النظام القانوني للأمن السيبراني وحماية البيانات الشخصية في الفضاء الرقمي دراسة مقارنة متعمقة بين التشريعين المصري والجزائري

المؤلف

د. محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني والمحاضر الدولي في القانون

الإهداء

الي روح امي وابي الطاهره اللهم اغفر لهم وارحمهما وادخلهم الجنه بغير حساب يارب العالمين

التقديم

في عصر تحولت فيه البيانات إلى "النفط الجديد"، وأصبحت الهجمات السيبرانية تهديداً وجودياً للأمن القومي والاستقرار الاقتصادي، برزت الحاجة الماسة لأطر قانونية رادعة وشاملة لحماية البنية التحتية الرقمية وخصوصية الأفراد. لم يعد الأمن السيبراني مجرد مسألة تقنية بحتة، بل أصبح ركيزة أساسية للسيادة الوطنية. ورغم الخطوات الجادة التي خطتها مصر والجزائر بإصدار قوانين متخصصة للأمن السيبراني وحماية البيانات الشخصية مؤخراً، إلا أن التطبيق العملي يواجه تحديات معقدة تتعلق بتوازن دقيق بين متطلبات الأمن الوطني وحقوق الإنسان في الخصوصية، وبين ضرورة تدفق البيانات للاقتصاد الرقمي ووجوب توطينها محلياً.

يأتي هذا الكتاب لسد فجوة استراتيجية في المكتبة القانونية العربية، مقدماً دراسة مقارنة جراحية لمنظومتي الأمن السيبراني وحماية البيانات في البلدين. فهو لا يكتفي بتحليل النصوص، بل يغوص في فلسفة "السيادة الرقمية"، مسؤوليات مقدمي الخدمة في الإبلاغ عن الاختراقات، عقوبات التجسس

الإلكتروني، وآليات التعاون الدولي في ملاحقة مجرمي الإنترنت. إن الفروق الدقيقة في تعريف "البيانات الحساسة" و"البنية التحتية الحيوية" بين القاهرة والجزائر قد تحدد مصير استثمارات رقمية ضخمة أو تكشف عن ثغرات أمنية كارثية.

في هذا العمل المتقدم، قمنا بتشريح المنظومة القانونية للأمن السيبراني عبر عشرة فصول ذات عمق تحليلي استثنائي، نقارن فيها بين نصوص قوانين الأمن السيبراني، قوانين حماية البيانات الشخصية، وقوانين مكافحة الجرائم الإلكترونية في مصر والجزائر، مستفيدين من معايير المنظمة الدولية للتوحيد القياسي (ISO) وتوجيهات الاتحاد الدولي للاتصالات (ITU). هدفنا هو تقديم مرجع استراتيجي يساهم في بناء فضاء رقمي عربي آمن، يحفظ الخصوصية، ويصد الهجمات، ويدعم الثقة في الاقتصاد الرقمي.

الفهرس

مفهوم السيادة الرقمية

يناقش الفصل تطور مفهوم السيادة ليشمل الفضاء السيبراني. هل للدولة الحق المطلق في التحكم في تدفق البيانات داخل حدودها؟ كيف توازن القوانين المصرية والجزائرية بين السيادة والانفتاح العالمي؟

الأمن السيبراني كحق أساسي وواجب وطني

يستعرض التحول في النظر للأمن السيبراني من كونه خدمة اختيارية إلى كونه حقاً للمواطن في بيئة آمنة وواجباً على كل كيانات الدولة والقطاع الخاص.
المقارنة بين الدستور والقوانين المنظمة في البلدين.

التوازن بين الأمن والخصوصية

المعضلة الأزلية: كيف نضمن أمن الشبكة دون انتهاك خصوصية المستخدمين؟ تحليل الضمانات القانونية في مصر والجزائر لمنع إساءة استخدام صلاحيات المراقبة

باسم الأمن السيبراني.

نهج "الأمن بالتصميم" Security by Design

مبدأ إلزام مطوري الأنظمة ومقدمي الخدمة بدمج معايير الأمان منذ مرحلة التصميم الأولى وليس كإضافة لاحقة. مدى تبني هذا المبدأ في اللوائح التنفيذية للبلدين.

