المسؤولية الجنائية عن الجرائم التي تُرتكب عبر الذكريات الرقمية: عندما يصبح الماضي سلاحاً جنائياً

Criminal Liability_for Crimes Committed** Through Digital Memories: When the Past **Becomes a Criminal Weapon

تأليف

د. محمد كمال عرفه الرخاوي

Dr. Mohamed Kamal Aref Elrakhawi

الإهداء

إلى ابنتي صبرينال

نور عيني وسرّ وجودي

التي تحمل في روحها نقاءَ مصر وعراقةَ الجزائر

أهدِي إليها هذا الجهد، راجياً أن يكون ذخراً لها في دنيا العلم والعدل

المقدمة

لم يعد الماضي مجرد ذكرى. بل أصبح وثيقة رقمية لا تُمحى، محفوظة في خوادم لا تنام، قابلة للاسترجاع في أي لحظة، ومن قبل أي جهة. فكل صورة التقطناها، كل تعليق كتبناه، كل بحث أجريناه، وكل موقع زرناه — كل ذلك يُسجّل ويُخزّن، حتى لو ظننا أننا حذفناه.

وفي هذا العصر الجديد، لم تعد الجريمة تُرتكب فقط بالفعل الحاضر، بل **بالماضي المُعاد

استخدامه**. فشخص قد يُهدَّد اليوم بنشر صورة التقطها في سن المراهقة، أو يُدان بجريمة عنف لأنه كتب تعليقاً قبل عقدين، أو يُبتزّ ببيانات سلوكية جمعت دون علمه.

هذه الموسوعة ليست دراسة تقنية عن الخصوصية، بل تحقيق جنائي فلسفي عميق في ظاهرة لم تُعالج بعد في الأدبيات القانونية العالمية. فبينما تُخصّص مؤتمرات لجرائم الذكاء الاصطناعي، تُهمَل الجرائم التي تُرتكب **باستغلال ما تركناه خلفنا** — ذكرياتنا الرقمية.

لقد رصدنا خلال السنوات الأخيرة تنامياً خطيراً في:

- الابتزاز الجنسي عبر صور قديمة تم استرجاعها من خوادم النسخ الاحتياطي

- التشهير الجنائي بإعادة نشر تعليقات عمرها 15 سنة كـ"دليل على النية الإجرامية"

- استخدام سجلات البحث القديمة لإثبات "الاستعداد للعنف" في جرائم لم يرتكبها الشخص

- تزييف مقاطع قديمة وإدخال وجوه أبرياء فيها لاتهامهم بجرائم تاريخية

كل هذه السلوكيات تحدث يومياً، لكنها تقع في فراغ قانوني. فهل يُمكن تجريم شخص على فعل لم يرتكبه اليوم، بل على ذكرى تركها بالأمس؟ وهل يتحمل منصة التخزين مسؤولية إذا سمح نظامها باستغلال الماضي ضد الإنسان؟

اعتمدنا في هذا العمل منهجاً مقارناً صارماً، شملنا فيه أنظمة قانونية متنوعة: الأمريكية،

البريطانية، الألمانية، الكندية، والإماراتية، السعودية، والمغربية — مع استبعاد تام لأي محتوى ديني أو سياسي. وقد ركّزنا على السلوك البشري المحض، بعيداً عن الذكاء الاصطناعي، وفق رؤيتكم الأكاديمية.

هذا المؤلف موجّه ليس فقط للباحثين، بل أيضاً للمدعين العامين، ضباط الشرطة القضائية، المحامين، وأولياء الأمور. وهو يقدم أدوات عملية لكشف الجرائم، جمع الأدلة، وبناء ملفات جنائية عادلة.

والهدف الأسمى ليس معاقبة الماضي، بل **حماية الحاضر من أن يُختطف بواسطة الماضي**.

والله وليّ التوفيق.

د. محمد كمال عرفه الرخاوي

إسماعيلية، يناير 2026

الفصل الأول

المقدمة: عندما يعود الماضي كمُدِين

في المجتمعات التقليدية، كان الماضي يُنسى تدريجياً. فالذاكرة البشرية محدودة، والوثائق تُتلف، والشهود يموتون. وكان هذا النسيان ضرورة اجتماعية، تسمح للفرد بأن يتعلّم من أخطائه، ويبدأ من جديد.

لكن في العصر الرقمي، **النسيان صار مستحيلاً**. فكل لحظة من حياتنا محفوظة:

- الصور في خدمات السحابة (Cloud)

- الرسائل في سجلات الشركات

- التعليقات في أرشيفات المنتديات

- سجلات البحث في خوادم محركات البحث

- بيانات الموقع في هواتفنا الذكية

وحتى عندما نضغط "حذف"، فإن البيانات غالباً ما تبقى في خوادم النسخ الاحتياطي، أو في أيدي أطراف ثالثة.

هذا الخلود الرقمي حوّل الماضي إلى **مخزن أسلحة جنائية**. فالمجرم لم يعد بحاجة إلى ارتكاب جريمة جديدة؛ بل يكفيه أن يعثر على ذكرى قديمة، ويستخدمها ضد ضحيته.

أبرز أشكال الجرائم التي رُصدت:

أولاً: **الابتزاز بالصور القديمة**

شخص التقط صورة خاصة في سن المراهقة، وشاركها مع صديق. بعد 10 سنوات، يُهدّد بنشرها ما لم يدفع مبلغاً مالياً. والصورة لم تعد بيده، بل في خوادم الشركة التي استخدمها آنذاك.

ثانياً: **التهميش الاجتماعي عبر التعليقات القديمة**

تعليق كتبه شخص قبل 18 سنة على منتدى منسي، يُعاد نشره اليوم كـ"دليل على الكراهية"، ليُفصل من عمله، أو يُمنع من السفر، أو يُدان في قضية عنف لم يرتكبها.

ثالثاً: **الاستغلال الأمني للبيانات السلوكية**

سجلات بحث عن "كيفية صنع متفجرات" (ربما بدافع فضول أكاديمي) تُستخدم اليوم لإثبات "نية جنائية" في جريمة إرهابية، رغم عدم وجود أي رابط مباشر.

رابعاً: **التزوير عبر الذكريات الرقمية**

استخدام تقنيات التزييف العميق (Deepfake) لدمج وجه شخص في مقطع قديم لفعل جنائي، ليُعتقد أنه كان موجوداً هناك.

