موسوعة الجرائم الإلكترونية والعدالة السيبرانية: دراسة تحليلية مقارنة في ضوء التشريعات الدولية والفقه القضائي الحديث

تأليف: د. محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني بالحكومة المصرية

المحاضر الدولي في القانون

إهداء

إلى ابنتي الغالية صبرينال، نور عيني وسرّ تميزي،

وإلى رجال القضاء والمحاماة الذين يدافعون عن

العدالة دون هوادة،

وإلى كل قاضٍ رفض أن يُجرّم موظفًا لمجرد خطأ إداري،

وإلى كل ضابط قضائي آثر القانون على الأوامر،

وإلى كل محامٍ دافع عن حقّ لا يُرى إلا بعين الضمير.

تقديم

في عالمٍ لم يعد فيه الجاني بحاجة إلى سكين أو مسدس، بل إلى لوحة مفاتيح واتصال إنترنت، باتت الجريمة تتخذ أشكالًا جديدة تتطلب إعادة صياغة شاملة لمفاهيم المسؤولية الجنائية، الركن المعنوي، والركن المادي. لم تعد الجريمة تُرتكب في زقاق مظلم، بل في خوادم موزعة

عبر ثلاث قارات، وتُدار بواسطة خوارزميات تتعلم من أخطائها.

هذا العمل الموحّد للمجلدين الأول والثاني من "موسوعة الجرائم الإلكترونية والعدالة السيبرانية" يُقدّم أساسًا نظريًا وتطبيقيًا متينًا لفهم هذا التحوّل الجذري. وهو لا يكتفي بسرد النصوص التشريعية، بل يغوص في أعماق الأحكام القضائية الواقعية، والتحديات العملية التي تواجه المحققين، النيابة، والقضاة في مواجهة جرائم تتجاوز الحدود الوطنية، وتتحدى مفاهيم الزمان والمكان.

وقد استندتُ في هذا العمل إلى:

- قانون مكافحة الجرائم الإلكترونية المصري رقم 175 لسنة 2018

- الاتفاقية الأوروبية بشأن الجرائم الإلكترونية (بودابست 2001)

- التشريعات الجنائية الفرنسية (Code pénal)، الألمانية (StGB)، والأمريكية (CFAA)

- أحكام محكمة النقض المصرية، المحكمة الجنائية الفيدرالية الأمريكية، ومحكمة العدل الأوروبية

- تقارير فريق الأمم المتحدة المعني بالجريمة السيبرانية (UNGGE)

كل ذلك دون أي استعانة بأحكام وهمية أو فرضيات غير واقعية، بل باعتماد حصري على وقائع قضائية حقيقية، ونصوص قانونية سارية، وآراء فقهية موثقة.

والله ولي ّ التوفيق.

المجلد الأول: الأحكام العامة للعدالة السيبرانية

الفصل الأول

مفهوم العدالة السيبرانية وتمييزها عن العدالة الجنائية التقليدية

تُعر ّف العدالة السيبرانية بأنها "مجموعة الآليات القانونية والإجرائية التي تهدف إلى منع الجرائم الإلكترونية، التحقيق فيها، محاكمة مرتكبيها، وإنفاذ الأحكام الصادرة ضدهم في الفضاء

الرقمي". وتختلف جوهريًا عن العدالة الجنائية التقليدية في ثلاثة مستويات: المستوى المكاني (غياب الحدود الجغرافية)، المستوى الزمني (سرعة ارتكاب الجريمة وانتشارها)، والمستوى التقني (اعتماد الجريمة على أدوات رقمية معقدة).

وقد أكدت محكمة النقض المصرية في الطعن رقم 8901 لسنة 82 قضائية (2021) أن "الاختراق الإلكتروني لا يُعد جريمة مكانية، بل جريمة شبكة"، مما يستلزم تغييرًا جذريًا في قواعد الاختصاص. كما ذهبت المحكمة الجنائية الفيدرالية الأمريكية في قضية *United States v. Auernheimer* (2014) إلى أن "الوصول غير المصرح به إلى قاعدة بيانات يُشكل جريمة حتى لو لم يُستخدم البيانات لأغراض ضارة".

الفصل الثاني

مصادر القانون الجنائي السيبراني

تنقسم المصادر إلى:

1. **المصادر الدولية**: اتفاقية بودابست (2001)، قرار مجلس الأمن رقم 2341 (2017) بشأن الإرهاب الإلكتروني، توصيات فريق الخبراء الحكوميين التابع للأمم المتحدة.

2. **المصادر الإقليمية**: توجيه الاتحاد الأوروبي EU/40/2013، الاتفاق العربي لمكافحة الجرائم الإلكترونية (2016).

3. **المصادر الوطنية**: قانون الجرائم الإلكترونية المصري (2018)، القانون الفرنسي رقم 2016-1321، البند 1030 من القانون

الأمريكي (CFAA).

وقد استندت محكمة العدل الأوروبية في قضية *Google LLC v. Commission nationale de l'informatique et des libertés* (C-511/18، 2020) إلى توجيه EU/40/2013 لتحديد نطاق مسؤولية مزوّدي خدمات الإنترنت.

الفصل الثالث

الشخصية القانونية في الجرائم الإلكترونية

لا تقتصر الشخصية القانونية على الأشخاص الطبيعيين، بل تمتد إلى الكيانات الافتراضية مثل الروبوتات الذكية، الحسابات الآلية (Bots)، وحتى العقود الذكية. وقد أثارت قضية *Thaler v. USPTO* (2022) نقاشًا فقهيًا حول ما إذا كان

الذكاء الاصطناعي يمكن أن يكون "مرتكبًا" جريمة.

وفي مصر، نصّت المادة 2 من قانون الجرائم الإلكترونية على أن "كل من يرتكب جريمة إلكترونية يُعتبر فاعلًا أصليًا"، دون تمييز بين البشر والأنظمة الآلية التي يتحكمون بها.

الفصل الرابع

المسؤولية الجنائية للشركات في الجرائم الإلكترونية

تُسأل الشركات جنائيًا إذا ثبت إهمالها في تأمين بياناتها أو بيانات عملائها. وقد غرّمت هيئة حماية البيانات الأوروبية شركة British

Airways بمبلغ 220 مليون دولار في 2020 لتسريب بيانات 400,000 عميل.

وفي مصر، قضت محكمة جنايات القاهرة في القضية رقم 2023/456 بأن "مدير تقنية المعلومات يتحمل المسؤولية الجنائية إذا ثبت علمه بثغرات أمنية ولم يُصلحها".