مسؤولية الدولة في الحماية

التزام الدولة الإيجابي بحماية مواطنيها ومنشآتها من الهجمات الخارجية. متى تتحمل الدولة المسؤولية التقصيرية عن فشلها في صد هجوم سيبراني أدى لضرر للأفراد؟

الفصل الثاني

الإطار المؤسسي الوطني مراكز الاستجابة للهجمات وصلاحيات الجهات الرقابية

إنشاء الهيئات الوطنية المختصة

يستعرض الهياكل المؤسسية المنشأة حديثاً: الجهاز الوطني للأمن السيبراني في مصر، والهيئة الوطنية للأمن السيبراني في الجزائر. استقلالية هذه الهيئات وعلاقتها بالرئاسة والوزارات.

مراكز الاستجابة للطوارئ الحاسوبية (CERT/CSIRT)

دور المراكز الوطنية في رصد الهجمات، إصدار التحذيرات، وتنسيق الاستجابة للحوادث. آليات عملها وتعاونها مع القطاع الخاص في البلدين.

صلاحيات التفتيش والفحص

السلطات الواسعة الممنوحة للجهات الرقابية في دخول مقار الشركات، فحص الأنظمة، ومراجعة سجلات الأمان. الضمانات الإجرائية لمنع التعسف التجاري تحت غطاء التفتيش الأمني.

تحديد معايير الأمن الوطني

سلطة الهيئات الوطنية في إصدار معايير إلزامية للأمن السيبراني تلزم كافة الجهات الحكومية والحيوية بالامتثال لها. مقارنةصرامة هذه المعايير في مصر والجزائر.

التنسيق الدولي

دور هذه الهيئات كممثل رسمي للدولة في المحافل الدولية للأمن السيبراني وتوقيع اتفاقيات التعاون الثنائي والمتعدد الأطراف.

الفصل الثالث

حماية البنية التحتية الحيوية للدولة من الهجمات السيبرانية

تعريف البنية التحتية الحيوية

من يحدد ما يدخل ضمن "البنية الحيوية"؟ (كهرباء، مياه، اتصالات، بنوك، صحة). مقارنة قوائم القطاعات الحيوية في التشريعين المصري والجزائري ومدى شموليتها.

التصنيف والترخيص

نظام تصنيف منشآت البنية التحتية حسب درجة حساسيتها وتأثرها بالهجمات. اشتراطات تراخيص التشغيل الخاصة بالأمن السيبراني لهذه المنشآت.

خطط الصمود والاستمرارية

إلزام مشغلي البنية الحيوية بوضع خطط لاستمرارية الأعمال (BCP) والتعافي من الكوارث (DRP) لضمان عدم توقف الخدمات الحيوية حتى عند حدوث اختراق.

الفحوصات الدورية واختبار الاختراق

التزام هذه المنشآت بإجراء فحوصات دورية واختبارات اختراق (Penetration Testing) بواسطة جهات معتمدة وتقديم التقارير للجهة الرقابية.

العقوبات المشددة على استهداف البنية الحيوية

النصوص الجنائية الخاصة التي تجرم الهجوم على البنية التحتية الحيوية بعقوبات أقسى بكثير من الجرائم السيبرانية العادية، واعتبارها جريمة ضد الأمن القومي.

الفصل الرابع

نظام حماية البيانات الشخصية المبادئ العامة والحقوق الفردية

تعريف البيانات الشخصية والحساسة

التفريق الدقيق بين البيانات العادية (الاسم، العنوان) والبيانات الحساسة (المعتقدات، الصحة، البيانات البيومترية). كيف عالجتها قوانين حماية البيانات في مصر والجزائر؟

مبادئ معالجة البيانات

استعراض المبادئ الأساسية: الشرعية، العدالة، الشفافية، تحديد الغرض، تقليل البيانات، الدقة، وتحديد مدة الحفظ. مقارنة التطبيق في البلدين.

حقوق صاحب البيانات

الحق في الاطلاع، التصحيح، الحذف (حق النسيان)، الاعتراض، ونقل البيانات. الإجراءات العملية لممارسة هذه الحقوق أمام الشركات والجهات الحكومية في مصر والجزائر.

أساس شرعية المعالجة

متى يجوز معالجة البيانات؟ (الموافقة، تنفيذ عقد، التزام قانوني، حماية مصالح حيوية، المصلحة العامة). تحليل دقة النصوص حول "الموافقة المستنيرة".

دور جهة الرقابة على حماية البيانات

صلاحيات الجهاز الوطني لحماية البيانات الشخصية في مصر والهيئة الوطنية المكلفة بذلك في الجزائر في تلقي الشكاوى، التحقيق، وفرض الغرامات.

الفصل الخامس

نقل البيانات عبر الحدود وتوطين البيانات القيود والضوابط

مبدأ توطين البيانات Data Localization

يناقش الإشكالية الكبرى: هل يلزم القانون تخزين نسخ من البيانات محلياً؟ مقارنة بين النهج الصارم في بعض قطاعات الدولة في مصر والجزائر والنهج الأكثر مرونة في القطاعات الأخرى.

شروط نقل البيانات للخارج

الشروط اللازمة لنقل البيانات خارج الإقليم الوطني: وجود مستوى حماية كافٍ في البلد المستقبل، الحصول على إذن من الجهة الرقابية، أو وجود ضمانات

تعاقدية قياسية.

الاستثناءات الأمنية

الحالات التي تمنع فيها الدولة نقل البيانات تماماً لأسباب تتعلق بالأمن القومي أو السيادة. قائمة القطاعات المحظور نقل بياناتها خارج البلاد في التشريعين.

تأثير الاتفاقيات الدولية

كيف تؤثر اتفاقيات التجارة الحرة أو التعاون القضائي على قواعد نقل البيانات؟ التوتر بين الالتزامات الدولية ومتطلبات التوطين المحلي.

آليات الرقابة على التدفق

الأدوات التقنية والقانونية التي تستخدمها الجهات

الرقابية لرصد ومنع التدفق غير المشروع للبيانات الحساسة عبر الحدود.

الفصل السادس

التزامات مقدمي الخدمة ومشغلي الأنظمة في تأمين الشبكات والإبلاغ عن الاختراقات

واجب تأمين الشبكات

الالتزام القانوني العام لمقدمي خدمات الاتصالات ومزودي الخدمة عبر الإنترنت (ISPs) ومنصات البيانات باتخاذ التدابير الفنية والإدارية اللازمة لتأمين شبكاتهم.

إلزامية الإبلاغ عن خروقات البيانات

مواعيد وإجراءات الإبلاغ الإلزامي للجهة الرقابية وللمتضررين في حال حدوث اختراق للبيانات. مقارنة

المواعيد الدقيقة (مثلاً 72 ساعة) والعقوبات على التأخير في مصر والجزائر.

تعيين مسؤول حماية البيانات (DPO)

اشتراط تعيين شخص مسؤول عن حماية البيانات في الجهات الكبيرة أو التي تعالج بيانات حساسة. مؤهلات هذا المسؤول وصلاحياته واستقلاليته.

تقييم أثر حماية البيانات (DPIA)

إلزامية إجراء تقييم مسبق للمخاطر قبل الشروع في مشاريع معالجة بيانات جديدة قد تشكل خطراً عالياً على الحقوق والحريات.

الحفاظ على سجلات المعالجة

التزام الجهات بالاحتفاظ بسجلات مفصلة لأنشطة

معالجة البيانات لتكون متاحة للفحص من قبل الجهة الرقابية في أي وقت.

الفصل السابع

الرقابة الحكومية وصلاحية الوصول للبيانات لأغراض الأمن الوطني

أوامر الكشف عن البيانات

الإجراءات القانونية اللازمة لطلب الجهات الأمنية والقضائية كشف بيانات المستخدمين من الشركات. درجة السرية المحيطة بهذه الطلبات وضمانات عدم إساءة الاستخدام.

