الجرائم الإلكترونية والإثبات الرقمي

دراسة تحليلية مقارنة في التشريعات المصرية والجزائرية واللبنانية والفرنسية

بين حماية الخصوصية الرقمية وضرورات كشف الحقيقة في الفضاء السيبراني

تأليف

د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والمؤلف القانوني والمحاضر الدولي في القانون

الإهداء

إلى روح والديّ العزيزين، الذين غرسا فيّ حب العلم

ومواكبة العصر، وجعلا من القيم ثوابت لا تتغير بتغير التقنيات، فكانا لي البوصلة في بحر المعرفة المتلاطم.

إلى ابنتي الغالية وقرة عيني صبرين، التي ترعرعت في عصر الرقميات، وأسأل الله أن يجعلها منارة للعلم والنور في هذا العالم المتشابك، وأن يحفظها من كل مكروه.

إلى كل قاضٍ يواجه تحديات الجرائم غير المرئية بميزان عدل راسخ، ومحققٍ يتتبع الآثار الرقمية بخفة ودقة، ومحامٍ يدافع عن الحقوق والحريات في الفضاء الافتراضي بشجاعة، أهدي هذا الجهد المتواضع.

فهرس المحتويات

المقدمة العامة

القسم الأول: الإطار المفاهيمي والتقني للجرائم الإلكترونية

الفصل الأول: طبيعة الجرائم الإلكترونية وتصنيفاتها في القوانين المقارنة

الفصل الثاني: الخصائص الفنية للجريمة الإلكترونية وأثرها على الإجراءات الجنائية

الفصل الثالث: الاختصاص القضائي الدولي والإقليمي في الجرائم عابرة الحدود

القسم الثاني: إجراءات الضبط والتحقيق في البيئة الرقمية

الفصل الرابع: سلطات الضبط القضائي في جمع الأدلة الرقمية وضماناتها

الفصل الخامس: التفتيش الرقمي وضبط الأجهزة وبيانات السحابة الإلكترونية

الفصل السادس: التنصت الإلكتروني واعتراض

الاتصالات بين الضرورة الأمنية وحرمة الحياة الخاصة

الفصل السابع: التعاون الدولي في مجال الجرائم الإلكترونية وتسليم المجرمين رقمياً

القسم الثالث: الإثبات الرقمي وحجيته أمام القضاء

الفصل الثامن: الطبيعة القانونية للأدلة الرقمية وحجيتها في الإثبات

الفصل التاسع: خبرة الحاسب الآلي ودور الخبراء في استخراج وتحليل الأدلة الرقمية

الفصل العاشر: توثيق الأدلة الرقمية وسلسلة الحراسة

الفصل الحادي عشر: بطلان الأدلة الرقمية المنتزعة بشكل غير قانوني

القسم الرابع: أنواع الجرائم الإلكترونية المستحدثة

الفصل الثاني عشر: جرائم الاعتداء على الأنظمة المعلوماتية الاختراق والتخريب والفيروسات

الفصل الثالث عشر: جرائم الاحتيال الإلكتروني والتجارة غير المشروعة

الفصل الرابع عشر: جرائم المحتوى غير المشروع التشهير والابتزاز والإرهاب الإلكتروني

الفصل الخامس عشر: جرائم العملات الرقمية وغسل الأموال عبر الإنترنت

القسم الخامس: التطبيقات القضائية والتحديات المستقبلية

الفصل السادس عشر: نماذج من اجتهاد محاكم النقض في الدول الأربع حول الأدلة الرقمية

الفصل السابع عشر: تحديات التشفير والعملات المشفرة وتقنيات الذكاء الاصطناعي في الجريمة

الخاتمة العامة والتوصيات

الملاحق العملية

المقدمة العامة

تحول الجريمة من الشارع إلى الشبكة وتحدي الإثبات التقليدي

أهمية الموضوع

تشهد البشرية اليوم تحولاً جذرياً في ظاهرة الإجرام، انتقلت فيه الجريمة من الشوارع المادية والأماكن المحسوسة إلى فضاء افتراضي لا يعرف حدوداً جغرافية ولا حواجز مادية. فلم تعد الجريمة تتطلب

وجود الجاني والضحية في مكان واحد، بل أصبحت ترتكب من قارة وتؤثر ضحاياها في قارة أخرى دون أن يغادر الجاني مكتبه. هذا التحول يطرح تحدياً وجودياً أمام النظم القضائية التقليدية التي وُضعت نصوصها لعالم مادي ملموس، بينما تواجه اليوم أدلة غير مرئية قابلة للتعديل والحذف في ثوانٍ معدودة.