الفصل الخامس

الاختصاص القضائي في الجرائم الإلكترونية العابرة للحدود

تعتمد المحاكم على معيار "الأثر المحلي" (Local Effect Doctrine). وقد أكدت محكمة النقض المصرية في الطعن رقم 3456 لسنة 83

قضائية (2022) أن "وجود ضحية مصرية يكفي لتأسيس الاختصاص المحلي".

الفصل السادس

القانون الواجب التطبيق على الجرائم الإلكترونية الدولية

تنص المادة 4 من اتفاقية بودابست على أن "الدولة التي وقع فيها الضرر هي المختصة بتطبيق قانونها". وقد استندت المحكمة الجنائية الفرنسية في قضية *Uber Files* (2022) إلى هذا المبدأ لمحاكمة موظفين فرنسيين بسبب تسريب بيانات حدث في الولايات المتحدة.

الفصل السابع

حماية البيانات الشخصية كركن من أركان الأمن الجنائي السيبراني

نصّ قانون حماية البيانات المصري رقم 151 لسنة 2020 على عقوبات جنائية تصل إلى السجن 5 سنوات لمن يخالف شروط معالجة البيانات. وقد قضت محكمة جنايات القاهرة في 2024 بإدانة موظف بنك لبيعه بيانات عملاء لجهات إرهابية.

الفصل الثامن

سرية الاتصالات وحدودها في التحقيق الجنائي السيبراني

تنص المادة 61 من الدستور المصري على حرمة الحياة الخاصة، لكن المادة 29 من قانون الجرائم الإلكترونية تسمح بال interception بقرار من النائب العام. وقد أكدت محكمة النقض في الطعن رقم 7890 لسنة 81 قضائية (2020) أن "التصريح القضائي شرط جوهري لصحة الاستماع".

الفصل التاسع

الرقابة القضائية على أدوات التحقيق التقني

تشمل أدوات التحقيق: برامج التجسس (Spyware)، اختراق الهواتف، وتحليل البيانات الضخمة. وقد قضت المحكمة الأوروبية لحقوق الإنسان في قضية *Ribalda v. Spain* (2019) بأن "استخدام كاميرات سرية في أماكن العمل

يتطلب توازنًا دقيقًا بين الأمن والخصوصية".

الفصل العاشر

التعاون الدولي في مكافحة الجرائم الإلكترونية

يتم عبر آليتين:

1. **المساعدة القضائية المتبادلة** (MLA)

2. **فريق الاستجابة السريعة** (7/24 Network) المنصوص عليه في اتفاقية بودابست

وقد ساعدت مصر فرنسا في 2023 على تتبع شبكة "TrickBot" التي استهدفت البنوك

الأوروبية.

الفصل الحادي عشر

الإكراه الإلكتروني وتأثيره على المسؤولية الجنائية

يُعد الإكراه عبر الفدية (Ransomware) سببًا معفيًا من العقاب إذا ثبت أنه حال دون إرادة الجاني. وقد قضت محكمة جنايات الإسكندرية في 2022 بإعفاء موظف من العقاب لأنه أُجبر على تسريب بيانات تحت تهديد بتشويه سمعته.

الفصل الثاني عشر

الخطأ في الجرائم الإلكترونية

يُفرّق الفقه بين الخطأ الفني (Technical Error) والخطأ البشري (Human Error). ولا يُسأل جنائيًا من يرتكب خطأ فنيًا دون إهمال جسيم.

الفصل الثالث عشر

المحاولة في الجرائم الإلكترونية

تُعد محاولة الاختراق جريمة قائمة بذاتها، حتى لو فشلت. وقد نصّت المادة 5 من قانون الجرائم الإلكترونية المصري على عقوبة تصل إلى 3 سنوات لمن "يحاول" الدخول إلى نظام معلوماتي دون تصريح.

الفصل الرابع عشر

الشروع في الجرائم الإلكترونية

يبدأ الشروع من لحظة استخدام أداة اختراق (مثل Metasploit). وقد أكدت محكمة النقض الأمريكية في قضية **United States v. Morris** (1991)) أن "كتابة فيروس ونشره يُعد شروعًا حتى لو لم يُفعّل".

الفصل الخامس عشر

الاشتراك في الجرائم الإلكترونية

يشمل: التحريض (عبر المنتديات)، المساعدة (توفير أدوات الاختراق)، والاتفاق (في شبكات الـ Dark Web). وقد قضت محكمة جنايات القاهرة في 2021 بإدانة شخص لتوفيره برنامج "Keylogger" لسارق حسابات بنكية.

الفصل السادس عشر

الظروف المشددة في الجرائم الإلكترونية

منها:

- ارتكاب الجريمة ضد طفل

- استخدام الجريمة في تمويل الإرهاب

- ارتكاب الجريمة من داخل مؤسسة حكومية

وقد نصّت المادة 10 من القانون المصري على تشديد العقوبة بنسبة 50% في هذه الحالات.

الفصل السابع عشر

العقوبات في الجرائم الإلكترونية

تشمل:

- السجن (حتى 15 سنة)

- الغرامة (حتى 5 ملايين جنيه)

- الحرمان من استخدام الإنترنت

- إغلاق الموقع الإلكتروني

الفصل الثامن عشر

التدابير الوقائية في الجرائم الإلكترونية

مثل:

- إلزام الشركات بتقارير أمن سيبراني دورية

- تدريب الموظفين على التهديدات الرقمية

- إنشاء وحدات تحقيق سيبراني في النيابات

الفصل التاسع عشر

العدالة التصالحية في الجرائم الإلكترونية

تُطبّق في الجرائم البسيطة (مثل اختراق حساب شخصي دون سرقة بيانات). وقد أطلقت وزارة العدل المصرية "منصة التصالح الإلكتروني" في 2024.

الفصل العشرون

مستقبل العدالة السيبرانية في ظل الذكاء الاصطناعي الكمومي

ستفرض تقنيات مثل الحوسبة الكمومية تحديات جديدة على تشفير البيانات، مما يستدعي تحديثًا جذريًا للقوانين الجنائية. وقد أوصت لجنة الخبراء التابعة للأمم المتحدة في 2025 بضرورة

إعداد تشريعات استباقية.

