الحماية الجنائية والمدنية لاختراق المواقع والحسابات الإلكترونية

تأليف: د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون

الإهداء

إلى روح أمي وأبي الطاهرة

داعيا الله لهم بالرحمة والمغفرة والفردوس الأعلى يا رب العالمين

وإلى ابنتي الحبيبة قرة عيني صبرينال المصرية الجزائرية

جميلة الجميلات التي تجمع جمال وسحر نهر النيل الخالد وجمال شط المتوسط وجبال الأوراس الشامخة وعظمة الجسور المعلقة

داعيا الله لها بالحفظ والبركة والخير والصحة والعافية

التقديم

يشهد العصر الرقمي الحالي تصاعداً غير مسبوق في جرائم اختراق المواقع والحسابات الإلكترونية، مما يستدعي وقفة قانونية فقهية عميقة لتحليل آليات الحماية الجنائية والمدنية المتاحة لمواجهة هذه الظاهرة. يأتي هذا العمل القانوني المتخصص كمرجع شامل يغوص في أعماق النظم القانونية المقارنة، مقدماً دراسة تحليلية للمسؤولية الجنائية للمخترقين والمسؤولية المدنية لمقدمي الخدمات والمواقع في حال الإخلال بأمن البيانات. إن الهدف من هذا الكتاب ليس فقط سرد النصوص العقابية، بل تفكيك البنية

القانونية للحماية، وكيفية إثبات الضرر، وتقدير التعويضات، وآليات التعاون الدولي في ملاحقة مجرمي الإنترنت. إننا أمام حاجة ماسة لفهم كيف تتوازن التشريعات بين زجر الجناة وتعويض الضحايا، مع الحفاظ على حرية التداول الرقمي. إن هذا الكتاب موجه للمحامين، والقضاة، ومختصي الأمن السيبراني، وصناع السياسات، ليكون دليلاً استرشادياً في بناء منظومة قانونية رادعة وعادلة، نسأل الله أن يجعل هذا الجهد خالصاً لوجهه الكريم، ونفعاً للعلم والعلماء.

د. محمد كمال عرفه الرخاوي

القسم الأول: الإطار العام لجرائم الاختراق الإلكتروني

الفصل الأول: المفهوم القانوني للاختراق الإلكتروني وأنواعه

يستهل هذا الفصل بتأسيس تعريف قانوني دقيق

لجريمة الاختراق الإلكتروني، متميزاً عن التعريف التقني، حيث يركز على عنصر التعدي على حرمة الأنظمة المعلوماتية. يتم تحليل أنواع الاختراق، من الدخول غير المصرح به إلى المواقع، إلى الاستيلاء على الحسابات الشخصية، وصولاً إلى التعديل على البيانات. يناقش الفصل التمييز بين الاختراق بدافع الفضول، وبدافع الربح، وبدافع التخريب، وكيف يؤثر الدافع على التكييف القانوني للجريمة. يتم دراسة عناصر الجريمة المادية والمعنوية، وركن الخطأ في البيئة الرقمية، مع استعراض الفقه القانوني حول اعتبار البيانات كمال محمي قانوناً. كما يتطرق الفصل إلى التطور التاريخي لتجريم الاختراق، وكيف انتقلت التشريعات من التجريم العام إلى نصوص خاصة بالجرائم الإلكترونية.

الفصل الثاني: محل الحماية القانونية في الجرائم الإلكترونية

يركز هذا الفصل على تحديد الحق القانوني الذي تحميه النصوص العقابية في جرائم الاختراق. يتم

تحليل ما إذا كان المحل هو الحق في الملكية الفكرية، أم الحق في الخصوصية، أم أمن المعلومات القومي. يناقش الفصل حماية البيانات الشخصية كحق أساسي من حقوق الإنسان، وكيف أن اختراق الحسابات يعد انتهاكاً لهذا الحق. يتم دراسة حماية الأموال الرقمية والعملات المشفرة ضمن نطاق الحماية القانونية للمال. كما يتطرق الفصل إلى حماية السمعة التجارية للمواقع الإلكترونية، وكيف أن اختراق موقع شركة يعد اعتداءً على كيانه الاعتباري، مع مقارنة بين النظم القانونية التي تحمي البيانات كملكية خاصة وتلك التي تحميها كحق شخصي.

الفصل الثالث: الجوانب التقنية للاختراق وأثرها على التكييف القانوني

يستعرض هذا الفصل العلاقة المعقدة بين التقنية والقانون، وكيف يفهم القاضي الآلية التقنية لتطبيق النص الجنائي. يتم تحليل طرق الاختراق الشائعة مثل التصيد الاحتيالي، وهجمات القوة الغاشمة، وثغرات البرمجيات، وكيفية وصفها في محاضر الضبط القضائي.

يناقش الفصل صعوبة إثبات النية الجنائية في ظل استخدام أدوات اختراق متاحة للعموم، وهل يعد possession الأدوات جريمة بحد ذاتها. يتم دراسة دور الخبراء الفنيين في شرح آلية الاختراق للمحكمة، لغة بسيطة تخلو من الغموض. كما يتطرق الفصل إلى إشكالية التشفير وإخفاء الهوية، وكيف تؤثر على قدرة السلطات على تحديد الجاني وتكييف فعله قانوناً بدقة.

الفصل الرابع: الاختصاص القضائي في جرائم الاختراق عابرة الحدود

يركز هذا الفصل على إحدى أكبر التحديات القانونية، وهي الطبيعة العابرة للحدود لجرائم الاختراق. يتم تحليل قواعد الاختصاص المكاني، وهل تختص محكمة مكان الجاني، أم مكان الضحية، أم مكان الخادم server. يناقش الفصل تعارض القوانين بين الدول، وكيف قد يكون الفعل مجرماً في دولة ومباحاً في أخرى. يتم دراسة مبادئ الاختصاص العالمي في الجرائم السيبرانية الخطيرة، والاتفاقيات الدولية التي

تنظم التعاون القضائي. كما يتطرق الفصل إلى صعوبة تنفيذ الأحكام الصادرة في دولة أخرى، وآليات الاعتراف المتبادل بالأحكام الجنائية والمدنية في الفضاء السيبراني.

الفصل الخامس: المسؤولية الجنائية للشخصيات الاعتبارية في الاختراق

يستعرض هذا الفصل مدى مسؤولية الشركات والمؤسسات عن جرائم الاختراق التي تتم من خلالها أو باستغلال أنظمتها. يتم تحليل نظرية مسؤولية الشخص الاعتباري في القانون الجنائي، وشروط تطبيقها على جرائم الإنترنت. يناقش الفصل مسؤولية شركة الاستضافة عن مواقع تُستخدم للاختراق، ومسؤولية منصة التواصل عن اختراق حسابات مستخدميها. يتم دراسة إجراءات الامتثال والرقابة الداخلية كسبب من أسباب الإعفاء من المسؤولية الجنائية. كما يتطرق الفصل إلى العقوبات المقررة على الأشخاص الاعتبارية، مثل الغرامات المالية الضخمة، وحل الشركة، ومنع مزاولة النشاط، مع تحليل فعاليتها

الرادعة.

القسم الثاني: الحماية الجنائية وزجر الجناة

الفصل السادس: تجريم الدخول غير المصرح به إلى الأنظمة المعلوماتية

يغوص هذا الفصل في النصوص العقابية الخاصة بالدخول غير المشروع، كأحد أركان جريمة الاختراق الأساسية. يتم تحليل مفهوم الإذن، وهل يكون صريحاً أم ضمنياً، ومتى يسقط هذا الإذن. يناقش الفصل العقوبات السالبة للحرية المقررة لهذه الجريمة، ومدى كفايتها للردع في ظل الخطورة المتزايدة. يتم دراسة الظروف المشددة للعقوبة، مثل إذا كان الاختراق موجهاً ضد أنظمة حكومية أو بنوك. كما يتطرق الفصل إلى محاولة الدخول غير المصرح به، وهل تعتبر جريمة كاملة أم محاولة يعاقب عليها، مع استعراض الاجتهادات القضائية حول بدء التنفيذ في البيئة الرقمية.

الفصل السابع: تجريم الاستيلاء على البيانات وسرقة الهوية

يركز هذا الفصل على جرائم سرقة البيانات الشخصية واستخدامها في انتحال الشخصية. يتم تحليل النصوص القانونية التي تجرم الحصول على بيانات دون وجه حق، ونقلها، أو تخزينها. يناقش الفصل جريمة انتحال الهوية الإلكترونية، والآثار الجنائية المترتب عليها مثل الاحتيال المالي أو التشهير. يتم دراسة حماية البيانات الحيوية Biometric Data، وخصوصية المعاقبة على سرقتها. كما يتطرق الفصل إلى تجريم الاتجار في البيانات المسروقة في الأسواق السوداء على الشبكة المظلمة، وآليات ملاحقة المتاجرين بها جنائياً عبر الحدود.

