Pakistan Journal of Criminology
Vol. 16, No. 01, January—March 2024 (489-504)

Criminal Protection of Digital Applications in the UAE Legislation: A Comparative Study

Ali Sultan Ali[1] & Raed S. A. Faqir[2]

Abstract

The study explores the UAE's legal framework for the protection of digital applications, examining their compatibility with criminal policy, judicial assessment, and government role. The investigation intricately examines the multifaceted aspects of this protection, including its inherent connection with criminal policy, the scope of judicial discretion regarding electronic evidence, and the pivotal role played by the UAE government in upholding these protective measures. It delineates, assesses practical application, and identifies enforcement entities. The study compares legal systems in Anglo-Saxon countries such as the UK and the USA, as well as in Latin countries such as France and Egypt. This study aims to endeavor to unearth nuanced findings and insightful observations and to strengthen measures to protect digital applications by studying technical aspects, legal implications, and criminal policy implications, and contributing to ongoing discourse on the protection of digital applications. Furthermore, it extends its scope beyond the mere technicalities, suggesting significant recommendations at the end, for the protection of digital applications with the legal spectrum.

Keywords: Digital applications, Criminal protection, Anglo-Saxon legal systems, Latin legal systems.

Introduction

In the 21st century, the United Arab Emirates (UAE) has a distinguished leadership in several areas including tourism and economic progress. Despite its developments and successes in these sectors, the UAE, like many other countries, has met substantial encounters posed by rapid technology. For example, the development of technology has probably presented challenges in handling cybersecurity, adapting to the shifting landscape of universal trade influenced by digital platforms, and confirming the steadiness of monetary foundations. The spectrum of these crimes "includes piracy devices, bank account breaches, and the execution of deepfakes. Given the importance of the UAE and the widespread use

[1] Master in Criminal Sciences, American University in the Emirates, Dubai, UAE. bosultoon@hotmail.com

[2] The author is an Associate Professor in Criminal Law, the College of Law, American University in the Emirates, United Arab Emirates. He serves as an associate professor in Criminal Law, Faculty of Law, Al-Balqa Applied University in Jordan. He can be reached at raed.faqir@aue.ae and r.faqir@bau.edu.jo, His ORCID ID: https://orcid.org/0000-0002-6102-0983

of computer technology across sectors, especially in the government, the enactment of legislative and criminal protection of computer software has become critical.

This study evaluates the current legal framework for safeguarding computer programs, focusing on digital application protection under UAE law. It examines its forms, relationship with criminal policy, judicial discretion in electronic evidence, and the challenge of balancing data privacy with investigative needs. Exploring conflicts between public interest and government data protection, it questions the applicability of existing laws to emerging technology-related offenses. Seeking to establish a simplified legal framework, the study collects pertinent data and adopts an analytical-legal approach to offer valuable recommendations for the legal and academic community.

This study examines cybercrimes like hacking and deepfake operations, emphasizing the need for legal safeguards for computer programs in the UAE due to extensive reliance on technology, especially in government. It aims to assess the legal framework for digital application protection, exploring its relationship with criminal policy, judicial discretion on electronic evidence, and the balance between data privacy and investigative requirements. The research aims to address conflicts between public interest and data protection laws, offering informed recommendations via an analytical-legal approach for the legal and academic community.

This research employs a doctrinal approach by using descriptive and detailed analysis to meticulously examine legal statutes from sources found in primary sources (statutes, regulations, and cases) regarding the criminal protection of digital applications, emphasizing their technical aspects, classifications, and legislative measures in the United Arab Emirates (UAE) alongside comparative analyses. Secondary sources, such as literary publications, official reports, legislative texts, scholarly journals, and online repositories, are utilized for comprehensive data gathering.

Literature Review

Downloadable digital apps serve various purposes and come with intellectual property rights and user obligations. Developers hold exclusive rights, and conflicts may result in legal actions for IP infringement or user violations. The internet-driven digital revolution is altering daily life, aiming for quality advancements aligned with competitive private sector standards, profoundly influencing public and private services, cultural and economic dynamics, social relationships, and the interaction between individuals and institutions (Nada, 2017).

Digital apps perform diverse tasks using the internet and cloud computing on devices, covering entertainment, e-commerce, and specialized services. Their development involves stages like idea conception, design, coding, testing, and launch, employing varied technologies for rich interfaces, data security, and the integration of AI, ML, and IoT. Legally, they encompass software used on electronic devices, such as email, editing tools like Photoshop, and accounting software (Abbas, 2020, p. 9). Smart apps utilizing AI, machine learning, and more have transformed human capabilities in work and education. These tech-driven programs accessible across devices and the internet have revolutionized communication, entertainment, finance, and other fields.