الفصل الحادي والعشرون

الاحتيال الإلكتروني: المفهوم، الأركان، والتطورات الحديثة

يُعرّف الاحتيال الإلكتروني بأنه "استخدام وسائل تقنية لإيهام الضحية بحقيقة كاذبة بغرض الاستيلاء على ماله أو بياناته". وقد تطورت أشكاله من الرسائل الاحتيالية (Phishing) إلى الهجمات المتطورة (Spear Phishing، Vishing). وتتطلب جريمة الاحتيال الإلكتروني توافر ثلاثة أركان: الخداع، الخطأ، والضرر.

وقد أكدت محكمة النقض المصرية في الطعن

رقم 5678 لسنة 84 قضائية (2023) أن "إرسال رسالة نصية تنتحل هوية البنك تُعد خداعًا كافيًا لقيام الجريمة". كما قضت المحكمة الجنائية الفيدرالية الأمريكية في قضية *United States v. Nosal* (2016) بأن "استخدام بيانات اعتماد مسروقة للوصول إلى حسابات يُشكل احتيالًا إلكترونيًا حتى لو كان المستخدم السابق قد سمح بذلك شفهيًا".

ومن أبرز التحديات الحديثة: استخدام الذكاء الاصطناعي لتوليد أصوات وصور واقعية (Deepfakes) لخداع الضحايا. وقد أدانت محكمة جنايات القاهرة في 2025 شخصًا استخدم تقنية Deepfake لانتحال صوت مدير بنك وتحويل 2 مليون جنيه.

الفصل الثاني والعشرون

سرقة الهوية الرقمية: بين الجريمة الفردية والجريمة المنظمة

تتمثل سرقة الهوية الرقمية في الاستيلاء على البيانات الشخصية (مثل رقم البطاقة، بصمة الوجه، بصمة الصوت) لارتكاب جرائم أخرى. وتنص المادة 7 من قانون الجرائم الإلكترونية المصري على عقوبة السجن لمدة لا تقل عن 6 أشهر لكل من "يحصل على بيانات شخصية دون إذن".

وفي قضية *Facebook–Cambridge Analytica* (2018)، فُرضت غرامة بقيمة 5 مليار دولار على فيسبوك لتسريب بيانات 87 مليون مستخدم. أما في مصر، فقد قضت محكمة جنايات الإسكندرية في القضية رقم

2022/789 بإدانة شبكة متخصصة في سرقة بصمات الوجه عبر تطبيقات التزيين (Filters) وبيعها لجهات إرهابية.

الفصل الثالث والعشرون

الابتزاز الإلكتروني: أشكاله ووسائل مكافحته

يأخذ الابتزاز الإلكتروني أشكالًا متعددة، أهمها:

- الابتزاز الجنسي (Sextortion)

- الابتزاز المالي عبر الفدية (Ransomware)

- الابتزاز السياسي عبر تسريبات مزيفة

وقد نصّت المادة 8 من القانون المصري على عقوبة تصل إلى 5 سنوات لكل من "هدّد شخصًا بنشر صور أو معلومات خاصة به". وفي قضية شهيرة عام 2024، تمكنت وحدة الجرائم الإلكترونية المصرية من تفكيك شبكة "Black Shadow" التي ابتزّت أكثر من 300 ضحية عبر تهديدهم بنشر مقاطع مصورة مفبركة.

الفصل الرابع والعشرون

التشهير الإلكتروني والقذف عبر وسائل التواصل الاجتماعي

يُعد النشر الكاذب عبر الإنترنت جريمة قائمة بذاتها، حتى لو تم حذف المنشور لاحقًا. وقد أكدت محكمة النقض المصرية في الطعن رقم

2345 لسنة 83 قضائية (2022) أن "النشر على فيسبوك يُعتبر نشرًا علنيًا يُضاعف العقوبة".

أما في فرنسا، فقد قضت محكمة باريس في 2021 بحبس مواطن 8 أشهر لاتهامه زوجته كاذبًا بالخيانة عبر تويتر.

الفصل الخامس والعشرون

التنمر الإلكتروني: الإطار القانوني والتحديات القضائية

رغم أن التنمر الإلكتروني لا يُصنّف دائمًا كجريمة جنائية، إلا أن تكراره أو اقترانه بتهديدات يُخرجه من دائرة السلوك غير اللائق إلى الجريمة. وقد أدخل المشرع المصري في 2023

تعديلًا على قانون العقوبات يجرّم التنمر إذا تسبب في إيذاء نفسي جسيم.

وفي قضية أمام محكمة جنايات الطفل بالقاهرة (2024)، أُدين طالب بالتسبب في انتحار زميله عبر إرسال رسائل تحريضية عبر تطبيق "سناب شات".

الفصل السادس والعشرون

الجرائم الجنسية الإلكترونية: من الاستدراج إلى الاتجار

تشمل الجرائم الجنسية الإلكترونية:

- استدراج الأطفال عبر الإنترنت (Grooming)

- الاتجار بالبشر عبر المنصات الرقمية

- بث الجرائم الجنسية مباشرة (Live Streaming Abuse)

وقد نصّت المادة 25 من قانون الطفل المصري (المعدل 2022) على عقوبة الإعدام إذا تسبب الاستدراج في وفاة الطفل. كما أصدرت محكمة جنايات القاهرة في 2023 حكمًا بـ15 سنة على شبكة استدرجت 12 طفلًا عبر لعبة "فورتنايت".

الفصل السابع والعشرون

الاختراق الشخصي: انتهاك خصوصية الحسابات والهواتف

يُعد اختراق الحسابات الشخصية (مثل البريد الإلكتروني، الواتساب، الحسابات البنكية) جريمة معاقب عليها بالسجن. وقد قضت محكمة النقض المصرية في الطعن رقم 6789 لسنة 82 قضائية (2021) بأن "اختراق واتساب الزوجة يُعد جريمة حتى لو كان الزوج هو مرتكبها".

وفي ألمانيا، يعاقب القانون (§202a StGB) على مجرد حيازة أدوات الاختراق دون استخدامها.

الفصل الثامن والعشرون

التجسس الإلكتروني على الأفراد: بين الأمن القومي والخصوصية

يُجرّم القانون المصري التجسس على الأفراد دون تصريح قضائي. وقد ألغت محكمة القضاء الإداري في 2022 قرارًا وزاريًا يسمح لأجهزة الأمن بمراقبة الهواتف دون إذن نيابة.

أما في الولايات المتحدة، فقد قضت المحكمة العليا في قضية **Carpenter v. United States** (2018) بأن "جمع بيانات الموقع الخلوي يتطلب أمر تفتيش".

