Arabian Gulf Journal of Humanities and Social Studies

ISSN: 3080-4086

الإصدار السابع - العدد العشرون || تاريخ الإصدار 2026-11-20

الحماية الجنائية للحياة الخاصة في ظل وسائل التواصل الاجتماعي (دراسة مقارنة)

Prohibition of crime Special video on social media (Drasa Maqarnan)

م.م. زهرة فخرالدين فهد

M.M. Zehra Fakhruldin Fahad

قسم الاعداد والتدريب – مديرية تربية كركوك

DOI: https://doi.org/10.64355/agjhss72069

مجلة خليج العرب للدراسات الإنسانية والاجتماعية || هذه المقالة مفتوحة المصدر موزعة بموجب شروط وأحكام ترخيص مؤسسة المشاع الإبداعي(CC BY-NC-SA)

الملخص:
أصبحت وسائل التواصل الاجتماعي بيئة مركزية لتكوين العلاقات وتبادل المعلومات وتوثيق الأحداث، لكنها في الوقت نفسه نقلت الاعتداء على الحياة الخاصة من نطاق محدود إلى فضاء واسع سريع الانتشار، عابر للحدود، قابل للنسخ وإعادة النشر، وصعب المحو الكامل، فلم يعد الاعتداء يقتصر على التجسس التقليدي أو إفشاء رسالة، بل أصبح يشمل التقاط الصور والفيديوهات دون رضا، نشر المحادثات والتسجيلات، تحديد الموقع الجغرافي، اختراق الحسابات، انتحال الشخصية، الابتزاز الإلكتروني، نشر البيانات الصحية والعائلية والمالية، وتداول المحتوى الجنسي الخاص.

يهدف البحث إلى بيان مدى كفاية الحماية الجنائية للحياة الخاصة في القانون العراقي، ومقارنتها بالنظامين المصري والفرنسي، مع الاستفادة من المعايير الدولية ذات الصلة، وينطلق من إشكالية أساسية مفادها أن الدستور العراقي أقر الحق في الخصوصية في المادة 17، وأن قانون العقوبات رقم 111 لسنة 1969 يتضمن صورًا متفرقة لحماية الأسرار والرسائل والحياة الخاصة، إلا أن البناء التشريعي العراقي لا يزال يفتقر إلى قانون نافذ شامل للجرائم المعلوماتية وحماية البيانات الشخصية، الأمر الذي يثير صعوبات في التكييف، والاختصاص، والإثبات، ومسؤولية المنصات الرقمية.

اعتمد البحث المنهج التحليلي للنصوص الدستورية والجزائية، والمنهج المقارن في دراسة القانون المصري والفرنسي، والمنهج النقدي لتقييم الفجوات واقتراح الإصلاح، وتوصل إلى أن القانون الفرنسي يقدم النموذج الأكثر تكاملًا بسبب الجمع بين الحماية المدنية في المادة 9 من القانون المدني، والتجريم التفصيلي في المواد 226-1 إلى 226-7 من قانون العقوبات، وحماية البيانات بموجب اللائحة العامة لحماية البيانات والقانون الفرنسي للمعلوماتية والحريات، أما القانون المصري فقد قطع خطوة مهمة من خلال الدستور وقانون العقوبات وقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 وقانون حماية البيانات الشخصية رقم 151 لسنة 2020، مع بقاء الحاجة إلى توضيح بعض التداخلات بين النصوص وتطوير التطبيق القضائي. ويظهر القانون العراقي حماية دستورية وجزائية مهمة، خصوصًا في المادة 438 من قانون العقوبات، إلا أن هذه الحماية تظل مجزأة وذات عقوبات محدودة ولا تستجيب بصورة كافية لخصوصية النشر الرقمي واسع النطاق.

ويقترح البحث إصدار قانون عراقي متكامل للجرائم المعلوماتية وحماية البيانات، يتضمن تعريفًا دقيقًا للحياة الخاصة والبيانات الشخصية، وتجريم نشر الصور والتسجيلات والمواقع الجغرافية والبيانات الحساسة دون رضا، ووضع ظروف مشددة للنشر عبر المنصات أو ضد الأطفال، وتنظيم جمع الأدلة الرقمية ومسؤولية الوسطاء وآليات الحذف العاجل، مع ضمان التوازن بين الخصوصية وحرية التعبير والصحافة والبحث العلمي.

الكلمات المفتاحية: الحياة الخاصة؛ الخصوصية الرقمية؛ وسائل التواصل الاجتماعي؛ الجرائم الإلكترونية؛ القانون العراقي؛ القانون المصري؛ القانون الفرنسي؛ البيانات الشخصية؛ الدليل الرقمي.

Abstract

Social media has transformed private-life violations into rapidly disseminated, cross-border, replicable and difficult-to-eradicate forms of harm. Contemporary violations include unauthorized recording and publication of images, disclosure of private messages, account intrusion, impersonation, cyber-extortion, geolocation tracking, publication of health and family data, and non-consensual sharing of intimate content. This article examines the criminal protection of privacy in Iraqi law and compares it with Egyptian and French law.

The study uses analytical, comparative and critical methods. It argues that Article 17 of the Iraqi Constitution recognizes personal privacy and that the Iraqi Penal Code No. 111 of 1969, particularly Article 438, criminalizes the public dissemination of news, images or comments concerning private or family secrets where publication is harmful. Nevertheless, Iraq lacks an enacted, comprehensive cybercrime and personal-data protection statute, which creates difficulties concerning legal characterization, digital evidence, jurisdiction, platform responsibility and urgent removal.

Egypt has developed a more explicit framework through the Constitution, Articles 309 bis and related provisions of the Penal Code, the Anti-Information Technology Crimes Law No. 175 of 2018, and the Personal Data Protection Law No. 151 of 2020. France offers the most integrated model through Article 9 of the Civil Code, Penal Code Articles 226-1 to 226-7, specific criminalization of non-consensual sexual-content dissemination, and the GDPR together with the French Data Protection Act. The article recommends that Iraq

adopt a comprehensive statute defining privacy and personal data, criminalizing digital publication of private images, recordings, location and sensitive data without consent, introducing aggravated penalties for mass dissemination and child victims, regulating digital evidence and intermediary duties, and preserving proportionality with freedom of expression and legitimate journalism.

Keywords: privacy; digital privacy; social media; cybercrime; Iraqi law; Egyptian law; French law; personal data; digital evidence.

المقدمة

لم تعد الحياة الخاصة مجالًا مغلقًا داخل المسكن أو الأسرة بالمعنى التقليدي، فقد أصبحت الشخصية الرقمية جزءًا من شخصية الإنسان القانونية والاجتماعية، وتتكون من الصور، والرسائل، وسجل البحث، والموقع الجغرافي، وقائمة الأصدقاء، والبيانات الصحية والمالية، والتفاعلات العامة والخاصة، ويترتب على ذلك أن الاعتداء على الخصوصية قد يقع من خلال فعل مادي مباشر، كالتقاط صورة أو تسجيل محادثة، أو من خلال معالجة آلية للبيانات، أو بواسطة إعادة نشر مادة حصل عليها الجاني من شخص آخر.

وتتميز الجريمة الواقعة عبر وسائل التواصل الاجتماعي بثلاثة عناصر تجعل الحماية التقليدية أقل كفاية. الأول هو الاتساع؛ فالنشر الذي كان يصل إلى عشرات الأشخاص قد يصل خلال دقائق إلى ملايين المستخدمين. والثاني هو الاستمرارية؛ إذ يمكن نسخ المادة وحفظها وإعادة توزيعها حتى بعد حذف المنشور الأصلي. والثالث هو التداخل بين أدوار الفاعلين؛ فالمعتدي قد يكون صاحب حساب، أو مدير مجموعة، أو مستخدمًا أعاد النشر، أو مزود خدمة، أو منصة تملك أدوات فنية للتحكم في الوصول والانتشار.

وتتصل حماية الحياة الخاصة بحقوق دستورية أخرى، منها الكرامة الإنسانية، وحرمة المسكن، وسرية المراسلات، وحرية التعبير، وحرية الصحافة، وحق الجمهور في المعرفة. لذلك لا يكفي أن يقرر المشرع التجريم بصورة مطلقة؛ بل يجب أن يرسم حدودًا واضحة بين النشر المجرم والنشر المشروع، وبين المعلومة الخاصة والمعلومة ذات الشأن العام، وبين النقد السياسي والسب أو التشهير، وبين التوثيق الصحفي المشروع والتشهير الرقمي[1].

أولًا: مشكلة البحث

تتمثل المشكلة في مدى قدرة قواعد التجريم التقليدية في العراق على حماية الحياة الخاصة من الاعتداءات التي تقع بواسطة وسائل التواصل الاجتماعي، ومدى اختلاف ذلك عن الحماية التي قررها المشرع المصري والفرنسي. وتنبثق عنها أسئلة فرعية:

1. ما المقصود بالحياة الخاصة والخصوصية الرقمية؟
2. ما الأساس الدستوري والجزائي لحماية الحياة الخاصة في العراق؟
3. هل تكفي المادة 438 من قانون العقوبات العراقي لمواجهة نشر الصور والتسجيلات والمحادثات عبر المنصات؟
4. ما الإضافة التي قدمها القانون المصري رقم 175 لسنة 2018 وقانون حماية البيانات رقم 151 لسنة 2020؟
5. كيف جمع القانون الفرنسي بين التجريم وحماية البيانات والجزاءات المدنية؟
6. ما حدود المسؤولية الجنائية للمستخدمين والمنصات ومديري الصفحات؟
7. كيف يمكن تحقيق التوازن بين حماية الخصوصية وحرية التعبير والصحافة؟

(1) للمزيد: United Nations, International Covenant on Civil and Political Rights, United Nations Treaty Series, vol. 999, 1966, Article 17, pp. 173؛ Council of Europe, European Convention on Human Rights, 1950, Article 8, pp. 11.

ثانيًا: أهمية البحث

تنبع أهمية البحث من أن حماية الخصوصية الرقمية أصبحت مسألة حقوقية وجنائية وإجرائية في الوقت نفسه. فمن الناحية الحقوقية، يؤدي النشر غير المشروع إلى الإهانة والوصم والابتزاز والعنف الأسري والمهني. ومن الناحية الجنائية، يتطلب الأمر تكييفًا دقيقًا للفعل بين إفشاء السر والقذف والتهديد والابتزاز والاختراق ومعالجة البيانات دون ترخيص. ومن الناحية الإجرائية، يثير الدليل الرقمي مسائل مصدره وسلامته وسلسلة حيازته واختصاص المحكمة. ومن الناحية التشريعية، تكشف المقارنة أن الحماية الفعالة لا تقوم على مادة عقابية منفردة، بل على منظومة تتكامل فيها القواعد الدستورية والمدنية والجنائية وقواعد البيانات والاتصالات والإثبات.

ثالثًا: أهداف البحث

يهدف البحث إلى تحليل المفهوم الجنائي للحياة الخاصة، وبيان النصوص العراقية النافذة ذات الصلة، وتقويم مدى انطباقها على وسائل التواصل الاجتماعي، ومقارنة ذلك بالنظامين المصري والفرنسي، ورصد أوجه القوة والقصور، واقتراح نموذج تشريعي عراقي يوازن بين الخصوصية والحقوق المتعارضة.

رابعًا: منهج البحث ونطاقه

اعتمد البحث المنهج التحليلي من خلال قراءة النصوص الدستورية والجزائية والتنظيمية، والمنهج المقارن من خلال المقارنة بين العراق ومصر وفرنسا، والمنهج النقدي عند تقييم ملاءمة النصوص للبيئة الرقمية. ويقتصر البحث على الحماية الجنائية الأساسية المرتبطة بوسائل التواصل الاجتماعي، مع الاستفادة من الحماية المدنية وحماية البيانات بالقدر اللازم لفهم النظام ككل. ويُقصد بالقانون الفرنسي النصوص النافذة حتى عام 2026، بما في ذلك التعديلات الحديثة على المادة 226-1 من قانون العقوبات.

خامسًا: خطة البحث

يقسم البحث إلى أربعة مباحث: يتناول الأول الإطار المفاهيمي والدستوري والدولي، ويتناول الثاني الحماية الجنائية في القانون العراقي، ويتناول الثالث الحماية في القانون المصري، ويتناول الرابع الحماية في القانون الفرنسي والمقارنة النقدية والتوصيات التشريعية.

المبحث الأول: الإطار المفاهيمي والدستوري والدولي

المطلب الأول: مفهوم الحياة الخاصة والخصوصية الرقمية

الفرع الأول: مفهوم الحياة الخاصة

يصعب وضع تعريف جامد للحياة الخاصة؛ لأنها تتغير بتغير الثقافة والتكنولوجيا وطبيعة الشخص والظروف المحيطة بالفعل. ومع ذلك، يمكن تعريفها بأنها المجال الذي يملك الفرد أن يقرر فيه، بصورة مستقلة، من يطلع على تفاصيله الشخصية والعائلية والجسدية والعاطفية والمالية والمكانية، وكيف تستخدم المعلومات المتعلقة به ولا تعني الخصوصية أن كل ما يفعله الشخص يجب أن يبقى سريًا على نحو مطلق، بل تعني وجود مصلحة مشروعة في التحكم في الوصول إلى المعلومات وفي منع التدخل غير المبرر.[2].

وتتكون الحياة الخاصة من دوائر متداخلة. الدائرة الأولى هي الخصوصية المكانية، وتشمل المسكن والمكان الخاص وغرفة الفندق والمركبة في بعض الحالات والمكان الذي يتوقع الشخص فيه عدم المراقبة. الدائرة الثانية هي الخصوصية الاتصالية، وتشمل الرسائل والمكالمات والمحادثات الخاصة والبريد الإلكتروني والرسائل المباشرة. الدائرة الثالثة هي الخصوصية الجسدية، وتشمل صورة الجسد والحالة الصحية والمعلومات الطبية والمحتوى الحميمي. الدائرة الرابعة هي الخصوصية العائلية والاجتماعية، وتشمل العلاقات والوقائع العائلية والظروف الشخصية. والدائرة الخامسة هي الخصوصية المعلوماتية، وتشمل البيانات التي تسمح بتحديد الشخص أو تتبع عاداته وموقعه وتفضيلاته.

(2) سولوف، دانيال ج.، فهم الخصوصية، Harvard University Press ، كامبردج، 2008، ص 1–31؛ نيسنبوم، هيلين، الخصوصية في السياق، Stanford University Press، 2010 ، ص.28.

وقد اتجه الفقه الحديث إلى اعتبار الخصوصية المعلوماتية حقًا في التحكم في البيانات، لا مجرد حق في السرية. فالبيانات قد تكون معروفة لبعض الأشخاص، لكنها تظل محمية من إعادة استخدامها لغرض مختلف أو نشرها على نطاق أوسع. ومن هنا يختلف نشر صورة على حساب خاص محدود عن إعادة نشرها على صفحة عامة، حتى لو كان الناشر الثاني قد حصل عليها من مصدر متاح له.[3]

الفرع الثاني: خصوصية وسائل التواصل الاجتماعي

تتسم وسائل التواصل الاجتماعي بتداخل المجالين العام والخاص. فالحساب قد يكون عامًا، لكن المنشور قد يكون موجهًا إلى دائرة محددة. وقد يضع المستخدم صورة بمحض إرادته، لكنه لا يفترض بالضرورة أن يحق للغير نسخها أو تعديلها أو استخدامها في إعلان أو نشرها مع تعليق مهين. كما أن قبول طلب صداقة لا يعني التنازل عن كل عناصر الخصوصية، ولا يعني أن المتلقي يملك الحق في تصوير المحادثة وإرسالها إلى الجمهور.

ويُعد الرضا في البيئة الرقمية عنصرًا معقدًا. فالرضا يجب أن يكون محددًا ومستنيرًا وحقيقيًا، ولا يجوز افتراضه من مجرد وجود الشخص في مكان عام إذا كان الفعل يتعلق بواقعة خاصة أو محتوى حميمي. كما أن الموافقة على التقاط الصورة لا تعني بالضرورة الموافقة على نشرها، والموافقة على إرسال محتوى إلى شخص واحد لا تعني الموافقة على تداوله في مجموعة أو منصة عامة.[4]

الفرع الثالث: أشكال الاعتداء الرقمي

من أهم صور الاعتداء على الحياة الخاصة في وسائل التواصل الاجتماعي:

1. التقاط أو تسجيل الكلام أو الصورة في مكان خاص دون رضا.
2. نشر صورة أو فيديو خاص ولو كان صحيحًا إذا أدى النشر إلى الإضرار بالشخص.
3. إفشاء الرسائل والمحادثات الخاصة أو تسجيل المكالمات.
4. نشر بيانات الصحة أو العنوان أو رقم الهاتف أو مكان العمل أو المعلومات المالية.
5. تتبع الموقع الجغرافي أو كشفه دون رضا.
6. اختراق الحساب أو الحصول على كلمة المرور أو الدخول إلى الرسائل.
7. إنشاء حساب باسم الغير أو استعمال صورته وانتحال صفته.
8. نشر محتوى حميمي أو جنسي دون موافقة، ولو كان قد أُنشئ أو أُرسل أصلًا برضا.
9. الابتزاز والتهديد بإفشاء صورة أو محادثة.
10. إعادة النشر أو الإعجاب أو الترويج لمحتوى غير مشروع بما يساهم في توسيع الضرر.

ولا يلزم أن يجتمع أكثر من وصف في الواقعة الواحدة. فقد يكون نشر صورة خاصة اعتداءً على الحياة الخاصة وقذفًا إذا تضمنت تعليقًا ماسًا بالشرف، وقد يكون تهديدًا أو ابتزازًا إذا اقترن بطلب مال أو منفعة، وقد يكون جريمة بيانات إذا جرى جمعها أو معالجتها بلا سند.

---

(3) ويستن، آلان ف.، الخصوصية والحرية،Atheneum ، نيويورك، 1967، ص 7؛ نيسنبوم، هيلين، الخصوصية في السياق، Stanford University Press،2010 ، ص 129

(4) European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Publications Office of the European Union, Luxembourg, 2018, pp. 43.

المطلب الثاني: الأساس الدستوري والدولي

الفرع الأول: الدستور العراقي

نصت المادة 17 أولًا من الدستور العراقي لسنة 2005 على أن «لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والآداب العامة». كما قررت المادة نفسها حرمة المساكن وسرية الاتصالات والمراسلات والبرقيات والهاتفية والإلكترونية، ولا يجوز مراقبتها أو التنصت عليها أو الكشف عنها إلا بقرار قضائي ولضرورة قانونية وأمنية.[5]

ويمثل النص العراقي أساسًا دستوريًا مباشرًا لحماية الخصوصية الرقمية؛ لأنه لم يقصر الاتصالات على شكل تقليدي، بل أشار إلى الاتصالات الإلكترونية. كما يربط النص الحماية بحقوق الآخرين والآداب العامة، وهو قيد ينبغي تفسيره تفسيرًا ضيقًا حتى لا يتحول إلى سبب عام لتقييد الخصوصية أو حرية التعبير. ويجب أن يكون أي تدخل قائمًا على قانون واضح، وأن يكون ضروريًا ومتناسبًا وخاضعًا لرقابة القضاء.

وتكمن أهمية المادة 17 في أنها تسمح بتفسير النصوص الجزائية القائمة تفسيرًا مواكبًا للتكنولوجيا، لكنها لا تعوض عن غياب قانون تفصيلي للبيانات والمنصات. فالنص الدستوري يقرر الحق، بينما يحتاج التجريم إلى تحديد الفعل والعنصر المعنوي والعقوبة وقواعد الاختصاص والإثبات.

الفرع الثاني: الدستور المصري

أكد الدستور المصري لسنة 2014، في المادة 57، أن للحياة الخاصة حرمة، وأنها مصونة لا تمس، وأن للمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسرية، ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة وفي الأحوال التي يبينها القانون. كما ألزم الدولة بحماية حقوق المواطنين في استعمال وسائل الاتصال العامة، ولا يجوز تعطيلها أو قطعها تعسفًا.[6]

ويتسم النص المصري بوضوح أكبر في تعداد المراسلات الإلكترونية واشتراط الأمر القضائي المسبب والمدة المحددة. كما أن صياغته تربط الخصوصية بحماية وسائل الاتصال، وهي حماية لا تقتصر على محتوى الرسالة بل تمتد إلى بيانات الاتصال والإجراءات التي تسمح بالوصول إليها.

الفرع الثالث: الأساس الفرنسي والدولي

يحمي القانون الفرنسي الحياة الخاصة مدنيًا في المادة 9 من القانون المدني، التي تقرر أن لكل شخص الحق في احترام حياته الخاصة، وتمنح القاضي سلطة اتخاذ تدابير لمنع الاعتداء أو وقفه، ومنها الحجز والمصادرة والأوامر الوقتية. أما الحماية الجنائية فتتركز في المواد 226-1 إلى 226-7 من قانون العقوبات.

وعلى المستوى الدولي، تنص المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية على عدم جواز التدخل التعسفي أو غير القانوني في خصوصية الشخص أو أسرته أو مسكنه أو مراسلاته، وعدم جواز الاعتداء غير المشروع على شرفه وسمعته، مع حقه في حماية القانون. كما تقرر المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان حق كل شخص في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته، ولا يجوز تدخل السلطة العامة إلا إذا كان منصوصًا عليه في القانون وضروريًا في مجتمع ديمقراطي لحماية مصالح مشروعة.[7][8]

وتؤسس هذه النصوص لمبدأين: أولهما أن الخصوصية حق مستقل وليس مجرد مصلحة ثانوية، وثانيهما أن تقييد الخصوصية أو تقييد حرية التعبير يجب أن يخضع لمعيار الشرعية والضرورة والتناسب. ولهذا يجب ألا تستخدم الحماية الجنائية لحماية الأسرار الحقيقية فحسب، بل لحماية الكرامة والاستقلال الشخصي، مع عدم تحويلها إلى وسيلة لمنع النقد المشروع أو كشف الفساد.

المبحث الثاني: الحماية الجنائية للحياة الخاصة في القانون العراقي

---

(5) جمهورية العراق، دستور جمهورية العراق لسنة 2005، المادة 17/أولًا وثانيًا وثالثًا، النسخة الرسمية المنشورة من وزارة الخارجية العراقية، 2005، ص 5–6 في النسخة الإلكترونية.

(6) جمهورية مصر العربية، دستور جمهورية مصر العربية لسنة 2014 المعدل، المادة 57، الهيئة العامة للاستعلامات، 2014، ص 20 تقريبًا بحسب النسخة الإلكترونية.

(7) Human Rights Committee, General Comment No. 16: Article 17, United Nations, 1988, paras. 10.

(8) United Nations, International Covenant on Civil and Political Rights, 1966, Article 17.

المطلب الأول: الحماية في قانون العقوبات العراقي

الفرع الأول: جريمة إفشاء الأسرار الوظيفية والاتصالات

يتضمن قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل نصوصًا متعددة لحماية السرية. فتجرم المادة 327 إفشاء الموظف أو المكلف بخدمة عامة أمرًا وصل إلى علمه بحكم وظيفته إذا كان يعلم بوجوب عدم إفشائه وكان من شأن الإفشاء الإضرار بمصلحة الدولة. وتجرم المادة 328 الأفعال التي تقع من الموظفين أو العاملين في دوائر البريد والبرق والهاتف من فتح أو إخفاء أو إتلاف رسالة أو برقية أو إفشاء سر تضمنته، كما تمتد إلى إفشاء المكالمة الهاتفية.(9)

وتتصل هذه النصوص بالحياة الخاصة من زاويتين. الأولى حماية السرية من جانب الموظف أو العامل الذي يملك بحكم وظيفته إمكانية الوصول إلى المراسلات. والثانية أنها تعكس اتجاهًا تشريعيًا قديمًا يربط الاعتداء بوسيلة الاتصال التقليدية وبصفة الفاعل. أما وسائل التواصل الاجتماعي، فلا يكون الفاعل فيها غالبًا موظفًا في مرفق البريد أو الهاتف، بل مستخدمًا عاديًا حصل على المعلومات من حساب أو محادثة. لذلك لا تكفي المادة 328 وحدها لمعالجة الإفشاء الرقمي.

الفرع الثاني: المادة 438 وحماية أسرار الحياة الخاصة والعائلية

تعد المادة 438 من أهم النصوص العراقية في الموضوع؛ إذ تعاقب بالحبس مدة لا تزيد على سنة وبغرامة أو بإحدى هاتين العقوبتين من نشر بإحدى طرق العلانية أخبارًا أو صورًا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، إذا كان من شأن نشرها الإساءة إليهم. كما تعاقب من اطلع من غير الفئات المشار إليها في المادة 328 على رسالة أو برقية أو مكالمة هاتفية فأفشاها لغير من وجهت إليه إذا كان من شأن ذلك إلحاق الضرر بأحد.(10)

ويكشف النص عن عناصر مهمة. أولًا، أن المشرع لا يشترط كذب الخبر؛ فحتى الخبر الصحيح قد يكون محل حماية إذا كان من أسرار الحياة الخاصة وكان من شأن نشره الإساءة. ثانيًا، أنه يشمل الأخبار والصور والتعليقات، وهي ألفاظ قابلة لاستيعاب الصور الرقمية والفيديو والتعليق المنشور على منصة. ثالثًا، أنه يشترط العلانية في الفقرة المتعلقة بالنشر، وهو ما يتحقق عادة في الصفحة العامة أو المجموعة المفتوحة، وقد يتحقق في مجموعة مغلقة إذا كان عدد الجمهور وطبيعة التداول يحققان معنى العلانية وفقًا لتفسير القضاء. رابعًا، أن النص يشترط قابلية الإساءة، مما يفرض على المحكمة بحث محتوى المنشور وسياقه وآثاره.

ومع ذلك، يثير النص صعوبات. فعبارة «بإحدى طرق العلانية» صيغت في زمن سابق على المنصات، وقد تحتاج إلى تفسير قضائي أو تعديل تشريعي صريح لإدراج الحسابات والمنصات وإعادة النشر. كما أن العقوبة تبدو محدودة بالنظر إلى قابلية الضرر الرقمي للتوسع والاستمرار. ولا يتضمن النص تنظيمًا خاصًا لإزالة المحتوى أو وقف التداول أو مصادرة الأجهزة أو حفظ الدليل الرقمي، كما لا يعالج نشر الموقع الجغرافي أو معالجة قواعد البيانات أو المسؤولية عن الخوارزميات.(11)

الفرع الثالث: القذف والسب والتهديد والابتزاز

قد تحمي المواد الخاصة بالقذف والسب والتهديد جانبًا من الحياة الخاصة بصورة غير مباشرة. فالمادة 433 تعرف القذف بأنه إسناد واقعة معينة إلى الغير بإحدى طرق العلانية من شأنها لو صحت أن توجب عقاب من أسندت إليه أو احتقاره عند أهل وطنه، وتعد العلانية عبر وسائل الإعلام ظرفًا مشددًا في بعض الصور. وتجرم المواد 434 وما بعدها السب والإهانة. كما تجرم مواد التهديد أفعال التهديد بإسناد أمور مخدشة بالشرف أو الإفشاء بها.

وتبرز أهمية هذه النصوص في حالات نشر صورة خاصة مع وصف مهين، أو نشر محادثة بقصد إسقاط السمعة، أو تهديد شخص بإفشاء محتوى حميمي. لكن القذف والسب يحميان الشرف والاعتبار، بينما تحمي المادة 438 المجال الخاص ذاته ولو كان المحتوى صحيحًا. ومن ثم يجب عدم اختزال الاعتداء على الخصوصية في القذف؛ لأن بعض الأفعال تكون مجرمة حتى مع انتفاء الكذب أو الإساءة اللفظية، كإعادة نشر صورة عائلية خاصة دون رضا.

---

(9) جمهورية العراق، قانون العقوبات رقم 111 لسنة 1969 المعدل، المواد 327–328، الجريدة الرسمية، بغداد، 1969؛ الإحالة إلى رقم المادة لأن الصفحات تختلف بين الطبعات.

(10) جمهورية العراق، قانون العقوبات رقم 111 لسنة 1969 المعدل، المادة 438؛ مجلس القضاء الأعلى العراقي، كاظم عبد جاسم الزيدي، «جريمة انتهاك حرمة الحياة الخاصة»، مقال منشور في موقع مجلس القضاء الأعلى، 17/5/2018، دون صفحات ثابتة.

(11) محمد أحمد المعداوي مجاهد عبد ربه، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دار النهضة العربية، القاهرة، 2018، ص 241

الفرع الرابع: الدخول غير المشروع والاختراق

لا يملك القانون العراقي النافذ، في بنيته العامة، نصًا واحدًا شاملًا يحمل عنوان الدخول غير المشروع إلى الحسابات ومنصات التواصل. وقد تلجأ جهات التحقيق إلى تكييف الفعل وفق نصوص الدخول إلى الأماكن أو السرقة أو التهديد أو الابتزاز أو الإضرار العمدي بحسب طريقة ارتكابه ونتيجته. وهذا التشتت يخلق خطر التوسع في القياس، بينما الأصل في التجريم أن يكون محددًا ولا يجوز التوسع فيه على حساب مبدأ الشرعية.

وقد عالجت مشروعات قوانين الجرائم المعلوماتية العراقية صورًا متعددة من الدخول غير المشروع والاعتداء على البيانات، إلا أن المشروع لا يساوي قانونًا نافذًا ولا يجوز الاستناد إليه لتجريم فعل أو تشديد عقوبة. وهذه نقطة منهجية أساسية: لا يجوز للباحث أو القاضي أن يعامل مشروع قانون الجرائم الإلكترونية بوصفه مصدرًا للقواعد النافذة. ويمكن الاستفادة منه في النقد التشريعي فقط.[12]

المطلب الثاني: أركان الاعتداء على الحياة الخاصة عبر التواصل الاجتماعي

الفرع الأول: الركن الشرعي

يتطلب الركن الشرعي وجود نص نافذ يحدد الفعل والعقوبة. وفي العراق يمكن أن يستند تجريم نشر الأخبار والصور والتعليقات الخاصة إلى المادة 438، والقذف والسب إلى المواد الخاصة بهما، والتهديد أو الابتزاز إلى النصوص ذات الصلة بحسب الواقعة. أما مجرد جمع البيانات أو تتبع الموقع أو إنشاء قاعدة معلومات خاصة دون نشر، فلا يكفي فيه القياس على المادة 438 ما لم تتحقق عناصر نص آخر.

الفرع الثاني: الركن المادي

يتكون الركن المادي من سلوك وموضوع ونتيجة أو خطر بحسب طبيعة النص. السلوك قد يكون التقاطًا أو تسجيلًا أو حفظًا أو نقلًا أو نشرًا أو إعادة نشر أو إفشاءً أو استخدامًا. والموضوع هو الخبر أو الصورة أو التعليق أو الرسالة أو المكالمة أو البيانات الخاصة. أما النتيجة في المادة 438 فتتمثل في كون النشر من شأنه الإساءة إلى المجني عليه، أو في إفشاء الرسالة أو المكالمة بما يلحق الضرر.

ولا يشترط أن يكون الجاني هو من أنشأ المحتوى. فإعادة نشر مادة خاصة قد تنشئ فعلًا جديدًا إذا كان الناشر يعلم طبيعتها الخاصة وقصد توسيع انتشارها. لكن يجب التفريق بين إعادة النشر المقصودة وبين مشاركة تلقائية أو إعادة إرسال دون علم بالمحتوى، مع مراعاة القصد والظروف.

الفرع الثالث: الركن المعنوي

الأصل أن الجرائم الماسة بالحياة الخاصة جرائم عمدية، وتتطلب العلم بأن الموضوع يتعلق بالحياة الخاصة أو السرية، واتجاه الإرادة إلى التسجيل أو النشر أو الإفشاء. وفي المادة 438 لا يلزم قصد خاص للإضرار بالضرورة إذا كانت صياغة النص تكتفي بأن يكون النشر من شأنه الإساءة، لكن العلم بطبيعة الفعل وتوقع أثره يظل لازمًا.

ويتعين على المحكمة استخلاص العلم من ظروف الحساب، وطريقة الحصول على المادة، والرسائل المصاحبة، والتحذيرات، وإصرار الجاني على إعادة النشر بعد طلب الحذف. ولا يكفي افتراض القصد من مجرد وجود المنشور إذا كان الحساب مخترقًا أو كان المتهم قد فقد السيطرة عليه، وهو ما يجعل نسبة الفعل الرقمي مسألة فنية وقانونية.

المطلب الثالث: الدليل الرقمي والاختصاص في العراق

الفرع الأول: قيمة الدليل الرقمي

تشمل الأدلة الرقمية لقطات الشاشة، وسجلات المنصة، وعناوين بروتوكول الإنترنت، وبيانات الهاتف، والرسائل المستخرجة، والتسجيلات، وبيانات النسخ الاحتياطي. ولا تكفي لقطة الشاشة وحدها دائمًا لإثبات المصدر والزمن وهوية المستخدم؛ فقد تكون قابلة للتعديل أو مأخوذة من حساب منتحل. لذلك ينبغي دعمها بمحضر ضبط إلكتروني، أو تقرير خبرة، أو طلب رسمي إلى المنصة، أو بيانات الهاتف ومزود الخدمة، مع توثيق سلسلة الحيازة.

(12) يُحذر من مساواة مشروع قانون الجرائم المعلوماتية العراقي بقانون نافذ؛ المرجع التشريعي النافذ في هذه النقطة هو قانون العقوبات رقم 111 لسنة 1969، ولا يُستند إلى المشروع إلا في النقد والاقتراح.

وتتطلب سلامة الدليل الحفاظ على النسخة الأصلية، وتسجيل وقت الاستخراج، وبيان الجهاز والبرنامج المستخدم، وحساب البصمة الرقمية عند الإمكان، ومنع التغيير اللاحق. كما يجب أن يكون الحصول على الدليل مشروعًا، لأن انتهاك خصوصية شخص آخر أثناء جمع الدليل قد يخلق نزاعًا حول مشروعيته.

الفرع الثاني: الاختصاص العابر للحدود

قد يكون الضحية في العراق، والجاني في دولة أخرى، والخادم في دولة ثالثة، والمنصة شركة عالمية. ويثور الاختصاص الإقليمي إذا وقع جزء من السلوك أو تحقق جزء من النتيجة في العراق. غير أن التحقيق يحتاج إلى تعاون دولي سريع للحصول على بيانات الحساب أو عنوان الاتصال أو سجل الدخول، وهو ما يتطلب اتفاقيات وإجراءات واضحة.

كما أن حذف المحتوى قد يكون أسرع من الحصول على أمر قضائي أو مخاطبة منصة أجنبية. ولذلك يحتاج العراق إلى آلية عاجلة تحفظ الدليل وتمنع الانتشار مؤقتًا، مع ضمان مراجعة قضائية وعدم تحويل طلبات الحذف إلى رقابة غير محدودة على التعبير.

المبحث الثالث: الحماية الجنائية في القانون المصري

المطلب الأول: الحماية الدستورية وقانون العقوبات

يمنح الدستور المصري حماية صريحة للحياة الخاصة والاتصالات الإلكترونية. ويكمل قانون العقوبات هذه الحماية في المواد 309 مكرر و309 مكرر (أ) وما يرتبط بها، حيث يجرم الاعتداء على حرمة الحياة الخاصة من خلال استراق السمع أو تسجيل أو نقل محادثات جرت في مكان خاص أو عن طريق الهاتف بغير رضا أو في غير الأحوال المصرح بها قانونًا، ويجرم إذاعة أو استعمال التسجيل أو المستند المتحصل عليه من هذه الجريمة.

وتكمن أهمية النص المصري في أنه يعالج مرحلتين: مرحلة الحصول على التسجيل أو المحادثة، ومرحلة إذاعته أو استعماله. وهذا ينسجم مع واقع التواصل الاجتماعي؛ فقد يحصل الجاني على مادة خاصة بطريقة غير مشروعة ثم ينشرها، وقد يحصل عليها برضا ثم ينشرها دون رضا. ويجب أن تفرق المحكمة بين المصدر غير المشروع للمادة وبين فعل النشر المستقل.

ويحمي قانون العقوبات أيضًا الشرف والاعتبار من خلال جرائم القذف والسب، وهو ما يتيح تكييفًا مزدوجًا عند نشر معلومات خاصة مصحوبة بعبارات مهينة. إلا أن حماية الخصوصية تتجاوز حماية السمعة؛ فالنشر قد يكون غير مشروع حتى لو لم يتضمن سبًا أو قذفًا.

المطلب الثاني: قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018

أدخل القانون المصري رقم 175 لسنة 2018 بنية أكثر تخصصًا للجرائم المرتكبة بواسطة تقنية المعلومات. ومن أهم أحكامه المادة 25 التي تجرم الاعتداء على أي من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهاك حرمة الحياة الخاصة، أو إرسال العديد من الرسائل الإلكترونية لشخص دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته. كما تتصل المادة 26 باستعمال تقنية المعلومات في معالجة معطيات شخصية للغير بما يربطها بمحتوى منافٍ للآداب أو إظهارها بطريقة تمس اعتباره أو شرفه.[13]

ويتميز هذا القانون بأنه يعترف بوسائل تقنية المعلومات بوصفها وسيلة ارتكاب مستقلة، ولا يترك كل فعل لتكييف النصوص التقليدية. كما يتضمن قواعد تتعلق بمسؤولية مديري المواقع والحسابات، وأوامر الحجب والإجراءات، وحجية الأدلة الرقمية وفق المنظومة الإجرائية ذات الصلة.

لكن بعض ألفاظ القانون، مثل «المبادئ أو القيم الأسرية»، قد تثير إشكالًا من حيث مبدأ الشرعية إذا استعملت بصورة واسعة وغير منضبطة. فالتجريم المرتبط بالخصوصية ينبغي أن يرتبط بعناصر قابلة للتحديد، مثل جمع البيانات دون سند أو نشر صورة خاصة دون رضا أو إفشاء مراسلات خاصة، لا بتقديرات أخلاقية عامة تسمح بتفاوت كبير في التطبيق.

كما ينبغي قراءة المادة 25 مع الدستور وقانون حماية البيانات وقواعد حرية الصحافة، حتى لا يتحول النص إلى وسيلة لمعاقبة التعبير المشروع أو النقد العام. فالمعيار يجب أن يركز على طبيعة البيانات وغياب الرضا والضرر أو الخطر غير المشروع، لا على مجرد كون المحتوى مخالفًا لتقييم اجتماعي عام.

(13) WIPO Lex، قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، مصر، نص صادر في 14 أغسطس 2018 ونافذ في 15 أغسطس 2018، الإحالة إلى رقم المادة في النص المنشور.

المطلب الثالث: قانون حماية البيانات الشخصية رقم 151 لسنة 2020

يمثل قانون حماية البيانات الشخصية المصري نقلة من التجريم اللاحق إلى الوقاية والتنظيم السابق. فهو ينظم جمع البيانات ومعالجتها وتخزينها ونقلها، ويقرر التزامات على المتحكم والمعالج، ويمنح الشخص حقوقًا تتعلق بالوصول والتصحيح والمحو والاعتراض، ويضع إطارًا للترخيص والرقابة.(14)

وتزداد أهمية القانون مع وسائل التواصل الاجتماعي لأن المنصة لا تكتفي بعرض المحتوى الذي ينشره المستخدم، بل تجمع بيانات الاستخدام والتفضيلات والموقع والاتصالات وتستخدمها في التخصيص والإعلانات والتحليل. ومن ثم فإن حماية الحياة الخاصة لا تقتصر على منع المستخدم من نشر صورة الغير، بل تشمل منع المعالجة غير المشروعة للبيانات بواسطة الجهات التي تملك القدرة التقنية.

ويجب التمييز بين البيانات التي ينشرها الشخص علنًا والبيانات التي يجوز معالجتها. فإتاحة البيانات للجمهور قد تكون عنصرًا في تقييم التوقع المشروع للخصوصية، لكنها لا تعني إباحة استخدامها لأي غرض أو دمجها مع بيانات أخرى أو بيعها أو استخدامها للتصنيف والمراقبة. ويقتضي ذلك تطبيق مبادئ الغرض المحدد، وتقليل البيانات، والشفافية، والأمن، والمساءلة.

المطلب الرابع: تقييم التجربة المصرية

تظهر قوة التجربة المصرية في تعدد مستويات الحماية: نص دستوري واضح، وقواعد تقليدية في قانون العقوبات، وقانون متخصص للجرائم المعلوماتية، وقانون للبيانات الشخصية. كما أن وجود نصوص تتناول التسجيل والإذاعة ومعالجة البيانات يوفر خيارات تكييف متعددة.

لكن التعدد قد يؤدي إلى تداخل. فقد تنطبق المادة 309 مكرر وقانون تقنية المعلومات وقانون البيانات على واقعة واحدة. وتحتاج النيابة والمحكمة إلى تحديد النص الأخص، ومنع ازدواج العقاب عن الفعل ذاته، ومراعاة استقلال الأفعال إذا تعددت مراحل السلوك. كما أن حماية البيانات لا ينبغي أن تضعف حماية الصحافة والتحقيقات والبحث العلمي، ويجب أن تظل الاستثناءات محددة وضرورية ومتناسبة.

المبحث الرابع: الحماية في القانون الفرنسي والمقارنة النقدية

المطلب الأول: المادة 9 من القانون المدني

تقرر المادة 9 من القانون المدني الفرنسي أن لكل شخص الحق في احترام حياته الخاصة، وتمنح القاضي سلطة اتخاذ إجراءات الحجز والمصادرة وغيرها لمنع الاعتداء أو وقفه، حتى على سبيل الاستعجال. وتُعد هذه المادة أساسًا مهمًا لحماية الصور والبيانات الشخصية، وهي تتيح تدابير سريعة قبل الفصل النهائي في التعويض.(15)

وتفيد هذه الحماية في وسائل التواصل الاجتماعي لأن الضرر يتضاعف مع الزمن. فالتعويض المالي اللاحق قد لا يكفي إذا ظل الفيديو متاحًا أو انتشر على حسابات متعددة. لذلك تتكامل الحماية المدنية العاجلة مع الحماية الجنائية، وتستطيع المحكمة أن تأمر بالحذف أو المنع أو حجز الوسيط وفق شروط التناسب.

المطلب الثاني: المواد 226-1 و226-2 و226-2-1 من قانون العقوبات

تعاقب المادة 226-1 بالحبس سنة وغرامة 45,000 يورو كل من تعمد، بأية وسيلة، الاعتداء على حميمية الحياة الخاصة للغير من خلال التقاط أو تسجيل أو نقل أقوال خاصة أو سرية دون رضا، أو تثبيت أو تسجيل أو نقل صورة شخص موجود في مكان خاص دون رضاه، كما تشمل التقاط أو تسجيل أو نقل الموقع الجغرافي لشخص دون رضاه. وتُفترض الموافقة في بعض الحالات إذا تم الفعل علنًا وبعلم الشخص دون اعتراض، وكان قادرًا على الاعتراض، مع أحكام خاصة بالقاصر وتشديد للعقوبة إذا كان الفاعل زوجًا أو شريكًا أو كانت الضحية من فئات معينة.(16)

(14) جمهورية مصر العربية، قانون حماية البيانات الشخصية رقم 151 لسنة 2020، المواد 1–5 و13–17 و36–48، الجريدة الرسمية، 2020، ص 1–25 بحسب نسخة الجريدة.

(15) République française, Code civil, article 9, Légifrance, version en vigueur en 2026، النص الرسمي الإلكتروني، الإحالة إلى رقم المادة.

(16) République française, Code pénal, article 226-1, version en vigueur depuis le 23/03/2024، Légifrance ؛ ويتضمن النص التقاط الأقوال والصور وتحديد الموقع الجغرافي دون رضا.

ويتميز هذا النص باستيعابه للتقنيات الحديثة، ولا سيما الموقع الجغرافي، وبفصل فعل الالتقاط أو التسجيل أو النقل عن فعل النشر أو الاستعمال. أما المادة 226-2 فتعاقب على الاحتفاظ أو حمل أو إتاحة التسجيل أو الوثيقة للجمهور أو الغير أو استعمالها إذا حصل عليها الجاني بإحدى الوسائل غير المشروعة المشار إليها في المادة 226-1.[17]

وتعالج المادة 226-2-1 نشر الأقوال أو الصور ذات الطابع الجنسي. فإذا انصبت الأفعال على هذا النوع من المحتوى، تشدد العقوبة، ويعاقب من ينشر التسجيل أو الوثيقة دون موافقة على النشر، حتى لو كان الحصول على المحتوى قد تم بموافقة الشخص أو بواسطة الشخص نفسه. وهذا يكرس بوضوح مبدأ استقلال الموافقة على الإنشاء أو الإرسال عن الموافقة على النشر.[18]

المطلب الثالث: اللائحة العامة لحماية البيانات والقانون الفرنسي للمعلوماتية والحريات

تقدم اللائحة العامة لحماية البيانات الأوروبية (GDPR) إطارًا وقائيًا واسعًا. فهي تنظم مبادئ المشروعية والإنصاف والشفافية، وتحديد الغرض، وتقليل البيانات، والدقة، وتحديد مدة التخزين، والسلامة والسرية. كما تقرر حقوق الوصول والتصحيح والمحو، والحق في تقييد المعالجة، والاعتراض، وقابلية نقل البيانات، وتفرض حماية البيانات منذ التصميم وبصورة افتراضية، وتلزم المسؤول عن المعالجة بإثبات الامتثال.[19]

وفي سياق وسائل التواصل الاجتماعي، يعني ذلك أن المنصة يجب أن توضح غرض جمع البيانات، وأساس المعالجة، وفئات المستلمين، وفترة الاحتفاظ، وآليات ممارسة الحقوق. كما أن «الحق في النسيان» لا يعني محو كل معلومة من التاريخ العام دون استثناء، بل يوازن بين مصلحة الشخص في الإزالة وحرية التعبير والالتزام القانوني والمصلحة العامة والأرشفة والبحث.

وتكتمل المنظومة بالجزاءات الإدارية والرقابية التي تفرضها السلطة الفرنسية لحماية البيانات CNIL، فضلًا عن المسؤولية المدنية والجنائية عند تحقق عناصر الجريمة. وهذا يبين أن حماية الخصوصية الرقمية لا تعتمد على العقوبة الجنائية وحدها؛ فالأدوات الوقائية والتنظيمية قد تكون أكثر سرعة وفعالية في وقف المعالجة أو إزالة البيانات.

المطلب الرابع: المقارنة بين العراق ومصر وفرنسا

أولًا: من حيث الأساس الدستوري

يتقارب العراق ومصر في الاعتراف الدستوري بالخصوصية والاتصالات الإلكترونية. غير أن النص المصري أكثر تفصيلًا في اشتراط الأمر القضائي المسبب والمدة المحددة في حالات المراقبة، بينما يقرر النص العراقي حماية الخصوصية والاتصالات مع ربط الكشف بقرار قضائي وضرورة قانونية وأمنية. أما فرنسا فتستند إلى منظومة حقوقية أوسع تجمع بين القانون المدني وقانون العقوبات والاتفاقية الأوروبية واللائحة الأوروبية.

ثانيًا: من حيث تحديد الأفعال المجرمة

يعتمد العراق على نصوص عامة أو متفرقة، أهمها المادة 438، ولا يتضمن نصًا نافذًا خاصًا بالموقع الجغرافي أو المحتوى الحميمي أو انتحال الحساب أو معالجة البيانات. أما مصر فقد أضافت قانونًا خاصًا بتقنية المعلومات وقانونًا للبيانات الشخصية، وإن بقيت بعض المصطلحات بحاجة إلى ضبط. أما فرنسا فقد فصلت بين التقاط الأقوال والصور، وإتاحة التسجيلات، ونشر المحتوى الجنسي، وتحديد الموقع، ومعالجة البيانات.

ثالثًا: من حيث العقوبة

العقوبة العراقية في المادة 438، وهي الحبس مدة لا تزيد على سنة والغرامة أو إحدى العقوبتين، قد لا تعكس اتساع الضرر الناجم عن النشر الجماهيري وإعادة التداول. ويجب ألا يكون الحل هو التشديد المطلق، بل وضع تدرج يميز بين فعل محدود الضرر والنشر التجاري أو الجماهيري أو المرتبط بالابتزاز أو القاصر أو المحتوى الجنسي. وفي فرنسا توجد عقوبات أصلية محددة، مع تشديدات بحسب صفة الفاعل

(17) République française, Code pénal, articles 226-1 و226-2، Légifrance، النسخة النافذة في 2026.

(18) République française, Code pénal, article 226-2-1، Légifrance؛ Loi n° 2016-1321 du 7 octobre 2016, art. 67.

(19) European Union, Regulation (EU) 2016/679, Official Journal of the European Union, 2016, Articles 5, 6, 12–22 and 25.

وطبيعة المحتوى، إلى جانب الجزاءات المدنية والإدارية. أما مصر فتتوزع العقوبات بين قانون العقوبات وقانون تقنية المعلومات وقانون البيانات.

رابعًا: من حيث حماية البيانات

يظهر الفرق الأكبر في وجود إطار شامل لحماية البيانات. ففرنسا تطبق GDPR والقانون الوطني، ومصر أصدرت قانونًا خاصًا للبيانات الشخصية، بينما يفتقر العراق إلى قانون نافذ شامل يحدد مبادئ المعالجة وحقوق صاحب البيانات ومسؤوليات المتحكم والمعالج وسلطة رقابية مستقلة. وهذه الفجوة لا يمكن سدها بتفسير المادة 438؛ لأن المادة تتعلق بالنشر الضار للأسرار، ولا تنظم دورة حياة البيانات منذ جمعها إلى تخزينها ونقلها ومحوها.

خامسًا: من حيث مسؤولية المنصات

لا ينبغي تحميل المنصة مسؤولية جنائية عن كل محتوى ينشره المستخدم، وإلا تحول الأمر إلى رقابة مسبقة واسعة. لكن لا ينبغي أيضًا إعفاؤها مطلقًا. ويجب التمييز بين المنصة التي لا تعلم بالمحتوى، والمنصة التي تتلقى إخطارًا واضحًا بوجود اعتداء جسيم وتملك القدرة المعقولة على الحد منه، والمنصة التي تصمم نظامها عمدًا لترويج المحتوى غير المشروع أو تنتفع من تداوله مع العلم بطبيعته.

سادسًا: من حيث الإزالة العاجلة

يحتاج العراق إلى نظام قضائي وإداري يتيح وقف الانتشار وحفظ الدليل. ويجب أن يكون أمر الإزالة محددًا بالمحتوى غير المشروع، لا أن يتحول إلى حجب حساب كامل إلا عند الضرورة. وينبغي إتاحة الاعتراض والمراجعة، مع حماية الأدلة قبل الحذف.

المطلب الخامس: التوازن بين الخصوصية وحرية التعبير

لا توجد حماية مطلقة للخصوصية ولا حرية مطلقة في النشر. ويجب أن تقوم الموازنة على معايير قابلة للتطبيق:

1. طبيعة الشخص: هل هو شخص عادي أم شخصية عامة؟
2. طبيعة المعلومة: هل تتعلق بالشأن العام أم بالأسرة والصحة والعلاقة الحميمية؟
3. طريقة الحصول: هل حصل الناشر عليها بطريقة مشروعة؟
4. الرضا: هل كان محددًا للنشر أو مقتصرًا على الإرسال الخاص؟
5. المصلحة العامة: هل يكشف النشر فسادًا أو خطرًا حقيقيًا؟
6. طريقة العرض: هل اقتصر على معلومة ضرورية أم أضيفت عبارات مهينة؟
7. مدى الضرر والانتشار: هل هو تداول محدود أم حملة جماهيرية؟
8. وجود بديل أقل مساسًا بالخصوصية.

وتتعاظم الحماية عندما يتعلق المحتوى بقاصر أو ضحية عنف أو مريض أو شخص لا يستطيع الدفاع عن نفسه. وفي المقابل، لا يجوز استخدام الخصوصية لمنع نشر معلومات موثقة وضرورية للمساءلة العامة، مع ضرورة إخفاء البيانات الزائدة التي لا تخدم المصلحة العامة.

الخاتمة

1. الحياة الخاصة في العصر الرقمي تشمل المكان والاتصالات والصورة والصوت والمعلومات الصحية والعائلية والموقع الجغرافي والبيانات التي تسمح بتكوين ملف عن الشخص.
2. الاعتراف الدستوري العراقي بالخصوصية والاتصالات الإلكترونية يوفر أساسًا قويًا، لكنه يحتاج إلى تشريع تفصيلي.
3. المادة 438 من قانون العقوبات العراقي تستوعب نشر الأخبار والصور والتعليقات الخاصة، ولو كانت صحيحة، إذا كان من شأن النشر الإساءة، لكنها لا تغطي جميع صور المعالجة الرقمية والاختراق والتتبع.

4. عدم وجود قانون عراقي نافذ شامل للجرائم المعلوماتية وحماية البيانات يسبب فراغًا أو تشتتًا في التجريم والإجراءات والمسؤولية.

5. القذف والسب والتهديد والابتزاز قد تتصل بالاعتداء على الحياة الخاصة، لكنها لا تغني عن جريمة انتهاك الخصوصية لأن الأخيرة قد تقع دون كذب أو إهانة.

6. أضاف القانون المصري رقم 175 لسنة 2018 حماية تقنية متخصصة، وأضاف قانون حماية البيانات رقم 151 لسنة 2020 إطارًا وقائيًا لمعالجة البيانات.

7. يقدم القانون الفرنسي أكثر النماذج تكاملًا، خصوصًا من خلال المواد 226-1 و226-2 و226-2-1، والمادة 9 مدني، وGDPR.

8. نشر المحتوى الحميمي دون موافقة على النشر يجب أن يعد فعلًا مستقلًا حتى لو أنشئ المحتوى أو أرسل بموافقة سابقة.

9. لقطة الشاشة ليست دليلًا مكتملًا بذاتها في كل الأحوال، بل ينبغي دعمها بوسائل إثبات المصدر والسلامة والهوية والزمن.

10. حماية المنصات يجب أن توازن بين عدم فرض رقابة عامة وبين إلزامها بالاستجابة المعقولة للإخطارات القضائية والمحتوى الجسيم غير المشروع.

تؤكد المقارنة أن الحماية الجنائية للحياة الخاصة في ظل وسائل التواصل الاجتماعي لا تقاس بعدد النصوص العقابية، بل بقدرة المنظومة على تحديد الحق والفعل المجرم والرضا والضرر والدليل والإجراء والعلاج. وقد وفر العراق أساسًا دستوريًا مهمًا، وقدم قانون العقوبات حماية معتبرة لأسرار الحياة الخاصة والعائلية من خلال المادة 438، لكن هذه الحماية صممت أساسًا لبيئة النشر التقليدي. ولذلك تواجه صعوبة في استيعاب التتبع الجغرافي، والمعالجة الآلية، وانتحال الحسابات، والنشر المتسلسل، والدور المركب للمنصات.

أما مصر فقد اتجهت إلى الجمع بين النصوص التقليدية والقانون المتخصص للجرائم المعلوماتية وقانون حماية البيانات. وتوفر هذه البنية قدرة أكبر على التكييف، لكنها تحتاج إلى ضبط المصطلحات ومراعاة الشرعية وحرية التعبير. ويقدم النموذج الفرنسي منظومة أكثر تكاملًا؛ إذ يحمي الحق مدنيًا ويجرم صور الاعتداء الأساسية ويفرد حكمًا للمحتوى الجنسي ويكمل ذلك بإطار شامل لحماية البيانات وحقوق الشخص.

والحل الملائم للعراق ليس نسخ النص الفرنسي أو المصري، بل بناء قانون وطني يستفيد من المقارنة ويحترم الدستور وخصوصية البيئة العراقية. وينبغي أن يكون القانون واضحًا في حماية البيانات والمحتوى الخاص، مرنًا في مواجهة التقنية، متدرجًا في العقوبة، سريعًا في الإزالة وحفظ الدليل، ومقيدًا بضمانات القضاء وحرية التعبير. وبذلك تتحول حماية الحياة الخاصة من إعلان دستوري ونصوص متفرقة إلى منظومة قابلة للتطبيق في الواقع الرقمي.

التوصيات

1. إصدار قانون عراقي مستقل للجرائم المعلوماتية وحماية البيانات الشخصية بدل الاعتماد على نصوص متفرقة أو مشروعات غير نافذة.

2. تعريف الحياة الخاصة والبيانات الشخصية والبيانات الحساسة والمحتوى الحميمي والحساب الرقمي.

3. تجريم التقاط أو تسجيل أو نشر الأقوال والصور والمحادثات والموقع الجغرافي دون رضا أو سند قانوني.

4. النص على أن الموافقة على إنشاء أو إرسال المحتوى لا تعني الموافقة على نشره أو إعادة نشره.

5. وضع عقوبة متدرجة، مع ظروف مشددة للنشر الجماهيري، أو تحقيق ربح، أو استعمال حسابات متعددة، أو استهداف قاصر، أو اقتران الفعل بابتزاز أو تهديد.

6. تنظيم مسؤولية إعادة النشر؛ فلا يعاقب المستخدم لمجرد التفاعل العرضي غير العالم، بينما تقوم المسؤولية عند العلم بطبيعة المحتوى والقصد إلى توسيع انتشاره.

7. إنشاء أو تحديد جهة مستقلة لحماية البيانات وتلقي الشكاوى ومراقبة المعالجة.

8. تقرير حقوق الوصول والتصحيح والمحو والاعتراض وتقييد المعالجة، مع استثناءات محددة للصحافة والبحث والمصلحة العامة.

9. وضع قواعد للدليل الرقمي تحفظ المصدر وسلسلة الحيازة وتمنع الوصول غير القضائي إلى البيانات الخاصة.

10. إنشاء إجراء عاجل لوقف النشر وحفظ الدليل، مع ضمان التسبيب والمراجعة والتظلم.
11. تدريب القضاة وأعضاء الادعاء العام والشرطة والخبراء على التحقيق الرقمي والجرائم المرتبطة بالمنصات.
12. إبرام اتفاقيات تعاون دولي وطلب الانضمام إلى الأطر الدولية الملائمة لمكافحة الجرائم الإلكترونية.
13. حماية حرية التعبير والصحافة من خلال اشتراط المصلحة العامة والتناسب وعدم تجريم النقد أو كشف الفساد حسن النية.
14. إلزام المنصات العاملة داخل العراق بتعيين قناة إخطار واضحة، وحفظ البيانات مدة محددة بأمر قضائي، والتعاون في حدود القانون.

قائمة المصادر والمراجع

أولًا: التشريعات والوثائق الرسمية

جمهورية العراق .(2005) .*دستور جمهورية العراق لسنة 2005* (المادة 17). وزارة الخارجية العراقية.

جمهورية العراق .(1969) .*قانون العقوبات رقم 111 لسنة 1969 المعدل* (المواد 327–328، 428، 433–438). الجريدة الرسمية.

مجلس القضاء الأعلى العراقي. (2018، 17 مايو). كاظم عبد جاسم الزيدي .*جريمة انتهاك حرمة الحياة الخاصة*.

جمهورية مصر العربية .(2014) .*دستور جمهورية مصر العربية لسنة 2014 المعدل* (المادة 57). الهيئة العامة للاستعلامات.

جمهورية مصر العربية .(1937) .*قانون العقوبات رقم 58 لسنة 1937 المعدل* (المواد 302–306، 309 مكرر، 309 مكرر أ). الجريدة الرسمية.

جمهورية مصر العربية. (2018، 14 أغسطس) .*قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018* (المواد 1، 2، 25–28). الجريدة الرسمية، العدد 32 مكرر (ج).

جمهورية مصر العربية .(2020) .*قانون حماية البيانات الشخصية رقم 151 لسنة 2020* (المواد 1–5، 13–17، 36–48). الجريدة الرسمية.

République française. (2026). *Code civil* (Article 9). Légifrance.

République française. (2026). *Code pénal* (Articles 226-1 à 226-7). Légifrance.

Council of Europe. (1950). *European Convention on Human Rights* (Article 8).

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. Official Journal of the European Union.

United Nations. (1966). *International Covenant on Civil and Political Rights* (Article 17). United Nations Treaty Series, 999.

ثانيًا: الكتب العربية

حجازي، عبد الفتاح بيومي .(2006) .*جرائم الكمبيوتر والإنترنت: الجرائم المعلوماتية في القانون العربي المقارن* .دار الفكر الجامعي.

رشاد، محمد .(2010) .*الحماية الجنائية لحرمة الاتصالات الشخصية: دراسة مقارنة* .دار الجامعة الجديدة.

سرور، أحمد فتحي .(2015) .*الوسيط في قانون العقوبات: القسم الخاص* .دار النهضة العربية.

عبد ربه، محمد أحمد المعداوي مجاهد .(2018) .*حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة* .دار النهضة العربية.

عبد اللطيف، محمد .(2011) .*الحماية الجنائية للحق في الحياة الخاصة: دراسة مقارنة* .دار النهضة العربية.

منصور، محمد حسين .(2014) .*المسؤولية الإلكترونية: دراسة في المسؤولية المدنية والجنائية عن استخدام وسائل التقنية الحديثة* .دار الجامعة الجديدة.

حسني، محمود نجيب .(2015) .*شرح قانون العقوبات: القسم الخاص* (طبعة محدثة). دار النهضة العربية.

ثالثًا: المراجع الفرنسية والأجنبية

European Union Agency for Fundamental Rights, & Council of Europe. (2018). *Handbook on European data protection law*. Publications Office of the European Union.

Gassin, R., Moreau, V., & Rassat, M.-L. (2019). *Droit pénal spécial*. Dalloz.

Merle, R., & Vitu, A. (1982). *Traité de droit criminel: Droit pénal spécial*. Cujas.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Pradel, J. (2017). *Droit pénal spécial* (19e éd.). Cujas.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

رابعًا: الدراسات والمقالات المحكمة

بوقرين، عبد الحليم. (2019). المسؤولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الاجتماعي: دراسة مقارنة .*مجلة جامعة الشارقة للعلوم القانونية*.

A comparative study between Iraqi and French legislation in the criminal protection of privacy. (2020). *Journal of Law and Administrative Studies*.

Comparative analysis of criminal sanctions for violations of privacy in the digital environment. (2024). *Journal of Legal and Social Studies and Research*.

Commission nationale de l'informatique et des libertés (CNIL). (n.d.). *Le règlement général sur la protection des données*.

Human Rights Committee. (1988). *General Comment No. 16: Article 17 (Right to Privacy)*. United Nations.