Electronic and smart apps serve diverse functions like communication, productivity, entertainment, and education using smart technology (Al-Zahrani, 2020; Ahmed, 2017). Social media apps transform global communication, but concerns exist regarding mental health and privacy (Al-Majid, 2020; Khalil, 2020). Productivity apps vary in features and usage, impacting task management and collaboration (Hussein, 2021). Gaming apps entertain but may raise concerns about addiction and productivity (El-Shaqaqawi, 2022; El-Shami, 2019). Educational apps revolutionize learning through interactive tools like Duolingo and flexible online courses (Rahim, 2020; Al-Hamdan, 2019). Health apps monitor fitness, mental health, and chronic diseases, promoting well-being (Ahmed, 2017; Ali, 2018). GPS navigation apps like Google Maps and Waze redefine travel experiences (Abdel, 2020; Ahmed, 2017). AI-driven smart apps reshape interactions in home control, healthcare, transportation, and education, enhancing efficiency and experiences (El-Shaqaqawi, 2022; Hussein, 2021). Fitness trackers, personalized shopping, and smart transportation apps streamline daily life and services (Khalil, 2019; Al- Zu'bi, 2019; Al-Shami, 2019).

Computer programs, such as word processors and gaming software, enhance productivity (El-Shaqaqawi, 2022). Operating systems manage hardware and user interaction across various types, including general-purpose, specialized, and embedded systems (Al-Shami, 2019). Productivity software like Microsoft Word and Excel aids in content creation and management (Ahmed, 2017). Software like Adobe Photoshop and Illustrator aids multimedia and graphic design, while antivirus and firewalls protect digital systems (Al-Zahrani, 2020; Al-Majid, 2020). Database apps range from relational (using SQL) to NoSQL for diverse data, with cloud databases offering scalability, reliability, and cost-efficiency (Al-Shami, 2019; Al-Majid, 2020).

Smart government apps utilize IoT, AI, and big data to enhance public services, facilitating citizen engagement and efficient urban planning through electronic government portals (Al-Ali, 2020). Smart city apps, driven by IoT and

AI, address urban challenges like traffic and waste management, creating more sustainable cities (Al-Shami, 2019). Digital identity systems provide secure online verification for e-government services (Al-Balushi, 2019). Public safety apps improve emergency response (Al-Balushi, 2019). Virtual collaboration tools enhance remote communication for officials and citizens (Saad Eddin, 2018).

In private enterprises, AI, ML, and data analytics optimize operations across sectors like healthcare, education, agriculture, manufacturing, and energy (Al-Hamadni, 2019; Hussein, 2021). CRM apps automate sales and customer service (Al-Ali, 2020). HRM apps manage recruitment and training (Al-Musnad, 2017). Financial management tools oversee accounting and compliance (Al-Saadi, 2021). Marketing automation enhances efficiency and customization in marketing tasks (Al-Majid, 2020).

Results and Discussions

The Concept of Digital Applications, Its Nature & Types

Digital apps are intellectual property protected by copyright, patents, and trade secret laws. Developers have exclusive rights and can enforce them against infringers for damages (Al-Faqi, 2019, p.80).

a. The Legal Nature of Digital Applications

The legal characterization of digital applications can be explicated through several theoretical perspectives:

- **Ownership Theory:** The ownership theory views digital applications as intellectual property. Developers hold exclusive control and distribution rights, while users have limited rights under terms of use. UAE's Copyright Law protects authors and rights holders for works including smart apps and computer programs within the country (UAE Federal Decree-Law No. 38 of 2021, Art. 2(2)).
- **Contract Theory:** This theory views digital app legality as a contractual agreement between developers and users, covering rights, duties, licensing, and warranties. The UAE's Civil Transactions Law (Article 126) allows contracts for various purposes. Article 141 emphasizes that agreements are formed upon an essential term agreement, with dispute resolution based on legal provisions and transaction nature.
- **Agency Theory:** The agency theory views developers as agents for users, committed to user needs and potential liability for app-related harm. UAE's Civil Transactions Law, Art. 924, defines agency as a contract where one acts on behalf of another lawfully, aligning with this theory in the developer-user relationship.
- **Damage Theory:** The tort theory holds developers accountable for app-related damages regardless of a contract. They're liable for harm caused by negligence. The UAE's Civil Transactions Law No. (1) of 1987, Arts. 282 and

289, specifies that wrongdoers must compensate for damages, with judges deciding the compensation if is not defined by law or contract.

- **Hybrid Theory:** Scholars suggest a hybrid legal perspective on digital apps, merging intellectual property, contracts, and agency theories (Abdelghani, 2020, p. 14). According to the UAE's Civil Transactions Law No (1) of 1987, Art. 924 defines an agency as one person acting on behalf of another within legal limits. In digital apps, developers can act as agents for users, operating specific app functions based on users' granted authority. This framework establishes rights and obligations between developers and users.