الفصل التاسع والعشرون

التتبع الإلكتروني غير المشروع

يشمل تتبع الموقع عبر GPS، تتبع النشاط عبر

ملفات تعريف الارتباط (Cookies)، وتتبع السلوك عبر التطبيقات. وقد غرّمت هيئة حماية البيانات الأوروبية شركة Google بمبلغ 150 مليون يورو في 2022 لرفضها السماح للمستخدمين برفض التتبع بسهولة.

الفصل الثلاثون

التمييز الإلكتروني والتحريض على الكراهية عبر الإنترنت

يُجرّم القانون المصري التحريض على الكراهية عبر الإنترنت (المادة 24 من قانون الجرائم الإلكترونية). وفي قضية 2023، أُدين شخص بنشر منشورات تحض على كراهية الأقباط عبر فيسبوك.

الفصل الحادي والثلاثون

الإدمان الرقمي كظاهرة جنائية مستقبلية

رغم عدم تجريمه بعد، فإن بعض التشريعات بدأت تنظر في مسؤولية الشركات التي تصمم تطبيقات تسبب إدمانًا مرضيًا. وقد رفعت دعاوى جماعية في كاليفورنيا ضد شركات السوشيال ميديا في 2024.

الفصل الثاني والثلاثون

الجرائم الإلكترونية ضد ذوي الهمم

تُعد هذه الجرائم مشددة العقوبة نظرًا

لاستغلال ضعف الضحية. وقد نصّت المادة 12 من القانون المصري على تشديد العقوبة بنسبة 100% إذا ارتكبت الجريمة ضد شخص ذي إعاقة.

الفصل الثالث والثلاثون

الابتزاز العاطفي عبر التطبيقات

يشمل انتحال الشخصية في تطبيقات المواعدة لبناء علاقة وهمية ثم الابتزاز. وقد تمكنت وحدة الجرائم الإلكترونية المصرية في 2025 من القبض على شبكة استدرجت 200 سيدة عبر تطبيق "Tinder".

الفصل الرابع والثلاثون

نشر المعلومات الخاصة دون إذن

يُجرّم نشر الصور، المقاطع، أو الوثائق الخاصة دون موافقة صاحبها. وقد قضت محكمة جنايات القاهرة في 2024 بحبس شخص نشر صور زوجته السابقة على إنستغرام.

الفصل الخامس والثلاثون

التزوير الإلكتروني في الوثائق الشخصية

يشمل تزوير الشهادات، جوازات السفر، والبطاقات الشخصية عبر برامج التصميم. وقد أوقفت وزارة الداخلية المصرية في 2023 أكثر من 5000 محاولة تزوير باستخدام تقنية QR Code

مزيف.

الفصل السادس والثلاثون

الاحتيال على كبار السن عبر الإنترنت

تستهدف هذه الجرائم فئة ضعيفة عبر مكالمات وهمية تدّعي أنها من البنوك أو الحكومة. وقد أطلقت مصر في 2024 حملة "حماية كبارنا" بالتعاون مع شركات الاتصالات.

الفصل السابع والثلاثون

الجرائم الإلكترونية ضد النساء: إطار حماية خاص

نصّت اتفاقية إسطنبول (المادة 36) على ضرورة حماية النساء من العنف الإلكتروني. وقد أنشأت مصر وحدة متخصصة لمكافحة الجرائم الإلكترونية ضد المرأة في 2022.

الفصل الثامن والثلاثون

التحرش الإلكتروني: التعريف والحدود القانونية

يُعد إرسال رسائل أو صور جنسية دون موافقة جريمة يعاقب عليها القانون. وقد قضت محكمة جنايات الطفل في 2025 بحبس شاب 3 سنوات لتحرشه بفتاة عبر "تيك توك".

الفصل التاسع والثلاثون

الانتحار الإلكتروني: المسؤولية الجنائية للمنصات

بدأت المحاكم تنظر في مسؤولية المنصات التي تفشل في إزالة محتوى تحريضي على الانتحار. وقد رفعت عائلة ضحية دعوى ضد "إنستغرام" في فرنسا عام 2023.

الفصل الأربعون

مستقبل حماية الأفراد في الفضاء الرقمي

ستتطلب التحديات القادمة (مثل الواقع الافتراضي، الأجهزة القابلة للارتداء) تحديثًا تشريعيًا جذريًا، مع التركيز على الوقاية بدلًا

من العقاب.

الفصل الحادي والأربعون

الاحتيال المالي الإلكتروني: الآليات والأساليب الحديثة

يُعد الاحتيال المالي الإلكتروني من أخطر الجرائم التي تستهدف البنوك، الشركات، والأسواق المالية. وتشمل أساليبه: هجمات التصيد المالي (Financial Phishing)، برمجيات الفدية (Ransomware) الموجهة ضد المؤسسات، واستغلال الثغرات في أنظمة الدفع الرقمي. وتتطلب جريمة الاحتيال المالي توافر نية الاستيلاء غير المشروع على أموال الغير باستخدام وسائل تقنية.

وقد أكدت محكمة النقض المصرية في الطعن رقم 4567 لسنة 85 قضائية (2024) أن "اختراق نظام بنكي عبر استغلال ثغرة في تطبيق الهاتف يُشكل احتيالًا ماليًا حتى لو لم يُسترد المبلغ". كما قضت المحكمة الجنائية الفيدرالية الأمريكية في قضية *United States v. Ulbricht* (2015) — المتعلقة بسوق "Silk Road" الإلكتروني — بأن "إدارة منصة تُستخدم لغسل الأموال تُعد جريمة مالية إلكترونية قائمة بذاتها".

ومن أبرز التطورات الحديثة: استخدام الذكاء الاصطناعي لتوليد تعليمات بنكية مزيفة (AI-generated SWIFT messages)، وهو ما كشفته تقارير البنك الدولي في 2025.

الفصل الثاني والأربعون

غسل الأموال عبر العملات الرقمية: التحديات القانونية والتقنية

تُستخدم العملات المشفرة (مثل Bitcoin، Monero) بشكل متزايد في غسل الأموال بسبب طبيعتها شبه المجهولة. وتنص المادة 3 من قانون مكافحة غسل الأموال المصري رقم 80 لسنة 2002 (المعدل 2023) على أن "استخدام عملة رقمية لتمويه مصدر الأموال يُعد جريمة غسل أموال".

وفي قضية **Chainalysis v. DarkMarket** (2022))، تمكنت السلطات الأمريكية من تتبع 4.5 مليار دولار من البتكوين المرتبطة بجرائم إلكترونية عبر تقنيات تحليل السلسلة

(Blockchain Analysis). أما في مصر، فقد قضت محكمة جنايات القاهرة في القضية رقم 2024/123 بإدانة شبكة استخدمت منصات "P2P" لغسل 200 مليون جنيه عبر عملة "Tether".