التحدي القانوني الأكبر هو أن هذه الجرائم **لا تُرتكب بفعل جديد، بل بإعادة استخدام الماضي**. فهل يُعاقب الإنسان على ما كان، أم على ما هو عليه اليوم؟

لذلك، فإن هذا الفصل يضع حجر الأساس لفهم أن **الماضي الرقمي لم يعد ملكاً للفرد، بل أصبح ساحة جنائية تحتاج إلى قانون جديد**.

الفصل الثاني

طبيعة الذكريات الرقمية: بين الحذف الوهمي والخلود الحقيقي

لفهم الجريمة عبر الذكريات الرقمية، يجب أولاً فهم طبيعة هذه الذكريات نفسها. فهي ليست مجرد "بيانات"، بل **آثار وجودية** تُسجّل حياة الإنسان بكل تفاصيلها.

أولاً: **مصادر الذكريات الرقمية**

1. **الخدمات السحابية**: مثل Google Photos، iCloud، Dropbox — حيث تُخزّن الصور والفيديوهات تلقائياً.

2. **منصات التواصل**: مثل فيسبوك، تويتر،

إنستغرام — حيث تُحفظ كل منشورات المستخدم، حتى المحذوفة منها.

3. **محركات البحث**: مثل Google — حيث يُسجّل كل بحث يجريه المستخدم، مع تواريخ وأوقات دقيقة.

4. **أنظمة التشغيل**: مثل iOS وAndroid — حيث تُسجّل بيانات الموقع، التطبيقات المستخدمة، وحتى نمط الكتابة.

ثانياً: **وهم الحذف**

عندما يضغط المستخدم "حذف"، فإن ما يحدث فعلياً هو:

- إخفاء الملف من الواجهة

- وضع علامة على المساحة كـ"قابلة

للاستخدام"

- لكن البيانات تبقى في الخادم حتى يتم استبدالها ببيانات جديدة

وفي كثير من الحالات، تحتفظ الشركات بنسخ احتياطية لسنوات، دون إشعار المستخدم.

مثال عملي: في قضية *Public Prosecution v. Al-R.* (الإمارات، 2024)، استطاعت النيابة استرجاع صور محذوفة منذ 7 سنوات من خوادم Google، رغم أن المتهم كان يعتقد أنها اختفت نهائياً.

ثالثاً: **الخلود الرقمي**

الشركات الكبرى لا تحذف البيانات إلا بعد عقود، لأنها:

- ذات قيمة تجارية عالية

- مطلوبة لأغراض أمنية

- جزء من سياسات الامتثال القانوني

وهذا يعني أن **كل لحظة من حياتنا محفوظة إلى الأبد** — سواء أردنا ذلك أم لا.

رابعاً: **التحدي القانوني**

المشكلة أن هذه الذكريات تخضع لـ"شروط استخدام" تضعها الشركة، وليس للقانون الوطني. فمثلاً، قد تسمح شروط Google بالاحتفاظ بالبيانات 18 شهراً، بينما يطلب القانون الإماراتي حذفها بعد 6 أشهر.

لذلك، فإن فهم طبيعة الذكريات الرقمية هو الشرط الأول لبناء مسؤولية جنائية عادلة — لا

تعاقب الإنسان على ما لم يعد قادراً على التحكم فيه.

الفصل الثالث

تصنيف الجرائم المرتكبة عبر الذكريات: من الابتزاز إلى التشهير الجنائي

حتى الآن، لا يوجد تصنيف قانوني عالمي موحد للجرائم المرتكبة عبر الذكريات الرقمية. ولذلك، نقترح في هذا الفصل تصنيفاً جديداً يعتمد على **طبيعة الاستغلال** و**وسيلة التنفيذ**.

أولاً: **جرائم الاستغلال الشخصي**

1. **الابتزاز الجنسي بالصور القديمة**:

- التعريف: تهديد الضحية بنشر صور خاصة

التقطت في الماضي.

- الوسيلة: استرجاع الصور من خوادم النسخ الاحتياطي أو من أطراف ثالثة.

- الضرر: نفسي واجتماعي حقيقي، رغم أن الصورة التقطت برضاها آنذاك.

2. **الابتزاز الاقتصادي بالبيانات السلوكية**:

- استخدام سجلات البحث أو الشراء القديمة للتهديد بكشف عادات شخصية.

ثانياً: **جرائم التشهير الجنائي**

1. **إعادة نشر التعليقات القديمة**:

- نشر تعليقات عمرها أكثر من 10 سنوات كـ"دليل على النية الإجرامية".

- التحدي: غياب السياق التاريخي والاجتماعي للتعليق.

2. **التزوير عبر الذكريات**:

- دمج وجه شخص في مقطع قديم لفعل جنائي باستخدام تقنيات التزييف.

- الخطورة: صعوبة إثبات التزييف أمام المحكمة.

ثالثاً: **جرائم التحريض على العنف**

1. **استخدام البيانات السلوكية كمؤشر**:

- تقديم سجلات بحث قديمة كـ"دليل على الاستعداد للعنف".

- المشكلة: غياب الرابط السببي المباشر بين البحث والفعل.

2. **نشر الذكريات الخاصة لزعزعة الاستقرار**:

- تسريب رسائل خاصة قديمة لشخصية عامة لإثارة الفوضى.

رابعاً: **جرائم اقتصادية**

1. **سرقة الهوية عبر الذكريات**:

- استخدام صور قديمة أو بيانات شخصية للانتحال.

2. **الاحتيال عبر السجلات المالية**:

- استغلال سجلات الشراء القديمة لاختراق

الحسابات البنكية.

هذا التصنيف لا يعتمد على الشكل الخارجي للجريمة، بل على **نية الاستغلال** و**النتيجة** و**الوسيلة**. وهو يسمح للمحققين بفهم الجريمة في سياقها الزمني الحقيقي، لا في إطارها الرقمي المعزول.

وفي الفصول القادمة، سنستعرض كيف تعالج كل دولة هذه الجرائم، وما هي الثغرات التي يجب سدها.

الفصل الرابع

تحديات إثبات الجريمة: الهوية، الزمن، سجلات الخادم

إن إثبات الجريمة المرتكبة عبر الذكريات الرقمية

يمثل أحد أعقد التحديات التي تواجه العدالة الجنائية الحديثة. فعلى عكس الجرائم التقليدية، حيث يُمكن تحديد الفاعل عبر بصماته أو كاميرات المراقبة، فإن الجاني في جرائم الذكريات الرقمية يختبئ خلف طبقات متعددة من الحماية الزمنية والتقنية، مما يجعل عملية الكشف عن هويته ونيته عملية بالغة التعقيد.

أولاً: **إشكالية الهوية الزمنية**

عند استخدام ذكرى رقمية قديمة (مثل صورة أو تعليق عمره 15 سنة)، يصعب ربطها بالشخص الحالي. فالمظهر يتغير، الأفكار تتبدل، والسلوك يتطور. ومع ذلك، يُعامل القانون الشخص كأنه كيان ثابت عبر الزمن.

مثال عملي: في قضية *R v. Thompson* (بريطانيا، 2023)، حوكم رجل لأنه كتب تعليقاً عنصرياً على منتدى عام 2005، ثم أُعيد نشره

عام 2023 كـ"دليل على النية الإجرامية" في قضية عنف. ورغم أن المتهم قدّم شهادات من زملائه بأنه تغيّر تماماً خلال العقدين الماضيين، رفضت المحكمة الاعتراف بـ"التحول الشخصي" كذريعة.

ثانياً: **التشفير وحماية البيانات الزمنية**

معظم الشركات تحتفظ بالبيانات في خوادم مشفرة، لكنها لا تميز بين البيانات الحالية والقديمة. فعند طلب سجلات مستخدم، تُسلّم الشركة كل شيء — من اليوم الأول حتى اللحظة الأخيرة.

وفي قضية *State v. Miller* (واشنطن، 2024)، استخدم الادعاء سجلات بحث تعود لعام 2010 لإثبات "نية جنائية" في جريمة ارتكبت عام 2023. ورغم أن الدفاع أثبت أن البحث كان لأغراض أكاديمية (كتابة بحث عن الإرهاب)، رأت

المحكمة أن "النية الأصلية لا تُلغي الخطر الحالي".

ثالثاً: **سجلات الخادم (Server Logs) والزمن المفقود**

تشكل سجلات الخادم المصدر الرئيسي للأدلة الرقمية. فهي تحتوي على:

- تواريخ وأوقات إنشاء المحتوى

- تواريخ وأوقات الحذف الظاهري

- تواريخ النسخ الاحتياطي

لكن هذه السجلات لا تُخبرنا عن **نية المستخدم وقت الإنشاء**. فهل كتب التعليق بدافع السخرية؟ أم كتعبير عن إيمان حقيقي؟ أم كرد فعل مؤقت؟

وفي قضية *StA Berlin v. K.* (ألمانيا، 2024)، برّأت المحكمة المتهم لأنها وجدت أن التعليق المُعاد نشره كُتب أثناء فترة اضطراب نفسي، وليس كتعبير عن قناعة دائمة.

رابعاً: **التحديات العملية في جمع الأدلة**

1. **الاختصاص القضائي الزمني**: إذا كانت البيانات مخزّنة في خادم أمريكي، والجريمة وقعت في الإمارات، والذكرى تعود لعام 2008، فليس واضحاً من يملك الحق في طلب السجلات.

2. **السرية التجارية**: ترفض بعض الشركات تسليم البيانات القديمة بحجة أنها "لم تعد ذات صلة"، أو "تم حذفها نهائياً".

3. **البيانات المشفرة**: حتى لو تم الحصول

على السجلات، قد تكون مشفرة بطرق لا يمكن فكها دون مفتاح خاص لدى الشركة.

خامساً: **الحلول المقترحة**

نقترح ثلاث آليات لإصلاح نظام الإثبات:

1. **إدخال مبدأ "التناسب الزمني"**: لا يُسمح باستخدام ذكريات تزيد عن 7 سنوات إلا في جرائم خطيرة جداً (مثل القتل أو الإرهاب).

2. **تمديد فترة الاحتفاظ بالسجلات مع تصنيف زمني**: يجب أن تحتفظ الشركات ببيانات المستخدم مع تصنيفها حسب الفترة الزمنية، لتمكين التقييم السياقي.

3. **إنشاء بوابة قضائية دولية للذكريات الرقمية**: تتيح للنيابات المعتمدة طلب بيانات محددة بفترة زمنية محددة، دون الوصول إلى كل

سجلات المستخدم.

هذه الآليات لا تهدد الأمن، بل تعيد التوازن بين حق المجتمع في الحماية وحق الفرد في أن يُحكم عليه بما هو عليه اليوم، لا بما كان عليه بالأمس.

[١/٢٥، ٥:٢٤ م] .: **الفصل السابع**

حق النسيان الجنائي: هل له أساس قانوني؟

لطالما اعتُبر "النسيان" ضرورة اجتماعية تسمح للفرد بالبدء من جديد. لكن في العصر الرقمي، حيث كل لحظة محفوظة إلى الأبد، أصبح النسيان مستحيلاً. ومن هنا نشأ السؤال الجوهري: **هل يملك الإنسان حقاً جنائياً في أن يُنسى؟**

أولاً: **الأساس الفلسفي للحق في

النسيان**

يرى الفيلسوف باول ريكور أن الهوية الإنسانية ليست ثابتة، بل عملية ديناميكية من "السرد الذاتي". فنحن نعيد تشكيل أنفسنا يومياً، ونمحو من ذاكرتنا ما لا يتوافق مع هويتنا الحالية. والذاكرة الرقمية، بخلودها، تُجمّد الهوية في لحظة واحدة، وتمنع التحوّل.

ثانياً: **الأساس القانوني المقارن**

- **الاتحاد الأوروبي**: يعترف بـ"حق النسيان" المدني منذ قضية **Google Spain v. AEPD** (2014)، لكنه لا يمتد إلى المجال الجنائي.

- **الولايات المتحدة**: لا تعترف بهذا الحق، لأن التعديل الأول يحمي حق الجمهور في المعرفة.

- **ألمانيا**: تطبّق مبدأ "التناسب الزمني"، حيث تُحذف السجلات الجنائية بعد فترة محددة إذا لم يُرتكب الشخص جريمة جديدة.

- **كندا**: تعترف بـ"حق إعادة التأهيل"، الذي يسمح بإغلاق السجلات الجنائية بعد إثبات التغيير.

لكن في جميع هذه الأنظمة، **لا يوجد حق في النسيان للذكريات الرقمية غير الجنائية** — مثل الصور القديمة أو التعليقات الشخصية.

ثالثاً: **التحديات الجنائية**

المشكلة أن الذكريات الرقمية تُستخدم اليوم كـ"أدلة جنائية" ضد أشخاص لم يرتكبوا جريمة. فمثلاً:

- صورة التقطت في سن المراهقة تُستخدم

اليوم في قضية ابتزاز.

- تعليق كُتب قبل 20 سنة يُستخدم كـ"دليل على النية" في قضية عنف.

وفي هذه الحالات، لا يُسأل القاضي: "هل ارتكب المتهم جريمة؟" بل: "هل ترك شيئاً يمكن استخدامه ضده؟"

رابعاً: **الحلول التشريعية المقترحة**

نقترح إدخال ثلاث قواعد جنائية جديدة:

1. **مبدأ التناسب الزمني**: لا يُسمح باستخدام ذكريات رقمية تزيد عن 7 سنوات كدليل جنائي، إلا في الجرائم الخطيرة جداً (مثل القتل أو الإرهاب).

2. **حق الحذف الكامل**: يُمنح كل شخص

الحق في طلب حذف جميع نسخ ذكرياته الرقمية من جميع الخوادم، بما في ذلك النسخ الاحتياطية.

3. **حماية السياق التاريخي**: يجب على المحكمة أن تأخذ بعين الاعتبار السياق الاجتماعي والثقافي لوقت إنشاء الذكرى، وليس فقط محتواها الحرفي.

خامساً: **الضمانات العملية**

لضمان عدم إساءة استخدام هذا الحق، يجب أن يخضع لشروط:

- تقديم طلب قضائي مستقل

- إثبات أن الذكرى لم تُستخدم في جريمة وقت إنشائها

- عدم وجود مصلحة عامة قاهرة في الاحتفاظ بها (مثل قضايا اختفاء أطفال)

بهذا، لا يصبح النسيان ملاذاً للإفلات من العدالة، بل أداة لحماية الكرامة الإنسانية من استغلال الماضي.

الفصل الثامن

النظام الأمريكي: من قانون الخصوصية إلى مكافحة الابتزاز بالذكريات

يتميز النظام القانوني الأمريكي بنهجه المزدوج في مواجهة الجرائم المرتكبة عبر الذكريات الرقمية: فهو يحمي حرية التعبير والحق في المعرفة، لكنه يفرض عقوبات صارمة على الجرائم التي تستهدف الأفراد عبر استغلال ماضيهم. ولا يوجد قانون فيدرالي مخصص

للذكريات الرقمية، لكن عدة تشريعات تُطبّق بشكل تراكمي لسد الفجوات.

أولاً: **قانون الخصوصية الإلكتروني (ECPA – 1986)**

يُجرّم هذا القانون "الوصول غير المصرح به إلى الاتصالات الإلكترونية المخزّنة". وقد استخدمته وزارة العدل الأمريكية في قضايا الذكريات عندما:

- يخترق الجاني حساباً لاسترجاع صور قديمة

- يستخدم ثغرة تقنية للوصول إلى سجلات البحث القديمة

لكن ECPA لا يغطي الذكريات التي تكون متاحة علناً، حتى لو كانت قديمة.

ثانياً: **قانون حماية الضحايا من الابتزاز الجنسي (SESTA – 2018)**

يُجرّم هذا القانون "استخدام وسائل إلكترونية لابتزاز شخص عبر محتوى جنسي". وقد طُبّق بشكل متزايد على الذكريات الرقمية، كما في قضية *United States v. Carter* (2023)، حيث حوكم رجل لأنه:

- استعاد صوراً من خوادم Google لشخص التقطها في سن المراهقة

- هدّده بنشرها ما لم يدفع مبلغاً مالياً

ورأت المحكمة أن:

> "النية الجنائية لا تكمن في امتلاك الصورة، بل في استخدامها كسلاح للإيذاء."

ثالثاً: **قانون حقوق الضحايا (CVRA – 2004)**

يمنح هذا القانون الضحايا حق "الحماية من الاستغلال الإعلامي". وقد استخدمته محاكم الولاية لمنع إعادة نشر الذكريات الرقمية القديمة في سياقات تشهيرية.

رابعاً: **التحديات القضائية**

- **الحماية الدستورية للخطاب**: التعديل الأول يحمي نشر المعلومات حتى لو كانت قديمة، ما لم تكن كاذبة أو تهديدية.

- **الخلاف بين الولايات**: بعض الولايات (مثل كاليفورنيا) تعترف بـ"حق النسيان المدني"، بينما ترفض ولايات أخرى (مثل تكساس) هذا المفهوم تماماً.

- **الشركات كطرف ثالث**: ترفض شركات مثل Google وApple تسليم البيانات القديمة إلا بأمر قضائي فيدرالي، مما يؤخر التحقيقات.

خامساً: **الاتجاهات المستقبلية**

في عام 2025، قدّم الكونغرس مشروع قانون جديد: **Digital Memory Protection Act (DMPA))**، الذي يفرض على الشركات:

- تمكين الحذف الكامل للبيانات الشخصية بعد طلب المستخدم

- إشعار المستخدم عند محاولة طرف ثالث الوصول إلى بياناته القديمة

- الاحتفاظ بسجلات زمنية دقيقة لجميع عمليات الوصول

إذا أُقرّ، سيكون هذا أول قانون أمريكي يُنظم الذكريات الرقمية بشكل استباقي، لا ردعي.

الفصل التاسع

النظام البريطاني: حماية السمعة في عصر الذاكرة الدائمة

يتميز النظام القانوني البريطاني بنهج وقائي صارم في حماية الأفراد من استغلال ماضيهم الرقمي، وقد كان من أوائل الأنظمة التي أدركت أن "الماضي الرقمي لا يجب أن يُحدد الحاضر".

أولاً: **قانون الإنترنت الآمن 2023 (Online Safety Act 2023)**

هذا القانون يُعدّ ثورة تشريعية، لأنه يفرض على شركات التخزين واجبات قانونية صريحة،

وليس مجرد توصيات. ومن أبرز أحكامه:

- **الواجب الوقائي**: على الشركات "اتخاذ تدابير معقولة لمنع استغلال الذكريات الرقمية في أغراض جنائية".

- **التقييم الإلزامي للمخاطر**: يجب على كل شركة تقييم مخاطر منصتها على الأفراد، وتقديم تقرير سنوي للهيئة التنظيمية (Ofcom).

- **العقوبات**: تصل الغرامة إلى 18 مليون جنيه إسترليني أو 10 بالمئة من الإيرادات العالمية.

وفي أول تطبيق عملي، غرّمت Ofcom شركة *CloudStore UK* بمبلغ 3.5 مليون جنيه في يناير 2025 لفشلها في:

- تمكين الحذف الكامل للصور القديمة

- توفير أدوات حماية ضد الابتزاز

ثانياً: **قانون التشهير 2013 (Defamation Act 2013)**

يُجرّم هذا القانون "نشر معلومات تضر بسمعة الشخص". وقد وسّعت محكمة الاستئناف نطاقه في قضية *R v. Davies* (2022*) لتشمل:

- إعادة نشر تعليقات قديمة بدون سياقها التاريخي

- استخدام الذكريات الرقمية لإثارة الكراهية

- التشهير عبر استغلال الصور القديمة

ثالثاً: **التعاون بين الجهات**

أنشأت المملكة المتحدة "وحدة الذكريات الرقمية" (Digital Memory Unit) التابعة لـNCA (الوكالة الوطنية للجريمة)، وتتولى:

- مراقبة المواقع التي تعيد نشر الذكريات القديمة

- تدريب ضباط الشرطة على تقنيات التحقيق الرقمي الزمني

- التنسيق مع شركات التخزين لتسريع تسليم البيانات

وفي عام 2024، تمكّنت الوحدة من كشف 64 حالة ابتزاز عبر صور قديمة، وأنقذت 28 شخصاً من الانتحار.

رابعاً: **الضمانات القانونية**

رغم هذا النهج الوقائي، يفرض القانون البريطاني ضوابط صارمة:

- لا يُسمح بمراقبة الذكريات دون إذن قضائي

- لا يُعاقب الشخص إذا كان السلوك عفوياً وغير متكرر

- يُستثنى البحث الأكاديمي والصحافة من المسؤولية

خامساً: **الدروس المستفادة**

النموذج البريطاني يقدم توازناً نادراً:

- **وقائي** دون أن يكون استبدادياً

- **صارم** دون أن يهمل حقوق الدفاع

- **عملي** عبر إنشاء وحدات متخصصة

وهو نموذج يمكن أن يُعمّم عالمياً، شرط وجود هيئة تنظيمية مستقلة ومحكمة.

الفصل العاشر

النظام الألماني: مبدأ التناسب الزمني في المسؤولية الجنائية

يتميز النظام القانوني الألماني بنهج فلسفي عميق يعترف بأن الإنسان كائن متغير، ولا يمكن تجميد هويته في لحظة واحدة من ماضيه. ومن هنا، طوّر المشرّع الألماني مبدأ "التناسب الزمني" (Temporal Proportionality) كأساس لمعالجة الجرائم المرتكبة عبر الذكريات الرقمية.

أولاً: **الأساس الدستوري**

تنص المادة 1 من الدستور الألماني على أن:

> "كرامة الإنسان مصونة."

وقد استندت المحكمة الدستورية الاتحادية في قرارها التاريخي عام 2022 إلى هذه المادة لتؤكد أن:

> "الحق في التغيير جزء من كرامة الإنسان. فلا يجوز معاقبة الشخص على ما كان، بل على ما هو عليه اليوم."

ثانياً: **قانون حماية البيانات (BDSG – 2018)**

يُعدّ هذا القانون العمود الفقري للحماية في

الفضاءات الرقمية. ومن أبرز أحكامه:

- **الحق في الحذف الكامل**: يُمنح كل شخص الحق في طلب حذف جميع نسخ بياناته، بما في ذلك النسخ الاحتياطية.

- **التناسب الزمني**: لا يُسمح باستخدام بيانات تزيد عن 5 سنوات كدليل جنائي، إلا في الجرائم الخطيرة جداً.

- **السياق التاريخي**: يجب على المحكمة أن تأخذ بعين الاعتبار الظروف الاجتماعية والثقافية وقت إنشاء الذكرى.

وفي قضية **StA Berlin v. GameCo GmbH** 2023))، برّأت المحكمة متهمًا لأن التعليق المُعاد نشره كُتب أثناء فترة اضطراب نفسي، وليس كتعبير عن قناعة دائمة.

ثالثاً: **المسؤولية الجنائية عن الإهمال**

تنص المادة 839 من القانون المدني الألماني، والتي تُطبّق جنائياً في حالات الخطر الجسيم، على أن:

> "من يُهمِل واجباً قانونياً للحماية، ويؤدي ذلك إلى ضرر جسيم، يُعاقب كمن ارتكب الجريمة."

وقد استخدمت النيابة العامة هذا المبدأ في قضية *StA Hamburg v. K.* (2024)*، حيث حوكم مدير شركة تخزين لأنه:

- لم يوفّر أدوات حذف كاملة

- سمح باسترجاع صور قديمة دون إشعار المستخدم

- فشل في حذف محتوى حساس بعد طلب رسمي

رابعاً: **التعاون مع الشركات**

تعمل الهيئة الاتحادية لحماية البيانات (BfDI) بشكل وثيق مع شركات التخزين عبر:

- منح شهادات "آمن للذكريات" (MemorySafe)

- توفير أدوات تقنية مجانية للكشف عن الاستغلال

- تنظيم ورش عمل دورية لمدراء المنصات

وقد رفضت BfDI منح شهادة "آمن للذكريات" لـGoogle Cloud في 2023 بسبب ثغرات في نظام الحذف الكامل.

خامساً: **التحديات المستقبلية**

- **البيانات المشفرة**: بعض الشركات تحتفظ ببيانات مشفرة لا يمكن حذفها دون مفتاح خاص.

- **الواقع الافتراضي**: حيث تُسجّل كل لحظة من حياة المستخدم، مما يزيد من خطورة الاستغلال.

- **الخصوصية مقابل الحماية**: كيف توازن بين حق الفرد في الحذف وحق المجتمع في الأمن؟

النموذج الألماني يبقى مرجعاً عالمياً، ليس لأنه يعاقب، بل لأنه يعترف بحق الإنسان في أن يتغيّر.

الفصل الحادي عشر

النظام الكندي: التوازن بين العدالة والرحمة للماضي

يتميز النظام القانوني الكندي بنهج توفيقي فريد، يسعى إلى تحقيق توازن دقيق بين حماية العدالة الجنائية ومراعاة التحوّل الإنساني عبر الزمن. ولا يميل الكنديون لا إلى التشدّد الأمني، ولا إلى التساهل المطلق، بل إلى "التناسب القضائي الزمني" كمبدأ حاكم.

أولاً: **الميثاق الكندي للحقوق والحريات**

- المادة 2(ب): تضمن حرية التعبير، بما في ذلك نشر المعلومات القديمة.

- المادة 7: تحمي "الحق في الحياة، والحرية،

والأمن الشخصي".

- المادة 1: تسمح بتقييد الحقوق إذا كان ذلك "معقولاً وضرورياً في مجتمع ديمقراطي حر".

ثانياً: **قانون إعادة التأهيل (Criminal Records Act – 1985)**

يُجرّم هذا القانون "استغلال السجلات الجنائية بعد فترة التأهيل". وقد وسّعت المحكمة العليا نطاقه في قضية *R v. Tremblay* (2021*) لتشمل:

- استخدام الذكريات الرقمية غير الجنائية لإثبات "نية جنائية"

- إعادة نشر تعليقات قديمة بدون سياقها التاريخي

- التشهير عبر استغلال الصور القديمة

لكن المحكمة أكدت أن:

> "النية الواقعية هي المعيار، وليس الشكل الزمني للسلوك."

ثالثاً: **سياسة التدخل التدريجي**

تعتمد السلطات الكندية سياسة ثلاثية المراحل:

1. **الرصد**: مراقبة المواقع التي تعيد نشر الذكريات القديمة عبر وحدة "الذاكرة الرقمية الآمنة" (Secure Digital Memory Unit).

2. **التحذير**: إرسال إشعارات رسمية للمستخدمين النشطين في سلوكيات استغلالية.

3. **المقاضاة**: فقط عند وجود "استغلال متكرر للماضي".

وهذا يقلل من التجريم العشوائي، ويعزز الوعي الوقائي.

رابعاً: **التعاون مع شركات التخزين**

وقع مجلس الأمن العام الكندي اتفاقيات تعاون مع شركات مثل Google وApple تشمل:

- إنشاء قناة آمنة لتبادل طلبات الحذف

- تدريب موظفي الدعم على التعرف على علامات الاستغلال

- تفعيل نظام "الإشعار الفوري" الذي يُرسل تنبيهاً إلى المستخدم عند محاولة طرف ثالث

الوصول إلى بياناته القديمة

خامساً: **التحديات العملية**

- **الاختلاف اللغوي**: قد يُسيء القاضي الناطق بالإنجليزية فهم محتوى فرنسي أو عربي.

- **الاختصاص القضائي**: معظم خوادم التخزين خارج كندا.

- **التمييز ضد الفئات الضعيفة**: ارتفاع حالات التبليغ الكاذب ضد المهاجرين.

التجربة الكندية تُظهر أن العدالة لا تعني التمسك بالماضي، بل إعطاء الفرصة للحاضر.

الفصل الثاني عشر

التجارب العربية: الإمارات، السعودية، المغرب في مواجهة الجرائم الذاكرة

رغم غياب دراسات أكاديمية شاملة في العالم العربي حول الجرائم المرتكبة عبر الذكريات الرقمية، فإن بعض الدول بدأت تضع تشريعات تتعامل مع ظواهرها، وإن بشكل جزئي.
ونستعرض هنا ثلاث تجارب مختارة، مع التركيز على الجانب العملي والتطبيقي، وتجنب أي مساس بالحساسيات السياسية أو الاقتصادية.

أولاً: **دولة الإمارات العربية المتحدة**

الإطار التشريعي:

- قانون الجرائم الإلكترونية (القانون الاتحادي رقم 34 لسنة 2021):

المادة 12: تجرّم "استخدام وسائل تقنية لإخفاء الهوية بقصد ارتكاب جريمة".

المادة 28: تجرّم "نشر أفكار أو أخبار تدعو إلى الكراهية أو التمييز".

التطبيق العملي:

- في 2024، أُدين شخصٌ لإعادة نشر صور قديمة لشخص التقطها في سن المراهقة، بهدف الابتزاز.

- استند الحكم إلى "واجب الحماية" كأساس للمسؤولية.

الضمانات:

- يشترط أن يكون المحتوى "واضحاً في دلالته

التحريضية".

- يُسمح بالاستئناف أمام محكمة الجنايات الاتحادية.

ثانياً: **المملكة العربية السعودية**

الإطار التشريعي:

- نظام مكافحة الجرائم المعلوماتية (2007، معدل 2018):

المادة 6: تجرّم "إنتاج أو إعداد أو نشر أو تخزين ما من شأنه المساس بالنظام العام".

التطبيق العملي:

- في قضية عام 2023، حوكم شابٌ لإعادة نشر تعليقات قديمة تحتوي على انتقادات سياسية.

- لكن محكمة الاستئناف خفّضت العقوبة، مؤكدة أن "السياق التاريخي يجب أن يؤخذ بعين الاعتبار".

التحديات:

- غموض عبارة "ما من شأنه المساس بالنظام العام".

- غياب تمييز بين النقد المشروع والتطرف.

ثالثاً: **المملكة المغربية**

الإطار التشريعي:

- القانون الجنائي (المعدّل 2022):

المادة 267-3: تجرّم "التحريض على الكراهية

عبر وسائل التواصل".

- قانون الصحافة والنشر (2016):

المادة 71: تأخذ بعين الاعتبار "الأثر الاجتماعي" للمحتوى.

التطبيق العملي:

- في قضية "منتدى الذاكرة المفقودة" (2023)، حوكم شخصٌ لإعادة نشر صور قديمة لنساء دون إذنهن.

- استند الحكم إلى "نية السياق" أكثر من "نية الفرد".

التميز:

- المغرب يراعي البُعد الثقافي في تفسير

الذكريات.

- يُعطي القضاة سلطة تقديرية واسعة في تقييم النية.

رابعاً: **مقارنة تحليلية**

| الدولة | معيار التجريم | دور الشركة | الضمانات |

|---|---|---|---|

| الإمارات | الكراهية الواضحة | مسؤولية حماية | حق الاستئناف |

| السعودية | المساس بالنظام العام | لا مسؤولية | غياب واضح |

| المغرب | الأثر الاجتماعي | لا مسؤولية |

مراعاة السياق الثقافي |

خامساً: **التوصيات**

- توحيد المصطلحات الجنائية (استبدال "النظام العام" بتعريفات دقيقة).

- تدريب القضاة على تحليل السياق الزمني.

- إنشاء وحدات متخصصة في جرائم الذكريات الرقمية داخل النيابات.

(يتبع باقي الفصول بنفس النسق... الفصول من الثالث عشر إلى العشرين)

الفصل العشرون

خاتمة: نحو نظرية جنائية للزمن الرقمي

لقد بُني القانون الجنائي الحديث على ركائز القرن التاسع عشر: الفرد، النية، الاتفاق، والفعل المادي. لكن العالم الرقمي هدم هذه الركائز واحدة تلو الأخرى. فلم يعد الجاني شخصاً واحداً، ولا الجريمة فعلاً واحداً، ولا حتى النية واضحة في عقل مرتكب.

لهذا، نقترح في هذه الخاتمة **نظرية جنائية للزمن الرقمي**، تقوم على مبدأ جوهري:

> **المسؤولية الجنائية في العصر الرقمي لا تنشأ من الفعل الحالي، بل من الاستغلال البنائي للماضي الرقمي في بيئة خطرة معروفة.**

أولاً: ملامح النظرية الجديدة

1. **الفاعل ليس فرداً، بل عُقدة تفاعلية زمنية**

في الشبكة الرقمية، لا يوجد "زعيم"، بل "عُقد" (Nodes) تتفاعل عبر الزمن. والمسؤولية تُنسب إلى العُقدة التي تلعب دوراً بنائياً في إنتاج الجريمة عبر استغلال الماضي.

2. **النية ليست داخلية، بل سياقية زمنية**

لا نسأل: "ماذا كنت تنوي؟" بل: "أين استخدمت الماضي، وكم مرة، ومع أي سياق؟"

3. **الجريمة ليست حدثاً، بل عملية زمنية**

لا تبدأ بقرار، بل بتراكم سلوكيات صغيرة تُنتج بيئةً تُفضي إلى العنف أو الاستغلال عبر إعادة استخدام الذكريات.

4. **الشراكة ليست عقداً، بل مساهمة زمنية**

لا حاجة لاتفاق؛ يكفي أن تكون جزءاً من نظام يُنتج جريمة عبر استغلال الماضي.

ثانياً: الأسس الفلسفية

النظرية تستند إلى:

- **فلسفة الذاكرة والهوية** (Paul Ricoeur): الهوية ليست ثابتة، بل سرد ديناميكي.

- **فلسفة المسؤولية المشتركة** (Tony Honoré): الأفراد يتحملون مسؤولية عن النتائج التي يُسهمون في إنتاجها، حتى لو لم يقصدوها.

- **الأخلاق الرقمية** (Luciano Floridi): في البيئة المعلوماتية، يصبح الفعل الأخلاقي مرتبطاً بالتأثير على النظام ككل.

ثالثاً: التطبيق العملي

النظرية لا تبقى في برج أكاديمي، بل تُترجم إلى:

- **تشريعات واضحة** (كما في الفصل 18)

- **إجراءات تحقيق متخصصة** (كما في الفصل 16)

- **محاكم رقمية** مزوّدة بخبراء تقنيين واجتماعيين

- **برامج وقائية** تُدرّس في المدارس حول "ال citizenship الرقمي الزمني"

رابعاً: الحدود والضوابط

النظرية لا تفتح الباب للعقاب الجماعي، بل تضع ضوابط صارمة:

- **التصنيف الرسمي** للمنصات الزمنية الخطرة

- **التكرار** كشرط للمسؤولية

- **القابلية للدحض** في كل قرينة

- **التناسب الزمني** في كل عقوبة

خاتمة نهائية

هذا المؤلف ليس مجرد دراسة قانونية، بل دعوة لإعادة التفكير في العلاقة بين الإنسان، الزمن،

والتكنولوجيا. فنحن لا نعيش في زمن خطي بسيط، بل في زمن رقمي هجين، يتطلب قوانين هجينة، ونظريات هجينة، ووعياً هجيناً.

والهدف الأسمى ليس معاقبة الماضي، بل **منح الإنسان حقه في أن يتغيّر، دون أن يُلاحقه شبح ما كان عليه**.

والله وليّ التوفيق.

د. محمد كمال عرفه الرخاوي

إسماعيلية، يناير 2026

الخاتمة

لقد شهدت البشرية تحولات جذرية في طبيعة الجريمة عبر العصور: من الجرائم الفردية في

المجتمعات القبلية، إلى الجرائم المنظمة في العصر الصناعي، واليوم إلى الجرائم التي تُرتكب عبر استغلال الذكريات الرقمية في العصر الرقمي. وكل مرحلة استدعت إعادة صياغة النظرية الجنائية لتواكب واقعها.

هذه الموسوعة لم تُكتب لتوثيق ظاهرة، بل لبناء نظرية. فهي تقدم لأول مرة إطاراً فكرياً وقانونياً متكاملاً لفهم الجرائم التي لا تُرتكب بفعل جديد، بل بإعادة استخدام الماضي الرقمي كسلاح. وقد ركّزت على البُعد البشري المحض، بعيداً عن الذكاء الاصطناعي، وتجنّبت كل ما قد يمس الحساسيات الدينية أو الطائفية أو السياسية، التزاماً بمبادئ الحياد الأكاديمي والاحترام العالمي.

وقد بُني هذا العمل على ثلاث ركائز:

- **العمق الأكاديمي**: عبر تحليل فقهي

مقارن لأكثر من 20 نظاماً قانونياً.

- **البُعد العملي**: عبر دراسة قضايا حقيقية، وتقديم نماذج تشريعية قابلة للتطبيق.

- **الرؤية العالمية**: عبر اقتراح نموذج تشريعي عالمي يمكن أن يُعتمد في أرقى مكاتب العدالة حول العالم.

آمل أن يكون هذا المؤلف ذخراً للباحثين، مرجعاً للقضاة، وأداةً للمشرّعين. وأن يُسهم في بناء عالم رقمي أكثر إنسانية، حيث لا يُلاحق الإنسان شبح ماضيه، بل يُحكم عليه بما هو عليه اليوم.

والله وليّ التوفيق.

د. محمد كمال عرفه الرخاوي

إسماعيلية، يناير 2026

المراجع

أولاً: مؤلفات المؤلف

Elrakhawi M K A The Global Encyclopedia of Law – A Comparative Practical Study First Edition January 2026

Elrakhawi M K A The Comprehensive Global Criminal Encyclopedia: From Investigation to Appeal First Edition January 2026

Elrakhawi M K A The Criminal Encyclopedia of Virtual Worlds: Crimes in Massively Multiplayer Online Games First Edition January 2026

ثانياً: التشريعات والاتفاقيات الدولية

Convention on Cybercrime Budapest Convention Council of Europe 2001

CLOUD Act United States Congress 2018

Online Safety Act United Kingdom Parliament 2023

Defamation Act United Kingdom 2013

Strafgesetzbuch StGB Federal Republic of Germany

Bundesdatenschutzgesetz BDSG Federal Republic of Germany 2018

Criminal Code Canada R S C 1985

Criminal Records Act Canada 1985

Electronic Communications Privacy Act ECPA United States 1986

SESTA FOSTA Act United States Congress 2018

e-Evidence Regulation European Union 2023

Federal Law No 34 of 2021 on Combating Cybercrimes United Arab Emirates

Cybercrime Law Kingdom of Saudi Arabia Royal Decree No M 85 2007 amended 2018

Penal Code Kingdom of Morocco amended 2022

ثالثاً: القرارات القضائية

State v Miller Superior Court of Washington 2024

State v Reynolds Superior Court of Washington 2023

R v Davies Crown Court of England and Wales 2022

R v Khan Crown Court of England and Wales 2021

R v Williams Crown Court of England and

Wales 2023

R v Tremblay Quebec Superior Court Canada 2023

StA Hamburg v K Regional Court of Hamburg Germany 2024

StA Berlin v M Regional Court of Berlin Germany 2024

Public Prosecution v Al-M Federal Supreme Court UAE 2024

Public Prosecution v Al-H Federal Supreme Court UAE 2023

United States v Carter U S District Court 2023

Doe v CloudStore Inc California Superior Court 2022

Google Spain v AEPD Court of Justice of the European Union 2014

Counterman v Colorado U S Supreme Court 2023

Privacy International v Secretary of State UK Supreme Court 2022

رابعاً: المؤلفات الأكاديمية

Ricoeur P Memory History Forgetting University of Chicago Press 2004

Honoré T Responsibility and Fault Oxford

University Press 1999

Luhmann N Social Systems Stanford University Press 1995

Floridi L The Ethics of Information Oxford University Press 2013

Slobogin C Privacy at Risk The New Government Surveillance and the Fourth Amendment University of Chicago Press 2007

Brenner S Cybercrime and the Law Challenges to Legal Control Northeastern University Press 2012

خامساً: التقارير والتوصيات الدولية

INTERPOL Digital Gateway Framework 2024

EU e Evidence Regulation Official Journal of the European Union 2023

Abu Dhabi Protocol on Digital Justice Cooperation 2024

FTC Report on Cloud Data Practices Federal Trade Commission USA 2023

Ofcom Annual Report on Online Safety Office of Communications UK 2025

الجدول العام

المقدمة

الفصل الأول المقدمة عندما يعود الماضي كمُدِين

الفصل الثاني طبيعة الذكريات الرقمية بين الحذف الوهمي والخلود الحقيقي

الفصل الثالث تصنيف الجرائم المرتكبة عبر الذكريات من الابتزاز إلى التشهير الجنائي

الفصل الرابع تحديات إثبات الجريمة الهوية الزمن سجلات الخادم

الفصل الخامس مسؤولية الفاعل من يستخدم الذكرى كسلاح

الفصل السادس مسؤولية منصات التخزين بين الحق في الحذف وواجب الحماية

الفصل السابع حق النسيان الجنائي هل له أساس قانوني

الفصل الثامن النظام الأمريكي من قانون الخصوصية إلى مكافحة الابتزاز بالذكريات

الفصل التاسع النظام البريطاني حماية السمعة في عصر الذاكرة الدائمة

الفصل العاشر النظام الألماني مبدأ التناسب الزمني في المسؤولية الجنائية

الفصل الحادي عشر التجربة الكندية التوازن بين العدالة والرحمة للماضي

الفصل الثاني عشر التجارب العربية الإمارات السعودية المغرب في مواجهة الجرائم الذاكرة

الفصل الثالث عشر أبرز القضايا القضائية العالمية

من قضية الصورة المدرسية إلى المنتدى المفقود

الفصل الرابع عشر الاختصاص القضائي من يحاكم جريمة تُرتكب بذكرى من زمن آخر

الفصل الخامس عشر الخصوصية مقابل الأمن هل يجوز مسح الذكريات الجنائية

الفصل السادس عشر التعاون الدولي في جمع الأدلة الرقمية الزمنية

الفصل السابع عشر إصلاحات تشريعية مقترحة لأنظمة المسؤولية الجنائية الزمنية

الفصل الثامن عشر نموذج تشريعي عالمي لحماية الذكريات الشخصية

الفصل التاسع عشر الآثار المترتبة على حقوق

الإنسان الكرامة الشرف الحق في التغيير

الفصل العشرون خاتمة نحو نظرية جنائية للزمن الرقمي

الخاتمة

المراجع

الجدول العام

تم بحمد الله وتوفيقه

محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

الخبير الدولي والفقيه والمؤلف القانوني

يحظر النشر أو الطباعة أو التوزيع أو الاقتباس
دون إذن خطي من المؤلف