إن الإشكالية الجوهرية التي يطرحها موضوع الجرائم الإلكترونية تكمن في التوازن الدقيق والصعب بين ضرورة تمكين أجهزة التحقيق من الوصول السريع للبيانات الرقمية قبل زوالها، وبين الحق الدستوري المكفول للأفراد في خصوصية بياناتهم وحرمة حياتهم الخاصة. فكيف نوفق بين سرعة التقنية وبطء الإجراءات؟ وكيف نضمن أن أدوات كشف الحقيقة الرقمية لا تتحول هي نفسها إلى أدوات انتهاك للحريات؟

جوهر الدراسة: اليقين التقني والعدالة الجنائية

تنطلق هذه الدراسة من مسلمة أساسية وهي أن العدالة في العصر الرقمي لم تعد تعتمد فقط على الاقتناع الوجداني للقاضي، بل أصبحت رهينة باليقين التقني وسلامة الإجراءات. فالدليل الرقمي، بحكم طبيعته الهشة والقابلة للتلاعب، يتطلب سلسلة من الضمانات الإجرائية والفنية الدقيقة تبدأ من لحظة الضبط ولا تنتهي إلا عند العرض على المحكمة. أي خلل في هذه السلسلة، سواء كان فنياً أو إجرائياً، قد يحول دليلاً قاطعاً إلى مجرد بيانات مشكوك في مصداقيتها.

في هذا السياق، تبرز أهمية المقارنة بين التجربة الفرنسية المتقدمة في تنظيم الفضاء السيبراني وإجراءات الضبط الرقمي، وبين التجارب العربية في مصر والجزائر ولبنان التي تسعى بخطى متسارعة لتحديث تشريعاتها ومواكبة التطور التكنولوجي، مع الحفاظ على الخصوصية الثقافية والقانونية للمجتمعات العربية.

منهجية المقارنة الرباعية

تتميز هذه الدراسة باعتماد منهج مقارن رباعي الأبعاد يجمع بين ثلاثة أنظمة عربية تنهل من مرجعيات مشتركة وتتشارك في التحديات الإقليمية، وبين النظام الفرنسي الذي شكل المصدر التاريخي للتشريع في هذه الدول ويعد رائداً أوروبياً في مجال الجرائم الإلكترونية.

فرنسا بوصفها الرائد الأوروبي في تطوير آليات الضبط الرقمي والإثبات الإلكتروني، حيث طورت تشريعات متقدمة مثل قانون الثقة في الاقتصاد الرقمي وقوانين مكافحة الإرهاب التي وسعت صلاحيات الضبط الرقمي، مقدمة نموذجاً لكيفية موازنة السلطات investigatory مع ضمانات حقوق الدفاع والخصوصية.

مصر التي أقرت قانوناً متخصصاً لمكافحة الجرائم الإلكترونية عام 2018، وشهدت تطوراً ملحوظاً في إنشاء نيابات متخصصة وتطوير قدرات الأجهزة الشرطية

في التعامل مع الأدلة الرقمية، في إطار استراتيجية وطنية شاملة للأمن السيبراني.

الجزائر التي عززت ترسانتها القانونية بقوانين جديدة تجرم الفعل الإلكتروني وتنظم الإثبات الرقمي، ساعية لتحديث منظومتها القضائية بما يتوافق مع المعايير الدولية ومعطيات العصر الرقمي.

لبنان الذي يتميز بمرونة نظامه القضائي وانفتاحه على التجارب المقارنة، ويسعى لتطوير تشريعاته لمواكبة الجرائم المستحدثة في ظل التحديات الأمنية والاقتصادية التي يمر بها.

إشكاليات البحث ومحاور التحليل

سيغوص هذا الكتاب في أعماق إشكاليات معقدة تشكل تحدياً حقيقياً للمشرع والقاضي والخبير التقني معاً:

كيف يمكن تحديد الاختصاص القضائي في جريمة عابرة للحدود يرتكب فاعلها من دولة وتقع نتائجها في دول متعددة؟

ما هي الضمانات الكفيلة لمنع التعسف في استخدام سلطات التفتيش الرقمي واعتراض الاتصالات؟

كيف نثبت صحة الدليل الرقمي ونضمن عدم تلوثه أو التلاعب به منذ لحظة الضبط حتى العرض على المحكمة؟

ما هو موقف التشريع من الأدلة المنتزعة عبر اختراق الأنظمة أو بدون إذن قضائي صحيح؟

كيف نتعامل مع تحديات المستقبل مثل التشفير التام والعملات المشفرة والذكاء الاصطناعي في ارتكاب الجرائم؟

غاية الدراسة: نحو تشريع رقمي عربي موحد

إن الغاية من هذا التحليل المقارن ليست مجرد استيراد النماذج الغربية، بل هي محاولة جادة لتقديم رؤية تركيبية تستلهم أفضل الممارسات الدولية مع تكييفها مع الواقع العربي. نسعى من خلال هذه الدراسة إلى تأكيد مبدأ أن مكافحة الجرائم الإلكترونية لا تتحقق فقط بتجريم الأفعال، بل ببناء منظومة إثبات رقمية متكاملة تحترم المعايير الفنية والقانونية الدولية، وتضمن محاكمة عادلة تحمي المجتمع من المجرمين وتحمي الأبرياء من التعسف.