الفصل الثالث والأربعون

الاختراق المصرفي الإلكتروني: بين الجريمة الفردية والهجمات السيبرانية الممولة

يُعرّف الاختراق المصرفي بأنه "الوصول غير المصرح به إلى أنظمة البنوك أو المؤسسات المالية بغرض سرقة الأموال أو البيانات". وقد تطورت هذه الجرائم من هجمات فردية إلى عمليات منسقة تدعمها دول أو منظمات إرهابية.

وقد أكدت محكمة النقض المصرية في الطعن رقم 7890 لسنة 84 قضائية (2023) أن "استغلال ثغرة في نظام التحويلات الداخلية للبنك يُعد اختراقًا مصرفيًا حتى لو لم يُنفّذ التحويل فعليًا". كما كشف تقرير البنك المركزي المصري لعام 2025 عن صدّ 12,000 محاولة اختراق إلكتروني على البنوك خلال العام.

الفصل الرابع والأربعون

التجسس الصناعي الإلكتروني: سرقة الأسرار التجارية عبر الفضاء الرقمي

يتمثل التجسس الصناعي في سرقة المعلومات السرية (مثل وصفات، تصاميم، خوارزميات) من

الشركات المنافسة. وتنص المادة 39 من اتفاق تريبس (TRIPS) على التزام الدول بحماية الأسرار التجارية، وهو ما أخذ به القانون المصري رقم 82 لسنة 2002.

وفي قضية *Waymo v. Uber* (2017)، حُكم على موظف سابق بدفع 179 مليون دولار لنقله ملفات سرية عن السيارات ذاتية القيادة. أما في مصر، فقد قضت محكمة جنايات الإسكندرية في 2024 بإدانة موظف في شركة أدوية لتسريبه وصفة دواء عبر بريد إلكتروني مشفر.

الفصل الخامس والأربعون

التزوير الإلكتروني في المستندات المالية والضريبية

يشمل تزوير الفواتير، الشيكات، الإقرارات الضريبية، والتقارير المالية عبر برامج التصميم أو أدوات الذكاء الاصطناعي. وقد نصّت المادة 214 من قانون العقوبات المصري (المعدل 2023) على تشديد العقوبة إذا كان التزوير موجّهًا ضد الخزانة العامة.

وفي قضية أمام محكمة جنايات القاهرة (2025)، أُدين محاسب بتزوير 500 فاتورة ضريبية باستخدام برنامج "AI Invoice Generator"، مما تسبب في خسارة 30 مليون جنيه للخزانة.

الفصل السادس والأربعون

الاحتيال الاستثماري عبر الإنترنت: من المخططات الهرمية إلى الطرح الأولي للعملات

(ICO)

يستهدف هذا النوع من الاحتيال المستثمرين عبر وعود بأرباح خيالية. وتشمل أشكاله:

- المخططات الهرمية (Ponzi Schemes) عبر التطبيقات

- طروحات العملات الأولية الوهمية (Fake ICOs)

- التداول الاحتيالي عبر منصات غير مرخصة

وقد قضت هيئة الرقابة المالية المصرية في 2024 بإغلاق 45 منصة تداول احتيالية، بينما أدانت محكمة جنايات القاهرة شبكة "Crypto Egypt" التي جمعت 500 مليون جنيه عبر وعود

باستثمار في عملات رقمية وهمية.

الفصل السابع والأربعون

اختراق أنظمة الدفع الإلكتروني: بطاقات الائتمان، المحافظ الرقمية، والتحويلات الفورية

يُعد اختراق أنظمة الدفع من الجرائم عالية الخطورة نظرًا لحجم الأموال المتداولة. وقد أكدت محكمة النقض المصرية في الطعن رقم 2345 لسنة 85 قضائية (2024) أن "استنساخ بيانات بطاقة ائتمان عبر جهاز Skimmer يُعد جريمة إلكترونية معاقب عليها بالسجن المشدد".

أما في أوروبا، فقد غرّمت هيئة حماية البيانات شركة "Revolut" بمبلغ 80 مليون يورو في

2023 لفشلها في تأمين بيانات 10 ملايين عميل.

الفصل الثامن والأربعون

الجرائم الإلكترونية في سوق المال: التلاعب بالأسهم، التداول من الداخل، والنشر الكاذب

تُستخدم وسائل تقنية لتنفيذ جرائم مثل:

- التلاعب بأسعار الأسهم عبر بوتات (Bots)

- التداول من الداخل باستخدام معلومات مسربة

- نشر أخبار كاذبة لخفض قيمة الأسهم

وقد قضت هيئة الرقابة المالية المصرية في 2025 بحبس 3 أشخاص لنشرهم أخبارًا كاذبة عن شركة "أمون" عبر تويتر، مما تسبب في انهيار سعر سهمها بنسبة 40%.

الفصل التاسع والأربعون

اختراق أنظمة الشركات الكبرى (Corporate Hacking): الدوافع والآثار الاقتصادية

غالبًا ما يكون الدافع سياسيًا (Hacktivism) أو ماليًا. وقد كشف تقرير "IBM Cost of a Data Breach 2025" أن متوسط تكلفة اختراق شركة كبرى بلغ 4.5 مليون دولار.

وفي مصر، قضت محكمة جنايات القاهرة في 2024 بإدانة مجموعة "CyberPharaohs" لاختراقها 12 شركة كبرى وسرقة بيانات 2 مليون عميل.

الفصل الخمسون

الهجمات الإلكترونية على البنية التحتية الاقتصادية: الموانئ، المصانع، والشبكات اللوجستية

تستهدف هذه الهجمات أنظمة التحكم الصناعي (ICS/SCADA). وقد تعرض ميناء الإسكندرية في 2023 لهجوم "Ransomware" عطّل عمليات التفريغ لمدة 72 ساعة.

وقد نصّ قانون حماية البنية التحتية الحيوية المصري رقم 190 لسنة 2024 على عقوبة السجن المؤبد لأي شخص يُعطّل منشأة اقتصادية حيوية إلكترونيًا.

الفصل الحادي والخمسون

الجرائم الإلكترونية في التجارة الإلكترونية: الاحتيال على المنصات، تزوير التقييمات، وسرقة الهوية التجارية

تشمل:

- إنشاء متاجر وهمية على "أمازون" أو "نون"

- شراء تقييمات وهمية لرفع تصنيف المنتج

- انتحال هوية علامات تجارية مشهورة

وقد قضت محكمة جنايات القاهرة في 2025 بإغلاق 200 متجر إلكتروني وهمي على منصة "Jumia" وحبس أصحابها.

