جرائم الإنترنت والتقنية: الحماية الجنائية في العصر الرقمي - دراسة مقارنة في التشريعات المصرية والجزائرية والفرنسية

تأليف د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون

الاهداء

الى روح امي وابي الطاهره داعيا لهم الله بالرحمه والمغفره والفردوس الاعلي يارب العالمين

والي ابنتي الحبيبه قره عيني صابرينال المصرية الجزائرية جميلة الجميلات التي تجمع بين جمال نهر

النيل الخالد وعظمه الاهرامات وجمال شط المتوسط وجبال الأوراس الشامخة داعيا الله لها بالصحه والخير والسعاده والبركه يارب العالمين

الفهرس

المقدمة

الفصل الأول مفهوم جرائم الإنترنت والتقنية وأبعادها القانونية

الفصل الثاني التطور التشريعي لمكافحة الجرائم الإلكترونية في الأنظمة المقارنة

الفصل الثالث جريمة الابتزاز الإلكتروني: الأركان والعقوبات

الفصل الرابع السب والقذف عبر منصات التواصل الاجتماعي فيسبوك وتويتر

الفصل الخامس اختراق الحسابات الشخصية: الجرائم والعقوبات

الفصل السادس نشر الأخبار الكاذبة والمعلومات المضللة: التجريم والمسؤولية

الفصل السابع إجراءات الضبط والتحقيق في الجرائم الإلكترونية

الفصل الثامن الأدلة الرقمية وقواعد الإثبات في الجرائم التقنية

الفصل التاسع الاختصاص القضائي في الجرائم الإلكترونية العابرة للحدود

الفصل العاشر حماية ضحايا الجرائم الإلكترونية: الآليات القانونية

الفصل الحادي عشر العقوبات المقررة للجرائم الإلكترونية في التشريعات المقارنة

الفصل الثاني عشر التدابير الوقائية والعلاجية في مكافحة الجرائم التقنية

الفصل الثالث عشر مسؤولية مقدمي خدمات الإنترنت ومنصات التواصل

الفصل الرابع عشر حقوق الخصوصية وحماية البيانات في مواجهة الجرائم الإلكترونية

الفصل الخامس عشر جرائم الإنترنت ضد الأطفال: الحماية الجنائية الخاصة

الفصل السادس عشر الجرائم الإلكترونية الاقتصادية والاحتيال الرقمي

الفصل السابع عشر الجرائم الإلكترونية والإرهاب السيبراني: الأبعاد الأمنية

الفصل الثامن عشر التوعية الرقمية والوقاية من الجرائم الإلكترونية

الفصل التاسع عشر التعاون الدولي في مكافحة الجرائم الإلكترونية

الفصل العشرون نحو تشريع عربي موحد للجرائم الإلكترونية: رؤية مستقبلية

الختام

المقدمة

تشهد الجريمة في العصر الرقمي تحولات جذرية غير مسبوقة حيث انتقلت من الفضاء المادي إلى الفضاء الافتراضي مما أوجد أنواعاً جديدة من الجرائم تتسم بالتعقيد التقني والعابرة للحدود الجغرافية فإن جرائم الإنترنت والتقنية تشمل طيفاً واسعاً من الأفعال الإجرامية مثل الابتزاز الإلكتروني والسب والقذف عبر منصات التواصل الاجتماعي واختراق الحسابات الشخصية ونشر الأخبار الكاذبة التي تهدد الأمن

الفردي والمجتمعي على حد سواء وتثير هذه الجرائم تحديات قانونية معقدة تتعلق بالإثبات الرقمي والاختصاص القضائي وحماية الضحايا في بيئة لا تعترف بالحدود التقليدية ومن هنا تأتي أهمية هذا الكتاب الذي يسعى إلى تحليل معمق للحماية الجنائية من جرائم الإنترنت والتقنية في التشريعات المصرية والجزائرية والفرنسية بهدف كشف أوجه الاتفاق والاختلاف وتقييم كفاءة الآليات القانونية في الردع والعقاب وجبر الضرر فإننا أمام حاجة ماسة لفهم كيفية تعامل القضاء والنيابة في هذه الدول مع الجرائم الإلكترونية في ظل التطور التقني المتسارع والتحديات المعاصرة مثل التشفير والذكاء الاصطناعي والعملات الرقمية وهذا الكتاب هو محاولة جادة لتقديم مرجع قانوني وتقني متكامل يخدم الباحثين والقضاة والمحامين وأجهزة الضبط في فهم ديناميكيات الجرائم الإلكترونية لتحقيق العدالة الرقمية الفعالة في عالم يتسم بالترابط التقني غير المسبوق والذي يتطلب وعياً عميقاً بالأبعاد المختلفة للجريمة الإلكترونية وسبل مكافحتها