In the UAE, the application of these theories depends on the legal framework and regulations in place. Article 2(2) of UAE Federal Decree-Law No. 38 of 2021 enforces strict liability, mandating compensation for harm, irrespective of fault. This applies to app developers, holding them responsible for damage, even if unintended. Additionally, Article 126 of the UAE's Civil Transactions Law highlights the importance of contracts, including digital app agreements. These agreements outline rights, obligations, and dispute resolution, ensuring legal clarity and protection for all app users and developers.

b. The Technical Nature of Digital Applications

Technical aspects of digital apps encompass software engineering, user interface design, security, privacy, performance, and legal compliance, influencing functionality, user experience, and safety.

- **Software Structure:** defines functions, scalability, and maintenance (Al-Samaan, 2019, p. 24). It involves programming languages, frameworks, and databases for adaptability (Ayoub, 2020, p. 8).
- User Interface Design: Crucial for intuitive, visually appealing interaction across devices.
- **Security and Privacy:** Priority is safeguarding against hacking using encryption, access controls, and clear privacy policies (Al-Salami, 2017, p. 69).
- **Performance and Optimization:** Essential for speed, responsiveness, and efficient data management (Al-Qarni, 2018, p. 101).
- **Compatibility and Interoperability:** Ensures smooth operation across devices and services, adhering to standards and integrating with various platforms (Al-khafif, 2017, p. 5).

Digital apps utilize computer technology and software for development. They incorporate user-friendly designs with visuals and audio, employing AI and machine learning for enhanced performance, data analysis, recommendations, and process optimization.

c. Types of Digital Applications

Digital apps, cited as transformative by Ali (2018, p. 10), serve diverse functions from communication to productivity, permeating vital sectors like healthcare, education, finance, and e-commerce (Al-Musnad, 2017, p. 45), fundamentally altering our tech interaction, lifestyle and work dynamics, and presenting business opportunities (Al-Zu'bi, 2019, p. 31). As technology progresses, its significance in shaping the future intensifies.

There are many types of digital applications, which can be categorized as follows:

- **Electronic and Smart Apps:** Digital apps, made for devices like smartphones and computers, use the internet and cloud computing to perform tasks in different fields. They're created through stages: concept, design, coding, testing, and deployment. They constantly integrate AI and IoT to enhance user experiences (Al-Ali, 2020, p. 126; Al-Shami, 2019, p. 128; Al-Balushi, 2019, p. 108).

Electronic and smart apps offer various functions, such as communication, productivity, entertainment, and education. Social media apps revolutionize global communication, while productivity apps impact task management and collaboration. Gaming apps offer entertainment but raise addiction concerns (Hussein, 2021, p.109; Khalil, 2019, p. 20; Al- Zu'bi , 2019, p. 33; Al-Shami, 2019, p.117). Educational apps revolutionize learning, health apps monitr fitness, and GPS navigation apps redefine travel experiences. AI-driven smart apps enhance efficiency and experiences in home control, healthcare, transportation, and education (Al-Zahrani, 2020, p. 57; Ahmed, 2017, p. 85; Al-Majid, 2020, p. 16; Khalil, 2020, p.16; Hussein, 2021, p. 99; El-Shaqaqawi, 2022, p. 65; El-Shami, 2019, p.113; Rahim, 2020, p. 99; Al-Hamdan, 2019, p. 74; Abdel, 2020, p. 110; Ahmed, 2017, p. 89).

- **Computer Software and Databases:** Computer programs enhance productivity, while operating systems manage hardware and user interaction. Content creation and management software like Microsoft Word and Excel aid in multimedia design (Al-Zahrani, 2020, p. 59; Al-Majid, 2020, p. 22; Faqir & Alrousan, 2023). Antiviruses and firewalls protect digital systems. Database apps range from relational to NoSQL for diverse data (Al-Shami, 2019, p.119; Al-Majid, 2020, p. 23).
- **Government and Private Smart Apps:** Smart government apps use IoT, AI, and big data to improve public services, citizen engagement, and urban planning. These apps address urban challenges like traffic and waste management, creating sustainable cities (Al-Musnad, 2017, p. 69). Digital identity systems provide secure online verification, while public safety apps improve emergency response (Al-Hamdani, 2019; p. 186; Hussein, 2021, p.141; Al-Saadi, 2021, p.

144; Al-Majid, 2020, p. 28; Al-Ali, 2020, p.126; Al-Shami, 2019, p.128; Al-Balushi, 2019, p.108).

The Criminal Protection of Digital Applications in UAE

Legal protection for digital applications encompasses intellectual property, data privacy, and cybersecurity laws. Copyrights, trademarks, and patents protect creators, while data privacy and cybersecurity regulations ensure user security, forming a comprehensive legal framework.

a. Federal Law on Crimes and Penalties

The UAE's Federal Law on Crimes and Penalties, as highlighted by Hajji (2016, p. 99), safeguards applications by criminalizing digital offenses and outlining penalties for perpetrators (Al-Obeid, 2016, p. 25; Alrousan & Faqir, 2023). This includes scrutiny of Penal Code articles specifying penalties for crimes involving digital applications:

- **Offense of Assaulting Defense Secrets:** Unauthorized access to defense secrets through information technology is a grave offense punishable by imprisonment, fines, and the potential loss of security clearance or citizenship. Governments deploy security measures like firewalls and encryption to protect these secrets, ensuring national security and citizen safety (Al-Suwaidi, 2019, p. 26). Federal Law No. 31 of 2021, Art. 168 (3), orders life imprisonment for sharing state defense secrets online. It highlights the severity of the crime and stresses the importance of vigilance and severe penalties to deter offenders and protect national security (Hassan, 2015, p. 38).
- **Offense of Insulting a Foreign State:** The rise in illegal activities through digital apps in foreign domains, aided by social media and online platforms, is a growing concern. Anonymity complicates law enforcement efforts and strains international diplomatic relations (Sowilem, 2020, p. 51). UAE's Federal Law No. 31 of 2021, Art. 174, imposes strict penalties for actions against foreign states. It includes life imprisonment for damaging political relations or risking UAE interests. Committing such actions, even digitally, carries a minimum five-year prison term and a fine of AED 100,000. This article showcases the UAE's commitment to diplomacy, security, and deterring activities that could threaten relations or national security.
- **Offense of Endangering Security or Order:** Digital apps pose security threats by swiftly spreading misinformation. Governments seek stricter laws and penalties to counter these offenses (Salleh, 2020, p. 21). UAE Federal Law No. 31 of 2021, Art. 215 targets individuals using communication or IT to disseminate information endangering national security or public order. It aims to safeguard

these interests by imposing temporary imprisonment, discouraging harmful actions, and ensuring stability (Faqir, 2023).

Stringent laws and penalties are vital to combat app-enabled crimes effectively. Raising awareness, global cooperation, advancing security technology, monitoring, and collaborating with social media platforms are key solutions to tackling internet crimes threatening national security and public order.

b. Anti-Rumor and Cybercrime Law

UAE's Decree-Law No. 34 of 2021 pioneers regional legislation against information technology-related crime, protecting digital applications, including social media and messaging apps (Amin and Al-Ghoul, 2019, p. 59). Similar laws in various countries hold digital platforms accountable for harmful content (Al-Kaswani, 2018, p. 75). The UAE's Combating Rumors and Cybercrimes Law, introduced in January 2022, tackles evolving cybercrime challenges, emphasizing cybersecurity and awareness.

- **General Issues:** Art. 1 of UAE Federal Decree-Law No. 34 of 2021 defines 'information technology' as covering electronic systems, software, websites, networks, and data handling means. This encompasses various digital applications like software, websites, mobile apps, social media, and cloud computing (Al-Balqasi, 2019, p. 26). To tackle the cyber aspect, emphasis on digital literacy, cybersecurity awareness, responsible use, and ongoing system and data security investment is crucial (Mahmoud, 2018, p. 99). This article forms the basis for legislating against cybercrimes in digital apps, ensuring a comprehensive system to protect digital systems today.
- **Offense of Cybersecurity Breach:** Digital application hacking involves unauthorized access, leading to financial losses, reputation damage, and legal consequences (Radi & Issa, 2017, p. 105). Governments enforce laws with penalties, and organizations prioritize cybersecurity measures like firewalls and encryption to protect digital systems and public trust (Al-Na'imi, 2018, p. 269). UAE Federal Decree-Law No. 34 of 2021 on Cybercrimes stipulates penalties, including fines from AED 100,000 to AED 300,000, and imprisonment, escalating to at least one year in prison and fines between AED 200,000 and AED 500,000 for unlawful breaches. Its purpose is to deter electronic crimes with strict penalties.

c. The Copyright Law

Copyright is vital in our tech-centric world, giving creators legal ownership of their work and defining public transmission. Protecting digital apps hinges on copyright adherence, granting creators exclusive rights and legal recourse for

infringement (Salfeety, 2012, p. 1). Author's rights in digital apps safeguard creativity, offering creators exclusive control and benefits.

- **Protecting Author Rights in Digital Applications:** Author rights in digital apps involve copyright, licensing, DRM, legal enforcement, and international treaties, providing avenues for updates and open-source initiatives. These rights, governed by intellectual property laws, aim to foster creativity. Copyright laws delineate temporary financial rights and permanent moral rights, balancing an individual's personality and the work's scope (Salah Al-din, 2019, p. 40). In digital apps, financial rights grant creator's temporary exclusivity to profit from their work. UAE law, specified in Article 20 of Federal Decree-Law No. 38 of 2021 on Copyright and Related Rights, outlines the duration of protection, including the author's lifetime plus 50 years after death, among other durations for different works.
- **Legal Protection of Digital Content:** Securing digital content entails legal protections like copyright, patents, trademarks, trade secrets, licensing agreements, and DRM, aiming to prevent unauthorized copying or distribution (Cheigui, 2014, P. 14). Cybersecurity and data protection laws are critical for safeguarding digital assets and user data (Al-Zoghbi, 2003, p. 41). Digital production, involving music, software, and media creation, presents global opportunities but faces piracy challenges. Strategies encompass DRM, copyright laws, and public awareness campaigns to protect digital assets. A comprehensive approach integrating technical, legal, and social measures is crucial to safeguarding digital apps and ensuring fair compensation for creators.

d. Industrial Property Protection Law

Article 2 of the UAE's Federal Law on Industrial Property Rights No. 11 of 2021 aims to balance innovation and community benefit by protecting creators' rights, including patents, trademarks, and designs, promoting innovation, ensuring secrecy, and combating infringement within a legal framework (Saidi, 2017, p. 62; Al-Mousawi, 2019, p. 98; El-Houry, 2017, p. 52; Taher, 2019, p. 22; Mazen, 2019, p. 13). This law also ensures global compliance, encourages innovation, attracts digital investments, penalizes false information in patent applications, criminalizes counterfeiting and piracy, and empowers judicial disclosure to deter infringement (Article 3, Federal Law No. 11 of 2021; Article 69, Article 70).

e. Commercial Property Law

Commercial property, governed by Federal Decree-Law No. 36 of 2021 in the UAE (Nihay, 2019, p. 40; Bataikh, 2022, p. 89; Ali Allah, 2023, P. 89; Wardi, 2022, p. 16), defines trademarks as distinctive symbols used to identify goods or

services, serving consumer choice, market integrity, and economic growth (Ali Allah, 2023, P. 89). Protection of trademarks is crucial due to their connection to app value, which are requires civil and criminal safeguards against infringements, with strict penalties outlined in Art. 49 and 50 of Federal Decree-Law No. 36 of 2021, including imprisonment, fines, and seizure of infringing items (Wardi, 2022, p. 16; Bataikh, 2022, p. 89). Moreover, recidivist offenders face intensified penalties to deter trademark violations, including those related to digital apps (Article 51).

Criminal Protection for Digital Applications in Comparative Legislation

a. Criminal Protection in Anglo-Saxon Countries

The UK's Computer Misuse Act 1990 tackles hacking, while the Data Protection Act 1998 safeguards privacy; similarly, the US laws—such as ECPA, ITADA, and CFAA—protect online communication, target identity theft, and criminalize unauthorized access (Al-Namr, 2017, p. 19; Al-Saeed, 2015, p. 86). These laws combat various cybercrimes like hacking, fraud, identity theft, espionage, and privacy breaches, ensuring online security (Goodrich, 2010, p. 318).

Latin countries like France and Egypt are fortifying legal defenses for digital applications to protect individual rights and counter cybercrimes, with France amending the Data Protection Act in 2018 and Egypt enacting the Electronic Crimes and Personal Data Protection Law in the same year (Ahmed, 2019, p. 108; Al-Qahtani, 2019, p. 108). These changes aim to enhance digital security against hacking and privacy breaches while balancing individual freedoms (Clarke, 2010, p. 78). In contrast, Anglo-Saxon countries focus on objective criminal laws tailored to the unique nature of digital applications, addressing challenges like cyber piracy, fraud, and identity theft, and serving as models for other nations (Al-Mansour, 2020, p. 23; Clough, 2019, p. 91). The UAE has updated its laws to protect digital applications by defining electronic crimes, imposing penalties, and strengthening its judicial framework (Garay, 2020, p. 236). Both the UAE and Anglo-Saxon countries are aligning their legal frameworks to combat advanced cybercrimes in the digital landscape.

Anglo-Saxon laws excel at defining cybercrimes, imposing strict penalties, and adapting to evolving technology, fostering global cooperation (David, 2018, p. 104). In contrast, Latin laws lag in adapting to digital security challenges. The UAE updated its legislation to safeguard digital apps, defining cybercrimes and penalties, but further updates are needed to match rapid tech changes (Al-Mansour, 2017, p. 23). The UAE and Anglo-Saxon nations strive to enhance digital protection against evolving cyber threats. Effective criminal protection in Anglo-Saxon countries involves adapting laws to technological

advancements, employing strong penalties as deterrents, fostering public-private collaboration, and engaging in global cooperation (Holt & Bossler, 2017, p. 51; Balkin, 2013, p. 54). Local training and awareness efforts are crucial for upholding digital security (Kerr, 2012, p. 205).

b. **Criminal Protection of Digital Applications in Latin Legal Systems Countries**

France's LCEN of 2004 establishes a robust legal framework shielding digital applications from cybercrimes (Shahri, 2016, p. 92), regulating digital activities, including data protection, and service provider obligations, and enhancing trust in digital tech for online security (Jaishankar, 2018, p. 18). The law highlights user data protection responsibilities for digital service providers, although concerns persist about surveillance and civil liberties (Al-Juhani, 2016, p. 170). The LCEN also promotes innovation and digital growth by exempting providers from content liability under specific conditions, aiming to foster innovation, create a conducive digital environment, and support economic expansion (Arts. 6, 7, 12, and 5 of Law No. 2004-575). It offers a comprehensive framework, empowering law enforcement units to combat cybercrimes and emphasizing the need for balance between cybersecurity and privacy (Shahri, 2016, p. 93; Al-Namr, 2017, p.27; Ahmed, 2017, p. 22).

Criminal protection for digital apps differs notably between Anglo-Saxon nations and Latin legal system countries like France and Egypt (Khedr, 2017, p. 224). While Latin law countries lack direct provisions for cybercrimes, specialized legislation in these regions, such as France and Egypt, addresses electronic fraud and data protection in alignment with GDPR. The absence of specific frameworks creates ambiguity, impacting risk assessment and cross-border cooperation, necessitating bridging this regulatory gap for robust digital app protection and enhanced global collaboration against cybercrime (Ahmed, 2017, p. 23).

Conclusion

Ever-evolving digital applications, prevalent in today's world, fall under intellectual property laws like copyrights and patents. Developers wield exclusive control, imposing usage terms and potential payment obligations on users, which can lead to disputes over infringement or violations, blending legal and technological complexities in this realm.

The study delves into various aspects of digital application development, law enforcement challenges, and the UAE's legal framework, highlighting the need for stricter laws against criminal application use, copyright protection, industrial property rights, and the significance of trademarks within digital apps. It

emphasizes the UAE's industrial property law that promotes innovation, safeguards patents (Federal Law No. 11 of 2021, Article 69), and governs trademarks under Federal Decree-Law No. 36 of 2021. However, it notes the need for stronger laws for collective digital works, employing encryption for protection. Globally, countries are establishing diverse legal frameworks to combat cybercrimes against digital apps, with Anglo-Saxon countries emphasizing collaboration between law enforcement and the private sector.

Latin legal system countries lack specific laws for digital applications, leading to increased cybercrime and an urgent need for cybersecurity measures. The French Digital Economy Fund Law raises user safety and innovation, while Egypt emphasizes the enforcement of cybercrime laws and strives to balance security measures with civil liberties. The need for diverse digital protection strategies becomes clear. Anglo-Saxon states prioritize criminalization, while Latin countries implement a broader regularity policy to complement security measures with individual freedoms. Latin legal frameworks aim for a comprehensive right, while Anglo-Saxon perspectives often focus on the specific criminal protection of digital applications, raising concerns about individual rights.

Recommendation

Based on the research's findings, the following recommendations are made:

- To strengthen the legal protection of digital applications through new legislation or updates to combat various types of attacks.
- To strengthen cooperation among various parties, including government agencies, corporations, and individuals, for promoting cybersecurity awareness, education, and practical measures.
- To establish a central authority for protecting digital applications.
- To propose significant legal penalties for offenses related to digital applications to deter criminals and ensure justice for victims.
- To make sure that legislation on the protection of digital applications is regularly reviewed and updated to effectively address evolving threats.
- To develop a comprehensive strategy for cybersecurity that integrates guidelines, stakeholder coordination, and awareness-raising campaigns.
- To inspire innovation for protecting digital applications through research and initiatives.

References

Abbas, A. (2020). *Information Technology Crimes and Intellectual Property Rights*. Beirut: Arab Institute for Sciences and Culture.

Abdel, R. A. (2020). *Virtual Reality and Augmented Reality Applications.* Beirut: Dar Al-Ma'rifah Al-Jadida.

Abdelghani, S. (2020). *Information Technology and Programming Principles - Analysis and Design of Information Systems, Building the Theory of Accounting Databases, a Guide with Terminology Used in the Field of Data Processing.* Cairo: Modern Book House.

Ahmed, I. (2019). *Protecting Digital Applications from Cybercrimes*. Cairo: Dar Al-Farabi.

Ahmed, M. H. (2017). *Digital Applications and New Media*. Riyadh: Dar Al-Farabi.

Al- Zu'bi, K. M. (2019). *Information Technology and Communications Technology and Their Applications.* Amman: Dar Al-Farjani.

Al-Ali, A. (2020). *Electronic Applications and Web Technologies*. Beirut: Dar Al-Kutub Al-Ilmiyah.

Al-Balqasi, M. (2019). *Networks and Information Security*. Cairo: University Education House.

Al-Balushi, F. (2019). *Artificial Intelligence Applications in Human Resources.* Dubai: Dar Al-Yaqeen.

Al-Faqi, A. F. (2019). *Objective Criminal Protection of Electronic Banking Operations - A Comparative Study.* Cairo: Dar Misr for Publishing and Distribution.

Al-Hamdan, A. B. A. (2019). *Electronic Applications: Design and Development.* Riyadh: Dar Al-Manhal.

Ali Allah, M. H. (2023). *Information Competition Between the United States of America and China - A Study in Cybersecurity*. Amman: Amjad Publishing and Distribution House.

Ali, A. M. (2018). *Web and Smart Devices Applications*. Cairo: Dar Al-Arabi Publishing.

Al-Juhani, A. (2016). *Criminal Protection of Digital Applications in Comparative Law.* Alexandria: Dar Al-Wafa for Publishing and Distribution.

Al-Kaswani, M. K. (2018). *Information Technology and E-Learning*. Amman: Innovation Publishing and Distribution House.

Al-khafif, I. A. (2017). *E-Learning. Beirut: Arab Community Library for Publishing and Distribution*, Dar Al-I'ssar Scientific Publishing and Distribution.

Al-Majid, F. (2020). *Artificial Intelligence and Machine Learning Applications*. Dubai: Dar Al-Hadara.

Al-Mansour, K. (2020). *Criminal Protection of Digital Applications in Jordanian Law.* Amman: Dar Al-Thaqafah Al-Jadeeda.

Al-Mousawi, W. A. (2019). *Encyclopedia of Artificial Intelligence*. Amman: Dar Al-Ayyam for Publishing and Distribution.

Al-Musnad, S. (2017). *Computer Applications and Modern Software*. Riyadh: Dar Al-Fikr Al-Arabi.

Al-Na'imi, M. T. W. (2018). *Information Forgery as a Form of Cybercrime.* Beirut: Aleppo Legal Publications.

Al-Namr, F. (2017). *Cybercrimes in Saudi Arabian Law.* Riyadh: Wisdom Publishing House.

Al-Obeid, F. B. N. (2016). *Smart Government - Practical Application of Government Electronic Transactions.* Riyadh: Al-Obeikan Library.

Al-Qahtani, N. (2019). *Digital Transformation and Computer Crimes in Saudi Law*. Amman: Wael Publishing House.

Al-Qarni, N. b. M. (2018). *Enhancing Self-Control for Children in the Era of Smart Devices.* Riyadh: Delail Center.

Alrousan, Ehab & Faqir, Raed S A. (2023). The Evolution of Anticipatory Policing in the United Arab Emirates: Proactive Crime Prevention & Technology, *Pakistan Journal of Criminology,* 15 (4), 311-329.

Al-Saadi, M. A. (2021). *Computer Applications in Libraries and Information Science*. Cairo: Dar Al-Maaref.

Al-Saadi, M. A. (2021). *Computer Applications in Libraries and Information Science*. Cairo: Dar Al-Ma'arif.

Al-Salami, A. A. R. (2017*). Information Technology*. Amman: Dar Al-Manahij for Publishing and Distribution.

Al-Samaan, A. H. (2019). *Writing for Multimedia and Integrated Newsrooms.* Cairo: The Egyptian-Lebanese House.

Al-Shami, M. (2019). *Computer Applications in Accounting and Finance*. Beirut: Dar Al-Ma'arif Al-Jadeeda.

Al-Suwaidi, A. S. (2019). *Criminal and Security Confrontation of Crimes Endangering Internal State Security* (Master's Thesis). Dubai: Dubai Police Academy.

Al-Zahrani, H. (2020). *Digital Applications and Social Networks*. Beirut: Dar Al-Kutub Al-Ilmiyah.

Al-Zoghbi, M. A. F. (2003). *Legal Protection of Databases According to Copyright Law.* Alexandria: Ma'arif Establishment.

Amin, A. S., & Al-Ghoul, R. M. (2019). *Multimedia Production*. Cairo: Sahab Publishing and Distribution House.

Ayoub, M. (2020). *E-Government Plans and Strategies*. Beirut: Al-Waraq Publishing and Distribution.

Balkin, J. (2013). *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*. Yale University Press.

Bataikh, A. (2022). *Legal Regulation of Smart Applications*. Dubai: Scientific Renaissance for Publishing and Distribution.

Cheigui, N. (2014). *Intellectual Property Rights, Copyright, Neighboring Rights, Industrial Property Rights.* Algeria: Dar Belqiss.

Clarke, N. J. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* Ecco.

Clough, J., & Mann, M. (2019). *The Routledge Handbook of Technology, Crime, and Justice*. Routledge.

David, S. W. (2018). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

El-Shaqaqawi, A. (2022). *Computer Applications in Business Management.* Beirut: Dar Al-Ilm Lil-Malayin.

El-Shoury, A. (2017). *Internet and Multimedia Applications: Multimedia, Internet, Email, and Communications.* Cairo: Dar Al-Talim Al-Jame'i.

Faqir, Raed S A & Alrousan, Ehab. (2023). Reimagining Criminology: The Transformative Power of the Postmodern Paradigm, *Pakistan Journal of Criminology,* 15 (3), 151-170.

Faqir, Raed S A. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview, *International Journal of Cyber Criminology*, 17 (2), 77-94.

Garay, J. (2020). *Cybercrime in the Greater Maghreb: Towards Effective Cooperation and Regional Solutions*. Springer.

Hajji, A. I. (2016). *Integrated E-Government and Smart Cities and Their Governance in the Face of Fourth and Post-Fourth Generation Wars.* Cairo: A-'Alam Al-Kutub.

Hassan, O. S. (2015). The UAE Legislator's Policy for Combating Cybercrimes. *Al-Fikr Al-Sharati Journal,* Police Research Center, Sharjah, Issue 95, October.

Holt, T. J., & Bossler, A. M. (Eds.). (2017). *Cybercrime: Theoretical Perspectives on Internet Crimes*. Routledge.

Hussein, J. (2021). *Artificial Intelligence and Machine Learning Applications in Industry*. Dubai: Dar Al-Rawafid.

Jaishankar, K. (2018). *Global Criminology: Crime and Victimization in a Globalized Era*. CRC Press.

Kerr, O. S. (2012). *Cybercrime: Digital Cops in a Networked Environment*. Oxford University Press.

Khalil, M. H. (2019). *Computer Applications in Health and Medicine*. Cairo: Dar Al-Hikmah.

Khalil, M. H. (2019). *Computer Applications in Health and Medicine*. Cairo: Dar Al-Hikma.

Khedr, E. E. (2017). *Electronic Crimes in Egyptian Law.* Cairo: Arab Renaissance Publishing House.

Mahmoud, K. M. (2018). *The Suitability of Computer Information Systems in Financial Institutions for Information Security Standards*. Beirut: Arab Organization for Administrative Development.

Mazen, H. M. (2019). *E-Learning Technology: Concept, Educational Application.* Cairo: Al-Asriya Library.

Nada, A. (2017). Smartphone Applications in Archives, A Descriptive and Analytical Study. *Arab Journal of Archives*, Documentation, and Information, Issue 41-42.

Nihay, S. (2019). *E-Learning Technology and Training: Strategies, Tools, Applications.* Beirut: Dar Al-Sahab for Publishing and Distribution.

Radi, S., & Issa, R. (2017). *Networks and Information Security: The World Wide Web - Types of Communication Networks - Hacking*. Cairo: University Education House.

Rahim, A. A. (2020). *Virtual Reality and Augmented Reality Applications*. Beirut: Dar Al-Ma'rifah Al-Jadidah.

Saad Eddin, N. (2018). *Computer Applications in Administrative and Economic Sciences*. Cairo: Dar Al-Arabi for Publishing.

Saidi, S. (2017). *Information Security and Systems in the Digital Age*. Alexandria: Dar Al-Fikr Al-Jame'i.

Salah Al-din, A. (2019). *E-Learning Technology and Training: Strategies, Tools, Applications*. Beirut: Dar Al-Sahab for Publishing and Distribution.

Salfeety, Z. A. A. (2012). *Legal Protection of the Author's Right in Palestine - A Comparative Study* (Master's Thesis, An-Najah National University).

Salleh, I. A. D. M. (2020). *Economics of Information Technology*. Cairo: University Thought House.

Shahri, S. A. (2016). *Criminal Protection of Digital Applications in Comparative Law*. Beirut: Dar Al-Ma'arifa.

Sowilem, M. A. (2020). *Criminal Evidence through Electronic Means*. Alexandria: University Press.

Taher, D. J. (2019). *Electronic Communication Technology and the Challenges of Chang*e. Cairo: Egyptian General Authority for Books.

Wardi, Z. H. (2022). *Information Sources and Beneficiary Services in Information Institutions*. Amman: Al-Waraq Publishing and Distribution Foundation.