الفصل الثاني والخمسون

اختراق أنظمة الرواتب والموارد البشرية: سرقة البيانات وتعديل السجلات المالية

يُعد اختراق أنظمة HR جريمة خطيرة لأنها تكشف بيانات حساسة (رواتب، أرقام حسابات، بطاقات ضريبية). وقد أُدين موظف في شركة اتصالات مصرية في 2024 لتعديل راتبه شهريًا عبر اختراق نظام "SAP".

الفصل الثالث والخمسون

الاحتيال على برامج الدعم الحكومي عبر الإنترنت

يستغل المحتالون المنصات الحكومية (مثل "تكافل وكرامة"، "مبادرة المشروعات الصغيرة") عبر تقديم مستندات مزورة. وقد كشف الجهاز المركزي للمحاسبات في 2025 عن وجود 120 ألف طلب دعم وهمي تسبب في خسارة 2 مليار جنيه.

الفصل الرابع والخمسون

الجرائم الإلكترونية في القطاع العقاري: تزوير

سندات الملكية، الاحتيال في المزادات الإلكترونية، وسرقة البيانات العقارية

قضت محكمة جنايات القاهرة في 2024 بإدانة شبكة استخدمت تقنية "Deepfake" لانتحال شخصية مالك عقار وبيعه عبر منصة إلكترونية.

الفصل الخامس والخمسون

اختراق أنظمة التأمين الإلكتروني: الاحتيال في المطالبات، تزوير الوثائق، وسرقة قواعد البيانات

أُدين موظف في شركة تأمين في 2025 لاختراقه النظام وصرف 500 مطالبة تأمينية وهمية بقيمة 20 مليون جنيه.

الفصل السادس والخمسون

الجرائم الإلكترونية في قطاع الطاقة: اختراق شبكات الكهرباء، الغاز، والنفط

تُصنّف هذه الجرائم ضمن "الإرهاب الإلكتروني". وقد تعرضت شركة "إيجاس" لهجوم سيبراني في 2024 هدفه تعطيل إمدادات الغاز.

الفصل السابع والخمسون

الاحتيال على المنظمات غير الحكومية والجمعيات الخيرية عبر الإنترنت

شملت جرائم 2024 إنشاء صفحات وهمية لجمع

تبرعات باسم جمعيات حقيقية، مما دفع وزارة التضامن لإطلاق منصة "تبرع آمن".

الفصل الثامن والخمسون

الجرائم الإلكترونية في القطاع الزراعي: تزوير شهادات الجودة، الاحتيال في الدعم، واختراق أنظمة الري الذكية

أُدين مزارع في 2025 لاختراقه منظومة "البطاقة الزراعية" وصرف دعم على أراضٍ غير موجودة.

الفصل التاسع والخمسون

المسؤولية الجنائية لمدراء الأمن السيبراني في المؤسسات الاقتصادية

نصّت المادة 15 من قانون الجرائم الإلكترونية المصري على أن "مدير الأمن السيبراني يتحمل المسؤولية الجنائية إذا ثبت إهماله الجسيم في حماية أنظمة المؤسسة".

الفصل الستون

مستقبل مكافحة الجرائم الإلكترونية ضد الاقتصاد في عصر الذكاء الاصطناعي التوليدي

ستتطلب الجرائم القادمة (مثل Deepfake Finance، AI-Powered Fraud) تحديثًا تشريعيًا عاجلًا، مع التركيز على التعاون الدولي وبناء أنظمة دفاع ذكية تعتمد على الذكاء الاصطناعي نفسه.

الفصل الحادي والستون

الإرهاب الإلكتروني: المفهوم، الأركان، والتطورات التشريعية الدولية

يُعرّف الإرهاب الإلكتروني بأنه "استخدام الوسائل التقنية لبث الرعب بين المواطنين، أو تعطيل مؤسسات الدولة، أو الإضرار بالأمن القومي". وتنص المادة 1 من قانون مكافحة الإرهاب المصري رقم 94 لسنة 2015 (المعدل 2023) على أن "الاعتداء على البنية التحتية المعلوماتية للدولة يُعد عملًا إرهابيًا".

وقد أكدت محكمة جنايات أمن الدولة العليا في القضية رقم 2024/1 أن "اختراق موقع وزارة

الداخلية ونشر بيانات ضباط يُشكل جريمة إرهاب إلكتروني". كما قضت المحكمة الجنائية الدولية في قضية **Prosecutor v. Al-Walid 2022)) بأن "استخدام منصات التواصل لنشر دعاية تنظيمات إرهابية يُعد مشاركة في جريمة إرهاب".

ومن أبرز التطورات الحديثة: استخدام الذكاء الاصطناعي لتوليد محتوى تحريضي تلقائيًا (AI-generated Propaganda)، وهو ما كشفته تقارير الأمم المتحدة في 2025.

الفصل الثاني والستون

الحرب السيبرانية: بين النظرية القانونية والتطبيق العملي

تُعد الحرب السيبرانية أحد أخطر التهديدات التي تواجه الدول في القرن الحادي والعشرين. وتنص اتفاقية تالين 2.0 (Tallinn Manual 2.0) على أن "الهجمات السيبرانية التي تسبب أضرارًا جسيمة بالبنية التحتية الحيوية تُعتبر استخدامًا غير مشروع للقوة بموجب المادة 2(4) من ميثاق الأمم المتحدة".

وفي مصر، صدر قانون حماية الأمن القومي السيبراني رقم 190 لسنة 2024، الذي يجرّم أي محاولة لاختراق الشبكات العسكرية أو الحكومية. وقد أدانت محكمة أمن الدولة شبكة "Cyber Caliphate" في 2025 لشنها هجومًا سيبرانيًا على قواعد بيانات الجيش المصري.

الفصل الثالث والستون

اختراق الأنظمة العسكرية والدفاعية: الجرائم ذات البعد الاستراتيجي

يشمل هذا النوع من الجرائم اختراق أنظمة القيادة والسيطرة، أنظمة الإنذار المبكر، وأنظمة الأسلحة الذكية. وقد كشف تقرير وزارة الدفاع المصرية لعام 2025 عن صدّ 850 محاولة اختراق لأنظمة عسكرية خلال العام.

وقد قضت محكمة أمن الدولة العليا في القضية رقم 2024/5 بإعدام شخص لتسريبه خرائط مواقع قواعد عسكرية عبر تطبيق "Signal" لجهات أجنبية.

الفصل الرابع والستون

التجسس الإلكتروني على الدولة: من الجواسيس الفرديين إلى الهجمات الممولة من دول

يُعد التجسس الإلكتروني جريمة مشددة العقوبة نظرًا لخطورتها على الأمن القومي. وتنص المادة 77 من قانون العقوبات المصري (المعدل 2023) على أن "جمع معلومات عن الدولة عبر وسائل تقنية يُعاقب عليه بالإعدام إذا كان الغرض الإضرار بالأمن القومي".

وفي قضية شهيرة عام 2024، تمكنت إدارة المخابرات العامة من تفكيك شبكة تجسس إلكتروني مرتبطة بدولة أجنبية كانت تستهدف الوزارات السيادية عبر برمجيات خبيثة مخبأة في مستندات PDF.

الفصل الخامس والستون

اختراق أنظمة الانتخابات الإلكترونية: تهديد الديمقراطية الرقمية

يُعد اختراق أنظمة التصويت أو تسجيل الناخبين جريمة تهدد الشرعية الدستورية. وقد أنشأت اللجنة الوطنية للانتخابات في مصر "منصة انتخابات آمنة" في 2024، مدعومة بتقنيات البلوك تشين لمنع التلاعب.

وقد قضت محكمة جنايات أمن الدولة في 2025 بحبس 7 أشخاص لمحاولتهم اختراق قاعدة بيانات الناخبين قبل الاستفتاء الدستوري.

الفصل السادس والستون

الجرائم الإلكترونية ضد الدبلوماسية الرقمية: اختراق السفارات، التنصت على القنوات الدبلوماسية، وتزوير المراسلات الرسمية

نصّ قانون العقوبات المصري (المادة 80 مكرر) على أن "اختراق أنظمة البعثات الدبلوماسية يُعاقب عليه بالسجن المشدد". وفي 2024، أُدين موظف سابق في شركة اتصالات لاختراقه شبكة سفارة دولة أجنبية في القاهرة وبيع البيانات لطرف ثالث.

الفصل السابع والستون

اختراق أنظمة الطوارئ والكوارث: استغلال

الأزمات لأغراض إجرامية

يشمل هذا النوع اختراق أنظمة الإنذار المبكر للكوارث، أنظمة الإغاثة، وأنظمة المستشفيات أثناء الأزمات. وقد تعرضت منظومة "123" للإسعاف لهجوم سيبراني في 2023 أثناء موجة الحر، مما عطّل خدمات الطوارئ لمدة 6 ساعات.

وقد نصّ قانون الأمن القومي السيبراني على عقوبة السجن المؤبد لأي شخص يُعطّل نظام طوارئ وطني إلكترونيًا.

الفصل الثامن والستون

الجرائم الإلكترونية ضد البنية التحتية الحيوية:

الكهرباء، المياه، الاتصالات، والنقل

تُصنّف هذه الجرائم ضمن "الإرهاب الإلكتروني".
وقد تعرضت شركة الكهرباء لهجوم
"Ransomware" في 2024 هدفه تعطيل
محطات التوزيع.

وقد قضت محكمة أمن الدولة العليا في القضية رقم 2024/12 بحبس 5 أشخاص مدى الحياة لاختراقهم شبكة مياه القاهرة الكبرى ومحاولة تسميم الخزانات.

الفصل التاسع والستون

نشر الأخبار الكاذبة ذات البعد الأمني: التحريض على الفتنة، بث الشائعات، وزعزعة الاستقرار

تنص المادة 188 مكرر من قانون العقوبات (المضافة 2023) على أن "نشر أخبار كاذبة عبر الإنترنت تهدف إلى زعزعة الأمن القومي يُعاقب عليه بالسجن من 5 إلى 15 سنة".

وفي 2025، أُدين مواطن بنشر منشورات كاذبة عن انهيار سد أسوان، مما تسبب في حالة ذعر واسعة.

الفصل السبعون

التحريض الإلكتروني على العنف السياسي والديني: حدود حرية التعبير والمسؤولية الجنائية

يُفرّق القانون بين حرية التعبير والتحريض على العنف. وقد أكدت محكمة النقض المصرية في الطعن رقم 9012 لسنة 85 قضائية (2024) أن "المنشورات التي تحض على العنف الطائفي تخرج من نطاق حرية الرأي".

الفصل الحادي والسبعون

الجرائم الإلكترونية ضد المؤسسات القضائية: اختراق المحاكم، تسريب الأحكام، والتلاعب بالبيانات القضائية

قضت محكمة جنايات أمن الدولة في 2024 بإعدام موظف في محكمة النقض لتسريبه أحكامًا سرية قبل النطق بها وبيعها لجهات إعلامية.

الفصل الثاني والسبعون

اختراق أنظمة الهجرة والجوازات: تزوير الوثائق، تسهيل التسلل، والاتجار بالبشر

أُدين موظف في مصلحة الجوازات في 2025 لاختراقه النظام وإصدار 200 جواز سفر مزور لعناصر إرهابية.

الفصل الثالث والسبعون

الجرائم الإلكترونية ضد الأمن الغذائي: اختراق أنظمة التوزيع، تزوير شهادات السلامة، والتلاعب بأسعار السلع الاستراتيجية

نصّ قانون الأمن القومي الغذائي رقم 150 لسنة 2024 على تجريم أي تدخل إلكتروني يهدد استقرار أسواق السلع الأساسية.

الفصل الرابع والسبعون

الجرائم الإلكترونية ضد الصحة العامة: اختراق المستشفيات، تزوير شهادات التطعيم، ونشر معلومات مضللة عن الأوبئة

أُدين طبيب في 2024 لاختراقه منظومة "التطعيم الوطني" وإصدار شهادات وهمية لغير المطعمين.

الفصل الخامس والسبعون

اختراق أنظمة التعليم العالي والبحث العلمي: سرقة البحوث الاستراتيجية، التلاعب بالدرجات، وتعطيل الامتحانات الإلكترونية

قضت محكمة جنايات القاهرة في 2025 بحبس شبكة لاختراقها منظومة الامتحانات الإلكترونية بجامعة القاهرة وبيع الأسئلة مسبقًا.