الفصل الأول

مفهوم جرائم الإنترنت والتقنية وأبعادها القانونية

تُعرف جرائم الإنترنت والتقنية بأنها كل فعل إجرامي يرتكب باستخدام الحواسيب أو الشبكات الإلكترونية أو يستهدف الأنظمة المعلوماتية مما يسبب ضرراً للأفراد أو المؤسسات أو الدول فإن هذه الجرائم تتسم بخصائص فريدة مثل اللامادية والعابرة للحدود والصعوبة التقنية في الكشف والإثبات وتختلف التصنيفات الفقهية لهذه الجرائم فمنها ما يصنفها حسب الوسيلة المستخدمة مثل جرائم الاختراق والتشويش ومنها ما يصنفها حسب الهدف مثل الجرائم المالية أو الجرائم ضد الأشخاص وتظهر الأبعاد القانونية لهذه الجرائم في ضرورة تطوير نصوص تجرم الأفعال الإلكترونية بشكل صريح مع الحفاظ على التوازن بين مكافحة الجريمة وحماية الحريات الرقمية وتختلف التشريعات في تعريف الجرائم الإلكترونية ففي فرنسا يعتمد القانون على نصوص متخصصة في الجرائم المعلوماتية بينما في مصر والجزائر توجد قوانين خاصة بالجرائم الإلكترونية

مع نصوص متفرقة في القوانين الجنائية العامة وإن فهم مفهوم الجرائم الإلكترونية بدقة هو المدخل الصحيح لتطبيق الحماية الجنائية الفعالة التي تواكب التطور التقني دون المساس بالحقوق والحريات الأساسية في الفضاء الرقمي

الفصل الثاني

التطور التشريعي لمكافحة الجرائم الإلكترونية في الأنظمة المقارنة

شهدت التشريعات المقارنة تطوراً ملحوظاً في مكافحة الجرائم الإلكترونية استجابة للتحديات التقنية المتزايدة ففي فرنسا صدر قانون الثقة في الاقتصاد الرقمي عام 2004 ثم تعديلات متتالية لتعزيز الحماية من الجرائم الإلكترونية وفي مصر صدر قانون مكافحة جرائم تقنية المعلومات عام 2018 الذي جرم أفعالاً مثل الاختراق والابتزاز الإلكتروني ونشر الأخبار الكاذبة وفي الجزائر صدر القانون 18-05 المتعلق بالجرائم

الإلكترونية عام 2018 الذي نظم التجريم والعقاب في هذا المجال وتظهر أهمية التطور التشريعي في مواكبة الأساليب الإجرامية المتطورة وتوفير أدوات قانونية فعالة لأجهزة العدالة وإن الدروس المستفادة تشير إلى ضرورة المرونة التشريعية التي تسمح بتكييف النصوص مع المستجدات التقنية دون الحاجة لتعديلات متكررة وإن التحديث المستمر للتشريعات الإلكترونية يتطلب مشاركة خبراء التقنية في الصياغة القانونية لضمان دقة التجريم وفعالية العقوبات في الردع والعقاب

الفصل الثالث

جريمة الابتزاز الإلكتروني: الأركان والعقوبات

تُعد جريمة الابتزاز الإلكتروني من أخطر الجرائم التقنية حيث يستخدم الجاني الوسائل الإلكترونية لتهديد الضحية بكشف معلومات خاصة أو صور محرجة مقابل مبالغ مالية أو منافع أخرى فإن أركان هذه الجريمة

تتمثل في ركن مادي يتمثل في استخدام الوسيلة الإلكترونية للتهديد وركن معنوي يتمثل في القصد الجنائي للحصول على منفعة غير مشروعة وتختلف العقوبات المقررة لهذه الجريمة بين الدول ففي فرنسا تصل العقوبة للسجن سبع سنوات وغرامة كبيرة بينما في مصر تصل للسجن المشدد والغرامة وفي الجزائر تتراوح بين الحبس والغرامة مع ظروف مشددة وتظهر أهمية تجريم الابتزاز الإلكتروني صراحة في توفير حماية فعالة للضحايا وتشجيعهم على الإبلاغ دون خوف من الفضيحة وإن إثبات هذه الجريمة يتطلب جمع أدلة رقمية دقيقة مثل سجلات المحادثات وعناوين الـ IP مما يستدعي كفاءات تقنية متخصصة في أجهزة الضبط والتحقيق

الفصل الرابع

السب والقذف عبر منصات التواصل الاجتماعي فيسبوك وتويتر

يشهد الفضاء الرقمي انتشاراً واسعاً لجرائم السب والقذف عبر منصات التواصل الاجتماعي مثل فيسبوك وتويتر إكس حيث يستخدم الجناة هذه المنصات لنشر عبارات مسيئة أو اتهامات كاذبة تضر بسمعة الأفراد والمؤسسات فإن التجريم القانوني لهذه الأفعال يتطلب تكييفاً دقيقاً يوازن بين حرية التعبير وحماية الشرف والسمعة وتختلف المعالجة القانونية بين الدول ففي فرنسا يميز القانون بين القذف العلني والسب البسيط بعقوبات متفاوتة بينما في مصر والجزائر توجد نصوص في قوانين العقوبات وقوانين الجرائم الإلكترونية تجرم هذه الأفعال عبر الوسائل الإلكترونية وتظهر التحديات الإثباتية في تحديد هوية الجاني خلف الحسابات الوهمية وحفظ الأدلة الرقمية قبل حذفها وإن فعالية المكافحة تتطلب تعاوناً مع شركات المنصات لإزالة المحتوى المسيء وتحديد هويات المستخدمين المخالفين وإن التوعية بمخاطر النشر المسيء عبر الإنترنت هي خط دفاع أولي لمنع هذه الجرائم قبل وقوعها

الفصل الخامس

اختراق الحسابات الشخصية: الجرائم والعقوبات

يُعد اختراق الحسابات الشخصية جريمة تقنية خطيرة تنتهك خصوصية الأفراد وتستهدف بياناتهم الحساسة حيث يستخدم الجناة تقنيات متطورة مثل التصيد والبرمجيات الخبيثة للوصول غير المصرح به للحسابات فإن أركان هذه الجريمة تتمثل في الدخول غير المشروع لنظام معلوماتي والبقاء فيه أو استخراج بيانات منه بقصد الإجرام وتختلف العقوبات بين الدول ففي فرنسا يعاقب على الاختراق بالسجن والغرامة مع ظروف مشددة إذا ترتب على الاختراق ضرر جسيم وفي مصر والجزائر تجرم قوانين الجرائم الإلكترونية الاختراق بعقوبات رادعة وتظهر أهمية حماية الحسابات الشخصية في العصر الرقمي حيث أصبحت بوابة للوصول للبيانات المالية والشخصية الحساسة وإن الوقاية من الاختراق تتطلب وعياً تقنياً من المستخدمين بتفعيل المصادقة الثنائية وتحديث كلمات المرور وإن تطوير قدرات أجهزة الضبط في تتبع المخترقين هو مفتاح نجاح المكافحة الجنائية لهذه

الفصل السادس

نشر الأخبار الكاذبة والمعلومات المضللة: التجريم والمسؤولية

يشهد العصر الرقمي انتشاراً واسعاً للأخبار الكاذبة والمعلومات المضللة عبر المنصات الإلكترونية مما يهدد الأمن المجتمعي والاستقرار السياسي فإن التجريم القانوني لهذه الأفعال يتطلب دقة في التعريف لتجنب المساس بحرية الرأي والتعبير المشروعة وتختلف التشريعات في معالجة هذه الظاهرة ففي فرنسا جرم القانون نشر المعلومات الكاذبة بقصد الإضرار خلال الفترات الانتخابية بينما في مصر والجزائر تجرم قوانين الجرائم الإلكترونية نشر الأخبار الكاذبة التي تثير الذعر أو تضر بالمصلحة العامة وتظهر التحديات في التمييز بين الخبر الكاذذ المتعمد والخطأ غير المقصود في النشر وإن إثبات القصد الجنائي في هذه الجرائم

يتطلب تحليلاً دقيقاً لظروف النشر ودوافع الناشر وإن الموازنة بين مكافحة الأخبار الكاذبة وحماية حرية الإعلام تتطلب معايير واضحة وشفافة لتجنب الاستخدام السياسي للنصوص التجريمية

الفصل السابع

إجراءات الضبط والتحقيق في الجرائم الإلكترونية

تخضع إجراءات الضبط والتحقيق في الجرائم الإلكترونية لضوابط تقنية خاصة تختلف عن الجرائم التقليدية حيث تتطلب كفاءات متخصصة في جمع الأدلة الرقمية وحفظها بشكل يضمن صحتها أمام القضاء فإن الضبط القضائي الإلكتروني يشمل حجز الأجهزة وتحليل البيانات واستخراج سجلات الاتصال مع احترام ضمانات الخصوصية وتختلف الإجراءات بين الدول ففي فرنسا توجد وحدات متخصصة في الجرائم الإلكترونية ضمن الشرطة القضائية بينما في مصر والجزائر تتطور الوحدات المتخصصة تدريجياً وتظهر أهمية البروتوكولات

الموحدة للضبط الرقمي في ضمان قبول الأدلة أمام المحاكم وإن تدريب رجال الضبط على التقنيات الحديثة هو استثمار في فعالية التحقيقات وإن التعاون مع شركات التقنية للحصول على بيانات المستخدمين يجب أن يخضع لضوابط قانونية صارمة تحمي الحقوق الأساسية

الفصل الثامن

الأدلة الرقمية وقواعد الإثبات في الجرائم التقنية

تُعد الأدلة الرقمية من أهم عناصر الإثبات في الجرائم الإلكترونية حيث تشمل سجلات الخوادم ورسائل البريد الإلكتروني ومحادثات التطبيقات وبيانات الموقع الجغرافي فإن قبول هذه الأدلة أمام القضاء يتطلب ضمانات فنية وقانونية تثبت أصالتها وعدم التلاعب بها وتختلف معايير قبول الأدلة الرقمية بين الدول ففي فرنسا تعترف المحاكم بالأدلة الرقمية إذا تم جمعها وفق إجراءات قانونية سليمة بينما في مصر والجزائر

تتطور الممارسات القضائية نحو قبول أوسع للأدلة التقنية وتظهر أهمية سلسلة حفظ الأدلة الرقمية في إثبات صحتها حيث يجب توثيق كل مرحلة من مراحل الجمع والنقل والتحليل وإن الخبراء الفنيين يلعبون دوراً محورياً في تفسير الأدلة الرقمية للمحاكم وإن تطوير قواعد إثبات مرنة تراعي طبيعة الأدلة الرقمية هو ضرورة لتحقيق العدالة في العصر الرقمي

الفصل التاسع

الاختصاص القضائي في الجرائم الإلكترونية العابرة للحدود

تثير الجرائم الإلكترونية إشكاليات معقدة حول الاختصاص القضائي نظراً لطبيعتها العابرة للحدود حيث قد يرتكب الجاني فعله من دولة ويستهدف ضحية في دولة أخرى وتخزن البيانات في خوادم بدولة ثالثة فإن تحديد المحكمة المختصة يتطلب معايير مرنة تأخذ بعين الاعتبار مكان ارتكاب الفعل ومكان وقوع الضرر

وجنسية الأطراف وتختلف المعالجة بين الدول ففي فرنسا يقبل القضاء بالاختصاص إذا وقع الضرر على إقليمها بينما في مصر والجزائر توجد نصوص تحدد قواعد الاختصاص في الجرائم الإلكترونية وتظهر أهمية التعاون القضائي الدولي في حل تنازع الاختصاص وإن مبدأ الاختصاص العالمي في الجرائم الإلكترونية الخطيرة يوسع نطاق الملاحقة الجنائية وإن تطوير معايير موحدة للاختصاص في الجرائم الإلكترونية يسهل الملاحقة الفعالة للجناة عبر الحدود

الفصل العاشر

حماية ضحايا الجرائم الإلكترونية: الآليات القانونية

تستحق ضحايا الجرائم الإلكترونية حماية قانونية خاصة نظراً لطبيعة الضرر الرقمي الذي قد يكون واسع الانتشار وصعب الإصلاح فإن الآليات القانونية للحماية تشمل أوامر إزالة المحتوى المسيء وحظر الاتصال الإلكتروني والتعويض عن الضرر المعنوي والمادي

وتختلف فعالية هذه الآليات بين الدول ففي فرنسا توجد إجراءات عاجلة لإزالة المحتوى عبر المنصات بينما في مصر والجزائر تتطور آليات الحماية تدريجياً وتظهر أهمية توفير قنوات إبلاغ سهلة وآمنة للضحايا لتشجيعهم على اللجوء للعدالة وإن الدعم النفسي والقانوني للضحايا جزء أساسي من منظومة الحماية وإن تطوير أنظمة تعويض سريعة وفعالة يضمن جبر ضرر الضحايا ويعزز ثقتهم في النظام القضائي الرقمي

الفصل الحادي عشر

العقوبات المقررة للجرائم الإلكترونية في التشريعات المقارنة

تتفاوت العقوبات المقررة للجرائم الإلكترونية بين الدول حسب جسامة الفعل وخطورته الاجتماعية ففي فرنسا تتراوح العقوبات بين الغرامات والسجن لسنوات مع ظروف مشددة للجرائم المنظمة أو الموجهة ضد البنى التحتية الحيوية وفي مصر تصل عقوبات بعض

الجرائم الإلكترونية للسجن المشدد والغرامة المالية الكبيرة وفي الجزائر تتراوح العقوبات بين الحبس والغرامة مع مصادرة الأجهزة المستخدمة في الجريمة وتظهر أهمية التناسب بين العقوبة وجسامة الجريمة الإلكترونية في تحقيق الردع الفعال وإن العقوبات المالية وحدها قد لا تكفي لردع الجناة المحترفين مما يستدعي عقوبات سالبة للحرية وإن الجمع بين العقوبات التقليدية والتدابير التقنية مثل حظر استخدام الإنترنت لفترات محددة يخلق نظاماً عقابياً متكاملاً يواكب طبيعة الجرائم الإلكترونية

الفصل الثاني عشر

التدابير الوقائية والعلاجية في مكافحة الجرائم التقنية

إلى جانب العقوبات تتجه التشريعات الحديثة نحو التدابير الوقائية والعلاجية لمنع الجرائم الإلكترونية ومعالجة أسبابها فإن هذه التدابير تشمل برامج التوعية الرقمية للمستخدمين وتعزيز أمن المعلومات

في المؤسسات وبرامج إعادة تأهيل الجناة التقنيين وتختلف التطبيقات بين الدول ففي فرنسا توجد برامج وقائية في المدارس والجامعات بينما في مصر والجزائر تتطور المبادرات الوطنية للتوعية الرقمية وتظهر أهمية الوقاية في تقليل فرص وقوع الجرائم الإلكترونية قبل حدوثها وإن الاستثمار في البنية التحتية للأمن السيبراني يحد من فرص الاختراق وإن برامج إعادة التأهيل للجناة التقنيين تحول مهاراتهم لخدمة المجتمع بدلاً من الإضرار به

الفصل الثالث عشر

مسؤولية مقدمي خدمات الإنترنت ومنصات التواصل

تُعد مسؤولية مقدمي خدمات الإنترنت ومنصات التواصل الاجتماعي من الإشكاليات القانونية المعقدة حيث يثور التساؤل حول مدى مسؤوليتهم عن المحتوى المنشور عبر خدماتهم فإن المبدأ العام في معظم التشريعات هو إعفاء مقدمي الخدمات من

المسؤولية عن محتوى المستخدمين ما لم يكن لديهم علم فعلي بالمحتوى غير القانوني ولم يتحركوا لإزالته وتختلف التطبيقات بين الدول ففي فرنسا يلزم القانون المنصات بإزالة المحتوى غير القانوني خلال مهلة محددة بينما في مصر والجزائر توجد التزامات مشابهة مع تفاوت في التفاصيل وتظهر أهمية توازن المسؤولية بين حماية المستخدمين وعدم تحميل المنصات أعباء رقابية مستحيلة وإن التعاون الطوعي بين السلطات والمنصات في مكافحة الجرائم الإلكترونية يعزز الفعالية دون المساس بحرية التعبير

الفصل الرابع عشر

حقوق الخصوصية وحماية البيانات في مواجهة الجرائم الإلكترونية

يُعد التوازن بين مكافحة الجرائم الإلكترونية وحماية حقوق الخصوصية من التحديات القانونية الكبرى في العصر الرقمي فإن إجراءات التحقيق في الجرائم

الإلكترونية قد تتطلب الوصول لبيانات شخصية حساسة مما يثير مخاوف مشروعة حول انتهاك الخصوصية وتختلف المعالجة بين الدول ففي فرنسا يخضع الوصول للبيانات لرقابة قضائية صارمة بموجب قانون حماية البيانات بينما في مصر والجزائر تتطور الضمانات الإجرائية لحماية الخصوصية وتظهر أهمية مبدأ التناسب في جمع الأدلة الرقمية حيث يجب أن يقتصر الوصول على البيانات الضرورية للتحقيق فقط وإن تعزيز أطر حماية البيانات الشخصية يحد من فرص استغلالها في الجرائم الإلكترونية وإن الرقابة القضائية المستقلة على إجراءات الوصول للبيانات هي ضمانة أساسية لحماية الحقوق في الفضاء الرقمي

الفصل الخامس عشر

جرائم الإنترنت ضد الأطفال: الحماية الجنائية الخاصة

تستهدف الجرائم الإلكترونية الأطفال بشكل خاص نظراً لضعفهم وقلة خبرتهم التقنية مما يستدعي

حماية جنائية مشددة فإن هذه الجرائم تشمل التحرش الإلكتروني والاستغلال الجنسي عبر الإنترنت ونشر محتوى ضار بالقاصرين وتختلف التشريعات في حماية الأطفال ففي فرنسا توجد نصوص خاصة تجرم استغلال الأطفال إلكترونياً بعقوبات مشددة وفي مصر والجزائر تجرم قوانين الجرائم الإلكترونية الأفعال الموجهة ضد الأطفال بعقوبات رادعة وتظهر أهمية التوعية الأسرية والمدرسية في حماية الأطفال من المخاطر الرقمية وإن التعاون مع منصات التواصل لإزالة المحتوى الضار بالقاصرين هو جزء أساسي من الحماية وإن إنشاء وحدات متخصصة للتحقيق في جرائم الإنترنت ضد الأطفال يضمن معالجة حساسة وفعالة لهذه القضايا

الفصل السادس عشر

الجرائم الإلكترونية الاقتصادية والاحتيال الرقمي

تشكل الجرائم الإلكترونية الاقتصادية تهديداً متزايداً

للاستقرار المالي حيث تشمل الاحتيال في المعاملات الإلكترونية وسرقة البيانات المالية والتلاعب بالأنظمة المصرفية فإن هذه الجرائم تتطلب كفاءات تقنية عالية في التحقيق والملاحقة وتختلف العقوبات بين الدول ففي فرنسا تصل عقوبات الاحتيال الإلكتروني للسجن والغرامات الضخمة وفي مصر والجزائر تجرم القوانين هذه الأفعال بعقوبات رادعة تحمي الاقتصاد الرقمي وتظهر أهمية التعاون بين القطاع المالي وأجهزة العدالة في كشف ومنع الجرائم الاقتصادية الإلكترونية وإن تطوير أنظمة دفع إلكتروني آمنة يحد من فرص الاحتيال وإن التوعية بمخاطر المعاملات المالية غير الآمنة عبر الإنترنت هي خط دفاع أولي للمستخدمين

الفصل السابع عشر

الجرائم الإلكترونية والإرهاب السيبراني: الأبعاد الأمنية

تُعد الجرائم الإلكترونية المرتبطة بالإرهاب السيبراني من أخطر التهديدات للأمن الوطني حيث يستخدم

الإرهابيون الفضاء الرقمي للتجنيد والتمويل ونشر الدعاية وتنسيق الهجمات فإن مكافحة هذه الجرائم تتطلب توازناً دقيقاً بين الأمن القومي وحماية الحريات الرقمية وتختلف المعالجة بين الدول ففي فرنسا توجد قوانين استثنائية لمكافحة الإرهاب السيبراني مع ضمانات قضائية وفي مصر والجزائر تعطي القوانين صلاحيات واسعة لأجهزة الأمن مع رقابة قضائية وتظهر أهمية التعاون الدولي في تتبع الشبكات الإرهابية عبر الحدود الرقمية وإن تطوير قدرات الاستخبارات الإلكترونية هو استثمار في الأمن الوطني وإن احترام حقوق الإنسان في مكافحة الإرهاب السيبراني يضمن شرعية الإجراءات وفعاليتها على المدى الطويل

الفصل الثامن عشر

التوعية الرقمية والوقاية من الجرائم الإلكترونية

تُعد التوعية الرقمية من أهم أدوات الوقاية من الجرائم الإلكترونية حيث تمكّن المستخدمين من التعرف على

المخاطر واتخاذ إجراءات وقائية فإن برامج التوعية يجب أن تشمل جميع الفئات العمرية وتتناول مواضيع مثل أمان كلمات المرور والتعرف على محاولات التصيد وحماية البيانات الشخصية وتختلف مبادرات التوعية بين الدول ففي فرنسا توجد حملات وطنية منتظمة بينما في مصر والجزائر تتطور البرامج التوعوية عبر وسائل الإعلام والمدارس وتظهر أهمية الشراكة بين الحكومة والقطاع الخاص والمجتمع المدني في نشر الثقافة الرقمية الآمنة وإن دمج التوعية الرقمية في المناهج التعليمية يضمن جيلاً واعياً بمخاطر الفضاء الرقمي وإن قياس فعالية برامج التوعية وتطويرها باستمرار يضمن وصول الرسالة الوقائية للفئات المستهدفة

الفصل التاسع عشر

التعاون الدولي في مكافحة الجرائم الإلكترونية

نظراً للطبيعة العابرة للحدود للجرائم الإلكترونية

يكتسب التعاون الدولي أهمية قصوى في مكافحتها فإن هذا التعاون يشمل تبادل المعلومات الاستخباراتية وتنسيق التحقيقات وتسليم المجرمين ومساعدة بعضها في جمع الأدلة الرقمية وتختلف آليات التعاون بين الدول فمنها يعتمد على معاهدات ثنائية ومنها على شبكات إقليمية ودولية مثل الإنتربول ويوروبول وتظهر التحديات في اختلاف التشريعات الوطنية حول تعريف الجرائم الإلكترونية وضمانات الإجراءات وإن توحيد المعايير الدنيا للتعاون يسهل الملاحقة الفعالة للجناة عبر الحدود وإن تعزيز قدرات الدول النامية في مكافحة الجرائم الإلكترونية يضمن عدالة عالمية في الفضاء الرقمي

الفصل العشرون

نحو تشريع عربي موحد للجرائم الإلكترونية: رؤية مستقبلية

نصل في هذا الفصل الختامي إلى الدعوة لتشريع

عربي موحد للجرائم الإلكترونية يجمع بين أفضل الممارسات الدولية والخصوصية العربية فإن هذا التشريع يجب أن يعرف الجرائم الإلكترونية تعريفاً شاملاً ويجرم الأفعال الخطيرة وينظم إجراءات فعالة للتحقيق والعقاب مع حماية الحقوق الرقمية وتظهر أهمية التوحيد في تسهيل التعاون القضائي العربي ومكافحة الجرائم العابرة للحدود في الفضاء الرقمي وإن تحقيق هذه الرؤية يتطلب حواراً تشريعياً مستمراً بين الدول العربية وتبادلاً للخبرات والتجارب الناجحة وإن التشريع العربي الموحد هو ضمانة لتحقيق أمن رقمي عربي مشترك يحمي المواطنين والمؤسسات من التهديدات الإلكترونية المتزايدة في العصر الرقمي

الختام

وبعد أن أتممنا كتابة الفصول العشرين التي تضمنها هذا الكتاب الموسوعي الشامل والذي غطى كافة الجوانب المتعلقة بجرائم الإنترنت والتقنية والحماية

الجنائية منها من منظور أكاديمي وقانوني وتقني عميق ومتخصص فإننا نأمل أن نكون قد وفقنا في تقديم إضافة علمية حقيقية تخدم الباحثين والطلاب والمهتمين بالقانون الجنائي الرقمي وأمن المعلومات في مختلف أنحاء العالم العربي والإسلامي والعالم أجمع فإن الجهد المبذول في هذا الكتاب هو جهد متواضع أمام عظمة الموضوع وشموليته وتعقيداته ولكنه جهد صادق ومخلص يهدف إلى وجه الله سبحانه وتعالى ونشر النفع بين الناس فإن العلم نور والجهل ظلام وما نحاوله هنا هو إضاءة بعض الزوايا المظلمة في فهمنا للجرائم الإلكترونية المعقدة التي تهدد الأمن الفردي والجماعي في العصر الرقمي ونأمل أن يكون هذا الكتاب نقطة انطلاق لتشريعات وإصلاحات أكثر فعالية في مكافحة الجرائم التقنية وحماية الضحايا في المستقبل القريب بإذن الله تعالى

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون

الطبعة الأولى 2026

حقوق الملكية محفوظة للمؤلف يمنع النسخ أو الطبع أو النشر أو التوزيع إلا بإذن خطي من المؤلف