القسم الأول

الإطار المفاهيمي والتقني للجرائم الإلكترونية

الفصل الأول

طبيعة الجرائم الإلكترونية وتصنيفاتها في القوانين المقارنة

المبحث الأول: تعريف الجريمة الإلكترونية وعناصرها

تُعرف الجريمة الإلكترونية بأنها كل فعل غير مشروع يرتكب باستخدام شبكة معلوماتية أو نظام حاسوبي، أو يكون النظام الحاسوبي هدفاً له. وتتميز هذه الجرائم بوجود ركن تقني أساسي، سواء كأداة لارتكاب الجريمة أو كمحل لها. ويستعرض الفصل التعريفات الواردة في التشريعات المصرية والجزائرية واللبنانية والفرنسية، مبرزاً أوجه الاتفاق والاختلاف في تحديد نطاق التجريم.

المبحث الثاني: تصنيف الجرائم الإلكترونية

يصنف الفصل الجرائم إلى ثلاث فئات رئيسية:

أولاً جرائم ضد الأنظمة والمعلومات: مثل الاختراق، تعطيل الخدمات، نشر الفيروسات.

ثانياً جرائم باستخدام التقنية: مثل الاحتيال الإلكتروني، السرقة، الابتزاز، غسل الأموال.

ثالثاً جرائم المحتوى: مثل التشهير، التحريض على الكراهية، الإرهاب الإلكتروني، المواد الإباحية.

ويقارن الفصل بين كيفية تعامل القوانين الأربعة مع كل فئة، وهل هناك جرائم مستحدثة في قانون دون آخر.

المبحث الثالث: التطور التشريعي في الدول الأربع

يتتبع الفصل المسار التاريخي للتشريع في كل دولة، بدءاً من الاعتماد على النصوص العامة في قوانين العقوبات، مروراً بإصدار قوانين خاصة بالجرائم المعلوماتية، وصولاً إلى أحدث التعديلات التي استجابت للمستجدات التقنية. ويحلل الفجوات التشريعية التي قد تستغلها الثغرات التقنية.

الفصل الثاني

الخصائص الفنية للجريمة الإلكترونية وأثرها على الإجراءات الجنائية

المبحث الأول: خصائص الجريمة الإلكترونية

تناقش الخصائص الفريدة التي تميز الجريمة الإلكترونية: اللامادية، السرعة الفائقة، العابرة للحدود، صعوبة الكشف، وقابلية البيانات للتعديل والحذف دون أثر. هذه الخصائص تفرض إعادة نظر جذرية في المفاهيم الإجرائية التقليدية مثل مكان وزمان ارتكاب الجريمة.

المبحث الثاني: تأثير الخصائص الفنية على الإجراءات

يحلل الفصل كيف أثرت هذه الخصائص على مراحل الدعوى الجنائية. فمثلاً ً، مفهوم "التلبس" يأخذ بعداً ً جديداً ً في العالم الرقمي، ومفهوم "حجز الأشياء" يتحول إلى "نسخ البيانات"، و"التفتيش" يشمل

الأنظمة والسحابات الإلكترونية. ويستعرض كيف اضطرت التشريعات الأربعة لتعديل مفاهيمها الإجرائية لاستيعاب هذه المتغيرات.

المبحث الثالث: تحديات الإثبات في البيئة الرقمية

يركز على الصعوبات الخاصة بإثبات الجرائم الإلكترونية، مثل صعوبة ربط الفعل بالشخص المادي (مشكلة انتحال الهوية)، وصعوبة حفظ الأدلة من الزوال، وتعقيد الفهم التقني للأدلة مما يستدعي الاستعانة بالخبراء. ويقارن بين الحلول التي قدمتها القوانين الأربعة لهذه التحديات.

الفصل الثالث

الاختصاص القضائي الدولي والإقليمي في الجرائم عابرة الحدود

المبحث الأول: إشكالية تحديد المكان في الجريمة الإلكترونية

يطرح الفصل إشكالية تحديد المحكمة المختصة عندما يكون الجاني في دولة، والضحية في ثانية، والخادم المستخدم في ثالثة. يناقش المعايير المختلفة للاختصاص: مكان ارتكاب الفعل المادي، مكان وقوع النتيجة، مكان وجود البيانات، وجنسية الجاني أو الضحية.

المبحث الثاني: معايير الاختصاص في التشريعات المقارنة

يستعرض الفصل كيف عالجت القوانين المصرية والجزائرية واللبنانية والفرنسية مسألة الاختصاص. فبينما توسع بعض القوانين دائرة الاختصاص لتشمل أي جريمة تؤثر على مصالح الدولة أو مواطنيها بغض النظر عن مكان الارتكاب، تضع قوانين أخرى ضوابط أضيق لحماية السيادة الوطنية للدول الأخرى.