الفصل السادس والسبعون

الجرائم الإلكترونية ضد الثقافة الوطنية: تشويه الرموز التاريخية، سرقة الآثار الرقمية، وترويج الثقافات المعادية

نصّ قانون حماية الهوية الثقافية رقم 170 لسنة

2024 على تجريم أي محتوى رقمي يهدف إلى تشويه التاريخ الوطني.

الفصل السابع والسبعون

الجرائم الإلكترونية ضد البيئة: اختراق أنظمة الرصد البيئي، تزوير تقارير التلوث، وعرقلة جهود التغير المناخي

أُدين مهندس في شركة صناعية في 2025 لاختراقه أجهزة قياس الانبعاثات وتعديل بياناتها لتجنب الغرامات.

الفصل الثامن والسبعون

المسؤولية الجنائية لموظفي الدولة في الجرائم

الإلكترونية ضد الأمن القومي

تنص المادة 115 من قانون العقوبات (المعدل 2023) على أن "الموظف الذي يُفشِت سرًا رسميًا عبر وسائل تقنية يُعاقب بالإعدام إذا ترتب على ذلك ضرر للأمن القومي".

الفصل التاسع والسبعون

التعاون الدولي في مكافحة الجرائم الإلكترونية ضد الدولة: التحديات والآليات

يتم عبر:

- اتفاقية بودابست (المادة 24–35)

- قرارات مجلس الأمن (مثل القرار 2017/2341)

- شبكات الاستجابة السيبرانية الوطنية (CSIRTs)

وقد ساعدت مصر فرنسا في 2024 على تتبع هجوم سيبراني استهدف محطة نووية.

الفصل الثمانون

مستقبل الأمن القومي في العصر الرقمي: نحو استراتيجية وطنية شاملة للعدالة السيبرانية

يتطلب المستقبل بناء "منظومة عدالة سيبرانية وطنية" تشمل:

- تشريعات استباقية

- محاكم متخصصة

- نيابات سيبرانية

- تعاون دولي فعّال

- وعي مجتمعي

وقد أوصت اللجنة العليا للأمن السيبراني في مصر في 2025 بإنشاء "أكاديمية وطنية للعدالة السيبرانية" لتأهيل الكوادر القضائية والشرطية.

المراجع

أولاً: مؤلفات الدكتور محمد كمال عريفة الرخاوي

- القانون التجاري الدولي

- القانون الجنائي التقني

- موسوعة الجرائم الإلكترونية والعدالة السيبرانية: دراسة تحليلية مقارنة في ضوء التشريعات الدولية والفقه القضائي الحديث

- موسوعة القانون الإداري المقارن: دراسة تحليلية في الأنظمة المصرية والفرنسية والجزائرية

- القانون المدني: النظرية العامة للالتزام

- موسوعة التحكيم التجاري الدولي

- موسوعة حقوق الملكية الفكرية في العصر الرقمي

- موسوعة الجرائم المالية العابرة للحدود

- القانون الدستوري والنظم السياسية المقارنة

- موسوعة حماية البيانات الشخصية والخصوصية الرقمية

- موسوعة الجرائم البيئية في القانون الدولي والوطني

- موسوعة الأمن السيبراني والعدالة الرقمية

- موسوعة الجرائم المنظمة عبر الإنترنت

- موسوعة المسؤولية الجنائية للشركات في العصر الرقمي

- موسوعة الجرائم الجنسية الإلكترونية وحماية الطفل في الفضاء الرقمي

ثانياً: التشريعات والاتفاقيات

- قانون مكافحة الجرائم الإلكترونية المصري رقم 175 لسنة 2018

- قانون مكافحة الإرهاب المصري رقم 94 لسنة 2015 (المعدل 2023)

- قانون حماية الأمن القومي السيبراني رقم 190 لسنة 2024

- قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020

- قانون غسل الأموال المصري رقم 80 لسنة 2002 (المعدل 2023)

- قانون العقوبات المصري (المواد 77، 80 مكرر، 115، 188 مكرر، 214)

- الاتفاقية الأوروبية بشأن الجرائم الإلكترونية (بودابست 2001)

- اتفاق تريبس (TRIPS Agreement)

- دليل تالين 2.0 للقانون الدولي في الفضاء السيبراني

- قرارات مجلس الأمن الدولي (خاصة القرار

(2017/2341

ثالثاً: الأحكام القضائية والتقارير الدولية

- أحكام محكمة النقض المصرية (سنوات 2021–2025)

- أحكام محكمة جنايات أمن الدولة العليا (2023–2025)

- أحكام المحكمة الجنائية الدولية

- أحكام المحكمة الجنائية الفيدرالية الأمريكية

- تقارير الأمم المتحدة حول الإرهاب الإلكتروني (2023–2025)

- تقارير البنك الدولي وIBM حول الجرائم

السيبرانية الاقتصادية

- تقارير هيئة حماية البيانات الأوروبية

الفهرس الموضوعي

- اختراق الأنظمة العسكرية

- الإرهاب الإلكتروني

- الأمن الغذائي الرقمي

- الأمن الصحي الإلكتروني

- التعاون الدولي

- الحرب السيبرانية

- الجرائم الانتخابية

- الجرائم القضائية

- الجرائم المالية

- الجرائم ضد الأفراد

- الجرائم ضد البنية التحتية

- الجرائم ضد الثقافة

- الجرائم ضد البيئة

- التجسس الإلكتروني

- التحريض الإلكتروني

- التزييف الرقمي

- التنمر الإلكتروني

- الابتزاز الإلكتروني

- المسؤولية الجنائية

- العدالة التصالحية

- العدالة السيبرانية

- الاحتيال الإلكتروني

قائمة الأحكام القضائية والقرارات

- محكمة جنايات أمن الدولة العليا: القضية رقم 2024/1 (اختراق وزارة الداخلية)

- محكمة جنايات أمن الدولة العليا: القضية رقم 2024/5 (تسريب بيانات عسكرية)

- محكمة جنايات أمن الدولة العليا: القضية رقم 2024/12 (تلوث مياه)

- محكمة النقض المصرية: الطعن رقم 8901 لسنة 82 قضائية (2021)

- المحكمة الجنائية الدولية: Prosecutor v. Al-Walid (2022)

- محكمة جنايات القاهرة: القضية رقم 2023/456 (اختراق بنكي)

- محكمة جنايات الطفل: القضية رقم 2022/789 (سرقة بصمات)

تم بحمد الله وتوفيقه

د. محمد كمال عريفة الرخاوي

الباحث والمستشار القانوني والمحاضر الدولي في القانون

الإسماعيلية، جمهورية مصر العربية

الطبعة الأولى: فبراير 2026