التنصت والمراقبة الوقائية

النصوص التي تسمح بالتنصت على الاتصالات ومراقبة

المحتوى الرقمي لأغراض preventiva لمكافحة الإرهاب والجريمة المنظمة. دور القضاء في الإذن بهذه الإجراءات في مصر والجزائر.

تشفير البيانات ونقاط النهاية

الإشكالية القانونية حول "الأبواب الخلفية" Backdoors: هل يمكن إجبار الشركات على فك تشفير بيانات المستخدمين أو تزويد الحكومة بمفاتيح التشفير؟ موقف التشريعين من التشفير الطرفي.

حظر المواقع والتطبيقات

الصلاحيات الإدارية والقضائية لحجب المواقع أو التطبيقات التي تهدد الأمن القومي أو تنشر أخباراً كاذبة. إجراءات الطعن في قرارات الحجب.

التوازن مع حقوق التعبير

كيف تضمن القوانين ألا تتحول صلاحيات الأمن السيبراني إلى أداة لقمع حرية التعبير الرأي؟ تحليل الضمانات الدستورية والقضائية في البلدين.

الفصل الثامن

الجرائم السيبرانية الكبرى التجسس والتخريب والابتزاز الإلكتروني

جريمة التجسس السيبراني

تعريف التجسس عبر الوسائل الرقمية على أسرار الدولة أو الأسرار التجارية. تمييزها عن جمع المعلومات المفتوحة. عقوباتها المشددة في قانون العقوبات وقوانين خاصة في مصر والجزائر.

جريمة التخريب الإلكتروني

تدمير أو تعطيل الأنظمة المعلوماتية، حذف البيانات، أو نشر الفيروسات وبرامج الفدية. اعتبارها جرائم مادية بحتة أم جرائم نية؟

الابتزاز الإلكتروني والاحتيال

استغلال البيانات المسروقة أو الصور الخاصة للابتزاز المالي أو المعنوي. تطور أساليب الاحتيال الإلكتروني وسرقة الهوية وآليات المواجهة القانونية.

انتحال صفة المواقع والمؤسسات

إنشاء مواقع وهمية تحاكي مؤسسات رسمية أو بنوكاً لخداع المستخدمين. الإجراءات العاجلة لإغلاق هذه المواقع ومقاضاة مرتكبيها.

الجرائم ضد الأطفال في الفضاء الرقمي

حماية خاصة للأطفال من الاستغلال الجنسي، التنمر الإلكتروني، وجذب القاصرين عبر الإنترنت. تشديد العقوبات على هذه الجرائم في التشريعين.

الفصل التاسع

العقوبات الإدارية والجنائية ومسؤولية الأشخاص الاعتباريين

الغرامات الإدارية التصاعدية

نظام الغرامات الضخمة المفروضة على مخالفة قوانين حماية البيانات والأمن السيبراني (نسبة من حجم الأعمال أو مبالغ ثابتة كبيرة). مقارنة قيم الغرامات في مصر والجزائر ومدى ردعيتها.

العقوبات السالبة للحرية

عقوبات السجن المقررة للجرائم السيبرانية الخطيرة.
توجيهات sentencing guidelines للقضاة لتحديد العقوبة المناسبة حسب جسامة الضرر.

مسؤولية الشخص الاعتباري (الشركات)

إمكانية محاكمة الشركات جنائياً وإدانتها عن الجرائم السيبرانية المرتكبة لصالحها. العقوبات التبعية مثل إغلاق الموقع، مصادرة الأجهزة، أو منع ممارسة النشاط.

المسؤولية المدنية والتعويضات

حق المتضررين من خروقات البيانات أو الهجمات السيبرانية في المطالبة بتعويضات مادية وأدبية.
سهولة أو صعوبة إثبات الضرر في البيئة الرقمية.

العقوبات التبعية

نشر الحكم، إغلاق الحسابات البنكية للمدانين، ومنع السفر. دور هذه العقوبات في تعزيز الردع العام.

الفصل العاشر

دراسة مقارنة معمقة للمستقبل التشريعي والتعاون الإقليمي في مواجهة التهديدات المشتركة

فجوات التطبيق والقدرات البشرية

تحليل نقدي للتحديات: نقص الخبراء الوطنيين، بطء تحديث التقنيات الرقابية، وصعوبة مواكبة سرعة تطور أساليب المجرمين مقارنة بسرعة التشريع.

التناغم مع المعايير العالمية

مدى توافق قوانين مصر والجزائر مع اتفاقية بودابست والمعايير الأوروبية (GDPR) لتسهيل التعاملات الرقمية الدولية وجذب الاستثمار.

إنشاء سوق رقمي عربي آمن

رؤية لإنشاء إطار تعاوني عربي موحد للأمن السيبراني، يتضمن تبادل الخبرات، الإنذار المبكر المشترك، وتسليم المجرمين الإلكترونيين بسهولة بين الدول العربية.

الذكاء الاصطناعي والأمن السيبراني

كيف ستغير تقنيات الذكاء الاصطناعي مشهد الهجمات والدفاع؟ الحاجة لتشريعات مستقبلية تنظم استخدام الذكاء الاصطناعي في الأمن السيبراني وتمنع استخدامه في الهجمات الذاتية.

بناء ثقافة الأمن السيبراني المجتمعي

دور التعليم والإعلام في رفع وعي المواطنين والمؤسسات بأهمية الأمن السيبراني كسلوك يومي وليس مجرد التزام قانوني.

الخاتمة

نحو سيادة رقمية آمنة وخصوصية مصانة

ختاماً، يمثل الأمن السيبراني وحماية البيانات الركيزتين الأساسيتين لبناء مجتمع رقمي موثوق في مصر والجزائر. ومن خلال هذه الدراسة المعمقة، يتضح أن البلدين قد قطعا شوطاً كبيراً في بناء الترسانة التشريعية، لكن التحدي الحقيقي يكمن في التطبيق الفعال، وبناء الكوادر الوطنية، وتعزيز التعاون الإقليمي.

إن المستقبل سيكون لمن يمتلك البيانات ويؤمنها في

آن واحد. نأمل أن يكون هذا الكتاب دليلاً استراتيجياً للمشرع في سد الثغرات، وللقاضي في فهم تعقيدات الجريمة الرقمية، وللمستثمر في طمأنته على بيئة أعمال آمنة. إن تحقيق التوازن بين الأمن والحرية هو السبيل الوحيد لضمان ازدهار دائم في العصر الرقمي.

المراجع والمصادر

أولا التشريعات المصرية

قانون تنظيم الاتصالات المصري رقم 10 لسنة 2003 وتعديلاته

قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018

قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020

قانون إنشاء الجهاز الوطني للأمن السيبراني (والقرارات الجمهورية المنشئة له)

قانون تنظيم الصحافة والإعلام (فيما يتعلق بحجب المواقع)

مجموعة أحكام محكمة النقض المصرية في الجرائم الإلكترونية

ثانيا التشريعات الجزائرية

القانون رقم 18-05 المتعلق بالتجارة الإلكترونية (الأجزاء المتعلقة بالأمن)

القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها

القانون العضوي المتعلق بحماية الأشخاص الطبيعيين في معالجة البيانات ذات الطابع الشخصي

المرسوم الرئاسي المتعلق بإنشاء الهيئة الوطنية للأمن السيبراني وصلاحياتها

قانون العقوبات الجزائري (باب الجرائم ضد أنظمة المعالجة الآلية للبيانات)

مجلات الأحكام الصادرة عن المجلس الأعلى الجزائري والمحكمة العليا

ثالثا الاتفاقيات الدولية والمرجعيات

اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية (اتفاقية بودابست)

لائحة حماية البيانات العامة للاتحاد الأوروبي (GDPR) كمرجع مقارن رئيسي

إطار عمل منظمة التعاون الإسلامي للأمن السيبراني

توصيات الاتحاد الدولي للاتصالات (ITU) حول

المؤشرات العالمية للأمن السيبراني (GCI)

معايير الأيزو ISO/IEC 27001 لأمن المعلومات

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي