلومات من الاختراقات والانتهاكات. وتتناول هذه الدراسة الأطر القانونية والتشريعات المتعلقة بالأمن السيبراني والمسؤولية القانونية التي تقع على عاتق مقدمي الخدمات الرقمية في حال حدوث انتهاكات أو اختراقات أمنية.

واعتمدت هذه الدراسة المنهج التحليلي المقارن من خلال دراسة القوانين والتشريعات المحلية والدولية ذات الصلة، وتحليل القضايا القانونية المتعلقة بمسؤولية مقدمي الخدمات الرقمية.

وتوصلت الدراسة إلى مجموعة من النتائج التي تبرز أهمية وضع تشريعات واضحة ومحددة لضمان التزام مقدمي الخدمات الرقمية بالمعايير الأمنية المطلوبة. كما أوصت الدراسة بضرورة تعزيز التعاون بين الهيئات التشريعية والجهات الفاعلة في مجال الأمن السيبراني لتعزيز الحماية القانونية للأفراد والمؤسسات.

الكلمات الدالة: الأمن السيبراني، المسؤولية القانونية، مقدمو الخدمات الرقمية، التشريعات، الحماية القانونية.

Abstract

This study aims to analyze the legal aspects of cybersecurity and its impact on digital service providers. With the rapid advancement in technology and the increasing reliance on digital services by individuals and businesses, cybersecurity has become a necessity to protect data and information from breaches and violations. This study examines the legal frameworks and legislation related to cybersecurity and the legal liability of digital service providers in cases of security breaches or .violations

The study employs a comparative analytical approach by reviewing relevant local and international laws and analyzing legal cases related to .the liability of digital service providers

The study concludes with several findings highlighting the importance of establishing clear and specific legislation to ensure that digital service providers comply with the required security standards. The study also recommends strengthening cooperation between legislative bodies and cybersecurity stakeholders to enhance legal protection for individuals .and organizations

Keywords: Cybersecurity, Legal Liability, Digital Service Providers, Legislation, Legal Protection

تعد قضايا الأمن السيبراني من أبرز التحديات التي تواجه مقدمي الخدمات الرقمية في العصر الحديث، حيث تتزايد الهجمات السيبرانية التي تستهدف بيانات الأفراد والمؤسسات، مما يستدعي وضع أطر قانونية فعالة لضمان حماية هذه البيانات وتحديد المسؤوليات القانونية للمؤسسات التي تقدم الخدمات الرقمية.

مشكلة الدراسة:

ما هي الأطر القانونية التي تحكم مسؤولية مقدمي الخدمات الرقمية في حال تعرض البيانات لانتهاكات أمنية؟

أسئلة الدراسة:

1. ما هي التشريعات الحالية المتعلقة بالأمن السيبراني والمسؤولية القانونية لمقدمي الخدمات الرقمية؟
 2. ما هي التحديات القانونية التي تواجه مقدمي الخدمات الرقمية فيما يخص الأمن السيبراني؟
 3. كيف يمكن تعزيز الأطر القانونية لضمان أمن البيانات وحماية المستخدمين؟
-

أهداف الدراسة:

- تحليل التشريعات الحالية المتعلقة بالأمن السيبراني.
 - تحديد المسؤولية القانونية لمقدمي الخدمات الرقمية في حالة حدوث اختراقات أمنية.
 - اقتراح حلول قانونية لتعزيز الأمن السيبراني.
-

منهجية الدراسة:

تعتمد الدراسة على المنهج التحليلي المقارن، من خلال تحليل القوانين الدولية والمحلية المتعلقة بالأمن السيبراني، ودراسة حالات قضائية ذات صلة.

الخطوة البحثية:

المبحث الأول: الأطر القانونية للأمن السيبراني

● المطلب الأول: التشريعات الدولية المتعلقة بالأمن السيبراني.

○ الفرع الأول: قوانين الاتحاد الأوروبي.

○ الفرع الثاني: القوانين الأمريكية والآسيوية.

● المطلب الثاني: التشريعات المحلية والمسؤوليات القانونية.

○ الفرع الأول: قوانين الدول العربية.

○ الفرع الثاني: التحديات في تطبيق القوانين.

المبحث الثاني: المسؤولية القانونية لمقدمي الخدمات الرقمية

● المطلب الأول: الالتزامات القانونية لحماية البيانات.

○ الفرع الأول: مسؤولية الشركات عن حماية بيانات المستخدمين.

○ الفرع الثاني: تداعيات الإهمال الأمني.

● المطلب الثاني: الآليات القانونية لتعويض المتضررين.

○ الفرع الأول: العقوبات القانونية.

○ الفرع الثاني: التعويضات المدنية.

الخاتمة:

النتائج:

1. أهمية وجود تشريعات واضحة تلزم مقدمي الخدمات الرقمية بتطبيق معايير أمنية صارمة.
2. ضرورة التعاون بين الجهات التشريعية وخبراء الأمن السيبراني لتعزيز الأطر القانونية.
3. الحاجة إلى تعزيز آليات المراقبة والامتثال لضمان التزام مقدمي الخدمات الرقمية بأفضل الممارسات الأمنية.
4. أهمية توعية المستخدمين بحقوقهم فيما يتعلق بحماية بياناتهم الشخصية على المنصات الرقمية.

التوصيات:

1. تعزيز التشريعات الحالية بما يضمن حماية أكبر لبيانات المستخدمين.
2. إنشاء آليات فعالة لمراقبة تطبيق معايير الأمن السيبراني لدى مقدمي الخدمات الرقمية.
3. تشجيع مقدمي الخدمات الرقمية على تبني أحدث التقنيات الأمنية وتقليل المخاطر الناجمة عن الهجمات السيبرانية.
4. توفير دورات تدريبية مستمرة لموظفي الشركات الرقمية حول أفضل ممارسات الأمن السيبراني والتعامل مع التهديدات المحتملة.

قائمة المصادر والمراجع:

- القوانين والتشريعات الدولية والمحلية المتعلقة بالأمن السيبراني.
- دراسات وأبحاث أكاديمية في مجال المسؤولية القانونية لمقدمي الخدمات الرقمية.
- تقارير المؤسسات المعنية بحماية البيانات والأمن السيبراني.