المبحث الثالث: التعاون الدولي واتفاقية بودابست

يناقش دور الاتفاقيات الدولية، وخاصة اتفاقية بودابست للجرائم الإلكترونية، في توحيد معايير الاختصاص وتسهيل التعاون. ويستعرض موقف الدول الأربع من الاتفاقية، ومدى انسجام تشريعاتها الداخلية مع مبادئها، وآليات المساعدة القانونية المتبادلة في هذا المجال.

القسم الثاني

إجراءات الضبط والتحقيق في البيئة الرقمية

الفصل الرابع

سلطات الضبط القضائي في جمع الأدلة الرقمية وضماناتها

المبحث الأول: صلاحيات الضبط القضائي في المجال الرقمي

يحلل الفصل السلطات الواسعة الممنوحة لرجال الضبط القضائي في البيئة الرقمية مقارنة بالتقليدية، مثل سلطة حجز الأجهزة، نسخ المحتويات، طلب البيانات من مقدمي الخدمة، وفك التشفير. ويقارن بين نطاق هذه الصلاحيات في القوانين الأربعة.

المبحث الثاني: ضمانات جمع الأدلة الرقمية

يركز على الضمانات الإجرائية اللازمة عند جمع الأدلة الرقمية، مثل ضرورة وجود محضر مفصل يصف الإجراءات التقنية المتبعة، وحضور شهود أو خبراء في حالات معينة، واحترام مبدأ التناسب بين خطورة الجريمة والإجراء المتخذ. ويقارن بين مستوى الحماية المقررة في كل دولة.

المبحث الثالث: دور مقدمي خدمة الإنترنت في الضبط

يناقش الالتزامات القانونية لمقدمي خدمة الإنترنت وشركات التكنولوجيا في التعاون مع أجهزة التحقيق، وحفظ البيانات، وتسليمها عند الطلب. ويستعرض التوازن بين واجب التعاون وحماية خصوصية المستخدمين وسرية الاتصالات في التشريعات الأربعة.

الفصل الخامس

التفتيش الرقمي وضبط الأجهزة وبيانات السحابة الإلكترونية

المبحث الأول: مفهوم التفتيش الرقمي وأنواعه

يُعرّف التفتيش الرقمي بأنه فحص الأجهزة الحاسوبية والهواتف الذكية والأنظمة المعلوماتية للكشف عن أدلة رقمية. ويميز الفصل بين التفتيش المحلي للأجهزة المضبوطة، والتفتيش عن بعد للأنظمة المتصلة

بالشبكة.

المبحث الثاني: تفتيش الأجهزة المحلية وضبطها

يتناول الإجراءات الواجب اتباعها عند تفتيش الأجهزة المادية، مثل إغلاق الجهاز بطريقة آمنة للحفاظ على البيانات، عزل الجهاز عن الشبكة لمنع المسح عن بعد، وتوثيق حالة الجهاز قبل وبعد الضبط. ويقارن بين الممارسات المثلى والنصوص القانونية في الدول الأربع.

المبحث الثالث: إشكالية البيانات السحابية

يطرح الفصل إحدى أهم الإشكاليات الحديثة: هل يجوز تفتيش جهاز مضبوط لاستخراج بيانات مخزنة على سحابة إلكترونية خارج الإقليم؟ يناقش الاجتهاد الفرنسي الحديث الذي ميز بين البيانات المحلية والسحابية، ويقترح معايير للتشريعات العربية تحمي خصوصية البيانات المخزنة خارجياً وتتطلب إجراءات

تعاون دولي للوصول إليها.

الفصل السادس

التنصت الإلكتروني واعتراض الاتصالات بين الضرورة الأمنية وحرمة الحياة الخاصة

المبحث الأول: الإطار القانوني للتنصت الإلكتروني

يستعرض النصوص المنظمة لاعتراض الاتصالات الإلكترونية في القوانين الأربعة، شاملًا البريد الإلكتروني، المحادثات الفورية، والمكالمات عبر بروتوكول الإنترنت. ويحدد الشروط الواجب توافرها للجوء إلى هذا الإجراء الاستثنائي.

المبحث الثاني: شروط الإذن بالتنصت والرقابة القضائية

يركز على دور السلطة القضائية في منح الإذن

بالتنصت، ومدة الإذن، والجرائم التي يجوز فيها اللجوء لهذا الإجراء. ويقارن بين الضمانات القضائية المشددة في فرنسا والتي تتطلب تدخلاً مكثفاً لقاضي الحريات، وبين الصلاحيات الأوسع الممنوحة للنيابة أو أجهزة الأمن في بعض الحالات في القوانين العربية، مناقشاً مدى توافق ذلك مع معايير حقوق الإنسان.

المبحث الثالث: حماية البيانات المجمعة عبر التنصت

يناقش مصير البيانات التي يتم جمعها عبر التنصت، وضرورة إتلاف ما لا علاقة له بالدعوى، وسرية المعلومات المجمعة، والجزاءات المترتبة على إساءة استخدام بيانات التنصت. ويقدم مقارنة لكيفية معالجة التشريعات الأربعة لهذه القضايا الحساسة.

الفصل السابع

التعاون الدولي في مجال الجرائم الإلكترونية وتسليم المجرمين رقمياً

المبحث الأول: آليات المساعدة القانونية المتبادلة

يشرح الإجراءات التقليدية للمساعدة القانونية (خطابات التكليف القضائي) وينقد بطئها في مواجهة سرعة زوال الأدلة الرقمية. ويستعرض الجهود المبذولة لتبسيط هذه الإجراءات في إطار الاتفاقيات الدولية والإقليمية.

المبحث الثاني: نقاط الاتصال المباشرة والشبكات الأمنية

يتناول الآليات الحديثة للتعاون المباشر بين أجهزة إنفاذ القانون في الدول المختلفة، مثل شبكات الاتصال على مدار الساعة (Network 7/24) التي تتيح تبادل المعلومات السريع في الحالات الطارئة. ويقارن بين مستوى مشاركة الدول الأربع في هذه الشبكات.

المبحث الثالث: تسليم المجرمين في الجرائم الإلكترونية

يناقش التحديات الخاصة بتسليم المتهمين في الجرائم الإلكترونية، مثل مشكلة ازدواجية التجريم، واستثناء الجرائم السياسية أو العسكرية، وضمانات المحاكمة العادلة في الدولة الطالبة للتسليم.
ويستعرض نماذج من قضايا التسليم في الدول الأربع.

القسم الثالث

الإثبات الرقمي وحجيته أمام القضاء

الفصل الثامن

الطبيعة القانونية للأدلة الرقمية وحجيتها في الإثبات

المبحث الأول: مفهوم الدليل الرقمي وأنواعه

يُعرّف الدليل الرقمي بأنه أي بيانات ذات قيمة إثباتية يتم إنشاؤها أو تخزينها أو نقلها بواسطة أجهزة إلكترونية. ويستعرض أنواع الأدلة الرقمية: ملفات النصوص، الصور، الفيديوهات، سجلات الاتصالات، بيانات الموقع الجغرافي، وغيرها.

المبحث الثاني: حجية الأدلة الرقمية في التشريعات المقارنة

يجيب الفصل على السؤال الجوهري: هل تعتبر النسخة الرقمية دليلاً أصلياً أم صورة؟ ويستعرض التطور التشريعي في الدول الأربع الذي ساوى بين الدليل الورقي والرقمي في الحجية، شريطة توافر شروط معينة تثبت سلامة المصدر وعدم التلاعب، مثل التوقيع الإلكتروني المؤمن وسجلات التحقق.

المبحث الثالث: معايير تقييم الدليل الرقمي من قبل القاضي

يناقش المعايير التي يعتمد عليها القاضي في تقييم قوة الدليل الرقمي واقتناعه به، مثل مصدر الدليل، طريقة جمعه، سلامة سلسلة الحراسة، وتقرير الخبير المختص. ويقارن بين حرية تقدير القاضي في الأنظمة الأربعة والقيود المفروضة عليه.

الفصل التاسع

خبرة الحاسب الآلي ودور الخبراء في استخراج وتحليل الأدلة الرقمية

المبحث الأول: ضرورة الاستعانة بالخبراء في الجرائم الإلكترونية

يؤكد على الدور المحوري للخبير التقني كـ "عين القاضي" في العالم الرقمي، نظراً لتعقيد الأدلة التقنية التي تتجاوز فهم غير المتخصصين. ويناقش الحالات التي يكون فيها الاستعانة بالخبير إلزامية

بموجب القانون أو ضرورية بحكم الواقع.

المبحث الثاني: تعيين الخبراء وصفاتهم المهنية

يتناول معايير اختيار الخبراء، سواء كانوا من الخبراء الرسميين التابعين للدولة أو من الخبراء الخاصين المعتمدين. ويقارن بين نظام الخبرة في مصر والجزائر الذي يعتمد كثيراً على الخبراء الرسميين، وبين النظام في فرنسا ولبنان الذي يمنح مرونة أكبر في الاستعانة بخبراء خاصين تحت إشراف القضاء.

المبحث الثالث: منهجية العمل الفني للخبير

يشرح الخطوات الفنية التي يجب أن يتبعها الخبير في استخراج وتحليل الأدلة الرقمية، بما يضمن علمية النتائج وموضوعيتها، مثل عمل نسخة طبق الأصل، التحليل على النسخة وليس الأصل، استخدام أدوات معتمدة، وتوثيق كل خطوة. ويقدم نقداً لبعض الممارسات غير المنضبطة التي قد تظهر في بعض

التقارير.

الفصل العاشر

توثيق الأدلة الرقمية وسلسلة الحراسة

المبحث الأول: مفهوم سلسلة الحراسة وأهميتها

يشرح مفهوم "سلسلة الحراسة" (Chain of Custody) كأهم ضمانة لصحة الدليل الرقمي. وهي السجل الوثائقي الذي يوضح كل شخص تعامل مع الدليل، ومتى، وأين، ولماذا، وما هي الإجراءات التي تمت. وأي فجوة في هذه السلسلة تثير شكوكاً جدية في مصداقية الدليل.

المبحث الثاني: إجراءات توثيق سلسلة الحراسة

يتناول الإجراءات العملية لتوثيق السلسلة، مثل

استخدام أكياس مضادة للعبث، تدوين التواقيع والتواريخ، حساب قيم التجزئة الرقمية (Hash Values) للتأكد من عدم تغير البيانات، واستخدام سجلات دخول وخروج دقيقة. ويقدم نموذجاً عملياً لسجل سلسلة حراسات يتوافق مع المعايير الدولية.

المبحث الثالث: أثر انقطاع سلسلة الحراسة على حجية الدليل

يناقش العواقب القانونية لانقطاع سلسلة الحراسة أو وجود ثغرات فيها. هل يؤدي ذلك تلقائياً إلى بطلان الدليل؟ أم أنه يترك الأمر لتقدير القاضي؟ ويقارن بين الاتجاه الصارم في القضاء الفرنسي الذي يميل لاستبعاد الأدلة الملوثَة، والاتجاهات الأخرى التي قد تقبل الدليل إذا اقتنع القاضي بسلامة مضمونه رغم الخلل الإجرائي.

الفصل الحادي عشر

بطلان الأدلة الرقمية المنتزعة بشكل غير قانوني

المبحث الأول: حالات بطلان الأدلة الرقمية

يستعرض الحالات التي تؤدي إلى بطلان الدليل الرقمي، مثل التفتيش بدون إذن قضائي، تجاوز نطاق الإذن، انتهاك خصوصية البيانات غير المرتبطة بالجريمة، أو عدم احترام إجراءات سلسلة الحراسة بشكل جوهري.

المبحث الثاني: نظرية ثمرة الشجرة المسمومة في الإثبات الرقمي

يطبق الفصل نظرية "ثمرة الشجرة المسمومة" على المجال الرقمي. فإذا تم الحصول على دليل رقمي بطريقة غير قانونية، فهل تبطل أيضاً الأدلة الأخرى المشتقة منه؟ يناقش الاجتهاد القضائي في الدول الأربع حول هذه المسألة، مقدماً رؤية نقدية تدعم إقصاء الأدلة الملوثة حفاظاً على شرعية الإجراءات

وحرمة الحياة الخاصة.

المبحث الثالث: سلطة القاضي في استبعاد الأدلة غير المشروعة

يحلل السلطة التقديرية للقاضي في استبعاد الأدلة الرقمية المنتزعة بشكل غير قانوني، ومدى إلزاميته بذلك. ويدعو لتعزيز هذه السلطة في التشريعات العربية لتكون رادعاً فعلياً ضد تعسف أجهزة التحقيق وانتهاك الخصوصية الرقمية.

القسم الرابع

أنواع الجرائم الإلكترونية المستحدثة

الفصل الثاني عشر

جرائم الاعتداء على الأنظمة المعلوماتية الاختراق

والتخريب والفيروسات

المبحث الأول: جريمة الدخول غير المشروع إلى الأنظمة

يتناول عنصر الجريمة المتمثل في اختراق نظام معلوماتي محمي دون إذن، سواء كان الهدف سرقة بيانات أو مجرد الدخول للاستطلاع. ويقارن بين التجريم في القوانين الأربعة والعقوبات المقررة.

المبحث الثاني: جرائم تعطيل الأنظمة ونشر الفيروسات

يناقش الجرائم التي تهدف إلى تخريب أو تعطيل عمل الأنظمة المعلوماتية، مثل هجمات حجب الخدمة (DDoS)، ونشر البرمجيات الخبيثة والفيروسات. ويستعرض الصعوبات في إثبات النية الجنائية وتحديد المسؤول المادي في الهجمات المعقدة.

المبحث الثالث: المسؤولية الجنائية للشركات ومقدمي الخدمة

يطرح إشكالية مسؤولية الأشخاص الاعتبارية وشركات التكنولوجيا عن الثغرات الأمنية أو عدم اتخاذ إجراءات حماية كافية، ومدى تجريم الإهمال في تأمين الأنظمة في التشريعات المقارنة.

الفصل الثالث عشر

جرائم الاحتيال الإلكتروني والتجارة غير المشروعة

المبحث الأول: صور الاحتيال الإلكتروني

يستعرض أشكال الاحتيال الحديثة مثل التصيد (Phishing)، انتحال الشخصية، المواقع الوهمية، وعمليات النصب في التجارة الإلكترونية. ويحلل العناصر المكونة لهذه الجرائم في القوانين الأربعة.

المبحث الثاني: إثبات نية الاحتيال في البيئة الافتراضية

يناقش التحدي الكبير في إثبات القصد الجنائي في جرائم الاحتيال الإلكتروني، حيث يصعب أحياناً التمييز بين الخطأ التجاري والاحتيال المتعمد. ويقارن بين القرائن التي يعتمدها القضاء في الدول الأربع لإثبات النية.

المبحث الثالث: تتبع الأموال واستردادها في الجرائم المالية

يتناول الآليات القانونية والتقنية لتتبع الأموال المسروقة عبر الشبكات المالية الإلكترونية، وإجراءات الحجز والاسترداد، والتعاون الدولي في هذا المجال.

الفصل الرابع عشر

جرائم المحتوى غير المشروع التشهير والابتزاز والإرهاب الإلكتروني

المبحث الأول: جرائم التشهير والسب عبر وسائل التواصل

يناقش التوازن الدقيق بين تجريم التشهير الإلكتروني وحماية حرية التعبير. ويستعرض الاجتهادات القضائية في الدول الأربع حول حدود النقد المسموح به وجرائم السب والقذف عبر الإنترنت، والعقوبات المشددة في بعض القوانين العربية.

المبحث الثاني: جريمة الابتزاز الإلكتروني

يتناول جريمة تهديد بنشر معلومات أو صور خاصة للحصول على مال أو منفعة، وهي جريمة في تزايد مستمر. ويحلل عناصر الجريمة وصعوبات الإثبات خاصة مع استخدام عملات رقمية أو هويات مجهولة.

المبحث الثالث: جرائم الإرهاب الإلكتروني والتحريض على الكراهية

يناقش تجريم استخدام الإنترنت لنشر الأفكار المتطرفة، التحريض على العنف، وتجنيدهم للإرهاب. ويستعرض الصلاحيات الاستثنائية الممنوحة لأجهزة التحقيق في هذه الجرائم، والتوازن المطلوب مع الحريات العامة.

الفصل الخامس عشر

جرائم العملات الرقمية وغسل الأموال عبر الإنترنت

المبحث الأول: الطبيعة القانونية للعملات المشفرة

يتناول الإشكالية القانونية لتصنيف العملات المشفرة مثل البيتكوين، هل هي أموال أم سلع أم أوراق مالية؟

وكيف تتعامل القوانين الأربعة مع هذا التصنيف وأثره على التجريم.

المبحث الثاني: غسل الأموال عبر المنصات الرقمية

يشرح الآليات المستخدمة في غسل الأموال عبر العملات المشفرة ومنصات التبادل غير المرخصة، وصعوبات التتبع بسبب خاصية إخفاء الهوية النسبية.

المبحث الثالث: أدلة البلوك تشين وإثبات الجرائم

يناقش إمكانية استخدام تقنية سلسلة الكتل (Blockchain) نفسها كأداة إثبات لتتبع المعاملات المشبوهة، ودور الخبراء في تحليل هذه السجلات المعقدة أمام القضاء.

القسم الخامس

التطبيقات القضائية والتحديات المستقبلية

الفصل السادس عشر

نماذج من اجتهاد محاكم النقض في الدول الأربع حول الأدلة الرقمية

المبحث الأول: اجتهادات محكمة النقض المصرية

يستعرض أحكاماً رائدة للمحكمة في قضايا الاختراق والابتزاز الإلكتروني، وموقفها من حجية التقارير الفنية وسلسلة الحراسة، وتطور فهمها للطبيعة التقنية للأدلة.

المبحث الثاني: تطور اجتهاد المجلس الأعلى للقضاء الجزائري

يناقش توجهات القضاء الجزائري في تفسير نصوص

قانون الجرائم الإلكترونية، وموقفه من إجراءات الضبط الرقمي وحماية الخصوصية، وجهوده في مواءمة التطبيق القضائي مع المعايير الدولية.

المبحث الثالث: اجتهاد محكمة التمييز اللبنانية في الجرائم المستحدثة

يبرز المرونة التي أظهرها القضاء اللبناني في التعامل مع قضايا الجرائم الإلكترونية، واعتماده على المبادئ العامة للعدالة والمقارنة مع التشريعات الأجنبية في غياب النصوص التفصيلية أحياناً.

المبحث الرابع: الصرامة التقنية في اجتهاد محكمة النقض الفرنسية

يتناول الدقة والصرامة التي تتسم بها الأحكام الفرنسية في مسائل الإثبات الرقمي، واشتراطها التزاماً صارماً بالإجراءات الفنية والقانونية، واستبعادها للأدلة التي تشوبها شوائب في سلسلة الحراسة أو

الإذن القضائي.

الفصل السابع عشر

تحديات التشفير والعملات المشفرة وتقنيات الذكاء الاصطناعي في الجريمة

المبحث الأول: تحدي التشفير التام

يناقش المعضلة الأمنية والقانونية الناتجة عن انتشار تقنيات التشفير التام (End-to-End Encryption) التي تجعل اعتراض الاتصالات وفك محتوياتها مستحيلاً تقنياً حتى بالنسبة لأجهزة التحقيق، والجدل الدائر حول "الأبواب الخلفية".

المبحث الثاني: الذكاء الاصطناعي والجرائم المستقبلية

يستعرض التحديات الناشئة عن استخدام الذكاء الاصطناعي في ارتكاب الجرائم، مثل التزوير العميق (Deepfakes) للصوت والصورة، والهجمات الإلكترونية الذاتية التعلم، وصعوبة نسب الفعل إلى إنسان محدد.

المبحث الثالث: إنترنت الأشياء كأدلة وجناة

يناقش كيف أصبحت الأجهزة المنزلية الذكية (كاميرات، مكبرات صوت، ثلاجات) مصادر محتملة لأدلة جنائية، وفي نفس الوقت نقاط اختراق محتملة، وما يترتب على ذلك من تحديات قانونية تتعلق بالخصوصية وطرق الضبط.

الخاتمة العامة والتوصيات

خلاصة الرحلة المقارنة

أكدت الدراسة أن الجرائم الإلكترونية تمثل تحدياً

وجودياً للعدالة الجنائية التقليدية، requiring تحديثاً مستمراً للنصوص والإجراءات والمفاهيم. وكشفت المقارنة عن تقدم ملحوظ في التجربة الفرنسية في التنظيم والضبط والإثبات الرقمي، وعن جهود حثيثة في الدول العربية لمواكبة هذا التطور، مع وجود فجوات تحتاج للسد خاصة في مجالات ضمانات الخصوصية وسلسلة الحراسة والتعاون الدولي الفعال.

الرؤية الإصلاحية والتوصيات

توصي الدراسة بمجموعة من الإجراءات الإصلاحية الموحدة:

أولاً توصيات تشريعية: تحديث قوانين الجرائم الإلكترونية باستمرار لمواكبة المستحدثات التقنية، تعزيز ضمانات الخصوصية الرقمية، والنص صراحة على إجراءات سلسلة الحراسة وعواقب الإخلال بها.

ثانياً توصيات مؤسسية: إنشاء نيابات وقضاء متخصص في الجرائم الإلكترونية مزود بالخبرات التقنية اللازمة،

تطوير معامل جنائية رقمية معتمدة، وإنشاء وحدات شرطة سيبرانية مدربة تدريباً عالياً.

ثالثاً توصيات إجرائية: اعتماد معايير موحدة لجمع وحفظ الأدلة الرقمية في الدول العربية، تعزيز آليات التعاون الدولي المباشر والسريع، وإلزامية الاستعانة بخبراء معتمدين في القضايا المعقدة.

رابعاً توصيات بحثية وتدريبية: تشجيع البحث العلمي في مجال القانون الرقمي، وتطوير برامج تدريبية مشتركة للقضاة والنيابة والمحامين والخبراء لمواكبة التطور التكنولوجي السريع.

كلمة ختامية

إن العدالة في العصر الرقمي ليست خياراً، بل هي ضرورة حتمية لضمان استقرار المجتمعات وأمن الأفراد. ولا تتحقق هذه العدالة إلا بموازنة دقيقة بين قوة القانون وقدرة التقنية، وبين سلطات التحقيق وحريات الناس. وبهذا الكتاب، نكون قد وضعنا لبنة في صرح

البناء القانوني الرقمي، آمين أن تسهم هذه الدراسة في تطوير منظومة عدالة عربية عصرية، قادرة على مواجهة تحديات الحاضر واستشراف مخاطر المستقبل، محافظة على كرامة الإنسان في عالم أصبح فيه الرقم هو السيد.

الملاحق العملية

الملحق الأول: نصوص المواد القانونية المتعلقة بالجرائم الإلكترونية والإثبات الرقمي في القوانين المصرية والجزائرية واللبنانية والفرنسية.

الملحق الثاني: نموذج محضر ضبط وتفتيش رقمي يراعي معايير سلسلة الحراسة الدولية.

الملحق الثالث: دليل إرشادي للقضاة والنيابة في تقييم الأدلة الرقمية وتقارير الخبراء.

الملحق الرابع: قائمة بأهم الاتفاقيات الدولية

والإقليمية المتعلقة بالجرائم الإلكترونية وموقف الدول الأربع منها.

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي