

السياسة الجنائية الوقائية العراقية تجاه حماية الشبكة

العنكبوتية و الاتصالات

الاستاذ: محمد علي حاجي ده آبادي

دكتوراه في القانون الجنائي وعلم الاجرام. أستاذ مشارك

في كلية القانون / جامعة قم ايران

Dr_hajidehabadi@yahoo.com

الباحث: محمد مبارك

قسم القانون الجنائي وعلم الاجرام , كلية القانون , جامعة قم , ايران

mohmed.abdlamer66@gmail.com

الملخص

أصبحت حماية الخصوصية في البيئة الرقمية من المسائل التي لا تكفي فيها الاستجابة العقابية اللاحقة. فالاعتداء الواقع عبر الشبكة العنكبوتية أو وسائل الاتصال قد ينتشر في ثوان، وقد يستحيل بعد ذلك استرداد البيانات أو إزالة الصور والمحادثات من جميع المنصات التي وصلت إليها. تبحث هذه الدراسة في مدى قيام السياسة الجنائية العراقية بوظيفة وقائية تسبق وقوع الاعتداء، ولا تقتصر على معاقبة مرتكبه بعد تحقق الضرر. وتتطلب من تحليل مواد الدستور العراقي لسنة ٢٠٠٥، وقانون العقوبات رقم ١١١ لسنة ١٩٦٩، وقانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١، وقانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم ٧٨ لسنة ٢٠١٢، وقانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم ٣١ لسنة ٢٠١٣، فضلاً عن قانون منع إساءة استعمال أجهزة الاتصالات رقم ٦ لسنة ٢٠٠٨ النافذ في إقليم كردستان. واعتمد البحث المنهج التحليلي النقدي، مع الاستعانة بالمقارنة حين تساعد على كشف النقص في التشريع العراقي، من غير نقل نموذج أجنبي بصورة آلية. وتبين أن العراق يملك أساساً دستورياً صريحاً لحماية الخصوصية وسرية الاتصالات، لكنه يعتمد في التجريم على نصوص متفرقة وضع معظمها قبل الانتشار الواسع للإنترنت. كما لا يوجد حتى الآن قانون اتحادي شامل لحماية البيانات الشخصية، ولا تنظيم إجرائي متكامل لحفظ الدليل الرقمي وجمعه وتداوله. وتقرّر الدراسة سياسة وقائية متعددة المستويات تجمع بين التجريم الدقيق، والتزامات أمن البيانات، والرقابة القضائية على اعتراض الاتصالات، والإخطار عن تسرب البيانات، والتوعية الرقمية، والتخصص المؤسسي، والتعاون الدولي. الكلمات المفتاحية: السياسة الجنائية الوقائية؛ الخصوصية الرقمية؛ الشبكة العنكبوتية؛ الاتصالات؛ البيانات الشخصية؛ القانون العراقي.

Abstract

The protection of privacy in the digital environment can no longer depend solely on punishment after harm has occurred. An infringement committed through the Internet or modern means of communication may spread within seconds, while the subsequent recovery of personal data or the complete removal of images and conversations may become practically impossible. This study examines whether Iraqi criminal policy performs a preventive function capable of preceding digital privacy violations. It analyses the Iraqi Constitution of 2005, Penal Code No. 111 of 1969, Criminal Procedure Code No. 23 of 1971, Electronic Signature and Electronic Transactions Law No. 78 of 2012, Law No. 31 of 2013 ratifying the Arab Convention on Combating Information Technology Offences, as well as Kurdistan Region Law No. 6 of 2008 on the misuse of communication devices. The study adopts an analytical and critical method, using comparison only where it reveals a specific gap in Iraqi law. It concludes that Iraq has an explicit constitutional basis for privacy and

confidentiality of communications, but its criminal protection remains fragmented and largely dependent on provisions drafted before the widespread use of the Internet. Iraq also lacks a comprehensive federal personal data protection law and a complete procedural system for preserving and handling digital evidence. The study proposes a multi-level preventive policy combining precise criminalisation, data-security duties, judicial control of interception, breach notification, digital awareness, institutional specialisation, and international cooperation. Keywords: Preventive criminal policy; digital privacy; Internet; communications; personal data; Iraqi law.

المقدمة

لم تعد حياة الإنسان الخاصة محصورة في منزله أو رسائله الورقية. جزء واسع منها صار محفوظاً في الهاتف والحاسوب والبريد الإلكتروني والحسابات السحابية وتطبيقات التواصل. وتضم هذه المساحة صوراً ومحادثات وبيانات مالية وصحية ومهنية، إلى جانب سجل الحركة والاتصال والبحث. لهذا لم يعد الاعتداء على الخصوصية يحتاج إلى دخول منزل أو الاستيلاء على ملف ورقي. قد يبدأ رابط خادع، أو كلمة مرور ضعيفة، أو موظف يملك صلاحية أوسع من حاجته، أو تطبيق يجمع بيانات تتجاوز الغرض المعلن للمستخدم. تختلف خطورة هذا الاعتداء عن صور المساس التقليدية. النسخة الرقمية قابلة للاستساخ من غير أن يفقد صاحبها الأصل، ويمكن نقلها إلى عدد كبير من الأشخاص خلال وقت قصير. وقد يبقى أثرها متاحاً بعد حذفها من المصدر الأول. كما أن الفاعل قد يوجد خارج العراق، بينما يوجد الخادم في دولة ثانية والضحية في دولة ثالثة. هذه الطبيعة تضعف أثر العقوبة إذا لم تسبقها تدابير تمنع الوصول غير المشروع أو تقلل فرص التسريب وتحفظ الدليل فور ظهوره. وقد وصفت الدراسات الجريمة السيبرانية بأنها جريمة يصعب كشفها بسبب طبيعة البيانات القابلة للمحو وسهولة إخفاء الأثر الإلكتروني، كما أن تجاوزها للحدود يجعل التعاون الدولي جزءاً من مواجهتها، لا مسألة إضافية عليها (الربيعي، ٢٠٢٤، ص ٧٧).

تتبع مشكلة البحث من وجود مسافة واضحة بين الاعتراف الدستوري بالخصوصية وبين الأدوات التشريعية المتاحة لحمايتها في الواقع الرقمي. فالمادة ١٧ من الدستور تقرر الحق في الخصوصية الشخصية، والمادة ٤٠ تحمي سرية الاتصالات والمراسلات، لكن قانون العقوبات رقم ١١١ لسنة ١٩٦٩ سابق بطبيعته على شبكات التواصل والحوسبة السحابية ومعالجة البيانات الضخمة. وقانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم ٧٨ لسنة ٢٠١٢ ينظم الثقة والحجية في المعاملة الإلكترونية أكثر مما ينظم المعالجة العامة للبيانات الشخصية. لهذا تبقى الحماية موزعة بين قواعد دستورية وجزائية وإجرائية وقطاعية، من دون قانون اتحادي يجمع المبادئ والالتزامات والحقوق والجزاءات في نظام واحد. وقد أكدت دراسة حديثة أن الإطار العراقي لا يزال قائماً على نصوص متفرقة ولا يرقى إلى حماية تشريعية متخصصة (الركابي وشبيري زنجاني، ٢٠٢٦، ص ٣٠٦٣).

يطرح البحث السؤال الرئيس الآتي: ما مدى كفاية السياسة الجنائية الوقائية العراقية لحماية الخصوصية عبر الشبكة العنكبوتية والاتصالات؟ ويتفرع عنه عدد من الأسئلة: ما الأساس الدستوري والقانوني لهذه الحماية؟ وهل تستطيع النصوص التقليدية استيعاب صور الوصول غير المشروع والاعتراض وجمع البيانات وإفشائها؟ وما موقع الوقاية التقنية والمؤسسية في السياسة الجنائية العراقية؟ وكيف يمكن تنظيم إجراءات البحث والحجز وحفظ الدليل الرقمي من غير إهدار الخصوصية؟

يهدف البحث إلى تحديد مضمون الوقاية الجنائية في المجال الرقمي، ورسم خريطة دقيقة للنصوص العراقية النافذة، وبيان ما توفره من حماية وما تتركه من فراغ. كما يسعى إلى التمييز بين القانون النافذ ومشروع القانون أو المقترح التشريعي، لأن الخلط بينهما يؤدي إلى بناء نتائج على قواعد لا تتمتع بالقوة الملزمة. وفي ضوء ذلك يقدم البحث تصوراً تشريعياً ومؤسسياً يربط حماية الخصوصية بأمن البيانات، ولا يحول مكافحة الجريمة السيبرانية إلى مبرر لمراقبة واسعة غير خاضعة للضمانات.

اعتمدت الدراسة المنهج التحليلي النقدي؛ فحللت النصوص العراقية النافذة بحسب درجتها ونطاق تطبيقها، ثم اختبرت قدرتها على منع الاعتداء قبل وقوعه أو الحد من نتائجه. واقتصرت المقارنة على أدوات محددة وردت في اللائحة الأوروبية العامة لحماية البيانات، ولا سيما تقليل البيانات في المادة ٥، والخصوصية منذ التصميم في المادة ٢٥، وأمن المعالجة في المادة ٣٢، والإخطار عن خرق البيانات في المادتين ٣٣ و ٣٤. والغاية من هذه المقارنة هي تقييم النقص في التنظيم العراقي وبيان ما يمكن تكييفه معه، لا نقل النموذج الأوروبي بحذافيره.

ينحصر نطاق البحث في الحماية القانونية للخصوصية والبيانات الشخصية وسرية الاتصالات داخل العراق. ويستعان بقانون إقليم كردستان بوصفه نموذجاً إقليمياً لا حكماً اتحادياً. أما التحليل الميداني لمعدلات الجريمة أو اتجاهات القضاء فلا يدخل في حدود الدراسة؛ ولذلك تقوم النتائج على النصوص والوثائق المنشورة، ولا تقدم قياساً إحصائياً لفاعلية التنفيذ.

درس قصي علي عباس حجية الدليل الإلكتروني في الإثبات الجنائي، وربط قبول هذا الدليل بأصالته وصلته بالدعوى وموثوقيته، كما أكد أهمية اتباع إجراءات صحيحة في جمعه وحفظه واستمرار سلسلة حيازته (عباس، ٢٠٢٤، ص ١١٥). يلتقي بحثه مع الدراسة الحالية في الجانب الإجرائي، بينما يظل اهتمامنا أوسع من الحجية القضائية؛ إذ يشمل حفظ البيانات سريعاً وتحديد نطاق التفتيش ومنع تحول التحقيق إلى كشف شامل للحياة الخاصة. تناولت نورهان محمد الربيعي الجريمة السيبرانية وآليات مكافحتها في دراسة مقارنة بين العراق والإمارات، وجمعت بين الجوانب الموضوعية والإجرائية. وأشارت إلى أن الوقاية تحتاج إلى الوعي بالأمن السيبراني وتحديث التشريعات والتعاون بين الدولة والقطاع الخاص (الربيعي، ٢٠٢٤، ص ٧٤). تستفيد الدراسة الحالية من هذا الاتجاه، لكنها لا تتعامل مع الأمن السيبراني والخصوصية على أنهما مترادفان. فقد يكون النظام آمناً تقنياً، ومع ذلك يجمع بيانات أكثر مما يحتاج أو يستخدمها لغرض لم يقبل به صاحبها.

وعالج الركابي وشبيري زنجاني التحديات التكنولوجية لحماية البيانات الشخصية في القانون العراقي والإيراني والأوروبي. وبيناً أن البيانات تشمل الاسم والصورة والصوت ورقم الهوية والبريد الإلكتروني والبصمة وغيرها من العناصر القابلة لتحديد الشخص، كما أكد غياب قانون عراقي محدد لحماية البيانات الشخصية (الركابي وشبيري زنجاني، ٢٠٢٦، ص ٣٠٦٨). وتمتاز دراستهما بإدخال التشفير وإخفاء الهوية والخصوصية منذ التصميم في التحليل القانوني. يستكمل البحث الحالي هذا الجانب من منظور السياسة الجنائية الوقائية، مع التحفظ على أي نص عقابي منسوب إلى قانون عراقي لم يثبت نفاذه.

وفرق محمد زيدون خلف جبار وحيدر غازي فيصل بين الجريمة الرقمية والأمن السيبراني وأمن المعلومات والخصوصية الرقمية، ونبها إلى أن الخلط بينها ينعكس على دقة المعالجة التشريعية (جبار وفیصل، ٢٠٢٥، ص ٩٥٨). يفيد هذا التمييز الدراسة الحالية بصورة مباشرة؛ فالأمن السيبراني إطار وقائي واسع، أما الخصوصية فهي حق للفرد قد ينتهك حتى من دون اختراق تقني، كما يقع عند جمع البيانات بصورة قانونية في ظاهرها ثم استخدامها لغرض آخر.

يتضح من عرض الدراسات السابقة أن الأدبيات تناولت الحماية الجنائية أو صور الجرائم أو الدليل الإلكتروني أو الأمن السيبراني، لكن الحاجة لا تزال قائمة لدراسة تجمع النص الدستوري والتجريم التقليدي والتنظيم التقني والإجراءات والمؤسسات ضمن مفهوم واحد للوقاية. هذه هي المساحة التي يحاول البحث معالجتها.

المبحث الأول: الإطار المفاهيمي والدستوري للحماية الوقائية

المطلب الأول: مفهوم الخصوصية الرقمية والسياسة الجنائية الوقائية

يصعب وضع تعريف جامد للخصوصية، لأنها تتغير بحسب طبيعة المعلومة والسياق وتوقع الشخص المعقول للسرية. وقد يكون الاسم معلومة عادية في موضع، ثم يصبح كاشفاً عن وضع صحي أو سياسي حساس إذا ربط بقاعدة بيانات أخرى. لذلك لا تنحصر الخصوصية في إخفاء المعلومات، بل تشمل قدرة الشخص على معرفة ما يجمع عنه، والغرض من الجمع، والجهة التي ستستخدم البيانات، والمدة التي ستحتفظ بها، والأشخاص الذين يمكنهم الوصول إليها. (شيدانيان وعبد، ٢٠٢٦، ص ٢٩٣). ترتبط الخصوصية الرقمية بثلاث دوائر. الأولى سرية الاتصالات، أي عدم اعتراض الرسائل والمكالمات والمحادثات أو الكشف عنها من غير سند. والثانية حماية البيانات الشخصية أثناء الجمع والمعالجة والتخزين والنقل. والثالثة حرمة المجال الشخصي في المنصات الرقمية، وتشمل الصورة والصوت والموقع والحسابات والملفات الخاصة. وقد ذهب جانب من الفقه إلى اعتبار الحق في الخصوصية من الحقوق الملازمة للشخص، بما يتيح لصاحبه طلب وقف الاعتداء من غير انتظار تحقق ضرر مالي (محمد، ٢٠٢٥، ص ٦٤). يقصد بالسياسة الجنائية الوقائية مجموعة الخيارات التشريعية والإجرائية والمؤسسية والاجتماعية والتقنية التي تخفف احتمال الجريمة أو تحد من آثارها. وقد تحقق العقوبة رداً عاماً، لكنها لا تعالج وحدها قاعدة بيانات تُركت من دون حماية، أو موظفاً مُنح صلاحيات لا يحتاجها، أو حساباً مخترقاً لم يوقف في الوقت المناسب. ولهذا تبدأ الوقاية الرقمية قبل المحكمة: من طريقة تصميم النظام، وتحديد الصلاحيات، وتفعيل المصادقة متعددة العوامل، وتشفير البيانات، وتسجيل الدخول، وحفظ النسخ الاحتياطية. (خضير وحמיד، ٢٠٢٥، ص ٢٥). لهذا تتكون الوقاية الرقمية من مستويات مترابطة. الوقاية الأولية تخاطب جميع المستخدمين والمؤسسات، مثل وضع معايير أمن إلزامية والتتقيف الرقمي. والوقاية الثانوية تستهدف البيئات أو الأشخاص الأكثر تعرضاً، كالمؤسسات الصحية والمصرفية والأطفال وضحايا الابتزاز. والوقاية الثالثة تبدأ بعد وقوع الاعتداء الأول لمنع تكراره أو اتساعه، مثل تجميد الحساب المعتدي وحفظ البيانات

وإزالة المحتوى غير المشروع بأمر قضائي. هذا التقسيم يكشف أن السياسة الجنائية لا تبدأ في قاعة المحكمة، بل تبدأ من تصميم النظام وكيفية جمع البيانات. (أندرسن وجينيون، ٢٠٠٨، ص ١٦٤).

المطلب الثاني: الأساس الدستوري والدولي

أقر دستور جمهورية العراق لسنة ٢٠٠٥ في المادة ١٧/أولاً حق كل فرد في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والآداب العامة. وتضيف المادة ٤٠ حماية أكثر اتصالاً بموضوع البحث، إذ تقر حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والإلكترونية وتضمن سريتها، ولا تجيز مراقبتها أو التنصت عليها أو الكشف عنها إلا لضرورة قانونية وأمنية وبقرار قضائي. النص الثاني لا يحمي مضمون الرسالة وحده، بل يضع قيداً إجرائياً على السلطة التي تريد اعتراضها. لا يجوز فهم عبارتي «الضرورة القانونية والأمنية» على أنهما تفويض عام. فالمادة ٤٦ تشترط أن يكون تقييد الحقوق بقانون أو بناء عليه، وألا يمس التقييد جوهر الحق. ينتج من اجتماع المواد ١٧ و ٤٠ و ٤٦ أن اعتراض الاتصال يجب أن يستند إلى نص واضح، وأن يكون ضرورياً ومحدداً ومتناسباً مع هدف مشروع، وأن يخضع لقرار قضائي. المراقبة الشاملة أو غير المحددة زمنياً تتعارض مع هذا البناء حتى لو رفعت شعار الأمن. وعلى المستوى الدولي، تحظر المادة ١٢ من الإعلان العالمي لحقوق الإنسان التدخل التعسفي في الحياة الخاصة والأسرة والمساكن والمراسلات، وتقرر الحق في حماية القانون. ويعيد العهد الدولي الخاص بالحقوق المدنية والسياسية في المادة ١٧ المضمون نفسه بصيغة التزام قانوني على الدول الأطراف. وقد صادق العراق على العهد بالقانون رقم ١٩٣ لسنة ١٩٧٠. وبذلك لا يكفي أن تمتنع الدولة عن الاعتداء؛ عليها أن توفر حماية قانونية ضد تدخل الأفراد والشركات أيضاً. تزداد أهمية هذا الالتزام عندما تعالج جهة عامة بيانات المواطنين. فالدولة لا تستطيع مطالبة القطاع الخاص بمعايير لا تراعيها في قواعد بيانات الهوية والصحة والتعليم والأمن. الوقاية الدستورية تقتضي أن يكون لكل قاعدة بيانات غرض مشروع ومعلن، وأن تقتصر البيانات على القدر اللازم، وأن تحدد صلاحيات الوصول ومدة الاحتفاظ وآلية التصحيح والحذف حيث يسمح القانون. إن تحويل المعلومات الورقية إلى بيانات رقمية يزيد قابلية البحث والربط والاستتساخ، ولذلك يحتاج إلى ضمانات أقوى، لا إلى مجرد نقل القواعد القديمة إلى وسيط جديد (الركابي وشبيري زنجاني، ٢٠٢٦، ص ٣٠٧٢). (محمد، ٢٠٢٦، ص ٦٥).

المبحث الثاني: أدوات الوقاية في التشريع العراقي النافذ

المطلب الأول: الحماية في قانون العقوبات

يتضمن قانون العقوبات رقم ١١١ لسنة ١٩٦٩ عدداً من النصوص التي يمكن تطبيقها على اعتداءات تقع بوسائل رقمية. فالمواد ٤٣٠ إلى ٤٣٢ تعالج التهديد، وهو الأساس الذي تستند إليه ملاحقة صور من الابتزاز الإلكتروني متى وجه الجاني تهديداً بإفشاء صور أو معلومات أو إسناد أمور مخدشة بالشرف لحمل الضحية على فعل أو امتناع. وتفيد المواد ٤٣٣ إلى ٤٣٥ في حالات القذف والسب الواقعين عبر الرسائل أو المنصات. كما تحمي المادة ٤٣٧ الأسرار التي تصل إلى الشخص بحكم وظيفته أو مهنته أو صناعته أو طبيعته عمله، فتخاطب خطراً داخلياً مهماً هو إساءة الموظف أو المهني استعمال البيانات التي أوتمن عليها. يمثل الابتزاز مثلاً واضحاً على الحاجة إلى التدخل السريع؛ فالجاني لا يريد دائماً نشر البيانات، بل يستخدم إمكان نشرها للضغط على الضحية. وقد درست الأدبيات العراقية المسؤولية الجنائية عن الابتزاز في مواقع التواصل بوصفه سلوكاً يجمع وسيلة الاتصال والتهديد والغاية التي يسعى إليها الفاعل (عاشور، ٢٠٢٠، ص ١٠٩). لذلك يجب أن تبدأ الحماية من لحظة التهديد، مع حفظ الرسائل وتأمين حساب الضحية، ولا تنتظر تنفيذ الإفشاء. المادة ٤٣٨ هي الأقرب إلى الخصوصية بمعناها المباشر. فهي تعاقب من ينشر، بإحدى طرق العلانية، أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الإساءة إليهم، كما تعاقب من يطلع من غير إذن على رسالة أو برقية أو مكالمات هاتفية فيفتشها لغير من وجهت إليه متى ترتب على ذلك ضرر. يمكن أن تمتد عبارة «طرق العلانية» إلى النشر الرقمي وفق تفسير يراعي تطور الوسيلة، لكن الجزء المتعلق بالمراسلات صيغ قبل البريد الإلكتروني وتطبيقات المحادثة والحوسبة السحابية. (شيدائيان وعبد، ٢٠٢٦، ص ٢٩٣). تظهر في هذا التنظيم ثلاث ثغرات. الأولى أن النص يركز في بعض صورته على النشر أو الإفشاء، بينما قد يتحقق المساس بمجرد الدخول غير المشروع أو النسخ أو الجمع السري ولو لم يثبت نشر البيانات. الثانية أن اشتراط الضرر في بعض الحالات قد يؤخر التدخل إلى ما بعد انتشار المعلومة. والثالثة أن القانون لا ينظم بصورة مستقلة الاتجار بالبيانات أو إعادة استخدامها لغرض مختلف أو بناء ملفات شخصية واسعة من مصادر متعددة. ولهذا خلصت دراسة عراقية حديثة إلى أن النصوص الدستورية والجزائية التقليدية لا تكفي وحدها لحماية المعلومات الشخصية من مخاطر التقنية (علي، ٢٠٢٣، ص ١١٦). لا يعني هذا القصور انعدام الحماية القائمة. يستطيع القضاء تطبيق النصوص النافذة متى اكتملت

أركانها، ويمكن أن يكون الهاتف أو المنصة وسيلة لارتكاب التهديد أو القذف أو إفشاء السر. لكن مبدأ الشرعية يمنع مد النص التقليدي إلى فعل جديد بطريق القياس. ولهذا يظل استعمال القواعد الحالية ممكناً في حدودها، على أن يتولى المشرع تعريف الأفعال الرقمية الجديدة وتجريمها بعبارات واضحة.

المطلب الثاني: قانون التوقيع الإلكتروني والمعاملات الإلكترونية

صدر قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم ٧٨ لسنة ٢٠١٢ لتوفير إطار قانوني للمعاملات الإلكترونية وإضفاء الحجية على التوقيع والمستند الإلكتروني. وتتبع قيمته الوقائية من اشتراط الثقة والسلامة وقابلية التحقق. فالمادتان ٤ و ٥ تنظمان حجية التوقيع الإلكتروني وشروط الاعتداد به، والمواد ١٣ إلى ١٧ تتناول المستندات والسجلات الإلكترونية وحجيتها. هذه الأحكام تقلل فرص الإنكار والتلاعب إذا طبقت ضمن أنظمة موثوقة. يتضمن القانون التزامات تتصل بالأمن والسرية. فالمادة ١٠/أولاً توجب على المرخص له استعمال وسائل موثوقة عند إصدار شهادة التصديق وتسلمها وحفظها، وتنظم المادة ١١ تعليق العمل بالشهادة في الحالات المحددة قانوناً. وتقرر المادة ١٢/ثانياً سرية بيانات التوقيع الإلكتروني ووسائله والمعلومات المقدمة إلى جهة التصديق. كما تلزم المادة ٢٥ المؤسسات المالية باتخاذ إجراءات تكفل أمن خدمات الدفع الإلكتروني وسريتها. وتكشف هذه النصوص عن وظيفة وقائية واضحة، لكنها تظل مرتبطة بمجال التوقيع والمعاملات الإلكترونية ولا تنشئ نظاماً عاماً لحماية جميع البيانات الشخصية، لكن نطاق القانون محدود. فهو لا يضع نظاماً عاماً لجميع البيانات الشخصية، ولا يمنح صاحب البيانات مجموعة متكاملة من الحقوق، ولا يحدد قواعد الموافقة والشفافية وتقليل البيانات والاحتفاظ بها. كما أن أمن التوقيع لا يساوي أمن جميع قواعد البيانات. لذلك لا يجوز تقديم القانون رقم ٧٨ لسنة ٢٠١٢ على أنه قانون لحماية البيانات أو قانون لمكافحة الجرائم الإلكترونية. قيمته مكملة ومحددة بمجاله.

المطلب الثالث: الاتفاقية العربية والقوانين القطاعية والإقليمية

صادق العراق بالقانون رقم ٣١ لسنة ٢٠١٣ على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وتوفر الاتفاقية إطاراً لتجريم الدخول غير المشروع، والاعتراض غير المشروع، والاعتداء على سلامة البيانات والأنظمة، إلى جانب التعاون وتسليم المجرمين والمساعدة المتبادلة. وتبرز أهميتها لأن الجريمة الرقمية لا تقف عند الحدود، ولأن حفظ بيانات المرور أو الحصول عليها من مقدم خدمة خارج العراق يتطلب تعاوناً منظماً وسريعاً. لا يغني التصديق على الاتفاقية عن تشريع وطني واضح. فالقاضي يحتاج إلى نص داخلي يحدد أركان الجريمة والعقوبة والاختصاص والإجراءات والضمانات. كما أن سرعة التعاون لا تعني تجاوز حماية الخصوصية. يجب أن يرتبط طلب البيانات بجريمة محددة، وأن يخضع للضرورة والتناسب، وأن يميز بين بيانات المشترك وبيانات المرور ومحتوى الاتصال؛ فكل نوع يكشف قدرأ مختلفاً من الحياة الخاصة. واعتمدت الجمعية العامة للأمم المتحدة، بالقرار ٢٤٣/٧٩ المؤرخ في ٢٤ كانون الأول ٢٠٢٤، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية. تنفذ الاتفاقية بوصفها مرجعاً دولياً حديثاً في التعاون وجمع الأدلة الإلكترونية وضمانات حماية الحقوق. ومع ذلك، لا يتعامل البحث معها كقانون عراقي نافذ تلقائياً؛ فترتب آثارها الداخلية يتوقف على استكمال الإجراءات الدستورية والقانونية اللازمة في العراق. وفي إقليم كردستان صدر قانون منع إساءة استعمال أجهزة الاتصالات رقم ٦ لسنة ٢٠٠٨. يعالج القانون صوراً من التهديد والقذف والسب ونشر المعلومات أو الصور المتصلة بالحياة الخاصة عبر وسائل الاتصال. ميزته أنه واجه الوسيلة الحديثة بنص خاص في وقت مبكر. إلا أن نطاقه إقليمي، فلا يجوز وصفه بأنه قانون اتحادي نافذ في جميع العراق. كما تعرض القانون للنقد بسبب تداخل بعض أحكامه مع قانون العقوبات واتساع عدد من عباراته، وهو ما قد يثير مشكلة التوازن بين الحماية وحرية التعبير. أما قانون الاتصالات اللاسلكية رقم ١٥٩ لسنة ١٩٨٠، فهو قانون قطاعي قديم ينظم استعمال الأجهزة والترددات والترخيص، وليس قانوناً لحماية الخصوصية الرقمية. ويسهم أمر سلطة الائتلاف المؤقتة رقم ٦٥ لسنة ٢٠٠٤ في الإطار المؤسسي بإنشاء هيئة الإعلام والاتصالات وتنظيم الترخيص والطياف. ويمكن للهيئة أن تؤدي وظيفة وقائية من خلال شروط التراخيص ومعايير أمن الشبكات وحماية المشتركين، بشرط وجود أساس قانوني واضح وتنسيق مع القضاء والجهات المتخصصة.

المبحث الثالث: قصور السياسة القائمة ومتطلبات البناء الوقائي

المطلب الأول: غياب التنظيم الشامل للبيانات الشخصية

أبرز أوجه القصور عدم وجود قانون اتحادي شامل لحماية البيانات الشخصية. والنتيجة أن الالتزامات تختلف باختلاف القطاع، وقد لا يعرف المواطن من يملك بياناته أو لماذا جُمعت أو إلى من نُقلت. كما يصعب تحديد واجب المؤسسة عند حدوث اختراق: هل يجب عليها إبلاغ

الجهة المختصة؟ وفي أي مدة؟ وهل تخطر الأشخاص الذين تعرضوا للخطر؟ وما الجزاء إذا أخفت الحادث؟ هذه الأسئلة ليست تفصيلات إدارية، بل عناصر وقائية؛ لأن الإخطار المبكر يسمح بتغيير كلمات المرور وإيقاف البطاقات ومراقبة الحسابات قبل توسع الضرر. ينبغي أن يعرف القانون البيانات الشخصية بأنها كل معلومة تتعلق بشخص طبيعي محدد أو قابل للتحديد، وأن يميز البيانات الحساسة، مثل المعلومات الصحية والبيومترية والدينية والمالية وبيانات الموقع. وقد بينت الدراسات أن البيانات القابلة للتعريف لا تقتصر على الاسم، بل تشمل الصورة والصوت ورقم الهوية والبريد الإلكتروني والبصمة والحالة العائلية والمالية (الركابي وشييري زنجاني، ٢٠٢٦، ص ٣٠٦٨). هذا التعريف الواسع يمنع التحايل عبر فصل المعلومة عن الاسم مع بقاء إمكانية تحديد صاحبها بوسائل أخرى. ويجب أن يقوم التنظيم على مبادئ المشروعية وتحديد الغرض وتقليل البيانات والدقة والأمن وتحديد مدة الاحتفاظ والمساءلة. فلا تجمع المدرسة مثلاً بيانات صحية لا تحتاجها، ولا تحتفظ شركة الاتصال بسجلات إلى أجل غير محدد، ولا يجوز نقل قاعدة بيانات حكومية إلى طرف ثالث لمجرد سهولة المعالجة. ويكون صاحب البيانات على علم بالمعالجة، مع استثناءات محددة يقرها القانون للضرورة وبضمانات مناسبة. وتوضح المقارنة مع اللائحة الأوروبية العامة لحماية البيانات كيف تتحول هذه المبادئ إلى التزامات قابلة للرقابة. فالمادة ٥ تجمع مبادئ المشروعية وتحديد الغرض وتقليل البيانات والدقة وتحديد مدة الاحتفاظ والسلامة والمساءلة. وتقرض المادة ٢٥ إدماج الحماية في تصميم النظام، بينما تربط المادة ٣٢ مستوى الأمن بطبيعة الخطر. أما المادتان ٣٣ و ٣٤ فتفرقان بين إخطار الجهة الرقابية وإخطار الشخص المتضرر عند ارتفاع الخطر. لا تصلح هذه الأحكام للنقل الحرفي إلى العراق، لكنها تقدم معياراً واضحاً لقياس ما ينقص التشريع الوطني. العقوبة الجنائية لا تناسب كل مخالفة. قد تكون الغرامة الإدارية وأمر التصحيح ووقف المعالجة أكثر فاعلية في حالات الإهمال البسيط، بينما يلزم التجريم عند الدخول العمدي غير المشروع أو الاتجار بالبيانات أو إفشاء البيانات الحساسة أو اعتراض الاتصال أو تعطيل وسائل الحماية. هذا التدرج يحفظ مبدأ التناسب ويمنع تضخم التجريم، وفي الوقت نفسه يجعل المخالفة الجسيمة مكلفة بما يكفي للردع.

المطلب الثاني: النقصان الإجرائي والدليل الرقمي

تعتمد فاعلية التجريم على القدرة على إثباته. والدليل الرقمي سريع التغير؛ قد يحذف عن بعد، أو يتبدل بتحديث تلقائي، أو يوجد في خادم خارج البلاد. ولهذا تحتاج الإجراءات إلى قواعد لحفظ البيانات بصورة عاجلة، وضبط الجهاز أو نسخ محتواه بطريقة تحافظ على سلامة الأصل، وتوثيق كل شخص تعامل مع الدليل، وتسجيل قيمة البصمة الرقمية للنسخة، وتحديد نطاق البحث حتى لا يتحول ضبط هاتف واحد إلى كشف شامل لحياة صاحبه ومن تواصلوا معه. (راضي، ٢٠٢٦، ص ١١٨٣). ينظم قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ التفتيش وضبط الأشياء والأوراق في المواد ٧٢ إلى ٧٥، ويعدد في المادة ٢١٣ الأدلة التي يمكن أن تبني المحكمة اقتناعها عليها. ويمكن للقواعد العامة أن تستوعب الدليل الإلكتروني من حيث المبدأ، لكنها لا تفصل التفتيش عن بعد، والحوسبة السحابية، والحفظ العاجل لبيانات المرور، ونسخ النظام، وسلسلة الحيازة الرقمية. وقد بينت دراسة عراقية حديثة أن سلامة جمع الدليل الإلكتروني وحفظه وسلسلة حيازته شروط جوهرية لموثوقيته أمام القضاء (عباس، ٢٠٢٤، ص ١١٥). يتطلب الإصلاح الإجرائي التمييز بين ضبط الجهاز والاطلاع على محتواه. فقد يكون أخذ الهاتف ضرورياً لمنع العبث، لكن فتح جميع التطبيقات والملفات يحتاج إلى إذن يحدد الهدف والمدة ونوع البيانات. كما ينبغي أن يبين القرار القضائي سبب عدم كفاية الوسيلة الأقل مساساً، وأن يحظر استخدام البيانات العرضية غير المرتبطة بالجريمة إلا بإذن جديد. بهذه الضمانات لا تصبح مكافحة الجريمة باباً لانتهاك الخصوصية التي يراود حمايتها. (الحمداي، ٢٠٢٥، ص ٧٣١). تحتاج المحاكم كذلك إلى معيار واضح لقبول الدليل الإلكتروني: سلامة المصدر، وإمكان التحقق من عدم التعديل، ومشروعية الحصول عليه، وكفاءة الفحص، ووجود سجل متصل لحيازته. ولا تتعارض حرية القاضي في تقدير الدليل مع اشتراط ضمانات فنية تمنحه الثقة. التدريب هنا ليس إجراءً ثانوياً؛ فالقاضي والمحقق والخبير إذا لم يفهموا الفرق بين لقطة الشاشة والنسخة الجنائية، أو بين الحساب الحقيقي والحساب المنتحل، فقد يرفضون دليلاً صحيحاً أو يقبلون مادة يسهل اصطناعها. (راضي، ٢٠٢٦، ص ١١٨٣؛ عباس، ٢٠٢٤، ص ١١٥).

المطلب الثالث: الوقاية المؤسسية والتقنية والاجتماعية

لا تستطيع جهة واحدة إدارة الوقاية الرقمية. وزارة الداخلية مسؤولة عن التحري والاستجابة الجنائية، والقضاء يمنح الأذونات ويراقب الإجراءات، وهيئة الإعلام والاتصالات تملك أدوات تنظيمية تجاه مقدمي الخدمات، والبنك المركزي يشرف على قطاع شديد الحساسية، والوزارات تحتفظ بقواعد بيانات واسعة. يؤدي تشتت الاختصاص من دون بروتوكول مشترك إلى تأخر الإبلاغ وضياع الدليل وتبادل المسؤولية. أعلنت وزارة الداخلية العراقية في ١٩ شباط ٢٠٢٥ استحداث «مديرية مكافحة الجرائم الإلكترونية» لتحقيق في الجرائم المرتكبة عبر مواقع التواصل

الاجتماعي (وزارة الداخلية العراقية، ٢٠٢٥). وتمثل هذه الخطوة أساساً للتخصص، غير أن أثرها يتوقف على انتشار الوحدات المؤهلة في المحافظات، وتوفير خبراء الفحص الرقمي، وفتح قنوات آمنة للبلاغات، ومراعاة أوضاع ضحايا الابتزاز، ولا سيما النساء والأطفال. كما أن نشر بيانات سنوية منزوعة الهوية عن البلاغات ونتائج القضايا يسمح بقياس الأداء بدلاً من الاكتفاء بالتقديرات العامة. نشرت جهة الاستجابة الوطنية للحوادث السيبرانية «استراتيجية الأمن السيبراني العراقي ٢٠٢٢-٢٠٢٥» بوصفها إطاراً للرؤية الوطنية (فريق الاستجابة للحوادث السيبرانية العراقي، ٢٠٢٢، ص ١). وقد انتهت المدة المعلنة في عنوان الوثيقة، فلا يصح افتراض استمرارها بعد سنة ٢٠٢٥ من دون تمديد أو استراتيجية لاحقة منشورة. وتحتاج المرحلة التالية إلى وثيقة محدثة ترتبط بخطة تنفيذ وميزانية ومسؤوليات ومؤشرات قابلة للقياس. ويجب أن تشمل حماية بيانات المواطن إلى جانب حماية البنية الحكومية؛ فاستمرار الخدمة لا يعني اكتمال الأمن إذا كانت البيانات نفسها معرضة للتسرب. تختلف التدابير التقنية باختلاف حجم البيانات وحساسيتها، إلا أن التشفير أثناء النقل والتخزين، والمصادقة متعددة العوامل، وضبط الصلاحيات، وتسجيل عمليات الدخول والتعديل، والاختبار الدوري، وإدارة الثغرات والنسخ الاحتياطي الأمن تمثل حداً أساسياً للجهات التي تعالج بيانات واسعة أو حساسة. وتبين الأدبيات الحديثة أن الخصوصية منذ التصميم وإخفاء الهوية والتشفير تخفض حجم الضرر منذ البداية (الركابي وشبيري زنجاني، ٢٠٢٦، ص ٣٠٧٦). ولا تتفع أدوات الحماية كثيراً إذا بقيت كلمات المرور الافتراضية أو ظلت صلاحيات العاملين مفتوحة بلا حاجة. ينبغي إخضاع الأنظمة ذات الخطورة العالية لتقييم أثر حماية البيانات قبل تشغيلها. فإذا أرادت جهة استخدام التعرف على الوجه أو ربط سجلات صحية بقاعدة هوية، فعليها تحديد الضرورة والمخاطر والبدائل ومدة الاحتفاظ والجهات التي ستصل إلى النتائج. هذا التقييم يفرض التفكير في الضرر قبل وقوعه، وهو جوهر السياسة الوقائية. (الاتحاد الأوروبي، ٢٠١٦، المادة ٣٥). وتبقى الوقاية الاجتماعية ضرورية. كثير من الاعتداءات يبدأ بخداع المستخدم لا بكسر النظام. حملات الوعي العامة يجب أن تشرح بلغة بسيطة كيفية التحقق من الروابط، وحماية الحساب، وعدم إرسال الرموز السرية، والإبلاغ المبكر عن الابتزاز. ويجب أن تدرج التربية الرقمية في المدارس والجامعات، مع تدريب الموظفين الذين يتعاملون مع بيانات المواطنين. وقد أوصت دراسات عراقية بنشر الوعي والثقافة بين مستخدمي الإنترنت حتى لا يقعوا ضحايا لأعمال الاحتيال أو انتهاك الخصوصية (علي، ٢٠٢٣، ص ١١٧).

المطلب الرابع: التزامات مقدمي خدمات الاتصالات والمنصات

يحتل مقدم خدمة الاتصال أو المنصة موقعاً لا يملكه المستخدم العادي. فهو يدير البنية التي تمر عبرها البيانات، ويحدد إعدادات الخصوصية، ويحتفظ بسجلات الدخول، ويستطيع إيقاف الحساب أو حفظ بياناته. لذلك لا تكون الوقاية مكتملة إذا خاطب القانون الجاني والضحية وترك الوسيط من غير التزامات واضحة. المقصود ليس تحميل مقدم الخدمة مسؤولية كل فعل يرتكبه المستخدم، بل إلزامه بما يقدر عليه فعلاً: أمن النظام، ووضوح شروط الاستخدام، والاستجابة للأوامر القضائية، وحفظ البيانات المطلوبة لمدة محددة، وعدم كشف المحتوى من غير سند قانوني. (بن سالم وشيباني، ٢٠٢٤، ص ٥٩). يجب أن يبدأ الالتزام بالشفافية. فالمستخدم ينبغي أن يعرف البيانات التي تجمع تلقائياً، مثل عنوان الاتصال والموقع ومعرف الجهاز وملفات الارتباط، والغرض من جمعها والمدة التي ستبقى فيها. الموافقة الطويلة التي لا يقرأها أحد لا تكفي إذا كانت الصياغة مبهمّة أو كان استخدام الخدمة مشروطاً بقبول جمع لا علاقة له بالغرض الأساسي. في المقابل، لا يجوز جعل كل معالجة رهينة موافقة قابلة للسحب؛ فبعض المعالجات ضرورية لتنفيذ العقد أو لحماية النظام أو للامتثال إلى واجب قانوني. المطلوب تحديد أساس كل معالجة وعدم خلط الأغراض. الالتزام الثاني هو الأمن الملائم للخطر. تختلف الحماية المطلوبة من منتدى صغير عن شركة اتصال تحتفظ ببيانات ملايين المشتركين. كلما زاد حجم البيانات أو حساسيتها، ارتفع معيار العناية. وتدخل ضمن هذا المعيار مراجعة صلاحيات العاملين، وفصل قواعد البيانات، وتشفير النسخ الاحتياطية، وإغلاق الحسابات غير النشطة، واختبار خطط الاستجابة. وقد أكدت الأدبيات أن القانون العراقي يحتاج إلى معايير صارمة للمعالجة وآليات رصد فعالة للانتهاكات، لأن مجرد الاعتراف النظري بالخصوصية لا يمنع التسريب (الركابي وشبيري زنجاني، ٢٠٢٦، ص ٣٠٧٢). أما الالتزام الثالث فيتعلق بحفظ الدليل. عندما يتلقى مقدم الخدمة أمراً قضائياً محدداً بحفظ بيانات حساب أو اتصال، ينبغي تجميد البيانات الموجودة وقت الأمر من غير تعديل، مع توثيق زمن الحفظ وسلامة النسخة. ولا يعني ذلك إنشاء احتفاظ شامل ودائم ببيانات جميع الناس. الاحتفاظ غير المحدد يزيد الخطر، لأن القاعدة المتضخمة تصبح هدفاً جذاباً للاختراق. النموذج المتوازن يقوم على مدد أصلية معلنة، ثم حفظ موجه في قضية محددة وبأمر مختص. ويجب تنظيم إزالة المحتوى أو تقييده. في حالات نشر صورة حميمة أو رقم هاتف أو عنوان منزل بقصد الإيذاء، قد يكون الانتظار إلى نهاية المحاكمة سبباً في تضاعف الضرر. يمكن إنشاء أمر قضائي مستعجل يوقف الوصول مؤقتاً إلى المحتوى، مع حق الناشر في الاعتراض ومراجعة القرار خلال مدة قصيرة. هذه الآلية تختلف عن

الحذف الإداري الغامض؛ لأنها تربط الإجراء بمخالفة محددة، وتضعه تحت رقابة القضاء، وتحافظ على نسخة سرية تصلح دليلاً حتى لا يؤدي الحذف إلى إفلات الفاعل. تتثير المنصات العابرة للحدود صعوبة إضافية. قد لا تملك الشركة مقراً في العراق، أو قد تحتفظ بالبيانات في دولة أخرى. ويمكن للقانون أن يلزم المنصة التي توجه خدماتها بصورة واسعة إلى السوق العراقي بتعيين ممثل قانوني وقناة مخصصة للأوامر القضائية وبلاغات الطوارئ. ويجب أن يجري طلب المحتوى عبر التعاون القانوني، لا من خلال مطالبات غير رسمية تقتقر إلى الضمانات. ويكون كشف بيانات المستخدم مقيداً بنوع الجريمة وخطورة الفعل ومدى اتصال البيانات بالتحقيق. ولا بد من مراعاة التشفير من طرف إلى طرف. فهذا التشفير يحمي المواطنين والمؤسسات من التجسس والسرقة، وإضعافه بباب خلفي عام يخلق ثغرة يمكن أن يستغلها المجرم كما تستغلها السلطة. تستطيع جهات التحقيق استخدام أدلة الجهاز والنسخ الاحتياطية والبيانات الوصفية والأدوات الإجرائية الموجهة بإذن قضائي، لكن فرض ضعف بنوي على جميع الاتصالات يتعارض مع وظيفة الوقاية نفسها. والتوازن السليم لا يقوم على إلغاء التشفير، بل على تحقيق محدد ومتناسب وخاضع للمراجعة. (مفوضية الأمم المتحدة السامية لحقوق الإنسان، ٢٠٢٢، ص ١٥). يستدعي انتشار الذكاء الاصطناعي إضافة واجبات أخرى على المنصات والمؤسسات التي تبني قراراتها على تحليل البيانات. فقد تكشف الخوارزمية معلومات حساسة من بيانات تبدو متفرقة، أو تصنف الشخص بطريقة تؤثر في عمله أو ائتمانه أو حصوله على خدمة. ينبغي إخضاع الأنظمة عالية الخطورة لتقييم سابق، وتمكين الفرد من معرفة الأساس العام للقرار والاعتراض عليه، ومنع استخدام البيانات في تدريب النماذج إذا تعارض ذلك مع الغرض الذي جُمعت لأجله. وتظهر هذه المسائل أن حماية الخصوصية لم تعد مقتصرة على منع الإفشاء؛ بل تشمل الحد من الاستنتاج والمراقبة والتحكم غير المرئي. (السردى والعنابي، ٢٠٢٦، ص ٥٧١).

المطلب الخامس: تقييم مقترحات قوانين الجرائم المعلوماتية

شهد العراق أكثر من مشروع أو مقترح لقانون الجرائم المعلوماتية، لكن وجود المسودة لا يجعلها قانوناً نافذاً. وفي ٦ تموز ٢٠٢٦ أنهى مجلس النواب القراءة الأولى لمقترح قانون مكافحة جرائم تقنية المعلومات، وبقيت المناقشات اللاحقة تتعامل معه بصفته مقترحاً تشريعياً (مجلس النواب العراقي، ٢٠٢٦). ولا يكتسب النص قوة الإلزام إلا بعد استكمال التصويت والمصادقة والنشر في الوقائع العراقية. وينطبق الحكم نفسه على مشروع سنة ٢٠١١ والصيغ السابقة. وفي ٢١ أيلول ٢٠٢٦ أرجأ مجلس النواب قراءة تقرير ومناقشة المقترح، ووجه اللجان المعنية إلى استضافة الخبراء والجهات المختصة لاستكمال دراسته قبل إعادة إدراجه على جدول الأعمال (مجلس النواب العراقي، ٢٠٢٦، ٢١ أيلول). الحاجة إلى القانون لا تبرر قبول أي صياغة. النصوص الواسعة التي تستخدم عبارات مثل الإضرار بسمعة الدولة أو النظام العام من غير تحديد قد تمس حرية التعبير وتترك التمييز بين الجريمة والنقد. القانون الوقائي الجيد يحدد الفعل والمحل والقصد، ويميز الدخول غير المأذون عن تجاوز حدود الإذن، ويفرق بين البحث الأمني حسن النية والهجوم الإجرامي، ويقرر ضمانات لحماية الصحفيين والباحثين والمبلغين. وينبغي ألا يجمع قانون واحد مسائل متباعدة من دون منطق واضح. فحماية البيانات الشخصية تحتاج حقوقاً والتزامات ورقابة مستقلة، بينما يركز قانون الجرائم المعلوماتية على التجريم والإجراءات. يمكن التنسيق بين القانونين، لكن دمجهما في باب عقابي صرف سيجعل حماية المواطن تابعة لوقوع الجريمة، مع أن معظم الوقاية تتعلق بطريقة مشروعة وآمنة في جمع البيانات قبل أن يظهر أي جانٍ.

الذاتية

يظهر من تحليل النصوص أن السياسة الجنائية العراقية لحماية الخصوصية الرقمية موجودة، لكنها موزعة وغير مكتملة. يوفر الدستور أساساً للحق في الخصوصية وسرية الاتصالات والرقابة القضائية على اعتراضها. ويعالج قانون العقوبات التهديد والقتل والأسرار ونشر شؤون الحياة الخاصة والإطلاع على المراسلات، بينما يضيف قانون التوقيع الإلكتروني التزامات محددة بالأمن والسرية، وتتيح الاتفاقية العربية أساساً للتعاون في الجرائم العابرة للحدود. غير أن هذه العناصر لم تنتظم بعد في سياسة واحدة تربط حقوق صاحب البيانات بواجبات الجهات الحائزة لها وإجراءات التحقيق والرقابة المستقلة. وهذه نتيجة تشريعية لا تعني، من دون بيانات قضائية وإحصائية منشورة، الحكم على مستوى التطبيق العملي في جميع المؤسسات.

النتائج

١. يحمي الدستور العراقي الخصوصية الشخصية في المادة ١٧ وسرية الاتصالات الإلكترونية في المادة ٤٠، ويقيد المساس بهما بمقتضى المادة ٤٦. وهذه النصوص تصلح أساساً لتشريع وقائي حديث.

٢. المواد ٤٣٠ إلى ٤٣٨ من قانون العقوبات قابلة للتطبيق على عدد من الاعتداءات الرقمية، لكنها لا تنشئ نظاماً متكاملًا للدخول غير المشروع وجمع البيانات والاتجار بها وإعادة استخدامها.
٣. لا يوجد قانون اتحادي عراقي نافذ وشامل لحماية البيانات الشخصية. وما ورد في بعض المصادر عن قانون عراقي رقم ٢٠ لسنة ٢٠١٨ أو رقم ٣٠ لسنة ٢٠٢٠ لم يثبت في الوقائع العراقية، فلا يجوز الاستناد إليه.
٤. قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم ٧٨ لسنة ٢٠١٢ يقدم ضمانات مهمة للسرية والسلامة في نطاقه، لكنه ليس قانوناً عاماً لحماية البيانات ولا قانوناً للجرائم السيبرانية.
٥. قانون منع إساءة استعمال أجهزة الاتصالات رقم ٦ لسنة ٢٠٠٨ قانون إقليمي خاص بكوردستان، ولا يسري بوصفه قانوناً اتحادياً على جميع العراق.
٦. المقترحات المتعاقبة لقانون الجرائم المعلوماتية لا تكتسب صفة القانون النافذ قبل استكمال الإجراءات الدستورية ونشرها في الجريدة الرسمية. والقراءة الأولى لمقترح سنة ٢٠٢٦ لا تغير هذه النتيجة.
٧. قانون أصول المحاكمات الجزائية يوفر قواعد عامة للتفتيش والضبط والإثبات، لكنه لا ينظم بصورة كافية الحفظ العاجل للبيانات والتفتيش الرقمي وسلسلة الحياة والبحث في الخدمات السحابية.
٨. الوقاية الفعالة لا تقوم على العقوبة وحدها. يلزم دمج التشريع مع الأمن التقني والتخصص المؤسسي والتوعية والإبلاغ المبكر والتعاون الدولي.

التوصيات

١. تشريع قانون اتحادي لحماية البيانات الشخصية يحدد البيانات العادية والحساسة، ويقرر مبادئ المشروعية وتحديد الغرض وتقليل البيانات والأمن وتحديد مدة الاحتفاظ، ويمنح الشخص حقوق العلم والوصول والتصحيح والاعتراض والحذف في الحدود التي يسمح بها القانون.
٢. إنشاء جهة رقابية مستقلة لحماية البيانات، تملك تلقي الشكاوى والتفتيش وإصدار أوامر التصحيح وفرض الجزاءات الإدارية، مع خضوع قراراتها للطعن القضائي.
٣. سن قانون دقيق لمكافحة جرائم تقنية المعلومات يجرم الدخول والاعتراض والتدخل في البيانات والأنظمة والاتجار غير المشروع بالبيانات، مع تجنب العبارات الفضفاضة التي قد تستخدم ضد التعبير المشروع.
٤. تعديل قانون أصول المحاكمات الجزائية لإضافة أحكام خاصة بالحفظ العاجل، وأوامر تقديم البيانات، والتفتيش الرقمي المحدد، وسلسلة الحياة، والبصمة الرقمية، والبيانات الموجودة خارج الإقليم.
٥. إلزام المؤسسات العامة والخاصة بالإبلاغ عن تسرب البيانات خلال مدة قانونية قصيرة، وإخطار المتضررين إذا كان الاختراق يعرض حقوقهم لخطر جدي.
٦. فرض معايير أمن متدرجة بحسب حجم البيانات وحساسيتها، وفي مقدمتها التشفير والمصادقة متعددة العوامل وتحديد الصلاحيات والاختبار الدوري وخطط الاستجابة للحوادث.
٧. تحديث الاستراتيجية الوطنية للأمن السيبراني بعد انتهاء مدة استراتيجية ٢٠٢٢-٢٠٢٥، وإدراج حماية الخصوصية والبيانات الشخصية ضمن أهدافها ومؤشرات قياسها.
٨. توسيع وحدات التحقيق الرقمي وتدريب القضاة والمحققين والخبراء، وإنشاء مسار أمن وسريع لشكاوى الابتزاز وانتحال الحسابات وتسريب الصور والمحادثات.
٩. إدخال الوعي بالخصوصية والأمن الرقمي في المناهج التعليمية وبرامج تدريب الموظفين، ونشر إرشادات واضحة للمواطنين عن حماية الحساب والإبلاغ وحفظ الدليل.
١٠. تفعيل التعاون القضائي الدولي على أساس الاتفاقية العربية وغيرها من الأطر التي يرتبط بها العراق، مع إخضاع تبادل البيانات لمبادئ الضرورة والتناسب والرقابة القضائية.

المصادر والمراجع

١. دستور جمهورية العراق لسنة ٢٠٠٥.
٢. قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.
٣. قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ المعدل.
٤. قانون الاتصالات اللاسلكية رقم ١٥٩ لسنة ١٩٨٠.
٥. قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم ٧٨ لسنة ٢٠١٢. الوقائع العراقية، العدد ٤٢٥٦، ٥ تشرين الثاني ٢٠١٢.
٦. قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم ٣١ لسنة ٢٠١٣. الوقائع العراقية، العدد ٤٢٩٢، ٣٠ أيلول ٢٠١٣.
٧. قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كردستان-العراق رقم ٦ لسنة ٢٠٠٨.
٨. أمر سلطة الائتلاف المؤقتة رقم ٦٥ لسنة ٢٠٠٤ الخاص بهيئة الإعلام والاتصالات العراقية.
٩. الإعلان العالمي لحقوق الإنسان لسنة ١٩٤٨، المادة ١٢.
١٠. العهد الدولي الخاص بالحقوق المدنية والسياسية لسنة ١٩٦٦، المادة ١٧؛ وقانون تصديقه العراقي رقم ١٩٣ لسنة ١٩٧٠.
١١. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠.
١٢. الاتحاد الأوروبي. (٢٠١٦). اللائحة العامة لحماية البيانات رقم ٦٧٩/٢٠١٦، ولا سيما المواد ٥ و ٢٥ و ٣٢ و ٣٣ و ٣٤.
١٣. الجمعية العامة للأمم المتحدة. (٢٠٢٤). اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، القرار ٧٩/٢٤٣، ٢٤ كانون الأول ٢٠٢٤.

ثانياً: البحوث والدوريات

١. عباس، قصي علي. (٢٠٢٤). حجة الدليل الإلكتروني في الإثبات الجنائي. مجلة كلية القانون والعلوم السياسية، الجامعة العراقية، (٢٦)، ١١٥-١٣٩.
٢. جبار، محمد زيدون خلف، وفيصل، حيدر غازي. (٢٠٢٥). ذاتية الجرائم الرقمية والأمن السيبراني. مجلة آشور للعلوم القانونية والسياسية، ٢(٣)، ٩٩٠-٩٥٨.
٣. الربيعي، نورهان محمد. (٢٠٢٤). الجريمة السيبرانية وآليات مكافحتها: دراسة مقارنة. مجلة الفارابي للعلوم الإنسانية، ٣(١)، ٩٠-٧٣.
- الركابي، علي حسين علوان موحد، وشبيري زنجاني، سيد حسن. (٢٠٢٦). التحديات التكنولوجية الرئيسية في حماية البيانات الشخصية في القانون العراقي والإيراني والأوروبي. مجلة مركز بابل للدراسات الإنسانية، ١٦(٥)، ٣٠٩٦-٣٠٦١.
٥. عاشور، أميل جبار. (٢٠٢٠). المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في مواقع التواصل الاجتماعي: دراسة مقارنة. مجلة أبحاث ميسان، ١٦(٣١)، ١٣٤-١٠٩.
٦. محمد، ياسر عبد المنعم. (٢٠٢٥). الحماية الجزائية للخصوصية على شبكة الإنترنت. مجلة الجامعة العراقية، ٧٣(٦)، ٦٩-٦٢.
٧. خضير، غفران هادي، وحديد، حسن حماد. (٢٠٢٥). أساليب السياسة الجنائية الوقائية للحد من جنوح الأحداث في التشريع العراقي. مجلة دراسات البصرة، العدد ٦٠، ٢٥-٥٦.
٨. الحمداني، ميسون خلف. (٢٠٢٥). الدليل الرقمي وعلاقته بالمساحات بالحق في الخصوصية المعلوماتية أثناء إثبات الجريمة. مجلة جامعة الأنبار للعلوم القانونية والسياسية، ١٥(١)، جزء ٢، ٧٣٠-٧٧٣.
٩. راضي، إيناس جمعة. (٢٠٢٦). الأدلة الرقمية كوسيلة حديثة للإثبات وتأثيرها على تشكيل القناعات القضائية. مجلة مركز بابل للدراسات الإنسانية، ١٦(٦)، ١١٨٣-١٢١٦.
١٠. شيدائيان، مهدي، وعبد، شاكر محمود. (٢٠٢٦). الحق في الخصوصية في القانون الجنائي. مجلة مركز بابل للدراسات الإنسانية، ١٦(٢)، ٢٩٣-٣٢٢.
١١. محمد، اسن سعد نجم الدين. (٢٠٢٦). تحديات حماية الحقوق الرقمية في الدستور العراقي: نحو إطار دستوري لحماية الخصوصية وحرية التعبير في الفضاء الإلكتروني. مجلة القادسية للقانون والعلوم السياسية، ١٧(٢)، جزء ١، ٦٥-٧٨.

١٢. السري، عمر قصي عبدالله، والعتابي، آية عبد المحسن رحيم. (٢٠٢٦). الحماية القانونية لخصوصية المعلومات في عصر القرارات الخوارزمية. مجلة آشور للعلوم القانونية والسياسية، ٣(١)، ٥٧١-٦٠٣.
١٣. بن سالم، وداد، وشيباني، عبد الله. (٢٠٢٤). النظام القانوني لمقدمي خدمة الإنترنت في ظل القانون ٠٩-٠٤ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. مجلة الاجتهاد للدراسات القانونية والاقتصادية، ١٣(١)، ٥٩-٨١.
١٤. Andresen, M. A., & Jenion, G. W. (2008). Crime prevention and the science of where people are .Criminal Justice Policy Review, 19(2), 164-180
- ثالثاً: الوثائق والمواقع الرسمية
١. فريق الاستجابة للحوادث السيبرانية العراقي. (٢٠٢٢). استراتيجية الأمن السيبراني العراقي ٢٠٢٢-٢٠٢٥. <https://cert.gov.iq/pdf/1.pdf>
٢. مجلس النواب العراقي. (٢٠٢٦، ١ أيلول). لجنة الأمن والدفاع النيابية تناقش مقترح قانون مكافحة جرائم تقنية المعلومات. <https://iq.parliament.iq/blog/٥-مقت-٥>
٣. وزارة الداخلية العراقية. (٢٠٢٥، ١٩ شباط). وزارة الداخلية تستحدث مديرية مكافحة الجرائم الإلكترونية. <https://moi.gov.iq/?article=١٨٠٧٥>
٤. مفوضية الأمم المتحدة السامية لحقوق الإنسان. (٢٠٢٢). الحق في الخصوصية في العصر الرقمي. وثيقة مجلس حقوق الإنسان A/HRC/51/17.
٥. مجلس النواب العراقي. (٢٠٢٦، ٢١ أيلول). مجلس النواب يصوت على توصيات أزمة الوقود وينهي قراءة ثلاثة قوانين؛ وتأجيل قراءة تقرير ومناقشة مقترح قانون مكافحة جرائم تقنية المعلومات.