الفصل الثامن: تجريم التعديل والتخريب في المواقع والحسابات

يستعرض هذا الفصل الجرائم التي تتجاوز الدخول إلى مرحلة التدمير أو التعديل. يتم تحليل تجريم حذف البيانات، أو تشفيرها طلباً للفدية Ransomware، أو تعديل المحتوى تشويهاً للسمعة. يناقش الفصل الفرق بين التخريب المادي للأجهزة والتخريب المنطقي للبيانات، من حيث العقوبة. يتم دراسة جريمة تعطيل الخدمات Denial of Service، واعتبارها شكلاً من أشكال التخريب الاقتصادي. كما يتطرق الفصل إلى المسؤولية الجنائية عن نشر البرمجيات الخبيثة التي تستخدم في التخريب، وسلسلة المسؤولية من المبرمج إلى المستخدم النهائي.

الفصل التاسع: العقوبات التكميلية والتدابير الاحترازية في الجرائم الإلكترونية

يركز هذا الفصل على العقوبات غير السالبة للحرية التي تهدف إلى منع العود وحماية المجتمع. يتم تحليل مصادرة الأجهزة المستخدمة في الجريمة، وإغلاق المواقع الإلكترونية المخالفة. يناقش الفصل حظر مزاولة نشاط معين متعلق بالإنترنت، ومنع السفر في

الجرائم عابرة الحدود. يتم دراسة نشر الحكم في الصحف الإلكترونية على نفقة المحكوم عليه كعقوبة تشهيرية رادعة. كما يتطرق الفصل إلى التدابير الاحترازية مثل المراقبة الإلكترونية للجناة بعد الإفراج عنهم، وضمانات عدم عودتهم لممارسة الاختراق، مع تقييم فعالية هذه التدابير في الواقع العملي.

الفصل العاشر: التعاون الدولي في الملاحقة الجنائية لمخترقي المواقع

يستعرض هذا الفصل آليات العمل المشترك بين الدول لمواجهة جريمة الاختراق. يتم تحليل دور الإنتربول ويوروبول في تنسيق العمليات المشتركة ضد شبكات الاختراق. يناقش الفصل اتفاقيات التسليم экстрадиция للمجرمين الإلكترونيين، والمعوقات السياسية والقانونية التي تواجهها. يتم دراسة تبادل الأدلة الرقمية بين السلطات القضائية، وضمانات قبولها أمام المحاكم الوطنية. كما يتطرق الفصل إلى إنشاء نيابات متخصصة في الجرائم الإلكترونية ذات اختصاص دولي، ومقترحات لإنشاء محكمة جنائية دولية

متخصصة في الجرائم السيبرانية الخطيرة التي تهدد الأمن العالمي.

القسم الثالث: الحماية المدنية وتعويض الضحايا

الفصل الحادي عشر: المسؤولية المدنية عن اختراق المواقع والحسابات

يبدأ هذا القسم بالتحليل القانوني لأسس المسؤولية المدنية الناشئة عن حوادث الاختراق. يتم تحليل نظرية الخطأ التقصيري، وكيف يثبت ضرر الاختراق وعلاقته السببية بفعل الجاني أو إهمال الموقع. يناقش الفصل المسؤولية العقدية لمقدمي الخدمات الذين يلتزمون بتأمين بيانات العملاء، وخرقهم لهذا الالتزام. يتم دراسة نظرية المخاطر في البيئة الرقمية، ومدى تطبيقها لإلزام الشركات بالتعويض حتى دون خطأ مثبت. كما يتطرق الفصل إلى تعدد المسؤولين مدنياً، الجاني المباشر وشركة الاستضافة، وكيفية توزيع التعويض بينهم بالتضامن أو على سبيل الانفراد.

الفصل الثاني عشر: عناصر المسؤولية المدنية الضرر والخطأ والسببية

يركز هذا الفصل على تفكيك أركان المسؤولية المدنية في قضايا الاختراق بدقة. يتم تحليل مفهوم الضرر الرقمي، هل هو مادي فقط أم يشمل الضرر المعنوي والسمعة. يناقش الفصل صعوبة إثبات العلاقة السببية في البيئة المعقدة، خاصة مع وجود ثغرات متعددة. يتم دراسة عبء الإثبات، وهل ينقلب على مقدم الخدمة في حال عدم توفر معايير الأمن القياسية. كما يتطرق الفصل إلى الضرر المستقبلي والمحتمل، مثل استخدام البيانات المسروقة في جرائم لاحقة، وكيفية التعويض عن خطر وقوعها، مع استعراض معايير تقدير الضرر في القضاء المقارن.

الفصل الثالث عشر: التعويضات المالية عن الأضرار المادية والمعنوية

يستعرض هذا الفصل معايير تقدير التعويضات في أحكام التعويض عن الاختراق. يتم تحليل طرق حساب الخسائر المباشرة، مثل الأموال المسروقة، وتكاليف استعادة الأنظمة. يناقش الفصل التعويض عن الأضرار المعنوية، مثل القلق، وانتهاك الخصوصية، والضرر بالسمعة التجارية. يتم دراسة التعويضات العقابية Punitive Damages في بعض التشريعات، ودورها في ردع الشركات المقصرة. كما يتطرق الفصل إلى فوائد التأخير على مبالغ التعويض، وآليات تنفيذ الأحكام التعويضية ضد الجناة عديمي الملاءة أو الشركات المفلسة.

الفصل الرابع عشر: مسؤولية مقدمي خدمات الإنترنت ومنصات التواصل

يركز هذا الفصل على المسؤولية المدنية للوسطاء التقنيين عن اختراقات تحدث عبر منصاتهم. يتم تحليل مبدأ الملاذ الآمن Safe Harbor، ومتى يفقد مقدم الخدمة هذه الحماية. يناقش الفصل واجب الرقابة على المحتوى، والإبلاغ عن الثغرات، وإشعار

المستخدمين بالاختراقات. يتم دراسة شروط الإعفاء من المسؤولية، مثل الاستجابة السريعة لإشعارات الإزالة Notice and Takedown. كما يتطرق الفصل إلى البنود الإعفائية في عقود الاستخدام، ومدى حجية هذه البنود في إسقاط حق المستخدم في المطالبة بالتعويض عن إهمال المنصة في تأمين حسابه.

الفصل الخامس عشر: التأمين السيبراني كأداة للتعويض المدني

يستعرض هذا الفصل دور عقود التأمين في تغطية أضرار اختراق المواقع والحسابات. يتم تحليل أنواع التغطيات التأمينية، مثل مسؤولية البيانات، وتكاليف الاستجابة للحوادث. يناقش الفصل شروط استحقاق التعويض التأميني، وإثبات وقوع الحادث وفق شروط البوليصة. يتم دراسة استثناءات التغطية، مثل الحروب السيبرانية، أو الإهمال الجسيم من المؤمن له. كما يتطرق الفصل إلى نزاعات التعويض بين شركات التأمين والشركات المؤمنة، ودور الخبراء في تقدير الخسائر المؤمن عليها، مع تحليل لسوق التأمين

السيبراني الناشئ كضمان مالي للضحايا.

القسم الرابع: الإجراءات والإثبات والمستقبل

الفصل السادس عشر: إجراءات الضبط القضائي وجمع الأدلة الرقمية

يغوص هذا الفصل في الإجراءات القانونية اللازمة لضبط جرائم الاختراق بشكل صحيح. يتم تحليل صلاحيات رجال الضبط القضائي في دخول الأنظمة ومصادرة الأجهزة. يناقش الفصل قواعد سلسلة الحراسة Chain of Custody للأدلة الرقمية، لضمان عدم تلوثها. يتم دراسة التفتيش عن بعد للأنظمة المعلوماتية، والضمانات القانونية لحماية الخصوصية أثناء التفتيش. كما يتطرق الفصل إلى حجز النطاقات الإلكترونية وإغلاق المواقع مؤقتاً لحين الفصل في الدعوى، والتوازن بين ضرورة الحفظ وحقوق التشغيل القانونية.

الفصل السابع عشر: حجية الأدلة الإلكترونية في الإثبات الجنائي والمدني

يركز هذا الفصل على قوة إثبات الأدلة الرقمية أمام المحاكم. يتم تحليل معايير قبول سجلات الخوادم Logs، ورسائل البريد الإلكتروني، ولقطات الشاشة. يناقش الفصل التوقيع الإلكتروني، والختم الزمني، ودور جهات التصديق في تعزيز حجية الأدلة. يتم دراسة الخبرة الفنية في استخراج وتحليل الأدلة، report_ الخبير كدليل رئيسي. كما يتطرق الفصل إلى التحديات القانونية للأدلة المستخرجة من تقنيات التشفير والعملات الرقمية، وكيفية توثيقها بما يرضي القاضي ويحقق اليقين القضائي.

الفصل الثامن عشر: التسوية والوساطة في منازعات الاختراق الإلكتروني

يستعرض هذا الفصل البدائل الودية لحل منازعات الاختراق دون اللجوء للقضاء الطويل. يتم تحليل اتفاقيات التسوية بين الشركات المخترقة والمخترقين

White Hat Hackers في برامج المكافآت. يناقش الفصل الوساطة في المنازعات المدنية للتعويض، وسرعة إنصاف الضحايا. يتم دراسة السرية في اتفاقيات التسوية، وحماية سمعة الشركات من العلانية السلبية. كما يتطرق الفصل إلى دور مراكز التحكيم الدولية المتخصصة في المنازعات التقنية، ومزاياها في السرعة والفهم التقني مقارنة بالمحاكم التقليدية، مع ضوابط العدالة في هذه الاتفاقيات.

الفصل التاسع عشر: الوقاية القانونية ومتطلبات الامتثال الأمني

يركز هذا الفصل على الجانب الوقائي، وكيف يقلل الامتثال القانوني من المسؤولية. يتم تحليل معايير الأمن السيبراني الإلزامية مثل ISO 27001، وأثرها في نفي الخطأ. يناقش الفصل واجب الإخطار القانوني عند وقوع الاختراق للجهات الرقابية والعملاء. يتم دراسة برامج الامتثال الداخلي، وتدريب الموظفين، كدرع قانوني للشركات. كما يتطرق الفصل إلى المسؤولية الشخصية لمديري الأمن CISO في حال

الإهمال، وضرورة توثيق إجراءات الحماية لتجنب المساءلة القانونية الجنائية والمدنية لاحقاً.

الفصل العشرون: الرؤية المستقبلية لتشريعات الحماية من الاختراق

يختتم هذا الفصل برؤية استشرافية لتطور الحماية القانونية مع تطور التقنية. يتم تحليل تأثير الذكاء الاصطناعي على طرق الاختراق والدفاع، والحاجة لتشريعات مرنة. يناقش الفصل حماية الحسابات في عالم الميتافيرس والإنترنت الجديد، والهوية الرقمية الموحدة. يتم دراسة الحاجة لاتفاقية دولية شاملة للجرائم السيبرانية تحت مظلة الأمم المتحدة. كما يتطرق الفصل إلى التوصيات النهائية للمشرع لتعزيز الحماية، وللقضاء في تفسير النصوص، مختتماً بأن الحماية القانونية هي شريك استراتيجي للحماية التقنية في بناء ثقة المجتمع الرقمي.

الختام

بهذا نصل إلى ختام هذا العمل القانوني المتخصص، الذي حاولنا فيه رصد آليات الحماية الجنائية والمدنية لمواجهة جرائم اختراق المواقع والحسابات الإلكترونية. إن ما تم عرضه في الفصول العشرين يؤكد أن الحماية الفعالة تتطلب تكاملاً بين النصوص العقابية الرادعة، وأنظمة التعويض العادلة، وإجراءات إثبات تقنية دقيقة. إن الرسالة التي يود المؤلف إيصالها هي أن الأمن السيبراني ليس مسؤولية تقنية فقط، بل هو التزام قانوني وأخلاقي يحمي الحقوق والحريات في الفضاء الرقمي. إن تطوير التشريعات ومواكبة التطور التقني هو الضمان الوحيد لتحقيق العدالة الرقمية. نسأل الله تعالى أن يكون هذا العمل قد وفق في تقديم إضافة علمية وعملية حقيقية، وأن ينفع به المحامين والقضاة والمختصين، وأن يجعله في ميزان حسنات الوالدين صبرينال. والحمد لله رب العالمين أولاً وآخراً.

الفهرس الموضوعي

الفصل الأول: المفهوم القانوني للاختراق الإلكتروني وأنواعه

الفصل الثاني: محل الحماية القانونية في الجرائم الإلكترونية

الفصل الثالث: الجوانب التقنية للاختراق وأثرها على التكييف القانوني

الفصل الرابع: الاختصاص القضائي في جرائم الاختراق عابرة الحدود

الفصل الخامس: المسؤولية الجنائية للشخصيات الاعتبارية في الاختراق

الفصل السادس: تجريم الدخول غير المصرح به إلى الأنظمة المعلوماتية

الفصل السابع: تجريم الاستيلاء على البيانات وسرقة الهوية

الفصل الخامس عشر: التأمين السيبراني كأداة للتعويض المدني

الفصل السادس عشر: إجراءات الضبط القضائي وجمع الأدلة الرقمية

الفصل السابع عشر: حجية الأدلة الإلكترونية في الإثبات الجنائي والمدني

الفصل الثامن عشر: التسوية والوساطة في منازعات الاختراق الإلكتروني

الفصل التاسع عشر: الوقاية القانونية ومتطلبات الامتثال الأمني

الفصل العشرون: الرؤية المستقبلية لتشريعات الحماية من الاختراق

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني
والمحاضر الدولي في القانون